SonicWall® SonicOS 6.5 連線能力

管理

SONICWALL®

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

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

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

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

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 連線能力
更新時間 - 2018 年 1 月
軟體版本 - 6.5
232-004132-00 修訂版 B

目錄

VPN 概述 12
VPN 概述 12
VPN 類型 13
IPsec VPN 13
DHCP over VPN 13
採用 IPsec 的 L2TP 14
SSL VPN 14
VPN 安全性 15
VPN 設定和顯示 15
VPN 全域設定 16
VPN 原則 17
目前使用中的 VPN 通道 18
VPN 自動新增的存取規則控制 18

站台對站台 VPN 20
規劃站台對站台設定 20
一般 VPN 設定 21
一般 22
網路 23
建議: 23
進階標籤 24
管理 GroupVPN 原則 26
設定使用預先共用密碼的 IKE 26
設定使用供應商憑證的 IKE 31
匯出 VPN 用戶端原則 35
建立站台對站台 VPN 原則 37
以預先共用密碼進行設定 37
以手動金鑰進行設定 43
以供應商憑證進行設定 47
設定遠端 SonicWall 網路安全裝置 54
設定 VPN 容錯移轉到固定路由 56

VPN 自動佈建 57
關於 VPN 自動佈建 57
至關重要的 SonicOS VPN 自動佈建 57
SonicOS VPN 自動佈建的優點 58
SonicOS VPN 自動佈建的運作方式 58
支援的平台 60
設定 VPN 存取點伺服器 60
啟動 VPN 存取點伺服器設定 61
在一般標籤上設定 VPN 存取點伺服器設定 61

在網路標籤上設定 VPN 存取點伺服器設定 63
在建議標籤上設定進階設定 64
在進階標籤上設定進階設定 66
設定 VPN 存取點用戶端 67

路由式 VPN 70
術語 70
使用基於路由的 VPN 71
新增通道介面 71
為通道介面建立靜態路由 75
網路的備援靜態路由 75

設定進階 VPN 設定 76
設定進階 VPN 設定 77
設定 IKEv2 設定 78
OCSP 配合 SonicWall 網路安全裝置使用 79
OpenCA OCSP 回應者 80
載入憑證以使用 OCSP 80
OCSP 配合 VPN 原則使用 80

設定 VPN 上的 DHCP 81
DHCP 轉接模式 81
針對 VPN 上的 DHCP 設定中心閘道 81
設定 VPN 上的 DHCP 的遠端閘道 82
目前 VPN 上的 DHCP 租用 84

設定 L2TP 伺服器和 VPN 用戶端存取 85
設定 L2TP 伺服器 85
查看目前使用中的 L2TP 工作階段 87
設定 Microsoft Windows L2TP VPN 用戶端存取 87
設定 Google Android L2TP VPN 用戶端存取 89

關於 SSL VPN 93
關於 NetExtender 93
建立 NetExtender 範圍的位址物件 94
設定存取權限 95
設定代理 95
安裝獨立用戶端 96
設定使用者的 SSL VPN 存取 96
針對本機使用者 96
針對 RADIUS 和 LDAP 使用者 97
針對 Tunnel All 模式存取 97
生物識別驗證 97

設定 SSL VPN 伺服器行為 99

區域上的 SSL VPN 狀態 100
SSL VPN 伺服器設定 100
RADIUS 使用者設定 101
SSL VPN 用戶端下載 URL 101

設定 SSL VPN 用戶端設定 102
設定預設裝置設定檔 102
設定 SonicPoint L3 管理預設裝置設定檔 106

設定 SSL VPN Web 入口網站 109
入口網站設定 110
入口商標設定 110

設定虛擬辦公室 111
存取虛擬辦公室入口網站 111
設定 SSL VPN 書籤 112
設定用於 IPv6 的裝置設定檔設定 114

瞭解 SonicWall 存取點 116
存取點功能矩陣 116
存取點功能 117
SonicPoint/SonicWave 功能 118
認證與合規性 119
存取點樓面規劃檢視 119
存取點拓撲檢視 120
入侵偵測/防護 120
虛擬存取點 120
存取點 WMM 設定 121
日本和國際存取點支援 121
規劃與實地調查 121
前提條件 121
站台調查和規劃 122
PoE 和 PoE+ 123
存取點部署最佳做法 124
基礎結構中的交換器 124
接線注意事項 126
頻道 126
產生樹狀目錄 126
VTP 和 GVRP 轉接通訊協定 126
連接埠彙總 126
PortShield 126
廣播限制/廣播風暴 127
速度和雙工 127
SonicPoint 自動佈建 127

存取點授權 128
SonicWave 授權 128
授權狀態 129
手動授權更新 129
自動授權更新 130
管理 SonicPoints 之前 130
更新 SonicPoint 韌體 130
重設 SonicPoint 131
存取點和 RADIUS 計費 131
設定 Radius 計費伺服器 132

存取點儀表板 133
功能限制 134
存取點快照 134
存取點連線/離線 134
用戶端關聯 134
即時頻寬 135
用戶端報告 135
OS 類型 135
熱門用戶端 135
即時用戶端監控 136

存取點基本設定 137
佈建概述 137
建立/修改佈建設定檔 138
佈建設定檔的一般設定 139
佈建設定檔的無線 0/1 基本設定 141
佈建設定檔的無線 0/1 進階設定 149
感應器 151
3G/4G/LTE WWAN 151
特定產品的設定須知 156
管理存取點 156
同步存取點 156
刪除存取點設定檔 156
刪除 SonicPoint/SonicWave 物件 157
重新啟動 SonicPoint/SonicWave 物件 157
修改 SonicPoint/SonicWave 物件 158

存取點樓面規劃 159
管理樓面規劃 159
選擇樓面規劃 160
建立樓面規劃 160
編輯樓面規劃 161
設定測量比例 162

管理存取點 163
可用存取點 163
已新增存取點 163
移除存取點 163
匯出影像 164
操作功能表 164

存取點拓撲檢視 165
管理拓撲檢視 165
在拓撲檢視中管理存取點 166
編輯存取點 166
顯示統計資料 167
監控存取點的狀態 167
刪除存取點 168

設定 SonicPoint 入侵偵測服務 170
掃描存取點 171
授權存取點 172

設定進階 IDP 173
對設定檔啟用進階 IDP 173
設定進階 IDP 174

存取點封包擷取 176

設定虛擬存取點 178
設定 VAP 之前 179
確定您的虛擬存取點需求 180
確定安全設定 180
網路定義範例 180
前提條件 180
VAP 設定工作表 181
存取點 VAP 設定任務清單 182
虛擬存取點設定檔 183
虛擬存取點排程設定 185
虛擬存取點設定檔設定 185
強制啟用 ACL 187
遠端 MAC 位址存取控制設定 188
虛擬存取點 188
虛擬存取點群組 190

設定 RF 監控 192
前提條件 193
RF 監控摘要 193
802.11 一般框架設定 193

802.11 管理框架設定 194
802.11 資料框架設定 194
發現的 RF 威脅工作站 195
將威脅站台新增到監視清單中 196
實用型 RF 監控欄位應用程式 197
使用感應器 ID 確定 RF 威脅位置 197

設定 FairNet 200
支援的平台 200
FairNet 功能 201
管理介面概述 201
設定 FairNet 202

設定 Wi-Fi 多媒體 204
WMM 存取類別 204
將流量指派到存取類別 206
指定防火牆服務和存取規則 206
VLAN 標籤 206
設定 Wi-Fi 多媒體參數 206
設定 WMM 207
為存取點建立 WMM 設定檔 208
刪除 WMM 設定檔 208

存取點 3G/4G/LTE WWAN 209

無線概述 212
裝置支援 212
合規性 213
FCC U-NII 新規則合規 213
RED 合規性 213
使用無線連接的考慮事項 213
最佳化無線效能建議 213
調節天線 214
無線節點計數實施 214
MAC 篩選條件清單 214

設定無線設定 215
存取點 215
存取點無線設定 216
存取點無線虛擬存取點 219
無線橋接 219
用戶端橋接無線設定 219
用戶端橋接進階無線設定 221
存取點與工作站 221

設定無線安全 224
關於驗證 224
設定 WEP 設定 225
設定 WPA2 PSK 和 WPA PSK 設定 226
WPA2 EAP 和 WPA EAP 設定 227

設定進階無線設定 229
訊號傳送和 SSID 控制 230
綠色存取點 230
進階無線設定 231
設定天線分極 232

無線 MAC 篩選條件清單 233
部署注意事項 233
設定無線 > MAC 篩選條件清單 234

設定無線 IDS 235
關於無線 IDS 235
存取點 IDS 235
欺詐存取點 235
設定 IDS 設定 236
IDS 設定 236
發現的存取點 238

設定使用內部無線的虛擬存取點 239
無線虛擬存取點設定任務清單 239
虛擬存取點設定檔 240
虛擬存取點排程設定 241
虛擬存取點設定檔設定 242
強制啟用 ACL 243
虛擬存取點 244
虛擬存取點一般設定 244
虛擬存取點進階設定 245
虛擬存取點群組 246
啟用虛擬存取點群組 247

3G/4G/數據機概述 249
選擇介面 249
了解 3G/4G 250
3G/4G 連接類型 250
SonicWave MiFi 延伸器 251
3G/4G 容錯移轉 251
3G/4G 前提條件 254
啟用 U0/U1/M0 介面 255

設定 3G/4G/數據機基本設定 256
設定 256
按需連接類別 257
管理/使用者登入 257
MiFi 延伸器設定 258

設定 3G/4G/數據機進階設定 259
遠端觸發撥出設定 259
頻寬管理 260
連接限制 260

設定 3G/4G/數據機連接設定檔 261
偏好設定檔 261
連接設定檔 261
一般設定 262
ISP 位址 263
參數設定 264
IP 位址 265
排程 265
資料限制 266
進階 267

監控 3G/4G 資料使用 268

VAP 樣本設定 270
為學校教職工存取設定 VAP 270
設定區域 270
建立新無線子網路 271
建立無線虛擬存取點設定檔 271
建立無線虛擬存取點 272
建立多個虛擬存取點 > 部署目前的虛擬存取點 272
向無線電波部署虛擬存取點 273
對多個虛擬存取點分組 273
將虛擬存取點群組與您的無線電波相關聯 273

SonicWall 支援 274
關於本文件 275

第 1 部分

VPN

- VPN 概述
- 站台對站台 VPN
- VPN 自動佈建
- 路由式 VPN
- 設定進階 VPN 設定
- 設定 VPN 上的 DHCP
- 設定 L2TP 伺服器和 VPN 用戶端存取

1

VPN 概述

VPN 選項提供設定和顯示 VPN 原則的功能。您可設定各種類型的 IPsec VPN 原則，例如站台對站台原則 (包含 GroupVPN) 和基於路由的原則。如需設定這類原則的具體詳細資訊，請參考以下章節:

- 站台對站台 VPN
- VPN 自動佈建
- 路由式 VPN

本章節提供 VPN 類型資訊、討論可供選擇的部分安全選項，並說明**管理**檢視上 **VPN > 基本設定**頁面的介面。後續章節則說明如何設定站台對站台和基於路由的 VPN、進階設定、VPN 上的 DHCP 和 L2TP 伺服器。

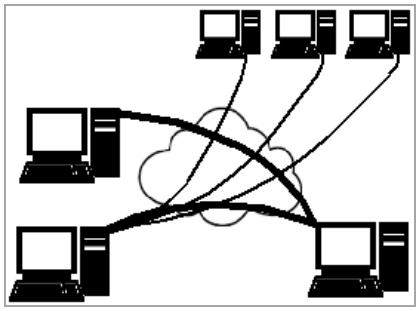
主題：

- VPN 概述
- VPN 類型
- VPN 安全性
- VPN 設定和顯示

VPN 概述

虛擬私人網路 (VPN) 通過公用網際網路在兩個或更多電腦或受防護網路之間提供安全連接。它提供身分驗證以確保資訊在正確的參與方之間往來。它也提供保護資料所需的安全性，防止傳輸途中資料遭檢視或竄改。

VPN 的建立方式為透過網際網路建立安全通道，這個通道是使用專屬連線、虛擬通道通訊協定或流量加密的虛擬點對點連線，且具有彈性，您可以隨時調整以增加更多節點、變更節點或完全移除節點。VPN 成本非常低，因為它使用現有網際網路基礎設施。



VPN 可支援遠端存取 (將使用者的電腦連接至公司網路) 或站台對站台 (連接兩個網路)。VPN 也可用於透過相異的中間網路互連兩個相似的網路: 例如透過 IPv4 網路連接兩個 IPv6 網路。

VPN 系統可分類為:

- 用於以通道傳送流量的通訊協定
- 通道的端點位置，例如位於客戶邊緣或網路供應商邊緣
- 連線拓撲類型，例如站台對站台或網路對網路
- 提供的安全層級
- VPN 系統為連接網路而呈現的 OSI 層，例如二層迴路或三層網路連線
- 同時連線數

VPN 類型

多種可設定以使用的 VPN 通訊協定類型:

- IPsec VPN
- DHCP over VPN
- 採用 IPsec 的 L2TP
- SSL VPN

IPsec VPN

SonicOS 支援建立和管理 IPsec VPN。這些 VPN 主要需在**管理**檢視的 **VPN > 基本設定**和 **VPN > 進階設定**上進行設定。

IPsec (網際網路通訊協定安全性) 是基於標準的安全性通訊協定，最初是針對 IPv6 所開發，不過也廣泛用於 IPv4 和二層通道通訊協定。其設計符合多數驗證的安全目標、完整性及機密性。IPsec 使用加密並將 IP 封包封裝到 IPsec 封包內。系統會在通道盡頭解除封裝，將原始 IP 封包解密並轉送至預定的目的地。

使用 IPsec 的優勢是安全設定的處理不需要變更個別使用者的電腦，且提供兩種安全服務類型:

- 驗證標頭 (AH)，本質上允許驗證資料傳送方。
- 封裝安全有效承載 (ESP)，支援傳送方驗證和資料加密。

您可使用 IPsec 建立基於原則的 VPN (站台對站台)，或是基於路由的 VPN 通道或二層通道通訊協定 (L2TP)

DHCP over VPN

SonicOS 可將防火牆設定為從 VPN 通道另一端的 DHCP 伺服器取得 IP 位址租用。在某些網路部署中，您希望將所有 VPN 網路置於一個邏輯 IP 子網路上，造成一種似乎所有 VPN 網路都位於同一 IP 子網路位址空間中的印象。這有利於使用 VPN 通道的網路的 IP 位址管理。

遠端和中心站台的防火牆針對初始 DHCP 流量及站台之間的後續 IP 流量的 VPN 通道進行設定。遠端站台的防火牆會通過其 VPN 通道傳遞 DHCP 廣播封包。中心站台的防火牆會將 DHCP 封包從遠端網路上的用戶端轉送到中心站台上的 DHCP 伺服器。

採用 IPsec 的 L2TP

二層通道通訊協定 (L2TP) 為一種通道通訊協定，用於支援 VPN 作為 ISP 服務交付的一部分。L2TP 本身不提供任何加密功能或機密性，且由於 L2TP 通訊協定缺乏機密性，故通常會和 IPsec 一起實作。設定 L2TP/IPsec VPN 的一般程序如下:

1 交涉 IPsec 安全關聯 (SA)，通常會透過網際網路金鑰交換 (IKE) 進行。此程序需經由 UDP 連接埠 500 執行，雖然存在其他金鑰方法，但一般會使用共用密碼 (也稱為*預先共用密碼*)、公開金鑰或兩端的 X.509 憑證。

2 在傳輸模式下建立封裝安全有效承載 (ESP) 通訊。ESP 的 IP 通訊協定號碼是 50 (TCP 為 6 而 UDP 為 17)。此時已建立安全頻道，但尚未進行通道傳送。

3 在 SA 端點間交涉和建立 L2TP 通道。實際的參數交涉是經由 SA 的安全頻道進行，且過程中使用 IPsec 加密。L2TP 使用 UDP 連接埠 1701。

程序完成時，會由 IPsec 封裝端點間的 L2TP 封包。由於 L2TP 封包本身經過封裝並隱藏在 IPsec 封包中，因此無法從加密的封包取得任何有關內部私人網路的資訊。此外，也不需要在端點間的防火牆上開啟 UDP 連接埠 1701，因為在解密和去除 IPsec 資料前 (只會在端點發生)，系統不會對內部封包執行任何動作。

SSL VPN

An SSL VPN (安全通訊端層虛擬私人網路) 是一種 VPN 形式，可搭配標準 Web 瀏覽器使用。SSL VPN 與傳統 IPsec VPN 相反，不需要在最終使用者電腦上安裝專用的用戶端軟體。可用於為遠端使用者提供 Web 應用程式、用戶端/伺服器用程式和內部網路連接的存取權。

SSL VPN 包含一或多個 VPN 裝置，使用者需使用 Web 瀏覽器來連接這些裝置。Web 瀏覽器和 SSL VPN 裝置之間的流量，會透過 SSL 通訊協定或其繼任者傳送層安全性 (TLS) 通訊協定進行加密。SSL VPN 提供多元功能、易於使用，且可精確控制使用各種電腦的各種使用者，便於從不同位置存取資源。SSL VPN 的兩種主要類型為:

- SSL 入口網站 VPN
- SSL 通道 VPN

SSL 入口網站 VPN 允許單一網站的 SSL 連接，讓最終使用者可安全存取多個網路服務。這個網站稱為入口網站，因為這是通往其他資源的入口 (單一頁面)。遠端使用者會任何現代 Web 瀏覽器存取 SSL VPN 閘道、使用閘道支援的驗證方法通過閘道驗證，然後進入一個作為其他服務入口的網頁。

SSL 通道 VPN 可讓 Web 瀏覽器透過在 SSL 下執行的通道，安全地存取多個網路服務，包含非基於 Web 的在內應用程式和通訊協定。SSL 通道 VPN 要求 Web 瀏覽器需能處理主動式內容，如此一來才能提供 SSL 入口網站 VPN 無法使用的功能。主動式內容的例子有 Java、JavaScript、Active X 或是 Flash 應用程式或外掛程式。

SSL 使用網際網路的超文字傳送協定 (HTTP) 層與傳送控制通訊協定 (TCP) 層之間的程式層。SSL 也採用 RSA 的公開金鑰/私人金鑰加密系統，其中還包含數位憑證。SRA/SMA 裝置利用 SSL 確保 VPN 通道安全性。SSL VPN 的一個優勢是多數 Web 瀏覽器已經內建 SSL。不需要特殊 VPN 用戶端軟體或硬體。

附註：SonicWall 讓您可以使用的 SRA/SMA 裝置與執行 SonicWall 的 SonicOS 網路安全裝置協調一致，或獨立於後者。如需 SonicWall SRA/SMA 裝置的資訊，請參閱 https://www.sonicwall.com/en-us/products。

VPN 安全性

IPsec VPN 流量透過兩個階段來保證安全：

1 **驗證**：第一階段利用公開金鑰/私人金鑰對的公開金鑰部分交換，確定流量傳送者和接收者的真實性。此階段成功後，VPN 通道才能建立。

2 **加密**：VPN 通道中的流量利用 AES 或 3DES 等加密演算法加密。

除非使用手動金鑰（必須將相同的金鑰輸入 VPN 中的各節點），用於認證 VPN 成員和加密/解密資料的資訊交換採用 Internet 金鑰交換 (IKE) 通訊協定來交換認證資訊（金鑰）並建立 VPN 通道。SonicOS 支援兩個版本的 IKE：

IKE 第 1 版 (IKEv1)	採用兩階段過程來確保 VPN 通道的安全性。首先，兩個節點互相進行驗證，然後交涉加密方法。 如需 IKEv1 的更多資訊，請參閱最初定義 IKE 的三個規格: RFC 2407、RFC 2408 和 RFC 2409，網站如下： • http://www.faqs.org/rfcs/rfc2407.html - *ISAKMP 解釋的網際網路 IP 安全網域* • http://www.faqs.org/rfcs/rfc2408.html - *RFC 2408 - 網際網路安全關聯和金鑰管理通訊協定 (ISAKMP)* • http://www.faqs.org/rfcs/rfc2409.html - *RFC 2409 - 網際網路金鑰交換 (IKE)*
IKE 第 2 版 (IKEv2)	此版的安全性提升、架構簡化且遠端使用者支援增強，因此為新 VPN 原則的預設類型。系統會使用一對訊息交換起始 VPN 通道。第一對訊息交涉加密演算法，交換 nonce（隨機產生並傳送的值，用以防止訊息重複），並執行公開金鑰交換。第二對訊息會驗證之前的訊息，交換身分和憑證，建立第一個 CHILD_SA。這些訊息的一部分經過加密，並利用第一個交換建立的金鑰來保護完整性，因此會隱藏身分以防止竊聽，訊息中的所有欄位都會經過驗證。 如需 IKEv2 的更多資訊，請參閱規範 RFC 4306，網站如下： http://www.ietf.org/rfc/rfc4306.txt。

重要：IKEv2 與 IKEv1 不相容。使用 IKEv2 時，VPN 中的所有節點都必須使用 IKEv2 建立通道。

IKEv2 不支援 VPN 上的 DHCP。

VPN 設定和顯示

VPN 頁面會根據選擇的選項提供一連串表格和設定。如需有關導覽表格和設定的資訊，請參閱*關於 SonicWall SonicOS 6.5*。

如需 **VPN > 基本設定**頁面的詳細資訊，請參閱以下章節:

- VPN 全域設定
- VPN 原則
- 目前使用中的 VPN 通道

VPN 全域設定

VPN > 基本設定頁面的**全域 VPN 設定**區段會顯示下列資訊:

啟用 VPN	選擇以透過 SonicWall® 安全原則啟用 VPN 原則。
唯一防火牆識別項	設定 VPN 通道時識別此 SonicWall 裝置。預設值為裝置的序號。可以將識別項變更為對您有意義的識別項。
檢視 IP 版本	設定 IP 版本檢視。選項有 **IPv4** 或 **IPv6**。

SonicWall VPN 同時支援 IPv4 和 IPv6 (網際網路通訊協定第 4 版和網際網路通訊協定第 6 版)。在視窗右上角選擇要使用的版本，便可在不同版本間切換。預設檢視為 IPv4。

VPN 原則

所有已定義的 VPN 原則都會顯示在 **VPN 原則**表中。每個項目顯示下列資訊：

- **名稱** - 預設名稱或使用者定義的 VPN 原則名稱。
- **閘道** - 遠端防火牆的 IP 位址。如果使用萬用字元 IP 位址 0.0.0.0，則它將顯示為 IP 位址。
- **目的地** - 目的地網路的 IP 位址。
- **金鑰套件** - 用於 VPN 原則的加密類型。
- **啟用** - 顯示原則是否已啟用。勾選方塊即可啟用 VPN 原則。清除方塊便可加以停用。
- **設定** - 用於管理個別 VPN 原則的選項:
  - **編輯**圖示用於編輯 VPN 原則。
  - **刪除**圖示會刪除該行上的原則。預先定義的 GroupVPN 原則無法刪除，因此其**刪除**圖示變暗。
  - **匯出**圖示可將 VPN 原則設定匯出為檔案，以便由 SonicWall 全域 VPN 用戶端在本機安裝。

下列按鈕會顯示在 **VPN 原則**表下方:

新增	存取 **VPN 原則**視窗以設定站台對站台 VPN 原則。
刪除	刪除所選原則 (需先勾選**名稱**欄中 VPN 原則名稱前的方塊)。無法刪除 GroupVPN 原則。
全部刪除	刪除 VPN 原則表中除預設 GroupVPN 原則以外的全部 VPN 原則。

與 VPN 原則 (站台對站台和 GroupVPN 原則) 有關的部分統計資料摘要也會列在表格下方:

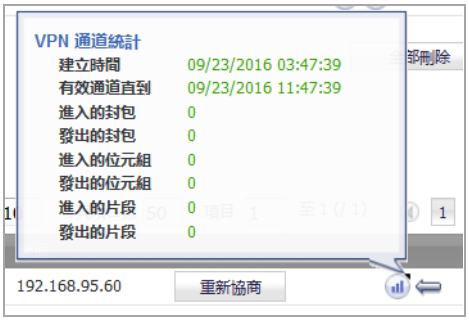
- 定義的 VPN 原則數
- 啟用的原則數
- 允許的最大原則數

最多可以定義 4 個 GroupVPN 原則，每個區一個。**VPN 原則**表中預設列出這些 GroupVPN 原則：**WAN GroupVPN**、**LAN GroupVPN**、**DMZ GroupVPN** 和 **WLAN GroupVPN**。按一下 GroupVPN 的**設定**欄中的**編輯**圖示，便會顯示**安全原則**視窗以供設定 GroupVPN 原則。

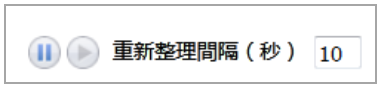
附註：如果 VPN 閘道 IP 相同，一個 VPN 原則不能有兩個不同的 WAN 介面。

目前使用中的 VPN 通道

此部分顯示目前使用中的 VPN 通道清單。**目前使用中的 VPN 通道**表會顯示各通道的以下資訊:

建立時間	建立通道的日期和時間
名稱	VPN 原則的名稱
本機	通道的本機 LAN IP 位址
遠端	遠端目的地網路 IP 位址
閘道	對等閘道 IP 位址
重新交涉按鈕	若選擇此項，將會強制 VPN 用戶端重新交涉 VPN 通道
統計圖示	將滑鼠移到**統計資料**圖示上時，會顯示 **VPN 通道統計資料**
	
左箭頭圖示	將滑鼠移到**左箭頭**圖示上時，會在 **VPN 原則**表中央顯示各個 VPN 原則

可使用「使用中的 VPN 通道」表頂端的選項來重新整理使用中的通道:



可藉由指定通道重新整理的頻率 (單位為秒) 來設定**重新整理間隔**。按一下**暫停**圖示即可暫停重新整理，或按一下**開始**圖示開始重新整理。

VPN 自動新增的存取規則控制

新增 VPN 原則時，SonicOS 自動建立不可編輯的存取規則，以允許流量穿越適當的區域。考慮以下 VPN 原則，其中本機網路設定為「防火牆防護的子網路」（本例中包括 LAN 和 DMZ），目的地網路設定為子網路 192.168.169.0。

雖然一般來說這能帶來極大的便利性，但您可能希望隱藏存取規則的自動建立功能以便支援 VPN 原則。大型軸幅式 VPN 部署就是這樣一種情況，其中所有幅站台都是使用位址空間的位址，這些位址空間可以輕鬆構成超網。例如，如果要實現從軸站台的 LAN 和 DMZ 到 2,000 個遠端站台中的各站台的一個子網路的存取，位址如下：

remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)

為各遠端站台建立 VPN 原則將需要 2,000 個 VPN 原則，但同時也會建立 8,000 條存取規則 (每個站台 4 條: LAN -> VPN、DMZ -> VPN、VPN -> LAN 和 VPN -> DMZ) 。然而，對於遠端站台的超網或位址範圍表示，只需 4 條規則就能輕鬆處理所有上述存取規則（更具體而言，允許或拒絕存取規則可按需要新增）：

remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255) 或
remoteRangeAll=Range 10.0.0.0-10.7.207.255

為啟用此級別的彙總，**VPN 原則**對話方塊的**進階**標籤提供了**自動新增 VPN 原則的存取規則設定**選項。預設情況下，此核取方塊勾選，意味著將自動建立伴隨的存取規則，就像往常一樣。建立 VPN 原則時取消勾選此核取方塊，您將能根據需要為 VPN 流量建立自訂存取規則。

2

站台對站台 VPN

SonicWall VPN 基於業界標準 IPsec VPN 實作，提供易於設定且安全的解決方案，可通過網際網路連接行動使用者、遠端工作者、遠端辦公室和合作夥伴。採用寬頻（DSL 或纜線）或撥號接入網際網路的行動電話使用者、遠端工作者和其他遠端使用者，可以通過防火牆上的 SonicWall Global VPN Client 和 GroupVPN 安全且輕鬆地存取您的網路資源。遠端辦公室網路可以利用支援網路對網路 VPN 連接的站台對站台 VPN 連接，安全連接到您的網路。

最多可以新增的原則數量取決於您所擁有的 SonicWall 型號，較大的型號允許較多連線。

附註：遠端使用者必須明確取得網路資源存取權。如需更多資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。根據您定義存取權的方式，可能會影響遠端用戶端利用 GVC 連接到 GroupVPN 的能力，不過也可能會影響使用 NetExtender 和 SSL VPN 虛擬辦公室書籤存取網路資源的遠端使用者。若要允許 GVC、NetExtender 或虛擬辦公室使用者存取網路資源，必須將網路位址物件或群組新增到 **VPN 存取**視窗上的允許清單中。若要存取此視窗，請選擇**管理**檢視，在**系統安裝**底下按一下**使用者 > 本機使用者和群組 > 本機使用者 > 新增 > VPN 存取**。

本節說明站台對站台原則，包括 GroupVPN。其他節則說明自動佈建和基於路由的 VPN。如需設定這類原則的具體詳細資訊，請參考以下章節:

- VPN 自動佈建
- 路由式 VPN

主題：

- 規劃站台對站台設定
- 一般 VPN 設定
- 管理 GroupVPN 原則
- 建立站台對站台 VPN 原則

規劃站台對站台設定

設定站台對站台 VPN 時提供許多選項，且可包含下列選項:

分公司 (閘道對閘道)	將一個 SonicWall 防火牆設定為通過 VPN 通道連接另一個 SonicWall 防火牆。或者將一個 SonicWall 防火牆設定為通過 IPsec 連接到另一家製造商的防火牆。
軸幅式設計	所有 SonicWall VPN 閘道都設定為連接到一個中心集線器，如公司防火牆。集線器必須有固定 IP 位址，但閘道可以有動態 IP 位址。如果閘道為動態，則集線器必須是 SonicWall 網路安全裝置。
網格設計	所有站台連接到所有其它站台。所有站台都必須有固定 IP 位址。

SonicWall 提供短片和知識庫文章，可協助您進行其中某些決策。

視訊：可以線上存取包含站台對站台 VPN 設定範例的參考視訊。例如，請參見如何使用共用密碼在主模式中建立站台到站台 VPN 或如何使用共用密碼建立加強模式站台到站台 VPN。
可以透過以下網址獲取其他視訊：https://www.sonicwall.com/en-us/support/video-tutorials。

提示：如需站台到站台 VPN 的資訊，請參見知識庫文章：
- *VPN: 多種類型站台對站台 VPN 的應用情節及設定 (SW12884)*
- *站台對站台 VPN 的故障排除文章 (SW7570)*

設計您的 VPN 設定時，請務必記錄所有相關的 IP 位址資訊，還可以建立一個網路圖以用作參考。其他注意事項:

- 防火牆必須有一個可路由的 WAN IP 位址，無論它是動態的還是靜態的。
- 在有動態和靜態 IP 位址的 VPN 網路中，必須由有動態位址的 VPN 閘道發起 VPN 連接。

一般 VPN 設定

本節回顧站台對站台設定的一般程序。程序可能因特定情況而異，後續章節將會說明其中某些情況。請注意，IPv4 和 IPv6 的 IPSec VPN 設定程序相當類似，不過 IPv6 目前不支援某些 VPN 功能，必要時會註明差異之處。

- IKEv1
- GroupVPN
- DHCP over VPN
- L2TP 伺服器
- 自動佈建
- FDQN

設定 VPN 的步驟如下:

1. 選擇**管理**檢視。
2. 在**連線**底下，選擇 **VPN > 基本設定**。
3. 在**檢視 IP 版本**欄位中選擇適當項目: IPv4 或 IPv6。
4. 在 **VPN 原則**區段中，按一下**新增**。
5. 完成**新增**頁面上的**一般**、**網路**、**建議**和**進階**區段。下列章節提供有關各頁面的其他資訊。

主題：

- 一般
- 網路
- 建議:
- 進階標籤

一般

在「一般」頁面上，開始定義站台對站台 VPN 原則。IPv4 和 IPv6 網路間有一些細微差異，下文將特別註明。

IPv4 新增 VPN 原則: 一般

1 若要設定 IPv4 VPN，請從下拉功能表中選擇**原則類型**。請注意，IPv6 無法使用此欄位。

2 從下拉功能表中選擇**驗證方法**。下列選項可供選擇，粗體項目表示預設值。「一般」檢視中的其餘欄位會根據您選擇的選項而改變。

IPv4	IPv6
手動金鑰	手動金鑰
使用預先共用密碼的 IKE	**使用預先共用密碼的 IKE**
使用供應商憑證的 IKE	使用供應商憑證的 IKE
SonicWall 自動佈建用戶端	
SonicWall 自動佈建伺服器	

3 輸入原則的**名稱**。

4 提供閘道名稱或位址及所需的驗證資訊。

附註：在設定 IKE 身分驗證時，IPv6 位址可用於本機和對等 IKE ID。

網路

在「網路」頁面上，定義包含站台對站台 VPN 原則的網路。

IPv4 新增 VPN 原則: 網路

在 VPN 原則的**網路**頁面上，從下拉功能表中選擇**本機網路**和**遠端網路**。

若使用 IPv6，僅提供下拉功能表選項，且只會列出 IPv6 可用的位址物件。由於不支援 DHCP，因此無法使用這些選項。此外，也移除了**本機網路**的**任何位址**選項和**遠端網路**的 **Tunnel All** 選項。可以選擇全零 IPv6 網路位址物件實現相同的功能和行為。

若使用 IPv4，則提供其他選項。在**本機網路**底下，您可**從清單中選擇本機網路**或選擇**任何位址**。若選擇了**任何位址**，就會在受信任區域和 VPN 區域之間建立自動新增規則

若使用 IPv4，在**遠端網路**底下，您可選擇下列其中一項:

- **使用此 VPN 通道作為所有網際網路流量的預設路由。**
- **從清單中選擇目的地網路**。若未列出任何項目，您可建立新的位址物件或位址群組。
- **使用 IKEv2 IP 集區**。選擇此項以支援 IKEv2 設定承載。

建議:

在「建議」頁面上，定義 VPN 原則的安全參數。IPv4 和 IPv6 的這個頁面相同，不過選項會因為您選擇項目而有所不同。IPv4 的**交換**欄位提供 IKEv1 和 IKEv2 選項，而 IPv6 僅提供 IKEv2。

進階標籤

IPv4 和 IPv6 的**進階**檢視相似，不過部分選項僅供其中一者使用:

進階設定：可用選項

選項	IP 版本	
	IPv4	IPv6
啟用多點傳送	X	
啟用保持運作		X
允許 TCP 加速	X	
阻止為 VPN 原則的自動建立存取規則		X
停用 IPsec 反重放		X
使用主要 IP 位址		X
指定本機閘道 IP 位址		X

附註：由於介面可以擁有多個 IPv6 位址，所以有時通道的本機位址可能定期發生變化。如果使用者需要一致的 IP 位址，則將 VPN 原則設定為繫結到介面，而不是繫結到區域，並手動指定位址。位址必須是此介面的一個 IPv6 位址。

IPv6 新增 VPN 原則: 進階

IPv4 新增 VPN 原則: 進階

管理 GroupVPN 原則

GroupVPN 功能為全域 VPN 用戶端 (GVC) 提供自動 VPN 原則佈建。SonicWall 網路安全裝置和 GVC 上的 GroupVPN 功能簡化了 VPN 部署和管理。您可利用用戶端原則佈建技術，為 GVC 使用者定義 VPN 原則。此原則資訊會自動從防火牆 (VPN 閘道) 下載到 GVC，免去遠端使用者佈建 VPN 連接的負擔。

GroupVPN 原則有利於防火牆管理員設定和部署多個 GVC。**GroupVPN** 僅適用於 GVC，您應搭配使用 XAUTH/RADIUS 或供應商憑證以增強安全性。如需為任何區域建立 GroupVPN 原則的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*，或導覽至**管理**檢視的**系統安裝**底下，並選擇**網路 > 區域 > 新增**。

SonicOS 為 WAN 區域和 WLAN 區域提供預設 GroupVPN 原則，因為這兩個區域通常是受信任程度較低的區域。預設 GroupVPN 原則列於 **VPN > 基本設定**頁面上的「VPN 原則」面板中，且可供自訂:

- WAN GroupVPN
- WLAN GroupVPN

提示：如需群組 VPN 和全域 VPN 用戶端的資訊，請參閱*多種類型群組 VPN/全域 VPN 用戶端的應用情形及設定* (SW7411)。

主題：

- 設定使用預先共用密碼的 IKE
- 設定使用供應商憑證的 IKE
- 匯出 VPN 用戶端原則

設定使用預先共用密碼的 IKE

設定使用預先共用密碼的 WAN GroupVPN 步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 按一下 **WAN GroupVPN** 原則的**編輯**圖示。

在**一般**檢視中，**使用預先共用密碼的 IKE** 是**驗證方法**的預設設定。共用密碼由防火牆自動產生，並寫入**共用密碼**欄位中。您也可以產生自己的共用密碼。自定義的共用密碼最少須包含 4 個字元。

附註：無法變更任何 GroupVPN 原則的名稱。

4 按一下**建議**繼續設定程序。

5 在 **IKE（階段 1）建議**部分，選擇下列設定：

- 從 **DH 群組**下拉功能表中選擇**群組 2** (預設)。

  附註：Windows XP L2TP 用戶端只能使用 DH 群組 2。

- 從「加密」下拉功能表中選擇 **DES**、**3DES** (預設)、**AES-128**、**AES-192** 或 **AES-256**。
- 從**驗證**下拉功能表中選擇所需的驗證方法: **MD5**、**SHA1**（預設）、**SHA256**、**SHA384** 或 **SHA512**。
- 在**存留時間 (秒)** 欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

6 在 **IPsec（階段 2）建議**部分，選擇下列設定：

- 從**通訊協定**下拉功能表中選擇 **ESP** (預設)。
- 從**加密**下拉功能表中選擇 **3DES** (預設)、**AES-128**、**AES-192** 或 **AES-256**。
- 在**驗證**下拉功能表中選擇所需的驗證方法: **MD5**、**SHA1**（預設）、**SHA256**、**SHA384**、**SHA512**、**AES-XCBX** 或**無**。
- 如果希望增加 Diffie-Hellman 金鑰交換以增強安全性，請勾選**啟用完全轉送保密**。
- 在**存留時間（秒）**欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

7 按一下進階。

8 選擇您希望套用於 GroupVPN 原則的下列可選設定：

進階設定

停用 IPsec 反重放	停止丟棄有重複序號的封包。
啟用多點傳送	允許 IP 多點傳送流量，如音訊流（包括 VoIP）和視訊流應用程式等，通過 VPN 通道。
接受多個用戶端建議	允許接受多個客戶建議，如「IKE (階段 1) 建議」或「IKE (階段 2) 建議」。
啟用 IKE 模式設定	允許 SonicOS 指派內部 IP 位址、DNS 伺服器或 WINS 伺服器給供應商用戶端，例如 iOS 裝置或 Avaya IP 電話。
透過該 SA 管理：	如果使用 VPN 原則管理防火牆，請選擇管理方法：**HTTP**、**SSH** 或 **HTTPS**。 **附註：** SSH 僅對 IPv4 有效。
預設閘道	用於針對此 VPN 原則，為傳入的 IPsec 封包指定預設網路路由的 IP 位址。傳入封包由防火牆解碼，並與防火牆中設定的固定路由比較。 由於封包可以有任何 IP 位址目的地，因此無法設定足夠多的固定路由來處理流量。對於通過 IPsec 通道接收的封包，防火牆尋找一個路由。如果未找到任何路由，安全裝置將檢查有無預設閘道。如果偵測到預設閘道，封包將通過此閘道路由。否則，丟棄封包。

用戶端驗證

需要 XAUTH 驗證 VPN 客戶	要求此 VPN 通道上的所有傳入流量均來自已通過驗證的使用者。此 VPN 通道不允許存在未認證的流量。預設已核取 **Trusted Users** 組。您可以從 **XAUTH 使用者的使用者群組**使用者功能表中的 XAUTH 使用者的使用者組中選擇另一個使用者群組或**任何人**。
允許未驗證的 VPN 客戶存取	用於啟用未驗證的 VPN 用戶端存取。如果清除**需要 XAUTH 驗證 VPN 客戶**，**允許未驗證的 VPN 客戶存取**功能表將啟用。從預先定義選項功能表中選擇一個位址物件或位址群組，或選擇**建立新位址物件**或**建立新位址群組**以新建一個。

9 按一下**用戶端**標籤。

10 選擇您希望套用於 GroupVPN 原則的下列設定：

使用者名稱和密碼的快取

在用戶端快取 XAUTH 使用者名稱和密碼	允許全域 VPN 用戶端快取使用者名稱和密碼: • 若選擇了**從不**，則不允許全域 VPN 用戶端快取使用者名稱和密碼。啟用連接時，以及每次發生 IKE 階段 1 金鑰重新交涉時，就會提示使用者輸入使用者名稱和密碼。這是預設值。 • 若選擇了**單一工作階段**，則每次啟用連接時，都會提示全域 VPN 用戶端使用者輸入使用者名稱和密碼，在連接停用前，使用者名稱和密碼一直有效。使用者名稱和密碼一直使用到 IKE 階段 1 金鑰重新交涉。 • 若選擇了**始終**，則只會在啟用連接時，提示全域 VPN 用戶端使用者輸入使用者名稱和密碼一次。提示時，使用者可以選擇快取使用者名稱和密碼。

用戶端連接	
虛擬轉接器設定	全域 VPN 用戶端 (GVC) 使用虛擬轉接器時，要求 DHCP 伺服器 (內部 SonicOS 或指定的外部 DHCP 伺服器) 為虛擬轉接器指派位址。 如果必須是可預測的位址，則獲得虛擬轉接器的 MAC 位址，並建立 DHCP 租用保留。為了減少提供可預測虛擬轉接器位址的管理負擔，可以設定 GroupVPN 接受虛擬轉接器 IP 設定的固定位址。 **附註：** 此功能要求使用 SonicWall GVC。 選擇以下一項： • 選擇**從不**，此 GroupVPN 連接不使用虛擬轉接器。這是預設值。 • 若虛擬轉接器僅從 DHCP 伺服器獲得 IP 設定，則按照 **VPN > VPN 上的 DHCP** 頁面的設定，選擇 **DHCP 租用**。 • 選擇 **DHCP 租用或手動設定**，當 GVC 連接到防火牆，防火牆的原則會指示 GVC 使用虛擬轉接器，但如果已經手動設定虛擬轉接器，則不傳送 DHCP 訊息。設定的值由防火牆記錄，以便能代理手工指派 IP 位址的 ARP。設計上，目前虛擬轉接器對 IP 位址指派沒有任何限制。只是不允許重複的固定位址。
允許連接到	與各閘道的目的地網路符合的用戶端網路流量，會通過此特定閘道的 VPN 通道傳送。選擇以下一項： • **僅該閘道**允許一次啟用一個連接。與閘道原則中指定的目的地網路符合的流量通過此 VPN 通道傳送。 如果同時選擇了此選項和**設定預設路由作為該閘道**，則網際網路流量也將透過 VPN 通道傳送。如果選擇了此選項但沒有選擇**設定預設路由作為該閘道**，則會封鎖網際網路流量。 • **所有安全的閘道**允許一次啟用一個或多個連接。與各閘道的目的地網路符合的流量通過此特定閘道的 VPN 通道傳送。 如果同時選擇了此選項和**設定預設路由作為該閘道**，則網際網路流量也將透過 VPN 通道傳送。 如果選擇了此選項但沒有選擇**設定預設路由作為該閘道**，則會封鎖網際網路流量。多個閘道中只有一個能啟用**設定預設路由作為該閘道**。 • **分離通道**允許 VPN 使用者同時擁有本機網際網路連接和 VPN 連接。這是預設值。
設定預設路由作為該閘道	如果所有遠端 VPN 連接均通過此 VPN 通道存取網際網路，則應勾選此核取方塊。只能設定一個 VPN 原則來使用此設定。預設情況下，未選擇此選項。
套用 VPN 存取控制清單	選擇此核取方塊以套用 VPN 存取控制清單。啟用此選項後，指定使用者僅可存取為其設定的網路 (如需更多資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**系統安裝使用者 > 本機使用者和群組**)。預設情況下未啟用此選項。
用戶端初始佈建	
用於簡易用戶端佈建的使用者預設金輪	與此閘道的初步交換使用加強模式，VPN 用戶端使用預設預先共用金鑰進行驗證。預設情況下未啟用此選項。

11 按一下**確定**。

12 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

設定使用供應商憑證的 IKE

重要：設定 IKE 使用供應商憑證的 GroupVPN 之前，必須在防火牆上安裝憑證。

以使用供應商憑證的 IKE 設定 GroupVPN 步驟如下

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 按一下 **WAN GroupVPN** 原則的**編輯**圖示。

4 在**安全原則**部分，從**驗證方法**下拉功能表中選擇**使用第三方憑證的 IKE**。

附註：VPN 原則名稱預設為 GroupVPN，無法變更。

5 從**閘道憑證**下拉功能表中為防火牆選擇一個憑證。

若開始本程序前您沒有下載供應商憑證，**閘道憑證**欄位會顯示**- 無任何經過驗證的第三者憑證 -**。

6 在**對等憑證**區段中，從**對等 ID 類型**下拉功能表中選擇以下其中一項:

識別名稱	基於憑證的「主旨識別名稱」欄位，由核發的憑證授權單位設定。
電子郵件 ID	基於憑證的「主旨備用名稱」欄位，並非所有憑證均預設包含此欄位。如果憑證不包含「備用主旨名稱」欄位，則此篩選條件無效。
網域 ID	

7 在**對等 ID 篩選條件**欄位中輸入對等 ID 篩選條件。

電子郵件 ID 和**網域名稱**篩選條件可以包含一個字串或部分字串，以識別所需的可接受範圍。輸入的字串不區分大小寫，可以包含萬用字元 *（代表多個字元）和 ?（代表一個字元）。例如，選擇了**電子郵件 ID** 時，字串 `*@sonicwall.com` 允許電子郵件地址結尾是 `@sonicwall.com` 的任何使用者存取；選擇了**網域名稱**時，字串 `*sv.us.sonicwall.com` 允許網域名稱結尾是 `sv.us.sonicwall.com` 的任何使用者存取。

8 勾選**僅允許被閘道簽署的對等憑證**，要求對等憑證必須由**閘道憑證**功能表中指定的發佈者簽署。

9 按一下**建議**標籤。

10 在 **IKE (階段 1) 建議**區段中，選擇下列設定:

a 從 **DH 群組**下拉功能表中選擇**群組 1**、**群組 2** (預設)、**群組 5** 或**群組 14**。

b

> **附註：**Windows XP L2TP 用戶端只能使用 DH 群組 2。

c 從**加密**下拉功能表中選擇 **DES**、**3DES** (預設)、**AES-128**、**AES-192** 或 **AES-256**。

d 從**驗證**下拉功能表中選擇所需的驗證方法: **MD5**、**SHA1**（預設）、**SHA256**、**SHA384**、**SHA512**、**AES-XCBX** 或**無**。

e 在**存留時間 (秒)** 欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

11 在 **IPsec (階段 2) 建議**區段中，選擇下列設定:

a 從**通訊協定**下拉功能表中選擇 **ESP** (預設)。

b 從**加密**下拉功能表中選擇 **3DES** (預設)、**AES-128**、**AES-192** 或 **AES-256**。

c 在**驗證**下拉功能表中選擇所需的驗證方法: **MD5**、**SHA1**（預設）、**SHA256**、**SHA384**、**SHA512**、**AES-XCBX** 或**無**。

d 如果希望增加 Diffie-Hellman 金鑰交換以增強安全性，請勾選**啟用完全轉送保密**。

e 在**存留時間（秒）**欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

12 按一下**進階**標籤，選擇您希望套用於 GroupVPN 原則的下列任意可選設定。

停用 IPsec 反重放	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達。
啟用多點傳送	允許 IP 多點傳送流量，如音訊流（包括 VoIP）和視訊流應用程式等，通過 VPN 通道。
接受多個用戶端建議	允許接受多個客戶建議，如「IKE (階段 1) 建議」或「IKE (階段 2) 建議」。
啟用 IKE 模式設定	允許 SonicOS 指派內部 IP 位址、DNS 伺服器或 WINDS 伺服器給供應商用戶端，例如 iOS 裝置或 Avaya IP 電話。
透過該 SA 管理	如果使用 VPN 原則管理防火牆，請選擇管理方法：**HTTP**、**SSH** 或 **HTTPS**。 **附註：** SSH 僅對 IPv4 有效。
預設閘道	勾選**透過此 SA 路由所有網際網路流量**核取方塊，中心站台和遠端站台一起使用。對於此 SA，預設 LAN 閘道用於為傳入的 IPsec 封包指定預設 LAN 路由的 IP 位址。
啟用 OCSP 檢查和 **OCSP 回應者 URL**	支援使用線上憑證狀態通訊協定 (OCSP) 來檢查 VPN 憑證狀態，並指定檢查憑證狀態的 URL。
需要 XAUTH 驗證 VPN 客戶	要求此 VPN 原則的所有傳入流量均來自已通過驗證的使用者。此 VPN 通道不允許存在未認證的流量。
XAUTH 使用者的使用者群組	允許選擇已定義的使用者群組進行驗證。
允許未驗證的 VPN 客戶存取	用於為未驗證的全域 VPN 用戶端存取指定網路區段。

13 按一下**用戶端**標籤，選擇您希望套用於 Global VPN Client 佈建的下列任意核取方塊：

在用戶端快取 XAUTH 使用者名稱和密碼

允許全域 VPN 用戶端快取使用者名稱和密碼:

- 選擇**從不**，不允許全域 VPN 用戶端快取使用者名稱和密碼。啟用連接時，以及每次發生 IKE 階段 1 金鑰重新交涉時，就會提示使用者輸入使用者名稱和密碼。
- 選擇**單一工作階段**，每次啟用連接時都提示使用者輸入使用者名稱和密碼，在連接停用前，在連接停用前，使用者名稱和密碼一直有效。使用者名稱和密碼一直使用到 IKE 階段 1 金鑰重新交涉。
- 選擇**始終**，僅在啟用連接時提示使用者輸入使用者名稱和密碼一次。提示時，使用者可以選擇快取使用者名稱和密碼。

虛擬轉接器設定

全域 VPN 用戶端 (GVC) 使用虛擬轉接器時，要求 DHCP 伺服器 (內部 SonicOS 或指定的外部 DHCP 伺服器) 為虛擬轉接器指派位址。

如果必須是可預測的位址，則獲得虛擬轉接器的 MAC 位址，並建立 DHCP 租用保留。為了減少提供可預測虛擬轉接器位址的管理負擔，請設定 GroupVPN 接受虛擬轉接器 IP 設定的固定位址。此功能要求使用 SonicWall GVC。

- 選擇**從不**，此 GroupVPN 連接不使用虛擬轉接器。
- 選擇 **DHCP 租用**，按照 **VPN > VPN 上的 DHCP** 頁面的設定，虛擬轉接器僅從 DHCP 伺服器獲得 IP 設定。
- 選擇 **DHCP 租用或手動設定**，當 GVC 連接到防火牆，防火牆的原則會指示 GVC 使用虛擬轉接器，但如果已經手動設定虛擬轉接器，則不傳送 DHCP 訊息。設定的值由防火牆記錄，以便能代理手工指派 IP 位址的 ARP。設計上，目前對虛擬轉接器的 IP 位址指派沒有任何限制。只是不允許重複的固定位址。

允許連接到	與各閘道的目的地網路符合的用戶端網路流量，會通過此特定閘道的 VPN 通道傳送。選擇以下其中一個選項: • **僅該閘道**允許一次啟用一個連接。與閘道原則中指定的目的地網路符合的流量通過此 VPN 通道傳送。 如果同時選擇了此選項和**設定預設路由作為該閘道**，則網際網路流量也將透過 VPN 通道傳送。如果選擇了此選項但沒有選擇**設定預設路由作為該閘道**，則會封鎖網際網路流量。 • **所有安全的閘道**允許一次啟用一個或多個連接。與各閘道的目的地網路符合的流量通過此特定閘道的 VPN 通道傳送。 如果同時選擇了此選項和**設定預設路由作為該閘道**，則網際網路流量也將透過 VPN 通道傳送。如果選擇了此選項但沒有選擇**設定預設路由作為該閘道**，則會封鎖網際網路流量。多個閘道中只有一個能啟用**設定預設路由作為該閘道**。 **附註：** 多個閘道中只有一個能啟用**設定預設路由作為該閘道**。 • **分離通道**允許 VPN 使用者同時擁有本機網際網路連接和 VPN 連接。這是預設值。
設定預設路由作為該閘道	如果所有遠端 VPN 連接均通過此 SA 存取網際網路，則應勾選此核取方塊。只能設定一個 SA 來使用此設定。
用於簡易用戶端佈建的使用者預設金輪	與此閘道的初步交換使用加強模式，VPN 用戶端使用預設預先共用金鑰進行驗證。

14 按一下**確定**。

15 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

匯出 VPN 用戶端原則

您可將含有全域 VPN 用戶端配置設定的檔案提供給最終使用者，只需從防火牆匯出 VPN 用戶端原則即可。

重要：防火牆必須啟用 GroupVPN SA (安全關聯) 以便匯出設定檔。

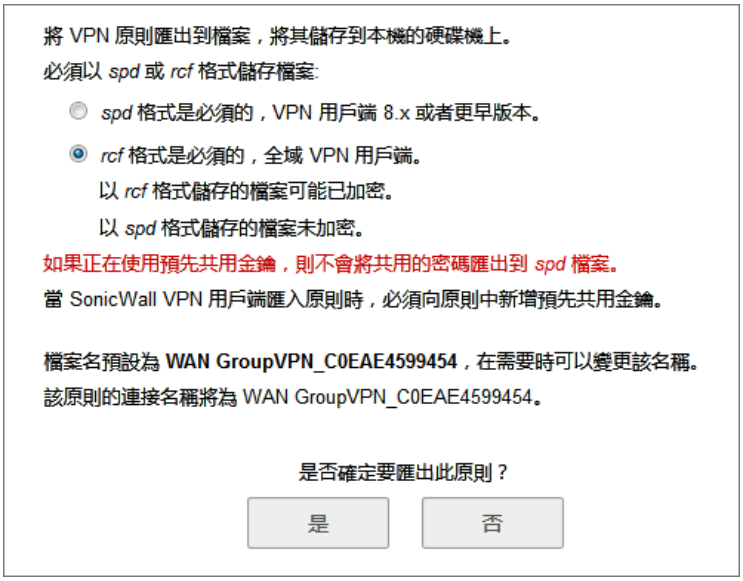
匯出全域 VPN 用戶端配置設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 確認您要匯出的原則已啟用。

4 按一下 **VPN 原則**表中此 GroupVPN 項目的**設定**列中的**匯出**圖示。



預設值為 **rcf 格式是必須的，全域 VPN 用戶端**。以 rcf 格式儲存的檔案可以用密碼加密。防火牆為設定檔提供預設檔案名稱，您可以變更。

5 按一下**是**。

6 在**選擇要匯出的用戶端存取網路**下拉清單中，選擇 **VPN 存取網路**。

7 若要對匯出的檔案加密，請在**密碼**欄位中輸入一個密碼，然後在**確認密碼**欄位中再次輸入。如果選擇不輸入密碼，則匯出檔案將不加密。

8 按一下**提交**。如果未輸入密碼，將顯示一條訊息確認您的選擇。

9 按一下**確定**。儲存之前可以變更設定檔。

10 儲存檔案。

11 按一下**關閉**。

可儲存或以電子方式傳送此檔案到遠端使用者，以便設定其 Global VPN Client。

建立站台對站台 VPN 原則

站台對站台 VPN 允許位於不同地點的辦公室透過公用網路建立彼此間的安全連接，如此便可延伸公司的網路，從單一地點為其他地點的員工提供資源。

可建立或修改現有的站台對站台 VPN 原則。若要新增原則，請按一下 **VPN 原則**表格底下的**新增**；若要修改現有的原則，請按一下該原則的**編輯**圖示。設定站台對站台 VPN 時可設定以下選項:

- 以預先共用密碼進行設定
- 以手動金鑰進行設定
- 以供應商憑證進行設定

本節還包含有關設定遠端 SonicWall 防火牆，以及設定固定路由以在 VPN 通道失敗時充當容錯移轉路由的資訊

- 設定遠端 SonicWall 網路安全裝置
- 設定 VPN 容錯移轉到固定路由

視訊：可以線上存取包含站台對站台 VPN 設定範例的參考視訊。例如，請參見如何使用共用密碼在主模式中建立站台到站台 VPN 或如何使用共用密碼建立加強模式站台到站台 VPN。

可以透過以下網址獲取其他視訊：https://www.sonicwall.com/en-us/support/video-tutorials。

以預先共用密碼進行設定

以預先共用密碼設定使用網際網路金鑰交換 (IKE) 的 VPN 原則步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 按一下**新增**以建立新原則，或按一下**編輯**圖示以更新現有的原則。

4 從**一般**標籤上的**原則類型**下拉功能表中，選擇**站台對站台**。

5 在**驗證方法**下拉功能表中，選擇**使用預先共用密碼的 IKE**。

6 在**名稱**欄位中輸入原則的名稱。

7 在 IPSec **主要閘道名稱或者位址**欄位中輸入遠端連接的主機名稱或 IP 位址。

8 如果遠端 VPN 裝置支援多個端點，可在 **IPsec 次要閘道名稱或者位址**欄位中，輸入遠端連接的第二主機名稱或 IP 位址 (可選)。

9 在 **IKE 驗證**區段中，於**共用密碼**和**確認共用密碼**欄位內輸入共用密碼。這組密碼用於設定 SA (安全關聯)。共用密碼不得少於 4 個字元，且應同時包含數字和字母。

10 若要查看這兩個欄位中的共用密碼，請清除**隱藏共用密碼**核取方塊。**隱藏共用密碼**核取方塊預設為勾選，因此共用密碼以黑色圓圈顯示。

11 也可以為此原則指定**本機 IKE ID** 和**對等 IKE ID**。預設情況下，**IP 位址** (ID_IPv4_ADDR) 用於主模式交涉，防火牆識別項 (ID_USER_FQDN) 用於加強模式。

您可從下拉功能表中選擇以下 ID:

- **IPv4 位址**
- **網域名稱**
- **電子郵件地址**
- **防火牆識別項**
- **金鑰識別項**

12 從下拉功能表中選擇完畢後，在**本機 IKE ID** 和**對等 IKE ID** 欄位中輸入位址、名稱或 ID。

13 按一下**網路**。

14 在**本機網路**底下，選擇以下其中一項:

從清單中選擇本機網路	若特定網路可存取 VPN 通道，請從下拉功能表中選擇一個本機網路。
任何位址	如果流量可從任意本機網路發起，或如果對等點已選擇**使用該 VPN 通道作為預設路由用於所有的網路流量**，請使用此選項。自動新增的規則將建立在可信任區域和 VPN 區域之間。 **附註：** IKEv2 不支援 VPN 上的 HCP。

15 在**從清單中選擇目的地網路**底下，選擇以下其中一項:

使用此 VPN 通道作為所有網際網路流量的預設路由	如果來自任何本機使用者的流量只有加密才可離開防火牆，請選擇此選項。 **附註：** 只能設定一個 SA 來使用此設定。
從清單中選擇目的地網路	從下拉功能表中選擇一個遠端網路。
使用 IKEv2 IP 集區	選擇此選項以支援 IKEv2 設定承載。

16 按一下**建議**。

17 在 **IKE (階段 1) 建議**底下，從**交換**下拉功能表中選擇以下其中一個選項:

主模式	將 IKEv1 階段 1 建議與 IPsec 階段 2 建議一同使用。Suite B 加密選項對於 IKE 階段 1 設定中的 DH 群組可用，且對於 IPsec 階段 2 設定中的加密可用。
加強模式	一般在動態指派 WAN 位址時使用。將 IKEv1 階段 1 建議與 IPsec 階段 2 建議一同使用。Suite B 加密選項對於 IKE 階段 1 設定中的 DH 群組可用，且對於 IPsec 階段 2 設定中的加密可用。
IKEv2 模式	使所有交涉透過 IKEv2 通訊協定發生，而不是使用 IKEv1 階段。 **附註：**如果選擇 **IKE v2 模式**，VPN 通道的兩端都必須使用 IKE v2。若選擇此項，**DH 群組**、**加密**和**驗證**欄位將以灰色顯示且無法定義。

18 在 **IKE (階段 1) 建議**底下設定其餘選項的值。多數 VPN 設定可接受 **DH 群組**、**加密**、**驗證**和**存留時間**的預設值。

附註：若在**交換**欄位選擇 **IKEv2 模式**，則 **DH 群組**、**加密**和**驗證**欄位將以灰色顯示，且無法為這些選項做任何選擇。

附註：確保通道另一端的階段 1 值符合。

a 針對 **DH 群組**，處於**主模式**或**加強模式**時，可從多個 Diffie Hellman 交換中進行選擇:

Suite B 加密中內含的 Diffie Hellman 群組	**其他 Diffie-Hellman 選項**
256 位隨機 ECP 群組	組 1
384 位隨機 ECP 群組	組 2
521 位隨機 ECP 群組	組 5
192 位隨機 ECP 群組	組 14
224 位隨機 ECP 群組	

b 針對**加密**欄位，如果選擇了**主模式**或**加強模式**，請從下拉功能表中選擇 **3DES** (預設)、**DES**、**AES-128**、**AES-192** 或 **AES-256**。

c 針對**驗證**欄位，如果選擇了**主模式**或**加強模式**，請選擇 **SHA-1** (預設)、**MD5**、**SHA256**、**SHA384** 或 **SHA512** 以增強驗證安全性。

d 針對所有**交換**模式，請輸入**存留時間 (秒)** 的值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

19 在 **IPsec (階段 2) 建議**區段中設定選項。多數 VPN SA 設定可接受**通訊協定**、**加密**、**驗證**、**啟用完全轉送保密**和**存留時間 (秒)** 的預設值。

附註：確保通道另一端的階段 2 值符合。

- 如果您在**通訊協定**欄位中選擇了 **ESP**，則在**加密**欄位中可以從包含在 Suite B 加密中的 6 種加密演算法中進行選擇：

Suite B 加密選項	其他選項
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	

- 如果您在**通訊協定**欄位中選擇了 **AH**，**加密**欄位就會以灰色顯示，且無法選擇任何選項。

20 按一下**進階**標籤，選擇您希望套用於 VPN 原則的下列任意可選設定。這些選項會隨您在**建議**標籤中選擇的選項而變化。

選項	主模式或加強模式 (請參閱下圖)	IKEv2 模式 (請參閱下圖)
進階設定		
啟用保持運作	選擇此項，即可在此 VPN 通道的對等點之間使用活動訊號訊息，如果通道的一端發生故障，使用「保持活動」活動訊號，便可在兩端再度可用時自動重新交涉通道，而不必等待建議的存留時間過期。 **附註：** 當 VPN 原則設定為 VPN 上的 DHCP 中心閘道，或是主要閘道名稱或位址為 0.0.0.0，系統就會停用「保持活動」選項。	IKEv2 模式無法選擇。
阻止為 VPN 原則的自動建立存取規則	若*未*選擇 (預設)，則允許 VPN 流量穿越適當區域。	若*未*選擇 (預設)，則允許 VPN 流量穿越適當區域。
停用 IPsec 反重放	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達
啟用 Windows 網路 (NetBIOS) 廣播	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。
啟用多點傳送	選擇此項，即可允許串流音訊 (包括 VoIP) 和視訊應用程式等多點傳送流量通過 VPN 通道。	選擇此項，即可允許串流音訊 (包括 VoIP) 和視訊應用程式等多點傳送流量通過 VPN 通道。
WXA 群組	選擇「無」(預設) 或「群組一」	選擇「無」(預設) 或「群組一」
僅顯示符合套件 B 的演算法	若只想顯示符合 Suite B 的演算法，請選擇此項。	若只想顯示符合 Suite B 的演算法，請選擇此項。
套用 NAT 原則	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。 **附註：** 一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。 **附註：** 一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。
允許 SonicPointN 三層管理	若要允許三層管理，請選擇此項。	若要允許三層管理，請選擇此項。
透過該 SA 管理	此選項請選擇 **HTTPS** 以透過 VPN 通道管理本機 SonicWall 防火牆。	此選項請選擇 HTTPS 以透過 VPN 通道管理本機 SonicWall 防火牆。
透過 SA 使用者登入	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。 **附註：** HTTP 使用者登入不允許遠端驗證。	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。 **附註：** HTTP 使用者登入不允許遠端驗證。

選項	主模式或加強模式 (請參閱下圖)	IKEv2 模式 (請參閱下圖)
預設 LAN 閘道 (可選)	若想在進入此通道前路由透過 LAN 前往未知子網路目的地的流量，請選擇此項。例如，若選擇了**使用該 VPN 通道作為預設路由用於所有的網路流量** (在本頁面上**網路**檢視的**遠端網路**底下)，請輸入路由器位址。	若想在進入此通道前路由透過 LAN 前往未知子網路目的地的流量，請選擇此項。例如，若選擇了**使用該 VPN 通道作為預設路由用於所有的網路流量** (在本頁面上**網路**檢視的**遠端網路**底下)，請輸入路由器位址。
VPN 原則繫結至	從下拉清單中選擇一個介面或區域。若使用 WAN 負載平衡，並希望 VPN 使用任一 WAN 介面，則區域 WAN 應為偏好的設定。 **重要：**若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。	從下拉清單中選擇一個介面或區域。若使用 WAN 負載平衡，並希望 VPN 使用任一 WAN 介面，則區域 WAN 應為偏好的設定。 **重要：**若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。
IKEv2 設定		
請不要在 IKE SA 協商時傳輸觸發封包	未啟用	*未*選擇 (預設)。應只在對等點無法處理觸發封包，而需要互操作時選擇。 建議作法為包括觸發封包，以便幫助 IKEv2 回應者從安全原則資料庫中選擇正確的受保護 IP 位址範圍。並非所有方案都支援此功能，因此禁止某些 IKE 對等點包括觸發封包可能是適當的。
接收 Hash & URL 憑證類型	未啟用	如果裝置能夠傳送並處理雜湊和憑證 URL，而不是憑證本身，請選擇此項。若選擇此項，系統會傳送訊息給對等裝置，通知支援 HTTP 憑證查詢。
傳輸 Hash & URL 憑證類型	未啟用	如果裝置能夠傳送並處理雜湊和憑證 URL，而不是憑證本身，請選擇此項。若選擇此項，系統會回應對等裝置傳來的訊息，確認支援 HTTP 憑證查詢。

主模式、加強模式和 IKEv2 模式的進階設定

其他 IKEv2 模式選項

21 按一下**確定**。

22 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

以手動金鑰進行設定

您可手動定義用於建立 IPsec VPN 通道的加密金鑰。需知道加密或驗證金鑰為何 (例如當其中一個 VPN 對等點需要特定金鑰)，或需停用加密和驗證時，可以定義手動金鑰。

設定使用手動金鑰的 VPN 原則步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 按一下**新增**以建立新原則，或按一下**編輯**圖示以更新現有的原則。

4 在**驗證方法**欄位中，從下拉清單選擇**手動金鑰**。視窗只會顯示「手動金鑰」選項。

5 在**名稱**欄位中輸入原則的名稱。

6 在 **IPsec 閘道名稱或者位址**欄位中輸入遠端連接的主機名稱或 IP 位址。

7 按一下**網路**。

8 在**本機網路**底下，選擇以下其中一個選項:

- 如果特定本機網路可以存取 VPN 通道，請在**從清單中選擇本機網路**下拉清單中選擇一個本機網路。
- 如果流量可從任意本機網路發起，請選擇**任何位址**。如果對等點已選擇**使用該 VPN 通道作為預設路由用於所有的網路流量**，請使用此選項。自動新增的規則將建立在可信任區域和 VPN 區域之間。

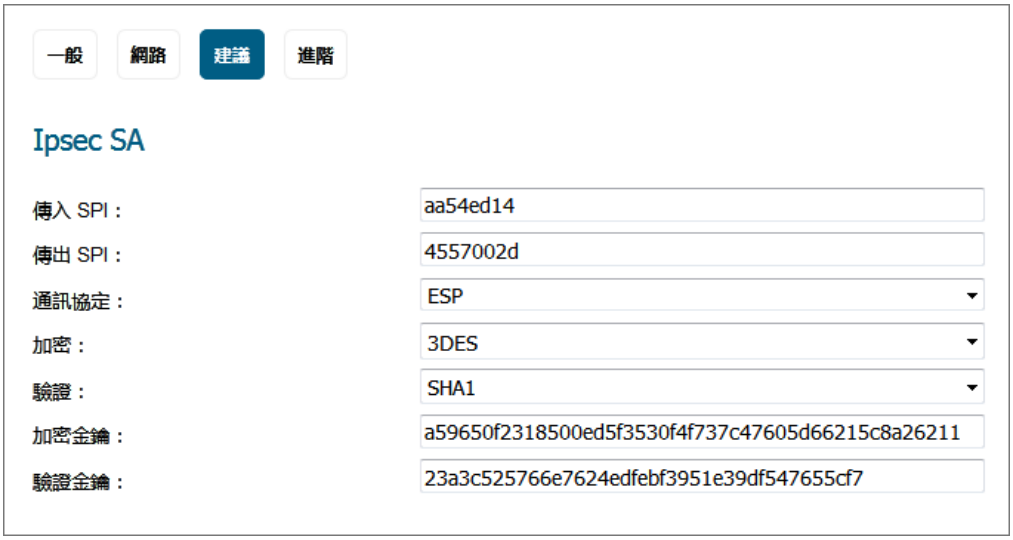
9 在**目的地網路**下面，選擇以下其中之一：

- 如果來自任何本機使用者的流量只有加密才可離開防火牆，請勾選**使用該 VPN 通道作為預設路由用於所有的網路流量**。

  附註：只能設定一個 SA 來使用此設定。

- 或選擇**從清單選擇目的地網路**，並選擇位址物件或組。

10 按一下**建議**。



11 定義一個**傳入 SPI** 和一個**傳出 SPI**。安全參數索引 (SPI) 為十六進位，其長度可以為 3 到 8 個字元。

重要：每個安全關聯 (SA) 都必須有唯一的 SPI，任兩個 SA 均不能有相同的 SPI。但是每個 SA 的傳入 SPI 可以與傳出 SPI 相同。

12 多數 VPN SA 設定可以接受**通訊協定**、**加密**和**驗證**的預設值；否則請從下拉清單中選擇值。

附註：通訊協定、**加密**和**驗證**的值必須與遠端防火牆上的值一致。

- 如果您在**通訊協定**欄位中選擇了 **ESP**，則在**加密**欄位中可以從包含在 Suite B 加密中的 6 種加密演算法中進行選擇：
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
  - **無**
- 如果您在**通訊協定**欄位中選擇了 **AH**，**加密**欄位就會以灰色顯示，且無法選擇任何選項。

13 在**加密金鑰**欄位中輸入一個 48 字元十六進位加密金鑰，或使用預設值。此加密金鑰用於設定遠端 SonicWall 加密金鑰，因此應記錄下來以便設定遠端防火牆。

提示：有效的十六進位字元包括 0、1、2、3、4、5、6、7、8、9、a、b、c、d、e 和 f。1234567890abcdef 是有效 DES 或 ARCFour 加密金鑰的一個例子。如果輸入的加密或驗證金鑰不正確，瀏覽器視窗底部會顯示一條錯誤訊息。

14 在**驗證金鑰**欄位中輸入一個 40 字元十六進位驗證金鑰，或使用預設值。記下此金鑰以便設定防火牆設定。

15 按一下**進階**。

16 選擇您希望套用於 VPN 原則的下列任意可選設定。

選項	定義
壓制為 VPN 原則自動存取規則的建立	若未選擇 (預設)，則允許 VPN 流量穿越適當區域。
啟用 Windows 網路 (NetBIOS) 廣播	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。
WXA 群組	選擇「無」(預設) 或「群組一」
套用 NAT 原則	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。 **附註：** 一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。 **提示：**可以線上存取包含介面設定範例的參考視訊。例如，請參見如何在有重疊網路的站台到站台 VPN 中設定 VPN 上的 NAT。可以透過以下網址獲取其他視訊：https://www.sonicwall.com/en-us/support/video-tutorials。
允許 SonicPointN 三層管理	若要允許三層管理，請選擇此項。
透過該 SA 管理	選擇 **HTTPS**、**SSH**、, **SNMP**，或這三項的任何組合，以便透過 VPN 通道管理本機 SonicWall 防火牆。
透過 SA 使用者登入	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。 **附註：** HTTP 使用者登入不允許遠端驗證。

選項	定義
預設 LAN 閘道 (可選)	若想在進入此通道前路由透過 LAN 前往未知子網路目的地的流量，請選擇此項。例如，若選擇了**使用該 VPN 通道作為預設路由用於所有的網路流量** (在本頁面上**網路**檢視的**遠端網路**底下)，請輸入路由器位址。
VPN 原則繫結至	從下拉清單中選擇一個介面或區域。 **重要：**若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。

17 按一下**確定**。

18 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

以供應商憑證進行設定

附註：若要以使用供應商憑證的 IKE 來設定 VPN 原則，前提條件是 SonicWall 防火牆上必須已經安裝供應商憑證授權單位核發的有效憑證。

透過 SonicWall 防火牆，您可選擇使用供應商憑證進行驗證，而非使用 SonicWall 驗證服務。使用供應商憑證所需的手動程序較使用本機憑證來得多，因此實作公開金鑰基礎設施 (PKI) 是瞭解數位憑證關鍵元件的必要措施。

SonicWALL 支援以下兩個憑證供應商:

- VeriSign
- Entrust

若要使用 IKE 和第三方憑證建立 VPN SA：

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 按一下**新增**以建立新原則，或按一下**編輯**圖示以更新現有的原則。

4 在**驗證方法**欄位中，選擇**使用第三方憑證的 IKE**。**VPN 原則**視窗的 **IKE 驗證**區段中會顯示供應商憑證選項。

5 在**名稱**欄位中輸入安全關聯的名稱。

6 在 **IPsec 主要閘道名稱或者位址**欄位中輸入主要遠端 SonicWall 的 IP 位址或完整網域名稱 (FQDN)。

7 若有次要遠端 SonicWall，請在 **IPsec 次要閘道名稱或者位址**欄位中輸入其 IP 位址或完整網域名稱 (FQDN)。

8 在 **IKE 驗證**下，從**本機憑證**清單中選擇一個供應商憑證。設定此選項之前，必須已經匯入本機憑證。

9 從**對等 IKE ID 類型**下拉功能表中選擇以下其中一種對等 ID 類型:

對等 IKE ID 類型選項	定義
預設憑證 ID	從憑證的預設 ID 取得驗證。
辨別名稱 (DN)	驗證是基於憑證的「主旨識別名稱」欄位，所有憑證預設包含此欄位。必須針對站台對站台 VPN 輸入整個「識別名稱」欄位。不支援萬用字元。 「主旨識別名稱」的格式由憑證授權單位決定。常用欄位有「國家」(C=)、「組織」(O=)、「組織單位」(OU=)、「一般名稱」(CN=)、「縣市」(L=)等，取決於憑證授權單位。X.509 憑證中的實際「主旨識別名稱」欄位是一個二進位物件，符合時必須轉換為字串。這些欄位透過斜線分隔，例如：**/C=US/O=SonicWall, Inc./OU=TechPubs/CN=Joe Pub**。

對等 IKE ID 類型選項	定義
電子郵件 ID (UserFQDN)	基於**電子郵件 ID (UserFQDN)** 類型的驗證是以憑證的「主旨備用名稱」欄位為依據，*並非*所有憑證均預設包含此欄位。如果憑證包含「主旨備用名稱」，則必須使用此值。針對站台對站台 VPN，不能使用萬用字元，必須輸入完整的電子郵件 ID，這是因為站台對站台 VPN 預期連接一個對等點，而群組 VPN 則預期連接多個對等點。
網域名稱 (FQDN)	基於**網域名稱 (FQDN)** 類型的驗證是以憑證的「主旨備用名稱」欄位為依據，*並非*所有憑證均預設包含此欄位。如果憑證包含「主旨備用名稱」，則必須使用此值。針對站台對站台 VPN，不能使用萬用字元，必須輸入完整的電子郵件 ID，這是因為站台對站台 VPN 預期連接一個對等點，而群組 VPN 則預期連接多個對等點。
IP 位址 (IPv4)	基於 IPv4 IP 位址。

附註：若要查找憑證詳細資料 (主旨備用名稱、識別名稱等)，請導覽至系統安裝 | **裝置 > 憑證**頁面。

10 在**對等 IKE ID** 欄位中輸入 ID 字串。

11 按一下**網路**。

12 在**本機網路**底下，選擇以下其中一個選項:

- 如果特定本機網路可以存取 VPN 通道，請在**從清單中選擇本機網路**下拉清單中選擇一個本機網路。
- 如果流量可從任意本機網路發起，請選擇**任何位址**。如果對等點已選擇**使用該 VPN 通道作為預設路由用於所有的網路流量**，請使用此選項。自動新增的規則將建立在可信任區域和 VPN 區域之間。

13 在**從清單中選擇目的地網路**底下，選擇以下其中一個選項:

- 如果來自任何本機使用者的流量只有加密才可離開防火牆，請選擇**使用該 VPN 通道作為預設路由用於所有的網路流量**。

附註：只能設定一個 SA 來使用此設定。

- 或選擇**從清單選擇目的地網路**，並從下拉清單中選擇位址物件或群組。
- 若想支援 IKEv2 設定承載，請選擇「IKEv2 IP 集區」，並從下拉清單中選擇位址物件或 IP 集區網路。

14 按一下**建議**標籤。

15 在 **IKE（階段 1）建議**部分，選擇下列設定：

Main Mode	將 IKEv1 階段 1 建議與 IPsec 階段 2 建議一同使用。Suite B 加密選項對於 IKE 階段 1 設定中的 DH 群組可用，且對於 IPsec 階段 2 設定中的加密可用。
加強模式	一般在動態指派 WAN 位址時使用。將 IKEv1 階段 1 建議與 IPsec 階段 2 建議一同使用。Suite B 加密選項對於 IKE 階段 1 設定中的 DH 群組可用，且對於 IPsec 階段 2 設定中的加密可用。
IKEv2 模式	使所有交涉透過 IKEv2 通訊協定發生，而不是使用 IKEv1 階段。 **附註：**如果選擇 **IKE v2 模式**，VPN 通道的兩端都必須使用 IKE v2。若選擇此項，**DH 群組**、**加密**和**驗證**欄位將以灰色顯示且無法定義。

16 在 **IKE (階段 1) 建議**底下設定其餘選項的值。多數 VPN 設定可接受 **DH 群組**、**加密**、**驗證**和**存留時間**的預設值。

附註：若在**交換**欄位選擇 **IKEv2 模式**，則 **DH 群組**、**加密**和**驗證**欄位將以灰色顯示，且無法為這些選項做任何選擇。

附註：確保通道另一端的階段 1 值符合。

a 針對 **DH 群組**，處於**主模式**或**加強模式**時，可從多個 Diffie Hellman 交換中進行選擇:

Suite B 加密中內含的 Diffie Hellman 群組	其他 Diffie-Hellman 選項
256 位隨機 ECP 群組	組 1
384 位隨機 ECP 群組	組 2
521 位隨機 ECP 群組	組 5
192 位隨機 ECP 群組	組 14
224 位隨機 ECP 群組	

b 針對**加密**欄位，如果選擇了**主模式**或**加強模式**，請從下拉功能表中選擇 **DES**、**3DES** (預設)、**AES-128**、**AES-192** 或 **AES-256**。

c 針對**驗證**欄位，如果選擇了**主模式**或**加強模式**，請選擇 **MD5**、 **SHA-1** (預設)、**SHA256**、**SHA384** 或 **SHA512** 以增強驗證安全性。

d 針對所有**交換**模式，請輸入**存留時間 (秒)** 的值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

17 在 **IPsec (階段 2) 建議**區段中設定選項。多數 VPN SA 設定可接受**通訊協定**、**加密**、**驗證**、**啟用完全轉送保密**和**存留時間 (秒)** 的預設值。

附註：確保通道另一端的階段 2 值符合。

a 從**協定**功能表選擇所需的協定。

如果您在**協定**欄位中選擇了 **ESP**，則在**加密**欄位中可以從包含在 Suite B 加密中的 6 種加密演算法中進行選擇：

Suite B 加密選項	其他選項
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**無**

如果您在**通訊協定**欄位中選擇了 **AH**，**加密**欄位就會以灰色顯示，且無法選擇任何選項。

b 如果希望增加 Diffie-Hellman 金鑰交換以增強安全性，請選擇**啟用完全轉送保密**，再從 **DH 群組**功能表中選擇**群組 2**。

c 在**存留時間（秒）**欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

18 按一下**進階**標籤。

19 選擇您希望套用於 VPN 原則的任意設定選項:

選項	主模式或加強模式	IKEv2 模式
進階設定		
啟用保持運作	選擇此項，即可在此 VPN 通道的對等點之間使用活動訊號訊息，如果通道的一端發生故障，使用「保持活動」活動訊號，便可在兩端再度可用時自動重新交涉通道，而不必等待建議的存留時間過期。 **附註：** 當 VPN 原則設定為 VPN 上的 DHCP 中心閘道，或是主要閘道名稱或位址為 0.0.0.0，系統就會停用「保持活動」選項。	IKEv2 模式無法選擇。
阻止為 VPN 原則的自動建立存取規則	若*未*選擇 (預設)，則允許 VPN 流量穿越適當區域。	若*未*選擇 (預設)，則允許 VPN 流量穿越適當區域。
停用 IPsec 反重放	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達
啟用 Windows 網路 (NetBIOS) 廣播	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。

選項	主模式或加強模式	IKEv2 模式
啟用多點傳送	選擇此項，即可允許串流音訊 (包括 VoIP) 和視訊應用程式等多點傳送流量通過 VPN 通道。	選擇此項，即可允許串流音訊 (包括 VoIP) 和視訊應用程式等多點傳送流量通過 VPN 通道。
WXA 群組	選擇「無」(預設) 或「群組一」	選擇「無」(預設) 或「群組一」
僅顯示符合套件 B 的演算法	若只想顯示符合 Suite B 的演算法，請選擇此項。	若只想顯示符合 Suite B 的演算法，請選擇此項。
套用 NAT 原則	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。 **附註：** 一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。 **附註：** 一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。
啟用 OCSP 檢查	若想檢查 VPN 憑證狀態和在指定欄位中提供 **OCSP 回應者 URL**，請選擇此項。	若想檢查 VPN 憑證狀態和在指定欄位中提供 **OCSP 回應者 URL**，請選擇此項。
允許 SonicPointN 三層管理	允許存取點的三層管理。	允許存取點的三層管理。
透過該 SA 管理	此選項請選擇 **HTTPS** 以透過 VPN 通道管理本機 SonicWall 防火牆。	此選項請選擇 HTTPS 以透過 VPN 通道管理本機 SonicWall 防火牆。
透過 SA 使用者登入	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。 **附註：** HTTP 使用者登入不允許遠端驗證。	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。 **附註：** HTTP 使用者登入不允許遠端驗證。
預設 LAN 閘道 (可選)	若想在進入此通道前路由透過 LAN 前往未知子網路目的地的流量，請選擇此項。例如，若選擇了**使用該 VPN 通道作為預設路由用於所有的網路流量** (在本頁面上**網路**檢視的**遠端網路**底下)，請輸入路由器位址。	若想在進入此通道前路由透過 LAN 前往未知子網路目的地的流量，請選擇此項。例如，若選擇了**使用該 VPN 通道作為預設路由用於所有的網路流量** (在本頁面上**網路**檢視的**遠端網路**底下)，請輸入路由器位址。
VPN 原則繫結至	從下拉清單中選擇一個介面或區域。若使用 WAN 負載平衡，並希望 VPN 使用任一 WAN 介面，則區域 WAN 應為偏好的設定。 **重要：**若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。	從下拉清單中選擇一個介面或區域。若使用 WAN 負載平衡，並希望 VPN 使用任一 WAN 介面，則區域 WAN 應為偏好的設定。 **重要：**若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。

IKEv2 設定

選項	主模式或加強模式	IKEv2 模式
請不要在 IKE SA 協商時傳輸觸發封包		*未*選擇 (預設)。應只在對等點無法處理觸發封包，而需要互操作時選擇。 建議作法為包括觸發封包，以便幫助 IKEv2 回應者從安全原則資料庫中選擇正確的受保護 IP 位址範圍。並非所有方案都支援此功能，因此禁止某些 IKE 對等點包括觸發封包可能是適當的。
接收 Hash & URL 憑證類型	未針對主模式或加強模式啟用	如果裝置能夠傳送並處理雜湊和憑證 URL，而不是憑證本身，請選擇此項。若選擇此項，系統會傳送訊息給對等裝置，通知支援 HTTP 憑證查詢。
傳輸 Hash & URL 憑證類型		如果裝置能夠傳送並處理雜湊和憑證 URL，而不是憑證本身，請選擇此項。若選擇此項，系統會回應對等裝置傳來的訊息，確認支援 HTTP 憑證查詢。

20 按一下**確定**。

21 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

設定遠端 SonicWall 網路安全裝置

1 按一下 **VPN > 設定**頁面上的**新增**。隨即顯示 **VPN 原則**對話方塊。

2 在**一般**標籤中，從**驗證方法**下拉功能表中選擇**手動金鑰**。

3 在**名稱**欄位中輸入 SA 的名稱。

4 在 **IPSec 閘道名稱或位址**欄位中輸入本機連接的主機名稱或 IP 位址。

5 按一下**網路**標籤。

6 在**本機網路**下面，選擇以下其中之一：

- 如果特定本機網路可以存取 VPN 通道，請從**從清單中選擇本機網路**下拉功能表中選擇一個本機網路。
- 如果流量可從任意本機網路發起，請選擇**任何位址**。如果對等點已選擇**使用該 VPN 通道作為預設路由用於所有的網路流量**，請使用此選項。自動新增的規則將建立在可信的區域和 VPN 區域之間。

7 在**目的地網路**下面，選擇以下其中之一：

- 如果來自任何本機使用者的流量只有加密才可離開防火牆，請勾選**使用該 VPN 通道作為預設路由用於所有的網路流量**。

  附註：只能設定一個 SA 來使用此設定。

- 或選擇**從清單選擇目的地網路**，並選擇位址物件或組。

8 按一下**建議**標籤。

9 定義一個**傳入 SPI** 和一個**傳出 SPI**。SPI 是十六進位 (0123456789abcedf)，可以包括 3 到 8 個字元。

注意：每個安全關聯必須有唯一的 SPI，任何兩個安全關聯不能有相同的 SPI。然而，每個安全關聯的傳入 SPI 可以與傳出 SPI 相同。

10 多數 VPN SA 設定可以接受**通讯協定**、**加密**和**驗證**的預設值。

附註：通讯協定、**加密**和**驗證**的值必須與遠端防火牆上的值一致。

11 在**加密金鑰**欄位中輸入一個 48 字元十六進位加密金鑰，或使用預設值。此加密金鑰用於設定遠端 SonicWall 加密金鑰，因此應記錄下來以便設定遠端 SonicWall。

12 在**驗證金鑰**欄位中輸入一個 40 字元十六進位驗證金鑰，或使用預設值。記下此金鑰以便設定遠端 SonicWall 設定。

提示：有效的十六進位字元包括 0、1、2、3、4、5、6、7、8、9、a、b、c、d、e 和 f。1234567890abcdef 是有效 DES 或 ARCFour 加密金鑰的一個例子。如果輸入的加密金鑰不正確，瀏覽器視窗底部會顯示一條錯誤訊息。

13 按一下**進階**標籤，選擇您希望套用於 VPN 原則的下列任意可選設定：

- **封鎖為 VPN 原則自動建立存取規則**選項預設停用，以便 VPN 流量穿越適當的區域。
- 選擇**啟用 Windows 網路功能 (NetBIOS) 廣播**以允許透過瀏覽 Windows® 網上芳鄰來存取遠端網路資源。
- 選擇**允許加速**允許符合本原則的流量重新導向到 WAN 加速 (WXA) 裝置。
- 若要轉譯通過此 VPN 通道通訊的本機和/或遠端網路，請選擇**套用 NAT 原則**。此時顯示兩個下拉功能表：
  - 若要對本機網路執行網路位址轉譯，請在**已轉譯的本機網路**功能表中選擇或建立位址物件。
  - 若要轉譯遠端網路，請在**已轉譯的遠端網路**下拉功能表中選擇或建立位址物件。

  附註：一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。
- 若要通過 VPN 通道管理遠端 SonicWall，請從**透過該 SA 管理**中選擇 **HTTP**、**SSH**、**SNMP**，或這三項的任何組合。
- 在**使用者透過 SA 登入**中選擇 **HTTP** 和/或 **HTTPS**，以便使用者利用 SA 登入。

  附註：HTTP 使用者登入不允許遠端認證。
- 若有一個閘道的 IP 位址，請將其輸入**預設 LAN 閘道（可選）**欄位。
- 從 **VPN 原則繫結至**功能表選擇一個介面。

  重要：若兩個介面的 VPN 閘道 IP 位址相同，則不能從 **VPN 原則繫結至**下拉功能表中選擇兩個不同的 WAN 介面。

14 按一下**確定**。

15 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

提示：由於已啟用 NetBIOS，使用者可以在其 Windows 網上芳鄰中查看遠端電腦。使用者還可以輸入伺服器或工作站的遠端 IP 位址，從而存取遠端 LAN 上的資源。

設定 VPN 容錯移轉到固定路由

可以設定一個固定路由，作為 VPN 通道停止工作時的備用路由。定義路由原則時，**允許 VPN 路徑優先**選項用於為 VPN 通道建立一個備用路由，以及將優先權賦予目的地位址物件相同的 VPN 流量。這導致以下行為：

- 當 VPN 通道使用中時：如果啟用**允許 VPN 路徑優先**選項，則自動停用與 VPN 通道的目的地位址物件符合的固定路由。所有流量均通過 VPN 通道路由至目的地位址物件。
- 當 VPN 通道停止工作時：自動啟用與 VPN 通道的目的地位址物件符合的固定路由。前往目的地位址物件的所有流量都通過固定路由進行路由。

*SonicWall SonicOS 6.5 系統安裝*提供更多有關設定網路路由原則的資訊。

若要將固定路由設定為 VPN 容錯移轉：

1 選擇**管理**檢視。

2 在**系統安裝**底下選擇**網路 > 路由**。

3 按一下**路由原則 > 新增**。

4 選擇適當的**來源**、**目的地**、**服務**、**閘道**和**介面**。

5 將**度量**定義為 **1**。

6 勾選方塊以啟用**允許 VPN 路徑優先**。

7 按一下**確定**。

3

VPN 自動佈建

您可設定各種類型的 IPsec VPN 原則，例如站台對站台原則 (包含 GroupVPN) 和基於路由的原則。如需設定這類原則的具體詳細資訊，請參考以下章節:

- 站台對站台 VPN
- 路由式 VPN

本節包含以下主題:

- 關於 VPN 自動佈建
- 設定 VPN 存取點伺服器
- 設定 VPN 存取點用戶端

關於 VPN 自動佈建

SonicOS 6.2.7 採納 VPN 自動佈建功能，簡化兩個 SonicWall 防火牆間站台到站台 VPN 的佈建。本章節提供概念性資訊並說明如何設定和使用 SonicOS VPN 自動佈建功能。

主題：

- 至關重要的 SonicOS VPN 自動佈建
- SonicOS VPN 自動佈建的優點
- SonicOS VPN 自動佈建的運作方式
- 支援的平台

至關重要的 SonicOS VPN 自動佈建

VPN 自動佈建功能簡化 SonicWall 防火牆的 VPN 佈建。這在大規模的 VPN 部署中特別實用。在傳統軸幅式的站台到站台 VPN 設定中，輪輻側有許多複雜的設定工作需要執行，例如設定安全關聯以及設定受防護的網路。在有許多遠端閘道或輪輻的大型部署中，這可能是個挑戰。SonicOS VPN 自動佈建提供簡化的設定程序，以減少遠端 VPN 對等上的許多設定步驟。

附註：在軸幅式站台到站台 VPN 設定中的***集線器***，可以指使用各種名稱，例如伺服器、集線器閘道、主要閘道、中心閘道。在 SonicOS VPN 自動佈建功能的環境中，***VPN 存取點伺服器***一詞是用於集線器。同樣地，***VPN 存取點用戶端***一詞是用於指輪輻、用戶端、遠端閘道、遠端防火牆或對等防火牆。

SonicOS VPN 自動佈建的優點

VPN 自動佈建功能的顯著優點是容易使用。類似 SonicWall 全域 VPN 用戶端 (GVC) 的佈建程序，這是透過隱藏 SonicOS 管理員的複雜初始設定來實現。

使用 SonicWall GVC 時，使用者只要指向在閘道的 GVC；安全性和連接設定都會自動發生。SonicOS VPN 自動佈建提供佈建站台到站台軸幅式設定的類似解決方案，簡化大規模部署的繁瑣事項。

新增的好處是在初始 VPN 自動佈建後，可在中心閘道控制原則變更以及在輪輻端自動更新。此解決方案在中央管理為首要要務的企業和受管理服務部署中尤其具備吸引力。

SonicOS VPN 自動佈建的運作方式

VPN 自動佈建有兩個步驟：

- 針對中心閘道或 VPN 存取點伺服器的 SonicWall 自動佈建伺服器設定：
- 針對遠端防火牆或 VPN 存取點用戶端的 SonicWall 自動佈建用戶端設定：

兩者的設定都是透過在 SonicOS 的 **VPN > 基本設定**頁面上新增 VPN 原則。

而在伺服器模式下，如同在傳統的站台到站台 VPN 原則中，您設定安全關聯 (SA)、受保護的網路和其他設定欄位。在用戶端模式下，則需要有限制的設定。大多數情況，遠端防火牆管理員只需要設定 IP 位址即可連線到對等伺服器 (中心閘道)，然後就能建立 VPN。

附註：SonicWall 不建議將單一設備同時設定為 AP 伺服器和 AP 用戶端。

仍提供 IP 安全性的主要元素時，SonicOS VPN 自動佈建在用戶端側是簡單的：

存取控制	網路存取控制是由 VPN 存取點伺服器提供。從 VPN 存取點用戶端觀點，目的地網路完全在 VPN 存取點伺服器管理員的控制之下。不過，會提供機制控制對於 VPN 存取點用戶端區域網路的存取。
驗證	使用機器驗證憑證來提供驗證。在 IPsec 建議的階段 1 中，網路金鑰交換 (IKE) 通訊協定利用*預先共用金鑰*或*數位簽章*來提供機器層級的驗證。設定 VPN 原則時，您可以從這些驗證方法中選擇一種： 對於預先共用金鑰驗證方法，管理員輸入 VPN 自動佈建用戶端 ID 和金鑰或密碼。對於數位簽章驗證方法，管理員從防火牆的本機憑證儲存區選取包含用戶端 ID 的 X.509 憑證。該憑證必須之前已儲存在防火牆上。 為增加安全性，支援透過 XAUTH 的使用者層級認證。使用者認證是在新增 VPN 原則時輸入。XAUTH 使用金鑰或神奇 Cookie 而非使用質詢/回應機制 (使用者動態輸入使用者名稱和密碼) 來將它們提取為授權記錄。除了提供額外的驗證外，使用者認證也提供進一步的遠端資源和/或 VPN 存取點用戶端所使用的本機代理位址的存取控制。使用者認證允許在多個 VPN 存取點用戶端裝置間共用單一的 VPN 存取點伺服器原則，只要區別後續的網路佈建即可。
資料機密性和完整性	資料機密性和完整性是由封裝的安全有效承載 (ESP) 金鑰套件在 IPsec 建議的階段 2 提供。

在會影響 VPN 存取點用戶端設定的 VPN 存取點伺服器發生原則變更時，VPN 存取點伺服器會使用 IKE 重設金鑰機制來確保新的安全關聯並建立適當的參數。

有關建立 IKE 階段 1 安全關聯

既然 VPN 存取點用戶端的目標是容易使用，許多 IKE 和 IPsec 參數便都是預設或自動交涉。VPN 存取點用戶端會起始安全關聯的建立，但是在起始時並不知道 VPN 存取點伺服器的設定。

為允許建立 IKE 階段 1，選擇會受限；VPN 存取點用戶端處理多種轉換 (結合安全性參數)，VPN 存取點伺服器可由此選擇其設定值。階段 1 轉換包含下列參數：

- Authentication - 執行以下任一動作：
  - PRESHRD - 使用預先共用密碼。
  - RSA_SIG - 使用 X.509 憑證。
  - SW_DEFAULT_PSK - 使用預設佈建金鑰。
  - XAUTH_INIT_PRESHARED - 使用預先共用密碼結合 XAUTH 使用者認證。
  - XAUTH_INIT_RSA - 使用 X.509 憑證結合 XAUTH 使用者認證。
  - SW_XAUTH_DEFAULT_PSK - 使用預設佈建金鑰結合 XAUTH 使用者認證。

  所有以上轉換包含階段 1 建議設定的受限或預設值：
  - 交換 - 加強模式
  - 加密 - AES-256
  - 雜湊 - SHA1
  - DH 群組 - Diffie Hellman 群組 5
  - 存留時間（秒數） - 28800

透過從 VPN 存取點用戶端建議中所包含的選擇單一轉換，VPN 存取點伺服器進行回應。如果 VPN 存取點伺服器選擇使用 XAUTH 驗證方法的轉換，VPN 存取點用戶端會等候階段 1 後的 XAUTH 質詢完成。如果選擇非 XAUTH 轉換，則會開始佈建階段。VPN 存取點伺服器會以適當的原則值佈建 VPN 存取點用戶端，包括共用密碼，如果一個是在 VPN 存取點伺服器上設定，且 VPN AP 客戶 ID 在 VPN 存取點伺服器設定。

在階段 1 之後，SA 會建立和原則佈建也已完成，目的地網路便會顯示在 **VPN > 設定**頁面的 **VPN 原則**區段中。

有關使用佈建原則建立 IKE 階段 2

在 VPN 存取點佈建交易期間接收的值是用於建立任何後續的階段 2 安全關聯。針對各個目的地網路，會起始個別的階段 2 SA。為觸發階段 2 SA 交涉，流量必須從遠端側後方起始。SA 是根據在**網路**標籤 (參見在網路標籤上設定 VPN 存取點伺服器設定) 上設定 VPN 存取點伺服器原則設定時指定的位址物件建立。

附註：如果在 AP 伺服器上相同 VPN 原則與多個遠端 AP 用戶端共用，每個遠端網路必須特別列為唯一的位址物件。在**網路**標籤上設定 VPN 存取點伺服器原則設定期間，新增到**遠端網路**區段時，可在位址群組中摘要個別位址物件。單一位址物件不可用於摘要多個遠端網路，因為 SA 是根據*特定*位址物件建立的。

成功時，產生的通道會顯示在**目前使用中的 VPN 通道**清單中。

NAT 規則也會新增到**網路 > NAT 原則**表。

由於階段 2 參數是由 VPN 存取點伺服器佈建，所以不可能設定不符。如果階段 2 參數在 VPN 存取點伺服器變更，所有階段 1 和階段 2 安全關聯會被刪除並重新交涉，確保原則同步。

支援的平台

以下執行 SonicOS 6.2.7 以上的 SonicWall 設備支援 SonicOS VPN 自動佈建：

- SonicWall SuperMassive™ 9200、9400、9600
- SonicWall NSA 2600、3600、4600、5600、6600
- SonicWall TZ300/300W、TZ400/400W、TZ500/500W、TZ600
- SonicWall SOHO Wireless

對於在 SonicWall GMS 管理下的設備，SonicOS VPN 自動佈建在以下版本中受支援：

- SonicWall GMS 8.3 和更高版本

設定 VPN 存取點伺服器

VPN 存取點伺服器設定值是在伺服器 (集線器) 防火牆上設定，只要在 SonicOS 的 **VPN > 設定**頁面上新增 VPN 原則即可。

由於將描述的設定數目，設定會在多個區段中展示：

- 啟動 VPN 存取點伺服器設定
- 在一般標籤上設定 VPN 存取點伺服器設定
- 在網路標籤上設定 VPN 存取點伺服器設定
- 在建議標籤上設定進階設定
- 在進階標籤上設定進階設定

啟動 VPN 存取點伺服器設定

若要使用 SonicOS VPN 自動佈建開始設定 VPN 存取點伺服器防火牆：

1 導覽至 **VPN > 設定**頁面，

2 為**檢視 IP 版本**選擇 **IPv4**。

3 在 **VPN 原則**表下，按一下**新增**。隨即顯示 **VPN 原則**對話方塊。

4 在**驗證方法:**下拉功能表中，選擇 **SonicWall 自動佈建伺服器**。

附註：頁面底部的**進階.../隱藏**按鈕可切換**建議**和**進階**選項的顯示和隱藏。這兩個選項上的設定包含可由您自行變更的預設值。

在一般標籤上設定 VPN 存取點伺服器設定

若要在一般標籤上設定 VPN 存取點伺服器設定：

1 在**名稱**欄位中，輸入 VAP 原則的描述性名稱。

2 若是**驗證方法**，可以選擇：

- **預先共用密碼** - 使用您接下來要輸入的 VPN 自動佈建用戶端 ID 和共用密碼。預設情況下已核取此選項。繼續步驟 3。
- **憑證** - 使用您接下來要選取的 X.509 憑證 (憑證必須之前已儲存在設備上)。跳至步驟 8。

  附註：如果 VPN 存取點伺服器原則要共用 (如在軸幅式部署中)，SonicWall 建議使用 X.509 憑證提供真正的驗證並且防止受到中間人攻擊。

3 若**驗證方法**選擇了**預先共用密碼**，則需在 **SonicWall 設定**底下的 **VPN AP 客戶 ID** 欄位中輸入 VPN 自動佈建用戶端 ID。系統會在此欄位中自動填入您在**名稱**欄位輸入的值，不過可以變更。

附註：此 VPN 原則值必須在 AP 伺服器和 AP 用戶端兩端相符。單一 AP 伺服器原則也可以用來終止多個 AP 用戶端。

4 勾選**使用預設佈建的金鑰**方塊，以允許 VPN 存取點用戶端使用所有 SonicWall 設備已知的預設金鑰，進行*初始*安全關聯。一旦建立 SA，VPN 存取點伺服器上設定的**預先共用密碼**會佈建到 VPN 存取點用戶端供未來使用。

如果清除此核取方塊，VPN 存取點用戶端必須使用已設定的共用密碼。這允許管理員只修改已在 VPN 存取點伺服器上設定的共用密碼，然後短暫允許預設佈建金鑰，以使用新的共用密碼值更新 VPN 存取點用戶端。

附註：為擁有最佳安全性，SonicWall 建議預設佈建金鑰選項僅在短時間啟用，也就是在管理審查下 VPN 存取點用戶端可使用共用密碼佈建期間啟用。

5 如有需要，可清除**隱藏共用密碼**核取方塊，然後再於**共用密碼**欄位中輸入任何值。預設情況下此核取方塊是勾選狀態，會隱藏輸入的字元。如果重新勾選此核取方塊，則**共用密碼**欄位的值會自動複製到**確認共用密碼**欄位。

6 在**共用密碼**欄位中輸入共用密碼。最少必須包含 4 個字元。

如果**使用預設佈建的金鑰**核取方塊為勾選狀態，則在 VPN 存取點伺服器上設定的**預先共用密碼**會佈建到 VPN 存取點用戶端。如果**使用預設佈建的金鑰**為清除狀態，則也必須在 VPN 存取點用戶端上設定共用密碼。

7 在**確認共用密碼**欄位中，再次輸入共用密碼。它必須與在**共用密碼**欄位中輸入的值相符。

8 如果您對**驗證方法**選擇了**憑證**，則在 **SonicWall 設定**下，從**本機憑證**下拉功能表選擇所要的憑證。

9 從 **VPN AP 客戶 ID 類型**下拉功能表中選擇以下選項之一：

- **辨別名稱 (DN)**
- **電子郵件 ID (UserFQDN)**
- **網域名稱 (FQDN)**
- **IP 位址 (IPv4)**

10 在 **VPN AP 客戶 ID 篩選條件**中，輸入相符字串或篩選條件，用於套用到 IKE 交涉期間顯示的憑證 ID。

11 繼續到在網路標籤上設定 VPN 存取點伺服器設定。

在網路標籤上設定 VPN 存取點伺服器設定

若要在網路標籤上設定 VPN 存取點伺服器設定：

1 按一下**網路**標籤。

2 在**本機網路**下，勾選**需要透過 XAUTH 驗證 VPN AP 用戶端**核取方塊，強制使用使用者認證，以增加建立 SA 時的安全性。

3 如果啟用 XAUTH 選項，從 **XAUTH 使用者的使用者群組**下拉功能表，選擇用於所允許使用者的使用者群組。您可以選擇現有群組，例如 *Trusted Users* 或其他標準群組，或者選擇**建立一個新的使用者群組**以建立自訂群組。

對於每位已驗證的使用者，驗證服務傳回一個或多個網路位址，這些位址會在佈建交換期間傳送至 VPN 存取點用戶端。

如果啟用 XAUTH 且選擇了使用者群組，在 VPN 存取點用戶端側的使用者必須符合下列條件才能成功驗證：

- 使用者必須屬於所選的使用者群組。
- 使用者可以通過在**使用者 > 設定 > 使用者驗證方法**中設定的驗證方法。
- 使用者有 VPN 存取權限。

4 如果 XAUTH 選項停用，從**允許未驗證的 VPN AP 用戶端存取**下拉功能表選擇一個網路位址物件或群組，或選擇**建立新位址物件/群組**以建立自訂物件或群組。所選的物件定義可透過此 VPN 連線存取的位址或網域的清單。它會在佈建交換期間傳送到 VPN 存取點用戶端，然後用做 VPN 存取點用戶端的遠端代理 ID。

5 在**遠端網路**下，選擇以下其中一個選項按鈕，然後若適用從關聯的清單進行選擇：

- **從清單中選擇目的地網路** - 從在 VPN 存取點用戶端側實際為可路由網路的遠端位址物件下拉功能表選擇網路物件，或建立自訂物件。

  附註：VPN 自動佈建不支援使用包含所有 AP 用戶端受保護子網路的「超級網路」。若要允許含有不同受保護子網路的多個 AP 用戶端連接到相同 AP 伺服器，請設定包括所有 AP 用戶端受保護子網路的位址群組，並在**從清單中選擇目的地網路**欄位中使用該群組。此位址群組必須保持在最新，因為會新增新的 AP 用戶端。

- **透過驗證服務獲取 NAT 代理** - 選擇此選項讓 RADIUS 伺服器為使用者傳回框架 IP 位址屬性，VPN 存取點用戶端會用此在向下傳送流量到 IPsec 通道之前 NAT 其內部位址。
- **選擇 NAT 集區** - 從下拉功能表選擇網路物件或建立自訂物件。選擇的物件會指定要指派給 VPN 存取點用戶端的位址集區，以搭配 NAT 使用。用戶端會轉譯其內部位址為 NAT 集區中的位址之後，再將流量向下傳送到 IPsec 通道。

  附註：部署 VPN 自動佈建時，您需要配置夠大的 NAT IP 位址集區給所有現有和預期的 VPN 存取點用戶端。否則，其他 VPN 存取點用戶端無法正常運作，如果集區中的所有 IP 位址已經配置。

  附註：設定大型 IP 集區不會耗用多於小型集區的記憶體，所以是安全且最佳的做法，來配置夠大的集區以提供冗餘。

6 繼續到在建議標籤上設定進階設定。

在建議標籤上設定進階設定

設定的參數會在階段 2 建立之前自動佈建到 VPN 存取點用戶端，所以在 VPN 存取點伺服器和 VPN 存取點用戶端之間沒有機會產生設定差異。

若要在建議標籤上設定 VPN 存取點伺服器設定：

1 在**一般**或**網路**標籤上，按一下**進階**按鈕以顯示**建議**標籤。

2 按一下**建議**標籤。

3 在 **IKE (階段 1) 建議**下，輸入以秒為單位的階段 1 建議存留時間。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

為簡化自動佈建，此區段中的其他欄位為灰顯並預設為：

- **交換**：**加強模式**
- **DH 群組**：**組 5**
- **加密**：**AES-256**
- **驗證**：**SHA1**

4 在 **Ipsec (階段 2) 建議**下，從**加密**下拉功能表選擇所要的加密演算法。預設為 **3DES**。

通訊協定欄位為灰顯且預設為 **ESP** 以使用封裝的安全承載 (ESP) 金鑰套件。

5 從**驗證**下拉功能表中選擇所需的驗證加密方法。預設值為 **SHA1**。

6 如果希望增加 Diffie-Hellman 金鑰交換以增強一層安全性，請選擇**啟用完全轉送保密**核取方塊。若已選擇，則會顯示 **DH 群組**下拉清單。從清單選擇所要的群組。預設為群組 2。

7 在**存留時間（秒）**欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

8 繼續到在進階標籤上設定進階設定。

在進階標籤上設定進階設定

若要在進階標籤上設定 VPN 存取點伺服器設定：

1 按一下**進階**標籤。

2 勾選**停用 IPsec 反重放**核取方塊，以防止丟棄有重複序號的封包。

3 選擇**啟用多點傳送**核取方塊以允許 IP 多點傳送流量，如串流音訊（包括 VoIP）和視訊應用程式等，從 VPN 存取點伺服器透過使用此原則建立的任何 VPN 存取點用戶端 SA 傳遞。

4 如果使用 SonicWall WAN 加速，從 **WXA 群組**下拉清單選取一個值。

5 選擇性地勾選**僅顯示符合套件 B 的演算法**。

6 選擇**允許 SonicPointN 三層管理**以允許管理 SonicWall SonicPoint 無線透過 VPN 通道存取裝置。

7 對於**透過該 SA 管理**，勾選一個或多個核取方塊，以允許遠端使用者透過使用 **HTTPS**、**SSH** 或 **SNMP** 的 VPN 通道管理 VPN 存取點伺服器。

8 對於**透過 SA 使用者登入**，勾選一個或多個核取方塊，以允許遠端使用者透過使用 **HTTP** 或 **HTTPS** 的 VPN 通道登入。

9 在**預設 LAN 閘道（可選）**欄位中，選擇性地輸入 VPN 存取點伺服器的預設 LAN 閘道 IP 位址。如果為特定流量找不到固定路由，VPN 存取點伺服器會將流量轉送出設定的預設 LAN 閘道。

> **附註：**此選項在部分版本的 SonicOS 中可能沒有作用。

10 在 **VPN 原則繫結至**下拉功能表中選擇介面或區域，將此 VPN 原則繫結至特定介面或區域。

11 完成時，按一下**確定**。

設定 VPN 存取點用戶端

VPN 存取點用戶端設定是在用戶端防火牆上設定，只要在 SonicOS 中的 **VPN > 設定**頁面上新增 VPN 原則即可。

若要使用 SonicOS VPN 自動佈建設定遠端用戶端防火牆設定：

1 導覽至 **VPN > 設定**頁面。

2 為**檢視 IP 版本**選擇 **IPv4**。

3 在 **VPN 原則**表下，按一下**新增**。隨即顯示 **VPN 原則**對話方塊。

4 在**驗證方法:**下拉功能表中，選擇 **SonicWall 自動佈建用戶端**。頁面即重新整理為不同欄位。

5 在**名稱**欄位中，輸入 VAP 原則的描述性名稱。

6 在 **IPsec 主要閘道名稱或位址**欄位，輸入 VPN 存取點伺服器的完整網域名稱 (FQDN) 或 IPv4 位址。

7 若是**驗證方法**，可以選擇：

- **預先共用密碼** - 使用您接下來要輸入的 VPN 自動佈建用戶端 ID 和共用密碼。預設情況下已核取此選項。繼續步驟 8。
- **憑證** - 使用您接下來要選取的 X.509 憑證 (憑證必須之前已儲存在設備上)。跳至步驟 14。

8 如果您對**驗證方法**選擇了**預先共用密碼**，則在 **SonicWall 設定**下，將 VPN 自動佈建用戶端 ID 輸入到 **VPN AP 客戶 ID** 欄位中。

用戶端 ID 取決於 VPN 存取點伺服器的設定 (SonicWall 防火牆設定為 **SonicWall 自動佈建伺服器**)。

附註：此 VPN 原則值必須在 AP 伺服器和 AP 用戶端兩端相符。單一 AP 伺服器原則也可以用來終止多個 AP 用戶端。

9 選擇性勾選**使用預設佈建的金鑰**核取方塊，以使用所有 SonicWall 設備已知的預設金鑰，進行*初始*安全關聯。在建立 SA 之後，VPN 存取點伺服器上設定的**預先共用密碼**會佈建到 VPN 存取點用戶端供未來使用。

附註：VPN 存取點伺服器必須設定為接受預設佈建金鑰。若未如此設定，SA 建立會失敗。

如果已選擇**使用預設佈建的金鑰**，請跳到步驟 13。

10 如果未選擇**使用預設佈建的金鑰**核取方塊，則選擇性清除**隱藏共用密碼**核取方塊，之後再在**共用密碼**欄位中進行輸入。預設情況下此核取方塊是勾選狀態，會隱藏輸入的字元。如果重新勾選此核取方塊，則**共用密碼**欄位的值會自動複製到**確認共用密碼**欄位。

11 在**共用密碼**欄位中，輸入共用密碼。這必須與 VPN 存取點伺服器上設定的共用密碼相同，並且最少必須包含四個字元。

12 在**確認共用密碼**欄位中，再次輸入共用密碼。它必須與在**共用密碼**欄位中輸入的值相符。

13 跳到步驟 15 以取得在**使用者設定**下輸入使用者認證的相關資訊。使用者認證為選擇性。

14 如果您對**驗證方法**選擇了**憑證**，則在 **SonicWall 設定**下，從**本機憑證**下拉功能表選擇所要的憑證。

15 在**使用者設定**下，將要用於選擇性使用者認證的使用者名稱輸入**使用者名稱**欄位中。此使用者名稱是透過 XAUTH 傳送以進行為使用者層級的驗證。

16 選擇性清除**遮罩使用者密碼**核取方塊，之後再在**使用者密碼**欄位中進行輸入。預設情況下選擇此核取方塊。如果選擇，輸入的字元會以點狀顯示。清除此核取方塊會以純文字顯示值，並自動複製在**使用者密碼**欄位中輸入的值到**確認使用者密碼**欄位。

17 在**使用者密碼**欄位中，輸入使用者密碼。

18 在**確認使用者密碼**欄位中，再次輸入使用者密碼。

19 就緒時，按一下**確定**以新增 VPN 原則。

4

路由式 VPN

基於原則 (或站點對站點) 的方法會強制 VPN 原則設定包括網路拓撲設定。詳細資料，請參閱站台對站台 VPN。這使得難以設定和維護有不斷變化的網路拓撲的 VPN 原則。

採用基於路由的 VPN 方法時，VPN 原則設定不包括網路拓撲設定。VPN 原則設定在兩個端點之間建立一個未編號的通道介面。隨後便可將靜態或動態路由新增到此通道介面。基於路由的 VPN 方法將網路設定從 VPN 原則設定變更為固定或動態路由設定。

基於路由的 VPN 不僅使 VPN 原則的設定和維護更容易，且提供了靈活的流量路由方式。您可以通過乾淨或冗餘的 VPN 為重疊網路定義多個路徑。

有關自動佈建 VPN 網路的資訊，請參閱 VPN 自動佈建瞭解詳情。

主題：

- 術語
- 使用基於路由的 VPN
- 網路的備援靜態路由

術語

本節中會用到以下術語:

VPN 通道原則	在無本機/遠端受防護網路的情況下設定的原則。發出封包時，SonicOS 無需查找任何通道原則。
VPN 通道介面	在**網路 > 介面**頁面上建立的編號通道介面，並繫結到通道原則。此介面將設定為主動發出網路監控原則、Syslog 原則等封包的路由項目或 SonicOS App 的輸出介面。SonicOS 通過 VPN 通道發出封包時，邏輯上與通過實體介面傳送封包相同，只是需要加密封包。
編號的通道介面	編號的通道介面具有 IP 位址。編號的通道介面是在**網路 > 介面**頁面上透過新增 VPN 通道介面來建立。從功能上看，編號通道介面是未編號通道的超集。您可以標準介面的相同方式設定編號的通道介面，包括 HTTPS、Ping、SNMP 和 SSH 管理、HTTP 和 HTTPS 使用者登入以及片段處理。您可以在設定 NAT 原則、防火牆存取控制清單和路由包括所有類型的動態路由 (RIP、OSPF、BGP) 時，使用編號的通道介面。
未編號的通道介面	未編號的通道介面沒有 IP 位址。未編號的通道介面是您在使用原則類型的通道介面設定 VPN 原則時建立的。預設其適用於簡易基於路由的 VPN，並且不需要 IP 位址。如果啟用原則設定對話的進階標籤中的**允許進階路由**選項，未編號的通道介面可以搭配使用 RIP 和 OSPF 動態路由。使用未編號的通道介面設定 RIP 或 OSPF 時，會從實體或邏輯 (VLAN) 介面借用 IP 位址。

使用基於路由的 VPN

基於路由的 VPN 設定分為兩步。

1 建立通道介面。用於保護兩個端點間流量的加密套件，需在通道介面中定義。

2 利用通道介面建立一個固定或動態路由。

當遠端閘道新增一個類型為**通道介面**的原則時，便會建立通道介面。通道介面必須繫結到一個實體介面，此實體介面的 IP 位址用作通道封包的源位址。

主題：

- 新增通道介面
- 為通道介面建立靜態路由

新增通道介面

若要新增通道介面：

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **VPN > 基本設定**。

3 按一下**新增**按鈕。

4 在**一般**標籤中，選擇原則類型為**通道介面**。

5 在**名稱**欄位中輸入易記的名稱。

6 按一下**建議**。

7 在 **IKE (階段 1) 建議**底下，從**交換**下拉功能表中選擇以下其中一個選項:

Main Mode	將 IKEv1 階段 1 建議與 IPsec 階段 2 建議一同使用。Suite B 加密選項對於 IKE 階段 1 設定中的 DH 群組可用，且對於 IPsec 階段 2 設定中的加密可用。
加強模式	一般在動態指派 WAN 位址時使用。將 IKEv1 階段 1 建議與 IPsec 階段 2 建議一同使用。Suite B 加密選項對於 IKE 階段 1 設定中的 DH 群組可用，且對於 IPsec 階段 2 設定中的加密可用。
IKEv2 模式	使所有交涉透過 IKEv2 通訊協定發生，而不是使用 IKEv1 階段。 **附註：**如果選擇 **IKE v2 模式**，VPN 通道的兩端都必須使用 IKE v2。若選擇此項，**DH 群組**、**加密**和**驗證**欄位將以灰色顯示且無法定義。

8 在 **IKE (階段 1) 建議**底下設定其餘選項的值。多數 VPN 設定可接受 **DH 群組**、**加密**、**驗證**和**存留時間**的預設值。

附註：確保通道另一端的階段 1 值符合。

a 針對 **DH 群組**，處於**主模式**或**加強模式**時，可從多個 Diffie Hellman 交換中進行選擇:

Suite B 加密中內含的 Diffie Hellman 群組	**其他 Diffie-Hellman 選項**
256 位隨機 ECP 群組	組 1
384 位隨機 ECP 群組	組 2
521 位隨機 ECP 群組	組 5
192 位隨機 ECP 群組	組 14
224 位隨機 ECP 群組	

b 針對**加密**欄位，如果選擇了**主模式**或**加強模式**，請從下拉功能表中選擇 **DES**、**3DES** (預設)、**AES-128**、**AES-192** 或 **AES-256**。

c 針對**驗證**欄位，如果選擇了**主模式**或**加強模式**，請選擇 **SHA-1** (預設)、**MD5**、**SHA256**、**SHA384** 或 **SHA512** 以增強驗證安全性。

d 針對所有**交換**模式，請輸入**存留時間 (秒)** 的值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

9 在 **IPsec (階段 2) 建議**區段中設定選項。多數 VPN SA 設定可接受**通訊協定**、**加密**、**驗證**、**啟用完全轉送保密**和**存留時間 (秒)** 的預設值。

附註：確保通道另一端的階段 2 值符合。

a 在**通訊協定**欄位中，選擇 **ESP** 或 **HA**。

b 如果您在**通訊協定**欄位選擇了 **ESP**，則可在**加密**欄位從 Suite B 加密所包含的 6 種加密演算法中進行選擇:

Suite B 加密選項	其他選項
AESGCM16-128	**DES**
AESGCM16-192	**3DES**
AESGCM16-256	**AES-128**
AESGMAC-128	**AES-192**
AESGMAC-192	**AES-256**
AESGMAC-256	**無**

附註：如果您在**通訊協定**欄位中選擇了 **AH**，**加密**欄位就會以灰色顯示，且無法選擇任何選項。

c 在「驗證」欄位中，從下拉清單選擇驗證方法:

- **MD5**
- **SHA1**
- **SHA256**
- **SHA384**
- **SHA512**
- **AES-XCBC**

d 若要增強安全性，請選擇**啟用完全轉送保密**。

e 在**存留時間（秒）**欄位中輸入一個值。預設值為 **28800**，強制通道每隔 8 小時重新交涉和交換金鑰。

10 下列進階選項可供設定；預設為不選擇任何項目:

選項	主模式或加強模式	IKEv2 模式
進階設定		
啟用保持運作	基於路由的介面無法選擇。	基於路由的介面無法選擇。

選項	主模式或加強模式	IKEv2 模式
停用 IPsec 反重放	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達	反重放是一種局部序列完整性，可偵測到重複 IP 資料包 (在有限時間範圍內) 的到達
允許進階路由	在**網路 > 路由**頁面上新增此通道介面到**路由通訊協定**表的介面清單中。	在**網路 > 路由**頁面上新增此通道介面到**路由通訊協定**表的介面清單中。
	附註：如果進階路由 (RIP、OSPF) 使用通道介面，則必須勾選此選項。使用此可選設定可避免新增所有的通道介面到**路由通訊協定**表中，有助於簡化路由設定。	
啟用傳輸模式		**IKEv2 模式**無法使用。
啟用 Windows 網路 (NetBIOS) 廣播	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。	選擇此項，即可允許透過瀏覽 Windows 網路上的芳鄰來存取遠端網路資源。
啟用多點傳送	選擇此項，即可允許串流音訊 (包括 VoIP) 和視訊應用程式等多點傳送流量通過 VPN 通道。	選擇此項，即可允許串流音訊 (包括 VoIP) 和視訊應用程式等多點傳送流量通過 VPN 通道。
WXA 群組	選擇「無」(預設) 或「群組一」	選擇「無」(預設) 或「群組一」
僅顯示符合套件 B 的演算法	若只想顯示符合 Suite B 的演算法，請選擇此項。	若只想顯示符合 Suite B 的演算法，請選擇此項。
套用 NAT 原則	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。	若希望防火牆轉譯透過 VPN 通道進行通訊，並經過本機網路、遠端網路或兩種網路的流量，請選擇此項。若選擇此項，請從兩個下拉功能表中選擇**已轉譯的本機網路**或**已轉譯的遠端網路**或其中一項。
	附註：一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。	**附註：**一般而言，如果通道需要 NAT，則應轉譯本機或遠端網路，而非二者都要轉譯。通道兩端使用相同或重疊的子網路時，**套用 NAT 原則**特別有用。
允許 SonicPointN 三層管理	允許 SonicPointN 的三層管理。	允許 SonicPointN 的三層管理。
透過該 SA 管理	此選項請選擇 **HTTPS** 以透過 VPN 通道管理本機 SonicWall 防火牆。	此選項請選擇 **HTTPS** 以透過 VPN 通道管理本機 SonicWall 防火牆。
透過 SA 使用者登入	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。	選擇 **HTTP**、**HTTPS** 或兩者同時選擇，以允許使用者利用 SA 登入。
	附註：HTTP 使用者登入不允許遠端驗證。	**附註：**HTTP 使用者登入不允許遠端驗證。
VPN 原則繫結至	從下拉清單中選擇一個介面或區域。若使用 WAN 負載平衡，並希望 VPN 使用任一 WAN 介面，則區域 WAN 應為偏好的設定。	從下拉清單中選擇一個介面或區域。若使用 WAN 負載平衡，並希望 VPN 使用任一 WAN 介面，則區域 WAN 應為偏好的設定。
	重要：若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。	**重要：**若兩個介面的 VPN 閘道 IP 位址相同，則不能從下拉清單中選擇兩個不同的 WAN 介面。

選項	主模式或加強模式	IKEv2 模式
IKEv2 設定		
請不要在 IKE SA 協商時傳輸觸發封包	未啟用	*未*選擇 (預設)。應只在對等點無法處理觸發封包，而需要互操作時選擇。 建議作法為包括觸發封包，以便幫助 IKEv2 回應者從安全原則資料庫中選擇正確的受保護 IP 位址範圍。並非所有方案都支援此功能，因此禁止某些 IKE 對等點包括觸發封包可能是適當的。
接收 Hash & URL 憑證類型	未啟用	如果裝置能夠傳送並處理雜湊和憑證 URL，而不是憑證本身，請選擇此項。若選擇此項，系統會傳送訊息給對等裝置，通知支援 HTTP 憑證查詢。
傳輸 Hash & URL 憑證類型	未啟用	如果裝置能夠傳送並處理雜湊和憑證 URL，而不是憑證本身，請選擇此項。若選擇此項，系統會回應對等裝置傳來的訊息，確認支援 HTTP 憑證查詢。

11 按一下**確定**。

12 按一下 **VPN > 基本設定**頁面上的**接受**以更新 VPN 原則。

為通道介面建立靜態路由

成功新增通道介面後，就可以建立一個固定路由。請參閱 *SonicWall SonicOS 6.5 系統安裝*的「網路」章節。可以將多個路由項目設定為針對不同網路使用相同通道介面。這樣就可以在不變更通道介面的情況下修改網路拓撲。

網路的備援靜態路由

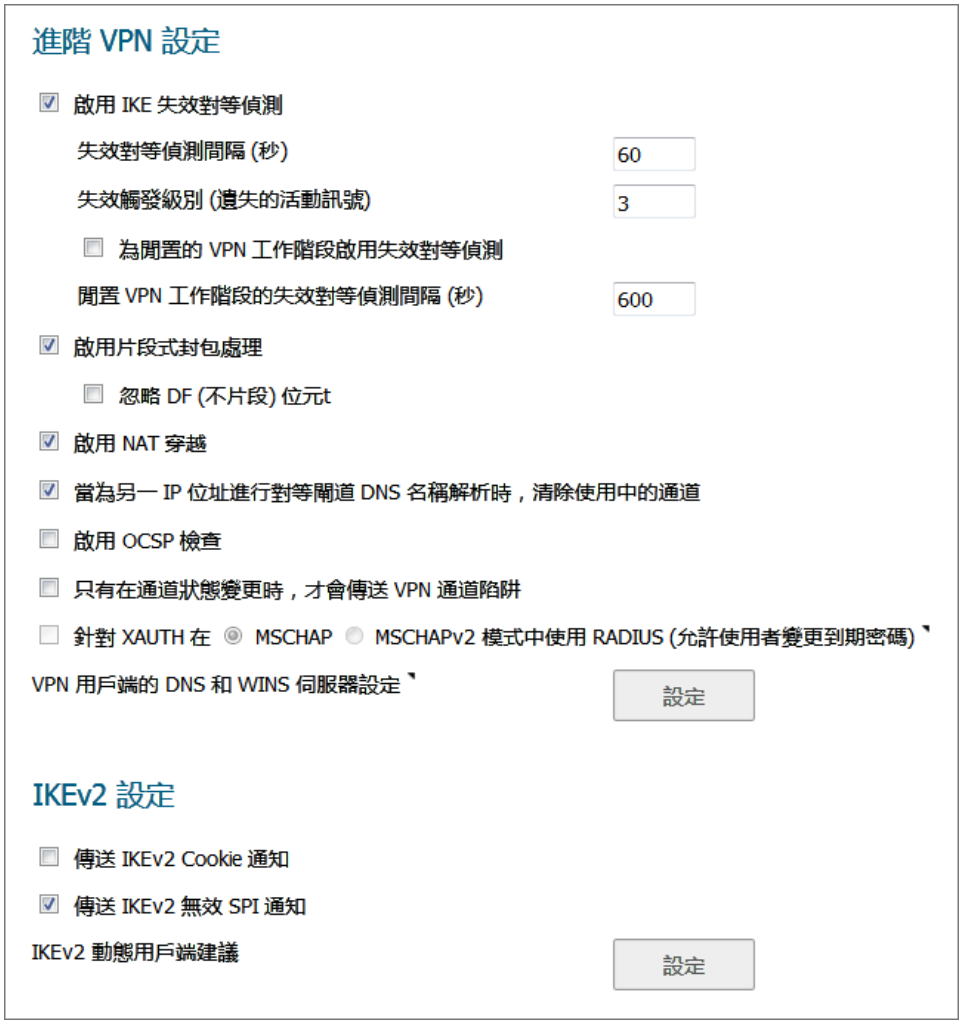
設定多個通道介面後，可以新增多個重疊固定路由，各固定路由使用不同的通道介面路由流量。這就為流量到達目的地提供了路由冗餘。如果沒有可用的冗餘路由，您可以新增靜態路由到丟棄通道介面，以防 VPN 流量送出預設路由。如需詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的「系統安裝 | 網路介面」指引瞭解詳情。

5

設定進階 VPN 設定

VPN > 進階頁面有兩個包含可以啟用選項的面板：

- 進階 VPN 設定
- IKEv2 設定



主題：

- 設定進階 VPN 設定
- 設定 IKEv2 設定

設定進階 VPN 設定

進階 VPN 設定全域影響所有 VPN 原則。本章節還為線上憑證狀態協定 (OCSP) 提供解決方案。OCSP 用於在沒有憑證撤銷清單 (CRL) 的情況下檢查 VPN 憑證狀態，以便您及時更新防火牆上使用的憑證狀態。

- **啟用 IKE 失效對等偵測** - 選擇是否希望讓防火牆放棄非使用中的 VPN 通道。
  - **失效對等偵測間隔（秒）** - 輸入兩次「活動訊號」之間的秒數。預設值為 60 秒。
  - **失效觸發級別（遺失的活動訊號）** - 輸入遺失的活動訊號數。預設值為 3。如果達到觸發級別，防火牆就會放棄 VPN 連接。防火牆使用階段 1 加密防護的 UDP 封包作為活動訊號。
  - **為閒置的 VPN 工作階段啟用失效對等偵測** - 如果希望防火牆在超過**閒置 VPN 工作階段的失效對等偵測間隔（秒）**欄位中定義的時間值後放棄閒置的 VPN 連接，請選擇此設定。預設值為 600 秒（10 分鐘）。
- **啟用片段式封包處理** - 如果 VPN 記錄報告顯示記錄訊息已片段的 `IPsec` 封包遺失，則選擇此功能。只有當 VPN 通道已建立並執行時才應使用此功能。
  - **忽略 DF（不片段）位元** - 選擇此核取方塊以忽略封包頭中的 DF 位。某些應用程式可能會在封包中顯見設定「不片段」選項，告知所有安全裝置不要將封包片段。啟用時，防火牆會忽略此選項，仍然將封包片段。
- **啟用 NAT 穿越** - 如果 NAT 裝置位於 VPN 端點之間，請選擇此設定。IPsec VPN 防護已認證端點之間交換的流量，但已認證端點不能在工作階段中途動態重新對應以實現 NAT 穿越。因此，為了在 IPsec 工作階段期間內保持動態 NAT 繫結，將一個 1 位元組 UDP 指定為「NAT 穿越存活」位元組並充當「活動訊號」，由 NAT 或 NAPT 裝置之後的 VPN 裝置傳送。「存活」位元組由 IPsec 對等點無聲地丟棄。
- **當為另一 IP 位址進行對等閘道名稱解析時清除使用中的通道** - 打破 SA 與舊 IP 位址的關聯，然後重新連接到對等閘道。
- **啟用 OCSP 檢查和 OCSP 回應 URL** - 支援使用線上憑證狀態協定 (OCSP) 來檢查 VPN 憑證狀態，並指定檢查憑證狀態的 URL。請參閱 OCSP 配合 SonicWall 網路安全裝置使用。
- **只有在通道狀態變更時，才會傳送 VPN 通道陷阱** - 僅當通道狀態變更時傳送陷阱，從而減少所傳送的 VPN 通道陷阱數。
- **針對 XAUTH 在** - 選擇此選項的主要原因是讓 VPN 用戶端使用者可以使用 MSCHAP 特性，以便在登入時修改過期的密碼。當使用 RADUIS 來驗證 VPN 用戶端使用者時，請選擇是否將 RADIUS 用於這些模式其中一種：
  - **MSCHAP**
  - **MSCHAPv2** 模式下使用 RADIUS XAUTH (允許使用者修改過期的密碼)

  另外，如果設定了此項，且在**使用者 > 設定**頁面選擇 LDAP 作為**登入驗證方法**，但是 LDAP 的設定不允許密碼更新，那麼 VPN 用戶端使用者的密碼更新將在利用 LDAP 驗證使用者之後，通過 MSCHAP-模式 RADIUS 進行。

  附註：只有在使用以下二者之一時 LDAP 才能完成密碼更新：
  - 帶有 TLS 的 Active Directory 且使用管理員帳戶與其繫結
  - Novell eDirectory。
- **VPN 用戶端的 DNS 和 WINS 伺服器設定** - 要為用戶端設定 DNS 和 WINS 伺服器設定，如通過 GroupVPN 的供應商 VPN 用戶端，或行動 IKEv2 用戶端，請按一下**設定**按鈕。此時顯示**新增 VPN DNS 和 WINS 伺服器**對話方塊。

  附註：此選項僅針對 TZ 裝置出現。

- **DNS 伺服器** - 選擇動態或手動指定 DNS 伺服器：
  - **從 SonicWall 的 DNS 設定動態繼承 DNS 設定** - SonicWall 裝置自動獲取 DNS 伺服器 IP 位址。
  - **手動指定** - 在 **DNS 伺服器 1/3** 欄位中輸入最多 3 個 DNS 伺服器 IP 位址。
- **WINS 伺服器** - 在 **WINS 伺服器 1/2** 欄位中輸入最多 2 個 WINS 伺服器 IP 位址。

設定 IKEv2 設定

IKEv2 設定影響 IKE 通知，且用於設定動態用戶端支援。

- **傳送 IKEv2 Cookie 通知** - 將 cookie 作為一種驗證工具傳送到 IKEv2 對等點。
- **傳送 IKEv2 無效 SPI 通知** - 當存在使用中的 IKE 安全關聯 (SA) 時，傳送無效的安全參數索引 (SPI) 通知到 IKEv2 對等點。預設情況下已核取此選項。
- **IKEv2 動態用戶端建議** - SonicOS 提供 IKEv2 動態用戶端支援，利用它可設定網際網路金鑰交換 (IKE) 屬性，而不必使用預設值。

  按一下**設定**按鈕將啟動**設定 IKEv2 動態用戶端建議**對話方塊。

SonicOS 支援這些 **IKE 建議**設定：

- **DH 群組**：**群組 1**、**群組 2**（預設）、**群組 5**、**群組 14**，以及下面 5 個包含在 Suite B 加密中的 DH 群組：
  - **256 位隨機 ECP 群組**
  - **384 位隨機 ECP 群組**
  - **521 位隨機 ECP 群組**
  - **192 位隨機 ECP 群組**
  - **224 位隨機 ECP 群組**
- **加密**：**DES**、**3DES**（預設）、**AES-128**、**AES-192**，**AES-256**
- **驗證**：**MD5**、**SHA1**（預設）、**SHA256**、**SHA384** 或 **SHA512**

然而，如果定義了 IKEv2 交換模式和 0.0.0.0 IPSec 閘道的 VPN 原則，則無法在單個原則基礎上設定這些 IKE 建議設定。

附註：遠端閘道上的 VPN 原則也必須利用相同的設定進行設定。

OCSP 配合 SonicWall 網路安全裝置使用

OCSP 設計用於擴充或替換公開金鑰基礎設施 (PKI) 或數位憑證系統中的 CRL。CRL 用於驗證 PKI 組成的數位憑證。這樣，憑證授權單位 (CA) 就可以在計劃到期日期前撤銷憑證，防止被盜或無效憑證影響 PKI 系統。

憑證撤銷清單的主要缺點是需要頻繁更新以使每個用戶端的 CRL 保持最新狀態。如果每個用戶端都要下載完整的 CRL，這種頻繁更新將大大增加網路流量。根據 CRL 更新頻率，可能存在這樣一個時間段：CRL 已撤銷一個憑證，但用戶端尚未收到更新，因而繼續允許使用此憑證。

線上憑證狀態協定可確定數位憑證的目前狀態，無需使用 CRL。通過 OCSP，用戶端或應用程式可直接確定指定數位憑證的狀態。因此，它能提供比 CRL 更及時的憑證狀態資訊。此外，用戶端通常只需檢查幾個憑證，不需要為少數幾個憑證而下載全部 CRL，從而節省開銷。這可以大大降低與憑證驗證相關的網路流量。

OCSP 通過 HTTP 傳送訊息，以便最大程度地相容現有網路。這需要仔細設定網路上的任何快取伺服器，避免收到可能過期的 OCSP 回應快取副本。

OCSP 用戶端與 OCSP 回應者通訊。OCSP 回應者可以是用來確定憑證狀態的 CA 伺服器，或是與此 CA 伺服器通訊的其他伺服器。OCSP 用戶端向 OCSP 回應者傳送狀態請求，並暫停接受憑證，直到回應者提供回應為止。用戶端請求包括通訊協定版本、服務請求、目的地憑證身分和可選擴充項等資料。可選擴充項不一定能獲得 OCSP 回應者的應答。

OCSP 回應者接收用戶端的請求，檢查此訊息的形式是否妥當，以及回應者是否能回應該服務請求。然後，它檢查此請求是否包含期望服務所需的資訊。如果所有條件均滿足，回應者就會向 OCSP 用戶端返回一個確切的回應。OCSP 回應者需要提供一個基本回應：GOOD（正常）、REVOKED（已撤銷）或 UNKNOWN（未知）。如果 OCSP 用戶端和回應者均支援可選的擴充項，那麼也可能提供其他回應。GOOD 狀態是期望的回應，因為它表示未撤銷憑證。REVOKED 狀態表示已撤銷憑證。UNKNOWN 狀態表示回應者沒有關於此憑證的資訊。

OCSP 伺服器通常以推 (push) 或拉 (pull) 方式與 CA 伺服器合作。CA 伺服器可設定為向 OCSP 伺服器推送 CRL 清單（撤銷清單）。此外，OCSP 伺服器可設定為定期從 CA 伺服器下載（拉） CRL。OCSP 伺服器還必須設定 CA 伺服器頒發的 OCSP 回應簽章憑證。此簽章憑證必須有適當的形式，否則 OCSP 用戶端將不接受來自 OSCP 伺服器的回應。

OpenCA OCSP 回應者

使用 OCSP 要求將 OpenCA（開放原始碼憑證授權單位）OCSP Responder 作為其唯一支援的 OCSP 回應者。OpenCA OCSP Responder 的網址是：http://www.openca.org。OpenCA OCSP Responder 是 rfc2560 相容 OCSP 回應者，執行於預設連接埠 2560（以向 rfc2560 致敬）。

載入憑證以使用 OCSP

為使 SonicOS 用作 OCSP 回應者的用戶端，必須將 CA 憑證載入到防火牆。

1 在**系統 -> 憑證**頁面，按一下「匯入」按鈕。隨即顯示「匯入憑證」頁面。

2 勾選**從 PKCS#7 (.p7b)、PEM (.pem) 或 DER (.der 或 .cer) 編碼檔案匯入 CA 憑證**選項，指定憑證的位置。

OCSP 配合 VPN 原則使用

防火牆 OCSP 設定既可以在原則級別上設定，也可以全域設定。若要針對單個 VPN 原則設定 OCSP 檢查，請使用 VPN 原則設定頁面的進階標籤。

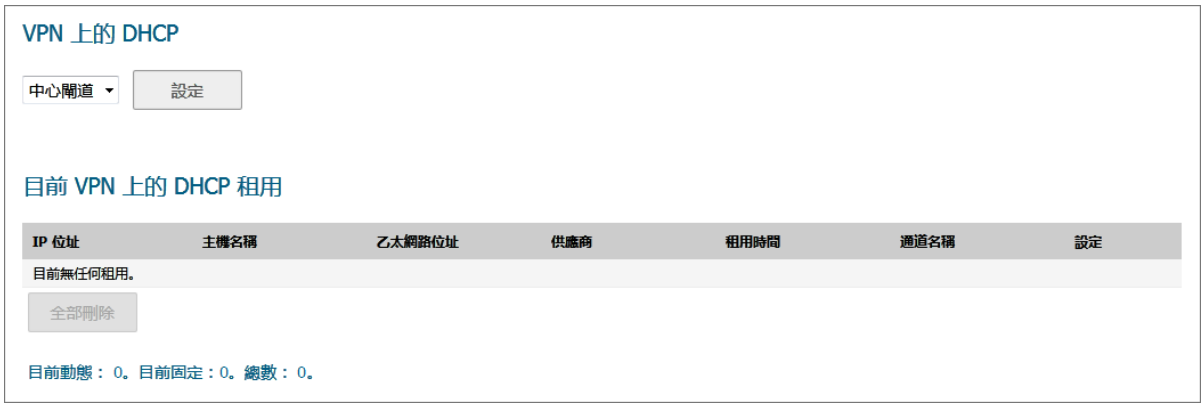
1 選擇**啟用 OCSP 檢查**旁邊的選項按鈕。

2 指定 OCSP 伺服器的 **OCSP 回應 URL**，例如 http://192.168.168.220:2560，其中 192.168.168.220 是 OCSP 伺服器的 IP 位址，2560 是 OpenCA OCSP 回應者服務的預設工作連接埠。

6

設定 VPN 上的 DHCP

VPN > VPN 上的 DHCP 頁面用於設定防火牆以從 VPN 通道另一端的 DHCP 伺服器獲得 IP 位址租用。某些網路部署希望將所有 VPN 網路置於一個邏輯 IP 子網路上，造成一種似乎所有 VPN 網路都位於同一 IP 子網路位址空間中的印象。這有利於使用 VPN 通道的網路的 IP 位址管理。



主題：

- DHCP 轉接模式
- 針對 VPN 上的 DHCP 設定中心閘道
- 設定 VPN 上的 DHCP 的遠端閘道
- 目前 VPN 上的 DHCP 租用

DHCP 轉接模式

遠端和中心站台的防火牆針對初始 DHCP 流量及站台之間的後續 IP 流量的 VPN 通道進行設定。遠端站台（**遠端閘道**）的防火牆通過其 VPN 通道傳遞 DHCP 廣播封包。中心站台（**中心閘道**）的防火牆將遠端網路用戶端的 DHCP 封包轉接到中心站台上的 DHCP 伺服器。

針對 VPN 上的 DHCP 設定中心閘道

若要設定中心閘道的 VPN 上的 DHCP：

1 選擇 **VPN > VPN 上的 DHCP**。

2 從 **VPN 上的 DHCP** 下拉功能表中選擇**中心閘道**。

3 按一下**設定**。

4 選擇以下一項

- 如果您要對 Global VPN Client 或遠端防火牆或對兩者都使用 DHCP 伺服器，請選擇**使用內部 DHCP 伺服器**選項。
    - 若要對 Global VPN Client 使用 DHCP 伺服器，請選擇**用於全域 VPN 用戶端**選項。
    - 若要對遠端防火牆使用 DHCP 伺服器，請選擇**遠端防火牆**選項。
- 若要將 DHCP 請求傳送到特定伺服器，請選擇**向以下列出的伺服器位址傳輸 DHCP 請求**。
    a) 按下**新增**。
    b) 在 **IP 位址**欄位中輸入 DHCP 伺服器的 IP 位址。
    c) 按一下**確定**。現在，防火牆將把 DHCP 請求導向指定伺服器。

5 在**轉接 TP 位址（可選）**欄位中輸入轉接伺服器的 IP 位址。

設定後，此 IP 位址將用作 DHCP 轉接代理 IP 位址 (giaddr) 代替此 SonicWall 的 LAN IP 位址。僅當遠端閘道上沒有設定轉接 IP 位址時才使用此位址，且必須保留其在 DHCP 伺服器上的 DHCP 範圍內。

6 按一下**確定**。

設定 VPN 上的 DHCP 的遠端閘道

若要設定 VPN 上的 DHCP 遠端閘道：

1 從 **VPN 上的 DHCP** 下拉功能表中選擇**遠端閘道**。

2 按一下**設定**。

3 設定**一般**時，如果 VPN 原則已啟用**本機網路透過這個 VPN 通道利用 DHCP 獲得 IP 位址**設定，則**透過此 VPN 通道的轉接 DHCP** 欄位會自動顯示 VPN 原則名稱。

附註：只有使用 IKE 的 VPN 原則能夠用作 DHCP 的 VPN 通道。VPN 通道必須使用 IKE 且必須相應設定本機網路。本機網路透過這個 VPN 通道利用 DHCP 獲得 IP 位址。

4 從 **DHCP 租用繫結至**功能表選擇 DHCP 租用繫結的介面。

5 若要從橋接 WLAN 介面接收 DHCP 請求，請啟用**從橋接 WLAN 介面接收 DHCP 請求**核取方塊。

6 如果在**轉接 IP 位址**欄位中輸入一個 IP 位址，此 IP 位址將用作 DHCP 轉接代理 IP 位址 (giaddr)，代替中心閘道的位址，且必須保留在 DHCP 伺服器上的 DHCP 範圍中。此位址也可用來從中心閘道後面通過 VPN 通道遠端管理此防火牆。

附註：如果需要通過通道進行管理，則「轉接 IP 位址」和「遠端管理 IP 位址」欄位不能為零。

7 如果在**遠端管理 IP 位址**欄位中輸入一個 IP 位址，此 IP 位址將用來從中心閘道後面管理防火牆，且必須保留在 DHCP 伺服器上的 DHCP 範圍中。

8 如果啟用**當偵測到 IP 詐騙時，封鎖通道上的流量**，防火牆將封鎖任何偽造認證使用者 IP 位址的流量通過 VPN 通道。但是，如果您有任何固定裝置，必須確保為此裝置輸入正確的乙太網路位址。乙太網路位址是身分識別過程的一部分，不正確的乙太網路位址可能導致防火牆做出 IP 欺騙回應。

9 如果 VPN 通道中斷，可以從本機 DHCP 伺服器獲得臨時 DHCP 租用。一旦通道再次可用，本機 DHCP 伺服器就會停止租用。勾選**如果通道無法使用，將從本機的 DHCP 伺服器獲得臨時租用**核取方塊。通過勾選此核取方塊，您就能在通道停止工作時獲得容錯移轉選項。

10 若要為臨時租用設定一定的時間，請在**臨時租用時間**框中輸入臨時租用的分鐘數。預設值為 **2** 分鐘。

11 若要設定 LAN 上的裝置，請按一下**裝置**標籤。

12 若要設定 **LAN 上固定裝置**，請按一下**新增**以顯示**新增 LAN 裝置項目**對話。

13 在 **IP 位址**欄位中輸入裝置的 IP 位址，然後在**乙太網路位址**欄位中輸入裝置的乙太網路位址。

固定裝置的一個例子是印表機，因為它無法動態獲取 IP 租用。如果未啟用**當偵測到 IP 詐騙時，封鎖通道上的流量**，則無必要輸入裝置的乙太網路位址。必須從 DHCP 伺服器上的可用 IP 位址集

區中排除固定 IP 位址，以免 DHCP 伺服器將這些位址指派給 DHCP 用戶端。還應排除用作**轉接 IP 位址**的 IP 位址。推薦保留一個 IP 位址塊以用作轉接 IP 位址。

14 按一下**確定**。

15 若要排除 LAN 上的裝置，請按一下**新增**以顯示**新增排除的 LAN 項目**對話。

16 在**乙太網路位址**欄位輸入裝置的 MAC 位址。

17 按一下**確定**。

18 按一下**確定**以結束 **VPN 上的 DHCP 設定**對話。

附註：必須在遠端防火牆上設定本機 DHCP 伺服器以將 IP 租用指派給這些電腦。

附註：如果遠端站台無法連接中心閘道並獲取租用，請確認遠端電腦未啟用「確定網路增強器」(DNE)。

提示：如果固定 LAN IP 位址不在 DHCP 範圍內，向此 IP 路由是可能的，即兩個 LAN。

目前 VPN 上的 DHCP 租用

目前 VPN 上的 DHCP 租用表顯示目前繫結的詳細資料：**IP 位址**、**主機名稱**、**乙太網路位址**、**租用時間**和**通道名稱**。表中最後一列**設定**，用於設定或刪除一個表項目（繫結）：以

- 編輯繫結，按一下**編輯**。
- 刪除繫結，以便在 DHCP 伺服器中釋放此 IP 位址，請從清單中選擇此繫結，然後按一下**刪除**圖示。完成此操作需要幾秒鐘時間。完成後，會在 Web 瀏覽器視窗的底部顯示一條確認更新的訊息。
- 按一下**全部刪除**將刪除全部 VPN 租用。

7

設定 L2TP 伺服器和 VPN 用戶端存取

SonicWall 網路安全裝置可以終止來自傳入 Microsoft Windows 或 Google Android 用戶端的 L2TP-over-IPsec 連接。在無法執行全域 VPN 用戶端 (GVC) 的情況下，可以利用 SonicWall L2TP 伺服器來安全存取防火牆之後的資源。

可以利用二層通道通訊協定 (L2TP) 來透過公用網路建立 VPN。L2TP 提供了不同 VPN 供應商之間的互操作性，PPTP 和 L2F 則無此能力，不過 L2TP 結合了這兩個協定的長處，是它們的擴充。

L2TP 支援 PPP 支援的多種驗證選項，包括密碼驗證協定 (PAP)、質詢握手身分驗證協定 (CHAP) 和 Microsoft 質詢握手身分驗證協定 (MS-CHAP)。可以利用 L2TP 驗證 VPN 通道的端點以提供額外的安全防護，還可以利用 IPsec 予以實現以提供安全的加密 VPN 解決方案。

主題：

- 設定 L2TP 伺服器
- 查看目前使用中的 L2TP 工作階段
- 設定 Microsoft Windows L2TP VPN 用戶端存取
- 設定 Google Android L2TP VPN 用戶端存取

附註：如需設定 L2TP 伺服器的更詳細資料，請參閱技術說明**在 SonicOS 中設定 L2TP 伺服器**，它位於 SonicWall 支援網站：https://www.sonicwall.com/support。

設定 L2TP 伺服器

VPN > L2TP 伺服器頁面提供用於將 SonicWall 網路安全裝置設定為 L2TP 伺服器的設定。

設定 L2TP 伺服器：

1 選擇**啟用 L2TP 伺服器**選項。

2 按一下**設定**以顯示 **L2TP 伺服器設定**對話方塊。

3 在 **L2TP 伺服器**標籤上的**保持運作時間 (秒)** 欄位中輸入數值 (秒數)。此數值用於指定傳送特殊封包以便讓連接保持開放的頻率。預設值為 **60** 秒。

4 在 **DNS 伺服器 1** 欄位中輸入首個 DNS 伺服器的 IP 位址。若有第二個 DNS 伺服器，請在 **DNS 伺服器 2** 欄位中輸入其 IP 位址。

5 在 **WINS 伺服器 1** 欄位中輸入首個 WINS 伺服器的 IP 位址。若有第二個 WINS 伺服器，請在 **WINS 伺服器 2** 欄位中輸入其 IP 位址。

6 選擇 **L2TP 使用者**。

7 選擇下列 IP 位址設定選項按鈕之一：

RADIUS/LDAP 伺服器提供的 IP 位址	預設情況下，未選擇此選項。如果 RADIUS/LDAP 伺服器向 L2TP 用戶端提供 IP 位址資訊，請選擇此項。「起始 IP」和「終止 IP」欄位不再提供使用。 **附註：** RADIUS 或者 LDAP 必須在使用者設定頁面選擇以使用此選項。如果已選擇此選項，將顯示效果的資訊式訊息。按一下**確定**。
使用本機 L2TP IP 集區	這是預設 IP 位址設定。如果 L2TP 伺服器提供 IP 位址，請選擇此項。 「起始 IP」和「終止 IP」欄位可供使用，請在**起始 IP** 和**終止 IP** 欄位中輸入 LAN 上私人 IP 位址的範圍。

8 如果已設定使用 L2TP 的特定使用者群組，請從 **L2TP 使用者的使用者群組**功能表中選擇或使用**任何人**。

9 選擇 **PPP**。可新增或移除驗證通訊協定，或重新排列驗證的順序。

10 按一下**確定**。

查看目前使用中的 L2TP 工作階段

使用中的 L2TP 工作階段面板顯示了目前處於使用中狀態的 L2TP 工作階段。

隨即顯示以下資訊。

使用者名稱	本機使用者資料庫或 RADIUS 使用者資料庫中指派的使用者名稱。
PPP IP	連接的來源 IP 位址。
區域	L2TP 用戶端使用的區域。
介面	用於存取 L2TP 伺服器的介面，可以是 VPN 用戶端或其他防火牆。
驗證	L2TP 用戶端使用的驗證類型。
主機名稱	連接到 L2TP 伺服器的 L2TP 用戶端名稱。

設定 Microsoft Windows L2TP VPN 用戶端存取

本節提供一個範例，說明如何利用內建的 L2TP 伺服器和 Microsoft 的 L2TP VPN 用戶端，設定 L2TP 用戶端對 WAN GroupVPN SA 的存取。

附註：SonicOS 僅支援 L2TP 用戶端的 X.509 憑證；不支援 L2TP 連接的以 PKCS #7 編碼的 X.509 憑證。

使 Microsoft L2TP VPN 用戶端能夠存取 WAN GroupVPN SA 的步驟如下：

1 導覽至 **VPN > 基本設定**頁面。

2 針對 WAN GroupVPN 原則，按一下**設定**欄中的**編輯**圖示。

3 在**一般**標籤中，從**驗證方法**功能表中選擇**使用預先共用密碼的 IKE**。

4 在**共用密碼**欄位輸入一個共用密碼以完成用戶端原則設定。

5 按一下**確定**按鈕。

6 移至 **VPN > L2TP 伺服器**頁面。

7 在 **L2TP 伺服器設定**區段中，勾選**啟用 L2TP 伺服器**方塊。

8 按一下**設定**按鈕。

9 提供以下 L2TP 伺服器設定：

- **保持運作時間（秒）**：*60*
- **DNS 伺服器 1**：*199.2.252.10*（或者使用 ISP 的 DNS）
- **DNS 伺服器 2**：*4.2.2.2*（或者使用 ISP 的 DNS）
- **DNS 伺服器 3**：*0.0.0.0*（或者使用 ISP 的 DNS）
- **WINS 伺服器 1**：*0.0.0.0*（或者使用 WINS IP）
- **WINS 伺服器 2**：*0.0.0.0*（或者使用 WINS IP）

10 按一下 **L2TP 使用者**。

11 設定以下選項:

- **使用本機 L2TP IP 集區**：啟用（預設已選擇）
- **起始 IP**：*10.20.0.1* (使用您自己的 IP)
- **終止 IP**：*10.20.0.20* (使用您自己的 IP)

12 從 **L2TP 使用者的使用者群組**下拉功能表中選擇**受信任的使用者**。

13 在**系統安裝**底下，導覽至**使用者 > 本機使用者和群組**頁面。

14 按一下**本機使用者**。

15 按下**新增**。

16 在**名稱**、**密碼**和**確認密碼**欄位指定使用者名稱和密碼。

17 按一下**確定**。

> **附註：**藉由編輯 VPN LAN 區域或另一個 VPN 區域 (於**原則**底下的**規則 > 存取規則**進行編輯)，可限制 L2TP 用戶端的網路存取。若要查找待編輯的規則，選擇**存取規則**表上的**所有類型**檢視，並查看 **L2TP IP 集區**的「來源」欄。

18 在您的 Microsoft Windows 電腦上，完成以下 L2TP VPN 用戶端設定以實現安全存取：

a 導覽至**開始 > 控制台 > 網路和共用中心**。

b 打開「新建連接精靈」。

c 選擇**連線到工作地點**。

d 按**下一步**。

e 選擇「虛擬私人網路連接」。按**下一步**。

f 為您的 VPN 連接輸入一個名稱。按**下一步**。

g 輸入防火牆的公用 (WAN) IP 位址。或者，您也可以使用一個指向此防火牆的網域名稱。

h 按一下**下一步**，然後按一下**完成**。

i 在「連接」視窗中按一下**屬性**。

j 按一下**安全**標籤。

k 按一下 **IPSec 設定**。

l 啟用**使用預先共用密碼進行身分驗證**。

m 輸入預先共用密碼再按一下**確定**。

n 按一下**網路**標籤。

o 將 **VPN 類型**從**自動**變更為 **L2TP IPSec VPN**。

p 按一下**確定**。

q 輸入您的 XAUTH 使用者名稱和密碼。

r 按一下**連接**。

19 導覽至 **VPN > 基本設定**頁面，確認您的 Microsoft Windows L2TP VPN 裝置已連接。VPN 用戶端顯示在**目前使用中的 VPN 通道**部分。

設定 Google Android L2TP VPN 用戶端存取

本節提供一個範例，說明如何利用內建的 L2TP 伺服器和 Google Android 的 L2TP VPN 用戶端，設定 L2TP 用戶端對 WAN GroupVPN SA 的存取。

使 Google Android L2TP VPN 用戶端能夠存取 WAN GroupVPN SA 的步驟如下：

1 導覽至 **VPN > 基本設定**頁面。

2 按一下 WAN GroupVPN 原則的**編輯**圖示。

3 從**驗證方法**下拉功能表中選擇**使用預先共用密碼的 IKE**（預設）。

4 在**共用密碼**欄位輸入一個共用密碼以完成用戶端原則設定。

5 按一下**建議**標籤。

6 提供 **IKE (階段 1) 建議**的以下設定：

- DH 群組：**組 2**
- 加密：**3DES**
- 身分驗證：**SHA1**
- 存留時間（秒數）：**28800**

7 提供 **IPsec (階段 2) 建議**的以下設定：

- 通訊協定：**ESP**
- 加密：**DES**
- 身分驗證：**SHA1**
- 啟用完全轉送保密：**啟用**
- 存留時間（秒數）：**28800**

8 按一下**進階**標籤。

9 設定以下選項:

- **啟用多點傳送**：已停用
- **透過該 SA 管理**：全部停用
- **預設閘道**: 0.0.0.0
- **需要透過 XAUTH 的 VPN 用戶端的驗證**：啟用
- **XAUTH 使用者的使用者群組**：Trusted Users

10 按一下**用戶端**標籤。

11 設定以下選項:

- **在用戶端快取 XAUTH 使用者名稱和密碼**：單一工作階段或始終
- **虛擬轉接器設定**：DHCP 租用
- **允許連接到**：分離通道
- **設定預設路由作為該閘道**：已停用
- **套用 VAP 存取控制清單**: 已停用
- **對於簡單用戶端佈建使用預設金鑰**：啟用

12 移至 **VPN > L2TP 伺服器**頁面。

13 按一下**啟用 L2TP 伺服器**核取方塊。

14 按一下**設定**按鈕。

15 提供以下 L2TP 伺服器設定：

- **保持運作時間（秒）**：60
- **DNS 伺服器 1**：199.2.252.10（或者使用 ISP 的 DNS）
- **DNS 伺服器 2**：4.2.2.2（或者使用 ISP 的 DNS）
- **DNS 伺服器 3**：0.0.0.0（或者使用 ISP 的 DNS）

- **WINS 伺服器 1**：0.0.0.0（或者使用 WINS IP）
- **WINS 伺服器 2**：0.0.0.0（或者使用 WINS IP）

16 按一下 **L2TP 使用者**。

17 設定以下選項:

- **RADIUS/LDAP 伺服器提供的 IP 位址**：已停用
- **使用本機 L2TP IP 集區**：啟用
- **起始 IP**：10.20.0.1 (或使用您自己的 IP)
- **終止 IP**：10.20.0.20 (或使用您自己的 IP)

18 在 **L2TP 使用者的使用者群組**下拉功能表中選擇**受信任的使用者**。

19 在**系統安裝**底下，導覽至**使用者 > 本機使用者和群組**頁面。

20 按一下**本機使用者**。

21 按下**新增**。

22 移至**使用者 > 本機使用者**頁面。按一下**新增使用者**按鈕。

23 在**設定**標籤中，指定使用者名稱和密碼。

24 在「VPN 存取」標籤中，將所需的網路位址物件新增到 L2TP 用戶端的存取清單網路。

附註：至少應將「LAN 子網路」、「LAN 主要子網路」和「L2TP IP 集區」位址物件新增到存取清單。

附註：您已完成 SonicOS 設定。

25 在您的 Google Android 裝置上，完成以下 L2TP VPN 用戶端設定以實現安全存取：

a 移至「應用」頁面，選擇**設定**圖示。從「設定」功能表選擇**無線和網路**。

b 選擇 **VPN 設定**，按一下**新增 VPN**。

c 選擇**新增 L2TP/IPSec PSK VPN**。

d 在「VPN 名稱」底下輸入易記的 VPN 名稱

e 設定 **VPN 伺服器**。

f 輸入防火牆的公用 IP 位址。

g 設定 **IPSec 預先共用密碼**：輸入您的 WAN GroupVPN 原則的密碼

h **L2TP 密碼**保持空白

i 如有需要可設定 LAN 網域設定，這些是可選設定。

j 輸入您的 XAUTH 使用者名稱和密碼。按一下**連接**。

26 移至 **VPN > 設定**頁面，驗證您的 Google Android 裝置已連接。VPN 用戶端顯示在「目前使用中的 VPN 通道」部分。

第 2 部分

SSL VPN

- 關於 SSL VPN
- 設定 SSL VPN 伺服器行為
- 設定 SSL VPN 用戶端設定
- 設定 SSL VPN Web 入口網站
- 設定虛擬辦公室

8

關於 SSL VPN

本章節介紹如何設定 SonicWall 網路安全裝置上的 SSL VPN 功能。SonicWall 的 SSL VPN 功能利用 NetExtender 用戶端實現對網路的安全遠端存取。

NetExtender 是一種供 Windows、Mac 或 Linux 使用者使用的 SSL VPN 用戶端，以透明方式下載，可用來在網路上安全執行任何應用程式和使用點對點通訊協定 (PPP)。NetExtender 允許遠端用戶端無縫存取本機網路上的資源。使用者可通過兩種方式存取 NetExtender：

- 登入 SonicWall 網路安全裝置提供的虛擬辦公室 Web 入口網站。
- 啟動獨立的 NetExtender 用戶端

每部 SonicWall 裝置可支援的同時遠端使用者數有上限，詳情請參閱下表。

最大併發 SSL VPN 使用者數

SonicWall 裝置型號	最大併發 SSL VPN 連接數	SonicWall 裝置型號	最大併發 SSL VPN 連接數	SonicWall 裝置型號	最大併發 SSL VPN 連接數
SM 9800	3000	NSA 6600	1500	TZ600	200
SM 9600	3000	NSA 5600	1000	TZ500/TZ500 W	150
SM 9400	3000	NSA 4600	500	TZ400/TZ400 W	100
SM 9200	3000	NSA 3600	350	TZ300/TZ300 W	50
		NSA 2650	250		
		NSA 2600	250	SOHO W	50

SonicOS 支援擁有 IPv6 位址的使用者使用 NetExtender 連接。位址物件下拉清單包含所有預先定義的 IPv6 位址物件。

附註：不支援 IPv6 Wins 伺服器。支援 IPv6 FQDN。

主題：

- 關於 NetExtender
- 設定使用者的 SSL VPN 存取
- 生物識別驗證

關於 NetExtender

NetExtender 獨立用戶端在您首次啟動 NetExtender 時安裝。然後，通過 Windows 系統的**開始**功能表，MacOS 系統的**應用程式**資料夾或 Dock，或者 Linux 系統的路徑名稱或快捷方式欄，就可以存取它。

SonicWall 的 SSL VPN NetExtender 是一種提供 Windows、Mac 和 Linux 使用者使用的透明軟體應用程式，遠端使用者可用於安全連接公司網路。利用 NetExtender，遠端使用者可以安全地在公司網路上執行任何應用程式。使用者可以上載下載檔案，安全網路磁碟機，存取資源，如同在本機網路上一樣。

NetExtender 使遠端使用者能夠全權存取受防護的內部網路。使用體驗幾乎與使用傳統 IPSec VPN 用戶端完全相同，但是使用 Firefox 時，系統會利用 XPCOM 外掛程式將 NetExtender Windows 用戶端自動安裝在遠端使用者的 PC 上。在 MacOS 系統上，支援的瀏覽器使用 Java 控件從虛擬辦公室門戶自動安裝 NetExtender。Linux 系統也可以安裝和使用 NetExtender 用戶端。Windows 使用者需從入口網站下載用戶端，若使用行動裝置，則需從應用程式商店下載 Mobile Connect。

使用者首次啟動 NetExtender 時會安裝 NetExtender 獨立用戶端，然後，透過 Windows 系統的開始功能表、MacOS 系統的應用程式資料夾或 Dock，或者 Linux 系統的路徑名稱或快捷方式欄，即可直接存取。

安裝後，NetExtender 會自動啟動並連接一個虛擬轉接器，以便對內部網路上允許的主機和子網路進行安全的 SSL VPN 點對點存取。

主題：

- 建立 NetExtender 範圍的位址物件
- 設定存取權限
- 設定代理
- 安裝獨立用戶端

建立 NetExtender 範圍的位址物件

在 SonicOS 6.2.2x 和更高版本中，作為 NetExtender 設定的一部分，必須為 NetExtender IP 位址範圍建立一個位址物件。設定裝置設定檔時將會使用這個位址物件。

您可以為 IPv4 位址範圍和 IPv6 位址範圍建立位址物件，以用在 **SSL VPN > 用戶端設定**設定中。在位址物件中設定的位址範圍用於定義 IP 位址集區，而 NetExtender 工作階段期間會將此集區中的位址指派給遠端使用者。這個範圍的大小必須足以容納您預定要支援的最大同時 NetExtender 使用者數。您可能為因應成長而需幾個額外的位址，但並非必要。

附註：如果在 SSL VPN 裝置所處的區段上存在其他主機，則位址範圍不得與任何已指派的位址重疊或衝突。

有關設定位址物件的詳情，請參閱 *SonicWall SonicOS 6.5 原則*的**位址物件**章節。請參閱快速參考資料，瞭解定義 SSL 位址物件所需的設定。

建立 NetExtender IP 位址範圍的位址物件：

1. 選擇**管理**檢視。
2. 導覽至**網路 > 位址物件**。
3. 按下**新增**。
4. 在**名稱**欄位中輸入描述性名稱。
5. 對於**區域指派**，從下拉清單中選擇 **SSL VPN**。
6. 對於**類型**，選擇**範圍**。
7. 在**起始 IP 位址**欄位中，輸入您要使用的範圍中的最小 IP 位址。

附註：IP 位址範圍必須與用於 SSL VPN 服務的介面處於同一子網路。

8 在**結束 IP 位址**欄位中，輸入您要使用的範圍中的最大 IP 位址。

9 按下**新增**。

10 按一下**關閉**。

設定存取權限

NetExtender 用戶端路由用於允許或拒絕 SSL VPN 使用者存取各種網路資源。使用位址物件可以輕鬆且動態地設定網路資源存取。**Tunnel All** 模式路由通過 SSL VPN NetExtender 通道路由遠端使用者的所有來往流量，包括目的地為遠端使用者本機網路的流量。方法為將下列路由新增到遠端用戶端的路由表中:

需新增到遠端用戶端路由表的路由

IP 位址	子網路遮罩
0.0.0.0	0.0.0.0
0.0.0.0	128.0.0.0
128.0.0.0	128.0.0.0

NetExtender 還為所有網路連接的本機網路新增路由。這些路由的度量高於任何現有路由，從而強制目的地為本機網路的流量通過 SSL VPN 通道傳送。例如，如果一個遠端使用者在 10.0.*.* 網路上有 IP 位址 10.0.67.64，則將新增路由 10.0.0.0/255.255.0.0，以便通過 SSL VPN 通道路由流量。

附註：如需設定 **Tunnel All** 模式，還必須為 0.0.0.0 設定一個位址物件，並讓 SSL VPN NetExtender 使用者和群組有權存取此位址物件。

當 NetExtender 連接和中斷連接時，管理員也可執行批處理檔案指令碼。指令碼可用於對應或斷開網路磁碟機和印表機，啟動應用程式，或者打開檔案或 Web 站台。NetExtender 連接指令碼可支援任何有效的批處理檔案命令。

設定代理

SonicWall SSL VPN 支援使用代理設定的 NetExtender 工作階段。目前僅支援 HTTPS 代理。從 Web 入口網站啟動 NetExtender 時，如果瀏覽器已經設定代理存取，NetExtender 將自動繼承代理設定。代理設定也可以在 NetExtender 用戶端喜好設定中手動設定。對於支援 Web 代理自動發現 (WPAD) 協定的代理伺服器，NetExtender 可以自動偵測代理設定。

NetExtender 為設定代理設定提供了三個選項：

- **自動偵測設定** - 如需使用此設定，代理伺服器必須支援 Web 代理自動發現通訊協定，此通訊協定可自動將代理設定指令碼推送到用戶端。
- **使用自動設定指令碼** - 如果知道代理設定指令碼的位置，您可以選擇此選項並提供指令碼的 URL。
- **使用代理伺服器** - 可以使用此選項來指定代理伺服器的 IP 位址和連接埠。也可以在**繞過防火牆**欄位中輸入 IP 位址或網域名稱，從而繞過代理伺服器，直接到這些位址。若需要，可以為代理伺服器輸入使用者名稱和密碼。如果代理伺服器要求使用者名稱和密碼，而您沒有指定，NetExtender 首次連接時將顯示一個視窗，提示您輸入使用者名稱和密碼。

當 NetExtender 使用代理設定連接時，它與代理伺服器建立 HTTPS 連接，而不是直接連到防火牆伺服器。代理伺服器隨即將流量轉送給 SSL VPN 伺服器。所有流量都由 SSL 利用 NetExtender 交涉的憑證加密，代理伺服器對此一無所知。對於代理和非代理使用者，連接過程相同。

安裝獨立用戶端

使用者首次啟動 NetExtender 時，NetExtender 獨立用戶端會自動安裝到使用者的 PC 或 Mac 上。安裝程式根據使用者的登入資訊建立一個設定檔。然後，安裝程式視窗關閉並自動啟動 NetExtender。如果使用者已安裝舊版 NetExtender，安裝程式會先解除安裝舊版 NetExtender 再安裝新版本。

NetExtender 獨立用戶端安裝完成後，Windows 使用者可以從 PC 的**開始 > 程式**功能表啟動 NetExtender，並設定 NetExtender 在 Windows 啟動時啟動。Mac 使用者可以從系統的**應用程式**資料夾啟動 NetExtender，或將其圖示拖到 Dock 中以便快速存取。在 Linux 系統中，安裝程式會在 **/usr/share/NetExtender** 中建立一個桌面快捷方式。可以將其拖到 Gnome 和 KDE 等環境的快捷方式欄中。

附註： 如需在 SonicWall 裝置安裝 NetExtender 的完整說明，請參見知識庫中的如何在 SonicOS 5.9 及更高版本 (SW10657) 上設定 SSL-VPN 功能（NetExtender 存取）。

視訊：SSL VPN 的設定方法的影片也解釋了設定 NetExtender 的程序。

設定使用者的 SSL VPN 存取

為使使用者能夠存取 SSL VPN 伺服器，必須將其指定到 **SSLVPN 服務群組**。若不屬於 **SSLVPN 服務**群組的使用者試圖通過虛擬辦公室登入，系統將拒絕其存取。

主題：

- 針對本機使用者
- 針對 RADIUS 和 LDAP 使用者
- 針對 Tunnel All 模式存取

針對本機使用者

新增和設定本機使用者與群組的詳細流程，請參閱 *SonicWall SonicOS 6.5 系統安裝*的**使用者**章節。以下提供快速參考資料，列出啟用 SSLVPN 服務所需的使用者設定。

若要設定本機使用者的 SSL VPN 存取：

1. 選擇**管理**檢視。
2. 導覽至**使用者 > 本機使用者和群組**。
3. 按一下想要編輯的使用者對應的**編輯**圖示，或者按一下**新增使用者**按鈕以建立新使用者。
4. 選擇**群組**。
5. 在**使用者群組**欄中，選擇 **SSLVPN 服務**再按一下**右箭頭**，將其移至**隸屬於**欄中。
6. 選擇 **VPN 存取**，再將適當的網路資源 VPN 使用者 (GVC、NetExtender 或虛擬辦公室書籤) 移至**存取清單**。

   附註：VPN 存取標籤會影響遠端用戶端使用 GVC、NetExtender 和 SSL VPN 虛擬辦公室書籤存取網路資源的能力。若要允許 GVC、NetExtender 或虛擬辦公室使用者存取網路資源，必須將網路位址物件或群組新增到 **VPN 存取**標籤上的**存取清單**。

7. 按一下**確定**。

針對 RADIUS 和 LDAP 使用者

設定 RADIUS 使用者和 LDAP 使用者的流程雷同。須將使用者新增至「SSLVPN 服務」使用者群組中。

設定使用者群組的詳細流程，請參閱 *SonicWall SonicOS 6.5 系統安裝*的**使用者**章節。以下提供快速參考資料，列出將使用者新增至適當群組所需的使用者設定。

設定 RADIUS 和 LDAP 使用者的 SSL VPN 存取步驟如下:

通用設定	設定 RADIUS 使用者	設定 LDAP 使用者
1 選擇**管理**檢視。		
2 導覽至**使用者 > 設定**。		
3 選擇**驗證**。		
4 在**使用者驗證方法**欄位中:	選擇 **RADIUS** 或 **RADIUS + 本機使用者**。	選擇 **LDAP** 或 **LDAP + 本機使用者**。
5 選擇：	**設定 RADIUS**	**設定 LDAP**
6 選擇：	**RADIUS 使用者**	**使用者和群組**
7 在適當欄位中選擇 **SSLVPN 服務**:	**所有 RADIUS 使用者所屬的預設使用者群組**	**預設 LDAP 使用者群組**
8 按一下確定。		

針對 Tunnel All 模式存取

新增和設定本機使用者與群組的詳細流程，請參閱 *SonicWall SonicOS 6.5 系統安裝*的**使用者**章節。以下提供快速參考資料，列出針對 **Tunnel All** 模式設定使用者和群組所需的使用者設定。

若要為 Tunnel All 模式設定 SSL VPN NetExtender 使用者和群組：

1. 選擇**管理**檢視。
2. 導覽至**使用者 > 本機使用者和群組**。
3. 按一下某 SSL VPN NetExtender 使用者或群組對應的**設定**圖示。
4. 選擇 **VPN 存取**。
5. 選擇 **WAN RemoteAccess Networks** 位址物件，再按一下**右箭頭**按鈕，將其移至**存取清單**。
6. 按一下**確定**。
7. 對所有使用 SSL VPN NetExtender 的本機使用者和群組重複進行流程。

生物識別驗證

重要：若要使用生物識別驗證功能，必須在行動裝置上安裝 Mobile Connect 4.0 或以上版本，並將其設為與防火牆連接。

SonicOS 支援生物識別驗證，需配合 SonicWall Mobile Connect。Mobile Connect 是應用程式，可讓使用者從行動裝置安全存取私人網路。您可透過 Mobile Connect 4.0 使用手指觸碰進行驗證，取代輸入使用者名稱和密碼。

允許此驗證方法所需的配置設定位於 **SSL VPN > 用戶端設定**頁面上。這些選項只會在 Mobile Connect 用於連接防火牆時顯示。

在 **SSL VPN > 用戶端設定**頁面上設定生物識別驗證之後，需在使用者的智慧型手機或其他行動裝置上啟用 Touch ID (iOS) 或指紋驗證 (Android)。

9

設定 SSL VPN 伺服器行為

SSL VPN > 伺服器設定頁面用於設定防火牆作為 SSL VPN 伺服器使用。

主題：

- 區域上的 SSL VPN 狀態
- SSL VPN 伺服器設定
- RADIUS 使用者設定
- SSL VPN 用戶端下載 URL

區域上的 SSL VPN 狀態

本章節顯示各區域上的 SSL VPN 存取狀態：

- 綠色表示使用中的 SSL VPN 狀態。
- 紅色表示非使用中的 SSL VPN 狀態。

按一下區域名稱以啟用或停用 SSL VPN 存取。

SSL VPN 伺服器設定

以下設定用於設定 SSL VPN 伺服器：

- **SSL VPN 連接埠** - 在此欄位中輸入 SSL VPN 連接埠號。預設為 **4433**。
- **憑證選擇** - 從此下拉功能表中選擇用於驗證 SSL VPN 使用者的憑證。預設方法是 **Use Selfsigned Certificate**。
- **使用者網域** - 輸入使用者的網域名稱，此網域名稱必須與 NetExtender 用戶端中網域欄位符合。預設值為 **LocalDomain**。

  附註：如果沒有使用驗證分割，此欄位必須與 NetExtender 用戶端中的網域欄位一致。

  如果使用了驗證分割，那麼使用者可在 NetExtender 中輸入以分割區設定的任何網域名稱，因此需選擇用於透過 RADIUS 或 LDAP 於外部驗證其名稱/密碼的分割區。在這種情況下，於此設定的名稱即為使用者輸入用於本機驗證的預設名稱，或者若使用者沒有本機帳戶，便是用於在預設分割區中進行驗證的預設名稱。

  請注意，無論是哪種情形，搭配使用外部驗證時，都不會將此使用者網域名稱傳送至 RADIUS/LDAP 伺服器，而是僅傳送不含網域名稱的簡單使用者名稱。

- **啟用 Web 管理通過 SSL VPN** - 若要通過 SSL VPN 啟用 Web 管理，從下拉功能表中選擇**啟用**。預設值為**已停用**。

- **啟用 SSH 管理通過 SSL VPN** - 若要通過 SSL VPN 啟用 SSH 管理，從下拉功能表中選擇**啟用**。預設值為**停用**。
- **非使用中狀態逾時（分鐘）** - 輸入使用者在登出之前非使用中的分鐘數。預設值為 **10** 分鐘。
-

RADIUS 使用者設定

此部分僅當設定 RADIUS 或 LDAP 來認證 SSL VPN 使用者時可用。

- **使用 RADIUS 在** - 勾選此核取方塊，讓 RADIUS 使用 MSCHAP（或 MSCHAPv2）模式。啟用 MSCHAP 模式 RADIUS 可允許使用者在登入時變更過期的密碼。有兩個模式可供選擇:
  - **MSCHAP**
  - **MSCHAPV2 模式（允許使用者變更過期的密碼）**

> **附註：**在 LDAP 中，只能在使用帶 TLS 的 Active Directory 時，或在與其繫結的情況下使用管理員帳戶或 Novell eDirectory 時變更密碼。
>
> 當已在**使用者 > 設定**頁面上選擇 LDAP 作為登入驗證方法，但是 LDAP 的設定不允許密碼更新時，如果設定了此選項，那麼 SSL VPN 使用者的密碼更新將會在利用 LDAP 驗證該使用者之後，透過 MSCHAP 模式的 RADIUS 進行。

SSL VPN 用戶端下載 URL

在頁面的這個區段中，可設定用戶端系統下載 SSL VPN 用戶端時所用的來源。可選擇從裝置下載檔案並放置在您的 SSL VPN 伺服器上，也可提供自己的 HTTP 伺服器以主控這個用戶端套件。

- **按一下這裡以下載 SSL VPN zip 檔案，此檔案包含了所有 SSL VPN 用戶端檔案** - 選擇此連結，從裝置下載所有用戶端 SSL VPN 檔案。打開並解壓縮此檔案，然後將資料夾放到您的 HTTP 伺服器上。
- **使用客戶的 HTTP 伺服器作為下載 URL： (http://)** 勾選此核取方塊，在提供的欄位中輸入 SSL VPN 用戶端下載 URL。

10

設定 SSL VPN 用戶端設定

在 **SSL VPN > 用戶端設定**頁面上，可編輯「預設裝置設定檔」和「SonicPoint 三層管理預設裝置設定檔」。「預設裝置設定檔」用於啟用區域上的 SSL VPN 存取、設定用戶端路由，以及設定用戶端 DNS 與 NetExtender 設定。「SonicPoint 三層管理預設裝置設定檔」用於啟用 SonicPoint 區域上的 SSL VPN 存取、設定用戶端路由，以及設定 SonicPoint 三層設定。

SSL VPN > 用戶端設定頁面也會顯示已設定並啟用 SSL VPN 存取的 IPv4 和 IPv6 網路位址和區域。

您還可以在此頁面上編輯 SonicPoint 三層管理預設裝置設定檔。

主題：

- 設定預設裝置設定檔
- 設定 SonicPoint L3 管理預設裝置設定檔

設定預設裝置設定檔

編輯「預設裝置設定檔」以選擇區域和 NetExtender 位址物件，以及設定用戶端路由，和設定用戶端 DNS 及 NetExtender 設定。

必須在一個區域上啟用 SSL VPN 存取後，使用者才能存取虛擬辦公室 Web 入口網站。SSL VPN 存取可在**網路 > 區域**頁面上設定 (功能表的**系統安裝**區段)。請參閱 *SonicWall SonicOS 6.5 系統安裝*的「網路」章節瞭解詳情。

主題：

- 設定選項
- 設定用戶端路由
- 設定用戶端設定

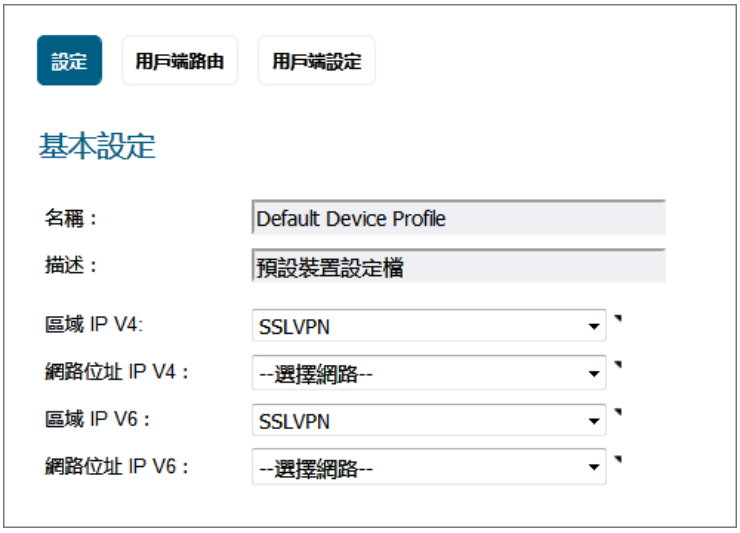
設定選項

設定預設裝置設定檔設定選項的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **SSL VPN > 用戶端設定**。

3 按一下**預設裝置設定檔**的**編輯**圖示。



附註：預設裝置設定檔的**名稱**和**說明**不能變更。

4 在**區域 IP V4** 下拉功能表中，選擇 **SSLVPN** 或自訂區域，以便設定此設定檔的區域繫結。

5 從**網路位址 IP V4** 下拉功能表中，選擇您為此設定檔建立的 IPv4 NetExtender 位址物件。如需指引，請參閱建立 NetExtender 範圍的位址物件。此設定選擇此設定檔的 IP 集區和區域繫結。如果位址物件符合此設定檔，NetExtender 用戶端將從此位址物件獲取 IP 位址。

6 在**區域 IP V6** 下拉功能表中，選擇 **SSLVPN** 或自訂區域，以便設定此設定檔的區域繫結。

7 從**網路位址 IP V6** 下拉功能表中，選擇您建立的 IPv6 NetExtender 位址物件。

8 按一下**確定**儲存設定再關閉視窗。

設定用戶端路由

您可在**用戶端路由**上控制 SSL VPN 使用者的網路存取許可。將 NetExtender 用戶端路由傳送給所有 NetExtender 用戶端，用於控制遠端使用者可以通過 SSL VPN 連接存取哪些私人網路和資源。

設定用戶端路由的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **SSL VPN > 用戶端設定**。

3 按一下**預設裝置設定檔**的**編輯**圖示。

4 選擇**用戶端路由**。

5 從 **Tunnel All 模式**下拉功能表中選擇**啟用**。

選擇此項系統便會強制 NetExtender 使用者的所有流量通過 SSL VPN NetExtender 通道，包括目的地為遠端使用者本機網路的流量。

6 選擇要允許 SSL VPN 存取的位址物件，再按一下**右箭頭**按鈕，將該位址物件移至**用戶端路由**清單。

7 重複步驟，直到移完所有要用於用戶端路由的位址物件。

若建立用戶端路由，也會建立系統將自動建立的存取規則。您也可手動設定 SSL VPN 區域的存取規則。請參閱 *SonicWall SonicOS 6.5 原則*瞭解有關存取規則的詳情。

8 按一下**確定**儲存設定再關閉視窗。

設定用戶端設定

「用戶端設定視窗」中有兩個選項區段:

- SSLVPN 用戶端 DNS 設定
- NetExtender 用戶端設定

SSLVPN 用戶端 DNS 設定

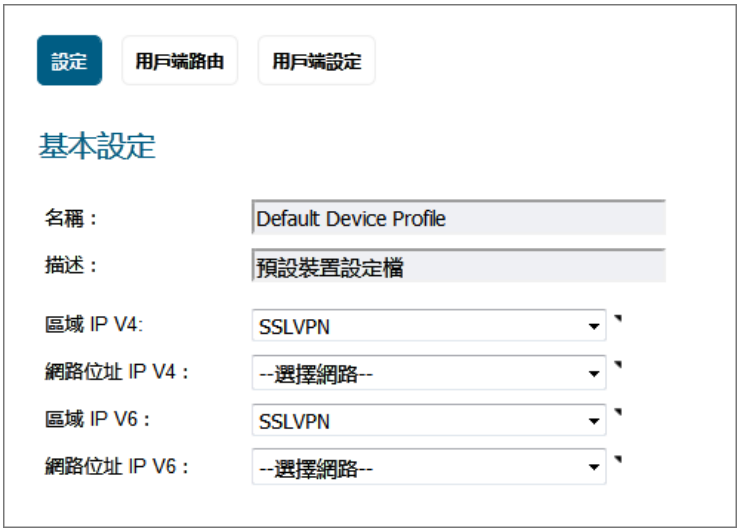
設定 SSLVPN 用戶端 DNS 設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **SSL VPN > 用戶端設定**。

3 按一下**預設裝置設定檔**的**編輯**圖示。

4 選擇**用戶端設定**。



5 在 **DNS 伺服器 1** 欄位中，選擇以下其中一項:

- 輸入主要 DNS 伺服器的 IP 位址。
- 按一下**預設 DNS 設定**為 **DNS 伺服器 1** 和 **DNS 伺服器 2** 欄位使用預設值。這些欄位將會自動填充。

附註：IP v4 和 IP v6 都支援。

6 （可選）在 **DNS 伺服器 2** 欄位中，如果沒有按一下**預設 DNS 設定**，請輸入備份 DNS 伺服器的 IP 位址。

7 (可選) 建立 **DNS 搜尋清單**的步驟如下:

a 在 **DNS 搜尋清單 (依序)** 欄位中，輸入 DNS 伺服器的 IP 位址。

b 按一下**新增**將其新增至以下清單。

c 根據需要多次重複步驟。

使用向上和向下箭頭按鈕，根據需要，在清單中捲動。若要從清單刪除一個位址，請選擇該位址再按一下**移除**。

8 （可選）在 **WINS 伺服器 1** 欄位中，輸入主要 WINS 伺服器的 IP 位址。

附註：僅支援 IPv4。

9 （可選）在 **WINS 伺服器 2** 欄位中，輸入備用 WINS 伺服器的 IP 位址。

10 若要自訂使用者連接和中斷連接時的 NetExtender 行為，請向下捲動至 **NetExtender 用戶端設定**。

11 為以下各項設定選擇**啟用**或**停用**，所有項目均預設為**停用**。

NetExtender 用戶端設定	定義
啟用用戶端自動更新	NetExtender 用戶端每次啟動時檢查有無更新。
中斷時結束用戶端	NetExtender 用戶端與 SSL VPN 伺服器中斷連接後結束。若要重新連接，使用者必須返回 SSL VPN 入口網站，或從「程式」功能表啟動 NetExtender。
在 IOS 裝置上允許觸控 ID	NetExtender 用戶端允許在 IOS 智慧型手機上進行 Touch ID 驗證。
在 Android 裝置上允許指紋驗證	NetExtender 用戶端允許在 Android 裝置上進行指紋驗證。
啟用透過 SSLVPN 的 NetBIOS	NetExtender 用戶端允許 NetBIOS 通訊協定。
結束時解除安裝用戶端	NetExtender 用戶端與 SSL VPN 伺服器中斷連接後解除安裝。若要重新連接，使用者必須返回 SSL VPN 入口網站。
建立用戶端連接設定檔	NetExtender 用戶端將建立一個連接設定檔，記錄 SSL VPN 伺服器名稱、網域名稱以及 (可選) 使用者名稱和密碼。

12 為提供靈活性，允許使用者將其使用者名稱和密碼快取在 NetExtender 用戶端中，可從**使用者名稱和密碼快取**欄位中選擇以下其中一種操作。這些選項使您能夠裝載均衡安全性需求與使用者每次使用的便利性需求。

- **僅允許儲存使用者名稱**
- **允許儲存使用者名稱和密碼**
- **禁止儲存使用者名稱和密碼**

13 按一下**確定**。

設定 SonicPoint L3 管理預設裝置設定檔

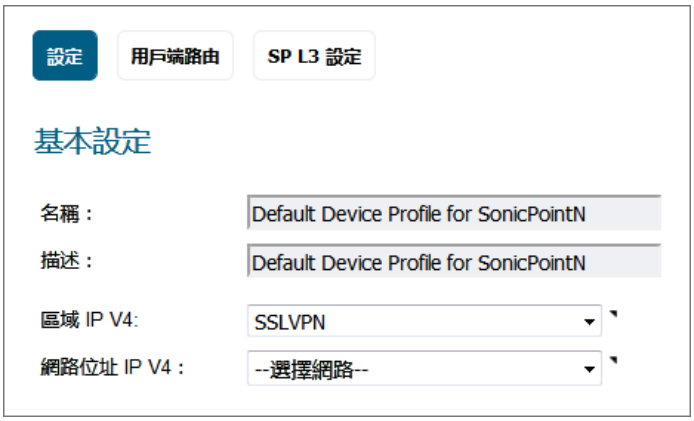
設定 SonicPoint L3 管理預設裝置設定檔，即可設定 SonicPoint 區域上的 SSL VPN 存取、設定用戶端路由和 SonicPoint 裝置的 L3 設定。

設定 SonicPoint L3 設定檔設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **SSL VPN > 用戶端設定**。

3 按一下 **SonicPoint L3 管理預設裝置設定檔**對應的**編輯**圖示。



附註：SonicPoint L3 管理預設裝置設定檔的**名稱**和**說明**不能變更。

4 若要設定此設定檔的區域繫結，在**設定**標籤上，從**區域 IP V4** 下拉功能表中選擇 **SSLVPN** 或自訂區域。

5 從**網路位址 IP V4** 下拉功能表中，選擇您建立的 IPv4 NetExtender 位址物件。如需指引，請參閱建立 NetExtender 範圍的位址物件。此設定選擇此設定檔的 IP 集區和區域繫結。如果位址物件相符，NetExtender 用戶端將從此位址物件獲取 IP 位址。

6 按一下**用戶端路由**標籤。

7 從**網路**清單中，選擇要允許 SSL VPN 存取的位址物件，再按一下**右箭頭**，將該位址物件移至**用戶端路由**清單。

8 重複步驟，直到移完所有要用於用戶端路由的位址物件。

建立用戶端路由會自動建立存取規則以允許此存取。也可以在**規則 > 存取規則**頁面上手動設定 SSL VPN 區域的存取規則。更多資訊請參閱 *SonicWall SonicOS 6.5 系統安裝*。

附註：設定 SSL VPN 的用戶端路由後，還必須設定所有 SSL VPN NetExtender 使用者和使用者群組，他們才能存取用戶端路由。請參閱設定使用者的 SSL VPN 存取瞭解詳情並取得快速參考清單。

9 按一下 **SP L3 設定**標籤。

10 從 **WLAN 通道介面**下拉功能表中選擇一個介面。

11 按一下**確定**。

11

設定 SSL VPN Web 入口網站

在 **SSL VPN > 入口網站設定**頁面上，可設定 SSL VPN 虛擬辦公室 Web 入口網站的外觀和功能。虛擬辦公室入口網站是利用登入啟動 NetExtender 的網站。它可以自訂以便與任何現有的公司網站或設計風格保持一致。

主題：

- 入口網站設定
- 入口商標設定

入口網站設定

入口網站設定用於自訂使用者登入時顯示的內容，請根據貴公司的要求加以變更。

選項	定義
入口網站標題	在此欄位中輸入 Web 瀏覽器頂端標題顯示的文字。預設值是 **SonicWall - 虛擬辦公室**。
入口網站橫幅標題	在此欄位中輸入頁面頂端標誌旁邊顯示的文字。預設值是**虛擬辦公室**。
首頁訊息	輸入 NetExtender 圖示上方顯示的 HTML 代碼。自行輸入文字，或按一下**範例範本**以填入可保留原文或進行編輯的預設範本。按一下**預覽**以查看首頁訊息的外觀。
登入訊息	輸入提示使用者登入虛擬辦公室時顯示的訊息之 HTML 代碼。自行輸入文字，或按一下**範例範本**以填入可保留原文或進行編輯的預設範本。按一下**預覽**以查看登入訊息的外觀。

下列選項自訂虛擬辦公室入口網站的功能：

- **登入後啟動 NetExtender** - 選擇此選項 NetExtender 會在使用者登入後自動啟動。預設情況下未勾選此選項。
- **顯示匯入憑證按鈕** - 選擇此按鈕以在虛擬辦公室頁面上顯示**匯入憑證**按鈕。它用於啟動將防火牆自簽章的憑證匯入 Web 瀏覽器的過程。預設情況下未勾選此選項。

  附註：從 **SSL VPN > 伺服器設定**頁面上的**憑證選擇**下拉功能表選擇 **Use Selfsigned Certificate** 時，此選項僅適用於 PC 上的 Internet Explorer 瀏覽器，且 PC 執行 Windows 操作系統。

- **為快取控制啟用 HTTP 中繼標籤（建議）** - 選擇此選項將 HTTP 標籤插入瀏覽器中，指示 Web 瀏覽器不要快取虛擬辦公室頁面。預設情況下未勾選此選項。

  附註：SonicWall 推薦啟用此選項。

- **在 SSL VPN 連接埠顯示 UTM 管理連結（不建議）** - 選擇此選項將會在 SSL VPN 入口網站上顯示 SonicWall 裝置的管理連結。預設情況下未勾選此選項。

  重要：SonicWall 不推薦啟用此選項。

入口商標設定

本節可以自訂在虛擬辦公室入口網站頂部顯示的商標。標誌必須是大小為 155 x 36 的 GIF 格式。推薦使用透明或者淺背景。

- **預設的入口網站標誌** - 顯示預設的入口網站標誌，亦即 SonicWall 標誌。
- **使用預設的 SonicWall 標誌** - 勾選方塊以使用裝置所提供的 SonicWall 標誌。預設情況下未勾選此選項。
- **自訂標誌** (輸入標誌的 URL) - 輸入要顯示的標誌 URL。

  提示：商標必須是 155 x 36 大小的 GIF 格式，推薦使用透明或者淺背景。

12

設定虛擬辦公室

SSL VPN > 虛擬辦公室頁面顯示 SonicOS 管理介面內部的虛擬辦公室 Web 入口網站。

主題：

- 存取虛擬辦公室入口網站
- 設定 SSL VPN 書籤
- 設定用於 IPv6 的裝置設定檔設定

存取虛擬辦公室入口網站

存取虛擬辦公室入口網站的方式有兩種。系統管理員可透過裝置介面存取，且有權限對整個網站進行適當變更。使用者則藉由不同流程以不同方式存取，且只能變更影響其特定設定檔的內容。

系統管理員存取 SSL VPN 虛擬辦公室入口網站的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **SSL VPN > 虛擬辦公室**。

使用者查看 SSL VPN 虛擬辦公室 Web 入口網站的步驟如下:

1 移至防火牆的 IP 位址。

2 按一下登入頁面底部寫著**按一下這裡進行 sslvpn 登入**的連結。

設定 SSL VPN 書籤

可將使用者書籤設定為顯示在虛擬辦公室首頁上。個人使用者無法修改或刪除管理員建立的書籤。

建立書籤時請記得，某些服務可以在非標準連接埠上執行，某些在連接時需要一個路徑。設定入口網站書籤時，需為**服務**類型搭配正確的**名稱 IP 位址**格式。設定這些選項時請參考下表。

附註：SonicOS 6.5 中不存在 ActiveX 和 Java 服務類型。升級時會將舊版的偏好設定轉換為 HTML5。

不同服務類型對應的書籤名稱或 IP 位址格式

服務類型	格式	名稱或 IP 位址欄位範例
RDP - ActiveX RDP - Java	IP 位址	10.20.30.4
	IP:連接埠（非標準）	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主機名稱	JBJONES-PC
VNC	IP 位址	10.20.30.4
	IP:連接埠（對應到工作階段）	10.20.30.4:5901（對應至階段 1）
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主機名稱	JBJONES-PC
	附註：請勿用工作階段或顯示編號代替連接埠。	**附註：**請勿使用 10.20.30.4:1 **提示：**對於連結到 Linux 伺服器的書籤，參見本表下方的提示。
Telnet	IP 位址	10.20.30.4
	IP:連接埠（非標準）	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主機名稱	JBJONES-PC
SSHv1 SSHv2	IP 位址	10.20.30.4
	IP:連接埠（非標準）	10.20.30.4:6818
	FQDN	JBJONES-PC.sv.us.sonicwall.com
	主機名稱	JBJONES-PC

重要：建立連結到 Linux 伺服器的**虛擬網路計算 (VNC)** 書籤時，除了在**名稱或 IP 位址**欄位中輸入 Linux 伺服器 IP 以外，還必須指定連接埠號和伺服器編號，格式如下：**ipaddress:port:server**。例如，如果 Linux 伺服器 IP 位址為 192.168.2.2，連接埠號為 5901，伺服器編號為 1，那麼**名稱或 IP 位址**欄位的值將是 **192.168.2.2:5901:1**。

新增入口網站書籤的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇 **SSL VPN > 入口網站辦公室**。

3 按下**新增**。

4 在**書籤名稱**欄位中輸入書籤的描述性名稱。

5 在**名稱或 IP 位址**欄位中輸入 LAN 上主機的完整網域名稱 (FQDN) 或 IPv4 位址。請參閱不同服務類型對應的書籤名稱或 IP 位址格式表格 (前一個表格) 瞭解特定**服務**類型預期的**名稱或 IP 位址**。

6 在**服務**下拉功能表中選擇適當的服務類型:

- **RDP (HTML5-RDP)**
- **SSHv2 (HTML5-SSHv2)**
- **TELNET (HTML5-TELNET)**
- **VNC (HTML5-VNC)**

根據您選擇的項目而定，顯示的選項會有所不同。

7 為所選的服務填寫剩餘欄位。如需瞭解選項和定義，請參閱下表:

如果服務設為 RDP (HTML5-RDP)，請設定以下項目:

畫面大小	在下拉功能表中，選擇使用者執行此書籤時要使用的預設終端服務畫面大小。 不同的電腦支援不同的介面大小，使用遠端桌面應用程式時，應當選擇從中執行遠端桌面工作階段的電腦支援的介面大小。
顏色	在下拉功能表中，選擇使用者選擇此書籤時終端服務畫面的預設顏色深度。
應用程式與路徑 (可選)	如有需要，可輸入遠端電腦上應用程式所在的本機路徑。
在以下資料夾開啟	如有需要，可輸入要從哪個本機資料夾中執行應用程式命令。

顯示視窗進階選項	按一下箭頭以展開項目，查看所有 Windows 進階選項。勾選方塊以啟用要使用的選項: • **重新導向剪貼簿** • **自動重新連接** • **視窗拖曳** • **重新導向音訊** • **桌面背景** • **功能表/視窗動畫**
自動登入	勾選方塊以啟用自動登入。若勾選此項，請選擇要使用的憑證: • **使用 SSL-VPN 帳戶憑證** • **使用自訂憑證** 若選擇自訂憑證，請輸入憑證的使用者名稱、密碼和網域。 **附註：**使用者名稱和網域可使用動態變數。請參閱動態變數
向 Mobile Connect 用戶端顯示書籤	勾選方塊以向 Mobile Connect 使用者顯示書籤。
如果服務設為 SSHv2 (HTML5-SSHv2)，請設定以下項目:	
自動接受主機金鑰	勾選方塊以啟用。
向 Mobile Connect 用戶端顯示書籤	勾選方塊以向 Mobile Connect 使用者顯示書籤。
如果服務設為 TELNET (HTML5-TELNET)，請設定以下項目:	
向 Mobile Connect 用戶端顯示書籤	勾選方塊以向 Mobile Connect 使用者顯示書籤。
如果服務設為 VNC (HTML5-VNC)，請設定以下項目:	
僅瀏覽	勾選方塊以將書籤設定為僅瀏覽模式。
共用桌面	啟用共用桌面功能。
向 Mobile Connect 用戶端顯示書籤	勾選方塊以向 Mobile Connect 使用者顯示書籤。

8 按一下**確定**儲存設定。

動態變數

文字用法	變數	使用範例
登入名稱	%EXPERTNAME%	US\%USERNAME%
網域名稱	%USERDOMAIN%	%USERDOMAIN\%USERNAME%

設定用於 IPv6 的裝置設定檔設定

SonicOS 支援擁有 IPv6 位址的使用者使用 NetExtender 連接。在 **SSL VPN > 用戶端設定**頁面上，首先設定傳統 IPv6 IP 位址集區，然後設定 IPv6 IP 集區。每個用戶端將指派兩個內部位址：一個 IPv4 和一個 IPv6。

附註：不支援 IPv6 Wins 伺服器。

在 **SSL VPN > 用戶端路由**頁面上，使用者可以從所有位址物件，包括所有預先定義 IPv6 位址物件的下拉清單中選擇一個用戶端路由。

附註：支援 IPv6 FQDN。

第 3 部分

存取點

- 瞭解 SonicWall 存取點
- 存取點儀表板
- 存取點基本設定
- 存取點樓面規劃存取點樓面規劃
- 存取點拓撲檢視
- 設定 SonicPoint 入侵偵測服務
- 設定進階 IDP
- 存取點封包擷取
- 設定虛擬存取點
- 設定 RF 監控
- 設定 FairNet
- 設定 Wi-Fi 多媒體
- 存取點 3G/4G/LTE WWAN

13

瞭解 SonicWall 存取點

附註：SonicWall SuperMassive 9800 不支援存取點。

SonicWall SonicPoint 和 SonicWave 是專門用於與 SonicWall 安全裝置配合使用的無線存取點，可為您的整個企業提供無線存取。介面的**管理**檢視上，**連線 | 存取點**用於管理與您的系統連接的存取點。

本節提供在網路中使用 SonicWall 存取點，以及將這些存取點與 SonicWall 網路裝置整合的相關資訊與最佳做法。

主題：

- 存取點功能矩陣
- 存取點功能
- 規劃與實地調查
- 存取點部署最佳做法
- 存取點授權
- 管理 SonicPoints 之前
- 存取點和 RADIUS 計費

存取點功能矩陣

SonicOS 提供多種功能，但並非所有 SonicWall 存取點都支援所有功能，詳情請參閱下表。

無線功能支援 (依存取點類型)

功能名稱	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
頻段切換	是	是	是	否
空中傳輸時間公平性	是	是	是	否
無線鑒別封包擷取	是	否	否	否
WDS AP 支援	是	是	是	否
平面設計圖檢視	是	是	是	是
拓撲檢視	是	是	是	是
SSLVPN 集中器	是	是	是	是
即時監控視覺化	是	是	是	否
動態 VLAN	是	是	是	否
3G/4G/LTE 延伸器	是	是	是	否

無線功能支援 (依存取點類型)

功能名稱	SonicWave	SonicPoint ACe/ACi	SonicPoint N2	SonicPoint Ne/Ni/NDR/N
用戶端指紋識別與報告	是	是	是	否
SNMP MIB 擴充	是	是	是	是
GRE 管理多核心支援	是	是	是	是
Restful API 支援	是	是	是	否
來賓服務：基於 IP 的來賓驗證繞過網路	是	是	是	是
來賓服務：來賓使用者群組的配額週期	是	是	是	是
原生橋接支援	是	是	是	是
無線內建無線電中繼器模式	僅適用 TZ 無線	僅適用 TZ 無線	僅適用 TZ 無線	僅適用 TZ 無線
無線內建無線電 WDS 模式	僅適用 TZ 無線	僅適用 TZ 無線	僅適用 TZ 無線	僅適用 TZ 無線

存取點功能

SonicWall 存取點與 SonicWall 下一代防火牆整合，可建立安全的無線解決方案，為有線和無線網路提供全方位防護。它們提供高速無線存取並提高了訊號品質與可靠性，運用最新功能實現 Gigabit 無線效能。SonicPoint/SonicWave 系列支援 IEEE 802.11a/b/g/n/ac 標準，讓貴組織能在高密度環境中使用頻寬密集型行動應用程式，且不會削弱訊號。

主題：

- SonicPoint/SonicWave 功能
- 認證與合規性
- 存取點樓面規劃檢視
- 存取點拓撲檢視
- 入侵偵測/防護
- 虛擬存取點
- 存取點 WMM 設定
- 日本和國際存取點支援

SonicPoint/SonicWave 功能

SonicPoint/SonicWave 存取點藉由提供更多天線、更寬的頻道、更多空間串流以及其他提升傳送量和可靠性的功能，在 5GHz 頻段中提供更高傳送量。SonicPoint AC 和 SonicWave 裝置支援 5GHz 與 2.4GHz 無線頻段，且具備以下關鍵技術元件:

- **更寬的頻道** - 80 MHz 和 160 MHz 頻道頻寬
- **高達 4 個空間串流** - 新增空間串流將成比例增加生產力。兩個空間串流的傳送量是單個空間串流的兩倍。四個空間串流將傳送量增加四倍。
- **多使用者 MIMO** - 多重輸入多重輸出空間分割多工功能，可同時傳輸和接收多個獨立資料流。

  SonicWave 和 SonicPoint AC 提供更高傳送量，使其更適合於無線顯示、HDTV、下載大檔案，以及校園和禮堂應用。
- **三層管理工作階段 I** - 提供了 DHCP 和通道解決方案，以支援三層網路中的存取點部署。
  - SonicWall 基於 DHCP 的發現通訊協定 (SDDP) 基於已知的 DHCP 協定，允許 SonicWall 閘道和存取點在三層本機網路中發現對方。
  - 遠端網路管理通訊協定 SonicWall 基於 SSL VPN 的管理通訊協定 (SSMP)，是基於 SonicWall SSL VPN 基礎結構允許已啟用 SonicWall SSL VPN 的網路安全裝置通過網際網路管理存取點。SonicWave 432e/432i/432o、SonicPoint AC/N2/N/Ni/Ne/NDR、所有 SuperMassive、NSA 和執行 SonicOS 6.2 或更高版本的 TZ 防火牆提供支援。
- **動態頻率選擇 (DFS) 支援** - 頒發 DFS 憑證後，存取點可以支援動態頻率選擇，允許在 5GHz 頻帶的敏感頻道中部署存取點。
- **存取點儀表板** - **存取點 > 儀表板**頁面會報告各存取點的統計資料。**儀表板**以圖形型式摘要頻寬和用戶端資訊，也提供即時用戶端監控詳細資料。
- **頻段切換** - 頻段切換功能讓存取點可將支援 5 GHz 的用戶端切換至該頻段；這個頻段的干擾和流量通常較少。但是，如果訊號出現干擾或強度減弱，系統會將用戶端導向至 2.4 GHz 頻段。用意在於進行使用者無線管理，協助提升整體容量、傳送量和使用者體驗。
- **開放式驗證、社交登入和 LHM** - SonicOS 6.2.7 和更高版本支援社交媒體 (例如 Facebook、Twitter 和 Google+) 的開放式驗證和社交登入功能，也支援 LHM (輕量級熱點訊息)。
- **射頻分析** - 射頻分析 (RFA) 功能有助於網路管理員瞭解存取點和其他相鄰無線存取點如何使用無線頻道。
- **保留 SonicWave 設定檔設定** - 可以設定存取點設定檔，如此一來即使刪除或重新同步了存取點，這些存取點仍可保留部分設定。
- **VLAN 標籤 -** 可以透過虛擬存取點 (VAP) 在 VLAN 中設定優先順序，因為 SonicPointN 和 AC 允許將 VAP 設定為使用同一 VLAN ID 連接 VLAN。您可以通過防火牆存取規則為 VLAN 流量設定優先順序。
- **無線診斷** - 存取點可以收集關鍵的執行階段資料，並將其儲存到永久儲存區中。如果存取點出現故障，SonicWall 管理設備會在存取點重新啟動時擷取該資料，並將其組合到技術支援報告 (TSR) 中。隨後的存取點故障將會覆寫此資料。
- **存取點 3G/4G WWAN** - 使用者可將 USB 數據機裝置插入 SonicWall 存取點，而存取點可執行撥號作業以連接網際網路。連接完成後，存取點可作為防火牆的 WWAN 裝置並提供 WAN 存取。
- **菊花式鏈結** - 菊花式鏈結允許小型環境（即，低密度交換器基礎結構）使用者在盡可能少地使用交換器連接埠的情況下部署多個存取點。例如，可將商店內分散的許多裝置連接到商店交換器基礎結構中，儘管此基礎結構在交換器連接埠密度/可用性方面是比較小型的，仍可包括多個存取點以覆蓋整個商店。存取點在 LAN2 介面中是以菊花式鏈結方式連接。

重要：菊花式鏈結存取點會影響傳送量；每次新增存取點都會降低傳送量。如果傳送量為：

- 關注問題，則保持傳送量在可接受水平，對於：
  - SonicPoint N2，菊花式鏈結的存取點不要超過 3 個。
  - SonicPoint ACe/ACi，菊花式鏈結的存取點不超要過 2 個。
- 非關注問題，菊花式鏈結的存取點不要超過 4 個。

如果採用 SonicWave 或 SonicPoint AC 型號和 SonicPoint N 或 N2 型號混合的模式，請將 SonicWave 或 SonicPoint AC 型號部署在鏈結的起始處。

認證與合規性

SonicWall 存取點經過嚴格測試，獲得各項業界認證。

Wi-Fi 聯盟認證

附註：SonicPoint 雙無線（SonicPointNDR 和 SonicPointACe/ACi/N2）已經過 Wi-Fi 聯盟的 Wi-Fi 認證，由「Wi-Fi 認證」標誌指定。

Wi-Fi 的認證標誌是 Wi-Fi 聯盟的認證標誌，表示此產品已經過 Wi-Fi 聯盟的嚴格測試，且已證明可與其他產品進行互操作，包括有 Wi-Fi 認證標誌的其他公司的產品。

FCC U-NII 新規則合規

自 SonicOS 6.2.5.1 開始，執行韌體版本 9.0.1.0-2 或更高版本的 SonicPointACe/ACi/N2 支援 FCC U-NII（未獲授權 - 國家資訊基礎設施）新規則（報告和順序 ET 案卷編號 13-49)。為符合 FCC 新規則中的動態頻率選擇 (DFS)，SonicPoint 存取點會偵測並避免干擾 DFS 頻段雷達訊號。

附註：使用符合 FCC 新規則的韌體製造的 SonicPointACe/ACi/N2 無線存取點僅支援 SonicOS 6.2.5.1 和更高版本。連接到執行 SonicOS 6.2.5.1 或更高版本的防火牆後，較舊的 SonicPointACe/ACi/N2 存取點會自動更新為符合 FCC 新規則的韌體。

RED 合規性和認證

SonicWall TZ 和 SOHO 無線裝置與 SonicWall 無線存取點皆符合歐盟無線電設備指令 (RED)。請造訪 SonicWall 支援入口網站，參閱「技術文件」底下的*無線電設備指令 (RED) 附錄*:
https://www.sonicwall.com/Support/Technical-Documentation/Radio-Equipment-Directive-(RED)-Addendum。

存取點樓面規劃檢視

SonicOS 6.5 提供更直觀的方法，便於管理大量 SonicWall 存取點裝置，您也可追蹤實體位置和即時狀態。

樓面規劃檢視是 SonicOS 中現有存取點管理套件的附加元件，可針對您的實際存取點無線部署環境提供即時情況，且可提升預估新部署無線覆蓋範圍的能力。樓面規劃檢視也提供實用工具，可從整合的操作功能表監控即時狀態、設定存取點、移除存取點，甚至可顯示 RF 覆蓋範圍。

存取點拓撲檢視

拓撲檢視可呈現從 SonicWall 防火牆到端點的網路拓撲，您可運用拓撲檢視來管理存取點。您可監控存取點即時狀態，且操作功能表也可提供設定選項。

此功能可顯示所有 WLAN 相關裝置間的邏輯關係，且使用者可在拓撲檢視中直接管理裝置。開啟**連線 | 存取點 > 拓撲檢視**時，系統會藉由連接防火牆已知的裝置來顯示一個類似樹狀目錄的圖，並呈現其關係。

拓撲檢視管理以圖表方式為管理員呈現 WLAN 網路，提供最常用的資訊和狀態。將裝置繪製為樹狀目錄上的節點，且可利用滑鼠和滑鼠滾輪來縮放樹狀目錄。樹狀目錄中顯示的資訊包含裝置類型、IP 位址、連接的介面、名稱、用戶端數量，而部分裝置上的模擬 LED 燈則表示狀態。工具提示泡泡顯示裝置的詳細資訊。

入侵偵測/防護

SonicWall 存取點對射頻 (RF) 裝置提供防護。RF 技術用於無線網路裝置對入侵者有吸引力。存取點使用直接 RF 監控功能來偵測威脅，不會中斷目前無線或有線網路的運作。這類功能包含:

- **入侵偵測服務** - 入侵偵測服務 (IDS) 使 SonicWall 網路安全裝置可以識別這類常見的無效無線活動並採取應對措施。IDS 會報告防火牆可藉由掃描存取點上的 802.11a/b/g/n/ac 無線頻段找到的所有存取點。
- **進階入侵偵測和防護** - 進階入侵偵測和防護 (IDP) 監控無線電頻譜中是否存在未授權存取點（入侵偵測），並自動採取應對措施（入侵保護）。在存取點上啟用了進階 IDP 時，其無線電功能將充當專用 IDP 感應器。
- **欺詐裝置偵測和防護** - 可以將存取點設定為採用專用感應器模式，以專注於在 2.4GHz 和 5GHz 頻段上被動或主動進行欺詐裝置偵測和防護。即使僅使用一個頻段，仍然可以掃描這兩個頻段。可以對欺詐裝置進行分析，以報告其是否連接到網路，以及有線或無線機制是否將之封鎖。
- **內建無線電掃描排程** - 現在可以為存取點安排排程，根據精細的排程選項執行入侵偵測/防護掃描，全天候掌握情況。為所有存取點型號編輯存取點設定檔時，可使用 **802.11n 無線**標籤 (或類似標籤) 上的排程選項。

虛擬存取點

虛擬存取點 (VAP) 是單個實體存取點的多路複用實例，讓單個存取點顯示為多個分立的存取點或 VAP。對於無線 LAN 用戶端，每個 VAP 都會顯示為一個獨立的實體存取點，而實際上只存在一個實體存取點。

- **虛擬存取點排程支援** - 為便於使用，可以單獨啟用或停用每個 VAP 排程。
- **虛擬存取點二層橋接** - 可以將每個 VAP 橋接到 LAN 區域上的對應 VLAN 介面，從而提供更高的靈活性。
- **虛擬存取點 ACL 支援** - 每個 VAP 均可支援單獨的存取控制清單 (ACL)，以提供更高效的驗證控制。
- **SonicPoint N 雙無線上的虛擬存取點群組共用** - 可以將相同的 VAP/VLAN 設定套用於雙無線。這樣，您即可將統一的原則用於兩個無線以及在網路交換器中共用 VLAN 轉接。

存取點 WMM 設定

存取點支援 Wi-Fi 多媒體 (WMM)，可在雜項應用程式上提供更優良的服務品質體驗，包括在 Wi-Fi 電話上提供 VoIP，在無線網路上提供多媒體流量。WMM 是一種基於 IEEE 802.11e 標準的 Wi-Fi 聯盟互操作認證。WMM 根據四個存取類別區分流量的優先順序：語音、視訊、最佳成就和背景。

附註：WMM 不保證傳送量。

每個存取類別都有自己的傳送佇列。WMM 要求存取點為多個優先順序存取類別實施多個佇列。為區分流量類型，存取點依賴應用程式或防火牆在 IP 資料中提供服務類型 (TOS) 資訊。一種方法是通過防火牆服務和存取規則提供 TOS；另一種方法是通過 VLAN 標籤提供此資訊。

可於**管理**檢視上的**連線 | 存取點 > Wi-Fi 多媒體**頁面設定 WMM 設定與對應。

日本和國際存取點支援

SonicOS 6.2.2.2 及更高版本對日本和國際 SonicPointACe/ACi/N2 無線存取點均支援。SonicOS 6.5 及更高版本支援日本和國際 SonicWave 432e/432i/432o 無線存取點。國際存取點是在美國與日本以外的國家部署以及運作。

當國際存取點連接到一台 SonicWall 網路安全設備時，SonicOS 會在**存取點 > 基本設定**頁面上顯示一個**註冊**按鈕。按一下**註冊**將打開一個對話方塊，您可以在其中選擇合適的**國家或地區代碼**。

附註：請務必選擇存取點部署所在國家或地區的相應國家或地區代碼，即使您註冊該存取點時不是在此國家或地區內。

對於註冊所用的國家或地區代碼非加拿大的國際存取點，其國家或地區代碼可在**連線 | 存取點 > 基本設定**頁面上的設定檔中變更。

重要：當存取點註冊的是加拿大的國家或地區代碼時，只能聯絡 SonicWall 支援來變更國家或地區代碼。

規劃與實地調查

在環境中部署 SonicWall 存取點以前，請先花時間瞭解設備要求。以下章節說明部署前的提條件，並列出實地調查過程中需確認的事項。

主題：

- 前提條件
- 站台調查和規劃
- PoE 和 PoE+

前提條件

以下是成功部署存取點所需的條件:

- SonicOS 需要公用網際網路存取權限，網路安全裝置才能下載和更新存取點的韌體映像。如果無法使用公用網際網路，則需手動取得和下載存取點韌體。

- 一個或多個 SonicWall 無線存取點。
- 如果使用 PoE/PoE+ 交換器為存取點供電，必須為以下其中一種:
    - 適用於 SonicWave 432e/432i/432o 且符合 802.3at 的乙太網路交換器
    - 適用於 SonicPointACe/ACi/N2 符合 802.3at 的乙太網路交換器
    - 適用於其他存取點型號且符合 802.3af 的乙太網路交換器
- 您應取得 SonicWall 網路安全裝置的支援合約以及 PoE/PoE+ 交換器。在發現交換器端或防火牆端存在問題或發佈新功能時，此合同將使您能夠升級到新版本。
- 安裝前請務必全面進行實地調查，以便瞭解需為安裝和實作做好哪些準備。
- 檢查接線和纜線基礎結構，以驗證 SonicWall 存取點之間的端到端執行，並檢查乙太網路交換器是否為 CAT5、CAT5e 或 CAT6。
- 為安裝點確認建築法規，並與建築物的設施工作人員配合工作，因為某些預定的安裝點可能存在違規現象。

站台調查和規劃

進行實地調查和規劃 SonicWall 存取點部署是成功實作的關鍵要素。調查和規劃時請參考以下準則:

- 對預定要部署存取點的所有區域進行全面的實地檢查。使用無線光譜掃描儀，留意所有現有的存取點以及廣播它們的頻道。SonicWall 目前建議使用 Fluke 或 AirMagnet 產品執行全面的調查。您也可以嘗試使用 NetStumbler/MiniStumbler，這項免費產品只要使用您的無線卡，就能執行適當的調查工作。
- 調查期間請善用樓面設計圖，可以標記存取點的位置和無線基地台的範圍。請影印多份樓面設計圖，因為根據實地調查結果，可能需採用新設計從頭來過。同時，在牆壁、走廊和電梯的位置處，可能會影響訊號。還應注意使用者所在的區域和不存在使用者的區域。

  進行實地調查期間，在有許多電子裝置的區域，注意可能會帶來干擾的電子裝置 (微波爐、CAT 掃描裝置等)，也需確認使用的纜線類型。
- 以三維方式進行調查 (左右、前後、上下)，因為無線訊號會跨越不同樓層。
- 根據電源和纜線決定可放置存取點的位置。記住，不應將存取點安置在緊靠金屬或混凝土牆壁的位置，而應儘量靠近天花板。
- 使用無線掃描工具檢查訊號強度和噪音。訊號與噪聲比應至少為 10 dB（11 Mbps 的最小值要求），但慣用的 20 dB。這兩個因素都會影響服務的品質。
- 根據您的調查結果，可能需重新放置部分存取點並重新測試。
- 儲存設定，記錄位置並備註資訊供未來參考。建立樓面規劃檢視將需用到這些資訊。
- 使用舊的 SonicPoint 型號時，您可能會發現某些區域或所有區域存在重疊的 802.11b/g 頻道而飽和，此情況下您可能想要使用 802.11a 無線來部署存取點。儘管 802.11a 的範圍有限，且這些裝置不允許新增外部天線，這仍可提供更大陣列的廣播頻道。
- 注意不要將無線訊號傳送到您無法控制的區域；檢查人們能夠篩選訊號並相應地調整存取點。
- 為輕度使用，可計劃為每個存取點設定 15-20 個使用者。對商業使用，應計劃為每個存取點設定 5-10 個使用者。
- 針對漫遊使用者進行計劃 - 這需要調整每個存取點上的電源，以便讓訊號的重疊程度降到最低。在重疊程度較大的區域中，如果多個存取點廣播同一個 SSID，可能會導致用戶端連接問題持續存在。
- 使用 SonicOS 的排程功能，在不使用存取點時將其關閉。SonicWall 建議非工作時間 (例如夜間和週末) 不要讓存取點運作。

PoE 和 PoE+

規劃時，務必注意纜線從存取點安裝的位置開始的長度，必須小於等於 100 公尺。如果您不使用 PoE 交換器，還需要考慮用於存取點的變壓器或 PoE 轉換器。確保不會製造電器火災危險。

纜線太長會造成電量損耗；存取點和 PoE 交換器之間的纜線長度為 100 公尺時，可能會導致最高 16% 的電量/訊號削弱，如此一來，PoE 交換器需要為連接埠供應更多電量，才能讓 SonicPoint 正常運作。

SonicPointACe/ACi/N2

為 SonicPointACe/ACi/N2 提供乙太網路供電/乙太網路供電+ (PoE/PoE+) 的任何交換器都必須完全符合 802.3at 的要求。不要在不符合要求的交換器上執行 SonicPoints，因為 SonicWall 不支援。

重要：關閉 pre-802.3at-spec 偵測，否則可能會導致連接問題。

SonicPoint AC（類型 1）可設定為 0、1、2，或 3 PD 級。SonicPoint AC（類型 2）設定為 4 PD 級。最小和最大功率輸出值如下：

- 類型 1，0 PD 級使用最小 0.5 W 到最大 15.4 W
- 類型 1，1 PD 級使用最小 0.5 W 到最大 4.0 W
- 類型 1，2 PD 級使用最小 4.0 W 到最大 7.0 W
- 類型 1，3 PD 級使用最小 7.0 W 到最大 15.4 W
- 類型 2，4 PD 級使用最小 15.4 W 到最大 30 W

重要：級別中出現不符項目將會導致交握混亂，並重新啟動 SonicPoint 存取點。

確保每個 SonicPointACe/ACi/N2 保證可獲得 25 W。

需要特別注意，確保所有 PoE/PoE+ 交換器可為其每個 PoE 連接埠提供最少 25 W 的功率。例如，支援 SonicPointACe/ACi/N2 的連接埠需要 25 W 的功率。如果交換器不能保證每個連接埠 25 W，則必須新增外部冗餘電源。您將需要緊密配合 PoE/PoE+ 交換器的製造商，以確保為交換器提供充足的電量，從而使所有 PoE/PoE+ 裝置都能正常執行。

舊版和 SonicPoint N/Ni/Ne/NDR

舊版 SonicPoints 和 SonicPoint N/Ni/Ne/NDR 設定為 0 PD 級，它使用最小 0.44 W 到最大 12.95 W 功率。

為舊版 SonicPoints 和 SonicPoint N/Ni/Ne/NDR 提供 PoE 的任何交換器都必須完全符合 802.3af 的要求。不要在不符合要求的交換器上執行 SonicPoints，因為 SonicWall 不支援。

關閉 pre-802.3af-spec 偵測，否則可能會導致連接問題。

確保每個連接埠能保證獲得 10 W，並將 PoE 優先順序設定為「嚴重」或「高」。

存取點部署最佳做法

本節針對 SonicWall 的無線存取點的設計、安裝、部署和設定問題，提供了相關的 SonicWall 建議和最佳做法。文中提供的資訊可讓您在任意規模的環境中正確部署存取點。本節還包括成功操作和部署所需的相關外部問題。

重要：對本節中引用的任何供應商乙太網路交換器，SonicWall 不提供任何直接的技術支援。如果交換器製造商發佈可能會使此處所含的資訊無效的新模型或韌體，則材料也會相應的變更，而不會告知 SonicWall。

主題：

- 基礎結構中的交換器
- 接線注意事項
- 頻道
- 產生樹狀目錄
- VTP 和 GVRP 轉接通訊協定
- 連接埠彙總
- PortShield
- 廣播限制/廣播風暴
- 速度和雙工
- SonicPoint 自動佈建

基礎結構中的交換器

多數交換器都能用於您的 SonicWall 基礎結構中，但是可能需要某些自訂設定或編程才能確保達到最佳效能。

測試過的交換器

下列交換器已搭配 SonicWall 存取點進行測試，請留意針對各交換器提供的指引。

- 思科 - 大多數思科交換器均可正常執行，但在部分型號上發現一些問題。
  - SonicWall 不建議使用思科 Express 交換器產品線部署 SonicWall 存取點。
  - SonicWall 發現 SonicPointACe/ACi/N2 乙太網路與 Cisco 交換器 2960X-PS-I 間存在節能乙太網路相容問題。在與 SonicPoint 連接的連接埠上停用 EEE。請參閱下列思科文件瞭解詳情: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/software/15-0_2_EX1/int_hw_components/configuration_guide/b_int_152ex1_2960-xr_cg/b_int_152ex1_2960-xr_cg_chapter_01001.pdf。
- D-Link PoE 交換器 - 關閉所有專用廣播控制和風暴控制機制，因為它們會干擾存取點上的佈建和獲取機制。
- Dell - 為了在存取點連接埠上快速啟動，請務必設定 STP。
- Extreme - 為了在存取點連接埠上快速啟動，請務必設定 STP。
- Foundry - 為了在存取點連接埠上快速啟動，請務必設定 STP。

- HP ProCurve - 為了在存取點連接埠上快速啟動，請務必設定 STP。
- Netgear - SonicWall 不建議您使用 Netgear PoE 交換器部署 SonicWall 存取點。

交換器程式建議

以下章節提供一些交換器命令範例，可用於 SonicWall 基礎結構中的交換器上。詳情請參閱適用的供應商範例。

簡單的 Dell 交換器設定（每個介面）

- spanning-tree portfast
- no back-pressure
- no channel-group
- duplex half（註：僅當發現 FCS 錯誤時使用）
- speed 100
- no flowcontrol
- no gvrp enable
- no lldp enable
- mdix on
- mdix auto
- no port storm-control broadcast enable

簡單的 D-Link 交換器設定

D-Link PoE 交換器沒有命令列介面，因此需使用其 Web 介面。

附註：如果在您的環境中使用了多點傳送，檢查 D-Link 是否為推薦的韌體版本。

在將 SonicWall 存取點新增到交換器之前，請停用交換器上的產生樹狀目錄、廣播風暴控制、LLDP 和防護引擎，這些選項可能會影響存取點的成功佈建、設定和功能。

HP ProCurve 交換器命令範例 (每個介面)

- name ‘link to SonicPoint X’ (或 SonicWave X)
- no lacp
- no cdp
- power critical
- no power-pre-std-detect（註：全域命令）
- speed-duplex 100-half（註：僅當發現 FCS 錯誤時使用）
- spanning-tree *xx* admin-edge-port（註：使用連接埠號替換 *xx*）
- mdix-mode mdix

接線注意事項

與您的設施組織合作，施作時務必參考以下接線準則。

- 確保接線為 CAT5、CAT5e 或 CAT6 端到端。
- 對於 SonicPoint AC 裝置，由於 802.3af 和 802.3at 中的訊號限制，PoE 交換器和存取點之間的乙太網路纜線長度不應超過 100 米。
- 隨著纜線長度的增加，因應 PoE 電量損耗 (最高可達 16%) 加以規劃。纜線線越長，連接埠需要的電量越多。

頻道

SonicWall 存取點的預設設定為**自動頻道**。設定此項後，存取點在啟動時會進行掃描，檢查是否有其他無線裝置正在傳送，然後找出未使用的頻道並用於進行傳送。在規模較大的部署中，這個程序可能會引發問題，因此請考慮為每個存取點指派固定頻道。

提示：SonicPoints 的圖表及其 MAC 位址有助於避免重疊。推薦在平面佈置圖上標記 SonicPoints 的位置和 MAC 位址。

產生樹狀目錄

當乙太網路連接埠以電力啟用時，大多數交換器將預設啟用連接埠上的產生樹狀目錄通訊協定，以確定網路拓撲中是否存在迴圈。在偵測的 50-60 秒時間內，連接埠不會通過任何流量，已知此功能會導致 SonicWall 存取點發生問題。

如果您不需要產生樹狀目錄通訊協定，請在交換器上全域停用，或在連接 SonicWall 存取點的每個連接埠上將其停用。如果無法停用，請聯絡交換器製造商，確定他們是否允許*快速產生樹狀目錄偵測*，此功能可在很短的時間內執行產生樹狀目錄，因此不會出現連接問題。請參考簡單的 Dell 交換器設定（每個介面），瞭解關於此方法的規劃樣本。

VTP 和 GVRP 轉接通訊協定

在與存取點直接連接的連接埠上關閉這些轉接通訊協定，因為已知它們會導致 SonicPoint 出現問題，尤其是高端 Cisco Catalyst 系列交換器。

連接埠彙總

預設情況下，很多交換器都打開了連接埠彙總，這會導致很多問題。應在直接連接 SonicWall 存取點的連接埠上停用連接埠彙總功能。且應在連接 SonicWall 存取點的連接埠上關閉 PAGP/Fast EtherChannel/EtherChannel 和 LACP。

PortShield

通過將 SonicWall 存取點設定為 PortShield 群組的一個成員，對其進行連接埠屏蔽。如果將存取點設定成 X 系列交換器，必須將其隸屬的 PortShield 群組設定成專屬連結的連接埠。

廣播限制/廣播風暴

廣播限制/廣播風暴功能對某些交換器而言存在問題，尤其是 D-Link。如果可能，請停用每個連接埠上的此特性，否額，請全域停用。

速度和雙工

速度和雙工選項有時可能會造成 SonicWall 存取點出現問題。目前**自動交涉**是 SonicWall 存取點上唯一的速度和雙工選項。若要解決或避免這些問題，請考慮以下事項:

- 鎖定交換器上的速度和雙工並重新啟動存取點，有助於解決連線問題。
- 檢查連接埠是否出現錯誤，因為這是確定雙工問題存在與否的最佳方式 (連接埠的傳送量也會減少)。

SonicPoint 自動佈建

主題：

- 自動佈建 (SDP & SSPP)
- 啟用自動佈建

自動佈建 (SDP & SSPP)

SonicWall 發現通訊協定 (SDP) 是一個 2 層通訊協定，由 SonicPoints 和執行 SonicOS 的裝置使用。SDP 是通過以下訊息自動佈建 SonicPoint 裝置的基礎：

- **廣告** - 無對等裝置的 SonicPoints 將定期地在啟動時發佈宣告，或通過廣播進行廣告。廣告將包含接收 SonicOS 裝置所使用的資訊，用於確定 SonicPoint 的狀態。之後 SonicOS 裝置將報告所有對等 SonicPoints 的狀態，並根據需要進行設定。
- **發現** - SonicOS 裝置將定期傳送發現請求廣播，以得到來自 L2 連接的 SonicPoint 裝置的回應。
- **設定指令** - 自 SonicOS 裝置到特定 SonicPoint 的單點傳送資訊，用於建立設定的加密金鑰，並為進入設定模式設定參數。
- **設定確認** - 自 SonicPoint 到其對等 SonicOS 裝置的單點傳送訊息，用於確認設定指令。
- **保持連接** - 自 SonicPoint 到其對等 SonicOS 裝置的單點傳送訊息，用於驗證 SonicPoint 的狀態。

如果通過 SDP 交換，SonicOS 裝置確定 SonicPoint 需要佈建或設定更新（例如計算總和檢查碼不符合或當韌體更新可用時），設定指令將參與 3DES 加密的、基於可靠 TCP 的 SonicWall 簡單設定協定 (SSPP) 頻道。然後 SonicOS 裝置會將更新通過此頻道傳送給 SonicPoint，之後 SonicPoint 將使用更新的設定重新啟動。SonicPoint 將提供狀態資訊，在整個發現和佈建過程中可在 SonicOS 裝置上查看此資訊。

啟用自動佈建

可啟用 SonicPoint 自動佈建以自動佈建以下無線 SonicPoint/SonicWave 佈建設定檔：

- SonicPoint
- SonicPoint N

- SonicPointNDR
- SonicPoint AC
- SonicWave

無線 SonicPoint 的初始設定從 SonicPoint 設定檔佈建，它與無線 LAN 管理區域相連。設定無線 SonicPoint 後，設定檔將保留沒有與任何 SonicPoint 相關聯的離線設定範本。因此修改設定檔不會自動對 SonicPoint 進行重新佈建。

引入 SonicPoint 自動佈建之前，管理員需要手動刪除所有 SonicPoint，然後將新 SonicPoint 與設定檔同步，此步驟比較費時。為簡化設定並縮減管理開銷，SonicPoint 引入了自動佈建功能。

網路 > 區域 > 設定 > 無線設定對話方塊中提供了用於啟用對每個 SonicPoint 佈建設定檔進行自動佈建的核取方塊。預設情況下未勾選 SonicPoint 佈建設定檔的核取方塊，不啟用自動佈建。

如果勾選佈建設定檔的核取方塊並變更此設定檔，則連結至此設定檔的所有存取點都將重新佈建，並重新啟動為新的執行狀態。

SonicPoints 遠端 MAC 存取控制

重要：您不能在啟用 IEEE 802.11i EAP 的同時啟用遠端 MAC 位址存取控制選項。如果您嘗試在啟用 IEEE 802.11i EAP 的同時啟用遠端 MAC 位址存取控制選項，將顯示此錯誤訊息：

```
Remote MAC address access control can not be set
when IEEE 802.11i EAP is enabled.
```

附註：虛擬存取點也支援遠端 MAC 存取控制。請參閱遠端 MAC 位址存取控制設定。

您可以強制在遠端 Radius 伺服器實施基於 MAC 身分驗證原則的無線電無線存取控制。如需操作過程的資訊，請參閱遠端 MAC 位址存取控制設定。

存取點授權

SonicWave 存取點的授權與 SonicPoint 存取點不同。

主題：

- SonicWave 授權
- 授權狀態
- 手動授權更新
- 自動授權更新

SonicWave 授權

自 SonicOS 6.5.0 版開始，SonicWall 對每部 SonicWave 裝置個別要求額外授權。授權可用於從 SonicWall 防火牆管理 SonicWave。最初 SonicWave 裝置隨附 6 個月管理授權。

SonicWall 防火牆會從 SonicWall 授權管理員 (LM) 辨識授權狀態，並為基本 SonicWave 存取點啟用管理功能。授權到期前 30 天內，防火牆會發出通知，提醒系統管理員更新授權。

如果 SonicWave 授權到期而您沒有更新，SonicWall 防火牆就會執行「服務中斷」動作，藉此停用管理中的 SonicWave，SonicWave 存取點則會在存取點橋接流量時停止運作。透過 MySonicWall (MSM) 付費更新授權時，授權管理員會擴充 SonicWave 授權，以便讓防火牆擷取新授權並執行「服務復原」動作，藉此啟用 SonicWave 存取點。

附註：在隔離的環境中，防火牆可能無法存取授權管理員，管理員可將 SonicWave 授權金鑰組輸入防火牆中，以便修改 SonicWave 授權狀態。只要 SonicWave 具備有效授權，就可由防火牆管理，防火牆充當授權代理與授權管理員同步 SonicWave 授權。

只有當 SonicWave 存取點具備有效授權，SonicWave 才可作為一般存取點使用，否則會遭系統停用，直到擴充新的有效授權。

授權狀態

驗證 SonicWave 授權狀態的步驟如下:

1 導覽至**連線 | 存取點 > 基本設定**。

2 向下捲動至「SonicPoint/SonicWave 物件」表格，查看存取點的**狀態**。

SonicWave 存取點的狀態可能為以下其中一種:

- **正常運作**，以綠色顯示，表示存取點已獲得授權。
- **未授權**，以紅色顯示，表示存取點的授權已失效。
- **即將到期**，表示授權將在 30 天以內到期。

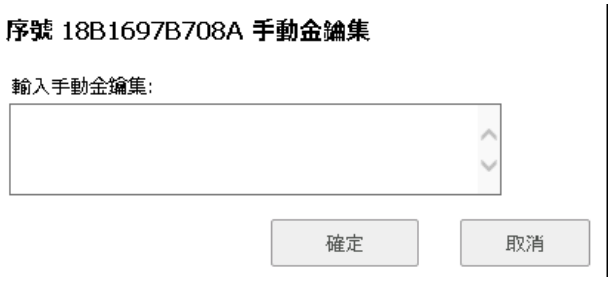
手動授權更新

當防火牆無法連線至授權管理員以更新 SonicWave 授權，仍可使用 GMS 或 SonicOS 管理介面來手動設定和更新授權。

1 在**管理**檢視上，導覽至**連線 | 存取點 > 基本設定**。

2 向下捲動至 **SonicPoint/SonicWave 物件**。

3 按一下需手動更新的 SonicWave 之「設定」欄中的開鎖圖示。



4 在金鑰欄位中輸入授權金鑰，然後按一下**確定**。

防火牆隨即會開始更新 SonicWave 存取點上的新授權金鑰。SonicWave 存取點會儲存更新的授權金鑰、開啟無線介面、還原流量橋接和開放主控台存取。

自動授權更新

防火牆會自動定期查詢 SonicWave 存取點。如果 SonicWave 存取點已更新，防火牆便會在對等清單中記錄新的授權到期時間，並更新 SonicWave 存取點上的新授權金鑰組，以及相應地控制其功能。

管理 SonicPoints 之前

在 SonicOS 管理介面中管理 SonicPoints 之前，您必須先完成以下操作：

1 檢查是否已將 SonicPoint 映像下載到您的 SonicWall 安全設備中。

2 設定存取點佈建設定檔。

3 設定無線區域。

4 將設定檔指派給無線區域。此步驟為可選步驟。如果您沒有為某區域指派預設的設定檔，則此區域中的 SonicPoint 將使用清單中的第一個設定檔。

5 為無線區域指派介面。

6 將存取點連接到無線區域中的介面。

7 測試存取點。

更新 SonicPoint 韌體

並非所有 SonicOS 韌體都包含 SonicPoint/SonicWave 韌體映像。查看**連線 | 存取點 > 基本設定**頁面頂端，找到**下載**連結。

如果您的 SonicWall 裝置具有網際網路連接，它將從連接 SonicPoint 裝置的防火牆伺服器下載正確的 SonicPoint 映像版本。

如果您的 SonicWall 設備*沒有*網際網路存取權限，或只能通過代理伺服器存取，則必須手動更新 SonicPoint 映像。

若要手動更新 SonicPoint 韌體：

1 從 http://www.mysonicwall.com 將 SonicPoint 映像下載到有網際網路存取權的本機系統。

您可以從以下其中一個位置下載 SonicPoint 映像：

- 在您可以下載 SonicOS 韌體的頁面上
- 在「下載中心」頁面上，選擇**類型**下拉功能表中的 **SonicPoint**。

2 將 SonicPoint 映像下載到您的 SonicWall 裝置可存取的本機 Web 伺服器上。

您可以變更 SonicPoint 映像的檔案名稱，但應保留副檔名的完整性（例如：`.bin.sig`）。

3 在 SonicOS 裝置的 SonicWall 使用者介面上，按一下瀏覽面板中的**系統 > 管理**。

4 在**系統 > 管理**頁面中**下載 URL** 區段的下面，選擇要下載的 SonicPoint 映像的相應核取方塊（可以下載多個映像）：

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

5 在欄位中，輸入您本機 Web 伺服器上的 SonicPoint 映像檔案的 URL。

附註：輸入 SonicPoint 映像檔案的 URL 時，請勿在欄位中包含 `http://`。

6 按一下**接受**。

重設 SonicPoint

SonicPoints 和 SonicWave 432 e/i 裝置後部臨近主控台連接埠的小孔中，有一個重設開關。使用拉直的迴紋針、牙籤或其他小而直的物品按下重設開關，便可隨時重設存取點。

附註：SonicWave 432o 沒有重設按鈕。

重設按鈕可將執行中的存取點模式設定重設為出廠預設值。而不會將設定重設為其他模式。根據存取點的執行模式，以及您按住重設按鈕的時間長短，存取點會以下列其中一種方式執行:

- 按住重設按鈕**超過三秒**但**不到八秒**，則在管理模式下執行的存取點會將管理模式設定重設為出廠預設值，並重新啟動存取點。
- 按住重設按鈕**超過八秒**，則在管理模式下執行的存取點會將管理模式設定重設為出廠預設值，並在安全模式下重新啟動存取點。
- 按住重設按鈕**超過三秒**，會將設定重設為出廠預設值，並重新啟動存取點。

存取點和 RADIUS 計費

附註：如需瞭解如何使用 RADIUS 驗證使用者，請參閱 RADIUS 伺服器設定。

RADIUS (遠端驗證撥入使用者服務) 是提供集中驗證、授權和計費的網路通訊協定。SonicOS 使用 RADIUS 通訊協定，從 NAS (網路存取伺服器，亦即存取點) 傳遞計費資訊到 Radius 計費伺服器。您可以善用帳戶資訊，在 RADIUS 計費伺服器端套用各種計費規則。帳戶資訊可根據每位使用者的工作階段期間或所傳輸的流量負載。

整體驗證、授權和計費程序如下：

1 使用者與連接到 SonicWall 防火牆的存取點建立關聯。

2 驗證是使用指定的方式執行。

3 啟用 IP 子網路/VLAN 指派。

4 存取點傳送 RADIUS 計費請求的開始訊息至計費伺服器。

5 視需要執行重新驗證。

6 根據重新驗證的結果，存取點傳送暫時計費更新至計費伺服器。

7 使用者與存取點中斷連接。

存取點傳送 RADIUS 計費請求的停止訊息至計費伺服器。

設定 Radius 計費伺服器

若要設定 Radius 計費伺服器：

1 將 Radius 用戶端項目新增到檔案 `/etc/freeradius/clients.conf`：

```
Client <IP address> {
     Secret = "<password>"
}
```

其中 <*IP address*> 是 RADIUS 伺服器的 IP 位址，而 <*password*> 是伺服器密碼。

附註：IP 位址是 RADIUS 伺服器所要連接的 SonicWall 閘道的 WAN IP。

2 新增使用者資訊到檔案 `/etc/freeradius/users`：

```
user_name Cleartext-Password := "<password>"
```

其中 *user_name* 是使用者的 ID，而 <*password*> 應以使用者的密碼取代。

3 若要啟動 freeradius，請執行命令：

```
sudo feeradius -X
```

(從命令行)。

14

存取點儀表板

在 SonicWave 和 SonicPoint AC 裝置上，**連線 | 存取點 > 儀表板**會使用圖表和圖形視覺化屬於基礎結構一部分的存取點相關資料。儀表板可顯示即時狀態和歷史狀態，以及每個用戶端的速率、作業系統類型和主機名稱；還能顯示 SonicWave 和 SonicPoint 裝置的狀態，並提供有助於監控和問題診斷的資訊。

儀表板可分為以下兩個區段:

- 功能限制
- 存取點快照
- 即時頻寬
- 用戶端報告
- 即時用戶端監控

功能限制

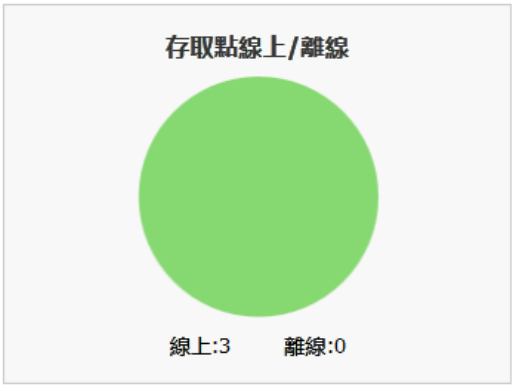
SonicWave 和 SonicPoint AC 裝置狀態顯示時，表示裝置是由 SonicWall 防火牆管理。防火牆和存取點都必須正常運作，否則將無法交換任何有效資料。SonicWave 存取點會保留七天的儀表板歷史資料，但是受限於記憶體限制，SonicPoint AC 裝置重新啟動後便會失去所有歷史資料。

存取點快照

連線 | 存取點 > 儀表板的**存取點快照**區段中會顯示兩個圖: **線上/離線存取點**和**用戶端關聯**。可在右上角指定這些圖的重新整理間隔。從下拉功能表中選擇分鐘數；選項範圍是 5 至 10 分鐘。

存取點連線/離線

線上/離線存取點圖顯示基礎結構中存取點的快速狀態。這項資料以圓形圖呈現；綠色表示在線上，紅色表示離線。圖表底部也會列出存取點的數量和狀態。



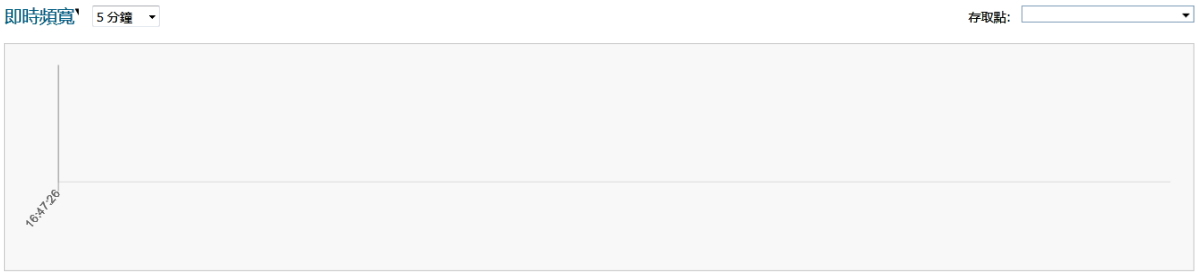
用戶端關聯

用戶端關聯圖顯示與設定中的每個存取點相關聯的用戶端數。在以下範例中，可以看到設定中的兩個存取點: 一個是 SonicPoint N2，一個是 SonicPoint N。拍攝此快照十，沒有用戶端正透過這兩個存取點存取網路。如果有使用者連接，系統會以條形圖形式顯示使用者數量。

即時頻寬

系統以圖形呈現所選存取點使用的頻寬，這個圖形會顯示在**連線 | 存取點 > 儀表板**的**即時頻寬**區段中。

附註：只有 SonicPoint ACe/ACi/N2 和 SonicWave 裝置支援**即時頻寬**功能。



若要選擇重新整理間隔，請依圖表標題從下拉功能表中選擇間隔期間。選項有: **1 分鐘**、**2 分鐘**、**5 分鐘**、**10 分鐘**和 **60 分鐘**。

若要變更顯示的存取點，請前往**存取點**下拉功能表並選擇其他裝置。圖表會針對該存取點更新資料。

用戶端報告

連線 | 存取點 > 儀表板的**用戶端報告**區段中會顯示兩個圖: **OS 類型**和**熱門用戶端**。

附註：只有 SonicPoint ACe/ACi/N2 和 SonicWave 裝置支援**即時頻寬**功能。

OS 類型

熱門用戶端

熱門用戶端圖表會顯示使用了最多頻寬的用戶端。前往**熱門**欄位，從下拉功能表中選擇一個數字，可顯示排名前 5、10、15 或 20 個頻寬耗用者。系統會顯示熱門使用者用於傳送和接收資料的值。

即時用戶端監控

系統以圖形呈現用戶端連接詳細資訊，這個圖形會顯示在**連線 | 存取點 > 儀表板**的**即時用戶端監控**區段中。這個圖提供透過存取點連接的每個使用者的詳細資訊。可查看 MAC 位址、主機名稱、OS 類型接收流量 (Rx) 和傳送流量 (Tx)。

15

存取點基本設定

佈建無線存取點最有效的方式，就是讓 SonicOS 防火牆自動偵測存取點，並使用其中一個預設設定檔。SonicOS 包含四個預設設定檔，SonicWall 存取點的每一代各一個: SonicWave 432e/432i/432o、SonicPointACe/ACi/N2、SonicPoint NDR/Ne/Ni 和 SonicPoint N。這些設定檔可照原樣使用，也可根據您的設定自訂。您也可根據 SonicWall 存取點類型建立新的設定檔。存取點設定檔的基本設定可在**管理**檢視上的**連線 | 存取點 > 基本設定**中進行設定。

主題：

- 佈建概述
- 建立/修改佈建設定檔
- 管理存取點

佈建概述

SonicPoint/SonicWave 佈建設定檔提供了一種可擴充的高度自動化方法，此方法可設定和佈建分布式無線體系結構中的多個存取點。SonicPoint/SonicWave 設定檔定義包括可在 SonicWall 存取點上設定的所有設定，例如針對 2.4GHz 和 5GHz 無線、SSID 和頻道操作的無線設定。

定義存取點設定檔後，即可將其套用到無線區域中。每個無線區域只能設定一個存取點設定檔。任何設定檔都可套用到任意數量的區域中。將存取點連接到區域時，系統會使用指派給此區域的設定檔自動對其進行佈建。

首次連接存取點並通電後，該存取點使用出廠預設值 (IP 位址: `192.168.1.20`，使用者名稱：`admin` 密碼：`password`）。初始化時，此裝置將嘗試查找與其對等的 SonicOS 裝置。SonicOS 裝置啟動時，也會透過 SonicWall 發現通訊協定搜尋存取點。如果存取點和對等 SonicOS 裝置搜尋到彼此，它們會透過加密交換進行通訊，使用指派給相關無線區域的設定檔來自動佈建新增的存取點裝置。

作為佈建過程的一部分，SonicOS 會指派唯一的名稱給發現的存取點，並記錄其 MAC 位址、介面以及發現時所在的區域。如果屬於設定檔的一部分，還可以為自動指派一個 IP 位址，讓存取點可以和 WPA-EAP 支援的驗證伺服器進行通訊。然後 SonicOS 將使用與相關區域關聯的設定檔設定 2.4GHz 和 5GHz 無線設定。

請注意，對設定檔所做的變更不會影響已佈建且處於正常運作狀態的裝置。可透過以下兩種方式變更正常運作的存取點設定:

- 透過手動設定變更

  需進行單一或少數變更時的最佳選擇，特別是在單獨存取點所需的設定，與指派給其區域的設定檔不同時。

- 透過取消佈建

  有效刪除存取點即可取消佈建裝置，此操作會清除其設定，並使該裝置進入自動重新讓其對等 SonicOS 裝置參與佈建過程的狀態。當某區域的設定檔已更新或變更，且此變更針對傳播而設定，則此技術將非常有用。可用於更新存取點上的韌體，或單純自動更新處於*受控*形式的多個存取點，而不是同時變更所有對等存取點因而導致服務中斷。

建立/修改佈建設定檔

在**管理**檢視上的**連線 | 存取點 > 基本設定**中，可設定和管理佈建設定檔以及個別物件。您可以新增任意數量的設定檔。

附註：*SonicPoint AC* 指的是 SonicPoint ACe/ACi/N2、*SonicPoint* 則代表所有 SonicPoint 裝置。*SonicWave* 指的是 SonicWave 432e/i/o。在執行 SonicOS 6.2.2 及更高版本、SonicOS 6.3 及更高版本或 SonicOS 6.4 及更高版本的裝置上支援 SonicPoint AC。SonicWave 裝置在 SonicOS 6.5 及更高版本上不受支援。

導覽至**連線 | 存取點 > 基本設定**頁面。四個預設 SonicOS 設定檔和您建立的所有自訂設定檔，都列在 **SonicPoint/SonicWave 佈建設定檔**區段底下。若要修改任何預設佈建設定檔，請按一下編輯圖示和並進行適當變更。

重要：由於為所有存取點類型建立或修改 **SonicPoint/SonicWave 佈建設定檔**的程序非常類似，本節將回顧為 SonicWave 裝置新增設定檔的步驟。文中將註明一般程序中的顯著差異，並在本節後半段詳細說明。

附註：無法刪除 SonicWall 提供的佈建設定檔，因此對應的**刪除**圖示以灰色顯示且無法使用。

「新增設定檔」選項提供多個視窗，將類似的設定歸類在一起。操作程序經過分組以配合這些視窗。

主題：

- 佈建設定檔的一般設定
- 佈建設定檔的無線 0/1 基本設定
- 佈建設定檔的無線 0/1 進階設定
- 感應器
- 3G/4G/LTE WWAN
- 特定產品的設定須知

存取新佈建設定檔的步驟如下:

1 在**管理**檢視上，導覽至**連線 | 存取點 > 基本設定**。

2 在 **SonicPoint/SonicWave 佈建設定檔**區段的**新增設定檔**欄位中，選擇要建立的設定檔類型。本範例中選擇了 SonicWave 設定檔。

附註：若要修改現有的設定檔，按一下要更新的設定檔對應的**編輯**圖示。

佈建設定檔的一般設定

設定一般群組選項的步驟如下:

1 設定 **SonicWave** 設定。

選項	操作
啟用 SonicWave	勾選即可啟用 SonicWave 存取點。預設為勾選。
保留設定	勾選即可保留自訂項目，直到下次重新啟動裝置。「編輯」按鈕已啟用，您可自訂要保留的設定 
啟用 RF 監控	勾選即可啟用無線 RF 威脅、即時監控和管理。
啟用 LED	勾選即可開啟 SonicWave LED。若未勾選 (預設)，LED 會維持關閉狀態。
啟用低功耗模式	勾選即可允許 SonicWave 在低功耗模式下運作，因為電源並非標準 802.3at PoE。
名稱首碼	輸入指定欄位中的名稱所用的首碼。
國家或地區代碼	從下拉功能表中選擇部署存取點所在國家或地區的國家或地區代碼。
EAPOL 版本	從下拉功能表中選擇 EAPoL 版本。請注意，V2 提供較優異的安全性。
頻段引導模式	從下拉功能表中選擇頻段切換模式。選項包括：**停用**、**自動**、**5GHz 優先**或**強制 5GHz**。

2 設定**虛擬存取點設定**的步驟如下:

a 若為**無線 0 虛擬存取點群組**，請從下拉功能表中選擇一個虛擬存取點物件群組。

b 若為**無線 1 虛擬存取點群組**，請從下拉功能表中選擇一個虛擬存取點物件群組。

3 向下捲動以查看其他「一般設定」。

4 設定動態 VLAN ID 指派。

> **附註：**若要啟用「動態 VLAN ID 指派」底下的選項，需在「系統安裝 | 網路」下建立 WLAN 區域和 VLAN 介面。

5 設定 **SSLVPN 通道設定**:

a 在指定欄位中輸入 **SSLVPN 伺服器**名稱或 IP 位址。

b 在指定欄位中輸入 SSLVPN 伺服器的**使用者名稱**。

c 輸入在 SSLVPN 伺服器上進行驗證所需的**密碼**。

d 在指定欄位中輸入**網域**名稱。

e 勾選方塊以啟用**自動重新連接**。

f 若要設定三層 SSLVPN，請連結至**連線 | SSL VPN > 用戶端設定**，並定義適當的設定。

6 設定管理員設定:

a 輸入網路管理員的使用者**名稱**。

b 輸入網路管理員的**密碼**。

佈建設定檔的無線 0/1 基本設定

不同類型存取點間無線 0 和無線 1 的基本設定雷同，只有些許差異，不同之處會在步驟中說明。

無線設定

若要設定無線 0/無線 1 基本設定：

1 選擇**無線 0 基本**或**無線 1 基本**選項。

2 選擇**啟用無線**，可自動在使用此設定檔佈建的所有存取點上啟用無線頻段。預設情況下已核取此選項。

3 從**啟用無線**下拉功能表中，為開啟無線的時間選擇排程或建立新排程。預設值為**始終開啟**。

4 從**模式**下拉功能表中選擇慣用的的無線模式。

無線模式選擇

無線 0 基本	無線 1 基本	定義
僅 5GHz 802.11n	僅 2.4GHz 802.11n	僅允許 802.11n 用戶端存取您的無線網路。802.11a/b/g 用戶端不能在此受限的無線模式下連接。
5GHz 802.11n/a 混合	2.4GHz 802.11n/g/b 混合模式 (SonicPoint AC/NDR 預設)	同時支援 802.11a 和 802.11n（無線 0）或 802.11b、802.11g 和 802.11n（無線 1）用戶端。如果無線網路包含多種類型的用戶端，請選擇此模式。
5GHz 802.11a 單一模式 (SonicPoint NDR 預設)		如果僅 802.11a 用戶端存取您的無線網路，則可選擇此模式。
	僅 2.4GHz 802.11g	如果您的無線網路僅包含 802.11g 用戶端，您可以選擇此模式，以提高 802.11g 的效能。如果想要避免 802.11b 用戶端關聯，也可以選擇此模式。
5GHz 802.11ac/n/a 混合模式 (SonicWave 和 SonicPoint AC 預設)		同時支援 802.11ac、802.11a 和 802.11n（無線 0）用戶端。如果無線網路包含多種類型的用戶端，請選擇此模式。
5GHz 802.11ac 單一模式		僅允許 802.11ac 用戶端存取您的無線網路。其他用戶端不能在此受限的無線模式下連接。

提示：僅適用於 802.11n 用戶端: 若想獲得最佳傳送量，SonicWall 建議使用 **802.11n 單一模式**無線模式。對多個無線用戶端身分驗證的相容性，可使用 **802.11n/b/g 混合模式**無線模式。

為使 802.11ac 用戶端達到最佳傳送量，SonicWall 建議使用 **802.11n 單一模式**無線模式。對多個無線用戶端身分驗證的相容性，可使用 **802.11ac/n/a 混合模式**無線模式。

附註：可用的 **802.11n 無線 0/1 設定**選項隨所選擇的模式而變化。如果為符合以下條件的模式設定無線設定：

- 支援 802.11n，則顯示下列選項：**無線波段**、**主要通道**、**輔助通道**、**啟用短期保護間隔**以及**啟用彙總**。
- 不支援 802.11n，則僅顯示**頻道**選項。

5 在 **SSID** 欄位中，為使用此設定檔的每個存取點的 SSID 輸入可識別的字串。這是將在可用無線連接的用戶端清單中出現的名稱。

提示：如果您組織中的所有 SonicPoint AC 或 NDR 共用同一個 SSID，則從一個 SonicPoint AC/NDR 漫遊到另一個時，使用者可更輕鬆地維護他們的無線連接。

6 從**無線頻段**下拉功能表中選擇一個無線頻段:

附註：**模式**設為 **5GHz 802.11a 單一模式**時，無法使用「無線頻段」選項。

- **自動** - 使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。若為某裝置選擇了此項，則**主要頻道**和**輔助頻道**都應設為**自動**。這是預設值。
- **標準 - 20MHz 頻道** - 指定無線 0 將僅使用標準 20MHz 頻道。
- **寬 - 40MHz 頻道** - 為**無線頻段**選擇了 **5GHz 802.11a 單一模式**以外的模式時，才可使用此選項。選擇此項便會指定無線 0 只使用寬 40 MHz 頻道。
- **寬 - 80 MHz 頻道** - 僅當為**無線頻段**選擇了 **5GHz 802.11ac/n/a 混合模式**或 **5GHz 802.11ac 單一模式**時，才可使用此選項，選擇此項便會指定無線 0 只使用寬 80 MHz 頻道。(**模式**設為 **5GHz 802.11n 單一模式**、**5GHz 802.11n/a 混合模式**或 **5GHz 802.11a 單一模式**時，無法使用此選項。)

7 根據選擇的「模式」和「無線頻段」選項，選擇一或多個頻道:

模式	無線頻段	頻道
僅 5GHz 802.11n	自動	**主要頻道**和**輔助頻道**欄位預設值為**自動**。
	標準 - 20 MHz 頻道	選擇**自動**或**標準頻道**下拉功能表中指定的其中一個無線頻道。
	寬 - 40 MHz 頻道	選擇**自動**或**主要頻道**中指定的其中一個無線頻道。**輔助頻道**自動定義為**自動**。
5GHz 802.11n/a 混合	自動	**主要頻道**和**輔助頻道**欄位預設值為**自動**。
	標準 - 20 MHz 頻道	選擇**自動**或**標準頻道**下拉功能表中指定的其中一個無線頻道。
	寬 - 40 MHz 頻道	選擇**自動**或**主要頻道**中指定的其中一個無線頻道。**輔助頻道**自動定義為**自動**。
5GHz 802.11a 單一模式	(無選項)	選擇**自動**或**頻道**下拉功能表中指定的其中一個無線頻道。

模式	無線頻段	頻道
5GHz 802.11ac/n/a 混合模式	自動	**頻道**欄位預設值為**自動**。
	標準 - 20 MHz 頻道	選擇**自動**或**頻道**下拉功能表中指定的其中一個無線頻道。
	寬 - 40 MHz 頻道	選擇**自動**或**頻道**欄位中指定的其中一個無線頻道。
	寬 - 80 MHz 頻道	選擇**自動**或**頻道**欄位中指定的其中一個無線頻道。
5GHz 802.11ac 單一模式	自動	**頻道**欄位預設值為**自動**。
	標準 - 20 MHz 頻道	選擇**自動**或**頻道**下拉功能表中指定的其中一個無線頻道。
	寬 - 40 MHz 頻道	選擇**自動**或**頻道**欄位中指定的其中一個無線頻道。
	寬 - 80 MHz 頻道	選擇**自動**或**頻道**欄位中指定的其中一個無線頻道。

8 勾選方塊以**啟用短期防護間隔**。可藉由縮短防護間隔來提高無線資料速率。確認無線用戶端可支援此功能以避免相容性問題。(**模式**設為 **5HGz 802.11ac 單一模式**時無法使用該此選項。)

9 勾選方塊以**啟用彙總**。可藉由在單次傳輸中傳送多個資料框架，來提高無線傳送量。確認無線用戶端可支援此功能以避免相容性問題。(**模式**設為 **5HGz 802.11ac 單一模式**時無法使用該此選項。)

無線安全

附註：SonicOS 介面可感知情境。如果在「一般」頁面上選擇了一個虛擬存取點群組，系統就會隱藏「無線安全」區段，您可跳過本節。

設定「無線安全」選項的步驟:

1 向下捲動至「無線安全」區段。

若要設定無線安全：

1 在**無線安全**區段中，從下拉功能表選擇**驗證類型**。

附註：可用的選項隨您所選擇的設定而不同。

2 參考下列表格決定其餘設定設定:

無線安全的 WEP 設定

	WEP 說明	
驗證類型	**WEP 金鑰模式**	**設定**
WEP (有線等效保密) 是 Wi-Fi 無線網路安全的標準。開向統使用和交換資訊以進行驗證，然後加密資料。共用金鑰會使用一組共用的密碼來進行驗證。		
WEP - 兩者皆是 (開放系統和共用金鑰)	**WEP 金鑰模式 = 無**	其餘設定將以灰色顯示且無法選擇。
	WEP 金鑰模式 = 64 位元、128 位元或 152 位元 位元數代表 WEP 金鑰的金鑰強度。	1 在**預設金鑰**欄位中選擇預設金鑰 (第一個嘗試的金鑰)。預設值為**金鑰 1**。 2 在**金鑰項目**欄位中，選擇金鑰為**英數字元**還是**十六進位 (0-9、A-F)**。 3 在金鑰 1、金鑰 2、金鑰 3 和金鑰 4 的欄位中，輸入傳輸資料時要使用的加密金鑰。
WEP - 開放系統		其餘設定將以灰色顯示且無法選擇。
WEP - 共用金鑰	**WEP 金鑰模式 = 64 位元、128 位元或 152 位元** 預設值為 **152 位元**。	1 在**預設金鑰**欄位中選擇預設金鑰 (第一個嘗試的金鑰)。預設值為**金鑰 1**。 2 在**金鑰項目**欄位中，選擇金鑰為**英數字元**還是**十六進位 (0-9、A-F)**。預設值為**十六進位**選項。 3 在金鑰 1、金鑰 2、金鑰 3 和金鑰 4 的欄位中，輸入傳輸資料時要使用的加密金鑰。

無線安全的 WPA2 設定

	說明
驗證類型	**設定**
WPA 和 WPA2 (Wi-Fi 安全存取) 是較新的通訊協定，用於保護無線裝置。選擇其中一個 **WPA2 - AUTO** 選項，允許裝置未啟用 WPA2 時使用 WPA 通訊協定。	
WPA2 - PSK	1 從下拉功能表中選擇**加密類型**。選項有 **AES** (預設)、**TKIP** 或**自動**。 2 設定**群組金鑰間隔** (單位為秒)。預設為 **86400**。 3 定義公開共用金鑰的**複雜密碼**。
WPA2 - EAP	1 從下拉功能表中選擇**加密類型**。選項有 **AES** (預設)、**TKIP** 或**自動**。 2 設定**群組金鑰間隔** (單位為秒)。預設為 **86400**。

無線安全的 WPA2 設定

	說明
驗證類型	**設定**
WPA2 - AUTO - PSK	1 從下拉功能表中選擇**加密類型**。選項有 **AES** (預設)、**TKIP** 或**自動**。 2 設定**群組金鑰間隔** (單位為秒)。預設為 **86400**。 3 定義公開共用金鑰的**複雜密碼**。
WPA2 - AUTO - EAP	1 從下拉功能表中選擇**加密類型**。選項有 **AES** (預設)、**TKIP** 或**自動**。 2 設定**群組金鑰間隔** (單位為秒)。預設為 **86400**。

RADIUS 伺服器設定

若在**無線安全**區段中選擇 **WPA2 - EAP** 或 **WPA2 - AUTO - EAP**，就會出現 **Radius 伺服器設定**區段。此功能使用 RADIUS 伺服器來產生驗證金鑰。必須為伺服器設定此功能，才能與 SonicWall 裝置進行通訊。

若要設定 Radius 伺服器設定：

1 按一下**設定**按鈕。顯示 **Radius 伺服器設定**對話方塊。此對話上顯示的選項取決於 SonicPoint 的類型。

SonicPointNDR 或 SonicPoint N

SonicPointACe/ACi/N2 - SonicWave

2 在 **Radius 伺服器重試**欄位中輸入從 1 到 10 的次數，是防火牆在嘗試故障轉移到其他 Radius 伺服器之前嘗試的次數。

3 在**重試間隔（秒）**欄位中輸入兩次重試之間等待的時間，從 0 到 60 秒。預設數字為 **0**，即不需要等待。

4 依照下表定義 **Radius 伺服器設定**:

RADIUS 驗證伺服器設定

選項	說明
伺服器 1 IP	RADIUS 驗證伺服器的名稱/位置
伺服器 1 連接埠	RADIUS 驗證伺服器通過其與用戶端和網路裝置進行通訊的連接埠。預設連接埠號是 **1812**。

RADIUS 驗證伺服器設定

選項	說明
伺服器 1 機密	RADIUS 驗證伺服器的密碼。
伺服器 2	備份 RADIUS 驗證伺服器的名稱/位置。
伺服器 2 連接埠	備份 RADIUS 驗證伺服器通過其與用戶端和網路裝置進行通訊的連接埠。預設連接埠號是 **1812**。
伺服器 2 機密	備份 RADIUS 驗證伺服器的密碼。

5 若使用 Radius 伺服器來追蹤使用量以進行計費，請設定 Radius 計費伺服器:

RADIUS 計費伺服器設定

選項	說明
伺服器 1 IP	RADIUS 計費伺服器的名稱/位置
伺服器 1 連接埠	RADIUS 驗證伺服器通過其與用戶端和網路裝置進行通訊的連接埠。
伺服器 1 機密	RADIUS 驗證伺服器的密碼。
伺服器 2	備份 RADIUS 驗證伺服器的名稱/位置。
伺服器 2 連接埠	備份 RADIUS 驗證伺服器通過其與用戶端和網路裝置進行通訊的連接埠。
伺服器 2 機密	備份 RADIUS 驗證伺服器的密碼。

6 若要傳送 NAS 識別項到 RADIUS 伺服器，請從 **NAS 識別項類型**下拉功能表中選擇類型

- **不包含** (預設)
- **SonicPoint 的名稱**
- **SonicPoint 的 MAC 位址**

7 若要傳送 NAS IP 位址到 RADIUS 伺服器，請在 **NAS IP 位址**欄位中輸入位址。

8 按一下**確定**。

強制啟用 ACL

每個存取點均可支援存取控制清單 (ACL)，以提供更高效的驗證控制。ACL 功能可配合 SonicOS 上目前可用的無線 MAC 篩選條件清單使用。使用強制啟用 ACL 功能，使用者可以啟用或停用 MAC 篩選條件清單、設定允許清單和設定拒絕清單。

啟用 MAC 篩選條件清單的步驟如下:

1 勾選方塊以**啟用 MAC 篩選條件清單**。MAC 篩選條件清單已啟用時，其他設定也會啟用，方便您進行設定。

2 在**允許清單**中，從下拉清單選擇一個選項。此選項用於識別您允許擁有存取權的 MAC 位址。

若想建立新的位址物件群組，其中包含您希望賦予存取權的位址，請選擇**建立 MAC 位址物件群組**。請參考 *SonicWall SonicOS 6.5 原則*瞭解操作方式。

3 在**拒絕清單**中，從下拉清單選擇一個選項。此選項用於識別您拒絕提供存取權的 MAC 位址。

若想建立新的位址物件群組，其中包含您不希望賦予存取權的位址，請選擇**建立 MAC 位址物件群組**。請參考 *SonicWall SonicOS 6.5 原則*瞭解操作方式。

4 勾選方塊以**啟用 MIC 失敗 ACL 黑名單清單**。

5 依據每分鐘次數設定 **MIC 失敗頻率閾值**。預設為 **3**。

遠端 MAC 位址存取控制設定

此選項用於強制在 RADIUS 伺服器上根據基於 MAC 的驗證實施無線存取控制。

允許無線存取控制的步驟如下:

1 勾選方塊以**啟用遠端 MAC 存取控制**。

2 按一下**設定**。

3 若尚未設定，請如 RADIUS 伺服器設定中所述設定 RADIUS 伺服器。

4 按一下確定。

佈建設定檔的無線 0/1 進階設定

這些設定會影響無線頻段的運作。SonicPoint/SonicWave 內建有兩個單獨的無線，因此它可以同時在這兩個波段上傳送和接收資料。

無線 1 進階標籤有和**無線 0 進階**標籤相同的選項，外加一些其他選項。不同存取點型號間的標籤雷同，請依照此程序為兩者進行設定。不同之處會在必要步驟中說明。

若要設定「無線 0/無線 1 進階」設定：

1 視需要按一下**無線 0 進階**或**無線 1 進階**。

2 如果要**隱藏信標中的 SSID**，請勾選方塊。 此選項可讓 SSID 傳送 null SSID 信標，代替通告無線 SSID 名稱。傳送無 SSID 信標會強制無線用戶端知道 SSID 才進行連接。預設情況下取消勾選此選項。

3 從**排程 IDS 掃描**下拉功能表中，為 IDS（入侵偵測服務）掃描選擇時間表。

選擇對無線網路的需求較低的時間，以最小化由於已丟棄的無線連接所造成的不便。可以通過選擇**建立新排程**建立您自己的排程，或選擇**已停用**來停用此功能，預設為停用。

> **附註：**IDS 提供多種入侵偵測功能來防護網路免受無線威脅。此功能可偵測針對 WLAN 基礎設施（由授權的存取點、射頻介質和有線網路組成）的攻擊。將授權的或有效的存取點定義為屬於 WLAN 基礎設施的存取點。存取點是 SonicPoint、SonicWave 或供應商存取點。

4 從**資料速率**下拉功能表 - 選擇傳送和接收資料的速度。**最佳**（預設）選項可自動選擇在有干擾和其他因素的情況下您的區域中的最佳可用速率。

5 從**傳送功率**下拉功能表中，選擇傳送功率。傳送功率會影響 SonicPoint 的範圍。

- **全功率**（預設）
- **半功率 (-3 dB)**
- **四分之一功率 (-6 dB)**
- **八分之一功率 (-9 dB)**
- **最小**

6 若要設定 SonicPoint NDR: 請從**天線分極**下拉功能表中選擇**最佳** (預設)。

天線分極設定可決定存取點使用哪個天線傳送和接收資料。選擇**最佳**選項後，存取點將自動選擇訊號最強且最清晰的天線。

7 在**訊號間隔（毫秒）**欄位中，輸入傳送無線 SSID 信標之間間隔的毫秒數。間隔下限為 100 毫秒 (預設)；間隔上限為 1000 毫秒。

8 在 **DTIM 間隔**欄位中，輸入以毫秒為單位的 DTIM 間隔。框架數下限為 1 (預設)；上限為 255。

對於傳入多點傳送封包的 802.11 省電模式用戶端，**DTIM 間隔**指定在傳送 DTIM（傳送指示訊息）之前等待的信標框架數。

9 若要設定 SonicPointNDR: 在**分段閾值 (位元組數)** 欄位中，輸入想要網路允許的分段資料位元組數。

分段閾值可限制最大框架大小。限制框架的大小可縮短傳送框架所需的時間，因此降低損壞此框架（以更多的資料開銷為代價）的可能性。分割無線框架，以增加在有射頻干擾或無線覆寫不佳的區域內的可靠性和傳送量。較低的閾值數會產生較多的片段。下限為 256 位元組，上限為 2346 位元組 (預設)。

10 在 **RTS 閾值（位元組數）**欄位中，為封包大小輸入閾值（以位元組計），請求傳送 (RTS) 將在封包傳送前以此閾值傳送。

傳送一個 RTS 可確保當多個用戶端處於同一個存取點的範圍（但彼此不再對方範圍內）的情況下不會出現無線衝突。下限閾值為 256 位元組，上限為 2346 位元組 (預設)。

11 在**最大用戶端關聯數**欄位中，輸入希望這個無線上使用此設定檔的每個存取點一次可支援的用戶端數量上限。最小用戶端數為 1，最大為 128，預設為 **32**。

12 在**工作站非使用中狀態逾時 (秒)** 欄位中，輸入存取點使無線用戶端逾時之前的無線用戶端非使用中狀態最長時間。最小時長為 60 秒，最大時長為 36000 秒，預設值為 **300** 秒。

13 若要設定**無線 1 進階**標籤設定，請定義該視窗專屬的下列設定；否則跳至下個步驟。

選項	設定
初始長度	從下拉功能表中選擇: • **長**（預設） • **短**
保護模式	從下拉功能表中選擇: • **無** • **始終** • **自動**
保護速率	從下拉功能表中選擇: • **1 Mbps**（預設） • **2 Mbps** • **5 Mbps** • **11 Mbps**
保護類型	從下拉功能表中選擇: • **僅 CTS** (預設) • **RTS-CTS**
啟用短插槽時間	選擇以允許用戶端更快速中斷關聯和重新建立關聯。指定此選項，可通過縮短存取點轉送封包給 LAN 之前的等待時間來增加 802.11n/g 無線頻段的傳送量。
請勿允許 802.11b 用戶端連接	如果正在使用 Turbo G 模式且因此不允許 802.11b 用戶端連接，請選擇此項。指定此選項可將無線連接限制到僅 802.11g 和 802.11n 用戶端。

14 從 **WMM（Wi-Fi 多媒體）**下拉功能表，選擇 WMM 設定檔是否與此設定檔關聯：

- **已停用** (預設)
- **建立新的 WMM 設定檔**。如需更多詳細資訊，請參閱設定 Wi-Fi 多媒體。
- 先前設定的 WMM 設定檔

15 勾選方塊以**啟用 WDS AP**。可利用多個存取點來擴充無線網路，不受到需要有線架構與其連結的傳統要求限制。

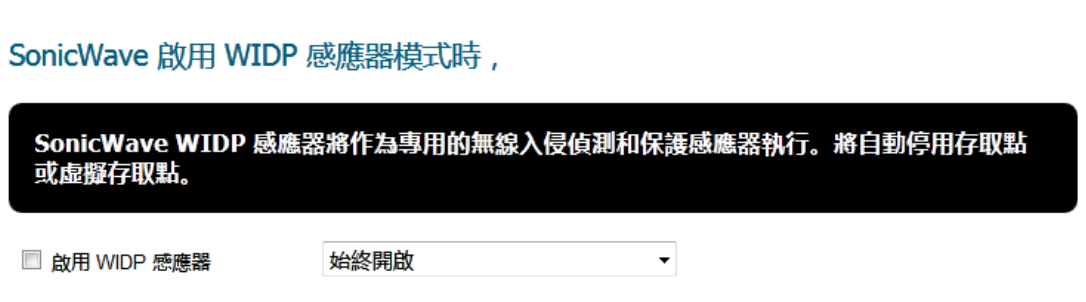
16 選擇**啟用綠色存取點**以允許存取點無線進入睡眠模式。這樣在沒有用戶端以使用中狀態連接時可節省電量。當有任何用戶端嘗試連接到存取點，它會立即進入全功率模式。可以在無線 0 (5GHz) 和無線 1 (2.4GHz) 上單獨設定綠色存取點。

17 在**綠色存取點逾時**欄位中輸入過渡時間 (以秒為單位)，這是存取點在無使用中連接時進入睡眠模式之前等待的時間。過渡時間從 20 秒到 65535 秒，預設值為 **20** 秒。

18 若設定 SonicWave 裝置，勾選方塊以**啟用空中傳輸時間公平性**。

此功能預設為停用。若啟用此功能，系統會將可使用 5 GHz 頻段的裝置之流量切換至該頻段，因為這個頻段的干擾和流量通常較少。如果 2.4 GHz 頻段的訊號強度或訊號條件較優異，則會將流量切換至此頻段。這麼做的用意在於最有效運用兩個頻段。

感應器



在**感應器**視窗中，啟用或停用無線入侵偵測和防禦 (WIDP) 模式。

重要：如果選擇此選項，系統將自動停用存取點或虛擬存取點功能。

若要設定感應器標籤：

1 選取 **Enable WIDF sensor（啟用 WIDF 感應器）**即可讓存取點作為專用 WIDP 感應器來執行。預設情況下未勾選此選項。

2 從下拉功能表中選擇存取點作為 WIDP 感應器執行的時間，或選擇**建立新排程...** 以指定不同的時間。預設值為**始終開啟**。

3G/4G/LTE WWAN

附註：如果沒有要設定數據機，可以跳過本節。

此功能為使用 SonicWave 裝置等無線存取點的防火牆裝置提供另一種無線 WAN 解決方案。您可將 USB 數據機裝置插入 SonicWave，它會執行撥號作業並連接至網際網路。成功連接後，SonicWave 可作為防火牆的 WWAN 裝置並提供 WAN 存取。

初次設定數據機時，可使用精靈來針對此選項運用自動發現功能。

主題：

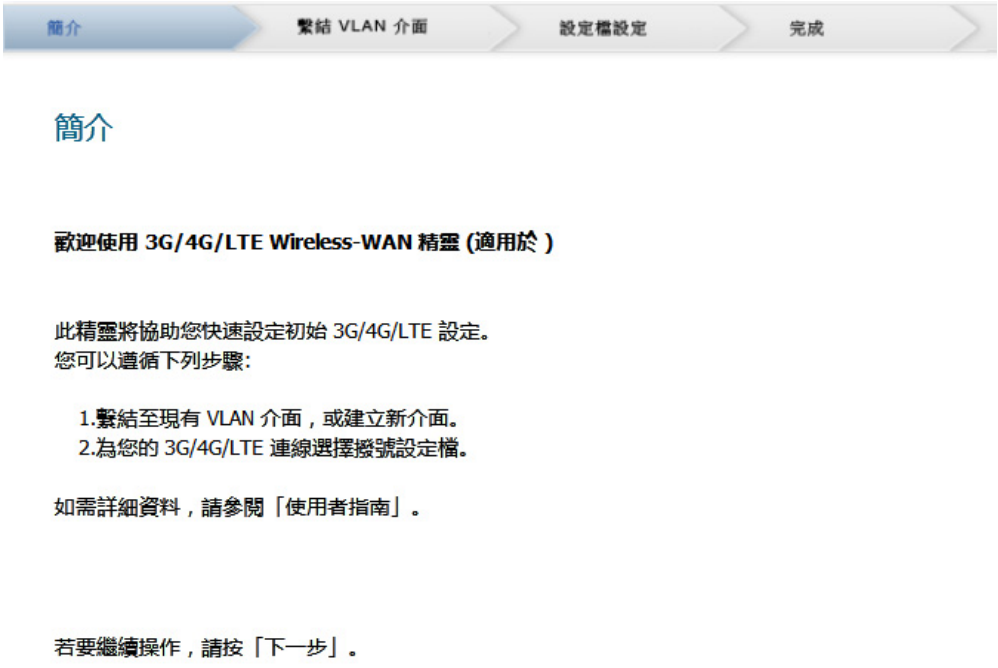
- 使用 3G/4G/LTE WWAN 精靈
- 手動設定 3G/4G/LTE WWAN 設定檔

使用 3G/4G/LTE WWAN 精靈

使用精靈來設定數據機的步驟如下:

1 按一下 **3G/4GLTE WWAN**。

2 捲動至底部，按一下 **3G/4G/LTE 精靈**。



3 按下一步。

4 從下拉功能表中選擇一個 **VLAN 介面**，或勾選方塊以**建立新的 VLAN 介面**。

若您選擇建立新的 VLAN 介面，其餘欄位將開放使用。提供請求的資料。

附註：若將 **IP 指派**設為 **DHCP**，「IP 位址」、「子網路遮罩」和「預設閘道」欄位均會隱藏。

5 按下一步。

6 在**國家或地區**欄位中選擇部署存取點所在的國家或地區。

7 從下拉功能表中選擇**服務供應商**。

8 從下拉功能表中選擇**計劃類型**。根據選擇的項目，系統會自動填入其他欄位會。

9 如有需要，可在適當欄位新增**使用者名稱**和**使用者密碼**。

10 按**下一步**。

11 再按一次**下一步**以套用設定。

手動設定 3G/4G/LTE WWAN 設定檔

您可運用下列程序手動設定 3G/4G/LTE WWAN 設定檔或手動進行變更。

手動將數據機設定為 WWAN 的步驟如下:

1 按一下 **3G/4GLTE WWAN**。

2 勾選方塊以啟用 3G/4G/LTE 數據機。

3 從**已繫結至 WAN VLAN 介面**下拉功能表中選擇一個 VLAN 介面。

如果下拉功能表中沒有列出任何介面，您需自行定義一個介面。請參閱 *SonicWall SonicOS 6.5 系統安裝*中的「網路 > 介面」章節。

附註：建立 VLAN 介面時，將區域設定為 WAN 區域，並將父級介面設為存取點連接的實體介面。

若使用 3G USB 數據機，將「IP 指派」設為「固定」，並為其指派私人 IP 位址。閘道和 DNS 伺服器欄位保持空白。

若使用 4G 和 QMI 數據機，將「IP 指派」設為「DHCP」。

4 在**連接設定檔**區段中，勾選方塊以**啟用連接設定檔**。

附註：某些傳統的 3G/4G 數據機需要撥號的連線設定檔。

5 在**國家或地區**欄位中選擇部署存取點所在的國家或地區。

6 從下拉功能表中選擇**服務供應商**。

7 從下拉功能表中選擇**計劃類型**。根據選擇的項目，系統會自動填入其他欄位。

8 如有需要，可在適當欄位新增**使用者名稱**和**使用者密碼**。

「設定檔」頁面上的所有設定都完成後，請務必按一下**確定**。

特定產品的設定須知

SonicPoint 的設定過程稍有不同，具體取決於您設定的是單無線 (SonicPoint N) 還是雙無線 (SonicPoint AC 和 SonicPoint NDR) 裝置。

管理存取點

主題：

- 同步存取點
- 刪除存取點設定檔
- 刪除 SonicPoint/SonicWave 物件
- 重新啟動 SonicPoint/SonicWave 物件
- 修改 SonicPoint/SonicWave 物件

同步存取點

按一下**連線 | 存取點> 基本設定**頁面頂端的**同步存取點**，從 SonicWall 裝置向 WLAN 區域發出查詢。所有連接的存取點都會向裝置報告它們的目前設定和統計資料。SonicOS 還會嘗試查找是否有未註冊防火牆的任何新連接存取點。

附註：此按鈕可用於輪詢存取點，但不向它們推送設定。

刪除存取點設定檔

附註：您無法刪除預先定義的設定檔，只能刪除您新增的設定檔。

在**連線 | 存取點> 基本設定**頁面上，您可從 **SonicPoint/SonicWave 佈建設定檔**區段中刪除個別設定檔或設定檔群組:

- 刪除單一存取點設定檔的步驟如下:
    1) 按一下其**刪除**按鈕。將顯示確認訊息。
    2) 按一下**確定**。
- 刪除一或多個存取點設定檔的步驟如下:
    1) 勾選要刪除的存取點名稱旁邊的核取方塊。**刪除**按鈕隨即啟用。
    2) 按一下**刪除**按鈕。將顯示確認訊息。
    3) 按一下**確定**。
- 刪除所有設定檔的步驟如下:
    1) 勾選列標頭中 **#** 旁邊的核取方塊。**全部刪除**按鈕隨即啟用。
    2) 按一下**全部刪除**按鈕。將顯示確認訊息
    3) 按一下**確定**。

刪除 SonicPoint/SonicWave 物件

在**連線 | 存取點> 基本設定**頁面上，您可從 **SonicPoint/SonicWave 物件**區段中刪除個別存取點或存取點群組:

- 刪除單一物件的步驟如下:
  a 按一下該物件的**刪除**按鈕。將顯示確認訊息。
  b 按一下**確定**。
- 刪除一或多個物件的步驟如下:
  a 勾選要刪除的物件旁邊的核取方塊。**刪除**按鈕隨即啟用。
  b 按一下**刪除**按鈕。將顯示確認訊息。
  c 按一下**確定**。
- 刪除所有物件的步驟如下:
  a 勾選列標頭中 **#** 旁邊的核取方塊。**全部刪除**按鈕隨即啟用。
  b 按一下**全部刪除**按鈕。將顯示確認訊息。
  c 按一下**確定**。

重新啟動 SonicPoint/SonicWave 物件

在**連線 | 存取點> 基本設定**頁面上，您可從 **SonicPoint/SonicWave 物件**區段中重新啟動個別存取點或存取點群組:

- 重新啟動單一物件的步驟如下:
  a 勾選要重新啟動的存取點名稱旁邊的核取方塊。**重新啟動**圖示隨即啟用。
  b 按一下**重新啟動**按鈕。將顯示確認訊息。
  c 選擇重新啟動類型：
    - **重新啟動**（預設）- 重新啟動到已設定的設定檔設定。
    - **重新啟動到出廠模式** - 重新啟動到出廠預設值。

△ 注意：**選擇此選項會用出廠預設值覆寫存取點設定檔。**

  d 按一下**確定**。
- 重新啟動所有物件的步驟如下:
  a 按一下**重新啟動全部**按鈕。
  b 選擇以下一項：
    - **重新啟動**（預設）- 重新啟動到已設定的設定檔設定。
    - **重新啟動到出廠模式**

△ 注意：**選擇此選項會用出廠預設值覆寫存取點設定檔。**

  c 按一下**確定**以重新啟動存取點，或按**取消**以關閉視窗，不重新啟動。

修改 SonicPoint/SonicWave 物件

可從**連線 | 存取點 > 基本設定**修改存取點物件。

1 按一下要修改的物件對應的**編輯**圖示。

2 變更要修改的設定。

3 按一下**確定**儲存新設定。

附註：網路裝置執行自動發現程序時，系統會自動新增新的 SonicPoint/SonicWave 存取點。

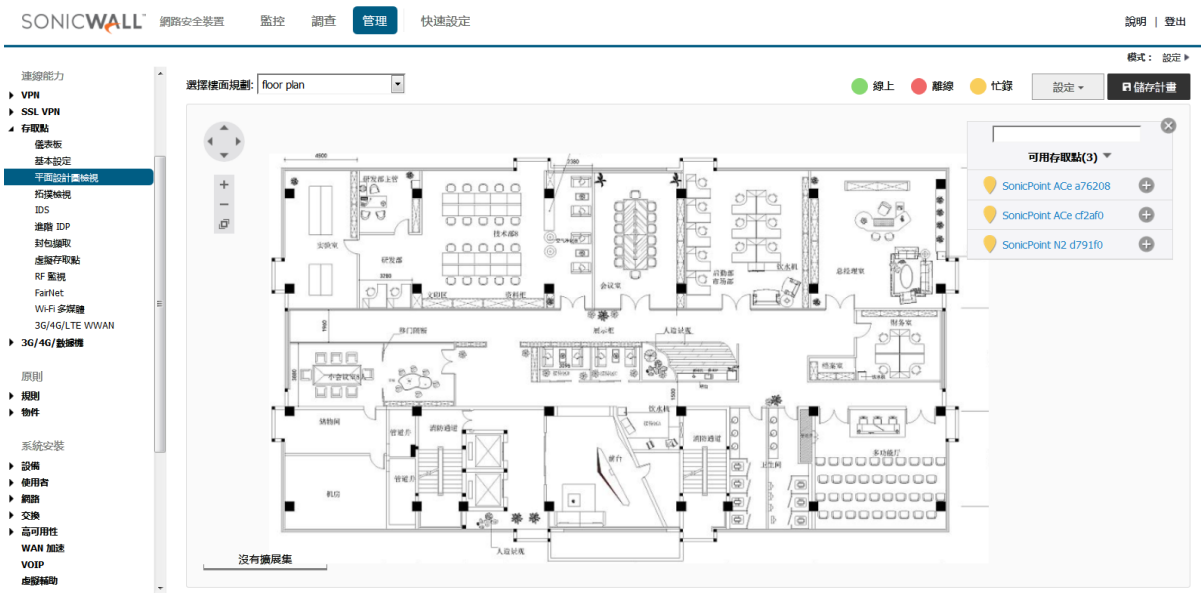
16

存取點樓面規劃

在**管理**檢視中的**連線 | 存取點 > 樓面規劃檢視**頁面上，SonicOS 使用者介面提供更直觀的方法，便於管理大量 SonicWave 和 SonicPoint 裝置。您也可追蹤實體位置和即時狀態。

樓面規劃檢視功能是 SonicOS 中現有無線存取點管理套件的附加元件，可針對您的實際無線部署環境提供即時情況，且可提升預估新部署無線覆蓋範圍的能力。FPMV 也提供單點式主控台，可從整合的操作功能表查看存取點統計資料、監控存取點即時狀態、設定存取點、移除存取點，甚至可顯示存取點 RF 覆蓋範圍。

下圖為典型樓面規劃檢視範例。



主題：

- 管理樓面規劃
- 管理存取點

管理樓面規劃

樓面規劃檢視功能提供多種檢視、新增和編輯樓面規劃的方式，本節將說明最常用的方式。

主題：

- 選擇樓面規劃
- 建立樓面規劃

- 編輯樓面規劃
- 設定測量比例

選擇樓面規劃

在**管理**檢視中選擇**連線 | 存取點 > 樓面規劃檢視**頁面時，顯示中的樓面規劃標題會出現在左上角的**選擇樓面規劃**欄位中。若要查看不同的樓面規劃，請從**選擇樓面規劃**下拉功能表中選擇其他樓面規劃。

選擇樓面規劃的另一種方式:

1 按一下**設定**。

2 選擇「樓面規劃清單」。

3 按兩下要顯示的規劃名稱。

建立樓面規劃

建立樓面規劃的步驟如下:

1 導覽至**連線 | 存取點 > 樓面規劃檢視**。

2 按一下**設定**。

3 選擇**建立樓面規劃**。

4 填入用於說明規劃的欄位。

5 按一下**接受**。

編輯樓面規劃

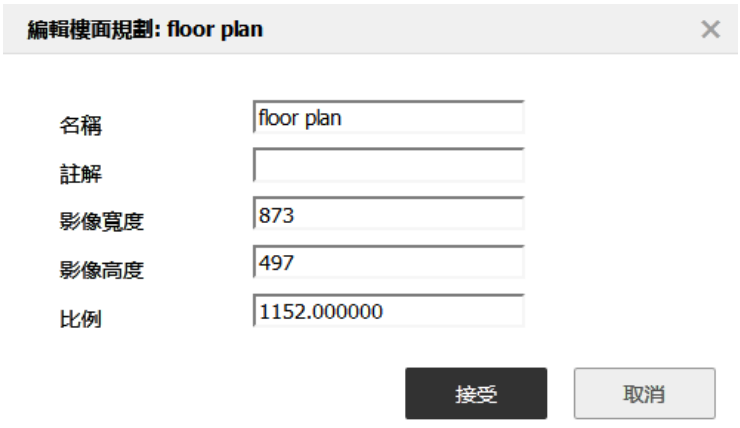
編輯樓面規劃的方式有很多種，以下為最常用的方式。

編輯顯示中樓面規劃的步驟如下:

1 導覽至**連線 | 存取點 > 樓面規劃檢視**。

2 按一下**設定**。

3 選擇**編輯目前的樓面規劃**。



4 視需要變更欄位。

5 按一下**接受**。

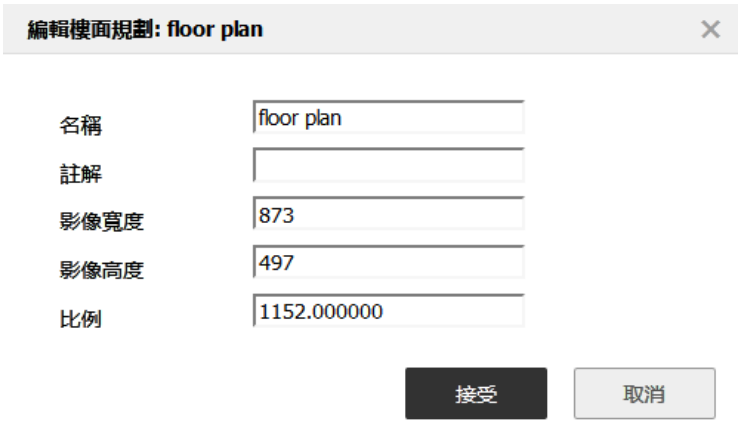
編輯清單中規劃的步驟如下:

1 導覽至**連線 | 存取點 > 樓面規劃檢視**。

2 按一下**設定**。

3 選擇**樓面規劃清單**。

4 按一下**編輯**圖示。



5 視需要變更欄位。

6 按一下**接受**。

設定測量比例

必須設定測量比例，才能顯示實際距離 (英尺) 關係和製成樓面規劃圖所用的像素。您可使用這個值來協助估算 RF 覆蓋範圍。

設定測量比例的步驟如下:

1 導覽至**連線 | 存取點 > 樓面規劃檢視**。

2 按一下**設定**。

3 選擇**測量比例**。視窗上會顯示「行長度」欄位。

4 輸入每英尺像素數。

5 按一下**結束繪圖**。

管理存取點

以色彩顯示存取點狀態

可在**樓面規劃檢視**中管理個別存取點。

主題：

- 可用存取點
- 已新增存取點
- 移除存取點
- 匯出影像

可用存取點

可供部署的存取點會顯示在**可用存取點**清單中。這個清單一般會顯示在右上角，不過可以拖放至任意位置。也可按一下角落的 **X** 關閉清單。若要顯示清單，按一下**設定 > 可用存取點**即可。

您可將這些存取點拖放至樓面規劃，並放置在任意位置。完成時請務必**儲存規劃**。

附註：已新增至樓面規劃的存取點不會顯示在這個面板中。

已新增存取點

已部署的存取點會顯示在**已新增存取點**清單中。這個清單一般會顯示在左上角，不過可以拖放至任意位置。也可按一下角落的 **X** 關閉清單。若要顯示清單，按一下**設定 > 已新增存取點**即可。

您可將這些存取點拖放至樓面規劃上的其他位置，也可從規劃中刪除。完成時請務必**儲存規劃**。

附註：已新增至樓面規劃的存取點不會顯示在這個面板中。

移除存取點

移除所有存取點的步驟如下:

1. 導覽至**連線 | 存取點 > 樓面規劃檢視**。
2. 按一下**設定**。
3. 選擇**移除所有新增的存取點**。
4. 按一下**儲存規劃**。

匯出影像

匯出樓面規劃影像的步驟如下:

1 導覽至**連線 | 存取點 > 樓面規劃檢視**。

2 按一下**設定**。

3 選擇**匯出為影像**。

4 然後選擇要儲存為 **JPG** 還是 **PNG** 格式。

5 將檔案儲存至之後可存取的位置。

操作功能表

您可使用滑鼠來啟用各種操作功能表:

- 將滑鼠停在樓面規劃上使用中的存取點時，會出現一個快顯視窗，顯示包括 ID、狀態、用戶端數和執行時間在內的存取點資訊。
- 按一下存取點即可顯示 RF 覆蓋範圍。
- 按兩下存取點便會出現「即時監控」視窗。
- 對存取點按一下右鍵，即可顯示操作功能表，功能表中包含編輯、顯示統計資料、監控狀態等選項。

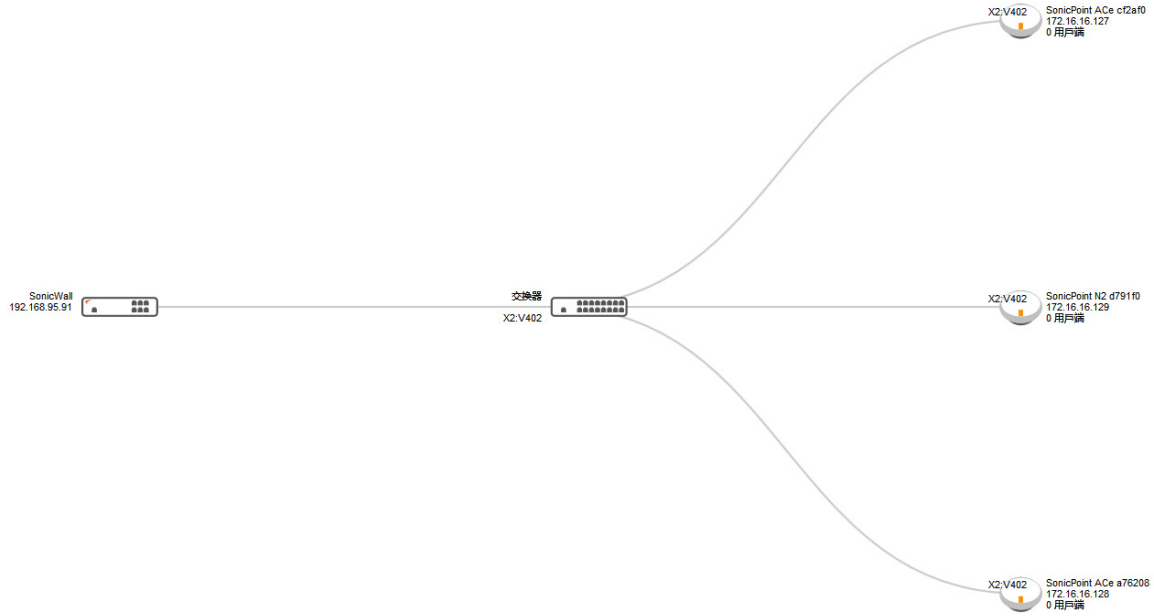
17

存取點拓撲檢視

在**管理**檢視中的**連線 | 存取點 > 拓撲檢視**頁面上，您可利用新的「拓撲檢視」功能管理存取點。拓撲檢視會顯示從 SonicWall 防火牆到無線存取點的網路拓撲，可監控存取點即時狀態，且操作功能表也提供設定選項。

此功能可顯示所有 WLAN 區域裝置間的邏輯關係，且讓使用者可在拓撲檢視中直接管理裝置。

連線 | 存取點 > 拓撲檢視頁面會顯示一個類似樹狀目錄的圖，呈現防火牆已知的連接裝置和其關係，與下圖雷同:



主題：

- 管理拓撲檢視
- 在拓撲檢視中管理存取點

管理拓撲檢視

拓撲檢視是相當簡單的介面，提供實用工具，可隨時檢視最新拓撲及修改基礎結構中的存取點。

若想確認拓撲是否為最新狀態，可隨時按一下右下角的「重新探索」按鈕。此操作會強制裝置檢查無線基礎結構是否有任何變動。

您也可在拓撲檢視中查看每部裝置的詳細資訊。只需將游標放在裝置上，就會出現一個工具提示泡泡。系統會根據裝置類型顯示名稱、IP 位址、介面和型號等資訊。還可查看存取點的其他資訊，例如狀態和用戶端數量等。

每個存取點也會使用不同顏色來表示狀態:

- 綠色 = 線上
- 紅色 = 離線
- 黃色 = 忙碌

在拓撲檢視中管理存取點

拓撲檢視提供一個操作功能表，其中包含可用於管理存取點的命令。

附註：只有存取點具有操作功能表，拓撲圖中的其他裝置均沒有。

主題：

- 編輯存取點
- 顯示統計資料
- 監控存取點的狀態
- 刪除存取點

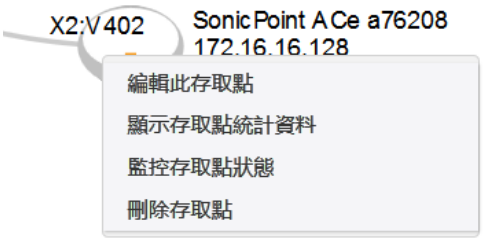
編輯存取點

在拓撲檢視中編輯存取點的步驟如下:

1 導覽至**連線 | 存取點 > 拓撲檢視**。

2 將滑鼠停在要編輯的存取點上。

3 對存取點按一下右鍵。



4 選擇**編輯此存取點**。

5 對物件設定進行必要變更。

6 按一下**確定**儲存新設定。

顯示統計資料

顯示存取點統計資料的步驟如下:

1 導覽至**連線 | 存取點 > 拓撲檢視**。

2 將滑鼠停在要顯示的存取點上。

3 對存取點按一下右鍵。

4 選擇**顯示存取點統計資料**。

5 若要重新整理統計資料，請按一下**重新整理**。

6 完成時，按一下**確定**。

監控存取點的狀態

在拓撲檢視中編輯存取點的步驟如下:

1 導覽至**連線 | 存取點 > 拓撲檢視**。

2 將滑鼠停在要監控的存取點上。

3 對存取點按一下右鍵。

4 選擇**監控存取點狀態**。

「存取點監控」會顯示該存取點的系統狀態，包含 CPU 使用量、記憶體使用量、接收速率和傳送速率。

5 若要重新整理資料，請按一下**重新整理**。

6 若要查看存取點的詳細資訊，請按一下「詳細資訊」圖示。

7 完成時，按一下**確定**。

刪除存取點

在拓撲檢視中編輯存取點的步驟如下:

1 導覽至**連線 | 存取點 > 拓撲檢視**。

2 將滑鼠停在要刪除的存取點上。

3 對存取點按一下右鍵。

4 選擇**刪除存取點**。

5 確認要刪除該存取點；若不要刪除則取消。

18

設定 SonicPoint 入侵偵測服務

欺詐裝置已發展成為對無線安全性最嚴重的一種潛在威脅。通常會將未經授權而在網路上使用的裝置視為欺詐裝置。不安全的存取點具備便利性、可負擔性和可用性，且還可輕鬆新增到網路中，這為引入欺詐裝置創造了有利的環境。真正的威脅以多種方式存在:

- 在無意間與欺詐裝置連接
- 透過不安全的頻道傳送敏感資料
- 對 LAN 資源進行不需要的存取

這並不表示特定無線裝置的安全性不足，而是整個無線網路的安全性存在缺陷。

入侵偵測服務 (IDS) 大幅增強了防火牆的安全功能，因為它可協助裝置識別最常見的不正當無線活動類型並採取應對措施。防火牆可藉由掃描存取點上的 802.11a、802.11g 和 802.11n 無線頻段找到所有存取點的 IDS 報告。

管理檢視上的**連線 | 存取點 > IDS** 頁面會報告防火牆偵測到的所有裝置和其相關聯存取點，並提供授權合法裝置的功能。


檢視樣式: 存取點: 所有存取點

#	存取點	MAC 位...	SSID	類型	通道	驗證	加密	供應商	訊號強度	最大速率	授權
	SonicPoint N2 d791f0- 7 天 18:49:...			--執行 SonicPoint/SonicWave 掃描--							
1	SonicPoint N2 d791f0	c0:ea:e4:bc :13:74	sonicwall-D376	5GHz	36	開放	無	SONICWALL	60% - 非常好	1300 Mbps	
2	SonicPoint N2 d791f0	00:17:c5:a6 :13:c1	sonicwall-9D9C	5GHz	36	開放	無	SONICWALL	18% - 差	300 Mbps	
3	SonicPoint N2 d791f0	c0:ea:e4:a7 :56:94	sonicwall-1490	5GHz	36	WPA2-PSK	TKIP	SONICWALL	99% - 完美	1300 Mbps	
4	SonicPoint N2 d791f0	00:17:c5:ee :90:f5	sonicwall-0432	5GHz	40	WPA2-PSK	TKIP	SONICWALL	0% - 差	54 Mbps	
5	SonicPoint N2 d791f0	c0:ea:e4:b7 :00:26	ndr_radio0	5GHz	44	開放	無	SONICWALL	18% - 差	450 Mbps	
6	SonicPoint N2 d791f0	00:17:c5:cd :63:5f	SWQA	5GHz	44	WPA2-PSK	AES	SONICWALL	39% - 一般	300 Mbps	
7	SonicPoint N2 d791f0	c0:ea:e4:b5 :a8:1c	sonicwall-1580	5GHz	44	WPA-PSK	AES	SONICWALL	78% - 非常好	1300 Mbps	
8	SonicPoint N2 d791f0	18:b1:69:7b :72:2e	sonicwall-3FE0	5GHz	48	開放	無	SONICWALL	18% - 差	1733 Mbps	
9	SonicPoint N2 d791f0	18:b1:69:09 :27:18	Spicy Nachos	5GHz	48	開放	無	SONICWALL	0% - 差	1300 Mbps	

下表說明了**已發現存取點**表和**連線 | 存取點 > > IDS** 頁面上顯示的項目。

已發現存取點表元件

表列或實體元件	說明
實體	
「重新整理」按鈕	重新整理介面，以顯示網路中最新的存取點清單。
「掃描全部」按鈕。	起始呼叫所有存取點和識別已連接裝置的作業。

已發現存取點表元件

表列或實體元件	說明
檢視樣式：存取點	若擁有多個存取點，可從**存取點**下拉功能表中單獨選擇存取點；若要查看所有存取點，請選擇**所有存取點**。
已發現存取點表	
存取點	存取點名稱: 只會在**檢視樣式: 存取點**下拉功能表中選擇了**所有 SonicPoint** 時顯示
MAC 位址 (BSSID)	偵測到的存取點的無線介面的 MAC 位址
SSID	裝置的無線 SSID
類型	裝置使用的無線頻段: 2.4 GHz 或 5 GHz
頻道	裝置使用的無線頻道
驗證	驗證類型
加密	密碼模式
製造商	存取點的製造商。
訊號強度	偵測的無線訊號的強度
最大速率	存取點無線允許的最大速率
授權	按一下「編輯」圖示後，便會將裝置新增到已授權裝置的位址物件組。

主題：

- 掃描存取點
- 授權存取點

掃描存取點

安全裝置啟動後將啟用掃描。啟動後請求掃描時，系統會將無線用戶端中斷幾秒鐘。掃描可通過以下方式影響流量:

- 非持續性無狀態協定（例如 HTTP）不應出現任何不良效果。
- 持續性連接（例如 FTP 協定）受到影響或中斷。
- WiFiSec 連接應自動重新建立，並恢復為對用戶端沒有任何嚴重的影響。

△ 注意：**掃描期間，按一下「掃描全部」會使所有使用中的無線用戶端中斷連接。如果擔心出現服務中斷現象，當 SonicWall 安全裝置處於存取點模式時，請勿請求進行掃描。在無用戶端處於使用中狀態或可接受短暫服務中斷情況之前，請耐心等候。**

執行掃描的步驟如下:

1 導覽至**連線 | 存取點 > IDS**。

2 在**檢視樣式: 存取點**下拉功能表 (表格頂端) 中，選擇**所有存取點**以掃描所有裝置，或選擇特定存取點，僅掃描一部裝置。

3 在表格底部:

- 若要掃描所有存取點，請按一下「掃描全部」。

  (可選) 也可選擇 **--執行存取點掃描--** 下拉功能表中的任一選項: 掃描兩個無線、**掃描無線 0 (5GHz)** 或**掃描無線 1 (2.4GHz)**。

- 若只要掃描一個存取點，請選擇 **--執行存取點掃描--** 下拉功能表中的任一選項: 掃描兩個無線、**掃描無線 0 (5GHz)** 或**掃描無線 1 (2.4GHz)**。

  附註：若只檢視一個存取點，**--執行存取點掃描--** 會從表格中上方移至右下方。

4 確認要執行掃描。

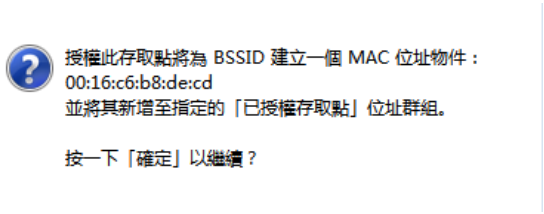
授權存取點

在此裝置設定為授權操作之前將安全裝置偵測到的存取點視為欺詐存取點。

若要授權存取點：

1 導覽至**連線 | 存取點 > IDS**。

2 按一下**授權**列中的**編輯**圖示，以編輯要授權的存取點。將顯示快顯視窗。



3 按一下**確定**。

4 檢查存取點的 MAC 位址是否已新增，確認授權已成功。(如需詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。)

19

設定進階 IDP

進階入侵偵測和防護 (IDP)，或無線入侵偵測和防護 (WIDP)，會監控無線電頻譜中是否存在未授權裝置 (入侵偵測)，並根據管理員設定自動採取應對措施 (入侵防護)。在存取點上啟用了進階 IDP 時，無線電功能將充當專用 IDP 感應器。

△ 注意：**在 SonicWall 存取點無線上啟用了進階 IDP 時，將停用它的存取點功能，並中斷任何無線用戶端的連接。**

SonicOS 無線入侵偵測和防護基於與 SonicWall 閘道協作的 SonicPoint 和 SonicWave 存取點。此功能可以將存取點轉變為專用的 WIDP 感應器，用於偵測連接到 SonicWall 網路的未授權存取點。

△ 注意：**SonicPoint N 設定為 WIDP 感應器時，無法作為存取點使用。**

當某個存取點識別為欺詐存取點時，其 MAC 位址將新增到所有欺詐接入中

設定進階 IDP 是一個分為兩個步驟的過程：

- 對設定檔啟用進階 IDP
- 設定進階 IDP

對設定檔啟用進階 IDP

以下適用於啟用進階 IDP 功能的清單。如需存取點設定檔的詳細資訊，請參閱建立/修改佈建設定檔。

對存取點設定檔啟用進階 IDP 掃描的步驟如下:

1 導覽至**連線 | 存取點 > 基本設定**頁面的 **SonicPoint/SonicWave 佈建設定檔**區段。

2 針對適當設定檔按一下**編輯**圖示。

3 按一下**感應器**。

ⓘ **提示：**所有 SonicPoint N 設定檔的**感應器**標籤均相同。

4 勾選**啟用 WIDP 感應器**。此下拉功能表隨即啟用。

5 在下拉功能表中，為 IDP 掃描選擇適當的排程，或選擇**建立新排程**以建立自訂排程。

△ 注意：**在 SonicPoint/SonicWave 無線電上啟用了進階 IDP 掃描時，將停用它的存取點功能，並斷開任何無線用戶端。**

6 按一下**確定**。

設定進階 IDP

若要設定進階 IDP：

1 導覽至**連線 | 存取點 > 進階 IDP**。

2 勾選**啟用無線入侵探查和防禦設定**以允許裝置搜尋欺詐存取點。此選項預設為不選擇，因此若選擇此項，其他選項將開放使用。

> **附註：**所有偵測到的存取點都會顯示在**連線 | 存取點 > IDS** 頁面上的**已發現存取點**表中，而且您可以授權任何允許的存取點。

3 對於**授權存取點**，選擇要將授權存取點指派到的位址物件群組。預設情況下，會將此選項設定為 **All Authorized Access Points**。

> **附註：**對於 SonicPoint N，不會建立任何存取點模式虛擬存取點 (VAP)。將建立一個站台模式 VAP，此 VAP 用於執行 IDS 掃描以及連接到不安全的存取點並向其傳送探查。

4 對於**欺詐存取點**，選擇要將未授權存取點指派到的位址物件群組。預設情況下，會將此選項設定為 **All Rogue Access Points**。

5 選擇以下兩個選項之一，決定將哪些存取點視為欺詐存取點 (一次只能啟用一個):

- 若選擇**新增任何未授權存取點到欺詐存取點清單**，不論未授權存取點是否連接到您的網路，系統都會自動將所有偵測到的未授權存取點指派到欺詐清單中。
- 若選擇**新增連接的未授權存取點到欺詐存取點清單**，只有當未授權存取點連接到您的網路時，系統才會將這些存取點指派到欺詐清單中。以下選項決定了 IDP 如何偵測已連接的欺詐裝置；兩項都可以選擇:
  - **啟啟用 ARP 快取查詢以偵測連接的欺詐存取點** - 進階 IDP 會在 ARP 快取中搜尋用戶端的 MAC 位址。如果找到一個位址，且它連接到的存取點未獲授權，則將此存取點歸類為欺詐存取點。
  - **啟用使用中的探查以偵測連接的欺詐存取點** - SonicPoint/SonicWave 將連接可疑裝置，並向防火牆的所有 LAN、DMZ 和 WLAN 介面傳送探針。如果防火牆收到這其中的任何探針，則會將此存取點歸類為欺詐存取點。

6 如果裝置不在欺詐清單中，但其 SSID 和託管存取點相同，請選擇**新增邪惡事物到欺詐存取點**以將裝置新增到欺詐清單。

7 選擇**封鎖來自欺詐存取點和它的相關用戶端的流量**可丟棄所有有與欺詐清單相符合的來源 IP 位址的傳入流量。從**欺詐裝置 IP 位址**下拉功能表，執行以下其中一種操作：

- 選擇**所有欺詐裝置**（預設）或您已建立的位址物件群組。
- 通過勾選**建立 IP 位址物件群組**建立一個新位址物件群組。隨即顯示**新增位址物件群組**視窗。

8 選擇**分離欺詐存取點和它的用戶端**可向欺詐裝置的用戶端傳送取消驗證訊息，以封鎖它們之間的通訊。

9 按一下**接受**按鈕以儲存您的變更。

20

存取點封包擷取

管理檢視上的**連線 | 存取點 > 封包擷取**功能提供深入的無線故障排除類型，供您用來收集用戶端站台的無線資料並輸出為可讀取的檔案。SonicWave 存取點支援此功能。

附註：由於掃描無線的天線為 1x1，受限於硬體限制而無法擷取部分資料框架。

存取點 > 封包擷取頁面上的擷取檢視會顯示 SonicWave 狀態、擷取的封包數量和封包緩衝區的大小。按一下右方**設定**欄提供的按鈕，即可為各 SonicWave 設定擷取設定。

可在設定對話方塊中設定模式、頻段和頻道設定，以便擷取特定頻道中的無線封包。最多可設定五個來源和目的地 MAC 位址。按一下要設定的 SonicWave 對應的**編輯**按鈕。

若要擷取其中一個已設定 SonicWave 無線的資料，請在**連線 | 存取點 > 封包擷取**頁面上按一下該列的**下載**按鈕。系統會以「wirelessCapture_[*SW name*].cap」格式為擷取檔案命名，其中的 *SW name* 為 SonicWave 名稱。可使用 Wireshark™ 來讀取檔案。

21

設定虛擬存取點

附註：將無線存取點與 SonicWall NSA 裝置配合使用時，支援虛擬存取點。

虛擬存取點 (VAP) 是單個實體存取點的多路複用表示，將自己表現為多個分立的存取點。對於無線 LAN 用戶端，每個虛擬存取點都會顯示為一個獨立的實體存取點，而實際上只存在一個實體。虛擬存取點用於通過設定單個實體介面上的多個自訂設定，控制無限使用者存取和安全設定。其中的每個自訂設定都作為單獨的（虛擬）存取點，可同時在單個內部無線裝置上進行分組和強制實施。

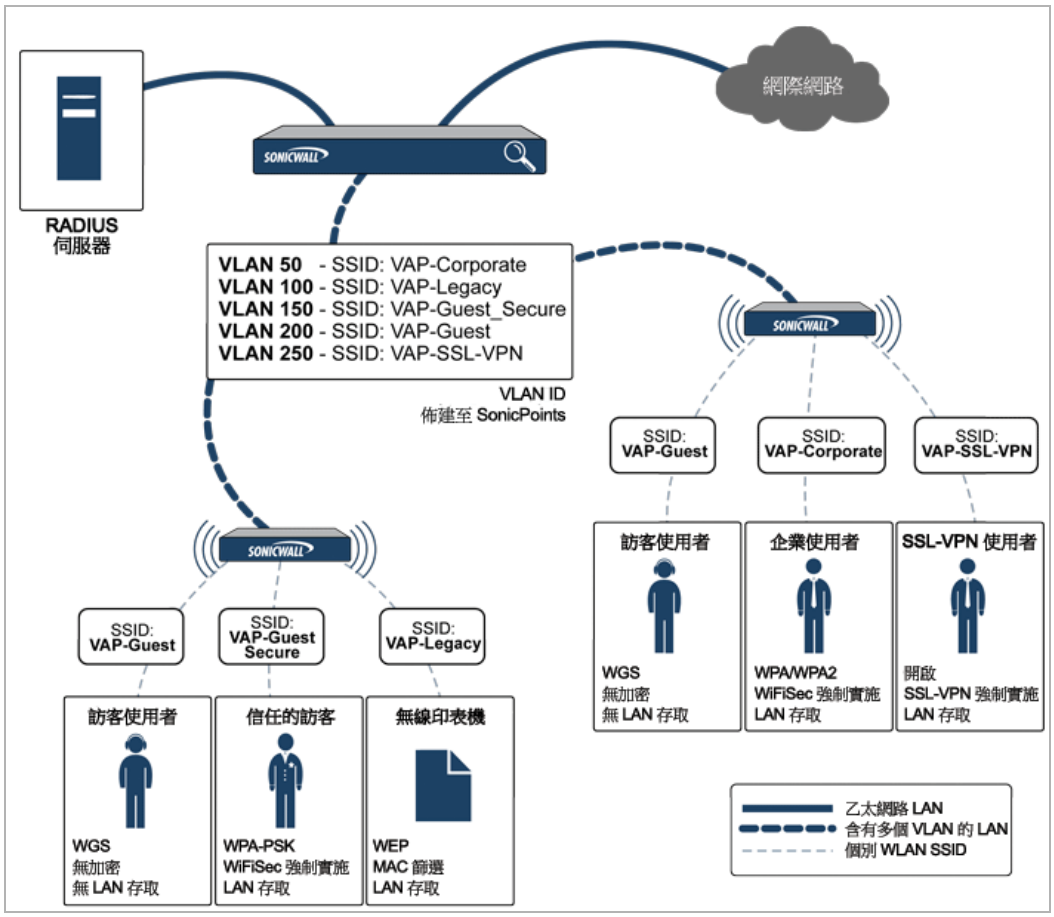
SonicWall VAP 功能符合適用於媒體存取控制 (MAC) 通訊協定層的 IEEE 802.11 標準，其中包括獨特的基礎服務集識別項 (BSSID) 和服務集識別項 (SSID)。此功能可對單個實體存取點上單一無線頻率佔用範圍中的無線網路服務進行分段。

虛擬存取點用於通過設定單個實體介面上的多個自訂設定，控制無限使用者存取和安全設定。其中的每個自訂設定都可作為單獨的 (虛擬) 存取點，且系統可同時在單個或多個實體存取點上對其進行分組和強制執行。

主題：

- 設定 VAP 之前
- 存取點 VAP 設定任務清單
- 虛擬存取點設定檔
- 虛擬存取點
- 虛擬存取點群組

虛擬存取點設定



VAPs 擁有以下優勢：

- 每個虛擬存取點都可有其獨自的安全服務設定（例如 GAV、IPS、CFS 等）。
- 可使用從此區域級別設定的存取規則輕鬆控制來自每個虛擬存取點的流量。
- 單獨的來賓服務或輕量級熱點訊息 (LHM) 設定可套用到每個存取點，便於多個來賓服務供應商展示一組通用的存取點。
- 可輕鬆套用頻寬管理和其他基於存取規則的控制。

設定 VAP 之前

設定虛擬存取點之前，您需先瞭解可選擇的選項和可執行的操作。

主題：

- 確定您的虛擬存取點需求
- 確定安全設定
- 網路定義範例
- 確定安全設定
- VAP 設定工作表

確定您的虛擬存取點需求

決定如何設定您的虛擬存取點時，可先考慮您的通訊需求，尤其是：

- 我需要支援多少個不同級別的無線使用者？
- 我想要如何防護這些不同級別的無線使用者的安全？
- 我的無線用戶端是否具有支援所選的安全設定所需的硬體和驅動程式？
- 我的無線使用者需要與哪些網路資源進行通訊？
- 任何這些無線使用者是否都需要與其他無線使用者進行通訊？
- 我想要將哪些安全服務套用到每個這些級別的使用者或無線使用者？

確定安全設定

瞭解您的安全要求後，便可定義能為這些使用者提供最有效無線服務的區域 (和介面) 及 VAP。以下為定義特定類型使用者方式的範例。

- **公司無線** - 高度信任的無線區域。使用 WPA2-AUTO-EAP 安全。強制實施 WiFiSec (WPA)。
- **WEP 和 PSK** - 中度信任的無線區域。包含兩個虛擬存取點和子介面，一個用於舊 WEP 裝置（例如無線印表機、舊手持式裝置），一個用於存取將使用 WPA-PSK 安全性的用戶端。
- **來賓服務** - 使用內部來賓服務使用者資料庫。
- **LHM** - 啟用輕量級熱點訊息的區域，其設定的目的在於使用外部 LHM 驗證背景伺服器。

網路定義範例

以下清單說明您可用來設定虛擬存取點以確保適當存取權的一種可能方式:

- **VAP #1，公司無線使用者** - 通常在辦公室工作的使用者群體，應為他們提供對所有網路資源的完全存取權限（假定連接已授權且安全）。這些使用者已屬於網路的目錄服務 Microsoft Active Driectory，此服務通過 IAS（網際網路驗證服務）提供 EAP 介面。
- **VAP#2，舊無線裝置** - 僅支援 WEP 加密的舊無線裝置集，例如印表機、PDA 和手持式裝置。
- **VAP#3，存取合作夥伴** - 業務合作夥伴、用戶端、經常存取辦公室的成員、需要存取此有限的受信任網路資源以及網際網路的人員。這些使用者不在公司的目錄服務中。
- **VAP# 4，來賓使用者** - 存取您想要為其提供僅對不信任（例如網際網路）網路資源的存取權限的用戶端。將為某些來賓使用者提供存取時所使用的簡單的臨時使用者名稱和密碼。
- **VAP#5，常見的來賓使用者** - 與來賓使用者相同，但這些使用者通過背景資料庫將具有更長久的來賓帳戶。

前提條件

設定虛擬存取點前，請先留意以下幾點:

- 每個 SonicWall 存取點都必須明確啟用虛擬存取點支援。若要確認，請導覽至**連線 | 存取點 > 基本設定**。然後按一下 **SonicPoint/SonicWave 佈建設定檔 > 一般設定**的**編輯**圖示: **啟用 SonicPoint/SonicWave** 核取方塊，並啟用無線 A 或 G。

- 存取點必須在 SonicWall 網路安全裝置上連結至 WLAN 區域，才能佈建該存取點。
- 將虛擬存取點與 VLAN 配合使用時，必須確保實體存取點發現和設定包保持為未新增標籤的狀態 (除非原生中止 VLAN 子介面進入防火牆) 。
- 還必須確定網路上沒有任何中間裝置 (例如支援 VLAN 的交換器) 在傳遞時對由存取點新增了 VLAN 標籤的 VAP 封包進行變更 (未封裝或未雙重封裝)。
- 請留意適用的最大存取點限制，這些限制根據您的 SonicWall 安全裝置而有所不同。

VAP 設定工作表

VAP 設定工作表表格提供了一些常見的虛擬存取點設定問題和解決方案，還提供了用於記錄您自己的設定的空間。

VAP 設定工作表

問題	範例	解決方案
我將需要支援多少個不同類型的使用者？	公司無線、來賓存取、存取合作夥伴、無線裝置均為通用的使用者類型，每個都需要獨自的虛擬存取點	規劃所需的不同虛擬存取點的數量。為所需的每個虛擬存取點設定區域和 VLAN。
	您的設定：	
每個虛擬存取點需要支援多少個使用者？	公司有 100 個員工，所有員工都有無線功能	將來賓區域的 DHCP 範圍設定為提供至少 100 個位址。
	公司通常有幾十個可使用無線的來賓	將來賓區域的 DHCP 範圍設定為提供至少 25 個位址。
	您的設定：	
我想要如何防護不同無線使用者的安全？	可存取公司 LAN 資源的公司使用者。	設定 WPA2-EAP
	只能存取網際網路的來賓使用者	啟用無線來賓服務，但不設定任何安全設定
	公司 LAN 上的舊無線印表機	設定 WEP 並啟用 MAC 位址篩選
	您的設定：	

VAP 設定工作表

問題	範例	解決方案
我的使用者需要與哪些網路資源進行通訊？	需要存取公司 LAN 和所有內部 LAN 資源的公司使用者，包括其他 WLAN 使用者。	啟用對您公司區域的介面信任。
	需要存取網際網路的無線來賓，不應允許此來賓與其他 WLAN 使用者通訊。	停用對您來賓區域的介面信任。
	您的設定：	
我想要將哪些安全服務套用到我的使用者？	您想要完整的 SonicWall 安全套件防護的公司使用者。	啟用所有 SonicWall 安全服務。
	由於不在您的 LAN 上所以無需考慮的來賓使用者。	停用所有 SonicWall 安全服務。
	您的設定：	

存取點 VAP 設定任務清單

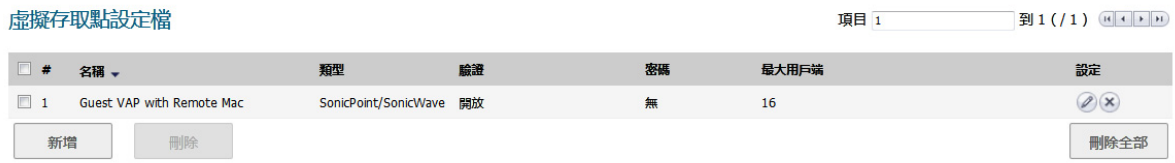
存取點 VAP 部署需要多個設定步驟。以下章節簡要概述了其中包含的步驟。

1. **網路區域** - 區域是虛擬存取點設定的重要部分。您建立的每個區域都擁有其獨自的安全和存取控制設定，您可以通過 VLAN 子介面建立並套用多個區域到單個實體介面。如需網路區域的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**管理 | 網路 > 區域**章節。
2. **介面 (或 VLAN 子介面)** - 介面 (X2、X3 等) 表示 SonicWall 網路安全裝置和實體存取點間的實體連接。個別區域設定將套用到這些介面，然後轉送至存取點。如需網路介面的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**管理 | 網路 > 介面**章節。
3. **DHCP 伺服器** - DHCP 伺服器將租用的 IP 位址指派給指定範圍內的使用者，稱為「範圍」。DHCP 範圍的預設範圍通常很大，足以滿足多數存取點，例如對僅使用 30 個位址的介面使用 200 個位址的範圍。基於此原因，必須仔細設定 DHCP 範圍才能確保不會用完可用的租用範圍。如需設定 DHCP 伺服器的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**管理 | 網路 > DHCP 伺服器**章節。
4. **虛擬存取點設定檔** - **虛擬存取點設定檔**功能用於建立存取點設定檔，可根據需求將這些設定檔輕鬆套用至新的虛擬存取點。如需更多資訊，請參閱**虛擬存取點設定檔**。
5. **虛擬存取點物件** - **虛擬存取點物件**功能用於設定一般 VAP 設定。通過虛擬存取點設定可設定 SSID 和 VLAN ID。如需更多資訊，請參閱**虛擬存取點**。
6. **虛擬存取點群組** - **虛擬存取點群組**功能用於對多個虛擬存取點物件進行分組，並將它們同步套用到存取點。
7. **將虛擬存取點群組指派給存取點佈建設定檔無線** - 佈建設定檔用於將虛擬存取點群組套用到佈建的新存取點。

8 **指派 WEP 金鑰 (僅用於 WEP 加密)** - 「指派 WEP 金鑰」功能用於將 WEP 加密金鑰套用到佈建的新存取點。每個存取點都設有 WEP 金鑰，這表示指派給存取點的任何啟用了 WEP 的虛擬存取點，都必須使用同一組 WEP 金鑰。最多可定義 4 個金鑰，啟用了 WEP 的虛擬存取點可獨立使用這 4 個金鑰。可從**設定 | 存取點 > 基本設定**頁面設定個別存取點或存取點設定檔的 WEP 金鑰。

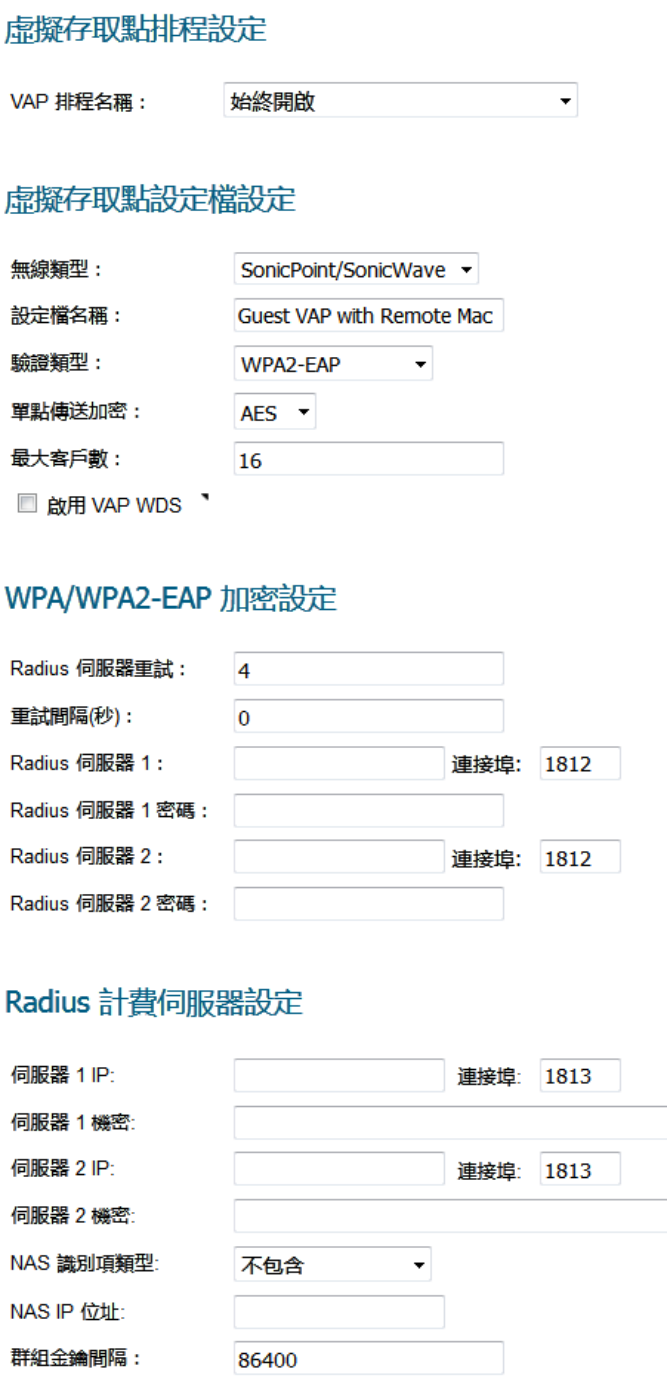
虛擬存取點設定檔

虛擬存取點設定檔用於預設定存取點設定並將其儲存在設定檔中。虛擬存取點設定檔可用於將設定輕鬆套用到新的虛擬存取點。可從**連線 | 存取點 > 虛擬存取點**頁面的**虛擬存取點設定檔**區段設定虛擬存取點設定檔。



若要設定現有 VAP 設定檔，按一下此設定檔的**編輯**圖示。按一下**新增**按鈕即可新增虛擬存取點設定檔。

附註：將顯示的選項取決於您選擇的其他選項。



主題：

- 虛擬存取點排程設定
- 虛擬存取點設定檔設定
- 強制啟用 ACL
- 遠端 MAC 位址存取控制設定

虛擬存取點排程設定

每個虛擬存取點都能擁有與其相關聯的排程，且藉由擴充，每個設定檔也都能擁有專為其定義的固定排程。

為排程與虛擬存取點設定檔建立關聯的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**存取點 > 虛擬存取點**。

3 若要建立新設定檔，請選擇**新增**，或若要編輯現有的設定檔，請選擇一個虛擬存取點設定檔，然後按一下**編輯**圖示。

4 在 **VAP 排程名稱**欄位中，從下拉功能表的選項中選擇所需的排程。

虛擬存取點設定檔設定

設定虛擬存取點設定檔設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要建立新設定檔，請選擇**新增**，或若要編輯現有的設定檔，請選擇一個虛擬存取點設定檔，然後按一下**編輯**圖示。

4 設定**無線類型**。若將存取點作為虛擬存取點使用，則預設值為 **SonicPoint/SonicWave** (目前唯一支援的無線類型)。

5 在**設定檔名稱**欄位中，為此虛擬存取點設定檔輸入易記的名稱。選擇描述性且易於記住的名稱，方便將該設定檔套用到新虛擬存取點。

6 從下拉清單中選擇**驗證類型**。從以下選項中選擇:

驗證類型	定義
開啟	未指定驗證；不安全的存取。
共用	使用共用密碼進行驗證，可確保基本安全。
兩者	不安全，共用存取。
WPA2-PSK	與受信任的公司無線用戶端配合使用的最佳安全性。使用 Windows 登入進行透明驗證支援快速漫遊功能。使用預先共用密碼進行驗證。
WPA2-EAP	與受信任的公司無線用戶端配合使用的最佳安全性。使用 Windows 登入進行透明驗證支援快速漫遊功能。使用可擴充驗證通訊協定。
WPA2-AUTO-PSK	可嘗試使用 WPA2 安全性進行連接，如果用戶端不支援 WPA2，連接會預設為 WPA。使用預先共用密碼進行驗證。
WPA2-AUTO-EAP	可嘗試使用 WPA2 安全性進行連接，如果用戶端不支援 WPA2，連接會預設為 WPA。使用可擴充驗證通訊協定。

系統會依據您選擇的驗證類型自動填入**單點傳送密碼**欄位。

附註：根據您選擇的選項，頁面上會顯示不同設定。

根據所選擇的**驗證類型**而定，「新增/編輯虛擬存取點設定檔」頁面上會新增一個含有選項的額外區段。

- 若您選擇「開放」，請參閱 Radius 伺服器和 Radius 計費取得 RADIUS 設定資訊。
- 若您選擇**兩者皆是**或**共用**，請參閱 WEP 加密設定瞭解設定的相關資訊。
- 若您選擇的選項需要預先共用密碼 (PSK)，請參閱 WPA-PSK > WPA2-PSK 加密設定瞭解設定的相關資訊。
- 若您選擇的選項使用可擴充驗證通訊協定 (EAP)，請參閱 Radius 伺服器和 Radius 計費瞭解設定的相關資訊。

WEP 加密設定

若您在上一道程序的步驟 6 中選擇了**兩者皆是**或**共用**，此處會出現 **WEP 加密設定**區段。WEP 設定通常由一個共同實體存取點中的多個虛擬存取點共用。

設定加密設定的步驟如下:

1 在**加密金鑰**欄位中，從下拉清單選擇**金鑰 1**、**金鑰 2**、**金鑰 3** 或**金鑰 4**。

2 若啟用了「遠端 MAC 存取控制」，請前往 Radius 伺服器和 Radius 計費設定 RADIUS 設定。

WPA-PSK > WPA2-PSK 加密設定

若您在步驟 6 中選擇的選項需要預先共用密碼 (**WPA2-PSK** 或 **WPA2-AUTO-PSK**)，此處會出現 **WPA/WPA2-PSK 加密設定**區段。定義完這些設定後，系統會使用預先共用密碼進行驗證。

設定加密設定的步驟如下:

1 在**複雜密碼**欄位中輸入密碼。

2 若啟用了「遠端 MAC 存取控制」，請前往 Radius 伺服器和 Radius 計費設定 RADIUS 設定。

Radius 伺服器和 Radius 計費

您可針對在步驟 6 中選擇的選項設定 RADIUS 伺服器。定義完這些設定後，系統會使用支援外部 802.1x/EAP 的 RADIUS 伺服器產生金鑰和進行驗證。在下列欄位中輸入值:

若要設定 Radius 伺服器設定:

欄位名稱	說明
Radius 伺服器重試	輸入拒絕使用者存取前使用者可嘗試驗證的次數。預設為 4。
重試間隔（秒）	輸入重試有效的期間。預設為 0。
RADIUS 伺服器 1	輸入 RADIUS 驗證伺服器的名稱/位置。
連接埠	輸入主要 RADIUS 驗證伺服器用來與用戶端和網路裝置進行通訊的連接埠。
RADIUS 伺服器 1 機密	輸入主要 RADIUS 驗證伺服器的密碼。
RADIUS 伺服器 2	輸入備份 RADIUS 驗證伺服器的名稱/位置。

欄位名稱	說明
連接埠	輸入備份 RADIUS 驗證伺服器用來與用戶端和網路裝置進行通訊的連接埠。
RADIUS 伺服器 2 金鑰	輸入備份 RADIUS 驗證伺服器的密碼。

若要設定 Radius 計費伺服器設定:

欄位名稱	說明
伺服器 1 IP	輸入第一 RADIUS 伺服器的 IP 位址。
連接埠	輸入主要 RADIUS 計費伺服器用來與用戶端和網路裝置進行通訊的連接埠。
伺服器 1 機密	輸入主要 RADIUS 計費伺服器的密碼。
伺服器 2 IP	輸入備份 RADIUS 伺服器的 IP 位址。
連接埠	輸入備份 RADIUS 計費伺服器用來與用戶端和網路裝置進行通訊的連接埠。
伺服器 2 機密	輸入備份 RADIUS 計費伺服器的密碼。
NAS 識別項類型	從下拉功能表中選擇 NAS 識別項類型。選項包括：「不包含 (預設)」、「存取點名稱」和「存取點 MAC 位址」
NAS IP 位址	輸入 NAS 系統 IP 位址。
群組金鑰間隔	群組金鑰有效的期間 (單位為秒)，這段時間過後將強制更新群組金鑰。預設值為 **86400** 秒 (24 小時)。

強制啟用 ACL

每個虛擬存取點均可支援單獨的存取控制清單 (ACL)，以提供更高效的身分驗證控制。無線 ACL 功能可配合 SonicOS 上目前可用的無線 MAC 篩選條件清單使用。使用強制啟用 ACL 功能，使用者可以啟用或停用 MAC 篩選條件清單、設定允許清單和設定拒絕清單。

每個虛擬存取點都可擁有自己的 MAC 篩選條件清單設定或使用全域設定。在啟用全域設定時，SonicWave、SonicPoint-N/ SonicPointNDR/ SonicPoint Ni/Ne、SonicPoint 或 SonicPoint-N 設備預設使用這些設定。在虛擬存取點 (VAP) 模式中，此群組的各虛擬存取點共用相同的 MAC 篩選條件清單設定。

ACL 實施設定

選項	說明
啟用 MAC 篩選清單	可通過允許或拒絕來自特定裝置的流量強制實施存取控制。預設情況下未勾選此選項，此區段的所有選項變暗且無法使用。
使用全域 ACL 設定	使用全域 ACL 設定 **附註：** 只有 SonicPointN 支援對每個虛擬存取點的 ACL 支援。如果 SonicPoint/SonicWave 使用某個虛擬存取點，則系統會預設套用全域 ACL 設定。

ACL 實施設定

選項	說明
允許清單	選擇一個 MAC 位址群組，只要裝置的 MAC 位址列在特定群組中，系統便會自動允許來自這些裝置的流量: • **建立新的 Mac 位址物件群組.....** • **所有 MAC 位址** **附註：** 推薦將**允許清單**設定為**所有 MAC 位址**。 • **預設 SonicPoint/SonicWave ACL 允許群組** • 自訂您建立的 MAC 位址物件群組
拒絕清單	從下拉功能表選擇 MAC 位址群組，以自動拒絕來自擁有此組中的 MAC 位址的所有裝置的流量。 **附註：** **拒絕清單**在**允許清單**之前執行。 • **建立新的 Mac 位址物件群組.....** • **無 MAC 位址** • **預設 SonicPoint/SonicWave ACL 拒絕群組** **附註：** 建議將**拒絕清單**設定為**預設 SonicPoint/SonicWave ACL 拒絕群組**。 • 自訂您建立的 MAC 位址物件群組

遠端 MAC 位址存取控制設定

附註：如果**驗證類型**為 **WPA/WPA2/WPA2-AUTO-EAP**，則不會出現此區段。

遠端 MAC 位址存取控制設定

選項	說明
啟用遠端 MAC 存取控制	勾選方塊以強制在遠端 Radius 伺服器根據基於 MAC 的驗證原則實施無線存取控制。預設情況下，未選擇此選項。 **附註：** 如果**驗證類型**不是 **WPA2-EAP/WPA2-AUTO-EAP**，選擇**啟用遠端 MAC 存取控制**便會出現 **Radius 伺服器設定**區段。

虛擬存取點

虛擬存取點設定功能用於設定一般虛擬存取點設定。通過虛擬存取點設定可設定 SSID 和 VLAN ID。虛擬存取點則可從**存取點 > 虛擬存取點**頁面設定。

若要設定現有 VAP，按一下該虛擬存取點的**編輯**圖示。按一下**新增**按鈕以新增 VAP。

主題：

- 第 189 頁「一般面板」
- 第 190 頁「進階標籤」

一般面板

在一般面板上設定下列功能。

虛擬存取點一般設定

功能	說明
名稱	為您的虛擬存取點建立易記的名稱。
SSID	輸入使用此 VAP 的存取點之 SSID 名稱。當搜尋可用的存取點時，此名稱會出現在無線用戶端清單中。
VLAN ID	使用支援 VLAN 的平台時，您可以有選擇性地選擇與此虛擬存取點相關聯的 VLAN ID。此虛擬存取點的設定將從您所選擇的 VLAN 繼承。
啟用虛擬存取點	啟用此虛擬存取點。預設情況下已核取此選項。
啟用 SSID 隱藏	隱藏 SSID 名稱的廣播並停用對探查請求的回應。如果不想要未授權的無線用戶端存取您的 SSID，請選擇此選項。預設情況下未勾選此選項。
啟用動態 VLAN ID 指派	勾選以啟用。動態 VLAN 只能在驗證類型設為 EAP 時啟用。

進階標籤

進階設定用於為特定虛擬存取點設定驗證和加密設定。選擇**設定檔名稱**以從使用者建立的設定檔繼承這些設定。由於**新增/編輯虛擬存取點**視窗和**新增/編輯虛擬存取點的設定檔**視窗的**進階**標籤相同，有關完整的驗證和加密設定資訊，請參見虛擬存取點設定檔。

虛擬存取點群組

SonicWall NSA 裝置提供有虛擬存取點群組功能。用於對多個虛擬存取點物件進行分組，以將其同步套用到存取點。虛擬存取點群組可從**連線 | 存取點 > 虛擬存取點**頁面設定。

新增虛擬存取點群組的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要建立新設定檔，請選擇**新增**，或若要編輯現有的設定檔，請選擇一個虛擬存取點設定檔，然後按一下**編輯**圖示。

4 在指定欄位中輸入**虛擬存取點群組名稱**。

5 從**可用的虛擬存取點物件**清單中選擇要新增的物件，然後按一下**左箭頭**將該物件移到**虛擬存取點群組成員**清單中。

或者按一下**全部新增**，將所有物件新增到群組。

6 選擇一個物件並使用**右箭頭**或**全部移除**按鈕，將物件從群組中移除。

7 按一下**確定**儲存您的設定。

22

設定 RF 監控

當今基於 802.11 的無線網路裝置所使用的射頻 (RF) 技術對入侵者頗具吸引力。如果不加管理，RF 裝置會使您的無線（和有線）網路對於外部的各種威脅（從拒絕服務 (DoS) 到網路安全破壞）處於開放狀態。為保護 SonicWall 無限存取點，SonicWall 可協助偵測威脅，而不會中斷目前無線或有線網路的運作。

SonicWall RF 監控提供對 SonicPoint 射頻流量的即時威脅監控和管理。除有即時威脅監控功能外，SonicWall RF 監控還提供了集中收集 RF 威脅和流量統計的系統；還提供了一種直接從 SonicWall 安全裝置閘道輕鬆管理 RF 功能的方法。

管理檢視上的**連線 | 存取點 > RF 監視**頁面提供一個中心位置，可在此選擇 RF 簽章類型、查看已發現的 RF 威脅工作站以及將發現的威脅工作站新增到監視清單。

主題：

- 前提條件
- RF 監控摘要

前提條件

為強制實施 RF 監控，必須在所有可用存取點上啟用 RF 監控選項。最簡單的啟用方式為更新存取點設定檔，然後將該設定檔套用至適用的存取點。找到 RF 監控選項的步驟如下:

1 在**管理**檢視上，導覽至**連線 | 存取點 > 基本設定**。

2 按一下要更新的設定檔對應的**編輯**圖示 (或若要建立新的設定檔，則從**新增設定檔**下拉功能表中**選擇 SonicPoint/SonicWave 類型**)。

3 在**一般**視窗中勾選方塊以**啟用 RF 監控**。

如需對設定檔進行設定的詳細資訊，請參閱建立/修改佈建設定檔。

RF 監控摘要

RF 監控摘要會顯示已設定為使用 RF 監控的存取點之相關資料，

也會以紅色顯示識別出的 RF 威脅數量及**測量間隔**設定。在欄位中輸入新數字，即可重設**測量間隔**。預設值為 **300** 秒。請務必按一下**接受**儲存設定。

按一下藍色的**存取點**連結，前往**連線 | 存取點 > 基本設定**頁面編輯設定檔或物件設定。

802.11 一般框架設定

「802.11 一般框架設定」面板會顯示一般威脅總數和啟用長久持續的選項。

勾選方塊即可啟用**長久持續**。通過將射頻光譜劃分為 14 個交錯的頻道，無線裝置可共用電視廣播。每個裝置在指定的（短）持續時間內都保留一個頻道，在此期間，任何一個裝置都保留有一個頻道，其他已知的裝置在此頻道上不廣播。長久持續攻擊通過保留多個射頻頻道較長的時間來使用此過程，並通過找到開放的廣播頻道有效地停止有效的無線流量。預設情況下未指定此選項。

請務必按一下**接受**儲存設定。

802.11 管理框架設定

802.11 管理框架設定面板用於設定您的管理框架設定，並針對每項設定顯示威脅的數量。

勾選方塊以啟用其中任意選項，所有選項皆預設為啟用。按一下**接受**儲存設定。下表說明**管理框架設定**。

802.11 管理框架設定

名稱	說明
所有管理威脅	顯示管理威脅的總數。
管理框架攻擊	DoS 攻擊的變體嘗試用管理框架攻擊無線存取點（例如關聯或驗證請求），此管理框架使用偽造的請求填充管理表。
無探查回應	無線用戶端傳送探查請求時，攻擊者返回包含空 SSID 的回應。此回應會使多個常見無線卡和裝置停止回應。
廣播取消驗證	這個 DoS 變異傳送欺騙的取消驗證框架給無線客戶，強迫它們連續的取消驗證和持續的和存取點之間再驗證
具備無效 SSID 的有效站台	在此攻擊中，欺詐存取點嘗試廣播受信任的站台 ID (ESSID)。儘管 BSSID 通常無效，站台仍對用戶端顯示，好像它是受信任的存取點。此攻擊的目的是通常從受信任的用戶端獲取驗證資訊。
Wellenreiter 偵測	Wellenreiter 是常用的軟體應用程式，攻擊者可使用它檢索來自週圍無線網路的資訊。
Ad-Hoc 站台偵測	Ad-Hoc 站台是可提供無線用戶端存取權限的節點，其存取方式為充當實際存取點和使用者之間的網橋。無線使用者通常受欺騙連接 Ad-Hoc 站台，而不是實際的存取點，因為它們可能有相同的 SSID。這使 Ad-Hoc 站台能夠攔截連接的用戶端與存取點之間傳送或接收的任何無線流量。

802.11 資料框架設定

802.11 資料框架設定面板用於設定您的管理框架設定，並針對每項設定顯示威脅的數量。

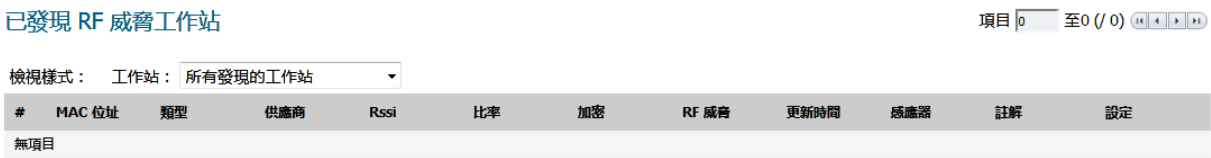
勾選方塊以啟用其中任意選項。按一下**接受**儲存設定。預設情況下，未選擇**未關聯工作站**，其他核取方塊處於啟用狀態。下表說明**資料框架設定**。

802.11 資料框架設定

名稱	說明
所有資料威脅	顯示資料威脅的總數。
未關聯工作站	無線站台在與存取點相關聯之前嘗試進行驗證，未關聯的站台在未關聯期間通過將攻擊的驗證請求傳送給存取點可建立 DoS。
NetStumbler 偵測	通常用於找到免費的網際網路存取和所需的網路。NetStumbler 與 GPS 接收器和對應軟體相結合，可自動對應無線網路的位置。攻擊者也將 NetStumbler 用於從週圍的無線網路擷取資訊。
EAPOL 封包攻擊	區域網路的擴充驗證協定 (EAPOL) 封包用在 WPA 和 WPA2 驗證機制中。由於這些封包類似其他驗證請求封包，由無線存取點公開接收，因此這些封包的攻擊會使 DoS 進入您的網路。
弱 WEP IV	WEP 安全機制使用您的 WEP 金鑰以及隨機選擇的 24 位數字作為初始向量 (IV) 來加密資料。由於隨機初始向量的數字比其它數字弱，網路攻擊者通常針對此類加密類型，使其更容易解密 WEP 金鑰。

發現的 RF 威脅工作站

RF 威脅工作站面板會顯示已發現 RF 威脅工作站的相關資訊。可顯示所有以發現的威脅工作站，也可只顯示監視清單群組中的威脅工作站，視您在**檢視樣式: 工作站**下拉功能表中選擇的項目而定。



以下詳細說明「威脅工作站」表中的資料:

已發現 RF 威脅工作站

名稱	說明
項目	顯示記錄的威脅的總數。如果適用，請使用箭頭按鈕瀏覽頁面。
檢視樣式：工作站	選擇項目清單中顯示的站台類型： • 所有已發現的系統。 • 僅在監視清單群中的工作站
# MAC 位址	按照 MAC 位址對項目排序。這是 RF 威脅站台的實體位址。
類型	按照從威脅站台接收的無線訊號的類型對項目排序。
供應商	按供應商對項目排序。這是威脅站台的製造商（由 MAC 位址確定）。
RSSI	按照 SonicPoint 報告的接收訊號的強度對項目排序。此項目以及**感應器**項目，在對 RF 威脅裝置的實際實體位置做三角測量時非常有用。
速率	按照威脅站台的傳送速率 (Mbps) 對項目進行排序。
加密	按照威脅站台上的無線訊號加密（**無**或**已加密**）對項目進行排序。
RF 威脅	按照 RF 威脅對項目進行排序（發生在最近的時間）。
更新時間	按照建立/更新此記錄的時間對項目進行排序。
感應器	按照記錄此威脅的 SonicPoint 的 ID 對項目排序。此項目以及 **Rssi** 項目，在對 RF 威脅裝置的實際實體位置做三角測量時非常有用。
註解	顯示用於新增有關威脅註解的文字框。
設定	設定已發現站台的監視清單。

提示：使用記錄的威脅統計可找到 RF 威脅裝置的大概位置。如需使用射頻管理威脅統計的實用性建議和資訊，請參見第 197 頁「實用型 RF 監控欄位應用程式」。

將威脅站台新增到監視清單中

RF 監控已發現威脅站台「監視清單」功能用於建立無線網路的威脅監視清單。監視清單用於篩選已發現 RF 威脅站台清單中的結果。

如需將站台新增到監視清單中，請執行以下操作：

1. 在 **SonicPoint > RF 監視**頁面中，移至**已發現 RF 威脅工作站**部分。
2. 按一下與您想要新增到監視清單的威脅站台相對應的**編輯**圖示。將顯示確認對話方塊。
3. 按一下**確定**將站台新增到監視清單。
4. 如果不慎將站台新增到監視清單，或要從清單刪除某站台，請按一下與您想要移除的威脅站台相對應的**移除**圖示。

   提示：將一個或多個站台新增到監視清單中後，您可以通過選擇**檢視類型**下拉清單中的**僅在監視清單群中的工作站**篩選結果，以便僅顯示即時記錄中的這些站台。

5. 按一下**接受**。

實用型 RF 監控欄位應用程式

本節概述了偵測 Wi-Fi 威脅來源時收集 RF 監控資料的實際用途。使用射頻資料查找威脅時請注意，無線訊號受多方面的影響。

- 訊號強度並非總能有效指出距離。

  牆壁、無線干擾、裝置功率輸出甚至環境的溫度和濕度等障礙都會影響無線裝置的訊號強度。

- MAC 位址並非永久位址。

  MAC 位址通常能指出裝置的類型和製造商，此位址容易發生改變，且可能受欺詐。同樣，RF 威脅的發起人有多個硬體裝置可供自行支配。

主題：

- 使用感應器 ID 確定 RF 威脅位置
- 第 198 頁「使用 RSSI 確定鄰近的 RF 威脅」

使用感應器 ID 確定 RF 威脅位置

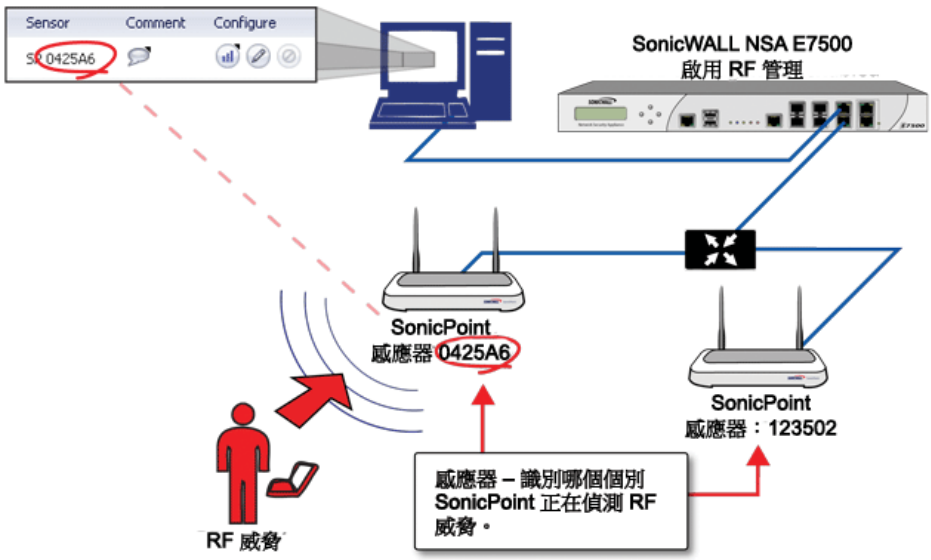
在**已發現 RF 威脅工作站**表中，**感應器**欄位可指出哪個存取點正在偵測特定威脅。使用感應器 ID 和存取點的 MAC 位址可輕鬆確定正在偵測威脅的存取點位置。

提示：尤其在本節中 (及作為一般的良好習慣)，您可能會發現保留位置記錄和您的存取點 MAC 位址非常有用。

1. 導覽至**連線 | 存取點 > RF 監控**頁面。
2. 在**已發現 RF 威脅工作站**表中，找到偵測目的地 RF 威脅的 SonicPoint 的**感應器**，並記錄其編號。
3. 導覽至**連線 | 存取點 > 基本設定**。
4. 在 **SonicPoint/SonicWave 物件**表中，找到與您在步驟 2 中記錄的感應器編號相符合存取點。
5. 記錄此 SonicPoint 的 **MAC 位址**。
6. 使用 MAC 位址查找存取點的實體位置。

   RF 威脅可能就位於此存取點服務的位置。

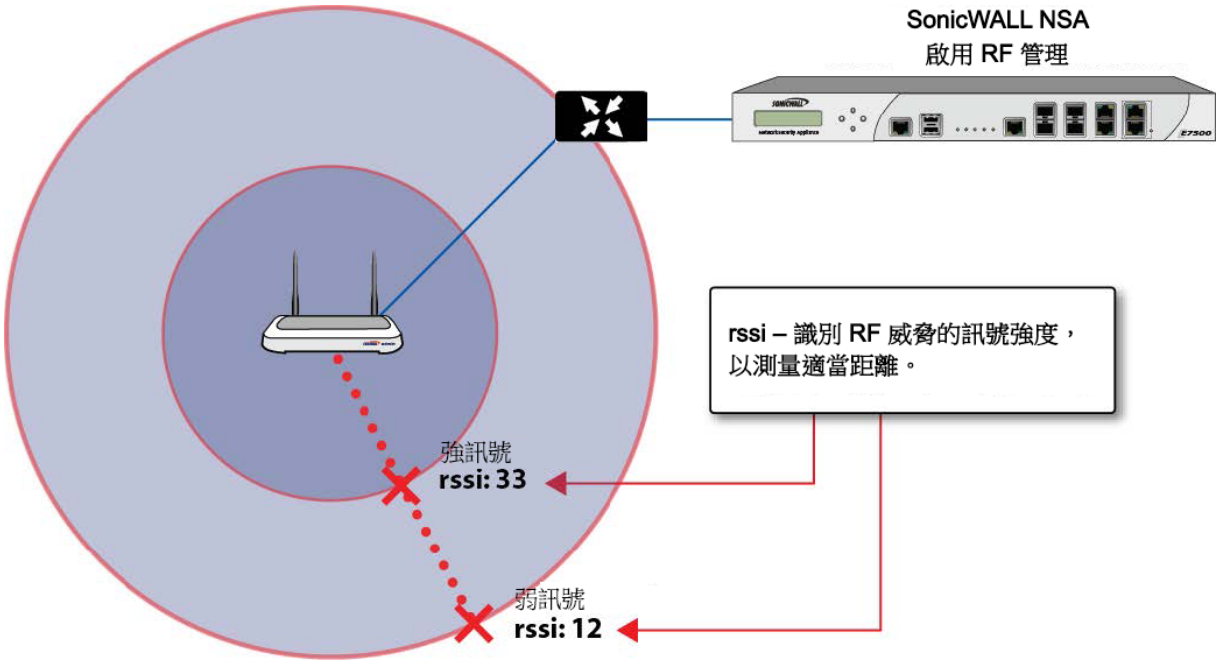
使用感應器 ID 確定 RF 威脅位置



使用 RSSI 確定鄰近的 RF 威脅

本節基於使用感應器 ID 確定 RF 威脅位置中的內容。在「已發現 RF 威脅工作站」清單中，Rssi 欄位可指出特定存取點正在使用什麼樣的訊號強度偵測 RF 威脅。

使用 RSSI 確定鄰近的 RF 威脅



Rssi 欄位用於輕鬆確定 RF 威脅對於正在偵測此威脅的存取點的鄰近程度。較高的 Rssi 編號通常表示威脅距離存取點較近。

重要：必須記住，牆壁可能會阻礙無線訊號。如果 Rssi 訊號非常弱，表示 RF 威脅的位置距離存取點非常遠，也可能代表威脅位於附近位置，但在所在房間或建築物之外。

1 導覽至**連線 | 存取點 > RF 監控**頁面。

2 在**已發現 RF 威脅工作站**表中，找到正在偵測目標 RF 威脅的存取點之**感應器**和 **Rssi**，並記錄這些編號。

3 導覽至**連線 | 存取點 > 基本設定**頁面。

4 在 **SonicPoint/SonicWave 物件**表中，找到與您在步驟 2 中記錄的感應器編號相符的 SonicPoint。

5 記錄此 SonicPoint 的 **MAC 位址**。

6 使用 MAC 位址查找 SonicPoint 的實體位置。

較高的 Rssi 編號通常表示 RF 威脅距離 SonicPoint 很近。較低的 Rssi 編號表示存在障礙物或距離 RF 威脅較遠。

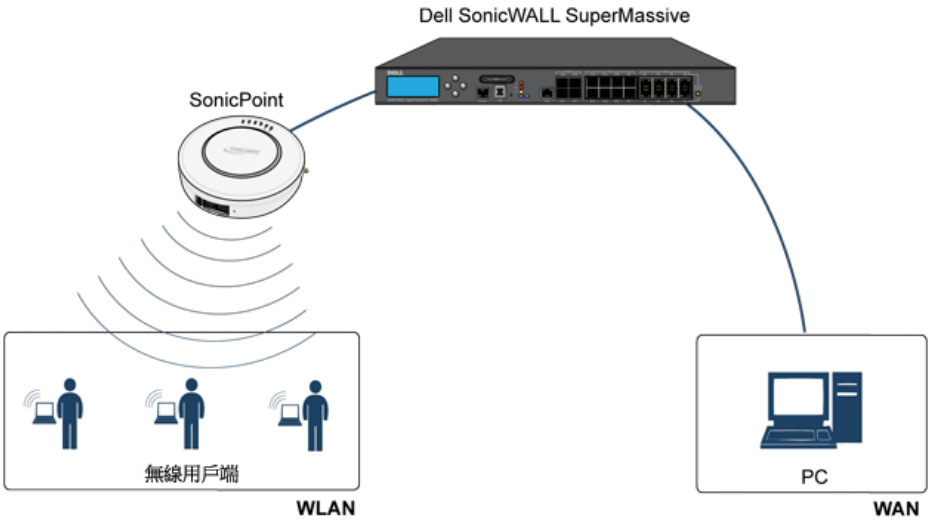
23

設定 FairNet

Fairnet 功能為網路管理員提供了一種易於使用的方法來控制關聯的無線用戶端的頻寬，並確保在這些無線用戶端之間公平地指派頻寬。管理員可以為所有無線用戶端、特定的 IP 位址範圍或單獨的用戶端設定 FairNet 頻寬限制，以實現公平性和提高網路效率。

以下是典型 FairNet 拓撲範例：

典型 FairNet 拓撲



若要部署 FairNet 功能，您的筆記型電腦或 PC 必須配備 IEEE802.11b/g/n 無線網路介面控制器。

主題：

- 支援的平台
- FairNet 功能
- 管理介面概述
- 設定 FairNet

支援的平台

以下裝置型號目前支援 FairNet 功能:

- SonicWall TZ 系列
- SonicWall NSA 系列
- SonicWall E-Class NSA 系列
- SonicWall SuperMassiv 系列

FairNet 功能

分布式協調功能 (DCF) 對每個存取媒體的用戶端提供了相同的時間機會。但不能保證所有無線用戶端之間的站台預處理資料流量都相等。FairNet 功能在現有 802.11 DCF 的頂層實施，可保證無線用戶端之間頻寬的公平性，而無需考慮流量的方向和數量。

流量控制功能可確定封包是否排隊或丟棄（例如，如果佇列已達到某長度限制，或流量超過某速度限制）。還可確定傳送封包的順序（例如，對某些封包優先傳送），以及延遲封包的傳送（例如，限制傳出流量的速率）。流量控制釋放要傳送的封包後，裝置驅動程式會拾取此封包，並在網路上傳送。

管理介面概述

下表說明 FairNet 畫面的元件。

FairNet 介面元件

名稱	說明
按鈕和核取方塊	
新增	針對 IP 位址或位址範圍新增 FairNet 原則。隨即顯示**新增 FairNet 原則**對話方塊。
刪除	刪除選定的 FairNet 原則。
接受	套用最新的設定。
取消	取消任何已變更的設定。
核取方塊	
啟用 FairNet	啟用 FairNet 功能。
FairNet 原則	在 **FairNet 原則**表格標題：選擇或取消選擇 **FairNet 原則**表中的所有原則。也可從原則清單中選擇單獨的原則。
FairNet 原則表格欄	
方向	顯示每個原則的方向。方向包括： • 上行連結 • 下行連結 • 兩者
起始 IP	顯示起始 IP 位址範圍。
終止 IP	顯示終止 IP 位址範圍。

FairNet 介面元件

名稱	說明
最小比率 (kbps)	保證用戶端的最小頻寬。最小速率為 1 Kbps。
最大比率 (kbps)	用戶端保證的最大頻寬。最大速率為 54000 Kbps。
介面	顯示套用 FairNet 原則的介面。這是存取點所連接的管理防火牆上的介面。
啟用	勾選此方塊時會啟用選定的 FairNet 原則。
設定	按一下**編輯**圖示即可編輯現有的 FairNet 原則。按一下**刪除**圖示即可刪除特定 FairNet 原則。

設定 FairNet

本節包含 FairNet 的設定範例。

將 FairNet 設定為提供更多的雙向頻寬的步驟如下：

1 導覽至**連線 | 存取點 > FairNet** 頁面。

2 按一下**新增**按鈕。

3 勾選**啟用原則**方塊。預設情況下已勾選此核取方塊。

4 從**方向**下拉功能表，選擇**雙向**。這會將原則套用到上載和下載內容的用戶端。這是預設值。

5 在**起始 IP** 欄位，輸入 FairNet 原則的起始 IP 位址 (例如，`172.16.29.100`)。

6 在**終止 IP** 欄位，輸入 FairNet 原則的終止 IP 位址 (例如，`172.16.29.110`)。

提示：IP 位址範圍必須位於對 WLAN 介面設定的子網路中。

7 在**最小速率 (kbps)** 欄位，輸入 FairNet 原則的最小頻寬。最小值和預設值為 100Kbps，最大值則為 300Mbps (300,000Kbps)。

8 在**最大速率 (kbps)** 欄位，輸入 FairNet 原則的最大頻寬。最小值和預設值為 100Kbps，最大值則為 300Mbps (300,000Kbps)，不過典型的設定為 20Mbps。

9 從**介面**下拉功能表中選擇存取點連接的介面 (例如 X2)。

10 按一下**確定**按鈕，將 FairNet 原則新增到 **FairNet 原則**表中。

11 按一下**啟用**核取方塊。

12 按一下**接受**按鈕。

您的 SonicWall FairNet 原則現已設定。

24

設定 Wi-Fi 多媒體

SonicOS 存取點支援 Wi-Fi 多媒體 (WMM)，針對頻寬密集型應用程式（如 VoIP、在 Wi-Fi 電話上提供 VoIP、在無線 IEEE 802.11 網路上提供多媒體流量）提供更好的服務品質 (QoS) 體驗。

WMM 是一項基於 IEEE 802.11e 標準的 Wi-Fi 聯盟互操作性認證。它根據四個存取類別設定流量優先順序：

- **語音** - 最高優先順序
- **視訊** - 第二優先順序
- **最佳成就** - 第三優先順序（用於電子郵件和網際網路瀏覽等應用）
- **背景** - 第四優先順序（用於對延遲不敏感的應用，如列印等）

附註：WMM 不保證傳送量。

主題：

- WMM 存取類別
- 將流量指派到存取類別
- 設定 Wi-Fi 多媒體參數
- 刪除 WMM 設定檔

WMM 存取類別

每個存取類別都有自己的傳送佇列。根據應用或防火牆提供的服務類別 (ToS) 資訊，將流量指派到相應的存取類別。SonicWall 安全裝置通過存取規則或 VLAN 標籤指派 TOS。

下表顯示了 WMM 存取類別與 802.1D 使用者優先順序的對應關係。

Wi-Fi 多媒體存取類別

優先順序	使用者優先順序（同 802.1D 使用者優先順序）	802.1D 名稱	WMM 存取類別 (AC)	WMM AC 名稱（易懂）
最低	1	BK	AC_BK	背景
	2	-	AC_BK	背景
	0	BE	AC_BE	最佳成就
	3	EE	AC_BE	最佳成就
	4	CL	AC_VI	視訊
	5	VI	AC_VI	視訊
	6	VO	AC_VO	語音
最高	7	NC	AC_VO	語音

WMM 通過一個稱為增強分布式頻道接入(EDCA) 的過程來設定流量優先順序。並藉由為各存取類別定義一系列不同的「退避」時間來設定流量優先順序。WMM 退避時間由兩個參數來定義：

- **仲裁框架間空間 (AIFS)** - 無線頻道變為空閒到 AC 可以開始交涉接入頻道的時間。
- **競爭視窗 (CW)** - 隨機退避時間的可能值範圍。指定隨機退避時間的範圍。CW 由最小值和最大值來定義：
  - **最小競爭視窗 (CWMin)** - CW 長度的初始上限。嘗試傳送之前，AC 會等待 0 到 CWMin 之間的隨機時間。AC 的優先順序越高，則所指派的 CWMin 越短。
  - **最大競爭視窗 (CWMax)** - CW 的上限。如果發生衝突，AC 將 CW 的大小加倍，直至達到 CWMax，然後再次嘗試傳送。CWMax 必須大於 CWMin。

一般來說，AC 的優先順序越高，則所指派的 AIFS、CWMin、CWMax 值越低。

附註：AIFS、CWMin 和 CWMax 的度量單位是所用 802.11 標準的時間槽的倍數。對於 802.11b，一個時間槽為 20 微秒。對於 802.11a 和 802.11g，一個時間槽為 9 微秒。

分別為存取點和工作站 (SonicWall 安全裝置) 設定 WMM 參數。下表顯示了存取點和 SonicWall 安全裝置的預設 WMM 參數。

存取點的預設 WMM 參數

WMM 存取類別 (AC)	WMM AC 名稱（易懂）	CWMin	CWMax	AIFS
AC_BE(0)	最佳成就	4	6	3
AC_BK(1)	背景	4	10	7
AC_VI(2)	視訊	3	4	1
AC_VO(3)	語音	2	3	1

SonicWall 安全裝置的預設 WMM 參數

WMM 存取類別 (AC)	WMM AC 名稱（易懂）	CWMin	CWMax	AIFS
AC_BE(0)	最佳成就	4	10	3
AC_BK(1)	背景	4	10	7

SonicWall 安全裝置的預設 WMM 參數

WMM 存取類別 (AC)	WMM AC 名稱（易懂）	CWMin	CWMax	AIFS
AC_VI(2)	視訊	3	4	2
AC_VO(3)	語音	2	3	2

將流量指派到存取類別

WMM 要求存取點為多個優先順序存取類別實施多個佇列。為區分流量類型，存取點依賴應用程式或防火牆在 IP 資料中提供服務類型 (TOS) 資訊。SonicWall 安全裝置通過兩種方法將流量指派到 WMM 存取類別：

- 指定防火牆服務和存取規則
- VLAN 標籤

指定防火牆服務和存取規則

可以區分使用某個連接埠的服務的優先順序，並將這些服務置於合適的傳送佇列。例如，可以將傳送到連接埠 2427 的 UDP 流量視為視訊流。在**原則 | 物件 > 服務物件**頁面上新增自訂服務。如需更多資訊，請參閱 *SonicWall SonicOS 6.5 原則*。

應在**原則 | 規則 > 存取規則**頁面上為新服務至少新增一個存取規則。例如，如果 LAN 區域上的工作站到 WLAN 區域上的無線用戶端發生此類服務，則可以在**新增規則**視窗的**一般**標籤中設定存取規則。在**新增規則**視窗的 **QoS** 標籤中，將定義一個顯見 DSCP 值。

之後，當通過防火牆使用 UDP 通訊協定，以目的地連接埠 2427 將封包傳送到存取點時，系統將根據存取規則中的 QoS 設定來設定它們的 TOS 欄位。

VLAN 標籤

可透過虛擬存取點在 VLAN 中設定優先順序，因為 SonicWave、SonicPoint N 和 AC 允許將虛擬存取點設定為使用相同 VLAN ID 連接 VLAN。您可以通過防火牆存取規則為 VLAN 流量設定優先順序。

防火牆存取規則類似於針對目的地為某連接埠 (如 2427) 的 UDP 服務設定優先順序的規則，但設定時會使用 WLAN 子網路等 VLAN (通過 VAP 的 VLAN) 介面，因為**來源**和**目的地**是 WLAN 對 WLAN 規則。請參閱 *SonicWall SonicOS 6.5 原則*中的「原則 | 規則 > 存取規則」瞭解詳情。

設定 Wi-Fi 多媒體參數

預設情況下，SonicWall 安全裝置設定一個 WMM 設定檔，參數設定為 802.11e 標準的值。

主題：

- 設定 WMM
- 為存取點建立 WMM 設定檔
- 刪除 WMM 設定檔

設定 WMM

自訂WMM 設定的步驟如下：

1 導覽至**連線 | 存取點 > Wi-Fi 多媒體**頁面。

2 若要修改 WMM 設定檔，按一下此設定檔的**編輯**圖示。要新建 WMM 設定檔，按一下**新增**按鈕。

3 針對新的 WMM 設定檔，輸入**設定檔名稱**。預設名稱為 **wmmDefault**。

4 修改參數以自訂 WMM 設定檔；系統會在視窗中自動填入預設 WMM 參數值。如需這些類別的資訊，請參見 Wi-Fi 多媒體存取類別表格。

附註：設定 WMM 設定檔時，您可以設定爭用視窗 (CWMin/CWMax) 的大小，以及在建立 WMM 設定檔時設定仲裁框架間間隔 (AIFS) 數。可以在存取點 (SonicPointN) 上為每個優先順序（AC_BK、AC_BE、AC_VI 和 AC_VO）以及為工作站（防火牆）設定這些值。

5 按一下**對應**標籤以自訂存取類別與 DSCP 值的對應關係。

6 將優先順序層級對應到 DSCP 值。預設的 DSCP 值與**原則 | 規則 > 存取規則**、**QoS** 對應中的值相同。

7 按一下**確定**。

為存取點建立 WMM 設定檔

可於**管理**檢視上的**連線 | 存取點 > Wi-Fi 多媒體**頁面設定 WMM 設定檔，包括參數和優先順序與對應。

在**存取點 > 基本設定**頁面設定 SonicWave、SonicPoint N 或 SonicPoint AC 設定檔時，也可以建立 WMM 設定檔或選擇現有的 WMM 設定檔。**設定**視窗的**進階/無線 0/1 進階**標籤上提供了一個 **WMM (Wi-Fi 多媒體)** 下拉功能表。

從 **WMM (Wi-Fi 多媒體)** 下拉功能表中選擇**建立新的 WMM 設定檔...**，便會顯示**新增 Wlan WMM 設定檔**視窗。

刪除 WMM 設定檔

若要刪除單個 WMM 設定檔，按一下此設定檔的**設定**列中的**刪除**圖示。

若要刪除多個 WMM 設定檔，請勾選要刪除的設定檔旁邊的方塊，然後按一下**刪除**按鈕。

若要刪除所有 WMM 設定檔，按一下**全部刪除**按鈕。此時會顯示一條顯示訊息，確認將刪除所有設定檔。

25

存取點 3G/4G/LTE WWAN

若有 3G/4G/LTE 裝置與您的存取點連接，**連線 | 存取點 > 3G/4G/LTE WWAN** 頁面可提供有關該裝置的監控資訊。

第一個面板提供連線資料和數據機狀態，第二個面板則以圖表呈現裝置的訊號強度。

按一下「重新整理」按鈕即可重新整理面板中的資料。

如果沒有在存取點上偵測到 3G/4G/LTE 裝置，**連線 | 存取點 > 3G/4G/LTE WWAN** 頁面會顯示以下訊息:

SonicPoint/SonicWave 3G/4G/LTE 設定

SonicPoint/SonicWave 可連接到 3G/4G/LTE 裝置以提供 WAN 連線。

SonicPoint/SonicWave 3G/4G/LTE 狀態

- 未偵測到任何裝置。

第 4 部分

無線

- 無線概述
- 設定無線設定
- 設定無線安全
- 設定進階無線設定
- 無線 MAC 篩選條件清單
- 設定無線 IDS
- 設定使用內部無線的虛擬存取點

26

無線概述

SonicWall 無線安全裝置支援 IEEE 802.11a, 802.11ac、802.11b、802.11g 和 802.11n 無線通訊協定，並通過無線傳輸傳送資料，這種傳輸一般稱為 WI-FI 或無線。SonicWall 無線安全裝置結合三個網路元件，提供完全安全的無線防火牆: 存取點、安全無線閘道及狀態防火牆 (具備靈活的 NAT 和 VPN 終端和啟動功能)。透過這種組合，無線安全裝置提供了無線靈活性，但並未降低網路的安全性。

通常，無線安全裝置是無線 LAN 的存取點，並作為 LAN 中電腦的中央存取點。此外，它還與網路中電腦共用相同的寬頻連接。由於無線安全裝置還提供防火牆防護，來自網際網路的入侵者無法存取您網路中的電腦或檔案。對於「始終開啟」的連接，例如由網路中電腦共用的 DSL 或 T1 線路，這一點尤為重要。

但是，無線 LAN 容易受到其他無線網路「竊聽」，這表示您應該為無線 LAN 建立無線安全原則。在無線安全裝置中，無線用戶端連接到防火牆的存取點層。無線流量並非直接橋接到有線網路，而是首先傳送到安全無線閘道層，在此需要用戶端通過使用者級別身分驗證。對來賓服務和 MAC 篩選條件清單的無線存取由無線安全裝置管理。如果符合所有安全條件，無線網路流量就會通過以下一種指派系統傳送：

- LAN
- WAN
- WLAN 上的無線用戶端
- Opt 連接埠上的 DMZ 或其他區域
- VPN 通道

主題：

- FCC U-NII 新規則合規
- 使用無線連接的考慮事項
- 最佳化無線效能建議
- 調節天線
- 無線節點計數實施
- MAC 篩選條件清單

裝置支援

SonicOS 支援的無線裝置包括:

- TZ 500W
- TZ 400W
- TZ 300W
- SOHO W

合規性

無線裝置需遵從各種要求，才能在特定區域銷售和使用這些裝置。如需 SonicWall 無線裝置的監管機關核准和限制的最新資訊，請參閱 https://www.sonicwall.com/support 中的「產品文件」頁面。每個裝置都有提供相關資訊的唯一監管文件或*入門指南*。

FCC U-NII 新規則合規

自 SonicOS 6.2.5.1 開始，TZ 系列和 SOHO 無線裝置支援 FCC U-NII（未獲授權 - 國家資訊基礎設施）新規則（報告和順序 ET 案卷編號 13-49)。為符合 FCC 新規則中的動態頻率選擇 (DFS)，TZ 系列或 SOHO 無線裝置偵測並避免干擾 DFS 頻段雷達信號。

附註：僅有 SonicOS 6.2.5.1 及更高版本支援有符合 FCC 新規則的韌體的 TZ 系列和 SOHO 無線裝置。

RED 合規性

自 SonicOS 6.5 起，TZ 系列和 SOHO 無線裝置支援無線電設備指令 (RED)。RED (2014/53/EU) 對安全性與執行狀況、電磁相容性和無限頻譜的有效使用制定了基本要求。

使用無線連接的考慮事項

評估無線與有線連接時，可考慮為您的基礎結構和環境帶來的優點與缺點:

行動性	使用您網路的是否大部分為筆記型電腦? 無線比有線連接更具便攜性。
便利性	無線網路不需要對個別電腦或開放式電腦機箱佈線即可安裝網路卡。
速度	如果網速對您很重要，您可能需要考慮使用乙太網路連接，而不是無線連接。
範圍和覆蓋率	如果您的網路環境包含許多實體障礙物或干擾因素，無線網路可能不是您的最佳選擇。
安全性	無線網路具有無限制無線傳送的特性，因此存在固有的安全問題。但是，無線安全裝置是防火牆，且擁有提供安全性的 NAT 功能，而且您可以使用 WPA 或 WPA2 保障資料傳送的安全。

最佳化無線效能建議

SonicWall 提供以下建議，有助於達到最佳無線效能:

- 將無線安全裝置放在所需網路的中央。這可透過鄰近的無線網路降低遭竊聽的風險。
- 最大限度減少無線安全裝置與接收點（例如 PC 或膝上型電腦）之間的牆壁或天花板數。
- 嘗試將無線安全裝置放置在與其他無線元件呈直線的位置。當無線元件彼此呈直線時可以達到最佳效能。
- 建築結構可能會影響無線效能。
    - 避免將無線安全裝置放置在牆壁、壁爐或其他較大固體附近。
    - 將無線安全裝置放置在電腦機箱、監視器和電器等金屬物體附近會影響裝置的效能。

    - 如果無線安全裝置安裝在金屬框、UV 窗膜、混凝土或砌石牆及金屬漆等類型的材料附近，會降低信號強度。
- 在高處安裝無線安全裝置有助於避開障礙物和改善建築物高層的效能。
- 鄰接的無線網路和裝置會影響信號強度、速度和無線安全裝置的範圍。
- 無線電話、收音機、微波爐和電視機等裝置可能對無線安全裝置造成干擾。

調節天線

可以調節無線安全裝置上的天線，已獲得最佳無線接收效果。首先將天線垂直指向上，然後根據需要調節。注意在某些區域，例如在無線安全裝置正下方的區域，接收效果相對較差。將天線直指向其他無線裝置不會改善接收效果。請勿將天線放置在金屬門或牆壁附近，因為這會造成干擾。

無線節點計數實施

連接到 WLAN 或通過 SonicWall GroupVPN 連接的使用者，不會計入 SonicWall 無線網路裝置上的節點實施。只將 LAN 上和 Opt 連接埠上的非無線區域的使用者計入節點限值。

「工作站狀態」表列出所有連接的無線節點。

MAC 篩選條件清單

SonicWall 無線安全裝置網路通訊協定提供原生 MAC 位址篩選功能。在啟用 MAC 位址篩選時，會在 802.11 層進行篩選，封鎖無線用戶端進行身分驗證和與無線存取點關聯。由於無法不經過身分驗證和關聯進行資料通訊，因此無法授予存取網路的權限，直至用戶端向網路管理員提供其無線網路卡的 MAC 位址。

27

設定無線設定

您可將無線裝置設為存取點、無線用戶端橋接或存取點和工作。

設定 802.11 無線天線設定的步驟如下:

1 導覽至**管理**檢視，選擇**連線 | 無線 > 基本設定**。

2 選擇希望無線裝置執行的**無線角色**。

重要：從一種模式切換到另一種模式會導致用戶端掉線，之後需要重新啟動。

附註：頁面上的選項會根據您選擇的**無線角色**而改變。

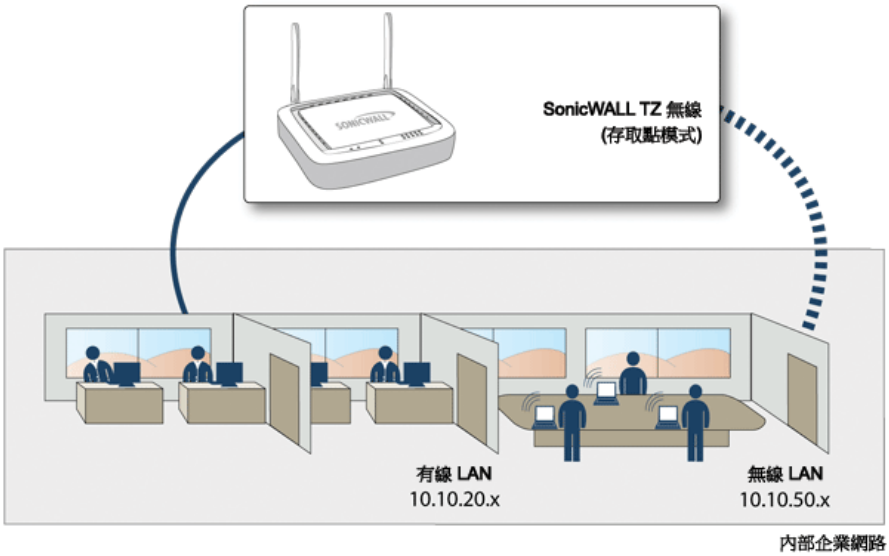
下列章節說明如何針對各**無線角色**選項設定裝置:

- 存取點
- 無線橋接
- 存取點與工作站

存取點

為**無線角色**選擇**存取點**，會將 SonicWall 設為無線用戶端的網際網路/網路閘道，如下圖所示:

無線傳送模式：存取點



主題：

- 存取點無線設定
- 存取點無線虛擬存取點

存取點無線設定

重要：將無線裝置設為存取點時，您有責任遵守所有為規範調控網域及/或有關無線電操作地區而制定的法令。

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 基本設定**。

3 在**無線角色**欄位中，從下拉功能表選擇**存取點**。

4 勾選方塊以**啟用 WLAN 無線**。如此一來可為行動使用者提供安全的無線存取。按一下**套用**，此設定隨即生效。WLAN 無線預設為停用。

5 在**排程**欄位中，從下拉功能表選擇 WLAN 無線進入使用中狀態的時間。「排程」清單顯示了您在**系統安裝 | 裝置 > 系統排程**頁面建立和管理的排程物件。預設值為**始終開啟**。

6 在**國家或地區代碼**欄位中，選擇使用裝置時所在的國家或地區。國家或地區代碼可確定無線操作由哪個法規區域監管。

7 從**無線模式**欄位中，從下拉功能表選擇慣用的的無線模式。無線安全裝置支援以下模式：

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

- **802.11n/a/ac 混合模式** - 如果 802.11a、802.11ac 和 802.11n 用戶端存取您的無線網路，則選擇此模式。
- **802.11ac 單一模式** - 如果僅 802.11ac 用戶端存取您的無線網路，則選擇此模式。

無線模式	定義
2.4GHz 802.11n/g/b 混合模式	同時支援 802.11b、802.11g 和 802.11n 用戶端。如果無線網路包含多種類型的用戶端，請選擇此模式。
僅 2.4GHz 802.11n	僅允許 802.11n 用戶端存取您的無線網路。802.11a/b/g 用戶端不能在此受限的無線模式下連接。
2.4GHz 802.11g/b 混合	同時支援 802.11g 和 802.11b 用戶端。如果您的無線網路包含這兩種類型的用戶端，請選擇此模式。
僅 2.4GHz 802.11g	如果您的無線網路僅包含 802.11g 用戶端，則選擇此模式，以提高 802.11g 的效能。如果想要避免 802.11b 用戶端關聯，也可以選擇此模式。
5GHz 802.11n/a 混合	如果 802.11a 和 802.11n 用戶端存取您的無線網路，則選擇此模式。
僅 5GHz 802.11n	如果僅 802.11n 用戶端存取您的無線網路，則可選擇此模式。
5GHz 802.11a 單一模式	如果僅 802.11a 用戶端存取您的無線網路，則可選擇此模式。
5GHz 802.11n/a/ac 混合模式	如果 802.11a、802.11n 和 802.11ac 用戶端存取您的無線網路，則選擇此模式。
5GHz 802.11ac 單一模式	如果想提高傳送量，請選擇此模式。

「無線設定」區段中的其餘選項可能根據您選擇的無線模式而改變。

主題：

- 802.11n 無線設定
- 802.11a/b/g 無線設定
- 802.11ac 無線設定

802.11n 無線設定

當**無線模式**欄位設定為僅支援 802.11n 的模式或包含 802.11n 的混合模式，請設定以下選項:

附註：根據設定所設定的裝置類型，顯示的選項可能有些微差異。

無線頻段	設定 802.11n 無線的頻帶
自動	使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。這是預設值。

標準 - 20 MHz 頻道	指定 802.11n 無線將僅使用標準 20 MHz 頻道。選定此選項後，將顯示**標準通道**下拉功能表
標準通道	此項預設為**自動**，使裝置可以根據訊號強度和完整性設定最佳頻道。您可以在調控網域範圍內選擇單個頻道。選擇特定的頻道還可幫助裝置避免受到此區域內其他無線網路的干擾。
寬 - 40 MHz 頻道	指定 802.11n 無線將僅使用寬頻 40 MHz 頻道。選定此選項後， 將顯示**主要通道**和**輔助通道**下拉功能表：
主要通道	此項預設為**自動**，您也可指定主要頻道。
次要通道	此下拉功能表的設定取決於您所選擇的主要頻道: • 如果主要通道設定為「自動」，則輔助通道也將設定為「自動」。 • 如果主要通道設定為某個特定的頻道，則次要通道將設定為可以避免受主要通道干擾的最佳頻道。
啟用短期保護間隔	啟用此項以使用更高的 Tx/Rx 率 (若支援)。僅適用於 802.11ac/n 模式。
啟用彙總	啟用 802.11n 框架彙總，將多個框架結合到一起以減少開銷並增加傳送量。僅適用於 802.11ac/n 模式。
啟用 WDS AP	允許 WDS 用戶端連接到此存取點。
SSID	系統會填入預設值 **sonicwall-** 加上 BSSID 的最後四個字元；例如 `sonicwall-C587`。可將 SSID 變更為任何英數字元值，最多包含 32 個字元。

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

802.11a/b/g 無線設定

當**無線模式**欄位設定為僅支援 802.11a、802.11g/b 混合或僅支援 802.11b 的模式，請設定以下顯示的選項:

頻道	使裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。這是預設值。您可以在調控網域範圍內選擇單個頻道。
啟用 WDS AP	允許 WDS 用戶端連接到此存取點。
SSID	系統會填入預設值 **sonicwall-** 加上 BSSID 的最後四個字元；例如 `sonicwall-C587`。可將 SSID 變更為任何英數字元值，最多包含 32 個字元。

802.11ac 無線設定

僅對 802.11ac 設定無線時，將顯示以下選項：

- 「無線頻段」下拉功能表 - 為 802.11ac 無線設定頻段，以便支援頻寬 - 80MHz 頻道。
- 從**通道**下拉功能表 - 選擇通道：
  - **自動** - 使無線安全裝置可以根據訊號的強度和完整性自動偵測和設定無線操作的最佳頻道。預設頻道設定為**自動**，將在右側顯示所選的操作頻道。此外，可以明確定義您的法規區域範圍內的操作頻道。
  - 特定的頻道 - 如需可用頻道的資訊，請參閱佈建設定檔的無線 0/1 基本設定。

存取點無線虛擬存取點

若使用無線虛擬存取點，在**無線虛擬存取點**區段中，從下拉功能表選擇**虛擬存取點群組**。您也可選擇先前定義的虛擬存取點群組。

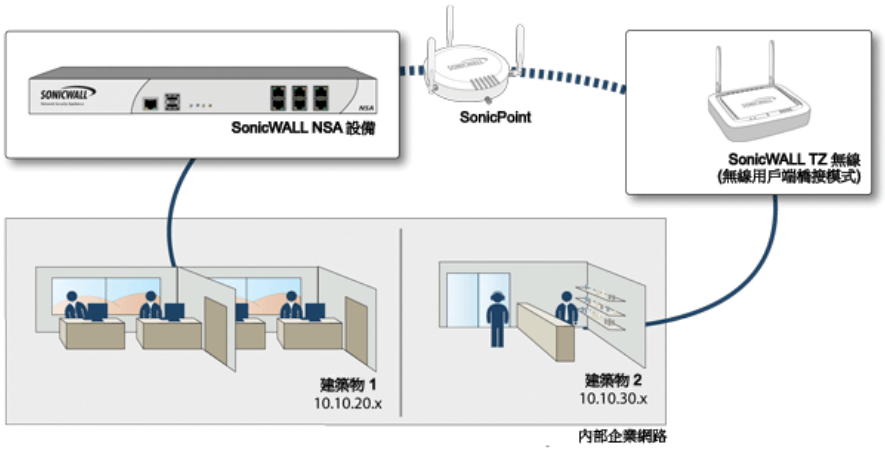
完成所有存取點設定後，按一下**接受**儲存設定。

無線橋接

無線裝置會藉由無線橋接至另一個 SonicWall 無線裝置或 SonicPoint 存取點來提供網際網路/網路存取，詳情請參閱無線傳送模式：無線橋接。選擇**無線用戶端橋接**作為**無線角色**，允許實體分離的位置之間的安全網路通訊，而無需連接長而昂貴的乙太網路纜線。

附註：如果無線虛擬存取點處於使用中狀態，裝置便無法作為無線用戶端橋接使用。

無線傳送模式：無線橋接



附註：如需無線橋接的更多資訊，請參閱 http://www.SonicWall.com/us/support.html 提供的 *SonicWall 安全無線網路整合解決方案指南*或 *SonicWall 無線橋接技術注釋*。

主題：

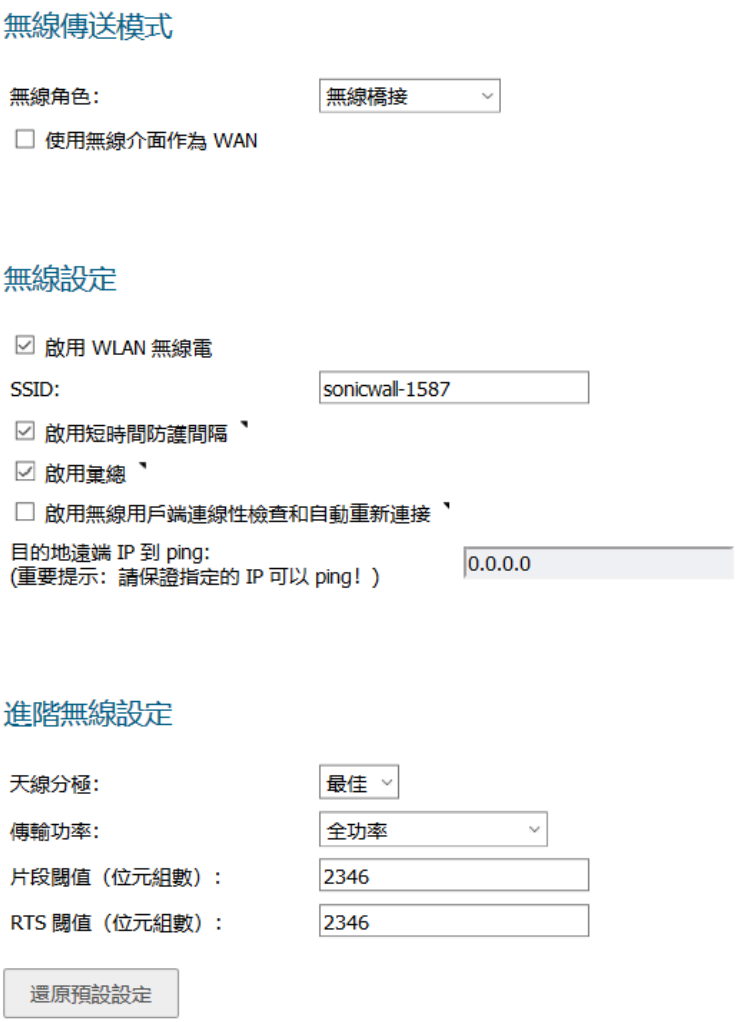
- 用戶端橋接無線設定
- 用戶端橋接進階無線設定

用戶端橋接無線設定

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 基本設定**。

3 在**無線角色**欄位中，從下拉功能表選擇**無線用戶端橋接** 。



4 若要**使用無線介面作為 WAN**，請勾選方塊。預設值為不勾選。

5 在**無線設定**區段下，勾選方塊以**啟用 WLAN 無線**。在「用戶端橋接」模式中，無線啟用後會作為用戶端而非存取點，且不會提供無線存取給用戶端。按一下**套用**，此設定隨即生效。WLAN 無線預設為停用。

6 選擇以下選項

SSID	系統會填入預設值 **sonicwall-** 加上 BSSID 的最後四個字元；例如 `sonicwall-C587`。可將 SSID 變更為任何英數字元值，最多包含 32 個字元。
啟用短期保護間隔	啟用此項以使用更高的 Tx/Rx 率 (若支援)。僅適用於 802.11ac/n 模式。
啟用彙總	啟用 802.11n 框架彙總，將多個框架結合到一起以減少開銷並增加傳送量。僅適用於 802.11ac/n 模式。
啟用無線用戶端連線檢查與自動重新連接	對使用者定義的 IP 位址執行 ping，以便定期檢查無線用戶端連線。若連接中斷，系統會自動重新連接。
要執行 ping 的目標遠端 IP	若在上述步驟中啟用了連線檢查功能，請輸入要執行 ping 的遠端 IP 位址。 重要：確保指定的 IP 位址可執行 ping。

用戶端橋接進階無線設定

設定進階無線設定的步驟如下:

1 設定**天線分極**。預設值為**最佳**。

2 下拉功能表中選擇傳輸功率:

- **全功率**會在 WLAN 上傳送最強的訊號。例如，如果訊號在建築物之間穿行，則選擇**全功率**。
- **半功率 (-3 dB)** 推薦在建築物內部的辦公室間使用。
- **四分之一功率 (6 dB)** 建議用於距離較短的通訊。
- **八分之一功率 (-9 dB)** 推薦用於較短距離的通訊。
- **最小功率**推薦用於很短距離的通訊。

3 指定**分段閾值 (位元組數)**。最小值為 **256**，最大值為 **2346**。預設為最大值。

4 設定 **RTS 閾值 (位元組數)**。最小值為 **1**，最大值 (預設值) 為 **2346**。

5 按一下**接受**儲存設定。

按一下**還原預設值**即可還原為出廠預設值。

存取點與工作站

當有兩部以上主機需透過 802.11 通訊協定互相連接，但距離太遠而無法建立直接連線，就會使用無線中繼器來橋接缺口。

SonicWall 無線安全裝置提供存取點和橋接模式。處於**存取點與工作站**模式時，建立為工作站的虛擬存取點可連接至另一個存取點。其他虛擬存取點則作為一般存取點使用。換句話說，設定為**存取點與工作站**的裝置會在中繼器模式下運作。在此模式下，您也可設定虛擬介面，讓工作站虛擬存取點作為 WAN 介面使用。

無線分散系統 (WDS) 可用於連接多個存取點。存取點可藉由 WDS 以標準化方式互相通訊，無需纜線。若要為漫遊用戶端和針對管理多個無線網路提供流暢的體驗，此功能相當重要，且此功能也可透過減少需要的纜線數量來簡化網路架構。

若要將無線裝置設定為存取點與工作站，請參考以下章節定應選項:

- 存取點與工作站無線設定
- 存取點與工作站無線虛擬存取點
- 工作站設定

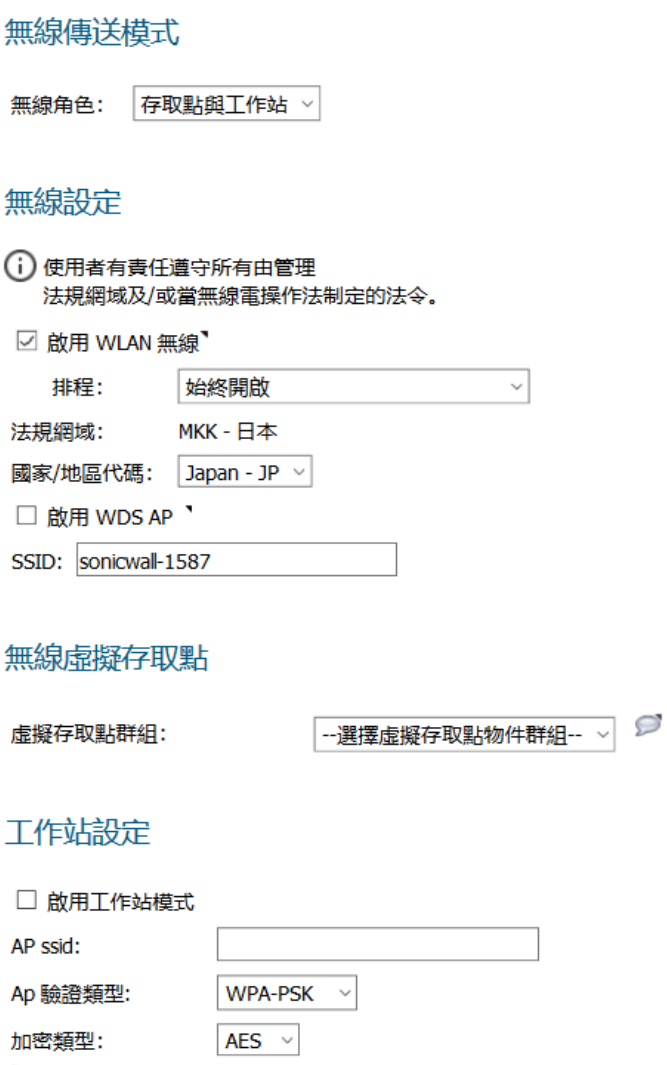
存取點與工作站無線設定

重要：將無線裝置設為存取點與工作站時，您有責任遵守所有為規範調控網域及/或有關無線電操作地區而制定的法令。

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 基本設定**。

3 在**無線角色**欄位中，從下拉功能表選擇**存取點與工作站**。



4 勾選方塊以**啟用 WLAN 無線**。如此一來可為行動使用者提供安全的無線存取。按一下**套用**，此設定隨即生效。WLAN 無線預設為啟用。

5 在**排程**欄位中，從下拉功能表選擇 WLAN 無線進入使用中狀態的時間。除了系統提供的選項，「排程」清單還會顯示您在**系統安裝 | 裝置 > 系統排程**頁面建立和管理的排程物件。預設值為**始終開啟**。

6 在**國家或地區代碼**欄位中，選擇使用裝置時所在的國家或地區。國家或地區代碼可確定無線操作由哪個法規區域監管。

7 勾選方塊以**啟用 WDS AP**。這會允許 WDS 用戶端連接到這部充當存取點的裝置。

8 確認 **SSID** 欄位填寫正確。系統會填入預設值 **sonicwall-** 加上 BSSID 的最後四個字元；例如 `sonicwall-C587`。可將 SSID 變更為任何英數字元值，最多包含 32 個字元。

9 按一下**接受**儲存設定。

存取點與工作站無線虛擬存取點

若使用無線虛擬存取點，在**無線虛擬存取點**區段中，從下拉功能表選擇**虛擬存取點群組**。您也可選擇先前定義的虛擬存取點群組。

完成所有存取點設定後，按一下**接受**儲存設定。

工作站設定

設定工作站設定的步驟如下:

1 勾選**啟用工作站模式**。

2 在指定欄位中輸入 **AP ssid**。

3 從下拉功能表中選擇 Ap 驗證類型。選擇以下其中一項:

- 開啟
- WPA-PSK
- WPA2-PSK

4 從下拉功能表中選擇**加密類型**。

5 輸入**預先共用密碼**。

6 從下拉功能表中選擇 **VLAN ID**。

7 若要**使用無線介面作為 WAN**，請勾選方塊。

8 若要**啟用 WDS 工作站**，請勾選方塊。

9 按一下**接受**儲存設定。

28

設定無線安全

在**連線 | 無線 > 安全**頁面上，為無線裝置設定驗證和加密設定。根據您選擇的驗證類型，顯示的選項會有所不同。

主題：

- 第 224 頁「關於驗證」
- 第 227 頁「WPA2 EAP 和 WPA EAP 設定」
- 第 225 頁「設定 WEP 設定」

關於驗證

下表說明驗證類型:

驗證類型

類型	功能和使用
WEP (有線等效通訊協定)	• 經由無線網路保護資料 • 通過 SonicWall 裝置後便不再提供保護 • 為傳送的資料提供最低限度的保護。 • 為加密使用固定金鑰 • 適用於較舊型裝置、PDA、無線印表機 • 不建議需要高度安全性的部署使用
WPA (Wi-Fi 安全存取)	• 良好的安全性（使用 TKIP） • 用於與受信任的公司無線用戶端配合使用 • 使用 Windows 登入進行透明驗證 • 大多數情況下不需要用戶端軟體 • 需使用 RADIUS 等單獨的驗證通訊協定進行使用者驗證 • 使用動態金鑰 **附註：** 只有在已於診斷頁面上啟用這個功能的情況下，才會顯示此選項。
WPA2 (Wi-Fi 安全存取第 2 版)	• 最佳的安全性（使用 AES） • 用於與受信任的公司無線用戶端配合使用 • 使用 Windows 登入進行透明驗證 • 某些情況下可能需要安裝用戶端軟體 • 支援 802.11i WPA/WPA2 EAP 驗證模式。 • 首次登入後無需背景驗證 • 支援兩種儲存和產生金鑰的通訊協定: PSK (預先共用密碼) 和 EAP (可擴充驗證通訊協定) **附註：** 僅於存取點模式下 (在**連線 | 無線 > 基本設定**頁面上選擇) 提供 EAP 支援。橋接模式不支援 EAP。
WPA2-AUTO	• 嘗試使用 WPA2 安全連接。 • 如果用戶端不支援 WPA2，連接會預設為 WPA。

設定 WEP 設定

驗證類型選擇了其中一個 WEP 選項時，可設定以下選項。

針對 WEP 驗證設定無線裝置的步驟如下:

1 導覽至**連線 | 無線 > 安全**頁面。

2 從**驗證類型**下拉功能表中選擇相應的身分驗證類型。

- **WEP - 兩者皆是（開放系統和共用密碼）**（預設）只要各欄位使用相同的金鑰，則**預設金鑰**的指派不重要。
- **WEP - 開放系統**：在開放系統身分驗證中，防火牆允許不經過身分驗證進行無線用戶端存取。所有 Web 加密設定將以灰色顯示且無法選擇。
- **WEP - 共用金鑰**：使用 WEP 並需要在允許身分驗證之前向無線用戶端分發共用密碼。如果選擇了**共用密碼**，則**預設金鑰**指派很重要。

3 從**預設金鑰**下拉功能表中，選擇哪個金鑰是預設金鑰：**金鑰 1**、**金鑰 2**、**金鑰 3** 或**金鑰 4**。

4 在**金鑰項目**選項中，選擇您的金鑰是**英數字元**還是**十六進位 (0-9, A-F)**：

5 最多可以在指定欄位中輸入四個金鑰。對於每個金鑰，選擇 **64 位元**、**128 位**或 **152 位**。位元數越多，金鑰越安全。請參閱下表，瞭解各類型金鑰所需的字元數。

金鑰類型

金鑰類型	WEP - 64 位元	WEP - 128 位元	WEP - 152 位元
英數字元	5 個字元	13 個字元	16 個字元
十六進位 (0-9, A-F)	10 個字元	26 個字元	32 個字元

6 按一下**接受**。

設定 WPA2 PSK 和 WPA PSK 設定

驗證類型選擇了其中一個 WPA PSK 選項時，可定義以下設定。

使用預設共用密碼針對 WPA 驗證設定無線裝置的步驟如下:

1 導覽至**連線 | 無線 > 安全**頁面。

2 從**驗證類型**下拉功能表中選擇相應的身分驗證類型。

- **WPA2 - PSK**: 使用 WPA2 和預設驗證金鑰進行連接。
- **WPA2 - Auto - PSK**: 自動嘗試使用 WPA2 和預設驗證金鑰進行連接，但如果用戶端不支援 WPA2，就會切換回 WPA。

3 從下拉功能表中選擇 **EAPOL 版本**設定:

- **V2** (預設) - 選擇第 2 版。這提供比版本 1 更好的安全性，但有些無線用戶端可能不支援。
- **V1** - 選擇第 1 版通訊協定。

4 在 **WPA2/WPA 設定**區段指定以下設定:

- **加密類型** - 選擇 TKIP。*臨時金鑰完整性通訊協定* (TKIP) 是按封包實施金鑰完整性的通訊協定，但是其安全性和傳送量較低。加密類型選項還有「AES」和「自動」。
- **群組金鑰更新** - 指定 SonicWall 安全裝置何時更新金鑰。選擇**逾時**在指定的間隔秒數後產生新群組金鑰；此為預設選項。使用固定金鑰時，請選擇**停用**。
- **間隔** - 如果在**群組金鑰更新**欄位中選擇了**逾時**，則輸入 WPA 自動產生新群組金鑰前的秒數。預設值為 **86400** 秒。如果您將**群組金鑰更新**選擇為**停用**，將不再顯示此選項。

5 在**密碼**欄位輸入用於產生金鑰的密碼。

6 按一下**接受**儲存並套用設定。

WPA2 EAP 和 WPA EAP 設定

驗證類型選擇了其中一個 WPA EAP 選項時，可定義以下設定。

使用預設共用密碼針對 WPA 驗證設定無線裝置的步驟如下:

1 導覽至**連線 | 無線 > 安全**頁面。

2 從**驗證類型**下拉功能表中選擇相應的身分驗證類型。

- **WPA2 - EAP**: 使用 WPA2 和可擴充驗證通訊協定進行連接。
- **WPA2 - Auto - EAP**: 自動嘗試使用 WPA2 和可擴充驗證通訊協定進行連接，但如果用戶端不支援 WPA2，就會切換回 WPA。

附註：僅於存取點模式下提供 EAP 支援，用戶端橋接模式不提供支援。

3 從下拉功能表中選擇 **EAPOL 版本**設定:

- **V1** - 選擇通過 LAN 版本 1 的可擴充的驗證通訊協定。
- **V2** - 選擇通過 LAN 版本 2 的可擴充的驗證通訊協定。這提供比版本 1 更好的安全性，但有些無線用戶端可能不支援。

4 在 **WPA2/WPA 設定**區段指定以下設定:

- **加密類型** - 選擇 TKIP。*臨時金鑰完整性通訊協定* (TKIP) 是按封包實施金鑰完整性的通訊協定，但是其安全性和傳送量較低。加密類型選項還有「AES」和「自動」。
- **群組金鑰更新** - 指定 SonicWall 安全裝置何時更新金鑰。選擇**逾時**在指定的間隔秒數後產生新群組金鑰；此為預設選項。使用固定金鑰時，請選擇**停用**。
- **間隔** - 如果在**群組金鑰更新**欄位中選擇了**逾時**，則輸入 WPA 自動產生新群組金鑰前的秒數。預設值為 **86400** 秒。如果您將**群組金鑰更新**選擇為**停用**，將不再顯示此選項。

5 在**可擴充驗證通訊協定設定 (EAP)** 區段中指定以下設定:

- **Radius 伺服器重試** - 輸入驗證的嘗試次數。預設為 **4**。
- **重複嘗試間隔 (秒)** - 輸入兩次重試之間等待的時間。預設值為 **0**（無延時）。
- **Radius 伺服器 1 IP** 和**連接埠** - 輸入主要 RADIUS 伺服器的 IP 位址和連接埠號。
- **Radius 伺服器 1 金鑰** - 輸入用於存取 Radius 伺服器的密碼
- **Radius 伺服器 2 IP** 和**連接埠** - 輸入次要 RADIUS 伺服器（如有）的 IP 位址和連接埠號。
- **Radius 伺服器 2 金鑰** - 輸入用於存取 Radius 伺服器的密碼

6 按一下**接受**套用 WPA2 EAP 設定。

29

設定進階無線設定

您可在「進階設定」上自訂無線裝置的各種功能。只有在防火牆作為存取點使用時才可使用此頁面。

主題：

- 訊號傳送和 SSID 控制
- 綠色存取點
- 進階無線設定
- 設定天線分極

訊號傳送和 SSID 控制

若要設定訊號傳送和 SSID 控制：

1 導覽至**管理**。

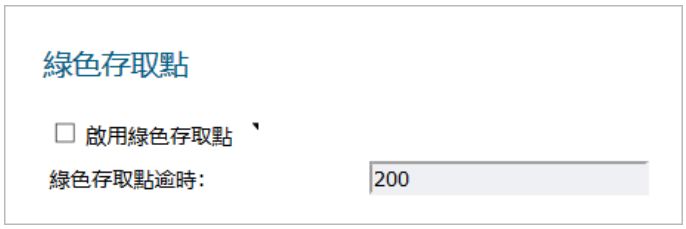
1 選擇**連線 | 無線 > 進階設定**頁面。

2 選擇**隱藏信標中的 SSID**，即可隱藏 SSID 名稱的廣播並停用對探查請求的回應。勾選此選項有助於防止未授權的無線用戶端看到您的無線 SSID。預設停用此設定。

3 輸入**信標間隔**的毫秒數。縮短間隔時間將使被動掃描更可靠、更快，因為訊號框架更頻繁地宣告網路為無線連接。預設值為 **200** 毫秒。

4 按一下「接受」儲存變更。按一下「還原預設值」即可還原為出廠預設值。

綠色存取點



若要設定電源效率：

1 若要提高電源效率，請選擇**啟用綠色存取點**。預設停用此設定。

2 在**綠色存取點逾時**欄位中指定逾時的數字。預設為 **200**。

3 按一下「接受」儲存變更。按一下「還原預設值」即可還原為出廠預設值。

進階無線設定

若要設定進階無線設定：

1 如果您預期只有 802.11g 流量，則選擇**啟用短插槽時間**提高效能。802.11b 與短時間槽不相容。預設停用此設定。

2 從**天線接收分極**下拉功能表中選擇無線安全裝置使用哪個天線傳送和接收資料。如需天線分極的詳細資訊，請參閱設定天線分極。預設為**最佳**。

3 從**傳輸功率**下拉功能表，選擇：

- **全功率**在 WLAN 上傳送最強的訊號。例如，如果訊號在建築物之間穿行，則選擇**全功率**。
- **半功率 (-3 dB)** 推薦在建築物內部的辦公室間使用。
- **四分之一功率 (-6 dB)** 推薦用於較短距離的通訊。
- **八分之一功率 (-9 dB)** 推薦用於較短距離的通訊。
- **最小功率**推薦用於很短距離的通訊。

4 從**初始長度**下拉功能表中，選擇**短**或**長**。**短**推薦用於提高無線網路的效率和傳送量。預設為**長**。

5 指定**分段閾值 (位元組數)**。最小值為 256，最大值為 2346，預設值為 **2346**。

您可將無線框架分段，以提高存在 RF 干擾或無線覆蓋不佳的區域內的可靠性和傳送量。較低的閾值數會產生較多的片段。增加此值意味著使用更低的費用傳送框架，但必須放棄和重新傳送損失或損壞的框架。

6 在 **RTS 閾值 (位元組數)** 欄位中指定請求傳送 (RTS) 的閾值。最小值為 1，最大值為 2347，預設值為 **2346**。

此欄位為封包大小（以位元組計）設定閾值，RTS 將在封包傳送前以此閾值傳送。傳送一個 RTS 可確保當多個用戶端處於同一個存取點的範圍（但彼此不再對方範圍內）的情況下不會出現無線衝突。如果網路傳送量慢或發生重新傳送大量框架的情況，則降低 RTS 閾值以啟用 RTS 清除。

7 在 **DTIM 間隔**欄位中指定 DTIM（傳送指示訊息）間隔。最小值為 1，最大值為 256，預設值為 **1**。

對於傳入多點傳送封包的 802.11 省電模式用戶端，DTIM 間隔指定在傳送 DTIM 之前等待的信標框架數。增加 DTIM 間隔值允許更高效地儲存功率。

8 在**連接逾時（秒數）**欄位中輸入用戶端關聯的秒數。預設值是 **300** 秒，容許範圍是 60 到 36000 秒。如果您的網路繁忙，可以透過增加此欄位中的秒數來提高逾時值。

9 為使用此設定檔的每個 SonicPoint 輸入**最大用戶端關聯數**。最小值為 1，最大值為 128，預設值為 128。此設定限制一次可以無線連接的工作站數。

10 從**資料速率**下拉功能表 - 選擇傳送和接收資料的速度。**最佳**選項可自動選擇在有干擾和其他因素的情況下您的區域中的最佳可用速率。或者您可以從 **1 Mbps** 到 **54 Mbps** 範圍內的選項中手動選擇資料速率。

11 從**保護模式**下拉功能表中，選擇保護模式：**無**、**一律**或**自動**。

防護可以減少衝突，尤其是在您有兩個重疊的 SonicPoints 時。但是，這會降低效能。**自動**可能是最佳設定，因為它僅在有重疊的 SonicPoint 時啟用。

12 從下拉功能表中選擇**保護速率**: **1 Mbps**、**2 Mbps**、**5 Mbps** 或 **11 Mbps**。保護速率決定了開啟保護模式的資料速率。最低的速率提供最高的防護級別，但資料傳送速率也最低。

13 從**保護類型**下拉功能表中，選擇用於建立無線連接的訊號交換類型：**僅 CTS**（預設）或 **RTS-CTS**。

附註：802.11b 流量僅與 **CTS** 相容。

14 按一下「接受」儲存變更。按一下「還原預設值」即可還原為出廠預設值。

設定天線分極

無線 SonicWall 安全裝置採用執行分集模式的雙 5 dBi 天線。預設實施分集模式意味著一個天線用於傳送，兩個天線均可能用作接收天線。由於無線訊號到達安全無線裝置的兩個天線，評估其訊號強度和完整性，然後使用收到的最佳訊號。兩個天線之間的選擇過程貫穿於整個操作期間，以始終提供最佳的訊號。為了允許使用外部（更高增益的單向）天線，可以停用天線分極。

SonicWall NSA 220 和 250M 無線安全裝置採用三個天線。將天線分極預設設為**最佳**，這是此類裝置的唯一設定。

天線分極設定決定了無線安全裝置使用哪個天線傳送和接收資料。**最佳**是預設值。選擇此項後，無線安全裝置將自動選擇訊號最強、最清晰的天線。

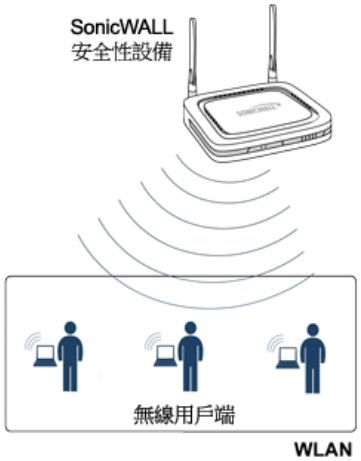
30

無線 MAC 篩選條件清單

無線網路提供原生 MAC 篩選功能，用於防止無線用戶端進行身分驗證和關聯無線安全裝置。如果在 WLAN 上實施 MAC 篩選，無線用戶端必須向您提供其無線網路卡的 MAC 位址。SonicOS 無線 MAC 篩選條件清單用於設定無線網路允許或拒絕存取的用戶端的清單。如果沒有 MAC 篩選，任何無線用戶端只要知道 SSID 或其他安全參數，便可以「破解」並加入您的無線網路。

以下說明典型的 234 MAC 篩選條件清單部署情境:

典型的 SonicWall MAC 篩選條件清單佈局



主題：

- 部署注意事項
- 設定無線 > MAC 篩選條件清單

部署注意事項

部署 MAC 篩選條件清單時考慮以下事項：

- 對於 SonicPoint-N 裝置，此功能需要閘道才能儲存 MAC 篩選條件清單的設定。
- 對於 SonicWall TZ 系列裝置的內部無線功能，需要將有些成員新增到 VAP 結構以儲存 MAC 篩選條件清單設定，且應該修改全部功能以根據驅動程式設定。
- 虛擬存取點可設定自己的 MAC 篩選條件清單，或是繼承在**連線 | 無線 > MAC 篩選條件清單**頁面上設定的全域設定。

設定無線 > MAC 篩選條件清單

設定 MAC 篩選條件清單的步驟如下:

1 選擇**管理**檢視。

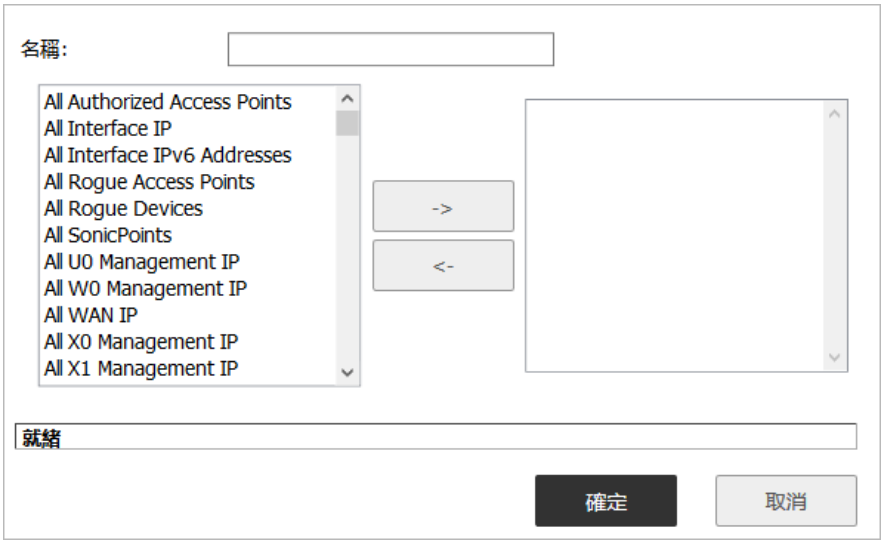
2 在**連線**底下，選擇**無線 > MAC 篩選條件清單**。

3 按一下**啟用 MAC 篩選條件清單**核取方塊。預設停用此設定。

4 從**允許清單**下拉功能表，選擇您要允許的位址群組。**所有 MAC 位址** (預設)、**預設 ACL 允許群組**或您建立的群組。

5 從**拒絕清單**下拉功能表，選擇您要拒絕的位址群組。「無 MAC 位址」(預設)、「預設 ACL 拒絕群組」或您建立的群組。

6 若要將新的位址物件新增至允許或拒絕清單，請從**允許清單**或**拒絕清單**下拉功能表中選擇**建立新 MAC 位址物件群組...**。



a 在**名稱：**文字欄位中，輸入新群組的名稱。

b 在左側列中，選擇要允許或拒絕的群組或各位址物件。您可以使用 **Ctrl 加點按**同時選擇多項。

c 按一下 -**向右 ->** 按鈕向群組新增項目。

d 按一下**確定**。將在下拉功能表顯示位址以供選擇。

e 若需要則選擇該物件。

7 按一下**接受**按鈕。

31

設定無線 IDS

主題：

- 關於無線 IDS
- 設定 IDS 設定

關於無線 IDS

無線入侵偵測服務 (IDS) 大幅增強了 SonicWall 無線安全裝置的安全功能，讓裝置可識別最常見的不正當無線活動類型並採取應對措施。無線 IDS 包含三種服務類型:

- 序號分析
- 關聯洪水攻擊偵測
- Rogue 存取點偵測

存取點 IDS

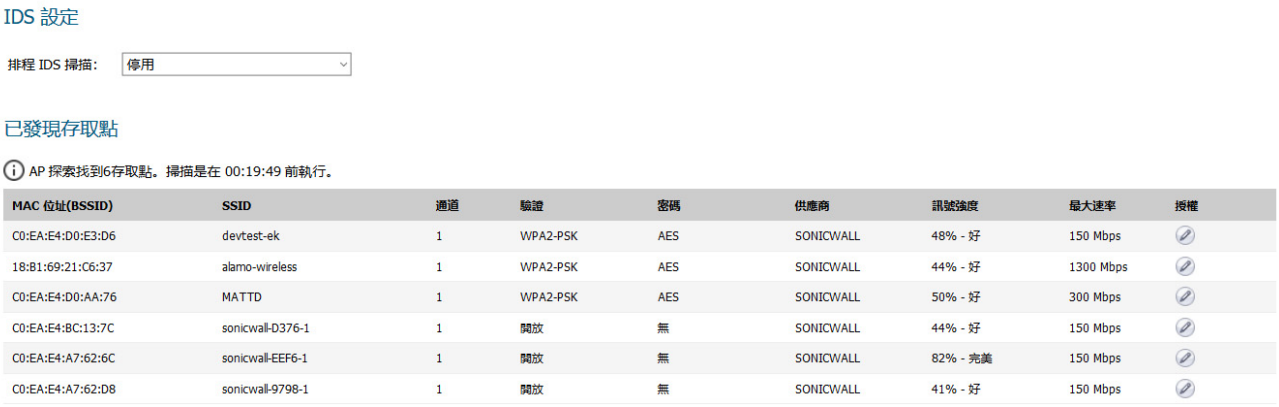
在無線安全裝置的**無線角色**設定為**存取點**模式時，全部三種 WIDS 服務類型均可用，但 Rogue 存取點偵測預設採取被動模式（僅在所選操作頻道被動監聽其他存取點信號框架）。選擇**立即掃描**可以即刻變更「無線角色」以允許無線安全裝置執行使用中掃描，並可能導致關聯無線用戶端在短時間內中斷連接。在**存取點**模式中，應該只有在未使用中關聯用戶端或可以接受用戶端中斷時才使用**立即掃描**功能。

欺詐存取點

欺詐存取點已發展成為對無線完全性最嚴重的一種潛在威脅。如果某存取點未經授權而在網路上使用，則通常將其視為欺詐存取點。不安全存取點具有便利性、可負擔性，並且還可輕鬆的新增到網路中，這為引入欺詐存取點創造了有利的環境。真正的威脅以多種方式存在，包括與欺詐裝置連接、透過不安全頻道傳送敏感資料以及對 LAN 資源進行不需要的存取。這並不表示特定無線裝置的安全性不足，而是整個無線網路的安全性存在缺陷。

安全裝置可以透過識別可能嘗試存取您網路的欺詐存取點彌補這個缺陷。它透過兩種方式實現這個目的: 主動掃描所有 802.11a、802.11g 和 802.11n 頻道上的存取點，以及被動掃描 (在存取點模式中) 單一操作頻道上的信標存取點。

設定 IDS 設定



主題：

- IDS 設定
- 發現的存取點

IDS 設定

若要排程執行 IDS 掃描的時間，從**排程 IDS 掃描**下拉功能表中選擇一個選項:

- **已停用**

  這是預設值。若選此項，將不會進行 IDS 掃描。

- **建立新排程...**

  隨即顯示**新增排程**對話方塊，您可參考本節下文說明建立自訂排程。

- **Work Hours**
- **M-T-W-TH-F 08:00 to 17:00**
- **After Hours**
- **M-T-W-TH-F 上午 12:00 to 上午 08:00**
- **M-T-W-TH-F 17:00 to 24:00**
- **SU-S 00:00 to 24:00**
- **Weekend Hours**

將新排程新增至排程 ID 掃描下拉功能表的步驟如下:

1 在**排程 IDS 掃描**欄位中，選擇**建立新排程...**。

2 輸入**排程名稱**。

3 選擇排程類型:

- 可在**一次性**區段排程一次性事件，且只可使用**一次性**區段中的欄位。
- 可在**重複**區段排程重複事件，且只可使用**重複**區段中的欄位。
- 可在**混合**區段排程混合事件，且可使用所有欄位。

4 在**一次性**區段中，使用下拉功能表排程 IDS 掃描的開始和結束時間。

5 在**重複**區段中:

a 挑選執行掃描的**日子**。

b 輸入**開始時間**，使用 24 小時格式。

c 輸入**停止時間**，使用 24 小時格式。

d 按一下**新增**，將這些參數新增至排程清單中。

e 若要從清單刪除項目，請醒目顯示該項目再按一下**刪除**。按一下**刪除全部**即可清除排程清單。

6 按一下**確定**，將此排程新增至下拉清單中。

發現的存取點

在無線安全裝置啟動時和按一下表格底部的**立即掃描**時，系統會進行主動掃描。裝置會掃描環境並識別鄰近的其他無線裝置。表上方的注顯示已發現的存取點數目和自上次掃描以來的時間（用天數、小時數、分鐘數和秒數表示）。

若要重新整理**已發現存取點**表，按一下**重新整理**。若要立即掃描，請按**立即掃描** (位於表格底部)。

重要：在存取點模式下運作時，**立即掃描**功能會導致服務短暫中斷。此中斷表現如下：

- 非持續性無狀態協定（例如 HTTP）不應出現任何不良效果。
- 持續性連接（例如 FTP 協定）受到影響或中斷。

如果對此有顧慮，請等到無用戶端處於使用中狀態或可接受可能發生中斷情況時，再使用**立即掃描**。

當無線安全裝置在橋接模式下執行時，**立即掃描**功能不會導致橋接中斷。

設定

已發現存取點表顯示所有 SonicPoint 或各 SonicPoint 可以偵測的每個存取點的資訊：

- **MAC 位址 (BSSID)**：偵測到的存取點的無線介面的 MAC 位址。
- **SSID**：存取點的無線 SSID。
- **頻道**：存取點使用的無線頻道。
- **驗證**：驗證類型。
- **密碼**：已使用的密碼。
- **供應商**: 存取點的製造商。SonicPoint 將顯示製造商 SonicWall 或 Senao。
- **信號強度**：偵測的無線訊號的強度
- **最大速率**：存取點無線允許的最大速率，通常為 54 Mbps。
- **授權**：按一下**授權**欄中的圖示，將存取點新增到授權存取點的位址物件群組。

在網路上授權存取點

直至識別為已獲得操作授權，將無線安全裝置偵測到的存取點視為欺詐存取點。若要授權存取點，請按一下**授權**圖示。

32

設定使用內部無線的虛擬存取點

虛擬存取點 (VAP) 是單個實體存取點的多路複用表示，將自己表現為多個分立的存取點。對於無線 LAN 用戶端，每個虛擬存取點都會顯示為一個獨立的實體存取點，而實際上只存在一個實體。虛擬存取點可用於透過設定單個實體介面上的多個自訂設定，控制無線使用者存取和安全設定。其中的每個自訂設定都作為單獨的（虛擬）存取點，可同時在單個內部無線裝置上進行分組和強制實施。

使用 VAP 的優點包含:

- **無線訊號保留** - 透過將單個實體存取點充當多個使用來避免頻道衝突問題，這樣可避免構建重複的基礎結構。多供應商越來越成為公用空間（例如機場）的標準。舉例來說，在機場可能需要支援 FAA 網路、一個或多個航線網路以及一個或多個無線 ISP。但在美國和歐洲，802.11b 網路只能支援三個可用（不重疊）頻道，在法國和日本，僅提供一個頻道。現有存取點使用頻道後，其他存取點會相互干擾並降低效能。虛擬存取點藉由允許將單個網路用於多種用途來保留頻道。
- **無線 LAN 基礎結構最佳化** - 在多個供應商之間共用同一個無線 LAN 基礎結構，而不是建立重疊的基礎結構，以降低安裝和維護 WLAN 的資本開支。

主題：

- 無線虛擬存取點設定任務清單
- 虛擬存取點設定檔
- 虛擬存取點
- 虛擬存取點群組
- 啟用虛擬存取點群組

無線虛擬存取點設定任務清單

無線虛擬存取點部署需要多個設定步驟。以下章節簡要概述了其中包含的步驟:

1 **網路區域** - 網路區域是虛擬存取點設定的重要部分。您建立的每個區域都擁有其獨自的安全和存取控制設定，您可以使用無線子網路建立並套用多個區域到單個實體介面。如需網路區域的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**管理 | 網路 > 區域**章節。

2 **無線介面** - W0 介面（及其 WLAN 子網路）代表 SonicWall 網路安全裝置與內部無線之間的實體連接。您單獨的區域設定將套用到這些介面，然後轉送到無線裝置。如需網路介面的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**管理 | 網路 > 介面**章節。

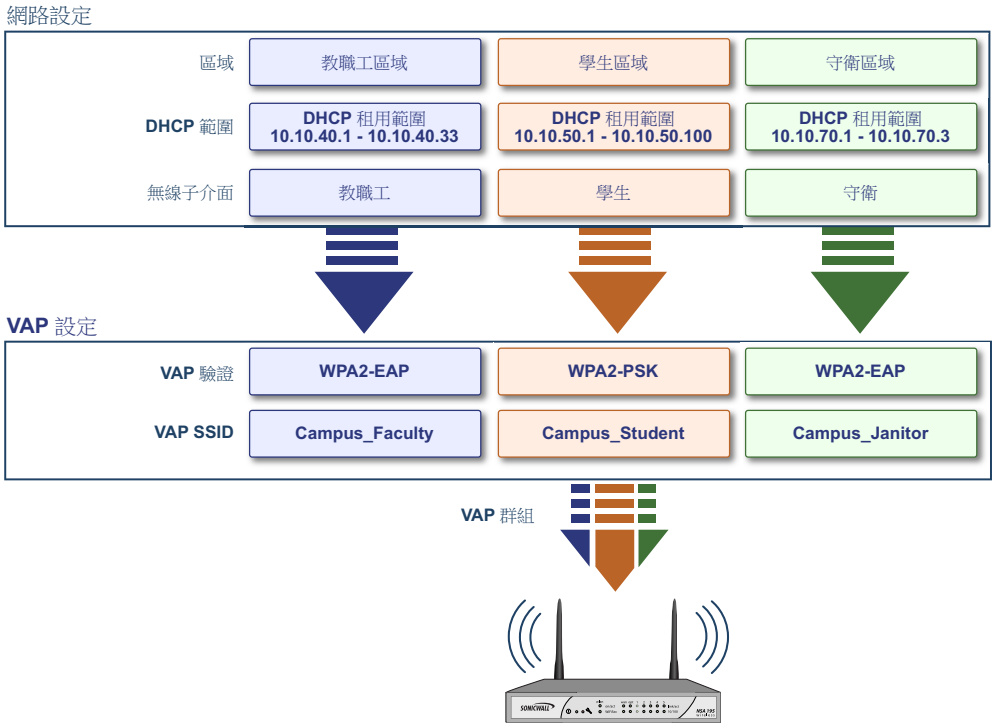
3 **DHCP 伺服器** - DHCP 伺服器將租用的 IP 位址指派給指定範圍內的使用者，稱為*範圍*。DHCP 範圍的預設範圍通常很大，足以滿足多數無線部署，例如對僅使用 30 個位址的介面使用 200 個位址的範圍。基於此原因，必須仔細設定 DHCP 範圍才能確保不會用完可用的租用範圍。如需設定 DHCP 伺服器的詳細資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*中的**管理 | 網路 > DHCP 伺服器**章節。

4 **虛擬存取點設定檔** - 虛擬存取點設定檔功能用於建立根據需要可輕鬆套用到新無線虛擬存取點的無線設定檔。如需更多資訊，請參閱**虛擬存取點設定檔**。

5 **虛擬存取點** - 虛擬存取點物件功能用於設定一般虛擬存取點設定。通過虛擬存取點設定可設定 SSID 和無線子網路名稱。如需更多資訊，請參閱虛擬存取點。

6 **虛擬存取點群組** - 虛擬存取點群組功能用於對多個虛擬存取點物件進行分組，並將它們同步套用到您的單個無線裝置。如需更多資訊，請參閱虛擬存取點群組。

7 **指派虛擬存取點群組到內部無線** - 將虛擬存取點群組套用於內部無線，並通過多個 SSID 提供給使用者。如需更多資訊，請參閱啟用虛擬存取點群組。



虛擬存取點設定檔

虛擬存取點設定檔用於預設定存取點設定並將其儲存在設定檔中。虛擬存取點設定檔允許將設定輕鬆套用到新虛擬存取點。虛擬存取點設定檔可從**管理 | 無線 > 虛擬存取點**頁面設定。選擇設定檔名稱並按一下**編輯**圖示，或按一下**新增**以建立新的虛擬存取點設定檔。完成時，按一下確定。

提示：在多個虛擬存取點使用相同驗證方法的情況下，此功能對於快速設定尤其有用。

主題：

- 虛擬存取點排程設定
- 虛擬存取點設定檔設定
- 強制啟用 ACL

虛擬存取點排程設定

每個虛擬存取點都能擁有與其相關聯的排程，且藉由擴充，每個設定檔也都能擁有專為其定義的固定排程。

為排程與虛擬存取點設定檔建立關聯的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要建立新設定檔，請選擇**新增**，或若要編輯現有的設定檔，請選擇一個虛擬存取點設定檔，然後按一下**編輯**圖示。

4 在 **VAP 排程名稱**欄位中，從下拉功能表的選項中選擇所需的排程。

虛擬存取點設定檔設定

設定虛擬存取點設定檔設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要建立新設定檔，請選擇**新增**，或若要編輯現有的設定檔，請選擇一個虛擬存取點設定檔，然後按一下**編輯**圖示。

4 設定**無線類型**。預設值為**內部無線**。如果使用內部無線進行虛擬存取點存取 (目前唯一支援的無線類型)，則保留此預設值。

5 在**設定檔名稱**欄位中，為此虛擬存取點設定檔輸入易記的名稱。選擇描述性且易於記住的名稱，方便將該設定檔套用到新虛擬存取點。

6 從下拉清單中選擇**驗證類型**。從以下選項中選擇:

驗證類型	定義
開啟	未指定驗證。
共用	使用共用密碼驗證 WEP 加密設定
兩者	若未設定共用密碼，便等同於開放網路。 若設定了共用密碼，表示含有加密資料流量的開放驗證
WPA2-PSK	與受信任的公司無線用戶端配合使用的最佳安全性。使用 Windows 登入進行透明驗證支援快速漫遊功能。使用預先共用密碼進行驗證。
WPA2-EAP	與受信任的公司無線用戶端配合使用的最佳安全性。使用 Windows 登入進行透明驗證支援快速漫遊功能。使用可擴充驗證通訊協定。
WPA2-AUTO-PSK	可嘗試使用 WPA2 安全性進行連接，如果用戶端不支援 WPA2，連接會預設為 WPA。使用預先共用密碼進行驗證。
WPA2-AUTO-EAP	可嘗試使用 WPA2 安全性進行連接，如果用戶端不支援 WPA2，連接會預設為 WPA。使用可擴充驗證通訊協定。

系統會依據您選擇的驗證類型自動填入**單點傳送密碼**欄位。

附註：根據您選擇的選項，頁面上會顯示不同設定。

7 在**最大用戶端**欄位中，輸入此虛擬存取點允許的最大同時用戶端連接數。

8 勾選方塊以**啟用 VAP WDS** (無線分散系統)。預設情況下，未選擇此選項。

9 勾選方塊以**允許 802.11b 用戶端連接**。預設情況下，此選項處於勾選狀態

根據所選擇的**驗證類型**而定，「新增/編輯虛擬存取點設定檔」頁面上會新增一個含有選項的額外區段。

- 若您選擇**兩者皆是**或**共用**，請參閱 WEP 加密設定瞭解設定的相關資訊。
- 若您選擇的選項需要預先共用密碼 (PSK)，請參閱 WPA-PSK > WPA2-PSK 加密設定瞭解設定的相關資訊。
- 若您選擇的選項使用可擴充驗證通訊協定 (EAP)，請參閱 WPA-EAP > WPA2-EAP 加密設定瞭解設定的相關資訊。

WEP 加密設定

若您在上一道程序的步驟 6 中選擇了**兩者皆是**或**共用**，此處會出現 **WEP 加密設定**區段。WEP 設定通常由一個共同實體存取點中的多個虛擬存取點共用。

在**加密金鑰**欄位中，從下拉清單選擇**金鑰 1**、**金鑰 2**、**金鑰 3** 或**金鑰 4**。

WPA-PSK > WPA2-PSK 加密設定

若您在步驟 6 中選擇的選項需要預先共用密碼 (**WPA2-PSK** 或 **WPA2-AUTO-PSK**)，此處會出現 **WPA/WPA2-PSK 加密設定**區段。定義完這些設定後，系統會使用預先共用密碼進行驗證。在下列欄位中輸入值:

欄位名稱	說明
複雜密碼	輸入使用者在連接基於 PSK 的驗證時需輸入的共用密碼。
群組金鑰間隔	輸入群組金鑰有效的期間。預設值為 86400 秒。設定為較低的值會導致連接問題。

WPA-EAP > WPA2-EAP 加密設定

若您在步驟 6 中選擇的選項需要 EAP (**WPA2-EAP** 或 **WPA2-AUTO-EAP**)，此處會出現 **Radius 伺服器設定**區段。定義完這些設定後，系統會使用支援外部 802.1x/EAP 的 RADIUS 伺服器產生金鑰和進行驗證。在下列欄位中輸入值:

欄位名稱	說明
Radius 伺服器重試	輸入拒絕使用者存取前使用者可嘗試驗證的次數。預設為 4。
重試間隔（秒）	輸入重試有效的期間。預設為 0。
RADIUS 伺服器 1	輸入 RADIUS 驗證伺服器的名稱/位置。
連接埠	輸入主要 RADIUS 驗證伺服器用來與用戶端和網路裝置進行通訊的連接埠。
RADIUS 伺服器 1 機密	輸入主要 RADIUS 驗證伺服器的密碼。
RADIUS 伺服器 2	輸入備份 RADIUS 驗證伺服器的名稱/位置。
連接埠	輸入備份 RADIUS 驗證伺服器用來與用戶端和網路裝置進行通訊的連接埠。
RADIUS 伺服器 2 金鑰	輸入備份 RADIUS 驗證伺服器的密碼。
群組金鑰間隔	輸入強制使用 WPA/WPA2 群組金鑰的期間 (單位為秒)。預設值為 86400。

強制啟用 ACL

每個虛擬存取點均可支援單獨的存取控制清單 (ACL)，以提供更高效的身分驗證控制。無線 ACL 功能可配合 SonicOS 上目前可用的無線 MAC 篩選條件清單使用。使用強制啟用 ACL 功能，使用者可以啟用或停用 MAC 篩選條件清單、設定允許清單和設定拒絕清單。

每個虛擬存取點都可擁有自己的 MAC 篩選條件清單設定或使用全域設定。在虛擬存取點 (VAP) 模式中，此群組的各虛擬存取點共用相同的 MAC 篩選條件清單設定。

啟用 MAC 篩選條件清單的步驟如下:

1 勾選方塊以**啟用 MAC 篩選條件清單**。MAC 篩選條件清單已啟用時，其他設定也會啟用，方便您進行設定。

2 若要**使用全域 ACL 設定**，請勾選方塊。這會與 SonicWall 網路安全裝置已有的 MAC 篩選條件清單建立關聯。請注意，若啟用此選項，將無法編輯允許或拒絕清單。

3 在**允許清單**中，從下拉清單選擇一個選項。此選項用於識別您允許擁有存取權的 MAC 位址。

若想建立新的位址物件群組，其中包含您希望賦予存取權的位址，請選擇**建立 MAC 位址物件群組**。請參考 *SonicWall SonicOS 6.5 原則*瞭解操作方式。

4 在**拒絕清單**中，從下拉清單選擇一個選項。此選項用於識別您拒絕提供存取權的 MAC 位址。

若想建立新的位址物件群組，其中包含您不希望賦予存取權的位址，請選擇**建立 MAC 位址物件群組**。請參考 *SonicWall SonicOS 6.5 原則*瞭解操作方式。

5 完成時，按一下**確定**。

虛擬存取點

虛擬存取點設定功能用於設定一般虛擬存取點設定。通過虛擬存取點設定可設定 SSID 和無線子網路名稱。虛擬存取點可從**管理**檢視上的**連線 | 無線 > 虛擬存取點**頁面設定。

主題：

- 虛擬存取點一般設定
- 虛擬存取點進階設定

虛擬存取點一般設定

定義虛擬存取點一般設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要編輯現有的虛擬存取點，按一下該存取點的**編輯**圖示。若要建立新存取點，按一下**虛擬存取點**區段中的**新增**。

4 在**名稱**欄位中，為存取點建立易記的名稱。

5 在 **SSID** 欄位中，輸入唯一名稱。此名稱為附加至封包標頭的唯一識別項，區分大小寫，最多可含 32 個英數字元。

6 從下拉功能表中選擇 **VLAN ID**。

7 勾選方塊以**啟用虛擬存取點**。

8 如果不想讓未授權的無線用戶端看到您的 SSID，請勾選方塊以**啟用 SSID 隱藏**。若啟用此選項，系統會隱藏 SSID 名稱的廣播並停用對探查請求的回應。

9 按一下**確定**。

虛擬存取點進階設定

進階選項用於為此虛擬存取點設定驗證和加密設定。列出的選項與用於定義虛擬存取點設定檔的選項相同。

定義虛擬存取點進階設定的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要編輯現有的虛擬存取點，按一下該存取點的**編輯**圖示。若要建立新存取點，按一下**虛擬存取點**區段中的**新增**。

4 按一下**進階**。

5 在**虛擬存取點進階設定**標題底下，從下拉清單中選擇**設定檔名稱**。該設定檔的所有設定都會自動從設定檔填入。

如果不想使用設定檔，**設定檔名稱**請維持設為**無設定檔**，並遵照虛擬存取點設定檔的說明填入其餘欄位。

6 按一下**確定**。

虛擬存取點群組

「虛擬存取點群組」功能用於對多個虛擬存取點物件進行分組，並將其同步套用到您的內部無線。虛擬存取點群組可從**管理**檢視上的**連線 | 無線 > 虛擬存取點**頁面設定。

附註：必須先設定多個虛擬存取點，才能建立虛擬存取點群組。若只有一個存取點，系統會自動將它新增至預設群組「內部 AP 群組」。

建立虛擬存取點群組的步驟如下:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 若要編輯現有的虛擬存取點群組，按一下該群組的**編輯**圖示。

4 若要將物件新增至群組，從**可用的虛擬存取點物件**清單中選擇要新增的物件，再按一下右箭頭。

5 若要從群組中刪除物件，從**虛擬存取點群組成員**清單中選擇要刪除的物件，再按一下左箭頭。

6 完成時，按一下**確定**。

啟用虛擬存取點群組

在設定虛擬存取點並將其新增到虛擬存取點群組後，必須將該群組套用至內部無線，並提供給使用者使用。

若要將群組提供給使用者使用:

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 基本設定**。

3 捲動至**無線虛擬存取點**。

4 在**虛擬存取點群組**欄位中，從下拉清單選擇**內部 AP 群組**。

5 按一下**接受**以更新設定。

第 5 部分

3G/4G/數據機

- 設定 3G/4G/數據機基本設定
- 設定 3G/4G/數據機進階設定
- 設定 3G/4G/數據機連接設定檔
- 監控 3G/4G 資料使用

33

3G/4G/數據機概述

配備 USB 擴充連接埠的 SonicWall 網路安全裝置可以支援外部 3G/4G 介面或類比數據機介面。

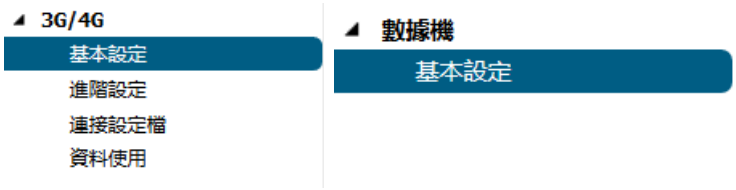
附註：SuperMassive 9800 不支援 3G/4G 和數據機介面。

主題：

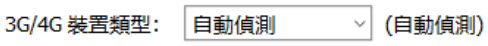
- 選擇介面
- 了解 3G/4G
- 3G/4G 前提條件
- 啟用 U0/U1/M0 介面

選擇介面

依照預設，裝置會嘗試偵測已連接的外部介面類型。若能成功識別類型，左側的導覽列會顯示偵測到的項目。



您可導覽至**連線 | 3G/4G/數據機 > 基本設定**頁面，手動指定要設定的介面類型。



3G/4G/LTE/數據機裝置類型下拉功能表提供以下選項:

- **自動偵測** - 若選擇此項，裝置會嘗試判斷連接的裝置類型。
- **3G/4G/LTE/行動** - 若選擇此項，需手動設定 3G/4G/LTE/行動介面。
- **類比數據機** - 若選擇此項，需手動設定類比據機介面。

了解 3G/4G

SonicWall 安全裝置支援透過行動電話網路進行資料連接的 3G/4G 無線 WAN 連接。3G/4G 連接可用於：

- 與不依賴電線或網線的連接的 WAN 容錯移轉。
- 預設連接無法使用時的臨時網路，例如商展和公共資訊機。
- SonicWall 裝置位於車內的行動網路。
- 主要 WAN 的有線連接是無法使用的，而 3G/4G 行動電話網路是可用的。

若要使用 3G/4G 介面，您必須有 3G/4G PC 卡或 USB 裝置，並與無線服務供應商簽訂了合約。應主要基於支援的硬體的可用性選擇 3G/4G 服務供應商。SonicOS 支援以下網頁中列出的裝置:
https://www.sonicwall.com/en-us/support/knowledge-base/170505473051240

SonicOS 支援以下 3G/4G 無線網路供應商（本清單可能變更）：

- AT&T
- H3G
- Orange
- Sprint PCS Wireless
- Telecom Italia Mobile
- Telefonica
- T-Mobile
- TDC Song
- Verizon Wireless
- Vodaphone

主題：

- 3G/4G 連接類型
- SonicWave MiFi 延伸器
- 3G/4G 容錯移轉
- 第 254 頁「3G/4G 前提條件」

3G/4G 連接類型

若啟動裝置前已安裝 3G/4G 裝置，這些 3G/4G 裝置會列在**管理**檢視上**系統安裝 | 網路 > 介面**的「介面設定」表中。名稱欄中以 **U0**、**U1** 或 **M0** (僅限 NSA 240) 列出介面名稱。

3G/4G 連接類型設定對配備 3G/4G 介面的 SonicWall 裝置的 WAN 連接提供靈活的控制。在**連線 | 3G/4G > 連接設定檔**上編輯設定檔時，便設定了連接類型。「3G/4G 設定檔設定」視窗的**參數**標籤上提供下列連接類型:

- **持續連接** - 在 3G/4G 介面連至 3G/4G 服務供應商後，將保持連接直到管理員中斷連接或發生網路事件（例如 WAN 無法使用）導致連接斷開。
- **連接資料** - 3G/4G 介面在 SonicWall 裝置偵測到指定類型的網路流量時自動連接。
- **手動連接** - 僅在管理員手動啟動連接時才連接 3G/4G 介面。

△ **注意：雖然可以在「系統安裝 | 網路 > 介面」頁面手動啟用 3G/4G 連接 (透過按一下 U0/U1/M0 介面的「管理」按鈕)，但不建議這樣做，因為這會導致自動連接無法正常運作。SonicWall 推薦使用上述連接類型管理 3G/4G 介面。**

SonicWave MiFi 延伸器

SonicOS 6.5 中的 SonicWave 3G/4G/LTE MiFi 延伸器功能，讓 SonicWall 無線存取點可連接 3G 或 4G 行動電話網路，並建立可供智慧型手機、筆記型電腦和平板電腦等裝置共用的無線熱點。這個 WWAN 解決方案可讓多個最終使用者和行動裝置共用 3G 或 4G 行動寬頻網際網路連線。

若要使用此功能，需將 USB 裝置插入 SonicWave 存取點中，接著該 USB 裝置就會透過 3G/4G 連接至網際網路。在 SonicOS 中，將 VLAN 介面繫結至 USB 數據機。

執行 SonicOS 6.5 的所有 SonicWall 防火牆和配備 USB 介面的所有 SonicWave 和存取點皆支援此功能。需要支援 3G (PPP)、4G (Hi-Link) 或 QMI 通訊協定的 USB 裝置。

使用下列設定進行 VLAN 設定:

- 將「區域」設為「WAN」。
- 將父級介面設為存取點所連接的實體介面。
- 若使用 3G USB 數據機，「IP 指派」應為「固定」，並為其指派私人 IP 位址。閘道和 DNS 伺服器欄位保持空白，存取點的佈建完成後系統會自動填入。
- 若使用 4G 和 QMI 數據機，「IP 指派」應為「DHCP」。數據機連接後將會從 USB 數據機伺服器取得 DHCP 租用。

此功能使用 SonicOS 3G/4G 模組提供的連接設定檔。前往**連線 | 3G/4G 數據機**頁面，為使用的 3G USB 數據機新增正確的設定檔。請參閱 **XXX** 取得設定資訊。

3G/4G 容錯移轉

重要：您可管理主要 WAN 介面中斷時 3G/4G 裝置的容錯移轉行為。為了使 3G/4G 介面能作為備用介面正常運作，必須將其設定為預設負載平衡群組中的最終備用介面。前往**系統安裝 | 網路 > 容錯移轉和負載平衡**頁面，編輯包含 3G/4G 裝置的群組。

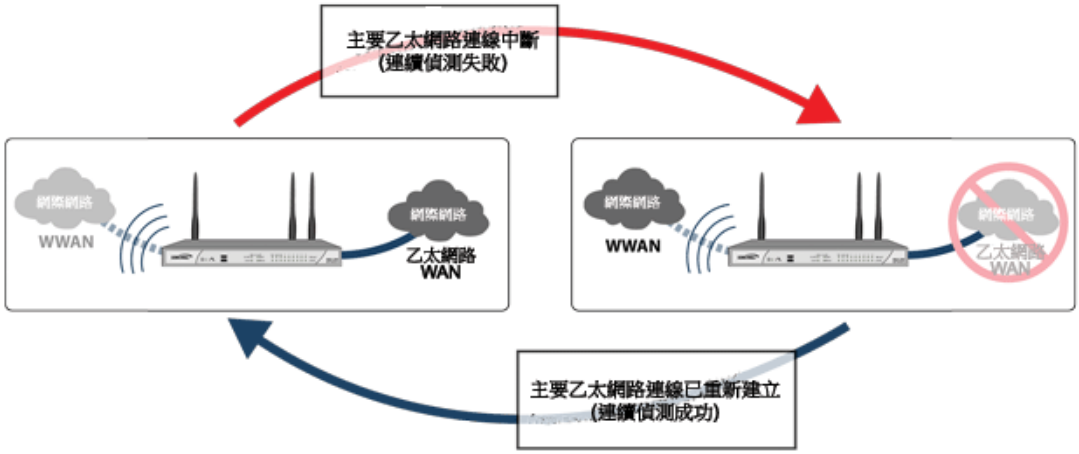
以下章節說明 WAN 至 3G/4G 容錯移轉的三種不同方式。所有這些章節都假定設定 U0/U1/M0 介面為負載均衡群組中的最終備用介面。

- 透過持續連接功能進行 3G/4G 容錯移轉
- 透過連接資料功能進行 3G/4G 容錯移轉
- 手動撥號 3G/4G 容錯移轉

透過持續連接功能進行 3G/4G 容錯移轉

下圖說明在 WAN 乙太網路連接失敗且已將 3G/4G 連接設定檔設定為**持續連接**時，將發生的事件順序。

3G/4G 容錯移轉的事件順序：持續連接



1 **主要乙太網路連接可用** - 乙太網路 WAN 介面已連接，並用作主要連接。在乙太網路 WAN 介面可用時，不會連接 U0/U1/M0 介面（除非設定了指定 3G/4G 作為目的地介面的明確路由）。

2 **主要乙太網路連接失敗** - 在乙太網路 WAN 連接斷開時，將啟動 U0/U1/M0 介面且*保持連接*狀態。

如果將另一個乙太網路 WAN 介面設定為負載平衡群組的一部分，則裝置在容錯移轉至 U0/U1/M0 介面之前，會先容錯移轉至次要乙太網路 WAN。在這種情況下，只有在主要和次要 WAN 路徑都無法使用時，才會容錯移轉至 U0/U1/M0 介面。

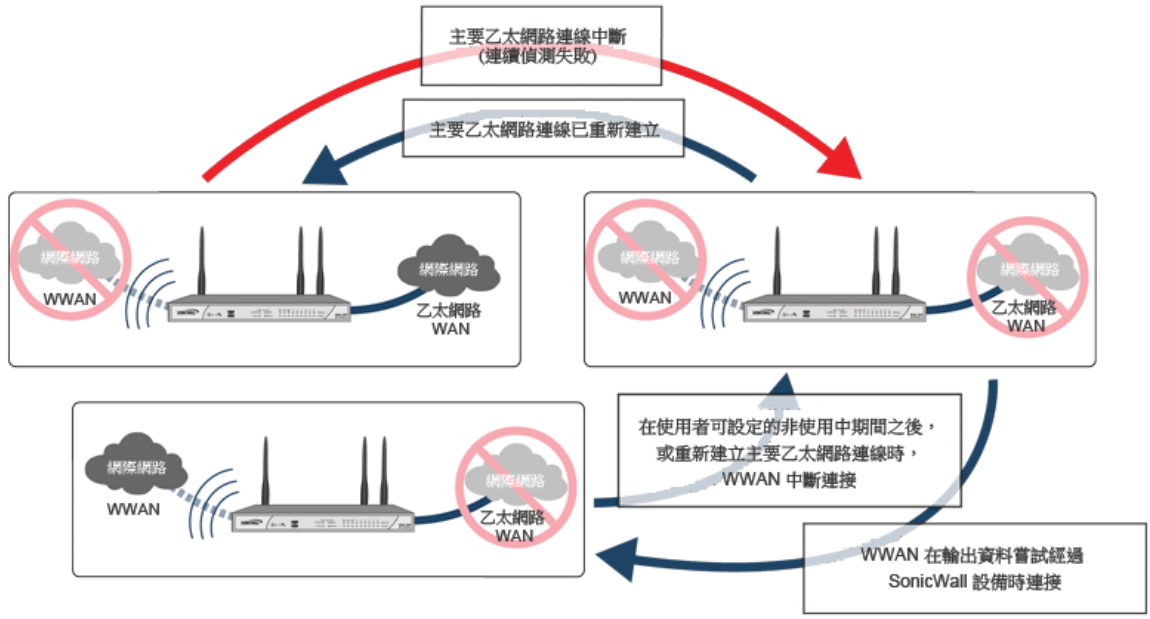
3 **在容錯移轉後重新建立主要乙太網路連接** - 當乙太網路 WAN 連接（如設定的主要 WAN 連接埠或次要 WAN 連接埠）重新可用時，所有 LAN 至 WAN 流量將自動傳回可用的乙太網路 WAN 連接。這包括活動的連接和 VPN 連接。將關閉 U0/U1/M0 介面連接。

△ 注意：**在將 U0/U1/M0 介面設定為負載平衡群組中的最終備用介面時，請勿設定基於原則的路由使用 U0/U1/M0 介面。如果將基於原則的路由設定為使用 U0/U1/M0 介面，將保持連接，直到達到最長連接時間 (如已設定)。**

透過連接資料功能進行 3G/4G 容錯移轉

下圖描繪在 WAN 乙太網路連接失敗且已將 3G/4G 連接設定檔設定為**連接資料**時，將發生的事件順序。

3G/4G 容錯移轉的事件順序：連接資料



1. **主要乙太網路連接可用** - 乙太網路 WAN 介面已連接，並用作主要連接。在乙太網路 WAN 介面可用時，不會連接 3G/4G（除非設定了指定 U0/U1/M0 介面作為目的地介面的明確路由）。
2. **主要乙太網路連接失敗** - 不會建立 U0/U1/M0 介面連接，直到輸出資料嘗試透過 SonicWall 裝置。
3. **建立 3G/4G 連接** - 在裝置或網路節點嘗試向網際網路傳送資料時，將建立 U0/U1/M0 介面連接。U0/U1/M0 介面保持連接，直到最長連接時間（如已設定）已到達。

   ⓘ **附註：**如果 3G/4G 設定為替代 WAN，且未勾選**當可能的話，先佔並且自動恢復到優先介面**核取方塊 (**系統安裝 | 網路 > 編輯預設 LB 群組**)，那麼即使乙太網路 WAN 可用，U0 連接仍會保持使用中狀態。

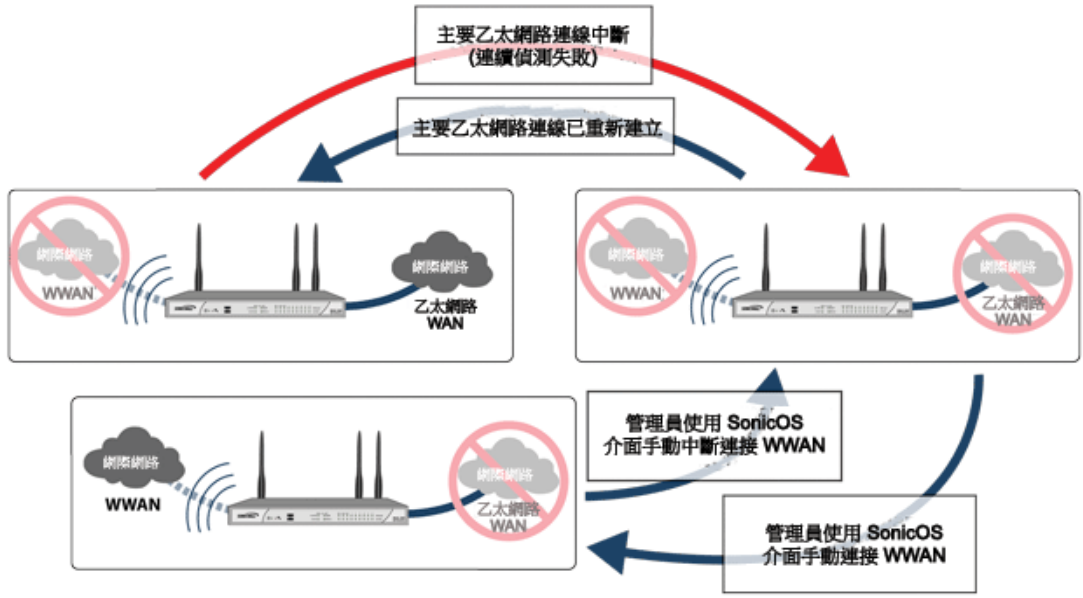
4. **在容錯移轉後重新建立 WAN 乙太網路連接** - 當乙太網路 WAN 連接重新可用或達到非使用中定時（如已設定）時，所有 LAN 至 WAN 流量將自動傳回可用的乙太網路 WAN 連接。將終止 U0/U1/M0 介面連接。

△ **注意：在將 U0/U1/M0 介面設定為負載平衡群組中的最終備用介面時，建議不要設定基於原則的路由使用 U0/U1/M0 介面。如果將基於原則的路由設定為使用 U0/U1/M0 介面，將保持連接，直到達到最長連接時間 (如已設定)。**

手動撥號 3G/4G 容錯移轉

注意：SonicWall 建議打算使用 U0/U1/M0 介面作為主要 WAN 介面的容錯移轉備用介面時，不要使用手動撥號 3G/4G 連接設定檔，發生 WAN 故障時，裝置將中斷 WAN 連線，直到管理員手動啟動 U0/U1/M0 介面連接。下圖描繪在 WAN 乙太網路連接失敗且已將 3G/4G 連接設定檔設定為「手動撥號」時，將發生的事件順序。

3G/4G 容錯移轉的事件順序：手動撥號



1. **主要乙太網路連接可用** - 乙太網路 WAN 已連接，並作為主要連接。在乙太網路 WAN 連接可用時，不會連接 3G/4G。
2. **主要乙太網路連接失敗** - 不會建立 U0/U1/M0 介面連接，直到管理員手動啟用連接。
3. **建立 3G/4G 連接** - 在管理員手動啟用 SonicWall 裝置的連接後，U0/U1/M0 介面的連接建立。U0/U1/M0 介面保持連接，直到您手動停用連接。
4. **在容錯移轉後重新建立 WAN 乙太網路連接** - 不管乙太網路連接是否重新可用，**所有 LAN 至 WAN 流量將仍然使用手動啟用的 3G/4G 連接**，直到您手動停用連接。手動中斷連接後，將使用可用的乙太網路連接。

3G/4G 前提條件

在設定 3G/4G 介面前，您必須滿足以下前提條件：

- 向支援的供應商無線供應商購買 3G/4G 服務計劃
- 設定和啟用 3G/4G 卡
- 在接通 SonicWall 安全裝置的電源**前**，插入 3G/4G 卡。

  重要：只有在關閉 SonicWall 安全裝置的電源時，才能插入或移除 3G/4G 卡。

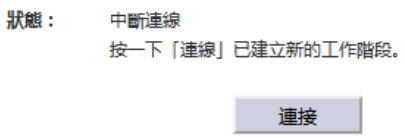
如需設定這些前提條件的資訊，請參見您具體型號的*《SonicWall 入門指南》*。

啟用 U0/U1/M0 介面

> **注意：不建議在「網路 > 介面」頁面上手動啟用 3G/4G 連接 (按一下 U0/U1/M0 介面的「管理」按鈕)。這會造成自動連接無法正常運作。SonicWall 建議使用 3G/4G 連接類型中說明的連接類型管理 3G/4G 介面。**

手動啟動 U0/U1/M0 外部 3G/4G 介面的連接的步驟如下：

1. 在**網路 > 介面**頁面，按一下 U0/U1/M0 介面的**管理**按鈕。**U0/U1/M0 連接狀態**對話顯示。
2. 按一下**連接**按鈕。一旦連接進入使用中狀態，**U0/U1/M0 連接狀態**對話將顯示有關工作階段的統計資訊。



3. 若要結束連接，請按下**中斷連線**。

34

設定 3G/4G/數據機基本設定

附註：SuperMassive 9800 不支援 3G/4G 和數據機介面。

設定 3G/4G 裝置或數據機的第一步是定義基本設定。如 3G/4G/數據機概述中所說明，裝置會嘗試偵測已連接的裝置類型，若能成功識別類型，左側的導覽列和設定頁面會變為顯示偵測到的項目。若要手動選擇裝置，請參閱選擇介面。

需定義以下基本設定:

針對 3G/4G 裝置	針對數據機
3G/4G 設定	Modem 設定
按需連接類別	按需連接類別
管理/使用者登入	管理/使用者登入

主題：

- 設定
- 按需連接類別
- 管理/使用者登入
- MiFi 延伸器設定

設定

本節中提供的指引假設安全裝置已自動偵測到裝置，或已手動設定裝置。以下以自動偵測到 3G/4G 裝置類型為例:

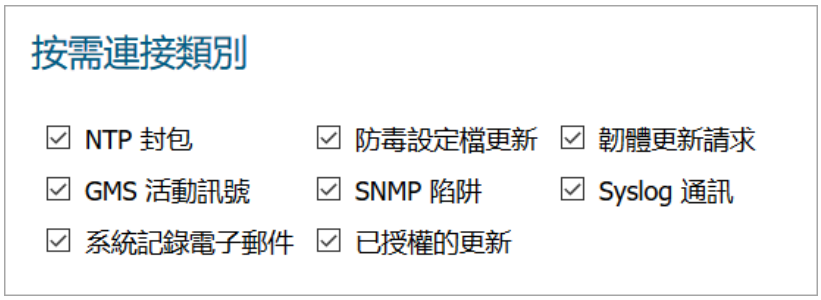
此處針對數據機顯示相同選項。請注意，「數據機設定」區段有兩個。第一個顯示已自動偵測到數據機；第二個提供需設定的選項。

必須設定**數據機設定**區段才能啟用透過數據機介面管理 SonicWall 裝置。

- **喇叭音量** - 選擇是否**開**或**關**（預設）喇叭。
- **數據機初始化** - 選擇以下其中一個選項:
  - **初始化 Modem 連接用於** - 從下拉清單中選擇國家或地區。
  - **使用 AT 命令初始化 Modem 連接** - 在欄位中輸入適當的 AT 命令。

按需連接類別

如果裝置類型選擇 **3G/4G/LTE/行動**或**類比數據機**，將顯示**按需連接類別**區段。這些設定用於設定介面在 SonicWall 裝置偵測到指定的流量類型時自動連接至服務供應商。預設選擇所有**按需連接類別**：



要為連接資料操作設定 SonicWall 裝置，必須為連接設定檔選擇**連接資料**作為**連線類型**。如需更多詳細資訊，請參閱設定 3G/4G/數據機連接設定檔。

管理/使用者登入

如果裝置類型選擇 **3G/4G/LTE/行動**或**類比數據機**，將顯示**管理/使用者登入**區段。必須設定**管理/使用者登入**部分以便透過介面對 SonicWall 裝置啟用遠端管理。

於**管理**欄位選擇任何或所有支援的通訊協定: **HTTPS**、**Ping**、**SNMP**、**SSH**。

在**使用者登入**欄位中，**選擇 HTTP** 或 **HTTPS** 或是兩者皆選。但請記得，HTTP 流量的安全性不如 HTTPS 來得高。

如果您將**管理**和/或**使用者登入**選擇為 HTTPS，將自動選擇**新增規則，以啟用從 HTTP 到 HTTPS 的重新導向**選項。如果啟用此選項，可自動將 HTTP 請求轉換為 HTTPS 請求，以增強安全性。如果您不想要轉換，請取消選擇此選項。

附註：在之前的 SonicOS 版本中，3G/4G 介面的探查監控在 **3G/4G > 設定**頁面中設定。現在需於**系統安裝 | 網路 > 容錯移轉和負載平衡**頁面設定探查監控。如需更多資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

MiFi 延伸器設定

3G/4G/LTE MiFi 延伸器功能讓 SonicWall SonicWave 存取點可連接 3G 或 4G 行動電話網路和建立無線熱點。多個最終使用者和行動裝置可共用 3G 或 4G 行動寬頻網際網路連接。

若要使用此功能，需將 USB 裝置插入 SonicWave 存取點中。在 SonicOS 中，將 VLAN 介面繫結至 USB 數據機。

設定存取點的步驟:

1 在**管理**檢視中，導覽至**連線 | 存取點 > 基礎設定**。

2 在 **SonicPoint / SonicWave 物件**底下，按一下要使用的存取點對應的**設定**按鈕。

3 按一下 **3G/4G/LTE WWAN** 按鈕。

附註：按一下此頁面底部的 **3G/4G/LTE WWAN 精靈**按鈕，即可讓精靈協助您建立或選擇 VLAN 介面和 3G/4G/LTE 連接設定檔。

4 勾選**啟用 3G/4G/LTE 數據機**核取方塊。

5 在**已繫結至 WAN VLAN 介面**下拉清單中選擇您為 USB 裝置建立的 VLAN。

6 若要使用特定連接設定檔，請勾選**啟用連接設定檔**核取方塊並填入相關欄位。許多情況下都可使用預設連接設定檔，如此一來此步驟為可選步驟。

7 按一下**確定**。

系統會將設定推送到存取點。您可在**管理**檢視中的**連線 | 存取點 > 3G/4G/LTE WWAN** 頁面上檢視基本狀態。

若有多個存取點和 3G/4G 數據機可供使用 (各兩個以上)，SonicOS 可同時使用並對其執行負載平衡。首先，為每個 SonicPoint 和數據機對指派唯一 VLAN，然後在**系統安裝 | 網路 > 容錯移轉和負載平衡**頁面上，將這些 VLAN 介面新增至 LB 群組。

35

設定 3G/4G/數據機進階設定

附註：SuperMassive 9800 不支援 3G/4G 和數據機介面。

進階設定頁面用於為 3G/4G 裝置和數據機設定以下功能:

- 遠端觸發撥出設定
- 頻寬管理
- 連接限制

遠端觸發撥出設定

遠端觸發撥出部分使您可以遠端啟動 WAN 數據機連接。以下過程描述「遠端觸發撥出」呼叫的工作原理：

1 網路管理員啟動與位於遠端辦公室的 SonicWall 安全裝置的數據機連接。

2 如果設定裝置為須驗證傳入呼叫，將提示網路管理員輸入密碼。在呼叫透過身分驗證後，裝置終止呼叫。

3 然後，根據設定的撥號設定檔，裝置啟動與撥號 ISP 的數據機連接。

4 您存取設備的 Web 管理介面以執行要求的任務。

在設定遠端觸發撥出功能前，先確保設定符合以下前提條件：

- 將 3G/4G 連接設定檔設定為**連接資料**。
- 將 SonicWall 安全裝置設定為使用 **HTTPS** 管理，以遠端存取裝置。
- 雖然非必填，但建議在**啟用非使用狀態中斷連接**欄位中輸入值。此欄位位於**設定檔設定 > 參數**頁面中，編輯裝置的設定檔即可使用此欄位。如果未在此欄位中輸入值，撥出呼叫將保持無限期連接，您必須透過按一下**中斷連接**按鈕手動終止工作階段。

設定遠端觸發撥出的步驟如下：

1 在**管理**檢視上，導覽至**進階**頁面:

- **連線 | 3G/4G > 進階設定**
- **連線 | 數據機 > 進階設定**

2 選擇**啟用遠端觸發撥出**核取方塊。

3 若想對遠端連接要求驗證，請勾選**要求驗證**方塊，並在**密碼**和**確認密碼**欄位中輸入密碼。

4 按一下**接受**儲存您的設定。

頻寬管理

頻寬管理部分用於啟用 3G/4G 介面的輸出或輸入頻寬管理服務。

附註：如需設定頻寬管理的資訊，請參閱 *SonicWall SonicOS 6.5 安全設定*中的**防火牆設定**。

若要設定頻寬管理：

1 在**管理**檢視上，導覽至**進階**頁面:

- **連線 | 3G/4G > 進階設定**
- **連線 | 數據機 > 進階設定**

2 勾選方塊以**啟用輸出頻寬管理**。

3 勾選方塊以**啟用輸入頻寬管理**。

4 從下拉功能表中選擇**壓縮放大器**：

1.0x（預設）、**1.5x 2.0x**、**2.5x**、**3.0x**、**3.5x**、**4.0x**

壓縮放大器適用於輸出和輸入頻寬。

5 按一下**接受**儲存您的設定。

「頻寬管理」底下的備註也說明了所選擇的頻寬管理類型，且提供用於變更類型的連結 (如有需要)。

連接限制

使用**連接限制**區段，您可以設定 3G/4G 或數據機連接上的主機/節點限制。在將裝置用作溢出或處於負載平衡狀態，以避免連接負擔過重時，此功能對部署特別實用。

在**主機最大數目**欄位中，輸入連接此介面時允許的最大主機數。預設值為 **0**，即允許無限數量的節點。

36

設定 3G/4G/數據機連接設定檔

附註：SuperMassive 9800 不支援 3G/4G 和數據機介面。

使用**連接設定檔**頁面設定 3G/4G 和數據機連接設定檔，也可設定主要和替代設定檔。

主題：

- 偏好設定檔
- 連接設定檔

偏好設定檔

設定偏好設定檔的步驟如下:

1 在**管理**檢視上，導覽至**連接設定檔**頁面:

- **連線 | 3G/4G > 連接設定檔**
- **連線 | 數據機 > 連接設定檔**

2 在**偏好設定檔**區段中，從下拉功能表中選擇**主要設定檔**。

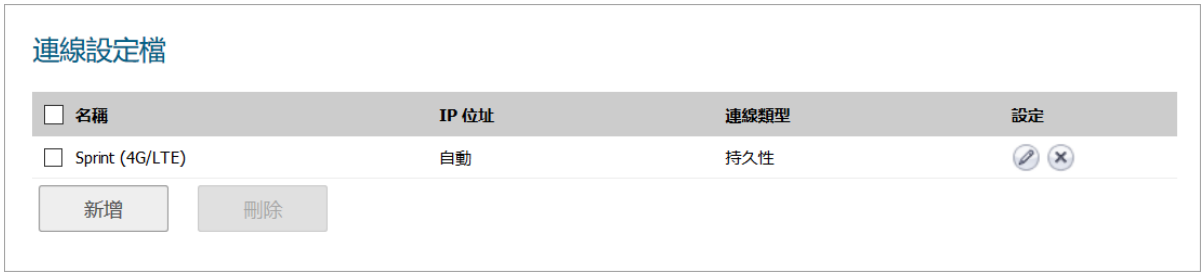
附註：為數據機提供的選項與 3G/4G 裝置專用選項有所不同。

3 如有需要，可從下拉功能表中選擇**替代設定檔 1** 和**替代設定檔 2**。

4 按一下**接受**儲存您的設定。

連接設定檔

若要建立連接設定檔，請按一下**新增**按鈕，或按一下表格**設定**欄中的**編輯**圖示以編輯現有的設定檔。



執行以下章節中的步驟：

針對數據機:	針對 3G/4G 裝置:
一般設定	一般設定
ISP 位址	
參數設定	參數設定
	IP 位址
排程	排程
	資料限制
進階	進階

附註：視您在**基本設定**頁面中選擇的 **3G/4G/數據機裝置類型**而定，並非所有選項都可用。

一般設定

新增或更新連接設定檔時，預設檢視會顯示**一般設定**，供您設定服務供應商。在選擇國家、服務供應商和計劃類型後，將自動填寫大部分服務供應商的其餘欄位。

若要設定一般連接設定：

1 選擇 SonicWall 裝置部署所在的**國家或地區**。

2 選擇您建立帳戶時採用的**服務供應商**。

附註：僅顯示您所在國家支援的服務供應商。

3 從**計劃類型**下拉功能表中選擇您訂閱的計劃。如果您的特定計劃類型：

- 列於下拉功能表中（很多基本計劃可能簡單標記為**標準**），將自動填寫**一般**標籤中的其餘欄位。驗證這些欄位正確無誤，然後跳至參數設定。
- 未列於下拉功能表中，則選擇**其他**。

4 在**設定檔名稱**欄位輸入設定檔的名稱。

5 驗證是否選擇了正確的**連線類型**。

附註：將自動填寫大多數服務供應商的此欄位。

6 驗證**已撥號碼**正確無誤。

附註：大多數服務供應商的已撥號碼是 ***99#**。

7 如果供應商要求，則在**使用者名稱**、**使用者密碼**和**確認使用者密碼**欄位中分別輸入您的使用者名稱和密碼。

ISP 位址

「ISP 位址」設定只會在設定數據機時顯示。此設定用於定義數據機與基礎結構其餘部分通訊的方式。

設定 ISP 位址的步驟如下:

1 選擇 **ISP 位址**。

2 在 **IP 位址**底下，選擇以下其中一項:

- **自動取得 IP 位址**
- **使用以下 IP 位址**並在欄位中輸入位址。

3 在 **DNS 伺服器**底下，選擇以下其中一項:

- **自動取得 IP 位址**
- **使用以下 IP 位址**，並在第一個欄位中輸入主要位址，在第二個欄位中輸入次要位址。

參數設定

參數設定用於定義服務連接時所使用的參數。三種連接類型是**持續**、**連接資料**和**手動**。這些連接類型的機制詳見了解 3G/4G。

設定參數設定的步驟如下:

1 按一下**參數**。

2 在**連線類型**下拉功能表，選擇連接設定檔是**持續連接**、**連接資料**還是**手動撥號**。

> **附註：**若要設定 SonicWall 裝置的遠端觸發撥出，**連線類型**必須是連接資料。

3 勾選方塊以**啟用非使用狀態中斷連接 (分鐘數)**，並輸入連接中斷前可處於非使用中狀態的分鐘數。注意如果**連線類型**是**持續連接**，此選項無法使用。

4 勾選方塊以**啟用最大連接時間 (分鐘數)**，並輸入不管工作階段是否使用中，均保持連接的分鐘數。

5 在**重新連接之前的延遲時間（分鐘數）**中輸入值，以使 SonicWall 裝置在指定的分鐘數之後自動重新連接。

6 勾選**每個電話號碼的重撥次數**方塊，然後在欄位中輸入數值，指定 SonicWall 裝置嘗試重新連接的次數。

7 勾選**兩次重撥之間的延遲時間 (秒鐘)** 方塊，然後在此欄位中輸入數值，指定重試之間的秒數。

8 勾選**撥號後停用 VPN** 核取方塊停用透過 3G/4G 介面的 VPN 連接。

9 勾選方塊以**強制 PAP 驗證**。

IP 位址

使用 **IP 位址**為 3G/4G 介面設定動態或固定 IP 位址。在大多數情況下，您會想**自動獲取 IP 位址**，但是如果您的服務供應商要求，可以為閘道 IP 位址和一個或多個 DNS 伺服器 IP 位址設定手動 IP 位址。

若要設定 IP 位址：

1 選擇 **IP 位址**。

預設情況下，將 3G/4G 連接設定檔設定為自動獲取 IP 位址和 DNS 伺服器位址。

2 若要指定固定 IP 位址，請勾選**使用以下 IP 位址**單選框，然後在欄位中輸入 IP 位址。

3 若要手動輸入 DNS 伺服器位址，請選擇**使用以下 IP 位址**，然後在欄位中輸入主要和次要 DNS 伺服器的 IP 位址。

排程

使用**排程**將連接限制在一週指定日的指定時間。此功能對於需要在一天的某些時間段限制存取權限的資料計劃較為有用，例如區分夜晚/週末閒時的計劃。

附註：啟用此功能後，如果**未**勾選某天的核取方塊，則在這一整天都會拒絕 3G/4G 存取。

若要設定存取排程：

1 按一下**排程**。

2 勾選**為連接設定檔限制時間**核取方塊啟用此介面的排程功能。

3 勾選您希望允許存取的一週中各天的核取方塊。

4 輸入各天所需的起始時間和結束時間（24 小時格式）。

資料限制

資料限制功能僅提供 3G/4G 裝置使用。可使用此功能限制每月的資料使用。此功能用於根據 3G/4G 供應商的帳單週期追蹤使用情況，並在達到規定的限值時中斷連接。

若要限制資料使用：

1 按一下**資料限制**。

提示：如果您的 3G/4G 帳戶有每月資料量或時間限制，強烈建議您啟用「資料使用限制」。

2 勾選**啟用資料使用限制**方塊，在達到當月的指定資料量或時間限制時自動停用 3G/4G 介面。

3 在**帳單週期開始日期**下拉功能表選擇月份中開始追蹤月資料或時間使用量的起始日。

4 在**限制**欄位中輸入值，然後選擇相應的限制單位：**GB**、**MB**、**KB** 或**分鐘**。

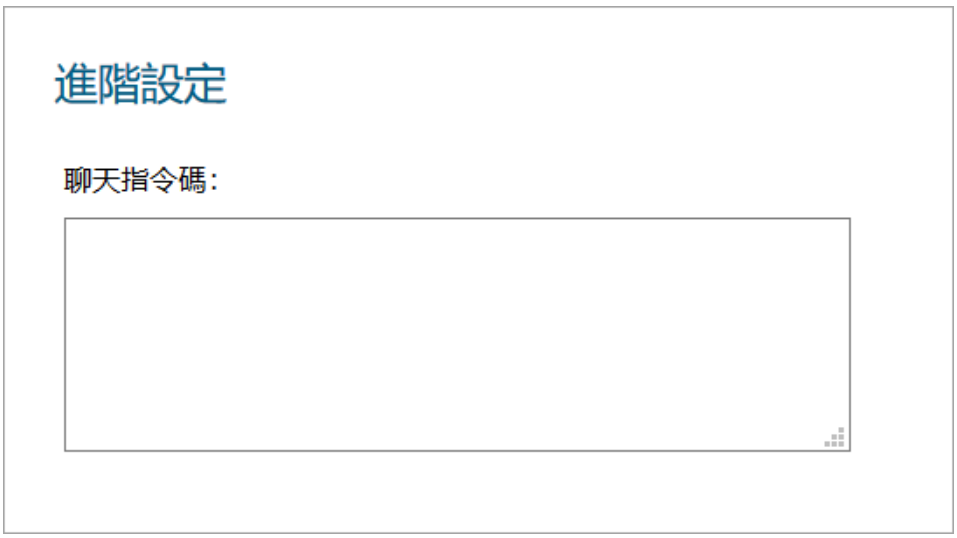
進階

使用**進階**手動設定在 3G/4G 連接過程中使用的聊天指令碼。

提示：只有在需要向標準撥號連接指令碼新增命令或特殊指令時，才需要設定聊天指令碼。

若要設定聊天指令碼：

1 按一下**進階**標籤。



2 在**聊天指令碼**欄位中輸入連接的聊天指令碼。

3 按一下**確定**。

37

監控 3G/4G 資料使用

附註：SuperMassive 9800 不支援 3G/4G 和數據機介面。

導覽至**管理**檢視上的**連線 | 3G/4G > 資料使用**，監控**資料使用**和檢視**工作階段歷史記錄**。

資料使用表顯示目前**年**、**月**、**週**、**日**和**帳單週期**的目前資料使用情況和連線時間。只有在 3G/4G 連接設定檔中啟用了**啟用資料使用限制**選項，才會計算帳單週期使用情況。

按一下相應的**重設**按鈕重設任何資料使用類別。

附註：**資料使用**表只是目前使用情況的估計，不應用於計算實際費用。如需準確的計量資訊，請聯絡您的服務供應商。

工作階段歷史記錄表顯示有關 3G/4G 工作階段的資訊摘要。若要檢視指定工作階段的附加資訊，請將光標置於**屬性**欄的**註解**圖示。若要清除表格，按一下**清除**按鈕。

第 6 部分

連線能力附錄

- VAP 樣本設定
- SonicWall 支援

A

VAP 樣本設定

本節提供基於真實世界無線需求的 VAP 設定範例。

主題：

- 為學校教職工存取設定 VAP
- 向無線電波部署虛擬存取點

為學校教職工存取設定 VAP

您可以使用針對經常在辦公室、校園工作的使用者群體的虛擬存取點，且已為其提供對所有網路資源的完整存取權限（假設連接已經過驗證且是安全的）。這些使用者應已屬網路的目錄服務 Microsoft Active Directory，此服務通過 IAS（網際網路驗證服務）提供 EAP 介面。本節包含以下內容:

- 設定區域
- 建立新無線子網路
- 建立無線虛擬存取點設定檔
- 建立無線虛擬存取點
- 建立多個虛擬存取點 > 部署目前的虛擬存取點

設定區域

在本節中，您將建立和設定具有 SonicWall 防火牆安全服務和增強的 WiFiSec/WPA2 無線安全性的新公司無線區域。如需更多關於區域的資訊，請參閱 *SonicWall SonicOS 6.5 系統安裝*。

1 登入 SonicWall 網路安全裝置的管理介面。

2 選擇**管理**檢視。

3 在**系統安裝**底下，選擇**網路 > 區域**。

4 按一下**新增...** 按鈕以新增新區域。

一般設定標籤

1 在**一般**標籤中，輸入易記的名稱，例如在**名稱**欄位中輸入「WLAN_Faculty」。

2 從**安全類型**下拉功能表中選擇**無線**。

3 勾選**允許介面信任**方塊以允許教職工使用者之間的通訊。

4 勾選您通常套用到無線 LAN 教職工的所有安全服務的方塊。

無線設定標籤

1 勾選**僅允許 SonicPoint/SonicWave 產生的流量**方塊。

2 從 **SonicPoint 佈建設定檔**下拉功能表 (若適用) 選擇佈建設定檔。

3 按一下**確定**按鈕儲存這些變更。

您的新區域現已顯示在**網路 > 區域**頁面底部，儘管您可能已注意到它尚未連結到成員介面。這是您的下一個步驟。

建立新無線子網路

在本節中，您將在目前的 WLAN 上建立和設定新無線子網路。此無線子網路將連結到您之前在設定區域中建立的區域。

若要建立新無線子網路：

1 在**管理**檢視底下，選擇**系統安裝 | 網路 > 介面**頁面

2 在**新增介面**欄位中，選擇**虛擬介面**。

3 在**區域**下拉功能表中，選擇您之前建立的區域。在本例中，我們選擇了 **WLAN_Faculty**。

4 輸入此介面的 **VLAN 標籤**。VLAN 允許內部無線識別哪些流量屬於此子網路。在本例中，我們選擇 100 作為子網路 VLAN 標籤。

5 從**父級介面**選擇 **W0** 介面。

6 輸入此子介面所需的 **IP 位址**。

7 按一下**確定**按鈕新增此子介面。

您的 WLAN 子網路介面現已顯示在介面設定清單中。

建立無線虛擬存取點設定檔

在本節中，您將建立並設定新虛擬存取點設定檔。您可以為每個虛擬存取點類型建立虛擬存取點設定檔，並使用它們將進階設定輕鬆套用到新的虛擬存取點。本節為可選，但在設定多個虛擬存取點時有利於更好地使用。

若要建立無線虛擬存取點設定檔：

1 選擇**管理**檢視。

2 在**連線**底下，選擇**無線 > 虛擬存取點**。

3 按一下**虛擬存取點設定檔**區段中的**新增**。

4 從下拉清單中選擇 **VAP 排程名稱**。

5 輸入此虛擬存取點設定檔的**設定檔名稱**，例如「Corporate-WPA2」。

6 從**驗證類型**下拉功能表中選擇 **WPA2-AUTO-EAP**。這將根據您目前的 RADIUS 伺服器設定（設定如下）使用自動使用者驗證。

7 在**最大用戶端**欄位中，輸入虛擬存取點需支援的最大同時連接數。

8 在**無線伺服器設定**區段中，輸入您目前的 RADIUS 伺服器資訊。此資訊將用於支援驗證登入新子網路。

9 按一下**確定**按鈕建立此虛擬存取點設定檔。

建立無線虛擬存取點

在本節中，您將建立和設定新虛擬存取點，並將其與您在建立新無線子網路中建立的無線子閘道聯。

若要建立無線虛擬存取點：

一般

1 導覽至**連線 | 無線 > 虛擬存取點**頁面。

2 按一下**虛擬存取點**區段中的**新增**按鈕。

3 在**名稱**欄位中輸入易記的名稱。

4 為 VAP 輸入 **SSID** 名稱。在本例中，我們選擇 **Campus_Faculty**。這是使用者在選擇連接的無線網路時看到的名稱。

5 從下拉清單中選擇 **VLAN ID**。此處應該會列出您建立的項目。在本例中，我們為 WLAN_Faculty 子網路選擇 VLAN 標籤。

6 勾選方塊以**啟用虛擬存取點**。

7 勾選方塊以**啟用 SSID 隱藏**，對使用者隱藏此 SSID。

8 按一下**確定**按鈕新增此虛擬存取點。

您的新虛擬存取點現將顯示在虛擬存取點清單中。

進階

1 按一下**進階**以編輯加密設定。

2 如果您在之前的章節中建立了虛擬存取點設定檔，則從**設定檔名稱**下拉功能表選擇該設定檔。我們已建立並選擇「Corporate-WPA2」設定檔，此檔案使用 **WPA2-AUTO-EAP** 驗證方法。如果您未設定虛擬存取點設定檔，請繼續第 2 步到第 4 步。否則，請繼續建立多個虛擬存取點 > 部署目前的虛擬存取點。

3 在**進階**標籤中，選擇**驗證類型**下拉功能表中的 **WPA2-AUTO-EAP**。這將根據您目前的 RADIUS 伺服器設定（設定如下）使用自動使用者驗證。

4 在**最大用戶端**欄位中，輸入併發連接虛擬存取點將支援的最大數量。

5 在 **WPA-EAP 加密設定**區段，輸入您目前的 RADIUS 伺服器資訊。此資訊將用於支援對無線子網路的身分驗證登入。

建立多個虛擬存取點 > 部署目前的虛擬存取點

由於您已成功設定用於教職工存取的無線子網路，您可以選擇新增更多的自訂虛擬存取點，或將此設定部署到內部無線。

提示：請記住，可在稍後新增更多的虛擬存取點。按照向無線電波部署虛擬存取點中的步驟可以同時部署到新 VAP。

向無線電波部署虛擬存取點

在下節中，您將對新虛擬存取點進行分組，並將它們與內部無線相關聯。如果未完成以下步驟，使用者將無法存取您的虛擬存取點:

- 對多個虛擬存取點分組
- 將虛擬存取點群組與您的無線電波相關聯

對多個虛擬存取點分組

在本節中，會將多個虛擬存取點新增到一個群組中，以便與您的實體存取點相關聯。

1 在**管理**檢視上，導覽至**連線 | 無線 > 虛擬存取點**。

2 按一下**內部 AP 群組**的**編輯**按鈕。

3 從清單中選擇所需的虛擬存取點，並按一下 **->** 按鈕，將它們新增到群組中。您可以選擇按一下**全部新增**按鈕，將所有虛擬存取點新增到單個群組中。

4 按**確定**按鈕儲存變更並建立群組。

5 若要設定 802.11g WEP 或 802.11a WEP/WPA 加密，或啟用 MAC 位址篩選，請編輯虛擬存取點或虛擬存取點設定檔，再前往**進階**標籤。如果任一虛擬存取點使用加密，則在無線虛擬存取點能正常工作前必須設定這些設定。

6 按一下**確定**按鈕儲存變更，並建立此無線佈建設定檔。

將虛擬存取點群組與您的無線電波相關聯

在設定虛擬存取點並將其新增到**內部 AP 群組**後，必須在**無線 > 設定**頁面指定群組以便通過內部無線使用虛擬存取點。

1 導覽至**連線 | 無線 > 基本設定**。

2 在無線虛擬存取點區段中，從**虛擬存取點**群組下拉功能表中選擇**內部 AP 群組**。

3 按一下**接受**按鈕繼續並將虛擬存取點群組與您的內部無線關聯。

附註：如果首次設定來賓服務，請務必在 *SonicWall SonicOS 6.5 系統安裝*的**使用者 > 來賓服務**底下執行必要設定。

B

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
- 註冊培訓和認證
- 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 連線能力
更新時間 - 2018 年 1 月
軟體版本 - 6.5
232-004132-00 Rev B

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

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

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

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

最終使用者產品合約

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

開放原始程式碼

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

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