SonicWall® SonicOS 6.5 安全設定

SONICWALL®

目錄

設定進階防火牆設定 7
偵測預防 8
動態連接埠 8
來源路由封包 10
連接 10
動態調整連接大小 12
存取規則服務選項 12
IP 和 UDP 總和檢查碼執行 13
Jumbo 框架 13
IPv6 進階設定 13
控制面洪水防護 14

設定頻寬管理 16
了解頻寬管理 16
設定頻寬管理設定 18
全域頻寬管理 21
進階頻寬管理 28
設定頻寬管理 31
升級到進階頻寬管理 40

設定洪水防護 42
TCP 檢視 43
UDP 檢視 51
ICMP 檢視 53

設定防火牆多點傳送設定 56
多點傳送窺探 57
多點傳送原則 57
IGMP 狀態表 58

管理服務品質 62
分類 62
標記 63
調節 63
802.1p 和 DSCP QoS 64
頻寬管理 73
術語 73

設定 SSL 控制 77
關於 SSL 控制 77

SSL 控制設定 83
啟用區域中的 SSL 控制 87
SSL 控制事件 87

管理 SonicWall 安全服務 89
SonicWall 安全服務 89
設定安全服務 89

設定內容篩選服務 93
關於 CFS 94
啟用 CFS 96
啟用本機 CFS 伺服器 97
設定 CFS 原則 98
設定 CFS 自訂類別 101

啟用 SonicWall 用戶端防毒 108
設定用戶端防毒服務 109

設定用戶端 CF 執行 115
在網路區域中啟用用戶端 CFS 116

管理 SonicWall 閘道防毒服務 118
SonicWall GAV 多層方法 118
SonicWall GAV 結構 121
啟用閘道防毒、防間諜軟體和 IPS 授權 122
設定 SonicWall 閘道防毒防護 123
查看 SonicWall GAV 特徵 132

啟用入侵保護服務 134
入侵保護服務銷售概述 134
啟用入侵保護服務 136

檢視捕獲 ATP 狀態 144
關於圖表 145
關於記錄表 146
上載檔案進行分析 148
檢視威脅報告 149

設定捕獲 ATP 157
關於捕獲 ATP 158
啟用捕獲 ATP 授權 159
啟用捕獲 ATP 159
關於捕獲 ATP > 設定頁面 160
設定捕獲 ATP 163
停用 GAV 或雲端防毒 165

啟用防間諜軟體服務 166
防間諜軟體概述 166
啟用防間諜軟體服務防護 166

設定 SonicWall 即時黑名單 173
即時黑名單篩選 173
設定 RBL 篩選 174

設定 Geo-IP 篩選條件 178
設定 Geo-IP 篩選 178
建立自訂國家/地區清單 181
自訂 Web 封鎖頁面設定 184
使用 Geo-IP 篩選診斷 186

設定 Botnet 篩選 189
設定 Botnet 篩選 189
建立自訂 Botnet 清單 191
自訂 Web 封鎖頁面設定 194
使用 Botnet 篩選診斷 196

關於反垃圾郵件 199
反垃圾郵件概述 199
反垃圾郵件服務的工作原理 200
購買反垃圾郵件授權 204

檢視反垃圾郵件狀態 206
反垃圾郵件服務狀態 207
監視狀態 207
電子郵件流量診斷擷取 208
MX 記錄查詢和橫幅檢查 210
GRID IP 檢查 211

啟用和啟用反垃圾郵件 212
啟用反垃圾郵件 213
安裝垃圾儲存區 214
設定電子郵件威脅類別 215
設定存取清單 216
設定進階選項 218
檢視反垃圾郵件統計 220

設定反垃圾郵件記錄 221
下載系統/記錄檔案 222

設定 RBL 篩選 225
關於 RBL 清單 226

啟用 RBL 篩選 226
管理 RBL 服務 227
使用者自訂 SMTP 伺服器清單 230
測試即時黑名單 232

指定轉接網域 233
關於開放轉接 233
列出允許的轉接網域 234

設定垃圾郵件設定 235

管理垃圾郵件摘要 236
管理垃圾郵件摘要 237
恢復為預設值 240

設定垃圾郵件檢視 241
關於「垃圾儲存區」標籤 242
搜尋郵件 243
管理垃圾儲存區中的郵件 246

設定使用者可視設定 248
設定使用者檢視設定 248

設定公司允許和封鎖清單 250
關於標籤 251
將項目新增到允許清單或封鎖清單 251
從允許清單或封鎖清單刪除項目 252
匯入通訊錄項目 252
匯出通訊錄項目 253
搜尋允許和封鎖清單 254

管理使用者 255
更新使用者表 256
啟用對非 LDAP 使用者的驗證 256
檢視使用者 257
新增使用者 259
以使用者身分登入 260

設定 LDAP 伺服器 261
可用 LDAP 伺服器 262
新增 LDAP 伺服器 262
設定 LDAP 查詢 266
新增 LDAP 對應 268
設定全域 LDAP 設定 270
編輯 LDAP 伺服器設定 271

刪除 LDAP 伺服器 271

下載反垃圾郵件桌面按鈕 272

關於 DPI-SSL 273
功能 273
部署方案 274
自訂 DPI-SSL 274
每個裝置型號的連接 275

設定用戶端 DPI-SSL 設定 276
檢視 DPI-SSL 狀態 276
設定用戶端 DPI-SSL 277

設定伺服器 DPI-SSL 設定 290
設定 DPI-SSL 伺服器設定 290

設定 DPI-SSH 293
關於 DPI-SSH 293
支援的用戶端/伺服器和連線 294
支援的金鑰交換演算法 294
注意 295
啟用您的 DPI-SSH 授權 295
設定 DPI-SSH 296

SonicWall 支援 299
關於本文件 300

1

設定進階防火牆設定

本章節提供了用於設定偵測預防、動態連接埠、來源路由封包、連接選擇和存取規則選項的進階防火牆設定。如需設定進階存取規則選項，請選擇**安全設定 | 防火牆設定 > 進階設定**。

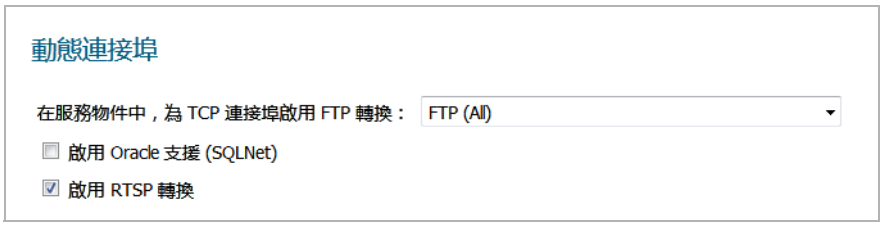
防火牆設定 > 進階設定頁面包括以下防火牆設定選項群組：

- 偵測預防
- 動態連接埠
- 來源路由封包
- 連接
- 動態調整連接大小
- 存取規則服務選項
- IP 和 UDP 總和檢查碼執行
- Jumbo 框架
- IPv6 進階設定
- 控制面洪水防護

偵測預防

- **啟用隱形模式** - 預設情況下，安全裝置回應傳入的連接請求為「封鎖」或「開放」。如果啟用隱匿模式，安全裝置不會回應封鎖的傳入連接請求。隱匿模式使您的安全裝置對駭客來說基本不可見。
- **隨機 IP ID** - 選擇**隨機 IP ID** 可防止駭客使用各種偵測工具偵測安全裝置的存在。IP 封包是給定的隨機 IP ID，它使駭客更難以獲得安全裝置的特徵。
- **對轉送流量使用遞減的 IP TTL** - 存留時間 (TTL) 是 IP 封包中的一個值，用於告知網路路由器封包在網路中存留的時間是否太長，是否應丟棄。選擇此選項，以減少轉送的且在網路中存留了一段時間的封包的 TTL 值。
    - **從不產生 ICMP 逾時的封包** - 防火牆產生逾時封包，以在其 TTL 值已遞減為零的情況下報告何時丟棄封包。如果不想要防火牆產生這些報告封包，可選擇此選項。

動態連接埠



- **在服務物件中，為 TCP 連接埠啟用 FTP 轉換** - 從下拉功能表中選擇服務群組，以啟用指定服務物件的 FTP 轉化。預設情況下，已選擇服務群組 **FTP（全部）**。

  FTP 在 TCP 連接埠 20 和 21 上執行，其中，連接埠 21 是控制連接埠，20 是資料連接埠。但是，在使用非標準連接埠（例如 2020、2121）時，SonicWall 預設丟棄封包，因為無法識別其是 FTP 流量。**在服務物件中，為 TCP 連接埠啟用 FTP 轉換**選項允許選擇服務物件以指定 FTP 流量的自訂控制連接埠。

  為了說明此功能的工作方式，請參照下例，其中 FTP 伺服器在監聽連接埠 2121 的 SonicWall 之後：

  a 在**原則 | 物件 > 位址物件**頁面上，使用以下值為 FTP 伺服器的私人 IP 位址建立**位址物件**：
    - **名稱**：FTP 伺服器私人
    - **區域**：LAN
    - **類型**：主機
    - **IP 位址**：192.168.168.2

  b 在**原則 | 物件 > 服務物件**頁面，使用以下值為 FTP 伺服器建立自訂服務：
    - **名稱**：FTP 自訂連接埠控制項
    - **通訊協定**：TCP(6)

- **連接埠範圍**：2121 - 2121

c 在**原則 | 規則 > NAT 原則**頁面上，建立以下 NAT 原則：

d 在**原則 | 規則 > 存取規則**頁面上，建立以下存取規則：

e 在**安全設定 | 防火牆設定 > 進階設定**頁面，從**在服務物件中，為 TCP 連接埠啟用 FTP 轉換**下拉功能表選擇 **FTP 自訂連接埠控制**服務物件。

附註：如需設定服務群組和服務物件的更多資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

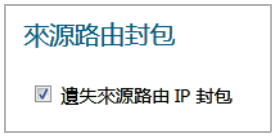
- **啟用 Oracle 支援 (SQLNet)** - 如果您的網路安裝了 Oracle9i 或更低版本的應用程式，則勾選此選項。對於 Oracle10g 或更高版本的應用程式，推薦不要勾選此選項。

  對於 Oracle9i 及更低版本的應用程式，資料通道連接埠與控制連接連接埠不同。啟用此選項時，將會掃描 SQLNet 控制連接以獲取正在交涉的資料通道。找到交涉的資料通道時，將為此資料通道動態建立連接項目並根據需要套用 NAT。在 SonicOS 內，SQLNet 和資料通道相互關聯並作為一個工作階段進行處理。

  對於 Oracle10g 及更高版本的應用程式，這兩個連接埠相同，因此無需單獨追蹤資料通道連接埠；也就無需啟用此選項。

- **啟用 RTSP 轉換** - 選擇此選項，以支援即時資料的按需交付，例如音訊和視訊。RTSP（即時資料流通訊協定）是一種應用程式層級通訊協定，用於控制有即時屬性的資料傳送。

來源路由封包

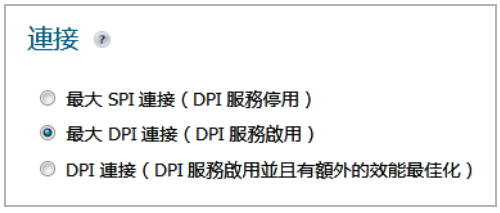


- **遺失來源路由 IP 封包** -（預設情況下已啟用）。如果要測試兩個特定主機之間的流量，且您正在使用來源路由，則可勾選此核取方塊。

  IP 來源路由是標準 IP 選項，它允許封包傳送方指定應使用部分或全部路由器將封包傳送至目的地。

  通常禁止使用此 IP 選項，因為竊聽者可能將之用來接收封包，方法是插入一個選項將封包從 A 經由路由器 C 傳送到 B。路由表應控制封包所採用的路徑，以免傳送方或下游路由器覆寫此路徑。

連接



重要：連接設定有任何變更時，都必須重新啟動 SonicWall 安全裝置才能實作所做的變更。

連接一節介紹精確調整防火牆，以最佳化最佳傳送量或深度封包偵測 (DPI) 服務偵測到的增加的同步連接數的功能。請參閱連接數目表格。

連接數目

平台	SPI 連接	DPI	
		最大連接數	效能最佳化
SuperMassive 9600	10,000,000	2,000,000	1,750,000
SuperMassive 9400	7,500,000	1,500,000	1,250,000
SuperMassive 9200	5,000,000	1,500,000	1,250,000
NSA 6600	2,000,000	1,000,000	750,000
NSA 5600	2,000,000	1,000,000	750,000
NSA 4600	1,000,000	500,000	375,000
NSA 3600	750,000	375,000	250,000
NSA 2600	500,000	250,000	125,000
TZ600	150,000	125,000	125,000
TZ500/TZ500 W	125,000	100,000	100,000
TZ400/TZ400 W			
TZ300/TZ300 W	50,000	50,000	50,000
SOHO W			

只能選擇一個選項。DPI 連接設定提供的安全防護層級均未變更。

- **最大 SPI 連接數（DPI 服務停用）**- 此選項（狀態封包檢測）不提供 SonicWall DPI 安全服務防護，並針對僅啟用狀態封包偵測的最大連接數最佳化防火牆。此選項應由**僅**需要狀態封包偵測的網路使用，不推薦用於大多數 SonicWall 網路安全裝置部署。
- **最大 DPI 連接（DPI 服務啟用）**- 這是預設值，推薦對大多數 SonicWall 網路安全裝置部署使用此設定。
- **DPI 連接（DPI 服務啟用並且有額外的效能最佳化）**- 此選項針對效能關鍵型部署。對於增加的防火牆 DPI 檢查傳送量，此選項將權衡最大的 DPI 連接數。

附註：如果選擇 DPI 連接而 DPI 連接數目大於 250,000，您可以讓防火牆動態調整 DPI 連接大小和 DPI-SSL 計數。如需詳細資料，請參閱動態調整連接大小。

最大的連接數取決於指定型號的 SonicWall 安全裝置的實體功能，如連接數目表格中所示。流量報告不會減少 NSA 防火牆和 SM 系列 防火牆上的連接數目。

將滑鼠放置在**連接**標題旁邊的**問號**圖示可以顯示您的具體 SonicWall 安全裝置各種設定變式的最大連接數顯示表格。快顯表格中顯示您的目前設定的項目。

動態調整連接大小

附註：NSA 3600 系列和更高版本及 SuperMassive 系列網路安全裝置上，支援動態調整連接大小。

如果對於**連接**勾選了**最大 DPI 連接（DPI 服務啟用）**或 **DPI 連接（DPI 服務啟用並且有額外的效能最佳化）**，並且 DPI 連接數目大於 250,000，則會顯示**動態調整連線大小**部分。設定此選項可使防火牆透過動態減少 DPI 連接數目 1250000 個，來增加 DPI-SSL 連接數目 750 個。

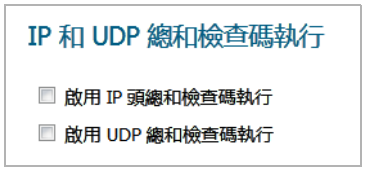
- **DPI 連線** - 可讓您以 125,000 的增量方式，選擇 DPI 連接的最大數目。更改此數目會變更 **DPI-SSL 連線**下拉功能表中的值。
- **DPI-SSL 連線** - 可讓您以 750 的增量方式，選擇 **DPI-SSL 連線**的最大數目。更改此數目會變更 **DPI-SSL 連線**下拉功能表中的值。

例如，如果在 **DPI 連線**下拉功能表中選擇的 DPI 連接數目是 **1250000**，**DPI-SSL 連線**下拉功能表中的 DPI-SSL 連接數目會是 **165000**。如果您從 **DPI 連線**下拉功能表選擇 **1000000**，DPI-SSL 連接的數目會變更為 **18000**。如果您從 **DPI-SSL 連線**下拉功能表選擇 **12000**，DPI 連接的數目會變更為 **2000000**。

存取規則服務選項

- **強制傳入和傳出 FTP 資料連接使用預設連接埠 20** - 預設值允許來自連接埠 20 的 FTP 連接，但會將傳出流量重新對應到 1024 等連接埠。如果已核取核取方塊，透過安全裝置的任何 FTP 資料連接都必須來自連接埠 20，否則連接將遺失。此事件將記錄為安全裝置的記錄事件。
- **為流入/來自同一個介面的 LAN 網間流量用防火牆規則** - 套用在 LAN 介面上接收的且其目的地為同一個 LAN 介面的防火牆規則。通常，僅在設定了備用 LAN 子網路的情況下才需要使用此選項。
- **一律為已捨棄的傳出 TCP 連線發出 RST** - 為已捨棄的傳出 TCP 連線傳送 RST (重設) 封包以丟棄連線。預設情況下已核取此選項。
- **在 LAN 區啟用 ICMP 重新導向** - 在 LAN 區介面上重新導向 ICMP 封包。預設情況下已核取此選項。
- **捨棄來源 IP 是子網路廣播位址的封包** - 當偵測到的 IP 位址被子網路識別為該位址時捨棄封包。

IP 和 UDP 總和檢查碼執行



- **啟用 IP 頭總和檢查碼執行** - 選擇此項以強制使用 IP 頭總和檢查碼。IP 頭中帶有不正確總和檢查碼的封包將遺失。預設已停用此選項。
- **啟用 UDP 總和檢查碼執行** - 選擇此選項以強制使用 UDP 封包總和檢查碼。帶有不正確總和檢查碼的封包遺失。預設已停用此選項。

Jumbo 框架

附註：NSA 3600 及更新裝置支援 Jumbo 框架。

- **啟用 Jumbo 框架支援** - 啟用此選項可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：Jumbo 框架封包的大小為 9000 kB，會將記憶體需求提高 4 倍。啟用 Jumbo 框架支援後，必須將介面 MTU 變更為 9000 位元組，如 *SonicWall SonicOS 6.5 系統安裝*中描述的。

IPv6 進階設定

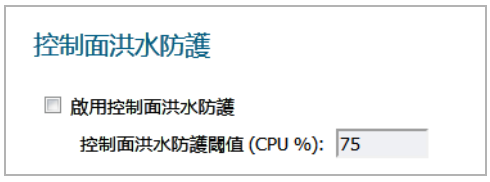
- **丟棄 IPv6 路由頭類型 0 封包** - 選擇此選項防止危害 IPv6 路由標頭類型 0 (RH0) 封包的潛在 DoS 攻擊。啟用此設定後，將丟棄 RH0 封包，除非其目的地是 SonicWall 安全裝置且剩餘段數為 0。「剩餘段數」表示在到達最終目的地前剩餘的路由段數。預設已啟用。更多資訊，請參見 http://tools.ietf.org/html/rfc5095。
- **為轉送的流量降低 IPv6 躍點限制** - 類似於 IPv4 TTL，勾選時，當躍點限制降低到 0 時，將丟棄封包。預設已停用。
- **丟棄並記錄網路封包，封包的來源或者目的地位址已經被 RFC 保留** - 勾選此選項以拒絕並記錄網路封包，封包定義了來源或目的地位址，作為保留供將來定義和按照 RFC 4921 IPv6 中指定使用的位址。預設已停用。
- **從不產生 IPv6 ICMP 逾時封包** - 預設情況下，SonicWall 裝置產生 IPv6 ICMP 逾時封包，此封包報告裝置何時因躍點限制降低到 0 而丟棄封包。勾選此選項以停用此功能；SonicWall 裝置將不會產生這些封包。預設情況下已核取此選項。
- **從不產生無法到達 IPv6 ICMP 目的地的封包** - 預設情況下，SonicWall 裝置產生 IPv6 ICMP 無法存取目的地的封包。勾選此選項以停用此功能；SonicWall 裝置將不會產生這些封包。預設情況下已核取此選項。
- **從不產生 IPv6 ICMP 重新導向封包** - 預設情況下，SonicWall 裝置產生重新導向封包。勾選此選項以停用此功能；SonicWall 裝置將不會產生重新導向封包。預設情況下已核取此選項。
- **從不產生 IPv6 ICMP 參數問題封包** - 預設情況下，SonicWall 裝置產生 IPv6 ICMP 參數問題封包。勾選此選項以停用此功能；SonicWall 裝置將不會產生這些封包。預設情況下已核取此選項。
- **允許使用網站-本機單點傳播位址** - 預設情況下，SonicWall 裝置允許站台-本機單點傳送 (SLU) 位址，且此核取方塊已核取。根據目前的定義，SLU 位址不明確並且可以存在於多個站台。使用 SLU 位址可能透過洩露、含糊不清和潛在的錯誤路由對安全造成不利影響。為避免此問題，請取消選擇此核取方塊以防止裝置使用 SLU 位址。
- **執行 IPv6 延伸標頭驗證** - 如果想要 SonicWall 裝置檢查 IPv6 擴充標頭的有效性，勾選此選項。此選項預設為停用。

  僅當勾選此選項和選項**為轉送的流量降低 IPv6 躍點限制**時，**強制執行 IPv6 延伸標頭順序檢查**選項變為可用。（您可能需要重新整理此頁面。）

  - **強制執行 IPv6 延伸標頭順序檢查** - 如果想要 SonicWall 設備檢查 IPv6 擴充標頭的順序，勾選此選項。此選項預設為停用。
- **為 ISATAP 啟用 NetBIOS 名稱查詢回應** - 如果想要 SonicWall 裝置產生 NetBIOS 名稱以回應廣播 ISATAP 查詢，勾選此選項。此選項預設為停用。

  附註：只有設定了一個 ISATAP 通道介面時，才能勾選此選項。

控制面洪水防護



- **啟用控制面洪水防護** - 如果控制面上的流量超過了在**控制面洪水防護閾值 (CPU %)** 中指定的閾值，希望防火牆僅將發往此防火牆的控制流量轉送到系統控制面的核心，勾選此選項。預設情況下未啟用此選項。

為給予合法的控制流量優先權，超出閾值的資料流量會被丟棄。此項限制可防止過多的資料流量到達控制面核心，而可能導致系統回應速度變慢和導致網路連線中斷。而為控制流量所設定的百分比乃獲得保證的流量。

- **控制面洪水防護閾值 (CPU %)** - 以百分比的形式輸入攻擊防護閾值。最小值為 5 (%)，最大值為 95，預設值為 **75**。

2

設定頻寬管理

頻寬管理 (BWM) 是將頻寬資源指派給網路上的關鍵應用程式的一種方法。

SonicOS 透過其傳出（輸出）和傳入（輸入）BWM 管理介面提供整合式流量調整機制。輸出 BWM 可套用到從受信任公用區域到不受信任加密區域的流量。輸入 BWM 可套用到從不受信任加密區域到受信任公用區域的流量。

主題：

- 了解頻寬管理
- 設定頻寬管理設定
- 全域頻寬管理
- 進階頻寬管理
- 設定頻寬管理
- 升級到進階頻寬管理

附註：儘管 BWM 是完全整合的服務品質 (QoS) 系統，在此系統中分類和調整是在單一 SonicWall 裝置上執行的，可有效消除對外部系統的依賴性，因此無需進行標記，但可以針對單個存取規則同時設定 **BWM** 和 **QoS**（第 2 層和/或第 3 層標記）。即使已對流量進行調整，這也會使這些外部系統受益於防火牆上執行的指派。如需 BWM QoS 的詳細資料，請參閱管理服務品質。

了解頻寬管理

SonicWall 網路安全裝置使用 BWM 控制輸入和輸出流量。BWM 使網路管理員可以確保最小頻寬，並根據管理介面的**原則 | 規則 > 存取規則**頁面上建立的存取規則設定流量的優先順序。透過控制應用程式或使用者的頻寬量，網路管理員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。

BWM 優先順序佇列表格 列出 SonicOS 優先順序佇列。

BWM 優先順序佇列

0 - 即時	3 - 中高	6 - 低
1 - 最高	4 - 中	7 - 最低
2 - 高	5 - 中低	

有多種頻寬管理類型，並可在**安全設定 | 防火牆設定 > 頻寬管理**頁面上選擇。

頻寬管理類別

BWM 類型	說明
進階	啟用進階頻寬管理最大輸出和輸入頻寬限制可以透過設定頻寬物件、存取規則和應用原則在任何介面上逐一設定。
全域	所有區域均可為服務指派保證的最大頻寬，同時還可設定流量優先順序。啟用介面上的全域 BWM 後，根據優先順序佇列，此介面的所有傳送流量都會受到頻寬管理的控制。 預設全域 BWM 佇列： **2** - 高 **4** - 中 **6** - 低 非由啟用 BWM 的存取規則或應用程式控制原則管理的全部流量，其預設優先順序為 **4 中等**。對於 1 Gbps 以上的流量，因佇列之故，最大頻寬限制為 1 Gbps，其可能會限制處理的封包數。
無	（預設）停用 BWM。

如果頻寬管理類別是**無**，且有三種使用此介面的流量類型且介面的連結容量是 100 Mbps，則全部三種流量類型的累計容量為 100 Mbps。

啟用介面上的**全域**頻寬管理後，此介面的所有傳送流量都會受到頻寬管理的控制。如果可用的輸入和輸出流量設定為 10 Mbps，則預設會將全部三種流量類型傳送到中等優先順序佇列。中等優先順序佇列預設具有 50% 的保證頻寬和 100% 的最大頻寬。如果未設定**全域**頻寬管理原則，則每個流量類型的累計連結容量為 10 Mbps。

附註：BWM 的每個規則都會消耗記憶體進行封包佇列，因此 SonicOS 上允許佇列的封包數和規則受平台限制（值可以變更）。

全域使用來自其他佇列之未使用過的保證頻寬，以取得最大頻寬。如果只有預設值或單一佇列流量，而且所有的佇列將總共 100% 配置為已保證，則**全域**會使用來自其他佇列之未使用過的全域頻寬，提供您最大頻寬以用於預設/單一佇列。

術語

頻寬管理 (BWM)
任何用於調整流量或監管流量的各種演算法或方法。調整通常是指管理傳出流量，監管通常是指管理傳入流量（又稱許可控制）。有多種不同的頻寬管理方法，包括各種佇列和丟棄技術，每種方法都有其各自的設計強度。SonicWall 使用基於令牌基於類的佇列方法進行傳出和傳入 BWM，並對指定類型的傳入流量使用丟棄機制。

保證頻寬
介面上宣告的可用總頻寬的百分比，永遠會授與特定類別的流量。適用於傳入和傳出 BWM。透過所有 BWM 規則所保證的總頻寬不能超過可用總頻寬的 100%。SonicOS 5.0 及更高版本增強了頻寬管理功能，可提供速率限制功能。您可以建立指定第 2、3 或 4 層網路流量的最大速率的流量原則。也可將保證的頻寬設定為 0%。

輸入 BWM
用於調整流量進入指定介面時的速率。對於 TCP 流量，實際成形發生於 TCP 視窗調整機制調整輸入流速率時。對於 UDP 流量，如果 UDP 無原生回饋控制項，將使用丟棄機制。

最大頻寬:	介面上聲明的可用總頻寬的百分比，用於定義指定類別的流量所允許的最大頻寬。適用於傳入和傳出 BWM。用作限制機制，可指定頻寬速率限制。增強頻寬管理功能，以提供速率限制功能。您可以建立指定第 2、3 或 4 層網路流量的最大速率的流量原則。當主要 WAN 連結無法切換至不能處理足夠多流量的次要連接時，將啟用頻寬管理。最大頻寬可設定為 0%，如此可阻止所有的流量。
輸出 BWM	調節介面傳送流量的速率。傳出 BWM 使用基於貸記（或令牌）的佇列系統，此系統帶有 8 個優先順序環，可處理按照存取規則劃分的不同類型的流量。
優先順序	流量分類中使用的額外維度。針對用於 BWM 的佇列結構，SonicOS 使用八個優先順序值（0 = 最高，7 = 最低）。按照佇列的優先順序對其進行處理。
佇列	有效地使用連結上的可用頻寬。佇列通常用於對分類後的流量進行排序並單獨進行管理。

設定頻寬管理設定

先啟用**安全設定 | 防火牆設定 > 頻寬管理**頁面上的頻寬管理，再啟用介面/防火牆/應用程式規則上的 BWM，然後為輸入和輸出流量的介面配置可用頻寬，透過此方式可啟用 BWM。然後會為每個類別的網路流量指派單獨的限制。透過為網路流量指派優先順序，需要快速回應時間的應用程式（例如 Telnet）會優先於需要較短回應時間的流量（例如 FTP）。

若要檢視 BWM 設定，請導覽至**安全設定 |防火牆設定 > 頻寬管理**頁面。

附註：此頁面的預設值包含三個擁有預設定的最大保證頻寬的優先順序。優先順序「中」具有最大的保證值，因為此優先順序佇列預設情況下用於不受 BWM 啟用的原則控制的所有流量。

附註：SonicWall 設定了預設值，用於提供便於使用的 BWM。建議您檢閱指定的頻寬需要，並在此頁面上輸入對應的值。

- **頻寬管理類別**選項：

  重要：將**頻寬管理類型**：
  - 從**全域**變更為**進階**後，所有應用程式規則原則中使用的預設 BWM 操作都會自動轉換為**進階 BWM** 設定。
  - 從**進階**變更為**全域**時，預設的 BWM 操作轉換為 **BWM 全域-中**。

  您在不同**類型**之間切換時，防火牆不儲存之前的操作優先順序層級。您可以在**原則 | 規則 > 應用程式控制**頁面檢視對話。

  - **進階** - 任何區域都可以具有保證的和最大的頻寬以及按介面指派的優先順序排列流量。
  - **全域** - 所有區域均可為服務指派保證的最大頻寬，同時還可設定流量優先順序。對於 1 Gbps 以上的流量，最大頻寬限制為 1 Gbps。
  - **無** - 停用 BWM。這是預設值。
- **介面 BWM 設定** - 將滑鼠放在**問號**圖示，將顯示一個表格，表明是否已為多個介面上的輸入和輸出停用或啟用 BWM 設定。

- **全域優先順序**頻寬表 - 顯示優先順序的資訊：

  附註：僅當選擇**全域** BWM 時，才可以使用此表格。當選擇**進階**或**無**時，表格會呈現灰顯。

  - **優先順序** - 顯示優先順序數字和名稱。
  - **啟用** - 選擇此核取方塊後，將啟用此優先順序的優先順序佇。
  - **保證流量** - 為啟用的優先順序以百分比啟用保證率。介面上設定的頻寬可用於計算絕對值。

必須勾選對應的**啟用**核取方塊，才能使速率生效。預設，只有啟用這些優先順序及其保證百分比：

- **2 高** 30%
- **4 中** 50%
- **6 低** 20%

提示：您無法停用優先順序 **4 中**，但是您可以變更其百分比。

所有保證的頻寬總和不得超出 100%。如果頻寬超出 100%，**總數**會變成紅色。此外，每個佇列的保證頻寬不得大於頻寬上限。

- **最大\爆發流量** - 為啟用的優先順序以百分比啟用最大\爆發率。必須勾選對應的**啟用**核取方塊，才能使速率生效。

操作物件

操作物件定義應用程式規則原則如何作用於符合事件。您可以自訂操作，也可以選擇其中一個預先定義預設操作。在「應用程式規則」頁面上新增或編輯原則時，預先定義的操作將顯示在「應用程式控制原則設定」頁面上。

自訂 BWM 操作不同於預設 BWM 操作。透過在**原則 | 物件 > 操作物件**頁面上新增新操作物件並選擇頻寬管理操作類型，可設定自訂 BWM 操作。在頻寬管理類別從**全域**變更為**進階**和從**進階**變更為**全域**後，自訂 BWM 操作和原則仍保留其優先順序層級設定。

預先定義預設操作清單上也提供了很多 BWM 操作選項。BWM 操作選項的改變取決於**防火牆設定 > 頻寬管理**頁面上的「頻寬管理類別」設定。如果**頻寬管理類別**設定為：

- **全域**，則所有八個 BWM 層級都將可用。
- **進階**，則未設定優先順序。優先順序是透過在**原則 | 物件 > 頻寬物件**下設定頻寬物件來設定。

新增原則：預設操作表格列出了新增原則時可用的預先定義預設操作。

新增原則：預設操作

如果 BWM 類型 =	
全域	**進階**
BWM 全域-即時	進階 BWM 高
BWM 全域-最高	進階 BWM 中
BWM 全域-高	進階 BWM 低
BWM 全域-中高	
BWM 全域-中	
BWM 全域-中低	
BWM 全域-低	
BWM 全域-最低	

全域頻寬管理

可以使用以下方法設定全域頻寬管理：

- 設定頻寬管理

  重要：BWM 必須先在**安全設定 | 防火牆設定 > 頻寬管理**上啟用。

- 在介面上設定全域 BWM
- 在存取規則中全域設定 BWM
- 在操作物件中設定全域 BWM
- 設定 App 規則
- 設定 AppFlow 監控
- 元素的頻寬設定
- 無區域的頻寬管理
- 加權公平佇列
- 啟用進階頻寬管理
- 設定頻寬原則
- 設定介面頻寬限制與進階 BWM

設定頻寬管理

若要將頻寬管理類別設定為全域：

1 導覽到**安全設定 | 防火牆設定 > 頻寬管理**。

2 將**頻寬管理類別**選項設定為**全域**。

3 透過在**啟用**欄中勾選相應的核取方塊啟用想要的優先順序。

附註：您必須在此頁面中啟用優先順序才能在存取規則、應用程式規則和操作物件中設定這些優先順序。

4 輸入希望對各選擇的優先順序設定的**保證流量**頻寬百分比。總數量不能超過 100%。

5 輸入希望對各選擇的優先順序設定的**最大\爆發流量**頻寬百分比。

6 按一下**接受**。

在介面上設定全域 BWM

重要：全域 BWM 必須如設定頻寬管理中所述先在**防火牆設定 > 頻寬管理**上啟用。

在介面上設定 BWM 的步驟是：

1 導覽至**系統安裝 | 網路 > 介面**。

2 針對適當介面按一下**編輯**按鈕。將顯示**編輯介面**對話方塊。

3 按一下**進階**。

附註：顯示的選項將根據介面的設定有所不同。

4 捲動至**頻寬管理**。

5 選擇**啟用介面輸出頻寬限制**和**啟用介面輸入頻寬限制**核取方塊的其中之一或兩者。預設不選擇這些選項。

當這些選項之一或兩者被選定時，如果無相應存取規則或應用程式規則，將介面上的總輸出流量限制為在**啟用介面輸入頻寬限制 (kbps)** 欄位中指定的值。

如果未選擇任一選項，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輸出流量。

6 在**最大介面輸入頻寬 (Kbps)** 欄位，輸入所有輸入流量可用的總頻寬（單位為 Kbps）。預設值為 **384.000000** Kbps。

7 按一下**確定**。

在存取規則中全域設定 BWM

重要：全域 BWM 必須如設定頻寬管理中所述先在**安全設定 | 防火牆設定 > 頻寬管理**上啟用。

您可以在各存取規則中設定 BWM。此方法可設定套用 BWM 的方向，還可設定優先順序佇列。

重要：在存取規則中設定任何優先順序之前，您必須先在**安全設定 | 防火牆設定 > 頻寬管理**頁面上啟用想要使用的優先順序。請參閱**防火牆設定 > 頻寬管理**頁面，以確定要啟用的優先順序。如果您選擇未在**防火牆設定 > 頻寬管理**頁面上啟用的頻寬優先順序，流量將自動對應到第 **4 優先順序（中）**。請參閱設定頻寬管理。

優先順序列出在**存取規則**對話方塊的**頻寬優先順序**表中，詳情請參閱 BWM 優先順序佇列表格。

在存取規則中全域設定 BWM 的方法是：

1 導覽至**原則 | 規則 > 存取規則**頁面。

2 對於您想要編輯的規則，請按一下**編輯**圖示。將顯示**編輯規則**對話方塊。

3 按一下 **BWM**。

4 勾選**啟用輸出頻寬管理 (僅「允許」規則)** 核取方塊及**啟用輸入頻寬管理 (僅「允許」規則)** 核取方塊其中之一或兩者。預設不選擇這些選項。

a 從**頻寬優先順序**下拉功能表中選擇適當的頻寬優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

5 按一下**確定**。

在操作物件中設定全域 BWM

重要：全域 BWM 必須如設定頻寬管理中所述先在**安全設定 | 防火牆設定 > 頻寬管理**上啟用。

如果不想使用預先定義全域 BWM 操作或原則，可以選擇建立相符於您需要的新操作或原則。

建立新的全域 BWM 操作物件：

1 導覽至**原則 | 物件 > 操作物件**頁面。

2 按一下**操作物件**表頂部的**新增**按鈕。此時會顯示**新增/編輯操作物件**對話方塊。

3 在**操作名稱**欄位中，輸入操作物件的名稱。

4 在**操作**下拉功能表中，選擇**頻寬管理**，實現對應用程式層級頻寬使用的控制和監控。對話方塊的選項將改變。

5 若要依照優先順序指定 BWM，請勾選**啟用輸出頻寬管理**和**啟用輸入頻寬管理**核取方塊中的其中之一或兩者。預設不選擇這些選項。

   a 從**頻寬優先順序**下拉功能表中選擇適當的頻寬優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

6 按一下**確定**。

設定 App 規則

在 App 規則中設定 BWM 用於建立管理通訊協定中指定檔案類型消耗的頻寬，而允許其他檔案類型使用不受限頻寬的原則。這使您可以區分同一個通訊協定中所需的流量和不需要的流量。

App 規則 BWM 支援以下**原則類型**：

- SMTP 用戶端
- HTTP 用戶端
- HTTP 伺服器
- FTP 用戶端
- FTP 用戶端檔案上載
- FTP 用戶端檔案下載
- FTP 資料傳送
- POP3 用戶端
- POP3 伺服器
- 自訂原則
- IPS 內容
- 應用程式控制內容
- CFS

附註：在 App 規則中設定 BWM 前，必須首先啟用 BWM。

在應用程式規則中設定 BWM 之前：

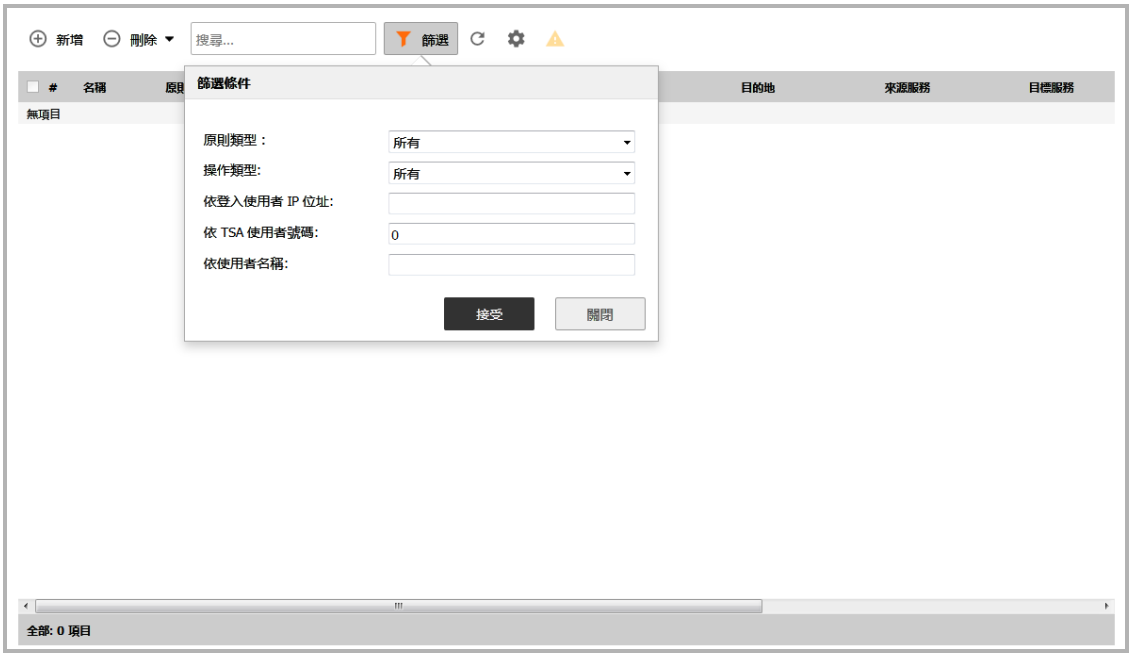
1 在**安全設定 | 防火牆設定 > 頻寬管理**中啟用希望使用的優先順序。請參閱設定頻寬管理。

2 在**操作物件**中啟用 BWM。請參見在操作物件中設定全域 BWM。

3 設定**介面**的 BWM。請參見在介面上設定全域 BWM。

若要在 App 規則中設定 BWM：

1 導覽至**原則 | 規則 > 應用程式控制**頁面。



2 在 **應用程式規則原則**下，從**操作類型**下拉功能表選擇操作類型。

3 對於想要設定的原則，按一下**設定**欄中的**編輯**圖示。**應用程式控制原則設定**對話顯示。

4 在**操作物件**下拉功能表中，選擇想要的 BWM 操作物件。

5 按一下**確定**。

設定 AppFlow 監控

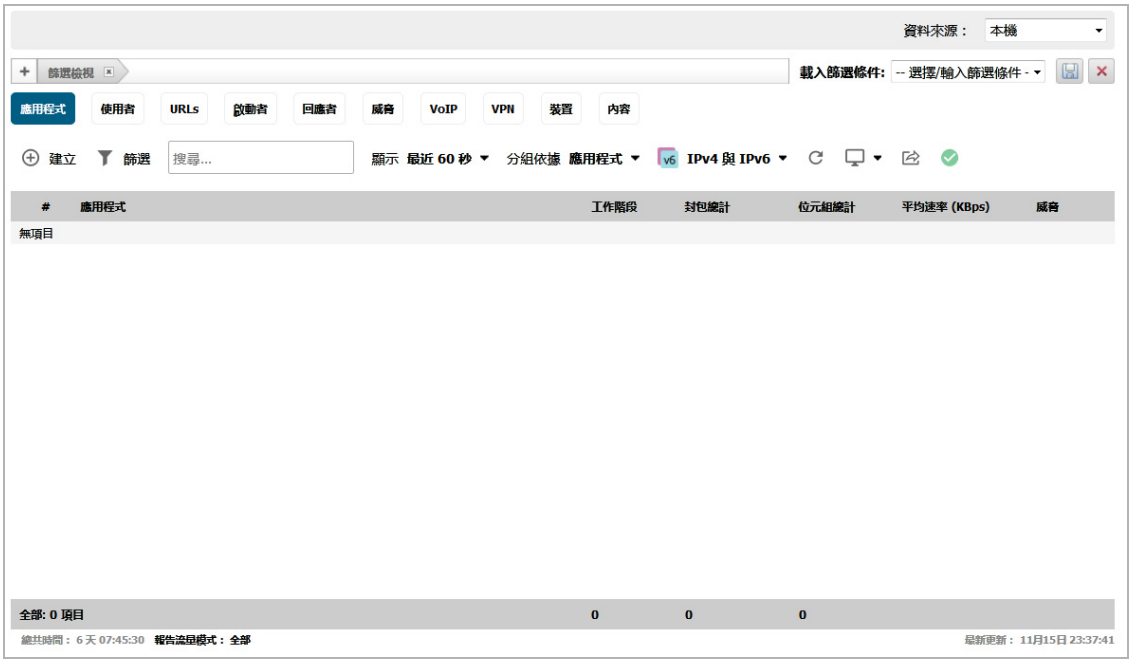
還可以透過選擇服務類型應用程式或簽章類型應用程式，然後按一下**建立規則**按鈕，在**記錄 > AppFlow 記錄**頁面設定 BWM。此處提供的「頻寬管理」選項取決於在**防火牆設定 > 頻寬管理**頁面的全域優先順序佇列表中啟用的優先順序層級。預設情況下啟用的優先順序層級為高、中和低。

附註：必須先啟用「SonicWall 應用程式視覺化」，才能繼續。

使用 AppFlow 監控設定 BWM：

1 選擇**調查**檢視。

2 導覽至**記錄 > AppFlow 記錄**頁面。



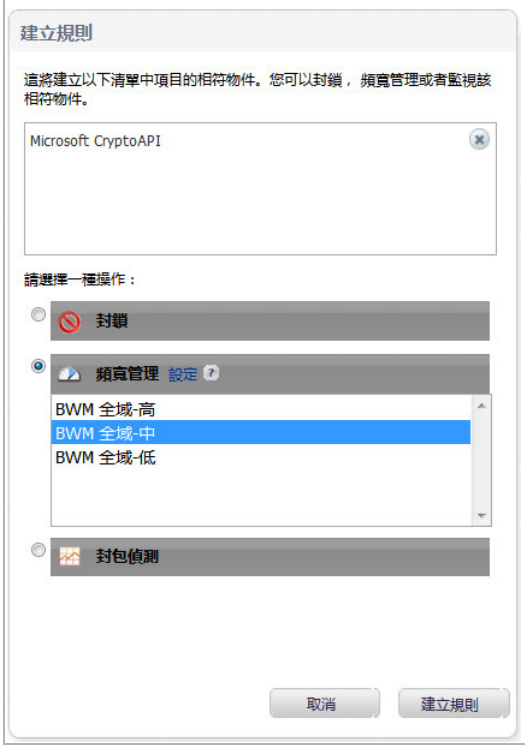
3 勾選想要套用全域 BWM 的服務型應用程式或簽章型應用程式。

附註：不能選擇一般應用程式。不能在一個規則中混合使用服務型應用程式和簽章型應用程式。

附註：建立服務型應用程式的規則將會建立防火牆存取規則，而建立簽章型 App 規則將會建立應用程式控制原則。

4 按一下**建立規則**。將顯示**建立規則**對話方塊。針對基於服務的應用程式選項的規則與針對基於簽章的應用程式選項的規則之間存在細微差異。

基於服務的應用程式選項

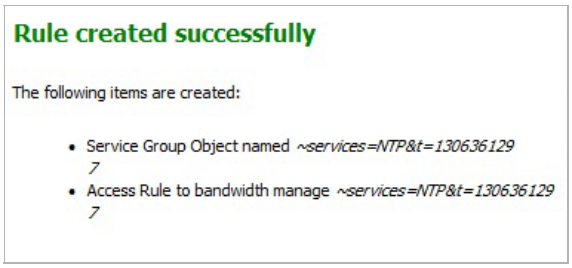


基於簽章的應用程式選項

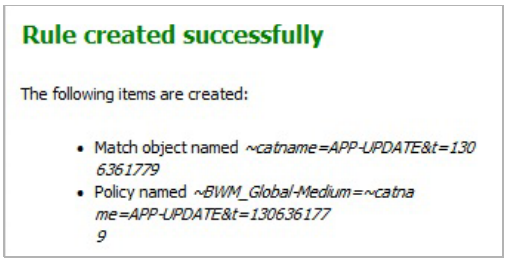
5 選擇**頻寬管理**選項按鈕。

6 選擇全域 BWM 優先順序。

7 按一下**建立規則**。將顯示確認對話方塊。為基於服務的應用程式選項建立的項目與為基於簽章的應用程式選項建立的項目之間存在細微差異。



基於服務的應用程式成功



基於簽章的應用程式成功

8 按一下**確定**。

9 如需驗證建立的規則，導覽至:

- **原則 | 規則 > 存取規則**頁面（針對基於服務的應用程式）。
- **原則 | 規則 > 進階應用程式控制**（針對基於簽章的應用程式）。

附註：對於基於服務的應用程式，新規則在**註解**欄中識別有**丁字**圖示，在**服務**欄中識別有首碼 `~services=<服務名稱>`。例如，`~services=NTP&t=1306361297`。

對於基於簽章的應用程式，新規則在**名稱**欄中使用首碼 `~BWM_Global-<優先順序>=~catname=<應用程式名稱>` 識別，在**物件**欄中使用首碼 `~catname=<應用程式名稱>` 識別。

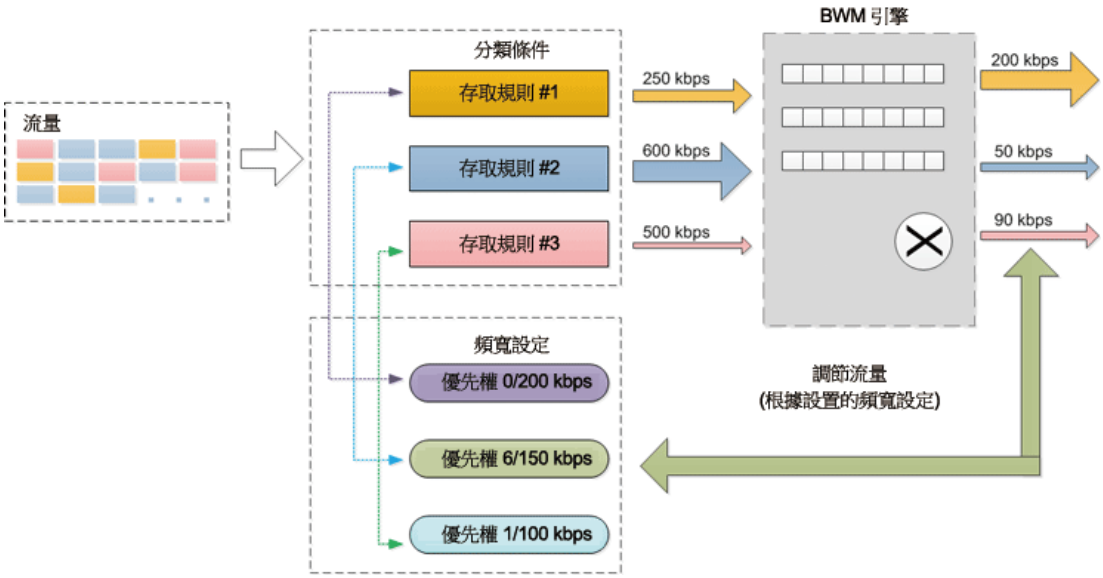
進階頻寬管理

進階頻寬管理使您能夠根據流量的優先順序和最大頻寬設定來管理流量的指定類別。進階頻寬管理包含三個主要元件：

- **分類器** - 將透過防火牆的封包分為相應的流量類別。
- **估算器** - 估計和計算在某時間間隔內流量類別使用的頻寬以確定此流量類別是否具有可用的頻寬。
- **排程器** - 根據估算器提供的流量類別的頻寬狀態排程流量傳送。

進階頻寬管理：基本概念解釋進階頻寬管理的基本概念。

進階頻寬管理：基本概念



頻寬管理設定基於用於指定流量類的頻寬限制的原則。完整的頻寬管理原則包含兩部分：分類器和頻寬規則。

頻寬規則用於指定實際參數，例如優先順序、保證的頻寬、最大頻寬和每 IP 頻寬管理，且在頻寬物件中進行設定。頻寬規則可以透過符合指定條件識別封包，並將其組織到各流量類。

分類器是在其中啟用頻寬物件的存取規則或 App 規則。存取規則和 App 規則針對具體的介面或介面區域進行設定。

頻寬管理中的第一步是對透過 SonicOS 防火牆的所有封包指派一個分類器（類別標記）。分類器識別屬於指定流量類別的封包。然後，將分類的封包傳送到 BWM 引擎以應用原則和成形。SonicOS 使用兩種分類器類型：

- 存取規則
- App 規則

包含子元素的規則稱為父規則。

設定頻寬物件：參數表格顯示在頻寬物件中設定的參數：

設定頻寬物件：參數

名稱	說明
保證頻寬	保證可以為指定流量類別提供的頻寬。
最大頻寬	流量類別可以利用的最大頻寬。
流量優先順序	流量類別的優先順序。 • **0** - 最高優先順序 • **7** - 最低優先順序
違反操作	在流量超過最大頻寬時防火牆採取的操作。 • **延時** - 封包佇列並在可能時將之傳送。 • **丟棄** - 立即丟棄封包。
啟用每 IP 頻寬管理	使防火牆能夠有效支援時間關鍵流量的元素功能，如語音和視訊。啟用每 IP 頻寬管理後，元素的頻寬設定將套用於其父規則下的各個 IP。

在將封包標籤為具體的流量類別後，BWM 引擎根據在頻寬物件中定義的、存取規則中啟用的和 App 規則中附加的頻寬設定收集封包以應用原則和成形。

分類器還會識別封包在流量流中的方向。可以設定輸出和/或輸入方向的分類器。對於頻寬管理，輸入和輸出的術語定義如下：

- **輸入** - 流量在指定流量流中從啟動者到回應者。
- **輸出** - 流量在指定流量流中從回應者到啟動者。

例如，介面 X0 後的用戶端連接至介面 X1 後的伺服器。流量方向表格顯示：

- 在用戶端和伺服器各方向的流量流方向
- 在各介面上的流量方向
- BWM 分類器表示的方向

流量方向

流量流方向	介面 X0 方向	介面 X1 方向	BWM 分類器
用戶端到伺服器	輸出	輸入	輸出
伺服器到用戶端	輸入	輸出	輸入

為了能與 WAN 區域中的傳統頻寬管理設定相容，術語傳入和傳出仍然適用於定義流量方向。這些術語僅適用於活動 WAN 區域介面。

- **傳出** - 從 LAN\DMZ 區域到 WAN 區域的流量（輸出）。
- **傳入** - 從 WAN 區域到 LAN\DMZ 區域的流量（輸入）。

元素的頻寬設定

元素的頻寬設定提供了一種方法，允許單項 BWM 規則套用於此規則的各個元素。每 IP 頻寬管理是一項「元素」功能，它是頻寬物件的子選項。啟用每 IP 頻寬管理後，元素的頻寬設定將套用於其父規則下的各個 IP。

元素的頻寬設定功能用於向父級流量類別下的各元素套用頻寬物件。元素的頻寬設定是「防火牆 > 頻寬物件」、父規則或流量類別的子選項。下表顯示在元素的頻寬設定下設定的參數。請參閱 *SonicWall SonicOS 6.5 原則*。

元素的頻寬設定：參數

名稱	說明
啟用每 IP 頻寬管理	啟用此選項後，最大元素頻寬設定將套用於父流量類別下的每個 IP 位址，這使防火牆能夠有效支援時間關鍵流量，如語音和視訊。
最大頻寬	可以指派到父級流量類別下的某 IP 位址的最大元素頻寬。 最大元素頻寬不能大於父級類別的最大頻寬。

啟用每 IP 頻寬管理後，其父規則下的每個 IP 將套用於元素的頻寬設定。

無區域的頻寬管理

無區域的頻寬管理功能允許在所有介面上進行頻寬管理，而不管其區域指派如何。以前，頻寬管理僅適用於以下這些區域：

- LAN/DMZ 至 WAN/VPN
- WAN/VPN 至 LAN/DMZ

在 SonicOS 6.2 及以上版本中，可以對所有區域的全部介面執行無區域的頻寬管理。

無區域的頻寬管理允許您在輸入方向、輸出方向或者雙向獨立設定最大頻寬限制，並使用存取規則和應用程式規則套用於任何介面。

附註：僅實體介面上擁有介面頻寬限制。容錯移轉和負載均衡設定不影響介面頻寬限制。

加權公平佇列

傳統上，SonicOS 頻寬管理根據封包的流量類別將流量指派到 8 個佇列。這 8 個佇列執行嚴格的優先順序佇列。總是最先傳送具有最高優先順序的封包。

嚴格的優先順序佇列可能導致高優先順序流量佔用介面上的所有可用頻寬，致使低優先順序流量無限期停留在佇列中。在嚴格的優先順序佇列中，排程器始終讓較高優先順序的佇列優先。這可能導致較低優先順序的佇列的頻寬匱乏。

加權公平佇列 (WFQ) 透過以循環配置資源機制服務各佇列中的封包緩解了頻寬匱乏問題，這樣在指定的時間間隔內，給所有佇列提供公平服務。高優先順序佇列獲得較多的服務，較低優先順序的佇列獲得較少的服務。佇列不會因為高優先順序而獲得所有服務，也不會因為低優先順序而得不到服務。

例如，設定流量類別 A 為優先順序 1，其最大頻寬為 400 kbps。設定流量類別 B 為優先順序 3，其最大頻寬為 600 kbps。這兩個流量類別都在最大頻寬僅為 500kbps 的介面佇列。兩個佇列以循環配置資源機制根據優先順序獲得服務。所以，服務兩個佇列，但流量類別 A 比流量類別 B 傳送更快。

連續採樣間隔的成形頻寬表格顯示各連續採樣間隔的成形頻寬：

連續採樣間隔的成形頻寬

採樣間隔	流量類別 A		流量類別 B	
	輸入 kbps	成形 kbps	輸入 kbps	成形 kbps
1	500	380	500	120
2	500	350	500	150
3	400	300	800	200
4	600	400	400	100
5	200	180	600	320
6	200	200	250	250

設定頻寬管理

- 啟用進階頻寬管理
- 設定頻寬原則
- 設定介面頻寬限制與進階 BWM

啟用進階頻寬管理

若要啟用進階頻寬管理：

1 在防火牆上，移至**安全設定 | 防火牆設定 > 頻寬管理**。

2 將**頻寬管理類別**選項設定為**進階**。

3 按一下**接受**。

附註：選擇**進階** BWM 後，優先順序欄位受到停用，無法在此設定。在進階 BWM 下，在頻寬原則中設定優先順序。請參閱設定頻寬原則。

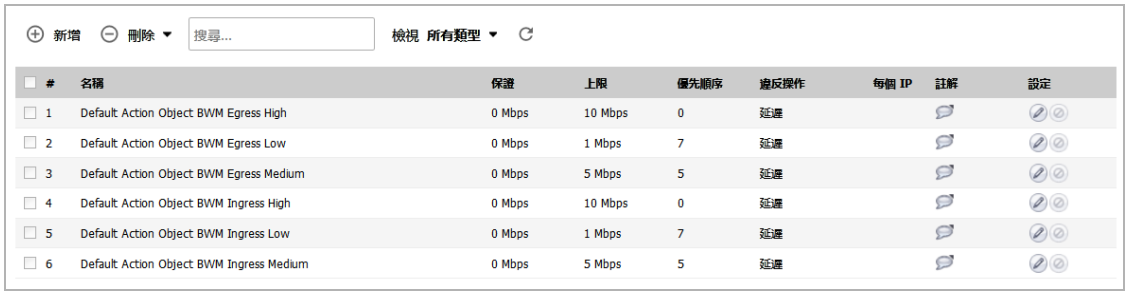
設定頻寬原則

- 設定頻寬物件
- 啟用元素的頻寬設定
- 在存取規則中啟用頻寬物件
- 在存取規則中啟用頻寬優先順序
- 在操作物件中啟用頻寬物件
- 在操作物件中啟用頻寬優先順序和頻寬物件

設定頻寬物件

設定頻寬物件的方法是：

1 導覽至**原則 | 物件 > 頻寬物件**。



2 執行以下任一動作：

- 按一下**新增**按鈕建立新頻寬物件。
- 按一下要變更的頻寬物件的**編輯**圖示。

頻寬物件設定對話顯示。

3 在**名稱**欄位中，輸入此頻寬物件的名稱。

4 在**保證頻寬**欄位，輸入此頻寬物件保證為某流量類提供的頻寬量（kbps 或 Mbps）。

a 從下拉功能表中，指定頻寬為 **kbps**（預設）或 **Mbps**。

5 在**最大頻寬**欄位中，輸入此頻寬物件為某流量類提供的最大頻寬量。

附註：在多個流量類爭奪共用頻寬時，實際指派的頻寬可能小於此值。

a 從下拉功能表中，指定頻寬為 **kbps**（預設）或 **Mbps**。

6 在**流量優先順序**欄位，輸入此頻寬物件為某流量類提供的優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

在多個流量類爭奪共用頻寬時，有最高優先順序的類佔先。

7 在**違反操作**欄位中，輸入在流量超出最大頻寬設定時此頻寬物件提供的操作：

- **延時** - 指定超量的流量封包將佇列並在可能時傳送。
- **丟棄** - 指定立即丟棄超量的流量封包。

8 在**註解**欄位中，輸入此頻寬物件的文字註解或描述。

9 按一下**確定**。

啟用元素的頻寬設定

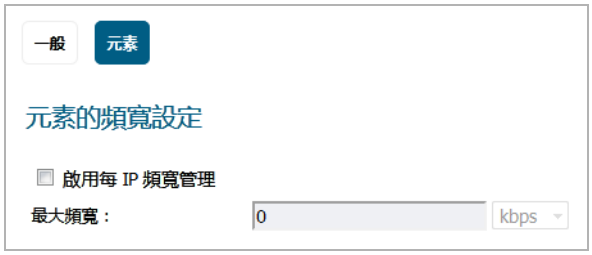
元素的頻寬設定使 SonicOS 可以對透過防火牆的各 IP 實施頻寬規則和原則。

若要在頻寬物件中啟用元素頻寬管理：

1 導覽至**原則 | 物件 > 頻寬物件**。

2 按一下要變更的頻寬物件的**編輯**圖示。**頻寬物件設定**對話顯示。

3 按一下**元素**。



4 選擇**啟用每 IP 頻寬管理**選項。預設情況下未勾選此選項。在啟用後，最大元素頻寬設定套用於父級流量類別下的各單獨 IP。

5 在**最大頻寬**欄位，輸入可以指派到父級流量類別下通訊協定的最大元素頻寬。

   a 從下拉功能表中，指定頻寬為 **kbps**（預設）或 **Mbps**。

6 按一下**確定**。

在存取規則中啟用頻寬物件

若選擇進階 BWM，您可在**規則 > 存取規則**中啟用頻寬物件（及其設定）。

若要在存取規則中啟用頻寬物件：

1 導覽至**原則 | 規則 > 存取規則**。

2 執行以下任一動作：

- 按一下**新增**按鈕建立新存取規則。將顯示**新增規則**對話方塊。
- 按一下適當存取規則的**編輯**圖示。將顯示**編輯規則**對話方塊。

3 按一下 **BWM**。

4 若要啟用輸出方向的頻寬物件，在**頻寬管理**下選擇**啟用輸出頻寬管理**核取方塊。

5 從**選擇頻寬物件**下拉功能表中選擇需要用於輸出方向的頻寬物件。

6 若要啟用輸入方向的頻寬物件，在**頻寬管理**下選擇**啟用輸入頻寬管理**核取方塊。

7 從**選擇頻寬物件**下拉功能表中選擇需要用於輸入方向的頻寬物件。

8 若要啟用頻寬使用追蹤，請選擇**啟用追蹤頻寬使用**選項。

9 按一下**確定**。

在存取規則中啟用頻寬優先順序

若選擇**全域 BWM**，您可以在**規則 > 存取規則**中啟用頻寬優先順序。

在存取規則中啟用頻寬優先順序：

1 導覽至**原則 | 規則 > 存取規則**。

2 執行以下任一動作：

- 按一下**新增**按鈕建立新存取規則。將顯示**新增規則**對話方塊。
- 按一下適當存取規則的**編輯**圖示。將顯示**編輯規則**對話方塊。

3 按一下 **BWM**。

4 若要啟用輸出方向的頻寬物件，在**頻寬管理**下選擇**啟用輸出頻寬管理**核取方塊。預設情況下未勾選此選項。

5 在**頻寬優先順序**下拉功能表中，選擇您要用於輸出方向的頻寬優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

6 若要啟用輸入方向的頻寬物件，在**頻寬管理**下選擇**啟用輸入頻寬管理**核取方塊。預設情況下未勾選此選項。

7 在**頻寬優先順序**下拉功能表中，選擇您要用於輸入方向的頻寬優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

8 按一下**確定**。

在操作物件中啟用頻寬物件

若選擇**進階 BWM**，您可在**規則 > 存取規則**中啟用頻寬物件（及其設定）。

若要在操作物件中啟用頻寬物件：

1 導覽至**原則 | 物件 > 操作物件**。

2 透過按一下**新增**按鈕建立新的操作物件。**操作物件設定**對話顯示。

3 在**操作名稱**欄位中輸入操作物件的名稱。

4 從**操作**下拉功能表中，選擇**頻寬管理**，這將實現對應用程式層級頻寬使用的控制和監控。**操作物件設定**對話方塊的選項將改變。

5 在**頻寬彙總方法**下拉功能表中，選擇相應的頻寬彙總方法。

- **依原則** (預設)
- **依動作**

6 若要啟用輸出方向的頻寬管理，請選擇**啟用輸出頻寬管理**選項。

a 從**頻寬物件**下拉功能表中選擇用於輸出方向的頻寬物件。

7 若要啟用輸入方向的頻寬管理，請選擇**啟用輸入頻寬管理**選項。

a 從**頻寬物件**下拉功能表中選擇用於輸入方向的頻寬物件。

8 若要啟用頻寬使用追蹤，請選擇**啟用追蹤頻寬使用**選項。僅在**啟用頻寬管理**選項的其中之一或兩者均選定時，才能使用此選項。

9 按一下**確定**。

在操作物件中啟用頻寬優先順序和頻寬物件

若選定**全域 BWM**，您可在**規則 > 存取規則**中指定 BWM 優先順序，並啟用頻寬物件（及其設定）。

在操作物件中啟用頻寬優先順序和頻寬物件：

1 導覽至**原則 | 物件 > 操作物件**。

2 透過按一下**新增**按鈕建立新的操作物件。**操作物件設定**對話顯示。

3 在**操作名稱**欄位中輸入操作物件的名稱。

4 從**操作**下拉功能表中，選擇**頻寬管理**，這將實現對應用程式層級頻寬使用的控制和監控。**操作物件設定**對話方塊的選項將改變。

5 若要在輸出方向啟用頻寬管理，請選擇**啟用輸出頻寬管理**當做優先順序選項。

   a 從**頻寬優先順序**下拉功能表中選擇用於輸出方向的頻寬物件。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

6 若要啟用輸入方向的頻寬管理，請選擇**啟用輸入頻寬管理**當做優先順序選項。

   a 從**頻寬優先順序**下拉功能表中選擇用於輸入方向的頻寬物件。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

7 按一下**確定**。

設定介面頻寬限制與進階 BWM

若要設定介面的頻寬限制：

1 導覽至**系統安裝 | 網路 > 介面**。

2 針對適當介面按一下**編輯**圖示 。將顯示**編輯介面**對話方塊。

3 按一下**進階**。

4 捲動至**頻寬管理**區段。

5 選擇**啟用介面輸出頻寬限制**選項。預設情況下未勾選此選項。

當此選項為：

- 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輸出流量。

a 在**最大介面輸出頻寬 (kbps)** 欄位，輸入此介面的最大輸出頻寬（千位元組/秒）。預設值為 **384.000000** Kbps。

6 選擇**啟用介面輸入頻寬限制**選項。預設情況下未勾選此選項。如需使用此選項的相關資訊，請參閱步驟 5。

7 按一下**確定**。

設定介面頻寬限制與全域 BWM

若要設定介面的頻寬限制：

1 導覽至**系統安裝 | 網路 > 介面**。

2 針對適當介面按一下**編輯**圖示 。將顯示**編輯介面**對話方塊。

3 按一下**進階**。

4 捲動至**頻寬管理**區段。

5 選擇**啟用介面輸出頻寬限制**選項。預設情況下未勾選此選項。

當此選項為：

- 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輸出流量。

a 在**最大介面輸出頻寬 (kbps)** 欄位，輸入此介面的最大輸出頻寬（千位元組/秒）。預設值為 **384.000000** Kbps。

6 選擇**啟用介面輸入頻寬限制**選項。預設情況下未勾選此選項。預設情況下未勾選此選項。如需使用此選項的資訊，請參見步驟 5。

7 按一下**確定**。

升級到進階頻寬管理

進階頻寬管理使用頻寬物件作為設定方法。頻寬物件是在**物件 > 頻寬物件**下設定，然後在**規則 > 存取規則**中啟用。

進階頻寬升級功能將所有活動、有效、傳統的 BWM 設定自動轉換頻寬物件設計模型。

在傳統的 BWM 設定中，BWM 引擎僅影響痛過主要 WAN 介面或活動負載均衡 WAN 介面的流量。不透過這些介面的流量不受頻寬管理限制，不管其**存取規則**或**應用程式規則**設定如何。

在進階頻寬管理下，BWM 引擎可以在任何介面實施頻寬管理設定。

在進階頻寬管理升級過程中，SonicOS 將傳統的 BWM 設定轉換為預設頻寬物件，並將其連結到原始分類器規則（**存取規則**或**應用程式規則**）。自動產生的預設頻寬物件繼承輸入和輸出方向的所有 BWM 參數。

以下兩幅圖顯示傳統的 BWM 設定。後面一幅圖顯示在進階頻寬管理升級過程中自動產生的新頻寬物件。

傳統的存取規則設定顯示來自**規則 > 存取規則 > 設定**對話的傳統的**存取規則**設定。

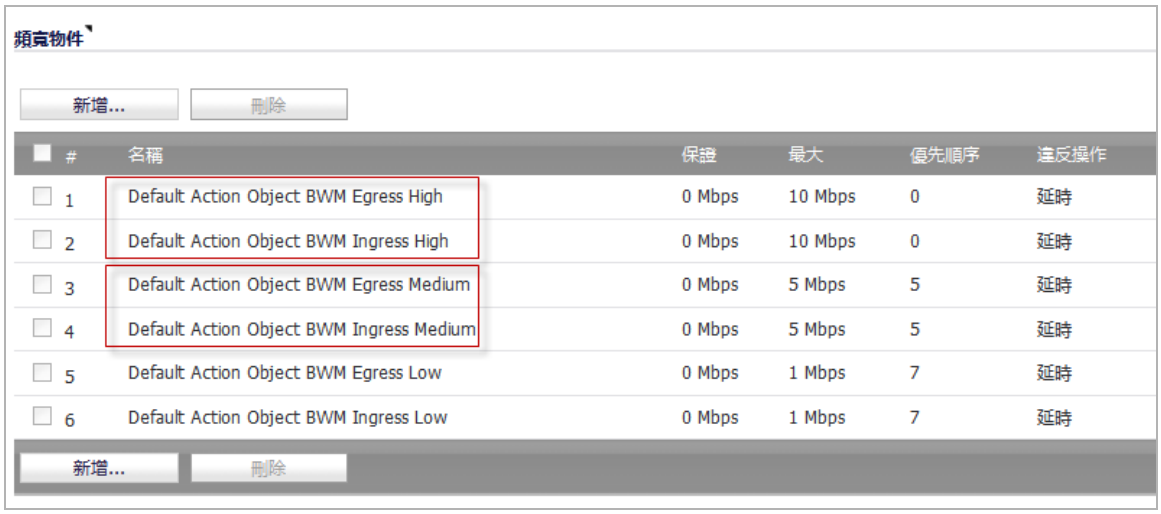
傳統的存取規則設定

傳統的操作物件設定 顯示來自**防火牆 > 操作物件 > 設定**對話的傳統的**操作物件**設定。

傳統的操作物件設定

自動產生的四個頻寬物件顯示在進階頻寬管理升級過程中自動產生的四個新頻寬物件。這些設定可以在**防火牆 > 頻寬物件**頁面檢視。

自動產生的四個頻寬物件



3

設定洪水防護

附註：控制面攻擊保護位於**防火牆設定 > 進階設定**頁面。

提示：必須按一下**接受**以啟用您選擇的任何設定。

防火牆設定 > 洪水防護頁面使您能夠進行以下操作：

- 管理：
  - TCP（傳輸控制通訊協定）流量設定，例如第 2 層/第 3 層洪水防護，WAN DDOS 防護
  - UDP（使用者資料包通訊協定）洪水防護
  - ICMP（網際網路控制訊息通訊協定 ）或 ICMPv6 洪水防護。

- 檢視透過安全裝置的流量的統計：
  - TCP 流量
  - UDP 流量
  - ICMP 或 ICMPv6 流量

SonicOS 透過監視流向定義目的地的 IPv6 UDP/ICM 流量來抵禦 UDP/ICMP 洪水攻擊。如果一個或多個來源超過設定的閾值，就丟棄到指定的目的地的 UDP/ICMP 封包。

主題：

- TCP 檢視
- UDP 檢視
- ICMP 檢視

TCP 檢視

主題：

- TCP 設定
- 第 3 層 SYN 攻擊保護 - SYN Proxy 檢視
- 設定第 3 層 SYN 洪水防護
- 設定第 2 層 SYN/RST/FIN/TCP 洪水防護 - MAC 黑名單
- WAN DDOS 防護 (非 TCP 洪水)

TCP 設定

- **嚴格強制 TCP 與 RFC 793 和 RFC 1122 相容** - 以確保嚴格遵循多個 TCP 逾時規則。此設定最大程度保證了 TCP 的安全性，但可能會使 Window Vista 使用者出現 Windows 縮放功能問題。預設情況下未勾選此選項。
    - **啟用 TCP 交握強制** - 需要對所有 TCP 連線成功進行三次交握。僅當未預設選擇**嚴格強制 TCP 與 RFC 793 和 RFC 1122 相容**時，此選項可用。
- **啟用 TCP 總和檢查碼強制** - 如果計算了無效的 TCP 總和檢查碼，將丟棄封包。預設情況下未勾選此選項。
- **啟用 TCP 交握逾時** - 強制 TCP 三次交握至其完成連接的逾時期限（以秒為單位）。如果 TCP 的三次交握未在逾時期限內完成，它會被丟棄。預設情況下已核取此選項。
    - **TCP 交握逾時 (秒)**：TCP 交握必須完成連接的最長時間。預設值為 **30** 秒。
- **預設 TCP 連線逾時** - 指派給 TCP 流量存取規則的預設時間。如果某個 TCP 在超出此設定值的一段時間處於活動狀態，則 TCP 連線會被防火牆清除。預設值為 **15** 分鐘，最小值為 1 分鐘，最大值為 999 分鐘。

    附註：設定過長的連接逾時將減慢舊有資源的回收，在極端情況下，可能導致連接快取耗盡。

- **最大區段存留時間 (秒)** - 確定任何 TCP 封包過期之前有效的秒數。此設定也可用於確定主動關閉的 TCP 連線處於 TIME_WAIT 狀態的時間（計算為段最大存留時間的兩倍或 2MSL），以確保正確的 FIN / ACK 交換，從而完全關閉 TCP 連線。預設值為 **8** 秒，最小值為 1 秒，最大值為 60 秒。
- **啟用半開放 TCP 連線數閾值** - 如果已達到 TCP 半開放連接的高標，將拒絕新的 TCP 連線。預設情況下，未監視半開放 TCP 連線，因此未選擇此選項。
    - **半開放 TCP 連線數上限** - 指定半開放 TCP 連線的最大數。預設最大值是連接快取最大值的一半。

第 3 層 SYN 攻擊保護 - SYN Proxy 檢視

主題：

- SYN 洪水防護方法
- 設定第 3 層 SYN 洪水防護

SYN 洪水防護方法

SYN/RST/FIN 洪水防護有助於防護防火牆之後的主機免受嘗試透過建立以下其中一種攻擊機制來消耗主機的可用資源的拒絕服務 (DoS) 或分布式 DoS 攻擊：

- 傳送使用無效或欺騙 IP 位址的 TCP SYN 封包、RST 封包或 FIN 封包。
- 建立數量過多的半開放 TCP 連線。

以下部分詳細介紹了一些 SYN 洪水防護方法：

- 使用無狀態 Cookie 的 SYN 洪水防護
- 指定層的 SYN 洪水防護方法
- 了解 SYN 監視清單
- 了解 TCP 交握

使用無狀態 Cookie 的 SYN 洪水防護

從 SonicOS 開始使用的 SYN 洪水防護方法使用了無狀態 SYN Cookie，這可增加 SYN 洪水防護的可用性，同時提高防火牆上的資源的總體利用率。使用無狀態 SYN Cookie，防火牆無需維護半開放連接的狀態。它使用加密計算（而非隨機）到達 SEQr。

指定層的 SYN 洪水防護方法

SonicOS 對受信任（內部）和不受信任（外部）這兩種不同環境產生的 SYN 洪水，提供了多種防護。來自*不受信* WAN 網路的攻擊通常發生在受防火牆防護的一個或多個伺服器上。來自*受信任* LAN 網路的攻擊通常是由於一個或多個受信網路內部感染病毒，從而對一個或多個本機或遠端主機進行攻擊。

為了對這兩種攻擊提供防火牆防禦，SonicOS 針對這兩種不同的層提供了單獨的 SYN 洪水防護機制。每種機制都收集並顯示了 SYN 洪水統計，還產生了重要 SYN 洪水事件的記錄訊息。

- **SYN Proxy（第 3 層）**- 此機制使用 SYN Proxy 實作，在將 WAN 用戶端的連接請求轉送至受防護的伺服器之前，先對此用戶端進行驗證，透過此方式屏蔽了受信任網路中的伺服器，使其免受 WAN 的 SYN 洪水攻擊。您可以只啟用 WAN 介面上的 SYN Proxy。
- **SYN 黑名單（第 2 層）**- 此機制封鎖指定裝置產生或轉送 SYN 洪水攻擊。您可以啟用任何介面上的 SYN 黑名單。

了解 SYN 監視清單

以上兩種 SYN 洪水防護機制的內部體系結構基於一個乙太網路位址清單，透過這些位址，大多數活動的裝置可將其初始 SYN 封包傳送至防火牆。此清單稱為 *SYN 監視清單*。由於此清單包含乙太網路位址，裝置將根據轉送 SYN 封包的裝置的位址追蹤所有 SYN 流量，而不考慮目的地位址的 IP 來源。

每個監視清單項目都包含一個名稱為*命中次數*的值。當裝置接收來自對應裝置的初始 SYN 封包時，命中值次數增加。當 TCP 三次完成後，命中次數值減少。任何指定裝置的命中次數通常等於自上次裝置重設命中次數起掛起的半開放連接數。裝置重設命中次數的預設值是每秒一次。

在確定記錄訊息或狀態變更的必要性時，用於記錄、SYN Proxy和 SYN 黑名單的閾值都將與命中次數值相比較。發生 SYN 洪水攻擊時，由於欺騙連接的嘗試，從轉送攻擊封包的裝置掛起的半開放連接的數量會明顯增加。正確設定攻擊閾值後，正常的流量會產生一些攻擊警告，但相同的閾值會在產生嚴重的網路降級之前偵測並轉移攻擊。

了解 TCP 交握

典型的 TCP 交握（簡化）從啟動者傳送帶有 32 位元順序 (SEQi) 編號的 TCP SYN 封包開始。然後回應者透過傳送等於 SEQi+1 的 ACK 和隨機 32 位元順序編號 (SEQr)，傳送用於確認接收順序的 SYN/ACK 封包。回應者也保持等待來自啟動者的 ACK 的狀態。啟動者的 ACK 封包應包含下一個順序 (SEQi+1) 以及從回應者接收的順序確認（透過傳送等於 SEQr+1 的 ACK）。交換如下所示：

1 啟動者 -> SYN (SEQi=0001234567, ACKi=0) -> 回應者

2 啟動者 <- SYN/ACK (SEQr=3987654321, ACKr=0001234568) <- 回應者

3 啟動者 -> ACK (SEQi=0001234568, ACKi=3987654322) -> 回應者

由於回應者需要保持所有半開放 TCP 連線的狀態，如果 SYN 發生的時間早於回應者處理或清除 SYN 的時間，則可能會消耗記憶體。儘管完成了三次交握，半開放 TCP 連線仍無法轉換到已建立的狀態。如果防火牆是在啟動者和回應者之間，它可有效的成為回應者或*代理*，TCP 與實際回應者（私人主機）的連接受其防護。

設定第 3 層 SYN 洪水防護

SYN 洪水防護模式是您可以選擇用於防禦半開放 TCP 工作階段和高頻率 SYN 封包傳送的防護層級。此功能用於設定三種不同的 SYN 洪水防護層級。

設定 SYN 洪水防護功能的方法是：

1 移至**安全設定 | 防火牆設定 > 攻擊保護**頁面的**第 3 層 SYN 攻擊保護 - SYN Proxy** 部分。

2 從 **SYN 洪水防護模式**下拉列表中，選擇保護模式的類型：

- **觀察和報告可能的 SYN 洪水** - 使裝置可以監視裝置上所有介面的 SYN 流量，並記錄超過封包計數閾值的可疑 SYN 洪水活動。此功能不會打開裝置上的 SYN Proxy，因此裝置轉送未修改的 TCP 三次交握。

  這是 SYN 洪水防護的最低侵略性層級。如果您的網路不在高風險環境中，請選擇此選項。

- **有可疑的攻擊時進行 Proxy WAN 用戶端連線** - 如果每分鐘嘗試的不完整連接數超過了指定的閾值，則此選項使裝置可以啟用 WAN 介面上的 SYN Proxy 功能。此方法可確保攻擊期間裝置可繼續處理有效流量，並且效能不會降級。代理模式將一直處於啟用狀態，除非所有 WAN SYN 洪水攻擊停止或所有 WAN SYN 洪水攻擊的裝置黑名單都使用 SYN 黑名單功能。

  這是 SYN 洪水防護的中間層級。如果您的網路遇到來自內部或外部資源的 SYN 洪水攻擊，請選擇此選項。

- **永遠進行 Proxy WAN 用戶端連線** - 將裝置設定為始終使用 SYN Proxy。此方法可封鎖所有欺騙 SYN 封包通過裝置。

  這是極度安全的度量值，可指示裝置回應所有 TCP 連線埠上的連接埠掃描，因為 SYN Proxy 功能會強制裝置回應所有 TCP SYN 連接嘗試。這會降級效能並可產生誤報。僅當網路處於高風險環境中時，請選擇此選項。

3 選擇 **SYN 攻擊閾值**設定選項提供了裝置丟棄封包之前 SYN 洪水活動的限制。裝置收集了 WAN TCP 連線的統計，同時追蹤最大值和平均最大值以及每秒鐘不完整的 WAN 連接數。透過這些統計資訊，裝置對 SYN 閾值使用建議值。

- **從收集的分析資料算出建議值** - 建議的攻擊閾值基於 WAN TCP 連線統計。
- **攻擊閾值 (不完全的連線嘗試次數 / 秒)** - 用於設定裝置丟棄封包之前每秒鐘嘗試的不完整連接數，值介於 5 和 200,000 之間。預設為**從收集的分析資料算出建議值**。

4 選擇**SYN-Proxy 選項**以在 SYN Proxy 模式中要對傳送給 WAN 用戶端的選項提供更多控制。

附註：如果選擇**觀察和報告可能的 SYN 洪水**作為 **SYN 洪水防護**模式，此部分的選項將無法使用。

裝置將 SYN Proxy套用到 TCP 連線時，使用已建立的 SYN/ACK 回應初始 SYN 封包，同時在向伺服器轉送連接請求時等待 ACK 回應。使用 SYN 洪水封包攻擊的裝置不會回應 SYN/ACK 回覆。由於缺少此類型的回應，防火牆將對其進行識別，並封鎖欺騙的連接嘗試。在不知道伺服器將如何正常回應 SYN/ACK 封包上的 TCP 選項的情況下， SYN Proxy 將強制防火牆產生 SYN/ACK 回應。

- **所有的 LAN/DMZ 伺服器皆支援 TCP SACK 選項** - 當可以丟棄封包並且接收的裝置指示接收了哪個封包時，此核取方塊將啟用 SACK（選擇性確認）。預設情況下未啟用此選項。只有在確定防火牆包含的所有伺服器都從支援 SACK 選項的 WAN 存取時，才能啟用此核取方塊。
- **限制 MSS 傳送到 WAN 用戶端 (當進行 Proxy 連線)** - 用於輸入最大的 MSS（最小段大小）值。這將設定 TCP 段大小的閾值，可防止傳送給目的地伺服器的段太大。例如，如果伺服器是 IPsec 閘道，則可能需要限制接收的 MSS，以在通道傳送流量時為 IPsec 標頭提供空間。代理序列期間伺服器在回應 SYN 產生的封包時，無法預測傳送給伺服器的 MSS 值。由於能夠控制段的大小，您可以控制傳送給 WAN 用戶端的已建立的 MSS 值。預設情況下未勾選此選項。

  如果指定預設值 **1460** 的替代值，則此大小的段或更小的段將被傳送到 SYN/ACK cookie 中的用戶端。當永遠啟用 SYN Proxy 時，將此值設定過低可能會降低效能。如果伺服器回應較小的 MSS 值，則將此值設定過高可能會中斷連線。

  - **傳送到 WAN 用戶端的最大 TCP MSS**。MSS 的值。預設值為 **1460**，最小值為 32，最大值為 1460。

  附註：使用代理 WAN 用戶端連接時，請謹慎地設定這些選項，因為發生 SYN 洪水時，這些設定僅影響連接。如此可確保在攻擊期間合法的連線可以繼續。

- **永遠記錄收到的 SYN 封包。**記錄所有收到的 SYN 封包

第 2 層 SYN/RST/FIN/TCP 洪水防護 - MAC 封鎖清單

SYN/RST/FIN 黑名單功能列出了超出 SYN、RST 和 FIN 黑名單攻擊閾值的裝置。在封包評估過程中，防火牆裝置將丟棄從黑名單裝置傳送的封包，使防火牆可以處理更多的此類封包，同時能夠防禦對本機網路的攻擊，還提供了對 WAN 網路的第二層防護。

裝置不能同時發生在 SYN/RST/FIN 黑名單清單和監視清單中。啟用黑名單後，防火牆將從監視清單中移除超過黑名單閾值的裝置，並將其置於黑名單中。相反，如果防火牆從黑名單中移除裝置，則會將其重新置於監視清單中。在來自此裝置的洪水已終止後的大約三秒鐘內，將從黑名單中移除其 MAC 位址位於黑名單中的任何裝置。

設定第 2 層 SYN/RST/FIN/TCP 洪水防護 - MAC 黑名單

- **SYN/RST/FIN 洪水黑名單的閾值（SYN / Sec）**- 指定每秒鐘允許的最大 SYN、RST、FIN 和 TCP 封包數。最小值為 10，最大值為 800000，預設值為 **1,000**。此值應大於 SYN Proxy 閾值，因為黑名單清單會嘗試封鎖更多強大的本機攻擊或者來自 WAN 網路的嚴重攻擊。

  ⓘ **附註：**除非啟用在所有介面上的**啟用 SYN/RST/FIN/TCP 洪水封鎖清單**，否則不能修改此選項。

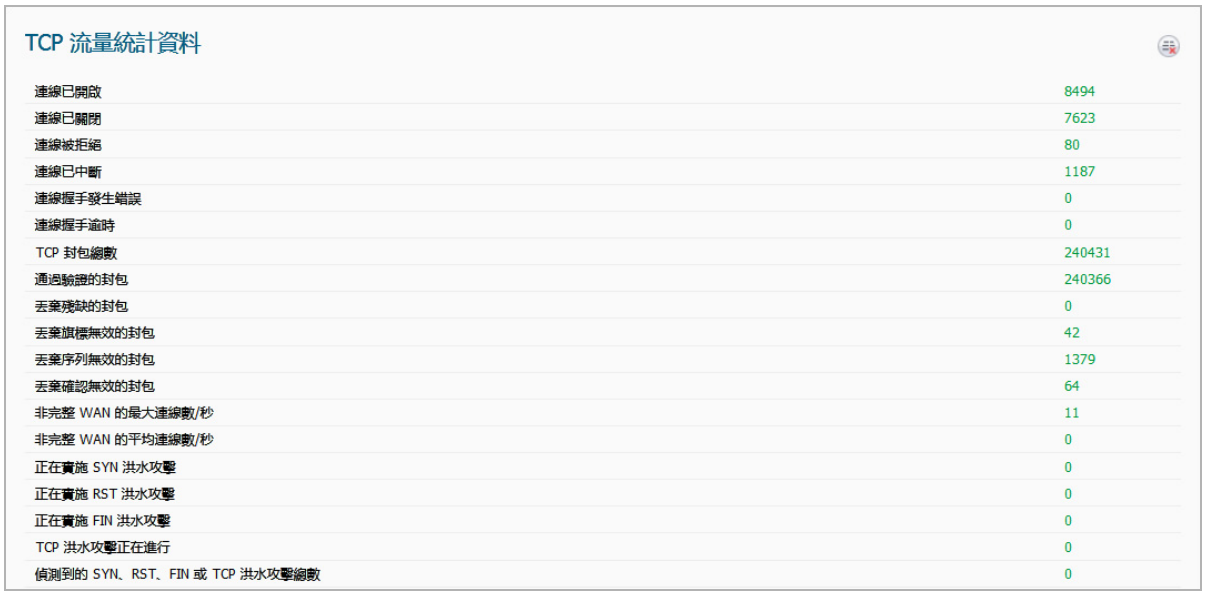
- **啟用所有介面上的 SYN/RST/FIN/TCP 洪水封鎖清單** - 將啟用防火牆上所有介面的黑名單功能。預設情況下未勾選此選項。選擇此選項後，以下選項變為可用：
  - **永不封鎖 WAN 機器** - 確保 WAN 上的系統從不會新增到 SYN 黑名單中。推薦選擇此選項，否則可能會中斷防火牆 WAN 連接埠的流量傳送。預設情況下未勾選此選項。
  - **永遠允許 SonicWall 管理流量** - 使通向防火牆 WAN IP 位址的黑名單裝置的 IP 流量不會被篩選掉。這將允許管理流量和路由通訊協定保持透過黑名單裝置的連線。預設情況下未勾選此選項。

WAN DDOS 防護 (非 TCP 洪水)

WAN DDOS 防護 (非 TCP 洪水)部分是一種已經被棄用的功能，並為 UDP 檢視和 ICMP 檢視中介紹的 **UDP 洪水防護**和 **ICMP 洪水防護**分別取代。

ⓘ **重要：**SonicWall 推薦您不要使用 **WAN DDOS 防護**功能，而應使用 **UDP 洪水防護**和 **ICMP 洪水防護**。

TCP 流量統計



TCP 流量統計表格介紹 **TCP 流量統計**表中的項目。如需清除並重新啟動表中顯示的統計，按一下此表的**清除統計**圖示。

TCP 流量統計

此統計	將增加/顯示
連線已開啟	當 TCP 連線啟動者傳送 SYN 或 TCP 連線回應者接收 SYN 時。
連線已關閉	當啟動者和回應者傳送 FIN 並接收 ACK 時如果 TCP 連線關閉時。
連線被拒絕	當遇到 RST 並且回應者處於 SYN_RCVD 狀態時。

TCP 流量統計

此統計	將增加/顯示
連線已中斷	當遇到 RST 並且回應者處於除 SYN_RCVD 之外的某種狀態時。
連線交握錯誤	當發生交握錯誤時。
連線交握逾時	當交握逾時的時候。
TCP 封包總數	根據每個處理的 TCP 封包。
通過驗證的封包	當： • TCP 封包通過總和檢查碼驗證（已啟用 TCP 總和檢查碼驗證）。 • 遇到有效的 SYN 封包（已啟用 SYN 洪水防護）。 • 在設定了 ACK 旗標的封包上成功驗證 SYN Cookie（已啟用 SYN 洪水防護）。
丟棄殘缺的封包	當： • TCP 總和檢查碼驗證失敗（已啟用 TCP 總和檢查碼驗證）。 • 遇到 TCP SACK 允許的選項，但計算的選項長度不正確。 • 遇到 TCP MSS（最大段大小）選項，但計算的選項長度不正確。 • TCP SACK 選項資料計算為小於最小值 6 位元組，或者對於資料塊大小 4 位元組設定的模不一致。 • TCP 選項長度確定為無效。 • TCP 標頭長度計算為小於最小值 20 位元組。 • TCP 標頭長度計算為大於封包的資料長度。

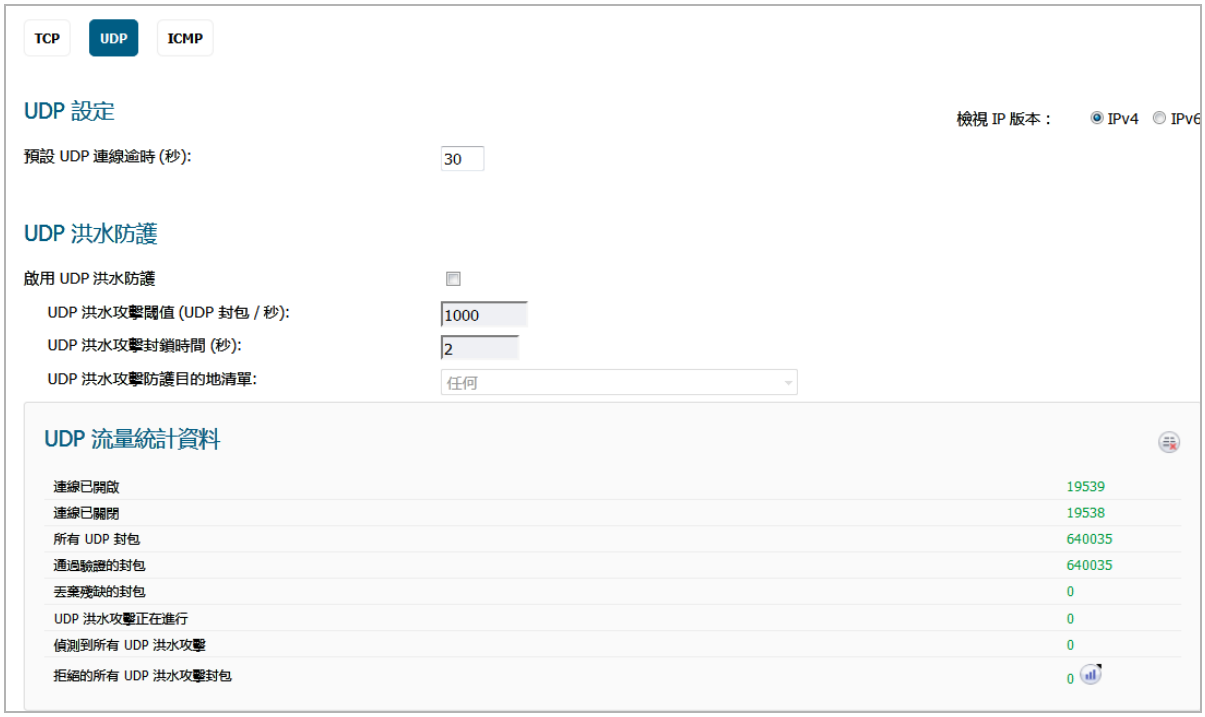
丟棄旗標無效的封包	當：
	• 接收了沒有位於連接快取的非 SYN 封包（已啟用 SYN 洪水防護）。
	• 建立工作階段期間，接收到其旗標為 SYN、RST+ACK 或 SYN+ACK 以外的封包（已啟用 SYN 洪水防護）。
	  • 如果封包已設定 FIN、URG 和 PSH 旗標，將記錄 TCP XMAS 掃描。
	  • 如果封包已設定 FIN 旗標，將記錄 TCP FIN 掃描。
	  • 如果封包未設定旗標，將記錄 TCP Null 掃描。
	• 使用除 SYN 旗標以外的旗標嘗試新 TCP 連線初始化。
	• 在已建立的 TCP 工作階段中收到帶有 SYN 旗標的封包。
	• 在已建立的 TCP 工作階段中收到無 ACK 旗標的封包。

丟棄序列無效的封包	當： • 接收到已建立的連接中的封包，其中，序號小於連接中最早未確認的序列。 • 接收到已建立的連接中的封包，其中，序號大於連接中最早未確認的序列 + 連接中最近公佈的視窗大小。
丟棄確認無效的封包	當丟棄確認無效的封包時。
非完整 WAN 的最大連接數/秒	當： • 接收到設定了 ACK 旗標但未設定 RST 和 SYN 旗標的封包，但 SYN Cookie 被確定為無效（已啟用 SYN 洪水防護）。 • 封包的 ACK 值（按照序號隨機偏移值調整）小於連接中最早確認的序號。 • 封包的 ACK 值（按照序號隨機偏移值調整）大於連接的下一個期望序號。

TCP 流量統計

此統計	將增加/顯示
非完整 WAN 的平均連接數/秒	每秒不完整 WAN 連接的平均數。
正在實施 SYN 洪水攻擊	當偵測到 SYN 洪水時。
正在實施 RST 洪水攻擊	當偵測到 RST 洪水時。
正在實施 FIN 洪水攻擊	當偵測到 FIN 洪水時。
TCP 洪水攻擊正在進行	當偵測到 TCP 洪水時。
偵測到的 SYN、RST、FIN 或 TCP 洪水總數	偵測到的洪水（SYN、RST、FIN 和 TCP）總數。
TCP 連線 SYN-Proxy 狀態(僅適用於 WAN)	僅限 WAN，是否啟用 TCP 連線 SYN-Proxy。
目前列入 SYN 黑名單的電腦	當裝置列於 SYN 黑名單時。
目前列入 RST 黑名單的電腦	當裝置列於 RST 黑名單時。
目前列入 FIN 黑名單的電腦	當裝置列於 FIN 黑名單時。
目前列入 TCP 黑名單的電腦	當裝置列於 TCP 黑名單時。
列入黑名單的 SYN 事件總數	當偵測到 SYN 黑名單事件時。
列入黑名單的 RST 事件總數	當偵測到 RST 黑名單事件時。
列入黑名單的 FIN 事件總數	當偵測到 FIN 黑名單事件時。
列入 TCP 黑名單的事件總數	當偵測到 TCP 黑名單事件時。
已拒絕的 SYN 黑名單封包總數	SYN 黑名單已拒絕的 SYN 封包總數。
已拒絕的 RST 黑名單封包總數	SYN 黑名單已拒絕的 RST 封包總數。
已拒絕的 FIN 黑名單封包總數	SYN 黑名單已拒絕的 FIN 封包總數。
已拒絕的 TCP 黑名單封包總數	SYN 黑名單已拒絕的 TCP 封包總數。
接收的 SYN Flood Cookie 無效	當 SNY Flood Cookie 無效時。
WAN DDOS 篩選狀態	DDOS 篩選是否啟用或停用。
WAN DDOS 篩選 - 拒絕的封包	當 WAN DDOS 篩選拒絕封包時。
WAN DDOS 篩選 - 洩露的封包	
WAN DDOS 篩選 - 允許清單計數	

UDP 檢視



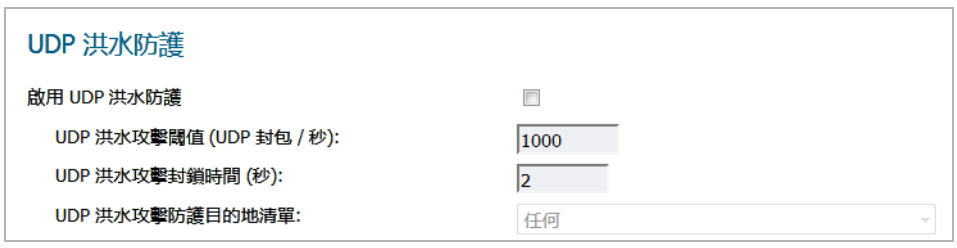
主題：

- UDP 設定
- UDP 洪水防護
- UDP 流量統計

UDP 設定

- **預設 UDP 連線逾時 (秒)** - 在 UDP 連接逾時前想要允許的閒置秒數。此值可被您為單獨規則設定的 UDP 連接逾時所替代。

UDP 洪水防護



UDP 洪水是一種拒絕服務 (DoS) 攻擊。透過向遠端主機上的隨機連接埠傳送大量 UDP 封包，可將其啟動。將透過處理攻擊封包消耗受到侵害的系統資源，最終導致系統無法被其他用戶端存取。

SonicWall UDP 洪水防護使用「監視和封鎖」方法防禦這些攻擊。裝置將監視 UDP 流量到指定的目的地。如果每秒的 UDP 封包速率超過了指定時間段內允許的閾值，裝置將丟棄後續的 UDP 封包以避免洪水攻擊。

將允許通過屬於 DNS 查詢或者回應或來自裝置設定的 DNS 伺服器的 UDP 封包，而不考慮 UDP 洪水防護的狀態。

以下設定可設定 UDP 洪水防護：

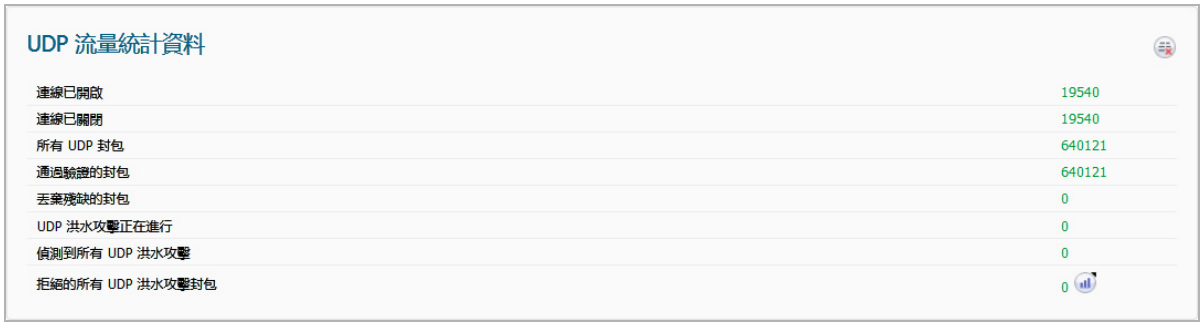
- **啟用 UDP 洪水防護** - 啟用 UDP 洪水防護。預設情況下未勾選此選項。

  附註：必須啟用**啟用 UDP 洪水防護**以啟用其他 **UDP 洪水防護**選項。

- **UDP 洪水攻擊閾值 (UDP 封包 / 秒)** - 允許傳送給觸發 UDP 洪水防護的主機、範圍或子網路的每秒的 UDP 封包最大數目。超出閾值將觸發 ICMP 洪水防護。最小值為 50，最大值為 1000000，預設值為 **1000**。
- **UDP 洪水攻擊封鎖時間 (秒)** - 裝置偵測到此時間段內 UDP 封包的速率超過攻擊閾值後，將啟用 UDP 洪水防護，並將開始丟棄後續的 UDP 封包。最小時長為 1 秒，最大時長為 120 秒，預設時間值為 **2** 秒。
- **UDP 洪水攻擊防護目的地清單** - 防護其免受 UDP 洪水攻擊的目的地位址物件或位址群組。預設值為任何。

  提示：選擇**任何**以將攻擊閾值套用至通過防火牆的 UDP 封包總和。

UDP 流量統計



UDP 流量統計表提供如 UDP 流量統計表格所示的統計。如需清除並重新啟動表中顯示的統計，按一下此表的**清除統計**圖示。

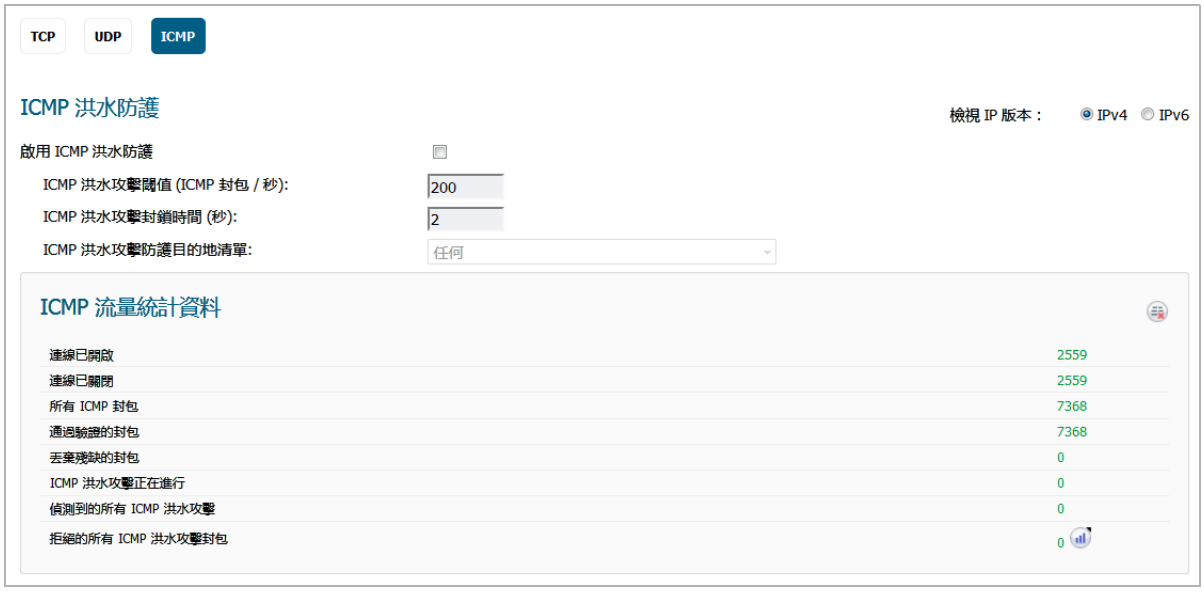
UDP 流量統計

此統計	將增加/顯示
連線已開啟	當連接打開時。
連線已關閉	當連接關閉時。
所有 UDP 封包	根據每個處理的 UDP 封包。
通過驗證的封包	UDP 封包通過總和檢查碼驗證（已啟用 UDP 總和檢查碼驗證）。
丟棄殘缺的封包	當： • UDP 總和檢查碼驗證失敗（已啟用 UDP 總和檢查碼驗證）。 • UDP 標頭長度計算為大於封包的資料長度。

UDP 流量統計

此統計	將增加/顯示
UDP 洪水攻擊正在進行	目前超過 UDP 洪水攻擊閾值的單獨轉送裝置的數量。
偵測到所有 UDP 洪水攻擊	某一類事件的總數，在這些事件中，轉送裝置已查過 UDP 洪水攻擊閾值。
拒絕的所有 UDP 洪水攻擊封包	由於 UDP 洪水攻擊偵測而丟棄的封包總數。 按一下**統計**圖示將顯示對話方塊顯示最近拒絕的封包： 

ICMP 檢視



主題：

- 檢視 IP 版本
- ICMP/ICMPv6 洪水防護

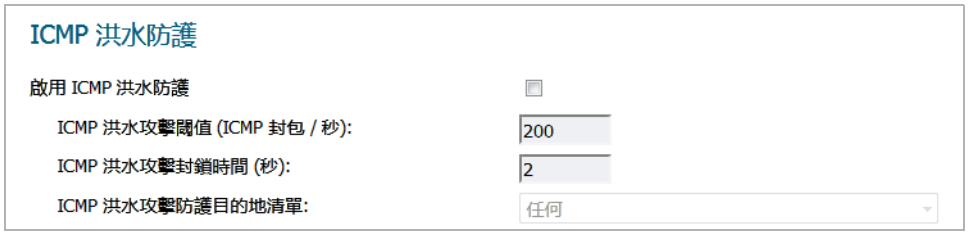
- ICMP/ICMPv6 流量統計

檢視 IP 版本

檢視 IP 版本選項按鈕用於指定 IP 版本：**IPv4** 或 **IPv6**。如果選擇：

- **IPv4**，標題和選項顯示 ICMP。
- **IPv6**，標題和選項顯示 ICMPv6。

ICMP/ICMPv6 洪水防護



ICMP 洪水防護同樣可用於 UDP 洪水防護，此外它還可監視 ICMP/ICMPv6 洪水攻擊。唯一的不同之處在於沒有允許繞過 ICMP 洪水防護的 DNS 查詢。

以下設定可設定 ICMP 洪水防護：

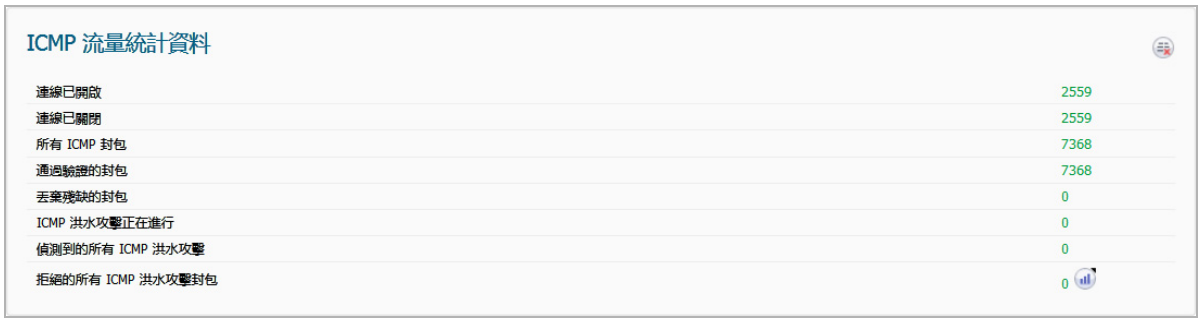
- **啟用 ICMP 洪水防護** - 啟用 ICMP 洪水防護。

  ⓘ **附註：**必須啟用**啟用 ICMP 洪水防護**以啟用其他 ICMP 洪水防護選項。

- **ICMP 洪水攻擊閾值 (ICMP 封包 / 秒)** - 允許傳送給主機、範圍或子網路的每秒的 ICMP 封包最大數目。超出此閾值將觸發 ICMP 洪水防護。最小次數為 10，最大次數為 100000，預設次數為 **200**。
- **ICMP 洪水攻擊封鎖時間 (秒)** - 裝置偵測到此時間段內 ICMP 封包的速率超過攻擊閾值後，將啟用 ICMP 洪水防護，並將開始丟棄後續的 ICMP 封包。最小時長為 1 秒，最大時長為 120 秒，預設時間值為 **2** 秒。
- **ICMP 洪水攻擊防護目的地清單** - 防護其免受 ICMP 洪水攻擊的目的地位址物件或位址群組。預設值為**任何**。

  ⓘ **提示：**選擇**任何**以將攻擊閾值套用至通過防火牆的 ICMP 封包總和。

ICMP/ICMPv6 流量統計



ICMP 流量統計表提供如 ICMP/ICMPv6 流量統計表格所示的統計。如需清除並重新啟動表中顯示的統計，按一下此表的**清除統計**圖示。

ICMP/ICMPv6 流量統計

此統計	將增加/顯示
連線已開啟	當連接打開時。
連線已關閉	當連接關閉時。
所有 UDP 封包	根據每個處理的 ICMP/ICMPv6 封包。
通過驗證的封包	ICMP/ICMPv6 封包通過總和檢查碼驗證（已啟用 ICMP/ICMPv6 總和檢查碼驗證）。
丟棄殘缺的封包	當： • ICMP/ICMPv6 總和檢查碼驗證失敗（已啟用 ICMP/ICMPv6 總和檢查碼驗證）。 • ICMP/ICMPv6 標頭長度計算為大於封包的資料長度。
ICMP/ICMPv6 洪水進行中	目前超過 ICMP/ICMPv6 洪水攻擊閾值的單獨轉送裝置的數量。
偵測到的所有 ICMP/ICMPv6 洪水	某一類事件的總數，在這些事件中，轉送裝置已查過 ICMP/ICMPv6 洪水攻擊閾值。
拒絕的所有 ICMP/ICMPv6 洪水封包	由於 ICMP/ICMPv6 洪水攻擊偵測而丟棄的封包總數。按一下**統計**圖示將顯示對話方塊顯示最近拒絕的封包： 

4

設定防火牆多點傳送設定

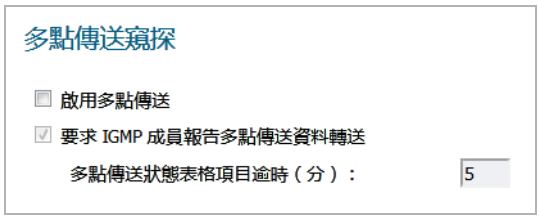
IP 多點傳送是將一個網際網路通訊協定 (IP) 封包同時傳送給多個主機的方法。多點傳送適用於快速增長的網際網路流量段 - 多媒體展示和視訊會議。例如，一個主機傳送音訊或視訊流，而有十個主機想要接收此類流。在多點傳送中，傳送主機傳送具有指定多點傳送位址的單個 IP 封包，10 個主機僅需要設定為監聽到達此位址的封包即可接收傳送。多點傳送是一點對多點的 IP 通信機制，在無連接模式中執行 - 主機透過「調諧」接收多點傳送傳送，此過程類似於調諧無線電。

安全設定 | 防火牆設定 > 多點傳送頁面用於管理防火牆上的多點傳送流量。

主題：

- 多點傳送窺探
- 多點傳送原則
- IGMP 狀態表
- 啟用 LAN 專用介面上的多點傳送
- 透過 VPN 啟用多點傳送

多點傳送窺探



本節提供多點傳送窺探的設定任務。

- **啟用多點傳送** - 勾選此核取方塊即可支援多點傳送流量。此核取方塊在預設情況下停用。
- **要求 IGMP 成員報告多點傳送資料轉送** - 選擇此核取方塊，透過調節要僅轉送到介面（介面使用 IGMP 加入到多點傳送群組位址）的多點傳送資料來改善效能。此核取方塊預設情況下呈啟用狀態。
- **多點傳送狀態表格項目逾時（分）** - 此欄位的預設值為 **5**。此欄位的值範圍為 5 到 60（分鐘）。在以下條件下可更新計時器預設值 5
  - 您懷疑成員查詢或報告在網路中已遺失。
  - 您想要減少網路上的 IGMP 流量，目前有較大數量的多點傳送群組或用戶端。在此條件中，您無需有路由器到路由器的流量。
  - 您想要同步與 IGMP 路由器的計時。

多點傳送原則

本節提供多點傳送原則的設定任務。

- **啟用全部多點傳送位址接收** - 預設情況下不啟用此選項按鈕。選擇此選項按鈕可接收所有（D 類）多點傳送位址。

  附註：接收所有多點傳送位址可能導致您的網路效能降低。

- **啟用以下多點傳送位址接收** - 預設情況下啟用此選項按鈕。在下拉功能表中，選擇**建立新的多點傳送物件**或**建立新的多點傳送群組**。

  附註：只能選擇與多點傳送區域相關聯的位址物件和群組。只能將 `224.0.0.1` 到 `239.255.255.255` 的位址繫結到多點傳送區域。

  附註：您總共至多可指定 200 個多點傳送位址。

建立多點傳送位址物件：

1 在**多點傳送窺探**下，選擇**啟用多點傳送**。

2 在**啟用以下多點傳送位址接收**下拉功能表的**多點傳送原則**下，選擇**建立新的多點傳送位址物件**。此時會顯示**新增位址物件**對話方塊。

3 在**名稱**欄位設定位址物件的名稱。

4 從**區域指派**下拉功能表，選擇**多點傳送**。

5 從**類型**下拉功能表，選擇**主機**、**範圍**、**網路**、**MAC** 或 **FQDN**。

6 取決於您選擇的類型，對話方塊的選項有所不同。如果選擇：

- **主機**或**網路**，將顯示 **IP 位址**欄位。輸入主機或網路的 IP 位址。IP 位址必須在多點傳送範圍：224.0.0.0 到 239.255.255.255。
- **網路**，將顯示**網路遮罩**欄位。輸入網路的網路遮罩。
- **範圍**，將顯示**起始 IP 位址**和**終止 IP 位址**欄位。輸入位址範圍的起始和終止 IP 位址。IP 位址必須在多點傳送範圍：224.0.0.1 到 239.255.255.255。

7 按一下**確定**。

IGMP 狀態表

本節介紹了 **IGMP 狀態表**中的欄位。

- **多點傳送群組位址** - 提供介面所加入的多點傳送群組位址。
- **介面/VPN 通道** - 提供 VPN 原則的介面（例如 **LAN**）。
- **IGMP 版本** - 提供 IGMP 版本（例如 **V2** 或 **V3**）。
- **剩餘時間**
- **排清** - 提供圖示，排清指定項目。
- **排清**和**排清全部** 按鈕 - 要快速排清指定項目，可勾選項目左邊的核取方塊並按一下**排清**。按一下**排清全部**可快速排清所有項目。

啟用 LAN 專用介面上的多點傳送

啟用防護牆的 LAN 專用介面上的多點傳送支援的步驟如下：

1 移至**安全設定 | 防火牆設定 > 多點傳送**頁面。

2 在**多點傳送窺探**下，選擇**啟用多點傳送**。

3 在**多點傳送原則**下，選擇**啟用全部多點傳送位址接收**。

4 按一下**接受**。

5 移至**網路 > 介面**頁面。

6 按一下想要設定的 LAN 介面的**設定**按鈕。將顯示**編輯介面**對話方塊。

7 按一下**進階**。

8 選擇**啟用多點傳送支援**。

9 按一下**確定**。

若要對透過 VPN 通道的位址物件啟用多點傳送支援，請執行以下操作：

1 移至**安全設定 | 防火牆設定 > 多點傳送**頁面。

2 在**多點傳送窺探**下，選擇**啟用多點傳送**。

3 在**多點傳送原則**下，選擇**啟用以下多點傳送位址接收**。

4 從下拉功能表中，選擇**建立新的多點傳送位址物件**。 此時會顯示**新增位址物件**對話方塊。

5 在**名稱**欄位，輸入多點傳送位址物件的名稱。

6 從**區域指派**下拉功能表，選擇一個區域：**DMZ**、 **LAN**、**多點傳送**、**SSLVPN**、**VPN**、**WAN** 或 **WLAN**。

7 當您從**類型**下拉功能表中選擇一個類型後，其他選項將根據選擇而改變。如果選擇：

- **主機**，請在 **IP 位址**欄位中輸入 **IP 位址**。
- 如果選擇**範圍**，請在起始 IP 位址和結束 IP 位址中分別輸入**起始**和**結束 IP 位址**。
- **網路**，在**網路遮罩**欄位輸入網路 IP 位址，在**網路遮罩/首碼長度**欄位輸入網路遮罩或首碼長度。
- **MAC**，在 **MAC 位址**欄位輸入 MAC 位址，並選擇**多重主目錄主機**核取方塊（預設情況下勾選此核取方塊）。
- **FQDN**，在 **FQDN 主機名稱**欄位輸入 FQDN 主機名稱。

8 按一下**確定**。

9 移至 **VPN > 設定**頁面。

10 在 **VPN 原則**表，按一下想要設定的群組 VPN 原則的**設定**圖示。隨即顯示 **VPN 原則**對話方塊。

11 按一下**進階**。

12 在**進階設定**部分，選擇**啟用多點傳送**。

13 按一下**確定**。

透過 VPN 啟用多點傳送

若要透過 VPN 啟用跨 WAN 的多點傳送，請執行以下操作：

1 全域啟用多點傳送：

a 導覽至**安全設定 | 防火牆設定 > 多點傳送**頁面。

b 勾選**啟用多點傳送**核取方塊。

c 按一下**接受**按鈕。

d 對於參與的所有安全裝置上的每個介面，重複步驟 a 至步驟 c。

2 啟用每個單獨介面上的多點傳送支援，以參與多點傳送網路。

a 導覽至**系統安裝 | 網路 > 介面**頁面。

b 按一下參與介面的**編輯**圖示。將顯示**編輯介面**對話方塊。

c 按一下**進階**。

d 選擇**啟用多點傳送支援**核取方塊。

e 按一下**確定**。

f 對於參與的所有裝置上的每個參與介面，重複步驟 a 至步驟 e。

3 啟用安全裝置之間 VPN 原則的多點傳送。

a 導覽至**連線 | VPN > 基本設定**頁面。

b 按一下包含多點傳送的原則的**編輯**圖示。隨即顯示 **VPN 原則**對話方塊。

c 按一下**進階**。

附註：IGMP 流量的預設 WLAN 多點傳送存取規則已設定為「拒絕」。如果所有參與的裝置在其 WLAN 區域中有多點傳送用戶端，則需要對這些裝置變更為「允許」才能啟用多點傳送。

d 在**進階設定**部分，選擇**啟用多點傳送**。

e 按一下**確定**。

4 檢查站台之間的通道是否已啟用。

5 啟動多點傳送伺服器應用程式和用戶端應用程式。由於多點傳送資料是從多點傳送伺服器傳送到多點傳送群組（224.0.0.0 到 239.255.255.255），防火牆將查詢此群組的 IGMP 狀態表，以確定此資料的傳送位置。同樣，如果裝置接收了 VPN 區域的資料，裝置將查詢其 IGMP 狀態表以確定應在何處傳送資料。

IGMP 狀態表（更新時）應提供相關資訊，以指示 X3 介面上存在多點傳送用戶端，且跨 224.15.16.17 群組的整個 vpnMcastServer 通道。

附註：透過選擇**啟用全部多點傳送位址接收**，您可以在檢視 **IGMP 狀態表**時檢視您所期望看到的內容之外的項目。這些是由您主機上可能執行的其他多點傳送應用程式所產生的。

5

管理服務品質

服務品質 (QoS) 是指旨在提供可預測的網路行為和效能的各種方法。此預測性排序對於指定類型的應用程式而言非常重要，例如 IP 語音 (VoIP)、多媒體內容，或業務關鍵型應用程式，例如訂單處理或信用卡處理。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。

主題：

- 分類
- 標記
- 調節
- 802.1p 和 DSCP QoS
- 頻寬管理
- 術語

分類

分類是必要的第一步驟，只有透過此步驟才能識別管理需求流量。SonicOS 使用存取規則作為介面對流量進行分類。透過使用位址物件、服務物件和排程物件元素組合，此功能提供了微調控制，使分類條件和**所有 HTTP 流量**一樣通用，且和**星期二上午 2:12 從 hostA 到 serverB 的 SSH 流量**一樣具體。

SonicWall 網路安全裝置可識別、對應、修改和產生行業標準的外部 CoS 指示符、DSCP 和 802.1p（請參閱 802.1p 和 DSCP QoS 一節）。

識別或分類之後，可對其進行管理。可由 SonicOS 頻寬管理 (BWM) 在內部執行管理，只要網路完全包含自發系統，SonicWall 頻寬管理將一直起效。引入外部或中間元素（例如具有未知設定的外部網路基礎設施，或競爭網際網路等頻寬的其他主機）後，提供保證和預測性的功能將降低。換言之，只要網路的終端和終端之間的任何元件都在您的管理範圍之內，BWM 將嚴格按照設定工作。引入外部實體後，BWM 設定的精確度和功效可能會下降。

但是並不是失去全部功能。SonicOS 對流量分類後，可對其進行**標籤**，以使此類別的流量與 CoS 標籤所容納的指定外部系統進行通信，因此它們可以參與提供 QoS。

附註：很多服務供應商不支援 CoS 標籤，例如 802.1p 或 DSCP。同時，具有標準設定的大多數網路裝置無法識別 802.1p 標籤，可能會丟棄已標籤的流量。

儘管 DSCP 不會導致相容性問題，但很多服務供應商僅需清除或忽略 DSCP 標誌，而不考慮編碼點。

如果想要在您的網路或服務供應商的網路上使用 802.1p 或 DSCP 標記，必須先確保支援這些方法。檢查您的內部網路裝置是否支援 CoS 優先順序標記，且是否經過正確的設定。檢查您的服務供應商 - 一些服務供應商使用這些 CoS 方法提供收費的 QoS 支援。

標記

對流量進行分類後，如果此流量由支援 QoS 的外部系統處理（例如 CoS 感知交換器或路由器可能在進階服務提供程式的基礎結構中或在私人 WAN 中可用），則必須對其進行標記，外部系統才能使用分類，並提供正確的處理和每跳轉送行為。

最初，這是在擁有 RFC791 的三個優先位元和 RFC1394 ToS（服務類型）欄位的 IP 層嘗試，但這由總數為 17 人的傳送量歷史記錄所使用。其繼任者 RFC2474 引入了更實用和更廣泛使用的 DSCP（區分服務代碼點），可提供多達 64 個分類以及使用者自訂的類。透過 RFC2598（加急轉送，旨在提供租用線路行為）和 RFC2697（保證類中的轉送層級，又稱金牌服務、銀牌服務、銅牌服務），DSCP 進一步得到增強。

DSCP 是一種流量安全標記方法，其針對的流量主要是由於沒有不相容的風險而遍歷公用網路的流量。最壞的情況是，沿路徑的躍點可能會丟棄或刪除 DSCP 標籤，但很少濫用或丟棄封包。

CoS 標記的其他常用方法是 IEEE802.1p。802.1p 發生在 MAC 層（第 2 層），與 IEEE 802.1Q VLAN 標記密切相關，且共用相同的 16 位元欄位，但它實際上是以 IEEE802.1D 標準定義的。和 DSCP 不同，802.1p 只能與支援 802.1p 的裝置配合使用，通常不擁有互操作性。此外，由於 802.1p 具有不同的封包結構，幾乎無法遍歷廣域網，甚至是私人 WAN。儘管如此，802.1p 一直在獲取 IP 供應商對語音和視訊的廣泛支援，因此引入了透過網路邊界（即廣域網連結）支援 802.1p 的解決方案，其形式為 **802.1p 到 DSCP 的對應**。

802.1p 到 DSCP 的對應允許透過 SonicOS 將 802.1p 標籤從一個 LAN 對應到 DSCP 值，使封包能夠安全地遍歷 WAN 連結。當封包到達 WAN 或 VPN 的另一端時，接收 SonicOS 裝置可將 DSCP 標籤重新對應到 802.1p 標籤，以便在此 LAN 中使用。如需更多資訊，請參閱 802.1p 和 DSCP QoS。

調節

可使用多種原則、佇列和調整方法中的任意一種調節（或管理）流量。SonicOS 透過其輸入和輸出頻寬管理 (BWM) 提供了內部調節功能，這在頻寬管理中有詳細說明。SonicOS 的 BWM 對於擁有足夠頻寬的完全自發的私人網路是非常有效的解決方案，但對於引入很多未知外部網路元素和頻寬內容的情況而言，效率會降低。如需爭用問題的說明，請參閱 DSCP 標記：範例情節。

主題：

- 透過支援 QoS 的網路的站台到站台 VPN
- 透過公用網路的站台到站台 VPN

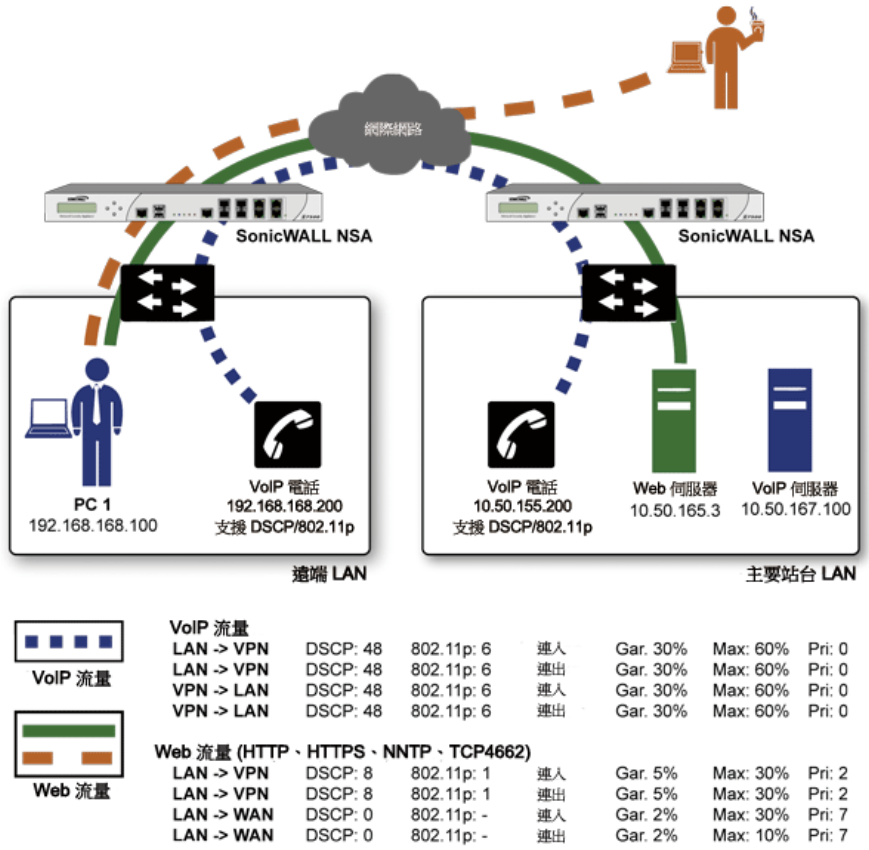
透過支援 QoS 的網路的站台到站台 VPN

如果兩個終端之間的網路路徑能夠感知 QoS，則 SonicOS 可對內部封裝封包進行 DSCP 標籤，以使其能夠在通道的另一端進行正確解釋，還可對外部 ESP 封裝封包進行 DSCP 標籤，以使傳送網路上的每個躍點都能夠得到解釋和使用。SonicOS 可將在內部網路上建立的 802.1p 標籤對應到 DSCP 標籤，以使其可以安全地遍歷傳送網路。如果在另一端接收到封包，則接收的 SonicWall 裝置會將 DSCP 標籤轉譯為 802.1p 標籤，以使內部網路可以正確解釋和使用。

透過公用網路的站台到站台 VPN

SonicOS 整合的 BWM 可非常有效地管理 VPN 連接的網路之間的流量，因為可在兩個端點對輸入和輸出流量進行分類和控制。如果端點之間的網路無法感知 QoS，則同樣會丟棄並處理 VPN ESP。由於通常不會控制這些中間網路或其路徑，因此很難充分保證 QoS，但 BWM 仍能夠協助您提供更多可預測的行為。

透過公用網路的站台到站台 VPN



為提供端到端 QoS，業務類別的服務供應商在不斷地對其 IP 網路提供流量調節服務。這些服務通常取決於要分類和標籤流量的客戶本機裝置，通常使用標準標記方法，例如 DSCP。SonicOS 能夠在流量分類之後對其進行 DSCP 標記，還可將 802.1p 標籤對應到 DSCP 標籤，以便穿越外部網路並保留 CoS。對於 VPN 流量，SonicOS 不僅能夠對內部（承載）封包進行 DSCP 標記，也可對外部（封裝）封包進行 DSCP 標記，因此支援 QoS 的服務提供程式甚至可對加密的 VPN 流量提供 QoS。

服務提供程式使用的實際的調節方法各不相同，但通常都包含了基於類別的佇列方法，例如用於對流量排定優先順序的加權公平佇列，以及避免壅塞的方法，例如尾部丟棄或隨機早期偵測。

802.1p 和 DSCP QoS

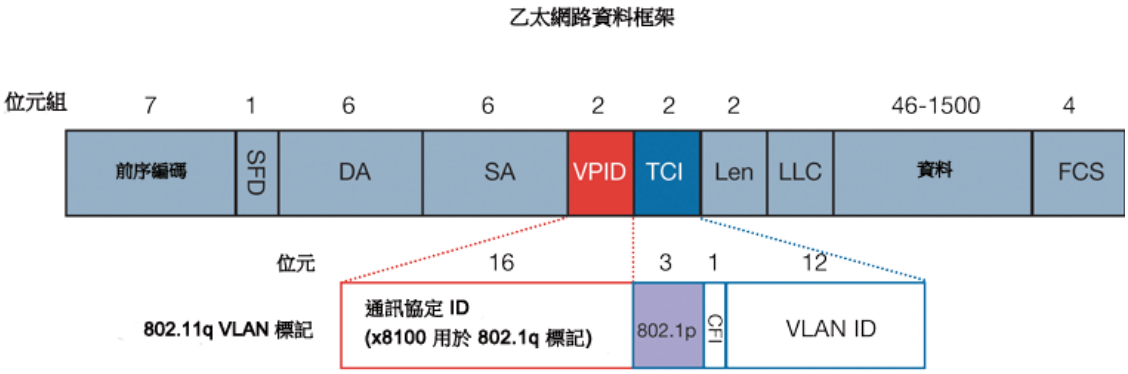
主題：

- 啟用 802.1p
- DSCP 標記

啟用 802.1p

SonicOS 支援第 2 層和第 3 層 CoS 方法，可與啟用了 QoS 的環境中外部系統進行廣泛的互操作。第 2 層方法是 IEEE 802.1p 標準，其中，插入到乙太網路框架標頭中的附加 16 位元中的 3 位元可用於指定框架的優先順序，如下圖所示：

乙太網路資料框架



- **TPID**：標籤通訊協定識別項從第 12 個位元組開始（6 個位元組的目的地欄位和 6 個位元組的來源欄位之後），長度為 2 個位元組，標籤的流量的乙太網路類型為 0x8100。
- **802.1p**：TCI（標籤控制資訊 - 從第 14 個位元組開始，長度為兩個位元組）的前三位元定義了使用者優先順序，總共為八個 (2^3) 優先順序層級。IEEE 802.1p 定義了這三個使用者優先順序位元的操作。
- **CFI**：規範格式指示器是只有一位元的旗標，對於乙太網路交換器，它始終設定為零。CFI 用於乙太網路網路和令牌環網之間的相容性原因。如果在乙太網路連接埠接收的框架其 CFI 設定為 1，則不應將此框架轉送到無標籤的連接埠。
- **VLAN ID**：VLAN ID（在 14 個位元組中從第 5 個位元組開始）是 VLAN 的識別。它擁有 12 位元，且允許 4,096 (2^12) 個唯一的 VLAN ID 識別。對於 4,096 個可用的 ID，ID 0 用於識別框架優先順序，ID 4,095 (FFF) 已保留，因此可用的最大 VLAN 設定為 4,094。

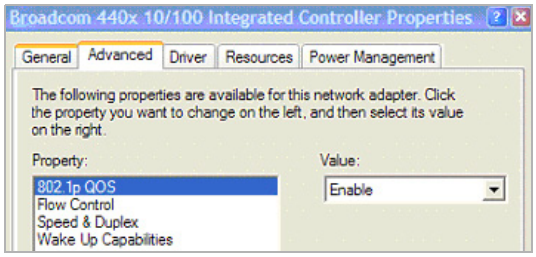
透過啟用想要處理 802.1p 標記的介面上的 802.1p 標籤即可啟動 802.1p 支援。可在任何 SonicWall 裝置上的任何乙太網路連接埠上啟用 802.1p。

帶有這些標記的 802.1p 欄位的行為由存取規則控制。預設 802.1p 存取規則操作**無**會將現有 802.1p 標籤重設為 0，除非使用了其他設定（如需詳細資料，請參見管理 QoS 標記）。

啟用 802.1p 標記將允許目的地介面識別由支援 802.1p 的網路裝置所產生的傳入 802.1p 標記，這可透過存取規則控制。SonicOS 插入的擁有 802.1p 標籤的框架其 VLAN ID 為 0。

802.1p 標籤只能根據存取規則插入，因此在使用了預設值的介面上啟用 802.1p 標記不會中斷與不支援 802.1p 的裝置的通信。

802.1p 需要您想要對其使用優先順序方法的網路裝置的指定支援。透過 IP 的很多語音和視訊裝置都提供了對 802.1p 的支援，但必須將此功能啟用。如果對此功能不確定，請檢查您的裝置文件，查看相關的 802.1p 支援資訊。很多伺服器和主機網路卡 (NIC) 同樣也提供了對 802.1p 的支援，但預設情況下此功能通常處於停用狀態。在 Win32 作業系統中，您可以在網路卡的屬性頁面上的**進階**檢視，檢查和設定 802.1p 設定。如果您的網路卡支援 802.1p，將會列出 **802.1p QoS**、**802.1p 支援**、**QoS 封包標籤**或一些類似選項：



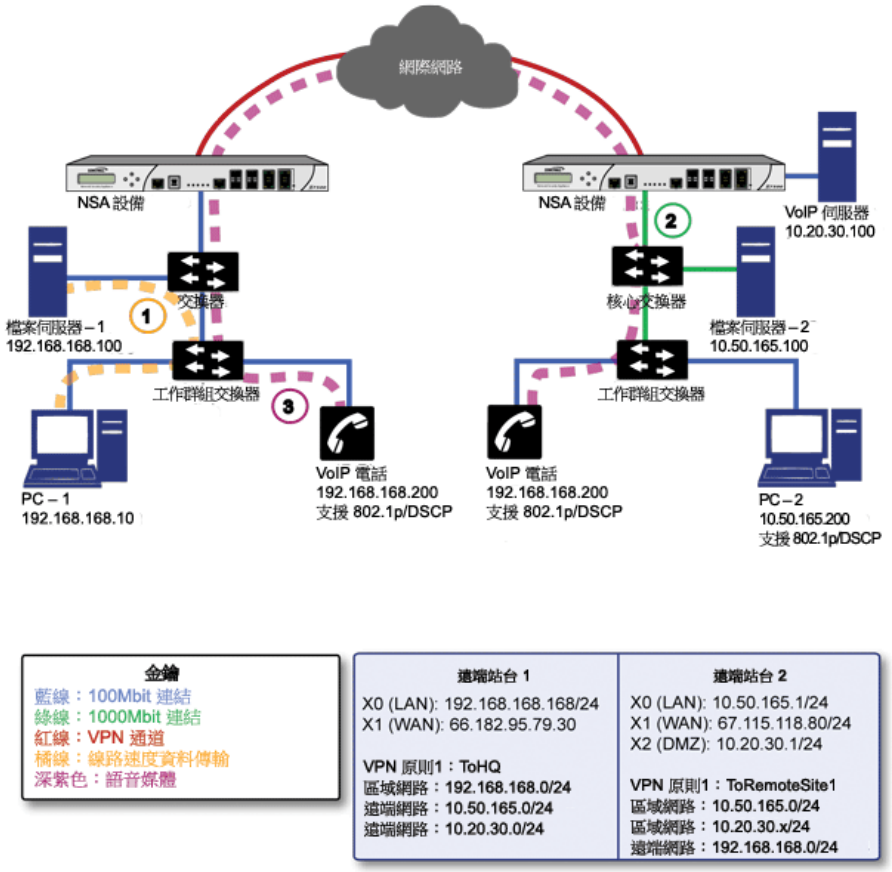
若要處理 802.1p 標記，網路介面上必須具有此功能，並將此功能啟用。網路介面將能夠產生帶有 802.1p 標記的封包，這由支援 QoS 的應用程式管理。預設情況下，為了維護與不支援 802.1p 的裝置的通信，一般的網路通信不會插入標記。

附註：如果您的網路介面不支援 802.1p，將無法處理 802.1p 標記的流量，會將其忽略。定義存取規則時，請務必啟用支援 802.1p 的目的地裝置上的 802.1p 標記。

還應注意，在支援 802.1p 的裝置上執行封包擷取（例如，使用診斷工具 Ethereal）時，一些裝置將不顯示擷取封包的 802.1q 標頭。相反，如果在不支援 802.1p 的裝置上執行封包擷取時，幾乎總是會顯示標頭，但主機無法處理封包。

在繼續管理 QoS 標記之前，先介紹「DSCP 標記」很重要，因為兩種標記方法之間存在潛在的相關性，也需要解釋一下為何存在相關性。

DSCP 標記：範例情節



在以上的情形中，我們透過 IPsec VPN 將**遠端站台 1** 連接到「主站台」。公司使用支援內部 802.1p/DSCP 的 VoIP 電話系統，並在主站台上託管了一個私人 VoIP 信號伺服器。主站台使用千兆位元和快速乙太網路混合型基礎結構，遠端站台 1 均為快速乙太網路。兩個站台均使用支援 802.1p 的交換器進行內部流量的優先順序排列。

1 遠端站台 1 的 PC-1 將 23 TB 的 PowerPoint™ 簡報傳送至檔案伺服器 1，工作組交換器和上游交換器之間的 100 mbit 連結已完全飽和。

2 在主站台，位於支援 802.1p/DSCP 的 VoIP 電話 10.50.165.200 處的呼叫者開始對 VoIP 電話 192.168.168.200 處的人員進行呼叫。呼叫 VoIP 電話 802.1p 使用優先順序 6（語音）標籤流量，DSCP 使用 48 標籤流量。

a 如果核心交換器和防火牆之間的連結為 VLAN，部分交換器會將接收到的 802.1p 優先順序標籤（除 DSCP 標籤外）包含到發動給防火牆的封包中，此行為對於各種交換器而言各不相同，但通常可設定。

b 如果核心交換器和防火牆之間的連結不是 VLAN，則防火牆將無法包含 802.1p 優先順序標籤。將移除 802.1p 優先順序，並將封包（僅包含 DSCP）轉送給防火牆。

如果防火牆透過 VPN/WAN 連結傳送封包，則可將 DSCP 標籤包含到封包中，但無法包含 802.1p 標籤。這可能會遺失 VoIP 流量的所有優先順序資訊，因為當封包到達遠端站台時，交換器將不能使用 802.1p MAC 層資訊對流量進行優先順序排序。由於連結飽和，遠端站台交換器處理 VoIP 流量的方式與優先順序較低的檔案傳送的處理方式相同，到達 VoIP 流產生的延遲（甚至可能是丟棄封包）使呼叫品質下降。

因此關鍵的 802.1p 優先順序資訊將如何透過 VPN/WAN 連結從主站台 LAN 傳送到遠端站台 LAN？透過使用 QoS 對應。

QoS 對應是將第 2 層 802.1p 標籤轉換為第 3 層 DSCP 標籤的一種功能，以便它們可以安全地遍歷（以對應的形式）不支援 802.1p 的連結；當封包到達下一個支援 802.1p 的分段時，QoS 對應會將 DSCP 轉換為 802.1p 標籤，以便可以使用 2 層 QoS。

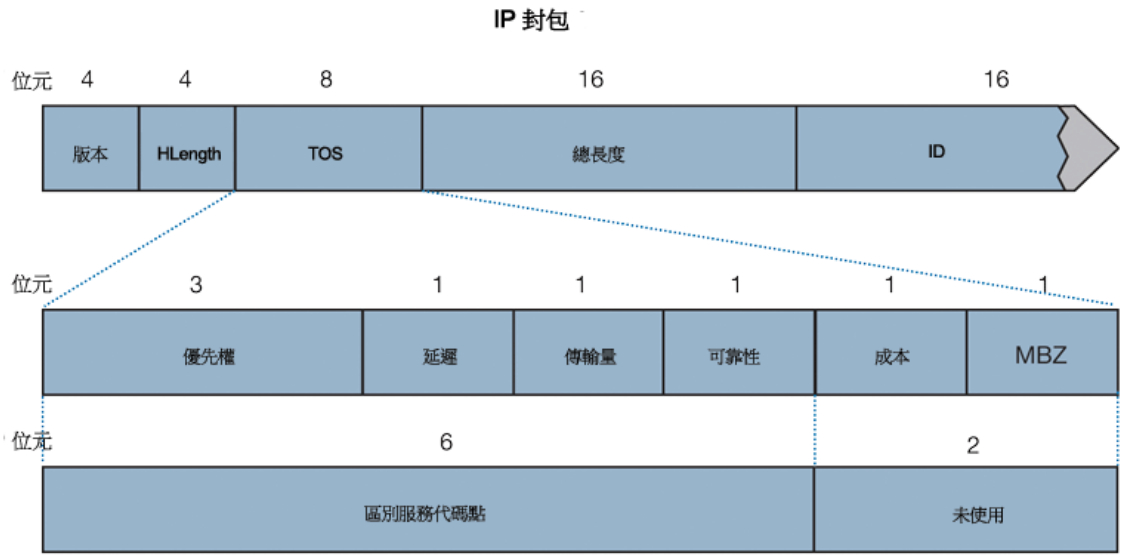
在以上的情形中，主站台的防火牆為 VoIP 封包以及封裝 ESP 封包指派 DSCP 標籤（例如值 **48**），以便能夠在 WAN 套用第 3 層 QoS。透過保留現有 DSCP 標籤或從 802.1p 標籤（如果存在）對應值可完成指派。如果 VoIP 封包到達連結的另一端，接收封包的 SonicWall 將遍歷對應過程，同時會將 DSCP 標籤對應到 802.1p 標籤。

3 遠端站台的接收 SonicWall 已設定為將 DSCP 標籤範圍 48-55 對應到 802.1p 標籤 6。封包結束防火牆後，將使用 802.1p 標籤 6。交換器會將其識別為語音流量，並透過檔案傳送排定優先順序，甚至能夠在連結飽和的情況下保證 QoS。

DSCP 標記

DSCP（差分服務代碼點）標記使用 IP 標頭中 8 位元 ToS 欄位中的 6 位元提供 64 類（或代碼點）流量。由於 DSCP 是第 3 層標記方法，且存在 802.1p 標記，因此無需考慮相容性問題。不支援 DSCP 的裝置將忽略標籤，在最差的情況下會將標籤值重設為 0。

DSCP 標記：IP 封包



上圖說明 IP 封包，在標頭的 ToS 部分擁有結束標記。ToS 位元最初用於優先順序和 ToS（延遲、傳送量、可靠性和成本）設定，但之後 RFC2474 又將其用於用途更廣的 DSCP 設定。

下表顯示了常用的代碼點，以及它們向舊優先順序和 ToS 設定的對應。

DSCP 標記：常用代碼點

DSCP	DSCP 說明	舊 IP 優先順序	舊 IP ToS (D, T, R)
0	最大努力型	0（例程 - 000）	-
8	1 級	1（優先順序 - 001）	-
10	1 級，黃金級 (AF11)	1（優先順序 - 001）	T
12	1 級，白銀級 (AF12)	1（優先順序 - 001）	D
14	1 級，青銅級 (AF13)	1（優先順序 - 001）	D、T
16	2 級	2（中間級 - 010）	-
18	2 級，黃金級 (AF21)	2（中間級 - 010）	T
20	2 級，白銀級 (AF22)	2（中間級 - 010）	D
22	2 級，青銅級 (AF23)	2（中間級 - 010）	D、T
24	3 級	3（Flash - 011）	-
26	3 級，黃金級 (AF31)	3（Flash - 011）	T
27	3 級，白銀級 (AF32)	3（Flash - 011）	D
30	3 級，青銅級 (AF33)	3（Flash - 011）	D、T
32	4 級	4（Flash 覆寫 - 100）	-
34	4 級，黃金級 (AF41)	4（Flash 覆寫 - 100）	T
36	4 級，白銀級 (AF42)	4（Flash 覆寫 - 100）	D
38	4 級，青銅級 (AF43)	4（Flash 覆寫 - 100）	D、T
40	快速轉送	5 (CRITIC/ECP[1] - 101)	-
46	加速轉送 (EF)	5 (CRITIC/ECP - 101)	D、T
48	控制	6（互連網控制 - 110）	-
56	控制	7（網路控制 - 111）	-

1. ECP：橢圓曲線群組

可對在任何介面和任何區域類型之間傳送的流量執行 DSCP 標記（無例外）。DSCP 標記由存取規則透過 **QoS** 檢視控制，可與 802.1p 標記配合使用，也可與 SonicOS 的內部頻寬管理配合使用。

主題：

- DSCP 標記和混合 VPN 流量
- 設定 802.1p CoS 4 控制的負載
- QoS 對應
- 管理 QoS 標記

DSCP 標記和混合 VPN 流量

在諸多的安全措施和特性中，IPsec VPN 使用防止重放機制，其基礎在於新增到 ESP 標頭中的單調遞增的序號。將丟棄具有重複序號的封包，因為此類封包不符合順序標準。此類標準可管理故障封包的處理。SonicOS 提供了 64 個封包的重放視窗，即，如果 64 個以上的封包延遲用於安全關聯 (SA) 的 ESP 封包，將丟棄此封包。

使用 DSCP 標記對遍歷 VPN 的流量提供第 3 層 QoS 時應考慮此項。如果您的 VPN 通道傳送各種流量，一部分標記了 DSCP 高優先順序（例如 VoIP），一部分標記了 DSCP 低優先順序，或未標記/最大努力型（例如 FTP），則您的服務提供程式將優先處理高優先順序 ESP 封包的傳送，然後再處理最大努力型 ESP 封包。在指定流量條件下，這可能會導致將最大努力型封包延遲 64 個封包以上，從而導致接收的 SonicWall 的防止重放防禦機制丟棄。

如果出現此類現象（例如低優先順序流量過分重傳），建議您為高優先順序和低優先順序流量類建立單獨的 VPN 原則。透過將高優先順序主機（例如 VoIP 網路）置於各自的子網路中可輕鬆完成。

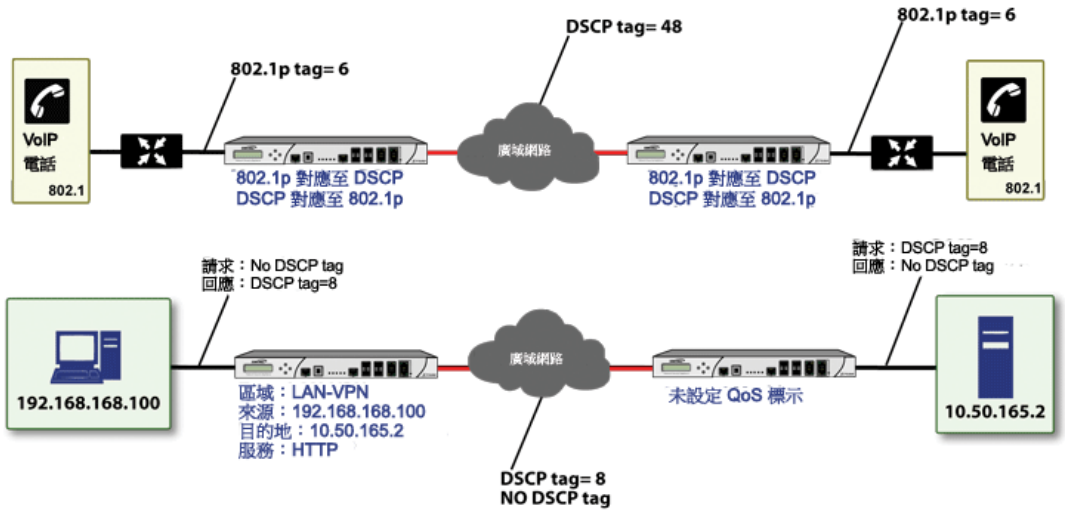
設定 802.1p CoS 4 控制的負載

如果想要將 DSCP 標籤 15 的傳入對應從預設 802.1p 對應 1 變更為 802.1p 對應 2，則由於對應範圍不能重疊，需要兩個步驟才能完成。嘗試指派重疊的對應會產生錯誤 DSCP 範圍已存在或與另一範圍重疊。首先，需要從對應到 802.1p CoS1 的目前終止範圍中移除 15（將終止對應範圍變更為從 802.1p CoS 1 到 DSCP 14），然後可將 DSCP 15 指派給 802.1p CoS 2 的起始對應範圍。

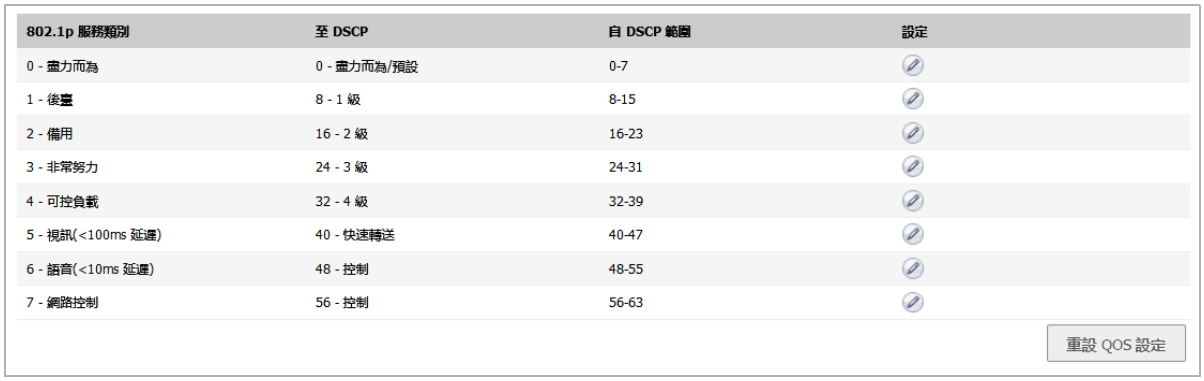
QoS 對應

QoS 對應的主要目的是允許 802.1p 標記總是能夠透過不支援 802.1p 的連結（例如 WAN 連結），方法為透過 WAN 連結傳送之前將它們對應到對應的 DSCP 標籤，然後在到達另一端時再從 DSCP 重新對應到 802.1p：

QoS 對應



附註：只有將**對應**作為存取規則的 QoS 檢視操作，才能進行對應。對應表僅定義存取規則的對應操作將要使用的通信。



例如，根據預設表，值為 **2** 的 802.1p 標籤將傳出對應到值為 **16** 的 DSCP，DSCP 標籤 **43** 將傳入對應到 802.1 值 **5**。

這些對應中的每一個都可以重新設定。如果想要將傳出對應 802.1p 標籤 **4** 從 DSCP 預設值 **32** 變更為 DSCP 值 **43**，則可以按一下 **4 - 可控負載**的**設定**圖示，然後從下拉框中選擇新**至 DSCP** 值：

802.1p CoS 1 重新對應終止範圍

802.1p CoS 2 重新對應起始範圍

您可以按一下**重設 QoS 設定**按鈕，以還原預設對應。

管理 QoS 標記

從**原則 | 規則 > 存取規則**頁面的**新增/編輯規則**對話方塊的 **QoS** 檢視設定 QoS 標記：

SonicOS 存取規則管理的 802.1p 和 DSCP 標記提供了 4 種操作：**無**、**保留**、**顯見**和**對應**。預設 DSCP 操作為**保留**，預設 802.1p 操作為**無**。

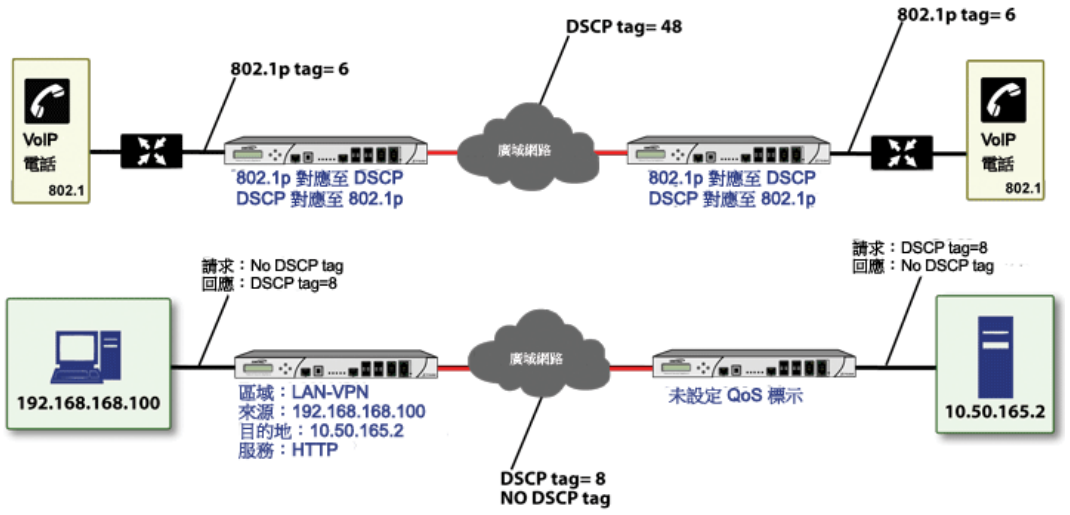
QoS 標記：行為表格說明了標記的兩種方法中每個操作的行為：

QoS 標記：行為

操作	802.1p（第 2 層 CoS）	DSCP（第 3 層）	備註
無	與此類流量相符合的封包（按照存取規則定義）傳送出輸出介面時，將不新增任何 802.1p 標記。	DSCP 標籤已顯見設定（或重設）為零。	如果此類流量的目的地介面是 VLAN 子介面，802.1q 標籤的 802.1p 部分將顯見設定為 0。如果此類流量指定用於 VLAN 且使用 802.1p 進行優先順序排序，則應使用**保留**、**顯見**或**對應**對此類流量定義指定的存取規則。
保留	將保留現有 802.1p 標記。	將保留現有 DSCP 標籤值。	
顯見	可從將要顯示的下拉功能表中指派顯見 802.1p 標記值 (0-7)。	可從將要顯示的下拉功能表中指派顯見 DSCP 標籤值 (0-63)。	如果 802.1p 或 DSCP 操作設定為**顯見**，而另一個設定為**對應**，將先進行顯見指派，然後根據此指派對應另一個。
對應	在**防火牆 > QoS 對應**頁面定義的對應設定將用於從 DSCP 標籤對應到 802.1p 標籤	在**防火牆 > QoS 對應**頁面定義的對應設定將用於從 802.1p 標籤對應到 DSCP 標籤。將顯示其他核取方塊，以**允許 802.1p 標記覆寫 DSCP 值**。選擇此核取方塊將斷言對應的 802.1p 值會覆寫用戶端可能已設定的任何 DSCP 值。這可用於覆寫用戶端自己設定的 DSCP CoS 值。	如果將**對應**設定為 DSCP 和 802.1p 的操作，對應將僅在一個方向進行：如果封包來自 VLAN 且到達時擁有 802.1p 標籤，DSCP 將從 802.1p 標籤對應；如果封包的目的地為 VLAN，將從 DSCP 標籤對應 802.1p。

相關範例，請參閱雙向 DSCP 標記操作，其中提供了雙向 DSCP 標記操作。

雙向 DSCP 標記操作



如果 HTTP 透過 192.168.168.100 的 Web 瀏覽器存取 10.50.165.2 的 Web 伺服器，會使內部（承載）封包和外部（封裝 ESP）封包標籤為 DSCP 值 8。如果封包來自於通道的另一端，並傳送到 10.50.165.2，它們將使用 DSCP 標籤 8。當 10.50.165.2 透過通道將回應封包傳送回 192.168.168.100（從第一個 SYN/ACK 封包開始）時，存取規則將使用 DSCP 值 8 標籤傳送到 192.168.168.100 的回應封包。

此行為將套用到 DSCP 和 802.1p 標記的四個 QoS 操作設定。

此行為的一個實用性應用是為到達 VPN 區域的流量設定 802.1p 標記規則。雖然不能透過 VPN 傳送 802.1p 標籤，但可以從通道輸出對透過 VPN 返回的回覆封包標籤 802.1 p。這就要求實體輸出介面的 802.1p 標籤處於活動狀態，且 [區域] > VPN 存取規則擁有「無」以外的 802.1p 標記操作。

確保 802.1p 與您相關的網路裝置相容，且在適用的 SonicWall 介面上啟用 802.1p 標記後，即可開始設定存取規則來管理 802.1p 標籤。

遠端站台 1網路可能有兩個存取規則，其設定如遠端站台 1：存取規則設定範例表格所示。

遠端站台 1：存取規則設定範例

設定	存取規則 1	存取規則 2
一般檢視		
操作	允許	允許
來源區域	LAN	VPN
到達區域	VPN	LAN
服務	VOIP	VOIP
來源	LAN 主要子網路	主站台子網路
目的地	主站台子網路	LAN 主要子網路
允許的使用者	全部	全部
排程	始終開啟	始終開啟
啟用記錄	啟用	啟用
允許片段的封包	啟用	啟用
Qos 檢視		
DSCP 標記操作	對應	對應
允許 802.1p 標記覆寫 DSCP 值	啟用	啟用
802.1p 標記操作	對應	對應

存取規則（管理 **LAN>VPN**）擁有以下效果：

- 來自 **LAN 主要子網路**並將透過 VPN 傳送至 **主站台子網路** 的 **VoIP** 流量（按照服務群組定義）應針對 DSCP 和 802.1p 標籤進行評估。
    - 將 DSCP 和 802.1p 標記操作共同設定為**對應**早在管理 QoS 標記中就有相關說明。
    - 傳送僅包含 802.1p 標記的流量（例如 CoS = 6）會使 DSCP 將 VPN 繫結內部（承載）封包標記為值 48。外部 (ESP) 封包也將使用值 48 標籤。
    - 假設主站台上的防火牆已對返回流量進行 DSCP 標籤 (CoS = 48)，則將在輸出對返回流量使用 CoS = 6 的 802.1p 標籤。
    - 傳送僅包含 DSCP 標記的流量（例如 CoS = 48）會將 DSCP 值保留到內部和外部封包中。
    - 假設主站台上的防火牆已對返回流量進行 DSCP 標籤 (CoS = 48)，則將在輸出對返回流量使用 CoS = 6 的 802.1p 標籤。
    - 傳送僅包含 802.1p 標記（例如 CoS = 6）和 DSCP 標記（例如因為 CoS= 63）的流量將優先考慮 802.1p 標記，並相應地進行對應。VPN 繫結內部（承載）封包使用值 48 進行 DSCP 標記。外部 (ESP) 封包也將使用值 48 標籤。

假設主站台上的防火牆已對返回流量進行 DSCP 標籤 (CoS = 48)，則將在輸出對返回流量使用 CoS = 6 的 802.1p 標籤。

若要檢查第二個存取規則的效果（VPN > LAN），可查看主站台設定的存取規則，如主站台：存取規則設定範例表格中所示。

主站台：存取規則設定範例

設定	存取規則 1	存取規則 2
一般檢視		
操作	允許	允許
來源區域	LAN	VPN
到達區域	VPN	LAN
服務	VOIP	VOIP
來源	LAN 子網路	遠端站台 1 子網路
目的地	遠端站台 1 子網路	LAN 子網路
允許的使用者	全部	全部
排程	始終開啟	始終開啟
啟用記錄	啟用	啟用
允許片段的封包	啟用	啟用
Qos 檢視		
DSCP 標記操作	對應	對應
允許 802.1p 標記覆寫 DSCP 值	啟用	啟用
802.1p 標記操作	對應	對應

來自**遠端站台 1 子網路**透過 VPN 發往 LAN 區域的 **LAN 子網路**的 **VoIP** 流量（按服務群組定義）將命中傳入 VoIP 呼叫的存取規則。到達 VPN 區域的流量將不包含任何 802.1p 標籤，僅包含 DSCP 標籤。

- 結束通道的包含 DSCP 標記的流量（例如 CoS = 48）將保留 DSCP 值。在將封包傳遞到 LAN 上的目的地之前，還將根據主站台的防火牆所設定的 **QoS 對應**（例如 CoS = 6）進行 802.1p 標記。
- 假設返回的流量已由主站台處接受呼叫的 VoIP 電話進行了 802.1p 標記（例如 CoS = 6），將根據透過 VPN 發回的內部和外部封包上的轉換對應 (CoS = 48) 進行 DSCP 標記。
- 假設返回的流量已由主站台處接受呼叫的 VoIP 電話進行了 DSCP 標記（例如 CoS = 48），則返回的流量將保留透過 VPN 發回的內部和外部封包上的 DSCP 標記。
- 假設返回的流量已由主站台處接受呼叫的 VoIP 電話進行了 802.1p 標籤（例如 CoS = 6）和 DSCP 標籤（例如 CoS = 14），將根據透過 VPN 發回的內部和外部封包上的轉換對應 (CoS = 48) 進行 DSCP 標籤。

頻寬管理

如需頻寬管理 (BWM) 的資訊，請參見頻寬管理 (BWM) 是將頻寬資源指派給網路上的關鍵應用程式的一種方法。。

術語

- **802.1p** - IEEE 802.1p 是第 2 層（MAC 層）服務類機制，透過在 802.1p 的附加 16 位元標頭中使用 3 個優先順序位元（共 8 個優先順序層級）來標籤封包。802.1p 處理需要相容的裝置才能產生標籤、識別並進行處理，且只能在相容的網路上使用。

- **頻寬管理 (BWM)** - 任何用於調整流量或原則流量的各種演算法或方法。調整通常是指管理傳出流量，監管通常是指管理傳入流量（又稱許可控制）。有多種不同的頻寬管理方法，包括各種佇列和丟棄技術，每種方法都有其各自的設計強度。SonicWall 使用基於令牌基於類的佇列方法進行傳出和傳入 BWM，並對指定類型的傳入流量使用丟棄機制。
- **服務類 (CoS)** - 指示符或識別項，例如第 2 層或第 3 層標記，將套用到分類之後的流量。服務品質 (QoS) 系統可使用 CoS 資訊區分網路上的流量類，並提供特殊處理（例如按優先順序佇列、降低延遲等），這由 QoS 系統管理員定義。
- **分類** - 用於識別（或區別）指定類型的流量。在 QoS 環境中，執行此操作的目的在於根據流量對延遲或封包遺失的敏感度提供自訂處理、典型的優先排序或取消優先排序。SonicOS 中的分類使用存取規則，並且根據以下元素中的任一或全部都可進行分類：來源區域、到達區域、來源位址物件、目的地位址物件、服務物件、排程物件。
- **碼位** - 主機或中間網路裝置對 IP 封包的 DSCP 部分進行標記的值。目前有 64 個碼位可用（從 0 到 63），可用於定義已標記流量的按升序排列優先順序的類。
- **調節** - 廣泛使用的一個術語，用於描述為網路流量提供服務品質的多種方法，包括但不限於丟棄、佇列、監管和調整。
- **DiffServ**（區分服務）一種用於區分 IP 網路上不同類型或類別的流量的標準，目的在於根據相關要求對流量提供調整處理。DiffServ 主要取決於 IP 封包的 ToS 標頭中標記的碼位值，這些碼位值用於區分不同類別的流量。DiffServ 服務層級在透過標記流量的每個路由器（或其他啟用 DiffServ 的網路裝置）上針對每個躍點執行。DiffServ 服務層級目前包含在最小**預設值**、**確保轉送**、**加速轉送**和 **DiffServ** 中。如需更多資訊，請參閱 DSCP 標記。
- **丟棄** - QoS 系統所使用的一種擁塞回避機制，用於嘗試在可能要發生擁塞的網路上進行預測，並透過丟棄超出限制的流量避免擁塞。還可將丟棄看做一種佇列管理演算法，因為它會嘗試避免所有佇列出現擁塞情況。進階丟棄機制遵守 CoS 標記，可避免丟棄敏感流量。常用的方法包括：
    - **尾部丟棄** - 處理滿佇列的一種不加選擇的方法，此此類佇列中，將丟棄最後一個入隊的封包，而不考慮其 CoS 標記。
    - **隨機早期偵測 (RED)** - RED 可監視佇列的狀態，以嘗試預測即將滿的佇列。然後以交錯的方式隨機丟棄封包，協助將可能發生的全域同步降到最低程度。RED 的基本實作（例如尾部丟棄）不考慮 CoS 標記。
    - **加權隨機早期偵測 (WRED)** - 將 DSCP 標記的因素包含到其丟棄決策過程的 RED 實作。
- **DSCP** -（差分服務代碼點）- 再利用 IP 標頭的 ToS 欄位，如 RFC2747 所述。DSCP 使用 64 個碼位值啟用 DiffServ（差分服務）。透過根據流量類標記流量，可對網路上的每個躍點正確地處理封包。
- **全域同步** - 丟棄的潛在副作用，設計用於處理滿佇列的擁塞回避方法。如果同時丟棄透過擁塞連結的多個 TCP 流（在發生尾部丟棄時），將發生全域同步。對於這些流中的每一個，如果原生 TCP 慢啟動機制幾乎同時開始，流將再次洪水攻擊連結。這將出現週期性的擁塞波和利用不足的現象。
- **承諾頻寬** - 介面上聲明的可用總頻寬的百分比，它可始終保證指定類別的流量。適用於傳入和傳出 BWM。透過所有 BWM 規則所保證的總頻寬不能超過可用總頻寬的 100%。SonicOS 增強了頻寬管理功能，可提供速率限制功能。現在您可以建立指定第 2、3 或 4 層網路流量的最大速率的流量原則。當主要 WAN 連結無法切換至不能處理足夠多流量的次要連接時，將啟用頻寬管理。也可將保證的頻寬設定為 0%。
- **傳入（輸入或 IBWM）** - 用於調整流量進入指定介面時的速率。對於 TCP 流量，透過延遲輸出確認 (ACK) 使傳送者減慢速率來調整輸入流量速率，可進行實際的調整。對於 UDP 流量，如果 UDP 無原生反饋控制項，將使用丟棄機制。
- **IntServ**（整合式服務）- 如 RFC1633 中定義。DiffServ 的替代 CoS 系統，IntServ 本質上不同於 DiffServ，在傳送其流量之前會使每個裝置請求（或保留）其網路要求。這需要網路上的每個躍點都能夠感

知 IntServ，還需要每個躍點保留每個流的狀態資訊。IntServ 不受 SonicOS 支援。最常用的 IntServ 實作為 RSVP。

- **最大頻寬** - 介面上聲明的可用總頻寬的百分比，用於定義指定類別的流量所允許的最大頻寬。適用於傳入和傳出 BWM。用作限制機制，可指定頻寬速率限制。頻寬管理功能已增強，可提供速率限制功能。現在您可以建立指定第 2、3 或 4 層網路流量的最大速率的流量原則。當主要 WAN 連結無法切換至不能處理足夠多流量的次要連接時，將啟用頻寬管理。可將最大頻寬設定為 0%，這將阻止所有流量。
- **傳出（輸出或 OBWM）** - 調節介面傳送流量的速率。傳出 BWM 使用基於貸記（或令牌）的佇列系統，此系統帶有 8 個優先順序環，可處理按照存取規則劃分的不同類型的流量。
- **優先順序** - 流量分類中使用的額外維度。SonicOS 使用 8 個優先順序環（0 = 最高，7 = 最低）包含用於 BWM 的佇列結構。將按照佇列的優先順序順序對其進行處理。
- **對應** - 對應與 SonicOS 的 QoS 實作相對，用於在第 2 層 CoS 標記 (802.1 p) 和第 3 層 CoS 標記 (DSCP) 之間相互轉換，目的在於保留透過不支援 802.1p 標記的網路連結的 802.1p 標記。對應通信完全由使用者定義，對應操作受存取規則控制。
- **標記** - 又稱**著色**或**上色** - 可將第 2 層 (802.1p) 或第 3 層 (DSCP) 資訊套用到封包中以便進行區分，從而使網路裝置能夠沿著其目的地路徑對其進行正確分類（識別）並優先排序。
- **MPLS**（多重通訊協定標籤交換）- 在 QoS 範圍內頻繁使用的一個術語，但大多數客戶的本機 IP 網路裝置對其不提供原生支援，包括 SonicWall 裝置。MPLS 是一個運營商類別的網路服務，它嘗試透過向網路中新增面向概念連接的路徑（標籤交換路徑 - LSP）來增強 IP 網路體驗。當封包離開客戶本機網路時，將由標籤邊緣路由器（LER）對其進行標記，以使此標籤可用於確定 LSP。MPLS 標記本身位於第 2 層和第 3 層之間，它對這兩層網路的 MPLS 特性都會產生影響。MPLS 成為 VPN 很常用的標記，可提供第 2 層和第 3 層 VPN 服務，但仍無法與現有 IPsec VPN 實作進行互操作。MPLS 還由於其 QoS 功能而眾所週知，可與一般的 DSCP 標記進行互操作。
- **每跳轉送行為 (PHB)** - 此處理方法將根據封包的 DSCP 分類，根據封包遍歷的每個支援 DiffServ 的路由器套用到此封包。此行為介於以下操作中：丟棄、重新標記（重新分類）、盡最大努力、確保轉送或加速轉送等。
- **監管** - 嘗試控制網路連結上的流量傳送的流量調整裝置。監管方法包括混亂封包丟棄、演算法調整以及各種佇列規則。
- **佇列** - 為有效利用連結的可用頻寬，通常使用佇列對分類後的流量進行排序和單獨管理。然後使用各種方法和演算法管理佇列，以確保較高的優先順序佇列總是有空間接收更多的流量，並且可在低優先順序佇列之前進行處理（或取消佇列）。一些常見的佇列規則包括：
  - **FIFO**（先進先出）- 一種非常簡單不加區別的佇列，其中先進入佇列的封包將先進行處理。
  - **基於類的佇列 (CBQ)** - 此佇列規則考慮了封包的 CoS，可確保優先處理高優先順序的流量。
  - **加權公平佇列 (WFQ)** - 嘗試使用簡單的公式並根據封包的 IP 優先順序和總流量處理佇列的一種規則。當存在大量不成比例的高優先順序流要處理時，WFQ 會變得不負載均衡，通常其效果與所需的效果相反。
  - **基於令牌的 CBQ** - CBQ 的一項使用令牌的增強功能，同時也是一個基於貸記的系統，有助於緩和或標準化連結利用率，避免出現突發流量以及利用不足的情況。供 SonicOS BWM 使用。
- **RSVP**（資源預留通訊協定）- 某些應用程式使用的一種 IntServ 信號傳送通訊協定，其中將請求對網路行為（例如延遲和頻寬）的預測需要，以使其能夠按照網路路徑進行保留。設定此保留路徑要求每個躍點始終啟用 RSVP，且每個躍點都同意保留請求的資源。此 QoS 系統比較佔用資源，因為它要求每個躍點都保持現有的流狀態。儘管 IntServ 的 RSVP 與 DiffServ 的 DSCP 差別較大，但兩者可以互操作。RSVP 不受 SonicOS 支援。

- **調整** - QoS 系統嘗試修改流量的速率，通常透過對傳送者使用一些反饋機制來實現。最常見的例子是 TCP 速率控制，其中，返回至 TCP 傳送者的確認 (ACK) 將進行佇列並延遲，以增加計算的往返時間 (RTT)，同時利用 TCP 的固有行為強制傳送者減慢傳送資料的速度。
- **服務類型 (ToS)** - IP 標頭中的一個欄位，在其中可指定 CoS 資訊。在以前會將其與 IP 優先順序位元一起使用來定義 CoS（儘管這種情況很少見）。現在 DiffServ 的碼位值經常使用 ToS 欄位。

6

設定 SSL 控制

本章節說明了如何計劃、設計、實作和維護 SSL 控制功能。

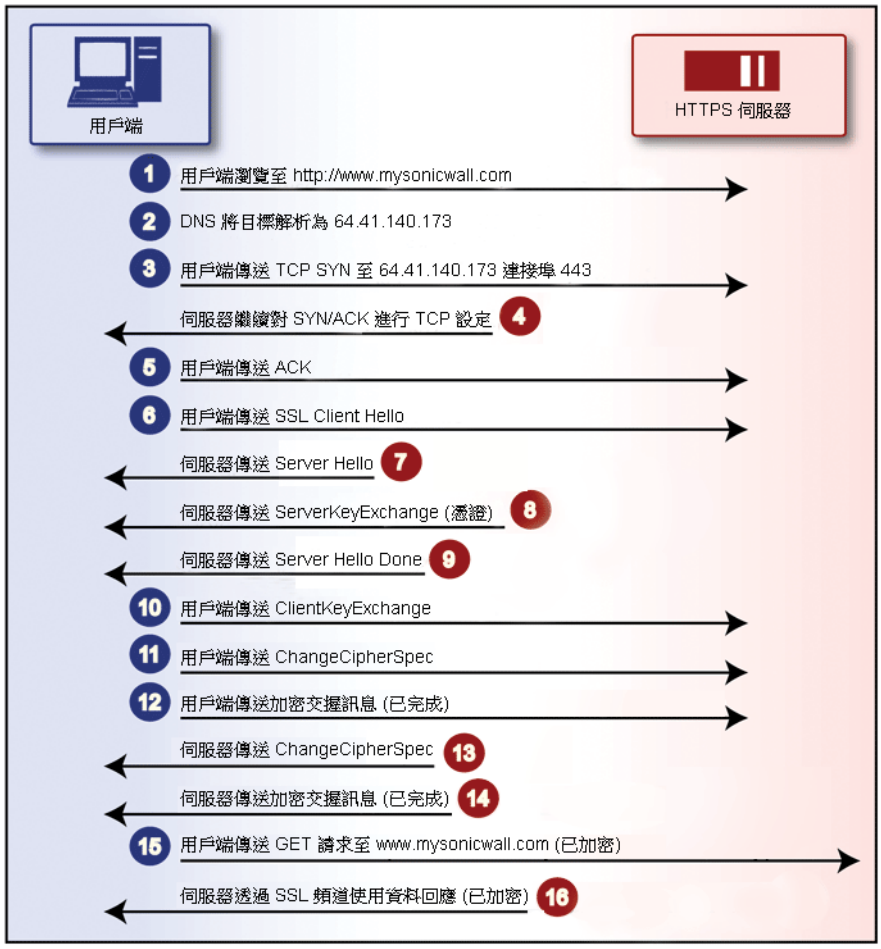
主題：

- 關於 SSL 控制
- SSL 控制設定
- 啟用區域中的 SSL 控制
- SSL 控制事件

關於 SSL 控制

SonicOS 包含 SSL 控制，這是用於對 SSL 工作階段提供交握可視性的一個系統，也是為控制 SSL 連接的建立而構建原則的一種方法。SSL（安全套接字層）是用於加密基於 TCP 網路通信的主要標準，具有最常用的 HTTPS 應用程式（透過 SSL 的 HTTP）；參見透過 SSL 的 HTTP 通信。SSL 為網路通信提供了基於數字憑證的端點識別和基於加密摘要的機密性。

透過 SSL 的 HTTP 通信



SSL 提供的安全效果是阻礙所有承載，包括建立 HTTPS 工作階段時用戶端請求的 URL（統一資源識別項，例如 https://www.mysonicwall.com）。這是因為使用 HTTPS 時將在加密的 SSL 通道內傳送 HTTP。直到建立了 SSL 工作階段（請參閱透過 SSL 的 HTTP 通信），用戶端才會請求實際的目標資源 (`www.mysonicwall.com`)，但由於已建立 SSL 工作階段，防火牆或其他任何中間裝置都將不能再檢查工作階段資料。因此，基於 URL 的內容篩選系統將不會考慮請求，無法使用除 IP 位址之外的任何其他方法確定權限。

由於基於主機頭的虛擬主機（在 SSL 控制的主要概念中定義）的效率和通用性，對於未加密的 HTTP，以 IP 位址為主的篩選未能正常運作，而由於基於主機頭的 HTTPS 站台較少，對於 HTTPS，IP 篩選可有效運作。但此信任依賴於 HTTPS 伺服器運算子的完整性，並假定未將 SSL 用於欺詐目的。

很大程度上，可將 SSL 合法地用於防護敏感通信，例如線上購物或線上銀行，或存在個人資訊交換或重要資訊交換的任何工作階段。成本和複雜性不斷降低的 SSL 也刺激了更多可疑 SSL 應用程式的發展，其設計的目的主要是混淆或隱藏，而不是安全。

越來越常見的偽裝方法是使用 SSL 加密的基於 Web 的代理伺服器隱藏瀏覽資訊並繞過內容篩選。可輕鬆地封鎖此順序（按照其 IP 位址排序）的常見 HTTPS 代理服務，但實際上無法封鎖透過簡單的 Web 搜尋即可就緒的數千個私人代理伺服器。面臨的挑戰是不斷增加的此類服務數量，而不是它們不可預測的性質。由於這些服務通常位於使用動態位址 DSL 和纜線數據機連接的家庭網路上，目的地會不斷地移動。嘗試封鎖未知的 SSL 目的地將需要封鎖所有 SSL 流量，而實際上這是不可行的。

透過向管理員提供分析基於原則的控制並將其應用到 SSL 工作階段建立的功能，SSL 控制提供了很多方法來解決此難題。而目前的實作不會解碼 SSL 應用程式資料，它允許基於閘道的識別但不允許可疑的 SSL 流量。

主題：

- SSL 控制的主要功能
- SSL 控制的主要概念
- 注意事項和建議

SSL 控制的主要功能

SSL 控制：功能和優點

功能	優點
基於一般名稱的黑名單和白名單	您可定義明確允許或拒絕的憑證主旨一般名稱的清單（在「主要概念」中有相關說明）。將在子字串中符合項目，例如 `prox` 的黑名單將符合 `www.megaproxy.com`、`www.proxify.com` 和 `roxify.net`。這使您可以輕鬆地封鎖使用憑證的所有 SSL 交換，此類憑證將發佈到可能會受到拒絕的名稱的主旨。相反，透過在白名單中列出組織的公用子字串，您可輕鬆地授權組織中的所有憑證。每個清單都包含最多 1,024 個項目。 由於評估是針對包含在憑證中的主旨一般名稱執行的，即使用戶端嘗試透過使用其他主機名稱或 IP 位址隱藏對這些站台的存取，也會始終偵測到憑證中的主旨，並將套用原則。
自我簽署的憑證控制	透過 SSL 防護合法站台的一般做法是使用眾所週知的憑證授權機構發佈的憑證，這是 SSL 受信的基礎。透過 SSL（例如 SonicWall 網路安全裝置）防護網路裝置的最常見做法是對其預設的安全方法使用自我簽署的憑證。因此，如果封閉環境中的自我簽署的憑證不是可疑的，公用網站或商業網站將使用自我簽署的憑證。使用自我簽署的憑證的公用網站通常表明嚴格使用了 SSL 進行加密，而不是用於受信任和識別。這並不是絕對有罪，有時表明其目的是為了隱藏，因為這對於 SSL 加密的代理網站很常見。 設定原則以封鎖自我簽署的憑證的功能使您可以避免暴露的可能性。為避免與使用自我簽署的憑證的已知/受信 SSL 站台的通信中斷，可使用白名單功能將其設定為顯見允許。
不受信任的憑證授權控制	與自我簽署的憑證的用法相似，遇到不受信任的 CA 頒發的憑證並不絕對表明是不名譽的憑證，但它確實表明信任不可靠。 SSL 控制會將 SSL 交換中的憑證的頒發者與防火牆憑證儲存中的憑證相比較。憑證儲存包含大約 100 個常見的 CA 憑證，非常類似於當今的 Web 瀏覽器。如果 SSL 控制遇到的 CA 頒發的憑證不在其憑證儲存中，將會禁止 SSL 連接。 對於執行其獨自的私人憑證授權的組織，可輕鬆地將私人 CA 憑證匯入到防火牆的憑證儲存中，以將私人 CA 識別為受信任項。此儲存最多可包含 256 個憑證。
SSL 版本、密碼長度和憑證驗證控制	SSL 控制根據交涉特性提供了 SSL 工作階段的額外控制，包括停用潛在可利用的 SSLv2、停用弱加密（密碼長度小於 64 位元）、在憑證的資料範圍無效的情況下停用 SSL 交涉的功能。這使管理員可以為網路使用者建立非常安全的環境，同時不會由於不可見的加密缺點或不考慮安全警告或對安全警告產生誤解而暴露於風險中。

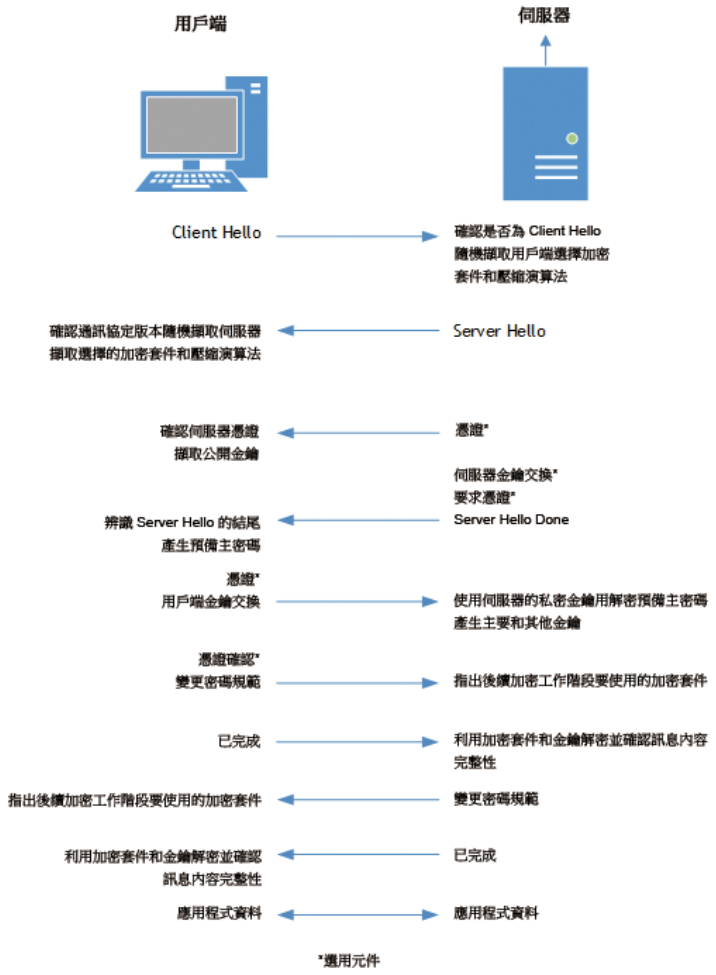
SSL 控制：功能和優點

功能	優點
區域型應用程式	SSL 控制在區域層級中套用，使您可以在網路上強制實施 SSL 原則。在區域中啟用 SSL 控制後，防火牆透過觸發檢查，將查找從此區域的用戶端傳送的用戶端問候。防火牆將查找為回應對設定原則的評估而傳送的伺服器問候和憑證。啟用 LAN 區域中的 SSL 控制的其中一個結果是將檢查 LAN 上用戶端啟動的、將到達任何目的地區域的所有 SSL 流量。
設定操作和事件通知	如果 SSL 控制偵測到違反了原則，將會記錄事件並封鎖連接，或將在允許連接繼續的情況下記錄事件。

SSL 控制的主要概念

- **SSL**- 安全套接字層 (SSL) 是 Netscape 於 1995 年引入的網路安全機制。SSL 設計為「在兩個通信應用程式（用戶端和伺服器）之間提供私密防護，同時也會對伺服器進行驗證，並選擇性地對用戶端進行驗證」。SSL 最常見的應用程式是 HTTPS，由 URL 指定，開頭為 `https://` 而非 `http://`，可將其識別為加密網際網路上的 Web 流量的標準方法。SSL HTTP 通常使用 TCP 連接埠 443 傳送，而一般 HTTP 使用 TCP 連接埠 80 傳送。儘管 HTTPS 是 SSL 最常用的，但 SSL 不僅僅限於防護 HTTP 的安全，還可用於防護其他 TCP 通訊協定的安全，例如 SMTP、POP3、IMAP 和 LDAP。SSL 工作階段的建立如建立 SSL 工作階段所示：

建立 SSL 工作階段



- **SSLv2** - SSL 的最早版本仍在普遍使用。曾發現 SSLv2 存在很多缺點、限制和理論缺陷（比較性地備註在 SSLv3 項目中），純粹的安全主義者對此不屑一顧。
- **SSLv3** - SSLv3 設計為保持向後與 SSLv2 的相容，同時新增了以下增強功能：
  - 替代金鑰交換方法，包括 Diffie-Hellman。
  - 支援金鑰交換和批量加密的硬體標誌。
  - SHA、DSS 和 Fortezza 支援。
  - 帶外資料傳送。
  - TLS - 傳送層安全，又稱 SSLv3.1，類似於 SSLv3，但透過 SSL 與 TLS 之間的差異表格所示的方式增強了 SSLv3：

SSL 與 TLS 之間的差異

SSL	TLS
使用初步 HMAC 演算法	使用 RFC 2104 中所述的 HMAC
請勿將 MAC 套用到版本資訊	將 MAC 套用到版本資訊
請勿指定填充值	將填充初始化為指定值
警示和警告的限制設定	詳細的警示和警告訊息

附註：SonicOS 6.2.2.1 及更高版本支援 TLS 1.1 和 1.2。

- **MAC** - 透過將演算法（例如 MD5 或 SHA1）套用到資料可計算 MAC（訊息驗證碼）。MAC 是訊息摘要，或易於計算的單向雜湊程式碼，但實際上無法恢復。換言之，如果單獨使用 MAC，將無法從理論上確定摘要基於哪個訊息。同樣也很難找到產生同一個 MAC 的兩個不同訊息。如果接收方的 MAC 計算與傳送方的 MAC 計算在給定的資料範圍內相符合，接收方將確保在傳送過程中不會改動資料。
- **用戶端問候** - 建立 TCP 工作階段後用戶端傳送到伺服器的第一則訊息。此訊息從 SSL 工作階段開始，包含以下元件：
  - **版本** - 用戶端想要在通信中使用的 SSL 的版本。通常是用戶端支援的 SSL 最新版本。
  - **隨機** - 32 位元時間戳記，外加 28 位元組的隨機結構。
  - **工作階段 ID** - 如果不存在任何工作階段 ID（本質上請求新工作階段），則可為空，也可以參考之前發佈的工作階段 ID。
  - **密碼集** - 加密演算法清單，以優先順序排列，受用戶端支援。
  - **壓縮方法** - 用戶端支援的壓縮方法清單（通常為空）。
- **伺服器問候** - SSL 伺服器對用戶端問候的回應。此部分是 SSL 控制檢查的 SSL 交換。伺服器問候包含在工作階段中交涉的 SSL 的版本以及密碼、工作階段 ID 和憑證資訊。儘管是單獨的 SSL 交換步驟，但實際的 X.509 伺服器憑證通常從和伺服器問候相同的封包開始（和結束）。
- **憑證** - X.509 憑證是不可變更的數字戳，用於電子安全審批。存在四種主要的憑證特性：
  - 使用一般名稱和可分辨名稱（CN 或 DN）識別憑證的主旨。
  - 包含可用於加密和解密雙方之間的資訊的公開金鑰。
  - 由發佈憑證的受信任組織（憑證授權單位）提供數位簽章。
  - 指示憑證的有效日期範圍

- **主旨** - 一般名稱 (CN) 識別的憑證保證。用戶端瀏覽 SSL 站台（例如 https://www.mysonicwall.com）時，伺服器會傳送之後由用戶端評估的憑證。用戶端檢查憑證的日期是否有效，是否由受信 CA 頒發，並且主旨 CN 是否符合請求的主機名稱（即，均為 www.mysonicwall.com）。儘管主旨 CN 不符合會產生瀏覽器警示，但並非總是欺騙的標誌。例如，如果用戶端瀏覽 https://mysonicwall.com（此網址會解析為與 www.mysonicwall.com 相同的 IP 位址），伺服器將顯示其憑證以及包含 www.mysonicwall.com 的主旨 CN。將對用戶端顯示警示，而不論有效的總連接數如何。
- **憑證授權單位 (CA)** - 憑證授權單位是一個受信任的實體，可對憑證按照預期進行簽章，以驗證憑證主旨的身分。常見的憑證頒發機構包括 VeriSign、Thawte、Equifax 和 Digital Signature Trust。通常，對於要在 SSL 框架中受信任的 CA，其憑證必須儲存在受信任儲存區中，例如大多數 Web 瀏覽器、操作系統和執行時環境使用的儲存區。SonicOS 受信的儲存區可透過**系統 > 憑證**頁面存取。CA 模型是在相關信任基礎上構建的，其中，用戶端信任 CA（擁有其受信儲存區中的 CA 憑證），CA 信任主旨（透過向主旨發佈憑證），因此用戶端可信任主旨。
- **不信任的 CA** - 不信任的 CA 是指未包含在用戶端的信任儲存區中的 CA。在 SSL 控制中，不信任的 CA 是其憑證不存在於**系統 > 憑證**中的任何 CA。
- **自我簽署的憑證** - 其發佈者的一般名稱和主旨的一般名稱相同的任何憑證，可指示憑證是自我簽署的憑證。
- **虛擬託管** - Web 伺服器所使用的一種方法，用於在單個伺服器中託管多個網站。虛擬託管的一般實作是基於名稱的（主機頭）虛擬託管，允許單個 IP 位址託管多個網站。如果使用主機頭虛擬託管，伺服器將透過評估用戶端傳送的「Host:」標頭評估請求的站台。例如，www.website1.com 和 www.website2.com 可能會解析為 64.41.140.173。如果用戶端傳送「GET /」以及「Host: www.website1.com」，伺服器可將對應的內容返回到此站台。

  主機頭虛擬託管通常在 HTTPS 中使用，因為只有建立了 SSL 連接才能讀取主機頭，但只有在伺服器傳送憑證之後才能建立連接。由於伺服器無法確定用戶端將請求哪個站台（在 SSL 交握期間知道的只有 IP 位址），也就無法確定要傳送的對應憑證。傳送任何憑證都可能會允許 SSL 交握開始，憑證名稱（主旨）不符合將觸發瀏覽器警示。
- **弱密碼** - 相對較弱的對稱性加密密碼。如果密碼長度小於 64 位元，將之劃分為弱密碼。大多數匯出密碼都是弱密碼。常見的弱密碼表格列出了常見的弱密碼：

常見的弱密碼

加密	加密	發生在
EXP1024-DHE-DSS-DES-CBC-SHA	DES(56)	SSLv3、TLS (匯出)
EXP1024-DHE-CBC-SHA	DES(56)	SSLv3、TLS (匯出)
EXP1024-RC2-CBC-MD5	RC2(56)	SSLv3、TLS (匯出)
EDH-RSA-DES-CBC-SHA	DES(56)	SSLv3、TLS
EDH-DSS-DES-CBC-SHA	DES(56)	SSLv3、TLS
DES-CBC-SHA	DES(56)	SSLv2、SSLv3、TLS
EXP1024-DHE-DSS-RC4-SHA	RC4(56)	SSLv3、TLS (匯出)
EXP1024-RC4-SHA	RC4(56)	SSLv3、TLS (匯出)
EXP1024-RC4-MD5	RC4(56)	SSLv3、TLS (匯出)
EXP-EDH-RSA-DES-CBC-SHA	DES(40)	SSLv3、TLS (匯出)
EXP-EDH-DSS-DES-CBC-SHA	DES(40)	SSLv3、TLS (匯出)
EXP-DES-CBC-SHA	DES(40)	SSLv3、TLS (匯出)

常見的弱密碼

加密	加密	發生在
EXP-RC2-CBC-MD5	RC2(40)	SSLv2、SSLv3、TLS (匯出)
EXP-RC4-MD5	RC4(40)	SSLv2、SSLv3、TLS (匯出)

注意事項和建議

1 **自我簽署和不信任 CA 的強制措施** - 如果強制使用其中任一選項，則強烈建議您將組織中任何安全網路裝置的一般名稱新增到白名單中，以確保與這些裝置的連線不會中斷。例如，SonicWall 網路安全裝置的預設主旨名稱為 192.168.168.168，SonicWall SSL VPN 裝置的預設一般名稱為 192.168.200.1。

2 如果您的組織使用自己私人的憑證授權單位 (CA)，則強烈建議您將私人的 CA 憑證匯入到**系統 > 憑證**儲存，特別是在您要封鎖不信任 CA 發佈的憑證時。如需此過程的更多資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

3 SSL 控制檢查目前僅針對 TCP 連接埠 443 流量執行。此時不會對非標準連接埠上的 SSL 交涉進行檢查。

4 **伺服器問候分段** - 在較少的情況下，SSL 伺服器會對伺服器問候資訊進行分段。在此情況下，目前實作的 SSL 控制將不會解碼伺服器問候資訊。SSL 控制原則將不會套用到 SSL 工作階段，但允許 SSL 工作階段。

5 **工作階段終止的處理** - 如果 SSL 控制偵測到違反了原則並終止了 SSL 工作階段，它將僅終止 TCP 層的工作階段。由於 SSL 工作階段此時處於初級狀態，目前不能重新導向用戶端，也不能向用戶端提供任何類別的終止資訊通知。

6 **白名單優先** - 白名單優先於所有其他 SSL 控制元素。與白名單中的項目相符合的任何 SSL 伺服器憑證都將允許 SSL 工作階段繼續（即使其他 SSL 工作階段元素違反了設定的原則）。這是按設計設定的。

7 預安裝的常見 CA 憑證數為 93。最終的儲存庫非常類似於可在大多數 Web 瀏覽器中找到的儲存庫。其他憑證相關的變更：

   a CA 憑證的最大數已從 6 增加到 256。

   b 單獨憑證的最大數已從 2,048 增加到 4,096。

   c 白名單和黑名單中的項目最大數為每個 1,024。

SSL 控制設定

附註：設定 SSL 控制之前，先確定您的防火牆有支援 IPv6。您可以透過使用**系統 > 診斷**頁面上的 **IPv6 檢查網路設定**工具來確認此項；請參閱 *SonicWall SonicOS 6.5 調查*。

SSL 控制位在**安全設定 | 防火牆設定 > SSL 控制**下的**管理**檢視上。SSL 控制擁有全域設定和每個區域的設定。預設情況下，在全域層級或區域層級啟用 SSL 控制。單獨的頁面控制如下所示（如需本部分使用的術語的更多資訊，請參閱 SSL 控制的主要概念）。

主題：

- 一般設定
- 操作
- 設定
- 自訂清單

一般設定

一般設定區段可讓您啟用或停用 SSL 控制：

- **啟用 SSL 控制** - SSL 控制的全域設定。必須啟用此選項才能使套用到區域的 SSL 控制起效。預設情況下未勾選此選項。

操作

您可在**操作**區段指定在偵測到違反 SSL 原則時所採取的行動，或者：

- **記錄事件** - 如果偵測到違反了以下**設定**部分中定義的 SSL 原則，將記錄此事件，但允許 SSL 連接繼續。預設情況下未勾選此選項。
- **封鎖連接和記錄事件** - 在違反原則事件中，將封鎖連接並記錄事件。預設情況下已核取此選項。

設定

設定區段可讓您指定要強制執行的 SSL 原則：

- **啟用黑名單** - 如自訂清單中的設定，控制黑名單中的項目偵測。預設情況下已核取此選項。
- **啟用白名單** - 按照以下**設定清單**部分中的設定控制白名單中的項目偵測。白名單項目優先於其他所有的 SSL 控制設定。預設情況下已核取此選項。
- **偵測到過期憑證** - 對於起始日期早於目前系統時間或終止日期晚於目前系統時間的憑證，控制對其的偵測。資料的有效性取決於防火牆的系統時間。在**系統 > 時間**頁面上，確保已正確設定系統時間，能夠更好地與 NTP 同步。預設情況下未勾選此選項。
- **偵測不完整的憑證** - 控制包含不完整資訊的憑證偵測。預設情況下未勾選此選項。
- **偵測弱密碼（<64 位元）** - 控制與長度小於 64 位元的對稱密碼交涉的 SSL 工作階段的偵測，通常指示匯出密碼的使用。預設情況下未勾選此選項。
- **偵測弱式摘要憑證** - 控制使用 MD5 或 SHA1 建立的憑證偵測。MD5 或 SHA1 兩者都被認為不安全。預設情況下未勾選此選項。
- **偵測自我簽署的憑證** - 在頒發方和主旨具有相同的一般名稱時控制憑證的偵測。預設情況下已核取此選項。

  透過 SSL 防護合法站台的一般做法是使用眾所週知的憑證授權機構發佈的憑證，這是 SSL 受信的基礎。透過 SSL（例如 SonicWall 安全裝置）防護網路裝置的最常見做法是對其預設的安全方法使用自我簽署的憑證。因此，如果封閉環境中的自我簽署的憑證不是可疑的，公用網站或商業網站將使用自我簽署的憑證。使用自我簽署的憑證的公用網站通常表明嚴格使用了 SSL 進行加密，而不是用於受信任和識別。這並不是絕對有罪，有時表明其目的是為了隱藏，因為這對於 SSL 加密的代理網站很常見。設定原則以封鎖自我簽署的憑證的功能使您可以避免暴露的可能性。為避免與使用自我簽署的憑證的已知/受信 SSL 站台的通訊中斷，可針對明確允許使用白名單功能。
- **偵測不信任的 CA 簽署憑證** - 在頒發方的憑證不在**系統 > 憑證**信任儲存中的情況下控制憑證的偵測。預設情況下已核取此選項。

  與自我簽署的憑證的用法相似，遇到不受信任的 CA 頒發的憑證並不絕對表明是不名譽的憑證，但它確實表明信任不可靠。SSL 控制會將 SSL 交換中的憑證簽發者與 SonicWall 防火牆中儲存中的憑證做比較，其中大多數知名 CA 憑證均包含在內 。對於執行其獨自的私人憑證授權的組織，可輕鬆地將私人 CA 憑證匯入到 SonicWall 的白名單，將私人 CA 識別為受信任項。
- **偵測 SSLv2** - 控制 SSLv2 交換的偵測與封鎖。SSLv2 容易受到密碼降級的攻擊，因為它不會對交握執行完整的檢查。推薦的最佳做法是在其合適的位置處使用 SSLv3 或 TLS。預設情況下未勾選此選項。
- **偵測 SSLv3** - 控制 SSLv3 交換的偵測與封鎖。預設情況下未勾選此選項。
- **偵測 TLSv1** - 控制 TLSv1 交換的偵測與封鎖。預設情況下未勾選此選項。

自訂清單

自訂清單區段允許您設定自訂白名單與黑名單。

- **設定黑名單和白名單** - 允許您定義用於比對 SSL 憑證中的一般名稱的字串。項目區分大小寫，將使用模式符合形式，如黑名單和白名單：模式符合表格所示：

黑名單和白名單：模式符合

項目	符合	不符合
sonicwall.com	https://www.sonicwall.com, https://csm.demo.sonicwall.com, https://mysonicwall.com, https://supersonicwall.computers.org, https://67.115.118.87 [1]	https://www.sonicwall.de
prox	https://proxify.org, https://www.proxify.org, https://megaproxy.com, https://1070652204 [2]	https://www.freeproxy.ru [3]

1. 67.115.118.67 是目前 sslvpn.demo.sonicwall.com 解析到的 IP 位址，此網站使用發佈給 sslvpn.demo.sonicwall.com 的憑證。這會導致符合為「sonicwall.com」，因為符合的發生基於憑證中的一般名稱。
2. 這是 IP 位址 63.208.219.44 的十進位表示法，其憑證將發佈給 www.megaproxy.com。
3. www.freeproxy.ru 將與「prox」不符合，因為此網站目前展示的憑證中的一般名稱為發佈給「-」的自我簽署的憑證。但這可透過啟用控制自我簽署憑證或不受信任的 CA 憑證輕鬆將其封鎖。

設定白名單和黑名單：

1 導覽至**安全設定 | 防火牆設定 > SSL 控制**頁面。

2 按一下**設定**按鈕。將顯示**SSL 控制自訂清單**對話。

3 如需將憑證新增到黑名單或白名單表，按一下**新增**。顯示**新增受信任的黑名單/白名單網域項目**對話。

4 在**憑證一般名稱**欄位中輸入憑證的名稱。

> **附註：**清單的符合將基於 SSL 交換中顯示的憑證中的主旨一般名稱，而不是在用戶端請求的 URL（資源）中。

可使用每個清單下的按鈕編輯和刪除憑證。

5 按一下**確定**。

對 SSL 控制設定所做的任何變更都不會影響目前建立的連接；僅檢查和影響提交變更之後的新 SSL 交換。

6 按一下**確定**。

7 按一下**接受**。

啟用區域中的 SSL 控制

全域啟用 SSL 控制並設定所需的選項後，必須在一個或多個區域中啟用 SSL 控制。在區域中啟用 SSL 控制後，防火牆透過觸發檢查，將查找從此區域的用戶端傳送的用戶端問候。然後防火牆將查找為回應對設定原則的評估而傳送的伺服器問候和憑證。啟用 LAN 區域中的 SSL 控制的其中一個結果是將檢查 LAN 上用戶端啟動的、將到達任何目的地區域的所有 SSL 流量。

附註：如果要啟用某區域（例如 LAN 區域）中的 SSL 控制，而此區域中的用戶端將存取連接防火牆的另一個區域（例如 DMZ 區域）中的 SSL 伺服器，推薦您將伺服器憑證的主旨一般名稱新增到白名單中，以確保連續的受信任存取。

如需啟用區域中的 SSL 控制：

1 導覽至**系統安裝 | 網路 > 區域**頁面。

2 選擇所需區域的**設定**圖示。顯示**編輯區域**對話。

3 選擇**啟用 SSL 控制**核取方塊。

4 按一下**確定**。從此區域啟動的所有新 SSL 連接現在都將接受檢查。

SSL 控制事件

如果使用者手動登入或透過 CIA/單點登入識別，記錄事件會將用戶端的使用者名稱包含到備註部分（未顯示）。如果使用者的身分無法使用，備註將指示此使用者為*無法識別*。

SSL 控制：事件訊息

#	事件訊息	發生的條件
1	SSL 控制：憑證日期無效	憑證的起始日期早於 SonicWall 系統時間或終止日期晚於系統時間。
2	SSL 控制：憑證鏈不完整	擁有頂級 CA 信任層級的中間 CA 頒發的憑證，但 SSL 伺服器不顯示中間憑證。此記錄事件是資訊型事件，不影響 SSL 連接。
3	SSL 控制：自我簽署的憑證	憑證是自我簽署（頒發者 CN 和主旨符合）。 **附註：**關於強制自我簽署的憑證控制的資訊，請參見注意事項和建議。
4	SSL 控制：不信任的 CA	頒發憑證的 CA 沒有位於防護牆的**系統 > 憑證**儲存中。 **附註：**關於強制自我簽署的憑證控制的資訊，請參見注意事項和建議。
5	SSL 控制：黑名單中找到的網站	將主旨符合模式的公用名輸入到黑名單中。
6	SSL 控制：使用的是弱密碼	交涉的對稱密碼長度小於 64 位元。關於弱密碼的清單，請參見常見的弱密碼表格。
7	參見 #2	參見 #2。

SSL 控制：事件訊息

#	事件訊息	發生的條件
8	SSL 控制：無法解碼伺服器問候資訊	無法破譯來自 SSL 伺服器的伺服器問候資訊。如果憑證和伺服器問候訊息位於不同的封包，也會出現此情況，在連接 SonicWall 裝置上的 SSL 伺服器時經常會發生此類事件。此記錄事件是資訊型事件，不影響 SSL 連接。
9	SSL 控制：SSL 控制：白名單中找到的網站	將主旨符合模式的公用名輸入到白名單中。始終允許白名單項目，即使在交涉中違反了其他原則，例如 SSLv2 或弱密碼。
10	SSL 控制：透過 SSLv2 的 HTTPS	使用 SSLv2 交涉 SSL 工作階段，容易受到某些中間人攻擊。推薦的最佳做法是使用 SSLv3 或 TLS。

7

管理 SonicWall 安全服務

- SonicWall 安全服務
- 設定安全服務

SonicWall 安全服務

SonicWall 提供多種基於訂閱的安全服務，為您的網路實現分層式安全。SonicWall 安全服務旨在無縫整合到您的網路以提供完整的防護。

防火牆管理介面上的**安全服務**中列出以下基於訂閱的安全服務：

- SonicWall 內容篩選服務
- SonicWall 用戶端防毒
- SonicWall 閘道防毒
- SonicWall 入侵保護服務
- SonicWall 防間諜軟體
- SonicWall RBL 篩選
- SonicWall Geo-IP 篩選條件
- SonicWall Botnet 篩選條件

提示：在註冊您的防火牆後，您可以嘗試免費試用版 SonicWall 內容篩選服務、SonicWall 用戶端防毒、SonicWall 閘道防毒、SonicWall 入侵保護服務和 SonicWall 防間諜軟體。

您可以直接從 SonicWall 管理介面或 https://www.mysonicwall.com 啟用和管理 SonicWall 安全服務。

設定安全服務

以下章節描述在**安全服務 > 基本設定**頁面的面板上執行的全域設定：

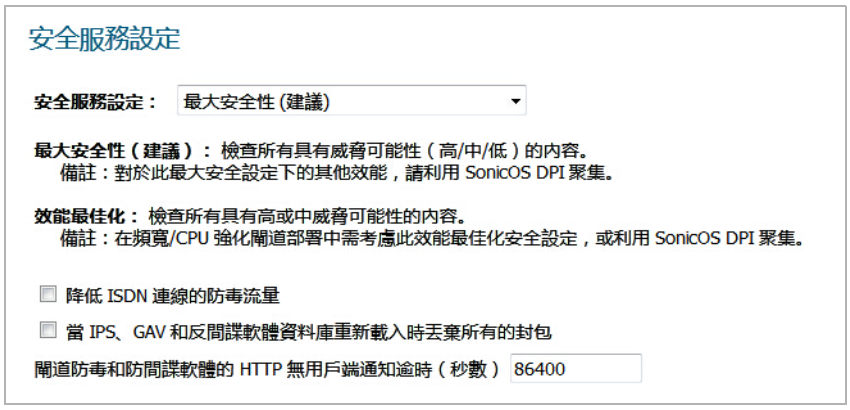
- 同步授權
- 安全服務設定
- 通過代理伺服器下載簽章和註冊
- 安全服務資訊
- 手動更新特徵標記資料

同步授權

要將您的 mysonicwall.com 帳戶與**安全服務摘要**表格同步，按一下**與 www.mysonicwall.com 同步授權**，然後按一下**同步**。

若要管理授權，請按一下**若要管理授權，請移至 www.mysonicwall.com**裡的連結。

安全服務設定

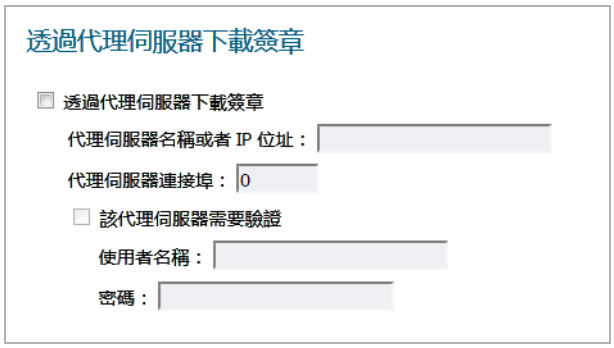


安全服務設定部分提供了以下選項用於微調 SonicWall 安全服務：

- **安全服務設定** - 此下拉功能表用於指定套用 SonicWall 安全服務實現最大安全性還是最優的效能：
  - **最大安全性（建議）** - 檢查所有有威脅可能性（高/中/低）的內容。為了在最大安全性設定下獲得更高效能，請利用 SonicOS HA 叢集。
  - **效能最佳化** - 檢查所有有高或中威脅可能性的內容。在頻寬或 CPU 強化閘道部署中需考慮此效能最佳化安全設定，或利用 SonicOS HA 叢集。

  最大安全性設定可提供最大程度的防護。**效能最佳化**設定利用對目前已知威脅的知識提供對威脅範圍內主動威脅的高度防範。
- **降低 ISDN 連接的防毒流量** - 選擇此功能以啟用 SonicWall 防毒機制，每天（每 24 小時）檢查一次更新，並為不能始終連至 Internet 的使用者減少傳出通訊的頻率。
- **當 IPS、GAV 和反間諜軟體資料庫重載的時候丟棄所有的封包** - 選擇此選項以指示防火牆在 IPS、GAV 和防間諜軟體資料庫正在更新時丟棄所有封包。
- **閘道防毒和防間諜軟體的 HTTP 無用戶端通知逾時** - 設定防火牆在 GAV 或防間諜軟體偵測到來自 HTTP 伺服器的威脅後多長時間通知使用者。預設逾時時限是一天（86400 秒）。

通過代理伺服器下載簽章和註冊



這部分允許 SonicWall 網路安全裝置在必須存取網際網路時通過代理伺服器下載簽章。此功能還允許通過代理伺服器註冊 SonicWall 網路安全裝置，同時不影響隱私防護。

啟用通過代理伺服器下載簽章或註冊裝置的步驟如下：

1. 勾選**透過代理伺服器下載簽章**核取方塊。
2. 在**代理伺服器名稱或者 IP 位址**欄位，輸入代理伺服器的主機名稱或 IP 位址。
3. 在**代理伺服器連接埠**欄位，輸入用於連接代理伺服器的連接埠號。
4. 如果代理伺服器需要**使用者名稱**和**密碼**，則勾選**該代理伺服器需要驗證**核取方塊。
5. 如果裝置尚未通過 MySonicWall.com 註冊，還會顯示兩個附加欄位：
   - **MySonicWall 使用者名稱** - 輸入註冊裝置的 mysonicwall.com 帳戶的使用者名稱。
   - **MySonicWall 密碼** - 輸入 mysonicwall.com 帳戶密碼。
6. 按一下頁面頂部的**接受**。

安全服務資訊

目前未使用此面板。

手動更新特徵標記資料

手動特徵庫更新功能適用於那些不可能或不需要（出於安全原因）始終具有可靠的寬頻 Internet 連接的網路。手動特徵庫更新功能為網路管理員提供了更新最新特徵庫的方法。網路管理員首先從 http://www.mysonicwall.com 下載特徵標記到單獨的電腦、USB 磁碟機或其他媒體上。然後，網路管理員將特徵庫上載到防火牆。相同的特徵標記更新檔案可用於所有符合以下要求的 SonicWall 網路安全裝置：

- 註冊到同一 mysonicwall.com 帳戶的裝置。
- 屬於相同級別 SonicWall 網路安全裝置的裝置。

手動更新特徵檔案的步驟如下：

1 在**安全服務 > 摘要**頁面，捲動至頁面底部的**手動更新特徵標記資料**標題。記錄裝置的**特徵標記檔案 ID**。

2 使用註冊 SonicWall 網路安全裝置時用的 mysonicwall.com 帳戶登入 http://www.mysonicwall.com。

> **附註：**特徵標記檔案只能用於註冊到之前下載特徵標記檔案所用 mysonicwall.com 帳戶的防火牆。

3 按一下 **下載**標題下的**下載特徵**。

4 在**特徵 ID：**旁邊的下拉視窗中，選擇您的防火牆的對應 SFID。

5 通過按一下**按一下此處下載特徵檔案**下載特徵庫更新檔案。

> **附註：**剩餘步驟可在斷開網際網路連接的環境下執行。

6 返回至防火牆管理介面的**安全服務 > 摘要**頁面。

7 按一下**匯入特徵標記**按鈕。

8 在出現的快顯對話方塊中，按一下**瀏覽**按鈕並導覽至特徵標記更新檔案的位置。

9 按一下**匯入**。防火牆啟用的安全服務已上載特徵庫。

8

設定內容篩選服務

附註：有線模式不支援內容篩選服務 (CFS) 許可。

您可以從**安全設定 | 安全服務 > 內容篩選**頁面啟用內容篩選物件和設定 SonicWall 內容篩選服務 (SonicWall CFS) 以及供應商內容篩選產品 Websense Enterprise。

主題：

- 關於 CFS
- 啟用 CFS
- 啟用本機 CFS 伺服器
- 設定 CFS 原則
- 設定 CFS 自訂類別

關於 CFS

SonicWall™ 內容篩選服務 (CFS) 提供教育機構、企業、圖書館和政府機構強制執行內容篩選。使用內容篩選物件，您可以在組織的防火牆後控制學生和員工使用他們經過 IT 處理的電腦時可存取的網站。

附註：如需 CFS 更詳細的說明以及如何授權和進行安裝，請參閱 *SonicWall SonicOS 6.5 版本須知*、*SonicWall™ 內容篩選服務功能*和 *SonicWall™ 內容篩選服務升級指南*。此外，有關如何為 CFS 原則建立內容篩選物件，請參閱 *SonicWall SonicOS 6.5 原則*。

CFS 會比較所要求的網站與包含數百萬筆評分的 URI、IP 位址和網站的大型雲端資料庫。也提供您工具建立和套用相關原則，以根據個別或群組身分識別或當天的時間允許或拒絕網站的存取。

主題：

-
- 關於 CFS 原則
- 關於內容篩選物件
- CFS 的工作原理

關於威脅 API

重要：設定威脅 API 之前，您必須啟用它。如需有關威脅 API 和如何啟用的更多資訊，請參閱*威脅 API 參考手冊*。

附註：SonicOS 威脅 API 要求防火牆具備內容篩選系統 (CFS) 授權。

SonicOS 6.5 支援威脅 API 功能。SonicOS 威脅 API 提供 API 存取給 SonicWall 防火牆服務。與目前的防火牆 GUI/CLI 使用者介面相比較，威脅 API 簡易且擅用標準 HTTP 通訊協定。透過傾向雲端部署，威脅 API 用起來可以比傳統的 SonicOS GUI/CLI 更簡易。

各種威脅可能源自 URL 或 IP 位址。這些威脅的清單可能很大而且頻繁變動。SonicOS 可能已經封鎖 URL 和 IP 位址的封鎖自訂清單，只是不方便，因為您必須登入並且手動更新清單。使用 API 介面會變得簡單多。

威脅清單已使用威脅 API 功能送出至 SonicOS。威脅可以下列任一格式新增：

- URLs (`https://malicious123.example.com/malware`)
- IP 位址 (`10.10.1.25`)

第三方可以產生威脅清單，使用威脅 API 將其傳送到防火牆。

若是威脅清單中的 IP 位址，SonicOS 最初會建立預設的威脅 API 位址群組，然後為威脅清單中的每一個 IP 位址建立位址物件 (AO)。您設定防火牆存取規則，其參照該位址群組並封鎖 IP 位址。

SonicOS 會新增 URL 到其 CFS 威脅 URI 清單。您會在關聯的 CFS 設定檔中啟用威脅 API 強制執行，並設定內容篩選系統 (CFS) 原則來封鎖威脅清單中的 URL。當威脅被 CFS 封鎖時，使用者會在其瀏覽器中看到封鎖訊息。

關於 CFS 原則

CFS 原則決定是否篩選封包 (透過套用設定的 CFS 操作) 或者僅是透過使用者允許。CFS 原則定義進行封包比較的篩選條件：

- 名稱
- 來源區域
- 目的地區域
- 來源位址
- 使用者/群組
- 排程

如果封包與所有這些定義的條件相符，則依據對應的 CFS 原則篩選封包，並且套用 CFS 操作。

附註：如果比對時使用者/群組的驗證資料無法使用，就不會比對此條件。此策略可預防效能問題，尤其是使用單一登入時。

每個 CFS 原則均有優先權層級並且會先檢查優先權較高者。

CFS 會在內部使用原則表來管理所有已設定的原則。對於每個原則要素，該表是由設定資料和執行階段資料構成。設定資料包括從使用者介面定義原則的參數，例如原則名稱、屬性和其他。執行階段資料包括用於處理封包的參數。

CFS 也使用原則查詢表來加速執行階段原則的查詢以比對條件：

- 來源區域
- 目的地區域
- IPv4 AO
- IPv6 AO

關於內容篩選物件

CFS 使用 CFS 原則中的「內容篩選物件」，識別要篩選的 URI 和網域，以及指定篩選時要進行的操作類型。如需內容篩選物件的更多資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

在 CFS 評分設計下，網域可解析至四個評分之一；優先順序從最高到最低的評分為：

1 封鎖
2 密碼
3 確認
4 BWM (頻寬管理)

如果 URL 未分類為這些評分之一，則允許操作。

CFS 的工作原理

1 封包抵達並由 CFS 進行檢查。
2 CFS 會對照設定的排除位址來進行檢查，如果發現相符就允許其通過。
3 CFS 會檢查其原則，並在封包中找出第一個符合下列條件的原則：
   - 來源區域
   - 目的地區域
   - 位址物件
   - 使用者/群組
   - 排程
   - 已啟用狀態
4 CFS 使用比對原則中定義的 CFS 設定檔來進行篩選，並為此封包傳回對應的操作。

   附註：如果沒有相符的原則，封包會通過而 CFS 沒有任何動作。

5 CFS 會執行比對原則的 CFS 操作物件中定義的操作。

關於 CFS 記錄

在**記錄和報告 | 記錄設定 > 基本設定**中，新的子類別**內容篩選**已經新增到**安全服務**類別。這些新的子類別列出這些記錄：

- CFS 警示
- 已存取的網站
- 已封鎖的網站

如需設定這些記錄的資訊，請參閱 *SonicWall SonicOS 6.5 記錄和報告*。

啟用 CFS

重要：在啟用 CFS 和設定 CFS 原則之前，如 *SonicWall SonicOS 6.5 原則*中所述設定您的內容篩選物件。

若要啟用 CFS：

1 導覽至**安全設定 | 安全服務 > 內容篩選**頁面。

2 從**內容篩選類型**下拉功能表中選擇內容篩選服務。

- **SonicWall CFS**（預設）
- **Websense Enterprise**

3 在**全域設定**區段中，指定可在**最大 URL 快取數 (項目)** 欄位中快取的最大 URL 項目數。預設為 **51200**。URL 評分會連同快取的 URL 項目一起儲存，以加速已知 URL 的處理。

4 若要為所有封包啟用內容篩選，請勾選**啟用內容篩選服務**核取方塊。預設情況下已核取此選項。若要為所有封包繞過內容篩選，請取消勾選此選項。

5 若要為 HTTPS 網站啟用內容篩選，請勾選**啟用 HTTPS 內容篩選**核取方塊。預設情況下未勾選此選項。

啟用此選項時，CFS 會依此順序執行 URL 評分查詢：

a 搜尋 CFS 用來取得 URL 評分的伺服器名稱的用戶端 `hello`。

b 如果伺服器名稱無法使用，請搜尋 CFS 用來取得 URL 評分的一般名稱的 SSL 憑證。

c 如果伺服器名稱或一般名稱都無法使用，CFS 會使用 IP 位址 來取得 URL 評分。

6 若要限制篩選時取得評分要求的時間，請勾選**當 CFS 伺服器無法使用時封鎖**核取方塊。預設情況下未勾選此選項。

a 選擇此選項時，將啟用**伺服器逾時**欄位。輸入 CFS 服務必須回應評分要求的最長時間（以秒為單位）。最小時長為 2 秒，最大時長為 10 秒，預設值為 **5** 秒。

7 若要為來自具有管理員權限的帳戶的所有要求，繞過內容篩選，請勾選**排除管理員**核取方塊。預設情況下已核取此選項。

8 若要為來自某類別的位址物件的所有要求，繞過內容篩選，請從**排除位址** 下拉功能表選擇位址物件。預設為**無**。您也可以透過選擇**建立新位址物件**來建立新的位址物件；如需建立位址物件的資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

9 按一下**接受**。

啟用本機 CFS 伺服器

本機 CFS 回應程式可讓內容篩選服務 (CFS) 直接透過本機回應程式 (而不是遠端公用回應程式) 接收 URL 評等。如需設定和使用本機 CFS 的相關資訊，請參閱 *《本機 CFS 管理指南》*。

若要啟用本機 CFS 回應程式:

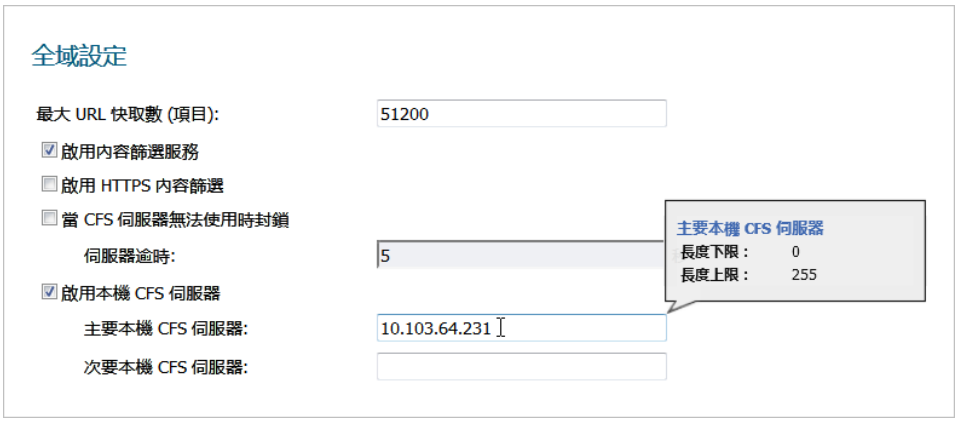
1 導覽至**安全設定 | 安全服務 > 內容篩選**頁面。

2 捲動到 **IPS 全域設定**部分。

3 選擇**啟用本機 CFS 伺服器**。

4 在**主要本機 CFS 伺服器**和 **次要本機 CFS 伺服器**欄位中輸入主要和次要本機 CFS 伺服器的 IP 位址。

5 將滑鼠懸停在**主要本機 CFS 伺服器**欄位右邊的**統計**圖示上， 將顯示所輸入伺服器的相關資訊。



6 按一下**接受**。

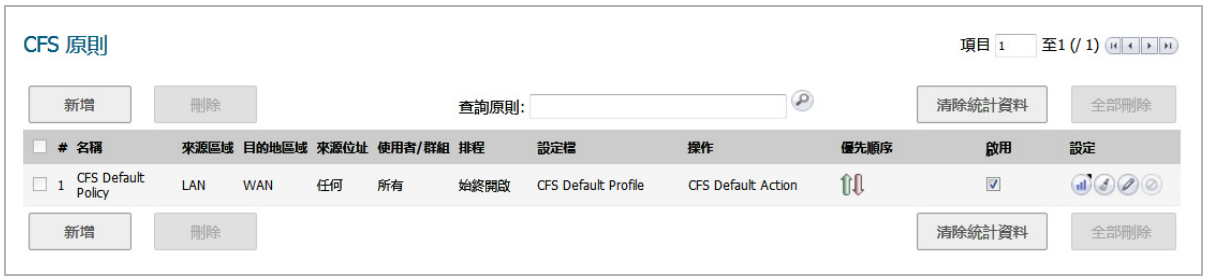
設定 CFS 原則

本節說明 CFS 原則表，並提供設定、編輯和刪除 CFS 原則的指示。

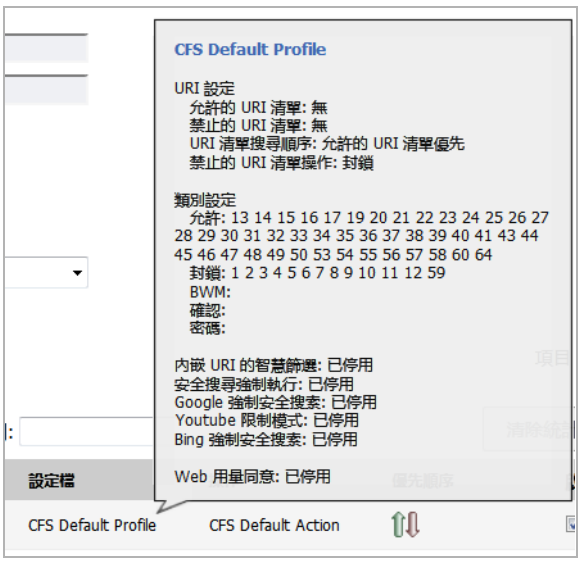
主題：

- 關於 CFS 原則表
- 設定 CFS 原則
- 編輯 CFS 原則
- 刪除 CFS 原則

關於 CFS 原則表



名稱	CFS 原則的名稱。
來源區域	CFS 原則的來源區域。
目的地區域	CFS 原則的目的地區域。
來源位址	CFS 原則的來源位址物件。
使用者/群組	CFS 原則套用的使用者或群組。
排程	CFS 原則生效的時間。
設定檔	CFS 設定檔物件是由 CFS 原則使用。將滑鼠停在 CFS 設定檔物件名稱上，會顯示 CFS 設定檔的細節：



操作

CFS 操作物件是由 CFS 原則使用。將滑鼠停在 CFS 操作物件名稱上，會顯示 CFS 操作的細節：

優先順序

按下 CFS 原則的優先順序，會顯示**變更原則優先權**快顯示功能表：

CFS 原則的優先順序會顯示在**從**之後。您可以透過在**至**欄位中輸入來變更優先順序。最高優先順序是 1；0 是最低優先順序。

啟用

若要啟用 CFS 原則，請勾選其核取方塊。預設會啟用原則，即 **CFS 預設原則**。

設定

為每個原則顯示這些圖示。

- **統計資料**；將滑鼠停在此圖示上會顯示**原則統計資料**快顯對話方塊。

- **清除統計**；按下此圖示 (掃帚) 會清除 CFS 原則的所有統計資料。將顯示確認對話方塊。

- **編輯**: 按下此圖示會顯示**編輯 CFS 原則**對話方塊。
- **刪除**: 按下此圖示會刪除 CFS 原則。將顯示確認對話方塊。

按一下**確定**。

附註：預設 CFS 原則即 **CFS 預設原則**無法刪除且圖示為灰顯。

您可以按下原則表下的連結或導覽至**防火牆 > 內容篩選物件**頁，存取所有 CFS 物件。

搜尋 CFS 原則表

您可以下列方式搜尋長表格中的特定 IP 位址：

1 在**依位址查詢原則**欄位中輸入 IP 位址。IP 位址可以使用以下任一格式：

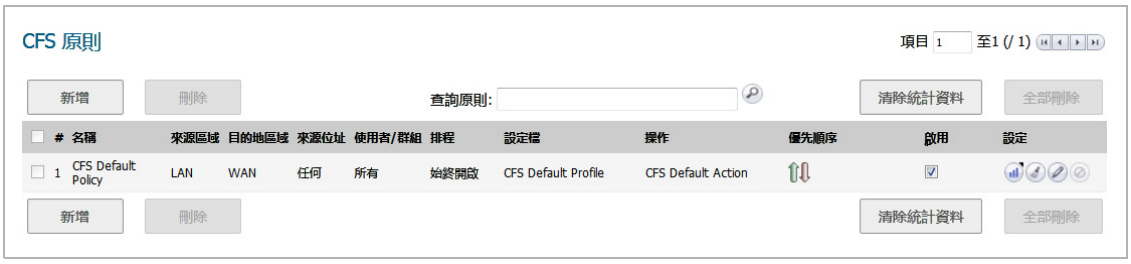
- 192.168.168.168
- fe80::c2ea:e4ff:fe59:a634

2 按一下**搜尋**（放大鏡）圖示。

設定 CFS 原則

若要設定 CFS 原則：

1 導覽至**安全設定 | 安全服務 > 內容篩選 | CFS 原則**頁面。



2 按下**新增**。隨即顯示 **CFS 原則**對話方塊。

3 在**名稱**欄位中，為新原則輸入易記的名稱。

4 從**來源區域**下拉功能表，選擇一個區域。

5 從**目的地區域**下拉功能表，選擇一個區域。

6 從**來源位址**下拉功能表，選擇一個位址。預設值為**任何**。您也可以透過選擇**建立新位址**來建立新的位址物件；如需建立位址物件的資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

7 從**使用者/群組**下拉功能表中，選擇套用原則的使用者或群組。預設值為**全部**。

8 從**排程**下拉功能表，選擇原則何時生效。預設值為**始終開啟**。您也可以透過選擇**建立新的排程**來建立自訂排程；如需建立排程的資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

9 從**設定檔**下拉列表中，選擇 CFS 設定檔物件。您也可以透過選擇**建立新的設定檔**來建立新的 CFS 設定檔物件；如需建立 CFS 設定檔物件的資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

10 從**操作**下拉列表中，選擇 CFS 操作物件。您也可以透過選擇**建立新的操作**來建立新的 CFS 操作物件；如需建立 CFS 操作物件的資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

11 按下**新增**。

12 若要建立更多 CFS 原則，請對每個原則重複步驟 3 到步驟 11。

13 按一下**關閉**。

編輯 CFS 原則

若要編輯 CFS 原則：

1 為要編輯的 CFS 編輯，按一下**編輯**圖示。隨即顯示 **CFS 原則**對話方塊。

附註：您無法編輯預設原則，即 **CFS 預設原則**。其**編輯**圖示會呈灰顯。

2 若要進行您的變更，請遵循設定 CFS 原則中的適當程序。

刪除 CFS 原則

若要刪除 CFS 原則：

1 執行以下其中一項操作：

- 為要刪除的 CFS 原則，按一下**刪除**圖示。

  附註：您無法刪除預設原則，即 **CFS 預設原則**。其**刪除**圖示會呈灰顯。

- 按下要刪除的一個或多個 CFS 原則的核取方塊。**刪除**按鈕隨即啟用，然後按一下。

若要刪除所有 CFS 原則：

1 按一下**全部刪除**按鈕。所有 CFS 原則會刪除，預設原則 **CFS 預設原則**除外。

設定 CFS 自訂類別

本節說明 CFS 自訂類別表，並提供設定、編輯和刪除 CFS 自訂類別的指示。也說明自訂類別表的匯入和匯出。

主題：

- 關於 CFS 自訂類別表
- 設定 CFS 自訂類別
- 匯出 CFS 自訂類別表
- 匯入 CFS 自訂類別表
- 編輯 CFS 自訂類別
- 刪除 CFS 自訂類別

關於 CFS 自訂類別表

網域 要套用自訂類別的網域的 IP 位址。

類別 從自訂類別選擇的類別。

設定 顯示每個網域的「編輯」和「刪除」圖示。

搜尋 CFS 自訂類別表

您可以下列方式搜尋長表格中的特定 IP 位址：

1 在依位址查詢原則欄位中輸入 IP 位址。IP 位址可以使用以下任一格式：

- `192.168.168.168`
- `fe80::c2ea:e4ff:fe59:a634`

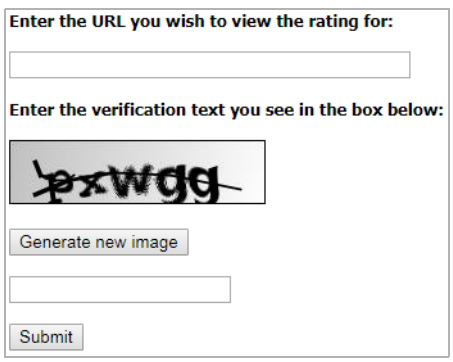
2 按一下**搜尋**（放大鏡）圖示。

請求評等檢查

如果您認為網站的評分不正確，或者想要提交新的 URL，請利用下列方式提交您的要求至 SonicWall 內容篩選服務：

- 按下**安全服務 > 內容篩選**頁面上方的連結；如果您認為某網站評等不正確或希望提交新的 URL，請按一下此處。
- 移至 http://cfssupport.sonicwall.com/Support/web/eng/newui/viewRating.jsp。

即顯示 **CFS URI 評等檢查請求**表單。



設定 CFS 自訂類別

您可以自訂特定 URL 的評等。最多支援 5,000 個有效項目。自訂類別的處理和後端伺服器所提供類別的處理類似。當 CFS 檢查 URL 的評分時，它會先檢查使用者評分，然後檢查後端伺服器的評分。CFS 類別的管理和建立是動態使用從後端伺服器傳來的設定字串。

主題：

- 啟用自訂類別
- 設定自訂類別

啟用自訂類別

您必須先啟用服務，才能使用自訂類別。

若要啟用自訂類別：

1 導覽至**安全設定 | 安全服務 > 內容篩選 | CFS 自訂類別**。

2 勾選**啟用 CFS 自訂類別**核取方塊。預設情況下未勾選此選項。

3 按一下**接受**。

設定自訂類別

若要定義自訂類別：

1 導覽至**安全設定 | 安全服務 > 內容篩選 | CFS 自訂類別**。

2 按下**新增**。此時會顯示 **CFS 自定義類別**對話方塊。

3 在**網域**欄位中，輸入套用自訂類別的網域的 IP 位址或網域名稱：

- IP 位址可以使用以下任一格式：
  - `192.168.168.168`
  - `fe80::c2ea:e4ff:fe59:a634`
- 網域名稱可省略 `www.` 首碼。如果有包含，會顯示確認訊息；當您按下**確定**，首碼會從**網域**欄位的網域名稱移除：

4 從清單選擇至多四個類別。

5 按下**新增**。

6 若要建立更多 CFS 自訂類別，請對每個原則重複步驟 3 到步驟 5。

> **附註：**您建立的每個自訂類別在 **CFS 自訂類別**表中是獨立項目；它們不是串連的。

7 按一下**關閉**。**CFS 自訂類別**表會更新。

匯出 CFS 自訂類別表

您可將 **CFS 自訂類別**表匯出到您可以進行編輯和儲存以備匯入的 `.wri` 檔案。

若要匯出 CFS 自訂類別表：

1 導覽至**安全設定 | 安全服務 > 內容篩選 | CFS 自訂類別**。

2 按一下**匯出**。將顯示**開啟 cfsCustomCategoryData.wri** 對話方塊。

3 您可以開啟檔案 (預設程式為記事本) 或儲存檔案。如果您：

- 開啟檔案。
- 儲存檔案，該檔案會下載到您的 Downloads 資料夾，檔名為 `cfsCustomCaegoryData.wri`；新行字元會新增到每個項目後。

附註：該檔案包括所有 **CFS 自訂類別**表的項目，全都在一行上。

4 按一下**確定**。

匯入 CFS 自訂類別表

您可以匯入含有 CFS 自訂類別表項目的檔案。此檔中的項目會覆寫表格中的現有項目。

檔案應包含此格式的項目：

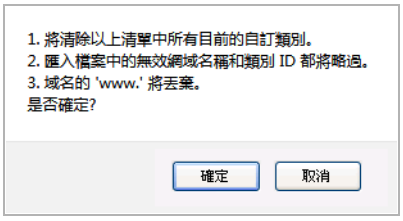
`DomainName/IPAddress: Rating1[, Rating2[, Rating3[, Rating4]]] Separator`

Token	定義
DomainName	網域名稱，例如 SonicWall。如果包含首碼 `www.`，則會忽略。
IPAddress	標準或 IPv6 IP 位址，例如： • `192.168.168.168` • `fe80::c2ea:e4ff:fe59:a634`
評等	從 1-255 的類別評等，如 **Add CFS 自訂類別**對話方塊中所示。您每個類別至多可指定 4 個評分。
分隔符號	歸位字元或新行分隔符號： 分隔符號 / 樣式 `\r\n` — Windows 樣式，新行分隔符號 `\n` — UNIX 樣式，新行分隔符號 `\r` — MAC OS 樣式，新行分隔符號

若要匯入自訂類別表：

1 導覽至**安全設定 | 安全服務 > 內容篩選 | CFS 自訂類別**。

2 按一下**匯入**。將顯示確認對話方塊。



CFS 自訂類別表中所有目前的項目會被檔案中的項目取代。您要保留的任何項目應在此檔案中。

提示：匯出 CFS 自訂類別表並對匯出的檔案進行變更，之後再匯入表格項目。

3 按一下**確定**。

編輯 CFS 自訂類別

若要編輯 CFS 自訂類別：

1 為要編輯的 CFS 自訂類別，按一下**編輯**圖示。此時會顯示 **CFS 自定義類別**對話方塊。

2 若要進行您的變更，請遵循設定 CFS 自訂類別中的適當程序。

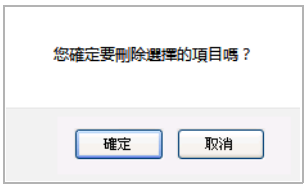
刪除 CFS 自訂類別

若要刪除 CFS 自訂類別：

1 執行以下其中一項操作：

- 為要刪除的 CFS 自訂類別，按一下**刪除**圖示。
- 按下要刪除的一個或多個 CFS 自訂類別的核取方塊。**刪除**按鈕隨即啟用，然後按一下。

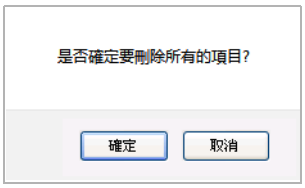
將顯示確認訊息。



2 按一下**確定**。

若要刪除所有 CFS 自訂類別：

1 按一下**全部刪除**按鈕。



2 按一下**確定**。所有 CFS 自訂類別會刪除。

9

啟用 SonicWall 用戶端防毒

防毒產品的性質決定了其通常需要在每台 PC 上進行定期、有效維護。當發現新病毒時，在組織中部署的全部防毒軟體都必須使用最新的病毒定義檔案進行更新。不這樣做會嚴重限制防毒軟體的有效性和干擾正常工作時間。已知病毒超過 50000 種，而且會定期爆發新病毒，維護和更新病毒防護的任務可能變得很繁重。然而，很多中小型企業沒有足夠的 IT 人力維護防毒軟體。因此產生的病毒防禦缺口可能導致資料遺失和員工生產率降低。

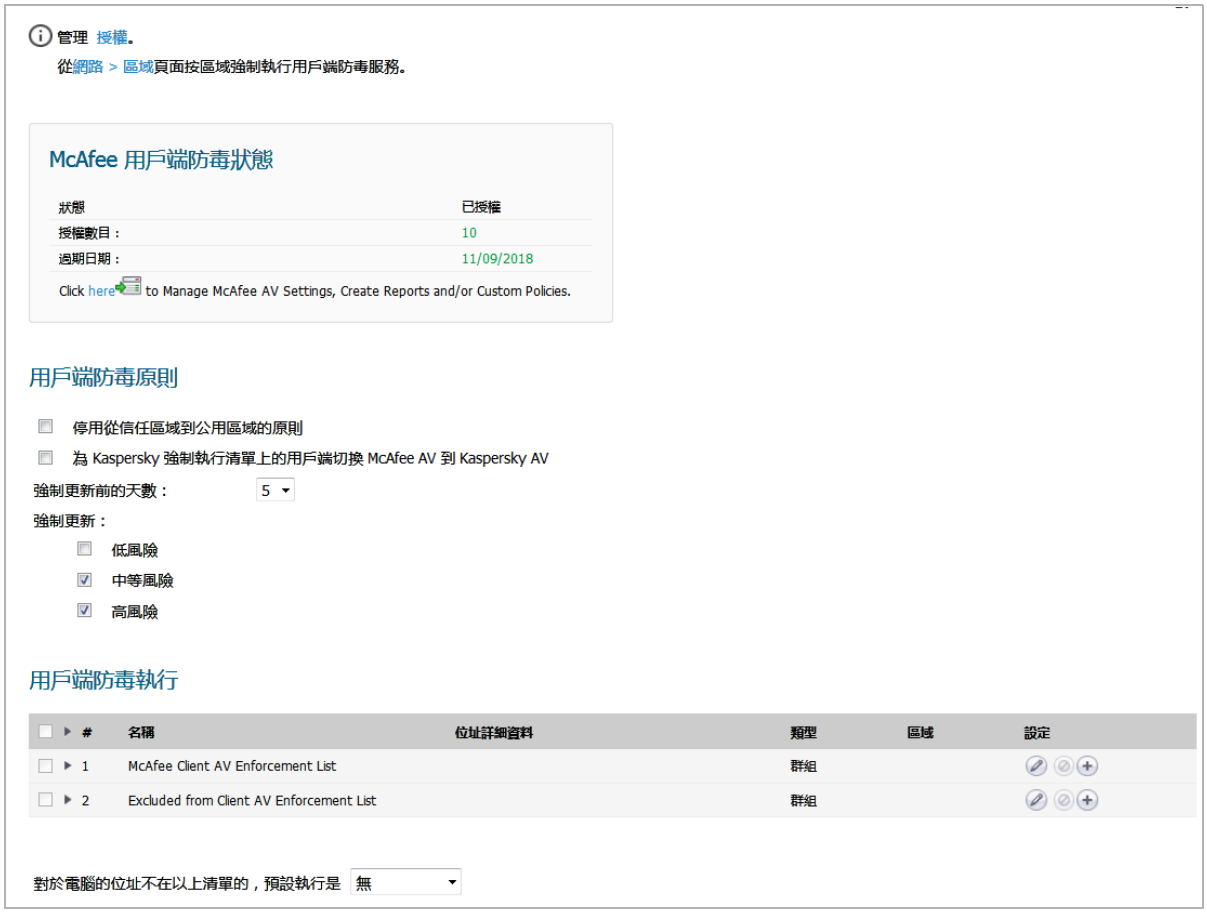
NIMDA 和「紅色警戒」等病毒的肆虐正顯示出中小型企業的病毒防禦問題。使用者如果沒有最新的病毒定義檔案，這些病毒就會增殖並感染很多其他使用者和網路。SonicWall 用戶端防毒可以防止這些情況，並提供新的病毒防護方法。SonicOS 持續監控病毒定義檔案的版本，並自動觸發向各使用者電腦下載和安裝新病毒定義檔案。此外，防火牆會在恢復對網際網路的防護前限制各使用者的存取，因此充當公司病毒防護原則的執行者。這種新方法可以確保在網路上的各 PC 上安裝和啟用最新版的病毒定義檔案，防止懶散的使用者停用病毒防護並使整個組織處於潛在的病毒爆發危險中。

附註：您必須購買防毒訂閱才能通過防火牆管理介面實施防毒。

SonicOS 支援 McAfee 和 Kaspersky 用戶端防毒的用戶端 AV 強制實施。這些服務分別授權，用於為部署購買所需的每個授權號碼。

設定用戶端防毒服務

如需啟用網路防毒服務的資訊，請參見啟用閘道防毒、防間諜軟體和 IPS 授權。



主題：

- 用戶端防毒狀態
- 用戶端防毒原則
- 防毒實施

用戶端防毒狀態

用戶端防毒狀態部分：

- 顯示有關防火牆是否已授權、授權數量和授權到期日期的資訊。
- 包含登入 MySonicWall 的連結，以管理和檢閱詳細的系統和網路資訊。按一下此連結，顯示 MySonicWall 登入的**授權 > 授權管理**頁面。
- 包含連到**網路 > 區域**頁面的連結，以按照區域設定用戶端防毒。

用戶端防毒原則

用戶端防毒原則部分提供以下功能：

- **停用從信任區域到公用區域的原則** - 如取消選擇，此選項在位於受信任區域中的電腦上實施防毒原則。勾選此選項則允許受信任區域（例如 LAN）中的電腦存取公用區域（例如 DMZ）中的電腦，即使 LAN 電腦上未安裝防毒軟體。
- **為 Kaspersky 強制執行清單上的用戶端切換 McAfee AV 到 Kaspersky AV** - 勾選此選項後，可以使用 Kaspersky AV 代替 McAfee AV 用於 Kaspersky 強制實施清單上的用戶端。
- **強制更新之前的天數** - 此功能定義在 SonicWall 要求下載最新病毒日期檔案之前，可以存取網際網路的最多天數。從 0 到 5 天中進行選擇：**5** 是預設值。
- **強制更新警示** - SonicWall 向擁有防毒訂閱的所有 SonicWall 裝置傳送病毒警示。有三個級別的警示，您可以選擇多個。在勾選此選項的情況下收到警示時，使用者會升級到最新版 VirusScan ASaP，然後才能存取網際網路。此選項替代「在強制更新前允許的最多天數」選擇。此外，每記錄一個病毒警示，都會向管理員傳送警示訊息。
    - **低風險** - 欄位中未報告且認為以後很難在欄位中發現的病毒都具有低風險。即使此類病毒包括極嚴重或不可預見的損害性承載，其風險仍然較低。預設情況下未勾選此選項。
    - **中等風險** - 如果欄位中發現了病毒，且病毒使用了不常見的感染機制，則視之為中等風險。如果其流行性較低且有效承載不嚴重，可將其降級為低風險。同樣，如果病毒傳播越來越廣，則可將其升級為高風險。預設情況下已核取此選項。
    - **高風險** - 要指派為高風險分級，必須在欄位中頻繁報告此病毒。此外，有效承載必須能夠導致至少部分嚴重損害。如果它導致極嚴重或不可預見的損害，即使流行級別較低，也可指派高風險。預設情況下已核取此選項。

防毒實施

用戶端防毒執行表含有兩個項目，均具備**群組類型**：

- ***供應商*用戶端防毒的實施清單** (其中***供應商***是 **McAfee** 或 **Kaspersky**，取決於您使用何者)
- **從用戶端防毒的實施清單排除**

若要查看與每個項目關聯的 IP 位址，請按一下**展開**圖示。每個項目的**位址詳細資料**、**類型**和**區域**會顯示。如果沒有設定執行清單，按一下**展開**圖示會顯示**無項目**。

若要隱藏 IP 位址，按一下**折疊**圖示。

您可以編輯或新增至此兩個項目，但是無法刪除它們。

主題：

- 建立用戶端防毒的實施清單
- 從用戶端防毒的實施清單排除位址物件
- 保護不在任一執行清單中的電腦

建立用戶端防毒的實施清單

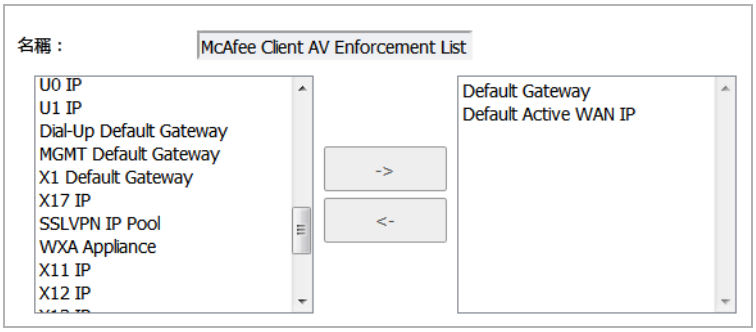
附註：預先定義的位址物件，例如介面 IP 或預設閘道，無法個別編輯或刪除；它們的**編輯**和**刪除**圖示呈灰顯狀態。您可透過編輯清單本身，從**用戶端防毒的實施清單**移除預先定義的位址物件。不過，您可以編輯或刪除任何已經定義的位址物件。

您需要使用已強制實施用戶端防毒的位址物件的 IP 位址，設定用戶端防毒的實施清單。

您可以透過建立包含 IP 位址範圍的位址物件，來定義 IP 位址的範圍，以接收防毒實施。需要實施防毒的電腦都需要擁有指定 IP 位址範圍內的固定 IP 位址。最多可以輸入 64 個 IP 位址範圍用於防毒實施。

若要從現有的位址物件建立用戶端防毒的實施清單：

1. 導覽至**安全設定 | 安全服務 > 用戶端防毒的實施**頁面。
2. 捲動到**用戶端防毒執行**部分。
3. 按一下***供應商*用戶端防毒的實施清單**的**編輯**圖示。隨即顯示**編輯位址物件群組**對話方塊。



4 從左側的清單中選擇需要用戶端防毒執行的 IP 位址。

5 按一下**右箭頭**按鈕將項目移動到右側的清單。

6 完成新增位址物件後，按一下**確定**。

若要新增位址物件到「用戶端防毒的實施清單」：

1 導覽至**安全設定 | 安全服務 > 用戶端防毒的實施**頁面。

2 捲動到**用戶端防毒執行**部分。

3 按一下*供應商***用戶端防毒的實施清單**的**新增**圖示。此時會顯示**新增位址物件**對話方塊。

4 在**名稱**欄位中輸入易記的名稱。

5 從**區域指派**下拉功能表中選擇區域。

6 從**類型**下拉功能表選擇類型。

7 在 **IP 位址**欄位，輸入位址物件的 IP 位址。

8 按一下**確定**。

從用戶端防毒的實施清單排除位址物件

SonicWall 用戶端防毒目前支援 Windows 平台。為了能存取網際網路，使用其他操作系統的電腦必須不受防毒原則控制。

△ **注意：為了確保為網路提供完整的病毒攻擊防護，推薦只有伺服器和不受支援的機器才能不受防護，且在將任何機器從防毒實施中排除時應在此機器上安裝供應商防毒軟體。**

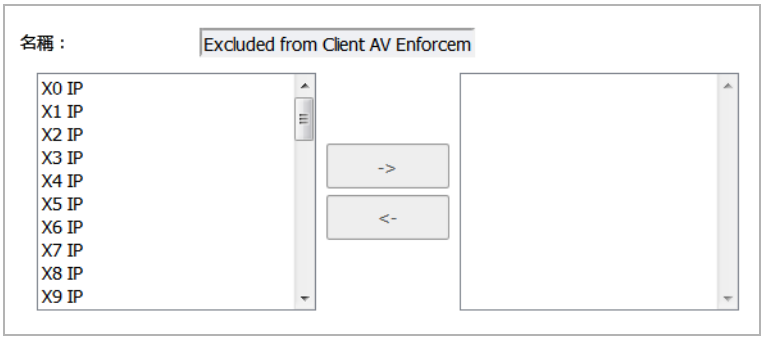
ⓘ **附註：**預先定義的位址物件，例如介面 IP 或預設閘道，無法個別編輯或刪除；它們的**編輯**和**刪除**圖示呈灰顯狀態。您可透過編輯清單本身，從**從用戶端防毒的實施清單排除**移除預先定義的位址物件。不過，您可以編輯或刪除任何已經定義的位址物件。

若要定義排除的位址物件：

1 導覽至**安全設定 | 安全服務 > 用戶端防毒的實施**頁面。

2 捲動到**用戶端防毒執行**部分。

3 按一下**從用戶端防毒的實施清單排除**的**編輯**圖示。隨即顯示**編輯位址物件群組**。



4 從左側的清單中選擇要排除的位址物件。

5 按一下**右箭頭**將物件移動到右側的清單。

6 完成排除位址物件後，按一下**確定**。

若要新增位址物件到「排除的用戶端防毒的實施清單」：

1 導覽至**安全設定 | 安全服務 > 用戶端防毒的實施**頁面。

2 捲動到**用戶端防毒執行**部分。

3 按一下**從用戶端防毒的實施清單排除**的**新增**圖示。此時會顯示**新增位址物件**對話方塊。

4 在**名稱**欄位中輸入易記的名稱。

5 從**區域指派**下拉功能表中選擇區域。

6 從**類型**下拉功能表選擇類型。

7 在 **IP 位址**欄位，輸入位址物件的 IP 位址。

8 按一下**確定**。

若要新增位址物件到「從用戶端防毒的實施清單排除」：

1 捲動到**用戶端防毒執行**部分。

2 按一下**從用戶端防毒的實施清單排除**的**新增**圖示。此時會顯示**新增位址物件**對話方塊。

3 在**名稱**欄位中輸入易記的名稱。

4 從**區域指派**下拉功能表中選擇區域。

5 從**類型**下拉功能表選擇類型。

6 在 **IP 位址**欄位，輸入位址物件的 IP 位址。

7 按一下**確定**。

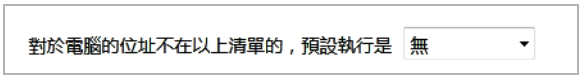
保護不在任一執行清單中的電腦

對於未包含在任一執行清單中的電腦，您可以指定要套用到它們的預設執行類型。

若要指定預設執行到不在執行清單的電腦：

1 捲動到**用戶端防毒執行**部分。

2 捲動到**安全服務 > 用戶端防毒的實施**頁面底部。



3 從**對於電腦的位址不在以上清單的，預設執行是**下拉功能表選擇預設執行的類型。

- **無**（預設值）
- 供應商防毒方案 (McAfee 或 Kaspersky，取決於您的系統)

10

設定用戶端 CF 執行

SonicWall 用戶端 CF 執行用於為企業、學校和圖書館和政府機構實施防護和提效原則。SonicWall 建立了革命性的內容篩選體系結構，使用可擴充的動態資料庫來封鎖受禁止和低效率的 Web 內容。

用戶端 CF 執行提供了控制性與靈活性的理想組合，可確保實現最進階別的防護和生產力。用戶端 CF 執行可防止個別使用者存取不當內容，同時減少組織的責任並提高效率。網站將根據所包含的內容類型獲得評級。內容篩選服務 (CFS) 可基於網站的評級以及使用者或群組的原則設定來封鎖或允許存取這些網站。

企業往往可通過在裝置上設定篩選原則，來控制在安全裝置的週圍進行瀏覽而產生的 Web 衝浪行為及內容。但是，當同一裝置不處於防火牆週圍時，就會對其失去控制。用戶端 CF 執行通過在安全裝置周圍以外封鎖受禁止和低效率的 Web 內容，填補了這一缺口。

SonicWall 安全裝置與用戶端 CF 執行配合使用，可以自動和一致的方式確保所有終端獲得最新的軟體更新，從而實現終極網路防護。此用戶端可配合 Windows 和 Mac PC 使用。

用戶端 CF 執行包含下列三個主要元件：

- 執行 SonicOS 的網路安全裝置，它的作用是促進和驗證 CFS 許可，啟用或停用實施，以及設定排除和其他設定。
- 在未安裝用戶端軟體的情況下，封鎖任何試圖存取網際網路的用戶端存取網站（直至安裝好用戶端軟體），且自動觸發安裝用戶端 CF 執行。
- 使用基於雲端的 EPRS 伺服器管理用戶端原則和用戶端組。此伺服器可通過 MySonicWall 或在裝置上執行的 SonicOS 進行存取。

主題：

- 啟用和設定用戶端 CF 執行
- 在網路區域中啟用用戶端 CFS

啟用和設定用戶端 CF 執行

本章節介紹如何在 SonicOS 中啟用和設定用戶端 CF 執行的設定。

若要向使用者顯示網站封鎖頁面，從而提示使用者安裝用戶端 CF 執行，必須先在 SonicWall 裝置上啟用用戶端 CF 執行。

附註：如果還未在 MySonicWall 上啟用內容篩選用戶端 (CFS)，則必須先將其啟用，才能在用戶端系統上實施用戶端內容篩選原則。

在安全服務中設定用戶端 CF 執行

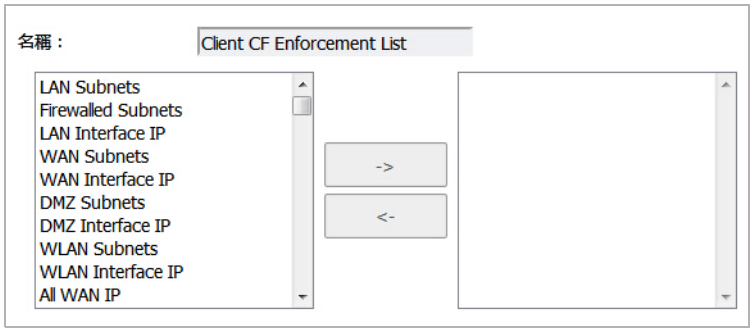
若要設定用戶端 CF 執行的設定值：

1 導覽至**安全設定 | 安全服務 > 用戶端 CF 執行**頁面。

2 在**用戶端 CF 執行原則**區段下面，從 **Grace 週期**下拉清單中選擇 CFS 實施原則保持有效的天數。

用戶端 CF 執行清單區段包含一張表格，其中包括「用戶端 CFS 實施」清單和「從用戶端 CF 執行中排除」清單。

若要設定任一表格，請按一下您希望設定的清單對應的**設定**圖示。隨即顯示編輯位址物件群組對話方塊。從可用清單中選擇要包括/不包括在群組中的值。



3 對於**用戶端 CF 執行清單**和**從用戶端 CF 執行中排除清單**。如果您在這些清單中新增了任何項目，您可以按一下清單標題旁邊的箭頭顯示這些項目。若要向任一清單中新增項目，請按一下此行中的「設定」圖示。

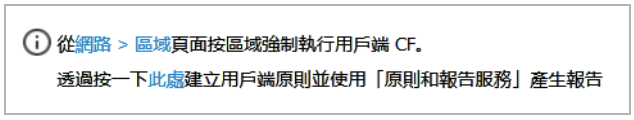
4 在標記對於電腦的位址不在以上清單的，預設執行是的欄位中，從下拉清單中選擇**用戶端 CF 執行**。此欄位位於**用戶端 CF 執行清單**區段下面。選擇此選項將提示通過此裝置連接到網際網路的其他所有電腦安裝已實施的用戶端。如果您只想在您所設定的電腦上實施此服務，您可以從下拉清單中選擇**無**。

5 按一下**接受**。

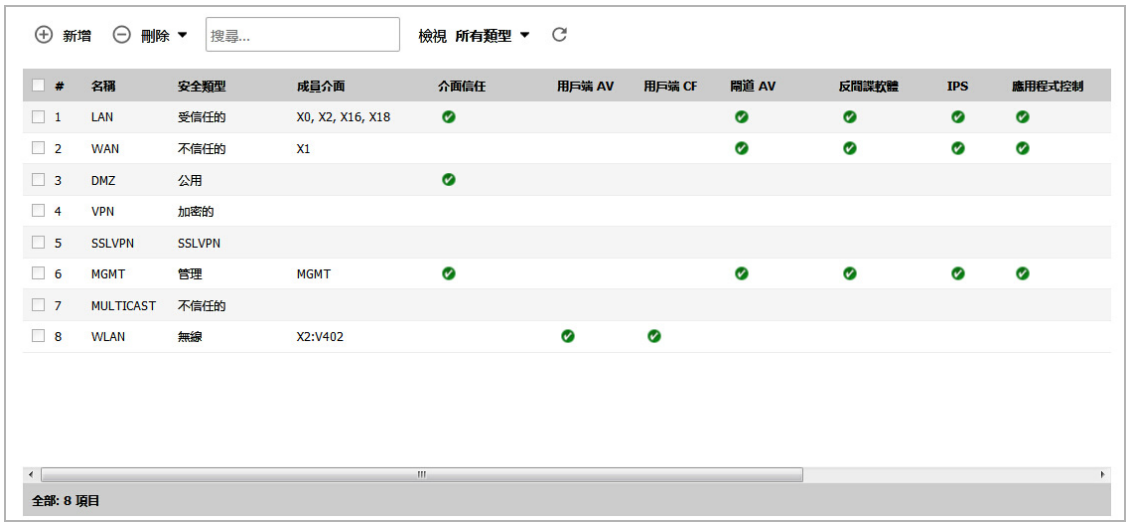
在網路區域中啟用用戶端 CFS

可通過執行下列步驟按區域實施用戶端內容篩選：

1 在**安全服務 > 用戶端 CF 執行**頁面的上方，按一下**備註**中的**網路 > 區域**連結。



隨即顯示**網路 > 區域**頁面。



2 按一下您想要在其中實施用戶端內容篩選服務的區域對應的**設定**按鈕。隨即顯示**新增區域**對話方塊。

3 勾選**啟用用戶端內容篩選服務**核取方塊。

4 按一下**確定**。

11

管理 SonicWall 閘道防毒服務

SonicWall 閘道防毒 (GAV) 通過使用 SonicWall 的 IPS 深度封包偵測 v2.0 引擎檢查通過 SonicWall 閘道的所有流量，直接在 SonicWall 安全裝置上提供即時病毒防護。SonicWall GAV 建立在 SonicWall 的免重組結構之上，可用於檢查多個應用程式通訊協定，以及一般 TCP 串流和壓縮流量。由於 SonicWall GAV 不執行重組，因此沒有掃描引擎所施加的檔案大小限制。Base64 解碼、ZIP、LHZ 和 GZIP (LZ77) 解壓縮也使用單次傳遞和按封包的方式執行。

SonicWall GAV 根據廣泛、動態更新的威脅病毒特徵，比對下載的檔案或通過電子郵件傳送的檔案，來提供威脅防護。在傳送到桌面之前就截獲和抑制病毒攻擊。SonicWall 的 SonicAlert 團隊、供應商病毒分析員、開源開發員和其他人員共同建立新特徵，並將其新增到資料庫。

可以設定 SonicWall GAV 提供針對內部威脅和網路外部威脅的防禦。它採用 SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、即時訊息和對等應用程式等多種通訊協定和基於串流的其他一些通訊協定，為您提供全面的網路威脅防護和控制。由於還可以壓縮包含惡意代碼和病毒的檔案，因而一般防毒解決方案無法存取，SonicWall GAV 採用了進階解壓縮技術，能夠按封包自動解壓縮和掃描檔案。

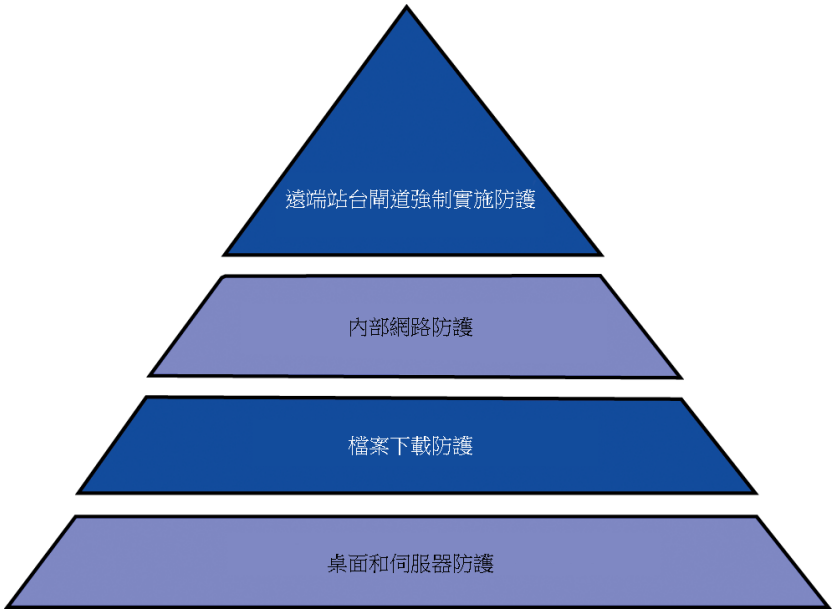
主題：

- SonicWall GAV 多層方法
- SonicWall GAV 結構
- 啟用閘道防毒、防間諜軟體和 IPS 授權
- 設定 SonicWall 閘道防毒防護
- 查看 SonicWall GAV 特徵

SonicWall GAV 多層方法

SonicWall GAV 為桌面、網路和遠端站台的網路提供全面的多層防毒防護。請參見 SonicWall GAV 多層方法。SonicWall GAV 在閘道實施防毒，以確保所有使用者有網路上的最新更新和監控檔案。

SonicWall GAV 多層方法

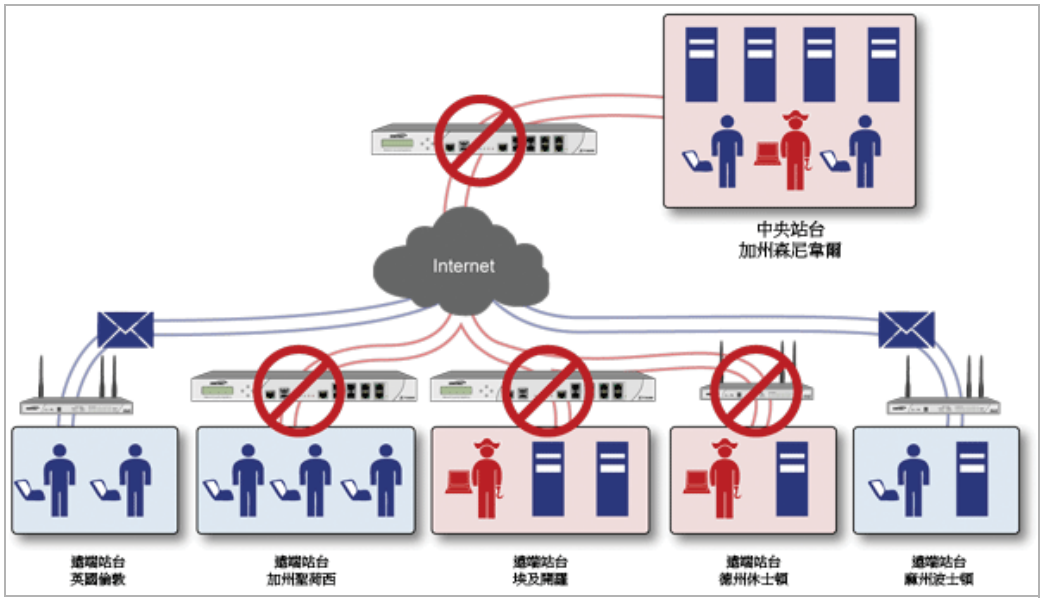


主題：

- 遠端站台防護
- 內部網路防護
- HTTP 檔案下載
- 伺服器防護
- 雲端防毒資料庫

遠端站台防護

遠端站台防護



1 使用者在遠端站台和公司辦公室之間傳送典型的電子郵件和檔案。

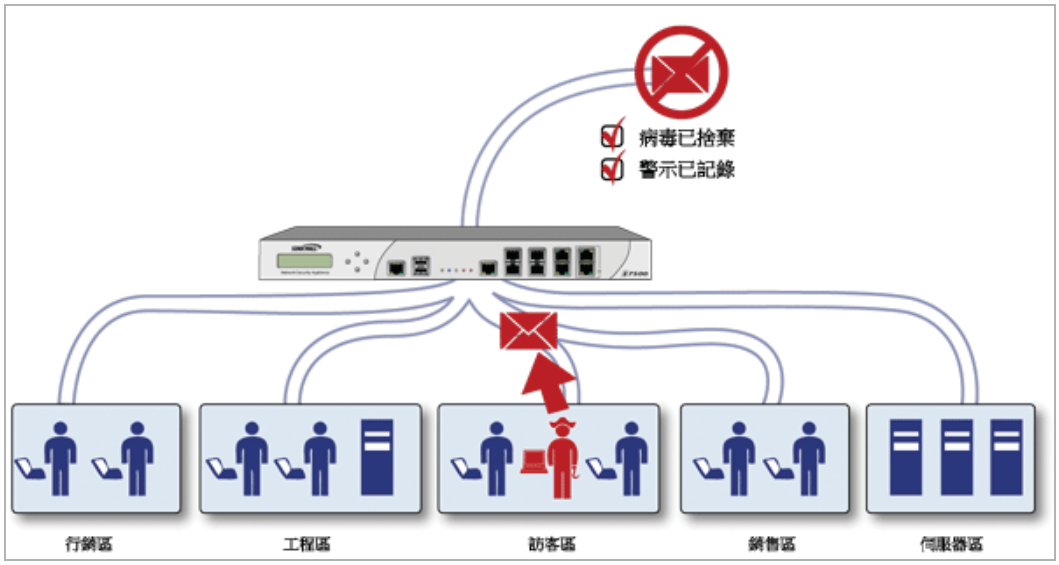
2 SonicWall GAV 會在 SonicWall 安全裝置上掃描和分析檔案和電子郵件。

3 在感染遠端桌面前，發現和封鎖病毒。

4 記錄病毒，並向管理員傳送警示。

內部網路防護

內部網路防護



1 內部使用者會感染病毒並在內部釋放。

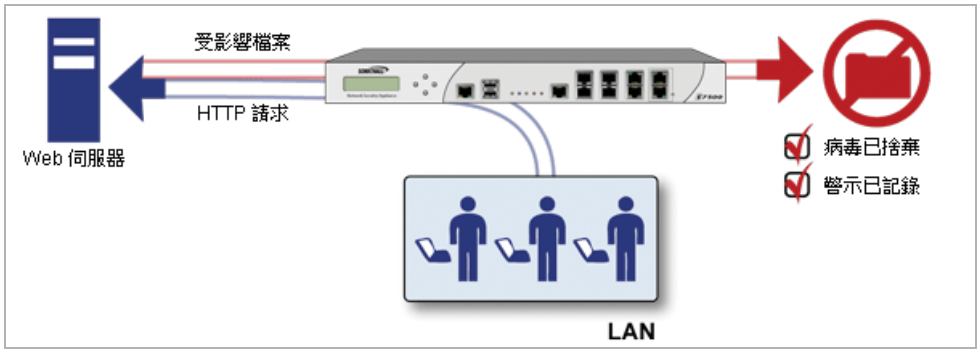
2 在其他網路使用者接收所有檔案前，都會在閘道處進行掃描。

3 如果發現病毒，檔案將丟棄。

4 記錄病毒，並向管理員傳送警示。

HTTP 檔案下載

HTTP 檔案下載



1 用戶端請求從網路下載檔案。

2 通過網際網路下載檔案。

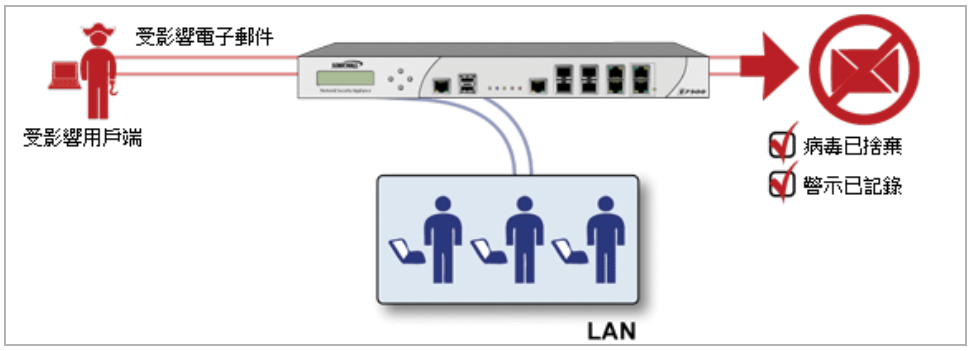
3 SonicWall GAV 引擎會分析檔案，查找惡意代碼和病毒。

4 如果發現病毒，檔案 8is 將丟棄。

5 記錄病毒，並向管理員傳送警示。

伺服器防護

伺服器防護



1 外部使用者發來一封電子郵件。

2 在電子郵件伺服器接收電子郵件前，會經過 SonicWall GAV 引擎分析，查找惡意代碼和病毒。

3 如果發現病毒，將封鎖威脅。

4 電子郵件返回至發件人，記錄病毒且警示傳送至管理員。

雲端防毒資料庫

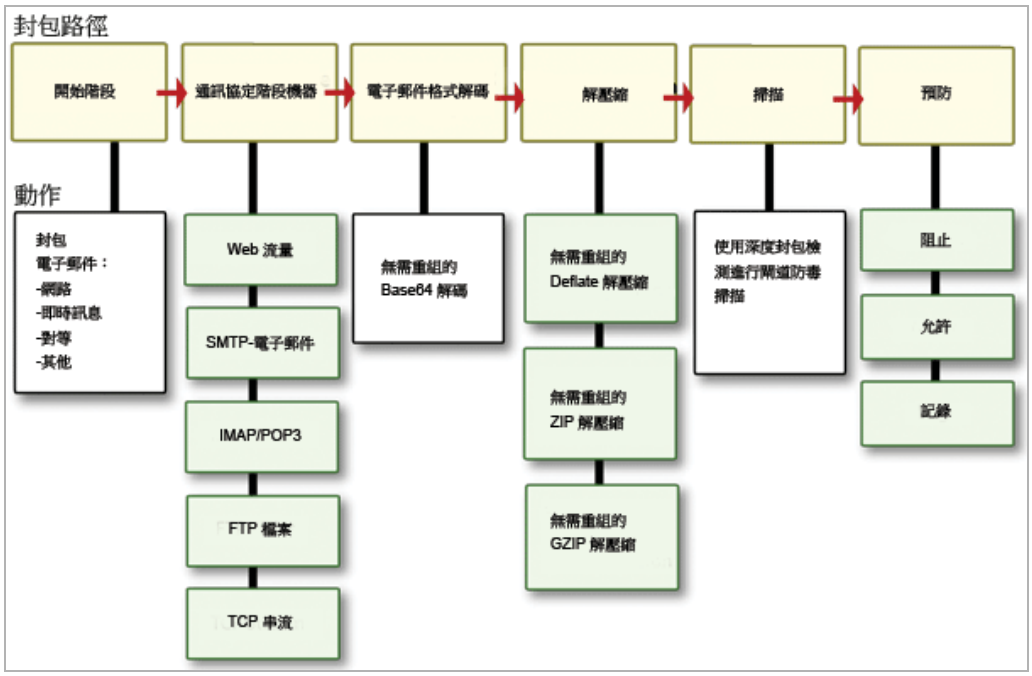
雲端閘道防毒功能引入了進階惡意軟體掃描解決方案，因而補充和擴充了 SonicWall 防火牆上現有的閘道防毒掃描機制，以抵禦外部世界持續增長的惡意軟體。

雲端閘道防毒通過諮詢基於資料中心的惡意軟體分析伺服器擴充了免重組深度封包偵測引擎。這種方法提供能掃描目前受支援的所有通訊協定上不限數量和大小的檔案的低延遲、即時解決方案，且不顯著增加裝置的處理開銷，因為保留了基於 RFDPI 的惡意軟體偵測的基礎。通過提供這種附加安全層，SonicWall 的下一代防火牆得以擴充目前提供的防護以涵蓋數百萬計惡意軟體。

SonicWall GAV 結構

SonicWall GAV 基於 SonicWall 的高效能 DPIv2.0（深度封包偵測版本 2.0）引擎，此引擎直接在 SonicWall 安全裝置上執行所有掃描。SonicWall GAV 採用按封包自動解壓縮和掃描檔案的進階解壓縮技術搜尋病毒和惡意軟體。請參見 SonicWall GAV 結構。SonicWall GAV 引擎可以執行 base64 解碼，而不是重組整個 base64 編碼郵件串流。由於 SonicWall GAV 不執行重組，因此沒有掃描引擎所施加的檔案大小限制。Base64 解碼、ZIP、LHZ 和 GZIP (LZ77) 解壓縮也使用單次傳遞和按封包的方式執行。SonicWall GAV 引擎的免重組病毒掃描功能繼承自深度封包偵測引擎，能在掃描資料流的同時不快取串流中的任何位元組。

SonicWall GAV 結構



GAV 建立在 SonicWall 的免重組結構上，可以檢查多個應用程式通訊協定以及一般 TCP 串流和壓縮流量。SonicWall GAV 通訊協定檢查基於各個受支援通訊協定的特定高效能狀態機。SonicWall GAV 通過檢查當今網路環境中最常用的通訊協定，包括 SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、即時訊息和對等應用程式等多種通訊協定以及其他一些基於串流的通訊協定，從而提供相關防護。這關閉了可能破壞網路安全的潛在後門，同時提高了員工生產率和儲存網際網路頻寬。

提示：如果您的 SonicWall 安全裝置已連接到網際網路並在 mySonicWall.com 註冊，您可以分別在管理介面的**安全服務 > 閘道防毒、安全服務 > 防間諜軟體**和**安全服務 > 入侵保護頁面**啟用 30 天免費試用版 SonicWall 閘道防毒、SonicWall 防毒和 SonicWall 入侵保護服務。

啟用閘道防毒、防間諜軟體和 IPS 授權

若要使用這些安全服務，您的裝置必須在 MySonicWall 上註冊。如需建立 MySonicWall 帳戶和註冊裝置的相關資訊，請參閱*入門指南*。如需在封閉環境中升級服務的相關資訊，請參閱 *SonicWall SonicOS 6.5 更新*。

由於 SonicWall 防間諜軟體是 SonicWall 閘道防毒、防間諜軟體和入侵保護服務的一部分，因此，您收到的啟用金鑰用於啟用 SonicWall 安全裝置上的全部三項服務。

如果您的 SonicWall 安全裝置未啟用 SonicWall 閘道防毒授權，必須向 SonicWall 分銷商或通過 mySonicWall.com 帳戶購買（僅限於美國和加拿大地區的客戶）。

啟用免費試用版

您可以嘗試免費試用版的 SonicWall 閘道防毒、SonicWall 防間諜軟體和 SonicWall 入侵保護服務。如需啟用任何或所有「安全服務」的免費試用資訊，請參見裝置的*入門指南*。

設定 SonicWall 閘道防毒防護

在 SonicWall 安全裝置上啟用 SonicWall 閘道防毒授權不會自動啟用防護。

若要設定 SonicWall 閘道防毒：

1 啟用 SonicWall 閘道防毒。

2 對區域套用 SonicWall 閘道防毒防護。

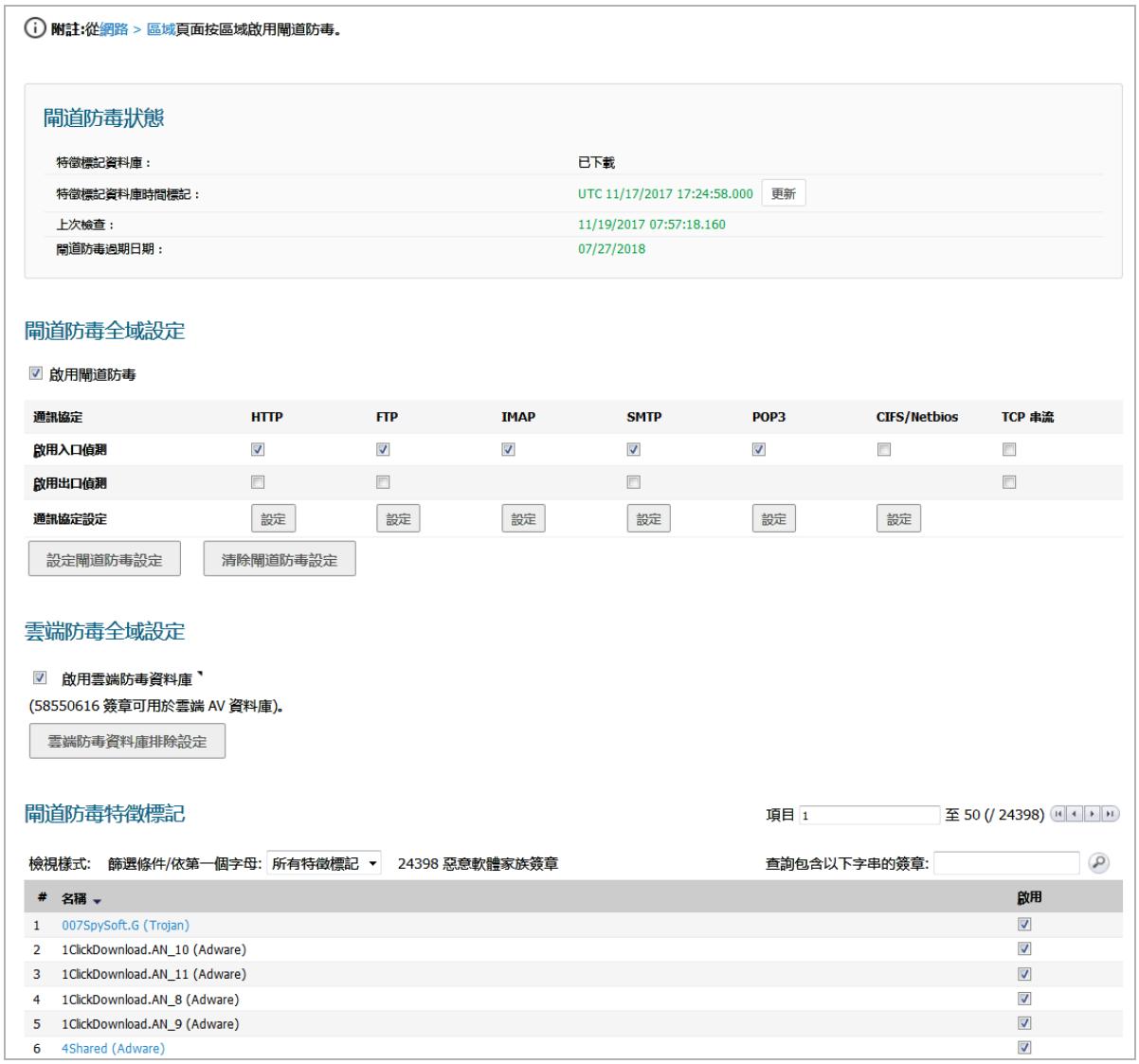
附註：如需設定 SonicWall 閘道防毒的完整說明，請參閱 SonicWall *閘道防毒管理指南*。

主題：

- 安全服務 > 閘道防毒頁面
- 啟用 SonicWall GAV
- 對區域套用 SonicWall GAV 防護
- 查看 SonicWall GAV 狀態資訊
- 指定通訊協定篩選
- 設定閘道防毒設定
- 設定雲端閘道防毒功能

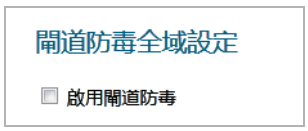
安全服務 > 閘道防毒頁面

安全服務 > 閘道防毒頁面提供用於在 SonicWall 安全裝置上設定 SonicWall GAV 的設定，並同時顯示防毒狀態和防毒特徵。



啟用 SonicWall GAV

必須在**閘道防毒全域設定**區段中選擇**啟用閘道防毒**核取方塊，以啟用 SonicWall 安全裝置上的 SonicWall GAV。



您必須在**系統安裝 | 網路 > 區域**頁面上指定您要套用 SonicWall GAV 防護的區域。

對區域套用 SonicWall GAV 防護

當您在**網路 > 區域**頁面上新增或編輯某個區域時，應對區域套用 SonicWall GAV。從**安全服務 > 閘道防毒**頁面，按一下**注**中的連結即可快速顯示**網路 > 區域**頁面：從網路 > 區域頁面（**閘道防毒狀態**區段中）按區域啟用閘道防毒。

附註：如需對區域套用 SonicWall GAV 防護的說明，請參閱對區域套用 SonicWall GAV 防護。

查看 SonicWall GAV 狀態資訊

閘道防毒狀態部分顯示防毒特徵資料庫的狀態，包括資料庫時間戳記以及 SonicWall 特徵伺服器上次檢查最新資料庫版本的時間。SonicWall 安全裝置會在啟動時，以及之後每小時自動嘗試同步資料庫。

主題：

- 檢查 SonicWall GAV 特徵標記資料庫狀態
- 更新 SonicWall GAV 特徵

檢查 SonicWall GAV 特徵標記資料庫狀態

閘道防毒狀態區段顯示以下資訊：

- **特徵標記資料庫**表明是否需要下載特徵標記資料庫或已下載。
- **特徵標記資料庫時間戳記**顯示上次更新 SonicWall GAV 特徵標記資料庫的時間，而不是上次更新 SonicWall 安全裝置的時間。
- **上次檢查**顯示 SonicWall 安全裝置上次在特徵標記資料庫中查找更新的時間。SonicWall 安全裝置會在啟動時，以及之後每小時自動嘗試同步資料庫。
- **閘道防毒到期日期**顯示 SonicWall GAV 服務過期的日期。如果您的 SonicWall GAV 訂閱過期，將停止 SonicWall IPS 檢查，且會從 SonicWall 安全裝置中移除 SonicWall GAV 設定。在更新 SonicWall GAV 授權後，這些設定自動恢復至之前的設定狀態。

閘道防毒狀態區段顯示**注：**從網路 > 區域頁面按區域啟用閘道防毒。按一下網路 > 區域連結將顯示用於對區域套用 SonicWall GAV 的**網路 > 區域**頁面。

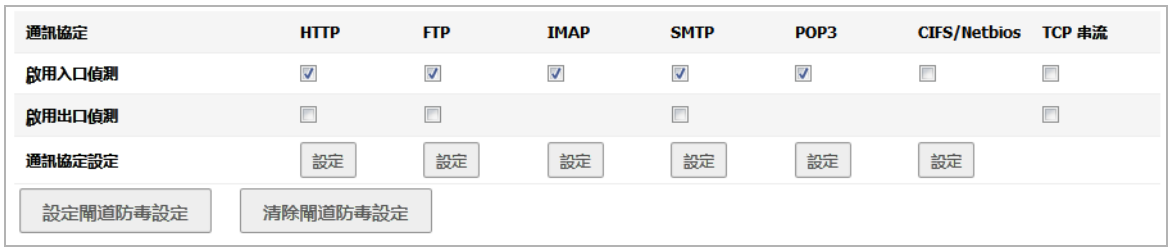
附註：如需對區域套用 SonicWall GAV 防護的說明，請參閱對區域套用 SonicWall GAV 防護。

更新 SonicWall GAV 特徵

預設情況下，執行 SonicWall GAV 的 SonicWall 安全裝置每小時自動檢查一次 SonicWall 特徵伺服器。管理員無需不斷檢查有無新的特徵更新。您還可以隨時通過按一下**閘道防毒狀態**區段的**更新**按鈕，手動更新 SonicWall GAV 資料庫。

SonicWall GAV 特徵更新是受防護的。SonicWall 安全裝置必須首先通過在「SonicWall 分布式實施結構」授權註冊時建立的預先共用密碼自行驗證身分。特徵請求通過 HTTPS 與完全伺服器憑證驗證一同傳送。

指定通訊協定篩選



SonicWall GAV 可以在應用程式層識別到傳送違反原則的資訊的通訊協定類型，因此可以在應用程式環境下執行特定操作適當地處理承載拒絕。

主題：

- 啟用輸入檢查
- 啟用出口偵測
- 限制檔案傳送
- 清除閘道防毒設定

啟用輸入檢查

預設情況下，SonicWall GAV 檢查所有傳入 **HTTP**、**FTP**、**IMAP**、**SMTP** 和 **POP3** 流量。可以選擇啟用一般 **TCP 串流**檢查基於 TCP 的所有其他流量，例如 SMTP 和 POP3，IM 和 P2P 通訊協定執行的非標準連接埠。

在 SonicWall GAV 環境中，**啟用輸入檢查**通訊協定流量的處理針對於；參見傳入流量檢查：SMTP 與所有其他流量表格：

- 來自指定為任意區域的受信任、無線或加密區域的非 SMTP 流量。
- 來自指定為不受信任區域的公用區域的非 SMTP 流量。
- 來自指定為受信任、無線、加密或公用區域的不受信任區域的 SMTP 流量。
- 來自指定為受信任、無線或加密區域的受信任、無線或加密區域的 SMTP 流量。

傳入流量檢查：SMTP *與*所有其他流量

SMTP 流量

目的地 來源	受信任	加密	無線	公用	不受信任
受信任	√	√	√		
加密	√	√	√		
無線	√	√	√		
公用	√	√	√	√	√
不受信任	√	√	√	√	√

所有其他流量

目的地 來源	受信任	加密	無線	公用	不受信任
受信任	√	√	√	√	√

傳入流量檢查：SMTP *與*所有其他流量

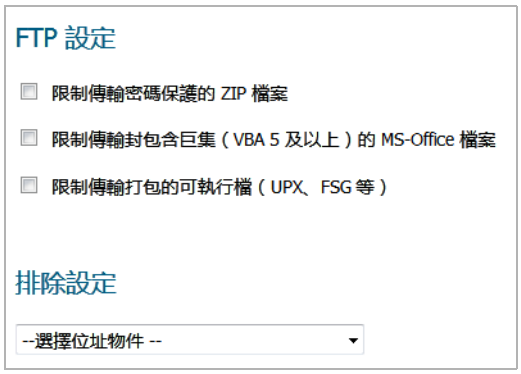
加密	√	√	√	√	√
無線	√	√	√	√	√
公用					√
不受信任					

啟用出口偵測

可以對 HTTP、FTP、SMTP 和 TCP 流量提供**啟用出口偵測**功能。

限制檔案傳送

對於各項通訊協定，除了 TCP 串流，您可以通過按一下**閘道防毒全域設定**區段的通訊協定下的**設定**按鈕限制有特定屬性的檔案的傳送。



主題：

- FTP 設定
- 排除設定

FTP 設定

這些限制傳送的 **FTP 設定**包括：

- **限制傳輸密碼保護的 ZIP 檔案** - 停用通過任何啟用通訊協定的受密碼防護 ZIP 檔案傳送。此選項僅適用於已啟用檢查的通訊協定（例如 HTTP、FTP、SMTP）。
- **限制傳輸封包含巨集（VBA 5 及以上）的 MS-Office 檔案** - 停用包含 VBA 宏的任何 MS Office 97 及以上檔案的傳送。
- **限制傳輸打包的可執行檔（UPX、FSG 等）** - 停用打包的可執行檔案的傳送。

  打包程式是用於壓縮且有時加密可執行檔案的實用程式。雖然有合理的應用程式實現這些功能，有時也用於隱蔽目的，使防毒應用程式不會偵測到可執行檔案。打包程式新增標題在記憶體中擴充檔案，然後執行此檔案。

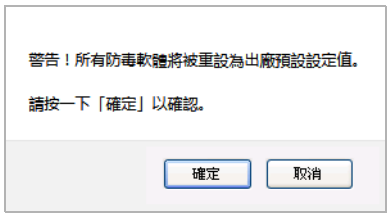
  SonicWall 閘道防毒目前可識別最常見的打包格式：UPX、FSG、PKLite32、Petite 和 ASPack。隨著 SonicWall GAV 特徵更新，還會動態新增更多格式。

排除設定

- 下拉清單 - 從限制傳送的 FTP 設定中排除所選的位址物件。

清除閘道防毒設定

1 如需將所有閘道防毒 (AV) 設定重設為出廠預設值，請按一下**清除閘道防毒設定**按鈕。將顯示確認訊息。



2 按一下**確定**。

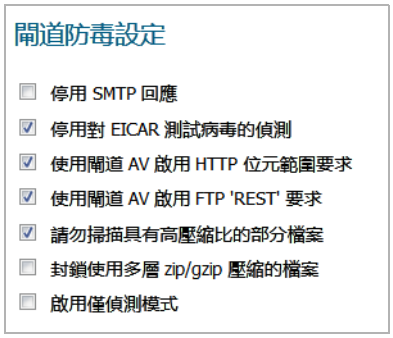
設定閘道防毒設定

按一下**閘道防毒全域設定**部分底部的**設定閘道防毒設定**按鈕，將顯示**閘道防毒設定檢視**對話方塊，可用於設定無用戶端通知警示和建立 SonicWall GAV 排除清單。

主題：

- 設定閘道防毒設定
- 設定 HTTP 無用戶端通知
- 設定 SonicWall GAV 排除清單

設定閘道防毒設定



設定閘道防毒選項的步驟如下：

1 如果在電子郵件或附件中偵測到病毒時需要抑制從 SonicWall GAV 向用戶端傳送電子郵件 (SMTP)，請勾選**停用 SMTP 回應**核取方塊。預設情況下未勾選此選項。

2 EICAR 標準防毒測試檔案是一種特殊病毒模擬器檔案，此檔案可檢查和確認 SonicWall 閘道防毒服務的正確執行。如需禁止刪除 EICAR，請勾選**停用對 EICAR 測試病毒的偵測**核取方塊。預設情況下已選擇此設定。

3 如需允許傳送位元組服務（僅傳送部分 HTTP 訊息或檔案的過程），請勾選**啟用具有閘道防毒功能的 HTTP 位元組範圍請求**核取方塊。預設情況下已選擇此設定。

預設情況下，SonicWall 閘道防毒 (GAV) 安全服務將停用 HTTP 位元組範圍請求，以避免分段擷取和潛在惡意內容的重組。方法是中斷連接，並防止使用者接收惡意承載。啟用此設定可覆寫此預設行為。

4 如需允許使用 FTP REST 請求檢索和重組分段訊息和檔案，請勾選**啟用具有閘道防毒功能的 FTP 'REST' 請求**核取方塊。預設情況下已選擇此設定。

預設情況下， SonicWall GAV 將停用 HTTP 'REST'（重新啟動）請求，以避免分段擷取潛在惡意內容的重組。方法是中斷連接，並防止使用者接收惡意承載。啟用此設定可覆寫此預設行為。

5 如需禁止掃描檔案或具有高壓縮比的部分檔案，請勾選**不掃描具有高壓縮比檔案的任何部分**核取方塊。預設情況下已選擇此設定。

6 如需封鎖具有高壓縮比的檔案，請勾選**封鎖使用多層 zip/gzip 壓縮的檔案**核取方塊。預設情況下未勾選此設定。

7 如需使閘道防毒服務處於僅探查模式（即僅探查和記錄病毒流量而不停止流量），請勾選**啟用僅偵測模式**核取方塊。預設情況下未勾選此設定。

設定 HTTP 無用戶端通知

HTTP 無用戶端通知功能在 GAV 偵測到來自 HTTP 伺服器的威脅時通知使用者。

如停用此功能，GAV 在偵測到來自 HTTP 伺服器的威脅時會封鎖威脅，使用者則收到空白 HTTP 頁面。通常，使用者會嘗試重新載入頁面，因為他們沒有意識到威脅。HTTP 無用戶端通知功能會通知使用者 GAV 偵測到來自 HTTP 伺服器的威脅。

提示：SonicWall 防間諜軟體也有 HTTP 無用戶端通知功能。

設定此功能的步驟如下。

1 勾選**啟用 HTTP 非客戶通知警示**核取方塊。預設情況下已核取此選項。

2 也可在**封鎖時要顯示的訊息**欄位中輸入訊息。預設訊息為防火牆閘道防毒服務已封鎖此請求。

提示：您可以在**安全服務 > 基本設定**頁面的**安全服務設定**標題下，設定 HTTP 無用戶端通知的逾時。

設定 SonicWall GAV 排除清單

排除清單中列出的任何 IP 位址的流量都不會進行病毒掃描。**閘道防毒排除清單**區段可用於選擇位址物件或定義流量不進行 SonicWall GAV 掃描的 IP 位址範圍。

注意：在指定排除出 SonicWall GAV 防護的 IP 位址時要謹慎。

若要新增排除防護的 IP 位址，請執行以下這些步驟：

1 導覽至**安全設定 | 閘道防毒 | 閘道防毒全域設定**部分。

2 按一下**設定閘道防毒設定**按鈕。

3 選擇**閘道防毒排除清單**區段的**啟用閘道防毒排除清單**核取方塊以啟用排除清單。

4 選擇以下選項之一：

- **使用位址物件**選項按鈕
  a) 從下拉功能表中選擇位址物件。
  b) 移至步驟 5。
- **使用位址範圍**選項按鈕。
  a) 按一下**新增**按鈕。顯示**新增 GAV 範圍項目**對話方塊。

  b) 在**起始 IP 位址**和**結束 IP 位址**欄位中輸入 IP 位址範圍。

c) 按一下**確定**。**閘道防毒排除清單**表格中顯示您的 IP 位址範圍。

附註：若要變更項目，按一下**設定**列中的**編輯**圖示。若要刪除項目，按一下**刪除**圖示。如需刪除排除清單中的所有項目，按一下**全部刪除**按鈕。

5 按一下**確定**。

設定雲端閘道防毒功能

啟用雲端閘道防毒功能的步驟如下：

1 導覽至**安全設定 | 閘道防毒 | 雲端防毒全域設定**部分。

2 勾選**啟用雲端防毒資料庫**核取方塊。（預設情況下已核取此選項。）

另外，也可以選擇排除對某些雲端特徵的實施，以緩解誤報問題或按需要啟用下載特定的病毒檔案。

若要設定排除清單：

1 按一下**雲端防毒資料庫排除設定**按鈕。隨即顯示**新增雲端 AV 排除**對話方塊。

2 在**雲端 AV 簽章 ID** 欄位中輸入特徵 ID。此 ID 必須為一個數值。

3 按一下**新增**按鈕。

4 對每個要新增的特徵重複步驟 2 和步驟 3。

5 另外，更新特徵 ID 的步驟如下：

a 在**清單**欄位中勾選特徵 ID。

b 在**雲端 AV 簽章 ID** 欄位中輸入更新的特徵。

c 按一下**更新**。

6 此外，如需刪除：

- 特徵 ID，請在**清單**欄位中勾選 ID，然後按一下**移除**按鈕。

- 所有特徵標記，請按一下**全部移除**按鈕。

7 另外，如需查看有關某特徵的最新資訊，請在清單中選擇此特徵 ID，然後按一下**簽章資訊**按鈕。特徵的資訊顯示在 SonicALERT 網站上。

8 在完成設定雲端防毒排除清單時按一下**確定**。

查看 SonicWall GAV 特徵

閘道防毒特徵標記區段用於查看 SonicWall GAV 特徵標記資料庫的內容。**閘道防毒特徵標記**表中顯示的所有項目都來自於下載到您的 SonicWall 安全裝置的 SonicWall GAV 特徵標記資料庫。惡意軟體家族特徵數顯示在此表之上。

附註：資料庫中的特徵項目隨著時間的推移不斷改變以應對新的威脅。

主題：

- 顯示特徵
- 移至閘道防毒特徵標記表
- 搜尋閘道防毒特徵標記資料庫

顯示特徵

您可以多種檢視樣式顯示特徵：

提示：篩選特徵時，找到的特徵數將與資料庫中的特徵總數一起顯示。

- **檢視樣式** - 從**首字母**下拉功能表中選擇其中一項：
  - **所有特徵** - 顯示表中的所有特徵標記，每頁顯示 50 個項目。
  - **0 - 9** - 顯示名稱以您在功能表中選擇的數字開頭的特徵。
  - **A - Z** - 顯示名稱以您在功能表中選擇的字母開頭的特徵。
- **搜尋字串** - 顯示包含特定字串的特徵：
  a 在**查詢特徵標記包含字串**欄位中輸入字串。
  b 按一下**放大鏡**圖示。

移至閘道防毒特徵標記表

SonicWall GAV 特徵在**閘道防毒特徵標記**表每頁顯示 50 個項目。**項目**欄位顯示第一個特徵的表編號。關於表格間瀏覽的資訊，參閱 *SonicWall SonicOS 6.5 關於 SonicOS*。

搜尋閘道防毒特徵標記資料庫

您可以通過在**查詢特徵標記包含字串**欄位輸入搜尋字串，然後按一下**搜尋**圖示來搜尋特徵標記資料庫。

閘道防毒特徵標記表中僅顯示符合指定字串的特徵。

12

啟用入侵保護服務

- 入侵保護服務銷售概述
- 啟用入侵保護服務

入侵保護服務銷售概述

SonicWALL 入侵保護服務 (IPS) 提供可設定的高效能深度封包偵測引擎，擴充了關鍵網路服務的防護，例如 Web、電子郵件、檔案傳送、Windows 服務和 DNS。SonicWall IPS 用於防護應用程式漏洞、蠕蟲病毒、特洛伊木馬以及對等、間諜軟體和後門攻擊。SonicWall 的深度封包偵測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。SonicWall IPS 通過 SonicWall 的行業領先分布式實施結構 (DEA) 免去了昂貴、耗時的新駭客攻擊特徵維護和更新。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。

主題：

- SonicWall 深度封包偵測
- SonicWall 的深度封包偵測的工作原理
- SonicWall IPS 術語
- IPS 狀態
- IPS 全域設定
- 在區域上設定 IPS 防護
- IPS 原則

SonicWall 深度封包偵測

深度封包偵測查看封包的資料部分。深度封包偵測技術包含入侵偵測和入侵保護。入侵偵測發現流量異常並向管理員傳送警示。入侵保護發現流量異常和作出應對，並封鎖流量通過。

深度封包偵測是允許防火牆根據規則對通過的流量進行分類的一項技術。這些規則包含有關封包第 3 層和第 4 層的資訊，以及描述封包承載的內容的資訊，包括應用程式資料（例如 FTP 工作階段、HTTP Web 瀏覽器工作階段，甚至中間件資料庫連接）。這項技術允許管理員偵測和記錄經過防火牆的入侵，並封鎖入侵（即丟棄封包或重設 TCP 連接）。SonicWall 的深度封包偵測技術還可用於正確處理 TCP 片段位元組流檢查，與無 TCP 片段的處理方式無異。

SonicWall 的深度封包偵測的工作原理

深度封包偵測技術使防火牆可以深入到協定的調查，以檢驗應用程式層的資訊和抵禦針對應用程式漏洞的攻擊。這是 SonicWall 入侵保護服務採用的技術。SonicWall 的深度封包偵測技術實現從 SonicWall 分布式實施結構推送動態特徵更新。

以下步驟描述了 SonicWall 深度封包偵測結構的工作原理。請參見 SonicWall 深度封包偵測結構：

1 模式定義語言解釋程式使用可撰寫用於偵測和封鎖已知和未知協定、應用程式和攻擊的特徵。

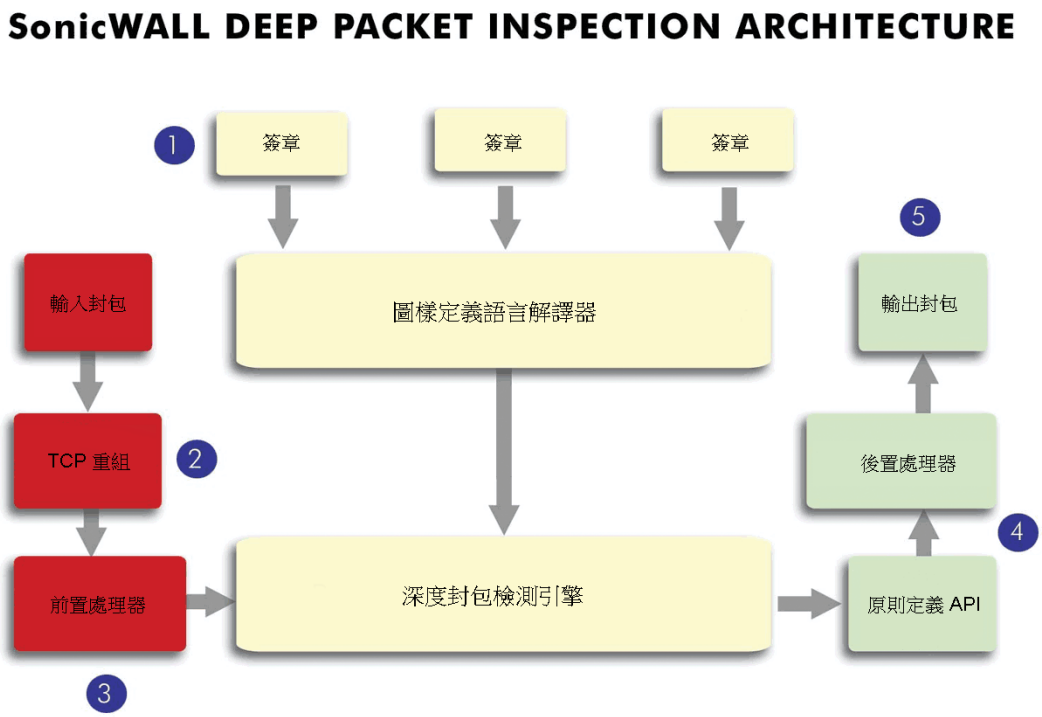
2 深度封包偵測框架將重組亂序抵達的 TCP 封包。

3 深度封包偵測引擎的預處理包括封包承載的規範化。例如，HTTP 請求可能使用 URL 編碼，因此此請求也使用 URL 解碼才能執行正確的承載模式符合。

4 深度封包偵測引擎的後處理器執行的操作可能只是不經修改簡單傳遞封包，或丟棄封包，甚或重設 TCP 連接。

5 SonicWall 的深度封包偵測框架支援各 TCP 片段之間的完整特徵符合，且不執行任何重組（除非封包亂序）。這將實現更高效地使用處理器和記憶體，從而提高效能。

SonicWall 深度封包偵測結構



SonicWall IPS 術語

- **狀態封包檢查** - 查看封包的標題以根據連接埠、協定和 IP 位址控制存取權限。
- **深度封包偵測** - 查看封包的資料部分。使防火牆可以深入到協定的調查，以檢驗應用程式層的資訊和抵禦針對應用程式漏洞的攻擊。
- **入侵偵測** - 識別和標記針對資訊技術的惡意活動的過程。
- **誤報** - 錯誤識別的攻擊流量模式。

- **入侵保護** - 發現流量中的異常和惡意活動並進行應對。
- **簽章** - 撰寫用於偵測和封鎖入侵、蠕蟲病毒、應用程式攻擊和對等與即時訊息流量的代碼。

啟用入侵保護服務

入侵保護服務 (IPS) 是在**安全設定 | 安全服務 > 入侵保護**頁面上設定，分為三個面板：

- IPS 狀態
- IPS 全域設定
- IPS 原則

主題：

- IPS 狀態
- IPS 全域設定
- 在區域上設定 IPS 防護
- IPS 原則

IPS 狀態

IPS 狀態面板顯示特徵標記資料庫的狀態資訊和您的 SonicWall IPS 授權。

IPS 狀態面板顯示以下資訊：

- **簽章資料庫**顯示特徵標記資料庫是否正在下載、已下載或是需要下載。特徵標記資料庫約一小時自動更新一次。您還可以隨時通過按一下 **IPS 狀態**區段的**更新**按鈕手動更新 IPS 資料庫。
- **簽章資料庫時間戳記**顯示上次更新 IPS 特徵標記資料庫的時間，而不是上次更新 SonicWall 安全裝置的時間。
- **上次檢查**顯示 SonicWall 安全裝置上次在特徵標記資料庫中查找更新的時間。SonicWall 安全裝置會在啟動時，以及之後每小時自動嘗試同步資料庫。
- **IPS 服務到期日期**顯示 IPS 服務過期的日期。如果您的 IPS 訂閱過期，將停止 SonicWall IPS 檢查，且會從 SonicWall 安全裝置中移除 IPS 設定。在更新 IPS 授權後，這些設定會自動恢復至之前的設定狀態。
- **附註**：從網路 > 區域頁面按區域啟用入侵保護服務。

  如果按一下此備註中的網路 > 區域，將顯示可在區域上設定 IPS 的**系統安裝 | 網路 > 區域**頁面。請參閱在區域上設定 IPS 防護。

IPS 全域設定

IPS 全域設定面板提供在防火牆上啟用 SonicWall IPS 的金鑰設定。

SonicWall IPS 通過在您的防火牆上啟用 IPS 並選擇攻擊級別全域啟用。您也可以選擇設定 **IPS 排除清單**。

主題：

- 啟用 IPS
- 設定 IPS 排除清單
- 重設 IPS 設定和原則

啟用 IPS

若要在您的防火牆上啟用 IPS，請執行以下操作：

1 導覽至**安全設定 | 安全服務 > 入侵保護**頁面。

2 捲動到 **IPS 全域設定**部分。

3 選擇**啟用 IPS**。

4 選擇您要為每個**特徵標記群組**執行的操作（**全部禁止**、**全部偵測**或兩者）：

- **高優先順序攻擊**
- **中優先順序攻擊**
- **低優先順序攻擊**

附註：若要在防火牆上啟用入侵保護，您必須為至少一個**特徵標記群組**指**全部禁止**操作。如果未選擇**全部禁止**操作，將不會在防火牆上出現任何入侵保護。

附註：為所有**特徵標記群組**選擇**全部禁止**和**全部偵測**可以防護網路不受最危險、最具破壞性的攻擊。

設定 IPS 排除清單

（可選）若要設定 IPS 排除清單，請執行以下操作：

1 導覽至**安全設定 | 安全服務 > 入侵保護**頁面。

2 捲動到 **IPS 全域設定**部分。

3 選擇**啟用 IPS**。

4 按一下**設定 IPS 設定**按鈕。

此時會顯示 **IPS 排除清單**對話方塊。

5 選擇**啟用 IPS 排除清單**。

6 選擇**使用位址物件**選項或**使用位址範圍**選項。

7 如果選擇了**使用位址物件**選項，請選擇您要從功能表中排除的位址物件。

8 如果選擇了**使用位址範圍**選項，請按一下**新增**按鈕。

此時會顯示**新增 IPS 範圍項目**對話方塊。

9 輸入要在 **起始 IP 位址**和 **結束 IP 位址**方塊中排除的 IP 位址範圍。

10 按一下**確定**。

重設 IPS 設定和原則

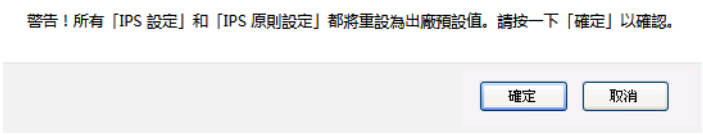
若要重設 IPS 設定和原則，請執行以下操作：

1 導覽至**安全設定 | 安全服務 > 入侵保護**頁面。

2 捲動到 **IPS 全域設定**部分。

3 按一下**重設 IPS 設定與原則**按鈕。

隨即顯示以下訊息。



4 按一下**確定**。

在介面的底部顯示以下訊息：狀態： 設定已更新。

在區域上設定 IPS 防護

您在**網路 > 區域**頁面對區域套用 SonicWall IPS 不僅會在各網路區域和 WAN 之間實施 SonicWall IPS，還會在內部區域之間實施。例如，在 LAN 區域啟用 SonicWall IPS 可以對所有進出的 LAN 流量實施 SonicWall IPS。

在**安全服務 > 入侵保護服務**頁面的 **IPS 狀態**區段，按一下**網路 > 區域**連結存取**網路 > 區域**頁面。您對網路 > 區域頁面上列出的區域套用 SonicWall IPS。

如需對區域啟用 SonicWall，請執行以下這些步驟：

1 導覽至**安全設定 | 網路 > 區域**或在**安全服務 > 入侵保護**頁面的 **IPS 狀態**部分，按一下**網路 > 區域**連結。顯示**網路 > 區域**頁面。

2 在**區域設定**表的**設定**列，按一下您要套用 SonicWall IPS 的區域的**編輯**圖示。顯示**編輯區域**視窗。

3 按一下**啟用 IPS** 核取方塊。顯示複選標記。若要停用 SonicWall IPS，清除此核取方塊。

4 按一下**確定**。

您還可以在**網路 > 區域**頁面對建立的新區域啟用 SonicWall IPS 防護。按一下**新增**按鈕顯示**新增區域**視窗，其中包含與**編輯區域**視窗相同的設定。

IPS 原則

IPS 原則面板用於查看 SonicWall IPS 特徵和設定按類別組或逐個特徵處理。特徵的類別按攻擊類型分組。

您可以通過以下方式查看特徵：

- 查看和設定類別設定
- 查看和設定特徵設定
- 查看和設定特定類別的特徵

- 優先順序功能表
- 查詢簽章 ID

查看和設定類別設定

在**查看樣式**行中，**類別**功能表可讓您選擇要在**類別**列中顯示的類別或特徵。您可以選擇**所有類別**、**所有特徵標記**或單個類別，如 **ACTIVEX** 或 **DNS**。如果您選擇單個類別，將顯示此類別的特徵。

類別列用於通過按一下列標題旁邊的向上或向下箭頭來按遞增或遞減排列類別和特徵。

若要查看或變更指定類別的 IPS 類別設定，請執行以下操作：

1 從**類別**功能表中選擇**所有類別**。

2 按一下此類別**設定**列中的**編輯**圖示。隨即顯示**編輯 IPS 類別**對話方塊。

3 從**禁止**和**偵測**功能表中，選擇**使用全域設定**、**啟用**或**停用**。如果選擇**使用全域設定**，將使用在 **IPS 全域設定**區段中設定的值，但您可以通過在這些功能表中選擇**啟用**或**停用**來覆寫 **IPS 全域設定**。

4 在剩餘的功能表中，選擇您需要的值。

5 對於**記錄冗餘篩選條件（秒數）**選項，如果您要使用在 **IPS 全域設定**區段中設定的值，請選擇使用全域設定。

6 按一下**確定**。

查看和設定特徵設定

若要查看或變更指定特徵的 IPS 特徵設定，請執行以下操作：

1 從**類別**功能表中選擇**所有特徵標記**。

2 按一下此特徵**設定**列中的**編輯**圖示。隨即顯示**編輯 IPS 特徵標記**對話方塊。

前五個對話方塊將灰色顯示，且包含無法對此特徵設定的資料。

3 從**禁止**和**偵測**功能表中，選擇**啟用**或**停用**。**使用類別設定選項**已停用。

4 在剩餘的功能表中，選擇您需要的值。

5 對於**記錄冗餘篩選條件（秒數）**選項，如果您要使用在 **IPS 全域設定**區段中設定的值，請選擇使用類別設定。

6 按一下**確定**。

查看和設定特定類別的特徵

查看和設定特定類別的特徵，請執行以下操作：

1 從**類別**功能表中選擇以下其中一個類別：隨即顯示此類別的特徵。

2 按一下此特徵**設定**列中的**編輯**圖示。隨即顯示**編輯 IPS 特徵標記**對話方塊。

前五個對話方塊將灰色顯示，且包含無法對此特徵設定的資料。

3 從**禁止**和**偵測**功能表中，選擇**啟用**或**停用**。**使用類別設定選項**已停用。

4 在剩餘的功能表中，選擇您需要的值。

5 對於**記錄冗餘篩選條件（秒數）**選項，如果您要使用在 **IPS 全域設定**區段中設定的值，請選擇使用類別設定。

6 按一下**確定**。

優先順序功能表

優先順序功能表用於指定您要顯示的特徵的優先順序。

指定您要顯示的特徵的優先順序：

- 從**優先順序**功能表中選擇以下其中一個優先順序：
  - 全部
  - 高
  - 中
  - 低

查詢簽章 ID

您可以使用**查詢簽章 ID** 方框查看或變更指定特徵的 IPS 特徵設定。

若要查看或變更指定特徵的 IPS 特徵設定，請執行以下操作：

1 在**查詢簽章 ID** 方框中輸入特徵 ID。

2 按一下此方框旁邊的**查詢**圖示。隨即顯示**編輯 IPS 特徵標記**對話方塊。

前五個對話方塊將灰色顯示，且包含無法對此特徵設定的資料。

3 從**禁止**和**偵測**功能表中，選擇**啟用**或**停用**。**使用類別設定選項**已停用。

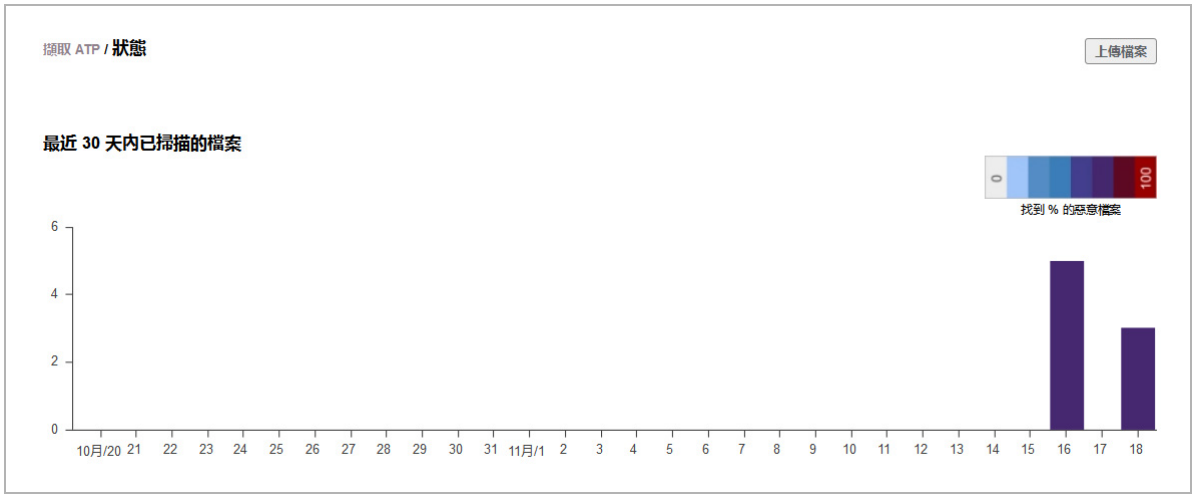
4 在剩餘的功能表中，選擇您需要的值。

5 對於**記錄冗餘篩選條件（秒數）**選項，如果您要使用在 **IPS 全域設定**區段中設定的值，請選擇使用類別設定。

6 按一下**確定**。

13

檢視捕獲 ATP 狀態



重要：擷取進階威脅防護 (ATP) 是防火牆的附加安全性服務，類似閘道防毒 (GAV)，有助於防火牆辨識檔案是否為惡意。

所有 SuperMassive、NSA、和執行 SonicOS 6.5 或更新版本的 TZ600 和 TZ500/TZ500W 設備均支援捕獲 ATP。

在啟用捕獲 ATP 之前，您必須先取得授權，而且必須啟用閘道防毒 (GAV) 和雲端防毒資料庫服務。授權捕獲 ATP 後，您可以在您的 MySonicWall 帳戶中檢視捕獲 ATP 狀態，以及設定和接收警示和通知。

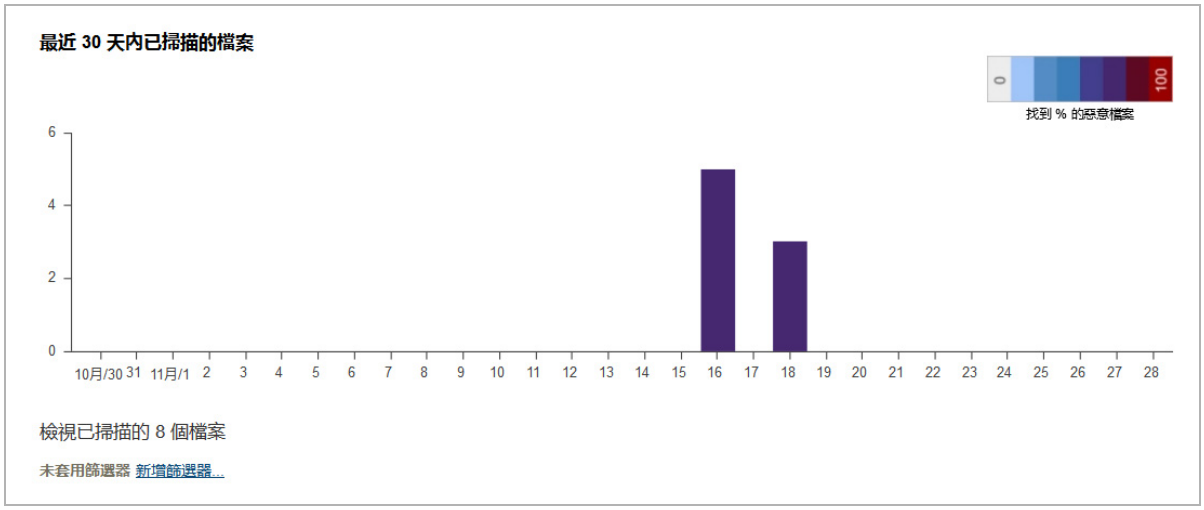
如需有關捕獲 ATP、其授權和使用您的 MySonicWall 帳戶設定和接收警示和通知的詳細資訊，請參閱 *SonicOS 6.5 捕獲進階威脅防護功能指南*。

捕獲 ATP > 狀態頁面顯示圖形和記錄表，提供每個要掃描的檔案的資訊。按下**上載檔案**按鈕，檔案可上載至捕獲 ATP 從此頁面進行掃描。

主題：

- 關於圖表
- 關於記錄表
- 上載檔案進行分析
- 檢視威脅報告

關於圖表

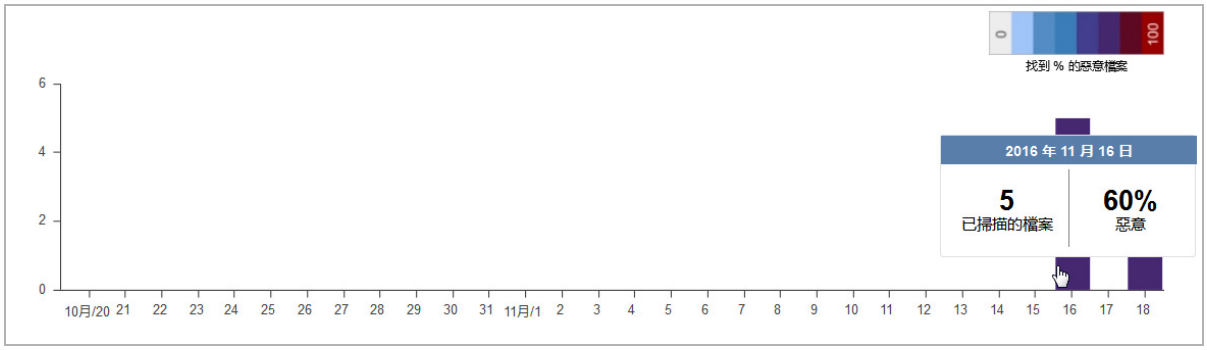


圖表顯示每天掃描的檔案數量。X 軸代表時間並僅顯示最近 30 天，每一天一列。Y 軸代表已掃描檔案的數量。

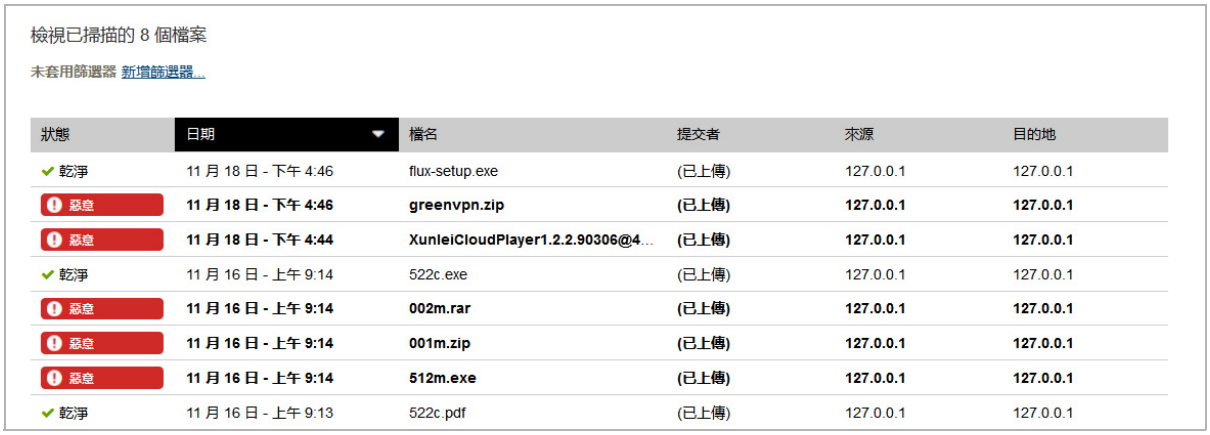
所發現惡意檔案的百分比是以圖表中每個直條的顏色表示。圖例顯示每個顏色所代表的檔案百分比，從代表找不到惡意檔案的零 (淡灰色) 到表示找到 100% 的檔案為惡意的紅色。

所掃描的檔案數顯示在圖表下方。

當滑鼠停在任一直條上，會快顯實際掃描的檔案數目以及在該日找到的惡意檔案數目。



關於記錄表


檢視已掃描的 8 個檔案

未套用篩選器 新增篩選器...

狀態	日期	檔名	提交者	來源	目的地
乾淨	11 月 18 日 - 下午 4:46	flux-setup.exe	(已上傳)	127.0.0.1	127.0.0.1
惡意	**11 月 18 日 - 下午 4:46**	**greenvpn.zip**	**(已上傳)**	**127.0.0.1**	**127.0.0.1**
惡意	**11 月 18 日 - 下午 4:44**	**XunleiCloudPlayer1.2.2.90306@4...**	**(已上傳)**	**127.0.0.1**	**127.0.0.1**
乾淨	11 月 16 日 - 上午 9:14	522c.exe	(已上傳)	127.0.0.1	127.0.0.1
惡意	**11 月 16 日 - 上午 9:14**	**002m.rar**	**(已上傳)**	**127.0.0.1**	**127.0.0.1**
惡意	**11 月 16 日 - 上午 9:14**	**001m.zip**	**(已上傳)**	**127.0.0.1**	**127.0.0.1**
惡意	**11 月 16 日 - 上午 9:14**	**512m.exe**	**(已上傳)**	**127.0.0.1**	**127.0.0.1**
乾淨	11 月 16 日 - 上午 9:13	522c.pdf	(已上傳)	127.0.0.1	127.0.0.1

狀態	掃描的狀態： • **掃描擱置** - 掃描在進行中 • **乾淨** - 掃描已完成但是尚未確認判斷。 • **掃描失敗** - 掃描已失敗。 • **惡意**圖示 - 掃描已完成並且判斷為惡意。
日期	掃描檔案的日期。
檔名	檔案的名稱。
提交者	提交檔案至捕獲 ATP 的防火牆的序號。
來源	檔案來源的 IP 位址。
目的地	檔案傳送目的地的 IP 位址。

在圖形下，記錄表顯示每個已掃描檔案的資訊。記錄表可讓您捲動所掃描檔案的清單。如果掃描失敗，該列會呈現灰色。如果找到惡意檔案，該列會用粗體和紅色**惡意**圖示顯示。按下任何一列開啟威脅報告。

此頁的標題為動態，並可依照是否套用篩選條件以兩種狀態顯示：

- 沒有套用篩選條件時 - **檢視已掃描 *n* 個檔案**。
- 套用篩選條件時 - **檢視已掃描 *n* 個檔案，總計 *y* 個**。

日期欄位的列可以遞增或遞減順序排序。用於排序的欄位標題為黑色而非灰色。新增或移除篩選條件時，會持續所選的排序順序。

主題：

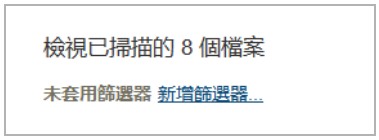
- 使用篩選條件標籤篩選顯示
- 為一個實例篩選顯示

使用篩選條件標籤篩選顯示

重要： 圖形、記錄表和篩選條件是繫結在一起的，會交互影響。

若要自定義記錄表中的顯示內容：

1 按一下**新增介面**連結。



顯示快顯對話方塊。

2 從下拉選單選擇您要的條件：

a 從第一個下拉選單選擇欄位名稱，例如**狀態** (預設)。

b 從第二個下拉選單選擇運算子：**is** (預設) 或 **is not**。

c 從第三個下拉選單選擇所選欄位的適當條件。顯示的內容依照您從第一個下拉選單所選擇項目而定。

3 按下**新增**。顯示篩選條件標籤並且表格結果會立即更新。

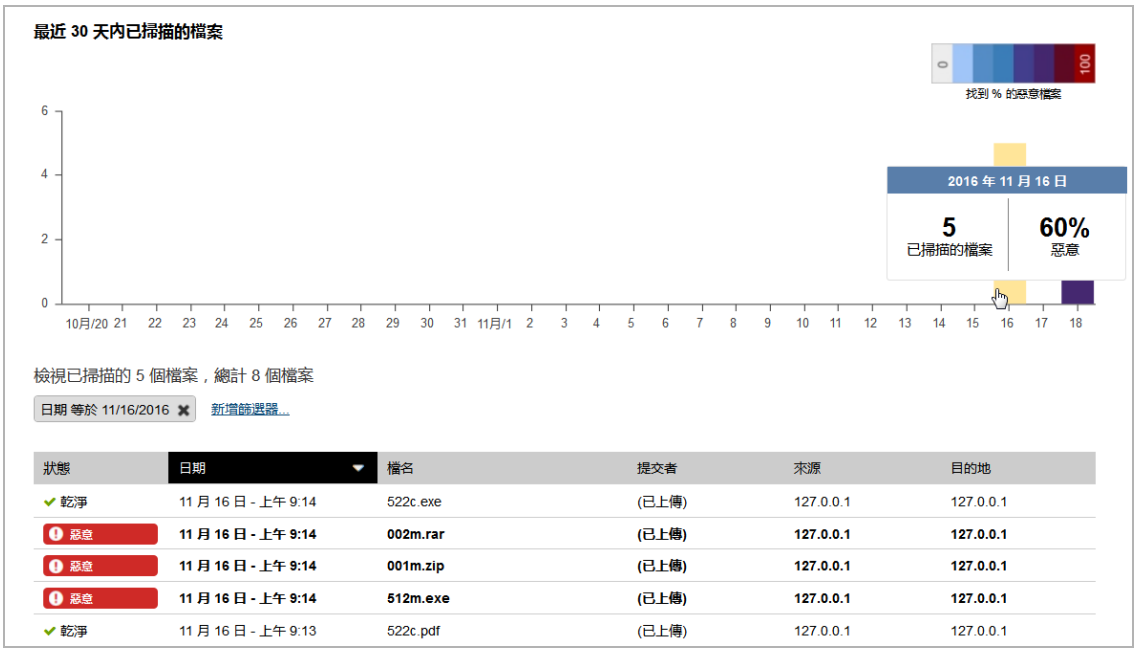
4 若要新增更多篩選條件，請重複步驟步驟 1 到步驟 3。同時只能套用一種篩選條件到記錄表。

若要刪除篩選條件，請按一下篩選條件標籤旁的 **X**。

為一個實例篩選顯示

若要為一個實例篩選顯示：

1 您可以按下圖表中的單一直條，設定記錄表的篩選條件，僅顯示該直條 (日期) 的詳細資料。



上載檔案進行分析

您可以使用**上載檔案**按鈕，手動上載要掃描的檔案。

若要上載檔案進行掃描：

1 導覽**捕獲 ATP > 設定**。

2 按下**上傳檔案**。會顯示**上傳要掃描的檔案**對話方塊。

3 按一下**瀏覽**按鈕。將顯示開啟檔案對話方塊。

4 選擇找到檔案並按一下**開啟**。

5 按一下**上傳**。將顯示狀態訊息。

附註：如果上傳失敗，會顯示錯誤訊息，例如：

6 狀態訊息會在幾秒後消失。在處理檔案之後，您可在狀態頁面上按下日誌表格中的任何檔案，查看該檔案的詳細分析結果。

檢視威脅報告

當您按下**捕獲 ATP > 狀態**頁面上記錄表中的任何一列，**捕獲 ATP 威脅**報告會顯示在新的瀏覽器視窗中。報告格式會依是否執行完整分析或是根據前置處理的判斷而有所不同。

主題：

- 從記錄表啟動威脅報告
- 檢視威脅報告頁首
- 檢視威脅報告頁尾
- 檢視靜態檔案資訊
- 檢視前置處理的威脅報告
- 檢視完整分析的威脅報告

從記錄表啟動威脅報告

您可以按下**捕獲 ATP > 狀態**頁面上記錄表中的任何一列，來啟動威脅報告。將滑鼠指標放在該列上醒目顯示該列，按下該列的任何一處即可在新的瀏覽器視窗啟動威脅報告。

附註：對於未包含任何支援的檔案類型的封存則不啟動威脅報告。

檢視威脅報告頁首

其他威脅報告的報告頁首均非常類似。本節說明頁首元件和變化之處。

橫幅包含兩部分：

- 上方橫幅為彩色：
  - 紅色指惡意檔案。
  - 藍色指乾淨檔案。

  最上方的項目顯示檔案提交給捕獲 ATP 進行分析的日期和時間。底部項目顯示所下載檔案的 IP 位址。
- 下方橫幅包含連接資訊：
  - 左側是連線來源的 IP 位址 (IPv4) 和連接埠編號。這是送出檔案的位址。
  - 中間是依其序號或易記名稱識別的防火牆。
  - 右側是連線目的地的 IP 位址 (IPv4) 和連接埠編號。這是檔案傳送目的地的位址。

檢視威脅報告頁尾

其他威脅報告的報告頁尾均非常類似。

檔案識別碼顯示在頁尾的左側每一行一個：

- MD5
- SHA1
- SHA258

此資訊會顯示在頁尾的右側：

序號	傳送檔案的防火牆的序號。如果手動上載檔案就不會顯示此項。
捕獲 ATP 版本	雲端中執行的捕獲 ATP 服務的軟體版本號。
產生的報告	報告產生時的 UTC 格式的時間戳記。

檢視靜態檔案資訊

靜態檔案資訊會顯示在威脅報告的左側，並且所有類型的報告均類似。

- 檔案大小 (以 kb 為單位)
- 檔案類型
- 檔案名稱則依防火牆所攔截的而定

檢視前置處理的威脅報告

根據檔案是否被發現為惡意或乾淨，前置處理器威脅報告的資料量會有所不同。

惡意檔案的前置處理器報告

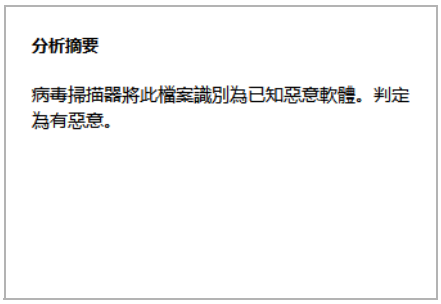
乾淨檔案的前置處理器報告

以下兩種狀況可看到乾淨威脅報告：

狀況 1	病毒掃描結果不明或良好。 檔案符合網域或廠商允許清單。
狀況 2	病毒掃描結果不明或良好。 檔案中沒有內嵌代碼

前置處理器報告中的分析摘要和狀況方塊

分析摘要



前置處理器威脅報告包含左側的**分析摘要**區段，其根據前置處理期間四個分析階段調查結果做總結。

狀況方塊

惡意狀況方塊

乾淨狀況方塊

四個前置處理階段的 true/false 結果會顯示在狀況方塊中。前置處理器分析的四個區域表格 根據每個前置處理階段的結果顯示處理情況。

前置處理器分析的四個區域

前置處理器階段結果	病毒掃描器偵測惡意軟體	允許清單的廠商信譽？[1]	允許清單的網域信譽？[1]	檔案中找到的內嵌程式碼？
True	惡意	非惡意	非惡意	繼續分析
False	繼續分析	繼續分析	繼續分析	非惡意

1. 廠商信譽篩選選項僅適用於 PE 檔案，而網域信譽可能不適用於透過 SMTP 傳送的檔案。在這些情況下，「繼續分析」狀態便為階段結果。

有些階段結果觸發立即判斷為惡意或非惡意，如前置處理器分析的四個區域表格中所述。否則，該階段結束時為「繼續分析」狀態。如果所有的前置處理階段產生「繼續分析」狀態，會將檔案傳送到雲端，由捕獲 ATP 進行完整分析。

前置處理器報告中的惡意軟體名稱

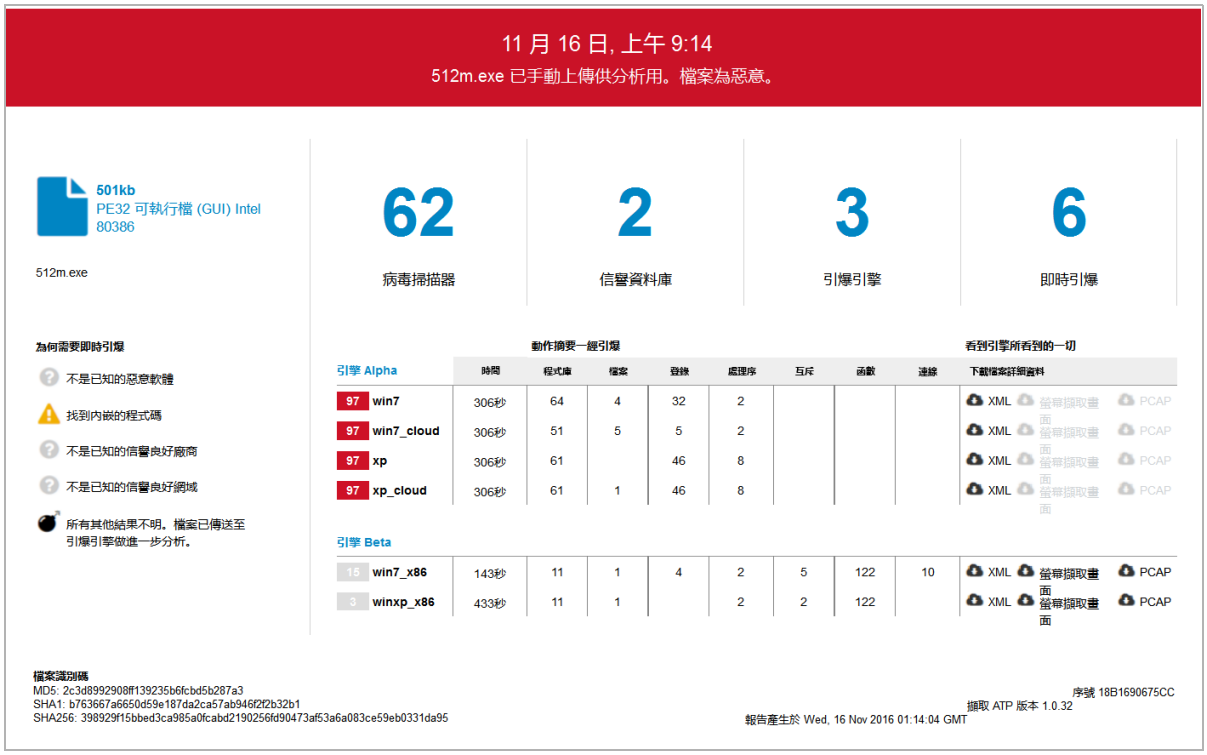
如果病毒掃描器在檔案中偵測到已知的惡意軟體，所有的惡意軟體名稱會列示在報告的內容區域中。

惡意軟體名稱

11 的 25 個病毒掃描器偵測到已知的惡意軟體。

Unwanted/Win32.Agent	antivir_detected
Generic36.BZFE (Trojan horse)	Trojan.GenericKD.2696853
PUA.Win32.Packer.Exe-2	Trojan.GenericKD.2696853
Trojan.Rogue	Riskware (0040eff71)
Trojan.Win32.Generic!BT	TROJ_GEN.R08JB01AL16
Trojan.Rogue!YC7ojpps/rU (trojan)	

檢視完整分析的威脅報告



11 月 16 日, 上午 9:14

512m.exe 已手動上傳供分析用。檔案為惡意。

501kb
PE32 可執行檔 (GUI) Intel 80386

512m.exe

62 病毒掃描器

2 信譽資料庫

3 引爆引擎

6 即時引爆

為何需要即時引爆

- 不是已知的惡意軟體
- 找到內嵌的程式碼
- 不是已知的信譽良好廠商
- 不是已知的信譽良好網域
- 所有其他結果不明。檔案已傳送至引爆引擎做進一步分析。

動作摘要—經引爆

看到引擎所看到的一切

引擎 Alpha

	時間	程式庫	檔案	登錄	處理序	互斥	函數	連線	下載檔案詳細資料
97 win7	306秒	64	4	32	2				XML 螢幕擷取畫面 PCAP
97 win7_cloud	306秒	51	5	5	2				XML 螢幕擷取畫面 PCAP
97 xp	306秒	61		46	8				XML 螢幕擷取畫面 PCAP
97 xp_cloud	306秒	61	1	46	8				XML 螢幕擷取畫面 PCAP

引擎 Beta

15 win7_x86	143秒	11	1	4	2	5	122	10	XML 螢幕擷取畫面 PCAP
3 winxp_x86	433秒	11	1		2	2	122		XML 螢幕擷取畫面 PCAP

檔案識別碼
MD5: 2c3d8992908ff139235b6fcbd5b287a3
SHA1: b763667a6650d59e187da2ca57ab946f2f2b32b1
SHA256: 398929f15bbed3ca985a0fcabd2190256fd90473af53a6a083ce59eb0331da95

序號 18B1690675CC
擷取 ATP 版本 1.0.32
報告產生於 Wed, 16 Nov 2016 01:14:04 GMT

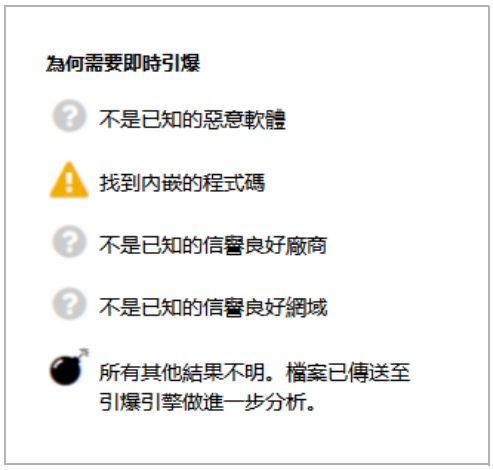
完整分析威脅報告為惡意及非惡意檔案提供同一組資訊，只有橫幅顏色不同。當發生以下情況，便會使用此威脅報告格式：

- 病毒掃描結果不明或良好。
- 檔案中有內嵌代碼。
- 檔案不符合網域或廠商允許清單。

主題：

- 為何需要即時引爆
- 狀況方塊
- 分析引擎結果表格

為何需要即時引爆



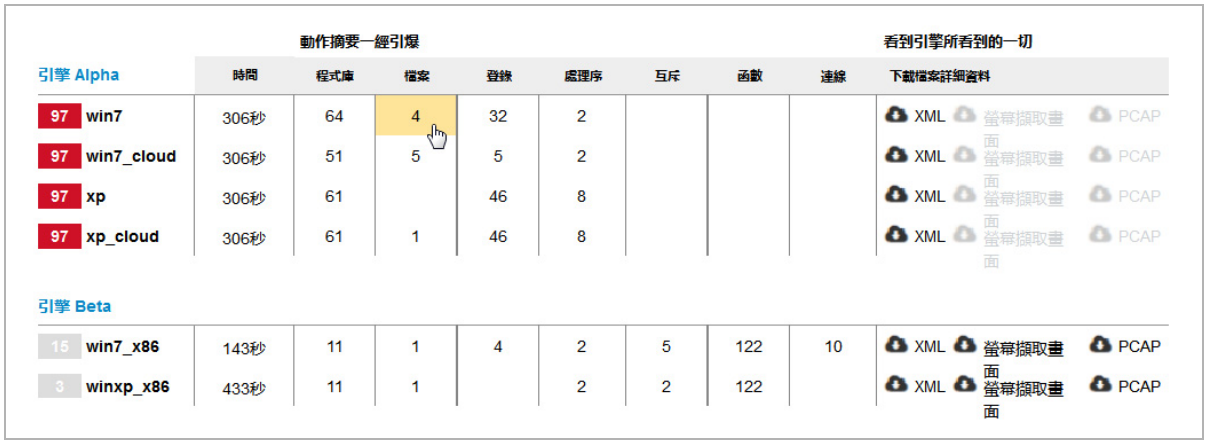
完整分析威脅報告左側顯示前置處理結果的總結，說明為何需要即時引爆。即時引爆這個詞的含意是指同時使用一個或多個分析引擎及多個環境來分析雲端伺服器中的檔案。

狀況方塊

病毒掃描器	此為防毒軟體廠商所採用的數字，無關於各自的判斷。 SonicWall 閘道防毒及雲端防毒各自算成一個。 許多 AV 產品和線上掃描引擎的其他病毒掃描器，全計入總數。
信譽資料庫	一個是廠商允許清單。 一個是網域允許清單。
引爆引擎	用於分析檔案的分析引擎數。 一個是 SonicWall 分析引擎。 協力廠商的其他分析引擎內含在計數中。
即時引爆	跨所有分析引擎所使用的環境總數。 環境是由分析引擎及供其執行之作業系統所組成。

完整分析威脅報告中的狀態方塊顯示前置處理結果的狀態，以及雲端伺服器中執行之分析的相關資訊。

分析引擎結果表格



在狀態方塊下，完整分析威脅報告會顯示多個表格，其中呈現每個分析引擎的結果。引擎是以希臘字母指定名稱，例如 Alpha、Beta、Gamma 等等。

每一列代表不同的環境，並指出執行引擎的作業系統。

每一個環境的分析總評分顯示在作業系統左方的亮顯方塊中。方塊顏色指出分數是否觸發惡意或非惡意判斷：

- 紅色指惡意判斷。
- 灰色指非惡意判斷。

一旦引爆，資料行會針對每一個環境提供分析持續時間和操作摘要：

時間	分析所用時間，s 代表秒鐘，m 代表分鐘，如果分析未完成則逾時。
程式庫	分析期間讀取的惡意軟體程式庫的累加計數。
檔案	建立、讀取、更新或刪除的檔案累加計數。
登錄	分析期間讀取的 OS 登錄累加計數。
處理序	分析期間建立的處理序累加計數。
互斥	分析期間使用的互斥物件的累加計數，用於鎖定獨佔存取的資源。
函數	分析期間執行的函數累加計數。
連線	分析期間建立的網路連線累加計數。

您可以按選**操作摘要**表格中的儲存格，跳至報告下方的完整資料。空白儲存格無法按選。

按下最後欄位中的項目，提供檔案的存取，其中包含依不同引擎進行分析的完整細節，您可以開啟或儲存：

XML	上述計數後所有詳細資料的 XML 檔。
螢幕擷取畫面	分析所產生的所有螢幕擷取畫面的 Zip 檔。
PCAP	pcapNG 或 libpcap 格式的封包捕獲檔案，含有分析期間所開啟連線的細節。

14

設定捕獲 ATP

重要：擷取進階威脅防護 (ATP) 是防火牆的附加安全性服務，類似閘道防毒 (GAV)，有助於防火牆辨識檔案是否為惡意。

所有 SuperMassive 系列、NSA 系列和執行 SonicOS 6.5 或更新版本的 TZ600 和 TZ500/TZ500W 防火牆均支援捕獲 ATP。但是，在主動/主動 DPI 模式中不支援捕獲功能。

在啟用捕獲 ATP 之前，您必須先取得授權，而且必須啟用閘道防毒 (GAV) 和雲端防毒資料庫服務。授權捕獲 ATP 後，您可以在您的 MySonicWall 帳戶中檢視捕獲 ATP 狀態，以及設定和接收警示和通知。

如需有關捕獲 ATP、其授權和使用您的 MySonicWall 帳戶設定和接收警示和通知的詳細資訊，請參閱 *SonicOS 6.5 捕獲進階威脅防護功能指南*。

主題：

- 關於捕獲 ATP
- 啟用捕獲 ATP 授權
- 啟用捕獲 ATP
- 關於捕獲 ATP > 設定頁面

- 設定捕獲 ATP
- 停用 GAV 或雲端防毒

關於捕獲 ATP

主題：

- 關於捕獲 ATP
- 檔案已做前置處理
- 封鎖檔案直到完全分析
- 檔案會經由加密的連線傳送

關於捕獲 ATP

捕獲進階威脅防護 (Capture Advanced Threat Protection，ATP) 透過傳輸檔案到雲端，讓 SonicWall 捕獲 ATP 服務分析檔案以判斷檔案中是否包含病毒或其他惡意元件，藉此協助防火牆識別檔案是否為惡意。然後，捕獲 ATP 會將結果傳送到防火牆。分析和報告是在防火牆處理檔案時，即時完成。

所有的檔案會經由加密的連線傳送到捕獲 ATP 雲端。檔案會在判定後的幾分鐘內進行分析和刪除，除非發現該檔案是惡意的。惡意檔案會透過加密的 HTTPS 連線提交給 SonicWall 威脅研究團隊，做進一步分析以及取得威脅資訊。檔案不會傳送至任何其他地點進行分析。在接收後的 30 天內取得威脅資訊，惡意檔案即刪除

捕獲 ATP 提供檔案分析報告 (威脅報告)，其內含詳細的威脅行為資訊。

防火牆位於您的內部部署，而捕獲 ATP 伺服器和資料庫則位於 SonicWall 設備。在傳輸資料之前，防火牆會建立與捕獲 ATP 雲端服務的安全連線。

捕獲 ATP 可配合閘道防毒 (GAV) 和雲端防毒服務工作。

如需捕獲 ATP 的詳細資訊，請參閱 SonicOS 6.2.6 捕獲進階威脅防護功能指南。

檔案已做前置處理

所有提交給進行分析的檔案會先由 GAV 服務進行前置處理，以判斷檔案為惡意或良性。您也可以使用 GAV 設定來選擇或定義要排除於 GAV 和「捕獲 ATP」掃描範圍的位址物件。

「捕獲 ATP」不會對要進行判斷為惡意或良性的前置處理檔案進行分析。如果檔案在前置處理過程中未判斷出為惡意或良性，就會將檔案提交給捕獲 ATP 進行分析。

封鎖檔案直到完全分析

對於 HTTP/HTTPS 下載，捕獲 ATP 具有**在得到判定前攔截文件下載**選項，可確保在檔案完全分析和判定為惡意或良性之前不會有封包通過。檔案會保留到最後封包被分析為止。如果檔案含惡意程式碼，會丟棄最後一個封包，並將檔案封鎖。威脅報告提供必要資訊來回應某個威脅或感染。

檔案會經由加密的連線傳送

所有的檔案會經由加密的連線傳送到捕獲 ATP 雲端。SonicWall 不會保留檔案。所有的檔案檔型無論是惡意或良性，在經過某段特定時間後，便會從捕獲 ATP 伺服器移除。

SonicWall 隱私政策可在以下網址進行存取：https://www.mysonicwall.com/privacypolicy.aspx。

啟用捕獲 ATP 授權

重要： 捕獲 ATP 需要閘道防毒服務而其該服務也必須獲得授權。

啟用捕獲 ATP 服務授權之後，**捕獲 ATP** 會出現在 DPI-SSL 下方的 SonicOS 左側瀏覽面板。如果捕獲 ATP 未被授權，就完全不會出現在左側瀏覽面板。

附註：如果在啟用捕獲 ATP 服務授權後未短暫出現**捕獲 ATP**，可在**更新 | 授權**頁面上按一下**同步**按鈕。

若要啟用授權，請移至**更新 | 授權**頁面，即可檢視所有服務授權和啟動捕獲 ATP 的授權。如需授權的更多資訊，請參閱 *SonicWall SonicOS 6.5 更新*。

啟用捕獲 ATP

重要：您在啟用捕獲 ATP 之前，必須先啟用閘道防毒和雲端防毒。

當捕獲 ATP 獲得授權但未啟用時，橫幅會顯示此訊息：

「捕獲 ATP」目前並未執行。請參閱下方的「基本設定檢查清單」以進行故障排除。

在停用模式中，會顯現**基本設定檢查清單**區段，但其他區段會停用。

若要啟用捕獲 ATP：

1. 導覽至**安全設定 | 安全服務 > 閘道防毒**。
2. 如管理 SonicWall 閘道防毒服務中所述啟用閘道防毒 (GAV) 和雲端防毒二者。
3. 或者，您可以設定 GAV 和雲端防毒設定，這也會套用到捕獲 ATP。
4. 導覽至**捕獲 ATP > 設定**。如果捕獲 ATP 未啟用，會顯示警告訊息：

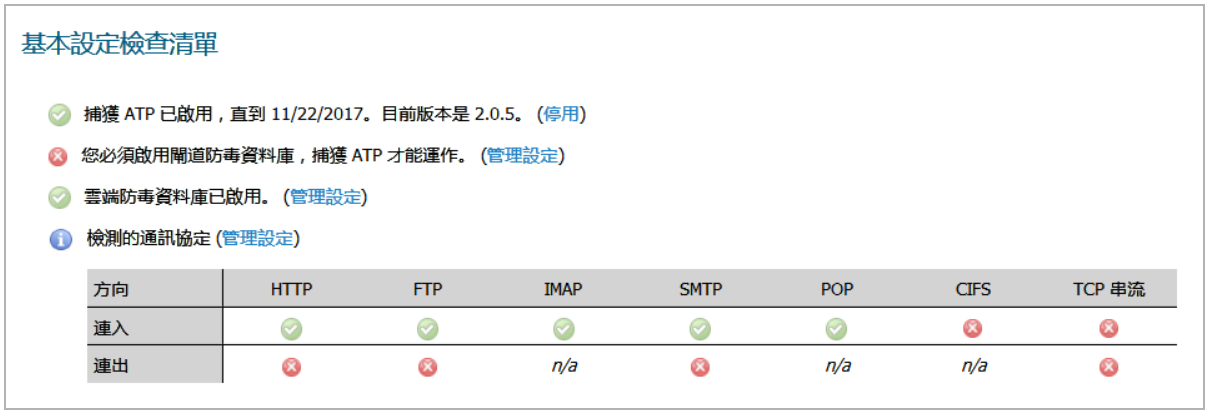
5. 在**基本設定檢查清單**區段中，按下 (**啟用它**) **捕獲 ATP 訂閱有效期限為 *date*，但該服務目前未啟用。** (**啟用它**)。警告訊息會消失而狀態指示器會轉為綠色勾選標記。

關於捕獲 ATP > 設定頁面

主題：

- 基本設定檢查清單
- 頻寬管理
- 排除
- 自訂封鎖行為

基本設定檢查清單



基本設定檢查清單：

- 顯示捕獲 ATP 及其元件、GAV 和雲端防毒的狀態。
- 顯示可能出現的任何錯誤狀態。
- 可啟用或停用捕獲 ATP 服務。
- 對於 GAV、雲端防毒和通訊協定檢測設定提供連到**安全性服務 > 閘道防毒**頁面的連結。
- 顯示通訊協定檢測設定的矩陣以及是否已啟用傳入和傳出方向。

附註：如需在此區段中顯示的訊息，請參見捕獲 ATP 狀態表格至通訊協定檢查設定表格。**已啟用**對應至綠色勾選標記，而**已停用**對應至紅色 X。

捕獲 ATP 狀態

圖示	訊息	連結	操作
啟用	捕獲 ATP 服務已啟用，直到 *renewal_date*。	停用	按下連結關閉捕獲 ATP 並使服務進入停用模式。您不需要按下**接受**即可套用此變更。
已停用	捕獲 ATP 訂閱有效期限為 *renewal_date*，但該服務目前未啟用。	啟用	按下連結開啟捕獲 ATP 並使服務進入啟用模式。您不需要按下**接受**即可套用此變更。
已停用	捕獲 ATP 訂閱將於 *renewal_date* 到期。	更新	按下連結移至 MySonicWall 以更新服務。

閘道防毒狀態

圖示	訊息	連結	操作
啟用	閘道防毒已啟用。	管理設定	按下連結以顯示「安全性服務 > 閘道防毒」頁面。
已停用	您必須啟用閘道防毒，捕獲 ATP 才能運作。	管理設定	按下連結以顯示「安全性服務 > 閘道防毒」頁面。

雲端防毒資料庫狀態

圖示	訊息	連結	操作
啟用	雲端防毒資料庫已啟用。	管理設定	按下連結以顯示**安全性服務 > 閘道防毒**頁面。
已停用	您必須啟用雲端防毒資料庫，捕獲 ATP 才能運作。	管理設定	按下連結以顯示**安全性服務 > 閘道防毒**頁面。

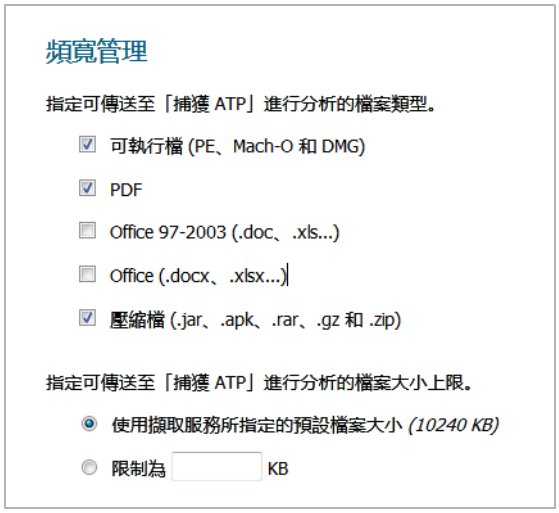
檢測的通訊協定表格也提供管理設定連結，可將您帶到安全服務 > 閘道防毒頁面。您可在該頁面啟用或停用特定網路流量通訊協定的檢查，包括 HTTP、FTP、IMAP、SMTP、POP、CIFS 和 TCP 串流。每個通訊協定可針對連入和連出流量分別管理。

下表**檢查的通訊協定**顯示每個方向各個通訊協定的目前檢查設定；請參見通訊協定檢查設定。

通訊協定檢查設定

圖示	訊息
啟用	通訊協定已檢查。
已停用	通訊協定未檢查。
n/a	檢查不適用於此方向的這個通訊協定。

頻寬管理



頻寬管理區段可讓您選擇可提交給捕獲 ATP 的檔案類型，以及指定所提交檔案的大小上限。您也可以指定要從檢查中排除的位址物件。

預設只有啟用**可執行檔 (PE、Mach-O 和 DMG)** 檔案類型。

檔案大小上限的預設選項是**使用擷取服務所指定的預設檔案大小 (10240 KB)**。這會指定此 10 MB 的檔案大小限制。

如果選擇**限制為 KB**，您可以輸入您自己的自訂值。此值必須為非零值，並且不得大於預設限制。

對於**選擇從捕獲 ATP 排除的位址物件**，選擇性從下拉清單選擇位址物件，或者選擇選項建立新的位址物件。捕獲 ATP 服務會將所選位址物件的成員從檢查中排除。

排除

排除區段可讓您從捕獲 ATP 排除位址物件或 MD5 雜湊函數。

若要排除位址物件：

1 從下拉功能表中選擇位址物件，或建立一個新的位址物件。

2 按一下**接受**。

若要排除 MD5 檔案：

1 按下 **MD5 排除清單設定**按鈕。隨即顯示**新增 MD5 排除**對話。

2 新增要排除的 32-hexadecimal-digit 雜湊函數。

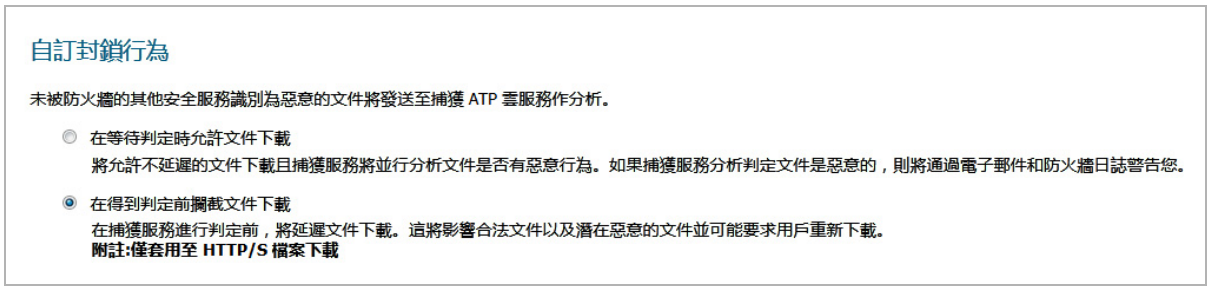
3 按下**新增**。

4 若要新增一個以上的檔案，請針對每個雜湊函數重複步驟 2 和步驟 3。

5 按一下**確定**。

6 按一下**接受**。

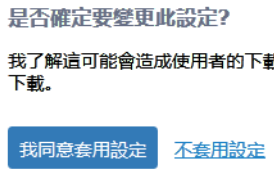
自訂封鎖行為



自訂封鎖行為區段可讓您選擇**在得到判定前攔截文件下載**功能。

預設選項是**在等待判定時允許文件下載**。此設定允許檔案下載而無延遲，同時捕獲服務分析檔案是否含有惡意元件。您可以設定電子郵件警示或檢查防火牆記錄，以得知捕獲服務分析是否判定檔案為惡意。

在得到判定前攔截文件下載功能應只有在想要最嚴格的控制時啟用。如果選擇此功能，會顯示警告對話方塊。

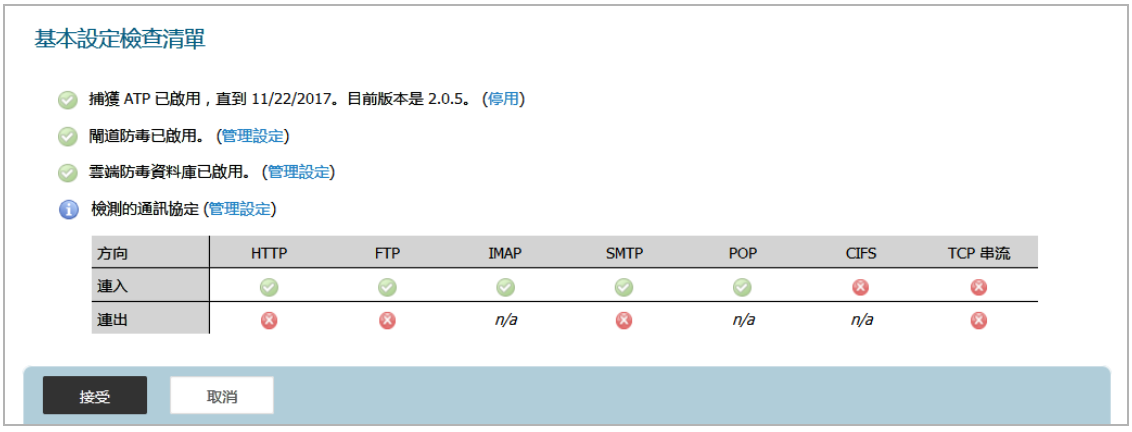


附註：在得到判定前攔截文件下載選項僅適用於 HTTP 和 HTTPS 下載。

設定捕獲 ATP

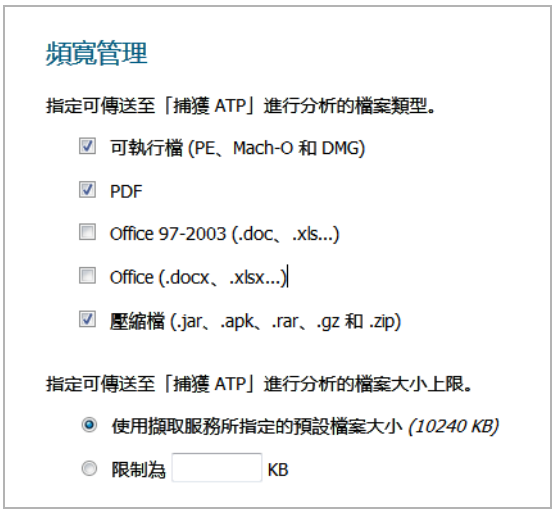
若要設定捕獲 ATP：

1 導覽至捕獲 ATP > 設定。



2 確保捕獲 ATP、GAV、雲端防毒資料庫和相關通訊協定已啟用。

3 在**頻寬管理**區段中，選擇要由捕獲 ATP 進行分析的檔案類型。預設只選擇**可執行檔 (PE、Mach-O 和 DMG)**。



4 預設選擇了**使用擷取服務所指定的預設檔案大小 *(10240 KB)***。若要指定自訂大小，請在**限制為 KB** 欄位中輸入 1 到 10240 之間的值。

5 (選擇性) 若要從捕獲 ATP 排除位址物件，請從**選擇從捕獲 ATP 排除的位址物件**下拉功能表選擇位址物件。

6 (選擇性) 若要根據其 MD5 總和檢查碼排除檔案，請按下 **MD5 排除清單設定**按鈕，以顯示**新增 MD5 排除**對話。

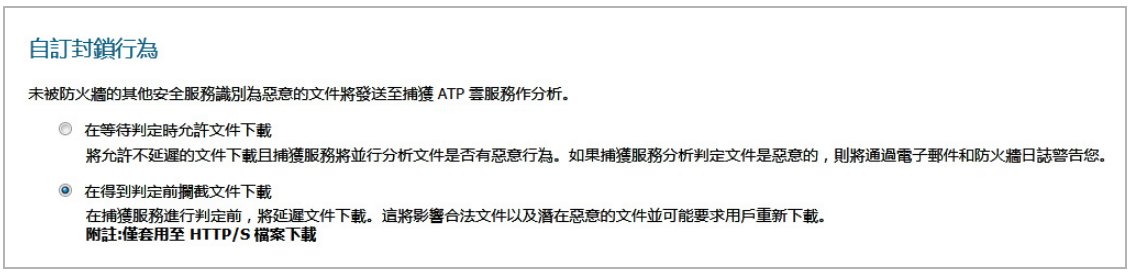
   a 新增 32 位的十六進位雜湊到 **MD5** 欄位。

   b 按一下**新增**。

   c 對每個要排除的檔案，重複步驟 a 和步驟 b。

   d 按一下**確定**。

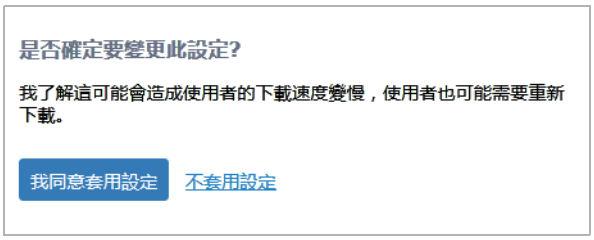
7 如果您將分析 HTTP/HTTPS 檔案，在**自訂封鎖行為**區段中您可以指定是否封鎖所有檔案直到分析完成為止。



預設選擇**在等待判定時允許文件下載**。

重要：在得到判定前攔截文件下載功能應只有在想要最嚴格的控制時啟用。

如果選擇此功能，會顯示警告對話方塊。



按一下：

- **我同意套用設定**按鈕會選擇**在得到判定前攔截文件下載**選項。您也必須按**接受**按鈕才能讓變更生效。
- **不套用設定**連結關閉對話方塊並保持勾選**在等待判定時允許文件下載**。

8 按一下**接受**。

停用 GAV 或雲端防毒

您可以將**安全設定 | 安全服務 > 閘道防毒**頁面上的閘道防毒或雲端防毒服務核取記號清除，即可停用閘道防毒或雲端防毒服務。如果在啟用捕獲 ATP 的同時停用任一種服務，會顯示快顯訊息來警告您捕獲 ATP 也會停用。

如果停用閘道防毒或雲端防毒，捕獲 ATP 會停止運作。例如，若未啟用閘道防毒，**捕獲 ATP > 設定**頁面會顯示**您必須啟用閘道防毒，捕獲 ATP 才能運作**與一個管理設定連結，將您引導至**安全服務 > 閘道防毒**頁面，讓您在該頁面啟用它。

15

啟用防間諜軟體服務

主題：

- 防間諜軟體概述
- 啟用防間諜軟體服務防護

防間諜軟體概述

SonicWall 防間諜軟體是 SonicWall 閘道防毒、防間諜軟體和入侵保護服務解決方案的一部分，此解決方案對病毒、蠕蟲病毒、特洛伊木馬、間諜軟體和軟體漏洞提供了全面的即時防護。

SonicWall 防間諜軟體服務可通過切斷間諜軟體的安裝來防止網路出現入侵的間諜軟體，可在閘道處提交，並可拒絕先前已安裝的間諜軟體向外傳送所收集的資訊。SonicWall 防間諜軟體與其他防間諜程式（例如用於從主機移除現有間諜軟體應用程式的程式）協同工作。您最好使用或安裝基於主機的防間諜軟體作為抵禦間諜軟體的附加措施。

SonicWall 防間諜軟體分析用於最常見間諜軟體傳送方法和基於 ActiveX 的元件安裝的傳入連接。它還檢驗經過閘道的傳入設定可執行檔案和 Cabinet 檔案，並重設將間諜軟體設定檔案串流傳送至 LAN 的連接。這些檔案套件可能是組合了廣告程式、按鍵記錄器或其他間諜軟體的免費軟體。

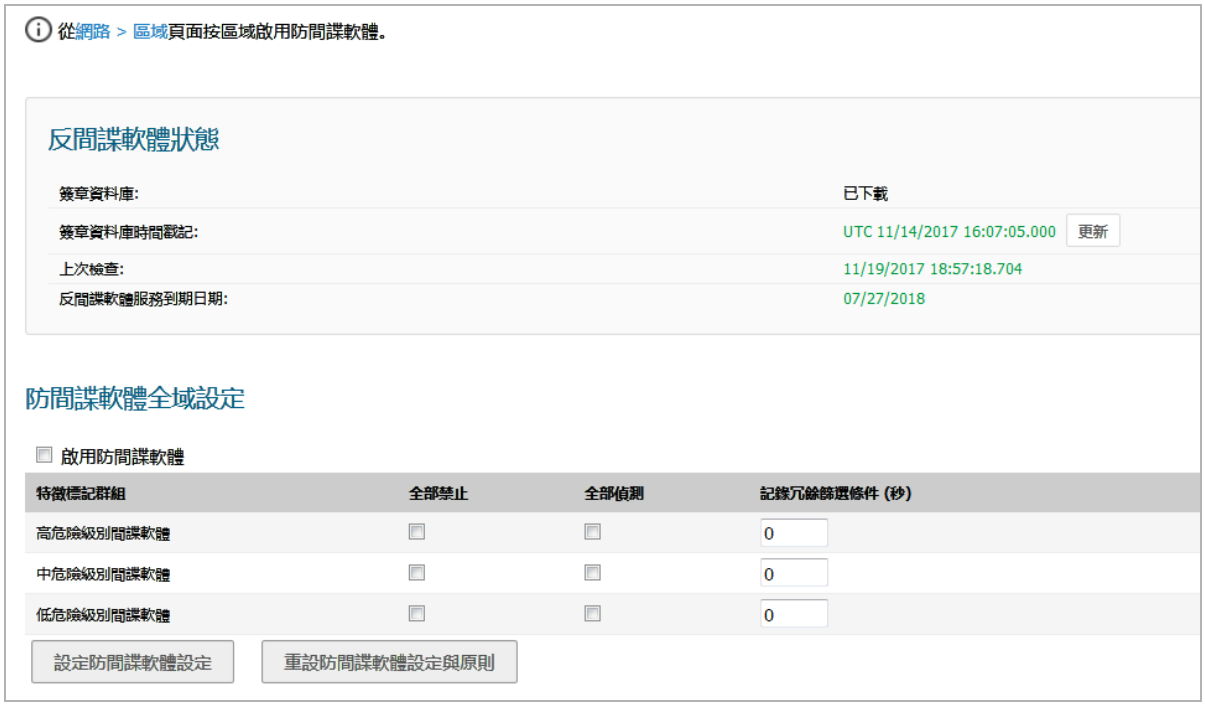
如果 LAN 工作站在安裝防間諜軟體服務之前已經安裝間諜軟體，此服務將檢查傳出通訊是否存在來自已感染間諜軟體的用戶端的資料流，如存在，就重設這些連接。例如，當間諜軟體分析了使用者的瀏覽習慣並嘗試發回使用者個人資料資訊時，防火牆會識別此流量並重設連接。

SonicWall 防間諜軟體服務提供以下防護：

- 封鎖通過 ActiveX 自動安裝元件傳送的間諜軟體，這是散佈惡意間諜軟體的最常見手段。
- 掃描並記錄通過網路傳送的間諜軟體威脅，並在刪除和/或封鎖新的間諜軟體時通知管理員。
- 封鎖現有的間諜軟體程式與網際網路上的駭客和伺服器進行背景通訊，從而防止機密資訊洩漏。
- 通過授予管理員有選擇性允許或拒絕個人間諜軟體程式安裝的權利，提供對網路應用程式的精確控制。
- 通過掃描和封鎖 SMTP、IMAP 或基於 Web 的電子郵件傳送受感染的電子郵件，防止電子郵件中間諜軟體的威脅。

啟用防間諜軟體服務防護

安全服務 > 防間諜軟體頁面顯示用於管理您的 SonicWall 安全裝置上的服務的設定。



安全服務 > 防間諜軟體頁面分為三區段：

- **反間諜軟體狀態** - 顯示有關特徵標記資料庫的狀態資訊、您的 SonicWall 防間諜軟體授權及其他資訊。
- **防間諜軟體全域設定** - 提供一些關鍵設定用於啟用 SonicWall 安全裝置上的 SonicWall 防間諜軟體，根據三種間諜軟體級別指定全域 SonicWall 防間諜軟體防護及其他設定選項。
- **防間諜軟體原則** - 用於查看 SonicWall 防間諜軟體特徵，以及設定按類別組或逐個特徵處理的方法。類別是基於產品或製造商組合到一起的特徵。

附註：在啟用 SonicWall 防間諜軟體授權後，您必須在 SonicWall 管理介面啟用和設定防間諜軟體，才能對網路流量應用防間諜軟體原則。

主題：

- 反間諜軟體狀態
- 防間諜軟體全域設定
- 對區域套用防間諜軟體防護
- 防間諜軟體原則
- 設定類別原則
- 設定特徵原則

反間諜軟體狀態

反間諜軟體狀態部分顯示特徵標記資料庫的狀態，包括資料庫時間戳記以及 SonicWall 特徵伺服器上次檢查最新特徵的時間。SonicWall 安全裝置會在啟動時，以及之後每小時自動嘗試同步資料庫。

- **特徵標記資料庫** - 指示已下載到 SonicWall 安全裝置的特徵標記資料庫。
- **特徵標記資料庫時間戳記** - 顯示上次更新特徵標記資料庫的日期和時間。**特徵標記資料庫時間戳記**指的是上次更新 SonicWall 防間諜軟體資料庫的時間，而不是上次更新 SonicWall 安全裝置的時間。

- **上次檢查** - 顯示 SonicWall 安全裝置上次查找特徵更新的時間。
- **防間諜軟體到期日期** - 顯示您的 SonicWall 防間諜軟體授權的到期日。如果您的 SonicWall 防間諜軟體訂閱過期，則將停止 SonicWall 防間諜軟體檢查，且會從 SonicWall 安全裝置中移除 SonicWall 防間諜軟體設定。在更新 SonicWall 防間諜軟體授權後，這些設定自動恢復至之前的設定狀態。

以下注釋中包含指向**網路 > 區域**頁面的連結，您可以在此頁面中設定個別區域的防間諜軟體：

附註：從系統安裝 | 網路 > 區域頁面按區域啟用防間諜軟體。

防間諜軟體全域設定

防間諜軟體全域設定面板使您可以基於下列攻擊級別在全域防範和/或偵測攻擊：

- **高危險級別間諜軟體** - 此類間諜軟體應用程式對您的網路而言危險程度最高（例如按鍵記錄器或色情程式），或者可能包含安全漏洞。刪除難度可能極高，甚至無法刪除。
- **中危險級別間諜軟體** - 此類間諜軟體應用程式可能導致網路中斷，例如增加網路流量致使效能下降。刪除難度可能極高。
- **低危險級別間諜軟體** - 此類間諜軟體應用程式的特徵是入侵活動較少，並且不構成直接威脅。它們可能儘量避免引起使用者注意，通常比較容易移除。

提示：SonicWall 推薦對**高危險級別間諜軟體**和**中危險級別間諜軟體**啟用**全部禁止**，以確保網路防範破壞性最高的間諜軟體。

防間諜軟體防護提供兩種方法管理全域間諜軟體威脅：偵測（**全部偵測**）和防護（**全部禁止**）。對於出現在 SonicWall 安全裝置全域級別的防間諜軟體，必須在其特徵標記群組面板中指定**全部禁止**操作。

在**特徵標記群組**面板中為某個特徵標記群組啟用**全部禁止**時，SonicWall 安全裝置會自動丟棄和重設此連接，以防止流量到達其目的地。

在**特徵標記群組**面板中為某個特徵標記群組啟用**全部偵測**時，SonicWall 安全裝置會記錄與組內任何特徵相符合的任何流量並發出警示，但不會對此流量採取任何操作。此連接將繼續抵達預期目的地。您可以在**記錄 > 檢視**頁面中查看 SonicWall 記錄，以及在**記錄 > 自動化**頁面中設定 SonicWall 安全裝置處理警示的方法。

注意：在僅選擇全部偵測時，請務必小心。僅選擇全部偵測將會記錄與群組內任何特徵相符合的流量並傳送警示，但不會對此流量採取任何操作。此流量將繼續抵達預期目的地。

在**特徵標記群組**面板中為某個特徵標記群組同時啟用**全部偵測**和**全部禁止**時，SonicOS 將會記錄與群組內任何特徵相符合的流量並傳送警示，同時自動丟棄和重設此連接，以防止流量到達目的地。

啟用輸出間諜軟體通訊檢查

啟用輸出間諜軟體通訊檢查選項可用於掃描傳出的間諜軟體通訊流量。

對區域套用防間諜軟體防護

如果您的防火牆正在執行 SonicOS，您在**網路 > 區域**頁面對區域套用 SonicWall 防間諜軟體不僅會在各網路區域和 WAN 之間實施防間諜軟體，還會在內部區域之間實施。例如，在 LAN 區域啟用防間諜軟體可以對所有進出的 LAN 流量實施防間諜軟體。

在**安全服務 > 防間諜軟體**頁面的上方，按一下**網路 > 區域**連結，以存取**系統安裝 | 網路 > 區域**頁面。您將對**網路 > 區域**頁面上列出的區域之一套用防間諜軟體。

在區域中啟用防間諜軟體：

1 在防火牆管理介面上，導覽至**系統安裝 | 網路 > 區域**頁面。（或從**安全服務 > 入侵保護**頁面的**反間諜軟體狀態**部分，按一下**網路 > 區域**連結）。顯示**網路 > 區域**頁面。

2 在**區域設定**面板的**設定**列中，按一下您要套用 SonicWall 防間諜軟體的區域的**編輯**圖示。顯示**編輯區域**視窗。

3 按一下**啟用防間諜軟體**核取方塊。顯示複選標記。若要停用 SonicWall 防間諜軟體，清除此核取方塊。

4 按一下**確定**。

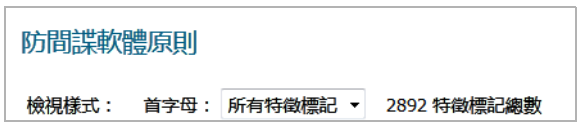
您還可以在**網路 > 區域**頁面對建立的新區域啟用 SonicWall 防間諜軟體防護。按一下**新增**按鈕顯示**新增區域**視窗，其中包含與**編輯區域**視窗相同的設定。

防間諜軟體原則

防間諜軟體原則部分用於查看和管理 SonicWall 防間諜軟體如何採取按類別組或逐個特徵的方式處理特徵。類別是按產品或製造商組合到一起的特徵，它們在**檢視樣式**功能表中列出。

防間諜軟體原則面板中列出的項目來自已下載到您防火牆的 SonicWall 防間諜軟體特徵標記資料庫。類別和特徵由防間諜軟體服務動態更新。類別和特徵會隨著時間的推移動態改變以應對新的威脅。

您可以使用**檢視樣式**功能表以多種檢視形式顯示特徵。此功能表用於指定在**防間諜軟體原則**面板中顯示的類別或特徵。您可以選擇**所有特徵標記**，或者選擇間諜軟體名稱的第一個字母或數字。



從功能表中選擇**所有特徵標記**將會按類別顯示所有特徵標記。**防間諜軟體原則**面板中顯示了所有類別及其特徵。通過類別標題分隔特徵項目。這些標題在**防護**和**偵測**列中顯示**全域**，表示您在**防間諜軟體全域設定**部分定義的全域設定。

主題：

- 防間諜軟體原則面板
- 顯示間諜軟體資訊
- 瀏覽防間諜軟體原則面板
- 搜尋特徵標記資料庫
- 對類別或特徵項目進行排序

防間諜軟體原則面板

防間諜軟體原則面板顯示了關於每個特徵項目的下列資訊：

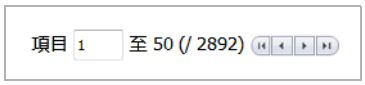
- **產品** - 顯示間諜軟體名稱或製造商。
- **名稱** - 以連結方式顯示間諜軟體的名稱。按一下此名稱連結可顯示關於此間諜軟體的 SonicAlert 資訊。
- **ID** - 特徵對應的 SonicWall 資料庫 ID 號。
- **防護** - 此列中的複選標記表示已啟用防護。任何時候在您變更全域或類別防護設定時，**偵測**列都會出現一個綠色複選標記。
- **偵測** - 此列中的複選標記表示已啟用偵測。任何時候在您變更全域或類別偵測設定時，**偵測**列都會出現一個綠色複選標記。
- **危險級別** - 按照**特徵標記群組**面板中的定義，將攻擊特徵定義為**低**、**中**或**高**。
- **註解** - 顯示原則的一般說明。
- **設定** - 按一下類別標題在**設定**列中的編輯圖示將會顯示**編輯防間諜軟體類別**視窗。按一下個別特徵在**設定**列中的編輯圖示將會顯示**編輯防間諜軟體簽章**視窗。這些視窗可用於定義與特定類別或特徵的全域設定不同的操作。

顯示間諜軟體資訊

在**防間諜軟體原則**面板中，按一下**名稱**列中的間諜軟體名稱連結將會顯示 **SonicALERT** 頁面，其中提供了關於此間諜軟體的詳細資料。

瀏覽防間諜軟體原則面板

項目欄位顯示第一個類別或特徵的面板編號。如果您顯示面板的第一頁，項目可能是第 1 至 50 個**項目**（共 58 個）。您可以在**項目**欄位中輸入數字，直接移至特定項目，或者使用瀏覽按鈕瀏覽面板。



SonicWall 防間諜軟體特徵在**防間諜軟體原則**面板中每頁顯示 50 個項目。

附註：您可以在 **Web 管理設定**部分的**系統安裝 | 設備 > 基本設定**頁面上，變更每面板 50 個項目的預設值。

搜尋特徵標記資料庫

您可以通過在**查詢特徵標記包含字串**欄位輸入搜尋字串，然後按一下圖示來搜尋特徵標記資料庫。

對類別或特徵項目進行排序

按一下**防間諜軟體原則**面板標題（**名稱**、**ID**、**防護**、**偵測**或**危險**級別）可根據標題對面板項目進行排序。列標題名稱旁邊的向上箭頭表示項目以遞減排列。列標題名稱旁邊的向下箭頭表示項目以遞增排列。

設定類別原則

您可以選擇按類別逐一覆寫全域防護和偵測設定。**全部禁止**和**全部偵測**全域設定（包括**高危險級別間諜軟體**、**中危險級別間諜軟體**和**低危險級別間諜軟體**）在**防間諜軟體全域設定**部分進行設定。類別中可能包含**特徵標記群組**面板中定義的任意危險級別組合。

可用的特徵類別在**防間諜軟體原則**部分的**檢視樣式**功能表中列出。按類別設定防護和偵測行為將會影響此類別中的所有特徵標記，而不論全域攻擊優先順序設定如何（低、中或高）

主題：

- 按類別覆寫全域防護和偵測設定
- 將 SonicWall 防間諜軟體設定重設為預設值

按類別覆寫全域防護和偵測設定

1 從**類別**功能表中選擇**所有類別**或單個類別：

2 如果選擇**所有類別**，請按一下需要變更的類別在**設定**欄位中的**編輯**圖示。即顯示**編輯防間諜軟體類別**對話。

3 如果選擇單個類別，請按一下**類別**功能表右側的**編輯**圖示。顯示**編輯防間諜軟體類別**對話。

4 如果您想要變更**防護**的全域設定，請從**防護**功能表中選擇**啟用**或**停用**。

5 如果您想要變更**偵測**的全域設定，請從**偵測**功能表中選擇**啟用**或**停用**。

6 如果您想要同時變更防護和偵測的全域設定，請從**偵測**和**防護**功能表中選擇**啟用**或**停用**。

7 下列設定可用於選擇需要在此 SonicWall 防間諜軟體類別中包含或排除的特定使用者/群組、IP 位址範圍及排程物件：

- **包含使用者/群組** - 選擇您想要在此包含的 SonicWall 防間諜軟體類別。預設值為**全部**。
- **排除使用者/群組** - 選擇您想要在此排除的 SonicWall 防間諜軟體類別。預設值為**無**。
- **包含 IP 位址範圍** - 選擇您想要在此 SonicWall 防間諜軟體類別中包含的 IP 位址範圍。預設值為**全部**。
- **排除 IP 位址範圍** - 選擇您想要在此 SonicWall 防間諜軟體類別中排除的 IP 位址範圍。預設值為**無**。
- **排程** - 選擇您想要啟用此 SonicWall 防間諜軟體類別的排程時間。預設值為**始終開啟**。

8 如果您想要變更預設全域設定的「記錄冗餘篩選條件」設定，請取消勾選**記錄冗餘篩選條件(秒數)**中的**使用類別設定**核取方塊，並輸入以秒為單位的時間值。

9 按一下**確定**以儲存您的變更。

提示：如果從**類別**功能表中選擇了**所有特徵標記**，則所有類別及其特徵都將顯示在**防間諜軟體原則**面板中，從而用於設定此類別及其中的特徵。

將 SonicWall 防間諜軟體設定重設為預設值

您可以通過按一下**防間諜軟體全域設定**部分中的**重設防間諜軟體設定與原則**按鈕，移除您所建立的所有自訂類別和特徵設定，以及重設全域**全部禁止**和**全部偵測**設定及**記錄冗餘篩選條件 (秒數)**設定。

設定特徵原則

從**類別**功能表中選擇**所有特徵標記**將會顯示在類別中組織的所有特徵標記。**所有特徵標記**選項將顯示防間諜軟體資料庫中的每個特徵。

如果類別的全域**全部禁止**和**全部偵測**設定已生效，則此類別及其所有特徵標記的**防護**和**偵測**列中都會顯示**全域**。

選擇特定特徵類別將顯示此類別中的特徵。

附註：您不能將自己的自訂特徵匯入到 SonicWall 防間諜軟體中，也不能刪除特徵項目。

注意：在覆寫高危險級別間諜軟體和中危險級別間諜軟體全域特徵行為時需要格外小心，因為這有可能造成漏洞。如果您在執行變更後想要恢復預設的全域特徵設定，請按一下重設防間諜軟體設定與原則按鈕還原預設值。

主題：

- 按類別覆寫全域防護和偵測設定
- 將 SonicWall 防間諜軟體設定重設為預設值

覆寫特徵的類別偵測和防護設定

若要覆寫特徵的類別偵測和防護屬性：

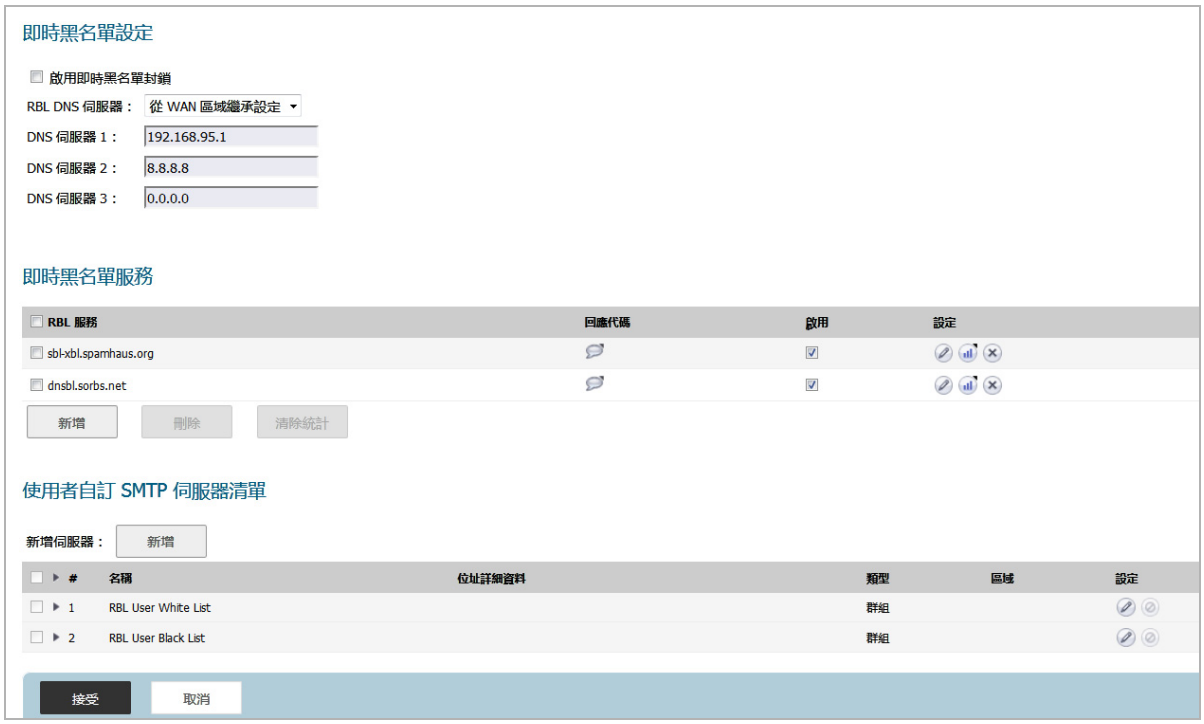
1. 在**防間諜軟體原則**面板中，顯示想要變更的特徵。按一下此項目在**設定**欄位中的**編輯**圖示，以顯示**編輯防間諜軟體**對話。
2. 如果您想要變更**防護**的類別設定，請從**防護**功能表中選擇**啟用**或**停用**。
3. 如果您想要變更**偵測**的類別設定，請從**偵測**功能表中選擇**啟用**或**停用**。
4. 如果您想要同時變更防護和偵測的類別設定，請從**偵測**和**防護**功能表中選擇**啟用**或**停用**。
5. 下列設定可用於選擇需要在此 SonicWall 防間諜軟體特徵中包含或排除的特定使用者/群組、IP 位址範圍及排程物件：
   - **包含使用者/群組** - 選擇您想要在此包含的 SonicWall 防間諜軟體類別。預設值為**全部**。
   - **排除使用者/群組** - 選擇您想要在此排除的 SonicWall 防間諜軟體類別。預設值為**無**。
   - **包含 IP 位址範圍** - 選擇您想要在此 SonicWall 防間諜軟體特徵中包含的 IP 位址範圍。預設值為**全部**。
   - **排除 IP 位址範圍** - 選擇您想要在此 SonicWall 防間諜軟體特徵中排除的 IP 位址範圍。預設值為**無**。
   - **排程** - 選擇您想要啟用此 SonicWall 防間諜軟體特徵的排程時間。預設值為**始終開啟**。
6. 如果您想要變更預設類別設定的「記錄冗餘篩選條件」設定，請取消勾選**記錄冗餘篩選條件(秒數)**中的**使用類別設定**核取方塊，並輸入以秒為單位的時間值。
7. 按一下**確定**以儲存您的變更。

將 SonicWall 防間諜軟體設定重設為預設值

您可以通過按一下**防間諜軟體全域設定**部分中的**重設防間諜軟體設定與原則**按鈕，移除您所建立的所有自訂類別和特徵設定，以及重設全域**全部禁止**和**全部偵測**設定及**記錄冗餘篩選條件 (秒數)**設定。

16

設定 SonicWall 即時黑名單



主題：

- 即時黑名單篩選
- 設定 RBL 篩選

即時黑名單篩選

SMTP 即時黑名單 (RBL) 是一種用於發佈 SMTP 垃圾郵件傳送者使用的 IP 位址的機制。有多個組織在編制此類資訊，有的免費提供，例如：http://www.spamhaus.org；有的則要收費，例如：https://ers.trendmicro.com/。

附註：SMTP RBL 是一種積極的垃圾郵件篩選技術，基於從已報告的垃圾郵件活動編制的清單，因此可能會產生誤報。SonicOS 實作的 SMTP RBL 篩選提供了多種微調機制有助於確保篩選的精確性。

RBL 清單供應商透過 DNS 發佈其清單。列入黑名單的 IP 位址出現在清單供應商 DNS 網域的資料庫中，使用相關 SMTP 伺服器的反轉 IP 作為網域名稱的首碼。127.0.0.2 至 127.0.0.9 的回應代碼表示某種類型的問題：

例如，如果 RBL 清單供應商 sbl-xbl.spamhaus.org 將 IP 位址為 1.2.3.4 的 SMTP 伺服器列入黑名單，則對 4.3.2.1.sbl-xbl.spamhaus.org 的 DNS 查詢將獲得 127.0.0.4 回應，表示此伺服器是已知的垃圾郵件來源，連接將中斷。

附註：當今的大部分垃圾郵件是從執行微弱 SMTP 伺服器實作的被綁架或僵屍機器傳送。與合法 SMTP 伺服器不同，這些僵屍機器很少嘗試重新傳送。一旦 RBL 篩選封鎖傳送嘗試，此垃圾郵件不再嘗試傳送。

設定 RBL 篩選

主題：

- 啟用 RBL 封鎖
- 新增 RBL 服務
- 設定使用者自訂 SMTP 伺服器清單
- 測試 SMTP IP 位址

啟用 RBL 封鎖

在 **RBL 篩選**頁面上的**即時黑名單設定**區段啟用**啟用即時黑名單封鎖**後，就會對照每個已啟用的 RBL 服務檢查來自 WAN 上主機的傳入連接或至 WAN 上主機的傳出連接，向 **RBL DNS 伺服器**下設定的 DNS 伺服器傳送 DNS 請求。

「RBL DNS 伺服器」功能表用於指定 DNS 伺服器。可以選擇**從 WAN 區域繼承設定**或**手動指定 DNS 伺服器**。如果選擇**手動指定 DNS 伺服器**，請在 **DNS 伺服器**欄位輸入 DNS 伺服器位址。

完成時，按一下**接受**。

會收集 DNS 回應並將之快取起來。如果任何查詢導致黑名單回應，將篩選此伺服器。回應利用 TTL 值進行快取，為非黑名單回應指派的快取 TTL 值為 2 小時。如果快取填滿，快取項目將按照 FIFO（先進先出）順序丟棄。

IP 位址檢查利用快取確定一個連接是否應中斷。最初，IP 位址不在快取中，必須傳送 DNS 請求。這種情況下，此 IP 位址適用「無罪推定」，檢查結果是允許連接。然後傳送 DNS 請求，結果在單獨的任務中將之快取起來。檢查來自此 IP 位址的後續封包時，如果將其列入黑名單，連接將中斷。

新增 RBL 服務

可以在**即時黑名單服務**區段新增更多 RBL 服務。

若要新增 RBL 服務，請按一下**新增**按鈕。在**新增 RBL 網域**視窗中，指定要查詢的 RBL 網域，啟用它並指定其預期回應代碼。多數 RBL 服務會在其網站上列出其提供的回應，不過選擇**封鎖所有回應**一般是可接受的。

RBL 服務表中會維護各 RBL 服務的統計資訊，滑鼠放在服務項目右側的（統計）圖示可以查看。

設定使用者自訂 SMTP 伺服器清單

使用者自訂 SMTP 伺服器清單允許使用位址物件來建立 SMTP 伺服器的白名單（明確允許）或黑名單（明確拒絕）。此清單中的項目將繞過 RBL 查詢程式。

附註：若要查看 RBL 使用者白名單清單和 RBL 使用者黑名單清單，按一下此清單核取方塊的向右箭頭。

主題：

- 設定白名單清單
- 設定黑名單清單

設定白名單清單

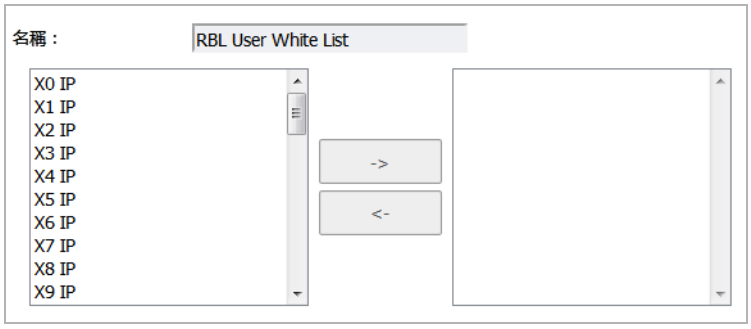
例如，為確保始終從合作夥伴網站的 SMTP 伺服器接收 SMTP 連接：

1 使用**新增伺服器： 新增**按鈕為伺服器建立位址物件。將打開**新增位址物件**視窗。

2 設定位址物件。

3 按一下**確定**。將位址物件新增到**使用者自訂 SMTP 伺服器清單**表格中的 **RBL User White List**。

4 按一下 **RBL User White List** 行的**設定**列的**編輯**圖示。顯示**編輯位址物件**視窗。



5 通過選擇位址物件並按一下向右箭頭來新增位址物件。

6 按一下**確定**。

表格將更新，此伺服器將始終能夠進行 SMTP 交換。

設定黑名單清單

1 按一下 **RBL User Black List** 行的**設定**列的**編輯**圖示。顯示**編輯位址物件**視窗。

2 通過選擇位址物件並按一下向右箭頭來新增位址物件。

3 按一下**確定**。

測試 SMTP IP 位址

調查檢視上的**工具 > 系統診斷**頁面，也提供了**即時黑名單查詢**功能，允許專門測試 SMTP IP 位址（或 RBL 服務、DNS 伺服器）。

如需用於測試的已知垃圾郵件來源清單，請參閱：http://www.spamhaus.org/sbl/latest/。

17

設定 Geo-IP 篩選條件

附註：TZ300 系列及以上裝置提供 Geo-IP 篩選功能。

Geo-IP 篩選功能用於封鎖來自/到達某地理位置的連接。SonicWall 防火牆使用 IP 位址來確定連接的位置。Geo-IP 篩選功能也可讓您建立影響 IP 位址識別的自訂國家/地區清單。

Geo-IP 篩選功能也可讓您在封鎖網站時建立自訂訊息。

您也可以使用 Geo-IP 篩選診斷功能，顯示解析的位置、監視 Geo-IP 快取統計資料、自訂國家/地區統計資料和查詢 GEO-IP 伺服器。

主題：

- 設定 Geo-IP 篩選
- 建立自訂國家/地區清單
- 自訂 Web 封鎖頁面設定
- 使用 Geo-IP 篩選診斷

設定 Geo-IP 篩選

若要設定 Geo-IP 篩選：

1 導覽至**安全設定 | 安全服務 > Geo-IP 篩選**頁面。

2 若要封鎖來自/到達某些國家的連接，選擇**封鎖來自/到達"國家/地區"標籤中所選取之國家/地區的連接**核取方塊。預設情況下已核取此選項。

如果啟用此選項，將會封鎖所有到達/來自所選國家的連接。可以指定排除清單為所選 IP 排除此行為，如下文步驟 10 中所述。

選擇此選項後，以下兩個選項可用。

3 為您的 Geo-IP 篩選選擇以下兩種模式中的一種：

- **所有連接**：篩選所有來自/到達防火牆的連接。預設情況下已核取此選項。
- **基於防火牆規則的連接**：只篩選和封鎖符合防火牆設定的存取規則的連接。

4 如果想在未下載 Geo-IP 資料庫時封鎖所有連接，請選擇**如果 GeoIP DB 未下載，阻止所有到公用 IP 的連接**選項。預設情況下未勾選此選項。

5 若要啟用您的自訂清單，請選擇**啟用自訂清單**核取方塊。預設情況下未勾選此選項。

如果**啟用自訂清單**核取方塊：

- 未勾選，則只會搜尋防火牆的國家/地區資料庫。移至步驟 6。
- 已勾選，則**依自訂清單覆寫防火牆國家/地區**核取方塊成為可用狀態。

透過勾選**啟用自訂清單**核取方塊來啟用自訂清單，可能影響 IP 位址的國家地區/識別。如果**依自訂清單覆寫防火牆國家/地區**：

- 也未勾選，則國家/地區識別會以此順序執行：
  1) 搜尋防火牆的國家/地區資料庫。如果未解析識別，則：
  2) 搜尋自訂國家/地區。
- 也勾選，則國家/地區識別會以此順序執行：
  1) 搜尋自訂國家/地區資料庫。如果未解析識別，則：
  2) 搜尋防火牆的國家/地區清單。

不論哪種狀況，會根據解析來採取行動。

6 若要記錄 Geo-IP 篩選相關的事件，請選擇**啟用記錄**。預設情況下未勾選此選項。

7 在**國家或地區**下的**選取的國家 / 地區**表中，選擇要封鎖的國家 / 地區。預設，不會封鎖任何國家 / 地區。

8 將**可用的國家/地區**表中選取的國家/地區拖曳到**選取的國家/地區**表。

附註：在**可用的國家/地區**表中選取後，會高亮顯示封鎖的國家/地區。

9 如果您要封鎖未列出的所有國家，請選擇**阻止所有的未知國家**選項。將封鎖所有到未知公用 IP 位址的連接。預設情況下未勾選此選項。

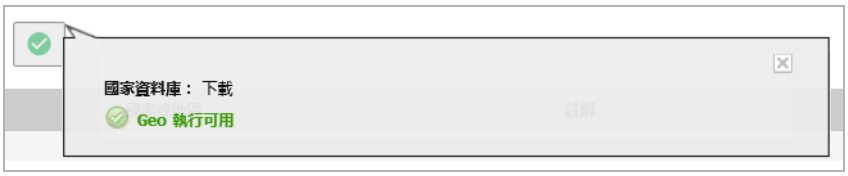
10 另外，通過執行以下其中一項操作，您也可以選擇對所有連接設定排除清單，使其不封鎖批准的 IP 位址：

- 從 **Geo-IP 排除物件**下拉功能表中選擇位址物件或位址群組。預設選項是 **Default Geo-IP and Botnet Exclusion Group**。
- 從 **Geo-IP 排除物件**下拉功能表中選擇**建立新位址物件...** 或**建立新位址群組...** 來建立新位址物件或位址群組。

  Geo-IP 排除物件是一個網路位址物件群組，用於指定從 Geo-IP 篩選封鎖中排除某個 IP 位址群組或範圍。即使來自受封鎖的國家/地區，允許此位址物件或位址群組中的所有 IP 位址。

  例如，如果將來自國家 A 的所有 IP 位址設為封鎖，且偵測到一個來自國家 A 的 IP 位址，但此位址在 **Geo-IP 排除物件**清單中，那麼將允許發往和來自此 IP 位址的流量。

  為了使這項功能正常工作，必須將國家資料庫下載到防火墻中。如果下載失敗，**自定義清單**頁面右上角的**狀態**指示燈會變黃色。綠色狀態表示已成功下載資料庫。按一下**狀態**按鈕顯示更多資訊。



  為了下載國家/地區資料庫，防火牆必須能夠解析位址 `utmgbdata.global.sonicwall.com`。

當使用者嘗試存取來自受封鎖國家/地區的網頁時，使用者 Web 瀏覽器上會顯示封鎖頁面訊息。

附註：如果與受封鎖國家的連接時間較短，防火牆沒有此 IP 位址的快取，可能不會立刻封鎖此連接。因此，與受封鎖國家的連接可能偶爾顯示在 AppFlow 監控上。但是，將立即封鎖與相同 IP 位址的再次連接。

11 按一下頁面頂部的**接受**按鈕以啟用變更。

建立自訂國家/地區清單

位址物件	指定給位址物件的名稱。
國家或地區	國家/地區的旗標圖示 (若知道的話) 和名稱。
註解	建立位址物件時會加上註解。
設定	包含**編輯**圖示和**刪除**圖示。
總計	顯示**自訂清單**中項目的數量。

IP 位址可能與錯誤國家或地區相關聯。此種錯誤分類可能導致不正確/不想要的 IP 位址篩選。透過覆寫與特定 IP 位址關聯的防火牆國家或地區，自訂國家/地區清單即可解決此問題。

主題：

- 建立自訂清單
- 編輯自訂清單項目
- 刪除自訂清單項目

建立自訂清單

重要：對於要使用自訂國家/地區清單的防火牆，您必須如設定 Geo-IP 篩選中所述啟用它。

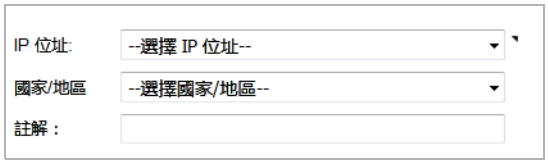
若要建立自訂國家/地區清單：

1 導覽至**安全設定 | 安全服務 > Geo-IP 篩選 > 設定**。

2 選擇**啟用自訂清單**。

3 按一下 **自訂清單**。

4 按下**新增**。將顯示**新增自訂清單**對話方塊。



5 從 **IP 位址**下拉功能表中選擇 IP 位址物件或建立新的位址物件。

重要：位址物件不可重疊自訂國家/地區清單中的任何其他位址物件。不過，不同位址物件可能具有相同的國家/地區 ID。

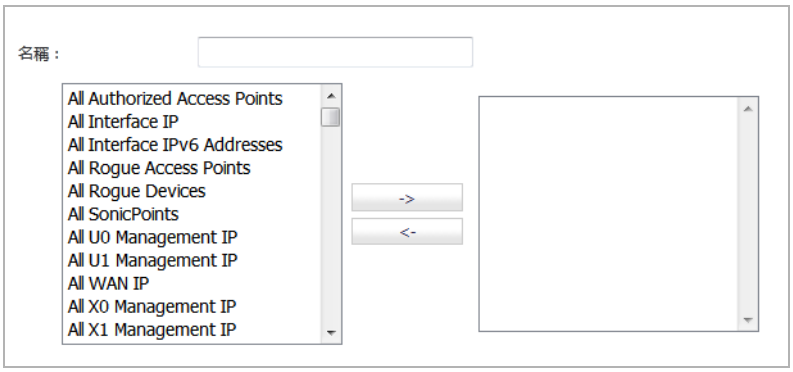
- **建立新位址物件...** - 顯示**新增位址物件**對話。

如 *SonicWall SonicOS 6.5 原則*中所述建立新的位址物件，並具備以下限制：

- 允許的類型為
  - **主機**
  - **範圍**
  - **網路**
  - 這些類型的任何組合的群組。

  所有其他類型為不允許的類型，並且無法新增到自訂國家/地區清單。

- **建立新位址群組...** - 顯示**新增位址物件群組**對話方塊。



如 *SonicWall SonicOS 6.5 原則*中所述建立新的位址物件

- 已定義的位址物件或位址群組

6 從**國家/地區**下拉功能表中選擇一個國家/地區。

7 可以選擇在**註解**欄位中新增註解。

8 按一下**確定**。

編輯自訂清單項目

若要編輯自訂清單項目：

1 在**自訂清單**檢視上，按下要編輯之項目的**設定**欄位中的**編輯**圖示。將顯示**新增自訂清單**對話方塊，其中含有 IP 位址和關於項目的任何註解。

2 從**國家/地區**下拉功能表中選擇您的國家/地區以及進行任何其他變更。

3 按一下**確定**。隨即更新**自訂清單**表。

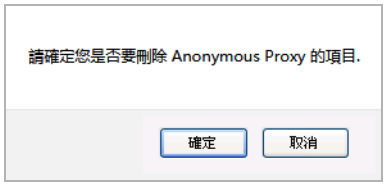
刪除自訂清單項目

若要刪除自訂清單項目：

1 執行以下其中一項操作：

- 按一下項目的**設定**欄中的**刪除**圖示。
- 勾選項目的核取方塊，然後按一下**刪除**按鈕。

將顯示確認訊息。

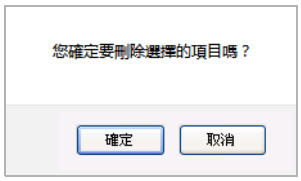


2 按一下**確定**。

若要刪除多個項目：

1 勾選要刪除項目的核取方塊。**刪除**按鈕即可供使用。

2 按一下**刪除**按鈕。將顯示確認訊息。

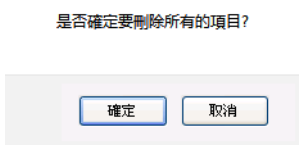


3 按一下**確定**。

若要刪除所有項目：

1 按一下表格標題中的核取方塊。

2 按一下**刪除**按鈕。將顯示確認訊息。



3 按一下**確定**。

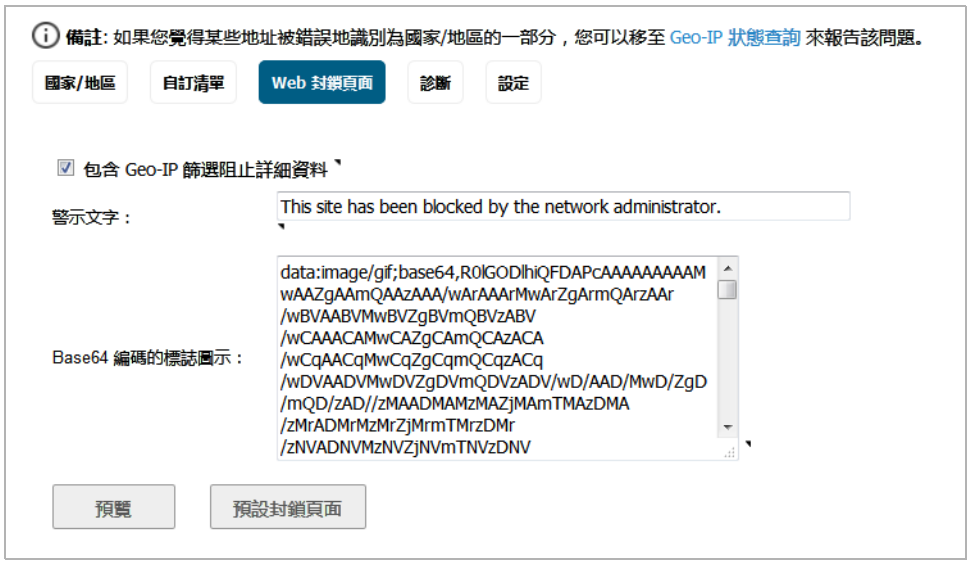
自訂 Web 封鎖頁面設定

Geo-IP 篩選含有一則預設訊息，會在使用者嘗試存取封鎖的頁面時顯示。您可以讓此訊息顯示更為詳細的資訊，例如封鎖 IP 位址的原因，以及 IP 位址和偵測到的來源國家。您也可以建立自訂訊息並包含自訂標誌。

若要建立自訂 Web 封鎖訊息：

1 導覽至**安全設定 | 安全服務 > Geo-IP 篩選 > 設定**頁面。

2 按一下 **Web 封鎖頁面**。



3 請確保已選擇**包含 Geo-IP 篩選阻止詳細資料**選項。啟用後，此選項會顯示封鎖的詳細資料，例如封鎖的原因、IP 位址和國家。停用後將不會顯示任何資訊。預設情況下，此選項處於勾選狀態。預設情況下已核取此選項。

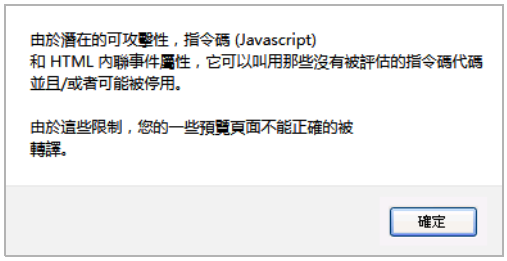
4 執行以下任一動作：

- 若要使用該站台被網路管理員封鎖的**警示文字**欄位中顯示的預設訊息，按一下**預設封鎖頁面**按鈕，然後移至步驟 6。
- 在**警示文字**欄位中指定要在 Geo-IP 篩選封鎖頁面中顯示的自訂訊息。您的訊息長度最多可以是 100 個字元。

5 另外，您也可以在 **Base64 編碼的標誌圖示**欄位中指定顯示 Base 64 編碼的 GIF 圖案，而非預設的 SonicWall 標誌。

附註：請確保此圖案是有效的且大小盡可能的小。推薦大小是 400 x 65。

6 若要預覽自訂的訊息和商標（或預設訊息和標誌），按一下**預覽**按鈕。將顯示警告訊息。



7 按一下**確定**。隨即顯示 **Web 站台封鎖**訊息。

8 關閉 **Web 頁面已封鎖**訊息。

9 按一下**接受**按鈕。

使用 Geo-IP 篩選診斷

安全服務 > Geo-IP 篩選頁面的**診斷**檢視含有以下幾種工具：

- 顯示解析的位置
- Geo-IP 快取統計
- 檢查 GEO 定位伺服器查詢
- 錯誤標記的位址

顯示解析的位置

按一下**顯示解析的位置**按鈕時，會出現解析的 IP 位址的顯示表，並顯示如下資訊：

- 索引
- IP 位址
- 國家/地區

Geo-IP 快取統計

Geo-IP 快取統計表包含如下資訊：

- 定位伺服器 IP
- 已解析項目
- 未解析項目
- 目前項目數目
- 最大項目數目
- 定位地圖數

自訂國家/地區統計資料

自訂國家/地區統計資料表包含清單中項目數量，以及項目已經發生的查詢次數的相關資訊：

- **項目數量**
- **呼叫的次數**
- **未查詢的次數**
- **已解析的次數**

檢查 GEO 定位伺服器查詢

Geo-IP 篩選還能夠查找 IP 位址以確定：

- 網域名稱或 IP 位址
- 來源國家，以及伺服器是否已歸類為 Botnet 伺服器

附註：還可以從**系統服務 > Botnet 篩選**頁面存取相似的 Botnet 定位伺服器查詢工具。Geo 定位和 Botnet 伺服器查詢工具還可以從**系統 > 診斷**頁面存取。

若要查詢 GEO 伺服器：

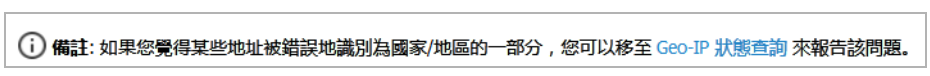
1 捲動至**診斷**檢視底部的**檢查 GEO 定位伺服器查詢**部分。

2 在**查詢 IP** 欄位輸入 IP 位址。

3 按一下**執行**。IP 位址的詳細資料顯示在**結果**標題下。

錯誤標記的位址

如果認為錯誤地將某個位址識別為國家的一部分，請通過在**安全設定 | 安全服務 > Geo-IP 篩選**頁面的**備註**中按一下 **Geo-IP 狀態查詢**連結，報告這個問題。此連結將顯示**提交 IP 以進行地理位置檢查**頁面。



18

設定 Botnet 篩選

附註：TZ300 系列及以上裝置提供 Botnet 篩選功能。

Botnet 篩選功能用於封鎖來自/到達 Botnet 命令和控制伺服器的連接，並製作自訂 Botnet 清單。

Botnet 篩選功能也可用來在封鎖網站時建立自訂訊息。

您也可以使用 Botnet 篩選診斷工具，顯示 Botnet、監視 Botnet 快取統計資料、自訂 Botnet 統計資料和查詢 Botnet 伺服器。

主題：

- 設定 Botnet 篩選
- 建立自訂 Botnet 清單
- 自訂 Web 封鎖頁面設定
- 使用 Botnet 篩選診斷

設定 Botnet 篩選

若要設定 Botnet 篩選：

1 導覽至**安全設定 | 安全服務 > Botnet 篩選 > 設定**頁面。

2 若要封鎖指定為 Botnet 命令和控制伺服器的所有伺服器，請選擇**封鎖到達/來自 Botnet 命令和控制伺服器的連接**選項。都封鎖試圖到達/來自 Botnet 命令和控制伺服器的所有連接。預設情況下未勾選此選項。

如果選擇此選項，選項按鈕和**如果 BOTNET DB 未下載，封鎖所有到公用 IP 的連接**選項即可供使用。

若要從此封鎖行為中排除所選 IP，請按如下步驟所述使用排除清單和/或如建立自訂 Botnet 清單中所述建立自訂 Botnet 清單。

3 如果勾選**封鎖到達/來自 Botnet 命令和控制伺服器的連接**，這些選項即可供使用：

a 為您的 Botnet 篩選選擇以下兩種模式中的一種：

- **所有連接**：篩選所有來自/到達防火牆的連接。這是預設的 Botnet 封鎖模式。
- **基於防火牆規則的連接**：只篩選符合防火牆設定的存取規則的連接。

b 如果您在未下載 Botnet 資料庫時封鎖所有公用 IP 的連接，請選擇**如果 BOTNET DB 未下載，封鎖所有到公用 IP 的連接**。預設情況下未勾選此選項。

4 若要啟用自訂 Botnet 清單，請選擇**啟用自訂 Botnet 清單**核取方塊。預設情況下未勾選此選項。

如未勾選**啟用自訂 Botnet 清單**核取方塊，則只會搜尋防火牆的 Botnet 資料庫。移至步驟 5。

透過勾選**啟用自訂 Botnet 清單**核取方塊來啟用自訂清單，可能影響 IP 位址的國家地區/識別。

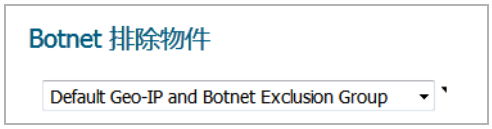
a 在 Botnet 識別期間，會先搜尋自訂 Botnet 清單。

b 如果未解析 IP 位址，則會搜尋防火牆的 Botnet 資料庫。

若 IP 位址是從自訂 Botnet 清單解析，可將其識別為 Botnet IP 位址或非 Botnet IP 位址，並採取相應的行動。

5 選擇**啟用記錄** Botnet 篩選相關的事件。

6 另外，您也可以為屬於已設定位址物件/位址群組的所有 IP 設定排除清單。所有屬於此清單的 IP 都將從封鎖中排除。從 **Botnet 排除物件**下拉功能表中選擇位址物件或位址群組以啟用排除清單。



預設排除物件是 Default Geo-IP and Botnet Exclusion Group。您可以如 *SonicWall SonicOS 6.5 原則*中所述建立您自己的位址物件或位址群組物件。

7 按一下頁面頂部的**接受**按鈕以啟用變更。

建立自訂 Botnet 清單

位址物件	位址物件或位址群組物件的名稱。
殭屍網路	圖示指出項目是否在建立時定義為 Botnet。黑色圓圈表示 Botnet，白色圓圈表示非 Botnet。
註解	任何您新增的有關項目的註解。
設定	包括項目的**編輯**和**刪除**圖示。
總計	顯示**自訂 Botnet 清單**中項目的數量。

IP 位址可能被錯誤標示為 Botnet。此種錯誤分類可能導致不正確/不想要的 IP 位址篩選。自訂 Botnet 清單可透過覆寫特定 IP 位址的 Botnet 標記，來解決此問題。

主題：

- 建立自訂 Botnet 清單
- 編輯自訂 Botnet 清單項目
- 刪除自訂 Botnet 清單項目

建立自訂 Botnet 清單

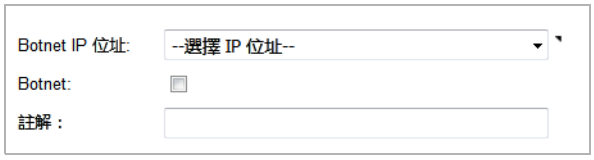
重要：對於要使用自訂 Botnet 清單的防火牆，您必須如設定 Botnet 篩選中所述啟用它。

若要建立自訂 Botnet 清單：

1 導覽至**安全設定 | 安全服務 > Botnet 篩選 > 設定**頁面。

2 按一下**自訂 Botnet 清單**。

3 按一下**新增**按鈕。將顯示**新增自訂 Botnet 清單**對話方塊。



4 從 **Botnet IP 位址**下拉功能表中選擇 IP 位址物件或建立新的位址物件。

重要：位址物件不可重疊自訂國家/地區清單中的任何其他位址物件。不過，不同位址物件可能具有相同的國家/地區 ID。

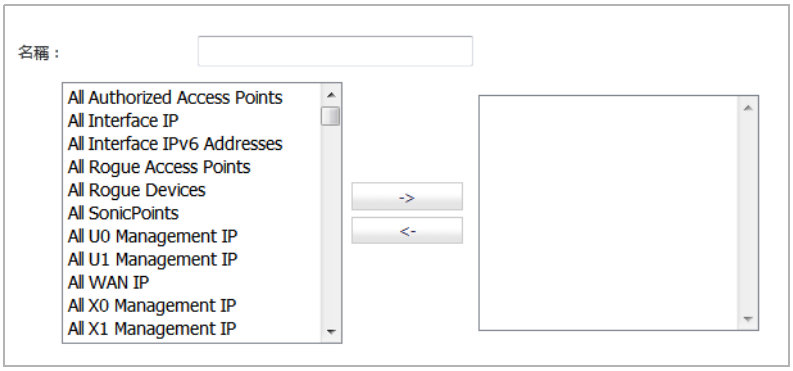
- **建立新位址物件...** - 顯示**新增位址物件**對話。

如 *SonicWall SonicOS 6.5 原則*中所述建立新的位址物件，並具備以下限制：

- 允許的類型為
  - **主機**
  - **範圍**
  - **網路**
  - 前三個類型的任何組合的群組。

  所有其他類型為不允許的類型，並且無法新增到自訂 Botnet 清單。

- **建立新位址群組...** - 顯示**新增位址物件群組**對話方塊。



如 *SonicWall SonicOS 6.5 原則*中所述建立新的位址物件

- 已定義的位址物件或位址群組

5 如果此位址物件是已知的 Botnet，請勾選 **Botnet** 核取方塊。

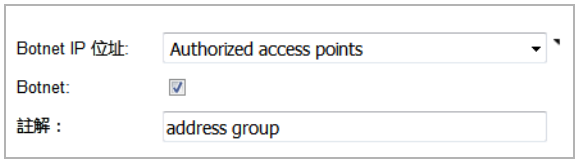
6 可以選擇在**註解**欄位中新增註解。

7 按一下**確定**。

編輯自訂 Botnet 清單項目

若要編輯自訂 Botnet 清單項目：

1 在**自訂 Botnet 清單**檢視上，按下要編輯之項目的**設定**欄位中的**編輯**圖示。**新增自訂 Botnet 清單**對話將顯示項目。



2 做出您的變更。

3 按一下**確定**。隨即更新**自訂 Botnet 清單**表。

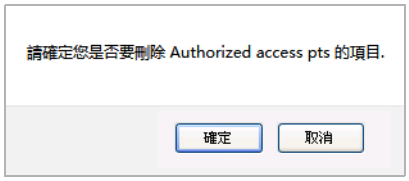
刪除自訂 Botnet 清單項目

若要刪除自訂 Botnet 清單項目：

1 執行以下其中一項操作：

- 按一下項目的**設定**欄中的**刪除**圖示。
- 勾選項目的核取方塊，然後按一下**刪除**按鈕。

將顯示確認訊息。

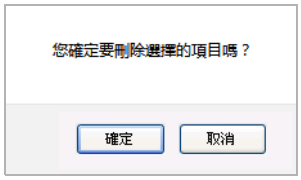


2 按一下**確定**。

若要刪除多個項目：

1 勾選要刪除項目的核取方塊。**刪除**按鈕即可供使用。

2 按一下**刪除**按鈕。將顯示確認訊息。

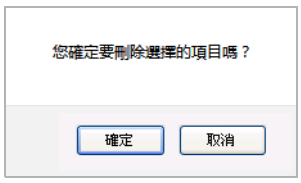


3 按一下**確定**。

若要刪除所有項目：

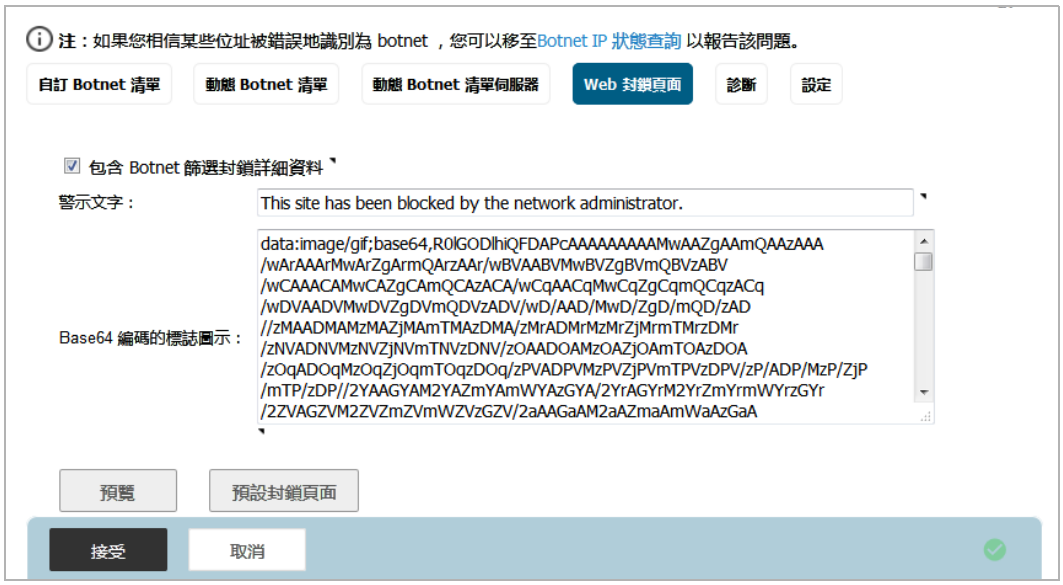
1 按一下表格標題中的核取方塊。

2 按一下**刪除**按鈕。將顯示確認訊息。



3 按一下**確定**。

自訂 Web 封鎖頁面設定



Botnet 篩選含有一則預設訊息，在封鎖頁面時顯示。您可以自訂此訊息並包括您自己的標誌。

若要建立自訂訊息並包含自訂標誌：

1 移至**安全服務 > Botnet 篩選**頁面。

2 請確保已選擇**包含 Botnet 篩選封鎖詳細資料**選項。預設情況下已核取此選項。

啟用後，此選項會顯示封鎖的詳細資料，例如封鎖的原因、IP 位址和國家。停用後，此選項則會隱藏所有的資訊。

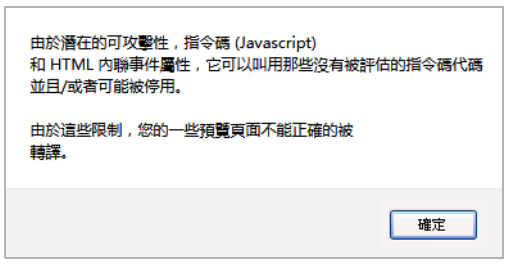
3 執行以下任一動作：

- 若要使用該站台被網路管理員封鎖。的**警示文字**欄位中顯示的預設訊息，按一下**預設封鎖頁面**按鈕，然後移至步驟 4。
- 在**警示文字**欄位中指定要在 Geo-IP 篩選封鎖頁面中顯示的自訂訊息。您的訊息長度最多可以是 100 個字元。

4 另外，您也可以在 **Base64 編碼的標誌圖示**欄位中指定要顯示的 Base 64 編碼的 GIF 圖案。

附註：請確保此圖案是有效的且大小盡可能的小。推薦大小是 400 x 65。

5 若要預覽自訂的訊息和商標（或預設訊息和標誌），按一下**預覽**按鈕。將顯示警告訊息。



6 按一下**確定**。隨即顯示 **Web 站台封鎖**訊息。

7 關閉 **Web 頁面已封鎖**訊息。

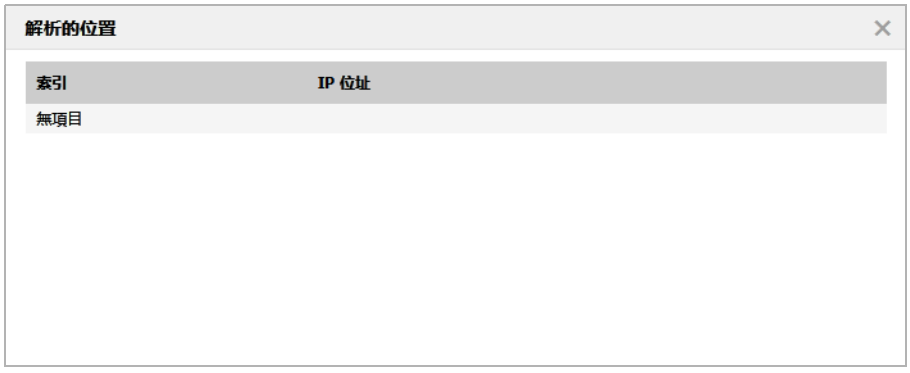
8 按一下**接受**按鈕。

使用 Botnet 篩選診斷

安全服務 > Botnet 篩選頁面的**診斷**檢視含有以下幾種工具：

- 顯示解析的 Botnet 位置
- Botnet 快取統計
- 自訂 Botnet 統計資料
- 檢查 Botnet 伺服器查詢

顯示解析的 Botnet 位置



按一下**顯示 Botnets** 按鈕時，會出現解析的 IP 位址表，並顯示如下資訊：

- **索引**
- **IP 位址** - Botnet 的 IP 位址

Botnet 快取統計

Botnets 快取統計表包含如下資訊：

- **定位伺服器 IP**
- **已解析項目**
- **未解析項目**
- **目前項目數目**
- **最大項目數目**
- **偵測到 Botnet**

自訂 Botnet 統計資料

自訂 Botnet 統計資料表包含清單中項目數量，以及項目已經發生的查詢次數的相關資訊：

- **項目數量**
- **呼叫的次數**
- **未查詢的次數**
- **已解析的次數**

檢查 Botnet 伺服器查詢

Botnet 篩選還能夠查找 IP 位址以確定：

- 網域名稱或 IP 位址
- 來源國家，以及伺服器是否已歸類為 Botnet 伺服器

附註：Botnet 伺服器查詢工具還可以從**系統 > 診斷**頁面存取。

若要查詢 Botnet 伺服器：

1 移至**診斷**檢視底部的**檢查 BOTNET 伺服器查詢**部分。

2 在**查詢 IP** 欄位輸入 IP 位址。

3 按一下**執行**。IP 位址的詳細資料顯示在**結果**標題下。

錯誤標記的位址

如果您認為某位址錯誤地標記為 botnet，或者您認為某位址應該標記為 botnet，請在 SonicWall Botnet IP 狀態查詢工具報告這個問題，按一下**安全服務 > Botnet 篩選**頁面底部**注**中的連結，或移至：SonicWall Botnet IP 狀態查詢。

19

關於反垃圾郵件

附註：反垃圾郵件是一項獨立、授權的功能，提供快速、高效和有效的方法來為現有的防火牆新增反垃圾郵件、防網路釣魚和防毒功能。

附註：SuperMassive 9800 不支援「反垃圾郵件」。

- 反垃圾郵件概述
- 什麼是反垃圾郵件？
- 優點
- 反垃圾郵件服務的工作原理
- 購買反垃圾郵件授權

反垃圾郵件概述

附註：SuperMassive 9000 系列上不支援「反垃圾郵件」。

主題：

- 什麼是反垃圾郵件？
- 優點
- 反垃圾郵件服務的工作原理
- 購買反垃圾郵件授權

什麼是反垃圾郵件？

反垃圾郵件特性提供快速、高效和有效的方法來為現有的防火牆新增反垃圾郵件、防網路釣魚和防毒功能。

在典型的反垃圾郵件設定中，您在 SonicOS 介面選擇反垃圾郵件功能並授權，從而新增此功能。這樣，防火牆就能使用與 SonicWall 電子郵件安全產品相同的先進垃圾郵件篩選技術來減少傳遞至使用者的垃圾郵件數量。

反垃圾郵件特性主要透過兩種方式來分析輸入郵件：

- 進階 IP 信譽管理
- 基於雲端的進階內容管理

「IP 位址信譽」利用 GRID 網路識別已知垃圾郵件傳送者的 IP 位址，拒收來自這些傳送者的任何郵件，甚至不允許連接。「GRID 網路傳送者 IP 信譽管理」對照一系列清單和統計檢查傳入連接請求的 IP 位

址，確保連接有較大的可能性會傳遞有價值的電子郵件。這些清單是利用 SonicWall GRID 網路的協同智慧編制。阻止已知垃圾郵件傳送者，無法連接防火牆，其垃圾郵件有效承載不會消耗目的地系統上的系統資源。

非來自已知垃圾郵件傳送者的電子郵件則根據 SonicWall 研究實驗室產生的「GRIDprints」進行分析，其基礎資料源於成百上千萬的業務端點、億萬郵件和 GRID 網路使用者數以億計的信譽投票。Grid 網路利用來自多個 SonicWall 解決方案的資料建立一個協同智慧網路，以防禦全球範圍的威脅。GRIDprints 以獨特方式識別郵件，不會暴露電子郵件中包含的資料。

反垃圾郵件服務將威脅分為以下幾類，一封電子郵件*只能屬於其中一類*：垃圾郵件、可能的垃圾郵件、網路釣魚、可能的網路釣魚、病毒或可能的病毒。評估電子郵件的威脅時，它採用以下優先順序：

- 網路釣魚
- 可能的網路釣魚
- 病毒
- 可能的病毒
- 垃圾郵件
- 可能的垃圾郵件

例如，如果一封郵件既是病毒，又是垃圾郵件，則將其歸類為病毒，因為病毒的優先順序高於垃圾郵件。

如果反垃圾郵件服務判斷一封郵件*不*屬於上述任何威脅，則將之視為正常電子郵件而傳遞至目的地伺服器。

優點

防火牆新增反垃圾郵件防護可篩選並拒收垃圾郵件，避免使用者在收件箱中看到它們，從而提高系統整體的效率。

- 減少網路中垃圾郵件消耗的頻寬和資源量
- 減少傳送至郵件伺服器的傳入郵件數
- 降低對公司的威脅，因為拒收後使用者將無從按一下帶病毒的垃圾郵件郵件，也不會因此感染電腦
- 更好地防護使用者免受網路釣魚攻擊

反垃圾郵件服務的工作原理

本節介紹反垃圾郵件特性，包括 SonicWall GRID 網路，以及它如何與作為一個整體的 SonicOS 交互。與 SonicOS 關係重大的兩點是位址和服務物件。可利用位址和服務物件來設定反垃圾郵件特性，使其配合 SonicOS 順利地工作。例如，使用反垃圾郵件服務物件設定 NAT 原則，以便封存輸入電子郵件並將其透過篩選條件傳送。

綜合反垃圾郵件服務分析郵件的標頭和內容，利用協同 GRIDprinting 封鎖垃圾郵件。

主題：

- GRID 網路
- 位址和服務物件

GRID 網路

使用傳送者 IP 信譽的 GRID 連接管理功能，SonicWall 電子郵件安全和 SonicOS 中的反垃圾郵件服務使用此功能。GRID 網路傳送者 IP 信譽是指定 IP 位址在 SonicWall GRID 網路成員中有的信譽。啟用此功能後，將不會接受來自信譽不良 IP 位址的電子郵件。如果 SonicOS 不接受來自已知不良 IP 位址的連接，則來自此 IP 位址的郵件將無法到達電子郵件伺服器。

「GRID 網路傳送者 IP 信譽」對照一系列清單和統計檢查傳入連接請求的 IP 位址，確保連接有較大的可能性會傳遞有價值的電子郵件。這些清單是利用 SonicWall GRID 網路的協同智慧編制。阻止已知垃圾郵件傳送者，無法連接防火牆，其垃圾郵件有效承載不會消耗目的地系統上的系統資源。

主題：

- 優點
- 使用傳送者 IP 信譽的 GRID 連接管理和連接管理優先順序

優點

- 在連接層級封鎖高達 80% 的垃圾郵件，使其根本無法進入網路。維護反垃圾郵件防護層級所需的資源非常少。
- 頻寬不浪費在伺服器接收垃圾郵件上，僅用於分析和刪除。
- 一個全球網路監視垃圾郵件傳送者，需要時可協助合法使用者恢復其 IP 信譽。

使用傳送者 IP 信譽的 GRID 連接管理和連接管理優先順序

請求傳送到作為第一接觸物件的防火牆時，反垃圾郵件服務評估請求者的「信譽」。信譽根據已知正常傳送者的白名單、已知垃圾郵件傳送者的封鎖清單和拒絕服務閾值編制。

如果啟用了 IP 信譽功能，來源 IP 位址將按照以下順序進行檢查：

評估訂單

評估	說明
允許清單	如果 IP 位址位於此清單上，將允許郵件透過連接管理。郵件將由防火牆照常進行分析。
封鎖清單	禁止此 IP 位址連接防火牆。
信譽清單	如果 IP 位址不在以上清單中，防火牆將檢查 GRID 網路，查看此 IP 位址是否有不良信譽。
延遲清單	延遲來自此 IP 位址的連接。必須經過設定的間隔後才允許連接。
DoS	如果 IP 位址不在以上清單中，防火牆將檢查此 IP 位址是否超過拒絕服務閾值。如果超過，裝置將根據現有 DoS 設定採取措施。

只有 IP 位址透過上述所有測試後，防火牆才會允許此伺服器建立連接並傳送郵件。如果 IP 位址未透過測試，SonicOS 將向請求伺服器傳送一則訊息，告知沒有 SMTP 伺服器。不接受連接請求。

位址和服務物件

SonicOS 的反垃圾郵件特性支援位址和服務物件來管理客戶的電子郵件伺服器。反垃圾郵件服務將這些物件用於 NAT 和存取規則原則。自動建立的規則是不可編輯的，如果停用反垃圾郵件服務，則刪除這些規則。

啟用時，反垃圾郵件服務建立 NAT 原則和存取規則以控制並重新導向電子郵件流量。原則和規則可以在「網路 > NAT 原則和防火牆規則」頁面上看到，但不可編輯。這些自動建立的原則僅在反垃圾郵件服務啟用時可用。

反垃圾郵件服務獲授權並啟用時，「反垃圾郵件 > 設定」頁面會顯示一個核取方塊，用於啟用反垃圾郵件功能。勾選此核取方塊時，如果沒有為已部署方案自訂存取規則和 NAT 原則，則將調用「目的地郵件伺服器原則精靈」。設定所產生的原則時，反垃圾郵件服務必須知道電子郵件路由至防火牆背後何處。

具體而言，它需要目的地郵件伺服器 IP 位址及其區域指派。如果無法找到此資料，就會啟動「目的地郵件伺服器原則精靈」。

需要為精靈提供如下資訊：

- **目的地郵件伺服器公用 IP 位址** - 外部 MTA（郵件傳輸代理程式）透過 SMTP 連接的 IP 位址。
- **目的地郵件伺服器私人 IP 位址** - Exchange 或 SMTP 伺服器（防火牆之後）的內部 IP 位址。
- **區域指派** - Exchange 伺服器所屬的區域。
- **入口電子郵件連接埠** - 將電子郵件送至的 TCP 服務連接埠編號，也稱為輸入 SMTP 連接埠。

精靈所建立的原則和位址物件可編輯並一直存在，即使停用反垃圾郵件服務。

主題：

- 啟用反垃圾郵件服務時建立的物件
- 精靈建立的物件
- 原則和物件變更

啟用反垃圾郵件服務時建立的物件

本節提供一個自動產生為防火牆存取規則、NAT 原則和服務物件的規則和物件類型的例子。這些物件是不可編輯的，如果停用反垃圾郵件服務，則將其移除。

原則 | 規則 > 存取規則頁面顯示為反垃圾郵件產生的規則。

#	區域	>	區域	優先順序	來源	目的地	服務	操作	包含的使用者	排除的使用者	停用 DPI	流量報告	Geo-IP 篩選	Botnet 篩選	封包監控	註解	啟用	設定
1	WAN	>	LAN	1	任何	User Mail Server Public IP	SMTP (Anti-Spam Inbound Port)	允許	所有	無								
2	WAN	>	LAN	2	任何	Default Active WAN IP	SonicWALL Anti-Spam Service	允許	所有	無								
3	WAN	>	LAN	3	任何	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	允許	所有	無								
4	WAN	>	LAN	4	任何	任何	任何	拒絕	所有	無								

紅框所示的行是啟用反垃圾郵件服務時產生的存取規則。綠框所示的行是不存在郵件伺服器原則時反垃圾郵件服務建立的預設規則。

您也可以建立以下存取規則：

- 從任何來源到所有 WAN IP 位址的傳入電子郵件 (SMTP) 的 WAN 到 WAN 規則
- 從電子郵件安全服務到所有 WAN IP 位址的已處理電子郵件的 WAN 到 LAN 規則，使用反垃圾郵件服務連接埠（預設：10025）

反垃圾郵件服務物件是在**原則 | 規則 > 服務物件**頁面建立。

#	名稱	通訊協定	起始連接埠	終止連接埠	類別	註解	設定
156	SonicWALL Anti-Spam Service	TCP	10025	10025	Default		

此服務由產生的 NAT 原則引用。

24	任何	Default Active WAN IP	Public Mail Server Address Group	SonicWALL Email Security Service	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	任何	任何
25	任何	初始	Public Mail Server Address Group	SonicWALL Email Junk Store	SMTP (Anti-Spam Inbound Port)	SonicWALL Anti-Spam Service	任何	任何
26	任何	初始	Default Active WAN IP	Destination Mail Server Private IP	SonicWALL Anti-Spam Service	SMTP (Send E-Mail)	任何	任何
27	任何	初始	Public Mail Server Address Group	Destination Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	任何	任何
28	任何	初始	User Mail Server Public IP	User Mail Server Private IP	SMTP (Anti-Spam Inbound Port)	SMTP (Send E-Mail)	任何	任何
29	任何	初始	Default Active WAN IP	SonicWALL Email Junk Store	SonicWALL Anti-Spam Service	初始	任何	任何
30	任何	初始	WAN Interface IP	初始	SSLVPN	初始	任何	任何
31	任何	X1 IP	任何	初始	任何	初始	X10	X1
32	任何	X1 IP	任何	初始	任何	初始	X3	X1

紅框所示的行是啟用反垃圾郵件服務時產生的原則。綠框所示的行是不存在郵件伺服器原則時反垃圾郵件服務建立的預設原則。

精靈建立的物件

管理員與精靈交互所建立的物件可以編輯並一直留在系統中，即使已停用反垃圾郵件服務。

以下考慮適用於原則的自動產生：

- 建立一個稱為 **Public Mail Server Address Group** 的系統位址群組物件，作為所產生原則的原始目的地的預設物件。此群組包含位址物件**目的地郵件伺服器公用 IP**，它獲得精靈期間提供的 IP 位址值。
- 如果 SonicWall 裝置已經存在針對 SMTP 的原則，則發生以下程式：
  - 如果現有原則的原始目的地是主機類型位址物件，則所產生的原則使用 **Public Mail Server Address Group** 物件作為其原始目的地。
  - 如果現有原則的原始目的地是非主機類型位址物件，則所產生的原則使用此非主機類型位址物件作為其原始目的地。
  - 如果 SMTP 有一個以上的公用 IP 位址，則您可以手動新增位址物件到 **Public Mail Server Address Group**。

原則和物件變更

在 `diag.html` 頁面，**重設 GRID 名稱快取**按鈕可用來清除 GRID 名稱快取中的所有項目。

刪除原則和物件按鈕可用來移除服務關閉時未刪除的反垃圾郵件位址和服務物件。按一下此按鈕時，SonicOS 嘗試移除所有自動產生的物件和原則。此操作只能在反垃圾郵件服務關閉時執行。

diag.html 頁面上與反垃圾郵件相關的其它選項有：

- **對反垃圾郵件相關的連接停用 SYN 洪水防護** - 對於 SMTP (25) 和反垃圾郵件服務 (10025) 連接埠，SYN 洪水防護預設開啟。此選項可停用防護。
- **僅使用 GRID IP 信譽檢查** - 勾選時，它將覆寫探查結果，並模擬反垃圾郵件服務無法使用（管理關閉）的情況。傳送電子郵件時，仍會進行 SYN 洪水檢查和 GRID IP 檢查，但不執行其它電子郵件掃描。

購買反垃圾郵件授權

使用反垃圾郵件特性時，要求滿足以下部署前提條件：

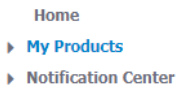
- 已授權的 SonicWall 網路安全裝置
- 用於裝置的反垃圾郵件授權
- 下列一種 Microsoft Windows 伺服器：
  - Windows Server 2012 R2（64 位元）
  - Windows Server 2012（64 位元）
  - Windows SBS 2008 R2 Server（64 位元）
  - SBS 2008（64 位元）

為防火牆購買反垃圾郵件授權可直接透過 mySonicWall.com 或分銷商進行。

附註：使用之前，SonicWall 網路安全裝置必須在 mySonicWall.com 上註冊。

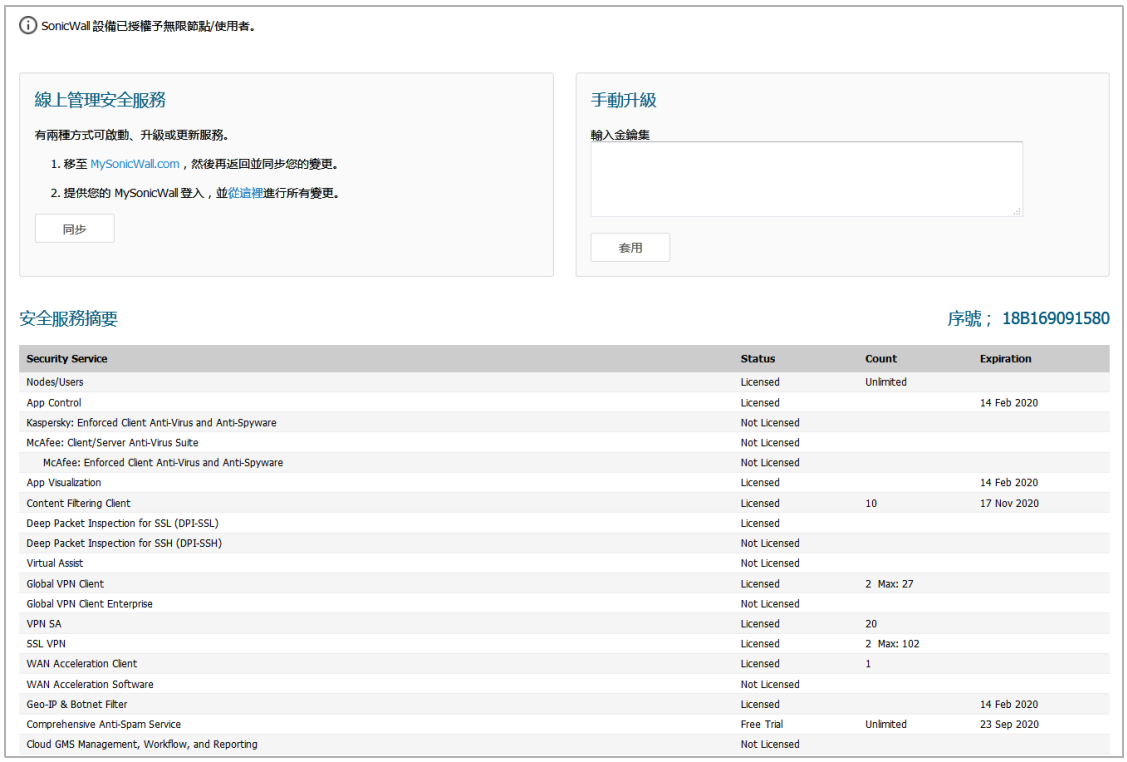
如需購買反垃圾郵件授權：

1. 在用來管理 SonicWall 裝置的電腦上打開 Web 瀏覽器。
2. 在**位置**或**位址**欄位，輸入 **http://www.mySonicWall.com** 。
3. 在相應的欄位中輸入 mySonicWall.com 帳戶的**使用者名稱**和**密碼**。
4. 按一下**提交**按鈕。
5. 導覽左側導航欄中的**我的產品**。



6. 選擇您希望為其新增反垃圾郵件功能的裝置。
7. 註冊反垃圾郵件授權。
8. 登入到裝置的 web 管理介面。

9 從 navigation bar.mySonicWall.com 導覽到**更新 | 授權**頁面。



Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
App Control	Licensed		14 Feb 2020
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
McAfee: Client/Server Anti-Virus Suite	Not Licensed		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed		
App Visualization	Licensed		14 Feb 2020
Content Filtering Client	Licensed	10	17 Nov 2020
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		
Deep Packet Inspection for SSH (DPI-SSH)	Not Licensed		
Virtual Assist	Not Licensed		
Global VPN Client	Licensed	2 Max: 27	
Global VPN Client Enterprise	Not Licensed		
VPN SA	Licensed	20	
SSL VPN	Licensed	2 Max: 102	
WAN Acceleration Client	Licensed	1	
WAN Acceleration Software	Not Licensed		
Geo-IP & Botnet Filter	Licensed		14 Feb 2020
Comprehensive Anti-Spam Service	Free Trial	Unlimited	23 Sep 2020
Cloud GMS Management, Workflow, and Reporting	Not Licensed		

10 在**線上管理安全服務**部分，按一下用以啟用或更新授權的連結。也可在**手動升級**部分輸入金鑰或金鑰組。

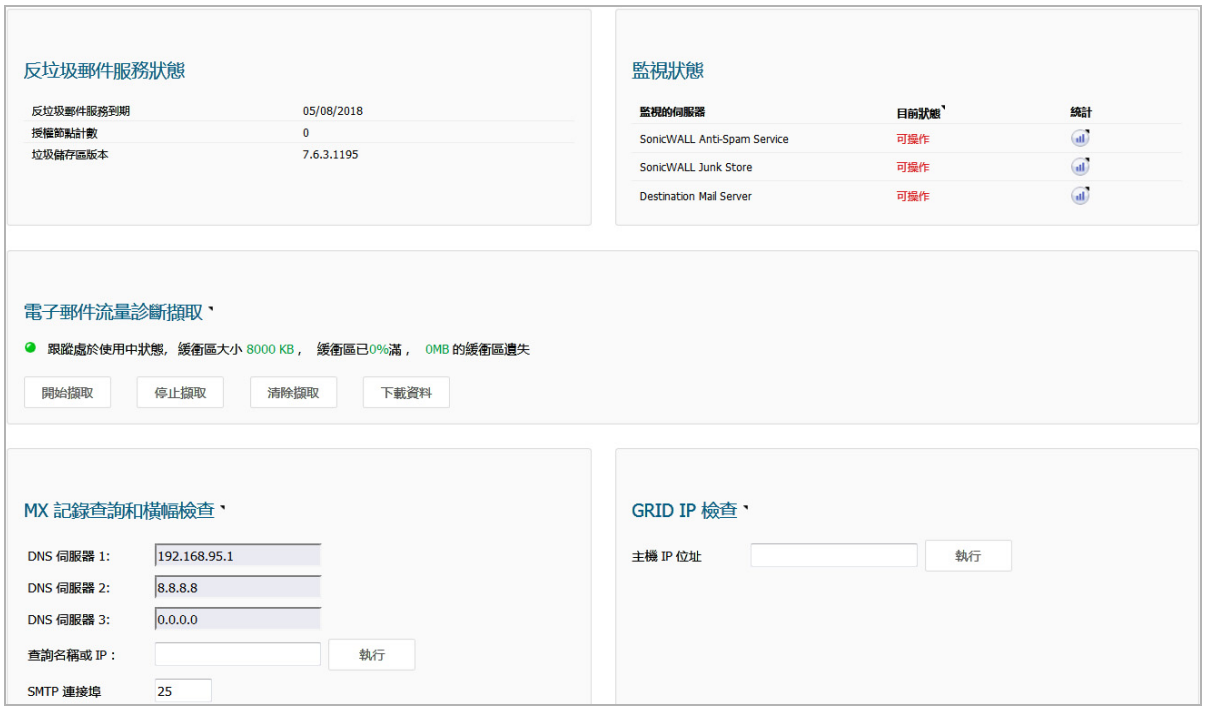
11 輸入 mySonicWall.com 登入資訊。

20

檢視反垃圾郵件狀態

附註：反垃圾郵件 > **狀態**不適用於 SuperMassive 9800。

在**監控 | 目前狀態 | 反垃圾郵件狀態**頁面檢視授權和監視的狀態。也可檢查網域和 IP 位址，確保其有效。



主題：

- 反垃圾郵件服務狀態
- 監視狀態
- 電子郵件流量診斷擷取
- MX 記錄查詢和橫幅檢查
- GRID IP 檢查

反垃圾郵件服務狀態

反垃圾郵件服務狀態部分列出反垃圾郵件功能的資訊：

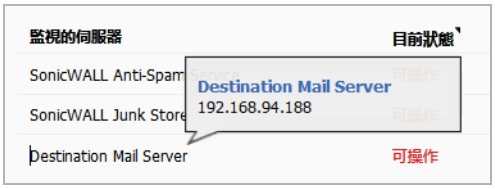
- **反垃圾郵件服務過期日期**
- **授權節點計數**
- **垃圾儲存區版本** - 如果未安裝啟用垃圾儲存區，則版本為 0.0.0.0。

監視狀態

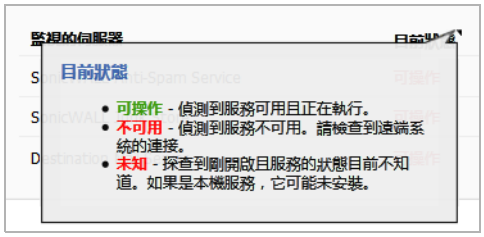
監視狀態部分顯示已監視反垃圾郵件服務的狀態和統計。

- **已監視服務** - 列出服務：
  - **SonicWall 反垃圾郵件服務**
  - **SonicWall 垃圾儲存區**
  - 目的地郵件伺服器

  提示：將滑鼠放在監視服務上，將快顯顯示伺服器位址。

- **目前狀態** - 顯示每項服務的目前狀態。將滑鼠放在標題上的小三角形圖示，將快顯顯示狀態的說明：

- **可操作**（綠色）- 監視服務已啟動且正在執行中。
- **不可用**（紅色）- 偵測到監視服務無法使用。請檢查到遠端系統的連接。
- **未知**（紅色）- 探查剛開啟並且監視服務的狀態目前不知道。如果是本機服務，它可能未安裝。

- **統計** - 包含每項服務的**統計**圖示。滑鼠放在這個圖示時，將顯示收集到的服務統計的快顯描述：

  - **成功** - 探查成功的次數。
  - **失敗** - 探查失敗的次數。
  - **成功率** - 總探查中成功的百分比。

電子郵件流量診斷擷取

電子郵件流量診斷擷取擷取經過防火牆的 SMTP 相關流量並提供應用程式資料格式報告。

附註：此報告僅包含輸入流量。

已顯示追蹤的狀態：

- **追蹤**狀態：
  - **使用中**
  - **關**
- **快取大小**
- **緩衝區已用 %**
- **MB 的緩衝區遺失**

對經過防火牆的 SMTP 相關流量產生應用程式格式化報告的方法是：

1 按一下 **啟動追蹤**按鈕。

2 可透過按一下**停止追蹤** 按鈕，可隨時停止擷取。

3 按一下**下載資料**，將報告下載為 `packet-hd.html` 檔案。將顯示警告訊息。

4 按一下**確定**。將顯示**打開 packet-dh.html** 對話方塊。

5 選擇以：

- 透過在**開啟方式**（預設）下拉功能表中選擇瀏覽器，在瀏覽器中開啟檔案。
- 選擇**儲存檔案**，儲存檔案。

6 按一下**確定**。如果已打開檔案，則檔案已下載到瀏覽器：

```
[ ] #19 08/31/2015 14:49:23.144 len:244/286 in:-- out:MGMT* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.............................Y.............................................................*
 *.....................................................................................*
 *.....................................c.Sc5...*

[ ] #20 08/31/2015 14:49:23.144 len:244/286 in:-- out:X2* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *....._T.....................Y.............................................................*
 *.....................................................................................*
 *.....................................c.Sc5...*

[ ] #21 08/31/2015 14:49:23.144 len:244/286 in:-- out:X0* UDP 0.0.0.0:68->255.255.255.255:67 [flags:]
Generated (Sent Out)
 *.............................Y.............................................................*
 *.....................................................................................*
 *.....................................c.Sc5...*

[ ] #22 08/31/2015 14:49:23.256 len:40/82 in:X1*(i) out:-- UDP 0.0.0.1:5933->10.200.0.52:53 [flags:]
Consumed, Module Id:47
 *............nosslsearch.google.com.....*

[ ] #26 08/31/2015 14:49:33.544 len:136/178 in:X1*(i) out:-- UDP 0.0.0.1:61785->10.203.28.37:162 [flags:]
Consumed, Module Id:47
 *0.......admins.x.........0m0...+.......C..K0...+...........+.....%....y0...+.....%.........0*..*
 *+.....%........Interface X0 Link Is Down*

[ ] #28 08/31/2015 14:49:33.544 len:136/178 in:X1*(i) out:-- UDP 0.0.0.1:61785->10.203.28.37:162 [flags:]
Consumed, Module Id:47
 *0.......admins.x.........0m0...+.......C..K0...+...........+.....%....y0...+.....%.........0*..*
 *+.....%........Interface X1 Link Is Down*
```

清除統計的方法是：

1 按一下**清除擷取**按鈕。

MX 記錄查詢和橫幅檢查

在 **MX 記錄查詢和橫幅檢查**部分，您可以執行以下操作：

- 為給定網域名稱執行 MX 紀錄查詢。
- 執行連接偵測結果主機伺服器或者提供 IP 位址以獲得 SMTP 標語。

DNS 伺服器預設顯示在 **DNS 伺服器 1/2/3** 欄位中，但無法變更。SMTP 連接埠顯示在 **SMTP 連接埠**欄位。

輸入網域名稱或 IP 位址後，綜合反垃圾郵件服務將嘗試連接到此伺服器並檢索 SMTP 標語。此功能可用於檢查電子郵件傳送者是否偽造位址以顯得更加合法。

查詢電子郵件傳送程式或網域的 MX 記錄的方法是：

1 在**查詢名稱或 IP** 欄位輸入網域名稱或 IP 位址。

2 按一下**執行**。將顯示結果。

結果中包括您所輸入的網域名稱或 IP 位址、已使用的清單中的 DNS 伺服器、已解析的電子郵件伺服器網域名稱和/或 IP 位址，以及從網域伺服器收到的橫幅或提示連接受到拒絕的訊息。橫幅的內容取決於您正在查找的伺服器。

GRID IP 檢查

GRID IP 檢查部分用於對給定主機 IP 位址進行 SonicWall GRID 網路 IP 信譽檢查。如需 GRID 網路的更多資訊，請參閱 GRID 網路。

執行 GRID IP 名稱偵測的方法是：

1 在 **主機 IP 位址**欄位輸入 IP 位址。

2 按一下**執行**。將顯示結果。

21

啟用和啟用反垃圾郵件

附註：反垃圾郵件不適用於 SuperMassive 9800。

反垃圾郵件 > 基本設定頁面用於啟用反垃圾郵件功能、設定電子郵件威脅類別、修改存取清單和設定進階選項。

主題：

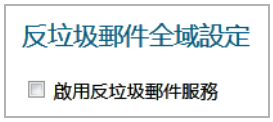
- 啟用反垃圾郵件
- 安裝垃圾儲存區
- 設定電子郵件威脅類別
- 設定存取清單
- 設定進階選項

啟用反垃圾郵件

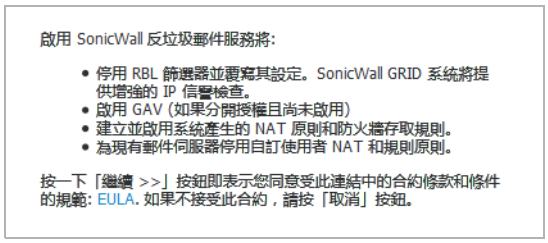
一旦註冊反垃圾郵件功能，啟用它即可啟動裝置級防護，防範垃圾郵件、網路釣魚和病毒郵件。

啟用反垃圾郵件的方法是：

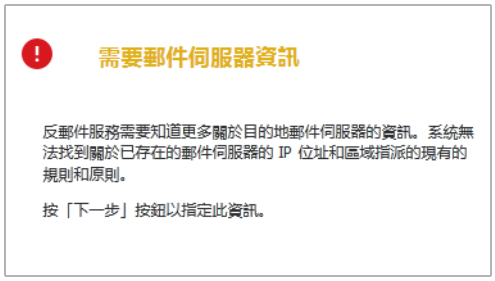
1 導覽至**反垃圾郵件 > 基本設定**頁面。



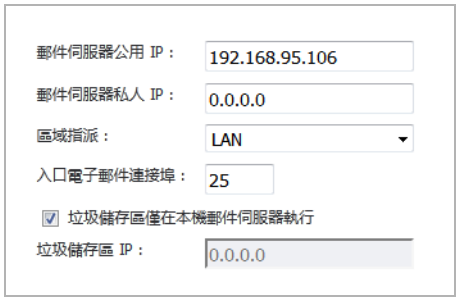
2 按一下**啟用反垃圾郵件服務**啟用反垃圾郵件功能。將顯示一則訊息，描述啟用反垃圾郵件服務的作用，並要求同意繼續操作。



3 如需繼續，按一下**繼續**按鈕。將顯示另一則關於要使用的郵件伺服器的訊息。



4 按**下一步**按鈕。將顯示一個要求伺服器資訊的對話方塊。將來自系統的資訊自動填入對話方塊設定。



5 也可變更資訊。

6 按**下一步**。將顯示一則訊息，解釋安裝過程中建立的事物。

7 按一下**確定**。

安裝反垃圾郵件應用程式後，您可：

- 下載並安裝垃圾儲存區；參見安裝垃圾儲存區
- 設定電子郵件威脅類別；參見設定電子郵件威脅類別。

安裝垃圾儲存區

反垃圾郵件功能可在 Microsoft Exchange 伺服器上建立一個垃圾儲存區。垃圾儲存區隔離郵件以供最終使用者分析，並提供統計資訊。登入到 Exchange 系統，打開一個瀏覽器以登入到管理介面，然後安裝垃圾儲存區。

附註：雖然 SonicWall 支援非 Exchange SMTP 伺服器，如 Sendmail 和 Lotus Domino 等，但不需要在這些伺服器上安裝垃圾儲存區。與 SonicWall 電子郵件安全產品相似，CASS 2.0 允許在獨立伺服器上安裝垃圾儲存區。

SonicWall 推薦使用者在獨立伺服器上安裝垃圾儲存區，以便充分利用 CASS 2.0 提供的最新功能。

安裝垃圾儲存區的步驟是：

1 登入到 Exchange 系統。

2 打開 Web 瀏覽器。

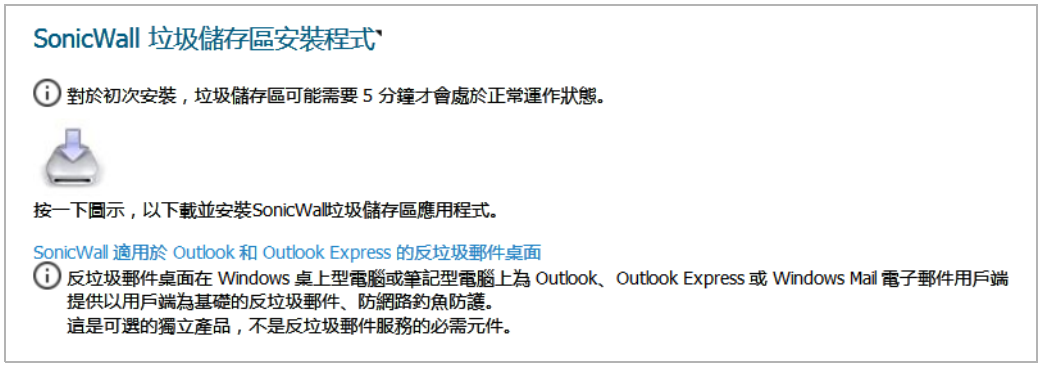
重要：如需下載安裝 SonicWall 垃圾儲存區應用程式，將要安裝垃圾儲存區應用程式的系統需要滿足以下條件：

- Internet Explorer 6 或更高版本
- Microsoft Exchange 伺服器
- 用於 IE 的電子郵件下載的 ActiveX 元件

3 登入到 SonicOS 介面。

4 導覽至**反垃圾郵件 > 設定**頁面。

5 移至 **SonicWall 垃圾儲存區安裝程式**部分。



6 按一下**垃圾儲存區安裝程式** 圖示以在您的 Windows 伺服器上安裝垃圾儲存區。

附註：首次安裝垃圾儲存區應用程式後，需要 5 - 15 分鐘進入操作狀態。

7 如果您的瀏覽器警告您，此 Web 站台試圖載入 SonicWall 電子郵件安全附加元件：

a 按一下「資訊欄」。

b 選擇快顯功能表中的**安裝 ActiveX 控制項**。將顯示安全警告頁面。

8 按一下**安裝**安裝 ActiveX 控制項。

9 在**反垃圾郵件 > 基本設定**頁面上，再次按一下**垃圾儲存區安裝程式**圖示。頁面上會顯示一個進度欄。

10 完成下載後，安裝程式啟動。

附註：移轉垃圾儲存區中的資料可能需要很長時間才能完成。

11 導覽至**監控 | 目前狀態 | 反垃圾郵件狀態**頁面，驗證 SonicWall 垃圾儲存區**可操作**。

設定電子郵件威脅類別

啟用反垃圾郵件功能時，請設定喜好設定。完成設定後，電子郵件將根據設定進行篩選和分類。

為使用者郵件設定預設值的方法是：

1 在**反垃圾郵件 > 基本設定**頁面，向下滑動至**電子郵件威脅類別**部分。

2 為包含或可能包含垃圾郵件、網路釣魚和病毒問題的郵件選擇預設值設定；如需瞭解下拉功能表可用的選項，請參見電子郵件威脅類別設定：選項表格：

- **可能的垃圾郵件**（預設：**儲存在垃圾儲存區**）
- **確定的垃圾郵件**（預設：**永久刪除**）
- **可能的網路釣魚**（預設：**標記 [可能的網路釣魚]**）
- **確定的網路釣魚**（預設：**儲存在垃圾儲存區**）
- **可能的病毒**（預設：**儲存在垃圾儲存區**）
- **確定的病毒**（預設：**永久刪除**）

電子郵件威脅類別設定：選項

類別	操作
篩選關閉	反垃圾郵件功能不會掃描和篩選此威脅類別的任何電子郵件，因而所有電子郵件都會傳遞給收件者。
標記 [*標記*]	在電子郵件的主旨行中加一個術語標記： • [可能的垃圾郵件] • [垃圾郵件] • [可能的網路釣魚] • [網路釣魚] • [可能的病毒] • [病毒] 選擇此選項允許使用者控制電子郵件，不需要時可將其歸入垃圾郵件之列。
儲存在垃圾儲存區	電子郵件儲存在垃圾儲存區。有適當權限的使用者和管理員可將其設定為非垃圾郵件。
永久刪除	永久刪除電子郵件。 注意：**選擇此選項時，您的機構可能會遺失有用的電子郵件。**

如果使用一個以上的網域，請選擇「多個網域」選項，更多資訊請聯絡 SonicWall 或 SonicWall 分銷商。

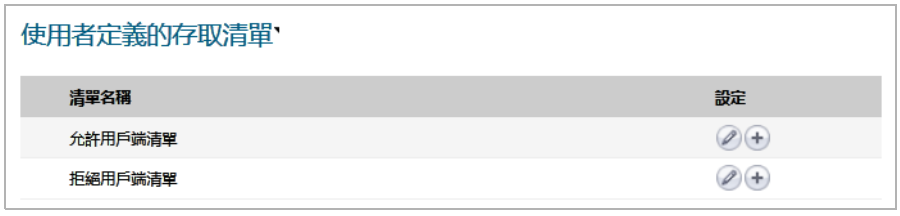
設定存取清單

使用者定義的存取清單部分的兩個清單透過指定允許或拒絕哪些用戶端可以連接以便傳遞電子郵件，使您可以管理固定允許和拒絕清單。

附註：在這些清單中的項目設定優於 GRID IP 信譽檢查結果。

設定清單的方法是：

1 在**反垃圾郵件 > 基本設定**頁面，向下滑動至**使用者定義的存取清單**部分。



2 按一下**編輯**圖示獲取您要編輯的**允許用戶端清單**或**拒絕用戶端清單**。將顯示**允許/拒絕用戶端清單**對話方塊。

3 從左欄選擇要新增到允許清單的項目。

4 按一下**向右的箭頭**按鈕。

從允許清單移除項目的方法是：

a 從允許清單選擇項目。

b 按一下**向左的箭頭**按鈕。

5 完成時，按一下**確定**按鈕。

向清單新增主機的方法是：

1 捲動至**使用者定義的存取清單**部分。

2 按一下**新增主機** ⊕ 圖示。將顯示**新增主機到允許/拒絕清單**對話方塊。

3 在**名稱**欄位中輸入主機名稱。

4 從**類型**下拉功能表選擇主機類型。下列設定將根據所選的主機類型而發生變更。

5 如果選擇：

- **主機**（預設）- 請在 **IP 位址**欄位中輸入 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。

- **FQDN** - 在 **FQDN 主機名稱**欄位輸入 FQDN 主機名稱。

6 按一下**確定**。

設定進階選項

在**進階選項**部分，您可以設定反垃圾郵件 > 基本設定：進階選項表格中說明的電子郵件選項。

反垃圾郵件 > 基本設定：進階選項

設定類型	設定	說明
反垃圾郵件進階設定	SonicWall 反垃圾郵件服務無法使用時允許/拒絕傳遞未處理的郵件	如果反垃圾郵件服務未啟用或因某種原因無法使用，您可以選擇讓所有未處理的電子郵件通過或拒絕所有未處理的電子郵件。垃圾郵件和正常郵件均將傳遞給使用者。 從下拉功能表中選擇： • **允許**（預設） • **拒絕**
	SonicWall 垃圾儲存區無法使用時標記並傳遞/刪除電子郵件	如果垃圾儲存區無法接受垃圾郵件，您可以選擇將其刪除，或加上警告性主旨行（如[網路釣魚] 請更新您的帳戶）再傳遞。 從下拉功能表中選擇： • **標記並遞送**（預設） • **刪除**
監視服務探針	探查間隔（分鐘）	設定在 WAN 和 LAN 網路探查電子郵件安全元件每分鐘的頻率.最短為 1 分鐘，最長為 60 分鐘，預設值為 **5** 分鐘。
	探查逾時（秒）	設定探查等待目的地回應的秒數，在識別失敗之前。最小時長為 30 秒，最大時長為 300 秒，預設值為 **30** 秒。

反垃圾郵件 > 基本設定：進階選項

設定類型	設定	說明
	成功次數閾值	設定在宣佈此項目是可操作的項目之前連續成功回應的次數。最小數值為 1 次回應，最大數值為 10 次回應，預設值為 **1** 次回應。
	失敗次數閾值	設定在宣佈此項目是不可到達的項目之前連續成功回應的次數。最小數值為 1 次回應，最大數值為 10 次回應，預設值為 **3** 次回應。
目的地郵件伺服器設定	伺服器公用 IP 位址	可用於外部連接的伺服器的 IP 位址。MTAs 將此 WAN IP 位址用於 SMTP 連接。數字將自動填寫為您在啟用安裝反垃圾郵件和垃圾儲存區時指定的位址。您可變更位址。
	伺服器私人 IP 位址	用於內部流量的伺服器的 IP 位址。這個是在裝置後的內部電子郵件伺服器 IP 位址 。數字將自動填寫為您在啟用安裝反垃圾郵件和垃圾儲存區時指定的位址。您可變更位址。
	入口電子郵件連接埠	裝置打開的用於接收輸入電子郵件的 TCP 服務連接埠。最小值為 0，最大值為 65535，預設值為 **已產生功能**。
垃圾郵件儲存區設定	使用目的地郵件伺服器的私人位址為垃圾郵件儲存區位址	如果垃圾儲存區位於目的地郵件伺服器上，請勾選此核取方塊。位址將自動填寫為您在啟用安裝反垃圾郵件和垃圾儲存區時指定的位址。您可變更位址。預設選擇此核取方塊，且垃圾儲存區 IP 位址欄位顯示為灰色。 ***變更位址的方法是：*** 1 取消選擇核取方塊。垃圾儲存區 IP 位址欄位變為可用。 2 請輸入伺服器所在位置的垃圾儲存區 IP 位址。
其它	啟用電子郵件子系統偵測	啟用網路上的電子郵件系統資源的可用的發現. 預設情況下選擇此核取方塊。

檢視反垃圾郵件統計

附註：反垃圾郵件 > 統計不適用於 SuperMassive 9800。

在**監控 | 事件摘要 > 垃圾郵件統計資料**頁面檢視反垃圾郵件功能的統計。

處理的訊息數目： 0
垃圾訊息的數目： 0
記錄開始時間： 2017-11-21 17:15:43

威脅	全部
TCP Cookie (SYN 攻擊) 驗證	0
固定主機拒絕清單	0
SonicWall GRID IP 信譽服務	0
可能的垃圾郵件	0
確定的垃圾郵件	0
可能的網路釣魚	0
確定的網路釣魚	0
可能的病毒	0
確定的病毒	0

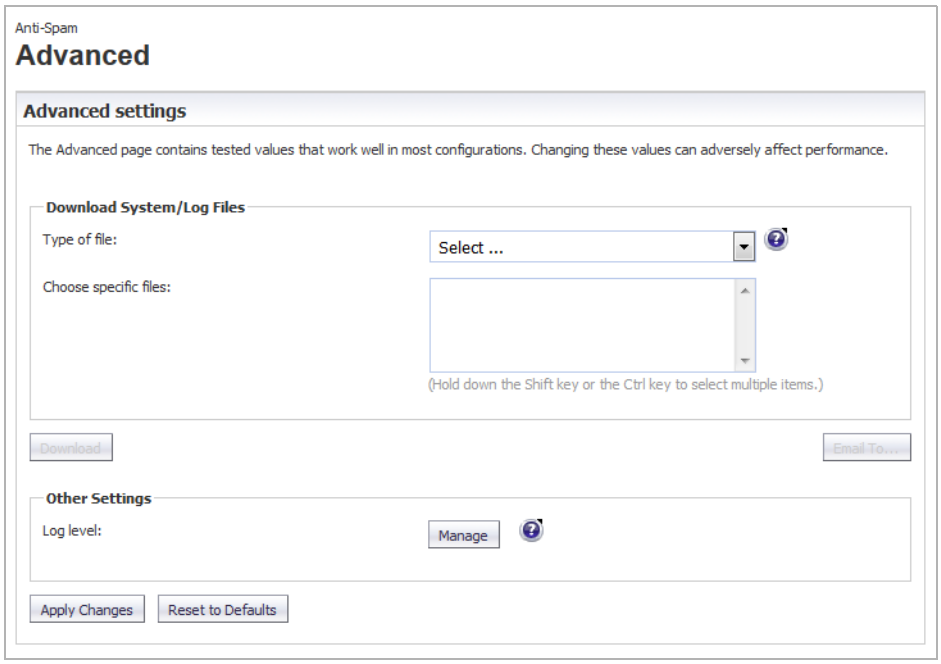
- **已處理郵件的總數** - 啟用反垃圾郵件功能以來已處理郵件的總數。
- **垃圾郵件的總數** - 啟用反垃圾郵件功能以來垃圾郵件的總數。
- **記錄開始時間** - 啟用反垃圾郵件功能的日期和時間。
- **威脅** - 列出服務和威脅的類型，以及提供的每種類型的服務和已封鎖的每種威脅的總數。
  - **TCP Cookie SYN 洪水確認**
  - **固定主機拒絕清單**
  - **SonicWall GRID 名聲服務**
  - **可能的垃圾郵件**
  - **確定的垃圾郵件**
  - **可能的網路釣魚**
  - **確定的網路釣魚**
  - **可能的病毒**
  - **確定的病毒**

23

設定反垃圾郵件記錄

附註：反垃圾郵件 > **進階**不適用於 SuperMassive 9800。

在**反垃圾郵件 > 進階設定**頁面上，您可以從伺服器下載記錄或系統設定檔，以及設定記錄層級。



主題：

- 下載系統/記錄檔案
- 選擇記錄資訊的數量和層級

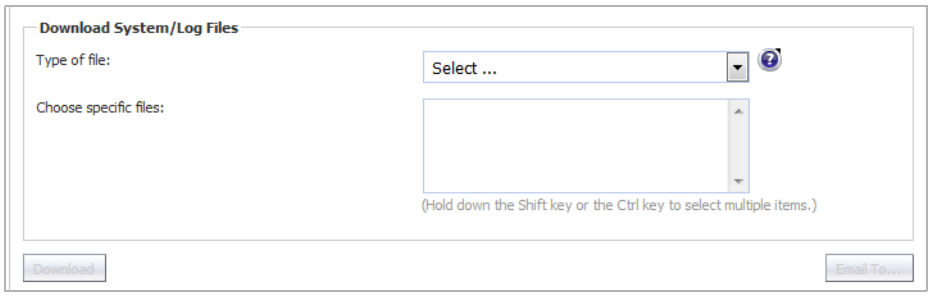
下載系統/記錄檔案

附註：有些記錄檔案名稱（例如 commonlogs 目錄中的檔案名稱）包含兩位數，例如 12.log。「12」表示此檔案是最近月份第 12 天的記錄。有些記錄檔案名稱以數字結尾，例如 MlfThumbUpdate_2.log。「2」表示這是更早的記錄。目前記錄為 MlfThumbUpdate.log。下一個最近記錄是 MlfThumbUpdate_0.log，再下一個是 MlfThumbUpdate_1.log，依此類推。

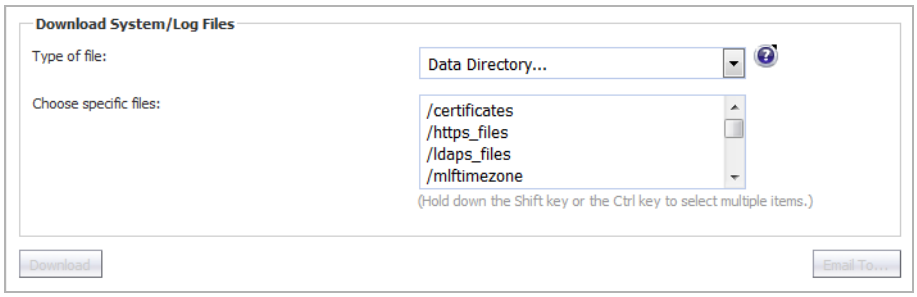
大多數記錄資料採用格林威治標準時間 (GMT)，而不是採用記錄伺服器的當地時間。這同樣適用於記錄檔案的名稱。

從 SonicWall 電子郵件安全伺服器下載記錄或系統設定檔的方法是：

1 導覽到**反垃圾郵件 > 進階設定**的**下載系統/記錄檔案**部分。



2 從**檔案類型**下拉功能表選擇要下載的檔案類型。將自動以此檔案類型填寫**選擇指定檔案**清單。

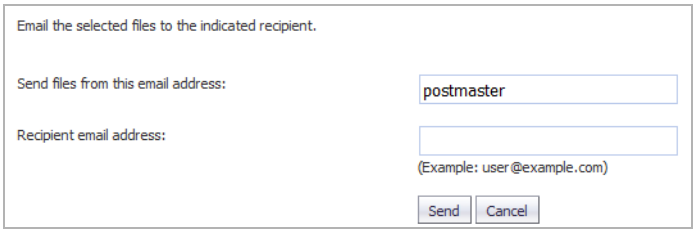


3 從**選擇指定檔案**清單，選擇一個或多個指定項目。如需選擇多個檔案，按住 Shift 鍵或 Ctrl 鍵同時勾選檔案。**下載** Download 和**電子郵件收件者...** Email To... 按鈕可用。

附註：所選檔案將壓縮到一個 zip 檔案中。

4 按一下：

- **下載**按鈕將檔案下載到本機硬碟。
- **電子郵件收件者...**按鈕，用電子郵件傳送**傳送至**對話方塊顯示的檔案。



a) 在**傳送來自此電子郵件地址的檔案**欄位輸入傳送者的電子郵件地址。預設為**郵件管理員**。

b) 在**收件者電子郵件地址**欄位輸入收件者的電子郵件地址。

c) 按一下**傳送**按鈕。

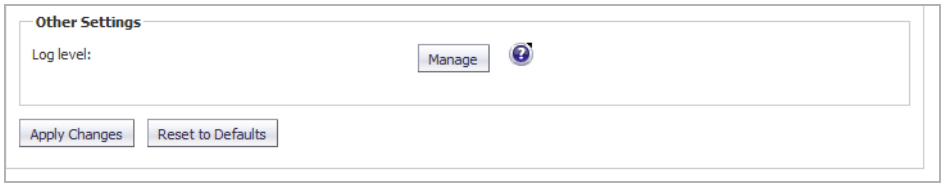
附註：根據電子郵件系統的限制，用電子郵件傳送非常大的檔案和目錄可能會出現問題。

選擇記錄資訊的數量和層級

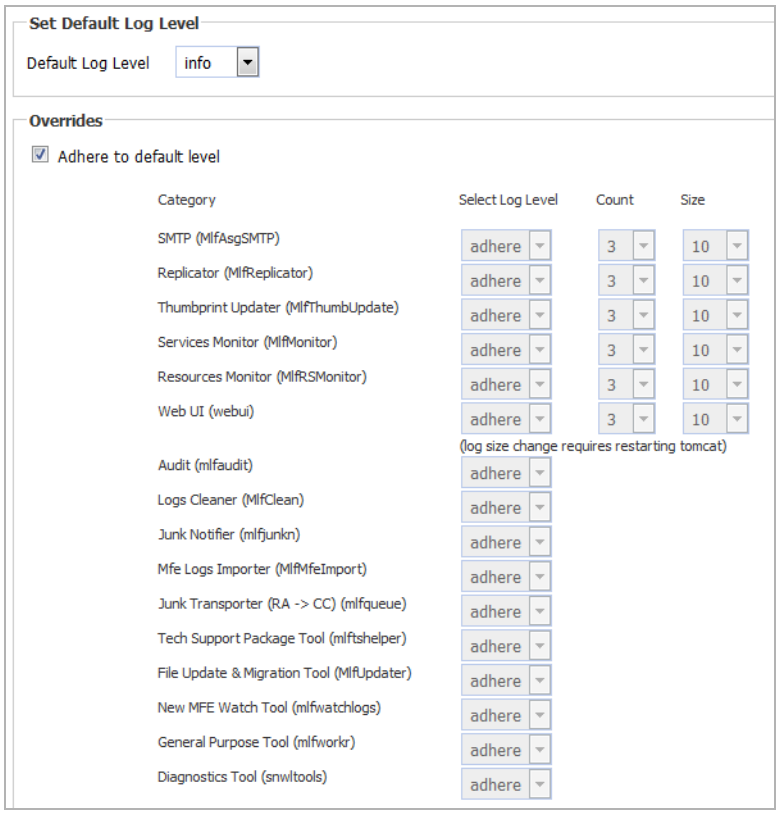
可以在**其他設定**部分選擇記錄中儲存的系統報告資訊層級和數量。

設定記錄資訊的層級和數量的方法是：

1 導覽到**反垃圾郵件 > 進階設定**的**其他設定**部分。



2 按一下**管理** Manage 按鈕。將顯示**設定記錄層級**對話方塊。



3 從**預設記錄層級**下拉功能表選擇預設記錄層級；記錄層級將從最低到最高列出：

附註：預設記錄層級越高，記錄的事件越多。例如，**資訊**層級也記錄**追蹤**和**偵錯**層級。

- **追蹤** - 最低層級
- **偵錯**

- **資訊** - 預設
- **警告**
- **錯誤**
- **嚴重** - 最高層級

除非特別指定覆寫，所有在此處設定的記錄都將嚴格遵守預設層級。

4 如需對**覆寫**部分的記錄進行修改，取消選擇**符合預設層級**核取方塊。用於所有服務類別的所有下拉功能表都變為可用。

5 如需變更指定服務和子服務的記錄層級，從要變更的服務/子服務的**選擇記錄層級**下拉功能表，選擇想要的記錄層級。層級與步驟 3 中的層級相同，外加**符合**選項。

> **附註：**所有服務和子服務類別的預設記錄層級是**符合**，即使用**預設記錄層級**下拉功能表中設定的記錄層級。

6 另外，選擇要保留的記錄檔案的數量。預設情況下，垃圾儲存區保留以下服務的 3 個記錄檔案：

- SMTP
- 憑證指紋更新器
- 資源監視器
- 複寫器
- 服務監視器
- Web UI

產生第四個記錄檔案後，將丟棄最舊的記錄檔案，第二舊的變為最舊，第三舊的變為第二舊。

a 您可從服務的**計數**下拉功能表選擇一個數字，增加為服務儲存的記錄數量。

- **3**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**

儲存較少數目的記錄可節省磁碟空間，但舊資料可能無法使用。更多數目的記錄可保留更多資料，但需要更多磁碟空間。

7 另外，可從**大小**下拉功能表選擇服務記錄的大小（參見步驟 6）。每個記錄的預設大小為 **10 Mb**。

您可以 10 MB 為增量增加記錄大小，範圍 10 Mb（預設）到 100 Mb。較小記錄大小可節省磁碟空間，但較大記錄包含更多資料。

> **重要：**需要重新啟動 Tomcat 伺服器來變更記錄大小。

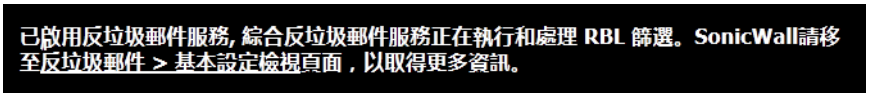
8 按一下**套用變更**按鈕以儲存所做的變更。

將記錄層級恢復為預設值的方法是：

1 按一下**重設為預設值** Reset to Defaults 按鈕。

設定 RBL 篩選

附註：反垃圾郵件服務是標準 SonicOS RBL 篩選的進階超集。因此，啟用「反垃圾郵件」後，將自動停用 RBL 篩選且顯示包含此資訊和**反垃圾郵件 > 基本設定**頁面連結的訊息。



如果反垃圾郵件服務未啟用，您可以在**即時黑名單設定**頁面上設定相關設定。但所有「反垃圾郵件」和「垃圾儲存區」頁面將無法使用。

附註：**反垃圾郵件 > 即時黑名單篩選條件**不適用於 SuperMassive 9800。

主題：

- 關於 RBL 清單
- 啟用 RBL 篩選
- 管理 RBL 服務
- 使用者自訂 SMTP 伺服器清單
- 測試即時黑名單

關於 RBL 清單

SMTP 即時黑名單 (RBL) 是發佈 SMTP 伺服器的 IP 位址的機制，垃圾郵件經常會透過此伺服器執行。有多個組織在編制此類資訊，有的免費提供，例如：http://www.spamhaus.org；有的則要收費，例如：https://ers.trendmicro.com/。

附註：SMTP RBL 是一種積極的垃圾郵件篩選技術，基於從已報告的垃圾郵件活動編制的清單，因此可能會產生誤報。SonicOS 實作的 SMTP RBL 篩選提供了多種微調機制有助於確保篩選的精確性。

RBL 清單供應商透過 DNS 發佈其清單。列入黑名單的 IP 位址出現在清單供應商 DNS 網域的資料庫中，使用相關 SMTP 伺服器的反轉 IP 作為網域名稱的首碼。127.0.0.2 至 127.0.0.11 的回應代碼表示某種類型的問題：

例如，如果 IP 位址為 1.2.3.4 的 SMTP 伺服器被 RBL 清單供應商 sbl-xbl.spamhaus.org 列入黑名單，則對 4.3.2.1.sbl-xbl.spamhaus.org 的 DNS 查詢將獲得 127.0.0.4 回應，表示此伺服器是已知的垃圾郵件來源，連接將中斷。

附註：當今的大部分垃圾郵件是從執行微弱 SMTP 伺服器實作的被綁架或僵屍機器傳送。與合法 SMTP 伺服器不同，這些僵屍機器很少嘗試重新傳送。一旦 RBL 篩選條件封鎖傳送嘗試後，此垃圾郵件不再嘗試傳送。

對黑名單查詢的 SonicOS 回應

會收集 DNS 回應並將之快取起來。如果任何查詢導致黑名單回應，篩選此伺服器。回應利用 TTL 值進行快取，為非黑名單回應指派的快取 TTL 值為 2 小時。如果快取填滿，快取項目將按照 FIFO（先進先出）順序丟棄。

IP 位址檢查利用快取確定一個連接是否應中斷。最初，IP 位址不在快取中，必須傳送 DNS 請求。這種情況下，此 IP 位址適用「無罪推定」，檢查結果是允許連接。然後傳送 DNS 請求，結果在單獨的任務中將之快取起來。檢查來自此 IP 位址的後續封包時，如果已將之列入黑名單，連接將中斷。

啟用 RBL 篩選

在啟用即時黑名單封鎖後，就會對照每個已啟用的 RBL 服務檢查來自 WAN 上主機的輸入連接或至 WAN 上主機的輸出連接，向 RBL DNS 伺服器下設定的 DNS 伺服器傳送 DNS 請求。

啟用即時黑名單篩選的步驟如下：

1 導覽至**安全設定 | 反垃圾郵件 > 即時黑名單篩選條件**頁面。

2 勾選**啟用即時黑名單封鎖**核取方塊。

3 從「RBL DNS 伺服器」下拉功能表中選擇 DNS 伺服器：

- **從 WAN 區域繼承設定**（預設）- 顯示 DNS 伺服器 IP 位址，但在 **DNS 伺服器 1/2/3** 欄位中變暗。
- **手動指定 DNS 伺服器** - **DNS 伺服器 1/2/3** 欄位將變為可用。

a) 在 **DNS 伺服器 1/2/3** 欄位中輸入一個或多個 DNS 伺服器 IP 位址。

4 按一下**接受**。

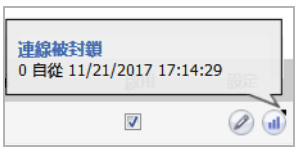
管理 RBL 服務

可以在**即時黑名單服務**區段新增更多 RBL 服務。

即時黑名單服務部分顯示可用 RBL 服務操作的相關資訊。

- **RBL 服務** - RBL 服務名稱。SonicWall 提供兩個服務名稱，但您也可新增其他名稱：
  - sbl-xbl.spamhaus.org - Spamhaus Project，它提供對網際網路網路的反垃圾郵件即時防護
  - dnsbl.sorbs.net - SORBS（垃圾郵件和開放式轉接封鎖系統），它提供對其基於 DNS 的黑名單 (DNSBL) 資料庫的存取
- **回應代碼** - 將滑鼠放在**註解**圖示以顯示回應代碼清單。如需回應代碼的資訊，請參見關於 RBL 清單。
- **啟用** - 選擇此核取方塊以啟用 RBL 服務。預設勾選所提供的兩項服務的核取方塊。

  如需停用 RBL 服務，則取消勾選其核取方塊。它不會刪除表中的項目，因此您可在以後啟用此服務。
- **設定** - 顯示各種操作的圖示：
  - **編輯**圖示 - 顯示**編輯 RBL 網域**對話方塊。請參閱編輯 RBL 服務。
  - **統計**圖示 - 顯示連線被封鎖的資訊：



如需清除這些統計資訊，按一下「清除統計」按鈕。

- **刪除**圖示 - 刪除 RBL 服務項目。請參閱刪除 RBL 服務。

主題：

- 正在清除統計資訊
- 新增 RBL 服務
- 編輯 RBL 服務

正在清除統計資訊

您可以清除針對黑名單服務所儲存的統計資訊。

清除統計資訊的步驟如下：

1 按一下其核取方塊以選擇服務。如需清除所有服務的統計資訊，請勾選 **RBL 服務**旁的標頭中的核取方塊。**清除統計**按鈕隨即啟用。

2 按一下**清除統計**按鈕。

新增 RBL 服務

新增 RBL 服務的步驟如下：

1 在**安全設定 | 反垃圾郵件 > 即時黑名單篩選條件**頁面，捲動至**即時黑名單服務**部分。

2 按一下**新增**按鈕。隨即顯示 **RBL 網域設定**對話方塊。

3 在 **RBL 網域**欄位中指定要查詢的 RBL 服務網域名稱。

4 勾選**啟用 RBL 網域**核取方塊以啟用要使用的服務。

5 勾選其核取方塊以指定預期的回應代碼。多數 RBL 服務會在其網站上列出其提供的回應，不過選擇**封鎖所有回應**一般是可接受的。

> **提示：**勾選**封鎖所有回應**核取方塊可勾選所有封鎖回應的核取方塊。取消勾選**封鎖所有回應**核取方塊可取消勾選所有封鎖回應的核取方塊。

6 按一下**確定**。RBL 服務將新增至**即時黑名單服務**表。

編輯 RBL 服務

編輯 RBL 服務的步驟如下：

1 在**安全設定 | 反垃圾郵件 > 即時黑名單篩選條件**頁面，捲動至**即時黑名單服務**部分。

2 按一下與要變更的 RBL 服務關聯的**編輯**圖示。顯示**新增 RBL 網域**對話方塊。

3 另外，也可在 **RBL 網域**欄位中編輯要查詢的 RBL 服務網域名稱。

> **提示：**勾選/取消勾選**即時黑名單服務**表中的**啟用**核取方塊可啟用或停用 RBL 服務。

4 另外，也可勾選/取消勾選**啟用 RBL 網域**核取方塊以啟用或停用要使用的服務。

5 也可勾選其核取方塊以勾選/取消勾選預期的回應代碼。

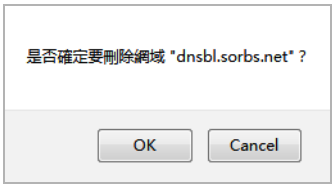
> **提示：**勾選**封鎖所有回應**核取方塊可勾選所有封鎖回應的核取方塊。取消勾選**封鎖所有回應**核取方塊可取消勾選所有封鎖回應的核取方塊。

6 按一下**確定**。

刪除 RBL 服務

刪除 RBL 服務的步驟如下：

1 在**即時黑名單服務**表中按一下此服務的**刪除**圖示。將顯示警告訊息：

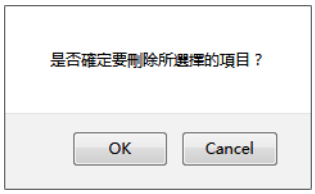


2 按一下**確定**。此項目將從**即時黑名單服務**表中刪除。

刪除一個或多個 RBL 服務的步驟如下：

1 勾選**即時黑名單服務**表中一個或多個服務的核取方塊。**刪除**按鈕隨即啟用。

2 按一下**刪除**按鈕。將顯示警告訊息：



3 按一下**確定**。此項目將從**即時黑名單服務**表中刪除。

使用者自訂 SMTP 伺服器清單

附註：您可以編輯，但不能刪除 **RBL User White List** 或 **RBL User Black List**。

使用者自訂 SMTP 伺服器清單部分允許使用位址物件來建立 SMTP 伺服器的白名單（明確允許：**RBL User White List**）或黑名單（明確拒絕：**RBL User Black List**）。這些清單中的項目將繞過 RBL 查詢程式。

為確保始終從合作夥伴網站的 SMTP 伺服器接收 SMTP 連接：

1 在**安全設定 | 反垃圾郵件 > 即時黑名單篩選條件**頁面，捲動至**使用者自訂 SMTP 伺服器清單**部分。

2 建立您要新增的伺服器位址物件：

a 按一下**新增**按鈕。此時會顯示**新增位址物件**對話方塊。

b 在**名稱**欄位中輸入伺服器的易記的名稱。

c 從**區域指派**下拉功能表中，選擇伺服器區域。

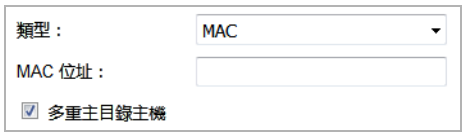
d 從**類型**下拉功能表中，選擇主機類型。下列設定將根據所選的主機類型而發生變更。

e 如果選擇：

- **主機**（預設）- 請在 **IP 位址**欄位中輸入 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** - 輸入：

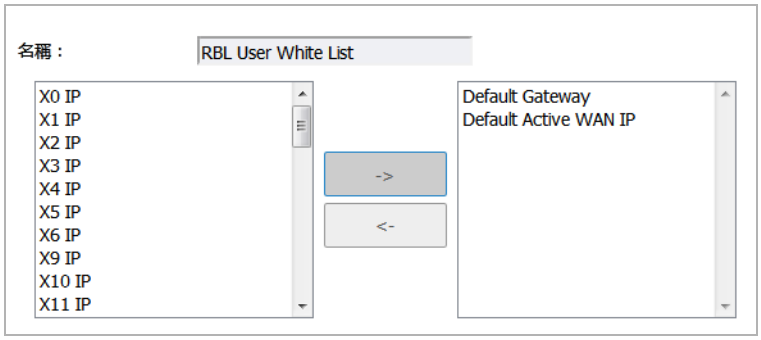
  - 在**網路**欄位中輸入網路。
  - 在**子網路遮罩**欄位中輸入子網路遮罩。
- **MAC**：



  - 在「MAC 位址」欄位中輸入 MAC 位址。
  - 如果主機為多重主目錄主機，請勾選**多重主目錄主機**核取方塊。否則，請取消勾選此核取方塊。預設情況下選擇此核取方塊。
- **FQDN** - 在 **FQDN 主機名稱**欄位輸入 FQDN 主機名稱。

f 按一下**確定**。

3 按一下 **RBL User White List** 的**設定**欄的**編輯**圖示。隨即顯示**編輯位址物件群組**對話方塊。



4 選擇要從左欄新增的位址物件。一次可選擇多個位址物件。

5 按一下**向右的箭頭**按鈕。

如需將位址物件從群組中刪除，請選擇此位址物件並按一下**左箭頭**按鈕。

6 按一下**確定**。表格已更新，此伺服器將始終能夠進行 SMTP 交換。

測試即時黑名單

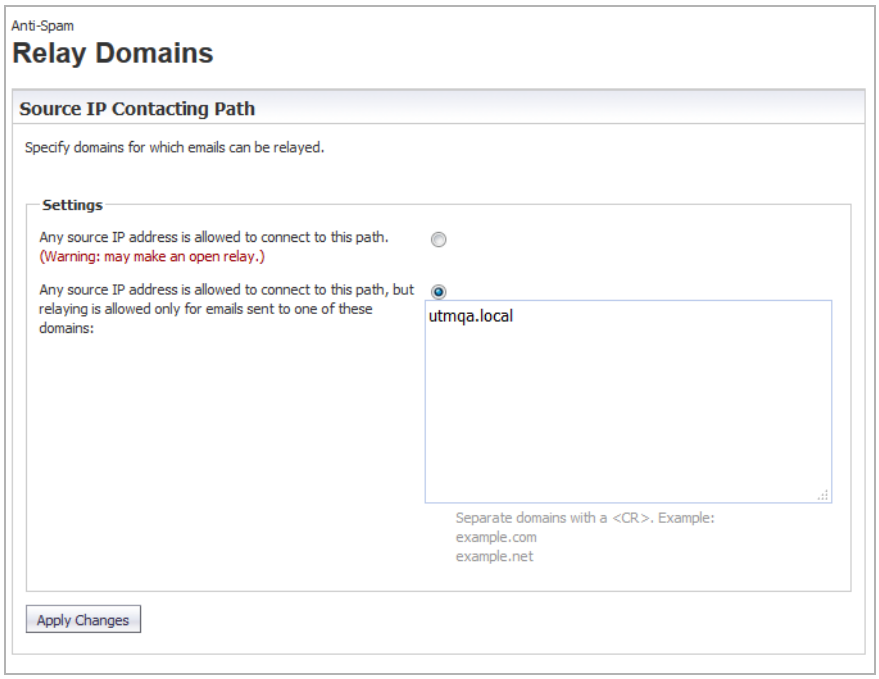
調查 | 工具 | 系統診斷頁面也在**診斷工具**部分提供了**即時黑名單查詢**功能，允許專門測試 SMTP IP 位址（或 RBL 服務、DNS 伺服器）。如需此功能的更多資訊，請參閱 *SonicWall SonicOS 6.5 調查*。

如需用於測試的已知垃圾郵件來源清單，請參閱：http://www.spamhaus.org/sbl/latest/。

25

指定轉接網域

附註：反垃圾郵件 > **轉接網域**不適用於 SuperMassive 9800。



反垃圾郵件 > 轉接網域頁面用於列出由 CASS 授權可用於轉接電子郵件的網域。限制可以轉接電子郵件的網域，可以避免開放式轉接的問題。

主題：

- 關於開放轉接
- 列出允許的轉接網域

關於開放轉接

開放轉接是指 SMTP 伺服器設定成一種方式，允許既不來自也不前往本機使用者的供應商進行轉接（傳送/接收電子郵件訊息）。因此，此類伺服器經常成為垃圾郵件傳送者的目的地。

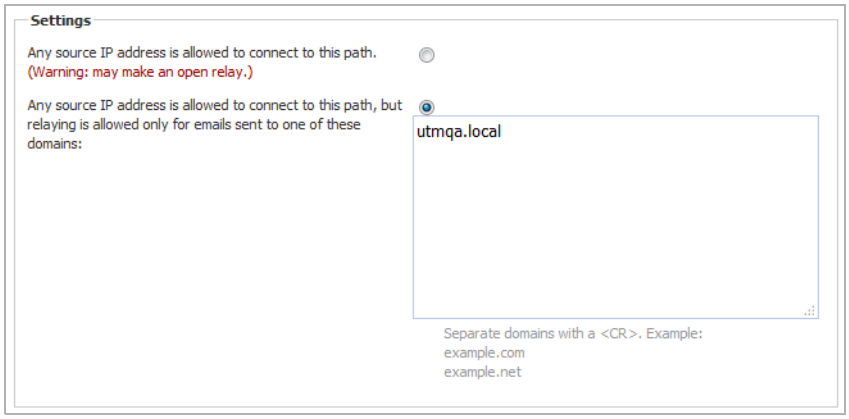
將 CASS 設定為開放轉接時，即使郵件目的地不為收件者網域，也將轉接郵件。未將 CASS 設定為開放轉接時，轉接擁有已列出收件者網域之一的電子郵件；對於未列出的網域，將拒絕郵件。列出允許的轉接網域可避免不必要的電子郵件轉接，即使郵件目的地不為此使用者。

列出允許的轉接網域

您可以列出所有轉接使用的網域。

列出已授權轉接網域的步驟是：

1 導覽**反垃圾郵件 > 轉接網域**的**設定**部分。



2 選擇是否限制轉接網域：

- **所有來源 IP 位址都允許連接此路徑** - 允許所有網域轉接郵件。移至步驟 4。

△ 注意：**選擇此選項可能使 CASS 變為開放轉接。即使郵件目的地不為收件者網域，也將轉接郵件，這可能導致垃圾郵件。**

- **所有來源 IP 位址都允許連接此路徑，但只許對向下列某個網域傳送的電子郵件進行轉接** - 僅允許列出的網域轉接郵件。

3 在此欄位中輸入允許轉接郵件的網域。以輸入鍵符號 (<CR>) 隔開網域。

4 按一下**套用變更**。

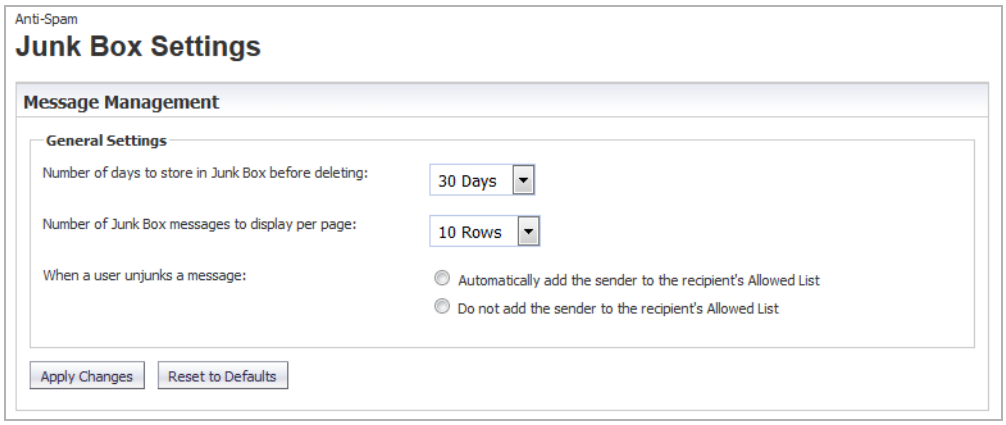
26

設定垃圾郵件設定

附註：反垃圾郵件 > **垃圾儲存區設定**不適用於 SuperMassive 9800。

反垃圾郵件 > **垃圾儲存區設定**頁面用於設定：

- 郵件在垃圾儲存區中存放的時間（經過此時間後即將之刪除）。
- 垃圾儲存區每頁顯示的郵件數。
- 使用者設定非垃圾郵件時執行的操作。



執行郵件管理的步驟如下：

1 在**郵件管理**部分，從**刪除之前儲存在垃圾儲存區的天數**下拉功能表選擇垃圾郵件刪除前的儲存天數。最小值為 1 天，最大值為 180 天，預設值為 **15 天**。

2 在**調查 | 記錄 | 反垃圾郵件垃圾儲存區**頁面的**傳入**檢視的**找到的郵件**部分，從**垃圾儲存區每頁顯示的郵件數**下拉功能表，選擇郵件顯示的行數。最小值為 10 行，最大值為 400 行，預設值為 **400 行**。

3 從**使用者設定非垃圾郵件時**選擇是否將非垃圾郵件發件人新增到收件者的允許清單；兩個選項均未預設選擇：

- **將發件人自動新增到收件者的允許清單中**
- **不將發件人新增到收件者的允許清單中**

4 按一下**套用變更**。

恢復到預設值的步驟為：

1 按一下**重設為預設值**按鈕。

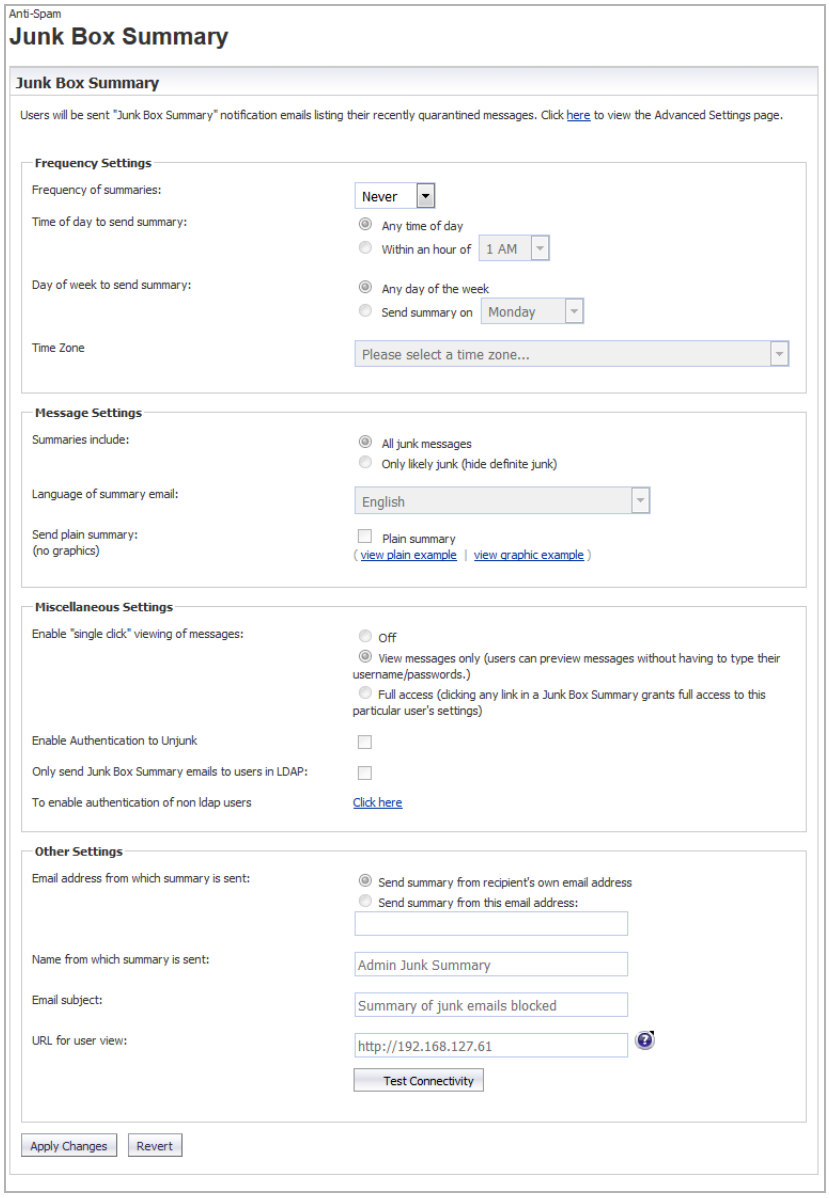
27

管理垃圾郵件摘要

附註：反垃圾郵件 > **垃圾郵件摘要**不適用於 SuperMassive 9800。

「垃圾儲存區」向使用者傳送一封電子郵件，列出所有已放入「垃圾郵件摘要」中的郵件。**反垃圾郵件 > 垃圾郵件摘要**頁面用於設定使用者的「垃圾郵件摘要」。

如需設定已登入的郵件類型，請按一下**反垃圾郵件 > 進階設定**頁面的連結。



反垃圾郵件 > 垃圾儲存區摘要設定頁面用於設定這些選項：

- **頻率設定** - 設定垃圾郵件摘要傳送至您的頻率和時間。
- **郵件設定** - 設定摘要中所包含的內容、語言及摘要是否包含圖形。
- **雜項設定** - 設定按一下檢視郵件和身分驗證等選項。
- **其他設定** - 設定摘要傳送者、電子郵件主旨及使用者 URL 等選項。

主題：

- 管理垃圾郵件摘要
- 恢復為預設值

管理垃圾郵件摘要

管理垃圾郵件摘要的步驟如下：

1 在**垃圾儲存區摘要設定**頁面的**頻率設定**部分中，從**摘要頻率**下拉功能表中選擇向您傳送摘要的頻率。

最小頻率為 **14 天**，最大頻率為 **1 小時**，預設值為 **1 天**。如需避免向您傳送摘要，請選擇**從不**。

2 從**摘要傳送時間**選項中選擇以自訂您使用者接收電子郵件通知的時間。

附註：個人使用者可覆寫此設定。

- **任何時間**（預設）
- **以下時刻之後的一小時內** - 從下拉功能表中選擇時間；預設值為 **12 AM**

3 如果已從**摘要頻率**下拉功能表中選擇 **7 天**或 **14 天**，**摘要傳送時間**選項將變為可用。如需自訂您使用者接收電子郵件通知的日期，請選擇以下任一項：

附註：個人使用者可覆寫此設定。

- **每週的任何一天**（預設）
- **摘要傳送時間** - 從下拉功能表中選擇一週的某一天；預設值為**星期一**

4 另外，也可從**時區**下拉功能表中，選擇在頻率確定中要使用的格林威治標準時間 (GMT)。

5 在**郵件設定**部分中，從**摘要包含**選項中選擇要包含在郵件摘要中的內容：

- **所有垃圾郵件**（預設）
- **僅可能的垃圾郵件（隱藏確切垃圾郵件）**

6 另外，也可從**摘要電子郵件的語言**下拉功能表中選擇一種語言。

7 如需**傳送普通文字摘要（無圖形）**，可按一下**普通文字摘要**核取方塊以選擇是否使摘要不包含圖形。預設情況下，摘要中包含圖形。

a 如需查看任一版本範例，按一下相應連結：

- 檢視普通文字範例

垃圾郵件匣摘要，針對：biz@example.com

過去 24 小時內，您公司收到了 8040 封垃圾郵件和 1122 封有效郵件。

垃圾郵件封鎖：24 封
下面所列是上一個「垃圾郵件匣摘要」之後的電子郵件，已經放到您的個人「垃圾郵件匣」中，並且會在 90 天後予以刪除。若要收到任何這些郵件，請按下「非垃圾」。該郵件便會傳送到您的「收件匣」。

垃圾郵件匣摘要

[非垃圾] [檢視]	johnn@180solutions.com	Re: 180 Advertising
[非垃圾] [檢視]	dmcswzzain@hotmail.com	-*- YES, Earn a Doctors income wi...
[非垃圾] [檢視]	support@ebay.com	Win Free Stuff
[非垃圾] [檢視]	spammer@corp.net	Take Some Viagra, its Cheap
[非垃圾] [檢視]	jlef@mb12.com	Enlarge another body part
[非垃圾] [檢視]	sally@getitup.com	Nigerian Prince wants your PIN number
[非垃圾] [檢視]	edd@aled.net	Mortgage rates that are just OK
[非垃圾] [檢視]	aber@ls.i.ua	95% off of our Yahts
[非垃圾] [檢視]	save@real-profesions.com	Become a surgeon in only two weeks
[非垃圾] [檢視]	openit@dareyou.com	Open this attachment: crack.exe
[非垃圾] [檢視]	cuz@find-family.com	Your long lost half cousin
[非垃圾] [檢視]	tic-tac@halatosis.com	Does your breath stink? Mine did
[非垃圾] [檢視]	smash-mouth@onthesun.com	Hey now, your an all-star, go play
[非垃圾] [檢視]	wow@cards-for-all.com	Playing cards of Canada's Most Wanted
[非垃圾] [檢視]	mr.tingles@petstylist.com	Pajamas for your Poodle
[非垃圾] [檢視]	info@paypal.com	Paypal lost your info. Please submit again
[非垃圾] [檢視]	strawberry@jam12.net	Platinum Membership to the Jam Club
[非垃圾] [檢視]	sir@mixalot.com	I like big butts and I can not lie
[非垃圾] [檢視]	hard-drive@yourpc.com	A Message From Your Computer: I need updates
[非垃圾] [檢視]	warning@alertsPC.com	*!Alert. Read this. Click on buttons or BOOM
[非垃圾] [檢視]	3l33l@haxor.i.ua	l33t H@x0r eZ xPl0ts
[非垃圾] [檢視]	ez@speller.com	Learn to read words like a Pro
[非垃圾] [檢視]	biggy@fat-guru.com	Secret strategies of staying unemployed and fat
[非垃圾] [檢視]	opportunity@yesyoucan.com	Crop dusting jobs for Arab Americans

若要管理個人垃圾郵件的封鎖設定，請使用您的標準使用者名稱和密碼由此處登入：
http://twinpeaks.corp.example.com

SonicWALL, Inc. 將其視為垃圾而予以封鎖

- 檢視圖形範例

b 關閉視窗。

8 在**雜項設定**部分中，從**啟用「按一下」檢視郵件**選項中選擇電子郵件垃圾儲存區摘要通知的檢視方式：

- **關閉**
- **僅檢視郵件（使用者不必輸入其使用者名稱/密碼即可預覽郵件。）**（預設）
- **最高存取權（按一下垃圾郵件摘要中的任何連結都會授予對此指定使用者的設定的最高存取權。）**

9 如需使使用者驗證非垃圾郵件，請選擇**啟用非垃圾郵件驗證**核取方塊。預設情況下未勾選此選項。

10 如需僅向 LDAP 中的使用者傳送垃圾郵件摘要通知，請選擇**僅向 LDAP 中的使用者傳送「垃圾郵件摘要」電子郵件**核取方塊。

11 如需啟用驗證非 LDAP 使用者，請按一下**如需啟用驗證非 ldap 使用者，請按一下這裡**連結。隨即顯示**反垃圾郵件 > 使用者**頁面；如需管理使用者的更多資訊，請參見管理垃圾郵件摘要。

12 在**其他設定**部分中，從**摘要的電子寄件地址**中選擇一個選項以選擇摘要傳送方式：

- **透過收件者自己的電子郵件地址傳送摘要**（預設）
- **透過此電子郵件地址傳送摘要**

a) 在欄位中輸入一個電子郵件地址

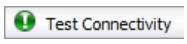
13 在**摘要的電子郵件發件人**欄位中，輸入要顯示在摘要電子郵件的使用者電子郵件中的名稱。預設名稱是 **Admin Junk Summary**。

14 在**電子郵件主旨**欄位，輸入垃圾郵件摘要電子郵件的主旨行。預設主旨行為**已封鎖垃圾郵件的摘要**。

15 **使用者檢視的 URL** 欄位將根據您的伺服器設定自動填入。它是垃圾郵件摘要電子郵件中的所有連結的基礎。如果已設定此設定，會向每個使用者傳送使用者已收到電子郵件威脅的「垃圾郵件摘要」電子郵件清單。

「垃圾郵件摘要」電子郵件包含能執行以下操作的 URL：

- 檢視隔離的電子郵件。
- 將隔離的電子郵件設定為非垃圾郵件；使用者可按一下垃圾郵件摘要電子郵件中的連結，設定郵件為非垃圾郵件。
- 登入至「垃圾儲存區」。

重要：如需變更此 URL，為確保正確連接，應在變更時按一下**測試連線性**  按鈕測試此連結。如果測試失敗，請檢查 URL 是否正確。

16 按一下**套用變更**按鈕。

恢復為預設值

你可以隨時將所有自訂設定恢復為預設值。

恢復到預設值的步驟為：

1 按一下**恢復**按鈕。

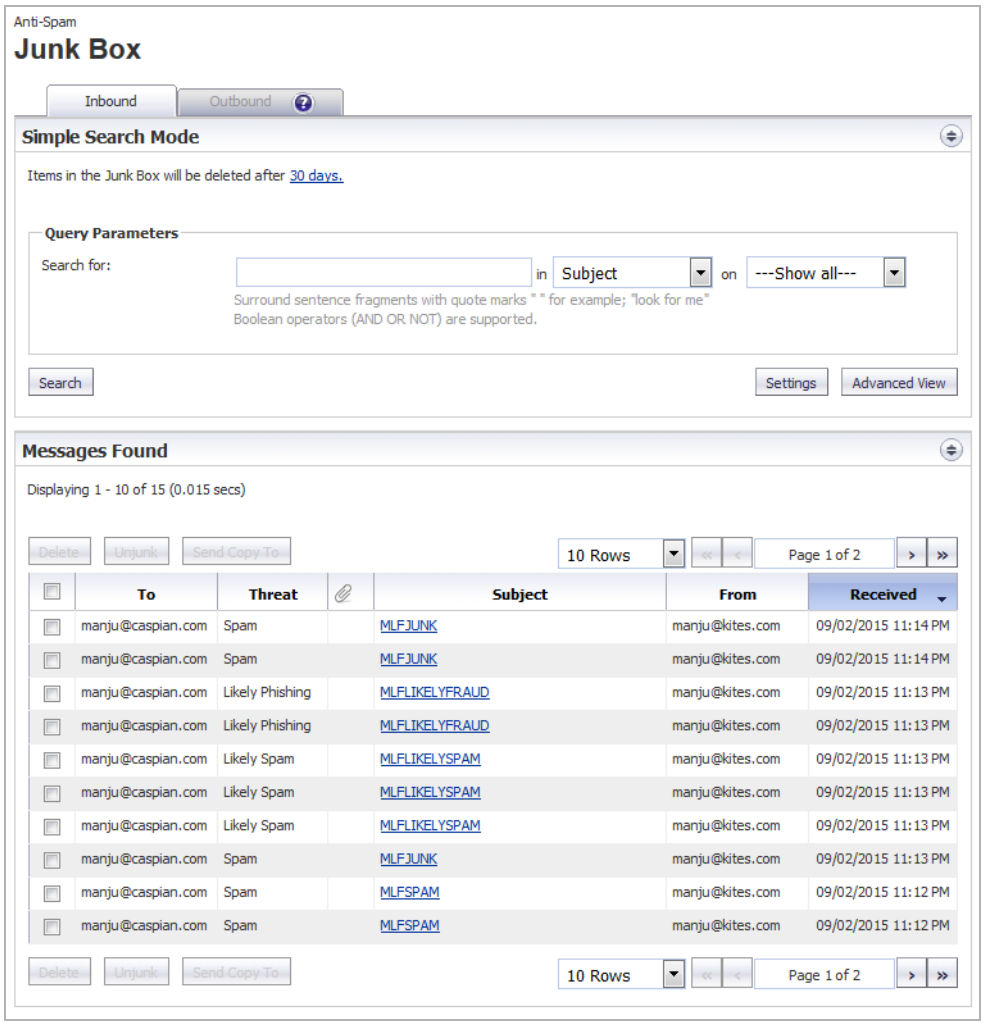
28

設定垃圾郵件檢視

附註：反垃圾郵件 > **垃圾儲存區**不適用於 SuperMassive 9800。

在**調查 | 記錄 | 反垃圾郵件垃圾儲存區**頁面，可以檢視、搜尋、管理目前位於 Exchange 或 SMTP 伺服器上的垃圾儲存區中的所有電子郵件。

附註：此功能只能在已安裝垃圾儲存區的情況下使用。



主題：

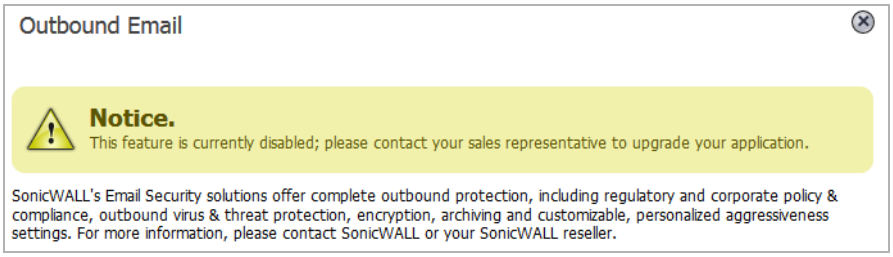
- 關於「垃圾儲存區」標籤
- 搜尋郵件

- 管理垃圾儲存區中的郵件

關於「垃圾儲存區」標籤

調查 | 記錄 | 反垃圾郵件垃圾儲存區頁面包含兩個標籤：

- **輸入**，僅列出輸入郵件
- **輸出**，僅列出輸出郵件

> **附註：**如果無法檢視**傳出**檢視，則必須升級您的垃圾儲存區授權。如果按一下**問號**圖示，即顯示此郵件：
>
> 
>

這兩個標籤的功能和顯示相同。每個檢視包含兩個部分：

- **簡單/進階搜尋模式**
- **找到的郵件**

您可以按一下**展開/收起**圖示，收起或展開任一部分。

在**簡單搜尋模式**部分中，有其他頁面的兩個連結：

- 如需變更垃圾郵件在刪除前所保留的持續時間，請按一下此部分頂部的**垃圾儲存區中的項目 nn 天後將刪除**末尾處的連結。
- 如需顯示**反垃圾郵件 > 垃圾儲存區設定**頁面，請按一下此部分底部的**設定**按鈕。

找到的郵件表中顯示的資訊

找到的郵件表顯示隔離郵件的相關資訊：

隔離郵件的相關資訊

此欄	包含或指示
核取方塊圖示	表中每個項目的核取方塊。按一下標題中的**核取方塊**圖示可選擇表中的所有項目。
目的地	收件者電子郵件地址。
威脅	電子郵件構成的威脅類型；如需威脅類別的更多資訊，請參見設定電子郵件威脅類別中的電子郵件威脅類別設定：選項表格。
回形針圖示	電子郵件包含附件。
主題	郵件主旨行。
來源	發件人電子郵件地址。
接收	注明郵件傳送時間。

使用**找到的郵件**表頂部和底部的按鈕執行以下「垃圾儲存區」管理任務（參見郵件表按鈕表格）（在**調查 | 記錄 | 反垃圾郵件垃圾儲存區**頁面）：

郵件表按鈕

按鈕	功能
刪除	永久刪除「垃圾儲存區」中的所選郵件；如需刪除所有郵件，請按一下表標題中的核取方塊
非垃圾郵件	從垃圾儲存區中移除所選郵件，將其傳遞給目的地使用者。每封郵件送達使用者郵件箱時，送達時間和日期由 Exchange 伺服器設定。
將副本傳送到	將所選郵件保留在垃圾儲存區中，將其副本傳送給使用者。

搜尋郵件

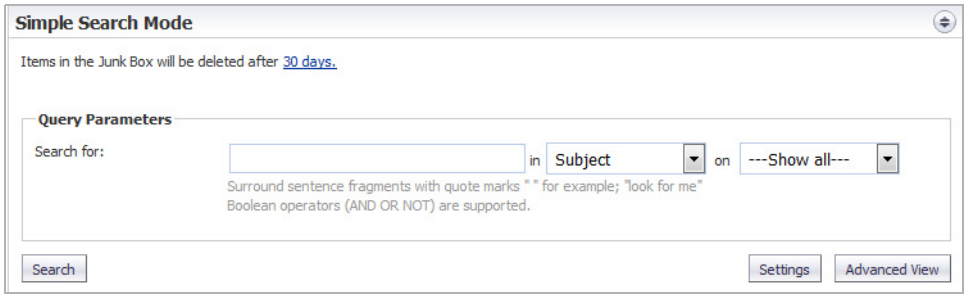
您可以對「垃圾儲存區」中「找到的郵件」執行兩種類型搜尋：

- 簡單；參見執行簡單搜尋
- 進階；參見執行進階搜尋

執行簡單搜尋

搜尋垃圾儲存區的步驟如下：

1 在**調查 | 記錄 | 反垃圾郵件垃圾儲存區**頁面，選擇**傳入**檢視或**傳出**檢視。



2 將要搜尋的文字輸入至**搜尋**欄位。

將句子片段括在引號 (「) 內。可使用布林運算子（AND、OR、NOT）。

3 在下拉功能表**在**選擇要搜尋的目的地電子郵件欄位：

- **主旨**（預設）
- **來源**
- **目的地**
- **唯一郵件 ID**

4 在**日期**下拉功能表中，選擇要搜尋的日期。

- **---顯示全部---**（預設）
- **今天**
- 指定日期；日期數將根據垃圾郵件保留的時間長度而有所差異

5 按一下**搜尋**按鈕開始搜尋。

結果將顯示在頁面的**找到的郵件**部分中，並在頂部顯示一封郵件。如果搜尋成功，此郵件將包含**成功！**字樣且整個郵件將以綠色高亮顯示。如果搜尋失敗，此郵件將包含**警告！**字樣且整個郵件將以黃色高亮顯示。

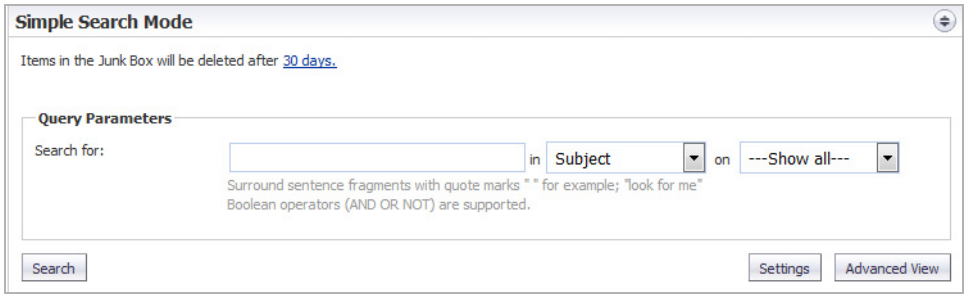
6 將**找到的郵件**表恢復至其原始狀態的步驟如下：

a 刪除**搜尋**欄位中的資料。

b 按一下**搜尋**。

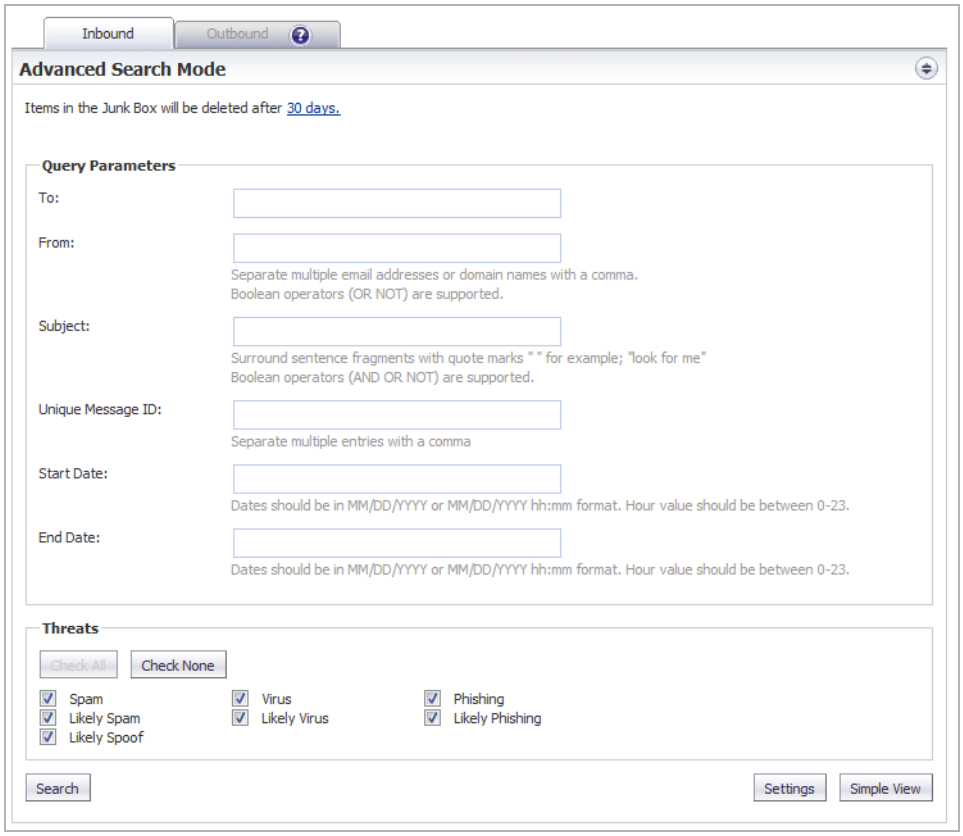
執行進階搜尋

1 在**調查 | 記錄 | 反垃圾郵件垃圾儲存區**頁面，選擇**傳入**檢視或**傳出**檢視。



附註：如需變更設定，請按一下**垃圾儲存區中的項目 *nn* 天後將刪除** 以顯示**反垃圾郵件 > 垃圾儲存區設定**頁面。

2 按一下**進階檢視**按鈕。**簡單搜尋模式**展開成為**進階搜尋模式**部分。



3 在**查詢參數**部分，將您的搜尋條件輸入至一個或多個**查詢參數**欄位：

參數	查詢條件
目的地	收件者電子郵件地址。
來源	發件人電子郵件地址。 用逗號隔開多個電子郵件地址或網域名稱。支援布林運算子 OR 和 NOT。
主題	郵件主旨。 將句子片段括在引號 (「) 內。支援布林運算子 AND、OR 和 NOT。
唯一郵件 ID	唯一郵件 ID。 用逗號隔開多個項目。
起始日期	要搜尋的起始日期。 輸入任一格式的日期： • MM/DD/YYYY • MM/DD/YYYY hh:mm（小時值應介於 0 至 23 [24 小時制] 之間）
結束日期	要搜尋的結束日期。 輸入任一格式的日期： • MM/DD/YYYY • MM/DD/YYYY hh:mm（小時值應介於 0 至 23 [24 小時制] 之間）

4 在**威脅**部分中，指定要搜尋的威脅類別。預設情況下，選擇所有類別。

按一下您不想包含的任何類別核取方塊，可在搜尋中取消選擇此類別。如需取消選擇所有類別，請按一下**取消全部勾選** Check None 按鈕。所有類別將取消勾選，**全部勾選** Check All 按鈕啟用且**取消全部勾選**按鈕變為灰色。

只有屬於某一電子郵件威脅類別（將其在**反垃圾郵件 > 設定**頁面上設定為**儲存在垃圾儲存區**）的郵件，才會包括在垃圾儲存區中。但是，無論某一類別的郵件是否儲存在垃圾儲存區，此頁面都將列出所有類別。

附註：如需變更這些設定，請按一下**設定**按鈕；隨即顯示**反垃圾郵件 > 垃圾儲存區設定**頁面。

5 按一下**搜尋**按鈕開始搜尋。

結果將顯示在頁面的**找到的郵件**部分中，並在頂部顯示一封郵件。如果搜尋成功，此郵件將包含**成功！**字樣且整個郵件將以綠色高亮顯示。如果搜尋失敗，此郵件將包含**警告！**字樣且整個郵件將以黃色高亮顯示。

6 如需返回至**簡單檢視**，請按一下**簡單檢視**按鈕。

7 將**找到的郵件**表恢復至其原始狀態的步驟如下：

a 刪除**搜尋**欄位中的資料。

b 按一下**搜尋**。

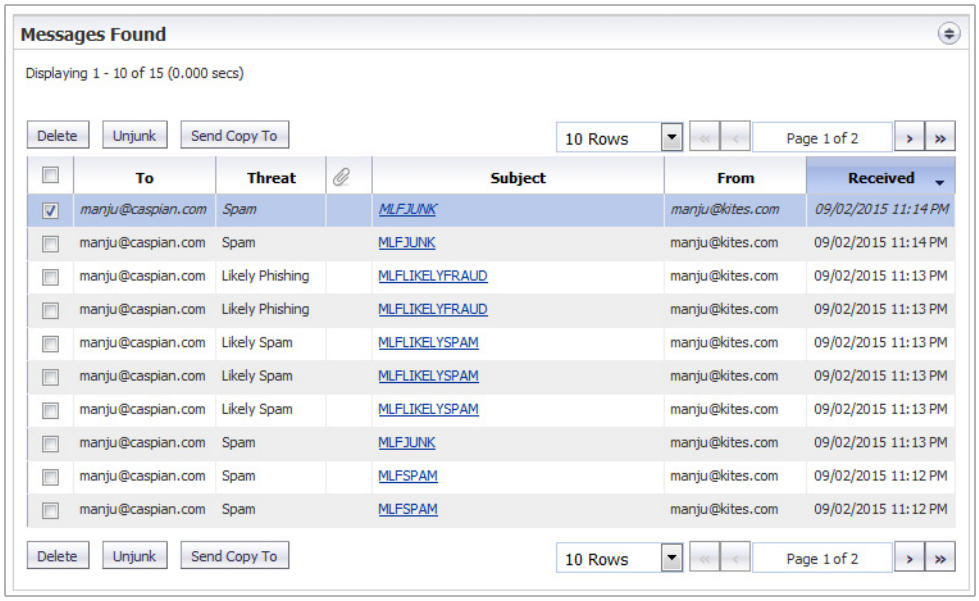
管理垃圾儲存區中的郵件

提示：如果您不搜尋「垃圾儲存區」，請按一下**簡單/進階搜尋模式**部分的**收起**圖示。

您可以刪除、傳送一份「垃圾儲存區」郵件，也可將其設定為非垃圾郵件。

管理垃圾儲存區的步驟如下：

1 在**調查 | 記錄 | 反垃圾郵件垃圾儲存區**頁面，捲動到**找到的郵件**表。



2 勾選您要管理的郵件的核取方塊。

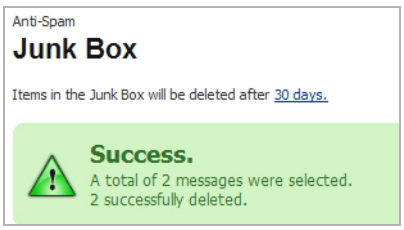
提示：如需選擇所有郵件，請勾選表標題中的核取方塊。所有核取方塊已核取。

3 執行郵件任務：

- 如需永久刪除「垃圾儲存區」中的所選郵件，請按一下**刪除**按鈕。

  附註：郵件將在 30 天後自動刪除。

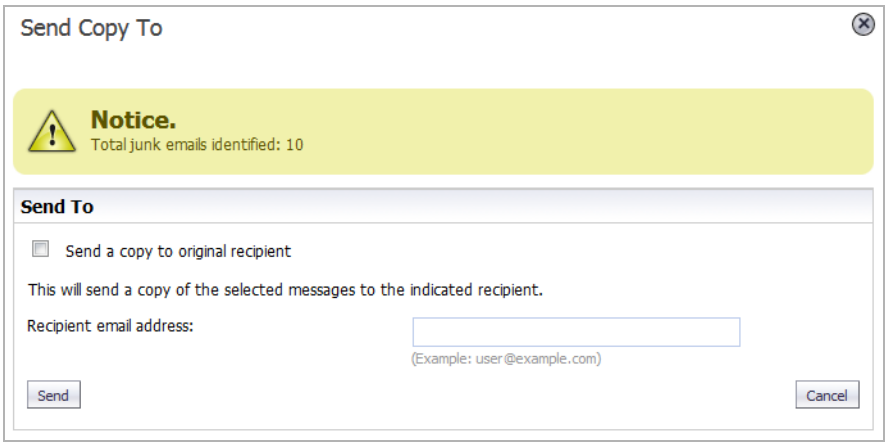
  將立即刪除所選郵件，刪除之前無確認對話方塊。如果刪除成功，頁面頂部會顯示一則綠色通知。如果刪除失敗，通知為紅色。



- 如需移除「垃圾儲存區」中的所選郵件並將其傳送至收件者，請按一下**非垃圾郵件**按鈕。

  所選郵件將成為非垃圾郵件且立即傳送，傳送之前無確認對話方塊。如果操作成功，頁面頂部會顯示一則綠色通知。如果操作失敗，通知為紅色。

- 要將所選郵件的副本傳送給使用者，請按一下**將副本傳送到**按鈕。隨即顯示**將副本傳送到**對話方塊。



a) 執行以下任一動作：

- 勾選**向原收件者傳送副本**核取方塊。
- 將電子郵件地址輸入至**收件者電子郵件**欄位。

b) 按一下**傳送** Send 按鈕。

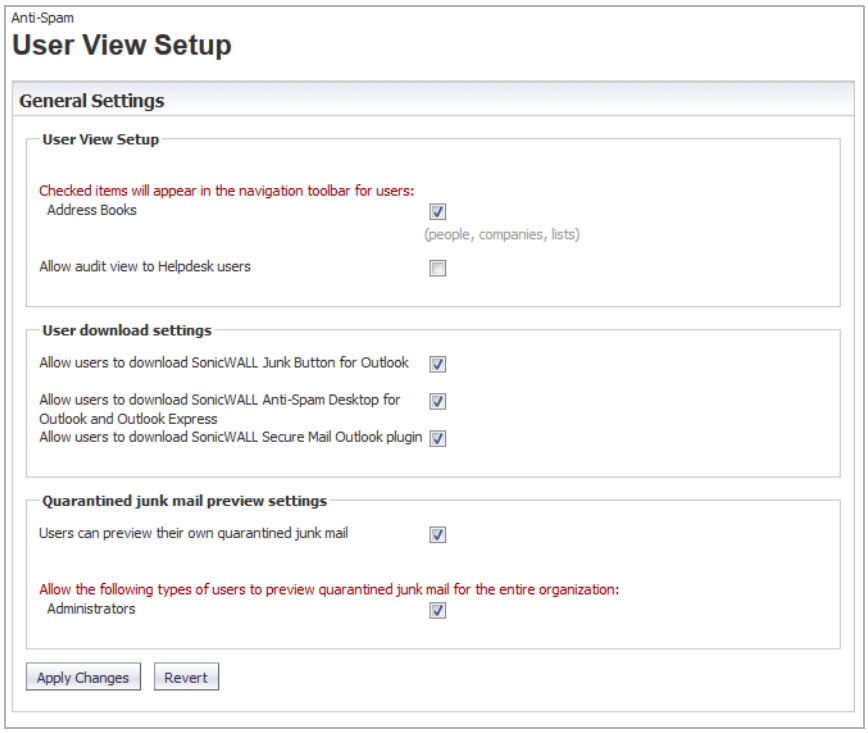
將立即傳送所選郵件 - 傳送之前無確認對話方塊。如果操作成功，頁面頂部會顯示一則綠色通知。如果操作失敗，通知為紅色。

29

設定使用者可視設定

附註：反垃圾郵件 > **使用者檢視設定**不適用於 SuperMassive 9800。

在**反垃圾郵件 > 使用者檢視設定**頁面上，您可以選擇和設定哪些設定對使用者可見。



主題：

- 設定使用者檢視設定
- 恢復到預設值

設定使用者檢視設定

附註：使用者的導航工具列上將顯示所選選項。

設定使用者看到的內容的步驟：

1 在**使用者檢視設定**部分，如果要使使用者能在導航工具列中看見自己的通訊錄（人員、公司和清單），請選擇**通訊錄**核取方塊。預設情況下已核取此選項。

2 如需允許支援使用者檢視電子郵件問題，勾選**允許支援使用者稽核檢視**核取方塊。預設情況下未勾選此選項。

3 在**使用者下載設定**部分，如需允許 Outlook 使用者下載垃圾郵件按鈕，勾選**允許使用者下載適用於 Outlook 的 SonicWall 垃圾郵件按鈕**核取方塊。預設情況下已核取此選項。

4 如需允許 Outlook 和 Outlook Express 使用者下載反垃圾郵件桌面，勾選**允許使用者下載適用於 Outlook 和 Outlook Express 的 SonicWall 反垃圾郵件桌面**核取方塊。預設情況下已核取此選項。

5 如需允許 Outlook 使用者下載 Secure Mail 插件，勾選**允許使用者下載 SonicWall Secure Mail Outlook 插件**核取方塊。預設情況下已核取此選項。

6 在**隔離垃圾郵件預覽設定**部分，如果要使使用者能預覽其隔離垃圾郵件，請勾選**使用者可預覽各自的隔離垃圾郵件**核取方塊。預設情況下已核取此選項。

7 如需允許管理員預覽整個組織的隔離垃圾郵件，勾選**管理員**核取方塊。預設情況下已核取此選項。

> **附註：** 預設情況下，管理員可存取預覽全公司的所有隔離垃圾郵件。若要變更此選項，請取消勾選**管理員**核取方塊。

8 完成所有必要的變更後，按一下**套用變更**按鈕。

恢復到預設值

您隨時可以將所有設定還原為出廠預設值。

隨時清除所做的變更並恢復預設值的步驟是：

1 按一下**恢復**按鈕。

30

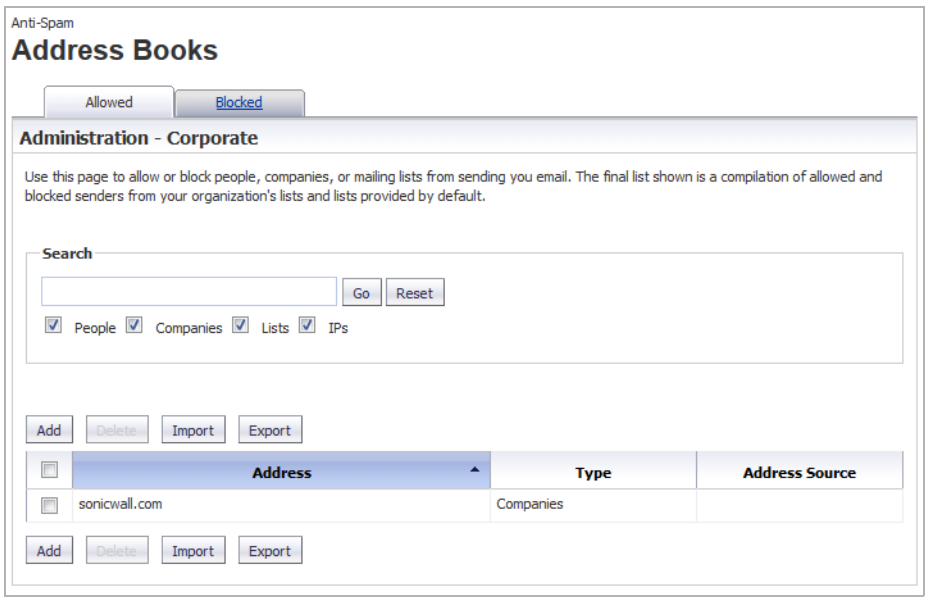
設定公司允許和封鎖清單

附註：反垃圾郵件 > 通訊錄不適用於 SuperMassive 9800。

在**反垃圾郵件 > 通訊錄**頁面上，您可以為您的機構設定「允許清單」和「封鎖清單」。這些清單彙集了公司的清單和防火牆提供的清單中允許的和封鎖的發件人。

附註：已封鎖檢視僅按人員、IP 和公司篩選位址，**允許**檢視則按人員、公司、IP 和清單篩選位址。

如果您的清單較長，您可以使用搜尋功能，僅顯示想要的表格項目。



主題：

- 關於標籤
- 將項目新增到允許清單或封鎖清單
- 從允許清單或封鎖清單刪除項目
- 匯入通訊錄項目
- 匯出通訊錄項目
- 搜尋允許和封鎖清單

關於標籤

允許和**已封鎖**這兩個標籤是相同的，除了兩個頁面的搜尋類別都有**人員**、**公司**和 **IP**，而**允許**頁面的搜尋類別還有**清單**。

主題：

- 允許清單
- 封鎖清單

允許清單

允許檢視用於允許人員、公司、IP 位址或清單向您的機構傳送電子郵件。您可以將通訊錄匯入允許清單，將公司通訊錄匯出到 Excel 試算表或文字檔。

封鎖清單

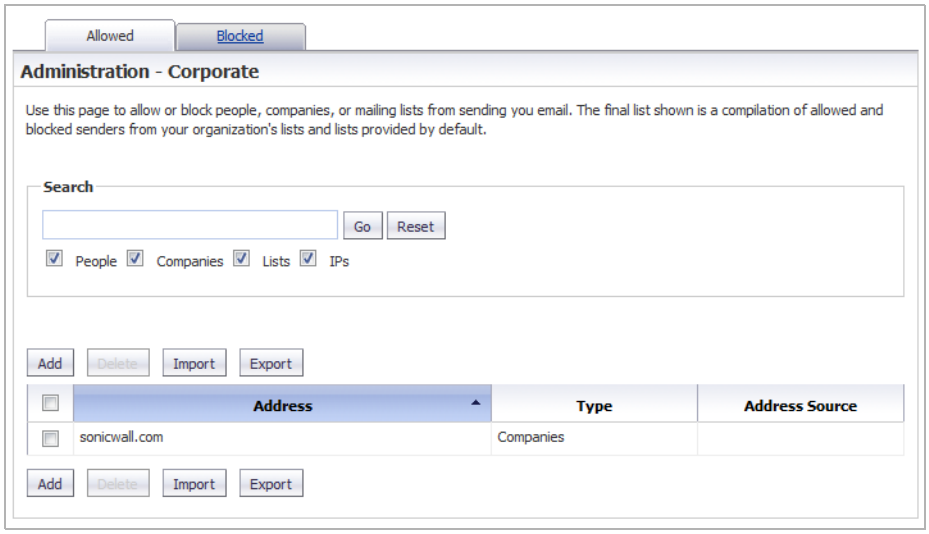
附註：所有使用者將自動封鎖由管理員新增到公司封鎖清單中的發件人，且只能由管理員刪除。

已封鎖檢視用於限制人員、公司和 IP 位址向您的機構傳送電子郵件。您可以將通訊錄匯入封鎖清單，將公司通訊錄匯出到 Excel 試算表或文字檔。

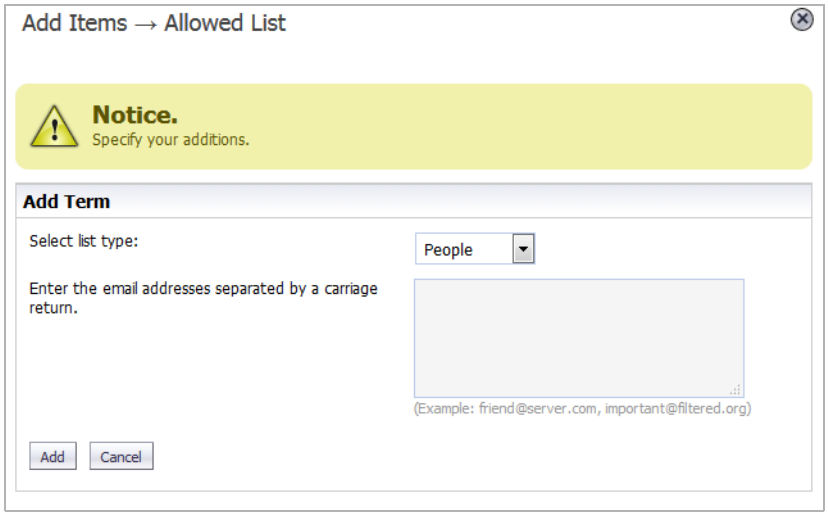
將項目新增到允許清單或封鎖清單

將項目新增到允許清單/封鎖清單的方法是：

1 導覽到**反垃圾郵件 > 通訊錄**相應的檢視。



2 按一下**新增**按鈕。將顯示**將項目新增到允許清單**對話方塊。



3 從**選擇清單類型**下拉功能表選擇清單使用者類型：

- **人員**
- **公司**
- **清單**（僅用於**允許**檢視）
- **IP**

4 在欄位中輸入位址/網域。根據所選清單類型，欄位名稱隨之改變：

- **人員 - 輸入以輸入鍵符號分隔的 IP 位址**
- **公司 - 請輸入網域，以輸入鍵符號分隔**
- **清單 - 請輸入郵件清單，以輸入鍵符號分隔**
- **IP - 輸入以輸入鍵符號分隔的 IP 位址**

5 按一下**新增**以完成操作。將位址/網域新增到**允許/已封鎖**檢視上的**清單**。

從允許清單或封鎖清單刪除項目

將傳送者從公司允許清單/封鎖清單刪除的方法是：

1 按一下相應檢視。

2 選擇想要刪除的電子郵件地址旁邊的核取方塊。**刪除**按鈕隨即啟用。

3 按一下**刪除**按鈕。隨即顯示一則成功訊息，確認已將之刪除。

ⓘ **提示：**如需刪除所有項目，按一下表格標題中的核取方塊。

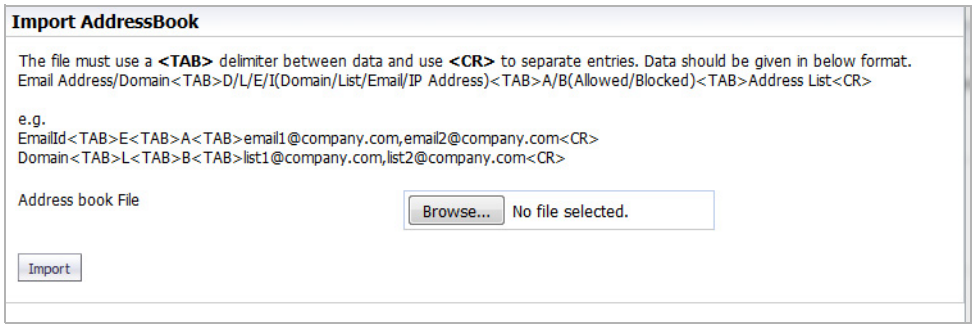
匯入通訊錄項目

您可以從一個或多個通訊錄中匯入項目。

匯入通訊錄項目的方法是：

1 按一下相應檢視。

2 按一下**匯入**按鈕。將顯示**匯入通訊錄**對話方塊。



3 按一下**瀏覽器**按鈕。將顯示視窗**檔案上載**對話方塊。

4 選擇要上載的檔案。其格式必須為：

<TAB>D/L/E/I<TAB>A/B<TAB>*位址清單*<CR>

其中

D/L/E/I - 網域/清單/電子郵件/IP 位址

A/B - 允許/封鎖

位址清單 - 通訊錄項目（由逗號隔開）

和電子郵件地址、網域、IP 位址和清單（以輸入鍵符號分隔）

例如：

<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>

<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>

5 按一下**打開**。

6 按一下**匯入**。

匯出通訊錄項目

您可以將項目匯出到 Excel 試算表或文字檔。

匯出通訊錄項目的方法是：

1 在相應檢視，按一下**匯出**按鈕。將顯示視窗**打開*檔案名稱*對話方塊。

2 選擇以下其中一種格式：

- **使用 Microsoft Excel 打開（預設）**
- **儲存檔案**

3 按一下**確定**。

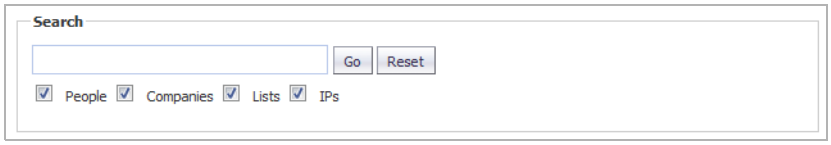
搜尋允許和封鎖清單

可使用搜尋欄位，在**允許**和**已封鎖**表格中快速查找允許和封鎖的項目。您可以從**允許**檢視或**已封鎖**檢視存取此欄位。

搜尋允許或封鎖清單的方法是：

1 按一下相應檢視。

2 移至**搜尋**部分。



3 在**搜尋**欄位輸入位址或網域。您可以輸入使用逗號分隔的多個項目。

4 此外，透過勾選搜尋欄下方的核取方塊，可以在不同的位址**類型**（**人員**、**公司**、**IP** 或**清單**）[僅限允許清單]之間篩選搜尋。預設情況下，已核取所有選項。

5 按一下**執行**按鈕開始搜尋。結果將顯示在**清單**表格中。

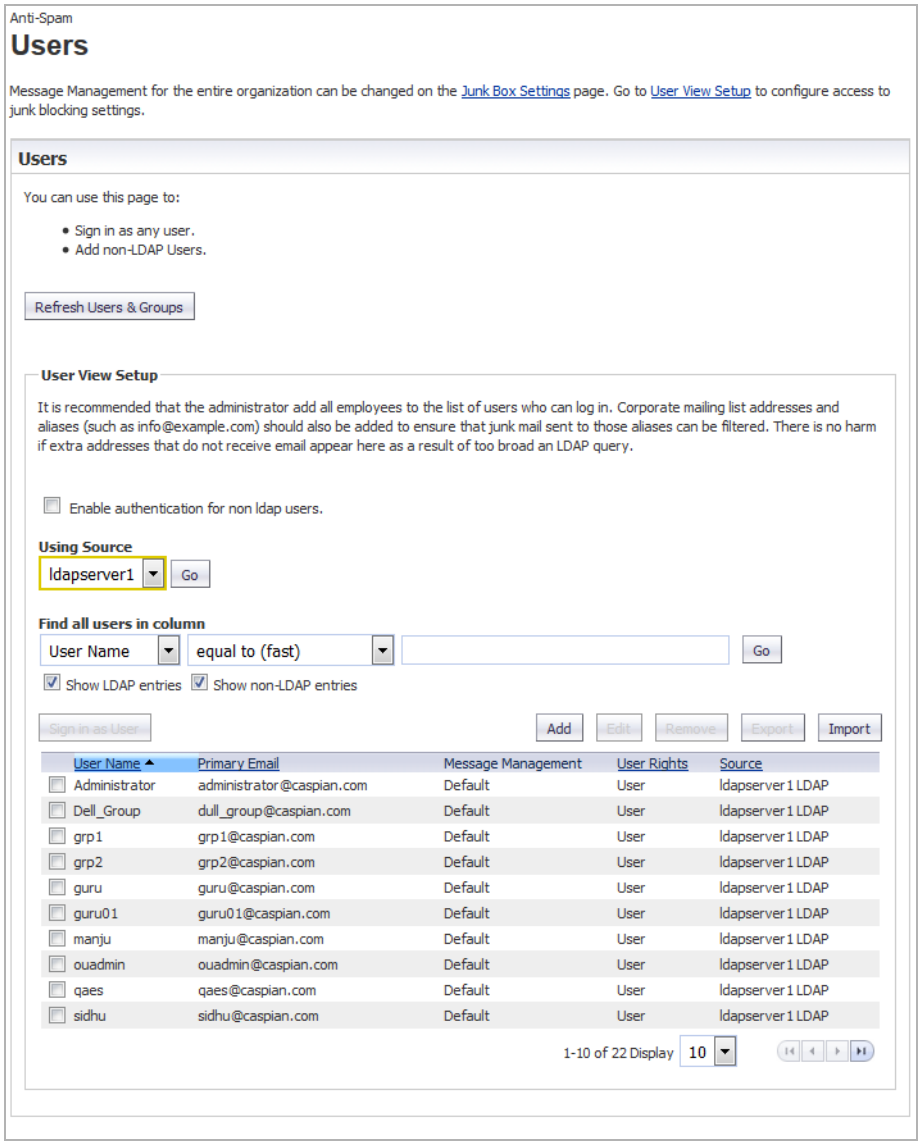
清除搜尋欄位的方法是：

1 按一下**重設**按鈕。

31

管理使用者

在**反垃圾郵件 > 管理使用者**頁面上，您可以新增、移除、管理所有使用者，包括「全域」和 LDAP 伺服器上的使用者。如需 LDAP 設定的更多資訊，請參見管理使用者。



使用者表顯示以下資訊：

欄	說明
使用者名稱	使用者的使用者名稱，此使用者名稱不能為主要電子郵件地址的一部分。
主要電子郵件	使用者的電子郵件地址。
郵件管理	顯示使用者是否遵循**反垃圾郵件 > 垃圾郵件摘要**頁面中的設定或是否已對其進行修改： • **預設** - 使用所有管理員設定 • **自訂** - 使用者已變更一個或多個設定
使用者權限	由於無法在 CASS 中修改使用者權限，因此始終為**使用者**。
來源	顯示使用者的伺服器名稱。

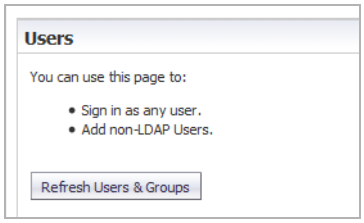
主題：

- 更新使用者表
- 啟用對非 LDAP 使用者的驗證
- 檢視使用者
- 新增使用者
- 以使用者身分登入

更新使用者表

更新「使用者表格」中使用者清單的步驟如下：

1 導覽至**反垃圾郵件 > 管理使用者**的**使用者**部分。



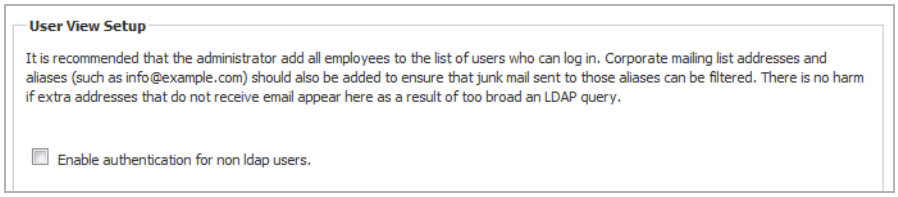
2 按一下**重新整理使用者和群組** Refresh Users & Groups 按鈕。

啟用對非 LDAP 使用者的驗證

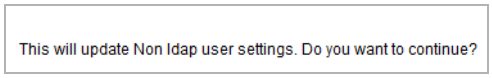
必須啟用非 LDAP 使用者驗證。

啟用對非 LDAP 使用者的驗證的步驟如下：

1 捲動至**反垃圾郵件 > 管理使用者**的**使用者檢視設定**部分。



2 勾選**啟用對非 ldap 使用者的驗證**核取方塊。將顯示警告訊息。



3 按一下**確定**。

檢視使用者

使用者表顯示可登入的所有使用者。您可以僅篩選目前您想查看的使用者，步驟如下：

- 選擇使用者類型：選擇要檢視的使用者類型
- 選擇來源（伺服器）；參見選擇要檢視的伺服器使用者
- 指定一個指定使用者；參見查找使用者

選擇要檢視的使用者類型

您可以查看所有使用者，僅 LDAP 使用者或僅非 LDAP 使用者。

選擇要顯示的使用者類型的步驟如下：

1 捲動至**反垃圾郵件 > 管理使用者**的**查看欄中的所有使用者**部分。

2 選擇以下使用者類型：

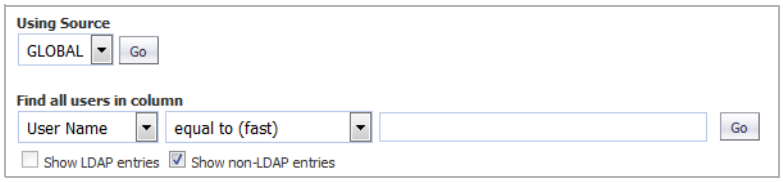
- 僅 LDAP - 勾選**顯示 LDAP 項目**核取方塊；當系統僅有 LDAP使用者時，這是預設值。
- 僅非 LDAP - 勾選**顯示非 LDAP 項目**核取方塊；當系統僅有非 LDAP使用者時，這是預設值。
- LDAP 和非 LDAP - 同時勾選這兩個核取方塊；當系統同時具有這兩類使用者時，這是預設值。

選擇要檢視的伺服器使用者

您可以限定**使用者**表以僅顯示指定伺服器中的使用者。

選擇來源（伺服器）的步驟如下：

1 移至**使用者檢視設定**的篩選部分。



2 從**使用來源**下拉功能表中，選擇要檢視的伺服器或來源：

- **全域**（預設）- 全域伺服器始終可用
- LDAP 伺服器名稱 - 如果已新增一個或多個 LDAP 伺服器，則列出所有伺服器名稱。

3 按一下**執行**按鈕。

查找使用者

您可以將檢視範圍僅限定於某一個使用者。

查找使用者的步驟如下：

1 移至**反垃圾郵件 > 管理使用者**中**使用者檢視設定**的篩選部分。

2 從**查找欄中的所有使用者**下拉功能表和欄位中，輸入選擇條件：

a 從第一個下拉功能表中，選擇：

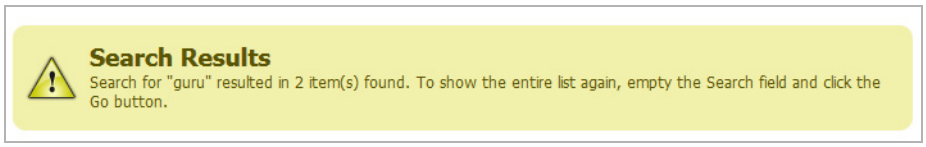
- **使用者名稱**
- **主要電子郵件**

b 按照第二個下拉功能表中的條件篩選搜尋：

- **等於（快）**（預設）
- **開頭字元（中等）**
- **包含（慢）**

c 在欄位中輸入使用者資訊。

3 按一下**執行**。**使用者**表僅顯示符合指定條件的電子郵件且頁面頂部將顯示一則訊息。



恢復使用者表顯示的步驟如下：

1 將搜尋條件從**查找欄中的所有使用者**欄位中移除。

2 按一下**執行**。

新增使用者

您可以將使用者新增至可以下列方式登入的使用者清單：

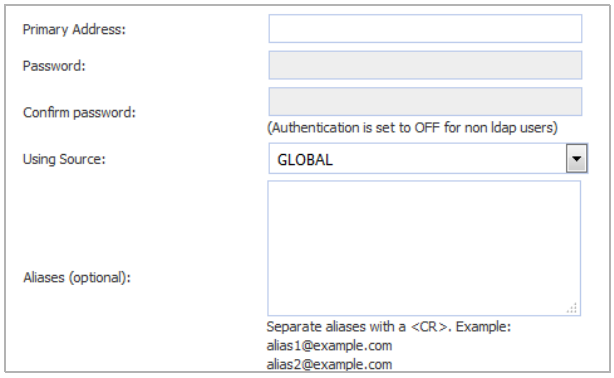
- 手動；參見將使用者手動新增至使用者表格
- 匯入；參見將使用者匯入使用者表

附註：建議您將所有雇員都新增到可登入使用者清單中。公司郵件清單位址和別名（如 info@example.com）也應該新增，以確保也篩選掉向那些別名傳送的垃圾郵件。此處顯示不接收電子郵件的其他位址，使得 LDAP 查詢面太寬，但沒有害處。

將使用者手動新增至使用者表格

若要將使用者新增到全域或 LDAP 伺服器：

1 按一下**使用者表**上面的**新增**按鈕。將顯示**新增使用者**對話方塊。



2 在**主要位址**欄位中輸入使用者的主要位址。

3 如果使用者為 LDAP 使用者，在**密碼**和**確認使用者**欄位中輸入使用者密碼。

4 從**使用來源**下拉功能表選擇使用者所屬伺服器。

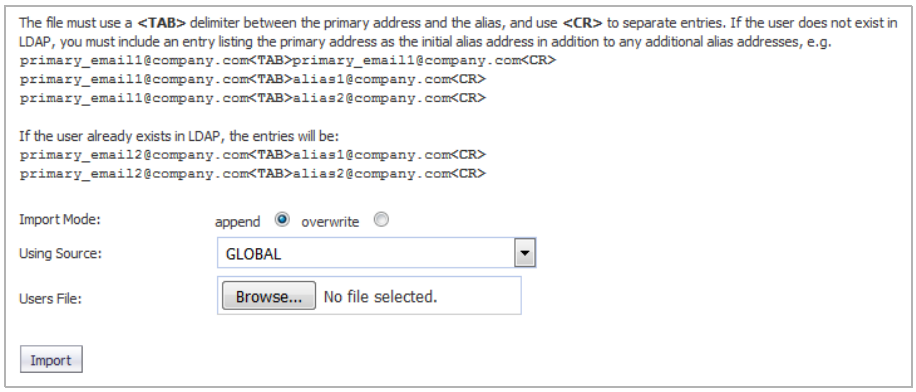
5 另外，也可在**別名**欄位中輸入任何使用者別名。用輸入鍵符號 (<CR>) 隔開每個項目。

6 按一下**新增**以完成使用者的新增。

將使用者匯入使用者表

從檔案匯入使用者清單的步驟如下：

1 按一下**使用者表**上面的**匯入**按鈕。隨即顯示**匯入使用者**對話方塊。



2 選擇**匯入模式**以選擇匯入檔案的處理方式：

- **附加** - 將使用者新增至包含審核使用者清單的檔案末尾處。
- **覆寫** - 將現有使用者替換為匯入使用者。

3 指定要用作來源的伺服器：

- **全域**
- LDAP 伺服器名稱

4 按一下**瀏覽器**按鈕。將顯示視窗**檔案上載**對話方塊。

5 選擇要上載的檔案。檔案必須滿足此格式，即在主要位址與別名之間使用標籤 <TAB> 分隔符號，並用輸入鍵符號 <CR> 分隔符號隔開項目：

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
```

例如：

```
primary_email1@company.com<TAB>primary_email@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
primary_email1@company.com<TAB>alias2@company.com<CR>
```

如果 LDAP 中已存在此使用者，項目將為：

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

6 按一下**打開**。

7 按一下**匯入**。

以使用者身分登入

您可以登入使用者帳戶查看其電子郵件安全**調查 | 記錄 | 反垃圾郵件垃圾儲存區**。

作為使用者登入的步驟如下：

1 導覽反垃圾郵件 > 使用者的**使用者**表。

2 勾選您想使用的登入身分的使用者核取方塊。**以使用者身分登入** Sign in as User 按鈕隨即啟用。

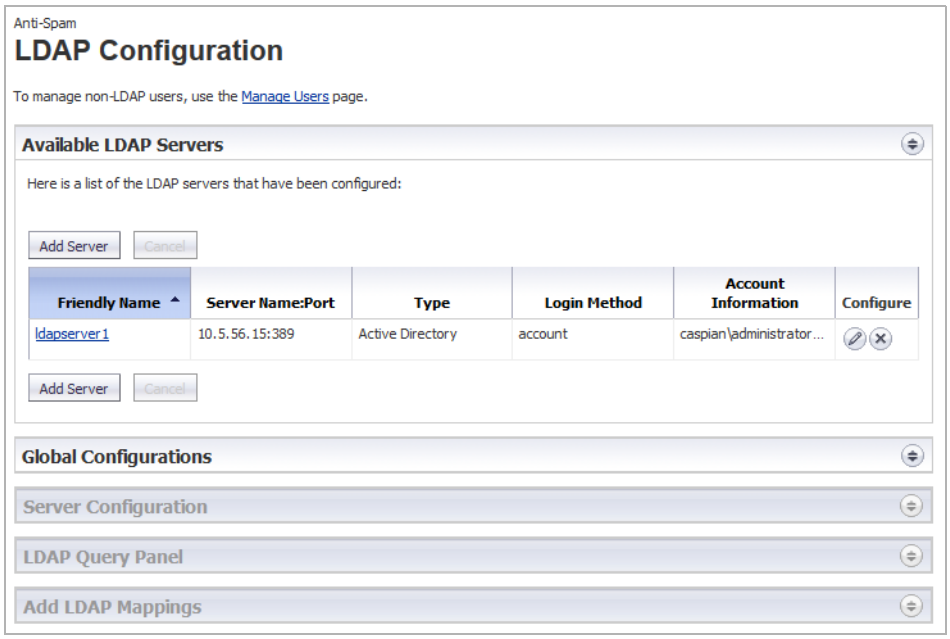
3 按一下**以使用者身分登入**按鈕。單獨的視窗顯示此使用者的電子郵件安全**反垃圾郵件 > 垃圾儲存區**頁面。

4 如需返回至 SonicOS **反垃圾郵件 > 管理使用者**頁面，按一下「電子郵件安全」頁面上的**登出**圖示。

32

設定 LDAP 伺服器

在**反垃圾郵件 > LDAP 設定**頁面上，您可以設定 LDAP 伺服器專用的各種設定。

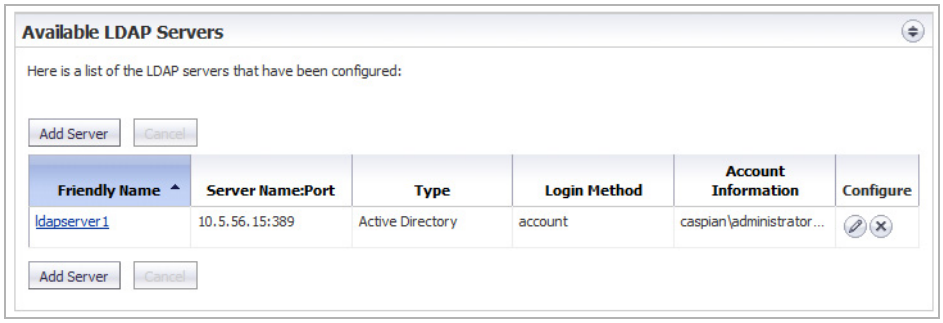


附註：按一下**展開/收起**圖示，可顯示或隱藏所有面板。

主題：

- 可用 LDAP 伺服器
- 新增 LDAP 伺服器
- 設定 LDAP 查詢
- 新增 LDAP 對應
- 設定全域 LDAP 設定
- 編輯 LDAP 伺服器設定
- 刪除 LDAP 伺服器

可用 LDAP 伺服器



此部分顯示在防火牆中設定的所有 LDAP 伺服器資訊：

- **易記的名稱** - 顯示伺服器的易記的名稱。按一下此連結可顯示**伺服器設定**、**LDAP 查詢面板**和**新增 LDAP 對應**部分。
- **伺服器名稱：連接埠** - 顯示伺服器的 IP 位址和連接埠。
- **類型** - 顯示伺服器類型，例如 Active Directory 或 OpenLDAP。
- **登入方法**
- **帳戶資訊** - 顯示
- **設定** - 包括 **編輯**和**刪除**圖示。

新增 LDAP 伺服器

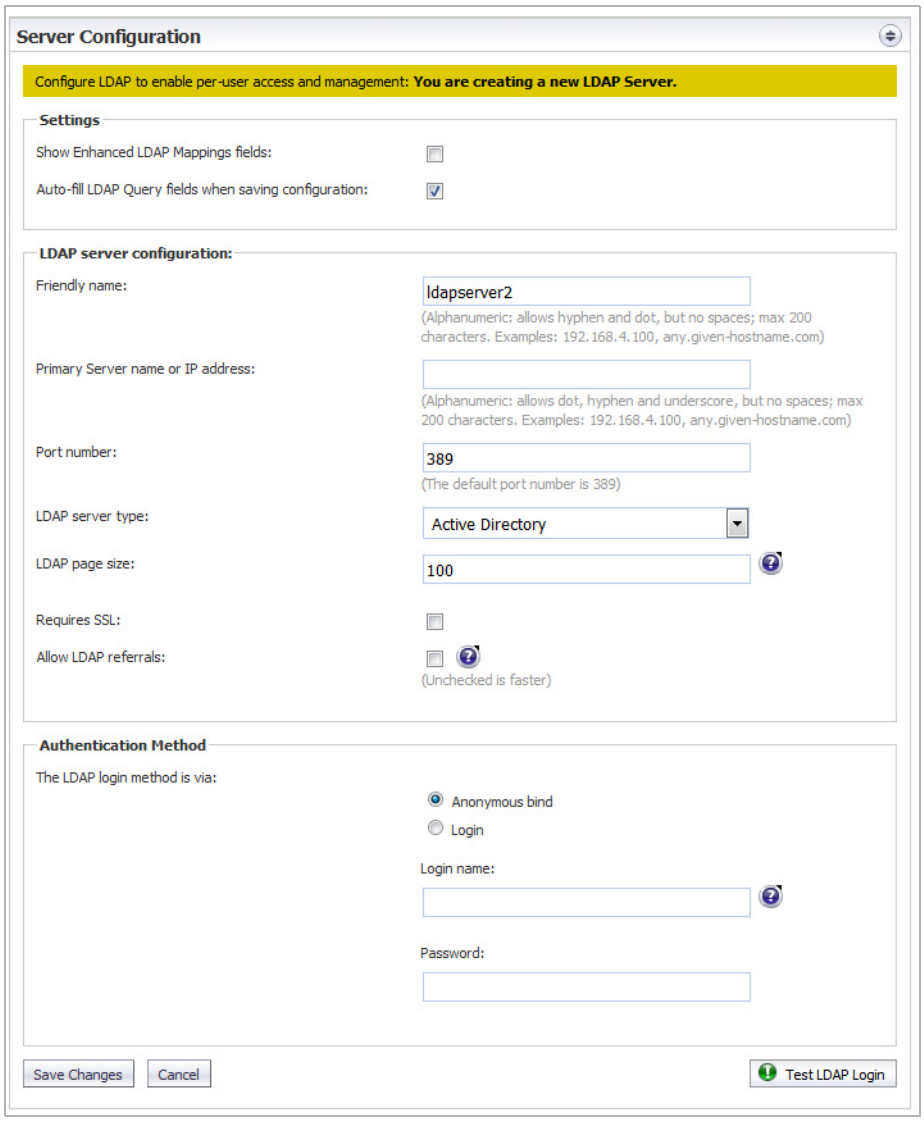
設定新 LDAP 伺服器以啟用針對各個使用者的存取和管理。

重要：當最終使用者登入其個人垃圾儲存區時，反垃圾郵件使用現有的 Active Directory 或 LDAP 伺服器驗證他們。必須正確填寫**反垃圾郵件 > LDAP 設定**頁面才會返回允許登入其垃圾儲存區的完整使用者清單。如果使用者沒有出現在此清單中，也會篩選其郵件，但他們無法登入到其個人垃圾儲存區。

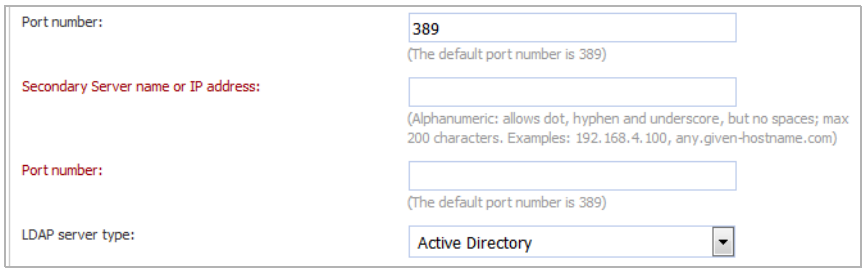
正確填寫 LDAP 設定需要填寫**伺服器設定**面板、**LDAP 查詢面板**和**新增 LDAP 對應**面板。

新增 LDAP 伺服器的步驟如下：

1 在**可用 LDAP 伺服器**部分，按一下**新增伺服器** Add Server 按鈕。將展開**伺服器設定**部分：



2 另外，也可在**設定**部分，啟用**顯示「增強 LDAP 對應」欄位**核取方塊。啟用此選項後，次要伺服器欄位將在 **LDAP 伺服器設定**部分顯示為紅色。



3 如需自動填入 **LDAP 查詢面板**中的欄位，請確保勾選**儲存設定時自動填入 LDAP 查詢面板**核取方塊。預設情況下已核取此選項。

4 在 **LDAP 伺服器設定**部分中，設定新 LDAP 伺服器設定：

提示：主要及次要伺服器名稱和 IP 位址可以達到 200 個字元，其中包括連字元 (-) 和 句點 (.)，但不包含空白字元。例如：

192.168.4.100
host-name123.com

- **易記的名稱**-輸入 LDAP 伺服器的易記的名稱。預設名稱為 `ldapservern`，其中 *n* 為序號。
- **主要伺服器名稱或 IP 位址** - LDAP 伺服器的名稱或 IP 位址。
- **連接埠編號** - LDAP 伺服器的連接埠編號。預設連接埠編號是 **389**。
- **次要伺服器名稱或 IP 位址** - LDAP 次要伺服器的名稱或 IP 位址。

  附註：僅當選擇**在設定中顯示「增強 LDAP 對應」欄位**部分時，**次要伺服器名稱或 IP 位址**和**連接埠編號**選項才顯示為紅色。

- **連接埠編號** - 次要 LDAP 伺服器的連接埠編號。預設連接埠編號是 **389**。
- **LDAP 伺服器類型** - 從下拉功能表中選擇：
  - **Active Directory**
  - **Lotus Domino**
  - **Exchange 5.5**
  - **Sun ONE iPlanet**
  - **其他**
- **LDAP 頁面大小** - 輸入要在 LDAP 伺服器上查詢的最大頁面大小。預設為 **100**。

注意：許多 LDAP 伺服器（包括 Active Directory）都有可指定要查詢的最大頁面大小的設定。如果「LDAP 頁面大小」設定超出最大頁面大小，則 LDAP 伺服器和 可能會出現效能問題。一般情況下它不需要調整，如果萬一需要調整，請諮詢 SonicWall 技術支援。

- **需要 SSL** - 如需使 LDAP 伺服器有 SSL，請選擇此核取方塊。預設情況下未勾選此選項。
- **允許 LDAP 轉介**-如果您有多台 LDAP 伺服器，其中各伺服器可能包含不同資訊，則選擇此選項。啟用 LDAP 轉介後，一台 LDAP 伺服器可以委派部分登入請求資訊給其他有更多資訊的 LDAP 伺服器。此委派稱為轉介，在管理員或使用者登入時發生。轉介的登入請求可能非常慢，耗時 20 秒或更長時間。預設情況下未勾選此設定。

  附註：如需加快管理員和使用者的登入速度，請在具備以下條件的情況下停用此選項：
  - 僅一台 LDAP 伺服器。
  - 兩台或更多 LDAP 伺服器且所有伺服器共用同一資訊。

  提示：安全的做法是停用轉介後測試是否有任何使用者無法登入。不會遺失任何資料或設定。

5 在**驗證方法**部分，設定使用者的 LDAP 登入方法：

- **匿名繫結**（預設）- 許多 LDAP 伺服器設定為向請求使用者清單的任何使用者提供使用者清單。這稱為*匿名繫結*。

  提示：先選擇此選項，然後再對其進行測試；參見步驟 8。

- **登入** - 如果**匿名繫結**選項失效，請選擇此選項。需提供使用者名稱和密碼才可讓 LDAP 返回使用者清單。

6 如果選擇：

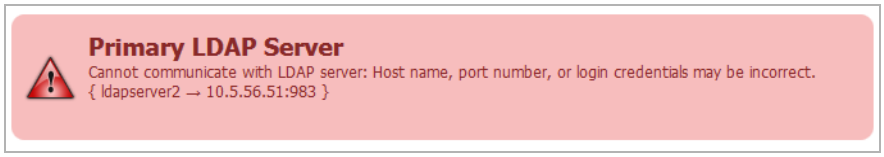
- **匿名繫結**，移至步驟 8。
- **登入**，移至步驟 7。

7 指定**登入名稱**和**密碼**。

登入名稱是用於讓使用者存取 LDAP 資源的憑證。每種 LDAP 伺服器類型都有一個登入名稱格式。請使用適合您伺服器的格式。

提示：如需查看不同格式的範例，請按一下**登入名稱**欄位旁的**問號**圖示。

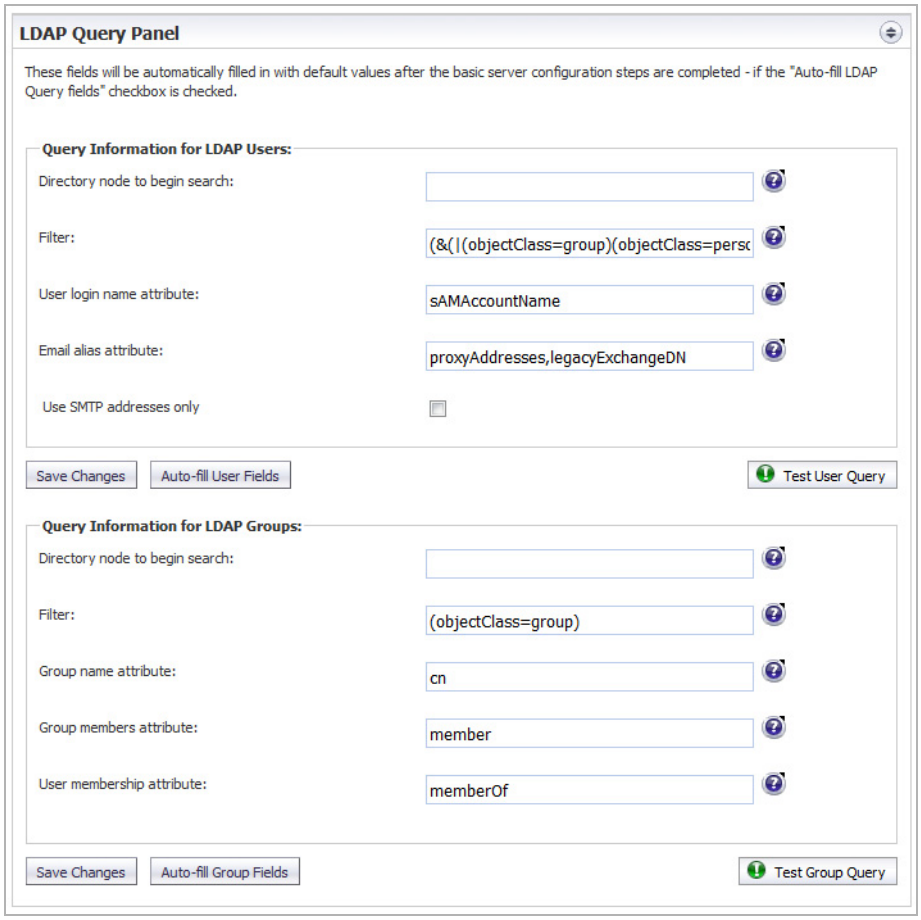
8 如需測試您剛剛設定的設定，請按一下**測試 LDAP 登入** Test LDAP Login 按鈕。顯示**測試結果**訊息：



9 按一下**儲存變更**，完成 LDAP 伺服器的新增。顯示 **LDAP 查詢面板**和**新增 LDAP 對應**面板。

設定 LDAP 查詢

提示：如果在**設定**部分中選擇了**儲存設定時自動填入「LDAP 查詢」**選項，**LDAP 查詢面板**將自動填入預設值。



允許使用者成功登入垃圾儲存區的步驟如下：

提示：如需整體檢查您的 LDAP 樹狀目錄以全面瞭解您的 LDAP 結構及其各種屬性和物件類別，請從以下網址執行免費程式 Softerra LDAP Browser 2.5：

http://www.ldapbrowser.com/download/index.php

在 Windows PC 中，下載此程式。執行此程式時，如需確定您網路的最佳查詢，請移至網路上的使用者並檢查其屬性。

1 在 **LDAP 查詢面板**中，移至 **LDAP 使用者的查詢資訊**部分。

提示：如果未在**設定**部分中指定**儲存設定時自動填入「LDAP 查詢」欄位**，可按一下**自動填入使用者欄位** Auto-fill User Fields 按鈕執行此操作。

2 如需使用可選的「群組」功能，請在**搜尋始於目錄節點**欄位中，指定完整的 LDAP 目錄路徑，它指向一個包含此目錄中所有群組資訊的節點（LDAP 內的目錄）。此路徑會將對 LDAP 群組的搜尋縮至合理的範圍。

LDAP 包含的資訊將組合成目錄樹狀目錄，這一點很像普通的檔案系統。每個目錄都指定為名稱=值對，其中：

- 名稱通常為：

DC（網域元件）	OU（組織單位）
DN（識別名稱）	O（組織）

- **值**通常為全限定主機名稱的一部分（例如 sales.companyxyz.com 中的 companyxyz）。

如需指定 LDAP 中指定的節點，則應使用以逗號分隔的清單。如需指定要搜尋的多個節點，則應在完全路徑之間使用與 (&) 字元。

例如，如果 companyxyz 內指定電腦的主機名稱為 computer27.sales.companyxyz.com，則 LDAP 路徑可能是：

```
DC=computer27,DC=sales,DC=companyxyz,DC=com
```

提示：如需查看各種目錄類型的範例，請按一下**搜尋始於目錄節點**欄位旁的**問號**圖示

3 以標準的 LDAP 篩選條件語法在**篩選條件**欄位中輸入 LDAP 篩選條件。

必須指示反垃圾郵件查找並識別使用者和郵件清單的方法。透過在**篩選條件**欄位中特別說明物件類別和郵件屬性，LDAP 查詢中將不包括非主要電子郵件帳戶（如印表機和電腦）。著重在主要使用者帳戶可加快查詢速度。

篩選條件欄位包含語法範例：

```
(&(|(objectClass=group)(objectClass=person)(objectClass=publicFolder))
(mail=*))
```

所有 LDAP 篩選條件都組成群組在括弧中，篩選條件本身用一對括弧圍住整個字串。從左邊開始的下一個字元是與 (&)。LDAP 篩選條件語法採用首碼表示法，這表示此篩選條件只返回三個子篩選條件（分別組成群組在括弧中）的邏輯「AND」。其他運算子包括表示 OR 的豎線 (|) 和表示 NOT 的感嘆號 (!)。

提示：如需查看各種目錄類型的範例，請按一下**篩選條件**欄位旁的**問號**圖示

4 在**使用者登入名稱屬性**欄位中指定使用者用作登入名稱的文字屬性。此欄位的公認屬性是 **sAMAccountName**，這是預設值。此屬性應該適用於 Microsoft Windows 及所有其它環境。

重要：此欄位需要接受**篩選條件**欄位且與其協同工作。如果變更 sAMAccountName，則必須同時在**篩選條件**欄位和**使用者登入名稱屬性**欄位中變更。

提示：如需查看各種目錄類型的範例，請按一下**使用者登入名稱屬性**欄位旁的**問號**圖示

5 在**電子郵件別名屬性**欄位中指定將單個使用者與其垃圾儲存區關聯的電子郵件地址、員工 ID、電話號碼或其他別名屬性。

在許多公司，最終使用者有多個電子郵件帳戶對應至一個有效的電子郵件帳戶。例如，JohnS@example.com 和 John.Smith@example.com 可能都是 John Smith 收件箱的有效電子郵件地址。反垃圾郵件的支援方式是允許最終使用者用一個垃圾儲存區將來自其不同電子郵件地址的所有電子郵件組成群組。

此欄位的唯一公認屬性是 **proxyAddresses**。所有其他屬性必須用逗號隔開。例如：

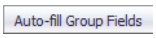
- proxyAddresses、legacyExchangeDN
- proxyAddresses、EmployeeID、PhoneNumber

提示：在 Microsoft Windows 環境中，一個屬性 **proxyAddresses** 通常就足夠了。
如需查看各種目錄類型的範例，請按一下**電子郵件別名屬性**欄位旁的**問號**圖示

6 另外，也可測試您的設定是否起作用，按一下 **LDAP 使用者的查詢資訊**部分下的**測試使用者查詢**  按鈕。

7 儲存變更的方法是按一下 **LDAP 使用者的查詢資訊**部分下的**儲存變更**。

8 移至 **LDAP 群組的查詢資訊**部分。

> **提示：**如果未在**設定**部分中指定**儲存設定時自動填入「LDAP 查詢」欄位**，可按一下**自動填入群組欄位**  按鈕執行此操作。

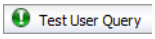
9 如需使用可選的「群組」功能，請在**搜尋始於目錄節點**欄位中，指定完整的 LDAP 目錄路徑，它指向一個包含此目錄中所有群組資訊的節點（LDAP 內的目錄）。這會將對 LDAP 群組的搜尋縮至合理的範圍。如需此設定的更多資訊，請參閱 步驟 2。

10 如需指示反垃圾郵件查找並識別使用者和郵件清單的方法，請以標準的 LDAP 篩選條件語法在**篩選條件**欄位中輸入 LDAP 篩選條件。此欄位包含語法範例。如需此設定的更多資訊，請參閱 步驟 3。

11 在**群組名稱屬性**欄位中指定與群組名稱對應的群組屬性

12 指定群組的常見方式是郵件清單。在 LDAP 的郵件清單項目中，有一個用於指定清單成員的指定欄位。在**群組成員屬性**欄位中輸入此資訊。

13 在某些 LDAP 設定中，每個使用者在 LDAP 的項目內都有一個屬性用於列出此使用者所屬的群組或郵件清單。在**使用者成員資格屬性**欄位中指定此屬性。

14 另外，也可測試您的設定是否起作用，按一下 **LDAP 群組的查詢資訊**部分下的**測試使用者查詢**  按鈕。

15 儲存變更的方法是按一下 **LDAP 群組的查詢資訊**部分下的**儲存變更**。

新增 LDAP 對應

如果使用 Microsoft Windows 環境，則需要在**新增 LDAP 對應**面板中指定 NetBIOS 網域名稱。

> **附註：**NetBIOS 網域名稱有時稱為 Windows 2000 以前的網域名稱。

新增 LDAP 對應的步驟如下：

1 確定您的網域名稱。

   a 登入到網域控制器。

   b 導覽到**開始 > 所有程式 > 系統管理工具 > Active Directory 網域和信任**。

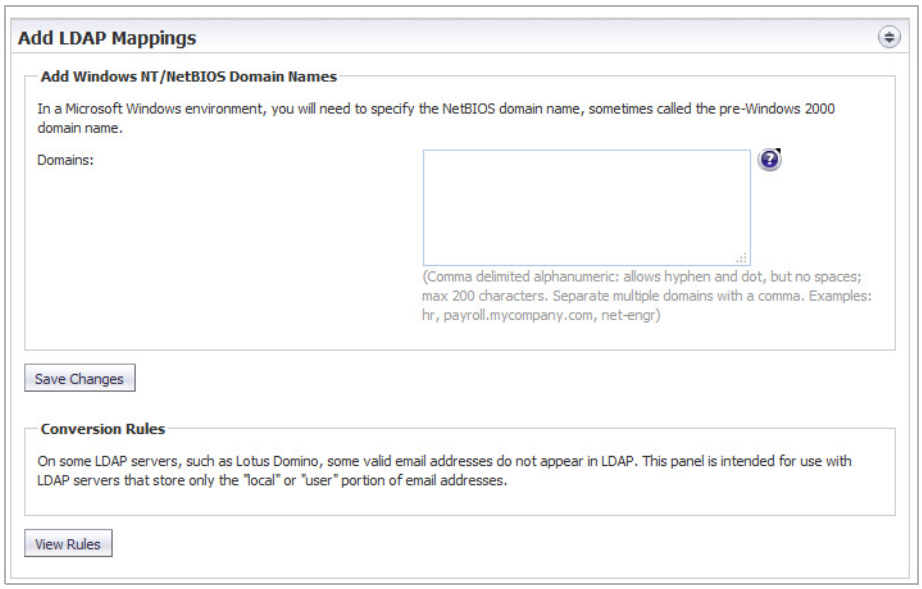
   c 在 **Active Directory 網域和信任**對話方塊中高亮顯示您的網域。

   d 按一下**操作**。

   e 按一下**屬性**。網域名稱出現在**一般**檢視上此網域的**屬性**對話方塊中。

   f 記錄網域名稱。

2 導覽**反垃圾郵件 > LDAP 設定**的**新增 LDAP 對應**面板。



3 將 NetBIOS 網域名稱新增至**網域**欄位。最多新增 200 個字元。用逗號分隔多個網域。允許使用連字元 (-) 和句點 (.)。

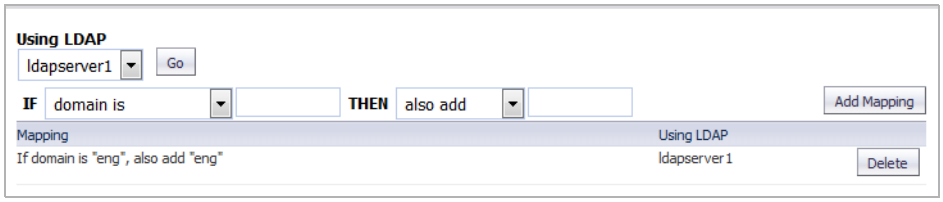
4 按一下**儲存變更**。

5 在某些 LDAP 伺服器（例如 Lotus Domino）中，一些有效的電子郵件地址不會顯示在 LDAP 中。**轉換規則**部分改變了 SonicWall 電子郵件安全裝置解釋某些電子郵件地址的方式，提供一種方法來將電子郵件地址對應到 LDAP 伺服器。

如果您：

- 有上述任一伺服器，請移至步驟 6。
- 沒有上述任一伺服器，並已完成設定 LDAP。

6 如需對應這些位址，請按一下**檢視規則** View Rules 按鈕。顯示 **LDAP 對應**對話方塊。



7 從下拉功能表中選擇所用的 LDAP 伺服器。

8 按一下**執行**。

9 另外，也可新增對應：

a 從 **IF/THEN** 下拉功能表和欄位中，選擇：

- **網域是** - 新增網域之間的其他對應；在此欄位中，指定要對應的網域
  - **替換為** - 用指定的網域替換此網域

    範例：**如果網域是** `engr.corp.com` **替換為** `corp.com`，則傳送位址為 `anybody@engr.corp.com` 的電子郵件將傳送至 `anybody@corp.com`
  - **也新增** - 將第二個網域新增到有效網域清單

範例：**如果網域是** corp.com **也新增** engr.corp.com，則當 corp.com 出現在有效 LDAP 網域清單中時，engr.corp.com 將新增至此清單

- **左側字元是** - 新增字元替換對應；在此欄位中，指定要替換的字元
  - **替換為**-將電子郵件地址中指定到 at 符號 (@) 左側的所有字元替換為新字元

    範例：**如果左側字元是** _ **替換為** -，則傳送位址為 Jane_Doe@corp.com 的電子郵件將傳送至 Jane-Doe@corp.com
  - **也新增** - 將第二個電子郵件地址新增到有效電子郵件地址清單

    範例：**如果左側字元是** _ **也新增** -，則傳送位址為 Jane_Doe@corp.com 或 Jane-Doe@corp.com 的電子郵件地址是有效的電子郵件地址

b 按一下**新增對應** Add Mapping 按鈕完成轉換規則的新增。

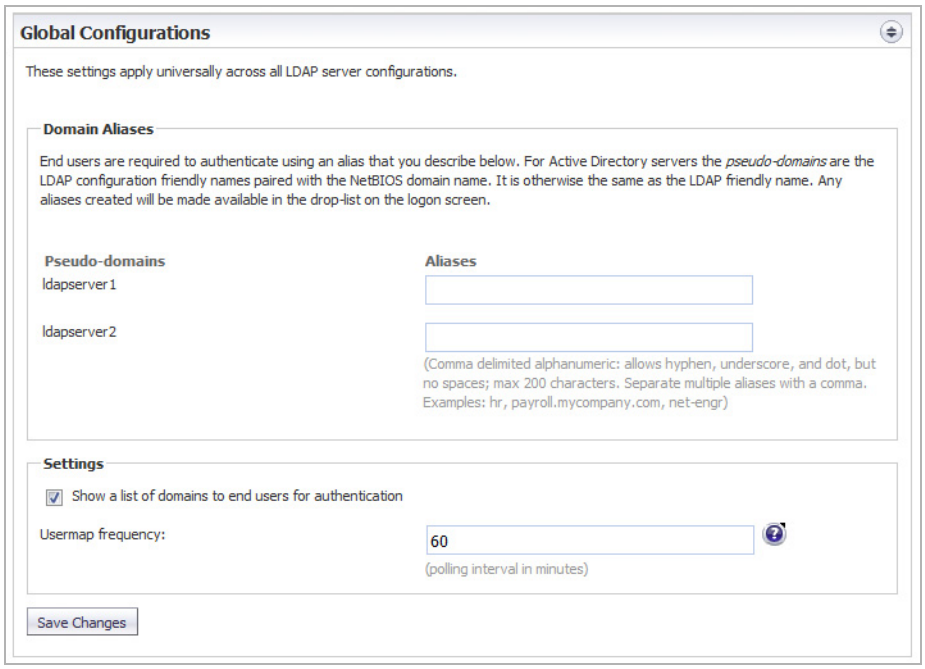
附註：如需刪除對應，請按一下此對應的**刪除**按鈕。

設定全域 LDAP 設定

全域 LDAP 設定通用於所有 LDAP 伺服器設定。

設定全域設定的步驟如下：

1 導覽**反垃圾郵件 > LDAP 設定**中的**全域設定**面板。



2 在**網域別名**部分中，輸入一個或多個伺服器的一個或多個別名，每台伺服器最多可輸入 200 個字元。用逗號分隔多個別名。允許使用連字元 (-)、底線 (_)，但不包含空白字元。

最終使用者必須使用此處設定的別名進行身分驗證。對於 Active Directory 伺服器，假網域是與 NetBIOS 網域名稱配對的 LDAP 易記的名稱。如果在**設定**部分中選擇了此選項，則任何別名都可在登入頁面的下拉功能表中進行身分驗證。

3 如需允許最終使用者在登入時查看網域和別名清單，請在**設定**部分中，選擇**向最終使用者顯示網域清單以進行身分驗證**。預設情況下已選擇此設定。

4 在**使用者地圖頻率**欄位中指定系統中使用者清單重新整理之間的分鐘數。

此設定套用於別名清單和群組成員清單。大多數情況下，增加此設定只會減少 LDAP 伺服器上的負載。根據您的其他設定，每 24 小時（1440 分鐘）獲取一次使用者清單是可以接受的，這樣可以減少 LDAP 伺服器的負載。

附註：使用者地圖頻率不會影響使用者的登入，因為它只是 LDAP 目錄的即時反射。

5 按一下**儲存變更**。

編輯 LDAP 伺服器設定

編輯 LDAP 伺服器設定需要與編輯伺服器相同的設定。

設定 LDAP 伺服器的步驟如下：

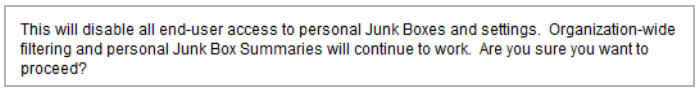
1 從可用 LDAP 伺服器清單中，按一下**編輯**圖示 。這些部分將展開以供編輯：

- **伺服器設定** - 參閱新增 LDAP 伺服器
- **LDAP 查詢面板** - 參閱 設定 LDAP 查詢
- **新增 LDAP 對應** - 參閱新增 LDAP 對應

刪除 LDAP 伺服器

刪除 LDAP 伺服器的步驟如下：

1 對於要刪除的伺服器，按一下刪除圖示。將顯示警告訊息：



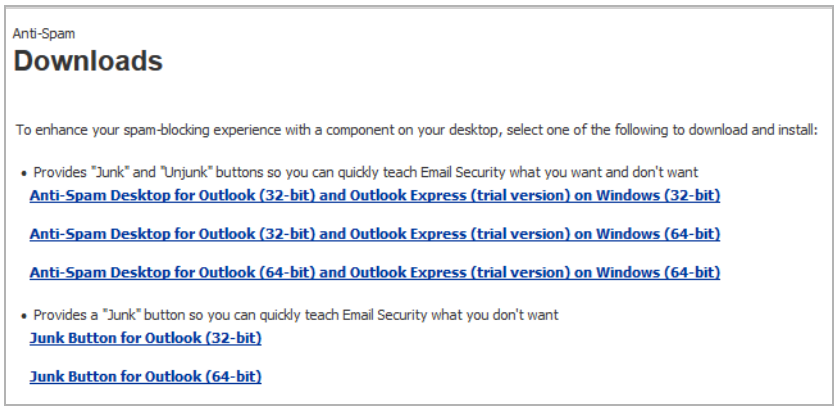
2 按一下**確定**。**反垃圾郵件 > LDAP 設定**頁面頂部隨即顯示一則成功訊息。

33

下載反垃圾郵件桌面按鈕

附註：反垃圾郵件 > 下載不適用於 SuperMassive 9800。

在**反垃圾郵件 > 下載反垃圾郵件工具**頁面上，您可以將 SonicWall 的最新垃圾郵件封鎖按鈕之一下載並安裝到桌面上。



透過按一下一個連結，你可以將這些按鈕下載到你的桌面：

- 「垃圾郵件」和「非垃圾郵件」按鈕，使 Email Security 迅速瞭解您需要什麼郵件、不需要什麼郵件。從以下版本中選擇一個：
  - **用於 Windows（32 位元）Outlook（32 位元）和 Outlook Express（試用版）的 Anti-Spam Desktop**
  - **用於 Windows（32 位元）Outlook（64 位元）和 Outlook Express（試用版）的 Anti-Spam Desktop**
  - **用於 Windows（64 位元）Outlook（64 位元）和 Outlook Express（試用版）的 Anti-Spam Desktop**
- 「垃圾郵件」按鈕，使 Email Security 迅速瞭解您的需求。從以下版本中選擇一個：
  - **用於 Outlook（32 位元）的「垃圾郵件」按鈕**
  - **用於 Outlook（64 位元）的「垃圾郵件」按鈕**

34

關於 DPI-SSL

主題：

附註：DPI-SSL 是一種需要單獨授權的功能，可提供對加密 HTTPS 流量或其他基於 SSL 的 IPv4 和 IPv6 流量的偵測。

- 功能
- 部署方案
- 自訂 DPI-SSL
- 每個裝置型號的連接

功能

主題：

- 支援的功能
- 安全服務

支援的功能

安全套接字層的深度封包偵測 (DPI-SSL) 擴充了 SonicWall 的深度封包偵測技術，可用於偵測加密的 HTTPS 流量和其他基於 SSL 的流量。SSL 流量經過透明解密（攔截），掃描威脅後，如果未發現任何威脅或漏洞，將重新進行加密，然後傳送至目的地。

DPI-SSL 提供了額外的安全防護、應用程式控制和資料防洩漏功能，可分析加密的 HTTPS 和其他基於 SSL 的流量。DPI-SSL 支援：

- 傳送層安全性 (TLS) 交握通訊協定 1.2 及更低版本 - 在 DPI-SSL 部署中進行防火牆與伺服器之間的 SSL 檢查/解密的過程中，支援 TLS 1.2 通訊協定。SonicOS 同樣已在其他領域支援 TLS 1.2。
- SHA-256 - 所有重簽章的伺服器憑證將使用 SHA-256 雜湊演算法進行簽章。
- 完美轉送保密 (PFS) - 基於完美轉送保密的密碼及其他更高強度的密碼將透過宣告的密碼套件中的弱密碼排定優先順序。因此，除非用戶端或伺服器不支援強密碼，否則其不會交涉弱密碼。

DPI-SSL 還支援透過 SSL 通道的應用程式層級頻寬管理。如果對應用程式啟用了 DPI-SSL，應用程式規則 HTTP 頻寬管理原則還將套用到透過 HTTPS 存取的內容。

安全服務

以下安全服務和功能可使用 DPI-SSL：

- 閘道防毒

- 閘道防間諜軟體
- 入侵保護
- 內容篩選
- 應用程式防火牆

部署方案

DPI-SSL 具有兩個主要的部署情節：

- **用戶端 DPI-SSL**：用於當裝置的 LAN 上的用戶端存取 WAN 上的內容時檢查 HTTPS 流量。可根據一般名稱或類別執行對 DPI-SSL 的排除。
- **伺服器 DPI-SSL**：用於當連接 WAN 的遠端用戶端存取位於裝置的 LAN 中的內容時檢查 HTTPS 流量。

代理部署

DPI-SSL 支援代理部署，代理部署中的所有用戶端瀏覽器都會設定為重新導向至代理伺服器，但不包括位於用戶端瀏覽器和代理伺服器之間的裝置。如果網域是虛擬主機伺服器的一部分，或在某些雲端部署，則此方案支援所有 DPI-SSL 功能，包括網域排除，其中同一伺服器 IP 還可供多個網域使用。

此外，典型資料中心伺服器場還帶有負載平衡器和/或反向 SSL 代理，可分載對伺服器的 SSL 處理。對於面向伺服器和執行解密的負載平衡器，此裝置通常僅查看負載平衡器 IP，負載平衡器隨後解密此內容，並確定要將此連接指派的具體伺服器。DPI-SSL 目前已包含全域原則選項，可停用基於 IP 的排除快取。即使基於 IP 的排除快取已關閉，也將繼續執行排除工作。

自訂 DPI-SSL

重要：將 NetExtender SSL VPN 閘道新增至基於 IP 的 DPI SSL 排除清單。由於 NetExtender 流量經 PPP 封裝，因此使 SSL VPN 解密此流量不會帶來有意義的結果。

一般而言，DPI-SSL 原則旨在確保透過此裝置的任何及所有流量的安全。這可能或可能不會符合您的安全需求，因此 DPI-SSL 用於對處理的內容進行自訂。

DPI-SSL 附帶一份從 DPI 處理排除的內建（預設）網域清單（資料庫）。您可以隨時新增至此清單、移除已新增的任何項目，並/或切換從 DPI 處理中排除與包含在 DPI 處理中之間的內建項目。DPI-SSL 還用於按照一般名稱或類別（例如銀行或醫療保健）排除或包含網域。

但是，無論按一般名稱還是類別排除的排除站台，都會構成安全風險，開發套件可能會繞過此應用程式並下載至用戶端電腦，或中間人劫持程式可能會為毫無警惕的用戶端提供偽造伺服器/憑證，從而在將來利用此漏洞。如需規避此類風險，DPI-SSL 可在執行排除前先對排除站台進行身分驗證。

隨著您網路中 HTTPS 連接百分比的增加及新 https 站台的出現，即便是最新的 SonicOS 版本，也不太可能包含完整的內建/預設排除清單。當因固有實現新用戶端應用程式或伺服器實現而發生 DPI-SSL 攔截時，部分 HTTPS 連接失敗且可能需要排除此裝置中的這些站台以提供無縫使用者體驗。SonicOS 將記錄您能夠排除和使用的上述故障連接，以將受信任項目新增至排除清單。

除了排除/包含站台外，DPI-SSL 還可為全域連接同時提供全域驗證原則和精確異常原則。例如，使用全域原則驗證連接，可能會封鎖受信任的新 CA 憑證或私人(或本機企業部署)安全雲端解決方案的自我簽署伺服器憑證等本質安全的部分連接。此精確選項用於從全域驗證原則中排除個別的網域。

您可以設定對某個網域的排除，此網域位於同一伺服器（憑證）所支援的所有網域的清單中。即，部分伺服器憑證包含多個網域名稱，但您希望僅排除其中一個網域，而無需排除單個伺服器憑證提供的所有網域。例如，您可以排除 youtube.com 而無需排除 google.com 等任何其他網域，即使 *.google.com 是已作為「主體替代名稱」延伸下的替代網域列出 youtube.com 的伺服器憑證的一般名稱。

每個裝置型號的連接

用戶端 DPI-SSL 支援的每個平台的最大併發連接數表格顯示每個平台和裝置可在其中執行用戶端 DPI-SSL 檢查的最大併發連接數。

用戶端 DPI-SSL 支援的每個平台的最大併發連接數

硬體模型	最大併發 DPI-SSL 連接數	硬體模型	最大併發 DPI-SSL 連接數	硬體模型	最大併發 DPI-SSL 連接數
SM 9800	48,000	NSA 6600	6,000	TZ600	750
SM 9600	12,000	NSA 5600	4,000	TZ500	750
SM 9400	10,000	NSA 4600	3,000	TZ500W	750
SM 9200	8,000	NSA 3600	2,000	TZ400	500
		NSA 2600	1,000	TZ400W	500
				TZ300	500
		SOHO W	100	TZ300W	500

附註：對於設定了 250,000 DPI 設定和動態調整連線大小的 SuperMassive 9200、6400 和 9600 以及 NSA 系列等，防火牆可以動態增加 DPI-SSL 連線。如需詳細資料，請參閱動態調整連接大小。

35

設定用戶端 DPI-SSL 設定

主題：

- 檢視 DPI-SSL 狀態
- 設定用戶端 DPI-SSL

檢視 DPI-SSL 狀態

DPI-SSL 狀態部分顯示目前的 DPI-SSL 連接數、峰值連接數及最大連接數。

設定用戶端 DPI-SSL

用戶端 DPI-SSL 部署情節通常用於當 LAN 上的用戶端瀏覽 WAN 上的內容時檢查 HTTPS 流量。在此情節中，對於所有檢查的內容防火牆通常沒有憑證和私鑰。執行 DPI-SSL 檢查後，將重寫遠端伺服器傳送的憑證，並使用在用戶端 DPI-SSL 設定中指定的憑證簽署此新產生的憑證。預設情況下，這是防火牆憑證授權單位 (CA) 憑證，但也可以是其他可指定的憑證。應指示使用者將憑證新增到其瀏覽器中的信任清單中，以避免憑證信任錯誤。

主題：

- 設定一般設定
- 選擇重新簽署憑證授權
- 設定排除和包含
- 用戶端 DPI-SSL 範例

設定一般設定

啟用用戶端 DPI-SSL 檢查的步驟如下：

1 導覽至**安全設定 | 加密服務 > DPI-SSL/TLS 用戶端**頁面上的**一般**檢視。

2 勾選**啟用 SSL 用戶端檢查**核取方塊。預設情況下，此核取方塊未啟用。

3 選擇以下要用於執行檢查的一個或多個服務；無預設勾選：

- 入侵預防
- 閘道防毒

- **閘道防間諜軟體**
- **應用程式防火牆**
- **內容篩選**

4 如需驗證解密 / 攔截連接的伺服器，請選擇**永遠驗證已解密之連線的伺服器**核取方塊。啟用後，DPI-SSL 將封鎖以下連接：

- 未信任憑證的網址連接。
- 無法根據此連接的伺服器憑證驗證用戶端問候中的網域名稱時。

預設情況下，此核取方塊未啟用。

重要：如果需要進階層級安全性，則僅啟用此選項。如顯示連接故障所述，連接失敗清單中將顯示封鎖的連接。

提示：如果啟用此選項，則使用**略過 CFS 類別為主的排除項目**選項（參閱排除/包含一般名稱）以從此全域驗證選項中排除指定的網域。這有利於覆寫受信任站台的所有伺服器驗證相關的錯誤。

5 如需停用排除的基於伺服器 IP 位址的動態快取，請選擇**部署之中的防火牆發現用於不同伺服器網域的單一伺服器 IP，例如： Proxy 設定**核取方塊。預設情況下，此核取方塊未啟用。

此選項用於代理部署，代理部署中的所有用戶端瀏覽器都會重新導向至代理伺服器，包括位於用戶端瀏覽器和代理伺服器之間的裝置。所有 DPI-SSL 功能均支援，包括網域為虛擬主機伺服器一部分時的網域排除，而伺服器陣列的一部分面對負載平衡器，或在部分雲端部署中，則多個網域可以使用相同的伺服器 IP。

在此部署中，此裝置所監測到的所有伺服器 IP 都是代理伺服器 IP。因此，在代理部署中，必須停用基於 IP 的排除快取。啟用此選項不會影響 SonicOS 執行排除的功能。

6 預設情況下，將繞過透過 DPI-SSL 連接限制的連接。如需在超出連接限制時允許新連接繞過解密，而不是斷開，則選擇**當超出連線限制時允許無解密的 SSL (旁路)**核取方塊。預設情況下已核取此選項。

如需確保斷開透過 DPI-SSL 連接限制的新連接，則取消選擇/停用此核取方塊。

7 如需在新增排除項之前稽核新的內建排除網域名稱，則選擇**在加入至排除項目之前稽核新的內建排除網域名稱**核取方塊。預設情況下，此核取方塊未啟用。

如果啟用此選項，只要內建排除清單發生改變（例如，升級至新的韌體影像或其他系統相關操作），則將透過 **加密服務 > DPI-SSL/TLS 用戶端**頁面 顯示此變更的通知快顯對話方塊。您可以檢查/稽核新變更，並接受或拒絕對內建排除清單所做的任何、部分或所有新變更。此時，將更新執行時排除清單以反映新的變更。

如果停用此選項，SonicOS 將接受對內建排除清單所做的所有新變更且自動新增這些新變更。

8 如需始終在套用一般名稱或類別排除原則前驗證伺服器，則選擇**在套用排除原則之前永遠驗證伺服器**核取方塊。啟用後，DPI-SSL 將封鎖以下排除連接：

- 未信任憑證的網址連接。
- 無法根據此連接的伺服器憑證驗證用戶端問候中的網域名稱時。

這是在套用排除原則前驗證伺服器連接的有用功能。啟用此選項可確保裝置不會盲目對連接套用排除原則，進而產生針對排除站台或屬於排除類別的站台的安全漏洞。這在排除銀行站台類別時尤為重要。

透過在套用排除原則前同時驗證伺服器憑證和用戶端問候中的網域名稱，SonicOS 可拒絕不受信任站台，並封鎖發生潛在的零天攻擊類型。SonicOS 實作採取「信任但驗證」的方法確保首先驗

證與排除原則條件相符合的網域名稱，進而避免毫無警惕的用戶端受到網路釣魚或與 URL 重新導向相關的攻擊。

預設情況下，此核取方塊未啟用。

重要：如果您要排除主體替代名稱延伸中的替代網域，推薦您啟用此選項。

提示：如果啟用此選項，則使用**略過 CFS 類別為主的排除項目**選項（參閱排除/包含一般名稱）以從此全域驗證選項中排除指定的網域。這有利於覆寫受信任站台的所有伺服器驗證相關的錯誤。

9 按一下**接受**。

選擇重新簽署憑證授權

僅當防火牆信任授權憑證時，重新簽署憑證將替換原來的憑證簽署授權。如果授權不受信任，那麼憑證將自我簽署。為了避免憑證錯誤，請選擇受 DPI-SSL 防護並受裝置信任的憑證。

附註：如需請求/建立 DPI SSL 憑證授權單位 (CA) 憑證的資訊，請參閱以下「知識庫」文章：*How to request/create DPI-SSL Certificate Authority (CA) certificates for the purpose of DPI-SSL certificate resigning* (SW14090)。

選擇重新簽署憑證的步驟如下

1 導覽至**安全設定 | 加密服務 > DPI-SSL/TLS 用戶端**頁面。

2 按一下**憑證**。

3 從**憑證**下拉功能表中選擇要使用的憑證。預設情況下使用**預設 SonicWall DPI-SSL CA 憑證**重新簽署檢查的流量。

附註：如果憑證未列出，可以從**系統安裝 | 設備 > 憑證**頁面匯入。請參閱 *SonicWall SonicOS 6.5 系統安裝*。

如需 PKCS-12 格式的憑證，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

4 若要將所選的憑證下載至防火牆，按一下（**下載**）連結。此時顯示**打開*檔案名稱***對話方塊。

提示：若要檢視可用的憑證，按一下（**管理憑證**）連結以顯示**系統 > 憑證**頁面。

a 請確保已核取**儲存檔案**選項按鈕。

b 按一下**確定**。

此檔案已下載。

5 按一下**接受**。

新增信任到瀏覽器

為實現重新簽署憑證授權，以成功執行重新簽署憑證，瀏覽器需要信任此憑證授權。透過將重新簽署憑證匯入到瀏覽器的受信 CA 清單中，可建立此信任。請按照瀏覽器的說明匯入重新簽署憑證。

設定排除和包含

預設情況下，DPI-SSL 啟用後會套用到裝置上的所有流量。您可以自訂哪些流量將套用 DPI-SSL 檢查：

- **排除/包含**清單將排除/包含指定的物件和組
- **一般名稱**將排除指定的主機名稱
- **CFS 類別為主的排除/包含**排除或包含基於 CFS 類別的指定類別

此自訂支援單個排除/包含某個網域的替代名稱，此網域位於同一伺服器（憑證）所支援的所有網域的清單中。在處理大量流量的部署中，可用於排除受信任的來源，以減少 DPI-SSL 對 CPU 的影響，並防止裝置達到併發 DPI-SSL 檢查的最大連接數。

附註：在使用 Google Drive、Apple iTunes 或任何其他有鎖定憑證的應用程式時，如果在防火牆中啟用了 DPI-SSL，則此應用程式可能會無法連接至伺服器。如需允許應用程式連接至伺服器，則應從 DPI-SSL 中排除關聯的網域；例如，如需允許 Google Drive 執行，則應排除：

- `.google.com`
- `.googleapis.com`
- `.gstatic.com`

由於 Google 在其所有應用中都使用一個憑證，因此排除這些網域可使 Google 應用程式繞過 DPI-SSL。或者，從 DPI-SSL 排除用戶端機器。

主題：

- 排除/包含物件/組
- 按一般名稱排除/包含

- 指定基於 CFS 類別的排除/包含
- 內容篩選
- 應用程式規則

排除/包含物件/組

若要自訂 DPI-SSL 用戶端檢查：

1 按一下**加密服務 > DPI-SSL/TLS 用戶端**頁面上的**物件**。

2 從**位址物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSL 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

> **提示：包含**下拉功能表可用於微調指定的排除清單。例如，透過從**排除**下拉功能表中選擇**遠端辦公室-加利福尼亞**位址物件，並從**包含**下拉功能表中選擇**遠端辦公室-奧克蘭**位址物件。

3 從**服務物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSL 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

4 從**使用者物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSL 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

5 按一下**接受**。

按一般名稱排除/包含

可以將信任網域名稱新增至排除清單。將信任網域新增至內建排除資料庫，可減少 DPI-SSL 對 CPU 影響，並可避免裝置達到 DPI-SSL 檢查的最大併發連接數。

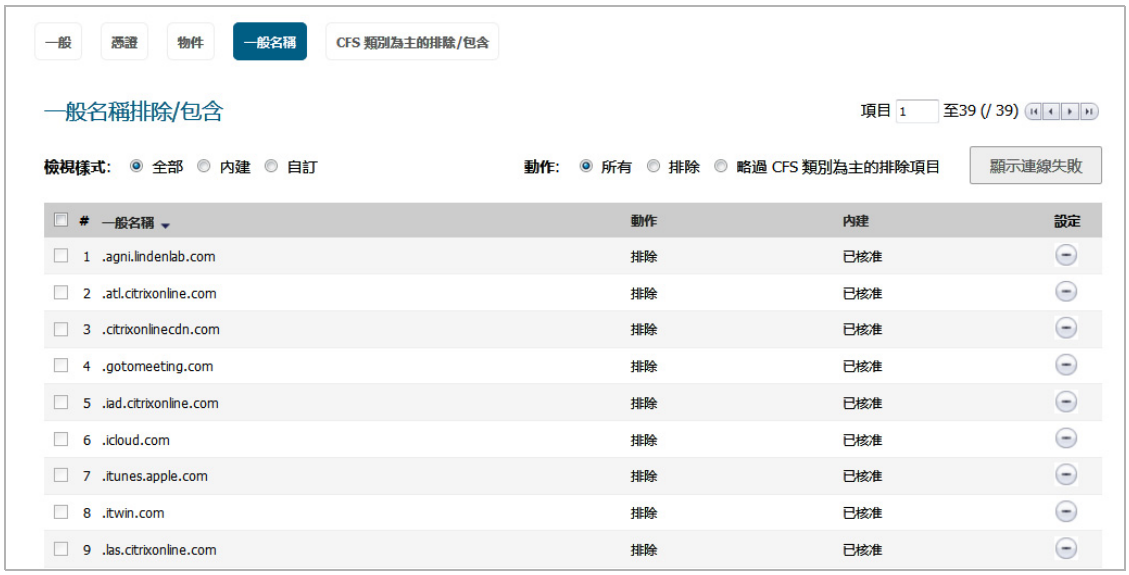
主題：

- 排除/包含一般名稱
- 刪除自訂一般名稱
- 顯示連接故障

排除/包含一般名稱

若要按一般名稱排除/包含項目：

1 按一下**一般名稱**。



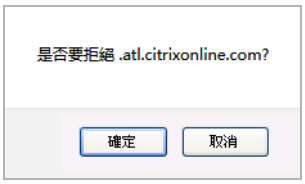
2 選擇下列選項可控制一般名稱的顯示：

- **檢視樣式**選項：
  - **所有**（預設）- 顯示所有一般名稱。
  - **內建** - 僅顯示非自訂一般名稱。
  - **自訂** - 僅顯示您新增的一般名稱。
- **操作**選項：
  - **所有**（預設）- 同時顯示排除的覆寫和 CFS 類別排除覆寫。
  - **排除** - 僅顯示排除的一般名稱。
  - **略過 CFS 類別為主的排除項目** - 僅顯示已選擇「覆寫基於 CFS 類別的排除」選項的自訂一般名稱。

附註：使用**略過 CFS 類別為主的排除項目**選項從全域包含選項，**永遠驗證已解密之連線的伺服器**和**在套用排除原則之前永遠驗證伺服器**中排除指定網域。

3 預設情況下，所有內建一般名稱均經過核准。您可以透過以下步驟拒絕內建一般名稱的核准：

a 按一下一般名稱**設定**欄中的**拒絕** ⊖ 圖示。將顯示確認訊息。



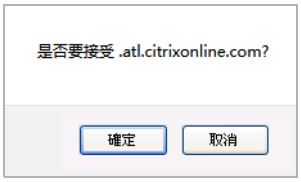
b 按一下**確定**。

拒絕圖示變為**接受** ⊕ 圖示且**內建**欄中的**核准**圖示變為**拒絕**。

附註：內建一般名稱無法修改或刪除，但可拒絕或接受。

接受拒絕的內建一般名稱的步驟如下：

a 按一下其**接受**圖示。將顯示確認訊息。



b 按一下**確定**。

4 如需新增自訂一般名稱，請按一下**一般名稱排除 / 包含**表下的**新增**按鈕。隨即顯示**新增一般名稱**對話方塊。

a 在此欄位中新增一個或多個一般名稱。用逗號或新行字元分隔多個項目。

b 指定**操作**類型：

- **排除**（預設）
- **覆寫 CFS 類別為主的排除項目**
- **略過驗證伺服器**如果驗證伺服器導致連線封鎖，則退出此網域的伺服器驗證。只有在伺服器是信任的網域時啟用此選項。

c DPI-SSL 會根據原則或設定動態決定連線是否應攔截 (包含) 或排除。當 DPI-SSL 獲取連線的網域名稱後，排除資訊即可供後續與相同伺服器/網域的連線使用。

如需停用動態排除快取（基於伺服器 IP 和一般名稱），請選擇**在套用排除原則之前永遠驗證伺服器**核取方塊。預設情況下未勾選此選項。

d 按一下**接受**。

一般名稱排除/包含表將更新且**自訂**出現在**內建**欄中。如果已選擇**在套用排除原則之前永遠驗證伺服器**選項，則**內建**欄中的**自訂**旁將顯示**資訊**圖示。

將滑鼠放在**資訊**圖示，查看選擇了哪些自訂屬性。如果透過**連線失敗清單**新增了一般名稱，則資訊圖示將指示失敗類型：

- **略過 CFS 類別排除**
- **略過伺服器驗證**
- **無法驗證伺服器**
- **用戶端交握失敗**
- **伺服器交握失敗**

如需刪除此項目，則按一下**設定**欄中的**刪除**圖示。

5 可透過指定篩選搜尋一般名稱。

a 在**篩選**欄位中，輸入一個以此語法指定的名稱：*名稱*：*mycommonname*。

b 按一下**篩選**按鈕。

6 按一下**接受**。

刪除自訂一般名稱

若要刪除自訂一般名稱：

1 執行以下任一動作：

- 按一下**設定**欄中自訂一般名稱的**刪除**圖示。
- 在**排除**中選擇此名稱，然後按一下**刪除**按鈕。
- 按一下**全部刪除**核取方塊以刪除所有自訂一般名稱。將顯示確認訊息。按一下**確定**。

2 按一下**接受**。

顯示連接故障

SonicOS 會將近期與 DPI-SSL 用戶端相關的連接故障儲存在清單中。它有如下強大功能：

- 列出 DPI-SSL 故障連接。
- 用於稽核故障連接。
- 提供一種自動排除部分故障網域的機制。

此對話方塊顯示執行時的連接故障。連接故障可能由下列任一原因造成：

- 無法與用戶端交握。
- 無法與伺服器交握。
- 無法驗證用戶端問候中的網域名稱。
- 無法驗證伺服器（伺服器憑證發行者不受信任）。

故障清單僅在執行時可用。每次故障的記錄數量是有限的，以確保單次故障類型不會超出整個緩衝區。

使用連接故障清單的步驟如下：

1 按一下**顯示連線失敗**按鈕。顯示**連線失敗清單**對話方塊。

此清單中的每個項目均顯示：

- **用戶端位址**
- **伺服器位址**
- **一般名稱** - 故障連接網域的一般名稱。您可以先內聯編輯此項目，再將其新增至自動排除清單。
- **錯誤訊息** - 提供與連接相關的上下文資訊，它使您能夠做出排除此連接的適當選擇。

2 新增項目至排除清單的步驟如下：

a 選擇此項目。

b 對此項目進行任何編輯。

c 按一下**排除**按鈕。

3 刪除項目的步驟如下：

a 選擇項目。

b 按一下**清除**按鈕。

4 如需刪除所有項目，按一下**清除所有**按鈕。

5 完成時，按一下**關閉**按鈕。

指定基於 CFS 類別的排除/包含

您可以透過內容篩選類別排除/包含項目。

指定基於 CFS 類別的排除/包含的步驟如下：

1 按一下**CFS 類別為主的排除/包含**。

清單狀態即顯示在檢視上方。

2 按一下**排除**（預設）或**包含**選項按鈕，選擇是否要包含或排除選定類別。預設情況下，未選擇所有類別。

3 選擇要包含/排除的類別。如需選擇所有類別，請按一下**選擇所有類別**核取方塊。

4 也可重複步驟 2 和步驟 3 以建立相反的清單。

5 另外，如需在某個網域的內容篩選類別資訊對 DPI-SSL 無法使用時排除連接，請選擇**如果內容篩選類別不可用時則排除連線**核取方塊。預設情況下未勾選此選項。

大多數情況下，HTTPS 網域的類別資訊可在本機用於防火牆快取。當類別資訊在本機無法使用時，DPI-SSL 將從雲端中獲取類別資訊，而不會封鎖用戶端或伺服器通訊。大多數情況下，類別資訊可供 DPI-SSL 制定決策。預設情況下，應在 DPI-SSL 中檢查這些站台。

6 按一下**接受**。

用戶端 DPI-SSL 範例

主題：

- 內容篩選
- 應用程式規則

內容篩選

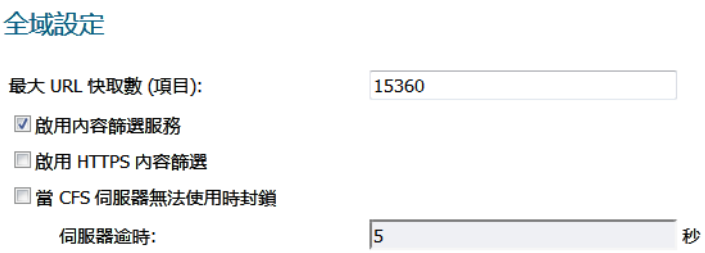
若要使用 DPI-SSL 對基於 HTTPS 和 SSL 的流量執行 SonicWall 內容篩選，請：

1 導覽至**安全設定 | 安全服務 | 內容篩選**頁面的**全域設定**部分。

2 選擇**啟用內容篩選服務**。

3 清除**啟用 HTTPS 內容篩選**核取方塊。

> **附註：**HTTPS 內容篩選基於 IP 和主機名稱。HTTP 內容篩選可執行重新導向以實施身分驗證或提供封鎖頁面，會封鎖 TTPS 篩選頁面，但不會提示。



4 確保從**內容篩選類型**下拉功能表中選擇 **SonicWall CFS**。

5 按一下**接受**。

6 導覽至**加密服務 > DPI-SSL/TLS 用戶端**頁面。

7 按一下**一般**。

8 選擇**啟用 SSL 用戶端檢查**核取方塊。

9 勾選**內容篩選**核取方塊。

10 按一下**接受**。

11 如需設定內容篩選的資訊，請參閱設定內容篩選服務。

12 導覽至使用 HTTPS 通訊協定的封鎖站台，以驗證是否正確封鎖。

附註：對於透過 DPI-SSL 的內容篩選，封鎖第一次 HTTPS 存取會使顯示的頁面為空。如果重新整理了頁面，使用者將看到防火牆封鎖頁面。

應用程式規則

需要在**安全設定 | 加密服務 > DPI-SSL/TLS 用戶端**頁面和**原則 | 規則 > 進階應用程式控制**頁面同時啟用應用程式防火牆規則，才能按這些規則執行篩選。

1 導覽至**安全設定 | 加密服務 > DPI-SSL/TLS 用戶端**頁面。

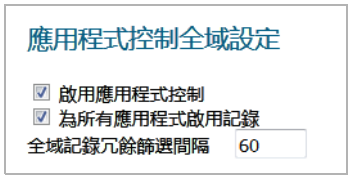
2 按一下**一般**。

3 勾選**啟用 SSL 用戶端檢查**核取方塊。

4 勾選**應用程式防火牆**核取方塊。

5 按一下**接受**。

6 導覽至**原則 | 規則 > 進階應用程式控制**頁面的**應用程式規則狀態全域設定**部分。



7 勾選**啟用應用程式控制**。

8 設定 HTTP 用戶端原則，以**封鎖頁面**作為原則的操作來封鎖 Microsoft Internet Explorer 瀏覽器。如需設定應用程式規則，請參閱 *SonicWall SonicOS 6.5 原則*。

9 按一下**接受**。

10 透過 Internet Explorer 存取使用 HTTPS 通訊協定的任何網站，並驗證是否已將之封鎖。

36

設定伺服器 DPI-SSL 設定

附註：如需 DPI SSL 的資訊，請參見。

當連接 WAN 的遠端用戶端存取位於防火牆的 LAN 中的內容時，伺服器 DPI-SSL 部署情節通常用於檢查 HTTPS 流量。伺服器 DPI-SSL 用於設定符合的位址物件和憑證。裝置偵測到位址物件的 SSL 連接後，將顯示符合的憑證，並與連接的用戶端交涉 SSL。

之後，如果符合的憑證將伺服器定義為「清除文字」，將對原始（發佈 NAT 重新對應）連接埠的伺服器建立標準 TCP 連接。如果未將符合項定義為「清除文字」，將交涉伺服器的 SSL 連接。這將允許端到端的連接加密。

附註：在此部署情節中，防火牆的所有者具有原始內容伺服器的憑證和私人金鑰。您需要將伺服器的原始憑證匯入到防火牆，並建立合適的伺服器 IP 位址，以在伺服器 DPI-SSL UI 中進行伺服器憑證對應。

主題：

- 設定 DPI-SSL 伺服器設定

設定 DPI-SSL 伺服器設定

主題：

- 設定一般伺服器 DPI-SSL 設定

- 設定排除和包含
- 設定伺服器與憑證的符合

設定一般伺服器 DPI-SSL 設定

啟用伺服器 DPI-SSL 檢查的步驟如下：

1 導覽至**安全設定 | 加密服務 > DPI-SSL/TLS 伺服器**頁面的**一般設定**部分。

2 選擇**啟用 SSL 伺服器偵測**核取方塊。

3 選擇將要用來執行檢查的服務：

- **入侵保護**
- **閘道防毒**
- **閘道防間諜**
- **應用程式防火牆**

4 按一下**接受**。

5 向下捲動至 **SSL 伺服器**部分，以設定套用於 DPI-SSL 檢查的一個或多個伺服器。請參閱設定伺服器與憑證的符合。

設定排除和包含

預設情況下，DPI-SSL 會套用到已啟用的裝置上的所有流量。您可以設定包含/排除清單，以自訂哪些流量將套用 DPI-SSL 檢查。**包含/排除**清單提供了用於指定指定物件、或群組的功能。在處理大量流量的部署中，可用於排除受信任的來源，以減少 DPI-SSL 對 CPU 的影響，並防止裝置達到併發 DPI-SSL 檢查的最大連接數。

若要自訂 DPI-SSL 伺服器檢查：

1 導覽至**加密服務 > DPI-SSL/TLS 用戶端**頁面的**包含/排除**部分。

2 從**位址物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSL 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

> **提示：包含**下拉功能表可用於微調指定的排除清單。例如，透過從**排除**下拉功能表中選擇**遠端辦公室-加利福尼亞**位址物件，並從**包含**下拉功能表中選擇**遠端辦公室-奧克蘭**位址物件。

3 從**使用者物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSL 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

4 按一下**接受**。

設定伺服器與憑證的符合

伺服器 DPI-SSL 檢查需要您指定使用哪個憑證對在其流量上執行 DPI-SSL 檢查的每個伺服器簽署流量。

若要設定伺服器與憑證的符合：

1 導覽至**加密服務 > DPI-SSL/TLS 用戶端**頁面的 **SSL 伺服器**部分。

2 按一下**新增**按鈕。將顯示 **SSL 伺服器設定**。

3 在**位址物件/群組**下拉功能表中，對想要套用 DPI-SSL 檢查的一個或多個伺服器選擇位址物件或群組。

4 在 **SSL 憑證**下拉功能表中，選擇用於簽署伺服器流量的憑證。詳細資料：

- 如需將新憑證匯入到裝置的更多資訊，請參見選擇重新簽署憑證授權。
- 如需建立 Linux 憑證的資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

5 選擇**清除文字**核取方塊，以啟用 SSL 卸載。新增伺服器與憑證的符合時，將顯示**清除文字**選項。此選項提供了傳送未加密資料到伺服器的一個方式。預設情況下，未選擇此選項。

> ⓘ **重要：**為使此類設定正常工作，需要在**原則 | 規則 > NAT 原則**頁面上為此伺服器建立 NAT 原則，以將指定用於卸載伺服器的流量從 SSL 連接埠對應到非 SSL 連接埠。必須將流量傳送到除了 443 的連接埠。例如，將 HTTPS 流量用於 SSL 卸載時，需要建立從連接埠 443 到連接埠 80 的輸入 NAT 原則重新對應流量，以能實現正常執行。

6 按下**新增**。

37

設定 DPI-SSH

DPI-SSH 提供加密資訊的深度封包偵測。

附註：閘道防間諜軟體服務對 DPI-SSH 無作用，因為防間諜軟體旳 TCP 串流不受支援。若勾選此核取方塊，系統不採取動作。

主題：

- 關於 DPI-SSH
- 支援的用戶端/伺服器和連線
- 支援的金鑰交換演算法
- 啟用您的 DPI-SSH 授權
- 設定 DPI-SSH

關於 DPI-SSH

深度封包偵測 (DPI) 技術允許封包篩選防火牆根據封包的第 3 層和第 4 層內容簽章將通過的流量分類。DPI 也提供描述封包承載的內容的相關資訊（第 7 層應用程式資料）。DPI 是現有的 SonicOS 功能，它會

檢查通過 SonicWall 防火牆的封包資料和標頭，搜尋通訊協定不相容、病毒、垃圾郵件、入侵或定義的準則，以決定封包是否可通過，或是否需要路由至不同的動作或其他追蹤目的地。

SSH（安全殼層）是密碼編譯的網路通訊協定，用於確保兩部連網電腦之間的安全資料通訊、遠端命令行登入及其他安全網路服務。SSH 會透過安全頻道連接不安全的網路、伺服器和執行 SSH 伺服器的用戶端以及 SSH 用戶端程式。兩種不同版本的通訊協定有區別，分別為 SSH-1 和 SSH-2。SonicWall 僅支援 SSH-2；SSH-1 工作階段未被攔截和檢查。

附註：不可同時使用不同版本號碼的 SSH 用戶端。

若要有效檢查加密的郵件如 SSH，必須先解密承載。DPI-SSH 的作用是中間人攻擊 (MITM) 或封包代理。預設的端對端通訊已中斷，而且預先共用金鑰無法使用。

DPI-SSH 將一個 SSH 通道分成兩個通道，而它會解密來自這兩個通道的封包，並執行檢查。如果封包通過 DPI 檢查，DPI-SSH 會將重新加密的封包傳送至通道。如果封包未通過檢查，它會依照原則路由到另一個目的地，或提交以收集統計資訊，而且 DPI-SSH 會重設連線。

支援的用戶端/伺服器和連線

SSH 不是殼層，而是安全通道，其透過此通道提供不同服務，包括殼層、檔案傳輸或 X11 轉送。

DPI-SSH 支援路由模式和有線模式二者。對於有線模式，只在安全 (內聯流量的主動 DPI) 模式中支援 DPI-SSH。對於路由模式，則無限制。

SSH 支援不同的用戶端和伺服器實作，如支援的用戶端/伺服器表格中所列。

支援的用戶端/伺服器

支援的 DPI-SSH 用戶端	支援的 DPI-SSH 伺服器
Cygwin 的 SSH 用戶端	Fedorz 上的 SSH 伺服器
Putty	Ubuntu 上的 SSH伺服器
secureCRT	
Ubuntu 上的 SSH	
centos 上的 SSH	
Cygwin 上的 SFTP 用戶端	
Cygwin 上的 SCP	
Winscp	

DPI-SSH 支援多達 250 連線。

支援的金鑰交換演算法

DPI-SSH 支援這些金鑰交換演算法：

- Diffie-Hellman-group1-sha1
- Diffie-Hellman-group14-sha1
- ecdh-sha2-nistp256

DPI-SSH 支援用戶端的 DSA 金鑰及伺服器端的 RSA 金鑰。

注意

如果本機機器中已儲存有 SSH 伺服器金鑰，則必須加以刪除。例如，若您已經有到伺服器的 SSH，並且伺服器 DSS 金鑰已儲存，如果未從本機檔案刪除 DSS 金鑰，則 SSH 工作階段將會失敗。

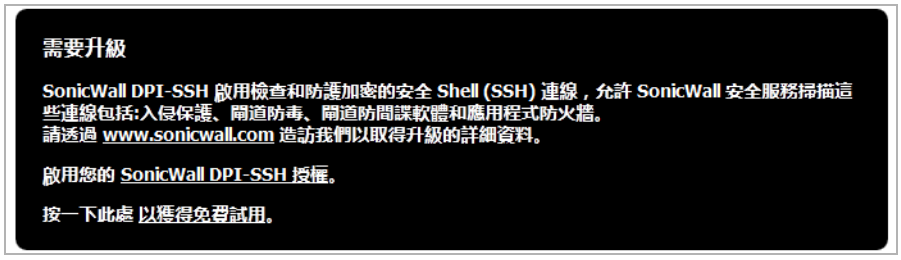
`ssh-keygen` 公用程式不可用來繞過密碼。

Putty 使用 GSSAPI。此選項僅針對 SSH2，其提供較強的加密驗證。對於第一次的通訊，它會將本機 Token 或密碼儲存到本機用戶端和伺服器。它會在 DPI-SSH 啟動前，交換訊息和進行操作，所以 DPI-SSH 對於之前交換些什麼，包括 GSSAPI Token 一無所知。DPI-SSH 將無法啟用 GSSAPI 選項。

在用戶端這一端，若啟用 DPI-SSH，可使用 SSH2.x 或 1.x 用戶端。不過，不可同時使用不同版本號碼的用戶端。

即使在**加密服務 > DPI-SSH**頁面中選取這些選項，也不支援閘道防間諜軟體和應用程式防火牆檢查。

啟用您的 DPI-SSH 授權

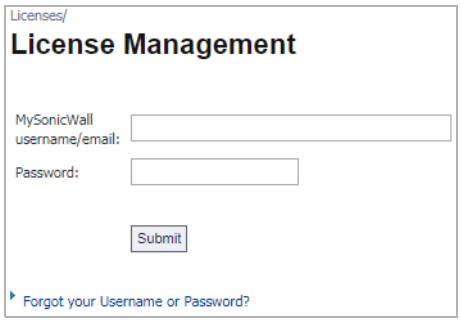


DPI-SSH 預設為完全授權，但您需要啟用您的授權。當您先選取**加密服務 > DPI-SSH**時，您會收到訊息：需要升級。

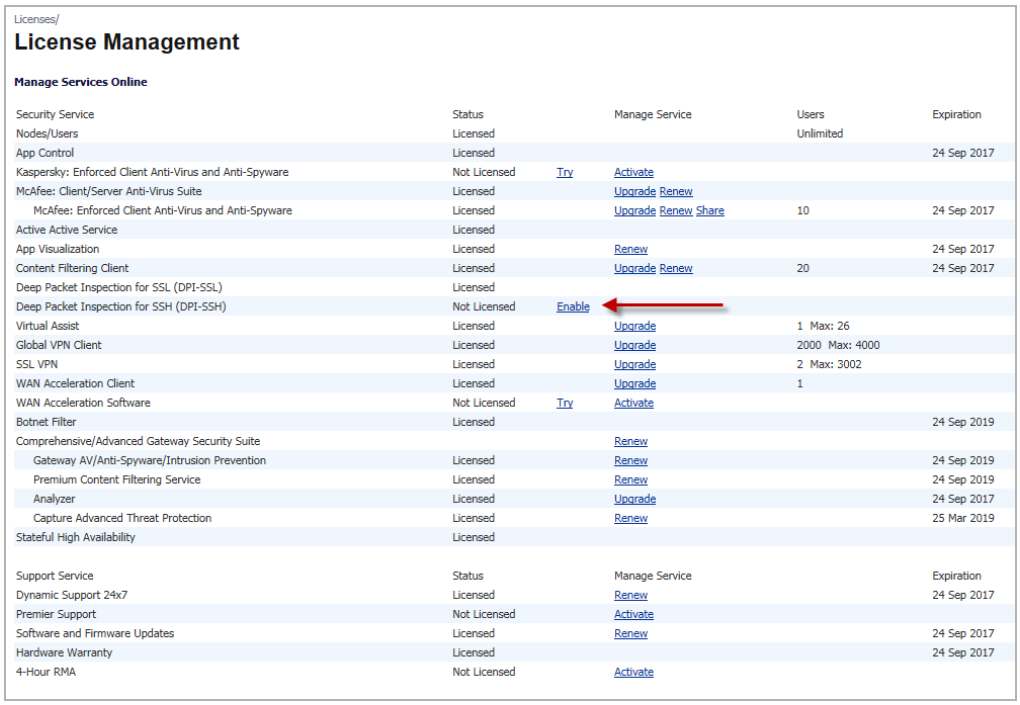
如果不需要升級，請跳至設定 DPI-SSH。

若要啟用您的授權：

1 按一下連結以**啟用您的 SonicWall DPH SSH 授權**。顯示**授權 > 授權管理**頁面。



2 使用您的認證登入 MySonicWall。**授權 > 授權管理**頁面顯示所有的服務，並且指出哪些已獲得授權。



Licenses/

License Management

Manage Services Online

Security Service	Status		Manage Service	Users	Expiration
Nodes/Users	Licensed			Unlimited	
App Control	Licensed				24 Sep 2017
Kaspersky: Enforced Client Anti-Virus and Anti-Spyware	Not Licensed	Try	Activate		
McAfee: Client/Server Anti-Virus Suite	Licensed		Upgrade Renew		
McAfee: Enforced Client Anti-Virus and Anti-Spyware	Licensed		Upgrade Renew Share	10	24 Sep 2017
Active Active Service	Licensed				
App Visualization	Licensed		Renew		24 Sep 2017
Content Filtering Client	Licensed		Upgrade Renew	20	24 Sep 2017
Deep Packet Inspection for SSL (DPI-SSL)	Licensed				
Deep Packet Inspection for SSH (DPI-SSH)	Not Licensed	Enable			
Virtual Assist	Licensed		Upgrade	1 Max: 26	
Global VPN Client	Licensed		Upgrade	2000 Max: 4000	
SSL VPN	Licensed		Upgrade	2 Max: 3002	
WAN Acceleration Client	Licensed		Upgrade	1	
WAN Acceleration Software	Not Licensed	Try	Activate		
Botnet Filter	Licensed				24 Sep 2019
Comprehensive/Advanced Gateway Security Suite			Renew		
Gateway AV/Anti-Spyware/Intrusion Prevention	Licensed		Renew		24 Sep 2019
Premium Content Filtering Service	Licensed		Renew		24 Sep 2019
Analyzer	Licensed		Upgrade		24 Sep 2017
Capture Advanced Threat Protection	Licensed		Renew		25 Mar 2019
Stateful High Availability	Licensed				

Support Service	Status	Manage Service	Expiration
Dynamic Support 24x7	Licensed	Renew	24 Sep 2017
Premier Support	Not Licensed	Activate	
Software and Firmware Updates	Licensed	Renew	24 Sep 2017
Hardware Warranty	Licensed		24 Sep 2017
4-Hour RMA	Not Licensed	Activate	

3 尋找 **SSH (DPI-SSH) 的深度封包偵測**。

4 按一下**啟用**。

5 選擇**繼續**。**SSH (DPI-SSH) 的深度封包偵測**現在顯示**已授權**。

設定 DPI-SSH

DPI-SSH 狀態

目前 DPI-SSH 連線 (目前/尖峰/最大): 0/0/1000

一般設定

啟用 SSH 檢查:

入侵保護： 閘道防毒： 閘道防間諜： 應用程式防火牆：

包含/排除

	排除：	包含：
位址物件/群組	無	全部
服務物件/群組	無	全部
使用者物件/群組	無	所有

接受 取消

主題：

- 設定用戶端 DPI-SSH 檢查
- 自訂用戶端 DPI-SSH 檢查

設定用戶端 DPI-SSH 檢查

您在 **加密服務 > DPI-SSH** 頁面的**一般設定**部分中設定用戶端 DPI-SSH 檢查。

啟用用戶端 DPI-SSH 檢查的步驟如下：

1 在**一般設定**區段中選擇**啟用 SSH 檢查**核取方塊。預設情況下未勾選此選項。

2 選擇一或多種服務檢查的類型；預設未做任何選擇：

- **入侵保護**
- **閘道防毒**
- **閘道防間諜軟體**

  附註：閘道防間諜軟體服務對 DPI-SSH 無作用，因為防間諜軟體旳 TCP 串流不受支援。若勾選此核取方塊，系統不採取動作。

- **應用程式防火牆**

3 按一下**接受**。

自訂用戶端 DPI-SSH 檢查

預設情況下，DPI-SSH 啟用後會套用到裝置上的所有流量。在**包含/排除**區段中您可以自訂套用到哪些流量 DPI-SSH 檢查。

若要自訂 DPI-SSH 用戶端檢查：

1 移至**加密服務 > DPI-SSH**頁面的**包含/排除**部分。

2 從**位址物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSH 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

3 從**服務物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSH 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

4 從**使用者物件/群組排除**和**包含**下拉功能表中，選擇 DPI-SSH 檢查要排除或包含的位址物件或組。預設情況下，**排除**設定為**無**而**包含**設定為**全部**。

5 按一下**接受**。

38

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。如要訪問支援入口網站，請前往 https://www.sonicwall.com/support。

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
- 註冊培訓和認證
- 要求技術支援或客戶服務

如要聯絡 SonicWall 支援，請造訪 https://www.sonicwall.com/support/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。

SonicOS 安全設定
已更新 - 2018 年 1 月
軟體版本 - 6.5
232-004134-00 修訂版 B