SonicWall™ SonicOS 6.5 調査

管理

SONICWALL™

圖例

警告：警告圖示表示，可能造成財產損害、人員受傷或死亡。

注意：注意圖示表示，若未遵循指示，可能造成硬體損害或資料損失。

重要須知、附註、提示、行動或影片：資訊圖示表示有支援資訊。

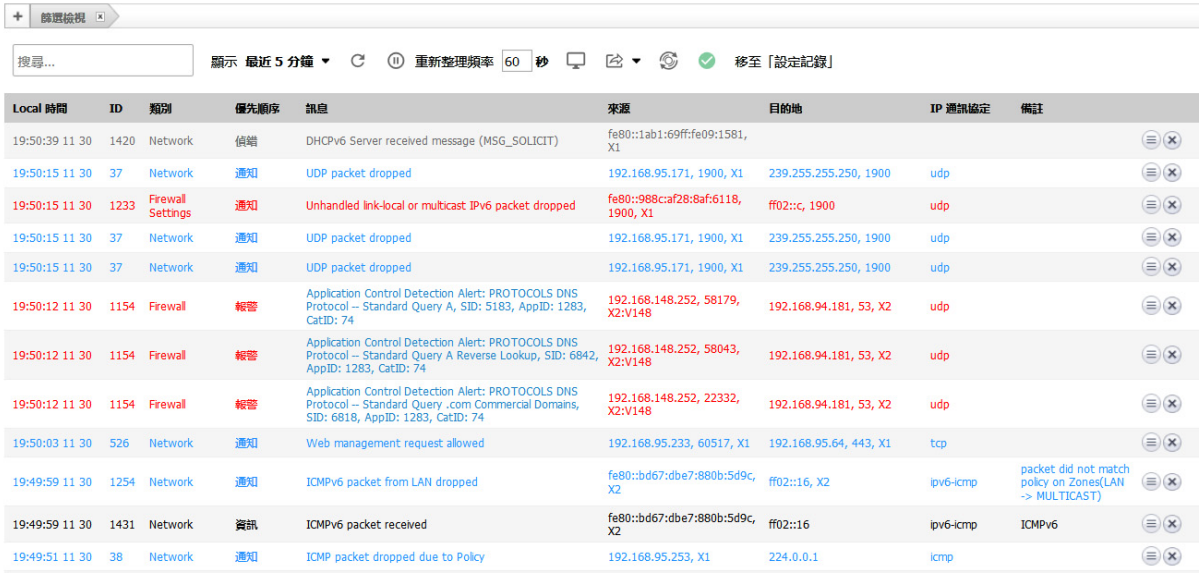
SonicOS 管理
已更新 - 2017 年 12 月
軟體版本 - 6.5
232-004136-00 修訂版 A

目錄

1

活動記錄

SonicWall 網路安全裝置維護有用於追蹤潛在安全威脅的事件記錄。



Local 時間	ID	類別	優先順序	訊息	來源	目的地	IP 通訊協定	備註
19:50:39 11 30	1420	Network	偵錯	DHCPv6 Server received message (MSG_SOLICIT)	fe80::1ab1:69ff:fe09:1581, X1			
19:50:15 11 30	37	Network	通知	UDP packet dropped	192.168.95.171, 1900, X1	239.255.255.250, 1900	udp	
19:50:15 11 30	1233	Firewall Settings	通知	Unhandled link-local or multicast IPv6 packet dropped	fe80::988c:af28:8af:6118, 1900, X1	ff02::c, 1900	udp	
19:50:15 11 30	37	Network	通知	UDP packet dropped	192.168.95.171, 1900, X1	239.255.255.250, 1900	udp	
19:50:15 11 30	37	Network	通知	UDP packet dropped	192.168.95.171, 1900, X1	239.255.255.250, 1900	udp	
19:50:12 11 30	1154	Firewall	報警	Application Control Detection Alert: PROTOCOLS DNS Protocol -- Standard Query A, SID: 5183, AppID: 1283, CatID: 74	192.168.148.252, 58179, X2:V148	192.168.94.181, 53, X2	udp	
19:50:12 11 30	1154	Firewall	報警	Application Control Detection Alert: PROTOCOLS DNS Protocol -- Standard Query A Reverse Lookup, SID: 6842, AppID: 1283, CatID: 74	192.168.148.252, 58043, X2:V148	192.168.94.181, 53, X2	udp	
19:50:12 11 30	1154	Firewall	報警	Application Control Detection Alert: PROTOCOLS DNS Protocol -- Standard Query .com Commercial Domains, SID: 6818, AppID: 1283, CatID: 74	192.168.148.252, 22332, X2:V148	192.168.94.181, 53, X2	udp	
19:50:03 11 30	526	Network	通知	Web management request allowed	192.168.95.233, 60517, X1	192.168.95.64, 443, X1	tcp	
19:49:59 11 30	1254	Network	通知	ICMPv6 packet from LAN dropped	fe80::bd67:dbe7:880b:5d9c, X2	ff02::16, X2	ipv6-icmp	packet did not match policy on Zones(LAN -> MULTICAST)
19:49:59 11 30	1431	Network	資訊	ICMPv6 packet received	fe80::bd67:dbe7:880b:5d9c, X2	ff02::16	ipv6-icmp	ICMPv6
19:49:51 11 30	38	Network	通知	ICMP packet dropped due to Policy	192.168.95.253, X1	224.0.0.1	icmp	

主題：

- 篩選檢視
- 活動記錄功能
- 顯示選項

篩選檢視

您可以在「活動記錄」左上角的**篩選檢視**輸入欄位，使用下拉選項和搜尋字串來縮小搜尋範圍。

若要篩選活動記錄：

1 在**調查**檢視中，按一下**記錄 | 活動記錄**。

2 依**篩選檢視**，按一下 **+** 號。

3 選擇任何您想要的篩選配置。您可以只在一個欄位上進行篩選，或者在所有欄位篩選參數。您可以在「來源 IP」和「目的地 IP」欄位中，輸入部分字串來進行篩選。

4 按一下**接受**。

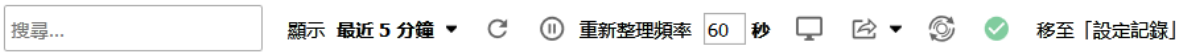
5 若要清除篩選條件，請依欄位名稱按一下 **X**，或依**檢視篩選**按一下 **X** 清除所有篩選條件。

活動記錄功能

活動記錄表格提供大量用於導航、檢視和匯出結果的設定。可以對表格欄進行自訂，以便檢視有關任何事件的完整資料，或僅檢視所需的資料。可以對表格項目進行排序，以按升序或降序顯示。

若要在**活動記錄**中排序項目，請按一下欄標題。項目將按升序或降序排列。欄名稱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。

活動記錄的首列包含幾個功能：



活動記錄功能

選項	功能	操作
搜尋...	搜尋	在**搜尋**欄位中輸入搜尋字串，「活動記錄」會顯示符合字串的記錄項目。按一下搜尋欄位中的 **X** 可刪除搜尋字串。
顯示 最近 5 分鐘	顯示	從下拉功能表，選擇活動記錄的間隔。活動記錄就會從該期間開始顯示。選項有**最近60 秒** (預設)、**最近 2 分鐘**、**最近 5 分鐘**、**最近10 分鐘**、**最近 15 分鐘**和**最近 30 分鐘**。
	重新整理	按一下可立即重新整理活動記錄。

活動記錄功能

選項	功能	操作
	啟動/停止自動重新整理	按一下可啟動或停止自動重新整理功能。
重新整理頻率 60 秒	重新整理間隔	在欄位中，輸入每次重新整理資料之間的秒數。
	顯示選項	按一下可開啟「顯示選項」視窗，然後選擇您要在「活動記錄」中顯示的項目。
	匯出至檔案	將資料匯出至外部檔案。從下拉功能表，選擇檔案格式：**CSV**、**純文字**或**電子郵件**。
	清除	刪除**活動記錄**中顯示的所有記錄。系統會要求您確認您的選擇，之後才會刪除事件。
	狀態	顯示資料庫中記錄的總數量，以及每個狀態類別的最新報告時間。
移至「設定記錄」	移至「設定記錄」	按一下此連結，您會被帶到**管理**檢視上的**記錄和報告 | 記錄設定 > 基本設定**，設定在「活動記錄」中追蹤的項目。

顯示選項

當您按下「顯示選項」圖示，就會顯示以下視窗：

選擇您要在「活動記錄」中顯示為欄位的項目。選項會在下列表格中定義。

一般	關於記錄事件的一般資訊	
	時間	發生事件的本機日期和時間時間。
	ID	識別事件號碼。
	類別	事件的類別。
	群組	事件的群組指定。
	事件	事件的名稱。
	訊息類型	訊息類型，通常為標準訊息字串
	優先順序	事件的優先權層級，例如通知（資訊）或錯誤
	訊息	有關事件的資訊
介面	封包觸發事件的通訊協定的相關資訊	
	來源	來源裝置的名稱（如果適用）。
	來源IP	來源裝置的 IP 位址。
	來源連接埠	來源的連接埠號碼。
	來源介面	來源網路和 IP 位址（如果適用）。
	目的地	目的地裝置的名稱（如果適用）。
	目的地IP	目的地裝置的 IP 位址。
	目的地連接埠	目的地的連接埠號碼。
	目的地介面	目的地網路和 IP 位址（如果適用）。
	乙太網路類型	封包的乙太網路類型（如果已知）。
	來源MAC	來源裝置的 MAC 位址（如果已知）。
	來源供應商	來源裝置製造商的名稱（如果已知）。[a]
	來源區域	來源區域（如果已知）。
	目的地MAC	目的地裝置的 MAC 位址（如果已知）。
	目的地供應商	目的地裝置製造商的名稱（如果已知）。a
	目的地區域	目的地區域（如果已知）。
通訊協定	有效的 NAT 原則相關資訊（如果有）。	
	來源名稱	通訊協定來源名稱
	來源NAT IP	來源 NAT IP 位址集區的來源位址。
	來源NAT 連接埠	來源連接埠的連接埠號碼。
	傳入 SPI	指明輸入封包是否處於狀態封包檢查 (SPI) 模式（如果適用）。
	目的地名稱	通訊協定目的地名稱
	目的地NAT IP	來源 NAT IP 位址集區的目的地位址。
	目的地NAT 連接埠	目的地 NAT 的連接埠號碼。
	傳出 SPI	指明輸出封包是否處於狀態封包檢查 (SPI) 模式（如果適用）。
	IP 通訊協定	用於傳送錯誤和控制訊息的通訊協定（如果已知）。
	ICMP 類型	ICMP 封包的 ICMP 類型（如果已知）。
	ICMP 代碼	ICMP 封包的 ICMP 代碼（如果已知）。

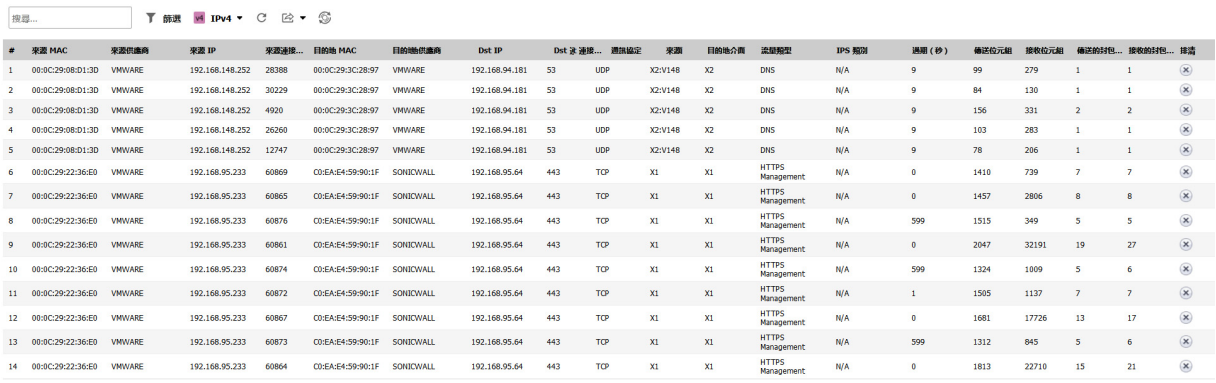
連線	關於 SPI、存取和 IDP 規則以及原則 (若有的話) 的資訊。	
	傳送位元組	已傳輸的位元組數目。
	接收位元組	接收的位元組數目。
	存取規則	觸發事件之存取規則的名稱（如果有）。
	NAT 原則	NAT 原則的名稱。
	VPN 原則	觸發事件之 VPN 原則的名稱（如果有）。
	使用者名稱	使用者名稱，其動作觸發事件。
	工作階段時間	事件前的工作階段持續時間。
	工作階段類型	觸發事件的工作階段類型。
	IDP 規則	觸發事件之 IDP 規則的名稱（如果有）。
	IDP 優先順序	IDP 規則的優先順序。
應用程式	有關將使用之應用程式的資訊。	
	HTTP OP	NPCS 物件 OP requestMethod HTTP OP 代碼。
	URL	NPCS 物件 OP requestMethod HTTP OP 代碼的 URL。
	HTTP 結果	收到網站點擊 rpkt cn1Label 封包的 HTTP 結果代碼（例如 200、403）
	封鎖類別	觸發事件的封鎖類別
	應用程式	將使用的應用程式。
其它	使用者、工作階段和應用程式的相關資訊（如果已知）。	
	防火牆操作	設定的防火牆動作。若未指定動作，顯示 N/A。
	備註	包含附註

a. 每一個有線或無線網路裝置均有其硬體製造商指派的 48 位元 MAC 位址。組織唯一識別項 (OUI) 是可唯一識別全球或全世界供應商、製造商或其他組織的 24 位元數字。前三個八位元組的 MAC 位址是 OUI。

2

連線記錄

SonicWall 網路安全裝置為追蹤連到 SonicWall 安全裝置的所有作用中連線，維護一份「連線記錄」。若要檢視「連線記錄」表，請導覽到**調查**檢視上的**記錄 | 連線記錄**。



#	來源 MAC	來源供應商	來源 IP	來源連接...	目的地 MAC	目的地供應商	Dst IP	Dst 連接...	通訊協定	來源	目的地介面	流量類型	IPS 類別	過期（秒）	傳送位元組	接收位元組	傳送的封包...	接收的封包...	排清
1	00:0C:29:08:D1:3D	VMWARE	192.168.148.252	28388	00:0C:29:3C:28:97	VMWARE	192.168.94.181	53	UDP	X2:V148	X2	DNS	N/A	9	99	279	1	1	
2	00:0C:29:08:D1:3D	VMWARE	192.168.148.252	30229	00:0C:29:3C:28:97	VMWARE	192.168.94.181	53	UDP	X2:V148	X2	DNS	N/A	9	84	130	1	1	
3	00:0C:29:08:D1:3D	VMWARE	192.168.148.252	4920	00:0C:29:3C:28:97	VMWARE	192.168.94.181	53	UDP	X2:V148	X2	DNS	N/A	9	156	331	2	2	
4	00:0C:29:08:D1:3D	VMWARE	192.168.148.252	26260	00:0C:29:3C:28:97	VMWARE	192.168.94.181	53	UDP	X2:V148	X2	DNS	N/A	9	103	283	1	1	
5	00:0C:29:08:D1:3D	VMWARE	192.168.148.252	12747	00:0C:29:3C:28:97	VMWARE	192.168.94.181	53	UDP	X2:V148	X2	DNS	N/A	9	78	206	1	1	
6	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60869	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	0	1410	739	7	7	
7	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60865	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	0	1457	2806	8	8	
8	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60876	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	599	1515	349	5	5	
9	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60861	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	0	2047	32191	19	27	
10	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60874	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	599	1324	1009	5	6	
11	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60872	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	1	1505	1137	7	7	
12	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60867	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	0	1681	17726	13	17	
13	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60873	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	599	1312	845	5	6	
14	00:0C:29:22:36:E0	VMWARE	192.168.95.233	60864	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP	X1	X1	HTTPS Management	N/A	0	1813	22710	15	21	

主題：

檢視連接

SonicWall 裝置的連線會列在**連線記錄**中。表格的欄位名稱說明如下：

來源 MAC	來源裝置的 MAC 位址。
來源供應商	來源裝置的製造商。
來源 IP	來源裝置的 IP 位址。
來源連接埠	來源裝置的連接埠號碼。
目的地 MAC	目的地裝置的 MAC 位址。
目的地供應商	目的地裝置的製造商。
Dst IP	目的地裝置的 IP 位址。
Dst 連接埠	目的地裝置的連接埠號碼。
通訊協定	用於連線的通訊協定，例如 TCP 或 ICMPv6。
來源介面	來源裝置上的介面。
目的地介面	目的地裝置上的介面。

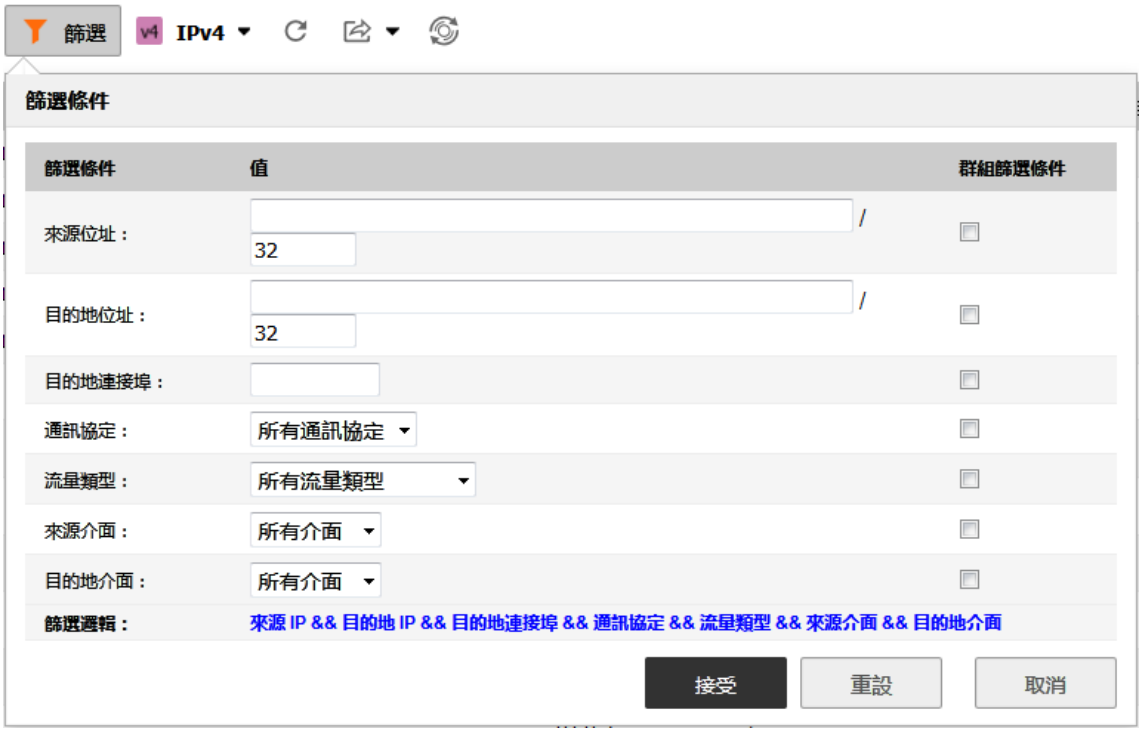
流量類型	連線的流量類型，例如一般或 HTTP 管理，
IPS 類別	使用的入侵保護系統 (IPS) 類型；N/A = 不適用。
過期（秒）	連線到期前剩餘的秒數。
傳送位元組	已傳送的位元組數目。
接收位元組	接收的位元組數目。
傳送的封包數	已傳送的封包數。
接收的封包數	接收的封包數。
排清	包含每個項目的**排清**圖示。

搜尋連線記錄

您可以使用**搜尋**欄位來尋找符合特定搜尋條件的連線。在**搜尋**欄位中輸入搜尋字串，「連線記錄」即顯示符合字串的項目。按一下**搜尋**欄位中的 **X** 可刪除搜尋字串。

篩選連線記錄

您可以篩選「連線記錄」表，使其僅顯示符合**篩選條件**選項中所指定條件的連線。



您可以依據下列進行篩選：

來源位址	目的地位址	目的連接埠	通訊協定
流量類型	來源介面	目的地介面	

篩選邏輯顯示篩選條件套用方式。

您在其中輸入值的欄位將會組合為包含邏輯 AND 的搜尋字串。例如，如果在**來源 IP** 和**目的地 IP** 中輸入值，則搜尋字串將查找符合的連接：

```
Source IP AND Destination IP
```

勾選任意兩項或多項準則旁邊的**群組**核取方塊可使用邏輯 **OR** 進行組合。例如，如果在**來源 IP**、**目的地 IP**、**通訊協定**中輸入值，然後勾選來源 IP 和目的地 IP 旁的群組，則搜尋字串將尋找符合的連接：

```
(Source IP OR Destination IP) AND Protocol
```

按一下**套用篩選條件**以立即將篩選條件套用到**活動連接**表格。按一下**重設篩選條件**清除篩選條件，然後再次顯示未篩選的結果。

可以將使用中連結清單匯出到檔案中。按一下**匯出結果**，並選擇是否想要將結果匯出為普通文字檔或逗號分隔值 (CSV) 檔案，以便匯入到試算表、報告工具或資料庫中。如果系統提示打開或儲存檔案，請選擇**儲存**。然後輸入檔案名稱和路徑，並按一下**確定**。

連線記錄功能

連線記錄表格提供數個用於導航、檢視和匯出結果的設定。可以對表格項目進行排序，以按升序或降序顯示。

若要在**活動記錄**中排序項目，請按一下欄標題。項目將按升序或降序排列。欄名稱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。

活動記錄的首列包含幾個功能：

活動記錄功能

選項	功能	操作
	IPv4/IPv6	IPv6 和 IPv4 的**連線記錄**的設定相同。若要變更檢視，請從下拉功能表中選擇 IP 版本。預設為 **IPv4**。
	重新整理	按一下可立即重新整理活動記錄。
	匯出至檔案	將資料匯出至外部檔案。從下拉功能表，選擇檔案格式：**CSV**、**純文字**或**電子郵件**。
	清除	刪除**活動記錄**中顯示的所有記錄。系統會要求您確認您的選擇，之後才會刪除事件。
	排清	按下此圖示可排清表格中的該連線。此選項是在表格的最右欄中找到。

3

Appflow 記錄

Appflow 記錄提供即時的傳入和傳出網路資料。Appflow 監控介面中提供了各種檢視和可自訂選項，用於協助按照應用程式、使用者、URL、啟動者、回應者、威脅、VoIP、VPN、裝置或內容來顯示流量資料。

主題：

- Appflow 表格選項
- Appflow 記錄功能
- 群組選項
- Appflow 狀態
- Appflow 顯示選項

Appflow 表格選項

Appflow 表格選項包含關於傳入和傳出的網路流量的詳細資料。每個選項或按鈕提供網路流量的特定檢視。

Appflow 表格選項

此標籤	顯示
應用程式	目前存取網路的應用程式清單。
使用者	目前連接到網路的使用者清單。

Appflow 表格選項

此標籤	顯示
URL	目前使用者存取的 URL 清單。 *若要啟用此報告：* 1 在**管理**檢視上，導覽至原則 | **物件 > 內容篩選物件**。 2 選擇 **CFS 動作物件**。 3 按一下 **CFS 預設動作**的**編輯**圖示。 4 勾選**啟用流量報告**核取方塊。 5 按一下**確定**。 6 在**管理**檢視上，導覽至系統安裝 | **網路 > 區域**。 7 對於要監視的區域，按一下**編輯**圖示。顯示**編輯區域**對話。 8 勾選**啟用用戶端內容篩選服務**核取方塊。 9 按一下**確定**。
啟動器	目前連接啟動者的詳細資料。
回應者	目前連接回應者的詳細資料。
威脅	網路所遭遇的威脅清單。
VoIP	目前 VoIP 和媒體流量。
VPN	目前連接到網路的 VPN 工作階段清單。
裝置	目前連接到網路的裝置清單。
目錄	關於流經網路的流量類型的資訊。 *若要啟用此報告：* 1 在**管理**檢視上，導覽至**安全設定 | 安全服務 > 入侵保護**。 2 在 **IPS 全域設定**區段中，勾選**啟用 IPS** 核取方塊。 3 按一下**接受**。 4 導覽至**原則 | 規則 > 應用程式控制**。 5 在**應用程式控制全域設定**區段中，勾選**啟用應用程式控制**核取方塊。 6 按一下**接受**。 7 導覽至**系統安裝 | 網路 > 區域**。 8 對於要監視的區域，按一下**編輯**圖示。 9 選擇**啟用 IPS**核取方塊。 10 按一下**確定**。

Appflow 記錄功能

Appflow 記錄功能允許自訂 Appflow 記錄表格。利用建立規則和向篩選條件新增項目的功能，可以實現更多應用程式控制和使用者控制。此外還提供了不同的檢視、暫停和播放功能、可自訂的資料間隔和重新整理頻率，以幫助顯示傳入的即時資料。按群組選擇資料並設定標籤上顯示的欄以精化顯示結果。

Appflow 記錄功能

選項	小元件	說明
建立	建立	啟動應用程式控制精靈。如需使用此精靈的更多資訊，請參見 *SonicWall SonicOS 6.5 原則*中的「原則 | 規則 > 應用程式規則和應用程式控制」。 **附註：**一般和服務類型應用程式不能包含在規則中。
篩選	篩選	關聯標籤中的資料。如需建立篩選條件的更多資訊，請參見篩選條件選項。
搜尋	搜尋...	在**搜尋**欄位中輸入搜尋字串，「Appflow 記錄」會顯示符合字串的記錄項目。按一下搜尋欄位中的 **X** 可刪除搜尋字串。
顯示*間隔* (其中*間隔*是監控操作之間的時間)	顯示 最近 5 分鐘	從下拉功能表，選擇活動記錄的間隔。活動記錄就會從該期間開始顯示。選項有**最近 60 秒** (預設)、**最近 2 分鐘**、**最近 5 分鐘**、**最近10 分鐘**、**最近 15 分鐘**和**最近 30 分鐘**。
依*選項*群組 (其中*選項*是下拉功能表的選項之一)	分組依據 應用程式	根據下拉功能表中的選項將選擇的項目分類。選項會根據所選擇的標籤而異。請參閱群組選項。
IP 版本		允許選擇網際網路通訊協定：**IPv4**、**IPv6** 或兩者 (**IPv4 和 IPv6**)（預設）。
顯示選項		按一下可開啟「顯示選項」視窗，然後從下拉功能表選擇選項：**表格檢視**、**圖表檢視**、**監控檢視**或**資料行顯示**。**資料行顯示**允許您自訂要顯示的資料行。
匯出至檔案		將資料流量匯出為逗號分隔變數 (.csv) 格式。
狀態		按一下以開啟狀態視窗。

群組選項

群組選項會根據指定的群組對資料進行排序，而每個群組包含不同分組選項。

按照按鈕群組選項

Appflow 表格選項	按照選項群組	說明
應用程式	應用程式（預設）	按單獨的應用程式顯示產生的所有流量。
	類別	按應用程式類別對產生的所有流量進行分組。
	簽章	按應用程式簽章對產生的所有流量進行分組

按照按鈕群組選項

Appflow 表格選項	按照選項群組	說明
使用者	使用者名稱（預設）	按指定使用者對產生的所有流量進行分組。
	IP 位址	按指定 IP 位址對產生的所有流量進行分組。
	網域名稱	按指定網域名稱對產生的所有流量進行分組。
	驗證類型	按指定授權方法對產生的所有流量進行分組。
URL	URL（預設）	按每個 URL 顯示產生的所有流量。
	網域名稱	按網域名稱對產生的所有流量進行分組。
	評等	基於 CFS 評等對產生的所有流量進行分組。
啟動器	IP 位址（預設）	按指定 IP 位址對產生的所有流量進行分組。
	介面	根據防火牆介面對所有流量進行分組。
	國家或地區	基於國家/地區 IP 資料庫，按每個國家/地區對產生的所有流量進行分組。
回應者	IP 位址（預設）	按 IP 位址對所有流量進行分組。
	介面	按介面對回應者進行分組。
	國家或地區	基於國家/地區 IP 資料庫，按每個國家/地區對回應者進行分組。
威脅	入侵	顯示在其中已識別入侵的流量。
	病毒	顯示在其中已識別病毒的流量。
	間諜軟體	顯示在其中已識別間諜軟體的流量。
	垃圾郵件	顯示歸為垃圾郵件類別的所有流量。
	殭屍網路	顯示已封鎖的連接前往/來自 Botnet 伺服器的所有流量。
	全部（預設值）	顯示已識別為威脅或歸為垃圾郵件類別的所有流量。
VoIP	媒體類型（預設）	根據媒體類型對 VoIP 流量進行分組。
	呼叫者 ID	根據呼叫者 ID 對 VoIP 流量進行分組。
VPN	遠端 IP 位址（預設）	根據遠端 IP 位址對 VPN 流量進行分組。
	本機 IP 位址	根據本機 IP 位址對 VPN 流量進行分組。
	名稱	根據通道名稱對 VPN 流量進行分組。
裝置	IP 位址（預設）	按網路內部的 IP 位址對流量進行分組。
	介面	按防火牆上的介面對流量進行分組。
	名稱	按裝置名稱或 MAC 位址對流量進行分組。
目錄	電子郵件地址（預設）	按電子郵件地址對內容進行分組。
	檔案類型	按偵測到的檔案類型對流量進行分組。

Appflow 狀態

Appflow 狀態會在**狀態**圖示在工具列中時顯示。**Appflow 狀態**提供授權資訊、狀態、應用程式規則的簽章更新、應用程式控制進階、GAV、IPS、防間諜軟體、CFS、反垃圾郵件、BWM、國家/地區資料庫、Geo-IP 封鎖或 Botnet 封鎖。工具提示還顯示資料庫中的最大流量以及 Appflow 的啟用方式。為便於設定 Appflow 監控顯示器，此工具提示提供每個項目相應 UI 頁面的連結，如 **Appflow > 流量報告**，用於設定 Appflow。

按一下右上角的 **X** 可關閉 **Appflow 狀態**。

Appflow 顯示選項

Appflow 顯示提供了三種檢視：**表格檢視**、**圖表檢視**和**監控檢視**。每個檢視都為您提供了唯一的即時傳入資料顯示。

表格檢視

在**表格檢視**中，依照上方所選擇的 Appflow 按鈕而定，表格會由顯示即時資料的欄位組成。這些欄可按類別排序。有些欄位對所有按鈕通用。不過，VoIP 標籤也有自己的指定欄位。工具提示會與大多數的欄位標題關聯，提供定義。

圖表檢視

圖表檢視顯示排名前列的項目數以及每個項目使用的頻寬百分比。使用的頻寬百分比的確定方法是，先獲取排名前列的項目所使用的頻寬總量，然後將頻寬總量除以排名前列的項目數量。然後，資料是顯示在圓形圖中。

監控檢視

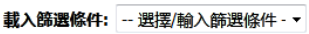
監控檢視根據指定時間段內使用的 Kbps 顯示網路使用情況。對於上方的每個 Appflow 按鈕，可以選擇在圖表下的下拉功能表中的其他選項：在**縮放**欄位中，**自動 Y 縮放比例**是預設值。您可以為不同縮放新增特定數字和單位。

篩選條件選項

附註：篩選條件選項雖可影響其它檢視，但它只適用於清單檢視。

Appflow 篩選選項可以篩選傳入的即時資料。您可以套用、建立和刪除篩選條件以自訂顯示的資訊。篩選選項會套用於所有 Appflow 按鈕。

Appflow 監控篩選條件選項

選項	小元件	說明
新增到篩選條件		將目前選擇新增到篩選條件。 若要使用篩選條件選項，必須選擇至少一個項目。選擇項目後，所有其他標籤將更新為與篩選條件中的項目有關的資訊。
從篩選條件中移除		按一下 **X**，從篩選條件檢視中移除所有目前選擇。
篩選元素		指示一種篩選元素。
載入篩選條件		提供列出現有篩選設定的下拉功能表，或者您也可以輸入新的名稱來建立新的篩選條件。
儲存		儲存目前的篩選條件設定。
刪除		刪除目前的篩選條件設定。
「篩選檢視」按鈕		關聯標籤中的資料。

建立篩選條件可減少在「Appflow 記錄」中看到的資料量。您可建立簡單或複雜的篩選條件，取決於您指定的準則。這樣，您可以專注於感興趣的點，而不會受到其他應用程式的干擾。

主題：

- 使用篩選檢視建立篩選條件
- 檢視篩選檢視中的項目
- 儲存篩選檢視
- 刪除篩選檢視

使用篩選檢視建立篩選條件

若要使用「篩選檢視」建立篩選條件：

1 導覽至**調查**檢視。

2 選擇**記錄 | Appflow 記錄**。

3 選擇一個按鈕：例如，**應用程式**或**使用者**。

4 在標籤上勾選要新增到篩選條件的項目的核取方塊。

5 按一下**篩選檢視**按鈕或**新增到篩選條件**按鈕。

在將項目新增到篩選條件之後，記錄中只能看到那些項目。在其他「Appflow 記錄」檢視中，只能看到與篩選項目相關的項目的資訊。

在「篩選檢視」中，帶有篩選條件的檢視以一個按鈕表示。

6 若要進一步精簡篩選條件，請選擇另一標籤然後重複步驟 4 和步驟 5。將每個標籤都新增到「篩選檢視」中。

檢視篩選檢視中的項目

若要快速檢視篩選檢視中的項目，請在「篩選檢視」橫幅中按一下顯示的選項。此時會出現一個下拉功能表，列出在該選項中選擇的所有項目。

若要關閉下拉功能表，請按一下選項名稱。

儲存篩選檢視

您可以在建立後儲存篩選檢視，供將來使用。

儲存篩選檢視：

1 按一下**載入篩選條件**下拉功能表。

2 選擇清單頂部的空行。

3 為篩選條件輸入一個方便易記的名稱。

4 按一下**載入篩選條件**下拉功能表旁的**儲存篩選條件**按鈕。

刪除篩選檢視

您可以刪除所有篩選檢視、某個標籤的篩選檢視，或僅刪除某個指定篩選檢視中的一些項目。

如何刪除篩選檢視

刪除	執行操作
所有篩選檢視	按一下**從篩選條件中移除**按鈕中的 X
某個指定篩選檢視	按一下此標籤的「篩選檢視」按鈕中的 X

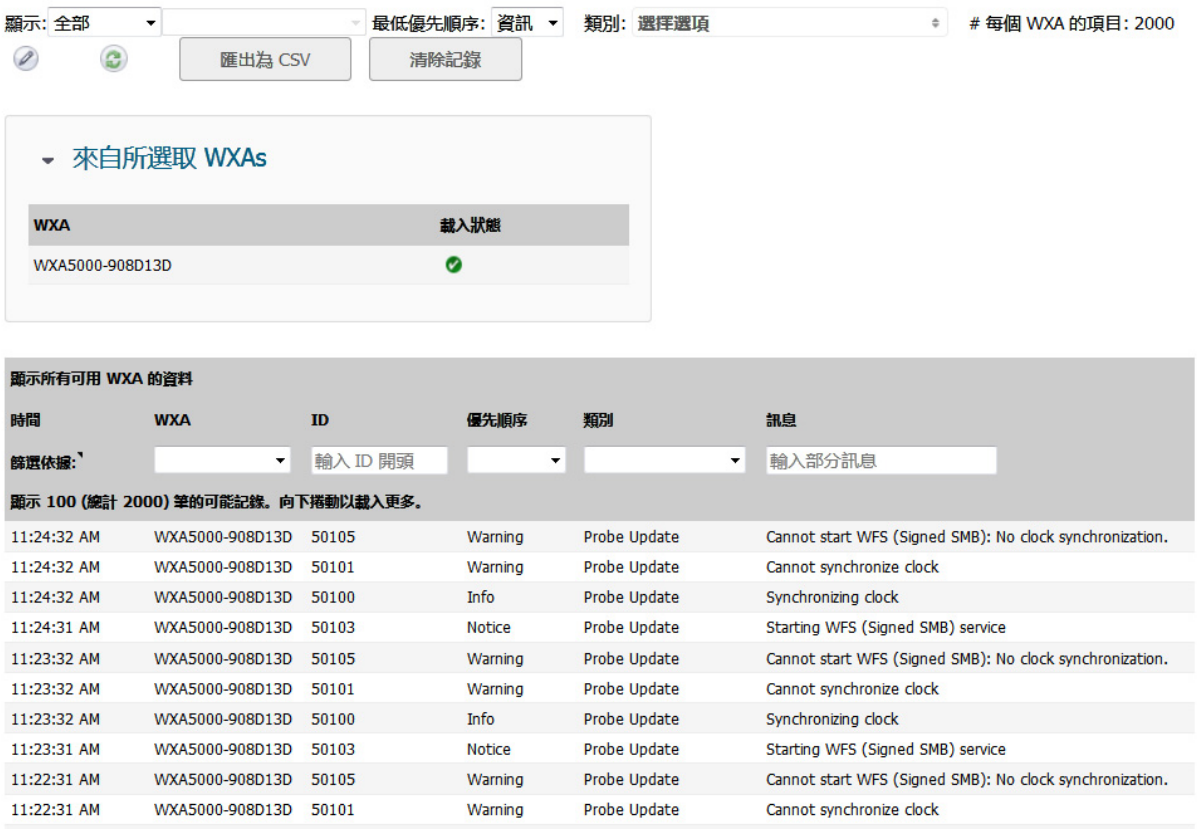
如何刪除篩選檢視

刪除	執行操作
某個篩選檢視中的一個或多個項目	按一下標籤的名稱以顯示下拉功能表，然後按一下要刪除的項目旁的 X
已儲存的篩選條件	在「加載篩選條件」下拉功能表中勾選此篩選條件，然後按一下「加載篩選條件」下拉功能表右邊的「刪除」按鈕。

4

WAN 加速記錄

調查檢視上的 **WAN 加速 > 記錄**頁面提供記錄事件訊息的詳細清單，並提供多個選項，以變更記錄訊息的顯示方式。「最小優先順序」和「類別」下拉功能表可用來決定從 WXA 擷取哪些記錄。資料上方的篩選條件決定實際要在畫面上顯示哪些項目。使用捲動功能讓在您向下捲動頁面時查看更多的記錄項目。



工具列中的功能表和按鈕決定從 WXA 擷取哪些記錄。記錄未全部都立即載入表格中。當您向下捲動時會附加更多記錄。

主題：

- 管理 WAN 加速記錄
- 所選 WXA 的資料
- 篩選 WAN 加速記錄

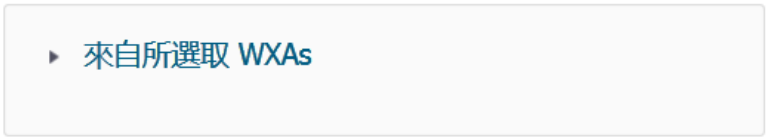
管理 WAN 加速記錄

WAN 加速 > 記錄頁面會顯示來自連接的 WXA 的記錄訊息。使用下列選向來管理 WAN 加速記錄中的資料。

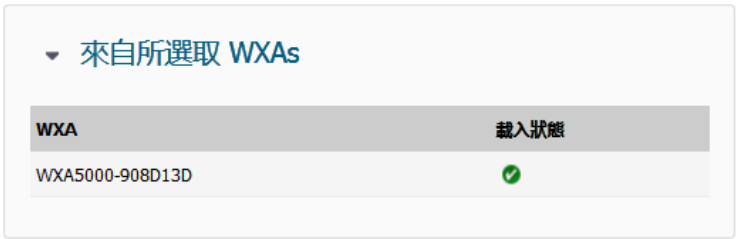
名稱	選項	說明
顯示	顯示: 全部	從功能表選擇是否要顯示**全部**、**對於群組**或**對於 WXA**
最小優先順序	最低優先順序: 資訊	顯示所選優先順序或更優先的記錄項目。
類別	類別: 選擇選項	顯示所選類別的記錄項目。勾選您要顯示的選項。取消勾選不要顯示的選項。
# 項目: 2000	# 每個 WXA 的項目: 2000	顯示所擷取和顯示在記錄清單中的項目數量。依照數量而定，您可能需要捲動表格才能檢視所有記錄項目。
編輯按鈕		顯示**記錄: 報告期間**視窗。您可以設定要檢視報告的記錄項目的期間，並從各個 WAN 加速器設定項目數的限制。
「**重新整理**」按鈕		重新整理 **WAN 加速 > 記錄**。按一下「重新整理」按鈕手動更新「記錄」頁面。
匯出為 CSV 按鈕	匯出為 CSV	將目前記錄的訊息匯出為逗號分隔值 (CSV) 檔，可儲存為試算表和進行檢視。時間、優先順序、類別、訊息和 ID 欄位會匯出。
清除記錄按鈕	清除記錄	從 WXA 裝置清除所有記錄的訊息。 **附註：**此操作無法回復。
篩選依據下拉功能表		從下拉清單中選擇，以及在文字欄位中輸入文字，來篩選結果：**ID**、**優先順序**、**類別**和**訊息**。您選擇的篩選條件決定從 WXA 系列裝置擷取的哪些記錄項目顯示在「記錄」畫面上。

所選 WXA 的資料

到 WAN 加速記錄的上方，在**記錄 | WAN 加速記錄**有標示為**所選 WXA 的資料**的窗格。



如果按一下箭頭，窗格會展開以顯示基礎結構中所選 WXA 的相關資訊。也顯示 WXA 的載入狀態。



篩選 WAN 加速記錄

記錄表標頭的設計是為提供有關記錄的基本資訊，以及讓您篩選記錄。

1 標頭部分的頂端線指出什麼 WXA 要包含在 WAN 加速記錄中。在本範例中，會顯示所有 WXA。

2 這些是表格的標頭。

3 這些是**篩選依據**欄位，您可用來自訂 WAN 加速記錄的檢視。

欄位	定義	
WXA	下拉功能表可讓您選擇要篩選的 WXA。	
ID	開放的欄位您可以輸入前幾個 ID，而記錄資料會立即篩選那些值。按一下欄位右側的 **X** 可清除內容。您可能需要重新整理畫面來清除篩選。 WXA 元件的 ID 號碼範圍為：	
	10000-19999	WXA 系統
	20000-29999	WXA 系統網路
	30000-39999	TCP 加速
	40000-49999	未簽署的 WFS
	50000-59999	已簽署的 WFS
	60000-69999	Web 快取
	70000-79999	管理
優先順序	下拉功能表可讓您選擇要篩選的優先順序層級。選項包括：**錯誤**、**資訊**、**注意**和**警告**。若要清除篩選條件，請選擇空白選項。	
類別	下拉功能表可讓您選擇要篩選的記錄類別。若要清除篩選條件，請選擇空白選項。	
訊息	開放的欄位您可以輸入訊息任何部分的字母或字詞來進行篩選。例如，您若輸入*監控*，便會篩選記錄，如此所有含有*監控*一詞的訊息都會篩選。按一下欄位右側的 **X** 可清除內容。您可能需要重新整理畫面來清除篩選。	

4 標頭部分的底部線指出要顯示多少筆記錄。如果您的記錄數量比畫面目前可顯示來的多，它會指示您向下捲動。並且當您篩選記錄時也會跟著變動，如此每次您變更篩選參數時也可看到有多少記錄。

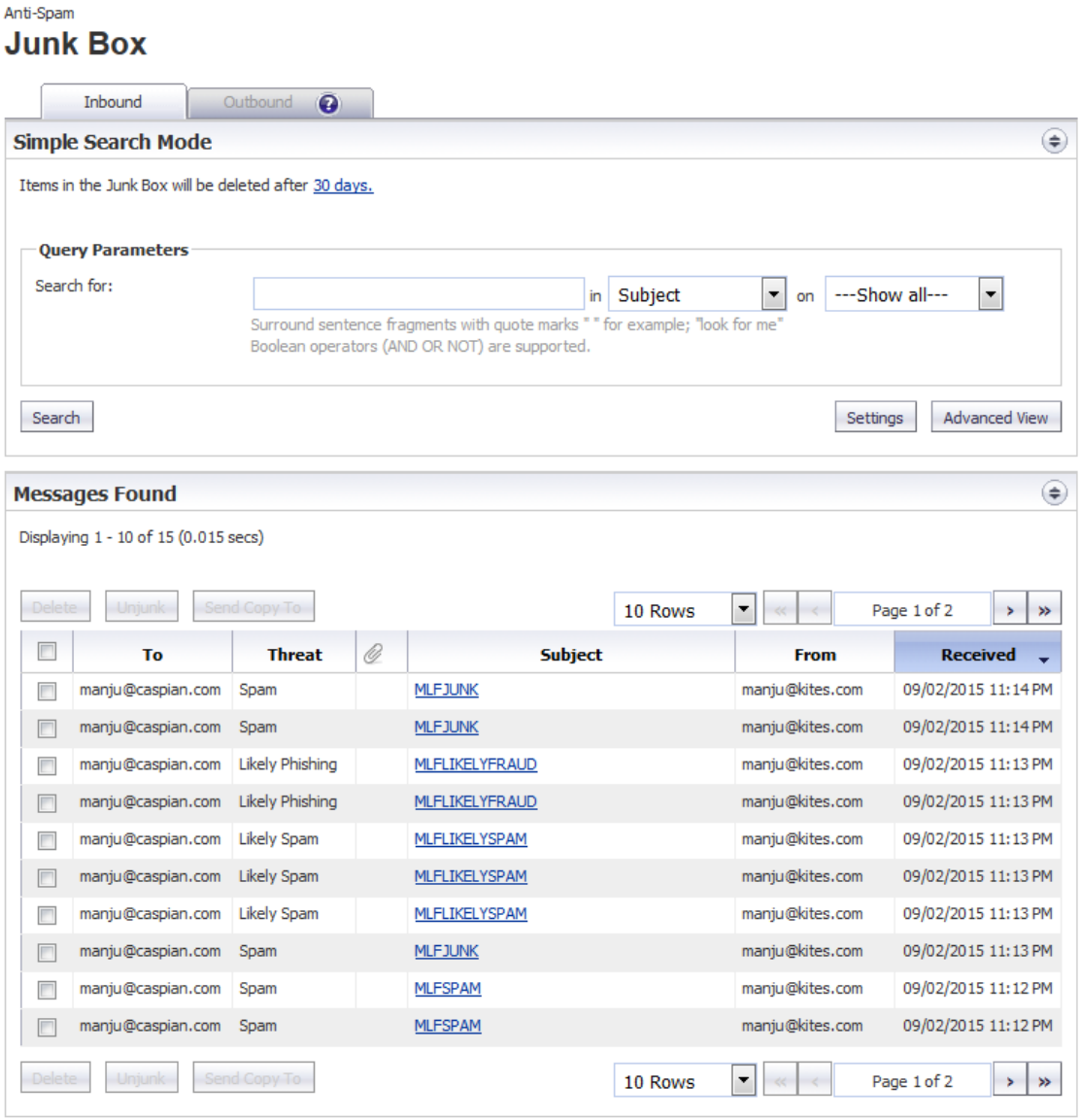
5

反垃圾郵件垃圾儲存區

反垃圾郵件特性提供快速、高效和有效的方法來為現有的防火牆新增反垃圾郵件、防網路釣魚和防毒功能。在典型的反垃圾郵件設定中，您在 SonicOS 介面選擇反垃圾郵件功能並授權，從而新增此功能。這樣，防火牆就能使用先進垃圾郵件篩選技術來減少傳遞至使用者的垃圾郵件數量。

您可以查看反垃圾郵件垃圾儲存區，以檢視、搜尋和管理目前位於 Exchange 或 SMTP 伺服器上的垃圾儲存區中的郵件。在**調查**檢視上，導覽到**記錄 | 反垃圾郵件垃圾儲存區**。

附註：此功能只能在已安裝垃圾儲存區的情況下使用。



主題：

導覽垃圾儲存區

反垃圾郵件垃圾儲存區含有幾個標籤、按鈕和圖示，您可以用來管理和檢視資料。

- **傳入**標籤僅列出傳入訊息。
- **傳出**標籤僅列出傳出訊息。

> **附註：**如果無法檢視**輸出**標籤，則必須升級您的垃圾儲存區授權。按一下**問號**圖示可取得更多資訊。

這兩個標籤的功能和顯示相同。每個標籤包含兩個部分：

- **簡單/進階搜尋模式**
- **找到的郵件**

您可以按一下**展開/收起**圖示，收起或展開任一部分。

在**簡單搜尋模式**部分中，有其他頁面的兩個連結：

- 如需變更垃圾郵件在刪除前保留的時間長度，請按一下**垃圾儲存區中的項目 30 天**後將刪除末尾處的連結。您會被帶至**管理**檢視上可進行變更的**安全設定 | 反垃圾郵件 > 垃圾儲存區設定**頁面。
- 如需顯示**反垃圾郵件 > 設定**頁面，請按一下此部分底部的**設定**按鈕。您會被帶至**管理**檢視上可進行變更的**安全設定 | 反垃圾郵件 > 垃圾儲存區設定**頁面。

管理訊息

找到的郵件表顯示垃圾儲存區中隔離郵件的相關資訊。

此欄	包含或指示
核取方塊	表中每個項目的核取方塊。勾選訊息旁的方塊可選取該項進行操作。如果勾選標題中的方塊，會選取表格中的所有項目。
目的地	收件者電子郵件地址。
威脅	電子郵件構成的威脅類型。
迴紋針圖示	電子郵件包含附件。
主題	郵件主旨行。
來源	發件人電子郵件地址。
接收	注明郵件傳送時間。

使用**找到的郵件**表頂部的按鈕執行以下「垃圾儲存區」管理任務：

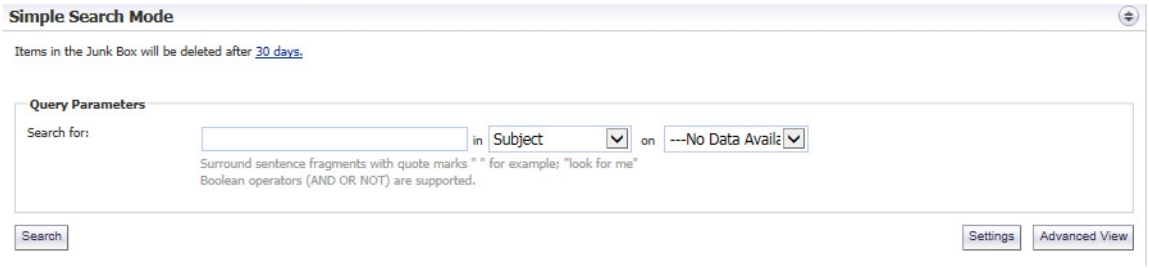
按鈕	功能
刪除	永久刪除「垃圾儲存區」中的所選郵件；如需刪除所有郵件，請按一下表標題中的核取方塊
非垃圾郵件	從垃圾儲存區中移除所選郵件，將其傳遞給目的地使用者。每封郵件送達使用者郵件箱時，送達時間和日期由 Exchange 伺服器設定。
將副本傳送到	將所選郵件保留在垃圾儲存區中，將其副本傳送給使用者。

執行簡單搜尋

若要執行垃圾儲存區資料的簡單搜尋：

1 在**調查**檢視上，導覽到**記錄 | 反垃圾郵件垃圾儲存區**。

2 選擇**傳入**標籤或**傳出**標籤。



3 在**搜尋**欄位中輸入搜尋字串。將句子片段括在引號 (「) 內。可使用布林運算子（AND、OR、NOT）。

4 在下拉功能表**在**選擇要搜尋的目的地電子郵件欄位：

- **主旨**（預設）
- **來源**
- **目的地**
- **唯一郵件 ID**

5 在**日期**下拉功能表中，選擇要搜尋的日期。

- **---顯示全部---**（預設）
- **今天**
- 指定日期；日期數將根據垃圾郵件保留的時間長度而有所差異

6 按一下**搜尋**按鈕開始搜尋。

結果將顯示在頁面的**找到的郵件**部分中，並在頂部顯示一封郵件。如果搜尋成功，此郵件將包含**成功！**字樣且整個郵件將以綠色高亮顯示。如果搜尋失敗，此郵件將包含**警告！**字樣且整個郵件將以黃色高亮顯示。

7 將**找到的郵件**表恢復至其原始狀態的步驟如下：

a 刪除**搜尋**欄位中的資料。

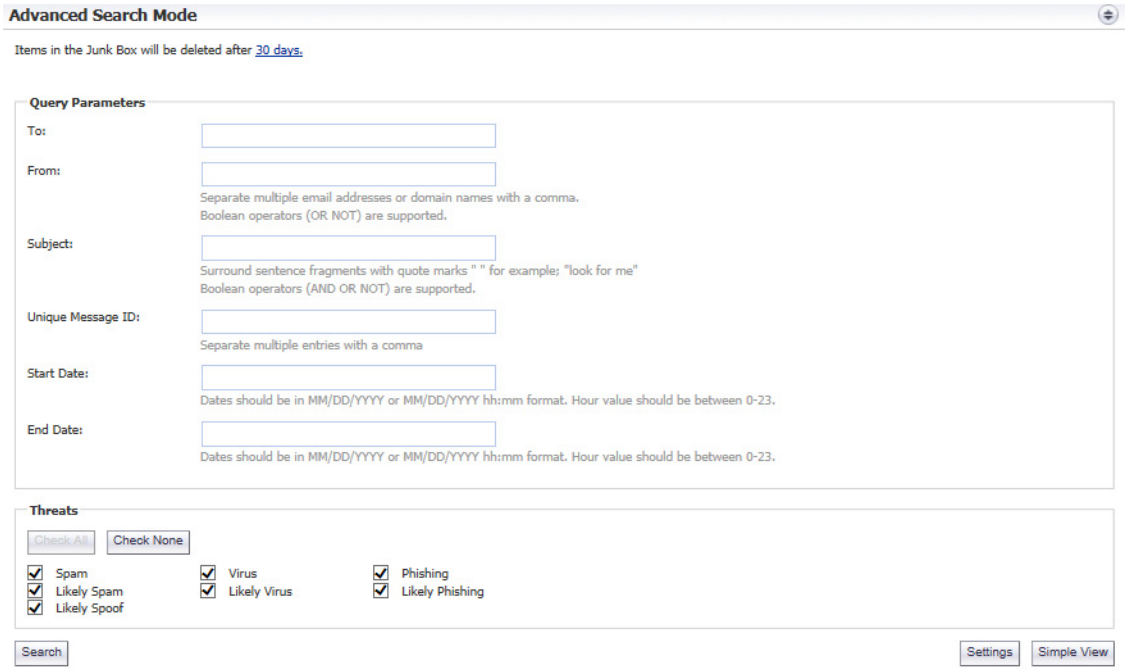
b 按一下**搜尋**。

執行進階搜尋

1 在**調查**檢視上，導覽到**記錄 | 反垃圾郵件垃圾儲存區**。

2 選擇**傳入**標籤或**傳出**標籤。

3 按一下**進階檢視**按鈕。



4 在**查詢參數**部分，將您的搜尋條件輸入至一個或多個**查詢參數**欄位：

參數	查詢條件
目的地	收件者電子郵件地址。
來源	發件人電子郵件地址。 用逗號隔開多個電子郵件地址或網域名稱。支援布林運算子 OR 和 NOT。
主題	郵件主旨。 將句子片段括在引號 (「) 內。支援布林運算子 AND、OR 和 NOT。
唯一郵件 ID	唯一郵件 ID。 用逗號隔開多個項目。
起始日期	要搜尋的起始日期。 輸入任一格式的日期： • MM/DD/YYYY • MM/DD/YYYY hh:mm（小時值應介於 0 至 23 [24 小時制] 之間）
結束日期	要搜尋的結束日期。 輸入任一格式的日期： • MM/DD/YYYY • MM/DD/YYYY hh:mm（小時值應介於 0 至 23 [24 小時制] 之間）

5 在**威脅**部分中，指定要搜尋的威脅類別。預設情況下，選擇所有類別。

清除核取方塊可刪除您不想包含在搜尋中的任何類別。如需取消選擇所有類別，請按一下**取消全部勾選**按鈕。所有類別將取消勾選，**全部勾選**按鈕啟用且**取消全部勾選**按鈕變為灰色。

6 按一下**搜尋**按鈕開始搜尋。

結果將顯示在頁面的**找到的郵件**部分中，並在頂部顯示一封郵件。如果搜尋成功，此郵件將包含**成功！**字樣且整個郵件將以綠色高亮顯示。如果搜尋失敗，此郵件將包含**警告！**字樣且整個郵件將以黃色高亮顯示。

7 如需返回至**簡單檢視**，請按一下**簡單檢視**按鈕。

8 將**找到的郵件**表恢復至其原始狀態的步驟如下：

a 刪除**搜尋**欄位中的資料。

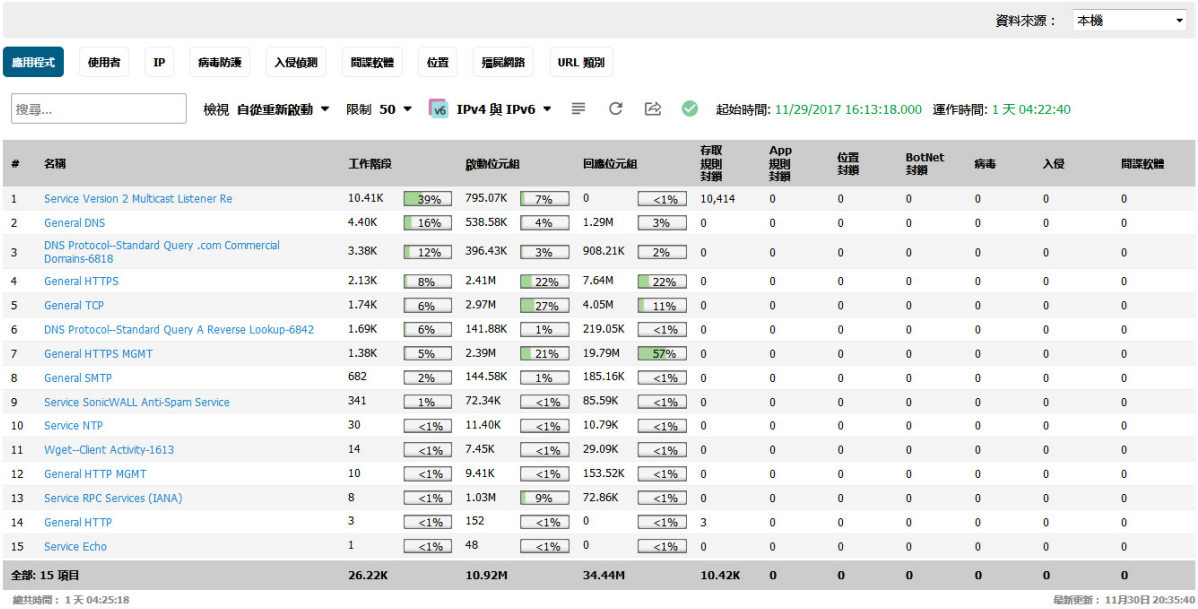
b 按一下**搜尋**。

6

Appflow 報告

Appflow 報告頁面按照應用程式、使用者、IP 位址、病毒、入侵、間諜軟體、位置、botnet 和 URL 評等來提供可設定的排程報告。Appflow 報告統計資料使您可以檢視網路中正在進行的頂層匯總報告，還可以一目了然地獲得下列問題的答案：

- 我的網路中正在執行的應用程式中最常用的有哪些？
- 在工作階段總數和位元組總數兩個方面，哪些應用程式正在消耗我的網路頻寬？
- 哪些應用程式具有病毒、入侵行為和間諜軟體？
- 我的使用者正在存取哪些網站類別？



#	名稱	工作階段		啟動位元組		回應位元組		存取規則封鎖	App 規則封鎖	位置封鎖	BotNet 封鎖	病毒	入侵	間諜軟體
1	Service Version 2 Multicast Listener Re	10.41K	39%	795.07K	7%	0	<1%	10,414	0	0	0	0	0	0
2	General DNS	4.40K	16%	538.58K	4%	1.29M	3%	0	0	0	0	0	0	0
3	DNS Protocol--Standard Query .com Commercial Domains-6818	3.38K	12%	396.43K	3%	908.21K	2%	0	0	0	0	0	0	0
4	General HTTPS	2.13K	8%	2.41M	22%	7.64M	22%	0	0	0	0	0	0	0
5	General TCP	1.74K	6%	2.97M	27%	4.05M	11%	0	0	0	0	0	0	0
6	DNS Protocol--Standard Query A Reverse Lookup-6842	1.69K	6%	141.88K	1%	219.05K	<1%	0	0	0	0	0	0	0
7	General HTTPS MGMT	1.38K	5%	2.39M	21%	19.79M	57%	0	0	0	0	0	0	0
8	General SMTP	682	2%	144.58K	1%	185.16K	<1%	0	0	0	0	0	0	0
9	Service SonicWALL Anti-Spam Service	341	1%	72.34K	<1%	85.59K	<1%	0	0	0	0	0	0	0
10	Service NTP	30	<1%	11.40K	<1%	10.79K	<1%	0	0	0	0	0	0	0
11	Wget--Client Activity-1613	14	<1%	7.45K	<1%	29.09K	<1%	0	0	0	0	0	0	0
12	General HTTP MGMT	10	<1%	9.41K	<1%	153.52K	<1%	0	0	0	0	0	0	0
13	Service RPC Services (IANA)	8	<1%	1.03M	9%	72.86K	<1%	0	0	0	0	0	0	0
14	General HTTP	3	<1%	152	<1%	0	<1%	3	0	0	0	0	0	0
15	Service Echo	1	<1%	48	<1%	0	<1%	0	0	0	0	0	0	0
全部: 15 項目		**26.22K**		**10.92M**		**34.44M**		**10.42K**	**0**	**0**	**0**	**0**	**0**	**0**

報告資料的檢視範圍包括自最後一次系統重新啟動以來、自系統重設以來，或者指定排程範圍。報告可透過 FTP 傳送，也可透過電子郵件傳送。

提示：儀表板 > Appflow 儀表板頁面以圖形格式顯示每種類別（IP 位址除外）的前十個項目。

若要設定 Appflow 報告，請遵循 *SonicWall SonicOS 6.5 記錄和報告*中所述有關**記錄和報告 | Appflow 設定 > 流量報告**的程序。

頁面底部顯示：

- 每欄的總數，例如項目數、啟動者和回應者傳送的位元組數、封鎖的位置數
- 裝置執行的時間總數，格式為天數、小時數、分鐘數和秒數
- 上次更新/重設的時間，格式為小時、分鐘、秒、月、天

主題：

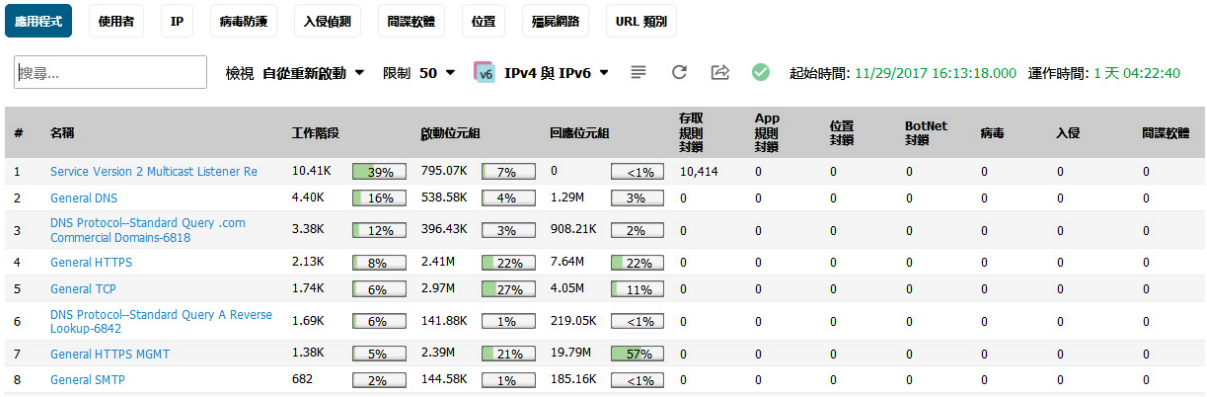
- Appflow 報告
- 通用功能
- 檢視 Appflow 資料
- 下載 Appflow 報告

Appflow 報告

報告 > Appflow 報告頁面會在單獨的檢視上顯示這些報告。按一下按鈕以查看您所要的檢視。

- 應用程式
- 使用者
- IP
- 病毒
- 入侵
- 間諜軟體
- 位置
- 殭屍網路
- URL 類別

應用程式

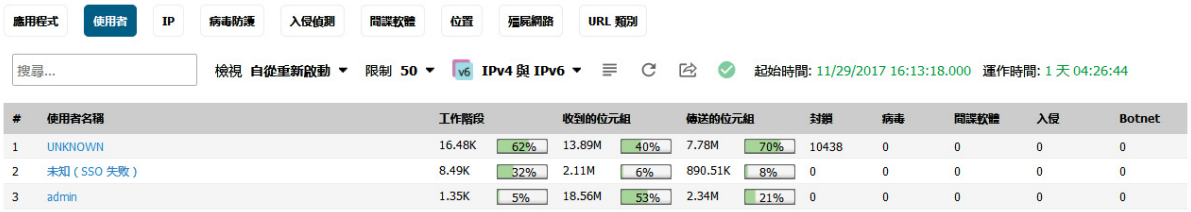


#	名稱	工作階段		啟動位元組		回應位元組		存取規則封鎖	App 規則封鎖	位置封鎖	BotNet 封鎖	病毒	入侵	間諜軟體
1	Service Version 2 Multicast Listener Re	10.41K	39%	795.07K	7%	0	<1%	10,414	0	0	0	0	0	0
2	General DNS	4.40K	16%	538.58K	4%	1.29M	3%	0	0	0	0	0	0	0
3	DNS Protocol--Standard Query .com Commercial Domains-6818	3.38K	12%	396.43K	3%	908.21K	2%	0	0	0	0	0	0	0
4	General HTTPS	2.13K	8%	2.41M	22%	7.64M	22%	0	0	0	0	0	0	0
5	General TCP	1.74K	6%	2.97M	27%	4.05M	11%	0	0	0	0	0	0	0
6	DNS Protocol--Standard Query A Reverse Lookup-6842	1.69K	6%	141.88K	1%	219.05K	<1%	0	0	0	0	0	0	0
7	General HTTPS MGMT	1.38K	5%	2.39M	21%	19.79M	57%	0	0	0	0	0	0	0
8	General SMTP	682	2%	144.58K	1%	185.16K	<1%	0	0	0	0	0	0	0

- **名稱** - 應用程式名稱，簽章 ID
- **工作階段** - 連接/流量的數目，以數字和百分比的形式顯示
- **啟動位元組** - 啟動者傳送的位元組數目，以數字和百分比的形式顯示
- **回應位元組** - 回應者傳送的位元組數目，以數字和百分比的形式顯示
- **存取規則封鎖** - 防火牆規則封鎖的連接/流量數目
- **App 規則封鎖** - DPI 引擎封鎖的連接/流量數目
- **位置封鎖** - GEO 執行封鎖的連接/流量數目

- **BotNet 封鎖** - Botnet 執行封鎖的連接/流量數目
- **病毒** - 帶有病毒的連接/流量數目
- **入侵** - 識別為入侵的連接/流量數目
- **間諜軟體** - 帶有間諜軟體的連接/流量數目

使用者



#	使用者名稱	工作階段		收到的位元組		傳送的位元組		封鎖	病毒	間諜軟體	入侵	Botnet
1	UNKNOWN	16.48K	62%	13.89M	40%	7.78M	70%	10438	0	0	0	0
2	未知 (SSO 失敗)	8.49K	32%	2.11M	6%	890.51K	8%	0	0	0	0	0
3	admin	1.35K	5%	18.56M	53%	2.34M	21%	0	0	0	0	0

- **使用者名稱**
- **工作階段** - 啟動/回應的工作階段/連接的數目，以數字和百分比的形式顯示
- **收到的位元組** - 使用者接收到的位元組數目，以數字和百分比的形式顯示
- **傳送的位元組** - 使用者已傳送的位元組數目，以數字和百分比的形式顯示
- **封鎖** - 封鎖的工作階段/連接數目
- **病毒** - 偵測到帶有病毒的工作階段/連接數目
- **間諜軟體** - 偵測到帶有間諜軟體的工作階段/連接數目
- **入侵** - 偵測為入侵的工作階段/連接數目

IP

#	IP 位址	工作階段		收到的位元組		傳送的位元組		封鎖	病毒	間諜軟體	入侵	Botnet
1	192.168.148.252	10.54K	20%	4.36M	9%	6.05M	13%	0	0	0	0	0
2	ff02::16	10.44K	19%	797.12K	1%	0	<1%	10441	0	0	0	0
3	fe80::bd67:dbe7:880b:5d9c	9.71K	18%	0	<1%	738.11K	1%	9712	0	0	0	0
4	192.168.94.181	8.48K	16%	883.35K	1%	2.09M	4%	0	0	0	0	0
5	192.168.95.64	2.50K	4%	4.78M	10%	12.78M	27%	3	0	0	0	0
6	192.168.94.64	2.45K	4%	4.28M	9%	3.60M	7%	0	0	0	0	0
7	192.168.94.188	2.42K	4%	3.13M	6%	4.25M	9%	0	0	0	0	0
8	192.168.148.64	2.04K	3%	5.15M	11%	2.24M	4%	0	0	0	0	0
9	192.168.95.233	996	1%	11.25M	24%	1.74M	3%	0	0	0	0	0
10	192.168.95.1	979	1%	193.26K	<1%	334.21K	<1%	0	0	0	0	0
11	fe80::4df1:822f:3f4c:adf8	729	1%	0	<1%	58.78K	<1%	729	0	0	0	0

- **IP 位址**
- **工作階段** - 啟動/回應的工作階段/連接的數目，以數字和百分比的形式顯示
- **收到的位元組** - 此 IP 位址接收到的位元組數目，以數字和百分比的形式顯示
- **傳送的位元組** - 此 IP 位址已傳送的位元組數目，以數字和百分比的形式顯示

- **封鎖** - 封鎖的工作階段/連接數目
- **病毒** - 偵測到帶有病毒的工作階段/連接數目
- **間諜軟體** - 偵測到帶有間諜軟體的工作階段/連接數目
- **入侵** - 偵測為入侵的工作階段/連接數目

病毒

- **病毒名稱**
- **工作階段** - 帶有此病毒的工作階段/連接數目

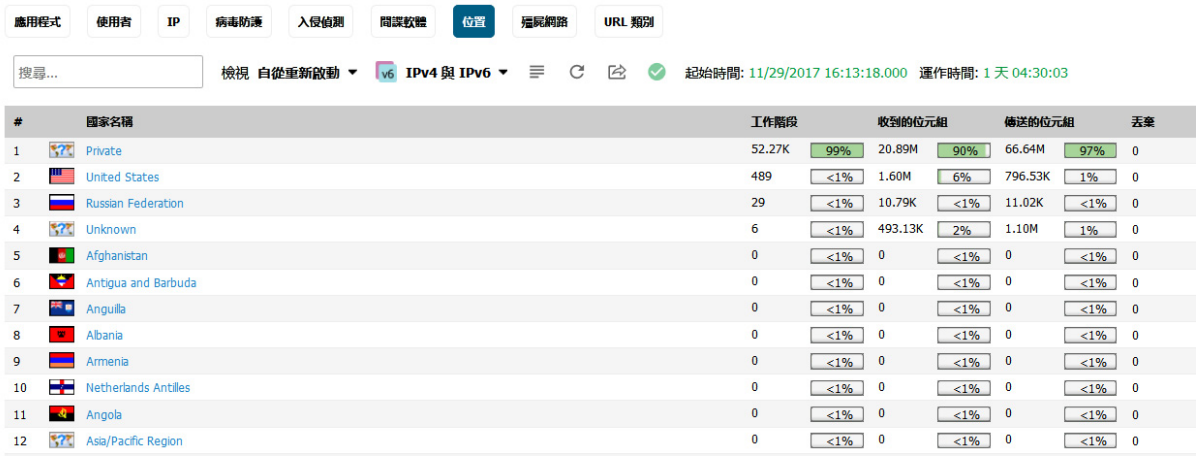
入侵

- **入侵名稱**
- **工作階段** - 偵測為入侵的工作階段/連接數目

間諜軟體

- **間諜軟體名稱** - 間諜軟體簽章的名稱
- **工作階段** - 帶有此間諜軟體的工作階段/連接數目

位置



#	國家名稱	工作階段		收到的位元組		傳送的位元組		丟棄
1	Private	52.27K	99%	20.89M	90%	66.64M	97%	0
2	United States	489	<1%	1.60M	6%	796.53K	1%	0
3	Russian Federation	29	<1%	10.79K	<1%	11.02K	<1%	0
4	Unknown	6	<1%	493.13K	2%	1.10M	1%	0
5	Afghanistan	0	<1%	0	<1%	0	<1%	0
6	Antigua and Barbuda	0	<1%	0	<1%	0	<1%	0
7	Anguilla	0	<1%	0	<1%	0	<1%	0
8	Albania	0	<1%	0	<1%	0	<1%	0
9	Armenia	0	<1%	0	<1%	0	<1%	0
10	Netherlands Antilles	0	<1%	0	<1%	0	<1%	0
11	Angola	0	<1%	0	<1%	0	<1%	0
12	Asia/Pacific Region	0	<1%	0	<1%	0	<1%	0

- **國家名稱** - 啟動/回應工作階段/連接的國家或地區的名稱和旗幟
- **工作階段** - 由此國家或地區啟動/回應的工作階段/連接數目，以數字和百分比的形式顯示
- **收到的位元組** - 由此國家或地區接收到的資料位元組數目，以數字和百分比的形式顯示
- **傳送的位元組** - 由此國家或地區已傳送的資料位元組數目，以數字和百分比的形式顯示
- **丟棄** - 已丟棄的工作階段/連接數目

殭屍網路

#	Botnet 名稱	工作階段
1	Botnet Detected	0
2	Botnet Blocked	0

- **Botnet 名稱**：
  - **Botnet Detected**
  - **Botnet Blocked**
- **工作階段** - 偵測到/已封鎖 botnet 的工作階段/連接數目

URL 類別

- **類別名稱** - URL 類別的名稱
- **工作階段** - 工作階段/連接的數目，以數字和百分比的形式顯示

通用功能

以下功能通用於所有標籤：

- 指定資料來源
- 下載 SonicWall 安全服務簽章
- 限制顯示的項目數
- 建立 CSV 檔案

指定資料來源

可以在**資料來源**下拉功能表中選擇報告資料的來源：

- **本機**（預設值）
- **Appflow 伺服器**（如果可用）
- **GMSFlow 伺服器**（如果可用）

下載 SonicWall 安全服務簽章

Appflow 報告功能需要您啟用最新的 SonicWall 安全服務簽章下載。如此您可擁有最新的動態防護更新。

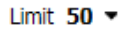
按一下任何標籤上的**狀態**圖示以檢視啟用的 SonicWall 安全服務清單（如下圖所示）。

此快顯視窗會為產生 AppFlow 報告的每個服務顯示以下內容：

- 服務是否已授權、未授權或授權無法使用（不適用）
- 服務是否已啟用、已停用或無法使用
- 相關資料庫是否已從服務下載或無法使用
- 指向相關 SonicWall 頁面的連結，用於設定服務

限制顯示的項目數

從**限制**下拉功能表中選擇其中一個數字，可以限制報告中顯示的項目數：



- **10**
- **25**
- **50**（預設值）
- **100**
- **150**
- 無限制

附註：位置、**Botnet** 和 **URL 評等**報告中的項目數不能限制。

建立 CSV 檔案

按一下**匯出**圖示可以特定檢視的 CVS 檔案。

檢視 Appflow 資料

在**檢視**下拉功能表中，您可以選擇 Appflow 資料的檢視：

自從重新啟動顯示自從上次重新開機或重新啟動防火牆後的 Appflow 資料。重新啟動的日期和時間以及自重新啟動以來的執行時間總數（格式為天數、小時數、分鐘數以及秒數）顯示為綠色。例如，起始時間：08/14/2014 15:40:06.000 運作時間：32 天 01:25:10

提示：這個執行時間與最近一次更新的日期和時間也一起顯示在此頁面底部。

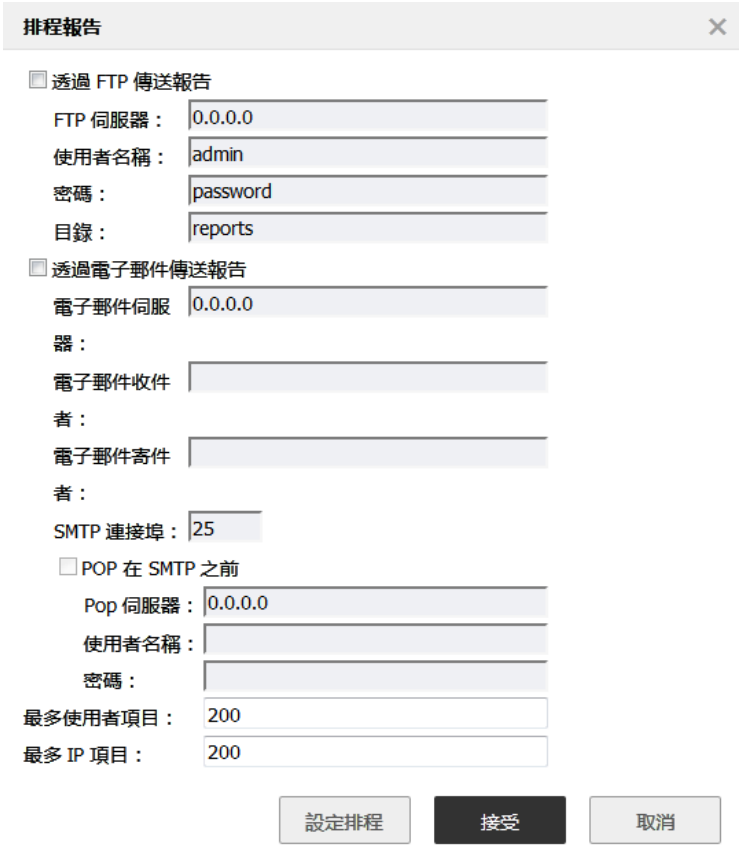
「自從上次重設」顯示自從上次重設防火牆後的 Appflow 資料。此報告顯示自您最後一次透過按**重設**按鈕清除統計資料以來的彙總統計資料。重設的日期和時間以及自重設以來的執行時間總數（格式為天數、小時數、分鐘數以及秒數）顯示為綠色。

重設選項使得您可以透過重設網路流量來快速檢視 Appflow 報告統計資料。重設將會清除頁面底部的計數器，其中顯示了工作階段總數、啟動者和回應者位元組總數，以及入侵和威脅總數等。

排程顯示依照定義的排程開始和結束時間顯示 Appflow 資料。此報告顯示在設定選項所指定的時間範圍內收集到的 Appflow 統計資料。到達排程的結束時間後，排程的 Appflow 統計資料將會自動匯出到 FTP 伺服器或電子郵件伺服器。Appflow 統計資料將會匯出為 CSV 檔案格式。匯出 Appflow 統計資料後，將會重新整理和清除這些資料。

若要設定排程 Appflow 報告：

1. 在**調查**檢視上，導覽至**報告 | Appflow 報告**。
2. 在**檢視**欄位中，選擇**排程**。
3. 按一下**設定**。



4 勾選方塊以自動傳送您的 Appflow 報告，使用一個或兩個選項：

- **透過 FTP 傳送報告**
- **透過電子郵件傳送報告**

5 若要透過 FTP 傳送報告，請設定以下選項：

a 在 **FTP 伺服器**欄位中輸入 FTP 伺服器位址。

b 在**使用者名稱**欄位中輸入使用者名稱，預設值是 **admin**。

c 在**密碼**欄位中輸入密碼。

d 在**目錄**欄位中輸入報告要傳送的目的地目錄。預設為 **reports**。

6 若要透過電子郵件傳送報告，請輸入以下這些選項：

a 在**電子郵件伺服器**欄位中輸入電子郵件伺服器。

b 在**電子郵件收件者**欄位中輸入收件者的電子郵件地址。

c 在**寄件者電子郵件地址**欄位中輸入發件人使用的電子郵件地址。

d 在 **SMTP 連接埠**欄位中新增 SMTP 連接埠編號。

7 如果您的電子郵件伺服器需要 SMTP 驗證，請勾選**在 SMTP 之前接收 POP** 核取方塊，並輸入以下選項：

- 在 **POP 伺服器**欄位中輸入 POP 伺服器的位址。
- 在**使用者名稱**欄位中輸入使用者名稱。
- 在**密碼**欄位中輸入密碼。

8 在**最多使用者項目**欄位中輸入使用者項目的最大數值，預設值是 **200**。

9 在**最多 IP 項目**欄位中輸入 IP 項目的最大數值，預設值是 **200**。

10 按一下**設定排程**按鈕以定義開始和結束排程。

11 在**排程名稱**欄位中輸入名稱。

12 在**排程類型**中，選擇：

- **單次**會建立單次排程。**單次**排程選項用於基於日曆開始日期和結束日期（包括以小時和分鐘表示的時間）設定報告排程。
- **重複**會建立持續性排程。**重複**排程選項允許基於星期以及開始和結束時間目的地（小時和分鐘）來選擇持續性排程。
- **混合**會同時建立單次排程和持續性排程。

  重複排程和**混合**排程將在**排程清單**中顯示您的選擇。

13 如果選擇**重複**或**混合**作為排程類型，則請完成以下排程時間：

- 指定排程的**天數**、**開始時間**和**結束時間**。
- 若排程類型為**混合**，在**單次**部分，為報告的**開始**和**結束**指定**年**、**月**、**日**、**小時**和**分鐘**。

14 按一下**確定**以儲存您的 AppFlow 報告排程。

15 在**排程報告**選項頁面中，按一下**套用**按鈕，開始使用您的 Appflow 報告排程物件設定。

下載 Appflow 報告

可將 Appflow 報告下載為以下其中一種格式：

- **CSV** (Microsoft Excel Comma Separated Values File) - 下載為 swarm.csv 檔案在 Excel 中打開

  ⓘ **附註：**此 CSV 檔案不同於按一下**建立 CSV 檔案**圖示所產生的 CSV 檔案。

- **DOC** (Microsoft Word Document) - 下載為 swarm.docx 檔案在 Word 中打開
- **PDF** - 在瀏覽器視窗中打開為 html 檔案

若要下載報告：

1 在**調查**檢視上，導覽至**報告 | Appflow 報告**。

2 按一下**傳送報告**圖示。

3 按一下**下載報告**按鈕。隨即顯示**開啟 *file*.wri.sfr** 視窗。

4 按一下**儲存**至儲存檔案。檔案已下載到您的 Downloads 資料夾。

5 打開瀏覽器視窗。

6 登入到 **mysonicwall.com**。

7 導覽至 **SW 工具 > App 報告**。此時顯示**上載報告**頁面。

8 按一下**瀏覽器**按鈕。隨即顯示**檔案上載**視窗。

9 找到檔案並按一下**開啟**。檔案名稱出現在**上載報告**頁面。

10 按一下**上載**按鈕。上載報告可能需要花費幾分鐘時間。

11 上載完成後，可以選擇以下任一或全部格式（檔案名稱為 **swarm**）：

- **CSV**
- **DOC**
- **PDF**

7

記錄報告

附註：記錄 > 報告頁面不適用於 SuperMassive 9800。

防火牆可以對事件記錄執行捲動分析，以顯示 25 個最常存取的網站、按 IP 位址消耗頻寬最多的前 25 個使用者和消耗最多頻寬的 25 項服務。您可以從**記錄 > 報告**頁面產生這些報告。

附註：SonicWall Analyzer 為防火牆提供全面的 Web 報告解決方案。如需 SonicWall Analyzer 的更多資訊，請移至http://www.sonicwall.com。

主題：

資料收集

調查檢視上的**報告 | 記錄報告**頁面包括以下功能：

- 資料收集

  按一下**開始資料收集**開始記錄分析。啟用記錄分析時，按鈕標籤變更為**停止資料收集**。

- 檢視資料

  按一下**重設資料**清除報告統計並開始新的採樣期間。資料收集停止或開始時，以及在防火牆重新啟動時，也重設採樣期間。

檢視資料

從**報告檢視**功能表選擇所需的報告。選項有**網站叫用次數**、**按 IP 位址判斷頻寬使用率**和**按服務判斷頻寬使用率**。這些報告的解釋如下。按一下**重新整理資料**更新報告。按一下「重設資料」以重設報告期間。按報告分析的時間長度顯示在**目前採樣期間**中。

網站叫用次數

從**報告檢視**功能表中選擇**網站叫用次數**可顯示包含 25 個最常存取網站的 URL 和目前採樣期間內某網站叫用次數的表格。

網站叫用次數報告確保大多數 Web 存取都是針對合適的網站。如果「網站叫用次數」報告中顯示娛樂、體育或其他不當網站，您可以選擇封鎖這些站台。如需封鎖不當網站的資訊，請參閱 *SonicWall SonicOS 6.5 安全設定*中「安全設定 | 安全服務 > 內容篩選」命令。

按 IP 位址判斷頻寬使用率

從**報告檢視**功能表中選擇**按 IP 位址判斷頻寬使用率**可顯示包含前 25 個網際網路頻寬使用者的 IP 位址和在目前採樣期間傳送的兆位元組數的表格。

按服務判斷頻寬使用率

從**報告檢視**功能表中選擇**按服務判斷頻寬使用率**可顯示包含前 25 個網際網路服務（HTTP、FTP、RealAudio 等）的名稱以及在目前採樣期間從服務接收的兆位元組數的表格。

按服務判斷頻寬使用率報告顯示使用的服務是否適合您的組織。如果視訊或推送廣播等服務消耗一大部分的可用頻寬，您可以封鎖這些服務。

8

使用 RF 分析

本章節說明了如何使用 SonicWall SonicOS 中的 RF 分析功能，以便最大程度地借助無線存取點裝置來使用無線頻寬。

主題：

RF 分析概述

RF 分析功能可幫助無線網路管理員理解管理的 SonicWall 存取點和所有其他相鄰無線存取點如何使用無線頻道。

附註：SonicWall RF 分析可分析供應商存取點，並將這些統計包含在 RF 資料中（只要通過 SonicWall 防火牆顯示和管理的至少一個 SonicWall 存取點）。

選擇 RF 分析

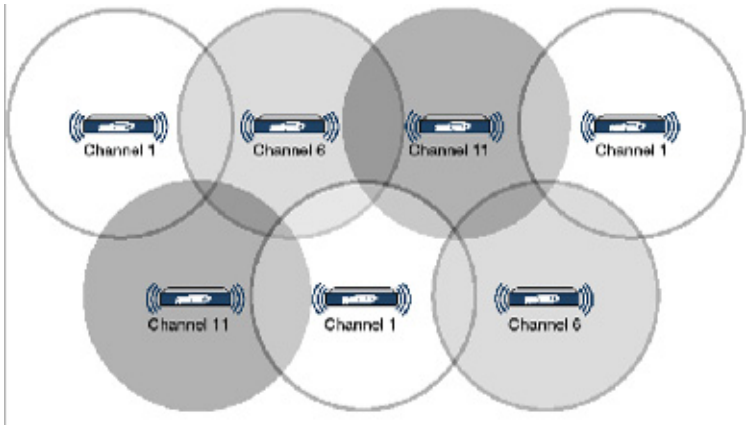
部署和維護無線基礎結構對於網路管理員而言是一項艱巨的任務。效能較低、連接性較差等無線問題是無線網路管理員經常遇到的問題，但這些問題通常只需分析並正確調整無線設定即可解決。

RFA 工具對於這些潛在的無線問題有感知能力。RFA 解決的兩個主要問題是超負荷頻道和受到相鄰頻道干擾的 SonicWall 存取點。RF 分析會計算每個執行的 存取點的 RF 評分，並通過用於在較差的 RF 環境中識別執行的存取點的方式顯示資料。

RF 環境

IEEE 802.11 指定了此裝置使用 ISM 2.4 GHz 和 5GHz 波段，且大多數目前部署的無線裝置使用 2.4 GHz 波段。由於每個頻道佔用了 20MHz 寬的光譜，可用的 11 個頻道中只有 3 個頻道不重疊。在美國，頻道 1、6 和 11 不重疊。大多數情況下，部署大量 SonicWall 存取點時使用這三個頻道。

SonicPoint 手動選擇頻道



整個 2.4GHz 波段劃分為三個單獨的頻道 1、6 和 11。若要達到此理想情況，需要兩個方面：頻道指派和電源調整。在大多數情況下，最好將相鄰的 SonicPoints 指派給不同的頻道。還應仔細監視 SonicPoint 傳送功率，因為此功率必須足夠大才能連接相鄰的用戶端，否則可能會對相同頻道中正在執行的其他 SonicPoint 產生干擾。

對 SonicWall 存取點使用 RF 分析

RF 分析使用評分、圖形和數字幫助使用者發現和識別潛在的或現有的無線問題。

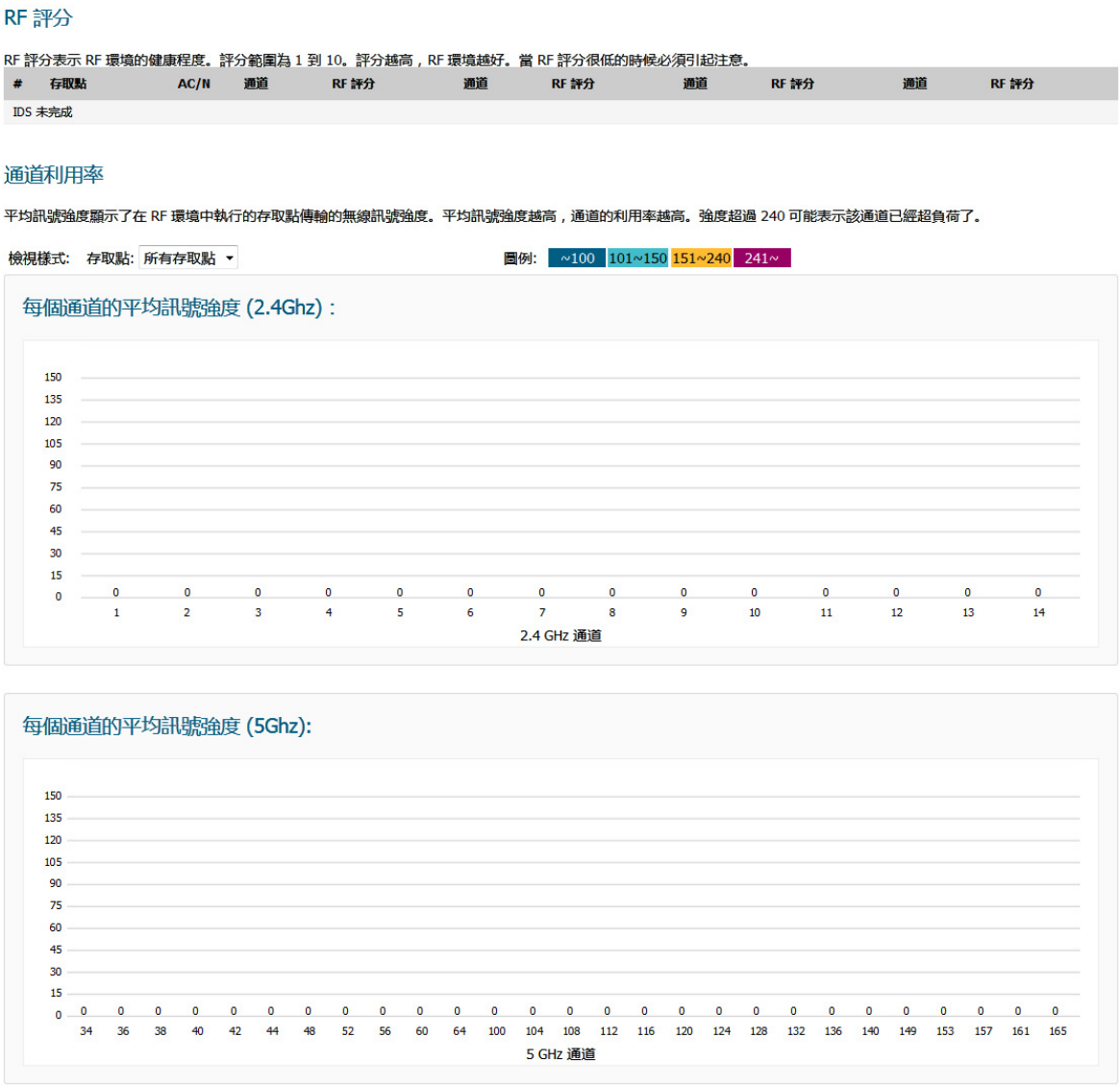
儘管最佳方案的情形是在給定的時間內同一個頻道內執行最少數量的存取點，但實際上很難達到此目的地，尤其是在部署大量存取點時。同樣，由於 ISM 波段對於公眾是免費的，該波段中可能有不受您控制的其他裝置正在執行中。

主題：

- 頻道利用率圖形和資訊
- 理解 RF 評分
- 查看超負荷的頻道
- RFA 嚴重干擾的頻道

頻道利用率圖形和資訊

在尋找如何對所有連接的 SonicPoints 利用頻道的顯示方法時，得出了以下的頻道利用率顯示圖：



每個頻道顯示兩個彩色列。每個彩色條頂部的數字指示偵測此頻道指定問題的 SonicWall 存取點的數量。SonicWall 存取點在啟動時對所有可用頻道執行 IDS 掃描，並由 RF 分析來分析這些結果，以確定每個頻道上的問題。

例如：如果連接了 10 個 SonicWall 存取點，其中的 6 個確定頻道 11 超負荷，則紫色列頂部的數字將為 6；如果 8 個 SonicWall 存取點確定頻道 6 受到嚴重干擾，則青色列頂部的數字將為 8。對頻道顯示零值表示沒有問題。

附註：顯示了頻道 12、13、14，但在某些國家和地區，不使用這些頻道。但仍會監控這些頻道，因為無線 cracker 會在頻道 12、13 或 14 上設定無線發射機，並對較低的頻道啟動拒絕服務攻擊。

理解 RF 評分

RF 評分是在 1-10 的比例上計算的分數，用於表示頻道的整體狀況。分數越高，RF 環境越好。分數低表明需要多加注意。

SonicWall 無線驅動程式在 RSSI 中報告訊號強度，此數字用在初步 RF 評分的方程式中可得到 1 到 100 的原始比例分數：

rfaScore100 = 100-((rssiTotal-50)*7/10))

簡化為：*rfaScore100* = -0.7*rssiTotal + 135;

最終的分數基於此 *rfaScore100*：

- 如果 RFA 分數高於 96，則將報告為 10。
- 如果 RFA 分數低於 15，則將其報告為 1。
- 所有其他分數都除以 10，以得到 1-10 的比例。

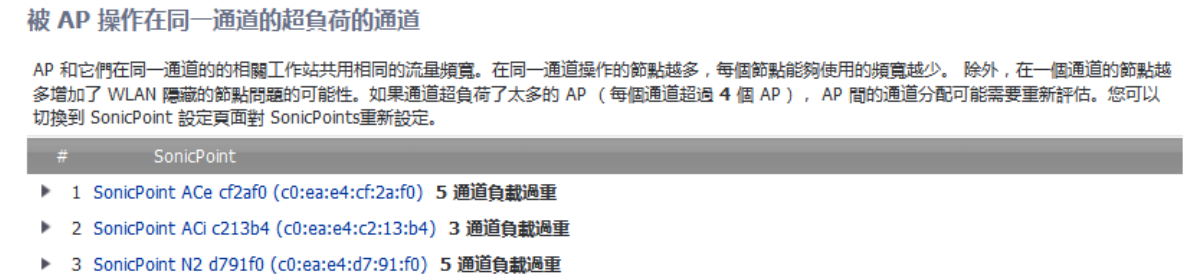
在 SonicOS 介面中，將顯示 SonicWall 存取點所使用的頻道的 RF 評分。

附註：此功能取決於 SonicPoint 在其中執行的頻道，如果頻道編號未知，RF 評分將無法使用。

查看超負荷的頻道

如果在同一個頻道中偵測到四個使用中的存取點，RF 分析將發出警告。無論它們的訊號強度如何，RF 分析都會將頻道標記為超負荷：

超負荷的頻道



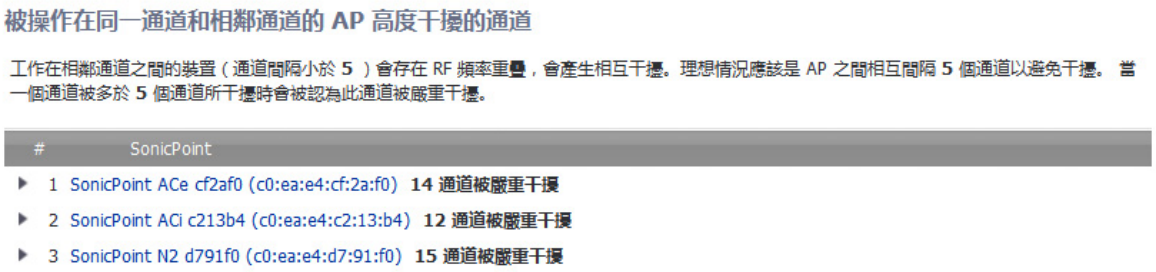
關於每個已發現存取點的資訊，包括：SSID、MAC、訊號強度和頻道。訊號強度顯示為兩個值：dBm 和百分比值。

RFA 嚴重干擾的頻道

同一個頻道中執行的存取點會產生干擾，相鄰頻道執行的存取點（頻道編號之差小於 5）也會相互干擾。

如果偵測到附近存在某個 SonicPoint，RFA 將發出警告，頻道編號之差小於 5 的頻道之間存在 5 個以上的使用中存取點。無論它們的訊號強度如何，RFA 都會將頻道標記為嚴重干擾。

嚴重干擾的頻道



關於每個已發現的存取點的資訊包括：SSID、MAC、訊號強度和頻道。訊號強度顯示為兩個值：dBm 和百分比值。

9

TCP 加速報告

調查檢視上的**報告 > TCP 加速**提供了用於檢視和監控 TCP 加速服務的選項。本章節詳述**統計**、**統計資料分解**和**連線**選項的管理介面功能。

主題：

統計資料選項

在**調查**檢視導覽到**報告 | TCP 加速報告>統計**，以選擇環境中的 WAN 加速器資料。「統計」選項會顯示圖形說明下列項目：

- 摘要
- 由 WXA 分解
- 時間序列
- 連線

若要為「統計」檢視設定報告：

1 在**顯示**欄位中，設定要顯示資料的選項。從下列項目中選擇：

- 全部
- **對於群組:**
- **對於WXA:**

如果您選擇了**對於群組:**或**對於 WXA:**，並且顯示其他欄位，這樣的話您可以進一步精簡您的選擇。

2 在**涵蓋期間**欄位中，選擇資料顯示在「統計」標籤上的時間段。選項包括：

- 最近小時數
- 最近 24 小時

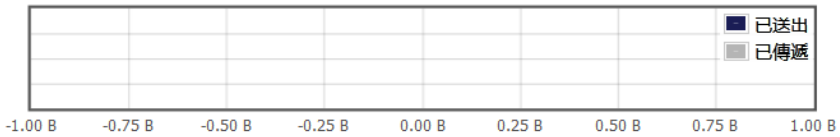
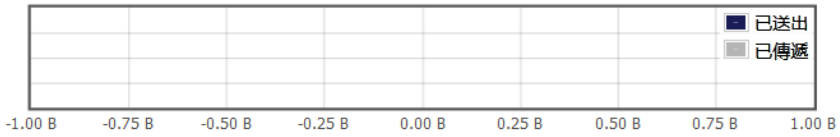
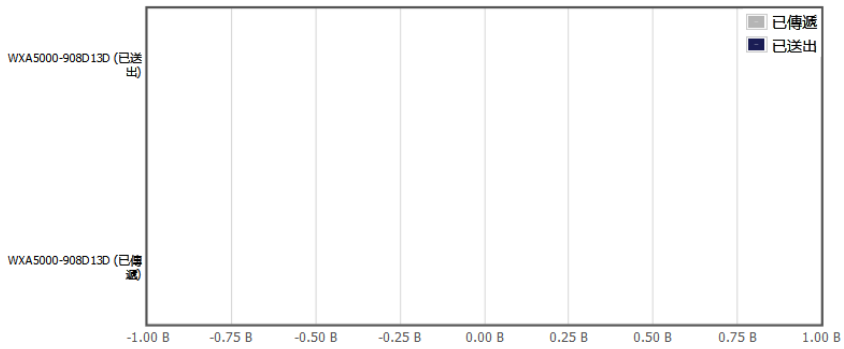
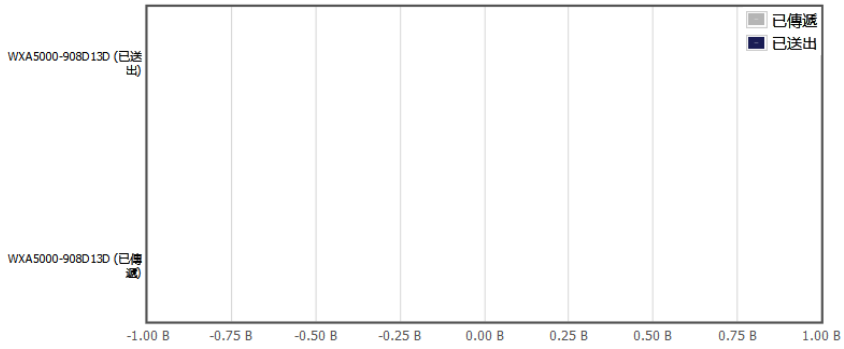
- 最近 3 天
- 最近 5 天
- 最近 10 天
- 最近 30 天

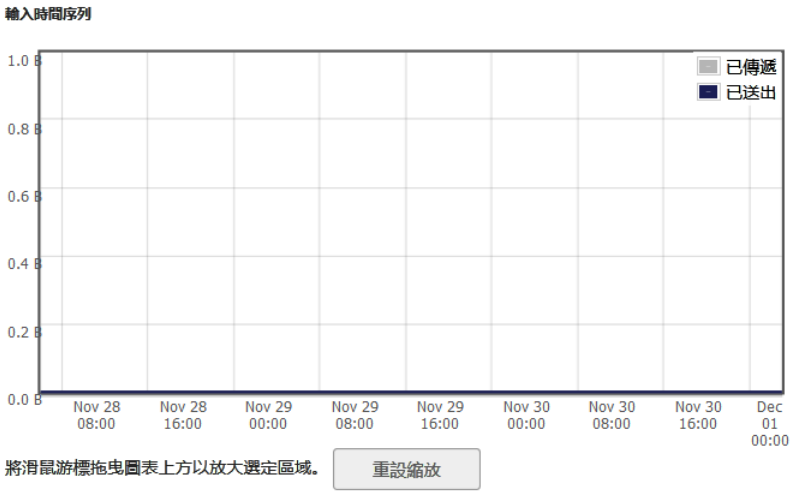
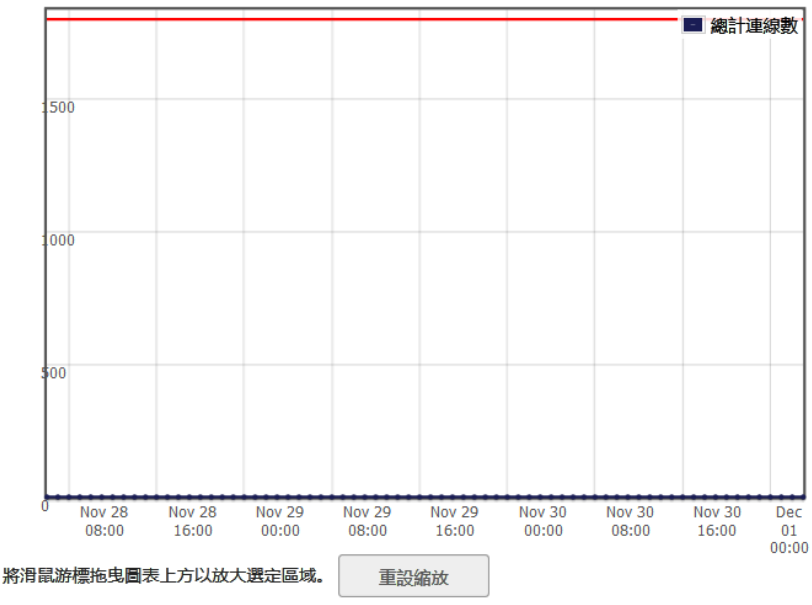
3 按一下**重新整理**圖示以重新整理將顯示的資料。

4 在**所選 WXA 的資料**部分，按下箭號可最小化或展開 WXA 清單。向左箭頭表示最小化的畫面，向下箭頭表示展開的畫面。

頁面的剩餘部分顯示與所選選項相關的資料。第一個部分是資料表**顯示所有可用 WXA 的資料針對最近 30 天**。它包含像是「所有資料減少」、「WAN 容量增量因素」「新連線」、「關閉的連線」和「尖峰連線」的輸出和輸入資料。

頁面底部以圖形顯示相關資訊。您可以透過選擇資料表下的按鈕之一，來變更圖形檢視。

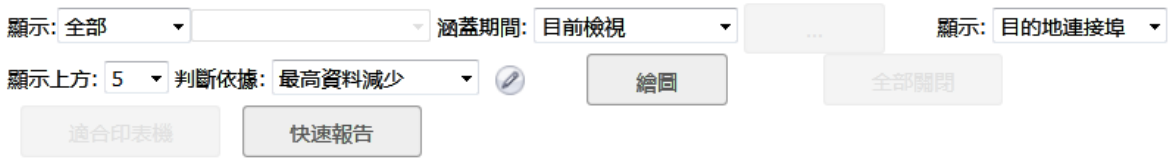
名稱	說明
摘要	輸出  輸入 
由 WXA 分解	輸出  輸入 

名稱	說明
時間序列	 
連線	

在**時間序列**報告和**連接**報告上，您可以放大特定資料集。只要使用滑鼠沿著您要放大的區段拉出一個方形，按一下**重設縮放**，即可重設圖形至其原始檢視。

分析統計資料

您可以使用「分解統計資料」檢視，根據特定欄位定義產生 TCP 加速報告。



名稱	說明
顯示	從**顯示**功能表，選擇您要顯示的資料類型： • 全部 • **對於群組** • **對於 WXA:** 如果選擇**對於群組**或**對於 WXA**，會顯示其他欄位。從下拉功能表中的選項選擇，以進一步精簡您的資料。
涵蓋期間	選擇資料顯示在「統計」標籤上的時間段。選項包括： • **最近小時數** • **最近 24 小時** • **最近 3 天** • **最近 5 天** • **最近 10 天** • **最近 30 天**
顯示器	選擇用於將顯示在圖表中的資料的欄位。**顯示**功能表選項為： **目的地連接埠** - 顯示相較於加速連線的目的地連接埠數量的資料量。 **目的地位址** - 顯示相較於加速 TCP 連線的目的地 IP 位址的資料量。 **來源位址** - 顯示相較於加速 TCP 連線的來源 IP 位址的資料量。 **位址** - 顯示相較於加速 TCP 連線的 WAN 上的目的地位址的資料量。 **WAN 上的位址** - 顯示相較於加速 TCP 連線的 LAN 上目的地位址的資料量。連線可由 LAN 或 WAN 上的電腦起始。
顯示上方	選擇要在圖形中顯示多少個連接埠或 IP 位址。選項為 **3**、**5**、**10**和 **15**。
判斷依據	選取顯示在圖形中的條件。選項包括： • 最高資料減少 • 最少資料減少 • 大多數資料已送出 • 大多數資料已傳遞 • 最高 # 連線

名稱	說明
繪圖	以圖形顯示所選擇的條件。
快速報告	 可讓選擇的選項用於產生報告，並可在畫面上檢視和傳送到印表機。

連線

在**調查**檢視上，導覽到**報告 | TCP 加速報告 > 連線**，以查看 TCP 加速連線結果的詳細清單。此報告會顯示資訊，例如開始和結束時間戳記、來源 IP 位址以及目的地 IP 位址和連接埠。使用這些結果來監控 TCP 加速服務的效能。

名稱	說明
顯示	從**顯示**功能表，選擇您要顯示的資料類型： • **全部** • **對於群組** • **對於 WXA:** 如果選擇**對於群組**或**對於 WXA**，會顯示其他欄位。從下拉功能表中的選項選擇，以進一步精簡您的資料。
每個 WXA 的項目上限	選擇要顯示在「連線」表格中的項目數量。
句含非截獲的	啟用或停用包含非截獲的流量，以顯示在「連線」表格中。「非截獲」的定義是衍生自防火牆到 WXA 設備的流量，但是不會加速。
「**重新整理**」按鈕	每當您變更條件時，即更新顯示的資料。
略過	按一下**連線**按鈕，以開啟顯示未加速連線清單的視窗，因為其資料不會壓縮或者遠端節點 WXA 不回應。 按一下**略過統計資料**圖示以查看略過資料： 

以下定義資料表的欄位標題。

名稱	說明
開始時間	指出連線的開始時間。
結束時間	指出連線的結束時間。
啟動者	顯示網路的哪一端起始連線。連線用的 LAN 會從本機開始，連線用的 WAN 則從遠端開始。
遠端節點	顯示在連線遠端的 WXA 系列裝置。
來源 IP	顯示器連線開始的 IP 位址。
來源連接埠	顯示發出連線要求的連接埠號。
目的 IP	顯示目的地 IP 位址。
目的連接埠	顯示目的地連接埠號。
輸出	顯示代表網路上傳出流量的條形圖。藍色列是已傳送的流量，灰色列是傳遞的流量。
輸入	顯示代表網路上傳入流量的條形圖。藍色列是已傳送的流量，灰色列是傳遞的流量
篩選條件	從下拉清單中選擇，以及在適當的輸入方塊中輸入文字，來篩選結果。可對欄位的組合進行篩選。

10

WFS 加速報告

本章節說明在**調查**檢視的**報告 | WFS 加速報告**中可供使用的管理介面功能和選項。

主題：

統計

在**調查**檢視導覽到**報告|WFS 加速報告>統計**，以選擇環境中的 WAN 加速器資料。「統計」選項會顯示圖形說明下列項目：

- 摘要
- 由 WXA 分解
- 時間序列

統計標籤顯示 WFS 加速服務的效能統計資料。

若要為「統計」檢視設定報告：

1 在**顯示**欄位中，設定要顯示資料的選項。從下列項目中選擇：

- **全部**
- **對於群組:**
- **對於WXA:**

如果您選擇了**對於群組:**或**對於 WXA:**，並且顯示其他欄位，這樣的話您可以進一步精簡您的選擇。

2 在**涵蓋期間**欄位中，選擇資料顯示在「統計」標籤上的時間段。選項包括：

- **最近小時數**
- **最近 24 小時**
- **最近 3 天**
- **最近 5 天**
- **最近 10 天**
- **最近 30 天**

3 在下一個**顯示**欄位中，從下拉功能表選擇以下選項之一：

- **僅延伸支援結果**
- **排除延伸支援的結果**
- **所有結果**

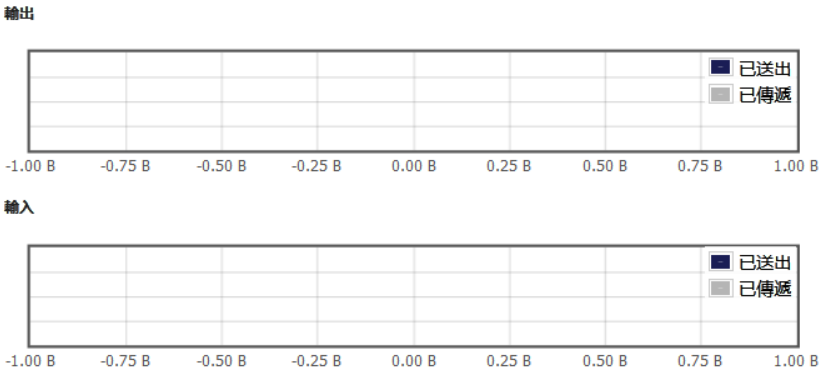
4 按一下**重新整理**圖示，以目前選擇的條件重新整理表格資料。

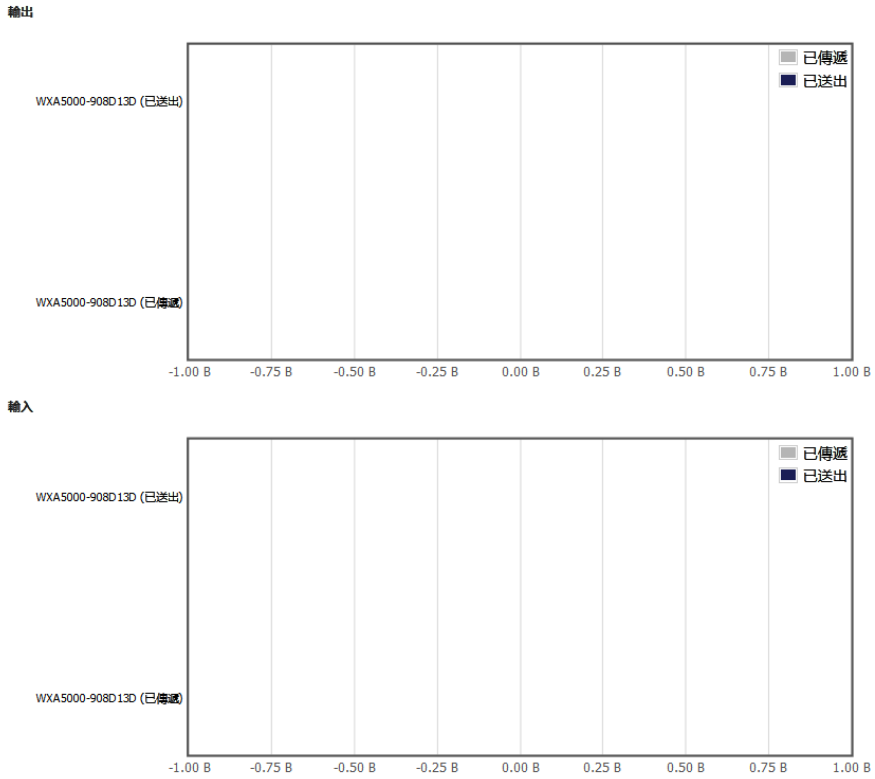
5 按一下「略過」按鈕以略過資料。

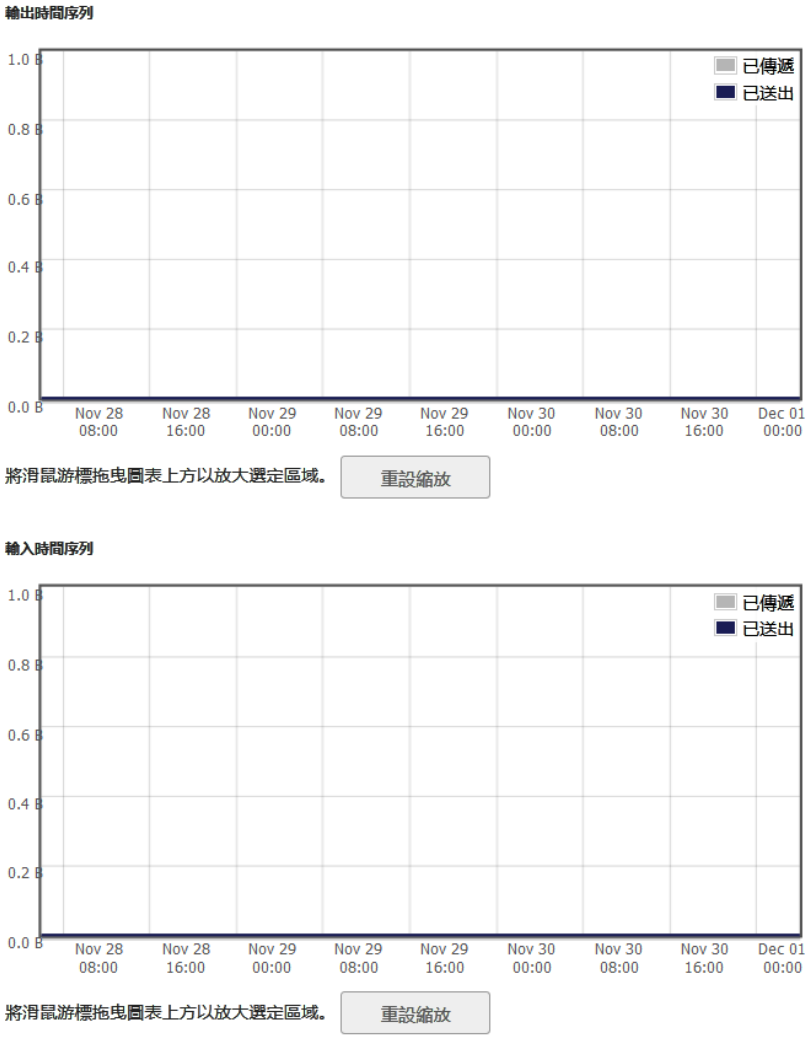
6 在**所選 WXA 的資料**部分，按下箭號可最小化或展開 WXA 清單。向左箭頭表示最小化的畫面，向下箭頭表示展開的畫面。

頁面的剩餘部分顯示與所選選項相關的資料。第一個部分是資料表**顯示所有可用 WXA 的資料針對最近 30 天**。它包含像是「所有資料減少」和「WAN 容量增量因素」的輸出和輸入資料。

頁面底部以圖形顯示相關資訊。您可以透過選擇資料表下的按鈕之一，來變更圖形檢視。

名稱	說明
摘要	顯示兩個條形圖，各代表網路上實際時間段的**傳送**或傳出流量和**已傳遞**或傳入流量。藍色列 (輸出) 是傳出或已傳送資料，而灰色列 (輸入) 是傳入資料。**傳送**指的是資料實際透過連線所傳送的量。**已傳遞**指的是所有已透過連線傳送的資料或資訊。 

名稱	說明
由 WXA 分解	 輸出 已傳遞 已送出 WXA5000-908D13D (已送出) WXA5000-908D13D (已傳遞) -1.00 B -0.75 B -0.50 B -0.25 B 0.00 B 0.25 B 0.50 B 0.75 B 1.00 B 輸入 已傳遞 已送出 WXA5000-908D13D (已送出) WXA5000-908D13D (已傳遞) -1.00 B -0.75 B -0.50 B -0.25 B 0.00 B 0.25 B 0.50 B 0.75 B 1.00 B

名稱	說明
時間序列	

連線

在**調查**檢視上，導覽到**報告 | WFS 加速報告 > 連線**，以查看 WFS 加速連線結果的詳細清單。使用這些結果來監控 WFS 加速服務的效能。

名稱	說明
顯示	從**顯示**功能表，選擇您要顯示的資料類型： • **全部** • **對於群組** • **對於 WXA:** 如果選擇**對於群組**或**對於 WXA**，會顯示其他欄位。從下拉功能表中的選項選擇，以進一步精簡您的資料。
每個 WXA 的項目上限	選擇要顯示在「連線」表格中的項目數量。
包含非截獲的	啟用或停用包含非截獲的流量，以顯示在「連線」表格中。「非截獲」的定義是衍生自防火牆到 WXA 設備的流量，但是不會加速。
「**重新整理**」按鈕	每當您變更條件時，即更新顯示的資料。
略過	按一下**連線**按鈕，以開啟顯示未加速連線清單的視窗，因為其資料不會壓縮或者遠端節點 WXA 不回應。 按一下**略過統計資料**圖示以查看略過資料： 
編輯圖示	按一下以定義「略過設定」選項。 **附註：**略過設定會影響 TCP 和 WFS 加速。 

11

WXA Web 快取報告

調查檢視上的**報告 | WXA Web 快取報告**提供調查 Web 快取服務的統計資料。

主題：

統計

在**調查**檢視導覽到**報告 | WXA Web 快取報告>統計**，以選擇環境中的 WAN 加速器資料。「統計」選項會顯示圖形說明下列項目：

- 摘要
- 由 WXA 分解
- 時間序列
- 請求

若要為「統計」檢視設定報告：

1 在**顯示**欄位中，設定要顯示資料的選項。從下列項目中選擇：

- 全部
- **對於群組:**
- **對於WXA:**

如果您選擇了**對於群組:**或**對於 WXA:**，並且顯示其他欄位，這樣的話您可以進一步精簡您的選擇。

2 在**涵蓋期間**欄位中，選擇資料顯示在「統計」標籤上的時間段。選項包括：

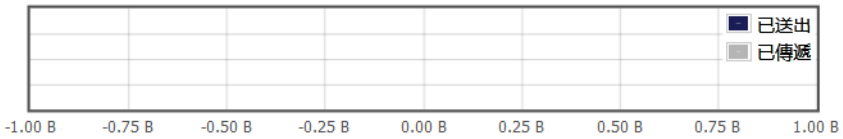
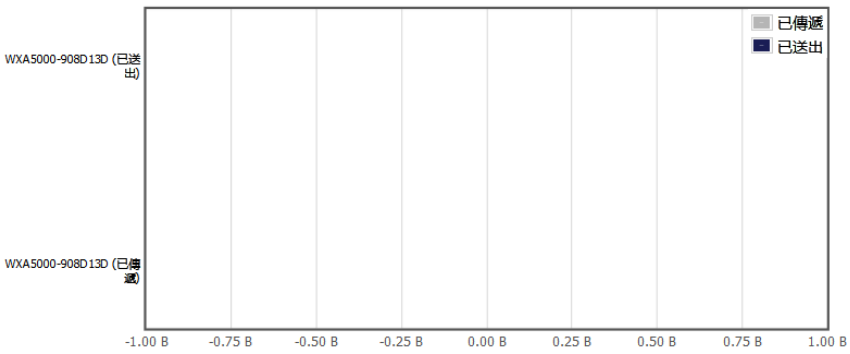
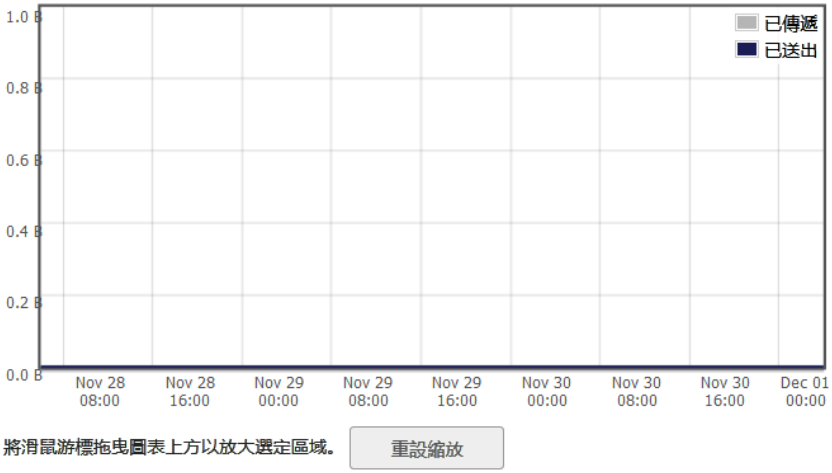
- 最近小時數
- 最近 24 小時
- 最近 3 天
- 最近 5 天
- 最近 10 天
- 最近 30 天

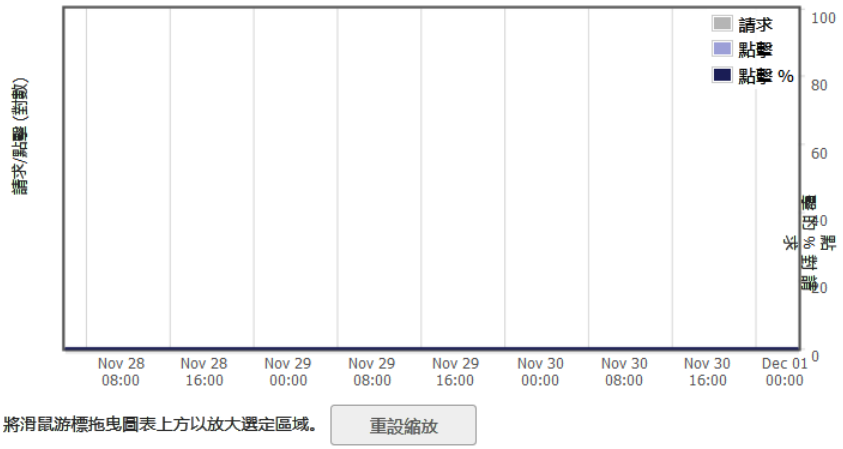
3 按一下**重新整理**圖示以重新整理將顯示的資料。

4 在**所選 WXA 的資料**部分，按下箭號可最小化或展開 WXA 清單。向左箭頭表示最小化的畫面，向下箭頭表示展開的畫面。

頁面的剩餘部分顯示與所選選項相關的資料。第一個部分是資料表**顯示所有可用 WXA 的資料針對最近 30 天**。它包含像是「所有資料減少」、「WAN 容量增量因素」、「請求」、「點擊」、「錯誤」和其他資訊。

頁面底部顯示所選涵蓋期間和圖表的 Web 快取資料。「已傳遞資料」是從 Web 伺服器傳送的位元組數，而不使用 WXA 設備的 Web 快取。「已傳送資料」是實際從 Web 伺服器傳送的位元組數，以回應使用者的請求，剩餘部分則從快取提供。「點擊」是從 Web 快取提供物件，而不是從網際網路擷取。可使用以下圖表類型：

名稱	說明
摘要	
由 WXA 分解	
時間序列	

名稱	說明
請求	

在**時間序列**報告和**請求**報告上，您可以放大特定資料集。只要使用滑鼠沿著您要放大的區段拉出一個方形，按一下**重設縮放**，即可重設圖形至其原始檢視。

分析統計資料

您可以使用「分解統計資料」檢視，根據特定欄位定義產生 WXA Web 快取報告。

名稱	說明
顯示	從**顯示**功能表，選擇您要顯示的資料類型： • **全部** • **對於群組** • **對於 WXA:** 如果選擇「對於群組」或「對於 WXA」，會顯示其他欄位。從下拉功能表中的選項選擇，以進一步精簡您的資料。
涵蓋期間	選擇資料顯示在「統計」標籤上的時間段。選項包括： • **最近小時數** • **最近 24 小時** • **最近 3 天** • **最近 5 天** • **最近 10 天** • **最近 30 天**
顯示上方	選擇要在圖形中顯示多少個連接埠或 IP 位址。選項為 **3**、**5**、**10**和 **15**。
判斷依據	選取顯示在圖形中的條件。選項包括： • **最高要求數** • **要求的大多數資料**
「**重新整理**」按鈕	每當您變更條件時，即更新顯示的資料。
適合印表機	產生適合印表機的報告。

12

封包監控

封包監控是用於監視穿越 SonicWall 裝置的個別資料封包的機制。可以監視封包，也可以對其進行鏡像處理。所監視的封包中包含資料和定址資訊。

主題：

概觀

SonicOS 封包監控功能提供了不使用外部實用工具即可查看網路流量所需的功能和靈活性。

封包監控包括以下功能：

- 用於自訂篩選、具有改進的粒度的控制機制（監視篩選條件）
- 顯示獨立於監視篩選條件設定的篩選條件設定
- 封包狀態指示是否丟棄、轉送、產生或以防火牆消耗封包
- 管理介面提供了三個輸出：
  - 已擷取封包的清單
  - 封包詳細資料
  - 選定封包的十六進位傾印
- 匯出功能包括用於封包十六進位傾印的文字或 HTML 格式，以及 CAP 檔案格式、pcap 和 pcapNG。
- 在緩衝區已滿時自動匯出到 FTP 伺服器
- 基於 IP 位址和連接埠的雙向封包監控
- 封包監控緩衝區已滿時的可設定覆寫

主題：

- 封包監控的運作方式
- 關於封包鏡像
- 支援的封包類型
- 匯出的檔案格式

封包監控的運作方式

您可以設定一般設定、監視篩選條件設定、顯示篩選條件設定、進階篩選條件設定，以及封包監控工具的 FTP 設定。在網路封包進入封包監控子系統時，將會套用監視篩選條件設定，並將結果封包寫入擷取緩衝區。當您在管理介面檢視緩衝區內容時，將套用顯示篩選條件設定。您可以在管理介面中記錄要檢視的擷取緩衝區，或者設定在緩衝區已滿時自動傳送至 FTP 伺服器。

系統提供了預設值，以便您無需設定即可開始使用封包監控。基本功能列於下表中。

封包：基本功能

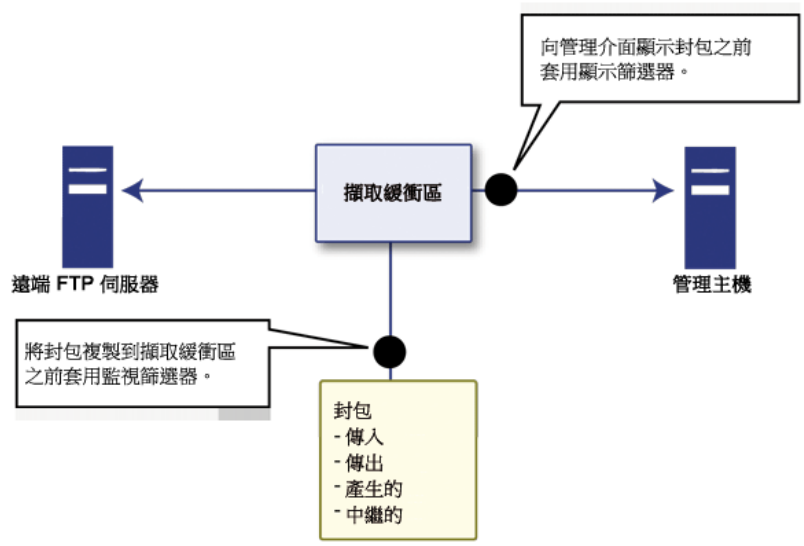
開始擷取	按一下以開始擷取所有封包，除了用於在防火牆與主控台系統中的管理介面之間通信的封包以外。
停止擷取	按一下以停止封包擷取。
開始鏡像	按一下以開始傳送所擷取封包的副本至另一個介面或傳送至遠端 SonicWall 裝置的程序。
停止鏡像	按一下以停止傳送所擷取封包至其他裝置。

封包：基本功能

記錄到 FTP 伺服器	按一下以記錄擷取資料至 FTP 伺服器。.
匯出為	以您在下拉功能表中選擇的檔案格式顯示或儲存目前緩衝區的快照。匯出的檔案將放置在執行管理介面的本機管理系統中。 • **Libpcap** - 如果想要使用 Wireshark（之前稱為 Ethereal）網路通訊協定分析器檢視資料，請選擇此選項。它也稱為 libcap 或 pcap 格式。隨即顯示一個對話方塊，用於使用 Wireshark 打開緩衝區檔案，或使用副檔名 **.pcap** 將其儲存到本機硬碟中。 • **Html** - 選擇此選項以使用瀏覽器檢視資料。可以使用「檔案 > 另存為」來將緩衝區的副本儲存到硬碟中。 • **文字** - 選擇此選項以使用文字編輯器檢視資料。隨即顯示一個對話方塊，用於使用已註冊的文字編輯器打開緩衝區檔案，或使用副檔名 **.wri** 將其儲存到本機硬碟中。 • **應用程式資料** - 選擇此選項以僅檢視封包內含的應用程式資料。在擷取過程中，將跳過不包含應用程式資料的封包。應用程式資料 = 已擷取的封包減去 L2、L3 和 L4 標頭。

請參閱顯示了各種篩選條件的封包監控子系統以獲得封包監控子系統高階視圖，其顯示了不同的篩選條件及應用方法。

顯示了各種篩選條件的封包監控子系統



關於封包鏡像

封包鏡像是將在一個介面上看到的封包的副本傳送至另一個介面或傳送至遠端 SonicWall 裝置的過程。

鏡像包括兩個方面：

- **分類** - 指的是識別要鏡像的選定封包組。系統將根據篩選條件來符合介面上的傳入和傳出封包。如果發現符合項，則套用鏡像操作。
- **操作** - 指的是將選定封包的副本傳送至某個連接埠或遠端目的地。與分類篩選條件相符合的封包將會傳送至其中一個鏡像目的地。具體的鏡像目的地包含在操作識別項中。

每個分類篩選條件都與某個操作識別項相關聯。最多可以定義兩個操作識別項，以支援兩個鏡像目的地（相同防火牆和/或遠端 SonicWall 防火牆上的實體連接埠）。操作識別項決定了封包的鏡像方式。支援以下操作識別項類型：

- 傳送副本到實體連接埠。
- 封裝封包並將其傳送至遠端 SonicWall 裝置。
- 傳送副本到有設定的 VLAN 的實體連接埠。

分類是在**封包監控設定**對話的**監視篩選條件**和**進階監視篩選條件**標籤中進行。

可以設定 SonicWall 防火牆來接收來自遠端 SonicWall 防火牆的遠端鏡像流量。在本機防火牆上，可以將收到的鏡像流量儲存在擷取緩衝區中，或者傳送到另一個本機介面。這是在**封包監控設定**對話的**鏡像**標籤上**遠端鏡像設定（接收者）**部分設定。

SonicOS 支援以下封包鏡像選項：

- 將封包鏡像到指定的介面（本機鏡像）。
- 僅鏡像選定的流量。
- 鏡像經過 SSL 解密的流量。
- 鏡像包括 2 層和 3 層標頭以及有效承載的完整封包。
- 將封包鏡像到遠端防火牆（遠端鏡像傳輸）。
- 接收來自遠端 SonicWall 裝置的鏡像封包（遠端鏡像接收）。

支援的封包類型

在指定您想要監視或顯示的乙太網路或 IP 封包類型時，可以使用此類型的標準首字母縮寫詞（如果支援），或者相應的十六進位表示。若要確定某個通訊協定的十六進位值，請參見 RFC 以獲取由 IANA 指派給它的數字。SonicOS 目前支援的通訊協定首字母縮寫詞如支援的封包類型表格所示。

支援的封包類型

支援的類型	通訊協定首字母縮寫詞	
支援的乙太網路類型	ARP	
	IP	
	PPPoE-DIS	**附註：**若要同時指定 PPPoE-DIS 和 PPPoE-SES，只需使用 PPPoE 即可。
	PPPoE-SES	
支援的 IP 類型	TCP	
	UDP	
	ICMP	
	IGMP	
	GRE	
	AH	
	ESP	

匯出的檔案格式

調查檢視的**工具 | 封包監控**頁面上的「匯出為」選項，可讓您用從下拉功能表中選擇的檔案格式顯示或儲存目前緩衝區的快照。儲存的檔案將放置在執行管理介面的本機管理系統中。關於格式的描述，請參閱封包：基本功能表格。

HTML 和文字格式的範例如下所示：

- HTML 格式
- 文字檔格式

HTML 格式

可以在瀏覽器中檢視 HTML 格式。HTML 格式範例顯示了緩衝區中第一個封包的標頭和部分資料。

HTML 格式範例

```
--File Index : 5.--

--990 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded      :       0
Number Of Packets Generated      :       250
Number Of Packets Consumed       :       140
Number Of Packets DROPPED        :       600
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2015 15:56:31.464):
 in:--, out:X0*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4712], Checksum=0xe425
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c..........E.......@.*
 9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.........d.P.h..y.....P.*
 2000e425 00003265 20373036 31363336 62203635 37343566 * ..%..2e 7061636b 65745f*
 36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
 32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
 36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1;*
 2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

文字檔格式

可以在文字編輯器中檢視文字格式的輸出。文字檔案格式範例顯示了緩衝區中第一個封包的標頭和部分資料。

文字檔案格式範例

```
--File Index : 7.--

--771 packets captured.--

-----Statistics------------
Number Of Bytes Failed To Report:        0
Number Of Packets Forwarded     :        0
Number Of Packets Generated     :        480
Number Of Packets Consumed      :        247
Number Of Packets DROPPED       :        44
Number Of Packets Status Unknown:        0

*Packet number: 1*
Header Values:
 Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2015 16:11:36.224):
 in:--, out:XO*, Generated (Sent Out)
Ethernet Header
 Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
 TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
 HTTP
Value:[0]
Hex and ASCII dump of the packet:
 00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c..........E...B...@.*
 6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`........d.P..Lp..R...P.*
 20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * ..... *nd for Netbios.*
 292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *), (Line:*. 20363137 204*
 36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
 37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
 46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

設定封包監控

如果要自訂封包監控的功能，請存取 SonicOS 管理介面的**調查**檢視上**工具 | 封包監控**頁面上的工具。封包監控具有六個主要設定區域：以下部分說明設定選項：

- 設定選項
- 設定監視篩選條件選項
- 設定顯示篩選條件選項
- 設定記錄
- 設定進階監視篩選條件選項
- 設定鏡像設定

設定選項

本章節說明何設定封包監控設定，包括每個封包要擷取的位元組數以及緩衝區覆寫選項。可以使用十進位或十六進位指定位元組數，最小值為 64。緩衝區覆寫選項在緩衝區已滿時透過從頭開始覆寫緩衝區，使得封包擷取得以繼續進行。

若要設定設定選項：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 在**要擷取的位元組數（每個封包）**欄位中，輸入要從每個封包中擷取的位元組數。最小值是 64，預設值是 **1520**。您也可以將此數字輸入為十六進位數字。

4 若要在緩衝區填滿後繼續擷取封包，請勾選**緩衝區已滿後，覆寫緩衝區中擷取的內容**核取方塊。此選項將使封包擷取在緩衝區填滿時，重新開始從緩衝區開頭處寫入擷取的封包。如果在**記錄**標籤中啟用了 FTP 伺服器記錄，則將不起作用，因為在啟用 FTP 的情況下，會自動覆寫緩衝區。預設情況下未勾選此選項。

5 在**排除篩選**部分，勾選**排除加密的 GMS 流量**，以防止與 SonicWall GMS 之間擷取或鏡像已加密的管理流量或 syslog 流量。此設定僅影響已設定的主要或次要 GMS 通道內的加密流量。不排除透過單獨通道傳送的 GMS 管理流量。預設情況下未勾選此選項。

6 使用**排除管理流量**設定，來防止將管理流量擷取或鏡像到裝置中。勾選可排除每種流量的核取方塊：

- **HTTP/HTTPS**（預設勾選）
- **SNMP**
- **SSH**

如果透過通道傳送管理流量，將不排除這些封包。

7 使用**排除 Syslog 流量到**設定，以防止將 syslog 流量擷取或鏡像到記錄伺服器中。勾選要排除的每種伺服器類型的核取方塊 (預設都未選取)：

- **Syslog 伺服器**
- **GMS 伺服器**

如果透過通道傳送 syslog 流量，將不排除這些封包。

8 使用**排除內部流量用於**設定，以防止擷取或鏡像在防火牆與其高可用性合作夥伴或已連接的存取點之間的內部流量。勾選要排除的每種流量的核取方塊：

- **HA**（預設勾選）
- **SonicPoint** (預設選擇此選項，在 SuperMassive 9800 上不支援)

  附註：以下選項僅適用於 SuperMassive 9800。顯示時，預設為已勾選。

- **BCP**
- **刀鋒間**
- **背板**

9 若要儲存設定並結束**封包監控設定**對話方塊，請按一下**確定**。

若要還原預設設定，請按一下**預設值**。

設定監視篩選條件選項

在此頁面中設定的所有篩選條件都將套用於封包擷取和封包鏡像。

設定監視篩選條件設定：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。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**按鈕。

4 如果使用防火牆規則篩選以擷取特定流量，請選擇**基於防火牆規則啟用篩選**。

附註：在勾選此選項之前，請確認您已選擇了一條或多條用於監視封包流量的存取規則。此項設定在**原則 | 規則 > 存取規則**頁面中完成，如需更多資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

5 使用以下選項指定封包監控篩選封包的方法：

附註：如果某個欄位或選項保留空白，則不針對此欄位進行篩選。封包的擷取或鏡像將不考慮其標頭的相應欄位所包含的值。

- **介面名稱** - 在您要執行封包擷取的地方輸入介面名稱。可以指定最多 10 個使用逗號分隔的介面。指定的介面名稱應與**系統安裝 | 網路 > 介面**頁面中列出的名稱相同；例如：
  - NSA 系列：X0、X1 和 X2:V100
  - TZ 系列：WLAN、WWAN、Modem、OPT、WAN 和 LAN

  若要設定除指定介面以外的所有介面，請使用負值；例如：!X0 或 !LAN。
- **乙太網路類型** - 指定對已擷取的封包執行篩選的乙太網路類型的名稱。可以指定最多 10 個使用逗號分隔的乙太網路類型。此選項不區分大小寫。目前支援以下乙太網路類型：ARP (arp)、IP (ip)、PPPoE-SES 和 PPPoE-DIS。後兩種類型只能由 PPPoE 單獨指定。

  例如，若要擷取所有支援的類型，可以輸入：ARP、ip、PPPOE。可以使用一個或多個負值來擷取除指定類型以外的所有乙太網路類型；例如：!ARP、!PPPoE。

  也可以使用十六進位值來表示乙太網路類型，或者混合使用十六進位值和標準表示；例如：ARP、0x800、ip。通常情況下，對於 SonicOS 中不支援的首字母縮寫的乙太網路類型，請您使用十六進位。如需更多資訊，請參閱支援的封包類型。
- **IP 類型** - 指定要執行封包擷取的 IP 封包類型的名稱。可以指定最多 10 個使用逗號分隔的 IP 類型。此選項不區分大小寫。支援以下 IP 類型：TCP、UDP、ICMP、GRE、IGMP、AH、ESP。

  可以使用一個或多個負值來擷取除指定類型以外的所有 IP 類型；例如：!TCP、!UDP。

  也可以使用十六進位值來表示 IP 類型，或者混合使用十六進位值和標準表示；例如：TCP、0x1、0x6。如需更多資訊，請參閱支援的封包類型。

附註：以下選項欄位需要位址或連接埠。可以指定最多 10 個位址或連接埠，以逗號分隔。例如：
- IP 位址：`10.1.1.1, 192.2.2.2, 1.2.3.4/24, 2.3.4.5/61`
- TCP 或 UDP 連接埠號：20, 21, 22, 25, 80, 8080

可以使用一個或多個負值來擷取來自除指定位址以外的所有位址或連接埠的封包；例如：
- IP 位址：`!10.3.3.3, !10.4.4.4., !1.2.3.4/24`
- TCP 或 UDP 連接埠號：!80, !8080, !20

- **來源 IP 位址** - 指定要執行封包擷取的來源 IP 位址。
- **來源連接埠** - 指定要執行封包擷取的來源連接埠。
- **目的地 IP 位址** - 指定要執行封包擷取的目的地 IP 位址。
- **目的地連接埠** - 指定要執行封包擷取的目的地連接埠位址。
- **啟用雙向位址和連接埠相符** - 當勾選此選項時，將使用在上述來源和/或目的地欄位中指定的 IP 位址和/或連接埠與每個封包中的來源和/或目的地欄位進行符合。預設情況下已核取此選項

附註：有關擷取各種類型封包的正常操作，請使以下選項處於未勾選狀態。選擇任一選項都會限制擷取的封包的類型。

- **僅轉送封包** - 勾選此選項以監視防火牆所轉送的所有封包。
- **僅消耗的封包** - 勾選此選項以監視防火牆內的內部來源所消耗的所有封包。
- **僅丟棄的封包** - 勾選此選項以監視在外圍丟棄的所有封包。

6 若要儲存設定並結束設定視窗，請按一下**確定**。

設定顯示篩選條件選項

本章節介紹如何設定封包監控顯示篩選條件設定。您在此處提供的值將與已擷取的封包中的相應欄位進行比較，且僅顯示符合的封包。這些設定僅套用於在管理介面中顯示已擷取的封包，而不影響封包鏡像。

附註：如果某個欄位保留空白，則不針對此欄位進行篩選。封包的顯示將不考慮其標頭的相應欄位所包含的值。

若要設定封包監控顯示篩選條件設定：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**顯示篩選條件**選項。

4 使用以下選項指定封包監控篩選封包的方法：

附註：如果某個欄位或選項保留空白，則不針對此欄位進行篩選。封包的擷取或鏡像將不考慮其標頭的相應欄位所包含的值。

- **介面名稱** - 指定要執行封包擷取的介面名稱。可以指定最多 10 個使用逗號分隔的介面。指定的介面名稱應與**系統安裝 | 網路 > 介面**頁面中列出的名稱相同；例如：
  - NSA 系列：X0、X1 和 X2:V100
  - TZ 系列：WLAN、WWAN、Modem、OPT、WAN 和 LAN

  若要設定除指定介面以外的所有介面，請使用負值；例如：!X0 或 !LAN。
- **乙太網路類型** - 指定對已擷取的封包執行篩選的乙太網路類型的名稱。可以指定最多 10 個使用逗號分隔的乙太網路類型。此選項不區分大小寫。目前支援以下乙太網路類型：ARP (arp)、IP (ip)、PPPoE-SES 和 PPPoE-DIS。後兩種類型只能由 PPPoE 單獨指定。

  例如，若要擷取所有支援的類型，可以輸入：ARP、ip、PPPOE。可以使用一個或多個負值來擷取除指定類型以外的所有乙太網路類型；例如：!ARP、!PPPoE。

  也可以使用十六進位值來表示乙太網路類型，或者混合使用十六進位值和標準表示；例如：ARP、0x800、ip。通常情況下，對於 SonicOS 中不支援的首字母縮寫的乙太網路類

型，請您使用十六進位。請參閱支援的封包類型。

- **IP 類型** - 指定要執行封包擷取的 IP 封包類型的名稱。可以指定最多 10 個使用逗號分隔的 IP 類型。此選項不區分大小寫。支援以下 IP 類型：TCP、UDP、ICMP、GRE、IGMP、AH、ESP。

  可以使用一個或多個負值來擷取除指定類型以外的所有 IP 類型；例如：!TCP、!UDP。

  也可以使用十六進位值來表示 IP 類型，或者混合使用十六進位值和標準表示；例如：TCP、0x1、0x6。請參閱支援的封包類型。

附註：以下選項欄位需要位址或連接埠。可以指定最多 10 個位址或連接埠，以逗號分隔。例如：

- IP 位址：`10.1.1.1,192.2.2.2,1.2.3.4/24,2.3.4.5/61`
- TCP 或 UDP 連接埠號：`20,21,22,25,80,8080`

可以使用一個或多個負值來擷取來自除指定位址以外的所有位址或連接埠的封包；例如：

- IP 位址：`!10.3.3.3,!10.4.4.4.,!1.2.3.4/24`
- TCP 或 UDP 連接埠號：`!80,!8080,!20`

- **來源 IP 位址** - 指定要執行封包擷取的來源 IP 位址。
- **來源連接埠** - 指定要執行封包擷取的來源連接埠。
- **目的地 IP 位址** - 指定要執行封包擷取的目的地 IP 位址。
- **目的地連接埠** - 指定要執行封包擷取的目的地連接埠位址。

附註：預設情況下已核取以下選項。

- **啟用雙向位址和連接埠相符** - 當勾選此選項時，將使用在上述來源和/或目的地欄位中指定的 IP 位址和/或連接埠與每個封包中的來源和/或目的地欄位進行符合。預設情況下已核取此選項。
- **已轉送** - 若要顯示防火牆已轉送的擷取封包，請勾選此核取方塊。
- **已產生** - 若要顯示防火牆已產生的擷取封包，請勾選此核取方塊。
- **已消耗** - 若要顯示防火牆已消耗的擷取封包，請勾選此核取方塊。
- **已丟棄** - 若要顯示防火牆已丟棄的擷取封包，請勾選此核取方塊。

5 若要儲存設定並結束對話方塊，請按一下**確定**。

設定記錄

本章節介紹如何設定封包監控記錄。這些設定提供了方法來設定將擷取緩衝區自動記錄到外部 FTP 伺服器。在緩衝區填滿時，封包將會傳送到 FTP 伺服器。這樣，就能繼續擷取，而不至於發生中斷。

如果設定了自動 FTP 記錄，它將取代緩衝區全滿時的覆寫設定。借助自動 FTP 記錄，擷取緩衝區不僅能在填滿時有效地執行覆寫，還能保留所有資料，而不是在每次覆寫緩衝區時將資料全部改寫。

主題：

- 設定記錄設定
- 重新啟動 FTP 記錄

設定記錄設定

設定記錄設定：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**記錄**標籤。

4 在 **FTP 伺服器 IP 位址**欄位中，輸入要對已擷取的封包記錄的 FTP 伺服器的 IP 位址。

附註：請確保防火牆可以存取此 FTP 伺服器的 IP 位址。不支援只能透過 VPN 通道存取的 IP 位址。

5 在**登入 ID** 欄位，輸入防火牆應該用來連接 FTP 伺服器的登入名稱。預設值為 **admin**。

6 在**密碼**欄位，輸入防火牆應該用來連接 FTP 伺服器的密碼。預設值為 **password**。

7 在**目錄路徑**欄位中，輸入記錄檔案的目錄路徑。已擷取的檔案將會在 FTP 伺服器上寫入此目錄位置（相對預設的 FTP 根目錄）。預設值為 **captures**。

以下是不同格式的檔案名稱的範例：

- 對於 **libcap** 格式，檔案將命名為 `packet-log--<>.cap`，其中，<> 包含執行編號及日期（包括小時、月、日和年）。例如，`packet-log-h3-22-06292017.cap`。
- 對於 **HTML** 格式，檔案將命名為 `packet-log_h-<>.html`，其中，<> 包含執行編號及日期（包括小時、月、日和年）。例如：`packet-log_h-3-22-06292017.html`。

8 若要啟用自動將擷取檔案記錄到遠端 FTP 伺服器，請勾選**自動記錄到 FTP 伺服器**核取方塊。已擷取的檔案將命名為如下格式（其中 <> 包含執行編號及日期，包括小時、月、日和年）：

- 對於 libcap 格式，使用 `packet-log-<>.cap`；例如：`packet-log_3-22-06292017.cap`。
- 對於 HTMTL 格式，使用`packet-log-<>.html`；例如：`packet-log_3-22-06292017.html`。

預設情況下未勾選此選項。

附註：必須在 **FTP 伺服器 IP 位址**欄位中指定 FTP 伺服器位址。

9 若要啟用將新產生具有包含偵錯資訊的註解的擷取檔案記錄到遠端 FTP 伺服器，請勾選**記錄 PCAPNG 檔到 FTP 伺服器**核取方塊。已擷取的檔案將命名為 `packet-log-<>.pcapng`（其中 <> 包含執行編號及日期，包括小時、月、日和年），例如：`packet-log_3-22-06292017.pcapng`。預設情況下已核取此選項。

10 若要啟用以 HTML 格式以及 libcap 格式傳送檔案，請勾選**記錄 HTML 檔案和 .cap 檔案 (FTP)**。預設情況下已核取此選項。

11 若要測試 FTP 伺服器連接並向其傳送擷取緩衝區內容，請按一下**現在記錄**。在這種情況下，檔案名稱中會包含一個 `F`。例如，`packet-log-F-3-22-08292006.cap` 或 `packet-log_h-F-3-22-06292017.html`。

12 若要儲存設定並結束對話方塊，請按一下**確定**。

重新啟動 FTP 記錄

如果由於連接故障或已停用的原因關閉了自動 FTP 記錄，可以在**設定 > 記錄**中將其重新啟動。

若要重新啟動 FTP 記錄：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**記錄**標籤。

4 確認頁面中每個項目的設定都正確無誤。請參閱設定記錄設定。

5 若要將 FTP 記錄狀態頁面變更為「使用中」，請勾選**自動記錄到 FTP 伺服器**核取方塊。

6 還可以按一下**現在記錄**按鈕來測試連接。

7 若要儲存設定並結束對話方塊，請按一下**確定**。

設定進階監視篩選條件選項

本章節介紹如何設定監視由防火牆產生的封包以及如何設定監視中間流量。

若要設定進階監視篩選條件設定：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**進階監視篩選條件**標籤

4 若要擷取防火牆產生的封包，請勾選**監控防火牆產生的封包。（該將繞過介面篩選條件）**。預設情況下未勾選此選項。

即使在其他監視篩選條件不符合的情況下，此選項仍可確保擷取由防火牆產生的封包。其中包括諸如由 HTTP(S)、L2TP、DHCP 伺服器、PPP、PPPOE 和路由等通訊協定產生的封包。擷取的封包如果來自系統堆疊，則會在傳入介面區域標記 s。否則將不指定傳入介面。

附註：如果即使其他擷取篩選條件無法符合也需要擷取防火牆產生的封包，請指定此選項。

5 若要擷取由防火牆基於各種原則產生的中間封包，請勾選**監控中間封包**核取方塊。包括諸如此類的封包：中間加密封包、IP 協助產生的封包、複製的多點廣播封包以及那些由於分段或重組而產生的封包

勾選此核取方塊會啟用此選項，但不會選擇用於監視指定類型的中間流量的後續核取方塊。預設情況下未勾選此選項。

6 選擇以下任意選項，以擷取或鏡像此類型的中間流量。監視篩選條件仍適用於這些封包。預設情況下未勾選以下任何選項。

- **監視中間多點傳送流量** - 用於多點傳送流量。
- **監視中間 IP 協助程式流量** - 用於複製的 IP 協助程式封包。
- **監視中間重組的流量** - 用於重組的 IP 封包。
- **監視中間片段流量** - 用於防火牆片段的封包。
- **監視中間遠端鏡像流量** - 用於解封裝後的遠端鏡像封包。
- **監視中間 IPsec 流量** - 用於加密和解密後的 IPSec 封包。
- **監視中間 SSL 解碼流量** - 用於 SSL 解密封包。

  附註：將 SSL 解密流量傳送到封包監控，且在監視的封包中某些 IP 和 TCP 標頭欄位可能不準確。IP 和 TCP 校驗不會在解密的封包上進行計算。TCP 連接埠號重新對應到連接埠 80。

  必須啟用 DPI-SSL 才能解密這些封包和那些套用了任何安全服務的封包。

- **監視中間解碼 LDAP 越過 TLS 的封包** - 用於解密的 LDAP over TLS (LDAPS) 封包。這些封包在輸入/輸出介面欄位中標有 `ldp`，並將包含有一些不準確欄位的乙太網路、IP 和 TCP 偽標頭。LDAP 伺服器連接埠設定為 389，以便外部擷取分析程式將其解碼為 LDAP。已擷取的 LDAP 繫結請求中的密碼已經過混淆處理。

  附註：將解密的 LDAPS 封包傳送到封包監控。

- **監視中間解碼單一登入代理訊息** - 用於與 SSO 驗證代理之間的解密訊息。這些封包在輸入/輸出介面欄位中標有 `sso`，並將包含有一些不準確欄位的乙太網路、IP 和 TCP 偽標頭。

  附註：將解密的 SSO 封包傳送到封包監控。

7 若要儲存設定並結束對話方塊，請按一下**確定**。

設定鏡像設定

本章節介紹如何設定封包監控鏡像設定。鏡像設定提供了將封包傳送至相同防火牆的其他實體連接埠，向遠端 SonicWall 防火牆傳送封包，或接收來自遠端 SonicWall 防火牆的封包的方法。

設定鏡像設定：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**設定**。此時會顯示**封包監控設定**對話方塊。

3 按一下**鏡像**標籤。

4 在**鏡像設定**下面，輸入所需的**最大的鏡像概率（每秒千位元組）**。如果在鏡像過程中超過此速率，超出的封包將不會進行鏡像，但將計為跳過的封包。此速率適用於鏡像到本機介面或遠端防火牆。預設值和最小值均為 **100** kbps，最大值為 1 Gbps。

5 勾選**僅 IP 封包鏡像**可阻止鏡像任何非 IP 的封包，例如 ARP 或 PPPoE。如果勾選此選項，它將覆寫在**監視篩選條件**標籤的**乙太網路類型**欄位中輸入的所有非 IP 乙太網路類型。

6 在**本機鏡像設定**的**鏡像已篩選的封包到介面**下拉功能表中，選擇在本機鏡像的封包的目的地介面。預設為**無**。

7 在**遠端鏡像設定（傳送者）**的**鏡像篩選的封包到遠端 SonicWall 防火牆（IP 位址）**欄位中，輸入要將鏡像封包傳送到的遠端 SonicWall 的 IP 位址。將封包封裝並傳送到遠端裝置（指定的 IP 位址）。

附註：此遠端 SonicWall 必須設定為接收鏡像封包。

8 在**加密遠端鏡像封包透過 IPSec（預先共用金鑰-IKE）**欄位中，輸入在向遠端防火牆傳送鏡像封包時用於加密流量的預先共用金鑰。設定此欄位將啟用此裝置與遠端防火牆之間的 IPSec 傳送模式通道。此預先共用金鑰由 IKE 用來交涉 IPSec 金鑰。

附註：啟用此選項還將啟用此裝置與遠端防火牆之間的 IPSec 傳送模式通道。

9 在**遠端鏡像設定（接收者）**下面的**從遠端的 SonicWALL 防火牆接收鏡像封包（IP 位址）**欄位中，輸入要接收鏡像封包的遠端裝置的 IP 位址。將封包解封並傳送到本機緩衝區或未在以下選項中指定的其它介面。

附註：此遠端 SonicWall 必須設定為傳送鏡像封包。

10 在**解密遠端鏡像封包透過 IPSec（預先共用金鑰-IKE）**欄位中，輸入先前已設定的預先共用金鑰，此金鑰在接收來自遠端防火牆的鏡像封包時用於加密/解密流量。此預先共用金鑰由 IKE 用來交涉 IPSec 金鑰。

附註：啟用此選項還將啟用此裝置與遠端防火牆之間的 IPSec 傳送模式通道。

11 若要將收到的封包鏡像到本機 SonicWall 上的其他介面，請從**傳送所接收的遠端鏡像封包到介面**下拉功能表中選擇此介面。預設為**無**。

12 若要將所有遠端鏡像封包儲存在本機擷取緩衝區中，請勾選**傳送已接收的遠端鏡像封包給擷取緩衝區**。此選項與將鏡像封包傳送到另一個介面的設定彼此獨立，如果需要，可以同時啟用。

13 若要儲存設定並結束對話方塊，請按一下**確定**。

驗證封包監控活動

本章節介紹如何判斷封包監控、鏡像或 FTP 記錄是否正在按照設定正常運作。

主題：

瞭解狀態指示器

封包監控部分顯示了用於封包擷取、鏡像和 FTP 記錄的狀態指示器。顯示式資訊工具提示顯示設定。

主題：

- 封包擷取狀態（追蹤）
- 鏡像狀態
- FTP 記錄狀態
- 目前緩衝統計
- 目前設定

封包擷取狀態（追蹤）

封包監控部分的第一行是封包擷取狀態指示器，標記為**追蹤**，並顯示以下三種狀態之一：

- **紅色** - 已停止擷取
- **綠色** - 正在執行擷取，並且緩衝區未滿
- **黃色** - 正在執行擷取，但緩衝區已滿

追蹤還顯示：

- 開啟/關閉指示器
- **緩衝區大小**，以 KB 計
- **擷取的封包**數目
- 已使用的緩衝區空間百分比（**緩衝區已用 %**）
- 已遺失的緩衝區容量（**MB 的緩衝區已遺失**）。在已開啟自動 FTP 記錄，但檔案傳送速度較慢的情況下，會發生封包遺失。如果在緩衝區再次填滿之前仍未完成傳送，新填充的緩衝區中的資料將會遺失。

  附註：儘管緩衝區覆寫選項在從頭覆寫時會清除緩衝區，但這不視為遺失資料。

鏡像狀態

存在三個用於封包鏡像的狀態指示器：

- **本機鏡像** - 傳送至相同 SonicWall 上的其他實體介面的封包

  對於本機鏡像，狀態指示器將顯示以下三種狀態之一：

- **紅色** - 已停止鏡像
- **綠色** - 已開啟鏡像
- **黃色** - 已開啟鏡像，但由於未指定本機鏡像介面，因此將之停用

本機鏡像行還顯示以下統計資料：

- 開啟/關閉指示器
- **鏡像到介面** - 指定的本機鏡像介面
- **已鏡像的封包** - 已在本機鏡像的封包總數
- **跳過的封包** - 由於在已設定監視的介面上載入/傳出的封包而跳過鏡像的封包總數
- **超出速率的封包** - 由於速率限制而跳過鏡像的封包總數

- **遠端鏡像傳輸** - 傳送至遠端 SonicWall 的封包

對於遠端鏡像傳輸，狀態指示器將顯示以下三種狀態之一：

- **紅色** - 已停止鏡像
- **綠色** - 已開啟鏡像，並已設定遠端 SonicWall IP 位址
- **黃色** - 已開啟鏡像，但由於遠端裝置拒絕鏡像的封包並傳送無法存取連接埠而停用 ICMP 訊息

遠端鏡像傳輸行還顯示以下統計資料：

- 開啟/關閉指示器
- **鏡像到** - 指定的遠端 SonicWall IP 位址
- **已鏡像的封包** - 已鏡像至遠端 SonicWall 裝置的封包總數
- **跳過的封包** - 由於在已設定監視的介面上載入/傳出的封包而跳過鏡像的封包總數
- **超出速率的封包** - 由於無法存取連接埠或其他網路問題而未能鏡像至遠端 SonicWall 的封包總數

- **遠端鏡像接收** - 接收自遠端 SonicWall 的封包

對於遠端鏡像接收，狀態指示器將顯示以下兩種狀態之一：

- **紅色** - 已停止鏡像
- **綠色** - 已開啟鏡像，並已設定遠端 SonicWall IP 位址

遠端鏡像接收行還顯示以下統計資料：

- 開啟/關閉指示器
- **接受來自** - 指定的遠端 SonicWall IP 位址
- **接收的鏡像封包** - 接收自遠端 SonicWall 裝置的封包總數
- **接收的鏡像封包但是跳過** - 由於封包錯誤而未能在本機鏡像的接收自遠端 SonicWall 裝置的封包總數

FTP 記錄狀態

FTP 記錄狀態指示器顯示以下三種狀態之一：

- **紅色** - 已關閉自動 FTP 記錄
- **綠色** - 已開啟自動 FTP 記錄

- **黃色** - 最近一次嘗試聯絡 FTP 伺服器失敗，因此現已關閉記錄

  附註：若要重新啟動自動 FTP 記錄，請參見重新啟動 FTP 記錄。

FTP 記錄行還顯示以下統計資料：

- 開啟/關閉指示器
- **FTP 伺服器透過/失敗數目：0/0** - 嘗試將緩衝區內容傳送到 FTP 伺服器的成功次數和失敗次數
- **FTP 執行緒繁忙/閒置** - FTP 進程執行緒的目前狀態
- **緩衝區狀態** - 擷取緩衝區的狀態

目前緩衝統計

目前緩衝統計行匯總了本機擷取緩衝區中每一種類型封包的數量。

- **已丟棄** - 已丟棄的封包的數量
- **已轉送** - 已轉送的封包的數量
- **已消耗** - 已消耗的封包的數量
- **已產生** - 已產生的封包的數量

目前設定

目前設定行提供有關以下內容已設定的動態資訊：

- **篩選條件**，同時包含**擷取篩選條件**和**顯示篩選條件**
- **一般**，同時包含**一般設定**和**進階設定**
- **記錄**
- **鏡像**，**鏡像設定**

在您將滑鼠指標放在其中一個資訊圖示上面時，將會顯示工具提示，顯示此選項的目前設定。

清除狀態資訊

若要清除封包監控佇列以及所顯示的統計資料：

1 導覽至**調查**檢視上的**工具 | 封包監控**頁面。

2 按一下**清除**按鈕。

使用封包監控和封包鏡像

除了**設定**按鈕以外，**工具 | 封包監控**頁面的底部還提供了多個按鈕，用於封包監控功能和顯示的一般控制。

- **設定** - 顯示**封包監控設定**對話方塊。更多資訊請參閱設定封包監控。
- **監視全部** - 重設目前監視篩選條件設定和進階頁面設定，以便監視所有本機介面上的流量。按一下此按鈕時會顯示確認對話方塊。
- **監視預設** - 重設目前監視篩選條件設定和進階頁面設定，以便恢復出廠預設值。按一下此按鈕時會顯示確認對話方塊。
- **清除** - 清除封包監控佇列以及所顯示的擷取快取、鏡像和 FTP 記錄統計資料。
- **重新整理** - 重新整理此頁面中的封包顯示視窗，以顯示新的快取資料。

此頁面中的其他按鈕和顯示將在以下章節中說明：

- 開始和停止封包擷取
- 開始和停止封包鏡像
- 檢視已擷取的封包

開始和停止封包擷取

您可以使用預設值開始封包擷取，而無需設定指定準則的封包擷取、顯示、FTP 匯出條件及其他設定。如果開始預設的封包擷取，SonicWall 安全裝置將擷取除內部通信以外的所有封包，並在緩衝區已滿或按一下**停止擷取**時停止擷取。

1. 導覽至**調查**檢視上的**工具 | 封包監控**頁面。
2. 如果想要將統計資料設回零，請按一下頁面底部的**清除**。
3. 在**封包監控**下面，按一下**開始擷取**。
4. 若要重新整理封包顯示以顯示新的緩衝區資料，請按一下頁面底部的**重新整理**。
5. 若要停止封包擷取，請按一下**停止擷取**。

您可以在**封包監控**頁面的**已擷取的封包**、**封包詳細資料**和**十六進位傾印**部分檢視已擷取的封包。

開始和停止封包鏡像

您可以透過按一下**開始鏡像**，使用您所設定的鏡像設定開始封包鏡像，而無需先設定準則的顯示、記錄、FTP 匯出條件及其他設定。按一下**停止鏡像**時將會停止封包鏡像。

啟動或停止封包監控：

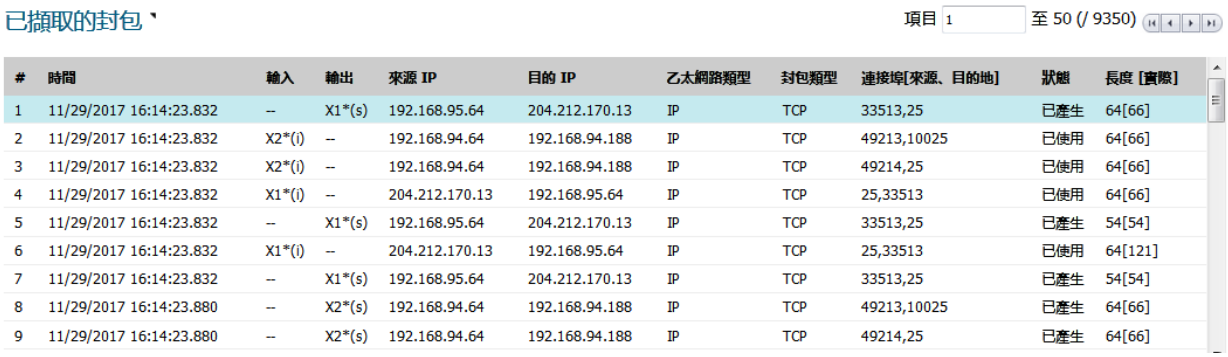
1. 導覽至**調查**檢視上的**工具 | 封包監控**頁面。
2. 在**封包監控**下面，按一下**開始鏡像**開始根據您所設定的設定對封包進行鏡像。
3. 若要停止封包鏡像，請按一下**停止鏡像**。

檢視已擷取的封包

工具 | 封包監控頁面提供了三個部分來顯示已擷取封包的不同檢視。

- 已擷取封包
- 封包詳細資料
- 十六進位傾印

已擷取封包



#	時間	輸入	輸出	來源 IP	目的 IP	乙太網路類型	封包類型	連接埠[來源、目的地]	狀態	長度 [實際]
1	11/29/2017 16:14:23.832	--	X1*(s)	192.168.95.64	204.212.170.13	IP	TCP	33513,25	已產生	64[66]
2	11/29/2017 16:14:23.832	X2*(i)	--	192.168.94.64	192.168.94.188	IP	TCP	49213,10025	已使用	64[66]
3	11/29/2017 16:14:23.832	X2*(i)	--	192.168.94.64	192.168.94.188	IP	TCP	49214,25	已使用	64[66]
4	11/29/2017 16:14:23.832	X1*(i)	--	204.212.170.13	192.168.95.64	IP	TCP	25,33513	已使用	64[66]
5	11/29/2017 16:14:23.832	--	X1*(s)	192.168.95.64	204.212.170.13	IP	TCP	33513,25	已產生	54[54]
6	11/29/2017 16:14:23.832	X1*(i)	--	204.212.170.13	192.168.95.64	IP	TCP	25,33513	已使用	64[121]
7	11/29/2017 16:14:23.832	--	X1*(s)	192.168.95.64	204.212.170.13	IP	TCP	33513,25	已產生	54[54]
8	11/29/2017 16:14:23.880	--	X2*(s)	192.168.94.64	192.168.94.188	IP	TCP	49213,10025	已產生	64[66]
9	11/29/2017 16:14:23.880	--	X2*(s)	192.168.94.64	192.168.94.188	IP	TCP	49214,25	已產生	64[66]

已擷取的封包部分顯示關於每個封包的下列統計資料：

- **#** - 相對開始擷取時的封包編號
- **時間** - 擷取此封包的日期和時間
- **輸入** - 將封包到達的防火牆介面標記為星號 (*)。子系統類型縮寫顯示在括弧中。子系統類型縮寫表格中定義了子系統類型縮寫。

  子系統類型縮寫

縮寫	定義
i	介面
hc	基於硬體的加密或解密
sc	基於軟體的加密或解密
m	多點傳送
r	封包重組
s	系統堆疊
ip	IP 協助程式
f	片段

- **輸出** - 發出並擷取封包時所在的防火牆介面子系統類型縮寫顯示在括弧中。如需子系統類型縮寫的定義，請參見子系統類型縮寫表格。
- **來源 IP** - 封包的來源 IP 位址
- **目的 IP** - 封包的目的地 IP 位址
- **乙太網路類型** - 封包的乙太網路報頭所提供的封包乙太網路類型
- **封包類型** - 取決於乙太網路類型的封包類型；例如：

乙太網路類型	封包類型：
IP 封包	TCP、UDP 或在 IP 上執行的其它通訊協定
PPPoE 封包	PPPoE 發現或 PPPoE 工作階段
ARP 封包	請求或回覆

- **連接埠 [來源，目的地]** - 封包的來源和目的地 TCP 或 UDP 連接埠
- **狀態** - 封包的狀態列位

  狀態列位顯示關於防火牆的封包狀態。防火牆可能丟棄、產生、消耗或轉送封包。您可以將滑鼠指標放在已丟棄或已消耗的封包上，以顯示以下資訊：

封包狀態	顯示的值	顯示值的定義
已丟棄	Module-ID = <*整數*>	通訊協定子系統 ID 的值
	Drop-code = <*整數*>	丟棄封包的原因
	Reference-ID: <*代碼*>	SonicWall 指定資料
已消耗的	Module-ID = <*整數*>	通訊協定子系統 ID 的值

- **長度 [實際]** - 長度值是此封包在緩衝區中擷取的位元組數。實際值（在括弧中）是在封包中傳送的位元組數。

封包詳細資料

在您按一下**已擷取的封包**部分的封包時，此封包的標頭欄位將會顯示在**封包詳細資料**視窗中。根據您選擇的封包類型，顯示內容將會不同。

封包詳細資料

```
Ethernet Header
 Ether Type: IP(0x800), Src=[c0:ea:e4:59:90:1f], Dst=[00:17:c5:0f:6e:84]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.95.64], Dst=[204.212.170.13]
TCP Packet Header
 TCP Flags = [SYN,], Src=[33513], Dst=[25], Checksum=0x6431
Application Header
 Smtp
```

十六進位傾印

在您按一下**已擷取的封包**部分的封包時，此封包的資料將會以十六進位和 ASCII 格式顯示在**十六進位傾印**部分中。十六進位格式顯示在視窗左側，相應的 ASCII 字元顯示在每一行的右側。十六進位值為零時，ASCII 值顯示為圓點。

十六進位傾印

```
00000000 0000c0ea e4599020 08004500 00340114 40004006 *.........Y. ..E..4..@.@.*
fb62c0a8 5e40c0a8 5ebcc03d 27293f58 142e0000 00008002 *.b..^@..^..=')?X........*
fffff601 00000101 02040590 04020103                    *................       *
```

13

封包重送

封包重送是一個整合到防火牆的工具，用於偵錯用途。您可以三種方式重送封包：

- 產生一個封包

  透過管理介面逐個指定封包標頭欄位和承載。
- 使用封包緩衝區

  輸入封包資料 (標頭和承載) 或者只是從其他地方複製後貼上。
- 重送 Pcap 檔案

  重送一連串儲存在 Pcap 檔案中的封包。

重送的封包被限制為不可在防火牆外周遊；它們會在透過介面傳輸之前丟棄。

主題：

單一封包

以下過程介紹如何產生用於分析的封包。IP 類型變更時，有些欄位也跟著變更。

封包產生

以下程序使用 **IP 類型** = **UDP**。

若要產生封包：

1 導覽至**調查**檢視上的**工具 | 封包重送**。

2 按一下**單一封包**。

3 選擇**封包產生**。

4 輸入以下資訊：

欄位	定義
接收介面	選擇您認為是接收封包所在的介面。
目的地 MAC	在目的地 MAC 位址中輸入。
來源 MAC	在來源 MAC 位址中輸入。
乙太網路類型	從下拉功能表中選擇通訊協定類型。預設值為 **IPv4**。
IP 類型	從下拉功能表中選擇 **UDP**。
來源 IP	在來源 IP 位址中輸入。
目的地 IP	在目的地 IP 位址中輸入。
TTL	在 IP 標頭中輸入。
來源連接埠	在 UDP 來源連接埠編號中輸入。
目的連接埠	在 UDP 目的地連接埠編號中輸入。

5 在**承載**欄位中輸入或複製承載十六進位資料。

6 按一下**傳送**按鈕。

產生的封包會傳送到防火牆引擎。

如果選擇 **IP 類型** = **ICMP**，這些欄位會與 UDP 不同：

欄位	定義
ICMP 類型	從下拉功能表中選擇**回應要求**或**回應**。
ID	在 ICMP 識別項中輸入。
順序	在 ICMP 序號輸入。

如果選擇 **IP 類型** = **IGMP**，這些欄位會與 UDP 不同：

欄位	定義
IGMP 類型	從下拉功能表中選擇 **IGMP 類型**。預設為**成員查詢**。
最大回應	在 ICMP 最大回應逾時中輸入。輸入值 (以秒為單位)。
群組 IP 位址	在查詢的群組 IP 位址中輸入。

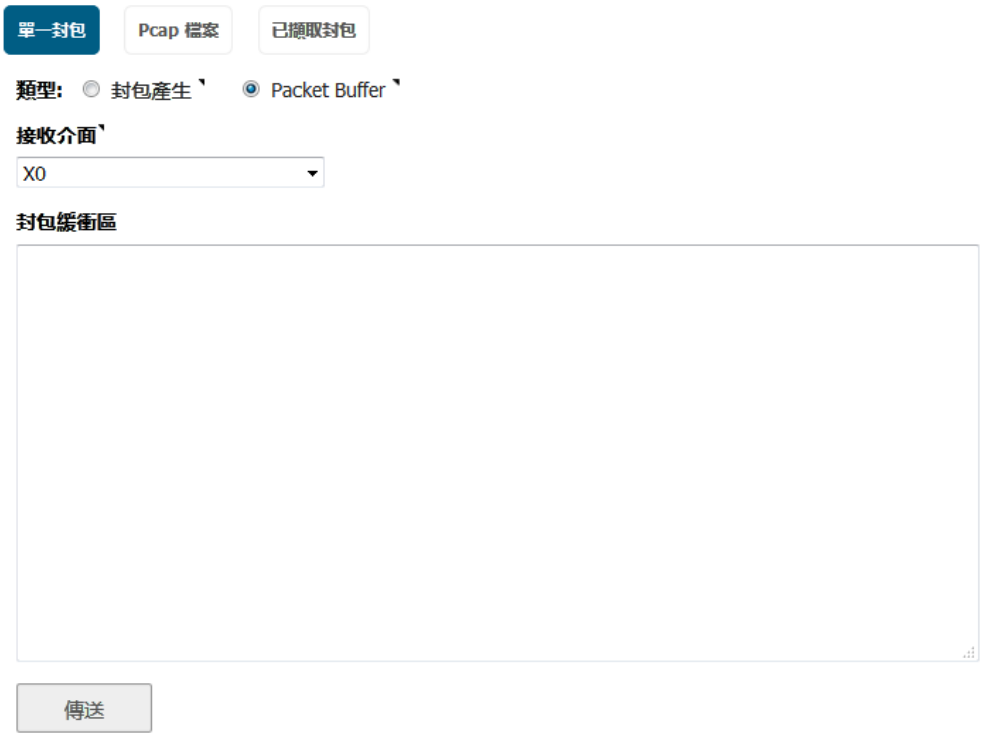
封包緩衝區

若要建置封包緩衝區：

1 導覽至**調查**檢視上的**工具 | 封包重送**。

2 按一下**單一封包**。

3 選擇**封包緩衝區**。



4 從下拉功能表中選擇**接收介面**。

5 在提供的文字方塊中以十六進為輸入**封包緩衝區**資料。

6 按一下**傳送**。

產生的封包會傳送到防火牆引擎。

重送 Pcap 檔案

Pcap 篩選可以 IP 位址或 MAC 位址定義。

若要以 IP 定義：

1 導覽至**調查**檢視上的**工具 | 封包重送**。

2 按一下 **Pcap 檔案**。

3 在**類型**欄位中選擇 **IP**。會提供兩個 IP 篩選條件。

4 對於各個 IP 篩選條件，完成下列欄位：

欄位	定義
IP 位址	在要查詢的目的地位址中輸入。
接收介面	從下拉功能表中選擇接收介面。如果 IP 封包具有以上所列目的地位址，會被認為來自此欄位中所選的介面。
新 IP 位址	如果啟用 (勾選方塊)，此欄位中列出的新 IP 位址會在重送封包時取代所篩選的目的地 IP 位址。

5 按一下**瀏覽**以搜尋和選擇要重送的 Pcap 檔案。

6 按一下**上載**以上載所選擇的檔案。

7 按一下**重送**以重送所上傳 Pcap 檔案中的封包。

8 完成時，按一下**刪除**以刪除上傳的檔案。

若要以 Mac 定義：

1 導覽至**調查**檢視上的**工具 | 封包重送**。

2 按一下 **Pcap 檔案**。

3 在**類型**欄位中選擇 **MAC**。會提供兩個 IP 篩選條件。

4 對於各個 IP 篩選條件，完成下列欄位：

欄位	定義
MAC 位址	在要查詢的目的地位址中輸入。
接收介面	從下拉功能表中選擇接收介面。如果封包具有以上所列目的地 MAC 位址，會被認為來自此欄位中所選的介面。
新 IP 位址	如果啟用 (勾選方塊)，此欄位中列出的新 IP 位址會在重送封包時取代所篩選的目的地 IP 位址。

5 按一下**瀏覽**以搜尋和選擇要重送的 Pcap 檔案。

6 按一下**上載**以上載所選擇的檔案。

7 按一下**重送**以重送所上傳 Pcap 檔案中的封包。

8 完成時，按一下**刪除**以刪除上傳的檔案。

已擷取封包

所擷取的重送封包會顯示在「已擷取的封包」選項上。導覽至**調查**檢視上的**工具 | 封包重送**，然後按一下**已擷取的封包**。**已擷取的封包**頁面提供了三個部分來顯示已擷取封包的不同檢視。

- 已擷取封包
- 封包詳細資料
- 十六進位傾印

使用這些選項來管理已擷取的封包：

- **清除** - 清除封包監控佇列以及所顯示的擷取快取、鏡像和 FTP 記錄統計資料。
- **重新整理** - 重新整理此頁面中的封包顯示視窗，以顯示新的快取資料。
- **匯出為 –** 以您在下拉功能表中選擇的格式匯出檔案。儲存的檔案將放置在本機管理系統中。

已擷取封包

已擷取的封包 ▾ 項目 1 至 50 (/ 9350)

#	時間	輸入	輸出	來源 IP	目的 IP	乙太網路類型	封包類型	連接埠[來源、目的地]	狀態	長度 [實際]
1	11/29/2017 16:14:23.832	--	X1*(s)	192.168.95.64	204.212.170.13	IP	TCP	33513,25	已產生	64[66]
2	11/29/2017 16:14:23.832	X2*(i)	--	192.168.94.64	192.168.94.188	IP	TCP	49213,10025	已使用	64[66]
3	11/29/2017 16:14:23.832	X2*(i)	--	192.168.94.64	192.168.94.188	IP	TCP	49214,25	已使用	64[66]
4	11/29/2017 16:14:23.832	X1*(i)	--	204.212.170.13	192.168.95.64	IP	TCP	25,33513	已使用	64[66]
5	11/29/2017 16:14:23.832	--	X1*(s)	192.168.95.64	204.212.170.13	IP	TCP	33513,25	已產生	54[54]
6	11/29/2017 16:14:23.832	X1*(i)	--	204.212.170.13	192.168.95.64	IP	TCP	25,33513	已使用	64[121]
7	11/29/2017 16:14:23.832	--	X1*(s)	192.168.95.64	204.212.170.13	IP	TCP	33513,25	已產生	54[54]
8	11/29/2017 16:14:23.880	--	X2*(s)	192.168.94.64	192.168.94.188	IP	TCP	49213,10025	已產生	64[66]
9	11/29/2017 16:14:23.880	--	X2*(s)	192.168.94.64	192.168.94.188	IP	TCP	49214,25	已產生	64[66]

已擷取的封包部分顯示關於每個封包的下列統計資料：

- **#** - 相對開始擷取時的封包編號
- **時間** - 擷取此封包的日期和時間
- **輸入** - 將封包到達的防火牆介面標記為星號 (*)。子系統類型縮寫顯示在括弧中。子系統類型縮寫表格中定義了子系統類型縮寫。

  子系統類型縮寫

縮寫	定義
i	介面
hc	基於硬體的加密或解密
sc	基於軟體的加密或解密
m	多點傳送
r	封包重組
s	系統堆疊
ip	IP 協助程式
f	片段

- **輸出** - 發出並擷取封包時所在的防火牆介面子系統類型縮寫顯示在括弧中。如需子系統類型縮寫的定義，請參見子系統類型縮寫表格。
- **來源 IP** - 封包的來源 IP 位址
- **目的 IP** - 封包的目的地 IP 位址
- **乙太網路類型** - 封包的乙太網路報頭所提供的封包乙太網路類型
- **封包類型** - 取決於乙太網路類型的封包類型；例如：

乙太網路類型	封包類型：
IP 封包	TCP、UDP 或在 IP 上執行的其它通訊協定
PPPoE 封包	PPPoE 發現或 PPPoE 工作階段
ARP 封包	請求或回覆

- **連接埠 [來源，目的地]** - 封包的來源和目的地 TCP 或 UDP 連接埠
- **狀態** - 封包的狀態列位

狀態列位顯示關於防火牆的封包狀態。防火牆可能丟棄、產生、消耗或轉送封包。您可以將滑鼠指標放在已丟棄或已消耗的封包上，以顯示以下資訊：

封包狀態	顯示的值	顯示值的定義
已丟棄	Module-ID = <*整數*>	通訊協定子系統 ID 的值
	Drop-code = <*整數*>	丟棄封包的原因
	Reference-ID: <*代碼*>	SonicWall 指定資料
已消耗的	Module-ID = <*整數*>	通訊協定子系統 ID 的值

- **長度 [實際]** - 長度值是此封包在緩衝區中擷取的位元組數。實際值（在括弧中）是在封包中傳送的位元組數。

封包詳細資料

在您按一下**已擷取的封包**部分的封包時，此封包的標頭欄位將會顯示在**封包詳細資料**視窗中。根據您選擇的封包類型，顯示內容將會不同。

封包詳細資料

```
Ethernet Header
 Ether Type: IP(0x800), Src=[c0:ea:e4:59:90:1f], Dst=[00:17:c5:0f:6e:84]
IP Packet Header
 IP Type: TCP(0x6), Src=[192.168.95.64], Dst=[204.212.170.13]
TCP Packet Header
 TCP Flags = [SYN,], Src=[33513], Dst=[25], Checksum=0x6431
Application Header
 Smtp
```

十六進位傾印

在您按一下**已擷取的封包**部分的封包時，此封包的資料將會以十六進位和 ASCII 格式顯示在**十六進位傾印**部分中。十六進位格式顯示在視窗左側，相應的 ASCII 字元顯示在每一行的右側。十六進位值為零時，ASCII 值顯示為圓點。

十六進位傾印

```
00000000 0000c0ea e4599020 08004500 00340114 40004006 *.........Y. ..E..4..@.@.*
fb62c0a8 5e40c0a8 5ebcc03d 27293f58 142e0000 00008002 *.b..^@..^..=')?X........*
fffff601 00000101 02040590 04020103                    *.................       *
```

14

網路探查

調查檢視上的**工具 | 網路探查**頁面提供了靈活的機制來監視網路路徑可行性。此監視的結果和狀態會動態顯示在**網路探查**頁面上，並且在系統記錄中記錄受影響的用戶端元件。

主題：

網路探查概觀

每個自訂網路監視器原則都指定了一個要探查的目的地位址物件。此位址物件可能是主機、群組、範圍或 FQDN。當目的地位址物件為擁有多個已解析位址的群組、範圍或 FQDN 時，網路監視器將探查每個探查目標並基於探查結果衍生網路監視器原則狀態。

從 6.2.5.1 開始，SonicOS 可監控本機或遠端網路中任何遠端主機的狀態。SonicOS 現在會即時檢查設備和目標主機間的流量可用性，藉此確保目標主機可以接收網路流量。SonicOS 也會在**工具 | 網路探查**頁面上顯示受監控主機的狀態。

狀態列中的元素顯示連接到目的地的網路連接狀態：

- 綠色表示原則狀態為「正常」。
- 紅色表示原則狀態為「停用」。
- 黃色表示原則狀態為「未知」。

將滑鼠放在原則的綠色、紅色或黃色指示燈上可查看探查狀態詳情。

此資訊會顯示在探查狀態中：

- 成功探查所占的百分比。
- 已解析的探查目標數量。
- 已傳送的探查總數。
- 收到成功探查回應的總數。
- 已解析的探查目標及其狀態的清單。

新增網路監視器原則

若要新增網路監視器原則：

1 導覽至**調查**檢視上的**工具 | 網路探查**。

2 按下**新增**。

3 輸入以下資訊以定義網路監視器原則：

- **名稱** - 輸入網路監視器原則的描述。
- **探查目標** - 選擇作為原則目的地的位址物件或位址群組。位址物件可能是主機、群組、範圍或 FQDN 物件。群組物件中的物件可能是主機、範圍或 FQDN 位址物件。可透過選擇建立新位址物件來動態建立新位址物件。
- **下一躍點閘道** - 手動指定從輸出介面到探查目標所使用的下一躍點。必須為顯見路由原則設定此選項。對於非顯見路由原則，探查將使用裝置的路由表來確定到達探查目標的輸出介面。如果未指定下一躍點閘道，探查將假設目的地直接連接到輸出介面的網路。
- **本機 IP 位址** - 從下拉功能表中選擇本機 IP 位址。
- **輸出介面** - 手動指定用於傳送探查的介面。必須為顯見路由原則設定此選項。對於非顯見路由原則，探查將使用裝置的路由表來確定到達探查目標的輸出介面。

4 從**探查類型**下拉功能表中，選擇用於網路監控原則的適當探查類型：

- **Ping (ICMP)** - 此探查使用路由表來查找指定探查目標的輸出介面和下一躍點。Ping 回應請求使用輸出介面的來源 IP 位址，透過輸出介面傳送出去。回應必須在指定的回應逾時時間以內透過同一介面返回，ping 操作才能算成功。
- **TCP** - 此探查使用路由表來查找指定探查目標的輸出介面和下一躍點。TCP SYN 封包使用輸出介面的來源 IP 位址傳送至探查目標。當目的地在回應逾時時間視窗內透過同一介面回應 SYN/ACK 或 RST 時，將為每個探查目標獨立計數一次成功的回應。在收到 SYN/ACK 時，將傳送 RST 以關閉連接。如果收到 RST，則不返回回應。
- **Ping (ICMP) - 顯見路由** - 此探查繞過路由表並使用在「輸出介面」下拉功能表中指定的介面來源 IP 位址向目的地傳送 Ping。如果未指定下一躍點閘道，探查將假設目的地直接連接到輸出介面的網路。

- **TCP - 顯見路由** - 此探查繞過路由表並使用在「輸出介面」下拉功能表中指定的介面來源 IP 位址向目的地傳送 TCP SYN 封包。如果未指定下一躍點閘道，探查將假設目的地直接連接到輸出介面的網路。在收到 SYN/ACK 時，將傳送 RST 以關閉連接。如果收到 RST，則不返回回應。

5 指定 TCP 探查的目標主機的目的地**連接埠**。對於 Ping 探查，不指定連接埠。

6 （可選操作）可調整以下探查閾值：

- **探查主機每** - 各次探查之間的秒數。此數字不能小於**回應逾時**欄位中的數字。預設值為 **5** 秒。
- **回應逾時** - 網路探查在為特定探查目標計數一次遺失的探查之前，等待每個單獨探查的回應的秒數。**回應逾時**不能超過**探查主機每**欄位中的數字。預設值為 **1** 秒。
- **將探查狀態設為「失敗」之前** - 觸發將主機狀態轉換為「失敗」之前連續遺失的探查次數。預設值為 **3** 個遺失間隔。
- **將探查狀態設為「正常」之前** - 觸發將主機狀態轉換為「正常」之前連續成功的探查次數。預設值為 **3** 個成功間隔。
- **所有主機必須回應** - 勾選此核取方塊將啟用，所有探查目標主機的狀態都必須為「正常」才能將原則狀態轉換為「正常」。如果未勾選此選項，在任何主機狀態為「正常」時，將原則狀態設為「正常」。預設已停用此選項。
- **RST 回應視為遺失** - 勾選此核取方塊可以啟用將 RST 回應計為遺失回應。

7 （可選操作）可在**註解**欄位中輸入關於原則的描述性註解。

8 按一下**新增**以提交網路監視器原則。

在設定固定路由時，可選擇設定用於此路由的網路監視器原則。使用網路監視器原則時，將基於原則的探查狀態來動態地停用或啟用固定路由。更多資訊，請參見 *SonicWall SonicOS 6.5 系統安裝*中的**系統安裝 | 網路 > 路由**。

15

使用診斷工具

調查檢視上的**工具 | 系統診斷**頁面提供了多項有助於排除網路故障的診斷工具以及進程監控。

- 技術支援報告
- 診斷工具概觀
- 檢查網路設定
- IPv6 檢查網路設定
- 連線監控

- 多核心監控
- 核心監控
- 連結監控
- 封包大小監控
- DNS 名稱查詢
- 查找網路路徑
- Ping
- 核心 0 執行序監控
- 即時黑名單查詢
- 反向名稱解析
- 連線限制前 X
- 檢查 GEO 位置和 BOTNET 伺服器查詢
- 追蹤路由
- PMTU 探索
- Web 伺服器監控
- 使用者監控
- 交換器診斷

技術支援報告

技術支援報告可產生詳細的 SonicWall 安全裝置設定和狀態報告，並使用**下載報告**按鈕將其儲存到本機硬碟中。然後，可以使用電子郵件將此檔案傳送到 SonicWall 技術支援部門，以幫助我們解決問題。

提示：您必須在 MySonicWall 上註冊 SonicWall 安全裝置才能獲得技術支援。

主題：

- 完成技術支援請求
- 產生技術支援報告

完成技術支援請求

在使用電子郵件向 SonicWall 技術支援團隊傳送技術支援報告之前，請在 https://www.mysonicwall.com 上填寫一份技術支援請求表單。提交此表單後，將會返回一個唯一的案例編號。在所有信件中包含此案例編號，因為此編號可以幫助 SonicWall 技術支援部門為您提供更好的服務。

產生技術支援報告

提示：如果您不需要產生報告，請按一下右上角的**折疊**按鈕，以提供更多空間給診斷工具。

如需產生技術支援報告 (TSR)，請完成以下步驟：

1 在**技術支援報告**部分，選擇以下任意報告選項：

- **敏感金鑰** - 將共用密碼、加密金鑰和驗證金鑰儲存到報告中。預設情況下未勾選此選項。
- **ARP 快取** - 儲存用於將 IP 位址與相應的 MAC 或實體位址關聯起來的表格。預設情況下未勾選此選項。
- **DHCP 繫結** - 儲存來自防火牆 DHCP 伺服器的項目。預設情況下未勾選此選項。
- **IKE 資訊** - 儲存關於 IKE 使用中設定的目前資訊。預設情況下未勾選此選項。
- **無線診斷** - 如果 SonicPoint 或內部無線發生故障並重新啟動，則列出記錄資料。預設選擇此選項。

  附註：此核取方塊只有在 SonicWall 存取點已啟用或裝置有內部無線的情況下才能使用。

- **目前使用者** - 列出目前登入的所有使用中的本機和遠端使用者。預設選擇此選項。

  附註：若要報告最多的使用者資訊，請同時勾選**目前使用者**和**使用者詳細資料**核取方塊。

- **非使用中使用者** - 列出所有含非使用中工作階段的使用者。預設選擇此選項。
- **使用者詳細資料** - 列出使用者工作階段的附加詳情，包括定時器、權限、管理模式（若管理）、群組成員、CFS 原則、VPN 用戶端網路及其他資訊。必須先啟用**目前使用者**報告核取方塊才能獲得此詳細報告。預設選擇此選項。
- **IP 堆疊資訊** - 預設情況下未勾選此選項。
- **DNS 代理快取** - 預設情況下未勾選此選項。
- **IPv6 NDP** - 預設情況下未勾選此選項。
- **IPv6 DHCP** - 預設情況下未勾選此選項。
- **Geo-IP/Botnet 快取** - 儲存目前已快取的 Geo-IP 和 Botnet 資訊。預設情況下未勾選此選項。

- **擷取 ATP 快取** - 儲存目前已快取的擷取資訊。
- **供應商名稱解析** - 預設情況下未勾選此選項。
- **報告中的 Debug 資訊** - 指定下載的 TSR 是否包含偵錯資訊。預設選擇此選項。

  TSR 以一種易於閱讀的格式進行組織。您可以控制是否包含偵錯資訊做為一個類別。偵錯資訊在報告末尾使用 `#Debug Information_START` 和 `#Debug Information_END` 標記括住。偵錯資訊包含一般支援工程師不使用的雜項資訊，但在某些情況下可能很有用。

2 按一下**下載報告**，將檔案儲存到您的系統中。按一下**下載報告**時，將會顯示警告訊息。

3 按一下**確定**儲存檔案。

4 將報告附加到**技術支援請求**電子郵件中。

5 若要將 TSR、系統喜好設定檔案和追蹤記錄傳送到 SonicWall 工程部門（而不是 SonicWall 技術支援部門），請按一下**傳送診斷報告給技術支援**。

> **附註：**TZ 系列裝置不支援最後追蹤記錄。然而，重新啟動情況下保留目前記錄，關閉電源則不保留。TZ 系列裝置的目前記錄包含的資訊類似於 NSA 及更新裝置的最後記錄。

傳送報告時，介面底部的**狀態**指示器將顯示請稍候！，然後顯示診斷報告傳送成功。您通常在與技術支援人員交談後執行此操作。

6 若要傳送診斷檔案到 SonicWall 技術支援進行當機分析，請勾選**安全的自動故障分析報告**核取方塊。預設情況下已核取此選項。

7 定期向 MySonicWall 傳送 TSR、系統喜好設定檔案和追蹤記錄以聯絡 SonicWall 工程部的步驟是：

  a 勾選**支持目的的定期安全的診斷報告**核取方塊。預設情況下已核取此選項。

  b 在**時間間隔（分鐘）**欄位中輸入定期報告之間的時間間隔（以分鐘為單位）。預設值為 **1440** 分鐘（24 小時）。

8 如需在 TSR 中包含流量表資料，請選擇**當傳送診斷報告時應包含原始的流量資料表格**。預設情況下未勾選此選項。

診斷工具概觀

SonicWall 提供一系列診斷工具，協助您解決許多您可能面臨的一般問題。每個工具彼此不同，所以顯示會隨工具而變動。不過，有些資料管理功能在工具間通用。

幾乎所有工具都在視窗底部有以下按鈕：

按鈕	功能
接受	儲存任何您對診斷支援報告或診斷工具進行的變更。
取消	快取任何您最初對診斷支援報告或診斷工具進行的變更。
重新整理	重新整理顯示在**診斷工具**部分中的資料。

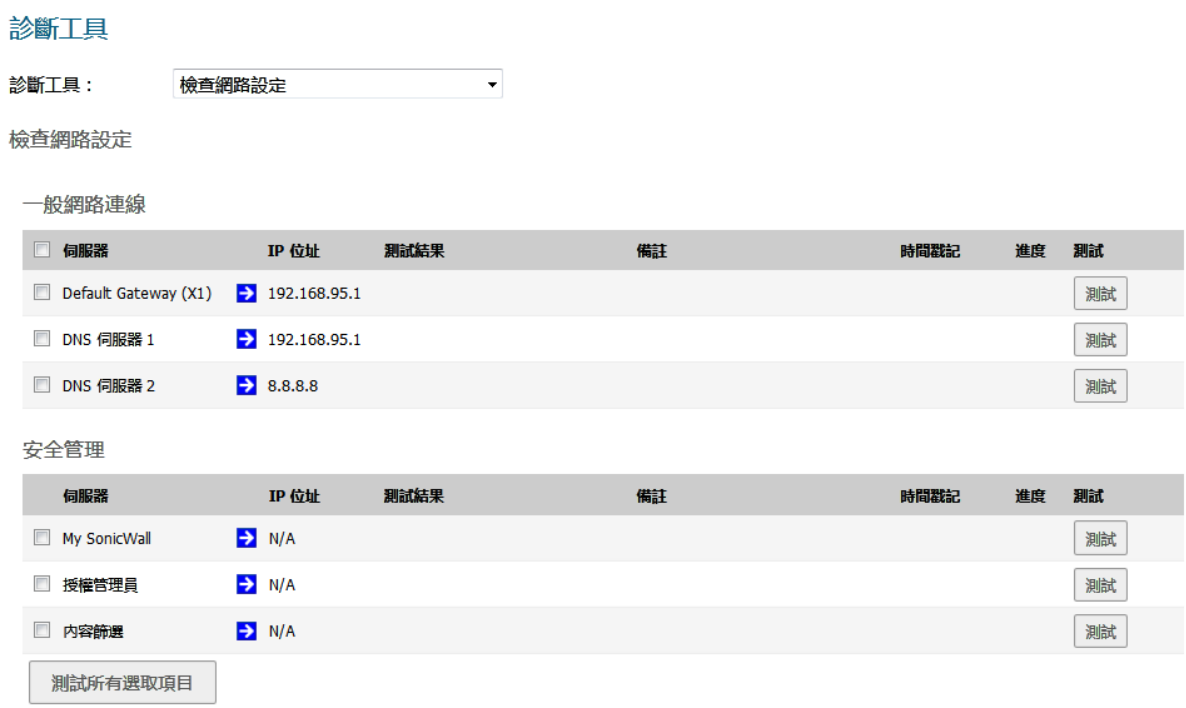
部分工具包含管理工具，可協助您管理資料清單。這些工具會操作類似其他記錄和報告上的選項。

- 搜尋
- 篩選

- 在檢視 (例如 IPv4 和 IPv6) 間切換。
- 重新整理
- 匯出
- 清除

從**工具 | 系統診斷**頁面的**診斷工具**下拉功能表中選擇工具。

檢查網路設定



檢查網路設定是一項診斷工具，用於自動檢查 SonicOS 多個預先定義功能區的網路連接和服務可用性，返回檢查結果，以及在偵測到任何異常時嘗試描述原因。此工具可幫助您在使用者遇到網路問題時查找問題。

具體而言，**檢查網路設定**會自動測試以下功能：

- 預設閘道設定
- DNS 設定
- MySonicWall 伺服器連接性
- 授權管理員伺服器連接性
- 內容篩選條件伺服器連接性

返回封包括兩個部分：

- **測試結果** - 提供測試結果摘要
- **注釋** - 提供詳細資料，以幫助管理員在存在任何問題時確定原因

「檢查網路設定」工具依賴於**調查**檢視的**工具 | 網路探查**上提供的**網路監視器**功能。每當執行**檢查網路設定**工具時（內容篩選條件測試時除外），**工具 | 網路探查**頁面都會顯示相應的網路監視器原則，以及專用的診斷工具原則名稱，而名稱格式為：

```
diagTestPolicyAuto_<IP_address/Domain_name>_0
```

附註：記錄訊息顯示一些特殊網路物件的上/下狀態。但是，這些物件的存在時間只有三秒，然後將自動刪除。

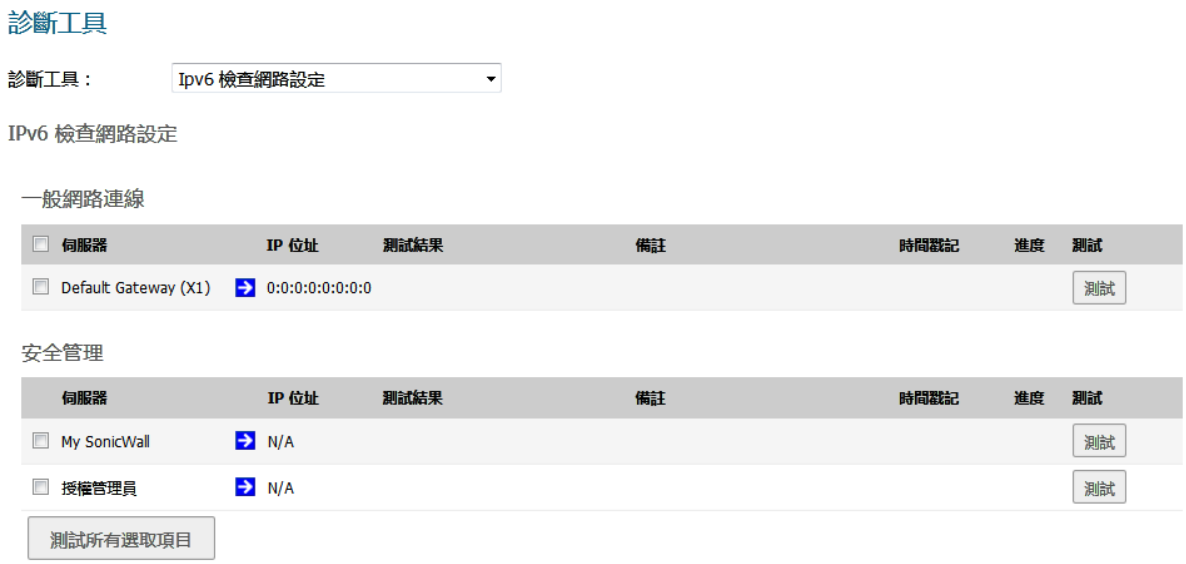
若要使用**檢查網路設定**工具，請先在**診斷工具**下拉清單中選擇此工具，然後按一下想要測試的項目對應行中的**測試**按鈕。結果將顯示在相同行中。綠色複選標記表示測試成功，紅色 X 表示測試出現問題。

若要同時測試多個項目，請勾選每個所需項目的核取方塊，然後按一下**測試所有選取項目**。

如果探查失敗，您可以按一下失敗項目的 **IP 位址**欄位左側的藍色箭頭，跳至設定頁面來調查根本原因。

IPv6 檢查網路設定

IPv6 檢查網路設定是診斷工具，測試防火牆是否支援 IPv6。



此工具會檢查各種連線，例如一般網路連線和安全管理，並顯示結果：

- **伺服器**
- **IP 位址**
- **測試結果**
- **備註**
- **時間戳記**
- **進度**

若要測試 IPv6 設定：

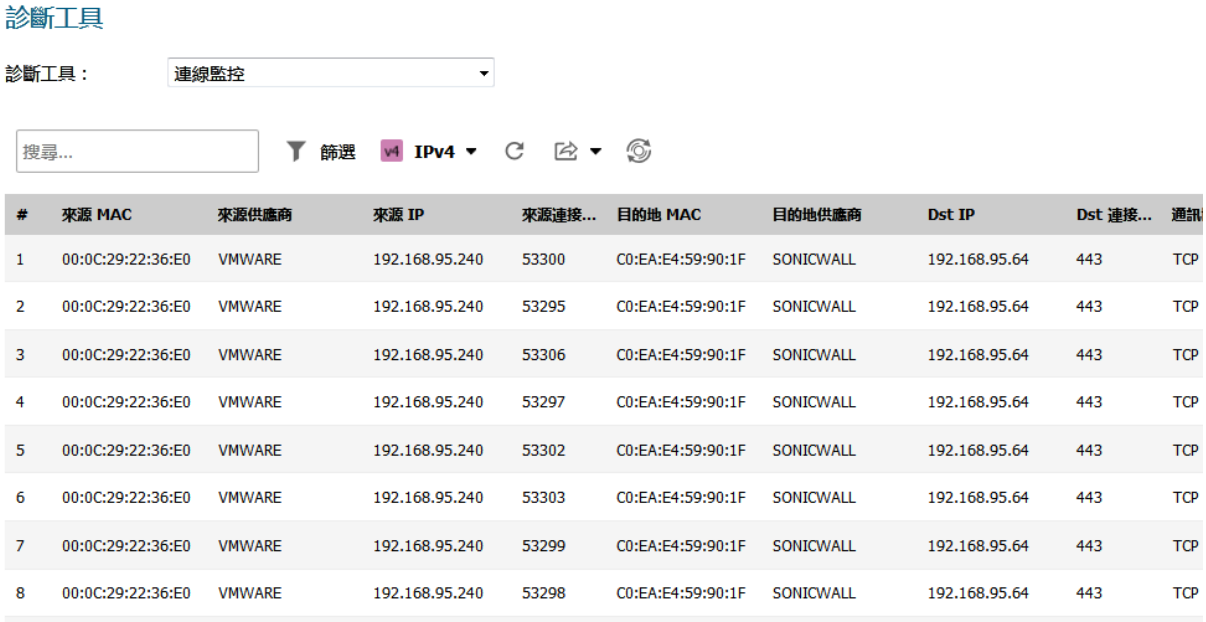
1 從**診斷工具**下拉功能表選擇 **Ipv6 檢查網路設定**。

2 若要測試：

- 單一連線，請按下其**測試**按鈕。
- 從任何或所有表格的兩個以上連線，勾選該連線的核取方塊，然後按下**測試所有選取項目**。

連線監控

連線監控顯示所有連接到防火牆的連線以及通過防火牆連接的即時、可匯出（純文字或 CSV）、可篩選的檢視。



#	來源 MAC	來源供應商	來源 IP	來源連接...	目的地 MAC	目的地供應商	Dst IP	Dst 連接...	通訊
1	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53300	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
2	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53295	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
3	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53306	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
4	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53297	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
5	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53302	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
6	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53303	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
7	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53299	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
8	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53298	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP

主題：

- 連線監控設定
- 連線監控資料

連線監控設定

可以對結果進行篩選，以便僅顯示符合指定準則的連接。

若要輸入篩選條件：

1 導覽至**調查**檢視上的**工具 | 系統診斷**。

2 在**診斷工具**欄位中，從下拉功能表選擇**連線監控**。

3 按一下**篩選**。

4 在您要篩選的欄位中輸入值。**來源位址**、**目的地位址**、**目的地連接埠**、**通訊協定**、**流量類型**、**來源介面**和**目的地介面**。

您在其中輸入值的欄位將會組合為包含邏輯 **AND** 的搜尋字串。搜尋字串會顯示在**篩選條件邏輯**欄位中。例如，如果在**來源 IP** 和**目的地 IP** 中輸入值，則搜尋字串將查找符合的連接：

```
Source IP AND Destination IP
```

5 勾選任意兩項或多項條件旁邊的**群組篩選條件**核取方塊可以將這些條件使用邏輯 **OR** 進行組合。

例如，如果在**來源位址**、**目的地位址**和**協定**中輸入值，然後勾選**來源位址**和**目的地位址**旁的**群組篩選條件**，搜尋字串將查找符合：

（*來源 IP 或目的地 IP*）和協定的連接。

6 按一下**接受**套用篩選條件。

7 按一下**重設**以清除篩選條件，然後再次顯示未篩選的結果。

可以將使用中連結清單匯出到檔案中。按一下**匯出**圖示，並選擇要將結果匯出為純文字檔或 CSV 檔案。如果系統提示打開或儲存檔案，請選擇**儲存**。然後輸入檔案名稱和路徑，並按一下**確定**。

連線監控資料

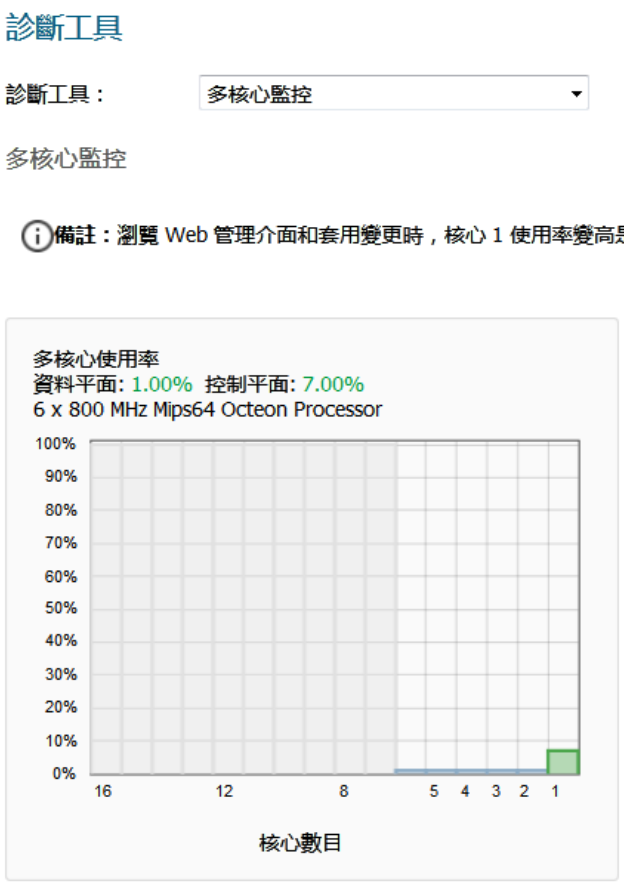
#	來源 MAC	來源供應商	來源 IP	來源連接...	目的地 MAC	目的地供應商	Dst IP	Dst 連接...	通訊
1	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53335	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
2	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53334	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
3	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53337	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
4	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53332	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
5	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53333	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
6	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53336	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP
7	00:0C:29:22:36:E0	VMWARE	192.168.95.240	53331	C0:EA:E4:59:90:1F	SONICWALL	192.168.95.64	443	TCP

連線監控表格顯示所有使用中連線的相關資訊。**來源 MAC**、**來源供應商來源 IP**、**來源連接埠**、**目的地 MAC**、**目的地供應商**、**目的地 IP**、**目的地連接埠**、**通訊協定**、**來源介面**、**目的地介面**、**流量類型**、**IPS 類別**、**過期（秒）**、**傳輸位元組**、**接收位元組**、**傳輸封包**、**接收封包**。按一下列標題可按此列排序。您也可以搜尋該資料表中的特定字串。

若要重新整理資料，按一下表格上方的**重新整理**圖示。您可以通過按一下**排清**列中的**刪除**圖示來排清每個連接。

多核心監控

多核心監控頁面顯示關於 SonicWall 安全裝置各個核心利用率的動態更新統計資料。



如果您的系統針對高可用性而設定，會顯示主要和次要防火牆的核心。若要並排檢視兩個監視器，請按下第一個監視器標頭中的小三角形。

核心監控

核心監控頁面顯示關於 SonicWall 安全裝置單個指定核心利用率的動態更新統計資料。**檢視樣式**提供可以顯示的較寬範圍的時間間隔，以查看核心使用情況。

連結監控

連結監控顯示防火牆介面的頻寬利用率。頻寬利用率顯示為總容量的百分比。可以設定連結監控顯示裝置上每個實體介面的傳入流量、傳出流量或同時顯示兩者。

封包大小監控

封包大小監控顯示防火牆介面上的封包大小。可以選擇四個時段，範圍從最近 30 秒到最近 30 天。可以設定封包大小監控顯示裝置上每個實體介面的傳入流量、傳出流量或同時顯示兩者。

若要設定封包大小監控：

1 在**檢視樣式**下拉功能表中選擇以下選項之一：

- **最近 30 秒**
- **最近 30 分鐘**
- **最近 24 小時**
- **最近 30 天**

2 從**介面名稱**下拉功能表中選擇要查看的實體介面。

3 在**方向**下拉功能表中選擇以下選項之一：

- **雙向** - 選擇在傳入和傳出方向傳送的封包
- **輸入** - 選擇到達介面的封包

- **輸出** - 選擇離開介面的封包

封包顯示在「平均封包大小」圖中，其中 X 軸指定封包經過介面的時間，Y 軸指定此時間點的平均封包大小。輸入封包顯示為綠色，輸出封包顯示為紅色。

DNS 名稱查詢

DNS 查詢工具會傳回網域名稱的 IPv4 和/或 IPv6 IP 位址，或網域的 IP 位址。如果輸入 IPv4 和/或 IPv6 IP 位址，工具會傳回該位址的網域名稱。如果輸入網域名稱，工具會傳回所使用的 DNS 伺服器和解析的位址。

您可以使用 **DNS 伺服器**選項按鈕，選擇**系統**或**已自訂** DNS 伺服器。選項會有改變，具體取決於您所選擇的項目。

IPv4/IPv6 DNS 伺服器欄位顯示在防火牆上設定的 DNS 伺服器的 IP 位址。如果欄位中沒有 IP 位址 (IPv4 為 `0.0.0.0` 或 IPv6 的 `::`)，則必須在**網路 > 設定**頁面中進行設定。

類型下拉功能表可任您指定：

- **IPv4** (預設值)，僅解析 IPv4 網域名稱。
- **IPv6**，僅解析 IPv6 網域名稱。
- **全部**，解析兩種類型的網域名稱。

重要：指定網域名稱時，不要將 *http* 或 *https* 加入名稱中。

防火牆將查詢 DNS 伺服器，並在**結果**部分顯示結果。

主題：

- 解析系統 DNS 伺服器
- 解析已自訂的 DNS 伺服器

解析系統 DNS 伺服器

若要解析系統 DNS 伺服器：

1 為 DNS 伺服器選擇**系統**。

2 在**查詢名稱或 IP** 欄位輸入要解析的網域名稱或 IP 位址。

3 從**類型**下拉功能表選擇 DNS 伺服器的 IP 類型。

- **IPv4**（預設）
- **IPv6**
- 全部 (IPv4 和 IPv6)

4 按一下**執行**。防火牆將傳回符合的位址和網域名稱對。

解析已自訂的 DNS 伺服器

若要解析已自訂的 DNS 伺服器：

1 選擇**已自訂**作為 **DNS 伺服器**。

2 如果 DNS 伺服器 IP 位址尚未填入，請在 IPv4 或 IPv6 欄位中輸入。

3 在**查詢名稱或 IP** 欄位輸入要解析的網域名稱或 IP 位址。

4 從**類型**下拉功能表選擇 DNS 伺服器的 IP 類型。

- **IPv4**（預設）
- **IPv6**
- 全部 (IPv4 和 IPv6)

5 按一下**執行**。至於系統 DNS 伺服器防火牆傳回相同資訊。

查找網路路徑

輸入一個 IP 位址，以確定網路路徑是否位於特定的網路介面上，能否到達路由器閘道 IP 位址，以及能否通過乙太網路位址到達。

Ping

Ping 測試從網際網路上的電腦中彈回一個封包並返回給傳送者。此測試顯示防火牆能否聯絡遠端主機。如果 LAN 中的使用者在存取網際網路服務時遇到問題，請嘗試 ping DNS 伺服器或位於 ISP 位置的其他電腦。如果測試不成功，則嘗試 ping ISP 以外的裝置。如果可以 ping 通 ISP 以外的裝置，則表明 ISP 連接存在問題。

1 從**診斷工具**功能表中選擇 **Ping**。

2 輸入目標裝置的 IP 位址或主機名稱。

3 在**介面**下拉功能表中，選擇想要從哪個 WAN 介面測試 ping。選擇**任何**將允許裝置在所有介面中做出選擇 - 包括未在下拉功能表中列出的介面。

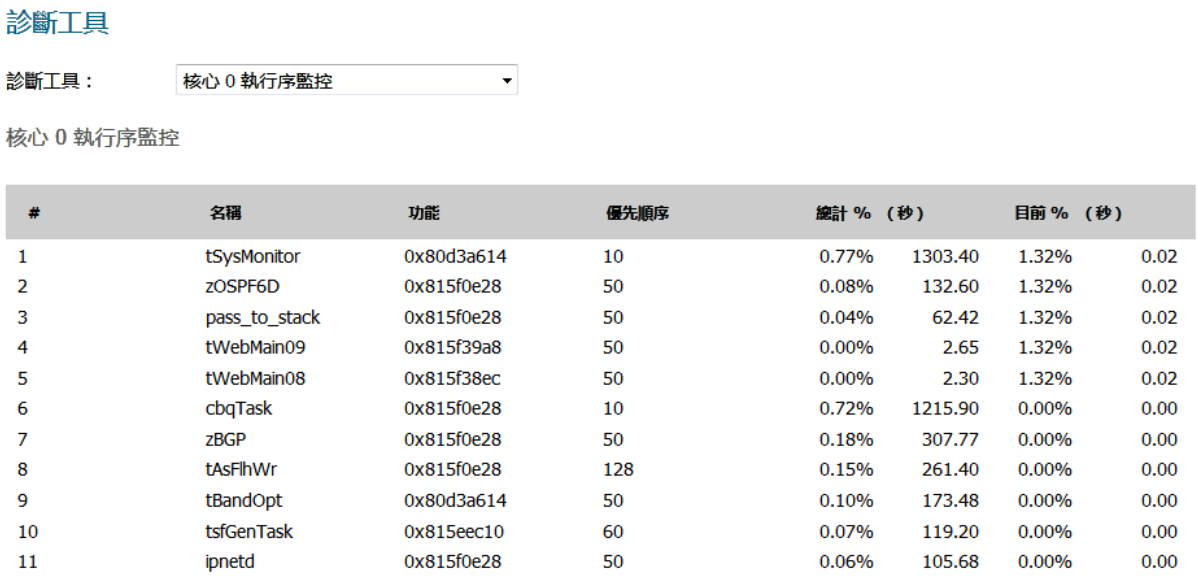
4 如果要 **IPv6 網路優先**，請勾選方塊。

5 按一下**執行**。

如果測試成功，防火牆將返回一條訊息，說明此 IP 位址為活動位址，並顯示返回時間（以毫秒 (ms) 為單位）。

核心 0 執行序監控

核心 0 執行序監控顯示核心 0 上的單獨系統進程、其 CPU 利用率及其系統時間。多核心 SuperMassive 9000 系列和多核心 NSA 系列裝置提供了**核心 0 執行序監控**。

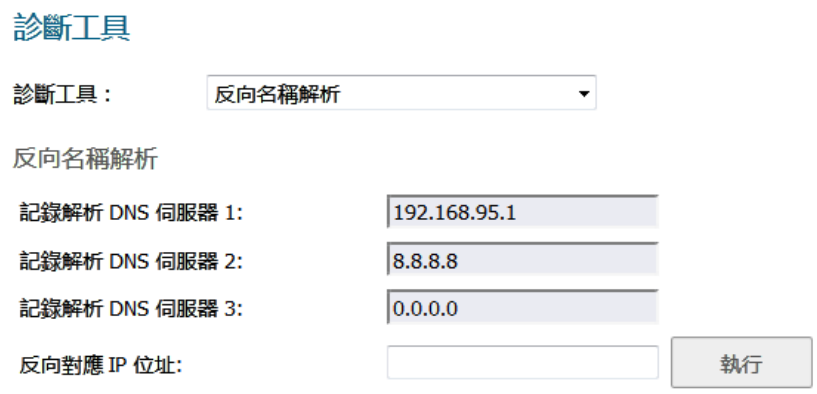


即時黑名單查詢

即時黑名單查詢工具用於測試 SMTP IP 位址、RBL 服務或 DNS 伺服器。在「IP 位址」欄位中輸入 IP 位址，在「RBL 網域」欄位中輸入 RBL 的 FQDN，以及在「DNS 伺服器」欄位中輸入 DNS 伺服器資訊。按一下**執行**。

反向名稱解析

反向名稱解析工具與 DNS 名稱查詢工具相似，不同之處在於它通過給定的 IP 位址查找伺服器名稱。



在**反向對應 IP 位址**欄位中輸入 IP 位址，此工具將查看為您的安全裝置設定的所有 DNS 伺服器，從而將此 IP 位址解析為伺服器名稱。

連線限制前 X

連線限制前 X 工具按照來源 IP 位址和目的地 IP 位址列出排名前 10 的連接。在使用此工具之前，必須為您的裝置啟用來源 IP 限制和/或目的地 IP 限制。如果沒有啟用這些選項，此頁面將顯示一條訊息，提示您可在哪裡啟用。

檢查 GEO 位置和 BOTNET 伺服器查詢

GEO 位置和 Botnet 伺服器查詢功能允許您基於 IP 位址封鎖與某個地理位置之間的連接，以及封鎖與 Botnet 命令和控制伺服器之間的連接。在**管理**檢視上，**安全設定 | 安全服務 > Geo-IP 篩選**頁面和 **Botnet 篩選**頁面下還提供了此工具的其他功能。更多資訊請參閱 *SonicWall SonicOS 6.5 安全設定*。

若要進行 GEO 位置和 BOTNET 伺服器查詢的故障排除：

1 從**診斷工具**下拉功能表選擇 **GEO位置和 BOTNET 伺服器查詢**。

2 在**查詢 IP** 欄位中輸入目的地主機的 IP 位址或網域名稱。

3 按一下**執行**。結果會顯示在**查詢 IP** 欄位下。

追蹤路由

TraceRoute (追蹤路由) 是一項診斷公用程式，用於協助診斷和排除網際網路中的路由器連接問題。透過使用與 Ping 封包相似的網際網路 UDP 封包，**TraceRoute** 可測試與路由器和其他沿網路路徑越來越遠的主機之間的互連性，直至連接失敗或遠端主機發出回應。

追蹤路由工具包含一個新的 **IPv6 網路優先**選項。利用路由器和其他主機測試互連時，SonicOS 使用返回的第一個 IP 位址，並顯示實際的追蹤路由位址。如果同時返回 IPv4 和 IPv6 位址，防火牆預設追蹤路由 IPv4 位址。如果 **IPv6 網路優先**選項啟用，防火牆將追蹤路由 IPv6 位址。

若要對追蹤路由進行故障排除：

1 從**診斷工具**下拉功能表選擇 **TraceRoute**。

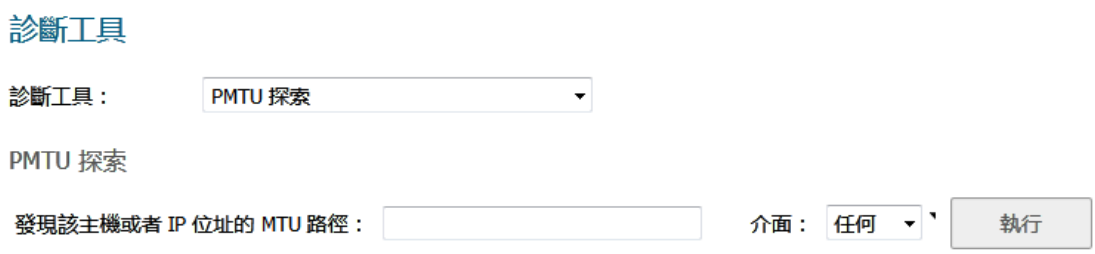
2 在**追蹤此主機或 IP 位址的路由**欄位中輸入目的地主機的 IP 位址或網域名稱。

3 在**介面**下拉功能表中，選擇想要從哪個 WAN 介面測試追蹤路由。選擇**任何**將允許裝置在所有介面中做出選擇 - 包括未在下拉功能表中列出的介面。

4 如需 IPv6 的 TraceRoute，請勾選 **IPv6 網路優先**核取方塊。

5 按一下**執行**。依路由而定，這可能需要幾分鐘時間。快顯表格會顯示到目的地主機的每個轉接段。通過追蹤路由，可以診斷防火牆與目的地之間的連接發生故障的位置。

PMTU 探索



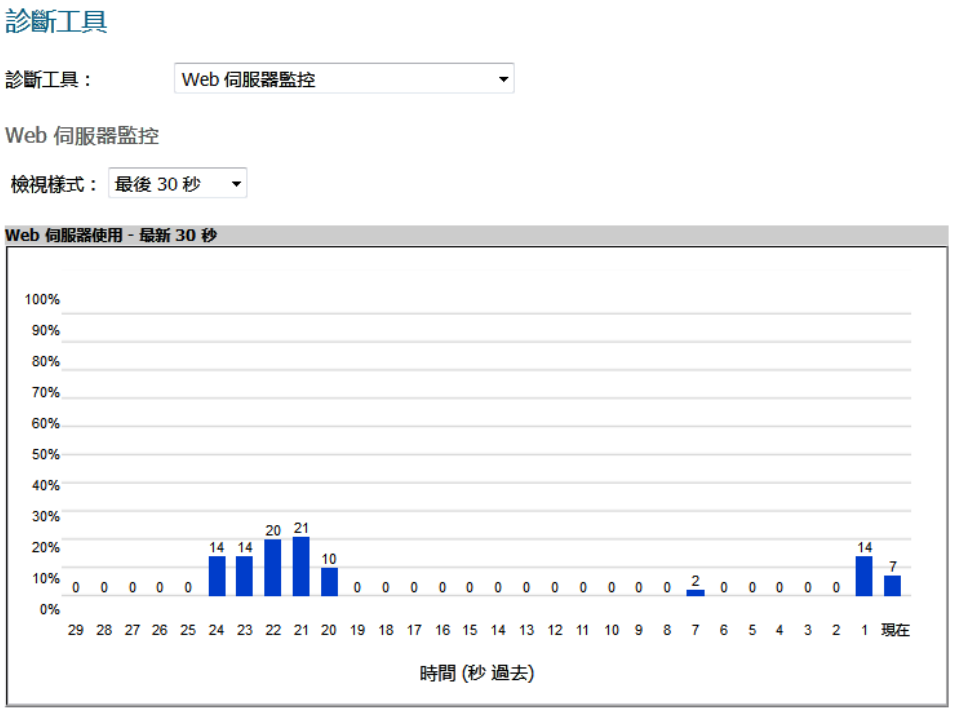
PMTU 探索是一項診斷工具，使用標準化技術來決定兩個網際網路通訊協定 (IP) 主機間網路路徑上的最大傳輸單元 (MTU) 大小，通常目的是為了避免 IP 分段。PMTU 探索適用於 IPv4 和 IPv6。

若要對 PMTU 探索進行故障排除：

1. 從**診斷工具**下拉功能表選擇 **PMTU 探索**。
2. 在**發現該主機或者 IP 位址的 MTU 路徑**欄位中輸入目的地主機的 IP 位址或網域名稱。
3. 在**介面**下拉功能表中，選擇想要從哪個 WAN 介面測試追蹤路由。選擇**任何**將允許裝置在所有介面中做出選擇 - 包括未在下拉功能表中列出的介面。
4. 按一下**執行**。

   依路由而定，這可能需要幾分鐘時間。快顯表格會顯示到目的地主機的每個轉接段。通過追蹤路由，可以診斷防火牆與目的地之間的連接發生故障的位置。

Web 伺服器監控



Web 伺服器監控工具會顯示 Web 伺服器隨時間的 CPU 利用率。

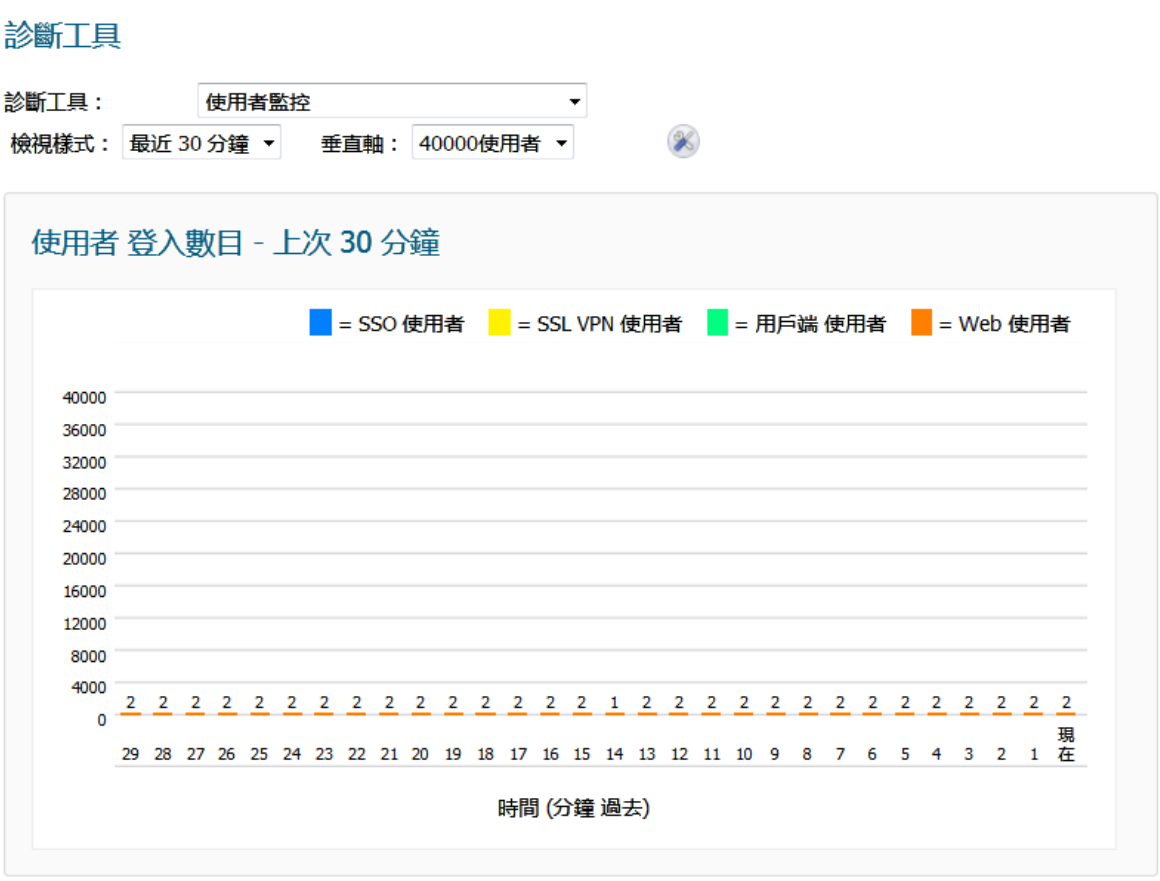
若要對 Web 伺服器監控進行故障排除：

1 從**診斷工具**下拉功能表選擇 **Web 伺服器監控**。

2 從**檢視樣式**下拉功能表中選擇顯示的時間段：

- **最近 30 秒**（預設）
- **最近 30 分鐘**
- **最近 24 小時**
- **最近 30 天**

使用者監控



使用者監控工具會顯示隨時間登入的使用者數量。

若要對使用者監控進行故障排除：

1 從**診斷工具**下拉功能表選擇 **使用者監控**。

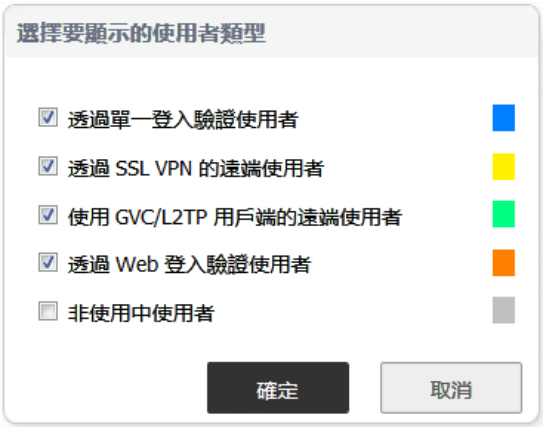
2 從**檢視樣式**下拉功能表中選擇顯示的時間段：

- **最近 30 秒**（預設）

- 最近 30 分鐘
- 最近 24 小時
- 最近 30 天

3 從**垂直軸**下拉功能表中，為垂直軸選擇最大使用者數量。

4 若要指定要顯示的使用者類型，請按一下**設定**圖示。即顯示快顯功能表。



附註：顯示的使用者類型會依使用者登入的方式而定，例如，您若不使用 SSL VPN，該選項就不會顯示。

a 勾選要顯示之使用者類型的核取方塊。

b 清除要隱藏之使用者類型的核取方塊。

c 按一下**確定**。

交換器診斷

交換器診斷工具會顯示與介面關聯之交換器的狀態和計數器。

若要對交換器診斷進行故障排除：

1 從**診斷工具**下拉功能表選擇 **交換器診斷**。

2 從**介面名稱**下拉功能表中選擇介面。

16

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
- 下載軟體
- 檢視視訊教學
- 與使用者論壇中的同儕和專家們協同合作
- 取得授權協助
- 存取 MySonicWall
- 瞭解 SonicWall 專業服務
- 註冊培訓和認證

若要聯絡 SonicWall 支援，請參閱 https://www.sonicwall.com/support/contact-support。

若要檢視 SonicWall 最終使用者產品合約 (EUPA)，請參閱 https://www.sonicwall.com/legal/eupa.aspx。根據您的地理位置選擇語言以查看適用您所在地區的 EUPA。