SonicWall™ SonicOS 6.5 系統安裝

管理

SONICWALL™

目錄

部分 1

關於系統安裝

- 關於設定您的 SonicOS 系統

1

關於設定您的 SonicOS 系統

關於 SonicOS 管理介面

基於 Web 的 SonicOS 管理介面可讓您設定搭載 SonicOS 6.5 的 SonicWall 網路安全設備 (防火牆):

SuperMassive 9600	NSA 6600	TZ600	SOHO Wireless
SuperMassive 9400	NSA 5600	TZ500/TZ500 Wireless	
SuperMassive 9200	NSA 4600	TZ400/TZ400 Wireless	
	NSA 3600	TZ300/TZ300 Wireless	
	NSA 2650		
	NSA 2600		

附註：本文件可能包含有關未在特定國家或地區發行之平台/版本的說明。

SonicOS 提供易於使用的圖形化管理介面，方便您設定自己的 SonicWall 安全設備。如需動態管理介面和相關功能資訊 (例如工具提示和動態表格)，請參閱*關於 SonicOS 指南*。

這份指南提供的設定相關說明包括:

- 密碼、登入安全、Web 管理、憑證和排程。
- 使用者驗證、群組、來賓服務和帳戶及分割。
- 網路設定，例如介面、區域和路由。
- 切換 VLAN 主幹、L2 探索、連結彙總和連接埠鏡像設定。
- 高可用性。
- WAN 加速。
- VOIP。
- 虛擬輔助。

如需設定相關資訊	請參閱
連線能力: VPN、SSL VPN、SonicPoint/SonicWave、無線	*SonicOS 連線能力*
原則: 存取規則、NAT 原則和所有物件，例如位址、mach 和頻寬	*SonicOS 原則*
授權、更新韌體及備份/重新啟動系統	*SonicOS 更新*
監控: 儀表板、威脅防護、流量、擷取 ATP	*SonicOS 監控*

如需設定相關資訊	請參閱
安全性: 安全設備設定、安全服務、反垃圾郵件、深度封包偵測 (DPI)	*SonicOS 安全設定*
記錄和報告：AppFlow 設定、記錄、法律資訊	*SonicOS 記錄和報告*
快速設定	*SonicOS 快速設定*

部分 2

設備

- 配置基本設定
- 管理 SNMP
- 管理憑證
- 設定時間設定
- 設定排程

2

配置基本設定

關於設備 | 基本設定

管理 | 系統安裝 | 設備 | 基本設定提供各種設定，可讓您為 SonicWall 安全設備配置各種安全和遠端管理功能。

您可以使用包括 HTTPS、SNMP 或 SonicWall 全球管理系統 (SonicWall GMS) 在內的多種方法來管理防火牆。

附註：若要將所有變更套用到 SonicWall 裝置，按一下**接受**；會在瀏覽器視窗的底部顯示一條確認更新的訊息。

存取設備 | 基本設定頁面:

1 按一下**管理**，隨即會顯示**管理**檢視。
2 按一下**系統設定**下方的**設備**，展開瀏覽窗格。
3 按一下**基本設定**。

主題：

- 第 18 頁「設定防火牆名稱」
- 第 19 頁「更改管理員名稱和密碼」

- 第 19 頁「設定登入安全」
- 第 22 頁「設定多管理員存取權」
- 第 26 頁「啟用進階稽核記錄支援」
- 第 26 頁「設定管理介面」
- 第 31 頁「設定前方面板管理介面 (僅限 SuperMassive 防火牆)」
- 第 32 頁「設定用戶端憑證檢查」
- 第 35 頁「檢查憑證有效期限」
- 第 35 頁「設定 SSH 管理」
- 第 36 頁「設定進階管理選項」
- 第 38 頁「手動下載 SonicPoint 映像」
- 第 39 頁「選取語言」

設定防火牆名稱

若要設定防火牆名稱:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 防火牆名稱**。

2 在**防火牆名稱**欄位中，輸入防火牆的序號 16 進位)。這組號碼專門用於識別 SonicWall 安全裝置，預設名稱為防火牆的序號。此序號也是裝置的 MAC 位址。如需變更**防火牆名稱**，請在**防火牆名稱**欄位中輸入專屬的英數字元名稱。此名稱必須至少包含 8 個字元，最多可包含 63 個字元。

3 如需在活動記錄中輕鬆識別主要/次要防火牆，請勾選**自動在防火牆名稱中附加 HA/叢集尾碼**。啟用這個選項後，系統就會在**調查**檢視中的**記錄 > 事件記錄**內，自動為防火牆名稱附加適用的尾碼。

- 主要的
- 備用
- 主要節點 *<節點編號>*
- 次要節點 *<節點編號>*

預設情況下未勾選此選項。如需更多事件紀錄的相關資訊，請參閱 *SonicOS 調查*。

4 在**防火牆網域名稱**欄位中輸入一個好記的名稱。這個名稱可以是專供內部使用者使用的名稱或外部註冊的網域名稱。這個網域名稱可以搭配**系統設定 | 使用者 > 設定**檢視中的**使用者 Web 登入設定**使用，提供使用者驗證重新導向。如需更多使用者 Web 登入設定的相關資訊，請參閱配置使用者 Web 登入設定 (第 XXX 頁)。

更改管理員名稱和密碼

每部 SonicWall 安全設備都有預設的管理員名稱 (admin) 和密碼 (password)。如果您還沒有參照初始設定指南或啟動指南，或者快速設定指南的說明更改密碼，我們強烈建議您馬上進行修改。檢閱者問題: 可以更改管理員名稱嗎？

若要更改管理員名稱和/或密碼:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 管理員名稱與密碼**。

2 在**管理員名稱**欄位中輸入新的名稱。**管理員名稱**可以從預設值 **admin** 變更為使用最多 32 個英數字元的任何字串。

3 按一下**接受**。

若要為 SonicWall 管理介面存取設定新密碼:

1 在**舊密碼**欄位中輸入舊密碼。

2 在**新密碼**欄位中輸入新密碼。新密碼最長可以是 32 個英數字元加特殊字元的組合。

> ⓘ **重要：**推薦將預設密碼 **password** 變更為您自己的自訂密碼。輸入一個其他人不容易猜到的強式密碼。一個強式密碼應該至少包含一個大寫字母、一個小寫字母、一個數字和一個特殊字元。例如 `MyP@ssw0rd`。

3 在**確認密碼**欄位中再次輸入新密碼。

4 按一下**接受**。

設定登入安全

交涉 HTTPS 管理工作階段時，內部 SonicOS Web 伺服器支援 TLS 1.1 和帶有複雜密碼 (128 位元或以上) 的 TLS 1.1 以上版本。不過不支援 SSL 實作。此增強的 HTTPS 安全級別可防止潛在的 SSLv2 回復漏洞，並確保符合支付卡行業 (PCI) 標準及其他安全和風險管理標準。

> ⓘ **提示：**SonicOS 使用大部分最新瀏覽器支援的 HTML5 等進階瀏覽器技術。SonicWall 推薦使用最新版的 Chrome、Firefox、Internet Explorer 或 Safari (不在 Windows 平台上運作) 瀏覽器來管理 SonicOS。不建議以行動裝置瀏覽器管理 SonicWall 系統。

設定 SonicOS 密碼限制強制措施，可確保管理員和使用者都能使用安全可靠的密碼。此密碼限制強制措施可滿足最新資訊安全管理系統所規定的保密性要求或通用標準和支付卡行業 (PCI) 標準等合規性要求。

主題：

- 第 20 頁「設定密碼規範」
- 第 21 頁「設定登入限制」

設定密碼規範

若要設定密碼規範:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 登入安全**。

2 若要要求使用者在指定的天數過後更改密碼:

a 選取**變更密碼的間隔天數**。將啟用此欄位。預設情況下未勾選此選項。

b 在這個欄位中輸入間隔時間。預設天數為 **90** 天，最短為 1 天，最多為 9999 天。

當使用者嘗試使用已過期的密碼登入時，系統會顯示彈出式視窗，提示使用者輸入新密碼。**使用者登入狀態**視窗現在包含一個**變更密碼**按鈕，以便使用者隨時變更其密碼。

3 若要指定密碼變更的最短間隔時間 (以小時為單位):

a 選取**密碼變更的間隔時數 (小時)**。將啟用此欄位。預設情況下未勾選此選項。

b 輸入小時數。最短時數和預設時數皆為 **1** 小時；最長為 9999 小時。

4 若要要求使用者在指定的密碼變更次數內必須使用非重複密碼:

a 選取**在限定次數內不能使用重複密碼**，這個欄位會隨即啟用。 預設情況下未勾選此選項。

b 輸入變更次數。預設的次數為 **4** 次，下限為 1 次，上限為 32 次。

5 如需要求使用者在建立新密碼時，至少需變更舊密碼中的 8 個英數/符號字元，請選取**新密碼中必須有 8 個字元與舊密碼不同**。如需瞭解如何指定可用的字元，請參閱步驟 7。

6 如需指定允許的最短密碼長度，請在**限定最短密碼長度**欄位中輸入字元數下限。預設字元數為 **8** 個字元，最少為 1 個字元，最多為 99 個字元。

7 在**限定密碼複雜度**下拉功能表中選擇使用者密碼必須具備的複雜程度:

- **無**（預設值）
- **必須有字母和數字字元**
- **必須有字母、數字和符號字元** - 對於符號字元，只允許使用 **!**、**@**、**#**、**$**、**%**、**^**、**&**、*、**(** 和 **)**；任何其它符號字元都不允許使用。

8 您將密碼複雜度選項設定為**無**時，**複雜度需求**中的選項即可供使用。輸入使用者密碼中必須使用的英數字元和符號字元數下限。每種字元的預設字元數皆為 **0**，不過所有選項的總字元數不得超過 99。

- **大寫字元**
- **小寫字元**
- **數字**
- **符號**

附註：只有在您選取了**必須有字母、數字和符號字元**時，才可使用**符號字元**欄位。

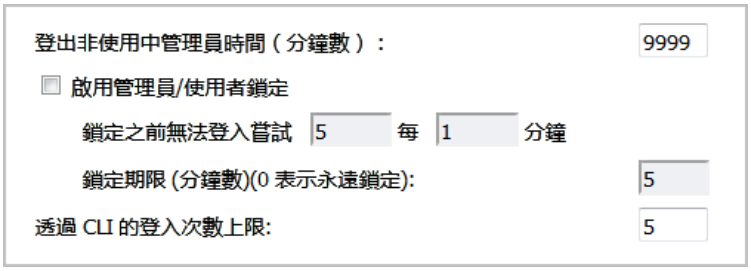
9 在**為指定目標套用上述密碼限制**下，選擇要為哪些使用者類別套用密碼限制。根據預設，系統會選取下列所有選項:

- **管理員** - 指的是有使用者名稱 **admin** 的預設管理員。
- **其他的完全權限的管理員**
- **限制的管理員**
- **來賓管理員**
- **其他的本機使用者**

設定登入限制

若要設定登入限制:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 登入安全**。



2 如需指定系統將您登出管理介面前允許的非使用狀態時間長度，請在**處於非使用狀態的管理員遭系統登出的時限 (分鐘)** 欄位中輸入所需時間 (以分鐘為單位)。預設情況下，SonicWall 安全裝置會在管理員保持非使用中狀態 **5** 分鐘後登出管理員。非使用中逾時的設定範圍為 1 到 9999 分鐘。

ⓘ **提示：**如果「管理員非使用狀態逾時」設定的時間超過 5 分鐘，請按一下檢視畫面右上角的**登出**來結束每個管理工作階段，以避免發生未經授權存取防火牆管理介面的情況。

3 如需將 SonicWall 安全設備設定為在登入憑證有誤時鎖定管理員或使用者，請選取**啟用管理員/使用者鎖定**。在達到指定的嘗試登入失敗次數後，管理員和使用者都會遭到鎖定，無法存取防火牆。預設已停用此選項。這個選項啟用後，下列欄位將可供使用。

△ **注意：如果管理員和某個使用者使用相同的來源 IP 位址登入防火牆，防火牆也會鎖定管理員。鎖定操作基於此使用者或管理員的來源 IP 位址。**

a 在第一個**遭鎖定前每分鐘允許的嘗試登入失敗次數**欄位中，輸入指定時間範圍內允許的嘗試失敗次數，使用者達到上限後即會遭到鎖定。預設次數為 **5** 次，最少為 1 次，最多為 99 次。

b 輸入允許嘗試失敗的時數上限。預設值為 **5** 分鐘，最短為 1 分鐘，最長為 240 分鐘 (4 小時)。

c 在**鎖定期限 (分鐘數)**欄位中，輸入使用者再次嘗試登入防火牆前必須等待的時間長度。預設值為 **5** 分鐘，最短為 0 分鐘 (永久鎖定)，最長為 60 分鐘。

4 在**透過 CLI 的嘗試登入次數上限**欄位中，輸入從會觸發鎖定操作的命令行介面 (CLI) 登入時，允許的嘗試登入錯誤次數。預設值為 **5**，最小值為 3，最大值為 15。

5 按一下**接受**。

設定多管理員存取權

SonicOS 支援多個並行管理員 (具備完整管理員權限、唯讀權限和有限權限的管理員)。

主題：

- 第 22 頁「關於多管理員支援」
- 第 25 頁「設定多管理員存取權」

關於多管理員支援

主題：

- 第 23 頁「什麼是多管理員支援？」
- 第 23 頁「優點」
- 第 23 頁「多管理員支援的工作方式」

什麼是多管理員支援？

初始版本的 SonicOS 僅支援具有完全管理權限的一個管理員登入防火牆。可授予附加使用者「有限管理員」存取權限，但一次只能有一個管理員有修改 SonicOS GUI 的所有區域的完全權限。

SonicOS 支援多個並行管理員。此功能允許具有完全管理權限的多個使用者登入。除了使用預設的 **admin** 使用者名稱，可以建立附加的管理員使用者名稱。

由於多個管理員同時進行設定變更可能存在衝突，只允許一個管理員進行設定變更。授予附加管理員對 GUI 的完全權限，但不能進行設定變更。

優點

多管理員支援具有以下優點：

提升生產力	同時允許多個管理員存取防火牆，之前當兩個管理員同時要存取裝置時，會強制登出其中一個管理員。
減少設定風險	新的唯讀模式允許使用者查看防火牆的目前設定和狀態，而沒有無意變更設定的風險。

多管理員支援的工作方式

主題：

- 第 23 頁「設定模式」
- 第 24 頁「使用者群組」
- 第 25 頁「先佔管理員的優先順序」
- 第 25 頁「GMS 和多管理員支援」

設定模式

為了允許多個並行管理員，同時避免多個管理員同時變更設定時可能造成的衝突，我們定義了下列設定模式:

設定模式	管理員具備完整的設定編輯權限。如果沒有管理員已登入到裝置，這是有完全和有限管理員權限的管理員（但非唯讀管理員）的預設行為。 **附註：**有完全設定權限的管理員也可以使用命令行介面 (CLI) 登入 (CLI；請參閱 *SonicOS 6.5 CLI 參考指南*)。
唯讀權限	管理員不能對設定作任何變更，但可以查看整個管理 UI 和執行監控操作。 僅向屬於 **SonicWall Read-Only Admins** 使用者群組的管理員授予唯讀存取權限，這是他們可以存取的唯一設定模式。
非設定模式	管理員可以查看與唯讀群組成員能查看的相同資訊，他們還可以啟動不可能導致設定衝突的管理操作。 只有隸屬於 **SonicWall 管理員**使用者群組的管理員可以使用非設定模式。在另一名管理員已處於設定模式，且新管理員選擇不先佔已有管理員時，可以進入這種模式。預設情況下，當管理員受到先佔退出設定模式，將其轉入非設定模式。在**系統 > 管理**頁面，可以修改這種行為登出先前的管理員。

設定模式可獲得的存取權限表格提供設定模式可獲得的存取權限的摘要。還列出了有限管理員的存取權限，但注意本表格並不包含有限管理員可用的所有功能。

設定模式可獲得的存取權限

功能	設定模式的完全權限管理員	非設定模式的完全權限管理員	唯讀管理員	有限管理員
匯入憑證	X			
產生憑證簽名請求	X			
匯出憑證	X			
匯出裝置設定	X	X	X	
下載 TSR	X	X	X	
使用其他診斷	X	X		X
設定網路	X			X
排清 ARP 快取	X	X		X
設定 DHCP 伺服器	X			
重新交涉 VPN 通道	X	X		
登出使用者	X	X		僅 X 來賓使用者
解鎖登出的使用者	X	X		
清除記錄	X	X		X
篩選記錄	X	X	X	X
匯出記錄	X	X	X	X
通過電子郵件傳送記錄	X	X		X
設定記錄類別	X	X		X
設定記錄設定	X			X
產生記錄報告	X	X		X
瀏覽完整 UI	X	X	X	
產生記錄報告	X	X		X

使用者群組

多管理員支援功能支援兩個新的預設使用者群組：

SonicWall 管理員	此群組的成員具有編輯設定的完全管理員權限。
SonicWall 唯讀管理員	此群組的成員具有查看完整管理介面的唯讀權限，但不能編輯設定，且不能切換到完全設定模式。

不建議將使用者包含在多個使用者群組中。不過如果您決定這樣做，則需遵循以下行為模式:

如果這個使用者群組的成員	是
SonicWall 管理員	同時隸屬於**受限管理員**或 **SonicWall 唯讀管理員**使用者群組，成員即具備完整的管理員權限。
限制的管理員	隸屬於 **SonicWall 唯讀管理員**使用者群組，成員即具備有限的管理員權限。
唯讀管理員	稍後被納入其他管理群組，則將由 **SonicWall 唯讀管理員**群組設定中的**如果這個唯讀管理員群組搭配其他管理群組使用**選項，決定成員是否仍僅限於擁有唯讀存取權，或者具備其他群組所設定的完全管理權限。

先佔管理員的優先順序

以下規則控管的是當需要對已登入裝置的管理員進行先佔時，各類管理員所具備的優先順序層級:

1 **admin** 使用者和 SonicWall 全域管理系統 (GMS) 都有最高優先順序，且可以先佔任何使用者。

2 屬於 **SonicWall Administrators** 使用者群組的使用者可以先佔任何使用者，**admin** 和 SonicWall GMS 除外。

3 屬於 **Limited Administrators** 使用者群組的使用者只能先佔 **Limited Administrators** 群組中的其他成員。

GMS 和多管理員支援

在使用 SonicWall GMS 管理防火牆時，GMS 頻繁登入裝置（用於確保已正確建立 GMS 管理 IPSec 通道等活動）。這些頻繁的 GMS 登入可能有礙裝置的本機管理，因為 GMS 可能先佔本機管理員。

設定多管理員存取權

若要設定多管理員存取權:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 多管理員**。

2 如需設定某名管理員先占另一名管理員所發生的情況時，請透過**其他管理員先佔**選項，決定遭到先占的管理員是否能夠轉換至非設定模式或登出:

如需允許下列操作	選擇
允許多個管理員以非設定模式存取裝置，而不會干擾其他管理員。預設情況下未勾選此選項。	**轉入非設定模式**
新的管理員會先占其他工作階段。 **附註：**選擇**登出**將停用非設定模式，且還會封鎖手動進入非設定模式。	**登出**

3 如需允許優先權較低的管理員在指定時間後可以對目前的管理員進行先占，請在**允許優先權較低的管理員進行先佔的非使用狀態時間長度 (分鐘)**欄位中輸入所需時間 (以分鐘為單位)。預設值為 **10** 分鐘，最短為 1 分鐘，最長為 9999 分鐘。

4 SonicOS 管理介面允許管理員透過管理介面傳送文字訊息給其他已登入設備的管理員。訊息會顯示在在瀏覽器的狀態列中。預設情況下未勾選此選項。 若要啟用這個選項:

   a 選取**啟用管理員內部通訊**。**訊息輪詢頻率 (秒數)**欄位隨即可供使用。

   b 在**訊息輪詢頻率 (秒數)** 欄位中指定管理員的瀏覽器檢查管理員內部訊息的頻率。特別是在可能有多位管理員需要存取裝置時，可縮短間隔，確保能夠及時傳送訊息。預設值為 **10** 秒，最小值為 1 秒，最大值為 99 秒。

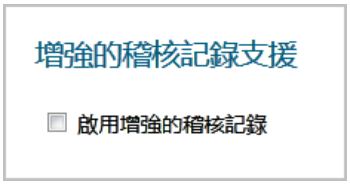
5 如需授予管理員、加密 (Crypto) 管理員和審核管理員存取權，請選取**啟用多重管理規則**。停用這個選項時，這些管理員便無法存取系統，也看不到所有相關的使用者群組和群組資訊。預設情況下未勾選此選項。

啟用進階稽核記錄支援

進階記錄項目包括**調查 | 記錄 > 事件記錄**頁面中的參數異動和使用者名稱。如需進一步的記錄相關資訊，請參閱 *SonicOS 調查*。

若要在調查 | 記錄 > 事件記錄頁面中啟用設定變更記錄功能:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 進階稽核記錄支援**。



2 選取**啟用進階稽核記錄**。預設情況下未勾選此選項。

3 按一下**接受**。

設定管理介面

您可以在這個部分中設定:

- 管理介面表格的顯示方式。
- 憑證使用情形。
- 要作為起始頁面的頁面。
- 您是否在設定或非設定模式下進行操作。
- 工具提示行為。
- 其他管理選項。

主題：

透過 HTTP 或 HTTPS 進行管理作業

您可以使用 HTTP 或 HTTPS 和 Web 瀏覽器管理 SonicWall 安全設備。預設已停用基於 Web 的 HTTP 管理。請使用 HTTPS 登入已設有原廠預設值的 SonicOS 管理介面。

若要透過 HTTP 或 HTTPS 進行管理:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。

2 如需在全域啟用 HTTP 管理，請選取**允許透過 HTTP 管理**。 預設情況下未勾選此選項。

3 HTTP 的預設連接埠為連接埠 **80**，也可以設定通過其他連接埠存取。在 **HTTP 連接埠**欄位中輸入所需的連接埠號碼。

> **重要：**如果設定了另一個連接埠用於 HTTP 管理，則在使用 IP 位址登入 SonicWall 安全裝置時，必須包含此連接埠號。舉例來說，如果將連接埠設定為 76，則必須在 Web 瀏覽器中輸入 *LAN IP Address*:76 (例如 http://192.18.16.1:76)。

4 用於 HTTPS 管理的預設連接埠為 **443**。如需變更預設連接埠，在登入 SonicWall 安全設備時更添一層保護，請在 **HTTPS 連接埠**欄位中輸入所需的連接埠號碼。

> **重要：**如果您設定了其他連接埠作為 HTTPS 管理埠，則當您使用 IP 位址登入 SonicWall 安全設備時，必須納入這個連接埠號碼。例如，如果您將連接埠設定為 700，則必須使用這個連接埠號碼和 IP 位址 (例如 https://192.18.16.1:700) 登入 SonicWall。

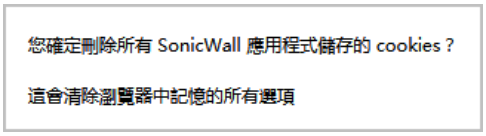
刪除瀏覽器 Cookie

> **重要：**刪除 Cookie 會導致您失去所有尚未儲存的管理介面變更。

若要刪除安全設備儲存的所有瀏覽器 Cookie:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。

2 按一下**刪除 Cookie**。將顯示確認訊息。



3 按一下**確定**。系統自您上次刪除 Cookie 後所儲存的所有 Cookie 都會遭到刪除。

切換設定模式

每部設備都包含**模式**選項，可供您切換管理介面的設定模式。如果您處於設定模式，則隨時可以切換至非設定模式；如果您處於非設定模式，則可切換至設定模式。

提示：除了在每個檢視的**模式**設定中切換模式外，您也可以運用這個方法來切換模式。如需各模式的更多相關資訊，請參閱*關於 SonicOS 指南*。

若要切換模式:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。

2 如果您處於:

- 設定模式，請按一下**結束設定模式**。按鈕將變更為:

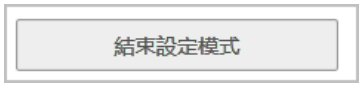
  頁面右上方的**模式**指示器會顯示為**非設定**:

  如果您嘗試儲存任一檢視中的任何變更，系統會顯示下列錯誤訊息:

- 非設定模式，請按一下**設定模式**。按鈕將變更為:

  頁面右上方的**模式**指示器會顯示為**設定**:

您不需要按一下**接受**。

3 若要返回原本的模式:

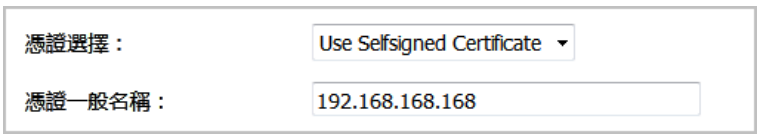
- 如要返回設定模式，請按一下**設定模式**。
- 如要返回非設定模式，請按一下**結束設定模式**。

選取安全憑證

安全憑證可提供資料加密和安全的網站。

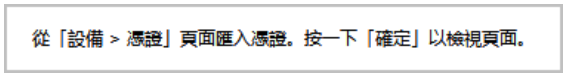
若要指定安全憑證的類型:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。



2 在**選擇憑證**下拉功能表中，選擇您的網站要使用的憑證類型:

- **使用自行簽署的憑證**，可讓您持續使用某個憑證，不用每次登入 SonicWall 安全設備時都必須下載新憑證。預設情況下已核取此選項。移至步驟 3。
- **匯入憑證**可讓您透過**設備 > 憑證**頁面選取已匯入的憑證，用來驗證管理介面。將顯示確認訊息：



a) 按一下**確定**。即顯示**設備 > 憑證**頁面。

b) 移至設備憑證。

3 在**憑證常用名稱**欄位中，輸入防火牆的 IP 位址或常用名稱。如果您選擇的是 **use selfsigned certificate**，SonicOS 會在這個欄位中輸入防火牆的 IP 位址。

4 按一下**接受**。

若要重新產生自行簽署的憑證:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。

2 按一下**重新產生憑證**。將顯示確認訊息：

3 按一下**確定**。

控管管理介面表格

SonicWall 管理介面可讓您控管管理介面中所有大型資訊表格的顯示方式，您可以更動的項目如下:

- 頁面中顯示的表格項目數量。
- 在背景自動重新整理表格的頻率。

某些表格會在每頁提供個別的項目設定，系統會在使用者登入時進行初始化處理，採用這裡所設定的值。查看這些頁面後，會保留其單獨的設定。在此處所做的後續變更僅在重新登入後才會影響這些頁面。

若要變更表格顯示方式及重新整理表格:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。

2 在**預設表大小**欄位中輸入需要的**個項目/每頁**。最小值為 1，最大值為 5000，預設值為 **50**。

3 在**自動更新表單的重新整理間隔**欄位中，輸入所需的重新整理間隔 (以秒為單位)。最短為 1 秒，最長為 300 秒，預設時數為 **10** 秒。

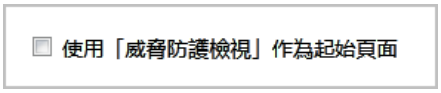
4 按一下**接受**。

指定起始頁面

您登入管理介面時，系統會顯示用於登出管理介面的檢視畫面。您可以改為顯示「系統儀表板檢視」。

若要在您登入時率先顯示監控 | 儀表板頁面:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。



2 選取**使用系統儀表板檢視作為起始頁面**。

3 按一下**接受**。下次您登入時，無論先前登出時顯示的檢視為何，系統都會顯示監控儀表板頁面。

管理工具提示

SonicOS 管理介面提供多種元素的嵌入式工具提示。如需更多工具提示的相關資訊，請參閱*關於 SonicOS*。

若要設定工具提示行為:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。

2 如要啟用工具提示，請選取**啟用工具提示**。

> **提示：**預設已啟用工具提示。若要停用工具提示，請清除**啟用提示**核取方塊。

3 若要設定系統顯示工具提示前的延遲時間 (以毫秒為單位)，請輸入適用的時間長度:

欄位設定內容	延遲顯示的項目
表單工具提示延遲時間	欄位。預設的時間為 **2000** 毫秒，最短為 500 毫秒，最長為 5000 毫秒。
按鈕工具提示延遲時間	按鈕和核取方塊選項按鈕。預設的時間為 **3000** 毫秒，最短為 500 毫秒，最長為 5000 毫秒。
文字工具提示延遲時間	管理介面文字。預設和最短時間為 **500** 毫秒，最長為 5000 毫秒。

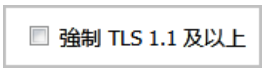
4 按一下**接受**。

強制使用指定的 TLS 版本

SonicOS 支援版本 1.0、1.1 和 1.2 的傳送層安全性 (TLS) 通訊協定。您可以確保使用的是更安全的 1.1 和 1.1 以上版本。

若要強制使用 TLS 1.1 和 1.1 以上版本:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | Web 管理設定**。



2 選取**強制使用 TLS 1.1 和 1.1 以上版本**。

3 按一下**接受**。

設定前方面板管理介面 (僅限 SuperMassive 防火牆)

附註：只有前方具備 LCD 面板的 SuperMassive 安全設備才會顯示這個部分。

您可以在前方面板管理介面中設定是否允許存取設定選單。

提示：首次安裝 SuperMassive 安全設備時，系統會自動啟用這項功能。

若要在前板管理介面中允許存取設定功能表：

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 前方面板管理介面**。

2 選取**啟用前方面板管理介面**。 預設情況下已核取此選項。

3 通過勾選**必須輸入 PIN 才能進入前板**來選擇是否必須使用 PIN 才能存取設定功能表。預設情況下已核取此選項。

   a 在 **PIN** 欄位中輸入 PIN 碼。

   b 在**確認 PIN** 欄位中輸入相同的 PIN 碼。

4 勾選**遮罩 PIN**，選擇是否要遮住 **PIN** 和**確認 PIN** 欄位中的 PIN。如果選擇進行遮罩，則 PIN 將顯示為一串黑點。如未勾選這個選項 (未選取)，就會顯示 PIN。預設情況下已核取此選項。

5 按一下**接受**。

設定用戶端憑證檢查

您可以選擇是否要使用通用存取卡 (CAC) 來驗證憑證。

附註：系統預設不會選取任何選項。

主題：

- 第 32 頁「關於通用存取卡」
- 第 32 頁「設定用戶端憑證驗證」
- 第 34 頁「使用用戶端憑證檢查」
- 第 35 頁「使用者鎖定故障排除」

關於通用存取卡

通用存取卡 (CAC) 是美國國防部 (DoD) 的智慧卡，供軍方人員和其他需要高安全級別的網路存取的政府和非政府人員使用。CAC 使用 PKI 驗證和加密。

附註：使用 CAC 需要連接到 USB 連接埠的外部讀卡器。

用戶端憑證檢查專為配合使用 CAC 而開發；但也適用於所有需要在 HTTPS/SSL 連接上提供用戶端憑證的情形。CAC 支援僅在 HTTPS 連接上可用於用戶端憑證。

附註：CAC 不能用於 Microsoft Internet Explorer 以外的其他瀏覽器。

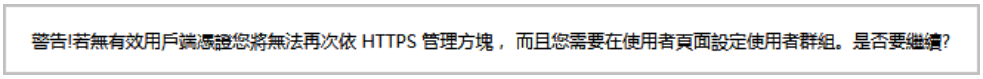
設定用戶端憑證驗證

附註：系統預設不會選取任何選項。

若要設定用戶端憑證檢查功能:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 用戶端憑證檢查**。

2 如需在 SonicWall 安全設備上啟用用戶端檢查功能和 CAC 支援，請選取**啟用用戶端憑證檢查**。您啟用這個選項後，即可使用其他選項。警告確認訊息隨即顯示:



3 按一下**確定**。

4 若要啟用用戶端憑證快取，請選取**啟用用戶端憑證快取**。

附註：快取啟用 24 小時後會失效。

5 若要指定要使用哪一個憑證欄位作為使用者名稱，請在**使用者名稱欄位**下拉功能表中選擇一個選項:

- **主旨: 一般名稱**（預設）
- **子 Alt: 電子郵件**
- **子 Alt: Microsoft 萬用主體名稱**

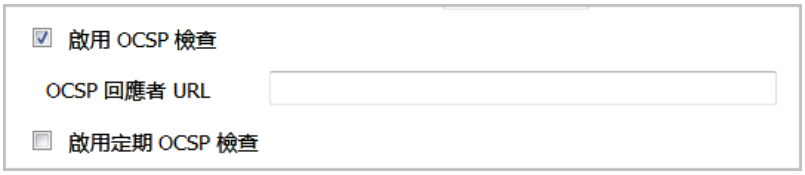
6 若要選取憑證授權單位 (CA) 憑證發行者，請從**用戶端憑證發行者**下拉功能表中選擇一個選項: 預設值為 **ComSign CA**。

附註：如果相應的 CA 不在清單中，則需要將此 CA 匯入 SonicWall 安全裝置中。請參閱第 51 頁「管理憑證」。

7 若要選取如何取得 CAC 使用者群組成員資格，以及如何確認正確的使用者權限，請在 **CAC 使用者群組成員資格擷取方法**下拉功能表中選擇所需選項:

- **本機已設定**（預設）- 選擇此選項後，應建立具有適當成員資格的本機使用者群組。
- **從 LDAP** - 選擇這個選項後，您必須在**管理 | 使用者 | 設定**中設定 LDAP 伺服器 (請參閱第 133 頁「為 LDAP 設定 SonicWall」)。

8 如需啟用線上憑證狀態通訊協定 (OCSP) 檢查來確認用戶端憑證是否仍然有效且尚未遭到撤銷，請選取**啟用 OCSP 檢查功能**。啟用這個選項後，**OCSP 回應 URL** 欄位和**啟用定期 OCSP 檢查**選項隨即顯示。



a 在 **OCSP 回應 URL** 欄位中，輸入要用於確認用戶端憑證狀態的 OSCP 伺服器 URL。

OCSP 回應 URL 通常嵌入在用戶端憑證以內，因此無需輸入。如果用戶端憑證中不包含 OCSP 連結，則可以輸入 URL 連結。此連結應指向用於處理 OCSP 檢查的伺服器端的通用閘道介面 (CGI)。例如：`http://10.103.63.251/ocsp`.

9 若要針對用戶端憑證啟用定期 OCSP 檢查，以便確認用戶端憑證是否仍然有效且尚未遭到撤銷:

a 選取**啟用定期 OCSP 檢查**。OCSP 檢查間隔欄位隨即可供使用。

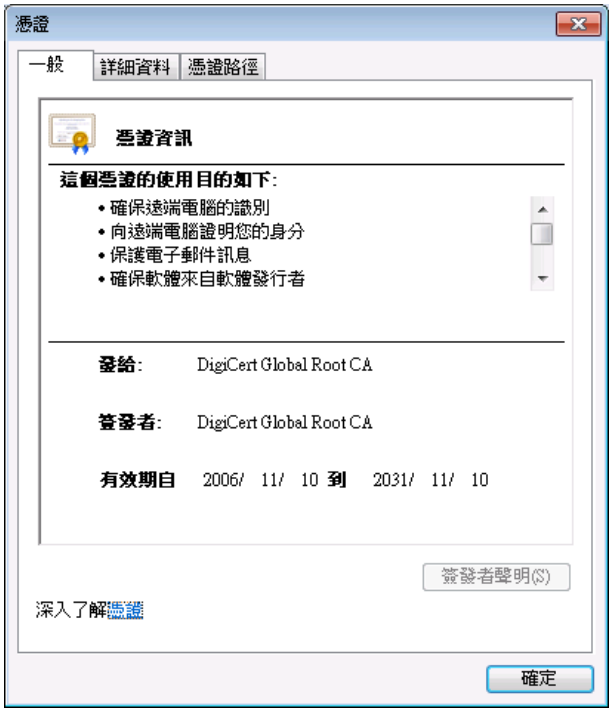
b **OCSP 檢查時間間隔: 1~72 (以小時計)** 欄位中，輸入 OCSP 檢查時間間隔 (以小時為單位)。最短間隔為 1 小時，最長為 72 小時，預設值為 **24** 小時。

10 按一下**接受**。

使用用戶端憑證檢查

如果使用不帶 CAC 的用戶端憑證檢查，則必須手動將用戶端憑證匯入瀏覽器。

如果使用帶 CAC 的**用戶端憑證檢查**，則將由中間件自動將用戶端憑證安裝到瀏覽器中。您透過 HTTPS 開始管理工作階段時，系統會顯示憑證選擇視窗，要求您確認憑證。



在從下拉功能表中選擇用戶端憑證後，將會恢復 HTTPS/SSL 連接；SonicWall 安全裝置將會檢查**用戶端憑證發行者**，以驗證此用戶端憑證是否有 CA 簽章。找到符合的項目後，系統就會顯示管理員登入網頁。如果沒有找到符合項，瀏覽器將顯示標準的瀏覽器連接故障訊息，例如：

. . . . . 無法顯示網頁！

如果在顯示管理員登入頁面之前已啟用 OCSP，則瀏覽器將執行 OCSP 檢查，並在檢查過程中顯示以下訊息。

正在進行用戶端憑證 OCSP 檢查. . . . . .

如果找到符合項，則顯示管理員登入頁面，您可以使用您的管理員憑證繼續管理 SonicWall 安全裝置。

如果未找到符合的項目，系統就會顯示瀏覽器:

OCSP 檢查失敗！請聯絡系統管理員！

使用者鎖定故障排除

在使用用戶端憑證功能時，以下情況下 SonicWall 安全裝置可能會鎖定使用者：

- 已核取**啟用用戶端憑證檢查**，但瀏覽器中沒有安裝用戶端憑證。
- 已核取**啟用用戶端憑證檢查**且在瀏覽器中安裝了用戶端憑證，但沒有選擇任何**用戶端憑證發行者**或者選擇了錯誤的**用戶端憑證發行者**。
- 已啟用**啟用 OSCP 檢查**，但 OSCP 伺服器無法使用，或者 SonicWall 安全裝置由於網路故障無法存取 OSCP 伺服器。

為恢復已鎖定使用者的存取權，系統提供了下列 CLI 命令：

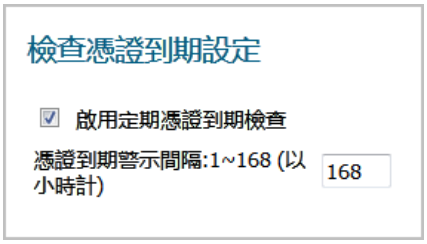
- `web-management client-cert disable`
- `web-management ocsp disable`

附註：如需 CLI 命令的清單和說明，請參閱 *SonicOS 6.2 CLI 參考指南*。

檢查憑證有效期限

若要啟用定期憑證效期檢查:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 檢查憑證有效期限設定**。



2 選取**啟用定期憑證效期檢查**。預設情況下已核取此選項。啟用後，**憑證效期警示間隔**欄位隨即可供使用。

3 如需設定憑證檢查間隔 (以小時為單位)，請在**憑證效期警示間隔：1~168 (以小時計)**中輸入所需的時間間隔。**1 - 168 (以小時計)** 欄位最短時間為 1 小時，最長為 168 小時，預設值為 **168**。

4 按一下**接受**。

設定 SSH 管理

如果使用 SSH 來管理防火牆，則可以變更 SSH 連接埠以獲得額外的安全防護。

若要變更 SSH 連接埠:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | SSH 管理設定**。

2 在 **SSH 連接埠**欄位中輸入所需的連接埠。預設 SSH 連接埠號是 **22**。

3 按一下**接受**。

設定進階管理選項

進階管理選項可讓您指定:

- 是否由 SNMP (預設) 或 SonicWall 全域管理系統 (GMS) 管理 SonicWall 安全設備。如需進一步瞭解 GMS，請參閱 *GMS 指南*。
- 建立 MGMT 介面的管理介面位址物件。

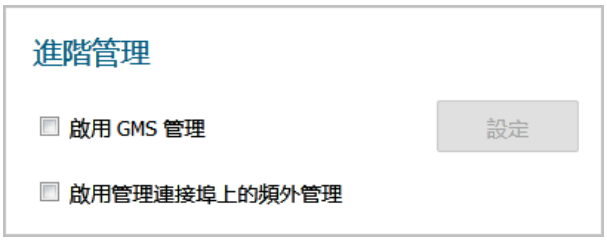
  這個管理介面提供了可靠的設備管理介面。此介面對網路連接有諸多限制。如果在 MGMT 子網路中有設定 NTP、DNS 和 SYSLOG 伺服器，設備會使用 MGMT IP 做為來源 IP 並自動建立 MGMT 位址物件和路由原則。所有來自管理介面的流量都將按照此原則進行路由。建立的路由會顯示在**系統設定 | 網路 | 路由**頁面中 (如需進一步瞭解路由，請參閱第 371 頁「設定路由通告和路由原則」)。

  MGMT 位址物件和路由原則會建立/更新 IPv4 管理 IP。因為預設情況下會建立 IPv6 管理 IP 位址物件，因此此功能不支援建立 IPv6 管理 IP 位址物件。

附註：系統預設不會啟用任一選項。

若要設定進階管理選項:

1 在**管理**檢視中，導覽至**系統設定 | 設備 | 基本設定 | 進階管理**。



2 如需允許 SonicWall GMS 管理防火牆，請選取**啟用 GMS 管理**。**設定**按鈕隨即啟用。如需設定 GMS 管理，請參閱第 36 頁「啟用 GMS 管理」。

3 如需自動建立 MGMT 介面 (以頻外介面的形式運作) 的管理介面位址物件，以及為新建立的位址物件設定路由原則，請選取**管理連接埠上的頻外管理**。

重要：如需避免刪除/建立路由原則帶來的衝突，更新此選項以建立管理介面位址物件，設定路由原則會導致系統重新啟動。

啟用 GMS 管理

附註：如需更多 SonicWall 全域管理系統的相關資訊，請移至 http://www.sonicwall.com*GMS Guide*。

若要設定安全設備的 GMS 管理功能:

1 導覽至**管理 | 系統設定 > 設備 | 基本設定 | 進階設定**。

2 選取**啟用 GMS 管理**。**設定**按鈕隨即啟用。

3 按一下**設定**。隨即顯示**設定 GMS 設定**對話方塊。

4 在 **GMS 主機名稱或 IP 位址**欄位中輸入 GMS 主控台的主機名稱或 IP 位址。

5 在 **GMS Syslog 伺服器連接埠**欄位中輸入連接埠。預設值為 **514**。

6 如需只傳送活動訊號狀態而不需傳送記錄訊息，請選取**僅傳送活動訊號狀態訊息**。預設已停用此選項。

7 如果 GMS 主控台置於網路中使用 NAT 的裝置之後，請選取 **NAT 裝置後的 GMS**。預設已停用此選項。

選取這個選項後，**NAT 裝置 IP 位址**欄位即可供使用。

a 在 **NAT 裝置 IP 位址**欄位中輸入 NAT 裝置的 IP 位址。

8 從**管理模式**下拉功能表中選擇以下 GMS 模式之一。

IPSEC 管理通道 將允許 GMS 管理主控台通過 IPsec VPN 通道來管理防火牆。移至步驟 9。

現有通道 透過 GMS 伺服器和防火牆間的連線使用現有 VPN 通道。將顯示一條訊息。

移至步驟 11。

HTTPS 允許從兩個 IP 位址進行 HTTPS 管理：GMS 主要代理和備用代理 IP 位址。SonicWall 防火牆還使用 3DES 和防火牆管理員的密碼傳送加密的 syslog 封包和 SNMP 陷阱。GMS 報告伺服器設定選項隨即顯示。移至步驟 10。

9 系統會顯示預設的 IPsec VPN 設定，其中包含 SonicOS 填入的值。驗證設定。

a 在**加密演算法**下拉功能表中，選取適用的演算法。

b (選用) 在**加密金鑰**欄位中輸入新的加密金鑰:

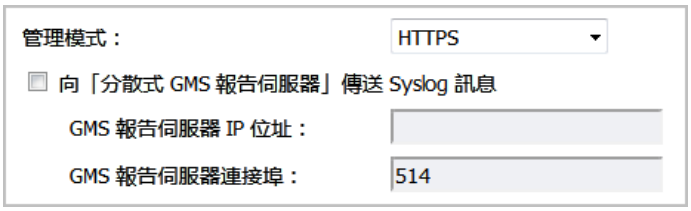
對於	金鑰必須為
DES	16 個 16 進位字元
3DES	48 個 16 進位字元

c (選用) 在**驗證金鑰**欄位中輸入新的驗證金鑰:

對於	金鑰必須為
MD5	32 個 16 進位字元
SHA1	40 個 16 進位字元

d 移至步驟 11。

10 SonicOS 必須瞭解 GMS 報告伺服器。



a 選取**向「分散式 GMS 報告伺服器傳送 Syslog 訊息」**。預設情況下未勾選此選項。 下列選項隨即可供使用。

b 在 **GMS 報告伺服器 IP 位址**欄位中，輸入 GMS 伺服器的 IP 位址。

c 在 **GMS 報告伺服器連接埠**欄位中，輸入 GMS 伺服器的連接埠。預設連接埠號是 **514**。

11 按一下**確定**。

手動下載 SonicPoint 映像

下載 URL 部分提供了指定網站 URL 位址以便下載 SonicPoint 映像的欄位。

如果您的防火牆：

- 有網際網路連線，則您連上 SonicPoint 裝置時，系統將從 SonicWall 伺服器自動下載正確的 SonicPoint 映像。
- 沒有網際網路接入，或只能通過代理伺服器存取網際網路，則必須手動指定 SonicPoint 韌體的 URL。您不需要加入 **http://** 首碼，但必須在 URL 的末端加入檔案名稱。此檔案名稱應有 `.bin` 副檔名。以下是使用 IP 位址和網域名稱的範例：

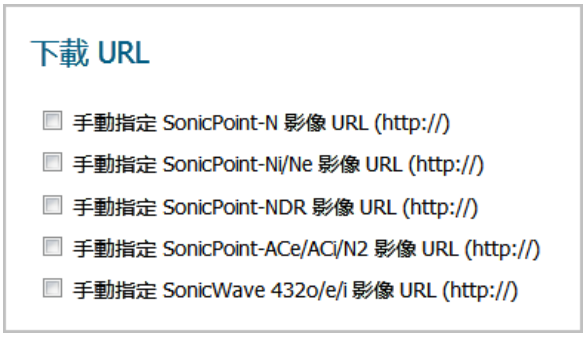
```
192.168.168.10/imagepath/sonicpoint.bin
software.sonicwall.com/applications/sonicpoint/sonicpoint.bin
```

詳情請參閱*更新指南*。

△ **注意：您必須根據您的安全設備目前執行的 SonicOS 韌體版本下載對應的 SonicPoint 映像。如需對應版本資訊請造訪 MySonicWall 網站。升級 SonicOS 韌體時，請務必升級至正確的 SonicPoint 映像。**

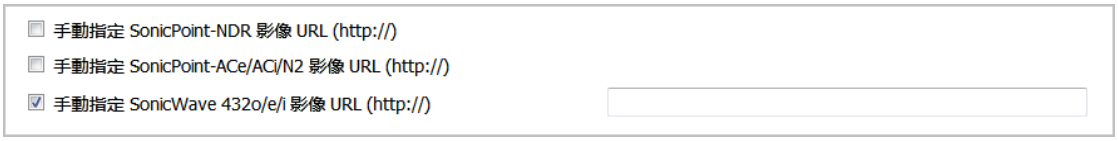
若要選取要下載的 SonicPoint 映像類型:

1 導覽至**管理 | 系統設定 > 設備 | 基本設定 | 下載 URL**。



- **手動指定 SonicPoint-N 映像 URL (http://)**
- **手動指定 SonicPoint-Ni/Ne 映像 URL (http://)**
- **手動指定 SonicPoint-NDR 映像 URL (http://)**
- **手動指定 SonicPoint-ACe/ACi/N2 映像 URL (http://)**
- **手動指定 SonicPoint-AC Wave2 影像 URL (http://)**

2 按一下適用的 SonicPoint 映像 URL。用於該 URL 的欄位隨即顯示。



3 在關聯欄位中，輸入映像下載位置。

4 按一下**接受**。

選取語言

如果韌體中包含英語以外的其他語言，您可以在**語言選擇**下拉功能表中選取所需語言。

附註：更動 SonicOS 管理介面的語言後，必須重新啟動安全設備。

若要選取管理介面的語言:

1 導覽至**管理 | 系統設定 > 設備 | 基本設定 | 語言**。

2 在**語言選擇**下拉功能表中選取所需語言。

3 按一下**接受**。

3

管理 SNMP

關於設備 | SNMP

您可以使用 SNMP 或 SonicWall 全域管理系統 (GMS) 管理 SonicWall 安全設備。 本節介紹如何設定 SonicWall 以使用 SNMP 進行管理。如需使用 GMS 管理 SonicWall 的相關資訊，請參閱 *SonicOS GMS 指南*。

主題：

關於 SNMP

SNMP（簡單網路管理協定）是基於使用者資料包協定 (UDP) 的網路協定，管理員可以利用它來監視 SonicWall 安全設備的狀態和接收網路中發生的重要事件通知。SonicWall 安全設備支援 SNMP v1/v2c/v3 以及除 **egp** 和 **at** 以外的所有相關管理資訊庫 II (MIBII) 群組。

SNMPv3 擴充了早期版本 SNMP 的功能，通過封包驗證和加密的組合提供安全的網路存取。

封包安全性通過以下手段保證：

- **訊息完整性**：確保封包在傳送途中未受到篡改。
- **身分驗證**：驗證訊息來自有效的來源。
- **加密**：對封包內容進行編碼，防止未經授權的來源查看。

SNMPv3 同時提供安全模型和安全級別。安全模型是在使用者和使用者所在的群組之間設定的身分驗證原則。安全級別是在給定安全模型內允許的安全級別。安全模型和相關的安全級別決定如何處理 SNMP 封包。SNMPv3 提供額外級別的驗證和加密，以及附加的授權和存取控制。

基於 SNMP 版本的安全級別、驗證和加密表格顯示不同版本的 SNMP 如何處理安全級別、驗證和加密。

基於 SNMP 版本的安全級別、驗證和加密

版本	等級	驗證類型	加密	驗證方法
v1	noAuthNoPriv	團體字串	否	團體字串符合
v2c	noAuthNoPriv	團體字串	否	團體字串符合
v3	noAuthNoPriv	使用者名稱	否	使用者名稱符合
	authNoPriv	MD5 或 SHA	否	身分驗證基於 HMAC-MD5 或 HMAC-SHA 演算法。
	authPriv	MD5 或 SHA	DES 或 AES	提供基於 HMAC-MD5 或 HMAC-SHA 演算法的身分驗證。除了基於 CBC-DES (DES-56) 標準的身分驗證以外，還提供 DES 56 位加密或 AES 128 位加密。

SonicWall 安全設備通過任意介面回覆用於 MIBII 的 SNMP `Get` 命令，且支援用於產生陷阱訊息的自訂 SonicWall MIB。自訂 SonicWall MIB 可以在 SonicWall 網站下載，並載入到 HP Openview、Tivoli 或 SNMPC 等供應商 SNMP 管理軟體中。

您可以檢視及設定 SNMP 設定。使用者無法查看或變更設定。SNMPv3 可以在使用者級或群組級變更。存取權限檢視可以讀取和/或寫入，並且可以設定為使用者或群組。單一檢視可以有多個物件 ID (OID) 與之關聯。

用於 SNMPv3 引擎 ID 的 SNMPv3 設定可以在**設定 SNMP** 對話方塊的**一般設定**功能表下設定。引擎 ID 用於授權接收到的 SNMP 封包。僅處理符合的封包引擎 ID。

設定 SNMP 存取權限

設定 SNMP 包括:

- 第 41 頁「啟用和設定 SNMP 存取權限」
- 第 44 頁「設定 SNMPv3 群組和存取權限」

啟用和設定 SNMP 存取權限

可以使用 SNMPv1/v2 以提供基本功能，或者設定 SonicWall 安全設備使用功能更豐富的 SNMPv3 選項。

若要使用 SNMP，您必須先將之啟用。

主題：

- 第 42 頁「設定基本功能」
- 第 43 頁「設定 SNMPv3 引擎 ID」
- 第 45 頁「設定 SNMPv3 檢視的物件 ID」
- 第 47 頁「建立群組並新增使用者」
- 第 48 頁「新增存取」

設定基本功能

若要啟用 SNMP:

1 移至**設備 | SNMP** 頁面。

2 選擇**啟用 SNMP** 核取方塊。預設情況下，停用 SNMP。

3 按一下**接受**。SNMP 資訊將填入 SNMP 頁面，而且**設定**按鈕會變成可用。

4 若要設定 SNMP 介面，請按一下**設定**。隨即顯示**設定 SNMP** 對話方塊。

5 在**一般**頁面上，在**系統名稱**欄位中輸入 SonicWall 安全設備的主機名稱。

6 或者，在**系統聯絡人**欄位中輸入網路管理員的姓名。

7 或者，在**系統位置**欄位中輸入電子郵件地址、電話號碼或呼叫器號碼。

8 如果使用 SNMPv3 設定選項，請在**資產編號**欄位中輸入資產編號。否則，此欄位為可選。

9 在**獲取社群名稱**欄位中輸入可以查看 SNMP 資料的管理員組或團體的名稱。預設名稱為 **public**。

10 或者，在**擷取社群名稱**欄位中輸入可以查看 SNMP 陷阱的管理員群組或社群的名稱。

11 在**主機 1** 至**主機 *n*** 欄位中輸入接收 SNMP 陷阱的 SNMP 管理系統的 IP 位址或主機名稱。您必須至少設定一個 IP 位址或主機名稱，但最多可達您的系統能夠使用的位址或主機名稱數上限。

12 如果您：

- 若要設定 SNMPV3，請移至第 43 頁「設定 SNMPv3 引擎 ID」。
- 立即完成設定 SNMP，按一下**確定**。

設定 SNMPv3 引擎 ID

如果使用 SNMPv3，則可以設定 SNMPv3 引擎 ID 和 SNMP 優先順序。設定 SNMPv3 引擎 ID 將為 SNMP 管理提供最高的安全性。

設定 SNMPv3 引擎 ID：

1 導覽到**設備 | SNMP**。

2 如果還沒有為系統設定 SNMP，請遵循第 42 頁「設定基本功能」中的步驟 1 到步驟 11。

3 按一下**進階**。隨即顯示**進階**頁面。

4 勾選**強制使用 SNMPv3** 核取方塊。這會停用 SNMPv1/v2，僅允許 SNMPv3 存取，從而為 SNMP 管理提供最高的安全性。

重要：如果您選取此選項，則必須先在**一般**頁面上指定資產號碼，然後再按一下**確定**。

5 在**引擎 ID** 欄位中輸入十六進位的引擎 ID 號。SonicOS 會自動填入此欄位，但您可以加以變更。此號碼與接收的 SNMP 封包進行比對以授權其處理；僅處理其引擎 ID 與此號碼符合的封包。

6 或者，也可以勾選**增加 SNMP 子系統優先順序**核取方塊。

對於高效系統執行，某些操作的優先順序高於對 SNMP 查詢的回應。啟用此選項會使 SNMP 子系統始終在較高的系統優先順序回應和操作。

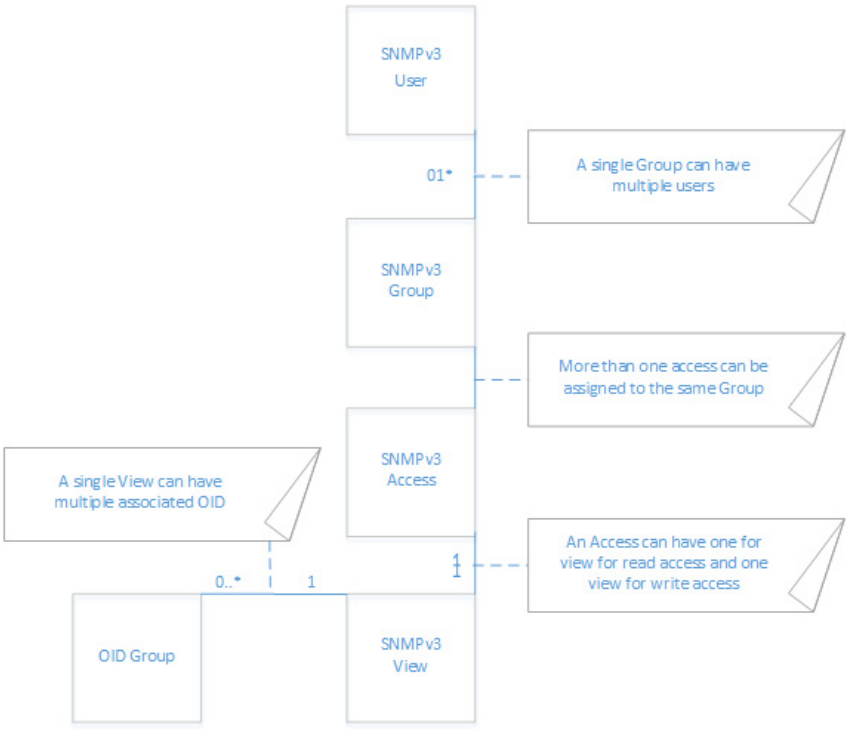
重要：啟用此選項可能會影響整個系統的效能。

7 按一下**確定**。現在將使用 SNMPv3 安全選項來處理封包。

設定 SNMPv3 群組和存取權限

SNMPv3 用於設定群組和存取權限並為其指派不同的安全級別。物件 ID 與不同的權限相關聯，可將單一檢視指派給多個物件。SNMPv3 群組和使用者存取權限顯示群組和使用者的存取如何與這些不同的權限相關聯。

SNMPv3 群組和使用者存取權限



設定 SNMPv3 檢視的物件 ID

SNMPv3 **檢視**會顯示使用者和群組的存取設定。您為使用者和群組建立設定，使用者無法變更這些安全設定。SNMPv3 檢視定義物件 ID (OID) 和物件 ID 群組，有時將其稱為 SNMPv3 存取權限物件。

SNMP **檢視**定義 OID 和 OID 群組的集合。無法變更或刪除預設檢視的初始集。預設檢視是最常用的一些檢視，如根檢視、系統檢視、IP、介面。這些檢視的 OID 是預先指派的。

此外，您可以為特定使用者和群組建立自訂檢視。

可以修改您自己建立的檢視。但無法修改系統建立的檢視。

若要設定 SNMPv3 檢視的 OID：

1 導覽到**設備 | SNMP**。

2 若要新增檢視，請在**檢視**區段中，按一下**新增**。隨即顯示**新增 SNMP 檢視**對話方塊。

3 在**檢視名稱**欄位中輸入一個有意義的名稱。預設的名稱是**新增 SNMP 檢視**。

附註：若是編輯現有檢視，名稱將無法編輯。

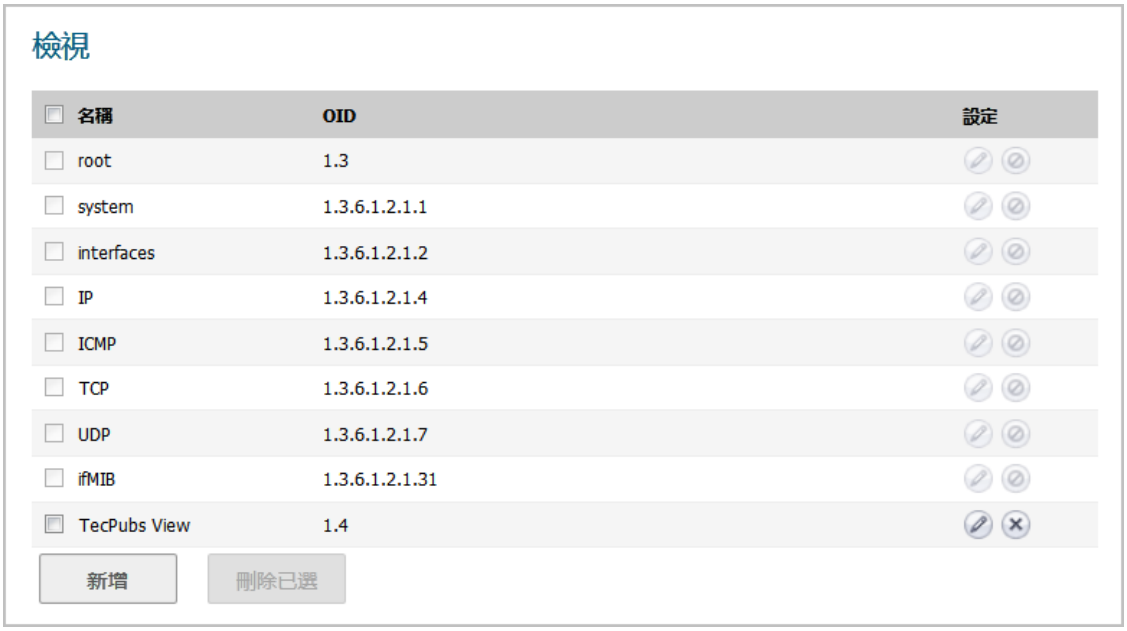
4 在**關聯檢視的 OID** 欄位中輸入一個未指派的 OID。

5 按一下**新增 OID**。

新檢視出現在 **OID 清單**中。若要從 OID 清單中刪除 OID，請選取 OID，然後按一下**刪除**。

6 新增其他任意檢視和關聯的 OID。

7 按一下**確定**。新的檢視已新增到**檢視**表格中。



建立群組並新增使用者

依預設，有一個群組***無群組***無法加以設定或刪除。不過，您可以將使用者新增至此預設群組。

主題：

建立群組

若要建立群組:

1 導覽到**設備 | SNMP**。

2 按一下**使用者/群組**表格下的**新增群組**。隨即顯示**新增 SNMP 群組**對話方塊。

3 在**群組名稱**欄位中輸入一個簡單易記的名稱。群組名稱最多可包含 32 個英數字元。

4 按一下**確定**。**使用者/群組**表格隨即更新，而且**設定**欄中的**編輯**與**刪除**圖示為可用狀態。

新增使用者

若要新增使用者:

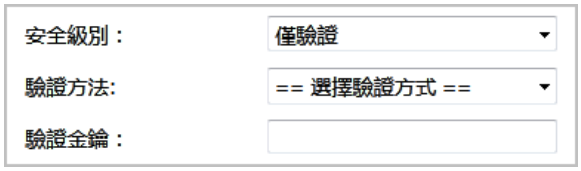
1 導覽到**設備 | SNMP**。

2 按一下**使用者/群組**表格下的**新增使用者**。隨即顯示**新增 SNMP 使用者**對話方塊。

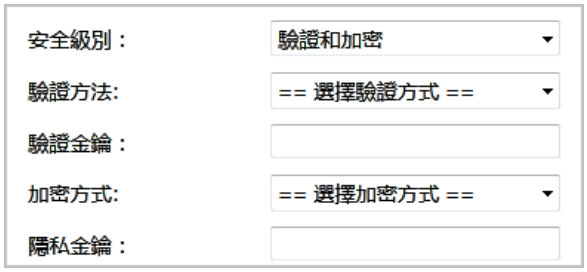
3 在**使用者名稱**欄位中輸入使用者名稱。

4 從**安全級別**下拉功能表中選擇安全級別：

- **無**（預設值）
- **身分驗證** - 顯示以下兩個新選項：



  - **驗證方法** - 選擇下列一種驗證方法：**MD5** 或 **SHA1**。
  - **認證金鑰** - 在此欄位中輸入認證金鑰。此金鑰可以是任意 8 到 32 個可列印字元的字串。
- **驗證和加密** - 更多選項如下所示：



  - **驗證方法** - 請參見上文。
  - **認證金鑰** - 請參見上文。
  - 從**加密方法**下拉功能表中選擇以下一種加密方法：**AES** 或 **DES**。
  - 在**隱私金鑰**欄位中輸入加密金鑰。此金鑰可以是任意 8 到 32 個可列印字元的字串。

5 從**群組**下拉功能表中選擇一個群組。（預設為***無群組***。）

6 完成時，按一下**確定**。將使用者新增到**使用者/群組**表格，並新增至適當的群組 (包括***無群組***)。

新增存取

SNMPv3 存取權限是一個物件：

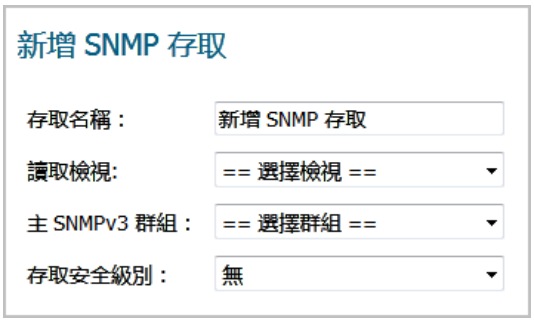
- 它定義 SNMPv3 檢視的讀寫存取權限。
- 可將其指派給 SNMPv3 群組。

可將同一存取權限物件指派給多個群組。可將多個檢視指派給一個存取權限。

建立存取權限物件的步驟如下：

1 導覽到**設備 | SNMP**。

2 在**存取**表格下面，按一下**新增**。隨即顯示**新增 SNMP 存取**對話方塊。



3 在**存取名稱**欄位中輸入一個簡單易記的名稱。

附註：現有項目的名稱無法編輯。

4 從**讀取**檢視下拉功能表在可用檢視清單中選擇一個檢視。

5 從**主 SNMPv3 群組**下拉功能表在可用群組清單中選擇一個群組。

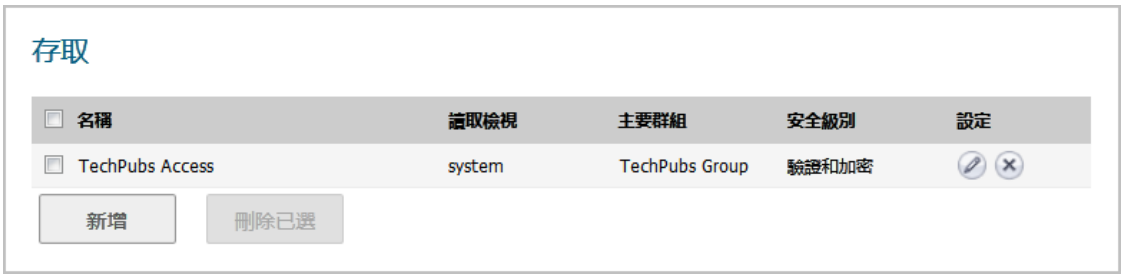
附註：只能將存取權限指派給一個 SNMPv3 群組，但是一個群組可以與多個存取權限物件相關聯。

存取權限不能指派給***無群組***。

6 從**存取安全級別**下拉功能表，選擇以下一個安全級別：

- **None**
- **僅身分驗證**
- **驗證和加密**

7 按一下**確定**。存取權限物件已新增到**存取**表中。



將 SNMP 設定為服務並新增規則

預設情況下，SonicWall 安全裝置停用 SNMP。若要啟用 SNMP，您必須先在**設備 | SNMP** 頁面上啟用 SNMP，然後再為各個介面啟用 SNMP。為此，請移至**網路 | 介面**頁面，並針對您想要為其啟用 SNMP 的介面，按一下**設定**。如需關於設定 SNMP 作為服務與新增規則的詳細資訊，請參閱第 224 頁「設定介面」。

如果您的 SNMP 管理系統支援探索，SonicWall 安全設備代理將自動探索網路上的 SonicWall 安全設備。否則，您必須將 SonicWall 安全設備新增到 SNMP 管理系統中的 SNMP 託管裝置清單中。

關於 SNMP 記錄

SNMP 記錄**記錄 | 事件記錄**頁面上檢視。如需關於事件記錄的詳細資訊，請參閱 *SonicOS 調查指南*。

僅對 SonicWall 安全設備正常傳送的警示訊息類別產生陷阱訊息。例如攻擊、系統錯誤或受封鎖的網站都會產生陷阱訊息。如果沒有在**記錄 | 事件記錄**頁面中選取任何類別，則不會產生任何陷阱訊息。

4

管理憑證

關於憑證

要實施用於 VPN 原則的憑證應用，必須找到來自供應商 CA 服務的有效 CA 憑證來源。獲得有效的 CA 憑證後，可以將其匯入防火牆以驗證您的本機憑證。您可以透過**設備 > 憑證**頁面，將有效的 CA 憑證匯入防火牆。匯入有效的 CA 憑證後，可以使用它來驗證您的本機憑證。

SonicOS 向 SonicWall 安全設備提供大量的憑證；這些是內建的憑證，而且無法刪除或設定。

關於數位憑證

數位憑證是一種借助受信任的供應商（也稱為憑證授權單位 (CA)）來驗證身分的電子方法。X.509 v3 憑證標準是與加密憑證搭配使用的規格，並允許利用您的憑證定義可包含的副檔名。SonicWall 已在其供應商憑證支援中實施此標準。

您可以將供應商 CA 簽署和驗證的憑證用於 IKE（網際網路金鑰交換）VPN 原則。IKE 是 IPsec VPN 解決方案的重要組成部分，它能在設定安全關聯 (SA) 之前使用數位憑證就對等裝置進行驗證。如果沒有數位憑證，VPN 使用者必須通過手動交換共用密碼或對稱金鑰才能進行身分驗證。使用數位簽章的裝置或用戶端無需在每次向網路中新增新裝置或用戶端時變更設定。

典型的憑證包括兩個部分：資料部分和簽章部分。資料部分通常包含：憑證所支援的 X.509 版本、憑證序號等資訊；關於使用者公開金鑰、識別名稱 (DN)、憑證有效期的資訊；以及憑證的目的地用途等可選資訊。簽章部分包含頒發 CA 所用的加密演算法，以及 CA 數位簽章。

SonicWall 安全設備可與任何符合 X.509v3 標準的憑證供應商實現相互操作。SonicWall 安全設備已通過下列憑證授權單位憑證供應商的測試：

- Entrust
- Microsoft
- OpenCA
- OpenSSL 和 TLS
- VeriSign

主題：

關於憑證和憑證請求表格

#	憑證	類型	驗證	過期	詳細資料	設定
1	HTTPS Management Certificate	本機憑證	自我簽署	Jan 19 03:14:07 2038 GMT		
2	ComSign CA	CA 憑證		Mar 19 15:02:18 2029 GMT		
3	thawte Primary Root CA - G3	CA 憑證		Dec 1 23:59:59 2037 GMT		
4	VeriSign, Inc.	CA 憑證		Aug 1 23:59:59 2028 GMT		
5	VeriSign Class 3 International Server CA - G3	CA 憑證		Feb 7 23:59:59 2020 GMT		
6	AddTrust External CA Root	CA 憑證		May 30 10:48:38 2020 GMT		
7	TC TrustCenter Class 2 CA II	CA 憑證		Dec 31 22:59:59 2025 GMT		
8	ACCVRAIZ1	CA 憑證		Dec 31 09:37:37 2030 GMT		
9	GlobalSign	CA 憑證		Mar 18 10:00:00 2029 GMT		
10	PSCProcert	CA 憑證		Dec 25 23:59:59 2020 GMT		
11	ACEDICOM Root	CA 憑證		Apr 13 16:24:22 2028 GMT		
12	COMODO Certification Authority	CA 憑證		Dec 31 23:59:59 2029 GMT		
13	DigiCert High Assurance EV Root CA	CA 憑證		Jul 25 17:57:44 2019 GMT		
14	Microsoft Internet Authority	CA 憑證		Apr 25 17:40:55 2020 GMT		
15	Atos TrustedRoot 2011	CA 憑證		Dec 31 23:59:59 2030 GMT		
16	TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	CA 憑證	在 9 天內到期	Dec 22 18:37:19 2017 GMT		
17	DST Root CA X3	CA 憑證		Sep 30 14:01:15 2021 GMT		
18	GeoTrust DV SSL CA	CA 憑證		Feb 25 21:32:31 2020 GMT		

憑證和憑證要求表格提供用於管理 CA 和本機憑證的所有設定。

檢視樣式功能表可讓您根據下列條件顯示您的憑證:

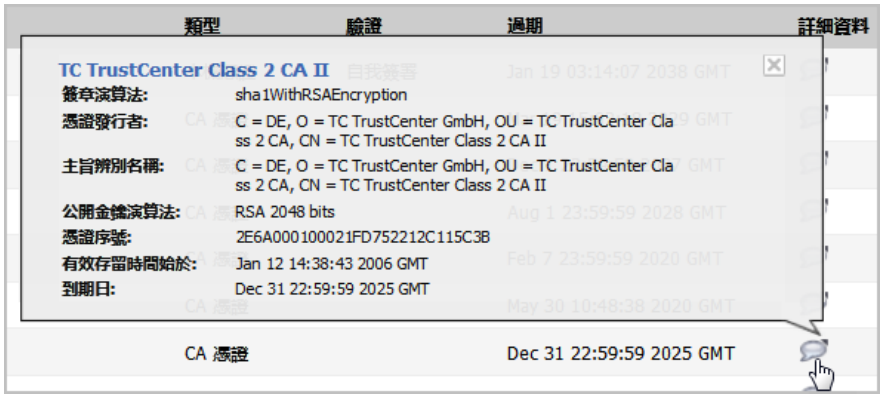
條件	顯示
所有條件	所有內建與匯入的憑證和憑證要求。這是預設值。
匯入憑證和要求	僅匯入的憑證和產生的憑證要求。 預設情況下未勾選此選項。
內建憑證	僅內建憑證。 預設情況下未勾選此選項。
包含已過期憑證和內建憑證	所有已過期憑證和內建憑證。 預設情況下未勾選此選項。

憑證和憑證要求表格中顯示關於憑證的資訊:

此欄	顯示
憑證	憑證的名稱。
類型	憑證的類型: • **CA 憑證** • **本機憑證** • **待處理要求**
已驗證	驗證資訊: • **自我簽署** • **在 *n* 天內到期** • **已過期**
到期	憑證到期日期和時間。
詳細資料	憑證的詳細資料。將指標移到**註解**圖示的上面可顯示憑證的詳細資料。關於憑證的詳細資料，請參見第 53 頁「關於憑證詳細資料」。
設定	包含 • **刪除**圖示，以刪除憑證項目 • **匯入**圖示 ，以匯入憑證撤銷清單（用於 CA 憑證）或已簽署的憑證（用於擱置的請求）。 **附註：**您無法刪除或匯入內建憑證。

關於憑證詳細資料

按一下**詳細資料**欄中的**註解**圖示，會顯示憑證的相關資訊，且根據不同憑證類型，可能包括下列資訊:



- 簽章演算法
- 憑證頒發方
- 主旨識別名稱
- 公開金鑰演算法
- 憑證序號
- 有效存留時間始於
- 到期日
- 狀態（用於擱置的請求和本機憑證）

詳細資料視憑證類型而定。對於擱置的請求，不顯示**憑證頒發方**、**憑證序號**、**有效存留時間始於**和**到期日**資訊，因為這些資訊將由憑證供應商產生。

匯入憑證

在您的 CA 服務供應商針對您的待處理請求頒發憑證或提供本機憑證後，您可以匯入憑證以用於 VPN 或 Web 管理身分驗證。也可以匯入 CA 憑證來驗證本機憑證和 IKE 交涉中使用的對等憑證。

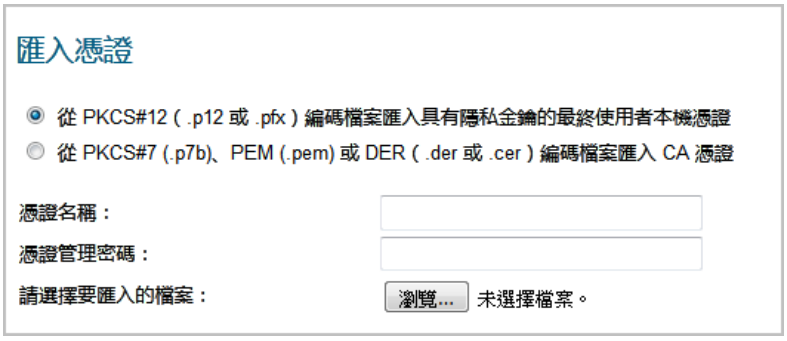
主題：

匯入本機憑證

若要匯入本機憑證：

1 導覽到**設備 > 憑證**。

2 按一下**匯入**。隨即顯示**匯入憑證**對話方塊。



3 在**憑證名稱**欄位中輸入憑證的名稱。

4 在**憑證管理密碼**欄位中輸入您的憑證授權單位所使用的密碼以加密 PKCS#12 檔案。

5 按一下**瀏覽**以找到憑證檔案。

6 按一下**開啟**設定憑證的目錄路徑。

7 按一下**匯入**，將憑證匯入防火牆。完成匯入後，可以在**憑證和憑證請求**表中查看此憑證項目。

8 將指標移到**詳細資料**列中的**註解**圖示將會顯示憑證的詳細資料。

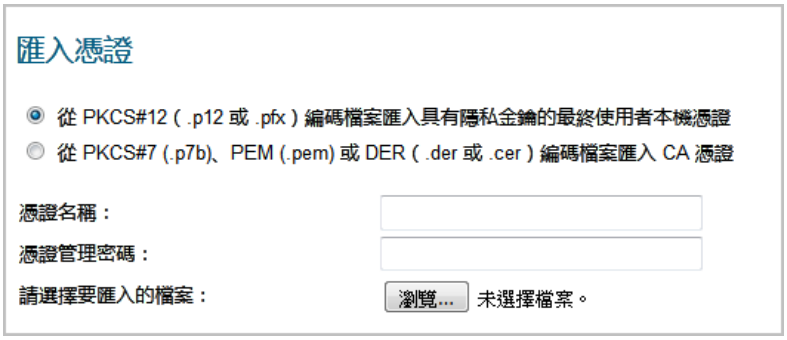
附註：已成功上載憑證，**已驗證**將滑鼠放在「**狀態**」時出現的視窗。

匯入憑證授權單位憑證

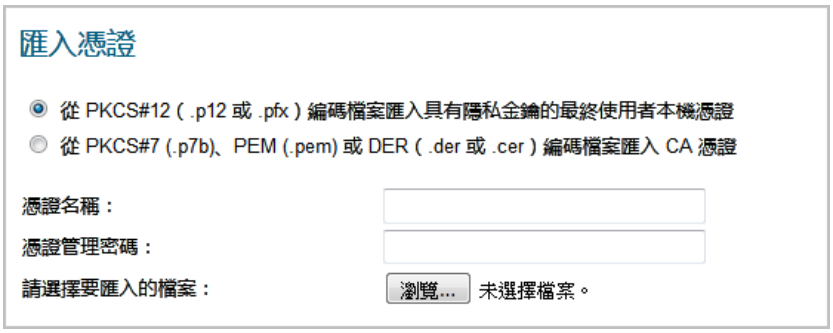
若要從憑證授權單位匯入憑證：

1 導覽到**設備 > 憑證**。

2 按一下**匯入**。隨即顯示**匯入憑證**對話方塊。



3 選擇**從 PKCS#7 (.p7b) 或 DER (.der 或 .cer) 編碼檔案匯入 CA 憑證**。**匯入憑證**對話方塊設定隨即發生變更。



4 按一下**瀏覽**以找到憑證檔案。

5 按一下**開啟**設定憑證的目錄路徑。

6 按一下**匯入**，將憑證匯入防火牆。完成匯入後，可以在**憑證和憑證請求**表中查看此憑證項目。

7 將指標移到**詳細資料**列中的**註解**圖示將會顯示憑證的詳細資料。

建立 PKCS-12 格式憑證檔案 (僅限 Linux 系統)

可使用帶有 OpenSSL 的 Linux 系統建立 PKCS12 格式憑證檔案。若要建立 PKCS-12 格式憑證檔案，需要有憑證的兩個主要元件：

- 私人金鑰（通常是檔案名稱中包含 `.key` 副檔名或字金鑰的檔案）
- 具有公開金鑰的憑證（通常是檔案名稱中包含 `.crt` 副檔名或字 cert 的檔案）

例如，Linux 上的 Apache HTTP 伺服器有私密金鑰和憑證，其位置如下:

- `/etc/httpd/conf/ssl.key/server.key`
- `/etc/httpd/conf/ssl.crt/server.crt`

可使用這兩個檔案執行以下命令：

```
openssl pkcs12 -export -out out.p12 -inkey server.key -in server.crt
```

在此範例中，**`out.p12`** 將成為 PKCS-12 格式憑證檔案，**`server.key`** 和 **`server.crt`** 是 PEM 格式的私人金鑰和憑證檔案。

執行 **`openssl`** 命令之後，系統將提示您輸入密碼，以防護/加密檔案。選擇密碼後，將完成 PKCS-12 格式憑證檔案的建立，然後會將其匯入到設備中。

刪除憑證

附註：內建憑證無法刪除。

如果憑證已過期，或者您決定不使用供應商憑證進行 VPN 驗證，您可以刪除匯入的憑證。可以一律刪除您建立的憑證。

若要刪除：

- 憑證，請按一下其**刪除**圖示。
- 一個或多個憑證:
  a 按一下其核取方塊。**刪除**和**全部刪除**按鈕會變成可用狀態。
  b 按一下**刪除**或**全部刪除**。
- 所有非內建憑證:
  a 按一下表格標題中的核取方塊。**刪除**和**全部刪除**按鈕會變成可用狀態。
  b 按一下**刪除**或**全部刪除**。

產生憑證簽署請求

提示：您應該建立憑證原則來配合本機憑證使用。憑證原則決定了驗證憑證所需的身分驗證要求和機構限制。

若要產生憑證簽署要求:

1 導覽到**設備 > 憑證**。

2 按一下**新增簽署要求**。隨即顯示**憑證簽署要求**對話方塊。

3 在**憑證別名**欄位中輸入憑證的別名。

4 使用辨別名稱元件表格中顯示的下拉功能表建立辨別名稱 (DN)，然後在相關欄位中輸入憑證的資訊。

附註：對於每個辨別名稱，您可以從相關下拉功能表選取您的國家或地區；對於所有其他元件，在相關文字欄位中輸入資訊。

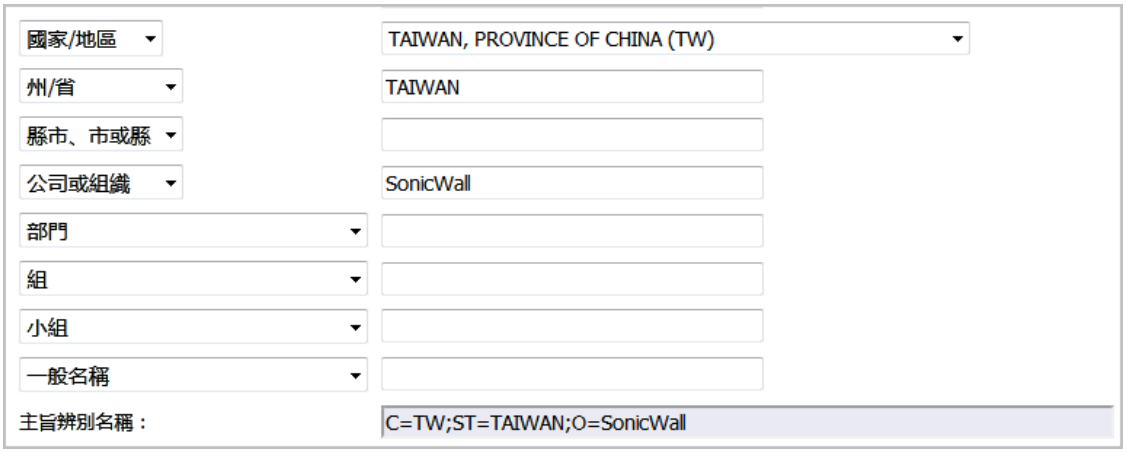
辨別名稱元件

從此下拉功能表	選取/輸入適當的資訊
國家或地區	國家或地區（預設） 狀態 縣市或縣 公司或組織
狀態	國家或地區 狀態（預設） 縣市、市或縣 公司或組織 部門
縣市、市或縣	縣市、市或縣（預設） 公司或組織 部門 群組 小組
公司或組織	公司或組織（預設） 部門 群組 小組 一般名稱 序號 電子郵件地址
部門	部門（預設） 群組 小組 一般名稱 序號 電子郵件地址
群組	群組（預設） 小組 一般名稱 序號 電子郵件地址

辨別名稱元件

從此下拉功能表	選取/輸入適當的資訊
小組	小組（預設）
	一般名稱
	序號
	電子郵件地址
一般名稱	一般名稱（預設）
	序號
	電子郵件地址

您在輸入元件資訊時，系統會在**主旨辨別名稱**欄位中建立辨別名稱 (DN)。



5 從下拉功能表選擇類型後，您也可將**備用主旨名稱**附加到憑證：

- **網域名稱**
- **電子郵件地址**
- **IPv4 位址**

6 從**簽章演算法**下拉功能表中選擇簽章演算法：

- **MD5**
- **SHA1**（預設）
- **SHA256**
- **SHA384**
- **SHA512**

7 從**主旨金鑰類型**下拉功能表中選擇主旨金鑰類型：

RSA（預設）	用於加密資料的公開金鑰加密演算法。
ECDSA	使用橢圓曲線數位簽章演算法加密資料，其具有每金鑰位元高強度安全性。

8 從**主體金鑰大小/曲線**下拉功能表選取主體金鑰大小或曲線。

附註：並非所有金鑰大小或曲線皆受到憑證授權單位的支援，因此，應該向憑證授權單位諮詢以瞭解支援的金鑰大小。

如果您選取的金鑰類型為 RSA，則選取金鑰大小	ECDSA，則選取曲線
1024 位（預設）	prime256vi: 256 位元質數體之 X9.62.SECG 曲線 (預設)
1536 位元	secp384r1: 384 位元質數體之 NIST/SECG 曲線
2048 位元	secp521r1: 521 位元質數體之 NIST/SECG 曲線
4096 位元	

9 按一下**產生**以建立憑證簽名請求檔案。

產生**憑證簽名請求**後，瀏覽器視窗底部的狀態區域將會顯示一條描述結果的訊息，**憑證和憑證請求**表格將顯示類別為**擱置的請求**的新項目。

10 按一下**匯出**圖示。隨即顯示**匯出憑證要求**對話方塊。

11 按一下**匯出**圖示，將檔案下載到您的電腦中。隨即顯示**打開*<certificate>***對話方塊。

12 按一下**確定**將檔案儲存在電腦中的目錄。

您已產生**憑證請求**，現在可以將其傳送給您的憑證授權單位進行驗證。

13 按一下**上傳**圖示，以上傳簽署要求的簽署憑證，隨即顯示**上傳憑證**對話方塊。

14 按一下**瀏覽**，以選取檔案。將顯示開啟檔案對話方塊。

15 選擇此檔案。

16 按一下**打開**。

17 按一下**上載**。

設定簡單憑證註冊通訊協定

簡單憑證註冊通訊協定 (SCEP) 用於支援以可縮放的方式安全可靠地向網路裝置頒發憑證。簡單憑證註冊通訊協定有兩種註冊應用情節：

- 由簡單憑證註冊通訊協定伺服器 CA 自動頒發憑證
- 將簡單憑證註冊通訊協定請求設為「待定」，並由 CA 管理員手動頒發憑證。

如需簡單憑證註冊通訊協定的更多資訊，請參見：http://tools.ietf.org/html/draft-nourse-scep-18 (*思科系統簡單憑證註冊通訊協定 draft-nourse-scep-18*)。

若要使用 SCEP 頒發憑證：

1 按第 56 頁「產生憑證簽署請求」中所述的步驟產生簽章請求。

2 捲動至**系統 > 憑證**頁面底部，並按一下**簡單憑證註冊通訊協定**。隨即顯示**簡單憑證註冊通訊協定設定**視窗。

3 從 **CSR 清單**中，SonicOS 會自動選取預設的 CSR 清單。如果您已設定多個 CSR 清單，則可以修改選擇。

4 在 **CA URL** 欄位中輸入憑證授權單位的 URL。

5 如果需要密碼，則在**撤銷密碼（可選）**欄位中輸入此憑證機構的密碼。

6 在**請求數目**欄位中，輸入請求數目。預設值為 **256**。

7 在**輪詢間隔**欄位中，可以修改傳送輪詢訊息的時間間隔預設值。預設值為 **30** 秒。

8 在**最大輪詢時間**欄位中，可以修改防火牆在逾時之前等待輪詢訊息回應的持續時間預設值，此預設值單位為秒。預設值為 **28800** 秒（8 小時）。

9 按一下**簡單憑證註冊通訊協定**，以提交簡單憑證註冊通訊協定註冊。

防火牆隨即將聯絡 CA 以要求憑證。需要的時間取決於 CA 以自動還是手動方式發行憑證。頒發憑證後，憑證將顯示在**系統 > 憑證**頁面中**已匯入的憑證和請求**或**所有憑證**類別下面的可用憑證清單中。

5

設定時間設定

關於設備 | 時間

管理 | 系統安裝 | 設備 | 時間將時間與日期設定定義為時間戳記記錄事件，以自動更新 SonicWall 安全服務，並用於其他內部用途。

預設情況下，SonicWall 安全設備會使用內部的公用 NTP 伺服器清單來自動更新時間。網路時間協定 (NTP) 是用於同步電腦網路中的電腦時鐘時間的協定。NTP 使用國際標準時間 (UTC) 來將電腦時鐘時間同步到毫秒級，有時甚至同步到零點幾毫秒級。

主題：

設定系統時間

您可以在**設備 | 時間**的**系統時間**區段中設定系統時間。

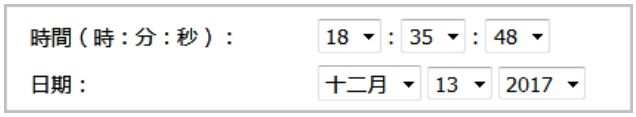
若要設定系統時間:

1 導覽到**設備 | 時間**。

2 從**時區**中，選取您所在的時區。

3 若要設定時間:

- 若要以自動的方式進行，請選取**使用 NTP 自動設定時間**，以使用內部清單中的 NTP (網路時間通訊協定) 伺服器。預設情況下已核取此選項。
- 若要以手動的方式進行，請清除**使用 NTP 自動設定時間**。**時間**與**日期**選項會變成可用狀態。



1) 使用**時間 (hh:mm:ss)** 下拉功能表選取 24 小時制的時間。

2) 從**日期**下拉功能表中選取日期。

4 若要為日光節約時間啟用自動調整，請選取**為日光節約時間自動調整時鐘**。對於遵守日光節約時間的地區，依預設會選取此選項。

5 若要為記錄事件使用國際標準時間 (UTC)，而不是當地時間，請選取**在記錄中顯示 UTC (而不是當地時間)**。 預設情況下未勾選此選項。

6 若要依國際格式顯示日期，在月份前面顯示日期，請選取**按國際格式顯示日期**。

預設情況下未勾選此選項。

7 若要使用手動輸入的 NTP 伺服器清單，而不是使用 NTP 伺服器的內部清單來設定防火牆時鐘，請選取**僅使用自訂的 NTP 伺服器**。

> **重要：**只有當您設定了一個或多個 NTP 伺服器時才選取此選項。如需有關 NTP 伺服器的更多資訊，請參閱第 63 頁「設定 NTP 設定」。

8 按一下**接受**。

設定 NTP 設定

網路時間協定 (NTP) 是用於同步電腦網路中的電腦時鐘時間的協定。NTP 使用國際標準時間 (UTC) 來將電腦時鐘時間同步到毫秒級，有時甚至同步到零點幾毫秒級。

提示：SonicWall 安全裝置使用內部 NTP 伺服器清單，因此手動輸入 NTP 伺服器為可選操作。

主題：

- 第 63 頁「使用 NTP 伺服器以更新防火牆時鐘」
- 第 63 頁「新增 NTP 伺服器」
- 第 64 頁「編輯 NTP 伺服器項目」
- 第 64 頁「刪除 NTP 伺服器項目」

使用 NTP 伺服器以更新防火牆時鐘

若要使用本機伺服器以設定防火牆時鐘:

1. 導覽到**設備 | 時間**。
2. 新增一個或多個 NTP 伺服器，如第 63 頁「設定 NTP 設定」中所述。
3. 選取**使用 NTP 來自動設定時間** (請參閱第 62 頁「設定系統時間」)。 預設情況下未勾選此選項。
4. 若要為 NTP 伺服器設定更新防火牆的頻率，請在**更新間隔 (分鐘數)** 中輸入間隔。預設值為 **60** 分鐘。
5. 按一下**接受**。

新增 NTP 伺服器

若要將 NTP 伺服器新增到防火牆設定中：

1. 導覽到**設備 | 時間**。
2. 在 **NTP 設定**區段中，按一下**新增**。隨即顯示**新增 NTP 伺服器**對話方塊。

3 在 **NTP 伺服器**欄位中輸入遠端 NTP 伺服器的 IP 位址。

4 從 **NTP 驗證類型**下拉功能表中選擇身分驗證類型：

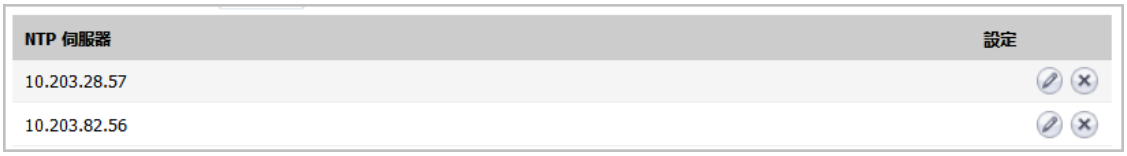
- **無驗證** - 不需要驗證且以下三個選項顯示為灰色。移至步驟 8。
- **MD5** - 需要驗證且以下三個選項為使用中狀態。

5 在**信任金鑰序號**欄位中輸入信任金鑰序號。最小值為 1，最大值為 99999。

6 在**金鑰序號**欄位中輸入金鑰序號。最小值為 1，最大值為 99999。

7 在**密碼**欄位中輸入密碼。

8 按一下**確定**。**NTP 伺服器**部分將顯示伺服器。



編輯 NTP 伺服器項目

若要編輯 NTP 伺服器項目：

1 導覽到**設備 | 時間**。

2 在 **NTP 伺服器**表格中，按一下項目的**編輯**圖示。隨即顯示**編輯 NTP 伺服器**對話方塊，此對話方塊與**新增 NTP 伺服器**對話方塊相同；請參閱第 63 頁「新增 NTP 伺服器」。

3 做出變更。

4 按一下**確定**。

刪除 NTP 伺服器項目

若要刪除 NTP 伺服器項目：

1 導覽到**設備 | 時間**。

2 在 **NTP 伺服器**表格中，按一下項目的**刪除**圖示。

若要刪除全部伺服器：

3 導覽到**設備 | 時間**。

4 在 **NTP 伺服器**表格下方，按一下**全部刪除**。

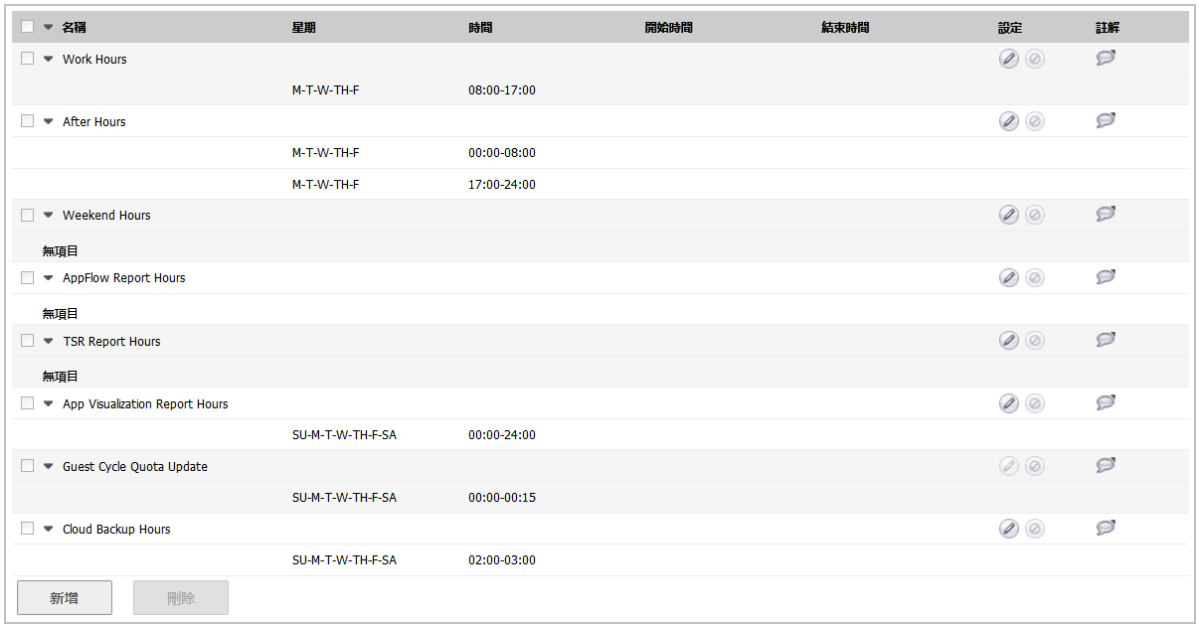
6

設定排程

關於排程

SonicOS 將排程物件及其安全功能與原則結合使用。您可以使用**管理 | 系統安裝 | 設備 | 排程**建立排程物件。可針對特定的安全功能或原則 (規則) 套用排程物件。例如，如果您在**管理 | 原則 | 規則 | 存取規則**頁面上新增存取規則，**新增規則**對話方塊會列出所有可用的預先定義排程物件，以及您使用**設備 | 排程**頁面建立的排程物件。排程可能包含多個用於單個排程的規則實施的日期和時間增量。

關於設備 | 排程



管理 | 系統安裝 | 設備 | 排程可讓您建立及管理預設和自訂排程物件，以針對各種 SonicWall 安全設備功能強制執行排程時間。

附註：您可以修改預設排程，但無法予以刪除。

排程表格顯示所有預先定義和自訂排程。預設排程包括:

Work Hours	AppFlow 報告工時	雲端備份時數
After Hours	應用程式視覺化報告時數	來賓客週期配額更新
Weekend Hours	TSR 報告時間	

主題：

新增自訂排程

若要建立自訂排程:

1 導覽到**管理 | 系統安裝 | 設備 | 排程**。

2 按下**新增**。將顯示**新增排程**對話方塊。

3 在**排程名稱**欄位中，輸入排程的描述性名稱。

4 為**排程類型**選擇下列其中一個選項按鈕:

單次	用於在設定的**開始**和**結束**時間及日期之間的一次性排程。選取此選項後，**單次**下方的欄位會變成可用狀態，而**重覆**下方的欄位會變成灰色。
重覆 (預設)	用於在設定的相同小時和星期時段內重複發生的排程（沒有開始或結束日期）。選取此選項後，**重覆**下方的欄位會變成可用狀態，而**單次**下方的欄位會變成灰色。
混合	用於在設定的開始日期和結束日期之間設定的相同小時和星期時段內重複發生的排程。選擇此選項後，將會啟用此頁面中的所有欄位。

重要： 時間必須為 24 小時制，例如 17:00 代表下午 5 點。

5 如果**單次**下方的欄位為可用狀態，請設定:

- 從**開始**列的下拉功能表中，選取**年**、**月**、**日期**、**時**和**分**，設定開始日期和時間。小時表示為 24 小時制。
- 從**結束**列的下拉功能表中，選取**年**、**月**、**日期**、**時**和**分**，設定結束日期和時間。小時表示為 24 小時制。

6 如果**循環**下方的欄位為可用狀態:

- 選取星期幾的核取方塊以套用至排程，或選取**全部**。
- 在**開始時間**欄位中，輸入排程開始的當日時間。
- 在**停止時間**欄位中，輸入排程停止的當日時間。

7 按一下**新增**，將排程新增至**排程清單**。

8 若要刪除：

- **排程清單**中的現有排程:
  1) 選取排程。
  2) 按一下**刪除**。
- 所有現有排程，按一下**全部刪除**。

9 按一下**確定**。隨即更新**排程**表格。

修改排程

若要修改預設和自訂排程:

1 導覽到**管理 | 系統安裝 | 設備 | 排程**。

2 對於要修改的排程，按一下**編輯**圖示。將顯示**編輯排程**對話方塊。

3 您可以變更排程的任何元件，例如時間、類型及 / 或天數，但預設排程的名稱無法變更，而且欄位會顯示為灰色。若要進行變更，請遵循第 66 頁「新增自訂排程」中的程序。

4 按一下**確定**。

刪除自訂排程

您可以刪除自訂排程，但無法刪除預設排程。

刪除個別排程

若要刪除您建立的個別排程物件:

1 導覽到**管理 | 系統安裝 | 設備 | 排程**。

2 在**排程**表格中，若要刪除:

- 自訂排程，請按一下其**刪除**圖示。
- 多個自訂排程:
  1) 選取要刪除之自訂排程旁的核取方塊。**刪除**會變成可用狀態。
  2) 按一下**刪除**。

刪除所有排程

刪除您所建立的所有排程物件的步驟如下：

1 導覽到**管理 | 系統安裝 | 設備 | 排程**。

2 在**排程**表格中，選取**名稱**欄標頭旁的核取方塊，以選取所有自訂排程。**刪除**會變成可用狀態。

3 按一下**刪除**。

部分 3

使用者管理

- 關於管理使用者
- 設定用於管理使用者的設定
- 管理驗證分割區
- 設定本機使用者與群組
- 管理來賓服務
- 管理來賓帳戶

7

關於管理使用者

關於使用者管理

附註：本主題提供 SonicWall 安全設備之管理功能的概述。

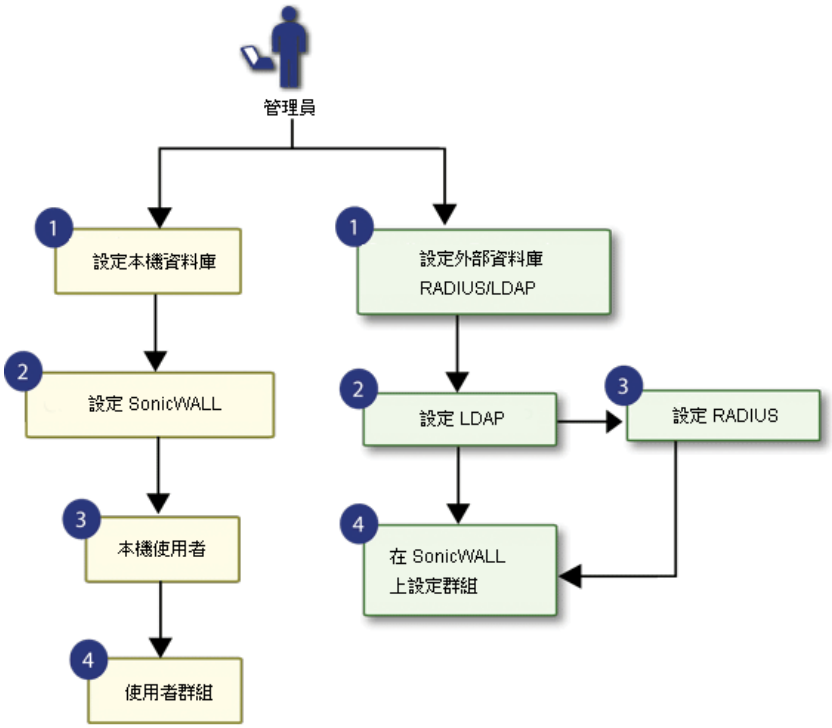
如需下列主題的詳細資訊與程序	請參閱下列主題
設定使用者驗證、Web 登入、工作階段管理、RADIUS 計費，以及原則	第 110 頁「設定用於管理使用者的設定」
在具有多個非互連網域的環境中，建立分割區以進行使用者驗證	第 164 頁「管理驗證分割區」
建立及管理本機使用者與本機群組	第 191 頁「設定本機使用者與群組」
設定來賓服務與帳戶	第 208 頁「管理來賓服務」和第 213 頁「管理來賓帳戶」

SonicWall 安全設備 (防火牆) 提供本機管理與遠端管理驗證使用者的機制。使用者層級驗證可讓使用者從網際網路上的遠端位置存取 LAN，並可以對嘗試存取網際網路的 LAN 使用者強制或繞過內容篩選原則。您還可以只允許驗證的使用者存取 VPN 通道和在加密的連接內傳送資料。

防火牆在所有使用者嘗試存取不同區域（例如 WAN、VPN、WLAN）的網路資源因而產生通過防火牆的網路流量時立即進行身分驗證。防火牆不會驗證登入 LAN 上的電腦，但僅執行本機任務的使用者。使用者級別的驗證可以使用本機使用者資料庫、LDAP、RADIUS 或者本機資料庫與 LDAP 或 RADIUS 的組合執行。對於有較多使用者的網路，使用 LDAP 或 RADIUS 伺服器進行使用者驗證可能更為高效。

SonicOS 還提供單點登入 (SSO) 功能。SSO 可以結合 LDAP 使用。請參閱使用者管理拓撲。

使用者管理拓撲



主題：

- 第 72 頁「使用本機使用者和群組進行驗證」
- 第 75 頁「使用 RADIUS 進行驗證」
- 第 75 頁「使用 LDAP/Active Directory/eDirectory 驗證」
- 第 79 頁「關於單一登入」
- 第 89 頁「安裝單點登入代理和/或終端服務代理」
- 第 106 頁「關於多管理員支援」
- 第 108 頁「設定多管理員支援」

使用本機使用者和群組進行驗證

主題：

- 第 72 頁「關於使用者資料庫」
- 第 73 頁「關於使用者群組」

關於使用者資料庫

防火牆提供本機資料庫以儲存使用者和群組資訊。您可以設定防火牆以使用此本機資料庫驗證使用者和控制他們的網路存取權限。在存取網路的使用者數相對較少時，本機資料庫是優於 LDAP 或 RADIUS 的一種選擇。建立很多使用者和群組的項目很花時間，但在項目建立完成後，維護起來並不難。

防火牆上的本機資料庫支援的使用者數因平台支援的最大使用者值表格顯示的平台而不同。最大的整體使用者限制等於 SSO 使用者的最大值，原生使用者的最大值等於 SSO 使用者的最大值。Web 使用者的最大值是從 web 和 GVC、SSL-VP 和 L2TP 用戶端登入的聯合使用者的最大值。

平台支援的最大使用者值

平台	SSO 使用者	Web 使用者	Web 伺服器執行緒	平台	SSO 使用者	Web 使用者	Web 伺服器執行緒
SM 9600	100,000	5,000	30	TZ600	500	500	8
SM 9400	90,000	5,000	30	TZ500/TZ500W	500	500	8
SM 9200	80,000	5,000	20	TZ400/TZ400W	500	150	8
NSA 6600	70,000	5,000	20	TZ300/TZ300W	500	150	8
NSA 5600	60,000	3,000	16				
NSA 4600	50,000	2,000	10				
NSA 3600	40,000	1,500	8	SOHO W	250	150	8
NSA 2650	30,000	1,000	8				
NSA 2600	30,000	1,000	8				

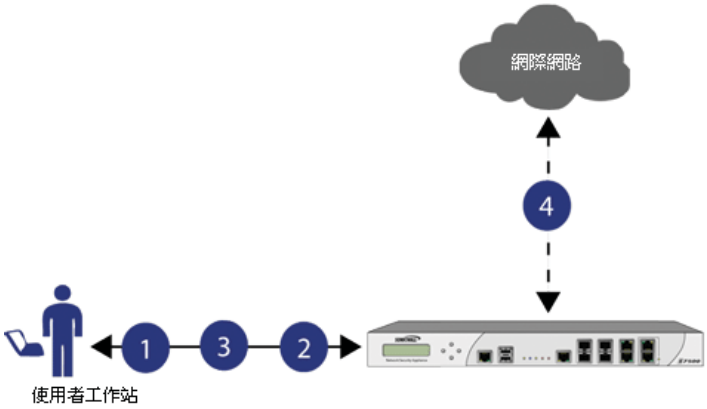
重要：若要達到處理數字的最大效率，SonicWall 建議：

- 無線使用者儘量使用 RADIUS 計費。
- 使用 SSO 代理版本 4 或更高版本；不使用任何早於版本 3.6.10 的 SSO 代理。
- 盡可能用 LogWatcher 在 DC 記錄模式下使用 SSO 代理。
- 如果需要用 NetAPI 或 WMI 來識別非網域使用者，則在不同的代理中識別。
- 盡可能設定排除來禁止任何未通過 SSO 識別的事物將之觸發。

關於使用者群組

要對使用者套用內容篩選服務 (CFS) 原則，使用者必須是本機群組的成員，且向群組套用了 CFS 原則。要使用 CFS，您不能使用 LDAP 或 RADIUS，除非將這種方法與本機身分驗證組合使用。在使用組合的身分驗證方法以運用 CFS 原則時，本機群組的名稱必須精確相符 LDAP 或 RADIUS 群組的名稱。在使用 **LDAP + 本機使用者**驗證方法時，您可以將 LDAP 伺服器中的群組匯入到防火牆上的本機資料庫。這大幅簡化了將套用 CFS 原則的符合群組的建立。請參閱使用者管理：使用本機使用者和群組進行驗證。

使用者管理：使用本機使用者和群組進行驗證



1. 使用者嘗試存取網路。
2. SNWL 需要使用者驗證：將工作站重新導向以進行驗證。
3. 使用者利用憑證進行驗證。
4. SNWL 本機資料庫根據使用者權限授予或拒絕其存取。

SonicOS 管理介面提供建立本機使用者和群組帳戶的方法。您可以新增使用者和編輯任何使用者的設定，包括以下設定:

群組成員資格	使用者可以屬於一個或多個本機群組。所有使用者預設屬於 **Everyone** 和 **Trusted Users** 群組。您可以移除使用者的這些群組成員身分，並新增其他群組的成員身分。
VPN 存取	您可以設定此使用者可以通過 VPN 用戶端發起存取的網路。在設定 VPN 存取設定時，您可以從網路清單中選擇。網路由其位址群組或位址物件名稱指定。 **附註：**使用者和群組的 VPN 存取設定會影響遠端用戶端使用 GVC、NetExtender 和 SSL VPN 虛擬辦公室書籤存取網路資源的能力。要允許 GVC、NetExtender 或虛擬辦公室使用者存取網路資源，必須將網路位址物件或群組新增到「VPN 存取」標籤上的「允許」清單。

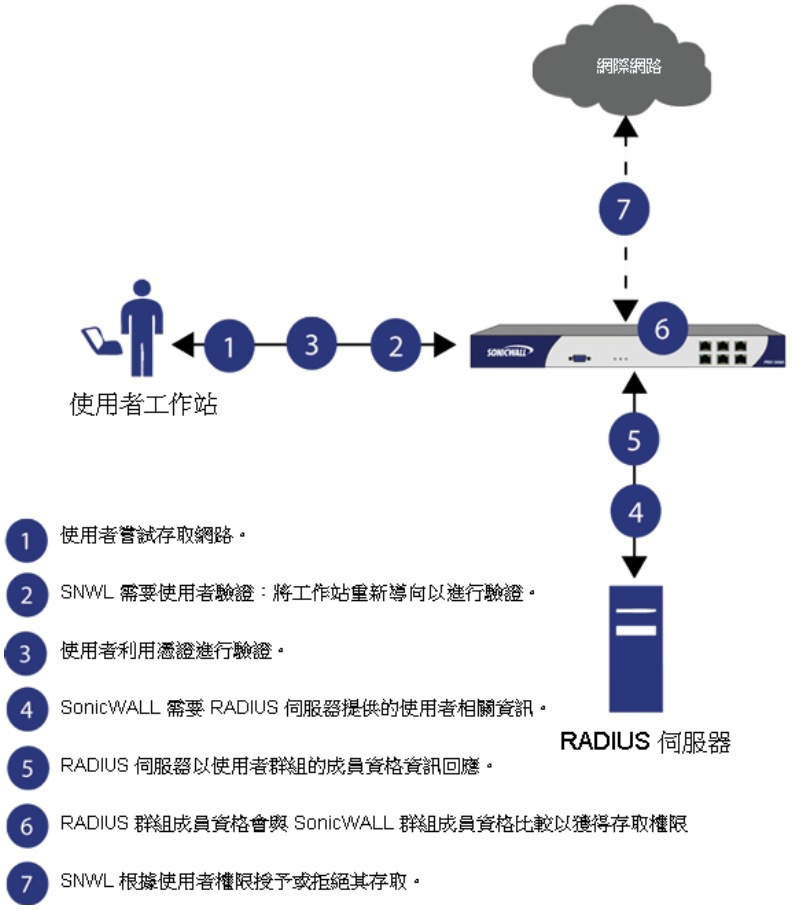
您還可以新增或編輯本機群組。以下是群組的可配置設定:

群組設定	對於管理員群組，您可以設定 SonicOS 以允許在未啟用登入狀態快顯視窗時登入管理介面。
群組成員	群組成員可以是本機使用者或其他本機群組。
VPN 存取	群組 VPN 存取的設定方式與使用者的 VPN 存取相同。您可以設定此群組成員可以通過 VPN 用戶端發起存取的網路。在設定 VPN 存取設定時，您可以從網路清單中選擇。網路由其**位址群組**或**位址物件**名稱指定。
CFS 原則	您可以對群組成員套用內容篩選 (CFS) 原則。只有在防火牆目前獲得專業版內容篩選服務授權時，才可以使用 CFS 原則設定。

使用 RADIUS 進行驗證

遠端驗證撥入使用者服務 (RADIUS) 是一種網路通訊協定，為 SonicWall 安全設備提供集中驗證、授權和計費，以驗證嘗試存取網路的使用者。RADIUS 伺服器包含帶有使用者資訊的資料庫， 並使用密碼驗證協定 (PAP)、質詢握手身分驗證協定 (CHAP)、Microsoft CHAP (MSCHAP) 或 MSCHAPv2 等身分驗證方案檢查使用者憑證。請參閱使用者管理：使用 RADIUS 進行驗證。

使用者管理：使用 RADIUS 進行驗證



RADIUS 與 LDAP 極為不同，除了主要提供安全驗證以外，還可以提供各項目的很多屬性，包括可用於傳回使用者群組成員身分的各種屬性。RADIUS 可以儲存數千使用者的資訊，如果有很多使用者需要存取網路，這會是一種好的使用者驗證方法。

使用 LDAP/Active Directory/eDirectory 驗證

輕型目錄存取協定 (LDAP) 定義了用於儲存和管理網路中元素的資訊的目錄服務結構，資訊包括使用者帳戶、使用者群組、主機和伺服器等。有多個不同的標準使用 LDAP 管理使用者賬戶、群組和權限。有些是您可以使用 LDAP 管理的專有系統，例如 Microsoft Active Directory (AD)；有些是提供 LDAP API 用於管理使用者儲存庫資訊的專有系統，例如 Novell eDirectory。有些是開放的標準如 SAMBA，即 LDAP 標準的實施。

除了 RADIUS 和本機使用者資料庫以外，SonicOS 還支援使用 LDAP 進行使用者驗證，支援多種架構，包括 Microsoft Active Directory、Novell eDirectory 目錄服務，以及應該允許 SonicOS 與任何架構互動之完全可設定的使用者定義選項。

Microsoft Active Directory 還適用 SonicWall 單點登入和 SonicWall SSO 代理。如需詳細資料，請參閱第 79 頁「關於單一登入」。

主題：

- 第 76 頁「LDAP 術語」
- 第 77 頁「SonicOS 中支援的 LDAP 目錄服務」
- 第 77 頁「LDAP 使用者群組鏡像」

LDAP 術語

在使用 LDAP 及其變數時，以下術語相當實用。

Active Directory (AD)	Microsoft 目錄服務，通常結合基於 Windows 的網路使用。Microsoft Active Directory 與 LDAP 相容。
屬性	儲存在 LDAP 目錄的物件中的資料項。物件可以有必需的屬性或允許的屬性。例如，dc 屬性是 dcObject（網域元件）物件的必需屬性。
cn	常用名稱屬性是 LDAP 中很多物件類別的必要元件。
dc	網域元件屬性通常存在於識別名稱的根中，且通常是必要屬性。
dn	「識別名稱」，是使用者或其他物件的全域唯一名稱。這由多個元件組成，通常以常用名稱 (cn) 元件開頭，以指定為兩個或多個網域元件 (dc) 的網域結尾。例如'cn=john,cn=users,dc=domain,dc=com'
eDirectory	用於基於 Novell NetWare 的網路的 Novell 目錄服務。Novell eDirectory 有可用於管理的 LDAP 閘道。
項目	儲存在 LDAP 目錄中的資料。項目儲存在「屬性/值」（或名稱/值）對中，其中，屬性按「物件類別」定義。範例項目有 cn=john，其中 cn（常用名稱）是屬性，john 是值。
物件	在 LDAP 術語中，將目錄中的項目稱為物件。在 LDAP 用戶端的 SonicOS 實施中，關鍵的物件是「使用者」和「群組」物件。LDAP 的不同實施可以使用不同形式指代這些物件類別，例如，Active Directory 指代將使用者物件稱為使用者，將群組物件稱為群組，而 RFC2798 將使用者物件稱為 inetOrgPerson，將群組物件稱為 groupOfNames。
物件類別	定義 LDAP 目錄可能包含的項目類型。AD 使用的範例物件類別有使用者或群組。 Microsoft Active Directory 的類可在 http://msdn.microsoft.com/library/ 瀏覽。
ou	組織單位屬性是大多數 LDAP 架構實施的必要元件。
架構	定義可儲存在目錄中的資料類型，以及如何儲存這些資料的一組規則或結構。資料以項目形式儲存。
TLS	傳送層安全性，SSL 的 IETF 標準化版本 (安全通訊端層)。支援 TLS 1.1 和 1.2。

SonicOS 中支援的 LDAP 目錄服務

為了與公司網路中最常用的目錄服務整合，SonicOS 支援與下列 LDAP 架構整合:

Microsoft Active Directory	Samba SMB
RFC2798 InetOrgPerson	Novell eDirectory
RFC2307 網路資訊服務	使用者定義的結構

SonicOS 為執行以下通訊協定的目錄伺服器提供支援:

LDAPv3 (RFC2251-2256, RFC3377)	LDAPv2 (RFC3494)
通過 TLS 的 LDAPv3 (RFC2830)	LDAP 提名 (RFC2251)
帶有 STARTTLS 的 LDAPv3 (RFC2830)	

LDAP 使用者群組鏡像

LDAP 使用者群組鏡像用於從 LDAP 伺服器向 SonicWall 安全設備自動複製 LDAP 使用者群組設定。您可以在 LDAP 伺服器上專門管理 LDAP 使用者群組，且不需要手動複製防火牆上的設定。使用者群組設定定期從 LDAP 伺服器上讀取和複製到防火牆。

複製到防火牆的 LDAP 使用者群組名稱包括以下格式的網域名稱: `name@domain.com`。 這可以確保來自不同網域的使用者群組名稱唯一。

這些功能和限制適用於鏡像的 LDAP 使用者群組:

- 您只能刪除 LDAP 伺服器上的 LDAP 使用者群組。他們不能刪除 SonicWall 安全設備上的鏡像 LDAP 使用者群組。在 LDAP 伺服器上刪除使用者群組時，也會自動刪除防火牆上的已鏡像群組。
- 您只能編輯 LDAP 伺服器上的 LDAP 使用者群組名稱 (及其註解欄位)。他們不能編輯防火牆上已鏡像的 LDAP 使用者群組名稱或其註解欄位。防火牆上的註解欄位顯示從 `LDAP 鏡像`。
- 您可以將使用者作為成員新增到 SonicWall 安全設備上的 LDAP 使用者群組。
- 您不能將群組新增到 SonicWall 安全設備上的其他群組。預設使用者群組只能在 LDAP 伺服器上設定。
- 您可以在 SonicWall 安全設備上設定內容，例如，為 LDAP 使用者群組設定 VPN、SSL VPN、CFS 原則以及 ISP 原則 (如需關於原則的詳細資訊，請參閱 *SonicOS 原則*。

  附註：如果已在任何存取規則、應用程式控制規則或其他原則中設定 LDAP 使用者群組，則不會刪除這些使用者群組。

- 當您停用 LDAP 使用者群組鏡像時，不會刪除 SonicWall 安全設備上的已鏡像使用者群組。它們已經變更，所以您可以手動予以刪除。如果未手動刪除本機鏡像使用者群組，則可以重新啟用。
- 系統在 SonicWall 安全設備上建立鏡像群組時，且鏡像群組的名稱符合使用者建立的已存在（非鏡像）本機群組，則不會替換本機群組。更新本機群組成員身分，以反映在 LDAP 伺服器上設定的群組嵌套。
- 如果系統在 LDAP 伺服器上找到名稱與 SonicWall 安全裝置上的一個預設使用者群組相同的使用者群組，則不會在 SonicWall 安全裝置上建立鏡像使用者群組。更新預設使用者群組中的成員身分，以反映在 LDAP 伺服器上設定的群組嵌套。
- 對於在 SonicOS 6.2 之前版本中建立的群組，如果 SonicWall 安全裝置上存在只有簡單名稱（無網域）的本機使用者群組，且此名稱符合 LDAP 伺服器上的使用者群組名稱（包含網域），將在 SonicWall 安全裝置上建立新本機使用者群組，且對其賦予與 LDAP 伺服器上對應使用者群組相同的網域。原始的本機使用者群組仍保留為無網域。給原群組的使用者賦予 LDAP 群組、新本機鏡像群組和原本機群組（無網域）的成員身分。

將 LDAP 整合至 SonicWall 安全設備

整合防火牆與 LDAP 目錄服務需要設定 LDAP 伺服器以進行憑證管理，在防火牆上安裝正確的憑證和設定防火牆以使用來自 LDAP 伺服器的資訊。如需 LDAP 的簡介，請參見第 75 頁「使用 LDAP/Active Directory/eDirectory 驗證」。

主題：

準備 LDAP 伺服器以進行整合

在開始 LDAP 設定之前，您應該準備 LDAP 伺服器和 SonicWall 以獲得 LDAP over TLS 支援。這需要：

- 在 LDAP 伺服器上安裝伺服器憑證。
- 安裝 CA（憑證授權單位）憑證用於在防火牆上發佈 CA。

以下過程介紹如何在 Active Directory 環境執行這些任務。

設定 Active Directory 伺服器上的 CA

若要設定 Active Directory 伺服器上的 CA：

ⓘ **提示：**如果已安裝憑證服務，請跳過前五個步驟。

1. 移至**開始 > 設定 > 控制台 > 新增/移除程式**
2. 選擇**新增/移除 Windows 元件**
3. 選擇**憑證服務**
4. 提示時選擇**企業根 CA**。
5. 輸入請求的資訊。如需 Windows 系統的憑證的資訊，請參閱 http://support.microsoft.com/kb/931125。
6. 啟動**網域安全原則**應用程式：移至**開始 > 執行**，然後執行命令：**dompol.msc**。
7. 打開**安全設定 > 公開金鑰原則**。
8. 右鍵按一下**自動憑證請求設定**。
9. 選擇**新增 > 自動憑證請求**。
10. 在精靈中逐步前進，然後從清單中選擇**網域控制器**。

從 Active Directory 伺服器匯出 CA 憑證

從 AD 伺服器匯出 CA 憑證的步驟為：

1. 啟動**憑證授權單位**應用程式：**開始 > 執行 > certsrv.msc**。
2. 右鍵按一下您建立的 CA，然後選擇**屬性**。
3. 在**一般**標籤，按一下**檢視憑證**按鈕。
4. 在**詳細資料**標籤，選擇**複製到檔案**。
5. 在精靈中逐步前進，然後 **Base-64 編碼 X.509 (.cer)** 格式。
6. 指定儲存憑證使用的路徑和檔案名稱。

將 CA 憑證匯入到 SonicOS

若要將 CA 憑證匯入到 SonicOS：

1 移至**系統 > CA 憑證**。

2 選擇**新增新 CA 憑證**。瀏覽並選擇您剛匯出的憑證檔案。

3 按一下**匯入憑證**按鈕。

按組織單位的 LDAP 群組成員

「按組織單位的 LDAP 群組成員」功能用於在 LDAP 伺服器上為某些組織單位 (OU) 中的使用者設定 LDAP 規則和原則。

使用者登入時，如果將使用者群組設為按 LDAP 位置賦予成員身分，則使用者成為符合其 LDAP 位置的所有群組的成員。

您可以將任何本機群組設為成員按其在 LDAP 目錄樹狀目錄中位置進行設定的群組，包括預設本機群組（**Everyone** 群組和 **Trusted Users** 群組除外）。

如果使用者是設定為 LDAP 位置的任何本機群組的成員：

- 將沿用這些本機群組在 LDAP 樹狀目錄中的位置。
- 將檢查使用者的本機群組相對於所有其他本機群組的位置。如果任何其他群組有與使用者所屬群組的相同 LDAP 位置，在此登入工作階段中，自動將使用者設為這些群組的成員。

當使用者嘗試登入時，不管成功與否，將把使用者的識別名稱都記錄在事件記錄中。如果使用者未能獲得期望的群組成員身分，記錄將有助於故障排除。

關於單一登入

主題：

什麼是單點登入？

單點登入 (SSO) 是提供對多個網路資源的特許存取的透明使用者驗證機制，其中，通過單一網域登入工作站或通過 Windows 終端服務或 Citrix 伺服器。

SonicWall 安全設備提供使用單點登入代理（SSO 代理）的 SSO 功能和 SonicWall 終端服務代理 (TSA) 識別使用者活動。SSO 代理根據工作站 IP 位址識別使用者。TSA 通過伺服器 IP 位址、使用者名稱和網域的組合識別使用者。

SonicWall SSO 在結合 Samba 使用時，也適用於 Mac 和 Linux 使用者。此外，瀏覽器 NTLM 驗證允許 SonicWall SSO 驗證傳送 HTTP 流量的使用者，而不涉及 SSO 代理或 Samba。

SonicWall SSO 在 SonicOS 管理介面的**使用者> 設定**頁面設定。SSO 獨立於**登入的驗證方法**設定，後者可同時用於 VPN/L2TP 用戶端使用者或管理使用者的身分驗證。

根據來自 SonicWall SSO 代理或 TSA 的資料，安全設備查詢 LDAP 或本機資料庫確定群組成員身分。防火牆原則選擇性檢查成員身分以控制給哪些人存取權限，成員身分還可用於選擇內容篩選和應用程式控制的原則以控制允許成員存取的內容。將從 SSO 獲得的使用者名稱用於使用者的流量和事件記錄報告和 AppFlow 監控中。

設定的非使用中時間計時器適用於 SSO，但工作階段限制不適用，不過，登出的使用者在再次傳送流量時會自動而明確地重新登入。

直接登入到工作站或終端服務/Citrix 伺服器但未登入到網域的使用者將不會接受身分驗證，除非他們傳送 HTTP 流量且啟用了瀏覽器 NTML 身分驗證（不過可以選擇性對其進行身分驗證以給予有限存取權限）。對於未經過 SonicWall SSO 驗證的使用者，介面會顯示一則訊息，表示需要手動登入安全設備，才能進一步進行驗證。

給受到識別但缺少群組成員身分的使用者設定的原則規則重新導向至「封鎖存取」頁面。

SonicWall SSO 的優點

SonicWall SSO 是根據管理員設定的群組成員身分和原則符合情況利用單點登入提供對多個網路資源存取權限的可靠而省時的功能。SonicWall SSO 對最終使用者透明，且需要最少的管理員設定。

SonicWall SSO 通過根據工作站 IP 位址流量或來自伺服器 IP 位址上指定使用者的流量（對於終端服務或 Citrix）自動確定使用者何時登入或登出，因而安全、便捷。SSO 身分驗證適用於可以使用 SonicWall Directory Connector 相容協定返回位於工作站或終端服務/Citrix 伺服器 IP 位址的使用者身分的任何外部代理。

SonicWall SSO 可用於使用使用者級別身分驗證的防火牆的任何服務，包括內容篩選服務 (CFS)、存取規則、群組成員身分和繼承以及安全服務（IPS、GAV 和防間諜軟體）包含/排除清單。

SonicWall SSO 代理可以安裝在 LAN 上的任何 Windows 伺服器上，TSA 可以安裝在任何終端伺服器上。SonicWall SSO 的其他優點包括：

設定簡單	使用者只需要登入一次，即可獲得多個資源的自動存取權限。
改善的使用者體驗	Windows 網域憑證可用於對任何流量類型驗證使用者身分，而無需使用 Web 瀏覽器登入裝置。
為使用者提供透明性	使用者無需重新輸入使用者名稱和密碼進行驗證。
安全通訊	用於資料傳輸防護的共用金鑰加密。
多個 SSO 代理	最多支援 8 個代理以提高安裝容量
多個 TSA	支援多個終端服務代理（每個終端伺服器一個）。數目取決於 SonicWall 網路安全裝置的型號，範圍從 8 至 512。
登入機制	適用於任何通訊協定，並非僅限 HTTP。
瀏覽器 NTLM 驗證	SonicWall SSO 可以驗證傳送 HTTP 流量的使用者身分，而無需使用 SSO 代理。

Mac 與 Linux 支援	使用 Samba 3.5 及更高版本，SonicWall SSO 支援 Mac 和 Linux 使用者。
按區域實施	如果在事件記錄或 AppFlow 監控中進行使用者識別，即使防火牆存取規則或安全服務原則未自動啟動，也可以為來自任何區域的流量觸發 SonicWall SSO。

平台和支援的標準

SSO 代理與支援 SonicOS SSO 的所有 SonicWall 版本相容。TSA 受支援。

SSO 功能支援 LDAP 和本機資料庫協定。SonicWall SSO 支援 SonicWall Directory Connector。為了使 SonicWall SSO 的所有功能可以正常工作，SonicOS 應使用 Directory Connector 3.1.7 或更高版本。

要結合使用 SonicWall SSO 與 Windows 終端服務或 Citrix，必須安裝 SonicOS 6.0 或更高版本，且必須在伺服器上安裝 SonicWall TSA。

要結合使用 SonicWall SSO 和瀏覽器 NTLM 驗證，必須安裝 SonicOS 6.0 或更高版本。瀏覽器 NTLM 驗證不需要 SSO 代理。

除非使用了僅瀏覽器 NTLM 驗證，否則使用 SonicWall SSO 需要在可以連至用戶端和從裝置連接（直接連接或通過 VPN 路徑）的 Windows 網域的伺服器上安裝 SSO 代理，且/或者在網域的任何終端伺服器上安裝 TSA。

執行 SSO 代理必須滿足以下要求：

- UDP 連接埠 2258（預設）必須開放，防火牆預設使用 UDP 連接埠 2258 與 SonicWall SSO 代理通訊，如果設定了自訂連接埠取代 2258，則這項要求適用於自訂連接埠
- 有最新 Service Pack 的 Windows Server
- .NET Framework 2.0
- Net API 或 WMI

附註：Mac 和 Linux PC 不支援 SSO 代理使用的 Windows 網路請求，因此需要安裝 Samba 3.5 或更高版本才能使用 SonicWall SSO。如果未安裝 Samba，Mac 和 Linux 使用者仍可以存取，但需要登入。如果將原則規則設為需要身分驗證，可能重新導向這些使用者至登入提示。如需詳細資料，請參閱第 103 頁「Mac 和 Linux 使用者調適」。

若要執行 TSA，必須滿足以下要求:

- UDP 連接埠 2259（預設）必須在安裝 TSA 的所有終端伺服器上開放，防火牆預設使用 UDP 連接埠 2259 與 SonicWall TSA 代理通訊，如果設定了自訂連接埠取代 2259，則這項要求適用於自訂連接埠
- 有最新 Service Pack 的 Windows Server
- Windows 終端伺服器系統上安裝的 Windows 終端服務或 Citrix

單點登入的工作方式

SonicWall SSO 需要最低管理員設定且對使用者透明。

以下情況將觸發 SSO:

- 要求使用者驗證的防火牆存取規則套用於並非來自 WAN 區域的流量
- 如果存取規則中未指定使用者群組，但出現以下任一情況，就會對區域上的所有流量觸發 SSO，而非僅針對下列情況的流量:
  - 區域上啟用了 CFS，且設定了多 CFS 原則
  - 區域上啟用了 IPS，且 IPS 原則要求身分驗證

- 區域上啟用了防間諜軟體，且防間諜軟體原則要求身分驗證
- 要求身分驗證的應用程式控制原則套用於來源區域
- 對區域設定了按區域的 SSO 實施

SSO 使用者表格也用於安全服務需要的使用者和群組識別，這些安全服務包括內容篩選、入侵保護、防間諜軟體和應用程式控制。

使用 SSO 代理的 SonicWall SSO 身分驗證

對於單個 Windows 工作站上的使用者，SSO 工作站上的 SSO 代理處理來自防火牆的身分驗證請求。使用 SSO 代理的 SonicWall SSO 身分驗證有六個步驟，如下圖所示。

在使用者流量通過防火牆時，即啟動 SSO 身分驗證過程。例如，當使用者存取網際網路時。在防火牆向執行 SSO 代理（SSO 工作站）的身分驗證代理傳送「使用者名稱」請求和工作站 IP 位址時，將暫時封鎖和儲存使用者傳送的封包。

執行 SSO 代理的身分驗證代理為防火牆提供目前登入到工作站的使用者名稱。將為登入的使用者建立使用者 IP 表項目，類似於 RADIUS 和 LDAP。

使用終端服務代理的 SonicWall SSO 身分驗證

對於從終端服務或 Citrix 伺服器登入的使用者，TSA 在身分驗證過程中取代 SSO 代理。過程有以下幾點不同：

- TSA 在使用者登入的相同伺服器上執行，且在傳送至防火牆的初始通知中包含使用者名稱和網域以及伺服器 IP 位址。
- 按使用者編號和 IP 位址識別使用者（對於非終端服務使用者，任意 IP 位址上只有一個使用者，因此不使用使用者編號）。非零使用者編號以 *x.x.x.x* `user` *n* 格式顯示在 SonicOS 管理介面上，其中，*x.x.x.x* 是伺服器 IP 位址，*n* 是使用者編號。
- 在使用者登出時，TSA 向 SonicOS 傳送結束通知，不會進行輪詢。

識別使用者後，安全設備查詢 LDAP 或本機資料庫（基於管理員設定）以查找使用者群組的成員身分，將其與原則相符合，並相應地向使用者授予或限制存取權限。成功完成登入次序後，將傳送儲存的封包。如果在完成次序前收到來自相同來源位址的封包，則只儲存最近的封包。

執行 SSO 代理的身分驗證代理以<網域>/<使用者名稱>格式返回使用者名稱。對於本機設定的使用者群組，可將使用者名稱設為:

- 從執行 SSO 代理的驗證代理傳回的完整名稱 (設定防火牆本機使用者資料庫中的名稱以進行比對)。
- 去除網域元件的簡單使用者名稱 (預設)。

對於 LDAP 協定，通過建立 `dc`（網域元件）屬性符合網域名稱的網域類物件的 LDAP 搜尋將<網域>/<使用者名稱>格式轉換為 LDAP 識別名稱。如果找到物件，其識別名稱會作為目錄子樹狀目錄以搜尋使用者物件。例如，如果傳回的使用者名稱是 `SV/bob`，則會搜尋帶有 `objectClass=domain` 和 `dc=SV` i 的物件。如果傳回的物件的識別名稱為 `dc=sv,dc=us,dc=sonicwall,dc=com`，將在此目錄子樹狀目錄下建立對 `objectClass=user` 和 `sAMAccountName=bob` 的物件搜尋 (以 Active Directory 為例)。如果未找到網域物件，將從目錄樹狀目錄頂部搜尋使用者物件。

找到網域物件後，儲存資訊以避免搜尋相同物件。如果嘗試在儲存的網域中查找使用者失敗，則儲存的網域資訊會予以刪除，並針對網域物件進行其他搜尋。

與使用 TSA 的 SSO 相比，使用 SSO 代理的 SonicWall SSO 對使用者登出的處理略有不同。安全設備以可設定的頻率輪詢執行 SSO 代理的身分驗證代理，以確定使用者何時登出。使用者登出時，執行 SSO 代理的身分驗證代理向防火牆傳送「使用者已登出」的回應，以此確認使用者已登出並終止 SSO 工作階段。與安全設備輪詢不同，TSA 本身會針對登出事件監控終端服務/Citrix 伺服器，並同時通知安全設備，終止

SSO 工作階段。對於這兩種代理，可以設定可設定的非使用中時間計時器，對於 SSO 代理，可以設定使用者名稱請求輪詢比率（設定短輪詢時間以快速偵測登出事件，或設定較長的輪詢時間降低系統花費）。

使用瀏覽器 NTLM 驗證的 SonicWall SSO 驗證

對於使用基於 Mozilla 的瀏覽器（包括 Internet Explorer、Firefox、Chrome 和 Safari）瀏覽的使用者，防火牆通過 NTLM（NT LAN 管理器）身分驗證支援識別。NTLM 是稱為「整合 Windows 安全」的瀏覽器身分驗證套件的一部分，受所有基於 Mozilla 的瀏覽器支援。NTLM 允許從裝置至瀏覽器的直接身分驗證請求，不涉及 SSO 代理。NTLM 通常用於沒有網域控制器的情況，例如通過 Web 遠端驗證使用者。

NTLM 驗證目前支援 HTTP，但不適用於 HTTPS 流量。

在 SSO 代理嘗試獲取使用者資訊前後，可以嘗試瀏覽器 NTLM 驗證。例如，如果先嘗試 SSO 代理但未能識別使用者，且流量是 HTTP，就會嘗試 NTLM。

若要對 Linux 或 Mac 用戶端以及 Windows 用戶端使用這種方法，您也可以啟用 SSO 探查用戶端的 **NetAPI** 或 **WMI**，這取決於 SSO 代理的具體設定。這會導致防火牆在請求 SSO 代理識別使用者之前，探查 NetAPI/WMI 連接埠上的回應。如果沒有回應，這些裝置的 SSO 立即失敗。對於：

- 對於 Windows PC，此類探查一般有效（除非個人防火牆將之封鎖）並使用 SSO 代理。
- 對於 Linux/Mac PC（假定未設定為執行 Samba 伺服器），探查將失敗，將繞過 SSO 代理，且在傳送 HTTP 流量時使用 NTLM 驗證。

在使用者使用 HTTP 瀏覽前，NTLM 無法識別使用者，所以將此前的所有流量視為未識別。此將套用預設的 CFS 原則，任何需要驗證使用者的規則都不會讓流量通過。

如果 NTLM 設定為在 SSO 代理之前使用，如果先收到 HTTP 流量，則會使用 NTLM 驗證使用者。如果先收到非 HTTP 流量，則會使用 SSO 代理進行驗證。

SSO 代理的工作方式

SSO 代理必須安裝在 Windows 網域可使用 IP 位址或使用 VPN 等路徑直接與用戶端和防火牆通訊的任何工作站或伺服器上。不過，建議 SSO 代理安裝在個別獨立的工作站或伺服器上。如需 SSO 代理的安裝說明，請參閱第 89 頁「安裝 SonicWall SSO 代理」。

支援多 SSO 代理以容納有數千使用者的大型安裝。您最多可以設定八個 SSO 代理，分別都在您網路中的專用、高效能 PC 上執行。

附註：使用 NetAPI 或 WMI 時，SSO 代理可支援約多達 2500 位使用者，依據其所執行硬體的效能等級，其在防火牆上的設定方式以及其他網路相關因素而定。根據類似的因素，當設定為從網域控制器安全記錄讀取，一個 SSO 代理可以支援透過機制是別的大量使用者，最多可能多達 50,000 位以上的使用者。

SSO 代理僅與用戶端和防火牆通訊。SSO 代理使用共用密碼加密 SSO 代理和防火牆之間的訊息。

附註：共用密碼在 SSO 代理中產生，在 SSO 設定期間在防火牆中輸入的金鑰必須完全符合 SSO 代理產生的金鑰。

防火牆通過預設的連接埠 2258 查詢 SSO 代理。然後，SSO 代理在用戶端和防火牆之間通訊以確定用戶端的使用者 ID。防火牆以管理員設定的頻率輪詢 SSO 代理以持續確認使用者的登入狀態。

記錄

SSO 代理根據管理員選擇的記錄層級向 Windows 事件記錄傳送記錄事件訊息。

防火牆還在其事件記錄中記錄 SSO 代理特定的事件：

附註：SSO 代理特定的記錄訊息的**注釋**欄位將包含文字<網域/使用者名稱>，通過 SSO 代理驗證身分。如需關於事件記錄的詳細資訊，請參閱 *SonicOS 調查*。

使用者登入被拒 - 原則規則不允許	已識別使用者，但使用者不屬於封鎖使用者流量之原則所允許的任何使用者群組。
使用者登入被拒 - 在本機找不到	在本機未找到使用者，而且在防火牆中已選取**僅允許本機列出的使用者**。
使用者登入被拒 - SSO 代理逾時	嘗試聯絡 SSO 代理已逾時。
使用者登入被拒 - SSO 代理設定錯誤	SSO 代理未正確設定，無法允許此使用者存取。
使用者登入被拒 - SSO 代理通訊問題	與執行 SSO 代理的工作站通訊時發生問題。
使用者登入被拒 - SSO 代理名稱解析失敗	SSO 代理無法解析使用者名稱。
SSO 代理傳回的使用者名稱太長	使用者名稱太長。
SSO 代理傳回的網域名稱太長	網域名稱太長。

終端服務代理的工作方式

TSA 可以安裝在已安裝終端服務或 Citrix 的任意 Windows 伺服器上。伺服器必須屬於可使用 IP 位址或使用 VPN 等路徑直接與防火牆通訊的 Windows 網域。

如需 TSA 的安裝說明，請參閱第 90 頁「安裝 SonicWall 終端服務代理」。

主題：

多 TSA 支援

要容納包含數千使用者的大型安裝，防火牆可設定為使用多個終端服務代理執行（每個終端伺服器一個）。支援的代理數取決於型號，如每個型號支援的終端服務代理表格所示。

每個型號支援的終端服務代理

SonicWall 網路安全裝置	支援的 TS 代理	SonicWall 網路安全裝置	支援的 TS 代理	SonicWall 網路安全裝置	支援的 TS 代理
SM 9800	512	NSA 6600	256	TZ600	4
SM 9600	512	NSA 5600	128	TZ500/TZ500 W	4
SM 9400	512	NSA 4600	64	TZ400/TZ400 W	4
SM 9200	512	NSA 3600	16	TZ300/TZ300 W	4
		NSA 2650	8		
		NSA 2600	8	SOHO W	4

對於 SonicWall 網路安全裝置，每個終端伺服器最多可支援 32 個 IP 位址，伺服器有多個 NIC（網路介面控制器）。每個終端伺服器都沒有使用者限制。

TSA 訊息的加密和工作階段 ID 的使用

如果 TSA 和防火牆之間的訊息包含使用者名稱和網域，TSA 使用共用密碼進行加密。始終加密使用者的首個開放通知，因為 TSA 包含使用者名稱和網域。

附註：共用密碼在 TSA 中產生，在 SSO 設定期間在防火牆中輸入的金鑰必須完全符合 TSA 金鑰。

TSA 在所有通知中都包含使用者工作階段 ID，而不是每次都包含使用者名稱和網域。這既高效又安全，且允許 TSA 在代理重新啟動後與終端服務使用者重新同步。

與本機子網路的連接

TSA 根據裝置返回的資訊動態學習網路拓撲結構，在習得後，就不會向裝置傳送未通過裝置的後續使用者連接的通知。因為 TSA 沒有「忘記」這些本機目的地的機制，如果移動裝置上介面之間的子網路，應該重新啟動 TSA。

來自終端伺服器的非網域使用者流量

防火牆有**允許非網域使用者的受限存取**設定，用於選擇性向非網域使用者 (登入其本機機器而非網域的使用者) 提供有限存取權，這與其他 SSO 使用者一樣適用於終端服務使用者。

如果您的網路包含非 Windows 裝置或執行個人防火牆的 Windows 電腦，請選取**探查使用者**，並針對 **NetAPI** 或 **WMI** 選擇選項按鈕，這取決於 SSO 代理的具體設定。這會導致防火牆在請求 SSO 代理識別使用者之前，探查 NetAPI/WMI 連接埠上的回應。如果沒有回應，這些裝置的 SSO 立即失敗。此類裝置不回應或可能封鎖 SSO 代理用於識別使用者的 Windows 網路訊息。

來自終端伺服器的非使用者流量

非使用者連接從終端伺服器打開，用於獲取 Windows 更新和防毒更新。TSA 可以識別來自登入的服務的連接是非使用者連接，並在傳送給裝置的通知中加以識別。

要控制這些非使用者連接的處理，裝置的 TSA 設定上有**允許終端伺服器的非使用者流量繞過存取規則中的使用者驗證**核取方塊。如勾選，就允許這些連接。如果未勾選此核取方塊，將服務視為本機使用者，可以通過勾選**允許受限存取非網域名稱使用者**設定和在具有相應服務名稱的裝置上建立使用者帳戶向其授予存取權限。

附註：來自 TSA 的 Ping (ICMP) 流量識別為非使用者流量，但不是系統服務流量。因此，不允許繞過使用者驗證，並且會在代理逾時之後丟棄。為了防止 ICMP 流量遭受丟棄，請在**原則 | 規則 > 存取規則**頁面中新增存取規則，以允許來自終端伺服器的 ICMP，而不需要使用者驗證。如需關於存取規則的更多資訊，請參閱 *SonicOS 原則*。

瀏覽器 NTLM 驗證的運作方式?

主題：

- 第 85 頁「網域使用者的 NTLM 驗證」
- 第 86 頁「非網域使用者的 NTLM 驗證」
- 第 86 頁「瀏覽器中的 NTLM 驗證憑證」

網域使用者的 NTLM 驗證

對於網域使用者，NTLM 回應通過 RADIUS 中的 MSCHAP 機制進行驗證。必須在裝置上啟用 RADIUS。如需關於 NTLM 驗證的更多資訊，請參閱第 110 頁「設定用於管理使用者的設定」。

非網域使用者的 NTLM 驗證

通過 NTLM，非網域使用者可以是登入到 PC 而未登入到網域的使用者，或是受到提示輸入使用者名稱和密碼但未輸入網域登入憑證的使用者。在這兩種情況下，NTLM 允許將其與網域使用者相區分。

如果使用者名稱符合防火牆上的本機使用者帳戶，則根據帳戶密碼在本機驗證 NTLM 回應。如果驗證成功，使用者可以登入且得到此帳戶的相應授權。使用者群組成員資格是從本機帳戶設定，而不是從 LDAP 設定，而且包含「受信任使用者」群組的成員資格 (因為密碼已在本機驗證)。

如果使用者名稱不符合本機使用者帳戶，則使用者無法登入。**允許非網域使用者的受限存取**選項不適用於透過 NTLM 驗證的使用者。

瀏覽器中的 NTLM 驗證憑證

對於 NTLM 驗證，瀏覽器或者使用網域登入憑證（如使用者登入到網域）從而提供完整的單點登入功能，或者提示使用者輸入所存取網站的使用者名稱和密碼（本例中為防火牆）。不同的因素都會影響瀏覽器在使用者登入到網域時使用網域登入憑證的能力。這些因素取決於所使用的瀏覽器的類型：

Internet Explorer（9.0 或更高版本）	使用使用者的網域憑證，並根據其「網際網路選項」中的「安全」標籤，以透明的方式驗證登入防火牆 (SonicWall 安全設備) 的網站是否位於本機內部網路中。這需要在「網際網路選項」中將防火牆新增到本機內聯網區域的網站清單中。 這可以通過「電腦設定」、「管理範本」、「Windows 元件」、Internet Explorer、「網際網路控制台」、「安全性網頁」下「指派網站到區域清單」中的網域群組原則完成。
Google Chrome	Chrome 與 Internet Explorer 的行為方式相同，包括需要在「網際網路選項」中將防火牆新增到本機內聯網區域的網站清單中。
Firefox	使用使用者的網域登入憑證，並透明地驗證登入到防火牆的網站是否列在其設定的 **network.automatic-ntlm-auth.trusted-uris** 項目中（通過在 Firefox 位址欄輸入 **about:config** 存取）。
Safari	雖然 Safari 支援 NTLM，但目前並不支援使用使用者網域登入憑證的全透明登入。 **附註：**Safari 不能在 Windows 平台執行。
非 PC 平台上的瀏覽器	Linux 和 Mac 等非 PC 平台可以通過 Samba 在 Windows 網域中存取資源，但沒有像 Windows PC 一樣「將 PC 登入到網域」的概念。因此，這些平台上的瀏覽器不能存取使用者的域登入憑證，且無法將其用於 NTLM。

在使用者未登入到網域或瀏覽器不能使用其網域登入憑證時，將提示輸入使用者名稱和密碼，或者如果使用者之前可能已儲存，將使用快取的登入憑證。

在上述各種情況中，如果使用使用者的網域登入憑證進行身分驗證失敗（這可能由於用於沒有所需的存取權限），瀏覽器將提示使用者輸入使用者名稱和密碼。這允許使用者輸入不同於網域登入憑證的其他憑證獲得存取權限。

附註：啟用 NTLM 以進行單點登入強制時，利用**受信任使用者**作為**允許的使用者**的 HTTP/HTTPS 存取規則必須新增至**管理 | 原則 > 規則 > 存取規則**頁面的 **LAN 到 WAN** 規則 (如需詳細資訊，請參閱 *SonicOS 原則*)。此規則會向使用者觸發 NTLM 驗證要求。如果未新增此存取規則，嚴格的內容篩選條件原則等其他設定將阻塞使用者的 Internet 存取並禁止驗證請求。

RADIUS 單點登入計費的工作方式

RFC 2866 指定使用 RADIUS 計費作為向計費伺服器傳送使用者登入工作階段計費訊息的網路存取伺服器 (NAS) 機制。這些訊息在使用者登入和登出時傳送。另外，也可以選擇在使用者工作階段期間定期傳送。

當客戶使用外部或供應商網路存取裝置執行使用者驗證（通常用於遠端或無線存取）且裝置支援 RADIUS 計費時，SonicWall 裝置可以用作 RADIUS 計費伺服器，可以使用客戶的網路存取伺服器傳送的 RADIUS 計費訊息進行網路中的單點登入 (SSO)。

附註：可將執行 SMA 11.4 或更高版本的 SonicWall SMA 1000 系列裝置設定為外部 RADIUS 計費用戶端，其中 SonicWall 防火牆充當 RADIUS 計費伺服器。

在遠端使用者通過 SonicWall SMA 或供應商裝置連接時，SMA 或供應商裝置向 SonicWall 裝置（設定為 RADIUS 計費伺服器）傳送計費訊息。SonicWall 裝置根據計費訊息中的資訊將使用者新增到其內部登入使用者資料庫中。

使用者登出時，SonicWall SMA 或第三方設備會向 SonicWall 安全設備傳送另一則計費訊息，然後登出使用者。

附註：網路存取伺服器 (NAS) 在傳送 RADIUS 計費訊息時，不要求使用者經過 RADIUS 驗證。即使在供應商裝置使用 LDAP、內部資料庫或任何其他機制驗證使用者時，NAS 也可以傳送 RADIUS 計費訊息。

RADIUS 計費訊息未加密。RADIUS 計費有防欺騙的內在安全性，因為使用請求驗證器和共用密碼。RADIUS 計費需要在裝置上設定可以傳送 RADIUS 計費訊息的網路存取伺服器 (NAS) 清單。這項設定提供各 NAS 的 IP 位址和共用密碼。

主題：

RADIUS 計費訊息

RADIUS 計費使用兩種計費訊息：

- **計費請求**
- **計費回應**

計費請求可以傳送**狀態類型**屬性指定的三種請求類型中的一種：

此要求	傳送
開始	當使用者登入時傳送。
停止	當使用者登出時傳送。
臨時更新	在使用者登入工作階段期間定期傳送。

遵循 RADIUS 標準的計費訊息由 RFC 2866 指定。每個訊息包含屬性清單和由共用密碼驗證的驗證器。

這些 SSO 相關屬性會在**計費要求**中設定:

狀態類型	計費要求的類型 (**開始**、**停止**，或**暫時更新**)。
使用者名稱	使用者的登入名稱。格式並非由 RFC 指定，可以是簡單的登入名稱或包含登入名稱、網域或識別名稱 (DN) 等各種值的字串。

Framed-IP-Address	使用者的 IP 位址。如果使用了 NAT，這必須是使用者的內部 IP 位址。
呼叫工作站識別碼	SMA 等部分設備使用的使用者 IP 位址的字串表示。
Proxy 狀態	用於將請求轉送至另一 RADIUS 計費伺服器的通過狀態。

SonicWall 與供應商網路裝置的相容性

為了使 SonicWall 安全設備與供應商網路設備相容，以透過 RADIUS 計費進行 SSO 登入，供應商設備必須能夠:

- 支援 RADIUS 計費。
- 傳送**開始**和**停止**訊息。傳送未作要求的**暫時更新**訊息。
- 在**開始**和**停止**訊息的**框架 IP 位址**或**主叫站 ID** 屬性中傳送使用者的 IP 位址。

附註：如果遠端存取伺服器使用 NAT 轉譯使用者的外部公開 IP 位址，則屬性必須提供用於內部網路的內部 IP 位址，且必須是此使用者的唯一 IP 位址。如果使用兩個屬性，則**框架 IP 位址**屬性必須使用內部 IP 位址，**主叫站 ID** 屬性應該使用外部 IP 位址。

應該在**開始**訊息和**暫時更新**訊息的**使用者名稱**屬性中傳送使用者的登入名稱。可以在**停止**訊息的**使用者名稱**屬性中傳送使用者的登入名稱，但不是必須的。**使用者名稱**屬性必須包含使用者的帳戶名稱，而且還可以包含網域，或者必須包含使用者的識別名稱 (DN)。

代理轉送

充當 RADIUS 計費伺服器的 SonicWall 安全設備可以最多向每個網路存取伺服器 (NAS) 的四個其他 RADIUS 計費伺服器使用代理轉送形式傳送請求。可以為各 NAS 分別設定各 RADIUS 計費伺服器。

為了避免需要為各 NAS 重新輸入設定的詳細資料，SonicOS 允許從設定的伺服器的清單中為各 NAS 選擇轉送。

各 NAS 用戶端的代理轉送設定包括逾時和重試次數。可以藉由選取以下選項，設定如何向兩個或多個伺服器轉送要求:

- **逾時時嘗試下一個伺服器**
- **轉送每個請求至所有伺服器**

非網域使用者

在以下情況中，向 RADIUS 計費伺服器報告的使用者確定為本機 (非網域) 使用者:

- 未使用網域傳送使用者名稱，且未設定為可通過 LDAP 查詢伺服器的網域。
- 未使用網域傳送使用者名稱，且設定為可通過 LDAP 查詢伺服器的網域，但未找到使用者名稱。
- 已使用網域傳送使用者名稱，但在 LDAP 資料庫中未找到網域。
- 已使用網域傳送使用者名稱，但在 LDAP 資料庫中未找到使用者名稱。

經過 RADIUS 計費驗證的非網域使用者受到與使用其他 SSO 機制驗證的使用者相同的約束，且適用以下限制：

- 只有在已設定**允許非網域使用者的受限存取**時，使用者才可以登入。
- 使用者不會成為「受信任使用者」群組的成員。

IPv6 注意事項

在 RADIUS 計費中，使用這些包含使用者的 IPv6 位址：

- Framed-Interface-Id / Framed-IPv6-Prefix
- Framed-IPv6-Address

目前，忽略所有這些 IPv6 屬性。

有些裝置在**主叫站 ID** 屬性中以文字形式傳遞 IPv6 位址。

如果其中不包含有效的 IPv4 位址，則忽略**主叫站 ID**。

包含 IPv6 位址屬性，但將不包含 IPv4 位址屬性的 RADIUS 計費訊息轉送至代理伺服器。如果未設定代理伺服器，則丟棄 IPv6 屬性。

RADIUS 計費伺服器連接埠

RADIUS 計費通常使用 UDP 連接埠:

1813	IANA 專用連接埠。SonicWall 安全設備預設會在連接埠 1813 上監聽。
1646	舊的非官方標準連接埠。

可以為 RADIUS 計費連接埠設定其他連接埠號碼，但 SonicWall 安全設備只能在一個連接埠上監聽。所以，如果您使用多個網路存取伺服器 (NAS)，必須將其設定為都能在相同的連接埠數目上通訊。

安裝單點登入代理和/或終端服務代理

設定 SSO 是包含安裝和設定 SonicWall SSO 代理和/或 SonicWall 終端服務代理 (TSA) 以及設定執行 SonicOS 的防火牆以使用 SSO 代理或 TSA 的過程。如需 SonicWall SSO 的說明，請參見第 79 頁「關於單一登入」。

主題：

安裝 SonicWall SSO 代理

SonicWall SSO 代理是 SonicWall Directory Connector 的一部分。SonicWall SSO 代理必須至少安裝在能使用 VPN 或 IP 存取 Active Directory 伺服器的 Windows 網域上的一個（最多八個）工作站或伺服器上。建議這些工作站或伺服器為個別獨立的工作站或伺服器。SonicWall SSO 代理必須能夠存取您的防火牆。

如需安裝 SonicWall SSO 代理，請參閱 *SonicWall Directory Services Connector 管理指南*中的步驟。您可以從 mysonicwall.com 下載此指南。

安裝 SonicWall 終端服務代理

在 Windows 網域的網路上的一個或多個終端伺服器上安裝 SonicWall TSA。SonicWall TSA 必須能夠存取您的 SonicWall 安全設備，而安全設備必須能夠存取 TSA。如果您有在終端伺服器上執行的軟體防火牆，可能需要開放 UDP 連接埠數目用於接收來自安全設備的訊息。

SonicWall TSA 可以從 MySonicWall 免費下載。

若要安裝 SonicWall TSA：

1 在 Windows 終端伺服器系統上，根據您的電腦下載下列其中一個安裝程式:

- SonicWall `TSAInstaller32.msi`（32 位元，3.0.28.1001 或更高版本）
- SonicWall `TSAInstaller64.msi`（64 位元，3.0.28.1001 或更高版本）

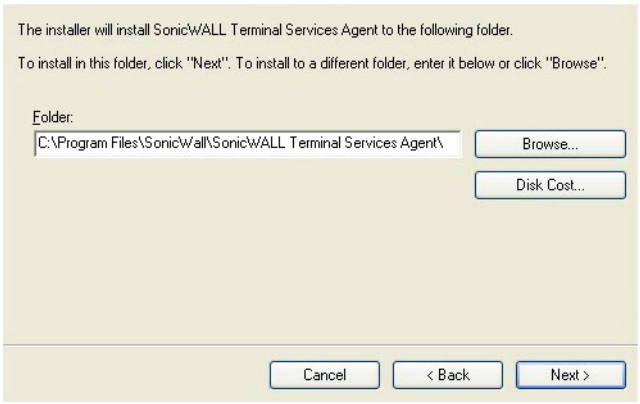
您可以在 http://www.mysonicwall.com 找到這些。

2 按兩下安裝程式開始安裝。

3 在「歡迎」頁面，按**下一步**繼續。「授權協定」顯示。

4 選取**我同意**。

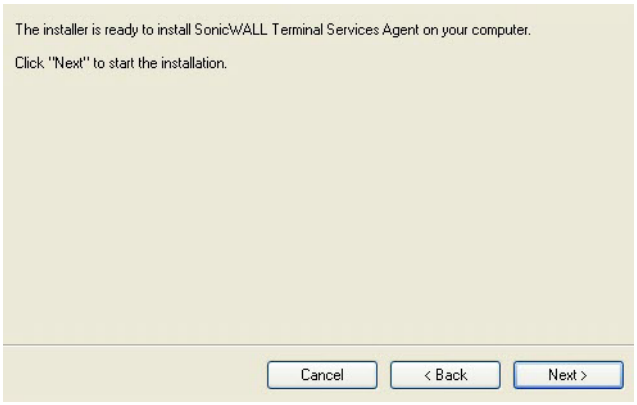
5 按**下一步**以繼續。隨即顯示「選取安裝資料夾」視窗。



6 選取目的地資料夾。結束時間:

- 使用預設資料夾 `C:\Program Files\SonicWall\SonicWall Terminal Services Agent\`，然後按**下一步**。
- 指定自訂位置:
    a) 按一下**瀏覽**。
    b) 選取資料夾。
    c) 按**下一步**。

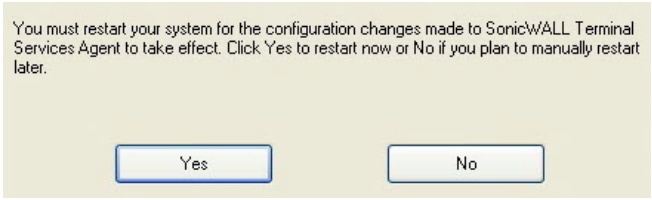
隨即顯示「自訂安裝」視窗。



7 按一下**下一步**以開始安裝。

8 等待 SonicWall 終端服務代理安裝。進度欄指示安裝狀態。

9 安裝完成時，按一下**關閉**結束安裝程式。隨即顯示一則訊息，確認系統重新啟動。



10 在啟動 SonicWall 終端服務代理之前，您必須重新啟動系統。若要重新啟動:

- 若要立即重新啟動，請按一下**是**。
- 若要稍後重新啟動，請按一下**否**。您必須先重新啟動系統，然後才可使用 TSA。

設定 SonicWall SSO 代理

SonicWall SSO 代理使用 NetAPI 或 WMI 與工作站通訊，這兩種方式都提供有關登入到工作站的使用者的資訊，包括網域使用者、本機使用者和 Windows 服務。WMI 預安裝在 Windows 伺服器 2003、Windows XP、Windows ME 和 Windows 2000 上。 對於其他 Windows 版本，請存取 `www.microsoft.com` 下載 WMI。在設定 SonicWall SSO 代理前，請先確認是否已安裝 WMI 或 NetAPI。

在設定 SonicWall SSO 代理前，必須安裝 .NET Framework 4.0 或更高版本。NET Framework 可以從 `www.microsoft.com` 下載。

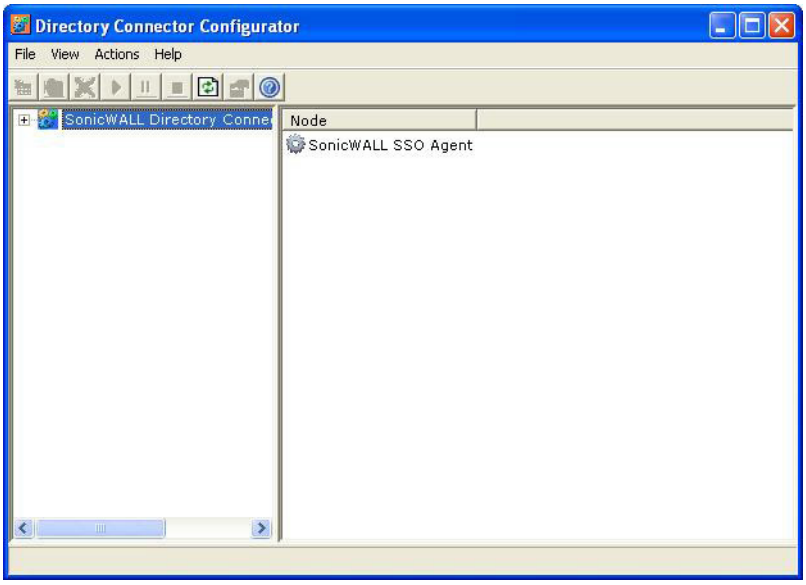
主題：

- 第 92 頁「設定 SonicWall SSO 代理的通訊屬性」
- 第 95 頁「新增 SonicWall 網路安全裝置」
- 第 96 頁「在 SonicWall SSO 代理中編輯裝置」
- 第 96 頁「在 SonicWall SSO 代理中刪除裝置」
- 第 97 頁「在 SonicWall SSO 代理中修改服務」

設定 SonicWall SSO 代理的通訊屬性

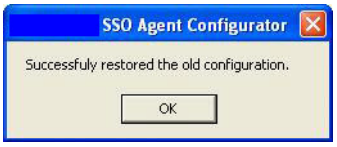
若要設定 SonicWall SSO 代理的通訊屬性：

1 通過按兩下桌面快捷方式或移至**開始 > 所有程式 > SonicWall > SonicWall Directory Connector > SonicWall 設定工具**啟動 SonicWall 設定工具。



附註：如果未設定預設防火牆的 IP 位址，或者設定錯誤，會顯示快顯視窗。按一下**是**使用預設的 IP 位址 (192.168.168.168)，或按一下**否**使用目前設定。

如果您按一下**是**，將顯示**已成功恢復舊設定**訊息。按一下**確定**。



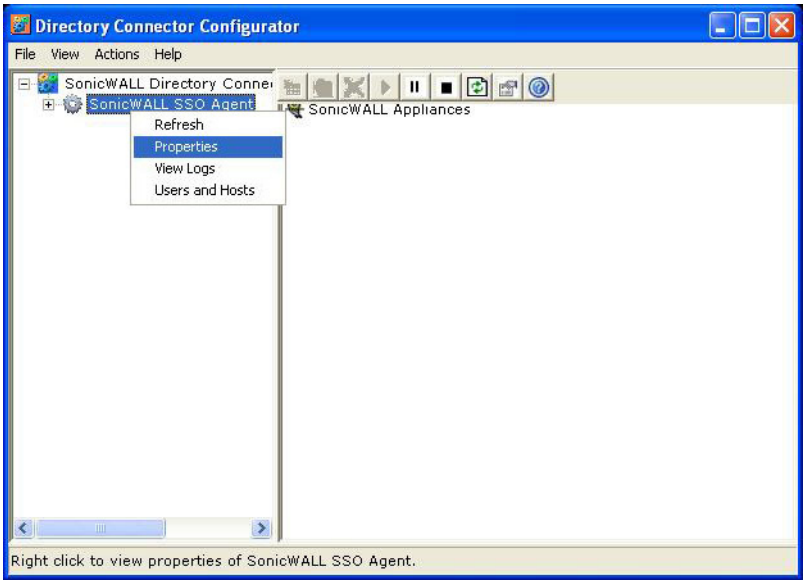
如果您按一下**否**，或者按一下**是**但預設值不正確，將顯示 **SonicWall SSO 代理服務未執行。 請檢查設定並啟動服務。**隨即顯示。按一下**確定**。

如果顯示 **SonicWall SSO 代理服務未執行。 請檢查設定並啟動服務**顯示，SSO 代理服務預設是停用。若要啟用服務。

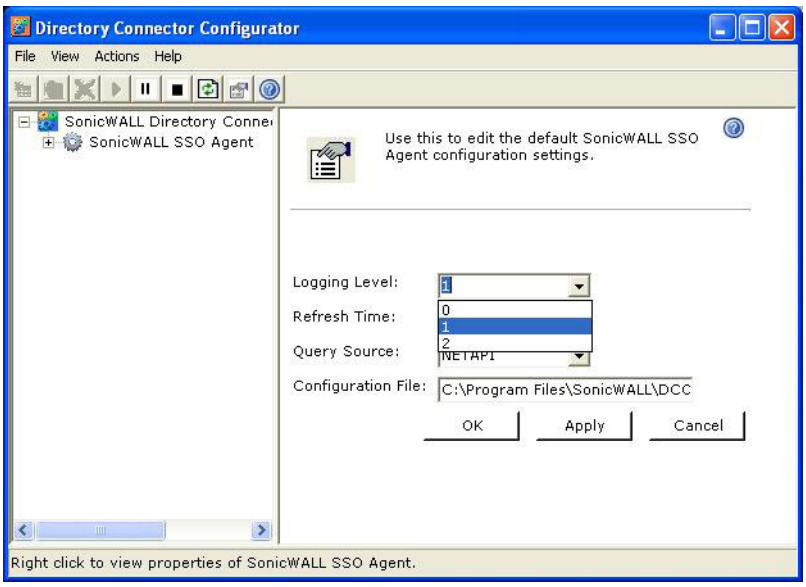
1) 按一下 **+** 圖示，以在左側導覽面板中展開 SonicWall Directory Connector 設定工具。
2) 高亮顯示下方的 SonicWall SSO 代理。

3) 按一下**開始**圖示。

2 在左側瀏覽面板中，通過按一下 **+** 圖示展開 SonicWall Directory Connector 設定工具。右鍵按一下 **SonicWall SSO 代理**，然後選擇**屬性**。



3 從**記錄層級**下拉功能表，選擇要在 Windows 事件記錄中記錄的事件級別。



選取下列其中一個層級:

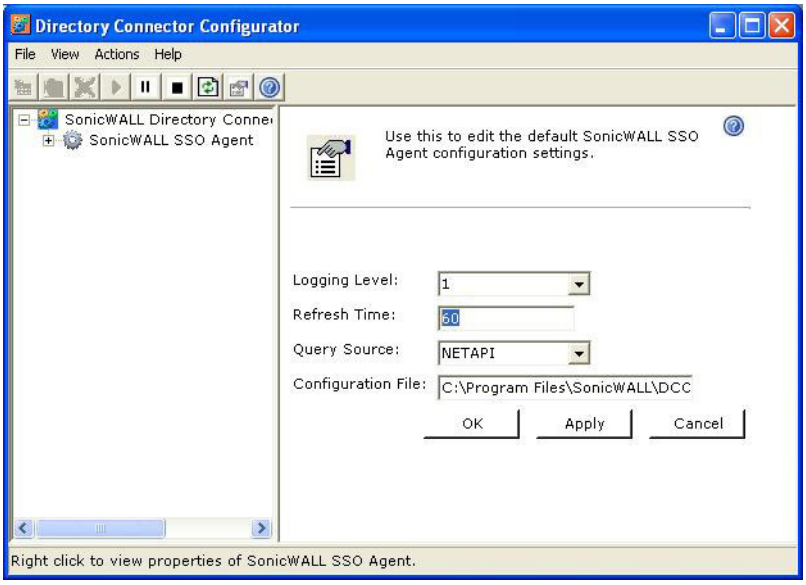
記錄層級 0 僅記錄關鍵事件。

記錄層級 1 記錄關鍵和很嚴重的事件。這是預設的記錄層級。

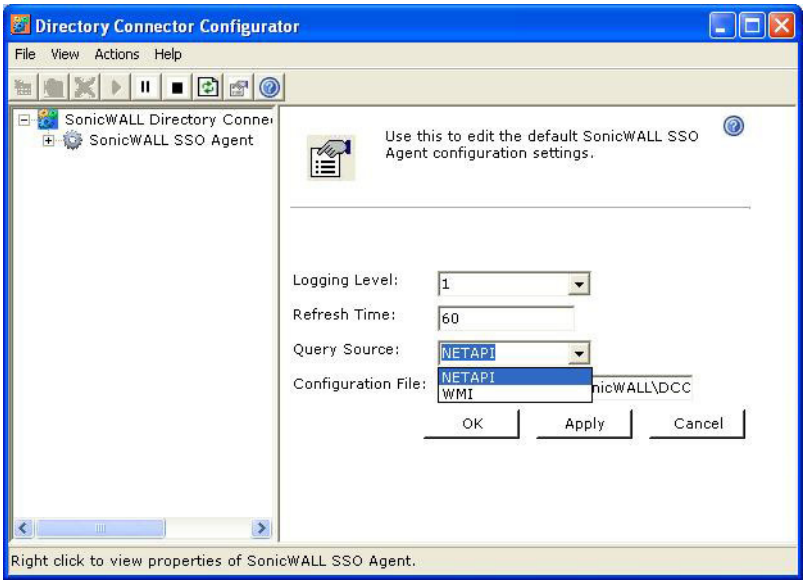
記錄層級 2 使用嚴重性的偵錯等級記錄來自設備的所有要求。

附註：如果 Windows 事件記錄達到其最大容量時，SSO 代理服務會終止。

4 在**重新整理時間**欄位，輸入 SSO 代理重新整理使用者記錄狀態的頻率（秒）。預設值為 **60** 秒。



5 從**查詢來源**下拉功能表中選擇 SSO 代理用於與工作站通訊的協定：**NETAPI** 或 **WMI**。

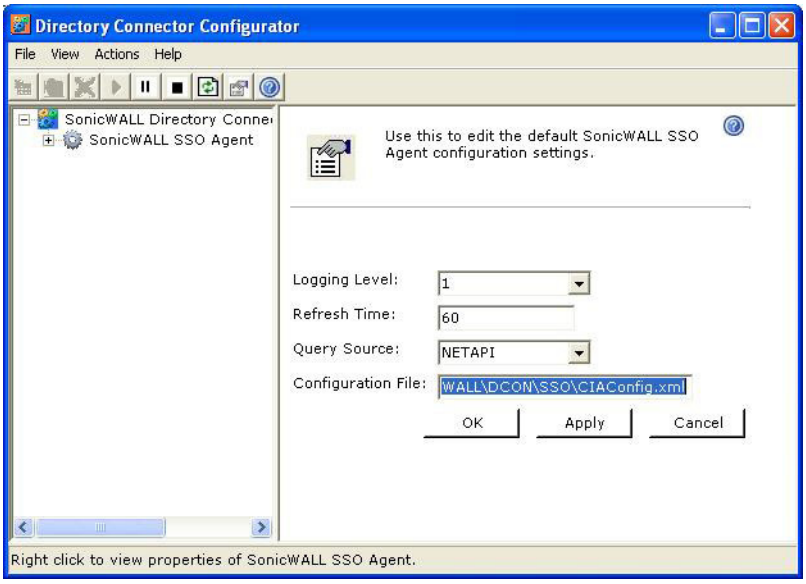


ⓘ **附註：**NetAPI 提供更快的效能，但準確率稍低。在使用 NetAPI 的情況下，不論使用者是否仍已登入，Windows 都會向工作站報告最後一次登入。這表示，當使用者從電腦登出後，設備仍顯示使用者為登入狀態。如果另一名使用者登入了同一台電腦，此時，前一使用者即從 SonicWall 登出。

WMI 提供更慢的效能，但準確率更高。

WMI 預安裝在 Windows 伺服器 2003、Windows XP、Windows ME 和 Windows 2000 上。 NetAPI 和 WMI 都可以手動下載和安裝。NetAPI 和 WMI 提供有關登入到工作站的使用者的資訊，包括網域使用者、本機使用者和 Windows 服務。

6 在**設定檔**欄位中，輸入設定檔的路徑。預設路徑是 `C:\Program Files\SonicWall\DCON\SSO\CIAConfig.xml`。



7 按一下**接受**。

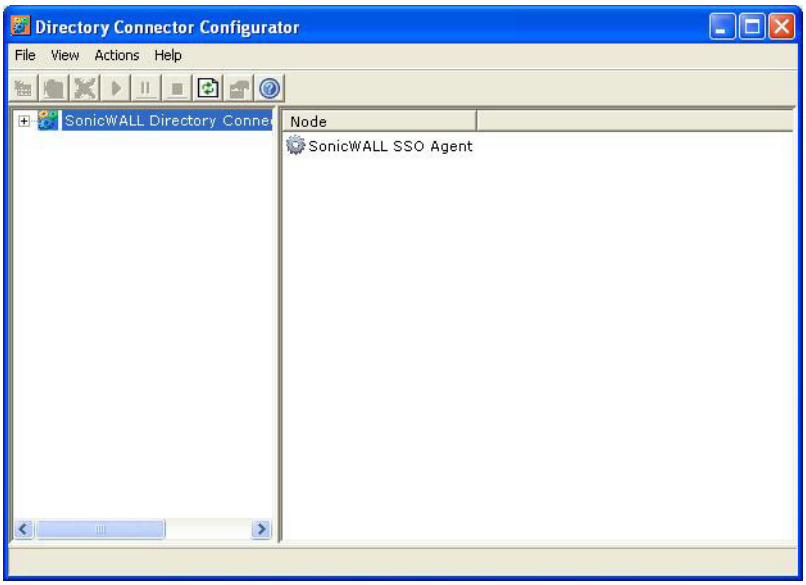
8 按一下**確定**。

新增 SonicWall 網路安全裝置

如果在安裝期間未新增安全設備，則使用這些說明手動新增或新增附加防火牆。

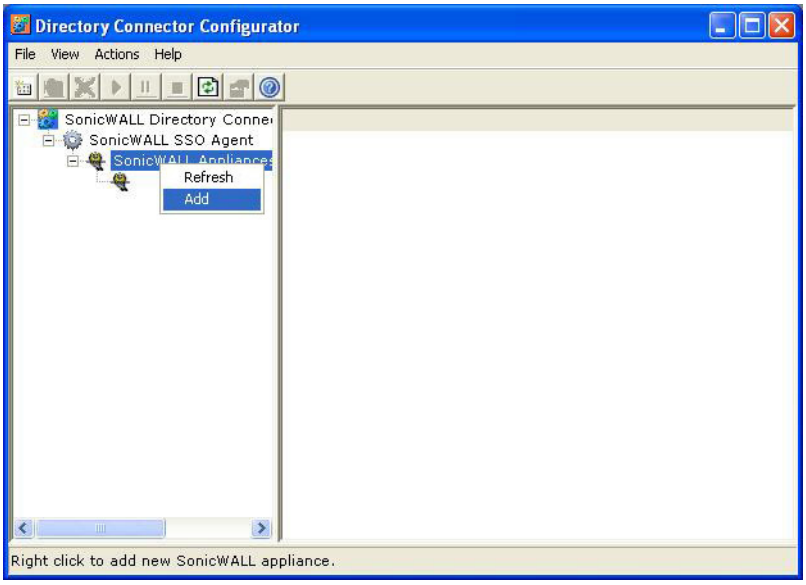
若要新增 SonicWall 安全設備:

1 啟動 SonicWall SSO 代理設定。



2 按一下 **+** 圖示，以展開左側列中的 SonicWall Directory Connector 和 SonicWall SSO 代理樹狀目錄。

3 以滑鼠右鍵按一下 **SonicWall 設備**。



4 選擇**新增**。

5 在**設備 IP** 欄位中，輸入您的 SonicWall 安全設備設備 IP 位址。

6 在**裝置連接埠**欄位輸入同一裝置的連接埠。預設連接埠號是 **2258**。

7 在**易記名稱**欄位中，為您的安全設備起一個易記的名稱。

8 您可以

- 在**共用金鑰**欄位中，輸入共用金鑰。
- 按一下**產生金鑰**以產生共用金鑰。

9 完成時，按一下**確定**。

您的安全設備會顯示在 SonicWall 設備樹狀目錄下的左側導覽面板。

在 SonicWall SSO 代理中編輯裝置

您可以編輯之前新增到 SonicWall SSO 代理中的安全設備的所有設定，包括 IP 位址、連接埠數目、易記的名稱和共用密碼。

若要在 SonicWall SSO 代理中編輯安全設備:

1 從左側導覽面板選取安全設備。

2 按一下左側導覽面板上方的**編輯**圖示。您還可以按一下右側視窗底部的**編輯**標籤。

在 SonicWall SSO 代理中刪除裝置

若要刪除您先前在 SonicWall SSO 代理中新增的安全設備:

1 從左側導覽面板選取安全設備。

2 按一下左側導覽面板上方的**刪除**圖示。

在 SonicWall SSO 代理中修改服務

您可以啟動、停止和暫停安全設備的 SonicWall SSO 代理服務。

結束時間:

- 暫停安全設備的服務，請從左側導覽面板選取安全設備，然後按一下**暫停**圖示。
- 停止安全設備的服務，請從左側導覽面板選取設備，然後按一下**停止**圖示。
- 恢復服務，請按一下**啟動**圖示。

> **附註：**在 SonicWall SSO 代理中對安全設備作出設定變更後，您可能收到重新啟動服務的提示。若要重新啟動服務，請按停止按鈕，然後按啟動按鈕。

設定 SonicWall 終端服務代理

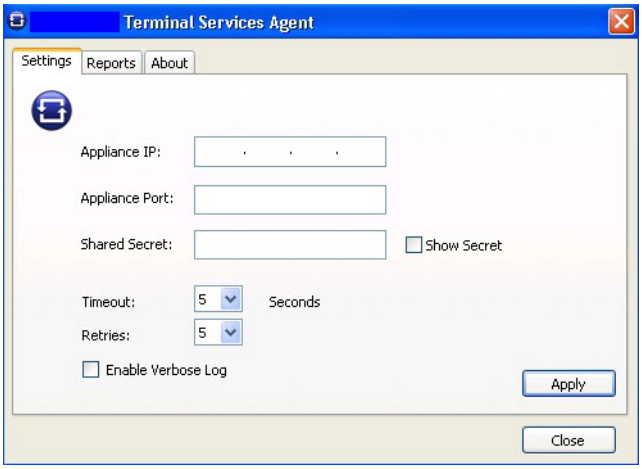
在安裝 SonicWall TSA 並重新啟動 Windows 伺服器系統後，您可以按兩下安裝程式建立的 SonicWall TSA 桌面圖示啟動此程式進行設定以產生故障排除報告 (TSR) 或查看狀態和版本資訊。

主題：

將 SonicWall 安全設備新增到 SonicWall TSA 設定

若要將 SonicWall 安全設備新增到 SonicWall TSA:

1 按兩下 SonicWall TSA 桌面圖示。SonicWall 終端服務代理視窗顯示。



2 在**設定**標籤，在**裝置 IP** 欄位中輸入防火牆的 IP 位址。

3 在**裝置連接埠**欄位中輸入通訊連接埠。預設連接埠為 **2259**，但可以使用自訂連接埠代替。此連接埠必須在 Windows 伺服器系統上開放。

4 在**共用密碼**欄位輸入加密金鑰。選取**顯示密碼**，以查看字元並驗證正確性。必須在防火牆上設定相同的共用密碼。

5 在**逾時**下拉功能表中，選取代理在重試通知前等待設備回覆的秒數。範圍為 5 至 10 秒，預設為 **5** 秒。

6 在**重試次數**下拉功能表中，選取代理在沒有收到回覆時重新嘗試向設備傳送通知的次數。範圍為 3 至 10 次重試，預設為 **5** 次。

7 若要在記錄訊息中啟用完整的詳細資料，請選取**啟用詳細記錄**。

> **提示：**僅在需要在故障排除報告中提供附加的詳細資料時才勾選此核取方塊。請避免在其他情況下啟用此核取方塊，因為這可能影響效能。

8 按一下**套用**。快顯訊息表示 SonicWall TSA 服務已透過新設定重新啟動。

9 按一下**確定**。

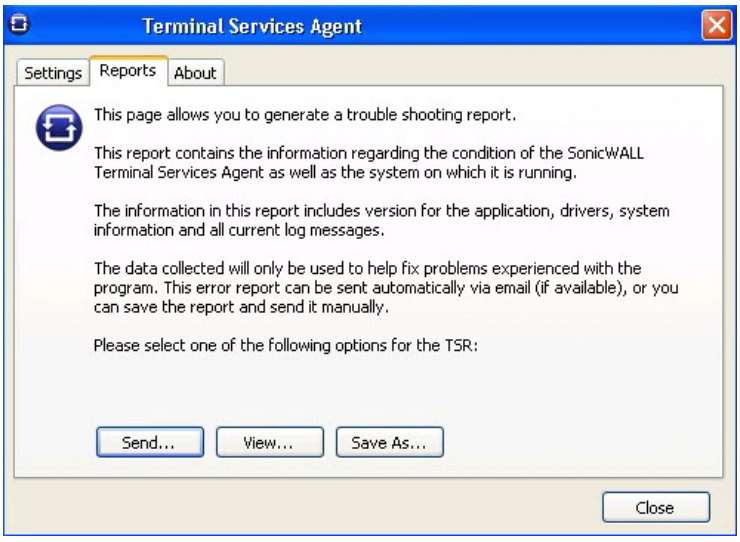
建立 SonicWall TSA 故障排除報告

您可以建立包含有關代理、驅動程式和系統設定的所有目前記錄訊息和資訊的故障排除報告，以檢查或傳送給 SonicWall 技術支援部門請求協助。

若要建立 SonicWall TSA 的 TSR：

1 按兩下 **SonicWall TSA** 桌面圖示。**SonicWall 終端服務代理**視窗顯示。

2 按一下**報告**標籤。



3 若要產生 TSR 並：

- 自動向 SonicWall 技術支援傳送電子郵件，請按一下**傳送**。

- 在預設文字編輯器中進行檢查，請按一下**查看**。
- 若要將其儲存至文字檔案，請按一下**另存為**。

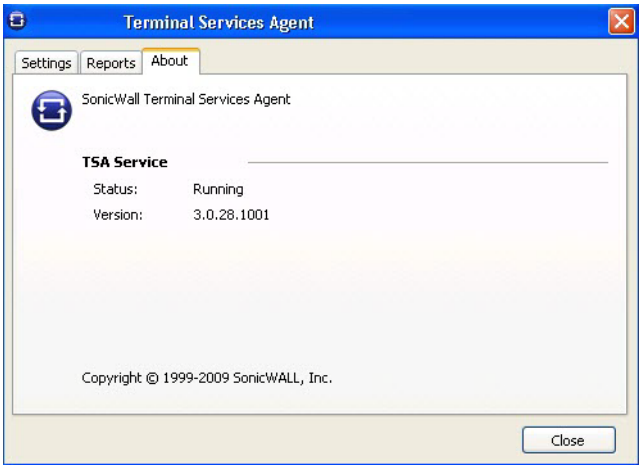
4 完成時，按一下**關閉**。

查看 SonicWall TSA 狀態和版本

若要顯示 Windows 伺服器系統上的 SonicWall TSA 服務的目前狀態，或查看 SonicWall TSA 的版本號碼：

1 按兩下 **SonicWall TSA** 桌面圖示。**SonicWall 終端服務代理**視窗顯示。

2 按一下**關於**標籤。



3 按一下**關閉**。

單點登入進階功能

主題：

- 第 99 頁「關於單一登入」
- 第 100 頁「關於進階設定」
- 第 100 頁「檢視 SSO 滑鼠懸停統計資料」
- 第 101 頁「使用 TSR 中的單點登入統計」
- 第 102 頁「檢查代理」
- 第 102 頁「補救措施」

關於單一登入

當使用者首次嘗試透過使用單一登入 (SSO) 的 SonicWall 安全設備傳送流量時，安全設備會將「使用者識別」要求傳送給 SonicWall SSO 代理。代理通過 Windows 網路查詢使用者的 PC，並向防火牆返回使用者名稱。如果使用者名稱符合原則中設定的條件，則 SonicWall 將使用者視為「已登入」。在使用者使用 SSO 登入 SonicWall 時，SSO 功能還會偵測登出情況。為了偵測登出情況，安全設備反復輪詢代理以檢查各使用者是否仍在登入狀態。這種輪詢及初始的識別請求可能導致對 SonicWall SSO 代理應用程式和執行的 PC 上產生較大負載，尤其是大量使用者連接時。

SonicWall SSO 功能利用頻率限制機制防止裝置的這些使用者請求攻擊代理。裝置上的自動計算和可設定的設定都會控制這種頻率限制的工作方式。SonicWall SSO 功能根據最近的輪詢回應時間，自動計算代理在輪詢期間可以處理的各訊息中的最大使用者請求數。此外，將多使用者請求的逾時自動設為較長時間，以降低輪詢期間的偶發長逾時的可能性。可設定的設定用於控制一次傳送給代理的請求數，可以調節以最佳化 SSO 效能和防止可能出現的問題。本章節提供有關選擇適合的設定的指導。

可以通過在專用的高效能 PC 上執行代理，或通過在單獨的 PC 上使用多個代理分擔負載來降低代理過載產生問題的可能性。在第二種方法中，如果其中一個代理 PC 執行失敗，可能產生冗餘。代理應該在 Windows 伺服器 PC 上執行（可以使用有些舊版本工作站，但在較新的 Windows 2000/XP/Vista 工作站版本和舊版本的 Service Pack 上作出的變更增加了 TCP 連接速率限制功能，會干擾 SSO 代理的執行）。

關於進階設定

設定 SSO 代理時，可使用**一次傳送的最大請求數目**設定 (如需關於 SSO 代理的詳細資訊，請參閱第 142 頁「設定 SonicOS 以使用 SonicWall SSO 代理」)。

這項設定控制可以同時從裝置向代理傳送的最大請求數。代理同時處理多個請求，並在 PC 中產生各單獨的執行緒進而分別處理。一次傳送過多的請求可能使執行代理的 PC 過載。如果傳送的請求數超出最大值，則將有些請求會置於內部「環形緩衝區」（參見第 101 頁「使用 TSR 中的單點登入統計」和第 100 頁「檢視 SSO 滑鼠懸停統計資料」）。請求在環形緩衝區等待過久會導致 SSO 身分驗證中的回應變慢。

在輪詢以檢查登入使用者的狀態時，這項設定與自動計算的傳送給代理每個訊息中的使用者請求數配合使用。每個訊息的使用者請求數根據最近的輪詢回應時間計算得出。SonicOS 儘量調高將此數目，以最大限度減少需要傳送的訊息數，從而降低代理上的負載和幫助減少裝置與代理之間的網路流量。但是，還會儘量保持此數目足夠小以允許代理在輪詢期間內處理訊息中的所有使用者請求。這樣可以避免逾時和故障等潛在問題以快速偵測登出的使用者。

檢視 SSO 滑鼠懸停統計資料

SSO 驗證設定對話方塊提供關於每個代理和所有 SSO 代理的滑鼠懸停統計資料。在 **SSO 代理**頁面上，代理旁邊的綠色 LED 式圖示表示代理已啟動且正在執行中。紅色 LED 圖示表示代理已關閉。

若要檢視下列項目的統計資料:

- 特定代理，請將您的滑鼠游標移至 SSO 代理的**統計資料**圖示上方。
- 所有 SSO 代理，請將您的滑鼠由標移至表格下方的**統計資料**圖示上方。

  提示：這也適用於**終端服務**標籤上的各 TSA。

若要關閉統計顯示，按一下**關閉**。

若要清除所有顯示值，按一下**按一下以重設**。

使用 TSR 中的單點登入統計

技術支援報告 (TSR) 中包含豐富的 SSO 效能和錯誤統計資料。這可用於衡量 SSO 在您安裝的程式中的效能。在**調查 > 工具 > 系統診斷**頁面下載技術支援報告，並搜尋標題「SSO 操作統計」。以下是需要特別留意的計數器:

1. 在 **SSO 環形緩衝區統計**下，查看**環形緩衝區溢出**和**在環形緩衝區花費的最長時間**。如果第二個值接近或超過輪詢比率，或者顯示任何環形緩衝區溢出，則表示沒有足夠快速地向代理傳送請求。此外，如果**在環形緩衝區等待的目前請求數**不斷增加，也表示發生了相同的情況。這表示應該增加**一次傳送的最大請求數目**以更快地傳送請求。但是，這樣會增加代理的負載，而且如果代理無法處理附加負載，也會導致問題，這時可能需要考慮將代理移至更強大的 PC 或增加附加代理。
2. 在 **SSO 操作統計**下，查看**逾時失敗的使用者 ID 嘗試**和**因其他錯誤失敗的使用者 ID 嘗試**。這些值應該是零或接近零，此處顯示的重大故障表示代理發生問題，可能由於無法處理嘗試的使用者驗證數。
3. 此外，在 **SSO 操作統計**下，查看**在定期輪詢中輪詢的總使用者數**、**逾時失敗的使用者輪詢**和**因其他錯誤失敗的使用者輪詢**。在這裡看到一些逾時和錯誤是可接受的，甚至是符合預期的，偶爾的輪詢故障不會導致問題。但是錯誤率應該較低（約 0.1% 或更低的錯誤率應該是可接受的）。如上所述，此處顯示的高故障率表示代理存在問題。
4. 在 **SSO 代理統計**下，查看**平均使用者 ID 請求時間**和**每個使用者的平均輪詢回應時間**。這些值應在幾秒內或更低，較大的值表示網路可能存在問題。注意，儘管如此，嘗試通過 SSO 驗證來自非 Windows PC 的流量（可能花費顯著更長的時間）導致的錯誤可能使**平均使用者 ID 請求時間**值失真，所以如果此值較高，但**每個使用者的平均輪詢回應時間**看似正確，即表示代理可能發生很多錯誤，可能由於嘗試驗證非 Windows 裝置所致，請參見步驟 6。
5. 如果使用多個代理，也須在 **SSO 代理統計**下查看對不同代理報告的錯誤和逾時率及其回應時間。各代理之間的顯著差異可能表示一個代理的特定問題，可以通過升級或變更此代理的設定來解決。

6 來自裝置而不是來自 PC 的流量可以觸發 SSO 識別嘗試，且可能導致出錯和/或逾時因而報告在這些統計資訊中。這可以通過使用此類裝置的 IP 位址設定位址物件組和執行以下一項或兩項操作來避免：

- 如果使用內容篩選，在 SSO 設定的**實施**標籤上對**繞過單點登入的流量來自**設定選擇位址物件。
- 如果設定了存取規則僅允許經驗證的使用者，則為此位址物件設定單獨的規則，將**允許的使用者**設為**全部**。

為了識別相應的 IP 位址，查看 TSR 和搜尋「SSO 嘗試使用的 IP 位址」。這會列出**發生錯誤後的等待時間**設定中前一期間的 SSO 錯誤。

附註：如果列出的任何 IP 位址適用於 Mac/Linux PC，請參見第 103 頁「Mac 和 Linux 使用者調適」。

為了限制因此產生的錯誤率，您還可以延長「使用者」標籤中的**發生錯誤後的等待時間**設定。

檢查代理

如果 TSR 報告中的統計資料表示代理可能存在問題，則下一步最好是在執行代理所在的電腦上，執行 Windows 工作管理員，並在**效能**標籤上查看 CPU 使用率，以及「處理程序」標籤上 `CIAService.exe` 處理程序的 CPU 使用率。如果後者使用較大的 CPU 時間百分比，且 CPU 利用率峰值接近，表示代理過載。為了嘗試降低負載，您可以減少**一次傳送的最大請求數目**設定，請參閱上文的使用 TSR 中的單點登入統計第步驟 1。

補救措施

如果無法負載平衡設定，以實現既避免代理 PC 過載，又仍能足夠快速向代理傳送請求，則應該採取以下一項操作：

- 考慮藉由增加輪詢時間，降低在 **SSO 驗證**對話方塊之**使用者**區段中設定的輪詢比率。這會減少代理的負載，但可能導致偵測登出的速度變慢。

  附註：在共用 PC 的環境中，可能最好保持輪詢間隔儘量最短以避免在不同使用者使用相同 PC 時未能偵測到登出所產生的問題，例如來自 PC 的第二名使用者的初始流量可能記錄為由前一位使用者傳送。

- 將代理移至更高效能的專用 PC。
- 設定附加的一個或多個代理。

設定存取規則

在 SonicOS 管理介面的**規則 > 存取規則**頁面上啟用 SonicWall SSO 會影響原則。在**規則 > 存取規則**下設定的規則，會對照從 SSO LDAP 查詢傳回的使用者群組成員資格進行檢查，並自動套用規則。

主題：

- 第 103 頁「自動產生的 SonicWall SSO 規則」
- 第 103 頁「Mac 和 Linux 使用者調適」
- 第 104 頁「允許從終端伺服器的 ICMP Ping」
- 第 104 頁「關於存取規則」

自動產生的 SonicWall SSO 規則

如果在 SonicOS 管理介面中已設定 SonicWall SSO 代理或 TSA，將建立存取規則和相應的 NAT 原則以允許代理回覆 LAN。這些規則使用 **SonicWall SSO 代理**或 **SonicWall 終端服務代理**位址群組物件，各設定的代理都有一個成員位址物件。自動將成員位址物件新增到群組物件和從群組物件刪除，如同新增或刪除代理一樣。隨著代理的 IP 位址變更，自動更新成員位址物件，包含在通過 DNS 解析 IP 位址（DNS 名稱在此指定代理）時。

如果在不同的區域設定 SonicWall SSO 代理或 TSA，將存取規則和 NAT 原則新增到各適用區域。各區域使用相同的 **SonicWall SSO 代理**或 **SonicWall 終端服務代理**位址群組。

附註：請勿在使用 SonicWall SSO 的相同區域啟用無線來賓服務。啟用無線來賓服務將停用此區域的 SSO，從而導致通過 SSO 驗證的使用者失去存取權限。請為來賓服務建立單獨的區域。

Mac 和 Linux 使用者調適

Mac 和 Linux 系統不支援 SonicWall SSO 代理使用的 Windows 網路請求，但可通過 Samba 3.5 或更高版本使用 SonicWall SSO。

在安裝 Samba 的 Mac 和 Linux 上使用 SSO

對於 Windows 使用者，安全設備使用 SonicWall SSO 自動驗證 Windows 網域中的使用者。這允許使用者通過安全設備使用正確的篩選和原則相符性獲得存取權限，且在 Windows 網域登入後無需通過任何附加登入過程接受識別。

Samba 是 Linux/Unix 或 Mac 機器使用的軟體包，用於向使用者賦予存取 Windows 網域上的資源（通過 Samba 的 `smbclient` 實用程式）和/或向 Windows 網域使用者賦予存取 Linux 或 Mac 機器上的資源（通過 Samba 伺服器）的權限。

SonicWall SSO 可以識別在 Windows 網域中使用安裝了 Samba 的 Linux PC 或 Mac 的使用者，但需要正確設定 Linux/Mac 機器、SSO 代理和裝置可能有的某些重新設定。例如，以下設定是必需的：

- 若要對 Linux/Mac 使用者使用 SonicWall SSO，必需設定 SonicWall SSO 代理使用 **NetAPI** 而不是使用 **WMI** 獲得來自使用者機器的使用者登入資訊。
- 為了使 Samba 能夠接收和回應來自 SonicWall SSO 代理的請求，必需將其設為網域的成員，且 Samba 伺服器必須執行且將之正確設定為使用網域驗證。

*使用 Samba 的單點登入*技術注釋描述了以上及其他設定的詳細資料。

Samba 3.5 或更高版本支援 SonicWall SSO。

附註：如果有多個使用者登入 Linux PC，將根據最近的登入情況授予從此 PC 存取流量的權限。

在未安裝 Samba 的 Mac 和 Linux 上使用 SSO

如果未安裝 Samba，Mac 和 Linux 使用者仍可以存取，但需要登入防火牆。這可能導致以下問題：

- 來自 Mac 或 Linux 系統的流量可能持續觸發 SSO 識別嘗試，直至使用者登入。如果有很多此類系統，可能導致 SSO 系統效能過載，不過其影響可能在某種程度因「發生錯誤後的等待時間」逾時減小。
- 如果使用了按使用者的內容篩選 (CFS) 原則，但沒有設定有關使用者級別驗證的原則規則，將對 Mac 和 Linux 系統的使用者套用預設的 CFS 原則，除非他們先手動登入。
- 如果將原則規則設為需要使用者級別驗證，來自 Mac 和 Linux 系統的使用者的 Web 瀏覽器連接在發生 SSO 失敗後將重新導向至登入頁面，但 SSO 失敗可能引起逾時進而導致使用者延時。

為了避免發生這些問題，在**規則 > 存取規則**頁面上設定存取規則時，可使用**不叫用單一登入以驗證使用者**選項 (如需關於設定存取規則的詳細資訊，請參閱 *SonicOS 原則*)。只有在已啟用 SonicWall SSO 時，才可看見此選項。如果已選取此選項，不會對於符合規則的流量嘗試進行 SSO，且相符的未驗證 HTTP 連線會直接導向登入頁面。通常，將**來源**下拉功能表設為包含 Mac 和 Linux 系統的 IP 位址的位址物件。

對於使用 CFS 的情況，會將啟用此選項的規則新增到 CFS「之前」，以便來自 Mac 和 Linux 系統的 HTTP 工作階段自動重新導向登入，讓這些使用者無需手動登入。

附註：對於允許完全繞過使用者驗證過程的裝置，請勿選擇**不要叫用 SSO 來驗證使用者**選項。啟用此選項時，可能受存取規則影響的任何裝置都必須能夠手動登入。應該對此類裝置新增單獨的存取規則，在其中將**允許的使用者**設為**全部**。

允許從終端伺服器的 ICMP Ping

在 Windows 中，使用者在終端伺服器上的傳出 ICMP ping 並非透過通訊端傳送，因此無法得到 TSA 識別，所以安全設備不會收到它們的通知。因此，如果要允許通過使用使用者級別身分驗證和 ping 的防火牆規則，必須建立單獨的存取規則允許全部通過。

關於存取規則

存取規則可讓您控制使用者的存取權限。在**規則 > 存取規則**頁面設定的規則，會對照從 SSO LDAP 查詢傳回的使用者群組成員資格進行檢查，並自動套用規則。存取規則是用於定義傳入和傳出存取原則、設定使用者身分驗證和啟用遠端安全設備管理的網路管理工具。**規則 > 存取規則**頁面提供可排序的存取規則管理介面。

附註：應賦予更具體的原則規則比一般原則規則更高的優先順序。一般的具體性層次結構是來源、目的地、服務。確定原則規則的具體性不考慮使用者名稱和相應的群組使用者權限等使用者識別元素。

預設情況下，防火牆的狀態封包偵測允許從 LAN 到網際網路的所有通訊，但封鎖從網際網路到 LAN 的所有流量。

可以定義其它網路存取規則，以便擴充或覆寫預設存取規則。例如，可建立封鎖特定類型的流量（例如 IRC 自 LAN 到 WAN），或允許指定類型的流量（例如從網際網路上的指定主機到 LAN 上的指定主機的 Lotus Notes 資料庫同步），或限制使用特定協定（例如 Telnet 到 LAN 上的授權使用者）。

注意：定義網路存取規則的功能是一個強大的工具。使用自訂存取規則可停用防火牆防護或封鎖對網際網路的所有存取。建立或刪除網路存取規則時需要謹慎。

如需關於存取規則的詳細資訊，請參閱 *SonicOS 原則*。

管理從終端伺服器使用 HTTP 登入的 SonicOS

SonicWall 安全設備通常根據一個 IP 位址上一個使用者的 HTTP 登入提供的身分驗證憑證授予通過原則的存取權限。對於終端伺服器上的使用者，這種在一個 IP 位址上驗證一個使用者的方法並不可行。但是，為了便於管理裝置，仍允許從終端伺服器進行 HTTP 登入，不過須滿足以下的限制和要求：

- 從終端伺服器的網際網路存取由 TSA 控制，且 HTTP 登入不會取而代之，終端伺服器上的使用者不會根據在 HTTP 登入中提供的憑證授予通過安全設備的任何存取權限。
- 來自終端伺服器的 HTTP 登入僅允許用於內建的 **admin** 帳戶及有管理員權限的其他使用者帳戶。嘗試使用非管理帳戶登入會失敗，錯誤為不允許從此位置登入。
- 在成功的 HTTP 登入中，會直接將管理使用者引入管理介面。不顯示小幅**使用者登入狀態**頁面。
- 用於從終端伺服器進行 HTTP 登入的管理使用者帳戶不需要與登入終端伺服器所使用的使用者帳戶相同。這在安全設備上顯示為完全獨立的登入工作階段。

- 一次只能有一名使用者從指定的終端伺服器管理安全設備。如果有兩名同時嘗試這樣做，最近登入的使用者佔先，另一名使用者將看到錯誤這不是最近用於登入的瀏覽器。
- 在由於與 TSA 的通訊問題而導致識別使用者失敗時，不會將 HTTP 瀏覽器工作階段重新導向至 Web 登入頁面（與在 SSO 中失敗相同）。取而代之的是移至顯示由於網路問題，您嘗試連接的目的地暫時無法使用訊息的新頁面。

查看和管理 SSO 使用者工作階段

本章節提供有助於您管理防火牆上的 SSO 的資訊。

主題：

登出 SSO 使用者

監控 | 目前狀態 > 使用者工作階段 > 使用中使用者頁面顯示安全設備上的使用者工作階段。如需關於檢視使用者設定及如何登出使用者的資訊，請參閱 *SonicOS 監控*。

附註：使用者設定 (在**使用者 > 設定**下設定) 中的變更不會反映到使用者的目前工作階段，必須手動登出使用者才能使變更生效。將重新透明登入使用者，此時，變更生效。

設定附加 SSO 使用者設定

使用者 > 設定頁面提供用於使用者工作階段設定、全域使用者設定和可接受使用原則設定以及 SSO 和其他使用者登入設定的設定選項。

在**使用者工作階段**下限制使用者工作階段的選項適用於使用 SSO 登入的使用者。將根據工作階段限制設定登出 SSO 使用者，但傳送後續流量時，會自動以透明的方式再次登入。

附註：請勿將登入工作階段的限制間隔值設定過低。這可能導致效能問題，尤其在部署很多使用者時。

目前 SSO 工作階段期間在**使用者 > 設定**頁面套用的變更不會反映在目前工作階段。

提示：您必須登出使用者才能使變更生效。使用者會立即重新自動登入，此時，變更生效。

使用封包監控查看 SSO 和 LDAP 訊息

調查 | 工具 > 封包監控中的「封包監控」功能提供選項，可擷取對 SSO 代理傳送和接收的解密訊息，以及解密的 LDAP over TLS (LDAPS) 訊息。如需更多資訊，請參閱 *SonicOS 調查*。

擷取 SSO 訊息

如需關於使用封包監控的進一步資訊，請參閱 *SonicOS 調查*。

若要擷取傳送至或來自 SSO 驗證代理的解密訊息：

1 導覽至**調查 | 工具 > 封包監控**。

2 在**十六進位傾印**區段下，按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**進階監視篩選條件**。

4 選取**監控中間封包**。

5 選取**監視中間解碼單一登入代理訊息**。

6 按一下**確定**。

封包將在輸入/輸出介面欄位中標有 **(sso)**。它們有虛擬乙太網路、TCP 和 IP 標頭，所以這些欄位中的某些值可能不正確。

這將允許向封包監控饋送解密的 SSO 封包，但仍將對其套用所有監視篩選條件。

擷取的 SSO 訊息會在**工具 > 封包監控**頁面中以完全解碼的形式顯示。

擷取 LDAP over TLS 訊息

若要擷取解密的 LDAP over TLS (LDAPS) 封包：

1 導覽至**調查 | 工具 > 封包監控**。

2 在**十六進位傾印**區段下，按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**進階監視篩選條件**。

4 選取**監控中間封包**。

5 選取**監控中繼解密的 LDAP over TLS 封包**。

6 按一下**確定**。

封包會在輸入/輸出介面欄位中標有 **(ldp)**。它們有虛擬乙太網路、TCP 和 IP 標頭，所以這些欄位中的某些值可能不正確。將 LDAP 伺服器連接埠設為 389，以使外部擷取分析程式（例如 Wireshark）知道將這些封包解碼為 LDAP。已擷取的 LDAP 繫結請求中的密碼已經過混淆處理。LDAP 訊息在「封包監控」顯示中未解碼，但可以在 WireShark 中匯出和顯示擷取的內容，以查看解碼的形式。

這將允許向封包監控饋送解密的 LDAPS 封包，但仍將對其套用所有監視篩選條件。

附註：LDAPS 擷取僅適用於來自防火牆的 LDAP 用戶端的連接，且不會顯示來自外部 LDAP 用戶端通過防火牆的 LDAP over TLS 連接。

關於多管理員支援

您可以設定多管理員設定檔，如第 191 頁「設定本機使用者與群組」中所述。

在使用 RADIUS 或 LDAP 身分驗證時，如果您要確保某些或全部管理使用者即使在無法連接 RADIUS 或 LDAP 伺服器時也始終能管理裝置，您可以使用 **RADIUS + 本機使用者**或 **LDAP + 本機使用者**選項，並在本機設定這些指定使用者的帳戶。

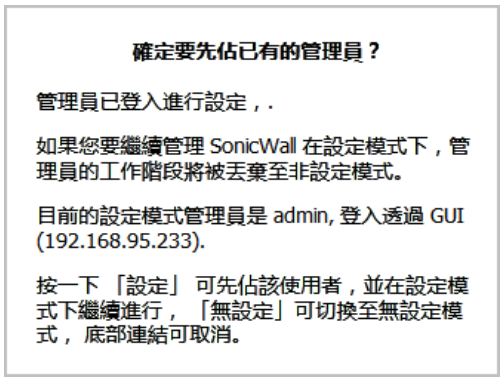
對於經 RADIUS 或 LDAPF 驗證的使用者，在 RADIUS 或 LDAP 伺服器（或其背景）上建立以使用者群組命名的 **SonicWall Administrators** 和/或 **SonicWall Read-Only Admins**，並將相關的使用者指派到這些群組。

附註：對於 RADIUS，您可能需要對 RADIUS 伺服器進行特殊設定，以返回使用者群組資訊。

主題：

先佔管理員

當管理員嘗試在其他管理員已登入的情況下登入時，會顯示以下訊息:

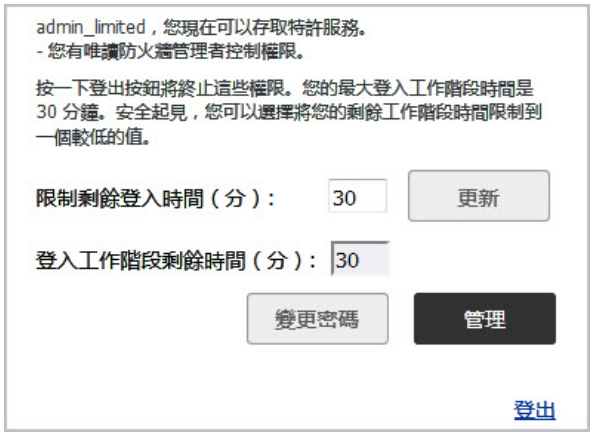


此訊息為您提供三個選項:

設定	先佔目前管理員。將目前管理員置於非設定模式，現賦予您完全管理員存取權限。
無設定	以「無設定」模式登入 SonicWall 安全設備。目前管理員的工作階段不受干擾。
請勿開始管理	返回登入畫面。

使用管理員權限登入

以具有管理員權限的使用者身分登入時 (也就是非**管理員**使用者)，隨即顯示**使用者登入狀態**訊息。



若要移至 SonicWall 管理介面，請按一下**管理**按鈕。您得到再次輸入密碼的提示。這是為了在管理員離開其電腦但未登出其工作階段時防護不受未經授權的存取。

停用使用者登入狀態快顯視窗

如果您希望允許某些使用者僅為了管理 SonicWall 安全設備而登入，而不是為了獲得安全設備的特殊權限存取，您可以停用**使用者登入狀態**快顯。若要停用快顯，請在新增或編輯本機群組時，選取**成員從網頁直接登入到管理介面**選項。

如果您要某些使用者帳戶僅用於管理目的，而其他使用者需要登入獲得設備的特殊權限存取，但仍需要能夠對其進行管理 (即有些使用者在登入後直接進入管理介面，而其他使用者利用**管理**按鈕，看見**使用者登入狀態**快顯對話方塊)，可以通過以下操作實現:

1 選取**成員從網頁直接登入到管理介面**選項，以建立本機群組。

2 將群組新增到相關的管理群組，但在管理群組中不選取此選項。

3 將僅用於管理目的這些使用者帳戶新增到新使用者群組。停用這些使用者的**使用者登入狀態**快顯。

4 將要指派權限和管理存取權限的使用者帳戶新增到頂層管理群組。

設定多管理員支援

主題：

- 第 108 頁「設定附加管理員使用者設定檔」
- 第 108 頁「使用 LDAP 和 RADIUS 時在本機設定管理員」
- 第 107 頁「先佔管理員」
- 第 107 頁「使用管理員權限登入」
- 第 109 頁「驗證多管理員支援設定」
- 第 109 頁「查看多管理員相關的記錄訊息」

設定附加管理員使用者設定檔

設定其他管理員的方式與設定其他本機使用者的方式相同，並將其加入適當的本機群組:

此群組	提供使用者
限制的管理員	有限的管理員設定權限。
SonicWall 管理員	完整的管理員設定權限。
SonicWall 唯讀管理員	僅適用於整個管理介面的檢視權限。

如需瞭解如何設定本機使用者與本機群組，請參閱第 191 頁「設定本機使用者與群組」。

使用 LDAP 和 RADIUS 時在本機設定管理員

在使用 RADIUS 或 LDAP 身分驗證時，如果您要確保某些或全部管理使用者即使在無法連接 RADIUS 或 LDAP 伺服器時也始終能管理 SonicWall 安全設備，您可以使用 **RADIUS + 本機使用者**或 **LDAP + 本機使用者**選項，並在本機設定這些指定使用者的帳戶。

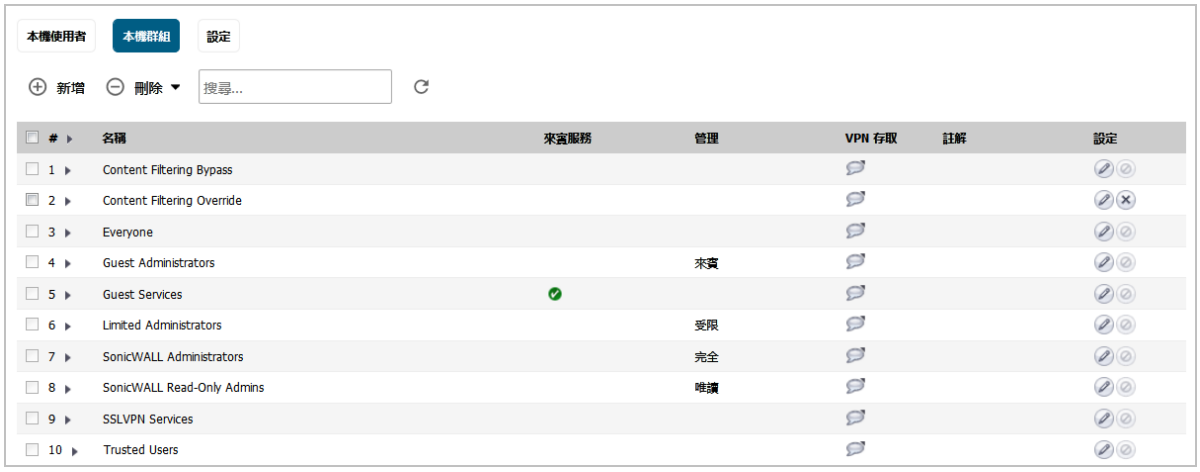
對於經 RADIUS 或 LDAPF 驗證的使用者，在 RADIUS 或 LDAP 伺服器（或其背景）上建立以使用者群組命名的 **SonicWall Administrators** 和/或 **SonicWall Read-Only Admins**，並將相關的使用者指派到這些群組。

附註：對於 RADIUS，您可能需要對 RADIUS 伺服器進行特殊設定，以返回使用者群組資訊。

若要瞭解使用 LDAP 或 RADIUS 時如何設定管理員，請參閱第 191 頁「設定本機使用者與群組」。

驗證多管理員支援設定

可以在**使用者 > 本機使用者和群組 > 本機群組**頁面查看有管理員和唯讀管理員權限的使用者帳戶。



您可以藉由查看管理介面右上角的**模式**，以判斷您處於何種設定模式:

進行變更時，狀態列會顯示:

嘗試變更時，狀態列會顯示:

查看多管理員相關的記錄訊息

以下事件會產生記錄訊息:

- GUI 或 CLI 使用者開始設定模式（包括管理員何時登入）。
- GUI 或 CLI 使用者結束設定模式（包括管理員何時登出）。
- GUI 使用者開始在非設定模式中管理（包括管理員何時登入，處在設定模式中的使用者何時受到先佔並重新置於唯讀模式）。
- GUI 使用者開始在唯讀模式中管理。

GUI 使用者結束以上任一管理工作階段（包括管理員何時登出）。

8

設定用於管理使用者的設定

使用者 | 設定

在**管理 | 系統安裝 | 使用者 | 設定**上，您可以設定所需的驗證方法、全域使用者設定和在使用者登入網路時向其顯示的可接受使用者原則。

主題：

- 第 128 頁「設定 RADIUS 身分驗證」
- 第 133 頁「為 LDAP 設定 SonicWall」
- 第 142 頁「設定 SonicOS 以使用 SonicWall SSO 代理」

設定使用者驗證和登入設定

重要：完成設定**使用者 | 設定**頁面時，按一下**接受**。

主題：

- 第 111 頁「使用者驗證設定」
- 第 114 頁「使用者 Web 登入設定」
- 第 115 頁「驗證繞過設定」
- 第 120 頁「使用者工作階段設定」
- 第 121 頁「SSO 驗證使用者的使用者工作階段設定」
- 第 122 頁「用於 Web 登入的使用者工作階段設定」
- 第 124 頁「登入後可接受的使用原則」
- 第 126 頁「自訂登入頁面」

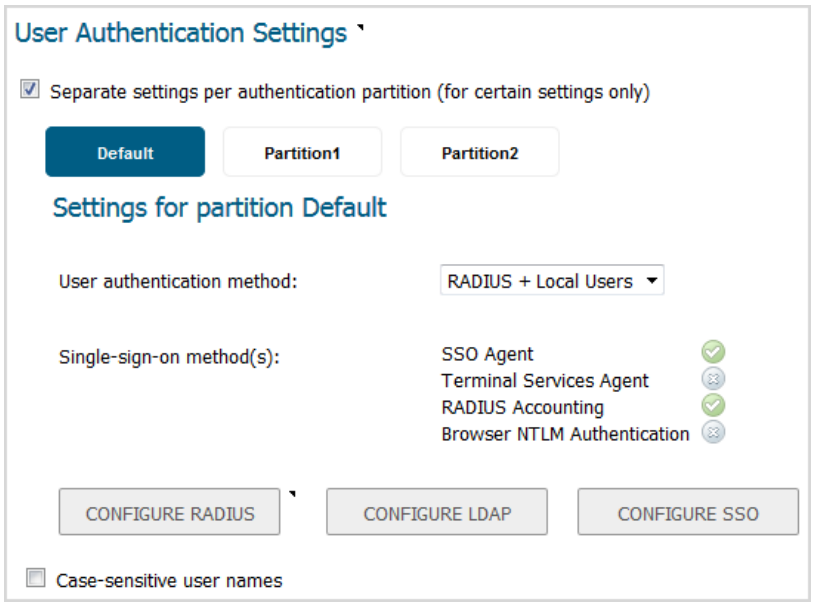
使用者驗證設定

設定使用者驗證設定的步驟如下：

1 導覽到**管理 | 系統安裝 | 使用者 | 設定**。

2 如果分割:

- 未啟用，請移至步驟 4。
- 已啟用，隨即顯示**依每個驗證分割區區分設定 (僅適用於特定設定)** 選項。選取此選項，隨即顯示**分割區設定**選項。



3 對於每個分割區，執行步驟 4。

4 從**使用者驗證方法**中，選取您網路使用的使用者帳戶管理類型:

本機使用者

可使用**使用者 | 本機使用者與群組**頁面，在安全設備中設定本機資料庫中的使用者。

如需關於使用本機資料庫進行驗證的資訊及詳細設定說明，請參閱第 72 頁「使用本機使用者和群組進行驗證」。

RADIUS

當您有 1,000 名以上使用者，或者想增加額外的安全層驗證存取安全設備的使用者時，可使用此選項。如果您選擇 RADIUS 進行使用者驗證，使用者必須使用 HTTPS 登入安全設備以加密傳送至安全設備的密碼。如果使用者嘗試使用 HTTP 登入安全設備，瀏覽器會自動重新導向至 HTTPS。

在一些情況下，除了 LDAP，可能還需要 RADIUS：

- LDAP 通常不支援 CHAP/MSCHAP 身分驗證（Microsoft Active Directory 和 Novell eDirectory 均不），因此如果是這樣且設定了 RADIUS，則 SonicWall 通過 RADIUS 來驗證 CHAP/MSCHAP。
- 如果 NTLM 用於 SSO，則只能在 MS-CHAP 模式下通過 RADIUS 對其進行驗證。

對於 L2TP 伺服器或 VPN 或 SSL VPN 用戶端（包括 NetExtender 和 Portal）的 CHAP/MS-CHAP，或者如果為 NTLM 所需要，可能需要 RADIUS。

附註：LDAP 一般仍用於非 CHAP 驗證，而 RADIUS 用於 CHAP 驗證。

如需使用 RADIUS 資料庫進行身分驗證的資訊，請參見第 75 頁「使用 RADIUS 進行驗證」。

如需詳細的設定說明，請參見第 128 頁「設定 RADIUS 身分驗證」。

RADIUS + 本機使用者	當您想使用 RADIUS 和安全設備本機使用者資料庫進行驗證時，可使用此選項。
LDAP	當您使用輕量型目錄存取通訊協定 (LDAP) 伺服器、Microsoft Active Directory (AD) 伺服器或 Novell eDirectory 維護所有使用者帳戶資料時，可使用此選項。 如需使用 LDAP 資料庫進行身分驗證的資訊，請參見第 75 頁「使用 LDAP/Active Directory/eDirectory 驗證」。 如需詳細的設定說明，請參見第 78 頁「將 LDAP 整合至 SonicWall 安全設備」。
LDAP + 本機使用者	當您想使用 LDAP 和安全設備本機使用者資料庫進行驗證時，可使用此選項。

5 對於**單一登入方法**，選擇以下一種方法：

附註：如果未使用單點登入驗證使用者，請勿選擇任何這些選項。

SonicWall SSO 代理	當您使用 Active Directory 進行驗證，而且相同網域中的電腦上已安裝 SSO 代理時，可使用此選項。如需詳細的 SSO 設定說明，請參見第 99 頁「關於單一登入」。
終端服務代理	當您使用終端服務，而且相同網域的終端伺服器上已安裝終端服務代理 (TSA) 時，可使用此選項。
僅限瀏覽器 NTLM 驗證	若要不使用 SSO 代理或 TSA 驗證 Web 使用者，可選擇此選項。使用者在傳送 HTTP 流量時即會識別。NTLM 要求設定 RADIUS（如使用 LDAP，則在 LDAP 基礎上進行設定）存取 MSCHAP 身分驗證。如果在上面選擇了 LDAP，則在選擇 NTLM 時會顯示用於 RADIUS 的單獨**設定**按鈕。
RADIUS 計費	若要網路存取伺服器 (NAS) 向計費伺服器傳送使用者登入工作階段計費訊息，可使用此選項。

6 選擇**使用者名稱區分大小寫**基於使用者帳戶名稱的大寫情況來啟用符合。

7 選擇**強制登入唯一性**封鎖在同時從多個位置使用相同的使用者名稱登入網路。此選項適用於本機使用者和 RADIUS/LDAP 使用者，但是不適用於使用者名稱為 **admin** 的預設管理員。預設情況下未勾選此選項。

8 若要讓使用者在變更其密碼後登入，請選取**變更密碼後強制重新登入**。預設情況下未勾選此選項。

9 如需顯示自上一次登入以來的使用者登入資訊，請勾選**顯示使用者最後的登入訊息**。預設情況下未勾選此選項。

如果啟用此選項，則使用者登入資訊 (包括上一次成功登入的時間戳記、所有使用者成功登入嘗試次數、失敗登入嘗試次數及管理員權限變更) 均會顯示在**調查 | 記錄 | 事件記錄**中。如需關於記錄的詳細資訊，請參閱 *SonicOS 調查*。

10 設定以下**一次性密碼**選項：

- **一次性密碼電子郵件格式** - 選擇**普通文字**或 **HTML**。
- **一次性密碼格式** - 從下拉功能表中選擇**字元**（預設）、**字元 + 數字**或**數字**。

  提示：格式選擇以及兩個密碼長度值會產生「差」、「好」、「很好」的密碼強度。最強的密碼長度長且格式為**字元**或**字元 + 數字**；最弱的密碼強度為**數字**格式，不論長度是多少。

- 在**一次性密碼長度**中，在第一個欄位輸入最小長度，在第二個欄位輸入最大長度。最小和最大長度須在 4 到 14 的範圍內，每個欄位的預設值為 **10**。最小長度不能超過最大長度。

使用者 Web 登入設定

設定使用者 Web 登入設定的步驟如下：

1 導覽到**管理 | 系統安裝 | 使用者 | 設定**。

2 按一下網頁登入。

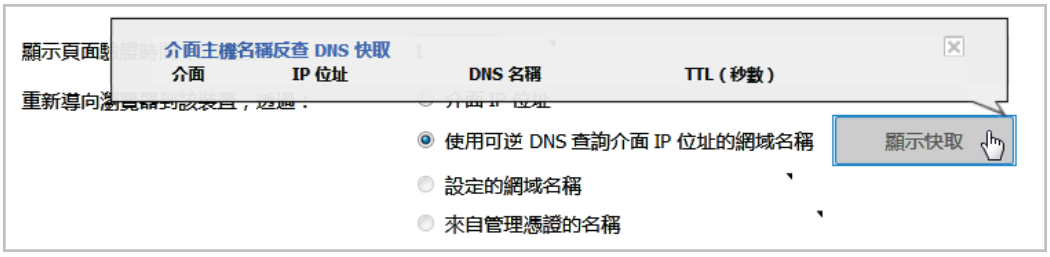
3 在**顯示使用者驗證頁面（分鐘數）**欄位中，輸入使用者在登入頁面逾時之前必須使用其使用者名稱和密碼登入的分鐘數。如果逾時，會顯示一條訊息告知再次嘗試登入之前必須執行的操作。預設時間為 **1** 分鐘。

在顯示登入驗證頁面時，會使用系統資源。通過設定在登入頁面關閉之前登入執行的時間限制，可以釋放這些資源。

4 從**將瀏覽器重新導向此設備的管道**中，選擇決定使用者瀏覽器最初如何重新導向 SonicWall 設備之 Web 伺服器的方式:

- **介面 IP 位址** - 選擇此選項將瀏覽器重新導向至裝置 Web 伺服器介面的 IP 位址。預設情況下已核取此選項。
- **使用可逆 DNS 查詢介面 IP 位址的網域名稱** - 這將啟用**顯示快取**按鈕，按一下後，顯示裝置 Web 伺服器的介面、IP 位址、DNS 名稱和 TTL（以秒為單位）。預設情況下未勾選此選項。

  按一下**顯示快取**，以確認用於重新導向使用者瀏覽器的網域名稱 (DNS 名稱)。



- **其設定的網域名稱** - 選取此選項可重新導向在**系統安裝 | 設備 > 基本設定**設定的網域名稱。在此頁面為 HTTPS Web 管理選擇匯入的憑證後，允許定向至來自管理憑證的名稱。

  附註：此選項只有在**系統安裝 | 設備 > 基本設定**上已指定網域名稱時才可供使用。否則，此選項為灰顯。

- **來自管理憑證的名稱** - 選取此選項可重新導向擁有正確簽署憑證的網域名稱。在此頁面為 HTTPS Web 管理選擇匯入的憑證後，允許定向至來自管理憑證的名稱。在**系統安裝 | 設備 > 基本設定**上設定網域名稱。

  附註：只有在**系統安裝 | 設備 > 基本設定**的 **Web 管理設定**區段中，為 HTTPS 管理匯入憑證時，才可使用此選項。請參閱第 16 頁「配置基本設定」。

  提示：如果正在使用匯入的管理憑證，請使用此選項。如果不會使用管理憑證，請選擇**其設定的網域名稱**選項。

  要進行 HTTPS 管理且瀏覽器不顯示無效憑證警告，需要匯入由憑證頒發機構正確簽章的憑證（管理憑證，而不是使用內部產生的自簽章憑證。必須為裝置及其主機網域名稱產生此類憑證。正確簽章的憑證是獲取裝置網域名稱的最佳途徑。

  如果您使用管理憑證，且要避免憑證警告，瀏覽器需要重新導向到此網域名稱，而不是 IP 位址。例如，如果您嘗試瀏覽 Internet 並重新導向以在 `https://gateway.sonicwall.com/auth.html` 登入，裝置上的管理憑證會認為此裝置真的是 `gateway.sonicall.com`，因此瀏覽器顯示登入頁面。但是，如果您重新導向至 `https://10.0.02/auth.html`，即使憑證表明它是 `gateway.sonicall.com`，瀏覽器也沒有辦法判斷是否正確，因此會顯示憑證警告。

5 如果您希望使用者在通過 HTTPS 登入後通過 HTTP 經由安全設備連接到網路，請選擇**當使用者完成登入以後從 HTTPS 導向到 HTTP**。如果有大量使用者通過 HTTPS 登入，您可能想將他們重新導向到 HTTP，因為 HTTPS 比 HTTP 消耗更多的系統資源。預設情況下已核取此選項。如果您取消選擇此選項，將看到警告對話方塊。

6 選擇**允許以 HTTP 帶有 RADIUS CHAP 模式登入**在 RADIUS 使用者嘗試登入 HTTP 時發佈 CHAP 問題。這樣，即使不使用 HTTPS，也能實現安全連接。確保檢查 RADIUS 伺服器支援此選項。預設情況下未勾選此選項。

  附註：如果您使用此方法登入，將受限於可以執行的管理操作，因為某些操作需要裝置知道管理員密碼；對於由遠端驗證伺服器執行的 CHAP 驗證，裝置不知道密碼。

  因此，如果勾選此設定，管理使用者組成員的任何使用者要因為執行管理操作而登入，可能都需要通過 HTTPS 手動登入。此限制不適用於內建的 **admin** 帳戶。

  附註：在使用 LDAP 時，可以通過將**登入驗證方法**設定為 **RADIUS**，然後選擇 LDAP 作為在 RADIUS 設定中設定使用者組成員的機制，此機制即可正常使用。

7 對於網頁驗證入口來賓驗證，若要允許驗證頁面以框架形式顯示在入口網站主機頁面中，請選取**允許框架形式的驗證頁面**。 預設情況下未勾選此選項。

8 按一下**接受**。

驗證繞過設定

SonicOS 「來賓服務」允許來賓使用者透過您的網路直接存取網際網路，而無需存取受保護的網路。若要執行此操作，SonicOS 會使用使用者電腦的 IP 位址。

當來賓使用者流量流經網路路由器時，使用 IP 位址作為識別碼非常有用，因為這會將來源 MAC 位址變更為該路由器的位址。不過，流經的使用者 IP 位址不變。

如果僅使用 MAC 位址進行識別，連線安全設備後，相同路由器後面的兩個用戶端將具有相同的 MAC。當其中一個用戶端經過驗證後，來自另一個用戶端的流量也會視為已驗證，並繞過來賓服務驗證。

藉由使用用戶端 IP 位址進行識別，所有路由裝置後的來賓用戶端皆需要單獨驗證。

主題：

將 URL 新增至驗證繞過

若要在存取規則中新增 HTTP URL 使用者驗證繞過:

1 導覽至**系統安裝 | 使用者 | 設定 > 驗證繞過**。

2 按下**新增**。隨即顯示**新增 URL** 快顯。

3 在**輸入 URL** 欄位中，輸入 URL。

4 按一下**確定**。隨即顯示快顯確認訊息。

5 按一下**確定**。

6 完成新增 URL 時，按一下**接受**。

設定自動設定

自動設定 URL 以繞過防火牆規則中的使用者驗證，實作方式是允許 (僅從一個 IP 位址) 通過的流量，否則這些流量會被需要使用者驗證的規則封鎖，並記錄存取的目的地。

若要設定自動設定:

1 導覽至**系統安裝 | 使用者 | 設定 > 驗證繞過**。

2 按一下**自動設定**。隨即顯示**原則使用者驗證繞過自動設定**對話方塊。

3 在 **IP 位址**欄位中輸入來源 IP 位址。**開始**會變成可用狀態。

4 按一下**啟動**。隨即顯示**追蹤進行中**指示器和**追蹤已啟動**訊息。

5 按一下**確定**。

轉換 URL 以進行萬用字元比對

繞過驗證支援萬用字元比對。此功能允許一個或多個追蹤的 URL 轉換為符合所有目前選取之 URL 的單一萬用字元。

附註：選取的 URL 必須在相同網域中。

轉換至網路

Windows Update 會透過 HTTPS 存取某些目的地，而這些目的地只能根據 IP 位址追蹤。然而，每次存取的實際 IP 位址可能有所不同，因此，不要嘗試為每個 IP 位址設定繞過，而是允許 HTTPS 繞過該網路中的所有 IP 位址。

轉換至網路繞過允許追蹤的 HTTPS 目的地 IP 位址轉換成下列任一項目:

- 類別 B (16 位元) 網路 (預設)
- 類別 C (24 位元) 網路

設定使用者工作階段

主題：

- 第 120 頁「使用者工作階段設定」

使用者工作階段設定

設定適用於通過安全設備驗證的所有使用者的設定的方法是：

1 在**非使用狀態逾時（分鐘數）**欄位中指定安全設備將多長時間非使用中的使用者登出。預設值為 **15** 分鐘。

2 從**不允許以下服務的流量，以免使用者在非使用中狀態中登出**下拉功能表中，選擇會封鎖登出非使用中使用者的服務或服務群組選項。勾選此選項使逾時的使用者進入非使用中狀態而不是登出，從而減少由於重新識別逾時的驗證使用者而導致的系統開銷和可能延時。非使用中的使用者不佔用系統資源，並可以顯示在**使用者>狀態**頁面。預設為**無**。

3 對於下面的**記錄未識別使用者的連線**選項，請選擇要執行的記錄類型，**不記錄任何使用者名稱**或**記錄使用者名稱**，（可選）記錄使用者名稱：

- **如果 SSO 無法識別使用者: 記錄使用者名稱，未知 SSO 失敗**（預設）
- **對於繞過 SSO 的連線: 記錄使用者名稱，SSO 繞過**（預設）

  附註：還可以在 **SSO 驗證設定**對話方塊的**實施的 SSO 繞過部分**標籤中設定此選項。

- **對於源自外部的連線：**預設為**不記錄任何使用者名稱**；如果選擇**記錄使用者名稱**，則預設使用者名稱為**未知（外部）**
- **對於其他未識別的連接：**預設為**不記錄任何使用者名稱**；如果選擇**記錄使用者名稱**，則預設使用者名稱為**未知**

4 通過**登出時剩餘使用者連接的操作**選項指定在使用者從 SonicWall 裝置登出後，如何處理餘下的使用者連接。

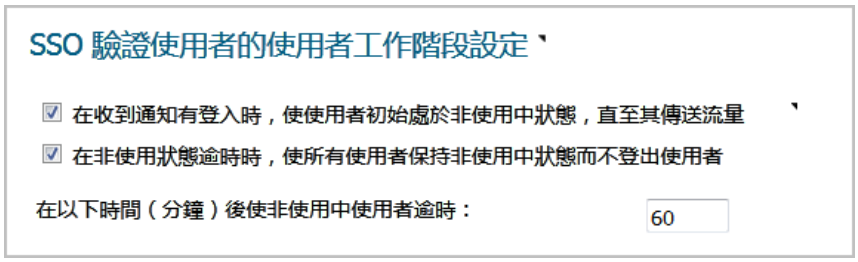
登出類型	操作 對於需要使用者驗證的連線 [a]	對於其他連線 [b]
由於非使用中而登出時	使它們處於活動狀態（預設） 終止 在以下時間後終止...分鐘	使它們處於活動狀態（預設） 終止 在以下時間後終止...分鐘
在使用中/報告的登出時	保持運作 終止它們（預設） 在以下時間後終止...分鐘	保持運作 終止 在以下時間後終止... 15 分鐘（預設）

a. 適用於通過僅允許特定使用者的存取規則的連接。
b. 適用於沒有特定使用者驗證要求的其他連接。

可以針對不同情況設定不同操作：

- 非使用中登出，使用者可能仍登入到此網域/電腦，也可能沒有
- 使用者主動登出或將登出情況報告給 SonicWall 裝置（後者通常意味著使用者已從網域/使用者登出）

SSO 驗證使用者的使用者工作階段設定



若要指定如何處理非使用中的 SSO 驗證使用者：

1 若要使已通過 SSO 機制為 SonicWall 裝置所識別，但是還未收到來自其流量的使用者進入非使用中狀態，以便它們不佔用資源，請勾選**在收到通知有登入時，使使用者初始處於非使用中狀態，直至其傳送流量**核取方塊。使用者將處於非使用中狀態，直至收到來自其的流量。預設情況下已核取此選項。

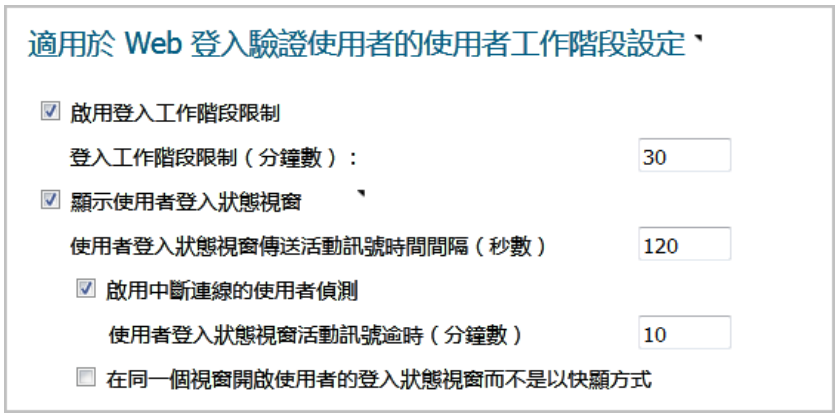
某些 SSO 機制未提供任何方式來讓 SonicWall 裝置主動地重新識別使用者，如果使用者由此類機制識別身分後未傳送流量，其將處於非使用中狀態，直至裝置最終收到此使用者的登出通知。對於其他可以重新識別的使用者，如果其保持非使用中且不傳送流量，經過在步驟 3 中設定的一定時間後，其將因逾時而移除。

2 如果一名主動登入的 SSO 識別使用者因無活動而逾時登出，則無法重新識別的使用者將回到非使用中狀態。為了讓在非使用中狀態後登出的使用者回到非使用中狀態，請勾選**在非使用中逾時時，使所有使用者保持非使用中狀態而不登出使用者**核取方塊。這樣做可以避免使用者再次使用中時重新識別使用者身分所需的開銷和可能的延遲。預設情況下已選擇此設定。

3 對於應該因逾時而登出的非使用中使用者，您可以設定以分鐘為單位的時間，如果他們保持非使用中狀態且不傳送流量，則在此時間後他們會因逾時而移除，方法是勾選**在以下時間（分鐘）後使非使用中使用者逾時**核取方塊且在欄位中指定逾時時間。預設勾選此設定，最小逾時值為 10 分鐘，最大為 10000 分鐘，預設為 **60** 分鐘。

附註：將非使用中使用者與使用中使用者分開的原因是為了儘量減少用於管理他們的資源，逾時計時器每 10 分鐘執行一次。因此，可能需要 10 多分鐘才能從使用中狀態移除非使用中使用者。

用於 Web 登入的使用者工作階段設定



為 Web 登入設定使用者工作階段設定的步驟如下：

1 **啟用登入工作階段限制**：可以通過勾選核取方塊且在**登入工作階段限制（分鐘數）**欄位中輸入時間長度，限制使用者通過 Web 登入登入到安全設備的時間。預設選擇此設定，預設值為 **30** 分鐘。

2 **顯示使用者登入狀態視窗** - 對於通過 Web 登入登入的使用者，在使用者工作階段期間，顯示帶有**登出**按鈕的狀態視窗。使用者可以按一下**登出**按鈕登出其工作階段。

附註：此視窗在整個使用者工作階段期間必須保持打開狀態，因為關閉它會將使用者登出。

重要：如果不啟用此選項，則狀態視窗不會顯示且使用者可能無法登出。在此情況下，必須設定登入工作階段限制以確保他們最終得以登出。

使用者登入狀態視窗顯示使用者已離開登入工作階段的分鐘數。使用者可以通過輸入數值和按一下**更新**按鈕將剩餘時間設為較小的分鐘數。

如果啟用此選項，則還可以啟用監控來自此視窗的使用中訊號的機制，以偵測且登出未登出但中斷連接的使用者。

如果使用者是 SonicWall 管理員或有限管理員使用者群組的成員，**使用者登入狀態**視窗有可以按一下以自動登入到安全設備管理介面的**管理**按鈕。如需停用管理使用者的**使用者登入狀態**視窗的資訊，請參見第 108 頁「停用使用者登入狀態快顯視窗」。如需群組設定過程的資訊，請參見第 191 頁「設定本機使用者與群組」。

- **使用者登入狀態視窗傳送活動訊號時間間隔（秒數）** - 設定用於偵測使用者是否仍有有效連接的活動訊號信號頻率最小活動訊號頻率為 10 秒，最大為 65530 秒，預設為 **120** 秒。

3 **啟用中斷連線的使用者偵測** - 讓安全設備偵測使用者的連接是否仍有效和結束工作階段。預設情況下已選擇此設定。

- **使用者登入狀態視窗活動訊號逾時（分鐘數）** - 設定在結束使用者工作階段前允許無活動訊號回應的時間。終止使用者工作階段之前的最短延遲為 1 分鐘，最大為 65535 分鐘，預設為 **10** 分鐘。

4 （可選）通過勾選**在同一個視窗開啟使用者的登入狀態視窗而不是以快顯方式**核取方塊，可以讓使用者的登入狀態視窗顯示在同一視窗中，而不是快顯視窗。

自訂

主題：

- 第 123 頁「登入前原則橫幅」

登入前原則橫幅

在本節中，您會建立一個原則聲明，在登入 Web 之前，在視窗中以橫幅的方式向所有使用者呈現。原則橫幅可能包含 HTML 格式設定。

若要建立登入前原則橫幅:

1 導覽到**管理 | 系統安裝 | 使用者 | 設定**。

2 按一下**自訂**。

3 捲動至**登入前原則橫幅**區段。

4 在**登入前原則橫幅**區段中，選取**登入頁面前啟動原則橫幅**。 預設情況下未勾選此選項。

5 在**原則橫幅內容**欄位中，輸入您的原則文字。您可以包含 HTML 格式。顯示給使用者的頁面包含用於使用者確認的**我接受**按鈕和**取消**按鈕。

> **提示：**按一下**範例範本**，將為您的原則橫幅視窗建立預設格式的 HTML 範本；請參閱第 124 頁「範例範本」。

6 按一下**接受**。

主題：

- 第 125 頁「範例範本」
- 第 124 頁「預覽訊息」

範例範本

按一下**範例範本**，使用預設的 AUP 範本來填寫內容，您可以修改:

```
<font face=arial size=3>
<center><b><i>Welcome</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>
```

只有當您想接受這些條款並繼續時，才按下「我接受」，否則請選取「取消」。

預覽訊息

按一下**預覽**即顯示使用者將看到的 AUP 訊息。

登入後可接受的使用原則

可接受的使用者原則 (AUP) 就是使用者必須同意遵守才能存取網路或網際網路的原則。很多企業和教育機構經常要求員工或學生在通過安全設備存取網路或存取網際網路時同意可接受的使用者原則。

登入後可接受的使用原則區段可讓您為使用者建立 AUP 訊息視窗。您可以在訊息本文中使用 HTML 格式。按一下**範例範本**，將為您的 AUP 視窗建立預設格式的 HTML 範本；請參閱第 125 頁「範例範本」。

若要建立登入後 AUP 訊息視窗:

1 導覽到**管理 | 系統安裝 | 使用者 | 設定**。

2 按一下**自訂**。

3 捲動至**登入後可接受的使用原則**區段。

4 指定設定：

- **顯示登入來自** - 選擇在使用者登入時您要顯示「可接受的使用者原則」頁面的網路介面。您（預設）可以選擇任意組合**受信任區域**（預設）、**WAN 區域（預設）**、**公開區域**（預設）、**無線區域**和 **VPN 區域**。
- **視窗大小（像素）** - 用於以像素數指定 AUP 視窗的大小。
  - 寬度：最小為 400 像素，最大為 1280 像素，預設為 **460** 像素。
  - 高度：最小為 200 像素，最大為 1024 像素，預設為 **310** 像素。
- **在視窗上啟用捲軸** - 如果您的內容超出視窗的顯示大小，請開啟捲軸。預設情況下已核取此選項。
- **可接受的使用者原則**頁面內容 - 在文字框中輸入您的「可接受的使用者原則」文字。您可以包含 HTML 格式。顯示給使用者的頁面包含用於使用者確認的**我接受**按鈕和**取消**按鈕。

5 按一下**接受**。

主題：

- 第 125 頁「範例範本」
- 第 126 頁「預覽訊息」

範例範本

按一下**範例範本**，使用預設的 AUP 範本來填寫內容，您可以修改:

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWall</center></b></i>
<font size=2>

<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>

Click "I Accept" only if you wish to accept these terms and continue,
or otherwise select "Cancel".
```

預覽訊息

按一下**預覽**即顯示使用者將看到的 AUP 訊息。

自訂登入頁面

SonicOS 允許自訂呈現給使用者的登入驗證頁面的文字。您可以用自己的語言來翻譯登入相關的頁面並套用變更，這樣無需重新啟動便可使其生效。

雖然整個 SonicOS 管理介面提供多種不同語言介面，但有時候，您並不希望將整個 UI 語言變更為特定的本機語言。

然而，如果安全設備要求使用者先進行驗證，然後才能存取其他網路，或啟用外部存取服務 (例如 VPN、SSL-VPN)，則這些登入相關頁面通常應該本地化，讓一般使用者能夠妥善運用。

自訂登入頁面特性提供以下功能：

- 預設保留原登入樣式
- 自訂登入相關頁面
- 使用預設登入相關頁面作為範本
- 將自訂頁面儲存到系統喜好設定中
- 允許在儲存到喜好設定中之前預覽變更
- 向一般使用者呈現自訂的登入相關頁面

可自訂以下登入相關的頁面：

- 管理員先佔
- 登入驗證
- 登出
- 登入已滿
- 不允許登入

- 登入鎖定
- 登入狀態
- 來賓登入狀態
- 原則存取封鎖
- 原則存取無法使用
- 原則存取無效
- 原則登入重新導向
- 原則 SSO 探查失敗
- 使用者密碼更新
- 使用者登入訊息

自訂其中一個頁面的步驟如下：

1 導覽到**管理 | 系統安裝 | 使用者 | 設定**。

2 按一下**自訂**。

3 捲動至**自訂登入頁面**區段。

4 從**選取登入頁面**中，選取要自訂的頁面。

5 捲動到頁面底部。

6 按一下**預設**，載入頁面的預設內容。

7 編輯此頁面的內容。

ⓘ **附註：**範本頁面中的 `var strXXX =` 行是自訂 JavaScript 字串。您可將其變更為自己慣用的語言。修改應遵從 JavaScript 語法。您還可以編輯 HTML 部分中的內容。

8 按一下**預覽**，預覽自訂頁面的外觀。將顯示一條訊息。

9 按一下**確定**。您的自訂頁面隨即顯示。

10 關閉視窗。

11 進行任何變更。

12 完成頁面編輯後，按一下**接受**。

△ 注意：**部署前，務必驗證自訂登入頁面的 HTML，因為 HTML 錯誤可能導致登入頁面不能正常工作。如果自訂登入頁面有問題，管理員始終可以使用備用登入頁面。若要存取備用登入頁面，請直接手動輸入以下 URL：*https://(device_ip)/defauth.html* 到瀏覽器的位址欄（區分大小寫）。這樣就會顯示無任何變更的預設登入頁面，以便您正常登入，重設自訂登入相關頁面。**

ⓘ **提示：**如果**登入頁面的內容**欄位保持空白並套用變更，則使用者看到的仍將是預設頁面。

設定 RADIUS 身分驗證

附註：如需瞭解為 SonicPoint 或 SonicWave 設定 RADIUS 的相關資訊，請參閱 *SonicOS 連線*。

如需 SonicOS 中 RADIUS 身分驗證的說明，請參見第 75 頁「使用 RADIUS 進行驗證」。如果您在**使用者 | 設定**頁面的**登入驗證方法**下拉功能表中選取 **RADIUS** 或 **RADIUS + 本機使用者**，則**設定 RADIUS** 按鈕會變成可用狀態。

如果您在**單一登入方法**選項中選擇了**僅瀏覽器 NTLM 驗證**，還可以使用 RADIUS 的單獨的**設定**按鈕。設定過程相同。

主題：

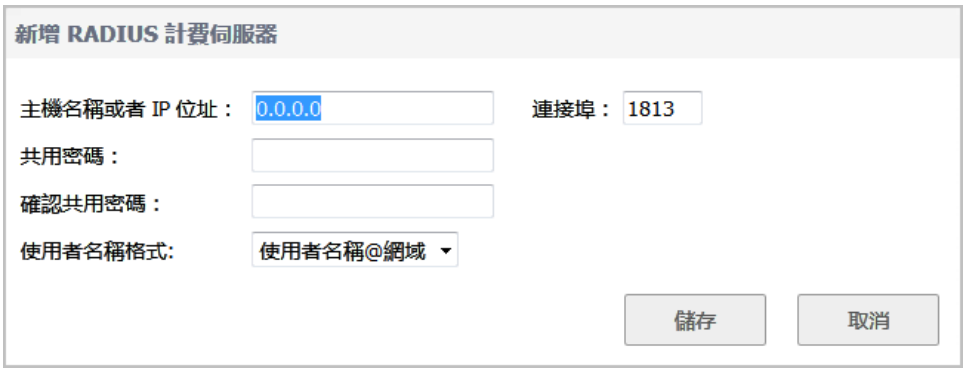
設定 RADIUS 設定

設定 RADIUS 設定的步驟如下：

1. 導覽到**管理 | 系統安裝 | 使用者 | 設定**。
2. 按一下**計費**。

3 若要在 SonicOS 中設定您的 RADIUS 伺服器設定，請按一下**傳送 RADIUS 計費資訊**。預設情況下未勾選此選項。 隨即顯示 **RADIUS 計費**與**使用者計費**區段。

4 在 **RADIUS 計費伺服器**表格中，按一下**新增**。隨即顯示**新增 RADIUS 計費伺服器**快顯。



5 在**主機名稱或 IP 位址**欄位中，輸入 IP 位址或主機名稱。預設值為 **0.0.0.0**。

6 在**連接埠**欄位中，輸入伺服器的連接埠。預設為 **1813**。

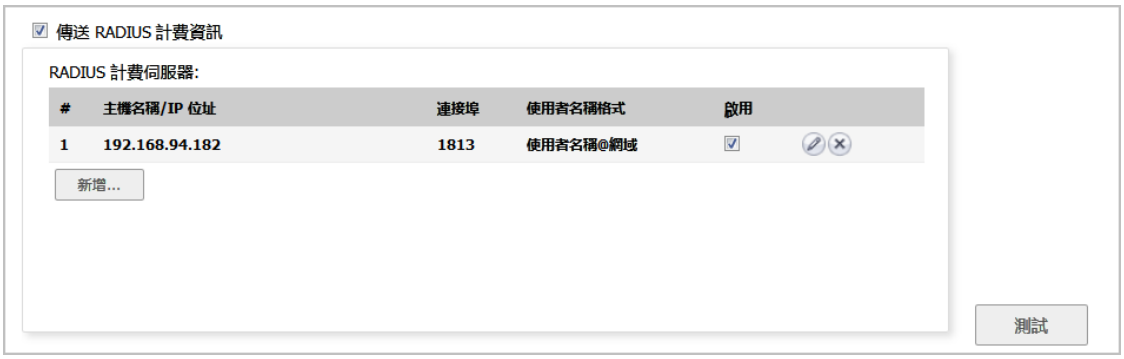
7 在**共用密碼**和**確認共用密碼**欄位中，輸入共用密碼。由英數字元組成的**共用密碼** (區分大小寫) 的長度範圍為 1 至 31 個字元。

8 從**使用者名稱格式**中選取使用者名稱的格式:

- **使用者名稱**
- **使用者名稱@網域** (預設)
- **網域\使用者名稱**
- **使用者名稱.網域**

9 按一下**儲存**。將顯示確認訊息。

10 按一下**確定**。伺服器即新增至 **RADIUS 計費伺服器**表格中。



11 在 **RADIUS 伺服器逾時 (秒)** 欄位中，輸入逾時值。允許的範圍為 1-60 秒，預設值為 **5**。檢閱者問題: 更好的定義。

12 在**重試次數**欄位中，輸入 SonicOS 將嘗試聯絡 RADIUS 伺服器的次數。如果在指定的重試次數內，RADIUS 伺服器未回應，則放棄連接。此欄位的允許範圍為 0 至 10，預設值為 **3** 次 RADIUS 伺服器重試。

13 若要將每個計費要求訊息傳送至所有設定的計費伺服器，或如果已使用驗證資料分割，要傳送至使用者分割區中的所有計費伺服器，請選取**將計費資料傳送至所有伺服器**。 預設情況下未勾選此選項。

14 若要設定與產生使用者計費資料相關的設定，請捲動至**使用者計費**區段。

15 選取一個或多個要傳送資料的使用者類型；依預設會選取「無」:

- **透過 Web 登入驗證的使用者**
- **遠端用戶端使用者**
- **訪客使用者**
- **SSO 驗證使用者**；後續選項會變成可用狀態
- **包含透過 RADIUS 計費識別的 SSO 使用者**

16 選擇要包含的使用者:

- **網域使用者** (預設)
- **本機使用者**
- **網域與本機使用者**

17 若要將臨時更新傳送給計費伺服器，請選取**傳送臨時更新**。 預設情況下未勾選此選項。

18 按一下**接受**。

19 若要測試已設定伺服器的存取權，請按一下**測試**。

RADIUS 使用者標籤

在 **RADIUS 使用者**標籤，您可以指定用於結合 RADIUS 身分驗證使用的本機或 LDAP 資訊的類型。您還可以定義 RADIUS 使用者的預設使用者群組。

若要設定 RADIUS 使用者設定：

1 按一下 **RADIUS 使用者**標籤。

2 如果只有 SonicOS 資料庫中列出的使用者使用 RADIUS 進行身分驗證，則選擇**僅允許本機列出的使用者**。

3 選擇**為 RADIUS 使用者設定使用者群組關係的方法**選項：

> **附註：**如果選擇**使用 RADIUS 伺服器上的 SonicWall 供應商特定屬性**或**在 RADIUS 伺服器上使用 RADIUS 篩選 ID 屬性**選項，必須正確設定 RADIUS 伺服器，以便在驗證使用者時將這些屬性傳回 SonicWall 裝置。RADIUS 伺服器應傳回零 (0) 或所選屬性的更多實例，每個實例都提供使用者所屬使用者群組的名稱。
> 如需供應商特定屬性設定的詳細資料，請參見技術說明，SonicOS Enhanced：使用「使用者級別身分驗證」以及 SonicOS Enhanced RADIUS Dictionary 檔案 `SonicWall.dct`。二者均位於 https://support.sonicwall.com/。

- **使用 RADIUS 伺服器上的 SonicWall 供應商特定屬性** - 套用在 RADIUS 伺服器上設定的供應商特定屬性。屬性必須提供使用者所屬的使用者群組。慣用的供應商特定 RADIUS 屬性為 `SonicWall-User-Group`。`SonicWall-User-Privilege` 也適用於某些使用者群組，但是受支援的主要原因是向後相容性，而且不受**為 RADIUS 使用者設定使用者群組關係的方法**設定支配；也就是說，即使選擇**使用 RADIUS 伺服器上的 SonicWall 供應商指定屬性**以外的選項，此屬性依然有效。
- **使用 RADIUS 伺服器上的 RADIUS 篩選 ID 屬性** - 套用在 RADIUS 伺服器上設定的篩選 ID 屬性。屬性必須提供使用者所屬的使用者群組。
- **使用 LDAP 以獲得使用者群組資訊**（預設）- 獲得來自 LDAP 伺服器的使用者群組。如果您未設定或需要進行變更，可以按一下**設定**按鈕設定 LDAP。如需設定 LDAP 的資訊，請參見第 133 頁「為 LDAP 設定 SonicWall」。
- **僅本機設定** - 如果您不計劃檢索來自 RADIUS 或 LDAP 的使用者群組資訊，則選擇此選項。
- **可以通過複製 RADIUS 使用者名稱在本機設定成員身分** - 對於管理 RADIUS 使用者群組的快捷方式。在本機安全裝置上建立有相同名稱的使用者和管理其群組成員身分時，RADIUS 資料庫中的成員身分將自動變更以反映您的本機變更。

4 如果您之前在 SonicOS 上設定了使用者群組，則從**所有 RADIUS 使用者所屬的預設使用者群組**下拉功能表中選擇群組。若要建立新的使用者群組，請參見第 132 頁「建立 RADIUS 使用者的新使用

者群組」。

5 可以：

- 按一下**確定**，如果已經完成設定 RADIUS 伺服器。
- 或者，按一下**套用**，繼續設定 RADIUS 使用者和/或測試設定。

建立 RADIUS 使用者的新使用者群組

在 **RADIUS 使用者設定**對話方塊中，您可以通過從**所有 RADIUS 使用者所屬的預設使用者群組**下拉功能表中選擇**建立新使用者群組...**來建立新群組：顯示新增群組對話方塊。如需建立新使用者群組，請參見第 201 頁「建立或編輯本機群組」。

使用 LDAP 設定使用者群組的 RADIUS

如果使用 RADIUS 進行使用者驗證，**RADIUS 使用者**標籤的 **RADIUS 設定**對話方塊中提供一個選項用於選擇 LDAP 作為設定 RADIUS 使用者群組成員身分的方法：

如果勾選**使用 LDAP 以獲得使用者群組資訊**，在通過 RADIUS 驗證使用者後，其使用者群組成員身分資訊將可以通過 LDAP 在 LDAP/AD 伺服器的目錄中查找。

附註：如果**未**選擇這種方法，且啟用了一次性密碼，RADIUS 使用者在嘗試通過 SSL VPN 登入時將收到一次性密碼失敗的訊息。

按一下**設定**對話方塊啟動 **LDAP 設定**視窗。如需設定 LDAP 設定的更多資訊，請參見第 78 頁「準備 LDAP 伺服器以進行整合」。

附註：在這種情況下，LDAP 未處理使用者密碼，且從目錄讀取的資訊通常無限制，所有如果沒有 TLS（例如 Active Directory 中未安裝憑證服務），可以選擇無 TLS 的操作，同時忽略警告。但是，必須確保 SonicOS 在明文登入 LDAP 伺服器（例如建立對 SonicOS 專用目錄具有唯讀存取權限的使用者帳戶）時不會有損安全性。在這種情況中，請勿使用管理員帳戶。

RADIUS 用戶端測試

在 **RADIUS 設定**對話方塊中，您可以通過輸入有效的使用者名稱和密碼和選擇一種**測試**用驗證方法來測試 RADIUS 用戶端使用者名稱、密碼和其他設定。執行測試將套用您所作的全部變更。

若要測試 RADIUS 設定：

1 按一下**測試**標籤。

2 在**使用者**欄位，輸入有效的 RADIUS 登入名稱。

3 在**密碼**欄位，輸入密碼。

4 為進行**測試**，選擇以下一種方法：

- **密碼驗證**：勾選此選項使用密碼進行身分驗證。
- **CHAP**：勾選此選項使用「質詢握手身分驗證通訊協定」。在初始驗證後，CHAP 通過使用三次握手定期驗證用戶端身分。
- **MSCHAP**：勾選此選項使用「Microsoft CHAP 實施」。MSCHAP 適用於 Windows Vista 之前的所有 Windows 版本。
- **MSCHAPv2**：勾選此選項使用「Microsoft 第 2 版 CHAP 實施」。MSCHAPv2 適用於 Windows 2000 及其後的 Windows 版本。

5 按一下**測試**按鈕。如果驗證成功，**狀態**訊息變更為**成功**。如果驗證失敗，**狀態**訊息變更為**失敗**。

6 若要完成 RADIUS 設定，按一下**確定**。

SonicOS 設定完成後，要求 RADIUS 身分驗證的 VPN 安全關聯提示接收 VPN 用戶端在對話方塊中輸入使用者名稱和密碼。

為 LDAP 設定 SonicWall

若要管理您的 LDAP 整合：

1 導覽到**使用者 | 設定**。

2 從**使用者驗證方法**中，選取 **LDAP** 或 **LDAP + 本機使用者**。

3 按一下**設定 LDAP**。

4 如果通過 HTTP 而不是 HTTPS 連接安全設備，訊息顯示將警告目錄服務中儲存的資訊的敏感性並提供變更 HTTPS 連接的途徑。如果對您連接的介面啟用了 HTTPS 管理（推薦），則按一下**是**。顯示 **LDAP 設定**對話方塊。

附註：動態學習的次要伺服器顯示為藍色，與設定的伺服器區別。

主題：

- 第 134 頁「設定」
- 第 135 頁「結構標籤」
- 第 136 頁「目錄標籤」
- 第 137 頁「提名標籤」
- 第 137 頁「使用者和群組標籤」
- 第 138 頁「LDAP 轉接」
- 第 139 頁「測試標籤」

設定

設定 LDAP 伺服器設定的步驟如下：

1 設定以下欄位：

- **名稱或者 IP 位址** - 您希望驗證的 LDAP 伺服器的 FQDN 或 IP 位址。如果使用名稱，請確保 DNS 伺服器可解析此名稱。另外，如果勾選「需要來自伺服器的有效憑證」選項使用 TLS，在此提供的名稱必須符合對其發佈了伺服器憑證的名稱（即 CN），否則 TLS 交換將失敗。
- **連接埠數目** - 預設的 LDAP over TLS 連接埠數目是 TCP 636。預設的 LDAP（未加密）連接埠數目是 TCP 389。如果使用 LDAP 伺服器上的自訂監聽連接埠，請在此指定。
- **伺服器逾時** - SonicOS 在逾時前等待來自 LDAP 伺服器的回應的秒數。範圍為 1 至 99999，預設為 **10** 秒。
- **全面操作逾時** - 任何自動操作所需的分鐘數。目錄設定或匯入使用者群組等操作可能需要數分鐘，尤其是在使用多個 LDAP 伺服器時。
- 選擇以下一個選項按鈕:
  - **匿名登入** - 有些 LDAP 伺服器允許匿名存取樹狀目錄。如果伺服器支援匿名存取（Active Directory 一般不支援），您可以選擇此選項。
  - **在樹狀目錄中提供使用者名稱/位置** - 選擇此選項構建識別名稱 (dn) 用於根據以下規則從登入使用者名稱和用於登入伺服器的使用者樹狀目錄欄位繫結到 LDAP 伺服器：
    - 第一個名稱元件以 `cn=` 開頭
    - 「樹狀目錄中的位置」元件都是用 `ou=`（以 `cn=` 開頭的某些 Active Directory 內建元件除外）
    - 網域元件都是用 `dc=`
    - 如果「用於登入伺服器的使用者樹狀目錄」欄位指定為 `dn`，且繫結 dn 符合以上第一項，但不符合第二和/或第三項，您還可以選擇此選項。
  - **提供繫結辨別名稱** - 如果繫結 dn 不符合以上第一項（如果第一個名稱元件不是以 `cn=` 開頭）。如果 dn 已知，則始終可以選擇此選項。如果繫結 dn 不符合以上第一項，您必須明確提供繫結 dn。
- **登入使用者名稱** - 指定有權限登入 LDAP 目錄的使用者名稱。在完整的'dn'表示法中，登入名稱將自動向 LDAP 伺服器顯示。這可以是具有 LDAP 讀取權限的所有帳戶（基本所有）；並不需要管理權限。

  ⓘ **附註：**這是使用者的姓名，不是其登入 ID（例如 John Smith，而不是 jsmith）。

- **登入密碼** - 以上指定的使用者帳戶的密碼。
- **通訊協定版本** - 選擇 LDAPv3 或 LDAPv2。大多數先進的 LDAP 實施（包括 Active Directory）都採用 LDAPv3。
- **使用 TLS (SSL)** - 使用傳送層安全性 (SSL) 登入 LDAP 伺服器。強烈建議使用 TLS 防護將通過網路傳送的使用者名稱和密碼資訊。大多數先進的 LDAP 伺服器實施（包括 Active Directory）都支援 TLS。取消勾選此預設值將顯示一條警示，您必須接受此警示才能繼續。
- **傳輸 LDAP '開始 TLS' 請求** - 有些 LDAP 伺服器實施支援「啟動 TLS」指令，而不是使用原生 LDAP over TLS。這允許 LDAP 伺服器監聽 LDAP 連接的一個連接埠（通常是 389）以及切換

到用戶端指示的 TLS。Active Directory 不使用此選項，且只有在 LDAP 伺服器要求時才選擇此選項。

- **需要來自伺服器的有效的憑證** - 在 TLS 交換期間驗證伺服器提供的憑證，將以上指定的名稱與憑證上的名稱相符合。取消選擇此預設選項將顯示一條警示，但 SonicOS 和 LDAP 伺服器之間的資訊交換仍使用 TLS，只是沒有驗證發佈。
- **本機用於 TLS 的憑證** - 只有在 LDAP 伺服器需要用戶端憑證進行連接時，可以選擇性使用。此功能對於返回密碼以確保 LDAP 用戶端身分的 LDAP 伺服器實施很有用（Active Directory 不返回密碼）。Active Directory 不需要這項設定。

  如果您的網路使用有提名的多個 LDAP/AD 伺服器，則選擇一個作為主要伺服器（可能是擁有大量使用者的伺服器），並對此伺服器使用以上設定。此伺服器將參考其他伺服器上的 SonicOS 獲得自己網域以外的網域使用者的資訊。為了使 SonicOS 能夠登入其他伺服器，各伺服器必須具有與主要伺服器相同的使用者設定登入憑證（使用者名稱、密碼和在目錄中的位置）。這可能需要在用於 SonicOS 登入的目錄中建立一個特殊使用者。注意只需要對此目錄的唯讀存取權限。
- **強制 PAP 至 MSCHAPv2** - 可選，如需強制 MS-CHAPv2 LDAP 驗證，則選擇此選項。如果還設定了 RADIUS 伺服器，則此伺服器將在 LDAP 驗證失敗時提供驗證。預設情況下未勾選此選項。

2 按一下**套用**。

結構標籤

設定 LDAP 伺服器結構設定的步驟如下：

1 按一下**結構**標籤。

2 **LDAP 結構** - 從 **LDAP 結構**下拉功能表中選擇以下選項之一：

> **附註：**選擇任意預先定義的結構將自動使用正確值填寫此結構使用的欄位。這些值無法進行變更且其欄位為灰色。

- **Microsoft Active Directory**
- **RFC2798 inetOrgPerson**
- **RFC2307 網路資訊服務**
- **Samba SMB**
- **Novell eDirectory**
- **使用者定義** - 將允許指定您自己的值，請只在有特定或專有的 LDAP 結構設定時才使用此選項。

3 **物件類別** - 選擇能夠反映以下兩個欄位所套用的各使用者帳戶的屬性。

4 **登入名稱屬性** - 選擇以下一項定義用於登入驗證的屬性：

- 用於 **Active Directory 的 sAMAccountName**
- 用於 RFC2798 inetOrgPerson 的 **inetOrgPerson**
- 用於 RFC2307 網路資訊服務的 **posixAccount**
- 用於 Samba SMB 的 **sambaSAMAccount**
- 用於 Novell eDirectory 的 **inetOrgPerson**

5 **有資格的登入名稱屬性** - 可以選擇使用者物件的屬性以 name@domain 格式設定備選的登入名稱（可選）。這尤其可用於有多個網域的情況，其中，簡單的登入名稱可能在多個網域中不唯一。

> **附註：**對於 **Microsoft Active Directory**，通常使用 name@domain 將其設定為用於登入的 **userPrinicpalName**，但也可將其設定為**郵件**以通過電子郵件地址啟用登入。對於 **RFC2798 inetOrgPerson**，將其設定為**郵件**。

6 **使用者群組成員資格功能** - 選擇包含有關使用者物件所屬群組的資訊的屬性。這是 Microsoft Active Directory 中的**隸屬於**屬性。其他預先定義的方案儲存群組物件中的群組成員資訊，而不是使用者物件，因此不使用此欄位。

7 **帶框架的 IP 位址屬性** - 選擇可用於檢索指派到目錄中使用者的固定 IP 位址的屬性。目前，這僅用於通過 L2TP 使用 SonicOS L2TP 伺服器的使用者連接。以後可能支援用於 Global VPN Client。在 Active Directory 中，固定 IP 位址在使用者屬性的「撥號」標籤中設定。

8 **使用者群組物件** - 這部分自動設定，除非您為 **LDAP 結構**選擇了**使用者定義**。

- **物件類別** - 指定屬性組的相關名稱。
- **成員功能** - 指定成員的相關屬性。
  - 選擇此屬性是**識別名稱**或**使用者 ID**。
- **從伺服器讀取** - 按一下從 LDAP 伺服器讀取使用者群組物件資訊。

  > **附註：**必須先在**目錄**標籤中輸入主要網域。

  - 選擇您是否要**自動更新結構描述設定**或**匯出結構描述的詳細資料**。

目錄標籤

設定 LDAP 伺服器目錄設定的步驟如下：

1 在**目錄**標籤中，設定以下欄位：

- **主要網域** - LDAP 實施使用的使用者網域。對於 AD，這是 Active Directory 網域名稱，例如 *yourADdomain.com*。可以選擇將對此欄位的變更自動更新到頁面其餘的樹狀目錄資訊。將所有結構預設設為 **mydomain.com**，但 Novell eDirectory 除外，並設為 **o=mydomain**。
- **用於登入伺服器的樹狀目錄** - 在**設定**標籤中指定的使用者所在的樹狀目錄。例如，在 Active Directory 中，「管理員」帳戶的預設樹狀目錄與使用者樹狀目錄相同。
- **包含使用者的樹狀目錄** - 使用者在 LDAP 目錄中通常所在的樹狀目錄。可以編輯提供的預設值，最多共可以提供 64 個 DN 值。SonicOS 將使用全部值搜尋目錄直至找到符合項，否則將查找完整個清單。如果您在 LDAP 或 AD 目錄中建立了其他使用者容器，應在此說明。
- **包含使用者群組的樹狀目錄** - 和上面一樣，但針對使用者群組容器，最多可以提供 32 個 DN 值。這僅適用於結構的使用者物件中沒有使用者群組成員身分屬性，且不使用 AD 的情況。
- 以上所述的樹狀目錄通常具有 URL 格式，但可以另外指定為識別名稱（例如 myDom.com/Sales/Users 可另外指定為 DN ou=Users,ou=Sales,dc=myDom,dc=com）。如果在此例中，DN 不符合正常的格式規則，以上第二種形式則是必需的。在 Active Directory 中，樹狀目錄頂部的容器屬性的「物件」標籤中顯示對應於樹狀目錄識別名稱的 URL。

  > **附註：**AD 有一些不符合以上所述的內建容器（例如頂層使用者容器的 DN 格式為 cn=Users,dc=…，其中使用 cn 而不是 ou），但 SonicOS 知道此情況以及任何處理它們，所以可以使用較簡單的 URL 格式輸入。

排序並不重要，但是由於以既定順序搜尋，所以將最常用的樹狀目錄放在各清單的前面是最高效的做法。如果要使用多個 LDAP 伺服器之間的提名，最好的排序是將位於主要伺服器上的樹狀目錄放在前面，其餘樹狀目錄以提名順序排列。

附註：在使用 AD 時，要為**用於登入伺服器的樹狀目錄**欄位確定使用者在目錄中的位置，可以從伺服器上的 Active Directory 使用者和設定控制面板手動搜尋目錄，或者從網域中的任意 PC 執行 Windows NT/2000/XP 資源套件中的 queryad.vbs 等目錄搜尋實用程式。

- **自動設定** - 這使 SonicOS 通過掃描一個或多個目錄查找包含使用者物件的所有樹狀目錄來自動設定**包含使用者的樹狀目錄**和**包含使用者群組的樹狀目錄**欄位。若要使用自動設定，首先在**用於登入伺服器的樹狀目錄**欄位輸入值（除非設定了匿名登入），然後按一下**自動設定**按鈕顯示以下視窗：

    a) 在**自動設定**對話方塊中，在**要搜尋的網域**欄位輸入所需的網域。

    b) 選擇以下一項：

    - **附加到現有樹狀目錄** - 這項選擇將新找到的樹狀目錄附加到目前設定。
    - **取代現有樹狀目錄** - 這項選擇將首先從頭開始移除所有目前設定的樹狀目錄。

2 按一下**確定**。

自動設定過程還可能查找使用者登入不需要的樹狀目錄。您可以手動移除這些項目。

如果使用有提名的多個 LDAP/AD 伺服器，可以對每個伺服器重複此過程，相應地替換**要搜尋的網域值**，並對隨後的各執行選擇**附加到現有樹狀目錄**。

提名標籤

設定 LDAP 伺服器提名設定的步驟如下：

1 按一下**提名**標籤。

2 設定以下欄位：

- **允許轉介** - 如果使用者資訊位於 LDAP 伺服器上，而不是設定的主要伺服器上，則選擇此選項。
- **在使用者驗證過程中允許連續的參考** - 如果手動設定了各目錄樹狀目錄以涵蓋多個 LDAP 伺服器，則選擇此選項。
- **在目錄自動設定的過程總允許連續的參考** - 選擇此選項允許在單個操作中從多個 LDAP 伺服器讀取樹狀目錄。
- **允許在網域搜尋中連續的參考** - 在有使用者位於包含單獨 LDAP 伺服器的多個子網路域的情況下使用單點登入時，選擇此選項。

使用者和群組標籤

設定 LDAP 使用者和群組設定的步驟如下：

1 按一下**使用者和群組**標籤。

2 設定以下欄位：

- **僅允許本機列出的使用者** - 要求 LDAP 使用者還必須存在於 SonicOS 本機使用者資料庫中才能允許登入。

- **可以通過複製 LDAP 使用者名稱在本機設定使用者群組成員** - 允許通過本機使用者與 LDAP 使用者設定的交集確定群組成員身分（和權限）。
- **預設 LDAP 使用者群組** - SonicOS 上 LDAP 使用者所屬的預設群組和在 LDAP 伺服器上設定的群組成員身分。
- **匯入使用者** - 您可以按一下此按鈕通過檢索 LDAP 伺服器中的使用者名稱設定 SonicOS 上的本機使用者。**匯入使用者**按鈕將打開對話方塊，其中包含可匯入的使用者名稱的清單。

  在「LDAP 匯入使用者」對話方塊中，勾選您要將其匯入 SonicOS 的各使用者的核取方塊，然後按一下**儲存勾選**。

  從 LDAP 伺服器讀取的使用者清單可能很長，您可能不想全部匯入。清單中提供了**從清單刪除**按鈕及其他多種移除不需要使用者的方法。您可以使用這些選項將清單縮短到便於管理的大小，然後選擇要匯入的使用者。

  SonicOS 上的使用者名稱與現有 LDAP 使用者名稱相同有利於在 LDAP 身分驗證成功後授予 SonicWall 使用者權限。
- **匯入使用者群組** - 您可以按一下此按鈕通過檢索 LDAP 伺服器中的使用者群組名稱設定 SonicOS 上的使用者群組。**匯入使用者群組**按鈕將打開對話方塊，其中包含可匯入到安全設備的使用者群組名稱的清單。

  在 LDAP 匯入使用者群組對話方塊中，勾選您要將其匯入 SonicOS 的各群組的核取方塊，然後按一下**儲存勾選**。

  SonicOS 上的使用者群組與現有 LDAP/AD 使用者群組的名稱相同有利於在成功 LDAP 身分驗證後授予 SonicWall 群組成員身分和權限。

  另外，您也可以在 LDAP/AD 伺服器上手動建立與 SonicWall 內建群組名稱相同的使用者群組（例如「來賓服務」、「內容篩選繞過」、「有限管理員」），並將使用者指派到目錄中的這些群組。這還允許在成功 LDAP 身分驗證後授予 SonicWall 群組成員身分。

  就 Active Directory 來說，安全設備可以利用為使用者傳回「memberOf」屬性的獨特優勢，更有效率地擷取群組成員資格。

LDAP 轉接

設定 LDAP 伺服器轉接設定的步驟如下：

1 按一下 **LDAP 轉接**標籤。

「RADIUS 至 LDAP 轉接」功能旨在用於拓撲，其中有包含 LDAP/AD 伺服器的中央站台，以及透過可能不支援 LDAP 之低端安全設備與其連接的中央 SonicWall。在這種情況下，中央 SonicWall 可以作為遠端 SonicWall 的 RADIUS 伺服器執行，充當 RADIUS 和 LDAP 之間的閘道，並將自身的身分驗證請求中移至 LDAP 伺服器。

2 設定以下欄位：

- **啟用 RADIUS 到 LDAP 轉接** - 啟用此功能。
- **允許 RADIUS 用戶端連接透過** - 勾選相關的核取方塊，將新增原則規則以相應允許收到的 RADIUS 請求。
- **RADIUS 共用密碼** - 這是所有遠端 SonicWall 共用的共用密碼。
- **用於舊版 VPN 使用者的使用者群組** - 定義「存取 VPN」舊權限對應的使用者群組。此使用者群組中的使用者進行身分驗證時，會通知遠端 SonicWall 賦予此使用者相應的權限。

- **用於舊版 VPN 用戶端使用者的使用者群組** - 定義「通過 XAUTH 從 VPN 用戶端存取」舊權限對應的使用者群組。此使用者群組中的使用者進行身分驗證時，會通知遠端 SonicWall 賦予此使用者相應的權限。
- **用於舊版 L2TP 使用者的使用者群組** - 定義「從 L2TP VPN 用戶端存取」舊權限對應的使用者群組。此使用者群組中的使用者進行身分驗證時，會通知遠端 SonicWall 賦予此使用者相應的權限。
- **用於舊版使用者的群組網際網路存取** - 定義「允許網際網路存取權限（當存取受限時）」舊權限對應的使用者群組。此使用者群組中的使用者進行身分驗證時，會通知遠端 SonicWall 賦予此使用者相應的權限。

附註：根據成員身分向名稱為「內容篩選繞過」和「有限管理員」的使用者群組返回「繞過篩選條件」和「有限管理能力」權限，這些設定不可設定。

測試標籤

設定 LDAP 伺服器測試設定的步驟如下：

1 選擇**測試**標籤測試設定的 LDAP 設定：

測試 LDAP 設定頁面允許通過使用指定的使用者和密碼登入憑證嘗試身分驗證來測試設定的 LDAP 設定。顯示為此使用者在 LDAP/AD 伺服器上設定的所有使用者群組成員身分和/或成框架 IP 位址。

關於多個 LDAP 伺服器的延伸支援

可設定多個主要 LDAP 伺服器，每個驗證分割區有一個伺服器，還有一個額外伺服器的清單。每個主要 LDAP 伺服器依照目前的 LDAP 伺服器進行設定。對於其他伺服器，雖然設定是最基本的 (來自主要伺服器的一般設定)，但包含登入 (繫結) 憑證與伺服器控制的子網域。

附註：Active Directory 具有 LDAP 伺服器與網域的 1:1 對應，其他 LDAP 伺服器可能不會有這種情況。具有 1:1 對應時，為每個 LDAP 伺服器設定網域會使得伺服器的選項變得更有效率，但如果不是這種情況，則選項的效率較低。

可依伺服器單獨設定的設定即為目前在管理介面的**系統安裝 | 使用者 | 設定 > 設定 LDAP** 對話方塊中的設定。如需關於設定 LDAP 的詳細資訊，請參閱第 133 頁「為 LDAP 設定 SonicWall」。

重要：為了正確操作，分割區中的所有 LDAP 伺服器必須設為相同架構。如果不是這樣，會發出警告。

轉介設定是全域設定的，在所有驗證分割區中的所有 LDAP 伺服器上是通用的。

附註：明確設定次要伺服器是可選的。每個主要與次要伺服器皆可單獨設定，或者使用可透過轉介存取的所有使用者/群組樹狀目錄來設定主要伺服器。

主題：

- 第 140 頁「關於設定次要伺服器」
- 第 140 頁「關於動態學習次要伺服器」
- 第 140 頁「關於備份伺服器」

關於設定次要伺服器

除了主要/次要設定以外，建立/設定永久次要伺服器與主要伺服器相同。它們之間在功能方面的唯一區別在於，進行搜尋時，如果無法從設定的使用者/群組樹狀目錄中得之位置，會將搜尋傳送到主要伺服器，視需要在次要伺服器上傳遞搜尋時，會使用傳送參照/轉介的主要伺服器。

關於動態學習次要伺服器

第一次透過轉介或參照存取次要伺服器時，安全設備可能會在根據各種設定的使用者樹狀目錄嘗試多個繫結網域名稱 (DN) 之後，繫結至次要伺服器。安全設備會針對次要伺服器內部建立一個記錄，安全設備會將繫結資訊儲存在該記錄中，以供未來使用。此處理程序包含未設定的次要伺服器，進而建立一個動態伺服器物件，該伺服器物件與設定之伺服器的伺服器物件一起保存在內部。

這些動態學習的伺服器物件允許依照設定的伺服器儲存其他資訊，以及目前的繫結資訊此資訊包含伺服器學習的使用者/群組樹狀目錄，以及該物件的統計資料。

附註：這些資訊在重新啟動期間不是持續性的，必要時會重新學習。不過，會利用主要伺服器儲存動態次要伺服器之使用者/群組樹狀目錄的設定。

關於備份伺服器

Active Directory 支援備份伺服器，透過 DNS 名稱系統實作備份。Active Directory 網域控制器是透過機器的 DNS 名稱或網域存取；在後者情況下，網域名稱會針對所有網域控制器複本的 IP 位址清單進行解析。當 LDAP 伺服器 DNS 名稱針對 IP 位址清單進行解析時，SonicWall 安全設備會逐一嘗試每個位址，直到出現任一回應為止。因此，將 LDAP 伺服器 DNS 名稱設定為主要網域名稱而非網域控制器機器名稱會導致冗餘，而如果主要伺服器沒有回應，則會使用備份服務器。

此機制在 Active Directory 中也適用於轉介和參照，因為它會將轉介中的次要網域 DNS 名稱傳回網域。

附註：在 Active Directory 中，備份服務器通常稱為複本伺服器。

可為每個設定的主要或次要 LDAP 伺服器設定一個或多個備份。此設定可記錄每個個別伺服器的狀態與統計資料，並透過非 Active Directory 安裝中的備份伺服器支援冗餘 (上述 DNS 名稱機制不提供此類支援)。

備份伺服器僅具備為其他伺服器設定的一部分設定，因為大部分設定與其備份的伺服器完全相同。依預設，只需要備份伺服器的主機名稱或 IP 位址。

關於從 LDAP 匯入和鏡像

若要在啟用 LDAP 使用者群組鏡像時，建立與 LDAP 目錄中的使用者群組形成鏡像的本機使用者群組，SonicWall 安全設備會定期自動從 LDAP 伺服器匯入使用者群組和使用者群組巢狀 (屬於其他群組成員的群組成員資格)

您可以在任何可選取一般使用者群組的位置選取鏡像使用者群組，例如，在存取規則和 CFS 原則中。儘管鏡像使用者群組可以成為其他本機使用者群組的成員，且本機使用者可成為其成員，但鏡像使用者群組確實有一些限制，例如，他們無法在 SonicWall 安全設備上，以本機方式新增其他使用者群組作為成員。LDAP 伺服器上為使用者群組成員的使用者會通過其本機鏡像群組自動接收任何存取權限。

主題：

- 第 141 頁「使用者匯入」
- 第 141 頁「使用者群組匯入與鏡像」

使用者匯入

從 **LDAP 設定**對話方塊或**系統安裝 | 使用者 | 本機使用者與群組**頁面匯入使用者時，可選擇指定要從何處匯入 LDAP 伺服器:

- 單一特定 LDAP 伺服器
- 驗證分割區中的所有伺服器 (啟用後者時)
- 所有 LDAP 伺服器

為了能夠區分從不同 LDAP 伺服器上不同網域中匯入的使用者 (這些使用者可能具有相同的使用者名稱)，也可以選擇使用包含該網域的其中一個完整使用者名稱格式來建立本機使用者物件。這是使用簡單使用者名稱以外的選項。

如果已使用其中一個完整使用者名稱格式匯入使用者帳戶，則:

- 對於使用該帳戶的 Web 或用戶端，完整使用者名稱必須與匯入的名稱完全一致。
- 透過 SSO 識別使用者時，由於名稱格式視 SSO 來源而有所不同，因此，使用者名稱與網域元件會對照使用者物件的使用者名稱與網域元件分別進行比對。例如，如果針對 `jdoe@mydomain.com` 從 LDAP 匯入使用者，而且 SSO 代理報告 `MYDOMAIN/jdoe`，這些會進行比對，而且該使用者帳戶會用來設定該使用者的其他群組成員資格。因此，對於 SSO 而言，選取完整的名稱格式並不重要，該選擇主要是為了顯示偏好。

  附註：只有在**系統安裝 | 使用者 | 設定**中已設定**使用 LDAP 以擷取使用者群組資訊**或**僅允許本機列出的使用者**選項時，才適用此選項。如需詳細資訊，請參閱第 133 頁「為 LDAP 設定 SonicWall」和第 142 頁「設定 SonicOS 以使用 SonicWall SSO 代理」。

使用者群組匯入與鏡像

使用驗證分割區時，分割區中的使用者必須取得為從該分割區匯入之使用者群組所設定的存取權限，而不是從其他分割區匯入之相同名稱群組使用者的存取權限。

例如，已匯入/已鏡像使用者群組會用於原則中，藉由比對原則中的群組名稱與使用者登入時從 LDAP 讀取的群組名稱，以選取適用的使用者群組。已匯入和已鏡像使用者群組的運作方式稍有不同 (主要是基於歷史原因):

- 手動匯入使用者群組時，會使用不含網域元件之簡單的群組名稱建立本機使用者群組物件。接著，當使用者群組成員資合與本機群組名稱進行比對時，只會比對簡單的群組名稱，而忽略任何網域元件。因此，在不同網域中具有相同名稱的使用者群組中，任何網域的使用者會取得為本機群組設定的成員資格。
- 當 LDAP 使用者群組鏡像對群組鏡像時，會使用該名稱 `group-name@domain.com` 建立本機使用者群組物件，以區別從不同網域鏡像的群組。然後，從 LDAP 讀取使用者的群組成員資格時，會將它們置於相同的格式中，並比較完整的群組名稱 (包括網域元件)。在不同網域中具有相同名稱的使用者群組中，網域的使用者只會取得從自己的網域鏡像的群組成員資格。

手動匯入的使用者群組也可以選擇匯入符合資格的群組名稱，以便依照上述的鏡像群組使用這些群組，為每個網域的使用者分別設定成員資格。從**系統安裝 | 使用者 | 設定 > 設定 LDAP** 對話方塊或**使用者 | 本機使用者與群組**頁面啟動匯入群組時，該對話方塊具有與使用者相同的選項，只是該格式的唯一選擇是**簡單名稱**或 **name@domain.com** (預設)。

附註：已匯入/已鏡像的使用者群組不需要明確的驗證分割區記錄/檢查，因為比對網域元件可隱含地確保僅選取使用者分割區中的網域的群組。

為了實現回溯相容性，以及為了方便不同分割區中標準群組的成員設定一般存取權，如果使用者群組是利用簡單名稱從 LDAP 匯入 (或手動建立)，則比對該群組時會忽略網域；因此，可以使用簡單名稱為任何網域/分割區中的使用者設定存取權限。

例如，如果您有:

- 分割區 A: `domain dom_a.com`
- 分割區 B: `domain dom_b.com`

然後從兩個分割區匯入管理員群組，選取匯入為 **name@domain.com**，您可以匯入本機使用者群組 `Administrators@dom_a.com` 和 `Administrators@dom_b.com`。每個分割區中的使用者只會收到為相關群組設定的存取權限；意即:

- 當分割區 A 的管理使用者登入時，而且 LDAP 查詢發現他們屬於 `dom_a.com` 中管理員群組的成員，則會為這些使用者提供 `Administrators@dom_a.com` 中的成員資格。
- 同樣地，當分割區 B 的管理使用者登入時，會收到 `Administrators@dom_b.com` 中的成員資格。

不過，如果您利用簡單名稱從任一網域匯入管理員群組，會取得名稱為管理員的本機使用者群組，而任一分割區中的管理使用者會取得為該群組設定的任何存取權限。

鏡像是全域啟用的。啟用時，會從所有設定和學習的 LDAP 伺服器鏡像使用者群組。

附註：可使用排除功能與萬用字元，來排除伺服器上的所有群組。

關於增強的 LDAP 測試

在 LDAP 測試中，您可以選取要測試的 LDAP 伺服器，而且除了目前的使用者驗證測試之外，您還可以新增連線和搜尋測試。請參閱 LDAP 測試表格。

LDAP 測試

測試	功能
連線/繫結	僅嘗試使用設定的繫結憑證來繫結至 LDAP 伺服器。
使用者驗證	測試可傳送給定的使用者名稱和密碼，並由 LDAP 伺服器驗證。
LDAP 搜尋	具有基本與進階模式: **基本模式**搜尋: • 具有指定登入名稱、合格登入名稱或一般名稱的使用者 • 具有指定名稱或成員的使用者群組 **進階模式**允許: • 明確的搜尋篩選條件 • 或者，變更搜尋基礎與範圍 (預設為從網域子樹狀目錄搜尋，其範圍為搜尋整個子樹狀目錄) • 搜尋多個物件 • 限制傳回的資訊

設定 SonicOS 以使用 SonicWall SSO 代理

若要設定您的安全設備以使用 SonicWall SSO 代理:

1 移至**使用者 | 設定**。

2 在**單一登入方法**部分，選擇 **SSO 代理**。使用此選擇新增和設定 TSA 以及用於 SSO 方法的 SSO 代理。

3 按一下**設定 SSO**。隨即顯示 **SSO 驗證設定**對話方塊。

主題：

SSO 代理標籤

在 **SSO 代理**標籤的**驗證代理設定**下，可查看已設定的任何 SSO 代理：

- 代理 IP 位址旁邊的綠色 LED 表示代理目前已啟動，正在執行。
- 紅色 LED 表示代理已關閉。
- 灰色 LED 表示代理已停用。

LED 通過使用 AJAX 動態更新。

1 按一下**新增**按鈕建立代理。頁面將更新，在表格頂部顯示新行，在頁面的下半部分顯示兩個新標籤（**設定**和**進階**）。

ⓘ **提示：**可以按一下任意項目以進行變更。按一下後此項目會變成可編輯欄位。

2 在**設定**標籤中輸入以下資訊：在輸入欄位值時，將頂部的行更新為紅色，以高亮顯示新資訊。

- 對於**主機名稱或者 IP 位址**，輸入安裝 SonicWall SSO 代理的工作站的名稱或 IP 位址。預設情況下，輸入 **0.0.0.0**。
- 在**連接埠**中，輸入 SonicWall SSO 代理用於與裝置通訊的連接埠數目。預設連接埠號是 **2258**。

  ⓘ **附註：**不同 IP 位址的代理可以有相同的連接埠數目。

- 在**共用密碼**中，輸入您在 SonicWall SSO 代理中建立或產生的共用密碼。共用密碼必須完全符合。在**確認共用密碼**欄位中重新輸入共用密碼。
- 在**逾時（秒）**中，輸入身分驗證嘗試逾時的秒數。此欄位自動填寫為預設值 **10** 秒。
- 在**重試次數**中，輸入身分驗證的嘗試次數。預設為 **6**。

3 按一下**進階**標籤。

4 在**一次傳送的最大請求數目**中，輸入裝置向代理一次傳送的最大同步請求數。預設為 **32**。

代理同時處理多個請求，並在代理 PC 中產生各單獨的執行緒進而分別處理。驗證代理可以處理的同步請求數取決於執行它的電腦以及網路的效能水平。提升此設定可以使 SSO 使用者驗證更加高效，但是將其設定過高可能會因為同時傳送太多請求，因此使電腦過載且導致逾時和驗證失敗，而使代理舉步維艱。

但是，如果裝置同時傳送的請求數太少，有些請求將需要等待，從而可能導致環形緩衝區溢出。太多等待中的請求會導致單點登入身分驗證中的回應變慢。如果在不獲得大量逾時的情況下，無法將此設定提升足夠高以避免環形緩衝區警告，請考慮將代理移到更高效能的專用電腦上，或者可以增加額外的代理。關於檢查 SonicOS TSR 中環形緩衝區溢出和相關統計資料的更多資訊，請參見第 99 頁「單點登入進階功能」。

ⓘ **提示：**查看「技術支援報告」的**單點登入驗證**部分的統計資訊。如果顯示大量逾時，降低此值可能有幫助。如果**在環形緩衝區花費的最長時間**達到或超過輪詢比率（在**使用者**標籤上設定），或者如果顯示任何環形緩衝區溢出，則可能應該提高此值。

5 按一下**一般設定**標籤下的**驗證代理設定**。

6 設定以下選項：

- 選擇**啟用 SSO 代理驗證**核取方塊使用 SSO 代理進行使用者身分驗證。預設情況下已選擇此設定。
- 勾選**無法從 NetAPI/WMI 獲取名稱時嘗試下一個代理**核取方塊在第一個代理無回應或出錯時，強制通過另一個 SSO 代理重新嘗試身分驗證。預設情況下未勾選此設定。

  附註：此設定僅影響使用 NetAPI/WMI 的代理，不會影響只使用網域控制器安全日志查詢機制的代理。

  重要：另請參見**使用者**標籤上的**輪詢驗證使用者的同一個代理**設定，如果啟用了此設定，則還需要設定這個設定。

  SSO 代理用於識別使用者的 NetAPI/WMI 協定由 Windows 提供，這些通訊協定的實際行為不受代理或裝置的控制。在使用 NetAPI 或 WMI 時，如果 Windows 對來自代理的請求作出無使用者名稱、無錯誤的回應，則預設情況下，裝置認為其他代理會收到同樣的回應且不會通過另一代理重試此請求（如果收到錯誤回應就會這麼做）。

  如果在您認為使用者應該已經識別時看到驗證失敗的記錄為 `SSO agent returned no user name`，請嘗試啟用此設定。如果啟用此設定，則在收到來自代理的無使用者名稱的回應時，裝置將把此回應視為錯誤且通過其他代理重試此請求。

  通常在只有部分代理能識別指定使用者時需要啟用此設定，例如，如果遠端站台的使用者無法為中心站台的代理所輕鬆識別，則有必要在遠端站台放置代理以識別那裡的使用者。

- 勾選**等待 SSO 時不封鎖使用者流量**核取方塊在識別使用者時使用預設原則。這可以防止瀏覽延遲。預設情況下未勾選此設定。

  當正在通過 SSO 識別使用者時，在識別完成之前通常會封鎖來自此使用者的流量，以便可以在適當的時候套用正確的原則。然而，有時候 SSO 代理會花費很長時間來識別使用者，這種延遲會導致使用者體驗到瀏覽延遲。

  此設定可以掩蓋此延遲，在等待 SSO 時允許使用者流量，且在識別完成之前套用預設原則。

  您還可以選擇當某個需要使用者身分驗證的存取規則要求識別使用者（也就是，如果未能識別使用者，則不允許此使用者的任何存取）時是否允許流量。

注意：在進行此設定時請小心，因為可能會臨時允許識別為不允許的使用者。如果對勾選的存取規則選擇此設定，則在那些需要使用者身分驗證的規則的進階設定部分會出現針對此選項的設定。

- 勾選**包括**核取方塊和**所有存取規則**（預設）或**選定的存取規則**選項按鈕允許在等待使用者識別時，要求使用者驗證的存取規則影響流量。

注意：這將暫時允許存取，而如果已識別使用者則可能不允許此類存取。

- 若要讓所有 SSO 代理同步它們的使用者資料庫，請選擇：
  - **同步所有代理** - 不論它們使用的是什麼識別機制，都一起同步，因此在每個代理上提供一個重複的同類使用者資料庫。
  - **將相同使用者識別機制的代理同步** - 僅同步那些使用相同識別機制的資料庫；此為預設值。

  每個 SSO 代理維護它自己的已識別使用者的資料庫，且可以有選擇地設定代理同步它們的資料庫，以便在每個代理上提供公用的重複使用者資料庫。公用的同步使用者資料庫可使使用者查詢更高效且提供更佳冗餘。通過在此處指定同步，裝置可以通知每個代理要同步的其他代理，因此避免不得不在代理中進行設定的複雜性。

預設情況下，裝置使這些代理設定為使用相同的使用者識別機制一起同步。例如，如果某些代理正在讀取網域控制器記錄，而其他代理使用 NetAPI，則兩組代理中的兩個獨立的外部資料庫會導致，網域控制器記錄中發現的那些使用者一個資料庫和 NetAPI 識別的那些使用者一個資料庫。

附註：可以通過在每個 SSO 代理中顯見地設定要同步的其他代理的清單來覆寫此設定。

- 在 **Windows 服務使用的使用者名稱**表中設定 Windows 服務使用者名稱清單。可以列出最多 64 個使用者名稱最終使用者電腦上的服務所使用；使用這些使用者名稱的登入均會視為服務登入且受到 SSO 代理的忽略。

  a) 按一下**新增**按鈕，將顯示**服務使用者名稱**對話方塊。

  b) 輸入服務使用者名稱。

  c) 按一下**確定**。

  d) 對每個使用者帳戶重複步驟 a 至步驟 c。

  Windows 服務使用使用者帳戶登入電腦或網域，就像真正的使用者那樣。SSO 代理所使用的某些 Windows API 不提供此類服務登入與真正使用者登入的區分，這可能導致 SSO 代理不正確地報告服務使用的使用者名稱，代替實際使用者名稱。

使用者標籤

1 按一下**使用者**標籤，可指定下列**使用者設定**選項：

- 勾選**僅允許本機列出的使用者**核取方塊只允許對裝置上本機列出的使用者進行身分驗證。預設停用此設定。
- 勾選**本機資料庫中的簡單使用者**核取方塊使用簡單使用者名稱。預設停用此設定。

  附註：除非啟用**僅允許本機列出的使用者**設定，否則此設定灰顯。

  從驗證代理或 NTLM 驗證返回的使用者名稱通常包含網域元件，例如 `domain1/bob`。在勾選此設定時，會忽略使用者名稱的網域元件，且僅將使用者名稱元件與 SonicWall 裝置的本機使用者資料庫中的名稱進行符合。如果不勾選此設定，與 SSO 驗證使用者符合的本機使用者帳戶名稱必須符合完整使用者名稱，包括任何網域元件。

  附註：網域元件可以有下列格式：
  - Windows：`DOMAIN1|bob` 或 `DOMAIN1/bob`，其中 `DOMAIN1` 是簡寫的 (NetBIOS) 網域名稱；如果本機使用者名稱區分大小寫，則它必須全部為大寫。
  - Novell：有上下文的使用者 Novell 名稱（例如 `bob.user.domain1`）或它們的 LDAP 識別名稱（例如 `cn=bob,ou=users,o=domain1`）。

- 勾選**允許受限存取非網域名稱使用者**核取方塊允許向登入到電腦但未登入到網域的使用者授予有限存取權限。即使已在本機設定，不會給這些使用者給予「受信任使用者」使用者群組的成員身分，因此也不會獲得為受信任使用者設定的任何存取權限。會通過適用於每個人的原則或專門將其列為允許使用者的原則來賦予其存取權限。預設停用此設定。

  將這些使用者在記錄中識別為 *`computer-name/user-name`*。在使用本機使用者資料庫驗證使用者時，停用**本機資料庫中的簡單使用者名稱**選項，必須使用完整的 *`computer-name/user-name`* 識別在本機資料庫中設定使用者名稱。

  附註：這不適用於通過 NTLM 驗證的使用者。對於 NTLM，僅當使用者名稱/密碼與在裝置上建立的本機使用者帳戶符合時，才會授予驗證的非網域使用者存取權限。

- 如果您的網路包含非 Windows 裝置，或執行了個人安全設備的 Windows 電腦:

  a) 勾選**探查使用者**核取方塊。

  b) 根據 SSO 代理的具體設定選擇以下選項之一：

- **透過 NetBIOS 的 NetAPI**
- **透過 TCP 的 NetAPI**
- **WMI**

提示：將滑鼠放在這些選項可顯示包含 TCP 連接埠號的小工具提示。

當 SSO 代理嘗試識別 Windows 網域中的使用者時，如果代理使用 NetAPI 或 WMI，則代理嘗試與發出流量的此使用者的電腦直接通訊。這可能導致以下問題：

- 當流量是來自非 Windows 裝置時，此類裝置不回應或可能封鎖 SSO 代理用於識別使用者的 Windows 網路訊息。
- 在有個人安全設備的電腦上會封鎖這些訊息。

結果可能是代理可能超載，有多個執行緒等待未獲得回覆的請求。

為了避免上述問題，請啟用此設定（預設為停用）並選擇 SSO 代理設定為使用的正確的 NetAPI/WMI 通訊協定。在向代理傳送請求以通過 NetAPI 或 WMI 識別使用者之前，SonicWall 裝置會探查發出流量的電腦，以驗證它是否在 NetAPI 或 WMA 協定使用的連接埠上作出回應。如果沒有，則此電腦會立即使 SSO 失敗，不會涉及代理。

附註：此設定不會影響從網域控制器讀取使用者登入資訊的代理。

- 如果啟用**探查使用者**設定，會導致安全設備在請求 SSO 代理識別使用者之前，探查 NetAPI/WMI 連接埠上的回應。**探查逾時（秒）**預設設為 **5** 秒。
- 勾選**探查測試模式**核取方塊以在 SSO 期間測試 SSO 探查功能是否正常工作，且不影響使用者驗證。在通過 SSO 代理啟動使用者驗證後，傳送探查結果。預設停用此設定。

  如果啟用此設定，則在啟動通過 SSO 代理的使用者驗證（通常在探查成功時執行）之後傳送探查結果。按正常情況更新探查統計資料，如果對代理成功驗證的使用者的探查失敗，則會通過主控台連接埠的訊息進行報告。
- 對於**設定使用者群組隸屬關係的機制**，選擇：
  - **使用 LDAP 以獲得使用者群組資訊**選項按鈕，以使用 LDAP 檢索使用者資訊預設情況下已核取此選項。
    - 若要設定 LDAP 設定，請按一下**設定**。顯示 **LDAP 設定**對話方塊。如需此對話方塊的設定資訊，請參閱第 155 頁「進階 LDAP 設定」。
  - **本機設定**選項按鈕，以使用在本機設定的使用者群組設定。
- 在**輪詢比率（分鐘）**欄位，輸入輪詢間隔，單位為分鐘（預設值為 **5**）。在識別使用者並登入後，SonicWall 會以此頻率輪詢驗證代理以驗證使用者是否仍然登入。

  如果使用 NTLM 驗證，那麼在 NTLM 設定中可以選擇強制通過 NTLM 重新驗證使用者而不是通過代理輪詢，讓裝置輪詢使用者。
- 如果網路拓撲結構要求根據使用者位置使用指定的代理，而不是輪詢所有代理以確定使用者是否仍登入，則勾選**輪詢驗證使用者的同一個代理**核取方塊。預設情況下停用此設定。

  重要：如果選擇了此設定，則還需要設定 **SSO 代理一般設定**標籤上的**無法從 NetAPI/WMI 獲取名稱時嘗試下一個代理**設定。

  預設情況下，裝置假設任何 SSO 代理都可以向任何使用者傳送 NetAPI 或 WMI 請求，因此當輪詢以查看使用者是否仍登入時，裝置可以根據目前負載選擇任意代理。如果不是這樣，網路佈局需要根據使用者的位置使用特殊的代理，那麼請啟用此設定。在啟用此設定時，在代理成功識別使用者後，後續可通過同一代理執行對使用者的輪詢。

  附註：此設定僅影響使用 NetAPI/WMI 的代理，不會影響只使用網域控制器安全日志查詢機制的代理。

- 在**等待時間（分鐘）**欄位以分鐘數輸入安全裝置在初次嘗試識別流量失敗後等待重試的時間。此功能會限制傳送到此代理的請求數，以避免繼續從反復使 SSO 失敗的來源收到後續流量時可能出現的攻擊。預設為 **1** 分鐘。

  附註：從 SSO 代理收到錯誤後等待的時間與代理報告無使用者登入後等待的時間是分別設定的，因此要分別進行設定。

- 在 **...找不到使用者之後**欄位中，輸入裝置在收到來自 SSO 代理的錯誤或代理報告無登入使用者時重新嘗試前應等待的分鐘數。預設為 **1** 分鐘。

2 為了在記錄中統一命名網域，為**當不同的 SSO 來源報告使用者網域的不同的網域名稱**選擇以下選項按鈕之一：

- **使用網域名稱作為接收**（預設）
- **總是使用連續的網域名稱**；移至步驟 a。

預設情況下，通過 SSO 識別的使用者登入 SonicWall 裝置，由識別此使用者的外部來源報告無論什麼網域名稱。然而，一個網域通常有兩個或三個不同的網域名稱變體（例如，Windows 網域有它的 DNS 名稱、NetBIOS 名稱以及 Kerberos 領網域名稱），而且不同的 SSO 來源可能對同一個網域中的使用者報告上述不同的網域名稱。

這種差別導致很難根據網域在記錄中追蹤使用者，您可以通過讓網域中的所有使用者使用相同的網域名稱變體，不論向 SonicWall 裝置報告什麼變體，都可以使網域名稱保持一致。

a 如果您已選擇**總是使用連續的網域名稱**，請按一下**選擇**按鈕。將顯示**為每個網域選擇變數名**顯示對話方塊，其中列出了已知的網域，從中可以選擇要使用的名稱。

b 選擇要使用的變體。每個網域的初始預設變體為**無**，意思是使用何種網域名稱通過 SSO 報告給裝置的行為不會改變，直到啟用**總是使用連續的網域名稱**且在這裡選擇要使用的網域名稱。

附註：如果在此清單中未顯示某個網域，請等待 SSO 識別了此網域中的某些使用者，然後再重複此步驟。

c 按一下**確定**。

如果在使用單點登入時，您看到**使用者 > 狀態**頁面中顯示預料之外的使用者名稱，或者使用者登入或失敗的使用者登入嘗試記錄中包含預料之外的使用者名稱，這可能由於應該在這裡設定 Windows 服務登入和使用者名稱以使 SSO 代理知道忽略這些使用者名稱。

如果有多個安全設備與 SSO 代理通訊，應該僅在一個安全設備上設定服務帳戶名稱的清單。在不同裝置上設定多個清單的後果尚不明確。

實施標籤

1 如果您要對來自指定區域的流量觸發 SSO，或者對來自內部代理 Web 伺服器或 IP 電話等非使用者裝置的流量繞過 SSO，請按一下**加強**標籤。

2 在**每一區域的 SSO 執行**下，選擇您要觸發 SSO 以在傳送流量時識別使用者的所有區域的核取方塊。

- **LAN**
- **DMZ**
- **VPN**
- **WLAN**

如果應用程式控制或其他原則已要求對區域實施 SSO，預先勾選這些核取方塊，且無法清除。如果對區域啟用了來賓服務，則不能實施 SSO，您也無法勾選核取方塊。在未啟動此服務的區域中，可通過此選項啟用 SSO 強制功能。

附註：在將安全服務原則或存取規則設為要求使用者驗證的區域上，將始終對受影響的流量啟動 SSO，因此無需在此啟用 SSO 實施。

這些按區域 SSO 實施設定可用於在事件記錄和 AppFlow 監控顯示中識別和追蹤使用者，即使內容篩選、IPS 或應用程式控制原則或者需要使用者驗證的存取規則未觸發 SSO。

3 若要使來自指定服務或位置的流量繞過 SSO 並對此流量套用預設的內容篩選原則，請從 **SSO 繞過**表中的清單選擇適當的服務或位置，或者向表中新增新服務或位置。此表顯示了繞過 SSO 的內建服務；這些服務無法刪除。

提示：您可以為此情況建立 SSO 繞過位址和/或服務群組物件並在此處和它們的存取規則中引用相同的物件。

附註：在要求使用者驗證的存取規則觸發 SSO 時，將不會套用 SSO 繞過設定。若要設定這種類型的 SSO 繞過，請對受影響的流量新增不需要使用者驗證的單獨存取規則。如需設定存取規則的詳細資訊，請參閱 *SonicOS 原則*。

預設情況下，將預設的內容篩選原則指派給不經由 SSO 通過 Samba 驗證的 Linux 和 Mac 使用者。若要將不接受 SSO 身分驗證的所有此類使用者重新導向，以手動輸入其登入憑證，請為 **HTTP** 服務建立從 **WAN** 區域到 **LAN** 區域的存取規則，在其中將**允許的使用者**設為**全部**。然後，設定使用者或使用者群組的相應 CFS 原則。如需設定存取規則的詳細資訊，請參閱 *SonicOS 原則*。

SSO 繞過可能是必要的，例如：

- 來自非使用者裝置的流量，例如內部郵件伺服器或 IP 電話。
- 不需要進行驗證且可能會受到 SSO 等待延遲的負面影響的使用者流量。

對於繞過 SSO 的流量，將套用預設內容篩選原則。如果任何 APP 規則或 IPS/防間諜軟體原則設定為包括/排除使用者，那麼這些規則或原則不會分別包括/排除此流量。

第二項設定適合於不需要進行身分驗證的使用者流量，且觸發 SSO 可能導致過長的服務延時的情況。

4 （可選）若要新增服務或位置：

a 按一下**新增**按鈕。將顯示**新增 SSO 繞過規則**對話方塊。

b 對於**繞過 SSO 以**，選擇**服務**或**位址**選項按鈕。

c 從下拉功能表中選擇服務或位址。

d 選擇**繞過類型**：

- **完全繞過（不觸發 SSO）**
- **觸發 SSO 但是在等待時繞過所包含封包**

e 按下**新增**。此項目新增到表中

5 選擇 SSO 繞過使用者名稱以進行記錄的步驟如下：

a 勾選**用於繞過 SSO 的記錄使用者名稱 *<繞過名稱>*** 核取方塊。

b 為繞過 SSO 使用者指定一個名稱。

預設選擇此設定且指定預設名稱 **SSO 繞過**。如果啟用此設定，那麼當流量繞過 SSO（如此處所設定）時，此流量會以給定的使用者名稱顯示在記錄和 AppFlow 監控中，而不是顯示為來自未知使用者，因此可以同 SSO 無法識別的使用者傳送的流量區別開。

提示：您也可以在**使用者工作階段設定**下的**使用者 | 設定**頁面設定記錄。

6 （可選）勾選**建立虛擬使用者**核取方塊。預設情況下未勾選此設定。

如果啟用此設定，則在收到 SSO 繞過流量時，將以給定使用者名稱為始發 IP 位址建立虛擬使用者項目。除了顯示在記錄和 AppFlow 監控中的名稱，虛擬使用者項目還顯示在**使用者 > 狀態**頁面中。此虛擬名稱會一直存在，直到來自此 IP 位址的流量在指定非使用中時間停止，或者如果是繞過服務，則直到從它收到非繞過流量。

附註：此虛擬使用者名稱僅適用於為完全 SSO 繞過設定的繞過規則。「任何設定為在等待它時觸發 SSO 但繞過保留封包的項」會導致按照觸發的 SSO 識別的結果來設定此使用者。

附註：此選項的記錄部分也可透過**使用者 | 設定**頁面的**使用者工作階段設定**區段中的**記錄未識別使用者的連線**選項進行設定。

a （可選）在**非使用中狀態逾時 (分鐘)**欄位中指定非使用中逾時值，以分鐘為單位。預設值為 **15** 分鐘。

終端服務標籤

1 按一下**終端服務**標籤可指定下列**終端服務代理設定**選項。

2 如需新增代理，請按一下**新增**按鈕。頁面已更新，在表格頂部顯示新行，在頁面的下半部分顯示新輸入欄位。對於現有代理：

- 代理旁邊的綠色 LED 式圖示表示代理已啟動，正在執行。
- 紅色 LED 圖示表示代理已關閉。
- 黃色 LED 圖示表示 TSA 閒置，裝置在 5 分鐘或更長時間內未收到回應。

由於是 TSA 向裝置傳送通知，而不是由裝置向代理傳送請求，缺少通知可能表示有問題，但更可能表示目前終端伺服器上沒有使用中使用者。

- 在**主機名稱或者 IP 位址**欄位，輸入安裝 SonicWall TSA 的終端伺服器的名稱或 IP 位址。如果終端伺服器時多宿主（有多個 IP 位址），且您按 IP 位址而不是按 DNS 名稱識別主機，請以逗號分隔清單的形式輸入所有 IP 位址。

  附註： 在輸入欄位值時，將頂部的行更新為紅色，以高亮顯示新資訊。

- 在**連接埠**中，輸入 SonicWall TSA 代理用於與裝置通訊的連接埠數目。預設連接埠號是 **2259**。

  附註：不同 IP 位址的代理可以有相同的連接埠數目。

- 在**共用密碼**欄位，輸入您在 SonicWall TSA 中建立或產生的共用密碼。共用密碼必須完全符合。在**確認共用密碼**欄位中重新輸入共用密碼。

3 按一下**一般設定**標籤，在**終端服務代理設定**下設定以下選項：

- 選擇**啟用終端服務代理驗證**核取方塊使用 TSA 進行使用者身分驗證。此選擇在預設情況下不啟用。
- 預設勾選**允許來自終端伺服器的流量繞過使用者驗證的存取規則**核取方塊。這允許 Windows 更新或防毒更新等與任何使用者登入工作階段不相關的服務流量通過，而不進行身分驗證。如果相應的存取規則設為要求使用者驗證，則通常會封鎖此流量。

  如果清除此核取方塊，如果存取規則要求使用者驗證，可能封鎖來自服務的流量。在這種情況下，您可以新增規則以允許前往服務流量目的地的**所有**存取，或以 HTTP URL 設定可以繞過存取規則中使用者驗證的目的地。

NTLM 標籤

1 按一下 **NTLM** 標籤。

NTLM 驗證受基於 Mozilla 的瀏覽器支援，可作為通過 SSO 代理識別使用者的一種補充方法，或作為無代理的獨立驗證方法，但有某些限制。安全設備直接與瀏覽器互動以驗證使用者。使用網域憑證登入的使用者接受透明驗證，在其他情況下，使用者可能需要輸入憑證才能登入裝置，但應該只需要輸入一次，因為憑證已儲存。

如需關於 NTLM 的詳細資訊，請參閱第 85 頁「瀏覽器 NTLM 驗證的運作方式?」。

2 設定這些設定；

- 從**使用 NTLM 來驗證 HTTP 流量**下拉清單中選擇以下一種選擇：
  - **從不** - 從不使用 NTML 驗證
  - **在透過代理嘗試 SSO 之前** - 在使用 SonicWall SSO 代理之前嘗試使用 NTLM 驗證使用者
  - **只有當透過代理的 SSO 失敗** - 先嘗試通過 SSO 代理驗證使用者，如果失敗，再嘗試使用 NTLM
- 對於**驗證網域**，執行以下一項操作：
  - 以「www.somedomain.com」形式輸入安全設備網域的完整 DNS 名稱
  - 勾選**使用來自 LDAP 設定的網域**核取方塊使用 LDAP 設定中使用的相同網域。

  只有在瀏覽器發現裝置網域是本機網域時，才會進行完全透明的身分驗證。
- 對於**重新導向瀏覽器至該應用程式，透過**，選擇以下一個選項確定如何初次將使用者的瀏覽器重新導向至安全設備自己的 Web 伺服器：
  - **介面 IP 位址** - 選擇此選項將瀏覽器重新導向至裝置 Web 伺服器介面的 IP 位址。
  - **使用可逆 DNS 查詢介面 IP 位址的網域名稱** - 這將啟用視窗底部的**顯示反向 DNS 快取**按鈕，按一下後，在幾秒內，快顯視窗顯示裝置 Web 伺服器的介面、IP 位址、DNS 名稱和 TTL。按一下此按鈕驗證用於重新導向使用者瀏覽器的網域名稱（DNS 名稱）。
  - **其設定的網域名稱** - 使用在**系統 > 管理**頁面設定的安全設備網域名稱。
  - **來自管理憑證的名稱** - 使用在**系統 > 管理**頁面為「HTTPS Web 管理」選擇的匯入憑證。
- 在**允許驗證的最多失敗次數**中輸入重試次數。
- 為了偵測使用者何時登出，在**輪詢計時器，透過 NTLM 驗證使用者**選項中選擇裝置對 Windows、Linux 和 Macintosh 使用者使用的輪詢方法。對各種電腦上的使用者選擇以下一種方法的選項按鈕：
  - **透過 SSO 代理輪詢** - 如果在網路中使用 SSO 代理，選擇此選項使用 SSO 代理輪詢使用者。對於通過 NTLM 驗證的使用者，代理沿用的使用者名稱必須符合用於 NTLM 驗證的使用者名稱，否則登入工作階段將終止。您可能想對 Linux 或 MacOS 使用者選擇另一種輪詢方法，因為這些系統不支援 SSO 代理使用的 Windows 網路請求。
  - **透過 NTLM 重複驗證** - 如果將瀏覽器設定為儲存網域登入憑證，或者使用者指示瀏覽器儲存登入憑證，則這種方法對使用者透明。
  - **不要重複驗證** - 如果選擇此選項，除了非使用中逾時的情況以外，不會偵測使用者登出。

  附註：當設定「多種內容篩選」原則且單點登入加強啟用 NTLM 時，必須在**防火牆 > 存取規則**頁面的 LAN 到 WAN 規則中新增 HTTP/HTTPS 存取規則，此規則將可信使用者列為允許的使用者。此規則向使用者觸發 NTLM 驗證請求。如果未新增此存取規則，嚴格的 CFS 原則將封鎖使用者的 Internet 存取並禁止驗證請求。

- 如果使用要求在 NTLM 訊息中包含舊 LAN 管理元件的舊式伺服器，請勾選**在 NTLM 中轉送舊式 LanMan** 核取方塊。這可能導致在預設不允許 NTLM 中包含 LanMan 的新式 Windows 伺服器中的身分驗證失敗，因為這樣不安全。

RADIUS 計費標籤

1 按一下 **RADIUS 計費**標籤顯示 **RADIUS 計費單一登入**標籤。

通過 RADIUS 計費的單點登入允許裝置作為外部供應商裝置的 RADIUS 計費伺服器，並根據來自這些裝置的計費訊息讓使用者登入或登出。對於因其他目的使用 RADIUS 計費的供應商裝置，SonicOS 也可以將 RADIUS 計費訊息轉送給另一 RADIUS 計費伺服器。

狀態列顯示面板中列出的各 RADIUS 計費用戶端的目前狀態。

- 綠色 - 用戶端使用中
- 黃色 - 用戶端閒置
- 灰色-未偵測到用戶端

2 若要新增新 RADIUS 用戶端，按一下**新增**...按鈕。**RADIUS 計費單一登入**標籤（**設定**、**RADIUS** 和**轉送**）顯示在此對話方塊下半部分的查看/編輯窗格中。

附註：在查看/編輯面板中所做的變更會直接顯示在**計費用戶端**表的高亮顯示項目內。完成後，按一下面板之外的任意位置將其關閉。對於**計費用戶端**表中的各個欄位，也可以通過直接在表中按一下它們進行更新。

3 在**用戶端主機名稱或 IP 位址**欄位中，輸入 RADIUS 用戶端主機的名稱或 IP 位址。

4 在**共用密碼**欄位和**確認金鑰**欄位中，輸入用戶端的共用密碼。

5 按一下 **RADIUS** 標籤。

6 從**使用者名稱屬性格式**下拉功能表中選擇使用者名稱登入使用的格式。

RADIUS 計費不會指定在 RADIUS 計費訊息中傳送的「使用者名稱」屬性的內容的格式。因此，您需要輸入用戶端傳送的格式。可以從一些常用格式中選擇：

- **使用者名稱**
- **網域\使用者名稱**
- **網域/使用者名稱**
- **使用者名稱@網域**
- **SonicWall SMA**
- **其他** - 非標準格式

重要：此預先定義格式適用於一般情況。如果不符合您的網路存取伺服器傳送的內容，則必須選擇**其他**作為**使用者名稱**屬性格式並輸入自訂的格式。

7 如果選擇：

- 標準格式，請移至步驟 8。
- 如果選擇**其他**，會顯示更多設定，以便您能夠設定在屬性中出現的元件：
  - **格式**
  - **元件**

a 在**格式**欄位，為每個元件輸入有限 scanf 型字串，包含 `%s` 或 `%[...]` 指令。此指令告訴裝置網路存取裝置 (NAS) 在**使用者名稱**屬性中傳送的內容。此格式並非由 RADIUS 計費 RFC 指

定。裝置在此屬性中能夠傳送的內容方面無限制，因此它的內容可以非常多變。您在這裡的設定指定裝置如何對**使用者名稱**屬性解碼以提取使用者名稱、網域和/或 DN。

提示：在選擇**其他**時，將這些欄位設為之前選擇的格式的格式字串和元件。所以，請首先選擇最符合網路存取伺服器傳送內容的預先定義格式。這為您輸入自訂格式奠定了很好的基礎。然後，變更為**其他**。

b 從**元件**下拉功能表中選擇以下選項之一：

- **未使用**
- **使用者名稱**（預設）
- **網域**
- **DN**

您在**格式**欄位中以有限 scanf 型字串輸入的元件包含一個或多個以下項：

- 使用者名稱
- 網域
- 完整的識別名稱 (DN)

附註：您可以在**元件**下拉功能表中按兩下，以顯示工具提示，其中包含有關如何輸入 scanf 型格式的說明。

c 按一下**新增元件**。將顯示**新增元件至 User-Name 屬性格式**對話方塊。

附註：如果您瞭解 scanf 型格式，可以直接編輯**格式**欄位，不用使用**新增元件**按鈕。

提示：對於後跟空白字元或位於末尾的元件，使用 %s。對於後跟一些其他字元的元件，使用 %[^x]x。例如，`name@domain` 格式的**格式**字串為 `%[^@]@%s`，有三個元件設定為**使用者名稱**、**網域**和**未使用**。

d 從**要加入的元件**下拉功能表中選擇元件類型：

- **使用者名稱**
- **網域**
- **DN**

e 在**使用者名稱後面的首碼文字**欄位中輸入用於分隔項目的文字。

f 按一下**新增**。**計費用戶端**表將更新且在 Radius 查看/編輯面板中出現更多選項。

g 對每個元件重複步驟 b 到步驟 f。

若要刪除您新增的最後一個元件，請按一下**移除上一個元件**。

8 在使用者登入後，RADIUS 計費用戶端可以選擇定期傳送臨時更新訊息。如果用戶端未在合理的一定間隔內傳送訊息，則 SonicWall 裝置監控這些訊息且在訊息停止傳送後假設此使用者已登出。此過程提供了一種後備機制，可防止遺失 RADIUS 計費停止訊息（在使用者登出時傳送）。

選擇**如果未收到計費臨時更新則登出使用者**選項：

- **已停用** - 不傳送訊息。
- **已啟用** - 手動指定**逾時**間隔。設定比 RADIUS 計費用戶端傳送臨時更新訊息的期間大的逾時值，且對於丟棄/遺失的臨時更新訊息，設定至少 2 到 3 倍於此期間的**逾時**值。

- **自動**（預設）- 讓裝置自動偵測是否正在定期傳送臨時更新訊息，如果是，則按照「已啟用」下的指定使用它們並自動設定對應的逾時值。

  附註：如果在一段時間後，重新載入頁面後逾時值停留在 0（零），則裝置並沒有偵測到訊息傳送且未使之逾時。

  可能需要相當長的時間來完成自動偵測，取決於用戶端傳送訊息的頻率。例如，如果用戶端每 10 分鐘傳送一次訊息，則可能需要 30 多分鐘才能在此處顯示測量逾時。

  提示：可以按一下**顯示資訊**連結，以在顯示對話方塊中查看進度。

  提示：若要重新執行自動偵測，請將設定變更為**已停用**，然後返回**自動**，每次變更後按一下**套用**。

9 按一下**轉送**標籤。

10 在**轉送**標籤下，您可以在以下欄位中輸入最多四個 RADIUS 計費伺服器：

- **名稱或 IP 位址**
- **連接埠**（預設 **1813**）
- **共用密碼**，用戶端向其轉送訊息的 RADIUS 計費伺服器的共用密碼
- **確認共用密碼**

在為伺服器輸入此資訊後，將顯示**從中選擇**下拉功能表。

11 對於每個伺服器，從**從中選擇**下拉功能表中選擇：

- **未轉送**
- 計費伺服器的 IP 位址

如果來自多個用戶端的請求要轉送到同一個計費伺服器，則在此伺服器已設定用於任何一個用戶端後，可以從**從中選擇**下拉功能表中為其他用戶端選擇此伺服器。將會複製所選計費伺服器的所有資訊，包括它的共用密碼，並轉而用於此用戶端。

12 在**逾時（秒）**欄位和**重試次數**欄位中，輸入逾時秒數和重試次數。**逾時（秒）**的預設值為 **10** 秒，**重試次數**的預設值為 **3**。

要確定哪些使用者已登出，SonicWall 網路安全裝置通過在傳送給 SSO 代理的單個請求訊息中向多個登入的使用者傳送請求來輪詢 SSO 代理。要設定安全設備可以在單個請求訊息中向測試標籤傳送的使用者請求數：

13 選擇從此用戶端轉送 RADIUS 計費訊息的方式：

- **逾時後嘗試下一個**
- **轉送給所有**

14 選擇**一般設定**標籤。

15 通過勾選**啟用 SSO 或 RADIUS 計費**核取方塊，啟用 SSO 或 RADIUS 計費。預設啟用此設定。

16 在**連接埠號碼**欄位中指定連接埠。預設連接埠號是 **1813**。

17 按一下**進階設定**標籤。

18 如需使此裝置追蹤用於「啟動/停止」訊息傳送的 RADIUS 計費訊息，請勾選**歸因於無線漫遊的開始/停止訊息除外**核取方塊。預設停用此設定。

RADIUS 計費用戶端傳送「啟動/停止」訊息以向安全設備通知連線/中斷連線的使用者。如果這些用戶端為或使用無線存取點，則無線使用者可在存取點之間漫遊，作為使用者連接到新存取點和從舊存取點斷開時，這可能會使其產生偽造的「啟動/停止」訊息。這些漫遊的「啟動/停止」訊息可能會干擾 SSO 驗證過程，此驗證過程通常將「停止」訊息處理為使用者登出通知。

如果啟用此選項，安全設備將追蹤 RADIUS 計費訊息以查找此「啟動/停止」序列。如果找到此序列，則安全設備會將「停止」訊息視為漫遊指示，而非使用者登出通知。

即如果這些訊息為下列情況，則安全設備認定「啟動/停止」訊息是由於在存取點之間切換漫遊：

- 已接收（以任意順序）：目前連接使用者的「啟動」訊息，指示同一使用者位於不同存取點，同時有來自上一位置的「停止」訊息。
- 它們在指定時間段內同時出現。

附註：最長切換時間應允許可能遺失和重新傳送的 RADIUS 計費訊息。推薦時間等於逾時乘以 RADIUS 計費用戶端的最大項目數。

19 若要讓安全設備忽略以下使用者的任何 RADIUS 計費訊息:

- 在特定 IP 位址中時，從**對於在這些 IP 位址的使用者**下拉功能表中選擇位址物件或位址群組，或建立新位址物件或位址群組。預設為**無**。
- 未在特定 IP 位址中時，從**對於不在這些 IP 位址的使用者**下拉功能表中選擇位址物件或位址群組，或建立新位址物件或位址群組。預設值為**全部**。
- 對於特定使用者名稱：

  a) 按下**新增**。顯示**新增 RADIUS 計費使用者名稱排除**顯示對話方塊。

  b) 從「忽略任何使用者名稱」下拉功能表中選擇

  - **開始**
  - **結束**

  c) 在**使用**欄位中輸入使用者名稱。

  d) 按一下**儲存**。此項目新增到清單中

  如需編輯項目，請先勾選，然後按一下**編輯**。

  如需移除項目，請先勾選，然後按一下**移除**。

測試標籤

1 如需測試已設定的代理設定，按一下**測試**標籤。

重要：在此頁面執行的測試適用於已作出的任何變更。

您可以測試裝置和 SSO 代理或 TSA 之間的連接。您還可以測試是否正確設定了 SSO 代理以識別登入到工作站的使用者。

2 如果您設定了多個代理，從**選擇代理測試**下拉功能表中選擇待測試的 SSO 代理或 TSA。下拉功能表包含最上方的 SSO 代理和標題 **--終端伺服器代理--** 下最末端的 TSA。

3 選擇需執行的測試類型：

- **檢查代理的連接**選項按鈕 - 測試與驗證代理的通訊。如果安全設備可連線至 SSO 代理，將顯示**代理就緒**訊息。在測試 TSA 時，**測試狀態**欄位顯示訊息，**從代理返回的資訊**欄位中顯示版本和伺服器 IP 位址。
- 僅對於 SSO 代理勾選**檢查使用者**選項按鈕，在**工作站 IP 位址**欄位中輸入工作站的 IP 位址。這將測試是否正確設定了 SSO 代理以識別登入到工作站的使用者。

  提示：如果顯示**代理未回應**或**設定錯誤**訊息，請檢查您的設定，然後再次執行這些測試。

4 按一下**測試**按鈕

5 在完成所有驗證代理設定後，按一下**確定**。

設定 SSO 的 RADIUS 計費

單一登入的 RADIUS 計費是在**使用者 | 設定**頁面上設定。

若要設定 SSO 的 RADIUS 計費：

1 顯示**使用者 | 設定**頁面。

2 按一下**設定 SSO** 按鈕。將顯示 **SSO 驗證設定**對話方塊。

3 按一下 **RADIUS 計費**標籤。如需設定 RADIUS 計費，請參見第 151 頁「RADIUS 計費標籤」。

4 按一下**套用**。

進階 LDAP 設定

如果您在第 142 頁「設定 SonicOS 以使用 SonicWall SSO 代理」中所述的**使用者**標籤中勾選**使用 LDAP** 以獲得使用者群組資訊，則必須設定 LDAP 設定。

設定 LDAP 以獲得使用者群組資訊：

1 在 **SSO 驗證設定**對話方塊的**使用者**標籤，按一下**使用 LDAP 以獲得使用者群組資訊**選項旁邊的**設定**按鈕。顯示 **LDAP 設定**對話方塊。

主題：

- 第 155 頁「「設定」標籤」
- 第 157 頁「結構標籤」
- 第 158 頁「目錄標籤」
- 第 159 頁「提名標籤」
- 第 160 頁「使用者和群組標籤」
- 第 162 頁「LDAP 轉接標籤」
- 第 163 頁「測試標籤」

「設定」標籤

2 在**名稱或者 IP 位址**欄位中，輸入 LDAP 伺服器的名稱或 IP 位址。

3 在**連接埠數目**欄位中，輸入 LDAP 伺服器的連接埠數目。您可以從下拉功能表中選擇的預設 LDAP 連接埠為：

- **預設 LDAP 連接埠 - 389**
- **預設 LDAP 越過 TLS 連接埠 - 636**
- **Windows 全域目錄連接埠 - 3268**
- **全域目錄越過 TLS 連接埠 - 3269**

4 在**伺服器逾時（秒）**欄位中，輸入在嘗試逾時前，安全設備等待來自 LDAP 伺服器的回應的秒數。允許值從 1 至 99999。預設值為 **10** 秒。

5 在**全面操作逾時（分鐘）**欄位中，輸入在逾時前安全設備執行自動操作的分鐘數。允許值從 1 至 99999。預設值為 **5** 分鐘。

> **附註：**某些操作（例如目錄設定或匯入使用者群組）可能需要若干分鐘，特別是如果執行多個 LDAP 伺服器。

6 從以下選項按鈕指定登入類型：

- **匿名登入**，可以匿名登入。有些 LDAP 伺服器允許匿名存取樹狀目錄。如果伺服器支援匿名存取（Microsoft Active Directory 一般不支援），您可以選擇此選項。**登入使用者名稱**和**登入密碼**欄位為灰顯。移至步驟 10。
- **在樹狀目錄中提供使用者名稱 / 位置**使用登入名稱存取樹狀目錄。**登入使用者名稱**和**登入密碼**欄位可用。移至步驟 7。

  > **附註：**確保在**目錄**標籤的**用於登入伺服器的樹狀目錄**欄位中輸入使用者樹狀目錄。

- **提供繫結辨別名稱**使用識別名稱存取樹狀目錄。「登入使用者名稱」欄位將變更為「繫結識別名稱」欄位，且「登入密碼」欄位可用。移至步驟 8。

7 若要使用使用者的姓名登入，請在**登入使用者名稱**欄位中輸入使用者的姓名。在完整的 `dn` 表示法中，登入名稱將自動向 LDAP 伺服器顯示。移至步驟 9。

> **附註：**在**登入使用者名稱**欄位中使用使用者的姓名，即使用者的識別名稱的第一個元件，而不是使用者名稱或登入 ID。例如，John Doe 通常以 jdoe 登入，但是在此處以 John Doe 而不是 jdoe 登入。

8 在**繫結識別名稱**欄位中，指定用於繫結到 LDAP 伺服器的完全識別名稱 (DN)。

9 在**登入密碼**欄位中輸入密碼。

10 從**通訊協定版本**下拉功能表中選擇 LDAP 版本：**LDAP 版本 2** 或 **LDAP 版本 3**（預設）。包括 Active Directory 在內的大多數 LDAP 實施都採用 LDAP 版本 3。

11 勾選**使用 TLS (SSL)** 核取方塊使用傳送層安全性 (SSL) 登入 LDAP 伺服器。預設情況下已核取此選項。

> **重要：**強烈建議使用 TLS 防護將通過網路傳送的使用者名稱和密碼資訊。大多數 LDAP 伺服器實施（包括 Active Directory）都支援 TLS。

12 也可勾選**傳送 LDAP '開始 TLS' 請求**核取方塊允許 LDAP 伺服器在相同的 TCP 連接埠在 TLS 和非 TLS 模式下執行。預設情況下未勾選此選項。

> **附註：**只有在 LDAP 伺服器對於 TLS 和非 TLS 使用相同的連接埠數目時才勾選**傳送 LDAP '開始 TLS' 請求**框，且只能在 LDAP 伺服器要求時勾選。

有些 LDAP 伺服器實施支援「啟動 TLS」指令，而不是使用原生 LDAP over TLS。這允許 LDAP 伺服器監聽 LDAP 連接的一個連接埠（通常是 389）以及切換到用戶端指示的 TLS。

13 勾選**需要來自伺服器的有效的憑證**核取方塊要求來自伺服器的有效憑證。在 TLS 交換期間，通過將以上指定的名稱與憑證上的名稱相符合，來驗證伺服器提供的憑證。預設情況下已核取此選項。

> **附註：**取消選擇此預設選項將顯示一條警示，但安全設備和 LDAP 伺服器之間的資訊交換仍使用 TLS，只是沒有驗證發佈。

14 從**本機用於 TLS 的憑證**下拉功能表中選擇本機憑證。這是可選的，僅用於 LDAP 伺服器需要用戶端憑證進行連接的情況。此功能對於返回密碼以確保 LDAP 用戶端身分的 LDAP 伺服器實施很有用（Active Directory 不返回密碼）。Active Directory 不需要這項設定。預設為**無**。

15 按一下**套用**。

結構標籤

1 按一下**結構**標籤。

2 從 **LDAP 結構**下拉功能表中，選擇以下一個 LDAP 結構。選擇任意預先定義的結構將自動使用正確值填寫此結構使用的欄位。

- **Microsoft Active Directory**（預設）
- **RFC2798 InetOrgPerson**
- **RFC2307 網路資訊服務**
- **Samba SMB**
- **Novell eDirectory**
- **使用者定義** - 用於指定自己的值。

  重要：僅當您有特定的或專有的 LDAP 結構設定時才使用此選項。

3 **物件類別**欄位定義能夠反映以下兩個欄位所套用的各使用者帳戶的屬性。除非您選擇了**使用者定義**，否則此欄位不可修改。

4 **登入名稱屬性**欄位定義登入驗證使用哪個屬性。除非您選擇了**使用者定義**，否則此欄位不可修改。

5 如果**有資格的登入名稱屬性**欄位不為空，可以指定使用者物件的屬性以 *name@domain* 格式設定備選的登入名稱。這尤其可用於有多個網域的情況，其中，簡單的登入名稱可能在多個網域中不唯一。將之設為 **Microsoft Active Directory** 和 **RFC2798 inetOrgPerson** 的**郵件**。

6 **使用者群組成員資格功能**欄位包含使用者物件所屬群組的資訊。這是 Microsoft Active Directory 中的**隸屬於**屬性。其他預先定義的方案儲存群組物件中的群組成員資訊，而不是使用者物件，因此不使用此欄位。除非您選擇了**使用者定義**，否則此欄位不可修改。

7 **額外使用者群組 ID 使用者功能**，以及**使用者群組物件**部分中的**額外使用者群組符合使用者群組功能**設定，允許為使用者設定額外的成員身分的結構，除了通過成員/隸屬於屬性發現的那些身分，例如 Active Directory 的主要群組屬性。

如果指定了**額外使用者群組 ID** 使用者屬性且已通過勾選「使用」核取方塊啟用，那麼在找到有此屬性的一個或多個實例的使用者物件後，在 LDAP 目錄中搜尋與此符合的額外使用者群組。如果找到**額外使用者群組符合**屬性設定為此值的群組，則此使用者也會成為此群組的成員。

提示：利用 Active Directory，使這些屬性的使用設定為 **primaryGroupID** 和 **primaryGroupToken** 將使使用者獲得其主要使用者群組成員的身分，特別是**網域使用者**。

8 **帶框架的 IP 位址屬性**欄位可用於檢索指派到目錄中使用者的固定 IP 位址。目前，這僅用於通過 L2TP 使用安全設備 L2TP 伺服器的使用者連接。以後的版本可能支援用於 SonicWall Global VPN Client (GVC)。在 Active Directory 中，固定 IP 位址在使用者屬性的「撥號」標籤中設定。

9 **物件類別**欄位定義了 LDAP 目錄可能包含的項目類型。AD 使用的範例物件類別有使用者或群組。

10 **成員屬性**欄位定義登入驗證使用哪個屬性。選擇屬性是否為：

- **識別名稱**
- **使用者 ID**

11 **額外使用者群組符合功能**，以及**額外使用者群組 ID 功能**，允許為使用者設定額外成員身分的結構，除了通過成員/隸屬於屬性發現的那些身分。如需詳細資料，請參閱步驟 7。

12 （可選）若要讀取結構的詳細資料，請按一下**從伺服器讀取**按鈕。將顯示**讀取 LDAP 結構描述**對話方塊。

a 指定：

- **自動更新結構描述設定**（預設）
- **匯出結構描述的詳細資料**

b 按一下**確定**。

目錄標籤

1 選擇**目錄**標籤。

2 在**主要網域**欄位，指定 LDAP 實施使用的使用者網域。對於 AD，這是 Active Directory 網域名稱，例如 *yourADdomain.com*。可以選擇將對此欄位的變更自動更新到頁面其餘的樹狀目錄資訊。將所有結構預設設為 **mydomain.com**，但 Novell eDirectory 除外，並設為 **o=mydomain**。

3 在**用於登入伺服器的樹狀目錄**欄位中，在為在**設定**標籤的**登入使用者名稱**欄位中指定的使用者帳戶儲存使用者物件的目錄中指定樹狀目錄。例如，在 Active Directory (AD) 中，「管理員」帳戶的預設樹狀目錄與使用者樹狀目錄相同。

附註：除非在**設定**標籤上選擇**在樹狀目錄中提供使用者名稱/位置**，否則此欄位為灰顯。

4 **包含使用者的樹狀目錄**表列出了使用者物件在 LDAP 目錄中通常所在的樹狀目錄。在使用者驗證期間，搜尋列出的樹狀目錄可找到此使用者。可以編輯提供的預設值 **mydomain.com/user**，最多可以提供 64 個 DN 值，且安全設備將搜尋目錄直至找到符合項，否則將查找完整個清單。

若要新增新的樹狀目錄：

a 按下**新增**。將顯示包含預設樹狀目錄的**新建樹狀目錄**對話方塊。

b 輸入新樹狀目錄。

可以只指定主要網域，其中還包括備用 LDAP 伺服器上的子網路域，或者為了提高搜尋效率，也可以在目錄中輸入特定的子樹狀目錄。

可以指定下列兩種格式的樹狀目錄：

- 路徑格式（例如 `domain.com/people`）
- 識別名稱格式（例如 `ou=people,dc=domain,dc=com`）；對於有非標準格式的 DN 的樹狀目錄，此格式為必需。在使用此格式時，必須在句點 (.) 和斜線 (/) 字元前加反斜線 (\)。如需對識別名稱中的字元進行轉義的額外要求的資訊，請參見 RFC2253。

c 按一下**確定**。此樹狀目錄新增到表中。

若要編輯表中的現有樹狀目錄：

a 選擇表中的樹狀目錄。

b 按一下**編輯**。

c 進行必要的變更。

d 按一下**確定**。對表中的樹狀目錄進行了變更。

若要移除表中的現有樹狀目錄：

a 選擇表中的樹狀目錄。

b 按一下**移除**。

5 排序並不重要，但是由於以既定順序搜尋，所以將最常用的樹狀目錄放在各清單的前面是最高效的做法。如果要使用多個 LDAP 伺服器之間的提名，最好的排序是將位於主要伺服器上的樹狀目錄放在前面，其餘樹狀目錄以提名順序排列。若要調整表中的項目的位置：

a 選擇要移動的樹狀目錄。

b 按一下**向上**或**向下**箭頭，直到此項目移至所需的位置。

c 對每個要調整位置的樹狀目錄重複步驟 a 和步驟步驟 b。

6 在**包含使用者群組的樹狀目錄**欄位中，指定使用者群組物件在 LDAP 目錄中通常所在的樹狀目錄。最多可以提供 32 個 DN 值。這僅適用於結構的使用者物件中沒有使用者群組成員身分屬性，且不使用 AD 的情況。若要新增新的樹狀目錄：

a 按下**新增**。將顯示包含預設樹狀目錄的**新建樹狀目錄**對話方塊。

b 輸入新樹狀目錄。如需格式資訊，請參見步驟 4。

c 按一下**確定**。此樹狀目錄新增到表中。

若要編輯表中的現有樹狀目錄：

a 選擇表中的樹狀目錄。

b 按一下**編輯**。

c 進行必要的變更。

d 按一下**確定**。對表中的樹狀目錄進行了變更。

若要移除表中的現有樹狀目錄：

a 選擇表中的樹狀目錄。

b 按一下**移除**。

7 排序並不重要，但是由於以既定順序搜尋，所以將最常用的樹狀目錄放在各清單的前面是最高效的做法。如果要使用多個 LDAP 伺服器之間的提名，最好的排序是將位於主要伺服器上的樹狀目錄放在前面，其餘樹狀目錄以提名順序排列。若要調整表中的項目的位置：

a 選擇要移動的樹狀目錄。

b 按一下**向上**或**向下**箭頭，直到此項目移至所需的位置。

c 對每個要調整位置的樹狀目錄重複步驟 a 和步驟步驟 b。

8 **自動設定**按鈕使安全設備通過掃描一個或多個目錄查找包含使用者物件的所有樹狀目錄來自動設定**包含使用者的樹狀目錄**和**包含使用者群組**的樹狀目錄欄位。必須首先設定**主要網域**和**用於登入伺服器的使用者樹狀目錄**。

附註：很可能找到使用者登入不需要的樹狀目錄，推薦手動移除此類項目。

a 按一下**自動設定**。將顯示 **LDAP 使用者/群組樹狀目錄自動設定**對話方塊。

b 選擇：

- **附加到現有樹狀目錄** - 新樹狀目錄新增到現有設定
- **取代現有樹狀目錄** - 先移除目前設定的所有樹狀目錄，再新增新樹狀目錄

c 按一下**確定**。

附註：這可能需要一些時間。

提示：如果使用有提名的多個 LDAP/AD 伺服器，可以對每個伺服器重複此過程，相應地替換**要搜尋的網域**，並對隨後的各執行選擇**附加到現有樹狀目錄**。

9 按一下**套用**。

提名標籤

1 選擇**提名**標籤。

2 如果網路中使用多個 LDAP 伺服器，可能需要 LDAP 提名。勾選一個或多個以下核取方塊：

- **允許轉介** - 如果使用者資訊位於 LDAP 伺服器上，而不是設定的主要伺服器，則選擇此選項。預設啟用此設定。
- **在使用者驗證過程中允許連續的參考** - 如果各目錄樹狀目錄位於多個 LDAP 伺服器，則選擇此選項。
- **在目錄自動設定的過程允許連續的參考** - 選擇此選項在相同操作中從多個 LDAP 伺服器讀取目錄樹狀目錄。預設啟用此設定。
- **允許在網域搜尋中連續的參考** - 選擇此選項在多個 LDAP 伺服器中搜尋子網路域。預設啟用此設定。

3 按一下**套用**。

使用者和群組標籤

1 選擇**使用者和群組**標籤。

2 勾選**僅允許本機列出的使用者**核取方塊要求 LDAP 使用者還必須存在於安全設備本機使用者資料庫中才能允許登入。

3 勾選**可以通過複製 LDAP 使用者名稱在本機設定使用者群組成員身分**核取方塊允許通過本機使用者與 LDAP 使用者設定的交集確定群組成員身分（和權限）。

4 從**預設 LDAP 使用者群組**下拉功能表，選擇 LDAP 使用者所屬的安全設備上預設群組和在 LDAP 伺服器上設定的群組成員身分。

> **提示：**還可以使用 LDAP 指派群組成員身分（和權限）。通過在 LDAP/AD 伺服器上建立與內建群組名稱相同的使用者群組（例如**來賓服務**、內容篩選繞過、有限管理員），並將使用者指派到目錄中的這些群組或在安全設備上建立與現有 LDAP/AD 使用者群組名稱相同的使用者群組，在成功通過 LDAP 身分驗證後，會自動向使用者賦予群組成員身分。

如果 Active Directory 利用其返回使用者「隸屬於」屬性的獨特優勢，安全設備可以更高效檢索群組成員。

5 按一下**匯入使用者**按鈕，通過檢索 LDAP 伺服器中的使用者名稱，可設定 SonicWall 上的本機使用者。顯示 **LDAP 匯入使用者**對話方塊，其中列出了可匯入 SonicWall 的使用者名稱。

a 勾選您要匯入 SonicWall 裝置的每個使用者對應的核取方塊。

b 然後按一下**儲存勾選**。

從 LDAP 伺服器讀取的使用者清單可能很長，您可能不想全部匯入。清單中提供了**從清單刪除**按鈕及其他多種移除不需要使用者的方法。您可以使用這些選項將清單縮短到便於管理的大小，然後選擇要匯入的使用者。

SonicWall 上的使用者名稱與現有 LDAP 使用者名稱相同有利於在 LDAP 身分驗證成功後授予 SonicWall 使用者權限。

6 如果要在原則規則、CFS 原則等中使用使用者群組的名稱，則需要在 SonicWall 裝置上複製 LDAP 伺服器上的這些使用者群組的名稱。按一下**匯入使用者群組**按鈕可將使用者群組從 LDAP 伺服器匯入 SonicWall 裝置。將顯示**從 LDAP 匯入使用者群組**對話方塊。

a 選擇：

- **從 LDAP 目錄匯入使用者群組**（預設）
- **自動設定群組供依 LDAP 位置 (OU) 設定成員資格**

將顯示 **LDAP 匯入使用者群組**對話方塊。

b 勾選您要匯入 SonicWall 裝置的每個使用者群組對應的核取方塊。

c 然後按一下**儲存勾選**。

從 LDAP 伺服器讀取的使用者群組清單可能很長，您可能不想全部匯入。清單中提供了**從清單刪除**按鈕及其他多種移除不需要使用者的方法。您可以使用這些選項將清單縮短到便於管理的大小，然後選擇要匯入的使用者。

SonicWall 裝置上的使用者群組與現有 LDAP/AD 使用者群組的名稱相同有利於在成功 LDAP 身分驗證後授予 SonicWall 群組成員身分和權限。

另外，您也可以在 LDAP/AD 伺服器上手動建立與 SonicWall 內建群組名稱相同的使用者群組（例如「來賓服務」、「內容篩選繞過」、「有限管理員」），並將使用者指派到目錄中的這些群組。這還允許在成功 LDAP 身分驗證後授予 SonicWall 群組成員身分。

如果 Active Directory 利用其返回使用者「隸屬於」屬性的獨特優勢，SonicWall 裝置可以高效檢索群組成員。

7 若要啟用 LDAP 使用者群組鏡像，請勾選**本機鏡像 LDAP 使用者組**核取方塊。

在啟用 LDAP 使用者群組鏡像後，SonicWall 裝置會定期自動從 LDAP 伺服器匯入使用者群組和使用者群組嵌套（成員關係，其中群組是其他群組的成員），以建立與 LDAP 目錄中的使用者群組形成鏡像的本機使用者群組。

這些鏡像使用者群組在**使用者 > 本機群組**頁面中單獨列出，且它們的名稱中包含其所在的網域。可以在存取規則、CFS 原則等中選擇這些群組，就像其他本機使用者群組一樣，但是有一些限制，例如不能在 SonicWall 裝置上將其他使用者群組新增為成員，但它們可以成為其他本機使用者群組的成員，本機使用者也可以成為它們的成員。

LDAP 伺服器上為使用者群組成員的使用者會通過其本機鏡像群組自動接收任何存取權限。

可以匯入的最大使用者群組數受限於每個產品，如果由於超過最大數量限制，而導致無法匯入在 LDAP 伺服器上找到的所有群組，則會產生事件記錄。

> ⓘ **提示：**為了避免超過此限制，選擇僅匯入那些有成員的群組和/或設定篩選條件以避免匯入不需要的群組。若要獲取裝置嘗試鏡像的所有使用者群組的 XML 清單，在您的瀏覽器位址欄中輸入以下位址：
>
> `https://<ip-address>/ldapMirror.xml`。
>
> 還可以通過顯示此設定的工具提示，來確定使用者群組的最大數量。

從在**目錄**標籤的**包含使用者群組的樹狀目錄**表中設定的目錄樹狀目錄匯入群組（請參見第 158 頁「目錄標籤」）。可以在下面的**在子樹狀目錄上排除這些群組**表中設定篩選條件。

8 在選擇**本機鏡像 LDAP 使用者群組**後，**重新整理時間（分鐘）**自動變為可用。輸入兩次重新整理之間間隔的最大時間。預設值為 **5** 分鐘。

9 （可選）若要立即重新整理，請按一下**立即重新整理**按鈕。

10 選擇要鏡像的群組：

- **LDAP 伺服器上的所有使用者組**
- **僅那些擁有使用者或者群組的群組**（預設）

11 通過將子樹狀目錄新增到**在子樹狀目錄上排除這些群組**表，可在 LDAP 目錄中排除鏡像這些子樹狀目錄。可以在 LDAP 目錄中排除最多 32 個子樹狀目錄，位於這些子樹狀目錄中或之下的使用者群組都不會鏡像。

a 按一下**新增**按鈕。將顯示**新建樹狀目錄**對話方塊。

b 輸入新樹狀目錄。

c 按一下**確定**。此樹狀目錄新增到表中。

若要編輯表中的現有樹狀目錄：

a 選擇表中的樹狀目錄。

b 按一下**編輯**。

c 進行必要的變更。

d 按一下**確定**。對表中的樹狀目錄進行了變更。

若要移除表中的現有樹狀目錄：

a 選擇表中的樹狀目錄。

b 按一下**移除**。

12 排序並不重要，但是由於以既定順序搜尋，所以將最常用的樹狀目錄放在各清單的前面是最高效的做法。如果要使用多個 LDAP 伺服器之間的提名，最好的排序是將位於主要伺服器上的樹狀目錄放在前面，其餘樹狀目錄以提名順序排列。若要調整表中的項目的位置：

a 選擇要移動的樹狀目錄。

b 按一下**向上**或**向下**箭頭，直到此項目移至所需的位置。

c 對每個要調整位置的樹狀目錄重複步驟 a 和步驟步驟 b。

13 按一下**套用**。

LDAP 轉接標籤

1 選擇 **LDAP 轉接**標籤。

2 勾選**啟用 RADIUS 到 LDAP 轉接**核取方塊啟用 RADIUS 到 LDAP 的轉接。此選擇在預設情況下不啟用。

「RADIUS 到 LDAP 轉接」功能可用於拓撲結構，其中有包含 LDAP/AD 伺服器的中央站台和有遠端衛星站台通過可能不支援 LDAP 的安全設備與之相連的中央安全設備。在這種情況下，中央安全設備可以作為遠端安全設備的 RADIUS 伺服器執行，充當 RADIUS 和 LDAP 之間的閘道，並將自身的身分驗證請求中移至 LDAP 伺服器。

3 在**允許 RADIUS 用戶端連接透過**下，勾選相關的核取方塊，將新增原則規則以相應允許收到的 RADIUS 請求。選項有：

- **受信任區域**
- **WAN 區域**（預設）
- **公用區域**
- **無線區域**
- **VPN 區域**（預設）

4 在 **RADIUS 共用密碼**欄位中，輸入所有遠端安全設備共用的共用密碼。

5 在用於舊版使用者的使用者群組欄位中，定義與舊版使用者對應的使用者群組：

- **用於舊版 VPN 使用者的使用者群組**
- **用於舊版 VPN 用戶端使用者的使用者群組**
- **用於舊版 L2TP 使用者的使用者群組**
- **用於舊版使用者的群組網際網路存取**

對於執行不支援使用者群組的非增強版韌體的遠端 SonicWall 裝置，這些設定允許裝置的互操作。在一個指定使用者群組中的使用者通過身分驗證後，將通知遠端 SonicWall 裝置賦予此使用者相應的權限。

附註：根據成員身分向名稱為「內容篩選繞過」和「有限管理員」的使用者群組返回「繞過篩選條件」和「有限管理能力」權限，這些設定不可設定。

6 按一下**套用**。

測試標籤

1 選擇**測試**標籤。

測試頁面允許通過使用指定的使用者和密碼登入憑證嘗試身分驗證來測試設定的 LDAP 設定。將顯示為此使用者在 LDAP/AD 伺服器上設定的所有使用者群組成員身分和/或成框架 IP 位址。

2 在**使用者名稱**和**密碼**欄位，輸入您設定的 LDAP 伺服器的有效 LDAP 登入名稱。

3 選擇**密碼驗證**或 **CHAP**（質詢握手身分驗證協定）。

附註：CHAP 僅適用於支援使用 LDAP 檢索使用者密碼的伺服器，在某些情況下，還要求設定 LDAP 伺服器以反向儲存密碼。CHAP 不適用於 Active Directory。

4 按一下**測試**。從 LDAP 伺服器返回的狀態和資訊顯示在**測試狀態**、**來自 LDAP 的訊息**和**返回的使用者屬性**欄位。

5 按一下**套用**。

6 按一下**確定**。

9

管理驗證分割區

關於驗證分割

主題：

關於使用者驗證分割

附註：如需本節中所使用之術語的定義，請參閱本節中使用的術語和縮寫詞表格。

SonicWall 安全設備在您管理多個非互連網域的環境中提供 LDAP、RADIUS 及/或單一登入 (SSO) 驗證的機制。這樣的環境需要透過下列特定媒介，以驗證特定網域中的使用者:

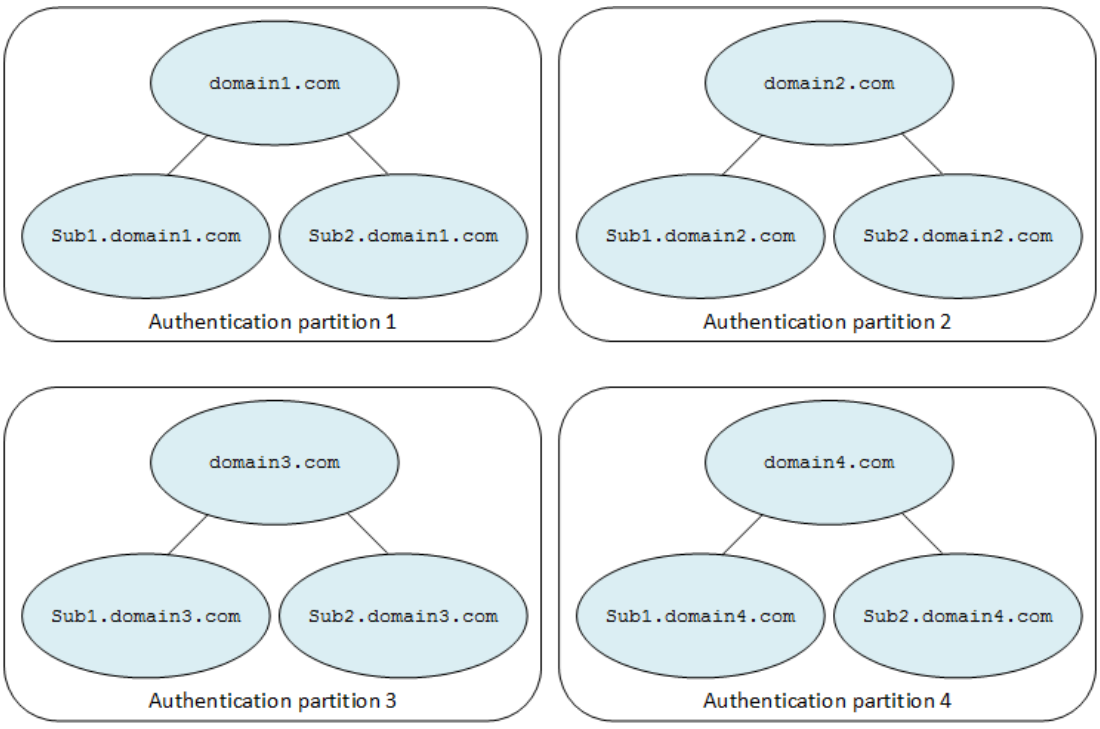
- 該網域的 LDAP/RADIUS 伺服器
- 位於該網域中的 SSO 代理

此類環境的機制是使用者驗證分割，其表示:

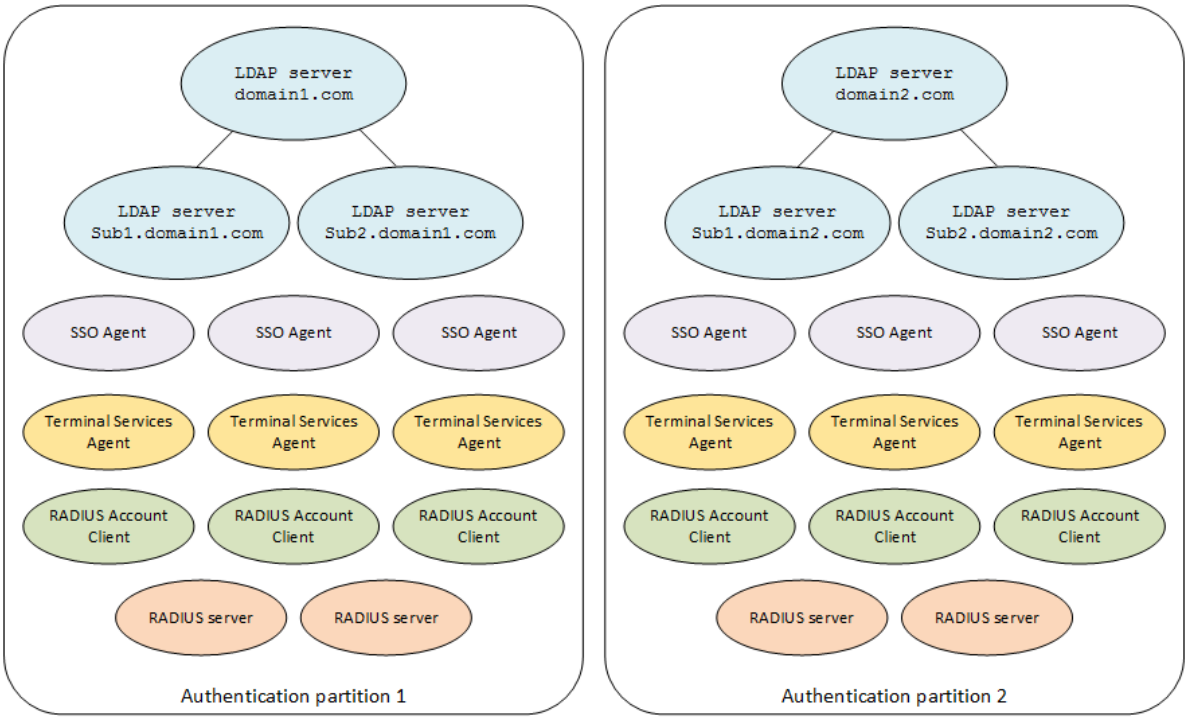
- 首先，將您的網路分割成獨立的分割區，每個分割區都有它自己的驗證伺服器/代理/用戶端。
- 接著，根據使用者所在的驗證分割區，對應相關驗證裝置 (伺服器/代理/用戶端) 驗證每個使用者。使用者分割區是依據下列情況選取:
    - 將使用者網域名稱與網域中設定的名稱進行比對。
    - 如果使用者的網域名稱無法使用，則根據分割區選取原則設定其實體位置。

驗證分割區通常會對應至一個或多個網域；例如，在 Windows 網域中，分割區通常會對應至 Active Directory 樹系。每個分割區有獨立的 LDAP 伺服器、RADIUS 伺服器、SSO 代理，及/或終端服務代理 (TSA)。參見驗證分割區和透過中央站台和遠端站台安裝。

驗證分割區



分割區內容



本節中使用的術語和縮寫詞

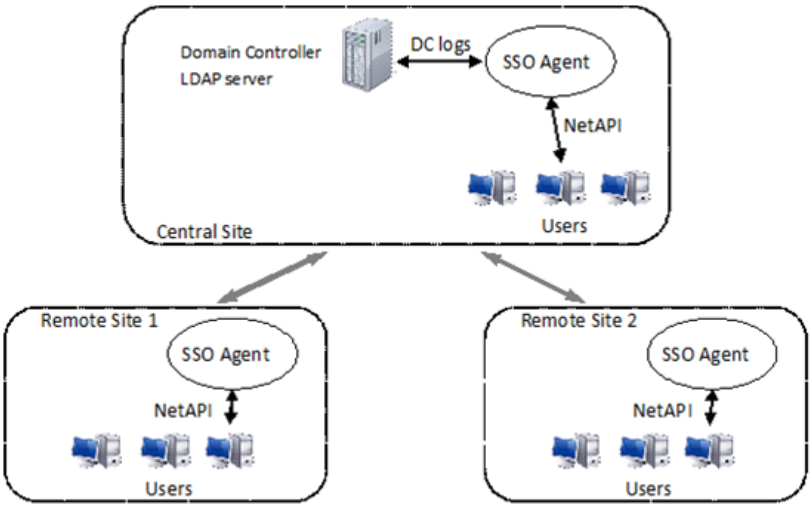
驗證分割	網路的其中一部分具有自己的驗證伺服器/代理/用戶端，與網路的其他部分分開
DC	網域控制器
LDAP	輕量型目錄存取通訊協定
RADIUS	遠端驗證撥入使用者服務
SSO	單點登入
TSA	終端服務代理

關於子分割區

驗證分割區選取用於驗證特定使用者的 LDAP 伺服器、RADIUS 伺服器、SSO 代理，以及 TSA。除了將伺服器和代理指派給分割區以外，可能有一些情況需要進一步將某些分割區指派給分割區中不同的使用者子集合。如果需要使用特定代理，子分割區允許為某些分割區使用者的子集合指派特定代理。如果驗證分割區設為其他分割區的子分割區，則代理專用於頂層或父級，驗證分割區的使用者可指派至子分割區。會在相關聯時使用子分割區的代理，但是可視需要使用父分割區的伺服器和代理。

例如，透過中央站台和遠端站台的安裝具有位於中央站台的網域控制器 (DC)/ LDAP 伺服器。不過，存取原則會防止位於中央站台的 SSO 代理存取遠端使用者電腦。對於使用 NetAPI 或在此拓撲中運作之 WMI 的 SSO，除了位於中央站台的代理以外，必須在每個遠端站台設置一個或多個 SSO 代理；請參閱透過中央站台和遠端站台安裝。對於 NetAPI/WMI，SSO 代理會直接與使用者電腦對話，而 DC 安全性記錄中的使用者識別會使用網域控制器的 SSO 代理。

透過中央站台和遠端站台安裝



頂層分割區的子分割可解決下列問題:

- 告知設備每個單獨站台的 SSO 代理用於該處使用者的 NetAPI 或 WMI 識別。
- 使用中央站台的 SSO 代理與 LDAP 伺服器，為 DC 記錄識別和使用者群組查詢所有站台的所有使用者。

使用在遠端站台指派給子分割區的代理，每個遠端站台可設定為中央站台的子分割區。使用不同的選取原則 (定義每個分割區之使用者子集合的位置)，一個或多個分割區可設定為父分割區的子分割區。在透過中央站台和遠端站台安裝中，整個安裝是一個分割區，而遠端站台是該分割區內的每個子分割區。從子分割區選取相關代理以識別遠端站台的使用者之後，會透過父分割區的 LDAP 伺服器查找使用者的群組成員資格。

子分割區的某些特殊情況為：

- LDAP 伺服器無法指派給子分割區。如果子分割區對應至擁有其自己的 LDAP 伺服器的子網域，則可將這些伺服器指派給父分割區。LDAP 伺服器訊息會將要求轉介給子網域。
- 對於 RADIUS 伺服器，子分割區會使用指派給該子分割區的伺服器或指派給父分割區的伺服器，但並非兩者均使用。如果 RADIUS 伺服器指派給子分割區，則這些伺服器會用於該子分割區中的使用者；否則，會使用父分割區的伺服器。
- 透過使用 NetAPI 或 WMI 的 SSO 代理 (以及從網域控制器記錄讀取)，如果子分割區及其父級有代理，則只有子分割區自己的 SSO 代理會用於位於子分割區中使用者的 NetAPI/WMI 識別；子分割區的 SSO 代理涉及直接存取使用者電腦。如果已設定子分割區的 SSO 代理，網域控制器記錄讀取可以由父分割區及/或子分割區中的 SSO 代理來完成。

將伺服器、代理與用戶端與子分割區搭配運作

通常，指派給子分割區的任何伺服器、代理及/或用戶端會用於該子分割區中的使用者，但除此之外，也會使用父分割區的某些特定伺服器、代理，及/或用戶端；請參閱將伺服器、代理與用戶端與子分割區搭配使用表格。

將伺服器、代理與用戶端與子分割區搭配使用

伺服器、代理、用戶端	使用
LDAP 伺服器	只能指派給頂層分割區，而不能指派給子分割區。 如果子分割區對應到擁有它自己的 LDAP 伺服器的子網域，則可將這些伺服器指派給父分割區，而 LDAP 的轉介/參照機制會將要求轉介給子網域的伺服器。 子分割區可以在這裡對應到擁有它自己的 LDAP 伺服器的子網域，不過，您可能會發現將這些伺服器指派至子分割區是更合乎邏輯的做法，而且這是允許的。指派到子分割區的伺服器會內部連結至父分割區。
RADIUS 伺服器	子分割區會使用指派給該子分割區的 RADIUS 伺服器或指派給父分割區的伺服器，但並非兩者均使用。如果 RADIUS 伺服器指派給子分割區，則這些伺服器會用於該子分割區中的使用者；否則，會使用父分割區的伺服器。
SSO 代理	使用 NetAPI 或 WMI 時，代理需要位於可以直接存取使用者 PC 的位置，從 DC (網域控制器) 記錄讀取時，需要存取 DC。SSO 代理可設定為執行兩項活動。 使用 DC 記錄與 NetAPI/WMI 時，SonicWall 安全設備控制要使用的項目及使用順序。安全設備： 1 讓代理在每個 DC 顯示的 DC 記錄中查找使用者。 2 如果記錄中找不到使用者，請另外做出後續要求嘗試 NetAPI/WMI。 使用子分割區時，此機制操作如下，可識別位於子分割區的使用者: 1 如果指派給子分割區的任何 SSO 代理已啟用 DC 記錄，則要求會傳送給這些 SSO 代理，以查找其 DC 記錄中的使用者。 2 如果步驟 1 中未識別使用者，而且如果指派給父分割區的任何 SSO 代理已啟用 DC 記錄，則要求會傳送給這些 SSO 代理，以查找其 DC 記錄中的使用者。 3 如果步驟 2 中未識別使用者，而且如果指派給子分割區的任何 SSO 代理已啟用 NetAPI 或 WMI，則要求會傳送給其中一項以識別使用者。 **附註：**對於位於子分割區的使用者，不會透過父分割區中的 SSO 代理嘗試 NetAPI/WMI。如果在已啟用 NetAPI 或 WMI 的情況下，沒有指派給子分割區的代理，則不會嘗試進行驗證。
TSA 與 RADIUS 計費用戶端	指派這些代理/用戶端傳送使用者的分割區僅影響用於使用者群組查找的 LDAP 伺服器選擇。由於父分割區的 LDAP 伺服器也用於其所有子分割區，因此可以將 TSA 和 RADIUS 計費用戶端指派給任一個子分割區。唯一的區別是為他們的使用者顯示哪個分割區，並且根據其實體位置將使用者指派給這些分割區。 **附註：**這僅適用於未提供網域的情況。

關於分割區間使用者漫遊

如果已設定網路拓撲以允許使用者從登入分割區存取他們自己的分割區網域伺服器，那麼登入某分割區中的網域使用者即可漫遊，並從不同分割區的實體網路進行連接。如果在這種情況下使用 SSO 代理，則設備會根據使用者的實體位置 (而非其主分割區的代理) 選取本機分割區的 SSO 代理。

本機分割區的 SSO 代理無法從網域控制器記錄中識別漫遊使用者，因為代理未從正確的網域控制器讀取。如果代理具有正確的權限，則可以透過 NetAPI 或 WMI 識別漫遊使用者，這需要 Windows 網域間信任。因此，當安全設備從 SSO 代理取得使用者名稱時，安全設備會檢查指定網域所在的分割區，並允許其根據使用者的實體位置覆寫最初選定的分割區。

識別漫遊使用者並設定其存取權限的程序是:

1 登入「網域 1」(在「分割區 1」中) 的使用者從「分割區 2」中的子網路連線；該使用者的分割區最初記錄為「分割區 2」。

2 如果「分割區 2」代理正在讀取網域控制器記錄，則會先傳送要求以檢查這些記錄。這些要求找不到未登入「分割區 2」網域的使用者。

3 要求傳送至「分割區 2」中的 SSO 代理以嘗試 NetAPI。代理會執行此操作，並將該使用者識別為來自「網域 1」的使用者。

4 安全設備會看見「網域 1」是在「分割區 1」中，而且會將使用者的分割區切換為「分割區 1」。然後，安全設備會透過「分割區 1」中的 LDAP 伺服器查找使用者的群組成員資格。

關於驗證分割區選取

主題：

選取原則

網路拓撲會影響 SonicOS 在網路上尋找驗證分割區的方式。SonicOS 提供幾個選項可尋找及選取使用者的分割區。

選項

選取依據	每個驗證分割區
IP 位址	透過分割區設定中的位址物件 (網路、範圍或群組) 對應至一組 IP 位址。
網路介面	透過分割區設定中選取的一個或多個介面，對應至要存取的網路。
網路區域	對應至分割區中選取的一個或多個網路區域。
使用者名稱網域元件	一個或多個網域的成員，並透過比對使用者在登入時提供的網域名稱加以選擇。此選項要求使用合格名稱的使用者登入，例如，`domain\user` 或 `user@domain.com`。 提供網域名稱時，此選項會覆寫上述依據位置的的選項。 此選項應該用於驗證 GVC、L2TP 及 SSL VPN 用戶端使用者；請參閱第 170 頁「遠端使用者」。 **附註：**對於 SSO 代理驗證，應該使用其中一個依據位置的選項，因為 SonicWall 安全設備需要在流程開始時衍生分割區，以選取要使用的 SSO 代理，而且此時安全設備還沒有使用者的登入名稱；請參閱第 168 頁「關於分割區間使用者漫遊」。

這些選項設定為一組單獨的選取原則，每個分割區設定一個或多個原則，以定義選取該分割區的選取方式。在使用者驗證期間，如果未提供任何網域，則會透過與存取規則比對非常類似的方式，將區域、介面及 IP 位址和設定的原則進行比對以選取分割區，指定預設分割區的預設選取原則對於未比對明確設定原則的任何內容都是全面性的。預設分割區一開始命名為「預設」，但可以重新命名，或預設選取原則可設為其他分割區，之後可以刪除自動建立的「預設」。

遠端使用者

選擇用於 GVC/L2TP 用戶端和 SSL VPN 使用者之驗證分割區的處理方式不同，因為這些遠端使用者會連線到驗證分割區，而不是來自驗證分割區。安全設備需要知道這些使用者的驗證分割區，才能選取正確的 LDAP 伺服器以查找其使用者群組成員資格，並從中查找其可存取的子網路。有兩個選項可驗證遠端使用者:

- 依使用者網域元件進行選擇，並要求遠端使用者提供包括網域的合格名稱。
- 有多個 WAN 介面及/或 WAN 區域，而且每個驗證分割區的使用者都連接到不同的公用 IP 位址。然後使用遠端使用者經過的 WAN 介面或區域來選取驗證分割區，而不要求遠端使用者提供合格的使用者名稱。

  附註：對於 GVC/L2TP 使用者，有獨立的 WAN 區域可讓每個區域使用不同的群組 VPN 原則，因此，可能更加安全地強制存取正確的驗證區域。

有多個 WAN 介面時，可以設定分割區選取原則以透過 WAN 介面選取遠端存取的分割區。如果只有一個 WAN 介面，則可設定一個特殊選取原則，且在無法從提供的使用者名稱衍生時，選取遠端存取的預設分割區。

附註：如果未設定選取原則，遠端存取使用者需要提供合格的使用者名稱，除非驗證使用者的伺服器已指派至依預設選取的分割區。

使用者登入的設備通知

如果 SonicWall 安全設備收到代理/用戶端的使用者登入通知，卻沒有為他們傳送識別要求 (例如，終端服務、RADIUS 計費，以及來自 SSO 代理讀取 DC 通知的登入通知)，安全設備不需要知道用於選擇代理/用戶端的驗證分割區，因為它會傳送要求到 SSO 代理。不過，若要選取正確的 LDAP 伺服器以查找其使用者群組成員資格，安全設備不需要知道這些使用者的驗證分割區。若出現使用者名稱網域元件，可藉由其進行選擇，或將每個這樣的代理/用戶端手動指派給驗證分割區來選擇。

Web 使用者登入

當使用者透過 SonicWall 安全設備的 Web 登入入口網站登入時，無論他們來自哪裡，我們皆想像其使用任何帳戶名稱。通常，會根據使用者登入來源來選取驗證分割區 (請參閱第 169 頁「選取原則」)，但如果使用者提供包含該網域的使用者名稱，則可以藉由使用包含網域的合格使用者名稱來登入，以覆寫該使用者名稱，進而選取驗證分割區。

CLI 登入

當使用者使用內建管理帳戶透過 CLI 登入時，分割是不相關的，因為該分割一律是在本機驗證。但是，使用透過 LDAP 或 RADIUS 驗證的其他管理員帳戶時，需要知道分割區以選取伺服器進行驗證。有三種不同的情況:

在主控台連接埠上登入	其中沒有 IP 位址來衍生分割區，所以需要 IP 位址時，使用者需要使用合格的使用者名稱登入。
來自防火牆內部的本機 SSH 連線	使用者所在的驗證分割區是透過 SSH 連線的來源 IP 位址選取，依照第 169 頁「選取原則」。
來自防火牆外部的遠端 SSH 連線	分割區選擇不是根據使用者的位置，但是在可能的情況下，可根據要連線的 WAN 介面，依遠端用戶端使用者的需求加以選擇；請參閱第 169 頁「選取原則」。

如果已根據使用者名稱網域元件設定 (請參閱第 169 頁「選取原則」)，那麼在任何情況下，使用者可以藉由透過合格的使用者名稱 (其包含來自選定驗證分割區的網域) 進行登入，以覆寫該使用者。也可以設定一個特殊選取原則，在無法從提供的使用者名稱衍生時，選取主控台連接步登入的預設分割區。

附註：如果未設定選取原則，使用者需要提供合格的使用者名稱，才能在主控台連接埠上登入，除非驗證使用者的伺服器已指派至依預設選取的分割區。

每個分割區的使用者驗證設定

在某些情況下，可能需要在不同分割區中以不同方式設定管理使用者驗證的特定設定。例如，如果某個分割區只有 RADIUS 伺服器，而另一個分割區只有 LDAP 伺服器，則必須在第一個分割區中選取 RADIUS，在另一個分割區中選取 LDAP，以進行使用者驗證。

依預設，所有此類設定全域適用，並且僅限於使用者驗證方法和單一登入方法。這些設定僅適用於頂層分割區；對於子分割區，會套用其父分割區的驗證設定。

關於多個 LDAP 伺服器的延伸支援

分割需要多個 LDAP 伺服器。可設定多個主要 LDAP 伺服器，每個驗證分割區有一個伺服器，還有一個額外伺服器的清單。如需關於多個 LDAP 伺服器與如何設定這些伺服器的詳細資訊，請參閱第 139 頁「關於多個 LDAP 伺服器的延伸支援」。

每個分割區的 DNS 伺服器與分割 DNS

無論是否具有驗證分割區，通常需要使用網域自己的 DNS 伺服器來解析網域中的裝置名稱，偶爾也可能需要使用不同的外部 DNS 伺服器來解析外部主機名稱。但是，多個驗證分割區通常需要使用不同的 DNS 伺服器來解析不同分割區中的主機名稱。

具有分割 DNS 功能的 DNS Proxy 允許設定與不同網域名稱相關聯的不同 DNS 伺服器。此功能與 DNS Proxy 是分開的，因此安全設備可以直接使用該功能來解析網域中的裝置名稱，而不需要啟用 DNS Proxy，包括多個具有驗證分割的不相關網域。如需關於分割 DNS 的詳細資訊，請參閱第 164 頁「管理驗證分割區」。

關於 RADIUS 驗證

使用 RADIUS 驗證還需要考慮一些其他注意事項，因為 SonicWall 安全設備無法像使用 LDAP 那樣保證衍生使用者的網域，也不能確保在 RADIUS 屬性中傳回的使用者群組網域。因此，安全設備可以尋找網域，以選取正確的網域使用者和使用者群組物件，且安全設備會使用 RADIUS 驗證嘗試下列操作以瞭解使用者的網域:

1. 讓使用者在登入時提供包含網域的合格使用者名稱。如果 RADIUS 伺服器透過 RADIUS 屬性 (篩選 ID 或 SonicWall 廠商專用屬性) 傳回使用者群組，則將其設定為傳回提供群組的完整名稱 (包括其網域)。
2. 在透過 RADIUS 驗證使用者之後，使用 LDAP 進行使用者群組查找 (此為慣用方法)。接著，如果使用者未使用其使用者名稱提供網域，可以從 LDAP 搜尋中學習，以找出其使用者群組。
3. 如果兩者都失敗，那麼當使用者從位於其實體位置的 IP 位址登入時，可以從驗證分割區查找該網域，但只有在每個分割區只有一個網域的情況下，才能確定提供使用者網域；因此，若要使用此方法，每個子網域皆必須有一個單獨的子分割區。

   附註：這對於跨網域的使用者群組成員資格不會產生作用。

總之，使用 RADIUS 驗證的最佳選擇是使用 LDAP 進行使用者群組查找。如果不可能執行 (無 LDAP 伺服器)，則下一個最佳選擇是讓 RADIUS 伺服器利用 RADIUS 屬性傳回完整的使用者群組名稱。

如果這些無法用來衍生從 RADIUS 傳回的使用者群組網域，則必須將使用者/使用者群組物件設定為在任何網域中進行比對。

從非分割設定升級

在沒有驗證分割的情況下，從現有設定啟動時，如果啟用分割:

- 會使用其中所有現有的伺服器、代理及用戶端，建立名稱為**預設**的單一驗證分割區。
- 設定單一預設分割區選取原則會設為選取**預設**分割區作為所有的預設分割區。

以此為基礎，可以新增分割區，而且相關的伺服器、代理及用戶端將輕鬆地從預設分割區移至這些分割區，或予以新增。

設定驗證分割區與原則

使用者 > 分割區頁面可讓您建立驗證分割區清單和原則清單以供選擇。對於每個分割區，您可以設定:

- 驗證分割區的名稱 (例如，其對應的網域或樹系名稱)。
- 分割區包含的網域。
- 為使用者選取驗證分割區的方式 (例如，設為單獨的分割區選取原則)。

設定驗證分割區和分割區選取原則之前，您可以從**監控 > 目前狀態 > 使用者工作階段 > 使用中使用者**頁面確定分割區中的使用者位置。

設定了驗證分割區之後，會在各種伺服器/代理/用戶端設定中新增選項，以便在新增/編輯伺服器、代理或用戶端時，可以選取驗證分割區。您可以從**使用者 > 設定**頁面設定伺服器、代理及用戶端。

主題：

- 第 172 頁「顯示及篩選使用者/分割區」
- 第 174 頁「設定及管理分割區」
- 第 186 頁「設定分割區選取原則」
- 第 190 頁「為驗證分割設定伺服器、代理及用戶端」

顯示及篩選使用者/分割區

監控 | 使用者工作階段 > 使用中使用者頁面顯示每個使用者所在的分割區。

附註：如需關於此頁面的詳細資訊，請參閱您的 SonicWall 安全設備的 *SonicOS 監控*。

主題：

- 第 173 頁「檢視使用者資訊」
- 第 173 頁「篩選使用者」

檢視使用者資訊

您可以檢視各種類別的使用者數目:

- 使用中/非使用中
- SSO 使用者 - 依識別方法
- 用戶端使用者 - 依用戶端類型
- Web 使用者
- SSL VPN 入口網站使用者

若要檢視此資訊，請按一下**使用中使用者工作階段**表格下方的**統計資料**圖示。隨即顯示**使用者計數**快顯對話方塊:

篩選使用者

篩選欄位可篩選分割區，以便僅顯示選定分割區中的使用者。您可以藉由指定一個或多個完整或部分使用者名稱、網域、IP 位址及/或使用者類型，以搜尋使用者。在項目前面使用驚嘆號 (!) 以排除使用者。組合字串時，若要比對:

- 任何列出的項目，使用逗號來分隔項目；也就是說，a,b 包含符合 a 或 b 的使用者
- 任何列出的項目，使用分號 (;) 來分隔項目；也就是說，a;b 包含同時符合 a 和 b 的使用者

若要搜尋終端伺服器使用者，請輸入 user-num=*usernumber*。類型篩選條件會比對**類型/模式**欄中的文字，包括當滑鼠懸停在上方時所顯示的任何文字。支援 IPv6 位址，但僅限於完全符合；例如，ip=2012::1,!ip=2012::1，或其他項目的組合，如篩選範例表格中所示。

篩選範例

name=bob	name=bob,john,sue	domain=mydomain
ip=192.1.1.1	ip=192.1.1.1,192.1.1.2	ip=192.1.1.0/24
type=config mode	type=sso,web	type=sso;netapi
type=sso;from logs on domain controller 192.1.1.10		
partition=somePartition	group=Trusted Users	
name=bob;ip=192.1.1.1 *(以比對名稱與 IP 位址)*		
!name=bob !ip=192.1.1.1 *(以排除使用者)*		

您也可以僅使用簡單字串；例如: bob 192.1.1.1 mydomain

設定及管理分割區

主題：

- 第 174 頁「系統安裝 | 使用者 > 分割區頁面」
- 第 178 頁「啟用/停用驗證分割」
- 第 179 頁「新增分割區和子分割區」
- 第 180 頁「刪除分割區和子分割區」
- 第 182 頁「指派伺服器、代理及用戶端」
- 第 184 頁「編輯分割區」

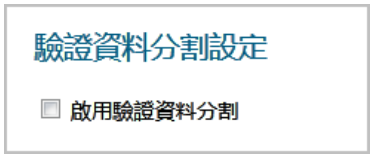
系統安裝 | 使用者 > 分割區頁面

系統安裝 | 使用者 > 分割區頁面有三個區段:

- 第 175 頁「驗證分割設定區段」
- 第 175 頁「驗證分割區區段」
- 第 177 頁「分割區選取原則區段」

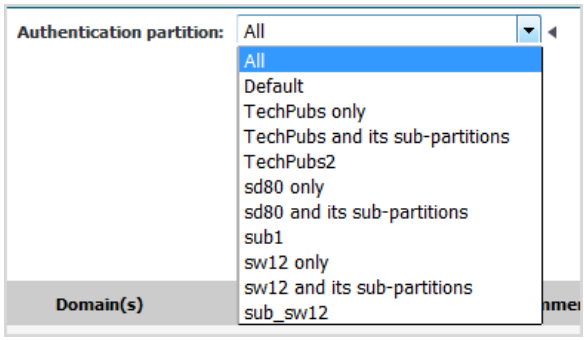
驗證分割設定區段

此區段可啟用/停用驗證分割。如果停用驗證分割，則不會顯示其他區段。



已啟用驗證分割時，**驗證分割區**和**驗證選取原則**這兩個區段皆會顯示。

啟用分割時，也會在頁面頂部顯示**驗證資料分割**下拉功能表，您可以從中選取**使用者 > 設定**和**使用者 > 本機使用者和群組**頁面中的設定也會套用的分割區。預設為**全部**，意即設定會套用至所有分割區。



驗證分割區區段

附註：此區段僅在驗證分割啟用時才顯示。

此區段顯示驗證分割區的表格，並可讓您建立、編輯、刪除及管理分割區。您在此處設定的分割區會控制哪些使用者使用哪些驗證。

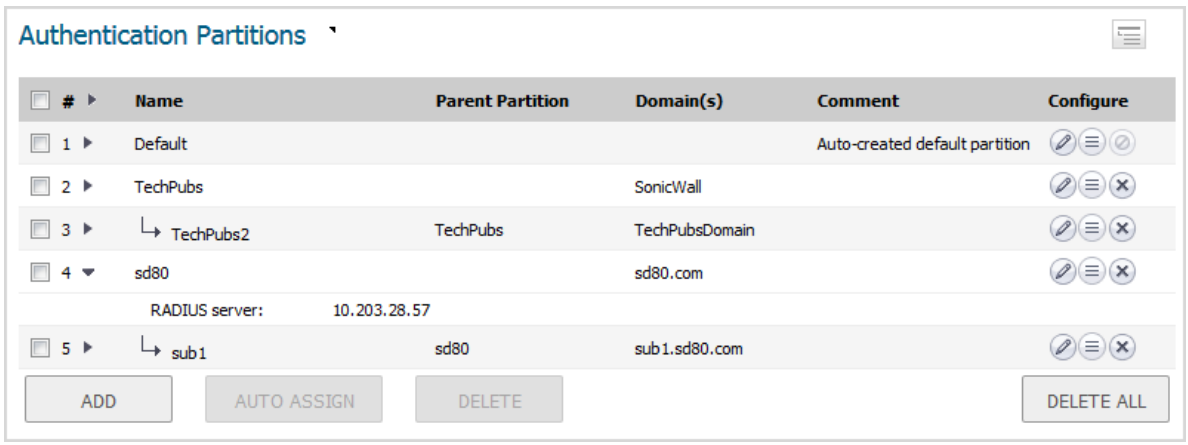
您可以展開分割區的樹狀目錄，以顯示指派到該分割區的伺服器、代理及用戶端。

分組子分割區 圖示	在分組子分割區及其父級驗證分割區之間進行切換，或取消分組子分割區，並利用頂層分割區對其進行排序。 **附註：**分組的子分割區緊隨其父分割區後顯示，具有**連結** ↳ 圖示，表示它們是子分割區。
選擇核取方塊	可讓您在表格中選取一個或多個分割區及/或子分割區。選取表格標題中的核取方塊，會選取**預設**分割區以外的所有項目。
名稱	指定驗證分割區的名稱。名稱前面的**連結** ↳ 圖示表示子分割區。
父分割區	指定子分割區的父級驗證分割區。父分割區的此欄為空白。
網域	指定分割區或子分割區所屬的網域。**預設**分割區的此欄為空白。
註解	顯示新增分割區時包含的註解。**預設**分割區的註解為**自動建立的預設分割區**。
設定	顯示分割區的**編輯**、**選擇** ≡，以及**刪除**圖示 **附註：****預設**分割區的**編輯**與**刪除**圖示顯示為灰色。
新增	顯示**新增驗證分割區**快顯對話方塊，以新增驗證分割區或子分割區。
自動指派	根據其 IP 位址或主機名稱，將任何未指派的 LDAP 伺服器、RADIUS 伺服器、SSO 代理、TSA 以及 RADIUS 計費用戶端自動指派給相關分割區。 **附註：****自動指派**與**刪除**按鈕顯示為灰色，除非已選取至少一個分割區或子分割區。
刪除	刪除選定的驗證分割區或子分割區。 **附註：**您無法刪除**預設**分割區。
全部刪除	從表格中刪除所有分割區和子分割區，除了**預設**分割區以外。

此表格中永遠有一個驗證分割區，即自動建立的**預設**分割區。您無法刪除此分割區。不過，您可以編輯該分割區，並為該分割區選取伺服器、代理及用戶端，以及子分割區。如果您停用驗證分割，所有 LDAP 伺服器、SSO 代理、TSA，以及 RADIUS 計費用戶端會重新指派至**預設**分割區；當您重新啟用驗證分割時，必須重新指派。RADIUS 伺服器不受影響，並且保留其指派的分割區。

展開樹狀目錄

展開驗證分割區的樹狀目錄，顯示指派至該分割區的伺服器、用戶端及代理:

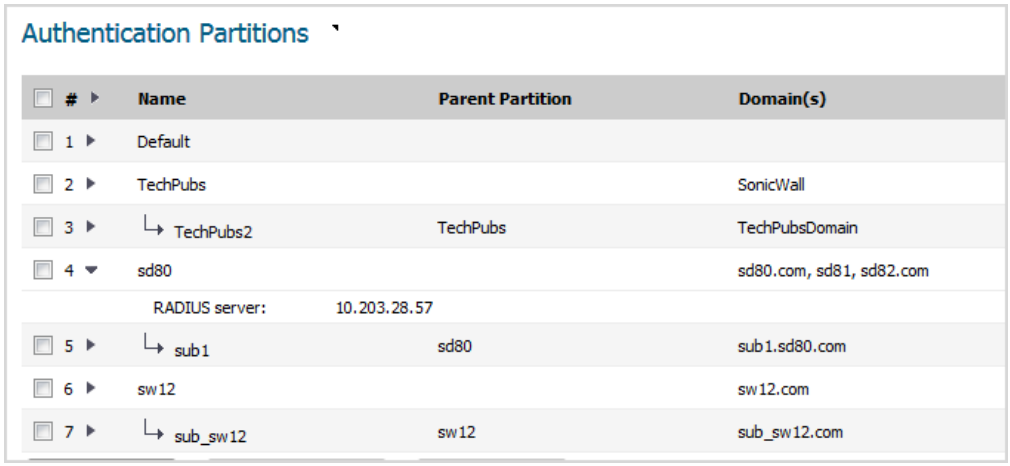


您可以展開下列的樹狀目錄:

- 所有表格項目，方法是按一下標題中核取方塊旁的三角形。
- 一個或多個表格項目，方法是按一下每個**展開**圖示。

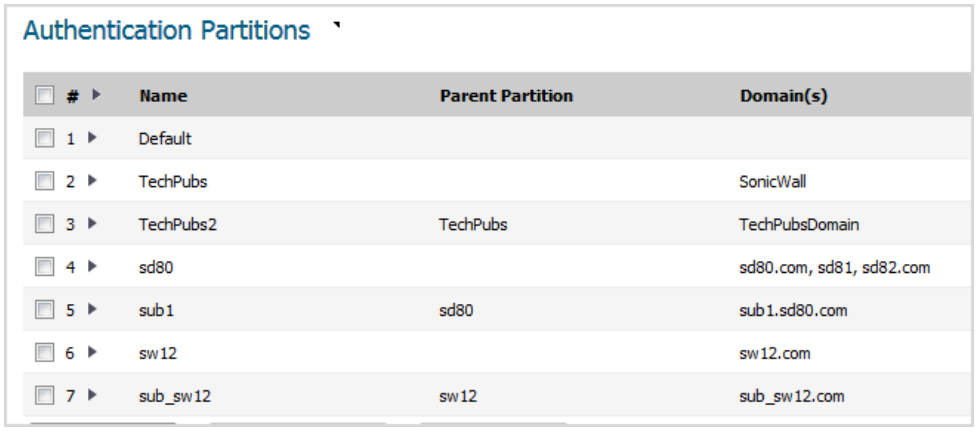
顯示階層

依預設，子分割區會顯示在父分割區下方，而且在子分割區名稱前面有一個**連結**圖示



。

您可以按一下**群組** 圖示，顯示與其父分割區層級相同的子分割區。



分割區選取原則區段

附註：此區段僅在驗證分割啟用時才顯示。

此區段顯示影響驗證分割區選擇的原則表格，並可讓您建立、刪除和編輯原則，以及變更您建立之任何原則的優先順序。這些原則根據要驗證之使用者的實體位置來選取**驗證分割區**表格中的分割區。當驗證的使用者其網域名稱無法用於比對選定分割區中的網域名稱時，將根據這些原則設定的實體位置來選取使用者的分割區。這些選取原則也適用於根據這些裝置的實體位置，將驗證裝置自動指派給分割區。

無法刪除「預設」分割區的「預設」選取原則，也無法變更其優先順序；該原則的優先順序一律是最低的。

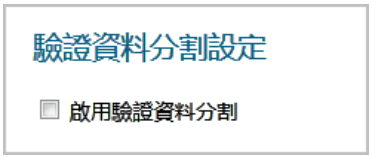
選擇核取方塊	可讓您在表格中選取一個或多個項目。選取表格標題中的核取方塊，會選取**預設**選取原則以外的所有項目。
優先順序	根據您指派的優先順序，排序分割區選取原則。按一下**優先順序箭頭**  ，隨即顯示**變更選取原則優先順序**快顯對話方塊。您無法變更**預設**選取原則的優先順序；其優先順序一律是最低的。
區域	顯示指派至分割區選取原則的區域。
介面	顯示指派至驗證分割區選取原則的介面。
分割區	顯示選取原則適用的驗證分割區。
註解	顯示建立或編輯選取原則時所輸入的註解。**預設**分割區的選取原則具有註解**自動建立的預設原則**。
設定	顯示**編輯**與**刪除**圖示，其針對預設原則顯示為灰色。
新增	顯示**新增分割區選取原則**快顯對話方塊，以針對驗證分割區或子分割區新增選取原則。
刪除	刪除選定的一個或多個原則。 **附註：**您無法刪除**預設**分割區的原則。**刪除**會顯示為灰色，除非已選取至少一個原則。
全部刪除	刪除**預設**分割區的原則以外之表格中的所有原則。

此表格中永遠有一個選取原則，即針對**預設**分割區自動建立的預設原則。除了選擇其適用的分割區以外，您無法選取該原則、刪除該原則、變更其優先順序，或編輯該原則。

啟用/停用驗證分割

若要啟用分割:

1 移至**使用者 > 分割區**頁面。



2 在**驗證分割設定**區段中，選取**啟用驗證分割**。隨即顯示**驗證分割區**和**分割區選取原則**區段。

若要停用分割:

1 移至**使用者 > 分割區**頁面。

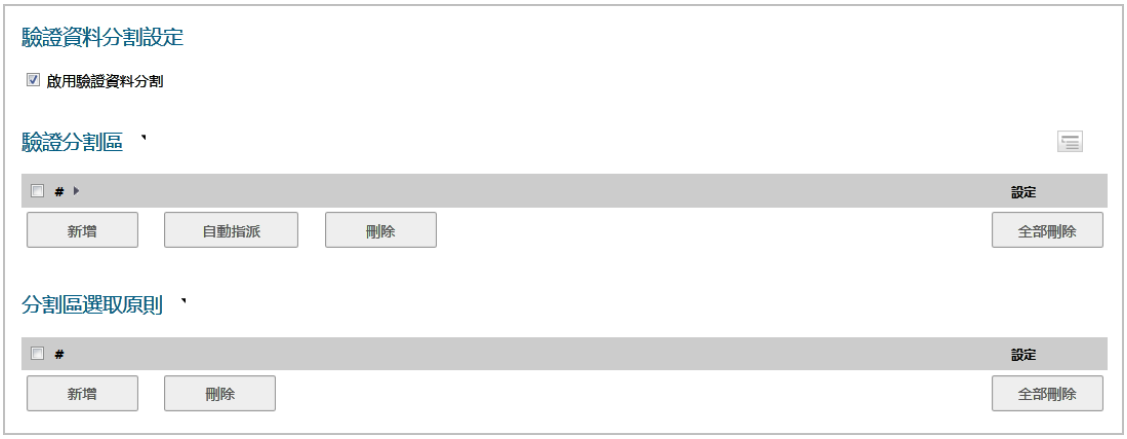
2 在**驗證分割設定**區段中，取消選取**啟用驗證分割**核取方塊。**驗證分割區**和**分割區選取原則**區段不再顯示。

重要：當您停用驗證分割時，所有分割的 LDAP 伺服器、SSO 代理、TSA，以及 RADIUS 計費用戶端皆會移至**預設**驗證分割區；RADIUS 伺服器不會受到影響，並保留在其設定的驗證分割區。如果之後啟用驗證分割，則需要重新設定所有其他伺服器、代理和用戶端。

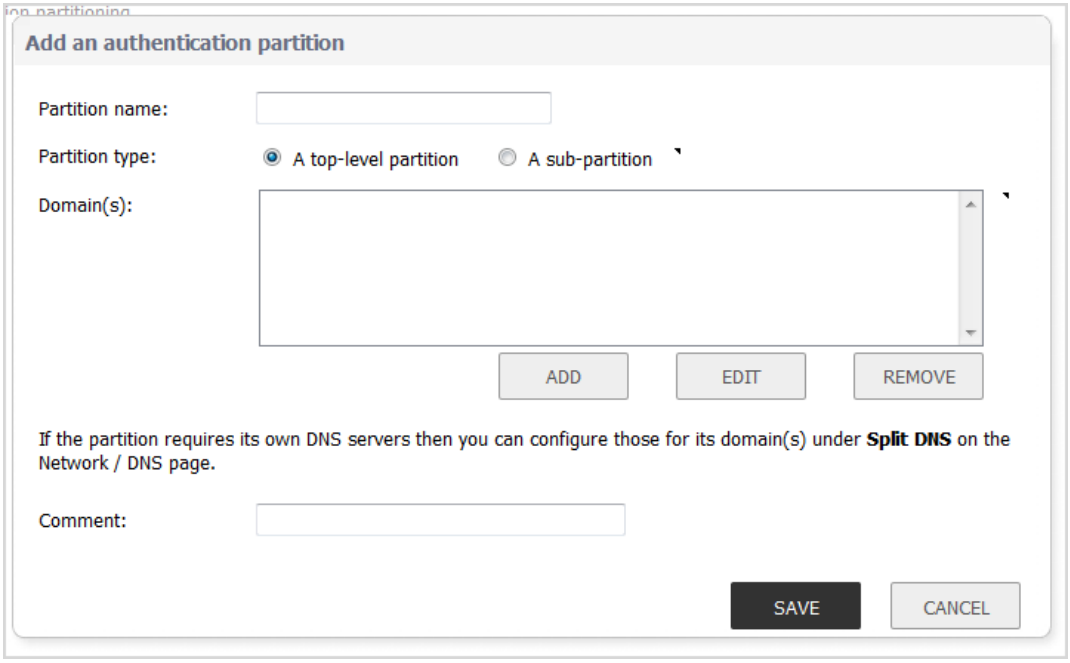
新增分割區和子分割區

若要新增分割區:

1 移至**使用者 > 分割區**頁面。



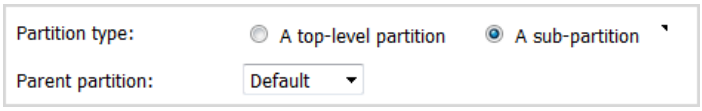
2 在**驗證分割區**區段中，按一下**新增**。隨即顯示**新增驗證分割區**快顯對話方塊。



3 在**分割區名稱**欄位，輸入有意義的易記名稱。名稱可以是 1 到 32 個英數字元。

4 對於**分割區類型**，選擇驗證分割區為:

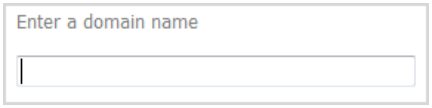
- **頂層分割區**；移至步驟 6。
- **子分割區**；**父分割區**下拉功能表顯示:



5 從下拉功能表選取父分割區。預設分割區為**預設**。

ⓘ **提示：**如果您的安裝沒有多個分割區，則會建立子分割區作為**預設**分割區的子分割區。

6 在**網域**清單下，按一下**新增**。隨即顯示**新增網域**快顯對話方塊。



7 輸入網域名稱。

8 按一下**確定**。

9 對於要新增的每個網域重複步驟 6 到步驟 8。

10 可以選擇在**註解**欄位中輸入註解。

11 按一下**儲存**。分割區及/或子分割區隨即加入**驗證分割區**表格中。子分割區的位置緊隨其父分割區之後，具有**連結**圖示，表示它們是子分割區。

刪除分割區和子分割區

ⓘ **附註：**在本節中，分割區是指分割區和子分割區。

您可以刪除單一分割區、多個分割區或所有分割區。如果您要刪除單一分割區，伺服器、代理及用戶端會重新指派至**預設**分割區。

ⓘ **附註：**您無法刪除**預設**分割區。

主題：

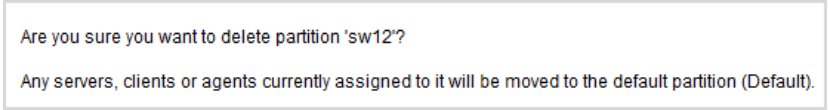
- 第 180 頁「刪除單一分割區」
- 第 181 頁「刪除多個分割區」
- 第 181 頁「刪除所有分割區 (除預設值以外)」

刪除單一分割區

若要刪除單一分割區:

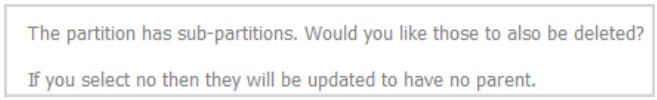
1 導覽到**使用者 > 分割區**。

2 在**驗證分割區**表格下，針對要刪除的分割區，按一下**設定**欄中的**刪除**圖示。確認訊息顯示:



3 按一下**確定**。如果分割區:

- 沒有子分割區，則會刪除分割區，而且伺服器/代理/用戶端會重新指派至**預設**分割區。
- 有子分割區，訊息顯示:



a) 執行以下其中一項操作：

- 若要刪除子分割區與父分割區，請按一下**是**。所有伺服器 / 代理 / 用戶端皆重新指派給**預設**分割區。
- 若要在刪除父分割區的同時，將子分割區轉換成頂層分割區，請按一下**否**。所有伺服器/代理/用戶端皆重新指派給**預設**分割區。
- 若不刪除父子分割區，請按一下**取消**。

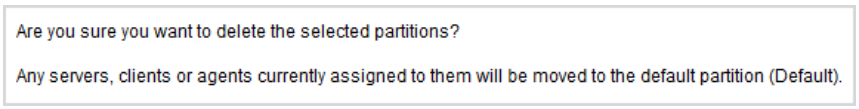
刪除多個分割區

若要刪除多個分割區

1 導覽到**使用者 > 分割區**。

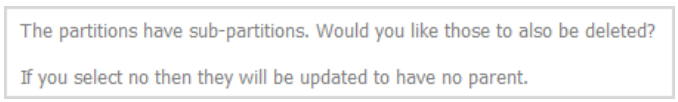
2 在**驗證分割區**表格中，按一下您要刪除之驗證分割區的核取方塊。您可以選取多個分割區。

3 按一下**刪除**。確認訊息顯示:



4 按一下**確定**。如果任何分割區:

- 沒有子分割區，則會刪除分割區，而且伺服器/代理/用戶端會重新指派至**預設**分割區。
- 有子分割區，訊息顯示:



a 執行以下其中一項操作：

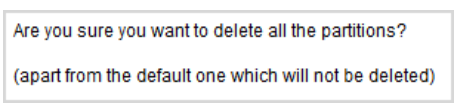
- 若要刪除子分割區與父分割區，請按一下**是**。所有伺服器 / 代理 / 用戶端皆重新指派給**預設**分割區。
- 若要在刪除父分割區的同時，將子分割區轉換成頂層分割區，請按一下**否**。所有伺服器/代理/用戶端皆重新指派給**預設**分割區。
- 若不刪除父子分割區，請按一下**取消**。

刪除所有分割區 (除預設值以外)

若要刪除所有分割區 (除預設值以外)

1 導覽到**使用者 > 分割區**。

2 在**驗證分割區**表格中，按一下**全部刪除**。確認訊息顯示:



3 按一下**確定**。所有伺服器/代理/用戶端皆重新指派給**預設**分割區。

指派伺服器、代理及用戶端

新增驗證分割區之後，將伺服器、代理及/或用戶端指派給分割區。您也可以藉由下列相同程序，隨時將其指派給驗證分割區。

您可以將未指派的伺服器、代理及用戶端自動指派給分割區。

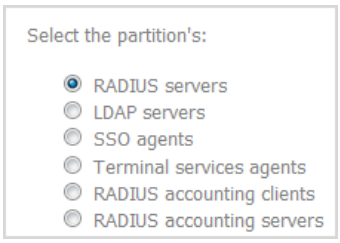
主題：

手動指派

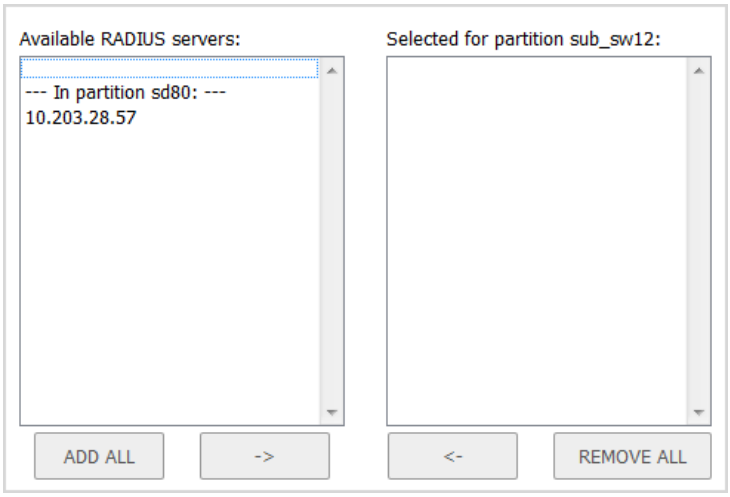
若要指派伺服器、代理及用戶端:

1 導覽到**使用者 > 分割區**。

2 在**驗證分割區**表格中，在**設定**欄中按一下分割區的**選擇**圖示。隨即顯示**選取什麼?** 快顯對話方塊。



3 選取要指派的伺服器、代理或用戶端類型。隨即顯示相應的**為分割區 *partitionName* 選取*伺服器/代理/用戶端***快顯功能表，包含可用伺服器、代理或用戶端的清單。



4 執行以下任一動作：

- 從**可用**清單選取伺服器/代理/用戶端，並按一下**向右鍵**按鈕。
- 藉由按下 **Ctrl** 鍵，同時選取每個項目，然後按一下**向右鍵**按鈕，以從**可用**清單選取多個項目。
- 按一下**新增全部**以選取所有項目。

5 按一下**儲存**。

自動指派

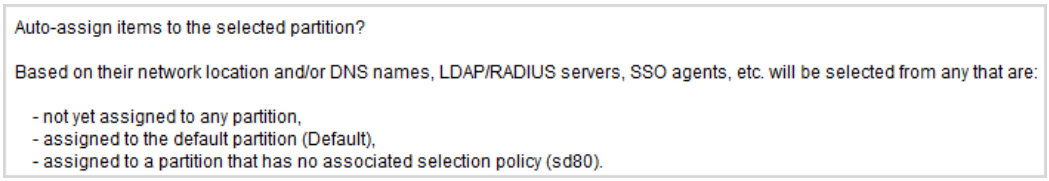
有一個**自動指派**按鈕，可用於根據其 IP 位址或主機名稱，將任何未指派的伺服器、代理及用戶端，自動指派給相關的分割區。

若要自動指派伺服器、代理及用戶端:

1 導覽到**使用者 > 分割區**。

2 在**驗證分割區**表格中，按一下要指派未指派的伺服器、代理及 / 或用戶端之驗證分割區的核取方塊。您可以選取一個以上的分割區。**自動指派**按鈕隨即啟用。

3 按一下**自動指派**。隨即顯示自動指派訊息。



4 按一下**確定**。

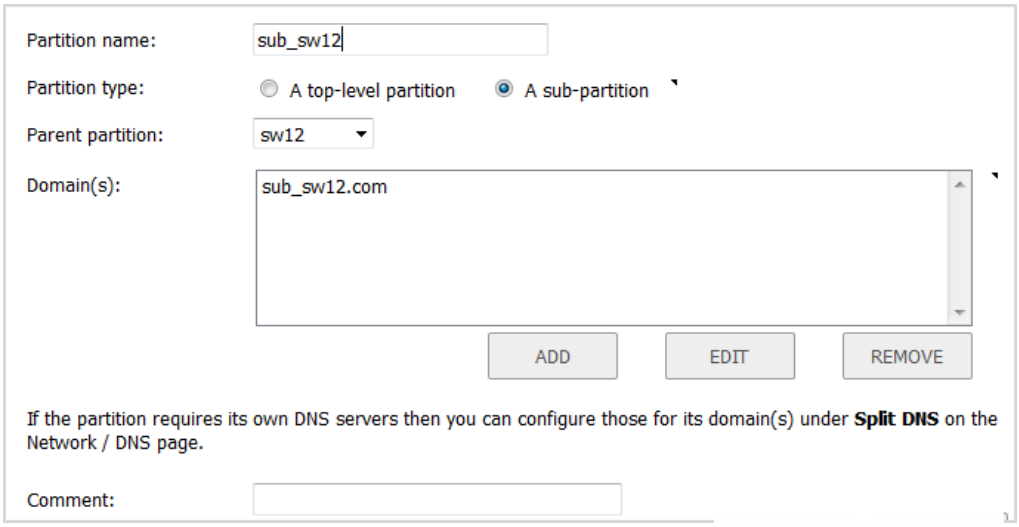
編輯分割區

您可以編輯所有分割區，包含**預設**分割區。

若要編輯分割區:

1 導覽到**使用者 > 分割區**。

2 在**驗證分割區**表格中，在您要修改的驗證分割區的**設定**欄中，按一下**編輯**圖示。隨即顯示**編輯驗證分割區**快顯。

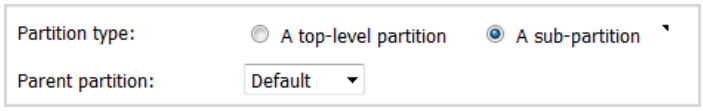


3 您可以在**分割區名稱**欄位中，變更分割區的名稱。名稱可以是 1 到 32 個英數字元。

4 藉由變更**分割區類型**，可將來自頂層分割區的分割區變更為子分割區，或將子分割區變更為頂層分割區；選擇驗證分割區目前是否為:

> **附註：**具有子分割區的頂層分割區無法變更為子分割區，除非您先刪除子分割區，將其重新指派至不同的頂層分割區，或讓它們成為頂層分割區。

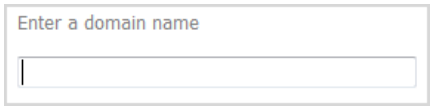
- **頂層分割區**，移至步驟 6。
- **子分割區**；**父分割區**下拉功能表顯示:



5 從**父分割區**下拉功能表選取父分割區。預設分割區為**預設**。

6 結束時間:

- 編輯網域，移至步驟 10。
- 刪除網域，移至步驟 15。
- 新增網域，在**網域**清單下，按一下**新增**。隨即顯示**新增網域**快顯對話方塊。

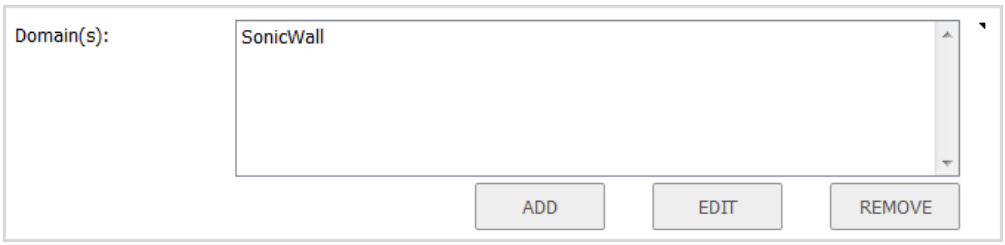


7 輸入網域名稱，可以是 1 到 32 個英數字元。

8 按一下**確定**。

9 移至步驟 17。

10 按一下以選取要編輯的網域。



11 按一下**編輯**按鈕。隨即顯示**編輯網域**對話方塊。

12 變更網域名稱。

13 按一下**確定**。

14 移至步驟 17

15 選取要刪除的網域。

16 按一下**移除**按鈕。

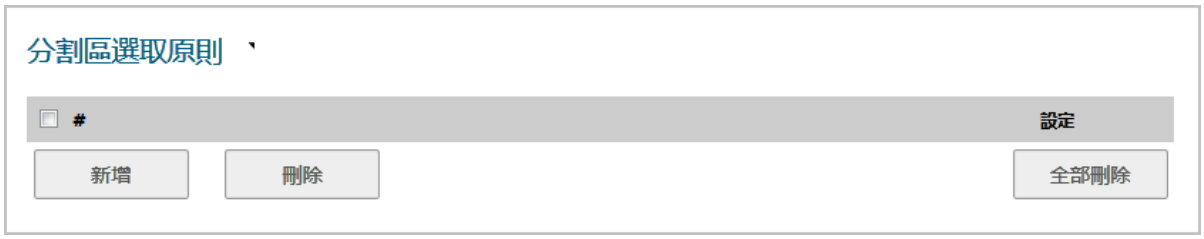
17 對於您要新增、編輯或刪除的每個網域，重複步驟 6。

18 可以選擇在**註解**欄位中輸入註解。

19 按一下**儲存**。

設定分割區選取原則

分割區選取原則可指定如何為使用者選取驗證分割區。您可以在**使用者 > 分割區**頁面的**分割區選取原則**區段中，新增、編輯及管理驗證分割區選取原則。如需分割區選取原則的完整描述，請參閱第 169 頁「關於驗證分割區選取」。



主題：

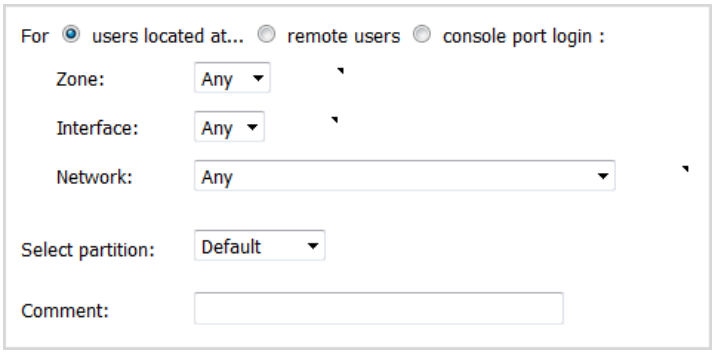
- 第 186 頁「新增驗證分割區選取原則」
- 第 188 頁「變更選取原則的優先順序」
- 第 188 頁「修改選取原則」
- 第 189 頁「刪除分割區選取原則」

新增驗證分割區選取原則

若要新增分割區選取原則:

1 移至**使用者 > 分割區**頁面。

2 在**分割區選取原則**區段中，按一下**新增**。隨即顯示**新增分割區選取原則**快顯對話方塊。



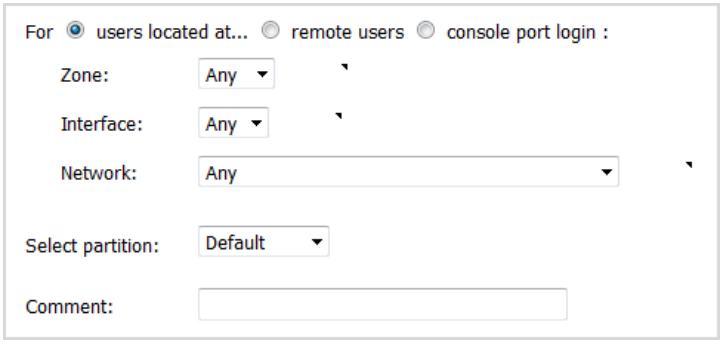
3 選擇使用者的登入位置；顯示內容取決於您的選擇:

對此選擇	移至
位於下列位置的使用者...	步驟 4；這是預設值
遠端使用者	步驟 7
主控台連接埠登入	步驟 9

4 如果您已選取**位於下列位置的使用者...**，請從**區域**、**介面**和**網路**下拉功能表中，選取分割區所在的位置:

附註：若要選取分割區，通常不需要指定區域、介面和網路。為達最佳效率，建議最好符合最低需求。

例如，如果透過特定介面找到分割區，那麼，只要選取該介面，並將**區域**保留為預設值，**任何**。如果分割區位於特定子網路，只要選取該子網路作為**網路**，並將**區域**和**介面**皆設為預設值，**任何**。



附註：每個下拉功能表中提供的選擇視站台而有所不同。

- **區域** - 預設值為**任何**
- **介面** - 預設值為**任何**
- **網路** - 預設值為**任何**；有建立新位址物件及/或位址群組的選項

5 從**選取分割區**下拉功能表選取分割區或子分割區。預設分割區為**預設**。

6 移至步驟 10。

7 如果您已選取遠端使用者，則選項會變更；請從**選取分割區**下拉功能表選取分割區或子分割區。預設分割區為**預設**。

8 移至步驟 10。

9 如果您已選取主控台連接埠登入，則選項會變更；請從**選取分割區**下拉功能表選取分割區或子分割區。預設分割區為**預設**。

10 可以選擇在**註解**欄位中輸入註解。

11 按一下**儲存**。

變更選取原則的優先順序

決定要使用的驗證分割區時，SonicOS 會從頂端 (1) 到底部 (*n*) 依序搜尋**分割區選取原則**表格。當您建立選取原則時，其優先順序如下所示:

1 區域，**任何**列在群組的最後一個

2 介面，**任何**列在群組的最後一個

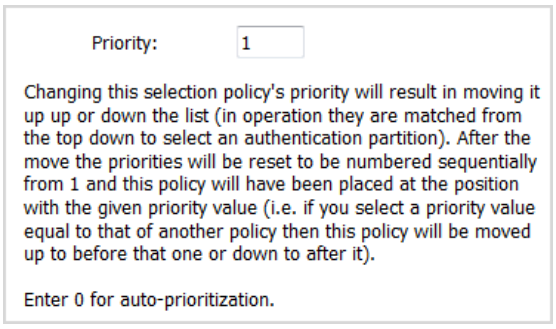
3 網路，**任何**列在群組的最後一個

您可以變更**預設**分割區選取原則以外之任何原則的優先順序，預設的優先順序一律是最低的。

變更選取原則的優先順序會在優先順序清單中將原則上移或下移。移動之後，會重設優先順序以符合新順序。

若要變更原則的優先順序:

1 在**分割區選取原則**表格中，為選取原則按一下**優先順序** 圖示。隨即顯示**變更選取原則優先順序**快顯對話方塊。



2 在**優先順序**欄位中，輸入所需要的優先順序。

附註：輸入 0 即可自動排列優先順序。

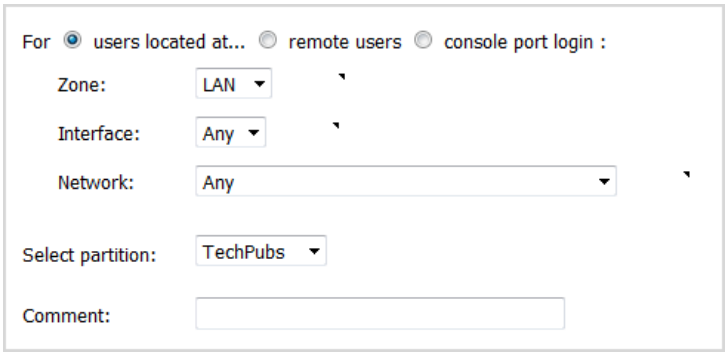
3 按一下**確定**。**分割區選取原則**表格隨即更新以反映新的順序，包含其他原則的重新排序。

修改選取原則

您可以修改自動建立之**預設**原則以外的任何分割區選取原則。對於預設原則，您只能變更**選定的分割區**。

若要變更分割區選取原則:

1 在**分割區選取原則**表格中，為選取原則按一下**設定**欄中的**編輯**圖示。隨即顯示**編輯分割區選取原則**快顯對話方塊。



2 這是與新增分割區選取原則相同的對話方塊；如需關於對話方塊的資訊，請參閱第 186 頁「新增驗證分割區選取原則」。

刪除分割區選取原則

您可以為**預設**驗證分割區刪除自動建立之**預設**原則以外的任何分割區選取原則。您可以刪除建立的單一原則、多個原則或所有原則。

若要刪除原則:

1 在**使用者 > 分割區**頁面的**分割區選取原則**區段中，針對要刪除的原則，按一下**設定**欄中的**刪除**圖示。確認訊息顯示:

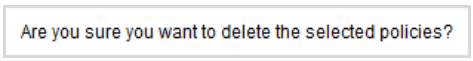
2 按一下**確定**。

若要刪除多個原則:

附註：無法刪除預設分割區選取原則。

1 在**使用者 > 分割區**頁面的**分割區選取原則**區段中，按一下一個或多個原則的核取方塊，以刪除原則。**刪除**按鈕隨即啟用。

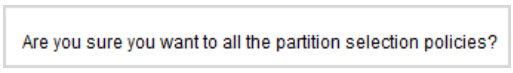
2 按一下**刪除**按鈕。確認訊息顯示:



3 按一下**確定**。

若要刪除所有原則:

1 在**使用者 > 分割區**頁面的**分割區選取原則**區段中，按一下**全部刪除**按鈕。確認訊息顯示:



2 按一下**確定**。

為驗證分割設定伺服器、代理及用戶端

對於每個分割區，您可以設定:

使用者驗證方法	本機使用者 RADIUS RADIUS + 本機使用者 LDAP LDAP + 本機使用者
單一登入方法	SSO 代理 終端服務代理 (TSA) RADIUS 計費 瀏覽器 NTLM 驗證

所有伺服器、代理及用戶端的驗證分割皆從**使用者 > 設定**頁面設定；如需如何設定這些項目以及**使用者 > 設定**頁面的完整說明，請參閱第 110 頁「設定用於管理使用者的設定」。如需分割如何影響伺服器與代理的設定的說明，請參閱設定伺服器與代理表格。

附註：伺服器、代理及用戶端的操作在第 167 頁「將伺服器、代理與用戶端與子分割區搭配運作」中有進一步的說明。

設定伺服器與代理

伺服器/代理	分割設定
RADIUS 伺服器	最多兩個 RADIUS 伺服器設定為主要/次要冗餘對。您可以設定多個 RADIUS 伺服器對，每個驗證分割區一個主要/次要對。
LDAP 伺服器	可設定一些主要 LDAP 伺服器，每個驗證分割區有一個伺服器，還有一個次要伺服器的清單 (請參閱第 139 頁「關於多個 LDAP 伺服器的延伸支援」)。通常，網域或一組互連網域的 LDAP 伺服器 (Active Directory 術語中的樹系) 會配置到每個驗證分割區。
SSO 代理	除了支援負載分擔和冗以外，多個 SSO 代理也支援將代理配置到驗證分割區。一個或多個代理群組會配置到每個驗證分割區，而且每個群組內會發生負載分擔與冗餘。
TS 代理	只有 LDAP 伺服器選擇才需要 TSA 分割以進行使用者群組成員資格查找。由於 TSA 一律使用使用者名稱提供完整的 Windows NetBIOS 網域名稱，所以設定是可選選項。因此，在大多數情況下，可以從使用者名稱衍生驗證分割區。
RADIUS 計費用戶端	只有 LDAP 伺服器選擇才需要 SSO RADIUS 計費用戶端分割以進行使用者群組成員資格查找。由於某些 (並非全部) RADIUS 計費用戶端使用其計費訊息中的使用者名稱提供網域名稱，所以設定是可選選項。因此，在某些情況下，可以從使用者名稱衍生驗證分割區。

10

設定本機使用者與群組

設定本機使用者

本機使用者是指透過 SonicWall 安全設備的本機資料庫儲存及管理的使用者。您可以在**管理 | 系統安裝 | 使用者 | 本機使用者與群組**中檢視及管理所有本機使用者、新增本機使用者，以及編輯現有的本機使用者。您還可以從 LDAP 伺服器匯入使用者。

主題：

- 第 192 頁「查看本機使用者」
- 第 192 頁「新增本機使用者」

- 第 197 頁「編輯本機使用者」
- 第 198 頁「從 LDAP 匯入本機使用者」
- 第 198 頁「設定來賓管理員」

查看本機使用者

您可以透過**使用者 | 本機使用者與群組**查看使用者所屬的所有群組。按一下使用者旁邊的**展開**圖示查看此使用者的群組成員身分。

使用者名稱右側的欄位中，會列出使用者所擁有的權限。展開的檢視顯示使用者各項權限的來源群組。

結束時間:

- 將滑鼠游標移至使用者的 **VPN 存取**欄中的**註解**圖示，即可查看使用者具備 VPN 存取權的網路資源。
- 在展開的檢視畫面中，按一下使用者的**設定**欄中的**移除**圖示，即可將該使用者從群組中移除。請參閱

  附註：如果指定的使用者無法從群組中刪除，這個圖示會變為灰色。

- 按一下使用者的**設定**欄中的**編輯**圖示，即可編輯使用者。請參閱第 197 頁「編輯本機使用者」。
- 按一下使用者的**設定**欄中的**刪除**圖示，就可以將使用者或群組從該列中移除。請參閱

  附註：如果指定的本機使用者無法從群組中刪除，這個圖示會變為灰色。

使用者 | 本機使用者與群組頁面底部會顯示本機使用者總數:

新增本機使用者

您可以透過**使用者 | 本機使用者與群組**頁面，將本機使用者新增至安全設備的內部資料庫中。

附註：如需瞭解 SSL VPN 用戶端使用者的建立流程，請參閱*連線指南*。

若要將本機使用者新增到資料庫：

1 導覽到**管理 | 系統安裝 | 使用者 | 本機使用者與群組**。

2 如果分割:

- 未啟用，請移至步驟 3。
- 已啟用，請在**驗證資料分割**下拉功能表中選取要套用設定的分割區。預設值為**全部**。

提示：只有在分割功能啟用時，系統才會顯示這個功能表。

3 按一下**新增使用者**。將顯示**新增使用者**對話方塊。

4 在**設定**中選取**這表示網域使用者**，指出是否要為使用已註冊的網域帳戶登入的任何網域使用者，套用群組成員資格、存取權和其他屬性。預設情況下未勾選此選項。 選取這個選項後，其他選項就會隨即顯示。

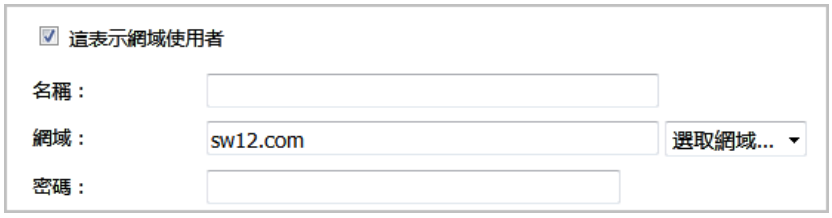
如果**這表示網域使用者**的狀態為:

- 已選取，則所有屬性 (例如群組成員資格和存取權) 都會套用到使用已命名的網域帳戶登入的使用者 (經由 RADIUS 或 LDAP 驗證)，或是經 SSO 識別為 HAT 網域使用者的使用者。您可以將這項屬性套用到已命名的特定網域使用者，或是具有指定名稱的任何網域使用者。
- 未選取，則本機使用者即為本機帳戶，且系統只會為使用這個帳戶登入且經過本機驗證的使用者套用所有相關設定，這時就必須在按照步驟 8 的說明設定密碼。

5 在**名稱**欄位中輸入使用者名稱。

6 如果本機使用者:

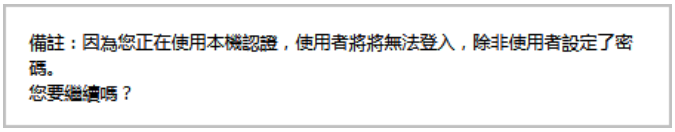
- 是網域使用者，則選項會有所異動；請移至步驟 7。



- 不是網域使用者，請移至步驟 8。

7 在**網域**欄位中輸入網域名稱。您可以在下拉功能表中選取**網域**名稱。如果您輸入的網域名稱未列在其中，您就必須輸入完整的網域名稱，否則系統會顯示以下訊息:

如果網域為本機網域，您就必須輸入密碼。如果您未輸入密碼，系統就會顯示以下訊息:



8 在**密碼**欄位，輸入使用者的密碼。密碼區分大小寫，並且應為包含 32 個字母和數字的組合，請勿使用家人、朋友或寵物的名字。

> **附註：**如果您未選取**這表示網域使用者**，就必須輸入密碼。

9 通過在**確認密碼**欄位重新輸入確認密碼。

10 (選用) 選取**使用者必須變更密碼**，即可強制要求使用者在首次登入時變更密碼。

11 選取**需要一次性密碼**，即可要求 SSL VPN 使用者提交系統產生的密碼，執行雙重驗證。

> **提示：**如果本機使用者沒有啟用一次性密碼，但其所屬群組已啟用，請確保設定好使用者的電子郵件地址，否則此使用者無法登入。

12 輸入使用者的電子郵件地址，以使其能夠收到一次性密碼 s。

13 在**帳戶存留時間**中，選取使用者帳戶遭到刪除或停用前的效期。視您的選擇而定，系統會顯示更多選項:

- **永不過期**可讓帳戶永不失效。這是預設值。移至步驟 16。
- **分鐘數**、**小時數**或**天數**可讓您指定存留時間，讓系統在期限過後刪除或停用使用者帳戶。如果您指定了存留時間限制，則選項也會有所異動:

14 在**帳戶存留時間**欄位中輸入存留時間。小時數、分鐘數或天數可指定的數值上限皆為 9999。

15 目的地

- 選取**在過期時剪除帳戶**，即可在存留時間屆滿時刪除使用者帳戶。預設情況下已核取此選項。
- 若停用此選項，則在存留時間屆滿後，系統只會停用帳戶。您隨後只要重設帳戶存留時間，就可以重新啟用帳戶。

16 可以選擇在**註解**欄位中輸入註解。

17 按一下**群組**。

群組

1 在**群組使用者中**:

a 選取使用者稍後所屬的一個或多個群組。

b 您可以

- 按一下**向右的箭頭 ->** 按鈕，將群組名稱移到**成員**清單。使用者將是所選群組的成員。
- 按一下**全部新增**。

附註：若要將使用者從群組中移除:

1 在**隸屬成員**清單中選取所需群組

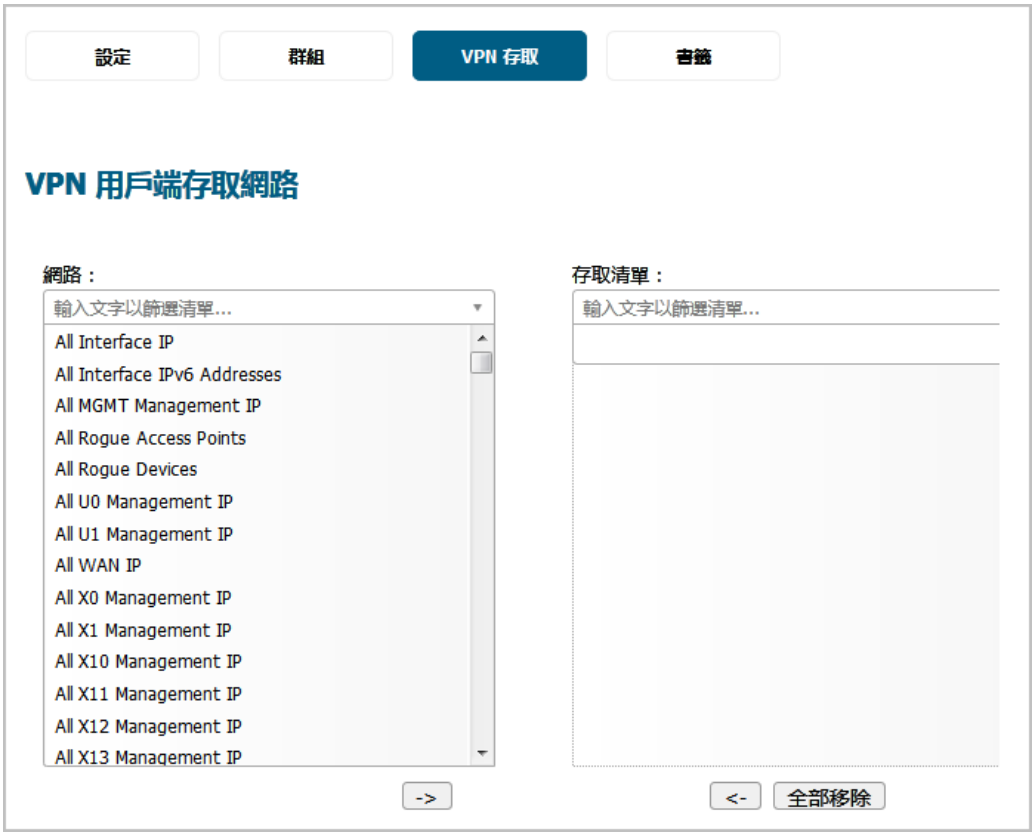
2 您可以

- 按一下**向左箭頭 <-** 按鈕。
- 按一下**全部移除**。

附註：您無法在**隸屬成員**中刪除**所有人**和**信任的使用者**。

2 如需設定 VPN 使用者 (GVC、NetExtender 或虛擬辦公室書籤) 可存取的網路資源，請按一下 **VPN 存取**。

VPN 存取



1 在**網路**中選擇一個或多個網路。

2 按一下**向右箭頭**按鈕，將選取的項目移動到**存取清單**中。

> **附註：** **VPN 存取**會影響遠端用戶端使用 GVC、NetExtender 和虛擬辦公室書籤存取網路資源的能力。如需允許這些使用者存取網路資源，必須將網路位址物件或群組新增至**存取清單**。

若要移除使用者的網路存取權:

- 在**存取清單**中選取所需網路，然後按一下**向左箭頭**按鈕。
- 按一下**全部移除**。

3 如需為每位身分為相關群組成員的使用者新增、編輯或刪除虛擬辦公室書籤，請按一下**書籤**。

書籤

4 如需新增書籤，請按一下**新增書籤**按鈕。如需設定 SSL VPN 書籤的相關資訊，請參閱設定 SSL VPN 書籤 (第 X 頁)。

> **附註：**使用者必須是 SSL VPN 服務群組的成員，才可供您設定他們的書籤。如果使用者不是成員，您必須將使用者加入 SSL VPN 服務群組，並提交異動資訊才能啟用書籤。

5 按一下**確定**完成使用者設定。

編輯本機使用者

您可以透過**使用者 | 本機使用者與群組**頁面編輯本機使用者。

若要編輯本機使用者：

1 在**本機使用者**表格中找出要編輯的使用者，然後按一下**設定**下的**編輯**圖示。**編輯使用者**對話方塊隨即顯示。

2 按照新增使用者的方式，配置**設定**、**群組**、**VPN 存取**和**書籤**選項。請參閱第 192 頁「新增本機使用者」。

從 LDAP 匯入本機使用者

您可以通過檢索 LDAP 伺服器中的使用者名稱設定防火牆上的本機使用者。防火牆上的使用者名稱與現有 LDAP/AD 使用者名稱相同有利於在 LDAP 身分驗證成功後授予 SonicWall 使用者權限。

從 LDAP 伺服器讀取的使用者清單可能很長，您可能只想要匯入較少的一部分。系統提供了**從清單移除**按鈕，以及數種供您選取不需要的使用者的方法。您可以利用這些方法，將清單縮減至方便管理的程度，然後再選取要匯入的使用者。如需瞭解如何從 LDAP 伺服器匯入使用者，請參閱**使用者 | 設定**。

設定來賓管理員

「來賓管理員」權限組為管理員提供的存取權限僅可用於管理來賓帳戶和工作階段。

若要設定來賓管理員帳戶:

1 導覽到**使用者 | 本機使用者與群組**。

2 按下**新增**。將顯示**新增使用者**對話方塊。

3 在**名稱**欄位中指定使用者名稱。

4 按一下**群組**。

5 在**使用者群組**清單中選擇**來賓管理員**。

6 按一下向右箭頭，將**來賓管理員**移動至**隸屬成員**清單。

7 按一下**確定**。

8 導覽到**網路 | 介面**。

9 按一下 LAN 介面的**編輯**圖示 。將顯示**編輯介面**對話方塊。

10 如需允許來賓管理員帳戶透過 LAN 登入安全設備，請在**使用者登入**下一併選取 **HTTP** 和 **HTTPS**。

11 按一下**確定**。

登入為來賓管理員

若要以來賓管理員的身分登入:

1 以來賓管理員的身分登入安全設備。系統隨即會顯示對話方塊，列出授權服務的存取權。

2 按一下**管理**按鈕。

來賓管理員登入後，可以透過**監控 | 使用者工作階段 > 有效的來賓使用者**頁面來管理使用者帳戶和工作階段，但無法存取任何資源或管理介面頁面。

設定本機群組

本機群組顯示在**本機群組**表中。某些本機群組為預設群組，可進行修改，但無法刪除。

核取方塊	用於勾選單獨本機群組。預設本機群組無法變更，因此其核取方塊為灰色。
展開/折疊圖示	預設為僅列出本機群組的名稱。按一下
名稱	按名稱同時列出預設和設定的本機群組。 如果在**系統 > 管理**頁面上啟用**啟用多個使用者角色**選項，則**使用者 > 本機群組**頁面將列出這些基於角色的預設管理員群組： • 系統管理員 • 密碼編譯管理員 • 稽核管理員
來賓服務	以綠色勾選標記圖示指示來賓服務對於本機群組而言是否處於使用中狀態。 對於遠端使用者，將顯示不適用遠端驗證的**註解**圖示。
管理	顯示可用於本機群組的管理功能類型。將滑鼠放在此圖示上可顯示與所列功能相關的工具提示。 對於遠端使用者，將顯示不適用遠端驗證的**註解**圖示。
VPN 存取	針對每個群組及群組成員顯示**註解**圖示。將滑鼠放在此圖示上可顯示本機群組的 VPN 存取狀態及此群組每個成員的狀態。
註解	列出為本機群組提供的任何註解。
設定	顯示每個本機使用者群組和群組成員的**編輯**和**刪除**圖示，以及群組成員的**移除**圖示。如果圖示為灰色，則此功能無法使用於此本機群組或群組成員。

主題：

- 第 201 頁「建立或編輯本機群組」
- 第 207 頁「從 LDAP 匯入本機群組」

建立或編輯本機群組

本章節介紹如何建立本機群組，但同樣適用於編輯現有的本機群組。在新增或編輯本機群組時，您可以將其他本機群組新增為群組的成員。

主題：

- 第 201 頁「新增本機群組」
- 第 207 頁「編輯本機群組」

新增本機群組

若要新增本機群組：

1 導覽到**使用者 | 本機使用者與群組**。

2 按下**新增**。顯示**新增群組**對話方塊。

主題：

- 第 201 頁「設定」
- 第 204 頁「成員」
- 第 204 頁「VPN 存取」
- 第 205 頁「書籤」
- 第 206 頁「管理」

設定

1 選擇使用者登入或通過 SSO 識別時，使用者獲得這個群組的成員資格的方式:

附註：使用者獲得這個使用者群組的成員資格時，可取得該群組所擁有的任何權限和存取權。

此與網域使用者群組相符 (預設)	使用者為與這個群組名稱相同的網域使用者群組的成員時，可獲得這個群組的成員資格。您可以針對群組成員資格進行相關設定: • 僅限特定網域中的網域使用者群組成員。 • 身分為任何網域中已命名群組的成員的使用者。 **附註：**選取這個選項後，其他選項會有所異動。
只會在本機設定成員	本機使用者為唯一獲得群組成員資格的使用者。 預設情況下未勾選此選項。
根據使用者在 LDAP 目錄中的位置設定成員資格	使用者登入或通過 SSO 識別時，如果 LDAP 伺服器上的使用者物件位於 **LDAP 位置**中指定的位置 (或位於適用的指定位置之下)，則使用者在這個工作階段中就會獲得這個使用者群組的成員資格。預設停用此設定。 **附註：**LDAP 伺服器上沒有相應的使用者群組，且群組的成員資格也未與網域使用者群組中所設定的任何成員資格有所關聯。 **附註：**選取這個選項後，其他選項會有所異動。

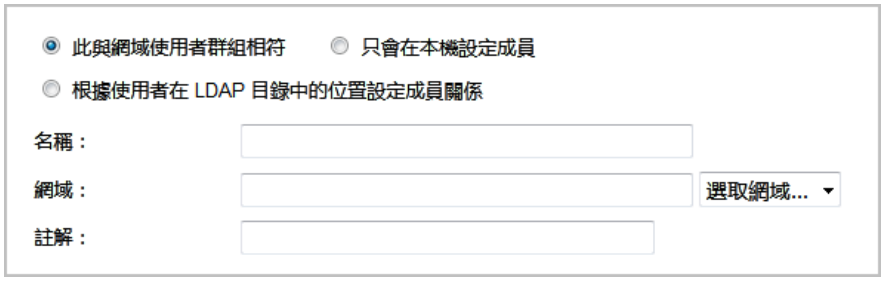
附註：在任何情況下，您也可以透過這個對話方塊中的**成員**頁面，讓本機使用者 (包括代表網域使用者的本機使用者) 和其他使用者群組成為指定群組的成員。

2 在**名稱**欄位中輸入本機群組的名稱。

附註：預先定義使用者或群組的名稱不能編輯，且欄位變灰。

3 如果選擇：

- **此與網域使用者群組相符**，則其他選項會有所異動。請移至步驟 4。

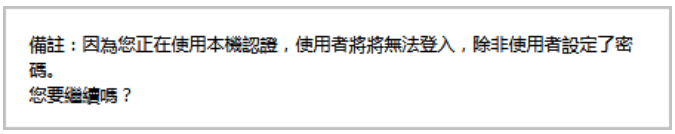


- **只會在本機設定成員**，請移至步驟 5。
- **根據使用者在 LDAP 目錄中的位置設定成員資格**，則其他選項會有所異動。請移至步驟 5。

提示：在**成員**標籤上，本機使用者和其它群組也可作為此群組的成員。

4 在**網域**欄位中輸入網域名稱。您可以在下拉功能表中選取**網域**名稱。如果您輸入的網域名稱未列在其中，您就必須輸入完整的網域名稱，否則系統會顯示以下訊息:

如果網域為本機網域，您就必須輸入密碼。如果您未輸入密碼，系統就會顯示以下訊息:



5 可以選擇在**註解**欄位中輸入描述註解。

6 如果您選取的是**此與網域使用者群組相符**或**只會在本機設定成員**，請移至步驟 9。

7 在 **LDAP 位置**欄位中，輸入位於 LDAP 目錄樹狀目錄中的位置。這個位置可以是一個路徑（例如 `domain.com/users`）也可以是 LDAP 識別名稱。

> **附註：**如果 LDAP 使用者群組鏡像已啟用，那麼在鏡像使用者群組中此欄位是唯讀的，且顯示在 LDAP 目錄鏡像群組中的位置。

8 在**使用者位置**選項中選擇位置所在:

- **指定位置或指定位置以下**（預設值）
- **指定位置**

9 或者勾選**需要一次性密碼**核取方塊為此群組請求一次性密碼。如果啟用此設定，使用者必須設定電子郵件地址。

10 結束時間:

- 如需完成群組新增作業，請按一下**確定**。
- 如需新增成員，請移至第 204 頁「成員」。

成員

1 按一下**成員**。

2 從**非成員使用者和群組**清單中，選擇想要新增的使用者和/或群組。

3 若要新增下列項目:

- 將使用者和/或群組新增至**成員使用者和群組**清單:
    a) 從**非成員的使用者和群組**清單中選取所需的使用者和/或群組。
    b) 按一下**向右箭頭 ->** 按鈕。
- 所有使用者和群組，請按一下**全部新增**。

附註：您可以將任何群組新增為另一群組的成員，**所有人**和 **All LDAP Users** 除外。注意您新增為其他群組成員的群組的成員身分。

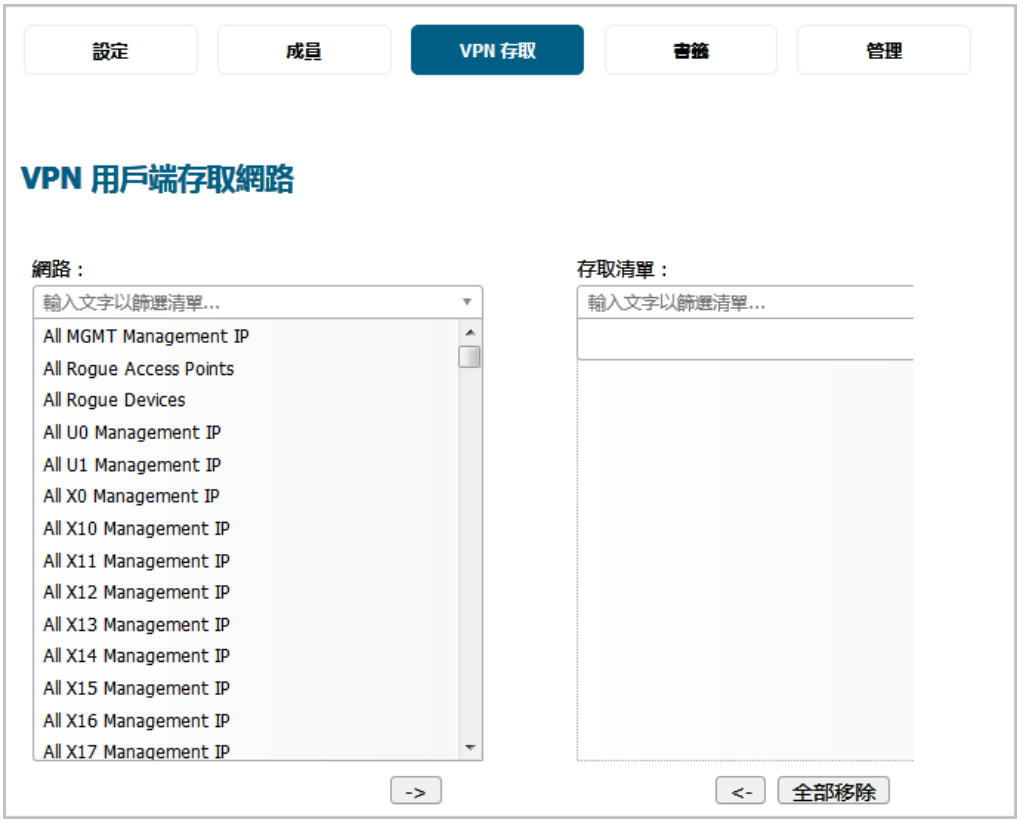
若要移除使用者和/或群組，從**成員使用者和群組**清單中，選擇使用者和/或群組，然後按一下**左箭頭 <-** 按鈕。若要移除所有的使用者和群組，按一下**全部移除**。

4 結束時間:

- 如需完成群組新增作業，請按一下**確定**。
- 如需指定 VPN 存取，請移至第 204 頁「VPN 存取」。

VPN 存取

1 按一下 **VPN 存取**。



2 從**網路**清單中，選擇此群組將預設擁有 VPN 存取權限的網路資源。

附註：群組的 VPN 存取設定會影響遠端用戶端和 SSL VPN 虛擬辦公室書籤。

3 按一下**右箭頭 ->** 按鈕將資源新增到**存取清單**中。

如需將資源自**存取清單**中移除，請選取所需資源，然後按一下**向左箭頭 <-** 按鈕。若要移除所有資源，請按一下**全部移除**。

4 結束時間:

- 如需完成群組新增作業，請按一下**確定**。
- 如需指定書籤，請移至第 205 頁「書籤」。

書籤

1 按一下**書籤**。

2 您可以新增、編輯或刪除作為相關群組成員的各使用者的虛擬辦公室書籤。如需設定 SSL VPN 書籤的相關資訊，請參閱 *SonicOS 連線指南*。

附註：在可以設定使用者的書籤之前，使用者必須是 SSLVPN 服務群組的成員。

3 結束時間:

- 如需完成群組新增作業，請按一下**確定**。
- 如需指定群組是否擁有管理權限，請移至第 206 頁「管理」。

管理

1 按一下**管理**。

2 如果給予新群組其他管理群組的成員身分使其成為管群理組，那麼可以勾選**成員從網頁直接登入到管理介面**。預設情況下未勾選此選項。

3 使用者原先具備授予唯讀管理的使用者群組 (也就是 SonicWall 唯讀管理群組或具有其中成員資格的群組) 的成員資格，隨後又被新增到其他的管理使用者群組時，則由**如果這個唯讀管理群組與其他管理群組配合使用**選項負責控管後續發生的情況。若要授予使用者下列項目:

- 選擇**使用其他群組的管理權限來覆寫這個項目 (無唯讀限制)**，即可授予由無唯讀限制的其他管理群組設定的管理權限。此設定允許將唯讀管理群組設為一組使用者的預設值，但仍使其成為其他管理群組成員以覆寫所選使用者的預設值，以便其執行設定。預設情況下已核取此選項。在**本機使用者**表格中，使用者的**管理**欄會顯示其他群組的指定設定，例如*受限*或*「完整」*。
- 如需為成員使用者提供其他群組設定、但將其限制為唯讀存取的管理級別，請選擇**將其他群組的管理權限限制為唯讀**。在**本機使用者**表格中，使用者的**管理**欄會顯示雙重指定設定，例如*唯讀受限*。

  ⓘ **提示：**如需混合使用這兩者，請在 SonicWall 唯讀管理中選擇第一個選項，然後建立為此群組成員的其他群組，但其已選擇第二個選項（反之不成立）。

  ⓘ **附註：**如果使用者為唯讀管理群組成員且在其他管理群組中無任何成員資格，則此成員將獲取限制為唯讀的完全級別存取權限（根據 SonicWall 管理員）。

4 按一下**確定**完成設定。

編輯本機群組

編輯本機群組的步驟如下：

1 按一下要編輯的群組的**編輯**按鈕。「編輯群組」對話方塊隨即顯示，這個方塊與「新增群組」對話方塊相同。

2 遵照第 201 頁「新增本機群組」中的步驟。

從 LDAP 匯入本機群組

將 SonicOS 中名稱相同的使用者群組作為既有的 LDAP/AD 使用者群組，即可在 LDAP 驗證成功時授予 SonicWall 群組成員資格和權限。您可以從自己的 LDAP 伺服器擷取使用者群組名稱，藉此在 SonicOS 中設定本機使用者群組。如需更多匯入本機群組的相關資訊，請參閱第 137 頁「使用者和群組標籤」。

按 LDAP 位置設定使用者成員身分

可以在 LDAP 伺服器上為某些組織單位 (OU) 中的使用者設定 LDAP 規則和原則。如需「按組織單位的 LDAP 群組成員」功能的更多資訊，請參閱第 79 頁「按組織單位的 LDAP 群組成員」。如需建立新成員的完整過程，請參閱第 132 頁「建立 RADIUS 使用者的新使用者群組」。

11

管理來賓服務

使用者 | 來賓服務

來賓帳戶是為使用者登入網路設定的臨時帳戶。您可以根據需要手動建立這些帳戶或批量產生帳戶。SonicOS 包含可以預先設定的設定檔，以在產生來賓帳戶時自動設定。來賓帳戶通常限定了預先定義的有效期。在有效期結束後，預設移除帳戶。

來賓服務用於確定來賓帳戶的限制和設定。**管理 | 系統安裝 | 使用者 | 來賓服務**頁面會顯示來賓設定檔清單。來賓設定檔確定產生來賓帳戶時使用的設定。您可以在**使用者 | 來賓服務**中新增、刪除及設定來賓設定檔。此外，您還可以確定登入安全裝置的所有使用者是否能看到使用者登入視窗，此視窗顯示目前登入工作階段的剩餘活動時間。

主題：

全域來賓設定

全域來賓設定部分會提供顯示來賓登入狀態視窗的選項。視窗會在目前工作階段中顯示剩餘時間。使用者在登入工作階段中必須讓這個視窗保持開啟，而且在登入狀態視窗中按一下**登出**按鈕即可登出。

若要設定來賓登入狀態視窗:

1 選取**顯示帶有登出按鈕的來賓登入狀態視窗**，即可讓使用者每次登入時，都會在使用者登入視窗中看到登出按鈕。 預設情況下已核取此選項。

2 按一下**接受**。

來賓設定檔

來賓設定檔表格中會列出您建立的設定檔，並可供您新增、編輯及刪除這些設定檔。不過，系統一律會提供 SonicOS 產生的**預設**來賓設定檔，這個設定檔可供您進行編輯，但無法予以刪除。

主題：

- 第 209 頁「新增來賓設定檔」
- 第 211 頁「編輯來賓設定檔」
- 第 211 頁「刪除來賓設定檔」

新增來賓設定檔

若要新增設定檔：

1 導覽至**管理 | 系統設定 | 使用者 | 來賓服務**。

2 按一下**來賓設定檔**表格下的**新增**，隨即顯示**新增來賓設定檔**對話方塊。

3 在**設定檔名稱**欄位中，輸入設定檔的名稱。

4 在**使用者名稱首碼**欄位中，針對這個設定檔所產生的每個使用者帳戶名稱，輸入這些名稱的第一部分。如需讓這個設定檔產生的來賓帳戶具備自動產生的使用者名稱，請選取**自動產生使用者名稱**。使用者名稱通常為首碼加上兩或三位的數字。預設情況下已核取此選項。

5 如需讓這個設定檔產生的來賓帳戶具備自動產生的密碼，請選取**自動產生使用者密碼**。產生的密碼為八個字元的唯一字母字串。預設情況下已核取此選項。

6 如需讓系統直接啟用這個設定檔所產生的來賓帳戶，請選取**啟用帳戶**。預設情況下已核取此選項。

7 如需在帳戶過期時將帳戶自資料庫中移除，請選取**自動剪除帳戶**。預設情況下已核取此選項。

8 如需一次僅允許使用某個帳戶的單一執行個體，請選取**強制登入唯一性**。在建立新來賓帳戶時，預設啟用此功能。如果您允許多個使用者使用相同帳戶登入，則清除**強制登入唯一性**核取方塊停用此功能。

9 如需在使用者首次登入帳戶後才開始執行帳戶過期計時器，請選取**首次登入時啟動帳戶**。預設情況下未勾選此選項。

10 如需定義帳戶在安全裝置上的效期，請在**帳戶存留時間**中輸入所需的時間長度。您可以在**帳戶存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **7 天**。

11 如需針對來賓服務工作階段已啟用，但沒有任何流量通過的情況定義時間長度上限，請在**閒置逾時**:中輸入逾時時間長度。如超過此設定值，工作階段將過期，但只要**帳戶存留時間**未截止，帳戶仍保持活動。**閒置逾時**不能超過在**工作階段存留時間**中設定的值。

您可以在**帳戶存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**

- **小時數**
- **天**

預設值為 **10 分鐘**。

12 如需指定配額週期類型，請從**配額週期類型設定**下拉功能表中選取所需設定:

- **非週期性** (預設)
- **每日**
- **每週**
- **每月**

13 如需定義來賓登入工作階段啟用後的效期，請在**工作階段存留時間**中指定所需的時間長度。預設為在來賓使用者首次登入帳戶時啟用。**工作階段存留時間**不能超過在**帳戶存留時間**中設定的值。

您可以在**工作階段存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **1 小時**。

14 如需限制使用者可接收的資料量，請在**接收限制**欄位中輸入所需數字 (單位為 Mb，輸入 0 以停用)。範圍是從 0 (無法接收任何資料) 到 999999999 MB，乃至於**無限** (預設)。

15 如需限制使用者可傳送的資料量，請在**傳送限制**欄位中輸入所需數字 (單位為 Mb，輸入 0 以停用)。範圍是從 0 (無法接收任何資料) 到 999999999 MB，乃至於**無限** (預設)。

16 可以選擇在**註解**欄位中輸入描述註解。預設為**自動產生**。

17 按一下**確定**。

編輯來賓設定檔

若要編輯來賓設定檔:

1 按一下該設定檔的**設定**欄中的**編輯**圖示。

2 遵照第 209 頁「新增來賓設定檔」中的步驟。

> **附註：**編輯**預設**設定檔時，您可以編輯所有選項 (但**設定檔名稱**和**使用者名稱首碼**除外)；這些選項都會變成灰色。

刪除來賓設定檔

除了**預設**設定檔外，您可以刪除所有來賓設定檔。

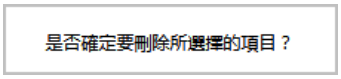
若要刪除來賓設定檔:

1 選擇以下其中一種格式：

- 要刪除的來賓設定檔的核取方塊。
- **來賓設定檔**表格中的核取方塊。系統會勾選所有核取方塊 (**預設**設定檔除外)。

刪除按鈕隨即啟用。

2 按一下**刪除**。將顯示確認訊息：



3 按一下**確定**。

12

管理來賓帳戶

使用者 | 來賓帳戶

管理 | 系統安裝 | 使用者 | 來賓帳戶會列出 SonicWall 安全設備上的來賓服務帳戶。您可以啟用或停用各帳戶、帳戶組或所有帳戶，您可以設定帳戶的自動刪除功能，並且可以新增、編輯、刪除和列印帳戶。

主題：

- 第 213 頁「查看來賓帳戶統計」
- 第 215 頁「新增來賓帳戶」
- 第 221 頁「啟用來賓帳戶」
- 第 221 頁「啟用來賓帳戶自動刪除」
- 第 222 頁「列印帳戶詳細資料」

查看來賓帳戶統計

來賓帳戶表格中會顯示來賓帳戶的相關統計資料。

主題：

- 第 214 頁「查看流量統計資料」

- 第 214 頁「查看帳戶過期資訊」
- 第 214 頁「查看工作階段過期資訊」
- 第 215 頁「查看接收和傳送限制統計資料」
- 第 215 頁「匯出來賓帳戶」

查看流量統計資料

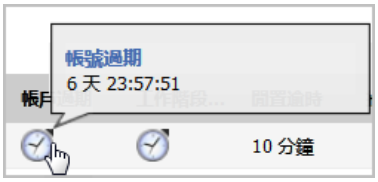
若要查看來賓帳戶的流量統計資料:

1 將滑鼠游標移至來賓帳戶**統計**欄中的**統計**圖示上。**流量統計**彈出式視窗中會針對所有已完成的工作階段，顯示傳送和接收的累計總位元組數和封包數。目前使用中的工作階段，在來賓使用者登出前均不會列入統計。

查看帳戶過期資訊

若要查看帳戶剩餘效期:

1 將滑鼠游標移至來賓帳戶**帳戶過期**欄中的**時鐘**圖示上。**帳戶過期**彈出式視窗中會顯示來賓帳戶剩餘的有效時間。



查看工作階段過期資訊

若要查看工作階段剩餘效期:

1 將滑鼠游標移至來賓帳戶**帳戶過期**欄中的**時鐘**圖示上。**帳戶過期**彈出式視窗中會顯示來賓帳戶剩餘的有效時間。

附註：如果使用者的工作階段尚未開始，**工作階段過期**彈出式視窗中會顯示未使用。

查看接收和傳送限制統計資料

對於表格中的每一個使用者帳戶，**接收限制**欄中會包含紅色的向下箭頭圖示，而**傳送限制**欄中則會顯示綠色的向上箭頭圖示。

若要查看接收/傳送限制統計資料:

1 將滑鼠游標移至來賓帳戶**接收限制/傳送限制**欄中的**箭頭**圖示上。**剩餘接收/傳送配額**彈出式視窗中會顯示來賓帳戶可下載或傳送的剩餘資料量。

匯出來賓帳戶

您可匯出 .csv 檔案格式的**來賓帳戶**表格，檔案中不僅包含所有顯示的資料，還包括限制統計資料和剩餘接收/傳送資料統計。

若要以 .csv 檔案格式匯出來賓帳戶:

1 按一下**來賓帳戶**表格下的**匯出**。**開啟 *guestaccounts_nnn*.csv** 對話方塊隨即顯示。

2 您可以：

- 開啟檔案予以查看。
- 儲存檔案供日後查看。

3 按一下**確定**。

新增來賓帳戶

您可以逐一新增來賓帳戶或自動產生多個來賓帳戶。

主題：

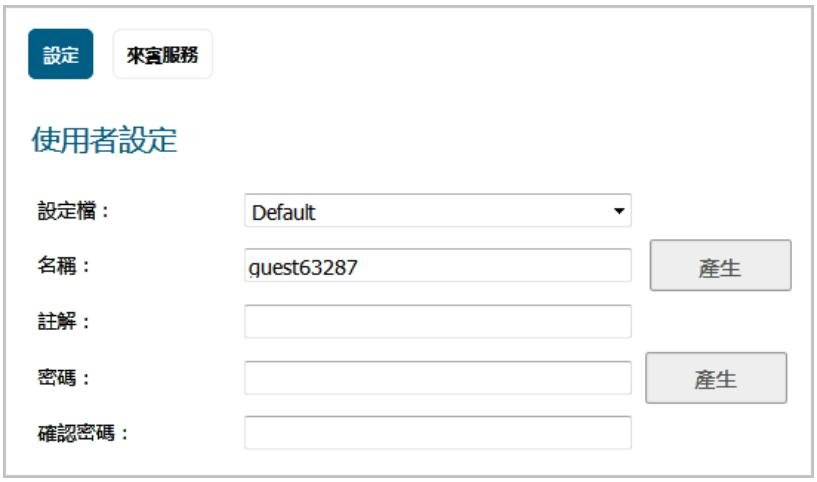
- 第 216 頁「新增來賓帳戶」
- 第 218 頁「產生多個來賓帳戶」

新增來賓帳戶

若要新增單獨的帳戶：

1 導覽到**管理 | 系統安裝 | 使用者 | 來賓帳戶**。

2 按一下**來賓帳戶**表格下的**新增來賓**。**新增來賓**對話方塊隨即顯示。



3 在**設定檔**中，選取要用來產生這個帳戶的來賓設定檔。預設設定檔為**預設**。

4 使用下列任一種方法為來賓帳戶命名:

- 在**名稱**欄位中輸入帳戶名稱。
- 按一下**產生**即可讓 SonicOS 建立名稱。產生的名稱格式為設定檔開頭名稱，再加上「guest」和一個隨機產生的 2 位到 5 位數的數字。例如：
  - guest1235 (供預設設定檔使用)
  - TechPubs guest51026 (供 TechPubs 來賓設定檔使用)

5 在**註解**欄位中加入註解說明。系統會**自動產生**預設註解。

6 使用下列任一種方法建立使用者帳戶密碼:

- 在**密碼**欄位和「確認」欄位中輸入密碼。密碼長度最長可達 32 個英數字元。
- 按一下**產生**。產生的密碼是隨機的八位字母字串。

  提示：記下密碼。否則您就必須重設密碼。

7 按一下**來賓服務**。

8 對於建立時即直接啟用的帳戶，請選取**啟用來賓服務權限**。預設情況下已核取此選項。

9 如需一次僅允許這個帳戶的一個執行個體登入安全裝置，請選取**強制登入唯一性**。如未選取這個選項，則可讓多位使用者同時使用這個帳戶。預設情況下已核取此選項。

10 如需在帳戶過期時將帳戶自資料庫中移除，請選取**帳戶過期時自動剪除帳戶**。預設情況下已核取此選項。

11 如需開始帳戶過期計時，請選取**首次登入時啟動帳戶**。

12 如需定義帳戶在安全設備安全裝置上的效期，請在**帳戶過期**中輸入到期日。您可以在**帳戶過期**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **7 天**。

如果**帳戶過期時自動剪除帳戶**：

- 已啟用，則帳戶將在過期後刪除。
- 已停用，則帳戶會保留在**來賓帳戶**表格中並設為**已過期**狀態，方便日後重新啟用。

  附註：這項設定會覆寫第 209 頁「來賓設定檔」中的帳戶存留時間設定。

13 如需針對來賓服務工作階段已啟用，但沒有任何流量通過的情況定義時間長度上限，請在**閒置逾時**:中輸入逾時時間長度。如超過此設定值，工作階段將過期，但只要**帳戶存留時間**未截止，帳戶仍保持活動。**閒置逾時**不能超過在**工作階段存留時間**中設定的值。

附註：此設定替代設定檔中的閒置逾時設定。

您可以在**帳戶存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**

- **小時數**
- **天**

預設值為 **10 分鐘**。

14 如需指定配額週期類型，請從**配額週期類型設定**下拉功能表中選取所需設定:

- **非週期性** (預設)
- **每日**
- **每週**
- **每月**

15 如需定義來賓登入工作階段啟用後的效期，請在**工作階段存留時間**中指定所需的時間長度。預設為在來賓使用者首次登入帳戶時啟用。**工作階段存留時間**不能超過在**帳戶存留時間**中設定的值。

附註：此設定替代設定檔中的工作階段存留時間設定。

您可以在**工作階段存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **1 小時**。

16 **接收限制 (0 以停用)**：輸入允許使用者接收的兆位元組數。最小值為 0，即禁止此限制；最大值為**無限制**，此為預設值。

17 **傳送限制 (0 以停用)**：輸入允許使用者傳送的兆位元組數。最小值為 0，即禁止此限制；最大值為**無限制**，此為預設值。

18 如需限制使用者可接收的資料量，請在**接收限制**欄位中輸入所需數字 (單位為 Mb，輸入 0 以停用)。範圍是從 0 (無法接收任何資料) 到 999999999 MB，乃至於**無限** (預設)。

19 如需限制使用者可傳送的資料量，請在**傳送限制**欄位中輸入所需數字 (單位為 Mb，輸入 0 以停用)。範圍是從 0 (無法接收任何資料) 到 999999999 MB，乃至於**無限** (預設)。

20 按一下**確定**產生帳戶。

產生多個來賓帳戶

若要產生多個帳戶

1 導覽到**管理 | 系統安裝 | 使用者 | 來賓帳戶**。

2 按一下**來賓帳戶**表格下的**產生**。**產生來賓帳戶**對話方塊隨即顯示。

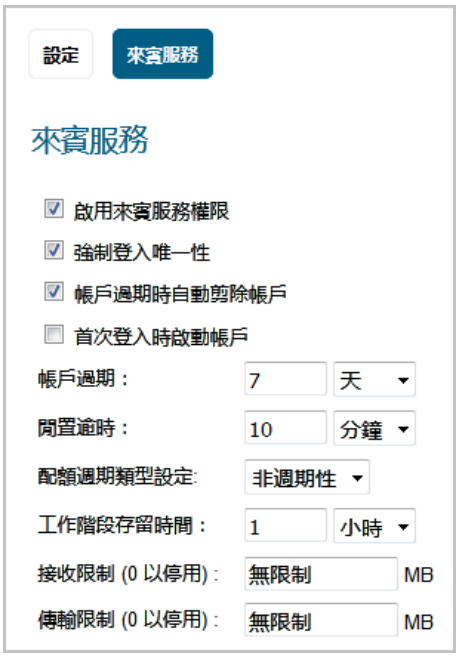
3 在**設定檔**中，選取要用於產生帳戶的來賓設定檔。系統預設為**預設**。

4 在**帳戶數量**欄位中，輸入您要產生的帳戶數量。您可以建立 1 到 6000 個帳戶。

5 **使用者名稱首碼**欄位中，輸入系統產生的帳戶名稱的首碼。例如，如果您輸入 **Guest**，則系統產生的帳戶名稱格式就會類似 `Guest123` 或 `Guest234`。預設的首碼為 **guest**。

6 在**註解**欄位中加入註解說明 (最長可包括 16 個英數字元)。

7 按一下**來賓服務**。



8 對於建立時即直接啟用的帳戶，請選取**啟用來賓服務權限**。預設情況下已核取此選項。

9 如需一次僅允許這個帳戶的一個執行個體登入安全裝置，請選取**強制登入唯一性**。如未選取這個選項，則可讓多位使用者同時使用這個帳戶。預設情況下已核取此選項。

10 如需在帳戶過期時將帳戶自資料庫中移除，請選取**帳戶過期時自動剪除帳戶**。預設情況下已核取此選項。

> ⓘ **附註：**此設定如不同於來賓設定檔中的自動刪除設定，將替代後者。

11 如需開始帳戶過期計時，請選取**首次登入時啟動帳戶**。

12 如需定義帳戶在安全設備安全裝置上的效期，請在**帳戶過期**中輸入到期日。您可以在**帳戶過期**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **7 天**。

如果**帳戶過期時自動剪除帳戶**：

- 已啟用，則帳戶將在過期後刪除。
- 已停用，則帳戶會保留在**來賓帳戶**表格中並設為**已過期**狀態，方便日後重新啟用。

附註：這項設定會覆寫第 209 頁「來賓設定檔」中的帳戶存留時間設定。

13 如需針對來賓服務工作階段已啟用，但沒有任何流量通過的情況定義時間長度上限，請在**閒置逾時**:中輸入逾時時間長度。如超過此設定值，工作階段將過期，但只要**帳戶存留時間**未截止，帳戶仍保持活動。**閒置逾時**不能超過在**工作階段存留時間**中設定的值。

附註：此設定替代設定檔中的閒置逾時設定。

您可以在**帳戶存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **10 分鐘**。

14 如需指定配額週期類型，請從**配額週期類型設定**下拉功能表中選取所需設定:

- **非週期性** (預設)
- **每日**
- **每週**
- **每月**

15 如需定義來賓登入工作階段啟用後的效期，請在**工作階段存留時間**中指定所需的時間長度。預設為在來賓使用者首次登入帳戶時啟用。**工作階段存留時間**不能超過在**帳戶存留時間**中設定的值。

附註：此設定替代設定檔中的工作階段存留時間設定。

您可以在**工作階段存留時間**欄位中指定 1 到 9999 的數字，並從下拉功能表中選取時間長度類型:

- **分鐘數**
- **小時數**
- **天**

預設值為 **1 小時**。

16 **接收限制 (0 以停用)**：輸入允許使用者接收的兆位元組數。最小值為 0，即禁止此限制；最大值為**無限制**，此為預設值。

17 **傳送限制 (0 以停用)**：輸入允許使用者傳送的兆位元組數。最小值為 0，即禁止此限制；最大值為**無限制**，此為預設值。

18 如需限制使用者可接收的資料量，請在**接收限制**欄位中輸入所需數字 (單位為 Mb，輸入 0 以停用)。範圍是從 0 (無法接收任何資料) 到 999999999 MB，乃至於**無限** (預設)。

19 如需限制使用者可傳送的資料量，請在**傳送限制**欄位中輸入所需數字 (單位為 Mb，輸入 0 以停用)。範圍是從 0 (無法接收任何資料) 到 999999999 MB，乃至於**無限** (預設)。

20 按一下**確定**產生帳戶。

啟用來賓帳戶

您可以一次啟用或停用任意個帳戶。

若要啟用一個或多個來賓帳戶：

1 找出您要啟用的一個或多個帳戶名稱，然後在旁邊的**啟用**欄中選取相應的核取方塊。如需啟用所有帳戶，請選取表格標題中的**啟用**核取方塊。

2 按一下**接受**。

啟用來賓帳戶自動刪除

您可以一次啟用或停用任意個帳戶的自動刪除。如果啟用了自動刪除，在過期後刪除帳戶。

附註：這會覆寫您在設定使用者設定檔或來賓帳戶時所指定的「自動剪除」選項。

若要啟用自動刪除：

1 在一個或多個帳戶名稱旁邊的**自動剪除**欄中選取相應的核取方塊。如需為所有帳戶啟用這個選項，請選取表格標題中的**自動剪除**核取方塊。

2 按一下**接受**。

編輯來賓帳戶

若要編輯來賓帳戶:

1 按一下該設定檔的**設定**欄中的**編輯**圖示。

2 遵照第 209 頁「新增來賓設定檔」中的步驟。

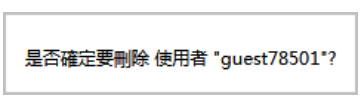
附註：編輯**預設**設定檔時，您可以編輯所有選項 (但**設定檔名稱**和**使用者名稱首碼**除外)；這些選項都會變成灰色。

刪除來賓帳戶

除了**預設**設定檔外，您可以刪除所有來賓設定檔。

若要刪除來賓帳戶

1 按一下指定來賓帳戶的**刪除**圖示。將顯示確認訊息：



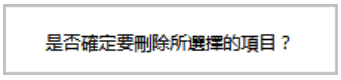
2 按一下**確定**。

若要啟用一個或多個來賓帳戶:

1 導覽到**管理 | 系統安裝 | 使用者 | 本機使用者與群組**。

2 選取要刪除的來賓設定檔的核取方塊。**刪除**按鈕隨即啟用。

3 按一下**刪除**。將顯示確認訊息：

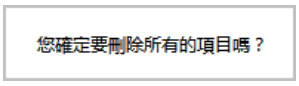


4 按一下**確定**。

若要刪除所有來賓帳戶:

1 選取**來賓帳戶**表格標題中的核取方塊。系統會勾選所有核取方塊 (**預設**設定檔除外)。**全部刪除**按鈕隨即啟用。

2 按一下**全部刪除**。將顯示確認訊息：



3 按一下**確定**。

列印帳戶詳細資料

您可以列印來賓帳戶的摘要資訊。

若要列印來賓帳戶的相關資訊。

1 按一下**列印**圖示，系統隨即會顯示帳戶摘要報告和**列印**對話方塊。

2 按一下**確定**將摘要報告傳送到印表機。

部分 4

網路

- 設定介面
- 設定 PortShield 介面
- 設定有線模式 VLAN 轉譯
- 設定容錯移轉和負載平衡
- 設定網路區域
- 設定 DNS 設定
- 設定 DNS 代理設定
- 設定路由通告和路由原則
- 管理 ARP 流量
- 設定鄰居搜索通訊協定
- 設定 MAC-IP 反詐騙檢視
- 設定 DHCP 伺服器
- 使用 IP 協助程式
- 設定 Web 代理轉送
- 設定動態 DNS

13

設定介面

關於介面

實體和虛擬介面

SonicOS 中的介面可能是：

- **實體介面** - 將實體介面繫結到單個連接埠上
- **虛擬介面** - 將虛擬介面指定為實體介面的子介面，並使得實體介面能夠承載指派至多個介面的流量。

主題：

實體介面

SonicWall 安全設備前方面板有一些實體介面。介面數量和類型取決於型號和版本（如需裝置介面的更多資訊，參閱相關*入門指南*）：

- **1 GE** - 高速銅線 GB 乙太網路連接埠
- **1 GE SFP** - 1 GB 乙太網路熱插接式 SFP 介面 [a]
- **10 GE SFP+** - 10 GB 熱插接式連接埠[a]
- **MGMT** - 一個 1 GB 乙太網路管理介面連接埠，用於保障安全模式下裝置韌體升級的安全。關於在安全模式下使用 MGMT 連接埠進行韌體升級的更多資訊，請參閱 *SonicOS 5.0 升級指南*。MGMT 連接埠的預設 IP 位址是 `192.168.1.254`。

a. 僅限 NSA 3600 系列和更高版本及 SuperMassive 系列

必須將實體介面指定給某個區域，以便設定存取規則來管理傳入和傳出流量。將安全區域繫結至各個實體介面，作為傳入和傳出流量的管道。如果沒有介面，流量將無法存取或結束此區域。

如需區域的更多資訊，請參見第 329 頁「關於區域」。

NSA 6600 和 SuperMassive 9000 系列上的 10 GB 乙太網路 SFP+ 連接埠

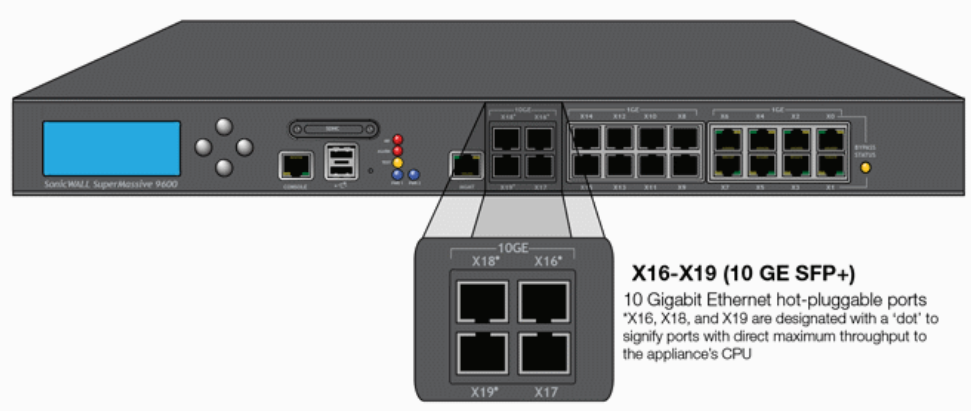
在 NSA 6600 和 SuperMassive 9000 系列裝置上，增強的小型插接式 (SFP+) 連接埠 X16、X18 和 X19 均指定了一個圓點，表示擁有直達 CPU 的最大傳送量。這些帶圓點的連接埠擁有直達 CPU 的專用（非共用）上行連結。

例如，在您使用 10Gb 企業主幹網，且使用 SuperMassive 9200 作為所在部門的閘道裝置時，這一特性非常有用。您應該將其中一個帶圓點的連接埠（X16、X18 或 X19）直接連接到主幹網。這將提供最快的存取，因為這些連接埠將 CPU 直接連接到與它們相連的所有事物。這些到主幹網的連接無需與網路中的使用者或其他任何裝置共用頻寬。若要獲得最大的速度和效率，應將帶圓點的連接埠直接連接到主幹網。

另一個範例，應將業務關鍵型連結和負載較重的多路複用連結連接到帶圓點的介面。業務關鍵型應用情形可能包括連接到 10Gb 主幹網的管理部門。為獲得最高效能，應透過帶圓點的介面連接上游的主幹網連接。這樣可以確保永遠不會由於瞬時高負載條件（可能在其他共用 CPU 上行連結的不帶圓點的介面上出現）而遺失重要的主幹網流量。

負載較重的多路複用應用情形可能包括各自擁有 10Gb 上行連結的多個下游企業交換器。為獲得最高效能，應透過帶圓點的介面連接各個交換器。這樣可以確保不同的進階別交換網域不會完全佔用其他網域的 CPU 資源。

10 GB 乙太網路熱插接式連接埠



SonicOS 管理介面中 X17 介面以星號標記，顯示此介面已連接到連接埠 X0 - X15 共用的交換網域，從而允許 X17 參與 SonicOS 進階交換功能。

虛擬介面 (VLAN)

SonicWall 安全裝置支援虛擬介面，後者是指派給實體介面的子介面。虛擬介面用於在一個實體介面上提供多個介面。

虛擬介面提供許多與實體介面相同的特性，包括區域指派、DHCP 伺服器，以及 NAT 和存取規則控制。

虛擬區域網路 (VLAN) 可描述為「基於標籤的 LAN 多路複用技術」，因為透過使用 IP 標頭標籤，VLAN 可模擬單個實體 LAN 內的多個 LAN。正如兩個在實體上相互區別、中斷連接的 LAN 彼此完全獨立，兩個不同的 VLAN 之間也是如此，但是，這兩個 VLAN 可以在同一線路上共存。VLAN 需要能夠感知 VLAN 的網路裝置來提供這種虛擬化 - 這些裝置包括能夠根據網路設計和安全原則識別、處理、移除和插入 VLAN 標籤(IDs)的交換器、路由器和防火牆。

VLAN 適用於多種用途，其中大部分用途是基於 VLAN 能夠提供邏輯廣播網域而非實體廣播網域（或者說 LAN 邊界）的能力。它不僅能將較大的實體 LAN 分割為較小的虛擬 LAN，還能將在實體上不相干的 LAN 聯合成為在邏輯上相鄰的虛擬 LAN。這樣做的好處包括：

- **提高效能** - 建立以邏輯方式分割的較小廣播網域可降低整體網路利用率，僅向需要的目的地傳送廣播，因而能夠將更多的可用頻寬保留用於應用程式流量。
- **降低成本** - 根據過去經驗，使用路由器進行廣播分段需要更多的硬體和設定工作。使用 VLAN 時，路由器的職能角色完全顛倒 - 不是用於禁止通訊的用途，而是根據需要促成獨立 VLAN 之間的通訊。
- **虛擬工作群組** - 工作群組是廣泛共用資訊的邏輯單位，例如營銷部門或工程部門。出於效率的考慮，應建立廣播網域邊界，以便與這些職能工作群組保持一致。但這種做法並非總能實現：工程部使用者和營銷部使用者可能存在混疊的情況，處於建築物內的同一樓層（並且使用相同的工作群組交換器），或者相反 - 工程團隊可能分佈在整個園區內。嘗試透過複雜的佈線來解決這一問題不僅成本高，而且無法進行持續的新增和移動操作。VLAN 允許快速重新設定交換器，以便保持與工作組要求相一致的邏輯網路設定。
- **安全** - 位於一個 VLAN 中的主機無法與位於其他 VLAN 中的主機通訊，除非某個網路裝置促成它們之間的通訊。

子介面

SonicOS 提供的 VLAN 支援是透過子介面實現的，後者是嵌套在實體介面下面的邏輯介面。每個唯一的（標籤）都需要自己的子介面。出於安全和控制的原因，SonicOS 沒有參與任何 VLAN 轉接通訊協定，而是要求對將要支援的每個 VLAN 進行設定，並指定相應的安全特性。

附註：VLAN ID 的範圍是 0 到 4094，有以下限制：保留 VLAN 0 用於 QoS，有些交換器會保留 VLAN 1 用於原生 VLAN。

附註：動態 VLAN 轉接通訊協定（例如 VTP [VLAN 轉接通訊協定] 或 GVRP [通用 VLAN 註冊協定]）不得用於來自防火牆上連接的其他裝置的轉接連結。

對於來自具備 VLAN 功能的交換器的轉接連結，採取的支援方法是將相關的 VLAN ID 聲明為防火牆上的子介面，且採用與實體介面幾乎相同的方式對其進行設定。也就是說，防火牆將僅處理已定義為子介面的 VLAN， 將丟棄作為無關的 VLAN 的其餘 VLAN。這種方法還允許轉接連結所連接的防火牆上的父級實體介面以一般介面的方式工作，從而為同一連結上可能同時存在的任何原生（無標籤）VLAN 流量提供支援。否則，此父類介面可能保持「未指派」狀態。

VLAN 子介面擁有實體介面的大部分功能和特性，包括區域可指派性、安全服務、GroupVPN、DHCP 伺服器、IP 協助程式、路由，以及完整的 NAT 原則和存取規則控制。此時 VLAN 子介面排除多點傳送支援。

SonicOS 安全物件

SonicOS 的介面定址配置可配合網路區域和位址物件工作。這種結構的基礎是 SonicOS 中的規則和原則所使用的安全物件。

安全物件包括直接連結到實體介面，並可透過**網路 | 介面**頁面管理的界面物件。**管理 | 原則 | 物件 > 位址物件**和**管理 | 原則 | 物件 > 服務物件**中分別定義了位址和服務物件。

區域處於 SonicOS 安全物件結構的頂層。SonicOS 包含預先定義的區域，並且用於定義自己的區域。預先定義的區域包括 LAN、DMZ、WAN、WLAN 和自訂區域。區域可以包含多個介面，然而將 WAN 區域限制為最大值是總介面數減一。在 WAN 區域內，可主動傳送流量的 WAN 介面可能有一個或多個，具體情況取決於**網路 | 容錯移轉與負載平衡**中的 WAN 容錯移轉和負載平衡設定。

如需更多的 SonicWall 安全設備 WAN 容錯移轉和負載平衡相關資訊，請參閱第 319 頁「網路 | 容錯移轉與負載平衡」。

在區域設定級別，區域的**允許介面信任**設定可自動完成建立寬鬆的區域內存取規則的相關過程。它將為整個區域建立一個綜合位址物件，以及一條寬鬆包容的區域位址到區域位址存取規則。

透明模式

SonicOS 中的透明模式使用介面作為管理層級的頂層。透明模式支援獨特的定址和介面路由。

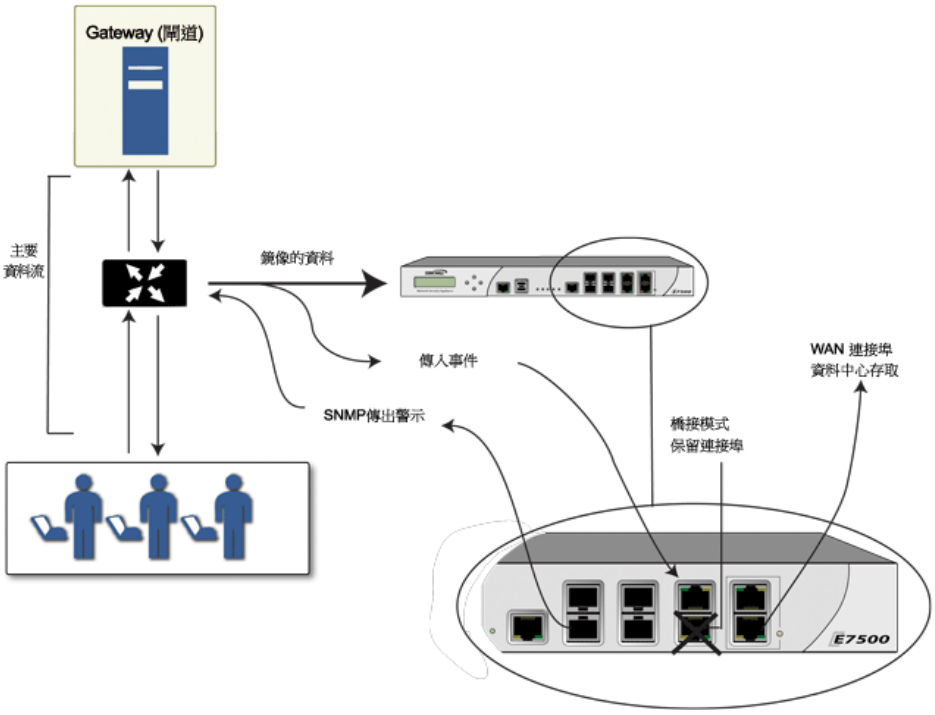
IPS 偵測器模式

SonicWall 安全設備支援 IPS 偵測器模式，這個模式源於用來入侵偵測的二層橋接模式。IPS 偵測器模式設定允許將安全設備上的介面連接到交換器上的鏡像連接埠以檢查網路流量。通常，此設定與主閘道內部的交換器配合使用，以監控內部網路中的流量。

在 IPS 偵測器模式：網路圖中，流量傳入區域網路中的交換器，並透過交換器鏡像連接埠鏡像至 SonicWall 安全裝置上的 IPS 偵測器模式連接埠中。安全設備會根據橋接配對所配置的設定來偵測封包。警示可能會觸發 SNMP 陷阱，並透過安全設備上的另一個介面將其傳送到指定的 SNMP 篩選條件。安全設備檢查過後就會捨棄網路流量。

安全設備的 WAN 介面用於連接到防火牆資料中心，以獲取簽章更新或其他資料。

IPS 偵測器模式：網路圖



在 IPS 偵測器模式中，安全設備上同一區域內的兩個介面之間會設定一個二層橋接，例如 LAN-LAN 或 DMZ-DMZ。也可以建立自訂區域以用於二層橋接。只有 WAN 區域不適用於 IPS 偵測器模式。

原因是，SonicOS 會對同一區域內的流量（例如 LAN-LAN 流量）偵測所有特徵，但某些指定方向（用戶端與伺服器端）特徵不適用於某些 LAN-WAN 的情況。

二層橋接的任一連接埠均可連接到交換器上的鏡像連接埠。在網路流量遍歷交換器的過程中，還將此流量傳送到鏡像連接埠，並透過鏡像連接埠傳入安全設備進行深度封包偵測。惡意事件會觸發警示和產生記錄項目，且如果已啟用 SNMP，還會向已設定的 SNMP 管理器系統的 IP 位址傳送 SNMP 陷阱。此流量實際不會繼續傳入二層橋接的另一個介面。IPS 偵測器模式不會讓安全設備接入網路流量，而是僅僅提供一種方法來偵測流量。

網路 | 介面頁面提供的**編輯介面**對話方塊，設有**僅探查這個橋接配對的流量**選項，可供您在設定 IPS 偵測器模式時使用。選取這個選項後，安全設備就會檢查所有透過鏡射交換器連接埠到達 L2 橋接的所有封包。您還必須同時針對 IPS 偵測器模式，選取**一律不路由流量到這個橋接配對上**選項，確保來自鏡射交換器連接埠的流量不會被送回網路上。

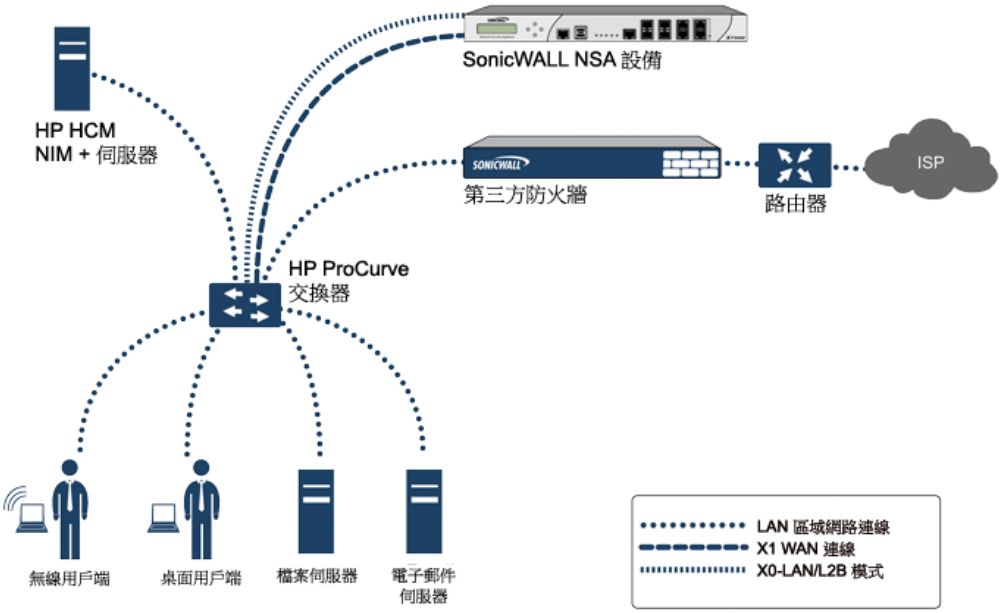
如需在 IPS 偵測器模式下設定介面的詳細說明，請參見第 261 頁「設定 IPS 偵測器模式」。

IPS 偵測器模式範例拓撲

在 Hewlett Packard ProCurve 交換環境中使用 SonicWall IPS 偵測器模式的範例。此應用情節依靠的是 HP ProCurve Manager Plus (PCM+) 和 HP Network Immunity Manager (NIM) 伺服器軟體套件所提供的用於限制或關閉正在傳出威脅的連接埠的功能。

此方法適用於以下網路環境: 目前已有安全設備並打算繼續使用，但您希望使用安全設備的安全服務作為探查器。

IPS 偵測器模式：範例拓撲



在此部署中，將針對*內部*網路的定址配置設定 WAN 介面和區域，並將其連接到內部網路。X2 連接埠透過二層橋接連接到 LAN 連接埠 - 但它不會連接任何物件。X0 LAN 連接埠設定為 HP ProCurve 交換器上另一個專門設定的連接埠。此特殊連接埠設定用於鏡像模式：它會將所有內部使用者和伺服器連接埠轉送到防火牆上的「偵測」連接埠。透過此連接埠，防火牆可以分析整個內部網路的流量，如果有任何流量觸發了安全特徵，它將立即透過 X1 WAN 介面將其擷取到 PCM+/NIM 伺服器，然後對正在傳出威脅的特定連接埠採取措施。

Firewall Sandwich

您可以部署和設定 SonicWall Firewall Sandwich 以提高整個 IT 基礎設施的可用性、可擴充性和可管理性。部署 Firewall Sandwich 提供下列功能：

- 擴充性 - 不論身在何處均可利用現有設備增加更多的容量
- 備援和復原 - 主要和次要元件

- 內嵌升級 - 升級防火牆和交換器，無需關閉系統
- 單點管理 - 管理多個防火牆叢集和刀鋒的原則
- 完整的安全性服務 - 包括具備 DPI-SSL

Firewall Sandwich 的部署和設定可利用以下支援的設備和服務實作：

- Dell Force10 S 系列交換器，例如執行 FTOS v9.8 或以上的 S5000、S4810、S4048 或 S6000
- SonicWall NSA 2600 和更高版本裝置以及 SuperMassive 系列裝置。
- SonicWall 服務，例如 GAV、IPS、ASPR、DPI-SSL 和 CFS 結合有線模式的 Single Sign-On All (全部單一登入)。

HTTP/HTTPS 重新導向

一般來說，當防火牆設定需要使用者驗證時，來自未驗證來源的 HTTP/HTTPS 流量會重新導向至 SonicOS 登入畫面，供使用者輸入自己的憑證。當 HTTP 和 HTTPS 流量是源自於使用者未登入的來源，且有一個或多個這類來源重複開啟新的連線而不斷觸發此重新導向時，將會導致問題的發生。這可能是正嘗試存取的非使用者裝置，或者也可能是正在嘗試進行拒絕服務 (DOS) 攻擊。這在防火牆上產生的效應就是會造成電腦上的高 CPU 負載，包括會啟動重新導向的資料平面工作，以及服務目標重新導向頁面的 Web 伺服器執行工作。

如需將影響降至最低，請務必在新增或編輯介面時，勾選**新增規則以啟用從 HTTP 到 HTTPS 的重新導向**核取方塊。勾選這個核取方塊後，SonicOS 就會新增存取規則，允許介面使用 HTTP；而這項規則的副作用，就是同時會導致 SonicOS 可在某些不造成安全性問題的情況下，將 HTTPS 重新導向至 HTTP。舉例來說，第一個步驟是先重新導向需要驗證的流量，其中並沒有需要隱藏的敏感資料。然後會在資料平面 (DP) 而非 CP 上進行 HTTP 程序。

附註：新增或編輯 VPN 通道介面，或者針對**模式/IP 指派**選取了**有線模式 (2 連接埠有線)**、**分接模式 (1 連接埠分接)** 或 **PortShield 交換器模式**時，系統都不會提供這個選項。

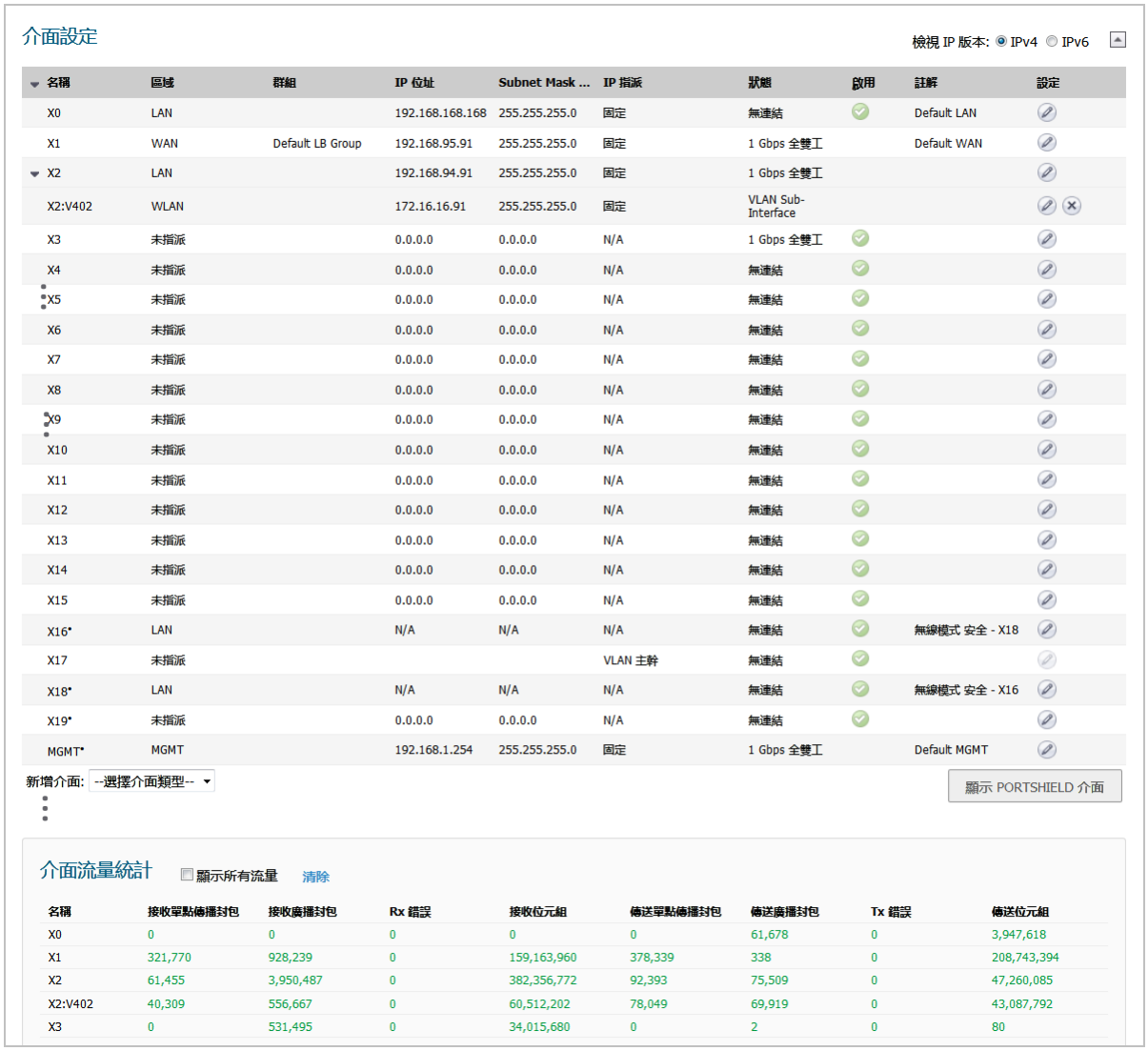
在介面上啟用 DNS 代理

當全域啟用 DNS 代理時，您可以在個別介面上啟用它。這可讓您個別為不同網路區段啟用功能。如需如何在介面上啟用 DNS 代理，請參見第 365 頁「啟用 DNS 代理」。

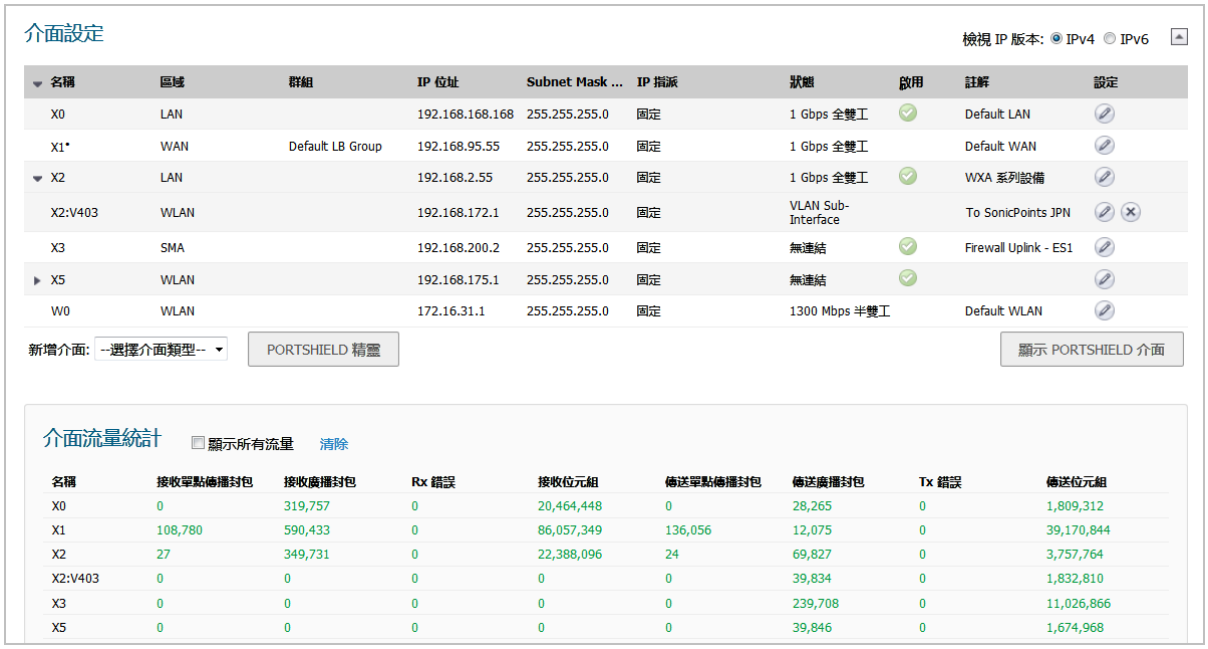
網路 | 介面

網路 | 介面頁面包含直接連結到實體介面的介面物件。SonicOS 的介面定址配置可配合網路區域和位址物件工作。NSA 2600 以上版本的安全設備和 TZ 與 SOHO 安全設備間有些許不同，這些差異處已加以註明。

NSA 2600 和 NSA 2600 以上版本的安全設備



TZ 和 SOHO 安全設備

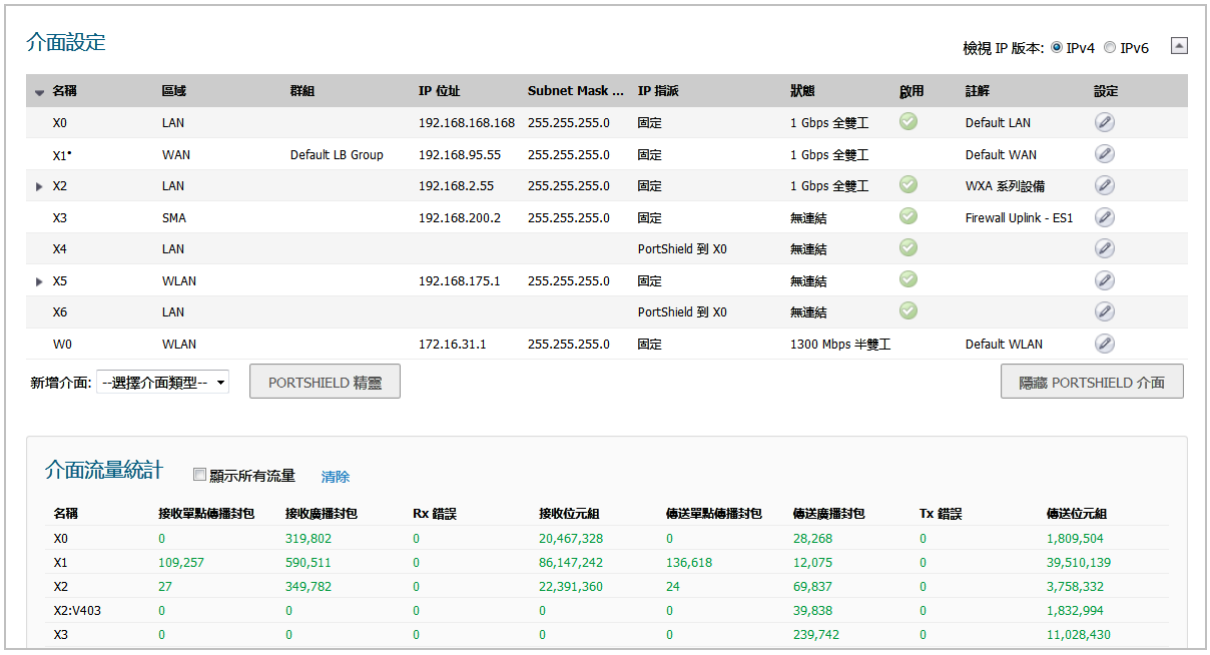


主題：

- 第 233 頁「顯示/隱藏 PortShield 介面 (僅限 IPv4)」
- 第 233 頁「介面設定」
- 第 234 頁「介面流量統計」
- 第 225 頁「實體和虛擬介面」
- 第 227 頁「SonicOS 安全物件」
- 第 228 頁「透明模式」
- 第 228 頁「IPS 偵測器模式」
- 第 234 頁「設定介面」
- 第 261 頁「設定 IPS 偵測器模式」
- 第 265 頁「設定有線和分接模式」
- 第 268 頁「帶有連結彙總的有線模式」
- 第 268 頁「二層橋接模式」
- 第 285 頁「設定二層橋接模式」
- 第 292 頁「設定 IPv6 介面」
- 第 292 頁「31 位元網路」
- 第 294 頁「PPPoE 未編號介面支援」

顯示/隱藏 PortShield 介面 (僅限 IPv4)

在 IPv4 模式中，您只要按一下**顯示 PortShield 介面**，系統就會在**介面設定**和**介面流量統計**表格中顯示 PortShield 介面。系統顯示 PortShield 介面後，按鈕就會變成**隱藏 PortShield 介面**。



若要隱藏 PortShield 介面，請按一下**隱藏 PortShield 介面**。

介面設定

介面設定表格中為每個介面列出了以下列資訊:

- **名稱** - 介面的名稱。
- **區域** - 預設列出 LAN、WAN、DMZ 和 WLAN。設定好的區域的名稱將在此欄中欄出。尚未設定的區域會指定為**未指派**。
- **群組** - 如果將介面指派至某個負載平衡群組，此組將會顯示在此欄中。
- **IP 位址** - 指派給介面的 IP 位址。
- **子網路遮罩** - 指派給子網路的網路遮罩。
- **IP 指派** - 可用的 IP 指派方法視介面指派到的目標區域而定:

  附註：有線模式和分接模式僅在 NSA 2600 和更高版本的安全設備可用。

  - **LAN**：固定、透明、二層橋接模式、有線模式、分接模式、PortShield 交換器模式、IP 未編號模式
  - **WAN**：固定、DHCP、PPPoE、PPTP、L2TP、有線模式、分接模式
  - **DMZ**：固定、透明、二層橋接模式、有線模式、分接模式、PortShield 交換器模式、IP 未編號模式
  - **WLAN**：固定、二層橋接模式、PortShield 交換器模式
  - **PortShield 至 X*n*** (僅限 IPv4 檢視): 如果已設定 PortShield 介面，PortShield 指派

- **狀態** - 連結狀態和速度。
- **已啟用** - 代表可透過**網路 | 介面**啟用/停用連接埠。已啟用的連接埠以**已啟用**圖示表示，已停用的連接埠以**已停用**圖示表示。按一下圖示後將顯示訊息驗證您想要啟用/停用連接埠。按一下**確定**。連接埠已啟用/停用，圖示隨之改變。
- **註解** - 任何使用者指定的註解。
- **設定** - 按一下**編輯**圖示可顯示**編輯介面**對話方塊，讓您設定指定介面的設定。如需介面設定相關資訊，請參閱第 234 頁「設定介面」。

介面流量統計

介面流量統計表為每個介面列出了所有已設定介面的接收和傳送資訊，包括 VLAN 子介面。

- **名稱** - 介面的名稱。
- **接收單點傳播封包** - 指示此介面所接收的點對點通訊數量。
- **Rx 廣播封包**或 **Rx 多點傳送封包** - 代表該介面接收的多點通訊數。
- **接收位元組數** - 指示此介面所接收的資料量（以位元組計）。
- **傳送單點傳播封包** - 指示此介面所傳送的點對點通訊數量。
- **Tx 廣播封包** - 指示此介面所傳送的多點通訊數量。
- **傳輸位元組數** - 指示此介面所傳送的資料量（以位元組計）。

如需清除目前的統計資料，請按一下**網路 | 介面**右上角的**清除**按鈕。

設定介面

主題：

- 第 268 頁「二層橋接模式」
- 第 285 頁「設定二層橋接模式」
- 第 291 頁「非對稱路由」
- 第 292 頁「設定 IPv6 介面」
- 第 292 頁「31 位元網路」
- 第 294 頁「PPPoE 未編號介面支援」

設定固定介面

如需介面的一般資訊，請參見第 225 頁「實體和虛擬介面」。

固定意味著將固定 IP 位址指派給介面。

設定固定介面的步驟是：

1 導覽到**管理 | 網路 | 介面**。

2 在**介面設定**表格中找出您想要設定的介面，然後按一下該介面的**設定**圖示。顯示**編輯介面**對話方塊。

3 在**區域**中選擇要指派給該介面的區域:

- **LAN**
- **WAN**
- **DMZ**
- **LAN**
- 自訂您已建立的區域
- **建立新區域**。隨即顯示**新增區域**對話。如需新增區域的說明，請參閱第 329 頁「關於區域」。

附註：顯示的選項隨著您選擇的**區域**而變化。

4 在 **IP 指派**中選取:

- **固定** (WAN 的預設設定)
- **固定 IP 模式** (LAN 的預設設定)

5 在 **IP 位址**和**子網路遮罩**欄位中輸入介面的 IP 位址和子網路遮罩。

附註：不能輸入與其他區域位於同一子網路中的 IP 位址。

6 如何設定下列項目:

- 設定 WAN 區域介面或 MGMT 介面時，請在**預設閘道**欄位中輸入閘道裝置的 IP 位址。

附註：如果需要透過不在 WAN 子網路 IP 位址空間的 WAN 介面到達目的地，那麼此 WAN 介面必須有預設閘道 IP，不管我們是否在 WAN 子網路上透過對等裝置的路由通訊協定接收預設動態路由。LAN 介面不一定要使用預設閘道 IP。

- 您在設定 WAN 區域介面或 MGMT 介面時，可選選擇市否要在**預設閘道 (選用)** 欄位中輸入閘道裝置的 IP 位址。

閘道裝置用於將此介面接入外部網路，無論是網際網路還是私人網路。

7 如何設定下列項目:

- 如需設定 LAN 區域介面，請移至步驟 8。
- 如需設定 WAN 區域介面，請在 **DNS 伺服器**欄位中輸入 DNS 伺服器的 IP 位址 (最多 3 個)。這些可以是公用或私人 DNS 伺服器。如需詳細資料，請參閱第 249 頁「設定 WAN 介面」。

8 在**註解**欄位中輸入任何可選的註解文字。這段文字會顯示在**介面設定**表格中的**註解**欄內。

9 如需透過這個介面啟用安全設備的遠端管理功能，請選擇支援的**管理**通訊協定: **HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。如果您選擇了 **HTTPS**，則系統會提供並選取**新增規則以啟用從 HTTP 到 HTTPS 的重新導向**。

若要允許存取 WAN 介面，以便從同一安全設備的其他區域進行管理，則必須建立存取規則。如需進一步瞭解如何允許從 LAN 區域存取 WAN 主要 IP，請參閱 *SonicOS 原則*。

10 如果想要允許擁有有限管理權限的選定使用者登入安全裝置，請在**使用者登入**中選擇 **HTTP** 和/或 **HTTPS**。

11 按一下**確定**。

附註：在變更防火牆位址之後，需要管理員密碼才能重新產生加密金鑰。

設定固定介面的進階設定

若要設定固定介面的進階設定。

1 在**編輯介面**對話方塊中按一下**進階**。

附註：固定介面的**進階**部分所提供的選項，會因所選區域而異。

編輯介面進階設定-WAN

編輯介面進階設定-LAN

2 對於**連結速度**，預設的選擇是**自動交涉**，連接的裝置將自動交涉乙太網路連接的速度和雙工模式。如需強制執行乙太網路速度和雙工模式，請在**連線速度**中選取下列其中一個選項:

對於 1 Gbps 介面	對於 10 Gbps 介面
1 Gbps - 全雙工	10 Gbps - 全雙工
100 Mbps - 全雙工	
100 Mbps - 半雙工	
10 Mbps - 全雙工	
10 Mbps - 半雙工	

△ 注意：**如果選擇某個特定的乙太網路速度和雙工模式，則還必須強制指定從乙太網路卡到安全設備的連接速度和雙工模式。**

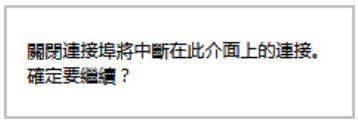
3 預設選擇**使用預設 MAC 位址**。您可以選擇覆寫介面的**使用預設 MAC 位址**，方法是選擇**覆寫預設 MAC 位址**，然後在該欄位中輸入 MAC 位址。

4 選取**關閉連接埠**，可讓這個介面因為維修或其他原因暫時離線。如果已連接，連結將中斷。預設情況下未勾選此選項。

取消選取這個選項時，系統會啟用介面，並且重新恢復連線。預設情況下未勾選此選項。

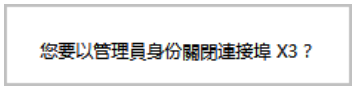
附註：無法關閉管理介面或目前正在使用的介面。

如果選擇此選項，將顯示確認訊息：

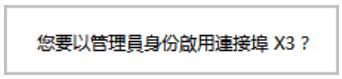


按一下**確認**以關閉連接埠。

提示：也可透過按一下介面**啟用**欄的**啟用**圖示關閉介面。將顯示確認訊息：



如果按一下**確認**，則**啟用**圖示變為**停用**圖示。如需啟用介面，按一下**停用**圖示。將顯示確認訊息：



如果按一下**確認**，則**停用**圖示變為**啟用**圖示。

5 對於 AppFlow 功能，選取**啟用流量報告**即可讓系統回報這個介面產生的流量。預設情況下已核取此選項。

6 (選用) 選取**啟用多點傳送支援**，即可在這個介面上接收多點傳送。預設情況下未勾選此選項。

7 (選用) 選取**啟用預設 802.1p CoS**，即可利用服務品質 (QoS) 管理所用的 802.1p 優先順序資訊，來標記經由這個介面的資訊。預設情況下未勾選此選項。

附註：此選項僅可用於 VLAN 介面。

將透過此介面傳送的封包標籤為 VLAN id=0 並攜帶 802.1p 優先順序資訊。若要使用此優先順序資訊，連接到此介面的裝置應支援優先順序框架。QoS 管理是由**管理 | 原則 | 規則 > 存取規則**中的存取規則予以控管。如需 QoS 和頻寬管理的資訊，請參閱 *SonicOS 原則*。

8 (選用) 如需在路由宣告中排除指定介面，請選取**從路由宣告中排除 (NSM、OSPF、BGP、RIP)** 預設情況下未勾選此選項。

9 也可選擇**僅管理流量**限制流量僅用於 SonicWall 管理流量和路由通訊協定。預設情況下未勾選此選項。

附註：只有 TZ 系列和 SOHO W 裝置有這個選項。

10 (可選)，如果您已啟用 DNS 代理，**啟用 DNS 代理**選項用於顯示 LAN、DMZ 或 WLAN 介面。如需在介面上啟用 DNS 代理，請選取這個選項。預設情況下未勾選此選項。

11 (選用) 選取**啟用非對稱路由支援**即可在介面上啟用非對稱路由支援。如果啟用此核取方塊，從此介面初始化的流量將支援非對稱路由，即初始封包或回應封包可以透過其他介面。預設情況下未勾選此選項。如需非對稱路由的更多資訊，請參閱第 530 頁「叢集設定中的非對稱路由」。

12 如果您設定了 LAN 介面，請移至第 240 頁「設定路由模式」。

13 (選用) 在**冗餘/彙總連接埠**中選取**連結彙總**或**連接埠冗餘**。更多資訊，請參見第 256 頁「設定連結彙總和連接埠冗餘」。

附註：此選項僅在 NSA 2600 及更高版本的裝置中可用。

14 若要指定介面不必分割封包即可轉送的最大封包大小 (MTU - 最大傳輸單元)，在**介面 MTU** 欄位輸入此連接埠將接收和傳送的封包的大小。

標準封包（預設）	1500
Jumbo 框架封包	9000

> **附註：**在連接埠可以處理 Jumbo 框架之前，必須啟用 Jumbo 框架支援，參閱 *SonicOS 原則*中的解釋。根據 Jumbo 框架封包緩衝大小的要求，Jumbo 框架對記憶體要求增加了 4 倍。
>
> NSA 3600 及更新裝置支援 Jumbo 框架。

15 (選用) 如需分割比介面的 MTU 更大的非 VPN 輸出封包，請選取**分割比這個介面的 MTU 大的非 VPN 輸出封包**。預設情況下已核取此選項。 選取後，下列選項即可供使用。

> **重要：管理 | 連線 | 進階設定**可供您指定分割輸出的 VPN 流量。詳情請參閱 *SonicOS 連線能力*。

16 (選用) 如需覆寫「不分割」封包位元，請選取**忽略不分割 (DF) 位元**。 預設情況下未勾選此選項。

17 如果您為這個介面設定了頻寬管理功能，請移至第 242 頁「在介面上啟用頻寬管理功能」。

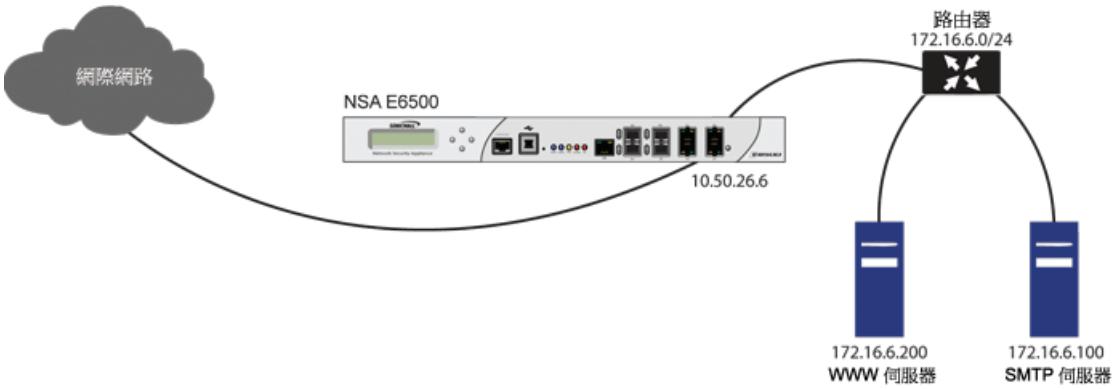
18 按一下**確定**。

設定路由模式

路由模式為用於路由單獨的公用 IP 位址範圍之間的流量的 NAT 提供了備選。考慮路由模式設定的拓撲，其中的安全設備正在路由以下兩個公用 IP 位址之間的流量：

- 10.50.26.0/24
- 172.16.6.0/24

路由模式設定



在 172.16.6.0 網路的介面上啟用路由模式後，系統會自動停用這個介面的 NAT 轉換功能，並且將所有傳入和傳出流量路由至用於設定 10.50.26.0 網路的 WAN 介面。

> **附註：**在 LAN、DMZ 和 WLAN 區域中使用介面的固定 IP 模式時，可以使用路由模式。對於 DMZ，在使用二層橋接模式時也可以使用路由模式。路由模式不適用於 WAN 模式。

如需設定路由模式：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下相應介面的**設定**圖示。將顯示**編輯介面**對話方塊。

3 按一下**進階**標籤。

4 如需為這個介面啟用路由模式，請在**專門的模式設定**之下，選取**專門的模式設定標題，再選取使用路由模式 — 新增 NAT 原則以阻止輸出\輸入轉換**。預設情況下未勾選此選項。選取這個選項後，就可使用後續的專門模式設定。

5 在 **NAT 原則輸出/輸入介面**下拉功能表中，選擇將用於傳送此介面的流量的 WAN 介面。預設值為**任何**。

6 若要指定介面不必分割封包即可轉送的最大封包大小 (MTU - 最大傳輸單元)，在**介面 MTU** 欄位輸入此連接埠將接收和傳送的封包的大小。

標準封包（預設）	1500
Jumbo 框架封包	9000

附註：在連接埠可以處理 Jumbo 框架之前，必須啟用 Jumbo 框架支援，參閱 *SonicOS 原則*中的解釋。根據 Jumbo 框架封包緩衝大小的要求，Jumbo 框架對記憶體要求增加了 4 倍。

NSA 3600 及更新裝置支援 Jumbo 框架。

7 如果安全設備上已啟用頻寬管理功能，系統隨即會顯示頻寬管理部分。如需為這個介面設定 BWM，請移至第 242 頁「在介面上啟用頻寬管理功能」。

8 按一下**確定**。

重要：安全設備會為已設定的介面和所選的 WAN 介面建立「無 NAT」原則。這些原則將替代可能已經為這些介面設定的所有更通用的 M21 NAT 原則。

在介面上啟用頻寬管理功能

您可以使用頻寬管理 (BWM) 來保證最小頻寬以及最佳化流量。您可以在**管理 | 安全設定 | 防火牆設定 > 頻寬管理**中啟用 BWM；如需頻寬管理 (BWM) 的相關資訊，請參閱 *SonicOS 安全設定*。透過控制應用程式或使用者的頻寬量，您可以防止少量應用程式或使用者消耗所有可用頻寬。負載均衡指派給不同網路流量的頻寬然後對流量指派優先順序可增強網路效能。

可啟用的頻寬管理種類:

- **進階** - 您可以透過設定頻寬物件、存取規則和應用程式原則，為各介面逐一設定最大輸出和輸入頻寬限制。
- **全域** - 您可以在全域範圍內啟用 BWM 設定，並將其套用於任何介面。
- **無** (預設)-停用 BWM。

如需設定頻寬管理和各種 BWM 類型的效果的資訊，請參閱 *SonicOS 安全設定*。

SonicOS 可以對任何介面上的輸出（傳出）和輸入（傳入）流量套用頻寬管理。傳出頻寬管理透過基於類的佇列完成。傳入頻寬管理透過實作使用 TCP 固有行為來控制流量的 ACK 延遲演算法完成。

基於類的佇列 (CBQ) 為防火牆提供了有保證的最大頻寬服務品質 (QoS)。發往介面的每個封包將在相應的優先順序佇列中排隊。隨後，調度程式使封包出列，並根據流量的保證頻寬和可用的連結頻寬，在連結上傳送封包。

啟用 BWM

若要啟用或停用輸入和輸出 BWM：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按下某個介面的**編輯**圖示。將顯示**新增/編輯介面**對話方塊。

3 如果這是未指派的介面，請根據第 234 頁「設定介面」中的各個專區來設定介面。

4 按一下**進階**標籤。

5 捲動至**頻寬管理**。

附註：進階設定會因為所選的安全設備型號和區域類型而有所差異。

6 為這個介面啟用頻寬管理功能。如需更多頻寬管理的相關資訊，請參閱 *SonicOS 安全設定*。

a 如需限制介面上的最大傳出流量頻寬，請選取**啟用介面輸出頻寬限制**。預設情況下未勾選此選項。

- 在**最大介面輸出頻寬**欄位，指定最大頻寬（單位為 kbps）。預設值為 **384.000000** kbps。

b 如需限制介面上的最大傳入流量頻寬，請選取**啟用介面輸入頻寬限制**。預設情況下未勾選此選項。

- 在**最大介面輸出頻寬**欄位，指定最大頻寬（單位為 kbps）。預設值為 **384.000000** kbps。

這些選項的狀態為:

- 勾選時，將定義最大可用輸出 BWM，但由於進階 BMW 基於原則，除非有相應存取規則或應用程式規則，否則不實施限制。
- 未勾選時，就不會在介面層級設定頻寬限制，但仍可以使用其他選項設定流量。

7 按一下**確定**。

設定透明 IP 模式下的介面（連接 L3 子網路）

透明 IP 模式可將 SonicWall 安全設備 WAN 子網路橋接到內部介面上。

若要設定用於透明模式的介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 找出您要設定的**未指派**介面，然後按一下該介面的**設定**圖示。將顯示**編輯介面**對話方塊。

3 您可以為區域選取

- **LAN** 或 **DMZ**。

  附註：可用的選項根據您選擇的區域類型而改變。

- 選取**建立新區域**，即可為可設定的介面建立新區域。隨即顯示**新增區域**對話。如需新增區域的說明，請參閱第 329 頁「關於區域」。

4 在**模式 / IP 指派**中，選取**透明 IP 模式 (連接 L3 子網路)**。

5 在**透明範圍**中，根據您想要透過這個介面存取的 IP 位址範圍，選取包含這個 IP 位址範圍的位址物件。位址範圍必須在內部區域以內，例如 LAN、DMZ 或其他與用於內部透明介面的區域相符合的受信任區域。

如果您沒有設定符合需求的位址物件，請選取**建立新的位址物件**。此時會顯示**新增位址物件**對話方塊。如需建立位址物件的相關資訊，請參閱 *SonicOS 原則*。

6 在**註解**欄位中輸入任何可選的註解文字。此文字將顯示在**介面**表的**註解**欄中。預設情況下未勾選此選項。

7 如需透過這個介面啟用安全設備的遠端管理功能，請選擇支援的管理通訊協定: **HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。預設情況下未勾選此選項。

若要允許存取 WAN 介面，以便從同一安全設備的其他區域進行管理，則必須建立存取規則。如需瞭解如何允許從 LAN 區域存取 WAN 主要 IP，請參閱 *SonicOS 原則*。

8 如需允許管理權限受限的指定使用者，直接透過這個介面登入安全設備，請在**使用者登入**中選取 **HTTP** 和/或 **HTTPS**。

9 如果您為**管理**和/或**使用者登入**通訊協定選取了 **HTTPS**，則系統會提供並選取**新增規則以啟用從 HTTP 到 HTTPS 的重新導向**。如需禁止 HTTP 到 HTTPS 的重新導向，請取消選取這個選項。

附註：為**使用者登入**通訊協定選取 **HTTP**，可停用重新導向。

10 按一下**確定**。

附註：更動安全設備位址之後，需使用管理員密碼才能重新產生加密金鑰。

設定透明 IP 模式介面的進階設定

若要設定透明 IP 模式介面的進階設定：

1 在**編輯介面**對話方塊中按一下**進階**。

2 對於**連結速度**，預設的選擇是**自動交涉**，連接的裝置將自動交涉乙太網路連接的速度和雙工模式。如需強制執行乙太網路速度和雙工模式，請在**連線速度**中選取下列其中一個選項:

對於 1 Gbps 介面	對於 10 Gbps 介面
1 Gbps - 全雙工	10 Gbps - 全雙工
100 Mbps - 全雙工	
100 Mbps - 半雙工	
10 Mbps - 全雙工	
10 Mbps - 半雙工	

△ 注意：**如果選擇某個特定的乙太網路速度和雙工模式，則還必須強制指定從乙太網路卡到安全設備的連接速度和雙工模式。**

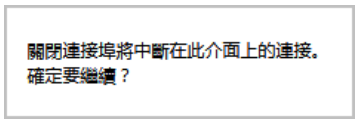
3 預設選擇**使用預設 MAC 位址**。您可以選擇覆寫介面的**使用預設 MAC 位址**，方法是選擇**覆寫預設 MAC 位址**，然後在該欄位中輸入 MAC 位址。

4 選取**關閉連接埠**，可讓這個介面因為維修或其他原因暫時離線。如果已連接，連結將中斷。預設情況下未勾選此選項。

取消選取這個選項時，系統會啟用介面，並且重新恢復連線。預設情況下未勾選此選項。

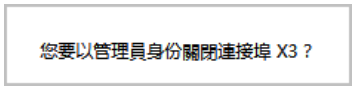
附註：無法關閉管理介面或目前正在使用的介面。

如果選擇此選項，將顯示確認訊息：

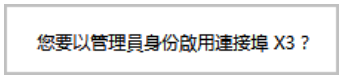


按一下**確認**以關閉連接埠。

提示：也可透過按一下介面**啟用**欄的**啟用**圖示關閉介面。將顯示確認訊息：



如果按一下**確認**，則**啟用**圖示變為**停用**圖示。如需啟用介面，按一下**停用**圖示。將顯示確認訊息：



如果按一下**確認**，則**停用**圖示變為**啟用**圖示。

5 對於 AppFlow 功能，選取**啟用流量報告**即可讓系統回報這個介面產生的流量。預設情況下已核取此選項。

6 (選用) 選取**啟用多點傳送支援**，即可在這個介面上接收多點傳送。預設情況下未勾選此選項。

7 (選用) 選取**啟用預設 802.1p CoS**，即可利用服務品質 (QoS) 管理所用的 802.1p 優先順序資訊，來標記經由這個介面的資訊。預設情況下未勾選此選項。

附註：此選項僅可用於 VLAN 介面。

將透過此介面傳送的封包標籤為 VLAN id=0 並攜帶 802.1p 優先順序資訊。若要使用此優先順序資訊，連接到此介面的裝置應支援優先順序框架。QoS 管理是由**管理 | 原則 | 規則 > 存取規則**中的存取規則予以控管。如需 QoS 和頻寬管理的資訊，請參閱 *SonicOS 原則*。

8 (選用) 如需在路由宣告中排除指定介面，請選取**從路由宣告中排除 (NSM、OSPF、BGP、RIP)** 預設情況下未勾選此選項。

9 也可選擇**僅管理流量**限制流量僅用於 SonicWall 管理流量和路由通訊協定。預設情況下未勾選此選項。

附註：只有 TZ 系列和 SOHO W 裝置有這個選項。

10 (選用) 如果您已啟用 DNS 代理，**啟用 DNS 代理**選項可用於顯示相關內容。如需在介面上啟用 DNS 代理，請選取這個選項。預設情況下未勾選此選項。

11 (選用) 選取**啟用非對稱路由支援**即可在介面上啟用非對稱路由支援。如果啟用此核取方塊，從此介面初始化的流量將支援非對稱路由，即初始封包或回應封包可以透過其他介面。預設情況下未勾選此選項。如需非對稱路由的更多資訊，請參閱第 530 頁「叢集設定中的非對稱路由」。

12 如果您設定了 TZ 系列和 SOHO 系列安全設備，請移至步驟 14。

13 (選用) 在**冗餘/彙總連接埠**中選取**連結彙總**或**連接埠冗餘**。更多資訊，請參見第 256 頁「設定連結彙總和連接埠冗餘」。

附註：此選項僅在 NSA 2600 及更高版本的裝置中可用。

14 勾選**使無償 ARP 能夠轉送到 WAN** 使用 WAN 介面的硬體 MAC 位址作為來源 MAC 位址，將在此介面收到的免費 ARP 封包轉到 WAN。

15 勾選**使無償 ARP 能夠自動產生到 WAN** 每當在向此介面的新機器的 ARP 表新增新項目時，將免費 ARP 封包自動傳送至 WAN。WAN 介面的硬體 MAC 位址用作 ARP 封包的來源 MAC 位址。

16 若要指定介面不必分割封包即可轉送的最大封包大小 (MTU - 最大傳輸單元)，在**介面 MTU** 欄位輸入此連接埠將接收和傳送的封包的大小。

標準封包（預設）	1500
Jumbo 框架封包	9000

附註：在連接埠可以處理 Jumbo 框架之前，必須啟用 Jumbo 框架支援，參閱 *SonicOS 原則*中的解釋。根據 Jumbo 框架封包緩衝大小的要求，Jumbo 框架對記憶體要求增加了 4 倍。

NSA 3600 及更新裝置支援 Jumbo 框架。

17 頻寬管理功能啟用後，如果您想要為這個介面設定 BWM，請移至第 242 頁「在介面上啟用頻寬管理功能」。

18 按一下**確定**。

設定無線介面

無線介面是已指派給無線區域並用於支援 SonicWall SonicPoint 安全存取點的介面。

附註：SonicPoints 只能在安全類型無線（預設為 WLAN）的介面上進行設定和管理。

若要設定無線介面:

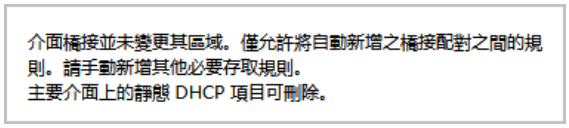
1 在**編輯介面**對話方塊中按一下**進階**。

2 按一下想要設定的介面對應的**設定**欄中的**編輯**圖示。顯示**編輯介面**對話方塊。

3 在**區域**，選擇 **WLAN** 或先前定義的自訂無線區域。

4 對於**模式/ IP 指派**，您可以選取下列其中一個選項:

- **固定 IP 模式** (LAN 的預設設定)；請移至
- **二層橋接模式**；詳情請參閱第 268 頁「二層橋接模式」。如果您選取了這個模式，系統會顯示下列訊息:



重要：選擇這個模式時，需要為橋接配對設定存取規則。如需設定存取規則的相關資訊，請參閱 *SonicOS 原則*。

5 在 **IP 位址**和**子網路遮罩**欄位中輸入此區域的 IP 位址和子網路遮罩。

附註：子網路遮罩的上限取決於您在 **SonicPoint/SonicWave 限制**中選取的 SonicPoints 數量。如果您將若干個介面或子介面設定為無線介面，則可能需要使用較小的子網路（較高）來限制此介面可能提供的 DHCP 租用數量。否則，如果您為每個無線介面使用 C 類子網路（子網路遮罩 `255.255.255.0`），則可能超出安全設備提供的 DHCP 租用限制。

6 在 **SonicPoint/SonicWave 限制**中，選取這個介面中允許的 SonicPoints 數量上限。

- 此值決定了可以在**子網路遮罩**欄位中輸入的最高子網路遮罩值。下表顯示了每個 **SonicPoint 限制**選項的子網路遮罩限制，以及在您輸入允許的最大子網路遮罩的情況下，介面所提供的 DHCP 租用數量。
- 除了此介面上允許存在的最大 SonicPoints 數量以外（每個消耗一個 IP 位址），可用的用戶端 IP 還提供了 1 個用於防火牆閘道介面的 IP。

允許的最大子網路遮罩大小

每個介面的 SonicPoint/SonicWave	最大子網路遮罩	可用的 IP 位址總數	可用的用戶端 IP 位址
無	30 位元 - 255.255.255.252	2	2
2	29 位元 - 255.255.255.248	6	3
4	29 位元 - 255.255.255.248	6	1
8	28 位元 - 255.255.255.240	14	5
16	27 位元 - 255.255.255.224	30	13
24	26 位元 - 255.255.255.192	62	29
32	26 位元 - 255.255.255.192	62	29
48	25 位元 - 255.255.255.128	126	77
64	25 位元 - 255.255.255.128	126	61
96	24 位元 - 255.255.255.0	190	93
128	23 位元 - 255.255.254.0	254	125

附註：允許的最大子網路遮罩大小表格描述了允許的最大子網路遮罩大小。您仍舊可以在 WLAN 介面上使用完全類別的子網路劃分（A 類、B 類或 C 類），或任何希望使用的可變長度子網路遮罩。我們鼓勵您使用較小的子網路遮罩（例如 24 位元 C 類：255.255.255.0 - 總計 254 個可用 IP），從而在您需要支援更大數量的無線用戶端時向用戶端指派更多的 IP 定址空間。我們鼓勵您使用較小的子網路遮罩（例如 24 位 C 類 - 255.255.255.0 - 總計 254 個可用 IP），從而在您需要支援更大數量的無線用戶端時向用戶端指派更多的 IP 定址空間。

7 在**註解**欄位中輸入任何可選的註解文字。此文字將顯示在**介面**表的**註解**欄中。

8 如果想要啟用透過此介面遠端管理防火牆，請選擇支援的管理通訊協定：**HTTPS**、**Ping**、**SNMP** 和 / 或 **SSH**。

若要允許存取 WAN 介面，以便從同一安全設備的其他區域進行管理，則必須建立存取規則。如需瞭解如何允許從 LAN 區域存取 WAN 主要 IP，請參閱 *SonicOS 原則*。

9 如果想要允許擁有有限管理權限的選定使用者登入安全裝置，請在**使用者登入**中選擇 **HTTP** 和/或 **HTTPS**。

10 按一下**確定**。

設定無線介面的進階設定

若要設定無線介面的進階設定：

1 在**編輯介面**對話方塊中，按一下**進階**標籤。

2 對於**連結速度**，預設的選擇是**自動交涉**，連接的裝置將自動交涉乙太網路連接的速度和雙工模式。如需強制執行乙太網路速度和雙工模式，請在**連線速度**中選取下列其中一個選項:

對於 1 Gbps 介面	對於 10 Gbps 介面
1 Gbps - 全雙工	10 Gbps - 全雙工
100 Mbps - 全雙工	
100 Mbps - 半雙工	
10 Mbps - 全雙工	
10 Mbps - 半雙工	

△ 注意：**如果選擇某個特定的乙太網路速度和雙工模式，則還必須強制指定從乙太網路卡到安全設備的連接速度和雙工模式。**

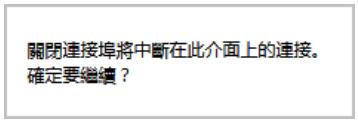
3 預設選擇**使用預設 MAC 位址**。您可以選擇覆寫介面的**使用預設 MAC 位址**，方法是選擇**覆寫預設 MAC 位址**，然後在該欄位中輸入 MAC 位址。

4 選取**關閉連接埠**，可讓這個介面因為維修或其他原因暫時離線。如果已連接，連結將中斷。預設情況下未勾選此選項。

取消選取這個選項時，系統會啟用介面，並且重新恢復連線。預設情況下未勾選此選項。

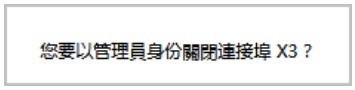
ⓘ **附註：**無法關閉管理介面或目前正在使用的介面。

如果選擇此選項，將顯示確認訊息：

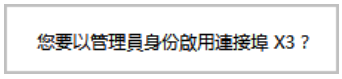


按一下**確認**以關閉連接埠。

提示：也可透過按一下介面**啟用**欄的**啟用**圖示關閉介面。將顯示確認訊息：



如果按一下**確認**，則**啟用**圖示變為**停用**圖示。如需啟用介面，按一下**停用**圖示。將顯示確認訊息：



如果按一下**確認**，則**停用**圖示變為**啟用**圖示。

5 對於 AppFlow 功能，選取**啟用流量報告**即可讓系統回報這個介面產生的流量。預設情況下已核取此選項。

6 (選用) 選取**啟用多點傳送支援**，即可在這個介面上接收多點傳送。預設情況下未勾選此選項。

7 (選用) 選取**啟用預設 802.1p CoS**，即可利用服務品質 (QoS) 管理所用的 802.1p 優先順序資訊，來標記經由這個介面的資訊。預設情況下未勾選此選項。

ⓘ **附註：**此選項僅可用於 VLAN 介面。

將透過此介面傳送的封包標籤為 VLAN id=0 並攜帶 802.1p 優先順序資訊。若要使用此優先順序資訊，連接到此介面的裝置應支援優先順序框架。QoS 管理是由**管理 | 原則 | 規則 > 存取規則**中的存取規則予以控管。如需 QoS 和頻寬管理的資訊，請參閱 *SonicOS 原則*。

8 (選用) 如需在路由宣告中排除指定介面，請選取**從路由宣告中排除 (NSM、OSPF、BGP、RIP)** 預設情況下未勾選此選項。

9 如果您設定了 SuperMassive 或 NSA 系列設備，請移至步驟 11。

10 也可選擇**僅管理流量**限制流量僅用於 SonicWall 管理流量和路由通訊協定。預設情況下未勾選此選項。

附註：只有 TZ 系列和 SOHO 系列安全設備設有這個選項。

11 (選用) 如果您已啟用 DNS 代理，**啟用 DNS 代理**選項可用於顯示相關內容。如需在介面上啟用 DNS 代理，請選取這個選項。預設情況下未勾選此選項。

12 (選用) 選取**啟用非對稱路由支援**即可在介面上啟用非對稱路由支援。如果啟用此核取方塊，從此介面初始化的流量將支援非對稱路由，即初始封包或回應封包可以透過其他介面。預設情況下未勾選此選項。如需非對稱路由的更多資訊，請參閱第 530 頁「叢集設定中的非對稱路由」。

13 如果您設定了 TZ 系列和 SOHO 系列安全設備，請移至步驟 14。

14 (選用) 在**冗餘/彙總連接埠**中選取**連結彙總**或**連接埠冗餘**。更多資訊，請參見第 256 頁「設定連結彙總和連接埠冗餘」。

附註：此選項僅在 NSA 2600 及更高版本的裝置中可用。

15 勾選**使無償 ARP 能夠轉送到 WAN** 使用 WAN 介面的硬體 MAC 位址作為來源 MAC 位址，將在此介面收到的免費 ARP 封包轉到 WAN。

16 勾選**使無償 ARP 能夠自動產生到 WAN** 每當在向此介面的新機器的 ARP 表新增新項目時，將免費 ARP 封包自動傳送至 WAN。WAN 介面的硬體 MAC 位址用作 ARP 封包的來源 MAC 位址。

17 若要指定介面不必分割封包即可轉送的最大封包大小 (MTU - 最大傳輸單元)，在**介面 MTU** 欄位輸入此連接埠將接收和傳送的封包的大小。

標準封包（預設）	1500
Jumbo 框架封包	9000

附註：在連接埠可以處理 Jumbo 框架之前，必須啟用 Jumbo 框架支援，參閱 *SonicOS 原則*中的解釋。根據 Jumbo 框架封包緩衝大小的要求，Jumbo 框架對記憶體要求增加了 4 倍。

NSA 3600 及更新裝置支援 Jumbo 框架。

18 如果您為這個介面設定了路由模式，請移至第 240 頁「設定路由模式」。

19 頻寬管理功能啟用後，如果您想要為這個介面設定 BWM，請移至第 242 頁「在介面上啟用頻寬管理功能」。

20 按一下**確定**。

設定 WAN 介面

附註：如果需要透過不在 WAN 子網路 IP 位址空間的 WAN 介面到達目的地，那麼此 WAN 介面必須有預設閘道 IP，不管我們是否在 WAN 子網路上透過對等裝置的路由通訊協定接收預設動態路由。

設定 WAN 介面可實現網際網路連接。您可以在 SonicWall 安全裝置上最多設定 *N* 減 *2* 個 WAN 介面，其中，*N* 是在裝置上定義的介面數（實體和 VLAN）。只有 X0 和 MGMT 介面不能設定為 WAN 介面。

若要設定 WAN 介面:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下想要設定的介面對應的**設定**欄中的**編輯**圖示。將顯示**編輯介面**對話方塊。

3 如果您正在設定未指派的介面，請從**區域**功能表中選擇 **WAN**。如果您選擇了**預設 WAN** 介面，則在**區域**功能表中已經勾選 **WAN**。

4 在 **IP 指派**中選擇下列其中一個 WAN 網路定址模式。

> ⓘ **附註：**可用的選項根據您從 「IP 指派」下拉功能表選擇的選項而變化。填寫在選擇選項後顯示的相應欄位。

- **固定** - 為使用固定 IP 位址的網路設定安全設備。
- **DHCP** - 設定安全設備，以便向網際網路上的 DHCP 伺服器請求 IP 設定。帶有 DHCP 用戶端的 NAT 是有線電視網路和 DSL 客戶常用的網路定址模式。
- **PPPoE** - 使用乙太網路點對點通訊協定 (PPPoE) 連接到網際網路。如果 ISP 要求使用者名稱和密碼，則在**使用者名稱**和**使用者密碼**欄位中相應輸入。使用 DSL 數據機時通常使用此通訊協定。
- **PPTP** - 使用 PPTP（點對點通道通訊協定）連接到遠端伺服器。它支援較早的需要通道連接的 Microsoft Windows 實作。
- **L2TP** - 使用 IPsec 連接 L2TP（二層通道通訊協定）伺服器，並對從用戶端到伺服器傳送的所有資料進行加密。但是，它不會對其他目的地的網路流量進行加密。
- **有線模式（2 連接埠有線）** - 允許在旁路、檢查或安全模式中將安全設備插入網路。如需更多資訊，請參見第 265 頁「設定有線和分接模式」。
- **分接模式（1 連接埠分接）** - 允許將安全設備插入網路以配合網路分接、連接埠鏡像或 SPAN 連接埠使用。如需更多資訊，請參見第 265 頁「設定有線和分接模式」。

5 如果使用 **DHCP**，可以選擇在**主機名稱**欄位中輸入描述性名稱和在**註解**欄位中輸入任何需要的註解。

6 如果使用 **PPPoE**、**PPTP** 或 **L2TP**，將顯示附加欄位：

- 如果顯示**排程**，從下拉清單中選擇所需排程，在此期間應連接介面。
- 在**使用者名稱**和**使用者密碼**中，輸入您的 ISP 提供的帳戶名稱和密碼。
- 如果顯示**伺服器 IP 位址**欄位，輸入您的 ISP 提供的伺服器 IP 位址。
- 如果顯示（**用戶端**）**主機名稱**欄位，則輸入裝置的主機名稱。這個防火牆名稱來自於**管理 | 系統安裝 | 設備 > 基本設定**。
- 如果顯示**共用密碼**欄位，輸入您的 ISP 提供的值。

7 如果想要啟用透過此介面遠端管理安全設備，請選擇支援的管理通訊協定：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

若要允許存取 WAN 介面，以便從同一安全設備的其他區域進行管理，則必須建立存取規則。如需建立存取規則的相關資訊，請參閱 *SonicOS 原則*。

8 如果使用 PPPoE、PPTP 或 L2TP，將顯示附加欄位：

- 對於 PPPoE，請選擇下列其中一個選項:
  - **自動取得 IP 位址**，即可從 PPPoE 伺服器取得 IP 位址。
  - **指定 IP 位址**，然後在欄位中輸入所需的 IP 位址，即可使用這個介面的固定 IP 位址。
  - **未編號的介面**，然後進行下列其中一種操作:

- 選擇未編號的介面。
- 通過選擇**建立新的未編號介面**來建立新的未編號介面。

  附註：介面必須為未指派。

- 對於 PPTP 或 L2TP，請設定下列選項:
  - 選取**非使用狀態中斷連接**，然後輸入所需的分鐘數，指定進入非使用狀態多久後開始中斷連線。取消選取這個選項，即可停用非使用中逾時。
  - 在 **IP 指派**中選取下列其中一個選項:
    - **DHCP**；IP 位址、子網路遮罩和閘道位址欄位將由伺服器自動提供。
    - **固定**，輸入這些欄位的相應值。

9 如果您使用 DHCP，則可自行決定是否選取下列選項:

- **啟動時對以前的 IP 發出更新請求**為 WAN 介面請求之前由 DHCP 伺服器提供的相同 IP 位址。
- **在發生任意上行連結時更新 DHCP 租用**在 WAN 介面每次斷開後重新連接時，向 DHCP 伺服器傳送租用更新請求。

在這些選項下面顯示的欄位由 DHCP 伺服器提供。佈建後，這些按鈕即可供使用；您可以選擇:

- **更新**為目前指派的 IP 位址重新啟動 DHCP 租用期間。
- **釋放**為目前的 IP 位址取消 DHCP 租用。連接將斷開。您需要從 DHCP 伺服器獲取新 IP 位址以重新建立連接。
- **重新整理**從 DHCP 伺服器獲取新 IP 位址。

10 如需允許管理權限受限的指定使用者，直接透過這個介面登入安全裝置，請在**使用者登入**中選擇 **HTTP** 和/或 **HTTPS**。

11 如果要將 HTTP 連接自動重新導向至連接安全設備的安全 HTTPS 連接，請勾選**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。

12 繼續在**進階**和**通訊**協定標籤（如顯示）中設定，如第 251 頁「設定 WAN 介面的進階設定」所述。

13 如需繼續進行進階設定，請移至第 251 頁「設定 WAN 介面的進階設定」。

14 如果您針對 **IP 指派**選取了 **PPPoE**、**PPTP** 或 **L2TP**，請移至第 253 頁「設定 WAN 介面的通訊協定設定」。

15 按一下**確定**。

設定 WAN 介面的進階設定

若要設定 WAN 介面的進階設定：

1 在**編輯介面**對話方塊中，按一下**進階**標籤。

2 對於**連結速度，預設的選擇是自動交涉**，連接的裝置將自動交涉乙太網路連接的速度和雙工模式。如果想要指定強制乙太網路速度和雙工模式，請從**連結速度**功能表中選擇以下選項之一：

- 對於 1 Gbps 介面，請選擇：
  - **1 Gbps - 全雙工**
  - **100 Mbps - 全雙工**

- **100 Mbps - 半雙工**
- **10 Mbps - 全雙工**
- **10 Mbps - 半雙工**

- 對於 10 Gbps 介面，只能選擇 **10 Gbps - 全雙工**。

重要：如果選擇某個特定的乙太網路速度和雙工模式，則還必須強制指定從乙太網路卡到防火牆的連接速度和雙工模式。

3 您可以選擇覆寫介面的**使用預設 MAC 位址**，方法是選擇**覆寫預設 MAC 位址**，並在欄位中輸入 MAC 位址。

4 勾選**關閉連接埠**核取方塊出於維護或其他原因暫時使此介面離線。如果連線，連結會中斷。清除核取方塊會啟用介面，並讓連結恢復連線。

5 對於 AppFlow 功能，選取**啟用流量報告**核取方塊即可讓系統回報這個介面產生的流量。

6 勾選**啟用多點傳送支援**核取方塊允許在此介面上接收多點傳送。

7 勾選**啟用 802.1p 標記**核取方塊，為透過此介面的資訊標記用於服務品質 (QoS) 管理的 802.1p 優先順序資訊。將透過此介面傳送的封包標籤為 VLAN id=0 並攜帶 802.1p 優先順序資訊。若要使用此優先順序資訊，連接到此介面的裝置應支援優先順序框架。QoS 管理是由**管理 | 安全設定 | 防火牆規則 > 服務品質對應**中的存取規則予以控管。如需 QoS 和頻寬管理的相關資訊，請參閱 *SonicOS 安全設定*。

8 另外，還可以選擇從**冗餘 / 彙總連接埠**下拉清單中選擇**連結彙總**或**連接埠冗餘**。更多資訊，請參見第 256 頁「設定連結彙總和連接埠冗餘」。

9 **介面 MTU** - 指定無需對封包進行片段即可由介面轉送的最大封包大小。識別此連接埠將接收和傳送的封包的大小：

標準封包（預設）	1500
Jumbo 框架封包	9000

附註：您必須先啟用 Jumbo 框架支援，連接埠才能處理 jumbo 框架。如需更多 jumbo 框架的相關資訊，請參閱 *SonicOS 安全設定*。根據 Jumbo 框架封包緩衝大小的要求，Jumbo 框架對記憶體要求增加了 4 倍。

NSA 3600 及更新裝置支援 Jumbo 框架。

- **片段非 VPN 出口封包大於該介面的 MTU** - 指定對大於此介面的 MTU 的所有非 VPN 傳出封包進行片段。您可以在**管理 | 連線 | VPN** 中設定 VPN 傳出封包的分割作業，如需進一步瞭解 VPN 流量，請參閱 *SonicOS 連線能力*。
- **忽略不片段 (DF) 位元** - 覆寫封包中的不片段 (DF) 位元。
- **不傳送 ICMP 片段出口封包大於介面 MTU** - 封鎖此介面可以接收片段封包的通知。

10 如果使用 DHCP，將顯示以下選項：

- 如果伺服器可能有所更動，請選取**使用 DHCP 時進行更新並啟用探索功能**。
- 勾選**在獲取租用的過程中，使用 DHCP 探索之間的 _ 秒間隔**，並在 DHCP 伺服器沒有立即回應時調整間隔秒數。

11 另外，也可以選擇對此介面啟用「頻寬管理」。如需頻寬管理的更多資訊，請參見第 242 頁「在介面上啟用頻寬管理功能」。

設定 WAN 介面的通訊協定設定

如果您在設定 WAN 介面時針對 **IP 指派**指定了 **PPPoE**、**PPTP** 或 **L2TP**，則**編輯介面**對話方塊就會顯示**通訊協定**標籤。

網際網路服務供應商 (ISP) 在「**通訊協定**」標籤的**設定獲取方式**區段提供欄位（例如 **SonicWall IP 位址**、**子網路遮罩**和**閘道位址**）。您將安全設備連上 ISP 後，這些欄位就會顯示實際值。

此外，如果指定了 PPPoE，SonicOS 將「**進階**」標籤中的介面 MTU 選項設為 **1492**，並在「**通訊協定**」標籤中提供附加設定。

若要設定 PPPoE 的附加設定：

1 在**編輯介面**對話方塊中，按一下**通訊協定**。

2 在 **PPPoE 用戶端設定**部分中啟用下列選項:

- **非使用中狀態中斷連接（分鐘數）：**輸入分鐘數（預設為 10），在這段時間後，SonicOS 如果偵測到未傳送封包，將中斷連接。預設情況下未勾選此選項。

- **為保持伺服器活動，嚴格使用 LCP 回應封包**：勾選此選項使 SonicOS 在偵測到 PPoE 伺服器未在一分鐘內傳送 ppp LCP 回應請求封包時中斷連接。只有在 PPPoE 伺服器支援傳送 LCP 回應功能時，才勾選此選項。預設情況下未勾選此選項。
- **如果伺服器在 _ 分鐘內不傳送流量，則重新連接 PPPOE 用戶端**：輸入分鐘數（預設為 5），在這段時間後，如果伺服器不傳送任何封包（包括 LCP 回應請求），SonicOS 將終止 PPPoE 伺服器的連接，然後重新連接。預設情況下已核取此選項。

設定通道介面

您可以在 SonicOS 設定幾種類型通道介面。**網路 | 介面**可用於設定已編號的通道介面、WLAN 通道介面和 IPv6 6to4 通道介面。捨棄通道介面可由**網路 | 路由**進行設定，而未編號的通道介面則會設定為 VPN 原則的一部分 (由**管理 | 連線 | VPN** 進行設定)；如需 VPN 原則的相關資訊，請參閱 *SonicOS 連線能力*。

編號的和未編號的通道介面是搭配 VPN 使用。編號的通道介面是指派其自身的 IP 位址，但是未編號的通道介面是從現有的實體或虛擬 (VLAN) 介面借用 IP 位址。

已編號和未編號通道介面類型，都支援固定路由和動態路由 (透過 RIP 和 OSPF)，同時編號的通道介面也可搭配 BGP 使用。

如需瞭解如何設定各種類型的通道介面，請參閱下列章節:

- 編號的通道介面；參見第 254 頁「設定 VPN 通道介面」
- 未編號的通道介面；請參閱 *SonicOS 連線能力*。
- 丟棄通道介面；參見第 383 頁「丟棄通道介面」
- IPv6 6to4 通道介面；參見第 776 頁「設定 6 至 4 自動通道」

設定 VPN 通道介面

您可以從新增介面下拉清單中選擇 VPN 通道介面來建立編號的通道介面。在新增 VPN 通道介面到介面設定表格後，即可搭配使用動態路由，包括 RIP、OSPF 和 BGP，或者固定路由可在基於固定路由的 VPN 設定中使用 VPN 通道介面作為介面。

VPN 通道介面的設定方法類似於標準介面，包括的選項有啟用裝置管理或使用 HTTP、HTTPS、Ping 或 SSH 的使用者登入，以及多點傳送、流量報告、非對稱路由、片段封包處理和不片段 (DF) 位元等。

附註：必須在遠端閘道上設定類似的 VPN 原則和編號的通道介面。指派到編號通道介面（本機閘道和遠端閘道）的 IP 位址必須位於相同子網路中。

VPN 通道介面部署表格列出 VPN 通道介面的部署方式

VPN 通道介面部署

通道介面可以設定的地方	通道介面不能設定為
固定路由	固定 ARP 項目介面
NAT	HA 介面
ACL（虛擬存取點存取控制清單）	WLB （WAN 負載平衡）介面
	固定 NDP （鄰居搜索通訊協定）項目介面
OSPF	OSPFv3/RIPnG：目前不支援 IPv6 進階路由
RIP	MAC_IP 反詐騙介面
BGP	DHCP 伺服器介面

對於所有平台，支援的 VPN 通道介面 (編號的通道介面) 最大數量為 64。未編號的通道介面的數量上限依平台而不同，並且在每個平台上直接對應到最大數量的支援的 VPN 原則。

若要設定 VPN 通道介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 在**介面設定**表格下方的**新增介面**中，選取 **VPN 通道介面**。此時會顯示**新增通道介面**對話方塊。

區域會定義為 VPN 且無法變更。

3 在 **VPN 原則**中選取 VPN 原則。

4 在**名稱**欄位中，為此介面輸入一個易記的名稱。此名稱可包含字元、句點或底線；不能包含空白字元或連字元。

5 在 **IP 位址**欄位輸入 IP 位址。預設值為 **0.0.0.0**，但是您需要輸入顯見 IP 位址，否則將顯示錯誤訊息。

6 在**子網路遮罩**欄位，輸入子網路遮罩。預設值為 **255.255.255.0**。

7 可以選擇在**註解**欄位中新增註解。

8 也可指定此介面允許的**管理**通訊協定：**HTTPS**、**Ping**、**SNMP** 和/或 **SSH**。

9 也可指定此介面允許的**使用者登入**通訊協定：**HTTP** 和/或 **HTTPS**。

10 按一下**進階**。

11 若要為此通道介面建立的流量允許流量報告，選擇**啟用流量報告**。預設情況下已核取此選項。

12 (選用) 選取**啟用多點傳送支援**，即可在介面上接收多點傳送。預設情況下未勾選此選項。

13 (選用) 選取**啟用非對稱路由支援**，即可在通道介面上啟用非對稱路由支援。預設情況下未勾選此選項。如需非對稱路由的更多資訊，請參閱第 530 頁「叢集設定中的非對稱路由」。

14 如需使用路由模式並新增 NAT 原則以以阻止輸出/輸入轉換，請選取**使用路由模式 — 新增 NAT 原則以阻止輸出/輸入轉換**。選取後，下列選項即可供使用。 預設情況下未勾選此選項。

15 選取路由模式後，如需指定 NAT 原則介面，請在 **NAT 原則輸出/輸入介面**中選取所需介面。可用的介面視您的安全設備而定。預設值為**任何**。

16 如需在這個介面上啟用分割封包處理功能，請選取**啟用分割封包處理**核取方塊。若未選擇此選項，分割封包將丟棄且 VPN 記錄報告將顯示記錄訊息分割 `IPsec` 封包已丟棄。預設情況下已核取此選項。

若已選擇此選項，**忽略不片段 (DF) 位元**選項可以使用。

17 選取**忽略不分割 (DF) 位元**，即可忽略封包標題中的 DF 位元。某些應用程式可能會在封包中明確設定「不分割」選項，告知所有安全設備不要切割封包。啟用此選項時，會致使安全設備忽略 DF 位元，仍然將封包分段。

18 按一下**確定**。將編號的 VPN 通道介面新增到**介面設定**表格。

設定連結彙總和連接埠冗餘

附註：NSA 2600 及更高版本安全設備支援連結彙總和連接埠冗餘。

連結彙總和連接埠冗餘都是在 SonicOS 管理介面**編輯介面**對話方塊的**進階**標籤中設定。

- 第 257 頁「連結彙總」 - 將多個乙太網路介面組合在一起構成單個邏輯連結，以支援大於單個實體介面所能支援的傳送量。這樣可以實現在兩個乙太網路網域之間傳送幾 GB 流量的能力。

  附註：NSA 2600 和 NSA 2600 以上版本的安全設備支援連結彙總。NSA 2600 支援網路介面的連結彙總，但 NSA 2600 不支援交換功能，因此不支援交換連結彙總，第 495 頁「交換 | 連結彙總」中提供了相關說明。

  二層橋接模式不支援連結彙總。

- 第 259 頁「連接埠冗餘」 - 為可連接至另一個交換器的任意實體介面設定單個冗餘連接埠，以防止在主介面或主交換器出現故障時遺失連接。

  附註：NSA 2600 和 NSA 2600 以上版本的安全設備支援連接埠冗餘。HA 控制介面不支援連結彙總和連接埠冗餘。

主題：

- 第 257 頁「連結彙總」
- 第 258 頁「連結彙總設定」
- 第 259 頁「連接埠冗餘」
- 第 260 頁「連接埠冗餘設定」

連結彙總

連結彙總用於透過將多達四個介面彙總為單個彙總連結（稱為「連結彙總組 (LAG)」），來增加防火牆與交換器之間的可用頻寬。彙總連結中的所有連接埠都必須連接到同一個交換器。安全設備使用輪詢機制演算法對連結彙總組中的介面流量進行負載平衡。連結彙總還提供了冗餘措施，因為如果 LAG 中的一個介面發生故障，其他介面仍舊保持連接。

不同供應商使用不同的術語來指代連結彙總，包括連接埠通道、乙太網路通道、主幹和連接埠集合等。

主題：

- 第 257 頁「連結彙總容錯移轉」
- 第 258 頁「連結彙總限制」

連結彙總容錯移轉

SonicWall 提供了多種方法來防止在發生連結故障時遺失連接，其中包括高可用性 (HA)、負載平衡群組（LB 組），以及現在的連結彙總。如果在安全設備上設定了上述全部三種功能，在發生連結故障時，將遵循以下優先順序。

1. 高可用性
2. 連結彙總
3. 負載平衡群組

高可用性的優先順序高於連結彙總。由於 LAG 中的每個連結都攜帶相同份額的負載，因此活動防火牆上發生連結遺失時將會強制容錯移轉至閒置的防火牆（如果其所有連結都保持連接）。只需在主彙總連接埠上設定實體監控。

將連結彙總與負載平衡群組配合使用時，連結彙總的優先順序較高。負載平衡僅在彙總連結中的所有連接埠都不工作時起作用。

連結彙總限制

- 連結彙總目前僅支援固定定址。固定連接埠頻道，名稱為 PAG （連接埠彙總），是設定乙太網路連接埠頻道的一種方式。不使用合作裝置（交換器或伺服器等）傳送 LACP 或 PAGP 封包來形成 EtherChannel。
- 透過乙太網路連接埠頻道設定的連結彙總群組 (LAG) 必須由 NSA 3600 或更高版本的安全設備進行手動設定/組合。
- 目前不支援動態連結彙總控制通訊協定 (LACP)。動態，即透過通訊協定搭配 IEEE LACP 或 Cisco PAGP 等乙太網路連接埠，是設定乙太網路連接埠頻道的另一種方式。在這種方法中，LACP 或 PAGP 封包在連接埠上發出。

連結彙總設定

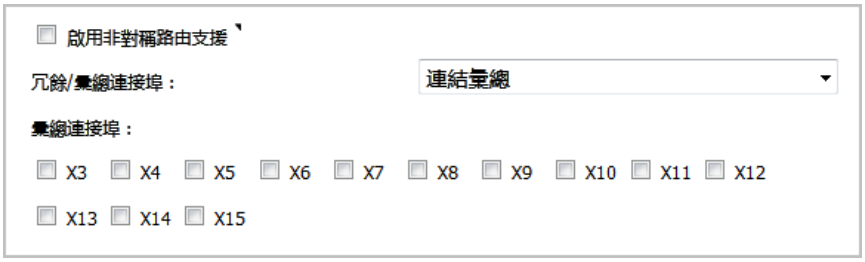
若要設定連結彙總：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 找出要指定為連結彙總群組主介面的介面，然後按一下該介面的**設定**圖示。顯示**編輯介面**對話方塊。

3 按一下**進階**。

4 在**冗餘/彙總連接埠**中，選取**連結彙總**。將顯示更多選項。

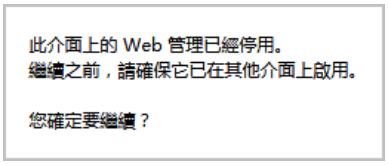


5 **彙總連接埠**選項會顯示安全設備上目前未指派的各個介面。系統不會選取任何連接埠。選擇其他最多三個介面以指派至此 LAG。

附註：在將介面指派至連結彙總組之後，其設定將由連結彙總主介面進行管理，且再也無法獨立進行設定。在**介面設定**表中，此介面的區域顯示為**彙總連接埠**，且移除了**設定**圖示。

6 將介面的**連結速度**設為**自動交涉**。

7 按一下**確定**。如果該介面尚未設定 Web 管理功能，則系統會顯示下列訊息。



a 按一下**確定**。

b 在其他介面上啟用 Web 管理功能。

重要：連結彙總要求在交換器上使用符合的設定。交換器採用的負載平衡方法，會因為供應商而有所不同。如需設定連結彙總的資訊，請參閱交換器文件。請記住，可能將連結彙總稱為「連接埠通道」、「乙太網路通道」、「主幹」或「連接埠分組」。

連接埠冗餘

連接埠冗餘提供了一種簡單的方法來為實體乙太網路連接埠設定冗餘連接埠。它是一種很有價值的功能（在高端部署中尤其如此），可以防止交換器故障成為單一故障點。

主介面啟用時，它將處理進出此介面的所有流量。當主介面發生故障時，次要介面將接管所有傳出和傳入流量。次要介面將獲取主介面的 MAC 位址，並針對容錯移轉事件傳送相應的免費 ARP。當主介面恢復工作時，它將從次要介面重新獲取所有流量處理職責。

在典型的連接埠冗餘設定中，主介面和次要介面分別連接到不同的交換器。這樣可以在主交換器發生故障時提供容錯移轉路徑。兩個交換器必須位於同一個乙太網路網域中。也可以設定連接埠冗餘的兩個介面連接到同一個交換器。

連接埠冗餘容錯移轉

SonicWall 提供了多種方法來防止在發生連結故障時遺失連接，其中包括高可用性 (HA)、負載平衡群組（LB 組），以及現在的連接埠冗餘。如果在安全設備上設定了上述全部三種功能，在發生連結故障時，將遵循以下優先順序。

1 連接埠冗餘

2 HA

3 負載平衡群組

將連接埠冗餘同高可用性配合使用時，連接埠冗餘的優先順序較高。一般來說，介面容錯移轉會引起高可用性容錯移轉，但如果該介面提供了冗餘連接埠，則只會發生介面容錯移轉，而不會發生高可用性容錯移轉。主連接埠和次要冗餘連接埠都故障時，就會發生高可用性容錯移轉 (如果次要安全設備具備使用中的相應連接埠)。

將連接埠冗餘同負載平衡群組配合使用時，連接埠冗餘的優先順序仍舊較高。與高可用性一樣，任何單個連接埠（主連接埠或次要連接埠）故障都將透過連接埠冗餘進行處理。當兩個連接埠都發生故障時，負載平衡將發揮作用，並嘗試查找一個替代介面。

連接埠冗餘設定

若要設定連接埠冗餘：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 找出要指定為連結彙總群組主介面的介面，然後按一下該介面的**設定**圖示。顯示**編輯介面**對話方塊。

3 按一下**進階**。

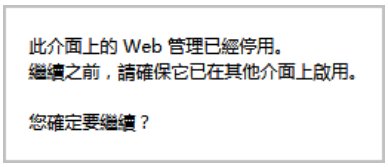
4 將介面的**連結速度**設為**自動交涉**。

5 在**冗餘/彙總連接埠**中，選取**連接埠冗餘**。系統隨即會顯示另一個選項。

6 **冗餘連接埠**選項會顯示目前尚未指派的所有可用介面。選取其中一個介面；預設為**無**。

附註：在將某個介面選為冗餘連接埠後，其設定將由主介面進行管理，並且再也無法獨立進行設定。在**介面設定**表中，此介面的區域顯示為**冗餘連接埠**，且移除了**設定**圖示。

7 按一下**確定**。如果該介面尚未設定 Web 管理功能，則系統會顯示下列訊息。



a 按一下**確定**。

b 在其他介面上啟用 Web 管理功能。

設定虛擬介面 (VLAN 子介面)

在新增 VLAN 子介面時，您需要將其指派給某個區域，為其指派一個 VLAN 標籤，並將其指派給某個實體介面。基於您的區域指派，以設定同一區域的實體介面的相同方法設定 VLAN 子介面。

若要新增虛擬介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 在**介面設定**表格底部的**新增介面**中，選取**虛擬介面**。將顯示**新增介面**對話方塊。

3 選擇一個要指派給此介面的區域。可以選擇 LAN、WAN、DMZ、WLAN 或自訂區域。區域指派無需與父（實體）介面相同。事實上，父介面甚至可以保留**未指派**狀態。

子介面網路設定的設定選項取決於所選的區域。

- **LAN**、**DMZ** 或受信任類型的自訂區域：**固定**或**透明**
- **WLAN** 或自訂無線區域：僅固定 IP（無 IP 指派清單）。

4 在 **VLAN 標籤**欄位中，為子介面指派一個 VLAN 標籤 (ID)。有效的 VLAN ID 範圍為 **0** (預設) 至 4094 (不過有些交換器會保留 VLAN 1 用於指定本機 VLAN，保留 VLAN 0 供 QoS 使用)。您必須使用相應的 VLAN ID，為預計使用防火牆防護的每個 VLAN 建立一個 VLAN 子介面。

5 在**父介面**中，選取這個子介面所屬的父 (實體) 介面。您可以指派的子介面數量沒有每介面限制 - 您可以指派不超過系統限制數量的子介面。

6 基於您所選擇的區域設定子介面網路設定。請參閱介面設定說明:

- 第 235 頁「設定固定介面」
- 第 237 頁「設定固定介面的進階設定」
- 第 243 頁「設定透明 IP 模式下的介面（連接 L3 子網路）」
- 第 246 頁「設定無線介面」
- 第 249 頁「設定 WAN 介面」

7 選擇子介面的管理和使用者登入方法。

8 按一下**確定**。

設定 IPS 偵測器模式

若要針對 IPS 偵測器模式設定安全設備，需要使用相同區域內的兩個介面作為 L2 橋接對。可以使用除 WAN 介面以外的任意介面。在本範例中，我們將使用 X2 和 X3 作為橋接對，並在 LAN 區域內進行設定。WAN 介面 (X1) 由安全設備使用，用途是視需求存取安全設備資料中心。交換器上的鏡像連接埠將連接到橋接對中的介面之一。

主題：

- 第 261 頁「用於 IPS 偵測器模式的設定任務清單」
- 第 262 頁「設定主要橋接介面」
- 第 262 頁「設定次要橋接介面」
- 第 263 頁「啟用和設定 SNMP」
- 第 263 頁「設定 IPS 偵測器模式」

用於 IPS 偵測器模式的設定任務清單

- 設定主要橋接介面
  - 選擇 LAN 作為主要橋接介面的區域
  - 指派一個固定 IP 位址
- 設定次要橋接介面
  - 選擇 LAN 作為次要橋接介面的區域
  - 啟用到主要橋接介面的 L2 橋接
- 啟用 SNMP 並設定可將陷阱傳送到的目的地 SNMP 管理器系統的 IP 位址

- 設定用於 LAN 流量的安全服務
- 將登入警示設定為「警示」或以下級別
- 將交換器上的鏡像連接埠連接到橋接對中的任一介面
- 連接並設定 WAN，以允許存取網際網路上的動態特徵資料

設定主要橋接介面

若要設定主要橋接介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下介面 X2 右邊欄中的**設定**圖示。將顯示**編輯介面**對話方塊。

3 從**區域**下拉功能表中選擇 **LAN**。將顯示更多選項。

附註：您不必設定**進階**或 **VLAN 篩選條件**標籤中的設定。

4 對於**模式/ IP 指派**，請選取**固定 IP 模式**。

5 為介面設定固定 IP 位址（例如 `10.1.2.3`）。您所選擇的 IP 位址不應該與交換器看到的任何網路發生衝突。

附註：主要橋接介面必須擁有固定 IP 指派。

6 設定**子網路遮罩**。

7 輸入描述性註解。

8 選擇介面的**管理**選項: **HTTPS**、**Ping**、**SNMP**、**SSH**。

9 選擇**使用者登入**選項: **HTTP**、**HTTPS**。

10 若要從 HTTP 重新導向到 HTTPS，請勾選**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。

11 按一下**確定**。

設定次要橋接介面

我們的範例將繼續使用 X3 作為次要橋接介面。

若要設定次要橋接介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下介面 X2 右邊欄中的**設定**圖示。將顯示**編輯介面**對話方塊。

3 從**區域**下拉功能表中選擇 **LAN**。將顯示更多選項。

附註：您不必設定「進階」或「VLAN 篩選條件」標籤中的設定。

4 對於 **IP 指派**，請選取**二層橋接模式**。

5 在**橋接目標**中，選取 **X2** 介面。

6 如果想要監控非 IPv4 流量，則不要啟用**封鎖所有非 IPv4 流量**設定。

7 選擇**從不路由流量到該橋接對上**，以確保不會將來自鏡像交換器連接埠的流量發回到網路中。

8 選擇**僅獲取該橋接對上的流量**，以啟用偵測或監控從鏡像交換器連接埠到達 L2 橋接的封包。

9 選擇**停用該橋接對上的狀態偵測**，將這些介面排除在高可用性狀態偵測範圍以外。如果這些介面已啟用深度封包偵測服務，則將繼續套用 DPI 服務。

10 選擇介面的**管理**選項: **HTTPS**、**Ping**、**SNMP**、**SSH**。

11 選擇**使用者登入**選項: **HTTP**、**HTTPS**。

12 若要從 HTTP 重新導向到 HTTPS，請勾選**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。

13 按一下**確定**。

啟用和設定 SNMP

啟用 SNMP 後，將針對 SonicWall 安全服務（例如入侵保護和閘道防毒(GAV)）產生的許多事件自動觸發 SNMP 陷阱。

目前有超過 50 個 IPS 和 GAV 事件可觸發 SNMP 陷阱。《*SonicOS 記錄事件參考指南*》中包含了 SonicOS 所記錄的事件清單，以及適用的 SNMP 陷阱編號。

若要確定在使用已啟用入侵保護的 IPS 偵測器模式時可能觸發的陷阱，請在《*SonicOS 記錄事件參考指南*》「記錄事件訊息索引」區段的表格中搜尋「**入侵**」。此事件的 SNMP 陷阱編號（如果可用）將欄在表格的 **SNMP 陷阱類型**欄中。

若要確定在啟用閘道防毒時可能觸發的陷阱，請在表格中搜尋「**安全服務**」，並在 **SNMP 陷阱類型**欄中檢視 SNMP 陷阱編號。

若要啟用和設定 SNMP：

1 導覽到**管理 | 系統安裝 | 設備 | SNMP**。

2 選擇**啟用 SNMP**。

3 按一下**接受**。**設定**按鈕隨即可供使用，系統也會顯示**檢視**、**使用者/群組**和**存取**區段。

4 按一下**設定**。將顯示 **SNMP 設定**對話方塊。

5 在**系統名稱**欄位，輸入將接收發自安全設備的陷阱的 SNMP 管理器系統的名稱。

6 在**系統聯絡人**欄位輸入 SNMP 聯絡人的姓名或電子郵件地址。

7 在**系統位置**欄位中，輸入系統位置的描述，例如 3 樓實驗室。

8 在**資產編號**欄位中輸入系統的資產編號。

9 在**獲取社群名稱**欄位，輸入擁有獲取來自防火牆的 SNMP 資訊的權限的團體名稱，例如公用。

10 在**擷取群體名稱**欄位，輸入將用來從防火牆向 SNMP 管理器傳送 SNMP 陷阱的團體名稱，例如公用。

11 在**主機 1/2/3/4** 欄位中，輸入將會接收陷阱的 SNMP 管理器系統的 IP 位址。

12 按一下**確定**。

設定 IPS 偵測器模式

若要設定 IPS 偵測器模式:

1 導覽到**管理 | 系統安裝。網路 | 介面**

2 按一下 **X2** 介面的**編輯**圖示。將顯示**編輯介面**對話方塊。

3 將**模式/ IP 指派**設定為**二層橋接模式**。這些選項將發生變更。

4 將**橋接到：**介面設定為 **X0**。

5 選取**僅探查這個橋接配對的流量**。

6 按一下**確定**以儲存和啟用此變更。對話方塊隨即關閉，**網路 | 介面**頁面重新顯示。

7 按一下 **X1 WAN** 介面的**編輯**圖示。將顯示**編輯介面**對話方塊。

8 為 X1 WAN 介面指派用於網路*內部* LAN 區段的唯一 IP 位址 - 這聽起來可能不對，但它實際上將成為您用來管理裝置的介面，也是安全設備用來傳送其 SNMP 陷阱以及獲取安全服務特徵更新的連接埠。

9 按一下**確定**。

10 您還必須修改防火牆規則，以允許從

- LAN 到 WAN 以及
- 從 WAN 到 LAN 的流量

11 將

- SPAN/鏡像交換器連接埠連接到安全設備上的 X0，而不是 X2（事實上 X2 中不會插入任何連接），
- 並將 X1 連接到內部網路

重要：小心地設定 SPAN/鏡像至 X0 的連接埠。

視訊： 可以線上存取包含介面設定範例的參考視訊。例如，可參見如何使用 PPPoE 連線設定 SonicWall WAN / X1 介面。可以透過以下網址獲取其他視訊：https://support.sonicwall.com/videos-product-select。

設定安全服務（統一威脅管理）

在此區段啟用的設定將用於控制在 IPS 偵測器模式下偵測的惡意流量類型。通常需要啟用入侵保護，但也可能需要啟用其他安全服務，例如閘道防毒或防間諜軟體。

若要啟用安全服務，您的 SonicWall 安全設備必須已獲得這些服務的授權，並且必須從 SonicWall 資料中心下載特徵碼。如需啟用及設定 IPS、GAV 和防間諜軟體的完整說明，請參閱 *SonicOS 安全性設定*。

主題：

設定記錄

您可以在**記錄 > 設定**頁面設定記錄來記錄防火牆所偵測到的攻擊項目。如需瞭解啟用登入功能的方法，請參閱 *SonicOS 記錄和報告*。

將鏡像交換器連接埠連接到 IPS 偵測器模式介面

使用標準 Cat-5 乙太網路纜線，將鏡像交換器連接埠連接到橋接對的任一介面。網路流量將自動從交換器傳送到安全設備並進行偵測。

如需設定鏡像連接埠的說明，請參閱交換器文件。

連接和設定連接資料中心的 WAN 介面

將安全設備上的 WAN 連接埠（通常為連接埠 X1）連接到您的閘道或擁有閘道存取權的裝置。安全設備會自動與 SonicWall 資料中心進行通訊。如需設定 WAN 介面的詳細說明，請參見第 249 頁「設定 WAN 介面」。

設定有線和分接模式

SonicOS 支援有線模式和分接模式，這兩種模式提供了不受干擾的網路增量插入方法。有線和分接模式設定表格說明有線和分接模式。

附註：NSA 2600 及更新裝置支援有線模式。

有線和分接模式設定

有線模式設定	說明
繞過模式	繞過模式用於快速和相對無干擾地將安全設備硬體引入網路中。在選擇網路插入點（例如核心交換器與外圍安全設備之間、虛擬機伺服器場前面、資料分類網域之間的轉換點）後，將把安全設備插入實體資料路徑，且只需極短的維護時間窗。安全設備上的一對或多對交換器連接埠將用於以全線速轉送跨分段的所有封包，且所有封包都保留在安全設備的 240Gbps 交換器結構上，而不是向上載遞至多核心偵測和加強路徑。儘管繞過模式不提供任何偵測或防火牆功能，但此模式用於透過實體方式，以最小的故障時間和風險，在網路中引入安全設備，並透過新插入的網路和安全基礎結構元件獲得一定級別的保障。您隨即可透過簡單的使用者介面驅動的重新設定，從繞過模式瞬間轉換至偵測或安全模式。
偵測模式	偵測模式是對繞過模式的擴充，而且無需對低風險、零延遲的封包路徑做出任何功能性變更。封包繼續透過安全設備的交換器結構，但同時也會鏡像至多核心 RF-DPI 引擎，以用於被動偵測、分類和流量報告。這樣無需實際進行任何中繼處理，就能展現安全設備的應用程式智慧和威脅偵測能力。
安全模式	安全模式是由偵測模式進一步發展而成，能夠將安全設備的多核心處理器主動置入封包處理路徑中。這樣可以充分運用偵測和原則引擎的全套功能，包括應用程式智慧和控制、入侵保護服務、基於閘道和雲端的防毒、防間諜軟體以及內容篩選條件等。安全模式可提供與一般 NAT 或二層橋接模式部署相同級別的可見性和加強，但卻沒有任何 L3/L4 轉換，也無需變更 ARP 或路由行為。因此，安全模式提供了可逐步實現的 NGFW 部署，而且對現有網路設計無需任何邏輯變更，而只需極少的實體變更。 在為 VLAN 轉譯建立有線模式對時應使用安全模式。

有線和分接模式設定

有線模式設定	說明
分接模式	分接模式提供了與偵測模式相同的可見性，但與後者不同的是，它透過安全設備上的單個交換器連接埠接收鏡像封包流，因此無需實體形式的中間插入。分接模式設計用於採用網路分流器、智慧分流器、連接埠鏡像或 SPAN 連接埠的環境，以便將封包傳送至外部裝置進行偵測或收集。與其他所有形式的有線模式類似，分接模式可在多個併發的連接埠實例上工作，並支援來自多個分流器的不連續流。

有線模式：功能區別表格摘要了幾種介面設定模式之間的主要功能差異：

有線模式：功能區別

介面設定	繞過模式	偵測模式	安全模式	分接模式	L2 橋接、透明、NAT、路由模式
主動/主動叢集 [a]	否	否	否	否	是
應用程式控制	否	否	是	否	是
應用程式可見性	否	是	是	是	是
ARP/路由/NAT[a]	否	否	否	否	是
綜合反垃圾郵件服務 [a]	否	否	否	否	是
內容篩選	否	否	是	否	是
DHCP 伺服器 [a]	否	否	否	否	是 [b]
DPI 偵測	否	是	是	是	是
DPI 預防	否	否	是	否	是
DPI-SSL[a]	否	否	是	否	是
高可用性	是	是	是	是	是
連結狀態傳播 [c]	是	是	是	否	否
狀態包偵測	否	是	是	是	是
TCP 交握強制 [d]	否	否	否	否	是
虛擬群組 [a]	否	否	否	否	是
VLAN 轉譯 [e]	否	否	是	否	否

a. 這些功能或服務對於在有線模式下設定的連接埠無法使用，但對於在其他相容工作模式下設定的所有介面，仍可在系統範圍內使用。

b. 在二層橋接模式下無法使用。

c. 借助**連結狀態傳播**功能，有線模式對中的介面會對轉換其合作夥伴所觸發的連結狀態進行鏡像。為了在備援路徑網路中正常操作，此為必要的功能。經由 VLAN 介面的有線模式，不支援連結狀態傳播功能。

d. 根據設計，已在有線模式下停用，以便在沿冗餘或非對稱路徑使用多個有線模式路徑或多個安全設備單位的情況下支援在網路中的其他位置發生容錯移轉事件。

e. 經由 VLAN 介面的有線模式，不支援 VLAN 轉譯功能。

附註：在有線模式下運作時，防火牆的專用「管理」介面將用於本機管理。若要啟用遠端管理和動態安全服務以及應用程式智慧更新，必須設定 WAN 介面（與有線模式介面分離）以供網際網路連線之用。由於 SonicOS 支援幾乎包含任何組合的混合模式介面，因此可以輕鬆實現這一點。

設定有線模式的介面

可以在除無線區域以外的 WAN、LAN、DMZ 和自訂區域設定有線模式。有線模式是二層橋接模式的簡化形式，且設定為一對介面。在有線模式下，目的地區域為**成對介面區域**。有線模式對將基於來源**區域**及其**成對介面區域**之間的流量方向套用存取規則。例如，如果來源**區域**為 **WAN**，**成對介面區域**為 **LAN**，則根據流量方向套用 WAN 到 LAN 和 LAN 到 WAN 規則。

在有線模式下，您可以啟用**連結狀態傳播**，將某個介面的連結狀態傳播到其配對的介面。如果某個介面發生故障，強制停用其成對介面，以鏡像第一個介面的連結狀態。有線模式對中的兩個介面始終具有相同的連結狀態。

在有線模式下，您可以**停用狀態偵測**。選擇**停用狀態偵測**時，將關閉狀態封包偵測。*未*選擇**停用狀態偵測**時，無需強制 3 路 TCP 握手即可建立新連接。**如果部署了非對稱路由，則必須選擇停用狀態偵測**。

若要設定有線模式的介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 找出您想要為有線模式設定的介面，然後按一下該介面的**設定**圖示。將顯示**編輯介面**對話方塊。

3 在**區域**中，選取 WLAN 以外的任何區域類型。

4 在**模式/ IP 指派**中，為介面進行下列設定:

- 如需設定為分接模式，請選取**分接模式 (1 連接埠分接)**
- 如需設定為有線模式，請選取**有線模式 (2 連接埠有線)**

5 在**有線模式類型**中，選擇適用的模式:

- **繞過（透過內部交換器/轉接）**
- **偵測（鏡像流量的被動 DPI）**
- **安全（內聯流量的使用中 DPI）**

6 在**成對介面**中選取要連線至上游安全設備的介面。成對介面必須是相同類型的介面（兩個 1 GB 介面或兩個 10 GB 介面）。

> **附註：成對介面**中只會提供尚未指派的介面。如需將介面設為未指定，請按一下該介面的**設定**，然後在**區域**中選取**未指定**。

7 按一下**確定**。

設定有線模式用於 WAN/LAN 區域對

以下設定是關於如何設定有線模式的範例。此範例用於與 LAN 區域配對的 WAN 區域。有線模式也可以設定用於 DMZ 和自訂區域。

設定有線模式用於 WAN/LAN 區域對：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下以下按鈕之一：

- **新增介面**按鈕。
- 按一下想要設定的介面的**設定**圖示。

將顯示**新增/編輯介面**對話方塊。

3 在 **IP 指定**中選取**有線模式 (2 連接埠有線)**。

4 在**區域**中選取 **WAN**。

5 在**配對的介面區域**中選取 **LAN**。

6 選擇**停用狀態偵測**選項。

7 選擇**啟用連結狀態傳播**選項。

8 按一下**確定**按鈕。**介面設定**表更新：

帶有連結彙總的有線模式

附註：經由 VLAN 介面的有線模式不支援連結彙總。

連結彙總 (LAG) 用於將多個連結組合為單個介面以增加頻寬。若要偵測 LAG 介面上的流量，可以內聯方式連接 SonicWall 安全設備，以便將一個連結上傳送的封包透明地橋接至目的地。此外也支援現有的有線模式功能 (例如連結狀態傳播)。每個 LAG 支援多達 8 個成員。

您可透過**網路 | 介面**設定有線模式和連結彙總功能。您在**編輯介面 > 進階**對話方塊中選取**連結彙總**時，系統也會一併列出未指派的介面。您可以為有線模式連線的每一邊選取成員介面。每一邊的成員數量要相等。建議成員介面的類型和頻寬大小也要相符。

若要設定 LAG 有線模式：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下想要設定的介面的**設定**圖示。

3 在**區域**中，選擇所需的區域。

4 在**模式/IP 指定**中，選取**有線模式 (2 連接埠有線)**。

5 在**有線模式類型**中選取**安全 (內聯流量的主動 DPI)**。

6 在**成對介面**中，選擇所需的介面。

7 在**成對介面區域**中，選擇所需的介面。

8 選擇**停用狀態偵測**選項。預設情況下已核取此選項。

9 (選用) 視需求選取**啟用連結狀態傳播**選項。預設情況下未勾選此選項。

10 按一下**進階**。

若要繼續進行進階設定:

1 在**冗餘/彙總連接埠**中，選取**連結彙總**。這些選項將發生變更。

2 在**彙總連接埠**中選取所需的連接埠。

3 在**成對介面彙總連接埠**中，選取所需的連接埠。

4 按一下**確定**。這項設定會顯示在**網路 | 介面**的**介面設定**表格中。

二層橋接模式

SonicOS 包括 **L2（二層）橋接模式**，以不顯眼的方式將安全設備整合到任何乙太網路網路。二層橋接模式表面上與 SonicOS 的透明模式相似，因為它使得安全設備能夠在兩個介面之間共用公用子網路，以及對所有流經的 IP 流量執行狀態偵測和深度封包偵測，但二層橋接模式的功能更加全面。

特別是，二層橋接模式採用了安全學習橋接結構，使其能夠傳遞和偵測其他許多透明安全設備整合方法所無法處理的流量類型。利用二層橋接模式，可以無干擾地將 SonicWall 安全設備新增到任何乙太網路網路，從而為所有流經的 IPv4 TCP 和 UDP 流量提供內聯式深度包偵測。在此應用情節中，安全設備沒有用於加強安全性，而是用於雙向掃描、封鎖病毒和間諜軟體以及入侵企圖。

與其他透明解決方案不同，二層橋接模式可傳遞所有流量類型，包括 IEEE 802.1Q VLAN、產生樹狀目錄通訊協定、多點傳送、廣播和 IPv6，從而確保無中斷地繼續所有網路通訊。

二層橋接模式的全面性還呈現在可以使用它來設定 IPS 偵測器模式。SonicWall 安全設備支援 IPS 偵測器模式，這個模式會使用橋接配對的單一介面，監控來自交換器上的鏡像連接埠的網路流量。IPS 偵測器模式提供入侵偵測，但無法封鎖惡意流量，因為安全設備未以內聯方式接入流量流動。如需 IPS 偵測器模式的更多資訊，請參見第 228 頁「IPS 偵測器模式」。

二層橋接模式為具備以下特徵的網路提供了理想的解決方案：已具備現有安全設備，但不計劃立即更換其現有安全設備，而是希望增加 SonicWall 深度封包偵測的安全性（例如入侵保護服務、閘道防毒和閘道防間諜軟體等安全服務）。如果您沒有訂閱 SonicWall 安全服務，可以透過 MySonicWall 申請免費試用。

也可以在高可用性部署中使用二層橋接模式。此應用情節將在第 281 頁「具有高可用性的二層橋接模式」中說明。

附註：二層橋接模式不支援連結彙總。

主題：

SonicOS 二層橋接模式的主要功能

SonicOS 二層橋接模式金鑰功能和優點表格簡要說明了二層橋接模式各項主要功能的優點。

SonicOS 二層橋接模式金鑰功能和優點

功能	優點
帶有深度封包偵測的二層橋接	這種透明操作方法意味著，無需重新編址或重新設定即可將 SonicWall 安全設備新增到任何網路中，從而實現在不破壞現有網路設計的情況下增加深度封包偵測安全服務。二層橋接模式的開發兼顧連接性和安全性，可傳遞所有乙太網路框架類型，從而確保無縫的整合。
安全學習橋接結構	真正的二層行為意味著，所有允許的流量都以原生方式流經二層橋接。其他透明操作方法都有賴於 ARP 和路由操控來實現透明度，事實證明這種做法常常出現問題；而二層橋接模式則動態地學習網路拓撲，從而確定最佳流量路徑。
通用乙太網路框架類型支援	所有乙太網路流量都可以透過二層橋接，這意味著可以無中斷地繼續所有網路通訊。其他許多透明操作方法僅支援 IPv4 流量，而二層橋接模式會偵測所有 IPv4 流量，並傳遞 (或在需要時封鎖) 其他所有類型的流量，包括 LLC、所有乙太網路類型，甚至包括專有的框架格式。

SonicOS 二層橋接模式金鑰功能和優點

功能	優點
混合模式操作	二層橋接模式可併發提供二層橋接和一般安全裝置服務，例如路由、NAT、VPN 和無線操作。這意味著，它可以在網路的一個區段中用作二層橋接，同時為網路的其餘部分提供全套安全服務。它還允許引入 SonicWall 安全設備作為單純的二層橋接，並提供平滑的遷移路徑遷移至完整的安全服務操作。
無線二層橋接 **附註：**不適用於 SuperMassive 9800。	對多個區域類型（包括 LAN、WLAN、DMZ 或自訂區域）使用單個 IP 子網路。這個功能可讓無線和有線用戶端順利共用相同的網路資訊，包括 DHCP 位址在內。二層通訊協定可在配對的介面之間執行，進而允許多種流量類型流經橋接 (包括括廣播和非 IP 封包)。

設定二層橋接模式和透明模式的重要概念

在提到二層橋接模式的操作和設定時，將會用到以下術語：

- **二層橋接模式** - 一種設定 SonicWall 安全設備的方法，能夠讓安全裝置能夠以內聯方式插入現有網路，並具有絕對的透明度，甚至優於透明模式。二層橋接模式還指為置入*橋接對*的*次要橋接介面*所選擇的 *IP 指派*設定。
- **透明模式** - 一種設定 SonicWall 安全設備的方法，可使用自動套用的 ARP 和路由邏輯，藉此在兩個或更多個介面之間產生單個 IP 子網路，如此一來，無需重新設定 IP 即可在現有網路中插入安全裝置。
- **IP 指派** - 在設定受信任的介面 (LAN) 或公用 (DMZ) 介面時，介面的 IP 指派可能是：
  - **固定** - 手動輸入介面的 IP 位址。
  - **透明模式** - 使用落入 WAN 主 IP 子網路範圍內的位址物件（主機、範圍或組）來指派介面的 IP 位址，從而有效地產生從 WAN 介面到所指派的介面的子網路。
  - **二層橋接模式** - 置於此種模式的介面將成為將之配對到的*主要橋接介面*的*次要橋接介面*。產生的橋接配對，行為將與擁有完全二層透明度的兩連接埠學習橋接相似，且會對所有流經橋接配對的 IP 流量進行全面的狀態容錯移轉和深度封包偵測。
- **橋接對** - 構成*主要橋接介面*和*次要橋接介面*的邏輯介面組。術語主要和次要並不暗示任何固有的操作主導或從屬級別；兩個介面將繼續根據其區域類型進行處理，並根據所設定的存取規則傳遞 IP 流量。經過橋接對的非 IPv4 流量由*次要橋接介面*上的*封鎖所有非 IPv4 流量*設定進行控制。系統可以支援的橋接對數量與它能提供的介面對數量相同。或者說，最大橋接對數量等於平台上的實體介面數量的一半。擁有橋接對成員資格不妨礙介面的一般行為；例如，如果將 X1 設定為與*次要橋接介面* X3 配對的*主要橋接介面*，則 X1 可以在作為主 WAN（傳統角色）工作的同時，透過*自動新增的 X1 預設 NAT 原則*執行用於網際網路繫結流量的 NAT。
- **主要橋接介面** - 在為其配對*次要橋接介面*後指派給介面的名稱。主要橋接介面可能屬於不信任的 (WAN)、受信任的 (LAN) 或公用 (DMZ) 區域。
- **次要橋接介面** - 指派給已針對*二層橋接模式*設定其 *IP 指派*的介面的名稱。次要橋接介面可能屬於受信任的 (LAN) 或公用 (DMZ) 區域。
- **橋接管理位址** - 主要橋接介面的位址由*橋接對*的兩個介面共用。如果主要橋接介面湊巧是主 WAN 介面，則這個位址將用於安全設備的傳出通訊，例如 NTP 和授權管理員更新。連接到橋接對的任一區段的主機還可以使用橋接管理位址作為其閘道，這在*混合模式*部署中很常見。
- **橋接合作夥伴** - 此術語用於指代*橋接對*的「另一個」成員。

- **非 IPv4 流量** - SonicOS 支援以下 IP 通訊協定類型：ICMP (1)、IGMP (2)、TCP (6)、UDP (17)、GRE (47)、ESP (50)、AH (51)、EIGRP (88)、OSPF (89)、PIM-SM (103)、L2TP (115)。對於更多機密型 IP 類型（例如戰鬥無線電傳送通訊協定 (126)）以及非 IPv4 流量類型（例如 IPX 或目前使用的 IPv6 流量），安全設備均不在本機進行處理。二層橋接模式可設定為傳遞或丟棄非 IPv4 流量。
- **擷取橋接模式** - 這種可選的二層橋接工作模式可防止將已進入二層橋接的流量轉送至非橋接對介面。預設情況下，二層橋接邏輯會將已進入二層橋接的流量沿 ARP 和路由表所確定的最佳路徑轉送至其目的地。在某些情況下，最佳路徑可能涉及到路由至或 NAT 至非橋接對介面。啟用擷取橋接模式可確保進入二層橋接的這類流量結束二層橋接，而不是採用在邏輯上最佳的路徑。一般而言，僅在具有冗餘路徑並且嚴格要求遵循路徑的複雜網路才需要使用這種工作模式。
- **單純的二層橋接拓撲** - 指的是將安全設備嚴格用於*二層橋接模式*，以便為網路提供內聯式安全性的部署方式。也就是說，將進入*橋接配對*一端的所有流量繫結到另一端，而不透過其他介面進行路由/NAT。這在以下情況下很常見: 已有現有的外圍安全設備；或者現有網路的部分路徑 (例如部門之間的路徑或兩部交換器之間的主幹連結上的路徑) 需要內聯式安全性。單純的二層橋接拓撲不是一種功能限制，而是對異構環境中的常見部署的一種拓撲描述。
- **混合模式拓撲** - 指的是*橋接配對*不是經由安全設備防火牆的唯一輸入/輸出點的部署情況。這意味著，進入*橋接對*一端的流量可能會透過其他介面進行路由/NAT。這種情況常見於使用安全設備為一個或多個橋接配對提供安全性，同時一併提供下列服務時:
  - 為橋接對或其他介面上的主機提供外圍安全性，例如 WAN 連接性。
  - 為更多區段（例如受信任的 (LAN) 或公用 (DMZ) 介面，這時的通訊將在這些區段上的主機與橋接對上的主機之間發生）提供防火牆和安全服務。
  - 使用 SonicPoint 提供無線服務（這時的通訊將在無線用戶端與橋接對上的主機之間發生）。

二層橋接模式與透明模式的比較

儘管透明模式無需重新編址即可將執行 SonicOS 的安全裝置引入到現有的網路中，但它擁有一定程度的干擾性，尤其對於 ARP、VLAN 支援、多個子網路和非 IPv4 流量類型。考慮在此應用情節中，透明模式的 SonicWall 安全設備剛剛新增到網路中，目的是實現最小干擾度的整合，尤其是：

- 極少或沒有任何計劃外故障時間
- 無需對網路的任何部分重新編址
- 無需重新設定或修改閘道路由器（在由 ISP 控制路由器的情況下很常見）

主題：

透明模式中的 ARP

ARP（在透明模式下，位址解析通訊協定網路介面卡上的唯一硬體位址透過此機制與 IP 位址進行關聯）使用的是*代理方式*。如果左側伺服器上的工作站之前已將路由器 (192.168.0.1) 解析為其 MAC 位址 00:99:10:10:10:10，要使這些主機能夠透過安全設備進行通訊，必須先清除這條快取的 ARP 項目。這是因為，安全設備為連接到以透明模式工作的介面的主機代理（或者說代其回應）了閘道 IP (192.168.0.1)。因此，當左側的工作站嘗試解析 192.168.0.1 時，它所傳送的 ARP 請求將由安全設備使用自己的 X0 MAC 位址 (00:06:B1:10:10:10) 進行回應。

此外，對於在 X1（主 WAN）介面收到的 ARP 請求，安全設備還代理了在透明範圍（192.168.0.100 至 192.168.0.250）內指定並指派給以透明模式工作的介面的 IP 位址 ARP。如果路由器之前已將伺服器 (192.168.0.100) 解析為其 MAC 位址 00:AA:BB:CC:DD:EE，要使路由器能夠透過安全設備與此主機進行通訊，必須先清除這條快取的 ARP 項目。這通常需要透過路由器的管理介面或透過重新啟動路由器來排清路由器的 ARP 快取。在清除路由器的 ARP 快取後，路由器會為 192.168.0.100 傳送新的 ARP 請求，而安全設備將使用其 X1 MAC 00:06:B1:10:10:11 來回應。

透明模式中的 VLAN 支援

儘管上述關係圖中描述的網路比較簡單，但即使對於使用 VLAN 進行流量分段的更大型網路而言也很常見。只要此網路符合下列條件：交換器與路由器之間的連結為 VLAN 轉接；透明模式的 SonicWall 安全設備能夠將 VLAN 終止為連結任一端的子介面，但它要求唯一編址；或者說，非透明模式工作要求至少在一端進行重新編址。這是因為，只有主 WAN 介面可以用作透明模式位址空間的*來源*。

透明模式中的多個子網路

對於大型網路而言，採用多個子網路（這些子網路可能在單個線路上、單獨的 VLAN 中、多個線路上或採用某種組合）的情況很常見。透明模式能夠透過使用固定 ARP 和路由項目來支援多個子網路。

透明模式中的非 IPv4 流量

透明模式會捨棄 (且通常會記錄) 所有非 IPv4 流量，禁止這類流量傳遞其他流量類型，例如 IPX 或未處理的 IP 類型。

二層橋接模式解決了這些常見的透明模式部署問題，後面的章節將對此加以說明。

- 第 272 頁「二層橋接模式中的 ARP」
- 第 273 頁「二層橋接模式中的 VLAN 支援」
- 第 273 頁「二層橋接 IP 封包路徑」
- 第 274 頁「二層橋接模式中的多個子網路」
- 第 275 頁「二層橋接模式中的非 IPv4 流量」
- 第 275 頁「二層橋接模式與透明模式的比較」
- 第 276 頁「透明模式相對二層橋接模式有的優點」

二層橋接模式中的 ARP

二層橋接模式採用的是學習橋接設計，依據此設計，它將動態確定哪些主機位於二層橋接（也稱為「橋接對」）的哪些介面上。ARP 將在本機上透過，這意味著透過二層橋接通訊的主機將會看到其對等方的實際主機 MAC 位址。例如，與路由器通訊 (192.168.0.1) 通訊的工作站將會視路由器為 00:99:10:10:10:10，而路由器將會視工作站 (192.168.0.100) 為 00:AA:BB:CC:DD:EE。

這種行為允許將以二層橋接模式工作的 SonicWall 安全設備引入現有網路中，而不會對大多數網路通訊造成除實體插入引起的瞬時中斷以外的其他干擾。

附註：在插入二層橋接模式的安全設備時，需要重新建立基於流的 TCP 通訊協定通訊（例如用戶端與伺服器之間的 FTP 工作階段）。這是特別設計的，目的是維護狀態封包偵測所提供的安全性。由於狀態封包檢查引擎無法獲知先前已存在的 TCP 連線，因此會捨棄這些*既有*的封包，並記錄事件「*在不存在/已關閉的連線上收到 TCP 封包；TCP 封包已捨棄*」。

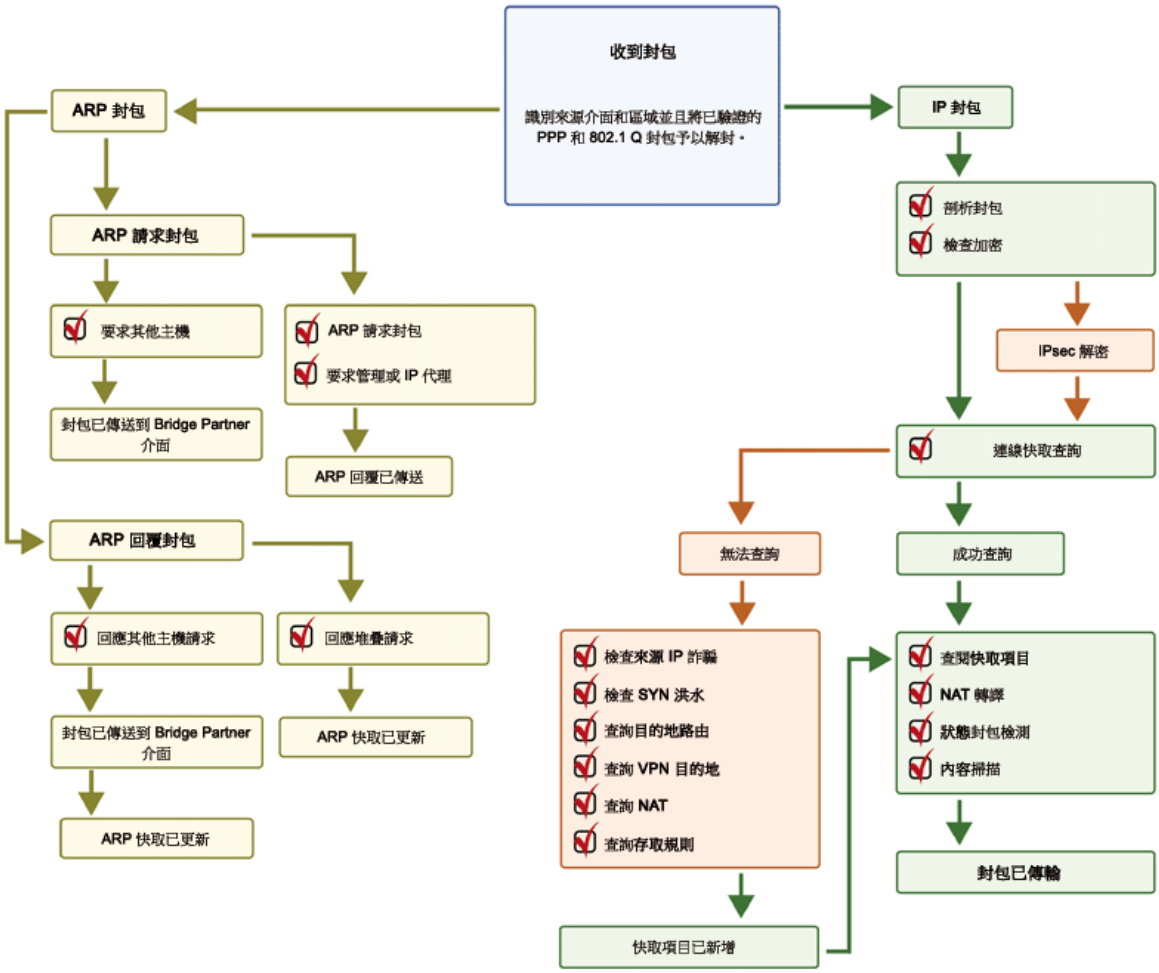
二層橋接模式中的 VLAN 支援

在 SonicWall 安全設備上，二層橋接模式可精確控管流經二層橋接的 802.1Q VLAN 流量。VLAN 的預設處理方式是在流量透過二層橋接時，允許和保留所有 802.1Q VLAN 標籤，同時仍舊對封裝的流量應用所有防火牆規則以及狀態偵測和深度封包偵測。還可以進一步指定允許/禁止透過二層橋接的 VLAN ID 白/黑名單。

這樣方便將以二層橋接模式工作的安全設備插入（例如以內聯方式）到攜帶任何數量的 VLAN 的 VLAN 轉接中，並為流經 VLAN 的所有 IPv4 流量提供完整的安全服務，而無需顯見設定任何 VLAN ID 或子網路。鑒於 VLAN 流量的處理方式，也可以選擇對流經二層橋接模式的所有 VLAN 流量套用存取規則。

二層橋接 IP 封包路徑

二層橋接 IP 封包流



以下一連串的事件描述了二層橋接 IP 封包流中的流程:

1 採用 802.1Q 封裝的框架進入二層橋接介面 (第一步、步驟 2 和步驟 12 僅適用於 802.1Q VLAN 流量)。

2 根據 VLAN ID 白/黑名單檢查 802.1Q VLAN ID。如果 VLAN ID 的狀態為:

- 不允許的 VLAN ID，則系統會捨棄封包並加以記錄。
- 允許的 VLAN ID，則系統會解除封包封裝、儲存 VLAN ID，而且讓內層封包 (包括 IP 標頭) 通過完整的封包處理程式。

3 由於二層橋接支援任意數量的子網路，因此不對封包的來源 IP 執行來源 IP 欺騙檢查。可以使用存取規則來設定二層橋接僅支援指定的子網路。

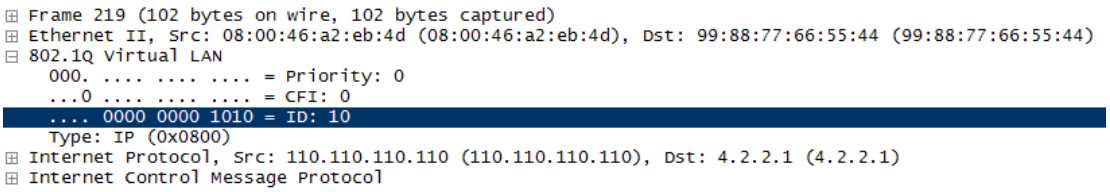
4 執行攻擊檢查。

5 對目的地區域執行目的地路由查詢，以便套用適當的存取規則。任何區域都是有效的目的地，包括與來源區域相同的區域（例如 LAN 對 LAN）、不受信的區域 (WAN)、加密區域 (VPN)、無線區域 (WLAN)、多點傳送區域或任何類型的自訂區域。

6 根據需要，執行和套用 NAT 查詢。

- 一般而言，進入二層橋接的封包會以*橋接合作夥伴*介面 (即橋接的另一端) 為目的地。這種情況下，無需執行轉譯。
- 在二層橋接管理位址為閘道的情況下（*混合模式拓撲*中有時會出現這種情況），將根據需要套用 NAT（詳細，請參閱第 276 頁「二層橋接路徑確定」）。

7 為封包套用存取規則。例如，在 SonicWall 安全設備上，以下封包解碼顯示：ICMP 封包攜帶 VLAN ID 10，來源 IP 位址 `110.110.110.110`，目的地 IP 位址 `4.2.2.1`。



可以設定一條存取規則，獨立於封包的 VLAN 成員資格，根據其任意 IP 元素（例如來源 IP、目的地 IP 或服務類型）來控制任何 IP 封包。系統會捨棄禁止的封包並加以記錄。允許的封包可繼續通過。

8 為此封包建立一條連接快取項目，並執行必要的 NAT 轉換（如果有）。

9 對 TCP、VoIP、FTP、MSN、Oracle、RTSP 和其他媒體流、PPTP 和 L2TP 執行狀態封包偵測和轉換。系統會捨棄禁止的封包並加以記錄。允許的封包可繼續通過。

10 執行深度封包偵測，包括 GAV、IPS、防間諜軟體、CFS 和電子郵件篩選。系統會捨棄禁止的封包並加以記錄。允許的封包可繼續通過。根據設定通知用戶端。

11 如果封包的目的地是加密區域 (VPN)、不受信的區域 (WAN) 或其他某個連接的介面（混合模式拓撲中可能出現後兩種情況），則將透過相應的路徑傳送封包。

12 如果封包的目的地不是 VPN/WAN/連接的介面，則系統會恢復已儲存的 VLAN 標籤，並將封包 (再次攜帶原始的 VLAN 標籤) 傳送到*橋接合作夥伴*介面。

二層橋接模式中的多個子網路

如同第 273 頁「二層橋接 IP 封包路徑」中的說明，二層橋接模式能夠處理通過橋接的子網路，而且數量不限。預設行為是允許所有子網路，但可以根據需要，透過套用存取規則來控制流量。

二層橋接模式中的非 IPv4 流量

預設情況下，不支援的流量會由某個二層橋接介面傳遞至橋接合作夥伴介面。這使得安全設備可以傳遞其他流量類型，包括 LLC 封包（例如產生樹狀目錄）、其他乙太網路類型（例如 MPLS 標籤交換封包 (EtherType 0x8847)、Appletalk (EtherType 0x809b) 和廣受歡迎的虛擬綜合網路服務 (EtherType 0xbad)）。這些非 IPv4 封包只會通過橋接，封包處理程式不會對這類封包進行偵測或控管。如果不需要這些流量類型，可透過在**次要橋接介面**設定對話中啟用**封鎖所有非 IPv4 流量**選項來變更橋接行為。

二層橋接模式與透明模式的比較

二層橋接模式與透明模式的比較

屬性	二層橋接的模式	透明模式
操作層	2 層 (MAC)	3 層 (IP)
ARP 行為	未變更 ARP（位址解析通訊協定）資訊。MAC 位址以本機方式遍歷二層橋接。系統會處理目的地為 SonicWall 安全設備的 MAC 位址的封包並傳遞其他封包，同時學習和快取來源和目的地。	由以透明模式工作的介面代理 ARP。
路徑確定	動態學習橋接對兩端的主機。無需聲明介面相關性。	主 WAN 介面始終是透明模式流量的主要輸入/輸出點，且用於確定子網路空間。以透明方式共用此子網路空間的主機必須透過使用位址物件指派進行顯見聲明。
最大介面數	兩個介面，一個主要橋接介面和一個次要橋接介面。	兩個以上介面。主介面始終是主 WAN。透明從屬介面的數量與可用介面數量相同。
最大配對數	允許的橋接對最大數量僅受可用的實體介面數量限制。它可以描述為「多個一對一配對」。	儘管透明模式允許多個介面同時作為主 WAN 的透明合作夥伴工作，但它僅允許主 WAN 子網路鏡像至其他介面。它可以描述為「單個一對一配對」或「單個一對多配對」。
區域限制	主要橋接介面可能是不受信的、受信任的或公用介面。次要橋接介面可能是受信任的或公用介面。	透明模式配對中的介面必須包括一個不受信的介面（主 WAN，作為配對子網路的主要介面）和一個或多個受信任/公用介面（例如 LAN 或 DMZ）。
支援的子網路	支援任意數量的子網路。可以寫入存取規則以根據需要控制發往/收自任意子網路的流量。	在其預設值下，透明模式僅支援單個子網路（被指派到的、從主 WAN 鏡像的子網路）。可以透過使用 ARP 項目和路由來手動新增更多子網路支援。
非 IPv4 流量	預設情況下，所有非 IPv4 流量都從一個橋接對介面橋接至橋接合作夥伴介面，除非在次要橋接介面設定頁中停用了此選項。它包括 IPv6 流量、STP（產生樹狀目錄通訊協定）和未識別的 IP 類型。	透明模式不處理非 IPv4 流量，而是將其丟棄並記錄。
VLAN 流量	VLAN 流量流經二層橋接並由狀態和深度封包偵測引擎進行完全偵測。	可以建立 VLAN 子介面，並提供透明模式位址物件指派，但安全設備會終止而不是傳遞 VLAN。

二層橋接模式與透明模式的比較

屬性	二層橋接的模式	透明模式
VLAN 子介面	可以在橋接配對介面上設定 VLAN 子介面，但這些介面將透過橋接傳遞至橋接合作夥伴介面，除非 VLAN 框架中的目的地 IP 位址與安全設備上的 VLAN 子介面的 IP 位址相符，在這種情況下將對子介面進行處理 (例如作為管理流量)。	可以將 VLAN 子介面指派給以透明模式運作的實體介面，但其運作模式會與父介面各自獨立。也可以為這些 VLAN 子介面提供透明模式位址物件指派，但無論如何，系統都會終止而不是傳遞 VLAN 子介面。
動態定址	儘管可以將主要橋接介面指派給 WAN 區域，但主要橋接介面僅允許固定定址。	儘管透明模式使用主 WAN 作為主要介面，但透明模式僅允許固定定址。
VPN 支援	設定一個額外的路由後可支援 VPN 操作。詳細資料請參見第 290 頁「VPN 與二層橋接模式的整合」。	無需特殊設定即可支援 VPN 操作。
DHCP 支援	可透過橋接對傳遞 DHCP。	以透明模式工作的介面可提供 DHCP 服務，或者使用 IP 協助程式傳遞 DHCP。
路由和 NAT	可智慧地路由來自/發往其他路徑的流量進/出二層橋接對。預設情況下，系統不會將流量從某個橋接配對介面 NAT 至橋接合作夥伴，但可視需求將流量 NAT 至其他路徑。可根據需要新增自訂路由和 NAT 原則。	可智慧地路由來自/發往其他路徑的流量。預設情況下，系統不會在 WAN 與透明模式介面之間來回 NAT 流量，但可視需求將流量 NAT 至其他路徑。可根據需要新增自訂路由和 NAT 原則。
狀態包偵測	流經所有子網路二層橋接的 IPv4 流量，都會套用完全狀態封包偵測，防火牆的 VLAN 流量也不例外。	來自/發往透明模式位址物件指派所指定的子網路的流量，會套用完全狀態封包偵測。
安全服務	完全支援所有安全服務（GAV、IPS、防間諜軟體、CFS）。（所有一般 IP 流量，以及所有採用 802.1Q 封裝的 VLAN 流量）。	對於來自/發往透明模式位址物件指派所指定的子網路的流量，完全支援所有安全服務（GAV、IPS、防間諜軟體、CFS）。
廣播流量	廣播流量將從橋接對接收介面傳遞至橋接合作夥伴介面。	將丟棄和記錄廣播流量，可能的例外情況是 NetBIOS，IP 協助程式可能會對其進行處理。
多點傳送流量	如果已透過**管理	安全設定	防火牆設定 > 多點傳送**啟用多點傳送，多點傳送流量就會受到偵測並通過二層橋接配對。它不依賴於 IGMP 訊息傳送，也沒必要在單獨的介面上啟用多點傳送支援。	如果已透過**管理	安全設定	防火牆設定 > 多點傳送**啟用多點傳送，並在相關介面上啟用了多點傳送支援，透明模式就會偵測及傳遞具備 IGMP 相依性的多點傳送流量。

透明模式相對二層橋接模式有的優點

二層橋接模式最多允許兩個介面。如果同一子網路中需要工作的介面數量超過兩個，應考慮採用透明模式。

二層橋接路徑確定

安全設備在橋接對介面上收到的封包必須轉送到通往其目的地的適當和最佳路徑，不論此路徑是橋接合作夥伴、其他某個實體介面或子介面，還是 VPN 通道。類似地，從其他（實體、虛擬或 VPN）路徑抵達的繫結至橋接對上的主機的封包必須發往正確的橋接對介面。

以下摘要內容按順序說明了針對下列情形套用於路徑確定的邏輯：

1 如果存在通往目的地的最具體的*非預設*路由，則選擇此路由。它包括下列範例情況：

   a 封包到達 X3（非二層橋接 LAN），目的地為主機 15.1.1.100 子網路，存在一條透過 X0（次要橋接介面，LAN）介面和 192.168.0.254 到達 15.1.1.0/24 子網路的路由。封包將透過 X0 轉送至目的地 MAC 位址 192.168.0.254，以及目的地 IP 位址 15.1.1.100。

   b 封包到達 X4（主要橋接介面，LAN），目的地為主機 10.0.1.100，存在一條透過 X5 (DMZ) 介面和 192.168.10.50 到達 10.0.1.0/24 的路由。封包將透過 X5 轉送至目的地 MAC 位址 192.168.10.50，以及目的地 IP 位址 10.0.1.100。

2 如果不存在通往目的地的具體路由，則將對目的地 IP 位址執行 ARP 快取查詢。符合的項目會指出適當的目的地介面。它包括下列範例情況：

   a 封包到達 X3（非二層橋接 LAN），目的地為主機 192.168.0.100（位在二層主要橋接介面 X2 上）。封包將透過 X2 轉送至已知的目的地 MAC 和 IP 位址 192.168.0.100（來源於 ARP 快取）。

   b 封包到達 X4（主要橋接介面，LAN），目的地為主機 10.0.1.10（位在 X5 - DMZ 上）。封包將透過 X5 轉送至已知的目的地 MAC 和 IP 位址 10.0.1.10（來源於 ARP 快取）。

3 如果沒有找到 ARP 項目：

   a 如果封包到達橋接對介面，將其傳送至橋接合作夥伴介面。

   b 如果封包從其他某條路徑到達，安全設備將會在橋接對的兩個介面分佈傳送一條 ARP 請求，以確定目的地 IP 所在的區段。

   在最後這種情況下，由於在收到 ARP 回應之前目的地未知，因此，目的地區域在此之前也保持未知。這使得安全設備在完成路徑確定之前無法套用相應的存取規則。完成路徑確認後，後續的相關流量就會套用正確的存取規則。

關於到達二層橋接配對介面的流量的位址轉譯 (NAT)，視其目的地會出現下列情況:

1 如果目的地為橋接合作夥伴介面，則不會執行任何 IP 轉譯 (NAT)。

2 如果目的地為其他路徑，則會視路徑套用適當的 NAT 原則:

   a 如果路徑為另一個連接的 (本機) 介面，則可能不需要轉譯。也就是說，由於觸發了*最終*的任意->原始 NAT 原則，因此獲得有效的路由。

   b 如果已確定此路徑將透過 WAN，則將套用預設的 *X1 WAN 自動新增 [介面] 傳出 NAT 原則*，並轉換封包的來源以便傳遞到網際網路。在第 281 頁「內部安全」中所述的混合模式拓撲中，這種情況比較常見。

二層橋接介面區域選擇

應根據網路的流量流動要求進行橋接對介面區域指派。透明模式要求使用主 WAN 作為來源介面，使用受信任的或公用介面作為透明介面，從而實現一個「更可信任的對不可信的」系統；與之不同的是，二層橋接模式允許對操作級別的信任提供更多的控制。具體而言，二層橋接模式允許將*主要橋接介面*和*次要橋接介面*指派給相同或不同的區域（例如 LAN+LAN、LAN+DMZ、WAN+自訂 LAN，等等）。這不僅影響到套用於流量的預設存取規則，還影響到對流經橋接的流量套用深度封包偵測安全服務的方式。選擇和設定要在橋接對中使用的介面時，需要考慮的重要方面包括：安全服務、存取規則和 WAN 連接性：

安全服務方向性

安全服務將是二層橋接模式的主要應用之一，因此瞭解安全服務的應用對於正確選擇橋接對介面區域而言非常重要。安全服務適用性基於以下條件：

1 **服務的方向：**

- GAV 基本上是一種傳入服務，用於偵測傳入 HTTP、FTP、IMAP、SMTP、POP3 和 TCP 流。它還擁有一個用於 SMTP 的附加傳出元素。
- 防間諜軟體基本上是一種輸入服務，用於偵測傳入 HTTP、FTP、IMAP、SMTP、POP3，以交付（即擷取）間諜軟體元件（通常根據其類 ID 進行識別）。它還擁有一個附加的傳出元件，在此元件中，對於由觸發識別這些間諜軟體元件的 IPS 特徵所歸結的方向性（即傳出），將使用傳出方向。由於這些元件通常由用戶端 (例如 LAN 主機) 透過 HTTP 從網際網路上的 Web 伺服器 (WAN 主機) 擷取，因此會使用傳出分類器 (如 IPS：流量方向中所述)。根據 IPS：流量方向，此連結為*傳出*連結，且要求具備傳出方向分類的特徵標記。
- IPS 擁有三種方向：傳入、傳出和雙向。傳入和傳出將於 IPS：流量方向中說明，雙向指的是表格中的所有交叉點。
- 為提高準確性，還考慮了其他元素，例如連接狀態（例如 SYN 或已建立）、相對流量的封包來源（例如發起者或回應者）。

2 **流量方向**。與 IPS 有關的流量方向主要取決於流量流動的來源區域和目的地區域。在安全設備收到封包時，通常立即獲知封包的來源區域，並透過路由（或 VPN）查詢快速確定其目的地區域。

基於來源和目的地，封包的方向性可歸類為*傳入*或*傳出*，（不要與輸入和輸出相混淆）IPS：流量方向表格中所顯示的條件用於做出決定。

IPS：流量方向 [a]

目的地/來源	不受信任	公用	無線	加密	受信任	多點傳送
不受信任	傳入	傳入	傳入	傳入	傳入	傳入
公用	傳出	傳出	傳出	傳入	傳入	傳入
無線	傳出	傳出	信任	信任	信任	傳入
加密	傳出	傳出	信任	信任	信任	傳出
受信任	傳出	傳出	信任	信任	信任	傳出

a. 表格資料可能發生變更。

除了此分類以外，對於傳入/傳出擁有附加信任級別的區域（這些區域內在擁有增強級別的安全性 [LAN|無線|加密<-->LAN|無線|加密]）的封包，還提供了特殊的*信任*分類。有信任分類的流量已套用所有特徵（傳入、傳出和雙向）。

3 **特徵方向**。它主要與 IPS 相關。在 IPS 中，SonicWall 特徵開發團隊向每個特徵都指派了一個方向，目的是提供最佳化手段，最大限度減少誤報。特徵方向包括：

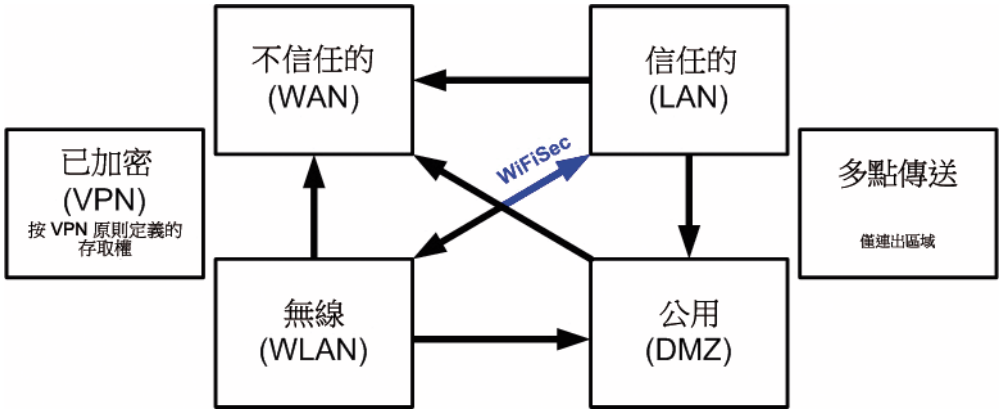
- **傳入** - 套用於*傳入*流量和*信任*流量。大多數特徵為傳入特徵，包括所有形式的應用程式漏洞以及所有枚舉和足跡法嘗試。約 85% 的特徵為傳入特徵。
- **傳出** - 套用於*傳出*流量和*信任*流量。傳出特徵的範例包括 IM 和 P2P 登入嘗試，以及對成功啟動的漏洞的回應（例如攻擊回應）。約 10% 的特徵為傳出特徵。
- **雙向** - 套用於所有流量。雙向特徵的範例包括 IM 檔案傳送、各種 NetBIOS 攻擊（例如震盪波通訊），以及各種 DoS 攻擊（例如目的地為連接埠 0 的 UDP/TCP 流量）。約 5% 的特徵為雙向特徵。

4 **區域應用**。若要觸發某個特徵，*必須在它所流經的至少一個區域中啟用*需要的安全服務。例如，存取 Microsoft 終端伺服器（在 X3 上，次要橋接介面，LAN）的網際網路主機（X1，WAN）將觸發*傳入*特徵「IPS 偵測警示：MISC MS 終端伺服器請求，SID：436，優先順序：低」（如果已在 *WAN*、*LAN* 或同時在兩者之中啟用 IPS）。

存取規則預設值

預設的區域對區域存取規則。應考慮預設存取規則，儘管可根據需要對其進行修改。存取規則預設值中所顯示的預設值：

存取規則預設值



WAN 連接性

網際網路 (WAN) 連接性是*堆疊*通訊所必需的，例如授權、安全服務特徵下載、NTP（時間同步）和 CFS（內容篩選服務）等。目前，僅透過主 WAN 介面進行這些通訊。如果需要這些類型的通訊，主 WAN 應具備連接網際網路的路徑。是否採用主 WAN 作為橋接對的一部分，對於其提供此類堆疊通訊的能力沒有任何影響。

附註：如果網際網路連接無法使用，可以手動執行授權和特徵更新 (http://www.mysonicwall.com/)。

範例拓撲

以下是描述常見部署的範例拓撲：

- **內聯式二層橋接模式**代表加入 SonicWall 安全設備安全裝置，進而在已部署安全設備的網路中提供安全服務。
- **外圍安全**代表在已在靠近網路外圍的位置部署安全設備的現有網路中，以*單純的二層橋接模式*加入 SonicWall 安全設備。
- **內部安全**描述以*混合模式*完全整合 SonicWall 安全設備 ，在此模式中，安全裝置用於同時提供二層橋接、WLAN 服務和經過 NAT 的 WAN 存取。
- **擁有高可用性的二層橋接模式**描述安全設備 HA 對與二層橋接共同提供高可用性的混合模式應用情節。
- **擁有 SSL VPN 的二層橋接模式**描述與二層橋接模式聯合部署 SonicWall SMA SSL VPN 或 SonicWall SSL VPN 系列設備的應用情節。

主題：

- 第 280 頁「無線二層橋接」
- 第 280 頁「內聯式二層橋接模式」
- 第 281 頁「外圍安全」
- 第 281 頁「內部安全」

- 第 281 頁「具有高可用性的二層橋接模式」
- 第 283 頁「擁有 SSL VPN 的二層橋接模式」

無線二層橋接

附註：SuperMassive 9800 不套用無線二層橋接。

在無線模式下，將無線 (WLAN) 介面橋接至 LAN 或 DMZ 區域之後，WLAN 區域將成為次要橋接介面，允許無線用戶端使用與其有線對等方相同的子網路和 DHCP 集區。

設定 WLAN 到 LAN 二層介面橋接：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下想要橋接的無線介面的**設定**圖示。將顯示**編輯介面**對話方塊。

提示：如果您設定了虛擬存取點，則 WLAN 區域中的介面下已有 VLAN 介面（如 X4），且虛擬存取點將設定為使用此 VLAN ID。

3 在**二層橋接模式**中選取**模式/IP 指派**。

附註：儘管會自動建立一條一般規則，以允許 WLAN 區域與您所選定的橋接介面之間的流量，但仍會應用 WLAN 區域類型安全屬性。必須手動新增任何特定規則。

4 在**橋接目標**中選取 WLAN 要橋接的目標介面。在此實例中，將選擇 X0（預設 LAN 區域）。

5 按正常方法設定其餘選項。如需設定 WLAN 介面的更多資訊，請參見第 246 頁「設定無線介面」。

內聯式二層橋接模式

此方法適用於以下網路環境: 目前已有安全設備並打算繼續使用，但您希望在使用安全設備的安全服務時，不對網路造成大幅度的異動。透過將安全設備置於二層橋接模式，X0 和 X1 介面將成為屬於 X1 WAN 介面的相同廣播網域/網路的一部分。

這個範例參照的是安裝在 Hewlett Packard ProCurve 交換環境中的 SonicWall 安全設備。

可以使用 HP 的 ProCurve Manager Plus (PCM+) 和 HP Network Immunity Manager (NIM) 伺服器軟體套件來管理交換器以及 SonicWall 安全設備的一些方面。

若要設定內聯式二層橋接模式:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下 **X0 LAN** 介面的**設定**圖示。

3 在**編輯介面**對話方塊中，為**二層橋接模式 (IP 路由選項)**指派 IP。這些選項將發生變更。

4 將**橋接到：**介面設定為 **X1**。

5 如要封鎖橋接配對的所有非 IP 流量，請選取**封鎖所有非 IP 流量**。 預設情況下未勾選此選項。

6 如需禁止流量被路由到橋接配對，請選取**一律不路由流量到這個橋接配對上**。 預設情況下未勾選此選項。

7 如僅需探查橋接配對的流量，請選取**僅探查這個橋接配對的流量**。 預設情況下未勾選此選項。

8 如需禁止在橋接配對上進行狀態偵測，請選取**停用這個橋接配對的狀態偵測功能**。 預設情況下未勾選此選項。

9 確保介面已設定使用 **HTTPS** 和 **SNMP**，以便透過 **PCM+/NIM** 從 DMZ 管理介面。

10 按正常方法設定其餘選項。

11 按一下**確定**以儲存和啟用此變更。

您還必須確實修改存取規則，允許從 LAN 到 WAN 以及從 WAN 到 LAN 的流量，否則這些流量將無法順利通過。如果將 PCM+/NIM 伺服器置於 DMZ 中，則還必須修改防火牆上的路由資訊。

外圍安全

外圍安全指的是安全設備被新增到外圍來提供安全服務的網路應用情形 (網路中不一定已有部署在安全設備和路由器間的安全設備)。在這種情況下，隸屬於安全設備的所有部分 (*主要橋接介面*部分)，一般會被視為信任級別低於安全設備左側的所有部分 (*次要橋接介面*部分)。因此，最好使用 X1（主 WAN）作為*主要橋接介面*。

允許來自連接到*次要橋接介面* (LAN) 的主機的流量透過防火牆傳出到其閘道（三層交換器上的 VLAN 介面，之後再透過路由器），而來自*主要橋接介面* (WAN) 的流量預設不允許傳入。

如果*次要橋接介面* (LAN) 部分中具備公用伺服器 (例如郵件和 Web 伺服器)，則可以新增允許相應 IP 位址和服務的 WAN->LAN 流量的存取規則，以便允許流向這些伺服器的傳入流量。

內部安全

在這個網路應用情形中，安全設備將作為外圍安全裝置，保護無線平台的安全。與此同時，它還將在網路的工作站和伺服器分段之間提供二層橋接安全，*而無需對任何工作站或伺服器重新編址*。

這種典型的部門間混合模式拓撲部署展示了安全設備如何同時提供橋接和路由/NAT 服務。*主要橋接介面*（伺服器）分段與*次要橋接介面*（工作站）分段之間的流量將透過二層橋接。

由於橋接配對的兩個介面都已指派到信任的 (LAN) 區域，因此將套用以下規則:

- 預設為允許所有流量，但也可視需求設定存取規則。

  從對比的角度出發，考慮如果將 X2（主要橋接介面）指派到公用 (DMZ) 區域，將會發生怎樣的情況：將允許所有工作站存取伺服器，但伺服器無法向工作站發起通訊。儘管這種做法或可支援流量流動要求 (即工作站向伺服器發起工作階段)，但會造成兩種不利影響:

- DHCP 伺服器將位於 DMZ 中。來自工作站的 DHCP 請求將透過二層橋接到達 DHCP 伺服器 (192.168.0.100)，但由於預設的 DMZ->LAN 拒絕存取規則，將丟棄來自伺服器的 DHCP 供應。因此必須新增一條存取規則，或修改預設存取規則，以允許從 DMZ 到 LAN 的這一流量。

- 從工作站到伺服器的流量的安全服務方向性將被分類為*傳出*，因為此流量將有受信任的來源區域和公用目的地區域。這可能不是最佳選擇，因為它所提供的安全性不及*傳入*或（理想選擇）*信任*分類。

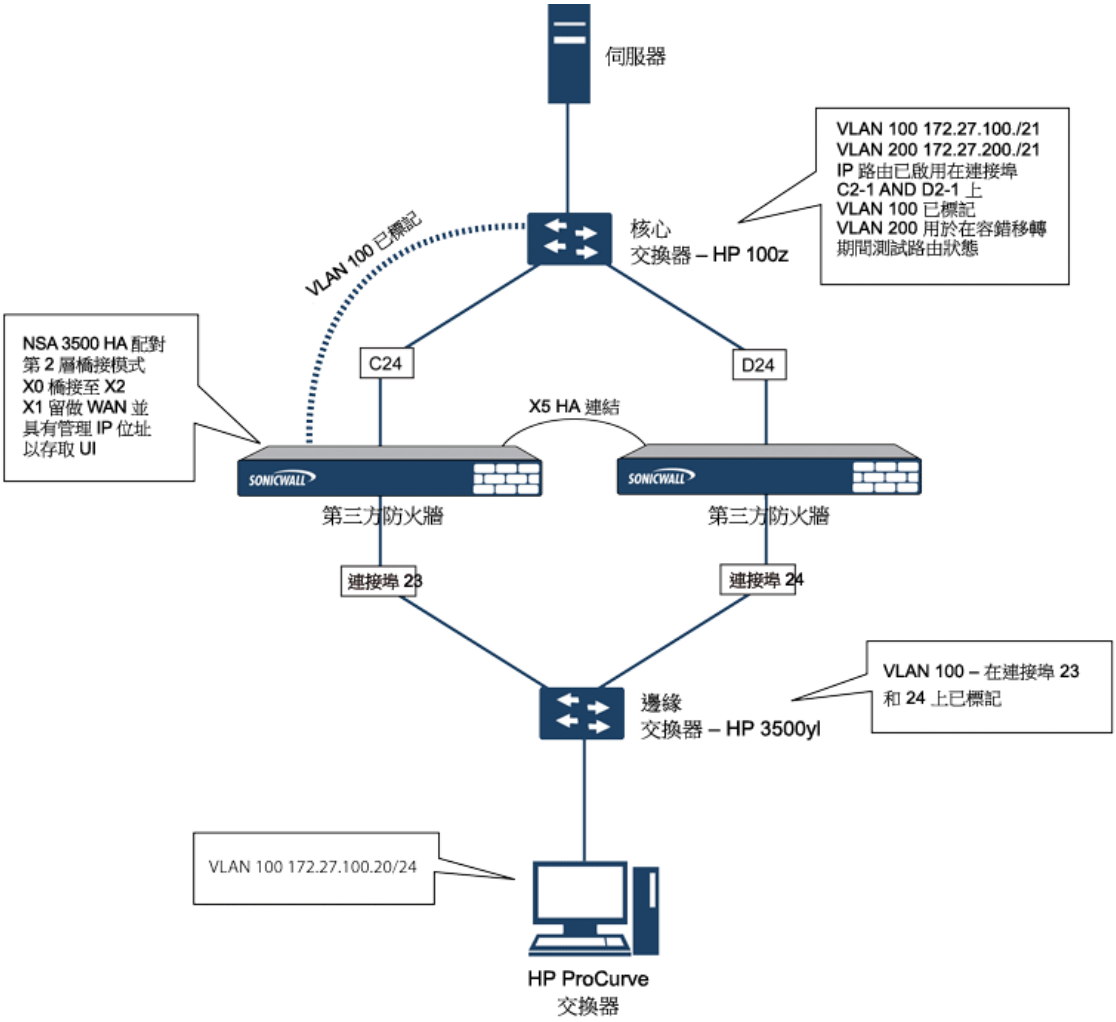
- 安全服務方向性將被分類為*信任*，並將套用所有特徵（*傳入*、*傳出*和*雙向*），從而為兩個分段提供最進階別的安全性。

如需設定二層橋接模式下的介面的詳細說明，請參見第 285 頁「設定二層橋接模式」。

具有高可用性的二層橋接模式

這種方法適用於同時需要高可用性 (HA) 和二層橋接模式的網路環境。這個範例適用於 SonicWall 安全設備，並假設使用已設定了 VLAN 的交換器。請參閱內部安全範例：同時需要高可用性和二層橋接模式。

內部安全範例：同時需要高可用性和二層橋接模式



安全設備 HA 配對包含兩部安全設備，這兩部裝置在指定的 HA 連接埠 X5 上是連接在一起的。每個裝置上的連接埠 X1 已設定用於正常 WAN 連接，且用於存取此裝置的管理介面。二層橋接模式採用的實作將連接埠 X0 橋接至連接埠 X2。

在設定此應用情節時，安全設備和交換器上都需要注意若干事宜：

在安全設備上:

- 在設定高可用性時，不要啟用虛擬 MAC 選項。在二層橋接模式設定中，此功能不起作用。
- 在類似這種內聯環境中，不建議啟用先佔模式。如果需要先佔模式，請遵循交換器文件中提供的建議，因為在這種情形下，觸發時間和容錯移轉時間值具有重大作用。
- 考慮保留一個介面用於管理網路（在此範例中使用 X1）。如果有必要向橋接介面指派 IP 位址用於偵測或其他目的，SonicWall 推薦將指派給交換器的管理 VLAN 網路用於安全和管理用途。

  附註：指派用於高可用性用途的 IP 位址不直接與實際流量流動交互。

在交換器上：

- 使用多個標記連接埠：如內部安全範例：同時需要高可用性和二層橋接模式所示，在邊緣交換器（連接埠 23 和 24）和核心交換器 (C24 - D24) 上分別為 VLAN 100 建立兩個標籤 (802.1q) 連接埠。安全設備會以內聯方式在這兩個交換器之間建立連結。在高效能環境中，通常推薦（使用

OSPF）為此類部署指定連結彙總/連接埠轉接、動態 LACP，甚至完全獨立的連結，而且必須考慮每個交換器的容錯能力。更多資訊，請查閱交換器文件。

- 在 HP ProCurve 交換器上，當兩個連接埠被標籤在相同的 VLAN 中，此連接埠組將自動置為容錯移轉設定。這種情況下，當一個連接埠發生故障時，另一個連接埠將立即啟用。

擁有 SSL VPN 的二層橋接模式

這個拓撲範例說明如何將 SonicWall 安全設備網路安全裝置正確安裝到您現有的 SonicWall EX 系列 SSL VPN 或 SonicWall SSL VPN 網路環境中。將安全設備置為二層橋接模式，並透過內部私人連接連接到 SSL VPN 裝置，可以掃描兩個方向上的病毒、間諜軟體和入侵行為。在此應用情節中，安全設備沒有用於加強安全性，而是用於雙向掃描、封鎖病毒和間諜軟體以及入侵企圖。經過正確設定的安全設備不會中斷網路流量，除非已確定此流量的行為或內容是不需要的。本章節將介紹 SonicWall 安全設備的單連接埠和兩連接埠部署方式。

WAN 到 LAN 存取規則

由於在此部署情節中，安全設備將僅用作防毒、防間諜軟體和入侵保護的實施點，因此必須修改其現有的安全原則，以允許 WAN 和 LAN 之間的流量雙向透過。如需允許流量在 WAN 和 LAN 間以雙向傳遞，請參閱 *SonicOS 原*。

設定網路介面和啟用 L2B 模式

在這個應用情形中，WAN 介面的用途如下:

- 存取管理員使用的管理介面
- MySonicWall 上的訂閱服務更新
- 裝置的預設路由以及後續 SSL VPN 裝置內部流量的「下一躍點」（這是 WAN 介面必須與 SSL VPN 裝置的內部介面位於同一 IP 段的原因所在）

安全設備上的 LAN 介面用於監控來自 SSL VPN 裝置外部介面的未加密用戶端流量。這是以二層橋接模式執行的原因所在（而不是重新設定 SSL VPN 裝置的外部介面，從而將 LAN 介面視為預設路由）。

在**網路 | 介面**中，按一下 **WAN** 介面的**設定**圖示，然後為 WAN 指派一個可存取網際網路的位址，以便安全設備取得特徵更新並與 NTP 進行通訊。

閘道和內部/外部 DNS 位址設定，必須與 SSL VPN 裝置的對應設定相符:

- **IP 位址**：它必須與 SSL VPN 裝置上的內部介面的位址相符合。
- **子網路遮罩**、**預設閘道**和 **DNS 伺服器**：將這些位址設為與 SSL VPN 裝置的設定相符合。

對於**管理**設定，請選擇 **HTTPS** 和 **Ping**。按一下**確定**以儲存並啟用變更。

若要配置 LAN 介面設定:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下 **LAN** 介面的**設定**圖示。

3 對於 IP 指派設定，選擇二層橋接模式。

4 對於**橋接到**設定，選擇 **X1**。

5 如果您必須傳遞 VLAN 標記的流量 (安全設備提供支援時)，請按一下 **VLAN 篩選條件**。

6 加入所有需要傳遞的 VLAN。

7 按一下**確定**以儲存和啟用此變更。

您與安全設備管理介面間的連線會自動中斷。現在，您可以中斷安全設備的 X0 介面和您的管理筆記型電腦或桌上型電腦間的連線，然後關閉安全設備，再實際將裝置連上網路。

在網路與 SSL VPN 裝置之間安裝安全裝置

不論採用哪種部署方法（單宿主或多宿主），都應該將安全設備置於 SSL VPN 裝置的 X0/LAN 介面與內部網路連接之間。這使得裝置能夠向外連接 SonicWall 的授權和特徵更新伺服器，以及掃描來自請求存取內部網路資源的外部用戶端的解密流量。

如果您的 SSL VPN 裝置採用雙連接埠模式且位於供應商防火牆後面，則為雙宿主裝置。

若要連接雙宿主 SSL VPN 設備：

1 將安全設備的 X0/LAN 連接埠，連接到 SSL VPN 裝置上的 X0/LAN 連接埠。

2 將安全設備的 X1/WAN 連接埠，連接到之前連接 SSL VPN 的連接埠。

3 開啟安全設備的電源。

如果您的 SSL VPN 裝置採用單連接埠模式且位於供應商防火牆的 DMZ 區域中，則為單宿主裝置。

若要連接單宿主 SSL VPN 設備：

1 將安全設備的 X0/LAN 連接埠，連接到 SSL VPN 裝置的 X0/LAN 連接埠。

2 將安全設備的 X1/WAN 連接埠，連接到之前連接 SSL VPN 的連接埠。

3 開啟安全設備的電源。

設定或驗證設定

在網路中的管理工作站上，現在應該能夠透過安全設備的 WAN IP 位址存取其管理介面。

若要設定進階設定:

1 確認已啟用 SonicWall 安全設備的所有安全服務。參見第 286 頁「授權服務」和第 287 頁「在每個區域啟用安全服務」。

2 在與 SonicWall SMA SSL VPN 設備聯合部署此裝置之前，必須停用 SonicWall 內容篩選服務。

   a 導覽至**管理 | 系統安裝 | 網路 > 區域**頁面。

   b 按一下 **LAN (X0)** 區域旁邊的**設定**。

   c 取消勾選**強制執行內容篩選服務**。

   d 按一下**確定**。

3 如果您尚未變更 SonicWall 安全設備上的管理密碼，可以在**管理 | 系統安裝 | 設備 > 基本設定**中執行這項操作。

4 若要從外部用戶端測試網路存取，請連接到 SSL VPN 裝置並登入。

5 連上後，請嘗試存取您的內部網路資源。如果存在任何問題，請檢查您的設定並參閱第 285 頁「設定二層橋接模式部署的通用設定」。

設定二層橋接模式

主題：

用於二層橋接模式的設定任務清單

- 選擇適合您網路的拓撲
- 第 285 頁「設定二層橋接模式部署的通用設定」
    - 授權安全服務
    - 停用 DHCP 伺服器
    - 設定並啟用 SNMP 和 HTTP/HTTPS 管理
    - 啟用 syslog
    - 在受影響的區域啟用安全服務
    - 建立存取規則
    - 設定記錄設定
    - 設定無線區域設定
- 第 288 頁「設定主要橋接介面」
    - 為主要橋接介面選擇區域
    - 啟用管理
    - 啟用安全服務
- 第 288 頁「設定次要橋接介面」
    - 為次要橋接介面選擇區域
    - 啟用管理
    - 啟用安全服務
- 將安全服務套用於相應的區域

設定二層橋接模式部署的通用設定

在多數二層橋接模式拓撲中使用 SonicWall 安全設備之前，必須為裝置配置下列設定。

- 第 286 頁「授權服務」
- 第 286 頁「停用 DHCP 伺服器」
- 第 286 頁「設定 SNMP 設定」
- 第 286 頁「在介面上啟用 SNMP 和 HTTPS」
- 第 287 頁「啟用 Syslog」

- 第 287 頁「在每個區域啟用安全服務」
- 第 287 頁「建立存取規則」
- 第 287 頁「設定記錄設定」
- 第 287 頁「設定無線區域設定」

授權服務

已成功註冊安全設備時:

1 瀏覽至**管理 | 更新 | 授權**。

2 按一下**線上管理安全服務**中的**同步處理**。

系統會隨即連上安全設備授權伺服器，並確保安全設備已獲得正確的授權。

若要檢視授權狀態，請移至**監控 | 目前狀態 | 系統狀態**頁面，並檢視所有安全服務 (閘道防毒、防間諜軟體和入侵保護) 的授權狀態。

停用 DHCP 伺服器

在有其他裝置作為 DHCP 伺服器的網路設定中，以二層橋接模式使用 SonicWall 安全設備時，必須先停用安全設備的內部 DHCP 引擎 (這個引擎在預設情況下已設定並執行)。

若要停用 DHCP 伺服器:

1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 取消選取**啟用 DHCP 伺服器**。

3 按一下**接受**。

設定 SNMP 設定

若要配置 SNMP 設定:

1 導覽到**管理 | 系統安裝 | 設備 | SNMP**。

2 選擇**啟用 SNMP**。

3 按一下**接受**。**設定**按鈕隨即可供使用，系統也會填入 SNMP 資訊。

4 按一下**設定**。隨即顯示**設定 SNMP** 對話方塊。如需瞭解如何設定 SNMP，請參閱第 41 頁「設定 SNMP 存取權限」。

在介面上啟用 SNMP 和 HTTPS

若要在介面上啟用 SNMP 和 HTTPS:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 找出您要管理的裝備所使用的介面，然後按一下該介面的**編輯**圖示。將顯示**編輯介面**對話方塊。

3 對於**管理**選項，請啟用 **HTTPS** 和 **SNMP**。

4 按一下**確定**。

啟用 Syslog

您可以透過**記錄 > Syslog** 頁面啟用 Syslog。如需瞭解啟用 Syslog 的方法，請參閱 *SonicOS 記錄和報告*。

在每個區域啟用安全服務

在**管理 | 系統安裝 | 網路 | 區域**中，確認您要使用的每個區域都啟用了安全服務。

然後，在每項服務的**管理 | 安全設定 | 安全服務**中，為您的環境啟用及配置最適用的設定。如需瞭解啟用及設定安全服務的相關資訊，請參閱 *SonicOS 安全設定*。

建立存取規則

如果您打算從其他區域管理安全設備，或者即將使用第三方伺服器提供管理、SNMP 或 syslog 服務，請建立存取規則來處理這些區域間的流量。在**管理 | 原則 | 規則 > 存取規則**中，找出伺服器區域和具備使用者和伺服器的區域間的交叉點，然後按一下該交叉點的圖示 (您的環境中可能有許多這類的交叉點)。建立新規則，以允許伺服器與此區域內的所有裝置進行通訊。如需存取規則的相關資訊，請參閱 *SonicOS 原則*。

設定記錄設定

在**管理 | 記錄和報告 | 記錄設定 | 名稱解析**中，將**名稱解析方法**設為**先 DNS 後 NetBIOS**。如需配置記錄設定的資訊，請參閱 *SonicOS 記錄和報告*。

設定無線區域設定

在使用 HP PCM+/NIM 系統的情況下，如果將要在指派到 WLAN/無線區域的介面上管理 HP ProCurve 交換器，則需要停用兩項功能，否則將無法管理交換器。

若要配置無線區域設定:

1. 導覽到**管理 | 系統安裝 | 網路 | 區域**。
2. 選取無線區域。
3. 在**無線**上，取消選取**僅允許 SonicPoint 產生的流量和 WiFiSec 增強**選項。
4. 按一下**確定**。

二層橋接模式設定過程

如需選擇最適合您的網路的拓撲的資訊，請參見第 277 頁「二層橋接介面區域選擇」。這個範例中使用的是一種與簡單二層橋接拓撲最相似的拓撲。

選擇一個介面作為主要橋接介面。如需進行此項選擇的資訊，請參見第 277 頁「二層橋接介面區域選擇」。這個範例中使用了 X1 (已自動指派至主 WAN):

主題：

- 第 288 頁「設定主要橋接介面」
- 第 288 頁「設定次要橋接介面」
- 第 289 頁「設定用於硬體故障的 L2 旁路」

設定主要橋接介面

若要設定主要橋接介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下 X1 (WAN) 介面右邊欄中的**設定**圖示。

3 為介面設定固定 IP 位址（例如 192.168.0.12）。

附註：主要橋接介面必須擁有固定 IP 指派。

4 僅限 WAN 介面:

a 設定預設閘道。這是安全裝置自身存取網際網路所必需的。

b 設定 DNS 伺服器。

5 為介面選擇一個或多個**管理**選項: **HTTPS**、**Ping** (預設選取)、**SNMP**、**SSH**。

附註：選取 **HTTPS** 後，系統會自動啟用並選取**新增規則以啟用從 HTTP 到 HTTPS 的重新導向**。

6 選擇**使用者登入**選項: **HTTP**、**HTTPS**。

7 若要從 HTTP 重新導向到 HTTPS，請勾選**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。

8 按一下**確定**。

選擇一個介面作為次要橋接介面。如需進行此項選擇的資訊，請參見第 277 頁「二層橋接介面區域選擇」。

設定次要橋接介面

這個範例中使用了 X0 (已自動指派至 LAN):

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下 X0 (LAN) 介面右邊欄中的**設定**圖示。

3 對於 **IP 指派**，請選取**二層橋接模式**。

4 在**橋接目標**中，選取 **X1** 介面。

5 為介面選擇一個或多個**管理**選項: **HTTPS**、**Ping** (預設選取)、**SNMP**、**SSH**。

附註：選取 **HTTPS** 後，系統會自動啟用並選取**新增規則以啟用從 HTTP 到 HTTPS 的重新導向**。

6 選擇**使用者登入**選項: **HTTP**、**HTTPS**。

7 若要從 HTTP 重新導向到 HTTPS，請勾選**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。

8 您可以選擇啟用**封鎖所有的非 IPv4 流量**，禁止二層橋接傳遞非 IPv4 流量。

9 如需控制流經二層橋接的 VLAN 流量，請按一下 **VLAN 篩選條件**。預設允許所有 VLAN 流量：

- 從下拉清單中選擇**封鎖列出的 VLAN（黑名單）**，並將想要封鎖的 VLAN 從左側面板新增到右側面板中。新增到右側面板的所有 VLAN 將被封鎖，而保留在左側面板的所有 VLAN 將被允許透過。

- 從下拉清單中選擇**允許列出的 VLAN（白名單）**，並將想要顯見允許的 VLAN 從左側面板新增到右側面板中。新增到右側面板的所有 VLAN 將被允許透過，而保留在左側面板的所有 VLAN 將被封鎖。

10 按一下**確定**。**介面設定**表格中顯示了更新的設定:

您現在可以根據需要，將安全服務套用於相應的區域。在本範例中，應該將其套用於 LAN、WAN 或同時套用於兩個區域。

設定用於硬體故障的 L2 旁路

L2 旁路可用於透過 LAN 旁路功能將介面橋接到另一個介面時執行安全設備的實體繞過。這樣，即使發生無法恢復的防火牆錯誤，仍然可以繼續傳送網路流量。

在 L2 繞過轉接關閉時，連接到繞過介面（X0 和 X1）的網路纜線像一根連續網路纜線一樣進行實體連接。**使實體繞過故障**選項透過在發生故障時繞過防火牆為使用者提供避免中斷網路流量的選擇。

L2 旁路僅適用於二層橋接模式中的介面。**使實體繞過故障**選項只有在從**模式/ IP 指派**中選擇了**二層橋接模式**選項時，才會顯示。除非橋接對的兩個介面之間存在實體繞過轉接時，才會顯示此選項。

啟用**使實體繞過故障**選項後，系統會自動設定另一個**二層橋接模式**選項，設定如下:

- **封鎖所有的非 IPv4 流量** - 已停用。如啟用，此選項將阻塞所有非 IPv4 乙太網路框架。所以，此選項被停用。
- **從不路由流量到該橋接對上** - 已啟用。啟用時，此選項封鎖封包傳送到除橋接對的對等網路以外的網路。所以，此選項被啟用。
- **僅獲取該橋接對上的流量** - 已停用。啟用時，在橋接對介面上收到的流量不被轉送。所以，此選項被停用。
- **停用該橋接對上的狀態偵測** - 未變更。此選項不受影響。

若要設定 L2 旁路：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下想要設定的介面對應的**設定**欄中的**編輯**圖示。將顯示**編輯介面**對話方塊。

3 選取**使實體繞過故障。**

> **附註：**只有使用 NSA-6600 或 NSA-6600 以上版本同時橋接 X0 和 X1 介面時，系統才會提供**使實體繞過故障**選項。

4 按一下**確定**。

VLAN 與二層橋接模式的整合

SonicWall 安全設備支援 VLAN。在帶有 VLAN 標籤的封包到達實體介面時，系統會評估 VLAN ID，以確定其是否受到支援。VLAN 標籤將被剝離，然後採用與其他任何流量相同的方式繼續處理封包。傳入和傳出封包路徑的簡化檢視，包括以下可能反復執行的步驟:

- IP 驗證和重組
- 解封裝（802.1q、PPP）
- 解密
- 連接快取查詢和管理

- 路由原則查詢
- NAT 原則查詢
- 存取規則（原則）查詢
- 頻寬管理
- NAT 轉換
- 進階封包處理（如果適用）
    - TCP 驗證
    - 管理流量處理
    - 內容篩選
    - 轉換和流量分析 (在 SonicWall 安全設備上): H.323、SIP、RTSP、ILS/LDAP、FTP、Oracle、NetBIOS、Real Audio、TFTP
    - IPS 和 GAV

這時，如果封包已驗證為可接受的流量，則將其轉送至其目的地。封包輸出路徑包括：

- 加密
- 封裝
- IP 片段

在輸出上，如果路由原則查詢確定閘道介面為 VLAN 子介面，則為封包標籤（封裝）相應的 VLAN ID 標頭。建立 VLAN 子介面會自動更新防火牆的路由原則表：

自動建立與 VLAN 子介面相關的 NAT 原則和存取規則的行為與實體介面完全相同。借助簡易高效的 SonicOS，可以輕鬆地自訂用於管理 VLAN 之間的流量的規則和原則。

在建立區域（作為一般管理的組成部分或作為建立子介面的一個步驟）時，區域建立頁面中會顯示一個核取方塊，以控制自動建立用於此區域的群組 VPN。預設情況下，只有新建立的無線類型區域會啟用**為此區域建立群組 VPN**（儘管在建立過程中，可以透過勾選此核取方塊為其他區域類型啟用此選項）。

VLAN 子介面之間的安全服務管理可在區域級別實現。所有安全服務都是可設定的，且適用於由實體介面、VLAN 子介面或二者的組合構成的區域。

不同工作群組之間可透過使用 VLAN 分段，輕鬆地套用閘道防毒和入侵保護服務，而無需為每個受防護的分段使用專用的實體介面。

VLAN 支援使得組織無需使用防火牆上的專用實體介面，即可在各種工作群組以及工作群組與伺服器陣列之間提供有意義的內部安全（而不是簡單的封包篩選）。

此處講解了將 VLAN 子介面指派至 WAN 區域和使用 WAN 用戶端模式（在指派至 WAN 區域的 VLAN 子介面上僅支援固定定址）的功能，以及支援 WAN 負載平衡和容錯移轉的功能。此外還展示了透過將 SonicPoints 連接到工作站交換器上的存取模式 VLAN 連接埠的方法，在整個網路中進行分發。這些交換器隨即回載到核心交換器，並由核心交換器透過主幹連結將所有 VLAN 連接到裝置。

VPN 與二層橋接模式的整合

在同時設定用於二層橋接模式的介面上設定 VPN 時，必須設定一個額外的路由，以確保傳入的 VPN 流量正確地穿過安全設備。

若要整合 VPN 與二層橋接模式:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下**新增**圖示。**新增路由原則**對話方塊隨即顯示。

3 按照下列說明設定路由:

- 來源：**任何**
- 目的地: *自訂 VPN 位址物件*（用於本機 VPN 通道 IP 位址範圍的位址物件。）
- 服務：**任何**
- 閘道：`0.0.0.0`
- 介面：**X0**

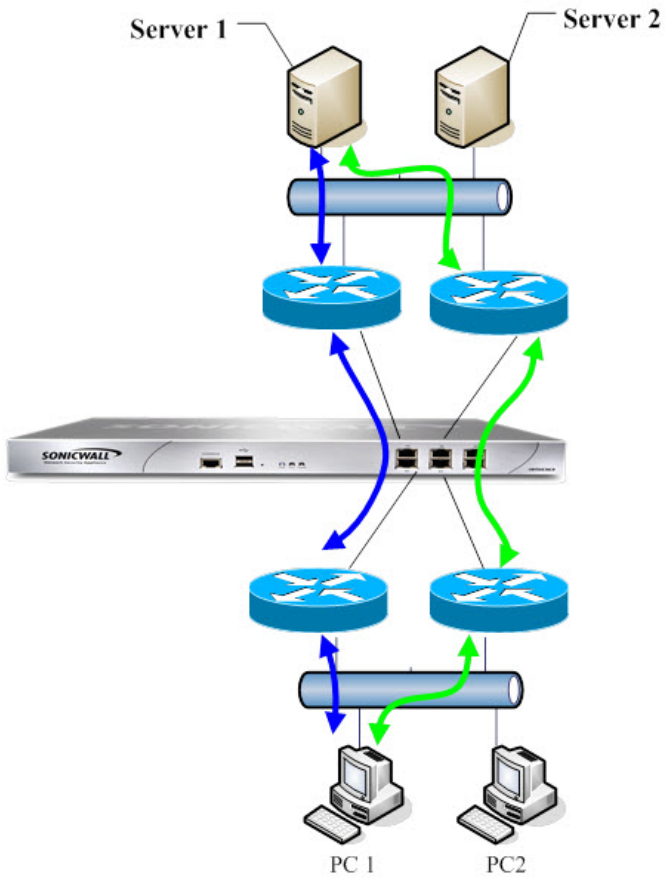
4 按一下**確定**。

非對稱路由

SonicOS 支援非對稱路由。非對稱路由是指沿某個方向的封包流所經過的介面不同於返回路徑所用的介面。當流量流過安全設備中不同的二層橋接對介面，或流經高可用性叢集中的不同安全設備時，就會出現這種情況。

任何執行深度封包檢查或狀態監控防火牆活動的安全設備，都必須「看到」與封包流相關的所有封包。傳統的 IP 路由則不同，流中的各封包在技術上可以沿不同的路徑轉送，只要它能到達目的地，中間的路由器不必看到每個封包。當今的路由器對各封包流確實會嘗試用一致的下一躍點轉送封包，但這僅適用於沿同一方向轉送的封包。路由器不會嘗試將返回流量引導至起來源路由器。這種 IP 路由行為會給不支援非對稱路由的安全設備叢集帶來問題，因為這組叢集節點都提供了一條到相同網路的路徑。透過叢集轉送封包到網路的路由器可以選擇任一叢集節點作為下一躍點。結果便是非對稱路由，沿某個方向的封包流所經過的節點不同於返回路徑所用的節點。流中的這一差異導致流量被這兩個叢集節點之一或被這兩個叢集節點同時丟棄，因為任一節點都沒有「看到」流中的所有流量。請參閱非對稱路由。

非對稱路由



Asymmetric Routing Traffic

在非對稱路由中，PC1 與 Server1 進行通訊，雙向流量流經不同的路由器，即同一連接的某些封包流過藍色路徑，而另一些封包流過綠色路徑。在此類部署中，路由器可能會執行某一冗餘路由通訊協定或負載平衡通訊協定，例如 Cisco HSRP 通訊協定。

SonicOS 使用狀態偵測。通過安全設備的所有連線都會以介面為目的地。但是，由於支援非對稱路由，因此 SonicOS 會追蹤輸入和輸出流量（即便在流經過不同介面時也是如此）並提供有狀態深層封包檢查。

附註：非對稱路由不同於沒有回覆的單向連接，即 TCP 狀態繞過。

設定 IPv6 介面

如需設定 IPv6 介面的完整描述，請參見第 767 頁「IPv6 介面設定」。

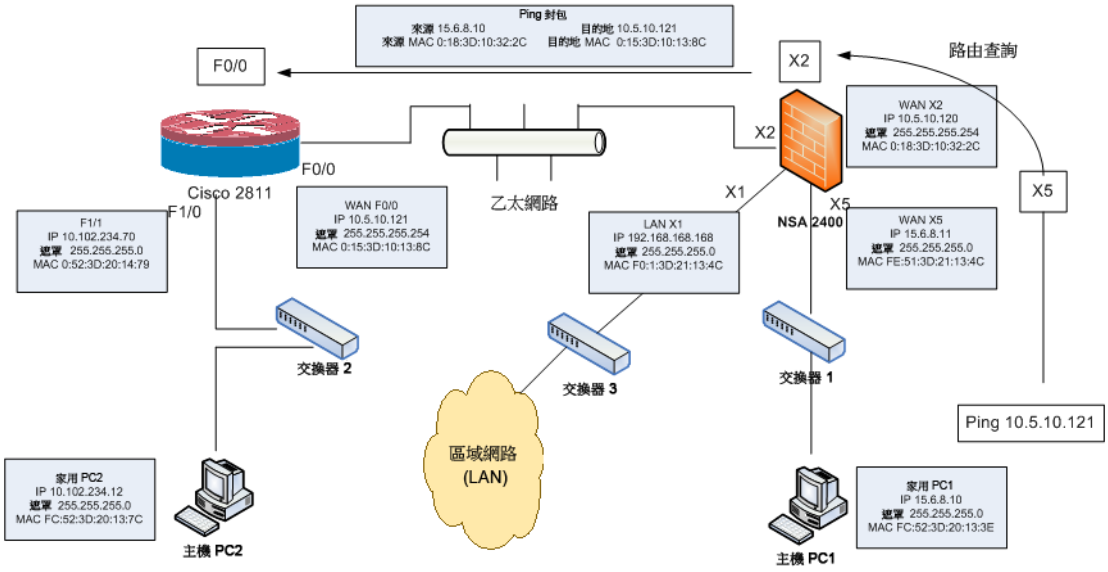
31 位元網路

SonicOS 6.2.7 支援 RFC 3021，這會定義 31 位元子網路遮罩的使用。此遮罩在子網路中僅允許兩個主機位址，不包含 “network” 或 “gateway” 位址，並且無廣播位址。這類設定可在較大網路內使用，連接兩部主機和點對點連結。源於此項變更的位址空間精簡輕易可見，在大型網路中的每個點對點連結只占用兩個位址而不是四個。

在此環境中，點對點連結與 PPP (點對點通訊協定) 不相等。使用 31 位元遮罩的點對點連結可使用或不使用 PPP 通訊協定。在點對點連結上 31 位元首碼的 IPv4 位址也可用於乙太網路。

主題：

範例網路環境



在此網路環境中，主機 PC1 和主機 PC2 可使用彼此造訪，而 LAN 網路中的主機可以造訪主機 PC2。

若要設定此環境的設定值：

1 對於主機 PC1，新增兩個路由項目：

- `Route add 10.5.10.0 mask 255.255.255.0  15.6.8.10`
- `Route add 10.102.234.0 mask 255.255.255.0  15.6.8.10`

2 對於主機 PC2，新增兩個路由項目：

- `Route add 10.5.10.0 mask 255.255.255.0  10.102.234.70`
- `Route add 15.6.8.0 mask 255.255.255.0  10.102.234.70`

3 在 Cisco 路由器 (F0/0) 上：

- `interface fastEthernet 0/0`
- `ip address 10.5.10.120 255.255.255.254`

4 在其他 Cisco 2811 上，新增一個路由項目：

```
!
ip route 15.6.8.0 255.255.255.0 10.5.10.120
!
```

5 在防火牆上，新增一個路由項目，啟用從 X2 到 X5 和 X5 到 X2 的 WAN 區域資料流。

```
Any    10.102.234.0    Any    X2 Default Gateway    X2
```

設定 SonicOS

若要設定 31 位元子網路的介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 編輯所需的介面。

3 將**子網路遮罩**設定為 255.255.255.254。

4 在 **IP 位址**欄位中輸入一組主機 IP 位址。

5 在**預設閘道**欄位中輸入其他主機 IP 位址。

6 根據您的網路依照需要設定其他欄位。

7 按一下**確定**。

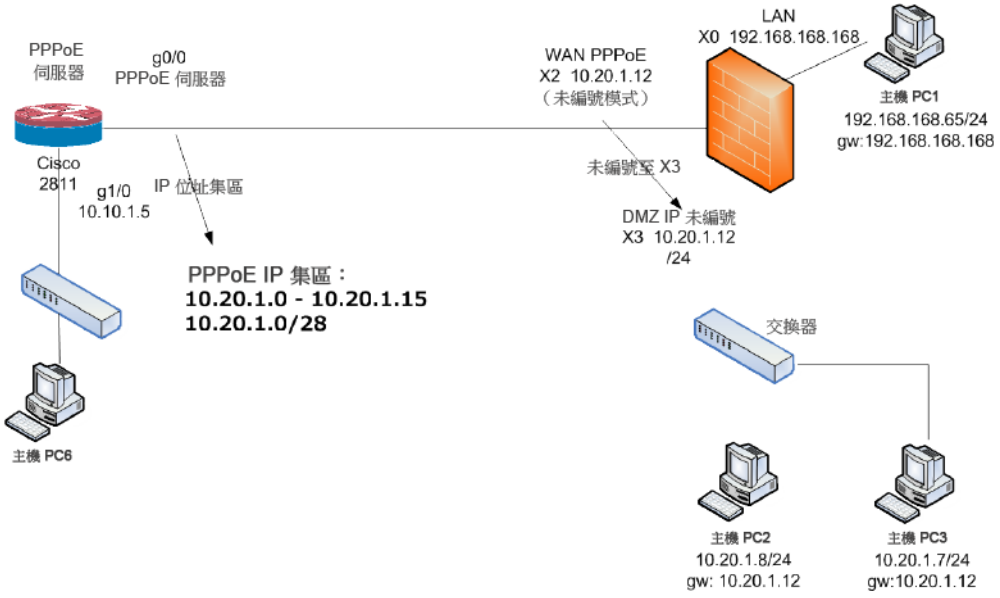
PPPoE 未編號介面支援

PPPoE 未編號的介面可讓您管理一個範圍內只有單一 PPPoE 連線的 IP 位址。網際網路服務供應商 (ISP) 提供可在子網路內配置的多組固定 IP 位址。第一個位址指定為網路位址，而最後一個位址指定為廣播位址。

PPPoE 的預設 MTU 為 **1492**。

主題：

範例網路拓撲



在此拓撲中，X2 是 PPPoE 未編號的介面，而 X3 是未編號的介面。

SonicOS 會新增 2 個原則至**網路 | 路由 > 路由原則**功能表。

SonicOS 也新增兩個 NAT 原則：

注意

若要在設定 X2 未編號至 X3 時將 X3 變更為其他模式，首先將 X2 變更為其他模式來終止與 X2 的關連性。否則，您若變更 IP 位址或介面 X3 的遮罩，會導致 X3 重新連線到 PPPoE 伺服器。

如果 X3 設定為未編號的介面，其他介面便無法使用二層橋接連線到 X3。

設定 PPPoE 未編號介面

若要設定 PPPoE 未編號介面：

1. 導覽到**管理 | 系統安裝 | 網路 | 介面**。
2. 透過按下其**編輯**圖示，在 WAN 介面上設定 PPPoE 用戶端設定：將顯示**編輯介面**對話方塊。
3. 選擇**未編號的介面**。下拉功能表隨即啟用。
4. 選擇**建立新的未編號的介面**。將顯示**新增未編號的介面**對話方塊。
5. 對於**區域**，選擇 **LAN**、**DMZ** 或建立新的區域。

   附註： 模式 / IP 指派會設定為 **IP 未編號**且變成灰色。

6. 對於 **IP 位址**，輸入您的 ISP 提供的位址。通常是供應商指派的第二組 IP 位址。
7. 在**子網路遮罩**欄位中輸入 ISP 所指定的子網路遮罩。
8. 完成設定此介面。
9. 按一下**確定**。
10. 完成設定第一個介面。
11. 按一下**確定**。

使用 PPPoE 未編號設定 HA

如需如何使用 PPPoE 未編號設定 HA，請參閱第 534 頁「設定使用中/待命高可用性設定」。

14

設定 PortShield 介面

附註：NSA 2600 安全設備不支援 PortShield，SOHO W 安全設備不支援 X- 系列解決方案。

網路 | PortShield 群組

主題：

關於 PortShield

PortShield 介面是具有一組連接埠的虛擬介面，包括 Dell X 系列上的連接埠、延伸的、交換器、指派的連接埠。使用 PortShield 結構，您可以將部分或所有 LAN 連接埠設定到單獨的安全上下文中，不僅為來自 WAN 和 DMZ 的流量，而且在網路中的裝置之間提供防護。每個內容實際上都具有自己的線速 PortShield，享有專屬深層封包偵測安全設備所提供的防護。

提示：即使未使用 PortShield 群組，也隨時可以在**管理 | 系統安裝 | 網路 | 介面**中將區域套用於多個介面。但是，除非這些介面使用 PortShield 群組，否則它們將不會共用相同的網路子網路。

您可以將任何連接埠組合指派到 PortShield 介面。系統會將所有未指派給 PortShield 介面的連接埠指派到 LAN 介面。

固定模式和透明模式

您可以採用兩種 IP 指派方法來建立 PortShield 介面:

- 固定模式
- 透明模式

以固定模式工作

在固定模式下建立 PortShield 介面時，您會手動建立一個要套用於 PortShield 介面的明確位址。對應至此介面的所有連接埠將由此位址識別。固定模式在指派給可信、公用或無線區域的介面上可用。

附註：以固定模式建立 PortShield 介面時，請確保其他 PortShield 介面未使用您指派給此介面的 IP 位址。

以透明模式工作

通過透明模式定址，目前介面可以使用位址物件指派來共用 WAN 子網路。介面的 IP 位址與 WAN 介面 IP 位址相同。透明模式在指派給可信和公用區域的介面上可用。

附註：請確認您指派給 PortShield 介面的 IP 位址位於 WAN 子網路內。

在透明模式下建立 PortShield 介面時，您會建立一系列要套用於 PortShield 介面的位址。您將這些位址包括在一個稱為位址物件的實體中。這些位址物件允許定義一次實體，並在整個 SonicOS 介面的多個引用實例中重複使用。使用位址物件建立 PortShield 介面時，對應至此介面的所有連接埠將由在位址範圍中指定的任何位址識別。

附註：每個位址固定的 PortShield 介面都必須分屬於不同的子網路。PortShield 介面不得重覆出現在多個子網路中。

SonicOS 支援 X- 系列交換器

主題：

關於 X- 系列解決方案

附註：NSA 2600 或 SOHO W 安全設備不支援 X- 系列解決方案。

重要網路元件 (譬如安全設備和交換器) 通常需要個別管理。SonicOS 允許使用安全設備管理介面和 GMS 統一管理安全設備和 Dell X- 系列交換器。

如介面數安全設備表格中所示，SonicWall 安全設備上的可用介面數量上限會依型號而有所不同。

介面數安全設備

防火牆型號	可用的介面數
SM 9600	20 個 (4 個 10 GbE SFP+、8 個 1 GbE SFP、8 個 1GE copper)、1 個 GbE 管理和 1 個主控台
SM 9400	20 個 (4 個 10 GbE SFP+、8 個 1 GbE SFP、8 個 1GE copper)、1 個 GbE 管理和 1 個主控台
SM 9200	20 個 (4 個 10 GbE SFP+、8 個 1 GbE SFP、8 個 1GE copper)、1 個 GbE 管理和 1 個主控台
NSA 6600	20 個 (4 個 10 GbE SFP+、8 個 1 GbE SFP、8 個 1GE copper)、1 個 GbE 管理和 1 個主控台
NSA 5600	18 (2 個 10 GbE SFP+、4 個 1 GbE SFP、12 個 1GE copper) 和 1 個管理

介面數安全設備

防火牆型號	可用的介面數
NSA 4600	18 (2 個 10 GbE SFP+、4 個 1 GbE SFP、12 個 1GE copper) 和 1 個管理
NSA 3600	18 (2 個 10 GbE SFP+、4 個 1 GbE SFP、12 個 1GE copper) 和 1 個管理
NSA 2650	
TZ600	10 GbE
TZ500 系列	8 GbE
TZ400 系列	7 GbE
TZ300 系列	5 GbE

特定部署中，所需的連接埠數量可能很容易超過可在安全設備上使用的介面數量上限。透過使用 X- 系列解決方案，就可以將 Dell X- 系列交換器上的連接埠看作安全設備的延伸介面，從而使可用的介面數增加到最多 192 個 (具體取決於 X- 系列交換器)。這些延伸連接埠可經由連接埠防護及/或設定來獲得高可用性 (HA)，同時也可視為安全設備的任何其他介面。

附註：X- 系列交換器、X- 交換器、外部交換器和延伸交換器可互換使用。

X- 系列交換器 SonicWall 安全設備支援表格中所列的 SonicWall 安全設備，可支援多達 4 部 X- 系列交換器 (如下所列)。

附註： 如需有關 X- 系列交換器及如何設定這些交換器的完整資訊，請參閱 *SonicWall X-系列解決方案部署指南*、*Dell Networking X1000 和 X4000 系列交換器使用者指南*及 *Dell Networking X1000 和 X4000 系列交換器入門指南*。

X- 系列交換器 SonicWall 安全設備支援

下列 SonicWall 安全設備

- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2650
- TZ600
- TZ500/TZ500W
- TZ400/TZ400W
- TZ300/TZ300W

支援這些 X- 系列交換器 (連接埠)

- X1008 (8 個 10/100/1000Base-T GbE)
- X1008P (8 個 10/100/1000Base-T GbE、2 個 1GbE SFP fiber、8 個 PoE 總計高達 123 W)
- X1018 (16 個 10/100/1000Base-T GbE、2 個 1GbE SFP fiber)
- X1018P (16 個 10/100/1000Base-T GbE、2 個 1GbE SFP fiber、16 個 PoE 總計高達 246W)
- X1026 (24 個 10/100/1000Base-T GbE、2 個 1GbE SFP fiber)
- X1026P (24 個 10/100/1000Base-T GbE、2 個 1GbE SFP fiber、24 個 PoE/12 個 PoE+ 總計高達 369W)
- X1052 (48 個 10/100/1000Base-T GbE、2 個 10GbE SFP/SFP+ fiber)
- X1052P (48 個 10/100/1000Base-T GbE、24 個 PoE/12 PoE+ 總計高達 369W)
- X4012 (12 個 10GbE SFP/SFP+ fiber)

附註：NSA 2600 或 SOHO W 安全設備不支援 X- 系列解決方案。

主題：

術語

HA	高可用性
延伸交換器	同 X- 系列交換器。
外部交換器	同 X- 系列交換器。
IDV	透過 VLAN 消除介面歧義 - 在延伸交換器上重新設定連接埠，以連接埠防護方式處理到安全設備介面，作為對應到 PortShield VLAN 的 VLAN 存取連接埠。
PoE	Power over Ethernet (透過乙太網路供電) - 透過乙太網路線供電同時傳輸資料的系統，僅以一條線同時提供資料連線和供電給裝置。
PoE+	乙太網路供電+ - PoE 的進階版本（802.3at 標準版），可提供比 PoE 更高的功率。
SFP	Small form-factor pluggable (小型熱插拔收發器) - 一種可熱插拔的精簡型收發器，用於通訊和資料通訊應用程式，支援 1Gb 光纖模組。
SFP+	Enhanced small form-factor pluggable (進階版小型熱插拔收發器) - 進階版的 SFP，支援 10 Gb 光纖模組。
SPM	單點管理
STP	Spanning Tree Protocol (跨距樹狀目錄通訊協定) - 一種網路通訊協定，確保無迴圈拓撲的乙太網路，並允許冗餘 (備用) 連結，以便在作用中的連接失效時提供備份路徑。

效能要求

SonicWall 安全設備目前能夠:

- 為最多四部 X- 系列交換器進行佈建。
- 管理數量增加的連接埠。

X- 系列交換器支援的主要功能

附註：如需這些功能的更多資訊，請參見 SonicWall X- 系列解決方案部署指南。

- 將 X- 系列交換器部署為延伸交換器
- PortShield 功能
- 設定延伸交換器的介面設定
- 管理基本延伸交換器全域參數
- 使用 GMS 管理延伸交換器
- 具備 PortShield 功能的高可用性 (HA)

  使用一般上行連結時，可支援 HA 模式中的 PortShield 功能。在這項設定中，使用中/待命安全設備和 X- 系列交換器間的連結會作為一般上行連結使用，以便承載所有 PortShield 流量。同時在這項設定中，作為 PortShield 主機使用的安全設備介面應連上個別的交換器，而不是連上使用中/待命裝置所連線的 X- 系列交換器。這是為了避免同一個 PortShield VLAN 封包進入循環狀態。PortShield 成員可以連上 X- 系列交換器 (由使用中/待命安全設備所控制) 的連接埠。
- 支援診斷延伸交換器
- 利用 SPM 設定支援上行連結中的 VLAN
- 專屬上行連結設定中的 VLAN 支援
- VLAN 流量透過一般上行連結的單點管理

  一般上行連結也支援 VLAN。這讓安全設備和 X- 系列交換器間的單一連結能夠承載管理 X- 系列交換器的安全設備管理流量，以及對應到安全設備介面的*透過 VLAN 消除介面歧義* (IDV) VLAN 的 PortShield 流量，還有一般上行連結介面下的 VLAN 子介面流量。

  附註： 在設定為專屬上行連結或一般上行連結到相同交換器的安全設備介面下，不可存在重疊的 VLAN。這是因為 VLAN 空間在 X- 系列交換器上是全域。

  附註：不支援 PortShield 的延伸交換器介面連接至一般上行連結介面，而無需選擇任何 VLAN 以存取/轉接設定。
- 特定 Dell X- 系列交換器的 SonicWall 安全設備 PoE/PoE+ 和 SFP/SFP+ 功能。
- 批次處理設定訊息 - 若要加快 X- 系列交換器的支援，可在傳送到 X- 系列交換器之前批次處理設定訊息。

PortShield 功能和 X- 系列交換器

PortShield 結構允許將安全設備連接埠設定到個別的安全區域中，進而針對跨區域裝置間的流量，為深度封包偵測安全設備提供防護。如需更多 PortShield 功能相關資訊，請參閱第 296 頁「設定 PortShield 介面」。

SonicWall X- 系列解決方案能夠將延伸交換器上的介面以連接埠屏蔽方式處理至安全設備介面。X- 系列交換器為 L2 交換器，並且預設延伸交換器上的所有連接埠均設定為預設 VLAN 1 的存取連接埠。延伸交換器的連接埠以連接埠屏蔽方式處理至安全設備介面時，會被重新設定為對應到 PortShield VLAN 的 VLAN 存取連接埠，也就是 PortShield 主機介面的 IDV VLAN。

主題：

- 第 301 頁「不同的 PortShield 流量環境」
- 第 301 頁「PortShield 前提條件 X- 系列交換器」

不同的 PortShield 流量環境

- 與作為部分同一 PortShield 群組的延伸交換器上的連接埠相連的網路裝置之間的流量，將由延伸交換器自動交換。
- 與延伸交換器上的連接埠相連的網路裝置及與作為部分同一 PortShield 群組的安全設備上的連接埠相連的裝置之間的流量，將由安全設備上的內部交換器交換。
- 與延伸交換器（目的地為安全設備介面）上的連接埠相連的網路裝置之間的流量，將由軟體中的資料路徑處理。此流量可能受存取規則、深層封包檢查及入侵保護等安全設備安全服務的影響。
- 連上延伸交換器連接埠的網路裝置，和連上安全設備 (隸屬於不同區域或不同 PortShield 群組) 連接埠的裝置，兩者間的流量會由軟體中的資料路徑轉送。這類流量會受到軟體內的安全設備安全服務影響。

PortShield 前提條件 X- 系列交換器

重要：如果拓撲有兩部或以上的 X- 系列交換器，則 X- 系列交換器可不予串聯或採取菊花式鏈結，也就是其中一部 X- 系列交換器可連上另一部已連上安全設備的 X- 系列交換器。

- X- 系列交換器（不包括 X1052/X1052P 型號）出廠交付時處於「非管理模式」，以防止對交換器未經授權的存取。您需要按下電源插頭附近的「模式」按鈕，並保持 7 秒鐘，以將交換器切換為管理模式。

  X1052/X1052P 型號出廠交付時預設值為「管理」模式。

  在交換器的初始設定中，如需確保在安全設備介面上啟用 DHCP 伺服器時，X- 系列交換器的 IP 不發生動態變更，請選擇**固定 IP**，而不是**動態 IP**。

  如需更多資訊，請參閱 *SonicWall X-系列解決方案部署指南*。
- 除了可在交換器上找到的初始 IP 位址、使用者名稱/密碼設定外，不推薦通過交換器 GUI/主控台直接在 X- 系列交換器上執行其他設定。這樣會使安全設備與 X- 系列交換器的設定狀態不同步。
- 若要從安全設備管理 X- 系列交換器，則安全設備的其中一個介面必須和 X- 系列交換器位於同一個子網路中。例如，如需管理預設 IP 為 `192.168.2.1` 的 X- 系列交換器，安全設備的某個介面需要設定在 `192.168.2.0/24` 子網路中，並連接到 X- 系列交換器。
- 請先從安全設備佈建/管理交換器，再從安全設備偵測 X- 系列交換器，藉此確保安全設備能夠連上 X- 系列交換器。
- VLAN 支援：
  - VLAN 支援無法使用於共用上行連結和一般上行連結。例如，可在設定為 X- 系列交換器的共用上行連結的安全設備介面下面設定 VLAN。
  - 如需 VLAN 支援的更多資訊，請參閱 *SonicWall X-系列解決方案部署指南*。
  - 在安全設備設定為專屬上行連結的情況下，不會出現重疊的 VLAN。例如，如果為專屬上行連結設定了 X3 和 X5，VLAN 100 無法出現在 X3 和 X5 下。這類設定會被拒絕。

Dell X 系列菊花式鏈結支援

附註：NSA 2600 平台不支援這項功能。

Dell TZ-X 菊花式鏈結解決方案能夠在菊花式鏈結模式中整合 SonicWall 安全設備和已建立連線的 Dell X- 系列交換器。在菊花式鏈結模式中，所有 Dell X- 系列交換器型號都可供您進行整合，例如 X1008/X1008P、X1018/X1018P、X1026/X1026P、X1052/X1052P, 和 X4012。

菊花式鏈結可讓具備大型設置 (例如倉庫) 的環境，在距離指定站台超過 1000 英呎的地點部署 2 部 X 系列交換器，並且透過光纖相互連線、讓第一台交換器 (父級交換器) 與安全設備建立連線，並且透過安全設備一併管理兩部交換器。這種部署方式也能夠讓您使用安全設備上的單一介面，存取更多 X 系列交換器上的介面。您還可以透過安全設備管理父級交換器和子級交換器上的所有介面。

主題：

假設和相依性

- Dell X- 系列交換器菊花式鏈結解決方案僅限支援單一層級的鏈結，不支援多層級的鏈結 (串連 2 部以上交換器)。舉例來說，父級交換器可連結至子級交換器，但子級交換器間無法建立連結。
- 您最多可部署 4 部延伸交換器。舉例來說，父級交換器最多可擁有 3 部子級交換器。
- 在菊花式鏈結模式中，子級交換器唯一支援的拓撲就是一般上行連結，子級交換器會透過單一上行連結連上父級交換器。其他拓撲結構 (例如專屬上行連結、隔離連結等) 皆不適用於子級交換器。

菊花式鏈結支援

在菊花式鏈結模式中建立連結的兩部交換器，都必須具備位於同一個子網路的 IP 位址，且安全設備也必須能夠連上這個子網路。在菊花式鏈結模式中佈建交換器時，必須進行兩個步驟:

1. 將父級交換器佈建為獨立交換器。
2. 將子級交換器佈建為菊花式鏈結交換器。

PoE/PoE+ 和 SFP/SFP+ 支援

SonicWall 安全設備不支援 PoE/PoE+，但是此功能可透過特定 X- 系列交換器加入，如 X- 系列交換器 PoE/PoE+ 和 SFP/SFP+ 支援表格所示。這個額外的功能可增強 SonicWall 安全設備的 SonicPoint 用量，尤其是支援 802.11ac (支援高達 30W 的最大電力；802.11a/b/g/h 支援高達 15.4 的最大電力) 的新 SonicPoints。

部分 X- 系列交換器也支援 SFP/SFP+，如 X- 系列交換器 PoE/PoE+ 和 SFP/SFP+ 支援表格所示。

附註：X- 系列交換器上的 PoE/PoE+ 連接埠設定是由 X- 系列交換器的 UI 管理，而不是透過 SonicWall 安全設備的**管理 | 系統安裝 | 網路 | PortShield 群組**進行。

X- 系列交換器 PoE/PoE+ 和 SFP/SFP+ 支援

此 X 系列交換器	支援
X1008	1 PoE PD 連接埠；預設，埠號 8 為 PD 連接埠
X1008P	8 PoE 連接埠，總計高達 123W；預設，埠號 1 到 8 支援 PoE
X1018	2 1GbE SFP 連接埠；預設，埠號 17 到 18 支援 SFP
X1018P	16 PoE 連接埠，總計高達 246W；預設，埠號 1 到 16 支援 PoE 2 1GbE SFP 連接埠；預設，埠號 17 到 18 支援 SFP
X1026	2 1GbE SFP 連接埠；預設，埠號 25 到 26 支援 SFP

X- 系列交換器 PoE/PoE+ 和 SFP/SFP+ 支援

此 X 系列交換器	支援
X1026P	24 PoE/12 PoE+ 連接埠，預設，總計高達 369W： • 埠號 1 到 12 支援 PoE+ • 埠號 13 到 24 支援 PoE 2 1GbE SFP 連接埠；預設，埠號 25 到 26 支援 SFP
X1052	4 10GbE SFP+ 連接埠；預設，埠號 49 到 52 支援 SFP+
X1052P	24 PoE/12 PoE+ 連接埠，預設，總計高達 369W： • 埠號 1 到 12 支援 PoE+ • 埠號 13 到 24 支援 PoE • 埠號 25 到 48 不支援 PoE 和 PoE+ 4 10GbE SFP+ 連接埠；預設，埠號 49 到 52 支援 SFP+
X4012	12 10GbE SFP+ 連接埠；預設，埠號 1 到 12 支援 SFP+

重要：沒有外部電源供應的 SonicPoint AC 必須在 X1026P 或 X1052P X- 系列交換器上透過埠號 1 到 12 屏蔽防護。

沒有外部電源的任何 SonicPoint 非 AC 型號可以對連接埠 1 到 8 (X1008P)、1 到 16 (X1018P) 或 1 到 24（X1026P 和 X1052P）進行連接埠屏蔽。

有外部電源的任何 SonicPoint 可以對任何乙太網路連接埠進行連接埠屏蔽。

X- 系列解決方案和 SonicPoints

延伸交換器上的連接埠可以屏蔽防護到安全設備的 WLAN 區域，並且 SonicPoint 可以連接到這些連接埠。

連接 SonicPoints 到 X- 系列交換器時，考慮 SonicPoint 的電源要求非常重要。SonicPointACe/ACi/N2 需要最少 25.5 W。如果您的 X- 系列交換器不支援 PoE+，您必須使用 SonicPoint 饋電器。至於哪些交換器支援 PoE+，請參閱第 302 頁「PoE/PoE+ 和 SFP/SFP+ 支援」。如需管理 SonicPoints 的詳細資訊，請參閱知識庫文章 *SonicWall TZ 系列和 SonicWall X-系列解決方案管理 SonicPoint ACe/ACi/N2 存取點* (SW13970)。

使用 GMS 管理延伸交換器

X- 系列交換器整合功能允許使用 SonicOS 管理介面和 SonicWall GMS 版本 8.1 SP1 或更高版本對安全設備和交換器進行統一管理。GMS 支援所有設定操作，例如佈建延伸交換器、設定延伸交換器介面設定值，以及可管理延伸交換器全域參數。

如需有關使用 GMS 管理延伸交換器的資訊，請參閱最新的《*SonicWall GMS 管理指南*》。

延伸交換器全域參數

延伸交換器全域參數表格顯示可通過 SonicOS 管理介面設定的延伸交換器全域參數。

附註：如需這些參數的更多資訊，請參閱 *SonicWall X-系列解決方案部署指南*。

延伸交換器全域參數

所有交換器	僅 X1026P 和 X1052P 交換器
STP 模式	**PoE 警示用量閾值**
STP 狀態	**PoE 陷阱**
	PoE 電源限制模式

關於連結

管理 (MGMT) 連結僅攜帶管理流量且無法進行連接埠屏蔽。

資料連結會攜帶所有 PortShield 流量。如果其攜帶的所有流量均為資料，則此連結稱為共同連結。在一些拓撲中，資料連結也攜帶管理流量，我們在此情況下稱其為共用連結。

共用或共同連結可攜帶所有連接埠屏蔽的組。

專屬連結僅可承載一個 PortShield 群組，而該群組在安全設備上必須屏蔽防護到專屬連接埠。

關於上行連結介面

上行連結介面可視為設定為承載標記/未標記流量的「主幹」連接埠。當延伸交換器新增了安全設備上行連結和 X- 交換器上行連結選項時，安全設備上設定為 SuperMassive 上行連結的連接埠，以及延伸交換器上設定為交換器上行連結的連接埠，都會被自動設定為可為所有 IDV VLAN 自動接收/傳送標記的流量。標記流量的 IDV VLAN 可讓韌體導出流量中的 PortShield 主機流量。

設定上行連結介面的條件

- 介面必須為實體介面，不允許虛擬介面。
- 介面必須為交換器介面。(在部分平台上，某些安全設備介面並未連上交換器。這類介面是不被允許的。)
- 介面不可為 PortShield 主機 (某些安全設備介面無法以連接埠屏蔽方式處理到這個主機) 或 PortShield 群組成員 (無法以連接埠屏蔽方式處理到其他安全設備介面)。
- 介面不可為橋接器主要或橋接器次要介面。
- 介面不可有任何子系 (不可為其他子介面的父介面)。

記錄和系統記錄支援

支援記錄重要設定事件，例如新增/刪除交換器、在延伸交換器上設定 PortShield 和網路事件 (例如連接埠上行/下行)。

支援的拓撲

重要：設定安全設備和 X- 系列交換器間的介面時，如 *SonicWall X-系列解決方案部署指南*中所述設定交換器。

附註：如需佈建和設定這些拓撲的更多資訊，請參閱 *SonicWall X-系列解決方案部署指南*。

如需使用 X- 系列交換器設定 PortShield 介面的基本詳細資訊，請參閱第 305 頁「管理連接埠」。

X- 系列交換器支援的主要支援拓撲：

- 一般上行連結設定

- 專屬上行連結設定

  重要：必須通過作為部分專屬連結的連接埠對 SonicPoints 進行連接埠屏蔽。

- 一般和專屬上行連結的混合設定
- 管理和資料流量的共用連結設定
- 為管理和資料上行連結的隔離連結
- 具有專屬上行連結的 HA 和 PortShield 設定
- 具有一般上行連結的 HA 和 PortShield 設定
- 透過 SPM 設定的 VLAN 和一般上行連結
- 具有專屬上行連結設定的 VLAN
- SonicPoint 存取的專屬連結

管理連接埠

重要：SOHO W 安全設備不支援 X- 系列解決方案。僅管所有安全設備連接埠的管理方式都相同，但這些安全設備的**管理 | 系統安裝 | 網路 | PortShield 群組**則有所差異，詳情請參閱第 313 頁「管理 SOHO W 防火牆上的連接埠」。

管理 | 系統安裝 | 網路 | PortShield 群組可讓您透過下列管道管理連接埠的 PortShield 介面指派作業:

- **連接埠圖形**
- **連接埠組態**
- **外部交換器組態**
- **外部交換器診斷**

主題：

- 第 306 頁「檢視連接埠圖形上的介面 (連接埠)」
- 第 308 頁「透過連接埠設定標籤查看 PortShield 介面狀態並進行編輯」

- 第 310 頁「檢視和管理外部交換器設定」
- 第 311 頁「監控外部交換器診斷並管理韌體」
- 第 313 頁「管理 SOHO W 防火牆上的連接埠」

檢視連接埠圖形上的介面 (連接埠)

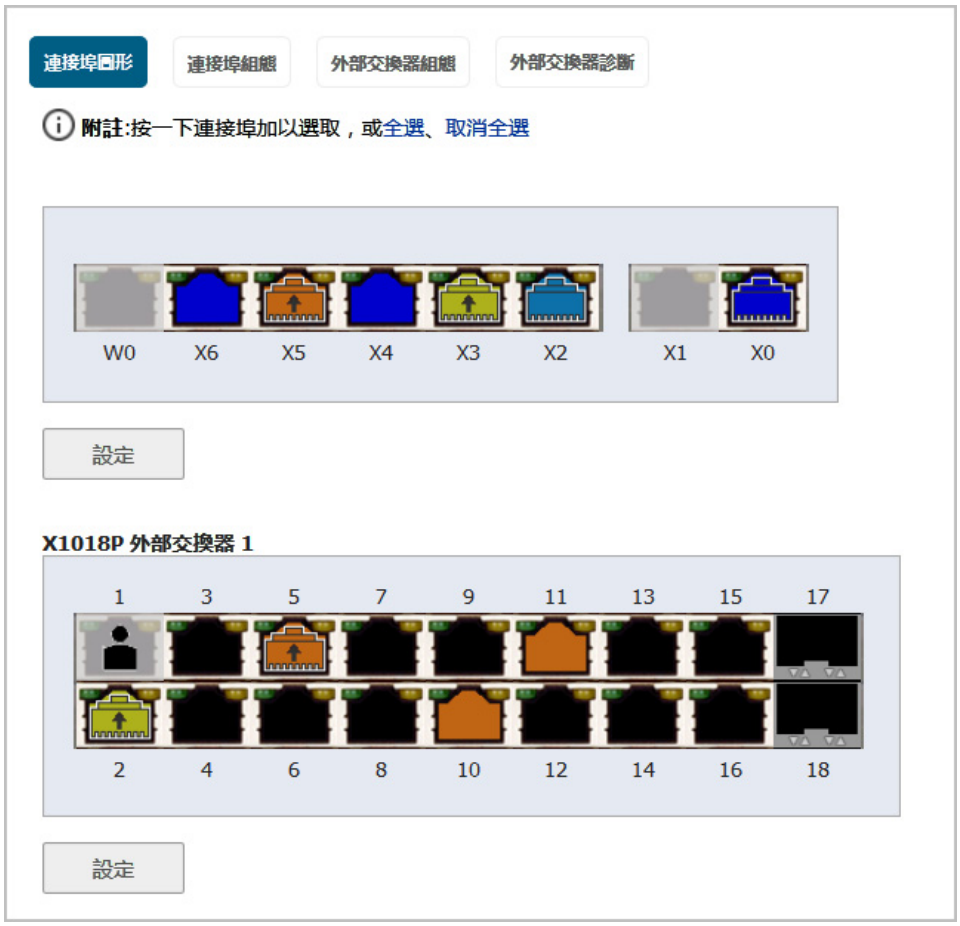
連接埠圖形會顯示安全設備的 PortShield 介面 (連接埠)。大型圖形代表安全設備的介面。介面的顏色代碼反應其設定：

介面設定的顏色代碼

此顏色	指定此類型的介面
黑色	未指派，即不屬於 PortShield 群組
黃色	已選擇要進行設定
相同顏色（黑色、黃色或灰色除外）	PortShield 群組的連接埠，主介面的顏色周圍有白色的輪廓
灰色	無法指派，即無法將其新增到 PortShield 群組
有人員圖形的灰色介面	交換器 MGMT
任何具有向上箭頭者（黑色、黃色或灰色除外）	上行連結

每個連接埠圖形標籤為其相關連接埠名稱：X0 - X*n*。選擇一個或多個介面後，可以按照第 314 頁「設定 PortShield 群組」的說明進行設定。

設定延伸交換器時



佈建一部或多部延伸交換器時，**連接埠圖形**會顯示安全設備和交換器的 PortShield 介面 (連接埠):

- 第一個圖形顯示了安全設備的連接埠，且並未加上標記。
- 下一個圖形顯示第一個外部交換器，外部交換器 1 的連接埠，其標記為 ***SwitchModel* 外部交換器 1**，例如 X1018P 外部交換器 1。
- 如果佈建更多外部交換器，後續圖形以其 ID 順序顯示其他外部交換器的連接埠，也就是外部交換器 2、外部交換器 3 和外部交換器 4。

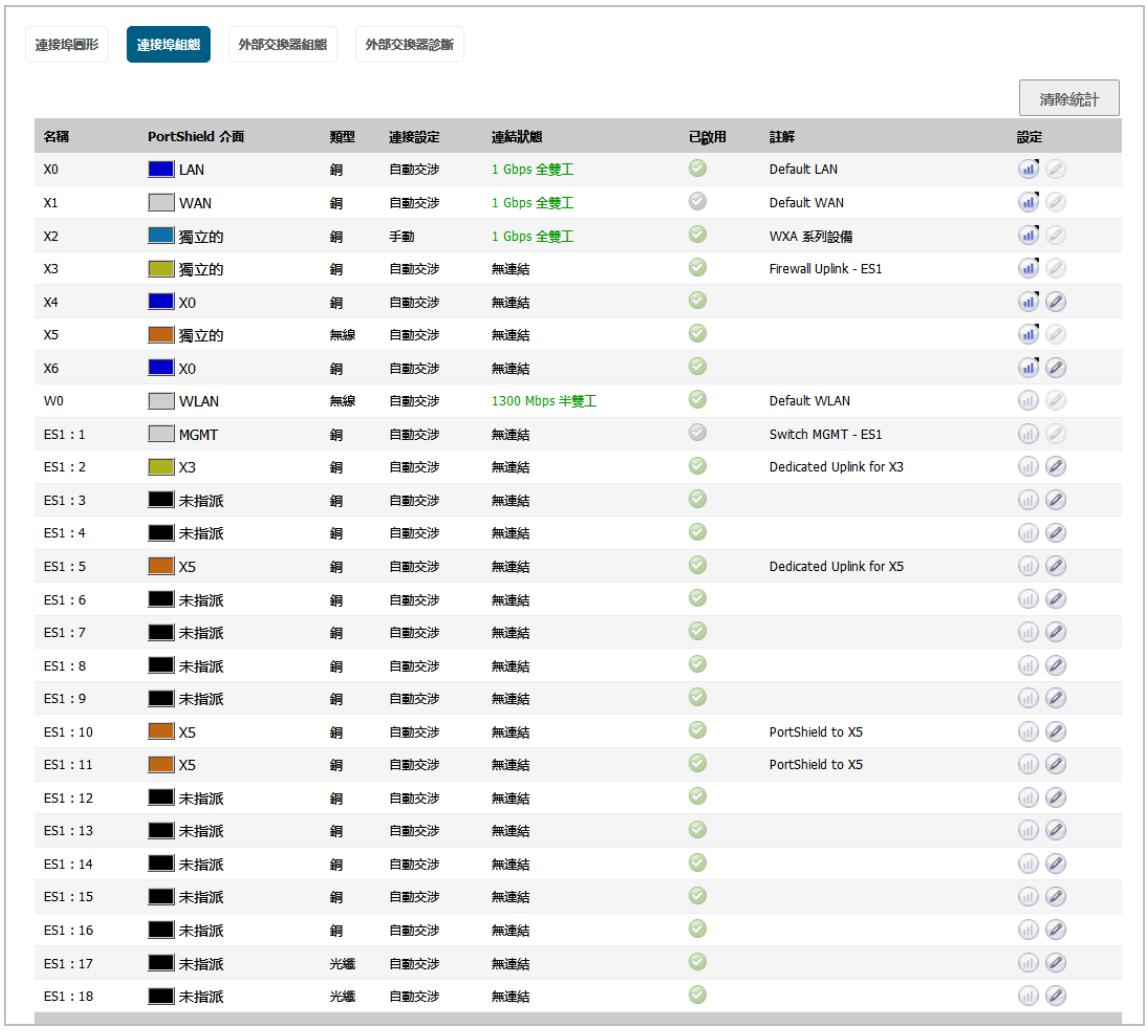
外部介面的顏色代碼與安全設備的顏色代碼相同；請參閱介面設定的顏色代碼表格。

透過連接埠設定標籤查看 PortShield 介面狀態並進行編輯

沒有延伸交換器

名稱	PortShield 介面	類型	連接設定	連結狀態	已啟用	註解	設定
X0	LAN	銅	自動交涉	無連結	✓	Default LAN	
X1	WAN	銅	自動交涉	1 Gbps 全雙工	✓	Default WAN	
X2	獨立的	銅	自動交涉	1 Gbps 全雙工	✓		
X3	未指派	銅	自動交涉	1 Gbps 全雙工	✓		
X4	未指派	銅	自動交涉	無連結	✓		
X5	未指派	銅	自動交涉	無連結	✓		
X6	未指派	銅	自動交涉	無連結	✓		

含有延伸交換器



名稱	PortShield 介面	類型	連接設定	連結狀態	已啟用	註解	設定
X0	LAN	銅	自動交涉	1 Gbps 全雙工	✓	Default LAN	
X1	WAN	銅	自動交涉	1 Gbps 全雙工	✓	Default WAN	
X2	獨立的	銅	手動	1 Gbps 全雙工	✓	WXA 系列設備	
X3	獨立的	銅	自動交涉	無連結	✓	Firewall Uplink - ES1	
X4	X0	銅	自動交涉	無連結	✓		
X5	獨立的	無線	自動交涉	無連結	✓		
X6	X0	銅	自動交涉	無連結	✓		
W0	WLAN	無線	自動交涉	1300 Mbps 半雙工	✓	Default WLAN	
ES1 : 1	MGMT	銅	自動交涉	無連結	✓	Switch MGMT - ES1	
ES1 : 2	X3	銅	自動交涉	無連結	✓	Dedicated Uplink for X3	
ES1 : 3	未指派	銅	自動交涉	無連結	✓		
ES1 : 4	未指派	銅	自動交涉	無連結	✓		
ES1 : 5	X5	銅	自動交涉	無連結	✓	Dedicated Uplink for X5	
ES1 : 6	未指派	銅	自動交涉	無連結	✓		
ES1 : 7	未指派	銅	自動交涉	無連結	✓		
ES1 : 8	未指派	銅	自動交涉	無連結	✓		
ES1 : 9	未指派	銅	自動交涉	無連結	✓		
ES1 : 10	X5	銅	自動交涉	無連結	✓	PortShield to X5	
ES1 : 11	X5	銅	自動交涉	無連結	✓	PortShield to X5	
ES1 : 12	未指派	銅	自動交涉	無連結	✓		
ES1 : 13	未指派	銅	自動交涉	無連結	✓		
ES1 : 14	未指派	銅	自動交涉	無連結	✓		
ES1 : 15	未指派	銅	自動交涉	無連結	✓		
ES1 : 16	未指派	銅	自動交涉	無連結	✓		
ES1 : 17	未指派	光纖	自動交涉	無連結	✓		
ES1 : 18	未指派	光纖	自動交涉	無連結	✓		

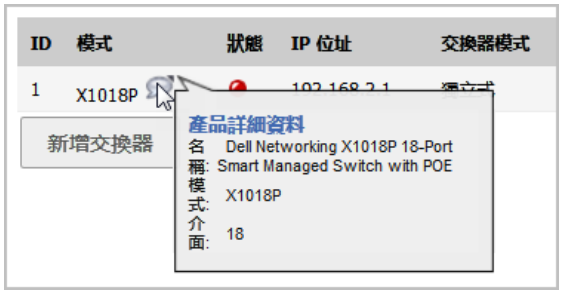
連接埠組態包含一個表格，其中會列出 PortShield 介面的相關資訊:

名稱	與 PortShield 介面介面相關的連接埠名稱，例如 X0 或 X15。任何外部交換器的連接埠會以格式 **ESs:*n*** 顯示，其中 ***s*** 是交換器 ID，而 ***n*** 是連接埠號碼。
PortShield 介面	代表 PortShield 介面指派的顏色代碼圖形以及介面所屬的 PortShield 群組。這個圖形是**連接埠圖形**上大型圖形的縮小版。
類型	連接埠類型： • **銅** • **無線**
連結設定	連結速度： • **自動交涉** • **1000 Mbps - 全雙工** • **100 Mbps - 全雙工** • **100 Mbps - 半雙工** • **10 Mbps - 全雙工** • **10 Mbps - 半雙工**
連結狀態	顯示： • 目前的連結速度為綠色，例如 **1000 Mbps - 全雙工**。 • **無連結**。
已啟用	**已啟用**圖示意義如下: • 綠色，如果啟用介面。 • 灰色，如果停用介面。
註解	設定介面後輸入的任何註解。
設定	包含兩個圖示： • **統計資料** - 按一下此圖示後，將顯示包含介面統計資料的快顯摘要：  **附註：**如要清除所有統計資料，請按一下**網路 | PortShield 群組 > 連接埠設定**頂顛端的**清除統計資料**。 • **編輯** - 按一下此圖示後，將顯示**編輯交換器連接埠**對話方塊。如需此對話方塊的更多資訊，請參見第 315 頁「在網路 | PortShield 群組上設定 PortShield 介面」中的步驟。

檢視和管理外部交換器設定

附註：如果尚未佈建外部交換器，此表會顯示**無項目**。

ID	外部交換器的 ID 編號：**1**、**2**、**3** 或 **4**。
模式	外部交換器的型號。本欄也包含每個交換器的**註解**圖示，用於顯示內含產品明細的快顯摘要。
狀態	交換器的狀態：綠色的**啟用**圖示表示交換器正常、可用。 **附註：**當延伸交換器電源已經關閉然後安全設備才重新啟動 (重新開機) 時，最長需要 5 分鐘時間，之後安全設備才會探索延伸交換器並將交換器的**狀態**報告為已啟動且可使用。
IP 位址	延伸交換器的 IP 位址。
交換器模式	交換器的模式，例如**獨立式**。
交換器管理	用於管理流量的交換器連接埠。
防火牆上行連結	設定為安全設備上行連結的安全設備連接埠。如果沒有任何設定為安全設備上行連結的安全設備連接埠，則此欄會顯示**無**。
交換器上行連結	設定為交換器上行連結的延伸交換器連接埠。如果未作為交換器上行連結設定任何交換器連接埠，此列將顯示**無**。
父級交換器 ID	菊花式鏈結交換器的父級交換器 ID 如果沒有任何設定為父級交換器的交換器連接埠，則此欄會顯示**無**。
父級交換器上行連結	設定為交換器上行連結的菊花式鏈結父級交換器連接埠。如果沒有任何設定為父級交換器上行連結的交換器連接埠，則此欄會顯示**無**。
設定	包含： • **編輯**圖示 - 按一下可顯示**編輯外部交換器**對話方塊。 • **刪除**圖示 - 按一下可刪除交換器項目。



外部交換器組態會針對安全設備上佈署的外部交換器提供相關資訊，並可讓您管理交換器。您也可以設定或刪除延伸交換器。若要設定延伸交換器，請參閱第 314 頁「設定 PortShield 群組」；若要刪除延伸交換器，請參閱 *SonicWall X-系列解決方案部署指南*。

監控外部交換器診斷並管理韌體

附註：如果尚未佈建外部交換器，表格會顯示**無項目**。

外部交換器診斷功能的用途如下:

- 監控外部交換器的統計資訊
- 上載韌體映像和/或啟動映像
- 重新啟動延伸交換器

主題：

變更顯示

外部交換器診斷功能一次只能顯示一部交換器的統計資料和其他資訊。預設情況下，會顯示外部交換器 1 **(ES1)** 的資料。當您有兩個或以上的外部交換器時，如需不同顯示外部交換器的資料，請從**交換器名稱**中選擇 **ES2**、**ES3** 或 **ES4**。

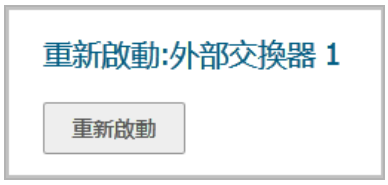
監控統計資訊

統計資料表顯示所有統計資料的流水記錄。如需重新收集統計資料，請按一下**清除**即可重新啟動計數器。

名稱	連接埠名稱，1 - *n*。
狀態	連接埠為**上行**或**下行**。
接收單點傳播封包	從此連接埠接收的單點傳送封包數。
Rx 多點傳播封包	從此連接埠接收的多點傳送封包數。
Rx 廣播封包	從此連接埠接收的廣播封包數。
接收位元組	從此連接埠接收的位元組數。
Rx 錯誤	從此連接埠接收的錯誤封包數。
傳送單點傳播封包	從此連接埠傳送的單點傳送封包數。
Tx 多點傳播封包	從此連接埠傳送的多點傳送封包數。
Tx 廣播封包	從此連接埠傳送的廣播封包數。
傳送位元組	從此連接埠傳送的位元組數。
FCS 錯誤	從此連接埠接收具有 FCS（框架校驗序列）錯誤的封包數。
單一衝突框架	從此連接埠偵測到的框架衝突數。
延遲衝突	在此連接埠傳送上一框架位元後偵測到的框架衝突數。
過度衝突	偵測到超出此連接埠中重試次數的框架衝突數。
內部 MAC 傳輸錯誤	在此連接埠上偵測到的非衝突傳送錯誤數。
超大封包	大於連接埠預期的已接收封包數。

Rx 暫停框架數	通過此連接埠接收的暫停框架數。
Tx 暫停框架數	通過此連接埠傳送的暫停框架數。

重新啟動外部交換器



重要：延伸交換器電源關閉後，安全設備重新啟動 (重開機) 時，安全設備最長可能需要 5 分鐘的時間才會找到延伸交換器，並回報交換器的**狀態 (已連線)**。

重新啟動外部交換器的步驟如下：

1 導覽到**管理 | 系統安裝 | 網路 | PortShield 群組**。

2 按一下**外部交換器診斷**。

3 從**交換器名稱**中選擇要重新啟動的外部交換器。

4 捲動至**重新啟動： 外部交換器**部分。

5 按一下**重新啟動**按鈕。

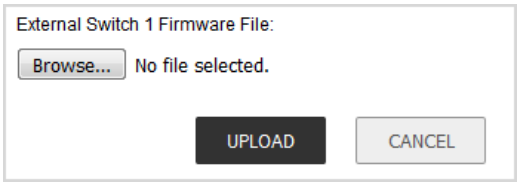
管理外部交換器韌體

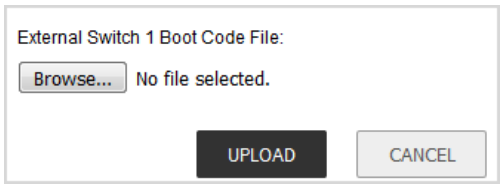
韌體管理： 外部交換器表顯示外部交換器的韌體和開機代碼資訊：

類型	**韌體**或**開機代碼**。
版本	外部交換器上韌體或開機代碼版本。
建立日期	韌體或開機代碼的建立日期。
建立時間	韌體或開機代碼的建立時間。
上載	**上傳**圖示；用於 • **韌體**，顯示**上傳外部交換器韌體**對話方塊: • **開機代碼**，顯示**上傳外部交換器開機代碼**對話方塊:

上載韌體或開機代碼的步驟如下：

1 按一下**上載韌體**或**開機代碼**。顯示**上傳外部交換器韌體**或**上傳外部交換器開機代碼**對話方塊。





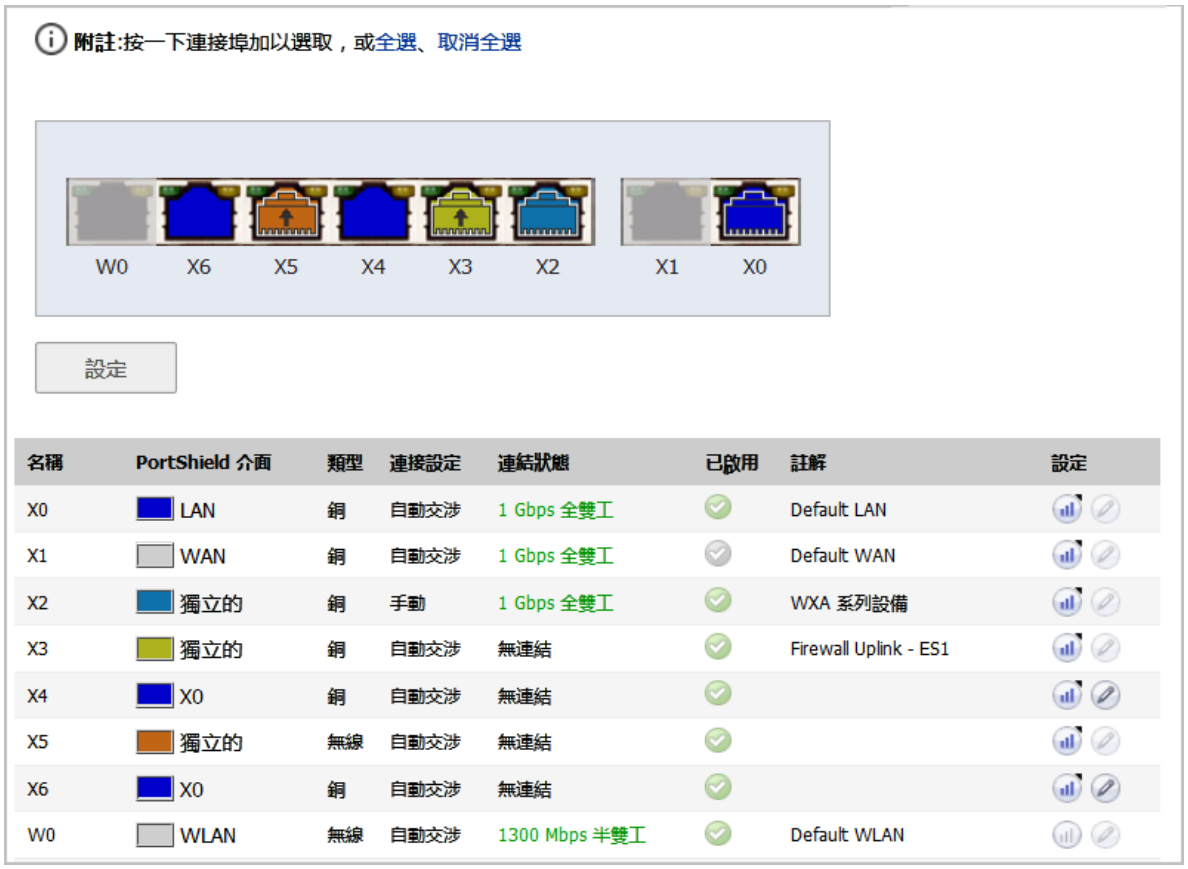
2 按一下**瀏覽**。隨即顯示**檔案上載**對話方塊。

3 選擇此檔案。

4 按一下**上載**。

管理 SOHO W 防火牆上的連接埠

SOHO W 安全設備的**網路 | PortShield 群組**頁面外觀有所不同。這個頁面會一併提供**連接埠圖形** (請參閱第 306 頁「檢視連接埠圖形上的介面 (連接埠)」) 和**連接埠組態** (第 308 頁「透過連接埠設定標籤查看 PortShield 介面狀態並進行編輯」) 資訊。



名稱	PortShield 介面	類型	連接設定	連結狀態	已啟用	註解	設定
X0	LAN	銅	自動交涉	1 Gbps 全雙工		Default LAN	
X1	WAN	銅	自動交涉	1 Gbps 全雙工		Default WAN	
X2	獨立的	銅	手動	1 Gbps 全雙工		WXA 系列設備	
X3	獨立的	銅	自動交涉	無連結		Firewall Uplink - ES1	
X4	X0	銅	自動交涉	無連結			
X5	獨立的	無線	自動交涉	無連結			
X6	X0	銅	自動交涉	無連結			
W0	WLAN	無線	自動交涉	1300 Mbps 半雙工		Default WLAN	

您可以按照第 314 頁「設定 PortShield 群組」中的說明設定安全設備介面。

設定 PortShield 群組

您可以透過 SonicOS 管理介面中的幾個不同頁面來設定 PortShield 群組:

- 第 314 頁「在網路 | 介面上設定 PortShield 介面」
- 第 314 頁「利用 PortShield 介面指南設定 PortShield 介面 (僅限 TZ 系列和 SOHO W 防火牆)」
- 第 315 頁「在網路 | PortShield 群組上設定 PortShield 介面」
- 第 317 頁「透過連接埠圖形設定外部交換器 PortShield 群組」

在網路 | 介面上設定 PortShield 介面

重要：如需將連接埠用作介面，則必須將其設定為一個 IP 位址。否則，**PortShield 介面**中就不會列出這個連接埠。

若要設定 PortShield 介面:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 在**介面**設定表中，按一下想要設定的介面的**設定**圖示。顯示**編輯介面**對話方塊。

3 在**區域**中，選擇一個介面對應的目標區域類型選項。將顯示更多選項。

附註：PortShield 介面僅可新增至**可信**、**公用**和**無線**區域。

4 在**模式/ IP 指派**下拉功能表中，選擇 **PortShield 交換器模式**。這些選項將再次發生變更。

5 在 **PortShield 至**中，選取這個連接埠的目標對應介面。只會顯示與您選擇的區域符合的連接埠。

6 按一下**確定**。

利用 PortShield 介面指南設定 PortShield 介面 (僅限 TZ 系列和 SOHO W 防火牆)

您可以按照 *SonicOS 快速設定指南*中的說明，利用 PortShield 介面指南設定 PortShield 介面。您可以透過下列方式取得 PortShield 介面指南:

- 在任何管理介面頁面中按一下**快速設定指南**。**設定指南**隨即顯示；請選取 **PortShield 介面指南**。
- 在 TZ 系列或 SOHO W 安全設備的**管理 | 系統安裝 | 網路 | 介面**頁面上，按一下 **PORTSHIELD 精靈**即可顯示 **PortShield 介面指南**。

在網路 | PortShield 群組上設定 PortShield 介面

連接埠圖形會以圖形方式呈現目前的 PortShield 介面設定。如需圖形顯示說明，請參閱第 306 頁「檢視連接埠圖形上的介面 (連接埠)」。

可按一下要分組的連接埠，使用圖形 **PortShield 群組**介面手動分組多個連接埠。通過群組連接埠，它們可以共用共同的網路子網路以及共同的區域設定。

附註：必須在群組為 PortShield 之前對介面進行設定。

若要設定 PortShield 群組:

1 在連接埠圖中，選擇要設定為 PortShield 群組的介面。這些介面將變成黃色。

2 按一下**設定**。**編輯交換器連接埠**對話方塊即會顯示。

附註：這個連接埠的介面名稱會變為灰色，且無法更動。

3 在**啟用連接埠**中，視需求選擇啟用或停用介面。預設為**已啟用**。

4 在 **PortShield 介面**中，選擇要指派哪一個介面作為這個 PortShield 介面的主介面。系統預設為**未指派**。

附註：可以對外部交換器連接埠停用 PortShield 選項。

5 在**連線速度**中，選擇這些介面的連線速度:

- **自動交涉**（預設）
- **1000 Mbps - 全雙工**
- **100 Mbps - 全雙工**
- **100 Mbps - 半雙工**
- **10 Mbps - 全雙工**
- **10 Mbps - 半雙工**

6 按一下**確定**。

透過連接埠圖形設定外部交換器 PortShield 群組

重要：延伸交換器電源關閉後，安全設備重新啟動 (重開機) 時，安全設備最長可能需要 5 分鐘的時間才會找到延伸交換器，並回報交換器的**狀態 (已連線)**。

當設定 PortShield 群組中的延伸交換器時，設定最長需要 5 分鐘時間才會顯示在**網路 | PortShield 群組**頁面上。

重要：必須在群組為 PortShield 之前對介面進行設定。

附註：如需瞭解如何設定各種拓撲的 PortShield 群組，請參閱 *SonicWall X-系列解決方案部署指南*。

附註：SOHO W 安全設備不支援延伸交換器。

網路 | PortShield 群組會以圖形方式呈現目前安全設備和延伸 (外部) 交換器上的 PortShield 介面設定。如果有一個外部交換器，則顯示兩個圖示；如果有兩個外部交換器，則顯示三個圖示，以此類推。交換器圖形標有交換器型號和外部交換器 ID：1、2、3、4。

您可以在想要進行分組的連接埠上按一下，然後使用圖形化的 PortShield 群組介面，手動將安全設備和交換器上的連接埠歸類在一起。通過群組連接埠，它們可以共用共同的網路子網路以及共同的區域設定。

若要設定具有外部交換器的 PortShield 群組:

1 遵照第 315 頁「在網路 | PortShield 群組上設定 PortShield 介面」中的程序設定安全設備上的連接埠。

2 在外部交換器的連接埠圖形中，選擇要設定為 PortShield 群組的介面。這些介面將變成黃色。

3 按一下**設定**按鈕。隨即顯示**編輯多重的交換器連接埠**對話方塊。

名稱欄位顯示為灰色，無法進行修改。這個欄位會顯示您所選的安全設備和外部交換器的連接埠名稱 (*n* 為所選連接埠):

- 防火牆連接埠命名為 **X*n***。
- 外部交換器 1 連接埠命名為 **ES1**： ***n***。
- 外部交換器 2 連接埠命名為 **ES2**： ***n***。
- 外部交換器 3 連接埠命名為 **ES3**： ***n***。
- 外部交換器 4 連接埠命名為 **ES4**： ***n***。

4 在**啟用連接埠**中選取下列其中一個選項:

- **已停用**

- **啟用**
- **-儲存目前設定-**（預設）- 預設情況下，會啟用延伸交換器上的所有連接埠。

5 在 **PortShield 介面**中，選擇要指派哪一個介面作為這些 PortShield 介面的主介面:

- **已取消指派**
- 連接埠名稱

  重要：如需將連接埠用作介面，則必須將其設定為一個 IP 位址。否則，**PortShield 介面**中就不會列出這個連接埠。

- **-儲存目前設定-**（預設）

  附註：可以對外部交換器連接埠停用 PortShield 選項。

  此處進行連接埠屏蔽的連接埠將自動設定為存取相應 PortShield VLAN 的 VLAN。

6 在**連線速度**中，選擇這些介面的連線速度:

- **自動交涉**
- **1000 Mbps - 全雙工**
- **100 Mbps - 全雙工**
- **100 Mbps - 半雙工**
- **10 Mbps - 全雙工**
- **10 Mbps - 半雙工**
- **-儲存目前設定-**（預設）- 預設情況下，延伸交換器上所有連接埠的連結速度均設定為**自動交涉**。

7 按一下**確定**。

15

設定容錯移轉和負載平衡

網路 | 容錯移轉與負載平衡

主題：

關於容錯移轉和負載平衡

容錯移轉和負載平衡 (LB)（合稱為 FLB），是一種主動監控 WAN 連接，並在 WAN 介面的故障/恢復上採取相應操作的機制。整體效果是對 WAN 連接故障/恢復的系統範圍內的回應。儘管您只有一個 WAN，但仍能受益，原因是作為一般部分的 FLB 在 WAN 上執行的恢復程式更快（如需使用一個 WAN 進行 FLB 的更多資訊，請參閱知識庫文章，SW13851，*當防火牆上僅使用一個 WAN 時，是否能停用全域負載平衡？*）。本質上，FLB 提供高可用性系統。

對於 FLB，可以支援多個 WAN 成員 (*N*-1，其中 *N* 是硬體平台上的介面總數）。例如：

- 主要 WAN 乙太網路介面
- 替代 WAN #1
- 替代 WAN #2
- 替代 WAN #<*n-1*> ...

重要：即便只有一個 WAN，也推薦始終啟用「負載平衡」。如需更多資訊，請參閱*當防火牆上僅使用一個 WAN 時，是否能停用全域負載平衡？*(SW13851)。

主要 WAN 乙太網路介面的含義與之前的「主要 WAN」概念相同。它是負載平衡群組中級別最高的 WAN 介面。**替代 WAN 乙太網路介面**對應於「次要 WAN」，其級別低於主要 WAN，但高於接下來的兩個可替換的 WAN。其他兩個 WAN 介面 - **替代 WAN #2** 和**替代 WAN #<*n-1*>** 都是新增介面，其中**替代 WAN #<*n-1*>** 在負載平衡組的四個 WAN 成員中級別最低。

容錯移轉與負載平衡的運作方式

主題：

WAN 介面故障

這是偵測到 WAN 介面故障時 FLB 所執行的操作（下行連結、探查失敗或 no-IP 設定）：

1. 正常關閉介面（若已提供，呼叫停止 API；例如，pppoe-stop、dialup-stop）。
2. 觸發停用與故障介面相關聯的路由（不包括標有切勿停用下行連結的路由）。
3. 使用故障介面排清動態 ARP 項目。
4. 將故障介面用作輸出介面，以排清快取項目。
5. 更新 WAN 預設路由，以指向替代 WAN（如果可用）。更新狀態資料（這是恢復程式的一部分）。
   - 也將更新 CASS 等其他應用程式所使用的位址物件。
   - 安全服務依靠此更新實現容錯移轉功能。
6. 通知相關方（VPN、BWM、CASS、DDNS、DNS）。
7. 主動監控故障介面狀態、恢復嘗試，如重新啟動 WAN 連接（呼叫啟動 API（若提供）；例如，pppoe-start、dial-start）。

WAN 介面恢復

這是偵測到 WAN 介面恢復時 FLB 所執行的操作（上行連結、探查成功或 IP 變更）：

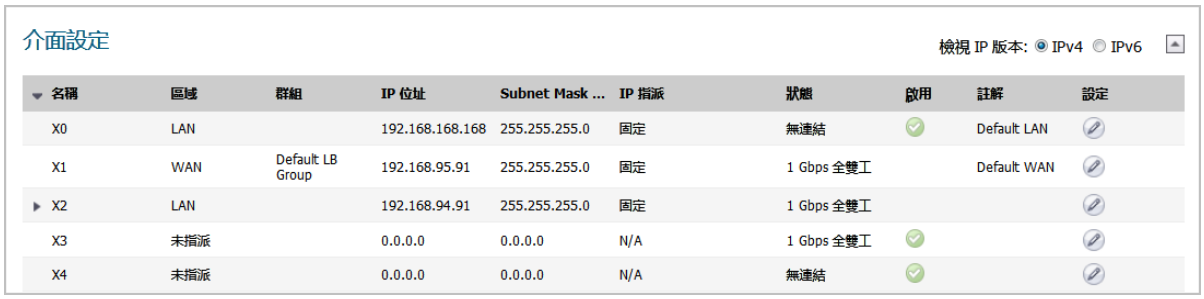
1. 上行連結時，啟動介面連接（呼叫啟動 API（若提供）；例如，pppoe-start、dial-start）。大多數情況下，它將已處於連接狀態，如果未連接，FLB 將嘗試促使其啟動。若偵測到掛起狀態，可執行正常關閉，並重新啟動（基於計時器）。
2. 確認連接後（只要上行連結或探查成功），將觸發啟用與此介面相關聯的路由。
3. 新增 ARP 項目（如需）。
   - 發出主動提供的 ARP 回應（針對介面），以更鄰接裝置。
4. 如果需要，請更新 WAN 預設路由（例如先佔）以使用可用的最佳 WAN。更新狀態資料。
   - 也將更新 CASS 等其他應用程式所使用的位址物件。
   - 安全服務依靠此更新實現容錯移轉功能。
5. 通知相關方（VPN、BWM、CASS、DDNS、DNS）。
6. 繼續監控介面狀態。

多個 WAN (MWAN)

多個 WAN (MWAN) 功能用於設定裝置上除一個介面以外的其他所有介面用於 WAN 網路路由（必須保留其中一個介面設定用於 LAN 區域，以便進行本機管理）。所有 WAN 介面都可以使用 SNWL 全域回應方主機進行探查。

網路介面

管理 | 網路 | 介面允許設定兩個以上的 WAN 介面供路由使用。您或許可以在**網路 | 介面**中設定 WAN 介面，但無法將其納入**網路 | 容錯移轉與負載平衡**。在啟用負載平衡的情況下，只有主要 WAN 乙太網路介面必須作為負載平衡群組的一部分。任何不屬於負載平衡群組的 WAN 介面都不會包括在負載平衡功能中，而只是執行正常的 WAN 路由功能。



附註：負載平衡群組可能包括虛擬 WAN 介面。但在負載平衡群組中使用虛擬 WAN 介面之前，請確保虛擬 WAN 網路同實體 WAN 一樣完全可路由。

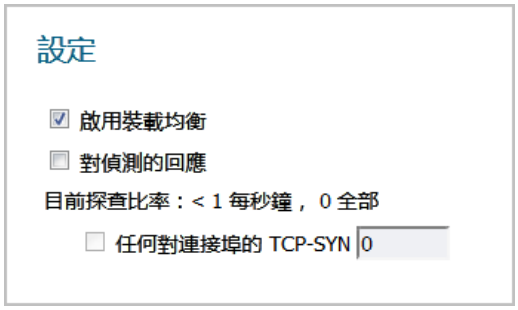
如果需要透過不在 WAN 子網路 IP 位址空間的 WAN 介面到達目的地，那麼此 WAN 介面必須有預設閘道 IP，不管我們是否在 WAN 子網路上透過對等裝置的路由通訊協定接收預設動態路由。

網路 | 容錯移轉與負載平衡

主題：

- 第 322 頁「設定」
- 第 322 頁「群組」
- 第 323 頁「統計」

設定



- **啟用負載平衡** - 必須啟用此選項，使用者才能存取容錯移轉和負載平衡設定的「負載平衡組和負載平衡統計」部分。如果停用此選項，則不提供可設定的容錯移轉和負載平衡選項。預設啟用此選項。

  重要：即便只有一個 WAN，也推薦始終啟用「負載平衡」。如需更多資訊，請參閱*當防火牆上僅使用一個 WAN 時，是否能停用全域負載平衡？*(SW13851)。

- **對偵測的回應** - 啟用此選項時，裝置可回應到達裝置任意介面的探查請求封包。預設情況下未勾選此選項。

  目前的探查速率和總數隨即顯示。

  - **任何對連接埠的 TCP-SYN** - 此選項在啟用**對偵測的回應**選項的情況下可用。勾選此選項時，裝置將僅回應有與設定值相同的封包目的地位址 TCP 連接埠號的 TCP 探查請求封包。預設情況下未勾選此選項。

群組

新增到負載平衡群組的負載平衡成員承擔了指定的「角色」。成員只能承擔以下角色之一：

- **主要** - 每個組只能有一個主要成員。此成員始終出現在成員清單的第一個或最上面的位置。

  附註：儘管可以為群組設定空的成員清單，但只要其中有成員就必須有主要成員。

- **替代** - 可以有一個以上的替代成員，但任何群組都不能只有替代成員。
- **最後的手段**- 只有一個成員可設計為「最後的手段」。只能使用其他群組成員來設定「最後的手段」。

群組中的每個成員都有某個級別。成員按照級別以遞減顯示。級別取決於介面在組成員清單中出現的順序。此順序在決定介面的使用優先順序以及在群組內的優先順序方面有重要作用。因此，一個群組內沒有任何兩個介面有相同的級別；每個介面都有不同的級別。

群組表

- **展開/折疊**圖示 - 按一下可展開或折疊要顯示成員的群組。
- **核取方塊** - 用於選擇群組；不能選擇預設群組。

- **類型** - 容錯移轉類型；僅適用於群組，不適用於成員。
- **IP 位址** - 群組成員的 IP 位址。
- **連結狀態** - 顯示連結為上行連結或下行連結。
- **裝載均衡** - 顯示負載平衡的狀態。
- **主要目標** - 顯示是否在主要目標上執行探查。
- **替代目標** - 顯示是否在替代目標上執行探查。
- **設定** - 顯示**編輯**圖示，對於群組，**刪除**圖示（無法刪除預設組，因此**刪除**圖示顯示為灰色）。
- **註解** - 顯示**註解**圖示，當滑鼠放在此圖示上時，顯示含群組狀態的快顯氣球。

統計

在**顯示統計為**下拉功能表中，選擇想要檢視其統計資訊的負載平衡群組。

負載平衡**統計**表顯示防火牆的以下負載平衡群組統計資訊：

- 介面 -
- 總連接數 -
- 新建連接 -
- 目前比率 -
- 平均比率 -
- 所有單點傳播位元組 -
- 接收單點傳播 -
- Rx 位元組 -
- Tx 單點傳播 -
- Tx 位元組 -
- 傳輸量 (KB/s) -
- 傳輸量 (Kbits/s) -

按一下**統計**表右上角的**清除**按鈕以清除資訊。

設定容錯移轉和負載平衡群組

主題：

一般設定

設定「群組」設定的步驟如下：

1 導覽到**管理 | 網路 | 容錯移轉與負載平衡**。

2 找出您想設定的群組，然後按一下該群組的**設定**圖示。將顯示**編輯 LB 群組**對話方塊。

3 在**名稱**欄位中編輯群組的顯示名稱。預設群組的名稱不能變更，欄位會變成灰色。

4 從**類型**下拉功能表中，選擇負載平衡的類型（或方法）；選項將根據所選類型發生變更：

- **基本容錯移轉** - 在啟用**先佔**核取方塊時，四個 WAN 介面使用「級別」來確定先佔順序。只有較進階別的介面可以先佔主動 WAN 介面。預設情況下已核取此選項。
- **循環配置資源** - 此選項現在用於重新排定 WAN 介面的順序，以便進行循環配置資源選擇。預設排序為：
  - 主要 WAN
  - 替代 WAN #1
  - 替代 WAN #2

- 替代 WAN #3

循環配置資源隨即返回主要 WAN 以繼續排序。

- **溢出** - 對主要 WAN 套用頻寬閾值。在超過此閾值之後，新的流量將按照循環配置資源指派至替代 WAN。如果主要 WAN 頻寬降至低於設定的閾值，循環配置資源將會停止，新的傳出流量再次只透過主要 WAN 向外傳送。

  附註：現有流量仍將與替代 WAN 保持關聯（因為這些流量已進入快取），直至其正常逾時為止。

- **比率** - 為負載平衡群組中的每個 WAN 設定百分比。為避免與設定錯誤相關的問題，請確保這些百分比對應所指示的正確 WAN 介面。

5 根據您從**類型**下拉功能表中選擇的選項，將顯示以下選項之一：

類型選擇	選項
基本容錯移轉	**當可能的話，先佔並且自動恢復到優先介面** 選擇以使級別確定先佔順序。預設選擇此選項。
溢出	**在循環配置資源方式下，當主要介面的*頻寬*超過 Kbit/s 時，新的流量將流向可替代的群組成員** 在此欄位中指定主要介面的頻寬。如果超過此值，那麼將根據在**已選的**欄中列出的順序把新的流量傳送到可替代的群組成員。 預設值為 **0**。
循環配置資源、溢出和**比率**	**使用來源和目的地 IP 位址繫結** 此選項在使用 HTTP/HTTPS 重新導向或在類似情況中時特別有用。例如，連接 A 和連接 B 需要在同一個 WAN 介面上，連接 A 中的來源和目的地 IP 位址與連接 B 中的來源和目的地 IP 位址相同，但正在使用不同的服務。在這種情況中，需要來源和目的地 IP 位址繫結才能在相同 WAN 介面上保有這兩個連線，如此交易才不會失敗。 預設情況下未勾選此選項。

6 在**群組成員**中新增、刪除及對成員介面排序： **選擇此處：/已選的**清單。在**已選的**清單中如何使用所選的成員取決於下列所選的**類型**：

- **基本容錯移轉：介面排序:**
- **循環配置資源：介面集區：**
- **溢出：主要的/可取代的集區：**
- **比率：介面配送：**

7 可透過選擇**群組成員：**欄中顯示的介面，然後按一下**新增>>**按鈕來新增成員。

8 您可以按如下步驟對**已選的**欄中的項目進行排序：

a 選擇一個項目。

b 按一下**上/下**按鈕。

9 如果選擇了**比率**，而非對項目進行排序，那麼可以指定每個介面的頻寬比率。請參閱第 326 頁「將頻寬設定為比率」。

重要：為避免與設定錯誤相關的問題，請確保這些百分比對應所指示的正確 WAN 介面。

10 在百分比 **(%)** 欄位中輸入一個要指派至介面的頻寬百分比。所有介面的總頻寬應最多新增 100%。隨即顯示總指派頻寬百分比。

11 可以透過按一下**修改比率**按鈕來修改比率，或透過按一下**自動調整**按鈕使比率自動調整。

12 您可以按如下步驟從**已選的**欄中刪除成員：

a 選擇顯示介面。

b 按一下**<<移除**按鈕。

附註：位於清單頂部的介面為主要 WAN 介面。

「介面級別」並未指定將在各個成員介面上執行的操作。所執行的操作將由「群組類型」指定。

13 或輸入下面的設定：

- **最後的備份** - 在此設定中項目是作為「最後手段」的介面，即，它是僅在**已選的：**組中所有其它介面都無法使用或無法使用時才使用的介面。若要指定「最後的備份」介面，在「群組成員」清單中選擇一個項目，然後按一下雙右箭頭按鈕。若要移除**最後的備份**介面，按一下雙左箭頭按鈕。

14 按一下**確定**。

將頻寬設定為比率

如果已選擇**比率**，**新增 >>**按鈕將替代為百分比 **(%)** 欄位且**雙右箭頭**按鈕和**上/下箭頭**按鈕將替換為**自動調整**按鈕。

輸入一個要指派至介面的頻寬百分比。隨即顯示總指派頻寬百分比。

重要：為避免與設定錯誤相關的問題，請確保這些百分比對應所指示的正確 WAN 介面。

若選擇了多個介面，則可：

- 按一下**自動調整**按鈕以在介面之間平均指派頻寬。
- 輸入一個要指派至介面的頻寬百分比。

修改介面頻寬百分比的步驟如下：

1 在**已選的**欄中選擇介面。

2 按一下**變更比率**按鈕。

3 在百分比 **(%)** 欄位中輸入新的百分比。

4 再次按一下**變更比率**按鈕。將更新指派的頻寬和總頻寬百分比。

探查設定

啟用邏輯探查時，可向遠端探查目標傳送測試封包，以驗證 WAN 路徑的可用性。系統新增了一個選項，用於透過以下額外的 WAN 介面進行探查：替代 WAN #3 和替代 WAN #4。

附註：用於替代 WAN 的 VLAN 不支援 QoS 或 VPN 終止。

若要設定特定群組的探查選項：

1 導覽到**管理 | 。網路 | 容錯移轉與負載平衡**

2 找出您想設定的群組，然後按一下該群組的**設定**圖示。將顯示**編輯 LB 群組**對話方塊。

3 按一下**探查**。

4 修改以下設定：

- **檢查介面的時間間隔：** *n* **秒** - 健康狀況檢查的時間間隔（以秒為單位）。預設值為 **5** 秒。
- **使介面在：** *n* **次遺失的間隔後無效** - 健康狀況檢查失敗的次數，超過此次數後介面將設定為「容錯移轉」。預設值為 **6** 秒。
- **使介面在：** *n* **次成功的間隔後有效** - 健康狀況檢查成功的次數，超過此次數後介面將設定為「可用」。預設值為 **3** 秒。
- **在此組中的所有介面上探查 responder.global.sonicwall.com** - 啟用此核取方塊可自動在此組中的所有介面上設定邏輯/探查監控。啟用時，使用目的地探查目標位址 `204.212.170.23:50000` 將 TCP 探查封包傳送至對 SNWL TCP 封包 `responder.global.sonicwall.com` 做出回應的全域 SNWL 主機。勾選此核取方塊後，剩餘的探查設定將會自動啟用內建設定。相同的探查將套用於全部四個 WAN 乙太網路介面。

  附註：撥號 WAN 探查設定也會恢復為預設的內建設定。

5 按一下**確定**。

指定群組成員的探查設定

若要指定「群組成員」探查設定:

1 導覽到**管理 | 。網路 | 容錯移轉與負載平衡**

2 找出您想設定的群組成員，然後按一下該群組的**設定**圖示。隨即顯示**探查設定**對話方塊。

3 選擇需完成的探查類型:

- **僅實體監控**（預設；所有其他選項顯示為灰色）。移至步驟 9。
- **邏輯的/探查監控啟用** - 所有其他選項可用。

4 在**邏輯/探查監控**中選擇探查成功的情況:

- **當主要目標或者替代目標回應時探查成功。**
- **當主要目標和替代目標回應時探查成功。**
- **當主要目標回應時探查成功。**
- **總是成功（無探查）**。- 預設；所有其他選項顯示為灰色。移至步驟 9。

5 在**主要目標**中，選取:

- **Ping (ICMP)**
- **TCP**（預設）

a 在**主要目標主機**欄位中，輸入主機名稱。預設值為 **responder.global.sonicwall.com**。

b 在**主要目標連接埠**欄位中，輸入應用程式連接埠。預設為 **50000**。

6 如果選取「當主要目標回應時探查成功」，請移至步驟 8。

7 從**替代目標**下拉功能表中，選擇：

附註：替代目標選項僅在針對啟用**邏輯/探查監控**選擇**當主要目標或者替代目標回應時探查成功**或**當主要目標和替代目標回應時探查成功**可用。

- **Ping (ICMP)**
- **TCP**（預設）

a 在**替代目標主機**欄位中，輸入主機名稱。預設值為 **responder.global.sonicwall.com**。

b 在**替代目標連接埠**欄位中，輸入應用程式連接埠。預設為 **50000**。

8 在**預設目標 IP** 欄位中，輸入預設閘道的 IP 位址。

附註：若針對**邏輯的/探查監控啟用**選擇**總是成功（無探查）**，則此選項將顯示為灰色。IP 位址 `0.0.0.0` 或 DNS 反解析失敗會使用設定的預設目的地 IP 。

9 按一下**確定**。

16

設定網路區域

關於區域

區域是一個或多個用於進行管理工作（例如定義和應用存取規則）的介面的邏輯群組，此過程相比嚴格遵守實體介面方案而言更加簡單和直觀。區域式的安全性提供強大而靈活的方法來管理內部和外部網路區段，使得管理員能夠隔離關鍵性內部網路資源並防止其受到未經核准的存取或攻擊。

網路安全區域只是使用易記且使用者可設定的名稱對一個或多個介面進行分組，並在從一個區域向另一個區域傳送流量時套用安全規則的一種邏輯方法。安全區域為防火牆提供一重額外的、更具靈活性的安全層。使用區域式的安全性，管理員可對相似的介面進行分組，並對它們套用相同的原則，無需為每個介面設定同一個原則。如需介面設定的更多資訊，請參見第 230 頁「網路 | 介面」。

SonicOS 區域可用於將安全原則套用到網路內部。這可讓您透過安全原則將網路資源分為不同的區域，以及允許或限制這些區域間的流量。藉由這種方法可以嚴格控制對工資單伺服器或工程代碼伺服器等關鍵性內部資源的存取。

透過區域還可以完全公開 NAT 表，供您針對從某個區域流向另一個區域的流量，控制其來源位址和目的地位址，藉此控管介面之間的流量。這意味著既可以在內部，也可以在 VPN 通道之間套用 NAT，而這正是使用者長期以來期盼實現的功能。由於現在可以在邏輯上將 VPN 群組到自己的 VPN 區域內，因此防火牆還可以透過 NAT 原則和區域原則來驅動 VPN 流量。

主題：

- 第 331 頁「安全類型」
- 第 331 頁「允許介面信任」
- 第 331 頁「對區域啟用 SonicWall 安全服務」

區域的工作方式

以下是針對安全區域工作方式提供的一種形象化的表示方法：想像有一座新建的大型建築物，裡面有多個房間，以及一群不瞭解建築物內部通道的新員工。此建築物擁有一個或多個出口，這些出口可視為 WAN 介面。建築物內的房間擁有一扇或多扇門，這些門可視為介面。這些房間可視為區域，每個裡面都有一定數量的員工。將員工分類並指定到建築物內的單獨房間。每個房間裡需要前往其他房間或離開建築物的員工都必須與每個房間出口處的看門人交談。此看門人便是區域間/區域內的安全原則，其職責是查詢一份名單，確認此員工是否已獲准進入另一個房間或離開此建築物。如果此員工已獲得許可（即安全原則允許），則可以通過門（介面）離開房間。

進入走廊時，員工需要詢問走廊監視員，以便找到房間或建築物出口所在的位置。此走廊監視員負責提供路由過程，因為他/她知道所有房間的位置，以及進出此建築物的路徑。此監視員還知道所有遠端辦公室的位址，後者可視為 VPN。如果建築物擁有多個進口/出口（WAN 介面），則走廊監視員還可以指示員工使用次要進口/出口，具體取決於員工所收到的指令（即僅在緊急情況下，或者需要指派進口/出口的進出流量時）。此功能可視為 WAN 負載平衡。

建築物內的房間有時可能有多扇門，而且房間內有時會有多群彼此不認識的員工。在本範例中，一群員工僅使用其中一扇門，而另一群員工則使用另一扇門，儘管他們都在同一個房間內。由於他們彼此不認識，為了與另一群員工中的某個人對話，使用者必須要求看門人（安全原則）指出另一群員工裡面的哪一位是他們希望談話的物件。看門人可以選擇不讓房間裡的一群員工與另一群員工對話。以上範例是區域具有多個繫結的介面並且不允許區域內流量的情況。

有時，員工可能希望拜訪遠端辦公室，遠端辦公室的員工也有可能進入此建築物內拜訪特定房間裡的員工。這類情況便是 VPN 通道。走廊和門口監視員將會核實是否允許此類存取，並允許流量通過。看門人還可以選擇強制員工在進入其他房間、離開房間或進入其他遠端辦公室之前換上某種服飾。這樣可以隱藏員工的真實身分，將員工偽裝成其他人。此過程可視為 NAT 原則。

預先定義區域

防火牆上的預先定義區域取決於裝置。SonicWall 安全裝置上預先定義的安全區域無法修改:

這個區域	具有此功能
DMZ	一般用於可公開存取的伺服器，並且一到四個介面，具體取決於您的網路設計。
LAN	可包含多個介面，具體取決於您的網路設計。即使每個介面所連接的網路子網路各有不同，但整合在一起時也可以作為單個實體進行管理。
MGMT	用於裝置管理並僅包含 MGMT 介面。還可以啟用其他區域中的介面進行 SonicOS 管理，但 MGMT 區域/介面僅為管理用途提高了單獨區域的安全性。
多點傳送	提供 IP 多點傳送支援，IP 多點傳送是一種從單一來源同時向多個主機傳送封包的方法。
SSLVPN	用於使用 SonicWall NetExtender 用戶端的安全遠端存取功能。
VPN	用於簡化安全遠端連線的虛擬區域。
WLAN	支援 SonicWall SonicPoint 和 SonicWave。指派到 Opt 連接埠時，會執行 SonicPoint 強制措施，自動捨棄所有從非 SonicPoint 裝置收到的封包。WLAN 區域支援下列通訊協定: • 發現通訊協定 (SDP)，可自動輪詢和識別已連接的 SonicPoint 和 SonicWave

這個區域	具有此功能
	• SonicWall 簡單佈建通訊協定，可使用設定檔設定 SonicPoint 和 SonicWave • 無線和來賓服務設定
WAN：	可包含多個介面。如果您正在使用安全設備的 WAN 容錯移轉功能，則必須在 WAN 區域內加入第二個網際網路介面。

附註：即使將介面群組到一個安全區域內，也不會妨礙您對區域內的單個介面定址。

安全類型

每個區域都有一種安全類型，它定義了提供給此區域的信任級別。

受信任	提供最高的信任級別，也就是說，如果流量來自受信任的區域，則系統只會套用最基本的監督機制。受信任的安全可以視為處於安全裝置的 LAN（受防護）端。LAN 區域始終是受信任的。
管理	MGMT 區域和 MGMT 介面所獨有，同時也提供最高的信任級別。
加密	專供 VPN 和 SSLVPN 區域使用。傳入和傳出加密區域的所有流量都已經過加密。
無線	適用於 WLAN 區域或任何僅連接至由 SonicWall SonicPoint 和 SonicWave 裝置所組成的網路的區域。無線安全類型是專為配合 SonicPoint 和 SonicWave 使用而精心設計。在無線區域置入介面後，該介面就會啟用 SDP (SonicWall 發現通訊協定) 和 SSPP (SonicWall 簡單佈建通訊協定)，能夠自動發現及佈建 SonicPoint 和 SonicWave。只有通過 SonicPoint 或 SonicWave 的流量可通過無線區域；所有其他流量都會遭到捨棄。
公用	提供的信任級別比不受信任的區域高，但不及受信任的區域。公用區域可視為在安全設備的 LAN（受防護）端與 WAN（未受防護）端之間的安全區域。例如，DMZ 便是公用區域，因為它的流量會流向 LAN 和 WAN。根據預設，系統會拒絕從 DMZ 流向 LAN 的流量，但允許 LAN 流向 ANY 的流量。也就是說，只有源於 LAN 的連線才能擁有 DMZ 和 LAN 間的流量。DMZ 預設僅擁有 WAN 的存取權，而沒有 LAN 的存取權。
不受信任	信任級別最低。由 WAN 和虛擬多點傳送區域使用。不受信任的區域可視為該區域位於 安全設備的 WAN (未受保護) 端。根據預設，如果沒有明定規則，來自不受信任的區域的流量無法進入其他任何區域類型，但來自其他所有區域類型的流量則進入不受信任的區域。

允許介面信任

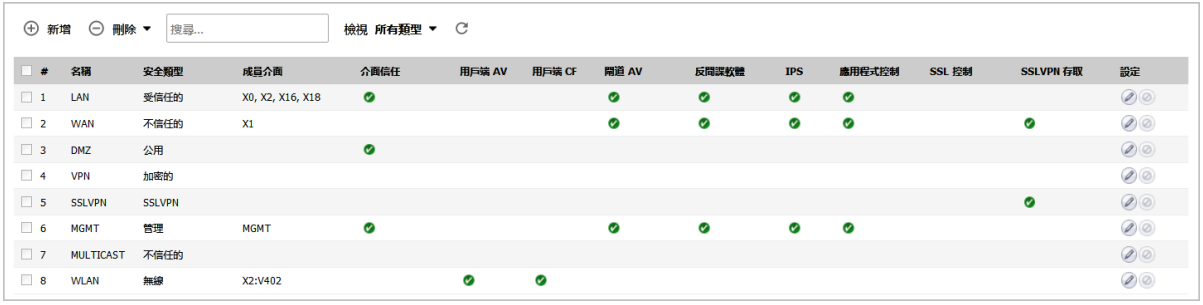
新增區域對話中的**允許介面信任**設定會自動建立存取規則，以允許流量在區域實例的介面之間流動。例如，如果向 LAN 區域同時指派了 **LAN** 和 **X3** 介面，則在 LAN 區域勾選**允許介面信任**核取方塊將會建立必要的存取規則，使得這些介面上的主機能夠相互通訊。

對區域啟用 SonicWall 安全服務

您可以對區域間的流量啟用 SonicWall 安全服務。例如，您可以對 WLAN 區域的傳入和傳出流量啟用 SonicWall 入侵保護服務，從而提高內部網路流量的安全性。您可在區域中啟用以下 SonicWall 安全服務:

強制執行內容篩選服務	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施內容篩選。
強制執行用戶端防毒服務	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施防毒防護。
啟用閘道防毒	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施閘道防毒防護。
啟用 IPS	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施入侵偵測和防護。
啟用應用程式控制服務	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施應用程式控制原則服務。
啟用防間諜軟體服務	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施入侵偵測和防護。
強制執行安全用戶端	對同一受信任且公用的 WLAN 區域安全類型的多個介面強制實施全域安全用戶端 (GSC) 防護。
建立群組 VPN	可為區域建立群組 VPN 原則，這項原則會顯示在**管理 | 連線 | VPN > 基本設定**的 VPN 原則表格中。您可以在 **VPN > 設定**中自訂群組 VPN 原則。如果您停用**建立群組 VPN**，群組 VPN 原則也會從 **VPN > 設定**中移除。如需更多建立 VPN 原則的相關資訊，請參閱 *SonicOS 連線能力*。
啟用 SSL 控制	啟用區域中的 SSL 控制。從此區域啟動的所有新 SSL 連接現在都將接受檢查。您必須先在**管理 | 防火牆設定 | SSL 控制**中指定在全域啟用 SSL 控制。如需更多 SSL 控制的相關資訊，請參閱 *SonicOS 安全設定*。
啟用 SSLVPN 存取	對區域啟用 SSLVPN 安全遠端存取。

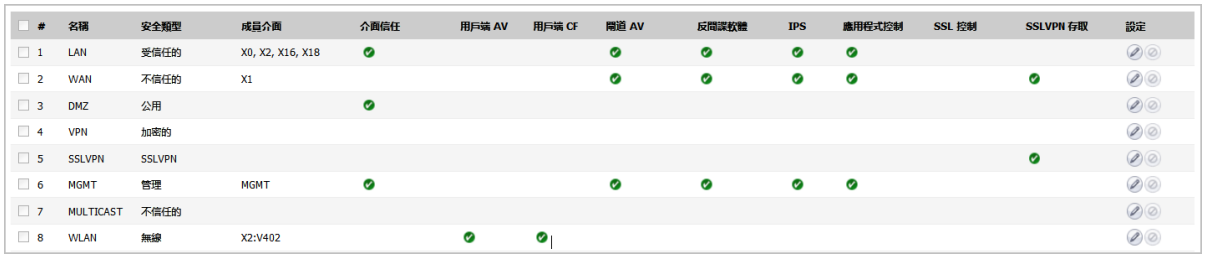
網路 | 區域



- 第 333 頁「區域設定表」
- 第 333 頁「新增新區域」
- 第 340 頁「刪除區域」
- 第 335 頁「設定來賓存取的區域」
- 第 338 頁「設定開放式驗證和社交登入的區域」
- 第 338 頁「設定 WLAN 區域」

區域設定表

區域設定表顯示 SonicWall 安全裝置預設的所有預先定義區域以及您所建立的所有區域的清單。表中顯示關於每個區域設定的以下狀態資訊：



#	名稱	安全類型	成員介面	介面信任	用戶端 AV	用戶端 CF	閘道 AV	反間諜軟體	IPS	應用程式控制	SSL 控制	SSLVPN 存取	設定
1	LAN	受信任的	X0, X2, X16, X18	✓			✓	✓	✓	✓			
2	WAN	不信任的	X1				✓	✓	✓	✓		✓	
3	DMZ	公用		✓									
4	VPN	加密的											
5	SSLVPN	SSLVPN										✓	
6	MGMT	管理	MGMT	✓			✓	✓	✓	✓			
7	MULTICAST	不信任的											
8	WLAN	無線	X2:V402		✓	✓							

名稱	區域的名稱。無法變更預先定義的 **LAN**、**WAN**、**WLAN**、**VPN** 和**加密**區域名稱。
安全類型	安全類型：**信任的**、**不信任的**、**公用**、**無線**或**加密**。
成員介面	區域成員介面。
介面信任	複選標記表示為此區域啟用了**允許介面信任**設定。
用戶端 AV	勾選標記代表系統已針對此區域傳入與傳出的流量啟用了 SonicWall 用戶端防毒服務。SonicWall 用戶端防毒用於管理區域內所有用戶端上的防毒用戶端應用程式。
閘道 AV	勾選標記代表系統已針對此區域的傳入與傳出的流量啟用了 SonicWall 閘道防毒服務。SonicWall 閘道防毒用於管理防火牆上的防毒服務。
反間諜軟體	勾選標記代表系統已針對通過此區域連接埠的流量，啟用了 SonicWall 防間諜軟體偵測和防護。
IPS	勾選標記代表系統已針對此區域傳入與傳出的流量啟用了 SonicWall 入侵保護服務。
應用程式控制	勾選標記代表系統已針對此區域傳入與傳出的流量啟用了應用程式控制服務。
SSL 控制	勾選標記代表系統已針對此區域傳入與傳出的流量啟用了 SSL 控制。從此區域起始的所有新 SSL 連接現在都將接受檢查。
SSL VPN 存取	勾選標記代表系統已針對此區域傳入與傳出的流量啟用了 SSL VPN 安全遠端存取。
設定	按一下**編輯**圖示會顯示**編輯區域**對話方塊。按一下**刪除**圖示將刪除此區域。刪除圖示在預設區域中為灰色；您無法刪除這些區域。

新增新區域

若要新增區域：

1 導覽到**管理 | 系統安裝 | 網路 | 區域**。

2 按一下**新增**圖示。隨即顯示**新增區域**對話。

3 在**名稱**欄位中輸入新區域的名稱。

4 在**安全類型**中選擇下列選項:

受信任	信任級別最高的區域 (例如內部 LAN 區段)。
公用	信任要求級別較低的區域 (例如 DMZ 介面)。
無線	WLAN 介面。
SSLVPN	已啟用內容篩選、用戶端防毒強制措施和用戶端 CF 服務的介面。 **附註：**選取這個安全類型後，這個對話方塊中的 VPN 和 SSL VPN 選項都會遭到停用。

5 如需允許區域內部通訊，請選取**允許介面信任**。自動建立允許流量在區域實例的介面之間流動的存取規則。預設情況下已核取此選項。

6 如果要使 SonicOS 自動產生此區域與相同信任級別其他區域之間的存取規則，請勾選**自動新增存取規則以允許相同信任級別的區域間的流量**。例如 CUSTOM_LAN -> CUSTOM _LAN 或 CUSTOM_LAN -> LAN。預設情況下已核取此選項。

> **附註：**如需瞭解這個選項和下列的存取規則選項，請參閱 *SonicOS 原則*，內有存取規則相關資訊。

7 如果要使 SonicOS 自動產生此區域與更低信任級別其他區域之間的存取規則，請勾選**自動新增存取規則以允許到更低信任級別的區域的流量**。例如 CUSTOM_LAN -> WAN 或 CUSTOM_LAN -> DMZ。預設情況下已核取此選項。

8 如果要使 SonicOS 自動產生此區域與更高信任級別其他區域之間的存取規則，請勾選**自動新增存取規則以允許來自更高信任級別的區域的流量**。例如 LAN -> CUSTOM_DMZ 或 CUSTOM_LAN -> CUSTOM_DMZ。預設情況下已核取此選項。

9 如果要使 SonicOS 自動產生此區域與更低信任級別其他區域之間的存取規則，請勾選**自動新增存取規則以拒絕到更低信任級別的區域的流量**。例如 WAN -> CUSTOM_LAN 或 DMZ -> CUSTOM_LAN。預設情況下已核取此選項。

10 如需使用網路主機上的用戶端防毒用戶端，在同一受信任或公用的 WLAN 區域的多個介面上強制實施用戶端防毒防護，勾選**啟用用戶端防毒執行服務**。預設情況下未勾選此選項。

附註：除非您在**安全類型**中選取了所需類型，否則這個選項會以灰色顯示且無法使用。

如需瞭解這個選項和下列的安全服務選項，請參閱 *SonicOS 安全設定*，內有更多這些服務的相關資訊。

11 如需使用網路主機上的用戶端 CF 用戶端，在同一受信任或公用的 WLAN 區域的多個介面上強制實施內容篩選，勾選**啟用用戶端內容篩選服務**。預設情況下未勾選此選項。

附註：除非您在**安全類型**中選取了所需類型，否則這個選項會以灰色顯示且無法使用。

12 如需為這個區域啟用 SSLVPN 安全遠端存取，請選取**啟用 SSLVPN 存取**。預設情況下未勾選此選項。

附註：如果選擇 **SSLVPN** 作為**安全類型**，此選項將顯示為灰色。

13 如需自動為此區域建立 SonicWall 群組 VPN 原則，請選取**建立群組 VPN**。您可以在**管理 | 連線 | VPN | 設定**中自訂群組 VPN 原則。 預設情況下未勾選此選項。

注意：停用建立群組 VPN 時，系統會移除所有對應的群組 VPN 原則。

附註：如果選擇 **SSLVPN** 作為**安全類型**，此選項將顯示為灰色。

如需進一步瞭解這個選項和其他連線選項，請參閱 *SonicOS 連線能力*。

14 如需為區域啟用 SSL 控制，請選取**啟用 SSL 控制**。從此區域啟動的所有新 SSL 連接現在都將接受檢查。預設情況下未勾選此選項。

附註：您必須先在**管理 | 安全設定 | 防火牆 | SSL 控制**中指定在全域啟用 SSL 控制。

15 如需在您的安全設備上為所有連至這個區域的用戶端強制啟用閘道防毒防護，請選取**啟用閘道防毒服務**。SonicWall 閘道防毒用於管理安全設備上的防毒服務。預設情況下未勾選此選項。

16 如需對同一受信任的、公用或 WLAN 區域的多個介面強制實施入侵偵測和防護，勾選**啟用 IPS**。預設情況下未勾選此選項。

17 如需對同一受信任或公用的 WLAN 區域安全類型多個介面強制實施防間諜軟體偵測和防護，勾選**啟用防間諜軟體服務**。預設情況下未勾選此選項。

18 如需對同一受信任或公用的 WLAN 區域安全類型的多個介面強制實施應用程式控制原則服務，勾選**啟用應用程式控制服務**。預設情況下未勾選此選項。如需更多應用程式控制的相關資訊，請參閱 *SonicOS 原則*。

19 按一下**確定**。現在，新區域已新增到安全設備。

設定來賓存取的區域

重要：您無法針對來賓存取設定不受信任、已加密、SSL VPN 或管理區域。

SonicWall 來賓服務提供了一種便捷的解決方案來為來賓或不信任的網路節點建立有線和無線來賓通道和/或鎖定僅網際網路網路存取權。此功能可擴充至您所選擇的 WLAN、LAN、DMZ 或公用/半公用區域中的無線或有線使用者。

若要設定來賓服務功能：

1 導覽到**管理 | 系統安裝 | 網路 | 區域**。

2 按一下想要為其新增來賓服務的區域的**設定**按鈕。顯示**編輯區域**對話。

3 按一下**來賓服務**。系統只會提供**啟用來賓服務**選項。

4 按一下**啟用來賓服務**，您即可使用所有其他選項，但系統預設不會選取這些選項。

5 選取下列用於來賓服務的設定選項:

啟用內部來賓通訊	允許來賓直接與連接到此區域的其他使用者通訊。
繞過來賓 AV 檢查	允許來賓流量繞過防毒防護。
對來賓繞過用戶端 CF 檢查	允許來賓流量繞過用戶端 CF 強制措施。
啟用外部來賓驗證	獲取存取權限之前，需要對連接您所選擇的裝置或網路的來賓進行驗證。選取這個選項後即可使用**設定**按鈕。按一下**設定**隨即會顯示**外部來賓驗證**對話方塊。 **附註：**選取這個選項後，下列 4 個選項會以灰色顯示且無法使用。
啟用網頁驗證入口驗證	可讓您建立具備 RADIUS 驗證機制的自訂登入頁面。選取這個選項後即可使用**設定**按鈕。按一下**設定**隨即會顯示**自訂登入頁面**對話方塊。
啟用無驗證的原則頁面	在使用者首次連線至 SonicPoint 或 SonicWave 時，將使用者導向來賓服務使用原則頁面。來賓使用者必須接受原則才能通過驗證 (而不是提供使用者名稱和密碼)。選取這個選項後即可使用**設定**按鈕。如需設定可自訂的 HTML 原則使用頁面，請按一下**設定**。**自訂原則訊息**對話方塊隨即顯示。
自訂驗證頁面	在使用者首次連接到網路時，將使用者重新導向至自訂驗證頁面。選取這個選項後即可使用**設定**按鈕。如需設定自訂驗證頁面，請按一下**設定**即可顯示**自訂登入頁面**對話方塊。
發佈驗證頁面	驗證成功後，立即將使用者導向指定頁面。選取這個選項後即可使用相關欄位。在欄位中輸入驗證後頁面的 URL。
繞過來賓驗證	允許將來賓服務功能整合到已使用某種形式的使用者級別驗證的環境中。這項功能可將驗證流程自動化，讓無線使用者無需經過驗證即可存取無線來賓服務，不會受到任何限制。選取後，您就可使用這個選項的下拉功能表，其中的選項如下: • **所有 MAC 位址** (預設) • 位址物件 • 位址群組 • **建立新的 MAC 物件** - 顯示**新增位址物件**對話方塊。[a] **附註：**此功能只能在需要無限制的來賓服務存取權限的情況下使用，或者在其他裝置上游已強制實施驗證的情況下使用。
重新導向 SMTP 流量	將進入此區域的 SMTP 流量重新導向至您所指定的 SMTP 伺服器。選取後，您就可使用這個選項的下拉功能表，其中的選項如下: • 位址物件 • **建立新的位址物件** - 顯示**新增位址物件**對話方塊。a
拒絕網路	封鎖流向您命名的網路的流量。選取後，您就可使用這個選項的下拉功能表，其中的選項如下: • 位址物件 • 位址物件群組 • **建立新的位址物件** a • **建立新的位址物件群組** a

通過網路	自動允許流量通過已啟用來賓服務的區域，流向指定的網路。選取後，您就可使用這個選項的下拉功能表，其中的選項如下: • 位址物件 • 位址物件群組 • **建立新的位址物件** a • **建立新的位址物件群組** a **附註：**顯示**新增位址物件**對話方塊。
最大來賓數	指定允許連接到此區域的最大來賓使用者數。最小數量為 1，最大數量為 4500，預設設定為 **10**。

a. 如需建立位址物件和位址物件群組的相關資訊，請參閱 *SonicOS 原則*。

6 按一下**確定**，對此區域套用上述設定。

設定開放式驗證和社交登入的區域

SonicOS 支援開放式驗證 (OAuth) 和社交登入：

- OAuth 協助使用者在應用程式間共用資料。
- 社交登入簡化各種社交媒體的登入程序

若要使用這些功能，如第 618 頁「設定開放式驗證、社交登入和 LHM」中所述建立區域。

設定 WLAN 區域

1 導覽到**管理 | 系統安裝 | 網路 | 區域**。

2 如果您要設定：

- 新的區域，按一下**新增...**按鈕。
- 現有區域，按一下 WLAN 區域的**編輯**圖示 。

顯示**新增/編輯區域**對話。

附註：根據區域的不同，可能會為**來賓服務**和**無線**提供標籤。

第 333 頁「新增新區域」描述了如何設定**一般**選標籤。

3 如需自動建立存取規則，以便允許區域實例的介面之間的流量移轉，請選取**允許介面信任**。例如，如果向 LAN 區域同時指派了 **LAN** 和 **X3** 介面，則在 LAN 區域勾選**允許介面信任**核取方塊將會建立必要的存取規則，使得這些介面上的主機能夠相互通訊。

4 如果您無法使用**無線**，請從**安全類型**中選取**無線**。

5 按一下**無線**標籤。

6 在**無線設定**部分中，選擇 **SSLVPN 強制措施**可要求所有進入 WLAN 區域的流量通過 SonicWall SSL VPN 裝置驗證。選取這個選項後，您就可使用下列兩個選項。 預設情況下未勾選此選項。

7 在 **SSL VPN 伺服器**中選取一個位址物件，將流量導向至 SonicWall SSL VPN 裝置或建立一個新的位址物件。如需建立位址物件和位址物件群組的相關資訊，請參閱 *SonicOS 原則*。

8 在 **SSL VPN 服務**中，選擇要為通過 SSL VPN 驗證的用戶端提供的服務或服務群組。

9 在 **SonicPoint/SonicWave 設定**部分中選擇 **SonicPoint/SonicWave 佈建設定檔**，套用至所有連結到這個區域的 SonicPoint/SonicWave。除非單獨為 SonicPoint/SonicWave 設定了不同的設定，否則任何時候在其連接到此區域時，都會自動使用 SonicPoint/SonicWave 佈建設定檔中的設定對其進行佈建。如需 SonicPoint/SonicWave 佈建設定檔的相關資訊，請參閱 *SonicOS 連線功能*。

附註：您也可為下列 4 項設定勾選**自動佈建**設定，允許設定檔連接的 SonicPoint/SonicWave 能夠在設定檔修改時自動進行佈建。預設情況下未勾選此選項。

10 如要套用到這個區域連接的所有 SonicPointN/Ni/Ne，請選取 **SonicPointN/Ni/Ne 佈建設定檔**。除非單獨為 SonicPointN/Ni/Ne 設定了不同的設定，否則任何時候在其連接到此區域時，都會自動使用 SonicPoint 佈建設定檔中的設定對其進行佈建。系統預設的佈建設定檔為 **SonicPointN**。

11 當您想要套用於所有連接到此區域的 SonicPointNDRs 時，選擇 **SonicPoint NDR 佈建設定檔**。除非單獨為 SonicPointNDR 設定了不同的設定，否則任何時候在其連接到此區域時，都會自動使用 SonicPointNDR 佈建設定檔中的設定對其進行佈建。系統預設的佈建設定檔為 **SonicPointNDR**。

12 如要套用到這個區域連接的所有 SonicPointACe/ACi/N2，請選取 **SonicPoint AC 佈建設定檔**。除非單獨為 SonicPointACe/ACi/N2 設定了不同的設定，否則任何時候在其連接到此區域時，都會自動使用 SonicPointACe/ACi/N2 佈建設定檔中的設定對其進行佈建。系統預設的佈建設定檔為 **SonicPointACe/ACi/N2**。

13 如要套用到這個區域連接的所有 SonicPointNDR，請選取 **SonicWave 432o/e/i 佈建設定檔**。除非單獨為 SonicPointNDR 設定了不同的設定，否則任何時候在其連接到此區域時，都會自動使用 SonicPointNDR 佈建設定檔中的設定對其進行佈建。系統預設的佈建設定檔為 **SonicWave**。

14 勾選**僅允許 SonicPoint / SonicPointN 產生的流量**，僅允許來自 SonicWall SonicPoints 的流量進入 WLAN 區域介面。這使得您的 WLAN 擁有最高的安全性。如果想要 WLAN 區域允許任何流量（不管流量是否來自無線連接），請清除此選項。

提示：若要使 WLAN 區域允許任何流量（不管流量是否來自無線連接），請清除**僅允許 SonicPoint / SonicPointN 產生的流量**。

附註：如需來賓服務設定資訊，請參見第 335 頁「設定來賓存取的區域」。

15 按一下**確定**，對 WLAN 區域套用上述設定。

刪除區域

若要刪除使用者建立的區域:

1 導覽到**管理 | 系統安裝 | 網路 | 區域**。

附註：在預先定義區域中，**刪除**圖示無法使用。不能刪除這些區域。可以刪除您所建立的任何區域。

2 按一下區域的**設定**欄中的**刪除**圖示。

若要刪除一個或多個使用者建立的區域:

1 導覽到**管理 | 系統安裝 | 網路 | 區域**。

附註：核取方塊不適用於預先設定區域。不能刪除這些區域。可以刪除您所建立的任何區域。

2 選取要刪除的區域。

3 在**刪除**中選取要刪除的區域:

- **刪除選取項目**
- **全部刪除**

17

設定有線模式 VLAN 轉譯

網路 | VLAN 轉譯

附註：所有支援有線模式的平台中都提供 VLAN 轉譯。

附註：您無法經由 VLAN 介面同時啟用 VLAN 轉譯和有線模式。

關於 VLAN 轉譯

VLAN 轉譯（對應）功能允許在安全模式下到達 VLAN 上有線模式介面的流量可對應到另一 VLAN 的輸出成對介面。對某些傳入不同 VLANS 上的 SonicWall 安全設備的流量重選路由，用於執行進一步分析、處理或僅重新對應流量。所有支援有線模式的裝置都支援此功能。

有線模式的優勢就是您可以預先佈建 VLAN 對應，如此一來您就可以在介面收到流量之前完成對應設定。您也可以在使用中的有線模式介面上新增和刪除對應。

主題：

對應模式

您可以在以下模式下建立 VLAN 對應：

- 單向對應 - 例如，用於：
  - 從低安全性網路向高安全性網路的安全列印
  - 從低安全性網路向高安全性網路傳送應用程式和操作系統更新
  - 在 SOC（安全作業中心）中監控多個網路

- 在高安全性網路中提供時間同步
- 傳送檔案
- 提供從低安全性網路向高安全性網路的「您有郵件」警告

- 雙向對應 - 例如，用於通過 TCP 等安全設備設定往返裝置的雙向連接。

對應持續性

為一對介面建立的 VLAN 對應會持續重新載入，且會儲存作為設定的一部分。如果有線模式配對 (安全模式) 具備與其相關聯的對應，則除非對應原則遭到刪除，否則無法更動有線模式。

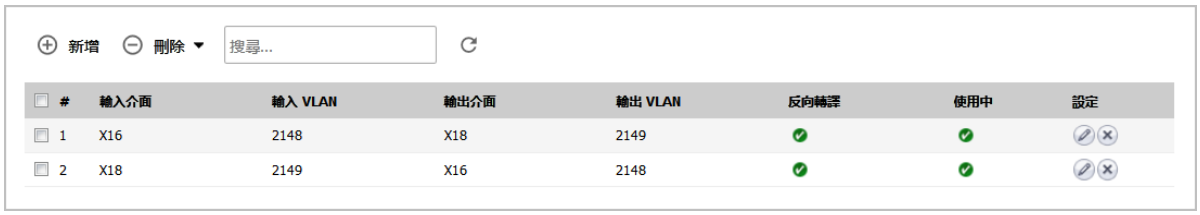
對應多介面對

您可以同時為多對介面建立 VLAN 對應。建立 VLAN 對應時，這些介面必須成為現有安全有線模式配對的一部分。您也可為含多個介面的介面建立對應，但僅有目前使用中的有線模式配對的對應，才可供您隨時使用。

如果配對的介面有所變更，系統就會顯示「介面具備有線模式 VLAN 項目時，無法變更有線模式配對介面」訊息。

範例

多介面對對應



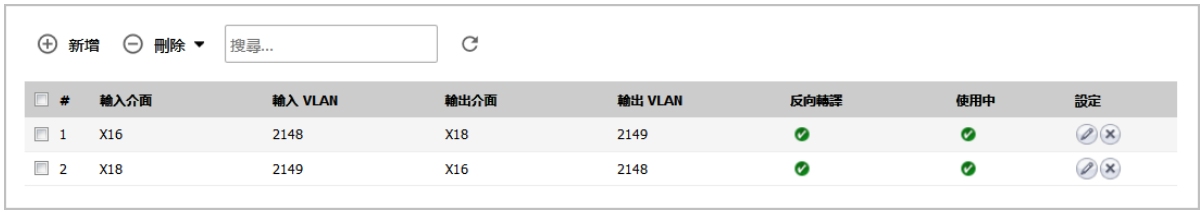
在多介面對對應中，存在 X12 至 X13（原則 1）及 X12 至 X15（原則 2）的對應。

目前只有 X12 和 X13 (原則 1 和 3) 以及 X14 和 X15 (原則 4 和 6) 構成有線模式配對，因此只有原則 1、3、4 和 6 處於使用中狀態 (如活動欄中的綠色勾選標記所示)。

附註：如果介面具備有線模式 VLAN 項目，則無法變更有線模式配對介面。

建立和管理 VLAN 對應

網路 | VLAN 轉譯可讓您建立及管理介面的 VLAN 對應。



新增圖示	**新增 VLAN 轉譯**對話方塊隨即顯示。
刪除圖示	**刪除**下拉功能表隨即顯示: • **刪除選取項目** • **全部刪除**
搜尋欄位	可讓系統僅顯示您所需的 VLAN 轉譯。
「**重新整理**」圖示	重新整理 VLAN 轉譯表。
原則數和核取方塊	原則數量及其關聯的核取方塊。
輸入介面	輸入介面的名稱。
輸入 VLAN	輸入介面的 VLAN 標籤。
輸出介面	流量對應的介面名稱。
輸出 VLAN	流量對應的介面 VLAN 標籤。
反向轉譯	指出對應為單向還是雙向: • **已停用** - 單向；欄位留空。 • **已啟用** - 雙向；綠色勾選標記。
使用中	對應對狀態： • **使用中** - 有線模式配對已對應且處於使用中狀態；綠色勾選標記。 • **非使用中** - 有線模式配對已對應但未處於使用中狀態 (已預先佈建)；欄位留空。
設定	顯示對應對的**編輯**和**刪除**圖示。

主題：

- 第 343 頁「建立 VLAN 對應」
- 第 347 頁「管理 VLAN 對應」

建立 VLAN 對應

您可以在有線模式配對之前或之後建立單向 VLAN 對應。建立 VLAN 對應分為兩步驟：

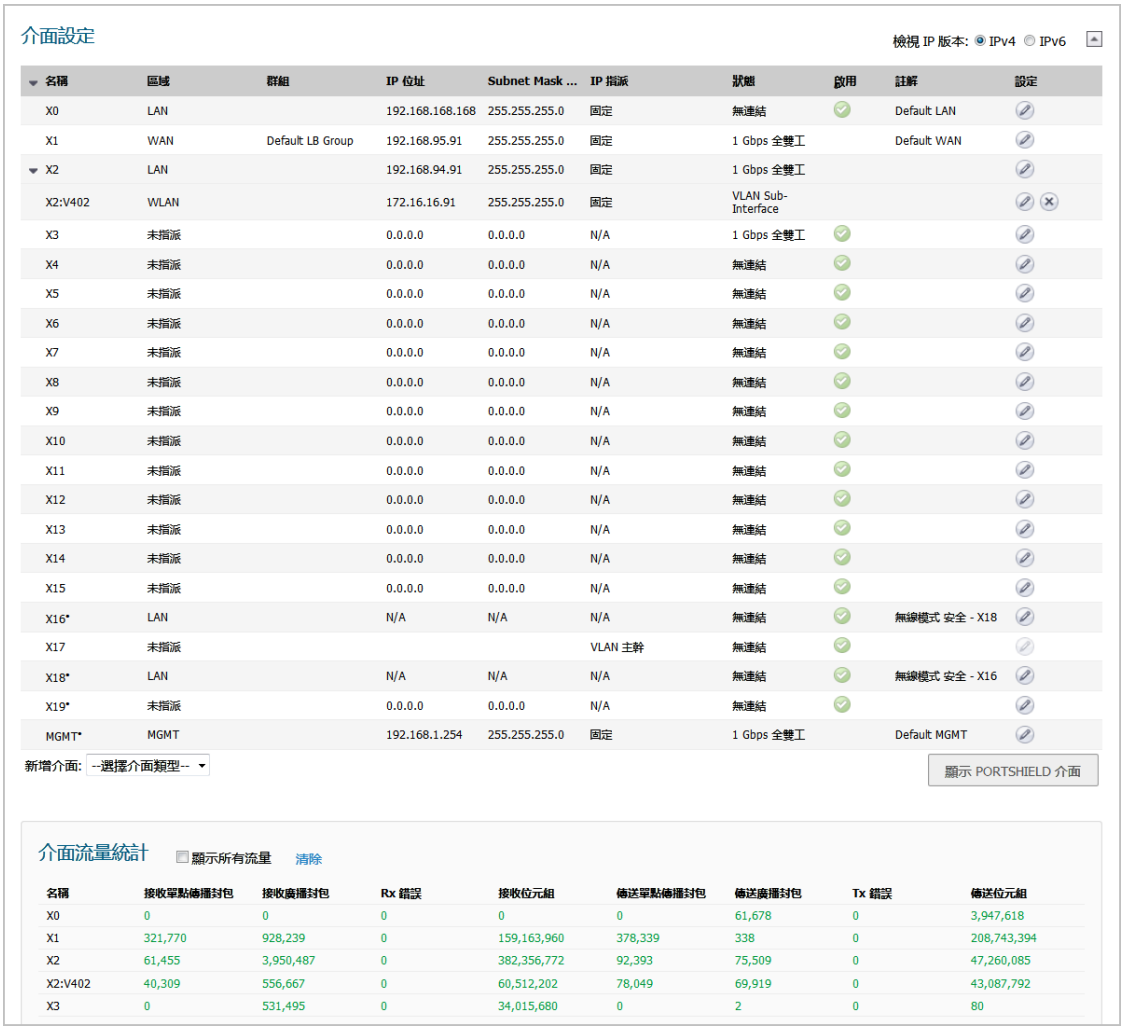
1 第 343 頁「在安全模式下建立有線模式配對」

2 第 346 頁「建立 VLAN 對應」

在安全模式下建立有線模式配對

若要在安全模式下建立有線模式配對:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。



2 找出要作為有線模式配對的一部分的介面，然後按一下**編輯**圖示。將顯示**編輯介面**對話方塊。

3 在**區域**中選擇用於有線模式配對的區域。這些選項將發生變更。

4 在**模式/ IP 指派**中選擇**有線模式 (2 連接埠有線)**。這些選項將再次發生變更。

5 在**有線模式類型**中選擇**安全 (內聯流量的主動 DPI)**。

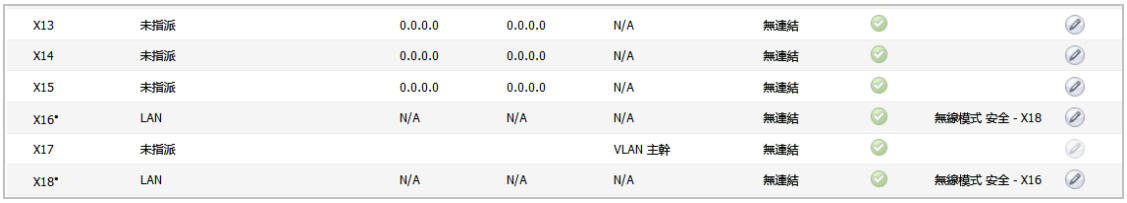
6 從**成對介面**下拉功能表中選擇要與目前介面配對的介面。

> **提示：**確保未指派您配對的介面。

7 在**成對介面區域**中選擇用於成對介面的區域。預設值為 **LAN**。

8 像設定一般有線模式對一樣設定其他選項，如第 265 頁「設定有線和分接模式」和第 265 頁「設定有線和分接模式」所示。

9 按一下**確定**。**網路 | 介面**頁面隨即更新。

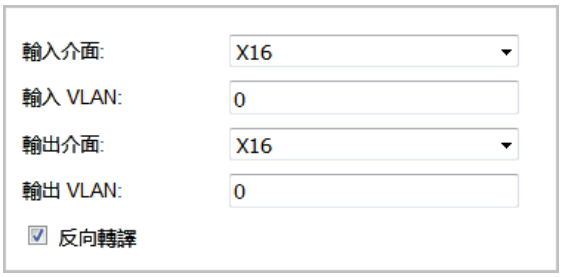


建立 VLAN 對應

建立 VLAN 對應的步驟如下：

1 導覽到**網路 | VLAN 轉譯**。

2 按一下**新增**圖示。隨即顯示**新增 VLAN 轉譯**對話方塊。



3 選擇您希望從**輸入介面**接收流量的配對中的有線模式介面。

4 將**輸入 VLAN** 設定為您希望接收對應流量的 VLAN。

5 選擇您想要對應流量至**輸出介面**下拉功能表的配對中的有線模式介面。

6 將**輸出 VLAN** 設定為您想要接收對應流量的 VLAN。

7 如需建立：

- 單向對應，確保未勾選**反向轉譯**核取方塊。例如將介面 A 上的 VLAN X 對應至介面 B 上的 VLAN Y。

  附註：預設情況下已核取此選項。

- 雙向對應，勾選**反向轉譯**核取方塊。例如，如需將介面 B 上的 VLAN Y 對應至介面 A 上的 VLAN X，以及將介面 A 上的 VLAN X 對應至介面 B 上的 VLAN Y。

8 按下**新增**。更新**有線模式 VLAN 轉譯**表。

管理 VLAN 對應

主題：

編輯對應

如需編輯對應，請按一下**設定**列中的**編輯**按鈕。隨即顯示**編輯 VLAN 轉譯**對話方塊。您可以變更除**反向轉譯**設定以外的任何對應。

篩選對應

如果您具有許多 VLAN 對應，則可僅顯示感興趣的對應，步驟如下：

1 在**搜尋**欄位中輸入介面名稱或 VLAN 標籤。

2 按 **Enter**。

僅顯示符合搜尋條件的對應。

重新顯示所有對應的步驟如下：

1 刪除**搜尋**欄位中的條件。

2 按下 **Enter** 鍵。

刪除對應

若要刪除對應:

1 若要刪除：

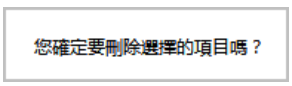
- 單個對應，步驟如下：
  - 按一下**設定欄中的刪除圖示**。

    將顯示確認訊息：

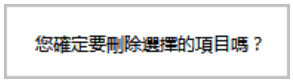
  - **按一下選擇**核取方塊，然後再從**刪除**下拉功能表中，選取**刪除**。

    將顯示確認訊息：

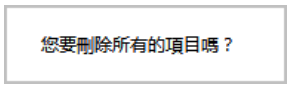
- 多個對應，按一下其**選擇**核取方塊，然後再從**刪除**下拉功能表中選取**刪除**。

  將顯示確認訊息：

- 所有對應，從**全部刪除**下拉功能表中，選取**刪除**。

  將顯示確認訊息：

2 按一下**確定**。

如果原則為雙向，則在刪除一個方向時兩個方向均將刪除。

18

設定 DNS 設定

網路 | DNS

網域名稱系統 (DNS) 是分布式的分層系統，它提供了一種方法使用完整網域名稱 (FQDN) 的英數字元名稱，而不是使用不便記憶的數字 IP 位址來識別網際網路上的主機。 **管理 | 系統安裝 | 網路 | DNS** 可讓您視需求手動配置您的 DNS 設定。這個頁面有兩種版本，視您使用的 IP 版本而定: IPv6 網路 | DNS 和 IPv4 網路 | DNS

IPv6 網路 | DNS

IPv4 網路 | DNS

主題：

- 第 351 頁「關於分割 DNS」
- 第 352 頁「管理 DNS 伺服器」

關於分割 DNS

分割 DNS 是一種增強，可讓您設定一組伺服器並將其與指定網域名稱 (可以是萬用字元) 關聯。當 SonicOS DNS 代理接收與網域名稱相符的查詢時，名稱會被傳輸到指定的 DNS 伺服器。分割 DNS 範例顯示其運作方式：

分割 DNS 範例

- 此拓撲有兩個具網路連接的防火牆：
  - 一個防火牆連線到網際網路。
  - 另一個是連線到企業網路的 VPN 通道。
- 預設 DNS 查詢會到公用 ISP DNS 伺服器。
- 所有 `*.sonicwall.com` 的查詢都會導至位於 VPN 通道後方的 DNS 伺服器。

如需檢視和設定分割 DNS 項目，請參見第 353 頁「為分割 DNS 設定網域專屬 DNS 伺服器」。

新增分割 DNS 項目後，所有 `sonicwall.com` 的查詢都會傳送到特定伺服器 (請參閱第 353 頁「為分割 DNS 設定網域專屬 DNS 伺服器」)。

您也可以設定多個 DNS 伺服器來處理 `sonicwall.com` 的查詢。

關於每分割區的 DNS 伺服器和分割 DNS

無論是否具有驗證分割區，通常需要使用網域自己的 DNS 伺服器來解析網域中的裝置名稱，偶爾也可能需要使用不同的外部 DNS 伺服器來解析外部主機名稱。而現在這種情況在有了多個驗證分割區時更加嚴重，因為這些分割區通常需要使用其他 DNS 伺服器來解析不同分割區內的主機名稱。

附註：此外，由於 LDAP 轉介通常會按照 DNS 名稱來提供偏好的伺服器 (即便是透過 IP 位址設定的 LDAP 伺服器也一樣)，因此有時還會意外需要使用網域所擁有的 DNS 伺服器。

需要其他外部 DNS 伺服器解析外部主機名稱的範例，牽涉到內部網域 DNS 伺服器無法解析的外用雲端服務。

SonicWall 安全設備會直接使用分割 DNS 功能來解析網域中的裝置名稱，不需要啟用 DNS 代理；具備驗證分割功能的多個不相關網域也同樣適用。

出現下列情況時，系統會將分割 DNS 中設定的 DNS 伺服器，直接用於內部網域中的主機名稱 DNS 查詢:

- 凡是安全設備的主要 DNS 快取中有項目時:
  - SMTP 伺服器
  - SYSLOG 伺服器
  - Web 代理伺服器和使用者 (內部) 代理伺服器
  - GMS 和待命 GMS

    - POP 伺服器
    - RADIUS 驗證和計費伺服器
    - LDAP 伺服器
    - SSO/終端服務代理和 RADIUS 計費用戶端
- 分割功能已啟用，且分割區具備一個網域或一個父/子網域的樹狀結構 (也就是一個 AD 樹系) 時，如果分割區的頂層網域設有分割 DNS 伺服器，則系統會將這些伺服器複製到內部的分割區結構中。這些 DNS 伺服器隨後會用於解析分割區中的代理、伺服器和用戶端名稱。
- 如果分割功能已啟用，且分割區設有多個不同的網域 (這是允許但不常見的情況)，則系統不會將任何 DNS 伺服器複製到分割區結構中，而是仰賴以下說明的機制運作。
- 如果分割功能已停用，或分割區並未設有任何 DNS 伺服器，或者需要解析與分割區無關的項目時，系統就會透過分割 DNS 提供的 API，依據要求選取要使用的 DNS 伺服器。

管理 DNS 伺服器

網路 | DNS 上的選項會因為您指定的是 Ipv6 還是 IPv4 而有所差異。一般來說，兩種版本的管理介面頁面都提供 **DNS 設定**和**分割 DNS** 部分，我們會一併說明。

主題：

選擇 IP 版本

若要選擇 IP 版本:

1 導覽到**網路 | DNS**。

2 在頁面右上角的**檢視 IP 版本**中，選擇:

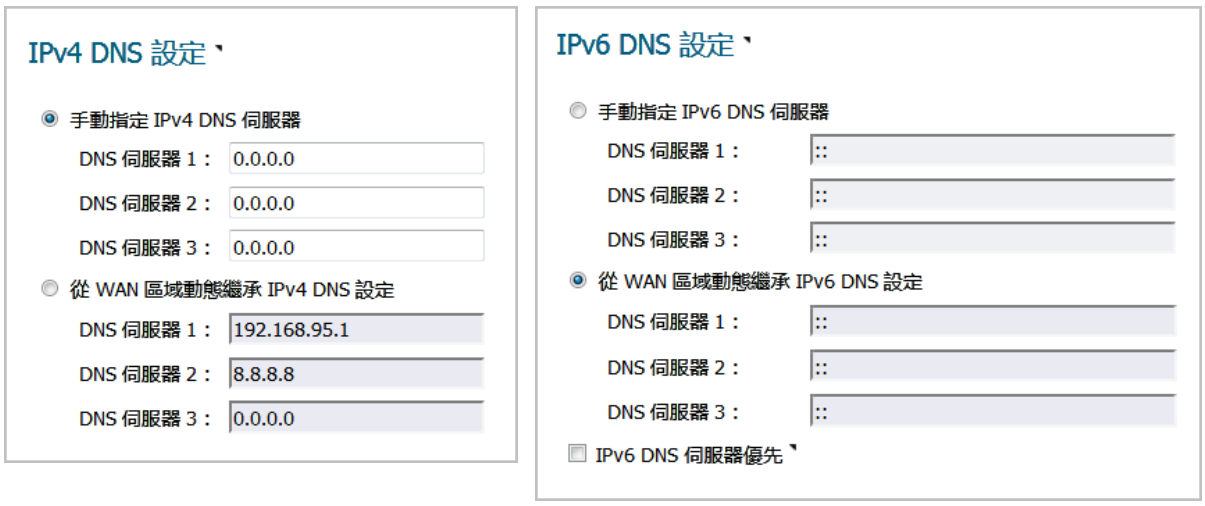
- **IPv4**
- **IPv6**

網路 | DNS 上的選項會因為您指定的是 Ipv6 還是 IPv4 而有所差異。

指定要使用的 DNS 伺服器

無論 IP 版本為何，您都可以指定 SonicOS 的 DNS 伺服器選擇方式。兩個 IP 版本的設定方法相同。

IPv4 DNS 設定/IPv6 DNS 設定部分



若要指定要使用的 DNS 伺服器:

1 導覽到**網路 | DNS**。

2 在 **IPv4/IPv6 DNS 設定**部分中，選擇下列其中一個選項:

- 手動指定 DNS 伺服器。
  a) 選取**手動指定 IPv4/IPv6 DNS 伺服器**。
  b) 在 **DNS 伺服器**欄位中輸入 IP 位址 (最多 3 個)。
  c) 如果您使用的是:
  - IPv4，請移至步驟 4。
  - IPv6，請移至步驟 3。
- 若要使用 WAN 區域所配置的 DNS 設定:
  a) 選取**從 WAN 區域動態繼承 IPv4 DNS 設定**。系統會自動將一個或多個 IP 位址填入 **DNS 伺服器**欄位中。
  b) 移至步驟 4。

3 如果只想使用 IPv6 伺服器，請選取**優先使用 IPv6 DNS 伺服器**。

△ 注意：**這個選項僅適用於 IPv6 DNS 伺服器設定無誤時。**

4 按一下**接受**以儲存您的變更。

為分割 DNS 設定網域專屬 DNS 伺服器

您也可以選擇設定獨立的網域專屬 DNS 伺服器，搭配 IPv6 或 IPv4 使用。兩個 IP 版本的設定方法相同。

IPv6 分割 DNS 部分

IPv4 分割 DNS 部分

網域名稱	DNS 伺服器的名稱。
DNS 伺服器	DNS 伺服器的 IPv4/Pv6 IP 位址。 **附註：網路 | DNS 代理**頁面會顯示 DNS 伺服器的狀態。
本機介面	指派至 DNS 伺服器的介面。
設定	對於每個伺服器包含**編輯**和**刪除**圖示。

若要新增網域專屬 DNS 伺服器，並將伺服器與指定的網域名稱建立關聯:

重要：分割 DNS 的項目數量上限為 32。如果清單已滿，就無法再新增項目。

1 導覽到**網路 | DNS**。

2 在**檢視 IP 版本**中選擇 IP 版本:

3 如需啟用分割 DNS 伺服器的 Proxy 處理功能，請選取**啟用分割 DNS 伺服器的 Proxy 處理功能**。 預設情況下已核取此選項。

4 按一下**分割 DNS** 表格下的**新增**。隨即顯示**新增分割 DNS 項目**對話。

提示：如果您選取了 DNS 代理，系統就會在**新增分割 DNS 項目**對話方塊中顯示相關頁面，即 **DNS 代理**。

IPv6 新增分割 DNS 項目

IPv4 新增分割 DNS 項目

IPv6 和 IPv4 新增分割 DNS 項目

5 選擇 IP 版本:

- **IPv4**
- **IPv6**
- 兩者

6 在**網域名稱**欄位中輸入網域名稱。名稱可包含萬用字元 (*；例如 *.sonicwall.com)。

7 如需為這個網域設定一個或多個 IPv4/IPv6 分割 DNS 伺服器，請在適用的欄位中輸入 IP 位址:

- **主要伺服器 (v4/v6)**
- **次要伺服器 (v4/v6)** (選用)
- **第三伺服器 (v4/v6)** (選用)

8 在**本機介面**中選擇一個介面。

9 如果您尚未啟用 DNS 代理，請移至步驟 13。

10 按一下 **DNS 代理**。

11 如需指定存留時間，請選取**在 DNS 回覆中手動設定 TTL 值**。

12 輸入快取項目的存留時間上限。

13 按一下**確定**。

> **提示：**無論您在設定時選擇了哪一個 IP 版本，系統一律會在兩個 IP 版本的**分割 DNS** 表格中顯示 DNS 伺服器。

編輯分割 DNS 項目

若要編輯分割 DNS 項目。

1 導覽到**網路 | DNS**。

2 在**分割 DNS** 表格中，按一下所需項目的**編輯**圖示。**編輯分割 DNS 項目**對話隨即顯示。

3 做出變更。

4 按一下**確定**。

刪除分割 DNS 項目

若要刪除分割 DNS 項目：

1 按下項目的**刪除**圖示。

若要刪除兩個或以上的分割 DNS 項目：

1 勾選要刪除項目的核取方塊。**刪除**按鈕即可使用。

2 按一下**刪除**按鈕。

若要刪除所有分割 DNS 項目：

1 按一下**全部刪除**按鈕。

DNS 和 IPv6

如需 SonicOS 的 IPv6 實作的完整資訊，請參見第 761 頁「IPv6」。

IPv6 **網路 | DNS** 頁面包含下列部分:

- 選擇版本: 請參閱第 352 頁「選擇 IP 版本」
- IPv6 DNS 設定; 請參閱第 352 頁「指定要使用的 DNS 伺服器」
- IPv6 分割 DNS: 請參閱第 353 頁「為分割 DNS 設定網域專屬 DNS 伺服器」

DNS 和 IPv4

IPv4 **網路 | DNS** 頁面包含以下區段：

- 選擇版本: 請參閱第 352 頁「選擇 IP 版本」
- IPv4 DNS 設定; 請參閱第 352 頁「指定要使用的 DNS 伺服器」
- IPv4 分割 DNS: 請參閱第 353 頁「為分割 DNS 設定網域專屬 DNS 伺服器」
- 第 359 頁「DNS 繫結攻擊預防」

- 第 359 頁「針對 FQDN 的 DNS 繫結」
- 第 360 頁「DNS 快取」

DNS 繫結攻擊預防

DNS 重新繫結是對嵌在網頁中的代碼進行的基於 DNS 的攻擊。正常情況下，來自嵌在網頁中的代碼（JavaScript、Java 和 Flash）的請求會繫結至其來源網站（參見「同源原則」）。DNS 重新繫結攻擊可用於提高基於 JavaScript 的惡意軟體的能力，以滲入私人網路和破壞瀏覽器的同源原則。

DNS 重新繫結攻擊程式會註冊一個網域，並將該網域委派給程式所控管的 DNS 伺服器。該伺服器會被設定為使用極短的存留時間 (TTL) 參數提供回應，進而禁止對結果進行快取。第一個回應會包含負責代管惡意代碼的伺服器的 IP 位址。後續所有請求包含來自可能位於防火牆後面並作為攻擊程式目的地的私人 (RFC 1918) 網路 IP 位址。由於二者都是完全有效的 DNS 回應，因此它們會授權沙箱指令碼存取私人網路中的主機。透過反覆這些短期但仍舊有效的 DNS 答覆中的位址，此指令碼能夠掃描網路和執行其他惡意活動。

啟用 DNS 重新繫結攻擊防護：

1 導覽到**網路 | DNS**。

2 捲動至 **DNS 重新繫結攻擊預防功能**部分。

3 選取**啟用 DNS 重新繫結攻擊預防功能**。預設情況下未勾選此選項。 兩個選項隨即可供使用。

4 在**操作**中，選取偵測到 DNS 重新繫結攻擊時執行的操作:

- **記錄攻擊** (預設值)
- **記錄攻擊並返回查詢拒絕回覆**
- **記錄攻擊並丟棄 DNS 回覆**

5 在**允許網域**中，針對應視為有效回應的本機連線/路由子網域，選取允許的網域 FQDN 位址物件或 FQDN 位址物件群組，其中必須包含允許的網域名稱 (例如 `*.sonicwall.com`)。

您也可透過選擇**建立 FQDN 位址物件...**或 **FQDN 位址物件群組...**建立新的 FQDN 位址物件或 FQDN 位址物件群組。

6 按一下**接受**。

針對 FQDN 的 DNS 繫結

若要啟用 FQDN 的 DNS 繫結

1 導覽到**網路 | DNS**。

2 捲動至 **FQDN 的 DNS 繫結**部分。

3 選取 **FQDN 物件僅快取已核准伺服器的 DNS 回覆**。預設情況下未勾選此選項。

4 按一下**接受**。

DNS 快取

若要顯示一般 DNS 快取內容，按一下**顯示 DNS 快取**按鈕。快取內容會顯示在彈出式視窗中:

內容	DNS 伺服器名稱
DNS 名稱	伺服器的 IP 位址
IP 位址	IPv4 位址
TTL（秒數）	存留時間
排清	按下這個會排清伺服器的 DNS 快取項目。
全部排清	按一下就可針對所有列出的伺服器清空全部的 DNS 快取項目。

19

設定 DNS 代理設定

網路 > DNS 代理

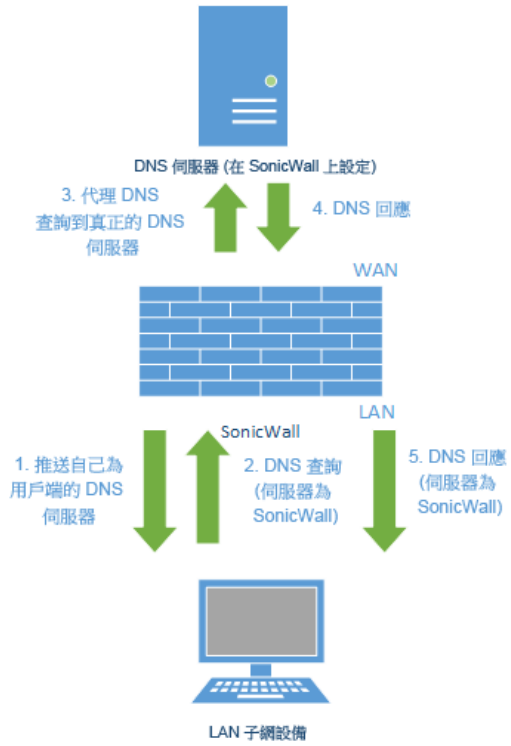
主題：

- 第 363 頁「關於 DNS 代理」
- 第 365 頁「啟用 DNS 代理」
- 第 366 頁「設定 DNS 代理設定」
- 第 367 頁「監視 DNS 伺服器狀態」
- 第 368 頁「監控分割 DNS 伺服器狀態」
- 第 370 頁「檢視 DNS 代理快取項目」
- 第 368 頁「檢視及管理靜態 DNS 快取項目」

關於 DNS 代理

IPv4 介面可以在 IPv4 網際網路上命名解析度，而 IPv6 介面僅可透過 DNS 代理在 IPv6 網際網路上命名解析度。若要允許 IPv4 用戶端存取混合 IPv4 和 IPv6 介面的網路中的 DNS 服務，SonicOS 支援 DNS 代理；請參見 DNS 代理。

DNS 代理



DNS 代理功能提供透明機制，可讓裝置代表用戶端代理主機名稱解析要求。代理可使用現有 DNS 快取，由您固定設定或動態得知以直接回應查詢。

代理可選擇性根據部分或完整網域規格，將 DNS 查詢重新導向到特定 DNS 伺服器。這在 VPN 通道或 PPPoE 虛擬連結提供多個網路連接時特別實用，並且需要將部分 DNS 查詢導向到一個網路，其他查詢導向到其他網路

透過 DNS 代理，LAN 子網路裝置使用 SonicWall 安全設備作為 DNS 伺服器，並傳送 DNS 查詢至安全設備。安全設備會將 DNS 查詢代理到實際的 DNS 伺服器。安全設備在此方式下是網路 DNS 流量的集中管理點，提供功能在單點管理網路的 DNS 查詢。

附註：若要保持安全性，傳入 DNS 查詢僅在存取規則和 DPI 檢查之後進行代理。

當 DNS 代理在介面上啟用時，SonicOS 會自動新增一個允許規則。如需與介面關聯的存取規則，請參見 *SonicOS 原則*。

當 **DNS 代理透過 TCP** 啟用時，還會自動新增另一個允許規則。

主題：

- 第 364 頁「支援的介面」
- 第 364 頁「DNS 伺服器活性偵測和容錯移轉」

- 第 364 頁「DNS 快取」
- 第 365 頁「DHCP 伺服器」
- 第 365 頁「啟用記錄設定」
- 第 365 頁「監視封包」

支援的介面

在實體介面、VLAN 介面或 VLAN 轉接介面上支援 DNS 代理功能。每個介面的區域應僅是 LAN、DMZ 或 WLAN。

DNS 伺服器活性偵測和容錯移轉

設定多個 DNS 伺服器時，為判定「最佳的」伺服器，SonicOS 會考慮以下因素：

- DNS 伺服器優先順序。
- DNS 伺服器狀態 (啟動、停機、未知)
- 容錯移轉後的持續時間。

DNS 快取

在 DNS 代理中，DNS 快取記憶體會儲存一般最常使用的網域和主機位址，並且當其接收符合 DNS 快取中的網域的 DNS 查詢時，安全設備會使用快取記錄直接回應用戶端，而無須處理 DNS 查詢和回應代理。

NS 快取有兩種：

靜態	由您手動設定。
動態	由 SonicOS 自動得知。對於每個 DNS 查詢，SonicOS DNS 代理會在 URI 進行深度檢查並記錄對快取的有效回應。

DNS 查詢與現有快取項目相符時，SonicOS DNS 代理會使用快取的 URI 直接回應。這通常降低網路流量，從而提升整體網路效能。

DNS 代理快取大小上限

靜態 DNS 代理快取大小

靜態 DNS 代理快取項目大小一律為 256，沒有平台差異。除非手動刪除，否則靜態 DNS 快取永遠不會遭到刪除。

動態 DNS 代理快取大小

動態 DNS 代理快取大小取決於平台，如動態 DNS 快取大小表格中所示。

動態 DNS 快取大小

平台	最大快取大小
SM 9600/SM 9400	4096
SM 9200	2048

動態 DNS 快取大小

平台	最大快取大小
NSA 6600/NSA 5600/NSA 4600	2048
NSA 3600/NSA 2600/NSA 2650	1024
TZ600	512
TZ500/TZ500 W/TZ400/TZ400 W/ TZ300/TZ300 W	512
SOHO W	512

如果安全設備嘗試新增項目至代理快取時已達到 DNS 代理快取大小上限，則安全設備會進行下列操作:

1 刪除 DNS 代理快取項目中到期時間最早者。

2 新增新的 DNS 代理快取項目。

DNS 快取的高可用性狀態同步

DNS 代理支援可設定狀態的 DNS 代理快取同步處理作業。系統動態新增、刪除或更新 DNS 代理快取時，DNS 代理會與閒置的安全設備保持同步。

DHCP 伺服器

在介面上啟用 DNS 代理時，裝置需要將做為 DNS 伺服器位址的介面 IP 推送至用戶端，所以 DNS 伺服器必須手動設定，並在 **DNS/WINS** 標籤上的 **DHCP 伺服器**設定中，使用介面位址做為 **DNS 伺服器 1** 位址。**動態範圍設定**對話中的**介面預先填入**選項，可使得這容易設定；如果所選介面已啟用 DNS 代理，DNS 伺服器 IP 會自動新增到 DNS/WINS 頁面。如需如何設定 DHCP 伺服器，請參閱第 448 頁「設定固定 DHCP 項目」。

啟用記錄設定

有數個事件與 DNS 代理相關，且需要按照 *SonicOS 調查*中所述進行設定。

監視封包

DNS 代理的程序是透過儀表板 > 封包監控進行監視。如需封包監控的相關資訊，請參閱 *SonicOS 調查*。

啟用 DNS 代理

若要啟用 DNS 代理，必需先在**網路 > DNS 代理**頁面中全域執行，然後再於每個介面中執行。這提供逐步控制，單獨為不同網路區段啟用功能。

若要啟用 DNS 代理：

1 導覽到**網路 | DNS 代理**。

2 選取**啟用 DNS 代理**。 預設情況下未勾選此選項。

3 按一下**接受**。

4 導覽到**網路 | 介面**。

5 按一下介面的**編輯**圖示，以啟用 DNS 代理。將顯示**編輯介面**對話方塊。

6 按一下**進階**。

7 選取**啟用 DNS 代理**。此選項僅在 DNS 代理全域啟用時才顯示。

8 按一下**確定**。

9 對每個介面重複步驟 5 到步驟 8，以啟用 DNS 代理。

10 按一下**接受**。

如需與介面相關聯的存取規則，請參閱 *SonicOS 原則指南*。

設定 DNS 代理設定

若要設定 DNS 代理：

1 導覽至**網路 | DNS 代理 | DNS 代理設定**。

2 在 **DNS 代理模式**中，選擇用於在安全設備和 DNS 伺服器間傳送/接收 DNS 代理封包的 IP 版本:

- **IPv4 至 IPv4** (預設)
- **IPv4 至 IPv6**

3 若要允許所有類型的 DNS 要求 (包括 SonicOS 所傳送的堆疊 DNS 封包) 都能經由 DNS 代理處理 (包括利用 DNS 伺服器外的目的地位址轉送 DNS 查詢)，請選取**強制 DNS 代理所有 DNS 請求**。如果這個選項遭到停用，則系統只會處理目的地為 SonicWall 安全設備的請求。 預設情況下未勾選此選項。

附註：這個選項只會對透過 UDP 的 DNS 造成影響。如果這個選項遭到停用，則系統只會啟用目的地為 SonicWall 安全設備的 DNS 代理請求。

4 若是僅透過 UDP 的 DNS 請求，請選擇**啟用 DNS 快取**。預設情況下已核取此選項。

5 按一下**接受**。

附註：有數個進階設定可設定，例如 DNS 代理通訊協定。如需這些設定的更多資訊，請聯絡技術支援。

監視 DNS 伺服器狀態

附註：已設定的 DNS 伺服器會顯示其 IP 位址。如果未設定伺服器，IP 位址為 0.0.0.0。若要設定伺服器，請按下連到**網路 > DNS** 的連結；請參見第 349 頁「設定 DNS 設定」。

您監視 **DNS 伺服器**區段中每個設定的上游 DNS 伺服器的狀態。伺服器狀態取決於伺服器的 DNS 回覆：

啟動 (綠色 LED 燈)	回覆成功。
未知 (黃色 LED 燈)	伺服器尚未收到 DNS 回覆。
中斷 (紅色 LED 燈)	失敗次數超過 20 次的限制。狀態保持中斷直到下一個成功的 DNS 查詢。

將滑鼠移到 LED 上，顯示有關所傳送代理 DNS 封包數和成功 DNS 代理查詢數的更多資訊：

監控分割 DNS 伺服器狀態

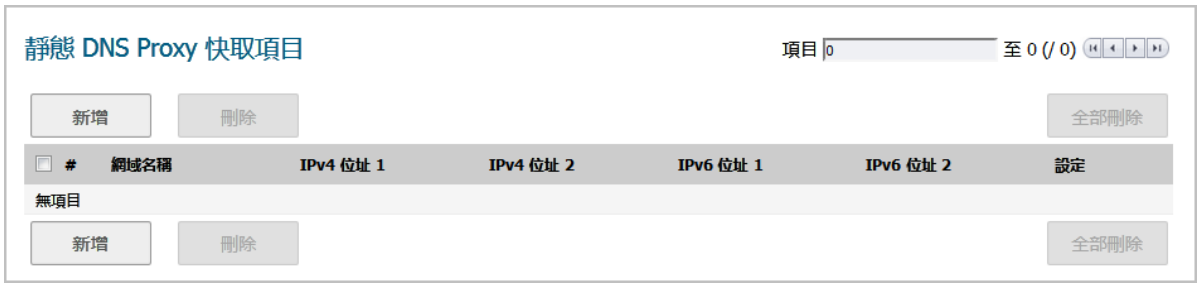
附註：已設定的分割 DNS 伺服器會顯示其 IP 位址。若要設定分割伺服器，請按一下連到**網路 > DNS** 的連結；請參閱第 349 頁「設定 DNS 設定」。

您可在**分割 DNS** 部分中，監控每個已設定的上游 DNS 伺服器狀態。伺服器狀態取決於伺服器的 DNS 回覆：

啟動 (綠色 LED 燈)	回覆成功。
未知 (黃色 LED 燈)	伺服器尚未收到 DNS 回覆。
中斷 (紅色 LED 燈)	失敗次數超過 20 次的限制。狀態保持中斷直到下一個成功的 DNS 查詢。

將滑鼠移到 LED 上，顯示有關所傳送代理 DNS 封包數和成功 DNS 代理查詢數的更多資訊：

檢視及管理靜態 DNS 快取項目



網域名稱	網域的名稱。
IPv4 位址 1	靜態 DNS 快取的主要 IPv4 位址。如未指定，為 0.0.0.0。
IPv4 位址 2	靜態 DNS 快取的次要 IPv4 位址。如未指定，為 0.0.0.0。
IPv6 位址 1	靜態 DNS 快取的主要 IPv6 位址。如未指定，為 ::。
IPv6 位址 2	靜態 DNS 快取的次要 IPv6 位址。如未指定，為 ::。
設定	對於每個項目，包含**編輯**和**刪除**圖示。

若要新增靜態 DNS 快取項目：

1 導覽到**網路 | DNS 代理**。

2 捲動至**靜態 DNS 代理快取項目**。

3 按一下表格上方或下方的**新增**按鈕。**新增靜態 DNS 快取**對話隨即顯示。

4 在**網域名稱**欄位輸入名稱。

5 為 IPv4 靜態 DNS 快取，在 **IPv4 位址 1** 欄位中輸入主要 IPv4 位址。

6 選擇性，為 IPv4 靜態 DNS 快取，在 **IPv4 位址 2** 欄位中輸入次要 IPv4 位址。

7 為 IPv6 靜態 DNS 快取，在 **IPv6 位址 1** 欄位中輸入主要 IPv6 位址。

8 選擇性，為 IPv6 靜態 DNS 快取，在 **IPv4 位址 2** 欄位中輸入次要 IPv6 位址。

9 按一下**確定**。

10 若要新增其他靜態 DNS 快取項目，請重複步驟 4 到步驟 9。

11 按一下**取消**。

刪除靜態 DNS 快取項目

若要刪除靜態 DNS 快取項目：

1 按下項目的**刪除**圖示。

若要刪除兩個或以上的靜態 DNS 快取：

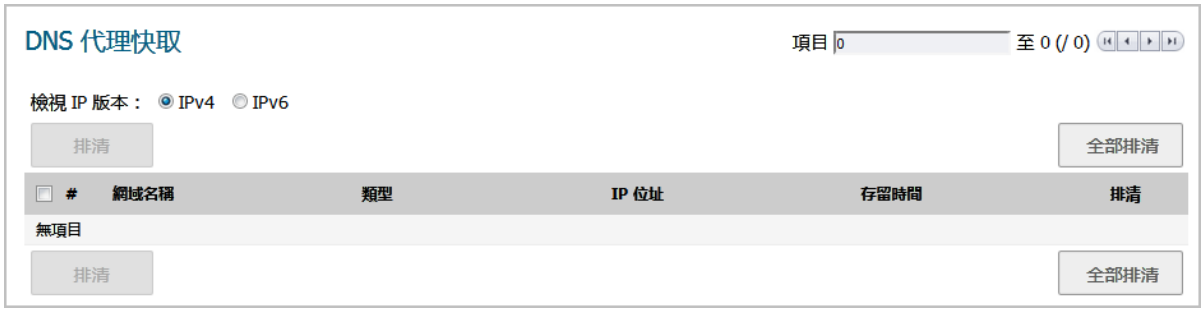
1 勾選要刪除項目的核取方塊。**刪除**按鈕即可使用。

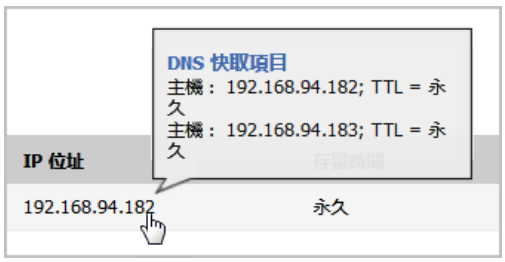
2 按一下**刪除**按鈕。

若要刪除所有靜態 DNS 快取：

1 按一下**全部刪除**按鈕。

檢視 DNS 代理快取項目



檢視 IP 版本	選擇 **IPv4** 或 **IPv6**。
網域名稱	DNS 伺服器的名稱。
類型	**動態** **靜態**
IP 位址	DNS 伺服器的 IPv4 或 IPv6 位址。將滑鼠放在項目上即顯示該項目的**主機**和存留時間 (**TTL**) 資訊: 
存留時間	您可以 • 在 *n 分 x 秒內到期* (動態 DNS) • **已過期** (動態 DNS) • 永久 (靜態 DNS)
排清	每個項目的**排清**圖示。

動態 DNS 快取是在 DNS 代理程序期間自動新增；靜態 DNS 快取是在您設定時新增的。動態 DNS 快取有 TTL 值並且可以排清。靜態 DNS 快取必須刪除；請參見第 369 頁「刪除靜態 DNS 快取項目」

排清動態 DNS 快取項目

若要排清動態 DNS 快取項目：

1 按下項目的**排清**圖示。

若要排清兩個或以上的動態 DNS 快取：

1 勾選要刪除項目的核取方塊。**排清**按鈕即可使用。

2 按一下**排清**按鈕。

若要排清所有動態 DNS 快取項目：

1 按一下**排清全部**按鈕。

20

設定路由通告和路由原則

關於路由

SonicWall 安全設備支援下列路由通訊協定:

- RIPv1 (路由資訊通訊協定)
- RIPv2
- OSPFv2 (開放最短路徑優先)
- OSPFv3
- PBR (原則式路由)

主題：

關於度量和管理距離

度量和管理距離會影響網路效能、可靠性和選擇的電路。

關於度量

*度量*是指派給固定和動態路由的加權成本。度量的用途是在數個路由中決定最適合的一個，通常是度量最低的閘道。這個閘道通常是預設的閘道。

度量值介於 1 到 254 之間，請參閱度量值描述表格。度量值越低越好，低度量優先於高成本。SonicOS 始終使用由 Cisco 定義的度量值，用於直接連接介面、固定編碼路由和所有動態 IP 路由協定。

度量值描述

度量值	說明
1	固定路由
5	EIGRP 摘要
20	外部 BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP

度量值描述

度量值	說明
140	EGP
170	外部 EIGRP
200	內部 BGP

關於管理距離

*管理距離*是一個值，用於決定使用哪一個路由來源，供來源不同的兩個相同路由使用。管理距離值越低，路由受到信任的程度就越高。

設定管理距離後，在配合下列情況選擇要使用的路由時，僅有 ZebOS 元件會使用管理距離:

- 填入 PBR
- 固定路由和某個從特定路由通訊協定收到的路由出現競爭情形時，需重新分配到其他路由通訊協定。

PBR 本身在排定路由的優先順序時不會使用管理距離，因此除非已使用動態路由，否則固定路由所設的管理距離不會發生作用。使用動態路由時，管理距離會提供一種機制，其中 PBR 中定義的固定路由，會與通訊協定 (例如 OSPF、RIP 或 BGP) 可能收到的對等動態路由進行比較。根據預設，網路服務模組 (NSM) 中置入的 PBR 固定路由，其管理距離等於為 PBR 路由定義的度量。使用自訂的管理距離值時，每個固定路由的管理距離可選擇設為不同的值。

舉例來說，如果某個簡單 (只有目的地) 的固定路由 (例如目的地為 `14.1.1.0/24`) 被定義為度量值 10，且管理距離設為預設值 (**自動**)，則系統在 NSM 填入該路由時，採用的管理距離和度量值就是 10。

現在我們假設從 RIP 和 OSPF 收到了同樣的 `14.1.1.0/24` 路由。RIP 路由預設的管理距離為 120，OSPF 路由則為 110，因此系統會優先採用預設的管理距離 (即度量) 為 10 的固定路由，NSM 不會在 PBR 中填入 OSPF 或 RIP 路由。如果固定路由的管理距離設為 115 (度量值同樣為 10)，則系統會優先採用 OSPF 路由 (管理距離為 110) 而不是固定路由，但系統仍然不會優先採用 RIP 路由。如果沒有 OSPF 路由，NSM 會撤銷 OSPF 路由，而且不會填入 RIP 路由，因為 RIP 路由的 120 AD 大於固定路由的 115 AD。

如果是上述以外的情況，PBR 中仍會優先採用固定路由，因為系統在新增所有從 NSM 填入 PBR 的非預設路由時，都會採用 110 的度量值，而這個值遠大於固定路由的度量值 (10)。

如果固定路由的管理距離為 110，度量值 > 110，則將固定路由度量與任何競爭的 OSPF 路由的 OSPF 度量 (或成本) 進行比較時，OSPF 會使用傳遞到 NSM 的度量值。

路由通告

SonicWall 安全設備會使用 RIPv1 或 RIPv2，向網路中的其他路由器通告其固定和動態路由。安全設備與遠端 VPN 閘道之間的 VPN 通道狀態發生的變化也會反映在 RIPv2 通告中。請根據您路由器的功能或設定，選擇要使用 RIPv1 或 RIPv2。

- RIPv1 是舊版通訊協定，功能較少，並且透過廣播而不是多點傳送方式傳送封包。
- RIPv2 是新版通訊協定，以多點傳送的方法將路由表格傳送到相鄰路由器和路由標籤來學習路由時，會包含子網路資訊。RIPv2 封包可向後相容，且部分提供監聽多點傳送封包選項的 RIPv1 實作也接受 RIPv2 封包。「啟用 RIPv2 (廣播)」選項會以廣播方式而不是多點傳送方式傳送封包，適用於混合了 RIPv1 和 RIPv2 路由器的異質網路。

ECMP 路由

SonicOS 6.5 支援等價多路徑 (ECMP) 路由，這種路由採用的技術能夠沿著多個成本相同的路徑路由封包。轉送引擎會藉由下一個躍點辨識路徑。轉送封包時，路由器必須決定要使用哪一個「下個躍點」(路徑)。多重路徑路由可用於連接大多數的路由通訊協定。

在 SonicOS 中，您可以使用 ECMP 路由，為特定路由的目的地指定多個下個躍點。在具有大量需求的環境中，採取這種做法的原因有好幾種。在大多數情況下，路由器可以只使用一個 ISP，並且因為某些原因，在第一個 ISP 故障時使用其他 ISP。多重路徑的另一個應用方式，就是讓某個路徑保持在待命狀態，且只有在頻寬需求超過預先設定的閾值時才予以啟用。SonicOS 最多可支援 4 個下個躍點路徑。

包括開放最短路徑優先 (OSPF)，和中間系統到中間系統 (ISIS) 等多種路由通訊協定，都明確允許 ECMP 路由。部分路由器實作也允許透過 RIP 和其他路由通訊協定使用等價多路徑。

基於原則的路由

簡單固定路由項目指定了如何處理符合特定標準（例如目的地位址、目的地遮罩、轉送流量的閘道、閘道所在的介面以及路由度量等）的流量。這種固定路由方法可滿足大多數固定要求，但僅限於根據目的地位址進行轉送。

基於原則的路由 (PBR) 可用於建立擴充的固定路由，從而提供更加靈活和精確的流量處理功能。SonicOS PBR 允許基於來源位址、來源網路遮罩、目的地位址、目的地網路遮罩、服務、介面和度量進行比對。利用此路由方法，可基於大量使用者定義的變數實現對轉送的完全控制。

FQDN 無法作為 PBR 項目的來源或目的地使用。

原則式 TOS 路由

SonicOS 支援原則式 TOS (服務類型) 路由，這種情況發生在透過服務類型 (TOS) 和 TOS 遮罩值定義原則式路由 (PBR) 原則時。經過定義後，系統在比對路由時，就會將 TOS 和遮罩值，與 IP 標頭中相關的 IP 封包 TOS/DSCP 欄位進行比較。

TOS 值的比較對象為 IP 封包標頭中的 8 位元欄位 (如需這個標頭的相關資訊，請參閱 *RFC 2474，區分服務*以及 *RFC 2168，明確壅塞通知*)。TOS 值可用於定義和量化效能需求 (例如尖鋒頻寬) 相關的服務，和以相對效能為基礎的服務 (例如類型區分)。

TOS 路由不同於現有的 SonicOS QoS 標記，QoS 標記不會影響封包路由，也不能根據傳入封包的 TOS 欄位，以不同的方式轉送封包。 TOS 路由會讓原則路由定義要與傳入封包進行比較的 TOS 值/TOS 遮罩配對，實現獨特的轉送方式，藉此提供上述功能。 系統只會在封包進入安全設備時套用 TOS 路由。

使用 TOS 路由後，就可能透過相同的來源 IP、目的地 IP 和服務值，但不同的 TOS/TOS 遮罩值來定義多個原則路由。這可讓具有已標記 TOS 欄位的封包，依據傳入封包內的 TOS 欄位值，以不同的方式轉送。

所有在 SonicOS 6.5 推出前定義的 PBR 原則路由，都沒有為 TOS/TOS 遮罩定義任何值。同樣地，TOS/TOS 遮罩欄位的預設值為零 (無定義值)。

系統會優先處理 TOS 值不是零的原則路由，再處理所有僅有目的地的簡單路由，但處理順序不會優先於定義來源或服務的政策路由。比較兩個 TOS 原則路由時，如果兩個路由皆具備同一組來源、目的地和服務值 (無論是經過定義或未經定義)，系統會先處理 TOS 遮罩位元數較大的 TOS 路由 (設為 1)，再處理 TOS 遮罩位元數設定值較小的 TOS 路由。

一般的 PBR 路由優先順序 (由高至低) 如下所示，排列順序是以 TOS 值不是任一或零的原則欄位為基準:

目的地、來源、服務、TOS
目的地、來源、服務
目的地、來源、TOS
目的地、來源
目的地、服務、TOS
目的地、服務
目的地、TOS
目的地
來源、服務、TOS
來源、服務
來源、TOS
來源
服務、TOS
服務
TOS

以 PBR 度量為基礎來排列的優先順序

SonicOS 可將度量加權成本指派給原則式路由 (PBR) 路由原則，進而能夠將設定好的度量值的路由優先順序提前，高於系統預設使用的路由特異性。度量值介於 0 到 255 之間。度量值越低越好，度量值越低，優先順序就越高。

一般的 PBR 路由優先順序 (由高至低) 如下所示，排列順序是以 TOS 值不是任一或零的原則欄位為基準:

目的地、來源、服務、TOS
目的地、來源、服務
目的地、來源、TOS
目的地、來源
目的地、服務、TOS
目的地、服務
目的地、TOS
目的地
來源、服務、TOS
來源、服務
來源、TOS
來源
服務、TOS
服務
TOS

在這 15 種分類中，系統會進一步根據定義的路由項目的累計特異性，來排定路由的優先順序。對於來源和目的地欄位，系統會計算位址物件代表的 IP 位址數量，藉此評估特異性。舉例來說，10.0.0.0/24

這個網路位址物件會包含 256 個 IP 位址，而 10.0.0.0/20 這個網路位址物件則代表 4096 個 IP 位址 /24 (24 位元) 網路首碼較長時，代表主機 IP 位址較少，而且較為明確具體。

新的度量加權選項可將設定好的度量值的優先順序提前，讓其順序優於路由特異性。啟用這個選項後，系統在排定優先順序時所用的設定如下所示 (由高至低):

1 路由類型 (由來源、目的地、服務和其值不是「任一」或零的 TOS 欄位組合而定)

2 度量值

3 來源、目的地、服務和 TOS 欄位的累計特異性

基於原則的路由和 IPv6

如需 SonicOS 的 IPv6 實作的完整資訊，請參見第 761 頁「IPv6」。

在**網路 | 路由**上選取路由原則的 IPv6 位址物件和閘道，即可讓 IPv6 完全支援原則式路由。您可以在**路由原則**表格中切換查看 **IPv4** 和 **IPv6** 項目。

下一代路由資訊通訊協定 (RIPng) 是用於 IPv6 的資訊路由通訊協定，它允許路由器通過基於 IPv6 的網路交換用於計算路由的資訊。

如需路由通告的資訊，請參見第 373 頁「路由通告」。如需設定路由原則的資訊，請參見第 373 頁「路由通告」。

OSPF 和 RIP 進階路由服務

除了基於原則的路由和 RIP 通告以外，SonicOS 還提供了啟用進階路由服務 (ARS) 的選項。進階路由服務為路由資訊通訊協定 (RIPv1 - RFC1058) 和 (RIPv2 - RFC2453) 以及開放最短路徑優先 (OSPFv2 - RFC2328) 提供完整的通告和監聽支援。僅對需要支援上述一種或兩種動態路由通訊協定的環境啟用進階路由服務。

各種規模的網路將 RIP 和 OSPF 廣泛用於實現自動化路由指派過程的內部閘道通訊協定 (IGP)。RIP 通常用於較小規模的網路，OSPF 則用於較大規模的網路，但網路規模不是確定通訊協定適用性的唯一要素，還應考慮網路速度、互操作性要求及整體相對複雜度等其他要素。RIPv1 和 RIPv2 均受 ARS 支援，二者之間的最大區別在於，RIPv2 支援 VLSM（可變長度子網路遮罩）、身分驗證和路由更新。路由資訊通訊協定差異表格說明了 RIPv1、RIPv2 和 OSPFv2/OSPFv3 之間的主要差異:

路由資訊通訊協定差異

	RIPv1	RIPv2	OSPFv2/OSPFv3
通訊協定度量	距離向量	距離向量	連結狀態
最大躍點數	15	15	無限制
路由表更新	定期廣播完整的路由表，融合速度較慢	定期廣播或多點傳送完整的路由表，融合速度較慢	多點傳送連結狀態通告（根據變化觸發），融合速度較快
支援的子網路大小	僅基於類別 (a/b/c) 的子網路支援	僅基於類別	VLSM
自發系統拓撲	不可分割、扁平	不可分割、扁平	基於區域，允許分段和彙總

主題：

- 第 377 頁「關於路由服務」
- 第 380 頁「OSPF 術語」

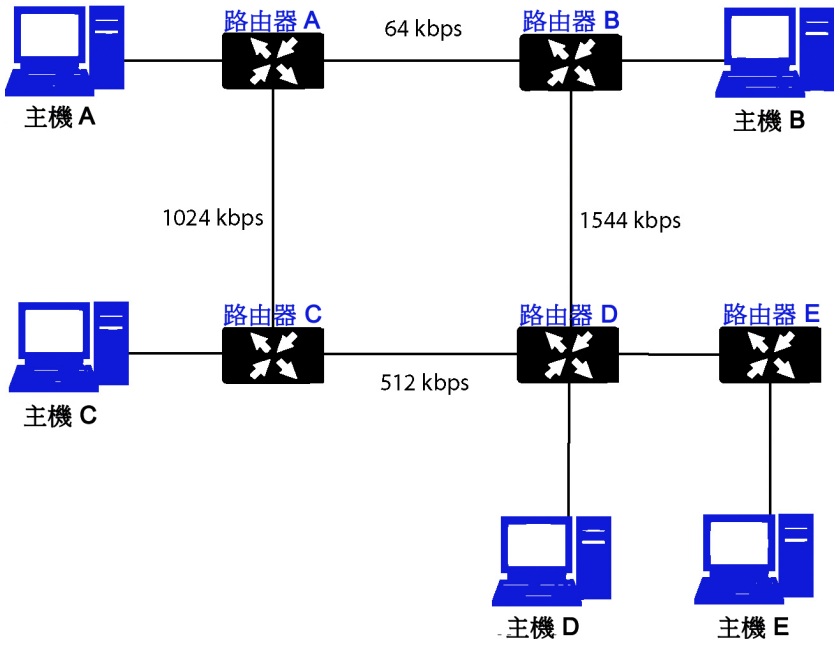
關於路由服務

主題：

通訊協定類型

距離向量通訊協定（例如 RIP 基礎路由）僅度量躍點數，而連結狀態通訊協定（例如 OSPF）在確定度量時會考慮連結狀態。例如，OSPF 用於確定介面度量的方法是將其參考頻寬（預設為 100mbit）除以介面速度 - 連結速度越快，費用越低，路徑的優先度越高。可考慮決定最低成本路由的範例網路中所顯示的範例網路：

決定最低成本路由的範例網路



在決定最低成本路由的範例網路中顯示的範例網路中，使用 RIP 時，如果主機 A 想要到達主機 B，費用最低的路由是從路由器 A 到路由器 B 之間相對較慢的 64kbps 連結。使用 OSPF 時，從路由器 A 到路由器 B 的費用為 1562，而從路由器 A 到路由器 C 到路由器 D 再到路由器 B 的費用為 364，因此後者成為優先路由。

最大躍點數

RIP 實施了 15 個躍點的限制，以防止在以下情況可能發生的路由迴圈：由於設定錯誤或融合速度過低的原因通過網路廣播和傳播錯誤的（例如失效的）路由資訊。在決定最低成本路由的範例網路的範例中，考慮路由器 D 與路由器 E 之間的連結發生故障且沒有部署安全措施的情形：

- 路由器 A 的路由資訊表明，它可以通過路由器 B 或路由器 C 以度量 3 到達網路 E。
- 當路由器 D 與路由器 E 之間的連結發生故障，並且路由器 A 廣播自己的路由資訊時，路由器 B 和路由器 C 確定，它們可通過路由器 A 以度量 4 到達網路 E。
- 路由器 B 和路由器 C 廣播其資訊，路由器 D 收到廣播資訊並確定它可通過路由器 B 或路由器 C 以度量 5 到達網路 E。
- 這一迴圈持續進行，直至達到躍點數 16（極限值）為止。

針對這種情況，RIP 通常還會採取其他措施，包括：

- 第 378 頁「水平分割」
- 第 378 頁「位置反轉」
- 第 378 頁「路由表更新」
- 第 378 頁「支援的子網路大小」
- 第 379 頁「自發系統拓撲」

水平分割

一種預防機制，使用這種機制時，透過某個介面得知的路由資訊不會傳送回同一介面。這種機制在廣播連結上通常有效，但對於框架轉接等通常可使用單個連結到達兩個單獨的自發系統的非廣播連結而言，則不起作用。

位置反轉

也稱為「路由中毒」，是水平分割的擴充形式，使用這種機制時，將以度量 16（無法達到）通告網路，以確保不會傳播錯誤的備用路由。

OSPF 不一定需要實施躍點數限制，因為它不會通告整個路由表，而是通常僅在發生變更時傳送連結狀態更新。OSPF 在較大型的網路中擁有重要優勢，因為它的融合速度更快，產生的更新流量更少，且支援的躍點數沒有限制。

路由表更新

如前所述，傳送整個路由表的做法會引入融合速度較慢、頻寬使用較高和增加出現失效路由資訊的可能性等問題。RIPv1 以規定的間隔（通常每 30 秒一次）廣播自己的整個路由表，RIPv2 可能採用廣播或多點傳送方式，而 OSPF 僅在網路結構發生變化時多點傳送連結狀態更新。OSPF 還有一項優勢，即使用指定的路由器 (DR) 在多路存取網路中形成臨近（後面將詳細介紹這些概念），以避免必須將更新傳送到整個網路。

支援的子網路大小

最早將 RIPv1 在網路嚴格劃分為 A 類、B 類和 C 類（以及後來的 D 類和 E 類）時實施。

A 類 `1.0.0.0` 到 `126.0.0.0` (保留 `0.0.0.0` 和 `127.0.0.0`)

- 最左邊位 0；7 個網路位；24 個主機位

- 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh（8 位分類子網路遮罩）
- 126 個 A 類網路，每個具有 16,777,214 個主機

B 類 128.0.0.0 至 191.255.0.0

- 最左邊位 10；14 個網路位；16 個主機位
- 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh（16 位分類子網路遮罩）
- 16,384 個 B 類網路，每個具有 65,532 個主機

C 類 192.0.0.0 至 223.255.255.0

- 最左邊位 110；21 個網路位；8 個主機位
- 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh（24 位分類子網路遮罩）
- 2,097,152 個 C 類網路，每個具有 254 個主機

D 類 225.0.0.0 到 239.255.255.255 (多點傳送)

- 最左邊位 1110；28 個多點傳送位址位
- 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm

E 類 240.0.0.0 到 255.255.255.255 (保留)

- 最左邊位 1111；28 個保留位址位
- 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

已證明這種位址指派方法效率非常低，因為它在分段方法（子網路劃分）和通過 VLSM - 可變長度子網路遮罩的方式進行彙總（超網劃分或 CIDR - 無類別網域間路由）兩方面都不具備靈活性。

VLSM 受 RIPv2 和 OSPF 支援，可用於通過網路的類別表示將較大的網路劃分為較小的網路：

> 例如，以分類網路 10.0.0.0/8 為例，並為其指派一個 /24 子網路遮罩。此子網路劃分將來自主機範圍的額外 16 位指派給網路範圍 (24-8=16)。若要計算此子網路劃分所提供的額外網路數量，需要對 2 求額外位數次方：2^16=65,536。這樣，您可以獲得 65,536 個網路，其中每個網路擁有 254 個可用主機，而不是獲得一個擁有 1670 萬個主機（這一數字通常超過了大多數 LAN 的需求）的網路。

VLSM 還可用於路由彙總 (CIDR)：

> 例如，您有 8 個 C 類網路：192.168.0.0/24 到 192.168.7.0/24。您可以提供單個到 192.168.0.0/21 的路由，將所有網路包含其中，而不必為其中每個網路提供單獨的路由聲明。

這種功能除了能夠提供更高效和靈活的 IP 位址空間指派以外，還能保持更小規模的路由表和路由更新。

自發系統拓撲

自發系統 (AS) 是處於通用管理控制之下並擁有相同路由特徵的路由器集合。當一組自發系統共用路由資訊時，通常將之稱為自發系統聯盟。（RFC1930 和 RFC975 中詳細解釋了這些概念）。簡而言之，AS 是根據實體網路元素設定的公用性包含這些元素的邏輯劃分。

對於 RIP 和 OSPF 而言，無法將 RIP 自發系統分段，且所有路由資訊都必須通過整個 AS 進行通告（廣播）。這可能會加大管理難度，並可能導致過多的路由資訊流量。另一方面，OSPF 採用了區域的概念，允許通過在邏輯上可管理的分段來控制 AS 內的資訊共用。區域 ID 是一個管理識別碼。OSPF 區域從主幹區域（區域 0 或 0.0.0.0）開始，其他所有區域必須連接到此主幹區域（儘管會有例外）。這種對路由 AS 分段的功能有助於確保 AS 不會變得過大，以致於無法管理，或者變得計算過於密集，以致於路由器無法進行處理。

OSPF 術語

大體上，OSPF 的設定和維護比 RIP 更加複雜。以下概念對於理解 OSPF 路由環境至關重要。

- **連結狀態** - 與 OSPF 相關時，連結是路由器上的輸出介面，此狀態描述此介面的特徵，例如它的成本。將以連結狀態通告 (*LSA*) 的形式傳送連結狀態，此通告包含在連結狀態更新 (*LSU*) 封包（五種 OSPF 封包之一）內。
- **成本** - 通過指定連結傳送封包所需開銷的量化。成本的計算方法為：參考頻寬（通常為 100mbit 或 10^8 位元）除以介面速度。成本越低，連結的優先順序越高。一些常見的路徑成本如不同介面的成本計算表格中所示：

  不同介面的成本計算

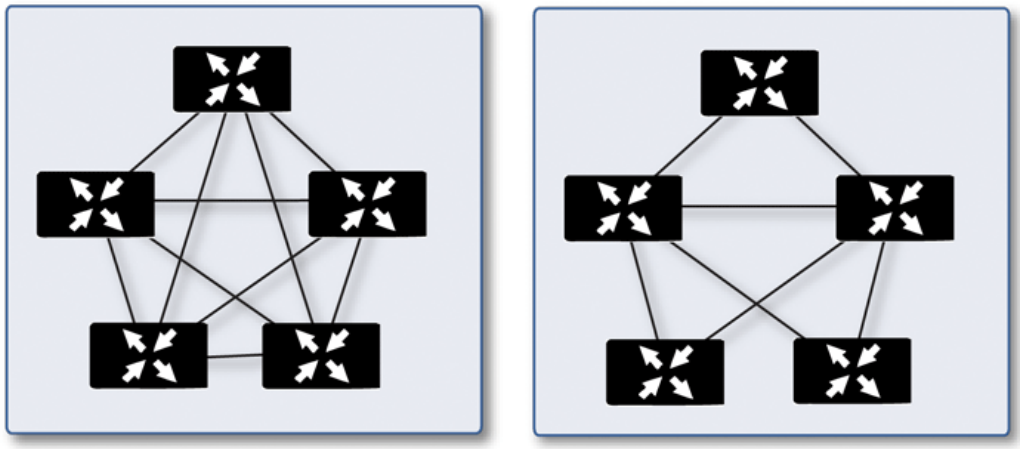
介面	除以 10^8（100mbit）= OSPF 成本
快速乙太網路	1
乙太網路	10
T1（1.544mbit）	64
DSL（1mbit）	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

- **區域** - 由 OSPF 路由器組構成的網路將共用共同的連結狀態資料庫。OSPF 網路必須必須圍繞骨幹區域（區域 0 或 0.0.0.0）構建，所有其他區域必須連接到骨幹區域（除非使用虛擬連結 - 通常不建議這樣做）。區域指派特定於 OSPF 路由器上的介面；換言之，擁有多個介面的路由器可以將這些介面設定用於相同或不同的區域。
- **鄰居** - 通過傳送問候封包，公用網路區段上的 OSPF 路由器可以成為鄰居。問候封包將充當某種形式的通告和識別，如果兩個 OSPF 路由器擁有某些共同的特徵，它們將在其他路由器的問候封包中看到自己的路由器 ID 後成為鄰居。*DR*（指定路由器）和 *BDR*（備份指定路由器）推選過程也會用到問候封包。兩個路由器要成為鄰居，它們必須有的共同特徵包括：
  - **區域 ID** - 區域 ID 用一個 32 位元值（通常以 IP 位址格式表示）識別 OSPF *區域*。OSPF 至少需要骨幹區域、區域 0（或 0.0.0.0）才能執行。
  - **驗證** - 通常，可以將驗證類型設定為「無」、「簡單文字」或 MD5。如果使用「簡單文字」，應僅將驗證其用於識別目的，因為它會以明文形式傳送。為了確保安全，應使用 MD5。
  - **計時器間隔** -「Hello」和「Dead」間隔必須相同。Hello 間隔指定 Hello 封包之間的秒數（作為一種存留機制），Dead 間隔指定如果未收到 Hello 封包，之後將路由器視為無法使用的秒數。
  - **虛設常式區標記** - *虛設常式區*是這樣的區域：它只需要單一輸出點，因此不需要外部連結通告的完整清單。為避免不恰當的連結狀態交換，兩個潛在鄰居上的虛設常式區標記必須相同。網路類型是另一個會影響鄰居關係的因素。OSPF 認可以下三類網路：
    - **廣播** - 例如乙太網路。在廣播網路中，可以與廣播網域中的所有其他路由器建立鄰居關係。
    - **點對點** - 例如序列連結。在點對點（或單點對多點）網路中，可以與連結另一端的路由器建立鄰居關係。
    - **NBMA**（非廣播多路存取）- 例如框架轉接。在 NBMA 網路中，必須明顯宣告鄰居。

- **連結狀態資料庫** - 連結狀態資料庫由已在某*區域*內建立*鄰接關係*的*相鄰* OSPF 路由器傳送和接收的 LSA 構成。此資料庫一旦完成，將包含給定區域的所有連結狀態資訊，此時將套用最短路由優先 (SPF) 演算法根據成本來確定所有已連接網路的最佳路由。SPF 演算法採用 Dijkstra 尋路演算法，基本上，此演算法將所有路由器視為圖形中的頂點，然後計算每個頂點之間的成本。
- **鄰接關係** - OSPF 路由器將與鄰近的路由器交換 LSA 以建立 LSDB。將根據網路類型以不同方式建立鄰接關係（參見上文的*鄰居*）。通常，網路類型為廣播（如乙太網路），因此，將通過以類似握手的方式交換 OSPF 封包來建立鄰接關係（參見下文的「OSPF 封包類型」）。為最大限度地減少相鄰路由器之間交換的資訊量，擁有多個 OSPF 路由器的區段（廣播網域）將使用 Hello 封包推選一個指定路由器 (DR) 和一個備份指定路由器 (BDR)。
- **DR**（指定路由器）- 在多路存取區段上，OSPF 路由器將推選一個 DR 和一個 BDR，區段上的所有其他路由器將與此 DR 和 BDR 建立鄰接關係。將根據路由器的 OSPF 優先順序推選 DR，此優先順序是一個可設定的值，範圍為 0（不適用於 DR）到 255。優先順序最高的路由器將成為 DR。在優先順序相同的情況下，路由器 ID 最大（基於介面定址）的路由器將成為 DR。在路由器成為 DR 後，其角色將不會受到爭議，直到它不再可用。

  然後，將在這些鄰接關係的 LSU 內，而不是區段上的每個可能的路由器配對組合之間交換 LSA。請參閱路由鄰接：指定的路由 (DR)。連結狀態更新將由非 DR 路由器傳送至多點傳送位址 `225.0.0.6`，RFC1583 指派了「OSPFIGP 指定路由器」位址。它們還會由 DR 路由器攻擊至多點傳送位址 `225.0.0.5`，所有路由器的「OSPFIGP 所有路由器」將接收 LSA。

  路由鄰接：指定的路由 (DR)



無 DR/BDR 的芳鄰　　含 DR/BDR 的芳鄰

- **OSPF 封包類型** - 五種類型的 OSPF 封包為：
  - **Hello**（1 類 OSPF）- 按一定間隔傳送，以建立和維護與相鄰 OSPF 路由器的關係，以及推選指定路由器。（*在 LSDB 同步的初始化和雙向階段傳送*）。
  - **資料庫說明**（2 類 OSPF）- 在建立鄰接關係時在 OSPF 路由器之間傳送。*在 LSDB 同步的 Exstart 階段*，DD 封包將建立一個用於追蹤 LSA 的 ISN（初始序號），它們將在相鄰 OSPF 路由器之間建立主/從關係。*在 LSDB 同步的 Exchange 階段*，它們包含簡短版本的連結狀態通告。因為 DD 交換可能會跨越多個封包，為確保完整性，將以輪詢（主）和回應（從）的方式進行交換。
  - **連結狀態請求**（3 類 OSPF）- *在 LSDB 同步的 Loading 階段*，將傳送 LSR 封包，以向鄰居請求資料庫更新。這是建立鄰接關係的最後一步。
  - **連結狀態更新**（4 類 OSPF）- 為回應連結狀態請求而傳送，LSU 封包將用連結狀態通告攻擊鄰接關係，以實現 LSDB 同步。

- **連結狀態確認**（5 類 OSPF）- 為確保 LSA 攻擊的可靠性，將確認所有更新。

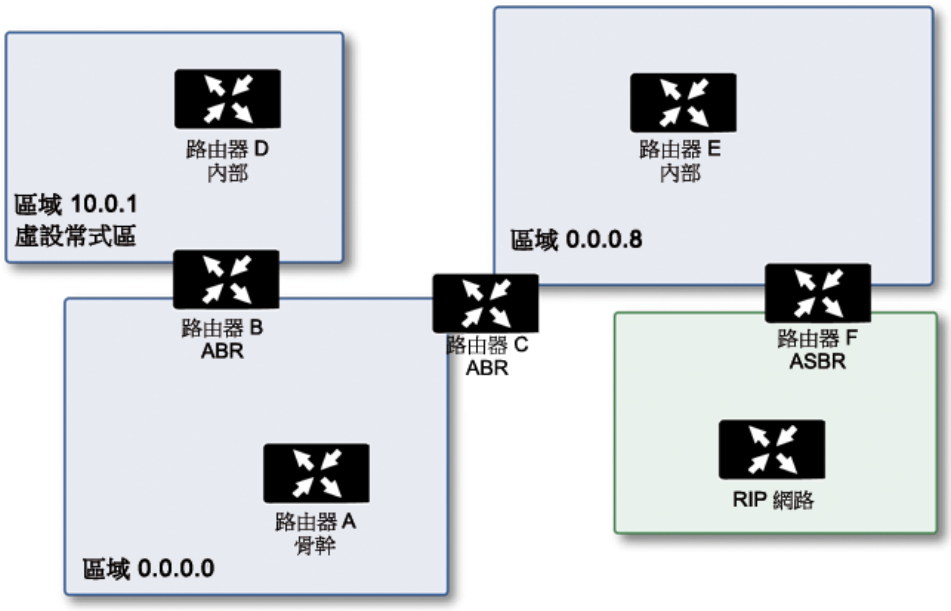
- **連結狀態通告 (LSA)** - 共有 7 種類型的 LSA：
  - 1 類（路由器連結通告）- 由 OSPF 路由器傳送，用於描述指向它所屬的每個區域的連結。僅將 1 類 LSA 攻擊到路由器的區域。
  - **2 類**（網路連結通告）- 由某區域的 DR 傳送，用於描述網路內的路由器組。僅將 2 類 LSA 攻擊到路由器的區域。
  - **3 類**（摘要連結通告）- 由 ABR（區域邊界路由器）在區域之間傳送，用於描述區域內的網路。3 類 LSA 還用於路由彙總目的，且不會傳送到完全虛設常式區。
  - **4 類**（AS 摘要連結通告）- 由 ABR 在區域之間傳送，用於描述不同 AS 中的網路。不會將 4 類 LSA 傳送到虛設常式區。
  - **5 類**（AS 外部連結通告）- 由 ASBR（自發系統邊界路由器）傳送，用於描述不同 AS 中網路的路由。不會將 5 類 LSA 傳送到虛設常式區。有兩種類型的外部連結通告：
    - **外部類型 1** - 在計算連結的度量時，類型 1 封包會將內部連結成本與外部連結成本相加。類型 1 路由始終優先於指向同一目的地的類型 2 路由。
    - **外部類型 2** - 類型 2 封包僅使用外部連結成本來確定度量。當只有一個指向外部 AS 的路由時，通常會使用類型 2。
  - **6 類**（多點傳送 OSPF 或 MOSPF）- 稱之為來源/目的地路由，不同於大多數轉送完全基於目的地的路由的演算法（如 OSPF）的單點傳送資料包。如需 MOSPF 的更多資訊，請參見 *RFC1584 - Multicast Extensions to OSPF*。
  - **7 類**（NSSA AS 外部連結通告）- 由作為 NSSA（參閱「虛設常式區」）的一部分的 ASBR 傳送。

- **虛設常式區** - 虛設常式區是指只需要一個路由（而不是最佳路由）的區域。此區域可能為只擁有單一輸出點的區域，也可能是不需要 SPF 最佳化的區域。必須將虛設常式區中的所有路由器設定為末梢路由器；它們不會接收完整的狀態資料庫並計算 SPF 樹狀目錄，而僅接收摘要連結資訊。

  存在有各種類型的虛設常式區：
  - **虛設常式區** - 標準虛設常式區接收除 5 類 LSA（AS 外部連結通告）以外的所有 LSA。這有助於使 LSDB 較小，並減少路由器上的計算開銷。
  - **完全虛設常式區** - 一種特殊的虛設常式區，將不會向其中傳遞 3 類（摘要連結）、4 類（AS 摘要連結）和 5 類 LSA。僅將區域間路由和預設路由傳送到完全虛設常式區。
  - **NSSA**（非純虛設常式區）- 由 RFC3101 描述，NSSA 是一種混合虛設常式區，它允許使用 7 類 LSA（NSSA AS 外部路由）攻擊 NSSA 內的外部路由，但不接受來自其他區域的 5 類 LSA。在將執行不同 IGP（如 RIP）的遠端站台連接到 OSPF 站台時（在這種情況下不需要將遠端站台的路由重新指派給主 OSPF 站台），NSSA 非常有用。NSSA *ABR*（區域邊界路由器）還能夠將 7 類 LSA 轉譯為 5 類 LSA（只能從 SonicOS CLI 執行此操作，請參見 *SonicOS CLI 參考指南*）。

- **路由器類型** - OSPF 支援 4 種類型的路路由器（基於其角色）。請參見支援 OSPF 的路由器類型範例。

支援 OSPF 的路由器類型範例



- **IR**（內部路由器）- 其介面全部位於同一區域的路由器。內部路由器的 LSDB 僅包含有關它自己的區域的資訊。
- **ABR**（區域邊界路由器）- 介面位於多個區域的路由器。ABR 會為其連上的每個區域 (其中一個區域通常為骨幹區域) 維護 LSDB。
- **骨幹路由器** - 介面連接到區域 0（即骨幹區域）的路由器。
- **ASBR**（自發系統邊界路由器）- 介面連接到非 OSPF AS（如 RIP 網路，它會將外部路由資訊從自身傳送到 OSPF AS）的路由器。

丟棄通道介面

丟棄通道介面是在設定的路由停止時使用不正確的路由來阻止流量傳送出去。傳送到丟棄通道介面的流量部會離開安全設備但是在表面上被丟棄。

儘管丟棄通道介面可以獨立使用，但丟棄通道介面應與 VPN 通道介面一起使用。如果固定路由繫結到通道介面，SonicWall 建議對於相同網路流量設定固定路由繫結到丟棄通道介面。如此一來，若通道介面停止，便會使用第二個固定路由，流量可有效率地丟棄。這可防止資料通過其他路由被轉送。

通過 VPN 通道介面設定路由時，若通道臨時出現故障，也應停用相應的路由項目。SonicOS 針對目的地為 VPN 防護網路的連接查找新路由項目。在無遠端 VPN 網路備用連結的部署中，其他正確的路由項目將無法使用。流量將傳送至錯誤的路由項目，通常為預設路由，這會造成在未加密情況下傳送內部資料等安全問題。

對於無備用連結的部署，應考慮按如下範例設定路由表：

路由 n： 本機 VPN 網路（來源）、遠端 VPN 網路（目的地）、VPN TI(egress_if)
路由 n+1：本機 VPN 網路（來源）、遠端 VPN 網路（目的地）、Drop If(egress_if)

按此範例設定 VPN 通道介面時，流量與丟棄介面相符合且未發出。WVPN 通道介面恢復時，流量也將恢復。

網路 | 路由

如果介面上有路由器，您可以在**管理 | 系統安裝 | 網路 | 路由**頁面上設定 SonicWall 安全設備中的固定路由。您可以建立固定路由原則，並使用這些原則建立固定路由項目，從而基於來源位址、來源網路遮罩、目的地位址、目的地網路遮罩、服務、介面、閘道和度量做出路由決定。透過此功能，可根據大量使用者定義的變數獲得對轉送的完全控制。

主題：

網路 | 路由 > 設定

管理 | 系統安裝| 網路 | 路由 > 設定中顯示的內容，會因為您選取的路由模式而更動:

- **簡單 RIP 通告**
- **進階路由**

簡單 RIP 通告

進階路由

網路 | 路由 > 路由原則

網路 | 路由 > 路由原則會顯示 IPv4 或 IPv6 的所有預設和/或自訂路由。兩個 IP 版本所顯示的內容基本相同，不過 IPv6 會顯示 IPv6 連結本機位址，而不是 IP 位址。

您可以選取下列項目，藉此變更**路由原則**表格中的路由原則檢視畫面:

- **IPv4** 或 **IPv6**
- **檢視**中的其中一個檢視設定:

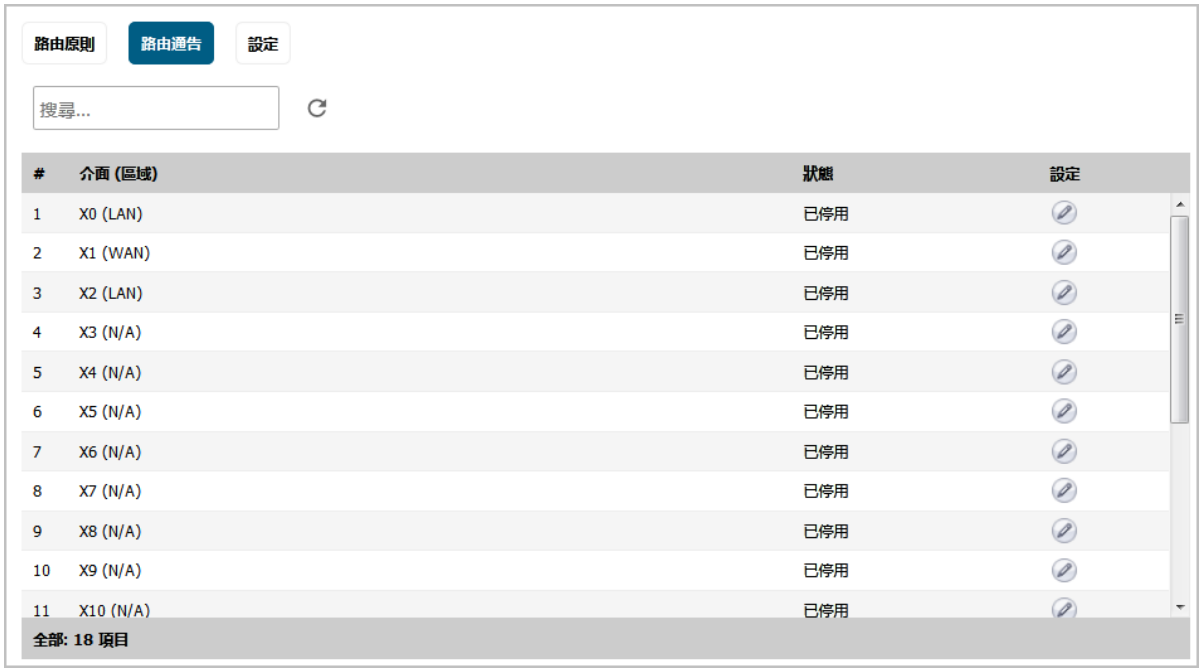
所有類型	包括**自訂原則**和**預設原則**在內的所有路由原則。選取**所有類型**時，**路由原則**表格一開始只會顯示**預設原則**。
自訂原則	您建立的原則。
預設原則	由 SonicOS 建立的原則。

您可以在**搜尋**欄位中輸入來源、目的地或介面，藉此篩選顯示的內容。

欄	路由原則設定
來源	來源的 IP 版本圖示和名稱。
目的地	目的地 IP 位址 (IPv4) 或 MAC 位址 (IPv6)。
服務	為路由原則設定的服務物件。
TOS/遮罩	為路由設定的 TOS 和 TOS 遮罩。
閘道	閘道 IP 位址 (IPv4) 或 MAC 位址 (IPv6)。
介面	為路由原則設定的介面。
度量	為路由優先順序設定的度量。
優先順序	路由原則的優先順序。
探查	是否設定了探查功能。
註解	**註解**圖示包含設定自訂路由時所輸入的註解內容；預設原則為自動新增的路由原則。
設定	**編輯**和**刪除**圖示，預設原則圖示會顯示為灰色。

網路 | 路由 > 路由通告

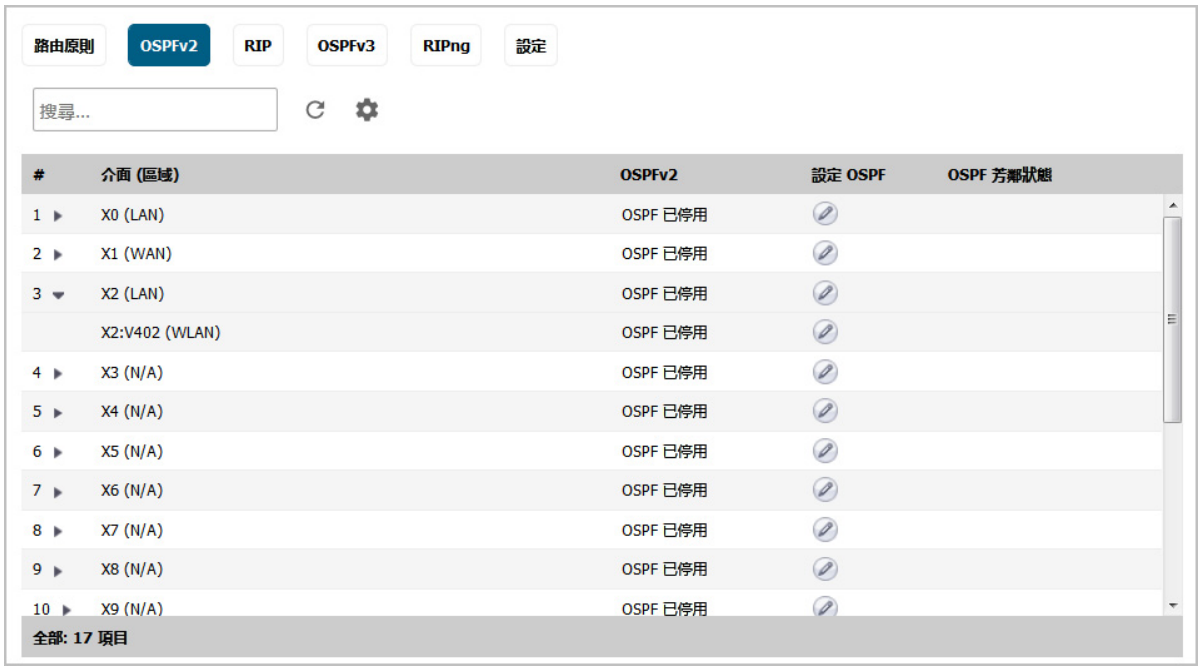
網路 | 路由只有在您針對**路由原則**選擇了**簡單 RIP 通告**時，系統才會顯示**> 路由通告**。



介面 (區域)	為路由通告設定的介面。如果區域尚未設定介面，則 **(區域)** 指定名稱就會顯示為 **(N/A)**。
狀態	**已啟用**或**已停用**。
設定	含**編輯**圖示。

網路 | 路由 > OSPFv2

網路 | 路由 > OSPFv2 僅會在您針對**路由模式**選擇了**進階路由**時才會顯示，其中會提供 OSPFv2 的狀態，並可讓您為介面設定 OSPFv2。



設定	用於顯示**設定**彈出式視窗的圖示，可供您設定預設路由的度量。
介面 (區域)	為 OSPFv2 設定的介面和其區域如果區域尚未設定介面，則 **(區域)** 指定名稱就會顯示為 **(N/A)**。
OSPFv2	指出是否在介面上啟用 OSPF。 • **已啟用 OSPF** • **已啟用 OSPF (被動)** • **已停用 OSPF**
設定 OSPF	用於顯示介面的**編輯**圖示 。
OSPF 芳鄰狀態	用於顯示**狀態**圖示，其中會指出是否有使用中/非使用中的芳鄰；按一下該圖示即可顯示 **OSPFv2 介面芳鄰**彈出式視窗，內有更多該介面的芳鄰詳細資訊。請參閱第 387 頁「網路 | 路由 > OSPFv2 > OSPFv2 介面芳鄰」。

網路 | 路由 > OSPFv2 > OSPFv2 介面芳鄰

按一下介面的**狀態**圖示，就會顯示這個彈出式視窗。

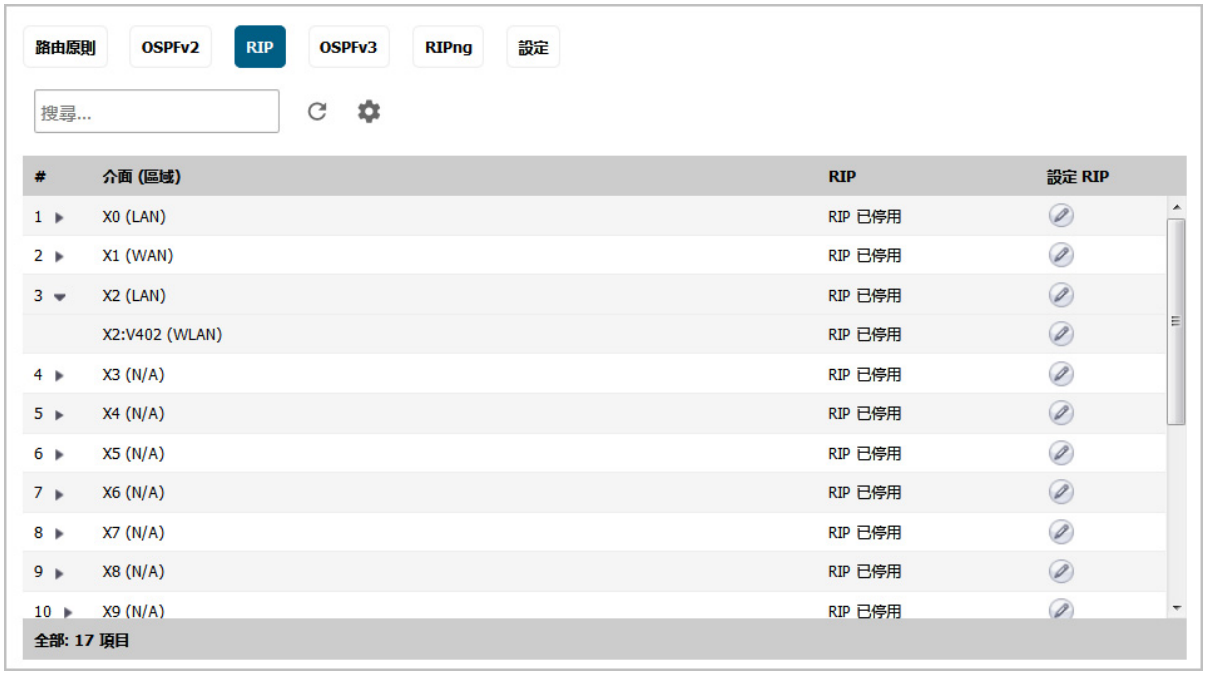
介面 X2:V402 (WLAN) OSPFv2 區域 0.0.0.0 鄰居

路由器 ID	目前狀態	優先順序	IP 位址
192.168.166.1	Full / DR	1	172.16.16.60

路由器 ID	芳鄰的路由器 ID。
目前狀態	OSPFv2 網路芳鄰的狀態 (如有建立): • **啟動** • **雙向** • **ExStart** • **交換** • **載入中** • **完全**
優先順序	芳鄰的路由器優先順序。
IP 位址	芳鄰路由器的 IP 位址。

網路 | 路由 > RIP

網路 | 路由 > RIP 僅會在您針對**路由模式**選擇了**進階路由**時才會顯示，其中會提供 RIP 的狀態，並可讓您為介面設定 RIP。



設定 用於顯示**設定**彈出式視窗的圖示，可供您設定預設路由的度量。

介面 (區域) 為 RIP 設定的介面和其區域如果區域尚未設定介面，則 **(區域)** 指定名稱就會顯示為 **(N/A)**。

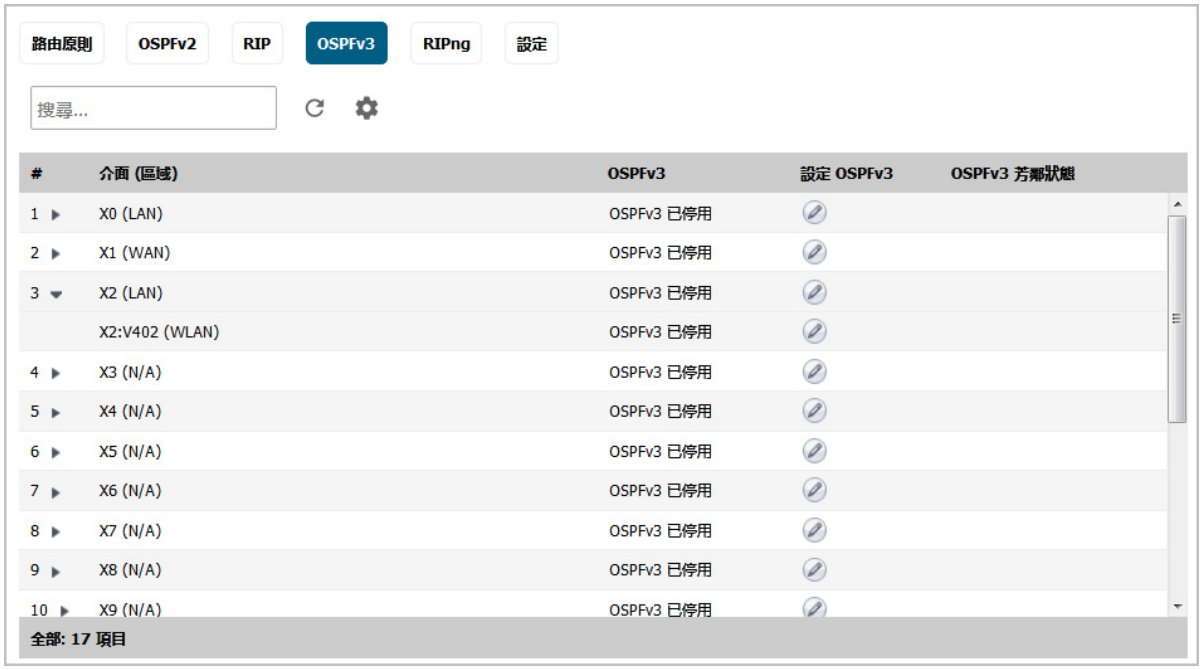
RIP 指出是否在介面上啟用 RIP。

- **已啟用 RIP**
- **已啟用 RIP (被動)**
- **已停用 RIP**

設定 RIP 用於顯示介面的**編輯**圖示 。

網路 | 路由 > OSPFv3

網路 | 路由 > OSPFv3 僅會在您針對**路由模式**選擇了**進階路由**時才會顯示，其中會提供 OSPFv3 的狀態，並可讓您為介面設定 OSPFv3。



設定	用於顯示**設定**彈出式視窗的圖示，可供您設定預設路由的度量。
介面 (區域)	為 OSPFv3 設定的介面和其區域如果區域尚未設定介面，則 **(區域)** 指定名稱就會顯示為 **(N/A)**。
OSPFv3	指出是否在介面上啟用 OSPF。 • **已啟用 OSPFv3** • **已啟用 OSPFv3 (被動)** • **已停用 OSPFv3**
設定 OSPFv3	用於顯示介面的**編輯**圖示 。
OSPFv3 芳鄰狀態	用於顯示**狀態**圖示，其中會指出是否有使用中/非使用中的芳鄰；按一下該圖示即可顯示 **OSPFv3 介面芳鄰**彈出式視窗，內有更多該介面的芳鄰詳細資訊。請參閱第 389 頁「網路	路由 > OSPFv3 > OSPFv3 介面芳鄰」。

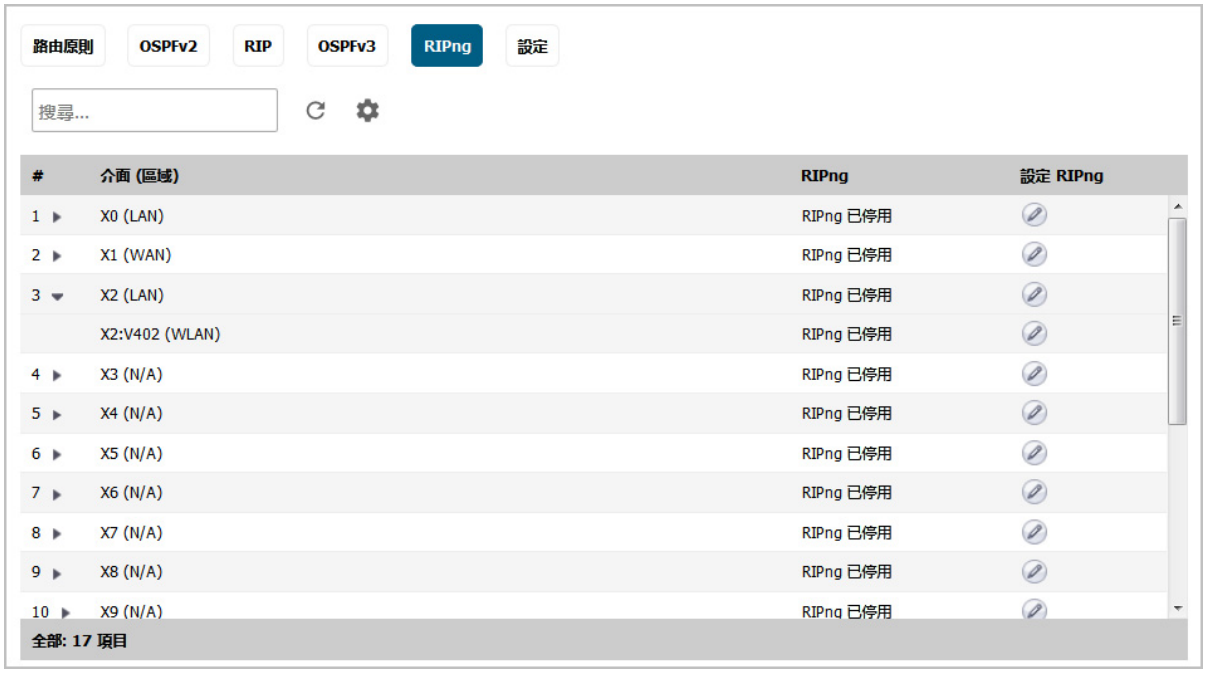
網路 | 路由 > OSPFv3 > OSPFv3 介面芳鄰

按一下介面的**狀態**圖示，就會顯示這個彈出式視窗。

路由器 ID	芳鄰的路由器 ID。
目前狀態	OSPFv3 網路芳鄰的狀態 (如有建立): • **啟動** • **雙向** • **ExStart** • **交換** • **載入中** • **完全**
優先順序	芳鄰的路由器優先順序。

網路 | 路由 > RIPng

網路 | 路由 > RIPng 僅會在您針對**路由模式**選擇了**進階路由**時才會顯示，其中會提供 RIPng 的狀態，並可讓您為介面設定 RIPng。



設定	用於顯示**設定**彈出式視窗的圖示，可供您設定預設路由的度量。
介面 (區域)	為 RIPng 設定的介面和其區域如果區域尚未設定介面，則 **(區域)** 指定名稱就會顯示為 **(N/A)**。
RIPng	指出是否在介面上啟用 RIPng。 • **已啟用 RIP** • **已啟用 RIP (被動)** • **已停用 RIP**
設定 RIPng	用於顯示介面的**編輯**圖示 。

設定路由

主題：

依照度量值排定路由優先順序

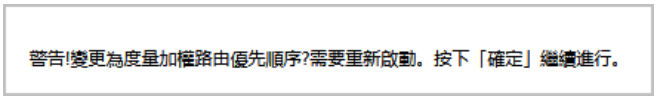
重要：必須啟用 SonicWall 安全設備才能變更度量加權路由優先順序。

度量加權選項可將度量值的優先順序提前，讓其順序優於路由特異性。系統在排定優先順序時所用的設定 (由高至低)，視是否選取了度量選項而定:

- 未選取 (預設):
  a 路由類型 (由來源、目的地、服務和其值不是任一的 TOS 欄位組合而定)。
  b 來源、目的地、服務和 TOS 欄位的累計特異性。
  c 度量。
- 已選擇：
  a 路由類型。
  b 度量。
  c 來源、目的地、服務和 TOS 欄位的累計特異性

若要變更為使用度量加權路由優先順序:

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > 設定**。
2 選取**根據路由類別內的度量設定路由的優先順序**。將顯示確認訊息。



3 按一下**確定**。
4 導覽至**管理 | 更新 | 重新啟動**，以手動方式重新啟動 SonicOS。

為透過路由器通告學習的預設路由設定度量

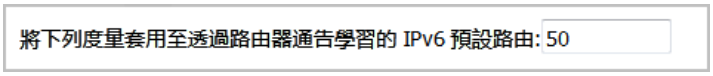
附註：這個設定只會在透過路由器通告學習的 IPv6 預設路由上生效。

若要為透過路由器告學習的預設路由設定度量:

1 導覽到**管理 | 網路 | 路由**。

2 按一下**路由原則**。

3 按一下**設定**圖示。**設定**對話方塊隨即顯示。



4 這個路由度量會套用至透過路由器通告學習的預設路由。在**將下列度量套用至透過路由器通告學習的 IPv6 預設路由**欄位中輸入度量。最小值為 1，最大值為 255，預設值為 **50**。

提示：度量值越低越好，度量值越低，優先順序就越高。

5 按一下**接受**。

設定路由通告

若要為網路介面啟用路由通告：

1 導覽到**管理 | 網路 | 路由**。

2 按一下**路由通告**。

3 按一下此介面**設定**列中的**編輯**圖示。將顯示**介面路由通告設定**。

4 從 **RIP 通告**下拉功能表選擇以下類型之一：

- **停用**（預設）- 停用 RIP 通告。
- **啟用 RIPv1** - RIPv1 是第一版路由資訊通訊協定。
- **啟用 RIPv2（多點傳送）** - 使用多點傳送方式（將單個封包傳送到網路中的特定節點）傳送路由通告。
- **啟用 RIPv2（廣播）** - 使用廣播方式（將單個封包傳送到網路中的所有節點）傳送路由通告。

通過選擇**停用**以外的其他類型，其他選項將變為可用。

5 從**通告預設路由下拉**功能表，選擇：

- **從不**（預設）
- **WAN 介面使用中的時候**（無法使用於 WAN 介面）
- **始終**

6 如果在安全設備中設定了固定路由，則啟用**通告固定路由**；停用此功能將從路由通告中排除這些固定路由。

7 如果想要通告 VPN 網路，則啟用**通告遠端 VPN 網路**。

8 在**路由變更延時時間（秒數）**欄位中，輸入在網路中廣播通告的時間間隔值（以秒為單位）。預設值為 **30** 秒，最小值為 1 秒，最大值為 99 秒。越小的值對應越高的網路廣播流量。**路由變更延**

時時間（秒數）設定定義了變更 VPN 通道狀態（啟用或停用）與使用 RIP 通告此變更之間的延遲。此延遲（以秒為單位）可防止因暫時變更 VPN 通道狀態而傳送不明確的路由通告。

9 在**已刪除的路由通告 (0-99)** 欄位中，輸入用於廣播已刪除的路由的通告數量。預設值為 **1**。

10 在**路由度量 (1-15)** 欄位中，輸入 **1**（預設） 到 15 之間的值。它是封包在從來源 IP 位址到目的地 IP 位址的過程中經過某個路由器的次數。

> **附註：**僅當在 **RIP 通告**下拉功能表中選擇了 RIPv2 通告選項時，以下選項才可用。如果選擇了**已啟用 RIPv1**，請移至步驟 13。

11 您可在 **RIPv2 路由標記（4 位十六進位數）**欄位中輸入一個路由標記值。此值仰賴於具體實施，並為路由器提供了一種用來劃分 RIPv2 通告發起方的機制。預設值為 **0**。

12 如果想要啟用 RIPv2 身分驗證，請從 **RIPv2 驗證**下拉功能表中選擇以下選項之一（預設選項是**停用**）：

- **使用者定義** - 將顯示兩個欄位：
  - **驗證類型 (4 位十六進位數)** - 在欄位中輸入 4 位十六進位數。預設為 **0**。
  - **驗證資料（32 位元十六進位數)** - 在欄位中輸入 32 位元十六進位數。
- **純文字密碼** - 將顯示**驗證密碼**欄位。在欄位中輸入最多含 16 個字元的密碼。
- **MD5 摘要** - 在**驗證金鑰 Id (0-255)** 欄位中輸入 0-255 之間的數字值。在**驗證資料（32 位十六進位數）**欄位中輸入 32 位元十六進位數值，或者使用產生的金鑰。
  - **驗證金鑰 Id (0-255)** - 在欄位中最多輸入 255 個字元。預設為 **1**。
  - **驗證金鑰** - 在欄位中最多輸入 32 個字元。

13 按一下**確定**。

設定固定路由和原則式路由

在 SonicOS 中，固定路由是通過基本路由原則進行設定的。對於每部安全設備的路由數量上限，請參閱 *SonicOS 原則*中的路由原則設定說明。

在設定固定路由時，可選擇設定用於此路由的網路監視器原則。使用網路監視器原則時，將基於原則的探查狀態來動態地停用或啟用固定路由。

若要設定固定路由或原則式路由:

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > 路由原則**。

2 按一下**新增**圖示。隨即顯示**新增路由原則**對話方塊。

3 在**來源**中，選擇用於固定路由的來源位址物件，或者選取**建立新位址物件**，動態建立一個新的位址物件。預設值為**任何**。

4 在**目的地**中，選擇目的地位址物件，或者選取**建立新位址物件**，動態建立一個新的位址物件。預設值為**任何**。

5 在**服務**中，選擇一個服務物件。對於允許所有流量類型的一般固定路由，只需選擇**任何**（預設）即可。

6 選擇要使用的路由類型:

- **標準路由** (預設) - 請移至步驟 8。
- **多重路徑路由** — **閘道數量**選項隨即顯示:

7 在**閘道數量**中，選取閘道數量上限:

- **2**
- **3**
- **4**

8 在**介面**中，選取要用於路由的介面，或者選取**建立 VPN 通道介面**，動態建立一個新的 VPN 原則。如需建立 VPN 原則的相關資訊，請參閱 *SonicOS 連線能力*。

9 在**閘道**中，選擇用於路由的閘道位址物件，或者選取**建立新位址物件**，動態建立一個新的位址物件。預設值為 **0.0.0.0**。如需建立位址物件的相關資訊，請參閱 *SonicOS 原則*。

10 輸入路由的**度量** (加權成本)。下限為 1，上限為 254。預設度量如下:

- 固定路由為 **1**
- 透過下列項目學習的動態路由:
  - RIP/RIPng 為 **120**
  - OSPFv2/OSPFv3 為 **110**
  - BGP 為 **20**

如需度量的更多資訊，請參閱第 372 頁「關於度量和管理距離」和第 374 頁「基於原則的路由」。

提示：度量值越低越好，度量值 (成本) 越低，優先順序就越高。SonicOS 始終使用由 Cisco 定義的度量值，用於直接連接介面、固定編碼路由和所有動態 IP 路由協定。

11 (選用) 輸入路由的**註解**。此欄位用於輸入新固定路由原則的描述性註解。

12 如需在介面連線中斷時自動停用路由，請選取**當介面連線中斷時停用路由**。預設情況下已核取此選項。

13 (選用) 如需為 VPN 通道建立備用路由，請選取**允許 VPN 路徑優先**。預設情況下未勾選此選項。

預設情況下，使用者設定的 VPN 通道固定路由的度量為 1，優先順序高於 VPN 流量。目的地位址物件相同時，**允許 VPN 路徑優先**選項會讓 VPN 流量的優先順序高於固定路由。當 VPN 路徑處於這些狀態時，將導致以下結果：

- **使用中**: 如果啟用**允許 VPN 路徑優先**選項，則自動停用與 VPN 通道的目的地位址物件符合的固定路由。所有流量均通過 VPN 通道路由至目的地位址物件。
- **停用**: 自動啟用與 VPN 通道的目的地位址物件符合的固定路由。前往目的地位址物件的所有流量都通過固定路由進行路由。

14 如果 WXA 獲得授權，請在 **WXA 群組**中選取 WXA 群組。預設為**無**。

15 結束時間:

- 如需使用已啟用探查功能的原則式路由，請移至步驟 16。
- 如需忽略已啟用探查功能的路由，及設定 TOS 和管理距離值，請移至步驟 20。
- 如需套用設定，請移至步驟 24。

16 在**探查**中，選取:

- **無**（預設值）。移至步驟 19。
- 網路監控物件；設定以啟用探查功能的原則式路由後，即可使用下列兩個選項。
- **建立新的網路監控物件**。隨即顯示**新增原則**對話方塊。如需瞭解如何建立網路監控物件，請參閱 *SonicOS 調查*中的程序說明。

17 如需在探查成功後停用路由，請選取**在探查成功時停用路由**。 預設情況下未勾選此選項。

重要：典型設定不會勾選**在探查成功時停用路由**核取方塊，因為通常情況下，管理員需要在探查路由目的地失敗時停用路由。此選項增加了您指定路由和探查時的靈活性。

18 如需在關聯的路監控原則處於「未知」狀態時，讓路由將探查式為成功 (即處於「啟用」狀態)，請選取**探查狀態預設為「啟用」**。它適用於在高可用性對中的一個裝置從「空閒」狀態轉換為「使用中」狀態時控制基於探查的行為，因為這一轉換會將所有網路監控原則狀態設為「未知」。

19 如要使用預設的 TOS 和管理距離值，請移至步驟 24。

20 按一下**進階**。

21 在 **TOS (16 進位)** 欄位中輸入 TOS 值。最大值為 FF。如未設定 **TOS** 和 **TOS 遮罩**欄位，則系統使用的值為 0。如需瞭解 TOS 和 TOS 遮罩值，請參閱第 374 頁「原則式 TOS 路由」。

22 在 **TOS (16 進位)** 欄位中輸入相同的值。

23 若要手動指定管理距離:

a 取消選取**自動**。**管理距離**欄位隨即可供使用。預設情況下已核取此選項。如需管理距離的相關資訊，請參閱第 372 頁「關於度量和管理距離」。

b 在**管理距離**欄位中輸入所需的管理距離。

24 按一下**確定**。

為捨棄通道介面設定固定路由

若要為丟棄通道介面新增固定路由：

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > 路由原則**。

2 按一下**新增**圖示。隨即顯示**新增路由原則**對話方塊。

3 按照第 393 頁「設定固定路由和原則式路由」中的說明，設定**來源**、**目的地**、**服務**和**路由**選項的值。

4 對於**介面**，選擇 **Drop_TunnelIf**。這些選項將發生變更。

5 依據第 393 頁「設定固定路由和原則式路由」中的說明完成選項設定。

6 按一下**確定**。此路由就會啟用並顯示在**路由原則**表中。

設定 OSPF 和 RIP 進階路由服務

附註：ARS 是全功能多通訊協定路由套件。它所提供的可設定選項和參數絕對數目不符合使用者介面的簡易性。SonicOS 管理介面中沒有對 ARS 功能進行限制，而是提供了其功能的縮寫表示，從而對最密切相關的路由功能提供控制，與此同時，通過 CLI 提供完整的命令套件 (請參閱 *SonicOS CLI 參考指南*)。ARS CLI 可通過經過驗證的 CLI 工作階段進行存取，其中包含 3 個模組：

- **route ars-nsm** - 進階路由服務網路服務模組。此元件提供對核心路由器功能的控制，例如介面繫結和可重新指派的路由等。
- **route ars-rip** - RIP 模組。提供對 RIP 路由器的控制。
- **route ars-ospf** - OSPF 模組。提供對 OSPF 路由器的控制。

一般而言，將安全設備整合至大多數 RIP 和 OSPF 環境中所需的所有功能，都可透過 Web 式 GUI 取得。利用 CLI 的更多功能，可以進行更進階的設定。

預設已停用進階路由服務，必須先將其啟用才能使用。

RIP 和 OSPF 路由通訊協定的操作取決於介面。每個介面和虛擬子介面都可能有單獨設定的 RIP 和 OSPF 設定，且每個介面都可以執行 RIP 和 OSPF 路由器。

主題：

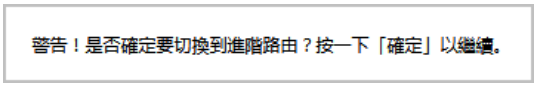
- 第 398 頁「啟用進階路由服務和 BGP」
- 第 399 頁「設定 OSPF」
- 第 403 頁「設定 RIP 和 RIPng」
- 第 406 頁「設定通道介面進階路由」

啟用進階路由服務和 BGP

若要啟用進階路由服務:

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > 設定**。

2 在**路由模式**中選取**進階路由**。將顯示確認訊息。



3 按一下**確定**。**網路 | 路由**中的選項將有所異動:

4 如需啟用 BGP，請在 **BGP** 中選取**已啟用 (使用 CLI 設定)**。預設值為**停用**。將顯示確認訊息。

5 按一下**確定**。**BGP 狀態**按鈕即可供使用。

設定 OSPF

附註：OSPF 設計概念不在本文件的討論範圍內。本章節說明如何設定 SonicWall 安全設備整合到 OSPF 網路中（不論是現有的還是新實施的 OSPF 網路），但不提供設計準則。關於本章節中使用的術語，請參考第 380 頁「OSPF 術語」。

主題：

- 第 399 頁「設定 OSPFv2」
- 第 401 頁「設定 OSPFv3」

設定 OSPFv2

若要設定 OSPFv2 的介面:

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > OSPFv2**。

2 按一下介面的**編輯**圖示 。**OSPFv2 介面設定**對話方塊隨即顯示。

3 在 **OSPFv2** 中，選取:

已停用(預設)	已在此介面上停用 OSPF 路由器。移至步驟 13。
啟用	已在此介面上啟用 OSPF 路由器。
被動	在這個介面上啟用 OSPF 路由器，但僅使用 1 類 LSA (路由器連結通告) 向本機區域通告連接的網路。所有選項 (**OSPF 區域**除外) 都會變成灰色；請移至步驟 9。

4 如需指定時間範圍，設定在多久後如未收到 Hello 資訊要移除 LSDB 中的項目，請在**失效間隔 (1 - 65535)** 欄位中輸入所需時間 (以秒為單位)。預設值為 **40** 秒，最小值為 1 秒，最大值為 65,535 秒。

重要：確保此數值與此區段中的其他 OSPF 路由器一致，以便成功建立鄰居關係。

5 如需指定 Hello 封包間的時間範圍，請在 **Hello 間隔 (1 - 65535)** 欄位中輸入所需時間 (以秒為單位)。預設值為 **10** 秒，最小值為 1 秒，最大值為 65,535 秒。

重要：確保此數值與此區段中的其他 OSPF 路由器一致，以便成功建立鄰居關係。

6 在**驗證**中，選取這個介面要使用的驗證類型。

已停用	如果沒有要使用的驗證機制，請移至步驟 8。
簡單密碼	OSPF 路由器使用純文字密碼作為識別之用。
訊息摘要	使用 MD5 雜湊妥善識別 OSPF 路由。

重要：確保此設定與此區段中的其他 OSPF 路由器一致，以便成功建立鄰居關係。

7 如果您指定了：

簡單密碼	輸入由 1 至 15 個英數字元組成的密碼。
訊息摘要	輸入由 1 至 15 個英數字元組成的密碼。

8 在 **OSPF 區域**欄位中輸入區域 ID。OSPF 區域可表示為 IP 或十進位表示法。舉例來說，連上 `X4:100` 的區域會以 `100.100.100.100` 或 `1684300900` 表示。預設為 **0**。

9 在 **OSPFv2 區域類型**中選取 OSPFv2 區域類型 (如需這些設定的詳細說明，請參閱第 380 頁「OSPF 術語」)：

一般	預設 - 接收和傳送所有適用的 LSA 類型。
虛設常式區	不接收 5 類 LSA (AS 外部連結通告)。
完全虛設常式區	不接收 3、4 或 5 類 LSA。
非純末梢區域	接收 7 類 LSA (NSSA AS 外部路由)。
完全非末梢區域	接收 1 類和 2 類 LSA。

10 結束時間:

- 如需指定跨過這個介面傳送封包的經常成本，請在**介面成本 (1 - 65535)** 欄位中輸入指定的經常成本。預設值為 **0**，通常用於指示乙太網路介面。預設最小值為 0（例如，快速乙太網路），最大值為 65,535（例如，pudding）。
- 如需自動確認成本，請選取**自動**，**介面成本**欄位將變為灰色。 預設情況下已核取此選項。

11 如需指定所需的路由器優先順序值，來確認區段的指定路由器 (DR)，請在**路由器優先順序 (0-255)** 欄位中輸入所需的值。此值越大，優先順序越高。出現等值優先順序時，路由器 ID 將成為打破等值優先順序的因素。設定數值 0 將使此介面上的 OSPF 路由器失去獲得 DR 狀態的資格。預設值為 **1**，最大值為 255。

12 如需啟用 MTU 相容性，請選取**啟用 MTU 相容性 (忽略 mtu)**。 預設情況下未勾選此選項。

13 按一下**確定**。

設定 OSPFv3

若要設定 OSPFv3 的介面:

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > OSPFv3**.

2 按一下介面的**編輯**圖示 。**OSPFv3 介面設定**對話方塊隨即顯示。

3 在 **OSPFv3** 中，選取:

已停用(預設)	已在此介面上停用 OSPF 路由器。移至步驟 12。
啟用	已在此介面上啟用 OSPF 路由器。
被動	在這個介面上啟用 OSPF 路由器，但僅使用 1 類 LSA (路由器連結通告) 向本機區域通告連接的網路。所有選項 (**OSPFv3 區域**除外) 都會變成灰色。

4 在 **OSPF 區域**欄位中輸入區域 ID。OSPF 區域可表示為 IP 或十進位表示法。舉例來說，連上 `X4:100` 的區域會以 `100.100.100.100` 或 `1684300900` 表示。預設為 **0**。

5 如果您針對 **OSPFv3** 選取了**被動**，請移至步驟 12。

6 如需指定時間範圍，設定在多久後如未收到 Hello 資訊要移除 LSDB 中的項目，請在**失效間隔 (1 - 65535)** 欄位中輸入所需時間 (以秒為單位)。預設值為 **40** 秒，最小值為 1 秒，最大值為 65,535 秒。

重要：確保此數值與此區段中的其他 OSPF 路由器一致，以便成功建立鄰居關係。

7 在 **OSPFv3 區域類型**中選取 OSPFv3 區域類型 (如需這些設定的詳細說明，請參閱第 380 頁「OSPF 術語」):

一般	預設 - 接收和傳送所有適用的 LSA 類型。
虛設常式區	不接收 5 類 LSA (AS 外部連結通告)。
完全虛設常式區	不接收 3、4 或 5 類 LSA。

8 如需指定 Hello 封包間的時間範圍，請在 **Hello 間隔 (1 - 65535)** 欄位中輸入所需時間 (以秒為單位)。預設值為 **10** 秒，最小值為 1 秒，最大值為 65,535 秒。

重要：確保此數值與此區段中的其他 OSPF 路由器一致，以便成功建立鄰居關係。

9 結束時間:

- 如需指定跨過這個介面傳送封包的經常成本，請在**介面成本 (1 - 65535)** 欄位中輸入指定的經常成本。預設值為 **0**，通常用於指示乙太網路介面。預設最小值為 0（例如，快速乙太網路），最大值為 65,535（例如，pudding）。
- 如需自動確認成本，請選取**自動**，**介面成本**欄位將變為灰色。 預設情況下已核取此選項。

10 如需指定所需的路由器優先順序值，來確認區段的指定路由器 (DR)，請在**路由器優先順序 (0-255)** 欄位中輸入所需的值。此值越大，優先順序越高。出現等值優先順序時，路由器 ID 將成為打破等值優先順序的因素。設定數值 0 將使此介面上的 OSPF 路由器失去獲得 DR 狀態的資格。預設值為 **1**，最大值為 255。

11 如需為介面設定執行個體 ID，請在**執行個體 ID (0 - 255)** 欄位中輸入所需的值。最小值和預設值為 0，最大值為 255。 預設情況下未勾選此選項。

> **重要：**這個選項一般為灰色，只能透過 SonicOS 命令行介面設定 (如需 SonicOS CLI 的相關資訊請參閱 *SonicOS 命令行介面*。

12 按一下**確定**。

全域 OSPFv3 設定

若要設定全域 OSPFv3:

1 導覽到**管理 | 系統安裝 | 網路 | 路由**。

2 按一下 **OSPFv3**。

3 按一下**設定**圖示。**設定**彈出式對話方塊隨即顯示:

4 設定下列選項:

- **OSPFv3 路由器 ID (n.n.n.n)** - 路由器 ID 可以是以 IP 位址表示法表示的任意值。它與安全設備上的所有 IP 位址都無關，並可以設為您的 OSPF 網路中的任意*唯*一值。

- **ABR 類型** - 出於相容性的目的，允許此 OSPF 路由器將參與的拓撲規範。選項有：
  - **標準** - 完全符合 RFC2328 的 ABR OSPF 操作。
  - **Cisco** - 用於同 Cisco 的 ABR 行為進行互操作，此選項預期在設定 ABR 標記之前設定並啟用主幹網。
  - **IBM** - 用於同 IBM 的 ABR 行為進行互操作，此選項預期在設定 ABR 標記之前設定主幹網。
  - **快捷方式** -「快捷方式區域」使得不論 ABR 路由器是否連接到區域 0，流量都能以較低的度量穿過非主幹網區域。
- **預設度量 (1-16777214)** - 用於指定在重新指派來自其他（例如預設、固定、已連接、RIP 或 VPN）路由資訊來源的路由時將會使用的度量。預設值（**未定義**）為 **1**，最大值為 16,777,214。
- **自動成本參考 B@ (Mb/s)** - 預設值為 100。
- **重新分配固定路由** - 啟用或停用向 OSPF 系統通告固定（基於原則的路由）路由。預設情況下未勾選此選項。

附註：以下項目適用於所有重新指派的路由：

- **度量** - 可以為此重新指派明確設定度量，或者可以使用**預設度量**選項中指定的值（**預設值**）。
- **度量類型** - 重新指派的路由通告將為 5 類 LSA，路由類型可選擇為**外部類型 1**（增加內部連結費用）或**外部類型 2**（僅使用外部連結費用）。

附註：除非選擇了重新指派路由選項，否則此欄位為灰顯。

- **重新分配已連接的網路** - 啟用或停用向 OSPF 系統通告本機連接的網路。預設情況下未勾選此選項。
- **重新分配 Rip 路由** - 啟用或停用向 OSPF 系統通告透過 RIP 得知的路由。預設情況下未勾選此選項。

5 按一下**接受**。

路由通訊協定部分將按介面顯示所有使用中 OSPF 路由器的狀態。

路由原則區段將 OSPF 所得知的路由顯示為 **OSPF** 或 **RIP 路由**。

狀態按鈕隨即可供使用。

設定 RIP 和 RIPng

主題：

- 第 403 頁「設定 RIP」

設定 RIP

若要在介面上設定 RIP 路由:

1 導覽到**管理 | 網路 | 路由**。

2 按一下 **RIP**。

3 按一下介面的**編輯**圖示 。**RIP 介面設定**對話方塊隨即顯示。

4 在 **RIP** 中選取所需模式:

已停用(預設)	已在此介面上停用 RIP；請移至步驟 12。
傳送及接收	此介面上的 RIP 路由器將傳送更新和處理收到的更新。
僅限傳送	此介面上的 RIP 路由器僅傳送更新，而不處理收到的更新。這與基本路由實施相似。
僅限接收	此介面上的 RIP 路由器僅處理收到的更新。
被動	此介面上的 RIP 路由器將不處理收到的更新，而僅將更新傳送至使用 CLIneighbor 命令指定的臨近 RIP 路由器。 **重要：**此模式只應在透過 ARS-RIP CLI 設定進階 RIP 選項時使用 (請參閱 *SonicOS CLI 參考指南*)。選取時，所有其他選項都會顯示為灰色。

5 如果您指定了：

- **僅限傳送**，請移至步驟 8。
- **被動**，請移至步驟 12。

6 在**接收**中，選取要用來接收 RIP 封包的 RIP 版本:

RIPv1	僅接收*廣播* RIPv1 封包。
RIPv2 (預設)	僅接收*多點傳送* RIPv2 封包。RIPv2 封包通過多點傳送傳送，儘管某些 RIP 路由器的實施（包括 SonicWall 裝置上的基本路由）能夠以廣播或多點傳送格式傳送 RIPv2。 **重要：**確保傳送 RIPv2 更新的裝置使用多點傳送模式，否則 ars-rip 路由器將不會處理這些更新。

7 如果您針對 **RIP** 選取了**僅限接收**，請移至步驟 11。

8 如需禁止在傳送至路由器的更新中，納入從這些路由器得知的路由，請選取**水平分割**。這是常用於防止路由迴圈的 RIP 機制；請參閱第 378 頁「最大躍點數」。預設情況下已核取此選項。

9 如需指定可選用的水平分割操作模式，請選取**反向阻礙**。這個模式不會禁止納入已得知的路由，反而會以無限度量 (16) 來傳送路由，進而指明這些路由無法到達；請參閱第 378 頁「最大躍點數」。預設情況下已核取此選項。

10 在**傳送**中，選取要用來傳送封包的 RIP 版本:

RIPv1	傳送*廣播* RIPv1 封包。
RIPv2 — 與 v1 相容	傳送與 RIPv1 相容的*多點傳送* RIPv2 封包。
RIPv2 (預設)	傳送*多點傳送* RIPv2 封包。

11 如需強制使用密碼，請選取**使用密碼**。**密碼**欄位隨即可供使用。 預設情況下未勾選此選項。

a 在**密碼**欄位中輸入密碼。

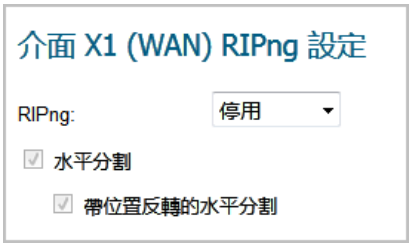
12 按一下**確定**。

設定 RIPng

若要在介面上設定 RIPng 路由:

1 導覽至**管理 | 系統安裝 | 網路 | 路由 > RIPng**。

2 按一下介面的**編輯**圖示 。**RIPng 介面設定**對話方塊隨即顯示。



3 在 **RIPng** 中選取所需模式:

已停用(預設)	已在此介面上停用 RIPng；請移至步驟 6。
啟用	這個介面上的 RIPng 路由器將傳送更新及處理收到的更新。
被動	這個介面上的 RIPng 路由器不會處理收到的更新，只會將更新傳送至使用 CLI`neighbor` 命令指定的臨近 RIP 路由器。 **重要：**只有在透過 ARS-RIP CLI 設定進階 RIPng 選項時，才應該使用這個模式 (請參閱 *SonicOS CLI 參考指南*)。

4 如需禁止在傳送至路由器的更新中，納入從這些路由器得知的路由，請選取**水平分割**。這是常用於防止路由迴圈的 RIP 機制；請參閱第 378 頁「最大躍點數」。預設情況下已核取此選項。

5 如需指定可選用的水平分割操作模式，請選取**反向阻礙**。這個模式不會禁止納入已得知的路由，反而會以無限度量 (16) 來傳送路由，進而指明這些路由無法到達；請參閱第 378 頁「最大躍點數」。預設情況下已核取此選項。

6 按一下**確定**。

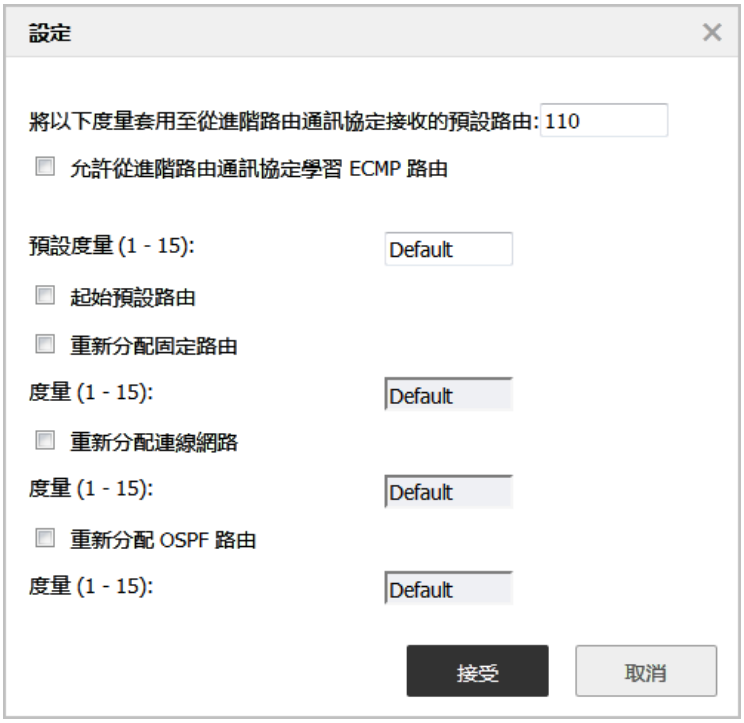
全域 RIPng 設定

若要設定全域 OSPFv3:

1 導覽到**管理 | 系統安裝 | 網路 | 路由**。

2 按一下 **OSPFv3**。

3 按一下**設定**圖示。**設定**彈出式對話方塊隨即顯示:



4 設定下列選項:

- **預設度量** - 用於指定在重新指派來自其他（例如預設、固定、已連接、OSPF 或 VPN）路由資訊來源的路由時將會使用的度量。預設值（未定義）為 **1**，最大值為 15。
- **原始預設路由** - 這個核取方塊的用途是開始或停止向 RIP 系統通告安全設備的預設路由。
- **重新分配固定路由** - 啟用或停用向 RIP 系統通告固定（基於原則的路由）路由。可以為此重新指派明確設定度量，或者可以使用**預設度量**設定中指定的值（預設值）。
- **重新分配已連接的網路** - 啟用或停用向 RIP 系統通告本機連接的網路。可以為此重新指派明確設定度量，或者可以使用**預設度量**設定中指定的值（預設值）。
- **重新分配 OSPF 路由** - 啟用或停用向 RIP 系統通告透過 OSPF 得知的路由。可以為此重新指派明確設定度量，或者可以使用**預設度量**設定中指定的值（預設值）。

5 按一下**接受**。

設定通道介面進階路由

VPN 通道介面可設定用於進階路由。為此，您必須在通道介面設定的**進階**標籤中啟用通道介面進階路由。詳情請參閱新增通道介面 (第 X 頁)。

啟用通道介面進階路由後，這個路由將與其他介面一同顯示**網路 | 路由**上的各種表格檢視畫面中。

若要設定進階路由選項:

1 找出您想要設定的通道介面，然後按一下**設定 RIP/RIPng** 或**設定 OSPF/OSPFv3** 欄中的**編輯**圖示。通道介面的 RIP 和 OSPF 設定與傳統介面的設定非常相似。

全域未編號設定

由於未編號通道介面並非實體介面，不具備固有 IP 位址，因此它們必須「借用」其他介面的 IP 位址。所以通道介面的進階路由設定中包含了以下用於指定通道來源 IP 位址和目的地 IP 位址的選項：

- **借來的 IP 位址來自於** - 將其 IP 位址用作通道介面的來源 IP 位址的介面。

  附註：借用的 IP 位址必須為固定 IP 位址。

- **遠端 IP 位址** - 通道介面連接到的遠端對等介面的 IP 位址。在使用另一個通道介面的 SonicWall 對 SonicWall 設定情形下，此位址應該是遠端對等通道介面的被借用介面 IP 位址。

設定通道介面進階路由的準則

以下準則可確保您順利設定通道介面進階路由:

- 借用介面必須擁有固定 IP 位址指派。
- 借用介面不能在其設定中啟用 RIP 或 OSPF。

  提示：SonicWall 推薦建立一個專門用作借用介面的 VLAN 介面。在使用有線連接的介面時，此推薦可避免發生衝突。

- 借用介面的 IP 位址應來自專用位址空間，且相對任何遠端通道介面端點擁有唯一的 IP 位址。
- 通道介面端點的遠端 IP 位址應該與借用介面處於相同的網路子網路中。
- 多個通道介面可以使用同一借用介面，前提是這些通道介面全部連接到不同的遠端裝置。
- 如果某個裝置上的多個通道介面連接到同一遠端裝置，則每個通道介面都必須使用唯一的借用介面。

根據網路設定的具體情況，要確保通道介面正常工作，這些準則可能並非不可或缺。但這些準則是 SonicWall 的最佳做法，可避免潛在的網路連線問題。

設定 BGP 進階路由

附註：支援 BGP 的裝置如下:

- NSA 2600 和 NSA 2600 以上版本的安全設備。
- 購買 SonicOS 擴充授權後，TZ400 系列、TZ500 系列和 TZ600 安全設備即可支援 BGP。

TZ300 系列或 SOHO 無線安全設備不支援 BGP。

邊界閘道通訊協定 (BGP) 是用於在自發系統 (AS) 之間交流路由資訊的大型路由通訊協定。這些自發系統是定義明確、單獨管理的網路網域。BGP 支援允許使用安全設備來替代位於網路自發系統邊緣的傳統 BGP 路由器。BGP 的目前 SonicWall 實作最適用於「單供應商/單主目錄」環境，在這種環境下，網路使用一個 ISP 作為網際網路供應商，且與此供應商採用單一連接。SonicWall BGP 還可以支援「單供應商/單主目錄」環境，其中，網路使用單個 ISP，但擁有連至供應商的少量單獨路由。您可以在 SonicOS 管理介面的**網路 | 路由**頁面啟用 BGP，然後再透過 SonicOS 命令行介面 (CLI；請參閱 *SonicOS CLI 參考指南*.) 進行完整設定。

如需 SonicWall 的 BGP 實施的完整資訊，請參見第 791 頁「BGP 進階路由」。

設定用於 BGP 工作階段的 IPSec 通道

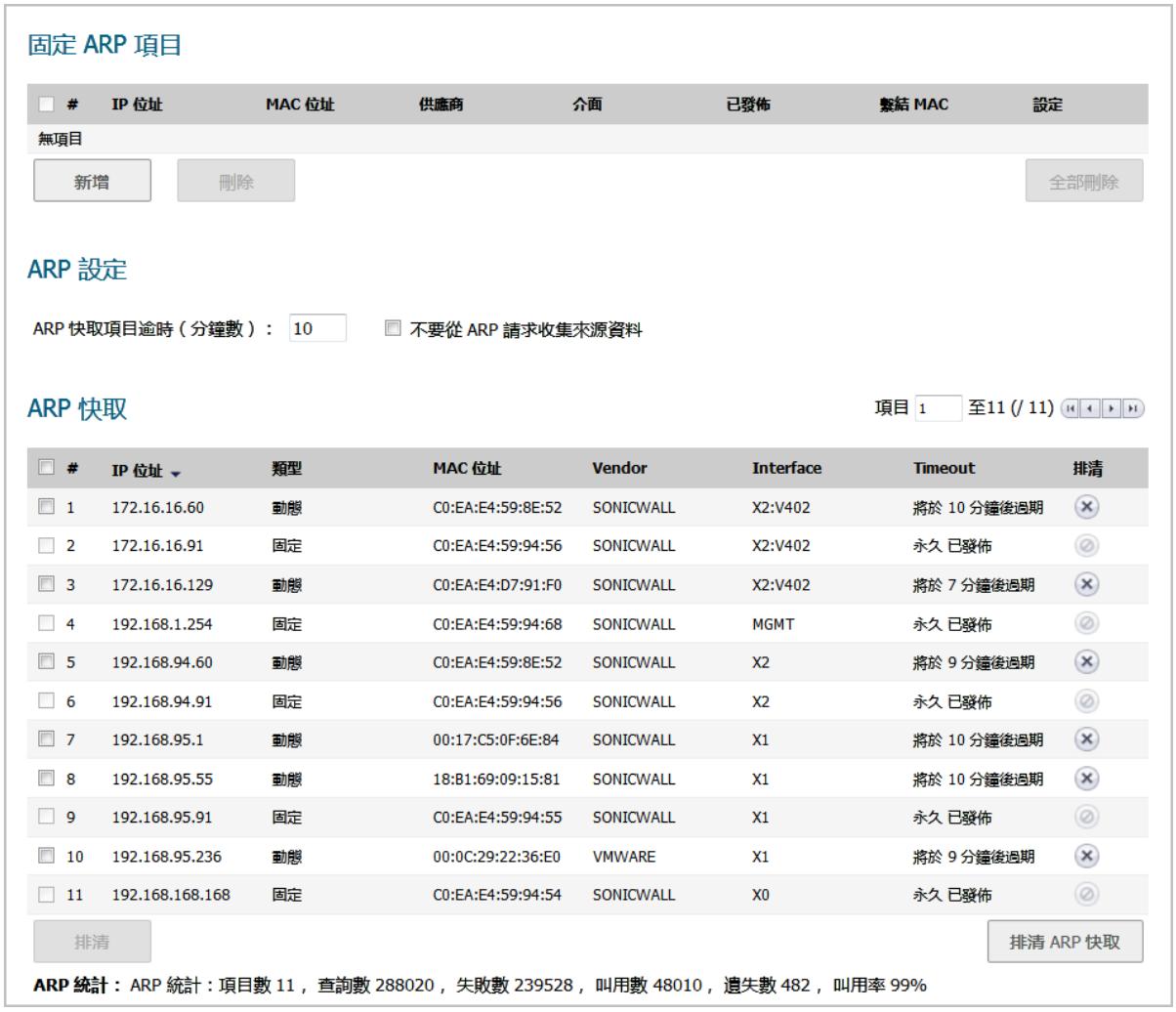
BGP 傳送封包暢通無阻。因此為了增強安全性，SonicWall 建議您設定 IPSec 通道供 BGP 工作階段使用。如需瞭解如何為 BGP 設定 IPSec 通道及啟用 BGP，請參閱第 791 頁「BGP 進階路由」。

在透過管理介面啟用 BGP 後，BGP 設定的具體設定使用 SonicOS 命令行介面 (CLI) 執行。如需在 SonicWall 安全設備安全裝置中實作 BGP 的完整資訊，請參閱第 791 頁「BGP 進階路由」。

21

管理 ARP 流量

網路 | ARP



固定 ARP 項目

#	IP 位址	MAC 位址	供應商	介面	已發佈	繫結 MAC	設定
無項目							

新增　刪除　全部刪除

ARP 設定

ARP 快取項目逾時（分鐘數）： 10　不要從 ARP 請求收集來源資料

ARP 快取　項目 1 至11 (/ 11)

#	IP 位址	類型	MAC 位址	Vendor	Interface	Timeout	排清
1	172.16.16.60	動態	C0:EA:E4:59:8E:52	SONICWALL	X2:V402	將於 10 分鐘後過期	
2	172.16.16.91	固定	C0:EA:E4:59:94:56	SONICWALL	X2:V402	永久 已發佈	
3	172.16.16.129	動態	C0:EA:E4:D7:91:F0	SONICWALL	X2:V402	將於 7 分鐘後過期	
4	192.168.1.254	固定	C0:EA:E4:59:94:68	SONICWALL	MGMT	永久 已發佈	
5	192.168.94.60	動態	C0:EA:E4:59:8E:52	SONICWALL	X2	將於 9 分鐘後過期	
6	192.168.94.91	固定	C0:EA:E4:59:94:56	SONICWALL	X2	永久 已發佈	
7	192.168.95.1	動態	00:17:C5:0F:6E:84	SONICWALL	X1	將於 10 分鐘後過期	
8	192.168.95.55	動態	18:B1:69:09:15:81	SONICWALL	X1	將於 10 分鐘後過期	
9	192.168.95.91	固定	C0:EA:E4:59:94:55	SONICWALL	X1	永久 已發佈	
10	192.168.95.236	動態	00:0C:29:22:36:E0	VMWARE	X1	將於 9 分鐘後過期	
11	192.168.168.168	固定	C0:EA:E4:59:94:54	SONICWALL	X0	永久 已發佈	

排清　排清 ARP 快取

ARP 統計： ARP 統計：項目數 11， 查詢數 288020， 失敗數 239528， 叫用數 48010， 遺失數 482， 叫用率 99%

ARP（位址解析通訊協定）將第 3 層（IP 位址）對應至第 2 層（實體或 MAC 位址），以便位於相同子網路中的主機相互通訊。ARP 是一種廣播通訊協定，可能會在您的網路中產生大量網路流量。為儘量減少廣播流量，因而維護 ARP 快取來儲存和重用之前學習的 ARP 資訊。

主題：

固定 ARP 項目

固定 ARP 功能用於在第 2 層 MAC 位址與第 3 層 IP 位址之間建立固定對應，同時提供以下功能：

主題：

設定固定 ARP

若要設定固定 ARP：

1 導覽到**網路 | ARP**。

2 按一下**固定 ARP 項目**表下面的**新增**。隨即顯示**新增固定 ARP** 對話方塊。

3 在 **IP 位址**欄位，輸入 SonicWall 安全設備的 IP 位址。

4 在**介面**中，選取要與此固定 ARP 項目關聯的安全設備的 LAN 介面。

5 在 **MAC 位址**欄位中，輸入安全設備的 MAC 位址。

6 若要讓安全設備使用特定的 MAC 位址來回應指定 IP 位址的 ARP 查詢，請選取**發佈項目**選項。預設情況下未勾選此選項。

例如，可以使用此選項讓安全設備透過新增安全設備的 MAC 位址來答覆指定介面上的次要 IP 位址。請參閱第 410 頁「使用固定 ARP 的次要子網路」。選擇此選項將使 **MAC 位址**欄位和**繫結 MAC 位址**選項變灰。

7 如果您選取了**發佈項目**，請移至步驟 10。

8 若要將指定的 MAC 位址繫結至特定的 IP 位址和介面，請選取**繫結 MAC 位址**。預設情況下未勾選此選項。

此選項可確保特定工作站（透過網路卡的唯一 MAC 位址進行識別）只能在安全設備的指定介面上使用。在 MAC 位址繫結到介面後，安全設備：

- 不會對任何其他介面回應該 MAC 位址。
- 移除可能已經存在的 MAC 位址的任何動態快取參照。
- 禁止對該 MAC 位址進行更多（非唯一的）固定對應。

選取繫結 MAC 位址時，系統會提供**動態更新 IP 位址**選項。

9 在使用 DHCP 來動態配置 IP 位址的情況下，若要允許將 MAC 位址繫結至某個介面，請選取**動態更新 IP 位址**，**繫結 MAC 位址**選項的子功能。

啟用這個選項後，系統將停用 **IP 位址**欄位，並將其設定為 0.0.0.0，同時也會提供 **MAC 位址**欄位，並且使用由安全設備的內部 DHCP 伺服器或外部 DHCP 伺服器 (如果正在使用 IP 協助程式) 配置的 IP 位址來填寫 ARP 快取。

10 按一下**確定**。

編輯固定 ARP 項目

若要編輯固定 ARP 項目：

1 導覽到**網路 | ARP**。

2 在**固定 ARP 項目**表中，按一下**設定**欄位中項目的**編輯**圖示。隨即顯示**編輯固定 ARP** 對話方塊。

3 做出變更。

4 按一下**確定**。項目即會更新。

使用固定 ARP 的次要子網路

固定 ARP 功能允許在其他介面上新增次要子網路，而且無需新增自動 NAT 規則。

主題：

- 第 411 頁「新增次要子網路」
- 第 411 頁「範例」

新增次要子網路

若要使用固定 ARP 方法新增次要子網路：

1 為將要用於次要子網路的閘道位址新增「已發佈」的固定 ARP 項目，從而為其指定將要連接到的安全設備介面的 MAC 位址。

2 新增用於此子網路的固定路由，使得安全設備將其視為有效流量，並確定將此子網路的流量路由到哪個介面。

3 新增存取規則，以便以此子網路為目的地的流量流經正確的網路介面。

4 可選: 在上游裝置中新增固定路由，以便這些裝置知道使用哪個閘道 IP 到達次要子網路。

範例

考慮以下網路範例 (請參見第 411 頁「新增次要子網路」)。

若要支援新增的設定：

1 為 192.168.50.1 建立一個發佈的固定 ARP 項目，該位址會做為次要子網路的閘道。

2 將其與適當的 LAN 介面關聯。在**網路 | ARP** 中，按一下**固定 ARP 項目**表下面的**新增**。

3 編輯此項目：

4 按一下**確定**。項目會顯示在**固定 ARP 項目**表中。

5 導覽到**網路 | 路由**。

6 新增用於 192.168.50.0/24 網路的固定路由，以及 X3 介面上的 255.255.255.0 子網路遮罩。如需新增固定路由的相關資訊，請參閱第 371 頁「設定路由通告和路由原則」。

7 若要使流量到達 192.168.50.0/24 子網路，並讓 192.168.50.0/24 子網路連接 LAN 上的主機，請移至**原則 | 規則> 存取規則**頁面。

8 新增適當的存取規則以允許流量通過。如需新增存取規則的相關資訊，請參閱 *SonicOS 原則*。

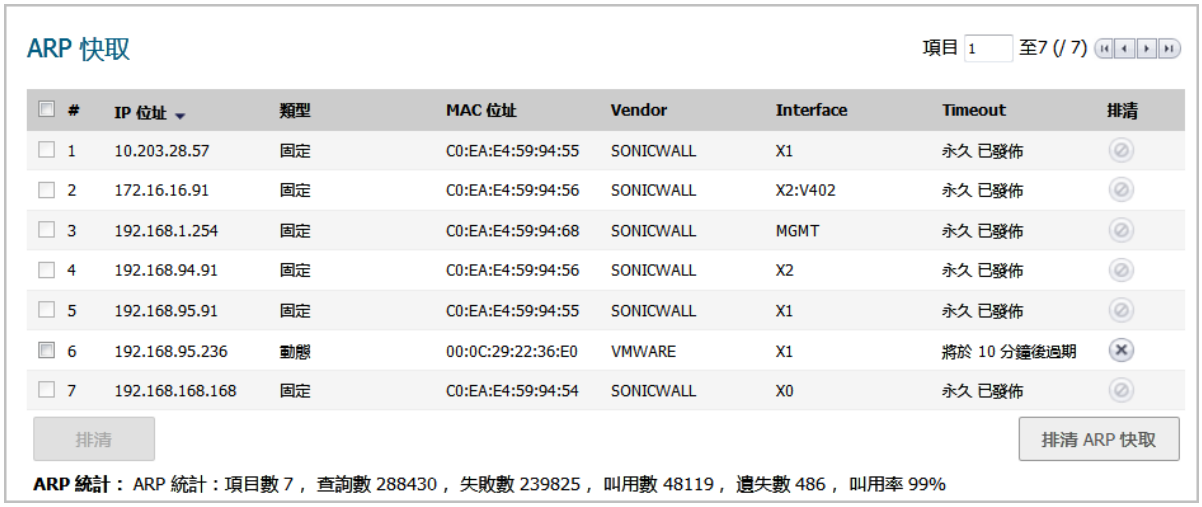
檢視固定 ARP 項目

IP 位址	作為閘道的安全設備 IP 位址。
MAC 位址	作為閘道的安全設備 MAC 位址。
供應商	安全設備製造商的名稱。
介面	與此項目關聯的 LAN 介面。
已發佈	以綠色核取記號指出，安全設備是否使用指定的 MAC 位址來回應指定 IP 位址的 ARP 查詢。
繫結 MAC	以綠色核取記號指出， MAC 位址是否繫結到指定的 IP 位址和介面。
設定	顯示項目的**編輯**和**刪除**圖示。

ARP 設定

ARP 快取項目逾時（分鐘）	指定項目逾時以及從快取排清的時間長度。最小時間為 2 分鐘，最大時間為 600 分鐘（10 小時），預設值為 **10** 分鐘。
不要從 ARP 請求收集來源資料	選擇此設定以禁止從 ARP 請求獲取來源資料。預設情況下未勾選此選項。

ARP 快取



IP 位址	安全設備的 IP 位址。
類型	指出 ARP 為**固定**或**動態**。
MAC 位址	與 IP 位址關聯的 MAC 位址。
供應商	安全設備製造商的名稱。
介面	與此 ARP 項目關聯的 LAN 介面。
逾時	指出此項目留在快取的時間。如果在設定時發佈項目，**逾時**顯示永久發佈。
排清	對於從 ARP 快取牌清項目，顯示**刪除**圖示。 **附註：**僅**動態**項目有**刪除**圖示。

排清 ARP 快取

如果網路中的裝置發生 IP 位址變化，有時可能需要排清 ARP 快取。由於 IP 位址與實體位址相關聯，因此有可能 IP 位址發生了變化，但仍舊與 ARP 快取中的實體位址相關聯。排清 ARP 快取可以在 ARP 快取中收集和儲存新資訊。

提示：若要設定具體的項目逾時時間，請在 **ARP 快取項目逾時（分鐘）**欄位中輸入以分鐘為單位的值。請參閱第 412 頁「ARP 設定」。

若要排清 ARP 快取表中的某個動態項目:

1 按下**排清**欄位中其**刪除**圖示。

要排清 ARP 快取表中的一個或多個動態項目:

1 勾選要排清的一個或多個項目的核取方塊。**排清**按鈕隨即啟用。

2 按一下**排清**。

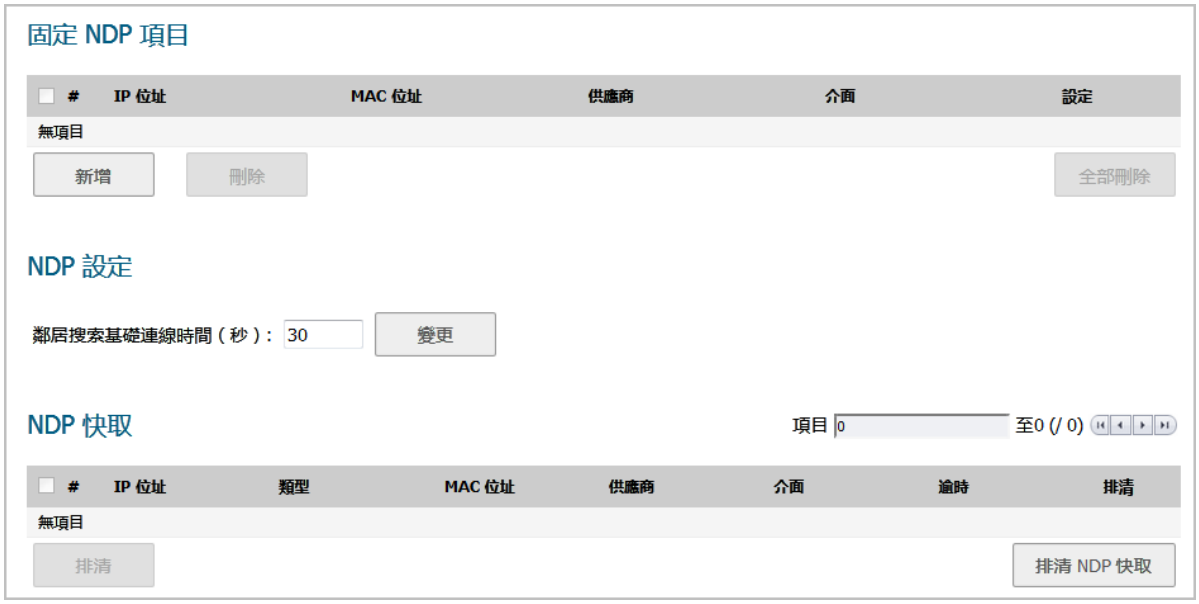
如何排清 ARP 快取表中的所有動態項目:

1 按一下**排清 ARP 快取**。

22

設定鄰居搜索通訊協定

網路 | 鄰居搜索（僅 IPv6）



鄰居發現通訊協定 (NDP) 是一個新的郵件通訊協定，它作為 IPv6 的一部分建立，用於執行 IPv4 中的 ICMP 和 ARP 完成的各種任務。和 ARP 一樣，鄰居搜索將構建一個動態項目的快取，且您可以設定固定鄰居搜索項目。IPv4/IPv6 鄰居訊息和功能表格顯示類似傳統 IPv4 鄰居訊息的 IPv6 鄰居訊息和功能。

IPv4/IPv6 鄰居訊息和功能

IPv4 鄰居訊息	IPv6 鄰居訊息
ARP 請求訊息	鄰居請求訊息
ARP 回覆訊息	鄰居宣告訊息

IPv4/IPv6 鄰居訊息和功能

IPv4 鄰居訊息	IPv6 鄰居訊息
ARP 快取	鄰居快取
免費 ARP	重複位址偵測
路由器請求訊息（可選）	路由器請求（必需）
路由器宣告訊息（可選）	路由器宣告（必需）
重新導向封包	重新導向封包

使用固定 NDP 功能，可以在三層 IPv6 位址與二層 MAC 位址之間建立固定對應。

主題：

固定 NDP 項目

IP 位址	遠端裝置的 IPv6 IP 位址。
MAC 位址	遠端裝置的 MAC 位址。
供應商	遠端裝置製造商的名稱。
介面	與遠端裝置關聯的介面。
設定	包含項目的**編輯**和**刪除**圖示。

NDP 設定

您在 **NDP 設定**中指定要到達鄰居的最長時間。

附註：對於 IPv6，您也可以在**網路 | 介面 > 編輯介面 > 進階**對話方塊中，為每一個介面設定這個值。如有介面啟用了路由器宣告功能，則您為該介面所設定的值就僅供該介面使用。如需詳細資料，請參閱第 234 頁「設定介面」。

若要指定最長時間：

1 在**鄰居搜索基礎連線時間（秒）**欄位中輸入數字。最小時長為 0 秒，最大時長為 3600 秒，預設值為 **20** 秒。

提示：這個選項的值設為 0 時，系統就會使用 NDP 設定的全域值。

2 按一下**變更**。

NDP 快取

NDP 快取表顯示所有目前的 IPv6 鄰居。

IP 位址	鄰接裝置的 IPv6 IP 位址。
類型	鄰居的類型： • **可達** - 已知可在 30 秒內到達此鄰居。 • **過時** - 已知不再能夠到達此鄰居，且已在 1200 秒內將流量傳送到此鄰居。 • **STATIC** - 將鄰居手動設定為固定鄰居。
MAC 位址	鄰接裝置的 IPv6 MAC 位址。
供應商	鄰接裝置製造商的名稱。
介面	與此鄰接裝置關聯的介面。
逾時	直到使用者逾時非使用中狀態的時間長度。
排清	包含項目的**刪除**圖示。

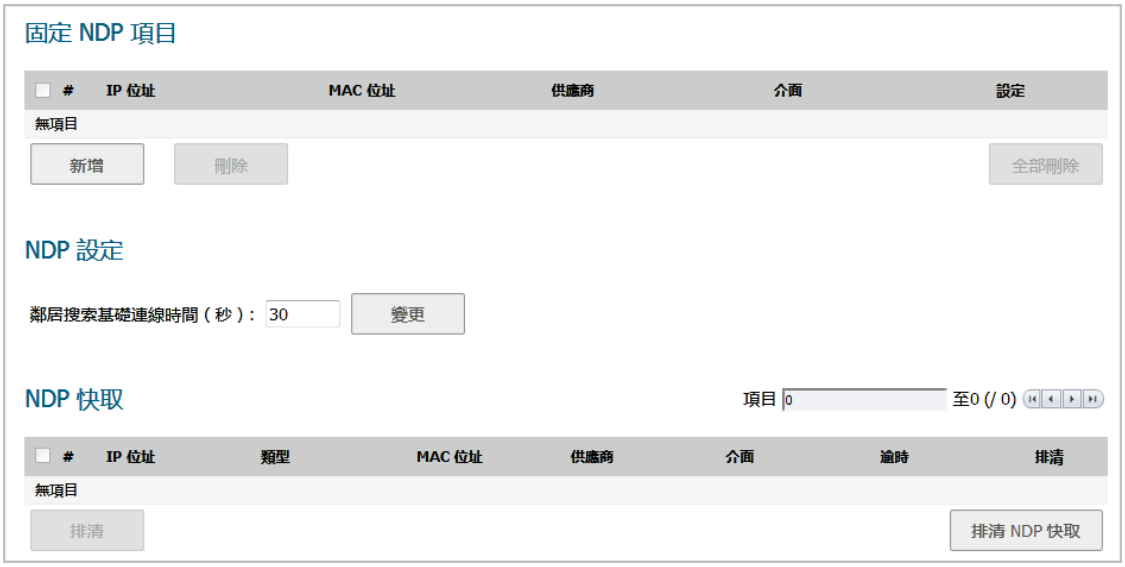
將顯示以下類型的鄰居：

- **可達** - 已知可在 30 秒內到達此鄰居。
- **過時** - 已知不再能夠到達此鄰居，且已在 1200 秒內將流量傳送到此鄰居。
- **固定** - 已手動將此鄰居設定為固定鄰居。

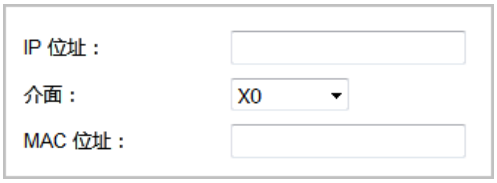
設定固定 NDP 項目

若要設定固定 NDP 項目，請執行以下步驟：

1 移至**網路 | 鄰居搜索**頁面。



2 按一下**固定 NDP 項目**表下面的**新增**。隨即顯示**新增固定 NDP** 對話方塊。



3 在 **IP 位址**欄位中，輸入遠端裝置的 IPv6 位址。

4 在**介面**中，選擇將作為項目使用的 SonicWall 安全設備介面。

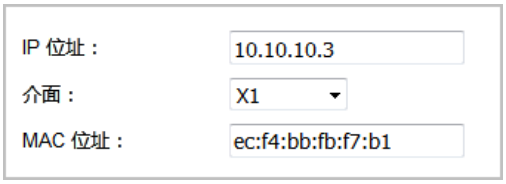
5 在 **MAC 位址**欄位中，輸入遠端裝置的 MAC 位址。

6 按一下**確定**。已新增了固定 NDP 項目。

編輯固定 NDP 項目

若要編輯固定 NDP 項目：

1 在**固定 NDP 項目**表中，按一下**設定**欄位中項目的**編輯**圖示。隨即顯示**編輯固定 NDP** 對話方塊。



2 做出變更。

3 按一下**確定**。項目即會更新。

排清 NDP 快取

如果網路中的裝置發生 IP 位址變化，有時可能需要排清 NDP 快取。由於 IP 位址與實體位址相關聯，因此有可能 IP 位址發生了變化，但仍舊與 NDP 快取中的實體位址相關聯。排清 NDP 快取可以在 NDP 快取中收集和儲存新資訊。

提示：若要設定具體的項目逾時時間，請在 **NDP 快取項目逾時（分鐘）**欄位中輸入以分鐘為單位的值。請參閱第 415 頁「NDP 設定」。

若要排清 NDP 快取表中的項目：

1 按下**排清**欄位中其**刪除**圖示。

若要排清 NDP 快取表中一個或多個項目：

1 勾選要排清的一個或多個項目的核取方塊。兩個排清按鈕隨即啟用。

2 按一下**排清**或**排清 NDP 快取**。

若要排情 NDP 快取表中的所有項目：

1 選取 **NDP 快取**表格標題中的核取方塊。兩個排清按鈕隨即啟用。

2 按一下**排清**或**排清 NDP 快取**。

23

設定 MAC-IP 反詐騙檢視

關於 MAC-IP 反詐騙檢視防護

基於 MAC 和 IP 位址的攻擊在目前的網路安全環境中越來越常見。這些類型的攻擊通常瞄準區域網路 (LAN)，且可能源自網路外部或內部。事實上，任何位置，只要內部 LAN 有所暴露，例如會議室、學校或圖書館等，都有可能給這些類型的攻擊提供可乘之機。這些攻擊還有其他多種名稱：中間人攻擊、ARP 破壞、SPITS。MAC-IP 反詐騙檢視功能透過為您提供多種方法來控制對網路的存取，以及透過消除位於 OSI 2/3 層的欺騙攻擊，降低了這類攻擊帶來的風險。

MAC-IP 反詐騙檢視功能的效能集中於兩個方面：

- 許可控制，這讓您能夠有權選擇存取網路的裝置。
- 消除欺騙攻擊，例如在第 2 層的拒絕服務攻擊。

若要實現上述目標，必須構建兩項資訊快取: MAC-IP 反詐騙檢視快取和 ARP 快取。

MAC-IP 反詐騙檢視快取將驗證傳入封包並確定這些封包是否允許進入網路內部。系統將在此快取中尋找傳入封包的來源 MAC 和 IP 位址。如果找到這些位址，則允許封包透過。MAC-IP 反詐騙檢視快取是透過下列一個或多個子系統構建而成:

- 以 DHCP 伺服器為基礎的租用 (SonicWall - DHCP 伺服器；僅限 IPv4)
- 以 DHCP 轉接為基礎的租用 (SonicWall - IP 協助程式；僅限 IPv4)

- 固定 ARP 項目；僅限 IPv4
- 使用者建立的固定項目

ARP 快取是透過下列子系統構建而成:

- ARP 封包；包括 ARP 請求和回應；僅限 IPv4
- 來自使用者建立項目的固定 ARP 項目；僅限 IPv4
- MAC-IP 反詐騙檢視快取

MAC-IP 反詐騙檢視子系統藉由鎖定 ARP 快取來控制輸出，因此不會有不良裝置或不必要的 ARP 封包欺騙輸出封包 (離開網路的封包)。這種做法可防止 SonicWall 安全設備根據對應，將封包路由到非預期的裝置。還可以透過在用戶端的 ARP 快取中重新整理用戶端自己的 MAC 位址來防範中間人攻擊。

IP 協助程式擴充

若要支援來自 IP 協助程式 DHCP 轉接子系統的租用 (**網路 | IP 協助程式**):

- 作為 DHCP 轉接邏輯的一部分，IP 協助程式學習在用戶端與 DHCP 伺服器之間交換的租用，然後將其儲存到閃存中。
- 這些經過學習的租用，會同步處理到閒置的 SonicWall 安全設備，作為 IP 協助程式狀態同步訊息的一部分。

系統會將租用提供的 MAC 和 IP 位址繫結，轉送到 MAC-IP 反詐騙檢視快取中。

如需更多 IP 協助程式相關資訊，請參閱第 459 頁「使用 IP 協助程式」。

網路 | MAC-IP 反詐騙

IPv6

IPv4

本章節說明如何計劃、設計和在 SonicWall SonicOS 中實作 MAC-IP 反詐騙檢視防護。

主題：

介面的設定

附註：綠色的勾選標記圖示代表已啟用的設定。

IPv6

介面的設定	會列出所有可套用 MAC-IP 反詐騙檢視設定的介面。預設的顯示設定為**全部**。
介面	**介面設定**中選取的介面。
強制的	指出是否在此介面上強制執行輸入反詐騙。
啟用	指出是否在此介面上啟用 MAC-IP 反詐騙檢視。
NDP 鎖定	指出是否在此介面上為每個傳輸封包啟用 MAC-IP 反詐騙檢視檢查功能。
固定 NDP	指出是否為每個固定 NDP 項目建立對應的 MAC-IP 反詐騙檢視表格項目。

詐騙偵測	指出是否為與反詐騙快取不符的封包，建立 MAC-IP 反詐騙檢視偵測到的清單。 **附註：**MAC-IP 反詐騙檢視清單中排除了下列介面: • 非乙太網路介面 • 連接埠屏蔽成員介面 • 二層橋接配對介面 • 高可用性介面 • 高可用性資料介面
允許管理	指出是否允許所有目的地為安全設備的流量，而無需有效的 MAC-IP 反詐騙檢視快取。
設定	包含項目的**統計資料**和**編輯**圖示。

IPv4

介面的設定	會列出所有可套用 MAC-IP 反詐騙檢視設定的介面。預設的顯示設定為**全部**。
介面	**介面設定**中選取的介面。
強制的	指出是否在此介面上強制執行輸入反詐騙。
啟用	指出是否在此介面上啟用 MAC-IP 反詐騙檢視。
ARP 鎖定	指出是否在此介面上為每個傳輸封包啟用 MAC-IP 反詐騙檢視檢查功能。
ARP 監控	指出是否啟用防止所連接機器的 ARP 破壞。
固定 ARP	指出是否為每個固定 ARP 項目建立對應的 MAC-IP 反詐騙檢視表格項目。
DHCP 伺服器	指出是否從 DHCP 租用填入 MAC-IP 反詐騙檢視項目 (SonicWall 的 DHCP 伺服器)。
DHCP 轉接	指出是否從 DHCP 租用填入 MAC-IP 反詐騙檢視項目 (DHCP 轉接 - IP 協助程式)。
詐騙偵測	指出是否為與反詐騙快取不符的封包，建立 MAC-IP 反詐騙檢視偵測到的清單。 **附註：**MAC-IP 反詐騙檢視清單中排除了下列介面: • 非乙太網路介面 • 連接埠屏蔽成員介面 • 二層橋接配對介面 • 高可用性介面 • 高可用性資料介面
允許管理	指出是否允許所有目的地為防火牆的流量，而無須有效的 MAC-IP 反詐騙檢視快取。
設定	包含項目的**統計資料**和**編輯**圖示。

反詐騙快取

MAC-IP 反詐騙檢視快取會列出所有的 MAC 位址到 IP 位址繫結，其中可包括目前狀態如下的所有裝置:

- 列為「已獲授權」，可存取網路。
- 標記為運作方式如同路由器，且設有網路的裝置。
- 標記為「已列入黑名單」(存取遭拒)，無法存取網路。

即便啟用 MAC-IP 反詐騙檢視功能，系統仍會略過某些封包類型。

- 非 IP 封包。
- 來源 IP 為 0 的 DHCP 封包。
- 來自 VPN 通道的封包。
- 作為其來源 IP 為無效的單點傳送 IP 的封包。
- 來自未在反詐騙設定下面啟用管理狀態的介面的封包。

反詐騙查詢統計資料會顯示在表格底部。

IP 位址	裝置的 IP 位址
類型	項目類型: **固定**或**租用**
介面	接收內送流量的介面
MAC 位址	裝置的 MAC 位址
供應商	裝置製造商 (如有相關資訊)
主機名稱	裝置主機名稱 (如有相關資訊)
路由	裝置在設定時被指定為可用路由器
黑名單	裝置在設定時被指定列入黑名單
設定	顯示每個項目的**統計**、**編輯**和**刪除**圖示

若要清除一部或多部裝置的快取統計資料:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 選取一部或多部裝置。

3 按一下**清除統計資料**。

若要查看可用的最新快取資料:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 按一下**反詐騙快取**表格底部的**重新整理**。

偵測到的反詐騙清單

偵測到的反詐騙清單中顯示了未能透過輸入反詐騙快取檢查的裝置。這份清單中的項目可新增為**反詐騙快取**表格中的固定反詐騙項目。

IP 位址	裝置的 IP 位址。
介面	接收內送流量的介面。
MAC 位址	裝置的 MAC 位址。
供應商	裝置製造商 (如有相關資訊)。
名稱	裝置的名稱。
封包	接收的封包數。
新增	顯示**編輯**圖示。

若要清空詐騙偵測清單:

1 按一下**排清**。

若要使用 NetBio 解析每部裝置的名稱:

1 按一下**解析**。

若要查看可用的最新快取資料:

1 按一下**詐騙偵測清單**表格底部的**重新整理**。

設定 MAC-IP 反詐騙檢視防護

主題：

顯示流量統計

若要在設定或反詐騙快取表格中顯示指定介面的流量統計資料:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 如需在**設定**表格中顯示指定介面的流量統計資料，請在**介面設定**中選取要顯示的介面；預設設定為**全部**。

3 將滑鼠游標移至該介面的**統計**圖示。

4 **流量統計**彈出式視窗隨即顯示:

設定表格

反詐騙快取表格

編輯 IPv6 介面的 MAC-IP 反詐騙檢視設定

若要指定特定介面的 MAC-IP 反詐騙檢視設定:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 在**介面設定**表格中，按一下所需介面的**設定**圖示。隨即顯示**編輯 MAC-IP 反詐騙檢視設定**對話方塊。

3 如需透過這個介面，依據反詐騙功能啟用 MAC 位址和 IP 位址流量，請在**反詐騙設定**部分中，選取**啟用 - 啟用以 MAC-IP 為基礎的反詐騙功能**。 預設情況下未勾選此選項。

4 如需在 MAC-IP 反詐騙檢視表格中，為每個固定 NDP 項目建立相應的項目，請選取**固定 NDP - 從固定 NDP 項目填入 MAC-IP 反詐騙項目**。 預設情況下未勾選此選項。

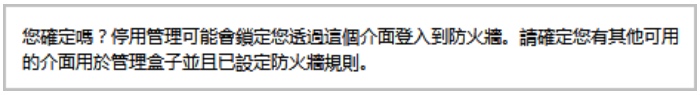
5 如需為反詐騙快取內的每一個 MAC-IP 繫結新增 NDP 快取項目，請在 **NDP 設定**部分中，選取 **NDP 鎖定 - 鎖定 NDP 快取中的 MAC-IP 繫結，避免其他繫結出現 NDP 破壞情形**。 預設情況下未勾選此選項。

6 如需為每個傳送封包啟用 MAC-IP 反詐騙檢查，請在**雜項設定**部分中，選取**強制執行 - 強制執行輸入反詐騙 - 捨棄與 MAC-IP 反詐騙快取不符的封包**。 預設情況下未勾選此選項。

7 如需為每部無法通過 MAC-IP 反詐騙檢視快取檢查的裝置建立詐騙偵測清單，請選取**詐騙偵測 - 為與反詐騙快取不符的封包建立 MAC-IP 詐騙偵測清單**。 預設情況下未勾選此選項。

8 如需允許所有目的地為安全設備的流量 (包括沒有有效的 MAC-IP 反詐騙檢視快取的流量在內)，請選取**許可管理 - 允許所有目的地為此裝置的流量無需有效的 MAC-IP 反詐騙快取**。 預設情況下已核取此選項。

注意：**如果您停用這個選項，則可能無法透過這個介面登入 SonicWall 安全設備。請確認您有其他可用於管理安全設備的介面，且已妥善設定相關規則和原則。如果您停用了這個選項，系統會顯示下列警告訊息:**



9 按一下**確定**。

編輯 IPv4 介面的 MAC-IP 反詐騙檢視設定

若要指定特定介面的 MAC-IP 反詐騙檢視設定:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 在**介面設定**表格中，按一下所需介面的**設定**圖示。隨即顯示**編輯 MAC-IP 反詐騙檢視設定**對話方塊。

3 如需透過這個介面，依據反詐騙功能啟用 MAC 位址和 IP 位址流量，請在**反詐騙設定**部分中，選取**啟用 - 啟用以 MAC-IP 為基礎的反詐騙功能**。 預設情況下未勾選此選項。

4 如需在 MAC-IP 反詐騙表格中，為每個固定 ARP 項目建立相應的項目，請選取**固定 ARP - 從固定 ARP 項目填入 MAC-IP 反詐騙項目**。 預設情況下未勾選此選項。

5 如需在 MAC-IP 反詐騙檢視表格中，為 DHCP 伺服器配置的每個 DHCP 租用建立相應的項目，請選取 **DHCP 伺服器 - 從 DHCP 租用填入 MAC-IP 反詐騙項目 (SonicWall 的 DHCP 伺服器)**。 預設情況下未勾選此選項。

6 如需在 MAC-IP 反詐騙檢視表格中依據 DHCP 轉接設定，為遠端 DHCP 伺服器配置的每個 DHCP 租用建立相應的項目，請選取 **DHCP 轉接 - 從 DHCP 租用填入 MAC-IP 反詐騙項目 (DHCP 轉接 - IP 協助程式)**。 預設情況下未勾選此選項。

7 如需為反詐騙快取內的每一個 MAC-IP 繫結新增 ARP 快取項目，請在 **ARP 設定**部分中，選取 **ARP 鎖定 - 鎖定 ARP 快取中的 MAC-IP 繫結，避免其他繫結出現 ARP 破壞情形**。 預設情況下未勾選此選項。

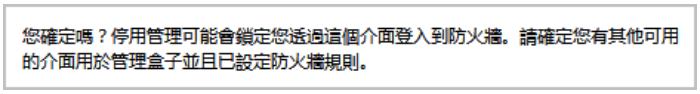
8 如需避免連線的裝置出現 ARP 破壞情形，同時保護所有用戶端電腦避免中間人攻擊，請選取 **ARP 監控 - 避免連線的機器出現 ARP 破壞情形**。 預設情況下未勾選此選項。

9 如需為每個傳送封包啟用 MAC-IP 反詐騙檢查，請在**雜項設定**部分中，選取**強制執行 - 強制執行輸入反詐騙 - 捨棄與 MAC-IP 反詐騙快取不符的封包**。 預設情況下未勾選此選項。

10 如需為每部無法通過 MAC-IP 反詐騙檢視快取檢查的裝置建立詐騙偵測清單，請選取**詐騙偵測 - 為與反詐騙快取不符的封包建立 MAC-IP 詐騙偵測清單**。 預設情況下未勾選此選項。

11 如需允許所有目的地為安全設備的流量 (包括沒有有效的 MAC-IP 反詐騙檢視快取的流量在內)，請選取**許可管理 - 允許所有目的地為此裝置的流量無需有效的 MAC-IP 反詐騙快取**。 預設情況下已核取此選項。

注意：**如果您停用這個選項，則可能無法透過這個介面登入 SonicWall 安全設備。請確認您有其他可用於管理安全設備的介面，且已妥善設定相關規則和原則。如果您停用了這個選項，系統會顯示下列警告訊息:**



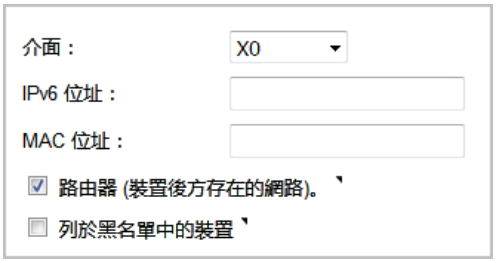
12 按一下**確定**。

為反詐騙快取新增裝置

若要為反詐騙快取新增裝置:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 按一下**反詐騙快取**表格下的**新增**。將顯示**新增固定 MAC-IP 反詐騙**對話方塊。



3 在**介面**中，選取裝置流量到達的目標介面。

4 在 **IP 位址**欄位，輸入裝置的 IP 位址。

5 在 **MAC 位址**欄位，輸入裝置的 MAC 位址。

6 若要將裝置指定為路由器，且可能設有網路，請選取 **A 路由器**。預設情況下已核取此選項。

7 若要將裝置列入黑名單，並封鎖來自該裝置的流量，請選取**列入黑名單的裝置**。預設情況下未勾選此選項。

將裝置列入黑名單會導致系列封鎖來自此裝置的封包 (無論裝置的 IP 位址為何)。

8 按一下**確定**。

刪除反詐騙快取項目

若要刪除單一固定反詐騙快取項目:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 按一下該項目的**刪除**圖示。

若要刪除一個或多個固定反詐騙快取項目:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 選取要刪除的項目。**刪除**按鈕隨即啟用。

3 按一下**刪除**。

若要刪除所有固定反詐騙快取項目

1 導覽到**網路 | MAC-IP 反詐騙**。

2 選取反詐騙快取表格標題中的核取方塊。**刪除**按鈕隨即啟用。

3 按一下**刪除**。

篩選要顯示的內容

您可以使用**篩選**功能，指定要在**反詐騙快取**和**詐騙偵測清單**表格中顯示的裝置。

若要篩選表格顯示內容:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 在要進行篩選的表格下方找到篩選欄位，在其中指定裝置的 IP 位址、介面、MAC 位址、主機名稱或名稱。您在填寫這個欄位時，必須使用篩選條件運算子語法選項表格中提供的適用運算子語法。

篩選條件運算子語法選項

運算子	語法選項
包含類型的值	• Ip=1.1.1.1 或 ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
String	• X1 • 00:01 • Tst-mc • 1.1.
AND	• Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string
OR	• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
Negative	• !ip=1.1.1.1;!just-string • !iface=x1,x2
Mixed	• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

從詐騙偵測清單新增固定項目

若要從詐騙偵測清單新增固定項目:

1 導覽到**網路 | MAC-IP 反詐騙**。

2 在**詐騙偵測清單**表格中找到所需裝置，然後按一下**新增**欄中的**編輯**圖示。隨即將顯示警示訊息，詢問您是否想要新增此固定項目。

3 按一下**確定**。

24

設定 DHCP 伺服器

網路 | DHCP 伺服器

網路 | DHCP 伺服器的 IPv6 和 IPv4 版本差異不大。

IPv6 網路 | DHCP 伺服器

IPv4 網路 | DHCP 伺服器

SonicWall 安全設備包含一個 DHCP（動態主機設定通訊協定）伺服器，用於向網路用戶端指派 IP 位址、子網路遮罩、閘道位址和 DNS 伺服器位址。**網路 | DHCP 伺服器**包括用於設定安全設備的 DHCP 伺服器的相關設定。

您可以使用安全設備的 DHCP 伺服器或網路中現有的 DHCP 伺服器。如果您的網路使用專屬的 DHCP 伺服器，則請勿勾選**啟用 DHCP 伺服器**。

防火牆的 DHCP 伺服器能夠指派的位址範圍和 IP 位址數量，取決於安全設備的型號、作業系統和授權。SonicWall 安全設備允許的最大 DHCP 租用數請參閱允許的最大 DHCP 租用數表格。

允許的最大 DHCP 租用數

平台	最大 DHCP 租用數	平台	最大 DHCP 租用數	平台	最大 DHCP 租用數
	16384	NSA 6600	16384	TZ600	4096
SM 9600	16384	NSA 5600	8192	TZ500/TZ500 W	4096
SM 9400	16384	NSA 4600	8192	TZ400/TZ400 W	4096
SM 9200	16384	NSA 3600	4096	TZ300/TZ300 W	4096
		NSA 2600	4096	SOHO W	4096

主題：

DHCP 伺服器選項功能

SonicWall DHCP 伺服器選項功能為 DHCP 選項（也稱為「供應商擴充」，基本定義參見 RFC 2131 和 2132）提供支援。DHCP 選項使得使用者能夠以預先定義的供應商指定資訊（儲存在 DHCP 訊息的選項欄位中）的形式指定附加的 DHCP 參數。將 DHCP 訊息傳送到網路中的用戶端時，它會提供供應商指定的設定和服務資訊。第 451 頁「RFC 定義的 DHCP 選項編號」一節按照 RFC 指派的選項編號列出了 DHCP 選項。

主題：

優點

SonicWall DHCP 伺服器選項功能提供了按編號或名稱選擇 DHCP 選項的簡單介面，使得 DHCP 設定過程更加快速、輕鬆且符合 RFC 規定的 DHCP 標準。

DHCP 伺服器選項功能如何工作

DHCP 伺服器選項功能允許基於 RFC 定義的選項編號，使用下拉功能表定義 DHCP 選項，以便管理員輕鬆地建立 DHCP 物件和物件群組，以及設定用於動態和固定 DHCP 租用範圍的 DHCP 一般選項。完成定義後，DHCP 選項將包含在 DHCP 訊息（此訊息隨後傳遞到網路中的 DHCP 用戶端）的選項欄位中，描述可用的網路設定和服務。

支援的標準

DHCP 伺服器選項功能支援以下標準：

- RFC 2131 - 動態主機設定通訊協定
- RFC 2132 - DHCP 選項和 BOOTP 供應商擴充

每個介面上的多個 DHCP 範圍

主題：

什麼是每個介面上的多個 DHCP 範圍？

通常，DHCP 用戶端和伺服器都位在同一 IP 網路或子網路中，但有時 DHCP 用戶端及其關聯的 DHCP 伺服器並未駐留在同一子網路中。每個介面上的多個 DHCP 範圍功能允許一個 DHCP 伺服器為跨越多個子網路的用戶端管理不同的範圍。

多個 DHCP 範圍的優點

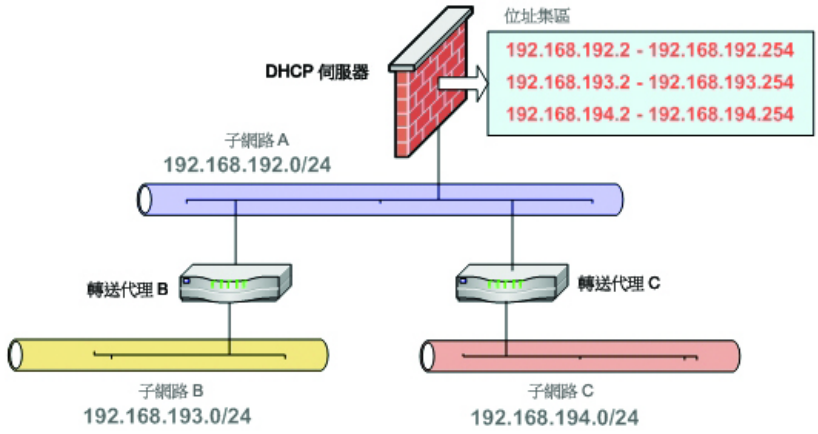
效率	單個 DHCP 伺服器可以為跨越多個子網路的用戶端提供 IP 位址。
相容 VPN 上的 DHCP	以統一的方式處理轉接 DHCP 訊息的處理，不論它來自 VPN 通道還是 DHCP 轉接代理。
用於站對站 VPN 的多個範圍	在使用內部 DHCP 伺服器時，可使用與 LAN/DMZ 子網路不同的範圍來設定遠端子網路。遠端子網路的範圍取決於在遠端閘道中設定的「轉接 IP 位址」。
用於群組 VPN 的多個範圍	在使用內部 DHCP 伺服器時，可使用與 LAN/DMZ 子網路不同的範圍來設定 SonicWall GVC 用戶端。GVC 用戶端的範圍取決於中央閘道內設定的「轉接 IP 位址 (可選)」選項。
相容衝突偵測	目前，在啟用此功能時，DHCP 伺服器將執行伺服器端衝突偵測。伺服器端衝突偵測的優勢在於，即使在 DHCP 用戶端未執行用戶端衝突偵測時，它仍會偵測衝突。但是，如果網路中有大量 DHCP 用戶端，伺服器端衝突偵測可能導致更長的等待時間，等待完成完整的 IP 位址指派。對於屬於「轉接」子網路範圍的 IP 位址，將不執行衝突偵測（和網路預發現）。DHCP 伺服器僅對連接到其介面的子網路範圍執行衝突偵測 ICMP 檢查。

每個介面上的多個 DHCP 範圍的工作方式

正常情況下，DHCP 用戶端會透過傳送一條廣播 DHCP 發現訊息來發起位址指派程式。由於多數路由器不轉送廣播封包，因此這種方法要求 DHCP 用戶端和伺服器位在同一 IP 網路或子網路。

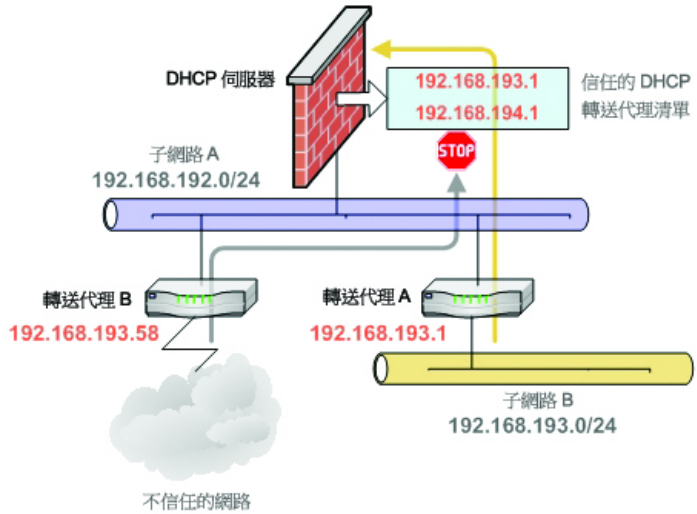
如果 DHCP 用戶端及其關聯的 DHCP 伺服器不在同一子網路中，則需要某種類型的供應商代理（例如 BOOTP 轉接代理、IP 協助程式等）在用戶端與伺服器之間傳送 DHCP 訊息；請參見共用同一 DHCP 伺服器的多個子網路。DHCP 轉接代理使用其輸入介面 IP 位址填充 giaddr 欄位，然後將其轉送至已設定的 DHCP 伺服器。當 DHCP 伺服器收到訊息時，它會查看 giaddr 欄位，以確認其是否擁有能夠用來向用戶端提供 IP 位址租用的 DHCP 範圍。

共用同一 DHCP 伺服器的多個子網路



每個介面上的多個 DHCP 範圍功能提供了安全增強功能來防範允許更廣泛的 DHCP 伺服器存取所固有的潛在漏洞。**DHCP 進階設定**對話利用「信任的代理」標籤提供安全性，在此標籤中可以指定可信的 DHCP 轉接代理；請參見可信的 DHCP 轉接代理。DHCP 伺服器將丟棄不在清單中的代理轉接的所有訊息。

可信的 DHCP 轉接代理



關於 DHCP 伺服器持續性

DHCP 伺服器持續性是安全設備儲存 DHCP 租用資訊，以及即使在用戶端重新啟動後仍舊為用戶端提供可預測的、不與網路中其他使用相衝突的 IP 位址的能力。

DHCP 伺服器持續性透過定期將 DHCP 租用資訊儲存到閃存中發揮作用。這樣可確保使用者擁有可預測的 IP 位址，並最大限度降低了重新啟動後發生 IP 定址衝突的風險。

DHCP 伺服器持續性在使用者重新啟動工作站時提供無縫的體驗。系統將儲存 DHCP 租用資訊，且使用者將保留相同的工作站 IP 位址。在通常由於維護或升級的原因重新啟動防火牆時，DHCP 伺服器持續性提供了以下好處：

- IP 位址唯一性：租用資訊儲存在閃存中，從而消除了將同一 IP 位址指派給多個使用者的風險。
- 設定簡單：透過在閃存中儲存租用資訊，自動恢復使用者的連接。

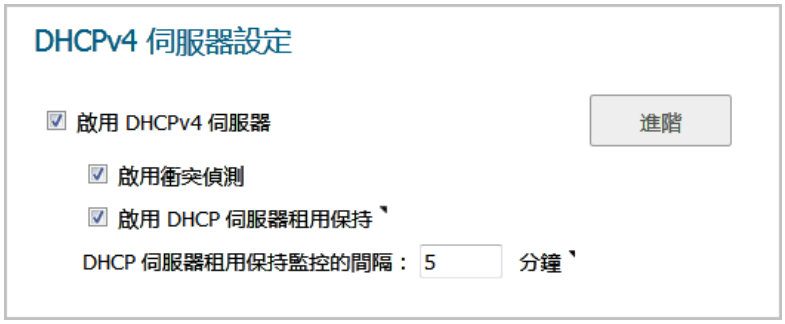
設定 DHCP 伺服器

若要使用 SonicWall 安全設備的 DHCP 伺服器:

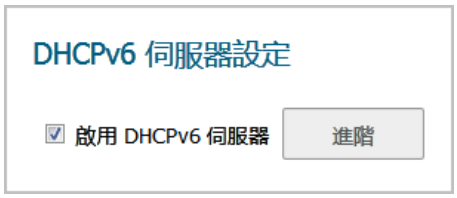
1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 在**檢視 IP 版本**中選擇要使用的 IP 版本:

- **IPv4**



- **IPv6**



3 如需將 IP 位址、子網路遮罩、閘道位址和 DNS 伺服器位址發埠到您的網路用戶端，請選取**啟用 DHCPv4/6 伺服器**。預設情況下已核取此選項。**進階**部分即可供使用，如果您使用的是 IPv4，則可使用伺服器設定選項。

4 如需設定 DHCPv6，請移至步驟 7。

5 如需在有另一部 DHCP 伺服器的情況下，為每個區域啟用自動 DHCP 範圍衝突偵測功能，請選取**啟用衝突偵測**。預設情況下已核取此選項。

目前，在啟用此功能時，DHCP 伺服器將執行伺服器端衝突偵測。伺服器端衝突偵測的優勢在於，即使在 DHCP 用戶端未執行用戶端衝突偵測時，它仍會偵測衝突。但是，如果網路中有大量 DHCP 用戶端，伺服器端衝突偵測可能導致更長的等待時間，等待完成完整的 IP 位址指派。

附註：對於屬於「轉接」子網路範圍的 IP 位址，將不執行衝突偵測。DHCP 伺服器僅對連接到其介面的子網路範圍執行衝突偵測 ICMP 檢查。

6 如需將網路中目前的 DHCP 租用狀態定期寫入 Flash，請選取**啟用 DHCP 伺服器持續性**。重新啟動時，系統將根據 Flash 中儲存的 IP.Lease 時間恢復先前的 DHCP 伺服器網路 DHCP 指派知識。預設情況下已核取此選項。 啟用這個選項後，即可使用 **DHCP 伺服器持續性監控間隔**選項。

- 如需控管系統檢查網路變更的頻率及寫入 Flash 的頻率 (如有必要)，請在 **DHCP 伺服器持續性監控間隔**中輸入所需時間 (以分鐘為單位)。預設值為 **5** 分鐘，最短為 5 分鐘，最長為 1440 分鐘 (24 小時)。

7 如需設定**選項物件**、**選項裙組**和**信任的代理**，請按一下**進階**。如需這些功能的設定的詳細資料，請參見第 438 頁「設定進階 DHCP 伺服器選項」。

8 按一下**接受**。

主題：

- 第 436 頁「為 DNS 代理設定 DHCP 伺服器」
- 第 438 頁「目前的 DHCPv4 租用情形」

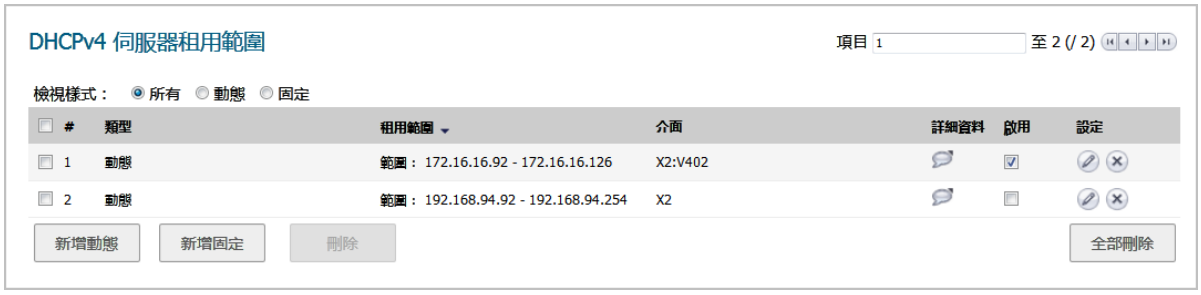
為 DNS 代理設定 DHCP 伺服器

在介面上啟用 DNS 代理時，裝置需要將做為 DNS 伺服器位址的介面 IP 推送至用戶端，所以您需要手動設定 DHCP 伺服器；在 **DNS/WINS** 標籤上的 DHCP 伺服器設定中，使用介面位址做為 **DNS 伺服器 1** 位址。DHCP 頁面中的**介面預先填入**核取方塊可使得這容易設定；如果所選介面已啟用 DNS 代理，DNS 伺服器 IP 會自動新增到 **DNS/WINS** 頁面。

DHCP 伺服器租用範圍

DHCPv6 伺服器租用範圍

DHCPv4 伺服器租用範圍



DHCP 伺服器租用範圍表中顯示了目前已設定的 DHCP IP 範圍。

- **類型**：動態或固定。
- **首碼**：僅 IPv6。
- **租用範圍**：IP 位址範圍，例如 `172.16.31.2-172.16.31.254`。
- **介面**：僅 IPv4。將此範圍指派到的介面。
- **詳細資料**：關於租用的詳細資料，在將滑鼠指標放在**註解**圖示上時顯示為工具提示。
- **啟用**：選取這個核取方塊即可啟用 DHCP 範圍。清除核取方塊將停用此範圍。
- **設定**：包含指定表格項目的**設定**和**刪除**圖示。

目前 DHCP 租用

主題：

- 第 437 頁「目前的 DHCPv6 租用情形」
- 第 438 頁「目前的 DHCPv4 租用情形」

目前的 DHCPv6 租用情形

目前 DHCP 租用資訊顯示在**目前 DHCP 租用**表中。每個繫結項目顯示：

- **IPv6 位址**
- **租用過期**
- **IAID**
- **DUID**
- 繫結的**類型 (動態**、**動態 BOOTP** 或**固定 BOOTP**）。
- **刪除**圖示

若要刪除繫結，釋出 DHCP 伺服器上的 IP 位址:

1 按一下所需項目旁邊的**刪除**圖示。例如，在已經從網路中刪除某個主機並需要重新使用其 IP 位址的情況下，使用**移除**圖示可移除此主機。

2 按一下**接受**。

目前的 DHCPv4 租用情形

目前 DHCP 租用資訊顯示在**目前 DHCP 租用**表中。每個繫結項目顯示：

- **IP 位址**
- **主機名稱**
- **租用過期**
- **乙太網路位址**
- **供應商**
- **類型 (動態**、**動態 BOOTP** 或**固定 BOOTP**）。
- **刪除**圖示

若要刪除繫結，釋出 DHCP 伺服器上的 IP 位址:

1 按一下所需項目旁邊的**刪除**圖示。例如，在已經從網路中刪除某個主機並需要重新使用其 IP 位址的情況下，使用**移除**圖示可移除此主機。

2 按一下**接受**。

設定進階選項

主題：

- 第 438 頁「設定進階 DHCP 伺服器選項」

設定進階 DHCP 伺服器選項

附註：IPv4 和 IPv6 的 DHCP 伺服器設定選項基本來說沒有差異。例外的部分會在步驟中說明。

主題：

- 第 439 頁「設定 DHCP 選項物件」
- 第 441 頁「設定 DHCP 選項群組」

- 第 443 頁「設定信任的 DHCP 轉接代理位址群組 (僅限 IPv4)」
- 第 443 頁「啟用可信的 DHCP 轉接代理」

第 451 頁「RFC 定義的 DHCP 選項編號」中按照 RFC 指派的選項編號提供了 DHCP 選項清單。

設定 DHCP 選項物件

若要設定 DHCP 選項物件：

1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 按一下 **DHCPv4/6 伺服器設定**下的**進階**。將顯示 **DHCP 進階設定**對話方塊。

IPv6 DHCP 進階設定

IPv4 DHCP 進階設定

3 按一下**新增選項**。此時會顯示**新增 DHCP 選項物件**對話方塊。

4 在**選項名稱**欄位中輸入選項的名稱。

5 在**選項編號**中，選取您的 DHCP 選項所對應的選項編號。如需選項編號和名稱的清單，請參考第 451 頁「RFC 定義的 DHCP 選項編號」。

6 如果**選項陣列**的狀態為:

- 灰色，請移至步驟 8。
- 可供使用，您可以視需求選取這個選項，在**選項值**欄位中輸入多個選項值。

7 如果：

- 可用的選項類型只有一種，例如**選項編號為 2 (時間偏移)** 時，**選項陣列**就會顯示為灰色。移至步驟 8。
- 有多個可用的選項類型，例如**選項編號為 77 (使用者類別資訊)** 時，**選項類型**就可供使用，系統也會顯示選項類型。如果：
  - 選項編號相關的選項類型只有一種，**選項類型**就會顯示為灰色。移至步驟 8。
  - 選項編號相關的選項類型不止一種，**選項類型**就可供使用，系統也會列出相關選項。選擇選項類型。

8 在**選項值**欄位中輸入選項值，例如 IP 位址。如果已核取**選項陣列**，則可以輸入多個用分號 (;) 分隔的值。

9 按一下**確定**。物件隨即會顯示在**選項物件**表格中。

DHCPv6 選項物件表格

DHCPv4 選項物件表格

設定 DHCP 選項群組

若要設定 DHCP 選項群組：

1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 按一下 **DHCPv4/6 伺服器設定**下的**進階**。將顯示 **DHCP 進階設定**對話方塊。

IPv6 DHCP 進階設定

3 按一下**選項群組**標籤。

4 按下**新增群組**。隨即顯示**新增 DHCP/v6 選項群組**對話方塊。

5 在**名稱**欄位中輸入群組的名稱。

6 從左側欄中選擇一個選項物件，然後按一下**右箭頭**按鈕，將此選項物件新增到群組中。若要同時選擇多個選項物件，請按住 **Ctrl** 鍵，同時選擇選項物件。

7 按一下**確定**。群組隨即會顯示在**選項群組**表格中。

DHCPv6 選項群組表格

DHCPv4 選項群組表格

設定信任的 DHCP 轉接代理位址群組 (僅限 IPv4)

若要設定 **Default Trusted Relay Agent List** 位址群組，必須先為每個受信的轉接代理設定一個位址物件，然後再將這些位址物件新增到 **Default Trusted Relay Agent List** 位址群組或自訂位址群組中。

您可以在**管理 | 政策 | 物件 > 位址物件**中設定位址物件和位址群組。如需瞭解如何設定位址物件和位址群組，請參閱 *SonicOS 原則*。

啟用可信的 DHCP 轉接代理

在 **DHCP 進階設定**對話中，可以使用 **Default Trusted Relay Agent List** 位址群組啟用**信任的轉接代理清單**選項，或使用現有的位址物件建立另一個位址物件。

若要啟用「信任的轉接代理清單」選項並選擇需要的位址群組：

1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 按一下 **DHCPv4/6 伺服器設定**下的**進階**。將顯示 **DHCP 進階設定**對話方塊。

3 按一下**信任的代理**。

4 選取**啟用信任的 DHCP 轉接代理清單**。預設情況下未勾選此選項。您隨即可使用**信任的轉接代理清單**。

5 在**預設的信任轉接代理清單**中選取位址群組。下拉功能表包含所有現有的位址群組以及**建立新位址物件群組**選項。

> **附註：**如需為此選項建立自訂位址群組，請選擇**建立新位址物件群組**。隨即顯示**新增位址物件群組**對話方塊。如需瞭解如何設定位址群組，請參閱 *SonicOS 原則*。

6 按一下**確定**，即可透過所選的位址群組來啟用**信任的轉接代理清單**選項。

設定用於動態範圍的 DHCP 伺服器

由於 SonicOS 允許每個介面上的多個 DHCP 範圍，因此在設定 DHCP 範圍時，無需將子網路範圍關聯到介面。

若要設定用於動態 IP 位址範圍的 DHCP 伺服器：

1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 按一下 **DHCPv4/6 伺服器租用範圍**表格下的**新增動態**。對於：

- IPv6，系統會隨即顯示**新增 DHCPv6 動態範圍**對話方塊。移至第 444 頁「新增 DHCPv6 動態範圍」。
- IPv4，系統會隨即顯示**動態範圍設定**對話方塊。移至第 446 頁「動態範圍設定」。

新增 DHCPv6 動態範圍

1 如需啟用這個範圍，請務必選取**啟用此 DHCP 範圍**。 預設情況下已核取此選項。

2 在**名稱**欄位中輸入範圍的名稱。

3 在**首碼**欄位中，輸入範圍發佈 IPv6 位址時所用的首碼。

4 在**範圍開始**和**範圍結束**欄位中，分別輸入所需內容。兩個位址都必須在首碼的範圍內。

5 在**有效存留時間**欄位中，輸入範圍所租用的 IPv6 位址的有效存留時間 (以分鐘為單位)。最小值為 0，最大值為 71582789，預設值為 **2160**。

6 在**慣用存留時間**欄位中，輸入範圍所租用的 IPv6 位址的慣用存留時間 (以分鐘為單位)。最小值為 0，最大值為 71582789，預設值為 **1440**。

7 可以選擇在**註解**欄位中輸入註解。

8 按一下 **DNS**。

DNS

1 在**網域名稱**欄位中輸入網域名稱。

2 選擇是否要進行下列操作:

- 若要**動態繼承 SonicWall 的 DNS 設定**，請移至步驟 4。
- **手動指定**。**DNS 伺服器 1/2/3** 欄位將可供使用。

3 在個別的 **DNS 伺服器 1/2/3** 欄位中輸入 DNS 伺服器的 IP 位址。

4 按一下**進階**。

進階

1 在 **DHCPv6 一般選項**中，選取 DHCP 選項物件或群組。預設為**無**。如需設定新的 DHCPv6 選項或群組，請參閱第 439 頁「設定 DHCP 選項物件」和/或第 441 頁「設定 DHCP 選項群組」。

2 如果您想要傳送這個範圍所有已設定的 DHCPv6 選項，不受 DHCPv6 用戶端傳送的訊息中所含的「選項要求」選項限制，請選取**一律傳送 DHCPv6 選項**。 預設情況下未勾選此選項。

3 按一下**確定**。

動態範圍設定

1 如需啟用這個範圍，請務必選取**啟用此 DHCP 範圍**。 預設情況下已核取此選項。

2 如需在**範圍開始**、**範圍結束**、**預設閘道**和**子網路遮罩**欄位中填入指定介面的預設值，請選取對話方塊底部附近的**預先填入介面**。此下拉功能表變成可用。預設情況下未勾選此選項。

   a 在下拉功能表中選擇介面。所填入的 IP 位址與所選的介面位於同一私人子網路中。

重要：若要從介面功能表中選擇某個介面，必須先對介面進行完整設定，且介面必須為區域類型 LAN、WLAN 或 DMZ，或為 VLAN 子介面。

3 使用在**範圍開始**和**範圍結束**欄位中填入的 IP 位址範圍項目或輸入您自己的 IP 位址範圍。

4 在**租用時間 (分鐘數)** 欄位中，輸入範圍發出另一個 IP 位址前，原 IP 位址的租用分鐘數。下限為 0，上限為 71582789，而預設值為 **1440** 分鐘 (24 小時)。

5 使用填入的閘道位址，或在**預設閘道**欄位中輸入閘道的 IP 位址。

6 使用填入的子網路遮罩，或在**子網路遮罩**欄位中輸入閘道子網路遮罩。

7 可以選擇在**註解**欄位中輸入註解。

8 如果網路中有 BOOTP 用戶端，請勾選**允許 BOOTP 用戶端使用範圍**。預設情況下未勾選此選項。

   BOOTP 代表 bootstrap 通訊協定，此通訊協定是無磁碟工作站用於從 BOOTP 伺服器獲取其 IP 位址、其他 TCP/IP 設定資訊及其開機映像檔案的 TCP/IP 通訊協定和服務。

9 按一下 **DNS/WINS** ，繼續設定 DHCP 伺服器功能。

DNS/WINS

10 如果您有 DNS 伺服器的網域名稱，請將其填入**網域名稱**欄位。

11 選擇是否要進行下列操作:

- 若要**動態繼承 SonicWall 的 DNS 設定**，請移至步驟 13。
- **手動指定**。**DNS 伺服器 1/2/3** 欄位將可供使用。

12 在個別的 **DNS 伺服器 1/2/3** 欄位中輸入 DNS 伺服器的 IP 位址。

13 如果網路中有正在執行的 WINS，請在 **WINS 伺服器 1** 欄位中輸入 WINS 伺服器 IP 位址。可以新增一個額外的 WINS 伺服器。

14 按一下**進階**。**進階**選項可讓您設定 DHCP 伺服器，向網路中的 VoIP 用戶端傳送 Cisco 呼叫管理程式資訊。

進階

1 在 **VoIP 呼叫管理員**下面的**呼叫管理員 1** 欄位中，輸入您的 VoIP 呼叫管理員的 IP 位址或 FQDN。可以新增兩個額外的 VoIP 呼叫管理員位址。

2 在**網路啟動設定**下面的**下一個伺服器**欄位中，輸入 PXE 用戶端在啟動過程的下一階段中使用的 PXE 啟動伺服器（TFTP 伺服器）的 IP 位址。

> **重要：網路啟動設定**下面的欄位用於預啟動執行環境 (PXE)，在此環境中，用戶端使用在網路介面上獲取的檔案啟動。PXE 用戶端從 DHCP 伺服器中獲取 PXE 啟動伺服器的 IP 位址和名稱以及開機檔案的名稱。
>
> 在使用這些選項時，請勾選 **DHCP 一般選項**下面的 **PXE** 。

3 在**開機檔案**欄位中，輸入 PXE 用戶端可透過 TFTP 從 PXE 啟動伺服器獲取的開機檔案名稱。

4 在**伺服器名稱**欄位中，輸入 PXE 啟動伺服器 (TFTP 伺服器) 的 DNS 主機名稱。

5 如需設定 DHCP 一般選項的資訊，請參見第 451 頁「設定用於 DHCP 租用範圍的 DHCP 一般選項」。

6 按一下**確定**。

7 按一下**接受**，以便設定在防火牆中生效。

如需 SonicWall 安全裝置中的 VoIP 支援功能的更多資訊，請參見第 593 頁「關於 VoIP」。

設定固定 DHCP 項目

固定項目是指派給需要永久 IP 設定的伺服器的 IP 位址。由於 SonicOS 允許每個介面上的多個 DHCP 範圍，因此在設定 DHCP 範圍時，無需將子網路範圍關聯到介面。

若要設定固定項目：

1 導覽到**管理 | 系統安裝 | 網路 | DHCP 伺服器**。

2 按一下 **DHCPv4/6 伺服器租用範圍**表格下的**新增固定項目**。對於：

- IPv6，系統會隨即顯示**新增 DHCPv6 固定範圍**對話方塊。移至第 449 頁「新增 DHCPv6 固定範圍」。
- IPv4，系統會隨即顯示**固定項目設定**對話方塊。移至第 450 頁「固定項目設定」。

新增 DHCPv6 固定範圍

1 如需啟用這個範圍，請務必選取**啟用 DHCPv6 範圍**。 預設情況下已核取此選項。

2 在**項目名稱**欄位中輸入固定 DHCPv6 項目的名稱。

3 在**首碼**欄位中，輸入範圍發佈 IPv6 位址時所用的首碼。

4 在**固定 IPv6 位址**欄位中，輸入 IPv6 位址。位址必須在首碼的範圍內。

5 在 **IAID** 欄位中採用十進位格式，輸入 IAID (介面關聯識別碼)長度下限為 10 個字元，上限為 4294967295 個字元。

6 在 **DUID** 欄位中輸入 DUID (裝置唯一識別碼)。長度上限為 128 個字元。

7 在**有效存留時間**欄位中，輸入範圍所租用的 IPv6 位址的有效存留時間 (以分鐘為單位)。最小值為 0，最大值為 71582789，預設值為 **2160**。

8 在**慣用存留時間**欄位中，輸入範圍所租用的 IPv6 位址的慣用存留時間 (以分鐘為單位)。最小值為 0，最大值為 71582789，預設值為 **1440**。

9 可以選擇在**註解**欄位中輸入註解。

10 如需瞭解如何指定 DNS 和進階設定，請分別參閱第 445 頁「DNS」和第 445 頁「進階」。

固定項目設定

1 如需啟用這個範圍，請務必選取**啟用此 DHCP 範圍**。 預設情況下已核取此選項。

2 在**項目名稱**欄位中輸入固定項目的名稱。

3 在**固定 IP 位址**欄位中輸入裝置的 IP 位址。

4 在**乙太網路位址**欄位中輸入裝置的乙太網路 (MAC) 位址。

5 如需在**租用時間**、**預設閘道**和**子網路遮罩**欄位中填入指定介面的預設值，請選取對話方塊底部附近的**預先填入介面**。此下拉功能表變成可用。預設情況下未勾選此選項。

   a 在下拉功能表中選擇介面。所填入的 IP 位址與所選的介面位於同一私人子網路中。

   重要：若要從介面功能表中選擇某個介面，必須先對介面進行完整設定，且介面必須為區域類型 LAN、WLAN 或 DMZ，或為 VLAN 子介面。

6 在**租用時間 (分鐘數)** 欄位中，輸入範圍發出另一個 IP 位址前，原 IP 位址的租用分鐘數。下限為 0，上限為 71582789，而預設值為 **1440** 分鐘 (24 小時)。

7 使用填入的閘道位址，或在**預設閘道**欄位中輸入閘道的 IP 位址。

8 使用填入的子網路遮罩，或在**子網路遮罩**欄位中輸入閘道子網路遮罩。

9 可以選擇在**註解**欄位中輸入註解。

10 如需瞭解如何指定 DNS/WINS 和進階設定，請分別參閱第 447 頁「DNS/WINS」和第 448 頁「進階」。

11 按一下**確定**將設定新增到防火牆。

12 按一下**接受**，以便設定在防火牆中生效。

如需 SonicWall 安全裝置中的 VoIP 支援功能的更多資訊，請參見第 593 頁「關於 VoIP」。

設定用於 DHCP 租用範圍的 DHCP 一般選項

本章節介紹用於 DHCP 租用範圍一般選項的設定任務。

附註：在設定 DHCP 租用範圍一般選項之前，必須先建立固定或動態 DHCP 伺服器租用範圍。

第 451 頁「RFC 定義的 DHCP 選項編號」中按照 RFC 指派的選項編號提供了 DHCP 選項清單。

若要設定用於 DHCP 伺服器租用範圍的 DHCP 一般選項：

1 如果：

- 調整現有的 DHCP 租用範圍:
  1) 在**網路 | DHCP 伺服器**的 DHCP 伺服器租用範圍下，找到出租用範圍。
  2) 按一下**設定**圖示。
  3) 在顯示的對話方塊中按一下**進階**。
- 建立新的 DHCP 租用範圍:
  1) 在**一般**和 **DNS/WINS** 標籤下設定相關選項後，請按一下**進階**標籤 (請參閱第 444 頁「設定用於動態範圍的 DHCP 伺服器」或第 448 頁「設定固定 DHCP 項目」)。

2 在 **DHCP 一般選項群組**下拉功能表中選擇一個 DHCP 選項或選項群組。

在已設定**網路啟動設定**欄位以配合使用 PXE 時，在此處勾選 **PXE**。

3 若要始終對此 DHCP 伺服器租用範圍使用 DHCP 選項，請勾選**永遠傳送一般選項**。

4 按一下**確定**。

RFC 定義的 DHCP 選項編號

選項編號	名稱	說明
2	時間偏移	與 UTC 的時間偏移（以秒為單位）
3	路由器	N/4 路由器位址
4	時間伺服器	N/4 時間伺服器位址
5	名稱伺服器	N/4 IEN-116 伺服器位址
6	DNS 伺服器	N/4 DNS 伺服器位址
7	記錄伺服器	N/4 記錄伺服器位址
8	Cookie 伺服器	N/4 引用伺服器位址
9	LPR 伺服器	N/4 印表機伺服器位址
10	Impress 伺服器	N/4 Impress 伺服器位址
11	RLP 伺服器	N/4 RLP 伺服器位址
12	主機名稱	主機名稱字串，例如 **(Server Unicast)**
13	開機檔案大小	開機檔案的大小，以 512 位元組區塊為單位
14	Merit 傾印檔案	若要傾印的用戶端和傾印到的檔案名稱
15	網域名稱	用戶端的 DNS 網域名稱

選項編號	名稱	說明
16	交換伺服器	交換伺服器位址
17	根路徑	根磁碟的路徑名稱
18	擴充檔案	獲取更多 BOOTP 資訊的修補程式名稱
19	IP 層轉送	啟用或停用 IP 轉送
20	來源路由啟用程式	啟用或停用來源路由
21	原則篩選條件	路由原則篩選條件
22	最大 DG 重組大小	最大資料包重組大小
23	預設 IP TTL	預設 IP 存留時間
24	路徑 MTU 逾時	路徑 MTU 逾時
25	MTU 平台	路徑 MTU 平台表
26	介面 MTU 大小	介面 MTU 大小
27	所有子網路均為本機子網路	所有子網路均為本機子網路
28	廣播位址	廣播位址
29	執行遮罩探索	執行遮罩探索
30	向其他網路提供遮罩	向其他網路提供遮罩
31	執行路由器探索	執行路由器探索
32	路由器請求位址	路由器請求位址
33	固定路由表	固定路由表
34	尾部封裝	尾部封裝
35	ARP 快取逾時	ARP 快取逾時
36	乙太網路壓縮	乙太網路壓縮
37	預設 TCP 存留時間	預設 TCP 存留時間
38	TCP 存留間隔	TCP 存留間隔
39	TCP 存留無用項目	TCP 存留無用項目
40	NIS 網域名稱	NIS 網域名稱
41	NIS 伺服器位址	NIS 伺服器位址
42	NTP 伺服器位址	NTP 伺服器位址
43	供應商特有資訊	供應商特有資訊
44	NetBIOS 名稱伺服器	NetBIOS 名稱伺服器
45	NeTBIOS 資料包發佈	NeTBIOS 資料包發佈
46	NeTBIOS 節點類型	NeTBIOS 節點類型
47	NetBIOS 範圍	NetBIOS 範圍
48	X 視窗字型伺服器	X 視窗字型伺服器
49	X 視窗顯示管理員	X 視窗顯示管理員
50	請求的 IP 位址	請求的 IP 位址
51	IP 位址租用時間	IP 位址租用時間
52	選項多載	多載「sname」或「file」
53	DHCP 訊息類型	DHCP 訊息類型
54	DHCP 伺服器識別項	DHCP 伺服器識別項

選項編號	名稱	說明
55	參數請求清單	參數請求清單
56	訊息	DHCP 錯誤訊息
57	DHCP 最大訊息大小	DHCP 最大訊息大小
58	更新時間值	DHCP 更新 (T1) 時間
59	重新繫結時間值	DHCP 重新繫結 (T2) 時間
60	用戶端識別項	用戶端識別項
61	用戶端識別項	用戶端識別項
62	Netware/IP 網域名稱	Netware/IP 網域名稱
63	Netware/IP 子選項	Netware/IP 子選項
64	NIS+ V3 用戶端網域名稱	NIS+ V3 用戶端網域名稱
65	NIS+ V3 伺服器位址	NIS+ V3 伺服器位址
66	TFTP 伺服器名稱	TFTP 伺服器名稱
67	開機檔案名稱	開機檔案名稱
68	主代理位址	主代理位址
69	簡單郵件伺服器位址	簡單郵件伺服器位址
70	郵局伺服器位址	郵局伺服器位址
71	網路新聞伺服器位址	網路新聞伺服器位址
72	WWW 伺服器位址	WWW 伺服器位址
73	Finger 伺服器位址	Finger 伺服器位址
74	聊天伺服器位址	聊天伺服器位址
75	StreetTalk 伺服器位址	StreetTalk 伺服器位址
76	StreetTalk 目錄協助位址	StreetTalk 目錄協助位址
77	使用者類別資訊	使用者類別資訊
78	SLP 目錄代理	目錄代理資訊
79	SLP 服務範圍	服務位置代理範圍
80	快速提交	快速提交
81	FQDN，完整網域名稱	完整網域名稱
82	轉接代理資訊	轉接代理資訊
83	網際網路儲存名稱服務	網際網路儲存名稱服務
84	未定義	N/A
85	Novell 目錄伺服器	Novell 目錄服務伺服器
86	Novell 目錄伺服器樹狀目錄名稱	Novell 目錄服務伺服器樹狀目錄名稱
87	Novell 目錄伺服器內容	Novell 目錄服務伺服器內容
88	BCMCS 控制器網域名稱清單	BCMCS 控制器網域名稱清單
89	BCMCS 控制器 IPv4 位址清單	BCMCS 控制器 IPv4 位址清單
90	驗證	驗證
91	未定義	N/A
92	未定義	N/A
93	用戶端系統	用戶端系統結構

選項編號	名稱	說明
94	用戶端網路裝置介面	用戶端網路裝置介面
95	LDAP 使用	輕量型目錄存取通訊協定
96	未定義	N/A
97	基於 UUID/GUID 的用戶端識別項	基於 UUID/GUID 的用戶端識別項
98	開啟群組的使用者驗證	開啟群組的使用者驗證
99	未定義	N/A
100	未定義	N/A
101	未定義	N/A
102	未定義	N/A
103	未定義	N/A
104	未定義	N/A
105	未定義	N/A
106	未定義	N/A
107	未定義	N/A
108	未定義	N/A
109	自發系統編號	自發系統編號
110	未定義	N/A
111	未定義	N/A
112	NetInfo 父伺服器位址	NetInfo 父伺服器位址
113	NetInfo 父伺服器標記	NetInfo 父伺服器標記
114	URL：	URL
115	未定義	N/A
116	自動設定	DHCP 自動設定
117	名稱服務搜尋	名稱服務搜尋
118	子網路集合	子網路選擇
119	DNS 網域搜尋清單	DNS 網域搜尋清單
120	SIP 伺服器 DHCP 選項	SIP 伺服器 DHCP 選項
121	無類別固定路由選項	無類別固定路由選項
122	CCC，CableLabs 用戶端設定	CableLabs 用戶端設定
123	GeoConf	GeoConf
124	供應商識別，供應商類別	供應商識別，供應商類別
125	供應商識別，供應商特有	供應商識別，供應商特有
126	未定義	N/A
127	未定義	N/A
128	TFTP 伺服器 IP 位址	用於 IP 電話軟體載入的 TFTP 伺服器 IP 位址
129	呼叫伺服器 IP 位址	呼叫伺服器 IP 位址
130	辨識的字串	用於識別供應商的辨識字串
131	遠端統計伺服器 IP 位址	遠端統計伺服器 IP 位址
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 優先順序	IEEE 802.1Q 第 2 層優先順序

選項編號	名稱	說明
134	Diffserv 代碼點	用於 VoIP 訊號和媒體流的 Diffserv 代碼點
135	手機應用程式的 HTTP 代理	手機特定應用程式的 HTTP 代理
136	未定義	N/A
137	未定義	N/A
138	未定義	N/A
139	未定義	N/A
140	未定義	N/A
141	未定義	N/A
142	未定義	N/A
143	未定義	N/A
144	未定義	N/A
145	未定義	N/A
146	未定義	N/A
147	未定義	N/A
148	未定義	N/A
149	未定義	N/A
150	TFTP 伺服器位址，Etherboot，GRUB 設定	TFTP 伺服器位址，Etherboot，GRUB 設定
151	未定義	N/A
152	未定義	N/A
153	未定義	N/A
154	未定義	N/A
155	未定義	N/A
156	未定義	N/A
157	未定義	N/A
158	未定義	N/A
159	未定義	N/A
160	未定義	N/A
161	未定義	N/A
162	未定義	N/A
163	未定義	N/A
164	未定義	N/A
165	未定義	N/A
166	未定義	N/A
167	未定義	N/A
168	未定義	N/A
169	未定義	N/A
170	未定義	N/A
171	未定義	N/A
172	未定義	N/A
173	未定義	N/A

選項編號	名稱	說明
174	未定義	N/A
175	乙太網路啟動	乙太網路啟動
176	IP 電話	IP 電話
177	乙太網路啟動 PacketCable 和 CableHome	乙太網路啟動 PacketCable 和 CableHome
178	未定義	N/A
179	未定義	N/A
180	未定義	N/A
181	未定義	N/A
182	未定義	N/A
183	未定義	N/A
184	未定義	N/A
185	未定義	N/A
186	未定義	N/A
187	未定義	N/A
188	未定義	N/A
189	未定義	N/A
190	未定義	N/A
191	未定義	N/A
192	未定義	N/A
193	未定義	N/A
194	未定義	N/A
195	未定義	N/A
196	未定義	N/A
197	未定義	N/A
198	未定義	N/A
199	未定義	N/A
200	未定義	N/A
201	未定義	N/A
202	未定義	N/A
203	未定義	N/A
204	未定義	N/A
205	未定義	N/A
206	未定義	N/A
207	未定義	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212	未定義	N/A
213	未定義	N/A

選項編號	名稱	說明
214	未定義	N/A
215	未定義	N/A
216	未定義	N/A
217	未定義	N/A
218	未定義	N/A
219	未定義	N/A
220	子網路分配	子網路分配
221	虛擬子網路分配	虛擬子網路選擇
222	未定義	N/A
223	未定義	N/A
224	私用	私用
225	私用	私用
226	私用	私用
227	私用	私用
228	私用	私用
229	私用	私用
230	私用	私用
231	私用	私用
232	私用	私用
233	私用	私用
234	私用	私用
235	私用	私用
236	私用	私用
237	私用	私用
238	私用	私用
239	私用	私用
240	私用	私用
241	私用	私用
242	私用	私用
243	私用	私用
244	私用	私用
245	私用	私用
246	私用	私用
247	私用	私用
248	私用	私用
249	私用	私用
250	私用	私用
251	私用	私用
252	私用	私用
253	私用	私用
254	私用	私用

DHCP 和 IPv6

如需 SonicOS 的 IPv6 實作的完整資訊，請參見第 761 頁「IPv6」。

25

使用 IP 協助程式

關於 IP 協助程式

重要：WAN 介面或設定用於 NAT 的介面不支援 IP 協助程式。

許多使用者資料包通訊協定 (UDP) 依靠廣播/多點傳送來尋找各自的伺服器，因此通常需要讓其伺服器位於相同的廣播子網路中。為了在伺服器與用戶端位於不同子網路的情況下提供支援，必須透過某種機制將這些 UDP 廣播/多點傳送轉送到這些子網路。將這種機制稱為「UDP 廣播轉送」。IP 協助程式可幫助廣播/多點傳送封包跨越 SonicWall 安全設備介面，並依據原則轉送到其他介面。IP 協助程式可讓安全設備將源於其介面的 DHCP 請求，轉送到中央 DHCP 伺服器。

IP 協助程式支援使用者定義的通訊協定和擴充原則。IP 協助程式可對現有的 NetBIOS/DHCP 轉接應用提供更好的控制。已擴充的一些內建應用程式包括：

已擴充的內建轉接應用程式

通訊協定	UDP 連接埠編號。
DHCP	67/68
Net-Bios NS	137
Net-Bios 資料包	138
DNS	53
時間服務	37

已擴充的內建轉接應用程式

通訊協定	UDP 連接埠編號。
LAN 喚醒 (WOL)	
mDNS	5353 多點傳送位址：224.0.0.251

IP 協助程式的 VPN 通道介面支援

VPN 通道介面可支援 IP 協助程式。有通道介面支援的 IP 協助程式中的 DHCP 轉接顯示了 IP 協助程式中 DHCP 轉接的一個簡單範例：

- PC 是從 DHCP 通訊協定獲取 IPv4 位址所需的裝置。
- 閘道 A 是已啟用閘道的 IP 協助程式。
- 閘道 B 是帶有 DHCP 伺服器的閘道。

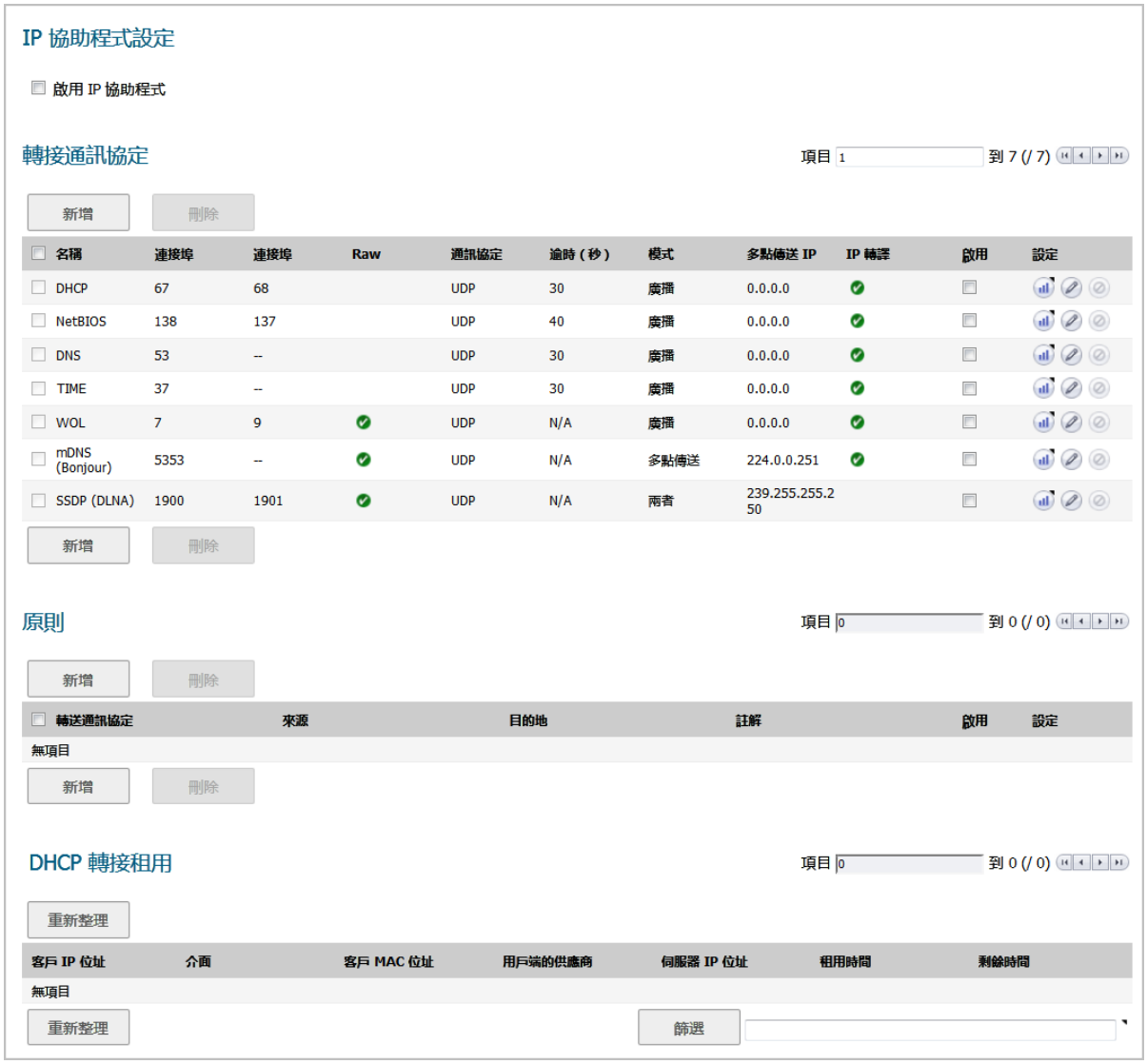
有通道介面支援的 IP 協助程式中的 DHCP 轉接

若要設定具有 VPN 通道介面的 IP 協助程式：

附註：有通道介面支援的 IP 協助程式中的 DHCP 轉接中的數字對應於排序的任務。

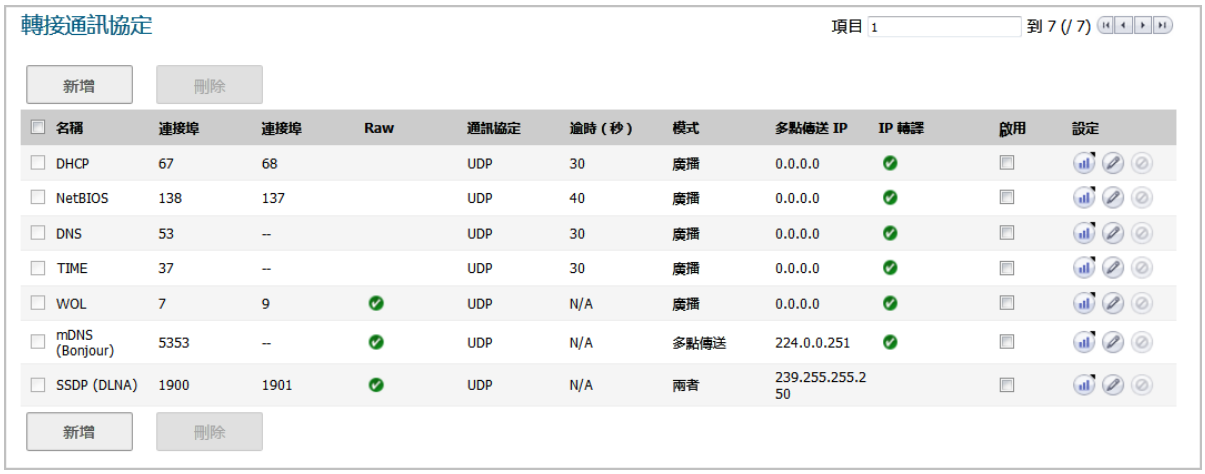
1 在 PC 中：
   a 連接到閘道 A 的 LAN (X0) 子網路。
   b 設定為透過 DHCP 模式獲取 IP 位址。
2 在閘道 A 和閘道 B 間設定一個 VPN 通道。
   - 新增 VPN 通道介面。
3 在閘道 B 中：
   a 新增一個從通道介面的 IP 位址到閘道 A 的 X0 介面的路由項目。
   b 新增通道介面的輸出介面。
   c 新增 IP 位址範圍作為 PC 的 DHCP 範圍。
4 在閘道 A 中：
   a 啟用 IP 協助程式。
   b 新增從 X0 到閘道 B 的通道介面位址的 IP 協助程式 DHCP 轉接通訊協定。此通訊協定為 DHCP。

網路 > IP 協助程式



主題：

轉送通訊協定



名稱 IP 協助應用程式名稱。

連接埠 IP 協助應用程式的第一個 UDP 連接埠編號。

連接埠 IP 協助應用程式的第二個 UDP 連接埠編號 (選用)。

Raw 指出設定 IP 協助應用程式時是否選取了原始模式。啟用了這個選項時，系統會忽略逾時。

通訊協定

逾時 (秒) IP 協助程式快取逾時秒數。**N/A** 代表已選取原始模式，系統會忽略逾時。

模式 指出通訊協定支援的模式:

- **廣播**
- **多點傳送**
- **兩者**

多點傳送 IP 通訊協定使用的多點傳送 IP。

IP 轉譯 指出 IP 協助程式原則轉送封包時，是否轉譯了來源 IP 位址。

啟用 指出是否已啟用 IP 協助程式政策。

設定 包含各項目的**統計**、**編輯**和**刪除**圖示。

附註：只有使用者產生的轉接通訊協定會遭到刪除。

原則

轉送通訊協定	原則使用的通訊協定。
來源	原則使用的介面或區域。
目的地	網路目的地。
註解	介面設定後輸入的註解。
啟用	指出是否已啟用 IP 協助程式政策。
設定	包含各項目的統計、編輯和刪除圖示。

DHCP 轉接租用

用戶端 IP 位址	用戶端裝置的 IP 位址。
介面	安全設備的接收介面。
用戶端 MAC 位址	用戶端裝置的 MAC 位址。
用戶端供應商	來源裝置製造商。
伺服器 IP 位址	DHCP 伺服器的 IP 位址。
租用時間	轉接租用時間。
剩餘時間	轉接租用剩餘時間。

若要重新整理 DHCP 轉接租用表格:

1 按一下**重新整理**。

設定 IP 協助程式

主題：

- 第 464 頁「啟用 IP 協助程式」
- 第 464 頁「管理轉接通訊協定」
- 第 466 頁「管理 IP 協助程式原則」

啟用 IP 協助程式

若要啟用 IP 協助程式功能:

1 導覽到**網路 > IP 協助程式**。

2 在 **IP 協助程式設定**中選取**啟用 IP 協助程式**

管理轉接通訊協定

主題：

查看流量統計資料

您可以在轉接通訊協定表格和原則表格中查看流量統計資料。

若要查看流量統計資料:

1 將滑鼠游標移至通訊協定或原則**統計**圖示上方。彈出式視窗中會顯示該項目的流量統計資料。

轉接通訊協定表格

原則表格

新增使用者定義的轉接通訊協定

若要新增轉接通訊協定:

1 導覽到**網路 > IP 協助程式**。

2 按一下**轉接通訊協定**部分中的**新增**。隨即顯示**新增 IP 協助應用程式**對話方塊。

3 選取**啟用應用程式**來啟用 IP 協助應用程式。

> **附註：**如果停用這個選項，則所有 IP 協助程式快取都會遭到刪除。

4 在**名稱**欄位中，為 IP 協助應用程式輸入一個不重覆的名稱 (區分大小寫)。

5 在**連接埠 1** 欄位中，為應用程式指定一個不重覆的 UDP 連接埠編號。

6 (選用) 在**連接埠 2** 欄位中，為應用程式指定一個不重覆的 UDP 連接埠編號。

7 (選用) 在**逾時**欄位中指定 IP 協助程式快取逾時 (以秒計算，每次增量以 10 秒為單位，範圍從 10 秒到 60 秒)。如果未指定逾時數值，則系統選擇的預設值為 **30** 秒。

> **提示：**如果選擇**原始模式**，忽略此欄位。

8 選擇所需**模式**:

- **廣播**
- **多點傳送**
- **兩者都**

9 如果您在**模式**中選取了**多點傳送**或**兩者**，則請在**多點傳送 IP** 欄位中指定這個通訊協定將使用的有效多點傳送 IP。

10 如需在 IP 協助程式原則轉送封包時允許轉譯來源 IP 位址，請選取**允許來源 IP 轉譯**。 預設情況下已核取此選項。

11 如需在 IP 協助程式原則轉送封包時禁止快取，請選取**原始模式**。支援單向轉送。 預設情況下未勾選此選項。

> **附註：****逾時**欄位中的所有時間設定都會遭到忽略。

12 按一下**確定**。

刪除自訂通訊協定

若要刪除自訂通訊協定:

1 導覽到**網路 > IP 協助程式**。

2 選取該通訊協定的**刪除**圖示。

若要刪除一個或多個自訂轉接通訊協定:

1 導覽到**網路 > IP 協助程式**。

2 找出要刪除的通訊協定，然後選取最左邊的核取方塊 (依通訊協定名稱)。**刪除**按鈕即可供使用。

3 按一下**刪除**。

若要刪除所有自訂轉接通訊協定:

1 導覽到**網路 > IP 協助程式**。

2 選取**轉接通訊協定**表格標題中的核取方塊。**刪除**按鈕即可供使用。

3 按一下**刪除**。

管理 IP 協助程式原則

IP 協助程式原則可用於將 DHCP 和 NetBIOS 廣播從一個介面轉送到另一個介面。

重要：WAN 介面或設定用於 NAT 的介面不支援 IP 協助程式。

主題：

- 第 466 頁「新增 IP 協助程式原則」
- 第 467 頁「編輯 IP 協助程式原則」
- 第 467 頁「刪除 IP 協助程式原則」
- 第 468 頁「透過 TSR 顯示 IP 協助程式快取」

新增 IP 協助程式原則

您最多可新增 128 個原則。

若要新增 IP 協助程式原則:

1 導覽到**網路 > IP 協助程式**。

2 按一下 **IP 協助程式原則**表格中的**新增**。隨即顯示**新增 IP 協助程式原則**對話。

3 預設將啟用原則。如需設定原則但不予啟用，請取消勾選**已啟用**核取方塊。

4 在**通訊協定**功能表中選擇通訊協定。預設值為 **DHCP**。

5 在**從：**中選取來源介面或區域。

6 在**至：**中選取下列其中一個選項:

- 目的地位址群組或位址物件。
- **建立新網路**可讓您建立新位址物件。此時會顯示**新增位址物件**對話方塊。如需更多建立位址物件的相關資訊，請參閱 *SonicOS 原則指南*。

7 在**註解**欄位中輸入任何可選的註解。

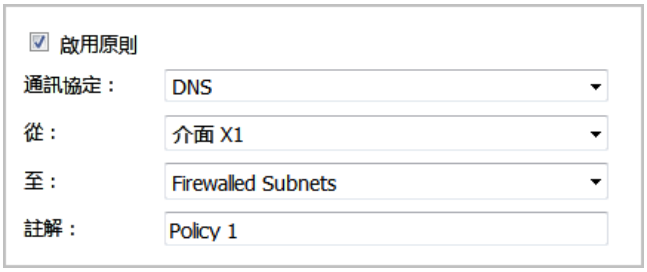
8 按一下**確定**。

編輯 IP 協助程式原則

若要編輯 IP 協助程式原則:

1 導覽到**網路 > IP 協助程式**。

2 在 **IP 協助程式原則**表格中，按一下指定項目的**設定**欄中的**編輯圖示**。隨即顯示**編輯 IP 協助程式原則**對話方塊。



3 其中的設定與**新增 IP 協助程式原則**對話方塊相同。如需該對話方塊的相關資訊，請參閱第 466 頁「新增 IP 協助程式原則」。

刪除 IP 協助程式原則

若要刪除自訂原則:

1 導覽到**網路 > IP 協助程式**。

2 在**原則**表格中，選取該原則的**刪除**圖示。

若要刪除一個或多個自訂原則:

1 導覽到**網路 > IP 協助程式**。

2 找出要刪除的原則，然後選取最左邊的核取方塊 (依轉接通訊協定)。**刪除**按鈕即可供使用。

3 按一下**刪除**。

若要刪除所有自訂原則:

1 導覽到**網路 > IP 協助程式**。

2 選取**原則**表格標題中的核取方塊。**刪除**按鈕即可供使用。

3 按一下**刪除**。

篩選要顯示的 DHCP 轉接租用

您可以使用**篩選**功能，指定要在**反詐騙快取**和**詐騙偵測清單**表格中顯示的裝置。

若要篩選表格顯示內容:

1 導覽到**網路 > MAC-IP 反詐騙**。

2 在要進行篩選的表格下方找到**篩選**欄位，在其中指定裝置的 IP 位址、介面、MAC 位址、主機名稱或名稱。您在填寫這個欄位時，必須使用篩選條件運算子語法選項表格中提供的適用運算子語法。

篩選條件運算子語法選項

運算子	語法選項
包含類型的值	• Ip=1.1.1.1 或 ip=1.1.1.0/24 • Mac=00:01:02:03:04:05 • Iface=x1
String	• X1 • 00:01 • Tst-mc • 1.1.
AND	• Ip=1.1.1.1;iface=x1 • Ip=1.1.1.0/24;iface=x1;just-string
OR	• Ip=1.1.1.1,2.2.2.2,3.3.3.0/24 • Iface=x1,x2,x3
Negative	• !ip=1.1.1.1;!just-string • !iface=x1,x2
Mixed	• Ip=1.1.1.1,2.2.2.2;mac=00:01:02:03:04:05; just-string;!iface=x1,x2

透過 TSR 顯示 IP 協助程式快取

TSR 將顯示所有 IP 協助程式快取、目前原則和通訊協定：

```
#IP_HELPER_START
IP 協助程式
-----IP Helper Global Run-time Data-------
 IP Helper is OFF
 IP Helper - DHCP Relay is OFF
 IP Helper - Netbios Relay is OFF
  Total Number Of Fwded Packets           :0
  Total Number Of Dropped Packets         :0
  Total Number Of Passed Packets          :0
  Total Number Of Unknown Packets         :0
  Total Number Of record create failure   :0
  Total Number Of element create failure  :0User-defined
-----IP Helper Applications -------
 Name: DHCP
  Port: 67, 68, Max Record: 4000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 8000, Timeout: 3, index: 1, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
```

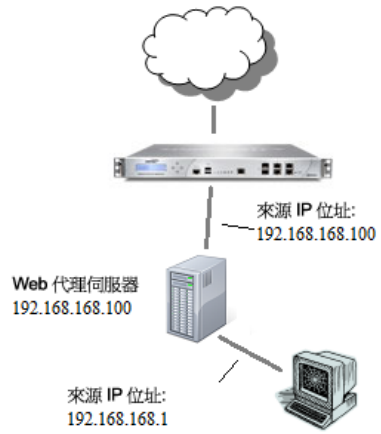
```
 名稱：NetBIOS
  Port: 138, 137, Max Record: 4000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 8000, Timeout: 4, index: 2, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 名稱：DNS
  Port: 53, 0, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 16000, Timeout: 3, index: 3, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 名稱：TIME
  Port: 37, 0, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: NO
  Max Element: 16000, Timeout: 3, index: 4, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 名稱：WOL
  Port: 7, 9, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: YES
  Max Element: 16000, Timeout: 3, index: 5, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
 Name: mDNS
  Port: 5353, 0, Max Record: 8000, Status: OFF
  CanBeDel: NO, ChangeIp: 1, Raw: YES
  Max Element: 16000, Timeout: 3, index: 6, proto: 1,
  Record Count: 0, Element Count: 0,
  Fwded: 0, Dropped: 0, Passed: 0
----------GEN APP Relay Policy-----------
----------------------------------Record Table-----------------------------
Record(hash)[ClientIP, ClientIf, ClientMac, Proto, Vpn, transId, Age(pkts)]
 Elmnt(hash)[serverIp, serverIf, srcIp, dhcpMac, transId, Vpn, proto(fm,to)]
--------------------------------------------------------------------------
----------DHCP Relay Policy-----------
--------NETBIOS Relay Policy-----------#IP_HELPER_END
```

26

設定 Web 代理轉送

網路 | Web 代理

在使用者通過位於內部網路（使用者與 SonicWall 安全設備之間）的代理伺服器存取 Web 時，安全設備所看到的 HTTP/HTTPS 連接源自代理伺服器，而不是使用者。



Web 代理伺服器會攔截 HTTP 請求並確定它是否已儲存所請求的 Web 頁面的副本。如果沒有，代理將完成對網際網路伺服器的請求，將請求到的資訊送回給使用者，並在本機儲存此資訊供未來的請求使用。在網路中設定 Web 代理伺服器可能有些麻煩，因為網路中的每台電腦都必須設定為將 Web 請求定向至此伺服器。

如果您的網路中有一台代理伺服器，則可將該伺服器移至 WAN 或 DMZ 區域，並使用**網路 | Web 代理**頁面中的設定來啟用 Web 代理轉送，而不必設定每台電腦的 Web 瀏覽器來指向該代理伺服器。安全設備自動將所有 Web 代理請求轉送至代理伺服器，而無需設定網路中的所有電腦。

主題：

設定自動代理轉送（僅用於 Web）

附註：若要啟用 Web 代理，請在用戶端來源的相關區域啟用 CFS 功能（在 TZ 系列裝置上使用 WXA 的 Web 快取時，沒有必要啟用 CFS 功能）。

若要設定自動代理轉送（僅用於 Web）：

1 將 Web 代理伺服器連接至集線器。

2 將此集線器連接到防火牆的 WAN 或 DMZ 連接埠。

附註：代理伺服器必須位於 WAN 或 DMZ 區域中；不能位於 LAN 中。

3 移至**網路 > Web 代理**。

4 如需自動將所有 Web 代理要求轉送至代理伺服器，請在**自動代理轉送 (僅用於 Web)** 部分的**代理 Web 伺服器 (名稱或 IP 位址)** 欄位中，輸入代理伺服器的名稱或 IP 位址。長度下限為 0 個字元，上限為 39 個字元。

5 在**代理 Web 伺服器連接埠**欄位中輸入代理 IP 連接埠。預設為 0。

6 如需在 Web 代理伺服器無法使用時讓用戶端直接存取網際網路，請選取**代理伺服器失敗時繞過代理伺服器**。預設已停用此選項。

附註：代理伺服器失敗時繞過代理伺服器核取方塊可使防火牆後面的用戶端在 Web 代理伺服器變為無法使用時繞過它。用戶端的瀏覽器將直接存取網際網路，如同沒有指定 Web 代理伺服器一樣。

7 如需強制公用區域的用戶端也使用代理伺服器，請選取**將公用區域用戶端請求轉送到代理伺服器**。預設已停用此選項。

8 按一下**接受**。

在安全設備更新後，會在瀏覽器視窗的底部顯示一則確認更新的訊息。

設定使用者代理伺服器

您可透過輸入主機名稱或 IP 位址，設定包含多達 32 個使用者代理伺服器。

若要設定使用者代理伺服器：

1 導覽到**網路 | Web 代理**。

2 移至**使用者代理伺服器**部分。

3 按下**新增**。將顯示**新增代理伺服器**顯示對話方塊。

附註：如果使用者的 Web 要求會先通過代理伺服器再到達 SonicWall 安全設備，則安全設備會看到來自代理伺服器的 Web 要求，而不是直接來自使用者的 Web 要求。因此，安全設備無法識別來自來源 IP 位址的使用者。不過一般來說，識別每個 Web 要求來源的代理伺服器，會在 HTTP 標頭中納入這項資訊。

如果這裡設定了任何內部代理伺服器，則安全設備會使用伺服器提供的資訊來識別使用者。

這種方式可用來識別透過內部網路的代理伺服器存取網路的使用者，也適用於透過 WAN 側外部代理伺服器進行的安全設備遠端 HTTP 管理作業。

4 輸入代理伺服器的名稱或 IP 位址。

5 按一下**確定**。

6 重複步驟 3 到步驟 5 以新增更多代理伺服器。

7 按一下**接受**。

8 在設定好介面後，可將其連接到主機。請參閱第 224 頁「設定介面」。

編輯使用者代理伺服器

若要編輯代理伺服器的名稱或 IP 位址：

1 導覽到**網路 | Web 代理**。

2 移至**使用者代理伺服器**部分。

3 在**使用者代理伺服器**表格中，選擇您想要編輯的代理伺服器。

4 按一下**編輯**按鈕。將顯示**編輯代理伺服器**顯示對話方塊。

5 變更代理伺服器的名稱或 IP 位址。

6 按一下**確定**。

刪除使用者代理伺服器

若要移除代理伺服器：

1 導覽到**網路 | Web 代理**。

2 移至**使用者代理伺服器**部分。

3 在**使用者代理伺服器**表格中，選擇您想要移除的代理伺服器。

4 按一下**移除**按鈕。

5 按一下**接受**。

27

設定動態 DNS

網路 | 動態 DNS

主題：

關於動態 DNS

動態 DNS (DDNS) 是由不同公司和機構提供的服務，允許動態變更 IP 位址來自動更新 DNS 記錄，而不用手動干預。利用此服務，即使在目的地的 IP 位址發生變更時，也能透過網域名稱而不是 IP 位址進行網路存取。例如，某個使用者有一條使用 ISP 提供的動態指派 IP 位址的 DSL 連接，使用者可以使用 DDNS 向 DDNS 服務供應商註冊此 IP 位址以及後續的所有位址變更，以便外部主機透過不變的網域名稱來存取它。

動態 DNS 實作因服務供應商而異。針對通訊方法、可註冊的記錄類型或可提供的服務類型，並沒有嚴格的標準。一些供應商既提供進階版本的服務，也提供免費版本的服務。就此而論，要支援特定的 DDNS 供應商，需要能夠與此供應商的指定實作明確的互通性。

大多數供應商強烈建議僅在發生 IP 位址變更時才更新 DDNS 記錄。頻繁的更新，尤其是在註冊的 IP 位址未發生變更時，供應商可能視之為濫用，並可能導致鎖定您的 DDNS 帳戶。請參考在供應商網頁中發佈的使用政策，並遵守相關準則。SonicWall 不針對 DDNS 供應商提供技術支援 - 使用者必須聯絡供應商。

支援的 DDNS 供應商

並非所有供應商提供的所有服務和功能都受到支援，受支援的供應商清單可能會有變更。SonicOS 目前支援動態 DNS 供應商表格中所列出的供應商服務:

動態 DNS 供應商

dns.org	SonicOS 需要使用者名稱、密碼、郵件交換器和備份 MX 來設定來自 `Dyndns.org` 的 DDNS。
changeip.com	僅需用於 SonicOS 設定的使用者名稱、密碼和網域名稱的單一傳統動態 DNS 服務。
no-ip.com	僅需用於 SonicOS 設定的使用者名稱、密碼和網域名稱的動態 DNS 服務。也支援主機名稱分組。
Yi.org	僅需用於 SonicOS 設定的使用者名稱、密碼和網域名稱的動態 DNS 服務。要求在 `yi.org` 管理頁面上建立一條 RR 記錄才能正確地進行動態更新。

由動態 DNS 供應商提供的附加服務

由動態 DNS 供應商提供的一些常見的附加服務包括：

萬用字元	允許對子網路域使用萬用字元參照。舉例來說，如果您註冊了 `yourdomain.dyndns.org` 則可透過 `*.yourdomain.dyndyn.org` (例如 `server.yourdomain.dyndyn.org`、`www.yourdomain.dyndyn.org`、`ftp.yourdomain.dyndyn.org` 等) 來存取您的站台。
郵件交換器	為您的網域建立 MX 記錄項目，以便 SMTP 伺服器透過 DNS 找到它並傳送郵件。 **附註：**ISP 經常封鎖連入 SMTP；您在嘗試託管郵件伺服器之前，請諮詢您的供應商。
備份 MX (由 `dns.org`、`yi.org` 提供)	允許指定在主 IP 位址停用時用於 MX 記錄的備用 IP 位址。
群組	允許對主機分組，以便在群組級別一次應用更新，而不必針對各個成員多次應用更新。
離線 IP 位址	允許指定在註冊的主 IP 離線時用於註冊主機名稱的備用位址。

如需設定 DDNS 設定檔的資訊，請參見第 477 頁「設定動態 DNS 設定檔」。

動態 DNS 設定檔表格

動態 DNS 設定檔表格會針對已設定的 DDNS 設定檔提供相關資訊。

檢視 IP 版本 可讓您切換 IPv4 和 IPv6 DDNS 設定檔表格。

設定檔名稱 在建立期間指派給 DDNS 項目的名稱。它可能是任意值，且僅用於識別。

網域 DDNS 項目的完整網域名稱 (FQDN)。

供應商 向其註冊項目的 DDNS 供應商。

狀態 DDNS 項目最近報告的狀態/目前狀態。

- **線上** 以管理方式將 DDNS 項目設為線上。此項目的目前 IP 設定將與時間戳記一同顯示。
- **在本機設定為離線模式** 以管理方式將 DDNS 項目設為離線。如果項目狀態為**已啟用**，則將執行在**新增 DDNS 設定檔進階**頁面中的**離線設定**部分所設定的操作。
- **濫用** DDNS 供應商將更新類型或頻率視為濫用。請核對 DDNS 供應商準則，以確定將哪些做法視為濫用。
- **無 IP 變更** 可能濫用。在無 IP 位址變更時進行的強制更新，可能會遭到某些 DDNS 供應商認定為濫用行為。自動更新只會在位址或狀態變更時進行。也只有絕對必要時 (例如註冊資訊有誤)，才必須採取手動或強制更新。
- **已停用** 由於設定錯誤或違反原則，已停用帳戶。請查看設定檔中的設定，並向供應商確認 DDNS 帳戶狀態。
- **無效的帳戶** 提供的帳戶資訊無效。請查看設定檔中的設定，並向供應商確認 DDNS 帳戶狀態。
- **網路錯誤** 由於可疑的網路錯誤，無法與 DDNS 供應商通訊。請確認可存取供應商且供應商處於線上狀態。稍後重試此操作。
- **供應商錯誤** DDNS 供應商此時無法執行所請求的操作。請查看設定檔中的設定，並向供應商確認 DDNS 帳戶狀態。稍後重試此操作。
- **非捐贈者帳戶** 指定供應商提供的某些功能（例如離線位址設定）僅供付費或捐贈訂閱者使用。如需可能需要付費或捐贈的服務的更多詳情，請諮詢供應商。

啟用 選取這個選項時，這個設定檔會以系統管理方式啟用，且安全設備將執行**新增 DDNS 設定檔**的**進階**頁面中所設定的**線上設定**操作。您也可以透過該項目的**新增 DDNS 設定檔**中的**啟用此動態 DDNS 設定檔**選項來控制這項設定。取消選取這個選項即會停用目標設定檔，而且在您重新啟用該設定檔前，該設定檔將不會與 DDNS 供應商進行任何通訊。

線上 勾選時，將以管理方式將此設定檔設為線上。您也可以透過該項目的**新增 DDNS 設定檔**中的**使用線上設定**選項來控制這項設定。在已啟用設定檔的情況下取消選取這個選項，會使設定檔進入離線狀態，且安全設備將執行**進階**頁面中所設定的**離線設定**操作。

設定 包含用於設定 DDNS 設定檔設定的**編輯**圖示，以及用於刪除 DDNS 設定檔項目的**刪除**圖示。

設定動態 DNS 設定檔

如需設定 DDNS 設定檔的一般資訊，請參見第 474 頁「關於動態 DNS」。

使用任何動態 DNS 服務都必須從使用您所選擇的一個或多個 DDNS 服務供應商來設定帳戶開始。可以同時使用多個供應商。請參考動態 DNS 供應商表格中列出的多位供應商。註冊過程通常涉及來自供應商的確認電子郵件，以及透過存取嵌在確認電子郵件中的唯一 URL 進行最終確認。在登入到所選供應商的頁面後，您應該存取管理連結（通常為「新增」或「管理」），並建立自己的主機項目。嘗試在 SonicOS 中使用動態 DNS 用戶端之前，必須執行此操作。**網路 | 動態 DNS**頁面所提供的設定，可供您設定 SonicWall 安全設備來使用您的 DDNS 服務。

若要在 SonicWall 安全設備上設定動態 DNS:

1 導覽到**網路 | 動態 DNS**。

2 按一下**新增**按鈕。隨即顯示**新增 DDNS 設定檔**對話方塊。

3 如果勾選了**啟用此 DDNS 設定檔**，設定檔會以系統管理方式啟用，且安全設備將執行**進階**頁面的**線上設定**部分中所定義的操作。預設情況下已核取此選項。

4 如果勾選**使用線上設定**，則以管理方式將此設定檔設為線上狀態。預設情況下已核取此選項。

5 在**設定檔名稱**欄位中輸入指定給 DDNS 項目的名稱。它可以是任意值，用於在**動態 DNS 設定**表中識別此項目。最小長度為 1 個字元，最大長度為 63 個字元。

6 在**供應商**中選取動態 DNS 供應商；動態 DNS 供應商表格中提供了這些供應商的相關說明。預設值為 **dyn.com**。

重要：您必須已透過自己選擇的 DNS 供應商建立動態服務記錄。

提示：僅有部分 DNS 供應商可提供所有選項。此外，頁面底部的**附註**會顯示 DNS 供應商是否使用 HTTP 或 HTTPS 通訊協定，以及該供應商的網站連結。

7 在**使用者名稱**欄位中，輸入 DNS 供應商帳戶的使用者名稱。最小長度為 1 個字元，最大長度為 63 個字元。

8 在**密碼**欄位中，輸入您的 DNS 密碼。最小長度為 1 個字元，最大長度為 31 個字元。

9 在**網域名稱**欄位中，輸入您向 DNS 供應商註冊的主機名稱的完整網域名稱 (FQDN)。確保提供與設定內容相同的主機名稱和網域。最小長度為 1 個字元，最大長度為 63 個字元。

10 您也可以視需求將這個 DDNS 設定檔指派給特定的 WAN 介面，方法是在**繫結到**中選取 WAN 介面。如果您正在設定多 WAN 負載平衡，則這個選項可讓您將可預測的 IP 位址發佈到 DDNS 服務。預設情況下，它將設為**任何**，這意味著此設定檔可自由使用安全設備上的任意 WAN 介面。

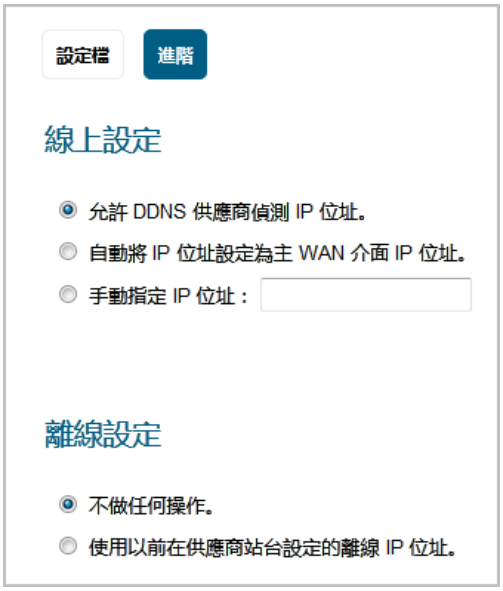
11 如果您選取的**供應商**為 **dyn.com**，請移至步驟 13。

12 使用 `dyn.org` 時，請在**服務類型**中選取您的服務類型所對應的服務類型。

動態	免費的動態 DNS 服務。這是預設值。
自訂	託管型基本 DNS 解決方案，提供一項統一的主要/次要 DNS 服務和一個基於 Web 的介面。支援動態和固定 IP 位址。
靜態	用於靜態 IP 位址的免費 DNS 服務。

13 按一下**進階**。

提示：通常可以保留此頁面中的預設值。



14 **線上設定**部分對在動態 DNS 供應商處註冊的 IP 位址提供控制。選擇：

允許 DDNS 供應商偵測 IP 位址	安全設備可讓 DNS 供應商指定 IP 位址 **附註：**僅 IPv4。預設情況下已核取此選項。

自動將 IP 位址設為主要 WAN 介面 IP 位址	會導致安全設備將其 WAN IP 位址宣告為註冊的 IP 位址，覆寫動態 DNS 伺服器的自動偵測結果。適用於不能正常偵測的情況。預設情況下已核取此選項。 **附註：**在 IPv6 中: 預設情況下已核取此選項。
手動指定 IP 位址	允許手動指定和宣告要註冊的 IP 位址。

15 **離線設定**部分在安全設備中的動態 DNS 項目已在本機離線的情況下，提供對在動態 DNS 供應商處註冊的 IP 位址的控制。選擇：

不做任何操作	允許先前註冊的位址繼續使用現有的動態 DNS 供應商。預設情況下已核取此選項。
使用先前在供應商站台設定的離線 IP 位址	您的供應商支援手動指定離線設定時即可選擇此選項，在此設定檔透過系統管理方式設為離線時使用離線設定。

16 按一下**確定**。

編輯 DDNS 設定檔

若要編輯 DDNS 設定檔:

1 導覽到**網路 | 動態 DNS**。

2 在動態 DNS 設定檔表格中，按一下所需設定檔的**編輯**圖示。隨即顯示編輯 DDNS 設定檔對話方塊。

3 進行變更；選項說明部分請按照第 477 頁「設定動態 DNS 設定檔」的指示操作。

4 按一下**確定**。

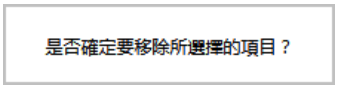
刪除 DDNS 設定檔

您可刪除一個或所有 DDNS 設定檔。

若要刪除 DDNS 設定檔。

1 導覽到**網路 | 動態 DNS**。

2 找出要刪除的設定檔，然後按一下**刪除**圖示。將顯示確認訊息：

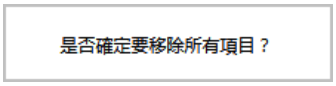


3 按一下**確定**。

若要刪除所有 DDNS 項目:

1 導覽到**網路 | 動態 DNS**。

2 按一下**全部刪除**。將顯示確認訊息：



3 按一下**確定**。

部分 5

交換

附註：本部分介紹了 SonicOS 的進階交換，它不同於從 TZ 裝置管理 Dell X 系列交換器。如需管理 X 系列交換器的更多資訊，請參見第 297 頁「SonicOS 支援 X- 系列交換器」。

- 關於交換
- 設定 VLAN 轉接
- 查看第 2 層發現
- 設定連結彙總
- 設定連接埠鏡像

28

關於交換

附註：在 NSA 2600、TZ 系列和 SOHO W 安全設備以外的所有產品中提供了交換功能。

附註：本節說明 SonicOS 的進階交換，它不同於從 SonicWall 安全設備管理 Dell X- 系列交換器。如需關於管理 X- 系列交換器的詳細資訊，請參閱第 297 頁「SonicOS 支援 X- 系列交換器」。

關於交換

主題：

什麼是交換？

SonicOS 提供第 2 層（資料連結層）交換功能。此功能支援以下交換功能：

- **VLAN 轉接** - 能夠在多台交換器之間轉接不同的 VLAN。
- **第 2 層網路發現** - 使用 IEEE 802.1AB (LLDP) 和 Microsoft LLTD 通訊協定以及交換轉送表發現連接埠可見的裝置。
- **連結彙總** - 能夠彙總連接埠以提高效能和冗餘。

  附註：在 NSA 3600 與更高版本的防火牆上支援連結彙總。在 NSA 2600 上，網路介面連結彙總是獨立於交換連結彙總的功能。NSA 2600 支援網路介面的連結彙總（參見第 495 頁「設定連結彙總」），但 NSA 2600 不支援交換，因此它不支援交換的連結彙總。

- **連接埠鏡像** - 用於指派一個鏡像連接埠以鏡像一組連接埠的輸入、輸出雙向封包。

- **Jumbo 框架** - 支援 Jumbo 框架使 SonicOS 能夠處理承載在 1500-9000 位元組之間的乙太網路框架。

  附註：NSA 3600 及更新裝置支援 Jumbo 框架。

交換的優點

SonicOS 提供安全與交換相結合的解決方案。第 2 層交換功能增強了 SonicWall 裝置在現有第 2 層網路中的部署和互操作能力。

附註：NSA 3600 及更新裝置支援進階交換。

網路安全設備的先進交換功能有以下優點：

- **高連接埠密度** - 一台裝置提供多達 26 個介面，其中包含 24 個交換連接埠，內部網路上的裝置數量因此得以減少。
- **跨多個交換連接埠的高安全性** - PortShield 結構支援將所有 LAN 交換連接埠靈活地設定為獨立的安全區域，如 LAN、WLAN 和 DMZ，從而防護其不受 WAN 和 DMZ 的影響，而且 LAN 內部的裝置之間也不互相影響。這樣，各安全區域都有自己的線速「微型交換器」，專用深度封包檢查防火牆為其提供防護。
- **VLAN 轉接** - 無需在每台交換器上設定 VLAN 資訊，簡化 VLAN 管理和設定；能夠在多台交換器之間轉接不同的 VLAN。
- **第 2 層網路發現** - 為連接到本裝置的所有裝置提供第 2 層網路資訊；使用 IEEE 802.1AB (LLDP) 和 Microsoft LLTD 通訊協定以及交換轉送表發現連接埠可見的裝置。
- **連結彙總** - 連接到支援彙總的交換器時，彙總連接埠可通過負載平衡提供更高的效能；連接到支援彙總的交換器或伺服器時，彙總連接埠可提供冗餘。
- **連接埠鏡像** - 用於輕鬆監視和檢查一個或多個連接埠上的網路流量，指派一個鏡像連接埠以鏡像一組連接埠的輸入、輸出或雙向封包。
- **Jumbo 框架** - 使 SonicOS 能夠處理承載在 1500-9000 位元組之間的乙太網路框架，允許提高傳送量和減少待處理的乙太網路框架數。在有些情況下，可能不會提高傳送量。但是，如果穿越的封包巨大，傳送量會有所改進。

  附註：NSA 3600 及更新裝置支援 Jumbo 框架。

交換的工作原理

某些交換功能是在 PortShield 群組上操作，需要在**網路 > PortShield 群組**頁面上進行初步設定。某些則是在現有的**網路 > 介面**設定上操作。如需關於在 SonicOS 中設定這些相關功能的詳細資訊，請參閱:

- 第 224 頁「設定介面」
- 第 296 頁「設定 PortShield 介面」

如需各交換功能操作的詳細資料，請參閱:

- 第 485 頁「設定 VLAN 轉接」
- 第 492 頁「查看第 2 層發現」
- 第 495 頁「設定連結彙總」
- 第 500 頁「設定連接埠鏡像」

術語

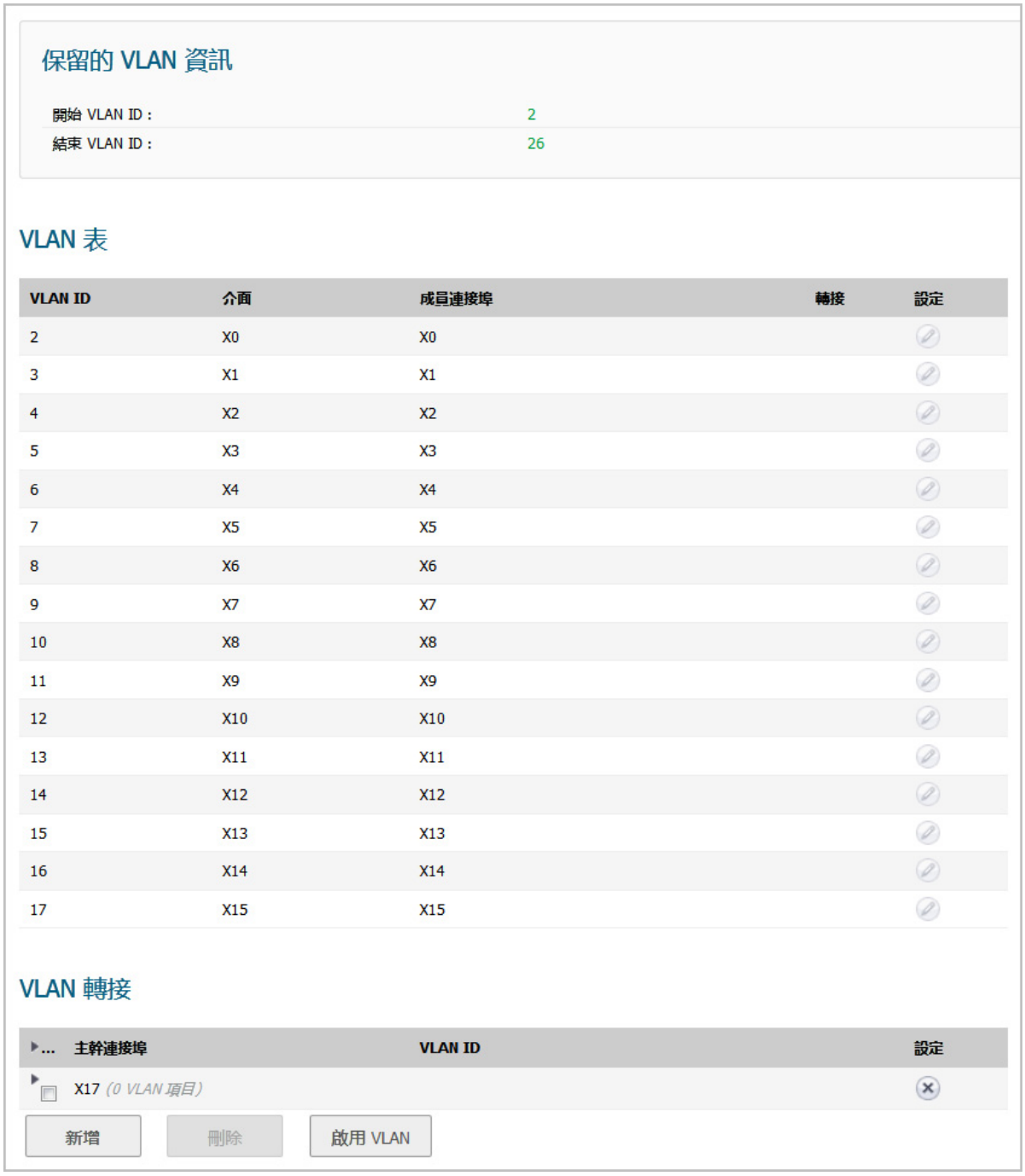
BPDU	橋接通訊協定資料單元 - 用於 RSTP，BPDU 是特殊資料框架，用於交換有關橋接器 ID 和根路徑成本的資訊。BPDU 每隔幾秒交換一次，以便交換器能夠追蹤網路拓撲，並啟動或停止連接埠轉送。
CoS	服務類別 - CoS (IEEE 802.1p) 定義了 8 種不同的服務類別，用 IEEE 802.1Q 報頭中的 3 位 user_priority 欄位表示；在 802.1 網路上使用標記框架時，此報頭新增到乙太網路框架。
DSCP	區分服務代碼點 - 也稱為 DiffServ，DSCP 是一種網路結構，定義了一個簡單、粗粒度、基於類別的機制來分類和管理網路流量，並在 IP 網路上提供服務品質 (QoS) 保證。DSCP 由 IETF 於 1998 年發佈的 RFC 2475 定義。DSCP 通過標記 IP 包頭中的 8 位欄位來工作。
IETF	Internet 工程任務組 - IETF 是一個負責開發和促進 Internet 標準的開放標準組織。
L2	OSI 第 2 層（乙太網路）- 七層 OSI 模型的第 2 層是資料連結層，乙太網路通訊協定在此層上執行。第 2 層用於在網路實體之間傳送資料。
LACP	連結彙總控制通訊協定 - LACP 是一個 IEEE 規範，提供一種將多個實體連接埠合併以形成單個邏輯頻道的方法。LACP 支援相連裝置進行負載平衡。
LLDP	連結層發現通訊協定 (IEEE 802.1AB) - LLDP 是一個第 2 層通訊協定，網路裝置利用它來表達其身分、功能和互連。此資訊儲存在各主機的 MIB 資料庫中，可利用 SNMP 查詢以確定網路拓撲。此資訊包括：系統名稱、連接埠名稱、VLAN 名稱、IP 位址、系統功能（交換、路由）、MAC 位址、連結彙總等等。
LLTD	連結層拓撲發現（微軟標準）- LLTD 是微軟公司專有通訊協定，功能與 LLDP 相似。它在有線或無線網路（乙太網路 802.3 或無線 802.11）上工作。Windows Vista 和 Windows 7 內建 LLTD，Windows XP 上可以安裝此協定。
PDU	通訊協定資料單元 - 對於交換功能而言，第 2 層 PDU 是框架。它包含連結層標頭和封包。
RSTP	快速產生樹狀目錄通訊協定 (IEEE 802.1D-2004) - RSTP 制定於 1998 年，是「產生樹狀目錄通訊協定」的改進版本。拓撲改變後，它能更快地實現產生樹狀目錄融合。

29

設定 VLAN 轉接

附註：在 NSA 2600、TZ 系列和 SOHO W 裝置以外的所有產品中提供了交換功能。

交換 | VLAN 主幹連線



主題：

- 關於轉接
- 第 487 頁「檢視 VLAN」
- 第 489 頁「編輯 VLAN」
- 第 489 頁「新增 VLAN 主幹連接埠」

- 第 490 頁「刪除 VLAN 主幹連接埠」
- 第 490 頁「啟用主幹連接埠上的 VLAN」

關於轉接

SonicOS 上的未指派交換連接埠可用作 VLAN 轉接連接埠。您可以啟用或停用主幹連接埠上的 VLAN，將 SonicOS 上的現有 VLAN 橋接到另一台通過主幹連接埠連接的交換器上的相應 VLAN。SonicOS 的主幹連接埠支援 802.1Q 封裝。各主幹連接埠上最多可啟用 32 個 VLAN。

VLAN 轉接功能提供以下功能：

- 變更現有 PortShield 群組的 VLAN ID
- 新增/刪除 VLAN 轉接連接埠
- 啟用/停用主幹連接埠上的客戶 VLAN ID

允許的 VLAN ID 範圍是 1-4094。某些 VLAN ID 會保留供 PortShield 使用，而保留範圍顯示在**管理 | 系統安裝 | 交換 | VLAN 主幹連線**上。

可以將某些 PortShield 群組標記為「已轉接」。一旦解散 PortShield 群組，轉接連接埠上關聯的 VLAN 會自動停用。

VLAN 既可以 PortShield 群組的形式存在於本機，也可是完完全全的遠端 VLAN。可以變更 SonicOS 上的 PortShield 群組的 VLAN ID。這樣便可與現有 VLAN 編號輕鬆整合。

SonicOS 不允許臨時變更連接埠的 VLAN 成員資格。連接埠的 VLAN 成員資格必須通過 SonicOS 管理介面中的 PortShield 設定進行變更。如需設定 PortShield 群組的更多資訊，請參見第 296 頁「設定 PortShield 介面」。

針對遠端 VLAN 會自動建立虛擬介面（稱為 VLAN 轉接介面）。另一主幹連接埠上啟用同樣的遠端 VLAN 時，不會建立新的介面。所有帶相同 VLAN 標記的封包進入不同的主幹連接埠時，都由同一虛擬介面處理。這是 VLAN 子介面與 VLAN 轉接介面的主要區別。

管理 | 系統安裝 | 網路 | 介面上的**名稱**欄位顯示 VLAN 主幹之「VLAN 主幹介面」的 VLAN ID。

可以啟用 VLAN 轉接上的任何 VLAN，無論本機還是遠端，以便橋接到另一交換器上的兩個相應 VLAN。例如，可以在連接埠 X2 的 VLAN 轉接上啟用本機 VLAN 345，此連接埠上還啟用了兩個遠端 VLAN。

VLAN 轉接與連結彙總和連接埠鏡像功能互操作。可以鏡像 VLAN 轉接連接埠，但不能將之用作鏡像連接埠本身。

設定為 VLAN 轉接的連接埠不能用於任何其他功能，只能保留供第 2 層使用。例如，無法為主幹連接埠設定 IP 位址。

在指定主幹連接埠上設定轉接 VLAN 介面後，若要刪除此主幹連接埠，必須移除此 VLAN 介面，即便此 VLAN 已在多個主幹連接埠上啟用。這是一個功能實現上的局限，將在未來版本中予以解決。

檢視 VLAN

主題：

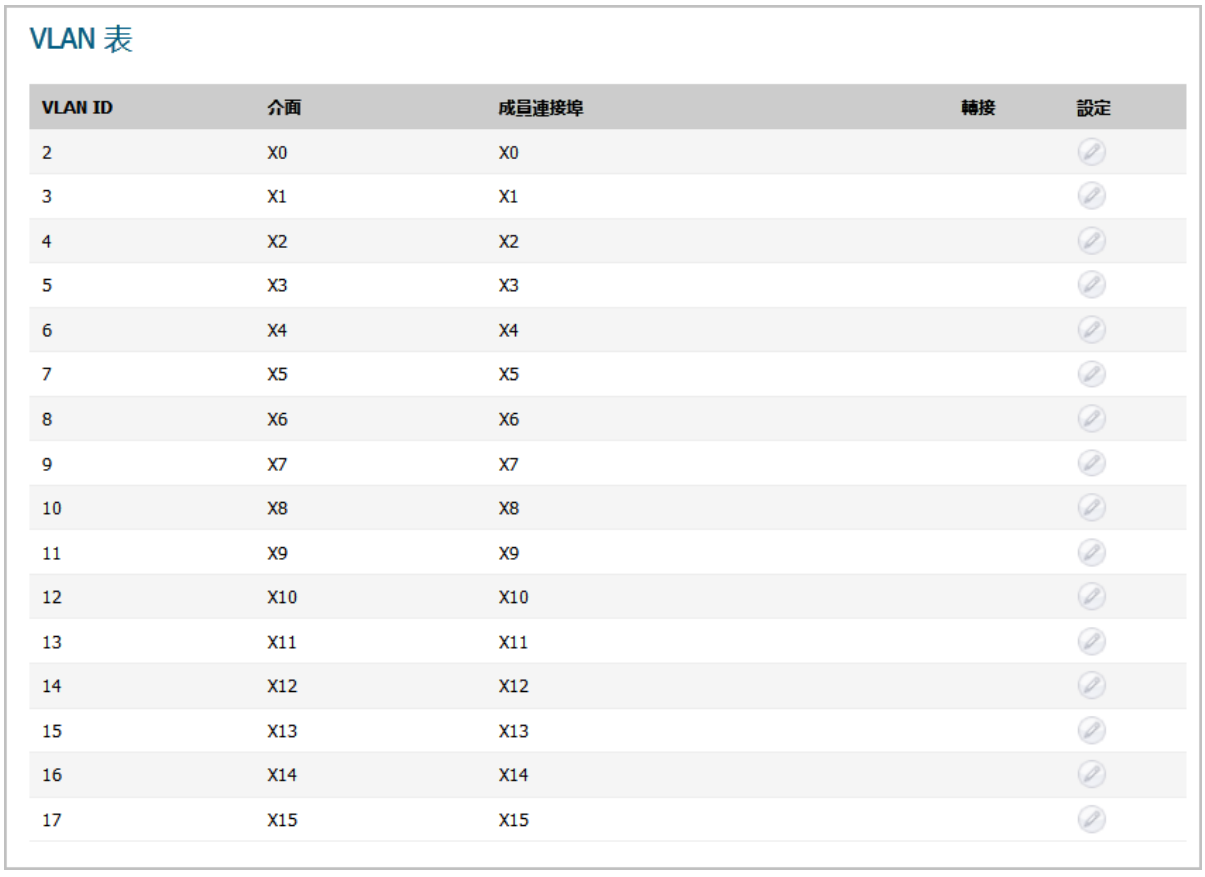
- 第 488 頁「保留的 VLAN 資訊」
- 第 488 頁「VLAN 表」
- 第 489 頁「VLAN 轉接表」

保留的 VLAN 資訊

保留的 VLAN 資訊表列出保留的 VLAN ID 的範圍：

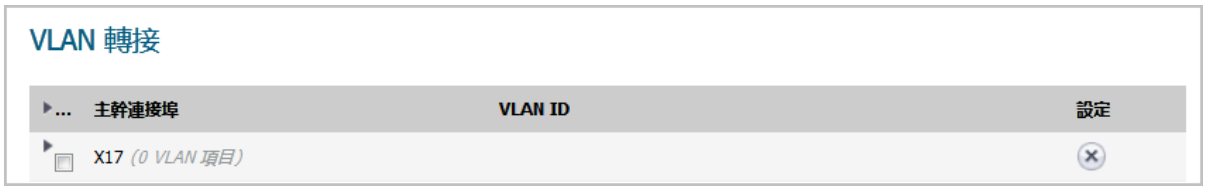
- **開始 VLAN ID**
- **結束 VLAN ID**

VLAN 表



VLAN ID	VLAN 的 ID。
介面	指派至 VLAN 的介面。
成員連接埠	與介面關聯的連接埠。
轉接	指出此 VLAN 是否已轉接。
設定	包含 VLAN 的**編輯**圖示。

VLAN 轉接表



主幹連接埠	主幹連接埠的介面以及與其關聯的 VLAN 項目數量
VLAN ID	VLAN 的 ID
設定	包含 VLAN 的**刪除**圖示

若要顯示主幹連接埠的 VLAN ID，請按一下主幹連接埠的**展開**圖示。若要顯示主幹連接埠的 VLAN ID，請按一下 **VLAN 主幹**表格標題中的**展開**圖示。若要隱藏 VLAN ID，請按一下相應的**收合**圖示。

編輯 VLAN

若要編輯 VLAN：

1 導覽到**交換 | VLAN 主幹連線**。

2 在 **VLAN 表格**中，針對您要編輯的 VLAN ID，按一下**設定**圖示。隨即顯示**編輯 PortShield 主機的 VLAN** 對話。

3 執行以下任一動作：

- 將其他 VLAN ID 輸入 **VLAN ID** 欄位中。除了系統指定的原始 VLAN ID 或**保留的 VLAN 資訊**表中的任何其他 VLAN ID 之外，您可以輸入任意 VLAN ID。
- 使用 **VLAN ID** 欄位中的 VLAN ID 號碼，其與您按下**設定**圖示的 VLAN ID 相符者。

4 若要啟用對此 VLAN 的轉接，請勾選**轉接**核取方塊。要停用對此 VLAN 的轉接，請取消勾選此核取方塊。

5 按一下**確定**。

新增 VLAN 主幹連接埠

若要新增 VLAN 主幹連接埠：

1 導覽到**交換 | VLAN 主幹連線**。

2 在 **VLAN 主幹**下，按一下**新增**。隨即顯示**新增 VLAN 主幹連接埠**對話方塊。

3 從**主幹連接埠**下拉功能表中選擇要新增的連接埠。

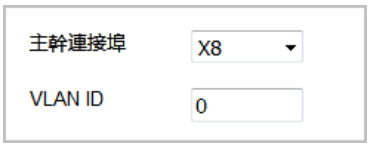
4 按一下**確定**。

啟用主幹連接埠上的 VLAN

啟用特定主幹連接埠上的自訂 VLAN ID 的步驟如下：

1 導覽到**交換 | VLAN 主幹連線**。

2 在 **VLAN 主幹**表格下方，按一下**啟用 VLAN**。顯示**啟用 VLAN** 對話。



3 從**主幹連接埠**下拉功能表中選擇一個主幹連接埠。這是您希望用來轉接 **VLAN ID** 欄位中所示 VLAN ID 的連接埠。

4 在 **VLAN ID** 欄位中，輸入要轉接的 VLAN ID。它可以是另一交換器上的 VLAN ID。

5 按一下**確定**。

刪除 VLAN 主幹連接埠

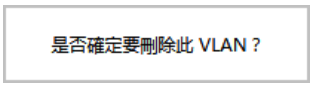
您可以一次刪除一個 VLAN 主幹連接埠、多個連接埠或者所有連接埠。

若要刪除一個 VLAN 主幹連接埠：

1 導覽到**交換 | VLAN 主幹連線**。

2 展開要刪除的 VLAN 主幹。

3 針對要刪除的 VLAN，按一下**設定**欄中的**刪除**圖示。將顯示確認訊息：



4 按一下**確定**。

5 針對要刪除的連接埠，按一下**設定**欄位中的**刪除**圖示。將顯示確認訊息：

6 按一下**確定**。

若要刪除多個 VLAN 主幹連接埠：

1 導覽到**交換 | VLAN 主幹連線**。

2 在 **VLAN 主幹**表格中，展開要刪除的 VLAN 主幹連接埠。

3 針對每個要刪除的 VLAN，按一下**設定**中的**刪除**圖示。將顯示確認訊息：

4 對每則訊息按下**確定**。

5 勾選您要刪除之 VLAN 主幹連接埠的核取方塊。**刪除**按鈕即可供使用。

6 按一下**刪除**。將顯示確認訊息。

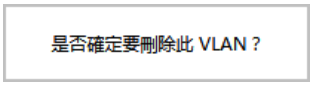
7 按一下**確定**。

若要刪除全部 VLAN 主幹連接埠：

1 導覽到**交換 | VLAN 主幹連線**。

2 在 **VLAN 主幹**表格中，按一下 **VLAN 主幹**表格標題中的**展開**圖示，以展開 VLAN 主幹連接埠。

3 針對每個要刪除的 VLAN，按一下**設定**中的**刪除**圖示。將顯示確認訊息：



4 勾選 **VLAN 主幹**表格標題中的核取方塊。**刪除**按鈕即可供使用。

5 按一下**刪除**。將顯示確認訊息。

6 按一下**確定**。

30

查看第 2 層發現

附註：NSA 2600、TZ 系列和 SOHO W 設備除外的所有防火牆上均有交換功能。

交換 | L2 發現

SonicWall 安全設備使用 IEEE 802.1AB (LLDP)/Microsoft LLTD 通訊協定和交換轉送表來探索連接埠可見的節點。這些是第 2 層協定，不跨越廣播網域。這些通訊協定的更多資訊可由此取得：

- https://en.wikipedia.org/wiki/Link_Layer_Topology_Discovery
- https://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

主題：

- 檢視 L2 發現
- 啟用 L2 發現

檢視 L2 發現

預設 **L2 發現**表僅顯示介面、透過連接不可見的節點數以及介面的**重新整理**圖示。

若要顯示 L2 發現資訊，請按下所要介面的**展開**圖示。就會顯示為介面發現的節點相關資訊。

- MAC 位址
- 供應商名稱
- IP 位址或 N/A (如果適用)
- 系統名稱（如果適用）
- 描述（如果適用）

啟用 L2 發現

系統啟動時，「探索」會處於作用中狀態，除非您重新整理 **L2 探索**表格，否則不會重新啟動。

若要在某個介面上重新啟動第 2 層探索:

1 導覽到**交換 | L2 發現**。

2 按一下指定介面的**重新整理**圖示。

若要在多個介面上重新啟動第 2 層探索:

1 導覽到**交換 | L2 發現**。

2 選取所需介面。**重新整理選定項目**按鈕即變成可用狀態。

3 按一下**重新整理選定項目**。

若要在所有介面上重新啟動第 2 層探索:

1 導覽到**交換 | L2 發現**。

2 勾選表格標題中的核取方塊。**重新整理選定項目**按鈕即變成可用狀態。

3 按一下**重新整理選定項目**。

31

設定連結彙總

附註：所有 NSA 3600 及以上版本和 SuperMassive 設備上均可切換。

交換 | 連結彙總

主題：

關於連結彙總

附註：NSA 3600 及更新防火牆支援連結彙總(LAG)。

連結彙總藉由允許您將 SonicWall 安全設備與其之間的兩個或多個連結互連，利用此方式將多個連結結合成一個可承載較高組合頻寬的大型虛擬管道，因此支援第 2 層網路中的連接埠冗餘和負載平衡。由於兩個裝置之間存在多個連結，如果一個連結故障，則可透過其他連結傳輸流量而不中斷。透過顯示的多個連結，流量也可以利用此方式負載平衡，以達成平均分配。負載平衡是由 SonicWall 安全設備根據來

源和目的地 MAC 位址配對進行控制。**交換 | 連結彙總**頁面提供有關和允許設定用於彙總介面的資訊和統計資料。

SonicOS 支援兩種類型的 LAG:

- 第 496 頁「靜態 LAG」
- 第 496 頁「動態 LAG」

靜態 LAG

在「靜態連結彙總」中，位於相同 VLAN (相同 PortShield 群組) 中的連接埠，或有資格進行連結彙總的 VLAN 主幹連接埠。一個邏輯群組最多可彙總四個連接埠，可以設定四個邏輯電路 (LAG)。透過靜態連結彙總，所有組態設定皆在參與的兩個 LAG 元件上設定。

此功能支援兩類主要用法：

防火牆到伺服器	實作方法是藉由在相同 VLAN (相同 PortShield 群組) 中的連接埠上啟用「連結彙總」。這種設定可提供連接埠冗餘，但由於裝置的硬體限制，不支援安全設備到伺服器方向的負載平衡。
防火牆到交換器	透過在 VLAN 主幹連接埠上啟用連結彙總來支援。裝載平衡是由硬體自動執行。安全設備支援以來源和目的地 MAC 位址配對為基礎的單一裝載平衡。

與 PortShield 設定相似，選擇一個介面代表彙總群組。此連接埠稱為*彙總器*。必須為彙總器連接埠指派一個唯一的金鑰。非彙總器連接埠可以選擇性地設定金鑰；如果交換器接線錯誤，金鑰可防止出現錯誤的 LAG。

附註：金鑰與 LAG ID 不同，其與介面號碼相同，而且無法變更。設定 LAG 群組時，必須指派金鑰。所有非彙總器連接埠必須具有與彙總器連接埠相同的金鑰。

連接埠連接到同一連結夥伴且其金鑰一致時，就會繫結在一起。固定連結彙總無法發現連結夥伴。這種情況下，連接埠僅依據金鑰而彙總。

像 PortShield 主機一樣，不能從 LAG 中移除彙總器連接埠，因為它代表著系統中的 LAG。

附註：一旦 VLAN 轉接連接埠啟用連結彙總，便無法再新增或刪除 LAG 上的 VLAN。

動態 LAG

SonicOS 支援在所有支援「進階交換」功能的所有 SonicWall 安全設備上，使用連結彙總控制通訊協定 (由 IEEE 802.3ad 定義的 LACP) 的動態連結彙總。

關於使用 LACP 的動態 LAG

LACP 允許交換通訊協定封包 (稱為「連結彙總控制通訊協定資料單元 (PDU)」中 LAG 群組之成員之間的連結彙總相關資訊。有了 LACP，即可快速偵測到設定、佈線中的錯誤，以及連結故障。

使用 LACP 可以有效地實現 LAG 的兩個主要優點，例如提高輸送量和連結冗餘。LACP 是 LAG 中成員之間使用的訊號通訊協定。它確保連結只有在正確設定和連接的情況下才能彙總成一個組合。LACP 可在兩種模式之一進行設定:

- **主動模式** - 當連接埠啟動時，裝置會立即傳送 LACP PDU。

  附註：SonicOS 6.5 僅支援 LACP 的「主動」模式。

- **被動模式** - 連接埠處於被動交涉狀態，其中連接埠只回應收到的 LACP PDU，但不會發起 LACP 交涉。

如果兩端皆設為主動，則可以在假設成功交涉其他參數的情況下形成 LAG 。如果一端設為主動，而另一端設為被動，則可以在被動連接埠回應從主動端接收的 LACP PDU 時形成 LAG。如果兩端皆為被動，則 LACP 無法交涉組合。部署中很少使用被動模式。

在設定中，相同 LAG 的所有成員連接埠必須在與彙總器連接埠相同的 VLAN 上設定。LAG 成員上收到的資料封包與使用 VLAN 的父級彙總器相關聯。當 LAG 的彙總器/成員連接埠狀態達到穩定的「收集/ 發佈」狀態時，連接埠已準備好傳輸和接收資料流量。

所有與 LAG 相關的資訊 (例如設定的彙總器連接埠)，此資訊會顯示在**交換 | 連結彙總**頁面:

- 屬於 LAG 一部分的成員連接埠。
- 形成 LAG 之每個連接埠的狀態。
- 透過 LACP 收到的合作夥伴 MAC 位址。

六個負載平衡選項可用於設定。建立 LAG 與彙總器連接埠時，必須選擇負載平衡選項。

ⓘ **重要：**建立 LAG 之後，您無法修改負載平衡選項。

檢視連結彙總

主題：

檢視狀態

狀態表顯示防火牆的 MAC 位址系統 ID。

檢視連結彙總連接埠

若要檢視「連結彙總連接埠」，請導覽至**系統設定 | 交換 | 連結彙總**

連接埠	作為彙總器連接埠或成員連接埠的介面
LAG ID	系統設定的連結彙總器。不是彙總器的連接埠具有其所屬之彙總器的 LAG ID。

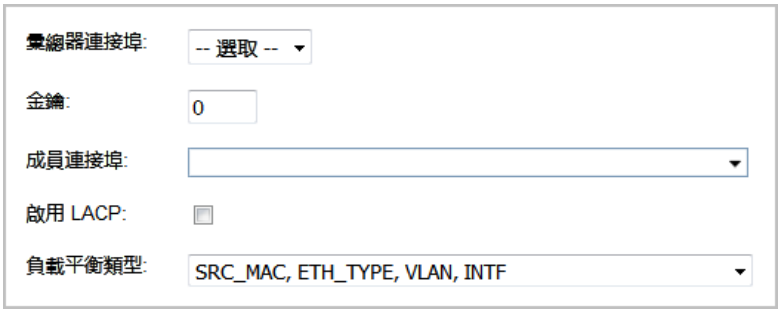
金鑰	指出**新增 LAG 連接埠**對話的連接埠成員資格。
彙總	以綠色核取記號指出彙總器連接埠；否則會是空白。
啟用 LACP	指出 LACP 是否啟用。
狀態	指出連接埠為**上行**或**下行**。
合作夥伴	完成實體連接後之連結夥伴的 MAC 位址；適用於 • 靜態 LAG，顯示 **00:00:00:00:00:00** • 動態 LAG，顯示合作夥伴的 MAC 位址
供應商	顯示設備製造商的名稱。
操作	顯示這些圖示： • **統計資料** - 當滑鼠在上方時快顯 **LAG 連接埠統計資料**：  • **編輯** (只能編輯彙總器連接埠) • **刪除**

建立邏輯連結 (LAG)

若要建立邏輯連結 (LAG)：

1 導覽到**交換 | 連結彙總**。

2 按下**新增**。**新增 LAG 連接埠**對話隨即顯示。



3 從**彙總器連接埠**選取介面。

4 藉由在**金鑰**欄位中輸入所需的金鑰，將連接埠成員資格指定至 LAG 群組。最小值為 1，最大值為 255。此欄位的預設值為 **0**，必須更換。

5 從**成員連接埠**下拉功能表中選取要彙總的連接埠。您可以為要彙總的每個連接埠勾選核取方塊，以選取連接埠的任何成員。

ⓘ **附註：**列出的連接埠視步驟 3 中選擇的介面而定。

6 若要為此連接埠啟用連結彙總控制通訊協定 (LACP)，請選取**啟用 LACP**。預設情況下未勾選此選項。

7 從**負載平衡類型**中，選取執行負載平衡的方法:

ⓘ **重要：**建立 LAG 之後，您無法修改負載平衡選項。

- **SRC_MAC、ETH_TYPE、VLAN、INTF** (預設)
- **DST_MAC、ETH_TYPE、VLAN、INTF**
- **SRC_MAC、DST_MAC、ETH_TYPE、VLAN、INTF**
- **SRC_IP、SRC_PORT**
- **DST_IP、DST_PORT**
- **SRC_IP、SRC_PORT、DST_IP、DST_PORT**

8 按一下**確定**。

刪除 LAG

若要刪除 LAG 的成員:

1 移至**系統設定 | 交換 | 連結彙總**。

2 按一下其**刪除**圖示，以刪除 LAG 的成員連接埠。

若要刪除彙總器連接埠:

1 移至**系統設定 | 交換 | 連結彙總**。

2 按一下其**刪除**圖示，以刪除所有成員連接埠。

ⓘ **附註：**必須先從 LAG 刪除所有成員連接埠，然後再刪除彙總器連接埠。

3 按一下其**刪除**圖示，以刪除彙總器連接埠。

32

設定連接埠鏡像

附註：所有 NSA 3600 和以上的防火牆上均可切換。

交換 | 連接埠鏡像

主題：

關於連接埠鏡像

可以在 SonicOS 上設定連接埠鏡像，以便將一個或多個交換器連接埠（或 VLAN）看到的網路封包的副本傳送到另一稱為鏡像連接埠的交換器連接埠。通過連接鏡像連接埠，您可以監視經過鏡像連接埠的流量。

在 NSA 2650 上，VLAN 主幹連接埠可能是鏡像或已鏡像連接埠。對於所有其他平台，可以鏡像 VLAN 主幹連接埠，但不能作為鏡像連接埠本身。

管理 | 系統安裝 | 交換 | 連接埠鏡像可讓您指派鏡像連接埠以鏡像輸入、輸出，或傳出及/或傳入一組連接埠的雙向封包。

檢視鏡像連接埠

連接鏡像連接埠後，就可以監視被鏡像連接埠上的流量。

群組名稱 介面群組的名稱。

鏡像連接埠 用作鏡像連接埠的介面，也就是鏡像所選取方向的其他連接埠的連接埠。

方向 將鏡像之流量的方向：

- **兩者** (雙向)
- **輸入**
- **輸出**

輸入 到達已鏡像連接埠的封包數目。對於僅輸出的連接埠，此數目一律為 0。

輸出 已鏡像連接埠上傳出的封包數目。對於僅輸入的連接埠，此數目一律為 0。

啟用 指出針對群組已啟用鏡像 (核取方塊中有核取記號) 或已停用 (核取方塊中為空白)。

設定 針對群組項目，包含**編輯**和**刪除**圖示，而且針對群組中的每個連接埠，包含**刪除**圖示。

設定連接埠鏡像群組

若要建立新的連接埠鏡像群組：

1 導覽到**交換 | 連接埠鏡像**。

2 按一下**新增群組**。將顯示**編輯鏡像群組**對話。

3 在編輯鏡像對話方塊，在**介面群組名稱**欄位中輸入群組的描述性名稱。預設的名稱是**新增群組**。

4 對於**方向**，選擇以下選項之一：

- **輸入** - 監視到達已鏡像連接埠的流量。
- **輸出** - 監視已鏡像連接埠傳出的流量。
- **兩者皆是** - 監視已鏡像連接埠兩個方向的流量。

5 從**所有介面**清單:

a 選取要鏡像流量的目標連接埠。鏡像連接埠必須使用未指派的連接埠。

b 按一下頂端的**右箭頭**按鈕，將連接埠移至**鏡像連接埠**欄位。

6 從**所有介面**清單:

a 選取要監視的一個或多個連接埠。連接鏡像連接埠後，就可以監視被鏡像連接埠上的流量。

b 按一下下方的**右箭頭**按鈕，將一個或多個連接埠移至**已鏡像連接埠**清單。

7 若要啟用這些連接埠的連接埠鏡像，勾選**啟用**核取方塊。

> **附註：**一次只能啟用一個輸入群組和一個輸出群組。如果群組有兩個方向，且已啟用，則無法啟用個別的輸入和輸出群組，或具有兩個方向的另一個群組。個別的輸入和輸出群組可單獨啟用。
>
> 此選項會顯示為灰色，直到您指定鏡像連接埠及其已鏡像連接埠為止。

8 按一下**確定**。

啟用已鏡像群組

當您建立群組時如果未啟用已鏡像群組，則可以為已鏡像群組選取**啟用**，以在**群組**表格上啟用鏡像。

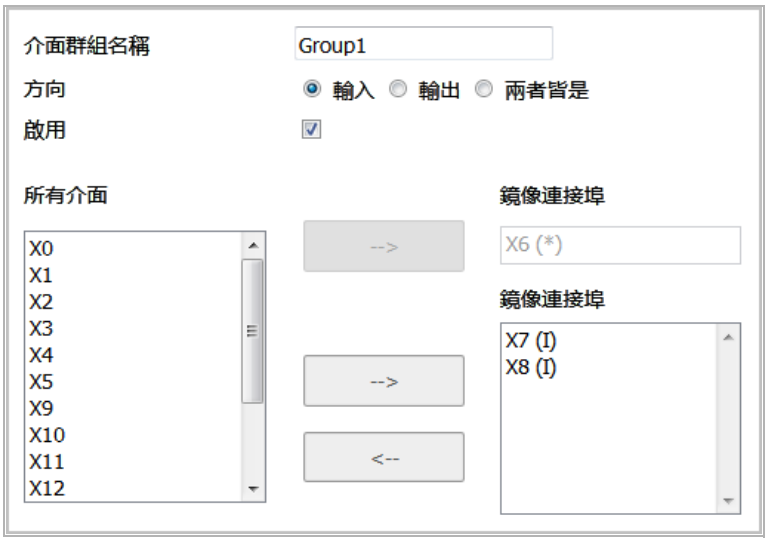
編輯連接埠鏡像群組

您可以編輯鏡像群組 (其顯示為灰色) 以外之已鏡像群組的所有屬性。

若要編輯連接埠鏡像群組:

1 導覽到**交換 | 連接埠鏡像**。

2 按一下鏡像連接埠的**編輯**圖示。隨即顯示群組的**編輯鏡像群組**對話方塊。



3 對任何選項進行變更。

> **附註：**您可以新增或刪除已鏡像連接埠，但無法新增或刪除鏡像連接埠本身。如果刪除群組的成員，不會顯示確認訊息。

4 如果已為群組啟用鏡像，則**啟用**為選取狀態。若要停用這些連接埠的連接埠鏡像，請取消勾選**啟用**。

> **附註：**一次只能啟用一個輸入群組和一個輸出群組。如果群組有兩個方向，且已啟用，則無法啟用個別的輸入和輸出群組，或具有兩個方向的另一個群組。個別的輸入和輸出群組可單獨啟用。

5 按一下**確定**。

刪除連接埠鏡像群組

您可以刪除鏡像群組的成員、鏡像群組、多個群組，或所有群組。

主題：

- 第 503 頁「移除連接埠群組成員」
- 第 504 頁「移除連接埠鏡像群組」
- 第 504 頁「移除多個連接埠鏡像群組」
- 第 504 頁「移除所有連接埠鏡像群組」

移除連接埠群組成員

您可以刪除第 502 頁「編輯連接埠鏡像群組」中所述連接埠群組的成員，也可在**群組**表中刪除它。

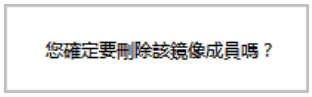
若要移除群組表格中連接埠群組的成員:

1 導覽到**交換 | 連接埠鏡像**。

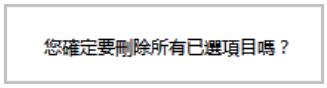
2 按下群組的**展開**按鈕，即顯示群組成員。

3 您可以

- 對於要刪除的成員，按一下**刪除**圖示。將顯示確認訊息。



- 按一下要刪除之成員的一個或多個核取方塊，然後按一下**刪除群組**。將顯示確認訊息。



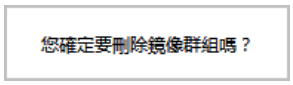
4 按一下**確定**。

移除連接埠鏡像群組

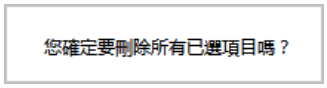
若要移除群組表中的連接埠鏡像群組：

1 您可以

- 對於要刪除的群組，按一下**刪除**圖示。將顯示確認訊息：



- 勾選群組的核取方塊，然後按一下**刪除群組**。將顯示確認訊息：



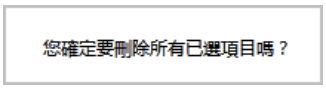
2 按一下**確定**。

移除多個連接埠鏡像群組

若要移除多個連接埠鏡像群組:

1 在**群組**表格中，勾選要刪除的鏡像群組旁的核取方塊。

2 按一下**刪除群組**按鈕。將顯示確認對話方塊。



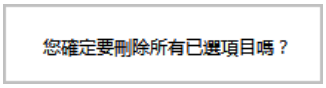
3 按一下**確定**。

移除所有連接埠鏡像群組

若要移除所有連接埠鏡像群組:

1 在**群組**表格中，勾選表格標題中的核取方塊。

2 按一下**刪除群組**按鈕。將顯示確認對話方塊。



3 按一下確認對話方塊中的**確定**。

部分 6

高可用性

- 關於高可用性和主動/主動叢集
- 設定高可用性
- 微調高可用性
- 監視高可用性

33

關於高可用性和主動/主動叢集

附註：TZ 系列及上述安全設備支援高可用性 (HA)。TZ500 系列與上述安全設備支援可設定狀態 HA 與主動/主動 DPI。請參閱第 515 頁「使用中/待命和主動/主動 DPI 前提條件」。NSA 3600 與上述安全設備支援主動/主動叢集。請參閱第 530 頁「主動/主動叢集的授權要求」。

NAT64 不支援狀態高可用性。

高可用性

本節提供 SonicOS 中高可用性 (HA) 的概念資訊，並介紹為 HA 連接安全設備的方法。

主題：

關於高可用性

主題：

什麼是高可用性？

高可用性 (HA) 是備援設計，可讓兩個執行 SonicOS 的相同 SonicWall 安全設備設定為提供可靠、連續的公用網際網路連接。一個 SonicWall 設定為主要裝置，另一個相同的安全設備設定為次要裝置。如果主要安全設備失效，次要安全設備將接管以確保受防護網路與網際網路之間的連接安全可靠。以這種方式設定的兩個安全設備也稱為高可用性對 (HA 對)。

當一個安全設備用作另一個安全設備的高可用性系統時，這兩個 SonicWall 安全設備可以透過高可用性共用 SonicWall 授權。兩個安全設備必須為相同的 SonicWall 型號。

若要使用此功能，必須在 MySonicWall 上將 SonicWall 安全設備註冊為相關產品。如需進一步資訊，請參閱第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」。

高可用性術語

使用中	硬體裝置有效工作的狀態。使用中識別項是一個邏輯角色，主要或次要硬體裝置均可充當這一角色。
容錯移轉	使用中裝置達到失效標準時，備用裝置充當使用中角色的實際過程。是否失效由第 533 頁「設定高可用性」中所述的各種可設定實體和邏輯監控設施來判斷。
HA	高可用性：非狀態、硬體容錯移轉功能。
IDV	透過 VLAN 消除介面歧義。
PoE	乙太網路供電是一項技術，可讓網路線攜帶電力。
PPP	點對點通訊協定提供標準方法，透過點對點連結傳輸多通訊協定圖表。
PPPoE	透過乙太網路傳送 PPP 的方式。
PPPoE HA	無狀態的 HA PPPoE 支援功能。
先佔	適用於容錯移轉後的狀態：主要裝置已經失效，次要裝置已充當使用中角色。先佔啟用時，主要裝置如果已恢復到已驗證的操作狀態，就會從次要裝置收回使用中角色。
主要的	主要硬體裝置本身。主要識別項是手動指定，不隨條件而變化。正常工作條件下，主要硬體裝置工作在使用中模式。
次要 (備份)	從屬硬體裝置本身。次要識別項是一個相對稱謂，與主要裝置配對的裝置就是次要裝置。正常工作條件下，次要硬體裝置工作在備用模式。主要裝置失效時，次要裝置進入使用中模式。

SHF	狀態硬體容錯移轉是 SonicOS 的一項功能，可讓現有網路流量在主要安全設備失效時由備份安全設備接管以維持作用中。
備用 (閒置)	硬體裝置被動待命的狀態。備用識別項是一個邏輯角色，主要或次要硬體裝置均可充當這一角色。使用中裝置確定失效時，備用裝置就會充當使用中角色。
STP	產生樹狀目錄通訊協定。

高可用性模式

高可用性包含幾種作業模式，可以從**高可用性 | 基本設定**進行選取:

- **無**-選擇**無**，以使用啟用可設定狀態 HA 和雙主機 DPI 的選項啟用標準高可用性設定和硬體容錯移轉功能。
- **使用中/待命** - 使用中/待命模式為基本高可用性功能提供兩個完全相同的安全設備作為高可用性對的設定。使用中裝置處理全部流量，而備用裝置共用其設定，並可以在使用中裝置停止工作時隨時接管以提供連續的網路連接。

  預設情況下，使用中/待命模式無狀態，這表示必須在容錯移轉後重新建立網路連接和 VPN 通道。為了避免這種情況，可以在使用中/待命模式中授權和啟用狀態同步。在此可設定狀態 HA 模式下，使用中裝置與備用裝置的動態狀態持續同步。使用中裝置遇到故障時，就會發生可設定狀態容錯移轉，待命安全設備成為使用中防火牆，現有網路連接無中斷。

  ⓘ **附註：**可設定狀態 HA：
  - 包含到 NSA 4600 和更高版本 NSA 平台及 SuperMassive 系列平台。
  - 僅在含 SonicOS 擴充授權或高可用性授權的 NSA 2600 和 NSA 3600 平台才受支援。
  - 僅在含 SonicOS 擴充授權或高可用性 (狀態) 升級授權的 TZ500 和更高版本 TZ 平台才受支援。

  如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」和第 517 頁「授權高可用性功能」。

- **主動/主動 DPI**-主動/主動深層封包檢查 (DPI) 模式可以與使用中/待命模式一同使用。主動/主動 DPI 模式啟用時，處理器密集型 DPI 服務，例如入侵保護 (IPS)、閘道防毒 (GAV) 和防間諜軟體等在待命安全設備上處理；與此同時，其他服務則在活動安全設備上處理，例如防火牆、 NAT 和其他類型的流量等。

  ⓘ **附註：**主動/主動 DPI 已：
  - 包含在 SM 9000 系列平台。
  - 僅在含 SonicOS 擴充授權或高可用性 (狀態) 授權的 NSA 5600 和以上版本的平台才受支援。

  如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」和第 517 頁「授權高可用性功能」。

- **主動/主動叢集** - 在此模式下，多個安全設備歸為一組，稱為叢集節點，多個使用中裝置負責處理流量（用作多個閘道）、執行 DPI 和分擔網路負載。每個叢集節點包括兩台裝置，用作一個可設定狀態 HA 對。除了負載分擔以外，主動/主動叢集還支援可設定狀態容錯移轉。每個叢集節點也可以只包括一台裝置，這種情況下，可設定狀態容錯移轉和主動/主動 DPI 無法使用。

  ⓘ **附註：**主動/主動叢集為:
  - 包含在 SM 9000 系列平台。
  - 僅在購買 SonicOS 擴充授權的 NSA 3600 和以上版本的平台才受支援。

  如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」和第 517 頁「授權高可用性功能」。

- **主動/主動 DPI 叢集**-此模式支援設定最多 4 個 HA 叢集節點用於容錯移轉和負載分擔，這些節點對網路流量的 DPI 安全服務進行應用程式負載均衡。啟動這種模式時，各叢集節點中的備用裝置可得到利用，從而獲得更好的效能。

  附註：主動/主動 DPI 叢集為:
  - 包含在 SM 9000 系列平台
  - 僅在購買 SonicOS 擴充授權的 NSA 3600 和以上版本的平台才受支援。

  如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」和第 517 頁「授權高可用性功能」。

當機偵測

對於使用中和待命安全設備而言，HA 功能均有縝密的自我診斷機制。當關鍵服務受影響，監控介面上偵測到實體 (或邏輯) 連結故障，或安全設備斷電時，就會容錯移轉到備用裝置。

自檢機制由軟體診斷程式管理，用於檢查安全設備的全系統完整性。診斷程式檢查內部系統狀態、系統進程狀態和網路連接。兩側均有衡量機制，用於判斷哪一側的連接效能更好，避免潛在的容錯移轉循環。

即時檢查 NAT、VPN 和 DHCP 等關鍵內部系統進程。儘早隔離故障服務，由容錯移轉機制自動修復。

虛擬 MAC 位址

虛擬 MAC 位址支援高可用性對共用同一 MAC 位址，從而大幅縮短容錯移轉後的融合時間。融合時間是指網路中的裝置根據高可用性引起的變化調整路由表所需的時間。

如果不啟用虛擬 MAC，使用中和備用安全設備各有自己的 MAC 位址。這些安全設備使用同一 IP 位址，當容錯移轉發生時，將打破所有用戶端和網路資源的 ARP 快取中的 IP 位址與 MAC 位址之間的對應關係。次要安全設備必須發出 ARP 請求，宣佈新的 MAC 位址/IP 位址對。在此 ARP 請求傳播到整個網路之前，以主要安全設備的 MAC 位址為目的地的流量可能遺失。

虛擬 MAC 位址可藉由使用主要和次要安全設備的相同 MAC 位址，來大幅簡化此程序。發生容錯移轉時，主要安全設備的所有來往路由對次要安全設備仍然有效。 所有用戶端和遠端站台繼續使用同一虛擬 MAC 位址和 IP 位址，無需中斷。

預設情況下，虛擬 MAC 位址由 SonicWall 韌體提供，且不同於主要或次要安全設備的實體 MAC 位址。這樣可消除設定錯誤的可能性，確保虛擬 MAC 位址的唯一性，防止可能的衝突。或者，您也可以在**高可用性 | 監控設定**上手動設定虛擬 MAC 位址。

即使狀態高可用性未經授權，虛擬 MAC 設定也是可用的。啟用虛擬 MAC 後，即便狀態同步未啟用，它也始終有效。

具有 PPPoE HA 的動態 WAN 介面

附註：SuperMassive 9800 上不支援具有 PPPoE HA 的動態 WAN 介面。僅支援 DHCP 伺服器動態 WAN 模式。

從 SonicOS 6.2.7.0 開始，PPoE 可在介面上以非狀態模式、HA 使用中/待命模式啟用。PPPoE HA 提供 HA，其中次要安全設備會在使用中安全設備故障時連線到 PPPoE 伺服器。

附註：一個 WAN 介面必須設定為 PPPoE；請參見第 249 頁「設定 WAN 介面」。

在使用中裝置連線到 PPPoE 伺服器後，安全設備會將 PPPoE 工作階段 ID 和伺服器名稱同步到次要防火牆。

在使用中安全設備失效時，它會在用戶端這一端透過逾時來終止 PPPoE HA 連線。然後，次要安全設備會在伺服器端終止原來的連線，並啟動新的 PPPoE 連線。所有原有的網路連接會重建，PPPoE 工作階段也重新建立，PPP 程序則重新交涉。

狀態同步與 DHCP

透過 SonicOS 6.2.7，DHCP 現在可在使用中/待命 (非狀態) 和狀態同步模式下在介面上啟用。

僅使用中安全設備可以取得 DHCP 租用。使用中安全設備會將 DHCP IP 位址連同 DNS 和閘道位址同步到次要安全設備。DHCP 用戶端 ID 也會同步，讓此功能即使未啟用虛擬 MAC 也能運作。

在容錯移轉期間，使用中安全設備會釋放 DHCP 租用，而次要安全設備會在其變為使用中裝置時，使用現有 DHCP IP 位址和用戶端 ID 更新 DHCP 租用。IP 位址不會變更，而網路流量包括 VPN 通道流量會繼續通過。

如果使用中安全設備在發生容錯移轉時沒有 IP 位址，則次要安全設備會啟動新的 DHCP 探索。

狀態同步與 DNS 代理

DNS 代理支援 DNS 快取的狀態同步。當動態新增、刪除或更新 DNS 快取時，它會與閒置的安全設備同步。

關於 HA 監控

在**高可用性 | 監控設定**上，可以設定實體和邏輯介面監控:

- 透過啟用實體介面監視，您可以對指定 HA介面進行連結偵測。連結在實體層偵測以確定其可行性。
- 邏輯監控涉及到設定 SonicWall 來監視一個或多個相連網路上的某一可靠裝置。

如果 HA 對中的使用中裝置未能定期與此裝置通信，將觸發容錯移轉到備用裝置。如果 HA 對中沒有任何裝置能夠連接到此裝置，則不會採取任何操作。

在**高可用性 | 監控設定**上設定的主要和次要 IP 位址可以在 LAN 或 WAN 介面上設定，以供多種用途使用:

- 作為各裝置的獨立管理位址（所有實體介面均支援）
- 支援備用裝置與 SonicWall 授權伺服器之間的授權同步
- 作為邏輯監控期間發出的探查 ping 的來源 IP 位址

為 HA 對中的各裝置設定不同的管理 IP 位址，就可以獨立登入到各裝置進行管理。注意，忽略傳送到此類 IP 位址的非管理流量。主要和次要安全設備的唯一 LAN IP 位址不能用作使用中閘道；連接到內部 LAN 的所有系統都需要使用虛擬 LAN IP 位址作為其閘道。

如果設定了 WAN 監視 IP 位址，則不需要 X0 監視 IP 位址。如果未設定 WAN 監視 IP 位址，則需要 X0 監視 IP 位址，因為在此情況中，備用裝置使用 X0 監視 IP 位址連接到授權伺服器，所有流量透過使用中裝置傳送。

次要/備用裝置的管理 IP 位址用於與 SonicWall 授權伺服器進行授權同步，授權伺服器按安全設備（而非按 HA 對）處理授權。即使次要裝置在建立 HA 關聯之前已經在 MySonicWall 上註冊，您仍然需要透過其管理 IP 位址存取次要安全設備，同時使用**管理 | 更新 | 授權**上的連結連接到 SonicWall 伺服器 (如需詳細資訊，請參閱 *SonicOS 更新*)。

使用邏輯監控時，HA 對將從主要和次要裝置 ping 指定的邏輯探查 IP 位址目的地。主要 IP 位址或次要 IP 位址欄位中設定的 IP 位址用作 ping 的來源 IP 位址。如果二者均能成功 ping 通目的地，則不會發生容錯移轉。如果二者均無法 Ping 到目標，沒有發生容錯移轉，因為 SonicOS 認為問題出在目標，而不是安全設備。但是，如果一個安全設備可以 Ping 到目標，而另一個無法，則 HA 對會容錯移轉至可 Ping 到目標的裝置。

高可用性 | 監控設定上的設定任務會在主要裝置上進行，然後自動同步到次要裝置。

關於使用中/待命 HA

HA 支援設定兩個執行 SonicOS 的相同安全設備來以提供可靠、連續的公用網際網路連線。一個安全設備設定為主要裝置，另一個相同的安全設備設定為次要裝置。如果主要安全設備失效，則次要安全設備將接管以確保受防護網路與網際網路之間的連線安全可靠。以這種方式設定的兩個安全設備也稱為高可用性對 (HA 對)。

使用中/待命 HA 提供標準高可用性和硬體容錯移轉功能，可選擇啟用狀態 HA 和主動/主動 DPI。

當一個安全設備作為另一個安全設備的高可用性系統時，HA 提供一種方式，可在兩個安全設備之間共用授權。若要使用此功能，必須在 MySonicWall 上將安全設備註冊為相關產品。兩個安全設備必須為相同的 SonicWall 型號。

主題：

使用中/待命 HA 的優點

- **更高的網路可用性** - 在高可用性設定中，當主要裝置失效時，次要安全設備會承擔其所有網路責任，確保受防護網路與網際網路之間的連接可靠。
- **成本效益** - 對於透過使用冗餘安全設備來提供高可用性的開發方案，高可用性是一種成本效益選項。對於高可用性對中的次要裝置，無需再購買一套授權。
- **虛擬 MAC 縮短容錯移轉後的融合時間** - 利用虛擬 MAC 位址設定，HA 對可以共用同一 MAC 位址，從而大幅縮短容錯移轉後的融合時間。融合時間是指網路中的裝置根據高可用性引起的變化調整路由表所需的時間。預設情況下，虛擬 MAC 位址由 SonicWall 韌體提供，不同於主要或次要安全設備的實體 MAC 位址。

使用中/待命 HA 的工作方式

附註：TZ300 系列和 TZ400 系列安全設備可以在沒有可設定狀態同步的情況下，以使用中/待命 HA 模式執行。無論是否有狀態同步，SOHO W 都不支援高可用性。

HA 要求一個 SonicWall 安全設備設定為主要 SonicWall，另一個相同的安全設備設定為次要 SonicWall。正常工作期間，主要 SonicWall 處於使用中狀態，次要 SonicWall 處於備用狀態。如果主要裝置連接斷開，次要 SonicWall 裝置將轉換到使用中模式，並擔負起主要裝置的設定和角色，包括已設定介面的 IP 位址。

基本使用中/待命 HA 提供狀態高可用性。容錯移轉到次要安全設備之後，原有的所有網路連接必須重新建立，VPN 通道也必須重新交涉。可以單獨授權和啟用狀態同步。如需詳細資料，請參閱第 513 頁「關於狀態同步」。

容錯移轉適用於主要 SonicWall 的功能或網路層連接喪失的情形。關鍵服務受影響，受監視介面上偵測到實體（或邏輯）連結故障，或者主要 SonicWall 斷電時，就會容錯移轉到次要 SonicWall。主要和次要 SonicWall 裝置目前僅能執行「使用中/待命高可用性」或「主動/主動 DPI」，尚不支援完整的「主動/主動高可用性」。

所有設定都有兩類同步：

- **增量** - 如果時間戳記同步且使用中裝置有變更，備用裝置將發生增量同步。
- **完成** - 如果時間戳記不同步且備用裝置可用，備用裝置將發生完整同步。增量同步失敗時，將自動嘗試完整同步。

關於狀態同步

狀態同步可顯著改善容錯移轉效能。在啟用後，網路連接和 VPN 通道資訊在兩個裝置之間持續同步，當主要安全設備失效時，次要防火牆可無縫地承擔起所有網路責任，現有網路連接不會中斷。

附註：已將可設定狀態 HA 包含到 NSA 4600 和更高版本 NSA 平台及所有 SuperMassive 系列平台。在含擴充授權或可設定狀態 HA 升級授權的 TZ500 和更高版本 TZ 平台、NSA 2600 和 NSA 3600 平台上支援可設定狀態 HA。如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」和第 517 頁「授權高可用性功能」。

主題：

狀態同步的優點

- **更高的可靠性** - 透過同步大部分關鍵網路連接資訊，狀態同步可防止安全設備故障引起停機和連接遺失。
- **更快速的容錯移轉效能** - 透過維護主要防火牆和次要安全設備之間的持續同步，可設定狀態同步支援次要安全設備在故障情況下接管，幾乎沒有停機時間或網路連線遺失。
- **對 CPU 效能的影響極小** - 使用率一般不到 1%。
- **對頻寬的影響極小** - 同步資料的傳送受到限制，不會干擾其他資料。

狀態同步的工作方式

狀態同步不進行負載均衡。它是一種使用中/待命設定，由主要安全設備處理所有流量。狀態同步啟用時，主要安全設備會主動與次要安全設備通訊，更新大部分網路連線資訊。當主要安全設備建立和更新網路連接資訊（VPN 通道、活動使用者、連接快取項目等）時，它會立即告知次要安全設備。這樣就確保了次要安全設備可以隨時轉換至使用中狀態，無需放棄任何連接。

同步流量受到限制，確保不干擾正常網路流量。所有設定變更都在主要安全設備上進行，並自動傳播到次要安全設備。無論哪一台安全設備目前是使用中的，高可用性對均使用相同的 LAN 和 WAN IP 位址。

使用 SonicWall 全域管理系統 (GMS) 管理安全設備時，GMS 登入共用 WAN IP 位址。容錯移轉時，GMS 管理繼續無縫進行，不會登出目前登入到安全設備的 GMS 管理員，但 **Get** 和 **Post** 命令可能以逾時結束，不會獲得任何回應。

已同步和未同步的資訊表格列出了狀態同步已同步的資訊和目前尚未同步的資訊。

已同步和未同步的資訊

已同步的資訊	未同步的資訊
VPN 資訊	動態 WAN 用戶端（L2TP、PPPoE 和 PPTP）
基本連接快取	深度封包檢查（GAV、IPS 和防間諜軟體）
FTP	IPHelper 繫結（例如 NetBIOS 和 DHCP）
Oracle SQL*NET	SYNFlood 防護資訊
即時音訊	內容篩選服務資訊
RTSP	VoIP 通訊協定
GVC 資訊	動態 ARP 項目和 ARP 快取逾時

已同步和未同步的資訊

已同步的資訊	未同步的資訊
動態位址物件	使用中無線用戶端資訊
DHCP 伺服器資訊	無線用戶端封包統計
多點傳送和 IGMP	欺詐存取點清單
使用中使用者	
ARP	
SonicPoint 狀態	
無線來賓狀態	
授權資訊	
加權負載均衡資訊	
RIP 和 OSPF 資訊	

狀態同步實例

容錯移轉時會發生以下事件序列：

1. PC 使用者連接到網路，主要安全設備為此使用者建立一個工作階段。
2. 主要安全設備與次要安全設備同步。次要裝置現在擁有此使用者的所有工作階段資訊。
3. 管理員重新啟動主要裝置。
4. 次要裝置偵測到主要裝置重新啟動，從備用狀態切換到使用中狀態。
5. 次要安全設備開始向 LAN 和 WAN 交換器傳送無故 ARP 訊息，使用與主要安全設備相同的虛擬 MAC 位址和 IP 位址。下游和上游網路裝置無需進行路由更新。
6. 當 PC 使用者試圖存取網頁時，次要安全設備擁有此使用者的所有工作階段資訊，能夠不間斷地繼續此使用者的工作階段。

關於主動/主動 DPI HA

重要：在主動/主動 DPI 模式中不支援捕獲功能。

可設定狀態 HA 對啟用主動/主動 DPI 時，深層封包檢查服務在 HA 對的待命安全設備上處理，與此同時，安全設備、NAT 和其他模組的處理則在使用中安全設備上進行。下列 DPI 服務會受影響：

- 入侵保護服務 (IPS)
- 閘道防毒 (GAV)
- 閘道防間諜軟體
- 應用程式控制

若要使用主動/主動 DPI 功能，您必須將其他介面設定為**主動/主動 DPI 介面**。例如，如果選擇讓 X5 成為主動/主動 DPI 介面，必須將 HA 對中的使用中裝置的 X5 實體連接到備用裝置的 X5。透過主動/主動 DPI 介面，使用中裝置上的某些封包流量分流到備用裝置。DPI 在備用裝置上執行，結果透過同一介面返回使用中裝置。其餘處理在使用中裝置上執行。

附註：已將主動/主動 DPI 包含到 SuperMassive 9200、9400 和 9600 平台。僅在含擴充授權的 NSA 5600 和 NSA 6600 上支援主動/主動 DPI。如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」和第 517 頁「授權高可用性功能」。

主動/主動 DPI HA 的優點

主動/主動 DPI 發揮了備用裝置未使用 CPU 週期的作用，但流量仍然透過使用中裝置到達和離開。備用裝置僅看到使用中裝置分載的網路流量，除 DPI 服務以外的其他模組只能由使用中裝置處理。

使用中/待命和主動/主動 DPI 前提條件

本節列出支援的平台，提供實體連接裝置所需的推薦和要求，並描述如何註冊、關聯和授權裝置以執行高可用性。

主題：

HA 的支援平台

購買 SonicWall 安全設備時所包括的授權會顯示在 HA、可設定狀態 HA，以及 A/A DPI 的授權需求表格。有些平台需要其他授權才能使用 HA 功能。HA 升級與擴充授權可透過 MySonicWall 或 SonicWall 經銷商購買。

附註：HA 授權必須在各安全設備上啟用，方法是在 SonicOS 管理介面的 MySonicWall 上註冊裝置；如果網際網路存取無法使用，則將授權金鑰組套用到各裝置。

HA、可設定狀態 HA，以及 A/A DPI 的授權需求

平台	HA	可設定狀態 HA	A/A DPI
SM 9600	包含	包含	包含
SM 9400	包含	包含	包含
SM 9200	包含	包含	包含
NSA 6600	包含	包含	擴充授權
NSA 5600	包含	包含	擴充授權
NSA 4600	包含	包含	N/A
NSA 3600	包含	擴充授權或 HA 授權	N/A
NSA 2600	包含	擴充授權或 HA 授權	N/A
TZ600	包含	可設定狀態 HA 升級或擴充授權	N/A
TZ500/TZ500 W	包含	可設定狀態 HA 升級或擴充授權	N/A
TZ400/TZ400 W	包含	N/A	N/A
TZ300/TZ300 W	包含	N/A	N/A
SOHO W	N/A	N/A	N/A

您可以在**管理 | 更新 | 授權**上檢視系統授權。透過此頁面還可以登入 MySonicWall。如需授權資訊，請參見第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」。

實體連接您的安全設備

附註：如需連接安全設備的完整步驟，請參閱防火牆的*入門指南*。如需連接主動/主動叢集防火牆的步驟，參閱第 531 頁「連接主動/主動叢集的 HA 連接埠」和第 531 頁「連接冗餘連接埠介面」。

如果將主要和次要安全設備連至使用產生樹狀目錄通訊協定的乙太網路交換器，注意可能需要調節 SonicWall 介面所連接的交換器連接埠上的連結啟用時間。例如，在 Cisco Catalyst 系列交換器上，需要為連接至 SonicWall 安全設備的介面的各連接埠啟用**產生樹狀目錄連接埠快速轉送**。

高可用性要求受影響的 SonicWall 安全設備之間擁有額外的實體連接。對於所需型號，您需要連接 HA 控制與 HA 資料。主動/主動 DPI 要求額外的連接。

在任何高可用性部署中，必須將所有裝置的 LAN 和 WAN 連接埠實體連接到適當的交換器。

需要將所有裝置的 X0 介面連接到相同的廣播網域，這很重要。否則，流量容錯移轉將失效。此外，X0 是預設的冗餘 HA 連接埠，如果正常的 HA 控制連結斷開，X0 可用於傳送裝置之間的偵測信號。如果在同一廣播網域中沒有 X0，則如果 HA 控制連結斷開，兩個裝置都變為使用中裝置。

WAN 連線可用於在 MySonicWall 上註冊安全設備，以及同步授權資訊。除非網路原則禁止與 SonicWall 授權伺服器即時通信，註冊和授權之前應連接 WAN (X1) 介面。

連接主動/主動 DPI 的主動/主動 DPI 介面

對於主動/主動 DPI，必須在各 HA 對或叢集節點的兩台安全設備之間連接至少一個附加介面，稱為**主動/主動 DPI 介面**。兩個安全設備上的相連介面必須是同一號碼，而且最初必須在**管理 | 系統安裝網路 | 介面**中顯示為未使用、未指派的介面。例如，如果 X5 是未指派介面，則可以將主要裝置的 X5 連接到次要裝置的 X5。啟用主動/主動 DPI 後，連接的介面將具有 **HA 資料-連結**的區域指派。

透過主動/主動 DPI 介面，使用中裝置上的某些封包流量分流到備用裝置。DPI 在備用裝置上執行，結果透過同一介面返回使用中裝置。

此外，為使主動/主動 DPI 具有連接埠冗餘，可以在各 HA 對的兩台安全設備之間實體連接第二個主動/主動 DPI 介面。在主動/主動 DPI 處理期間，如果第一個主動/主動 DPI 介面發生故障，第二個介面可以接管兩台裝置之間的資料傳送。

連接主動/主動 DPI 的主動/主動 DPI 介面的步驟如下：

1. 決定將哪一個介面用於 HA 對的安全設備之間的其他連接。各台安全設備必須選擇同一介面。
2. 在 SonicOS 管理介面管理介面上，導覽至**管理 | 系統安裝 | 網路 | 介面**，確保預定之主動/主動 DPI 介面的**區域**為**未指派**。
3. 使用標準乙太網路纜線直接連接這兩個介面。
4. 此外，為使主動/主動 DPI 具有連接埠冗餘，可以在各 HA 對的兩台安全設備之間實體連接第二個主動/主動 DPI 介面。

在 MySonicWall 上註冊與建立安全設備的關聯

若要使用高可用性，您必須在 MySonicWall 上註冊這兩個安全設備並建立關聯。在 MySonicWall 頁面按一下已註冊安全設備的連結時，將顯示此安全設備的「服務管理」頁面。在「服務管理」頁面的底部，您可以按一下「相關產品」下的「HA 備用」連結。然後，按照說明為 HA 對選擇和關聯其他裝置。如需註冊安全設備的更多資訊，請參閱安全設備的*入門指南*。

安全設備關聯為 HA 對之後，就可以共用授權。除高可用性授權外，還包括 SonicOS 授權、支援訂閱和安全服務授權。用於諮詢服務的授權則不可共用，例如 SonicWall GMS 預防性維護服務的授權。

主要和次要安全設備不要求啟用相同的安全服務。安全服務設定作為設定初始同步的一部分以自動更新。使用授權同步可使次要安全設備保持與容錯移轉之前相同的網路防護層級。

MySonicWall 提供了幾種關聯兩台安全設備的方法。您可以註冊一台新的安全設備，然後選擇一台已註冊裝置與之關聯。或者，也可以關聯兩台均已註冊過的裝置。還有一種方法是先選擇一台已註冊裝置，再新增一台新安全設備與之關聯。

重要：即使您已先在 MySonicWall 註冊您的安全設備，在登入每台安全設備單獨的管理 IP 位址時，仍需要在 SonicOS 管理介面上分別註冊主要和次要安全設備。這將使次要裝置可以和 SonicWall 授權伺服器同步，並與關聯的主要安全設備共用授權。限制網際網路存取後，您可以將共用授權手動套用到這兩個安全設備。

授權高可用性功能

購買 SonicWall 安全設備時包括的 HA 授權會顯示在隨 SonicWall 安全設備提供的 HA 授權表格。有些平台需要附加授權才能使用狀態同步或主動/主動 DPI 功能。SonicOS 擴充授權或高可用性授權可以透過 MySonicWall 或向 SonicWall 分銷商購買。

附註：狀態高可用性授權必須在各台安全設備上啟用，方法是在 MySonicWall 管理介面的 SonicOS 上註冊裝置，或者將授權金鑰組套用到各裝置（如果網際網路存取無法使用）。

隨 SonicWall 安全設備提供的 HA 授權

平台	使用中/待命 HA [a]	可設定狀態 HA	A/A 叢集	A/A DPI
SM 9600	包含	包含	包含	包含
SM 9400	包含	包含	包含	包含
SM 9200	包含	包含	包含	包含
NSA 6600	包含	包含	擴充授權	擴充授權
NSA 5600	包含	包含	擴充授權	擴充授權
NSA 4600	包含	包含	擴充授權	N/A
NSA 3600	包含	擴充授權 HA 授權	擴充授權	N/A
NSA 2650	包含	擴充授權 HA 授權	N/A	N/A
NSA 2600	包含	擴充授權 HA 授權	N/A	N/A
TZ600	包含	擴充授權 可設定狀態 HA 升級授權	N/A	N/A
TZ500/TZ500 W	包含	擴充授權 可設定狀態 HA 升級授權	N/A	N/A
TZ400/TZ400 W	包含	N/A	N/A	N/A
TZ300/TZ300 W	包含	N/A	N/A	N/A
SOHO W	N/A	N/A	N/A	N/A

a. NA = 功能無法使用

您可以在**管理 | 更新 | 授權**上檢視系統授權。透過此頁面還可以登入 MySonicWall 及將授權套用到安全設備。如需進一步資訊，請參閱 *SonicOS 更新*。

如果 HA 對中的安全設備無法網際網路存取，也有辦法同步授權。當網路原則禁止與 SonicWall 授權伺服器即時通信時，可以使用授權金鑰組將安全服務授權手動套用到安全設備。在 MySonicWall 上註冊安全設備時，會產生此安全設備的授權金鑰組。如果新增一份新的安全服務授權，金鑰組會更新。但是，只有將授權套用至安全設備時，才可執行授權的服務。

重要：在無網際網路連接的高可用性部署中，HA 對中的兩台安全設備均必須套用授權金鑰組。

維護

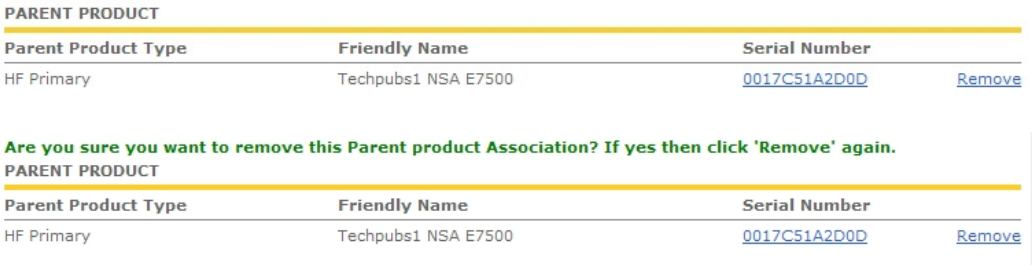
主題：

移除 HA 關聯

可以隨時在 MySonicWall 上移除兩台 SonicWall 安全設備之間的關聯。如果更換安全設備或重新設定網路就可能需要移除現有的 HA 關聯。例如，如果其中一台 SonicWall 安全設備失效，就需要更換。或者，您可以需要將 HA 主要安全設備與次要防火牆或 HA 次要裝置交換，直到網路重新設定完成。在任一情況下，都必須首先移除現有的 HA 關聯然後建立一個新的關聯，新關聯將使用新安全設備或改變兩台裝置之間的父子關係 (參閱第 519 頁「更換 SonicWall 安全裝置」)。

若要移除兩台已註冊 SonicWall 安全設備:

1. 登入 MySonicWall。
2. 在左側導覽列中，按一下**我的產品**。
3. 在**我的產品**頁面的**已註冊產品**下，捲動尋找將移除關聯的次要安全設備。按一下產品**名稱**或**序號**。
4. 在**服務管理 - 關聯產品**頁面中，向下捲動至**父級產品**部分，就在**關聯產品**部分上面。
5. 在**父級產品**下，移除此安全設備的關聯的步驟是：
   a. 按一下**移除**。
   b. 等待頁面重新載入。
   c. 向下捲動。
   d. 再次按一下**移除**。



更換 SonicWall 安全裝置

如果 SonicWall 安全設備發生硬體故障並還在保修期內，SonicWall 將進行更換。這樣，您需要在 MySonicWall 上移除包含故障安全設備的 HA 關聯，並新增包含替換裝置的新 HA 關聯。如果您聯絡 SonicWall 技術支援來進行更換（也稱為 RMA），我們將為您提供最佳的支援服務。

在裝置架中將新裝置替換故障的安全設備後，可更新 MySonicWall 和您的 SonicOS 設定。

更換故障 HA 主要裝置與更換 HA 備用裝置略微不同。下面幾節將說明這兩個程式：

- 第 519 頁「更換 HA 主要裝置」
- 第 519 頁「更換 HA 次要裝置」

更換 HA 主要裝置

更換 HA 主要裝置：

1. 在剩餘的 SonicOS（次要裝置）的 SonicWall 安全設備管理介面的「高可用性」頁面中，取消勾選**啟用高可用性**停用此功能。
2. 勾選**啟用高可用性**。

   現在，舊次要裝置變為主要裝置。其序號自動顯示在「主要 SonicWall 序號」欄位中。
3. 在**次要 SonicWall 序號**欄位中輸入替換裝置的序號。
4. 按一下**同步設定**。
5. 在 MySonicWall 中移除舊的 HA 關聯。請參閱第 518 頁「移除 HA 關聯」。
6. 在 MySonicWall 中，註冊替換 SonicWall 安全設備 ，並建立將新的主要（原次要）裝置作為 HA 主要裝置的 HA 關聯，替換裝置作為 HA 次要裝置。請參閱第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」。
7. 請聯絡 SonicWall 技術支援部門將安全服務授權從原 HA 對轉移到新 HA 對。

   當 HA 主要裝置發生故障時需要執行此操作，因為授權與 HA 對中的主要裝置相聯。

更換 HA 次要裝置

更換 HA 次要裝置：

1. 在 MySonicWall 上按照第 518 頁「移除 HA 關聯」的說明移除舊的 HA 關聯。
2. 在 MySonicWall 上，註冊替換 SonicWall 安全設備。
3. 按照第 519 頁「更換 HA 主要裝置」的說明建立使用原 HA 主要裝置的 HA 關聯，使用替換裝置作為 HA 次要裝置。

主動/主動叢集

附註： NSA 3600 和上述安全設備支援主動/主動叢集。請參閱隨 SonicWall 安全設備提供的 HA 授權表格和 A/A 叢集的授權要求表格

關於主動/主動叢集

主動/主動叢集最多由四個叢集節點組成，利用多個使用中裝置處理流量 (用作多個閘道)，執行 DPI 和分擔網路負載。一個叢集節點可以包含一個可使用狀態 HA 對、一個無狀態 HA 對與標準容錯移轉，或單一獨立裝置，這種情況下，可設定狀態容錯移轉和主動/主動 DPI 無法使用。僅當叢集節點是一個可設定狀態 HA 對時，才能使用動態狀態同步。傳統 SonicWall 高可用性通訊協定或可設定狀態 HA 協定用於叢集節點內部，即 HA 對的裝置之間的通信。

如果一個叢集節點是一個可設定狀態 HA 對，則可以啟用叢集節點內部的主動/主動 DPI 以提高效能。

利用主動/主動叢集，您可以將某些流量指派給叢集中的各節點，提供冗餘和負載分擔，支援更高的傳送量，同時不會發生單點故障。

利用主動/主動叢集，您可以將某些流量指派給叢集中的各節點，提供冗餘和負載分擔，支援更高的傳送量，同時不會發生單點故障。

典型的推薦設定包括 4 個相同型號的 SonicWall 安全設備，設定為 2 個叢集節點，各節點包含一個可設定狀態 HA 對。對於更大的部署，叢集可以包括八個安全設備，設定為四個叢集節點 (或 HA 對)。在各叢集節點內部，可設定狀態 HA 保持動態狀態同步，以便實現無縫容錯移轉和零資料損失的單點故障。可設定狀態 HA 不是必需的，但強烈建議使用，以便在容錯移轉期間提供最佳效能。

負載分擔是透過將不同叢集節點設定為網路中的不同閘道而實現的。通常，這是由主動/主動叢集下游的其他裝置（更靠近 LAN 裝置）處理，如 DHCP 伺服器或路由器等。

叢集節點也可以是單一安全設備，可使用兩個安全設備建置主動/主動叢集設定。其中一個安全設備發生故障時，容錯移轉不是可設定狀態，因為叢集節點中的任一安全設備都沒有 HA 次要裝置。

主動/主動叢集在多個層級上實現了冗餘：

- 叢集提供冗餘叢集節點，發生故障時，各節點均可處理任何其他節點的流量。
- 叢集節點包含一個可設定狀態 HA 對，發生故障時，次要安全設備可以擔負起主要防火牆的責任。
- 連接埠冗餘，指定位使用的連接埠為另一連接埠的備用連接埠，提供介面層級的防護，無需容錯移轉到另一安全設備或節點。
- 可以啟用主動/主動 DPI，提高各叢集節點內的傳送量。

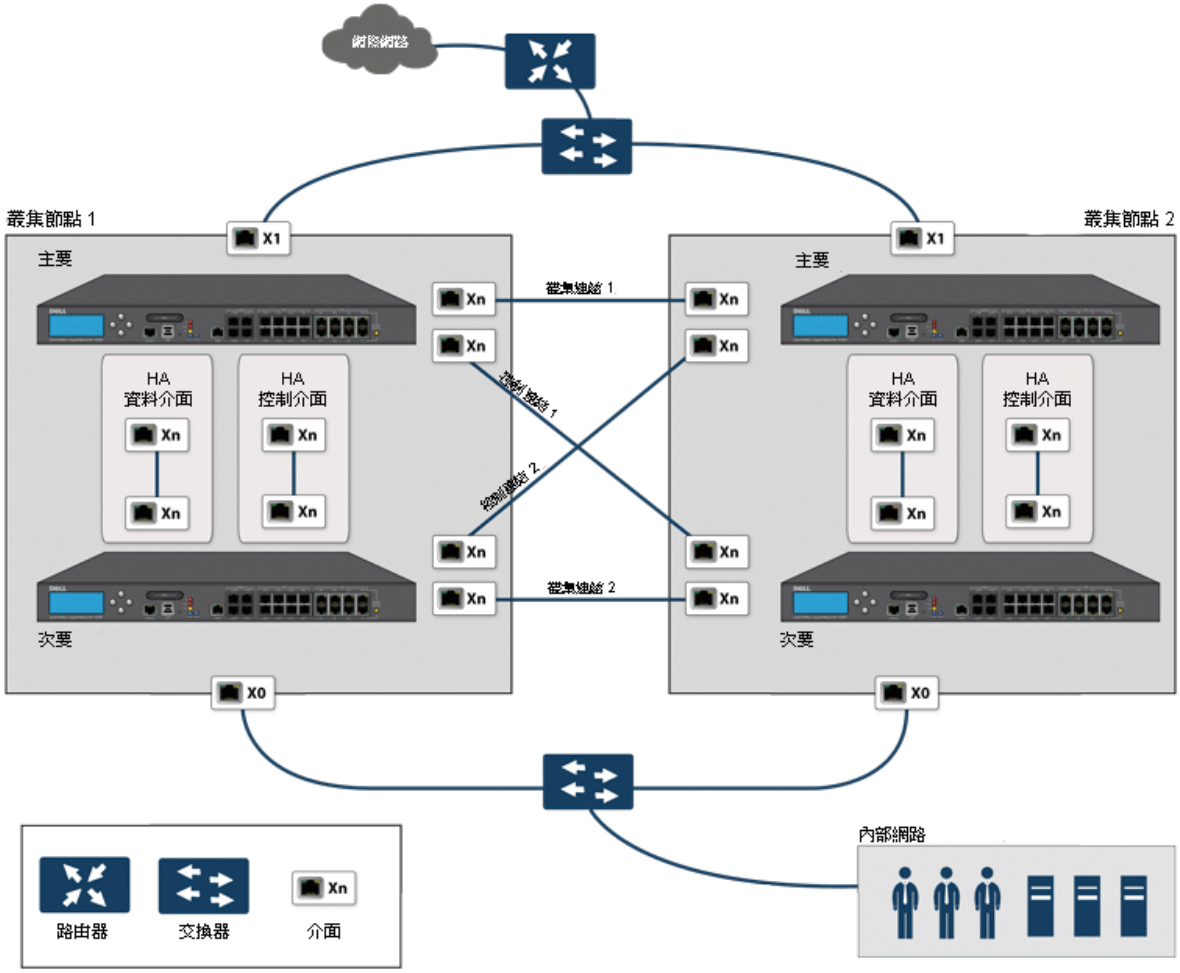
主題：

- 第 521 頁「範例：主動/主動叢集 - 四裝置部署」
- 第 522 頁「範例：主動/主動叢集 - 二裝置部署」
- 第 522 頁「主動/主動叢集的優點」
- 第 523 頁「主動/主動叢集的工作方式」
- 第 528 頁「主動/主動叢集支援的功能。」

範例：主動/主動叢集 - 四裝置部署

主動/主動四裝置叢集顯示了一個四裝置叢集。各叢集節點包含一個 HA 對。所有四台安全設備的指定 HA 連接埠連接到一個第 2 層交換器。這些連接埠用於叢集節點管理、監視透過 SVRRP 傳送的狀態訊息以及設定同步。各 HA 對中的兩台裝置還利用另一介面彼此相連（圖中顯示為 Xn 介面）。這是主動/主動 DPI 所需的主動/主動 DPI 介面。透過啟用主動/主動 DPI，某些封包分載到 HA 對的備用裝置進行 DPI 處理。

主動/主動四裝置叢集

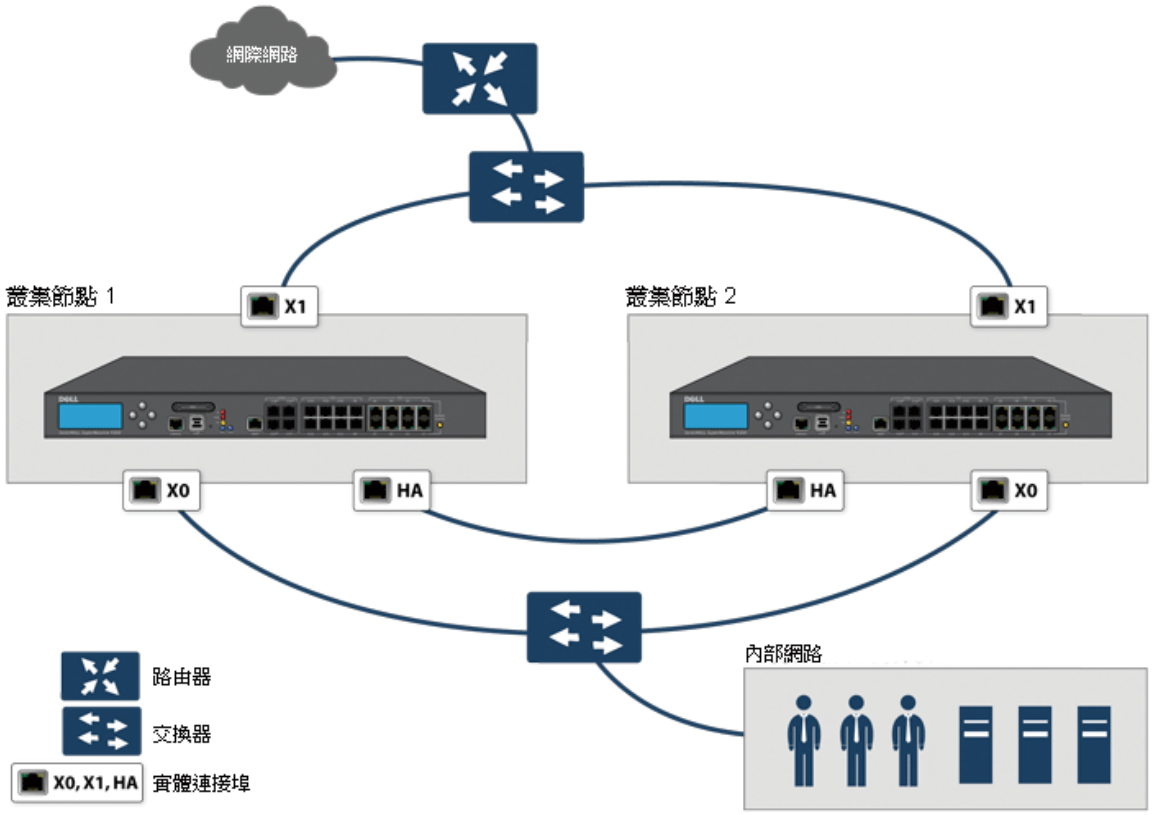


如需實體連接冗餘連接埠和冗餘交換器的更多資訊，請參閱「*主動/主動叢集全網格部署技術說明*」。

範例：主動/主動叢集 - 二裝置部署

主動/主動二裝置叢集顯示了一個二裝置叢集。二裝置叢集不使用 HA 對。每個叢集節點僅包含一台安全設備。兩台安全設備上的指定 HA 連接埠透過交叉網線直接互連。SonicWall 虛擬路由器冗餘通訊協定 (SVRRP) 利用此 HA 連接埠連接傳送叢集節點管理和監視狀態訊息。SVRRP 管理訊息由主節點傳送，監視資訊由叢集中的各安全設備傳送。HA 連接埠連接還用於叢集節點間的設定同步。

主動/主動二裝置叢集



主動/主動叢集的優點

主動/主動叢集擁有如下優點：

- 叢集中的所有安全設備皆用來獲得最大傳送量。
- 可以與主動/主動 DPI 一起執行，以便在各 HA 對的待命安全設備上並行處理 IPS、GAV、防間諜軟體和應用程式規則服務（這些都是處理器需求最為密集的服務），同時在活動安全設備上執行其他處理。
- 支援負載分擔，允許將指定流量指派給叢集中的各節點。
- 叢集中的所有節點都為其他節點提供冗餘，如果某個節點停止工作，其他節點可根據需要處理流量。
- 介面冗餘為流量提供備用處理機制，而無需容錯移轉。
- 支援全網格和非全網格部署。

主動/主動叢集的工作方式

針對主動/主動叢集引入了多個重要概念。

主題：

關於叢集節點

主動/主動叢集由一組叢集節點組成。一個叢集節點可以包含一個可設定狀態 HA 對、一個無狀態 HA 對或單個獨立裝置。僅當叢集節點是一個可設定狀態 HA 對時，才能使用動態狀態同步。傳統 SonicWall 高可用性通訊協定或可設定狀態 HA 協定用於叢集節點內部，即 HA 對的裝置之間的通信。

如果一個叢集節點是一個可設定狀態 HA 對，則可以啟用叢集節點內部的主動/主動 DPI 以提高效能。

關於叢集

叢集中所有安全設備的產品型號必須相同，且執行相同版本的韌體。

在叢集內部，所有安全設備彼此相連和通訊；請參閱主動/主動二節點叢集。叢集節點間的通信使用新的通訊協定，稱為 SonicWall 虛擬路由器冗餘通訊協定 (SVRRP)。叢集節點管理和監視狀態資訊利用 SVRRP 傳送。

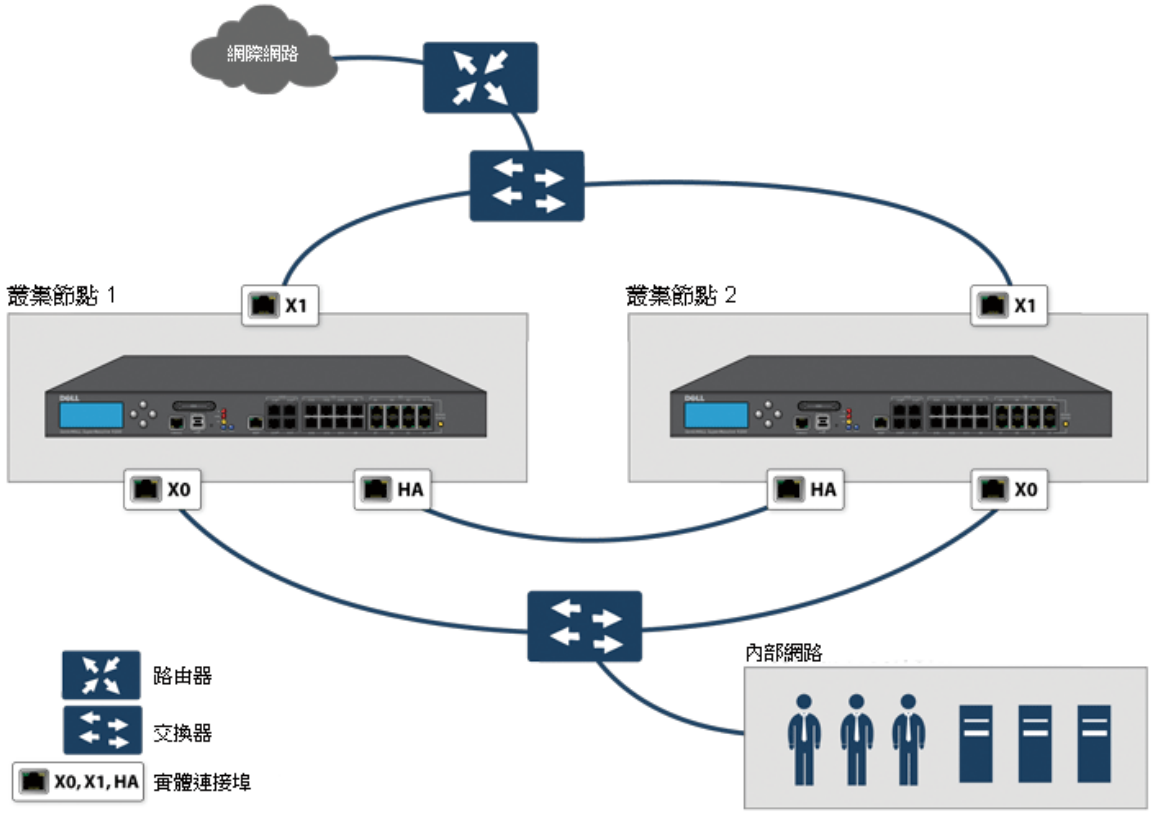
所有叢集節點共用同一設定，由主節點同步。主節點還負責將韌體同步到叢集中的其他節點。HA 連接埠連接用於同步設定和韌體更新。

動態狀態不在叢集節點間同步，僅在叢集節點內同步。當一個叢集節點包含一個 HA 對時，可以在此叢集節點內啟用可設定狀態 HA，以便實現動態狀態同步，並在需要時進行可設定狀態容錯移轉。整個叢集節點發生故障時，容錯移轉將是無狀態式。這意味著，原有的網路連接必須重建。例如，Telnet 和 FTP 工作階段必須重新建立，VPN 通道必須重新交涉。

第 526 頁「關於容錯移轉」提供了有關容錯移轉工作方式的更多資訊。

一個叢集中的叢集節點目前以 4 個為限。如果各叢集節點都是一個 HA 對，則此叢集包括 8 個安全設備。

主動/主動二節點叢集



叢集內允許的操作

允許的管理操作類型取決於叢集中安全設備的狀態。在主節點的活動安全設備上，管理員使用者擁有適當的權限，可以執行所有操作，包括所有設定操作。在非主節點的使用中安全設備上，僅允許執行一部分操作，在處於備用狀態的安全設備上可以執行的操作更少。 允許的管理操作表格列出了非主節點的使用中安全設備和叢集中待命安全設備允許的操作。

允許的管理操作

管理操作	活動非主節點	備用
唯讀操作	已允許	已允許
在 MySonicWall 上註冊	已允許	已允許
與 SonicWall 授權管理員同步授權	已允許	已允許
調查 | 工具 | 系統診斷中的診斷工具 (如需這些工具的資訊，請參閱 **SonicOS 調查**)。	已允許	已允許
封包擷取	已允許	已允許
HA 同步設定（設定同步到節點內的 HA 對等點）	不允許	不允許
HA 同步韌體（韌體同步到節點內的 HA 對等點）	已允許	不允許
管理性登出使用者	已允許	不允許
身分驗證測試（例如測試 LDAP、測試 RADIUS、測試身分驗證代理）	已允許	不允許

關於虛擬群組

主動/主動叢集還支援虛擬群組的概念。目前最多支援 4 個虛擬群組。

虛擬群組是指叢集設定中所有已設定介面的虛擬 IP 位址集合（未使用/未指派的介面沒有虛擬 IP 位址）。首次啟用主動/主動叢集時，此安全設備上的介面的已設定 IP 位址轉譯為虛擬群組 1 的虛擬 IP 位址。因此，虛擬群組 1 包括 X0、X1 以及任何其他已設定且已指派到一個區域的介面的虛擬 IP 位址。

在容錯移轉背景下，也可將虛擬群組看作是流量的邏輯群組，因為根據遇到的故障情況，流量的邏輯群組可以從一個節點容錯移轉到另一個節點。每個虛擬群組都有一個叢集節點充當所有者，另一個或幾個叢集節點充當備用節點。一個虛擬群組在某一時間只能由一個叢集節點所有，此節點成為此虛擬群組相關的所有虛擬 IP 位址的所有者。將虛擬群組 1 的所有者指定為主節點，負責將設定和韌體同步到此叢集中的其他節點。如果虛擬群組中的所有者節點遇到故障，一個備用節點將成為所有者。

作為主動/主動叢集設定的一部分，將叢集中其他安全設備的序號輸入 SonicOS 管理介面，並為各防火牆指派一個等級號碼以用作備用順序。套用主動/主動叢集設定時，還可以建立最多 3 個虛擬群組，對應於增加的其他叢集節點，但不會為這些虛擬群組建立虛擬 IP 位址。您需要在**管理 | 系統安裝 | 網路 | 介面**上設定這些虛擬 IP 位址。

確定虛擬群組所有權（哪個叢集節點擁有哪個虛擬群組）涉及到兩個因素：

- **叢集節點的等級** - 等級在 SonicOS 管理介面中設定，用於指定各節點接管虛擬群組所有權的優先順序。
- **叢集節點的虛擬群組連結權重** - 指虛擬群組中正常工作且設定了虛擬 IP 位址的介面數量。

叢集中設定了兩個以上的叢集節點時，這些因素確定哪個叢集節點最有能力取得虛擬群組的所有權。在包含兩個叢集節點的叢集中，一個節點有故障，另一個節點自然取得所有權。

SVRRP 用於將虛擬群組連結狀態和所有權狀態傳達給叢集中的所有叢集節點。

將虛擬群組 1 的所有者指定為主節點。設定變更和韌體更新只能在主節點上進行，主節點隨後利用 SVRRP 將設定和韌體同步到叢集中的所有其他節點。對於一個指定介面，必須設定虛擬群組 1 的虛擬 IP 位址後，才能設定其他虛擬群組。

負載分擔和多重閘道支援

虛擬群組的流量僅由所有者節點處理。到達某個虛擬群組的封包將留在相同的虛擬群組上的安全設備。在典型設定中，各叢集節點都擁有一個虛擬群組，因而需要處理對應於此虛擬群組的流量。

這種虛擬群組功能支援帶冗餘的多種型號閘道。在含有兩個叢集節點的部署中，X0 虛擬群組 1 IP 位址可以是一個閘道，X0 虛擬群組 2 IP 位址可以是另一個閘道。流量如何指派到各閘道要由網路管理員決定。例如，可以使用智慧 DHCP 伺服器，將閘道指派發佈到直接相連用戶端網路上的 PC，或在下游路由器上使用基於原則的路由。

啟用主動/主動叢集時，SonicOS 內部 DHCP 伺服器關閉，無法啟用。需要 DHCP 伺服器的網路可以使用能夠感知多重閘道的外部 DHCP 伺服器，以便發佈閘道指派。

附註：啟用主動/主動叢集時，SonicOS 內部 DHCP 伺服器關閉。

對相關設定頁面的影響

初次啟用主動/主動叢集時，所有已設定介面的現有 IP 位址轉譯為虛擬群組 1 的虛擬 IP 位址。建立虛擬群組 1 或任何虛擬群組時，會為虛擬 IP 位址建立擁有適當名稱的預設介面物件，例如「虛擬群組 1」或「虛擬群組 2」等。同一介面可以擁有多個虛擬 IP 位址，一個位址對應一個已設定的虛擬群組。您可以在**管理 | 系統安裝 | 網路 | 介面**中檢視這些虛擬 IP 位址。

附註：主動/主動叢集中的所有叢集節點共用同一設定

介面上的每個虛擬 IP 位址都與一個虛擬 MAC 位址相關聯，虛擬 MAC 位址由 Sonic OS 自動產生。虛擬 MAC 位址的格式為 00-17-c5-6a-XX-YY，其中 XX 是介面號，如 03 表示連接埠 X3，YY 是內部群組號，如 00 表示虛擬群組 1，01 表示虛擬群組 2 等。

附註：主動/主動虛擬 MAC 位址不同於高可用性虛擬 MAC 位址。啟用主動/主動叢集時，不支援高可用性虛擬 MAC 位址功能。

對於各虛擬群組的受影響介面物件，會自動建立 NAT 原則。這些 NAT 原則將指定節點的現有 NAT 原則擴充到對應的虛擬介面。您可以在**管理 | 原則 | 規則!** 中檢視這些 NAT 原則 **NAT 原則**。根據需要，可以設定其他 NAT 原則，並將其專門用於某一虛擬群組。如需 NAT 原則的相關資訊，請參閱 *SonicOS 原則*。

啟用主動/主動叢集後，增加 VPN 原則時必須選擇虛擬群組號。

關於 SVRRP

主動/主動叢集中的叢集節點間的通信使用新的通訊協定，稱為 SonicWall 虛擬路由器冗餘通訊協定 (SVRRP)。叢集節點管理和監視狀態訊息是利用 SVRRP 透過主動/主動叢集連結傳送。

SVRRP 還用於將主節點的設定變更、韌體更新和簽章更新同步到叢集中的所有其他節點。在各叢集節點中，僅活動裝置處理 SVRRP 訊息。

如果主動/主動叢集連結發生故障，會在 X0 介面傳送 SVRRP 活動訊號訊息。然而，在主動/主動叢集連結停止工作期間，設定不會同步。韌體或簽章更新、原則變更和其他設定變更無法同步到其他叢集節點，直到修復主動/主動叢集連結。

關於容錯移轉

啟用主動/主動叢集時，可以發生兩類容錯移轉：

高可用性容錯移轉

在一個 HA 對內，次要裝置接管主要裝置的責任。如果此對啟用了可設定狀態 HA，則容錯移轉不會中斷網路連接。

主動/主動容錯移轉

如果一個虛擬群組的所有者節點中的所有裝置都遇到故障，此虛擬群組的備用節點將取得虛擬群組所有權。主動/主動容錯移轉將虛擬群組的所有權從一個叢集節點轉移到另一個叢集節點。成為虛擬群組所有者的叢集節點，還成為此虛擬群組相關的所有虛擬 IP 位址的所有者，並開始使用對應的虛擬 MAC 位址。

主動/主動容錯移轉是無狀態式，意味著網路連接需要重設，VPN 通道需要重新交涉。作為虛擬群組新所有者的叢集節點利用新擁有的虛擬 IP 位址對應的虛擬 MAC 產生 ARP 請求時，2 層廣播將拓撲結構的變化告知網路裝置。這可大大簡化容錯移轉過程，因為僅相連交換器需要更新其學習表格。所有其他網路裝置繼續使用相同的虛擬 MAC 位址，無需更新其 ARP 表，因為未打破虛擬 IP 位址與虛擬 MAC 位址之間的對應關係。

當高可用性容錯移轉和主動/主動容錯移轉均可能時，高可用性容錯移轉優先於主動/主動容錯移轉:

- 高可用性容錯移轉可以是可設定狀態，而主動/主動容錯移轉是無狀態式。
- HA 對中的待命安全設備負載很輕，擁有接管必要處理所需的資源，不過如果啟用了主動/主動 DPI，它可能已經在處理 DPI 流量。此備用叢集節點可能已經在處理數量上與故障裝置相當的流量，容錯移轉後可能會過載。

主動/主動容錯移轉始終以主動/主動先佔模式工作。先佔模式是指，兩個叢集節點發生容錯移轉後，如果虛擬群組的原所有者節點恢復到已驗證的操作狀態，它將從備用節點手中奪取活動角色。如果一個虛擬群組的兩個叢集節點的所有虛擬 IP 介面均正常，且連結權重相同，則原所有者由於等級較高而擁有較高的優先順序。

關於 DPI 和主動/主動叢集

主動/主動 DPI 可以與主動/主動叢集一起使用。主動/主動 DPI 啟用時，它利用 HA 對中的待命安全設備進行 DPI 處理。

為提高主動/主動叢集的效能，推薦啟用主動/主動 DPI，因為它使用 HA 對中的待命安全設備進行深度封包檢查 (DPI) 處理。

關於使用活動/叢集的高可用性監控

主動/主動叢集啟用時，各叢集節點均支援 HA 對的 HA 監控設定。HA 監控功能與以前版本一致。HA 監控可以設定為實體/連結監控和邏輯/探查監控。登入主節點後，需要在**管理 | 系統安裝 | 高可用性 | 監控設定**上，依各個節點增加監控設定。

附註：高可用性 | 監控設定僅適用於您登入的 HA 對，而不是整個叢集。

實體介面監視支援對受監視介面進行連結偵測。連結在實體層偵測以確定其可行性。

實體介面監視啟用時，無論邏輯監控啟用與否，HA 容錯移轉均優先於主動/主動容錯移轉。如果活動裝置上的連結發生故障或連接埠中斷連接，HA 對中的備用裝置將變為活動狀態。

附註：對於已設定虛擬 IP 位址的介面，主動/主動實體監控是隱含的，用於計算虛擬群組連結權重。不能停用這些介面的實體監控。這與 HA 監控不同。

邏輯監控涉及到設定 SonicOS 來監視一個或多個相連網路上的某一可靠裝置。如果 HA 對中的使用中裝置未能定期與此裝置通信，將觸發容錯移轉到備用裝置。如果 HA 對中的任何裝置都不能連接到此裝置，則認為問題出在此裝置上，不會進行容錯移轉。

如果實體監控和邏輯監控均停用，則連結故障或連接埠斷開時將發生主動/主動容錯移轉。

在**管理 | 系統安裝 | 高可用性 | 監控設定**上設定的主要和次要 IP 位址可以在 LAN 或 WAN 介面上設定，以用於多種用途:

- 作為各裝置的獨立管理位址，與裝置的活動或備用狀態無關（所有實體介面均支援）
- 支援備用裝置與 SonicWall 授權伺服器之間的授權同步
- 作為邏輯監控期間發出的探查 ping 的來源 IP 位址

為 HA 對中的各裝置設定監視 IP 位址，就可以獨立登入到各裝置進行管理。注意，將忽略傳送到監視 IP 位址的非管理流量。主要和次要安全設備的唯一 LAN IP 位址不能用作活動閘道；連接到內部 LAN 的所有系統都需要使用虛擬 LAN IP 位址作為其閘道。

附註：僅在 WAN 介面上設定 HA 監控/管理 IP 位址時，需要在所有已設定虛擬 IP 位址的 WAN 介面上進行設定。

次要/備用裝置的管理 IP 位址用於與 SonicWall 授權伺服器進行授權同步，授權伺服器按安全設備（而非按 HA 對）處理授權。即使備用裝置在建立 HA 關聯之前已經在 MySonicWall 上註冊，您必須透過其管理 IP 位址存取次要安全設備，同時使用**管理 | 更新 | 授權**上的連結連接到 SonicWall 伺服器。這樣就可以在備用裝置與 SonicWall 授權伺服器之間同步授權（如主動/主動叢集或可設定狀態 HA 授權）。

使用邏輯監控時，HA 對將從主要和次要 SonicWall ping 指定的邏輯探查 IP 位址目的地。主要 IP 位址或次要 IP 位址欄位中設定的 IP 位址用作 ping 的來源 IP 位址。如果二者均能成功 ping 通目的地，則不會發生容錯移轉。如果二者均無法 ping 到目標，也不會發生容錯移轉，因為這種情況下 SonicWalls 認為問題出在目邀，而非 SonicWalls。但是，如果一個 SonicWall 能夠 ping 到目標，另一個 SonicWall 不能，HA 對將容錯移轉到能夠 ping 到目標的 SonicWall。

管理 | 系統安裝| 高可用性 | 監控設定上的設定任務在主要裝置上進行，然後自動同步到次要裝置。

主動/主動叢集支援的功能。

主題：

注意

啟用主動/主動叢集時，WAN 上僅能使用固定 IP 位址。

主動/主動叢集啟用時不支援下列功能:

- DHCP 伺服器
- L3 透明模式
- L2 橋接 / L2 透明模式
- 動態 DNS
- 有線模式

虛擬群組 1 上不支援下列功能:

- SonicWall GVC
- SonicOS SSL VPN
- IP 協助程式

向後相容性

主動/主動叢集功能不向後相容。從不支援主動/主動叢集的舊版本升級到 SonicOS 時，強烈建議您先停用高可用性，再從執行舊版本 SonicOS 的 HA 對中匯出喜好設定。這樣，升級後匯入喜好設定不會發生衝突。

SonicPoint 相容性

當 SonicWall SonicPoints 或 SonicWaves 與主動/主動叢集一同使用時，有兩點需要考慮:

- SonicPoints 和 SonicWaves 僅與主節點通訊，用於下載韌體和其他方面的操作。
- SonicPoints 和 SonicWaves 需要存取獨立 DCHP 伺服器。SonicPoints 和 SonicWaves 需要 DHCP 伺服器向無線用戶端提供 IP 位址，但啟用主動/主動叢集時，嵌入的 SonicOS DHCP 伺服器會自動停用。

WAN 負載均衡相容性

主動/主動叢集中啟用 WAN 負載均衡 (WLB) 時，叢集中的所有節點使用同一 WLB 介面設定。

WAN 介面故障可能觸發 WLB 容錯移轉、HA 對容錯移轉，或主動/主動容錯移轉到另一叢集節點，具體情況如下:

- 由於 WLB 探查故障，WAN 在邏輯上停止工作 - WLB 容錯移轉
- 實體 WAN 停止工作，但實體監控啟用 - HA 對容錯移轉
- 實體 WAN 停止工作，但實體監控未啟用 -主動/主動容錯移轉

路由拓撲和通訊協定相容性

本節說明主動/主動叢集設定在路由拓撲和路由通訊協定方面的目前局限和特殊要求。

主題：

- 第 529 頁「2 層網橋支援」
- 第 529 頁「OSPF 支援」
- 第 529 頁「RIP 支援」
- 第 529 頁「BGP 支援」
- 第 530 頁「叢集設定中的非對稱路由」

2 層網橋支援

叢集設定不支援 2 層網橋介面。

OSPF 支援

主動/主動叢集支援 OSPF。啟用時，OSPF 在各活動叢集節點支援 OSPF 的介面上執行。從路由角度看，所有叢集節點都是並行路由器，各路由器都有叢集節點介面的虛擬 IP 位址。一般而言，所有其他節點會播發一個節點播發的網路。

各叢集節點的 OSPF 路由 ID 必須是唯一的，並且將從主節點上設定的路由 ID 產生，如下所述：

- 如果使用者在 OSPF 設定中輸入的路由器 ID 為 **0** 或 **0.0.0.0**，則將為各節點的路由器 ID 指派此節點的 X0 虛擬 IP 位址。
- 如果使用者輸入的路由器 ID 為 **0** 或 **0.0.0.0** 之外的值，則將為各節點的路由器 ID 指派一個連續遞增的值。例如，在一個 4 節點叢集中，如果主節點設定的路由 ID 為 `10.0.0.1`，則路由 ID 指派如下：
  - 節點 1：`10.0.0.1`
  - 節點 2：`10.0.0.2`
  - 節點 3：`10.0.0.3`
  - 節點 4：`10.0.0.4`

RIP 支援

支援 RIP，且像 OSPF 一樣，它也在各叢集節點支援 RIP 的介面上執行。從路由角度看，所有叢集節點都是並行路由器，並擁有叢集節點介面的虛擬 IP 位址。一般而言，所有其他節點會播發一個節點播發的網路。

BGP 支援

叢集支援 BGP，它同樣表現為並行 BGP 路由器，使用叢集節點介面的虛擬 IP 位址。與 OSPF 和 RIP 一樣，在主節點上進行的設定變更會套用於所有其他叢集節點。對於 BGP，其設定只能透過 CLI 套用，因此設定將在利用 **`write file`** CLI 命令儲存執行設定時發佈 (請參見 *SonicOS 6.2 CLI 參考指南*)。

叢集設定中的非對稱路由

SonicOS 支援非對稱路由，以供流量流經安全設備上不同的第 2 層橋接對介面，或供流量流經高可用性叢集中的不同安全設備。

主動/主動叢集前提條件

附註：除了本節所述的要求以外，請確保已滿足第 515 頁「使用中/待命和主動/主動 DPI 前提條件」所述的前提條件。

對於主動/主動叢集，還需要附加實體連接：

- **主動/主動叢集連結** - 每個主動/主動叢集連結必須使用至少 100MB 介面，但偏好使用 1GB 介面。

主動/主動叢集設定可以包括設定虛擬群組 ID 和冗餘連接埠。本節提供了執行這兩個任務的程式，詳見第 533 頁「高可用性 | 基本設定」。

主題：

- 第 530 頁「主動/主動叢集的授權要求」
- 第 531 頁「連接主動/主動叢集的 HA 連接埠」
- 第 531 頁「連接冗餘連接埠介面」

主動/主動叢集的授權要求

購買 SonicWall 安全設備時包括的主動/主動叢集授權會顯示在 A/A 叢集的授權要求表格。有些平台需要附加授權才能使用主動/主動叢集功能。SonicOS 擴充授權可透過 MySonicWall 或 SonicWall 分銷商購買。

附註：主動/主動叢集授權必須在各台安全設備上啟用，方法是在 MySonicWall 管理介面的 SonicOS 上註冊裝置，或者將授權金鑰組套用到各裝置（如果網際網路存取無法使用）。

A/A 叢集的授權要求

平台	授權要求[a]
SM 9600	包含
SM 9400	包含
SM 9200	包含
NSA 6600	擴充授權
NSA 5600	擴充授權
NSA 4600	擴充授權
NSA 3600	擴充授權
NSA 2650	N/A
NSA 2600	N/A
TZ600	N/A
TZ500/TZ500 W	N/A
TZ400/TZ400 W	N/A
TZ300/TZ300 W	N/A
SOHO W	N/A

a. N/A = 不適用; 包含 = 包含基本授權

您可以在**管理 | 更新 | 授權**上檢視系統授權。透過此頁面還可以登入 MySonicWall。如需授權相關資訊:

- 一般而言，請參閱 *SonicOS 更新*。
- HA 安全設備，請參閱第 516 頁「在 MySonicWall 上註冊與建立安全設備的關聯」。

如果主動/主動叢集中的安全設備具備網際網路存取，則必須在您登入各台安全設備之個別管理 IP 位址的同時，從 SonicOS 管理介面分別註冊叢集中的各台安全設備。這將使次要裝置可以和 SonicWall 授權伺服器同步，並與關聯的主要安全設備共用授權。

連接主動/主動叢集的 HA 連接埠

對於主動/主動叢集，必須將其中的所有裝置的指定 HA 連接埠實體連接到同一 2 層網路。

SonicWall 推薦將所有指定 HA 連接埠連接到同一 2 層交換器。可以使用專用交換器，或使用內部網路中的現有交換器上的某些連接埠。所有這些交換器連接埠都必須設定為允許 2 層流量在其間自由通行。

如果是雙裝置主動/主動叢集部署，各叢集節點僅有一台安全設備，可以使用交叉網線直接連通 HA 連接埠。這種情況下無需交換器。

SonicWall 虛擬路由器冗餘通訊協定 (SVRRP) 利用此 HA 連接埠連接傳送叢集節點管理和監視狀態訊息。SVRRP 管理訊息由主節點傳送，監視資訊由叢集中的各安全設備傳送。

HA 連接埠連接還用於將主節點的設定同步到部署中的其他叢集節點。這包括韌體或簽章升級、VPN 和 NAT 的政策以及其他設定。

連接冗餘連接埠介面

可以將一個未使用的實體介面作為冗餘連接埠指派給一個已設定的實體介面（稱為主要介面）。在各叢集節點上，各主要和冗餘連接埠對必須實體連接到同一交換器，最好是連接到網路中的冗餘交換器。

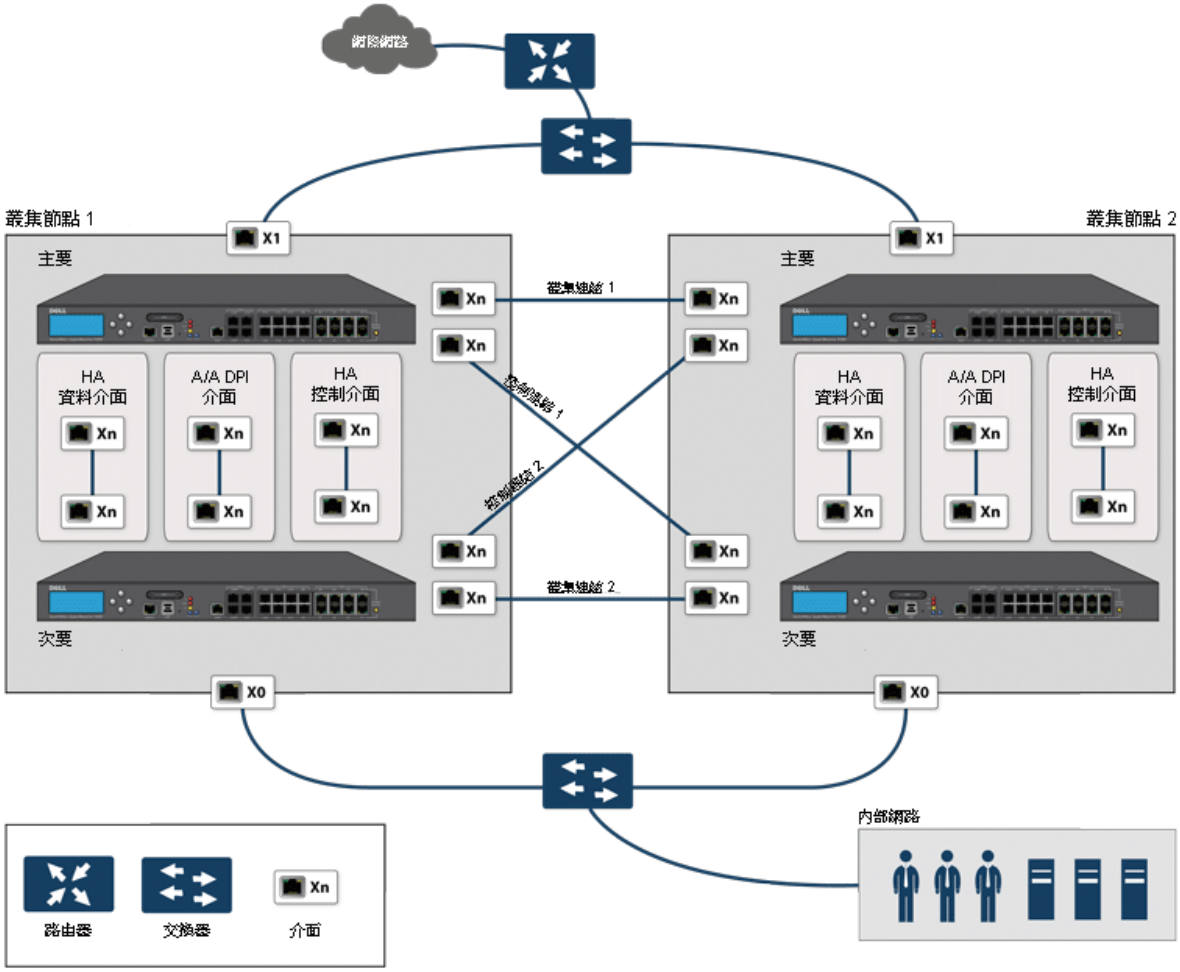
附註：由於所有叢集節點共用同一設定，因此各節點必須設定相同的冗餘連接埠並將其連接到相同的交換器。

若要使用主動/主動叢集，必須在 MySonicWall 上註冊叢集中的所有 SonicWall 安全設備。*各* HA 對中的兩台安全設備也必須在 MySonicWall 上關聯為 HA 主要和 HA 次要安全設備。也就是說，先關聯叢集節點 1 之 HA 對中的兩台安全設備，再關聯叢集節點 2 之 HA 對中的兩台安全設備，其他叢集節點依此類推。

主動/主動 DPI 叢集高可用性

主動/主動 DPI 叢集高可用性支援設定最多 4 個 HA 叢集節點用於容錯移轉和負載分擔，這些節點對網路流量的深度封包檢查 (DPI) 安全服務進行應用程式負載均衡。請參閱主動/主動 DPI 叢集高可用性。

主動/主動 DPI 叢集高可用性



對於叢集連結和控制連結，叢集節點 1 中的各裝置連接到對等節點（叢集節點 2）中的各裝置。最佳做法是在各節點的各裝置中使用同一組介面。(例如，將一台裝置中的 X8 連接到對等裝置中的 X8，對 X9、X10 等也這樣做。)但是，對連接埠使用並無任何限制。

34

設定高可用性

重要：高可用性不能和 PortShield 一起使用，SonicWall X-系列解決方案除外。在設定高可用性之前，從**管理 | 系統安裝 | 網路 | PortShield 群組**移除任何現有的 PortShield 設定。如需將 HA 與 PortShield 搭配使用的資訊，請參閱第 297 頁「SonicOS 支援 X- 系列交換器」與 *SonicWall X-系列解決方案部署指南*。

高可用性 | 基本設定

您可以在**管理 | 系統安裝 | 高可用性 | 基本設定**上設定高可用性 (HA):

- 第 534 頁「設定使用中/待命高可用性設定」
- 第 535 頁「使用動態 WAN 介面設定 HA」
- 第 537 頁「設定主動/主動 DPI 高可用性設定」

附註：如需高可用性的更多資訊，請參閱第 508 頁「關於高可用性」和第 515 頁「使用中/待命和主動/主動 DPI 前提條件」。如果主動/主動叢集環境使用 VPN 或 NAT，則請在完成主動/主動設定之後參閱第 545 頁「設定主動/主動叢集的 VPN 和 NAT」。

除非為 X0 或任何 WAN 介面設定 HA 監控 IP 位址，否則授權與特徵更新在待命安全設備上不會產生作用。如果未設定這些介面，則會顯示訊息:

設定使用中/待命高可用性設定

高可用性 | 基本設定上的設定任務是在主要防火牆上進行，然後自動同步到次要防火牆。

若要設定使用中/待命：

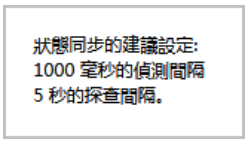
1 導覽到**系統安裝 | 高可用性 | 基本設定**。

2 從**模式**中，選取**使用中/待命**。

3 選擇**啟用狀態同步**。預設情況下未勾選此選項。

狀態高可用性為啟用時，主要與次要防火牆之間不會同步工作階段狀態。如果發生容錯移轉，任何在容錯移轉時已處於使用中狀態的工作階段都需要重新交涉。

顯示建議訊息。



4 按一下**確定**。

5 如需要在升級韌體版本時備份設定，請勾選**升級韌體時產生 / 覆寫備份韌體和設定**。預設情況下未勾選此選項。

6 若要設定高可用性對，使得主要防火牆在失效重新啟動後立即恢復主要角色，請選擇**啟用先佔模式**。預設情況下未勾選此選項。

> **提示：**啟用「可設定狀態高可用性」時，建議停用先佔模式，因為先佔模式對容錯移轉到次要防火牆可能過度積極。

7 選取**啟用虛擬 MAC** ，以允許主要和次要防火牆共用一個 MAC 位址。這可以在發生容錯移轉時，大大簡化網路 ARP 表和快取的更新過程。預設情況下未勾選此選項。

> **重要：**如果已設定 PPPoE 未編號，則必須選擇**啟用虛擬 MAC**。

只需要通知這兩台防火牆與之相連的交換器。所有外圍裝置將繼續路由到此單一共用 MAC 位址。

8 按一下 **HA 裝置** ，以設定次要防火牆序號。主要裝置的序號隨即顯示，但欄位會顯示為灰色，無法進行編輯。

9 輸入**備份裝置**的**序號**。

10 按一下 **HA 介面**。

11 選擇用作 **HA 控制介面**的介面。如果防火牆偵測到已設定此介面，此選項將以灰色顯示並且顯示介面。

12 選擇用作**主動/主動 DPI 介面**的介面。如果防火牆偵測到已設定此介面，此選項將以灰色顯示並且顯示介面。

13 完成所有高可用性設定後，按一下**接受**。所有設定將同步到次要防火牆，次要防火牆將重新啟動。

使用動態 WAN 介面設定 HA

高可用性 | 基本設定上的設定任務是在主要防火牆上進行，然後自動同步到次要防火牆。

若要使用動態 WAN 介面設定 HA：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 如第 249 頁「設定 WAN 介面」中所述，設定 WAN 介面為 PPPoE。

3 導覽到**高可用性 | 基本設定**。

4 從**模式**中選取 HA 模式。如果已選擇**主動/主動 DPI** 或**主動/主動叢集**，則會顯示關於授權和特徵更新的訊息。

> 只有當 X0 或任何一個 WAN 介面設定了 HA 監控 IP 後，待命防火牆上的授權和簽章才會更新。

5 按一下**確定**。

6 確保未選取**啟用狀態同步**。 預設情況下未勾選此選項。

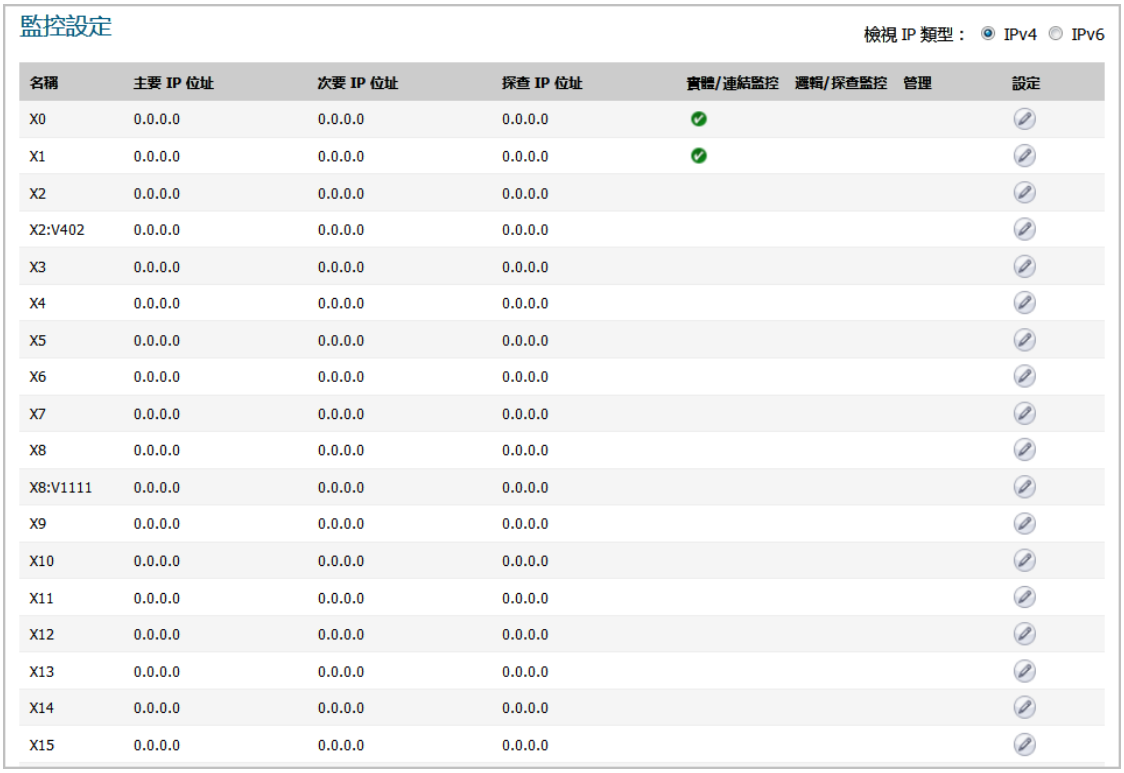
7 確保未選取**啟用先佔模式**。 預設情況下未勾選此選項。

8 選擇**啟用虛擬 MAC**。預設情況下未勾選此選項。

9 設定 **HA 裝置**和 **HA 介面**選項，如第 534 頁「設定使用中/待命高可用性設定」中所述。

10 按一下**套用**。

11 導覽到**高可用性 | 監控設定**。



名稱	主要 IP 位址	次要 IP 位址	探查 IP 位址	實體/連結監控	邏輯/探查監控	管理	設定
X0	0.0.0.0	0.0.0.0	0.0.0.0	✔			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✔			
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0				
X4	0.0.0.0	0.0.0.0	0.0.0.0				
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X6	0.0.0.0	0.0.0.0	0.0.0.0				
X7	0.0.0.0	0.0.0.0	0.0.0.0				
X8	0.0.0.0	0.0.0.0	0.0.0.0				
X8:V1111	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X10	0.0.0.0	0.0.0.0	0.0.0.0				
X11	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				

12 按一下 PPPoE 介面的**設定**圖示。將顯示**編輯 HA 監控**對話方塊。

13 選擇**啟用實體/連接監控**核取方塊。預設情況下未勾選此選項。

14 確保**主要 IPv4 位址**和**次要 IPv4 位址**設定為 0.0.0.0。

15 確保未選取其他選項。

16 按一下**確定**。

設定主動/主動 DPI 高可用性設定

管理 | 系統安裝| 高可用性 | 基本設定上的設定任務是在主要防火牆上進行，然後自動同步到次要防火牆。

若要設定主動/主動 DPI：

1 導覽到**高可用性 | 基本設定**。

2 在**模式**下拉功能表中，選擇**主動/主動 DPI**。關於授權與特徵更新的訊息隨即顯示。

3 按一下**確定**。

主動/主動 DPI 的**啟用狀態同步**選項會自動啟用，此選項以灰色顯示。

4 如需要在升級韌體版本時備份設定，請勾選**升級韌體時產生 / 覆寫備份韌體和設定**。預設情況下未勾選此選項。

5 一般情況下，應停用主動/主動 DPI 的先佔模式。確保未選取**啟用先佔模式**。預設情況下未勾選此選項。

附註：此選項要求主要防火牆在失效重新啟動後立即恢復主要角色，因此僅適用於使用中/待命設定。

6 若要允許 HA 對中的兩個安全設備共用一個 MAC 位址，請選取**啟用虛擬 MAC**。此選項可以在發生容錯移轉時，大幅簡化網路 ARP 表格和快取的更新過程。只需要通知這兩個安全設備與之相連的交換器。所有外圍裝置將繼續路由到此單一共用 MAC 位址。預設情況下未勾選此選項。

7 按一下 **HA 裝置**標籤。主要裝置的序號會顯示，而欄位顯示為灰色，無法進行編輯。

8 輸入**備份裝置**的**序號**。

9 按一下 **HA 介面**。

10 從 **HA 控制介面**選取 HA 控制介面。如果安全設備偵測到已設定此介面，此選項將以灰色顯示並且顯示介面。

11 選擇 **HA 資料介面**的介面號。如果安全設備偵測到已設定此介面，此選項將以灰色顯示並且顯示介面。

12 選擇用作**主動/主動 DPI 介面**的介面號。如果安全設備偵測到已設定此介面，此選項將以灰色顯示並且顯示介面。

在主動/主動 DPI 處理期間，此介面用於在這兩個安全設備之間傳送資料。下拉功能表中僅出現未指派的可用介面。兩個安全設備上的相連介面必須是同一號碼，而且最初必須在**管理 | 網路 | 介面**中顯示為未使用、未指派的介面。例如，如果 X5 是未指派介面，則可以將主要裝置的 X5 連接到次要裝置的 X5。啟用主動/主動 DPI 後，連接的介面將具有 **HA 資料-連結**的**區域**指派。

13 完成所有高可用性設定後，按一下**接受**。所有設定將同步到待命安全設備，而且待命安全設備會重新啟動。

設定主動/主動叢集

主題：

- 第 539 頁「設定主動/主動叢集高可用性」
- 第 540 頁「設定主動/主動叢集高可用性監控」
- 第 542 頁「設定主動/主動 DPI 叢集高可用性」
- 第 545 頁「設定主動/主動叢集的 VPN 和 NAT」

設定主動/主動叢集高可用性

主動/主動叢集高可用性支援設定最多 4 個 HA 叢集節點用於容錯移轉和負載分擔。每個節點可包含一個安全設備或一個 HA 對。

設定主動/主動叢集高可用性的步驟如下：

1 登入到主叢集節點的主要裝置。

2 導覽到**管理 | 系統安裝 | 高可用性 | 基本設定**。

3 在**模式**下拉功能表中，選擇主動/主動**叢集**。 關於授權與特徵更新的訊息隨即顯示。

4 按一下**確定**。**HA 裝置變更為 HA 裝置與節點**。

5 選擇**啟用狀態同步**。

6 若要在上傳新韌體至安全設備時，自動備份韌體與組態設定，請選取**升級韌體時產生 / 覆寫備份韌體與設定**。當主節點將新安全設備同步至叢集中的其他安全設備時，會在這些安全設備上建立次要裝置。

7 若要設定主動/主動叢集資訊，請按一下 **HA 裝置與節點**。

8 在**叢集節點**表格中，在相應的**主要裝置序號**與**次要裝置序號**欄位中，輸入每個叢集節點中安全設備的序號。

9 從**虛擬群組*與*級別**下拉功能表中，選取叢集節點 1 針對各虛擬群組擁有的等級。預設情況下，叢集節點 1 是群組 1 的**所有者**，而且通常列為其他群組的**待命**節點。

若要從叢集中排除安全設備，則**虛擬群組*與*級別**請選取**無**。

10 在第二行，從**虛擬群組*與*級別**下拉功能表中，選取叢集節點 2 針對各虛擬群組擁有的等級。

11 按一下 **HA 介面**。

12 從 **HA 控制介面**選取 HA 控制介面。如果安全設備偵測到已設定此介面，此選項將以灰色顯示並且顯示介面。

13 選取**啟用切換式主動/主動叢集連結**。這些選項將發生變更。

14 從**主動/主動叢集連結**，選取在主動/主動處理期間，用於這兩個裝置之間傳送資料的介面。只會列出未指派的可用介面。

15 如果您選取**啟用切換式主動/主動叢集連結**，請移至步驟 17。

16 從**主動/主動叢集連結 2**，選取在主動/主動處理期間，用於這兩個裝置之間傳送資料的介面。只會列出未指派的可用介面。

17 按一下**套用**。所有設定將同步到備用裝置，備用裝置將重新啟動。

18 移至**高可用性 | 監控設定**，並依照第 540 頁「設定主動/主動叢集高可用性監控」中的步驟。

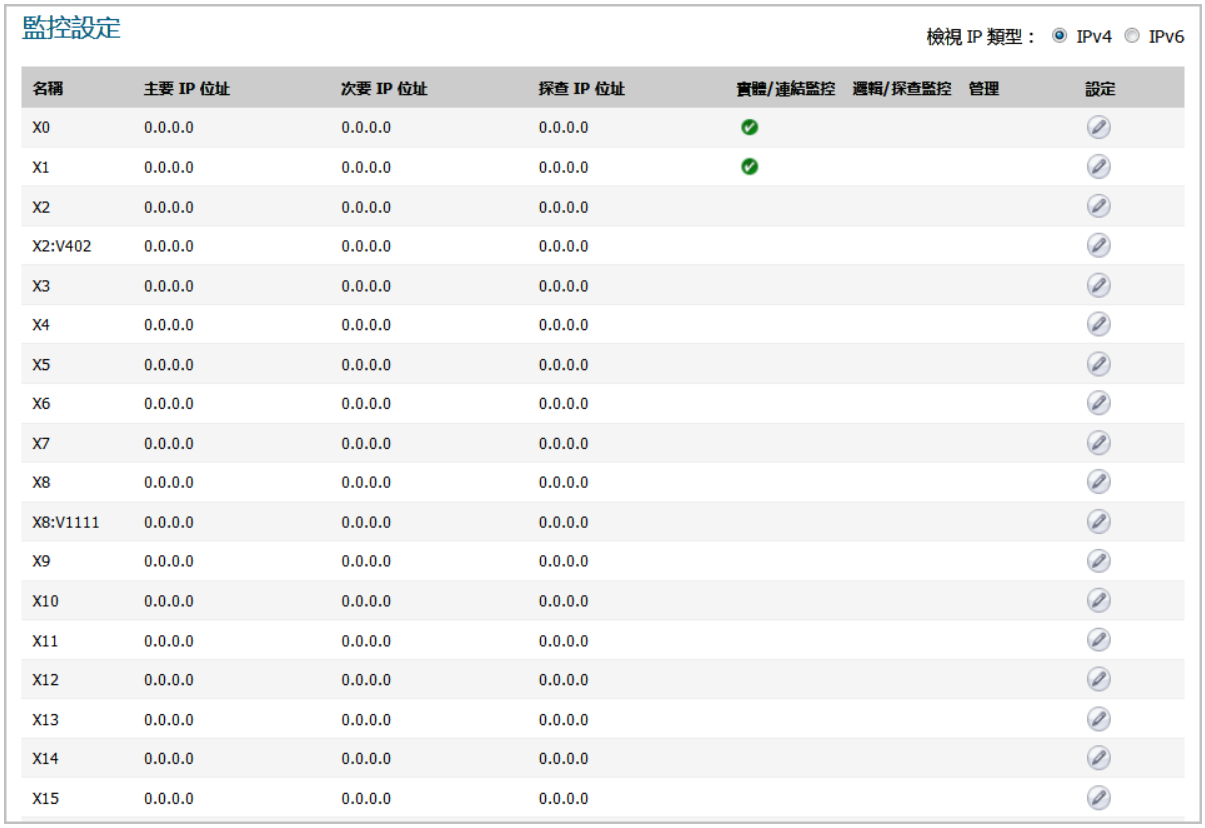
19 移至**高可用性 | 進階設定**，並依照第 555 頁「高可用性 | 進階設定」中的步驟。

20 移至**管理 | 系統安裝 | 網路 | 介面**頁面，驗證您已成功設定所需的主動/主動介面。

21 移至**高可用性 | 監控設定**，驗證主動/主動叢集的設定。

設定主動/主動叢集高可用性監控

高可用性 | 監控設定上的設定任務是在主要裝置上進行，然後自動同步到次要裝置。這些設定僅影響頁面頂部選擇的叢集節點中的 HA 對。



若要設定獨立的 LAN 管理 IP 位址以及設定實體和/或邏輯介面監視：

1 在主節點上以管理員身分登入到 SonicOS 管理介面。

2 導覽到**管理 | 系統安裝 | 高可用性 | 監控設定**。

3 在頁面右上側，從下拉功能表中選擇要設定的**節點**。

4 按一下 LAN 上某個介面的**設定**圖示，例如 X0。

5 若要啟用主要和次要裝置上的指定 HA 介面之間的連結偵測，請勾選**啟用實體/連結監控**核取方塊。

6 在**主要 IP 位址**欄位，輸入主要裝置的唯一 LAN 管理 IP 位址。

7 在**備份 IP 位址**欄位，輸入次要裝置的唯一 LAN 管理 IP 位址。

8 勾選**允許管理主要/次要 IP 位址**的核取方塊。為某個介面啟用此選項時，在**管理 | 系統安裝 | 高可用性 | 監控設定**的**監控設定**表格中，此介面的**管理**欄中會出現一個綠色圖示。只能對啟用此選項的介面執行管理。

9 在**邏輯探查 IP 位址**欄位，輸入應監視其連接的 LAN 網路上某個下游裝置的 IP 位址。這通常是一個下游路由器或伺服器。（如果需要在 WAN 端進行探查，應使用上游裝置）。主要和次要防火牆將定期 ping 此探查 IP 位址。如果二者均能成功 ping 通目的地，則不會發生容錯移轉。如果二者均無法成功 ping 通目的地，也不會發生容錯移轉，因為這種情況下它會認為問題出在目的地，而非防火牆。但是，如果一台防火牆能夠 ping 到目標，另一台不能，則會容錯移轉到能夠 ping 到目標的防火牆。

主要 IP 位址和**備份 IP 位址**欄位必須用 LAN 介面（如 X0）或 WAN 介面（如 X1，用於探查 WAN）上的獨立 IP 位址設定，以便對功能是否正常進行邏輯探查。

10 按一下**確定**。

11 若要設定任何其他介面的監視，請重複上述步驟。

12 完成選定叢集節點的所有高可用性監控設定後，按一下**套用**。

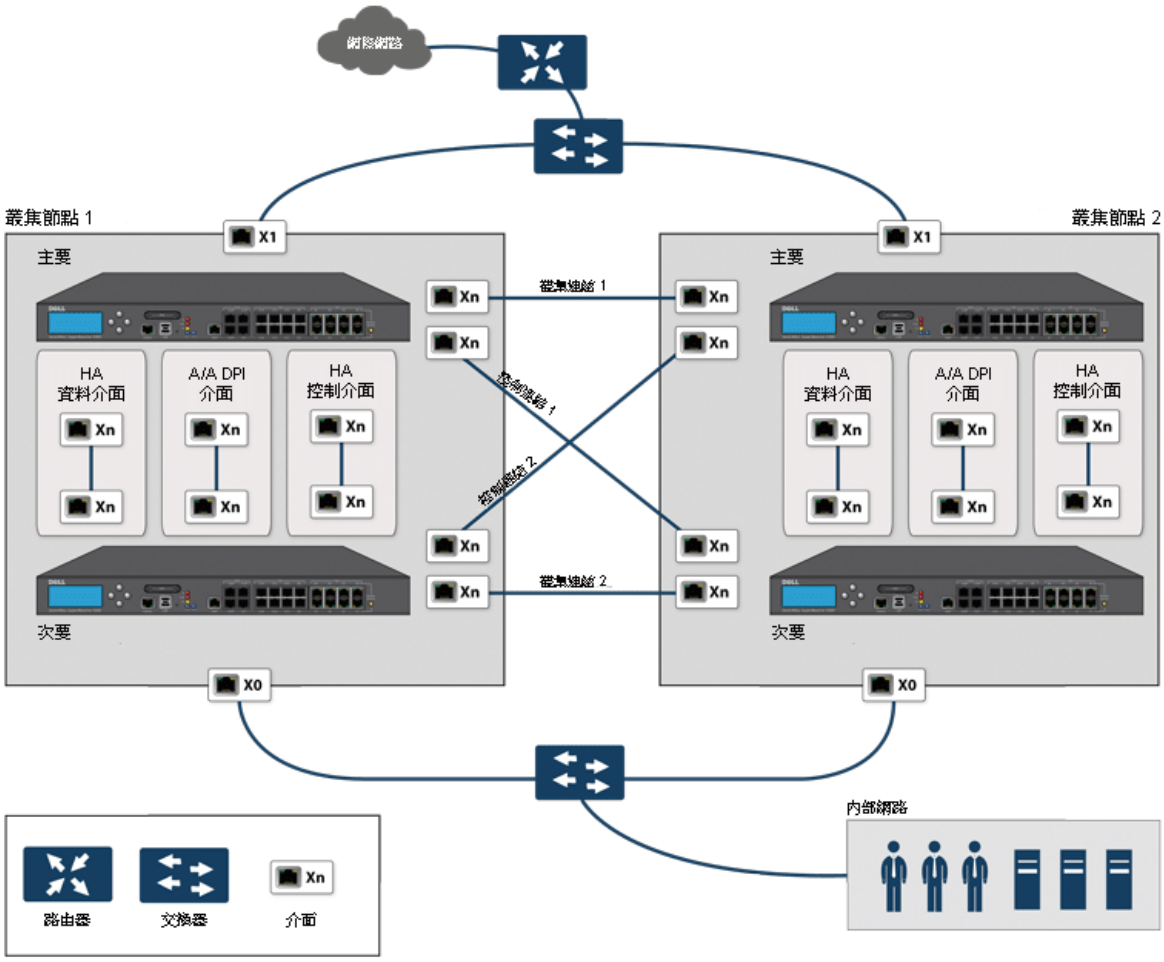
13 也可選擇其他叢集節點，重複上述設定步驟，按一下**套用**。

如需驗證設定的其他資訊，請參閱第 545 頁「驗證主動/主動叢集設定」。

設定主動/主動 DPI 叢集高可用性

主動/主動 DPI 叢集高可用性支援設定最多 4 個 HA 叢集節點用於容錯移轉和負載分擔，這些節點對網路流量的深度封包檢查 (DPI) 安全服務進行應用程式負載均衡。請參閱主動/主動 DPI 叢集高可用性。

主動/主動 DPI 叢集高可用性



對於叢集連結和控制連結，叢集節點 1 中的各裝置連接到對等節點（叢集節點 2）中的各裝置。最佳做法是在各節點的各裝置中使用同一組介面。(例如，將一台裝置中的 X8 連接到對等裝置中的 X8，對 X9、X10 等也這樣做。)但是，對連接埠使用並無任何限制。

設定主動/主動 DPI 叢集高可用性的步驟如下：

附註：如果您已按照第 516 頁「實體連接您的安全設備」所述實體連接主動/主動 DPI 介面，就可以在 SonicOS 管理介面中設定主動/主動 DPI。

1 登入到主叢集節點的主要裝置。

2 導覽到**管理 | 系統安裝 | 高可用性 | 基本設定**。

3 從**模式**中，選取**主動/主動 DPI 叢集**。

4 主動/主動 DPI 叢集的**啟用狀態同步**選項會自動啟用。

5 選取**升級韌體時產生 / 重寫備份韌體和設定**，以便在上傳新韌體至安全設備時，自動建立韌體和設定的備份。當主節點將新韌體同步到叢集中的其他安全設備時，就會在這些安全設備上建立備份。

6 按一下 **HA 裝置**，設定主動/主動叢集資訊。

7 對於標籤頂部的 **HA 備用裝置**選項，

- 如果設定的次要安全設備是此安全設備所屬叢集節點的一部分，請選取**內部**。
- 如果設定的次要安全設備是其他叢集節點的一部分，請選取**外部**。

8 在表格中，輸入各叢集節點之安全設備的序號。

> **提示：**主要裝置的序號可能已填入並顯示為灰色。

9 在序號右邊的**虛擬群組 *X* 級別**欄位中輸入叢集節點 1 針對各虛擬群組的等級。預設情況下，叢集節點 1 是群組 1 的**所有者**，通常將其確定為群組 2 的**備用**節點。若要從一個叢集中排除一台防火牆，其**虛擬群組 *X* 級別**請選擇**無**。

10 在第二行，在序號右邊的**虛擬群組 *X* 級別**欄位中輸入叢集節點 2 針對各虛擬群組的等級。

11 按一下 **HA 介面**標籤。選擇用作 **HA 控制介面**的介面。如果安全設備偵測到已設定此介面，此選項將以灰色顯示。

12 選擇用作**主動/主動 DPI 介面**的介面。如果安全設備偵測到已設定此介面，此選項將以灰色顯示。

13 選擇**主動/主動 DPI 介面**。在主動/主動 DPI 處理期間，此介面用於在這兩台裝置之間傳送資料。下拉功能表中僅出現未指派的可用介面。

14 選擇**主動/主動叢集連結**介面。

15 完成所有高可用性設定後，按一下**接受**。所有設定將同步到備用裝置，備用裝置將重新啟動。

16 移至**管理 | 系統安裝 | 高可用性 | 監控設定**，並依照第 540 頁「設定主動/主動叢集高可用性監控」中的步驟。

17 移至**管理 | 系統安裝 | 高可用性 | 進階設定**，並依照第 555 頁「微調高可用性」中的步驟。

18 移至**管理 | 系統安裝 | 網路 | 介面**，驗證您已成功設定所需的主動/主動介面。

19 移至**監控 | 目前狀態 | 高可用性狀態**，驗證主動/主動叢集的設定。如需關於**高可用性狀態**的資訊，請參閱 *SonicOS 監控*。

設定主動/主動叢集的 VPN 和 NAT

在主動/主動叢集環境下設定下列功能時，有一些額外事項需要考慮：

- 第 545 頁「設定主動/主動叢集的 VPN」
- 第 545 頁「設定主動/主動叢集的 NAT 原則」

設定主動/主動叢集的 VPN

在主動/主動叢集模式下執行時，VPN 原則設定需要關聯一個虛擬群組。您可以在**管理 | 連線 | VPN | 基本設定**上設定用於建立此關聯的選項。如需設定 VPN 原則的相關資訊，請參閱 *SonicOS 連線*。

群組位址物件可用於本機網路。這些虛擬群組位址物件是在新增虛擬 IP 位址時由 SonicOS 建立，刪除虛擬 IP 時也會將其刪除。為遠端網路建立 VPN 原則時，虛擬群組位址物件也可供使用。例如，自訂名稱 **Active-Active-Lan-Host-1**。

設定主動/主動叢集的 NAT 原則

在主動/主動叢集模式下執行時，NAT 原則設定包括虛擬群組設定。預設 NAT 原則是在新增虛擬 IP 位址時由 SonicOS 建立，刪除虛擬 IP 時也會將其刪除。建立自訂 NAT 原則時，您可以指定虛擬群組；例如，在介面 X1 上為虛擬群組 2 自動建立的 NAT 原則。如需建立 NAT 原則的相關資訊，請參閱 *SonicOS 原則*。

驗證主動/主動叢集設定

本節介紹幾種驗證主動/主動叢集和主動/主動 DPI 設定是否正確的方法。參見以下章節：

- 第 545 頁「比較叢集中的防火牆的 CPU 活動」
- 第 546 頁「驗證監控 | 目前狀態 | 高可用性狀態中的設定」
- 第 546 頁「TSR 中的其他參數」
- 第 546 頁「對 DPI 符合的回應」
- 第 546 頁「記錄」

比較叢集中的防火牆的 CPU 活動

可設定狀態 HA 對啟用主動/主動 DPI 後，可以觀察到 HA 對中的安全設備的 CPU 利用率發生變化。活動裝置的 CPU 活動減少，備用裝置的 CPU 活動增多。

可以在「多核心監控」上檢視 CPU 利用率。在主節點的使用中安全設備上，移至**監控 | 裝置執行狀況 | 即時監控**，並捲動至多核心監控，以顯示主動/主動叢集中所有安全設備的活動。如需多核心監控的相關資訊，請參閱 *SonicOS 監控*。

在「多核心監控」上檢視叢集中的使用中裝置時，叢集中的所有安全設備都會顯示。但是，如果登入的是叢集中備用裝置的獨立 IP 位址，則「多核心監控」頁面僅顯示此指定 HA 對中兩個安全設備的核心使用情況。

附註：若要查看叢集中所有安全設備的核心使用情況，SonicWall 建議在主節點的使用中裝置上檢視「多核心監控」。

驗證監控 | 目前狀態 | 高可用性狀態中的設定

在**主動/主動叢集節點狀態**表格中，**監控 | 目前狀態 | 高可用性狀態**提供部署中整個主動/主動叢集的狀態和各叢集節點的狀態。如需檢視 HA 狀態的相關資訊，請參閱 *SonicOS 監控*。

TSR 中的其他參數

您可以在**調查 | 工具 | 系統診斷**上產生「技術支援報告」，從而判斷可設定狀態 HA 對的主動/主動 DPI 設定是否正確。「技術支援報告」中應出現下列設定參數並顯示正確的值:

- 啟用主動/主動 DPI
- 主動/主動 DPI 介面設定

如需產生 TSR 的相關資訊，請參閱 *SonicOS 調查*。

產生用於此目的 TSR 的步驟如下：

1 使用共用 IP 位址登入到可設定狀態 HA 對。

2 導覽至**調查 | 工具 | 系統診斷**。

3 在**技術支援報告**下，按一下**下載報告**。

對 DPI 符合的回應

網路流量中找到 DPI 符合時，回應或操作始終從執行主動/主動 DPI 的可設定狀態 HA 對的活動裝置發出。

附註：這並不表示所有處理都是在活動裝置上進行。

深度封包檢查發現與 IPS 簽章、病毒附件、應用程式規則原則和其他惡意軟體符合的網路流量。發現符合時，SonicOS 執行丟棄封包或重設 TCP 連接等操作。

某些 DPI 符合操作會將附加 TCP 封包注入現有流中。例如，當一個 SMTP 工作階段攜帶一個病毒附件時，SonicOS 會向 SMTP 用戶端傳送一個 n552 錯誤回應代碼，並附帶一條訊息：電子郵件附件包含病毒。錯誤回應代碼傳送後，TCP 重設，連接終止。

這些附加 TCP 封包是待命安全設備上的 DPI 處理的結果。產生的封包透過主動/主動 DPI 介面傳送至使用中安全設備，並從使用中安全設備發出，彷彿處理作業是發生在使用中的安全設備上。這可確保無縫操作，似乎 DPI 處理是在活動安全設備上完成。

記錄

如果啟用了主動/主動 DPI，並且待命安全設備上的 DPI 處理產生上述 DPI 符合操作，則將此操作記錄在可設定狀態 HA 對的活動裝置上，而非偵測到符合的備用裝置上。這並不表示所有處理都是在活動裝置上進行。

高可用性相關的記錄事件可以在**調查 | 工具 | 記錄 | 事件記錄**中檢視。如需記錄的相關資訊，請參閱 *SonicOS 調查*。

IPv6 高可用性監控

如需 SonicOS 的 IPv6 實作的完整資訊，請參見第 761 頁「IPv6」。

IPv6 高可用性 (HA) 監視作為 IPv4 中 HA 監控的擴充程式實作。在設定 IPv6 的 HA 監控後，可以從 IPv6 監視位址管理主要和備份安全設備，且 IPv6 探查可以偵測 HA 對的網路狀態。

為了輕鬆設定兩個 IP 版本，您可以在**管理 | 系統安裝 | 高可用性 | 監控設定**中顯示的 IPv6 和 IPv4 之間切換。

IPv6 HA 監控設定頁面繼承自 IPv4，所以設定程式幾乎完全相同。只需選取 IPv6 並參閱第 508 頁「關於高可用性」和第 547 頁「IPv6 HA 監控考慮事項」，以瞭解設定詳細資料。

IPv6 HA 監控考慮事項

在設定 IPv6 HA 監控時請考慮以下因素：

- 在**編輯 HA 監控**對話方塊中，**啟用實體/連結監控**和**覆寫虛擬 MAC** 顯示為灰色，因為它們是第 2 層屬性。也就是說，IPv4 和 IPv6 使用這些屬性，所以必須在 IPv4 監視頁面進行設定。
- 主要/備份 IPv6 位址必須在介面的相同子網路中，且不能與主要/備份安全設備的全域 IP 和連結本機 IP 相同。
- 如果將主要/備用監視 IP 設為（非 **::**），就不能是相同的。
- 如果已啟用**允許管理主要/次要 IPv6 位址**，則主要/備用監控 IPv6 位址不能為未指定 (即 **::**)。
- 如果已啟用**邏輯/探查 IPv6 位址**，則探查 IP 不能為未指定。

設定網路 DHCP 和介面設定

啟用主動/主動叢集時，SonicOS 內部 DHCP 伺服器關閉，無法啟用。需要 DHCP 伺服器的網路可以使用外部 DHCP 伺服器。啟用主動/主動叢集之前，應在管理介面上停用 SonicOS DHCP 伺服器，並刪除所有 DHCP 伺服器租用範圍。

在**管理 | 系統安裝 | 網路 | 介面**上，可以為虛擬群組中的介面設定其他虛擬 IP 位址，以及為這些介面設定冗餘連接埠。

如需執行這些任務的資訊，請參見：

- 第 547 頁「停用 SonicOS DHCP 伺服器」
- 第 548 頁「設定虛擬 IP 位址」
- 第 548 頁「設定冗餘連接埠」

停用 SonicOS DHCP 伺服器

若要停用 SonicOS DHCP 伺服器並刪除所有 DHCP 伺服器租用範圍：

1. 登入叢集節點的主要裝置，並導覽至**管理 | 系統安裝 | 網路 | DHCP 伺服器**。
2. 選擇 IP 版本: **IPv4** 或 **IPv6**。
3. 清除**啟用 DHCPv4/6 伺服器**。
4. 在 **DHCPv4/6 伺服器租用範圍**下，為**檢視樣式**選取**全部**，以選取表格中的所有租用範圍。
5. 按一下**全部刪除**按鈕。
6. 按一下確認對話方塊中的**確定**。
7. 按一下**接受**。

設定虛擬 IP 位址

首次啟用主動/主動叢集時，此安全設備上的介面的已設定 IP 位址自動轉換為虛擬群組 1 的虛擬 IP 位址。因此，虛擬群組 1 包括 X0、X1 以及任何其他已設定且已指派到一個區域的介面的虛擬 IP 位址。

主動/主動叢集要求為其他虛擬群組設定其他虛擬 IP 位址。各介面指派多個虛擬 IP 位址，一個位址對應一個虛擬群組。各附加虛擬 IP 位址均與叢集中的另一虛擬群組相關聯。各介面最多可以擁有 4 個虛擬 IP 位址。VLAN 介面也可以擁有最多 4 個虛擬 IP 位址。

附註：對於處理某一流量的虛擬群組，如果其介面沒有設定相應的虛擬 IP 位址，則無法轉送此流量的封包。

在一個介面上設定虛擬 IP 位址的步驟如下：

1 登入到叢集節點的主要裝置。

2 導覽到**管理 | 系統安裝 | 網路 | 介面**。

3 在**介面**設定表中，按一下想要設定的介面的**設定**圖示。

4 在**編輯介面**對話中，將虛擬 IP 位址輸入 **IP 位址（虛擬群組 X）**欄位中，其中 *X* 是虛擬群組號。

附註：新的虛擬 IP 位址與此介面的現有虛擬 IP 位址必須處於同一子網路。

5 按一下**確定**。所設定的虛擬 IP 位址出現在**介面設定**表中。

設定冗餘連接埠

冗餘連接埠可以與主動/主動叢集一起使用。可以將一個未使用的實體介面作為冗餘連接埠指派給一個已設定的實體介面（稱為「主要介面」）。如果主介面發生實體連結故障，冗餘介面可以繼續處理流量，不會有任何中斷。此功能的優勢是在發生實體連結故障時，無需進行裝置容錯移轉。

您可以在**管理 | 系統安裝 | 網路 | 介面 > 編輯介面 > 進階**對話方塊中設定冗餘連接埠。**冗餘連接埠**欄位僅在主動/主動叢集啟用時可用。

附註：由於所有叢集節點共用同一設定，因此各節點必須設定相同的冗餘連接埠並將其連接到相同的交換器。

如需實體連接冗餘連接埠和冗餘交換器的資訊，請參閱 *「主動/主動叢集全網格部署技術說明」*。

設定一個介面的冗餘連接埠的步驟如下：

1 登入到叢集節點的主要裝置。

2 導覽到**管理 | 系統安裝 | 網路 | 介面**。

3 在**介面設定**表中，按一下想要建立冗餘連接埠的主要介面的**設定**圖示。例如，按一下 **X2** 的**設定**圖示。將顯示**編輯介面**對話方塊。

4 按一下**進階**。

5 在**冗餘/彙總連接埠**中，選取**連接埠冗餘**。對話方塊的選項將改變。

6 從**冗餘連接埠**中，選取冗餘連接埠。僅未使用的介面可供選擇。例如，選擇 **X4** 用作冗餘連接埠。

7 按一下 **3**。

在**介面設定**表格中，選定的介面顯示為灰色。備註表明它是冗餘連接埠，並且列出主要介面。介面還會出現在主要連接埠的**編輯介面**對話中的**冗餘連接埠**欄位中。

附註：主要和冗餘連接埠必須實體連接到同一交換器，最好是連接到網路中的冗餘交換器。

8 在各叢集節點上複製冗餘實體連接，主要和冗餘連接埠使用相同的介面號。所有叢集節點共用與主節點相同的設定。

主動/主動叢集全網格

主題：

主動/主動叢集全網格概述

主動/主動叢集全網格設定是主動/主動叢集設定選項的增強功能，可防止網路中的任何單點故障。所有防火牆和其他網路裝置均結成夥伴以實現完整的冗餘。全網格確保部署中沒有單點故障，無論是裝置（安全設備/交換器/路由器）還是連結。每台裝置均透過兩條線路連接到相連裝置。全網格主動/主動叢集提供最高水平的可用性和高效能。

附註：安全設備上游網路中的路由器應預先針對虛擬路由器冗餘通訊協定 (VRRP) 進行設定。

主題：

關於全網格部署

主動/主動叢集全網格設定是主動/主動叢集設定選項的增強功能，提供最高水平的可用性和高效能。全網格部署可為網路提供極高水平的可用性，因為所有裝置都有一個或多個冗餘夥伴，包括路由器、交換器和安全設備。每台裝置均透過兩條線路連接到相連裝置，因此整個網路中不存在單點故障。例如，每個 SonicWall 防火牆使用冗餘連接埠兩次連接到各網路裝置。

附註：全網格部署要求啟用並實作連接埠冗餘。

主動/主動叢集全網格的優點

- **核心網路中不存在單點故障**：在主動 / 主動叢集全網格部署中，不僅是安全設備，整個核心網路都不存在單點故障。如果一條路徑上的交換器、路由器、安全設備同時發生故障，總是存在一條備用路徑可用於流量處理，從而提供最高級別的可用性。
- **連接埠冗餘：**主動/主動叢集全網格在各叢集節點內採用 HA 冗餘和連接埠冗餘，在叢集內採用節點層級冗餘。利用連接埠冗餘，如果主要連接埠失效，備用連結將以透明方式接管，因而無需裝置層級的容錯移轉。

冗餘連接埠和冗餘交換器

冗餘連接埠可以與主動/主動叢集一起使用。如果一個連接埠發生故障，流量將透過冗餘連接埠無縫處理，不會引起 HA 或主動/主動容錯移轉。啟用主動/主動叢集時，**管理 | 系統安裝 | 網路 | 介面 > 編輯介面**對話方塊中的**冗餘連接埠**欄位即變成可用狀態。

設定冗餘連接埠時，介面必須未使用，也就是未將其指派給任何區域。兩個連接埠必須實體連接到同一交換器，最好是連接到網路中的冗餘交換器。

附註：由於所有叢集節點共用同一設定，因此各節點必須設定相同的冗餘連接埠並將其連接到相同的交換器。

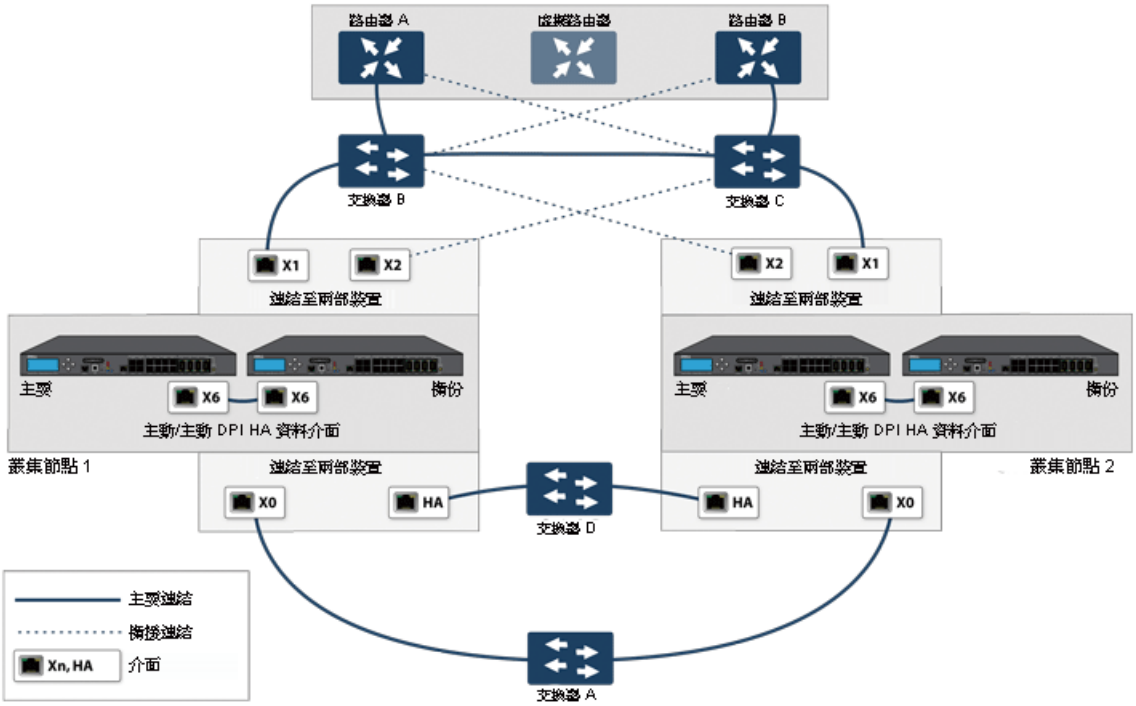
所有叢集節點均正常工作並處理流量時，冗餘連接埠保持待命，一旦夥伴連接埠因為任何原因停止工作便可使用。如果一個叢集節點停止工作，引起主動/主動容錯移轉，剩餘叢集節點中的冗餘連接埠就會立即投入使用，處理故障節點擁有的虛擬群組的流量。這就是負載分擔。

例如，有一個部署，其中虛擬群組 1 歸叢集節點 1 所有，虛擬群組 2 歸叢集節點 2 所有。叢集節點設定有冗餘連接埠 X3 和 X4。所有節點正常工作時，X4 上無流量。如果叢集節點 2 停止工作，虛擬群組 2 將也歸叢集節點 1 所有。此時，開始將冗餘連接埠 X4 用於分擔負載。虛擬群組 1 流量透過 X3 傳送，虛擬群組 2 流量則透過 X4 傳送。在較大部署中，如果叢集節點 1 擁有 3 或 4 個虛擬群組，流量將在冗餘連接埠間指派：虛擬群組 1 和 3 的流量透過 X3 傳送，虛擬群組 2 和 4 的流量則透過 X4 傳送。

如果設定了冗餘交換器，SonicWall 推薦利用冗餘連接埠與之相連。雖然可以不使用冗餘連接埠連接冗餘交換器，但這涉及到使用探查的複雜設定。根據高可用性的需求，冗餘交換器可以放在網路中的任何地方。例如，如果透過冗餘交換器傳送的流量是業務關鍵型，可以將它部署在 WAN 側。

WAN 側冗餘所示的部署包括 WAN 側的冗餘路由器、交換器和連接埠，但不是全網格部署，因為 LAN 側未使用冗餘。

WAN 側冗餘



部署冗餘連接埠或交換器時不需要全網格，但全網格部署包括它們。全網格部署使用各主要流量連接埠（LAN、WAN 等）上的冗餘連接埠，除冗餘交換器外，還使用冗餘上游路由器。

如需全網格部署的更多資訊，請參閱「*主動/主動叢集全網格部署技術說明*」。

設定主動/主動叢集全網格

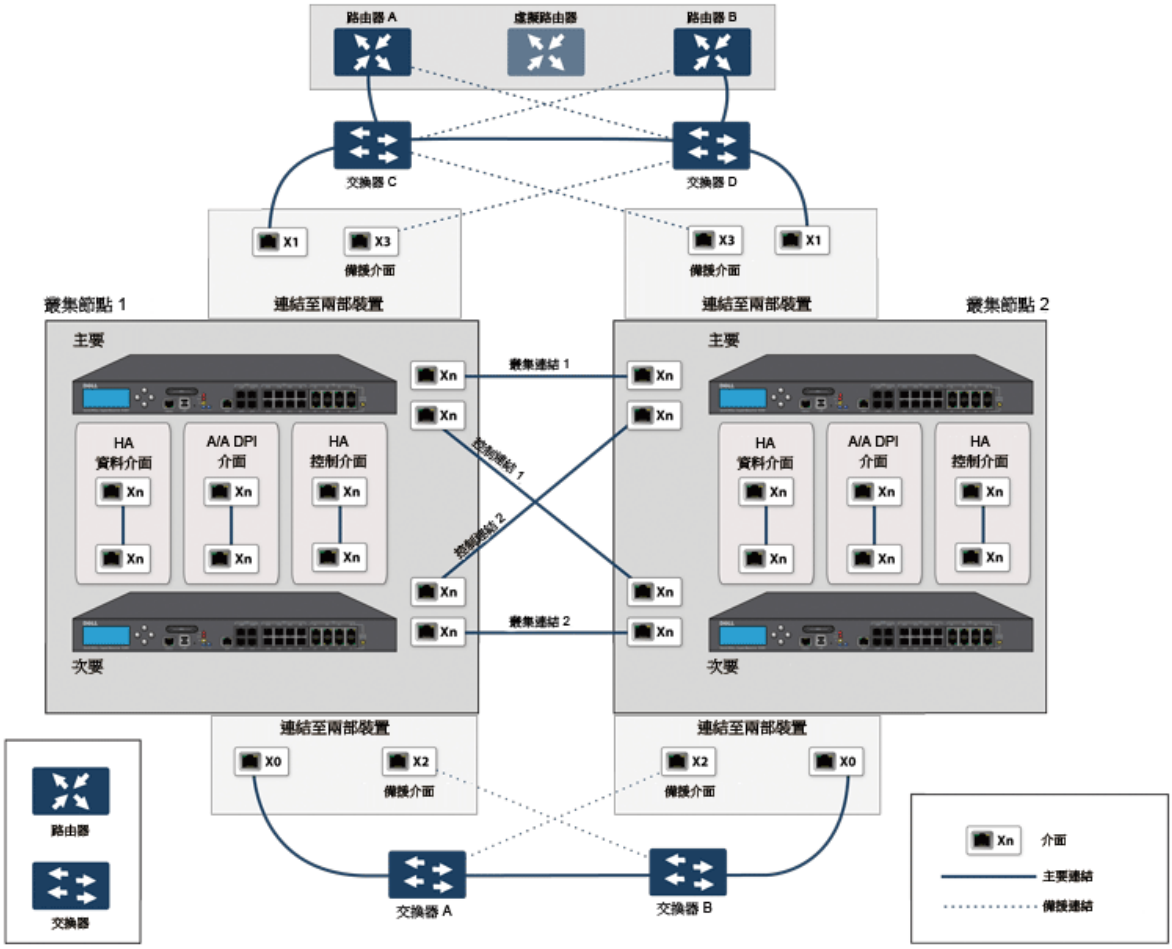
本節介紹 4 裝置主動/主動叢集全網格部署的設定程式（參見主動/主動四裝置叢集全網格）：

- 第 551 頁「主動/主動全網格的佈線」
- 第 553 頁「設定主動/主動叢集安全設備」
- 第 554 頁「設定主動/主動叢集全網格二裝置部署」

所述的部署是實例。基於下列因素，實際的部署可能不同：

- 網路的拓撲/設計和所用網路裝置的類型（交換器、路由器、負載均衡器等）
- 所需的可用性水平
- 資源制約

主動/主動四裝置叢集全網格



主動/主動全網格的佈線

以下程式說明主動/主動四裝置叢集全網格所示部署的佈線。

若要實體連接網路裝置以實現全網格部署：

1 將所有防火牆的所有 HA 連結連接到交換器 E 上的一個基於連接埠的 VLAN。

2 在設定中，X2 是 X0 的冗餘連接埠。X0、X2 連接埠的纜線連接如下：

   a CN2-主要防火牆的 X0 連接到交換器 A，X2 連接到交換器 B。

   b CN2-備用防火牆的 X0 連接到交換器 A，X2 連接到交換器 B。

   c CN2-主要防火牆的 X0 連接到交換器 B，X2 連接到交換器 A。

   d CN2-備用防火牆的 X0 連接到交換器 B，X2 連接到交換器 A。

3 在交換器 A 和交換器 B 上：

   a 將連接到 X0、X2 介面的所有交換器連接埠設定到同一基於連接埠的 VLAN 中。

   b 啟用產生樹狀目錄，同時啟用連接到防火牆的連接埠的 Port Fast（或同等命令）。

4 X3 是 X1 的冗餘連接埠。X1、X3 連接埠的纜線連接如下：

   a CN2-主要防火牆的 X1 連接到交換器 C，X3 連接到交換器 D。

   b CN2-備用防火牆的 X1 連接到交換器 C，X3 連接到交換器 D。

   c CN2-主要防火牆的 X1 連接到交換器 D，X3 連接到交換器 C。

   d CN2-備用防火牆的 X1 連接到交換器 D，X3 連接到交換器 C。

5 在交換器 C 和交換器 D 上：

   a 將連接到 X1、X3 介面的所有交換器連接埠設定到同一基於連接埠的 VLAN 中。

   b 啟用產生樹狀目錄，同時啟用連接到防火牆的連接埠的 Port Fast（或同等命令）。

6 用纜線連接交換器 A 和交換器 B。

7 用纜線連接交換器 C 和交換器 D。

8 如果路由器 A 和路由器 B 具有冗餘連接埠支援，則像連接防火牆連接埠和交換器一樣，將路由器連接到交換器。也就是說，將路由器 A 的主要連接埠連接到交換器 C，備用連接埠連接到交換器 D。用同樣方式連接路由器 B 的連接埠。

9 如果路由器沒有冗餘連接埠支援，但有交換支援，請在路由器 A 上的同一 VLAN 中建立兩個連接埠，並將 IP 位址指派給 VLAN 而不是連接埠。然後將一個連接埠連接到交換器 C，另一個連接埠連接到交換器 D。對路由器 B 進行類似的設定。（這是主動/主動四裝置叢集全網格中所示的設定）。

10 主動/主動 DPI 可以與主動/主動叢集一起使用。連接埠 X6 和 X7 是兩個 HA 資料連接埠，用於冗餘和負載分擔，可將流量從使用中安全設備分流到待命安全設備。執行如下佈線（為簡明起見，主動/主動四裝置叢集全網格未顯示 X6、X7 連接埠和佈線）：

   a 用交叉網線將 CN1-主要的 X6 連接到 CN1-備用的 X6。

   b 用交叉網線將 CN1-主要的 X7 連接到 CN1-備用的 X7。

   c 用交叉網線將 CN2-主要的 X6 連接到 CN2-備用的 X6。

   d 用交叉網線將 CN2-主要的 X7 連接到 CN2-備用的 X7。

設定主動/主動叢集安全設備

主題：

設定程式

若要設定主動/主動叢集安全設備:

1 關閉除 CN1-主要裝置以外的所有其他防火牆。

2 在**管理 | 系統安裝 | 高可用性 | 基本設定**頁面上:

   a 從**模式**中，選擇**主動/主動叢集**。

   b 選擇**啟用狀態同步**。

   c 按一下 **HA 裝置與節點**。

   d 在相應**主要裝置序號 #**和**備份裝置序號 #**欄位中輸入叢集節點主要及備份裝置的序號。

   e 對於 CN1，從**虛擬群組 1 級別**選取**所有者**，並從**虛擬群組 2 級別**選取**待命**。

   f 對於 CN2，從**虛擬群組 1 級別**選取**所有者**，並從**虛擬群組 2 級別**選取**待命**。

   g 啟用主動/主動 DPI，X6 和 X7 用作兩個 HA 資料連接埠。

   h 按一下**套用**。

3 在**管理 | 系統安裝網路 | 介面網路 | 介面**上:

   a 新增 X0 和 X1 介面的虛擬群組 (VG) IP 位址。

   b 新增冗餘連接埠設定（X2 作為 X0 的冗餘連接埠，X3 作為 X1 的冗餘連接埠）。

4 在**管理 | 系統安裝 | 高可用性 | 監控設定**上，在叢集中各裝置的 X0 和 X1 上新增監視/管理 IP 位址。

5 開啟所有其他安全設備。CN1-主要安全設備的設定完全同步到所有其他安全設備。

6 使用專用監控/管理位址登入各安全設備，並執行以下操作:

   a 在 MySonicWall 上註冊安全設備。

   b 與 MySonicWall 同步授權。

單點故障測試

連接並設定好上述部署後，CN1 擁有虛擬群組 1 (VG1)，CN2 擁有虛擬群組 2 (VG2)。

將 X0 上的 VG1 IP 位址設定為某一組流量的閘道，將 X0 上的 VG2 IP 位址設定為其他組流量的閘道。您可以利用不同方法實現這一設定:

- 使用智慧 DHCP 伺服器，可將閘道指派發佈到直接相連用戶端網路上的 PC。
- 在下游路由器上使用基於原則的路由。

完成流量設定後，兩個叢集節點均會主動處理網路流量。

若要在所有裝置和連結上進行單點故障測試:

1 **裝置故障**：在下述各種裝置故障情況下，流量應繼續流經兩個叢集節點:

   a 交換器 A 斷電，交換器 B 正常並就緒。

   b 交換器 B 斷電，交換器 A 正常並就緒。

   c 從 SonicOS 管理介面重新啟動 CN1 中的活動裝置，CN1 中的備用裝置正常並就緒（這種情況與 CN1-活動裝置發生軟體故障相似）。

   ⓘ **附註：**這種情況下將會發生可設定狀態 HA 容錯移轉。

   d 關閉 CN1-活動裝置，CN1-備用裝置正常並就緒（這種情況與 CN1-活動裝置發生硬體故障相似）。

   ⓘ **附註：**這種情況下將會發生可設定狀態 HA 容錯移轉。

   e 對 CN2 重複步驟 c 和步驟 d。

   f 關閉路由器 A，路由器 B 正常並就緒。

   g 關閉路由器 B，路由器 A 正常並就緒。

2 **連結故障**：在下述各種連結故障情況下，流量應繼續流動:

   a 在叢集節點的各使用中安全設備上，斷開 X0 纜線，X2 保持連接。

   b 在叢集節點的各使用中安全設備上，斷開 X1 纜線，X3 保持連接。

   c 斷開從上游交換器到路由器（活動防火牆的虛擬路由器）的主要連結。

   d 斷開 X6（主動/主動 DPI HA 資料介面）。

設定主動/主動叢集全網格二裝置部署

您也可以採用兩個安全設備部署主動/主動叢集全網格，其中各叢集節點僅包含一個安全設備 (無 HA 備份)。不過，這種設定具有如下局限：

- 容錯移轉不是可設定狀態，且現有連接需要重建。
- 在容錯移轉時，如果各裝置上的流量大於單台安全設備容量的 50%，那麼容錯移轉後，將丟棄超過 50% 的流量。

二裝置全網格的設定程式與四裝置全網格相似，例外如下：

- 涉及各節點中備用裝置的步驟不適用。
- 設定可設定狀態同步和主動/主動 DPI 的步驟不適用。
- 無需交換器來連接 HA 連接埠（因為只有兩台裝置，可以透過交叉網線互連）。

35

微調高可用性

高可用性 | 進階設定

管理 | 系統安裝 | 高可用性 | 進階設定能夠微調高可用性設定，以及同步高可用性安全設備間的設定和韌體。**高可用性 | 進階設定**使用中/待命和主動/主動設定的完全相同。

活動訊號間隔和**容錯移轉觸發級別（遺失的活動訊號）**設定同時適用於 SVRRP 活動訊號（主動/主動叢集活動訊號）和 HA 活動訊號。**高可用性 | 進階設定**上的其他設定僅適用於叢集節點內的 HA 對。

附註：如需高可用性的更多資訊，請參閱第 508 頁「關於高可用性」和第 515 頁「使用中/待命和主動/主動 DPI 前提條件」。

設定進階高可用性

若要設定進階設定：

1 在主節點（即虛擬群組 1 IP 位址，X0 或其他介面且啟用 HTTP 管理）上以管理員身分登入 SonicOS 管理介面。

2 導覽到**管理 | 系統安裝 | 高可用性 | 進階設定**。

3 可調整**活動訊號間隔**，以控制主動/主動叢集中安全設備的通訊頻率。此設定適用於主動/主動叢集中的所有裝置。預設值為 **1,000** 毫秒 (1 秒)，最小值為 1,000 毫秒，而最大值為 300000。

附註：SonicWall 建議將此活動訊號間隔至少設定為 1000。

如果您的部署要處理大量網路流量，可以使用較高的值。較低的值有可能導致不必要的容錯移轉，尤其是當安全設備處於較大負載的情況下。

此計時器會連結到**容錯移轉觸發級別（遺失的活動訊號）**計時器。

4 設定**容錯移轉觸發級別**，即可以錯過多少次活動訊號而不發生容錯移轉。此設定適用於主動/主動叢集中的所有裝置。預設值為 **5**，最小值為 4，最大值為 99。

此計時器會連結到活動訊號間隔計時器。如果**容錯移轉觸發級別**設定為 5，**活動訊號間隔**設定為 10000 毫秒 (10 秒)，則 50 秒鐘無活動訊號後將觸發容錯移轉。

5 設定**探查間隔**，即傳送至指定 IP 位址以監視網路關鍵路徑是否仍然可及的探查的間隔時間（秒）。此間隔用於本機 HA 對的邏輯監控。預設值是 **20** 秒，容許範圍是 5 到 255 秒。

提示： SonicWall 推薦將此間隔至少設定為 5 秒。

您可以在**管理 | 系統安裝 | 高可用性 | 進階設定**上設定探查 IP 位址。請參閱第 558 頁「高可用性 | 監控設定」。

6 設定**探查計數**，即連續探查多少次無回應後，SonicOS 即可認定網路關鍵路徑無法使用或探查目標不可及。此計數用於本機 HA 對的邏輯監控。預設值是 **3**，容許範圍是 3 到 10。

7 設定**選擇延遲時間**為主要安全設備考慮介面啟動和穩定需要等候的秒數。預設值為 **3** 秒，最小值為 3 秒，最大值為 255 秒。

提示：此計時器對於交換器連接埠有跨距樹狀目錄延遲設定時相當有用。

8 設定**動態路由保持時間**，即新啟用的安全設備將之前獲取的動態路由保持在其路由表中的秒數。預設值為 **45** 秒，最小值為 0 秒，最大值為 1200 秒（20 分鐘）。

附註：只有在**管理 | 系統安裝 | 網路 | 路由**上選取**進階路由**選項時，才會顯示**動態路由保持時間**設定。

提示： 在大型或複雜網路中，較大的值可以改善容錯移轉期間的網路穩定性。

使用 RIP 或 OSPF 動態路由的高可用性對發生容錯移轉時，會使用此設定。在此期間，新啟用的裝置重新瞭解網路中的動態路由。當**動態路由保持時間**過期時，SonicOS 刪除舊路由，並實作從 RIP 或 OSPF 瞭解到的新路由。

9 如果希望只有在所有彙總連結當機時進行容錯移轉，則勾選**僅當所有的彙總連結當機時進行使用中/待命容錯移轉**。預設情況下未勾選此選項。

10 若要讓設備同步 HA 對內的所有憑證和金鑰，請選取**包含憑證/金鑰**。預設情況下已核取此選項。

11 (可選) 若要同步主要和次要 HA 防火牆之間的 SonicOS 喜好設定，請按一下**同步設定**。

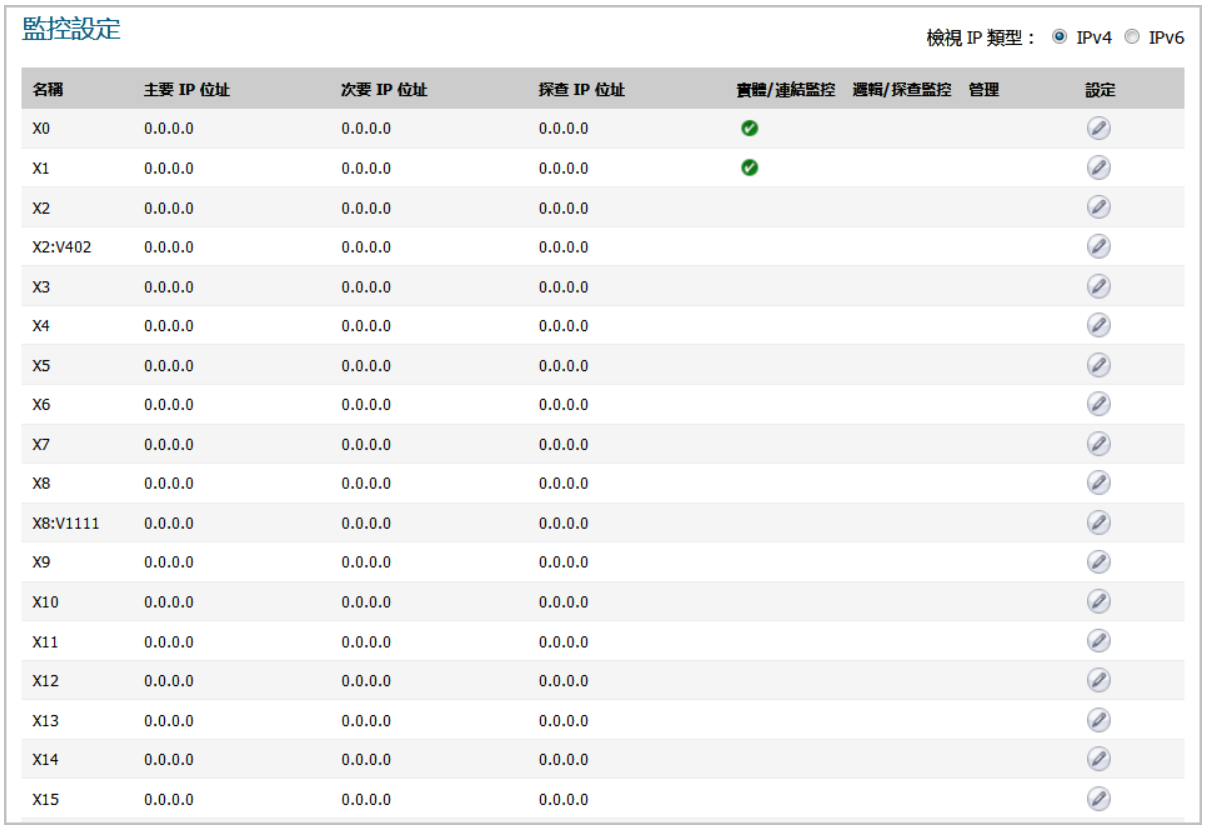
12 (可選) 若要同步主要和次要 HA 防火牆之間的韌體版本，請按一下**同步韌體**。

13 (可選) 若要嘗試使用中/待命 HA 容錯移轉到次要安全設備，以測試 HA 容錯移轉功能是否正常，請按一下**強制使用中/待命容錯移轉**。

14 完成所有高可用性設定後，按一下**接受**。所有設定都會同步到叢集中的次要安全設備或其他裝置。

監視高可用性

高可用性 | 監控設定



名稱	主要 IP 位址	次要 IP 位址	探查 IP 位址	實體/連結監控	邏輯/探查監控	管理	設定
X0	0.0.0.0	0.0.0.0	0.0.0.0	✔			
X1	0.0.0.0	0.0.0.0	0.0.0.0	✔			
X2	0.0.0.0	0.0.0.0	0.0.0.0				
X2:V402	0.0.0.0	0.0.0.0	0.0.0.0				
X3	0.0.0.0	0.0.0.0	0.0.0.0				
X4	0.0.0.0	0.0.0.0	0.0.0.0				
X5	0.0.0.0	0.0.0.0	0.0.0.0				
X6	0.0.0.0	0.0.0.0	0.0.0.0				
X7	0.0.0.0	0.0.0.0	0.0.0.0				
X8	0.0.0.0	0.0.0.0	0.0.0.0				
X8:V1111	0.0.0.0	0.0.0.0	0.0.0.0				
X9	0.0.0.0	0.0.0.0	0.0.0.0				
X10	0.0.0.0	0.0.0.0	0.0.0.0				
X11	0.0.0.0	0.0.0.0	0.0.0.0				
X12	0.0.0.0	0.0.0.0	0.0.0.0				
X13	0.0.0.0	0.0.0.0	0.0.0.0				
X14	0.0.0.0	0.0.0.0	0.0.0.0				
X15	0.0.0.0	0.0.0.0	0.0.0.0				

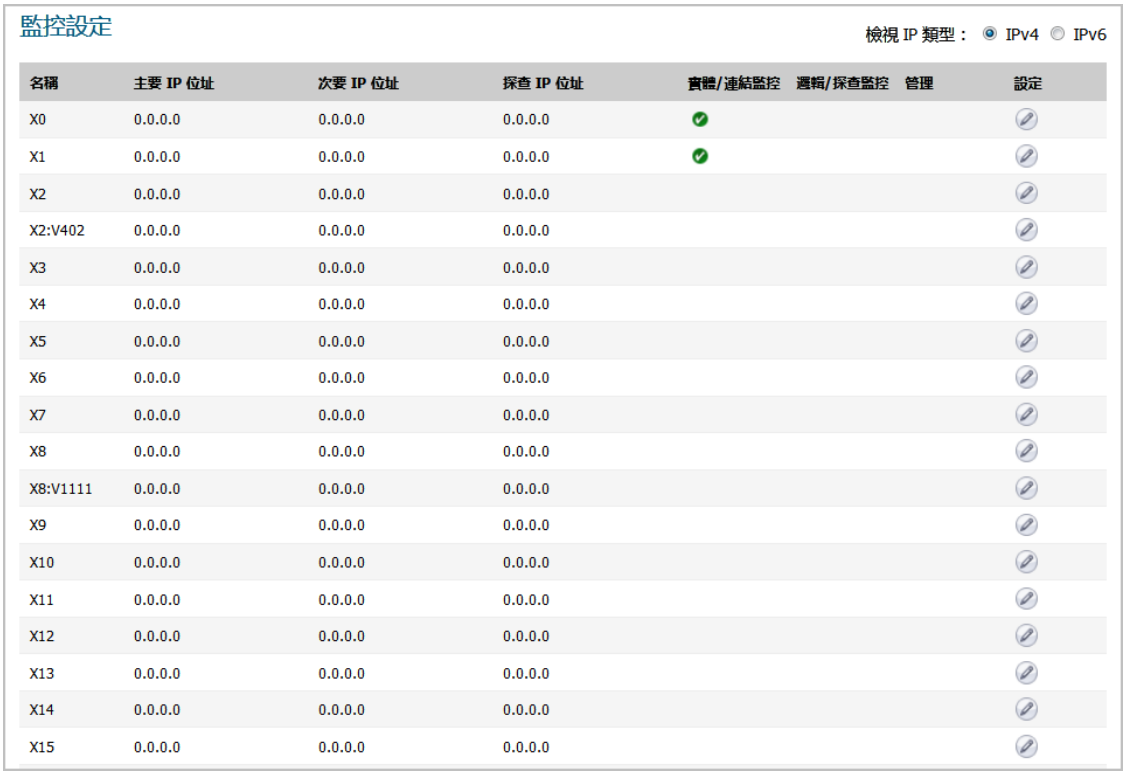
在**管理 | 系統安裝 | 高可用性 | 監控設定**上，您可以使用 LAN 或 WAN 介面，為 HA 對中的各裝置設定獨立的管理 IP 位址。您還可以設定實體/連結監控和邏輯/探查監控。如需 HA 監控設定的更多資訊，請參見第 507 頁「關於高可用性和主動/主動叢集」。

設定使用中/待命高可用性監控

若要設定獨立的 LAN 管理 IP 位址以及設定實體和/或邏輯介面監視：

1 在主要 SonicWall 安全設備上，以管理員身分登入 SonicOS 管理介面。

2 導覽到**管理 | 系統安裝 | 高可用性 | 監控設定**。



3 按一下 LAN 上某個介面的**設定**圖示，例如 **X0**。將顯示**編輯 HA 監控**對話方塊。

4 若要啟用主要和次要裝置上的指定 HA 介面之間的連結偵測，請選取**啟用實體/連結監控**。預設情況下已核取此選項。

5 在**主要 IPv4/v6 位址**欄位中，輸入主要裝置的唯一 LAN 管理 IP 位址。預設值為 **0.0.0.0**。

6 在**次要 IPv4/v6 位址**欄位中，輸入次要裝置的唯一 LAN 管理 IP 位址。預設值為 **0.0.0.0**。

7 選取**允許管理主要/次要 IP 位址**。為某個介面啟用此選項時，在**監控設定**表格中，此介面的**管理**欄中會出現一個綠色圖示。只能對啟用此選項的介面執行管理。預設情況下未勾選此選項。

8 在**邏輯探查 IPv4/v6 位址**欄位，輸入應監視其連接的 LAN 網路上某個下游裝置的 IP 位址。這通常是一個下游路由器或伺服器。（如果需要在 WAN 端進行探查，應使用上游裝置）。預設情況下未勾選此選項。

主要和次要安全設備將定期 ping 此探查 IP 位址。如果二者均能成功 ping 通目的地，則不會發生容錯移轉。如果二者均無法 ping 到目標，也不會發生容錯移轉，因為這種情況下，會認為問題出

在目標，而不是安全設備。但是，如果一個安全設備能夠 ping 到目標，另一個無法，則會容錯移轉到可 ping 到目標的安全設備。

主要 IPv4/v6 位址和**備份 IPv4/v6 位址**欄位必須用 LAN 介面（如 X0）或 WAN 介面（如 X1，用於探查 WAN）上的獨立 IP 位址設定，以便對功能是否正常進行邏輯探查。

9 也可以手動指定介面的虛擬 MAC 位址，方法是選擇**覆寫虛擬 MAC** 並在此欄位中輸入 MAC 位址。MAC 位址的格式是 6 對用分號隔開的十六進位數，如 `A1:B2:C3:d4:e5:f6`。預設情況下未勾選此選項。

重要：應謹慎選擇虛擬 MAC 位址，防止設定錯誤。

在**管理 | 系統安裝 | 高可用性 | 進階設定**上已選取**啟用虛擬 MAC** 時，SonicOS 韌體會自動產生所有介面的虛擬 MAC 位址。讓 SonicOS 韌體產生虛擬 MAC 位址可消除設定錯誤的可能性，確保虛擬 MAC 位址的唯一性，防止可能的衝突。

10 按一下**確定**。

11 若要在任何其他介面上設定監視，請針對每個介面重複步驟 3 到步驟 10。

12 完成所有高可用性設定後，按一下**接受**。所有設定將自動同步到次要裝置。

部分 7

WAN 加速

- 使用 WAN 加速

37

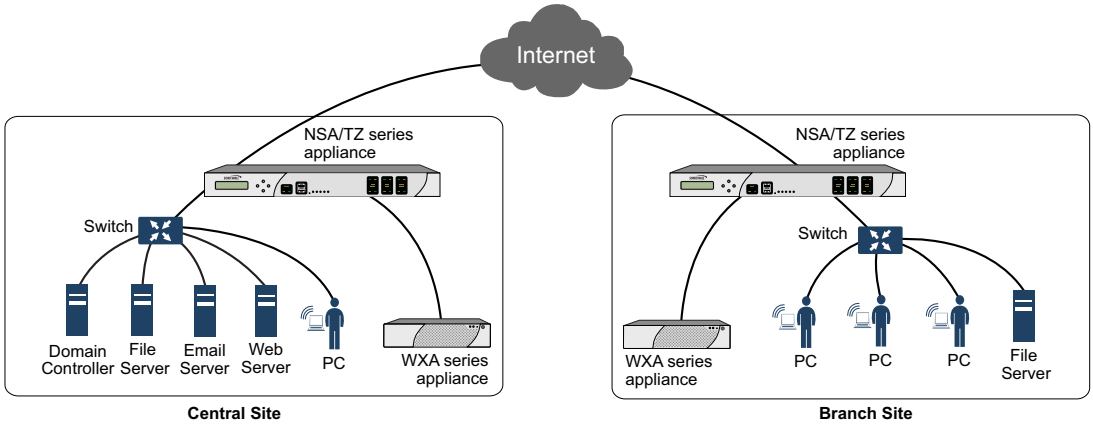
使用 WAN 加速

關於 WAN 加速

WAN 加速服務用於透過使用傳送控制協定 (TCP) 和 Windows 檔案共用 (WFS) 加快中央站台與分支站台之間的 WAN 流量。SonicWall WXA 系列設備與 SonicWall NSA 系列設備聯合部署。在這種部署類型中，NSA 系列設備提供動態安全服務，例如攻擊防護、虛擬私人網路 (VPN)、路由和 Web 內容篩選。WAN 加速服務可以提高 NSA 系列設備效能。

SonicWall WXA 系列設備拓撲顯示 SonicWallWXA 系列設備和 SonicWall 安全設備的基本網路拓撲。

SonicWall WXA 系列設備拓撲



主題：

支援的平台

在下列平台上，WAN 加速可供 SonicOS 6.2 和以上版本使用:

- SuperMassive 9200、9400，以及 9600
- TZ600、TZ500/500W、TZ400/400W、TZ300/300W
- NSA 6600/5600/4600/3600/2650/2600

WXA 叢集目前僅適用於 NSA 和 SuperMassive 系列安全設備。

傳送控制通訊協定加速

TCP 加速服務是藉由使用壓縮來減少通過 WAN 之資料量的處理程序。這會加快中央站台和分支站台之間經過的選定流量。選定流量會儲存在 SonicWall WXA 系列設備的共用資料庫作為資料區塊，並標記為參考索引。這允許 WXA 系列設備僅透過 WAN 傳送較小的參考索引，而不是傳送實際資料。

Windows 檔案共用加速

WAN 加速是指加速應用程式、提高傳送量和減少延遲的各種技術。Windows 檔案共用 (WFS) 加速是 WAN 加速的子集合。

在您的網路中使用 WFS 加速，可透過使用預先讀取和預先寫入功能，以及差異式檔案傳輸，估計串流行為，減少高延遲和低寬頻的影響，以避免重新傳輸未變更的部分檔案。WFS 加速可讓分支使用者透過 WAN 以近似 LAN 的速度存取及共用常用檔案。

部署 WFS 加速解決方案的分佈式企業也許可以將儲存空間合併至公司中央站台，而無需備份及管理先前留在分支站台的資料。

在沒有合併儲存空間的情況下，從其他站台存取本機和分支儲存空間資料的成本和延遲也會降低。

WXA 系列設備為下列項目提供 WFS 加速:

- 未簽署 SMB 流量 - 在支援未簽署 SMB 流量的網路中，設定 WFS 加速的程序已大幅簡化，因為未簽署 SMB 流量沒有安全性階層。因此，WXA 系列設備可以在未加入網域的情況下攔截流量，不需要設定自訂 DNS 區域、反向對應，以及檔案共用。
- 已簽署 SMB 流量 - 在需要 SMB 簽署的網路中，WXA 系列設備必須加入網域，因為已簽署 SMB 流量有安全性階層。已簽署 SMB 設定比未簽署 SMB 設定更加複雜，並提供更多粒度。已簽署 SMB 設定也具有更多選項的進階設定模式。

已簽署 SMB 的延伸支援

已簽署 SMB 流量的延伸支援工作由單一 WXA 負責執行，並且是在 WXA 叢集其他地方使用之群組設定的外部進行設定。藉由在 Windows 網域上加以設定，使用者才能完全從支援已簽署 SMB 之網路上的 WFS 加速模組的額外功能中獲益。將 WXA 系列設備加入網域後，您將可以設定想要將其包含在 WFS 加速過程中的遠端伺服器上的共用。

重要：強烈建議您在需要遠端存取共用的分支站台上設定 WXA 系列裝置之前，先在檔案伺服器所在的站台上設定 WXA 系列裝置。

Web 快取

「Web 快取」功能會儲存近來頻繁通過網路請求的網頁與 Youtube 影片的副本。當使用者請求其中一個網頁時，就會從本機 Web 快取檢索，而不是從網際網路檢索，從而節省頻寬和回應時間。提供最低、一般和加強快取。這些將決定置於 Web 快取中的物件及其停留時間。

WAN 加速服務的部署前提條件

需要 SonicWall 安全設備以部署 SonicWall WXA 系列設備。

通過 SonicWall WXA 系列設備的流量需要網際網路通訊協定第 4 版本 (IPv4)。WAN 加速服務與 IPv6 不相容。

部署注意事項

部署 SonicWall WXA 系列設備時，請考慮以下事項:

- NSA 與 SuperMassive 系列安全設備支援 WXA 叢集，其中多個 WXA 可插入安全設備。
- 對於 WXA 叢集，支援 WXA 系列設備使用 SonicWall NSA 2600 或更高版本，以及執行 SonicOS 6.2.2 或更高版本韌體的 SuperMassive 系列安全設備。
- WXA 500 可藉由插入 CD 啟動電腦，以在記憶體模式中執行。或者，它可以安裝到硬碟中。在後者情況下，提供更多功能。
- 通常，WXA 系列設備透過其各自的 SonicWall 安全設備，部署在站對站 VPN 設定中。不過，您也可以使用路由或 L2 橋接模式。
- 如果在高可用性設定中使用 WXA 系列設備，則需要兩個高可用性對的交換連接。

- 可應使用 WXA 設定精靈進行 WXA 系列設備的初始設定 (可透過透過在 SonicWall 安全設備的管理介面中按一下**快速設定**使用該精靈)。如需有關 WXA 設定精靈的詳細資訊，請參閱 *SonicOS 快速設定*。
- 加密流量是非常隨機的，不會從 WXA 系列設備的 WAN 加速服務中實際收益。因此，SSL 和 TLS 流量類型不會加速。
- 使用已簽署 SMB 的 WFS 加速支援使用 Active Directory、Kerberos 及 NTLM 的 Windows 檔案，以進行驗證和授權。
- 將已簽署 SMB 與 NTLM 用戶端搭配使用的 WFS 加速為網域中有效的 SonicWall WXA 系列設備提供憑證。SonicWall WXA 系列設備透過網域控制器獲取 Kerberos 憑證。這允許具有有效網域憑證的使用者使用尚未加入網域的用戶端裝置。
- 先在管理的 SonicWall 安全設備上建立 DHCP 範圍，然後再實際連接 WXA 系列設備。
- 如果分支辦公室有網域控制器和 DNS 伺服器，建議您使用這些 DHCP 範圍內的 DNS 伺服器位址與網域 DNS 名稱。在設定的 DHCP 範圍中，設定唯一的網域名稱與網域 DNS 伺服器 IP 位址。WXA 系列設備會根據資訊類型自動探索 Kerberos、LDAP 及 NTP 伺服器，以協助將設備加入網域。
- 檢閱 LDAP、Kerberos 及 NTP 服務。在未明確設定網站與服務的多站台網域中，WXA 系列設備可能不會選擇最靠近的伺服器。
- SonicWall 建議 WXA 系列設備從網域控制器擷取 NTP 更新。如果未設定 NTP 伺服器，則會自動完成此操作。
- SonicWall 建議將擁有 WXA 名稱或 IP 位址的 Active Directory DNS 區域設定為僅接受安全更新。
- 將 WXA 系列設備連接到的介面區域屬性設定為 LAN 區域。

關於 WXA 叢集

附註：NSA 2600 及更新裝置支援 WXA 叢集。

SonicOS 支援使用兩個或多個 NSA 系列設備或 SuperMassive 設備的 WXA 叢集。最大型的 SonicWall WXA 系列設備可支援最多 1200 個連接，可大致轉換為對多達 240 個並行使用者的支援。WXA 叢集支援的使用者數現已增加：

- SonicOS 可以同時監控或探查多個 WXA 系列設備，並為每個 WXA 儲存易記的名稱。
- SonicOS 可實現以下三種形式的負載分擔：TCP 加速、未簽署 SMB 加速以及 Web 快取。
- 可以指定 VPN 原則始終使用相同的 WXA 群組。
- 連接數量是群組內的所有 WXA 系列設備之間平均指派。
- 當其中一個 WXA 達到連接能力後，使用群組中的下一個 WXA。

主題：

- 第 566 頁「叢集的支援平台」
- 第 566 頁「什麼是 WXA 叢集?」
- 第 567 頁「WXA 叢集如何運作?」

叢集的支援平台

下列支援 WXA 叢集:

- WXA 韌體版本 1.3.2 及更高版本。
- 在下列 SonicWall 安全設備中:

SM 9600	NSA 6600
SM 9400	NSA 5600
SM 9200	NSA 4600
	NSA 2600
	NSA 3600

什麼是 WXA 叢集?

WXA 叢集定義為兩個或多個 WXA 系列設備配合使用，以提高傳送量和彈性。

優點

叢集 WXA 系列設備大幅增加了可同時加速的連線數目。透過簡單地增加更多 WXA 裝置，您可以提高數倍容量。根據 WXA 型號的使用者上限和連線上限表格顯示每個 WXA 平台可用的最大使用者數目和連線數目。

根據 WXA 型號的使用者上限和連線上限

	WXA 系列設備				
	WXA 6000	WXA 4000	WXA 2000	WXA 5000	WXA 500 Live
平台	軟體	硬體			
設備	硬體				
設備	虛擬				
設備	軟體				
使用者上限	2000	240	120	360	20
上限					
連線	10,000	1,200	600	1,800	100

叢集 WXA 設備提供下列優點:

- 為使用者和 WAN 基礎結構提高加速解決方案的可擴充性
- 是彈性的解決方案，可以擴充以滿足企業和應用需求
- 是靈活的解決方案，允許一個或多個 WXA 專用於特定任務或網路區段
- 是適用於 WAN 加速的彈性基礎結構

WXA 叢集如何運作?

WXA 叢集藉由將多個 WXA 系列設備連接在一起，並使用負載平衡和連線平衡來增加可能的同時連線數來完成操作。沒有必要在遠端和本機位置都實作 WXA 叢集，但每個位置至少應該有一個 WXA。

連接多個 WXA 並一起運作時，可透過 WAN 加速的資料量顯著增加。

在 WXA 叢集設定中，WXA 是群組的成員，而且有多個群組。每個群組中的 WXA 具有相同設定，但 WXA 的不同群組可以有不同的設定。

WXA 設定是從 SonicWall 安全設備上的 SonicOS 推送。

主題：

限制

WXA 叢集不支援已簽署 SMB 的 WFS 加速。如果您使用專用於加速已簽署 SMB 的單一 WXA，則支援已簽署 SMB 的 WFS 加速。該 WXA 可能或可能不是群組的一部分。不過，將其保留在叢集群組之外，可以僅處理加速的已簽署 SMB 流量。

WXA 叢集的授權

WXA 叢集的授權是根據您希望支援之同時加速的連線數目上限而定。客戶可為要加速的特定連線數購買 WXA 叢集授權。

在 WXA 500、WXA 5000 及 WXA 6000 上，根據所需的連線數購買 WXA 叢集授權。每個授權代表允許的連線數上限。只有經過授權的連線數上限才會加速。如果超過連線數上限通過 SonicWall 安全設備，仍會建立超過的連線，但不會加速。

在 WXA 2000 與 WXA 4000 上，不需要額外授權。對於這些型號，設備內建的連線數上限也是要加速的連線數上限。

如果將 WXA 2000 或 WXA 4000 新增至其中具有 WXA 500、WXA 5000 或 WXA 6000 的叢集，則連線數會相應增加。例如，將 WXA 2000 新增至叢集會對允許的限制增加 600 個並行連線。

您可以將任何數目的虛擬 WXA 500、WXA 5000 及 WXA 6000 新增至 SonicWall 安全設備，但加速的連線數取決於購買的授權而定。

如果超過允許的加速連線數，無論叢集中有多少 WXA，所有超過的連線會繞過叢集。管理員有責任確保足夠數量的 WXA 連接到安全設備，以處理他們希望支援的授權連線數。

允許在路由原則上加速

設定 WXA 之後，您可以為路由原則允許加速。您可以在**系統安裝 | WAN 加速**頁面上或在**網路 | 路由**頁面上為路由原則允許加速 (請參閱第 371 頁「設定路由通告和路由原則」)。

如果您尚未在網路上設定 VPN，而且您使用自訂的路由原則，則需要在每個站台上新增兩個路由原則: 一個用於傳出流量，一個用於傳入流量。

系統安裝 > WAN 加速

主題：

- 第 568 頁「啟用 WAN 加速」
- 第 569 頁「管理群組」
- 第 573 頁「透過 WXA 表格管理 WXA」
- 第 588 頁「為 VPN 原則設定 WXA」
- 第 589 頁「設定 SSL VPN 流量的加速」

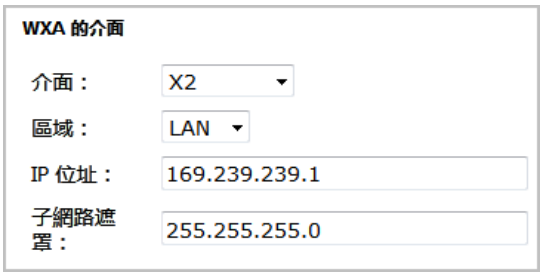
啟用 WAN 加速

若要啟用 WAN 加速:

1 導覽到**系統安裝 > WAN 加速**。

2 在 **WAN 加速**區段中，選取**啟用 WAN 加速**。

3 按一下**介面編輯**圖示，選取要連接 WXA 的介面。隨即顯示 **WXA 的介面**快顯。



4 從**介面**中，選取要連接 WXA 的介面。

5 從**區域**中，選取介面的區域。

6 在 **IP 位址**欄位中，輸入選定介面的 IP 位址。

> **重要：**用於配置位址至 WXA 的 DHCP 範圍，是根據介面的 IP 位址和網路遮罩決定。

7 在**子網路遮罩**欄位中，輸入選定介面的網路遮罩。

8 按一下**確定**。

管理群組

此欄	指示或顯示
名稱	群組的名稱
TCP 加速	TCP 加速是**啟用**或**停用**。
WFS 加速	WFS 加速是**啟用**或**停用**。
Web 快取	• Web 快取是**啟用**或**停用**。 • 快取策略: **最低**、**一般**或**加強**。
WXA	找到的可用 WXA (線上和叢集就緒) 數量和為群組設定的數量: *已找到*/*已設定*。
VPN	其加速受群組控制的 VPN 數量。

此欄	指示或顯示
SSL VPN	其加速受群組控制的 SSL VPN 數量。
路由	其加速受群組控制的路由數量。
連線	目前通過群組中 WXA 的連線數量。如果您將滑鼠移至數字上方，快顯隨即出現並顯示以下內容: • 群組中每個 WXA 型號支援的連線總和。 • 可加速的同時連線整體授權數。
預設	綠色圖示表示預設群組。
設定	群組的**編輯**和**刪除**圖示。
監控	**監控**按鈕可顯示 **WXA 連線**監控。

主題：

新增群組

若要新增群組:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**區段中，按一下**新增**圖示，隨即顯示**新增群組**對話方塊。

3 在**名稱**欄位中，為群組輸入有意義的名稱。

4 若要指定群組作為預設群組，請選取**使用為預設的群組**。 預設情況下未勾選此選項。

5 如果您:

- 不打算使用 TCP 加速，請移至步驟 10。
- 要使用 TCP 加速，請按一下 **TCP 加速**。

6 按一下**啟用 TCP 加速**。

7 從 **TCP 加速模式**中選取模式:

- **除了預設為已排除的以外之所有 TCP 服務** (此為預設值；服務物件下拉功能表顯示為灰色)；請移至步驟 9
- **除了已指定於服務物件的以外之所有 TCP 服務**
- **除了已指定於服務物件及預設為已排除的以外之所有 TCP 服務**
- **僅限指定於服務物件的 TCP 服務** (僅針對服務物件啟用 TCP 加速)

> **提示：**若要查看排除的 TCP 服務，請將滑鼠懸停在 **TCP 加速模式**，以顯示列出排除服務的快顯。

8 從**服務物件**中，選取要排除或包含的服務物件。

9 若要將位址物件從 TCP 加速中排除，請從**位址物件一律排除**中選取位址物件；預設值為**無**。

10 如果您:

- 不打算使用 WFS 加速，請移至步驟 12。
- 要使用 WFS 加速，請按一下 **WFS 加速**。

11 選取**啟用 WFS 加速**。

12 如果您:

- 不打算使用 Web 快取，請移至步驟 19。
- 要使用 Web 快取，請按一下 **Web 快取**。

13 選取**啟用 Web 快取**。

14 從 **Web 伺服器連接埠**中，選取服務物件，代表截獲其流量並傳送至 WXA Web 快取的 Web 伺服器連接埠。預設為 **HTTP**。

15 從**用戶端包含位址物件**中，選取位址物件或群組，代表其 Web 流量應透過 WXA Web 快取轉移的本機子網路。預設為 **LAN 子網路**。

16 從**用戶端排除位址物件**中，選取位址物件或群組，包含其 Web 伺服器流量不應透過 WXA Web 快取轉移的 Web 伺服器目的地位址。預設為**無**: 不排除任何 Web 伺服器，並將透過 WXA 傳送所有相應的流量。

17 從**快取策略**中選取快取策略，決定要快取之物件的類型及屬性，以及指出留在快取中時間長度的屬性:

最小	提供基本快取，Web 快取將據此快取物件，除非 HTTP 標頭特別表示不要進行 (例如，過去發生的無快取或到期時間)
中等	比較不嚴格，將物件儲存在快取中的時間較長。這是預設值。
加強	此快取會忽略標題選項，例如，無儲存和重新載入，並且會覆寫到期時間。 注意：**使用這個策略應該非常小心，因為它違反了 HTTP 標準，可能會導致不必要的後果。**

附註：中等和**加強**模式包含 YouTube 影片的快取。

18 或者，在**管理員電子郵件**欄位中，輸入管理員電子郵件地址。

19 按一下**確定**。

設定預設群組

通常，預設群組是在設定群組時指定 (請參閱第 570 頁「新增群組」)，但是您可以隨時變更預設群組。

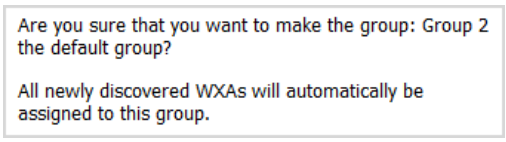
若要變更預設群組:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格中，取消選取預設群組。

3 選取要作為預設的群組。**設為預設值**按鈕會變成可用狀態。

4 按一下**設為預設值**。將顯示確認訊息。



5 按一下**是**。綠色指標隨即顯示在預設群組的**預設**欄中。

編輯群組

若要編輯群組:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格中，為要編輯的群組，按一下**編輯**圖示。將顯示**編輯群組**對話方塊。

3 遵照第 570 頁「新增群組」中步驟 3 到步驟 19 的步驟。

刪除群組

您可以刪除一個或多個群組。無法刪除與 WXA 關聯的群組，也無法刪除用於管理一個或多個 VPN、SSL VPN 或路由上之加速的群組。

若要刪除群組:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格中，選取要刪除的群組。

3 針對群組按一下**刪除**圖示。將顯示確認訊息。

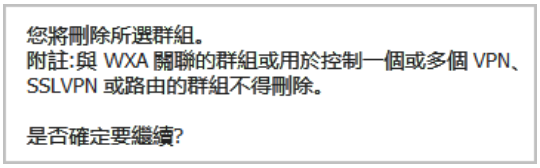
4 按一下**是**。

若要刪除多個群組:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格中，選取要刪除的群組。表格上的刪除圖示會變成可用狀態。

3 按下 **Delete (刪除)** 圖示。將顯示確認訊息。



4 按一下**是**。

透過 WXA 表格管理 WXA

ID	WXA 系列設備的 MAC 位址。
名稱	WXA 系列設備的名稱。
組	WXA 系列設備所屬的群組。
IP	WXA 系列設備的 IP 位址。
模式	WXA 系列設備的型號。

韌體	安裝在 WXA 系列設備上的韌體版本。 **附註：**按一下 WXA 系列設備的韌體版本會帶您到**管理 | 更新 | WXA 韌體**。如需有關 WXA 韌體與如何進行更新的詳細資訊，請參閱 *SonicOS 更新*。
操作狀態	顯示 WXA 系列設備的操作狀態: • **叢集就緒** - 綠點表示 WXA 可供叢集使用。 • **運作時間** - WXA 已運行的天數和時數。 • **負載** - WXA 上的滾動平均負載，以百分比表示。
元件	• **TCP 加速** • **WFS 加速** • **已簽署 SMB 的 WFS 延伸支援** • **Web 快取** 顯示加速元件的狀態: • 綠點表示服務正在 WXA 上執行。 • 白點表示服務正在 WXA 上執行，並且可用於加速流量，但是該元件目前在 WXA 的群組設定中為停用。
連線	目前通過 WXA 的連線數量。工具提示也顯示: • 此特殊 WXA 型號支援的連線數上限: • 可存取的同時連線整體授權數。
設定	**編輯**與**刪除**圖示。 **附註：**使用中的 WXA 系列設備無法刪除。
管理	**管理**按鈕，其顯示**管理 WXA** 對話方塊。
探查	**探查**按鈕，其探查 WXA 並更新表格中的統計資料。

主題：

篩選 WXA 表格

依預設，表格中會顯示所有 WXA。您可以將顯示限制為只有選定群組或取消指派的 WXA。

若要篩選 WXA 表格顯示項目:

1 導覽到**系統安裝 > WAN 加速**。

2 從**顯示**中，選取要顯示的項目:

全部（預設值）	顯示所有 WXA
選擇的群組	僅顯示屬於選定群組的 WXA
已取消指派	僅顯示未指派至群組的 WXA

3 如果您已選取**選擇的群組**，請在**群組**表格中，選取包含要顯示之 WXA 的群組。

探查

探查可驗證 WXA 系列設備的存在與狀態，也可以將最新的「群組」設定推送至 WXA 系列設備。您可以探查個別的 WXA 或所有 WXA。

若要探查所有 WXA:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**全部探查**。隨即更新 WXA 表格。

若要探查個別的 WXA:

1 導覽到**系統安裝 > WAN 加速**。

2 在 WXA 表格中，為 WXA 按一下**探查**欄中的**探查**按鈕。隨即更新 WXA 的顯示。

重新整理 WXA 表格

重新整理 WXA 表格會重新整理 WXA 的清單，以及每個 WXA 上不同加速元件的狀態。

若要重新整理 WXA 表格:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**重新整理**圖示。

啟用已簽署 SMB 的 WFS 延伸支援

提示：使用「已簽署 SMB 的 WFS 設定指南」，快速地設定您的已簽署 SMB 的 WFS 延伸支援。若要存取「已簽署 SMB 的 WFS 設定指南」，請按一下 SonicOS 管理介面上的**快速設定**。如需關於本指南的更多資訊，請參閱 *SonicOS 快速設定*。

附註：設定已簽署 SMB 的 WFS 延伸支援是在群組設定外部進行。

當您設定已簽署 SMB 的 WFS 延伸支援時，請選取專用於加速已簽署 SMB 流量的 WXA 系列設備。

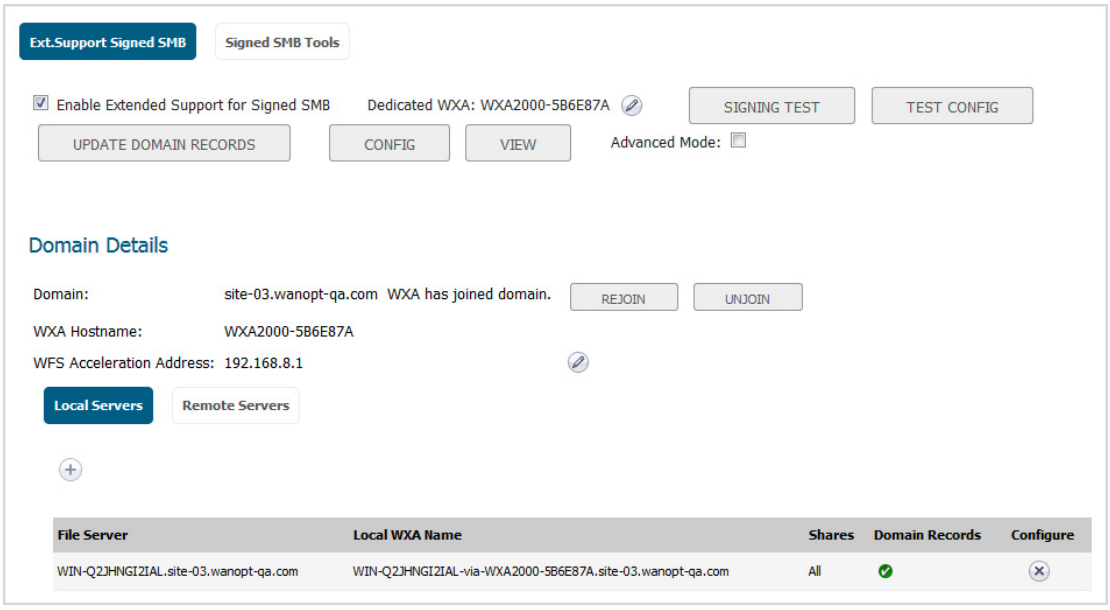
主題：

延伸支援已簽署 SMB

若要設定已簽署 SMB 加速的延伸支援:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

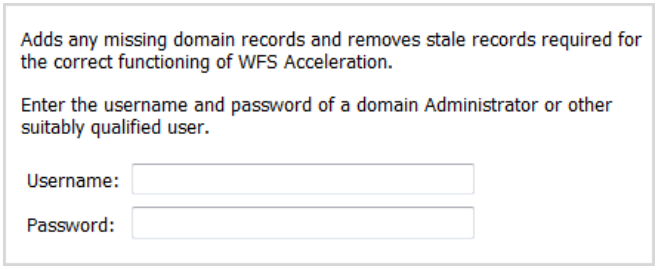


3 選取**啟用已簽署 SMB 的延伸支援**。 預設情況下已核取此選項。

4 按一下**編輯**圖示，以選取專用於延伸支援的 WXA。

> **重要：**變更專用於已簽署 SMB 加速之延伸支援的 WXA，會造成任何使用中工作階段和檔案傳輸終止，因而可能導致資料遺失。
>
> 新的 WXA 必須加入網域且針對相關伺服器和共用設定。使用者裝置的路徑必須變更，以反映新 WXA 的設定。否則，若要維持相同路徑，第一個 WXA 必須先退出網域，而且必須先移除所有網域記錄，才能使用相同的主機名稱與相同設定來設定新的 WXA。

5 按一下**更新網域記錄**，以新增任何缺少的網域記錄並移除 SPN 別名和「受信任進行委派」的陳舊記錄。隨即顯示**更新網域記錄**快顯。

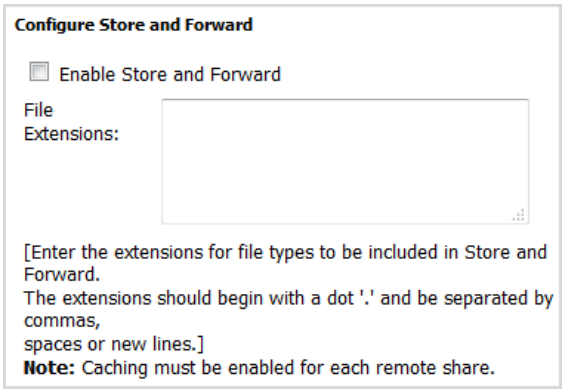


6 分別在**使用者名稱**與**密碼**欄位中，輸入網域管理員的使用者名稱與密碼。

7 按一下**更新記錄**。

8 如果您未使用「儲存與轉送」，請移至步驟 17。

9 若要設定「儲存與轉送」的設定值，請按一下**設定**。隨即顯示**設定儲存與轉送**對話方塊。



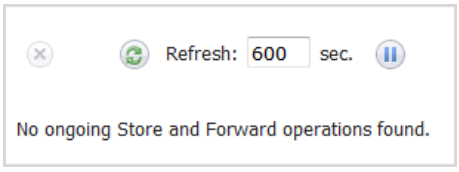
10 選取**啟用儲存與轉送**。 預設情況下未勾選此選項。

11 在**檔案副檔名**欄位中，輸入要儲存與轉送之檔案類型的副檔名。副檔名應以點 (.) 開頭，並以逗號、空格或新行分隔。

附註：每一個遠端共用應啟用快取。

12 按一下**確定**。

13 若要檢視「儲存與轉送」的目前檔案操作，請按一下**檢視**，隨即顯示**儲存與轉送**對話方塊。



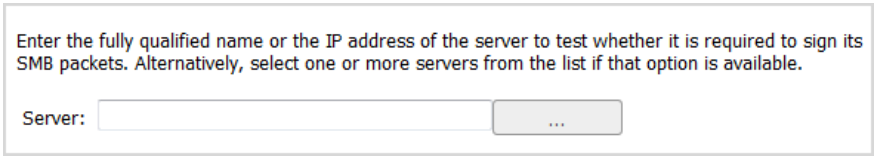
14 結束時間:

- 若要重新整理顯示，請按一下**重新整理**圖示。
- 若要暫停顯示，請按一下**暫停**圖示。

15 若要變更重新整理頻率，請在**重新整理**欄位中輸入頻率。最小時長為 1 秒，最大時長為 999 秒，預設值為 **600** 秒。

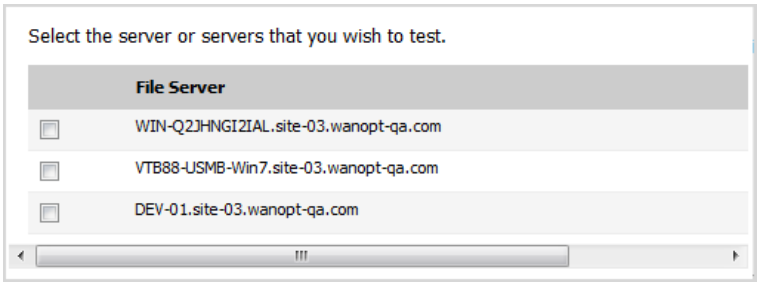
16 如果您不想測試簽署，請移至步驟 24。

17 若要測試特定伺服器的流量是否需要簽署，請按一下**簽署測試**。隨即顯示**簽署測試**對話方塊。



18 您可以

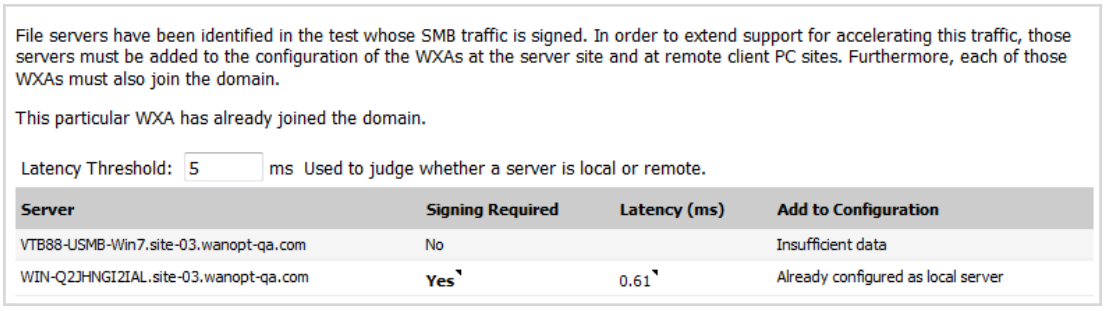
- 輸入要測試之伺服器的完整名稱或 IP 位址。
- 按一下**清單 (...)** 按鈕，以顯示伺服器的清單。隨即顯示**選擇要測試的伺服器**快顯:



19 請選取一個或多個伺服器。

20 按一下**確定**。快顯關閉。

21 按一下**確定**。請耐心等待，可能需要幾分鐘的時間才能顯示測試結果。



重要：如果需要 SMB 簽署，則 WXA 系列設備必須加入網域。測試結果表示 WXA 系列設備是否已加入網域。

提示：如果需要簽署，將滑鼠懸停在工具提示上:

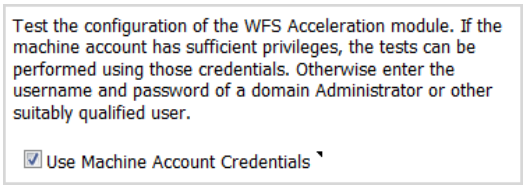
- **是** - 將顯示簽署所需要的位址
- 延遲時間 - 顯示伺服器超過**延遲閾值**中設定的時間。

22 若要指定閾值以確定伺服器是本機或遠端，請在**延遲閾值**中輸入時間 (以毫秒為單位)。最小時長為 1 毫秒，最大為 99999999 毫秒，預設值為 **5** 秒。

23 按一下**確定**。

24 如果您不想測試 WFS 加速模組，請移至步驟 29。

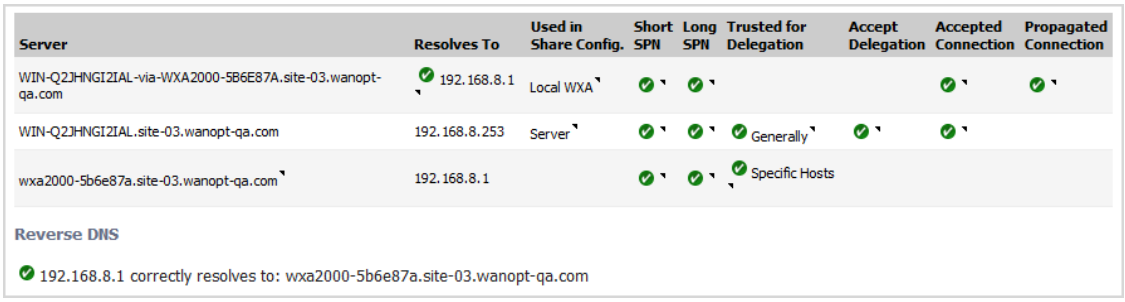
25 若要測試 WFS 加速模組的設定，請按一下**測試設定**。隨即顯示**測試設定**快顯。



26 如果 WXA 系列設備擁有自己的機器帳戶，並具適當權限，請選取**使用機器帳戶憑證**。 預設情況下已核取此選項。

附註：如果 WXA 沒有適當權限，您需要輸入網域管理員的管理員使用者名稱和密碼。

27 按一下**執行測試**。請耐心等待，可能需要幾分鐘的時間才能顯示測試結果。



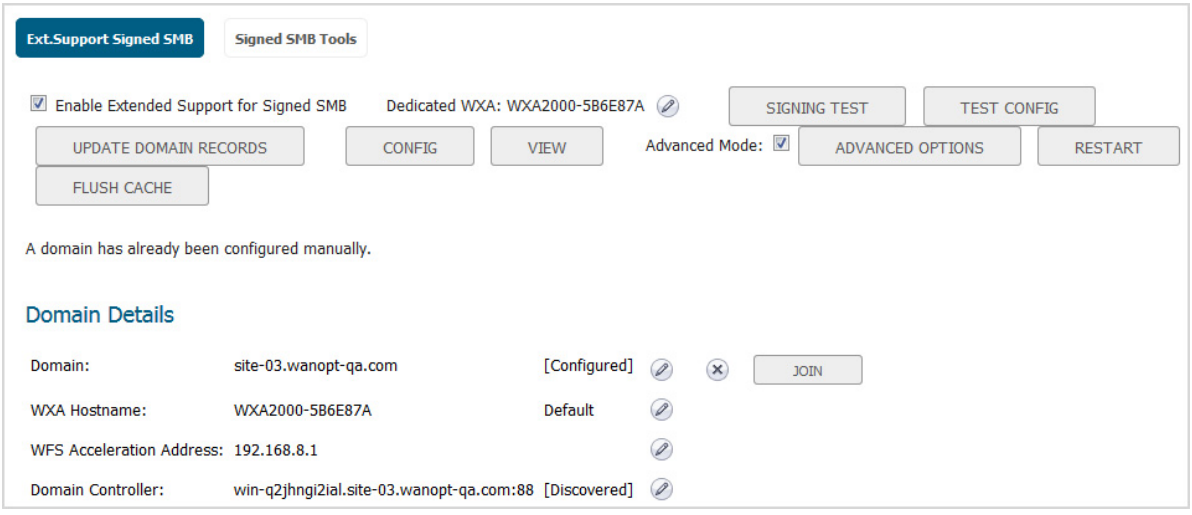
伺服器	伺服器服務主體名稱 (SPN) 已測試
解析為	IP 位址；綠色核取標記表示正確解析
用於共用設定	表示如何使用 SPN 作為名稱以識別設備
短 SPN	表示短 SPN 是否顯示在機器帳戶上
長 SPN	表示長 SPN 是否顯示在機器帳戶上
受信任進行委派	綠色核取標記表示伺服器是否為受信任進行委派: • 一般 - 通常，伺服器是受信任進行委派。 • 特定主機 - 將滑鼠移至工具提示上方，顯示伺服器為受信任進行委派的主機
接受委派	綠色核取標記表示伺服器接受委派；將滑鼠懸停在工具提示上會顯示使用伺服器短名稱或長名稱呈現憑證的主機。
已接受連線	綠色核取標記表示伺服器已接受驗證的連線；將滑鼠懸停在工具提示上會顯示連線。
已傳播連線	綠色核取標記表示伺服器已傳播驗證的連線；將滑鼠懸停在工具提示上會顯示連線。
反向 DNS	顯示反向 DNS 的解析方式

28 按一下**關閉**。

29 若要使用進階模式，請選取**進階模式**。 預設情況下未勾選此選項。

進階模式

選取**進階模式**後，「已簽署 SMB 加速的延伸支援」對話方塊上的選項會隨即變更:



若要設定進階模式:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 選取**進階模式**。這些選項將發生變更。

4 按一下**進階模式**。隨即顯示**進階選項**對話方塊。

5 從**用戶端簽署**中，選取簽署選項用戶端必須使用:

- **自動**（預設）
- **強制**
- **已停用**

6 從**伺服器簽署**中，選取簽署選項伺服器必須使用:

- **自動**（預設）
- **強制**
- **已停用**

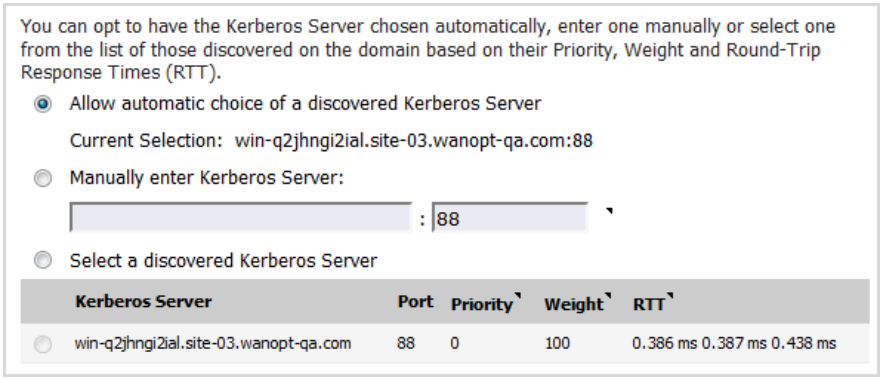
7 在**最大傳輸**欄位中輸入用戶端可傳輸的資料量上限 (以位元為單位)。預設為 **4096**。

8 按一下**確定**。

9 若要重新已簽署 SMB 服務的 WFS 延伸支援，請按一下**重新啟動**。

10 若要排清快取，請按一下**排清快取**。

11 在**網域詳細資料**區段中，按一下**網域控制器**的**編輯**圖示，以設定 Kerberos 伺服器。隨即顯示**設定 Kerberos 伺服器**對話方塊。

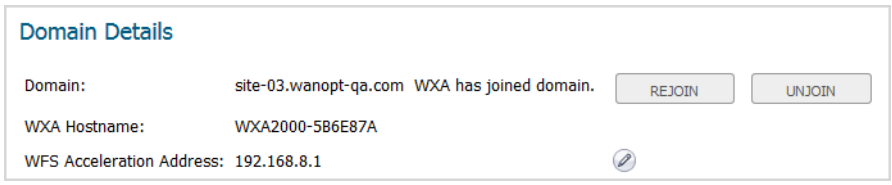


12 指定如何選擇 Kerberos 伺服器:

- **允許自動選擇發現的 Kerberos 伺服器** - 顯示目前選擇及其連接埠。
- **手動輸入 Kerberos 伺服器** - 名稱及連接埠欄位變成可用狀態。
  - 輸入 Kerberos 伺服器的名稱和連接埠，以用於在網域上驗證。
- **選擇已發現的 Kerberos 伺服器** - **Kerberos 伺服器**表格中發現的項目變成可用狀態。
  - 選擇其中一個項目。

13 按一下**確定**。

網域詳細資料



網域	網域名稱及 WXA 是否已加入該網域。
WXA 主機名稱	WXA 的名稱
WFS 加速位址	WFS 加速模組的 IP 位址

主題：

- 第 581 頁「重新加入網域」
- 第 581 頁「退出網域」
- 第 582 頁「正在加入網域」
- 第 582 頁「刪除網域」

重新加入網域

若要重新加入網域:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**重新加入**。

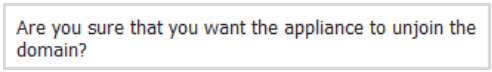
退出網域

若要退出網域:

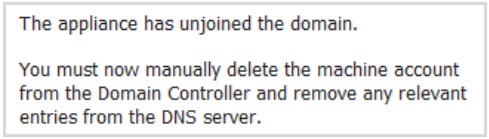
1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**退出**。將顯示確認訊息。



4 按一下**是**。將顯示確認訊息。



5 按一下**確定**。**退出**按鈕會變成**刪除**圖示。

6 從網域控制器手動刪除機器帳戶。

7 將任何相關項目從 DNS 伺服器移除。

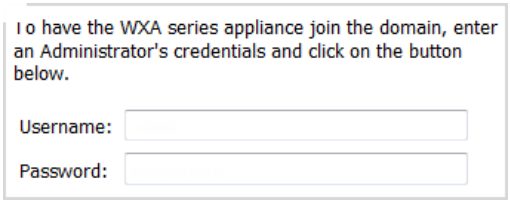
正在加入網域

若要加入網域:

1 導覽到**系統安裝 > WAN 加速**。

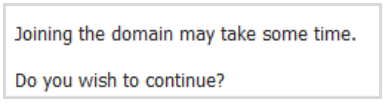
2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**加入**。隨即顯示**加入網域**對話方塊。

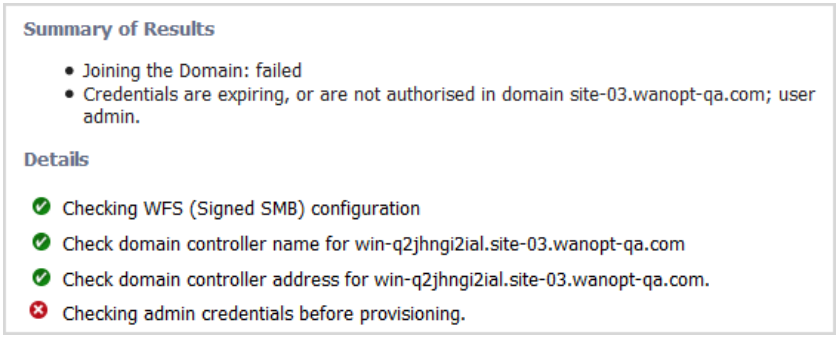


4 分別在**使用者名稱**與**密碼**欄位中，輸入管理員的使用者名稱與密碼。

5 按一下**加入網域**。



6 按一下**是**。**加入網域結果**快顯會顯示是否已成功加入，以及處理程序的詳細資料。



7 按一下**關閉**。

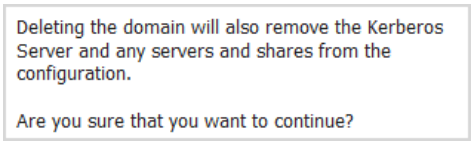
刪除網域

若要刪除網域:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按下 **Delete (刪除)** 圖示。



4 按一下**是**。

本機/遠端伺服器表格

檔案伺服器	檔案伺服器的名稱。
本機 WXA 名稱	本機 WXA 伺服器的名稱。
共用網域記錄	綠色核取標記表示網域記錄是最新的，紅色的 X 表示需要更新記錄。若要更新，請按一下**更新網域記錄**。
設定	顯示**刪除**圖示。

主題：

- 第 583 頁「刪除伺服器」
- 第 583 頁「新增本機檔案伺服器」

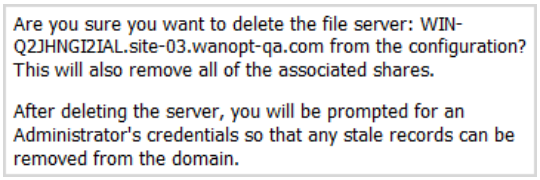
刪除伺服器

若要刪除伺服器:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 在**伺服器**表格中，針對要刪除的伺服器按一下**刪除**圖示。將顯示確認訊息。



4 按一下**刪除**。顯示對話方塊。

5 分別在**使用者名稱**與**密碼**欄位中，輸入管理員的使用者名稱與密碼。

6 按下**確定**

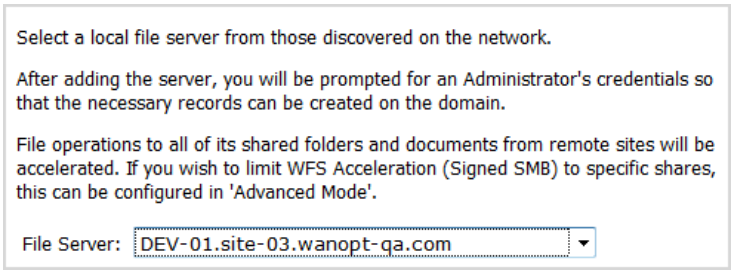
新增本機檔案伺服器

若要新增本機檔案伺服器:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

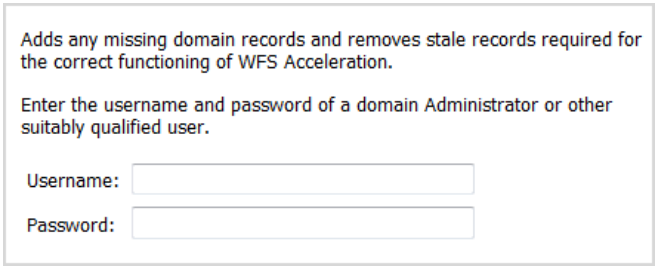
3 在**本機伺服器**下，按一下**新增**圖示。**新增本機檔案伺服器**對話方塊隨即顯示。



4 從**檔案伺服器**選取檔案伺服器。

5 按一下**確定**。

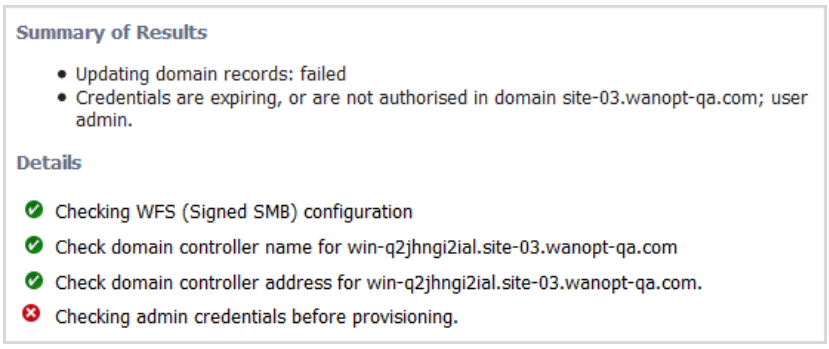
6 隨即顯示**更新網域記錄**對話方塊。



7 分別在**使用者名稱**與**密碼**欄位中，輸入管理員的使用者名稱與密碼。

8 按一下**更新記錄**。

9 按一下**是**。**更新網域結果**快顯會顯示是否已成功加入，以及處理程序的詳細資料。



10 按一下**關閉**。

顯示遠端伺服器

若要顯示伺服器表格中的遠端伺服器:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 在**網域詳細資料**下，按一下「遠端伺服器」。**伺服器**表格會顯示所有設定的遠端伺服器。

新增遠端伺服器

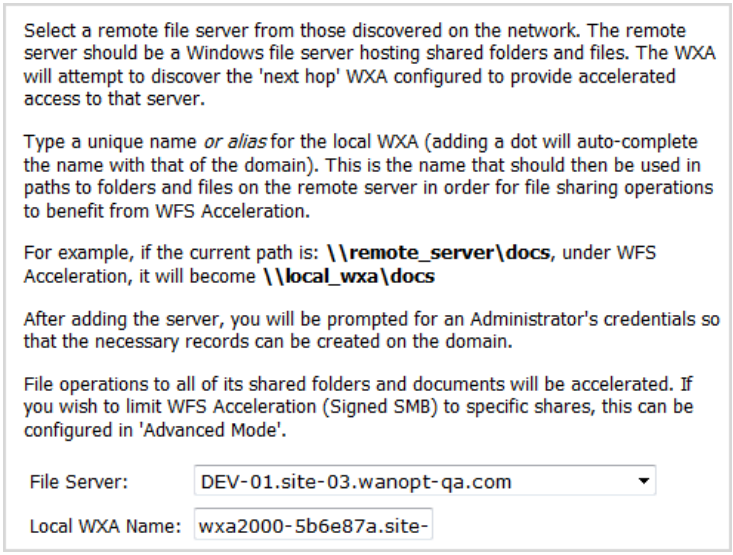
若要新增遠端伺服器:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**遠端伺服器**。**遠端伺服器**表格隨即顯示。

4 在**遠端伺服器**下，按一下**新增**圖示。**新增遠端檔案伺服器**對話方塊隨即顯示。

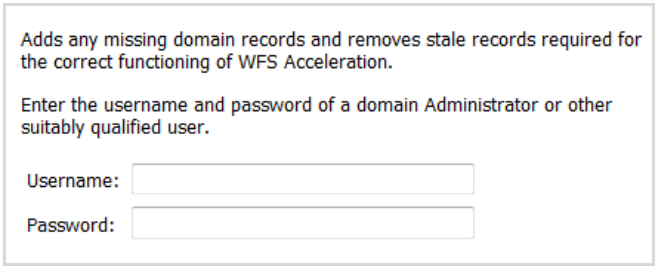


5 從**檔案伺服器**選取檔案伺服器。

6 在**本機 WXA 名稱**欄位中，輸入 WXA 伺服器的唯一名稱或別名。

7 按一下**確定**。

8 隨即顯示**更新網域記錄**對話方塊。



9 分別在**使用者名稱**與**密碼**欄位中，輸入管理員的使用者名稱與密碼。

10 按一下**更新記錄**。

11 按一下**是**。**更新網域結果**快顯會顯示是否已成功加入，以及處理程序的詳細資料。

使用已簽署 SMB 工具

主題：

- 第 586 頁「DNS 名稱查詢」
- 第 586 頁「可用的共用」

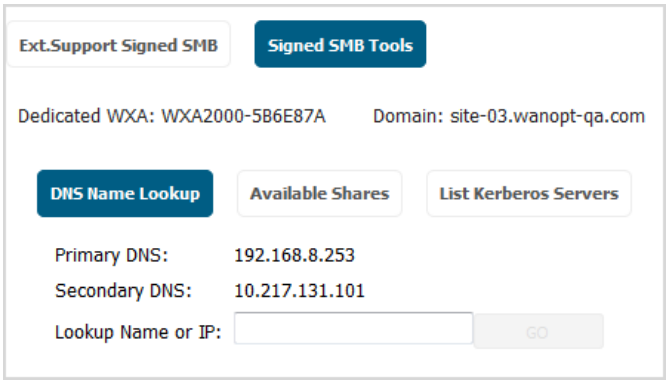
DNS 名稱查詢

若要查詢 DNS 名稱:

1 導覽到**系統安裝 > WAN 加速**。

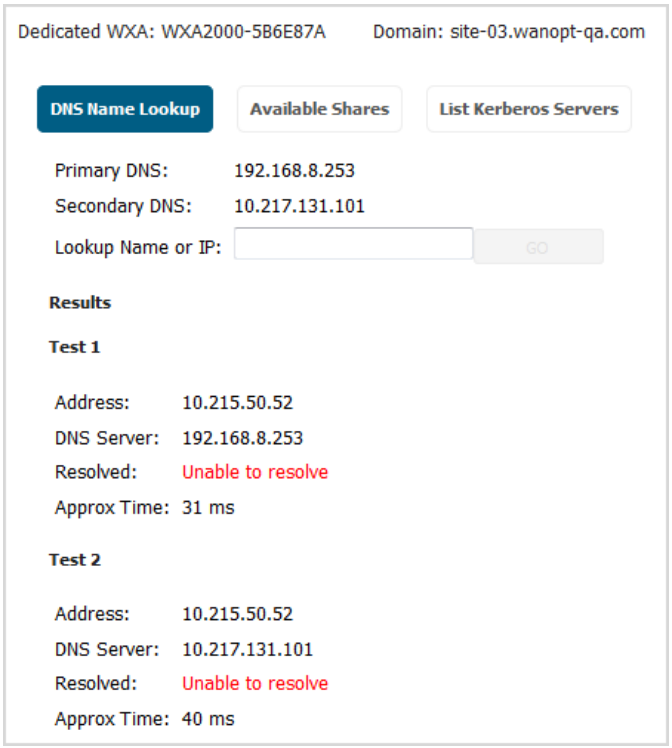
2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**已簽署 SMB 工具**。



4 在**查詢名稱或 IP** 欄位中，輸入要查詢的伺服器。**執行**按鈕會變成可用狀態。

5 按一下**執行**。將顯示結果：



可用的共用

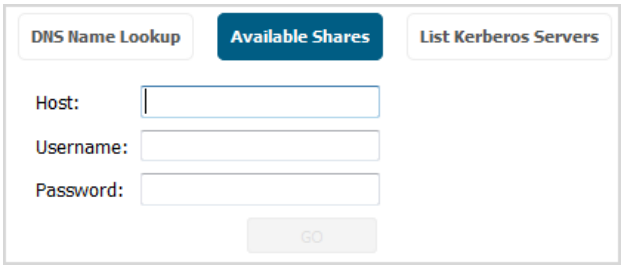
若要查詢可用的共用:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**已簽署 SMB 工具**。

4 按一下**可用的共用**。



5 在**主機**欄位中，輸入要查詢的伺服器。

6 分別在使用者名稱與密碼欄位中，輸入管理員的使用者名稱與密碼。**執行**按鈕會變成可用狀態。

7 按一下**執行**。隨即顯示「可用的共用」快顯。

8 按一下**確定**。

列出 Kerberos 伺服器

若要列出 Kerberos 伺服器:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下**延伸支援已簽署 SMB**，隨即顯示**已簽署 SMB 加速的延伸支援**對話方塊。

3 按一下**已簽署 SMB 工具**。

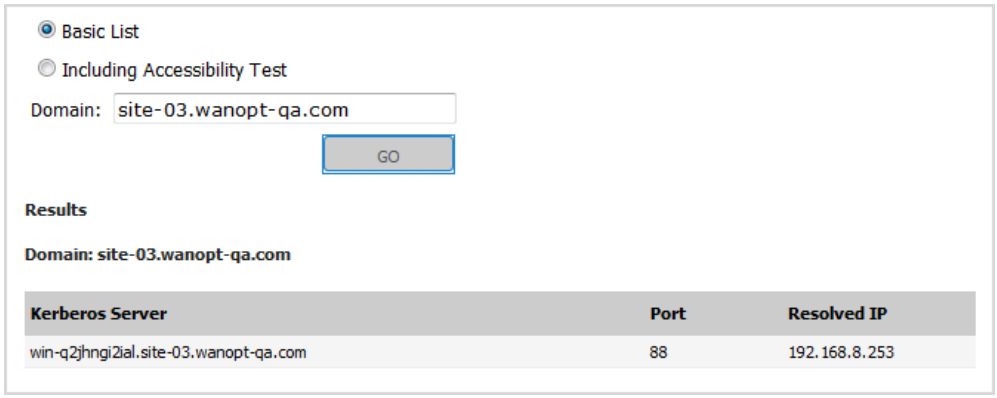
4 按一下**列出 Kerberos 伺服器**。

5 選擇如何列出伺服器:

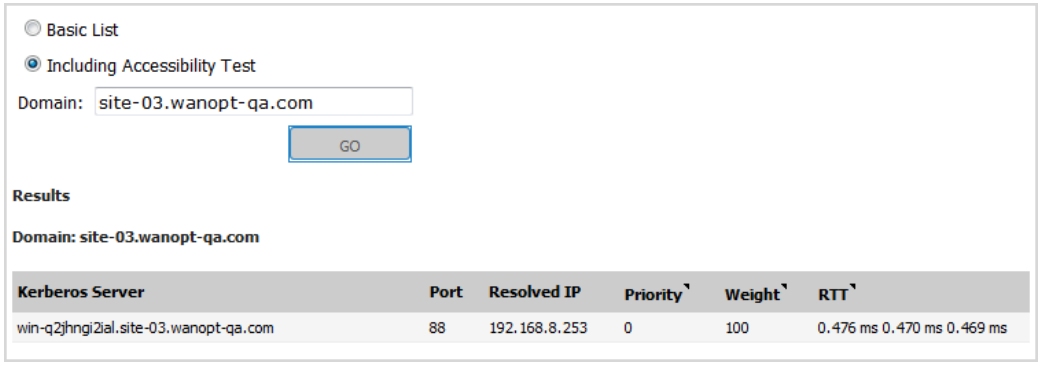
- **基本清單** - 僅顯示 Kerberos 伺服器的連接埠和解析 IP。
- **包含協助工具測試** (預設) - 包含伺服器的優先順序、權重及 RTT。

6 按一下**執行**。結果顯示:

- **基本清單**：



- 包含協助工具測試：



Kerberos 伺服器	Kerberos 伺服器的名稱。
連接埠	Kerberos 伺服器的連接埠。
解析的 IP	伺服器名稱解析的 IP 位址。
優先順序	Kerberos 伺服器的優先順序。慣用較低的值。
權數	Kerberos 伺服器相對權數具有相同的優先順序。慣用較高的值。
RTT	探查 Kerberos 伺服器的來回時間 (RTT)。

為 VPN 原則設定 WXA

VPN 原則表格顯示具有 WXA 加速設定的所有 VPN 原則。

若要針對 VPN 原則編輯 WXA 加速設定:

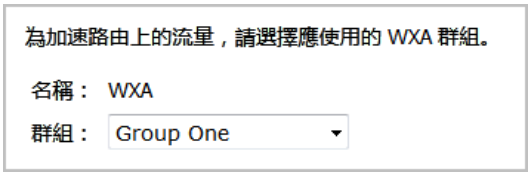
1 導覽到**系統安裝 > WAN 加速**。

2 按一下 **VPN 原則**。

3 若要篩選原則，請從**群組**表格中選取 WXA 群組。

4 從**顯示**中，選取**選擇的群組**。預設值為**全部**。

5 按一下原則的**編輯**圖示。隨即顯示**編輯 VPN** 對話方塊。



6 從**群組**中，選取將套用至 VPN 原則的 WXA 群組。

7 按一下**確定**。

設定 SSL VPN 流量的加速

您可以從 WXAC 用戶端啟用或停用 NetExtender SSL VPN 的加速。

附註：WXA 必須獲得授權，才可支援 NetExtender WAN 加速用戶端 (WXAC)。

若要啟用 WXAC:

1 導覽到**系統安裝 > WAN 加速**。

2 按一下 **SSL VPN**。

3 從**群組**中，選取要啟用之 WXAC 的群組 (預設為**無**)。「接受」按鈕會變成可用狀態。

4 按一下**接受**。

5 目前正在使用的使用中授權數目會顯示在**群組**下拉功能表下。

顯示及編輯 WXA 的路由原則

來源	發出 VPN 流量的閘道。
目的地	VPN 流量的目的地。
註解	設定路由時包含的選擇性註解。
組	套用至路由的群組。
編輯	顯示**編輯**圖示。

若要刪選路由表格中顯示的路由:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格下，從**顯示**中選取特定群組的路由。預設值為**全部**。

若要編輯路由原則:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格下，按一下**路由原則**。

3 針對所需的路由按一下**編輯**圖示 。隨即顯示**編輯路由**快顯。

4 從**群組**中選取要套用的路由。

5 按一下**確定**。

監控群組連線

您可以透過折線圖或橫條 (堆疊) 圖，檢視通過 WXA 的連線數目總計。您也可以檢視特定群組的連線總計。

若要顯示連線:

1 導覽到**系統安裝 > WAN 加速**。

2 在**群組**表格下，按一下**監控**。

> **提示：**您也可以在**群組**表格中，為所需的群組按一下**監控**，以顯示連線。

3 從**群組**中，選取要顯示連線的群組。預設值為**全部**。

4 從**圖表類型**中，選取您希望資料顯示的方式:

- **折線** (預設)
- **堆疊** (橫條)

5 若要放大圖表的選定區域，請將滑鼠游標拖曳到所需的區域。

6 若要將圖表恢復至其預設縮放，請按一下**重設縮放**。

部分 8

VoIP

- 關於 VoIP
- 設定 SonicWall VoIP 功能

38

關於 VoIP

關於 VoIP

主題：

什麼是 VoIP？

IP 語音 (VoIP) 是一組技術的總稱，利用這些技術，語音流量可通過網際網路通訊協定 (IP) 網路傳送。VoIP 將音訊呼叫的語音流轉換為封包，而不是公用電話交換網 (PSTN) 使用的傳統類比電路切換語音通訊。

VoIP 將語音電話和資料合併為單一整合 IP 網路系統，是網路與電信融合的主要推動力量。VoIP 最重要的作用是節省公司成本，它消除了昂貴的冗餘基礎設施和電信服務使用費，同時也提供增強的管理特性和呼叫服務功能。

VoIP 安全性

公司實施 VoIP 技術可以降低通訊成本，並將企業語音服務擴充到分佈於各地的團隊，但語音與資料網路的融合也會帶來安全風險。VoIP 安全性和網路完整性是任何 VoIP 部署的必要部分。

一方面，VoIP 繼承了當今資料網路飽受折磨的安全威脅，另一方面，VoIP 作為一項應用新增到網路上使得這些威脅更加危險。VoIP 元件的新增，給網路安全性提出了新的要求。

VoIP 包括一系列複雜標準，這就為軟體實現中的缺陷和漏洞敞開了大門。困擾現有每一種操作系統和應用程式的各類缺陷和漏洞，同樣適用於 VoIP 裝置。當今許多 VoIP 呼叫伺服器和閘道裝置是基於易受攻擊的 Windows 和 Linux 操作系統而構建。

VoIP 的安全設備需求

VoIP 比基於 TCP/UDP 的標準應用程式更複雜。VoIP 訊號和通訊協定非常複雜，且安全設備通過網路位址轉譯 (NAT) 修改來源位址和來源連接埠資訊時還會引入不一致性，因此 VoIP 難以有效穿越標準安全設備。下面是幾個原因。

- **VoIP 採用兩個單獨的通訊協定工作** - 一個訊號通訊協定（用戶端與 VoIP 伺服器之間）和一個媒體協定（用戶端之間）。媒體通訊協定 (RTP/RTCP) 用於各個工作階段的連接埠/IP 位址對由訊號通訊協定動態交涉。防火牆需要動態追蹤並維護此資訊，為工作階段安全打開選定的連接埠，並在適當的時候關閉連接埠。
- **多個媒體連接埠通過訊號工作階段動態交涉** - 媒體連接埠的交涉包含在訊號通訊協定的有效承載中（IP 位址和連接埠資訊）。防火牆需要對每個封包執行深層檢查以獲取資訊，並動態維持工作階段，因而需要額外的安全設備處理。
- **來源和目的地 IP 位址嵌入 VoIP 訊號封包中** - 支援 NAT 的安全設備在封包的 IP 頭級別轉譯 IP 位址和連接埠。完全對稱的 NAT 安全設備會頻繁調整其 NAT 繫結，且可能任意關閉針孔，使得輸入封包無法傳入其所防護的網路，因而服務供應商將無法向客戶傳送傳入呼叫。為了有效支援 VoIP，NAT 安全設備有必要在封包穿越安全設備時，執行深層封包檢查並轉換其嵌入的 IP 位址和連接埠資訊。
- **不同 VoIP 系統使用不同的訊息格式，防火牆需要處理包含各種訊息格式的訊號通訊協定套件** - 兩家供應商使用相同的通訊協定套件，並不意味著其系統能夠互操作。

為了克服複雜的 VoIP 和 NAT 帶來的眾多障礙，供應商們提供工作階段邊界控制器 (SBC)。SBC 位於安全設備的 Internet 端，試圖通過終止並重新發起所有 VoIP 媒體和訊號流量來控制 VoIP 網路的邊界。對於不支援 VoIP 的安全設備，SBC 本質上充當 VoIP 流量的代理。SonicWall 安全設備是支援 VoIP 的安全設備，因而網路上無需 SBC。

附註：只要 VoIP 應用程式符合 RFC 標準，所有可執行 SonicWall 6.2 的 SonicOS 裝置上都支援 VoIP。

VoIP 通訊協定

VoIP 技術基於兩個主要通訊協定：H.323 與 SIP。這些通訊協定可全域套用，或依各防火牆規則套用。

主題：

H.323

H.323 是國際電信聯盟 (ITU) 制定的一項標準。它是一個全面的通訊協定套件，適用於電腦、終端、網路裝置、網路服務之間的語音、視訊及資料通訊。H.323 旨在支援使用者通過私人 IP 網路和 Internet 等無連接封包切換網路進行點到點多媒體通話。H.323 受到視訊會議裝置、VoIP 裝置、Internet 電話軟體和裝置的製造商廣泛支援。

H.323 訊號採用 TCP 和 UDP 的結合，訊息編碼採用 ASN.1。H.323v1 於 1996 年發佈，H.323v5 於 2003 年發佈。作為一項古老的標準，H.323 為許多早期 VoIP 供應商所接受。

H.323 網路由四類不同的實體組成：

- **終端** - 用於多媒體通訊的用戶端點。例如，支援 H.323 的 Internet 電話或 PC。
- **Gatekeeper** - 執行服務以完成呼叫建立和拆卸，並註冊 H.323 終端進行通訊。包含：

- 位址轉譯
- 註冊、許可控制和狀態 (RAS)
- Internet 定位服務 (ILS) 也屬此類（但它不是 H.323 的一部分）。ILS 使用 LDAP（輕型目錄存取通訊協定），而非 H.323 訊息。

- **多點控制單元 (MCU)** - 用於終端間多點通訊的會議控制和資料指派。
- **閘道** - H.323 網路與其它通訊服務（如電路切換公用電話交換網 (PSTN) 等）之間的互操作。

SIP

工作階段起始通訊協定 (SIP) 標準由網際網路工程任務組 (IETF) 制定。RFC 2543 發佈於 1999 年 3 月。RFC 3261 發佈於 2002 年 6 月。SIP 是一種用於起始、管理、終止工作階段的訊號通訊協定。SIP 支援「存在」和行動性，可在使用者資料包通訊協定 (UDP) 和傳送控制通訊協定 (TCP) 上執行。

使用 SIP，VoIP 用戶端可以發起和終止呼叫工作階段，邀請成員加入會議工作階段，以及執行其它電話任務。SIP 還支援私人交換器 (PBXs)、VoIP 閘道和其它通訊裝置以標準化協作方式通訊。SIP 的另一個設計目的是避免像 H.323 那樣產生繁重的開銷。

SIP 網路由如下邏輯實體組成：

- **使用者代理 (UA)** - 發起、接收、終止呼叫。
- **代理伺服器** - 代表 UA 轉送或回應請求。代理伺服器可將請求傳送給多個伺服器。背靠背使用者代理 (B2BUA) 是一類代理伺服器，它將通過其中的呼叫的每一段視為兩個不同的 SIP 呼叫工作階段：一個是它與主叫方之間的工作階段，另一個是它與被叫方之間的工作階段。其它代理伺服器則將同一呼叫的所有段視作單一 SIP 呼叫工作階段。
- **重新導向伺服器** - 回應請求但不轉送請求。
- **註冊伺服器** - 處理 UA 身分驗證和註冊。

SonicWall 的 VoIP 功能

主題：

VoIP 安全性

- **流量有效性** - 對穿越安全設備的每一個 VoIP 訊號和媒體封包進行狀態檢查，確保流量有效。設計封包來利用實現方案中的漏洞，以在目的地裝置中引起緩衝區溢出等後果，是許多攻擊者的慣用攻擊方式。SonicWall 安全設備可偵測到格式錯誤和無效的封包並予以丟棄，使其無法到達預定的目標裝置。

- **VoIP 通訊協定的應用層防護** - 通過 SonicWall 防入侵服務 (IPS) 實現全面的應用級別 VoIP 防護 。IPS 整合一個可設定的高效能掃描引擎和一個動態更新並設定的攻擊與漏洞簽章資料庫，可防範複雜的特洛伊木馬和多態病毒對網路的威脅。SonicWall 利用一系列 VoIP 專用簽章擴充其 IPS 簽章資料庫，從而封鎖惡意流量到達受防護的 VoIP 電話和伺服器。
- **DoS 和 DDoS 攻擊防禦** - 防範 DoS 和 DDoS 攻擊，如同步攻擊 (SYN Flood)、死亡之 Ping (Ping of Death) 和 LAND (IP) 攻擊等，這些攻擊旨在停用網路或服務。
  - 利用 TCP 審核 VoIP 訊號封包的順序，封鎖視窗以外的無序和重傳封包。
  - 使用隨機化 TCP 序號（由加密隨機數發生器在連接建立期間產生）審核各 TCP 工作階段中的資料流，防範重放和資料插入攻擊。
  - 利用同步攻擊防禦確保攻擊者無法通過開啟許多 TCP/IP 連接（這些連接無法完全建立，原因一般是其使用欺騙性來源位址）來攻擊伺服器。
- **狀態監控** - 狀態監控確保封包（即使其本身看起來有效）與其相關 VoIP 連接的目前狀態相稱。
- **加密 VoIP 裝置支援** - SonicWall 支援能夠利用加密來防護 VoIP 對話中的媒體交換的 VoIP 裝置，或不支援加密媒體但利用 IPsec VPN 來防護 VoIP 呼叫的安全 VoIP 裝置。
- **應用層防護** - SonicWall 通過 SonicWall 防入侵服務 (IPS) 提供全面的應用級別 VoIP 防護。SonicWall IPS 基於一個可設定的高效能深層封包檢查引擎，可為關鍵網路服務，包括 VoIP、Windows 服務和 DNS 等提供增強的防護。SonicWall 的深層封包檢查引擎使用可擴充簽章語言，還能主動防護新發現的應用程式和通訊協定的漏洞。利用不同的簽章粒度，SonicWall IPS 可以基於全球、攻擊組或單個簽章來偵測和防禦攻擊，提供最大的靈活性並控制誤報。

VoIP 網路

- **無線區域網路 (WLAN) 上的 VoIP** - SonicWall 利用分布式無線解決方案將全部 VoIP 安全性擴充到相連的無線網路。與 SonicWall 背後的有線網路相連的 VoIP 裝置所具有的全部安全特性，使用無線網路的 VoIP 裝置同樣擁有。

  附註：SonicWall 的安全無線解決方案包括必要的網路支援手段，可將安全 VoIP 通訊擴充到無線網路。欲瞭解詳細資料，請參閱 SonicWall 網站 http://www.sonicwall.com 上提供的「SonicWall 安全無線網路整合解決方案指南」。

- **頻寬管理 (BWM) 和服務品質 (QoS)** - 頻寬管理（入口和出口）可用來確保有頻寬可用於時間敏感的 VoIP 流量。BWM 整合到 SonicWall 服務品質 (QoS) 特性中，提供對某些類型應用至關重要的預測能力。
- **WAN 冗餘和負載平衡** - WAN 冗餘和負載平衡允許一個介面充當次要 WAN 連接埠。此次要 WAN 連接埠可用於簡單的主動/被動設定，僅當主要 WAN 連接埠關閉或無法使用時，流量才會通過次要連接埠路由。基於目的地拆分流量的路由，可以實現負載平衡。
- **高可用性** - 高可用性由 SonicOS 的高可用性來保障，即使發生系統故障，也能確保可靠、連續的連接。

VoIP 網路互操作性

- **VoIP 裝置的即插即防護支援** - SonicOS 能夠自動處理 VoIP 裝置的增加、變更和移除，確保沒有一個 VoIP 裝置不受防護。利用先進的監控和追蹤技術，一旦有 VoIP 裝置插入安全設備背後的網路，就會自動將其防護起來。

- **對所有 VoIP 訊號封包進行全面的語法審核** - 接收到的訊號封包會在 SonicOS 中進行全面的解析，確保其符合相關標準定義的語法。通過執行語法審核，安全設備可確保畸形封包無法通過，防止其對目的地裝置產生有害影響。
- **支援動態建立和追蹤媒體流** - SonicOS 追蹤每個 VoIP 呼叫，從請求建立呼叫的第一個訊號封包從呼叫結束時。只有基於成功的呼叫進度，主叫方與被叫方之間才會開啟更多連接埠（用於其它訊號和媒體交換）。

  作為呼叫建立的一部分而交涉的媒體連接埠由安全設備動態指派。後續呼叫，即使在相同的各方之間，也會使用不同的連接埠，從而挫敗可能正在監控特定連接埠的攻擊者。要求的媒體連接埠僅在呼叫完全連接時開啟，並在呼叫終止時關閉。將丟棄試圖使用呼叫範圍以外連接埠的流量，從而為安全設備背後的 VoIP 裝置提供額外的防護。
- **審核所有媒體封包的標頭** - SonicOS 檢查並監控媒體封包內的標頭，允許偵測和丟棄無序和重傳封包（視窗以外）。此外，通過確保有效標頭存在，可以偵測並丟棄無效的媒體封包。通過追蹤媒體流和訊號，SonicWall 為整個 VoIP 工作階段提供防護。
- **訊號和媒體的可設定非使用中逾時** - 為確保丟棄的 VoIP 連接不會無限期保持開啟，SonicOS 監控 VoIP 工作階段相關的訊號和媒體流的使用。將關閉空閑時間超過所設定的逾時時間的流，防止潛在的安全漏洞。
- **SonicOS 允許管理員控制來電** - SonicOS 要求所有來電都由 H.323 Gatekeeper 或 SIP 代理授權並進行身分驗證，以便封鎖未經授權的來電和垃圾電話。這樣，管理員便可確保 VoIP 網路僅用於公司授權的那些呼叫。
- **全面的監控和報告** - 針對所有支援的 VoIP 通訊協定，SonicOS 提供許多監控和故障排除工具：
  - 使用中 VoIP 呼叫的動態即時報告，顯示主叫方和被叫方以及所用的頻寬。
  - 所有 VoIP 呼叫的審核記錄，顯示主叫方和被叫方、通話時長以及所用的總頻寬。記錄看到的異常封包（例如不良回應），詳細顯示相關各方和看到的狀況。
  - 詳細的 syslog 報告以及 VoIP 訊號和媒體流的 ViewPoint 報告。SonicWall ViewPoint 是一個基於 Web 的圖形化報告工具，它根據從安全設備收到的 syslog 資料流，提供關於安全和網路使用中的詳盡細緻的報告。幾乎可以針對安全設備活動的任何方面產生報告，包括各使用者或群組的使用模式、特定安全設備或安全設備群組上發生的事件、攻擊的類型和時間、資源消耗和限制等。

支援的介面

下列 SonicOS 區域支援 VoIP 裝置：

- 受信區域（LAN、VPN）
- 不受信區域 (WAN)
- 公用區域 (DMZ)
- 無線區域 (WLAN)

支援的 VoIP 通訊協定

主題：

- 第 598 頁「H.323」
- 第 598 頁「SIP」
- 第 598 頁「SonicWall VoIP 供應商互操作性」

- 第 599 頁「編解碼器」
- 第 599 頁「SonicOS 不執行深層封包檢查的 VoIP 通訊協定」

H.323

SonicOS 為 H.323 提供如下支援：

- 支援執行 H.323 所有版本（目前為 1 至 5）的 VoIP 裝置
- Microsoft 基於 LDAP 的 Internet 定位服務 (ILS)
- LAN H.323 終端使用多點傳送發現 Gatekeeper
- Gatekeeper 註冊、許可和狀態 (RAS) 訊息的狀態監控與處理
- 支援對媒體流進行加密的 H.323 終端
- DHCP 選項 150。DHCP 伺服器可設定為向 DHCP 用戶端返回 VoIP 特定 TFTP 伺服器的位址
- 除了支援 H.323 以外，SonicOS 還支援採用如下附加 ITU 標準的 VoIP 裝置：
    - T.120，用於應用程式共用、電子白板、檔案交換和聊天
    - H.239，允許通過多個頻道傳送音訊、視訊和資料
    - H.281，用於遠端攝影機控制 (FECC)

SIP

SonicOS 為 SIP 提供如下支援：

- SIP 基礎標準（RFC 2543 和 RFC 3261）
- SIP INFO 方法 (RFC 2976)
- SIP 中臨時回應的可靠性 (RFC 3262)
- SIP 專用事件通知 (RFC 3265)
- SIP UPDATE 方法 (RFC 3311)
- SIP 伺服器的 DHCP 選項 (RFC 3361)
- SIP 即時訊息擴充 (RFC 3428)
- SIP REFER 方法 (RFC 3515)
- SIP 對稱回應路由擴充 (RFC 3581)

SonicWall VoIP 供應商互操作性

與 SonicWall VoIP 互操作的部分裝置清單表格列出可與 SonicWall VoIP 交互操作的主要領導製造商的許多裝置。

與 SonicWall VoIP 互操作的部分裝置清單

H.323	SIP
軟體電話： Avaya Microsoft NetMeeting OpenPhone PolyCom SJLabs SJ Phone 電話/可視電話： Avaya Cisco D-Link PolyCom Sony Gatekeeper： Cisco OpenH323 Gatekeeper 閘道： Cisco	軟體電話： Apple iChat Avaya Microsoft MSN Messenger Nortel Multimedia PC Client PingTel Instant Xpressa PolyCom Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP User Agent 電話/ATA： Avaya Cisco Grandstream BudgetOne Mitel Packet8 ATA PingTel Xpressa PolyCom PolyCom Pulver Innovations WiSIP SoundPoint SIP 代理/服務： Cisco SIP Proxy Server Brekeke Software OnDo SIP Proxy Packet8 Siemens SCS SIP Proxy Vonage

編解碼器

- **SonicOS 支援來自任何編解碼器的媒體流** - 媒體流攜帶由 VoIP 裝置內的硬體/軟體編解碼器（編碼器和解碼器）處理的音訊和視訊信號。編解碼器利用編碼和壓縮技術減少表示音訊/視訊信號所需的資料量。編解碼器的一些範例如下：
  - H.264、H.263 和 H.261（視訊）
  - MPEG4、G.711、G.722、G.723、G.728、G.729（音訊）

SonicOS 不執行深層封包檢查的 VoIP 通訊協定

SonicWall 網路安全裝置目前不支援下列通訊協定的深層封包檢查，因此，這些協定只應用在非 NAT 環境下。

- H.323 或 SIP 的專有擴充
- MGCP
- Megaco/H.248
- Cisco 瘦小用戶端控制通訊協定 (SCCP)
- IP-QSIG
- 專有通訊協定（Mitel MiNET、3Com NBX 等）

BWM 和 QoS

VoIP 的最大挑戰之一是確保通過 IP 網路提供高品質語音通話。IP 主要設計用於傳送可以容忍延遲的異步資料流量。但是，VoIP 對延遲和丟包非常敏感。管理接入和設定流量優先順序是確保高品質即時 VoIP 通訊的重要要求。

SonicWall 的整合頻寬管理 (BWM) 和服務品質 (QoS) 特性提供了用於管理 VoIP 通訊的可靠性和品質的工具。

服務品質

QoS 包括多種方法，目的是提供可預測的網路行為和效能。網路可預測性對於 VoIP 和其他關鍵性應用程式至關重要。再多的頻寬也無法提供這種可預測性，因為網路最終將用盡任何數量的頻寬。只有正確設定並實作 QoS，才能妥善管理流量，保證網路服務達到所需的層級。

SonicOS 的 QoS 特性還能識別、對應、修改、產生工業標準 802.1p 和區分服務代碼點 (DSCP) 服務類別 (CoS) 標誌符。

SonicOS 如何處理 VoIP 呼叫

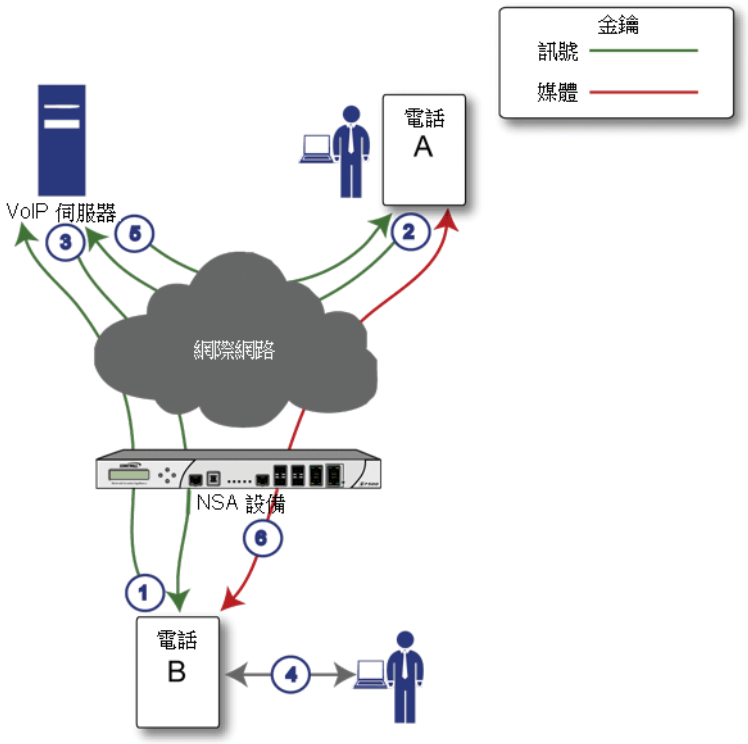
SonicOS 為所有 VoIP 呼叫情況提供高效且安全的解決方案。下面是 SonicOS 如何處理 VoIP 呼叫流程的一些例子：

- 第 600 頁「來電」
- 第 601 頁「本機呼叫」

來電

來電事件順序顯示了來電期間發生的事件順序。

來電事件順序



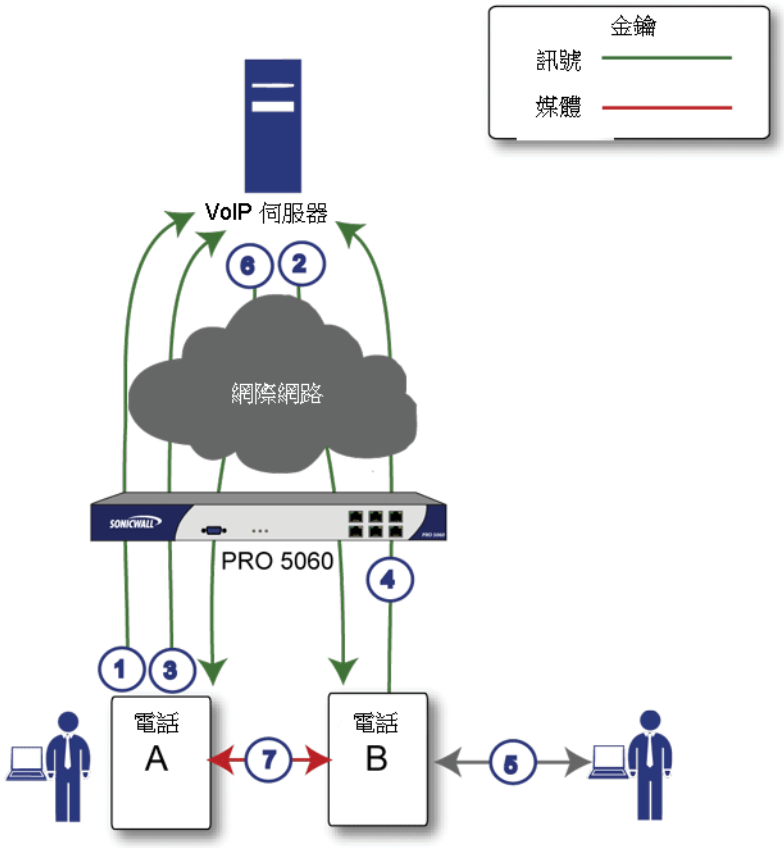
下面說明來電事件順序所示的事件順序：

1. **電話 B 在 VoIP 伺服器中註冊** - 安全設備通過監控傳出的 VoIP 註冊請求，建立可接入 IP 電話的資料庫。SonicOS 在電話 B 的私人 IP 位址和註冊訊息中使用的安全設備公用 IP 位址之間進行轉譯。VoIP 伺服器不知道電話 B 位於安全設備之後，並有一個私人 IP 位址 - 它會將電話 B 與安全設備的公用 IP 位址建立關聯。
2. **電話 A 發起對電話 B 的呼叫** - 電話 A 使用電話號碼或別名發起對電話 B 的呼叫。傳送此資訊到 VoIP 伺服器時，它還會提供有關其支援的媒體類型和格式的詳細資料，以及對應的 IP 位址和連接埠。
3. **VoIP 伺服器審核呼叫請求並向電話 B 傳送請求** - VoIP 伺服器向安全設備的公用 IP 位址傳送呼叫請求。當它到達安全設備時，SonicOS 會驗證請求的來源和內容。然後，安全設備會確定電話 B 的私人 IP 位址。
4. **電話 B 振鈴並接聽** - 當電話 B 接聽時，它會返回資訊到 VoIP 伺服器，告知其支援的媒體類型和格式，以及對應的 IP 位址和連接埠。SonicOS 轉譯此私人 IP 資訊以使用安全設備的公用 IP 位址，並將訊息傳送到 VoIP 伺服器。
5. **VoIP 伺服器將電話 B 的媒體 IP 資訊返回到電話 A** - 電話 A 現在擁有足夠資訊來開始與電話 B 交換媒體。電話 A 不知道電話 B 位於安全設備之後，因為它得到的是 VoIP 伺服器提供的安全設備公用位址。
6. **電話 A 和電話 B 通過 VoIP 伺服器交換音訊/視訊/資料** - 利用內部資料庫，SonicOS 確保媒體僅來自電話 A，且僅使用電話 B 允許的指定媒體流。

本機呼叫

本機 VoIP 來電事件順序顯示了本機 VoIP 呼叫期間發生的事件順序。

本機 VoIP 來電事件順序



下面說明本機 VoIP 來電事件順序所示的事件順序：

1 **電話 A 和電話 B 在 VoIP 伺服器中註冊** - 安全設備通過監控傳出的 VoIP 註冊請求，建立可接入 IP 電話的資料庫。SonicOS 在電話的私人 IP 位址和安全設備公用 IP 位址之間進行轉譯。VoIP 伺服器不知道電話位於安全設備之後。它將同一 IP 位址與這兩部電話關聯，但連接埠號不同。

2 **電話 A 通過向 VoIP 伺服器傳送一個請求來發起對電話 B 的呼叫** - 即使它們位於同一安全設備之後，電話 A 也不知道電話 B 的 IP 位址。電話 A 使用電話號碼或別名發起對電話 B 的呼叫。

3 **VoIP 伺服器驗證呼叫請求並向電話 B 傳送請求** - VoIP 伺服器向安全設備的公用 IP 位址傳送呼叫請求。然後，安全設備確定電話 B 的私人 IP 位址。

4 **電話 B 振鈴並經接聽** - 當電話 B 經接聽時，安全設備會轉譯其私人 IP 資訊以使用安全設備的公用 IP 位址，並將訊息傳送到 VoIP 伺服器。

5 **VoIP 伺服器將電話 B 的媒體 IP 資訊返回到電話 A** - SonicOS 將訊息中的被叫方和主叫方資訊均轉譯回電話 A 和電話 B 的專用位址和連接埠。

6 **電話 A 和電話 B 直接交換音訊/視訊/資料** - 安全設備在這兩部電話直接通過 LAN 直接路由流量。兩部電話直連可降低傳送資料到 VoIP 伺服器的頻寬要求，並且無需安全設備執行位址轉譯。

39

設定 SonicWall VoIP 功能

設定任務

針對 VoIP 部署設定 SonicWall 安全設備是以 SonicWall 管理介面中的基本網路設定為基礎。本節假設安全設備已針對網路環境進行設定。

附註：如需 VoIP 的一般資訊，請參見第 593 頁「關於 VoIP」。

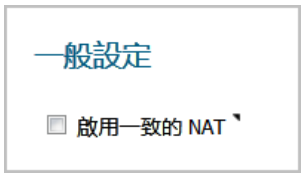
主題：

設定 VoIP

您可透過**管理 | 系統設定 | VOIP** 上的設定來設定 VoIP。此頁面分為三個部分：**一般設定**、**SIP 設定**和 **H.323 設定**。

主題：

一般設定



一般設定下方有一個選項：啟用一致的 NAT。

一致的 NAT 增強標準的 NAT 原則，為需要連接一致的 IP 位址的對等應用程式（如 VoIP）提供更好的相容性。一致的 NAT 使用 MD5 雜湊方法始終為每個內部專用 IP 位址和連接埠對指定相同的對應公用 IP 位址和 UDP 連接埠對。

例如，NAT 會將私人 (LAN) IP 位址和連接埠對（192.116.168.10/50650 和 192.116.168.20/50655）轉譯為公用 (WAN) IP/連接埠對，如 IP 位址和連接埠對表格所示：

IP 位址和連接埠對

私人 IP/連接埠	轉譯的公用 IP/連接埠
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

啟用一致的 NAT 後，來自主機 192.116.168.10 或 192.116.168.20（使用 IP 位址和連接埠對表格相同的連接埠）的所有後續請求將導致使用相同的轉譯過的位址和連接埠對。沒有一致的 NAT，連接埠以及可能包括 IP 位址都會在每次請求時發生變化。

附註：啟用一致的 NAT 會導致整體安全性略微降低，因為位址和連接埠對的可預測性增強。大部分基於 UDP 的應用程式與傳統的 NAT 相容。因此，除非您的網路使用需要一致的 NAT 的應用程式，否則不要啟用它。

啟用一致的 NAT

啟用一致的 NAT 的步驟是：

1 選擇**啟用一致的 NAT** 選項。預設情況下未勾選此選項。

2 按一下**接受**。

SIP 設定

預設情況下，SIP 用戶端在其傳送給 SIP 代理的 SIP（工作階段起始通訊協定）工作階段定義通訊協定 (SDP) 訊息中使用私人 IP 位址。如果 SIP 代理位於防火牆的公用 (WAN) 端，SIP 用戶端位於防火牆的私人 (LAN) 端，則不會轉譯 SDP 訊息，SIP 代理無法到達 SIP 用戶端。

啟用 SIP

啟用 SIP 的步驟如下：

1 導覽至**管理 | 系統設定 | VOIP | SIP 設定**。

2 選擇要全域啟用 SIP 轉換或根據防火牆規則來啟用:

- **使用全域控制以啟用 SIP 轉換**。預設情況下已核取此選項。
- **使用防火牆規則型控制以啟用 SIP 轉換**。請確保設定防火牆規則以控制 SIP 轉換，如 *SonicOS 原則中所述*。

3 如果您未設定 SIP 轉換，請移至步驟 12。

4 預設未勾選**啟用 SIP 轉譯**。選擇此選項的目的是：

- 在 LAN（受信）與 WAN/DMZ（不受信）之間轉換 SIP 訊息。

  若希望安全設備執行 SIP 轉換，則需要檢查此設定。如果 SIP 代理位於安全設備的公用 (WAN) 端，SIP 用戶端位於 LAN 端，則 SIP 用戶端在傳送給 SIP 代理的 SIP/工作階段定義通訊協定 (SDP) 訊息中會預設嵌入/使用私人 IP 位址，因而不會改變這些訊息，SIP 代理不知道如何回應安全設備之後的用戶端。

- 使安全設備能夠瀏覽各條 SIP 訊息，變更私人 IP 位址和指派的連接埠。
- 控制並開啟 RTP/RTCP 連接埠，為使 SIP 工作階段呼叫發生，必須開啟這些連接埠。

NAT 轉譯第 3 層位址，但不轉譯第 7 層 SIP/SDP 位址，這就是需要選擇**啟用 SIP 轉譯**以轉換 SIP 訊息的原因。

> **提示：**一般而言，應該選取**啟用 SIP 轉換**，除非其他 NAT 穿越解決方案要求關閉此功能。SIP 轉換以雙向模式工作，會轉換 LAN 與 WAN 之間的往來訊息。

選擇**啟用 SIP 轉譯**後，其他選項可用。

5 若要在以 TCP 為基礎的 SIP 工作階段執行 SIP 轉換，請選取**在 TCP 連線上啟用 SIP 轉換**。 預設情況下已核取此選項。

6 針對**服務物件中的 TCP/UDP 連接埠**從執行轉換選取服務物件。預設值為 **SIP**。

7 選擇**允許信令連接埠傳輸非 SIP 封包**以支援 Apple iChat 和 MSN Messenger 等應用程式，這些程式使用 SIP 訊號連接埠傳送其它專有訊息。預設情況下未勾選此選項。

> **重要：**勾選此核取方塊可能會使網路遭受畸形或無效 SIP 流量引起的惡意攻擊。

8 如果將 SIP 代理伺服器用作 B2BUA，啟用**啟用 SIP 背對背使用者代理 (B2BUA) 支援**設定。預設停用此選項，僅當安全設備可看到語音呼叫的兩段時（例如，LAN 上的一部電話呼叫 LAN 上的另一部電話），方可啟用此選項。

> **提示：**如果防火牆不可能看到語音呼叫的兩段（例如，只能撥打或接聽 WAN 上的電話時），則應停用**啟用 SIP 背對背使用者代理 (B2BUA) 支援**設定，以避免不必要的 CPU 使用。

9 使用 **SIP 信令非使用狀態逾時（秒數）**和 **SIP 媒體非使用狀態逾時（秒數）**選項，定義呼叫可以處於空閒狀態（無流量交換）的時間量，經過此時間後，防火牆就會封鎖後續流量。將呼叫置於保持時，便進入空閒狀態。指定下列情況的閒置時間上限:

- **SIP 訊號非使用狀態逾時**中沒有要交換的訊號 (控制) 訊息。 最短時間為 30 秒，最長時間為 1000000 秒 (約 1.2 天)，預設值為 **3600** 秒 (60 分鐘)。
- **SIP 媒體非使用中逾時**中沒有要交換的媒體 (例如，音訊或視訊) 封包。最短時間為 30 秒，最長時間為 3600 秒 (1 小時)，預設值為 **120** 秒 (2 分鐘)。

10 使用**用於轉換的其它 SIP 訊號連接埠 (UDP)**設定，指定非標準 UDP 連接埠用於承載 SIP 訊號流量。一般情況下，SIP 訊號流量通過 UDP 連接埠 5060 承載。但是，某些商用 VOIP 服務使用其它連接埠，例如 1560。此設定不為零時 (**0** 為預設值；最大值為 65535)，安全設備可在這些非標準連接埠上執行 SIP 轉換。

提示：Vonage 的 VoIP 服務使用 UDP 連接埠 5061。

11 如需追蹤 SIP 終端註冊異常，選擇**啟用 SIP 端點註冊異常追蹤**選項。預設情況下未勾選此選項。選擇此選項後，以下選項變為可用：

- **註冊追蹤間隔 (秒)** - 指定異常檢查間隔。預設值為 **300** 秒（5 分鐘）。
- **失敗的註冊閾值** - 指定異常檢查前註冊失敗次數。預設值為 **5** 次失敗。
- **端點封鎖間隔 (秒)** - 預設值為 **3600** 秒（60 分鐘）。

12 您可以

- 按一下**接受**。
- 移至第 607 頁「H.323 設定」。

H.323 設定

設定 H.323 設定

設定 H.323 設定的步驟如下：

1 導覽至**管理 | 系統設定 | VOIP | H.323 設定**。

2 選擇要全域啟用 H.323 轉換或根據防火牆規則來啟用:

- **使用全域控制以啟用 H323 轉換**。 預設情況下已核取此選項。
- **使用防火牆規則型控制以啟用 H323 轉換**。請確保設定防火牆規則以控制 H.323 轉換，如 *SonicOS 原則中所述*。

3 如果您未設定 H.323 轉換，請移至步驟 5。

1 選擇**啟用 H.323 轉換**，以允許防火牆檢查和修改可感知 H.323 通訊協定狀態的封包內容。預設已停用此選項。選擇此選項後，其他 H.323 選項可用。

防火牆在 H.323 封包內執行動態 IP 位址和傳送連接埠對應，這對受信和不受信網路/區域中的 H.323 各方之間的通訊是必要的。

停用**啟用 H.323 轉換**可繞過由防火牆執行的 H.323 特定處理。

2 選擇**僅接受來自 Gatekeeper 的傳入呼叫**，確保所有來電都經過 Gatekeeper 進行身分驗證。Gatekeeper 會拒絕未通過身分驗證的呼叫。

3 **H.323 信令/媒體非使用狀態逾時（秒數）**欄位指定呼叫可以處於空閒狀態的時間量，經過此時間後，防火牆就會封鎖後續流量。將呼叫置於保持時，便進入空閒狀態。預設時間為 **300** 秒 (5 分鐘)，最短時間為 60 秒 (1 分鐘)，最長時間為 122400 秒 (34 小時)。

4 **預設 WAN/DMZ Gatekeeper IP 位址**欄位的預設值為 **0.0.0.0**。在此欄位中輸入預設 H.323 Gatekeeper IP 位址，使基於 LAN 的 H.323 裝置能夠利用多點傳送位址 `225.0.1.41` 發現 Gatekeeper。如果不輸入 IP 位址，基於 LAN 的 H.323 裝置的多點傳送發現訊息將接受已設定的多點傳送處理。

5 按一下**接受**。

主題：

- 第 608 頁「設定 WAN 介面的頻寬」
- 第 608 頁「設定 VoIP 存取規則」

設定 WAN 介面的頻寬

附註：如需在 WAN 介面進行頻寬管理 (BWM) 和設定 BWM 的資訊，參見 *SonicOS 原則*。

設定 VoIP 存取規則

預設情況下，防火牆上的封包狀態檢查允許從 LAN 到 Internet 的所有通訊，而封鎖從 Internet 到 LAN 的所有流量。可以定義其它網路存取規則，以便擴充或覆寫預設存取規則。

若要定義用戶端的 VoIP 存取以從 WAN 使用 VoIP 服務供應商，您可以設定來源與目的地介面或區域之間的網路存取規則，使防火牆之後的用戶端可傳送和接收 VoIP 呼叫。

提示：雖然可以建立允許傳入 IP 流量的自訂規則，但防火牆不會停用對「拒絕服務」（如「同步攻擊和「死亡之 Ping」等）攻擊的防禦。

附註：您必須先為 **WAN** 介面在**管理 | 系統安裝| 網路 > 介面**上選取「頻寬管理」，然後才可設定網路存取規則的頻寬管理。

若要為 SonicWall 安全設備上的 VoIP 流量新增存取規則，請參閱 *SonicOS 原則*。

設定 VoIP 記錄

您可以啟用 VoIP 事件記錄，其顯示在**調查 | 記錄 | 事件記錄**中。若要啟用 VoIP 記錄，請參閱 *SonicOS 調查*。

部分 9

虛擬輔助

- 設定虛擬輔助

40

設定虛擬輔助

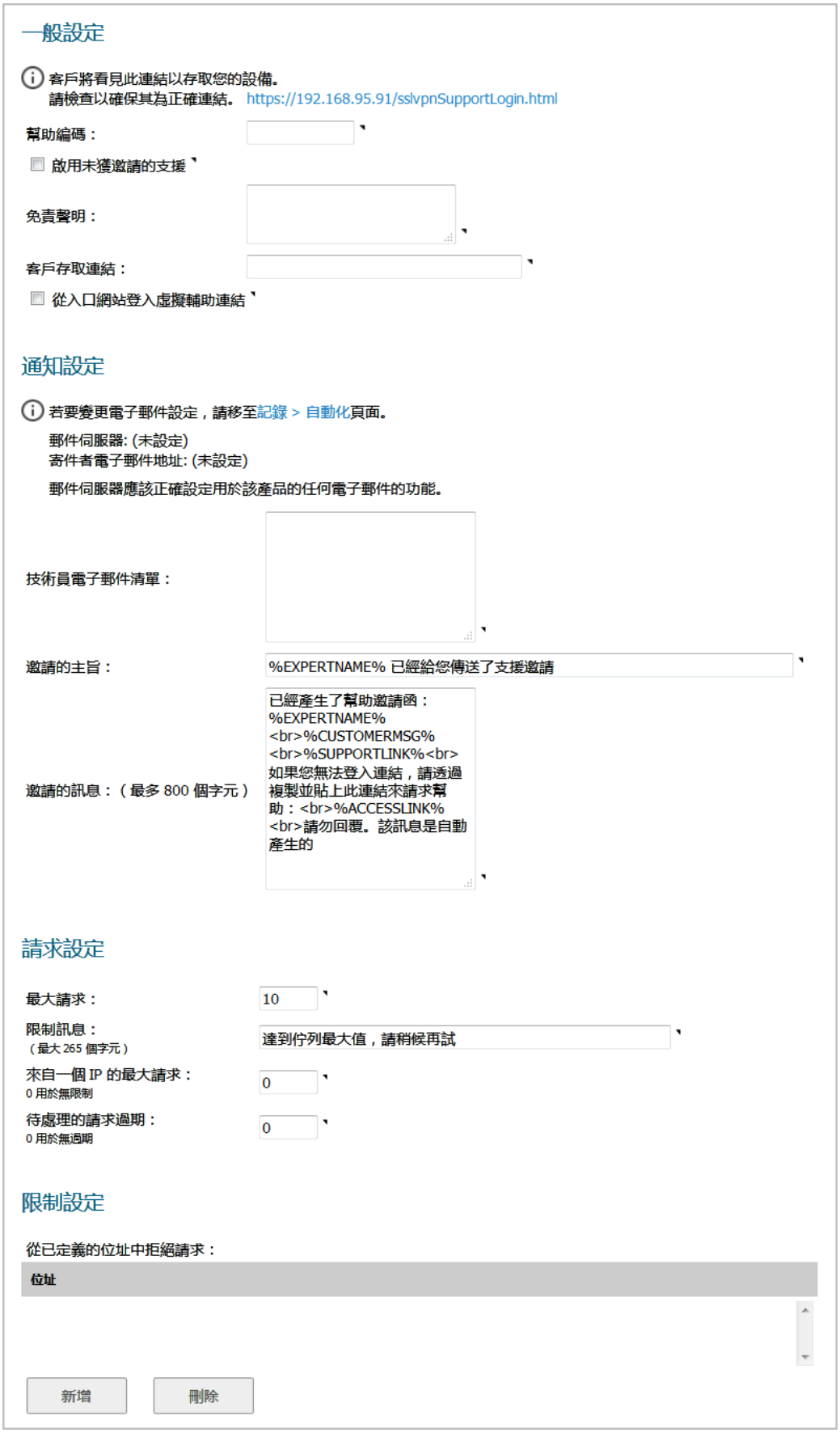
關於虛擬輔助

虛擬輔助讓您無需到達客戶現場，即可為客戶的技術問題提供支援。此功能可以為支援人員節省大量時間，同時還能提高他們回應支援需求的靈活性。您可以允許或邀請客戶加入一個接收支援的「佇列」，然後通過遠端控制客戶的電腦來診斷和修復技術問題，從而為每個客戶提供虛擬輔助。

附註：提供虛擬輔助的技術員或管理員必須位於 SonicWall 安全設備的本機網路內部。

最大限度提高虛擬輔助靈活性

您可以透過**系統設定 | 虛擬輔助**上的設定控制「虛擬輔助」。


一般設定
客戶將看見此連結以存取您的設備。
請檢查以確保其為正確連結。 https://192.168.95.91/sslvpnSupportLogin.html
幫助編碼：
啟用未獲邀請的支援
免責聲明：
客戶存取連結：
從入口網站登入虛擬輔助連結
通知設定
若要變更電子郵件設定，請移至記錄 > 自動化頁面。
郵件伺服器: (未設定)
寄件者電子郵件地址: (未設定)
郵件伺服器應該正確設定用於該產品的任何電子郵件的功能。
技術員電子郵件清單：
邀請的主旨：
%EXPERTNAME% 已經給您傳送了支援邀請
邀請的訊息：（最多 800 個字元）
已經產生了幫助邀請函：
%EXPERTNAME%

%CUSTOMERMSG%

%SUPPORTLINK%
如果您無法登入連結，請透過複製並貼上此連結來請求幫助：
%ACCESSLINK%

請勿回覆。該訊息是自動產生的
請求設定
最大請求：
10
限制訊息：
（最大 265 個字元）
達到佇列最大值，請稍候再試
來自一個 IP 的最大請求：
0 用於無限制
0
待處理的請求過期：
0 用於無過期
0
限制設定
從已定義的位址中拒絕請求：
位址
新增
刪除

設定虛擬輔助

希望最大限度提高虛擬輔助功能的靈活性的，您應該花些時間正確調整所有設定。

主題：

為使用者提供存取權

您需要決定如何為客戶提供存取權限以通過虛擬輔助獲得支援。

- 無需邀請即可啟用虛擬輔助支援。
- 通過為客戶設定全域幫助編碼，您可以限制誰能夠進入系統請求幫助。編碼最多可以是八 (8) 位字元，並可以在「幫助編碼」欄位中輸入。客戶通過技術員或管理員提供的電子郵件獲得此編碼。

若要為使用者提供存取權:

1 導覽到**管理 | 系統設定 | 虛擬輔助**。

2 若要提供全域編碼讓客戶先進入，進而能夠要求協助，請在**幫助編碼**欄位中輸入最多 8 個英數字元。若要表示不需要程式碼，此欄位請保留空白。

提示：幫助編碼可用於限制某人進入系統請求幫助。

3 若要讓客戶能夠在未受到技術員邀請的情況下，透過支援登入網頁要求協助:

a 將**幫助編碼**欄位保留空白。

b 選取**啟用未獲邀請的支援**。

附註：如果未選取此選項，客戶只能透過收到技術員發送的電子郵件邀請，才能獲得協助。選取此選項，可讓客戶從登入頁面要求協助。

4 若要建立客戶在獲得支援前必須閱讀和同意的書面訊息，則請於**免責聲明**欄位中輸入免責聲明。

5 若要從網路外部存取 SSL VPN 安全設備，請在**客戶存取連結**欄位中輸入 URL。如果將此欄位保留空白，傳送給客戶的支援邀請將使用技術員存取安全設備所使用的 URL。

提示：如果要從網路外部透過不同的 URL 存取 SSL VPN 安全設備，請設定此選項。

6 若要在客戶導覽至技術員登入頁面時，重新導向支援登入頁面，請選取**從入口網站登入顯示虛擬輔助連結**。

7 按一下**接受**。

8 若要確保客戶看見的存取連結正確無誤，請按一下**一般設定**參考說明中的連結。隨即顯示您在步驟 5 中設定的存取連結；例如

> **系統不接受未收到邀請的請求您的管理員必須選擇「啟用未收到邀請的支援」選項。**

自訂通知

在**通知設定**區段中，您可以自訂各方面的邀請和技術員通知。

若要自訂邀請與技術員通知:

重要：設定通知設定之前，先在**管理 | 記錄與報告 | 記錄設定 | 自動化**中設定電子郵件伺服器與電子郵件位址；若要快速顯示此頁面，請按一下**通知設定**區段中參考說明中的連結。如需有關設定電子郵件伺服器的資訊，請參閱 *SonicOS 記錄與報告*。

1 導覽到**管理 | 系統設定 | 虛擬輔助**。

2 捲動至**通知設定**。

3 在**技術員電子郵件清單**欄位中建立技術員電子郵件位址的清單，當未受邀請的客戶進入支援佇列時，會收到通知電子郵件。最多可以在此清單中新增 10 個電子郵件，之間以分號分隔。

4 若要自訂支援邀請電子郵件的主旨行，請使用變數表格中列出的變數，在**邀請郵件主旨**欄位中輸入所需的文字。系統將提供邀請主旨行範例。

變數

針對	使用
技術員姓名	%EXPERTNAME%
邀請中的客戶訊息	%CUSTOMERMSG%
支援連結	%SUPPORTLINK%
SSL-VPN 連結	%ACCESSLINK%

5 若要自訂邀請電子郵件的內文，請使用變數表格中列出的變數，在**邀請訊息**欄位中輸入所需的文字。訊息最多可包含 800 個字元。將提供邀請主旨樣本。

6 按一下**接受**。

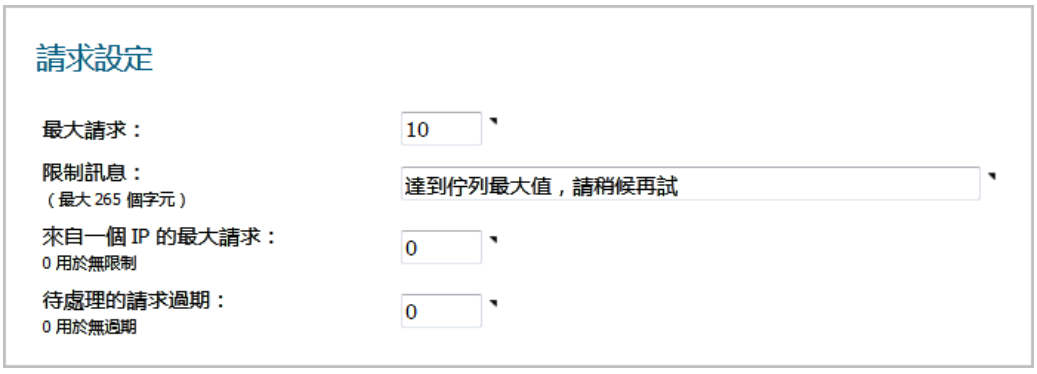
管理要求

您可以在**要求設定**區段中管理及限制支援要求。

若要管理及限制支援要求:

1 導覽到**管理 | 系統設定 | 虛擬輔助**。

2 捲動至**要求設定**。



3 若要限制佇列中一次可等待協助的客戶數，請在**最大請求**欄位中輸入限制。到達限值時，將封鎖新的請求。預設佇列大小為 **10** 個請求。

4 若要在達到最大要求數限制時，由於佇列中沒有可用位置而向客戶顯示訊息，請在**限制訊息**欄位中輸入訊息。您可以建立最多含 256 個字元的訊息。將提供樣本訊息。

5 若要限制來自單一 IP 的要求數，請在**來自一個 IP 的最大請求數**欄位中輸入限制。這可以防止相同的客戶同時多次請求虛擬輔助且因此多次將客戶放入佇列。輸入 **0**（預設）表示沒有限制。

6 為了避免客戶在高峰期間無限期等待虛擬輔助的支援，您可以在**擱置的請求已過期**欄位中輸入限制 (分鐘數)，設定客戶在未收到支援的情況下，可在佇列中等待支援的時間。如果您不想設定限制，則輸入 **0**（預設）。

7 按一下**接受**。

封鎖來自特定 IP 位址的要求

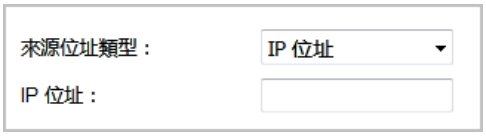
如果您遇到來自無益或無效來源的請求，可以封鎖來自訂的 IP 位址的請求。

若要封鎖來自 IP 位址的要求:

1 導覽到**管理 | 系統設定 | 虛擬輔助**。

2 捲動至**限制設定**。

3 按下**新增**。將顯示**管理員位址**對話方塊。



4 從**來源位址類型**選取來源位址的類型:

- **IP 位址** - 預設
- **IP 網路** - 選項變更；移至步驟 7。

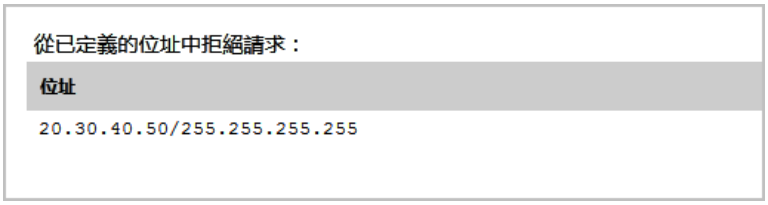
5 在 **IP 位址**欄位中，輸入要封鎖的 IP 位址。

6 移至步驟 9。

7 在**網路位址**欄位中，輸入要封鎖的網路位址。

8 在**子網路遮罩**欄位中，輸入位址的子網路遮罩。

9 按一下**確定**。項目隨即新增至**從已定義的位址中拒絕請求**表格。



10 按一下**接受**。

刪除封鎖的位址

若要將項目從「從已定義的位址中拒絕請求」欄位中刪除:

1 導覽到**管理 | 系統設定 | 虛擬輔助**。

2 捲動至**限制設定**。

3 選取要刪除的項目。

4 按一下**刪除**。

部分 10

附錄

- 設定開放式驗證、社交登入和 LHM
- BGP 進階路由
- IPv6
- SonicWall 支援

A

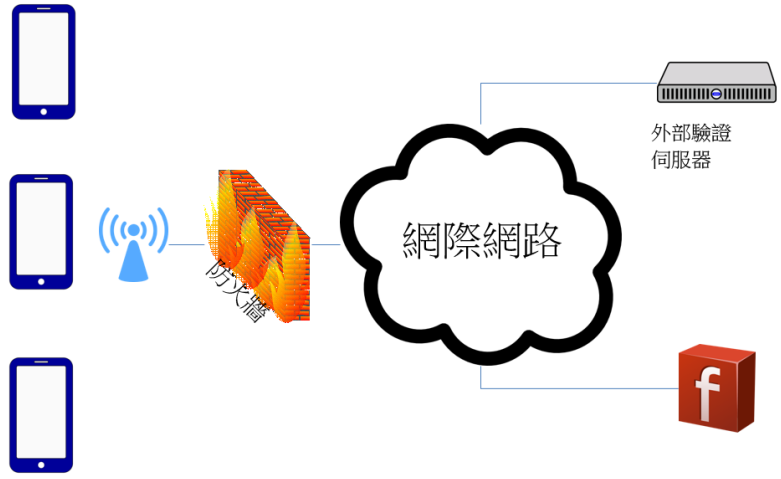
設定開放式驗證、社交登入和 LHM

附註：SuperMassive 9800 不支援設定開放式驗證、社交登入和 LHM。

關於 OAuth 和社交登入

社交登入是一種單一登入驗證形式，使用社交網路服務例如 Facebook、Twitter 或 Google+ 的現有使用者認證，登入第三方網站而不是特別為該網站建立新的登入帳戶。開放式驗證 (OAuth) 社交登入功能可以搭配來賓服務，使用傳遞驗證在無線區域、LAN 區域或 DMZ 區域上使用；請參見外部驗證伺服器登入拓撲。傳遞驗證是對信任的網域內的網域控制器執行驗證的一種方法。無線來賓服務在公共 WiFi 熱點和為訪客設定的企業 WiFi 服務中廣為使用。

外部驗證伺服器登入拓撲



主題：

什麼是 OAuth 和社交登入？

OAuth 是驗證的開放式標準。OAuth 代表資源擁有者，提供用戶端應用程式存取伺服器資源的安全委派存取權，並且會指定資源擁有者的程序，以授權第三方存取其伺服器資源，而無須共用其憑證。

社交登入是一種單一登入 (SSO) 形式，使用社交網路服務例如 Facebook、Twitter 或 Google+ 的現有登入資訊，登入第三方網站而不是特別為該網站建立新的登入帳戶。

OAuth 和社交登入的優點

主題：

- OAuth
- 社交登入

OAuth

OAuth 是常用機制，協助使用者在應用程式間共用資料。您可以將其用作 Web 應用程式的登入提供者來善用 OAuth。

其他優點

- 限制網路上的客戶設定檔
- 較少密碼要追蹤
- 不需要提交密碼，但是信任可能會是個問題
- 您仍然可以防止從 OAuth 提供者進行存取
- 降低 ID 遭竊的風險。驗證是由提供者負責
- 使用之前核可的 API 進行驗證，降低錯誤失敗的風險
- 資料伺服器上的儲存需求較低

缺點

- 您無法針對自己的應用程式制定使用者設定檔
- 使用者在沒有現有帳戶而向 OAuth 提供者建立帳戶時會混淆

社交登入

社交登入的設計是為簡化登入程序，實現較高的註冊轉換率。

其他優點

- 快速註冊
- 記憶較少的登入資料
- 目標豐富的內容
- 使用多重識別
- 收集訪客資料
- 詳細或個人化的使用者經驗
- 熟悉的登入環境
- 較少登入失敗
- 容易用於手機

缺點

- 信任層級低
- 排除非社交使用者
- 資料正確性可以偽造
- 社交網路的已封鎖內容
- 安全性問題

OAuth 和社交登入的運作方式

開放式驗證 (OAuth) 和社交登入功能可以搭配內部無線服務和做為無線區域來賓服務的 SonicPoints 使用。來賓可以使用您公司的企業 WiFi 登入網際網路。無線來賓服務在公共 WiFi 熱點和為訪客設定的企業 WiFi 服務中廣為使用。

OAuth 和社交登入二者使用無線來賓服務，其包括網際網路存取，並可設定為使用以下連線方法之一或二者都使用：

- 第 620 頁「無重新導向」
- 第 621 頁「重新導向到登陸頁面」

無重新導向

無重新導向提供來賓開放式網際網路存取而無需加密，所以來賓被允許自由連接至提供的 WiFi。

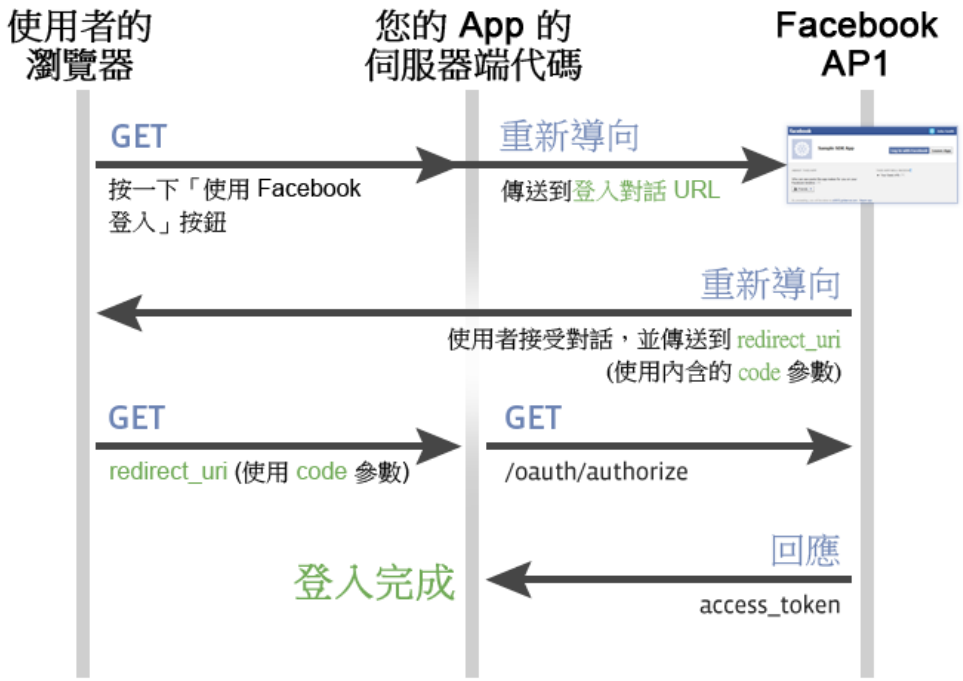
無重新導向也提供 WPA/WEP 密碼存取，來賓需要密碼才能使用提供的 WiFi。密碼可透過其他途徑提供，例如收據。

重新導向到登陸頁面

登陸網頁提供大多數廣為使用的熱點存取。當第 2 層 WiFi 存取開放時，來賓會在存取第一層時被導向到登陸網頁；請參見 Oauth Flow。部分其他重新導向存取選項包含：

- 在登陸頁面上無身分驗證
- 來賓可以建立新的登入帳戶，然後使用它登入
- 來賓可以使用透過傳送到手機的簡訊、電子郵件或其他方式所收到的代碼註冊
- 正在使用行動應用程式掃描 QR 代碼
- 使用社交登入

Oauth Flow



支援的平台

開啟式驗證和社交登入在 SonicWall 防火牆上受支援：

- 執行 SonicOS 6.2.7 和更高版本
- 在執行 GMS 8.3 的 GMS 管理下

開發和生產的需求

- Facebook 帳戶
    - 啟用 Facebook For Developers

- 外部伺服器
  - 可公用存取
  - 具有網域名稱
  - PHP 支援
  - SSL 憑證
- Sonicwall 防火牆
  - 外部伺服器可連接 (透過 IP 或 FQDN)
  - 無線 (內部或 SonicPoint)

有關輕量級熱點訊息 (LHM)

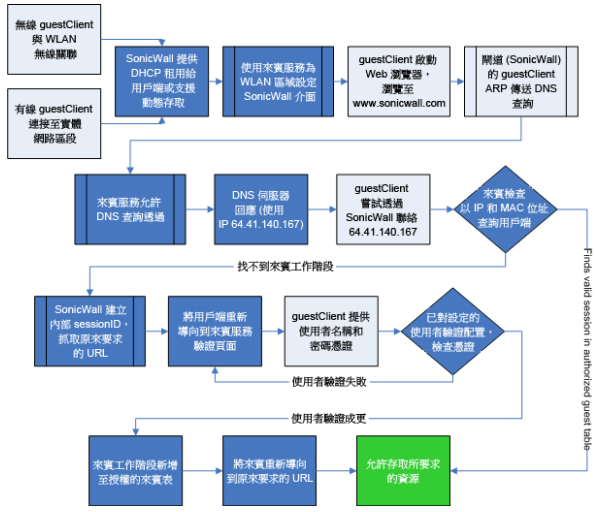
輕量級熱點訊息 (LHM) 利用 SonicWall 來賓服務模型，其中可將使用者分類和針對透過 SonicWall 安全裝置的區分網路存取權授權。例如，SonicWall 可設定任何透過屬於支援來賓服務之 WLAN (無線 LAN) 區域的介面的使用者連接，只能存取網際網路 (不受信任網路) 但不能存取 LAN (受信任網路)。這允許單一防火牆提供受信任和來賓使用者同時存取。

LHM 透過將驗證和授權程序分開來擴充來賓服務模型，而得以讓驗證在 SonicWall 外部發生。這允許廣泛自訂驗證介面，並且也允許使用任何種類的驗證配置。

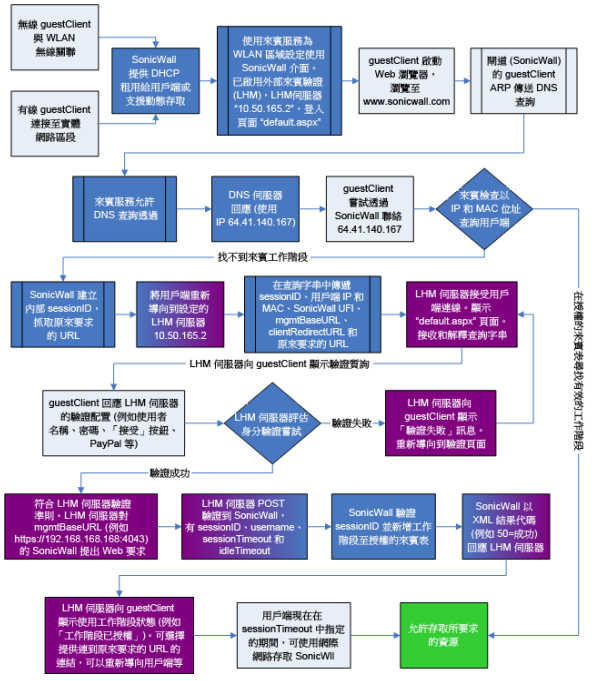
並列檢視原始來賓服務流程，並且 LHM 授權流程會顯示在授權流程的比較表格中：

授權流程的比較

原始來賓服務授權流程

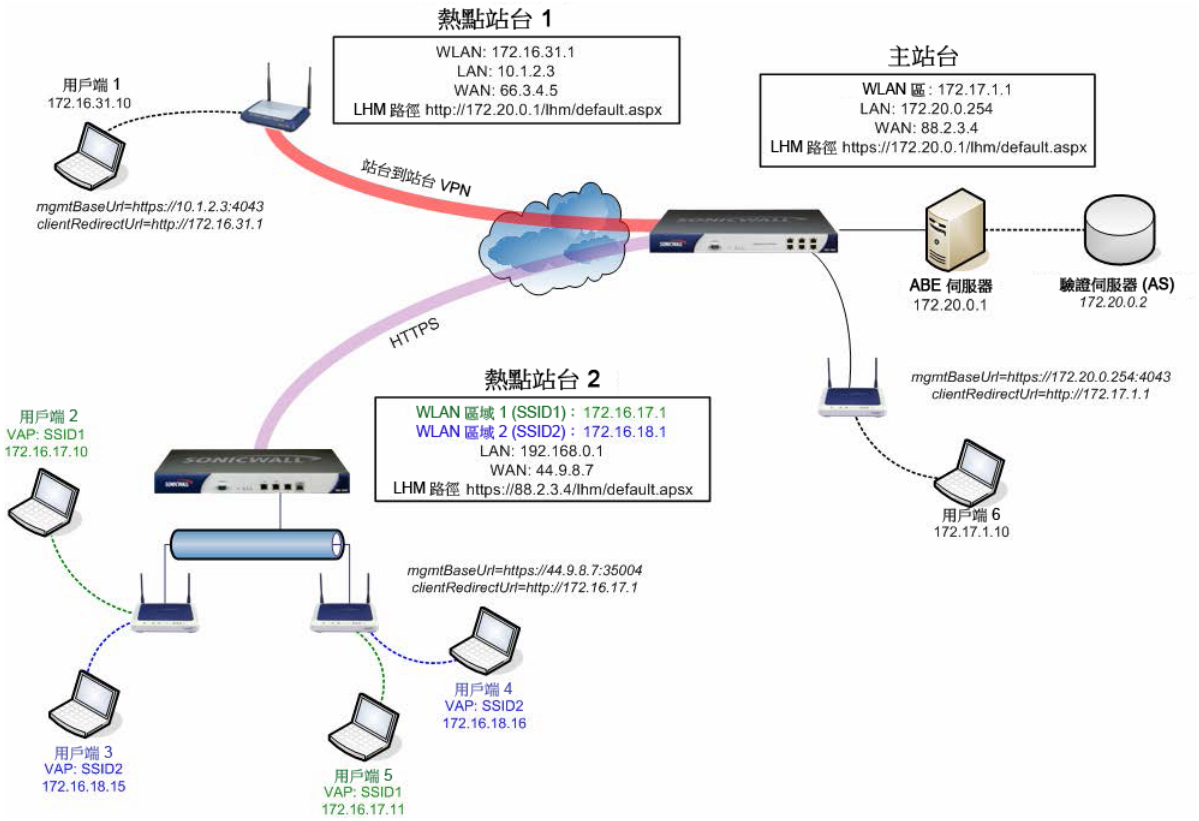


LHM 授權流程



LHM 定義 SonicWall 無線存取裝置 (例如 SOHO W 防火牆、TZ Wireless 系列防火牆或配備管理 SonicWall 安全裝置的 SonicPoint) 和驗證後端 (ABE) 之間的通訊方式和語法，以驗證熱點使用者並提供他們參數繫結的網路存取。LHM 設定範例描述一般設定。

LHM 設定範例



LHM 允許網路業者提供多個熱點位置的集中管理，透過使用 SonicWall 的無線來賓服務和任何現有 ABE 間的介面。LHM 是一般化 WISPr 和 GIS 規格的改編。

LHM 的設計是為滿足特別常見的操作環境的要求，而非廣泛的環境。特別是 LHM 允許熱點使用者管理和驗證完全在網路業者的 ABE 上發生，支援任何方式建立和管理帳戶，以及任何程度的網站自訂和商標。此方式可整合到任何現有環境而無須仰賴特定計費、會計或資料庫系統，也提供網路業者從外觀和感覺到重新定向無限制控制的網站設計。

為社交登入設定 Facebook

主題：

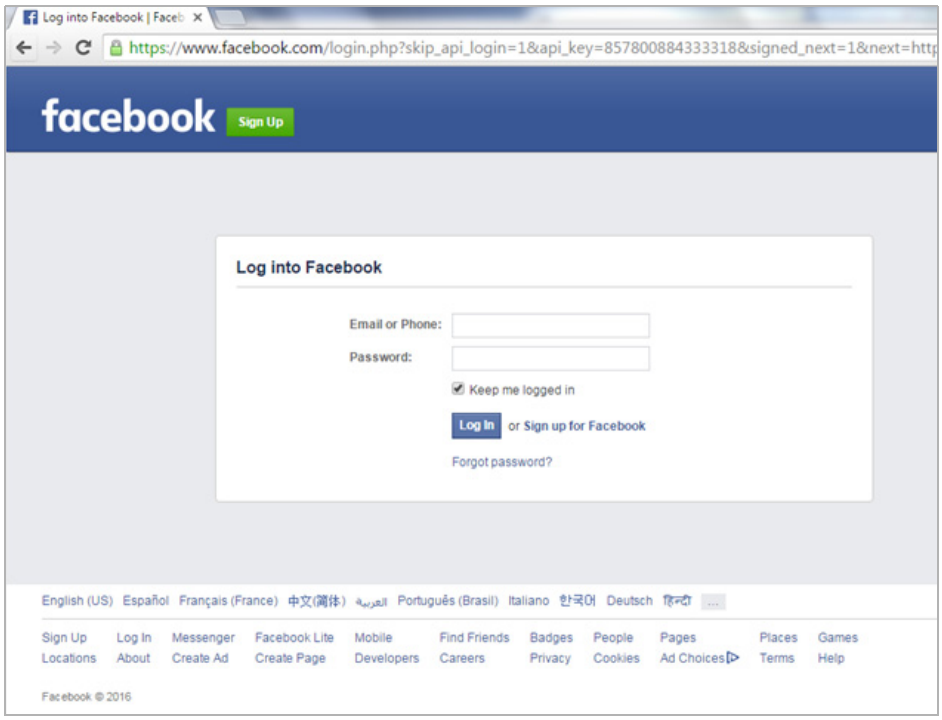
- 第 624 頁「Facebook 設定」
- 第 625 頁「用戶端 OAuth 設定」
- 第 625 頁「來賓狀態 (示範)」

Facebook 設定

若要登入 Facebook for Developers：

1 打開 Web 瀏覽器

2 登入您的 Facebook for Developers 帳戶，網址：https://developers.facebook.com/。

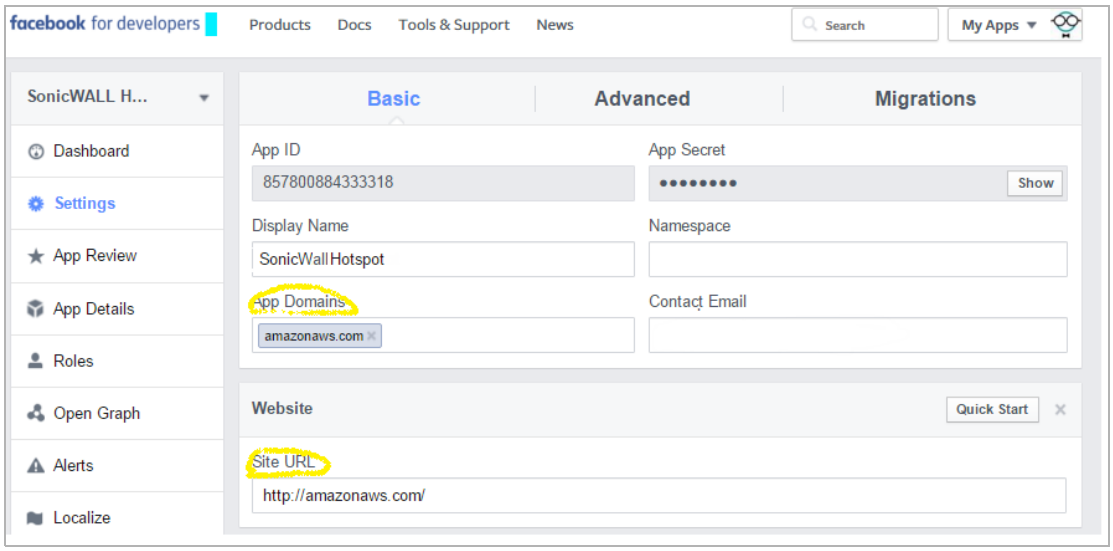


3 完成登入程序或註冊新的開發人員帳戶。

4 按一下左欄位的**設定**。

請參閱設定 Facebook for Developers 的範例填寫表單，但是調整 Facebook **設定**以搭配使用您的 LHM 伺服器。

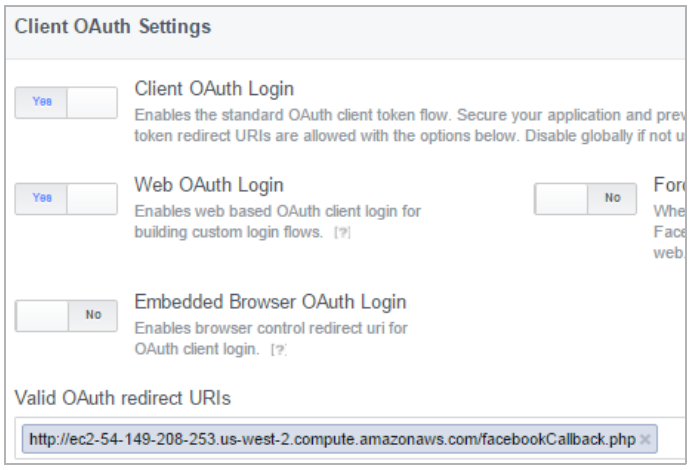
設定 Facebook for Developers 的範例



用戶端 OAuth 設定

您應在 Facebook for Developers (https://developers.facebook.com/) 調整您的用戶端 OAuth 設定 (**產品 > Facebook 登入 > 設定**)，類似 OAuth Facebook 設定的範例中所示。

OAuth Facebook 設定的範例



來賓狀態 (示範)

當允許無線用戶端存取 SonicWall WiFi 時，擁有者的帳戶名稱和資訊是傳送到 SonicOS。您可以收集和儲存此資訊到您自己的資料庫中。

設定開放式驗證和社交登入

主題：

- 第 625 頁「關於設定來賓服務」
- 第 625 頁「關於設定社交登入」
- 第 626 頁「在 SonicOS 中設定社交登入」

關於設定來賓服務

雖然 SonicOS 提供其自己的來賓帳戶管理，您仍可使用您自己的 IT 基礎結構以更好因應您的企業需求。此設定可透過設定外部來賓驗證或社交登入完成。**來賓服務**位於 SonicOS 無線區域、LAN 區域或 DMZ 區域 (**管理 | 系統安裝 | 網路 | 區域**) 的**新增/編輯區域**對話方塊中。

關於設定社交登入

此功能簡化麻煩的使用者登入，並提供可靠的人口資訊給 Web 開發人員。

若要準備設定社交登入：

1 如同第 333 頁「新增新區域」**中所述來建立無線區域、LAN 區域或 DMZ 區域，**然後設定或編輯具有安全功能的網路區域。

2 在 SonicOS 中，外部伺服器也可建立或選取為輕量級熱點訊息 (LHM) 伺服器 IP 或 FQDN 位址物件。

在 SonicOS 中設定社交登入

您需要進行一些設定才能妥善設定您的安全設備。安全設備會封鎖大部分的網際網路應用程式，但是有幾項需要允許，以使此功能正常運作用。

重要：LHM 伺服器應先投入服務，再設定社交登入。

若要為社交登入設定您的安全設備:

1 導覽至**管理 | 系統安裝 | 網路 | 區域** ，以設定或編輯具有無線安全功能的網路區域。如需新增網路區域的更多資訊，請參見第 333 頁「新增新區域」。

附註：外部伺服器也可建立或選取為輕量級熱點訊息 (LHM) 伺服器 IP 或 FQDN 位址物件。

2 按一下 WLAN **編輯**圖示以存取 WLAN 網路區域。顯示**編輯區域**對話。

3 按一下**來賓服務**。

4 選取**啟用來賓服務**。其他選項隨即啟用。

5 選取**啟用外部來賓驗證**。**設定**隨即啟用。

6 按一下**設定**。**外部來賓驗證**對話方塊顯示。

7 針對**外部 Web 伺服器設定**，您應有已經投入服務的 LHM 伺服器。從**主機**選取與該伺服器關聯的位址物件。

8 如第 335 頁「設定來賓存取的區域」中所述設定其他選項。

9 在**社交網路登入**部分，選取**啟用社交網路登入**。社交網路隨即啟用。

10 選擇要啟用的一個或多個社交網路以進行開放式驗證：

- **Facebook**
- **Google**
- **Twitter**

SonicOS 會自動建立必要的密碼驗證網路網域，以允許驗證伺服器和使用者間的驗證程序流量。自動新增的位址物件群組名稱為**預設社交登入密碼群組**。此位址物件群組是附加到目前設定的密碼網路 (若有的話)，或加入到新群組，其名稱為**社交登入密碼群組**。

11 按一下**驗證頁面**標籤。

12 輸入**登入頁面**位置，例如 `login.php`，但是根據開發人員的輸入頁面。這些指令碼由您自己的 LHM 伺服器主控，所以您應能夠確保它們正常運作。

13 完成剩餘欄位。

14 按下**確定**。

確認社交登入設定

您可以檢視**管理 | 原則 | 物件**，確認開放式驗證和社交登入的設定是否正確。如需物件的更多資訊，請參閱 *SonicOS 原則*。

若要確認設定：

1 導覽至**管理 | 原則 | 物件 | 位址物件**。

2 選取**位址群組**，其中應該會顯示:

- 網域已自動新增。
- Facebook、Google 和/或 Twitter 登入流量可成功通過。

使用社交登入、LHM 和 ABE

主題：

關於 ABE

ABE 包含 Web 伺服器 (WS) 以主控使用者互動和 (可選) 驗證伺服器 (AS) 的內容，提供目錄服務驗證。AS 可以是任何種類的使用者驗證機制，包括但不限於 RADIUS、LDAP 或 AD；唯一的要求是 WS 能夠針對驗證目的與 AS 通訊。WS 和 AS 可在單一伺服器或個別伺服器上進行管理。

LHM 也提供能力給 AS 以使用 SonicWall 安全裝置的內部使用者資料庫進行使用者驗證。如需訊息的詳細資訊，請參見第 634 頁「訊息格式」、 第 636 頁「本機驗證請求」和第 636 頁「本機驗證回覆」。

ABE 需要與熱點 SonicWall 通訊才能交換結果代碼和工作階段資訊。所有通訊為 HTTPS 並且可能直接發生 (例如 SonicWall 安全裝置的 LAN、WAN、X0 介面) 或透過到其中一個 SonicWall 安全裝置的管理介面位址的 VPN 通道。LHM 管理介面是自動透過路由 (路徑) 查詢傳遞，並且只有管理介面透過自動新增的存取規則接受 LHM 管理訊息。

LHM 通訊發生在特定 LHM 管理連接埠，其必須在 SonicWall 安全裝置上定義，並且 LHM 管理連接埠必須與標準 HTTPS 管理連接埠不同。

為允許 ABE 與 SonicWall 通訊，以及將用戶端重新導向到 SonicWall 上的適當介面，兩個參數是由 SonicWall 建構且透過用戶端重新導向到 ABE 來傳遞。以下通訊參數必須用於 ABE 和 SonicWall 間的所有通訊。

- `mgmtBaseUrl` - ABE 用來與 SonicWall 通訊的 IP 位址和連接埠。它是由 HTTPS 通訊協定指示項、所選 LHM 管理介面的 IP 和 LHM 連接埠 (例如 `https://10.1.2.3:4043`) 組成。
- `clientRedirectUrl` - SonicWall 上的 IP 位址 (和選擇性的連接埠)，用戶端會在各種工作階段重新導向，也就是 TZW 上的 LAN 管理 IP 或 SonicOS 裝置上的 WLAN IP (例如 `http://172.16.31.1`)。

參數值是由 SonicWall 在工作階段建立期間 (參見第 628 頁「工作階段建立」) 以及工作階段狀態同步 (參見第 634 頁「訊息格式」) 傳遞至 ABE，並且應由 ABE 用作建構所有相關 URL 的基礎。以下是在 SonicWall 安全設備上 ABE 所參照的頁面：

- *wirelessServicesUnavailable.html* - ABE 是無法使用的訊息。.此重新導向一般是由 SonicWall 傳送，但也可由 ABE 參照。文字可設定。
- *externalGuestRedirect.html* - 在工作階段建立時由 SonicWall 提供的初始重新導向訊息。文字可設定。
- *externalGuestLogin.cgi* - ABE 張貼工作階段建立資料的頁面。
- *externalGuestLogoff.cgi* - ABE 張貼工作階段終止資料的頁面。
- *localGuestLogin.cgi* - ABE 張貼的頁面以對於 SonicWall 的內部使用者資料庫驗證使用者認證。
- *createGuestAccount.cgi* - ABE 張貼的頁面以在 SonicWall 的內部資料庫建立來賓帳戶。
- *externalGuestUpdateSession.cgi* - ABE 張貼的頁面以更新現有工作階段的 *sessionLifetime* 和 *idleTimeout* 參數 (參見第 634 頁「工作階段更新」)。

有關從 SonicWall 到 ABE 的通訊，ABE 上託管的 URL (包括主機、連接埠和頁面/資源) 在 SonicWall 安全設備是完全可設定的。主機可以使用 IP 位址或完整網域名稱 (FQDN) 指定。使用 FQDN 時，名稱是在第一次使用時解析並由 SonicWall 儲存為 IP 位址。

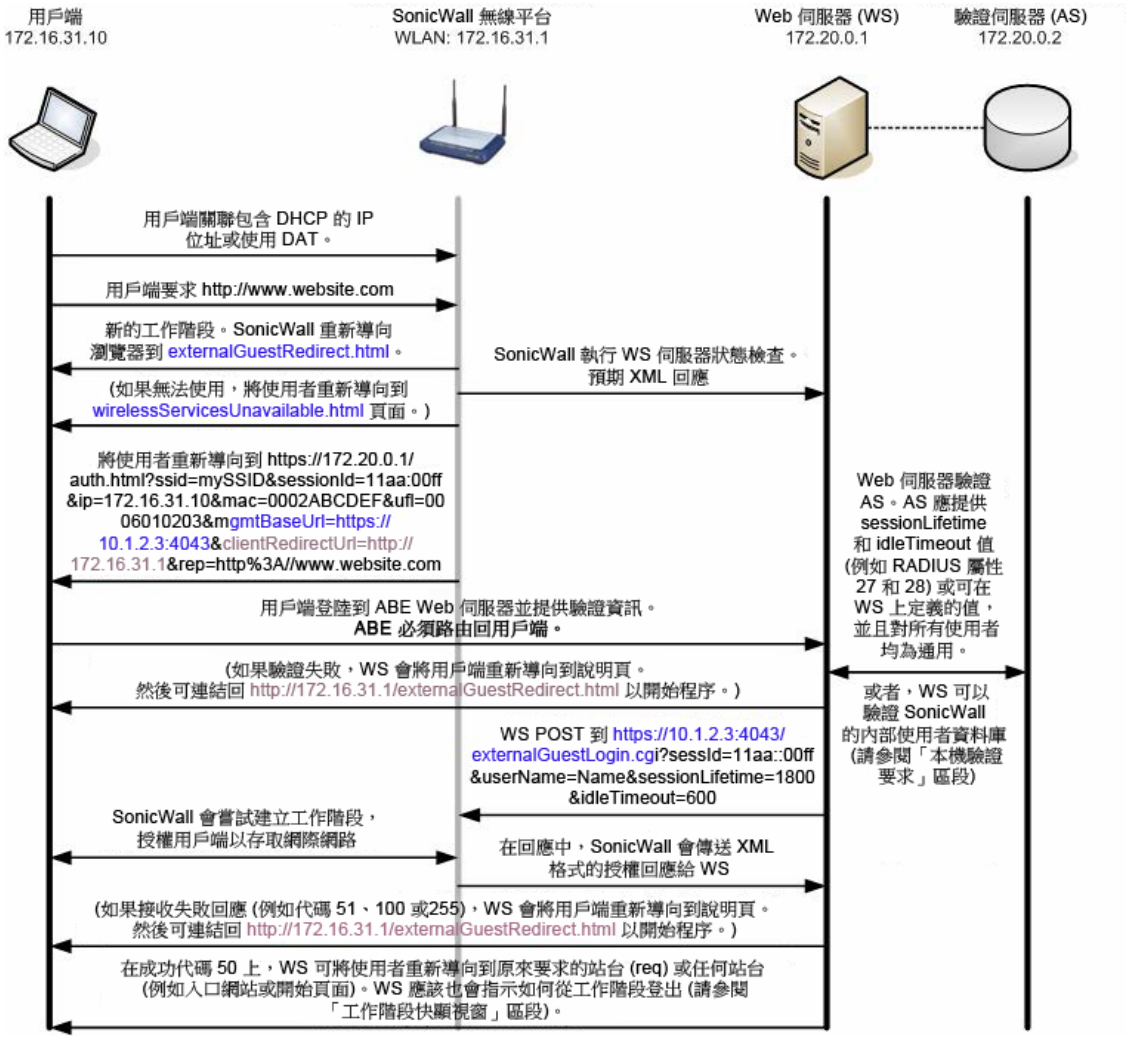
工作階段生命週期

以下章節說明工作階段生命週期的階段以及工作階段快顯示窗和 Web 伺服器 (WS) 狀態檢查元件：

工作階段建立

工作階段建立發生在無線用戶端嘗試存取以及 SonicWall 安全設備對於根據 MAC 位址的用戶端沒有使用中工作階段資訊時。

工作階段建立流程



1 無線用戶端與 SonicWall 關聯。從內部 DHCP 伺服器取得 IP 位址，或使用固定定址搭配動態位址轉譯 (DAT) 功能。

2 用戶端要求 Web 資源 `http://www.website.com`。

- SonicWall 安全設備判斷這是新的工作階段。

3 SonicWall 安全設備重新導向用戶端到內部託管的 `externalGuestRedirect.html` 頁面。`externalGuestRedirect.html` 頁面提供管理員可設定文字，說明作階段將重新導向以進行驗證。

4 在此重新導向期間，安全設備會透過 JavaScript 將嘗試重新導向到已設定目標重新導向頁面，來檢查 ABE 的可用性。

- 如果在指定的期間沒有發生重新導向到 WS (值在 SonicWall 上可設定，介於 1 到 30 秒)，安全設備會將工作階段重新導向到內部 l `wirelessServicesUnavailable.html` 頁面。

5 除了 JavaScript 可用性檢查外，SonicWall 提供可選的完整 Web 伺服器狀態 (參見第 633 頁「Web 伺服器狀態檢查」)。此選項可設定為在可設定的間隔 (介於 1 到 60 分鐘) 執行。如果錯誤回應代碼 1、2 或 255 發生，安全設備會記錄回應並將瀏覽器重新導向到內部 `wirelessServicesUnavailable.html` 頁面。此頁面提供管理員可設定文字說明資源。

6 如果可用，安全設備會將用戶端重新導向到 AS 上主控的驗證入口網站：
`https://172.20.0.1/auth.html?ssid=mySSID&sessionId=11aa::00ff&ip=172.16.31.10&mac=0002ABCDEF&ufi=0006010203&mgmtBaseUrl=https://10.1.2.3:4043&clientRedirectUrl=http://172.16.31.1&req=http%3A//www.website.com`

- *ssid* - 無線網路的 ESSID (無線網路名稱)，重新導向的用戶端與此關聯。
- *sessionId* - SonicWall 所產生 16 位元組 MD5 雜湊值的 32 位元組十六進位表示，由 SonicWall 和 WS 用於為用戶端編制索引 (例如 `11aa3e2f5da3e12ef978ba120d2300ff`)。
- *ip* - 用戶端的 IP 位址。
- *mac* - 用戶端 MAC 位址。
- *req* - 原來請求的網站會以引數傳遞到驗證伺服器。
- *ufi* - SonicWall 唯一的防火牆識別項。若要用於網站識別。
- *mgmtBaseUrl* - SonicWall 上 IP 後續通訊用的通訊協定、IP 位址和連接埠。
- *clientRedirectUrl* - SonicWall 上的通訊協定、IP 位址 (和可選的連接埠)，ABE 用於用戶端重新導向。
- *req* - 用戶端原來要求的 URL (如有的話)，URL 會編碼。

7 用戶端提供驗證資訊 (例如使用者名稱、密碼、Token 等)。

附註： WS 必須能夠聯繫用戶端，例如透過 VPN、NAT 或路由。

8 WS 會對 AS 驗證使用者。

- AS 提供工作階段特定資訊，也就是名稱、工作階段逾時和閒置逾時值。
- 工作階段特定值可由 WS 全域套用而非從 AS 取得；部分值僅需要傳遞至安全設備。
- 逾時值是以秒表示，範圍為從 1 到 863,913,600 (等於 9999 天)。

9 如果驗證失敗，WS 應將用戶端重新到向到說明失敗的頁面。應提供連結回到 `http(s)://172.16.31.1/externalGuestRedirect.html` 以重新啟動程序。

10 如果成功，WS 透過 HTTPS 或 VPN 和 POST 連接到安全設備：
`https://10.1.2.3:4043/externalGuestLogin.cgi?sessId=11aa::00ff&userName=Name&sessionLifetime=1800&idleTimeout=600`。

- 安全設備會嘗試建立工作階段並以相同連線傳送結果到 WS。結果如第 634 頁「訊息格式」中所述。

11 如果收到失敗回應 (例如代碼 51、100 或 255)，WS 應會將用戶端重新導向到說明失敗的頁面。可提供連結回到： `http(s)://172.16.31.1/externalGuestRedirect.html` 以重頭開始程序。

12 如果成功 (代碼 50)，WS 可將使用者重新導向到原來要求的站台 (`req`) 或任何站台 (例如入口網站或開始頁面)。WS 應該也會指示如何從工作階段登出 (例如將頁面、快顯視窗、URL 加入書籤)。

工作階段快顯視窗

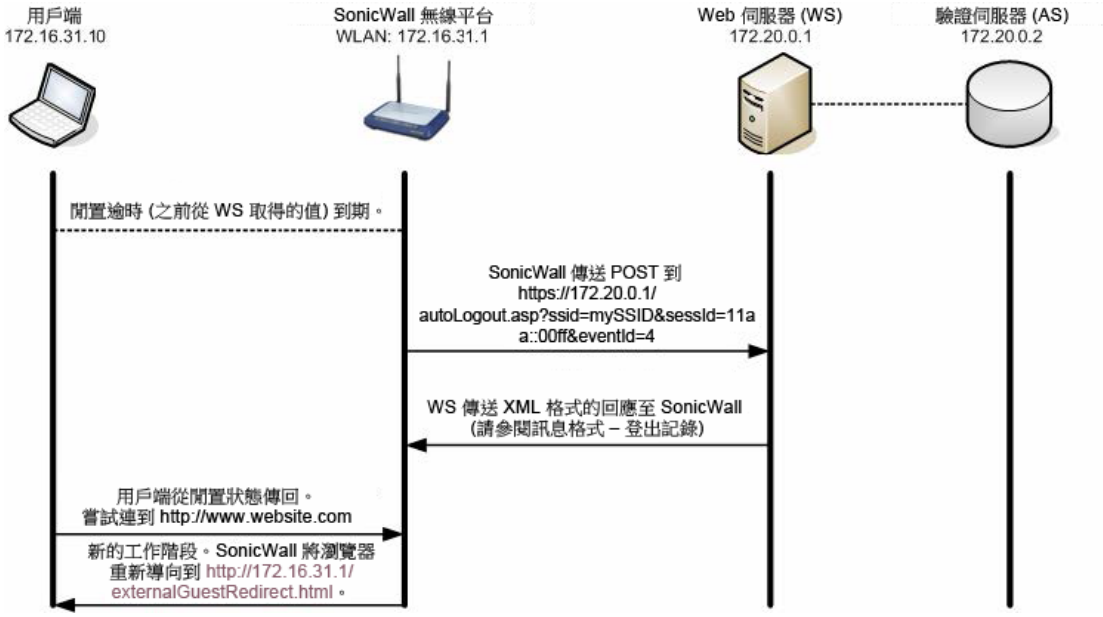
建議透過工作階段快顯視窗管理該工作階段。這應該是在工作階段建立時具現化的瀏覽器視窗，提供工作階段時間資訊 (例如存留時間、閒置逾時值、計時器倒數) 和登出按鈕。提供範例代碼。

- 按一下**登出**結束工作階段並觸發使用者登出事件。
- 嘗試關閉視窗應會提供警告訊息，表示關閉視窗會結束工作階段。
- 關閉視窗會結束工作階段並觸發使用者登出事件。

閒置逾時

當超過閒置逾時 (在第 628 頁「工作階段建立」，步驟 8 中指定) 時會發生閒置逾時。

閒置逾時流程



1 閒置計時器 (如第 628 頁「工作階段建立」) 到期。

2 因為用戶端的瀏覽器可能目前未開啟，我們不會以重新導向起始此程序。反而，SonicWall 會傳送 POST 到 WS：
`https://172.20.0.1/autoLogout.asp?ssid=mySSID&sessId=11aa::00ff&eventId=4` (參見第 634 頁「訊息格式」有關登出事件 ID)。

- 安全設備上可設定 POST 的傳送目的地資源 (從**管理 | 系統安裝 | 網路 | 區域**)。編輯 WLAN 區域 (在**編輯區域**對話方塊中: **來賓服務 > 外部來賓驗證 > 進階 > 自動工作階段登出 > 登出 CGI**。
- WS 主控的頁面一定會預期和解釋 *sessId* 和 *eventId* 值。

3 Ws 會以相同連線傳送 XML 結果到 WS。結果如第 637 頁「登出回覆」中所述。

4 如果用戶端從閒置狀態返回，並嘗試聯繫 Web 資源，安全設備會將使用者重新導向到內部 `externalGuestRedirect.html` 頁面，從頭開始工作階段建立程序 (參見第 628 頁「工作階段建立」)。

ⓘ **附註：**為保存資源，建議閒置逾時設定為最長 10 分鐘。

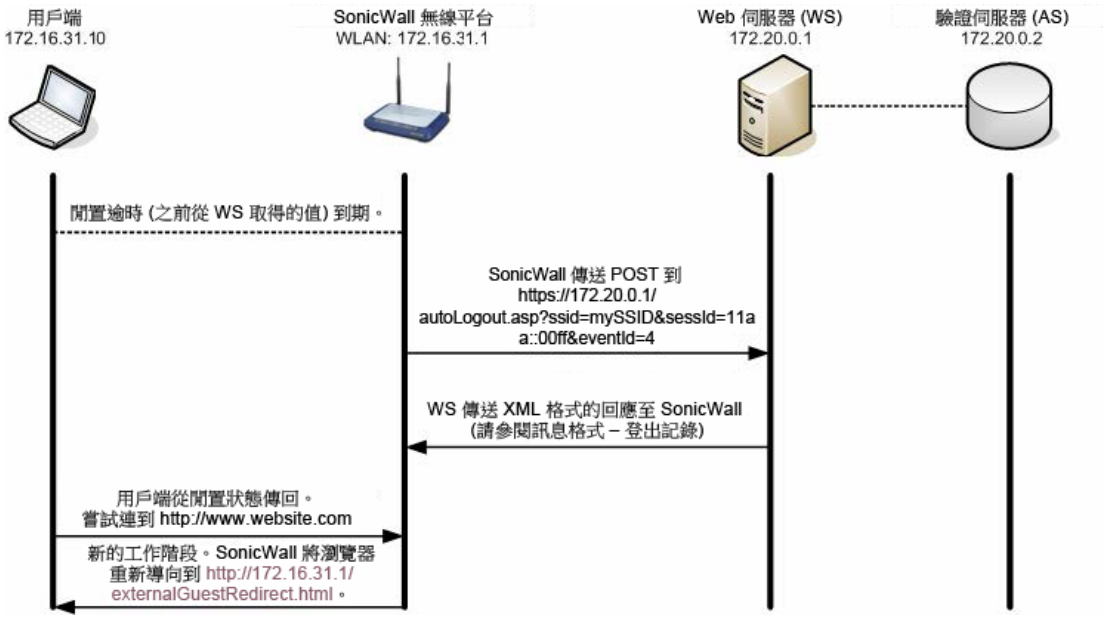
工作階段逾時

當工作階段存留時間到期時事件會發生。交換和以上閒置逾時相同，只是工作階段逾時 *eventId* 值為 3，而非 4 的閒置逾時。

使用者登出

當使用者透過關閉工作階段快顯視窗，或使用工作階段快顯視窗提供的登出按鈕，主動結束工作階段，事件就會發生。工作階段快顯視窗是使用者登出的慣用方式，不過允許工作階段的存留時間到期，無須此方式即可達成相同結果。後者會移除對工作階段快顯視窗的相依性，但是管理資源的效率較低。

使用者登出流程



1 用戶端使用登出按鈕登出或關閉工作階段快顯視窗。

2 WS 傳送 POST 至：
`https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=1` (有關登出事件 ID，請參見第 634 頁「訊息格式」)。

- `sessId` - 由安全設備在工作階段建立 (參見第 628 頁「工作階段建立」) 期間所產生的值，是由安全設備和 WS 用於為用戶端編制索引。
- `eventId` - 說明登出請求事件。

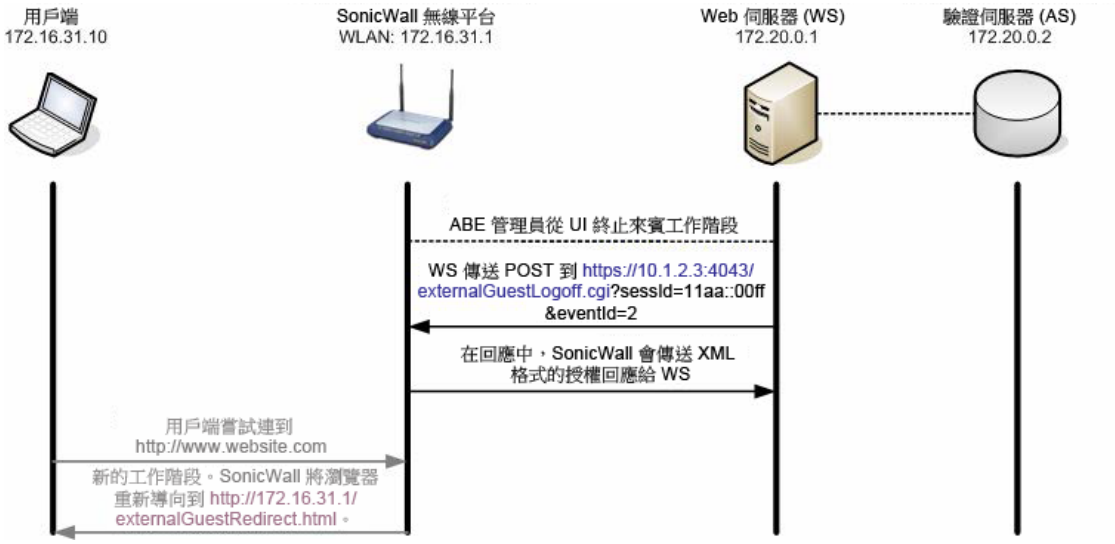
3 SonicWall 安全設備會以相同連線回應結果給 WS。結果如第 637 頁「登出回覆」 中所述。

4 如果用戶端嘗試聯繫 Web 資源，安全設備會將使用者重新導向到內部 `http://172.16.31.1/externalGuestRedirect.html` 頁面，從頭開始工作階段建立程序 (參見第 628 頁「工作階段建立」)。

管理員登出 (可選)

當 ABE 管理員透過管理介面從來賓工作階段登出時事件會發生。目前無法從 SonicOS 管理介面本身終止 ABE 建立的來賓工作階段。建立的來賓工作階段在 SonicOS 管理介面上是如此顯示 (或明顯從內部 WGS 來賓工作階段) 並且無法編輯。

管理員登出流程



1 ABE 管理員從管理 UI 終止來賓工作階段。

2 WS 傳送 POST 至安全設備：`https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=2`.(有關登出事件 ID，請參見第 634 頁「訊息格式」)。

- `sessId` - 由安全設備在工作階段建立期間所產生的值，是由安全設備和 WS 用於為用戶端編制索引。
- `eventId` - 說明登出請求事件。

3 SonicWall 會以相同連線傳送結果給 WS。結果如第 637 頁「登出回覆」中所述。

4 如果用戶端從閒置狀態返回，並嘗試聯繫 Web 資源，安全設備會將使用者重新導向到內部 `http://172.16.31.1/externalGuestRedirect.html` 頁面，從頭開始工作階段建立程序(參見第 628 頁「工作階段建立」)。

Web 伺服器狀態檢查

若要提供比簡單的 Web 伺服器 (WS) 可用性更細微的 ABE 狀態 (如第 629 頁「工作階段建立流程」的強制步驟 4 即 JavaScript 重新導向)，SonicWall 可選擇性地傳送安全的 HTTP GET 操作到 WS，以便判斷伺服器操作狀態。目標 URL 是可設定的，查詢的間隔 (介於 1 到 60 分鐘) 也是。WS 會以 XML 格式回應，列出伺服器的安全狀態。詳細請參閱第 634 頁「訊息格式」。

如果收到錯誤回應代碼 (1、2 或 255)(指出 WS 本身可用，但是部分其他 ABE 錯誤狀況已發生)，SonicWall 會記錄回應並將所有後續驗證要求重新導向到內部 `wirelessServicesUnavailable.html` 頁面。此頁面提供管理員可設定文字說明資源。

當收到回應代碼 0 (伺服器啟動) 時安全設備會繼續嘗試在設定的間隔查詢 ABE 並恢復重新導向到 WS (而不是到 `wirelessServicesUnavailable.html` 頁面)。

工作階段狀態同步

在可設定的間隔 (介於 1 到 60 分鐘)，安全設備會選擇性地傳送安全的 HTTP POST 操作到包含所有目前使用中來賓工作階段的 XML 清單的 WS。CGI post 提供 `sessionList` 做為所有使用中來賓工作階段的 XML 清單。詳細請參閱第 634 頁「訊息格式」。

功能本身是透過安全設備上的核取方塊啟用，但是預設為停用。目標 URL 是可設定的。

訊息驗證

此功能確保 CGI 資料在安全設備和源自 SonicWall 安全設備/ABE 裝置的 ABE 之間交換，並且未經竄改。如果啟用，其他名稱為 hmac 的 CGI 參數會新增到所有交換的 CGI 資料。以下是現在重新導向 URL 外觀的範例，其訊息驗證已啟用：

```
https://10.1.2.3/login.asp?sessionId=faad7f12ac26d5c2fe3236de2c149a22&ip=172.16.31.2&mac=00:90:4b:6a:37:32&ufi=0006B1020148&mgmtBaseUrl=https://10.0.61.222:4043/&clientRedirectUrl=http://192.168.168.168:80/&req=http%3A//www.google.com/&hmac=cd2399aeff26d5c2fe3236d211549acc
```

附註：SonicWall 安全設備 URL 在 req (並且僅限 req) 變數的值內為下列字元編碼：

```
% = %25
: = %3A
= %20 (space)
? = %3F
+ = %2B
& = %26
= = %3D
```

在前面範例中，HMAC 簽章是使用下列資料產生：

```
HMAC (
   faad7f12ac26d5c2fe3236de2c149a22 +
   172.16.31.2 +
   00:90:4b:6a:37:32 +
   0006B1020148 +
   https://10.0.61.222:4043/ +
   https://10.0.61.222:4043/ +
   http%3A//www.google.com/
)
```

如果啟用訊息驗證，則 SonicWall 裝置預期 HMAC 簽章為源自 ABE 的 CGI post 資料的一部分。如果 SonicWall 偵測到 HMAC 遺失或不正確，則會傳回錯誤代碼 251，而要求的操作 (例如來賓登入、帳戶建立) 會中止。

工作階段更新

工作階段更新允許 ABE 更新安全設備上現有工作階段的工作階段存留時間和閒置逾時值。這允許例如來賓使用者購買額外的時間以及加入現有的工作階段。

- 工作階段更新可在工作階段存留時間的任何時間，從 ABE 傳送到 SonicWall。
- *userName* 和 *sessionLifetime* 值必須在訊息中指定。
- 可指定 *sessID* 值。如果包含，更新屬於指定的工作階段。如果省略，更新屬於所有與指定的 *userName* 相符的工作階段。

詳細請參閱第 634 頁「訊息格式」。

訊息格式

主題：

- 第 636 頁「本機驗證回覆」
- 第 636 頁「登出要求」
- 第 637 頁「登出回覆」
- 第 633 頁「Web 伺服器狀態檢查」
- 第 633 頁「工作階段狀態同步」
- 第 639 頁「工作階段狀態同步回覆」
- 第 639 頁「本機帳戶建立請求」
- 第 639 頁「本機帳戶建立回覆」
- 第 640 頁「更新工作階段請求」
- 第 640 頁「更新工作階段回覆」

附註：XML 結構位置可能發生變更。
SonicWall 安全設備 IP 位址和連接埠是在 *mgmtBaseUrl* 變數中指定。

外部驗證要求

WS 傳送安全的 HTTP POST 操作到：
`https://sonicwall.ip.add.ress:port/externalGuestLogin.cgi`。post 參數包括這些引數：

- *sessId*：工作階段 ID
- *userName*: 完整使用者 ID
- *sessionLifetime*：使用者的工作階段存留時間 (秒)
- *idleTimeout*: 最大閒置逾時 (秒)

外部驗證回覆

安全設備傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <AuthenticationReply>
      <ResponseCode>{response code}</ResponseCode>
      <ReplyMessage>{reply message}</ReplyMessage>
   </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

`{response code}` 包括外部驗證回應代碼表格中所列的值之一。

外部驗證回應代碼

回應代碼	回應意義
50	登入成功
51	已超過工作階段限制
100	登入失敗 --存取拒絕
251	訊息驗證失敗 -- 無效的 HMAC

外部驗證回應代碼

回應代碼	回應意義
253	無效的工作階段 ID
254	無效或遺失 CGI 參數
255	內部錯誤

本機驗證請求

WS 傳送安全 HTTP POST 操作到：
`https://sonicwall.ip.add.ress:port/localGuestLogin.cgi`。post 參數包括這些引數：

- *sessId*：工作階段 ID
- *userName*: 完整使用者 ID
- *passwd*：來賓的純文字密碼

本機驗證回覆

SonicWall 傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <AuthenticationReply>
      <ResponseCode>{response code}</ResponseCode>
      <ReplyMessage>{reply message}</ReplyMessage>
   </AuthenticationReply>
</SonicWallAccessGatewayParam>
```

`{response code}` 包括本機驗證回應代碼表格中所列的值之一。

本機驗證回應代碼

回應代碼	回應意義
50	登入成功
51	已超過工作階段限制
52	無效的使用者名稱/密碼
100	登入失敗 --存取拒絕
251	訊息驗證失敗 -- 無效的 HMAC
253	無效的工作階段 ID
254	無效或遺失 CGI 參數
255	內部錯誤

登出要求

WS 傳送安全 HTTP POST 操作到：
`https://sonicwall.ip.add.ress:port/externalGuestLogoff.cgi`。post 參數包括下列引數：

- *sessId*：GW 工作階段 ID
- *eventId*：登出事件 ID。必須是以下其中一項：

登出事件 ID	事件意義
1	來賓手動登出
2	管理員將指定的來賓登出
3	來賓工作階段逾時
4	來賓閒置逾時到期

登出回覆

安全設備傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <LogoffReply>
        <ResponseCode>{response code}</ResponseCode>
        <ReplyMessage>{reply message}</ReplyMessage>
   </LogoffReply>
</SonicWallAccessGatewayParam>
```

{response code} 包括登出回應代碼表格中所列的值之一：

登出回應代碼

回應代碼	回應意義
150	登出成功
251	訊息驗證失敗 -- 無效的 HMAC
253	無效的工作階段 ID
254	無效或遺失 CGI 參數
255	內部錯誤

Web 伺服器狀態檢查

WS 傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <ServerStatus >{status code}</ ServerStatus >
</SonicWallAccessGatewayParam>
```

{response code} 包括 Web 伺服器狀態檢查回應代碼表格中所列的值之一。

Web 伺服器狀態檢查回應代碼

回應代碼	回應意義
0	伺服器啟動
1	資料庫中斷
2	設定錯誤
255	內部錯誤

工作階段狀態同步

GW 會定期傳送安全的 HTTP POST 操作到包含所有目前使用中來賓工作階段的 XML 清單的 AS。目標 URL 和時期都可由 GW 管理員設定。

CGI post 參數包含此引數：

- *sessionList*：所有使用中 GW 來賓工作階段的 XML 清單。

工作階段清單傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <SessionSync>
      <SessionCount>{Session Count}</SessionCount>
      <SessionList>
      <Session>
      <Ssid>{ESSID}</Ssid>8
      <ID>{Session ID}</ID>
      <UserName>{User Name}</UserName>
      <IP>{IP Address}</IP>
      <MAC>{MAC Address}</MAC>
      <Idle>
      {Time Idle (expressed in seconds)}
      </Idle>
      <SessionRemaining>
      {Session Remaining (expressed in seconds)}
      <SessionRemaining>
      <BaseMgmtUrl>
      {https://ip.add.re.ss:port}
      </BaseMgmtUrl>
      <RxBytes>
      {total bytes received}
      </RxBytes>
      <TxBytes>
      {total bytes transmitted}
      </TxBytes>
      </Session>
   </SessionList>
</SessionSync>
</SonicWallAccessGatewayParam>
```

工作階段狀態同步回覆

WS 傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <SessionSync>
      <ResponseCode>{response code}</ResponseCode>
   </SessionSync>
</SonicWallAccessGatewayParam>
```

{response code} 包括工作階段狀態同步回覆回應代碼表格中所列的值之一。

工作階段狀態同步回覆回應代碼

回應代碼	回應意義
200	同步成功
201	同步失敗
255	內部錯誤

本機帳戶建立請求

WS 傳送安全 HTTP POST 操作到：
`https://sonicwall.ip.add.ress:port/createGuestAccount.cgi`。post 參數包括這些引數：

- *userName*: 完整使用者 ID (最長長度：32)
- *passwd*：來賓的純文字密碼 (最長長度：64)
- *註解*：(可選)(最長長度：16).預設**(NULL)**
- *enforceUniqueLogin*: 可選: 1=true，0=false。預設 **1**
- *activateNow*：可選: 1=true，0=false。預設 **0**
- *autoPrune*：可選: 1=true，0=false。預設 **1**
- *accountLifetime*：使用者的帳戶存留時間 (以秒表示)
- *sessionLifetime*：使用者的工作階段存留時間 (以秒表示)
- *idleTimeout*: 最大閒置逾時 (以秒表示)

本機帳戶建立回覆

安全設備傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <AccountCreationReply>
      <ResponseCode>{response code}</ResponseCode>
      <ReplyMessage>{reply message}</ReplyMessage>
```

```
    </AccountCreationReply>
  </SonicWallAccessGatewayParam>
```

{response code} 包括本機帳戶建立回覆回應代碼表格中所列的值之一。

本機帳戶建立回覆回應代碼

回應代碼	回應意義
10	帳戶建立成功
11	帳戶上限
12	帳戶存在
251	訊息驗證失敗 -- 無效的 HMAC
254	無效或遺失 CGI 參數
255	內部錯誤

更新工作階段請求

ABE 的 POST 可以此格式在 `externalGuestUpdateSession.cgi` 製作到安全設備：

```
https://10.1.2.3:4043/externalGuestUpdateSession.cgi?sessId=11aa::00ff&userName=gue
st&sessionLifetime=600&idleTimeout=180
```

post 參數包括這些引數：

- *sessId*：可指定此值。如果未指定此值，則更新所有與指定的使用者名稱相符的來賓工作階段。
- *userName*: 此值必須指定，因其定義已更新的使用者工作階段的名稱 (或者若未提供工作階段 ID 則可能是工作階段)。
- *sessionLifetime*：此值必須指定，因其定義指派到工作階段的秒數。可以是 1 到 863,913,600 的任何數字。
- *idleTimeout*: 可指定此值。其：
  - 定義指派到工作階段的秒數。
  - 可以是 1 到 863,913,600 的任何數字。
  - 必須小於或等於 *sessionLifetime*。

  如果未提供 *idleTimeout*，保留工作階段的現有 *idleTimeout* 值。

更新工作階段回覆

安全設備傳回此格式的 XML 回應：

```
<?xml version="1.0" encoding="UTF-8">
<SonicWallAccessGatewayParam
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
   SonicWallAccessGatewayParam.xsd">
   <UpdateSessionReply>
      <ResponseCode>{response code}</ResponseCode>
      <ReplyMessage>{reply message}</ReplyMessage>
   </ UpdateSessionReply >
</SonicWallAccessGatewayParam>
```

{response code} 包括更新工作階段回覆回應代碼表格中所列的值之一。

更新工作階段回覆回應代碼

回應代碼	回應意義
210	工作階段更新成功
211	工作階段更新失敗
251	訊息驗證失敗 -- 無效的 HMAC
254	無效或遺失 CGI 參數
255	內部錯誤

常見問題集 (FAQ)

主題：

LHM 伺服器指令碼必須以 ASP 撰寫嗎？

否。LHM 伺服器指令碼可使用任何能夠處理 Web 請求和 XML (兩個 LHM 的核心元件) 的平台撰寫。這包含 Perl、PHP、ASP、ASP.NET 和 J2EE。

為何這些新指令碼以 ASP.NET 撰寫？

新指令碼選擇 ASP.NET 是因為其普遍性，還有它能很好處理許多事情，不僅是它容易處理 XML 而已。

我可以如何使用 LHM 來提供有限使用者來賓服務存取權？

雖然來賓服務 (之前稱為 WGS 或無線來賓服務) 是專為為無線 (熱點) 使用者設計，來賓服務也可供有線使用者採用，只要將有線介面 (或介面，如果是在具有 PortShield 的 PRO1260 上) 置入停用在 SonicPoint 強制措施的無線區域中即可。然後將所有來賓服務選項套用到有線使用者，包括其他、LHM、動態位址轉譯、允許/拒絕網路。

驗證和授權之間有何差異？

*驗證*說明使用者回應某些種類的質詢的程序。質詢可以是任何內容，傳統上多是 `username:password`。LHM 會透過摘要驗證內容來中斷傳統模型的相依性。驗證器的角色是由 LHM 伺服器履行，而驗證方式則只能通過想像來約束。可考慮以下驗證方式：

- 提供有效的使用者名稱和密碼
- 猜測電腦產生的號碼
- 完成此問卷調查
- 以至少 80% 的分數通過測驗
- 按一下**我接受**按鈕

驗證後，可授權用戶端執行一些操作。

*授權*是授予某些事物的存取權的程序。為讓授權有用，授權者必須備有阻止用戶端獲取受保護資源的措施。若是 LHM，SonicWall 為用戶端的閘道 (不論有線或無線)，所以它可以非常有效地作為授權者執行操作。在 SonicWall 收到用戶端驗證器的 OK (確定) 後，它會建立來賓服務工作階段並允許用戶端存取網際網路。

我可以透過 LHM 使用 LDAP、RADIUS、按鈕、當日時間、茶葉占卜、問卷調查、相關氣壓、密碼，甚至驗證器來提供存取權嗎？

是。

可以 SonicWall 為我撰寫能夠做出該操作的指令碼嗎？

我們已提供一系列樣本指令碼做為範例，您可以自由修改，但我們不提供自訂指令碼。不過我們可以讓您聯繫能夠提供自訂指令碼的人員。有許多 SonicWall 夥伴擁有 Web 開發團隊，能夠提供這些服務。

我想要使用 SonicWall 所提供的樣本指令碼。我需要做些什麼才能使用它們嗎？

您需要：

- Microsoft Windows 2000、XP、執行 IIS 5.0 或更高版本的 2003 平台、執行最新 Service Pack 和 Hotfix。
- Microsoft .NET 1.1 (或更高版本) Framework：
  http://www.microsoft.com/downloads/details.aspx?FamilyId=262D25E3-F589-4842-8157-034D1E7CF3A3&displaylang=en

- 最新 .NET Framework Service Pack：
  http://www.microsoft.com/downloads/details.aspx?familyid=A8F5654F-088E-40B2-BBDB-A83353618B38&displaylang=en

若要使用指令碼：

1 複製您要用於 `wwwroot` 目錄 (通常是在 `C:\inetpub\wwwroot`) 的 LHM 指令碼。

2 在您的 SonicWall 設定來賓服務以使用外部來賓驗證，如第 644 頁「所有 LHM 設定是指什麼？我要如何設定它們？」中所述。

部分指令碼需要寫入權限，尤其是使用資料庫者。依據您的設定而定，兩位或三位個別「使用者」對於要求寫入的指令碼目錄需要擁有寫入權限。

- 第一個帳戶 (所有平台) 是 **IUSR_MACHINENAME** (其中 *machinename* = 本機的名稱)。
- 第二個帳戶在：
  - Windows XP 是 **ASPNET** (ASP.NET 機器帳戶)。
  - 其他平台是 **IWAM_MACHINENAME** (其中 *machinename* = 本機的名稱)。
- 如果資料庫讀取/寫入存取權即使在指派這些權限後仍然無法使用，可能需要為 **NETWORK SERVICE** 帳戶新增讀取/寫入權限。

ⓘ **附註：**1.1 之前的 .NET Framework 版本在網域控制器上有使用者權限問題 (http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315158)。強烈建議安裝 1.1 (或更高版本)。

3 環境設定好之後，您需要自訂指令碼。這項操作已盡可能加以簡化，只要把重要的可設定位元置於 `myvars.aspx` 檔案中即可。所有項目都妥善註解，而其目的和語法應該都很顯眼。也可進一步自訂指令碼，但是一般是不需要的。

LHM 伺服器可以位在何處？

LHM 伺服器可以實際上在網路中的任何地方，只要來賓用戶端能夠聯繫到。它可以位在中央網路作業中心，由該處針對多個熱點管理 LHM，或者與單一 SonicWall 安全裝置並存。

為什麼我的來賓用戶端無法聯繫 LHM 伺服器，或者為何 LHM 伺服器上的頁面未載入？

來賓用戶端會直接與 LHM 伺服器通訊；而通訊不會由 SonicWall 安全裝置代理。換句話說：

- 來賓用戶端子網路必須能夠聯繫 LHM 伺服器。
- LHM 伺服器必須知道如何聯繫來賓用戶端的子網路 (透過路由、NAT 或 VPN)。
- 防火牆存取規則必須設定為允許賓用戶端子網路聯繫 LHM 伺服器。

LHM 交換在 SonicWall 和 LHM 伺服器間如何運作 (確切的版本、一般環境)？

1 來賓用戶端關聯、取得 DHCP 租用，並啟動 Web 瀏覽器。

2 DNS 可通過 SonicWall 安全設備。URL FQDN 會解析至其 IP 位址。

3 SonicWall 安全設備會檢查來賓用戶端是否具備驗證工作階段。

- 若是新的，SonicWall 安全設備會將用戶端重新導向到內部重新導向 (正在重新導向，請稍候) 頁面。

4 內部重新導向頁面會嘗試將來賓用戶端重新導向至 LHM 伺服器。

- 如果失敗，它會將用戶端重新導向到內部伺服器關機 (無線網際網路存取暫時不可用。請按一下此處重試。) 頁面。

5 來賓用戶端會重新導向至 LHM 伺服器。在重新導向 URL 中，安全設備內嵌 querystring 資訊，說明萌芽工作階段 (例如 sessionID、用戶端的 MAC 和 IP 位址、安全設備的 LHM 管理 IP 和連接埠、UFI、原來要求的 URL)。

- LHM 伺服器指令碼會抓取 querystring 資訊。
- 用戶端直接從 LHM 伺服器擷取 LHM 登陸頁面。

6 依據使用的授權模型 (例如 username:password、passcode、**I Accept** 按鈕)，LHM 伺服器會決定來賓用戶端是否值得存取。

7 LHM 伺服器會向設定的管理連接埠 (例如 TCP 4043) 的 SonicWall 安全設備起始 Web 請求 externalGuestLogin.cgi 頁面。

- LHM 伺服器會 POST sessionID (在步驟 5 中取得) 連同 username (從使用者取得或由使用者組成) 和 session-lifetime 以及 idle-timeout (二者均由其決定)。

8 安全設備會驗證 sessionID，嘗試建立工作階段，然後回應 POST，並包含結果代碼，說明是否能夠授權 (建立) 來賓工作階段。

9 LHM 伺服器會解釋結果代碼並報告結果 (例如工作階段已授權 – 您現在可以開始瀏覽、工作階段建立失敗 – 糟糕、工作階段上限) 給來賓用戶端。

所有 LHM 設定是指什麼？我要如何設定它們？

與其進入第 622 頁「有關輕量級熱點訊息 (LHM)」的完整詳細資料，不如只說明設定的意思以及可以如何進行設定：

無線 SonicOS 上的 LHM 設定是在**編輯區域 -WLAN** ` 對話方塊進行。

主題：

一般

本機 Web 伺服器設定定

用戶端重新導向通訊協定	SonicWall 安全裝置在透過正在重新導向，請稍候頁面執行初始內部用戶端重新導向時，所使用的通訊協定 (HTTP 或 HTTPS)。(此訊息可從 **Web 內容**標籤的**重新導向訊息**區域進行設定。)此步驟是在重新導向到 LHM 伺服器之前。

外部 Web 伺服器設定

Web 伺服器通訊協定	在 LHM 伺服器上執行的通訊協定 (HTTP 或 HTTPS)
Web 伺服器主機	LHM 伺服器的 IP 或可解析的 FQDN。
Web 伺服器連接埠	LHM 伺服器上所選通訊協定的 TCP 連接埠操作。
連線逾時	LMH 伺服器被視為在重新導向嘗試時無法使用之前的持續時間 (以秒計)。逾時時，會向用戶端顯示在 **Web 內容**標籤上設定的伺服器當機訊息。

訊息驗證

啟用訊息驗證	在與 LHM 伺服器通訊時使用 HMAC 摘要和內嵌的查詢字串。如果您在使用 HTTP 與 LHM 伺服器通訊時擔憂訊息竄改，這會相當有用。可選。
驗證方法	選擇 **MD5** 或 **SHA1**。
共用密碼	雜湊的 MAC 的共用密碼。如使用，也需要再 LHM 伺服器指令碼上設定。

驗證頁面

外部驗證頁面

ⓘ **附註：**這些頁面在 LHM 伺服器可能每一個是獨有的頁面，或者可能都是相同頁面，但含有每個狀態訊息的個別事件處理程式。為使用新開發的指令碼，提供的範例如下。

登入頁面	用戶端被重新導向的第一個頁面 (例如 `lhm/accept/default.aspx`)。
工作階段過期頁面	用戶端在工作階段到期被重新導向的頁面 (例如 `lhm/accept/default.aspx?cc=2`)。工作階段到期後，使用者必須建立新的 LHM 工作階段。
閒置逾時頁面 -	用戶端在超過閒置計時器時被重新導向的頁面 (例如 `lhm/accept/default.aspx?cc=3`)。超過閒置計時器後，使用者可以使用相同認證再次登入，只要工作階段還有時間剩下。
最大工作階段頁面	用戶端在達到工作階段數上限時被重新導向的頁面 (例如 `lhm/accept/default.aspx?cc=4`)。

Web 內容

重新導向封包

向用戶端展示的預設或自訂訊息 (通常不超過一秒) 說明工作階段即將重新導向至 LHM 伺服器。使用這個間質性頁面 (而不是直接前往 LHM 伺服器)，讓安全設備可以驗證 LHM 伺服器的可用性。

伺服器關閉訊息

當重新導向判定 LHM 伺服器在不可用狀態時，向用戶端展示的預設或自訂訊息。

進階

下列參數為選用。

自動工作階段登出	當工作階段登出時 (自動或手動)，時間增量與發佈 SonicWall 安全裝置的網頁。
伺服器狀態檢查	時間增量與發佈 SonicWall 的網頁，決定了 LHM 伺服器上或背後元件的可用性 (例如後端資料庫)。
工作階段同步	時間增量與發佈整個來賓服務工作階段表格的 SonicWall 的網頁。這可讓 LHM 伺服器同步處理來賓使用者在會計、帳單或啟發學習法方面的狀態。

我是否能從預設的 TCP4043 變更 LHM 管理連接埠？

是。這在 SonicOS 很容易做到，只要修改外部來賓驗證服務物件的連接埠值即可。

我是否需要使用 HMAC 選項？如果我想要使用，該如何使用？

HMAC 功能是選用的。它確保 SonicWall 傳送至 LHM 伺服器，再 LHM 伺服器傳送至 SonicWall 安全設備的訊息未經竄改。HMAC 獲得此項的方法是藉由計算在兩個對等項之間傳遞的資訊相關鍵控式 (密碼輔助) 訊息驗證碼，並且將計算出的摘要加入到資料中。一旦接收到資料，另一端會計算摘要本身，並拿它與傳輸的 MAC 做比較。若兩個相符，資料就會完整地傳遞。如果您是在不安全的環境，或有其他安全性考量，則應考慮使用 HMAC 選項。

若選擇使用 HMAC，您可實作自己的 HMAC 常式，而最簡單的方法是使用 SonicWall 撰寫的 `SonicSSL.dll` 程式庫，以及隨 OpenSSL 免費提供的 `libeay32.dll`，而 SonicWall 可應要求提供這兩個檔案。

使用 HMAC：

1. 複製 `libeay32.dll` 檔案至 LHM (IIS) 伺服器的路徑 (例如複製到 `C:\Windows\system32` 資料夾中)。
2. 複製 `SonicSSL.dll` 檔案到相同伺服器上的任何位置。
3. 使用 `regsvr32SonicSSL.dll` 命令註冊 `SonicSSL.dll` 檔案。

完成後，LHM 指令碼可使用 `Server.CreateObject(SonicSSL.Crypto)` 物件供 HMAC 計算之用。HMAC 功能包含在指令碼說明第 647 頁「LHM 指令碼程式庫」中。

重要：SonicWall 安全設備 URL 編碼 (從其 ASCII 表示法轉換特定字元為十六進位表示法) `querystring` 的 `req` (原來要求的 URL) 部分，但是 URL 編碼的 SonicWall 方式與 Microsoft 方式稍有不同 (例如，`Request.QueryString` 所採用)。因為兩方式的此差異，在 HMAC 上執行的字串在安全設備和 LHM 伺服器間可能不同。所提供的指令碼會透過手動編碼 `querystring` 的 `req` 部分來彌補此項，並且與 SonicWall 方式一致。

SonicWall 對於這些指令碼提供任何支援嗎？

提供的指令碼是做為範例，SonicWall 技術支援並不支援，SonicWall 支援也不會協助設定您的 LHM 後端環境。未來的諮詢支援服務也許處理此狀況。

我撰寫了新指令碼，或者我對您的指令碼做些增強，或者我剛改善您的指令碼使其比之前更好，SonicWall 是否感興趣？

是！我們始終在尋找使用 LHM 的新方式，以及能夠對可用指令碼的程式庫有所貢獻的人。我們考慮在任何平台上撰寫的 LHM 指令碼並使用任何驗證方式。請傳送電子郵件到 products@sonicwall.com 說明您的指令碼，我們會考慮將其加入我們的程式庫。提交指令碼可給予 SonicWall 權限自由修改和/或重新分配所提交的指令碼。

LHM 指令碼程式庫

SonicWall LHM 指令碼程式庫是建立為資源，提供給使用或想要使用來賓服務適用的 LHM 的人們。目標是為吸引更多貢獻者和使用者，協助程式庫成長為容納大型、各種不同和實用集合的指令碼，任何人都可以修改或原樣使用。

程式庫的第一個貢獻包括六個指令碼：部分回應一般使用者的要求 (accept、guestbook 和 adauth)，部分則回應非一般要求 (lhmquiz、random 和 paypal)。它們是在 Visual Studio .NET 開發環境外撰寫，所以樣式可能不同。不過對所有指令碼通用，如：

- 將可設定的變數模塊化，例如檔案路徑、伺服器 IP 位址、使用快顯登出視窗、salt 值和計時器設定。這些可設定的值會收集到 myvars.aspx 檔案中，以便每個環境編輯可在一處執行，而不用搜尋可設定的元素。
- 廣泛說明逐步內容。

chooser.aspx 登陸頁已在指令碼目錄的最上層提供。此指令碼是為展示環境設計，可選取較低層級 (特定) 的指令碼而無須在 SonicWall 安全設備上重新設定 LHM 設定，以指向特定指令碼。換句話說，安全設備上的' LHM 可設定為指向上層 chooser.aspx 指令碼，然後列舉所有子目錄 (較低層指令碼，例如 random、accept、adauth)。上層 chooser.aspx 指令碼會在新視窗開啟目標下層 default.aspx 指令碼，然後傳遞整個原始 querystring。

所有以 default.aspx 頁面開始的指令碼和用戶端重新導向會依需要自動執行。因此 SonicWall 上的 LHM 設定應在適當路徑指向 default.aspx 頁面 (例如 lhm/accept/default.aspx 或 lhm/adauth/default.aspx)。部分指令碼有個別的管理功能頁；這些均在指令碼說明中註明。

每個指令碼也會提供 logout.aspx 頁面。此頁面的使用可以 myvars 中的 logoutPopup 變數控制。設定 1 值可啟用快顯登出視窗。從安全設備順利收到回應代碼 (50) 後，LHM 驗證程序會叫用視窗。指令碼將 sessID、mgmtBaseUrl 和 sessTimer 變數傳送至 logout.aspx 視窗，如此一來，當/如果使用者想要手動終止工作階段，該視窗便可追蹤工作階段時間，針對正確的工作階段 (sessID) 將登出事件發佈回到安全設備 (在 mgmtBaseUrl)。

關於登出快顯視窗的使用

- 不需要使用登出快顯視窗。工作階段在其設定的存留時間到期後，會自行逾時。快顯視窗只是提供使用者一個手動終止自己的工作階段的機制。
- 視窗使用 javascript 彈出技術啟動，如此快顯封鎖程式會封鎖視窗。
- 關閉視窗不會使工作階段插斷。只有登出按鈕可使工作階段結束。
- 由於倒數計時器在用戶端執行，因此採取一些步驟來阻止重新整理頁面。重新整理頁面會重設用戶端倒數計時器，但不影響實際的工作階段計時器。F5 鍵和滑鼠右鍵事件被擷取和隱藏，不是在所有的瀏覽器上都能運作。
- 登出快顯視窗的使用，應與指令碼驗證配置一致。
    - 有些指令碼具有非獨佔登入程序，意思是使用者可以重複地登入 (例如 Accept 和 ADAuth 指令碼)。建議多在這些非獨佔指令碼使用登出快顯視窗。

- 有些指令碼為非獨佔，只是收集的資料應保持唯一性 (例如 Guestbook 和 LHMQuiz 指令碼)。在這些指令碼上使用登出快顯視窗是可接受的，但可能導致收集到多餘的資料。
- 有些指令碼是獨佔的，意思是在經過使用者驗證後，若無某種成本 (例如 PayPal 指令碼或 Random 指令碼，其中 useDB 已啟用)，無法重複執行驗證程序。不建議在這些指令碼上使用登出快顯視窗，因為沒有可讓使用者再登入的簡單方法。

指令碼也為 .NET 程序錯誤提供隱藏式輸入，其中隱藏文字的方式是使用與背景色相符。在發生失敗或錯誤的情況下，可能提供錯誤輸出，然後在網頁上點擊 CTRL-A 使其顯現後，選取所有的文字。

以下為每一個指令碼的描述、有何功用，以及運作方式。 將新指令碼加入到程式庫時，隨著它們的類似描述有助於了解、自訂及整合。

主題：

Accept 指令碼

驗證模型	來賓用戶端按一下**我接受**按鈕。	
目的	向用戶端展示可接受的使用原則、服務條款或歡迎畫面。	
myvars 變數	logoutPopup	控制登出快顯視窗的使用。設定為： • **0** 停用快顯視窗。 • **1** 啟用快顯視窗。
	sessTimer	工作階段計時器以秒計。
	idleTimer	閒置計時器以秒計。
	username	使用者名稱套用至來賓工作階段。由於指令碼未包含用戶端的使用者名稱，它可能： • 在這裡明確地為所有的用戶端設定。 • 設定為 useMAC 以將使用者名稱設定為 MAC 位址。
	strHmac	可選 HMAC 功能的共用密碼。
	hmacType	若 HMAC 在使用中時所使用的摘要類型：**MD5** 或 **SHA1**。
	標誌	標誌 (影像) 檔案名稱使用於頁首。
工作階段流程	1 來賓用戶端按一下**我接受**按鈕。 2 LHM 發佈字串會與 sessionID、使用者名稱 (MAC 任一預設)、預設的工作階段存留時間和閒置存留時間組合。 3 指令碼執行 LHM 發佈至 SonicWall 安全設備以授權該工作階段。	
其他注意事項	只需要基本的 LHM 設定。	

主題：

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
         Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/accept/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
```

```
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Set the userName to the grabbed client MAC address if so configured in myvars
   If userName = "useMAC" Then
      userName = mac
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req
```

```
      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
```

```
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
Authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub


</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}
```

```
.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Accept Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Welcome <%=
ip%></b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
   <td><br></td>
   </tr>
   <tr>
      <td align=left>
      By clicking the <b>Accept</b> button below, you accept the following terms of
service:<br><br><b>
      1. You will not try to download bad things.<br>
      2. You will not try to upload bad things.<br>
      3. You will not try to use all the bandwidth so that others have none.<br>
      4. You will be happy when the SonicWALL blocks bad things from reaching
you.</b><br><br>
      </td>
      <td>
   </tr>
   <tr>
      <td><br><asp:button id="btnSubmit" class="button" text="  Accept  "
onClick="btnSubmit_Click" runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
         Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"
```

```
   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
         LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."
```

```
      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>
```

```
<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
```

```
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
```

```
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the username to record for LHM session since this does not gather one. Set to
userName="useMAC" to use the MAC addess.
Dim userName="useMAC"
'Dim userName = "LHM Guest User"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"
```

```
'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

ADAuth 指令碼

驗證模型

來賓用戶端提供其使用者名稱和密碼。然後對照 Active Directory 或 LDAP 資料庫驗證這些認證。

目的

透過 LDAP 使用 Active Directory 的傳統授權模式支援每一使用者工作階段計時器和閒置計時器設定，而此設定是在授權期間透過選擇性地從資料庫擷取 LDAP 屬性來提供。

myvars 變數

`logoutPopup`	控制登出快顯視窗的使用。設定為： • **0** 停用快顯視窗。 • **1** 啟用快顯視窗。
`myLdapServer`	提供驗證之 LDAP/AD 伺服器的 IP 位址或可解析的 FQDN。
`myLdapDomain`	LDAP/AD 網域名稱
`retrAttr`	指定是否從驗證使用者的 LDAP 屬性 (之後定義) 來擷取工作階段和閒置計時器值。設定為： • **0** 停用擷取。 • **1** 嘗試擷取。
`useCN`	如果 `reAttr=1`，那麼此旗標會設定是否使用一般名稱 (`cn`) 來擷取屬性或 AD 預設登入名稱 (`sAMAccountName`)。 設定為 **1** 以使用 `cn`。驗證 AD 時，此旗標應設定為 **0**。
`sessAttr`	要對其擷取工作階段計時器的 LDAP 屬性 (以秒計)。如果無法擷取任何值，或擷取的值不是數字時，便使用預設工作階段計時器 (`sessTimer` 如下定義)。
`idleAttr`	要對其擷取閒置計時器的 LDAP 屬性 (以秒計)。如果無法擷取任何值，或擷取的值不是數字時，便使用預設閒置計時器 (`idleTimer` 如下定義)。
`sessTimer`	預設工作階段計時器以秒計。
`idleTimer`	預設閒置計時器以秒計。
`strHmac`	可選 HMAC 功能的共用密碼。
`hmacType`	若 HMAC 在使用中時所使用的摘要類型：**MD5** 或 **SHA1**。
標誌	標誌 (影像) 檔案名稱使用於頁首。

工作階段流程	1 來賓用戶端輸入其 LDAP/AD 使用者名稱和密碼。 2 所提供的認證用於與已設定的 LDAP 伺服器繫結。 3 若繫結成功，使用者便已驗證。 4 若設定 `reAttr` 旗標，會嘗試從 LDAP DB 擷取定義的 `sessAttr` 和 `idleAttr` 屬性 (例如 `pager` 和 `mobile`)。若擷取有效的結果，便會使用這些結果，否則使用預設值。 5 指令碼執行 LHM 發佈至 SonicWall 安全設備以授權該工作階段。
其他注意事項	要求 LHM 伺服器能夠與已設定的 LDAP/AD 伺服器透過路由、NAT 或 VPN 進行通訊。若使用 `reAttr` 選項，其要求定義 LDAP 屬性以讓使用者特定的值生效。 **附註：**`pager` 和 `mobile` 屬性被選取的原因是它但的不太常使用，另一個原因是它們可以直接透過 Microsoft 的使用者和電腦 MMC 做設定)。

主題：

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Math" %>
<%@ Import Namespace="System.DirectoryServices" %>
<%@ Import Namespace="System.Collections" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Assembly name="System.DirectoryServices, Version=1.0.3300.0,
Culture=neutral,PublicKeyToken=b03f5f7f11d50a3a"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/adauth/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig
```

```
Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
   authResult.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
```

```
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtPassword.Text = ""
   authResult.Text=""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Try to connect to LDAP with the user supplied attributes
   Try
      Dim ldapPath as String = "LDAP://" & myLdapServer
      Dim ldapUser as String = myLdapDomain & "\" & txtName.Text
      Dim validateUser as New DirectoryEntry(ldapPath,ldapUser,txtPassword.Text)

      'This is the actual authentication piece
```

```
      Dim nativeCheck as Object = validateUser.NativeObject

      'If retrAttr is set in the myvars file, attempt to retrieve the session and
idle values from LDAP
      If retrAttr = "1" Then
         Dim mySearch as New DirectorySearcher(validateUser)

         'Check the myvars for selecting either sAMAccountName or cn
         If useCN = "0" Then
            mySearch.Filter = "(sAMAccountName=" & Server.URLEncode(txtName.Text) &
")"
         Else
            mySearch.Filter = "(cn=" & Server.URLEncode(txtName.Text) & ")"
         End If
         mySearch.PageSize="1"
         mySearch.PropertiesToLoad.Add(sessAttr)
         mySearch.PropertiesToLoad.Add(idleAttr)
         Dim adResult as SearchResult

         'If we get results on the attribute query, set timer values
         adResult = mySearch.FindOne
         If Not (adResult is Nothing) Then
            If (adResult.Properties.Contains(sessAttr)) Then
                  'Check to see if the LDAP value returned is a number
                  Dim isNumber as New RegEx("^\d+$")
                  If (isNumber.IsMatch(adResult.Properties(sessAttr)(0).ToString()))
Then
                     sessTimer=adResult.Properties(sessAttr)(0).ToString()
                  End If
            End If 'End If sessAttr
            If (adResult.Properties.Contains(idleAttr)) Then
                  'Check to see if the LDAP value returned is a number
                  Dim isNumber as New RegEx("^\d+$")
                  If (isNumber.IsMatch(adResult.Properties(idleAttr)(0).ToString()))
Then
                     idleTimer=adResult.Properties(idleAttr)(0).ToString()
                  End If
            End If 'End if idleAttr
         End If 'End if adResult is present
      End If 'End if retrAttr is in use

      authResult.Text="<font color=""green""><b>Credentials
Accepted.</b></font><br>Session Lifetime: " & round(sessTimer/60) & "
minutes.<br>Idle Timer: " & round(idleTimer/60) & " minutes."

      'Auth succeeded - move on to LHM Auth
      LHM()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         authResult.Text="<font color=""Red""><b>Credentials
Rejected.</b></font><br>Please enter a valid username and password. "
   End Try

End Sub

Sub LHM()

      'Let the user know that we are setting up the session, just in case it takes
more than a second
      LHMResult.Text = "Authorizing session. Please wait."
```

```
      'The LHM cgi on the SonicWALL - this does not change
      Dim loginCgi as String = "externalGuestLogin.cgi"

      'Assemble the data to post back to the SonicWALL to authorize the LHM session
      Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

      'Combine mgmtBaseUrl from the original redirect with the login cgi
      Dim postToSNWL as String = mgmtBaseUrl & loginCgi

      'Convert the loginParams to a well behaved byte array
      Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

      Try
         'Create the webrequest to the SonicWALL
         Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

         'Calculate the length of the byte array
         toSNWL.ContentLength = byteArray.Length

         'Set the method for the webrequest to POST
         toSNWL.Method = "POST"

         'Set the content type
         toSNWL.ContentType = "application/x-www-form-urlencoded"

         'Open the request stream
         Dim dataStream As Stream = toSNWL.GetRequestStream()

         'Write the byte array to the request stream
         dataStream.Write(byteArray, 0, byteArray.Length)

         'Close the Stream object
         dataStream.Close()

         'Get the response
         Dim snwlReply As WebResponse = toSNWL.GetResponse()

         'Display the status - looking for 200 = OK.
         'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

         'Grab the response and stuff it into an xml doc for possible review
         Dim snwlResponse as XmlDocument = New XmlDocument()
         snwlResponse.Load(snwlReply.GetResponseStream())

         'Set the xPath to the SNWL reply, and get the response
         Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

         'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

         'Response code 50 - Login Succeeded
         If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

            'Do we want to provide a logout popup window?
            If logoutPopup = "1" Then
               'Popup hack using Javascript for logout window
               Dim sb As New System.Text.StringBuilder()
               sb.Append("<script language='javascript'>")
```

```
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
          End If

            LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

        'Response code 51 - Session Limit Exceeded
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
            LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

        'Response code 100 - Login Failed.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

        'Response code 251 - Bad HMAC.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        'Response code 253 - Invalid SessionID.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

        'Response code 254 - Invalid CGI.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        'Response code 255 - Internal Error.
        ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
            LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

        End If

        'Close the streams
        dataStream.Close()
        snwlReply.Close()
```

```
        'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
        Catch ex as Exception
           catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
           LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
     End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM ADAuth Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LDAP/AD LHM
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Wecome <%= ip%> to SonicWALL's LHM AD/LDAP
Authenticator.</b><br><br>Enter your LDAP or Active Directory username and password
to obtain secure guest internet access.<br><br>If your domain account specifies
session timeout values, those values will be applied to your account, otherwise you
```

```
will receive the default one hour (60 minutes) of access with a five minute idle
timeout.<br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white">Authentication domain:
<%=myLdapDomain%></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your login name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your password:</td>
      <td width="30%"><asp:TextBox id="txtPassword" textmode="password"
runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPassword"
ControlToValidate="txtPassword" ErrorMessage="Please enter your password."
runat="server" /></td>
   </tr>
   <tr>
      <td></td><td><asp:Label id=authResult runat="server" /> </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
```

```
<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
```

```
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
      End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";
```

```
function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
```

```
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
```

```
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is encouraged because the login event is
non-exclusive.
Dim logoutPopup as String = "1"

'Set the LDAP server IP or Name
Dim myLdapServer as String = "10.50.128.40"

'Set the LDAP domain
Dim myLdapDomain as String = "sv.us.sonicwall.com"

'Set the retrAttr to 0 to use default session and idle timeouts
'Set the retrAttr to 1 to try to retrieve the session and idle timeouts from LDAP
attributes.
Dim retrAttr as String ="1"

'Set useCN=1 to use common name (e.g. "joe levy", non-Active Directory LDAP) for
attribute retrieval (retrAttr).
'Set useCN=0 to use saMACcountName (e.g. "jlevy", Active Directory / Windows) for
attribute retrieval.
Dim useCN as String = "0"

'If using retrAttr=1, you must define the ldap attributes from which to retrieve the
values
   'Set the ldap attribute from which to retrieve the session timeout value (use is
optional)
   Dim sessAttr as String = "pager"
```

```
   'Set the ldap attribute from which to retrieve the idle timeout value (use is
optional)
   Dim idleAttr as String = "mobile"

'If retrAttr=0, of if no attributes value can be retrieved, use the following
timeout values
   'Set the default LHM Session Timeout (for when no attributes is retrieved)
   Dim sessTimer as String = "3600"

   'Set the default LHM Idle Timeout (for when no attributes is retrieved)
   Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------
</script>
```

來賓指令碼

驗證模型

來賓用戶端提供其名稱、地址、電話、電子郵件、URL (選用) 和註解 (選用) 資訊。

目的

收集市場資訊，並將資訊寫入資料庫以供日後使用。

myvars 變數

`logoutPopup`	控制登出快顯視窗的使用。設定為： • **0** 停用快顯視窗。 • **1** 啟用快顯視窗。
`sessTimer`	工作階段計時器以秒計。
`idleTimer`	閒置計時器以秒計。
`strHmac`	可選 HMAC 功能的共用密碼。
`hmacType`	若 HMAC 在使用中時所使用的摘要類型：**MD5** 或 **SHA1**。
標誌	標誌 (影像) 檔案名稱使用於頁首。

工作階段流程

1 來賓用戶端輸入其個人資訊，然按一下「提交」。
2 輸入的資訊會寫入本機 `.mdb` 資料庫檔案以供日後使用。
3 LHM 發佈字串會與 `sessionID`、使用者名稱 (以 Web 表單形式提供)、預設的工作階段存留時間和閒置存留時間組合。
4 指令碼執行 LHM 發佈至 SonicWall 安全設備以授權該工作階段。

其他注意事項

由於正將指令碼寫入資料庫，所以有必要為 **IUSR_MACHINENAME** 和 **IWAM_MACHINENAME** (或 **ASPNET**) 帳戶設定寫入權限，如第 642 頁「我想要使用 SonicWall 所提供的樣本指令碼。我需要做些什麼才能使用它們嗎？」中所述。

主題：

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
```

```
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
```

```
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtAddress.Text = ""
   txtCity.Text = ""
   txtState.Text = ""
   txtZip.Text = ""
   txtPhone.Text = ""
   txtEMail.Text = ""
   txtURL.Text = ""
   txtComment.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Try
      'Try to write the submitted info to the database file
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

      Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
"','" & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try
```

```
   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
```

```
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If
```

```
      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
```

```
      <td>Wecome <%= ip%> to SonicWALL's LHM Guestbook. In exchange for providing us
with your contact information,
      along with your permission to occassionally contact you while you are in the
middle of dinner, we will
      provide you with <b>one complimentary hour of secure internet access.</b><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your address:</td>
      <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your city:</td>
      <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your State:</td>
      <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your zip code:</td>
      <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip code."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your phone number:</td>
      <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone number."
Display="Dynamic" runat="server" />
```

```
      <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\(\d{3}\)?)|(\d{3}-))?\d{3}-
\d{4}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your  email address:</td>
      <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
      <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*" ErrorMessage="Please
enter a valid email address." Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="valTxtEnail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email address."
Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your web site URL (optional):</td>
      <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
   </tr>
   <tr>
      <td valign="top" width="30%"><br>Enter a comment (optional):</td>
      <td width="30%"><asp:TextBox id="txtComment" width="300px" height="100px"
textmode="MultiLine" tabindex="4" runat="server" /></td>
   </tr>
   <tr>
      <td></td>
      <td><br><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
```

```
<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/guestbook/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1
004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://1
0.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.go
ogle.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
```

```
        LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
     End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If
```

```
   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   txtName.Text = ""
   txtAddress.Text = ""
   txtCity.Text = ""
   txtState.Text = ""
   txtZip.Text = ""
   txtPhone.Text = ""
   txtEMail.Text = ""
   txtURL.Text = ""
   txtComment.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Try
      'Try to write the submitted info to the database file
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("guestbook.mdb") & ";"

      Dim MySQL as string = "INSERT INTO Guestbook (Name, Address, City, State, Zip,
Phone, EMail, URL, Comment) VALUES ('" & txtName.Text & "','" & txtAddress.Text &
"','" & txtCity.Text & "','" & txtState.Text & "','" & txtZip.Text & "','" &
txtPhone.Text & "','" & txtEMail.Text & "','" & txtURL.Text & "','" &
txtComment.Text & "')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(txtName.Text) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)
```

```
      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"
```

```
      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub
</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
```

```
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Guestbook Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM
Guestbook</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td>Wecome <%= ip%> to SonicWALL's LHM Guestbook. In exchange for providing us
with your contact information,
      along with your permission to occassionally contact you while you are in the
middle of dinner, we will
      provide you with <b>one complimentary hour of secure internet access.</b><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3><font color="white"><center><b>Thank you for your
participation.</b></center></td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="0" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="30%"><asp:TextBox id="txtName" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="txtName" ErrorMessage="Please enter your name." runat="server"
/></td>
   </tr>
```

```
   <tr>
      <td width="30%"><br>Enter your address:</td>
      <td width="30%"><asp:TextBox id="txtAddress" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtAddress"
ControlToValidate="txtAddress" ErrorMessage="Please enter your address."
runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your city:</td>
      <td width="30%"><asp:TextBox id="txtCity" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtCity"
ControlToValidate="txtCity" ErrorMessage="Please enter your city." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your State:</td>
      <td width="30%"><asp:TextBox id="txtState" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtState"
ControlToValidate="txtState" ErrorMessage="Please enter your State." runat="server"
/></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your zip code:</td>
      <td width="30%"><asp:TextBox id="txtZip" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtZip"
ControlToValidate="txtZip" ErrorMessage="Please enter your zip code."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx1 runat="server" Display="Dynamic"
ControlToValidate="txtZip" ErrorMessage="Please enter in the format #####"
ValidationExpression="^\d{5}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your phone number:</td>
      <td width="30%"><asp:TextBox id="txtPhone" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valTxtPhone"
ControlToValidate="txtPhone" ErrorMessage="Please enter your phone number."
Display="Dynamic" runat="server" />
      <asp:RegularExpressionValidator id=regEx2 runat="server" Display="Dynamic"
ControlToValidate="txtPhone" ErrorMessage="Please enter in the format ###-###-####"
ValidationExpression="((\(\d{3}\)?)|(\d{3}-))?\d{3}-
\d{4}"></asp:RegularExpressionValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your  email address:</td>
      <td width="30%"><asp:TextBox id="txtEmail" runat="server" /></td>
      <td width="40%"><asp:RegularExpressionValidator id=regEx3 runat="server"
ControlToValidate="txtEmail" ValidationExpression=".*@.*\..*" ErrorMessage="Please
enter a valid email address." Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="valTxtEnail" runat="server"
ControlToValidate="txtEmail" ErrorMessage="Please enter you email address."
Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your web site URL (optional):</td>
      <td width="30%"><asp:TextBox id="txtURL" runat="server" /></td>
   </tr>
```

```
   <tr>
      <td valign="top" width="30%"><br>Enter a comment (optional):</td>
      <td width="30%"><asp:TextBox id="txtComment" width="300px" height="100px"
textmode="MultiLine" tabindex="4" runat="server" /></td>
   </tr>
   <tr>
      <td></td>
      <td><br><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear All "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the LHM Session Timeout
Dim sessTimer as String = "3600"

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

LHMQuiz 指令碼

驗證模型

來賓用戶端進行測驗。以及格分數當作驗證認證

目的

這是教室環境中通常會要求提供的網路存取方式。將課堂測驗的及格分數當作驗證方式，如此一來，講師就可確保學員有掌握及學習到課程教材，而不會被網路上各種無法抗拒的誘惑吸引過去。指令碼也會將及格的測驗以電子郵件方式寄給接受測試者，同時將不及格者郵寄給監考人/講師。

myvars 變數

`logoutPopup`	控制登出快顯視窗的使用。設定為： • **0** 停用快顯視窗。 • **1** 啟用快顯視窗。
`passingScore`	分數 (一個表示百分比例的整數) 必須通過測驗標準。
`quizFile`	測驗的 XML 來源檔名 (例如 `quiz.xml`、`shortquiz.xml`)。
`quizName`	測驗名稱，通用於指令碼。
`quizFrom`	以電子郵件傳送測驗時所使用的寄件者：電子郵件地址。
`quizTo`	不及格測驗要傳送至的收件者：電子郵件地址 (例如考試監考人或講師)。
`imagePath`	電子郵件包含正確和不正確答案的附件。這會設定那些影像檔的路徑。這通常設定為和指令碼檔案本身相同的路徑。
`smtpServer`	用於傳遞測驗結果的 SMTP 伺服器 IP 位址或可解析的 FQDN。若使用本機 IIS SMTP 伺服器執行個體，此可設定為 `127.0.0.1`。
`sessTimer`	工作階段計時器以秒計。
`idleTimer`	閒置計時器以秒計。
`strHmac`	可選 HMAC 功能的共用密碼。
`hmacType`	若 HMAC 在使用中時所使用的摘要類型：**MD5** 或 **SHA1**。
標誌	標誌 (影像) 檔案名稱使用於頁首。

工作階段流程

1 系統提示來賓用戶端輸入其完整名稱和電子郵件地址。需要正確/有效的電子郵件地址來傳遞及格的測驗。

2 輸入名稱和電子郵件後，會將來賓用戶端重新導向到 `quiz.aspx` 頁面。這是管理複選考試之處。

3 考試題目本身包含在 `quiz.xml` 檔案中，由 `quiz.xsd` (XML 結構定義) 檔案所定義。`quiz.xml` 檔案可以編輯且應該編輯，以自訂測驗，但是 `quiz.xsd` 文件則不應編輯，除非有絕對必要。

包含兩種測驗版本：`quiz.xml` (內含 10 道題目) 和 `shortquiz.xml` (內含 2 道指令碼運作的考試題目)。測驗題目數沒有限制，每道題目的答案數也沒有限制，其中每一道都需標示正確答案：使用 `correct=yes`。必須直截了當修改所提供 `quiz.xml` 檔案，如有必要。

4 測驗結束時，會顯示結果。如果是：
   - 不及格分數，會將考試結果以電子郵件傳送給講師 (電子郵件地址如 myvars 中所定義)，而系統會提示來賓用戶端再進行一次考試。未授權 LHM 工作階段。
   - 不及格分數，會將考試結果以電子郵件傳送給接受測試者，且會授權 LHM 工作階段。

   以電子郵件傳送的考試為 HTML 格式，其包含 checkmark.gif 和 block.gif (對與錯) 圖形檔附件，顯示在電子郵件中。
5 如果通過考試，LHM 發佈字串會與 sessionID、使用者名稱 (以 Web 表單形式提供)、預設的工作階段存留時間和閒置存留時間組合。
6 指令碼執行 LHM 發佈至 SonicWall 安全設備以授權該工作階段。

其他注意事項

需要存取 SMTP 伺服器才能傳遞考試結果。由於指令碼透過伺服器轉送郵件，需要設定 SMTP 伺服器以從 LHM 伺服器轉接。藉由設定 SMTP 伺服器做最佳整合，允許從 LHM 伺服器的 IP 位址轉接。

大部分 IIS 安裝包含本機 SMTP 伺服器，所以便於使用此本機 SMTP 伺服器進行郵件傳遞，方法是透過在 myvars 中設定 smtpServer 變數為 127.0.0.1。

即使是使用本機 SMTP 伺服器進行郵件傳遞，也需要轉接。在大部分的組態設定中，這可由以下執行：

1 移入 IIS MMC 配置器。
2 以右鍵按一下**預設 SMTP 虛擬伺服器**。
3 選擇**屬性**。
4 選擇**存取**標籤。
5 按一下**轉接**按鈕。
6 新增 127.0.0.1 至存取授與清單。

當使用非本機 SMTP 伺服器時，應設定 SMTP 伺服器以允許 LHM 伺服器依實際的 IP 位址轉接。

主題：

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>

<!-- #INCLUDE file="myvars.aspx" -->

<script runat="server">

'Sample LHM redirect querystring:
'http://10.50.165.231/xmlquiz/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig

Dim ip as String
Dim sessionId as String
```

```
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim emailAddr as String
Dim userName as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)
   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
```

```
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

'When the submit button is clicked, pass the variables we need and load the quiz
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   Context.Items.Add("req", req)
   Context.Items.Add("sessionId", sessionId)
   Context.Items.Add("emailAddr",clientEmail.Text)
   Context.Items.Add("userName",clientName.Text)
   Context.Items.Add("mgmtBaseUrl",mgmtBaseUrl)
   Server.Transfer("quiz.aspx",true)

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
```

```
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Quiz
Authorization</b></font></td>
      <td><center><img width="216" height="51" src="sonicwall.gif"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td width="30%"><br>Enter your full name:</td>
      <td width="20%"><asp:TextBox id="clientName" runat="server" /></td>
      <td ><asp:RequiredFieldValidator id="valTxtName"
ControlToValidate="clientName" ErrorMessage="Please enter your name."
Display="Dynamic" runat="server" /></td>
   </tr>
   <tr>
      <td width="30%"><br>Enter your real email address:</td>
      <td width="20%"><asp:TextBox id="clientEmail" runat="server" /></td>
      <td ><asp:RegularExpressionValidator id="fromEmail" runat="server"
ControlToValidate="clientEmail" ValidationExpression=".*@.*\..*"
ErrorMessage="Please enter a valid email address." Display="Dynamic" />
      </asp:RegularExpressionValidator>
      <asp:RequiredFieldValidator id="fromRequired" runat="server"
ControlToValidate="clientEmail" ErrorMessage="Please enter your email address."
Display="Dynamic" />
      </asp:RequiredFieldValidator>
      </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" /><br></td>
   </tr>

   <tr class="heading">
      <td colspan=3 align="left"><font color="white"><b>Welcome Quiztaker <%=
ip%></b></font></td>
   </tr>
</table>
<table width="70%" border="0" cellpadding="2" cellspacing="0">
   <tr>
```

```
      <td>
      <br>You have been redirected here by Lightweight Hotspot Messaging.
      This environment has been setup to demonstrate the flexibility of LHM,
including
      support for both wired and wireless clients, and also the ability for LHM to
use
      more than just username and password authentication for providing
access.<br><br>
      The page that you are about to continue on to is a <%= quizName %> written in
ASP.net.
      A passing score of <%= passingScore%>% will serve as the authentication for
LHM, and will grant
      you network access. You must pass the test to continue, and will be prompted to
retake
      the entire quiz if you you do not pass. <br><br>
      When you are done, the completed test will be emailed to you at the address you
      specify above.<br><br>
      So it's not just a good way to prove your understanding of some
      key SonicOS concepts, but also a practical example of the versatility of LHM.
      </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
```

```
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()
```

```
      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
```

```
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
     End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
```

```
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick
```

```
</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
```

```
     <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because although the login
event
'is non-exclusive, the login event produces data where redundancy is undesirable.
Dim logoutPopup as String = "0"

'Set the passing score
Dim passingScore as Integer = 80

'Set the filename of the quiz XML source
Dim quizFile as String = "quiz.xml"
'Dim quizFile as String = "shortquiz.xml"

'Set the name of the Quiz
Dim quizName as String = "SonicOS Quiz"

'Set the emailed quiz results "from" email address
Dim quizFrom as String = "joelevy@sonicwall.com"

'Set the email address to send failed test results to (the proctor/instructor)
Dim quizTo as String = "joelevy@sonicwall.com"

'Set the path for check and block embedded images - usually the same path as the quiz
Dim imagePath as String = "C:\inetpub\wwwroot\lhm\lhmquiz\"

'Set the IP or resolvable FQDN for the SMTP Server
'Make sure the server is configured to relay from the IP address of this server
'If setting to 127.0.0.1 (local IIS SMTP), you need to allow IIS SMTP to relay from
127.0.0.1
Dim smtpServer as String = "127.0.0.1"

'Set the LHM Session Timeout
Dim sessTimer as String = "86400"

'Set the LHM Idle Timeout
Dim idleTimer as String = "3600"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"
```

```
'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

quiz.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>
<%@ Import Namespace="System.Web" %>
<%@ Import Namespace="System.Web.Mail" %>

<!-- Original quiz code from www.codeproject.com -->

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Set the path to the XML quiz data
Dim strXmlFilePath as String = Server.MapPath(quizFile)

'Setup our variables
Dim emailAddr as String
Dim userName as String
Dim req as String
Dim sessionId as String
Dim mgmtBaseUrl as String
Dim xDoc as XmlDocument = New XmlDocument()
Dim intTotalQuestion as Integer
Dim intQuestionNo as Integer = 1
Dim intScore as Integer = 0
Dim arrAnswerHistory as new ArrayList()
Dim arrRightOrWrong as new ArrayList()
Dim arrCorrect as new ArrayList()

Sub Page_Load(src as Object, e as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
```

```
   'Grab context items set in default.aspx
   emailAddr = Context.Items("emailAddr")
   userName = Context.Items("userName")
   req = Context.Items("req")
   sessionId = Context.Items("sessionId")
   mgmtBaseUrl = Context.Items("mgmtBaseUrl")

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Load xml data
   xDoc.Load(strXmlFilePath)

   'Start a new quiz?
   If Not Page.IsPostBack Then

      'Yes. Count total question
      intTotalQuestion = xDoc.SelectNodes("/quiz/mchoice").Count

      'Record start time
      ViewState("StartTime") = DateTime.Now

      ShowQuestion(intQuestionNo)
   End If
End Sub

Sub btnSubmit_Click(src as Object, e as EventArgs)

   'Retrieve variables from ViewState
   intTotalQuestion = ViewState("TotalQuestion")
   intQuestionNo = ViewState("QuestionNo")
   intScore = ViewState("Score")
   arrAnswerHistory = ViewState("AnswerHistory")
   arrRightOrWrong = ViewState("RightOrWrong")
   arrCorrect = ViewState("AnswerList")
   req = ViewState("origReq")
   userName = ViewState("origUserName")
   emailAddr = ViewState("origEmailAddr")
   mgmtBaseUrl = ViewState("mgmtUrl")
   sessionId = ViewState("sessID")

   'Correct answer?
   If rblAnswer.SelectedItem.Value = ViewState("CorrectAnswer") Then
      intScore += 1
      arrRightOrWrong.Add(0)
   Else
      arrRightOrWrong.Add(rblAnswer.SelectedItem.Value)
   End If

   'Remember all selected answers
   arrAnswerHistory.Add(rblAnswer.SelectedItem.Value)
   arrCorrect.Add(ViewState("CorrectAnswer"))

   'End of quiz?
   If intQuestionNo=intTotalQuestion Then

      'Yes. Show the result.
      QuizScreen.Visible = False
      ResultScreen.Visible = True
```

```
      'Render result screen
      ShowResult()

   Else

      'Not yet. Show another question.
      QuizScreen.Visible = True
      ResultScreen.Visible = False
      intQuestionNo += 1

      'Render next question
      ShowQuestion(intQuestionNo)
   End If
End Sub

Sub ShowQuestion(intQuestionNo as Integer)
   Dim xNodeList as XmlNodeList
   Dim xNodeAttr as Object
   Dim strXPath as String
   Dim i as Integer
   Dim tsTimeSpent as TimeSpan

   strXPath = "/quiz/mchoice[" & intQuestionNo.ToString() & "]"

   'Extract question
   lblQuestion.Text = intQuestionNo.ToString() & ". " &
xDoc.SelectSingleNode(strXPath & "/question").InnerXml

   'Extract answers
   xNodeList = xDoc.SelectNodes(strXPath & "/answer")

   'Clear previous listitems
   rblAnswer.Items.Clear

   For i = 0 to xNodeList.Count-1

      'Add item to radiobuttonlist
      rblAnswer.Items.Add(new ListItem(xNodeList.Item(i).InnerText, i+1))

      'Extract correct answer
      xNodeAttr = xNodeList.Item(i).Attributes.ItemOf("correct")
      If not xNodeAttr is Nothing Then
         If xNodeAttr.Value = "yes" Then
            ViewState("CorrectAnswer") = i+1
         End If
      End If
   Next

   'Output Total Question and passing score
   lblTotalQuestion.Text = intTotalQuestion
   lblPassingScore.Text = passingScore

   'Output Time Spent
   tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))
   lblTimeSpent.Text = tsTimeSpent.Minutes.ToString() & ":" &
tsTimeSpent.Seconds.ToString()

   'Store data to viewstate
   ViewState("TotalQuestion") = intTotalQuestion
   ViewState("Score") = intScore
```

```
   ViewState("QuestionNo") = intQuestionNo
   ViewState("AnswerHistory") = arrAnswerHistory
   ViewState("RightOrWrong") = arrRightOrWrong
   ViewState("AnswerList") = arrCorrect
   ViewState("origReq")=req
   ViewState("origUserName")=userName
   ViewState("origEmailAddr")=emailAddr
   ViewState("mgmtUrl")=mgmtBaseUrl
   ViewState("sessID")=sessionID

End Sub

Sub ShowResult()
   Dim strResult as String
   Dim intCompetency as Integer
   Dim i as Integer
   Dim strXPath as String
   Dim tsTimeSpent as TimeSpan

   tsTimeSpent = DateTime.Now.Subtract(ViewState("StartTime"))

   strResult  = "<center>"

   if passingScore <= Int(intScore/intTotalQuestion*100).ToString()
      strResult += "<h2><font color=""green"">You Passed!</h3></font>"
   else
      strResult += "<h2><font color=""red"">You Failed!</h3><b>Please review the
answers and retake the test.</b><br></font>"
   End If

   strResult += "User Name: " & userName & "<br>"
   strResult += "Elapsed Time: " & tsTimeSpent.Minutes.ToString() & ":" &
tsTimeSpent.Seconds.ToString() & "<br>"
   strResult += "Correct Answers: " & intScore.ToString() & " out of " &
intTotalQuestion.ToString() & "<br>"
   strResult += "Your Percentage: " & Int(intScore/intTotalQuestion*100).ToString()
& "%<br>"
   strResult += "Required Percentage:" & passingScore.ToString() & "%<br>"
   strResult += "</center>"

   strResult += "<h3>Quiz Results</h3>"
   For i = 1 to intTotalQuestion
      strXPath = "/quiz/mchoice[" & i.ToString() & "]"
      strResult += "<b>" & i.ToString() & ". " & xDoc.SelectNodes(strXPath &
"/question").Item(0).InnerXml & "</b><br>"
      If arrRightOrWrong.Item(i-1)=0 Then
         strResult += "<img src = ""checkMark.gif""><font color=""green""> "
         strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
      Else
         strResult += "<img src = ""Block.gif""><font color=""red""> "
         strResult += "<b>You answered:</b> " & xDoc.SelectNodes(strXPath &
"/answer[" & arrAnswerHistory.Item(i-1).ToString() & "]").Item(0).InnerXml & "<br>"
         strResult += "The correct anwer is: " & xDoc.SelectNodes(strXPath &
"/answer[" & arrCorrect.Item(i-1).ToString() & "]").Item(0).InnerXml &
"</font><br><br>"
      End If
   Next

   'Setup the common Mail settings
```

```
   Dim objMail As MailMessage
   objMail = New MailMessage()
   objMail.From = quizFrom
   objMail.Body = strResult
   objMail.BodyFormat = MailFormat.Html

   'Path to the attachments for the Check and X images - update these in myvars.aspx
   objMail.Attachments.Add(New MailAttachment(imagePath & "block.gif"))
   objMail.Attachments.Add(New MailAttachment(imagePath & "checkMark.gif"))

   'Address of the SMTP server - can be localhost if SMTP is running on IIS - in
myvars.aspx
   SmtpMail.SmtpServer = smtpServer

   'Determine pass/fail
   If passingScore <= Int(intScore/intTotalQuestion*100).ToString()

      'Mail the passing test result to the test-taker
      'Be sure to update the mail fields in myvars.aspx
      objMail.To =emailAddr
      objMail.Subject = quizName & " Results for " & emailAddr

      'Send the mail
      SmtpMail.Send(objMail)
      strResult +="Your test is being emailed to you at " & emailAddr

      'Send the session Auth message to LHM
      postLHM()

   else
      'Mail failing test results to the instuctor
      objMail.To =quizTo
      objMail.Subject = "Failing " & quizName & " Test Results for " & emailAddr

      'Send the mail
      SmtpMail.Send(objMail)
      strResult += "<a href=""quiz.aspx"">Click here to retake the quiz</a>"
   End If

   'Write it
   lblResult.Text = strResult

End Sub

Sub postLHM()

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
```

```
      'Let the user know that we are setting up the session, just in case it takes
more than a second
      LHMResult.Text = "Authorizing session. Please wait."

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
```

```
        End If

        LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
        LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it
      'in the same color as the background, but still show the quiz results.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
    End Try
End Sub

</script>
```

```
<html>
<head>
<title><%= quizName %> </title>
</head>
<style>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</style>

<HTML>
<HEAD>
<TITLE>LHM Quiz Script</TITLE>
</HEAD>

<body>
<span id="QuizScreen" runat="server">
<form runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b><%= quizName %>  - <%=
userName%></b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>This quiz
has <asp:label id="lblTotalQuestion" runat="server" /> questions</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td colspan="2">
         <b><asp:label id="lblQuestion" runat="server" /></b><br>
         <asp:radiobuttonlist id="rblAnswer" RepeatDirection="vertical"
TextAlign="right" RepeatLayout="table" runat="server" /><br>
         <asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
         <asp:requiredfieldvalidator ControlToValidate="rblAnswer"
ErrorMessage="Please select an answer" runat="server" />
      </td>
   </tr>
   <tr class="heading">
      <td width="70%"><font color="white"><b>Score required to pass <asp:label
id="lblPassingScore" runat="server" />%</b></font></td>
```

```
     <td width="30%" align="right"><font color="white"><b>Time spent <asp:label
id="lblTimeSpent" runat="server" /></b></font></td>
   </tr>
</table>
</form>
</span>

<span id="ResultScreen" runat="server"> <asp:label id="lblResult" runat="server" />
<br>
<asp:Label id=LHMResult runat="server" />
<asp:Label id=catchError runat="server" />
</span>

</body>
</html>
```

PayPal 指令碼

驗證模型

來賓用戶端使用其 PayPal 帳戶，透過**立即購買**按鈕購買 1 小時或 24 小時存取權。透過 PayPal 付款至熱點提供者的 PayPal 商家帳戶。

目的

幾乎所有人都會使用 PayPal 在網際網路上進行購買或銷售。設定買家帳戶以及連結至任何付款形式 (例如信用卡、銀行卡、活期存款戶頭)，是非常容易的事。

將僅買家帳戶升級到商家帳戶，也一樣簡單。若擁有商家帳戶，PayPal 使用者可以接受從其他購買商品或服務的 PayPal 使用者的付款。經由 PayPal 執行金融轉帳，提供商家一個在線上銷售的方式，接受任何付款形式，完全不需要設定任何複雜的付款處理程序。如此也許可解決成為收費熱點提供者的單一最大障礙。

Paypal 提供**立即購買**按鈕功能，允許單擊交易。按鈕是在 PayPal 協助下產生的形式，包含要購買之項目或服務的相關資訊。當買家按一下**立即購買**按鈕後，工作階段會使用內含所有交易明細之 `querystring` 重新導向至 PayPal 網站 (例如賣家、品項、價格)。指令碼會使用自訂、伺服器端的「立即購買」常式，而不使用基本的**立即購買**按鈕 (其為用戶端，而不是伺服器端程式碼)。

另外，包含在「立即購買」重新導向中的是自動傳回路徑。自動傳回是 PayPal 的一項功能，它會在 PayPal 交易後，將買家傳回到商家的網站。當使用 PDT (`pdtPath` 時，需要自動傳回，如下所述)。

自訂「立即購買」重新導向，也會將 LHM `sessionID` 和 `mgmtBaseUrl` 內嵌到 PayPal「立即購買」重新導向中的自訂字串。這可讓我們追蹤工作階段，縱使它離開 LHM 伺服器，移至 PayPal，然後再返回 (經由 PDT 的自動傳回)。

基本的 PayPal 付款系統以電子郵件方式提供付款通知給商家。這方式對於實體商品買賣是可接受的，因為購買/出貨交易並不需要即時發生，商家可以等數小時或數天收到通知後再送出產品。對於要求瞬時交貨的交易，例如購買熱點存取，便需要更即時的付款方式。

PayPal 提供兩種付款通知方法：

- 即時付款通知 (IPN)，此運作方式是由 PayPal 對商家網站進行 Web 服務通話，表示某筆特定交易已經結清。遺憾的時，這項作業並非始終即時進行 (等待這個非同步通知需要 20 分鐘時間)，所以此指令碼並未採用。(可在 https://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/ipn-intro-outside 讀取更多 IPN 相關資訊)

- 付款資料傳送 (PDT：請參見 http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-intro-outside)。此方法使用 PayPal 的自動傳回方法，絕對即時發生。PDT 提供即時通知給交易狀態 (SUCCESS 或 FAIL) 以及 payment_status (已完成、待處理、已拒絕、失敗、已退款、已撤銷或 Cancelled_Reversal) 的商家。立即得知交易及付款狀態，便能立即提供服務，不會有收不到款項的風險。

myvars 變數

logoutPopup	控制登出快顯視窗的使用。設定為： • **0** 停用快顯視窗。 • **1** 啟用快顯視窗。
debugFlag	設定 PayPal PDT 轉帳的偵錯輸出： • **0** =關 • **1** = 開
pdtPath	由 PDT 自動傳回將來賓用戶端重新導向的路徑 (如上面的「目的」一節所述)。
paypalCGI	PayPal CGI 的 URL 充當 PayPal 交易的閘道。URL 本身不應變更，但有兩個選項： • 實況 (真實) PayPal 網站。 • Paypal 沙箱 (PayPal 開發人員網路的一部分)，其可用於測試。
myBusiness	熱點提供者的電子郵件地址 (PayPal 辨識企業的方式)。這必須符合要接收交易款項之商家帳戶的電子郵件。
Token	付款資料傳送選項會為每個商家產生一個獨特的 Token。這是您指定 PayPal 提供之獨特 Token 所在。Token 必須正確無誤，否則 PDT 交易 (非實際 PayPal 交易) 會失敗。
itemName1 itemName2	兩個存取選項的名稱，例如 1 小時安全網際網路存取和 24 小時安全網際網路存取。
itemNumber1 itemNumber2	兩個存取選項的項目編號 (大多是任意的內部 PayPal 參考) 例如 1hour 和 24hour。
itemTimer1 itemTimer2	兩個存取選項的工作階段計時器，以秒計，例如 **1** 小時為 3600，**24** 小時為 86400。
itemAmount1 itemAmount2	兩個存取選項的美元價格，例如 0.01 (一分) 和 0.02 (兩分)。限時促銷價。
itemButton1 itemButton2	兩個存取選項的按鈕文字，例如 1 小時存取 – $0.01 和 24 小時存取 – $0.02。
strHmac	可選 HMAC 功能的共用密碼。
hmacType	若 HMAC 在使用中時所使用的摘要類型：**MD5** 或 **SHA1**。
標誌	標誌 (影像) 檔案名稱使用於頁首。

工作階段流程

1 來賓用戶端啟動其網頁瀏覽器，由 LHM 重新導向至 `http://<lhmserver>/paypal/default.aspx`，其中 `<lhmserver>` 是您的 LHM 伺服器。

2 來賓用戶端 (買家) 按其中一個**立即購買**按鈕，例如 **1 小時存取 - $0.01**。

3 用戶端使用 querystring 重新導向至 PayPal 網站，其內含與商家、品項、LHM 工作階段 (在自訂變數中) 和自動傳回 URL (在 myvars 中定義為 pdtPath) 相關的所有資訊。

pdtPath 常駐於 LHM 伺服器上。該路徑應和 default.aspx 路徑 (如 SonicWall 安全設備上的設定) 相同，但應指向 pdt.aspx 檔案。這樣一來，當 PayPal 交易完成，且 PayPal 將用戶端重新導向回到商家網站時，用戶端會重新導向回到 `http://<lhmserver>/paypal/pdt.aspx` 網頁。

HTTP 可在 LHM 伺服器上使用，因為 LHM 伺服器本身並未輸入任何敏感資訊，而且來賓用戶端和 PayPal 之間可直接透過 HTTPS 進行 PayPal 交易。

範例立即購買重新導向字串：

```
https://www.sandbox.paypal.com/cgi-bin/webscr?cmd=_xclick&business=demo@sonicwall.com&item_name=1%20Hour%20Access&item_number=1hour&amount=0.01&currency_code=USD&lc=US&bn=PP-BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://lhmserverpaypal/default.aspx&return=http://lhmserver/lhm/paypal/pdt.aspx&custom=35378e67833faa3de83aa3b771https%3a%2f%2f172.16.17.1%3a4043%2f
```

4 來賓用戶端登入 PayPal (或依需求建立新帳戶)，並完成與 PayPal 的交易。交易完成後，用戶端重新導向回到 `http://<lhmserver>/paypal/pdt.aspx`。涵蓋在重新導向中是 querystring，其內含交易 ID (tx)、狀態 (st)、金額 (amt)、貨幣類型 (cc)、自訂值 (cm) 和加密的簽章 (sig)。

範例重新導向字串：

```
http://lhmserver/lhm/paypal/pdt.aspx?tx=4LN76482JF4605045&st=Completed&amt=0.01&cc=USD&cm=35378e67833faa3b771https%3a%2f%2f172%2e16%2e17%2e1%3a4043%2f&sig=qdsNC4flKwtPviggoGAXCpeV9gS%2f2E%2bGGVbTZ3STrUV1Ci9K3c2zTdJMuuKCmRiif1SybsZtUqDYqzzfMg64AF3PKCk85rrPubYT4K4aC
```

5 來賓用戶端在上述的 URL 存取 pdt.aspx 指令碼，會在 LHM 伺服器上啟動 PDT 處理序。指令碼建構一個 querystring 其依 cmd=_notify-synch 組成 (表示它是 PDT 交易) 連同 tx (交易 ID) 一起，而 at 變數設定為商家的 Token (定義在 myvars 中)。然會這會發佈至 paypalCGI URL (如 myvars 中所定義)。

6 PayPal 使用 FAIL 程式碼的 SUCCESS 回應 POST。

- FAIL - 指令碼向用戶端指出 PayPal 交易失敗，提示他們尋求協助。

•SUCCESS - 提供交易明細：

```
成功
txn_type=web_accept
payment_date=00%3A39%3A48+Oct+30%2C+2005+PDT
last_name=Niqual
item_name=1+Hour+Secure+Internet+Access
payment_gross=0.01
mc_currency=USD
business=lhmdemo%40sonicwall.com
payment_type=instant
payer_status=verified
tax=0.00
payer_email=lhmClient%40sonicwall.com
txn_id=84K306380G150640T
quantity=1
receiver_email=lhmdemo%40sonicwall.com
first_name=Sah
payer_id=XWRZGABD6UV2W
receiver_id=REW4W5WANU294
item_number=1hour
payment_status=Completed
payment_fee=0.01
mc_fee=0.01
shipping=0.00
mc_gross=0.01
custom=35378e67833faa3de833755d3aa3b771https%3
A//172.16.17.1%3A4043/
charset=windows-1252
```

7 指令碼檢查 payment_status 確認已完成付款。若未完成，未完成付款訊息會提供給使用者。

8 若已完成 payment_status，指令碼也會包含用戶端名稱、項目名稱、金額、交易 ID、商務和用於產生用戶端收據的自訂變數、LHM 工作階段的使用者名稱，以及識別 LHM sessionID 和 mgmtBaseUrl。

9 指令碼向來賓用戶端顯示 PayPal 交易收據。

10 指令碼執行 LHM 發佈至 SonicWall 安全設備以授權該工作階段。

其他注意事項

要求 PayPal 商家帳戶。

要求針對自動傳回和 PDT 設定 PayPal 帳戶 (請參見 http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside)

對於測試，強烈建議透過 PayPal 開發人員網路 (https://developer.paypal.com) 和 (https://www.sandbox.paypal.com) 設定 (免費) PayPal 沙箱帳戶

重要：因為來賓用戶端直接導引至 PayPal 網站，所有的 PayPal 網站 IP 位址必須在 SonicWall 安全設備上設定，做為來賓服務上允許的網路設定。這些包括下列各項：

www.paypal.com

```
64.4.241.32
64.4.241.33
216.113.188.32
216.113.188.35
216.113.188.66
216.113.188.67
```

www.paypalobjects.com

```
216.113.188.25
64.4.241.62
216.113.188.9
```

www.sandbox.paypal.com

```
66.135.197.160
```

developer.paypal.com

```
66.135.197.163
```

主題：

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Note: For PayPal authorization to work, it is necessary to set up the PayPal sites
(www.paypal.com, www.paypalobjects.com, and www.sandbox.paypal.com) as a bypass
network on WGS. This is so that WGS/LHM users can access PayPal directly to complete
the payment transactions. This list currently includes the following addresses:
[64.4.241.32, 64.4.241.33, 216.113.188.32, 216.113.188.35, 216.113.188.66,
216.113.188.67], [216.113.188.25, 64.4.241.62, 216.113.188.9] and [66.135.197.160].

'Sample LHM redirect querystring:
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig
```

```
Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Sub Page_Load(src as Object, e as EventArgs)

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Set the button Text for the two buttons with the variable configured in myvars
   btnBuyNow1.Text=itemButton1
   btnBuyNow2.Text=itemButton2

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
```

```
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

Sub btnBuyNow_Click(Sender As Object, E As EventArgs)

'sample redirect generated by this routine:
'https://www.paypal.com/cgi-
bin/webscr?cmd=_xclick&business=jlevy@sonicwall.com&item_name=24%20Hour%20Secure%20
Internet%20Access&item_number=24hour&amount=0.02&currency_code=USD&lc=US&bn=PP-
BuyNowBF&no_note=1&no_shipping=1&cancel_return=http://127.0.0.1/lhm/paypal/default.
aspx&return=http://www.moosifer.com/pdt.aspx

'sample redirect from the paypal server back the LHM server on transaction
completion (modified).
'http://127.0.0.1/lhm/paypal/pdt.aspx?tx=4PG453F7LS133715V&st=Completed&amt=0.02&cc
=USD&cm=&sig=EZhZtJygi7RTXulJt4SEhVBRi%2bJwLaC9z9kRLsrsXk4gQKnzvI5vjGy0vdhKPXAVyhbh
%2bwBxWon2cieEQDJ9P6R9qqjuKnzvI5vjGy0vdhKPXAVyJ3GtOq5Jd3%2fvTY3s7FrRcKdKnzvI5vjGy0v
dhKPXAVyyEKNxY3d

   Dim str, itemName, itemNumber, itemAmount As String
```

```
   Dim sb As New StringBuilder()

   'Determine which button was pressed, and set item attributes appropriately
   Select Case Sender.Text
      Case itemButton1
         itemName = itemName1
         itemNumber = itemNumber1
         itemAmount = itemAmount1
      Case itemButton2
         itemName = itemName2
         itemNumber = itemNumber2
         itemAmount = itemAmount2
   End Select

   'The paypal CGI URL - You can select either the real CGI or the sandbox CGI in
myvars
   sb.Append(paypalCGI & "?")
   'The cmd passed to PayPal - do not change!
   sb.Append("cmd=_xclick")
   'The email address of the paypal merchant receiving payment. Replace in myvars
with your paypal email address.
   sb.Append("&business=" & myBusiness)
   'The name of the item being purchased. This is the first item option (e.g. 1
hour). Set in myvars
   sb.Append("&item_name=" & itemName)
   'The optional item id
   sb.Append("&item_number=" & itemNumber)
   'The price being charged for the item (access)
   sb.Append("&amount=" & itemAmount)
   'The currency
   sb.Append("&currency_code=USD")
   'The country
   sb.Append("&lc=US")
   'The banana nullifier
   sb.Append("&bn=PP-BuyNowBF")
   'Disables the note option on the transaction
   sb.Append("&no_note=1")
   'Disables the shipping option on the transaction
   sb.Append("&no_shipping=1")
   'Build the path to return the client to (the LHM server address) on a cancelled
transaction
   sb.Append("&cancel_return=http://" & Request.ServerVariables("SERVER_NAME") &
Request.ServerVariables("URL"))
   'The return (success page) path to return the buyer to after the transaction. This
is the PDT receiver/processor page.
   sb.Append("&return=" & pdtPath)
   'The LHM sessionID - append this so that it can be returned to us later by the PDT
transaction - do not change!
   sb.Append("&custom=" & sessionId & Server.URLEncode(mgmtBaseUrl))
   'Optional notify_url that paypal will asynchronously send IPN confirmation to. Not
used since it's not real-time.
   'sb.Append("&notify_url=http://www.moosifer.com/ipn.aspx")
   str = sb.ToString
   Response.Redirect(str)

End Sub

</script>

<STYLE>
body {
```

```
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
      <td colspan=3><br></td>
   </tr>
   <tr>
      <td colspan=3 align="left">Purchase Secure Internet Access through SonicWALL's
LHM and PayPal's Buy Now feature.
      <br><br>The two Buy Now buttons below will send you to PayPal's website where
you can use your PayPal account to pay <b>$<%= itemAmount1 %> for <%= itemName1
%></b>, or <b>$<%= itemAmount2 %> for <%= itemName2 %></b>.
      <br><br>
      PayPal will then redirect you to this site to initiate the  Payment Data
Transfer (PDT) exchange. The PDT exchange begins with the LHM server posting a
paypal constructed querystring back to paypal. The response to the post will then be
parsed by the LHM server to determine if the PayPal transaction was successful.  Once
all data are exchanged and verified, LHM will authorize access on the SonicWALL for
the period of time purchased.
      <br><br>
      The clock for access will start immediately upon successful session
authorization, and can be used on the local SonicWALL appliance by the client (as
```

```
tracked by IP and MAC address) so long as session time remains. The idle timeout will
effectively be disabled by setting the idle timer to the same value as the session
timer.
      <br><br>
      Please select "<%= itemName1 %>" or "<%= itemName2 %>" below. You will be
redirected to the PayPal site, and will be returned to this site on transaction
completion.

      <br><br>
      </td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td align="center"><asp:Button ID="btnBuyNow1" Class="button"
OnClick="btnBuyNow_Click" runat="server" />
        <asp:Button ID="btnBuyNow2" Class="button" OnClick="btnBuyNow_Click"
runat="server" /></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr>
      <td colspan=3><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=3><asp:Label id=catchError runat="server"/></td>
   </tr>
</table>

</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
```

```
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")


   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"
```

```
      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()
```

```
     'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
     Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
     End Try
End Sub

</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
```

```
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}
```

```
document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
```

```
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
Dim logoutPopup as String = "0"

'Set the debug flag (0 = off, 1 = on)
Dim debugFlag as String = "0"

'Set the path and file for the PDT responder script - this should be the same path as
the LHM settings
'configured on the SonicWALL "External Web Server Settings" page, but pointing to
the PDT handler script.
'Refer to http://www.paypal.com/cgi-bin/webscr?cmd=p/xcl/rec/pdt-techview-outside
for information on PDT
Dim pdtPath as String = "http://10.50.165.2/lhm/paypal/pdt.aspx"

'Set the path the PayPal processing CGI. Use the sandbox
(https://developer.paypal.com) and (https://www.sandbox.paypal.com) for testing
'Using the sandbox requires a developer network account and login.
Dim paypalCGI as String = "https://www.sandbox.paypal.com/cgi-bin/webscr"
'Dim paypalCGI as String = "https://www.paypal.com/cgi-bin/webscr"

'Set the email addres of the paypal merchant account to which payment will be made
'The following is a valid sandbox account, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox account) for use.
Dim myBusiness as String = "lhmdemo@sonicwall.com"

'Set this to token from PayPal account. It must be your actual, valid token.
'Refer to http://paypaltech.com/PDTGen/PDTtokenhelp.htm for information on the
identity token
'The following is a valid sandbox token, but requires authentication by the parent
(real) account.
'You must replace this with you own (real or sandbox token) for use.
Dim token as String = "ucistq6vmKGWPxwJbrTJFDhFq889RxYt_6Mkz_3viraSzjiQJ5iPYCZ5Mdq"

'Set the names for the purchase item options (e.g. 1 hour Access, 3 hours access,
etc.)
Dim itemName1 as String = "1 Hour Secure Internet Access"
Dim itemName2 as String = "24 Hours Secure Internet Access"

'Set the paypal querystring number for purchase item options  (e.g. 1hour, 60mins,
itemone, etc.)
```

```
Dim itemNumber1 as String = "1hour"
Dim itemNumber2 as String = "24hour"

'Set the purchase item options session and idle timers (timers use  thesame value
since we do not want sessions idling out)
Dim itemTimer1 as String = "3600"'One hour, in minutes
Dim itemTimer2 as String = "86400"'24 hours

'Set the costs in dollars for purchase item options (e.g. one penny = 0.01, one
dollar = 1.00, etc.)
Dim itemAmount1 as String = "0.01"
Dim itemAmount2 as String = "0.02"

'Set the button names and descriptions for purchase item options
Dim itemButton1 as String = "1 Hour Access - $0.01"
Dim itemButton2 as String = "24 Hours Access - $0.02"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"
'------------------------End of Configurable Settings-------------------------

</script>
```

pdt.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
```

```
'http://127.0.0.1/lhm/paypal/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim sessTimer as String
Dim idleTimer as String
Dim userName as String
Dim hmac as String
Dim firstname, lastName, itemName, mcGross, mcCurrency, itemNumber, business, txn,
payStatus As String

Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles
MyBase.Load

   'Use the override class to accept untrusted certificates from the SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   Dim tx, PDTvalidateQuery As String
   Dim strResponse As HttpWebResponse
   Dim temp As String
   Dim PDTArray() As String
   Dim iParts, sResults(0, 0), aParts(), sParts(), sKey, sValue, snwlCustom As String
   Dim i As Integer

   'Set tx to value of tx passed in via Querystring from PayPal
   tx = Request.QueryString("tx")

   'Set string = to the cmd value, tx and at that needs to be
   'POSTed back to PayPal to validate the PDT
   PDTvalidateQuery = "cmd=_notify-synch&tx=" & tx & "&at=" & token

   'Now we need to POST this info back to PayPal for validation of the PDT
   'Create the request back
   Dim req As HttpWebRequest = CType(WebRequest.Create(paypalCGI), HttpWebRequest)

   'Set values for the request back
   'set method
    req.Method = "POST"
    'set content type
    req.ContentType = "application/x-www-form-urlencoded"
    'set length
    req.ContentLength = PDTvalidateQuery.Length

   'Write the request back to PayPal
   Dim stOut As StreamWriter = New StreamWriter(req.GetRequestStream(),
Encoding.ASCII)
   stOut.Write(PDTvalidateQuery)
   stOut.Close()

   Try
      strResponse = CType(req.GetResponse(), HttpWebResponse)
   Catch ex As SystemException
```

```
   catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
End Try

      'Once we write the stream back to PayPal, we need to read the response.

      Dim IPNResponseStream As Stream = strResponse.GetResponseStream
      Dim encode As Encoding = System.Text.Encoding.GetEncoding("utf-8")
      Dim readStream As New StreamReader(IPNResponseStream, encode)

      'Read the response in String variable "temp"
      temp = readStream.ReadToEnd

   'Debug flag, set in myvars - prints the whole output from the POST reply
   If debugFlag = "1" Then
      OutputEntirePDTString(temp)
   End If

      'Check to see if the 1st line of the response was "SUCCESS"
      If Mid(temp, 1, 7) = "SUCCESS" Then

          'if it is SUCCESS, the code below puts the response in a nice array
          temp = Mid(temp, 9)
          sParts = Split(temp, vbLf)
          iParts = UBound(sParts) - 1
          ReDim sResults(iParts, 1)

          For i = 0 To iParts

              aParts = Split(sParts(i), "=")
              sKey = aParts(0)
              sValue = aParts(1)
              sResults(i, 0) = sKey
              sResults(i, 1) = sValue

              'You can add more case statements here for other returned variables

        Try
              Select Case sKey
                  Case "first_name"
                      firstname = Server.URLDecode(sValue)
                  Case "last_name"
                      lastName = Server.URLDecode(sValue)
                  Case "item_name"
                      itemName = Server.URLDecode(sValue)
                  Case "mc_gross"
                      mcGross = sValue
                  Case "mc_currency"
                      mcCurrency = sValue
          Case "item_number"
             itemNumber = Server.URLDecode(sValue)
          Case "business"
             business = Server.URLDecode(sValue)
          Case "txn_id"
             txn = sValue
          Case "payment_status"
             payStatus = sValue
                 Case "custom"
             snwlCustom = sValue
             sessionID = snwlCustom.SubString(0,32)
             mgmtBaseUrl=(Server.URLDecode(Mid(snwlCustom,33)))
             End Select
```

```
        Catch ex as Exception
           catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        End Try

            Next

        If payStatus = "Completed" Then
           'Transaction Succeeded - Give the Guest a receipt
           Dim receipt as String

           receipt =  "<h3>Transaction Succeeded. Thank you for selecting SonicWALL
LHM.</h3><br>"
           receipt + = "<b>Transaction Invoice:</b><br><br>"
           receipt + = "Name: " & firstname & " " & lastName & "<br>"
           receipt + = "Description: " & itemName & "<br>"
           receipt + = "Amount: " & mcCurrency & " " & mcGross &"<br>"
           receipt + = "Paid to: " & business &"<br>"
           receipt + = "Transaction ID: " & txn &"<br>"
           receipt + = "<br><br>"

           paypalResult.Text = receipt

           LHMResult.Text = "Authorizing your LHM session."

           'Setup the LHM session variables and call LHM Routine
           'Set the session and idle timers to match the variables set in myvars
           If itemNumber = itemNumber1 Then
              sessTimer=itemTimer1
              idleTimer=itemTimer1
           Else
              sessTimer=itemTimer2
              idleTimer=itemTimer2
           End If

           userName = firstname & " " & lastName

           LHM()
        Else
           'The transaction itself was a success, but the payment status was not
Completed.
           paypalResult.Text = "The transaction succeeded, but the payment was not
completed. The session cannot be authorized at this time."
        End If

        Else
            ' If PDT response is not "SUCCESS"
           paypalResult.Text = "The PayPal transaction did not succeed. The returned
status is: <b>" &  temp & "</b>"
        End If

        'Close the streams
        readStream.Close()
        strResponse.Close()

    End Sub

   'This is the parser for the debug function to print the entire resonse to the PDT
POST
    Private Function OutputEntirePDTString(ByVal myPDTString As String) As String
        Dim tempString() As String = Split(myPDTString, vbLf)
        Dim x As Integer
```

```
        For x = 0 To tempString.GetUpperBound(0)
            Response.Write(tempString(x) & "<br>")
        Next
    End Function

Sub LHM()

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" &
Server.URLEncode(userName) & "&sessionLifetime=" & sessTimer & "&idleTimeout=" &
idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"
```

```
      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
         If logoutPopup = "1" Then
            'Popup hack using Javascript for logout window
            Dim sb As New System.Text.StringBuilder()
            sb.Append("<script language='javascript'>")
            sb.Append("window.open('logout.aspx?sessId=")
            sb.Append(Server.URLEncode(CStr(sessionId)))
            sb.Append("&mgmtBaseUrl=")
            sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
            sb.Append("&sessTimer=")
            sb.Append(Server.URLEncode(CStr(sessTimer)))
            sb.Append("','logOut','toolbar=no,")
            sb.Append("addressbar=no,menubar=no,")
            sb.Append("width=400,height=250');")
            sb.Append("<")
            sb.Append("/")
            sb.Append("script>")
            RegisterStartupScript("stp", sb.ToString)
         End If

         LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now begin your secure Internet access session."

      'Response code 51 - Session Limit Exceeded
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
         LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 100 - Login Failed.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
```

```
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM PayPal Script</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Access with PayPal
Buy Now</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo%>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
   </tr>
   <tr class="heading">
```

```
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">

   <tr>
   <td><br></td>
   </tr>
   <tr>
      <td><asp:Label id=paypalResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</BODY>
</HTML>
```

隨機指令碼

驗證模型

來賓用戶端輸入演算法驗證、隨機產生的密碼。

目的

傳統密碼驗證要求先產生密碼再使用，並且儲存在驗證平台上。例如，無線來賓服務要求在使用帳戶之特別 SonicWall 安全設備上產生帳戶。隨機指令碼透過使用加 Salt 的演算法來產生和驗證密碼的方法，消除此相依性。這表示密碼絕不需要儲存在任何地方，只要 salt 相同，密碼就完全是移轉的 (也就是說可以在任何網站上使用，即使 LHM 伺服器不同)。

實際含義是，來賓帳戶密碼可以大量產生、散發，而且未來任何時候都可以使用。舉例來說，密碼可以產生 (使用特殊的 salt)、列印 (例如在憑證、名片、刮刮卡上)、散發，並可在任何使用採用相同演算 salt 的 LHM 伺服器的網站上使用。密碼可被指定一個絕對 (非相對) 到期日，到時候可變更 salt 將到期的密碼作廢。

同樣的，可使用一般的 salt 來驗證一組跨多網站使用的密碼 l，而獨特的 salt 則確保在某一個網站產生的密碼，不可在另一個具不同 salt 的網站上使用。因此，雖然使用一般演算法來產生和驗證所有的密碼，將 salt 附加到雜湊函數能提供所需的唯一性。

`default.aspx` 指令碼是 `generator.aspx` 指令碼之外，也是產生密碼之處。從 1 到 999 密碼的任何密碼，只能一次產生一個。產生之後，可列印個別密碼，或可將整份清單匯出成 `.csv` 檔。

支援範圍涵蓋兩種類別的密碼：1 小時和 24 小時。任何一種類型的密碼可由產生器指令碼產生。

產生演算法運作方式：

1 產生隨機碼 (根密碼) 的 `randChars` (預設整數值六) 字元，如 `myvars` 中的定義。隨機碼產生器的字元集可在 `default.aspx` 檔案內修改。
2 salt (在 `myvars` 中定義為 salt 字串) 放在根密碼的前面。

3 接著在所產生的字串上計算 SHA1 雜湊。然後從雜湊獲得三組字元配對；對於：
   - 1 小時密碼，獲得 408 組 (字元 4,5 + 0,1 + 8,9)。
   - 24 小時密碼，獲得 752 組 (字元 7,8 + 5,6 + 2,3)。
4 從雜湊選擇的六個字元接著會串連至根密碼。
5 結果產生可分配的密碼。

驗證演算法反向運作：

1 來賓用戶端輸入其密碼 (呼叫此 `enteredCode`)。
2 指令碼擷取輸入之代碼的前 `randChars` 個字元 (呼叫此根密碼)。
3 salt 放在根密碼的前面，並且計算 SHA1 雜湊。獲得 408 組字元，並附加到根密碼。408 組接著會與 `enteredCode` 比對：
   - 如果 408 組相符，便驗證為 1 小時密碼。
   - 408 組不相符，便會試用 752 組。若此與 `enteredCode` 相符，便會驗證為 24 小時密碼。
   - 若都不相符，則代碼無效。

   在驗證 `enteredCode` 之後，會查詢 `usedcodes.mdb` 資料庫以查看是使已使用代碼。如果未在資料庫中找到 `enteredCode`，LHM 工作階段授權順序才能開始，方法是將 MAC 位址當成使用者名稱使用。授權 LHM 工作階段，且 LHM 伺服器已收到通知後，`enteredCode` 的根密碼會寫入到 `usedcodes.mdb` 資料庫，如此就不會重複使用。當 (如果) salt 改變了，最好還是排清資料庫。

myvars 變數

`logoutPopup`	控制登出快顯視窗的使用。設定為： • **0** 停用快顯視窗。 • **1** 啟用快顯視窗。
`useDB`	控制已用過的密碼資料庫的使用。如果 `useDB` 是： • **0**，那麼資料庫不供讀取或寫入，允許重複使用密碼。 • **1**，那麼使用過的密碼會寫入到資料庫中，而新的驗證處理序會檢查資料庫，以判斷是否已使用過密碼。
`randChars`	要包含在根密碼中的隨機字元數。預設值為六。此會產生 12 字元密碼，因為雜湊元件始終增加額外六個字元。
`salt`	運算雜湊時所使用的 salt。務必使用好的 salt 以防止不必要的密碼移轉/衝突。
`sessTimer`	工作階段計時器以秒計。
`idleTimer`	閒置計時器以秒計。
`strHmac`	可選 HMAC 功能的共用密碼。
`hmacType`	若 HMAC 在使用中時所使用的摘要類型：**MD5** 或 **SHA1**。
標誌	標誌 (影像) 檔案名稱使用於頁首。

工作階段流程	1 來賓用戶端輸入其密碼。 2 密碼是使用演算法驗證技術進行馬驗證，如上面的**目的**一節中所述。 3 若已驗證代碼，會針對上一次在 `usedcodes.mdb` 資料庫中的使用做檢查。 4 如果未顯示，則會起始 LHM 工作階段 (1 小時或 24 小時)，並使用 MAC 位址當作使用者名稱。 5 起始 LHM 工作階段之後，指令碼會將根密碼寫入 `usedcodes.mdb` 資料庫，如此就無法重複使用。 6 指令碼執行 LHM 發佈至 SonicWall 安全設備以授權該工作階段。
其他注意事項	由於正將指令碼寫入資料庫，所以有必要為 **IUSR_MACHINENAME** 和 **IWAM_MACHINENAME** (或 **ASPNET**) 帳戶設定寫入權限，如第 642 頁「我想要使用 SonicWall 所提供的樣本指令碼。我需要做些什麼才能使用它們嗎？」中所述 `generator.aspx` 指令碼應位於 Web 伺服器的安全 (無法公開存取) 區域。

主題：

- 第 738 頁「default.aspx」
- 第 746 頁「generator.aspx」
- 第 751 頁「logout.aspx」
- 第 757 頁「myvars.aspx」
- 第 757 頁「print.aspx」

default.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

'Sample LHM redirect querystring:
```

```
'http://127.0.0.1/lhm/random/default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004
f&ip=10.50.165.231&mac=00:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.5
0.165.193:4043/&clientRedirectUrl=https://10.50.165.193:444/&req=http%3A//www.googl
e.com/ig

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String

Dim passCode as String
Dim grabCode as String

Sub Page_Load(Source as Object, E as EventArgs)

   LHMResult.Text=""
   catchError.Text=""
   authResult.Text=""

   ip=Request.QueryString("ip")
   sessionId=Request.QueryString("sessionId")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'customCode grabs the "cc=" querystring value sent by the SonicWALL. This allows
you to use the same
   'page (e.g. this page) for the "Session Expiration" (?cc=2), "Idle Timeout"
(?cc=3) and "Max Sessions" (?cc=4) page.
   If customCode <> "" Then
      Select Case customCode
      Case "2"
         LHMResult.Text="<br><H3><font color=""red"">Your LHM session has expired.
You may try to initiate a new session.</font></H3>"
      Case "3"
         LHMResult.Text="<br><H3><font color=""red"">You have exceeded your idle
timeout. Please log back in.</font></H3>"
      Case "4"
         LHMResult.Text="<br><H3><font color=""red"">The maximum number of sessions
has been reached. Please try again later.</font></H3>"
      End Select
   End If

   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'Note - the routine below for handling the hmac requires the use of the
SonicSSL.dll and libeay.dll libraries.
   'The DLL must be copied to the IIS server, and the SonicSSL dll must be registered
with "regsvr32 sonicssl.dll"
```

```
   If hmac <> "" Then

      'SonicWALL URL Encode routine is different from Microsoft - this is the
SonicWALL method
      req=Replace(req,"%","%25")
      req=Replace(req,":","%3A")
      req=Replace(req," ","%20")
      req=Replace(req,"?","%3F")
      req=Replace(req,"+","%2B")
      req=Replace(req,"&","%26")
      req=Replace(req,"=","%3D")

      Dim strHmacText as String
      Dim objCrypto as Object
      Dim strHmacGenerated
      Dim loginError as String

      'Initialize the Crypto object
      objCrypto = Server.CreateObject("SonicSSL.Crypto")

      'The text to be encoded
      strHmacText = sessionId & ip & mac & ufi & mgmtBaseUrl & clientRedirectUrl &
req

      'Calculate the hash with a key strHmac, the return value is a string converted
form the output sha1 binary.
      'The hash algorithm (MD5 or SHA1) is configured in myvars and in the Extern
Guest Auth config on the SonicWALL
      If hmacType = "MD5" Then
         strHmacGenerated = objCrypto.hmac_md5(strHmacText, strHmac)
      Else
         strHmacGenerated = objCrypto.hmac_sha1(strHmacText, strHmac)
      End If

      If strHmacGenerated <> hmac Then
         Dim hmacFail as String
         hmacFail = "<font color=""red"">The HMAC failed validation. Please notify an
attendant.</font><br><br>"
         hmacFail+="<font color=""9CBACE"">Received HMAC: " & hmac & "<br>Calculated
HMAC: " & strHmacGenerated & "<br>"
         hmacFail+="Make sure the digest functions on the SonicWALL and LHM server
match.<br>"
         hmacFail+="Also make sure the shared secret on the SonicWALL and myvars
match</font>"
         catchError.Text=hmacFail
      End If

   End If

End Sub

sub OnBtnClearClicked (Sender As Object, e As EventArgs)
   enteredCode.Text = ""
   LHMResult.Text=""
   catchError.Text=""
end sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'The following subroutine validates client provided passcodes.
   'The first 6 characters (definable in myars) are grabbed.
```

```
   'These characters are then run though a SHA1 hash with a salt that is defined in
myvars.

   '3 pairs of substrings are then retrieved from the hash.
   'The code is validated if the 3 pairs concatenated to the randChars (defined in
myvars) characters consist of the following:

   'Validating the 4 0 8 pairs (4,5+0,1+8,9 characters) will provide 1 hour of guest
access.
   'Validating the 7 5 2 pairs (7,8+5,6+2,3 characters) will provide 24 hours of
guest access.

   grabCode = enteredCode.Text.SubString(0,randChars)

   'Manually compute SHA1 on salt+randomCode, and convert result to base64 - gives
stranger output
   Dim sha1 As sha1 = sha1.Create()
   Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
grabCode))
   Dim hashResult as String = Convert.ToBase64String(manualHash)

   'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
   'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

   'First try to match on 1 hour code
   passCode  = ""
   passCode = grabCode & hashResult.SubString(4, 2)
   passCode = passCode & hashResult.SubString(0, 2)
   passCode = passCode & hashResult.SubString(8, 2)
   If enteredCode.Text = passCode Then
      sessTimer = "3600"
      authResult.Text="<font color=""green""><b>1 hour code validated.</b></font>"

      'Check the used passcode DB if useDB is enabled in myvars.
      If useDB = "1" Then
         wasItUsed()
      End If
   Else
      'Now try to match on 24 hour code
      passCode = ""
      passCode = grabCode & hashResult.SubString(7, 2)
      passCode = passCode & hashResult.SubString(5, 2)
      passCode = passCode & hashResult.SubString(2, 2)
      If enteredCode.Text = passCode Then
         sessTimer = "86400"
         authResult.Text="<font color=""green""><b>24 hour code
validated.</b></font>"

         'Check the used passcode DB if useDB is enabled in myvars.
         If useDB = "1" Then
            wasItUsed()
         End If

      Else
         authResult.Text="<font color=""Red""><b>Passcode cannot be
validated.</b><br>The passcode is case-sensitive.<br>Please try again.</font>"
      End if
   End If
```

```
End Sub

Sub wasItUsed ()

   'Check to see if the root (randChars) of the passcode is already in the used
database.
   Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"
   Dim MySQL as string = "SELECT * From passCodes Where passCode = '" & grabCode &
"'"
   Dim MyConn as New OleDBConnection (strConn)
   Dim cmd as New OleDBCommand (MySQL, MyConn)
   Dim objDR As OleDbDataReader
   Dim isUsed As Boolean

   MyConn.Open()
   objDR = cmd.ExecuteReader()
   isUsed = objDR.Read()
   objDR.Close()
   MyConn.Close()

   'If the passcode is not found in the database
   if isUsed = False
      LHM()
   Else
      authResult.Text="<font color=""Red""><b>Passcode has already been
used.</b><br>Please see an attendant for assistance.</font>"
   End If

End Sub

Sub writeToDB ()

   'Try to write the submitted (only randChars characters instead of the whole
passcode) info to the database file
   Try
      Dim strConn as string = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=" &
server.mappath("usedcodes.mdb") & ";"

      Dim MySQL as string = "INSERT INTO passCodes (passCode) VALUES ('" & grabCode &
"')"
      Dim MyConn as New OleDBConnection (strConn)
      Dim cmd as New OleDBCommand (MySQL, MyConn)
      MyConn.Open ()
      cmd.ExecuteNonQuery ()
      MyConn.Close ()

      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
   End Try

End Sub

Sub LHM()

   'The writeToDB sub is in the Response code 50 - Login Succeeded routine, after the
LHM exchange succeeds. You may move it to the top to write the passcode to the DB
before the LHM transaction for testing purposes.
   'writeToDB ()

   enteredCode.Text = "Code Accepted."
```

```
   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogin.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & "&userName=" & mac &
"&sessionLifetime=" & sessTimer & "&idleTimeout=" & idleTimer

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/AuthenticationReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 50 - Login Succeeded

      If snwlResponse.SelectSingleNode(codePath).InnerXml = "50"

         'Do we want to provide a logout popup window?
```

```
        If logoutPopup = "1" Then
           'Popup hack using Javascript for logout window
           Dim sb As New System.Text.StringBuilder()
           sb.Append("<script language='javascript'>")
           sb.Append("window.open('logout.aspx?sessId=")
           sb.Append(Server.URLEncode(CStr(sessionId)))
           sb.Append("&mgmtBaseUrl=")
           sb.Append(Server.URLEncode(CStr(mgmtBaseUrl)))
           sb.Append("&sessTimer=")
           sb.Append(Server.URLEncode(CStr(sessTimer)))
           sb.Append("','logOut','toolbar=no,")
           sb.Append("addressbar=no,menubar=no,")
           sb.Append("width=400,height=250');")
           sb.Append("<")
           sb.Append("/")
           sb.Append("script>")
           RegisterStartupScript("stp", sb.ToString)
        End If

        LHMResult.Text = "<br><b><font color=""green"">Session
authorized:</font></b> You may now go to the URL you originally requested: <a
target=""_blank"" href=""" & req & """>" & req & "</a>"

        'Write the passcode the DB if the LHM session succeeds and if useDB = 1.
        If useDB = "1" Then
           writeToDB ()
        End If

     'Response code 51 - Session Limit Exceeded
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "51"
        LHMResult.Text = "<br><b><font color=""red"">Session Limit
Reached:</font></b> The maximum number of guest session has been reached. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

     'Response code 100 - Login Failed.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "100"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> Your session cannot be created at this time. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

     'Response code 251 - Bad HMAC.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed message authentication.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     'Response code 253 - Invalid SessionID.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed to match a known session
identity. Sorry for the inconvenience. Please close and relaunch your browser to try
again."

     'Response code 254 - Invalid CGI.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization was missing an essential parameter.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

     'Response code 255 - Internal Error.
     ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
```

```
        LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
         catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
         LHMResult.Text = "<br><b><font color=""red"">Session creation
failed:</font></b> The request for authorization failed due to an unspecified error.
Sorry for the inconvenience. Please close and relaunch your browser to try again. If
the problem persists, please notify an attendant."
      End Try
End Sub


</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" onKeyPress="if(event.keyCode==13)
{document.getElementById('btnSubmit').click(); return false}" runat="server">

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Powered
by SonicWALL LHM</b> </font></td>
```

```
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Wecome <%= ip%> to SonicWALL's LHM Algorithmic
Authenticator.</b><br><br>Enter your unique randomly generated passcode to obtain
secure guest internet access.<br><br>Valid passcodes are not stored anywhere, so
validation is not performed against any kind of database. Instead, when a passcode
is entered, it is algorithmically validated. Once a passcode is successfully used,
it is written to a "used passcode" database so that it cannot be reused.<br><br>The
validator will recognize 1 hour and 24 hour passcodes - these characteristics were
encoded within the passcodes themselves during generation.<br><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><br>
      <td width="30%">Enter your passcode:</td>
      <td width="30%"><asp:TextBox id="enteredCode" runat="server" /></td>
      <td width="40%"><asp:RequiredFieldValidator id="valEnteredCode"
ControlToValidate="enteredCode" ErrorMessage="Please enter your passcode."
runat="server" /></td>
   </tr>
   <tr>
      <td></td><td colspan=2><asp:Label id=authResult runat="server" /> </td>
   </tr>
   <tr>
      <td></td>
      <td><asp:button id="btnSubmit" class="button" text="  Submit  "
onClick="btnSubmit_Click" runat="server" />
        
      <asp:button id="btnClear" class="button" text=" Clear "
CausesValidation="False" onClick="OnBtnClearClicked" runat="server" />
      </td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td colspan=2><asp:Label id=catchError runat="server" /></td>
   </tr>
</table>
</form>
</BODY>
</HTML>
```

generator.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
```

```
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Data" %>
<%@ Import Namespace="System.Data.OleDB" %>
<%@ Import Namespace="System.Security" %>
<%@ Import Namespace="System.Security.Cryptography" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

Dim genCodes As New ArrayList()
Dim codeType As String

Sub Page_Load(Source as Object, E as EventArgs)
   If Not isPostBack Then
      Heading.Text=" "
      btnExport.Visible = False
   End If
End Sub

Sub btnSubmit_Click(Sender As Object, E As EventArgs)
   'The following generates passcodes beginning with a random character generator.
   'The number of characters in randomCode is configurable in myvars.
   'The randomCode output is then run though a SHA1 hash with a salt that is defined
in myvars.
   'Note: If you are using this in a live environment, it is important to change the
salt to prevent algorithm compromise.

   '3 pairs of substrings are then retrieved from the hash, and concatenated to the
randomCode to form the passcode.

   'In the current sample implementation:
   'The 4 0 8 pairs (4,5+0,1+8,9 characters) from the hash will provide 1 hour of
guest access.
   'The 7 5 2 pairs (7,8+5,6+2,3 characters) from the hash will provide 24 hours of
guest access.

   Dim myLooper As Integer
   Dim passCode as String

      For myLooper = 1 to Convert.ToInt32(codeCount.Text)

         Dim x As Integer = 0
         Dim isitRand as boolean = False
         Dim intRand as Integer = 0
         Dim randomCode as String = ""

         For x = 1 to randChars
            Do Until isItRand = True
               '48 to 57 for numbers, 65 to 90 for uppercase, 97 to 122 for lowercase
               intRand = Int((122 - 48 + 1) * Rnd + 48)
               'Select the legal characterset for randomCode by including legal
characters below.
               If InStr(1, "abcdefgh jk mn pqrstuvwxyzABCDEFGH JKLMN PQRSTUVWXYZ
23456789 ",Chr(intRand), 1) Then
                  isItRand = True
               End If
            Loop
```

```
            randomCode = randomCode & Chr(intRand)
            isItRand = False
         Next

         'Manually compute SHA1 on salt+randomCode, and convert result to base64 -
gives stranger output
         Dim sha1 As sha1 = sha1.Create()
         Dim manualHash As Byte() = sha1.ComputeHash(Encoding.UTF8.GetBytes(salt &
randomCode))
         Dim hashResult as String = Convert.ToBase64String(manualHash)

         'Alternatively, use forms hash routine - only provides upper case A-Z + 0-9
output.
         'Dim hashResult as String =
FormsAuthentication.HashPasswordForStoringInConfigFile(salt & randomCode,"SHA1")

         If dropDownList1.SelectedItem.Value = "1 Hour" Then
            passCode = randomCode & hashResult.SubString(4, 2)
            passCode = passCode & hashResult.SubString(0, 2)
            passCode = passCode & hashResult.SubString(8, 2)
            genCodes.Add(passCode)
         Else
            passCode = randomCode & hashResult.SubString(7, 2)
            passCode = passCode & hashResult.SubString(5, 2)
            passCode = passCode & hashResult.SubString(2, 2)
            genCodes.Add(passCode)
         End If

      Next

      btnExport.Visible = True
      heading.Text = "Your " & codeCount.Text & " <b>" &
dropDownList1.SelectedItem.Value & "</b> Passcodes:"
      genOutput.DataSource = genCodes
      genOutput.DataBind()
      codeCount.Text=""

      'Store the genCodes array in session state for retrieval for printing and
exporting
      Session("myGenCodes") = genCodes
      Session("codeType") = dropDownList1.SelectedItem.Value

   End Sub

   Sub printIt(Src As Object, e As DataListCommandEventArgs)
      If not Session.Item("myGenCodes") is Nothing Then
         genCodes=Session.Item("myGenCodes")
         codeType=Session.Item("codeType")
         'response.write(CStr(genCodes.Item(e.Item.ItemIndex)))

         'Popup hack using Javascript so that individual entries can be printed from
the DataList
         Dim sb As New System.Text.StringBuilder()
         sb.Append("<script language='javascript'>")
         sb.Append("window.open('print.aspx?genCode=")
         sb.Append(Server.URLEncode(CStr(genCodes.Item(e.Item.ItemIndex))))
         sb.Append("&sessLife=")
         sb.Append(Server.URLEncode(codeType))
         sb.Append("','printCode','toolbar=no,")
         sb.Append("addressbar=no,menubar=no,")
         sb.Append("width=400,height=250');")
```

```
         sb.Append("<")
         sb.Append("/")
         sb.Append("script>")
         RegisterStartupScript("stp", sb.ToString)
      End If

   End Sub

   Sub exporter(Sender As Object, E As EventArgs)

   If not Session.Item("myGenCodes") is Nothing Then
      genCodes=Session.Item("myGenCodes")

      'Convert the genCodes array to a string with CRs for later conversion to a byte
array
      Dim i as Integer
      Dim genCodeString as String
      for i = 0 To genCodes.Count - 1
         genCodeString += CStr(genCodes.Item(i)) & Chr(13)
      Next

      'response.write(genCodeString)

      'Create the byte array and send it to the browser as genCodes.csv
      Dim data() As Byte = System.Text.ASCIIEncoding.ASCII.GetBytes(genCodeString)
      Response.Clear()
      Response.AddHeader("Content-Type", "application/Excel")
      Response.AddHeader("Content-Disposition", "inline;filename=genCodes.csv")
      Response.BinaryWrite(data)
      Response.End()
   End If

End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Random Script</TITLE>
</HEAD>

<BODY>
<form id="frmValidator" runat="server">
```

```
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>Algorithmic
Authentication</b></font></td>
      <td><center><img width="216" height="51" src="<%= logo %>"></center></td>
      <td width="50%" align="right" valign="center"><font color="white"><b>Passcode
Generator</b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="90%" border="0" cellpadding="2" cellspacing="0">
   <tr>
      <td><b>Wecome to SonicWALL's LHM Algorithmic Generator.</b><br><br>This will
allow you to create randomly generated passcodes for secure guest internet
access.<br><br>Valid passcodes are not stored anywhere, so validation is not
performed against any kind of database. Instead, when a passcode is entered, it is
algorithmically validated. Once a passcode is successfully used, it is written to a
"used passcode" database so that it cannot be reused.<br><br>The validator will
recognize 1 hour and 24 hour passcodes - these characteristics were encoded within
the passcodes themselves during generation.<br><br>
      </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><br>
      <td width="15%">Passcode type:</td>
      <td width="10%"><asp:DropDownList id="DropDownList1" runat="server">
          <asp:ListItem>1 Hour</asp:ListItem>
          <asp:ListItem>24 Hours</asp:ListItem>
       </asp:DropDownList></td>
      <td width="20%">Number to generate:</td>
      <td width="20%"><asp:TextBox id="codeCount" runat="server" /></td>
      <td width="50%"><asp:RequiredFieldValidator id="valcodeCount"
ControlToValidate="codeCount" ErrorMessage="Enter a value." Font-Size="10"
Display="Dynamic"  runat="server" />
      <asp:RangeValidator id="Range1" ControlToValidate="codeCount" MinimumValue="1"
MaximumValue="999" Type="Integer" Font-Size="10" ErrorMessage="Values from 1 to
999." runat="server" /></td>
   </tr>
   <tr>
      <td colspan=3></td>
      <td><asp:button id="btnSubmit" class="button" text=" Submit "
onClick="btnSubmit_Click" runat="server" />  <asp:button id="btnExport"
class="button" text=" Export " CausesValidation="False" onClick="exporter"
runat="server" /><br></td>
      <td><br></td>

   </tr>
   <tr><tr class="heading">
```

```
      <td colspan=5><font color="white"><asp:Label id=heading runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
</table>

<asp:DataList id="genOutput" Runat="Server" RepeatColumns="4"
RepeatDirection="Horizontal" CellPadding="0" Cellspacing="0" GridLines="Both"
align="center" OnItemCommand="printIt">
  <ItemTemplate>
   <td>
   <asp:Label Text='<%# Container.DataItem %>' Runat="Server"/>
   </td>
   <td>
   <asp:ImageButton id="print" runat="server" ImageUrl="print.gif"
EnableViewState="False" CausesValidation="False" CommandName='<%#
Container.DataItem %>' />
   </td>
  </ItemTemplate>
</asp:DataList>

</form>
</BODY>
</HTML>
```

logout.aspx

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

'This class allows SSL certs signed by unknown CAs to be accepted.
'This is necessary for the POST to the SonicWALL authorizing the LHM session.
Public Class acceptAllCerts
   Implements System.Net.ICertificatePolicy
   Public Function CheckValidationResult(ByVal srvPoint As ServicePoint, _
   ByVal cert As X509Certificate, ByVal request As WebRequest, ByVal problem As
Integer) _
      As Boolean Implements ICertificatePolicy.CheckValidationResult
      Return True
   End Function
End Class

Dim sessionId as String
Dim mgmtBaseUrl as String
Dim eventId as String = "&eventId=1"

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   sessionId=Request.QueryString("sessId")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   sessTimer=Request.QueryString("sessTimer")
```

```
   'Use the override class in myvars.aspx to accept untrusted certificates from the
SonicWALL
   'This is necessary for the POST to the SonicWALL authorizing the LHM session.
   System.Net.ServicePointManager.CertificatePolicy = New acceptAllCerts

   'When the page loads, make the loggedIn span visible
   loggedIn.Visible=True
   loggedOut.Visible=False

   Me.Button1.Attributes.Add("OnClick", "self.close()")

End Sub

'The Logout button
Sub btnSubmit_Click(Sender As Object, E As EventArgs)

   'Let the user know that we are setting up the session, just in case it takes more
than a second
   LHMResult.Text = "Authorizing session. Please wait."

   'The LHM cgi on the SonicWALL - this does not change
   Dim loginCgi as String = "externalGuestLogoff.cgi"

   'Assemble the data to post back to the SonicWALL to authorize the LHM session
   Dim loginParams as String = "sessId=" & sessionId & eventId

   'Combine mgmtBaseUrl from the original redirect with the login cgi
   Dim postToSNWL as String = mgmtBaseUrl & loginCgi

   'Convert the loginParams to a well behaved byte array
   Dim byteArray As Byte() = Encoding.UTF8.GetBytes(loginParams)

   Try
      'Make the loggedOut span visible
      loggedIn.Visible=False
      loggedOut.Visible=True

      'Create the webrequest to the SonicWALL
      Dim toSNWL as WebRequest = WebRequest.Create(postToSNWL)

      'Calculate the length of the byte array
      toSNWL.ContentLength = byteArray.Length

      'Set the method for the webrequest to POST
      toSNWL.Method = "POST"

      'Set the content type
      toSNWL.ContentType = "application/x-www-form-urlencoded"

      'Open the request stream
      Dim dataStream As Stream = toSNWL.GetRequestStream()

      'Write the byte array to the request stream
      dataStream.Write(byteArray, 0, byteArray.Length)

      'Close the Stream object
      dataStream.Close()

      'Get the response
```

```
      Dim snwlReply As WebResponse = toSNWL.GetResponse()

      'Display the status - looking for 200 = OK.
      'Response.Write(CType(snwlReply, HttpWebResponse).StatusCode)

      'Grab the response and stuff it into an xml doc for possible review
      Dim snwlResponse as XmlDocument = New XmlDocument()
      snwlResponse.Load(snwlReply.GetResponseStream())

      'Set the xPath to the SNWL reply, and get the response
      Dim codePath as String =
"SonicWALLAccessGatewayParam/LogoffReply/ResponseCode"

      'Response.Write(snwlResponse.SelectSingleNode(codePath).InnerXml)

      'Response code 150 - Logout Succeeded
      If snwlResponse.SelectSingleNode(codePath).InnerXml = "150"
        LHMResult.Text = "<br><b><font color=""green"">Your session has been logged
out.<br><br>Thank you for using LHM Guest Services.</font></b>"

      'Response code 251 - Bad HMAC.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "251"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed message authentication. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 253 - Invalid SessionID.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "253"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed to match a known session identity. Sorry for
the inconvenience. Please close and relaunch your browser to try again."

      'Response code 254 - Invalid CGI.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "254"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request was missing an essential parameter. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      'Response code 255 - Internal Error.
      ElseIf snwlResponse.SelectSingleNode(codePath).InnerXml = "255"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again."

      End If

      'Close the streams
      dataStream.Close()
      snwlReply.Close()

      'If there is some asp.net error trying to talk to the SonicWALL, print it in
the same color as the background.
      Catch ex as Exception
        catchError.Text = "<font color=""9CBACE"">" & ex.ToString & "</font>"
        LHMResult.Text = "<br><b><font color=""red"">Session logout
failed:</font></b> The request failed due to an unspecified error. Sorry for the
inconvenience. Please close and relaunch your browser to try again. If the problem
persists, please notify an attendant."
      End Try
End Sub
```

```
</script>
<STYLE>
body {
   font-size: 10pt;
   font-family: verdana,helvetica,arial,sans-serif;
   color:#000000;
   background-color:#9CBACE;
}

tr.heading {
   font-size: 10pt;
   background-color:#006699;
}

tr.smalltext {
   font-size: 8pt;
}

.button {
   border: 1px solid #000000;
   background-color: #ffffff;
   font-size: 8pt;
}
</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Logout Page</TITLE>

<SCRIPT LANGUAGE="Javascript">

//'Javascript Seconds Countdown Timer
var SecondsToCountDown = <%= sessTimer%>;
var originalTime=" ";

function CountDown()
{
   clockStr="";

   dayStr=Math.floor(SecondsToCountDown/86400)%100000
   if(dayStr>0){
      if(dayStr>1){
         dayStr+=" days ";
      } else dayStr+=" day ";
      clockStr=dayStr;
   }
   hourStr=Math.floor(SecondsToCountDown/3600)%24
   if(hourStr>0){
      if(hourStr>1){
         hourStr+=" hours ";
      } else hourStr+=" hour ";
      clockStr+=hourStr;
   }
   minuteStr=Math.floor(SecondsToCountDown/60)%60
   if(minuteStr>0){
      if(minuteStr>1){
         minuteStr+=" minutes ";
      } else minuteStr+=" minute ";
      clockStr+=minuteStr;
   }
   secondStr=Math.floor(SecondsToCountDown/1)%60
```

```
   if(secondStr>0){
      if(secondStr>1){
         secondStr+=" seconds ";
      } else secondStr+=" second ";
      clockStr+=secondStr;
   }

   if(SecondsToCountDown > 0)
   {
      --SecondsToCountDown;
   }

   if(originalTime.length < 2)
   {
      originalTime = clockStr;
   }

   // Make sure the form is still there before trying to set a value
   if(document.frmValidator){
      document.frmValidator.originalTime.value = originalTime;
      document.frmValidator.countdown.value = clockStr;
   }

   setTimeout("CountDown()", 1000);
   if(SecondsToCountDown == 0)
   {
      document.frmValidator.countdown.value = "Session Expired";
   }
}

//'Disable right-click so that the window doesn't get refreshed since the countdown
is clientside.
document.oncontextmenu = disableRightClick;
function disableRightClick()
{
  return false;
}

//'Disable F5 key, too, on IE at least.
function noF5()
{
   var key_f5 = 116;
   if (key_f5==event.keyCode)
   {
      event.keyCode=0;
      return false;
   }
   return false;
}

document.onkeydown=noF5
document.onmousedown=disableRightClick

</SCRIPT>

</HEAD>

<BODY onload='CountDown()'>
<span id="loggedIn" runat="server">
<form id="frmValidator" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
```

```
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="smalltext"><td><br></td></tr>
   <tr class="smalltext">
      <td>Original Session Time:</td>
      <td><asp:textbox width=250 id="originalTime" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td>Remaining Session Time:</td>
      <td><asp:textbox width=250 id="countdown" runat="server" /></td>
   </tr>
   <tr class="smalltext">
      <td colspan=2><br>You may use this window to manually logout your session at
any time, or you may safely close this window if you prefer to let your session
timeout automatically.</font></td>
   </td>
   <tr>
      <td colspan=2><center><asp:button id="btnSubmit" class="button" text="  Logout
" onClick="btnSubmit_Click" runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

<span id="loggedOut" runat="server">
<form id="logout" runat="server">
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"><b>SonicWALL LHM Logout
Window</b></font></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"> </td>
   </tr>
   <tr>
      <td><asp:Label id=LHMResult runat="server" /></td>
   </tr>
   <tr>
      <td><asp:Label id=catchError runat="server" /></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td><center><asp:button id="Button1" class="button" text="  Close  "
runat="server" /></center></td>
   </tr>
</table>
</form>
</span>

</BODY>
</HTML>
```

myvars.aspx

```
<script language="VB" runat="server">

'Set the logoutPopup window flag - 0 = no popup, 1 = popup
'The use of the logoutPopup in this script is discouraged because the login event is
exclusive.
'The login event can be made non exclusive in this script by setting useDB to 0.
Dim logoutPopup as String = "0"

'Set the use of the database for storing and checking used passcodes. 0 = do not use
DB, 1 = use DB.
Dim useDB as String = "1"

'The number of characters in the randomCode
Dim randChars as Integer = 6

'Set the salt the generation of the SHA1 hash
Dim salt as String = "moosifer"

'The LHM Session Timeout is set by the passcode in this script
Dim sessTimer as String

'Set the LHM Idle Timeout
Dim idleTimer as String = "300"

'Set the secret for use with optional HMAC auth, as configured in the Extern Guest
Auth config on the SonicWALL
Dim strHmac as String = "password"

'Set the digest method for the HMAC, either MD5 or SHA1
Dim hmacType as String = "MD5"
'Dim hmacType as String = "SHA1"

'Set the logo image to use
Dim logo as String = "sonicwall.gif"

'------------------------End of Configurable Settings-------------------------

</script>
```

print.aspx

```
<!-- #INCLUDE file="myvars.aspx" -->

<script language="VB" runat="server">

Dim genCode as String
Dim sessLife as String

'Grab the code and the session lifetime from the generator page
Sub Page_Load(src as Object, e as EventArgs)
   genCode=Request.QueryString("genCode")
   sessLife=Request.QueryString("sessLife")
End Sub

</script>
<STYLE>
body {
  font-size: 10pt;
```

```
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}
tr.heading {
  background-color:#006699;
}
</STYLE>
<BODY>
<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><img width="216" height="51" src="<%= logo
%>"></td>
   </tr>
   <tr class="heading">
      <td colspan=2 align="center"><font color="white"> </td>
   </tr>
   <tr><td><br><br></td></tr>
   <tr>
      <td>Your Pass Code is:</td>
      <td><b><%= genCode%></b></td>
   </tr>
   <tr><td><br></td></tr>
   <tr>
      <td>Session Lifetime is:</td>
      <td><b><%= sessLife%></b></td>
   </tr>
</table>

<script language='javascript'>window.print();</script>

</BODY>
</HTML>
```

Chooser.aspx 指令碼

```
<%@ Page Language="VB" Debug="true" %>
<%@ Import Namespace="System" %>
<%@ Import Namespace="System.Net" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Xml" %>
<%@ Import Namespace="System.Text" %>
<%@ Import Namespace="System.Security" %>
<%@ Import namespace="System.Security.Cryptography.X509Certificates"%>

<script language="VB" runat="server">

Dim ip as String
Dim sessionId as String
Dim mac as String
Dim ufi as String
Dim mgmtBaseUrl as String
Dim clientRedirectUrl as String
Dim req as String
Dim hmac as String
Dim customCode as String
Dim qString as String
```

```
Sub Page_Load(src as Object, e as EventArgs)

   'Grab the querystring one element at a time since we need to do a custom URL
encode on the req variable
   sessionId=Request.QueryString("sessionId")
   ip=Request.QueryString("ip")
   mac=Request.QueryString("mac")
   ufi=Request.QueryString("ufi")
   mgmtBaseUrl=Request.QueryString("mgmtBaseUrl")
   clientRedirectUrl=Request.QueryString("clientRedirectUrl")
   req=Request.QueryString("req")
   hmac=Request.QueryString("hmac")
   customCode=Request.QueryString("cc")

   'SonicWALL URL Encode routine is different from Microsoft - this is the SonicWALL
method
   req=Replace(req,"%","%25")
   req=Replace(req,":","%3A")
   req=Replace(req," ","%20")
   req=Replace(req,"?","%3F")
   req=Replace(req,"+","%2B")
   req=Replace(req,"&","%26")
   req=Replace(req,"=","%3D")

   'Rebuild the querystring variable
   qString = "sessionId=" & sessionId & "&ip=" & ip & "&mac=" & mac & "&ufi=" & ufi &
"&mgmtBaseUrl=" & mgmtBaseUrl & "&clientRedirectUrl=" & clientRedirectUrl & "&req="
& req

   'Add the optional hmac and cc vars if they are there.
   If hmac <> "" Then
      qString+="&hmac=" & hmac
   End If

   If customCode <> "" Then
      qString+="&cc=" & customCode
   End If

   'Bind the directory data
   Dim lhmDir As New DirectoryInfo(Server.MapPath("."))
   lhmList.DataSource = lhmDir.GetDirectories
   lhmList.DataBind()


End Sub

</script>

<STYLE>
body {
  font-size: 10pt;
  font-family: verdana,helvetica,arial,sans-serif;
  color:#000000;
  background-color:#9CBACE;
}

tr.heading {
  background-color:#006699;
}
```

```
.button {
   border: 1px solid #000000;
   background-color: #ffffff;
}

tr.hidden {
   font-size: 5pt;
   color:#9CBACE;
}

</STYLE>

<HTML>
<HEAD>
<TITLE>LHM Script Chooser</TITLE>
</HEAD>

<BODY>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
   <tr class="heading">
      <td width="50%" valign="center"><font color="white"><b>LHM Script
Chooser</b></font></td>
      <td><center><img width="216" height="51" src="sonicwall.gif"></center></td>
      <td width="50%" align="right" valign="center"><font
color="white"><b></b> </font></td>
   </tr>
   <tr class="heading">
      <td colspan=3 align="center"><font color="white"> </td>
   </tr>
</table>

<table width="100%" border="0" cellpadding="2" cellspacing="0">
   <tr><td><br></td></tr>
   <tr><td><H3>Please select one of the LHM Scripts below</H3></td></tr>
   <tr><td>Your original querystring information will be passed to the target script,
and it will open in a new window.</td></tr>
   <tr><td><br></td></tr>
</table>

<asp:Repeater id="lhmList" runat="server">
   <ItemTemplate >
        <li><a href = <%# DataBinder.Eval(Container.DataItem, "Name").ToString() &
"/default.aspx?" & qString & " target=""_blank""" %> >
        <%# DataBinder.Eval(Container.DataItem, "Name").ToString() %>
        </a>
        </li>
    </ItemTemplate>
 </asp:Repeater>

<table>
<tr class="hidden">
<td>default.aspx?sessionId=0b712fd83b9f5313db5af1cea6b1004f&ip=10.50.165.231&mac=00
:0e:35:bd:c9:37&ufi=0006b11184300&mgmtBaseUrl=https://10.50.165.193:4043/&clientRed
irectUrl=https://10.50.165.193:444/&req=http%3A//www.google.com/ig</td></tr>
</table>

</BODY>
</HTML>
```

B

IPv6

IPv6

本附錄說明 IPv6 的 SonicOS 實施，IPv6 的工作方式以及如何為網路設定 IPv6。

主題：

關於 IPv6

主題：

IPv6 就緒認證

SonicWall 符合 IPv6 論壇規定的「IPv6 就緒」階段 1 和階段 2 的要求，此論壇是為部署 IPv6 提供技術指導的國際性團體。IPv6 Ready Logo Program（IPv6 就緒性標誌計劃）是一項旨在透過證明 IPv6 已就緒可用來提高使用者信心的合規與互操作性測試計劃。

「IPv6 就緒」系列測試從階段 1 的基本級最低覆寫率擴充階段 2 的更高覆寫率：

- 階段 1（銀質）標誌：在第一階段，標誌表示產品包含 IPv6 強制核心通訊協定，並可與其他 IPv6 實作的相互操作。
- 階段 2（金質）標誌：「IPv6 就緒」步驟包含適當的維護、技術一致性和明確的技術參考。「IPv6 就緒標誌」表示產品已成功滿足 IPv6 標誌委員會 (v6LC) 規定的嚴格要求。

SonicWall 經認證已符合階段 2（金質）IPv6 就緒狀態。目前正在制定未來的工作階段 3 層級「IPv6 就緒」覆寫率。

更多資訊，請參見：http://www.ipv6ready.org/

附註：SonicOS 不支援 IPv6 精靈。

IPv6 技術概述

每台連接至網際網路的裝置（電腦、印表機、智慧行動電話、智慧量表等）都需要一個 IP 位址。第 4 版網際網路通訊協定 (IPv4) 提供大約 43 億個唯一 IP 位址。隨著網際網路、智慧行動電話和 VoIP 電話的全球性迅速普及，將很快用盡這 43 億個 IP 位址。

2011 年 2 月 3 日，網際網路號碼指派局 (IANA) 向區域網際網路註冊管理機構 (RIR) 指派了最後剩餘的 IPv4 位址區塊。在 RIR 於今年晚些時候向 ISP 指派完這些位址後，將消耗殆盡全世界的新 IPv4 位址供應。

幸好網際網路工程任務推動小組 (IETF) 早在 1992 和 1998 年就已開始計劃這一天的到來，當時就已發佈 RFC 2460 用於定義第 6 版網際網路通訊協定 (IPv6)。透過將位址長度從 32 位元延長至 128 位元，IPv6 較之 IPv4 極大地增加了可用的位址數：

- IPv4：4,294,967,296 個位址
- IPv6：340,282,366,920,938,463,463,374,607,431,768,211,456 個位址

了解 IPv6 位址

IPv6 位址由八組數字組成，每群組包含四位十六進位數值並以冒號分隔：

`XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX`

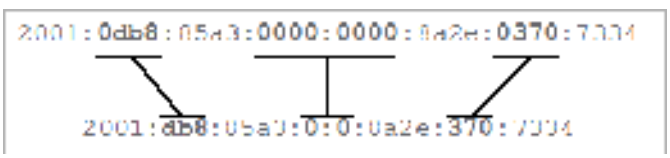
IPv6 位址在邏輯上分為兩部分：64 位元（子）網路首碼和 64 位元介面識別項。以下是一個 IPv6 位址範例：

`2001:0db8:85a3:0000:0000:8a2e:0370:7334`

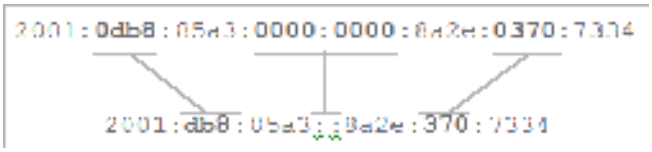
附註：IPv6 位址中的十六進位數值不區分大小寫。

IPv6 位址可以使用以下兩個規則縮寫：

1 16 位元值中的前導零可以忽略。因此，本範例中的位址可以從完整形式縮寫，如下所示：



2 任意個均由四個零組成的連續群組（理論上 16 位元零）可以使用雙冒號（::）表示。結合這兩個規則，本範例中的位址可以從完整形式縮寫，如下所示：



ⓘ **提示：**空位址的縮寫，或 0:0:0:0:0:0:0:0 為 ::。

IPv6 位址類型

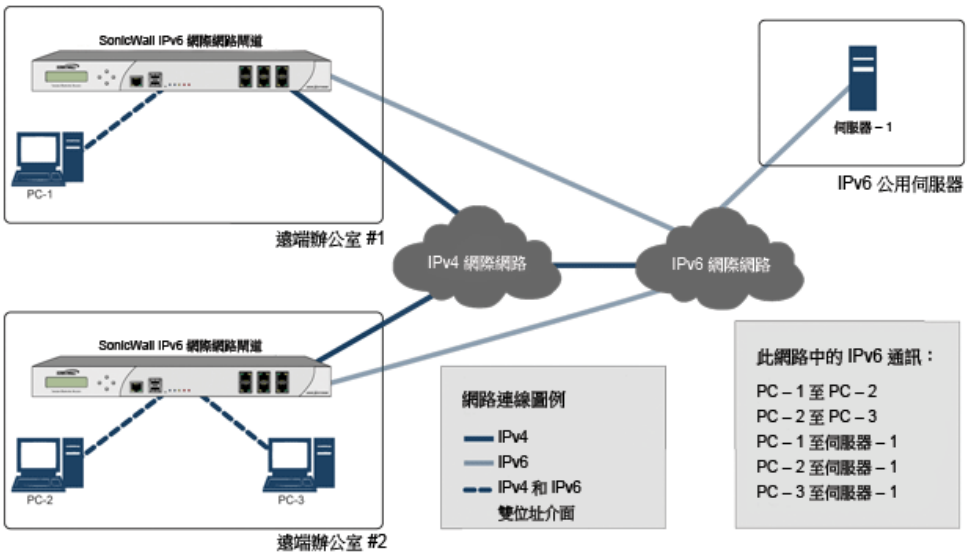
位址類型	完整的位址	縮寫的位址
單點傳送位址	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
多點傳送位址	FF01:0:0:0:0:0:0:101	FF01::101
回送位址	0:0:0:0:0:0:0:1	::1
未指定位址	0:0:0:0:0:0:0:0	::

ⓘ **附註：**網路必須具備 IPv4 網際網路連線才能連至 IPv6 網際網路。

ⓘ **附註：**本機網路站台的電腦必須啟用 IPv6 堆疊。

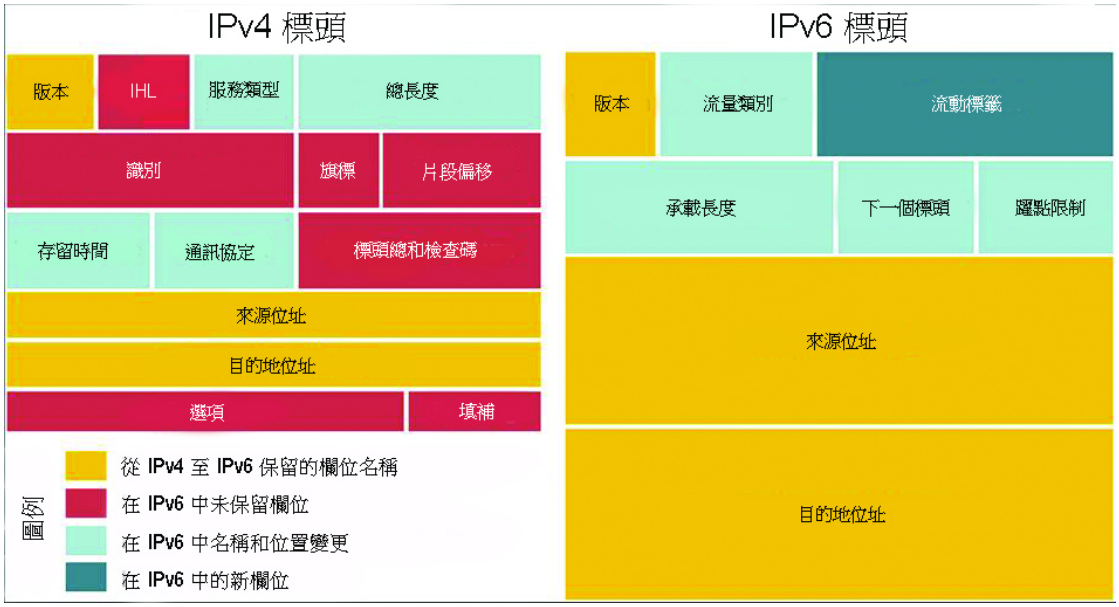
典型 IPv6 部署是一幅典型 IPv6 部署的連線模型簡化圖。

典型 IPv6 部署



IPv4 和 IPv6 標頭元素的對比會比較 IPv4 和 IPv6 之間的標頭元素。

IPv4 和 IPv6 標頭元素的對比



IPv6 優點

IPv6 具備一些關鍵功能改善了 IPv4 的某些局限性。新的 IP 標準在很多重要方面擴充了 IPv4：

- 6 至 4 通道（允許 IPv6 節點透過 IPv4 網路連接外部 IPv6 服務）
  - 6to4 自動通道
  - GRE 通道
- IPv6 手動通道
- 新的簡化 IPv6 標頭格式
- 極大增加了可用的 IPv6 位址
- 有效、分層的定址和路由基礎結構
- 使用鄰居發現通訊協定 (NDP) 和 DHCPv6 的主機和路由器自動位址指派
- 無狀態和有狀態的位址設定
- 內建安全性 - 強烈建議 AH 和 ESP
- 更好的 QoS 支援 - 標頭中的流標籤
- 新鄰接節點互動通訊協定
- 使用擴充標頭以擴充新功能

  從 SonicOS 6.2.5.1 開始：
  - 擴充標頭偵測報告和記錄支援
  - 延伸標頭順序檢查執行
  - 支援逐跳擴充標頭
  - 輸入類型 0 的路由標頭封包檢查

目前支援的 SonicWall IPv6 服務和功能

如需目前支援的 IPv6 服務和功能完整清單，請參閱以下知識庫文章: *SonicOS 6.2.x 韌體支援/不支援的 IPv6 功能*。

目前不支援的 SonicWall IPv6 功能

附註：SonicOS 6.2 是雙 IP 堆疊韌體。IPv4 仍支援 IPv6 尚不支援的功能。

如需目前不支援的 IPv6 服務和功能完整清單，請參閱以下知識庫文章: *SonicOS 6.2.x 韌體支援/不支援的 IPv6 功能*。

支援的 IPv6 RFC

本章節列出 SonicOS 6.2 支援的 IPv6 RFC：

- 第 765 頁「TCP/IP 堆疊和網路通訊協定」
- 第 766 頁「IPsec 合規」
- 第 766 頁「NAT 合規」
- 第 766 頁「DNS 合規」

TCP/IP 堆疊和網路通訊協定

- RFC 1886 支援 IPv6 的 DNS 擴充 [IPAPPL dns 用戶端]
- RFC 1981 IPv6 路徑 MTU 發現
- RFC 2113 IP 路由器警示選項
- RFC 2373 IPv6 定址體系結構
- RFC 2374 IPv6 可彙總全域單點傳送位址格式（由 3587 廢除）
- RFC 2375 IPv6 多點傳送位址指派
- RFC 2460 IPv6 規定
- RFC 2461 IPv6 的鄰居發現
- RFC 2462 IPv6 無狀態位址自動設定
- RFC 2463 IPv6 規定的 ICMPv6
- RFC 2464 透過乙太網路傳送 IPv6 封包
- RFC 2473 IPv6 規定中的一般封包通道
- RFC 2474 IPv4 和 IPv6 標頭中的區分服務欄位（DS 欄位）定義
- RFC 2545 使用 IPv6 網域間路由的 BGP-4 多重通訊協定擴充
- RFC 2553 IPv6 的基礎套接介面擴充
- RFC 2710 IPv6 的多點傳送監聽發現 (MLD)
- RFC 2711 IPv6 路由器警示選項
- RFC 2784 一般路由封裝

- RFC 2893 IPv6 主機和路由器的轉換機制
- RFC 2991 單點傳送和多點傳送下一躍點選擇中的多路徑問題
- RFC 3056 透過 IPv4 雲端的 IPv6 網域連接
- RFC 3484 第六版網際網路通訊協定 (IPv6) 的預設位址選擇（無原則掛鉤）
- RFC 3493 IPv6 的基礎套接介面擴充
- RFC 3513 第六版網際網路通訊協定 (IPv6) 定址體系結構
- RFC 3542 IPv6 的進階套接應用程式編程介面 (API)
- RFC 3587 IPv6 全域單點傳送位址格式（廢除 2374）

IPsec 合規

- RFC 1826 IP 身分驗證標頭 [舊 AH]
- RFC 1827 IP 封裝式安全措施承載 (ESP) [舊 ESP]

NAT 合規

- RFC 2663 IP 網路位址轉譯器 (NAT) 技術和考慮因素。
- RFC 3022 傳統 IP 網路位址轉譯器（傳統 NAT）。

DNS 合規

- RFC 1886 支援 IPv6 的 DNS 擴充

不支援的 IPv6 RFC

本章節列出 SonicOS 6.2 目前不支援的 IPv6 RFC：

- RFC 2002 IP 行動支援
- RFC 2766 網路位址轉譯 - 通訊協定轉換 (NAT-PT)
- RFC 2472 IPv6 over PPP
- RFC 2452 用於傳送控制通訊協定的 IPv6 管理資訊基礎。
- RFC 2454 用於使用者資料包通訊協定的 IPv6 管理資訊基礎。
- RFC 2465 用於 IPv6 的管理資訊基礎：文字使用慣例和一般群組。

設定 IPv6

主題：

- 第 767 頁「IPv6 介面設定」
- 第 776 頁「設定 IPv6 通道介面」
- 第 785 頁「使用 IPv6 存取 SonicWall 管理介面。」
- 第 785 頁「IPv6 網路設定」

- 第 787 頁「IPv6 存取規則設定」
- 第 787 頁「IPv6 進階防火牆設定」
- 第 787 頁「IPv6 IPSec VPN 設定」
- 第 788 頁「IPv6 的 SSL VPN 設定」

IPv6 介面設定

IPv6 介面可以在**網路 | 介面**頁面透過按一下**介面設定**表右上角的**檢視 IP 版本**選項按鈕的 IPv6 選項進行設定。

預設情況下，所有 IPv6 介面顯示為不使用 IP 位址路由。可以在相同介面新增多個 IPv6 位址。只能在 WAN 介面上設定自動 IP 指派。

附註：IPv6 不支援 PortShield 介面。

可以設定每個介面是否接收路由宣告。可以在各介面啟用或停用 IPv6。

附註：介面的區域指派在切換到 IPv6 模式之前，必須透過 IPv4 介面頁面進行設定。

主題：

- 第 767 頁「IPv6 介面設定的局限性」
- 第 768 頁「為 IPv6 固定模式設定介面」
- 第 769 頁「設定進階 IPv6 介面選項和多個 IPv6 位址」
- 第 770 頁「設定路由器宣告設定」
- 第 771 頁「設定路由宣告首碼設定」
- 第 771 頁「設定 DHCPv6 模式的介面」
- 第 773 頁「設定 IPv6 介面的進階設定」
- 第 774 頁「檢視 DHCPv6 通訊協定資訊」
- 第 774 頁「設定自動模式的介面」
- 第 775 頁「PPPoE」
- 第 775 頁「設定 VLAN 子介面」
- 第 776 頁「設定有線模式的介面」

IPv6 介面設定的局限性

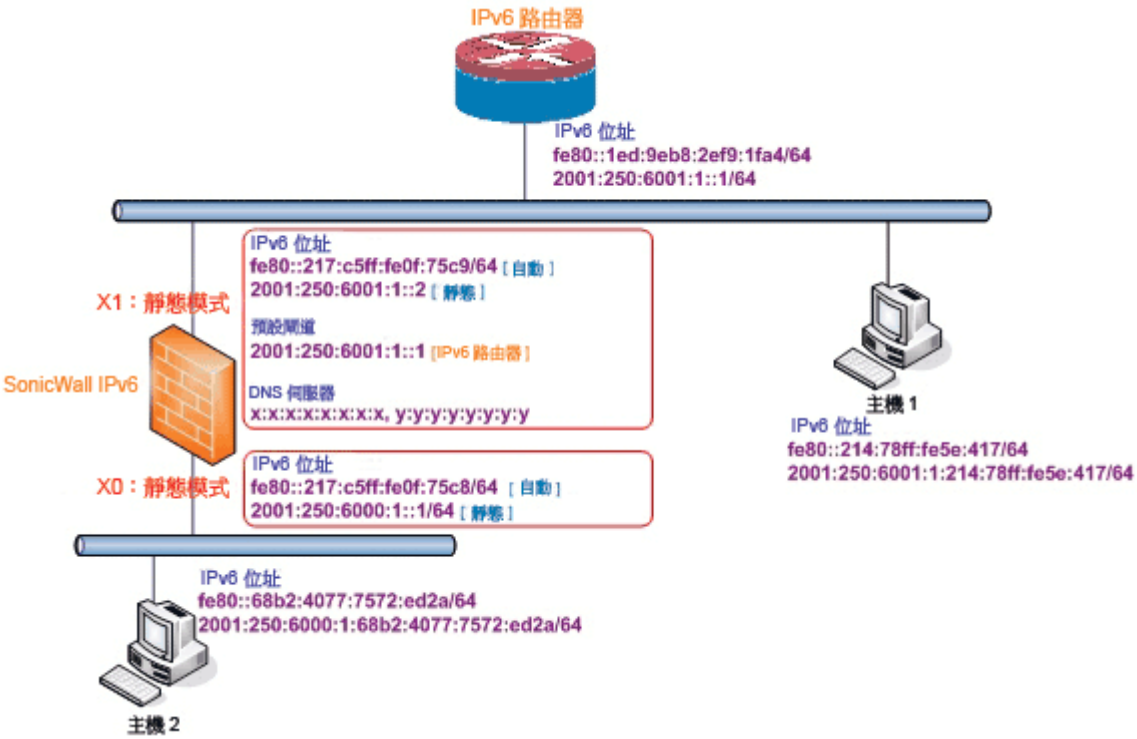
- 無法為 IPv6 設定 HA 介面。
- 只能將 SwitchPort 群組的父級介面設定為 IPv6 介面，因此交換器連接埠群組的所有子級都必須從此清單中排除。
- 區域和二層橋接群組是 IPv4 和 IPv6 在介面上共用的設定。在 IPv4 側設定後，介面的 IPv6 側使用相同的設定。
- 只能為 WAN 區域介面設定預設閘道和 DNS 伺服器。
- IPv6 支援有線模式，但無法編輯任何設定。SonicOS 使用為 IPv4 設定的相同設定選項代替。

為 IPv6 固定模式設定介面

固定模式為使用者提供指派固定 IPv6 位址的一種方式，這不同於自動指派的位址。IPv6 介面使用固定模式仍然可以監聽路由宣告和向相應的首碼選項學習自發位址。固定模式不中斷 IPv6 介面上的無狀態位址自動設定的執行，除非使用者手動停用。

IPv6 固定模式設定顯示在固定模式中設定的 IPv6 樣本拓撲結構。

IPv6 固定模式設定



在這種模式中，可以指派三種 IPv6 位址：

- 自動位址
- 自發位址
- 固定位址

若要設定固定 IPv6 位址的介面：

1 移至**網路 | 介面**頁面。

2 按一下頁面右上角的 **IPv6** 按鈕。裝置的 IPv6 位址顯示。

3 按一下您要為其設定 IPv6 位址的介面的**設定**圖示。顯示**編輯介面**對話方塊。

> **附註：**必須在 IPv4 定址頁面設定介面的區域指派。若要修改 IPv6 介面的區域指派，請按一下頁面右上角的 **IPv4** 按鈕，修改介面的區域，然後返回到 IPv6 介面頁面。

4 在 **IP 指派**下拉功能表中，選擇**固定**。

5 輸入介面的 **IPv6 位址**。

6 輸入位址的**首碼長度**。

7 如果這是主要 WAN 介面，請輸入**預設閘道**的 IPv6 位址。如果這不是主要 WAN 介面，則將忽略任何預設閘道項目，所以您可以將其保留為 `::`。（雙冒號是空位址的縮寫，或 `0:0:0:0:0:0:0:0`。）

8 如果這是主要 WAN 介面，請輸入最多三個 **DNS 伺服器** IPv6 位址。再次說明，如果這不是主要 WAN 介面，將忽略任何 DNS 伺服器項目。

9 勾選**啟用路由宣告**使其成為傳播網路和首碼資訊的發佈介面。

10 勾選**發佈 IPv6 主要固定位址**的子網路首碼向介面發佈首碼清單新增預設首碼。此首碼是介面 IPv6 主要固定位址的子網路首碼。此選項將協助連結上的所有主機停留在相同子網路中。

設定進階 IPv6 介面選項和多個 IPv6 位址

若要修改進階 IPv6 介面選項或設定多個固定 IPv6 位址：

1 在**編輯介面**對話中，按一下**進階**標籤。

2 按一下**新增位址**按鈕設定介面的多個固定 IPv6 位址。顯示**新增介面 IPv6 位址**對話方塊。

> **附註：**只能為設定為固定 IPv6 位址模式的介面新增多個 IPv6 位址。無法為**自動**或 **DHCPv6** 模式設定多個 IPv6 位址。

3 為介面的附加位址輸入 **IPv6 位址**。

4 輸入位址的**首碼長度**。

5 勾選**發佈 IPv6 位址的子網路首碼**，向介面發佈首碼清單新增預設首碼。此首碼是介面 IPv6 主要固定位址的子網路首碼。此選項將協助連結上的所有主機停留在相同子網路中。

6 按一下**確定**。

7 以下附加選項可以在**進階**標籤的**進階設定**標題下設定：

- 選擇**停用介面上的所有 IPv6 流量**封鎖介面處理所有 IPv6 流量。停用 IPv6 流量可以改進非 IPv6 流量的防火牆效能。預設情況下未勾選此選項。

  > **提示：**如果防火牆在純 IPv4 環境中部署，SonicWall 建議啟用此選項。

- 選擇**啟用接聽路由器宣告**允許防火牆接收路由宣告。如果停用，介面篩選所有接收的路由宣告訊息，這可以透過封鎖接收惡意網路參數（例如首碼資訊或預設閘道）來增強安全性。預設情況下已核取此選項。

  > **附註：**如果停用此選項，所有指派的自發 IPv6 位址會從此介面移除。

  此選項在**自動**模式中無法使用。在**自動**模式中，始終啟用此選項。

  - 勾選**啟用無狀態位址自動設定**允許將自發 IPv6 位址指派到此介面。如果取消勾選，所有指派的自發 IPv6 位址將從此介面移除。

    此選項在**自動**模式中無法使用。在**自動**模式中，始終啟用此選項。

- 輸入**重複地址偵測重新傳送**的數值指定在執行重複位址偵測 (DAD) 時向介面指派暫定位址前傳送的連續鄰居請求訊息數。最小值為 0，最大值為 9，預設值為 **1**。值 0 表示未在介面執行 DAD。

- 在**鄰居搜索的基本可存取時間 (秒)**中，輸入以秒為單位的基本值，以用於運算介面的隨機可連線時間值。最小值為 0，最大值為 9999，預設值為 **30**。

  值 0 表示未指定參數，而在**網路 | 鄰居搜索**中使用全域設定。如果在此介面上啟用 RA，不過會使用**路由器宣告**標籤上**可連線時間**選項中的值。

- 選擇**啟用每個介面最大 NDP 大小**，對每個介面啟用最大的 NDP 大小。每個介面應有最大 NDP 大小，以防系統資源用盡。
    - 在「每個介面最大 NDP 大小」欄位中輸入最大 NDP 大小。最小值是 64，最大值是 9999，而 WAN 介面的預設值是 **128**，其他則是 **1200**。
- 與 IPv4 無故 ARP 類似，IPv6 節點使用鄰居請求訊息偵測相同連結上的重複的 IPv6 位址。在向 IPv6 介面指派暫定位址前，DAD 必須在任何單點傳送位址上執行（任意廣播位址除外）。

設定路由器宣告設定

路由宣告允許 IPv6 路由器向 IPv6 主機發佈 DNS 遞歸伺服器位址。基於路由宣告的 DNS 設定是網路中有用、可選的替代設定，其中，IPv6 主機的位址透過 IPv6 無狀態位址自動設定進行自動設定，其中獲取伺服器位址和與伺服器通信的延遲的影響嚴重。路由宣告允許主機在每個連結上獲取最近的伺服器位址。此外，它還向提供連結設定資訊的相同 RA 訊息學習這些位址，從而避免了附加通訊協定執行。這在某些行動環境中十分有益，例如在行動 IPv6 中。SonicWall 的 IPv6 實作與路由器和首碼發現中的 RFC 4861 完全相容。

附註：只有在介面處於固定模式下，才可以啟用路由宣告。

若要為 IPv6 介面設定路由器宣告：

1 在**編輯介面**對話中，按一下**路由器宣告**標籤。

2 勾選**啟用路由器宣告**核取方塊，使其成為傳播網路和首碼資訊的播發介面。

3 此外，您可以選擇修改以下路由器宣告設定：

- **路由器宣告間隔範圍 (秒)** - 輸入從介面傳送主動提供的多點傳送路由器宣告之間的時間間隔 (以秒為單位)。宣告是以最小和最大間隔之間的隨機值傳送：
    - 最小間隔 - 輸入各個路由器宣告間所允許的最短間隔。最短時間為 3 秒，最長時間為 1350 秒，而預設最短時間為 **200** 秒。
    - 最大間隔 - 輸入各個路由器宣告間所允許的最長間隔。最短時間為 4 秒，最長時間為 1800 秒，而預設最長時間為 **600** 秒。
- **連結 MTU** - 為介面連結輸入建議的 MTU。最小值為 0，最大值為 99999，而預設值為 **0**，即表示防火牆不會宣告連結的連結 MTU。
- **可連線時間 (秒)** - 輸入節點在收到可達到確認後認為可達到鄰居的時間。最小值為 0，最大值為 9999999999，而預設值為 **0**，即表示此防火牆未指定此參數。
- **重傳時間** - 輸入重新傳送的鄰居請求訊息之間的時間。最小值為 0，最大值為 9999999999，而預設值為 **0**，即表示此防火牆未指定此參數。
- **目前躍點限制** - 輸入應填寫到輸出 IP 封包的 IP 標頭躍點數欄位中的預設值。最小值為 0，表示此防火牆未指定此參數；最大值為 255，而預設值為 **64**。
- **路由存留時間 (秒)** - 輸入接受防火牆為預設路由器的存留時間。最小值為 0，表示路由器不是預設路由器；最長時間為 9000 秒，而預設值為 **1800** 秒。
- **路由器喜好設定** - 指出宣告預設路由器是否應優於其他預設路由器。從下拉功能表選擇**高**、**中** (預設) 或**低**。

4 勾選**管理**核取方塊即可在路由宣告訊息中設定受管理的位址設定標誌。如果設定，旗標即表示透過動態主機設定通訊協定可以獲得 IPv6 位址。

5 勾選**其他設定**核取方塊即可在路由宣告訊息中設定其他設定標誌。如果設定，旗標即表示透過動態主機設定通訊協定可以獲得其他設定資訊。

設定路由宣告首碼設定

宣告首碼提供主機用於在連結上確定和位址自動設定的首碼。

若要設定路由器宣告首碼：

1 移至**編輯介面**對話的**路由器宣告**標籤上的**首碼清單設定**表格。

2 按一下**新增首碼**按鈕。**新增宣告首碼**對話方塊會顯示。

3 輸入將與路由宣告訊息一起發佈的**首碼**。

4 輸入**有效存留時間 (分鐘)**，設定首碼可用於在連結上確定的時間長度。最小值為 1；最大值為 71582789，表示存留時間為無限，而預設值為 **43200** 分鐘。

5 輸入**慣用存留時間 (分鐘)**，設定透過無狀態位址自動設定從首碼產生的位址保持為慣用的位址的時間長度。最小值為 1；最大值為 71582789，表示存留時間為無限，而預設值為 **10080** 分鐘。

6 另外，選擇**連結**核取方塊在首碼資訊選項中啟用連結旗標，表示這首碼可用於連結確定。

7 另外，選擇**自發**核取方塊在首碼資訊選項中啟用自發位址設定旗標，表示這首碼可用於無狀態位址設定。

8 按一下**確定**。

設定 DHCPv6 模式的介面

DHCPv6（用於 IPv6 的 DHCP）是為 IPv6 主機提供狀態位址設定或無狀態設定的用戶端/伺服器通訊協定。將介面設定為 DHCPv6 模式後，將 DHCPv6 用戶端啟用為學習 IPv6 位址和網路參數。

DHCPv6 定義兩個不同的設定模式：

- **DHCPv6 狀態模式**：DHCPv6 用戶端需要 IPv6 位址與其他網路參數（例如 DNS 伺服器、網域名稱等）。
- **DHCPv6 無狀態模式**：DHCPv6 用戶端僅獲取 IPv6 位址以外的網路參數。

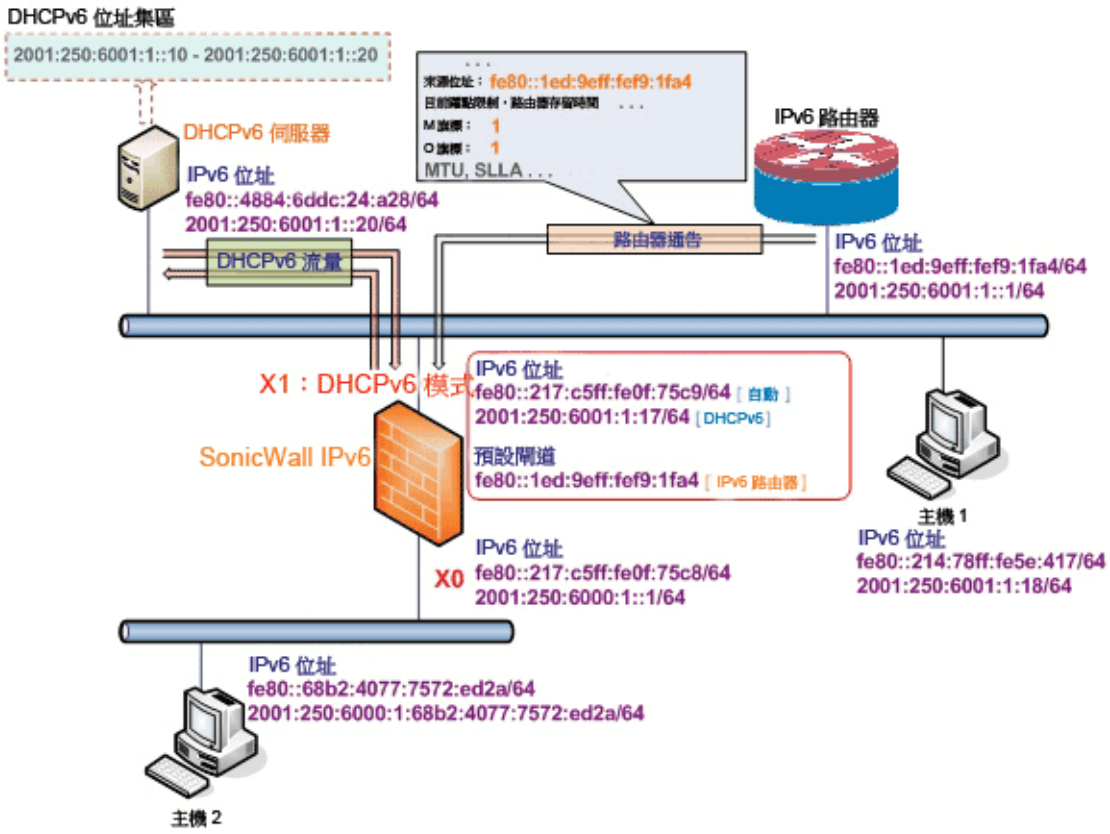
選擇哪種模式取決於宣告的路由器宣告訊息中的受管理 (M) 位址設定及其他 (O) 設定旗標：

DHCPv6 基礎結構

旗標		設定
M	O	
0	0	無 DHCPv6 基礎結構。
1	1	IPv6 主機對 IPv6 位址和其他網路參數設定使用 DHCPv6。
0	1	IPv6 主機只對 IPv6 位址指派使用 DHCPv6。
1	0	IPv6 主機只有對其他網路參數設定使用 DHCPv6，也稱為 DHCPv6 無狀態。

DHCPv6 拓撲顯示 DHCPv6 拓撲結構範例。

DHCPv6 拓撲



可以在 DHCPv6 下指派三種 IPv6 位址類型：

- 自動位址
- 自發位址
- 透過 DHCPv6 用戶端指派的 IPv6 位址

若要設定 DHCPv6 位址的介面：

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 如果您要設定未指派的介面，請按一下頁面右上角的 **IPv4** 選項按鈕。

3 對於要設定的介面，按一下**編輯**圖示。顯示**編輯介面**對話方塊。

4 從**區域**下拉功能表中選擇 **WAN**。將顯示更多選項。

5 從 **IP 指派**下拉功能表中選擇 **DHCP**。

6 按一下**確定**。

7 按一下頁面右上角的 **IPv6** 按鈕。裝置的 IPv6 位址顯示。

8 按一下您要為其設定 IPv6 位址的介面的**設定**圖示。顯示**編輯介面**對話方塊。

9 在 **IP 指派**下拉功能表中，選擇 **DHCPv6**。這些選項將發生變更。

10 對於為 DHCPv6 模式設定的 IPv6 介面，可以設定以下選項：

- **啟用 DHCPv6 首碼委派** - 如果啟用此選項，則這些選項可用：

- **傳輸慣用的代理首碼** - 選擇此選項可要求 DHCAPv6 用戶端嘗試傳送兩個欄位中指定的慣用的代理首碼。
- **啟動時傳輸更新之前授權首碼的提示** - 選擇此選項可要求 DHCAPv6 用戶端嘗試在防火牆啟動時更新先前指派的代理首碼。

- **使用快速認可選項** - 如果啟用，DHCPv6 用戶端使用「快速提交選項」以使用兩個訊息交換用於位址指派。
- **在啟用時傳輸更新以前 IP 的提示** - 如啟用，在防火牆啟動時，DHCPv6 用戶端將嘗試更新指派的位址。

11 設定介面的 **DHCPv6 模式**。按照 RFC 的要求，DHCPv6 用戶端根據路由宣告訊息決定應該選擇哪種模式（有狀態或無狀態）。此定義會限制使用者的選擇，由系統自行決定 DHCPv6 模式。SonicWall 的 DHCPv6 實作定義了兩種不同的模式用於負載均衡合規與靈活性：

- **自動** - IPv6 介面按照最近接收的路由器宣告訊息中 M 和 O 設定，使用無狀態/狀態自動設定來設定 IPv6 位址。請參閱 DHCPv6 基礎結構表格。
- **手動** - 不管收到的路由器宣告如何，DHCPv6 模式總是手動設定。

僅請求無狀態資訊選項會確定使用哪種 DHCPv6 模式。如果取消勾選此選項，DHCPv6 用戶端則處於有狀態模式，如果勾選此選項，DHCPv6 用戶端處於無狀態模式下，僅獲取網路參數。

12 另外，也可以勾選**僅請求無狀態資訊**核取方塊使 DHCPv6 用戶端只向 DHCPv6 伺服器請求網路參數設定。IPv6 位址透過無狀態自動設定進行指派。

13 另外，您也可以選擇設定**管理**登入或**使用者登入**。

14 另外，按一下**進階**標籤設定進階選項和/或按一下**通訊協定**標籤檢視 DHCPv6 有狀態和無狀態設定資訊。

15 按一下**確定**以完成設定。

設定 IPv6 介面的進階設定

若要設定進階 IPv6 介面設定：

1 在**編輯介面**對話中，按一下**進階**標籤。

2 選擇**停用介面上的所有 IPv6 流量**封鎖介面處理所有 IPv6 流量。停用 IPv6 流量可以改進非 IPv6 流量的防火牆效能。預設情況下未勾選此選項。

> ⓘ **提示：**如果防火牆在純 IPv4 環境中部署，SonicWall 建議啟用此選項。

3 選擇**啟用接聽路由器宣告**允許防火牆接收路由宣告。如果停用，介面篩選所有接收的路由宣告訊息，這可以透過封鎖接收惡意網路參數（例如首碼資訊或預設閘道）來增強安全性。預設情況下未勾選此選項。

> ⓘ **附註：**如果停用此選項，所有指派的自發 IPv6 位址會從此介面移除。

此選項在自動模式中無法使用。在自動模式中，始終啟用此選項。

選擇此選項後，「啟用無狀態位址自動設定」選項也變成可用。

- 勾選**啟用無狀態位址自動設定**允許將自發 IPv6 位址指派到此介面。如果取消勾選，所有指派的自發 IPv6 位址將從此介面移除。

  > ⓘ **附註：**如果停用此選項，所有指派的自發 IPv6 位址會從此介面移除。

  此選項在自動模式中無法使用。在自動模式中，始終啟用此選項。

4 輸入**重複地址偵測重新傳送**的數值指定在執行重複位址偵測 (DAD) 時向介面指派暫定位址前傳送的連續鄰居請求訊息數。最小值為 0，表示 DAD 未在介面上執行；最大值為 9，而預設值為 **1**。

與 IPv4 無故 ARP 類似，IPv6 節點使用鄰居請求訊息偵測相同連結上的重複的 IPv6 位址。在向 IPv6 介面指派暫定位址前，DAD 必須在任何單點傳送位址上執行（任意廣播位址除外）。

5 在**鄰居搜索的基本可存取時間 (秒)**中，輸入以秒為單位的基本值，以用於運算介面的隨機可連線時間值。最小值為 0，最大值為 9999，預設值為 **30**。

值 0 表示未指定參數，而在**網路 | 鄰居搜索**中使用全域設定。如果在此介面上啟用 RA，不過會使用**路由器宣告**標籤上**可連線時間**選項中的值。

6 選擇**啟用每個介面最大 NDP 大小**，對每個介面啟用最大的 NDP 大小。每個介面應有最大 NDP 大小，以防系統資源用盡。預設情況下已核取此選項。

在「每個介面最大 NDP 大小」欄位中輸入最大 NDP 大小。最小值是 64，最大值是 9999，而 WAN 介面的預設值是 **128**，其他則是 **1200**。

檢視 DHCPv6 通訊協定資訊

在 DHCpv6 模式中設定 IPv6 介面時，**通訊協定**標籤顯示附加 DHCPv6 資訊。

- **DHCPv6 一般資訊**
  - **DHCPv6 狀態：**如果介面設定是針對：
    - 無狀態模式，DHCPv6 狀態為無狀態。
    - 狀態模式，DHCPv6 狀態為**已啟用**或**已停用**。

      如果介面在狀態 DHCPv6 模式中，將滑鼠放在**註解**圖示上即可顯示介面的目前路由器宣告資訊。
  - **DHCPv6 伺服器**：DHCPv6 伺服器的 IPv6 位址。
  - **DHCPv6 DUID**：DUID (DHCP 唯一識別項) 或主機識別項。
- **透過 DHCPv6 獲得的狀態位址**：顯示任何獲得的狀態 IPv6 位址的資訊：
  - IAID (身分識別關聯識別項)
  - 類型
  - IPv6 位址
  - 租用過期
- **無狀態組態設定需要經由 DHCPv6**
  - **DNS 伺服器 1/2/3**：任何 DNS 伺服器的 IPv6 位址。

  您可以按下適當的按鈕更新、釋放或重新整理 DNS 伺服器。
- **經由 DHCPv6 取得委派的首碼**：顯示任何獲得的狀態 IPv6 位址的委派首碼的資訊：
  - IAID
  - 類型
  - IPv6 首碼
  - 首碼長度
  - 租用過期

  您可以按下適當的按鈕更新、釋放或重新整理首碼。

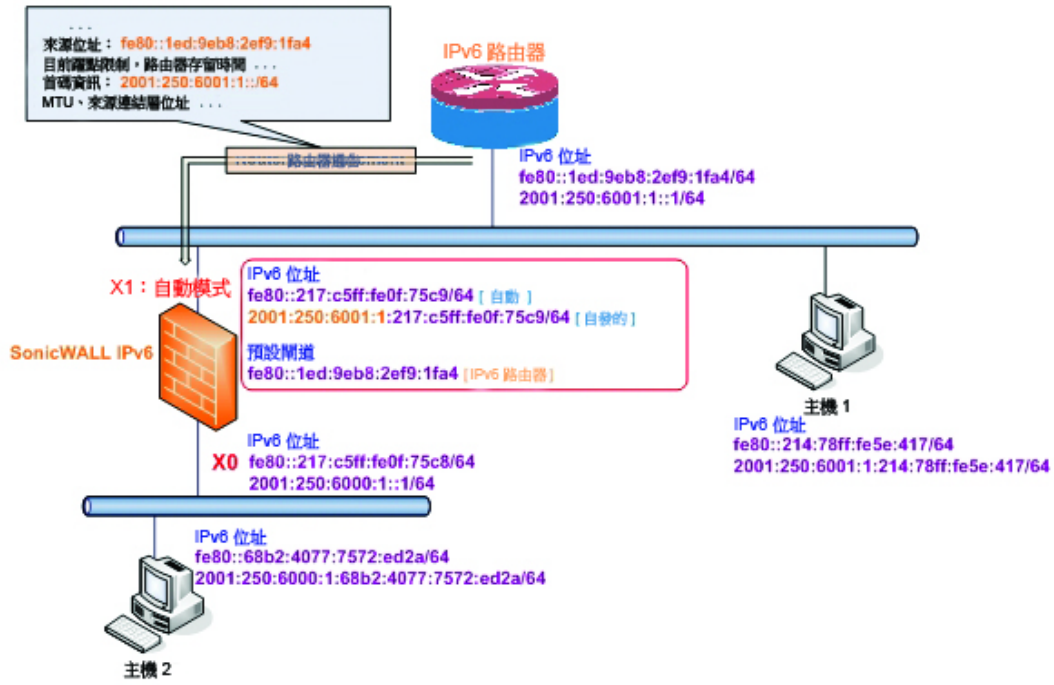
設定自動模式的介面

自動模式使用 IPv6 的無狀態位址自動設定指派 IPv6 位址。此模式不需要網路管理員的任何手動位址設定。安全設備會監聽網路並接收來自相鄰路由器的首碼資訊。IPv6 無狀態位址自動設定功能執行所有設定的詳細資料，例如 IPv6 位址指派，在發生位址衝突或存留間隔過期時刪除位址，以及根據收集自連結路由器的資訊選擇預設閘道。

附註：只能為 WAN 區域設定自動模式。出於安全考慮，LAN 區域介面上沒有自動模式。

IPv6 自動模式設定會顯示在自動模式中設定的 IPv6 樣本拓撲結構。

IPv6 自動模式設定



在這種模式下，可以指派兩種 IPv6 位址：

- 自動位址 - 介面預設連結 - 本機位址。這永遠不會逾時，且無法編輯或刪除。
- 自發位址 - 指派自無狀態位址自動設定。如果使用者不想等到有效存留時間過期，可以手動刪除位址。

若要設定自動模式的 IPv6 介面:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下頁面右上角的 **IPv6** 按鈕顯示 IPv6 位址。

3 按一下您要為其設定 IPv6 位址的介面的**設定**圖示。將顯示**編輯介面**對話方塊。

4 在 **IP 指派**下拉功能表中選擇**自動**。

5 另外，您可以選擇在**進階**標籤輸入**重複地址偵測重新傳送**的數值指定在執行重複位址偵測 (DAD) 時向介面指派暫定位址前傳送的連續鄰居請求訊息數。值 0 表示未在介面執行 DAD。

6 按一下**確定**。

PPPoE

IPv6 僅支援 PPPoE 用戶端模式。

設定 VLAN 子介面

在 IPv6 中設定 VLAN 子介面的程式與在 IPv4 中設定完全相同。詳細資料，請參閱第 260 頁「設定虛擬介面 (VLAN 子介面)」。

所有 VLAN 子介面在 IPv6 中設定之前，必須在 IPv4 中設定。

設定有線模式的介面

附註：NSA 2600 及更新裝置支援有線模式。

在 IPv6 中設定有線模式介面的程式與在 IPv4 中設定完全相同。詳細資料，請參閱第 267 頁「設定有線模式的介面」。

所有有線模式介面必須在 IPv4 中設定，無法在 IPv6 中編輯有線模式設定。在 IPv4 中啟用的任何功能（例如「連結狀態傳播」）將套用於 IPv6。

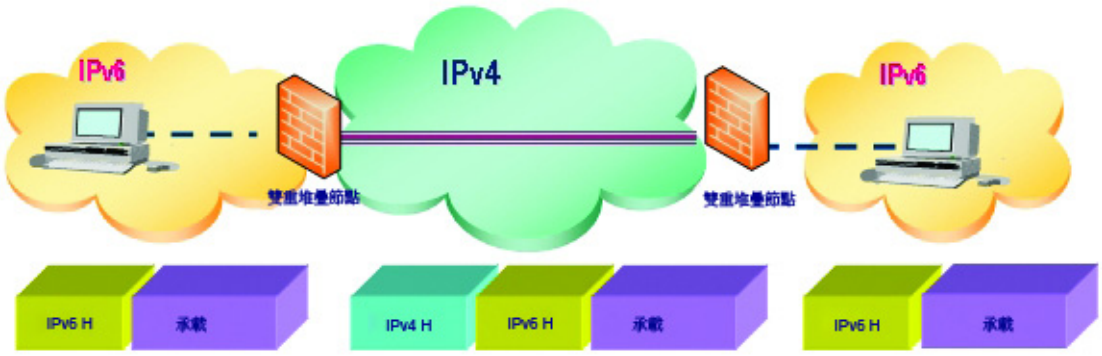
設定 IPv6 通道介面

本節說明如何以通道方式透過 IPv6 網路傳送 IPv4 封包和透過 IPv4 網路傳送 IPv6 封包。例如，為了透過 IPv4 網路傳送 IPv6 封包，會在通道的輸入側將 IPv6 封包封裝到 IPv4 封包中。在封裝的封包到達通道的輸出時，將解封 IPv4 封包。

通道可以是自動或手動設定。設定的通道按封裝節點上的設定資訊確定端點位址。自動通道根據嵌入式 IPv6 資料包的位址確定 IPv4 端點。IPv4 多點傳送通道透過鄰居發現機制確定端點。

IPv6 至 IPv4 通道介面描述了 IPv6 至 IPv4 通道。

IPv6 至 IPv4 通道介面



主題：

- 第 776 頁「設定 6 至 4 自動通道」
- 第 778 頁「設定用於非 2002 首碼存取的 6 至 4 轉接」
- 第 778 頁「設定手動 IPv6 通道」
- 第 779 頁「設定 GRE IPv6 通道」
- 第 779 頁「IPv6 首碼委派」
- 第 781 頁「6rd 通道介面」
- 第 782 頁「設定 ISATAP 通道」

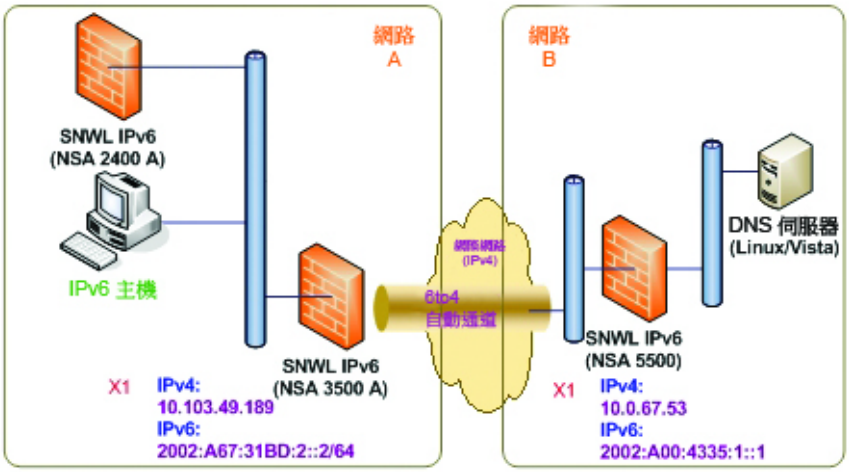
設定 6 至 4 自動通道

6 至 4 自動通道是自動通道：通道端點提取自封裝式 IPv6 資料包。無需手動設定。

6 至 4 通道使用形式為 2002:*tunnel-IPv4-address*::/48 的首碼透過 IPv4 對 IPv6 流量進行通道傳送（例如，如果通道的 IPv4 端點的位址為 a01:203，則 6 至 4 通道首碼為 2002:a01:203::1）。路由器向 IPv6 用戶端發佈 2002:*[IPv4]:xxxx*/64 形式的首碼。如需完整的資訊，請參見 RFC 3056。

6 至 4 自動通道拓撲結構顯示 6 至 4 自動通道拓撲結構的範例。

6 至 4 自動通道拓撲結構



在 IPv6 至 IPv4 通道介面中，客戶無需指定通道端點，但需要啟用 6 至 4 自動通道。擁有 2002 首碼的所有封包都傳送至通道，且通道的 IPv4 目的地將從目的地 IPv6 位址中提取。

6 至 4 通道易於設定和使用。使用者必須使用具有 2002 首碼的全域 IPv4 位址和 IPv6 位址。因此，總而言之，使用者只能存取擁有 2002 首碼的網路資源。

附註：只能在安全設備上設定一個 6 至 4 自動通道。

附註：VPN 通道介面自動建立了 IPv6 連結本機位址。.

若要在防火牆上設定 6 至 4 自動通道:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 您可以

- 按一下**新增介面**按鈕。
- 從**新增介面**下拉功能表中選擇**通道介面**。

將顯示**編輯介面**對話方塊。

3 選擇 6 至 4 通道介面的**區域**。這通常是 WAN 介面。

4 在**通道類型**下拉功能表中，選擇 **6to4 自動通道介面**。

5 在**名稱**欄位中指定名稱。預設情況下，將介面**名稱**設為 **6to4AutoTun**。

6 勾選**啟用 IPv6 6to4 通道**核取方塊。預設情況下，此核取方塊處於勾選狀態。

7 另外，您可以設定一個或多個**管理**登入通訊協定：**HTTPS**、**Ping** 或 **SNMP**。

附註：選擇 **HTTPS** 可自動啟用**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項。使用其他通訊協定時無法選取這個選項。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。

8 另外，您可以設定以下兩個**使用者登入**通訊協定或其中一項通訊協定：**HTTP** 或 **HTTPS**。

> **附註：**僅選擇 **HTTPS** 可自動啟用**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。如果您還選擇了 **HTTP**，則系統將取消選擇**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項，且您無法選擇此選項。

9 按一下**確定**。

設定用於非 2002 首碼存取的 6 至 4 轉接

預設情況下，6 至 4 自動通道只能存取擁有 2002 首碼的目的地。6 至 4 轉接功能可用於存取非 2002 首碼的目的地。

如何啟用 6 至 4 轉接:

1 導覽到**管理 | 系統安裝 | 網路 | 路由**。

2 按一下**新增**按鈕建立路由原則，透過 6 至 4 自動通道介面，傳送以 2003 首碼為目的地的所有流量:

可以向 6 至 4 自動通道介面新增此固定路由以啟用轉接功能，這樣就可以透過 6 至 4 通道存取具有非 2002: 首碼的 IPv6 目的地。

> **附註：**閘道必須是具有 2002: 首碼的 IPv6 位址。

設定手動 IPv6 通道

若要在防火牆上設定 6 至 4 通道:

1 導覽到**管理 | 系統安裝 | 網路 | 介面**。

2 按一下**新增介面**按鈕。將顯示**編輯介面**對話方塊。

3 選擇通道介面的**區域**。

4 在**通道類型**下拉功能表中，選擇 **IPv6 手動通道介面**。這是預設值。

5 輸入通道介面的**名稱**。

6 在**通道介面 IPv6 位址**欄位中輸入位址。此欄位的開頭已經是 **::**。

7 從**繫結到**下拉功能表中選擇通道繫結到的介面。預設值為 **X1**。

8 從**遠端 IPv4 位址**下拉功能表中，為通道端點選擇 IPv4 位址物件。

9 從**遠端 IPv6 位址**下拉功能表中，選擇 IPv6 位址物件，此物件可以是群組、範圍、網路或主機。

10 另外，您可以設定一個或多個**管理**登入通訊協定：**HTTPS**、**Ping** 或 **SNMP**。

> **附註：**選擇 **HTTPS** 可自動啟用**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。使用其他通訊協定時無法選取這個選項。

11 另外，您可以設定以下兩個**使用者登入**通訊協定或其中一項通訊協定：**HTTP** 或 **HTTPS**。

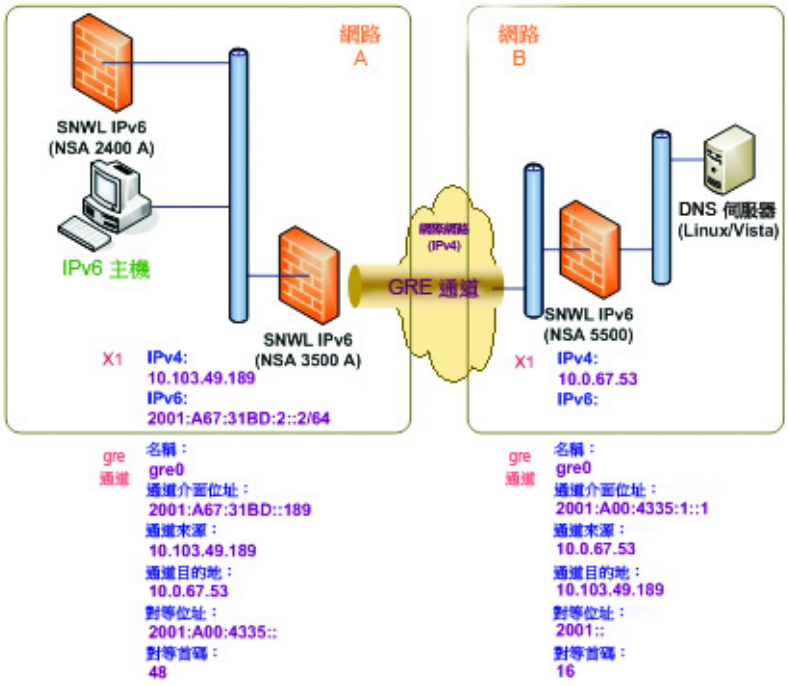
> **附註：**僅選擇 **HTTPS** 可自動啟用**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項。如需此選項的更多相關資訊，請參閱第 230 頁「HTTP/HTTPS 重新導向」。如果您還選擇了 **HTTP**，則系統將取消選擇**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項，且您無法選擇此選項。

12 按一下**確定**。

設定 GRE IPv6 通道

GRE 可用於透過 IPv4 或 IPv6 以通道方式傳送 IPv4 和 IPv6 流量。GRE 通道是固定通道，其中，兩個端點由手動指定。GRE IPv6 通道設定顯示 GRE IPv6 通道範例。

GRE IPv6 通道設定



GRE 通道的設定類似於手動通道，但選擇 **GRE 通道介面**作為**通道類型**。

IPv6 首碼委派

IPv6 首碼委派也稱為 DHCPv6 首碼委派 (DHCPv6-PD)，是 DHCPv6 的擴充。在 DHCPv6 中，由 DHCPv6 伺服器將位址指派到 IPv6 主機。在 DHCPv6-PD 中，由 DHCPv6-PD 伺服器將完整的 IPv6 子網路位址及其他參數指派到 DHCPv6-PD 用戶端。

在啟用 DHCPv6-PD 時，可以套用於附加到 WAN 區域的所有 DHCPv6 介面。DHCPv6-PD 是與 DHCPv6 共存的附加子網路設定模式。

IPv6 位址是 DHCPv6-PD 伺服器提供的首碼和 DHCPv6-PD 用戶端提供的尾碼的組合。首碼長度預設為 64 位元，但可以編輯。

防火牆啟動時，將自動建立稱為*來自 DHCPC6 代理的首碼*的預設位址物件群組。授權自上游介面的首碼是此群組的成員。

IPv6 首碼委派的設定在：

- 上游介面
- 一個或多個下游介面

當上游介面向 DHCPv6-PD 伺服器學習首碼委派後，SonicOS 計算 IPv6 位址首碼並將其套用於所有下游介面，下游介面將這些資訊發佈到網路分段的所有主機中。

本章節包含以下設定程式：

- 第 780 頁「在上游介面設定 IPv6 首碼委派」

- 第 780 頁「在下游介面上設定 IPv6 首碼委派」

重要：在網路中停用首碼委派之前，建議慣用的在上游介面釋放首碼委派。

在上游介面設定 IPv6 首碼委派

若要在上游介面設定 IPv6 首碼委派：

1 移至**管理 | 系統安裝 | 網路 | 介面**。

2 在**檢視 IP 版本**中，選擇 **IPv6**。

3 對於想要設定為上游介面的介面，按一下其**設定**欄中的**編輯**圖示。**編輯介面**對話顯示。

附註：區域一律為 **WAN**。

4 從 **IP 指派**功能表中，選擇 **DHCPv6**。

5 選擇**啟用 DHCPv6 首碼委派**選項。

6 從 **DHCPv6 模式**功能表中選擇**手動**。

7 若要查看設定的 DHCPv6 資訊，請按一下**通訊協定**標籤。

DHCPv6 一般資訊面板中顯示 **DHCPv6 DUID**。

狀態位址需要經由 DHCPv6 面板中顯示狀態 **IAID**。

經由 DHCPv6 取得委派的首碼面板中顯示授權 **IAID**。

8 按一下**更新**按鈕。其他欄的資訊也得以顯示。

在下游介面上設定 IPv6 首碼委派

若要在下游介面設定 IPv6 首碼委派：

1 移至**管理 | 系統安裝 | 網路 | 介面**。

2 選擇 **IPv6** 選項。

3 對於想要設定為下游介面的介面，按一下其**設定**欄中的**編輯**圖示。**編輯介面**對話顯示。

4 選擇**啟用路由器宣告**選項。

5 按一下**進階**標籤。

如果獲取了上游首碼，將顯示在 **IPv6 位址**面板中。

6 如果無法獲取上游首碼，則替代位址顯示在 **IPv6 位址**面板中。

7 按一下**新增位址**按鈕顯示**新增 IPv6 位址**對話方塊。

8 選擇**新增下游授權的 IPv6 位址**選項。

9 （可選）選擇**發佈固定 IPv6 位址的子網路首碼**選項。

10 按一下**路由器宣告**標籤。

11 選擇**啟用路由器宣告**選項。

如果在**一般**標籤下選擇了**發佈固定 IPv6 位址的子網路首碼**選項，首碼將列出在**首碼清單設定**面板中。

12 若要查看新 IPv6 PD 介面，請移至**管理 | 系統安裝 | 網路 | 路由**。

13 選擇 **IPv6** 選項。

顯示具有首碼委派的兩個新 IPv6 介面（上游和下游）。

6rd 通道介面

IPv6 快速部署 (6rd) 允許 IPv6 在 IPv4 網路中快速、輕鬆部署。6rd 使用服務供應商的現有 IPv6 位址首碼，以確保 6rd 執行網域僅限於服務供應商的網路，也受到服務供應商的直接控制。

6rd 通道介面是在 IPv4 網路中傳送 6rd 封裝式 IPv6 封包的虛擬介面。

附註：6rd 通道介面必須繫結到實體或虛擬介面。

部署 6rd 後，IPv6 服務等同於原生 IPv6。IPv6 位址與 IPv4 位址的 6rd 對應提供從 IPv6 首碼自動確定 IPv4 通道端點的方式，從而允許 6rd 的無狀態操作。

6rd 網域包含多個 6rd 使用者邊緣 (CE) 路由器和一個或多個 6rd 邊界轉接 (BR) 路由器。6rd 封裝的 IPv6 封包遵循服務供應商網路內的 IPv4 路由拓撲結構。

使用使用者邊緣路由器和邊界轉接路由器的典型 6rd 實作只需要一個 6rd 通道介面。服務於多個 6rd 網域的邊界轉接路由器可能具有多個 6rd 通道介面。但是，每個 6rd 網域只能有一個 6rd 通道介面。

IPv6 封包在進入或結束服務供應商的 6rd 網域時穿過邊界轉接。由於 6rd 無狀態，可以使用任何廣播方式將封包傳送至邊界轉接，其中，將來自單一來源的封包傳送到潛在接收器群組中的最近節點或傳送到全部由相同目的地位址識別的多個節點。

服務供應商可以在單個網域或多個網域中部署 6rd。6rd 網域只能有一個 6rd 首碼。不同的 6rd 網域必須使用不同的 6rd 首碼。

在**管理 | 系統安裝 | 網路 | 路由**的**路由原則**面板中，有 4 個用於 6rd 通道介面的預設路由原則。

有兩個設定模式：

- 手動
- DHCP

可以手動設定以下四個 6rd 參數，或如果您選擇 DHCP 作為設定模式，這些參數將由 DHCPv4 伺服器自動設定。

- IPv4 遮罩長度
- 6rd 首碼
- 6rd 首碼長度
- 6rd BR IPv4 位址

在 DHCP 模式中，從繫結的介面接收 6rd 參數。在手動模式中，6rd 參數必須手動設定。

設定 6rd 通道介面

6rd 通道介面的設定方式與其他 IPv6 通道介面相同。設定 6rd 通道介面需要繫結介面。

若要設定 6rd 通道介面：

1 移至**管理 | 系統安裝 | 網路 | 介面**。

2 在**檢視 IP 版本**中，選擇 **IPv6**。

3 在**介面設定**面板，按一下**新增介面**按鈕。

附註：只有在選擇 DHCP 作為設定模式時，才會顯示**通訊協定**標籤。

4 從**區域**下拉功能表中，選擇 **WAN**。

5 停用**介面類型**功能表。已核取**通道介面**，因為在步驟 3 中已經從**新增介面**功能表中進行選擇。

6 從**通道類型**功能表中選擇 **6rd 通道介面**。

7 在名稱框中，輸入通道介面的名稱，例如 **6rd 通道**。

8 在**通道介面 IPv6 位址**欄位中輸入通道介面的 IPv6 位址。例如 **2001::2**。

9 在**首碼長度**欄位中，輸入 IPv6 首碼的長度。例如，**64**。

10 從**繫結到**下拉功能表中，選擇所需的介面，例如 **X1**。

11 從**設定模式**下拉功能表中，選擇所需的模式：**手動**或 **DHCP**。

> **附註：**如果選擇**手動**作為**設定模式**，則執行步驟 12 至步驟 15。
> 如果選擇 **DHCP** 作為**設定模式**，則跳過步驟 12 至步驟 15。

12 在 **6rd 首碼**欄位中，輸入 6rd 首碼，例如 **2222:2222::**（僅**手動**模式）。

13 在 **6rd 首碼長度**欄位中，輸入 6rd 首碼的長度，例如 **32**（僅**手動**模式）。

14 在 **IPv4 遮罩長度**欄位中，輸入 IPv4 子網路遮罩的長度（僅**手動**模式）。

15 在 **BR IPv4 位址**欄位中，輸入 6rd 邊界轉接的 IPv4 位址（僅**手動**模式）。

16 （可選）在**註解**欄位中，輸入說明通道介面的註解。

17 選擇**自動新增預設路由**選項。

18 選擇所需的**管理**選項，或選擇所需的**使用者登入**選項。

如果選擇**手動**作為**設定模式**，6rd 通道介面設定就會顯示在**一般**標籤下。

如果選擇 **DHCP** 作為**設定模式**，6rd 通道介面設定就會顯示在**通訊協定**標籤下。

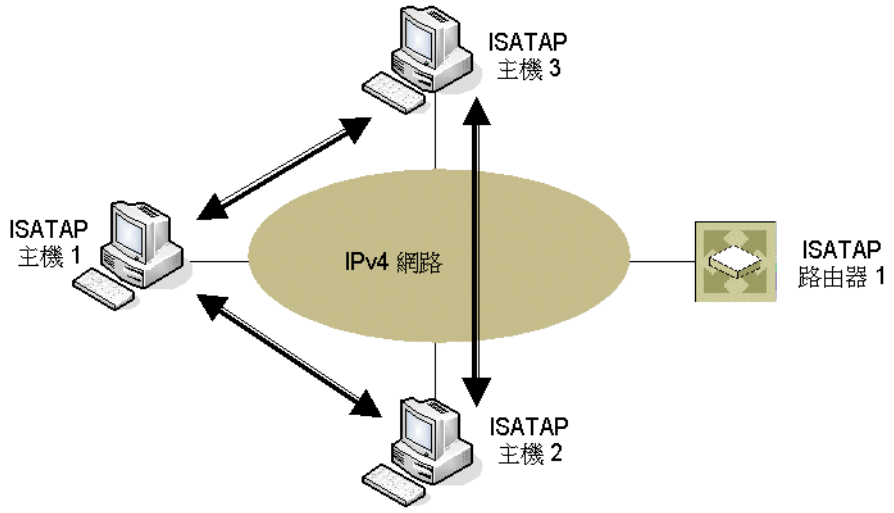
設定 ISATAP 通道

ISATAP（內部網站自動通道定址通訊協定）可用於透過只有 IPv4 的基礎結構提供 IPv6 連線。ISATAP 是透過 IPv4 網路連接雙堆疊 (IPv6/IPv4) 節點與其他雙堆疊節點或 IPv6 節點的簡單通道機制。ISATAP 將 IPv4 網路視為 IPv6 的連結層。

ISATAP 可在多個情節中用於提供 ISATAP 主機之間，和 ISATAP 主機與 IPv6 網路上主機之間的單點傳送連線。

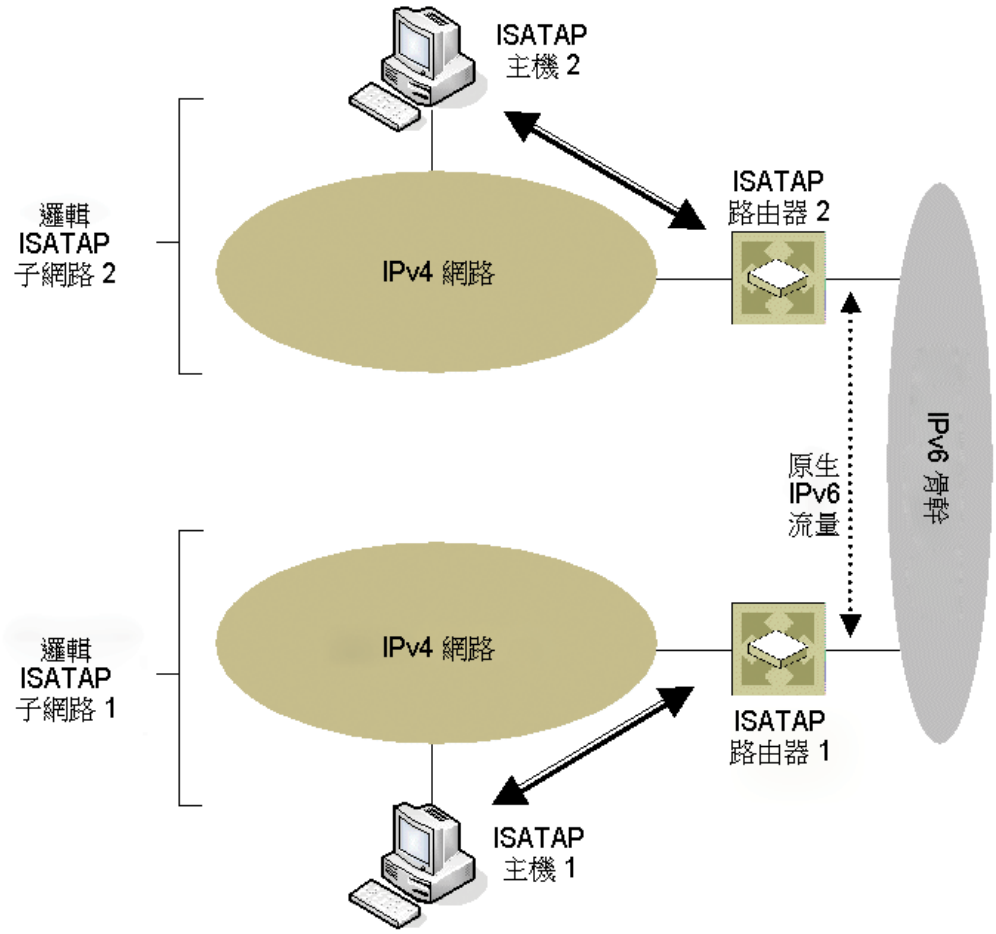
在 ISATAP 主機和相同邏輯 ISATAP 子網路之間傳送流量顯示在相同邏輯 ISATAP 子網路上的 ISATAP 主機之間傳送 ISATAP 流量：

在 ISATAP 主機和相同邏輯 ISATAP 子網路之間傳送流量



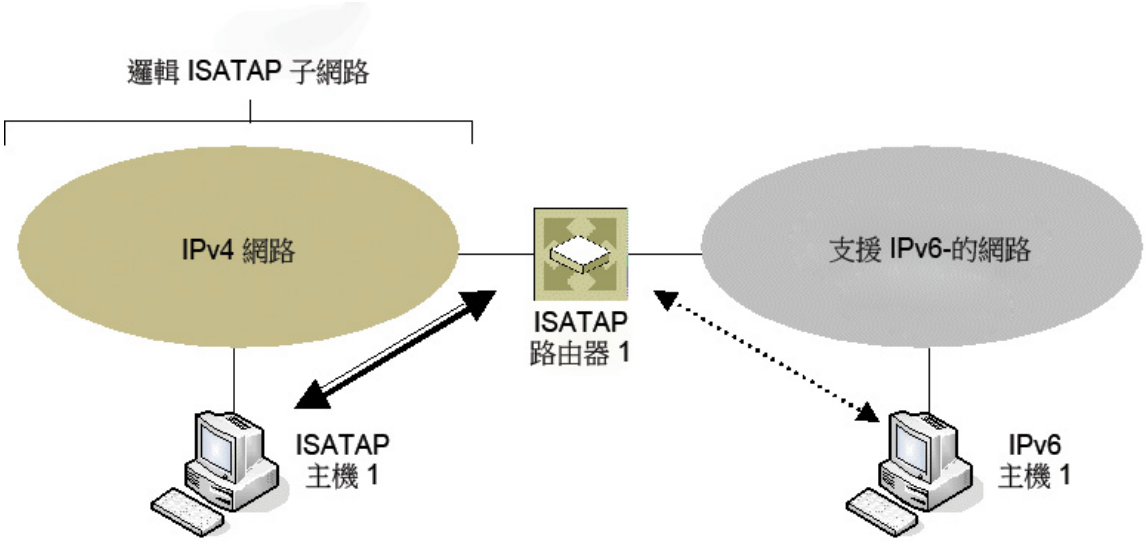
在 ISATAP 主機和不同 ISATAP 子網路之間傳送流量顯示在不同 ISATAP 子網路上的主機之間傳送 ISATAP 流量：

在 ISATAP 主機和不同 ISATAP 子網路之間傳送流量



在 ISATAP 主機與啟用 IPv6 的網路上的主機之間傳送封包顯示在 ISATAP 主機與啟用 IPv6 的網路上的主機之間傳送封包。

在 ISATAP 主機與啟用 IPv6 的網路上的主機之間傳送封包



在在 ISATAP 主機與啟用 IPv6 的網路上的主機之間傳送封包顯示的情節中，ISATAP 主機可以直接互相通信，無需透過 ISATAP 路由器或 IPv6 網路。這允許啟用 IPv6 的應用程式利用現有 IPv4 基礎結構的連線。

其他兩個情節需要 ISATAP 路由器的 IPv6 介面連接到 IPv6 網路，以支援在面向 ISATAP 介面的 IPv4 網路與 IPv6 介面之間的轉送。

需要在主機和路由器上實作和執行 ISATAP。Windows XP 和 Windows 7 平台上預設啟用雙堆疊節點支援。

SonicOS 中的 ISATAP 支援允許安全設備在面向 LAN 的介面上用作 ISATAP 路由器，並允許在 ISATAP 通道介面和連接到 IPv6 網路的 IPv6 介面之間轉送 IPv6 封包。

若要設定 ISATAP 通道:

1 在**管理 | 系統安裝 | 網路 | 介面**的**檢視 IP 版本**中，選擇 **IPv6**。

2 按一下**新增介面**按鈕。

3 在**一般**標籤中，為通道介面選擇**區域**。

4 在**通道類型**下拉清單中，選擇 **ISATAP 通道介面**。

5 輸入通道介面的**名稱**。

6 **繫結到 IPv4 位址** - 從下拉功能表選擇介面。ISATAP 通道使用繫結介面的 IPv4 位址作為 6over4 通道的 IPv4 終止位址。

7 **IPv6 子網路首碼** - 從下拉功能表選擇位址物件 (或選擇「建立新位址物件」)。IPv6 子網路首碼是 64 位元首碼，ISATAP 主機將之用於 ISATAP 位址自動設定。

8 **通道介面連結 MTU** - 介面連結的推薦 MTU。值 0 表示防火牆不發佈連結的 MTU。

9 在**註解**欄位中輸入任何可選的註解文字。此文字將顯示在**介面**表的**註解**欄中。

10 如果想要啟用透過此介面遠端管理防火牆，請選擇支援的管理通訊協定：**HTTPS**、**Ping** 或 **SNMP**。

11 如果想要允許擁有有限管理權限的選定使用者登入安全設備，請在**使用者登入**中選擇 **HTTP** 和/或 **HTTPS**。

此外，您可以在**管理 | 安全設定 | 防火牆設定 | 進階設定**中，指定 SonicOS 如何解決 ISATAP 主機查詢。如需指定進階防火牆設定的相關資訊，請參閱 *SonicOS 安全設定*。

使用 IPv6 存取 SonicWall 管理介面。

在安全設備上設定 IPv6 位址後，您可以在瀏覽器的 URL 欄位輸入安全設備的 IPv6，藉此存取 SonicWall 管理介面。

IPv6 網路設定

主題：

IPv6 DNS

IPv6 的 DNS 使用與 IPv4 相同的設定方法。按一下**管理 | 系統安裝 | 網路 | DNS** 左上角**檢視 IP 版本**選項按鈕中的 **IPv6** 選項。

位址物件

IPv6 位址物件或位址群組的新增方式與 IPv4 位址物件相同。如需設定位址物件的相關資訊，請參閱 *SonicOS 原則*。

附註：支援類型為主機、範圍和網路的位址物件。IPv6 主機目前不支援 MAC 和 FQDN 的動態位址物件。

IPv4 介面為每個介面定義了一對預設位址物件 (DAO) 和一個位址物件群組。IPv4 DAO 的基本規則是，每個 IPv4 位址對應於 2 個位址物件：介面 IP 和介面子網路。還有一些 AO 群組，分別用於區域介面 IP、區域子網路、所有介面 IP、所有介面管理 IP 等。

IPv6 介面為每個介面準備了相同的 DAO 集。由於可以將多個 IPv6 指派給一個介面，因而可以動態新增、編輯和刪除所有這些位址。因此，需要動態建立和刪除 IPv6 DAO。

為解決此問題，將不會為 IPv6 介面動態產生 DAO。將建立數量有限的介面 DAO，導致只能為其他需要參考介面 DAO 的模組提供有限支援。

基於原則的路由

在**管理 | 系統安裝 | 網路 | 路由**上選擇路由原則的 IPv6 位址物件和閘道，即可讓 IPv6 完全支援基於原則的路由。

下一代路由資訊通訊協定 (RIPng) 是用於 IPv6 的資訊路由通訊協定，它允許路由器通過基於 IPv6 的網路交換用於計算路由的資訊。

新增了選項按鈕用於在 RIP 和 RIPng 之間切換：

IPv6 NAT 原則

您可以在**管理 | 原則 | 規則 | NAT 原則**中，為 IPv6 或 NAT64 設定 NAT 原則。設定 IPv6 NAT 原則時，來源和目的地物件只能是 IPv6 位址物件，除非指定了 NAT64 的 IP 版本。如需更多設定 NAT 原則的相關資訊，請參閱 *SonicOS 原則*。

附註：目前不支援 IPv6 探查 NAT 原則。

NAT64 狀態偵測網路串流支援

狀態偵測網路串流 (通常包括應用程式層資料) 需要立即建立快取項目。根據封包篩選的規則表，這些快取項目通常是非法，但是因為應用程式層資料中的特定指示詞而允許 (例如，FTP 資料連線的輸入快取項目的新增)。

在 SonicOS 中，這些網路串流是從一般應用程式層通訊協定串流，像是 HTTPS 或 SNMP，以不同方式處理。這些狀態偵測網路串流包括 FTP、TFTP、H.323、MSN、Oracle、PPTP、RTSP 和 RealAudio。狀態偵測網路串流在用戶端和伺服器透過控制通道彼此通訊時，需要預期建立資料快取。

我們的系統支援 FTP (包括主動和被動模式) 和 NAT64 的 TFTP 通訊協定。

鄰居發現通訊協定

鄰居發現通訊協定 (NDP) 是一個新的郵件通訊協定，它作為 IPv6 的一部分建立，用於執行 IPv4 中的 ICMP 和 ARP 完成的各種任務。和 ARP 一樣，鄰居搜索將構建一個動態項目的快取，且管理員可以設定固定鄰居搜索項目。下表顯示類似傳統 IPv4 鄰居訊息的 IPv6 鄰居訊息和功能。

IPv4 與 IPv6 鄰居訊息

IPv4 鄰居訊息	IPv6 鄰居訊息
ARP 請求訊息	鄰居請求訊息
ARP 轉接訊息	鄰居宣告訊息
ARP 快取	鄰居快取
免費 ARP	重複位址偵測
路由器請求訊息（可選）	路由器請求（必需）
路由器宣告訊息（可選）	路由器宣告（必需）
重新導向封包	重新導向封包

使用固定 NDP 功能，可以在三層 IPv6 位址與二層 MAC 位址之間建立固定對應。

若要設定固定 NDP 項目，請執行以下步驟：

1. 導覽到**管理 | 系統安裝 | 網路 | 鄰居搜索**。
2. 按一下**新增**按鈕。
3. 在 **IP 位址**欄位中，輸入遠端裝置的 IPv6 位址。
4. 在**介面**下拉功能表中，選擇將作為項目的防火牆介面。
5. 在 **MAC 位址**欄位中，輸入遠端裝置的 MAC 位址。
6. 按一下**確定**。已新增了固定 NDP 項目。

   NDP 快取表顯示所有目前的 IPv6 鄰居。將顯示以下類型的鄰居：

   - REACHABLE - 已知可在 30 秒內連接到鄰居。

- STALE - 無法連接到鄰居，已在 1200 秒內將流量傳送至鄰居。
- STATIC - 將鄰居手動設定為固定鄰居。

DHCPv6 設定

在**管理 | 系統安裝 | 網路 | DNS** 的**檢視 IP 版本**選項按鈕中選擇 **IPv6** 選項後，就可以利用與 IPv4 相似的方式來設定 DHCPv6 伺服器。

IPv6 存取規則設定

IPv6 存取規則的設定方式與 IPv4 存取規則相同，但需要選擇 IPv6 位址物件，而不是 IPv4 位址物件。如需更多防火牆存取規則的相關資訊，請參閱 *SonicOS 原則*。

在新增 IPv6 存取規則時，來源和目的地只能是 IPv6 位址物件。

IPv6 進階防火牆設定

您可以在**管理 | 安全設定 | 防火牆設定 | 進階設定**中指定 IPv6 的進階防火牆設定，包括封包限制和流量限制。如需指定進階防火牆設定的相關資訊，請參閱 *SonicOS 安全設定*。

IPv6 IPSec VPN 設定

在**管理 | 連線 | VPN | 設定**左上角的**檢視 IP 版本**選項按鈕中選擇 **IPv6** 選項後，就可以利用與 IPv4 VPN 相似的方式，為 IPv6 設定 IPSec VPN。如需設定 VPN 的相關資訊，請參閱 *SonicOS 連線能力*。

IPv6 目前不支援某些 VPN 功能，包括：

- 支援 IKEv2，但目前不支援 IKE
- 不支援 GroupVPN
- 不支援 VPN 上的 DHCP。

在設定 IPv6 VPN 原則時，對話方塊的**一般**部分中，必須使用 IPv6 位址來設定閘道。不支援 FQDN。在設定 IKE 身分驗證時，IPV6 位址可用於本機和對等 IKE ID。

在 VPN 原則的**網路**部分中，則必須為**本機網路**和**遠端網路**選擇 IPV6 位址物件 (或僅包含 IPv6 位址物件的位址群組)。

不支援 DHCP Over VPN，因此受防護網路的 DHCP 選項無法使用。

本機網路的**任何位址**選項和**遠端網路**的 **Tunnel All** 選項已移除。選擇全零 IPv6 網路位址物件可實現相同的功能和行為。

在**建議**部分中，Pv6 和 IPv4 的設定完全相同，不過 IPv6 僅支援 **IKEv2 模式**。

在**進階**部分中，您只能為 IPv6 VPN 原則指定**啟用保持運作**和 **IKEv2 設定**。

附註：由於介面可以擁有多個 IPv6 位址，所以有時通道的本機位址可能定期發生變化。如果使用者需要一致的 IP 位址，則將 VPN 原則設定為繫結到介面，而不是繫結到區域，並手動指定位址。位址必須是此介面的一個 IPv6 位址。

IPv6 的 SSL VPN 設定

SonicOS 支援擁有 IPv6 位址的使用者使用 NetExtender 連接。在**管理 | 連線 | SSL VPN | 用戶端設定**中，請先設定傳統的 IPv6 IP 位址集區，然後再設定 IPv6 IP 集區。每個用戶端將指派兩個內部位址：一個 IPv4 和一個 IPv6。如需設定 SSL VPN 的相關資訊，請參閱 *SonicOS 連線能力*。備忘錄: 連線能力

您可以在**管理 | 連線 | SSL VPN | 用戶端設定**的**編輯裝置設定檔**對話方塊中，為所有位址物件 (包括所有預先設定的 IPv6 位址物件在內) 選取用戶端路由。

附註：支援 IPv6 FQDN。

IPv6 視覺化

App Flow 報告和即時監控的 IPv6 視覺化功能進一步擴充了 IPv4 視覺化功能，能夠即時監控介面/應用程式速率，並且為管理介面中的工作階段提供能見度。您可以查看員工正在存取哪些網站、他們的網路中正在使用哪些應用程式和服務及其使用程度，進而監督組織對內與對外傳送的內容。如需這些視覺化工具的更多相關資訊，請分別參閱 *SonicOS 調查*和 *SonicOS 監控*部分。

IPv6 視覺化功能限制

IPv6 的視覺化具有以下功能限制:

- 不支援 IPv6 URL 評等，因為 CFS 不支援 IPv6 的所有方面。
- 不支援 IPv6 國家或地區資訊。
- 不支援 IPv6 外部報告。

設定 IPv6 視覺化

IPv6 和 IPv4 的 App Flow 報告和即時監控視覺化的設定相同。如需這些視覺化工具的更多相關資訊，請分別參閱 *SonicOS 調查*和 *SonicOS 監控*部分。

IPv6 高可用性監控

IPv6 高可用性 (HA) 監視作為 IPv4 中 HA 監控的擴充程式實作。在設定 IPv6 的 HA 監控後，可以從 IPv6 監視位址管理主要和備用裝置，且 IPv6 探查可以偵測 HA 對的網路狀態。

您可以在**管理 | 系統安裝 | 高可用性 | 監控設定**上切換使用 IPv6 和 IPv4 檢視，即可輕鬆設定兩種 IP 版本。檢閱者問題: 該如何設定 HA 監控？

主題：

- 第 789 頁「IPv6 高可用性監控功能限制」
- 第 789 頁「IPv6 高可用性探查」
- 第 789 頁「設定 IPv6 高可用性監控」

IPv6 高可用性監控功能限制

IPv6 HA 監控的功能限制如下:

- 不能在 IPv6 HA 監控設定頁面中變更實體/連接監控屬性。在 IPv4 HA 監控設定頁面設定屬性。
- 不能在 IPv6 HA 監控設定頁面中「覆寫虛擬 MAC」屬性。在 IPv4 HA 監控設定頁面設定屬性。
- 無法同時對 IPv4 和 IPv6 啟用 HA 探查。也就是說，如果啟用了 IPv4 探查，必須停用 IPv6 探查，反之亦然。

IPv6 高可用性探查

定期從主要和備用裝置發出 ICMPv6 封包以探查 IPv6 位址，還會監視來自受探查的 IPv6 位址的回應。如果活動安全設備無法到達探查的 IPv6 位址，但閒置的安全設備可以，則備用的安全設備具有更好的網路狀態和容錯移轉動作。

IPv6 HA 探查中使用 IPv6 位址、ICMPv6 回顯請求和 ICMPv6 迴響回應。IPv4 和 IPv6 中用於判斷主要和備用裝置的網路狀態的邏輯相同。

設定 IPv6 高可用性監控

IPv6 HA 監控設定頁面繼承自 IPv4，所以設定程式幾乎完全相同。只需選擇 IPv6 並參閱第 761 頁「IPv6」瞭解詳細設定資訊即可。

在設定 IPv6 HA 監控時請考慮以下因素：

- **實體/連接監控**和**虛擬 MAC** 無法使用是因為這兩者具有第二層屬性。也就是說，IPv4 和 IPv6 皆使用這些屬性，因此您必須在 IPv4 監控頁面進行設定。
- 主要/備份 IPv6 位址必須位於介面所屬的子網路，且不能與主要/備份安全設備的全域 IP 或連結本機 IP 相同。
- 如果將主要/備用監視 IP 設為（非 ::），就不能是相同的。
- 如果啟用了**管理**，就必須指定主要/備用監視 IP (即 ::)。
- 如果啟用了探查核取方塊，則探查 IP 不能為未指定。

IPv6 診斷和監視

SonicOS 完整補充了 IPv6 診斷工具，包括：

- 第 789 頁「封包監控」
- 第 790 頁「IPv6 Ping」
- 第 790 頁「IPv6 DNS 名稱查詢和反向名稱解析」

封包監控

調查 | 工具 | 封包監控完全支援 IPv6。此外，IPv6 關鍵字可用於篩選封包擷取。如需更多封包監控的相關資訊，請參閱 *SonicOS 調查*。

IPv6 Ping

在 Ping 一個網域名稱時，這項工具會使用系統傳回的第一個 IP 位址，並顯示實際的 Ping 位址。如果同時返回 IPv4 和 IPv6 位址，安全設備預設 Ping IPv4 位址。這項 Ping 工具包括 **IPv6 網路優先**選項，啟用了這個選項時，安全設備就會 Ping IPv6 位址。如需更多 IPv6 Ping 的相關資訊，請參閱 *SonicOS 調查*。

IPv6 DNS 名稱查詢和反向名稱解析

執行 IPv6 DNS 名稱查詢或 IPv6 反向名稱解析時，必須輸入 DNS 伺服器位址。可以使用 IPv6 或 IPv4 位址。如需這些工具的更多相關資訊，請參閱 *SonicOS 調查*。

C

BGP 進階路由

BGP 進階路由

本附錄概述 SonicWall 的邊界閘道通訊協定 (BGP) 實作、BGP 的執行方式，以及如何針對您的網路設定 BGP。

附註：購買 SonicOS 擴充授權後，TZ400 系列、TZ500 系列和 TZ600 裝置支援 BGP。TZ300 系列或 SOHO 無線裝置不支援 BGP。

主題：

關於 BGP

主題：

什麼是 BGP？

BGP 用於在自發系統 (AS) 之間交流路由資訊的大型路由通訊協定。這些自發系統是定義明確、單獨管理的網路網域。BGP 支援允許 SonicWall 安全裝置替代網路自發系統使用的傳統 BGP 路由器。BGP 的目前 SonicWall 實作最適用於「單供應商/單主目錄」環境，在這種環境下，網路使用一個 ISP 作為網際網路供應商，且與此供應商採用單一連接。SonicWall BGP 還可以支援「單供應商/單主目錄」環境，其中，網路使用單個 ISP，但擁有連至供應商的少量單獨路由。您可以在 SonicOS 管理介面的**網路 | 路由**頁面啟用 BGP，然後再透過 SonicOS 命令行介面 (CLI; 請參閱 *SonicOS CLI 參考指南*) 進行完整設定。

請參考以下的 BGP 授權要求表格瞭解 BGP 授權要求。

BGP 授權要求

平台	需要附加授權
SM 9600	無，已包含 BGP
SM 9400	無，已包含 BGP
SM 9200	無，已包含 BGP
NSA 6600	無，已包含 BGP
NSA 5600	無，已包含 BGP
NSA 4600	無，已包含 BGP
NSA 3600	SonicOS 擴充 01-SSC-7091
NSA 2650	SonicOS 擴充授權
NSA 2600	SonicOS 擴充授權
TZ600	SonicOS 擴充授權
TZ500/TZ500 W	SonicOS 擴充授權
TZ400/TZ400 W	SonicOS 擴充授權
TZ300/TZ300 W	N/A
SOHO W	N/A

附註：可以在 www.mysonicwall.com 購買授權。

背景資訊

路由通訊協定不僅是透過網路傳送的封包，還包含各路由器和路由器群組用於發現、組織和交流網路拓撲結構的所有機制。路由通訊協定使用取決於指定的各通訊協定參與者的分布式演算法，且在網路網域內的路由器隨著網路節點變更狀態而動態變化時尤為有用。

路由通訊協定通常與兩個資料庫交互：

- **路由資訊庫 (RIB)** - 用於儲存路由通訊協定本身所需的全部路由資訊。
- **轉送資訊庫 (FIB)** - 用於實際的封包轉送。

從 RIB 選擇的最佳路由用於填充 FIB。RIB 和 FIB 都隨著各路由通訊協定接收路由更新或裝置的連線變更而動態變化。

有兩個基本路由通訊協定類別：

- **內部閘道通訊協定 (IGP)** - 內部閘道通訊協定是用於在 AS 內部的網路內進行路由通信的路由通訊協定。有兩代 IGP。第一代由距離向量通訊協定組成。第二代由連結狀態通訊協定組成。距離向量通訊協定相對簡單，但在擴充到大量路由器時會出現問題。連結狀態通訊協定更為複雜，也具有

更好的擴充能力。現有的距離向量通訊協定有內部閘道路由通訊協定 (IGRP)、增強內部閘道路由通訊協定 (EIGRP)、路由資訊通訊協定 (RIP) 和 RIPv2 （增強版 RIP）。IGRP 和 EIGRP 是專有的 Cisco 通訊協定。目前使用的連結狀態通訊協定有先開啟最短的路徑 (OSPF) 通訊協定和較少使用的中間系統到中間系統 (IS-IS) 通訊協定。

SonicOS 支援 OSPFv2 和 RIPv1/v2 通訊協定，這是兩個最常用的路由內部閘道通訊協定，允許客戶在其 IGP 網路中使用我們的產品，並避免配備單獨的傳統路由器產生附加成本。

- **外部閘道通訊協定 (EGP)** - 標準的普適型外部閘道通訊協定是 BGP（更準確地說是 BGP4）。BGP 是用於在稱為自發系統 (AS) 的定義明確網路網域之間進行路由資訊和原則通信的大型路由通訊協定。自發系統是獨立於其他自發系統的單獨管理網路網域。BGP 用於在自發系統之間傳送路由和路由原則。ISP 通常使用 BGP 與其客戶及其他 ISP 傳送路由和路由原則。

  給每個自發系統都指派了 16 位元編號。和 IP 位址一樣，AS 編號也可以是公用或私人的。公用 AS 編號是有限的資源，會基於很多因素的考慮提供。有多重主目錄至兩個或多個 ISP 的大型網路的 ISP 客戶通常具備公用 AS，較小型客戶則具備由其 ISP 供應商管理的私人 AS。

  隨著我們的產品為支援企業級需求而不斷發展，有些客戶可能想要將我們的產品套用於 AS 以替代傳統的 BGP 路由器。

自發系統

給每個自發系統都指派了 16 位元編號。和 IP 位址一樣，AS 編號也可以是公用或私人的。公用 AS 編號是有限的資源，會基於很多因素的考慮提供。有多重主目錄至兩個或多個 ISP 的大型網路的 ISP 客戶通常具備公用 AS，較小型客戶則具備由其 ISP 供應商管理的私人 AS。

BGP 拓撲結構的類型

BGP 是很靈活、複雜的路由通訊協定。因此，BGP 路由器可融入多種拓撲結構設定中，例如網際網路核心路由器、中間 ISP 路由器、ISP 客戶前端裝置 (CPE) 或小型私人 BGP 網路中的路由器。不同拓撲結構所需的 BGP 路由數相差懸殊，核心路由器需要大於 300,000 個 BGP 路由，而使用單一 ISP 和為 AS 之外的所有目的地使用預設路由則不需要 BGP 路由。通常要求 ISP 客戶從其邊緣路由器 (CPE) 至 ISP 執行 BGP，而不論他們從 ISP 接收的路由數。這允許 ISP 客戶控制使用哪些網路向外界發佈。人們通常擔心客戶發佈一個自己並不擁有的網路或網路組，會有黑洞網際網路流量透過這些網路。實際上，ISP 供應商小心地篩選來自客戶的無效宣告（BGP 的優勢之一），所以以上擔心並無必要。

有三種規模的 BGP 網路：

- **單供應商/單主目錄** - 網路從單一 ISP（單一供應商）接收單一路由（單主目錄）。ISP 客戶從其 ISP 接收的路由數取決於其 AS 的性質。僅使用一個 ISP 作為網際網路供應商且此供應商只有單一連接（單供應商/單主目錄）的 ISP 客戶無需接收任何路由，將目的地在 AS 以外的所有流量移至其 ISP。這些客戶仍可以將其網路內的部分或全部內容發佈給 ISP。
- **單供應商/多重主目錄** - 網路從單一 ISP（單一供應商）接收多個路由（多重主目錄）。使用單個 ISP，但與其 ISP 有多個連接的 ISP 客戶只能在各 ISP 閘道接收預設路由 (0.0.0.0/0)。如果某 ISP 連接中斷，將撤回從中斷的 CPE 路由器向內部路由器傳送的預設路由，網際網路流量則流向連線至 ISP 的 CPE 路由器。客戶的內部網路也將在各 CPE 路由器閘道發佈至 ISP，並在與客戶的指定連接中斷時允許 ISP 使用替代路徑。
- **多供應商/多重主目錄** - 使用多個 ISP，且各 ISP 有一個或多個單獨閘道路由器的 ISP 客戶。在這種情況下，客戶的 AS 必須是公用 AS，也可能是中轉 AS 或非中轉 AS。中轉 AS 接收和轉送來自 ISP 的流量，此流量去往可透過其他 ISP 連接的網路（流量的目的地不在客戶的 AS 內）。非中轉 AS 應該只接收去往 AS 的流量，丟棄所有其他流量。中轉 AS 中的 BGP 路由器通常接收各 ISP 的完整 BGP 路由表的一大部分（在大多數情況下是全部）。

經由 VPN 通道介面的 BGP

BGP 介面支援已編號和未編號的通道介面。可設定 BGP 和未編號的通道介面的所有平台，皆支援這項功能。

為什麼使用 BGP？

- 即使您並非處在網際網路上的大型網路中，BGP 也可以作為多宿主、負載均衡和冗餘用例的標準：
  - **單供應商/單主目錄** - 不常用於 BGP，但仍可用於將網路發佈到 ISP。單主目錄網路不符合用於 RIR 中公用 AS 的條件。
  - **單供應商/多重主目錄** - 按照 RFC2270 使用單一私人 AS（64512 至 65535）的推薦，經常選用，可以發揮 BGP 的優勢，同時儲存公用 ASN。
  - **多供應商/多重主目錄** - 高度冗餘，通常用於各 ISP 的專用路由器。需要公用 ASN。大記憶體佔用
- 路由匯總實現可擴充性。

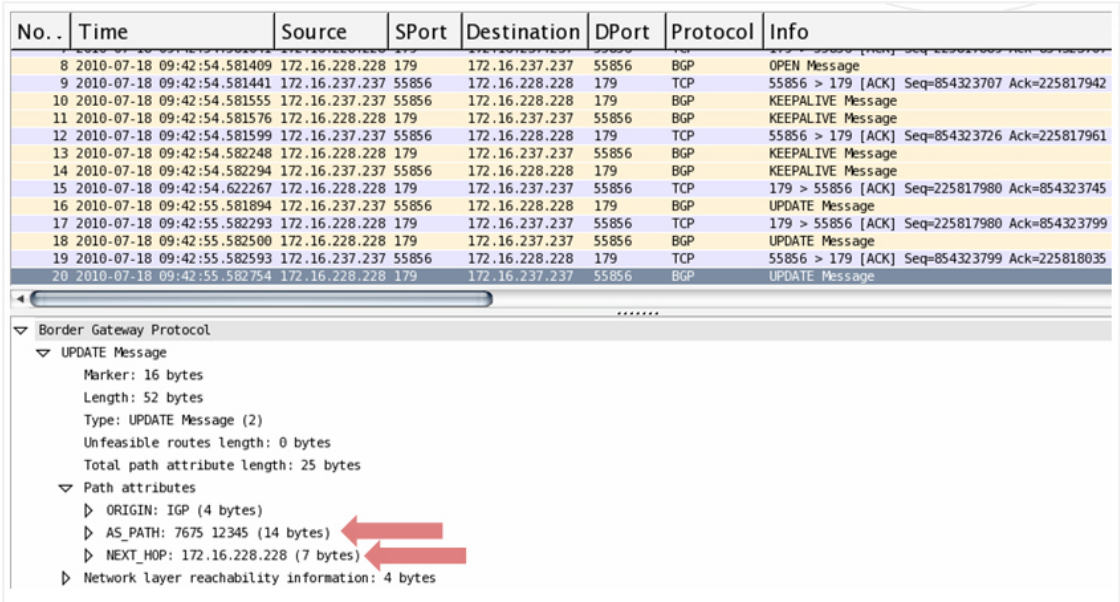
BGP 的工作方式

BGP 使用 TCP 連接埠 179 進行通信。將 BGP 視為一種路徑向量通訊協定，包含目的地的端對端路徑描述。BGP 鄰居可以是內部 (iBGP) 或外部 (eBGP) 的：

- **iBGP** - 鄰居位於相同 AS 內。
- **eBGP** - 鄰居位於不同 AS 中。

路徑在標籤為各種路徑屬性的更新訊息中發佈。AS_PATH 和 NEXT_HOP 是描述 BGP 更新訊息中路由路徑的兩個最重要屬性。

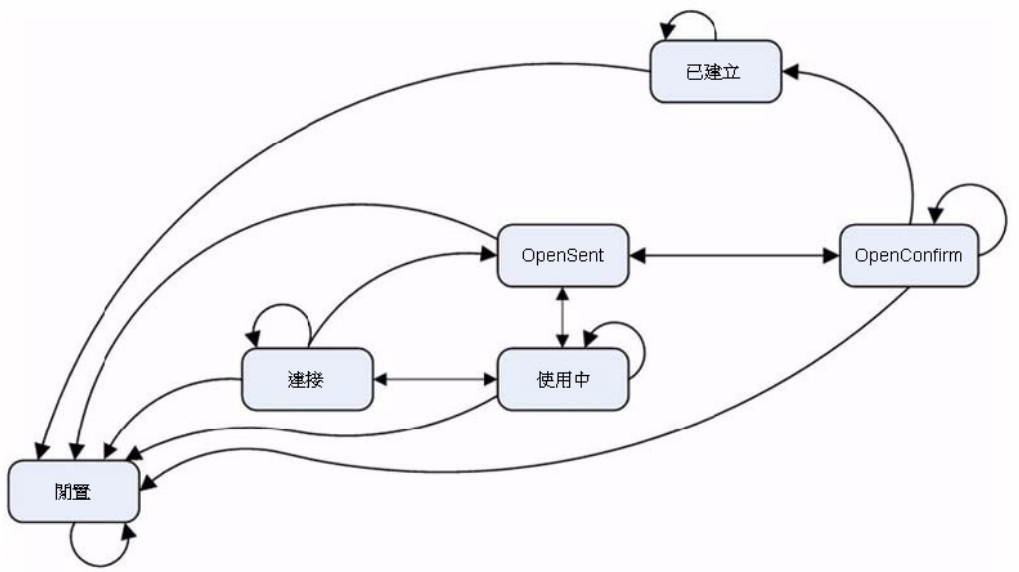
- **AS_PATH**：表示路由通信往來的 AS。在下例中，AS_PATH 來自 AS 7675，去往 AS 12345。對於內部 BGP，AS_PATH 為來源和目的地指定相同的 AS。
- **NEXT_HOP**：表示路徑前往的下一路由器的 IP 位址。穿過 AS 邊界發佈的路徑繼承了邊界路由器的 NEXT_HOP 位址。BGP 依賴內部路由通訊協定連通 NEXT_HOP 位址。



BGP 有限狀態機

用於定義 BGP 的 RFC 1771 描述了 BGP 與以下狀態機相關的工作。下圖後面的表格提供了有關各種狀態的附加資訊。

BGP 有限狀態機



BGP 有限狀態說明

狀態	說明
閒置	在建立新 BGP 工作階段或重設現有工作階段後，等待「啟動」事件。在發生錯誤事件時，恢復到「閒置」狀態。在「啟動」事件後，BGP 啟動，重設連接重試計時器，啟動 TCP 傳送連接和監聽連接
連接	TCP 層連接後，轉換為「已傳送開啟訊息」狀態，然後傳送「開啟」訊息。如果沒有 TCP，轉換為「使用中」。如果連接重試計時器過期，重設計時器，並啟動傳送連接。否則，轉換為「閒置」狀態。
使用中	嘗試與對等項建立 TCP 連接。如連接成功，轉換為「已傳送開啟訊息」狀態，然後傳送「開啟」訊息。如果連接嘗試過期，重新啟動計時器，然後恢復到「連接」狀態。還會主動監聽其他對等項的連接。在發生其他事件時，返回到「閒置」狀態。 活動狀態不穩表示有 TCP 傳送問題，例如 TCP 重新傳送或未連接對等項。
已傳送開啟訊息	等待來自對等項的「開啟」訊息。驗證接收情況。如驗證失敗，傳送「通知」並進入「閒置」狀態。如驗證成功，傳送「保持活動」並重設保持活動計時器。交涉保持時間，較小值取勝。如較小值為零，保持計時器和保持活動計時器不會重新啟動。
已確認開啟訊息	等待「保持活動」或「通知」。如果收到「保持活動」訊息，則轉換為「已建立」狀態。如果收到「更新」或「保持活動」訊息，重新啟動保持計時器（除非交涉保持時間為零）。如果收到「通知」，則轉換為「閒置」狀態。 傳送定期「保持活動」訊息。如果 TCP 層中斷，則轉換為「閒置」狀態。如果發生錯誤，則傳送含錯誤代碼的「通知」，並轉換為「閒置」狀態。
已建立	工作階段開啟，與對等項交換更新資訊。如果收到「通知」，則轉換為「閒置」狀態。檢查更新資訊有無錯誤。發生錯誤時，會傳送「通知」，並轉換為「閒置」狀態。保持時間過期時，中斷 TCP。

BGP 訊息

BGP 通信包含以下幾個訊息：

- **開啟** - 在建立 TCP 工作階段後，BGP 對等項之間的第一條訊息。包含建立對等工作階段的必需資訊，例如 ASN、保持時間以及多產品擴充和路由重新整理等功能。
- **更新** - 這些訊息包含路徑資訊，例如路由宣佈或撤回。
- **保持連接** - 有關保持 TCP 層活動和發佈活動連接的定期訊息。
- **通知** - 有關終止 BGP 工作階段的請求。包含錯誤代碼「cease」的非嚴重通知。子代碼提供更多詳細資料，如通知子代碼表格中所示：

通知子代碼

子代碼	說明
1 - 已達到的最大首碼數	已超過設定的「鄰居最大首碼」值
2 - 管理關閉	出於管理目的關閉工作階段
3 - 對等項未設定	已移除對等設定
4 - 管理重設	出於管理目的重設工作階段
5 - 已拒絕連接	BGP 工作階段的拒絕（有時是臨時的）
6 - 其他設定變更	出於某種原因管理重設工作階段

- **路由重新整理** - 用於對等項重新傳送其路由的請求。

BGP 屬性

BGP 更新訊息可以包含如 BGP 更新訊息屬性表格所示的屬性：

BGP 更新訊息屬性

值	代碼
1	ORIGIN
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF
6	ATOMIC_AGGREGATE
7	AGGREGATOR
8	COMMUNITY
9	ORIGINATOR_ID
10	CLUSTER_LIST
11	DPA
12	ADVERTISER（歷史記錄）
13	RCID_PATH / CLUSTER_ID（歷史記錄）
14	MP_REACH_NLRI
15	MP_UNREACH_NLRI
16	EXTENDED COMMUNITIES

BGP 更新訊息屬性

值	代碼
17	AS4_PATH
18	AS4_AGGREGATOR
19	SAFI 指定屬性 (SSA)（已棄用）
20	連接器屬性（已棄用）
21	AS_PATHLIMIT（已棄用）
22	PMSI_TUNNEL
23	通道封裝屬性
24	流量工程
25	IPv6 位址指定擴充團體
26	AIGP（臨時 - 2011 年 2 月 23 日過期）
27-254	未指派的
255	保留用於開發

如需 BGP 屬性的更多資訊，請參見：http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xml

BGP 術語

ARD	自發路由網域 - 擁有共用管理路由原則的網路/路由器的集合。
AS	自發系統 - 指派有識別號的 ARD，通常在邊界路由器執行 BGP4。
BGP4	邊界閘道通訊協定 4: 最普遍的 EGP。
CIDR	無分類的網域間路由，允許透過路由組的高效路由宣告。
CPE	客戶前端裝置 - 用於在客戶網路與 ISP 交互的裝置。
EGP	外部閘道通訊協定 - 用於在自發系統之間進行路由資訊通訊的任何通訊協定（通常是 BGP4）。
完整路由	完整的全域 BGP 路由表。
FIB	轉送資訊庫 - 用於查找輸出介面和轉送封包時的下一躍點的現有路由表。
視窗*	視窗 (LG) 伺服器是執行 LG 伺服器的組織中路由器的唯讀檢視。通常，可公用存取的視窗伺服器由 ISP 或 NOC 執行。
多重主目錄	與一個或多個 ISP 有多個連接的 ISP 客戶。
多供應商	使用多個 ISP 連接網際網路的 ISP 客戶。
NSM	網路服務模組 - 用於聚集介面至 FIB 和 RIB 的 ZebOS 元件。單獨的路由通訊協定守護程式與所有 RIB 更新的 NSM 交互。NSM 使用來自 RIB 的最佳路由資訊獨立更新 FIB。
部分路由	完整 BGP 路由表的子集，通常針對於作為 ISP 網域一部分的目的地。
RIB	路由資訊庫 - NSM 擁有的執行時資料庫，用於儲存路由通訊協定收集和使用的所有路由資訊。

注意

比例	目前，SonicOS 支援 512 至 2,048 個基於原則的路由 (PBR)。這對於完全甚或部分路由表是不夠的。RIB 中存在的路由數可能大於 PBR（是 FIB）中安裝的數目。當透過路由通訊協定收到多個競爭路由時，會發生這種情況。在 RIB 包含去往指定網路目的地的多個競爭路由時，只能選擇一個路由安裝到 FIB 中。 目前，我們的實作最適合於單供應商/單主目錄客戶。如果從 ISP 收到預設路由，或客戶收到很少量的 ISP 指定路由，單供應商/多重主目錄也很適用。第二種情況允許內部路由器採用最優路徑到達 AS 外部的目的地，但仍處於 ISP 網路網域內（名稱為部分路由）。
負載平衡	目前 SonicOS 或 Zebos 中沒有多路徑支援（「最多路徑」功能）。這樣就封鎖了負載均衡，且不拆分網路。
回送	目前沒有回送介面支援。
NAT	BGP 適用於路由。但不能與 NAT 良好共存。
非對稱路徑	狀態安全設備目前不處理非對稱路徑，尤其是穿越多個安全設備的情況。

設定 BGP

主題：

BGP 的 IPSec 設定

BGP 傳送封包暢通無阻。因此為了增強安全性，SonicWall 推薦設定 IPSec 通道用於 BGP 工作階段。IPSec 通道和 BGP 的設定各自獨立。如要瞭解為 BGP 設定 IPSec 通道的相關資訊，請參閱 *SonicOS 連線能力*。

若要設定用於 BGP 的 IPSec 通道:

1 您可以在 SonicOS 管理介面的**管理 | 連線 | VPN** 設定部分中完整設定 IPSec 通道。設定 IPSec 通道時，請務必確認下列選項已設定完成:

選項	值
原則類型	**站台到站台** **附註：**透過 IPSec 的 BGP 必須使用站台到站台 VPN 通道。
IPsec 主要閘道名稱或位址	遠端對等的 IP 位址
本機 IKE ID	SonicWall 安全設備的 IP 位址
對等 IKE ID	遠端對等的 IP 位址
**網路	從清單中選擇目的地網路**	遠端對等 IP 位址
**進階	啟用保持運作**	啟用

重要：透過 IPSec 設定 BGP 時:

1 設定 IPSec 通道。

2 設定 BGP 前，請先透過通道確認連線狀態。

附註：如需瞭解如何設定 VPN 原則，請參閱 *SonicOS 連線能力*。

2 新增路由原則時，請為**服務**選項選取 **BGP**，藉此在**管理 | 系統安裝 | 網路 | 路由**頁面上啟用 BGP。如需瞭解如何新增路由原則，請參閱第 407 頁「設定 BGP 進階路由」；如需瞭解基本 BGP 設定，請參閱第 799 頁「基本 BGP 設定」。

3 透過 SonicOS 命令行介面完成路由設定。如需 SonicOS CLI 相關資訊，請參閱 *SonicOS 命令行介面指南*。

4 在安全設備上設定 VPN 原則時，請在遠端對等上完成相應的 IPSec 設定。

5 遠端對等的 IPSec 設定完成後，請返回**管理 | 連線 | VPN | 基本設定**，然後啟用 VPN 原則來啟動 IPSec 通道。

6 在 SonicWall 安全設備上使用 Ping 診斷功能來對 BGP 對等 IP 位址進行 Ping。如需更多 Ping 診斷功能的相關資訊，請參閱 *SonicOS 調查*。

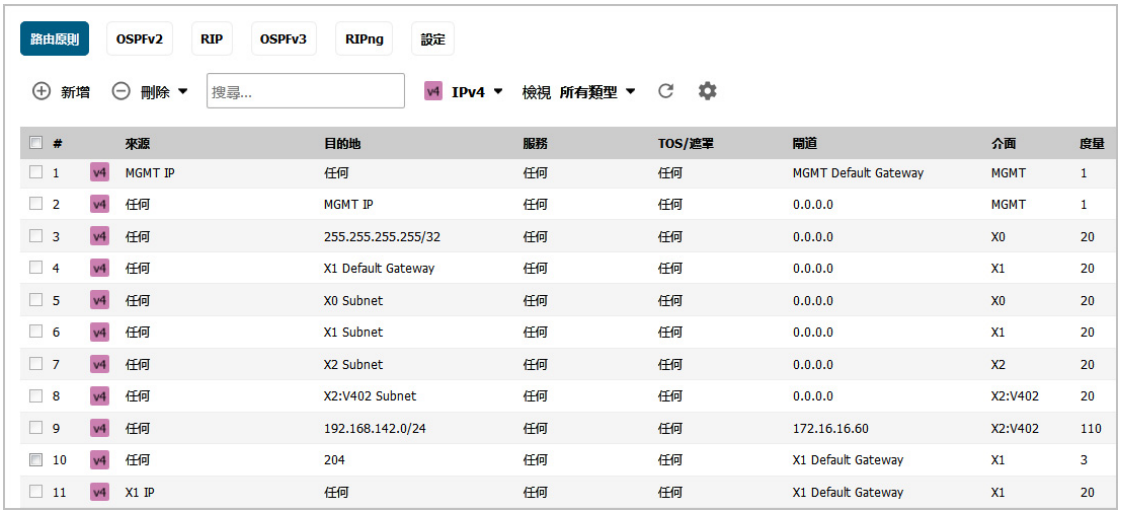
7 使用 Wireshark 確保要求和回應都封裝在 ESP 封包中。

附註：如本例中的設定，傳送的流量不會經過用於 BGP 的 IPSEC 通道。此流量的傳送和接收暢通無阻，這正符合預期的行為，因為目的地是保障 BGP 的安全性，而不是所有傳送的網路流量。

基本 BGP 設定

若要在 SonicWall 安全設備上設定 BGP:

1 導覽到**管理 | 系統安裝 | 網路 | 路由**。



#		來源	目的地	服務	TOS/遮罩	閘道	介面	度量
1	v4	MGMT IP	任何	任何	任何	MGMT Default Gateway	MGMT	1
2	v4	任何	MGMT IP	任何	任何	0.0.0.0	MGMT	1
3	v4	任何	255.255.255.255/32	任何	任何	0.0.0.0	X0	20
4	v4	任何	X1 Default Gateway	任何	任何	0.0.0.0	X1	20
5	v4	任何	X0 Subnet	任何	任何	0.0.0.0	X0	20
6	v4	任何	X1 Subnet	任何	任何	0.0.0.0	X1	20
7	v4	任何	X2 Subnet	任何	任何	0.0.0.0	X2	20
8	v4	任何	X2:V402 Subnet	任何	任何	0.0.0.0	X2:V402	20
9	v4	任何	192.168.142.0/24	任何	任何	172.16.16.60	X2:V402	110
10	v4	任何	204	任何	任何	X1 Default Gateway	X1	3
11	v4	X1 IP	任何	任何	任何	X1 Default Gateway	X1	20

2 按一下**設定**。

3 在**路由模式**中選取**進階路由**。

4 在 **BGP** 中選取**已啟用 (使用 CLI 設定)**。將顯示確認訊息。

附註：在透過管理介面啟用 BGP 後，BGP 設定的具體設定使用 SonicOS 命令行介面 (CLI) 執行。如需連接至 SonicOS CLI 的詳細資料，請參閱 *SonicOS 命令行介面指南*。

5 透過主控台介面登入 SonicOS CLI。

6 透過輸入 **configure** 命令進入設定模式。

7 輸入 **configure routing bgp** 命令進入 BGP CLI。此提示顯示：

```
ZebOS version 7.7.0 IPIRouter 7/2009

ARS BGP>
```

8 現在，您在 BGP 非設定模式中。類型**?** 查看非設定命令清單。

9 輸入 **show running-config** 查看目前的 BGP 執行設定。

10 若要進入 BGP 設定模式，輸入 **configure terminal** 命令。輸入 **?** 查看設定命令的清單。

11 在完成設定後，輸入 **write file** 命令。如果此單元是「高可用性」對或叢集的一部分，設定變更將自動傳達至一個或多個其他單元。

BGP 路徑選擇過程

BGP 路徑選擇過程屬性表格說明了設定 BGP 路徑選擇過程時所用的屬性。

BGP 路徑選擇過程屬性

屬性	說明
權數	慣用的向鄰居學習的路由具有最高權重值。僅適用於本機路由器。
本機喜好設定	為管理目的慣用的向鄰居學習的路由。與整個 AS 共用。
網路或**彙總**路徑	慣用的在本機來源於**網路**和**彙總位址**命令的路徑。
AS_PATH	慣用的具有最短 AS_PATH 的路徑。
原始來源	慣用的擁有最低原始來源類型的路徑（如「更新」訊息中發佈）：IGP < EGP < 不完整。
多出口識別 (MED)	對於去往來源 AS 的路徑的鄰居提供路徑喜好設定資訊。
最近	慣用的最近收到的路徑。
路由器 ID	慣用的來自擁有最小路由器 ID 的路由器的路徑。

權數

權重命令按位址家族向學習自鄰居的所有路由指派權重值。如相同首碼向多個同等項學習，則慣用的具有最高權重高的路由。權重僅適用於本機路由器。

使用 **set weight** 命令指派的權重替代使用上述命令指派的權重。

如為對等群組設定權重，則對等群組中的所有成員都具有相同的權重。此命令還可用於向指定的對等群組成員指派不同的權重。

這個範例顯示的是權重設定:

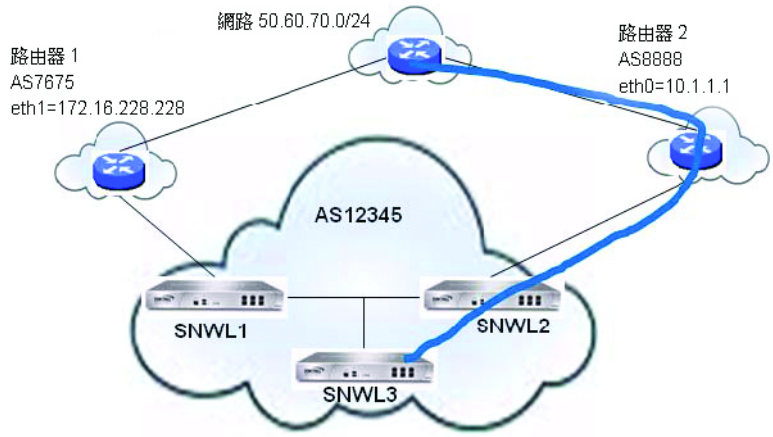
```
router bgp 12345
   neighbor 12.34.5.237 remote-as 12345
   neighbor 12.34.5.237 weight 60


router bgp 12345
   neighbor group1 peer-group
   neighbor 12.34.5.237 peer-group group1
   neighbor 67.78.9.237 peer-group group1
   neighbor group1 weight 60
```

本機喜好設定

「本機喜好設定」屬性用於表示裝置路由表中各外部路由的慣用的程度。「本機喜好設定」屬性包含在傳送至相同 AS 中裝置的所有更新訊息中。「本機喜好設定」不與外部 AS 交流。BGP 本機喜好設定拓撲結構是顯示本機喜好設定如何影響相鄰 AS 之間的路由的拓撲結構範例。

BGP 本機喜好設定拓撲結構



SNWL1 和 SNWL2 設定表格中顯示的 BGP 設定是在 SNWL1 和 SNWL2 中輸入。SNWL2 中的較高本機慣用的值致使 SNWL2 成為 AS 12345（SonicWall AS）向外部 AS 發佈的慣用的路由。

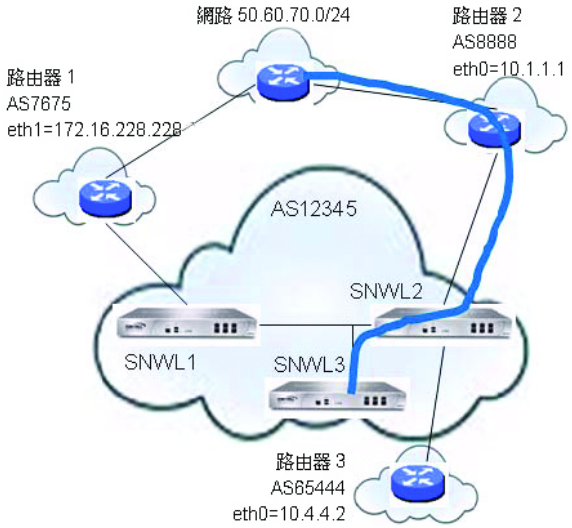
SNWL1 和 SNWL2 設定

SNWL1 設定	SNWL2 設定
x0 = 12.34.5.228	x0 = 12.34.5.237
x1 = 172.16.228.45	x1 = 10.1.1.2
----------	----------
router bgp 12345	router bgp 12345
neighbor 172.16.228.228 remote-as 7675	neighbor 10.1.1.1 remote-as 8888
neighbor 12.34.5.237 remote-as 12345	neighbor 12.34.5.228 remote-as 12345
bgp default local-preference 150	bgp default local-preference 200

使用路由對應的本機喜好設定

路由對應類似於存取控制清單。其中包含一系列用於確定裝置如何處理路由的允許和/或拒絕語句。路由對應套用於輸入流量，而不是輸出流量。使用路由對應的 BGP 本機喜好設定拓撲結構顯示使用路由對應設定本機喜好設定的拓撲結構範例。

使用路由對應的 BGP 本機喜好設定拓撲結構



SNWL1 和 SNWL2 設定和路由對應表格中顯示的 BGP 設定是在 SNWL1 和 SNWL2 中輸入。

SNWL1 和 SNWL2 設定和路由對應

SNWL1 設定	SNWL2 設定
x1 = 172.16.228.45	x0 = 12.34.5.237 x1 = 10.1.1.2 x4 = 10.4.4.1
----------	----------
router bgp 12345 neighbor 172.16.228.228 remote-as 7675 neighbor 12.34.5.237 remote-as 12345 bgp default local-preference 150	router bgp 12345 neighbor 10.1.1.1 remote-as 9999 neighbor 10.1.1.1 route-map rmap1 in neighbor 12.34.5.237 remote-as 12345 .... ip as-path access-list 100 permit ^8888$ ... route-map rmap1 permit 10 match as-path 100 set local-preference 200 route-map rmap1 permit 20 set local-preference 150

在 SNWL2 (rmap1) 設定的路由對應套用於來自鄰居 `10.1.1.1` 的輸入路由。有兩個允許條件：

- **route-map rmap1 permit 10**：此允許條件符合經設定允許來自 AS 8888 流量的存取清單 100，並將來自 AS 8888 的路由設為本機慣用的值 200。
- **route-map rmap1 permit 10**：此允許條件將不符合存取清單 100 的所有其他流量（即來自 8888 以外的其他 AS 的流量）設為本機慣用的值 150。

AS_Path 預置

AS_Path 預置是在路徑更新開始時新增附加 AS 編號的一項操作。這會使此路由的路徑更長，從而降低其慣用的性。

AS_Path 預置可套用於輸入和輸出路徑。如果受鄰居超控，則 AS_Path 預置可能不起作用。

輸入和輸出路徑設定

輸出路徑設定	輸入路徑設定
router bgp 12345	router bgp 7675
bgp router-id 10.50.165.233	bgp router-id 10.50.165.228
network 12.34.5.0/24	network 7.6.7.0/24
neighbor 10.50.165.228 remote-as 7675	neighbor 10.50.165.233 remote-as 12345
neighbor 10.50.165.228 route-map long out	neighbor 10.50.165.233 route-map prepend in
!	!
route-map long permit 10	route-map prepend permit 10
set as-path prepend 12345 12345	set as-path prepend 12345 12345

本設定將使路由安裝到鄰近的 10.50.165.233，AS_Path Prepended 為 12345 12345。這可以透過輸入 **show ip bgp** 命令檢視。

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.228
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 12.34.5.0/24     10.50.165.233            0             0 12345 12345 12345 i
*> 7.6.7.0/24       0.0.0.0                        100  32768 i
Total number of prefixes 2
```

多出口識別 (MED)

set metric 命令可用於路由對應中設定路徑的優先性：

```
router bgp 7675
network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map highmetric out
!
route-map highmetric permit 10
   set metric 300
```

多出口識別 (MED) 是可用於影響路徑優先性的可選屬性。這是非傳遞性的，表示在單個裝置上設定，不會在更新訊息中發佈給鄰居。在此部分中，可考慮使用第 805 頁「bgp always-compare-med 命令」和第 805 頁「bgp deterministic-med 命令」。

bgp always-compare-med 命令

bgp always-compare-med 命令允許比較來自不同 AS 的路徑的 MED 值以選擇路徑。慣用的擁有較低 MED 的路徑。

例如，考慮 BGP 表中的以下路由，啟用 **always-compare-med** 命令：

```
Route1: as-path 7675, med 300
Route2: as-path 200, med 200
Route3: as-path 7675, med 250
```

路由 2 將成為勾選的路徑，因為它擁有最低的 MED。

如果停用 **always-compare-med** 命令，在比較路由 1 和路由 2 時就不會考慮 MED，因為它們擁有不同的 AS 路徑。僅比較路由 1 和路由 3 的 MED。

bgp deterministic-med 命令

選擇的路由也受 **bgp deterministic-med** 命令影響，此命令在選擇相同自發系統中不同對等項發佈的路由時會比較 MED。

啟用 **bgp deterministic-med** 命令時，將來自相同 AS 的路由歸入群組，將比較各群組的最佳路由。如果顯示 BGP 表：

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP 將擁有包含路由 1 的群組和包含路由 2 和路由 3（相同 AS）的第二個群組。

將比較各群組的最佳路由。路由 1 是其所在群組的最佳路由，因為它是來自 AS 200 的唯一路由。

路由 1 與 AS 400 群組中的最佳項路由 2（最低 MED）進行比較。

由於兩個路由並非來自相同 AS，在比較中不會考慮 MED。外部 BGP 路由優於內部 BGP 路由，因此路由 3 成為最佳路由。

BGP 團體

團體是共用相同的屬性，且可以使用傳遞性 BGP 團體屬性設定的首碼群組。首碼可以具有多個團體屬性。路由器可以具備一個、多個或所有屬性。BGP 團體可以視為一種標籤形式。下面是 BGP 團體設定的範例。

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 send-community
   neighbor 10.50.165.228 route-map comm out
!
access-list 105 permit 12.34.5.0/24
access-list 110 permit 23.45.6.0/24
!
route-map comm permit 10
   match ip address 105
   set community 7675:300
!
```

```
route-map comm permit 20
   match ip address 110
   set community 7675:500
!
router bgp 7675
   bgp router-id 10.50.165.228
   network 7.6.7.0/24
   neighbor 10.50.165.233 remote-as 12345
   neighbor 10.50.165.233 route-map shape in
!
ip community-list 1 permit 7675:300
ip community-list 2 permit 7675:500
!
route-map shape permit 10
   match community 1
   set local preference 120
route-map shape permit 20
   match community 2
   set local preference 130
```

同步和自動摘要

同步設定控制路由器是否根據學習自 iBGP 鄰居的路由在 IGP 中的存在情況發佈這些路由。同步啟用時，BGP 將僅發佈可透過 OSPF 或 RIP（相對於 BGP 的外部閘道通訊協定）連接的路由。同步是發生 BGP 路由宣告問題的常見原因。

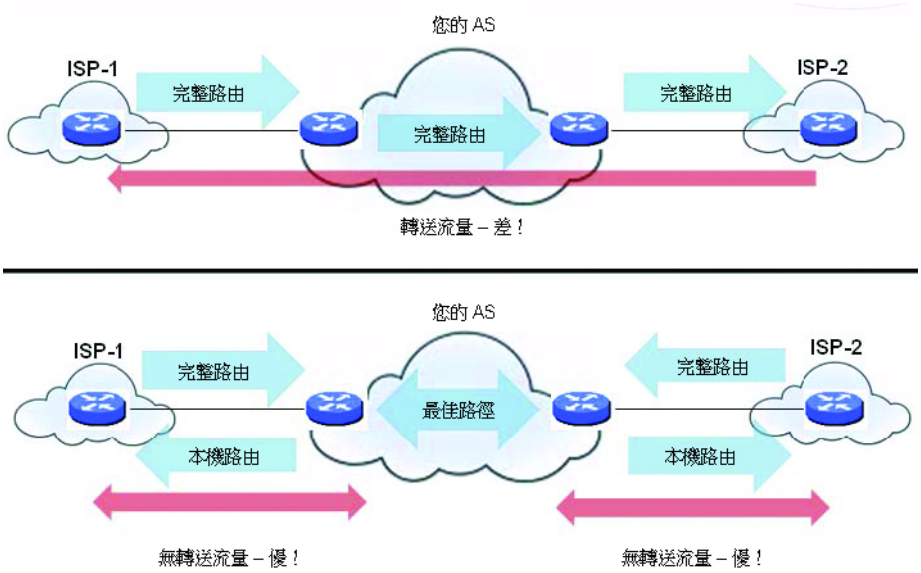
自動摘要設定控制是否按類別發佈路由。自動摘要是發生 BGP 設定問題的另一個常見原因。

預設情況下，在 Zebos 中停用自動摘要和同步。

防止意外中轉 AS

正如之前所述，AS 對等項既可以是中轉對等項（允許從外部 AS 到另一 AS 的流量），也可以是非中轉對等項（要求所有流量來自或終止於相應的 AS）。請參閱中轉對等項與非中轉對等項。中轉對等項顯著擴大了路由表。一般來說，您不會想將 SonicWall 安全設備設定為中轉對等項。

中轉對等項與非中轉對等項



為了防止您的安全設備意外成為中轉對等項，您要設定輸入和輸出篩選條件，例如:

- 第 807 頁「輸出篩選條件」
- 第 808 頁「輸入篩選條件」

輸出篩選條件

僅允許來自本機 AS 的路由輸出：

```
ip as-path access-list 1 permit ^$


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 filter-list 1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 filter list 1 out
```

僅允許擁有的首碼輸出：

```
ip prefix-list myPrefixes seq 5 permit 12.34.5.0/24
ip prefix-list myPrefixes seq 10 permit 23.45.6.0/24


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list myPrefixes out
   neighbor 172.1.1.2 prefix-list myPrefixes out
```

輸入篩選條件

丟棄所有擁有的和私人的輸入首碼。

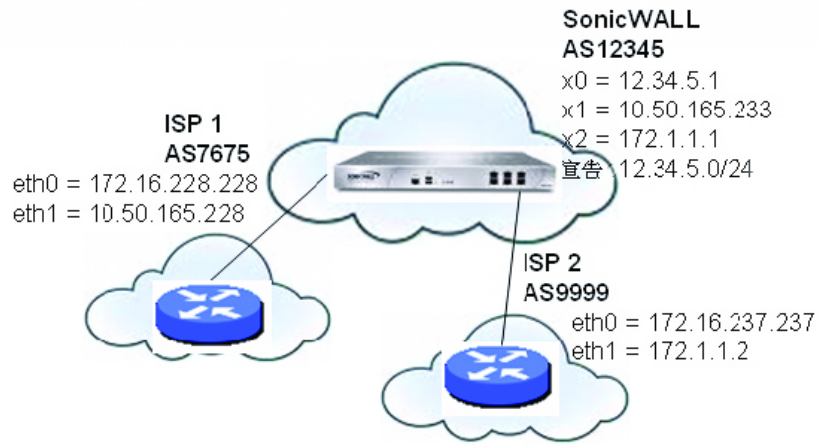
```
ip prefix-list unwantedPrefixes seq 5 deny 12.34.5.0/24 le 32
ip prefix-list unwantedPrefixes seq 10 deny 23.45.6.0/24 le 32
ip prefix-list unwantedPrefixes seq 20 deny 10.0.0.0/8 le 32
ip prefix-list unwantedPrefixes seq 21 deny 172.16.0.0/12 le 32
ip prefix-list unwantedPrefixes seq 22 deny 192.168.0.0/16 le 32
ip prefix-list unwantedPrefixes seq 30 permit 0.0.0.0/0 le 32


router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   network 23.45.6.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 prefix-list unwantedPrefixes in
   neighbor 172.1.1.2 prefix-list unwantedPrefixes in
```

使用多重主目錄 BGP 進行負載分擔

用於負載分擔拓撲結構的多重主目錄 BGP 中顯示的拓撲是 SonicWall 安全設備使用多重主目錄 BGP 網路在兩個 ISP 之間分擔負載的範例。

用於負載分擔拓撲結構的多重主目錄 BGP



SonicWall 安全設備的設定如下:

```
router bgp 12345
   bgp router-id 10.50.165.233
   network 12.34.5.0/24
   neighbor 10.50.165.228 remote-as 7675
   neighbor 10.50.165.228 route-map ISP1 out
   neighbor 172.1.1.2 remote-as 9999
   neighbor 10.50.165.228 route-map ISP2 out
!
route-map ISP1 permit 10
match ip address 1
set weight 100

route-map ISP1 permit 20
match ip address 2
```

```
route-map ISP2 permit 10
match ip address 1


route-map ISP2 permit 20
match ip address 2
set weight 100


access-list 1 permit 12.34.5.0/25
access-list 2 deny 12.34.5.0/25
access-list 2 permit any
```

驗證 BGP 設定

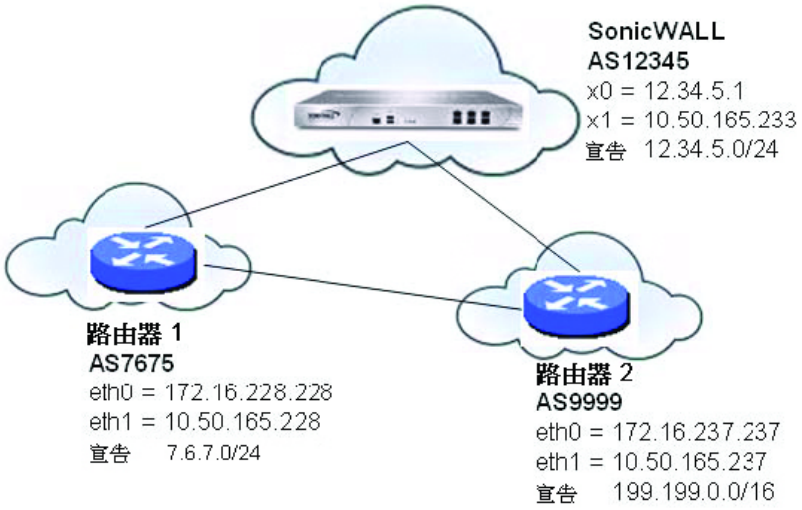
主題：

- 第 809 頁「檢視 BGP 路由」
- 第 811 頁「設定 BGP 偵錯和記錄」

檢視 BGP 路由

BGP 拓撲顯示的是基本 BGP 拓撲結構，其中 SonicWall 安全設備設定為可讓 BGP 連接至位於兩個不同 AS 的兩個路由器。

BGP 拓撲



此網路的 FIB 中的路由可以在 SonicOS 管理介面中或透過使用 CLI 檢視。

主題：

- 第 810 頁「在管理介面中檢視 FIB 路由」
- 第 810 頁「在 CLI 中檢視 FIB 路由」
- 第 810 頁「檢視 CLI 中的 RIB 路由」

在管理介面中檢視 FIB 路由

按一下 **BGP 狀態**，即可透過**管理 | 系統安裝 | 網路 | 路由 > 設定**，在 SonicOS 管理介面中檢視 BGP 設定摘要。**BGP 狀態**對話方塊會顯示 **show ip bgp summary** 和 **show ip bgp neighbor** 命令的輸出情形。

您也可以如同第 810 頁「在 CLI 中檢視 FIB 路由」中所述，透過 CLI 檢視 FIB 中的 BGP 路由。

在 CLI 中檢視 FIB 路由

若要檢視 CLI 中的 FIB 路由：

```
SonicWall> configure
(config[SonicWall])> route ars-nsm

ZebOS version 7.7.0 IPIRouter 7/2009
ARS NSM>show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

B       7.6.7.0/24 [20/0] via 10.50.165.228, X1, 05:08:31
B       199.199.0.0/16 [20/0] via 10.50.165.237, X1, 05:08:31
C       10.50.165.192/26 is directly connected, X1
C       127.0.0.0/8 is directly connected, lo0
C       12.34.5.0/24 is directly connected, X0
```

檢視 CLI 中的 RIB 路由

若要檢視 CLI 中的 RIB 路由:

```
ARS BGP>show ip bgp
BGP table version is 98, local router ID is 10.50.165.233
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l -
labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 7.6.7.0/24       10.50.165.228            0             0 7675 i
*> 12.34.5.0/24     0.0.0.0                        100  32768 i
*> 199.199.0.0/16   10.50.165.228            0             0 7675 9999 i
Total number of prefixes 3
```

附註：最後一個路由是透過 AS7675 學習並去往 AS9999 的路徑。

設定 BGP 偵錯和記錄

SonicWall BGP 提供用於顯示 BGP 流量相關記錄事件的全面偵錯命令選擇。可以在 CLI 使用**?? bgp** 命令後面加上 BGP 偵錯關鍵字表格中所顯示的關鍵字之一，設定 BGP 記錄。

BGP 偵錯關鍵字

BGP 偵錯關鍵字	用途
全部	所有 BGP 偵錯。
抑制	BGP 抑制的偵錯。
事件	BGP 事件的偵錯。
篩選條件	BGP 篩選條件的偵錯。
fsm	BGP 有限狀態機 (FSM) 的偵錯。
保持活動	BGP 保持活動的偵錯。
nht	NHT 訊息的偵錯。
nsm	NSM 訊息的偵錯。
更新	輸入/輸出 BGP 更新的偵錯。

若要停用 BGP 偵錯，輸入「no」形式的命令。例如，若要停用事件偵錯，輸入**no debug events** 命令。

您也可以在**管理 | 調查 | 記錄 | 事件記錄**的 SonicOS GUI 中檢視 BGP 記錄訊息。BGP 訊息作為記錄訊息中**進階路由**類別的一部分顯示。如需更多記錄相關資訊，請參閱 *SonicOS 記錄和報告*。

若要允許未直接連接的 BGP 對等項，請使用 **ebgp-multihop** 關鍵字與 **neighbor** 命令。例如：

```
neighbor 10.50.165.228 ebgp-multihop
```

IPv6 BGP

IPv6 邊界閘道通訊協定 (BGP) 在自發系統 (AS) 之間交流 IPv6 路由資訊。具備 IPv6 BGP 支援的 SonicWall 安全裝置可以替代網路自發系統使用的傳統 BGP 路由器。

系統會透過**管理 | 系統安裝 | 網路 | 路由**啟用 IPv6 BGP，但您必須透過 SonicOS 命令行介面 (CLI) 進行設定。

適用下列限制:

- 僅 NSA 平台上支援 IPv6 BGP。
- IPv6 BGP 取決於 IPv6 功能和 ZebOS (Zebra OS)。
- IPv6 BGP 中不支援 MPLS/VPN 和多點傳送。

主題：

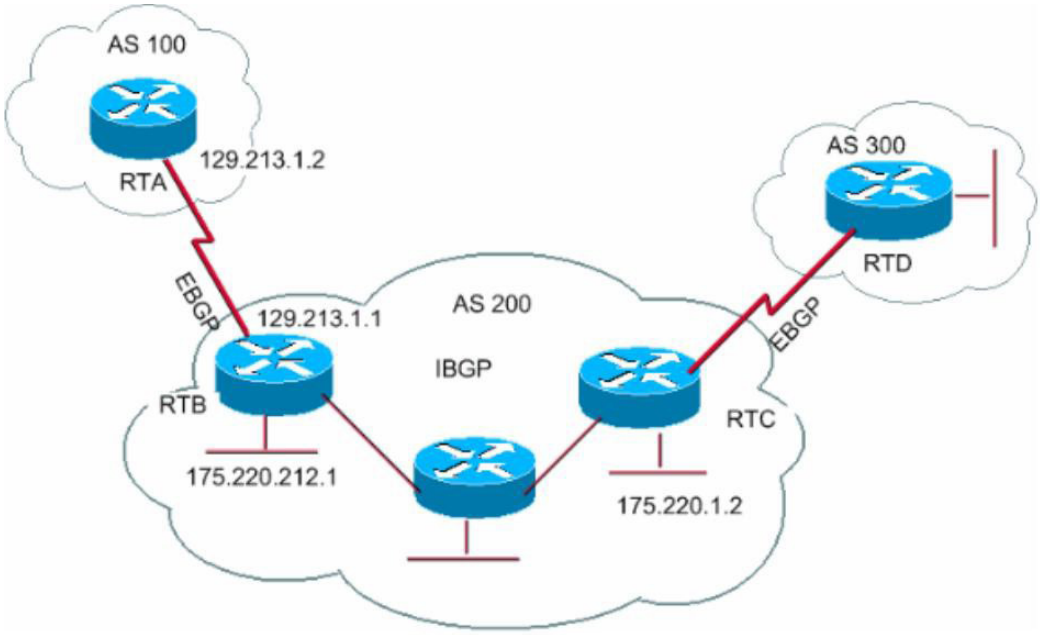
- 第 817 頁「設定 AS 規則運算式」
- 第 819 頁「EBGP 路由選擇」
- 第 822 頁「IPv6 BGP 同步」
- 第 823 頁「BGP 路由反射」
- 第 826 頁「IPv6 BGP 本機慣用的」
- 第 829 頁「BGP 對等群組更新原則」
- 第 831 頁「BGP 聯盟」

設定多個自發系統

如果自發系統 (AS) 擁有多個 BGP 路由器，AS 可以用於其他 AS 的轉換服務。BGP 在不同 AS 的路由器之間執行時使用外部 (eBGP)。BGP 在相同 AS 的路由器之間執行時使用內部 (eBGP)。

在包含多種 BGP 路由器設定的自發系統中，AS 200 是 AS 100 和 AS 300 的轉換 AS。

包含多種 BGP 路由器設定的自發系統



若要如包含多種 BGP 路由器設定的自發系統所示設定多個 AS，請設定路由器 RTA、RTB 和 RTC，如下所示：

在 RTA：

```
router bgp 100
   neighbor 129.213.1.1 remote-as 200
address-family ipv6
   redistribute connected
   neighbor 129.213.1.1 activate
```

在 RTB：

```
router bgp 200
```

```
   neighbor 129.213.1.2 remote-as 100
   neighbor 175.220.1.2 remote-as 200

address-family ipv6
   redistribute connected
   neighbor 129.213.1.2 activate
   neighbor 175.220.1.2 activate
```

在 RTC：

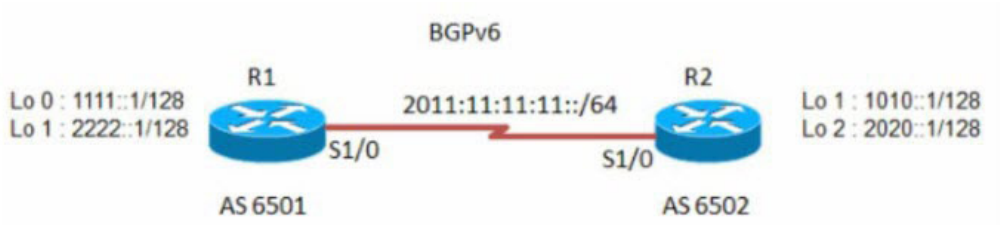
```
router bgp 200
   neighbor 175.220.212.1 remote-as 200

address-family ipv6
   neighbor 175.220.212.1 activate
   neighbor 175.220.212.1 activate
```

設定基本 BGP over IPv6

可以設定 IPv6 BGP 對等路由器以透過 IPv6 位址族或 IPv4 位址族傳送 IPv4 或 IPv6 路由資訊。請參閱基本 BGP over IPv6 設定表格。

基本 BGP over IPv6 設定



若要設定基本 BGP over IPv6:

1 設定路由器 R1 和 R2:

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502

address-family ipv6
   neighbor 2011:11:11:11::2 activate

exit-address-family
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

設定 EBGP Multihop

EBGP Multihop 用於在兩個未直接相連的外部對等機之間建立相鄰連接。Multihop 僅可用於 eBGP，不適用於 iBGP。如果安全設備具有無直接連接的外部鄰居，您可以使用 **ebgp-multihop** 命令建立鄰居連接。

若要設定 EBGP Multihop:

1 設定路由器 R1 和 R2:

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502
   neighbor 2011:11:11:11::2 ebgp-multihop


address-family ipv6
   neighbor 2011:11:11:11::2 activate
exit-address-family
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501
   neighbor 2011:11:11:11::1 ebgp-multihop


address-family ipv6
   network 1010::1/128
   network 2020::1/128
   neighbor 2011:11:11:11::1 activate
```

設定 IPv6 BGP 輸出路由篩選條件

IPv6 BGP 輸出路由篩選條件 (ORF) 可用於通篩選除來源處的多餘路由更新來最大限度減少在對等路由器之間傳送的 BGP 更新數。

若要設定 IPv6 BGP 輸出路由篩選條件 (ORF):

1 設定路由器 R1 和 R2:

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 prefix-list pref1 in
   neighbor 2011:11:11:11::2 prefix-list pref2 out
exit-address-family


ipv6 prefix-list pref1 seq 10 deny 1010::1/128
```

```
ipv6 prefix-list pref1 seq 20 permit any
ipv6 prefix-list pref2 seq 10 deny 1111::1/128
ipv6 prefix-list pref2 seq 20 permit any
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

若要檢查 R1 和 R2 上的路由，請使用 **show bgp ipv6 unicast** 命令。

R1 上的路由應具有 IPv6 位址 1010::1/128。

R2 上的路由應具有 IPv6 位址 1111::1/128。

在 R1：

```
R1> show bgp ipv6 unicast
```

在 R2：

```
R2> show bgp ipv6 unicast
```

設定 IPv6 BGP 分佈清單

IPv6 BGP 分佈清單可用於通篩選除來源處的多餘路由更新來最大限度減少在對等路由器之間傳送的 BGP 更新數。

若要設定 IPv6 BGP 分佈清單:

1 設定路由器 R1 和 R2:

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 distribute-list acl1 in
   neighbor 2011:11:11:11::2 distribute-list acl2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

若要檢查 R1 和 R2 上的路由，請使用 **show bgp ipv6 unicast** 命令。

R1 上的路由應具有 IPv6 位址 1010::1/128。

R2 上的路由應具有 IPv6 位址 1111::1/128。

在 R1：

```
R1> show bgp ipv6 unicast
```

在 R2：

```
R2> show bgp ipv6 unicast
```

IPv6 BGP 路由對應

IPv6 BGP 路由對應可用於通篩選除來源處的多餘路由更新來最大限度減少在對等路由器之間傳送的 BGP 更新數。

若要設定 IPv6 BGP 路由對應:

1 設定路由器 R1 和 R2:

在 R1：

```
router bgp 6501
   bgp router-id 1.1.1.1
   neighbor 2011:11:11:11::2 remote-as 6502


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::2 activate
   neighbor 2011:11:11:11::2 route-map map1 in
   neighbor 2011:11:11:11::2 route-map map2 out
exit-address-family


ipv6 access-list acl1 deny 1010::1/128
ipv6 access-list acl1 permit any
ipv6 access-list acl2 deny 1111::1/128
ipv6 access-list acl2 permit any
!
route-map map1 permit 1 match ipv6 address acl1
!
route-map map2 permit 1 match ipv6 address acl2
!
```

在 R2：

```
router bgp 6502
   bgp router-id 2.2.2.2
   neighbor 2011:11:11:11::1 remote-as 6501


address-family ipv6
   redistribute connected
   neighbor 2011:11:11:11::1 activate
```

若要檢查 R1 和 R2 上的路由，請使用 **show bgp ipv6 unicast** 命令。

在 R1：

```
R1> show bgp ipv6 unicast
```

R1 上的路由應具有 IPv6 位址 1010::1/128。

在 R2：

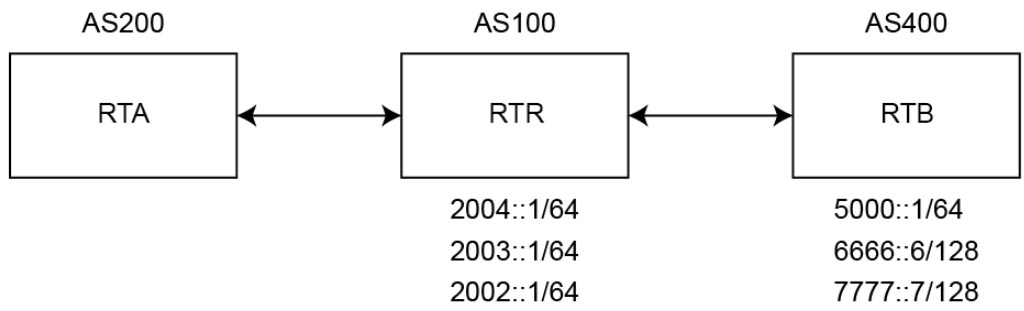
```
R2> show bgp ipv6 unicast
```

R2 上的路由應具有 IPv6 位址 1111::1/128。

設定 AS 規則運算式

您可以設定可符合並用於拒絕或允許來自 AS 的位址的規則運算式。請參閱自發系統規則運算式設定表格。

自發系統規則運算式設定



RTB 發佈以下這些路由：

- 2004::/64
- 2003::/64
- 2002::/64

RTC 發佈以下這些路由：

- 5000::/64
- 6666::6/128
- 7777::7/128

若要檢查路由器 RTA 上的路由:

1 使用 **show bgp ipv6 unicast** 命令:

在 RTA：

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf     Weight     Path
*> 2002::/64      ::ffff:a00:101     0          0          100        i
*> 2003::/64      ::ffff:a00:101     0          0          100        i
*> 2004::/64      ::ffff:a00:101     0          0          100        i
*> 5000::/64      ::ffff:a00:101     0          0          100        400i
*> 6666::6/128    ::ffff:a00:101     0          0          100        400
*> 7777::7/128    ::ffff:a00:101     0          0          100        400
```

若要設定 RTA 上的 AS 規則運算式並拒絕來源於 AS100 的所有路由：

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
   exit-address-family


ip as-path access-list 1 deny ^100$
ip as-path access-list 1 permit .*
```

若要檢查路由器 RTA 上的路由:

1 使用 **show bgp ipv6 unicast** 命令。

在 RTA：

```
RTA> show bgp ipv6 unicast

BGP table version is 4, local router ID is 10.0.1.2

Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal, l - labeled

S Stale

Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric     LocPrf     Weight     Path
```

```
*> 5000::/64      ::ffff:a00:101    0          0         100       400i
*> 6666::6/128    ::ffff:a00:101    0          0         100       400i
*> 7777::7/128    ::ffff:a00:101    0          0         100       400i

Total number of prefixes 3
```

若要修改 AS 路徑以拒絕學習自 AS100 的所有路由：

在 RTA：

```
router bgp 200
   neighbor 10.0.1.1 remote-as 100
   neighbor 10.0.1.1 update-source X2
   neighbor 2004::1 remote-as 100
   neighbor 2004::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.1 activate
   neighbor 10.0.1.1 filter-list 1 in
   neighbor 2004::1 activate
exit-address-family

ip as-path access-list 1 deny _100_
ip as-path access-list 1 permit .*
```

若要檢查路由器 RTA 上的路由:

1 使用 **show bgp ipv6 unicast** 命令。

在 RTA：

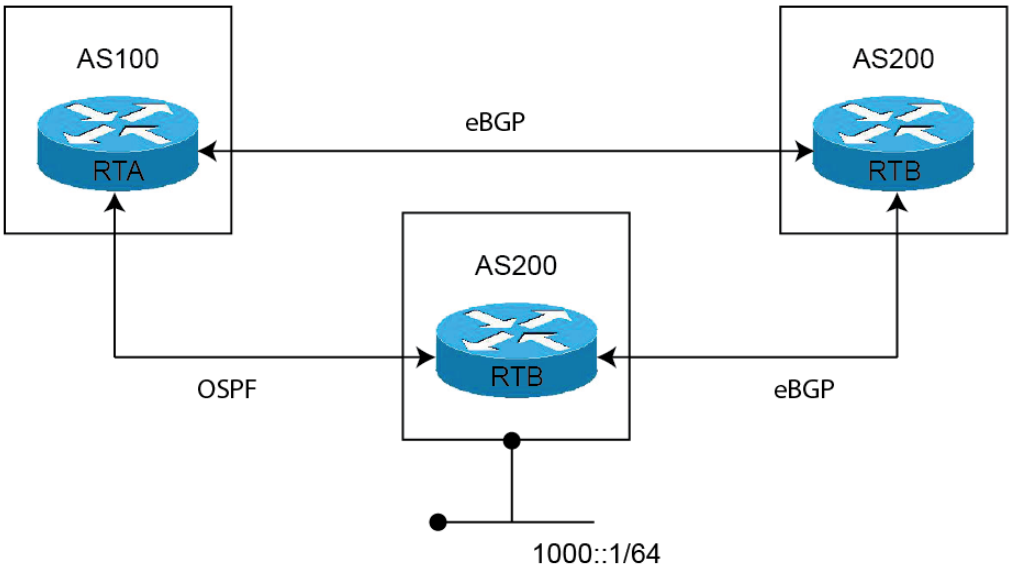
```
RTA> show bgp ipv6 unicast
```

EBGP 路由選擇

路由根據所執行的路由通訊協定的管理距離進行選擇。管理距離較短的路由通訊協定較之管理距離較長的路由通訊協定具有更高的優先順序。EBGP 的管理距離為 20。OSPF 的管理距離為 110。

自發系統 EBGP 路由選擇設定表格顯示 BGP 路由器使用的三個 AS 和路由通訊協定。

自發系統 EBGP 路由選擇設定



AS300 中的 RTC 路由器對 AS100 和 AS200 發佈路由 1000::/64。

從 RTC (AS300) 至 RTA (AS100) 的路由執行 OSPF。

從 RTC (AS300) 至 RTB (AS200) 的路由執行 eBGP。

從 RTA (AS100) 至 RTB (AS200) 的路由執行 eBGP。

RTA (AS100) 接收來自 OSPF 和 eBGP 的路由 1000::/64 的更新。選擇並將學習自 eBGP 的路由新增到 RTA 的路由表，因為 eBGP 的管理距離小於 OSPF 的管理距離。

在 RTA：

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   distance bgp 150 150 150
   neighbor 3001::1 activate
exit-address-family
```

在 RTB：

```
router bgp 200
   bgp log-neighbor-changes
   neighbor 1001::1 remote-as 300
   neighbor 2003::1 remote-as 100

address-family ipv6
   network 6666::6/128
   neighbor 1001::1 activate
   neighbor 2003::1 activate
exit-address-family
```

在 RTC：

```
router bgp 300
   neighbor 3002::1 remote-as 200
```

```
!
address-family ipv6 network 1000::/64
   neighbor 3002::1 activate
exit-address-family
```

若要檢查路由器 RTA 上的路由，請使用 **show ipv6 route** 命令。

```
RTA> show ipv6 route

IPv6 Routing Table

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime


B   1000::/64 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   2003::/64 via ::, X1, 00:30:50
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, 00:01:07
C   fe80::/64 via ::, X1, 00:30:53
```

由於 RTC 與 RTA 直接相連，來自 OSPF 的路由實際優於 BGP 學習的路由。為了確保為路由表選擇 RTA 與 RTC 之間的路由，您可以使用 **distance** 命令將 BGP 路由的預設管理距離變更為長於 OSPF 路由的管理距離。例如：

```
   distance bgp 150 150 150
```

您還可以使用 **backdoor neighbor** 命令設定 BGP 路由為慣用的路由。例如：

在 RTA：

```
router bgp 100
   neighbor 3001::1 remote-as 200
!
address-family ipv6
   network 1000::/64
   backdoor neighbor 3001::1 activate
exit-address-family
```

若要檢查路由器 RTA 上的路由:

1 使用 **show ipv6 route** 命令。

```
RTA> show ipv6 route

IPv6 Routing Table


Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B
- BGP
Timers: Uptime


O   1000::/64 [110/2] via fe80::217:c5ff:feb4:57f2, X4, 00:30:53
C   2003::/64 via ::, X1, ?? 12:31:18
B   6666::6/128 [20/0] via fe80::204:27ff:fe0c:b006, X1, ?? 12:00:03
C   fe80::/64 via ::, X1, ?? 12:31:21
```

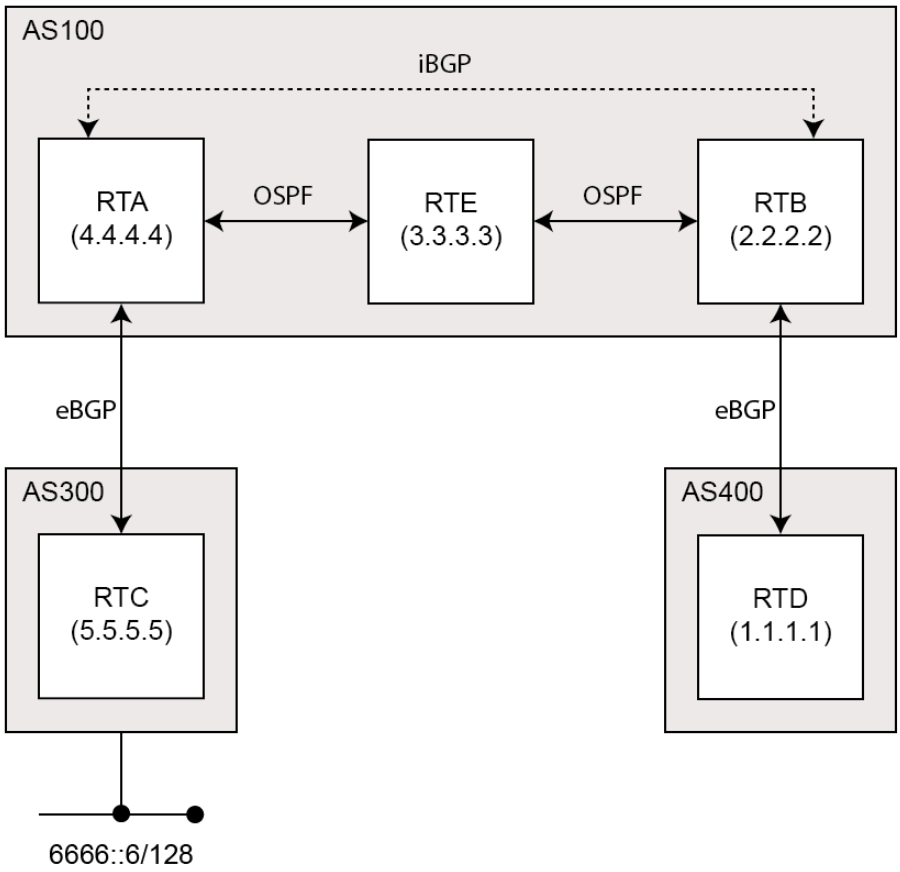
IPv6 BGP 同步

IPv6 BGP 同步保持所有 BGP 路由更新為所有可用路由和網路的 IPv6 位址。

在 BGP 同步中，如果 AS (AS100) 從另一個 AS (AS300) 向第三個 AS (AS400) 傳送流量，則 BGP 不發佈此路由，直到 AS100 中的所有路由器向 IGP 學習此路由。在這種情況中，IGP 是 iBGP。AS100 必須等待至 iBGP 向 AS100 中的所有路由器傳播此路由。然後，eBGP 向外部 AS 發佈此路由。

在本例中，RTB 透過 iBGP 學習位址 6666::6/128，然後向 RTD 發佈位址。

IPv6 BGP 同步範例



附註：您可以透過向 RTB 上的 6666::6/128 新增固定路由和確保其他路由可以達到 6666::6/128 讓 RTB 認為 IGP 已傳播路由資訊。

在本例中，RTC (AS2) 向 RTA (AS100) 發佈位址 6666::6/128。在 AS100 中，RTA 和 RTB 執行 iBGP，所以 RTB 學習位址 6666::6/128 並可以透過下一躍點 5.5.5.5 (RTC) 到達。下一躍點透過 iBGP 傳送。但是，要達到下一躍點 (RTC)，RTB 必須透過 RTE 傳送流量，但 RTE 不知道 IP 位址 6666::6/128。

如果 RTB 向 RTD (AS400) 發佈 6666::6/128，則嘗試從 RTD 到達 6666::6/128 的流量必須經過 AS100 中的 RTB 和 RTE。但是由於 RTE 未學習 6666::6/128，因此會在 RTE 丟棄所有封包。

若要在 AS100 中設定 RTB 上的 BGP 同步：

在 RTB：

```
router bgp 100
```

```
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   synchronization
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

如果您不透過中間 AS 從一個 AS 向另一個 AS 傳送流量，可以停用同步。如果中間 AS 中的所有路由器都執行 BGP，您也可以停用同步。停用同步可以在 IGP 中傳送較少的路由，並允許 BGP 更快匯合。

若要在 AS100 中停用 RTB 上的 BGP 同步：

在 RTB：

```
router bgp 100
   neighbor 10.103.10.129 remote-as 100
   neighbor 3001::1 remote-as 100
   neighbor 3001::1 update-source X4
   neighbor 5000::1 remote-as 400
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.103.10.129 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

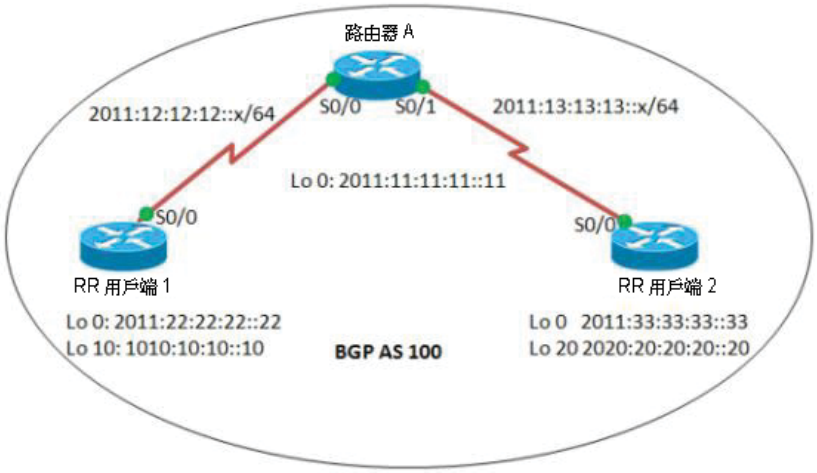
BGP 路由反射

預設情況下，AS 中的所有 iBGP 路由器必須採用完全網狀設定。每個路由器必須設定為每個其他路由器的對等路由器。

透過路由反射，所有 iBGP 無需完全結網。路由反射使 AS 中的各 iBGP 路由器無需與所有其他 iBGP 路由器通信。可以將 iBGP 路由器指定為路由反射器，並向多個 iBGP 用戶端傳送 iBGP 學習的路由。

當設定路由器為路由反射器時，將作為所有其他 iBGP 路由器獲取 iBGP 學習的路由的單一點。路由反射器充當伺服器，而不是 AS 中的每個其他路由器的對等路由器。所有其他 IBGP 路由器變為路由反射器的用戶端。路由器只要有至少一個路由反射器用戶端，就成為路由反射器。

BGP 路由反射設定



若要在 AS 中設定路由反射：

在 RouterA：

```
interface Serial0/0
   ipv6 address 2011:12:12:12::1/64
   ipv6 ospf 10 area 0

interface Serial0/1
   ipv6 address 2011:?? 01:13:13::1/64
   ipv6 ospf 10 area 0

router bgp 100

bgp router-id 1.1.1.1
no bgp default ipv4-unicast
bgp log-neighbor-changes
   neighbor 2011:?? 10:22:22::22 remote-as 100
   neighbor 2011:22:22:22::22 update-source Loopback0
   neighbor 2011:33:33:33::33 remote-as 100
   neighbor 2011:33:33:33::33 update-source Loopback0
!
address-family ipv6
   neighbor 2011:?? 10:22:22::22 activate
   neighbor 2011:22:22:22::22 route-reflector-client
   neighbor 2011:33:33:33::33 activate
   neighbor 2011:33:33:33::33 route-reflector-client
exit-address-family
!
ipv6 router ospf 10
   router-id 1.1.1.1
```

在 RRClient1：

```
interface Loopback0
   ipv6 address 2011:?? 10:22:22::22/128
   ipv6 ospf 10 area 0
```

```
!
interface Loopback10
   ipv6 address 1010:?? 10:10:10::10/128

interface Serial0/0
   ipv6 address 2011:12:12:12::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 2.2.2.2
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:?? 11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 1010:10:10:10::10/128
exit-address-family
!
ipv6 router ospf 10
   router-id 2.2.2.2
```

RRClient2:

```
interface Loopback0
   ipv6 address 2011:33:33:33::33/128
   ipv6 ospf 10 area 0
!
interface Loopback20
   ipv6 address 2020:?? 08:20:20::20/128
!
interface Serial0/0
   no ip address
   ipv6 address 2011:?? 01:13:13::2/64
   ipv6 ospf 10 area 0
!
router bgp 100
   bgp router-id 3.3.3.3
   bgp log-neighbor-changes
      neighbor 2011:11:11:11::11 remote-as 100
      neighbor 2011:?? 11:11:11::11 update-source Loopback0
!
address-family ipv6
   neighbor 2011:11:11:11::11 activate
   network 2020:?? 08:20:20::20/128
exit-address-family
!
ipv6 router ospf 10
   router-id 3.3.3.3
   log-adjacency-changes
```

若要檢查路由:

1 使用 **show bgp ipv6 unicast** 命令:

在 RRClient1：

```
RRClient1> show bgp ipv6 unicast
```

您應該使用路由 2020:20:20:20::20/128。

在 RRClient2：

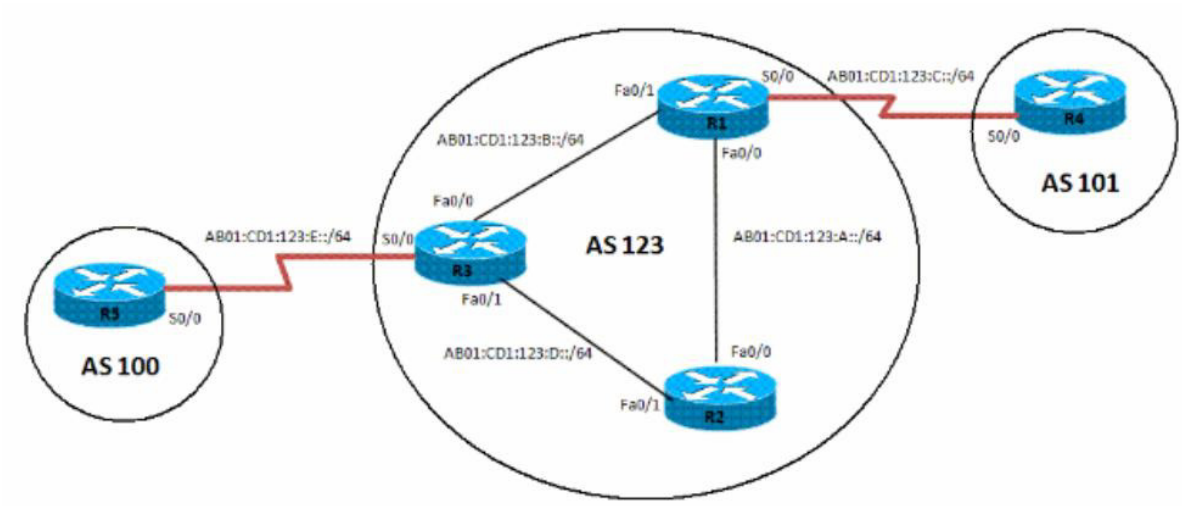
```
RRClient2> show bgp ipv6 unicast
```

您應該使用路由 1010:10:10:10::10/128。

IPv6 BGP 本機慣用的

本機慣用的指定通向某網路的路由作為來自 AS 的網路慣用的出口路由。具有最高本機慣用的類別路由是慣用的路由。本機慣用的的預設值是 100，但可以使用 **set local-preference** 命令來變更。

IPv6 BGP 本機慣用的設定



若要設定 AS 中慣用的路由的本機慣用的：

在 R1：

```
interface Loopback0
   ipv6 address 1111:111:111:A::/64 eui-64
   ipv6 ospf 10 area 0

interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 1.1.1.1 log-adjacency-changes
   redistribute connected route-map CONNECTED
!
route-map CONNECTED permit 10
   match interface Serial0/0
!
router bgp 123
bgp router-id 1.1.1.1
```

```
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 remote-as 101
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 next-hop-self
   neighbor AB01:CD1:123:C:C604:16FF:FE98:0 activate exit-address-family
```

在 R2：

```
interface Loopback0
   ipv6 address 2222:222:222:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
!
   ipv6 router ospf 10 router-id 2.2.2.2 log-adjacency-changes
!
router bgp 123
bgp router-id 2.2.2.2
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 remote-as 123
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 update-source Loopback0

address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 3333:333:333:A:C603:3FF:FEF0:0 activate
exit-address-family
```

在 R3：

```
interface Loopback0
   ipv6 address 3333:333:333:A::/64 eui-64
   ipv6 ospf 10 area 0
!
interface FastEthernet0/0
   ipv6 address AB01:CD1:123:B::/64 eui-64
   ipv6 ospf 10 area 0
!
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
!
interface FastEthernet0/1
   ipv6 address AB01:CD1:123:D::/64 eui-64
   ipv6 ospf 10 area 0
```

```
!
ipv6 router ospf 10
   router-id 3.3.3.3
   redistribute connected route-map CONNECTED
!
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 update-source Loopback0
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 remote-as 123
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 update-source Loopback0
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 activate
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 next-hop-self
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 activate
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 next-hop-self
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 route-map LOCAL_PREF out
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 activate
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map LOCAL_PREF permit 10
   match ipv6 address prefix-list 10
   set local-preference 500
!
route-map LOCAL_PREF permit 20
!
route-map CONNECTED permit 10
   match interface Serial0/0
```

在 R4：

```
interface Serial0/0
   ipv6 address AB01:CD1:123:C::/64 eui-64
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64

router bgp 101
bgp router-id 4.4.4.4
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 remote-as 123
!
address-family ipv6
   neighbor AB01:CD1:123:C:C601:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64 network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64 exit-address-family
```

在 R5：

```
interface Serial0/0
   ipv6 address AB01:CD1:123:E::/64 eui-64
   clock rate 2000000
!
interface Loopback10
   ipv6 address BC01:BC1:10:A::/64 eui-64
!
interface Loopback11
   ipv6 address BC02:BC1:11:A::/64 eui-64
!
interface Loopback12
   ipv6 address BC03:BC1:12:A::/64 eui-64
!
router bgp 202
bgp router-id 5.5.5.5
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 remote-as 123
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 ebgp-multihop 5
!
address-family ipv6
   neighbor AB01:CD1:123:E:C603:3FF:FEF0:0 activate
   network BC01:BC1:10:A::/64
   network BC02:BC1:11:A::/64
   network BC03:BC1:12:A::/64
exit-address-family
```

若要驗證路由:

1 使用 **show bgp ipv6 unicast** 命令:

在 R2：

```
R2> show bgp ipv6 unicast
```

在設定本機慣用的之前，R2 具有 R1 作為所有習得 IPv6 位址的下一躍點。在將 R3 上的本機慣用的設定為 500 後，R2 對首碼 BC01:BC1:10:A::/64 具有不同的慣用的出口路由。現在，R2 可以透過 R3 的出口路徑到達首碼 BC01:BC1:10:A::/64，現將此路由指定為本機慣用的。

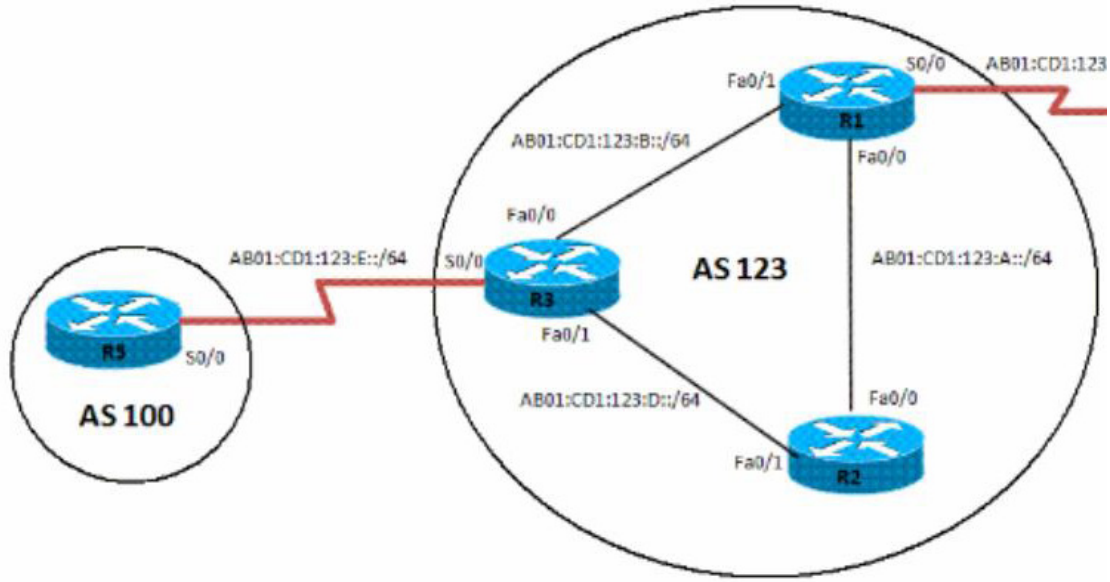
BGP 對等群組更新原則

BGP 對等群組是一組共用相同更新原則的 BGP 鄰居。更新原則通常按路由對應、分佈清單和篩選條件清單設定。

在您定義對等群組和向其新增鄰居時，指派到此對等群組的所有更新原則均套用於對等群組的所有鄰居。您無需定義各鄰居的原則。

對等群組的成員繼承此對等群組的所有設定。您可以設定某些成員變更更新原則，但只有在對輸入流量設定這些原則時才適用。如果原則套用於輸出流量，您就無法設定成員以變更群組原則。

BGP 對等群組更新原則設定



若要設定 IPv6 BGP 對等群組及其更新原則：

在 R3：

```
router bgp 123
   no synchronization
   bgp router-id 3.3.3.3
neighbor interalmap peer-group
   neighbor interalmap remote-as 123
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 remote-as 202
   neighbor AB01:CD1:123:E:C605:16FF:FE98:0 ebgp-multihop 5
!
address-family ipv6
   neighbor interalmap activate
   neighbor interalmap route-map 1 out
   neighbor 1111:111:111:A:C601:3FF:FEF0:0 peer-group interalmap
   neighbor 2222:222:222:A:C602:3FF:FEF0:0 peer-group interalmap
exit-address-family
!
ipv6 prefix-list 10 seq 5 permit BC01:BC1:10:A::/64
!
route-map 1 permit 10
   match ipv6 address prefix-list 1 set tag 333
   set metric 273
   set local-preference 312
```

若要驗證是否已設定正確的本機慣用路由:

1 使用 **show bgp ipv6 unicast** 命令:

在 R3：

```
R3> show bgp ipv6 unicast
```

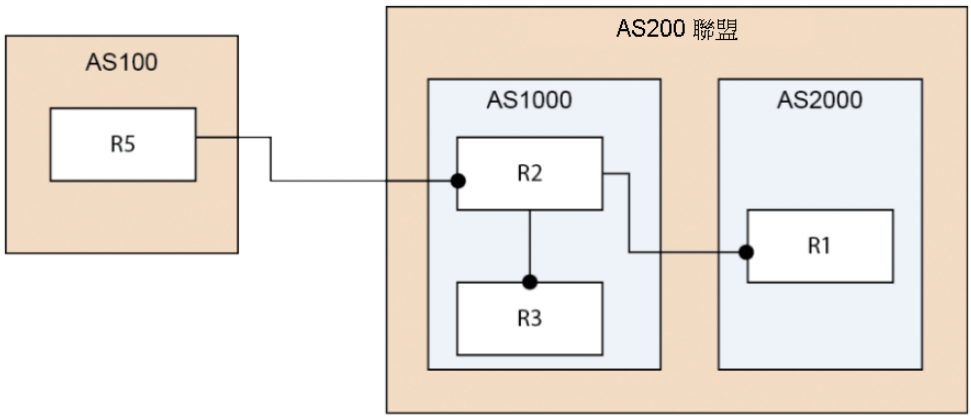
驗證 IPv6 位址 BC01:BC1:10:A::/64 從 AS100 傳遞至 R1 和 R2，且將度量和本機慣用的設為相應的路由對應設定。

BGP 聯盟

您可以將一個 AS 分為多個 AS，然後將這些 AS 指派到一個 AS 聯盟。BGP 聯盟的實作縮小了 AS 的 iBGP 網，且聯盟仍可以作為單個 AS 向外部對等系統發佈路由。

聯盟內的每個 AS 執行完全結網的 iBGP，且聯盟內的每個 AS 還執行與聯盟內其他 AS 的 eBGP 連接。聯盟內的這些 eBGP 對等系統像使用 iBGP 一樣交換路由資訊。這樣，聯盟保留下一躍點、度量和本機慣用的資訊。聯盟對外部顯示為單個 AS。

BGP 聯盟設定



若要設定 BGP 聯盟：

R1：

```
router bgp 2000
   bgp log-neighbor-changes
   bgp confederation identifier 200
   bgp confederation peers 1000
   neighbor 2003::1 remote-as 1000
!
address-family ipv4
   neighbor 2003::1 activate
exit-address-family
!
address-family ipv6
   network 3002::/64
   network 4000::/64
   neighbor 2003::1 activate
exit-address-family
```

在 R2：

```
router bgp 1000
   bgp confederation identifier 200
   neighbor 10.0.1.1 remote-as 1000
!
address-family ipv6
   neighbor 10.0.1.1 activate
```

```
exit-address-family
```

在 R3：

```
router bgp 1000
   bgp confederation identifier 200
   bgp confederation peers 2000
   neighbor 10.0.1.2 remote-as 1000
   neighbor 3001::1 remote-as 2000
   neighbor 5000::1 remote-as 100
   neighbor 5000::1 update-source X2
!
address-family ipv6
   neighbor 10.0.1.2 activate
   neighbor 3001::1 activate
   neighbor 5000::1 activate
exit-address-family
```

在 R5：

```
router bgp 100
   bgp router-id 5.5.5.5
   bgp log-neighbor-changes
   neighbor 2002::1 remote-as 200
!
address-family ipv6
   network 6666::6/128
   network 7777::7/128
   neighbor 2002::1 activate
exit-address-family
```

驗證 R1、R2 和 R3 可以學習 R5 發佈的此路由：

```
6666::6/128 和 7777::7/128
```

驗證 R2 可以向 R1 學習此路由，即使兩者未直接相連：

```
3002::/64 和 4000::/64
```

附註：將 IPv6 BGP 設定資料和 IPv6 BGP 路由傾印到終止並駐留程式 (TSR) 檔案。

附註：IPv6 BGP 使用 ZebOS 偵錯介面。關閉所有偵錯交換器的預設設定。在主控台輸入 CLI **debug** 命令可以打開偵錯交換器。

D

SonicWall 支援

客戶購買附帶有效維護合約的 SonicWall 產品以及擁有試用版，即享有技術支援。

支援入口網站為您提供了自助式工具，方便您全天候快速地自行解決問題。如要存取支援入口網站，請前往 https://support.sonicwall.com。

支援入口網站可以讓您：

- 檢視知識庫文章和技術文件
- 下載軟體
- 檢視視訊教學
- 與使用者論壇中的同儕和專家們協同合作
- 取得授權協助
- 存取 MySonicWall
- 瞭解 SonicWall 專業服務
- 註冊訓練和認證

若要聯絡 SonicWall 支援，請參閱 https://support.sonicwall.com/contact-support。

如需查看 SonicWall 最終使用者產品合約 (EUPA)，請參閱以下網址內容: https://www.sonicwall.com/legal/eupa.aspx。根據您的地理位置選擇語言以查看適用您所在地區的 EUPA。

關於本文件

圖例

警告：警告圖示表示，可能造成財產損害、人員受傷或死亡。

注意：注意圖示表示，若未遵循指示，可能造成硬體損害或資料損失。

重要須知、附註、提示、行動或影片：資訊圖示表示有支援資訊。

SonicOS 管理
已更新 - 2017 年 12 月
軟體版本 - 6.5
232-004133-00 修訂版 A