

SonicWall™ SonicOS 6.5 快速設定

SONICWALL™

目錄

使用 SonicWall 快速設定指南	4
關於快速設定指南	4
在 NAT 啟用時設定固定 IP 位址	4
啟動指南	5
瀏覽指南	6
使用設定指南	7
設定指南	7
存取設定指南	9
部署方案 (僅限無線平台)	9
變更管理員密碼	10
時區	10
設定模組化裝置類型	11
設定 3G/4G/LTE	11
設定數據機	14
WAN 容錯移轉撥號連線	14
WAN 網路模式	15
LAN 設定	20
LAN DHCP 設定	21
調控網域註冊 (僅限無線平台)	22
WLAN Radio 設定 (僅限無線平台)	22
WLAN 安全設定 (僅限無線平台)	26
WPA/WPA2 模式設定 (僅限無線平台)	27
WLAN VAP (虛擬存取點) 設定 (僅限無線平台)	28
連接埠指派	29
設定摘要	33
設定指南已完成	34
使用 PortShield 介面指南	35
PortShield 介面指南	35
使用公用伺服器指南	39
公用伺服器指南	39
公用伺服器類型	40
私人網路	41
伺服器公用資訊	42
公用伺服器設定摘要	43
使用 VPN 指南	45
VPN 指南	45
設定站台對站台 VPN	45

建立 WAN GroupVPN	51
使用無線指南 (僅限無線平台)	56
無線指南	56
調控網域註冊	57
無線 LAN 設定	57
WLAN Radio 設定	59
WLAN 安全設定	62
WPA 模式設定	63
WLAN VAP (虛擬存取點) 設定	65
WLAN VAP (虛擬存取點) 設定 - 建立 VAP	65
WLAN VAP (虛擬存取點) 設定 > WLAN 子網路和區域	66
無線設定摘要	67
使用 App Rule 指南	69
App Rule 指南	69
應用程式規則原則類型	70
使用 WXA 設定指南	78
WXA 設定指南	78
入門	79
介面頁面	80
啟用加速頁面	82
群組頁面	82
WXA 頁面	83
加速元件	84
VPN 頁面	85
路由頁面	85
完成頁面	86
已簽署 SMB 的 WFS 設定指南	86
選擇專屬 WXA	87
啟用延伸支援	87
網域詳細資料	88
加入網域	89
設定共用	90
設定本機檔案伺服器	90
設定遠端檔案伺服器	91
新增網域記錄	92
完成頁面	93
SonicWall 支援	95
關於本文件	96

使用 SonicWall 快速設定指南

- 第 4 頁「[關於快速設定指南](#)」
 - 第 4 頁「[在 NAT 啟用時設定固定 IP 位址](#)」
 - 第 5 頁「[啟動指南](#)」
 - 第 6 頁「[瀏覽指南](#)」

關於快速設定指南

❗ 重要：設定新的 SonicWall 安全裝置時啟動的初始設定指南，與從 SonicOS 管理介面按一下快速設定所顯示的快速設定指南不同。如需有關初始設定指南的資訊，請參見新安全裝置的[入門指南](#)。

❗ 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。

快速設定提供易於使用的設定指南幫助您進行初始原則和安全性的建立。

- 確保您的網際網路連線安全
- 為 PortShield 選擇初始連接埠指派 (僅限 TZ 系列和 SOHO W 安全裝置)
- 提供公共接入權給外部伺服器
- 建立站台對站台 VPN 原則
- 設定 WAN 無線電介面 (僅限 TZ W 系列和 SOHO W 安全裝置) 的網路設定和安全功能。
- 為安全性設定應用程式規則
- 設定 WXA 系列裝置 (僅限具有 WXA 系列裝置的系統)

主題：

- 第 4 頁「[在 NAT 啟用時設定固定 IP 位址](#)」
- 第 5 頁「[啟動指南](#)」
- 第 6 頁「[瀏覽指南](#)」

在 NAT 啟用時設定固定 IP 位址

使用 NAT 設定 SonicWall 無需 LAN 中的所有電腦都有公用 IP 位址。這是儲存網際網路 IPv4 位址集區中可用 IP 位址的一種方式。NAT 還可用於隱藏網路的定址方案。如果您沒有足夠的單獨 IP 位址指派給網路中的所有電腦，您可以在網路設定中使用 NAT。

本質上，NAT 將網路中的 IP 位址轉譯為另一網路的 IP 位址。作為安全裝置的一種封包篩選形式，這可以透過將經過 SonicWall 的封包的內部 (LAN) IP 位址，替換為固定位址集區中的一個偽 IP 位址，來防護網路不受外部駭客入侵。隱藏 LAN 上的電腦的實際 IP 位址，外部使用者無法看到。

本章節介紹在 NAT 模式中設定 SonicWall 網路安全裝置。如果您的 ISP 為您指派了單個 IP 位址，請按照以下說明。

提示： 確保您的網路資訊包含 WAN IP 位址、子網路遮罩和 DNS 設定。這些資訊由您的 ISP 取得。

啟動指南

附註： 初始**啟動指南**會在您首次啟用 TZ 系列或 SOHO W 安全裝置時自動出現。本指南與設定指南不同。如需更多資訊，請參見 TZ 系列或 SOHO W 安全裝置的**入門指南**。

設定指南會在您首次啟用 NSA 系列或 SM 安全裝置時自動出現。

若要在初始啟動以外的任何時間啟動 SonicWall 設定指南，請按一下快速設定管理介面任何頁面上方的**快速設定**。顯示**歡迎**頁面。

附註： PortShield 指南僅針對 TZ 系列安全裝置出現，而無線指南僅針對 TZ W 系列和 SOHO W 安全裝置出現。其他指南 (如 App Rule 指南) 的顯示需要有效的授權。

歡迎

歡迎使用設定指南

選取以下其中一個指南，助您輕鬆設定 SonicWall:

- **設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- **PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- **公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- **VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- **無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- **App Rule 指南** - 設定 App Rule 的安全性功能
- **WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

從此頁面，您可以選擇以下任一指南：

- 第 7 頁「**使用設定指南**」
- 第 35 頁「**使用 PortShield 介面指南**」(此指南僅適用於 TZ 系列和 SOHO W 裝置)
- 第 39 頁「**使用公用伺服器指南**」
- 第 45 頁「**使用 VPN 指南**」
- 第 56 頁「**使用無線指南 (僅限無線平台)**」(此指南僅適用於無線裝置)
- 第 69 頁「**使用 App Rule 指南**」
- 第 78 頁「**使用 WXA 設定指南**」(此指南僅適用於帶 WXA 系列裝置的系統)

瀏覽指南

您可透過分別按**下一頁** 和**返回** 按鈕在指南間來回移動。各頁面的標題會顯示在指南的上方。完成設定指南步驟和進程之後，已完成頁面的標題顏色會發生改變，且會在標題旁出現一個核取標記。



i | **附註：**頁面標題不會出現在無線指南上。

任何時候按一下**結束指南** 按鈕可結束指南。如果您在完成設定前結束，則會出現一個快顯對話框，要求確認結束而不儲存任何設定：

如果您現在結束 SonicWall 指南，系統將不會儲存您的變更。

是否確定要結束指南？

按一下**確定**結束指南，按一下**否**繼續完成設定。

使用設定指南

- 第 7 頁「設定指南」
 - 第 9 頁「存取設定指南」
 - 第 9 頁「部署方案（僅限無線平台）」
 - 第 10 頁「變更管理員密碼」
 - 第 10 頁「時區」
 - 第 11 頁「設定模組化裝置類型」
 - 第 11 頁「設定 3G/4G/LTE」
 - 第 14 頁「設定數據機」
 - 第 14 頁「WAN 容錯移轉撥號連線」
 - 第 15 頁「WAN 網路模式」
 - 第 20 頁「LAN 設定」
 - 第 21 頁「LAN DHCP 設定」
 - 第 22 頁「調控網域註冊（僅限無線平台）」
 - 第 22 頁「WLAN Radio 設定（僅限無線平台）」
 - 第 27 頁「WPA/WPA2 模式設定（僅限無線平台）」
 - 第 28 頁「WLAN VAP（虛擬存取點）設定（僅限無線平台）」
 - 第 29 頁「連接埠指派」
 - 第 33 頁「設定摘要」
 - 第 34 頁「設定指南已完成」

設定指南

i | **附註：**初始**啟動指南**會在您首次啟用 TZ 系列或 SOHO W 安全裝置時出現。本指南的說明在 TZ 系列或 SOHO W 安全裝置的**入門指南**中。

第一次登入 NSA 系列或 SuperMassive 系列安全裝置時，初始**設定指南**會自動啟動。對於所有 SuperMassive 系列、NSA 系列、TZ 系列和 SOHO W 安全裝置，您可以隨時從管理介面啟動**設定指南**，按一下管理介面上方的**快速設定**即可。

i | **提示：**您還可以從 SonicWall 管理介面的**管理**檢視，設定所有 WAN 和網路設定。

設定指南會協助您設定這些設定：

- 部署方案 (僅限無線安全裝置)
- 管理員密碼和時區
- 模組化裝置類型
- WAN 聯網模式和 WAN 網路設定
- LAN 網路設定
- LAN DHCP 設定
- 連接埠指派 (僅限 TZ 系列和 SOHO W 安全裝置)

主題：

- 第 9 頁「[存取設定指南](#)」
- 第 9 頁「[部署方案 \(僅限無線平台\)](#)」
- 第 10 頁「[變更管理員密碼](#)」
- 第 10 頁「[時區](#)」
- 第 11 頁「[設定模組化裝置類型](#)」
- 第 15 頁「[WAN 網路模式](#)」
- 第 11 頁「[設定 3G/4G/LTE](#)」
- 第 20 頁「[LAN 設定](#)」
- 第 21 頁「[LAN DHCP 設定](#)」
- 第 22 頁「[調控網域註冊 \(僅限無線平台\)](#)」
- 第 22 頁「[WLAN Radio 設定 \(僅限無線平台\)](#)」
- 第 26 頁「[WLAN 安全設定 \(僅限無線平台\)](#)」
- 第 27 頁「[WPA/WPA2 模式設定 \(僅限無線平台\)](#)」
- 第 29 頁「[連接埠指派](#)」
- 第 33 頁「[設定摘要](#)」
- 第 34 頁「[設定指南已完成](#)」

存取設定指南

使用設定指南設定：

- 1 按一下 SonicOS 管理介面上方的**快速設定**。顯示**歡迎**頁面。

歡迎

歡迎使用設定指南
選取以下其中一個指南，助您輕鬆設定 SonicWall:

- **設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- **PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- **公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- **VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- **無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- **App Rule 指南** - 設定 App Rule 的安全性功能
- **WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

- 2 勾選**設定指南**。預設情況下已核取此選項。
- 3 按下一步。如果您擁有：
 - 無線裝置，此時顯示**部署方案**頁面；請參見第 9 頁「**部署方案（僅限無線平台）**」。
 - 有線裝置，此時顯示**變更管理員密碼**頁面；請參見第 10 頁「**變更管理員密碼**」。

部署方案（僅限無線平台）

部署情節

有線和無線部署情節

- **沒有無線** - 無線關閉。
- **辦公閘道** - 為有線及無線使用者提供安全的存取。
- **無線用戶端橋接** - 在無線用戶端橋接模式下操作以安全地橋接兩個網路。
- **安全或者開放存取點** - 新增安全無線接入到已有的有線網路。

- 1 選擇以下一個部署方案：

i | **附註：**顯示的設定頁面隨著您選擇的部署類型而改變。

沒有無線（預設）

無線電關閉。

辦公閘道

為有線及無線使用者提供安全的存取。

無線用戶端橋接

在無線橋接模式下操作以安全橋接兩個網路。

安全或者開放存取點

新增安全無線存取權到現有的有線網路。

- 2 按下一步。即顯示變更管理員密碼頁面。

變更管理員密碼

變更管理員密碼

請選擇強式密碼。強式密碼應為數字和字母的組合且最長為 32 個字元。

舊密碼：

新密碼：

確認密碼：

重要：每個裝置帶有預設的使用者名稱為 **admin**，預設密碼為 **password**。您不能變更預設的使用者名稱，但是，強烈建議您變更密碼。

- 1 在舊密碼欄位中輸入舊密碼。

附註：當您隨後存取設定指南時，此欄位會呈灰顯並含有遮罩的舊密碼。

- 2 在新密碼和確認密碼欄位中輸入新密碼。

重要：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 按下一步。即顯示時區頁面。

時區

變更時區

SonicWall 的內部時鐘會自動透過存取網際網路上的網路時間伺服器進行設定。

請從下拉功能表中選擇「時區」。

時區：

自動為夏令時調整時鐘。

- 1 從時區下拉列表中選擇相應的時區。SonicWall 的內部時鐘由網際網路上的網路時間伺服器自動設定為此時區的正確時間。

- 2 另外，也可選擇自動為夏令時調整時鐘。預設情況下已核取此選項。

- 3 按下一步。

- 4 顯示的頁面取決於您擁有的安全裝置類型，若是無線安全裝置，則取決於您選擇的部署：

- 有線安全裝置或為無線安全裝置選擇的此部署：沒有無線、辦公間道或安全或者開放存取點，設定模組化裝置類型頁面會顯示。
- 選擇了此部署的有線安全裝置：無線用戶端橋接，LAN 設定頁面會顯示。

設定模組化裝置類型

設定模組化裝置類型

您的 SonicWall 裝置包含 USB 插槽。

請從下拉功能表中選擇將要使用的裝置類型

裝置類型:

- 1 從**裝置類型**下拉列表中選擇一種裝置類型：
 - 無（預設值）
 - 3G/4G/LTE/行動
 - 類比數據機
- 2 按下一步。顯示的下一個頁面取決於您的裝置類型選擇：

此裝置類型	顯示此頁面	移至
無	WAN 網路模式	第 15 頁「 WAN 網路模式 」。
3G/4G/LTE/行動	設定 3G/4G/LTE	第 11 頁「 設定 3G/4G/LTE 」。
類比數據機	設定數據機	第 14 頁「 設定數據機 」。

設定 3G/4G/LTE

設定 3G/4G/LTE

您的 SonicWall 包含一個 3G/4G/LTE 裝置。

是否要立即設定 3G/4G/LTE?

是 - 我將為主要或備份網際網路連線使用 3G/4G/LTE。

否 - 此時我不使用 3G/4G/LTE。

- 1 指定如何設定 3G/4G 裝置：
 - 對於主要或備份網路連接，請勾選**是 - 我將為主要或備份網際網路連線使用 3G/4G**。這是預設值。
 - 如果裝置現在未使用，請勾選**否 - 此時我不使用 3G/4G**。
- 2 按下一步。
- 3 如果選擇：
 - **是** - 此時顯示 **3G/4G 數據機 > WAN 容錯移轉 3G/4G/LTE/數據機連接** 頁面。移至第 12 頁「[WAN 容錯移轉 3G/4G/LTE/數據機連接（第 1 頁）](#)」。
 - **否** - 此時顯示 **WAN 網路模式** 頁面；請移至第 15 頁「[WAN 網路模式](#)」。

WAN 容錯移轉 3G/4G/LTE/數據機連接 (第 1 頁)

i | 附註：您必須完成此頁面才能繼續設定您的安全裝置。

WAN 容錯移轉 3G/4G/LTE/數據機 連接

選擇了 WAN 容錯移轉 3G/4G/LTE/數據機 連接。

從下面清單中選擇服務供應商和計劃類型。
SonicWall 將使用此資訊自動設定
必需的連接參數。

如果未找到相應國家/地區、供應商或計劃類型，則請從下面清單中選擇「其他」。

國家/地區：

服務供應商：

計劃類型：

- 1 從國家/地區下拉列表中選擇您的國家或地區。
- 2 從服務供應商下拉列表中選擇您的服務供應商。具體選項取決於您所選擇的國家/地區。
- 3 從計劃類型下拉列表中選擇您的計劃類型。具體選項取決於您所選擇的服務供應商。
- 4 按下一步。第 2 個 WAN 容錯移轉 3G/4G/數據機連接頁面會顯示，其中填充的選項是根據您在「國家或地區」、「服務供應商」和「計劃類型」中的選擇而定。

WAN 容錯移轉 3G/4G/LTE/數據機連接 (第 2 頁)

WAN 容錯移轉 3G/4G/LTE/數據機 連接

您選擇了 T-Mobile - Internet。驗證下列帳戶資訊。

如果不知道電話號碼、使用者名稱或密碼，請諮詢您的網路
供應商或稍後從
3G/4G/LTE/數據機 > 「連線設定檔」頁面設定 3G/4G/LTE/數據機 介面。

設定檔名稱：

連線類型：

已撥號碼：

使用者名稱： (可選)

密碼： (可選)

確認密碼： (可選)

APN：

i | 附註：如果您在國家/地區、計劃類型或服務供應商中選擇其它，則第 2 頁沒有填充資訊，您必須輸入所需資訊。移至第 13 頁「WAN 容錯移轉 3G/4G/LTE/數據機 (第 2 頁-其他)」。

- 1 驗證顯示的資訊。
- 2 如果有任何可選設定沒有填充，請現在輸入。
- 3 按下一步。**WAN 網路模式**對話方塊會顯示。
- 4 移至第 15 頁「**WAN 網路模式**」。

WAN 容錯移轉 3G/4G/LTE/數據機 (第 2 頁-其他)

WAN 容錯移轉 3G/4G/LTE/數據機 連接

未選擇服務計劃。填寫下列帳戶資訊。

如果不知道電話號碼、使用者名稱或密碼，請諮詢您的網路供應商或稍後從 **3G/4G/LTE/數據機** > 「**連線設定檔**」頁面設定 3G/4G/LTE/數據機 介面。

設定檔名稱：	<input type="text" value="我的連線設定檔"/>
連線類型：	<input type="text" value="GPRS/EDGE/HSDPA"/>
已撥號碼：	<input type="text" value="*99#"/>
使用者名稱：	<input type="text"/> (可選)
密碼：	<input type="text"/> (可選)
確認密碼：	<input type="text"/> (可選)
APN：	<input type="text"/>

- 1 如果您在**國家/地區**、**服務供應商**或**計劃類型**中選擇**其它**，則第 2 頁沒有填充資訊，您必須提供所需資訊：
 - **設定檔名稱** - 在此欄位中為設定檔輸入一個方便易記的名稱；預設為**我的連線設定檔**。
 - **連線類型** - 從下拉列表中選擇連線類型。
 - **已撥號碼** - 在此欄位中輸入裝置用於連接到網際網路的撥號號碼。
 - **使用者名稱** (可選) - 在此欄位中輸入您的 ISP 使用者名稱。
 - **密碼** (可選) - 在此欄位中輸入您的 ISP 密碼。
 - **確認密碼** (可選) - 在此欄位中再次輸入您的 ISP 密碼。
- 2 按下一步。此時顯示 **WAN 網路模式** 頁面。
- 3 移至第 15 頁「**WAN 網路模式**」。

設定數據機

設定數據機

您的SonicWall 包含撥接式數據機。

您現在要設定數據機嗎？

- 是 - 我將使用撥號帳戶作為主要或者備份網路連接。
- 否 - 現在不使用數據機。

- 指定如何設定數據機：
 - 對於主要或備份網路連接，請勾選是 - 我將使用撥號帳戶作為主要或者備份網路連接。預設情況下已核取此選項。
 - 如果數據機現在未使用，請勾選否 - 現在不使用數據機。
- 按下一步。
- 如果選擇：
 - 否 - 此時顯示 WAN 網路模式頁面；請移至第 15 頁「WAN 網路模式」。
 - 是 - 此時顯示 WAN 容錯移轉撥號連線頁面；請移至第 14 頁「WAN 容錯移轉撥號連線」。

WAN 容錯移轉撥號連線

如果您選擇了 WAN 容錯移轉撥號連線，則必須輸入在主要WAN乙太網路失聯時 SonicWall 將來用以連線到您的 ISP 的撥號帳戶資訊。

WAN 容錯移轉撥號連線

選擇了 WAN 容錯移轉撥號連線。請填寫撥號帳戶資訊，SonicWall 將會用來在主要的 WAN 乙太網路中斷連線時連接到 ISP。

如果不知道電話號碼、使用者名稱或密碼，請諮詢您的 ISP 或稍後從數據機 > 設定頁面設定數據機。

設定檔名稱：	<input type="text" value="連線設定檔案"/>
電話號碼：	<input type="text"/>
使用者名稱：	<input type="text"/>
密碼：	<input type="password"/>
確認密碼：	<input type="password"/>
APN:	<input type="text"/>

- 輸入以下設定：
 - i** 提示：如果您不知道電話號碼、使用者名稱、密碼或其它設定，請諮詢您的 ISP，稍後從數據機 > 設定頁面設定數據機。

設定檔名稱	為設定檔輸入一個方便易記的名稱；預設為 我的連線設定檔 。
電話號碼	用於撥號的電話號碼。
使用者名稱	您的 ISP 使用者名稱。
密碼	您的 ISP 密碼。
確認密碼	再次輸入您的 ISP 密碼。
APN	您的 ISP 存取點名稱。

- 2 按下一步。此時顯示 **WAN 網路模式** 頁面。
- 3 移至第 15 頁「**WAN 網路模式**」。

WAN 網路模式

WAN 網路模式

選擇用來連接您的網際網路服務供應商 (ISP) 的方式：

- 基於路由器的連接 - 使用 **固定 IP** 位址或者 **IP 位址範圍**。
- 基於電纜/數據機的連接 - 使用 **DHCP** 指派的動態 IP 位址。
- **DSL 連接** - 使用 **PPPoE** 為 ISP 客戶驗證軟體。
- **VPN 連接** - 使用 **PPTP** 加密連接。

- ① **提示：**如果您按一下通訊協定名稱，會顯示一個快顯，描述此通訊協定以及您為什麼要使用它。例如，如果您按一下 **DHCP**，會顯示 DHCP 的描述：

DHCP 用戶端

DHCP 表示「動態主機設定協定」。該通訊協定用於自動分配 TCP/IP 設定。

SonicWall 包含 DHCP 用戶端和 DHCP 伺服器。用戶端用於透過 WAN 連結（例如，纜線數據機網路）從網路自動設定 SonicWall。ISP 需要使用 DHCP 用戶端以便從 DHCP 伺服器獲取位址。

此外，SonicWall 的 DHCP 伺服器用於設定 LAN 連結中的電腦。

- 1 選擇 WAN 網路模式：

基於路由器的連接 - 使用固定 IP 位址 為用於識別網路中每台裝置的數字。IP 位址由四個數字組成，以點分開，數字的值從 0 到 254。IP 位址範例：

192.168.168.1、10.0.0.1 或 216.217.36.130。這是 SonicWall 安全裝置的預設值。預設情況下已核取此選項。

網路中每個 IP 位址必須是獨一無二的。因此，不可以將網路中其它裝置使用的 IP 位址指派給 SonicWall。

基於纜線/數據機的連接 - 使用 DHCP 指派的動態 IP 位址。 DHCP 表示動態主機設定通訊協定。此協定用於自動指派 TCP/IP 設定。

SonicWall 安全裝置包含 DHCP 用戶端和 DHCP 伺服器。用戶端用於通過 WAN 連結（例如，纜線數據機網路）從網路自動設定 SonicWall。ISP 需要使用 DHCP 用戶端以便從 DHCP 伺服器獲取位址。

DSL 連接 - 將 PPPoE 用於 ISP 用戶端驗證軟體。 乙太網路點對點通訊協定 (PPPoE) 為管理 DSL 和有線寬頻服務廣泛部署的解決方案。PPPoE 需要使用者名稱和密碼驗證才能連接到網際網路。

VPN 連接 - 將 PPTP 用於加密的連接。 點對點通道通訊協定 (PPTP) 用於通過 IP 網路的通道點對點通訊協定。PPTP 需要伺服器 IP 位址、使用者名稱和密碼驗證以連接網際網路。

2 按下一步。顯示的下一個頁面取決於您的 WAN 網路模式選擇。

3 如果選擇：

- 基於路由器的連接，請移至第 16 頁「[WAN 網路模式：NAT 已啟用](#)」
- 基於電纜/數據機的連接，移至第 17 頁「[WAN 網路模式：通過 DHCP 用戶端進行 NAT](#)」。
- DSL 連接，請移至第 18 頁「[WAN 網路模式 - 通過 PPPoE 用戶端進行 NAT](#)」。
- VPN 連接，請移至第 19 頁「[WAN 網路模式：通過 PPTP 用戶端進行 NAT](#)」。

WAN 網路模式：NAT 已啟用

WAN 網路模式：NAT 已啟用

您需要填寫下列欄位才能連接網際網路。如果您沒有該資訊，請聯絡您的 ISP。

SonicWall WAN IP 位址：	<input type="text" value="192.168.95.55"/>
WAN 子網路遮罩：	<input type="text" value="255.255.255.0"/>
閘道 (路由器) 位址：	<input type="text" value="192.168.95.1"/>
DNS 伺服器位址：	<input type="text" value="192.168.95.1"/>
DNS 伺服器位址 #2(可選)：	<input type="text" value="8.8.8.8"/>

在該 WAN 介面上允許 HTTPS 管理

在該 WAN 介面上允許 Ping

警告：允許從 WAN 進行 HTTPS 管理會是個潛在的弱點。請從「[密碼設定指南](#)」頁面選擇優良的密碼。

按「[下一頁](#)」按鈕繼續進行。

1 位址設定已根據您的系統填入。請驗證它們是否正確。

i 附註：如果您不確定此資訊，請聯絡您的網際網路服務供應商 (ISP)。按一下選項/遮罩名稱中的連結，會出現含有位址/遮罩的說明的快顯。

SonicWall WAN IP 位址	IP 位址為用於識別網路中每台裝置的數字。IP 位址由四個數字組成，以點分開，數字的值從 0 到 254。IP 位址範例：192.168.168.1、10.0.0.1 或 216.217.36.130。 網路中每個 IP 位址必須是獨一無二的。因此，不可以將網路中其它裝置使用的 IP 位址指派給 SonicWall。
WAN 子網路遮罩	子網路遮罩定義哪些 IP 位址用於區域網路，哪些 IP 位址用於網際網路。例如，如果指派給電腦的 IP 位址為 192.168.168.200，子網路遮罩為 255.255.255.0，那麼電腦會認為所有的 192.168.168.x 位址是用於區域網路，而所有其他位址則用於網際網路。 WAN 子網路遮罩應當由 ISP 指派。如果不知道您的 WAN 子網路遮罩，則使用指派給電腦的子網路遮罩或聯絡 ISP。
閘道路由器位址	WAN 閘道（路由）位址是橋接您的網路和網際網路的路由器 IP 位址。WAN 路由器可以直接與 SonicWall 裝置的 WAN 連接埠相連，或通過纜線或 DSL 數據機間接相連。 WAN 閘道（路由）位址必須與 SonicWall 安全裝置的 WAN IP 位址在相同的子網路中。WAN 閘道（路由）位址通常以數字 .1 或 .254 結束。因此，如果 WAN IP 位址為 216.0.36.128，則閘道位址為 216.0.36.1 或 216.0.36.254。如果不知道閘道位址，請聯絡 ISP。
DNS 伺服器位址	DNS 伺服器位址是 DNS 伺服器的 IP 位址。
DNS 伺服器位址 #2 (選用)	如果存在第二個 DNS 伺服器位址，請輸入於此欄位中。

- 2 要允許 HTTPS，請勾選**允許該 WAN 介面的 HTTPS**。預設情況下已核取此選項。

 **注意：**允許從 WAN 管理 HTTPS 將造成潛在的攻擊。如果啟用此設定，請確保您已在此指南的「密碼」頁面或通過「管理」>「系統安裝」>「設備」>「基本設定」頁面輸入了一個強式密碼。

- 3 要允許 ping，請勾選**允許該 WAN 介面的 Ping**。預設情況下已核取此選項。
- 4 按**下一步**。即顯示 **LAN 設定** 頁面。
- 5 移至第 20 頁「**LAN 設定**」。

WAN 網路模式：通過 DHCP 用戶端進行 NAT

SonicWall DHCP 用戶端會自動嘗試為您的 SonicWall WAN 介面取得 IP 位址。

當您使用纜線數據機連線到 ISP 時，最常見的是 DHCP 式設定。如果您的 ISP 沒有提供您任何固定 IP 位址，則您將可自動取得 IP 位址。

WAN 網路模式：帶 NAT 的 DHCP 用戶端

SonicWall DHCP 用戶端將會自動嘗試為 SonicWall 的 WAN 介面獲取 IP 位址。

當您使用纜線數據機連接您的 ISP 時，DHCP 式的設定是最常見的。

如果您的 ISP 未向您提供任何固定 IP 位址，則很可能可以自動獲取 IP 位址。

- 允許該 WAN 介面的 HTTPS
- 允許該 WAN 介面的 Ping

警告：允許從 WAN 進行 HTTPS 管理會是個潛在的弱點。請從「密碼設定指南」頁面選擇優良的密碼。

1 要允許 HTTPS，請勾選允許該 WAN 介面的 HTTPS。預設情況下已核取此選項。

注意：允許從 WAN 管理 HTTPS 將造成潛在的攻擊。如果啟用此設定，請確保您已在此指南的「密碼」頁面或通過「密碼設定指南」輸入了一個強式密碼。

- 2 要允許 ping，請勾選允許該 WAN 介面的 Ping。預設情況下已核取此選項。
- 3 按下一步。LAN 設定頁面顯示。
- 4 移至第 20 頁「LAN 設定」。

WAN 網路模式 - 通過 PPPoE 用戶端進行 NAT

如果您有 DSL 連線，則必須提供您的 ISP 或網路管理員所提供的 PPPoE 帳戶資訊。

WAN 網路模式：帶 NAT 的 PPPoE 用戶端

請輸入您的 ISP 或網路管理員提供給您的 PPPoE 帳戶資訊。

請注意，PPPoE 密碼是區分大小寫的。

- 自動獲取 IP 位址
- 使用以下 IP 位址：

PPPoE 使用者名稱：

PPPoE 密碼：

- 非使用中狀態時中斷連接（分鐘數）： 10
- 允許該 WAN 介面的 HTTPS
- 允許該 WAN 介面的 Ping

1 選擇如何獲取 IP 位址：

自動

請勾選自動獲取 IP 位址；這是預設值。

移至步驟 2。

手動

請勾選使用以下 IP 位址。將啟用此欄位。
在此欄位中輸入 PPPoE IP 位址。

- 2 在 **PPPoE 使用者名稱** 欄位中輸入 PPPoE 使用者名稱。
- 3 在 **PPPoE 密碼** 欄位中輸入 PPPoE 密碼。
 - ① **附註：**密碼區分大小寫。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。
- 4 另外，要在一段時間非使用中之後中斷連接，請勾選**非使用中狀態時中斷連接（分鐘數）**。預設情況下未勾選此選項。選擇此選項時，將啟用此欄位。
 - a 在**非使用中狀態時中斷連接（分鐘數）**欄位中，輸入中斷連接前的最長非使用中時間（單位：分鐘）；預設值為 **10**，最小是 0（不允許任何時間），最大為 999 分鐘。
- 5 要允許 HTTPS，請勾選**允許該 WAN 介面的 HTTPS**。預設情況下已核取此選項。
 - △ **注意：**允許從 WAN 管理 HTTPS 將造成潛在的攻擊。如果啟用此設定，請確保您已在此指南的「密碼」頁面或通過「密碼設定指南」輸入了一個強式密碼。
- 6 要允許 ping，請勾選**允許該 WAN 介面的 Ping**。預設情況下已核取此選項。
- 7 按下一步。LAN 設定頁面顯示。
- 8 移至第 20 頁「LAN 設定」。

WAN 網路模式：通過 PPTP 用戶端進行 NAT

- ① **附註：**您必須提供 PPTP 伺服器 IP 位址、使用者名稱和密碼才能繼續。

WAN 網路模式：帶 NAT 的 PPTP 用戶端

PPTP 伺服器 IP 位址：

PPTP 使用者名稱：

PPTP 密碼：

自動獲取 IP 位址
 使用以下 IP 位址

SonicWall WAN IP 位址：

WAN 子網路遮罩：

閘道 (路由器) 位址：

允許該 WAN 介面的 HTTPS
 允許該 WAN 介面的 Ping

警告：允許從 WAN 進行 HTTPS 管理會是個潛在的弱點。請從「密碼設定指南」頁面選擇優良的密碼。

- 1 在 **PPTP 伺服器 IP 位址** 欄位中輸入 PPTP 伺服器的 IP 位址。
 IP 位址為用於識別網路中每台裝置的數字。IP 位址由四個數字組成，以點分開，數字的值從 0 到 254。IP 位址範例：192.168.168.1、10.0.0.1 或 216.217.36.130。
 網路中每個 IP 位址必須唯一。因此，不可以將網路中其它裝置使用的 IP 位址指派給 SonicWall。
- 2 在 **PPTP 使用者名稱** 欄位中輸入 PPTP 伺服器使用者名稱。
- 3 在 **PPTP 密碼** 欄位中輸入 PPTP 伺服器密碼。
- 4 選擇如何獲取 IP 位址：

- 自動 - 請勾選**自動獲取 IP 位址**；這是預設值。移至**步驟 5**。
- 手動 - 請勾選**使用以下 IP 位址**。以下欄位會變為可用。

a) 在 **SonicWall WAN IP 位址** 欄位中輸入裝置的 WAN 位址。

b) 在 **WAN 子網路遮罩** 欄位輸入 WAN 子網路遮罩。

子網路遮罩定義哪些 IP 位址用於區域網路，哪些 IP 位址用於網際網路。例如，如果指派電腦的 IP 位址為 192.168.168.200，子網路遮罩為 255.255.255.0，那麼電腦會認為所有的 192.168.168.x 位址是用於區域網路，而所有其它的位址則用於網際網路。

WAN 子網路遮罩由 ISP 指派。如果不知道您的 WAN 子網路遮罩，則使用指派給電腦的子網路遮罩或聯絡 ISP。

c) 在 **閘道（路由）位址** 欄位中，輸入閘道（路由器）位址。

5 要允許 HTTPS，請勾選**允許該 WAN 介面的 HTTPS**。預設情況下已核取此選項。

△ 注意：允許從 WAN 管理 HTTPS 將造成潛在的攻擊。如果啟用此設定，請確保您已在此指南的「密碼」頁面或通過「密碼設定指南」輸入了一個強式密碼。

6 要允許 ping，請勾選**允許該 WAN 介面的 Ping**。預設情況下已核取此選項。

7 按下一步。顯示 LAN 設定頁面。

8 移至第 20 頁「LAN 設定」。

LAN 設定

此頁面可讓您將 SonicWall 設為預設閘道。

LAN 設定

將 SonicWall 設定為預設閘道。

輸入 LAN IP 位址和子網路遮罩。

SonicWall LAN IP 位址:	192.168.168.168
LAN 子網路遮罩:	255.255.255.0

設定指南基於提供的設定自動填入 LAN 設定欄位。

1 驗證 LAN IP 位址和 LAN 子網路遮罩是否正確。

SonicWall LAN IP 位址

SonicWall LAN 的 IP 位址。網路中每個 IP 位址必須唯一。因此，不可以將網路中其它裝置使用的 IP 位址指派給 SonicWall。

LAN 子網路遮罩

子網路遮罩定義哪些 IP 位址用於區域網路，哪些 IP 位址用於網際網路。例如，如果指派電腦的 IP 位址為 192.168.168.200，子網路遮罩為 255.255.255.0，那麼電腦會認為所有的 192.168.168.x 位址是用於區域網路，而所有其它的位址則用於網際網路。

LAN 子網路遮罩定義區域網路的大小。LAN 子網路遮罩 255.255.255.0 適用於大多數網路。

2 按下一步。即顯示 LAN DHCP 設定頁面。

LAN DHCP 設定

DHCP（動態主機設定通訊協定）用於自動指派 TCP/IP 設定。DHCP 伺服器簡化了網路位址管理，節省了設定每台電腦 IP 設定所花費的大量時間。

- i** **重要：** SonicWall 裝置包含 DHCP 用戶端和 DHCP 伺服器。重要的是不會將 IP 位址混淆。
- 伺服器用於設定介面內部的電腦。此功能為可選項。
 - 相對而言，用戶端是用於通過 WAN 連接的網路 SonicWall 裝置的自動設定（例如，一個纜線數據機網路）。

此頁面可讓您輸入和設定 DHCP 伺服器。

LAN DHCP 設定

設定您的 DHCP 伺服器。

在 LAN 啟用 DHCP 伺服器

輸入 LAN 上您的網路裝置的 IP 位址範圍。位址範圍必須在與 SonicWall Web 管理位址相同的子網路內。SonicWall 的預設網道位址目前設定為：**192.168.168.168/255.255.255.0**。

以下範圍已存在。如果需要，可以在此處變更此範圍。

LAN 位址範圍： 到

1 勾選在 LAN 啟用 DHCP 伺服器核取方塊。預設情況下已勾選此核取方塊。

2 設定指南自動填充 LAN 位址範圍欄位。驗證位址是否正確。

輸入 LAN 上您網路裝置的 IP 位址範圍。此位址範圍必須與 SonicWall Web 管理位址在相同的子網路中。SonicWall 的預設網道位址目前依照已設定的 IP 位址設定。

3 按下一步。接下來顯示什麼取決於安全裝置為有線或無線。

4 如果您的安全裝置是：

有線

移至第 33 頁「設定摘要」

無線且部署情節為沒有無線

移至第 29 頁「連接埠指派」

無線且為任何其他部署情節

移至第 22 頁「調控網域註冊 (僅限無線平台)」

調控網域註冊 (僅限無線平台)

❶ | **重要：**您負責遵守法規區域和/或有關無線電運營場所規定的所有法規。

❷ | **附註：**法規區域從國家或地區代碼自動產生。

調控網域註冊

使用者有責任遵守所有為規範調控網域及/或有關無線電操作地區而制定的法令。請從以下清單選擇正確的國家/地區代碼。

法規區域：
國家/地區代碼：

1 從國家/地區代碼下拉功能表中選擇一個國家或地區。

❶ | **重要：**對於國際（非美國或日本）TZ 系列無線和 SOHO W 無線裝置，務必選擇裝置部署所在國家或地區的相應國家或地區代碼，即使您不是在此國家或地區內。對於部署在美國和日本的裝置，法規區域和國家或地區代碼是自動選擇的，且不能變更。

❷ | **重要：**如果您選擇加拿大的國家/地區代碼，除非您聯絡 SonicWall 支援部門，否則將無法變更。

2 按下一步。此時顯示一條有關在您的用戶端電腦上保持最新無線驅動程式的資訊訊息。

SonicWall 建議用戶端電腦上的無線驅動程式要保持在最新狀態，以獲得較佳的無線連線能力、相容性與效能。

在致電 SonicWall 技術支援部門提供任何無線連線與效能相關問題的協助之前，請先將用戶端電腦上的無線驅動程式升級至最新版本。

有關將驅動程式升級至最新版本，請參閱無線網路卡製造商的說明指示。

3 按一下**確定**。隨即顯示 **WLAN Radio** 設定頁面。

WLAN Radio 設定 (僅限無線平台)

此頁面可讓您為您的 SonicWall 設定 SSID、無線模式和操作頻道。

WLAN Radio 設定

設定 SSID, radio 模式, 和您的 SonicWall 操作通道。

SSID 作為您的無線網路的主要識別項。SSID 可能長達 32 個字元和數字的長度, 並且區分大小寫。

選擇期望的無線模式和您的 SonicWall 操作通道。

SSID:	<input type="text" value="sonicwall-1587"/>
無線電模式:	<input type="text" value="2.4GHz 802.11n/g/b 混合模式"/>
無線波段:	<input type="text" value="自動"/>
主要通道:	<input type="text" value="自動"/>
次要通道:	<input type="text" value="自動"/>
<input checked="" type="checkbox"/> 啟用短期守護間隔	
<input checked="" type="checkbox"/> 啟用彙總	
備註: 考慮到無線操作, 使用者必需遵守所有的法規政府和本機發佈的。	

- 1 在 **SSID** 欄位中輸入 SSID (服務集 ID)。SSID 作為您的無線網路的主要識別項。您可以指定最多 32 個英數字元; SSID 區分大小寫。裝置產生的預設 SSID 為 **sonicwall-** 加 BSSID (廣播服務集 ID) 的最後四個字元; 例如, **sonicwall-** 變為 **sonicwall-F2DS**。
- 2 從**無線電模式**下拉功能表中選擇慣用的無線模式。無線安全裝置支援**無線模式選擇**表格中顯示的模式。

附註: 可用選項會有改變, 具體取決於選擇的模式。如果為符合以下條件的模式設定無線設定:

- 支援 802.11n (除 5GHz 802.11n/a/ac 混合模式以外), 會顯示以下選項: **無線波段、主要通道、次要通道**。
- 不支援 802.11n, 則僅顯示**頻道**選項。
- 支援 5GHz 802.11n/a/ac 混合模式或 5GHz 802.11ac 單一模式, 此時顯示**無線波段和頻道**選項。

提示: 為使 802.11n 用戶端達到獨一無二的最佳傳送量速度, SonicWall 建議使用**僅 802.11n** 無線模式。對多個無線用戶端身分驗證的相容性, 可使用 **802.11n/b/g 混合模式**無線模式。為使 802.11ac 用戶端達到獨一無二的最佳傳送量速度, SonicWall 推薦使用**僅 802.11ac**無線模式。對多個無線用戶端身分驗證的相容性, 可使用 **802.11ac/n/a 混合模式**無線模式。

無線模式選擇

2.4GHz	5Ghz	定義
僅 2.4GHz 802.11n	僅 5GHz 802.11n	僅允許 802.11n 用戶端存取您的無線網路。802.11a/ac/b/g 用戶端不能在此受限的無線模式下連接。
2.4GHz 802.11n/g/b 混合模式 這是預設值。	5GHz 802.11n/a 混合 ^a	同時支援 802.11a、802.11b、802.11g, 和 802.11n 用戶端。如果無線網路包含多種類型的用戶端, 請選擇此模式。

無線模式選擇

2.4GHz	5GHz	定義
僅 2.4GHz 802.11g		如果您的無線網路僅包含 802.11g 用戶端，您可以選擇此模式，以提高 802.11g 的效能。如果想要避免 802.11b 用戶端關聯，也可以選擇此模式。
2.4GHz 802.11g/b 混合		如果您的無線網路包含 802.11b 和 802.11g 用戶端，您可以選擇此模式，以提高效能。
	5GHz 802.11a 單一模式	如果僅 802.11a 用戶端存取您的無線網路，則可選擇此模式。
	5GHz 802.11n/a/ac 混合模式	同時支援 802.11a、802.11ac，和 802.11n 用戶端。如果無線網路包含多種類型的用戶端，請選擇此模式。
	5GHz 802.11ac 單一模式	如果僅 802.11ac 用戶端存取您的無線網路，則可選擇此模式。

a. 802.11n/a 混合模式提供 802.11n 和 802.11a 用戶端無線連線。

SonicWall 建議單獨對於 802.11n 用戶端使用 802.11n 單一模式，以擁有最佳的傳送量。對多個無線用戶端連線相容性，使用 802.11n/a 混合模式。對 802.11a 無線用戶端連線相容性，使用 802.11a 單一模式。

3 如果您選擇的模式支援：

- 802.11a 單一模式、802.11g 單一模式，或 802.11g/b 混合模式，請移至[步驟 4](#)
- 5GHz 802.11ac 單一模式和 5GHz 802.11n/a/ac 混合模式，請移至[步驟 6](#)
- 802.11n 單一模式或 802.11n 混合模式（除 5GHz 802.11n/a/ac 混合模式之外），請移至[步驟 8](#)

4 僅針對 802.11a/g：從**頻道**下拉功能表中選擇用於無線電的頻道：

自動	使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。除非由於某種原因必須使用或避免使用特定的頻道，否則請使用 自動 。
特定的頻道	可以在法規區域範圍內選擇單個頻道。選擇特定的頻道還可幫助您避免受到此區域內其他無線網路的干擾。 附註： 可用頻道取決於安全裝置中的無線電類型和您的法規區域。

5 移至[步驟 11](#)。

6 對於 802.11ac，此時顯示**無線波段**和**頻道/標準頻道**選項。

從**無線波段**下拉功能表中，選擇 802.11a 或 802.11ac 無線電的無線波段：

自動	使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。 附註： 頻道下拉功能表設定為 自動 ，無法變更。
標準 - 20 MHz 頻道	指定 802.11ac 無線將僅使用標準 20 MHz 頻道。這是預設值。 選擇此選項時，從 頻道 下拉功能表中，選擇一個法規區域範圍內的單個頻道。選擇特定的頻道還可幫助您避免受到此區域內其他無線網路的干擾。 附註： 可用頻道取決於安全裝置中的無線電類型和您的法規區域。

寬 - 40 MHz 頻道 指定 802.11ac 無線將僅使用寬頻 40 MHz 頻道。選定此選項後，將顯示**頻道**下拉功能表。

附註：可用頻道取決於安全裝置中的無線電類型和您的法規區域。

寬 - 80 MHz 頻道 指定 802.11n 無線將僅使用寬頻 80 MHz 頻道。選定此選項後，將顯示**頻道**下拉功能表。

附註：可用頻道取決於安全裝置中的無線電類型和您的法規區域。

7 移至**步驟 11**。

8 對於 802.11n 單一模式或 802.11n 混合模式，此時顯示**無線波段**、**主要通道**，和**次要通道**設定：

無線電模式：	5GHz 802.11n/a 混合模式
無線波段：	自動
主要通道：	自動
次要通道：	自動

從**無線波段**下拉功能表中，選擇適用於 802.11n 或 802.11ac 無線電的頻段：

自動 使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。這是預設值。

附註：主要通道和次要通道下拉功能表設定為**自動**，無法變更。

標準 - 20 MHz 頻道 指定 802.11n 無線將僅使用標準 20 MHz 頻道。選擇此選項時，會顯示**頻道**下拉功能表，而非**主要通道**和**次要通道**下拉功能表。

標準通道 預設情況下，此項設定為**自動**，使裝置可以根據訊號強度和完整性設定最佳頻道。您也可以在此區域的範圍內選擇單個頻道。選擇特定的頻道還可幫助您避免受到此區域內其他無線網路的干擾。

附註：可用頻道取決於安全裝置中的無線電類型和您的法規區域。

寬 - 40 MHz 頻道 指定 802.11n 無線將僅使用寬頻 40 MHz 頻道。選定此選項後，將顯示**主要通道**和**次要通道**下拉功能表：

主要通道 預設情況下設定為**頻道 36 (5180MHz)**。您可以選擇指定的其他頻道或**自動**。

附註：可用頻道取決於安全裝置中的無線電類型和您的法規區域。

次要通道 無論主要通道設定是怎樣的，此下拉功能表的設定設為**自動**。

9 另外，可勾選**啟用短期保護間隔**核取方塊，相對於 800ns 的標準防護間隔，指定一個 400ns 的短期防護間隔。預設情況下未勾選此設定。

附註：如果選擇**5GHz 802.11g/b 混合模式**、**5GHz 802.11a 單一模式**，或**2.4GHz 802.11g 單一模式**，此選項無法使用。

防護間隔是為了確保不同的傳送不會互相干擾而設計的傳送之間間隔的設定時間。防護間隔可避免傳播延遲、回應以及反射。存取點會將在此間隔內收到的任何訊號內容識別為不需要的符號間干擾，並拒絕此資料。防護間隔是傳送時的間隔，目的在於避免由於受到干擾或多路徑延遲造成的資料遺失。

802.11n 標準指定兩種防護間隔：400ns（短）和 800ns（長）啟用短期保護間隔可以透過減少每個裝置不必要的空閒時間來降低網路開銷。400 毫微秒 (ns) 的短期防護間隔，適用於大多數辦公室環境，因為反射點之間以及用戶端之間的距離短。將迅速接收大多數反射。防護間隔越短，頻道使用效率越高，但是較短防護間隔也會增大干擾風險

然而，一些室外部署，可能需要更長的防護間隔。隨著區域的變大，例如在倉庫或戶外環境中，在短期防護間隔結束後反射和回應很可能會繼續，所以對 800 ns 的長期防護間隔的需求變得更加重要。

- 10 另外，要啟用 802.11n 框架彙總（此功能將多框架結合以降低開銷和提高傳送量），請勾選**啟用彙總**核取方塊。

i 附註：如果選擇 5GHz 802.11g/b 混合模式、5GHz 802.11a 單一模式，或 2.4GHz 802.11g 單一模式，此選項無法使用。

資料通過無線網路作為封包流（稱為資料框架）傳送。框架彙總可將這些封包彙總到更少、更大的封包中，因此可提升整體效能。框架彙總已新增到 802.11n 規範中，可獲得效能的額外提升。框架彙總是只有 802.11ac 和 802.11n 用戶端才能利用的一項功能，因為舊系統無法理解更大封包的新格式。

i 提示：啟用短期保護間隔和啟用彙總選項可稍微提高傳送量。當使用者具有較強的訊號且干擾較小時，它們可以在最佳的網路條件下發揮最大作用。在達不到最佳條件的網路中（受到干擾、訊號較弱等），這些選項可能會導致傳送錯誤，從而削弱傳送量中的任何有效增益。

- 11 按下一步。隨即顯示 **WLAN 安全設定** 頁面。

WLAN 安全設定 (僅限無線平台)

此頁面可讓您設定 SonicWall 安全裝置的 WLAN 安全設定。如需這些設定的更多資訊，請參見 [SonicOS 連線指南](#)。

WLAN 安全設定

最佳化您的 SonicWall 的 WLAN 安全能力。

選擇以下一個安全模式用於您的 SonicWall。

- WPA2/WPA2-AUTO 模式** - Wi-Fi 安全存取 (WPA) 是安全的無線通訊協定，以 802.11i 標準為基礎。這也是在您的無線用戶端支援 WPA 情況下推薦的通訊協定。
- 連線性 - 警告！** 該模式不提供加密或者存取控制並且允許無限制的無線連接到該裝置。

- 1 選擇一種安全模式：

WPA2/WPA2-AUTO 模式

Wi-Fi 防護接入 (WPA) 模式是基於 802.11i 標準的安全無線通訊協定。這也是在您的無線用戶端支援 WPA/WPA 協定情況下的推薦通訊協定。預設情況下已核取此選項。

連線 (預設)

此模式允許對裝置有無限制的無線存取。

注意：此模式不提供加密或存取控制。

2 按下一步。下一個頁面取決於您的選擇：

此選項	顯示	移至
WPA/WPA2 模式	WPA/WPA2 模式設定頁面	第 27 頁「WPA/WPA2 模式設定 (僅限無線平台)」
連線能力	WLAN VAP (虛擬存取點) 設定頁面	第 28 頁「WLAN VAP (虛擬存取點) 設定 (僅限無線平台)」

WPA/WPA2 模式設定 (僅限無線平台)

此頁面可讓您設定 SonicWall 安全裝置的 WPA/WPA2 設定。如需這些設定的更多資訊，請參見 *SonicOS 連線指南*。

WPA模式設定

為 SonicWall 設定 WPA 設定。

驗證類型：

WPA2/WPA 設定

加密類型：

群組金鑰更新：

間隔 (秒數)：

預先共用金鑰設定 (PSK)

複雜密碼：

1 從**驗證類型**下拉功能表中，選擇：

- WPA2-PSK (預設)
- WPA2-EAP
- WPA2-自動-PSK
- WPA2-自動-EAP

部分選項變更取決於您的選擇。

2 從**加密類型**，選擇：

- AES (預設)
- TKIP
- 自動

3 從**群組金鑰更新**，選擇：

- 逾時 (預設)
- 已停用 - 間隔 (秒數) 欄位未顯示，因為「群組金鑰更新」從未逾時。

- 在**間隔 (秒數)** 欄位中，輸入「群組金鑰更新」的有效逾時間隔。最小為 30 秒，最大為 2592000 秒 (30 天)，預設值為 **86400** 秒 (24 小時)。
- 會顯示哪些選項取決於您選擇的**驗證類型**：

如果選擇	移至
PSK	步驟 6
AES	步驟 8

- 在**密碼**欄位中，輸入要使用的密碼。

預先共用金鑰設定 (PSK)

複雜密碼：

- 移至[步驟 11](#)。

- 在**Radius 伺服器 IP** 欄位中，輸入 Radius 伺服器的 IP 位址。

可擴充驗證通訊協定設定 (EAP)

Radius 伺服器 IP 1： 連接埠：

Radius 伺服器密碼 1：

Radius 伺服器 IP 2： 連接埠：

Radius 伺服器密碼 2：

- 在**連接埠**欄位中，輸入伺服器的連接埠編號。
- 在**Radius 伺服器密碼**欄位中，輸入用於 Radius 伺服器的密碼。
- 按下一步。如果您指定了：
 - PSK 複雜密碼，會顯示 [WLAN VAP \(虛擬存取點\) 設定 \(僅限無線平台\)](#) 頁面。
 - Radius 伺服器，會在 [WLAN VAP \(虛擬存取點\) 設定 \(僅限無線平台\)](#) 頁面之前顯示一則有關更新安全裝置存取規則的訊息。

防火牆的存取規則將在 WAN 介面上為 Radius 伺服器自動更新

WLAN VAP (虛擬存取點) 設定 (僅限無線平台)

設定指南自動建立一個 VAP SSID。您可以透過此頁面建立多達六個以上的 VAP。

WLAN VAP (虛擬存取點) 設定

VAP SSID

您已經建立了 1 SSID: **sonicwall-1587**

您要建立其他的虛擬存取點嗎？

是的，我要建立其他的虛擬存取點。

備註：您最多可以建立 7 個虛擬存取點。

- 1 自動建立一個 VAP SSID (請參見第 22 頁「[WLAN Radio 設定 \(僅限無線平台\)](#)」)。若要：
 - 跳過建立更多 VAP，請移至[步驟 5](#)。
 - 建立另一個 VAP，請勾選**是的，我要建立其他的虛擬存取點**核取方塊。將顯示更多選項。

VAP SSID:

WLAN 安全設定

為該 VAP 選擇一種安全模式。

WPA2/WPA2-AUTO 模式 - Wi-Fi 安全存取 (WPA) 是安全的無線通訊協定，以 802.11i 標準為基礎。
這也是在您的無線用戶端支援 WPA 情況下推薦的通訊協定。

連線性 - 警告！ 該模式提供了無加密或者存取控制並且允許無限制的對裝置的無線存取。

- 2 在 **VAP SSID** 欄位中輸入 VAP 的名稱。
- 3 選擇一種安全模式：
 - **WPA2/WPA2-Auto 模式** - Wi-Fi 安全存取 (WPA) 模式是安全的無線通訊協定，以 802.11i 標準為基礎。這也是在您的無線用戶端支援 WPA/WPA 協定情況下的推薦通訊協定。
 - **連接 (預設)** - 此模式允許對裝置有無限制的無線存取。

 **注意：**此模式不提供加密或存取控制。

- 4 要指定最多 6 個新 VAP，重複[步驟 2](#) 和 [步驟 3](#)。
- 5 按下一步。即顯示[連接埠指派](#)頁面。

連接埠指派

此頁面可讓您選擇初始連接埠指派。

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器

1 請選擇將如何指派連接埠：

- 使用目前的 - 此設定保持您的目前設定。預設情況下已核取此選項。
 - a) 要查看目前連接埠設定，請將滑鼠放在資訊 ⓘ 圖示上面。此時顯示一個工具提示顯示目前連接埠指派：



- 預設 WAN/LAN 交換器 - 此選項在頁面底部顯示連接埠設定：

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器

Diagram showing the physical ports on the device:

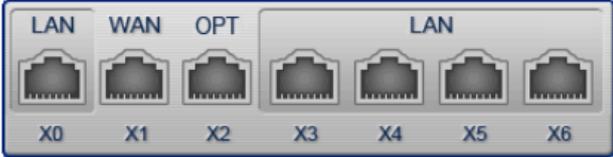
- LAN (X0)
- WAN (X1)
- LAN (X2, X3, X4, X5, X6)

- WAN/OPT/LAN 交換器 - 此選項在頁面底部顯示連接埠設定：

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器



按「下一頁」按鈕繼續進行。

- WAN/LAN/HA - 此選項在頁面底部顯示連接埠設定：

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器



按「下一頁」按鈕繼續進行。

- WAN/LAN/LAN2 交換器 - 此選項在頁面底部顯示連接埠設定：

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器



按「下一頁」按鈕繼續進行。

- 2 按下一步。會顯示摘要頁面。

設定摘要

SonicWall 設定摘要

辦公室閘道

WAN 介面 - NAT 已啟用 (已指派固定 IP)
IP 位址 : 192.168.95.55
子網路遮罩 : 255.255.255.0
閘道 : 192.168.95.1
DNS : 192.168.95.1, 8.8.8.8

允許 HTTPS: 是
允許 Ping: 是

Modem 介面 - 停用

WLAN 介面 - 具有 DHCP 伺服器的閘道 172.16.31.1 已啟用
SSID : sonicwall-1587
無線模式 : 5GHz 802.11n/a 混合
國家/地區代碼: JP
無線波段 : 自動 主要通道 : 自動 次要通道: 自動
安全模式 : 連線模式

虛擬存取點
無 VAP

LAN 介面 - 已啟用
IP 位址 : 192.168.168.168
子網路遮罩 : 255.255.255.0
DHCP 已啟用 : 192.168.168.1 - 192.168.168.167

連接埠指派
無變化

若要使用這些設定，請按一下「套用」。

- ① 附註：SonicWall 設定摘要顯示的內容取決於您輸入的設定。如果您已設定 TZ 系列無線或 SOHO W 無線裝置，但在部署情節頁面上勾選無無線，則會顯示無無線：

SonicWall 設定摘要

無無線

WAN 介面 - NAT 已啟用 (已指派固定 IP)
IP 位址 : 192.168.95.55
子網路遮罩 : 255.255.255.0
閘道 : 192.168.95.1
DNS : 192.168.95.1, 8.8.8.8

- 3 驗證設定是否是您所需要的。
- 4 按一下**套用**。將顯示一條訊息，提示設定正在進行更新：



設定更新完成後，會顯示設定完成頁面。

設定指南已完成

設定指南已完成

恭喜! 您已成功完成 SonicWall 設定指南。您可在此查看其他選項和進階設定選項: SonicWall Web 管理介面。請注意，從現在起您將登入 Web 管理介面，於：

URL : **http(s)://192.168.95.55/**

使用者名稱 : **admin**

密碼 : **<之前設定的密碼>**

您可以選擇按一下 [此處](#) 或者存取 [SonicWall 網站](#) 來註冊您的裝置。

在您能夠善用韌體更新和其他選用功能之前，這會是必要的。

- 1 如果您還未註冊裝置，現在可以透過按一下句中的兩個連結之一完成此操作，**接下來，您應該按一下這裡或存取 SonicWall 網站註冊您的裝置。**此時設定指南關閉，您會重新導向到相應位置。
- 2 按一下關閉。

使用 PortShield 介面指南

❗ | 附註：PortShield 介面指南僅可在 TZ 系列和 SOHO W 安全裝置上使用。

- 第 35 頁「PortShield 介面指南」

PortShield 介面指南

可以使用 **PortShield 介面指南** 選擇 SonicWall TZ 系列和 SOHO W 安全裝置的整合管理 LAN 交換器中的初始連接埠指派。

選擇連接埠指派：

- 1 按一下 SonicWall 管理介面上方的**快速設定**。顯示**快速設定歡迎**頁面。

歡迎

歡迎使用設定指南

選取以下其中一個指南，助您輕鬆設定 SonicWall:

- **設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- **PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- **公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- **VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- **無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- **App Rule 指南** - 設定 App Rule 的安全性功能
- **WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

❗ | 附註：可用的指南取決於您系統的設定。

- 2 選擇 **PortShield 介面指南**。

3 按下一步。此時顯示連接埠指派頁面。



1 請選擇將如何指派連接埠；出現的圖形顯示介面連接埠的指派：

- 使用目前的 - 此設定保持您的目前設定。預設情況下已核取此選項。

要查看目前連接埠設定，請將滑鼠放在資訊圖示上面。工具提示會顯示目前的連接埠指派：



① 附註：以下選項會在頁面底部顯示連接埠設定：

- 基本的 WAN/LAN 交換器：

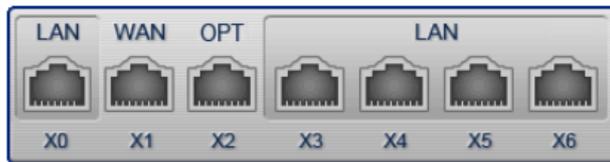


- WAN/OPT/LAN 交換器:

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器



按「下一頁」按鈕繼續進行。

- WAN/LAN/HA:

連接埠指派

為 SonicWall 選擇指派初始連接埠。

- 使用目前的 ⓘ - 使用此選項保持目前的設定。
- 預設 WAN/LAN 交換器
- WAN/OPT/LAN 交換器
- WAN/LAN/HA
- WAN/LAN/LAN2 交換器



按「下一頁」按鈕繼續進行。

- WAN/LAN/LAN2 交換器:



- 2 按下一步。摘要頁面顯示您在指南中指派的連接埠的摘要。確認設定；如需修改任何設定，按一下後退返回到連接埠指派頁面。



- 3 按一下套用。將顯示一條訊息，提示設定正在進行更新：



設定更新完成後，會顯示完成對話方塊。



- 4 按一下關閉。

使用公用伺服器指南

- 第 39 頁「公用伺服器指南」

公用伺服器指南

您使用公用伺服器指南來帶領您逐步完成設定 SonicWall 安全裝置，以提供對內部伺服器的公用存取。

要設定內部伺服器的公用存取權：

- 1 按一下快速設定管理介面上方的**快速設定**。顯示**歡迎**頁面。

歡迎

歡迎使用設定指南
選取以下其中一個指南，助您輕鬆設定 SonicWall:

- **設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- **PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- **公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- **VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- **無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- **App Rule 指南** - 設定 App Rule 的安全性功能
- **WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

① | 附註：可用的指南取決於您系統的設定。

- 2 選擇公用伺服器指南。
- 3 按下一步。隨即顯示**公用伺服器類型**頁面。

公用伺服器類型

公用伺服器類型

請選擇您要提供公用存取權的伺服器類型。選擇其中一個預先定義的伺服器，將會預設為一般與該伺服器類型關聯的服務。您可以取消勾選不要的伺服器，但是必須至少選擇一項服務。

如果未列出特別服務，您可以選擇 '其他' 並在下列步驟中您將有機會建立新的服務或者定義包含您的所有需求的服務群組。

伺服器類型：

服務：
 HTTP (TCP 80)
 HTTPS (TCP 443)

按「下一頁」按鈕繼續進行。

- 1 從**伺服器類型**下拉功能表中選擇伺服器類型：
 - Web 伺服器（預設）
 - FTP 伺服器
 - 郵件伺服器
 - 終端服務伺服器
 - 其他
- 2 從**服務**選項選擇要使用的服務。選擇哪個選項取決於伺服器類型。除 **FTP 伺服器**和**其它**以外，您可以選擇不止一種服務。預設情況下，除非**伺服器類型**選擇**其他**，否則會選擇所有服務。

伺服器類型	選擇
Web 伺服器	<ul style="list-style-type: none">• HTTP (TCP 80)• HTTPS (TCP 443) <p>注意：允許從 WAN 管理 HTTPS 將造成潛在的攻擊。</p>
FTP 伺服器	<ul style="list-style-type: none">• FTP (TCP 21)
郵件伺服器	<ul style="list-style-type: none">• SMTP (TCP 25)• POP3 (TCP 110)• IMAP (TCP 143)
終端服務伺服器	<ul style="list-style-type: none">• Microsoft RDP (TCP 3389)• Citrix ICA (TCP 1494)

伺服器類型

選擇

其他

從**服務**下拉功能表中選擇服務，或者建立一個新服務或群組。

The screenshot shows a configuration window with the following elements:

- 伺服器類型 :** 其他 (Other)
- 服務 :** A dropdown menu is open, showing a list of services. The top two items are "-選擇服務-" (Select Service). Below them are "建立新服務..." (Create New Service...) and "建立新群組..." (Create New Group...). The list continues with: 任何 (Any), AD Directory Services, AD Server, NT Domain Login, HTTP, HTTP Management, HTTPS, HTTPS Management, SonicWALL SSO Agents, SonicWALL TS Agents, RADIUS Accounting, IDENT, IMAP3, IMAP4, ISAKMP, LDAP, and LDAP (UDP).
- 按「下一頁」按鈕** (Click the "Next Page" button)
- 結束指南** (End Guide) button at the bottom left.

- 3 按下一步。隨即顯示**專用網路**頁面。

私人網路

伺服器專用網路設定

請輸入可識別此伺服器的名稱和伺服器的私人 (內部) IP 位址。將會視需要使用您提供的名稱和 IP 位址資訊，建立代表私人伺服器的網路物件，並將其指派至適當的區域。

您可以輸入選擇性的註解，以協助進一步識別伺服器。

如果您不知道此資訊，請在繼續之前聯絡伺服器的管理員或您的網路管理員。

伺服器名稱 :	<input type="text"/>
伺服器專用 IP 位址 :	<input type="text" value="0.0.0.0"/>
伺服器註解 :	<input type="text"/>

- 1 在**伺服器名稱**欄位中輸入易記的名稱。

- 2 在**伺服器私人 IP 位址**欄位中輸入伺服器的 IP 位址。指定指派到伺服器所在區域的位址範圍中的一個 IP 位址。**公用伺服器指南**會自動將伺服器指派到其 IP 位址所屬的區域。
 - ① **附註：**如果您輸入的 IP 位址與一個現有網路物件相符合，將重新命名此物件為您在此處指定的伺服器名稱。
- 3 另外，可以在**伺服器註解**欄位中輸入一個註解，以便進一步識別此公用伺服器。
- 4 按**下一步**。隨即顯示**伺服器公用資訊**頁面。

伺服器公用資訊

伺服器公用資訊

請指定伺服器的公用 (外部) IP 位址。預設值為您的 SonicWall WAN 介面的位址，並且應只有此伺服器將透過網際網路以不同的位址存取時才加以變更。

指定不同位址將導致公用伺服器網路物件的建立繫結至 WAN 區域。

如果不瞭解此位址，最好保留預設值。

伺服器公用 IP 位址：

- 1 在**伺服器公用 IP 位址**欄位中指定伺服器的公用 (外部) IP 位址。預設值為您的 SonicWall 安全裝置的公用 IP 位址。
 - ① **重要：**只有當在網際網路上用不同的位址存取此伺服器時，才可以變更此伺服器的公用 IP 位址。
如果您輸入不同 IP，公用伺服器指南將為此 IP 位址建立位址物件，並將位址物件與 WAN 區域繫結。
如果不瞭解此位址，最好保留預設值。
- 2 按**下一步**。會顯示**摘要**頁面。

公用伺服器設定摘要

公用伺服器設定摘要

請檢查以下設定並按一下「套用」以建立下列新物件。

伺服器位址物件

1. 建立指派到主機 192.168.10.1 的 LAN 區域的 'Huhcorp VoIP Server Private'。
2. 重用指派到 192.168.95.55 的 WAN 區域的 'X1 IP' 位址物件。

伺服器服務群組物件

1. 建立 'Huhcorp VoIP Server Services' 和 HTTP 和 HTTPS 服務。

伺服器 NAT 原則

1. 建立輸入伺服器 NAT 原則，以將原始目的地 'X1 IP' 的資料重新寫入已轉換的目的地 'Huhcorp VoIP Server Private'。
2. 建立輸出伺服器 NAT 原則，以將 'Huhcorp VoIP Server Private' 中的封包重新寫入已轉換的來源 'X1 IP'。
3. 建立回繞 NAT 原則，以允許從內部區域存取公用 IP 位址 192.168.95.55 上的伺服器。

伺服器存取規則

1. **WAN > LAN** - 允許「任何」到 'X1 IP' 的服務群組 'Huhcorp VoIP Server Services'。
將所有安全度較低的區域中的規則建立到 LAN 區域。

1. 摘要頁面顯示您在指南中選擇之設定的摘要。確認設定；如需修改任何設定，按一下**後退**返回到適當頁面。

對此物件

指南會建立

伺服器位址物件

新伺服器的位址物件。因為本例中新增的伺服器的 IP 位址在指派給 DMZ 的 IP 位址範圍內，指南會將位址物件與 DMZ 區域繫結。這會為物件提供一個名稱，即您為伺服器指定的名稱加上 `_private`。

如果您指定另一區域範圍內的 IP，會將位址物件與此區域繫結。如果您指定的 IP 位址超出已設定的任何區域範圍，指南會將位址物件與 LAN 區域繫結。

因為本例中的伺服器使用**伺服器公用 IP 位址**的預設 WAN IP 位址，指南說明在建立新伺服器與 WAN 之間的原則時將使用現有的 WAN 位址物件。如果您指定另一位址，伺服器為繫結到 WAN 區域的此位址建立物件，並為新位址物件指派您為伺服器指定的名稱加上 `_public`。

伺服器服務群組物件

新伺服器所使用服務的服務群組物件。本例中的伺服器是 Web 伺服器，因此服務群組包含 HTTP 和 HTTPS。這樣，您有在建立或編輯此伺服器的存取原則時可以使用便捷的群組。

伺服器 NAT 原則

NAT 原則以將有新服務群組中一項服務，定址為 WAN 位址的所有輸入封包的目的地位址，轉譯為新伺服器的位址。因此，在本例中，如果有 HTTPS 服務類型的封包輸入且定址為 WAN 介面 (10.0.93.43)，NAT 原則將此位址轉譯為 172.22.2.44。

指南還會建立回送 NAT 原則，將來自網路內部並定址為 WAN IP 位址的 HTTP 和 HTTPS 流量轉譯回郵件伺服器的位址。

伺服器存取規則

存取原則允許從 WAN 區域到 DMZ 的所有郵件服務流量。

- 按一下**套用**。將顯示一條訊息，提示設定正在進行更新：



設定更新完成後，會顯示**共用伺服器指南完成**頁面。



提示：用於從內部和外部存取新伺服器的新 IP 位址，會顯示在**設定**頁面的 URL 欄位中。

- 按一下**關閉**按鈕關閉指南。

使用 VPN 指南

- 第 45 頁「VPN 指南」
 - 第 45 頁「設定站台對站台 VPN」
 - 第 51 頁「建立 WAN GroupVPN」

VPN 指南

VPN 指南指導您逐步完成建立新的站台對站台 VPN 原則或設定 WAN GroupVPN，以接受來自 Global VPN Client 的連接。在設定完成後，指南會為選擇的 VPN 原則建立所需的 VPN 設定。您可以使用 SonicWall 管理介面選擇可選的進階設定選項。

主題：

- 第 45 頁「設定站台對站台 VPN」
- 第 51 頁「建立 WAN GroupVPN」

設定站台對站台 VPN

您可使用 **VPN 指南** 建立站台對站台 VPN 原則。

設定站台對站台 VPN 的方法是：

- 1 按一下快速設定管理介面上方的**快速設定**。顯示**歡迎**頁面。

歡迎

歡迎使用設定指南

選取以下其中一個指南，助您輕鬆設定 SonicWall:

- **設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- **PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- **公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- **VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- **無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- **App Rule 指南** - 設定 App Rule 的安全性功能
- **WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

❗ 附註：可用的指南取決於您系統的設定。

- 2 選擇 **VPN 指南**：
- 3 按下一步。隨即顯示 **VPN 原則類型** 頁面。

VPN 原則類型

VPN 原則類型

請選擇您想要設定的 VPN 原則類型。

站台對站台 - 快速設定一個連接到另一個 SonicWall 裝置的站台對站台 VPN 連接。

WAN GroupVPN - 快速設定 WAN GroupVPN 以接受從全域 VPN 用戶端傳入的VPN 連接。

- 1 選擇**站台對站台**。
- 2 按下一步。將顯示**建立站台間原則**頁面。

建立站台間原則

建立站台間原則

請輸入您要指派給此站對站 VPN 原則的唯一名稱，以及要用於通道的預先共用金鑰。

如果您知道遠端對等 IP 位址或完整的網域名稱，請勾選核取方塊並在以下 '遠端對等 IP 位址' 方塊中輸入資訊。

原則名稱：

預先共用的金鑰：

知道自已的遠端對等 IP 位址 (或 FQDN)：

遠端對等 IP 位址 (或 FQDN):

i | 提示：如果您已建立原則，快速設定會填充欄位。

- 1 在**原則名稱**欄位中，輸入用於指稱原則的名稱。例如波士頓辦公室。
- 2 在**預先共用的金鑰**欄位中，輸入用於在 IKE 階段 1 交涉期間驗證流量的字元字串。您可以使用 SonicWall 產生的預設預先共用密碼。
- 3 若要讓 SonicWall 能夠以知道的遠端對等發起聯絡，請勾選**知道自已的遠端對等 IP 位址 (或 FQDN)**。預設情況下未勾選此選項。
如果未勾選此選項，對等項必須啟動聯絡才能建立 VPN 通道，而安全裝置才會使用加強模式進行 IKE 交涉。
- 4 如果勾選**知道自已的遠端對等 IP 位址 (或 FQDN)**，請在**遠端對等 IP 位址 (或 FQDN)** 欄位中輸入遠端對等項的 IP 位址或完整的網域名稱 (FQDN)，例如 `boston.yourcompany.com`。預設值為 `0.0.0.0`。
- 5 按下一步。將顯示**網路選擇**頁面。

選擇網路

網路選擇

請選擇您希望可透過此站對站 VPN 通道存取的網路。如果您尚未為 VPN 通道的每一端建立網路物件，您可以選擇「建立新位址群組/物件...」選項 (在「區域和目的地網路」中)，建立新的物件。

如果您需要存取 VPN 通道的每一端一個以上的 IP 子網路，請建立子網路物件群組，並將群組指定為區域/目的地網路

本機網路：

目的地網路：

- 1 從**本機網路**選擇受此 SonicWall 防護且連接至此 VPN 的本機網路資源。您可以選擇裝置上的任意位址物件或群組，包括網路、子網路、各伺服器及介面 IP 位址。預設為 **Firewalled Subnets**。

如果您需要的物件或群組尚未建立，請選擇**建立新位址物件**或**建立新位址群組**。在出現的對話方塊中建立新物件或群組。然後選擇新物件或群組。

有關如何建立新的：

- 位址物件，請參見第 47 頁「[建立位址物件](#)」。
- 位址群組，請參見第 48 頁「[建立位址群組](#)」。

- 2 從**目的地網路**選擇 VPN 通道的目的地端的網路資源。如果此物件或群組不存在，請選擇**建立新位址物件**或**建立新位址群組** (更多資訊，請參見[步驟 1](#))。
- 3 按下一步。將顯示安全設定頁面。

建立位址物件

- 1 選擇**建立新位址物件**。此時會顯示**新增位址物件**對話方塊。

名稱：

區域指派：

類型：

IP 位址：

- 2 在**名稱**欄位中，輸入可用於指稱位址物件的名稱。
- 3 從**區域指派**選擇位址物件所屬的區域，例如 **VPN**。預設為 **DMZ**。
- 4 從**類型**選擇位址物件的類型；選項變更是基於您的選擇：
 - 主機 (預設)

類型：

IP 位址：

在 IP 位址中，輸入主機的 IP 位址。

- 範圍



請在**起始 IP 位址**和**結束 IP 位址**欄位中分別輸入起始和結束 IP 位址。

- 網路

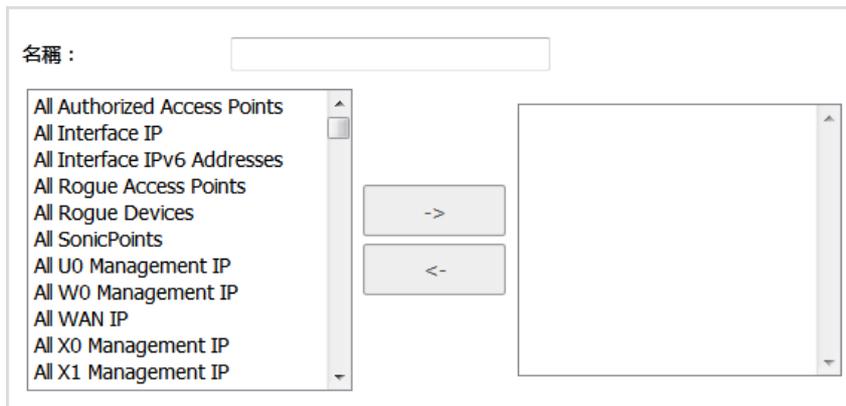


請在**網路**和**網路遮罩/首碼長度**欄位中分別輸入網路 IP 位址和網路遮罩/首碼長度。

- 5 按一下**確定**建立群組並返回到**網路選擇**頁面。
- 6 從**目的地網路**下拉功能表，選擇新建立的群組。

建立位址群組

- 1 選擇**建立新位址群組**。隨即顯示**新增位址物件群組**對話方塊。



- 2 在**名稱**欄位中，輸入可用於指稱位址群組的名稱，例如 **LAN 群組**。
- 3 從左邊的清單選擇 **LAN 子網路**。
- 4 按一下**向右的箭頭**按鈕。
- 5 按一下**確定**建立群組並返回到**網路選擇**頁面。
- 6 從**目的地網路**下拉功能表，選擇新建立的群組。

安全性設定

安全設定

請選擇您要用於 IKE 階段 1 和 IPSEC 階段 2 的安全性設定。如果您要求更具體的安全性設定，可調整本精靈完成後的新站台對站台 VPN 原則 (在完成本指南之後)。

附註：全域 VPN 用戶端 1.x 版無法使用 AES 加密，所以如果您選擇此方法，則只能連接全域 VPN 用戶端 2.x 版和以上版本。

DH 群組：	群組 2
加密：	3DES
驗證：	SHA-1
存留時間 (秒數)：	28800

- 1 在安全設定頁面，選擇用於 IKE 階段 1 和 IPSEC 階段 2 的安全設定。如果您需要更多特定的安全設定，可以在此指南完成後調整站台對站台 VPN 原則。
 - 您可以使用預設值。移至 [步驟 6](#)。
 - 選擇其他安全性設定。
- 2 從 **DH 群組**，選擇 Diffie-Hellman (DH 或 ECP) 群組，供數值 VPN 在 IKE 交涉期間使用，以建立金鑰對。隨後的各 DH 群組使用更大的數值作為開頭。如需 DH 群組選項，請參見 [Suite B 加密中內含的 Diffie Hellman 群組](#) 表格。

Suite B 加密中內含的 Diffie Hellman 群組

Diffie-Hellman (DH)	橢圓曲線加密 (ECP)
組 1	256 位隨機 ECP 群組
群組 2 (預設)	384 位隨機 ECP 群組
組 5	521 位隨機 ECP 群組
組 14	192 位隨機 ECP 群組
	224 位隨機 ECP 群組

- 3 從**加密**選擇加密通過 VPN 通道的資料的方法。方法以安全性順序列出：
 - **DES** - 是最不安全的方法，但其加密和解密所需的時間最短。
 - **3DES (預設)** - VPN 將此用於通過通道的所有資料。
 - ① **重要：** SonicWall 全域 VPN 用戶端版本 1.x 無法進行 AES 加密，因此如果您選用 AES 方式，只有 SonicWall 全域 VPN 用戶端版本 2.x 和更高版本可以連接。
 - **AES-128**
 - **AES-192**
 - **AES-256** - 是最安全的方法，但其加密和解密所需的時間最長。
- 4 從**驗證**選擇在 IKE 交涉期間進行金鑰交換時用於驗證金鑰的雜湊法。
 - **MD5**
 - **SHA-1 (預設)**

- SHA256
 - SHA384
 - SHA512
- 5 在**存留時間 (秒數)**中，輸入在需要重新驗證前保持 VPN 通道開放的時間長度。預設是：**28800** 秒 (8 小時)，最大是 9999999 (2777 小時)，最小是 120 秒 (2 分鐘)。
 - 6 按下一步。將顯示**站台對站台原則設定摘要**頁面。

站台對站台原則設定摘要

站對站 VPN 原則設定摘要

VPN 原則 *site-to-site*

一般原則設定
 原則名稱： site-to-site
 預先共用金鑰： 123456
 IKE 階段 I 交換： 加強模式

本機/目的地網路設定
 本機網路： Firewall Subnets
 遠端網路： Authorized access pts

安全設定
 驗證類型： 3DES
 驗證類型： SHA-1
 DH 群組： 群組 2
 存留期 (秒)： 28800

- 1 站對站 VPN 原則設定摘要頁面，會顯示使用 VPN 指南定義的設定。確認設定；如需修改任何設定，按一下後退返回到適當頁面。
- 2 按一下**套用以完成指南**，並建立您的 VPN 原則。在顯示 **VPN 指南完成** 頁面之前會顯示**正在儲存 SonicWall 設定...**訊息。

正在儲存 SonicWall 設定...

正在更新 SonicWall 設定，請稍候。

VPN 指南完成

VPN 指南完成

恭喜!您已成功完成 SonicWall VPN 指南。

其他和進階設定選項可在此找到:[SonicWall Web 管理介面](#)。

- 1 按一下**關閉**按鈕關閉指南。

建立 WAN GroupVPN

VPN 指南可用來快速設定 WAN GroupVPN 以接受從 Global VPN Client 傳入的 VPN 連接。

建立 WAN GroupVPN 的方法是：

- 1 按一下快速設定管理介面上方的**快速設定**。顯示**歡迎**頁面。

歡迎

歡迎使用設定指南
選取以下其中一個指南，助您輕鬆設定 SonicWall:

- 設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- 公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- 無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- App Rule 指南** - 設定 App Rule 的安全性功能
- WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

- 2 在**歡迎**頁面，選擇 **VPN 指南**。
- 3 按**下一步**。隨即顯示 **VPN 原則類型**頁面。

VPN 原則類型

VPN 原則類型

請選擇您想要設定的 VPN 原則類型。

- 站台對站台** - 快速設定一個連接到另一個 SonicWall 裝置的站台對站台 VPN 連接。
- WAN GroupVPN** - 快速設定 WAN GroupVPN 以接受從全域 VPN 用戶端傳入的VPN 連接。

- 1 選擇 **WAN GroupVPN**。
- 2 按**下一步**。將顯示 **IKE 階段 1 金鑰方法**頁面。

IKE 階段 1 金鑰方法

IKE 階段 1 金鑰方法

請選擇所要使用的 IKE 階段 1 金鑰方法。您可以選擇使用預設金鑰，或指定您自己預先共用的金鑰。請注意，如果您選擇後者方法，所有全域 VPN 用戶端將會針對此金鑰顯示提示，當您連接至 'WAN GroupVPN' 時，會被提示給所有 SonicWall 全域 VPN 用戶端。

- 使用預設金鑰
- 使用預先共用的金鑰：

- 在 IKE 階段 1 金鑰方法頁面，您選擇驗證金鑰用於此 VPN 原則：
 - 使用預設金鑰：-所有全域 VPN 用戶端將自動使用安全裝置產生的預設金鑰，來透過 SonicWall 安全裝置進行驗證。預設情況下已核取此選項。
 - 使用預先共用的金鑰：必須將金鑰指派給各 Global VPN Client，因為在連接到 WAN GroupVPN 時會提示使用者需要此金鑰。在使用預先共用的金鑰欄位中指定自訂的預先共用金鑰；由安全裝置產生預設的自訂金鑰，如 **ECE38B6AB8188A5D**。
 - 重要：**如果您選擇使用預先共用的金鑰，並使用產生的值作為自訂金鑰，也必須將金鑰指派到 Global VPN 用戶端。
- 按下一步。將顯示安全設定頁面。

安全性設定

安全設定

請選擇您要用於 IKE 階段 1 和 IPSEC 階段 2 的安全性設定。如果您要求更具體的安全性設定，可調整本精靈完成後的新站台對站台 VPN 原則 (在完成本指南之後)。

附註：全域 VPN 用戶端 1.x 版無法使用 AES 加密，所以如果您選擇此方法，則只能連接全域 VPN 用戶端 2.x 版和以上版本。

DH 群組：	<input type="text" value="群組 2"/>
加密：	<input type="text" value="3DES"/>
驗證：	<input type="text" value="SHA-1"/>
存留時間 (秒數)：	<input type="text" value="28800"/>

- 在安全設定頁面，選擇用於 IKE 階段 1 和 IPSEC 階段 2 的安全設定。如果您需要更多特定的安全設定，可以在此指南完成後調整 WAN GroupVPN VPN 原則。您可以：
 - 使用預設設定。移至 [步驟 6](#)。
 - 選擇其他安全性設定。
- 從 DH 群組，選擇 Diffie-Hellman (DH 或 ECP) 群組，供數值 VPN 在 IKE 交涉期間使用，以建立金鑰對。隨後的各 DH 群組使用更大的數值作為開頭。例如，請參閱 [Suite B 加密中內含的 Diffie Hellman 群組表格](#)。

- 3 從**加密**選擇加密通過 VPN 通道的資料的方法。方法以安全性順序列出：
 - **DES** - 是最不安全的方法，但其加密和解密所需的時間最短。
 - **3DES** (預設) - VPN 將此用於通過通道的所有資料。
 - ① **重要：** SonicWall 全域 VPN 用戶端版本 1.x 無法進行 AES 加密，因此如果您選用 AES 方式，只有 SonicWall 全域 VPN 用戶端版本 2.x 和更高版本可以連接。
 - **AES-128**
 - **AES-192**
 - **AES-256** - 是最安全的方法，但其加密和解密所需的時間最長。
- 4 從**驗證**選擇在 IKE 交涉期間進行金鑰交換時用於驗證金鑰的雜湊法。
 - **MD5**
 - **SHA-1** (預設)
 - **SHA256**
 - **SHA384**
 - **SHA512**
- 5 在**存留時間 (秒數)**中，輸入在需要重新驗證前保持 VPN 通道開放的時間長度。預設是：**28800** 秒 (8 小時)，最大是 9999999 (2777 小時)，最小是 120 秒 (2 分鐘)。
- 6 按下一步。將顯示**使用者驗證**頁面。

使用者驗證

使用者驗證

您可以對所有來自全域 VPN 用戶端的連入 VPN 連線啟用使用者驗證。這會向使用者顯示提示，要求輸入有效的使用者名稱和密碼，之後才能連線到 SonicWall。接著會對照以下指定的內部使用者資料庫使用者群組物件成員來驗證使用者。

啟用使用者驗證

驗證使用者群組物件：

允許未驗證的 VPN 用戶端存取：

- 1 如需要求 VPN 使用者在連接時經過安全裝置進行驗證，選擇**啟用使用者驗證**核取方塊；預設情況下已核取此選項。
 - ① **附註：** 如果您啟用使用者驗證，必須在 SonicWall 資料庫輸入使用者進行身分驗證。在**使用者 > 本機和群組**頁面上，將使用者輸入到 SonicWall 資料庫。如需更多資訊，請參閱 *SonicOS 系統安裝指南*。
- 2 如果您：
 - 如果您選擇（啟用）**啟用使用者驗證**，必須從**驗證使用者群組物件**選擇包含 VPN 使用者的使用者群組。預設為 **Trusted Users**。

- 如果您取消選擇（停用）**啟用使用者驗證**，必須從**允許未驗證的 VPN 用戶端存取**選擇位址物件或位址群組。預設為 **Firewalled Subnets**。

3 按下一步。將顯示**設定虛擬 IP 轉接器**頁面。

設定虛擬 IP 轉接器

設定虛擬 IP 轉接器

全域 VPN 用戶端具有選用的虛擬介面卡，可在用戶端連線到 SonicWall 時取得特殊的 IP 位址，使其在與內部裝置通訊時顯示為在內部 X0 介面網路上。虛擬 IP 位址可從 SonicWall 的內部 DHCP 伺服器，或從位於 SonicWall X0 介面上的現有 DHCP 伺服器取得。

備註：如果已啟用虛擬轉接器，內部 DHCP 伺服器將用於介面 X0 上的現有範圍。

使用虛擬 IP 轉接器

1 如需使用 SonicWall 的內部 DHCP 伺服器為各 VPN 用戶端指派 LAN 區域 IP 範圍中的 IP 位址，勾選**使用虛擬 IP 轉接器**核取方塊。預設情況下未勾選此選項。

全域 VPN 用戶端有一個可選的虛擬轉接器，將其連接到安全裝置時，用其可獲取特殊 IP 位址。啟用此選項後，當使用者連接時，其在與內部裝置通訊時似乎在內部 X0 介面網路上。

虛擬 IP 位址可以從安全裝置的內部 DHCP 伺服器，或從位於安全裝置 X0 介面上的現有 DHCP 伺服器獲取。

附註：如果已啟用虛擬轉接器，將使用內部 DHCP 伺服器，並為 192.168.168.1-192.168.168.167 在介面 X0 上建立新的 DHCP 範圍。

2 按下一步。將顯示 **WAN GroupVPN 設定摘要** 頁面。

WAN GroupVPN 設定摘要

WAN GroupVPN 設定摘要

WAN GroupVPN 設定

預先共用的金鑰設定
使用預設金鑰。

安全設定

驗證類型： 3DES
驗證類型： SHA-1
DH 群組： 群組 2
存留期 (秒)： 28800

驗證設定

使用者驗證： 啟用
XAUTH 使用者的使用者群組： Trusted Users

虛擬 IP 設定

虛擬 IP 指派： 已啟用
DHCP Over VPN： 中央閘道 DHCP 轉接已啟用
內部 DHCP 伺服器： 啟用
介面的 DHCP 範圍 X0： 使用已有範圍

- 1 設定摘要頁面詳細列出您為 GroupVPN 設定的設定。確認設定；如需修改任何設定，按一下後退返回到相應頁面。
- 2 按一下套用完成指南並建立 GroupVPN。在顯示 VPN 指南完成頁面之前會顯示正在儲存 SonicWall 設定...訊息。



VPN 指南完成



- 1 按一下關閉按鈕關閉指南。

連接 Global VPN Client

遠端 SonicWall Global VPN Client 安裝 Global VPN Client 軟體。應用程式安裝後，將使用連接指南設定其 VPN 連接。要設定 VPN 連接，用戶端必須有以下資訊：

- SonicWall 的 WAN 連接埠的公用 IP 位址（或網域名稱）
- 共用密碼（如果您在 VPN 指南中選擇了自訂預先共用密碼）。
- 身分驗證的使用者名稱和密碼。

使用無線指南 (僅限無線平台)

- 第 56 頁「無線指南」

無線指南

無線指南指導您逐步完成設定 WLAN 無線介面的網路設定和安全功能。

設定網路設定和安全功能：

- 1 按一下快速設定。隨即顯示歡迎使用指南頁面。

歡迎

歡迎使用設定指南

選取以下其中一個指南，助您輕鬆設定 SonicWall：

- 設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- 公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- 無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- App Rule 指南** - 設定 App Rule 的安全性功能
- WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

- 2 選擇無線指南。
- 3 按下一步。此時顯示調控網域註冊頁面。

調控網域註冊

調控網域註冊

使用者有責任遵守所有為規範調控網域及/或有關無線電操作地區而制定的法令。請從以下清單選擇正確的國家/地區代碼。

法規區域： MKK - 日本

國家/地區代碼：

i | **重要：**您負責遵守法規區域和/或有關無線電運營場所規定的所有法規。

i | **附註：**法規區域從國家/地區代碼自動產生。

1 從**國家或地區代碼**下拉功能表中選擇一個國家或地區。

i | **重要：**對於國際（非美國或日本）TZ 系列無線和 SOHO W 無線裝置，務必選擇裝置部署所在國家或地區的相應國家或地區代碼，即使您不是在此國家或地區內。對於部署在美國和日本的裝置，法規區域和國家或地區代碼是自動選擇的，且不能變更。

i | **重要：**如果您選擇加拿大的國家/地區代碼，除非您聯絡 SonicWall 支援部門，否則將無法變更。

2 按**下一步**。此時顯示**無線 LAN 設定**頁面。

無線 LAN 設定

無線 LAN 設定

步驟 1：無線 LAN 設定

IP 指派：

設定 SonicWall 作為您的 WLANS 的預設閘道
輸入一個有效的 IP 位址和子網路遮罩。

WLAN IP 位址：

WLAN 子網路遮罩：

1 從**IP 指派**下拉功能表中選擇 IP 指派的類型：

- 固定（預設）
- 二層橋接的模式

i | **附註：**選項會根據您選擇的 IP 指派而變更。

2 如果選擇：

- 固定：

步驟 1：無線 LAN 設定

IP 指派：

設定 SonicWall 作為您的 WLANS 的預設閘道
輸入一個有效的 IP 位址和子網路遮罩。

WLAN IP 位址：

WLAN 子網路遮罩：

- a) 在 **WLAN IP 位址** 欄位輸入 WLAN IP 位址。預設值為 **172.16.31.1**。
- b) 在 **WLAN 子網路遮罩** 欄位輸入 WLAN 子網路遮罩。預設值為 **255.255.255.0**。
- c) 移至**步驟 3**。

- 二層橋接模式，此時出現一則訊息顯示介面橋接的區域：

介面橋接不能變更它的區域。僅允許橋接對間的規則自動新增。請手動新增其他必要的存取規則。

- a) 按一下訊息中的**確定**。這些選項將發生變更：

步驟 1：無線 LAN 設定

IP 指派：

目前的 SonicWall WLAN 正工作在二層橋接模式
選擇橋接介面

橋接到：

- b) 從**橋接到**選擇一個橋接到的介面。預設值為 **X0**。
- c) 移至**步驟 3**。

3 按下一步。此時會顯示一條有關使用戶端電腦上的無線驅動程式保持最新的訊息。

SonicWall 建議用戶端電腦上的無線驅動程式要保持在最新狀態，以獲得較佳的無線連線能力、相容性與效能。

在致電 SonicWall 技術支援部門提供任何無線連線與效能相關問題的協助之前，請先將用戶端電腦上的無線驅動程式升級至最新版本。

有關將驅動程式升級至最新版本，請參閱無線網路卡製造商的說明指示。

4 按一下**確定**。隨即顯示 **WLAN Radio 設定** 頁面。

WLAN Radio 設定

WLAN Radio 設定

設定 SSID, radio 模式, 和您的 SonicWall 操作通道。

SSID 作為您的無線網路的主要識別項。SSID 可能長達 32 個字元和數字的長度, 並且區分大小寫。

選擇期望的無線模式和您的 SonicWall 操作通道。

SSID:

無線電模式:

無線波段:

主要通道:

次要通道:

啟用短期守護間隔

啟用彙總

備註: 考慮到無線操作, 使用者必需遵守所有的法規政府和本機發佈的。

- 1 在 **SSID** 欄位中輸入 SSID (服務集 ID)。SSID 作為您的無線網路的主要識別項。您可以指定最多 32 個英數字元; SSID 區分大小寫。安全裝置產生的預設 SSID 為 **sonicwall-** 加 BSSID (廣播服務集 ID) 的最後四個字元; 例如, **sonicwall-** 變為 **sonicwall-F2DS**。
- 2 從**無線電模式**選擇慣用的無線電模式。無線安全裝置支援**無線模式選擇**表格中顯示的模式。

- i** **附註:** 可用選項會有改變, 具體取決於選擇的模式。如果為符合以下條件的模式設定無線設定:
- 支援 802.11n (除 5GHz 802.11n/a/ac 混合模式以外), 會顯示這些選項: **無線波段、主要通道、次要通道**。
 - 不支援 802.11n, 則僅顯示**頻道**選項。
 - 支援 5GHz 802.11n/a/ac 混合模式或 5GHz 802.11ac 單一模式, 此時顯示**無線波段和頻道**選項。
- i** **提示:** 為使 802.11n 用戶端達到獨一無二的最佳傳送量速度, SonicWall 建議使用**僅 802.11n** 無線模式。對多個無線用戶端身分驗證的相容性, 可使用 **802.11n/b/g 混合模式** 無線模式。為使 802.11ac 用戶端達到獨一無二的最佳傳送量速度, SonicWall 推薦使用**僅 802.11ac** 無線模式。對多個無線用戶端身分驗證的相容性, 可使用 **802.11ac/n/a 混合模式** 無線模式。

無線模式選擇

2.4GHz	5Ghz	定義
2.4GHz 802.11n/g/b 混合模式 (預設)	5GHz 802.11n/a 混合	同時支援 802.11a、802.11b、802.11g, 和 802.11n 用戶端。如果無線網路包含多種類型的用戶端, 請選擇此模式。
僅 2.4GHz 802.11n	僅 5GHz 802.11n	僅允許 802.11n 用戶端存取您的無線網路。802.11a/ac/b/g 用戶端不能在此受限的無線模式下連接。

無線模式選擇

2.4GHz	5Ghz	定義
僅 2.4GHz 802.11g		如果您的無線網路僅包含 802.11g 用戶端，您可以選擇此模式，以提高 802.11g 的效能。如果想要避免 802.11b 用戶端關聯，也可以選擇此模式。
2.4GHz 802.11g/b 混合		如果您的無線網路包含 802.11b 和 802.11g 用戶端，您可以選擇此模式，以提高效能。
	5GHz 802.11a 單一模式	如果僅 802.11a 用戶端存取您的無線網路，則可選擇此模式。
	5GHz 802.11n/a/ac 混合模式	同時支援 802.11a、802.11ac，和 802.11n 用戶端。如果無線網路包含多種類型的用戶端，請選擇此模式。
	5GHz 802.11ac 單一模式	如果僅 802.11ac 用戶端存取您的無線網路，則可選擇此模式。

- 3 如果您選擇的模式支援：

此無線電模式	移至
2.4GHz 802.11n/g/b	步驟 4
2.4GHz 802.11g/b 混合	
僅 2.4GHz 802.11g	
5GHz 802.11a 單一模式	
5GHz 802.11ac 單一模式	步驟 6
5GHz 802.11n/a/ac 混合模式	
2.4GHz 802.11n/g/b 混合模式	步驟 8
僅 2.4GHz 802.11n	
僅 5GHz 802.11n	

- 4 從**頻道**下拉功能表中選擇用於無線電的頻道：

自動（預設）	使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。除非由於某種原因必須使用或避免使用特定的頻道，否則請使用 自動 。
特定的頻道	可以在法規區域範圍內選擇單個頻道。選擇特定的頻道還可幫助您避免受到此區域內其他無線網路的干擾。
	附註： 可用頻道取決於您選擇的 無線電模式 、安全裝置中的無線電類型和您國家/地區可用的頻道。

- 5 移至**步驟 9**。

- 6 此時顯示**無線波段**和**通道**選項。

 **附註：**所有範例使用 FCC 通道。

SSID:	sonicwall-1587
無線模式:	5GHz 802.11n/a/ac 混合模式 ▼
無線波段:	自動 ▼
通道:	自動 ▼

從**無線波段**下拉功能表中，選擇 802.11a 或 802.11ac 無線電的無線波段：

- **自動** - 使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。這是預設值。
 - **頻道**下拉功能表設定為 **自動**，無法變更。
- **標準 - 20 MHz 頻道** - 指定 802.11ac 無線將僅使用標準 20 MHz 頻道。
 - a) 選擇此選項時，從**頻道**下拉功能表中，選擇一個法規區域範圍內的單個頻道。選擇特定的頻道還可幫助您避免受到此區域內其他無線網路的干擾。預設通道是**自動**。
- **標準 - 40 MHz 頻道** - 指定 802.11ac 無線將僅使用寬頻 40 MHz 頻道。選定此選項後，將顯示**頻道**下拉功能表。預設通道是**自動**。
- **標準 - 80 MHz 頻道** - 指定 802.11n 無線將僅使用寬頻 80 MHz 頻道。選定此選項後，將顯示**頻道**下拉功能表。預設通道是**自動**。

7 移至**步驟 9**。

8 **無線波段、主要通道和輔助通道**設定顯示：

無線模式:	5GHz 802.11n 單一模式 ▼
無線波段:	頻寬 - 40 MHz 通道 ▼
主要通道:	自動 ▼
輔助通道:	自動 ▼

從**無線波段**下拉功能表中，選擇適用於 802.11n 或 802.11ac 無線電的頻段：

- **自動** - 使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。這是預設值。
 - **主要通道**和**輔助通道**下拉功能表設定為**自動**，無法變更。
- **標準 - 20 MHz 頻道** - 指定 802.11n 無線將僅使用標準 20 MHz 頻道。選擇此選項時，會顯示**標準頻道**下拉功能表，而非**主要通道**和**輔助通道**下拉功能表。
 - **標準頻道** - 預設情況下，此項設定為**自動**，使安全裝置可以根據信號強度和完整性設定最佳頻道。您也可以在此法規區域的範圍內選擇單個頻道。選擇特定的頻道還可幫助您避免受到此區域內其他無線網路的干擾。
- **標準 - 40 MHz 頻道** - 指定 802.11n 無線將僅使用寬頻 40 MHz 頻道。選定此選項後，將顯示**主要通道**和**輔助通道**下拉功能表：
 - **主要通道** - 預設情況下設定為**自動**。您也可以指定特定的其他頻道。
 - **輔助通道** - 此選項的設定取決於**主要通道**設定，無法變更：

- 9 或者，可按下**啟用短期保護間隔**，相對於 800ns 的標準保護間隔，指定一個 400ns 的短期保護間隔。預設情況下已選擇此設定。

- i** 附註：如果選擇這些模式之一，則此選項無法使用。
- 2.4GHz 802.11g/b 混合
 - 僅 2.4GHz 802.11g
 - 5GHz 802.11a 單一模式

防護間隔是為了確保不同的傳送不會互相干擾而設計的傳送之間間隔的設定時間。防護間隔可避免傳播延遲、回應以及反射。存取點會將在此間隔內收到的任何訊號內容識別為不需要的符號間干擾，並拒絕此資料。防護間隔是傳送時的間隔，目的在於避免由於受到干擾或多路徑延遲造成的資料遺失。

802.11n 標準指定兩種防護間隔：400ns（短）和 800ns（長）啟用短期保護間隔可以透過減少每個裝置不必要的空閒時間來降低網路開銷。400 毫微秒 (ns) 的短期防護間隔，適用於大多數辦公室環境，因為反射點之間以及用戶端之間的距離短。將迅速接收大多數反射。防護間隔越短，頻道使用效率越高，但是較短防護間隔也會增大干擾風險

然而，一些室外部署，可能需要更長的防護間隔。隨著區域的變大，例如在倉庫或戶外環境中，在短期防護間隔結束後反射和回應很可能會繼續，所以對 800 ns 的長期防護間隔的需求變得更加重要。

- 10 另外，要啟用 802.11n 框架彙總（此功能將多框架結合以降低開銷和提高傳送量），請勾選**啟用彙總**核取方塊。預設情況下已選擇此設定。

- i** 附註：如果選擇這些模式之一，則此選項無法使用。
- 2.4GHz 802.11g/b 混合
 - 僅 2.4GHz 802.11g
 - 5GHz 802.11a 單一模式

資料通過無線網路作為封包流（稱為資料框架）傳送。框架彙總可將這些封包彙總到更少、更大的封包中，因此可提升整體效能。框架彙總已新增到 802.11n 規範中，可獲得效能的額外提升。框架彙總是只有 802.11ac 和 802.11n 用戶端才能利用的一項功能，因為舊系統無法理解更大封包的新格式。

- i** 提示：啟用短期保護間隔和啟用彙總選項可稍微提高傳送量。當使用者具有較強的訊號且干擾較小時，它們可以在最佳的網路條件下發揮最大作用。在達不到最佳條件的網路中（受到干擾、訊號較弱等），這些選項可能會導致傳送錯誤，從而削弱傳送量中的任何有效增益。

- 11 按下一步。隨即顯示 **WLAN 安全設定** 頁面。

WLAN 安全設定

WLAN 安全設定

最佳化您的 SonicWall 的 WLAN 安全能力。

選擇以下一個安全模式用於您的 SonicWall。

- **WPA2/WPA2-AUTO 模式** - Wi-Fi 安全存取 (WPA) 是安全的無線通訊協定，以 802.11i 標準為基礎。這也是在您的無線用戶端支援 WPA 情況下推薦的通訊協定。
- **連線性 - 警告！** 該模式不提供加密或者存取控制並且允許無限制的無線連接到該裝置。

1 選擇一種安全模式：

- **WPA2/WPA2- AUTO 模式** - Wi-Fi 防護接入 (WPA) 模式是基於 802.11i 標準的安全無線通訊協定。這也是在您的無線用戶端支援 WPA/WPA 協定情況下的推薦通訊協定。
- **連接** (預設) - 此模式允許對裝置有無限制的無線存取。預設情況下已核取此選項。

△ | **注意：**此模式不提供加密或存取控制允許無限制無線存取安全裝置。

2 按下一步。顯示的頁面取決於您所選擇的安全模式。

3 如果選擇：

- **WPA2/WPA2- AUTO 模式**，此時顯示 **WPA 模式設定** 頁面。移至第 63 頁「**WPA 模式設定**」。
- **連接**，此時顯示 **WLAN VAP (虛擬存取點) 設定** 頁面。移至第 65 頁「**WLAN VAP (虛擬存取點) 設定**」。

WPA 模式設定

WPA模式設定

步驟 4：WPA 模式設定
為 SonicWall 設定 WPA 設定。

驗證類型：

WPA2/WPA 設定

加密類型：

群組金鑰更新：

間隔 (秒數)：

預先共用金鑰設定 (PSK)

複雜密碼：

① | **附註：**如需各種驗證類型、加密類型和共用金鑰的說明，請參閱 *SonicOS 6.5 連線能力*。

1 從**驗證類型**下拉功能表中，選擇加密模式。顯示的選項取決於您選擇的模式。

- **WPA2-PSK** (預設)
- **WPA2-EAP**
- **WPA2-AUTO-PSK**
- **WPA2-AUTO-EAP**

2 從**加密類型**下拉功能表中，選擇：

- **AES** (預設)
- **TKIP**
- **自動**

- 3 從**群組金鑰更新**下拉功能表中選擇二者之一：
 - **逾時**（預設）
 - **停用**；時間間隔欄位不顯示。
- 4 在**間隔（秒數）**欄位中，輸入逾時前的時長。預設為 **86400 秒**（24 小時），最小為 30 秒，最大為 2592000 秒（30 天）。
- 5 如果選擇以下任一項：
 - PSK 模式，請移至**步驟 6**。
 - EAP 模式，請移至**步驟 9**。
- 6 **複雜密碼**欄位隨即顯示。

預先共用金鑰設定 (PSK)

複雜密碼：

輸入用於產生金鑰的密碼。

- 7 按**下一步**。顯示 **WLAN VAP (虛擬存取點)設定**頁面。
- 8 移至第 **65** 頁「**WLAN VAP (虛擬存取點) 設定**」。
- 9 將**密碼**欄位替換為**可擴充驗證通訊協定設定 (EAP)**欄位。

可擴充驗證通訊協定設定 (EAP)

Radius 伺服器 IP 1：	<input type="text"/>	連接埠：	<input type="text"/>
Radius 伺服器密碼 1：	<input type="text"/>		
Radius 伺服器 IP 2：	<input type="text"/>	連接埠：	<input type="text"/>
Radius 伺服器密碼 2：	<input type="text"/>		

- 10 在 **Radius 伺服器 1 IP** 和**連接埠**欄位，輸入主要 RADIUS 伺服器的 IP 位址和連接埠號。
- 11 在 **Radius 伺服器 1 密碼**欄位中，輸入用於存取 Radius 伺服器的密碼
- 12 另外，也可以在 **Radius 伺服器 2 IP** 和**連接埠**欄位中，輸入次要 RADIUS 伺服器（如有）的 IP 位址和連接埠號。
- 13 另外，也可以在 **Radius 伺服器 2 密碼**欄位中，輸入用於存取 Radius 伺服器的密碼
- 14 按**下一步**。如果您選擇了 EAP 模式，此時會顯示一則有關更新安全裝置存取規則的訊息。

防火牆的存取規則將在 WAN 介面上為 Radius 伺服器自動更新

- 15 按一下**確定**。顯示 **WLAN VAP (虛擬存取點)設定**頁面。

WLAN VAP (虛擬存取點) 設定

WLAN VAP (虛擬存取點) 設定

VAP SSID

您已經建立了 1 SSID: **sonicwall-1587**
您要建立其他的虛擬存取點嗎？

是的，我要建立其他的虛擬存取點。

備註：您最多可以建立 7 個虛擬存取點。

- 1 如果您：
 - 不想建立 WLAN VAP，請移至**步驟 2**。
 - 想要建立 WLAN VAP，請移至第 65 頁「**WLAN VAP (虛擬存取點) 設定 - 建立 VAP**」
- 2 按下一步。此時顯示**無線設定摘要**頁面。
- 3 移至第 67 頁「**無線設定摘要**」。

WLAN VAP (虛擬存取點) 設定 - 建立 VAP

WLAN VAP (虛擬存取點) 設定

VAP SSID

您已經建立了 1 SSID: **sonicwall-1587**
您要建立其他的虛擬存取點嗎？

是的，我要建立其他的虛擬存取點。

備註：您最多可以建立 7 個虛擬存取點。

- 1 已自動建立一個 VAP SSID；在設定過程中可能新增了更多 VAP SSID。您可以建立多達六個 VAP SSID，總計為七個 VAP SSID。要建立另一個 VAP，請勾選**是的，我要建立其他的虛擬存取點**核取方塊。將顯示更多選項。

WLAN VAP (虛擬存取點) 設定

VAP SSID

您已經建立了 1 SSID: **sonicwall-1587**

您要建立其他的虛擬存取點嗎？

是的，我要建立其他的虛擬存取點。

VAP SSID:

WLAN 安全設定

為該 VAP 選擇一種安全模式。

- WPA2/WPA2-AUTO 模式** - Wi-Fi 安全存取 (WPA) 是安全的無線通訊協定，以 802.11i 標準為基礎。
這也是在您的無線用戶端支援 WPA 情況下推薦的通訊協定。
- 連線性 - 警告！** 該模式提供了無加密或者存取控制並且允許無限制的對裝置的無線存取。

2 在 VAP SSID 欄位中輸入 VAP 的名稱。

3 選擇一種安全模式：

- WPA2/WPA2-AUTO 模式** - Wi-Fi 防護接入 (WPA) 模式是基於 802.11i 標準的安全無線通訊協定。這也是在您的無線用戶端支援 WPA/WPA 協定情況下的推薦通訊協定。
- 連接 (預設)** - 此模式允許對安全裝置有無限制的無線存取。

△ | **注意：** 此模式不提供加密或存取控制，並允許無限制無線存取安全裝置。

4 按下一步。此時顯示 WLAN VAP (虛擬存取點) 設定 > WLAN 子網路和區域頁面。

WLAN VAP (虛擬存取點) 設定 > WLAN 子網路和區域

WLAN VAP (虛擬存取點) 設定

WLAN 子網路和區域

您正在設定 WLAN 子網路和區域設定為 VAP SSID: **1111**.

請為新的 WLAN 子網路選擇一個唯一的名稱和 IP 位址。

這個新的子網路將屬於預設的 WLAN 區域，或者您可以建立

一個新的 WLAN 區域。

Vlan 標籤應該是一個 1 到 4094 的數字。

WLAN VLAN 標籤:

WLAN IP 位址:

WLAN 子網路遮罩:

WLAN 區域:

建立新區域:

- 1 在 **WLAN VLAN 標籤** 欄位中輸入唯一的 VLAN 標籤。標籤應該是一個 1 到 4094 的數字。
- 2 在 **WLAN IP 位址** 欄位中輸入唯一的 IP 位址。
- 3 在 **WLAN 子網路遮罩** 欄位輸入 WLAN 子網路遮罩。
- 4 您可以
 - 從 **WLAN 區域** 下拉功能表中選擇區域。預設為 **WLAN**。
 - 另外，也可以建立一個新的區域：
 - a) 按一下 **建立一個新的區域**。
 - a) 在 **建立一個新的區域** 欄位中輸入新區域的名稱。
 將使用這個新區域替代從 **WLAN 區域** 下拉功能表中指定的任何區域 (將為灰顯)。
- 5 按 **下一步**。再次顯示 **WLAN VAP (虛擬存取點) 設定** 頁面。
- 6 結束時間：
 - 建立另一個 WLAN VAP，重複第 65 頁「**WLAN VAP (虛擬存取點) 設定**」中的步驟。
 - 繼續而不建立其他 WLAN VAP，請按 **下一步**。此時顯示 **無線設定摘要** 頁面。

無線設定摘要

無線設定摘要

無線設定摘要
檢閱您的 SonicWall WLAN 設定摘要。

WLAN 介面 - 已啟用
WLAN IP 位址: 172.16.31.1

無線設定
SSID: sonicwall-1587
無線模式: 2.4GHz 802.11n/g/b 混合
國家/地區代碼: JP
無線波段: 自動 主要通道: 自動

安全模式 - WPA 模式
驗證類型: WPA2_PSK
加密類型: 自動

VAP 設定 - 沒有建立 VAP。

無線設定摘要

無線設定摘要
檢閱您的 SonicWall WLAN 設定摘要。

WLAN 介面 - 已啟用
WLAN IP 位址: 172.16.31.1

無線設定
SSID: sonicwall-1587
無線模式: 僅 5GHz 802.11n
國家/地區代碼: JP
通道: 自動通道 - 自動

安全模式 - WPA 模式
驗證類型: WPA2_PSK
加密類型: 自動

VAP 設定 - 將建立這些新的 VAP:

	SSID	介面	區域	驗證	密碼
1	1111	12	WLAN	WPA2_AUTO_PSK	自動

- 1 驗證設定是否正確。
 - a 若要更正任何設定，請按一下 **上一步** 直至您到達適當的頁面。
 - b 做出變更。
 - c 按一下 **下一步** 直至您到達 **無線設定摘要** 頁面。

- 按一下**套用**。將顯示一條訊息，提示設定正在進行更新：



設定更新完成後，會顯示**無線指南完成**頁面。



- 按下**完成**。

使用 App Rule 指南

- 第 69 頁「App Rule 指南」

App Rule 指南

App Rule 指南精靈為很多常見用例提供應用程式規則的安全設定方法，但並非針對每個用例。如果在指南執行期間的任何時候，您都無法找到所需的選項，可以按一下**結束指南**，然後使用手動設定繼續進行。

附註： 進行手動設定時，請務必設定所有元件，包括相符物件、操作、電子郵件地址物件（如果需要），最後，還有引用這些元件的原則。

設定應用程式規則：

- 1 按一下 SonicOS 管理介面上方的**快速設定**。顯示**歡迎**頁面。

歡迎

歡迎使用設定指南

選取以下其中一個指南，助您輕鬆設定 SonicWall:

- 設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- 公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- 無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- App Rule 指南** - 設定 App Rule 的安全性功能
- WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

- 2 選擇 **App Rule 指南**。
- 3 按下一步。App Rule 指南簡介頁面隨即顯示。

應用程式規則指南簡介

本指南將協助您使用原則快速設定 SonicWall，以檢查應用程式層級網路流量。

使用本指南，您將可根據一系列預先定義的步驟建立應用程式規則原則。

- 4 按下一步。應用程式規則原則類型頁面隨即顯示。

應用程式規則原則類型

應用程式規則原則類型

請選擇要為其建立應用程式規則原則的網路應用程式類型。

- 將原則套用到 SMTP 電子郵件
- 將原則套用到正在接收的 POP3 電子郵件
- 將原則套用到 Web 存取
- 我要對 FTP 檔案傳輸程式套用原則

- 1 選擇要設定的網路應用程式類型：
 - 將原則套用到 SMTP 電子郵件（預設）
 - 將原則套用到正在接收的 POP3 電子郵件
 - 將原則套用到 Web 存取
 - 我要對 FTP 檔案傳輸程式套用原則
- 2 按下一步。
- 3 下一個頁面取決於您選擇的原則類型。如果您選擇將原則套用到：
 - SMTP 電子郵件，請移至第 70 頁「選擇 App Rule 的 SMTP/POP3 規則」。
 - POP3 電子郵件，請移至第 70 頁「選擇 App Rule 的 SMTP/POP3 規則」
 - Web 存取，請移至第 71 頁「選擇 App Rule 的 Web 存取規則」
 - FTP 檔案傳送，請移至第 72 頁「選擇 App Rule 的 FTP 規則」

選擇 App Rule 的 SMTP/POP3 規則

POP3 規則是 SMTP 規則的子集。

選擇 App Rule 的 SMTP 規則

選擇 App Rule 的 SMTP 規則

- 在電子郵件主旨中查找內容
- 在電子郵件本文中查找內容
- 在電子郵件附件中查找內容
- 指定允許透過的電子郵件的最大大小
- 查找指定的附件副檔名
- 查找指定的附件名稱
- 查找除了指定外所有的附件副檔名
- 除了所指定的附件名稱，檢查所有附件名稱

選擇 App Rule 的 Pop3 規則

選擇 App Rule 的 POP3 規則

- 查找指定的附件副檔名
- 查找指定的附件名稱
- 查找除了指定外所有的附件副檔名
- 查找除了指定外所有的附件名稱
- 檢查電子郵件主旨中的內容

- 1 從提供的選項（參見選擇應用程式防火牆的 SMTP 和 POP3 規則表格）中選擇規則的類型：

選擇應用程式防火牆的 SMTP 和 POP3 規則

規則	SMTP	POP3
在電子郵件主旨中查找內容	✓ (預設)	✓
在電子郵件本文中查找內容	✓	
在電子郵件附件中查找內容	✓	
指定允許透過的電子郵件的最大大小	✓	
查找指定的附件副檔名	✓	✓ (預設)
查找指定的附件名稱	✓	✓
查找除了指定外所有的附件副檔名	✓	✓
查找除了指定外所有的附件名稱	✓	✓

- 2 按下一步。
- 3 下一個頁面取決於您選擇的規則。如果選擇：
 - 除指定允許透過的電子郵件的最大大小外的所有 SMTP 和 POP3 原則規則類型，請移至第 73 頁「App Rule 物件關鍵字和原則指示」。
 - 指定允許透過的電子郵件的最大大小，請移至第 75 頁「應用程式規則物件電子郵件大小」。

選擇 App Rule 的 Web 存取規則

選擇 App Rule 的 Web 存取規則

- 檢查具有特定副檔名的下載檔案
- 查找指定 URI 的存取
- 查找某些 web 瀏覽器的使用
- 查找除了那些指定外的任何 web 瀏覽器的使用
- 查找上載到 web 郵件帳戶的附件名稱
- 檢查上載到 web 郵件帳戶中的附件的副檔名

- 1 選擇管理 Web 存取的規則：
 - 檢查具有特定副檔名的下載檔案
 - 查找特定 URIs 的存取
 - 查找某些 web 瀏覽器的使用
 - 查找除了那些指定外的任何 web 瀏覽器的使用
 - 查找上載到 web 郵件帳戶的附件名稱
 - 檢查上載到 web 郵件帳戶中的附件的副檔名
- 2 按下一步。
- 3 顯示的頁面取決於所選擇的規則：
 - 對於查找某些 web 瀏覽器的使用和查找除了那些指定外的任何 web 瀏覽器的使用規則，此時會顯示應用程式規則物件設定頁面；請移至第 75 頁「應用程式規則操作類型」。
 - 對於所有其他規則，此時會顯示 App Rule 物件關鍵字和原則指示頁面；請移至第 73 頁「App Rule 物件關鍵字和原則指示」。

選擇 App Rule 的 FTP 規則



- 1 從提供的選項中選擇 FTP 檔案名稱、副檔名或內容：
 - 檢查指定檔案內容的檔案傳輸
 - 檢查指定檔案名稱的檔案下載 (讀入)
 - 檢查指定副檔名的檔案的下載 (讀入)
 - 檢查指定檔案名的檔案的上載 (寫入)
 - 檢查指定副檔名的檔案的上載 (寫入)
 - 使所有的 FTP 存取唯讀 (無上載)
 - 不許使用 SITE 命令
- 2 按下一步。
- 3 移至第 73 頁「App Rule 物件關鍵字和原則指示」。

App Rule 物件關鍵字和原則指示

App Rule 物件關鍵字和原則指示

請從下拉功能表中選擇值。

方向：

內容：

清單：

新增

更新

移除

全部移除

從檔案上載

- 1 在方向下拉功能表中，選擇要掃描的流量方向。
 - 傳入（預設）
 - 傳出
 - 兩者
- 2 如果選擇：
 - 以下兩種 FTP 應用程式規則類型之一，請移至**步驟 3**：
 - 使所有的 FTP 存取唯讀（無上載）
 - 不許使用 SITE 命令
 - 對任何其他應用程式規則類型，執行以下任一動作：
 - ① **附註：**如果選擇帶有**除指定項**字樣的 SMTP 或 POP3 規則，您在這裡輸入的內容將是不會導致操作發生的唯一內容。
 - 手動新增內容的步驟是：
 - a) 在**內容**欄位，輸入或貼上要符合的內容的十六進位表示。
 - b) 按下**新增**。
 - c) 重複**步驟 a** 和**步驟 b**，直至所有內容均已新增到**清單**欄位。
 - 匯入包含內容值清單的預先定義文字檔案中的關鍵字的步驟是：
 - ① **附註：**檔案中必須每行一個值。

a) 按一下**從檔案上載**。此時顯示**上載物件值**對話方塊。



b) 選擇包含物件值的檔案。

c) 按一下**上載**。

3 按下一步。應用程式規則操作類型頁面隨即顯示。

4 移至第 75 頁「**應用程式規則操作類型**」。

應用程式規則物件設定



1 在方向下拉功能表中，選擇要掃描的流量方向。

- 傳入（預設）
- 傳出
- 兩者

2 在內容欄位，輸入或貼上要符合的內容的十六進位表示。

3 按下**新增**。

4 重複**步驟 2** 和 **步驟 3**，直至所有內容均已新增到**清單**欄位。

5 按下一步。應用程式規則操作類型頁面隨即顯示。

6 移至第 75 頁「**應用程式規則操作類型**」。

應用程式規則物件電子郵件大小

應用程式規則物件電子郵件大小

請為電子郵件的最大大小和方向選擇值。

方向：

最大電子郵件大小（位元組數）：

- 1 在方向下拉功能表中，選擇要掃描的流量方向。
 - 傳入（預設）
 - 傳出
 - 兩者
- 2 在最大電子郵件大小（位元組數）欄位，輸入電子郵件訊息的最大位元組數。最小和預設大小為 0，最大大小為 1410065407 位元組。
- 3 按下一步。
- 4 移至第 75 頁「[應用程式規則操作類型](#)」。

應用程式規則操作類型

此頁面可用的選項取決於您指定的原則類型：SMTP、POP3、Web 存取或 FTP 檔案傳送。

應用程式規則操作類型

請選擇 App Rule 動作

- 封鎖操作 - 封鎖並傳輸自訂電子郵件回覆。
- 封鎖操作 - 封鎖不傳輸電子郵件回覆。
- 新增電子郵件識別（在電子郵件尾部追加文字）。
- 僅用於記錄。
- 繞過 DPI。

- 1 從提供的選項中，選擇要執行的操作；請參見[應用程式規則操作](#)表格。
i | 附註：並非每條存取規則的操作類型/設定都可用。

應用程式規則操作

操作類型/設定	SMTP	POP3	Web 存取	FTP
封鎖操作 -				
封鎖並傳送自訂電子郵件回覆	✓ ^a			
封鎖但不傳送自訂電子郵件回覆	✓			

應用程式規則操作

操作類型/設定	SMTP	POP3	Web 存取	FTP
停用附件並新增自訂文字		✓ a		
自訂阻塞頁面			✓ a	
重新導向到新位置			✓	
重設連接			✓	✓ a
新增封鎖訊息				✓
新增電子郵件橫幅（在電子郵件尾部追加文字）	✓			
僅記錄	✓	✓	✓	✓
繞過 DPI	✓	✓	✓	✓

a. 預設值

- 2 按下一步。移至第 76 頁「應用程式規則操作設定」。

應用程式規則操作設定

應用程式規則操作設定

請輸入封鎖電子郵件的回覆訊息

內容：

- 1 根據您在上一個頁面選擇的設定，在內容欄位，輸入錯誤訊息、電子郵件訊息、URI 重新導向、自訂阻塞頁面或橫幅頁面的文字。
- 2 按下一步。
- 3 移至第 76 頁「為應用程式規則原則選擇名稱」。

為應用程式規則原則選擇名稱

為應用程式規則原則選擇名稱

原則名稱：

- 1 在原則名稱欄位，輸入有意義的名稱。
- 2 按下一步。
- 3 移至第 77 頁「確認原則設定」。

確認原則設定



- 1 驗證設定是否正確。

① | 附註：若要更正任何設定，請按一下上一步直至您到達包含要變更設定的頁面。

- 2 按一下套用。正在儲存 SonicWall 設定訊息隨即顯示。



設定更新完成後，會顯示應用程式規則原則完成頁面。



- 3 按一下關閉。

使用 WXA 設定指南

- 第 78 頁「[WXA 設定指南](#)」
 - 第 79 頁「[入門](#)」
 - 第 80 頁「[介面頁面](#)」
 - 第 82 頁「[啟用加速頁面](#)」
 - 第 84 頁「[加速元件](#)」
 - 第 85 頁「[VPN 頁面](#)」
 - 第 86 頁「[完成頁面](#)」
- 第 86 頁「[已簽署 SMB 的 WFS 設定指南](#)」
 - 第 87 頁「[選擇專屬 WXA](#)」
 - 第 88 頁「[網域詳細資料](#)」
 - 第 89 頁「[加入網域](#)」
 - 第 90 頁「[設定共用](#)」
 - 第 90 頁「[設定本機檔案伺服器](#)」
 - 第 91 頁「[設定遠端檔案伺服器](#)」
 - 第 92 頁「[新增網域記錄](#)」
 - 第 93 頁「[完成頁面](#)」

WXA 設定指南

TZ 系列裝置支援單一連接的 WXA 系列設備，藉以提供 WAN 加速。它們不支援 WXA 叢集。

NSA 系列裝置在叢集中使用一個或多個 WXA 系列設備，藉以提供 WAN 加速。每個 WAN 使用一系列的元件，跨 WAN、遠端檔案共用操作和 Web 瀏覽來加速 TCP 連線。**WXA 設定指南** 逐步帶領您完成 SonicWall 安全裝置的初始設置和設定步驟，如果結合 WXA 的叢集，即可為本機使用者提供 WAN 加速的功能。

使用 **WXA 設定指南** 之前，請思考下列：

- SonicWall 安全裝置必須經過設置、設定和許可。
- 除了 Web 快取，本**指南**會假設加速的流量將透過站台對站台 VPN。因此，WXA 系列設備不得在路由或二層橋接模式中設定。雖然 WXA 系列設備可以使用此設定，但 **WXA 設定指南** 不予支援。只有站台對站台虛擬私人網路 (VPN) 與此**指南**相容。
- 不支援 IPv6。WXA 系列設備通過或加速的流量必須使用 IPv4。

- 使用 **WXA 設定指南** 將覆寫任何現有設定。
- 在使用 **WXA 設定指南** 之前，不得接通 WXA 系列設備的電源。在執行 **WXA 設定指南** 時，會前進到裝置通電的步驟。

如要設定 WXA 裝置：

- 第 79 頁「**入門**」
- 第 80 頁「**介面頁面**」
- 第 82 頁「**啟用加速頁面**」
- 第 82 頁「**群組頁面**」
- 第 84 頁「**加速元件**」
- 第 85 頁「**VPN 頁面**」
- 第 86 頁「**完成頁面**」
- 第 86 頁「**已簽署 SMB 的 WFS 設定指南**」

入門

如為 WAN 加速設定關聯 WXA 系列設備：

- 1 按一下 SonicOS 管理介面上方的**快速設定**。將顯示**設定指南的歡迎**頁面。

歡迎

歡迎使用設定指南

選取以下其中一個指南，助您輕鬆設定 SonicWall:

- **設定指南** - 此精靈將協助您快速設定 SonicWall 以確保您的網際網路連線安全。完成後，您即可使用 SonicWall Web 管理介面進行其他設定。
- **PortShield 介面指南** - 在 SonicWall 的整合式受管 LAN 參數中選擇指派的初始連接埠。
- **公用伺服器指南** - 快速設定您的 SonicWall 以提供內部伺服器的公用存取權。
- **VPN 指南** - 建立新的站對站 VPN 原則或設定 WAN GroupVPN 為接受來自全域 VPN 用戶端的連線。
- **無線指南** - 設定 WLAN 無線訊號介面的網路設定和安全性功能。
- **App Rule 指南** - 設定 App Rule 的安全性功能
- **WXA 設定指南** - 為 WAN 加速設定結合的 WXA 系列設備

- 按下一步。將顯示 WAN 加速簡介頁面。

WAN 加速功能簡介

NSA 或 TZ 系列設備使用 WXA 系列設備以提供 WAN 加速。WXA 使用多項元件跨 WAN、遠端檔案共用操作和 Web 瀏覽來加速 TCP 連線。

本指南將會逐步完成初始設定和 NSA 或 TZ 系列設備的設定，如此一來，當與 WXA 結合時，它會將加速的 WAN 流量傳遞到本機使用者。

備註：

- 必須對 NSA 或者 TZ 系列裝置設定、組態和授權。
- 除了 Web 快取，本指南會假設加速的流量將透過站台對站台 VPN。它可能使用 WXA 在路由或 L2 橋接模式，本指南不涵蓋該設定。請參閱 SonicOS 系統設定指南以取得詳細資料。
- WXA 韌體不支援 IPv6。WXA 通過或加速的流量必須使用 IPv4。
- 本指南可能覆寫任何現有的設定。可在每一步驟儲存資料。如果您選擇保有目前的設定，請關閉指南，不要再繼續。

- 按下一步。將顯示介面頁面。

介面頁面

介面頁面指導您完成設定 SonicWall 安全裝置上與 WXA 系列設備相連的介面的過程。

設定介面的步驟是：

介面

在 TZ 或者 NSA 系列裝置上選擇一個將用於連接 WXA 系列裝置的未使用介面。

如有必要或需要，可設定將用於該介面，且將當成 WXA 閘道使用的 IP 位址。通常這個 IP 位址來自尚未在本機使用或在 VPN 上的私用範圍 (10.*.*.*、172.16.*.*- 172.31.*.*、192.168.*.*、169.239.239.*)。

介面：

保持現有的介面設定

區域：

IP 位址：

網路遮罩：

① 提示：如果以前設定過此介面，將顯示**保持現有的介面設定**選項，並且預設為勾選狀態。

介面：

保持現有的介面設定

區域：

IP 位址：

網路遮罩：

如果設定：

- 正常，請確保選項是已勾選並移至**步驟 6**。
- 應該變更，取消勾選選項。

- 1 按一下**介面**下拉功能表。
- 2 從**介面**下拉功能表，選擇用來連接 WXA 系列設備的介面。
- 3 從**區域**下拉功能表，選擇所要的區域。
- 4 在**IP 位址**文字欄位中輸入所要的 IP 位址。此 IP 位址通常來自一個專用範圍，而不是本機已使用或 VPN 上。
- 5 在**網路遮罩**文字欄位中輸入所要的網路遮罩。預設值為 **255.255.255.0**。
- 6 按下一步。將顯示**啟用加速**頁面。

① | 附註：按下一步儲存變更並覆寫現有的值。

啟用加速頁面

啟用加速頁面指導您完成連接 WXA 系列設備與 NSA/TZ 系列安全裝置的過程。

啟用加速

WAN 加速現將啟用。然後將開始進行探查以找出已連接的 WXA。

使用標準乙太網路線，將 WXA 系列設備 '上標示 eth0' 的連接埠連到之前指定的 NSA/TZ 介面: X268473346 如果有多個 WXA，可使用中繼交換器。

當所有的 WXA 已經完成啟動，請按「下一步」繼續...

- 1 連接裝置。
- 2 為裝置通電。
- 3 完成重新啟動。
- 4 所有 WXA 裝置已通電後，按一下下一步按鈕繼續。

啟用加速頁面將顯示有關探查 WXA 裝置的訊息。

連接 WXA

 請稍候...
探查 WXA 裝置

附註： 虛擬 WXA（WXA 5000 虛擬裝置和 WXA 500 Live CD）需要授權。在此階段，如果 NSA/TZ 系列安全裝置沒有用於 WAN 加速的授權，將顯示「授權」頁面。

- 1 輸入適當的授權資訊。
- 2 按一下下一步按鈕繼續。

完成處理後，將顯示**群組**頁面。

群組頁面

連接到 TZ 或 NSA 系列的 WXA 裝置將組成群組。一組 WXA 將在一個或多個已設定的 VPN 上，加速流量和檔案共用操作。個別加速元件的設定都會指定，並套用於整組的 WXA 裝置。

群組頁面可讓您設定群組，向該群組配置 WXA 裝置，以及指定加速設定，然後再指定群組來控制一個或多個 VPN 上的加速。

選擇 WXA 群組的步驟是：

群組

連接到 TZ 或 NSA 系列設備的 WXA 會組成 **群組**。有一組 WXA 會被指定在一個或多個已設定之 VPN 上加速流量和檔案共用操作的任務。

整組的 WXA 都會指定和套用個別加速元件的設定。

本指南可讓您設定一個群組、將 WXA 配置到該群組，並在指派該群組前指定加速設定，以於一或多個 VPN 上管理該加速項目。

從現有的群組中選擇，或選擇建立及設定新的群組。

- Group One
- 建立新群組

1 選擇：

- 一個群組。移至 **步驟 3**
- 建立新的群組。群組頁面將改變。

建立新群組

輸入新群組的名稱

群組名稱：

- 2 在 **群組名稱** 欄位輸入新群組的名稱。
- 3 按一下下一步，將顯示 **WXA** 頁面。

WXA 頁面

若要提供 WAN 加速服務，WXA 群組必須包含一個或多個 WXA 系列設備。WXA 的數量取決於已配置該群組的 VPN 需要支援多少個並行連接。不同 WXA 型號支援不同的連接數量，因此所需的數量也是可用型號類型的功能。

WXA 頁面顯示已找到的 WXA。

WXAs

為提供 WAN 加速服務，群組中必須包含一個或多個 WXA 系列設備。群組中使用的 WXA 數量取決於群組分配到的 VPN 需要支援多少同時連線。不同的 WXA 模式支援不同的連線數量，因此所需的數字也是可用模式類型的函數。

將 WXA 從已發現之清單指派到群組，輸入一個 WXA 使用的易記名稱。

ID	名稱	目前的群組	狀態
<input checked="" type="checkbox"/> 00:0C:29:08:D1:3D	<input type="text" value="WXA5000-908D13D"/>	Group One	Up

- 1 如果尚未進行此操作，給 WXA 群組的 WXA 裝置通電。
- 2 按一下 **重新整理 WXA 清單** 按鈕。

- 3 為群組選擇 WXA 裝置。

i 附註：如果選擇已經是群組成員的 WXA 裝置，會顯示一個警告訊息：

您已選擇納入之前指派給其他群組的一個或多個 WXA。這可能影響通過防火牆的流量。
是否確定要繼續？

按一下**確定**繼續，或按**取消**丟棄。

- 4 按下一步。隨即顯示加速元件頁面。

加速元件

加速元件頁面可啟用或停用 WAN 加速服務的個別元件。

加速元件

不同的加速元件和它們目前的「啟用」狀態顯示如下。若要啟用或者停用每個元件，請勾選或者取消勾選相應的核取方塊。

- TCP 加速
- WFS 加速
- Web 快取

- 1 勾選或取消勾選所需加速元件的核取方塊：

i 附註：如果某元件之前已啟用，將自動勾選其核取方塊。

- **TCP 加速** - 預設情況下已核取此選項。
- **WFS 加速** - 預設情況下未勾選此選項。

i 附註：如果選擇了 **WFS 加速**，在完成 **WXA 設定指南** 之後，將自動啟動已簽署 **SMB** 的 **WFS 設定指南**。

- **Web 快取** - 預設情況下未勾選此選項。

- 2 按一下下一步按鈕繼續。如果選擇：

- **TCP 加速**和/或 **WFS 加速**，將顯示 **VPN** 頁面，移至第 **85** 頁「**VPN 頁面**」。
- 僅限 **Web 快取**，完成頁面顯示；移至第 **86** 頁「**完成頁面**」。

VPN 頁面

VPN 頁面顯示所有 IPv4 VPN 的清單。如果在 VPN 上已允許加速，則勾選 VPN 原則名稱旁的核取方塊。

VPNs

指定哪一個已設定之 VPN 將具有所選群組控制的加速， Group One 方法只需選取適當的核取方塊即可。

VPN 原則名稱	使用這個群組	目前的群組
site-to-site	<input checked="" type="checkbox"/>	

i 附註：如果 VPN 尚未設定，將顯示頁面：

VPNs

沒有設定的 VPN。
按「下一步」以繼續...

- 1 對於要允許加速的 VPN 原則，勾選原則名稱旁的核取方塊。
- 2 按下一步按鈕。將顯示路由頁面。

路由頁面

路由

指定哪一個已設定之路由將具有所選群組控制的加速， Group One 方法只需選取適當的核取方塊即可。

來源	目的地	註解	使用這個群組	目前的群組
Any	X2:V148 IP		<input checked="" type="checkbox"/>	Group One

i 附註：如果路由尚未設定，路由頁面會顯示訊息：

路由

沒有設定路由。
按「下一步」以繼續...

- 1 選擇要使用路由的核取方塊。
- 2 按下一步。隨即顯示完成頁面。

完成頁面

完成頁面確認您已成功完成 WXA 設定指南。



1 結束時間：

- 設定另一個 WXA 群組，按一下**設定另一個群組**。將顯示**群組**頁面。
 - 1) 重複第 82 頁「**群組頁面**」至第 86 頁「**完成頁面**」中的步驟。
- 設定已簽署 SMB 的延伸支援，按一下**已簽署 SMB 的延伸支援**。將顯示**對簽署 SMB 的 WFS 擴充支援設定指南**。請參閱第 86 頁「**已簽署 SMB 的 WFS 設定指南**」。
- 結束 WXA 設定指南，按一下**關閉**。

已簽署 SMB 的 WFS 設定指南

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。**已簽署 SMB 的 WFS 設定指南**指導您設定 Windows 網域中的 WXA 系列設備，以便使用者可以充分從支援已簽署 SMB 的網路 WFS 加速模組功能中受益。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 系列設備之前，先在檔案伺服器所在的站台上設定 WXA 系列設備。

提示：您可以從**管理 > 系統安裝 > WAN 加速**頁面，在較晚的日期設定已簽署 SMB 加速的延伸支援。

主題：

- 第 87 頁「**選擇專屬 WXA**」
- 第 87 頁「**啟用延伸支援**」
- 第 88 頁「**網域詳細資料**」
- 第 89 頁「**加入網域**」
- 第 90 頁「**設定共用**」
- 第 90 頁「**設定本機檔案伺服器**」
- 第 91 頁「**設定遠端檔案伺服器**」
- 第 92 頁「**新增網域記錄**」
- 第 93 頁「**完成頁面**」

如為 WAN 加速設定關聯 WXA 系列設備：

- 1 按一下 WXA 設定指南「完成」頁面的已簽署 SMB 的延伸支援。將顯示介紹頁面。

已簽署 SMB 的 WFS 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。已簽署 SMB 的 WFS 指南將會引導您完成選取 WXA 系列設備，並在 Windows 網域進行設定，如此一來，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。

設備加入網域後，您就有機會在遠端伺服器上設定共用，而該伺服器包含在 WFS 加速程序中。

建議您先在檔案伺服器所在的站台設定 WXA，然後在需要遠端存取共用的子站台設定 WXA。

- 2 按下一步。顯示選擇專屬 WXA 頁面。

選擇專屬 WXA

選擇專屬 WXA 頁面可讓您選擇要用於加速網路上已簽署 SMB 流量的 WXA 系列設備。WXA 系列設備可以是群組的一部分，或專用於 WFS 加速。

選擇專屬 WXA

選擇將用於加速網路上已簽署 SMB 流量的 WXA。WXA 可以是群組的一部分，或專用於 WFS 加速的群組。

專屬 WXA:

- 1 從專屬 WXA 下拉功能表，選擇 LAN 上 WXA 系列設備的 IP 位址。
- 2 按下一步按鈕。顯示選擇啟用延伸支援頁面。

啟用延伸支援

此頁面可讓您選擇 WFS 加速位址，這是加速流量的 LAN 上 WXA 系列設備的位址。該位址可以是 WXA 裝置本身或更常是 NSA 或 TZ 系列裝置的 IP 位址。若是後者，NAT 將用於適當地重新導向流量至 WXA 裝置。

啟用延伸支援

選擇 WFS 加速位址，然後按「下一步」啟用已簽署 SMB 的 WFS 延伸支援。

WFS 加速位址是流量正加速之 LAN 上 WXA 系列設備的 IP 位址。位址可以是 WXA 設備本身或更常是 NSA/TZ 系列設備的位址。若是後者，NAT 將會用於將適當流量重新導向至 WXA 設備。

WFS 加速位址:

- 1 從 WFS 加速位址下拉功能表，選擇 WFS 加速位址。
- 2 按下一步以啟用已簽署 SMB 的 WFS 延伸支援。關於正在初始化網域的訊息會在網域詳細資料頁面之前顯示。

網域詳細資料

 正在初始化。請稍候...

網域詳細資料

網域詳細資料頁面顯示指南所判定有關本機網域的資訊：

- 網域
- WXA 主機名稱
- 預設主機名稱
- **i** | 附註：如果預設主機名稱已經設定為 WXA 主機名稱，則只有 WXA 主機名稱會顯示。
- WXA 裝置是否已加入網域 (狀態)

網域詳細資料

網域： tb20dc3.sonicwall.com

WXA 主機名稱:

預設的主機名稱: WXA5000-908D13D

輸入主機名稱以代表網域上的 WXA，否則會使用預設的名稱。
按「下一步」讓 WXA 加入網域。

- 1 如果 WXA 主機名稱欄位包含正確的主機名稱，移至 **步驟 3**。
- 2 或者，可在 WXA 主機名稱欄位中輸入 WXA 主機名稱。如果不提供名稱，則會使用預設主機名稱。
- 3 按一下下一步按鈕繼續。如果
 - 主機名稱已經是網域的一部分，會顯示**設定共用**頁面。移至第 90 頁「**設定共用**」。
 - 主機名稱不是網域的一部分，會顯示**加入網域**頁面。移至第 89 頁「**加入網域**」。
 - 如果未發現本機網域，**完成**頁面會顯示錯誤訊息，包含可協助您進行故障排除為何未發現網域的資訊。

已完成

發生錯誤代表無法繼續執行已簽署 SMB 的 WFS 指南。

錯誤詳細資料: 發現的網域和設定的網域不同。您必須先在已簽署 SMB 頁面改正才能再繼續。

請稍候再試。

- i** | **重要：**設定網域、WXA 主機名稱,和/或 Kerberos 伺服器是在**系統安裝 > WAN 加速**頁面上完成，如需進一步資訊，請參見 *SonicOS 系統安裝指南*。

加入網域

加入網域頁面用於輸入您的管理員憑證，以使 WXA 系列設備可以加入網域。

- ❶ 附註：根據目前狀態和設定，可以選擇「取消加入網域」或「重新加入網域」（如果 WXA 之前已加入網域）。

加入網域

要讓 WXA 系列設備加入網域，請輸入系統管理員憑證，並按一下以下按鈕。

附註：加入網域可能需要些時間。請耐心等待。

使用者名稱：

密碼：

- 1 在使用者名稱和密碼文字欄位中，輸入管理員憑證。
- 2 按一下加入網域按鈕。

加入網域過程開始，並顯示一則訊息。



請耐心等待，這可能需要一段時間。過程完成時，會顯示加入網域結果。

加入網域

加入網域結果

結果摘要

- 已成功加入網域

詳細資料

- ✔ Checking WFS (Signed SMB) configuration
- ✔ Check domain controller name for l10n095181.tb20dc3.sonicwall.com
- ✔ Check domain controller address for l10n095181.tb20dc3.sonicwall.com.
- ✔ Synchronizing clock with domain controller 192.168.94.181
- ✔ Checking wadmin credentials before provisioning.
- ✔ Checking NETBIOS domain.
- ✔ NETBIOS domain is TB20DC3.
- ✔ Preparing to join WXA to domain.
- ✔ Joining WXA to domain tb20dc3.sonicwall.com.
- ✔ Starting clock synchronization
- ✔ Checking WFS (Signed SMB) configuration
- ✔ Set trusted for delegation
- ✔ Registering WFS (Signed SMB) server in DNS
- ✔ Starting WFS (Signed SMB)

- 3 按一下下一步按鈕繼續。

設定共用

設定共用頁面根據 WXA 系列設備的位置和您的網路設定，提供選擇設定共用所在位置的選項。

設定共用

根據此 WXA 系列設備的位置和您的網路設定選擇您要做什麼。

- 此 WXA 位於「總公司」，而我想要設定本機檔案伺服器，讓遠端站台的使用者在存取這些伺服器時，能從加速的檔案操作中獲益。
- 此 WXA 位於「分公司」，而我想要設定位於遠端站台的檔案伺服器，讓分公司的使用者能藉由「下一躍點」WXA 加速存取那些遠端伺服器上的共用。
- 區域網路 (LAN) 的檔案伺服器是由遠端站台的使用者存取。此外，LAN 上的使用者會存取遠端站台的檔案伺服器。因此，我想要設定本機和遠端伺服器。
- 我不想要同時設定伺服器和共用，所以請略過這一段。

- 1 選擇其中一個選項：

設定共用選項

目的地	選擇	移至
設定本機檔案伺服器	此 WXA 位於「總公司」，並且我想要設定本機檔案伺服器，以使遠端站台的使用者在存取這些伺服器時可得益於加速的檔案操作。	第 90 頁「設定本機檔案伺服器」。
設定遠端檔案伺服器	此 WXA 位於「分公司」，並且我想要設定位於遠端站台的檔案伺服器，以使分部的使用者透過「下一躍點」WXA 獲得對這些遠端伺服器上共用的加速存取。	第 91 頁「設定遠端檔案伺服器」。
設定本機和遠端檔案伺服器	區域網路 (LAN) 的檔案伺服器是由遠端站台的使用者存取。因此，我想要設定本機和遠端伺服器。	第 90 頁「設定本機檔案伺服器」然後第 91 頁「設定遠端檔案伺服器」。
跳過伺服器和共用設定	我現在不想設定伺服器和共用，因此跳過本部分。預設情況下已核取此選項。	第 93 頁「完成頁面」。

- 2 按下一步。顯示的頁面取決於您選擇的選項，請參見設定共用選項表格。

設定本機檔案伺服器

設定本機檔案伺服器頁面列出發現的本機檔案伺服器，您可以將其選擇和新增到 WXA 系列設備的設定。

將加速來自遠端站台的所有伺服器共用資料夾和文件的檔案操作。如要限制 WFS 加速 (已簽署 SMB) 至特定共用，請在 SonicOS 管理介面的管理 > WAN 加速頁面上設定共用；如需進一步資訊，請參閱 SonicOS 系統安裝指南。

在本機檔案伺服器上設定共用

從網路上發現到的選擇本機檔案伺服器。然後，按下「新增」按鈕將伺服器加入到 WXA 的設定。

從遠端站台到其所有共用資料夾和文件的檔案操作都會加速。若您想要將已簽署 SMB 的 WFS 延伸支援限制為特定共用，就可以在 WFS 已簽署 SMB 頁面的「進階設定模式」下進行設定。

已發現的檔案伺服器

L10N094188.tb20dc3.sonicwall.com L10N094189.tb20dc3.sonicwall.com	加入到 WXA 設定
--	------------

在 WXA 上設定的本機檔案伺服器

檔案伺服器	移除
L10N095181.tb20dc3.sonicwall.com	✕

- 1 從檔案伺服器名稱下拉功能表，選擇本機檔案伺服器。
- 2 按一下新增伺服器和共用。伺服器會新增到在 WXA 上設定的本機檔案伺服器表格中。
- 3 按一下下一步按鈕繼續。將顯示一則表示將儲存伺服器資訊的訊息，然後顯示新增網域記錄頁面。
- 4 移至第 92 頁「新增網域記錄」。

設定遠端檔案伺服器

設定遠端伺服器頁面為您提供選擇遠端檔案伺服器和輸入本機 WXA 名稱的選項。遠端檔案伺服器應是託管共用資料夾和檔案的 Windows 檔案伺服器。WXA 會嘗試發現 WXA 設定用於提供伺服器加速存取的「下一躍點」。

將加速所有的伺服器共用資料夾和文件的檔案操作。如要限制 WFS 加速 (已簽署 SMB) 至特定共用，請在 SonicOS 管理介面的管理 > WAN 加速頁面上設定共用；如需進一步資訊，請參閱 SonicOS 系統安裝。

在遠端伺服器上設定共用

從在網路上發現的以及在其他 WXA 上設定的選擇遠端 檔案伺服器。

您必須一次選擇一個，再輸入代表伺服器且由本機使用者使用的唯一名稱。例如，若目前路徑為：\\remote_server\docs，在 WFS 加速下會變成 \\local_wxa\docs

一旦已選擇檔案伺服器及輸入本機名稱，請按下 '新增' 按鈕將伺服器加入到 WXA 設定。

遠端檔案伺服器

L10N094188.tb20dc3.sonicwall.com L10N094189.tb20dc3.sonicwall.com
--

本機 WXA 名稱:

加入到 WXA 設定

遠端檔案伺服器設定在 WXA

檔案伺服器	本機 WXA 名稱	刪除
L10N095181.tb20dc3.sonicwall.com	L10N095181	✕

- 1 從**遠端檔案伺服器名稱**，選擇要新增到 WXA 設定的遠端檔案伺服器。
- 2 在本機 **WXA 名稱** 欄位中，輸入本機 WXA 系列設備的唯一名稱或別名。在本機 WXA 名稱後輸入一點將自動填寫完成此網域的名稱。
 - ❗ **重要：**此名稱之後套用於遠端伺服器中資料夾和檔案的路徑中，以便檔案共用操作能從 WFS 加速中受益。
- 3 按一下加入到 **WXA 設定**。
- 4 按一下**下一步**按鈕繼續。會顯示**新增網域記錄**頁面。

新增網域記錄

新增網域記錄頁面顯示遠端伺服器名稱、本機 WXA 名稱及其狀態。這用於在設定中向遠端伺服器和本機 WXA 新增網域記錄。

新增網域記錄

若要將記錄加入到網域控制器和 DNS 伺服器，您必須輸入系統管理員憑證，並按一下以下的「新增網域記錄」按鈕。

要略過此步驟，請按「下一頁」。然而，稍後必須新增記錄才能讓 WFS 加速正常運作。

使用者名稱：

密碼：

- 1 檢閱列出的遠端伺服器和本機 WXA。
- 2 如果：
 - 您需要新增網域記錄，請移至**步驟 3**。
 - 清單即完成並且正確，或者您想要稍後再新增，請移至**步驟 5**。
- 3 在**使用者名稱**和**密碼**欄位中，輸入管理員憑證。
- 4 按一下**新增網域記錄**。將顯示訊息，同時 SonicOS 在驗證網域記錄。



驗證之後，會顯示**結果摘要**。

新增網域記錄

更新網域記錄

結果摘要

- 已成功更新網域記錄
- Conflicting service principal names already exist on domain controller 192.168.94.181:
cifs/L10N095181->L10N095181.tb20dc3.sonicwall.com,cifs
/L10N095181.tb20dc3.sonicwall.com->L10N095181.tb20dc3.sonicwall.com
- Unable to set Trusted for Delegation

詳細資料

- ✔ Checking WFS (Signed SMB) configuration
- ✔ Check domain controller name for l10n095181.tb20dc3.sonicwall.com
- ✔ Check domain controller address for l10n095181.tb20dc3.sonicwall.com.
- ✔ Checking wadmin credentials before provisioning.
- ✔ Checking NETBIOS domain.
- ✔ NETBIOS domain is TB20DC3.
- ✔ Checking WFS (Signed SMB) configuration
- ✘ Set trusted for delegation
- ✔ Registering WFS (Signed SMB) server in DNS
- ✔ Starting WFS (Signed SMB)

- 5 按一下下一步按鈕繼續。隨即顯示完成頁面。

完成頁面

完成頁面確認您已成功完成 **WFS 設定精靈**。

已完成

這可完成已簽署 SMB 指南的 WFS 延伸支援 WAN 加速。

- 1 按一下關閉結束 **WFS 設定精靈**。
- 2 瀏覽至**管理 > WAN 加速**頁面。

ID	名稱	組	IP	模式	軟體	操作狀態	元件	連線	設定	管理	探查	
00:0C:29:08:D1:3D	WXA5000-908D13D	Group One	192.168.148.252	WXA 5000	1.3.2-0-7	總集就緒: 8 days, 4 hrs 運作時間: 3.00%	✔ TCP 加速 ✔ WFS; ✔ Web 快取	SSMB 0	⚙️	✖️	管理	探查

- 3 在 **WXAs** 表格中，為新設定的 WXA 按一下**管理**按鈕。**管理 WXA** 對話方塊即顯示。

管理 WXA ✕

WXA: WXA5000-908D13D

UTC 時間:

WXA 用於延伸支援已簽署 SMB 流量。強烈建議使用網域控制器同步處理 WXA 上的時間，因此 NTP 伺服器欄位必須保留空白。

NTP 伺服器:

Web 快取

- 4 按一下**重新整理**以便將使用此指南做出的變更更新 **WAN 加速** 頁面。

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
- 檢視視訊教學
- 存取 MySonicWall
- 瞭解 SonicWall 專業服務
- 檢閱 SonicWall 支援服務和保固資訊
- 註冊訓練和認證
- 需要技術支援或客戶服務

若要聯絡 SonicWall 支援人員，請參閱 <https://support.sonicwall.com/contact-support>。

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。

SonicWall 快速設定
已更新 - 2017 年 11 月
軟體版本 - 6.5
232-004129-00 修訂版 A

Copyright © 2017 SonicWall Inc. 保留所有權利。

SonicWall 是 SonicWall Inc. 和/或其分支機構在美國和/或其他國家/地區的商標或註冊商標。所有其他商標和註冊商標為其各自擁有者的財產。

本文件內含資訊係依 SonicWall Inc. 和/或其分支機構的產品提供。本文件未透過禁止反悔或其他方式明確表示或暗示授與有關智慧財產權或與銷售 SonicWall 產品相關之任何權利。除了本產品所附授權合約之使用條款所規定以外，SonicWall 和/或其分支機構對於有關其產品之任何明示、暗示或法定擔保，包括 (但不限於) 適售性、適合某特定用途或未侵權等，概不負責。在任何情況下，SonicWall 和/或其分支機構對於因使用本文件或無法使用本文件所造成之任何直接損害、間接損害、衍生性損害、懲罰性損害、特殊損害或附隨性損害 (包括但不限於利潤損失、業務中斷或資訊損失等損害) 概不負責，即使已告知 SonicWall 和/或其分支機構可能發生上述損害亦同。SonicWall 和/或其分支機構不表示或保證本文件內容之正確性或完整性，並保留未事先通知隨時變更規格與產品說明之權利。SonicWall Inc. 和/或其分支機構並未承諾更新本文件內含之資訊。

如需更多資訊，請造訪 <https://www.sonicwall.com/legal>。

最終使用者產品合約

如需查看 SonicWall 最終使用者產品合約，請移至 <https://www.sonicwall.com/en-us/legal/license-agreements>。根據您的地理位置選擇語言以查看適用您所在地區的 EUPA。

開放原始程式碼

SonicWall 可以提供機器可讀取的開放原始程式碼副本，並按照每個授權需求提供限制的授權，例如 GPL、LGPL、AGPL。若要取得完整的機器可讀取副本，請寄送您的書面申請連同金額為 US 25.00 的保付支票或匯票至 SonicWall Inc.：

一般公用授權原始程式碼請求
SonicWall Inc. Attn: Jennifer Anderson
5455 Great America Parkway
Santa Clara, CA 95054