Proscend M331-6

強固型 4G 路由器

使用手冊

1.00 版本

目錄

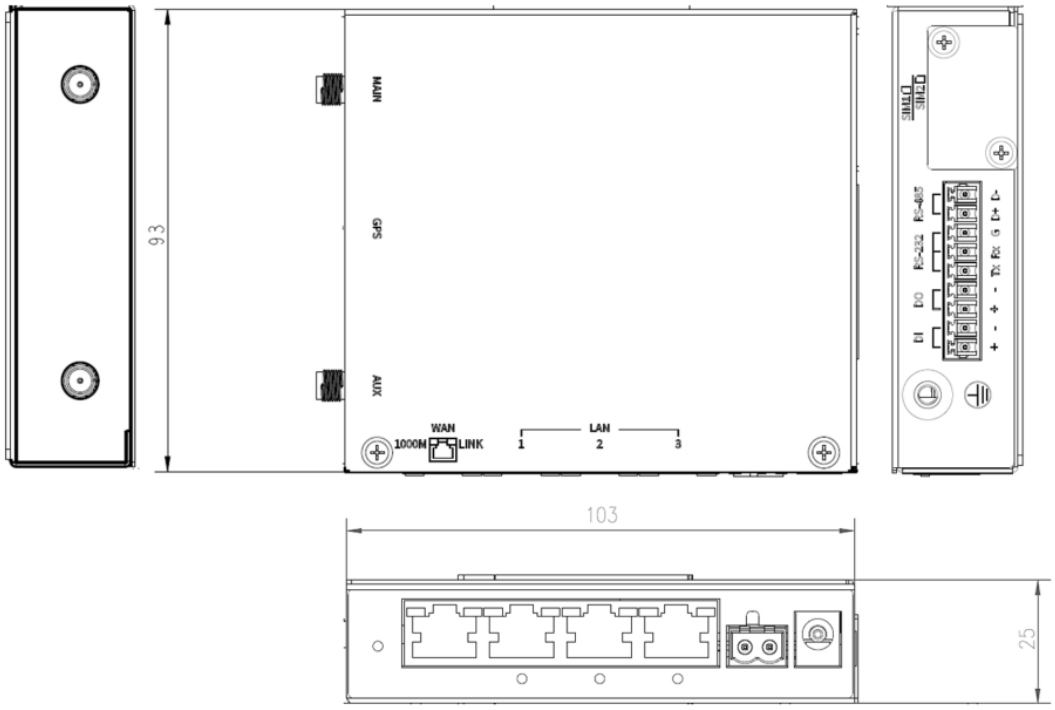
1 產品介紹

昇頻 M331-6 強固型 4G 路由器專為提供高效能智慧聯網和網路備援方案而打造，以載波聚合技術創造高速連網傳輸效率，實現關鍵工業物聯網與多元垂直商務應用。堅固耐用、輕盈小巧的金屬機身，易於安裝適用於狹小有限空間。無風扇散熱寬溫設計，穩定運行在各種嚴苛的環境。內建 3 個 GbE LAN 連接埠、1 個 GbE WAN 連接埠和雙 SIM 卡功能，擁有彈性靈活的擴充配置。

1.1 產品特色

- 支援多頻段FDD LTE / TDD LTE / WCDMA / LTE CAT6。
- 內建雙Micro SIM卡槽。
- 可拆卸天線設計，用於連接多種外接式天線。
- LED指示燈顯示連線和數據傳輸狀態。
- 工規溫度範圍為-30至+70°C，適用於嚴峻環境。
- 提升驗證和傳輸的安全性和加密性。

1.2 產品尺寸



1.3 產品規格

行動通訊介面

- 4G: FDD LTE, TDD LTE
- 3G: WCDMA
- LTE Data Rate: CAT6

硬體介面

- 2 x Micro SIM 插槽
- 3 x LAN 10/100/1000 Mbps 網路連接埠
- 1 x WAN10/100/1000 Mbps 網路連接埠
- 1 x RESET 按鈕
- 2 x SMA 接頭，用於可拆卸式 LTE 天線
- 1 x DC 直流電源輸入

機構資訊

- 外殼：金屬外殼
- 尺寸（寬 x 高 x 深）：103 x 25 x 93 mm
- 重量：290 g

LED 指示燈

- 1 x 電源狀態
- 1 x LTE 訊號強度
- 1 x SIM 狀態
- 2 x 網速和鏈結狀態（每 LAN/WAN 連接埠）

電源

- 消耗電量：7 Watts（最大）
- DC 電源輸入：12 VDC

軟體功能

- **網路協定**
  IPv4, IPv6, IPv4/IPv6 dual stack, DHCP server and client, PPPoE, Static IP, SNTP, DNS Proxy, Message Queue Telemetry Transport (MQTT Broker)
- **路由/防火牆**
  NAT, Virtual Server, DMZ, MAC Filter, URL Filter, IP Filter, Static Routing, IPS, SPI, Policy Route
- **VPN**
  OpenVPN, IPSec (3DES, AES128, AES196, AES256, MD5, SHA-1, SHA256), GRE, PPTP, L2TP
- **其他**
  DDNS, QoS, UPnP, SMS Action
- **警報**
  SMS, VPN/WAN Disconnect, SNMP Trap, E-mail
- **管理**
  用於遠程和本機管理的網頁、CLI 系統記錄監視器 SNMP
  透過 SSH v2、HTTPS 進行遠程管理
  透過 Telnet、SSH v2、HTTP/HTTPS 進行本地管理

使用環境

- 工作溫度 -30 ~ +70°C
- 儲存溫度 -40 ~ +85°C
- 環境相對濕度 10 ~ 95%HR (非凝結)
- 濕度 0 ~ 95%HR (非凝結)

標準和認證

- NCC & BSMI CNS15936 & CNS15598-1

2 硬體安裝

本章介紹如何安裝和連接硬體。

2.1 安裝 SIM 卡

M331-6 有兩個 **Micro SIM** 卡插槽，為網路提供備援。

1. 在插入或取出 SIM 卡之前，請確保已關閉電源，或已從 M331-6 行動通訊路由器上拔下電源連接器。
2. 先用螺絲起子拆下金屬保護蓋（如有）。
3. 取出 SIM 卡（如有），輕按它會從插槽中彈出。
4. 將 SIM 卡插入卡槽，上部 SIM 插槽 1(下部 SIM 插槽 2)的 SIM 卡缺角位於左側(右側)。
5. 推動 SIM 卡，並輕按以鎖定到插槽中。
6. 用螺絲起子裝上金屬保護蓋。

備註：

▪ 請使用工作溫度範圍為-40°C 至+105°C 的工業 SIM 卡，以確保行動通訊路由器正常運作。

2.2 LED 指示燈

下表解釋了前面板上的 LED 指示燈。

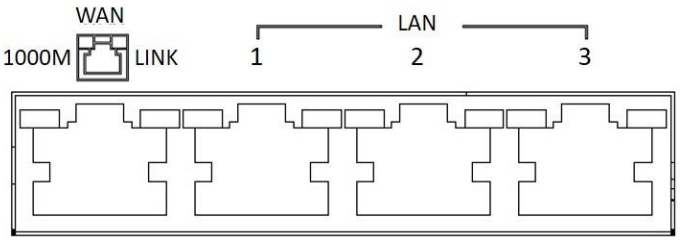
LED	恆滅	恆亮	慢閃爍	快閃爍	Heartbeat
系統	斷電	運行中	不適用	不適用	不適用
SIM	不工作	已連接	正在連接	錯誤	讀取中
訊號	沒訊號	高訊號	中等訊號	低訊號	不適用

2.3 RESET 按鈕

功能	運行中
重設	按住按鈕 1 秒鐘。
重設為預設設定	按住按鈕 5 秒以上。

2.4 LED 乙太網路埠口指示燈

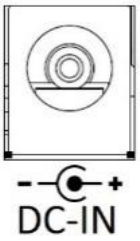
三個 LAN 連接埠和一個 WAN 連接埠，各有兩個 LED 指示燈。



LED	閃爍	恆亮	恆滅
1000M(左)	不適用	1000Mbps	10/100Mbps
LINK(右)	資料傳輸中	鏈結建立	鏈結斷開

2.5 連接電源

通過 DC 插孔為 M331-6 行動通訊路由器供電。



DC 電源孔位於前面板上。

電源輸入電壓為 12 VDC。

2.6 天線安裝

左側面板上的兩個 SMA 連接器用於連接外部 LTE 天線。

- 左邊 MAIN：用於 LTE 發送和接收。
- 右邊 AUX：用於可選的 LTE 接收，以獲得更好的下載速度。

3 透過網頁瀏覽器進行設定

3.1 存取網頁管理頁面

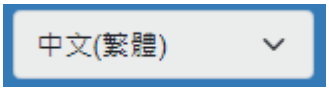
網頁管理頁面是一個基於 HTML 的管理介面，用於快速輕鬆地設定行動通訊路由器。可以透過網頁介面監控路由器的狀態、配置和管理。

正確連接後，行動通訊路由器的硬體如前所述。啟動您的網頁瀏覽器並輸入 http://192.168.1.1/。

行動通訊路由器的預設 IP 位址和子網路遮罩為 192.168.1.1 和 255.255.255.0。由於行動通訊路由器在您的網路中作為 DHCP 伺服器，因此行動通訊路由器將自動為網路中的 PC 或 NB 分配 IP 位址。

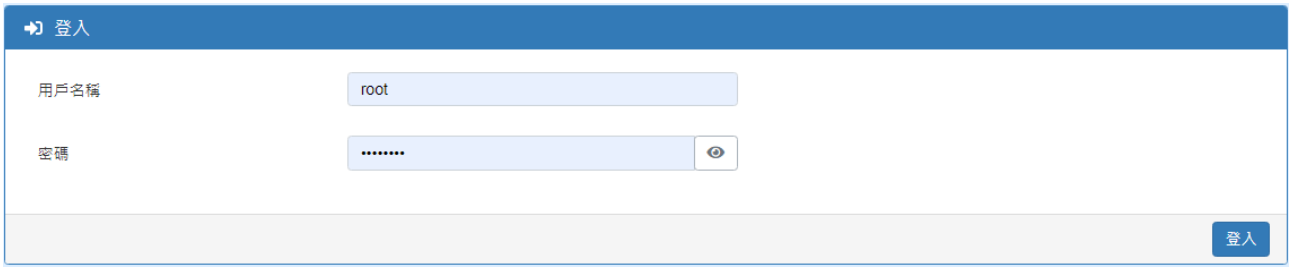
標題列選單 > 選擇語言

您可以選擇不同語言顯示網頁。



登入路由器

在本節中，請填寫預設的使用者名稱 **root** 和預設的密碼 **2wsx#EDC**，然後按登入。



3.2 導覽網頁管理頁面

主螢幕分為以下三個部分。

A - 標題列, B - 導覽視窗 和 C - 主視窗。

(1) A ： 標題列

標題列提供說明顯示路由器的情況。

標題列	
項目	**描述**
語言	從標題列右上角的下拉清單中選擇您的語言。
登入/登出	按兩下以登入或登出網頁。

(2) B ： 導覽視窗-主選單和子功能表

功能表項目分為主功能表和子功能表，用於配置設定。

導覽視窗	
主功能表/子功能表	**描述**
產品狀態	設備整體狀態
系統	此系統部分允許您設定以下項目，包括日期與時間、系統記錄檔、警報、乙太網路埠和用戶清單。
日期與時間	此部分允許您設定路由器和 NTP 伺服器的日期與時間。日期與時間

	設定有兩種模式，包括「Sync with local system」和「從時間伺服器獲取」。預設模式是「從時間伺服器取得」。
系統記錄檔	此部分允許行動通訊路由器記錄資料並顯示資料狀態。
警報	此部分允許您設定警報。
乙太網路埠口	此部分允許您設定乙太網路交換機埠口設定。
用戶清單	此部分允許您瞭解此路由器已連接的設備數量及狀態。有兩種類型，一種是 DHCP 用戶，另一種是目前使用中，預設值為顯示兩種類型的所有狀態。
網際網路	此部分允許您設定網際網路，包括 Connection Table、IPv6 DNS 伺服器和網際網路健康檢查。
Connection Table	此部分允許設定乙太網路網際網路和每張 SIM 卡 APN 的優先順序。
乙太網路	此部分提供三個選項來獲取乙太網路 WAN 的 IP。
IPv6 DNS 伺服器	此部分允許您配置 IPv6 DNS 伺服器設定。
網際網路健康檢查	針對 SIM 卡不同 APN 以及乙太網路網際網路進行健康檢查設定。
行動通訊	此部分允許您配置設定 SIM 設定、SIM 使用流量、簡訊、服務基站和 DNS 伺服器。
SIM 設定	此部分允許用戶配置 SIM 卡的設定。
SIM 使用流量	此部份顯示目前 SIM 卡、電信商、APN 以及即時、每小時、每天、每週和每月的圖表。
簡訊	此部分提供兩種設定，一種是簡訊操作，另一種是查看簡訊。
服務基站	此部分顯示服務基站的資訊。
DNS 伺服器	此部分允許您配置特定的 DNS 伺服器設定。
區域網路	此部分允許您設定區域網路 IPv4。
IPv4	設定 IP 位址和子網路遮罩。以及填寫 DHCP 伺服器設定的資訊。
IPv6	此部分允許您設定區域網路 IPv6。
IPv6 Config	選擇您的 IPv6 類型，其中顯示從網際網路委派前綴或固定， 然後配置 DHCP Server 設定。
路由	此部分允許您設定靜態路由和策略路由。
靜態路由	此部分允許您設定靜態路由。靜態路由是預先確定的路徑，網路資訊必須遵循該路徑才能到達特定主機或網路。
策略路由	此部分允許用戶設定策略路由和檢查策略路由設定的狀態。策略路由僅在已啟動的介面上起作用，但在已停用的介面上自動停用。
VPN	此部分允許您設定 OpenVPN、IPsec、GRE、PPTP 伺服器和 L2TP。
OpenVPN	此部分允許您設定 OpenVPN 的連接。預設模式為停用。介面將顯示連接狀態，讓您在連接成功或失敗時跟蹤情況。

IPSec	此部分允許您設定 IPsec Tunnel。該設定有五個標記：連線、憑證 ID、X.509 憑證、CA 憑證和進階。
GRE	此部分允許您配置 GRE 設定。預設模式為關閉。
PPTP 伺服器	此部分提供 2 個子設定，包括伺服器設定和用戶端設定。
L2TP	此部分允許您設定 L2TP，並提供三種設定模式，包括關閉、伺服器和用戶端模式。
防火牆	此部分允許您設定基本規則、通訊埠轉發、DMZ、Management IP、ACL、IP 過濾器、MAC 過濾器、URL 過濾器、NAT 和 IPS。
基本規則	此部分允許您配置基本規則設定。
通訊埠口轉發	此部分允許您設定通訊埠口轉發，按下  編輯按鈕進行設定。
DMZ 主機	此部份允許您配置 DMZ 設定。
Management IP	此部分允許用戶設定能夠從區域網路或網際網路端存取裝置的 Management IP。此 IP 具有比防火牆設定更高的管理許可權。
ACL	此部分允許管理對路由器自身服務的存取。
IP 過濾器	此部分允許您設定 IP 過濾器。按下  編輯按鈕 ，您可以編輯過濾器的 IP 協定、來源/埠口和目的地/埠口。預設值為停用模式和黑名單。
MAC 過濾器	此部份允許您設定 MAC 過濾器。按下  編輯按鈕 ，您可以編輯您需要過濾的 MAC 位址。
URL 過濾器	此部分允許您設定 URL 過濾器。按下  編輯按鈕 ，您可以編輯過濾器和資訊的類型。
NAT	此部分允許您配置 NAT 設定。
IP Passthrough	IP Passthrough 使路由器能夠將行動通訊介面的 IP 傳遞到指定的區域網路埠口。
IPS	此部分允許您配置 IPS 設定。IPS 可防止系統受到網路攻擊。
服務	此部分允許您設定 SNMP、動態 DNS 伺服器、MQTT、UPnP 、SMTP、IP 別名和 QoS。
SNMP	此部分允許用戶設定 SNMP 功能。
動態 DNS 伺服器	此部分允許用戶設定動態 DNS。
MQTT	此部分允許用戶設定 MQTT。它允許 MQTT 用戶端在特定主題或通道內發送消息。默認情況下，路由器不允許匿名者讀/寫 MQTT 主題或通道。因此，您需要在網頁 UI 上為 MQTT 用戶端建立用戶名稱和密碼。
UPnP	此部分允許配置 UPnP 設定，選擇「停用」或「啟用」模式。行動通訊路由器預設 UPnP 停用。

SMTP	此部分提供為伺服器發送電子郵件的方法。例如，當警報收到伺服器的通知時，將發送電子郵件以通知。
IP 別名	此部分允許您配置 IP 別名設定。
QoS	QoS（服務品質）是指控制最大頻寬和允許最小頻寬的網路能力。
管理	此部分為您提供管理路由器、設定管理員以及了解當前軟體和韌體的狀態。此外，您還可以備份和恢復設定。
本機資訊	此部分允許您確認路由器的設定檔、當前軟體、韌體版本和系統已運行時間。
管理員	此部分允許您設定系統名稱並更改新密碼。對於 Session TTL，您可以設定登出的時間。如果不需要此超時限制，則可以填寫「0」。
連絡人/值勤	此部分允許您建立群組和添加用戶。
SSH	Secure Shell（SSH）允許用戶通過安全通道設定系統。
網頁	允許用戶更改網頁管理頁面 HTTP(S) Port，按下 Apply 套用設定重新啟動後，請根據自行設定的 Port 前往網頁管理頁面。
遠程登入	此部分允許用戶選擇是否通過區域網路/網際網路提供 telnet。預設值為停用。
韌體更新	此部分允許升級設備的韌體。
設定檔	此部分支持備份或恢復設定檔。
恢復出廠設定	此部分支援您按下恢復原廠值並重新啟動按鈕，以恢復出廠預設設定並立即重啟設備。
重新啟動	此部份允許您按重新開機按鈕立即重新啟動。
預約重新啟動	該設定允許您定期安排重新啟動時間。
登入失敗就封鎖	Fail2Ban 是一種入侵防禦功能，可保護設備免受暴力登入攻擊。
網路診斷工具	此部分允許您使用 Ping 和 Traceroute 診斷。
Ping	請指定要 ping 的主機。
Traceroute	請指定要 traceroute 的主機。

4 導覽視窗 > 網際網路

此部分支援設定網際網路，包括 Connection Table、IPv6 DNS 伺服器和網際網路健康檢查。

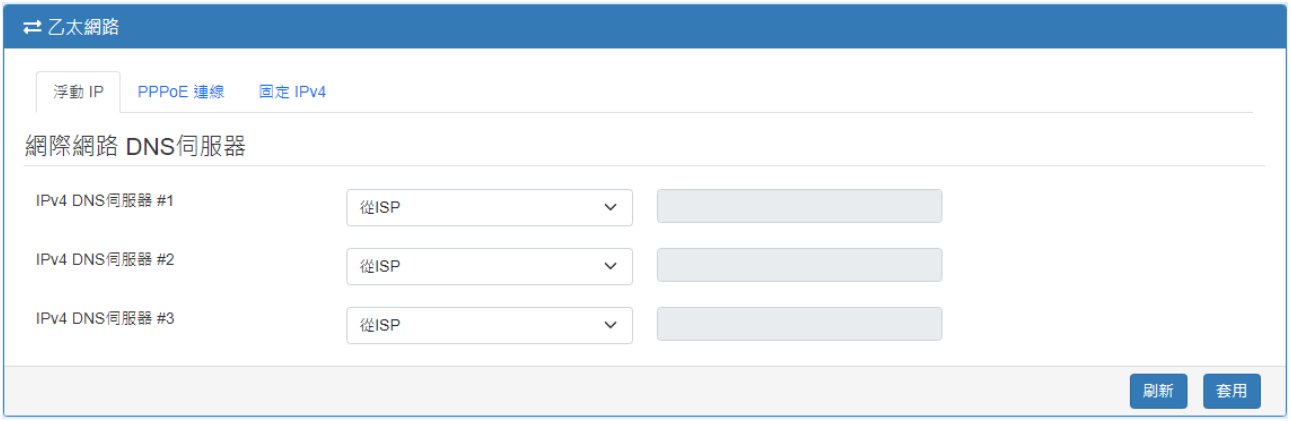
4.1 Connection Table

此部分允許設定乙太網路網際網路和每張 SIM 卡的 APN 優先順序。預設為固網優先，當固網斷線時，會自動切換成行動上網。

網際網路 > Connection Table	
項目	**描述**
Profile	有 3 個 profile 可供切換，用戶可自行設定 profile。
名字	Profile 的命名。
故障轉移	自動：檢測通過之介面優先, 然後是鏈結成功之介面。多個介面檢測通過(或鏈結成功)，低優先權值之介面優先。 主用/備用：優先使用主用介面，主用介面檢測不通過則改用備用介面，備用介面不會進行檢查。
Priority	網路備援優先權設定。

乙太網路

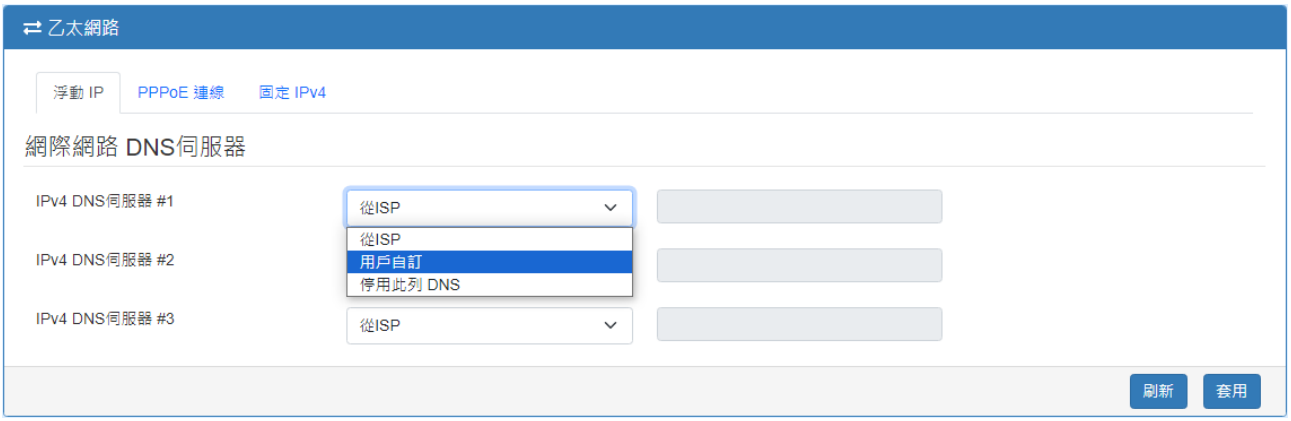
本部分提供三個選項來獲取乙太網路網際網路的 IP。這些選項包括浮動 IP、PPPoE 連線和固定 IPv4。預設值為浮動 IP。



網際網路 > 乙太網路	
項目	**描述**
網際網路乙太網路	• **浮動 IP**：DHCP 伺服器分配的 IP 位址、子網路遮罩、閘道和 DNS。 • **PPPoE 連線**：您的 ISP 將為您提供用戶名和密碼。此選項通常用於 DSL 服務。 • **固定 IPv4**：用戶自定義 IP 位址、子網路遮罩和預設閘道。

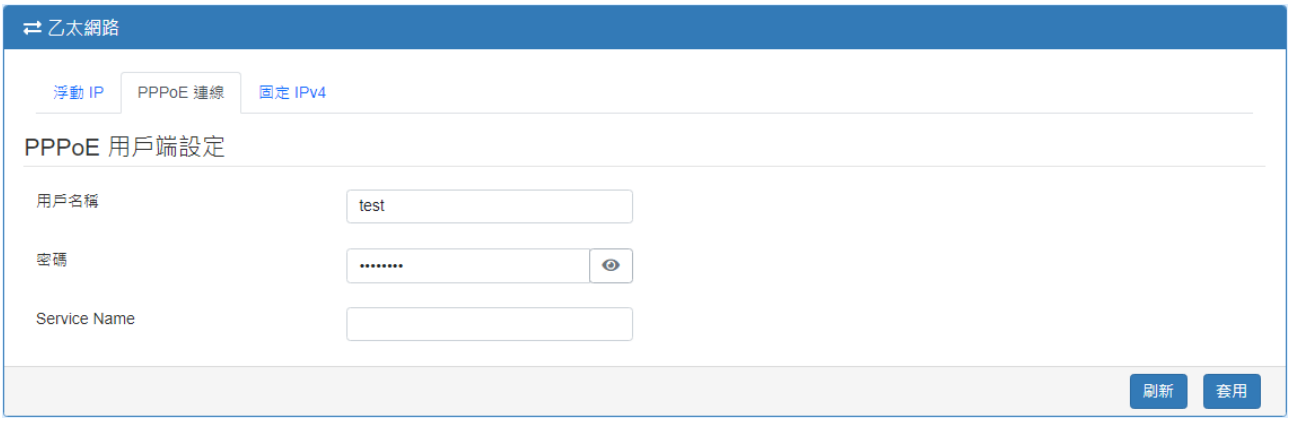
選擇「浮動 IP」 時，您可以配置 DNS 伺服器設定。

對於 IPv4 DNS 伺服器，它提供了三個選項進行設定，每個選項都提供了「從 ISP」，「用戶自訂」和「停用此列 DNS」以供設定。

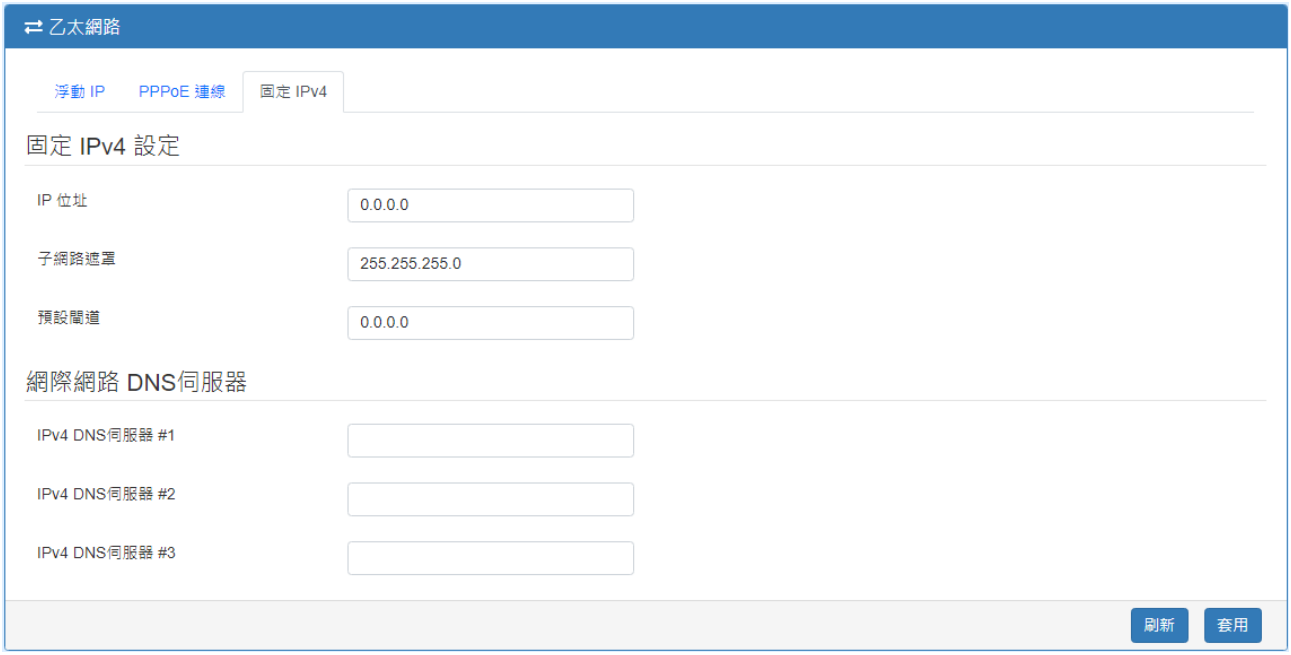


網際網路 > 乙太網路 > 浮動 IP	
項目	**描述**
IPv4 DNS 伺服器 #1 **IPv4 DNS 伺服器 #2** **IPv4 DNS 伺服器 #3**	• 每個選項都提供了「從 ISP」，「用戶自訂」和「停用此列 DNS」以供設定。 • 當您選擇「從 ISP」時，IPv4 DNS 伺服器 IP 將由 ISP 分配。 • 當您選擇「用戶自訂」時，用戶將手動輸入 IPv4 DNS 伺服器 IP。

當您選擇 PPPoE 連線時，介面會顯示用戶名稱和密碼以供填寫。Service Name 是一個可選填的設定。



當您選擇固定 IPv4 時，介面會顯示設定資訊，包括 IP 位址、子網路遮罩和預設閘道。

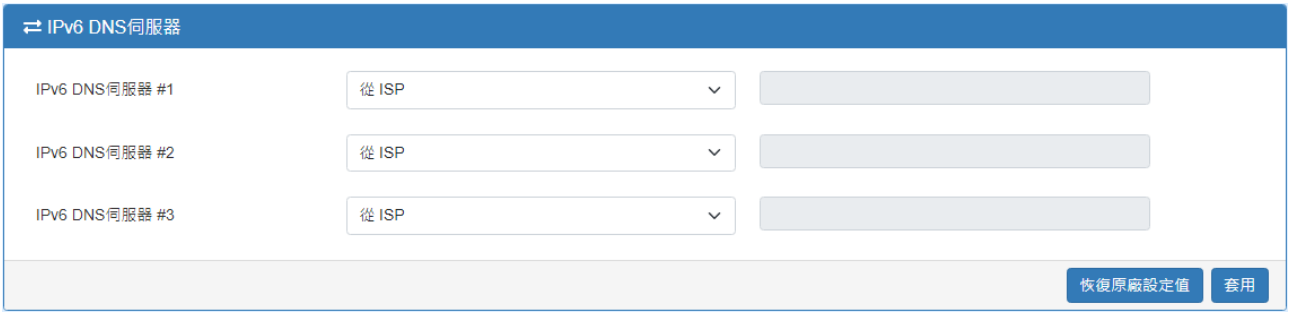


網際網路 > 乙太網路 > 固定 IPv4	
項目	**描述**
固定 IP 設定	
IP 位址	填寫 IP 位址。
子網路遮罩	填寫子網路遮罩。
預設閘道	填寫預設閘道。
網際網路 DNS 伺服器設定	
IPv4 DNS 伺服器 #1~3	用戶可以手動輸入 IPv4 DNS 伺服器 IP。

4.2 IPv6 DNS 伺服器

本部分允許您配置 IPv6 DNS 伺服器設定。

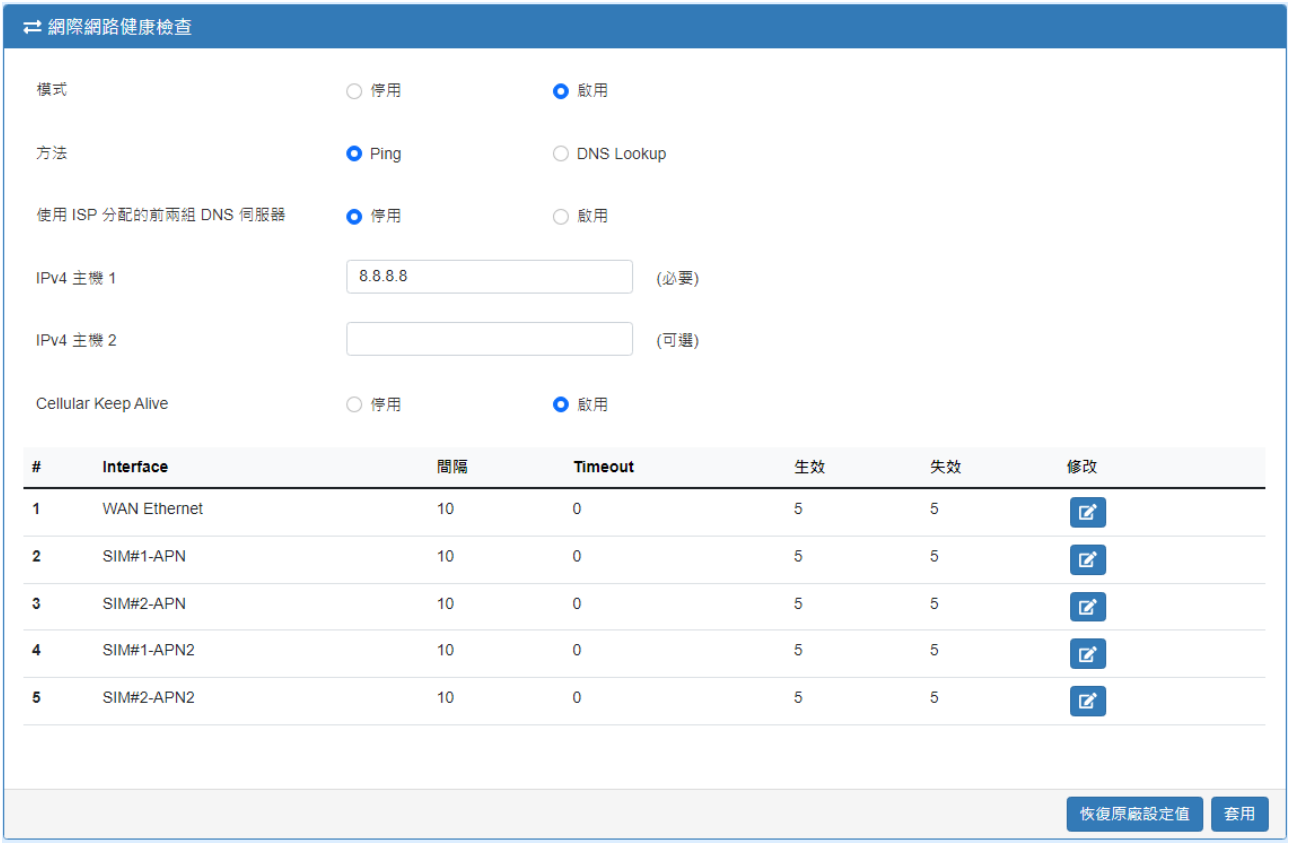
對於 IPv6 DNS 伺服器，它提供了三個選項進行設定，每個選項都提供了「從 ISP」，「用戶自訂」和「停用此列 DNS」以供設定。



網際網路 > IPv6 DNS	
項目	**描述**
IPv6 DNS 伺服器 #1 **IPv6 DNS 伺服器 #2** **IPv6 DNS 伺服器 #3**	• 每個選項都提供了「從 ISP」，「用戶自訂」和「停用此列 DNS」以供設定。 • 當您選擇「從 ISP」時，IPv6 DNS 伺服器 IP 將由 ISP 分配。 • 當您選擇「用戶自訂」時，用戶將手動輸入 IPv6 DNS 伺服器 IP。

4.3 網際網路健康檢查

本部分允許用戶設定網際網路健康檢查，針對 SIM 卡不同 APN 以及乙太網路網際網路進行健康檢查設定。



網際網路 > 網際網路健康檢查	
項目	**描述**
網際網路健康檢查	• 從「停用」或「啟用」中進行選擇。預設值為啟用。 • 選擇停用時，連接不會被視為 IP 路由錯誤關閉。
方法	此設定指定網際網路連接的健康檢查方法。此值可以是 PING、DNS Lookup。預設值為 Ping。 DNS Lookup : 如果從任何一個 DNS 伺服器收到 DNS 回應，則無論結果是肯定的還是否定的，連接都將被視為已建立。
使用 ISP 分配的前兩組 DNS 伺服器	• 如果選取此設定，則來自 ISP 的前兩個 DNS 將作為 DNS Lookup 的目標，用於檢查連接運行狀況。 • 如果未選取此設定，則必須填寫主機 1，而主機 2 的值是可選的。
IPv4 主機 1	輸入 IPv4 主機 1 的位址。
IPv4 主機 2	輸入 IPv4 主機 2 的位址。此欄位是選填的。
Cellular Keep Alive	啟用 Cellular Keep Alive 可以繼續發送網際網路健康檢查，以避免無網路流量導致運作被中斷。

5 導覽視窗 > 行動通訊

本部分允許您配置 SIM 設定、SIM 使用流量、簡訊、服務基站和 DNS 伺服器。

5.1 SIM 設定

此部分允許用戶配置 SIM 卡設定（如下圖）。

1. 勾選 SIM Card Lock Setting 啟用並輸入 SIM 卡 PIN 碼（如果有）。
2. 輸入電信商 APN 設定以建立網路連接（如果有），例如：連上中華電信行動網路，請輸入：internet。
3. 按下套用以套用 SIM 卡設定，如沒有成功連線，請重新開機。


SIM 設定
使用中 SIM 卡
SIM#1
斷線 (SIM#1)
The SIM card will not switchable after it is disconnected by the user.
停用漫遊
否
是
重試連線次數
3
(1 ~ 100) * 60 秒
SIM#1 設定
SIM#2 設定
Net Mode
鎖定 4G
1
狀態
已就緒
SIM Card Lock Setting
啟用
如有 SIM PIN，請勾選
修改 SIM PIN
變更
Unblock SIM card
Unblock
APN1
2
APN
internet
如需連上中華電信行動網路，請輸入 internet
用戶名稱
密碼
密碼
認證
NONE
Protocol
IPv4
MTU
1500
最小: 700; 最大: 1500
APN2
APN
用戶名稱
密碼
密碼
認證
NONE
Protocol
IPv4
MTU
1500
最小: 700; 最大: 1500
流量限制
已使用流量 (MB)
19
模式
停用
啟用
最大流量限制 (MB)
0
每月重設
日期: 31
時: 23
分: 0
秒: 0
現在時間
日期: 16
時: 14
分 16
秒 6
3
套用後，如沒有成功連線，請重新開機
恢復原廠設定值
套用

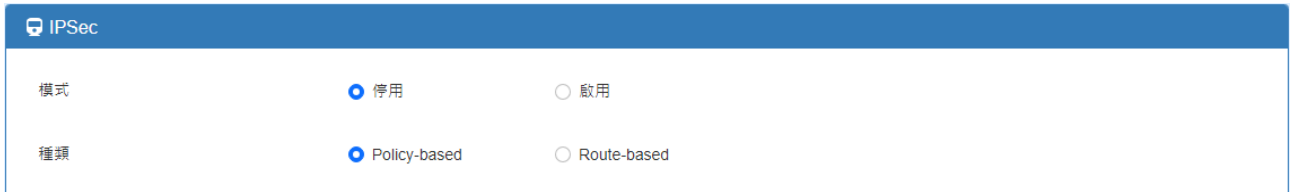
6 導覽視窗 > VPN

此部分允許您設定 OpenVPN、IPsec、GRE、PPTP 伺服器和 L2TP。

6.1 IPSec

此部分允許您設定 IPSec Tunnel。該設定有五個標記：連線、憑證 ID、X.509 憑證、CA 憑證和進階。

對於透過 PSK 進行身份驗證的 IPSec Tunnel，只需要設定連線和憑證 ID。對於透過 RSA 或 TLS 進行身份驗證的 IPsec Tunnel，設定必須涵蓋連線、憑證 ID、X.509 憑證和 CA 憑證四個部分。

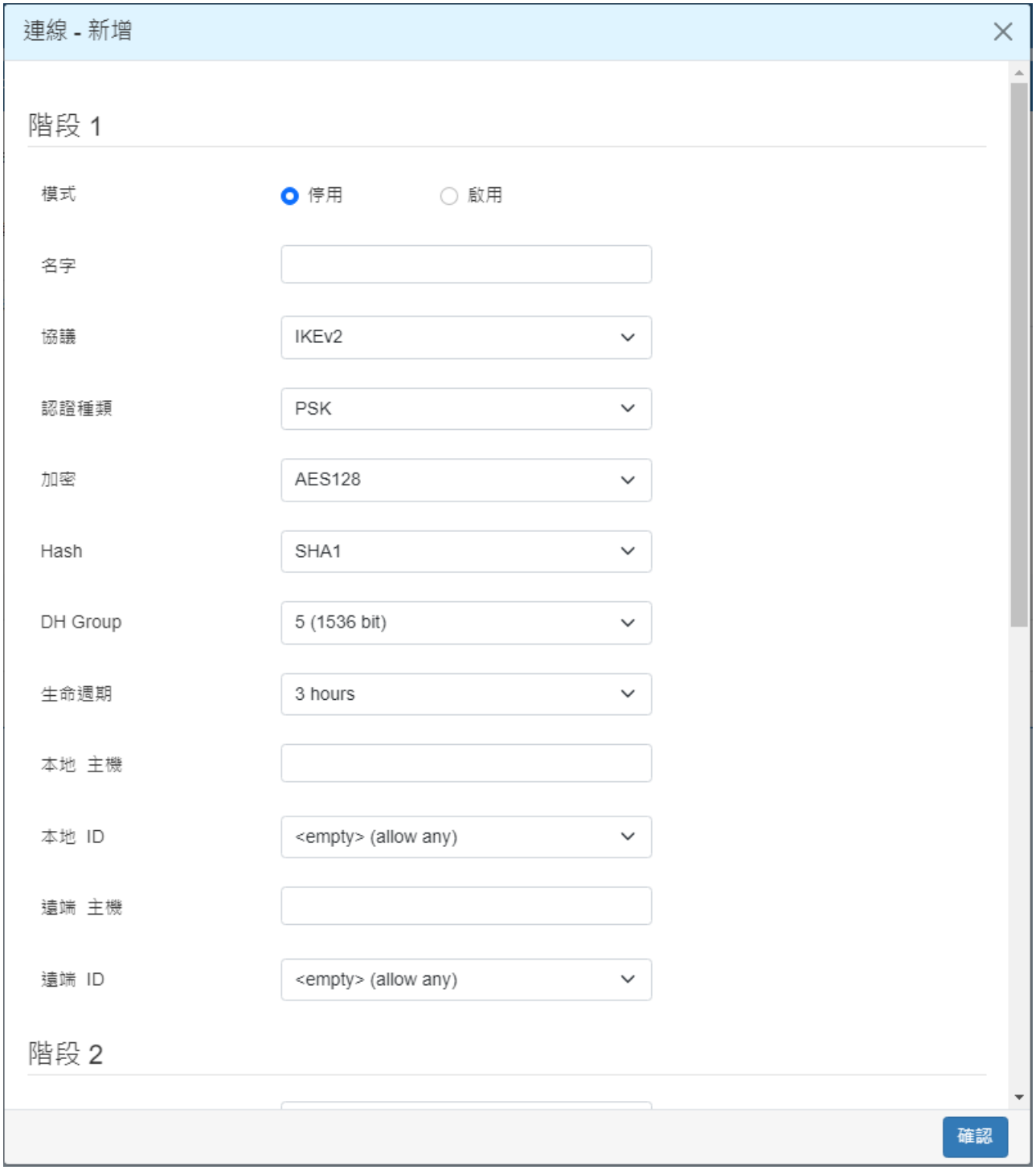


VPN > IPSec	
項目	**描述**
模式	從「停用」或「啟用」中進行選擇。預設值為停用。
種類	從「Policy-based」或「Route-based」中進行選擇。預設值為「Policy-based」。

IPSec > 連接

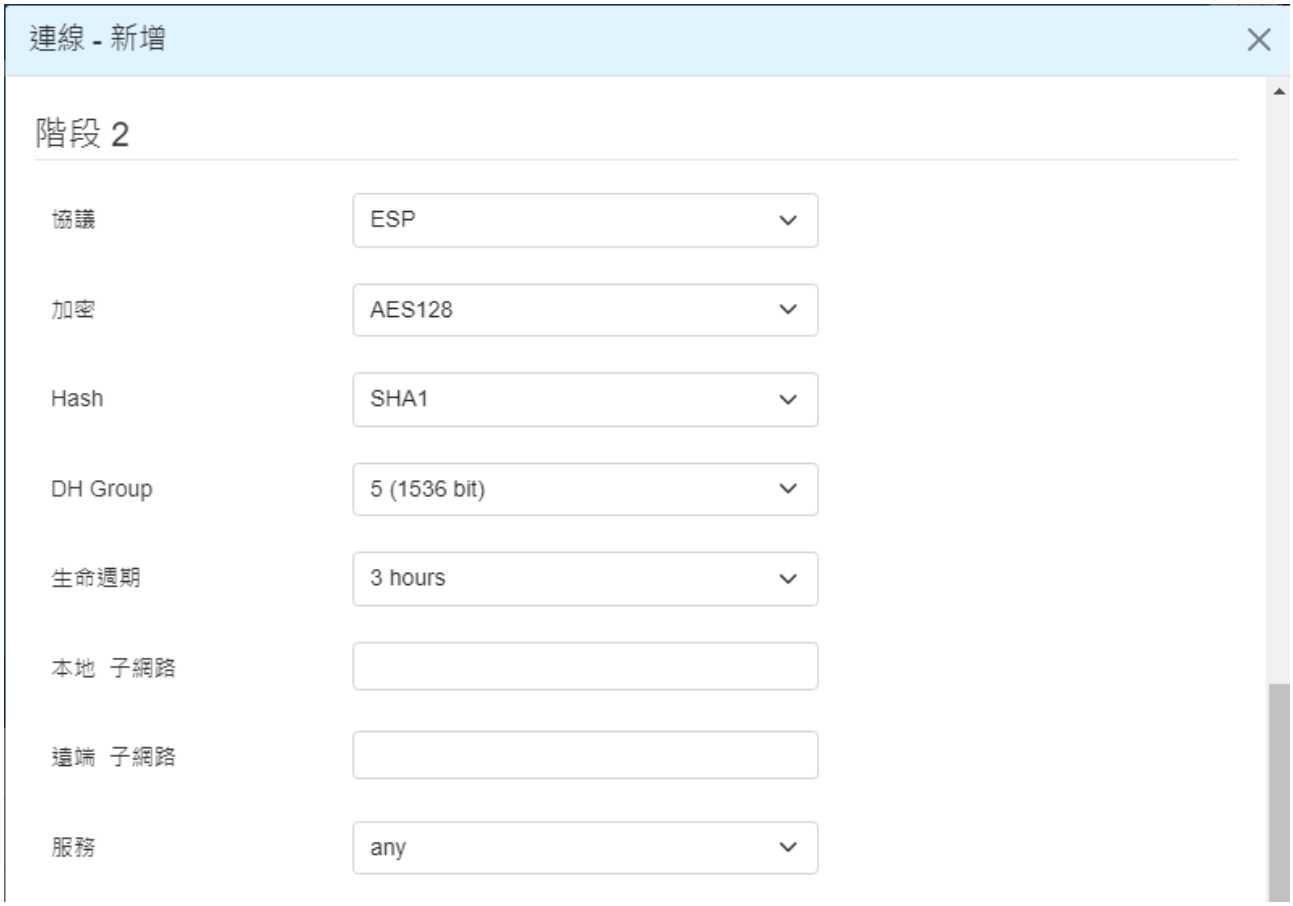
每個連線都會顯示**狀態**、**IKE 資訊**和 **Tunnel 資訊**。在預設設定中，連線清單為空。您可以透過按下 New 建立新連線。

IPSec >階段 1 設定


連線 - 新增
階段 1
模式
停用
啟用
名字
協議
IKEv2
認證種類
PSK
加密
AES128
Hash
SHA1
DH Group
5 (1536 bit)
生命週期
3 hours
本地 主機
本地 ID
<empty> (allow any)
遠端 主機
遠端 ID
<empty> (allow any)
階段 2
確認

VPN > IPSec > 連線 >Phase 1 設定	
項目	**描述**
模式	停用或啟用選定的 IPSec 連線。
名字	簡稱或描述。
協議	從 IKEv1 或 IKEv2 中選擇。預設為 IKEv2。
認證種類	從 PSK（預設）、RSA、EAP-TLS 中選擇。 （注意：EAP-TLS 僅適用於 IKEv2。）
加密	加密算法。 從 AES128（預設）、AES192、AES256 、3DES、DES、GCM64、GCM96、GCM128 等選項中選擇。
Hash	Hash 演算法。 從 MD5、SHA1（預設）或 SHA256 中選擇。
DH Group	Diffie-Hellman 算法。 由 1(768 bit), 2(1024 bit), 5(1536 bit) (default), 14(2048 bit), 15(3072 bit), 16(4096 bit), 17(6144 bit) or 18(8192 bit)中選擇。
生命週期	連接的加密通道的長度。 選擇 30 分鐘、1 小時、2 小時、3 小時、6 小時、12 小時或 24 小時。
本地 主機	路由器網際網路介面的 IP 位址。 如果值為空，連線將自動偵測正確的 IP 位址。
本地 ID	用於本地與對等網路的身份認證。 從建立的身份驗證 ID 中選擇或為空。
遠端 主機	遠端網際網路介面的 IP 位址。 如果該值為空，則連線將充當伺服器角色來等待傳入請求。
遠端 ID	用於遠端與對等網路的身份認證。 從建立的身份驗證 ID 中選擇或為空。

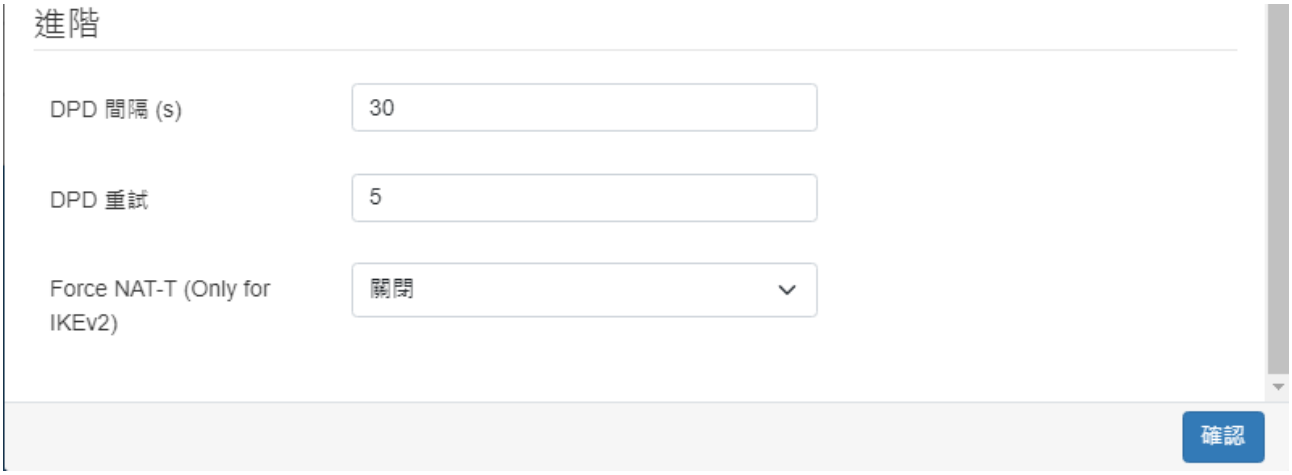
IPSec >階段 2 設定



VPN > IPSec > 連線 >Phase 2 設定	
項目	**描述**
協議	僅支援 ESP。
加密	加密算法。 從 AES128 (預設) 、AES192、AES256 、3DES、DES、GCM64、GCM96、GCM128 等選項中選擇。
Hash	Hash 演算法。 從 MD5、SHA1 (預設) 或 SHA256 中選擇。
DH Group	Diffie-Hellman 算法。 由 1(768 bit), 2(1024 bit), 5(1536 bit) (default), 14(2048 bit), 15(3072 bit), 16(4096 bit), 17(6144 bit) or 18(8192bit)中選擇。
生命週期	連接的加密通道的長度。 選擇 30 分鐘、1 小時、2 小時、3 小時、6 小時、12 小時或 24 小時。

本地 子網路	路由器後面的私有子網路。 可用格式為 A.B.C.D、A.B.C.D/M、A.B::C.D 或 A.B::C.D/M 如果值為空，連線會將其設定為第一階段設定的「本機主機」。 *備註：*此選項僅適用於 Policy-based 的 IPsec VPN 種類。
遠端 子網路	對等網路後面的私有子網路。 可用格式為 A.B.C.D、A.B.C.D/M、A.B::C.D 或 A.B::C.D/M 如果該值為空，則連線會將其設定為第一階段設定的「遠端主機」。 *備註：*此選項僅適用於 Policy-based 的 IPsec VPN 種類。
服務	限制 VPN 流量只使用特定協定。 從任意、TCP、UDP 或 L2TP 中進行選擇。

IPSec 進階設定



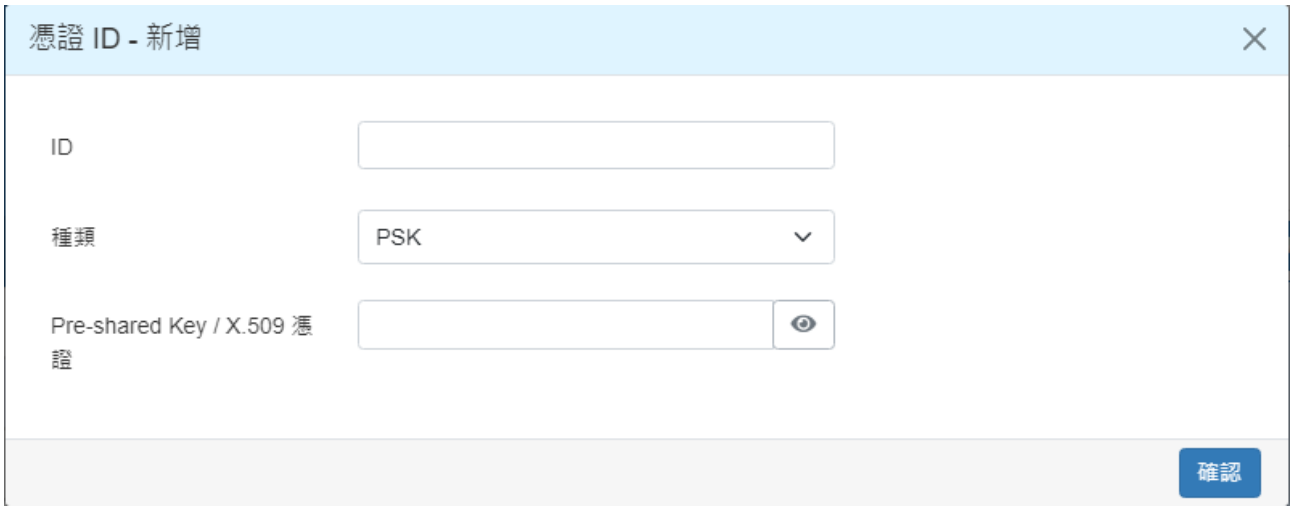
VPN > IPSec > 連線 >進階設定	
項目	**描述**
DPD 間隔(s)	對等網路死亡檢測的時間間隔。 預設值為 30 秒。
DPD 重試	對等網路死亡檢測的最大重試次數。 預設為 5 次。
Force NAT-T (Only for IKEv2)	為選定的 IPSec 連線啟用或停用 NAT-T。

*備註：*詳細與 Check point 連線的設定，請參閱附錄 Application Note。

IPSec > 憑證 ID

本部分提供用於驗證 IPsec 連線的憑證 ID。

預設情況下，憑證 ID 清單為空。您可以透過按下 New 建立新的身份驗證 ID。



VPN > IPSec > 憑證 ID	
項目	**描述**
ID	用於身份驗證的 ID，僅適用於 PSK 類型。
種類	從 PSK 或 RSA 中選擇。預設為 PSK。 PSK：使用 Pre-shared Key 來驗證連線。 RSA：使用憑證來驗證連線。
Pre-shared Key/ X.509 憑證	Pre-shared Key：輸入 Pre-shared Key。 X.509 憑證：用於身份驗證的 X.509 憑證，由 X.509 憑證部分產生或匯入。

根據上述選項，提供一些可以驗證 IPsec 連線的組合。

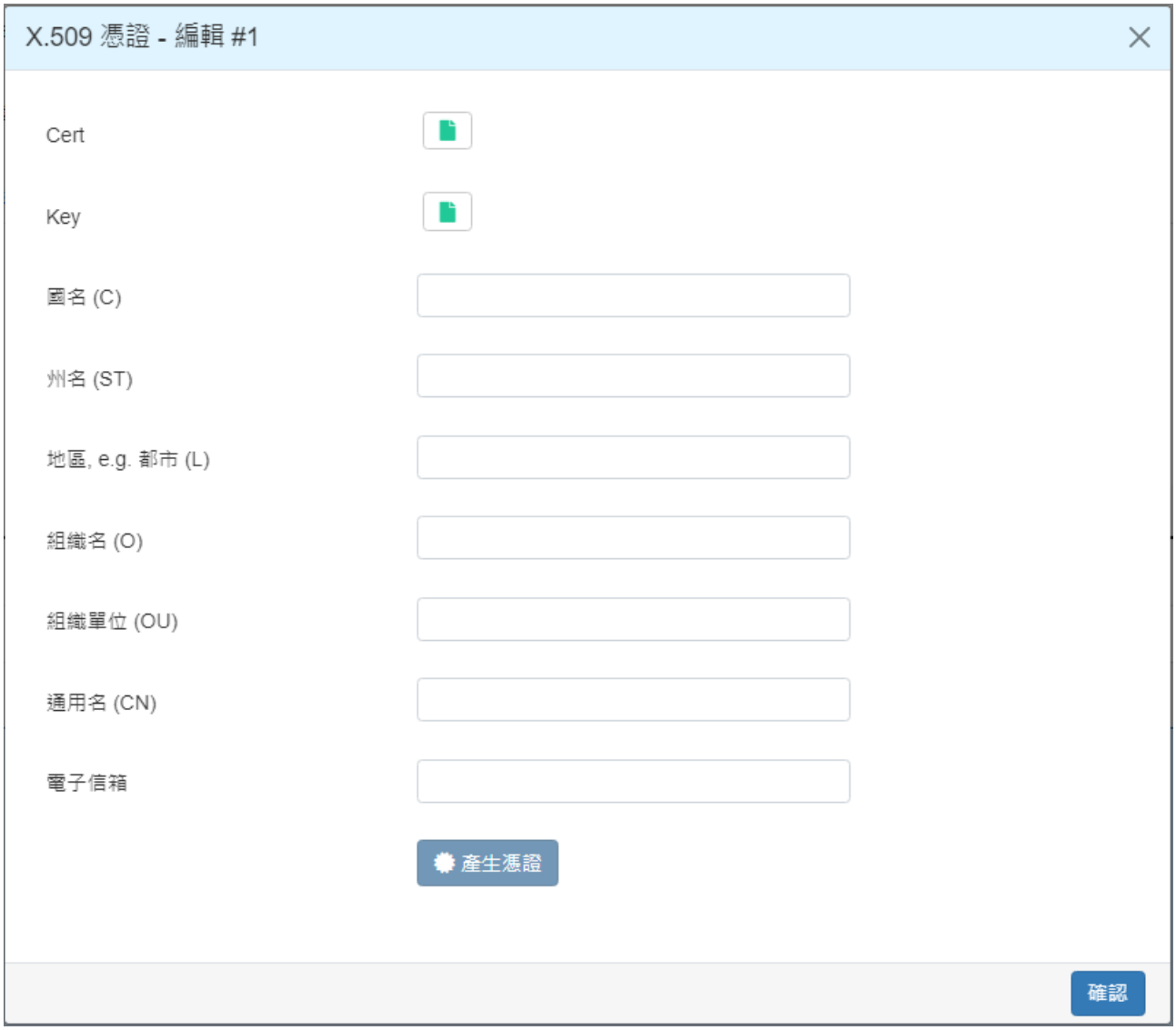
VPN > IPsec > 憑證 ID				
#	ID	類型	Pre-shared Key/ X.509 憑證	描述
1		PSK	password	PSK 連線的預設密碼。
2	remote.ipsec	PSK	2wsx#EDC	僅適用於具有遠端 IPsec ID 的 PSK 連線的密碼。 通常，這種情況用於驗證對端網路閘道器。
3	local.ipsec	PSK		連線 ID。 通常，這種情況用於公佈路由器的 ID。
4	test	RSA	CreatedX.509	ID 欄位將被省略，並且使用 X.509 的通用名稱(CN)作為 ID 欄位。

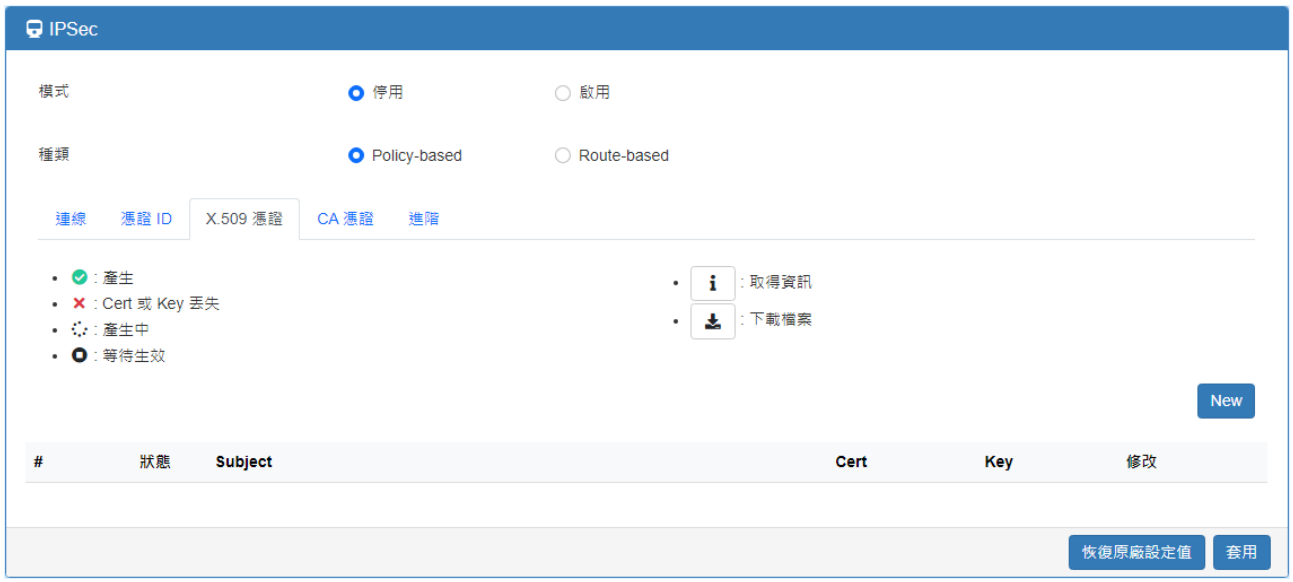
IPsec > X.509 憑證

本節提供 IPsec 驗證 ID 所使用的憑證設定。

每張憑證都會顯示**狀態**和 **Subject 的**資訊。

預設情況下，X.509 憑證清單為空。您可以透過按下 New 建立新的身份驗證 ID，此部份須結合自簽 CA 憑證使用。


X.509 憑證 - 編輯 #1
Cert
Key
國名 (C)
州名 (ST)
地區, e.g. 都市 (L)
組織名 (O)
組織單位 (OU)
通用名 (CN)
電子信箱
產生憑證
確認

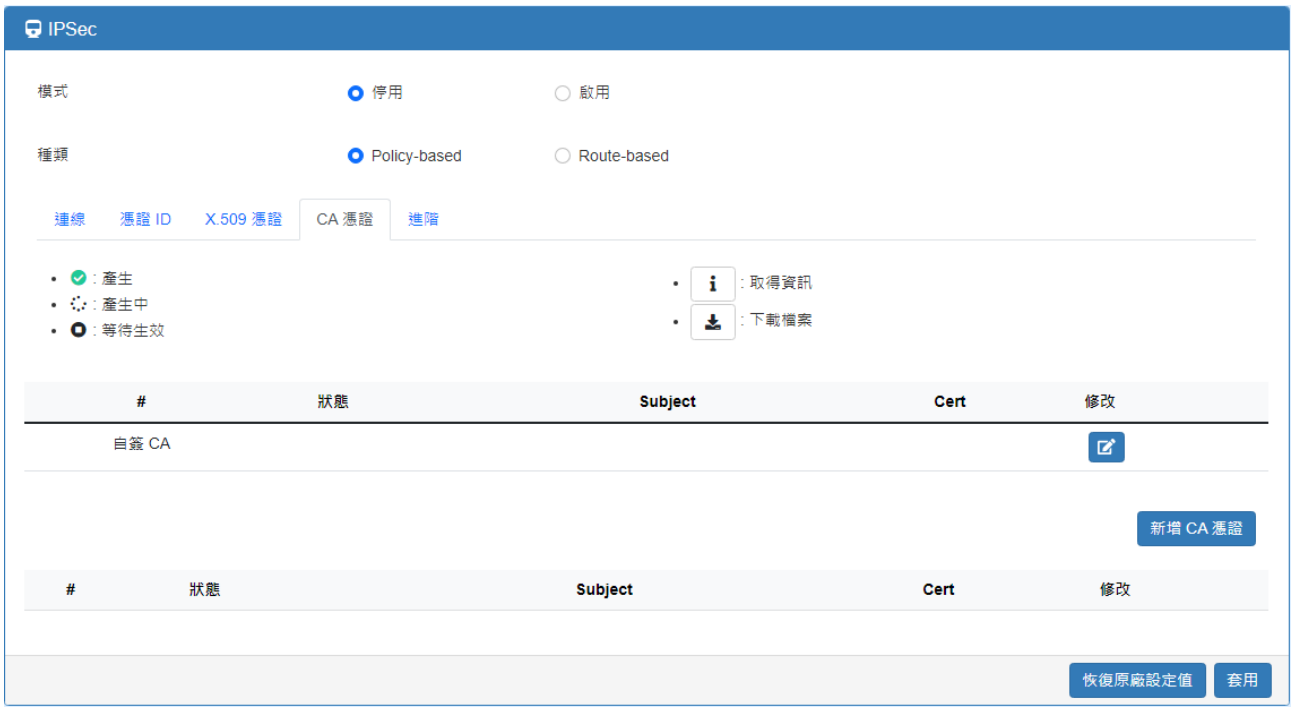

IPSec
模式
停用
啟用
種類
Policy-based
Route-based
連線
憑證 ID
X.509 憑證
CA 憑證
進階
: 產生
: Cert 或 Key 丟失
: 產生中
: 等待生效
: 取得資訊
: 下載檔案
New
狀態 Subject Cert Key 修改
恢復原廠設定值
套用

IPSec > CA 憑證

本節提供 CA 憑證設定，可以檢查 X.509 憑證是否有效。

有一個自簽名 CA（由路由器產生），亦可支援用戶將自簽名 CA 匯入到路由器中。自簽名 CA 將幫助路由器驗證自簽名 X.509 憑證，該憑證在 X.509 憑證部分匯入。

每個 CA 憑證都會顯示**狀態**和 **Subject** 資訊並提供控制按鈕，讓用戶可以下載或編輯憑證/密鑰檔案。



產生憑證

路由器產生的憑證有兩種，一種是自簽名 CA，另一種是 X.509。

產生自簽章 CA 憑證：

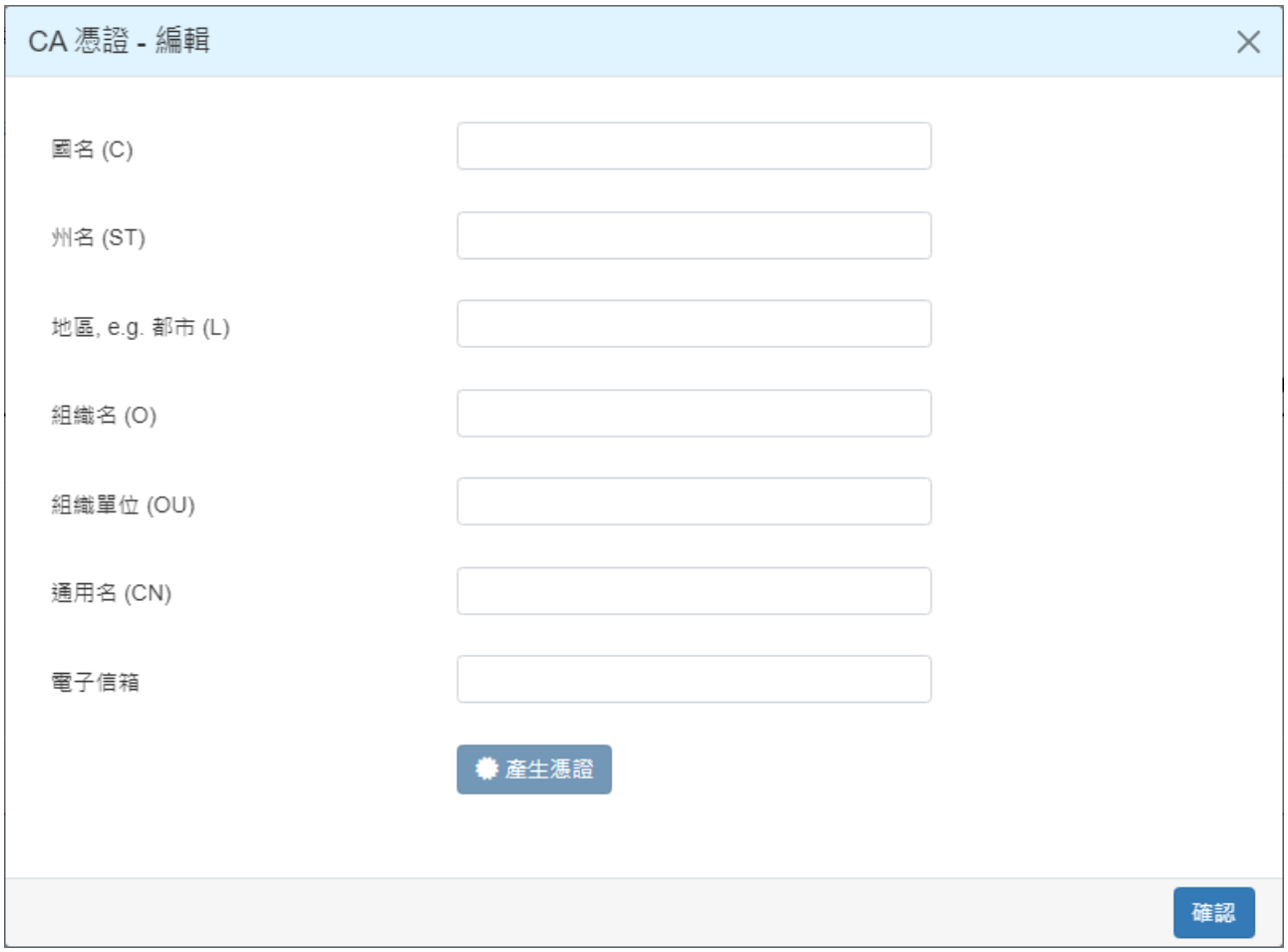
1. 到 CA 憑證的分頁標籤。
2. 按下  按鈕來編輯**憑證設定**。
3. 填寫 CA 憑證資訊。
4. 按下 產生憑證 按鈕並 確定
5. 按下 套用 按鈕以套用更改。

產生 X.509 憑證：

1. 確保已產生自簽 CA 憑證。

2. 到 X.509 憑證的分頁標籤。
3. 透過新建按鈕新增 X.509 憑證（如無）。
4. 按下  按鈕來編輯**憑證設定**。
5. 填寫 X.509 憑證資訊。
6. 按下產生憑證按鈕並確定
7. 按下套用按鈕以套用更改。

憑證設定



VPN > IPSec > 憑證 ID	
項目	**描述**
國名 (C)	2 個字母的國家/地區代碼（必填），例如：US。
州名 (ST)	州名，例如：某個國家。
地區, e.g. 都市 (L)	地區名稱，例如：城市名。

組織名 (O)	組織名稱（必填），例如：公司名稱。
組織單位 (OU)	組織單位名稱。
通用名 (CN)	與憑證關聯的主機名稱（必填），例如：example.com。
電子信箱	維護者的電子信箱。

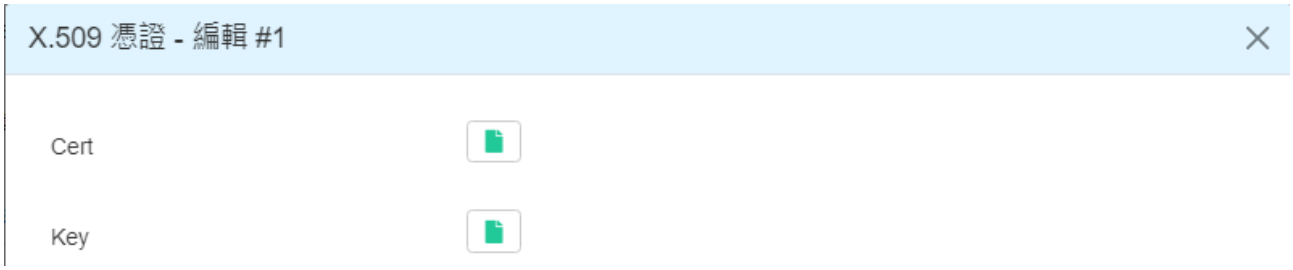
憑證匯入

與**產生憑證**相同，路由器支援 CA 和 X.509 憑證匯入。
匯入 CA 憑證：

1. 到 CA 憑證的分頁標籤。
2. 按下新增 CA 憑證按鈕。
3. 從瀏覽器視窗選擇 CA 憑證資訊。
4. 當文件被選擇並且一切正常後，新的 CA 憑證將顯示 狀態。

產生 X.509 憑證：

1. 到 X.509 憑證的分頁標籤。
2. 按下 New 按鈕。清單將彈出空白的 X.509 條目。
3. 按下 編輯按鈕來導覽**憑證設定**。
4. 按一下 Cert 匯入按鈕 。
5. 從瀏覽器視窗中選擇 X.509 憑證檔案。
6. 當文件被選擇並且一切正常時，狀態應該是 Cert 或 Key 丟失。
7. 按下 Key 匯入按鈕 。
8. 從瀏覽器視窗中選擇 X.509 密鑰檔案。
9. 當顯示 狀態，匯入程序完成。



下載憑證

如果產生或匯入了憑證，將會有下載按鈕下載每個 Cert 和 key 檔案。

備註： 當連線通過 RSA 或 EAP-TLS 進行驗證時，用戶必須下載 X.509 憑證、key 和 CA 憑證，並將檔案匯入遠端網路閘道器。

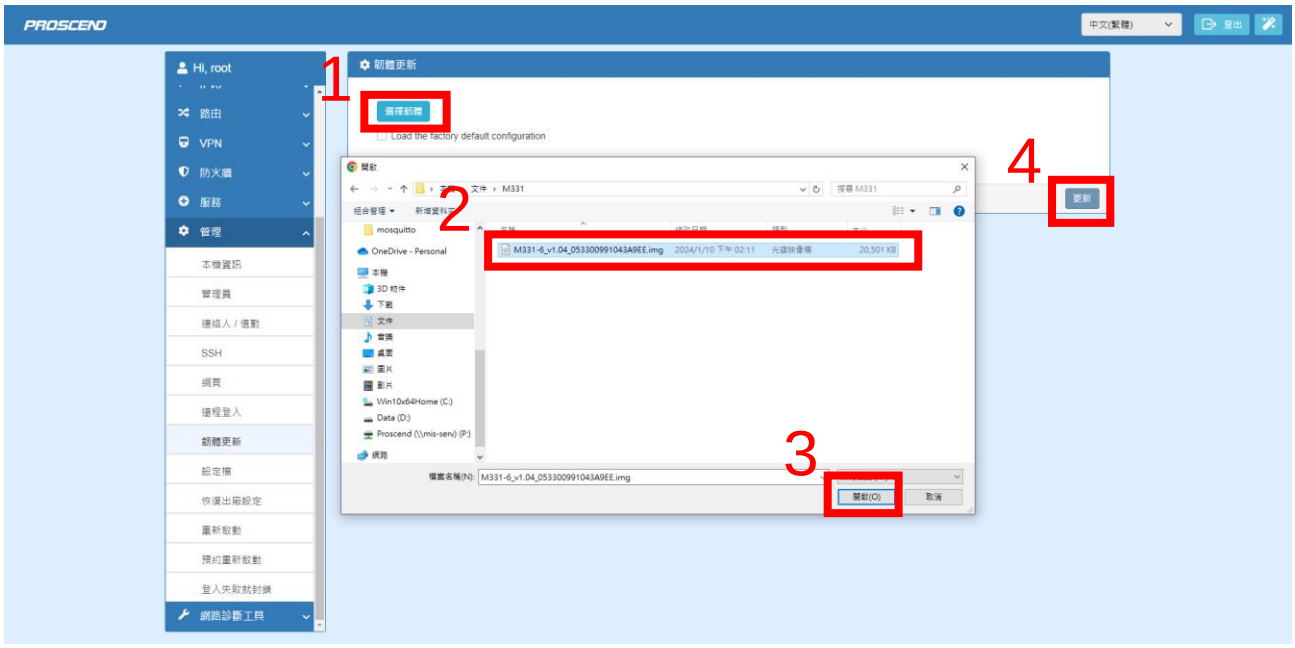
7 導覽視窗 > 管理

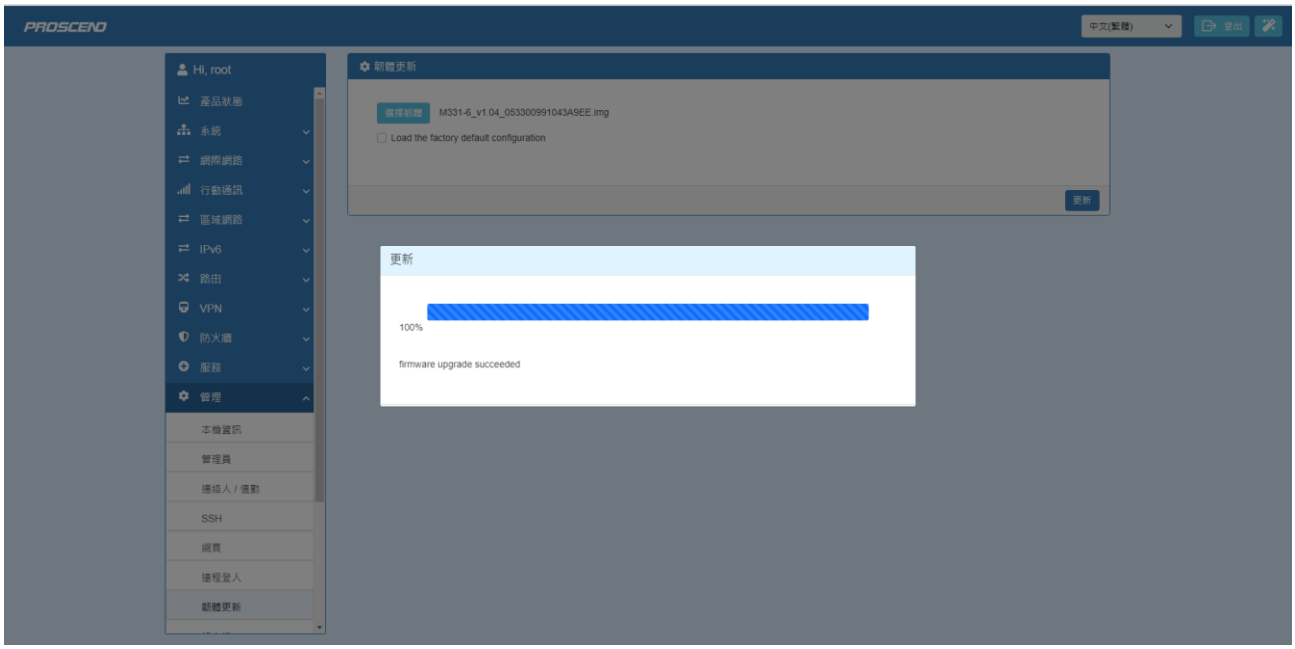
此部分為您提供管理路由器、設定管理員以及了解當前軟體和韌體的狀態。此外，您還可以備份和恢復設定。

7.1 韌體更新

此部分允許升級設備的韌體。

1. 按下選擇韌體（請聯絡客服並提供相關資訊以取得所需韌體）。
2. 選取所需韌體。
3. 按下開啟。
4. 按下更新，並至少等待 3 分鐘，更新完成後頁面會自動重新存取網頁管理頁面，亦可於網頁瀏覽器自行輸入 http://192.168.1.1/ 以存取網頁管理頁面。


PROSCEND
中文(繁體)
登出
Hi, root
韌體更新
1
選擇韌體
Load the factory default configuration
2
4
更新
3
開啟(O)
取消
路由
VPN
防火牆
服務
管理
本機資訊
管理員
連絡人 / 信動
SSH
網頁
遠程登入
韌體更新
設定檔
恢復出廠設定
重新啟動
預約重新啟動
登入失敗封鎖
網路診斷工具


PROSCEND
中文(繁體)
登出
Hi, root
韌體更新
選擇韌體
M331-6_v1.04_053300991043A9EE.img
Load the factory default configuration
更新
更新
100%
firmware upgrade succeeded

8 故障排除指南

8.1 故障排除資訊

如果您遇到任何問題，請先參考以下故障排除指南表，瞭解常見問題的解決方案：

如果您在下表找不到您遇到的問題，請參閱使用手冊以獲取可以幫助您解決問題的更多資訊。

問題類型表		
#	問題類型	描述
1	電源燈號未亮。	行動通訊路由器沒電。
2	無法存取網頁管理頁面。	行動通訊路由器存取問題。
3	無法使用行動通訊路由器上網。	您的 LTE 網路沒有網際網路。

電源燈號未亮問題

#問題 1：行動通訊路由器沒電。

對於可能的解決方法，請嘗試以下操作：

a. 從電源上拔下並重新插入電源配接器。

b. 斷開乙太網路線並重新連接行動通訊路由器的乙太網路埠口。

如果上述方法未能解決您的「沒電」問題，請聯繫您的支援工程師進行進一步的故障排除。（這可能涉及需要識別和解決的可能軟體或硬體問題）。

無法存取網頁管理頁面問題

#問題 2：行動通訊路由器存取問題。

對於可能的解決方法，請嘗試以下操作：

a. 檢查您的 PC 乙太網路卡是否已啟用並設定為自動獲取 IP/DNS 位址。

b. 斷開乙太網路線並將其與行動通訊路由器的乙太網路埠口連接。

c. Ping 區域網路 IP（預設 IP 為 192.168.1.1），ping 應為 PASS。

d. 如果 ping 正常，請嘗試再次存取網頁管理頁面。

如果上述方法未能解決您的存取問題，請聯繫您的 MIS 或任何建立網路基礎設施的人來解決 ping 失敗問題。

如果確認您的網路基礎設施正常（硬體工作正常且設定正確），請聯繫您的支援工程師進行進一步的故障排除。（這可能涉及需要識別和解決的可能軟體或硬體問題）。

無法使用行動通訊路由器上網問題

#問題 3：您的 LTE 網路沒有網際網路。

問題可能出在 SIM 卡的物理接觸上。

- 對於可能的解決方案 1，請嘗試以下操作：

a. 取出 SIM 卡。

b. 請重新插入（確保 SIM 卡處於正確的位置）。

c. 通過關閉/啟動電源重新啟動行動通訊路由器。

d. 等待至少 3 分鐘，然後再次檢查您是否正確接收網際網路。

如果以上方法沒有解決您的「沒有網際網路」問題，請繼續嘗試以下的解決方案 2。

- 對於可能的解決方案 2，請嘗試以下操作：

a. 存取網頁管理頁面（預設 URL 為 http://192.168.1.1/）。

b. 通過轉到「行動通訊 > SIM 設定」網頁來檢查 SIM 設定是否正常，詳情請參閱使用手冊 SIM 設定。

c. 如果您更改任何設定，請在套用后等待 2 分鐘，然後再次檢查網際網路。

d. 如果沒能成功連上網際網路，請重新開機。

如果上述方法未能解決您的「沒有網際網路」問題，請檢查您的 SIM 卡是否處於活動狀態並啟用了流量（通過聯繫您的 SIM 卡供應商或在其他設備中嘗試該 SIM 卡）。

如果您仍然遇到「沒有網際網路問題」，請聯繫您的支援工程師進行進一步的故障排除。（這可能涉及需要識別和解決的可能軟體或硬體問題）。

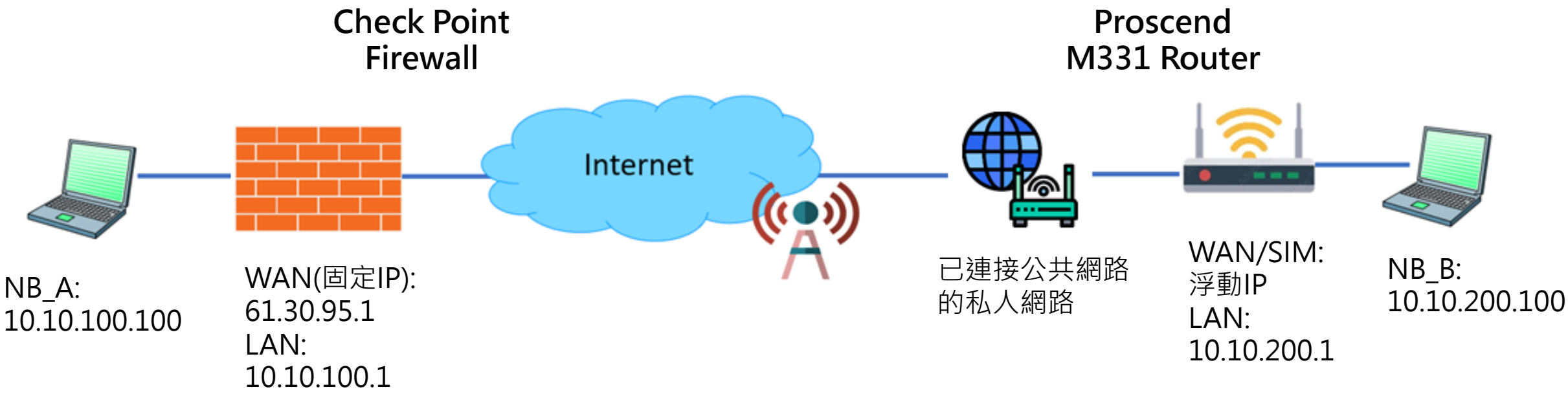
Application Note

PROSCEND

CheckPoint Firewall IPsec VPN with M331

01/29/24

Topology



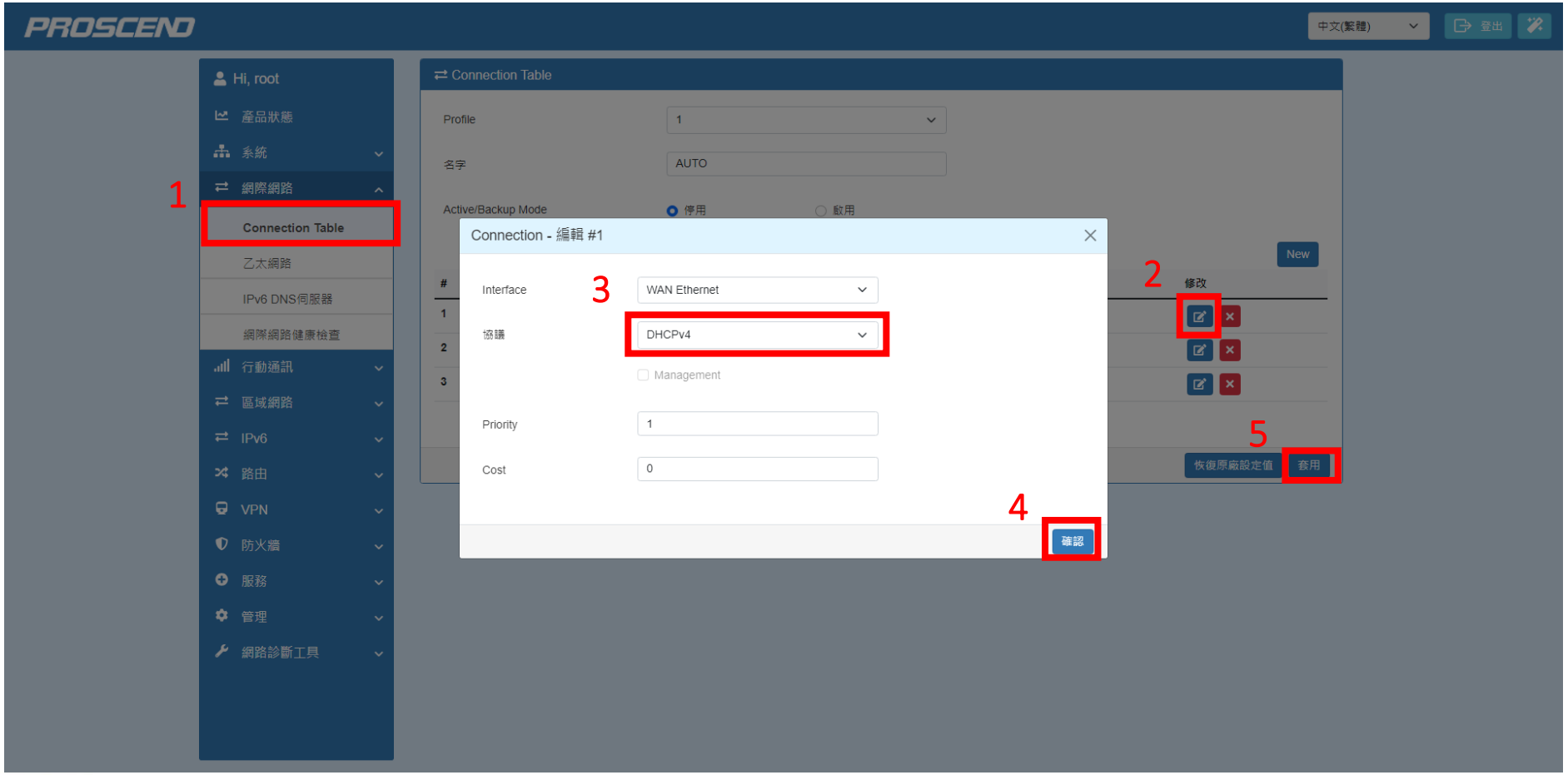
1. M331 4G Router可以為WAN或SIM Card方式
2. Lab環境使用IKEv1 Aggressive Mode
3. M331如使用浮動IP，須連接到已有公共網路的私人網路或直連到有DHCP功能的公共網路。

M331版本資訊

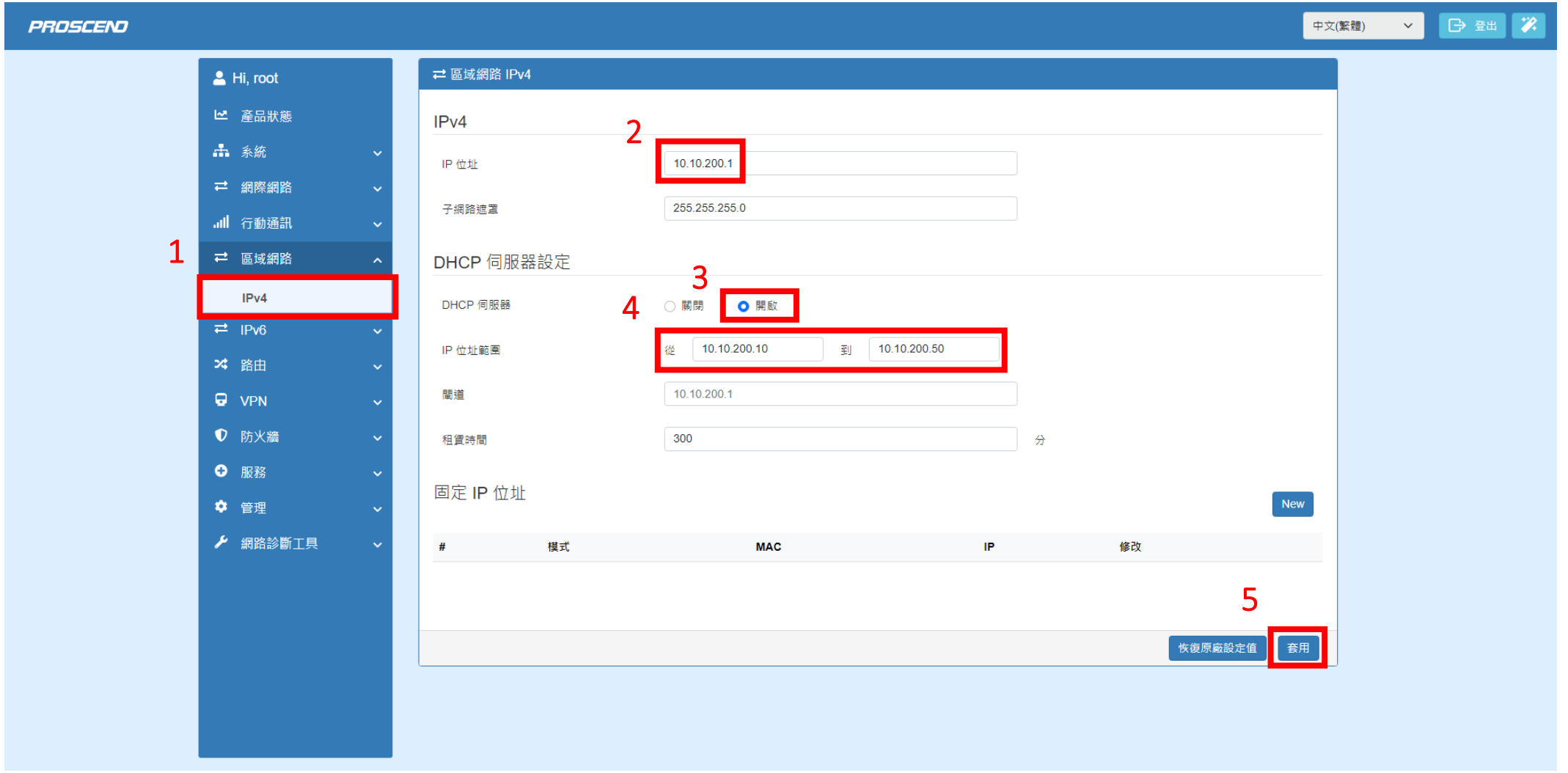

PROSCEND
中文(繁體)
登出
Hi, root
產品狀態
系統
網際網路
行動通訊
區域網路
IPv6
路由
VPN
防火牆
服務
管理
本機資訊
管理員
連絡人 / 值勤
SSH
網頁
遠程登入
韌體更新
本機資訊
目前使用中的分割區 B
型號名稱 M331
主機名稱 M331
區域乙太網路 MAC 位址 00:03:79:08:FF:D8
Bootloader 版本 V100.03
韌體版本 V1.03
韌體 MCSV 05330095103384E6
硬體 MCSV 05330095103384E6
雙韌體 A MCSV 05330095103384E6
雙韌體 B MCSV 05330095103384E6
序號 BLEQ448C0000
數據機韌體版本 LE20B01SIM7600M22_THREMALB01V02
IMEI 868020033397034
運行時間 10:26:32
刷新

M331 WAN設定

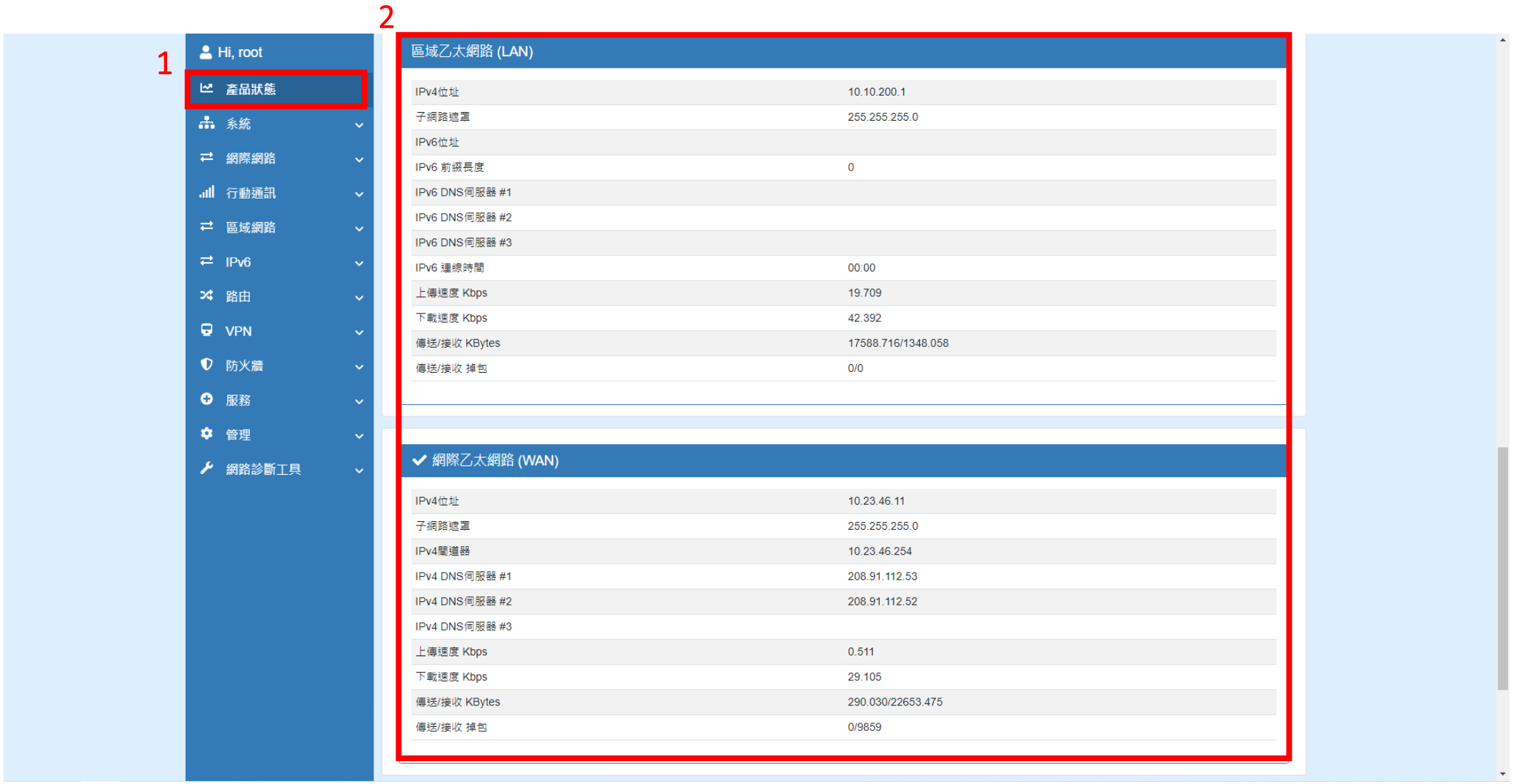
依現場環境調整，WAN可能為DHCPv4/Static IP/PPPoE方式，SIM則為DHCP模式。
此應用使用DHCP，設備連接WAN到已有公共網路的私人網路。



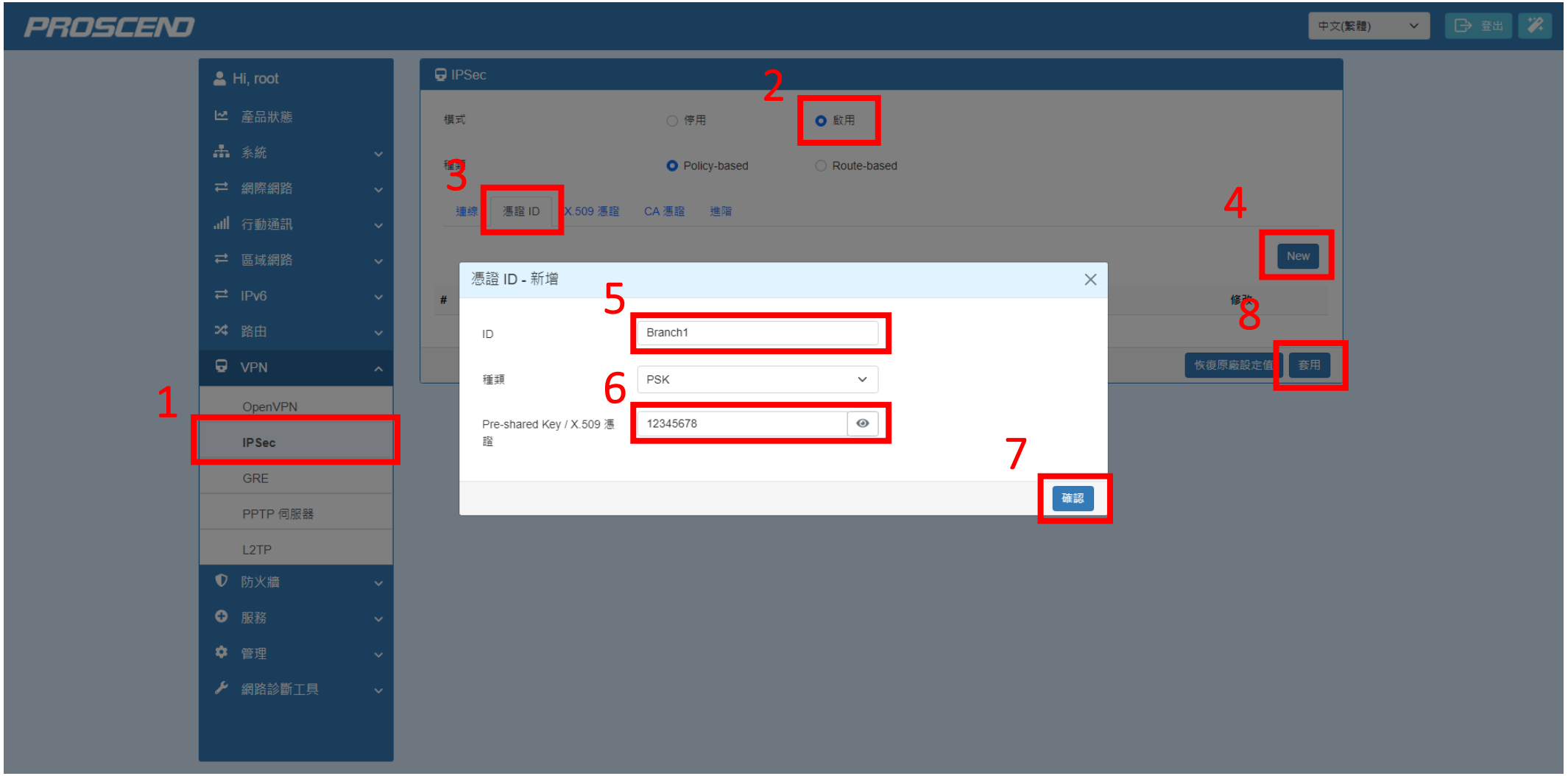
M331 LAN網路設定



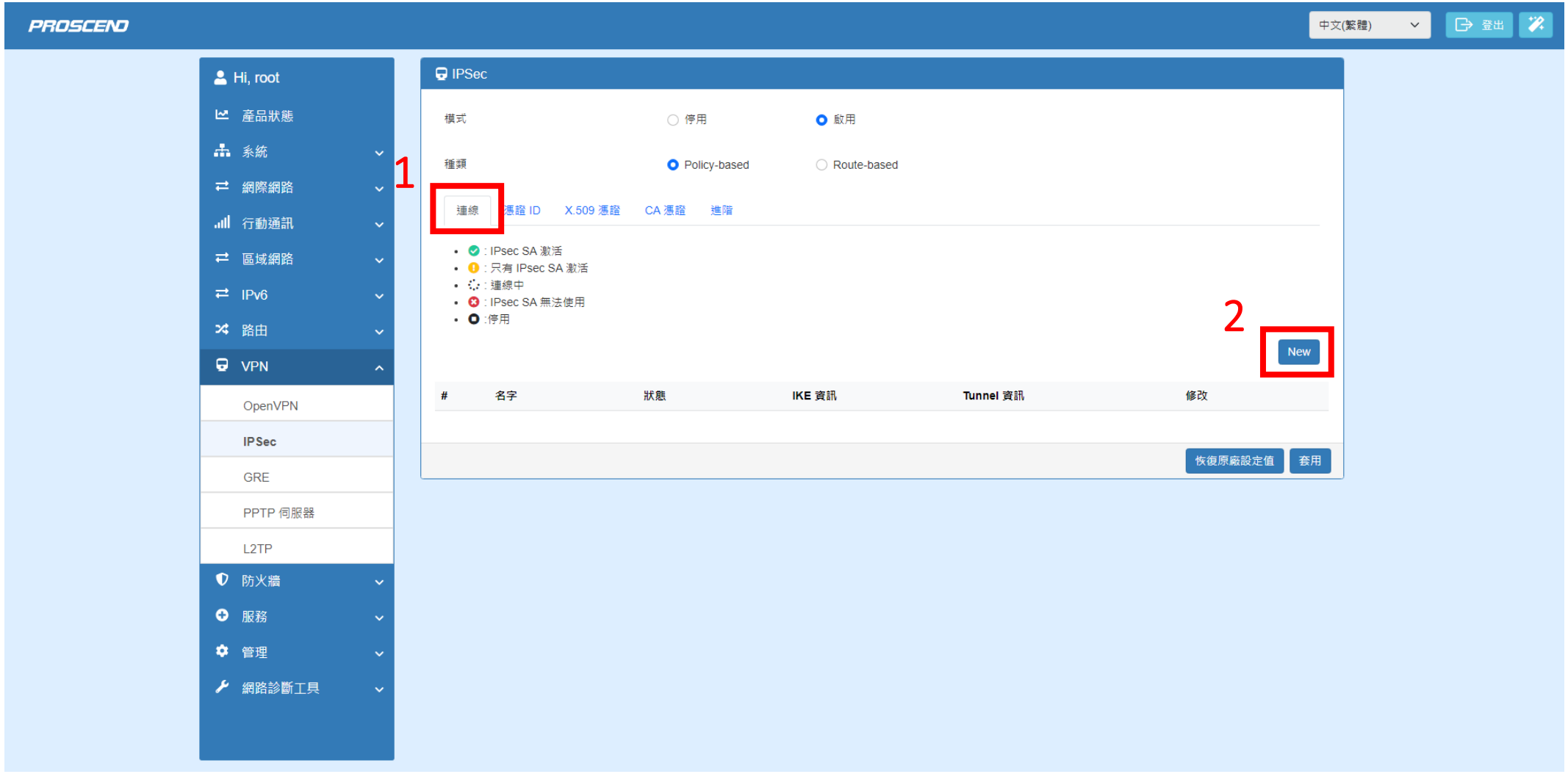
M331 WAN/LAN網路資訊



M331-6#1 VPN IPSec設定 - 1



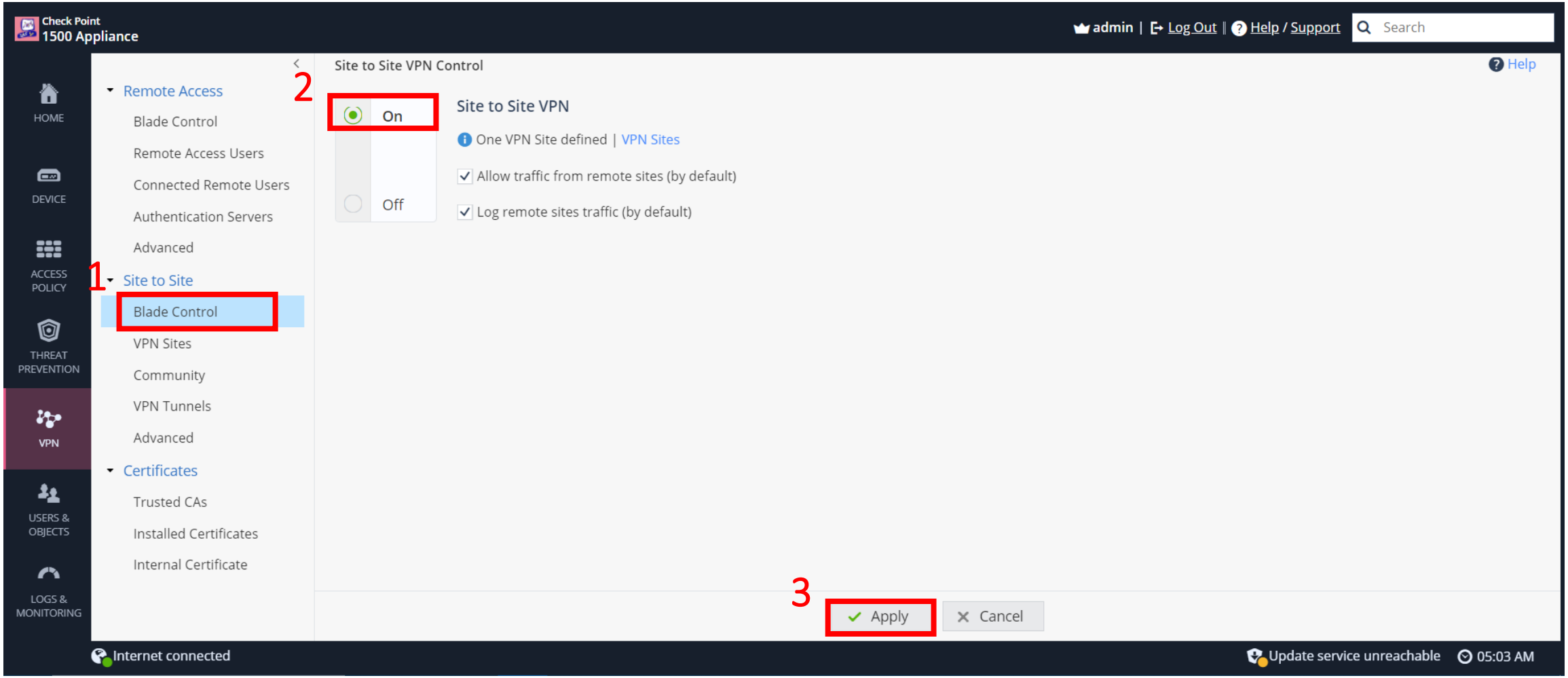
M331-6#1 VPN IPSec設定 - 2



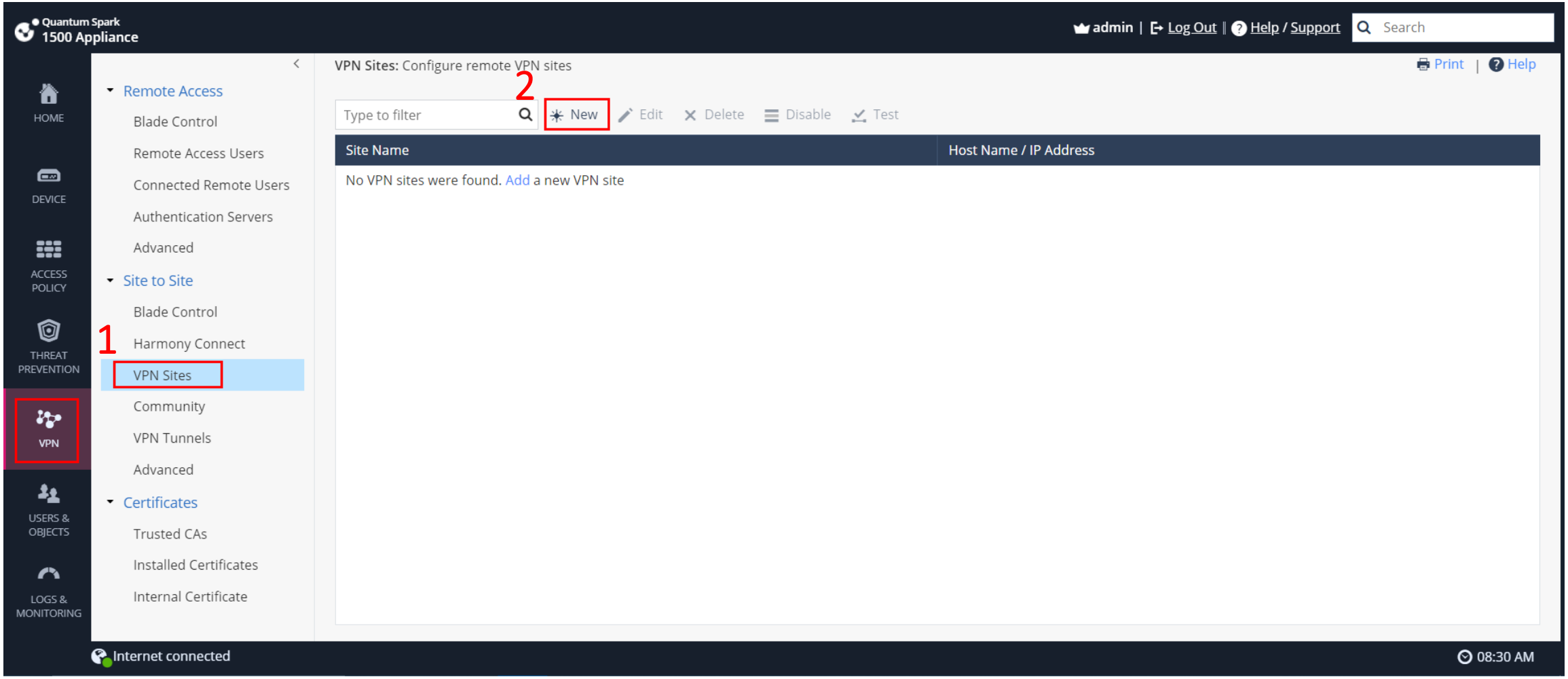
M331-6#1 VPN IPSec設定 - 3

M331-6#1 VPN IPSec設定 - 4

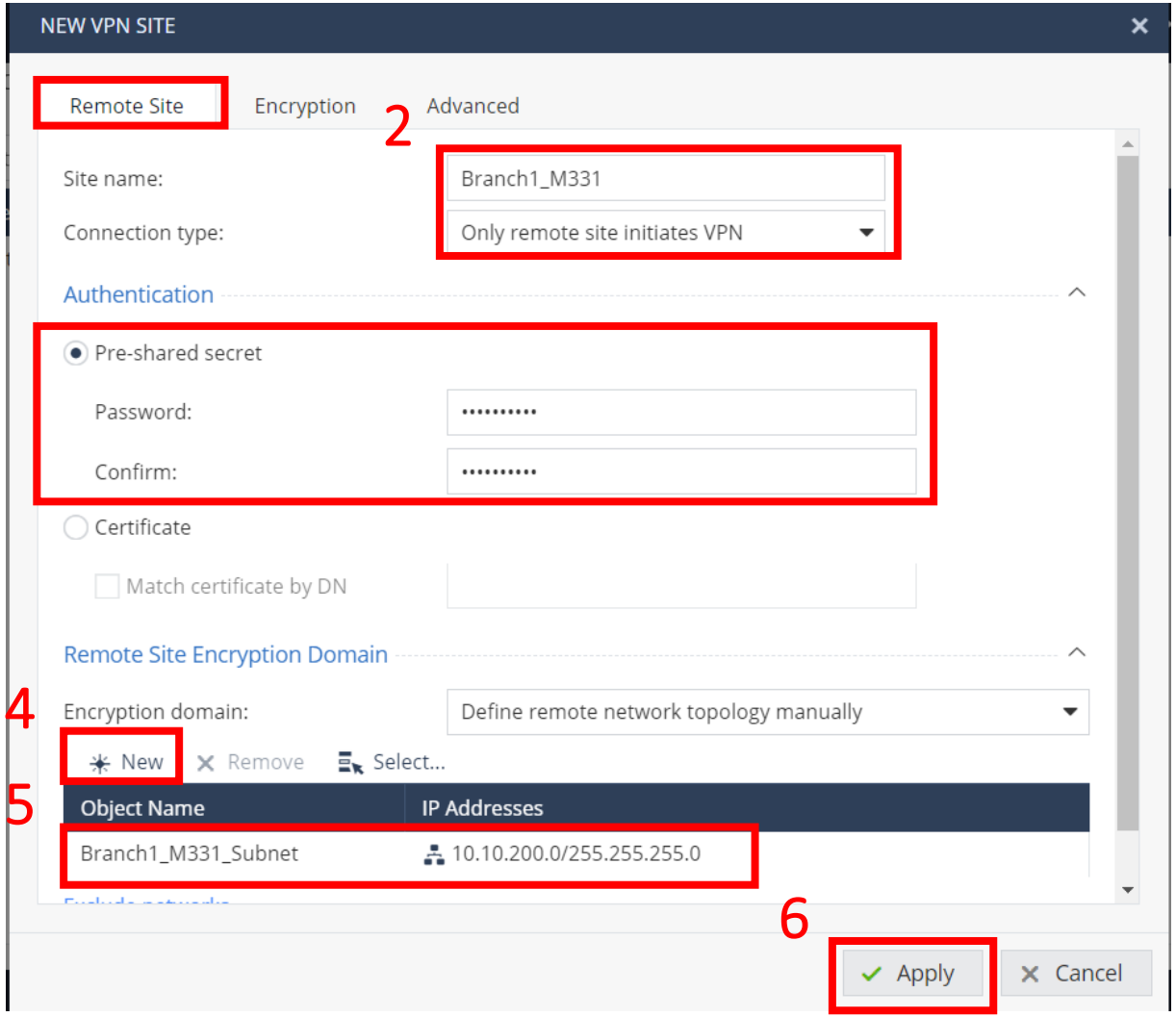
CheckPoint VPN設定 - 1



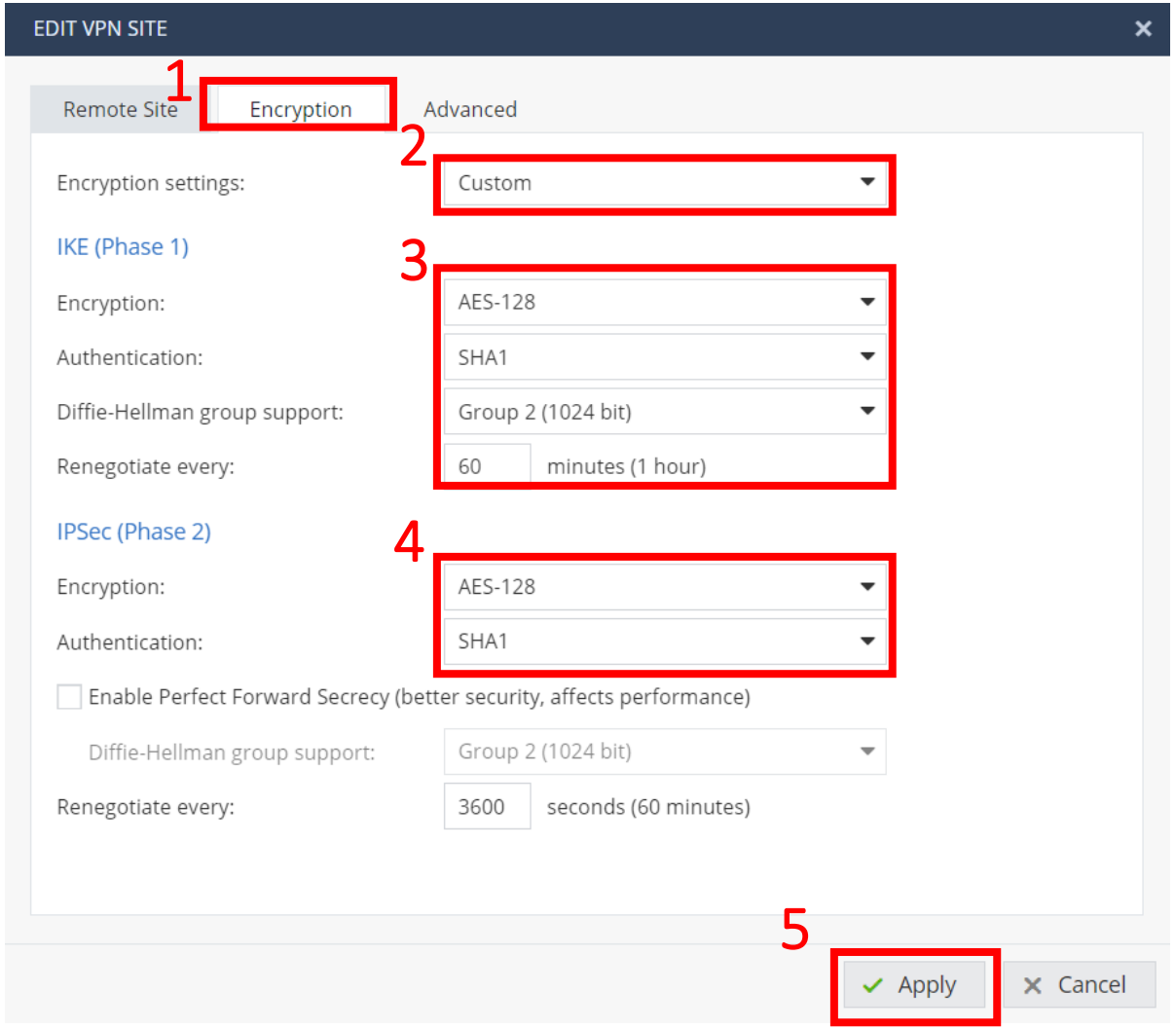
CheckPoint VPN設定 - 2



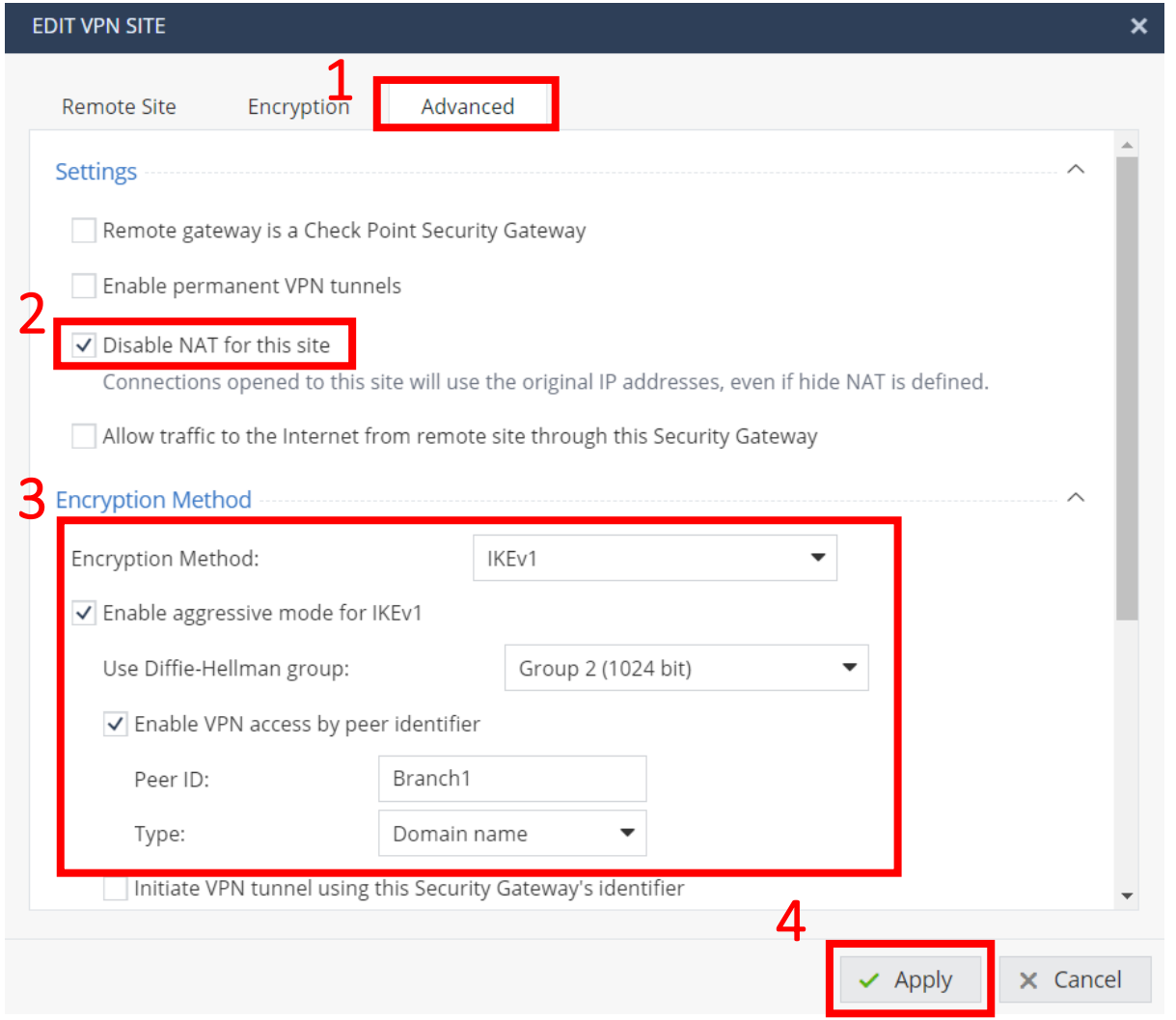
CheckPoint VPN設定 - 3



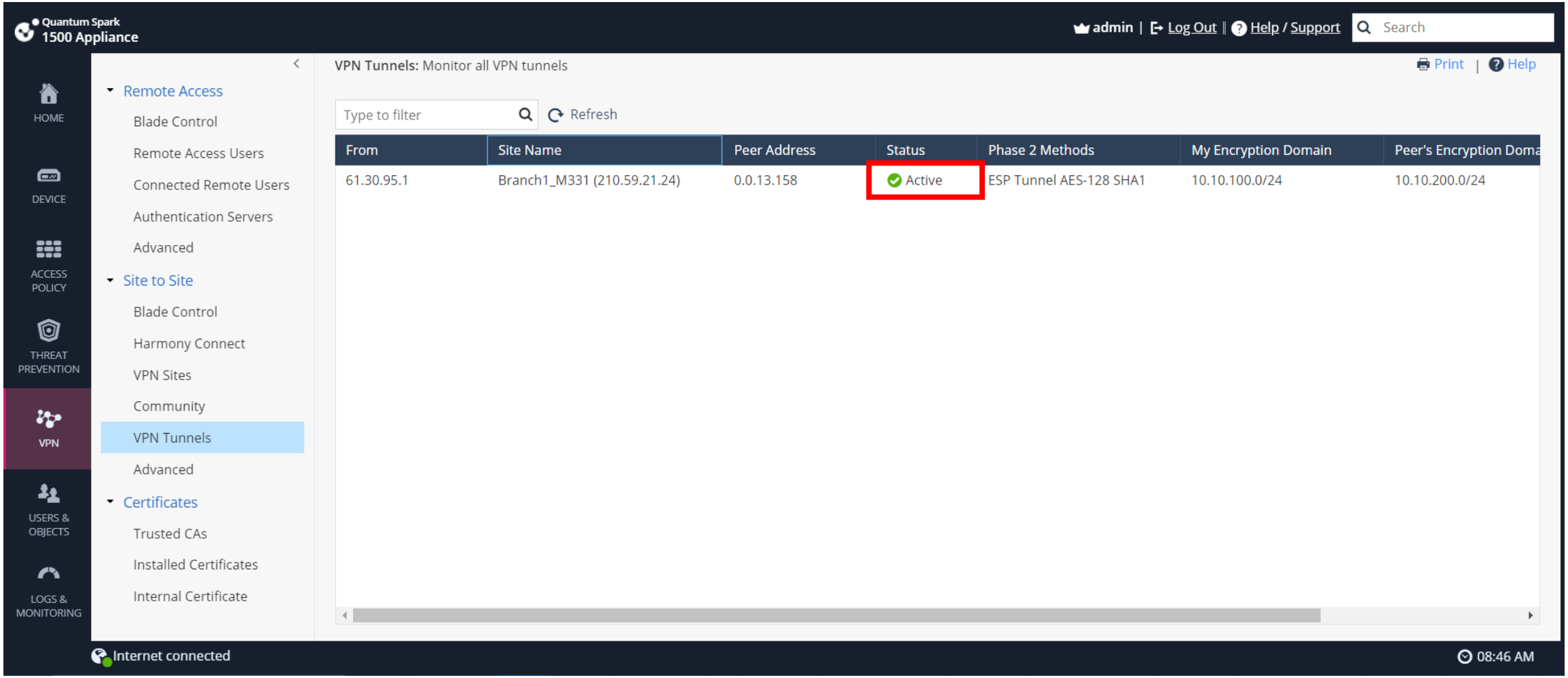
CheckPoint VPN設定 - 4



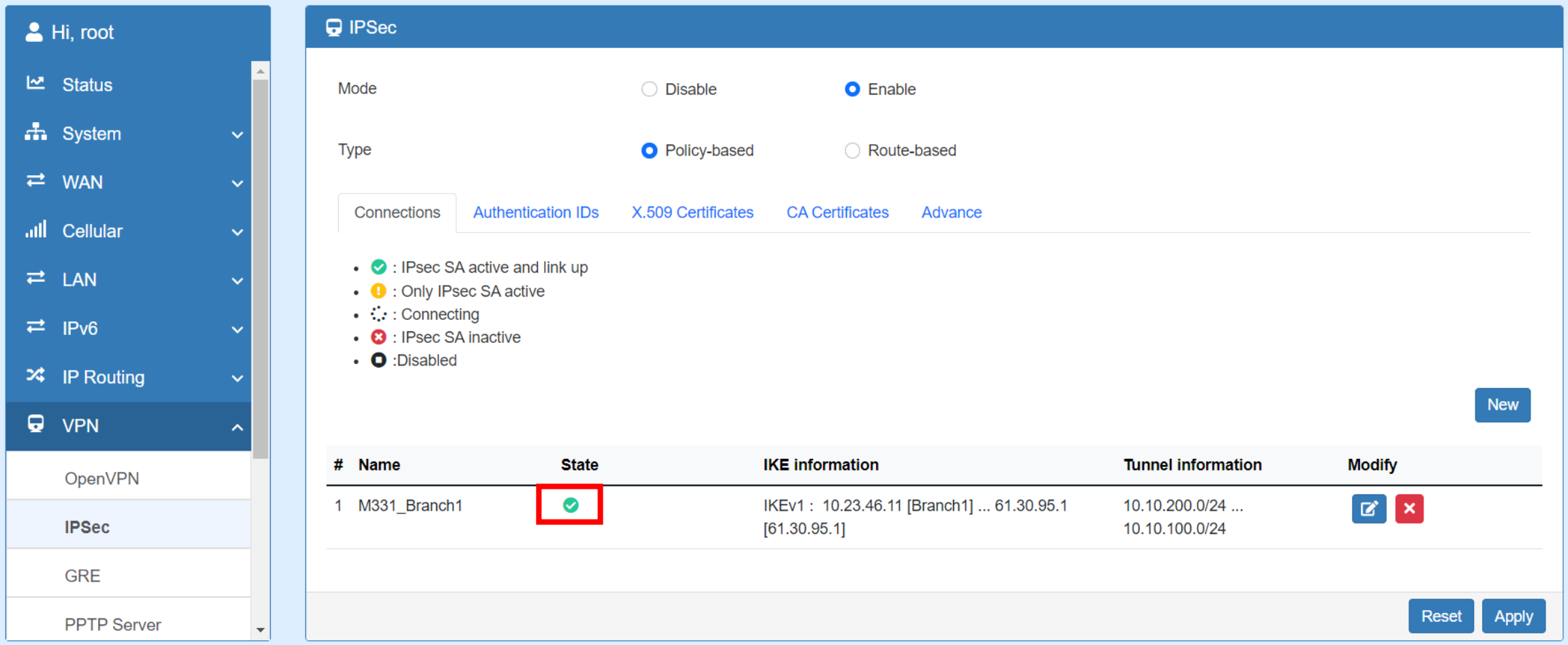
CheckPoint VPN設定 - 5



CheckPoint VPN狀態



M331 IPSec狀態



NB_B (M331端) Ping/tracert CheckPoint

```
乙太網路卡 乙太網路:

   連線特定 DNS 尾碼 . . . . . . . . :
   連結-本機 IPv6 位址 . . . . . . . . : fe80::70e3:e814:ecac:da8%23
   IPv4 位址 . . . . . . . . . . . . : 10.10.200.100
   子網路遮罩 . . . . . . . . . . . .: 255.255.255.0
   預設閘道 . . . . . . . . . . . . .: 10.10.200.1
```

```
C:\Users\Johnny>
C:\Users\Johnny>
C:\Users\Johnny>ping 10.10.100.100

Ping 10.10.100.100 (使用 32 位元組的資料):
回覆自 10.10.100.100: 位元組=32 時間=4ms TTL=253
回覆自 10.10.100.100: 位元組=32 時間=4ms TTL=253
回覆自 10.10.100.100: 位元組=32 時間=3ms TTL=253
回覆自 10.10.100.100: 位元組=32 時間=3ms TTL=253

10.10.100.100 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4, 已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 3ms，最大值 = 4ms，平均 = 3ms

C:\Users\Johnny>tracert -d 10.10.100.100

在上限 30 個躍點上追蹤 10.10.100.100 的路由

  1    <1 ms    <1 ms    <1 ms  10.10.200.1
  2     *        *        *     要求等候逾時。
  3     3 ms     2 ms     2 ms  10.10.100.100

追蹤完成。
```

Thank you

Enabling Infinite Future

PROSCEND