CHECK POINT™

QUANTUM SPARK 2500 系列 Quick Setup Guide

JLEAD 鉅立資訊

Check Point Quantum Spark 防火牆快速安裝手冊

為保障貴客戶權益，收到本設備之後，請於**收到設備 30 天內啟用**

免付費服務電話: 0809-081-866

保固期限 ： 該設備註冊之日起計二年

預設 IP 及 帳密
LAN IP Address : https://192.168.1.1:4434
User Name : admin (預設)
Password : (自行設定)

目　錄

第七章 系統備份設定

第八章 遠端管理防火牆設定

第一章 安裝及設定 Quantum Spark 防火牆

1. 認識 Check Point Quantum Spark 防火牆

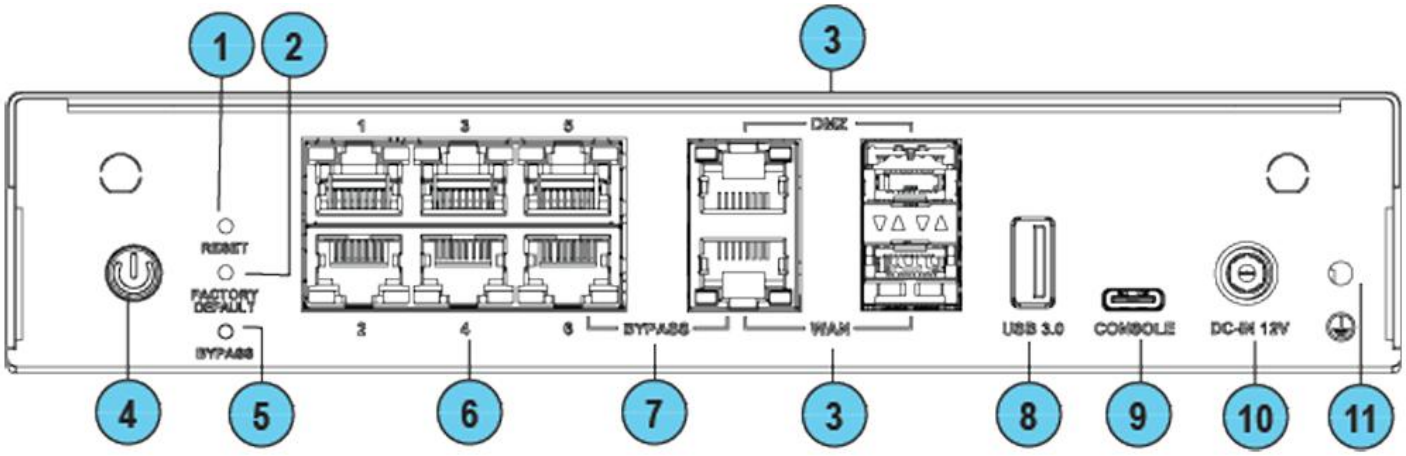
對於小規模辦公室或遠端且有許多分部的企業而言，持續維護網路安全相當困難，因為公司內只有少數人、甚至沒有人員具備 IT 專業。而中小型與遠端辦公室仍然需要與大企業主要辦公室相同級別的保護，以對抗複雜的網路攻擊和零時差威脅。Quantum Spark 2530 資安防護閘道是小型企業與遠端多分點辦公室的理想首選。它能提供簡易且直覺的網頁式本地管理介面，適用於小型辦公環境的本地管理與支援。若是必須由總部管理資安的多分點企業，則可運用內部或雲端託管進行遠端管理，並可為各分點辦公室數以千計的繁多裝置應用提供持續性的資安政策。

Check Point 2530 優勢

- 首年升級提供 SandBlast 多合一次世代威脅防護授權 (SNBT)：應用多層保護防堵複雜的網路威脅-應用程式控管、網頁過濾、IPS、殭屍網路防護、防毒、電子郵件安全與 SandBlast 零時差防護方案 (沙箱機制)。第二年起，提供 NGFW 授權：應用程式控管、IPS、SSL VPN、入侵偵測防禦。
- 共 8 個 1G 乙太網路連接埠：提供 6個 Internal Port、1 個 WAN port、1 個 DMZ Port。
- 可支援中控式管理(管理機需另購)和雲端式管理。

2. Quantum Spark 2530 產品外觀

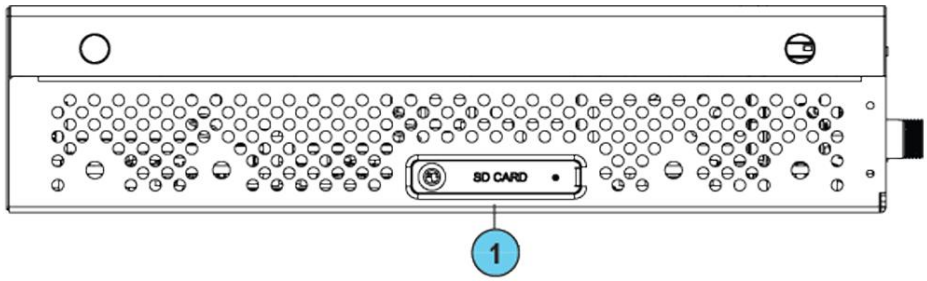
- **背面板**



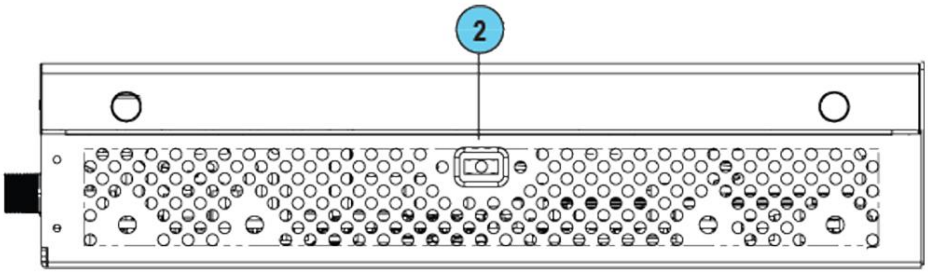
1. 重設-短按可重置系統，但不會移除任何使用者參數。
2. 出廠預設值-持續按住按鈕12秒，即可將硬體設備還原其出廠預設值。
3. WAN和DMZ連接埠SFP外殼1GbE-SFPWAN連接埠1、SFPDMZ連接埠1
4. 電源按鈕按下即可關閉或開啟設備。
5. 略過按下即可將設備開啟或關閉BYPASS模式(僅限有線)
6. LAN、WAN和DMZ連接埠 RJ451GbE-LAN連接埠1-6、WAN連接埠1、DMZ連接埠1
7. BYPASS(僅限有線旁路型號)-當軟體或硬體發生故障時，DMZ連接埠與LAN-6連接埠之間會啟動旁路機制。當旁路機制啟動時，流量會處於不安全狀態。
8. USB連接埠3.0 (Type-A)- USB連接埠3.0用於軟體下載。
9. 主控台在此接上USB(Type-C)序列主控台纜線。
10. 12VDC輸入 連接至電源基礎設施的電源線。
11. 接地螺絲-保護接地端子

- **側面面板**

第 1 面



第 2 面



1. SD卡插槽。- 在此插入micro-SD卡。
2. 防盜插槽。 - 將防盜纜線插入此處。 使用Kensington和 SunboxTL-623M纜線作為參考

- **燈號說明**

管理LED		■ **關閉**：沒有管理 ■ 顏色：請見下方
網際網路LED		■ **關**：沒有網際網路連線 ■ **閃爍藍色**：正在嘗試連線至網際網路。 ■ **藍色**：已連線 ■ **閃爍紅色**：連線失敗
´電源LED(狀態)		■ **穩定藍色**：正常操作 ■ **閃爍藍色**：開機進行中以及安裝韌體。在程序完成之後，LED會穩定亮起藍燈。 ■ **紅色**：錯誤/警示 **注意**：當硬體設備第一次開啟時，此LED會是紅色。

· **管理 LED**

管理 LED 會顯示重試機制的狀態：

動作	管理LED活動
Zero Touch正在執行中。	閃爍紅色(緩慢)
已成功連線至Zero Touch雲端伺服器並且儲存部署指令碼。	閃爍紅色(快速)
Zero Touch程序已完成。SMP啟用不需要。	LED關閉
啟用睡眠時間。	閃爍藍色(緩慢)
重新啟用。	閃爍藍色(快速)
SMP已連線。	穩定藍色。
SMP模式已關閉。	LED關閉
閘道無法連線至SMP，將會從重試指令碼退出。	持續紅色。

· **網際網路 LED (網路孔)**

網路 LED (RJ45 WAN 和 LAN 連接埠)。

每個連接埠會使用雙色 LED 以反映連結/活動與速度(從 10M 到 1GbE)。

無連結　　：　LED1(綠色)關閉、LED2(琥珀色)關閉

1G 連結　　：　LED1(綠色)開啟、LED2(琥珀色)關閉

1G 活動　　：　LED1(綠色)閃爍、LED2(琥珀色)開啟

100M 連結 ：　LED1(綠色)開啟、LED2(琥珀色)關閉

100M 活動 ：　LED1(綠色)閃爍、LED2(琥珀色)關閉

10M 連結　：　LED1(綠色)開啟、LED2(琥珀色)關閉

10M 活動　：　LED1(綠色)閃爍、LED2(琥珀色)關閉

3. 安裝 Quantum Spark 2530 設備

[請注意] 請避免將 Check Point-2530 的 Internal Port 連接到現有網路上，Checkpoint-2530 預設 DHCP Server 服務，如接到現有網路上會造成網路異常。

1. 使用 RJ45 網路線，串接於 WAN 網路埠。

2. 另一端接於數據機或是上一層對外網路的網路設備，貴客戶若只有一個寬頻線路，建議使用 Check Point-2530 的 WAN Port。

3. 請使用內附的電源變壓器 (12V / 3.0A) 連接至Check Point-2530 電源接孔，另一端連接至電源插座。

4. 使用 RJ-45 網路線，將電腦或筆記型電腦連接於 Internal Port網路埠任一埠上。

5. 請觀察前方面版燈號。POWER 燈號恆亮藍燈時，即表示完成開機。

4. 所需環境介紹

在進行設定之前，請貴客戶先閱讀以下注意事項：

1. 請確認網際網路連線是否正常運作：建議先以電腦直接連接 ISP 提供之寬頻設備，測試並確認電腦能正常的連接到網際網路。

2. 建議貴客戶使用 Windows 10/11 作業系統 及 Edge/Firefox/Chrome 瀏覽器來設定 Check Point Quantum Spark 2530。

3. 建議使用瀏覽器，以圖形介面進行安裝設定，在開始設定之前建議貴客戶先將瀏覽器升級至最新的版本，並確認 Java 正確的安裝。

4. Check Point-2530 透過區域連線埠（Internal Port）即可進行設定。電腦或設備需做相關區域網路 TCP/IP 設定即可 (詳細請參考 4.1. 電腦端設定)。

4-1. 電腦端設定

請依貴客戶使用的作業系統，選擇相對應的章節參考設定。

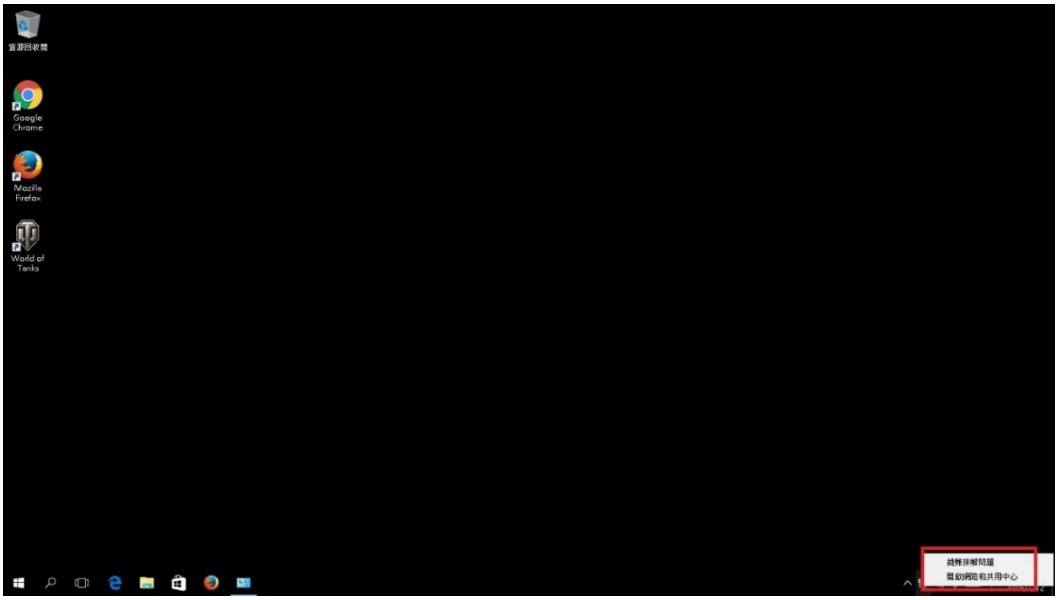
4-1-1. Windows 10

設定目的：確認你的電腦區域網路設定為 DHCP Client，可以自動從 Check Point-2530 DHCP Server 獲得正確 IP。

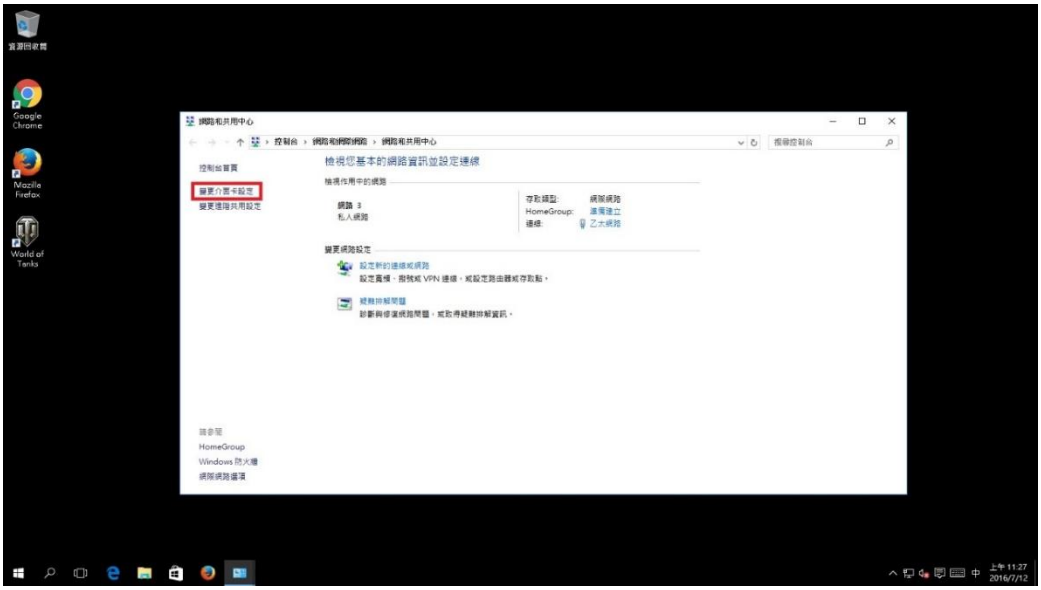
步驟一：確定電腦的網路埠正確連接到 CheckPoint-2530 的 WAN 網路埠

步驟二：請確定 CheckPoint-2530 的燈號顯示正常(POWER 恆亮)，CheckPoint-2530 預設為 DHCP Server 會配發 192.168.1.1~192.168.1.254 的 IP 給電腦

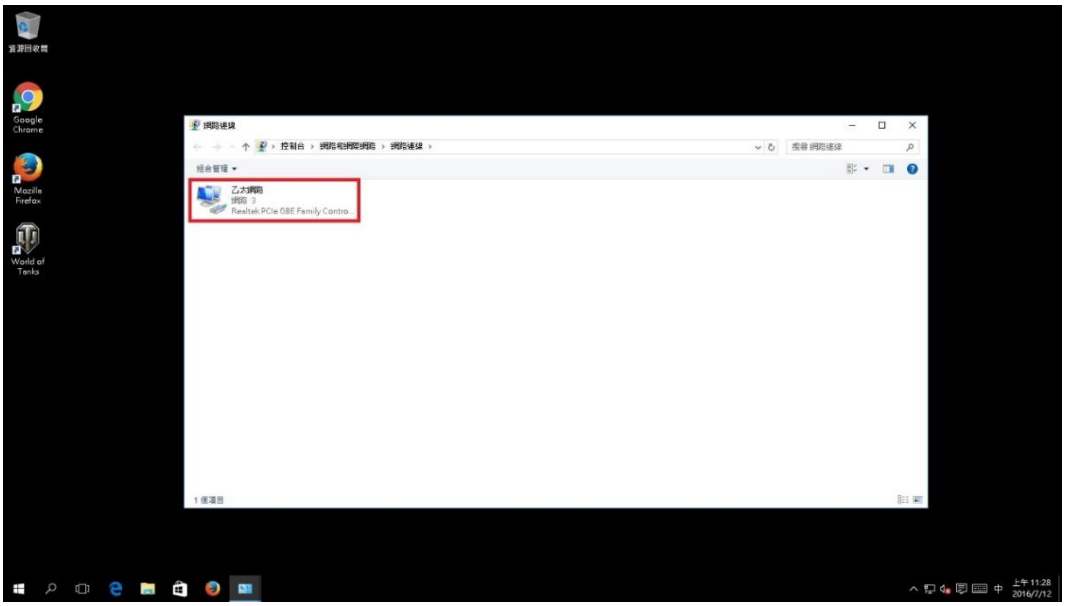
步驟三：請到貴客戶的電腦端



步驟四：請點選畫面右下角"網路連線圖形 按右鍵 選取 "開啟網路和共用中心"

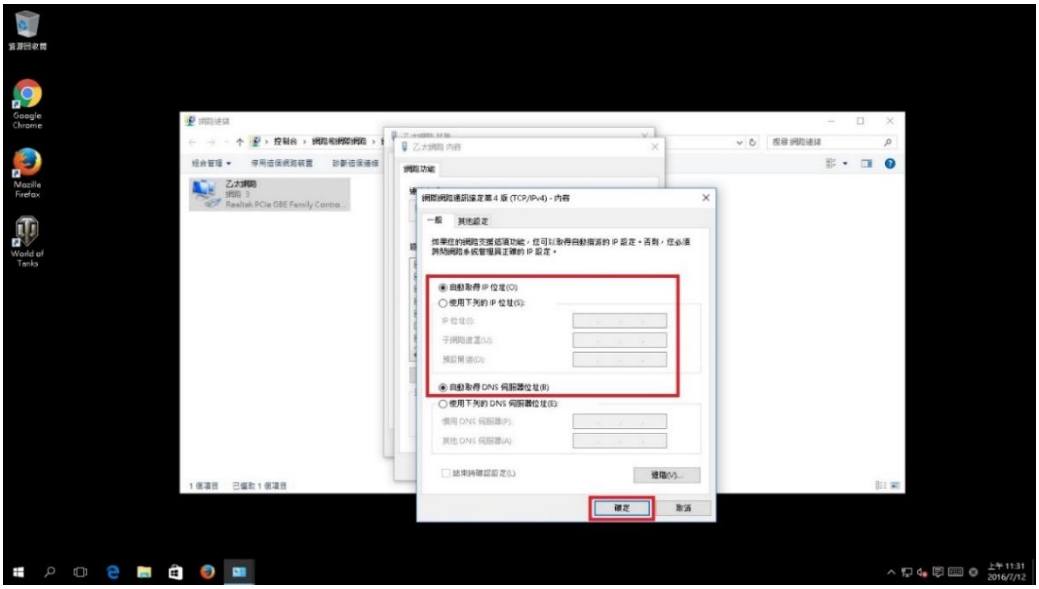


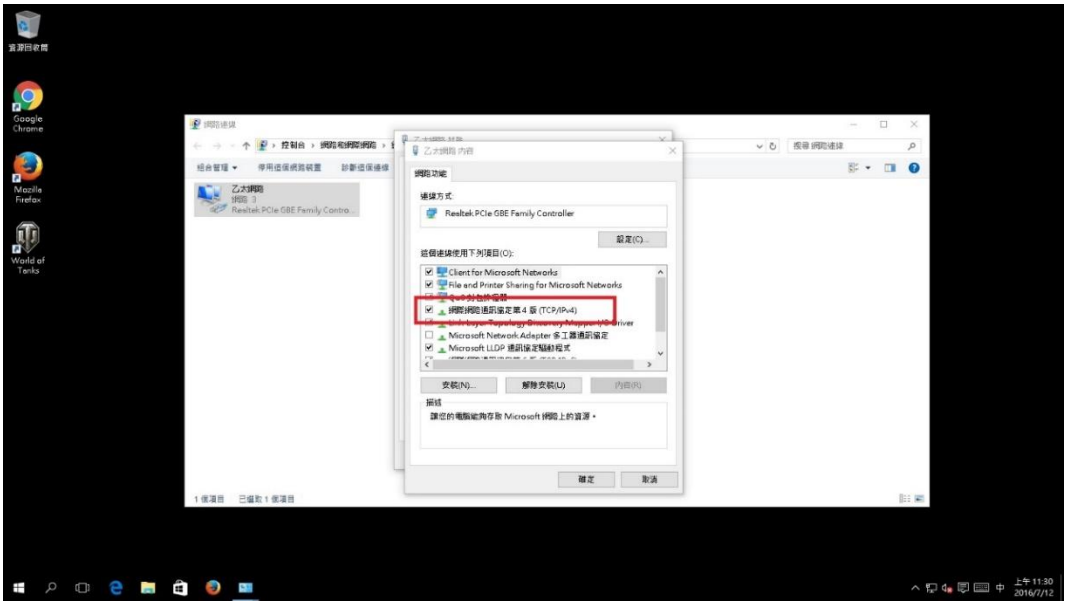
步驟五：請點選 "變更介面卡設定"



步驟六：點選 "乙太網路"

步驟七：在乙太網路內容視窗，選擇 "網際網路通訊協定第 4 版(TCP/IPv4)"





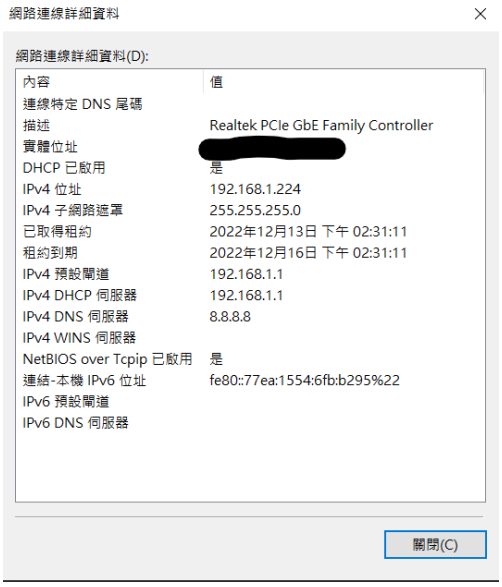
步驟八：請選擇 "自動取得 IP 位址(O)" →請選擇 "自動取得 DNS 伺服器位址(B)"

然後點選 "確定"

步驟九：請點選 "關閉"

步驟十：請在區域連線上點選滑鼠右鍵 → 請點選 "狀態"

步驟十一：請點選 "詳細資料"



步驟十二：請檢查 IP Address 是否為 192.168.1.X(最後一碼依 DHCP Server 配發 "192.168.1.1~192.168.1.254" 有所不同， 如 192.168.1.2)，Subnet Mask 則為 255.255.255.0，Default Gateway 應為 192.168.1.1，如果無誤請直接關閉此視窗，若不正確請將電腦重新開機後再確認一次。

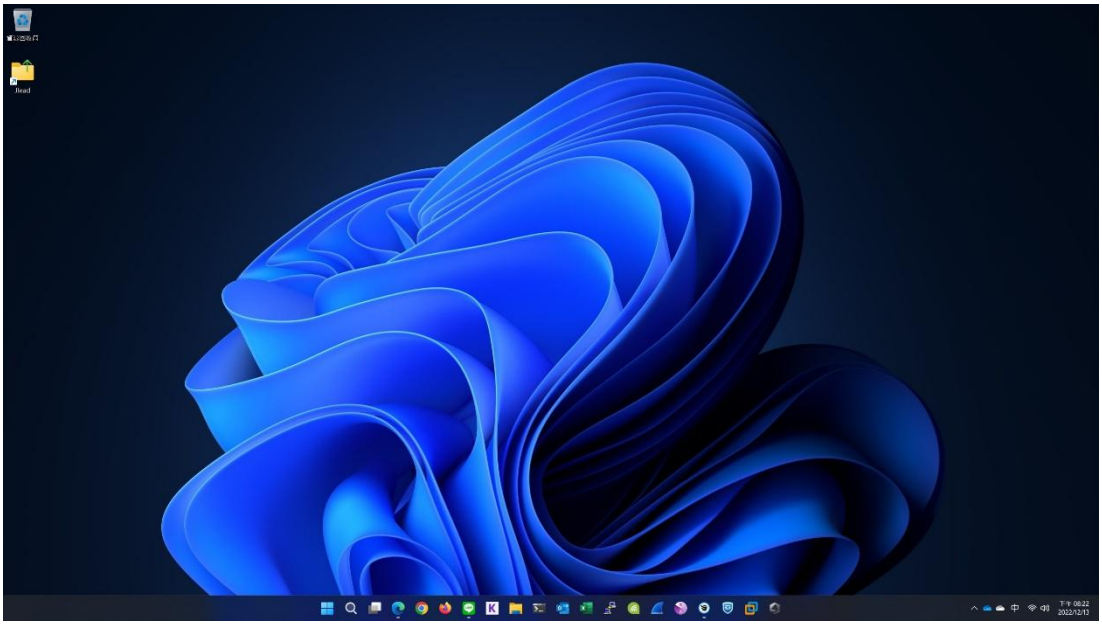
1. Windows 11

設定目的：確認你的電腦區域網路設定為 DHCP Client，可以自動從 Check Point-2530 DHCP Server 獲得正確 IP。

步驟一：確定電腦的網路埠正確連接到 CheckPoint-2530 的 WAN 網路埠

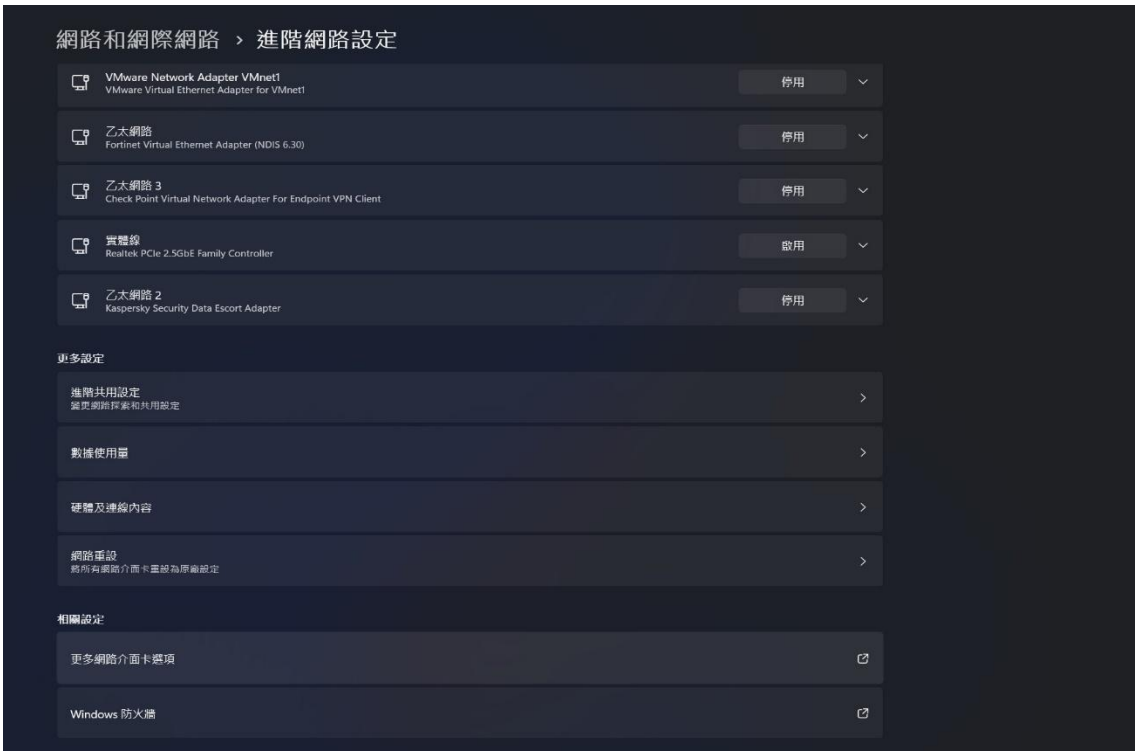
步驟二：請確定 CheckPoint-2530 的燈號顯示正常(POWER 恆亮)，CheckPoint-2530 預設為 DHCP Server 會配發 192.168.1.1~192.168.1.254 的 IP 給電腦

步驟三：請到貴客戶的電腦端



步驟四：請點選鍵盤按鈕 win+I，會顯示下圖

步驟五：請點選進階網路設定



步驟六：請點選更多網路介面卡選項

步驟七：點選 "乙太網路"

步驟八：在乙太網路內容視窗，選擇 "網際網路通訊協定第 4 版(TCP/IPv4)

步驟九：請選擇 "自動取得 IP 位址(O)" →請選擇 "自動取得 DNS 伺服器位址(B)"

然後點選 "確定"

步驟十：請點選 "關閉"

步驟十一：請在區域連線上點選滑鼠右鍵 → 請點選 "狀態"

步驟十二：請點選 "詳細資料"

步驟十三：請檢查 IP Address 是否為 192.168.1.X(最後一碼依 DHCP Server 配發 "192.168.1.1~192.168.1.254" 有所不同)，Subnet Mask 則為 255.255.255.0，Default Gateway 應為 192.168.1.1，如果無誤請直接關閉此視窗，若不正確請將電腦重新開機後再確認一次。

※ 正確地完成以上的動作後，請依 4-2 章節設定瀏覽器。

ii. 瀏覽器設定

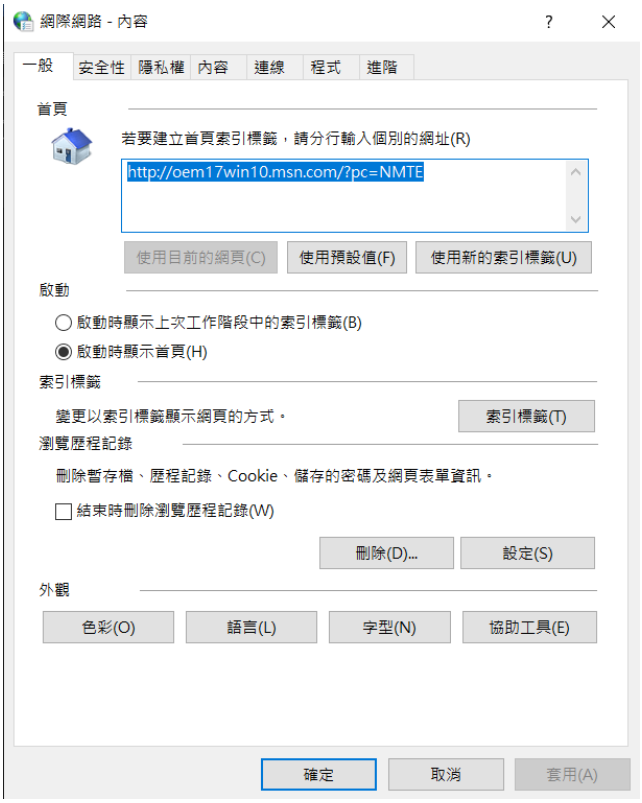
在設定本產品之前，必須先設定 Web 瀏覽器，本說明書以 Edge , FireFox 以及 Chrome 為範例，請依貴客戶的需求選擇相對應的章節進行設定

1. Edge

設定目的：確認你的電腦瀏覽器設定正確，不會自動撥號連線，也沒有設定 Proxy 伺服器。

步驟一：鍵盤輸入 Windows 標誌鍵 + I → 點選 "網路和網際網路" →點選 "網路和共用中心" →點選 "網際網路選項"會出現以下畫面

(此時若還不能上網，如果跳出 ADSL 撥號連線視窗請將其關閉)



步驟二：

點選 "區域網路設定" 會出現 "區域網路(LAN)設定" 的視窗

都不要勾選→確定後請點選 "確定"，→ 再點選一次 "確定" 完成設定

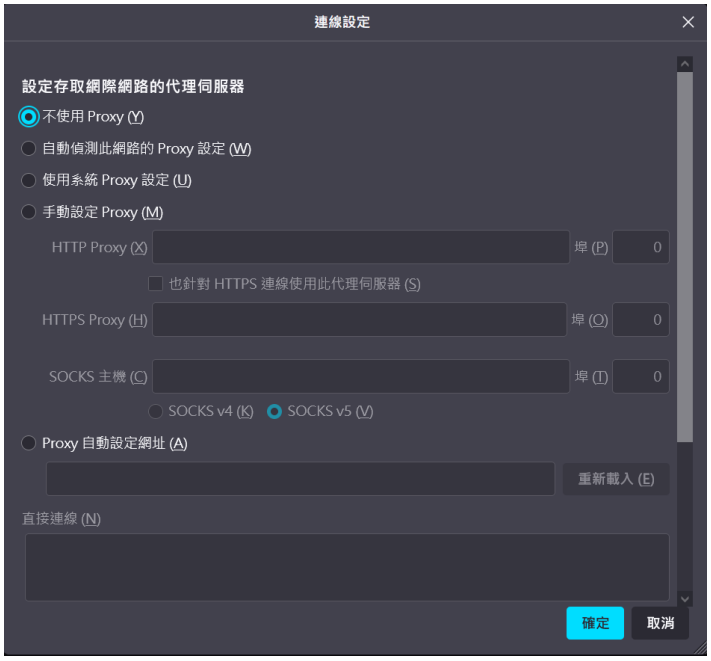
※正確地完成以上的動作後，表示貴客戶已經可以透過貴客戶的電腦來連接到 CheckPoint-2530，接下來請跳至 1.5.1 進入預設 Web 設定畫面。

2. FireFox

設定目的：確認你的電腦瀏覽器設定正確，沒有設定 Proxy 伺服器。

步驟一：開啟 "FireFox 瀏覽器" → 點選 "設定" →在一般頁面下拉網路設定，點選 "設定"會出現下圖

(此時若還不能上網，如果跳出 ADSL 撥號連線視窗請將其關閉)



請選取 "不使用 Proxy (Y) " ，按 "確定" 完成設定。

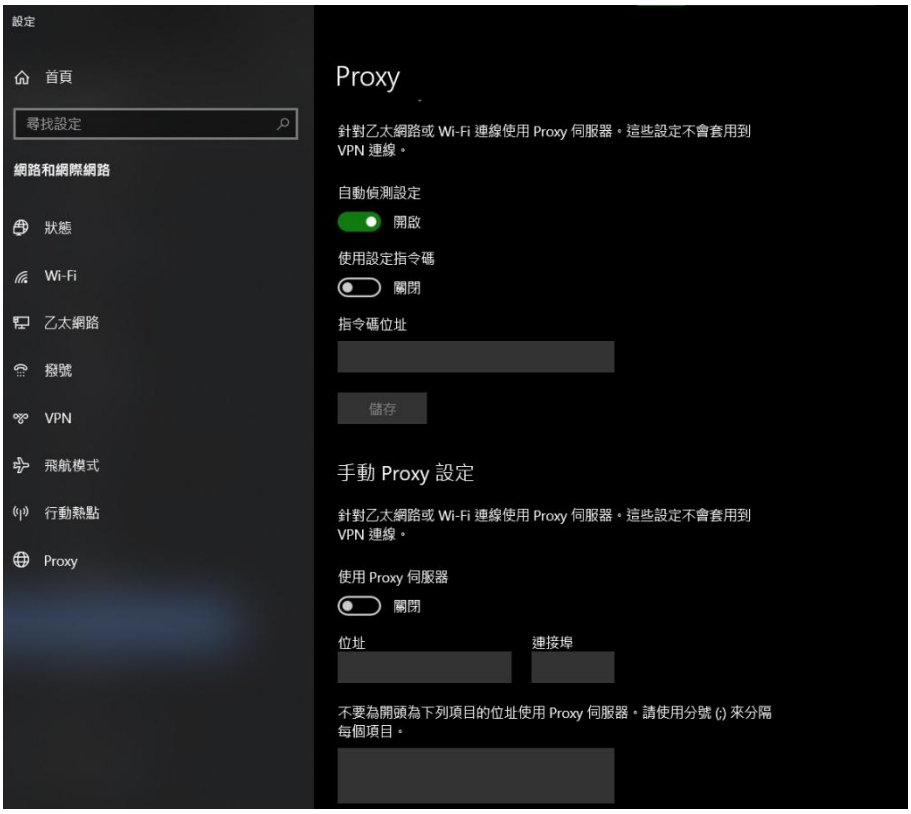
※正確地完成以上的動作後，表示貴客戶已經可以透過貴客戶的電腦來連接到 CheckPoint-2530，接下來請跳至 1.5.1 進入預設 Web 設定畫面。

3. Google Chrome

設定目的：確認你的電腦瀏覽器設定正確，沒有設定 Proxy 伺服器。

步驟一：開啟 "Chrome 瀏覽器" → 點選右上角 "設定"→ 點選左側 "系統" 會出現下圖：

步驟二：再選取 "開啟電腦的 Proxy 設定"



關閉 Proxy 伺服器設定，→"儲存" 完成設定

※正確地完成以上的動作後，表示貴客戶已經可以透過貴客戶的電腦來連接到 CheckPoint-2530，接下來請跳至 1.5.1 進入預設 Web 設定畫面。

第二章 開始設定 Quantum Spark 防火牆

1. 進入預設 Web 啟動「首次設定精靈」

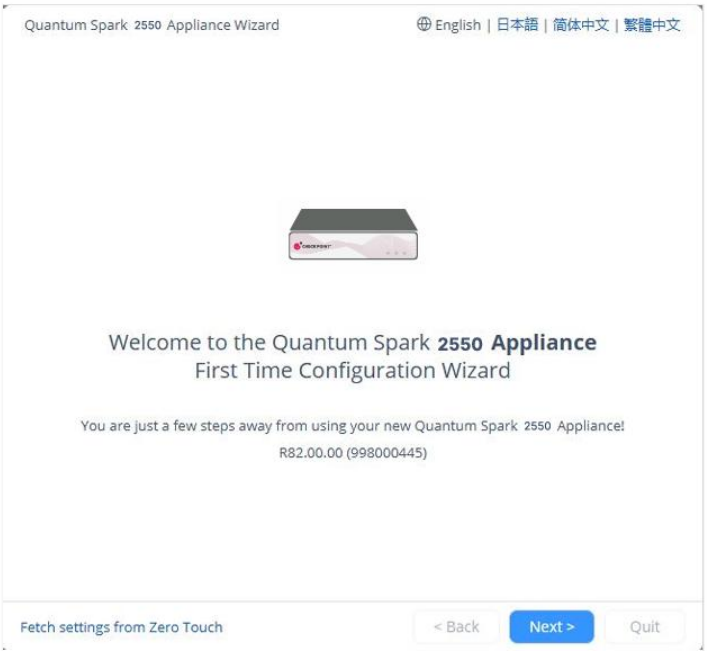
設定前請先確認已完成 第一章 第 3 節. 安裝 Quantum Spark 2530 設備，第 4 節. 所需環境介紹。

開啟貴客戶的網頁瀏覽器 → 請在網址輸入"https://192.168.1.1:4434"

edge 會出現以下的畫面，" 選取進階，繼續前往 192.168.1.1"

透過精靈設定 CheckPoint-2530

步驟一：初次設定會直接進入以下的畫面(預設語言為英文) ，若要變更 WebUI 應用程式的語言，選取頁面頂端的語言連結(英文/日文/繁體中文)。



步驟二: 設定密碼，輸入管理者的帳號與密碼

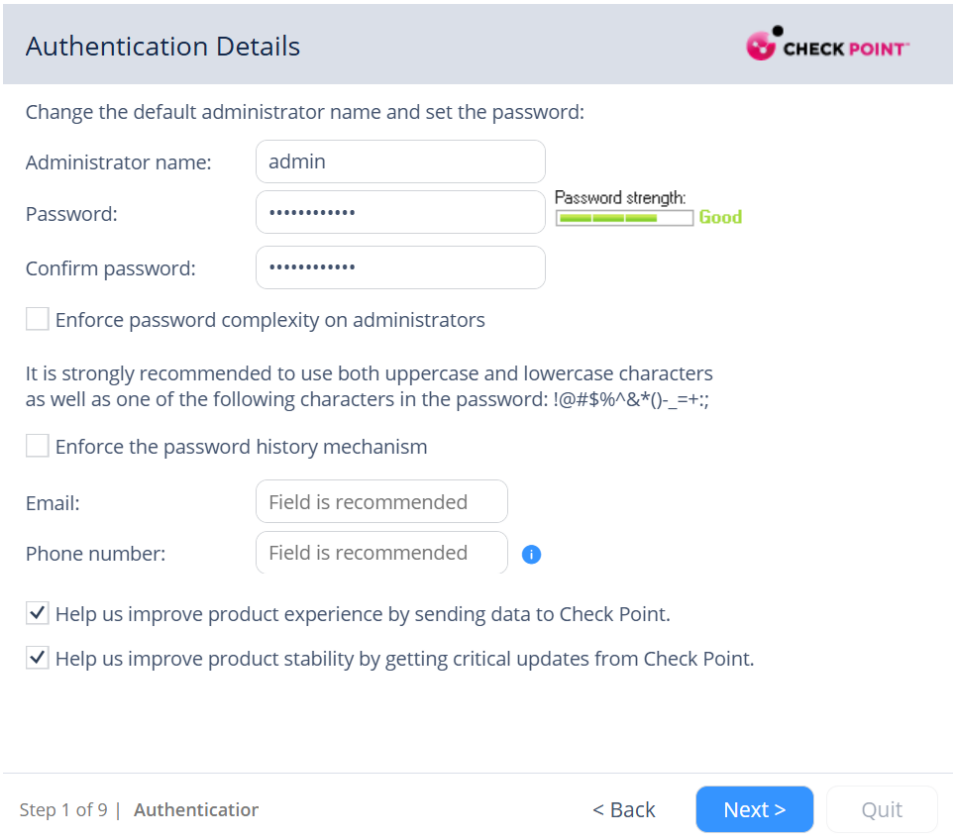
■ 驗證詳細資料

在驗證詳細資料頁面中，輸入登入硬體設備 WebUI 所需的詳細資料：

管理員名稱：我們建議您變更預設的管理員登入名稱「admin」。名稱有區分大小寫。

密碼：強式密碼至少會有 6 個字元，其中包括至少一個大寫字母、一個小寫字母以及一個特殊字元。

使用密碼強度表來衡量您的密碼強度。



注意：強度表只是一個指標，並不會強制建立具有指定數量的字元或字元組合的密碼。若要實施密碼複雜性，請按一下核取方塊。

步驟三: 設定時間與時區

■ 硬體設備日期與時間設定

在硬體設備日期與時間設定頁面，手動設定硬體設備的日期、時間以及時區設定，或是使用「網路時間通訊協定」選項。

如果您選擇選項手動設定時間，硬體設備會使用電腦中的日期與時間作為初始值。如果需要，請變更時區設定以顯示您的正確位置。根據預設，會自動啟用日光節約時間。您可以在 WebUI 應用程式中的裝置>日期與時間頁面變更此時間。

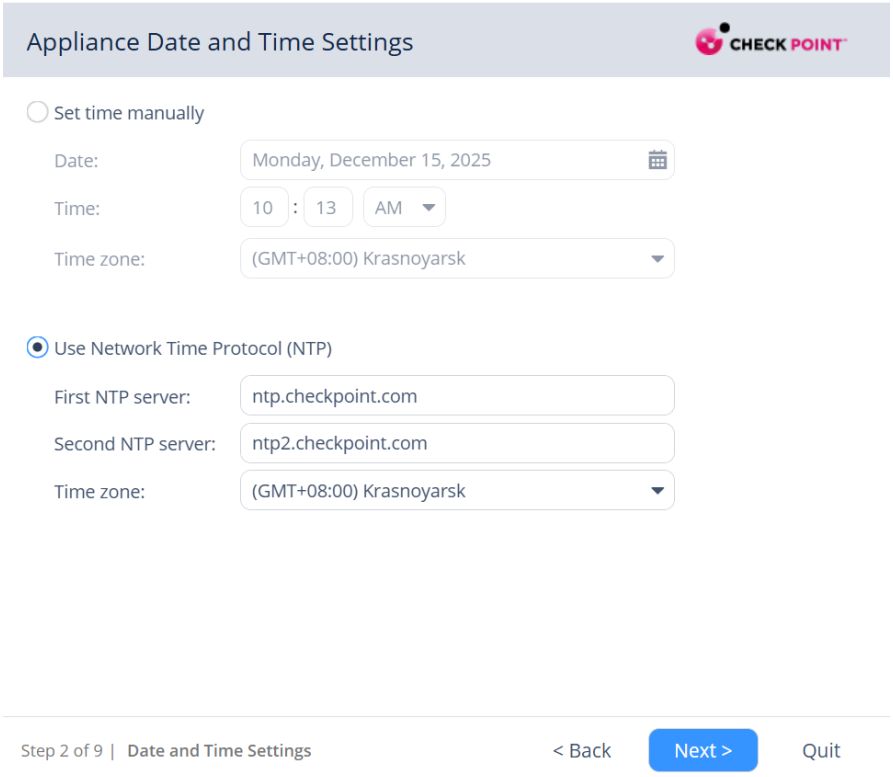
日期：根據預設，日期會在電腦上顯示。如果需要，請設定不同的日期。

時間：根據預設，時間會在電腦上顯示。如果需要，請設定不同的時間。

時區：根據預設，時區會在電腦上顯示。如果需要，請選擇時區設定以反映您準確的所在位置。

主要 NTP 伺服器：主要 NTP 伺服器的 IP 或主機名稱。預設伺服器為 ntp.checkpoint.com

次要 NTP 伺服器：次要 NTP 伺服器的 IP 或主機名稱。預設伺服器為 ntp2.checkpoint.com



步驟四: 設定設備名稱與網域名稱

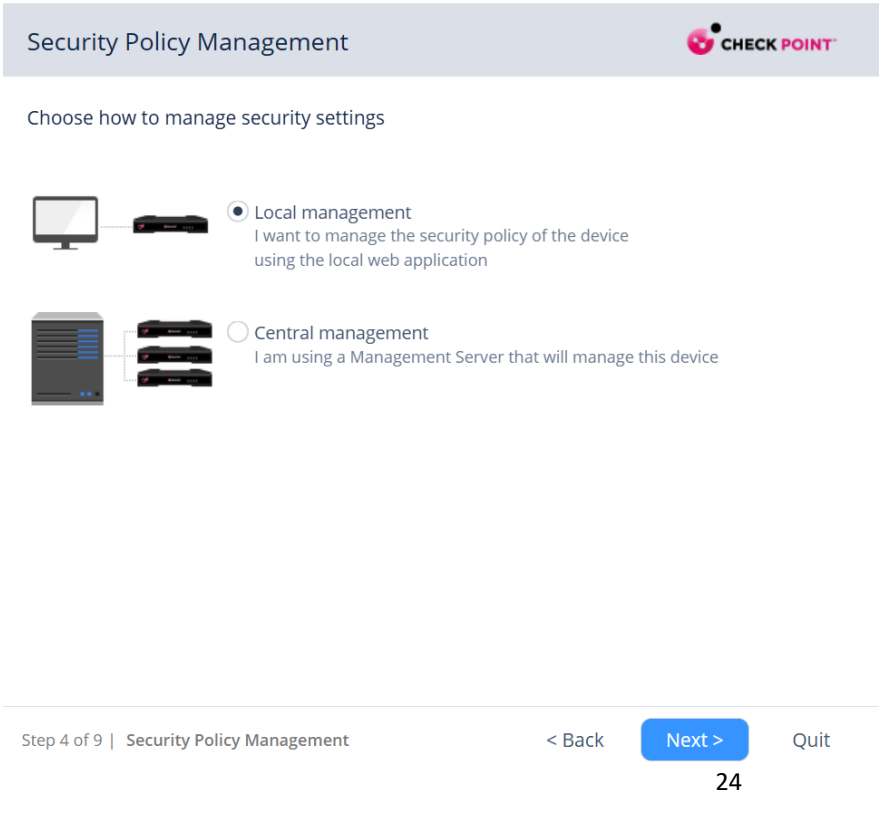
■ 硬體設備名稱

在硬體設備名稱頁面中輸入名稱以識別硬體設備，然後輸入網域名稱(可以不必輸入)。

當閘道為指定的物件名稱執行 DNS 解析時，網域名稱會附加至物件名稱。如此可以讓網路中的主機按其內部名稱查詢主機。

步驟五: 設定管理模式 單點管理/中心端管理

■ 安全性原則管理



中央管理(Central)：遠端的「安全管理伺服器」可使用網路物件以及安全性原則管理 SmartConsole 中的安全閘道。

本機管理(Local)：硬體設備使用網路應用程式來管理安全性原則。在您使用「首次設定精靈」配置硬體設備之後，將會自動實施預設安全性原則。藉由硬體設備 WebUI 的協助，可以配置您啟動的「軟體刀鋒」並且微調安全性原則。

本「入門指南」描述如何配置本機的部署。

步驟六: 設定網際網路

■ 網際網路連線

在網際網路連線頁面中，設定您的網際網路連線細節，或是選擇稍後設定網際網路連線。

若要立即設定網際網路連線：

1. 選擇立即設定網際網路連線。
2. 從連線類型下拉式清單中，選擇用於連線至網際網路的協定。
3. 輸入選取連線協定的欄位。您針對每個協定輸入的資訊必須各有不同。您可以透過網際網路服務提供者(ISP)取得。

- 靜態IP：固定(非動態)的IP位址。
- DHCP：動態主機設定通訊協定(Dynamic Host Configuration Protocol, DHCP)會自動將指定範圍內的IP位址發給網路上的裝置。這是在您透過網路數據機連接時常見的選項。
- PPPoE(乙太網路上的PPP)：用於封裝乙太網路框架內的點對點通訊協定(PPP)框架的網路通訊協定。主要會與DSL服務搭配使用，在此服務中，個別使用者會透過乙太網路和都會乙太網路連接至DSL數據機。輸入ISP登入使用者名稱與ISP登入密碼。注意：在「首次設定精靈」中僅支援動態IP。
- PPTP：點對點通道通訊協定(PPTP)實施虛擬私人網路。PPTP在TCP以及GRE通道作業中使用控制通道以封裝PPP封包。
- L2TP：第二層通道通訊協定(L2TP)是用於支援虛擬私人網路(VPN)的通道通訊協定。此通訊協定並未提供任何加密或保密。它依賴的是加密通訊協定，此協定會在通道內部傳輸以提供隱私。
- 橋接器：連接資料連結層(第二層)的多個網路區段。
- DNS伺服器(靜態IP與橋接器連接)：在相關欄位中輸入DNS伺服器位址資訊。對於DHCP、

PPPoE、PPTP、L2TP、行動網絡以及，DNS 設定是由您的服務提供者所提供。您可以稍後在 WebUI 應用程式的裝置> DNS 底下中覆寫這些設定。

我們建議您將 DNS 設定為硬體設備需要，以便針對不同功能執行 DNS 解析。舉例來說，在授權啟用期間或是當應用程式控制、網站篩選、防毒軟體或是防垃圾郵件服務啟用時連線至 Check Point 使用者中心。

*請依照網路類型參照 5-2-1. 設定外部連線 (單條寬頻網路)

若要測試您的 ISP 連線狀態：按一下連線。

硬體設備會連接至您的 ISP。成功或失敗會顯示在頁面底部。

步驟七: 設定區域網路

■ 區域網路

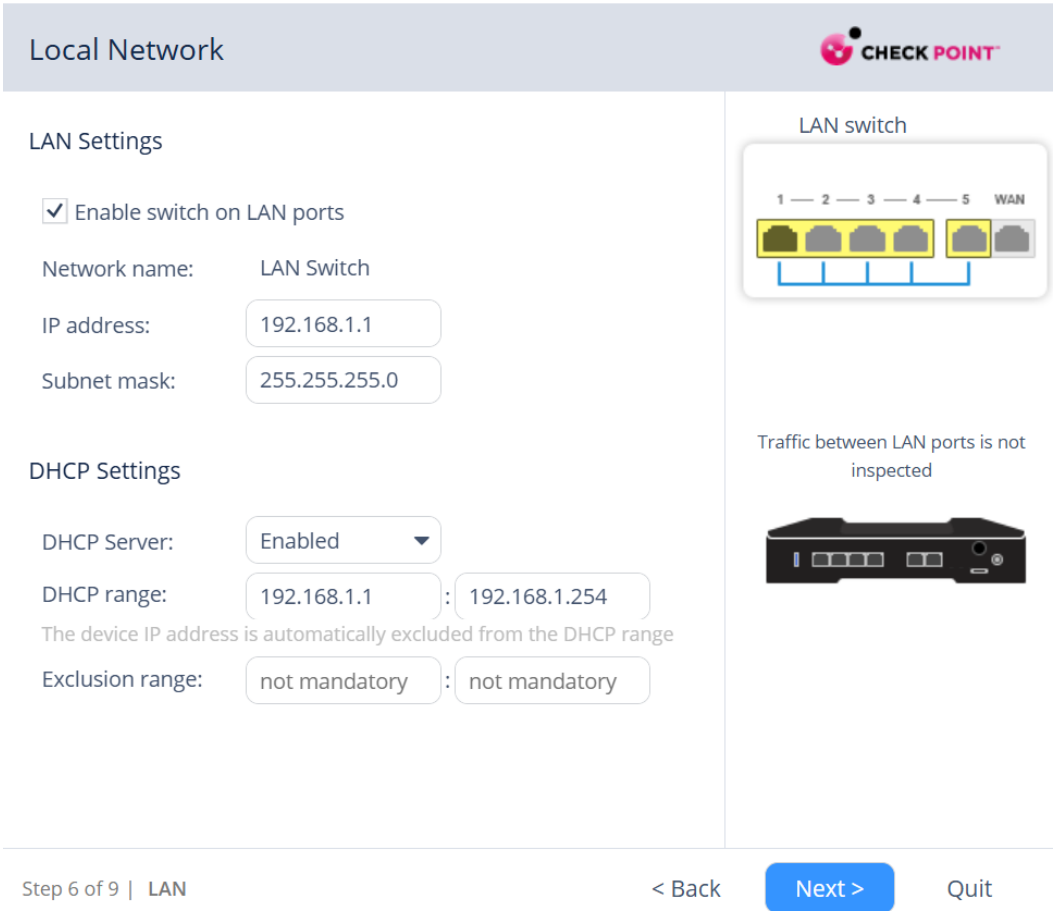
在區域網路頁面中，選擇啟用或是停用 LAN 連接埠的開關，並且配置您的網路設定。根據預設，它們為啟用狀態。在硬體設備的原始 IP 保存為別名 IP 時，您可以變更 IP 位址並且保持連線，直到您初次將硬體設備開機為止。

相關資訊

- 啟用LAN連接埠的開關：彙總所有LAN連接埠作為開關，同時此開關會有一個IP位址。如果已停用此選項(已清除核取方塊)，則會將區域網路定義為僅LAN1。
- 網路名稱：輸入網路名稱。
- IP位址：您可以修改IP位址並且維持連接性。硬體設備的原始IP保存為別名IP以維持連接性，直到精靈完成為止。
- 子網路遮罩：輸入子網路遮罩。
- DHCP伺服器與範圍欄位：根據預設，DHCP為啟用狀態，並且有預設的網路範圍。請務必設定適當範圍，不要在網路中包括預先定義的靜態IP。

- 排除範圍：設定DHCP伺服器未定義的IP位址的排除範圍。定義在網路中指定IP位址時DHCP會排除的IP位址範圍。硬體設備的IP位址會自動從範圍排除。舉例來說，如果硬體設備IP為1.1.1.1，則範圍也會從1.1.1.1開始，但是其自身的IP位址例外。

重要事項：如果您選擇停用 Enable Switch on LAN ports，請確定您的網路線已連接 LAN1 連線埠。否則，在您按一下下一步時將會遺失連線。



步驟八: 設定存取範圍

■ 管理員存取

在管理員存取頁面中，設定管理員是否可以從指定的 IP 位址或任何 IP 位址使用硬體設備。

若要設定管理員存取權限：

1. 選擇可允許管理員存取的來源位置：
   - LAN：所有內部實體連接埠。
   - 受信任的無線：已知的無線網路。
   - VPN：從遠端網站透過VPN通道使用加密流量或是使用遠端存取客戶。
   - 網際網路：清除網際網路的流量(不建議)。
2. 選擇 IP 位址，管理員可以透過此 IP 位址存取硬體設備：
   - 任何IP位址。
   - 僅指定的IP位址：選取此選項能夠讓管理員透過指定的IP位址或網路存取硬體設備。按一下新增以設定IP位址資訊。
   - 網際網路中的指定IP位址以及其他來源的任何IP位址：選擇此選項可允許管理員僅可從網際網路中的特定IP位址存取，或是從任何IP位址

的其他選取來源存取。此選項為預設值。

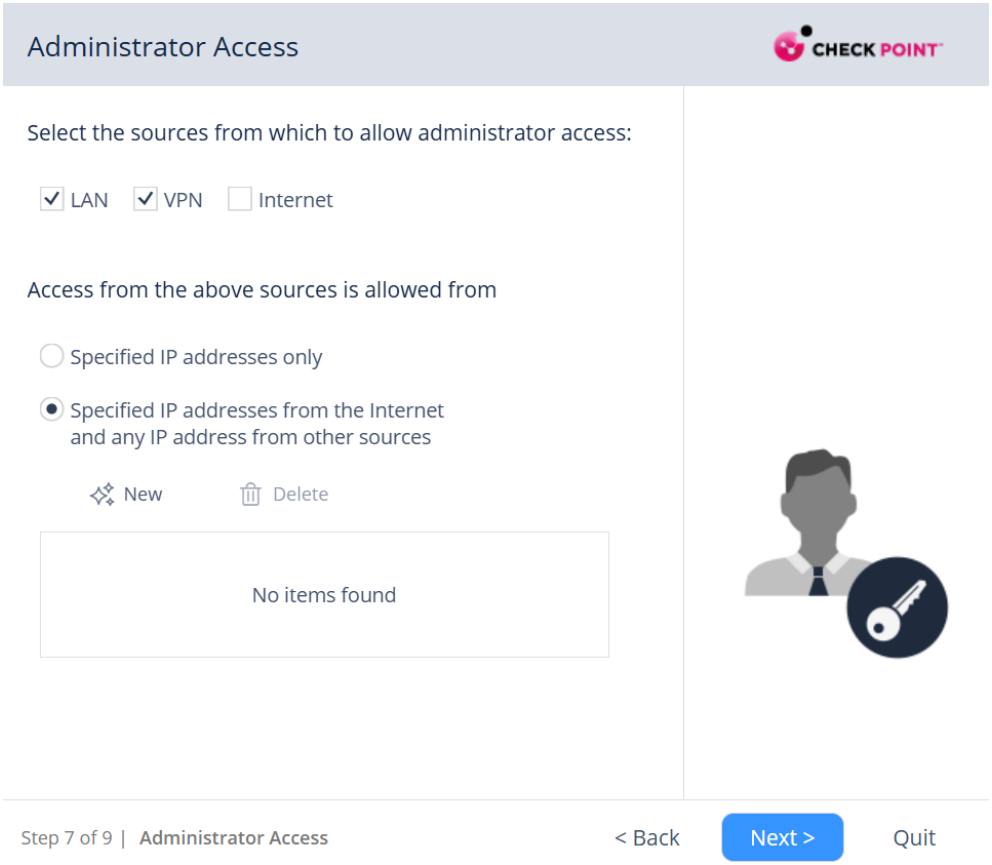
若要指定 IP 位址：

1. 按一下新增。

2. 在 IP 位址設定視窗中，選擇一個選項：

- 特定IP位址：輸入IP位址或是按一下從我的電腦取得IP。
- 特定網路：輸入網路IP位址以及子網路遮罩。

3. 按一下套用。



步驟九: 設定硬體設備註冊

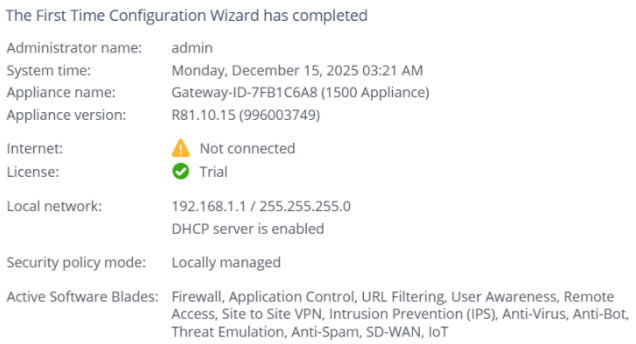
■ 硬體設備註冊

硬體設備可以連接至 Check Point 使用者中心，利用其憑證可以取得授權資訊並且啟動硬體設備。

如果您已經設定網際網路連線：按一下啟用授權。您會被告知已經成功啟動硬體設備，並且會看見每個「軟體刀鋒」的授權狀態。

步驟十: 檢視摘要

■ 摘要



摘要頁面顯示使用「首次設定精靈」設定元素的詳細資料。按一下 Finish，以完成「首次設定精靈」。

將電腦網卡 IP 修改為跟防火牆同一網段後，在瀏覽器輸入新設定的 IP，登入網頁確認，狀態設置完成

4. 設定外部連線 (單條寬頻網路)

甲、 固定制 IP 客戶

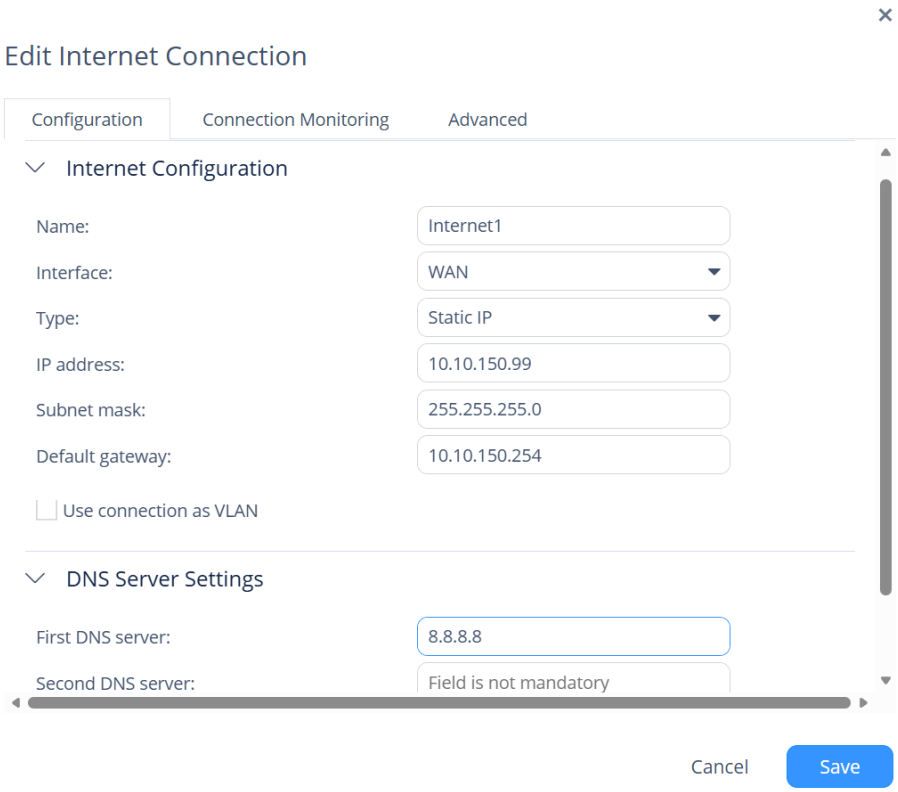
請下拉 "connection type"，選取 Static IP 後，輸入寬頻網路業者提供 IP 位址資料以及預設閘道器 IP 位址資料

IP 網址/網路遮罩：10.10.150.99/255.255.255.0，

Default gateway 10.10.150.254(此為範例，請貴客戶依寬頻網路業者提供資料鍵入)

以及 DNS 資料 8.8.8.8

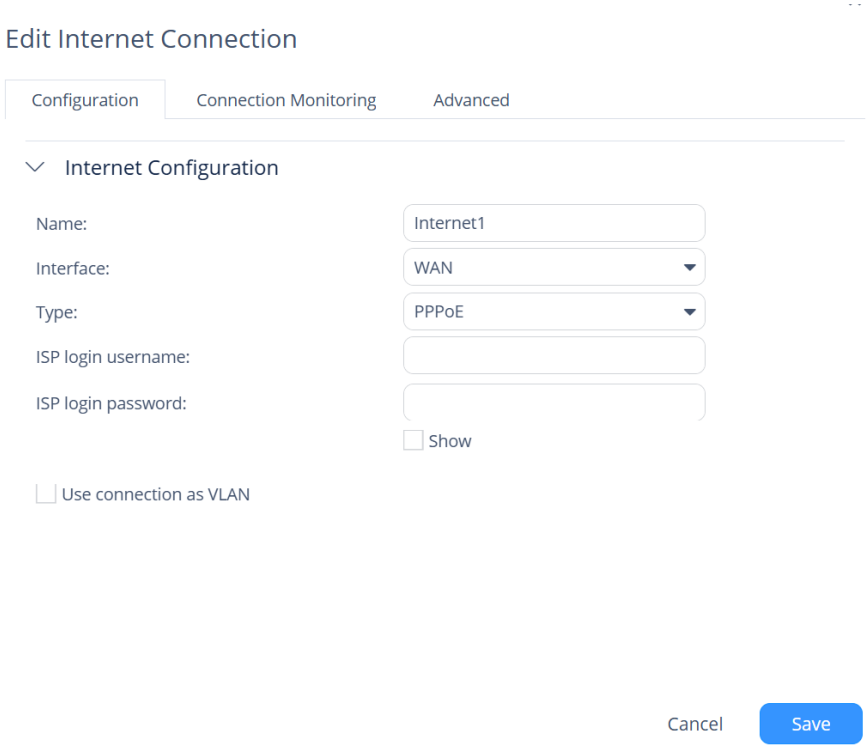
完成後按 "Apply" 完成設定



乙、 非固定制 IP 客戶 (PPPoE)

如客戶對外網路是 PPPOE 模式，則在 Connection type 選取，

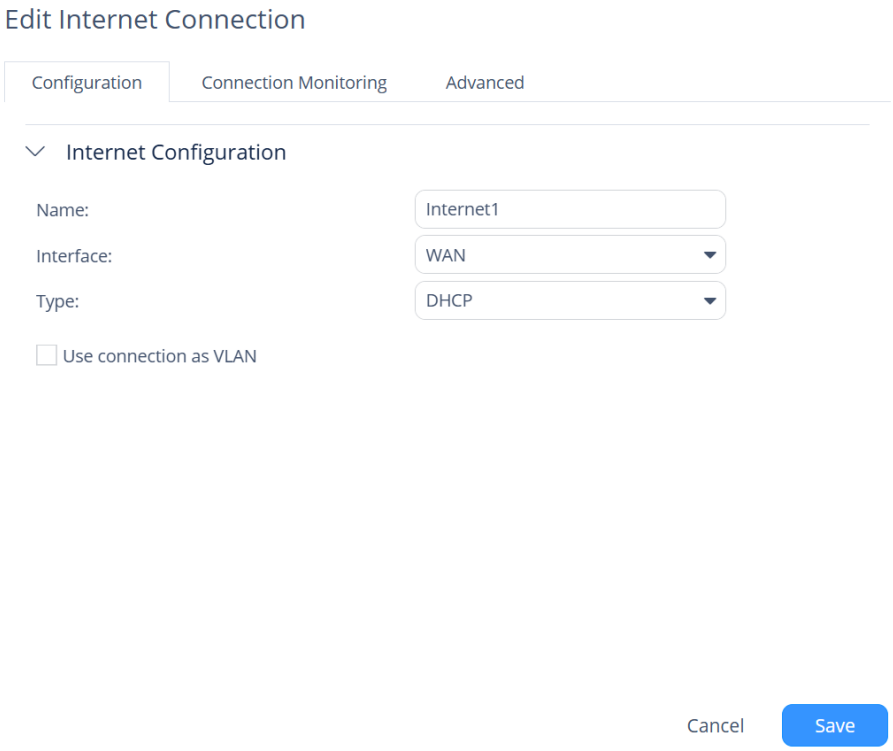
如 DHCP 正常則在左下角顯示綠色勾勾以及獲得 IP 位址，如獲取失敗請連繫 ISP 網路業者



丙、 DHCP 制客戶

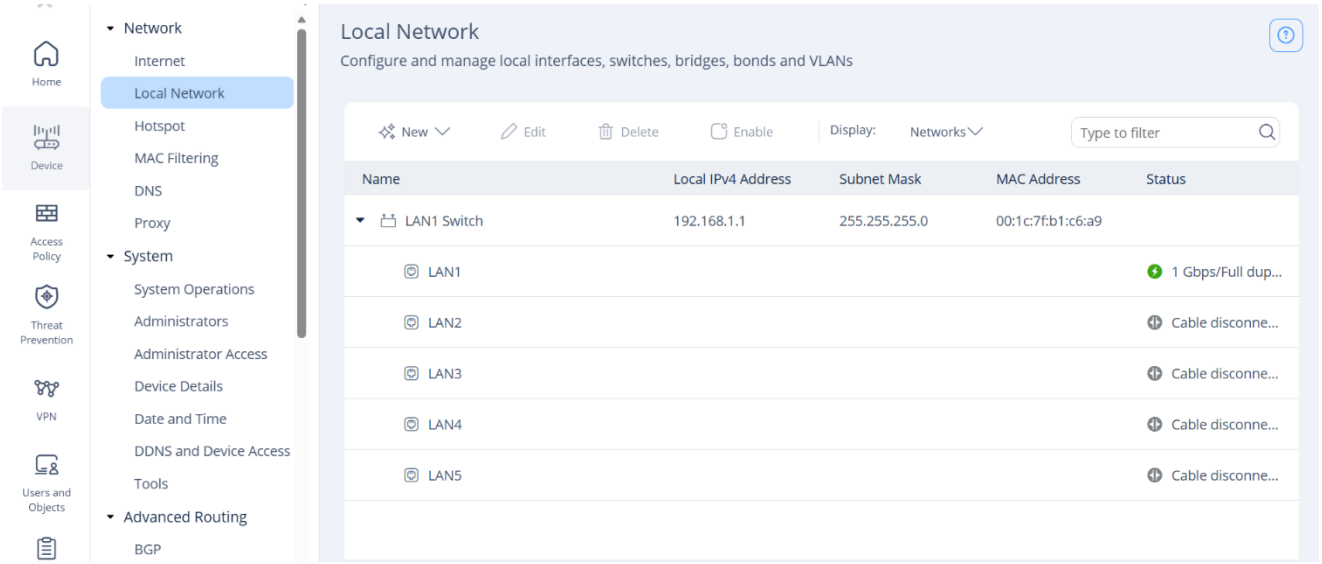
如客戶對外網路是 DHCP 模式，則在 Connection type 選取 DHCP，

如 DHCP 正常則在左下角顯示綠色勾勾以及獲得 IP 位址，如獲取失敗請連繫 ISP 網路業者



2. 設定內部網路組態

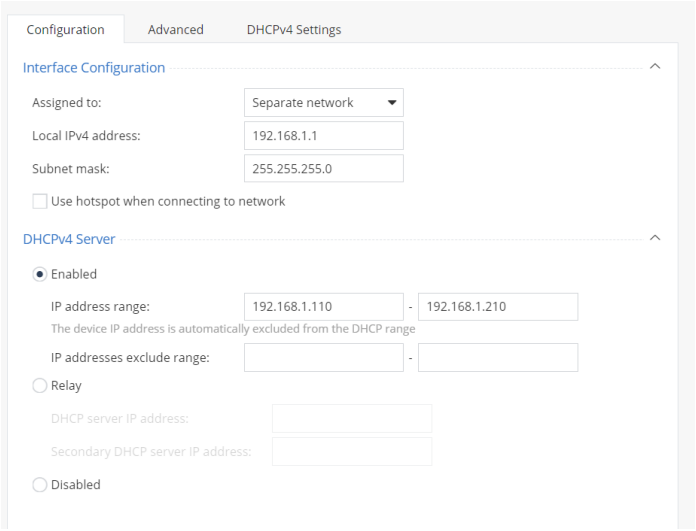
貴客戶請登入 CheckPoint2530，點選 "DEVICE" -> "Local Network" ->選取 LAN1 按 "Edit"，進入下一步驟



在位址模式下，更改所需的 IP 位址及網路遮罩（例如： 192.168.1.99/255.255.255.0）

請注意：請務必更改 DHCP 派發 IP 範圍，點選 DHCP Server 位址範圍，修改為：

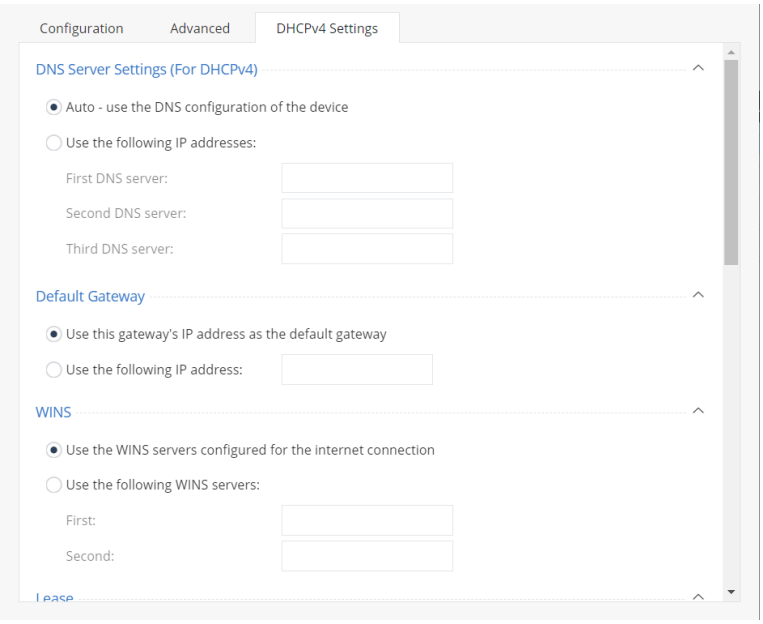
IP : 192.168.1.110-192.168.1.210 (此為範例，請貴客戶依實際狀況更改)



選取 DHCPv4 setting 頁面，確定點選 Auto-Use the DNS configuration of the device

完成後，點選 "確定"，設定完成

請注意：此時連線會中斷 ， 請更改電腦 IP 位址為 固定 IP 後（例如：192.168.1.99）再連線到 CheckPoint2530 系統（例如：https://192.168.1.254)

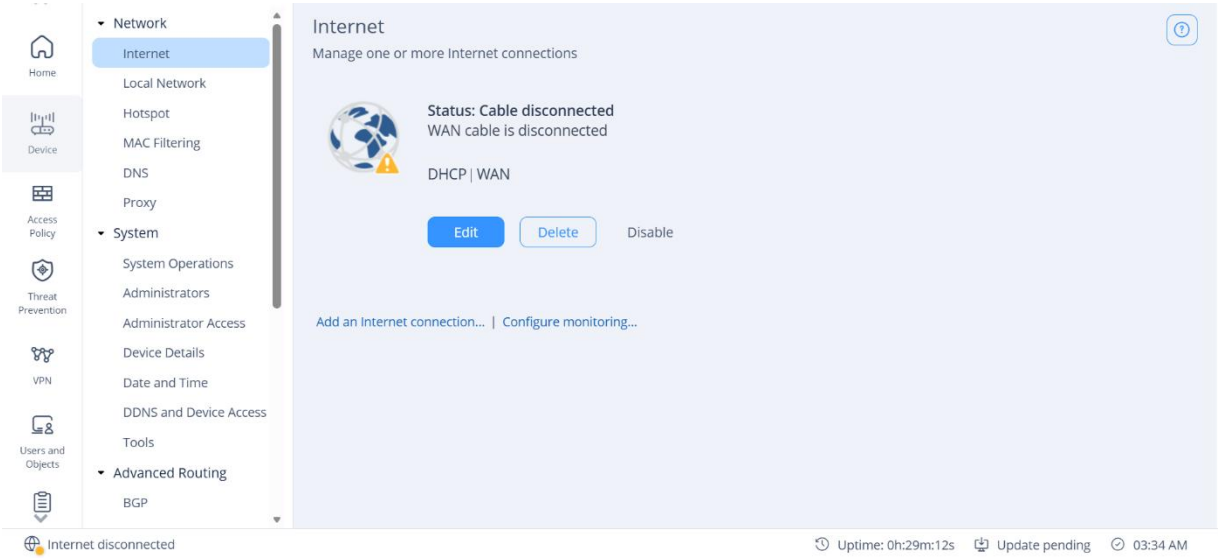


3.設定外部網路組態

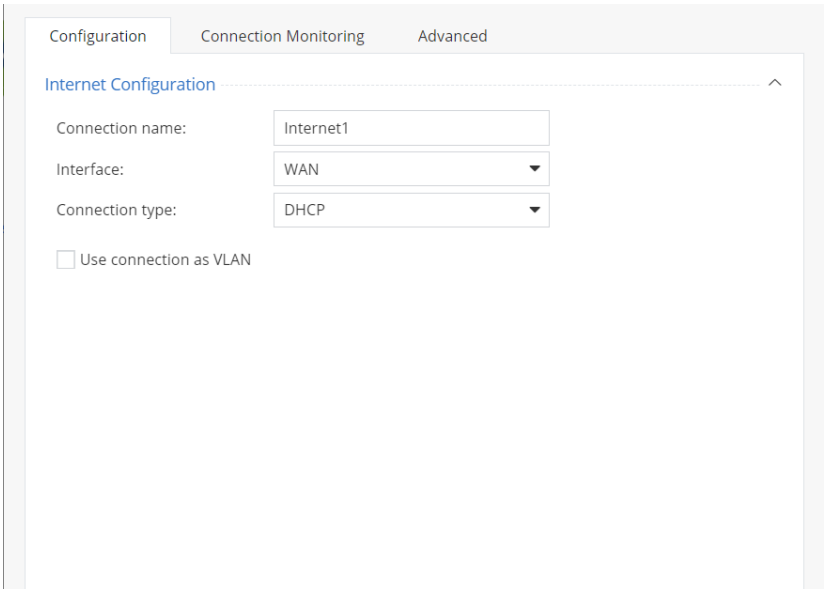
- 固定制用戶，請參考 2.2.1 設定。
- 非固定制用戶 (PPPoE)，請參考 2.2.2 設定。
- DHCP 制用戶，請參考 2.2.3 設定。

1.固定制 IP 客戶

貴客戶請登入 CheckPoint2530，點選 "DEVICE" -> "Internet" ->按 "Edit"，進入下一步驟



請注意 ： 系統預設值為 DHCP



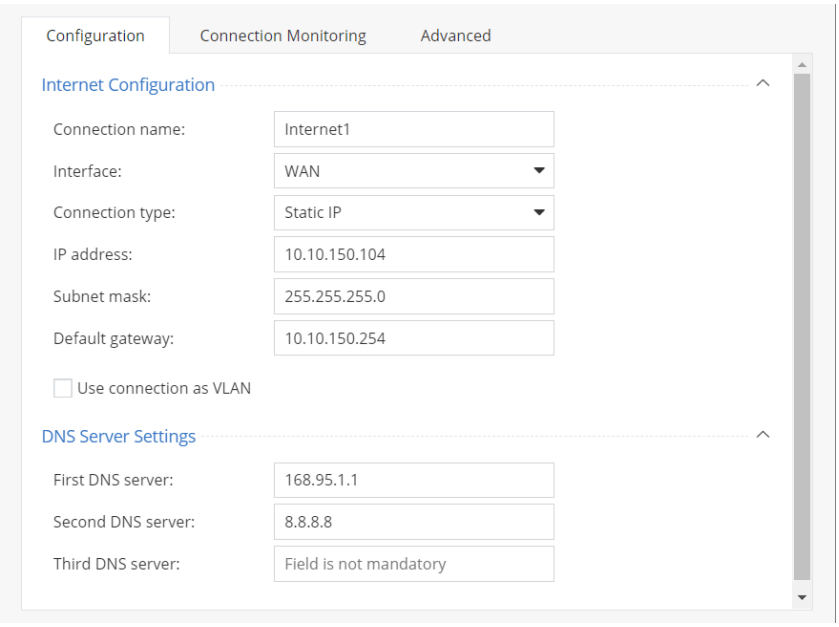
請下拉 "connection type"，選取 Static IP 後，輸入寬頻網路業者提供 IP 位址資料以及預設閘道器 IP 位址資料

IP 網址/網路遮罩：10.10.150.104/255.255.255.0，

Default gateway 10.10.150.254(此為範例，請貴客戶依寬頻網路業者提供資料鍵入)

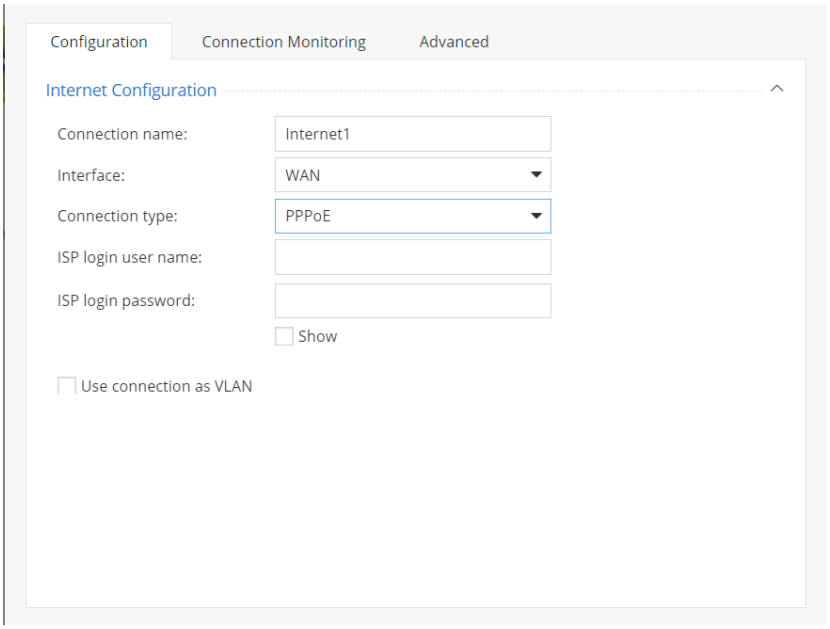
以及 DNS 資料 168.85.1.1、8.8.8.8

完成後按 "Apply" 完成設定



2.非固定制 IP 客戶 (PPPoE)

貴客戶請登入 CheckPoint2530，點選 "DEVICE" -> "Internet" ->按 "Edit"，進入下一步驟

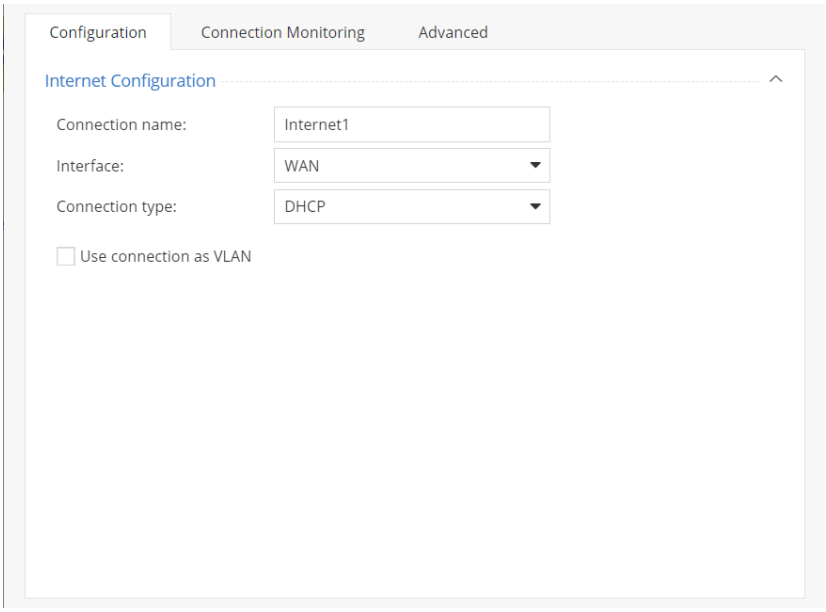


請下拉 "connection type"，選取 PPPOE 後，輸入寬頻網路業者提供的使用者帳號以及密碼，

完成後按 "Apply" 完成設定

3.DHCP 制客戶

貴客戶請登入 CheckPoint2530，點選 "DEVICE" -> "Internet" ->按 "Edit"，進入下一步驟

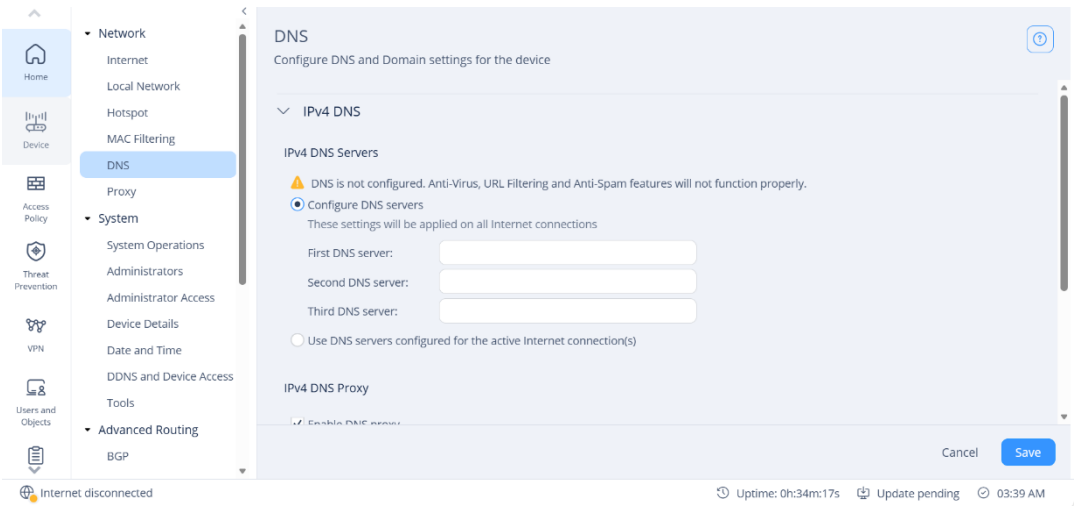


系統預設值為 DHCP，檢查 "connection type"為 DHCP 後，

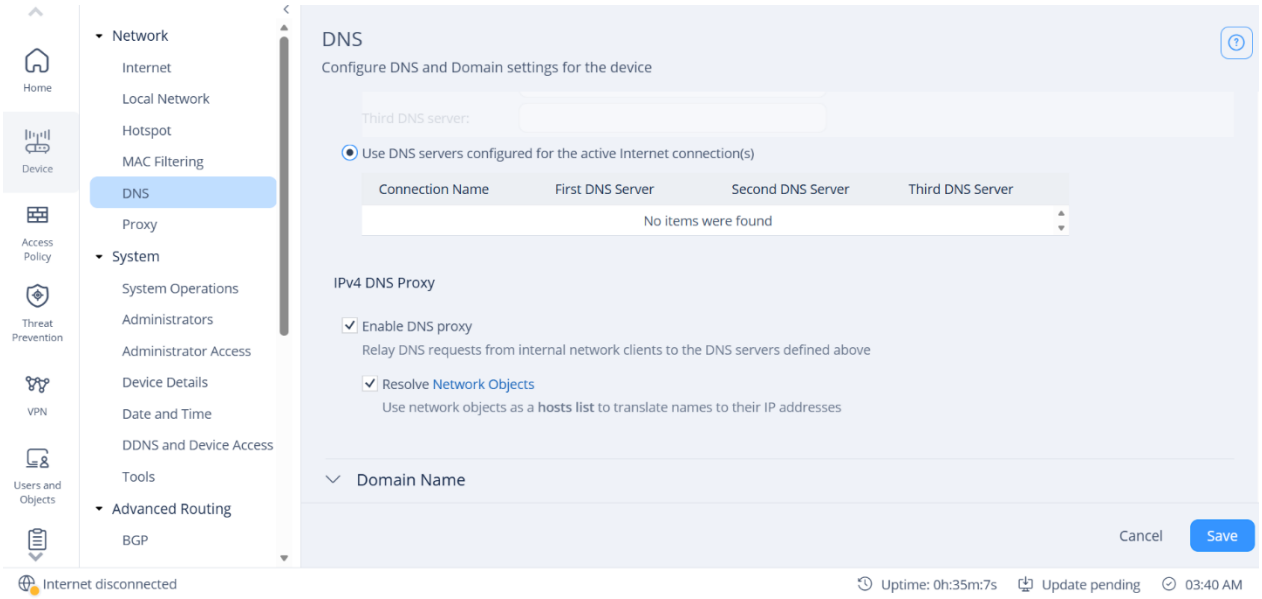
按 "Apply" 完成設定

4. 設定 DNS/NTP 伺服器位址

貴客戶請登入 CheckPoint2530，點選 "DEVICE" -> "DNS" ->按 "Configure"，手動設定 DNS IP



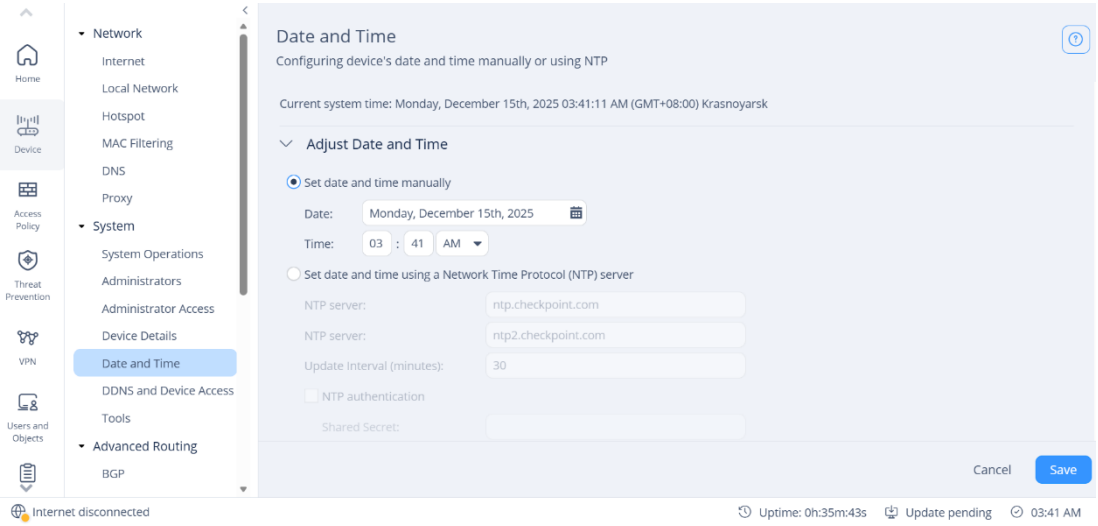
或選取 Use DNS servers configured for the active connection(s)，自動使用電信業者提供的 DNS



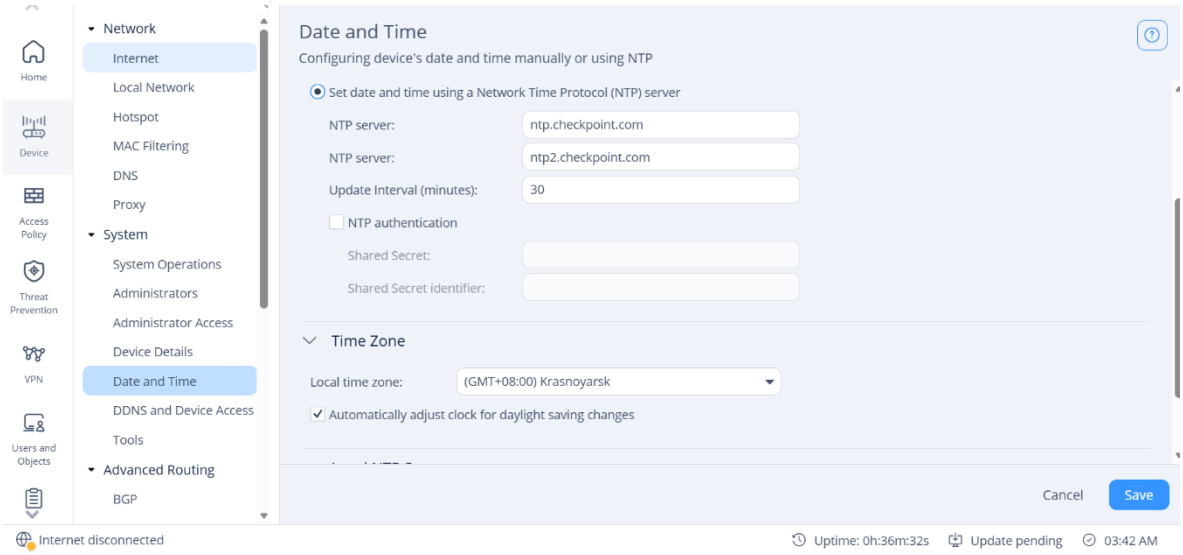
完成後按 "Apply" 完成設定

貴客戶可以在 "DEVICE" -> "Date and Time" 中設定時間，

如需手動設定可以點選 Set date and time manually，手動修改時間



如需設定 NTP server 可以點選 Set date and time using a Network Time Protocol (NTP) server



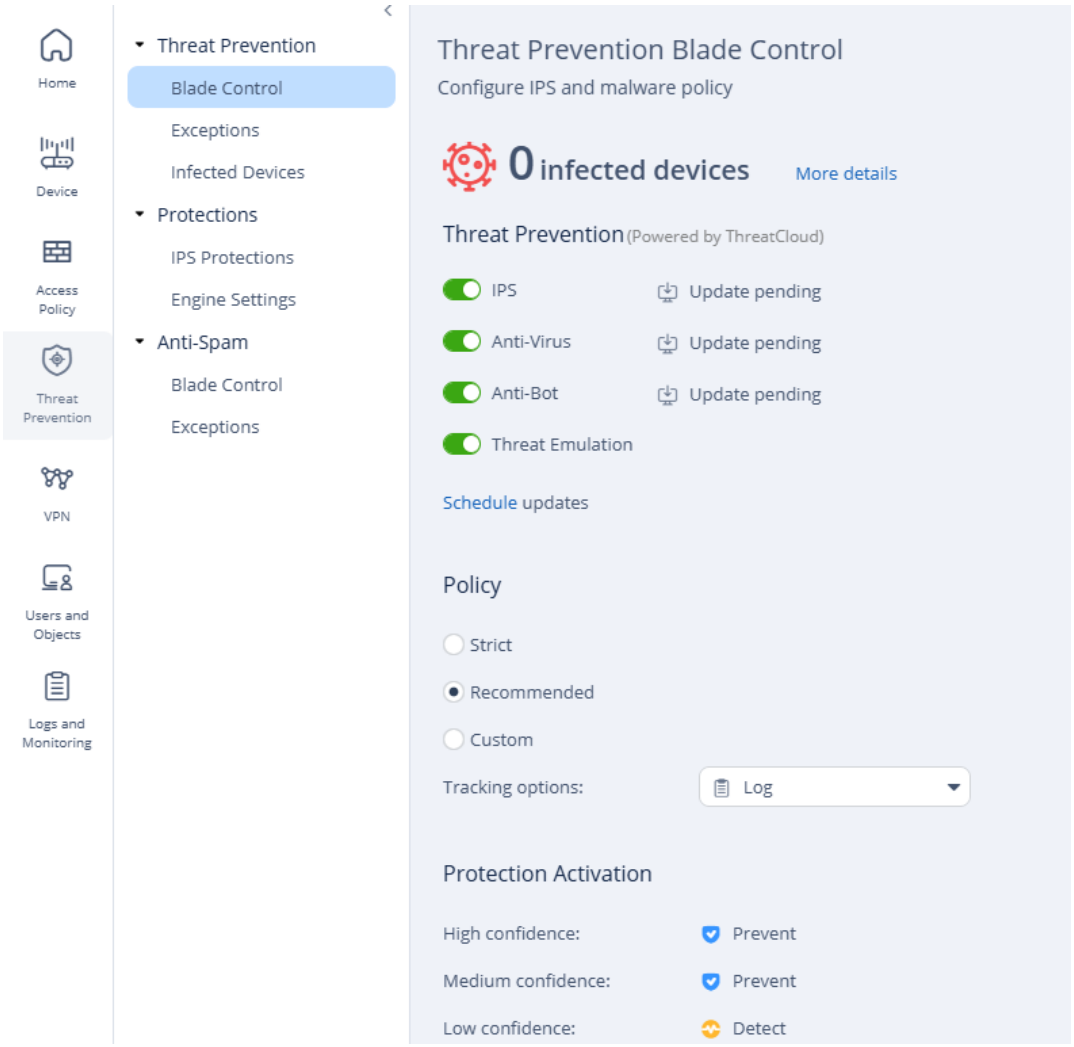
完成後按 "Apply" 完成時間設定

5. 設定防火牆開啟相關服務

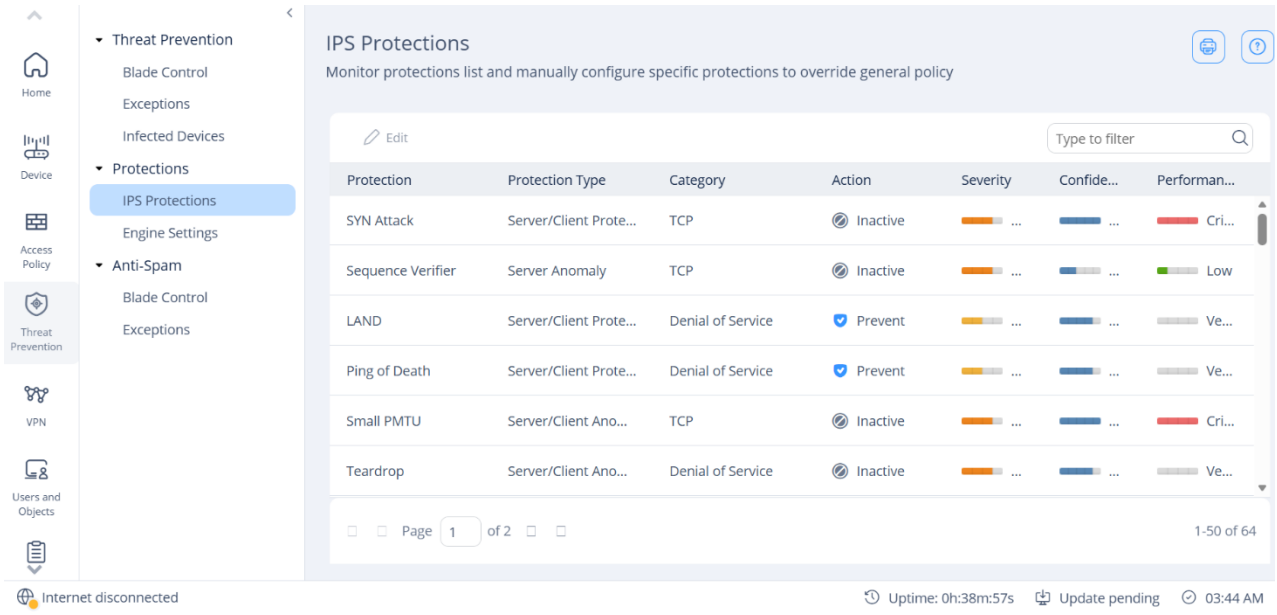
貴客戶請登入 CheckPoint2530，點選 "HOME" -> "Security Dashboard" ，在頁面中可以選擇開啟或關閉防火牆相關的功能

6. 設定 IPS/Application Control/URL Filtering/Anti-Bot/AV&AM

貴客戶請登入 CheckPoint2530，點選 "THREAT PREVENTION" -> "Blade Control" ，在頁面中可以選擇開啟或關閉 IPS/Anti-Virus/Anti-Bot/Threat Emulation，也可以進行資料庫的更新，在 Policy 的部分可以依照客戶需求調整嚴謹度，預設等級為 Recommended



可以點選 "THREAT PREVENTION" -> "IPS Protection"，在頁面中可以針對 IPS 的內容作細部設定



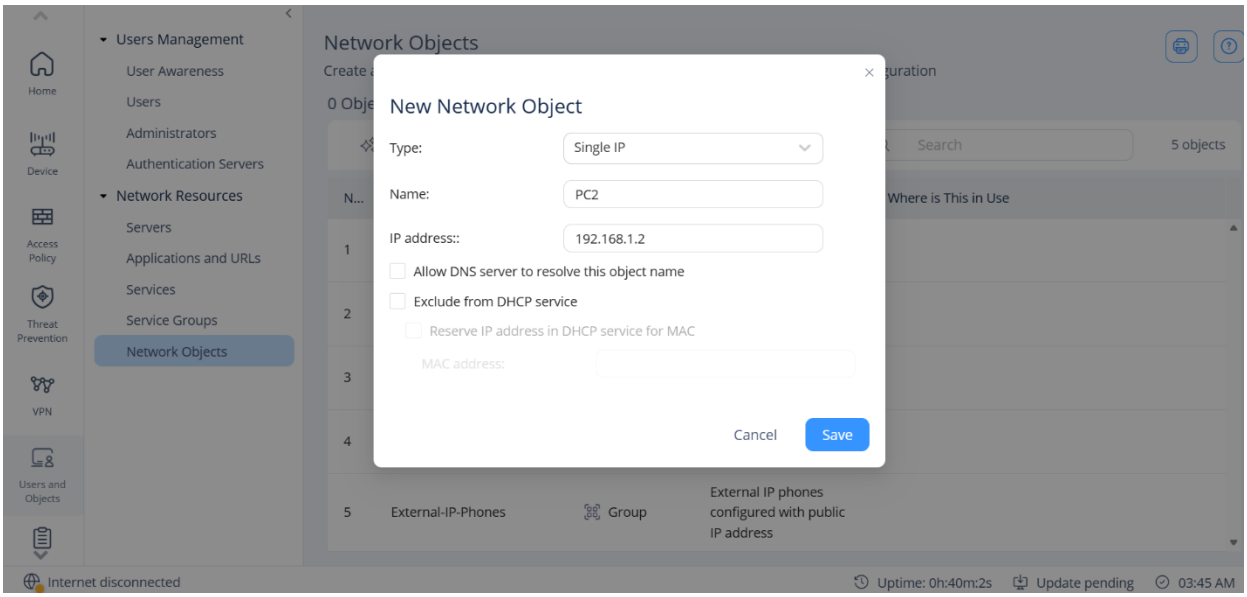
7. IP-Mac Binding

如需設定 IP-Mac Binding 須前往 "USER&OBJECTS" -> "Network Objects"，在頁面中上方點選 New，

會跳出 NEW NETWORK OBJECT 的視窗，將 Type 選項改為 Single IP 並輸入物件 IP 以及物件名稱，

並勾選 Reserve IP address in DHCP service for MAC ，並在 MAC address 欄位輸入 MAC 位址

注意:格式須為 AA:AA:AA:AA:AA:AA



設定完成後按 "Save" 完成設定

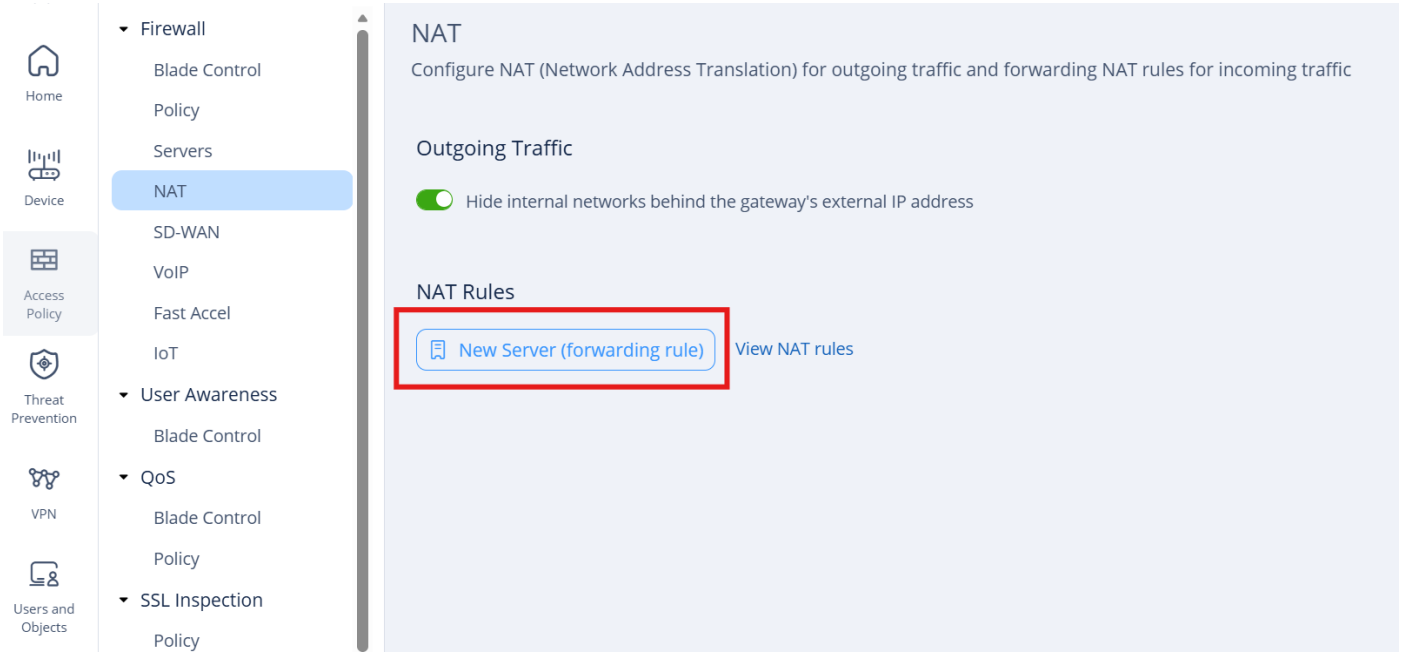
第三章 建立企業內部網站服務

如果貴客戶需要架設內部的伺服器 IP 地址對應（如：網頁伺服器，郵件伺服器），或是某些網路服務需要設定 通訊埠(port)的對應(如：網路遊戲、BitTorrent)，即可於 NAT 設定。

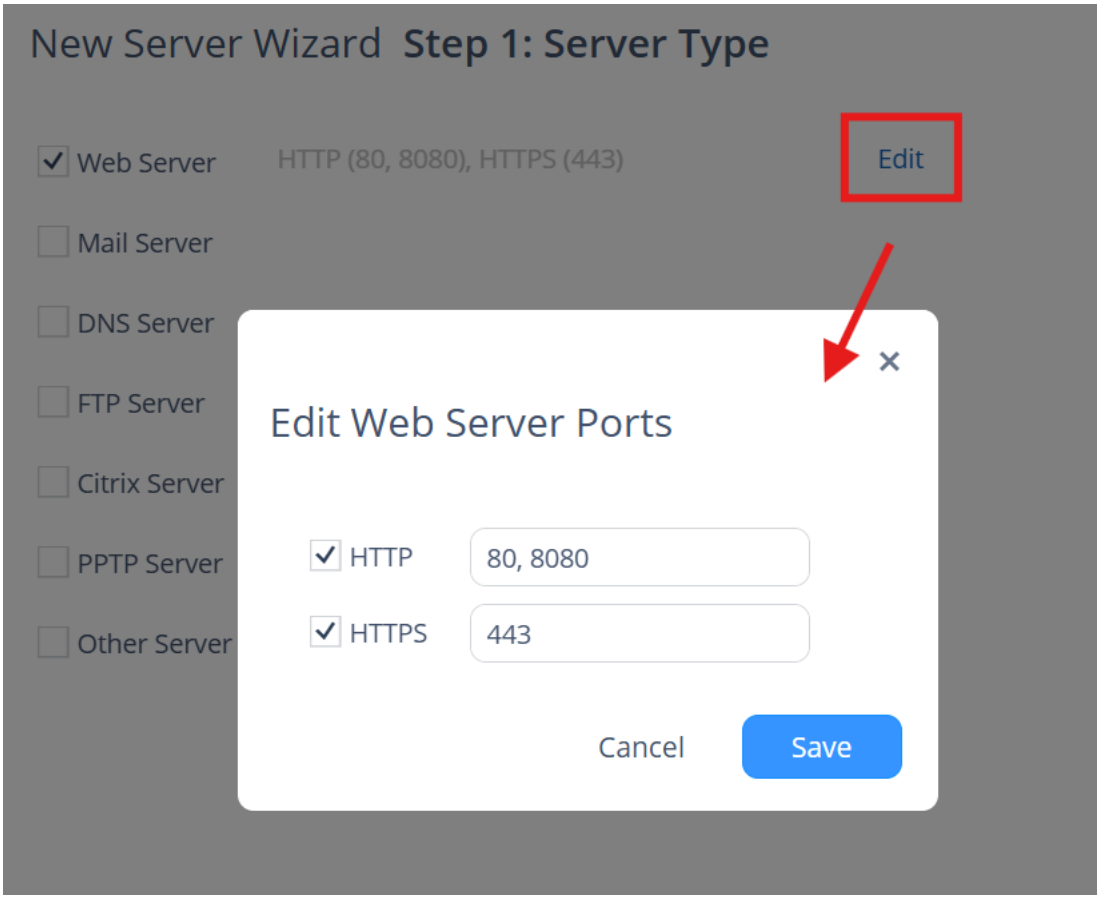
1. 設定 Web(網頁)伺服器

貴客戶請確認完成內部網路組態及外部網路組態設定，確認網際網路連線正常

開啟 Web UI 選擇左邊分頁的[ACCESS POLICY]→[Firewall]→[NAT],選擇右邊選單 NAT Rules 的[New Server(forwarding rule)]進行設定。



選擇[Web Server], 並於後方[edit]，設定所需對應的 port 端設定。



設定網頁伺服器內容：

Name(用戶名)：WebServer　(此為範例，請貴客戶依需求輸入)

IP Address(IP 地址)：172.16.1.100　(此為範例，請貴客戶依需求輸入)

Comments(註解)：web server(只可英文)(此為範例，請貴客戶依需求輸入)

☑Allow DNS Server to resolve this object name(此為範例，請貴客戶依需求輸入)

→允許 DNS 伺服器解析此對象名稱

☑Exclude from DHCP service(此為範例，請貴客戶依需求輸入)

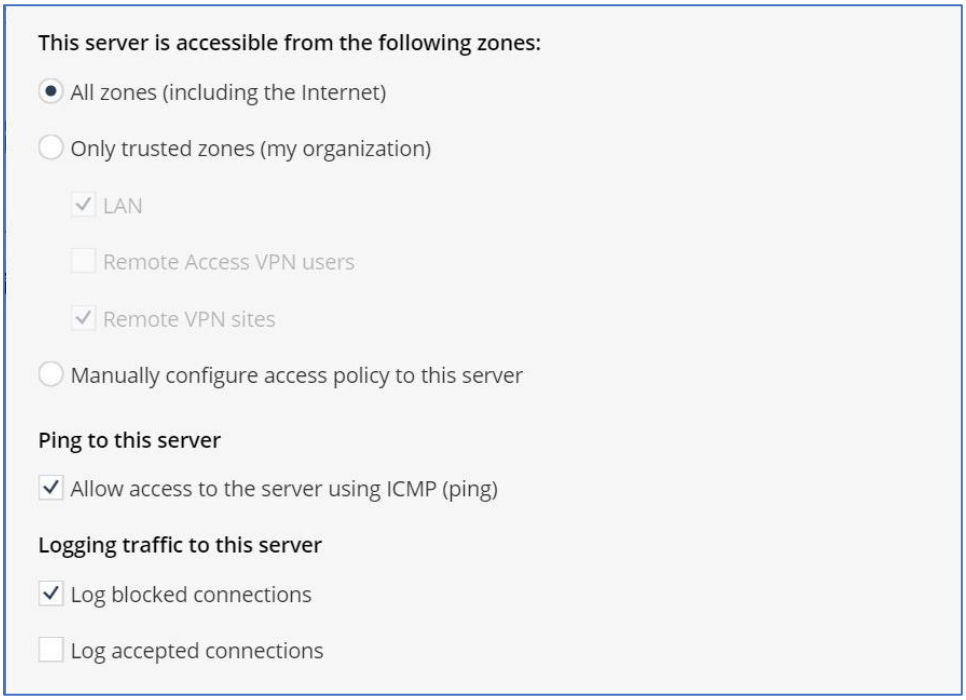
→從 DHCP 服務排除

□Reserve IP address in DHCP service for MAC

→於 DHCP 服務中透過 MAC 保留 IP

MAC address：

設定訪問來源：



選擇可訪問此伺服器的區域：

◉All zones(including the internet) (此為範例，請貴客戶依需求輸入)

→所有區域皆可以訪問

○Only trusted zones(my organization)

□LAN

□Remote Access VPN Sites

□Remote VPN Sites

→只有受信任的區域可以訪問

○Manually configure access policy to this server

→手動配置對此服務器的訪問策略

Ping to this server：

☑Allow access to the server using ICMP (ping) (此為範例，請貴客戶依需求輸入)

→允許使用 ICMP 到伺服器

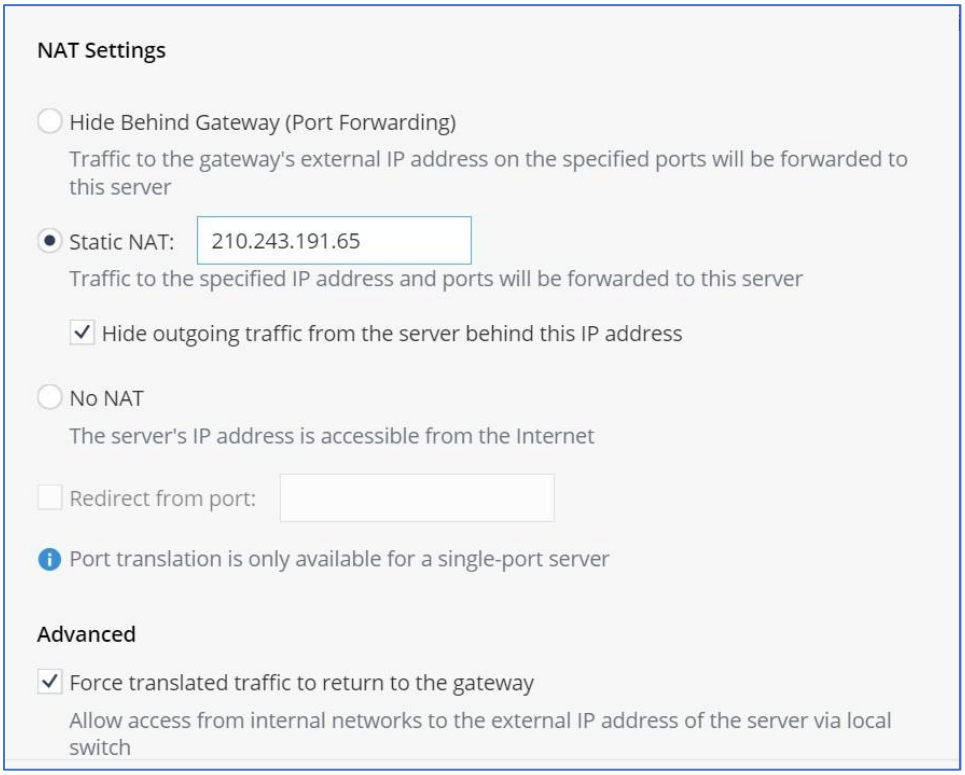
Logging traffic to this server：

☑Log blocked connections　(此為範例，請貴客戶依需求輸入)

□Log accepted connections

→將流量記錄到此服務器

網路地址轉換設定



網路地址轉換設置：

○Hide Behind Gateway(port Forwarding)

→隱藏在網關後面(端口轉發)

◉Static NAT：[210.243.191.65] (此為範例，請貴客戶依需求輸入)

→靜態 NAT

☑Hide outgoing traffic from the server behind this IP address(此為範例，請貴客戶依需求輸入)

○No NAT

→無 NAT

Redirect from port：[_____]

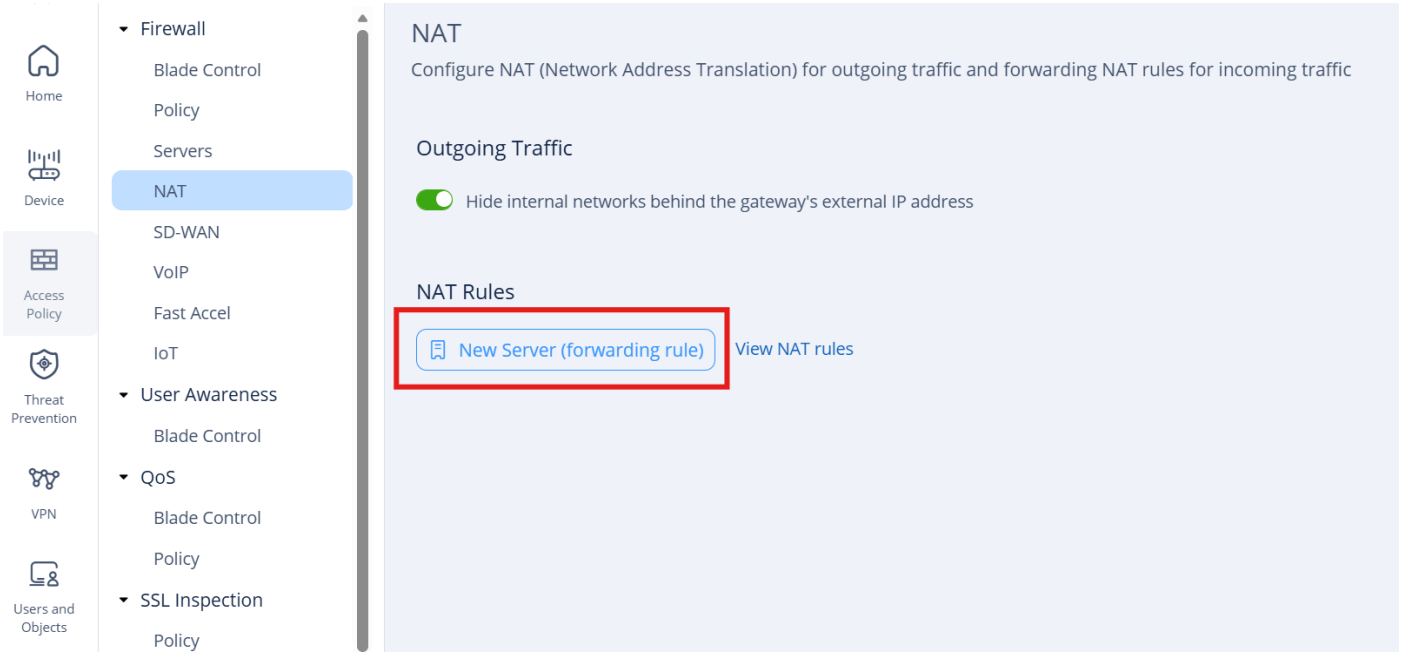
設定完成後到[ACCESS POLICY]→[Servers]確認是否有設定成功。

確認已有設定成功，再到[ACCESS POLICY]→[Firewall]→[NAT],選擇[Hide NAT rules]，確認是否有自動產生出對應的 rule。

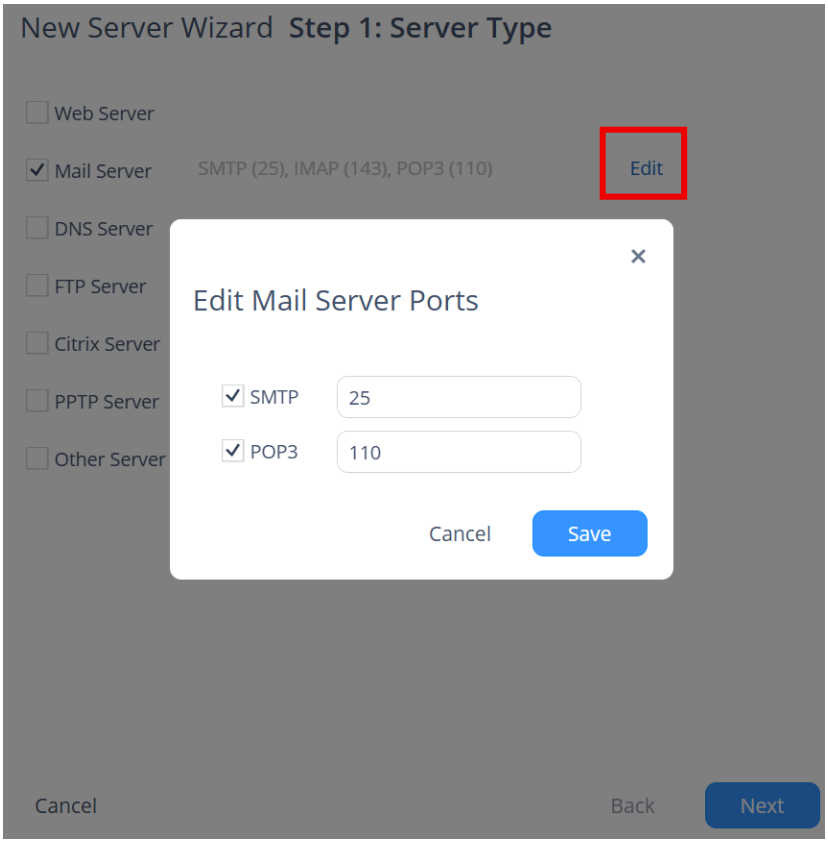
2. 設定(Mail)郵件伺服器

貴客戶請確認完成內部網路組態及外部網路組態設定，確認網際網路連線正常

開啟 Web UI 選擇左邊分頁的[ACCESS POLICY]→[Firewall]→[NAT],選擇右邊選單 NAT Rules 的[New Server(forwarding rule)]進行設定。



選擇[Mail Server], 並於後方[edit]，設定所需對應的 port 端設定。



.設定郵件伺服器內容：

Name(用戶名)：MailServer　(此為範例，請貴客戶依需求輸入)

IP Address(IP 地址)：172.16.1.200　(此為範例，請貴客戶依需求輸入)

Comments(註解)：可不填 (只可英文)(此為範例，請貴客戶依需求輸入)

☑Allow DNS Server to resolve this object name(此為範例，請貴客戶依需求輸入)

→允許 DNS 伺服器解析此對象名稱

☑Exclude from DHCP service(此為範例，請貴客戶依需求輸入)

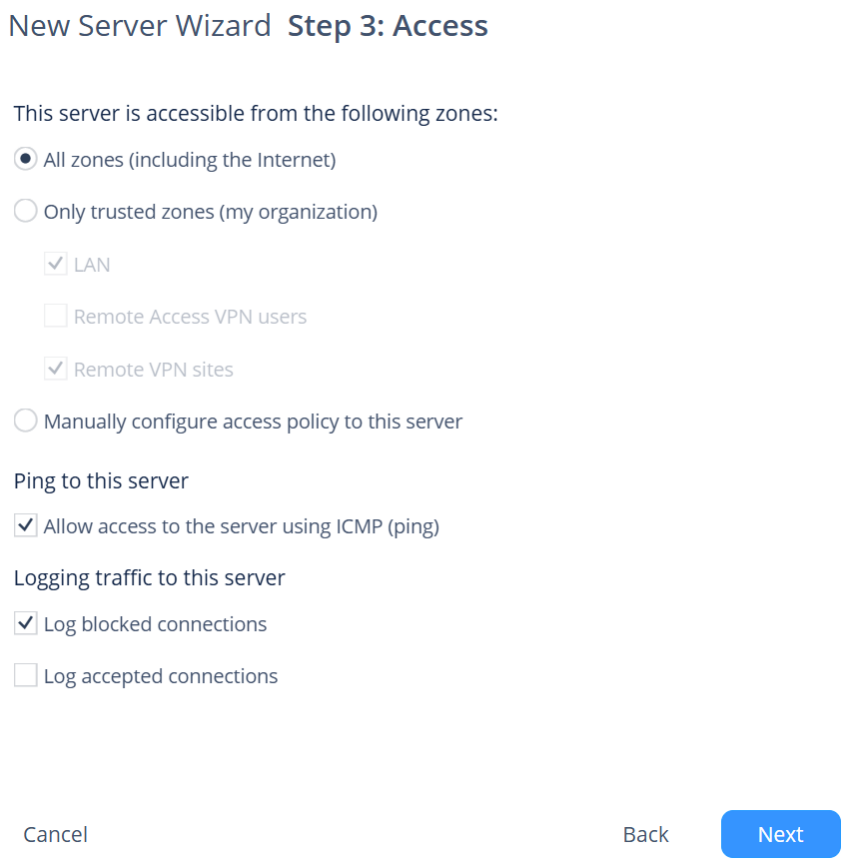
→從 DHCP 服務排除

□Reserve IP address in DHCP service for MAC

→於 DHCP 服務中透過 MAC 保留 IP

MAC address：

設定訪問來源：



選擇可訪問此伺服器的區域：

◉All zones(including the internet) (此為範例，請貴客戶依需求輸入)

→所有區域皆可以訪問

○Only trusted zones(my organization)

□LAN

□Remote Access VPN Sites

□Remote VPN Sites

→只有受信任的區域可以訪問

○Manually configure access policy to this server

→手動配置對此服務器的訪問策略

Ping to this server：

☑Allow access to the server using ICMP (ping) (此為範例，請貴客戶依需求輸入)

→允許使用 ICMP 到伺服器

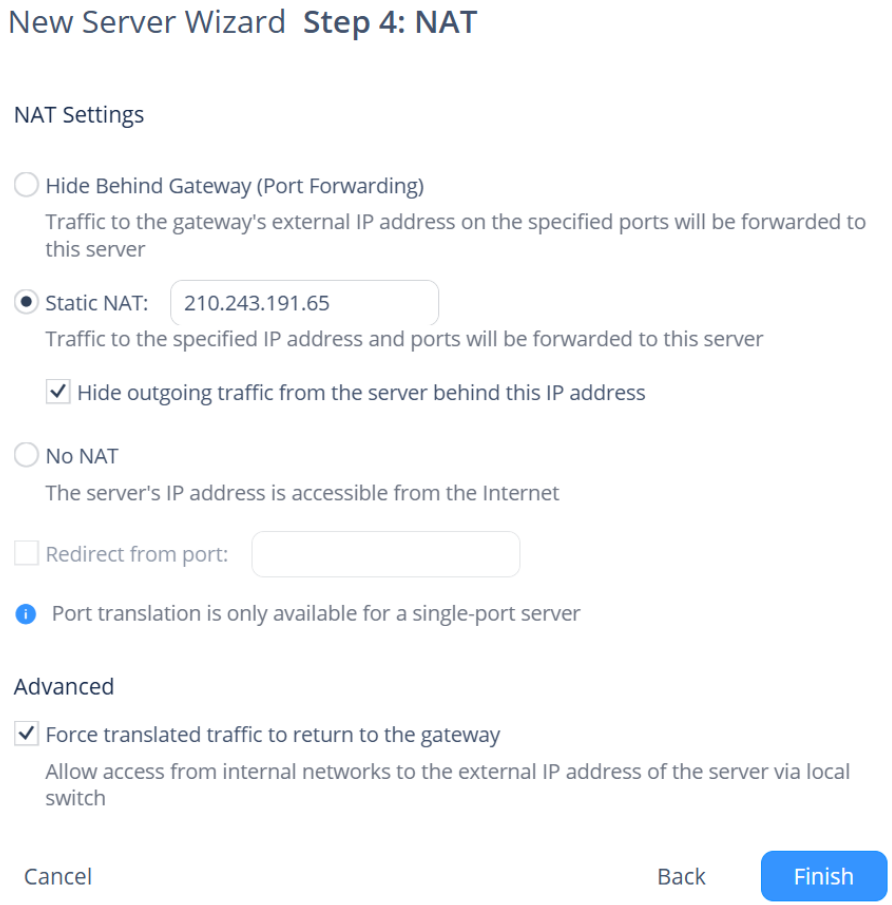
Logging traffic to this server：

☑Log blocked connections　(此為範例，請貴客戶依需求輸入)

□Log accepted connections

→將流量記錄到此服務器

網路地址轉換設定



網路地址轉換設置：

○Hide Behind Gateway(port Forwarding)

→隱藏在網關後面(端口轉發)

◉Static NAT：[210.243.191.65] (此為範例，請貴客戶依需求輸入)

→靜態 NAT

☑Hide outgoing traffic from the server behind this IP address(此為範例，請貴客戶依需求輸入)

○No NAT

→無 NAT

Redirect from port：[_____]

設定完成後到[ACCESS POLICY]→[Servers]確認是否有設定成功。

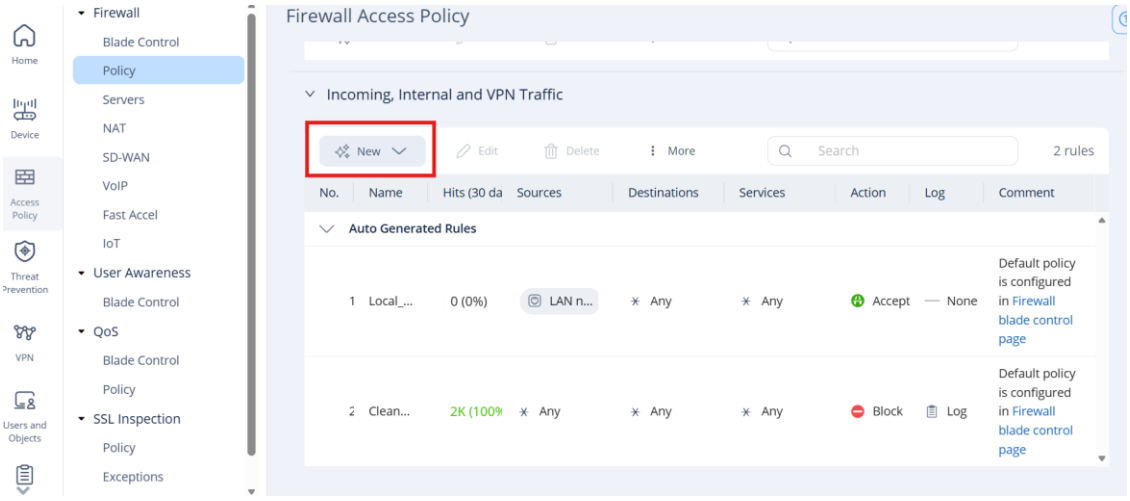
確認已有設定成功，再到[ACCESS POLICY]→[Firewall]→[NAT],選擇[Hide NAT rules]，確認是否有自動產生出對應的 rule。

3. 設定對外服務伺服器

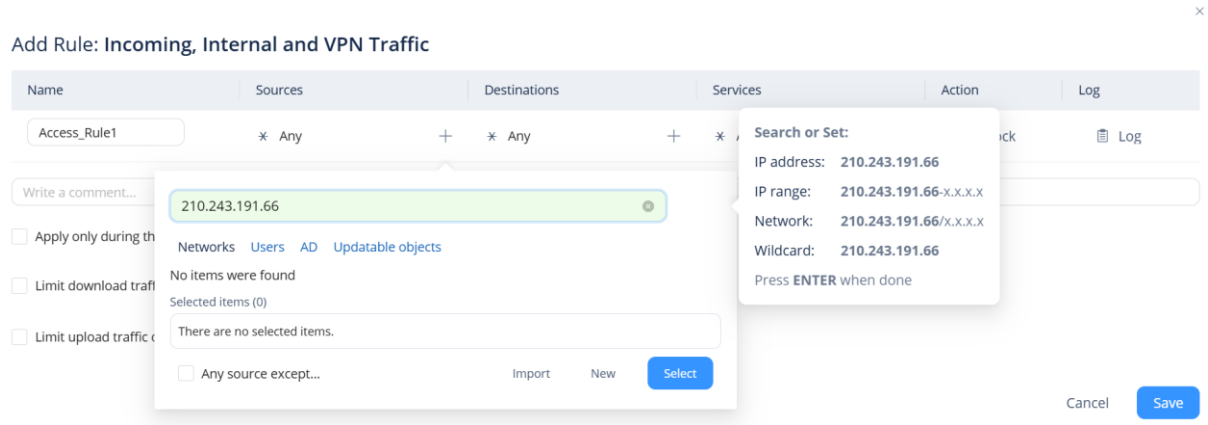
貴客戶若有需求要將內部 PC 開放由外部連線 (如，PC 需外部人員連線遠端桌面協助設定)

貴客戶請確認完成內部網路組態及外部網路組態設定，確認網際網路連線正常

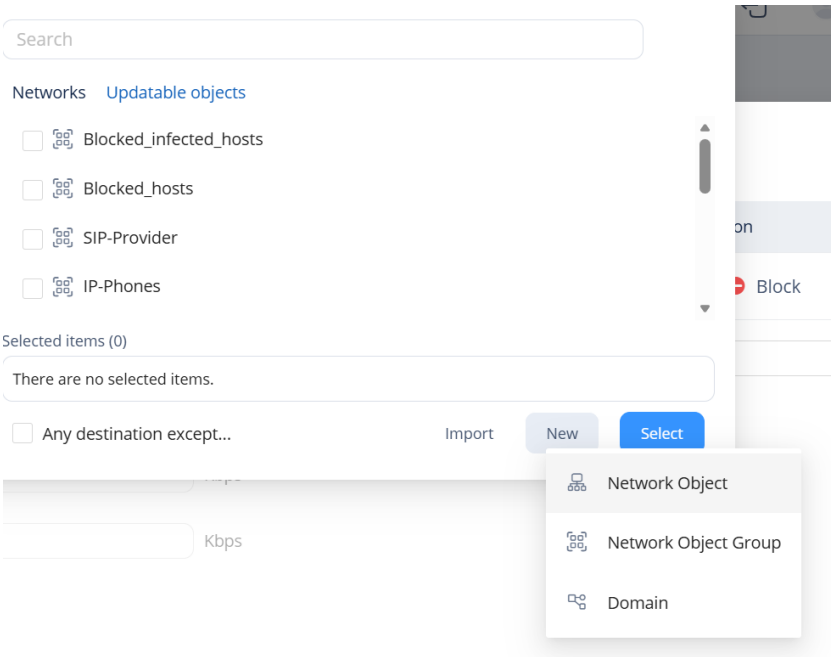
開啟 Web UI 選擇左邊分頁的[ACCESS POLICY]→[policy]選擇右邊選單下方[incoming]的[New] 進行設定。



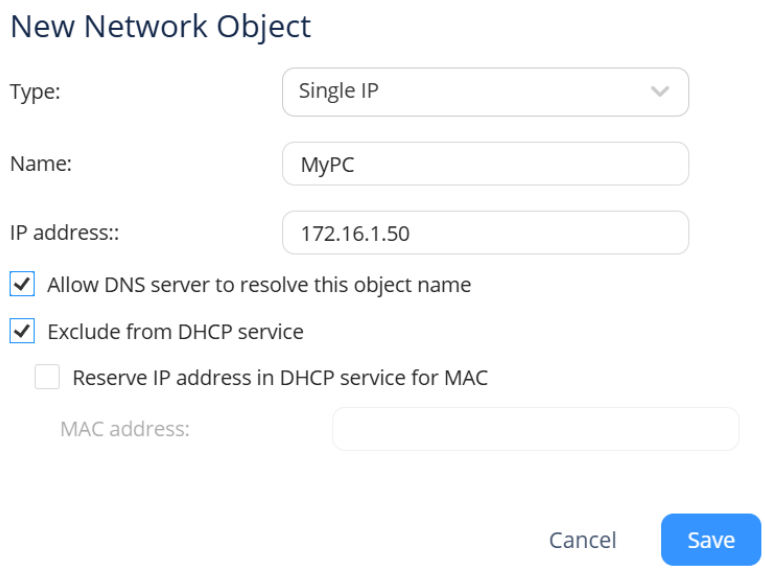
選擇[Source], 然後輸入服務網路位址/範圍：210.243.191.66(此為範例，請貴客戶依需求輸入，請勿使用外部網路介面 IP，若只有一個真實外部 IP，請使用 Port 轉發方式)



選擇[Destination]，選擇[New]中的[Network object]



於 New Network object 中的[type]選擇 Single IP



IPV4 address：172.16.1.50 (此為範例，請貴客戶依需求輸入)

Object name：MyPC (此為範例，請貴客戶依需求輸入)

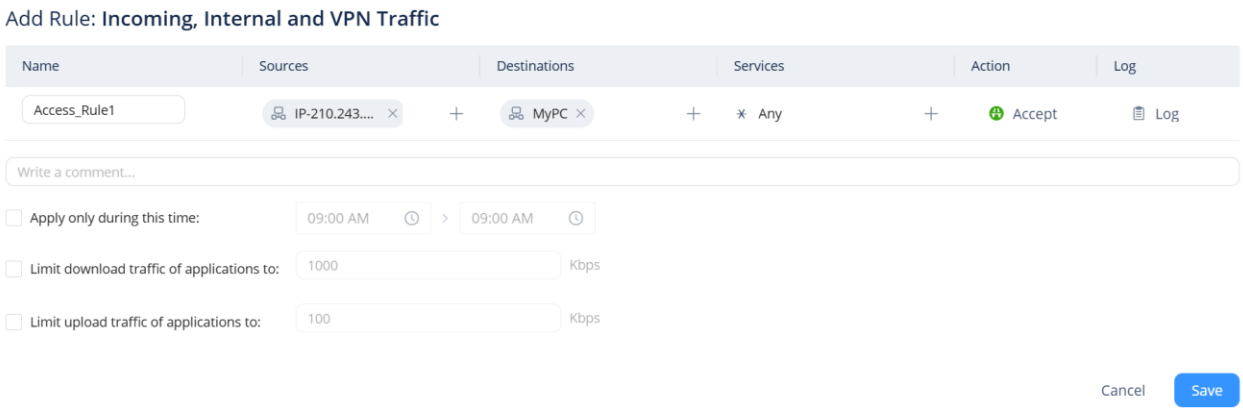
☑Allow DNS Server to resolve object name (此為範例，請貴客戶依需求輸入)

→允許 DNS 伺服器解析此對象名稱

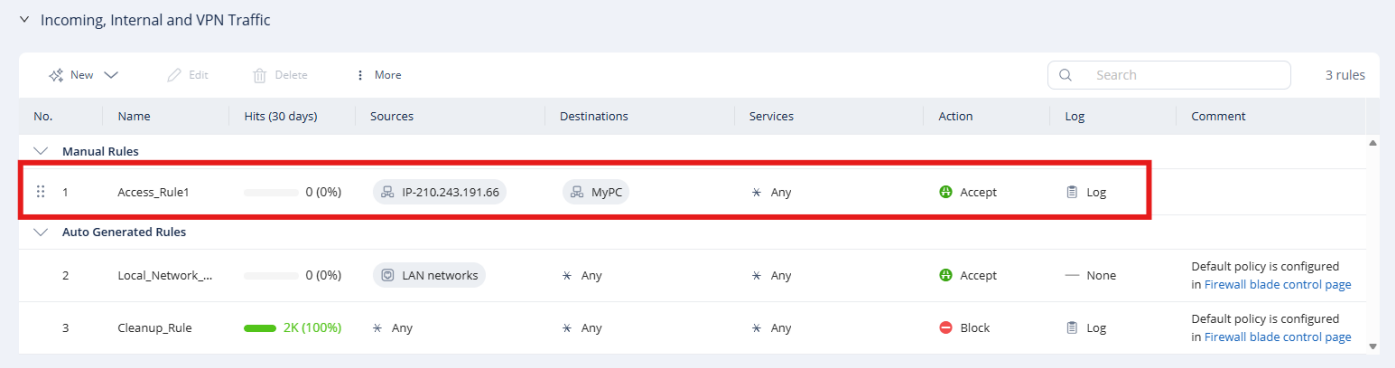
☑Exclude from DHCP (此為範例，請貴客戶依需求輸入)

→從 DHCP 服務排除

確認都有設定完成後，選[save]確認



設定完成後到[ACCESS POLICY]→[Servers]確認是否有設定成功。

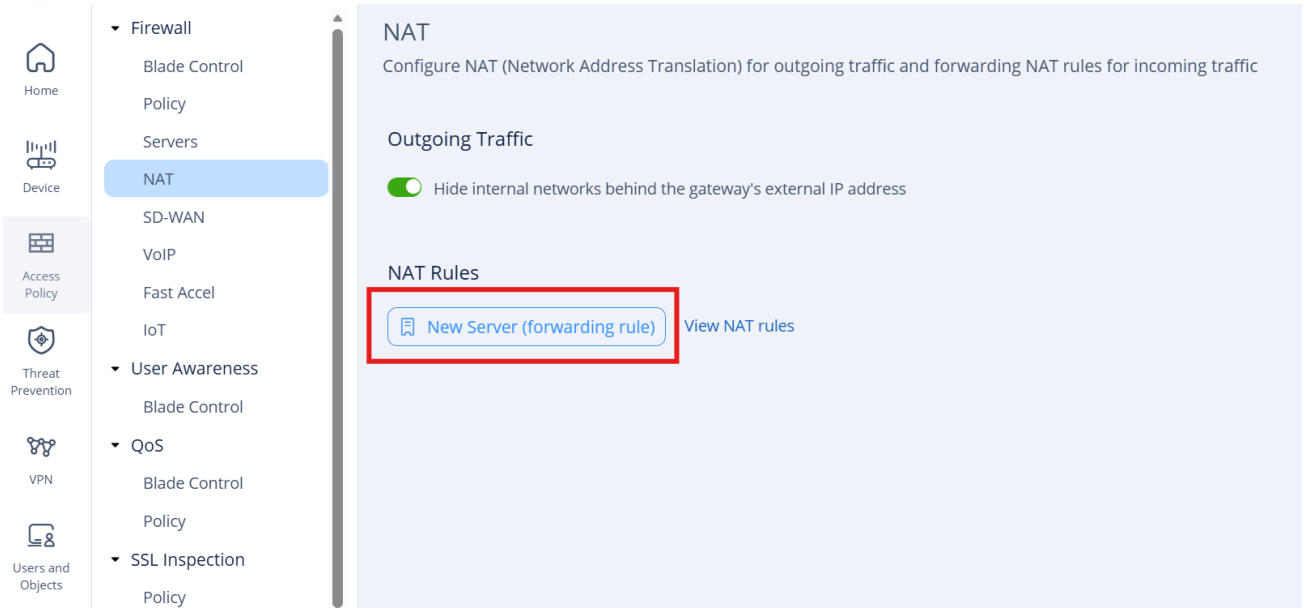


4. 設定開啟 BitTorrent 服務

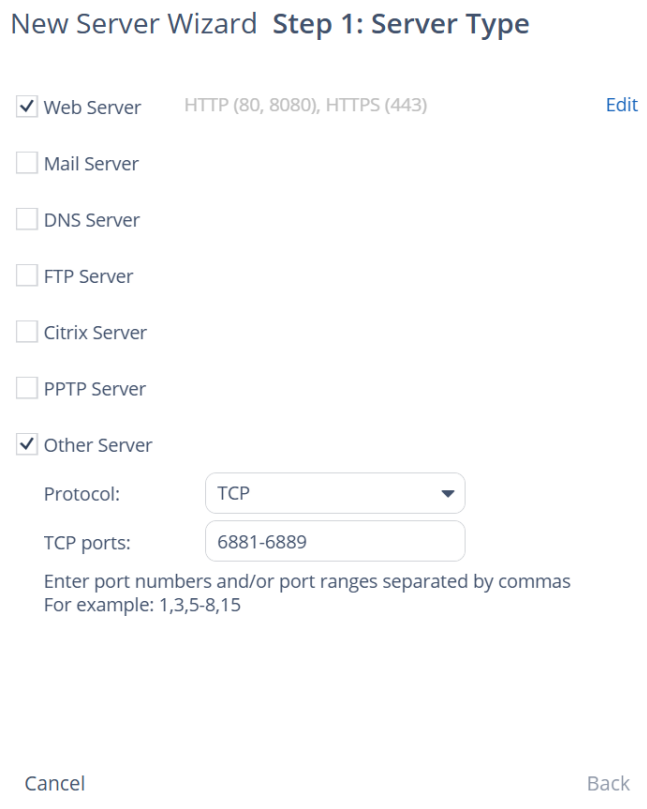
開起單一 PC 可使用 BitTorrent 服務

貴客戶請確認完成內部網路組態及外部網路組態設定，確認網際網路連線正常

開啟 Web UI 選擇左邊分頁的[ACCESS POLICY]→[Firewall]→[NAT],選擇右邊選單 NAT Rules 的[New Server(forwarding rule)]進行設定。



選擇[Other Server], 選擇 Protocol，然後設定所需對應的 port 端設定。



Procotol：TCP　(此為範例，請貴客戶依需求輸入)

TCP ports：6881-6889　(此為範例，請貴客戶依需求輸入)

設定對外伺服器內容：

Name(用戶名)：My_PC　(此為範例，請貴客戶依需求輸入)

IP Address(IP 地址)：172.16.1.10　(此為範例，請貴客戶依需求輸入)

Comments(註解)：BitTorrent access (只可英文)(此為範例，請貴客戶依需求輸入)

☑Allow DNS Server to resolve this object name(此為範例，請貴客戶依需求輸入)

→允許 DNS 伺服器解析此對象名稱

☑Exclude from DHCP service(此為範例，請貴客戶依需求輸入)

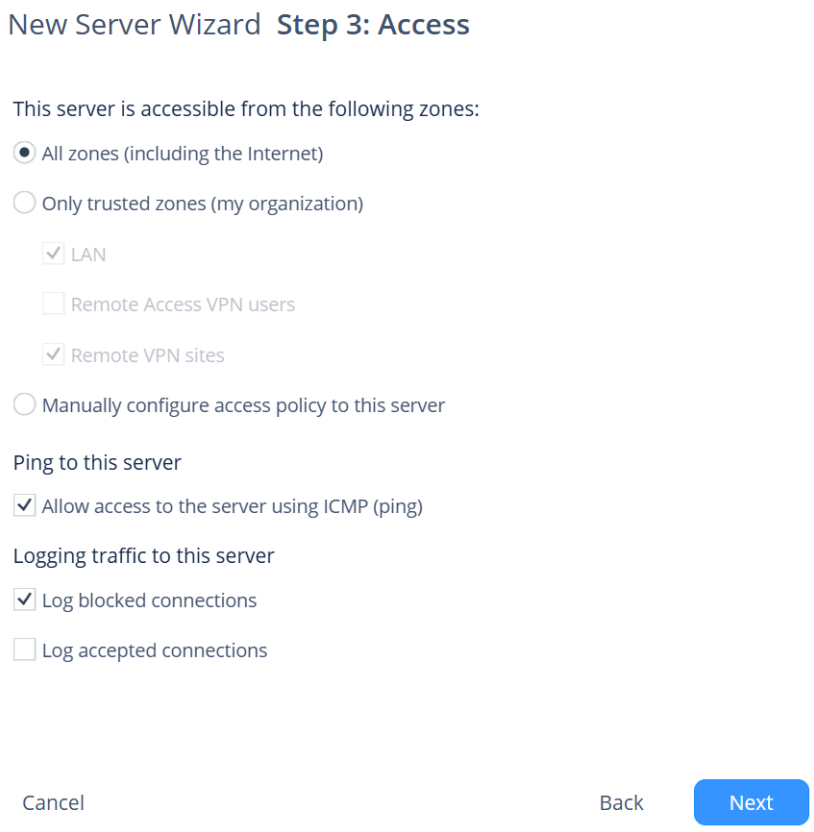
→從 DHCP 服務排除

□Reserve IP address in DHCP service for MAC

→於 DHCP 服務中透過 MAC 保留 IP

MAC address：

設定訪問來源：



選擇可訪問此伺服器的區域：

◉All zones(including the internet) (此為範例，請貴客戶依需求輸入)

→所有區域皆可以訪問

○Only trusted zones(my organization)

□LAN

□Remote Access VPN Sites

□Remote VPN Sites

→只有受信任的區域可以訪問

○Manually configure access policy to this server

→手動配置對此服務器的訪問策略

Ping to this server：

☑Allow access to the server using ICMP (ping) (此為範例，請貴客戶依需求輸入)

→允許使用 ICMP 到伺服器

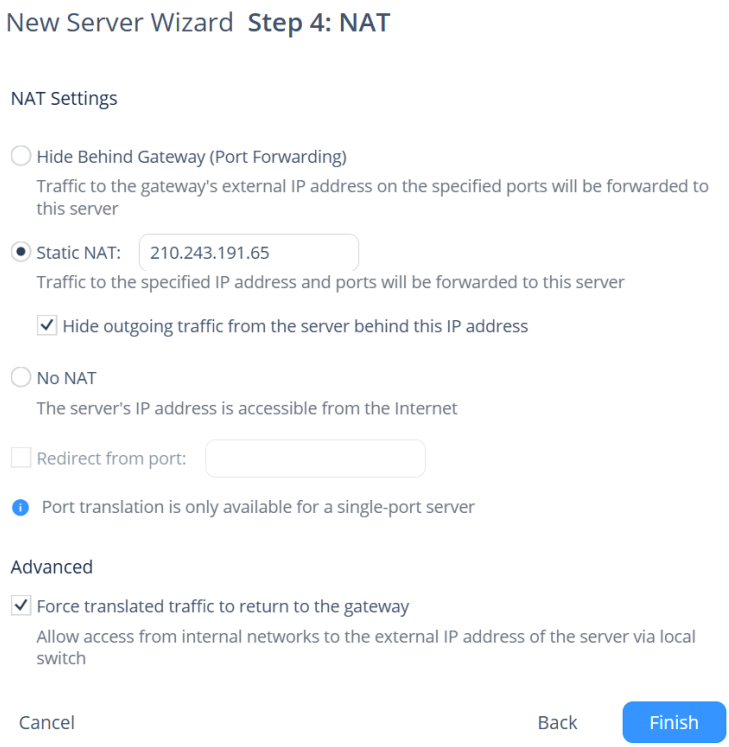
Logging traffic to this server：

☑Log blocked connections　(此為範例，請貴客戶依需求輸入)

□Log accepted connections

→將流量記錄到此服務器

網路地址轉換設定



網路地址轉換設置：

○Hide Behind Gateway(port Forwarding)

→隱藏在網關後面(端口轉發)

◉Static NAT：[210.243.191.65] (此為範例，請貴客戶依需求輸入)

→靜態 NAT

☑Hide outgoing traffic from the server behind this IP address(此為範例，請貴客戶依需求輸入)

○No NAT

→無 NAT

Redirect from port：[_____]

設定完成後到[ACCESS POLICY]→[Servers]確認是否有設定成功。

確認已有設定成功，再到[ACCESS POLICY]→[Firewall]→[NAT],選擇[Hide NAT rules]，確認是否有自動產生出對應的 rule。

第四章 線路 Fail-over 設定

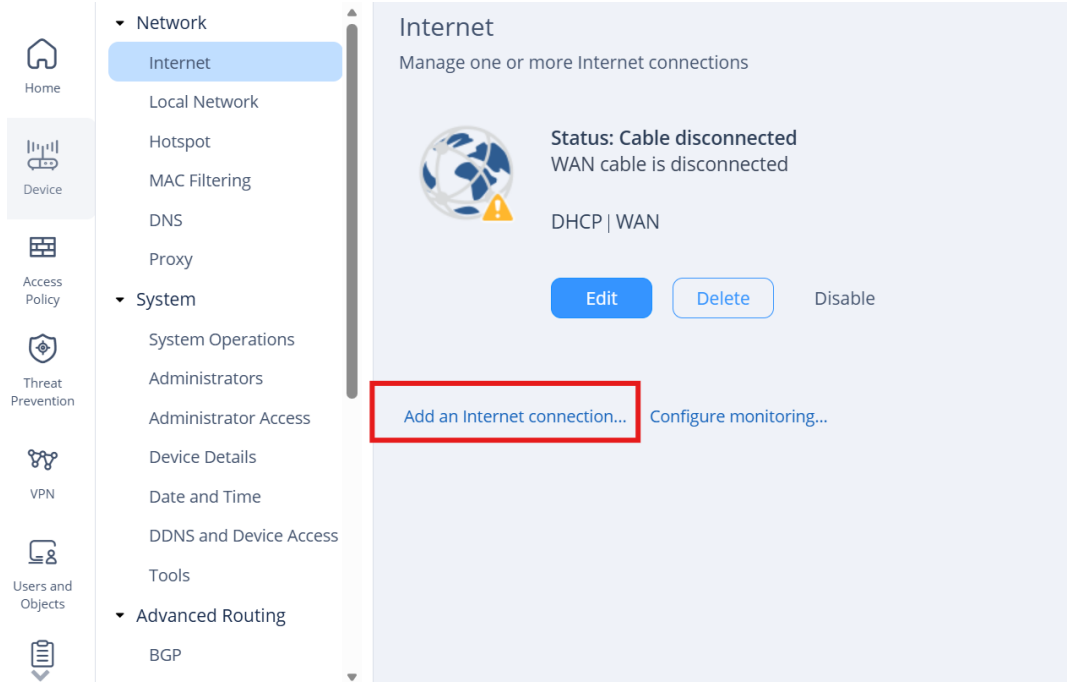
1. ISP Redundancy

ISP Redundancy 只支援 IPv4 模式，可以在高可用性(備援)或負載共享模式下配置多個互聯網連接。

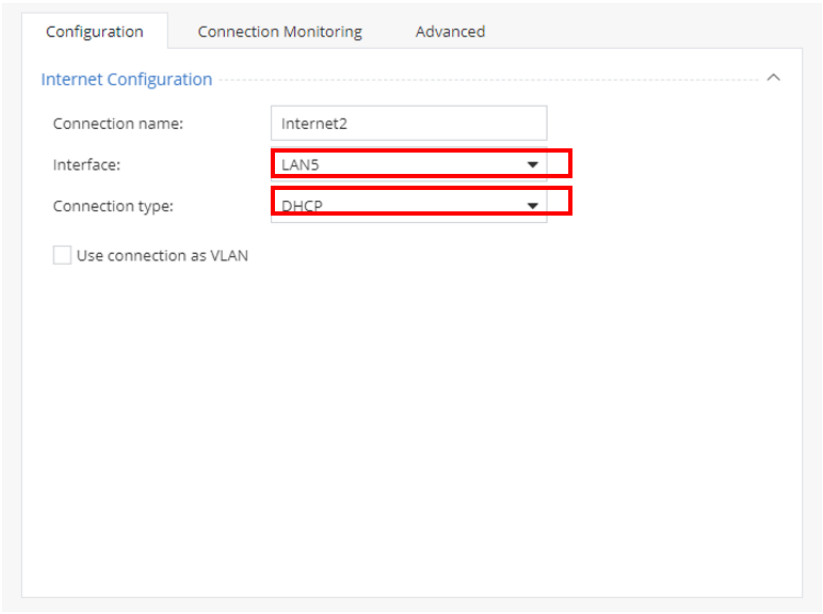
當您配置多個互聯網連接時，在 **Device** > **Internet** 面可讓您在這些選項之間切換。 每個 Internet 連接的 Advanced 設置允許您根據設置的模式，配置每個連接的優先級或權重。

- **High Availability 模式- 優先級** - 選擇連接的優先級。 只有在較高優先級的連接不可用時，才會使用較低優先級的連接。
- **Load Balancing 模式- 權重** - 到 Internet 的流量根據其權重在所有可用連接之間分配。

步驟一：點選左上角 "DEVIC"→ 點選 "Network"中的" Internet" 會出現下圖：



步驟二:點選 Add an Internet connection，輸入線路名稱、選擇的網路 port 以及此網路的類型 ex 固定 IP or DHCP。

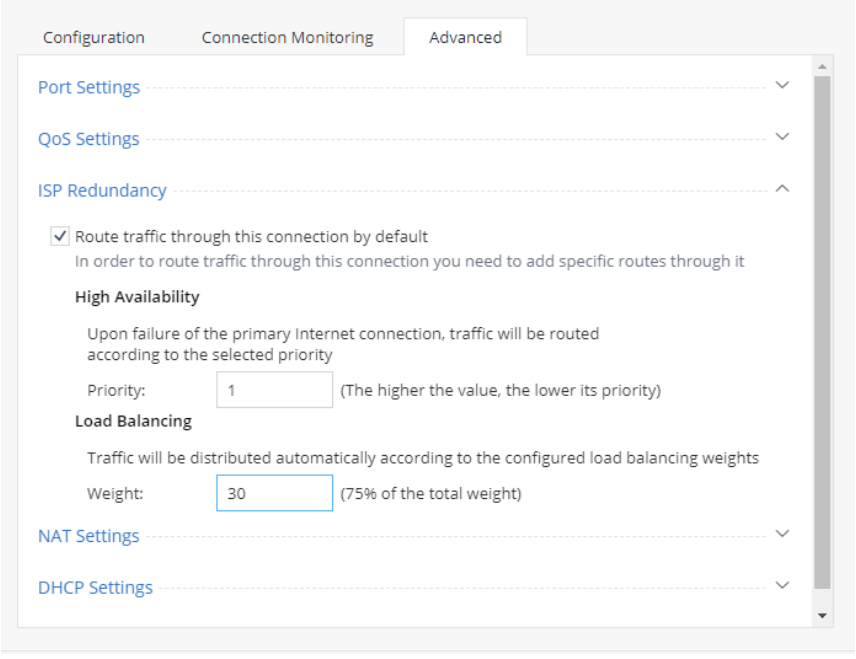


步驟三:設定完成後可以看到兩條線路的狀態(預設為高可用性/備援模式)

步驟四:點選 Configure 可以選擇模式 HA(高可用性/備援模式)或 Load Balancing(負載共享模式)

步驟五: 選取 Load Balancing(負載模式)模式

步驟六: 選取需要設定的線路後，圖示為 Internet1(primary)，點選 Edit 可以修改線路的權重，以及其他設定，如下圖



設定完成後按 "Apply" 完成設定

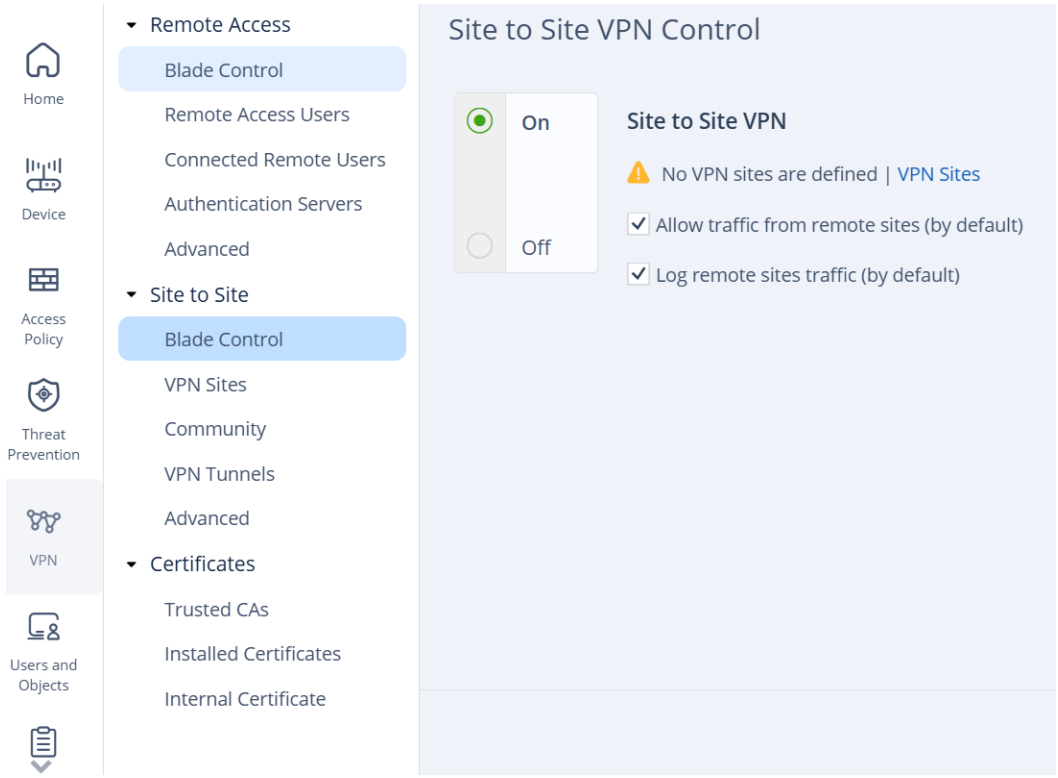
第五章 VPN 連線設定

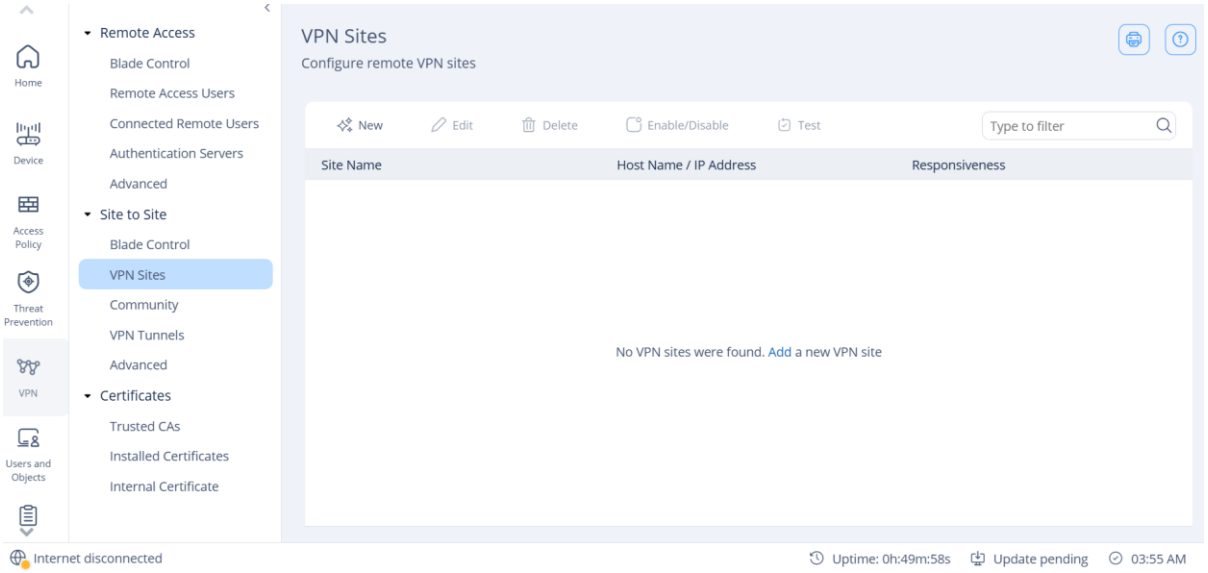
1. IPsec VPN (Site-to-Site)設定

貴客戶有點對點 VPN 連線需求，可依本章介紹設定 VPN，請先確認以下重點：

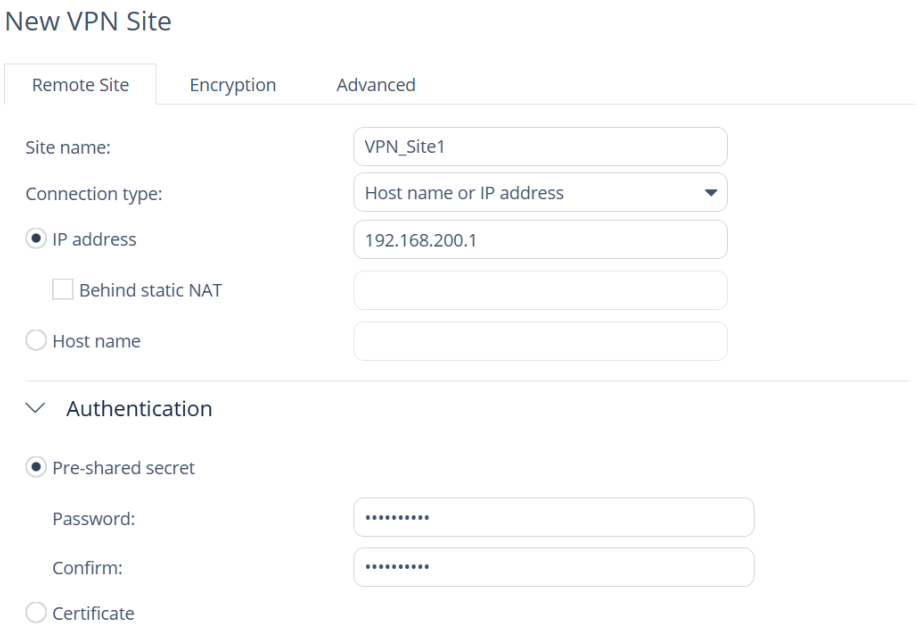
- 兩端點皆需固定 IP
- 兩端點內部網路 IP 網段為不相同網段. (例如一端為 192.168.1.0/24，另一端為 192.168.2.0/24)

登入 CheckPoint 防火牆後，於左邊功能欄位點選 VPN 選項，再到 Site to Site 功能下選擇 Blade Control，將 Site to Site VPN 功能選項選擇 On。

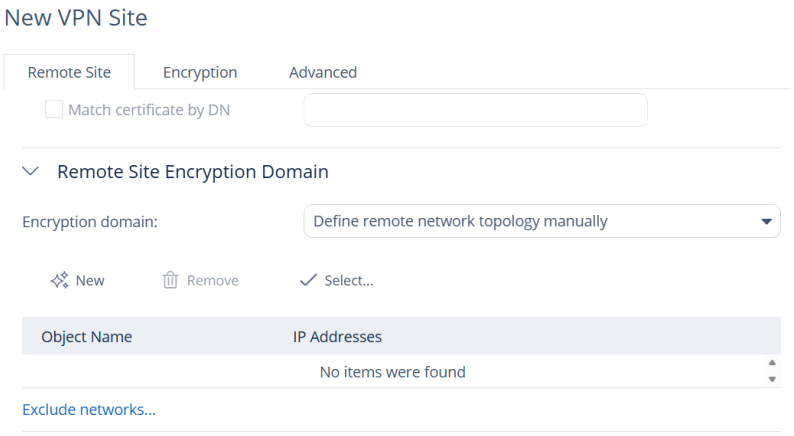




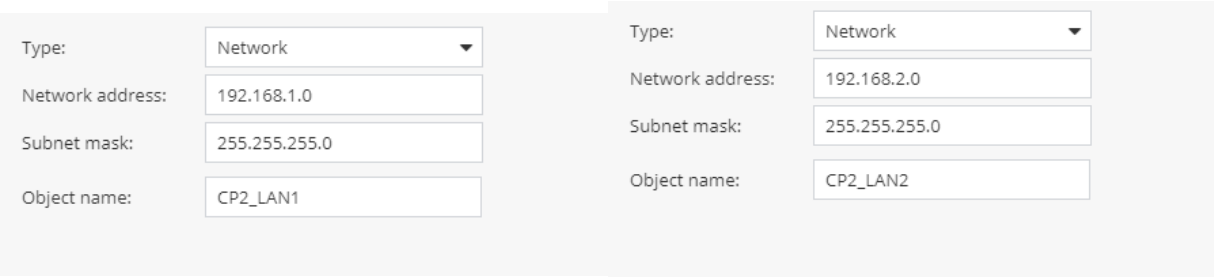
到 VPN Sites 中，點選 New 來新增一筆新的 VPN Site



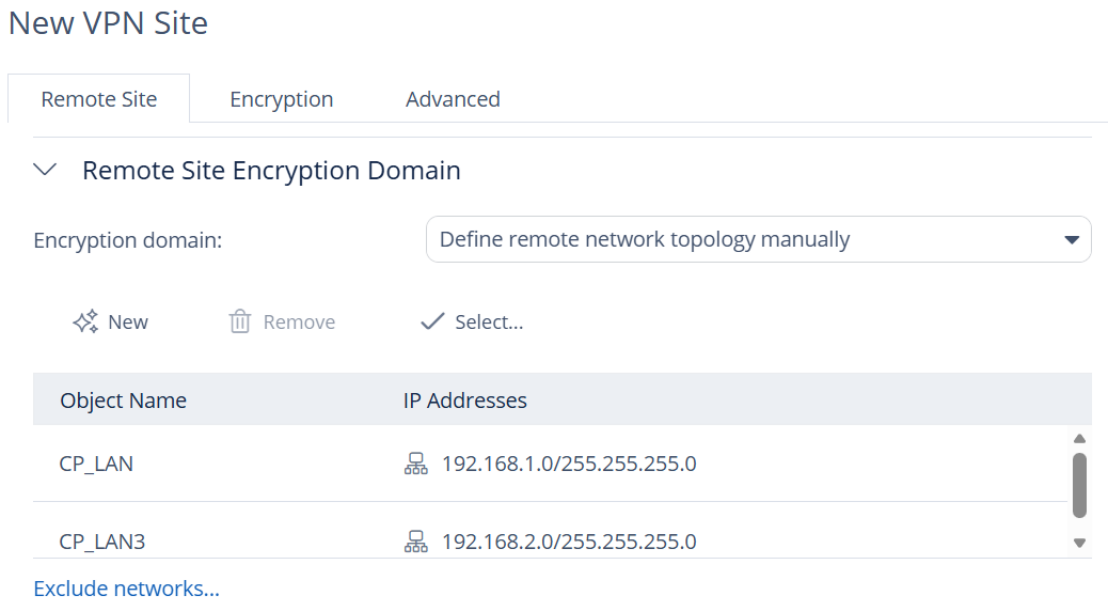
在 Site Name 中，命名此 VPN Site 的名稱。在 IP Address 中輸入對端設備的 IP : 192.168.200.1(此為範例，請貴客戶依需求輸入)，並於 Pre-shared secret 輸入一組兩 VPN Site 相同的共享密鑰 1qaz@WSX(此為範例，請貴客戶依實際狀況輸入)。



在 Remote Site Encryption Domain 下的 Encryption domain 選擇 Define remote network topology manually 並在下方選擇 New 來加入要存取的對端子網段。



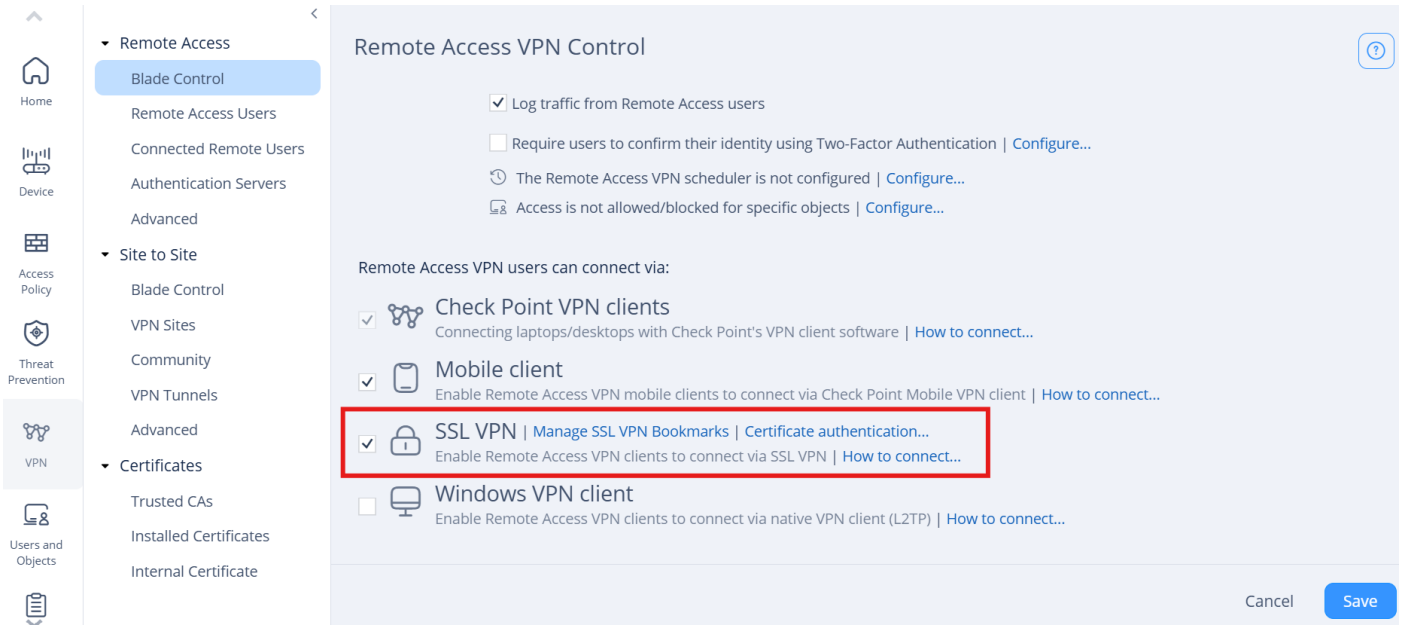
將要存取的對端子網 192.168.1.0/24 及 192.168.2.0/24(此為範例，請貴客戶依實際狀況輸入)新建成為物件，完成後按 Save 繼續。



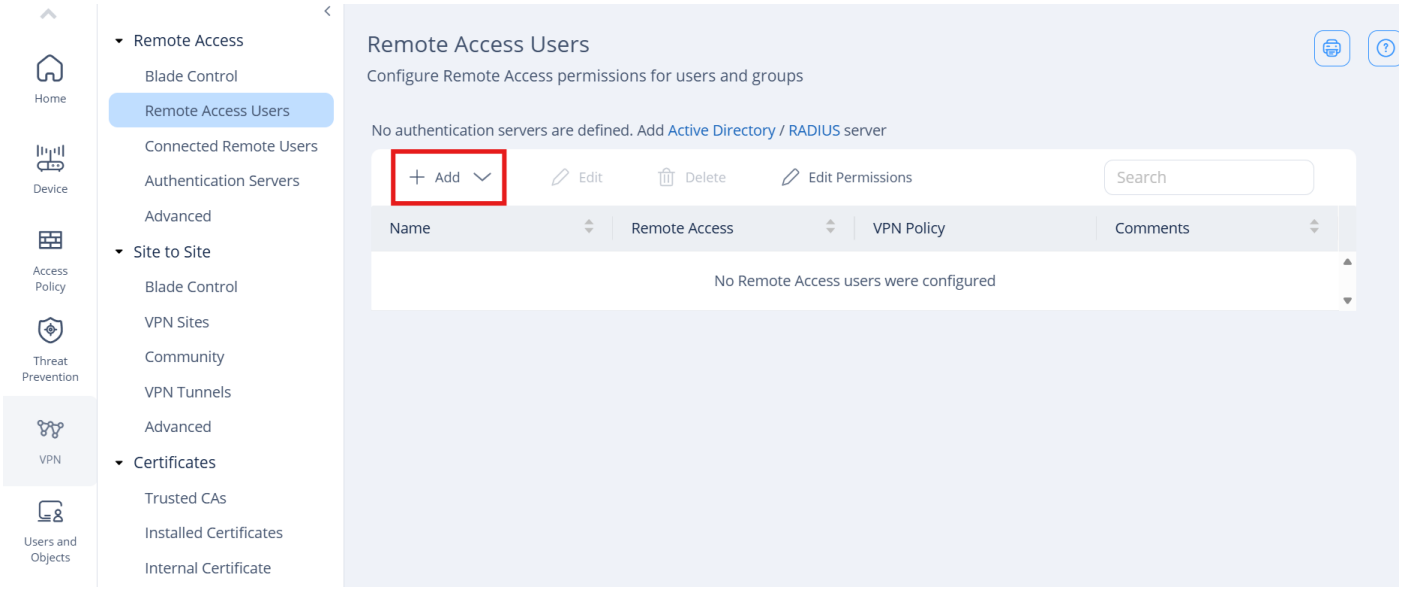
新增後按 Apply 完成。

2. SSL VPN 設定

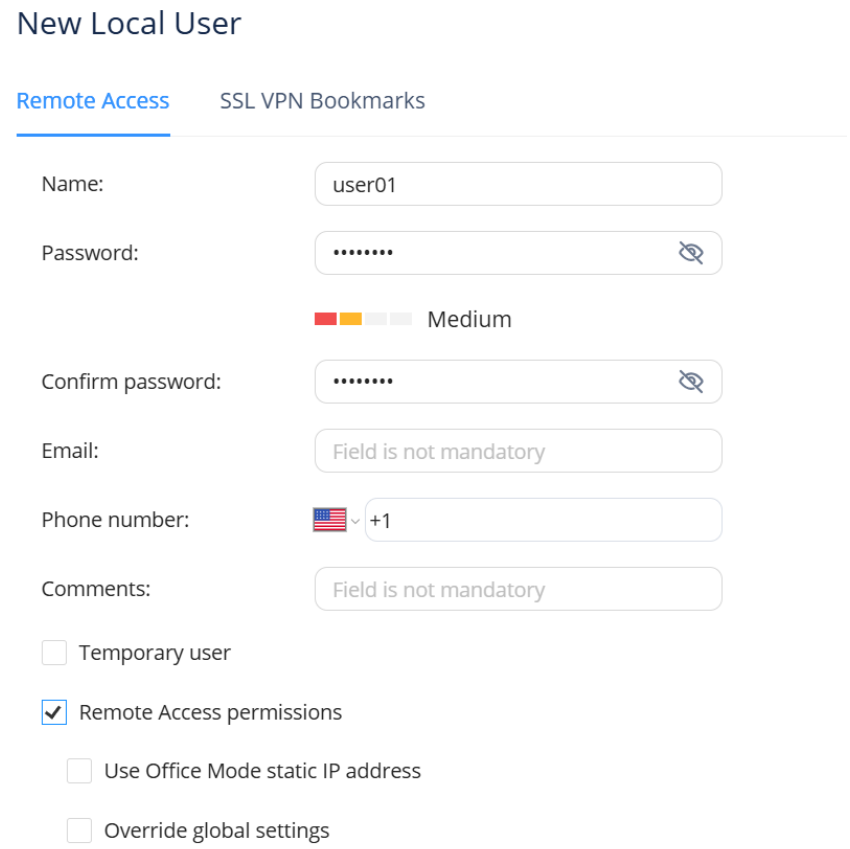
i. SSL-VPN 設定步驟



登入 CheckPoint 防火牆後，於左邊功能欄位點選 VPN，再到 Remote Access > Blade Control 底下，將 Remote Access 功能選擇 On 啟用，再將 VPN Remote Access users can connect via: 底下的 SSL VPN 選項打勾。

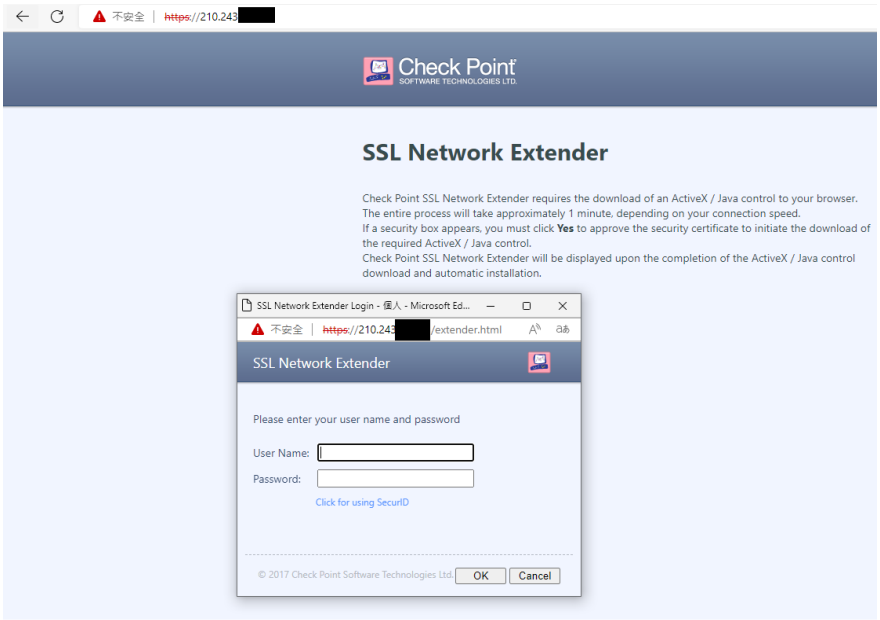


到 Remote Access Users 底下，點選 Add 加入 VPN 的使用者。



輸入要新增的 VPN 使用者帳號密碼，並勾取 Remote Access permissions 完成後按 Apply 結束。

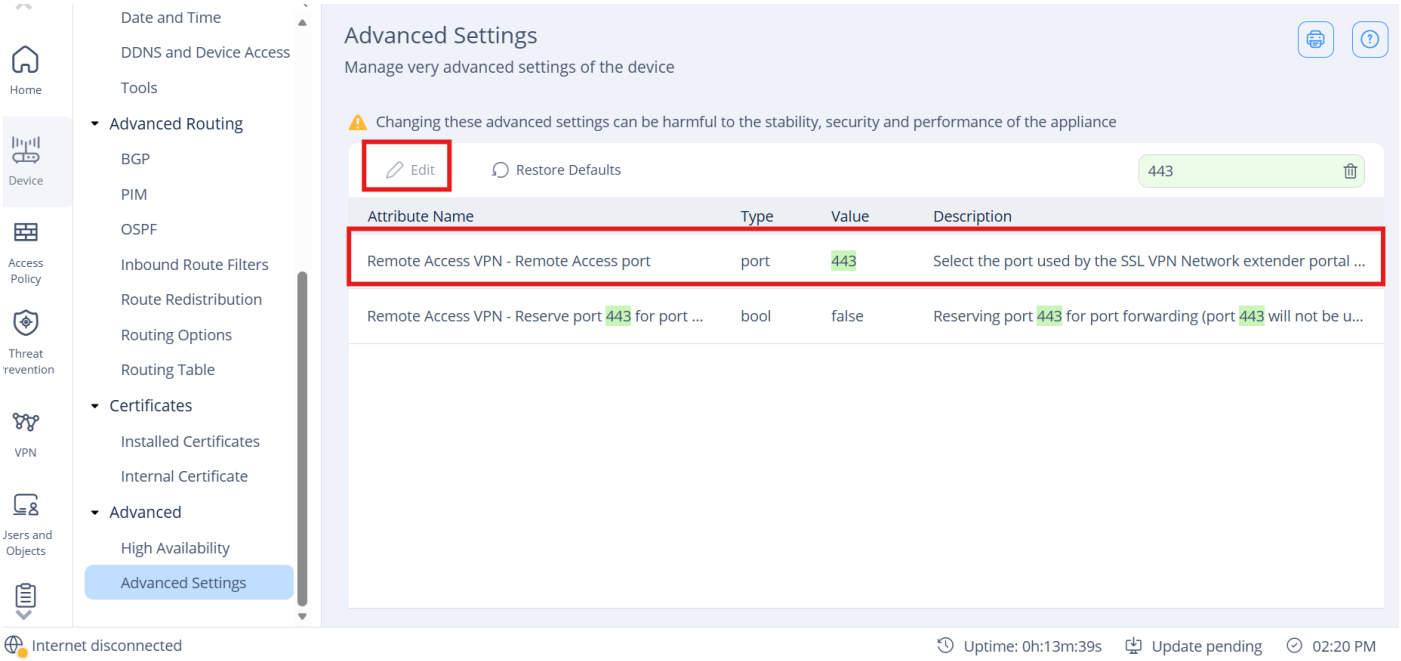
ii. SSL-VPN 用戶端登入



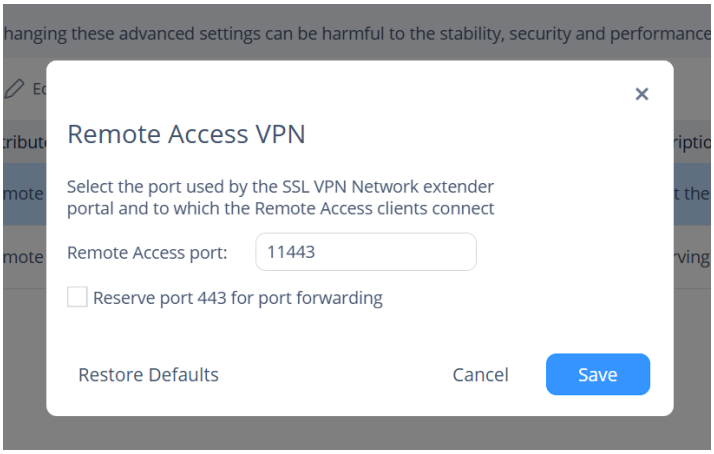
到網頁瀏覽器上，輸入 VPN Site 的 https://(IP 位址)，並在跳出視窗中輸入使用者的 VPN 帳號密碼後按 OK 完成。

*若瀏覽器封鎖跳出視窗，請記得先允許跳出視窗並重整頁面

*若想更改預設的阜號 443，請依以下步驟：



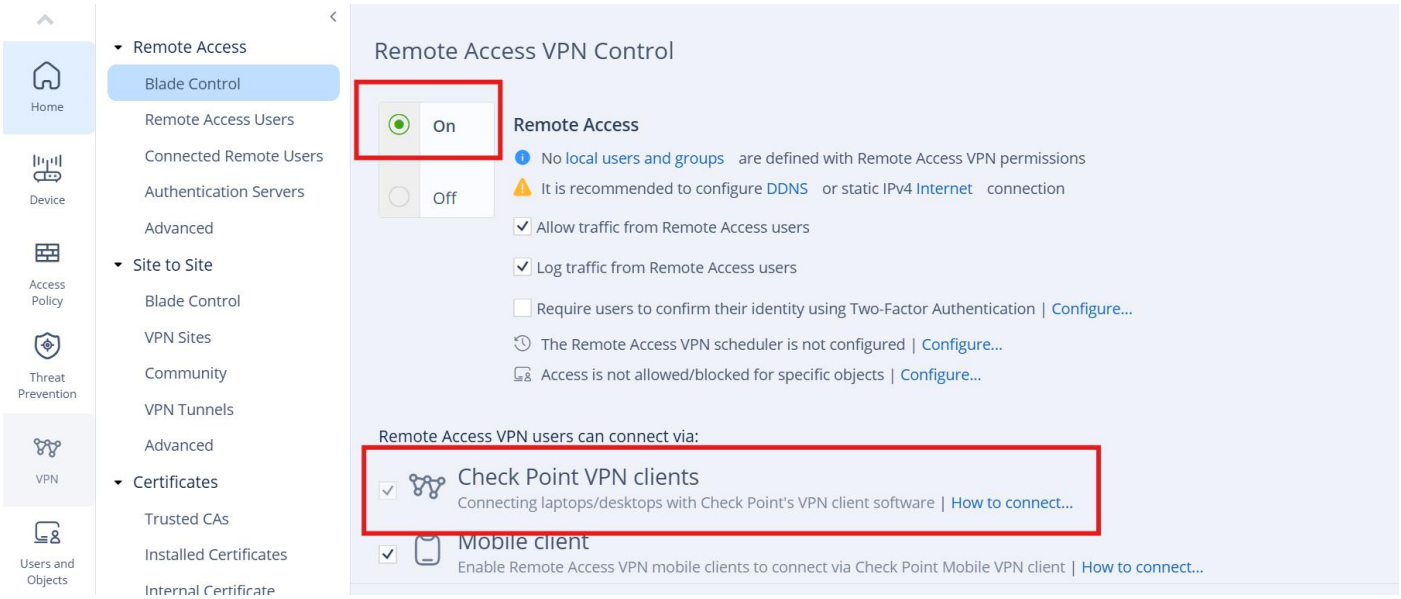
點選左邊功能欄 DEVICE > Advanced Setting，找到 VPN Remote Access – Remote Access port 後點選 Edit。



在 Remote Access Port 中輸入欲更改的阜號，並按 Save 完成。

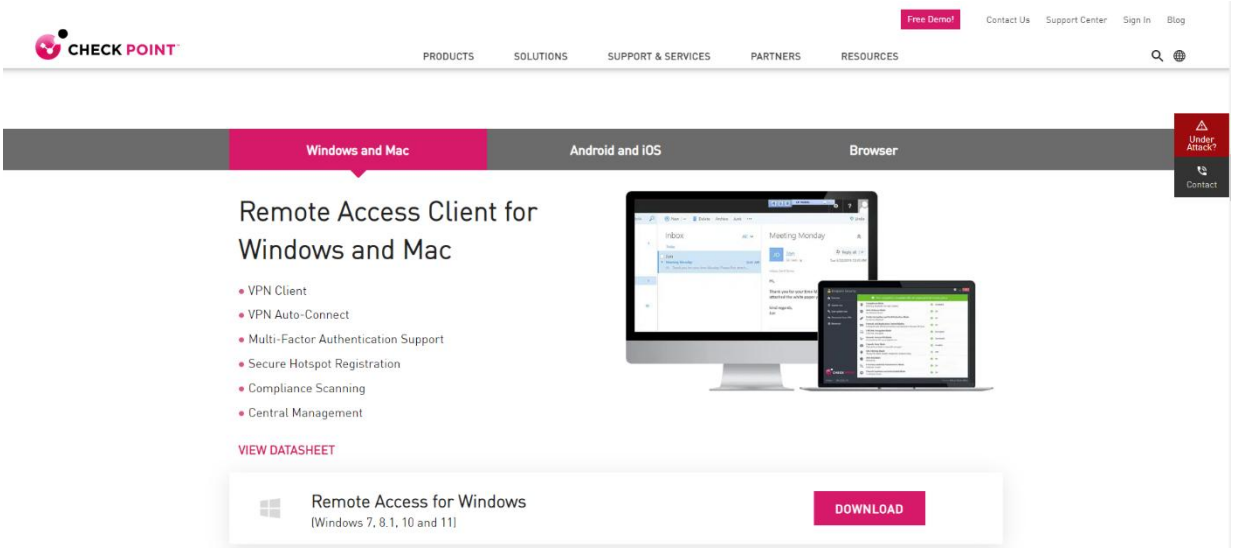
Check Point Remote VPN 設定

i. Check Point VPN 設定

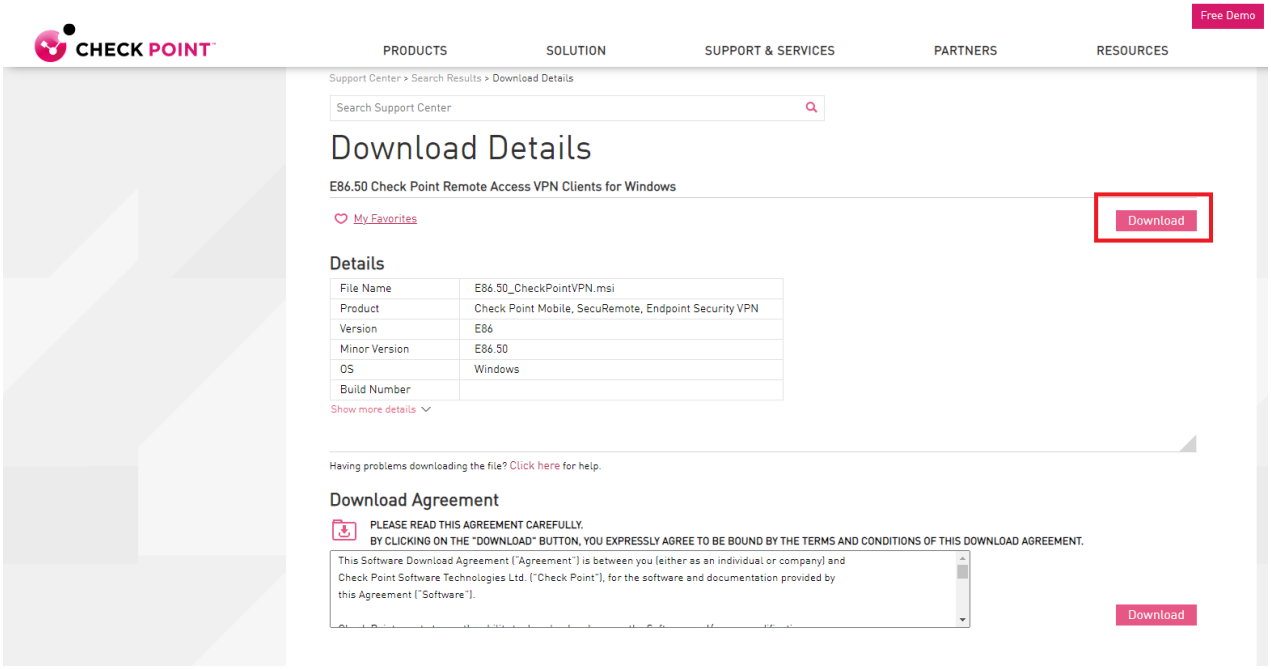


登入 CheckPoint 防火牆後，於左邊功能欄位點選 VPN，再到 Remote Access > Blade Control 底下，將 Remote Access 功能選擇 On 啟用，再將 VPN Remote Access users can connect via: 底下的 Check Point VPN clients 選項打勾。

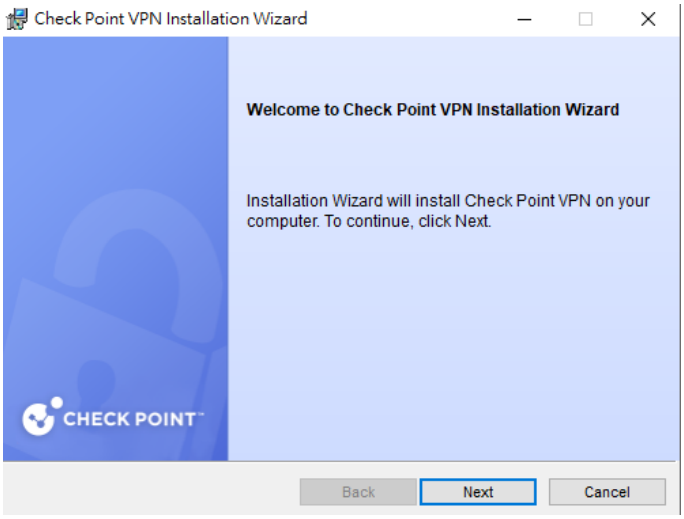
ii. Check Point VPN 客戶端設定



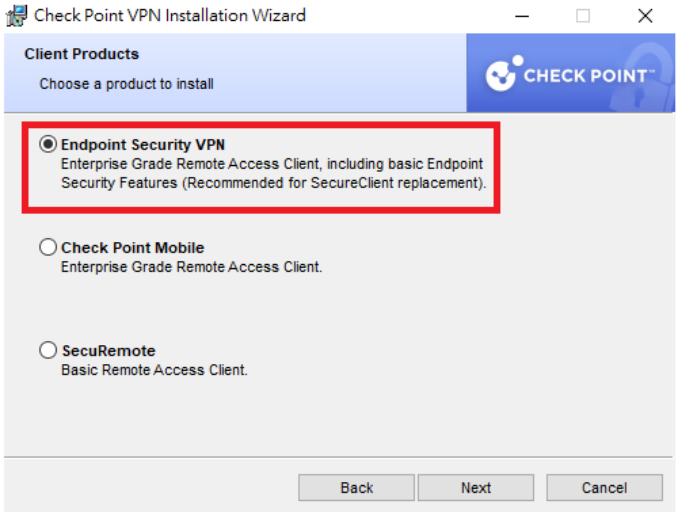
至 https://www.checkpoint.com/quantum/remote-access-vpn/#downloads 找到對應客戶終端裝置系統的下載頁面，點選 DOWNLOAD 進入。



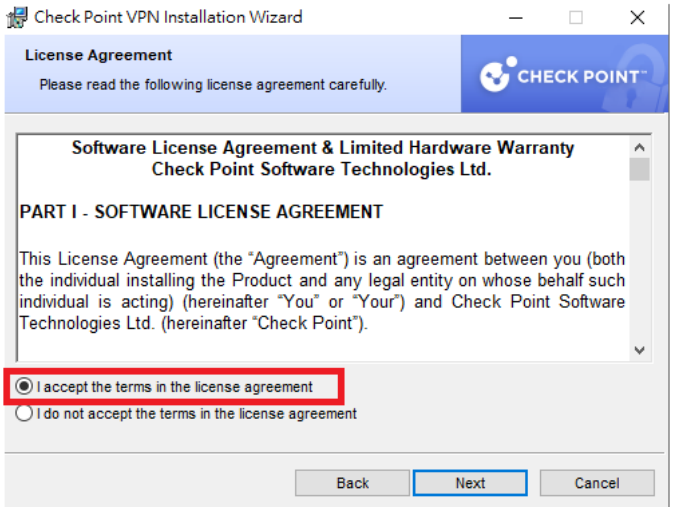
進入頁面後再點取畫面中紅框位置的 Download 下載 Checkpoint Remote VPN 應用程式。



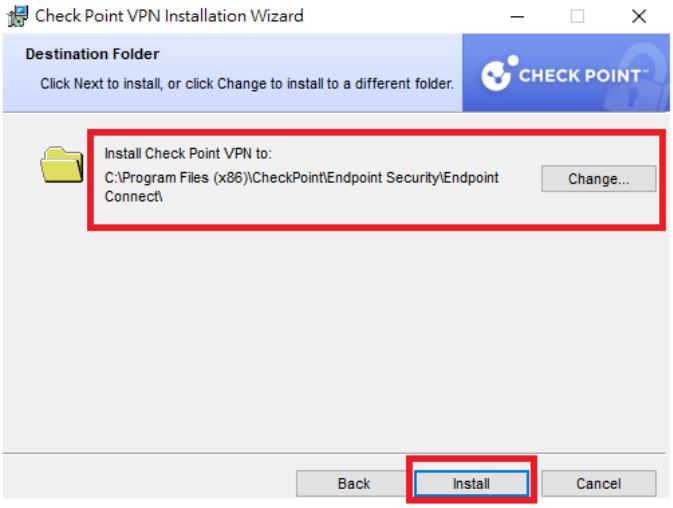
雙擊下載的檔案進入 Check Point VPN Installation Wizard，並點 Next 進入下一步。



選擇 Endpoint Security VPN 並按 Next 下一步。

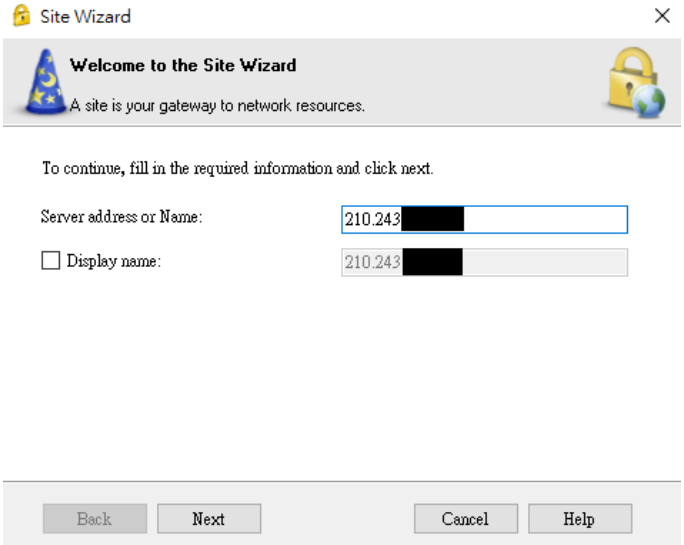


詳讀軟體使用聲明後勾選 I accept the terms in the license agreement 並點 Next 下一步。

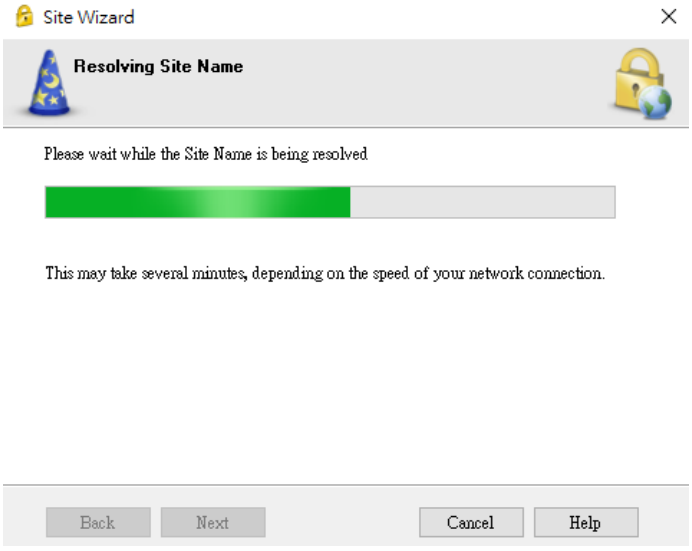


如果需要更換下載目錄，按 Change 更換，如不需要請直接點 Install 下載並等待安裝完成。

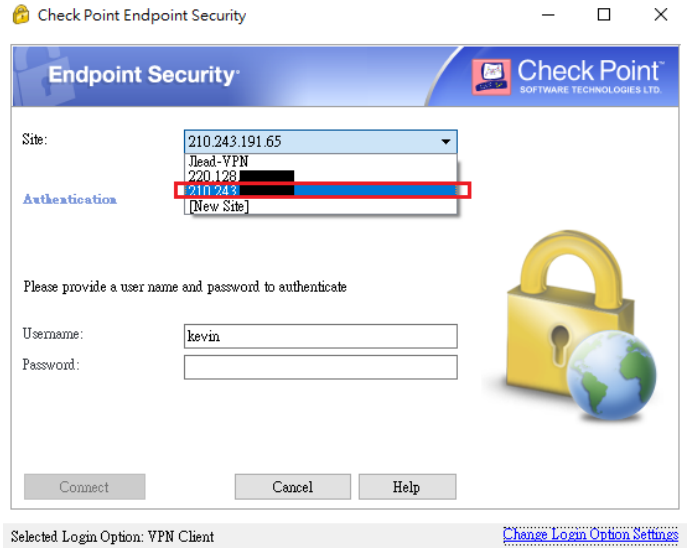
完成後進到 Site Wizard 歡迎介面，點 Next 下一步。



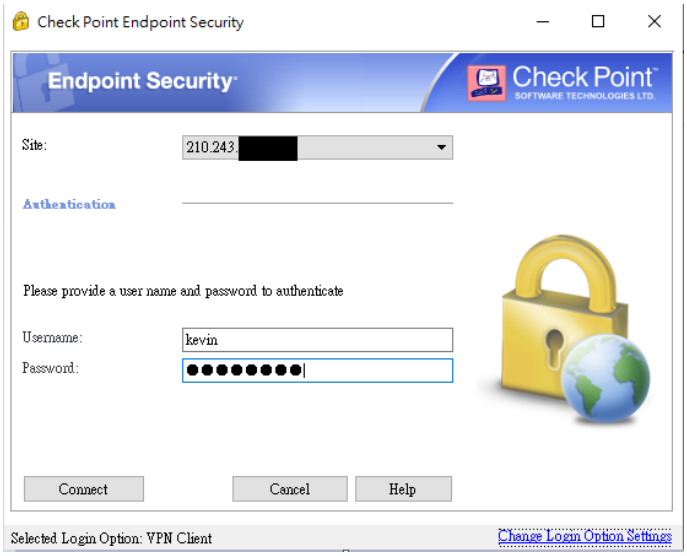
輸入防火牆的對外 IP，並點 Next 進到下一步。



等待設定完成後再點 Next 進到下一步。



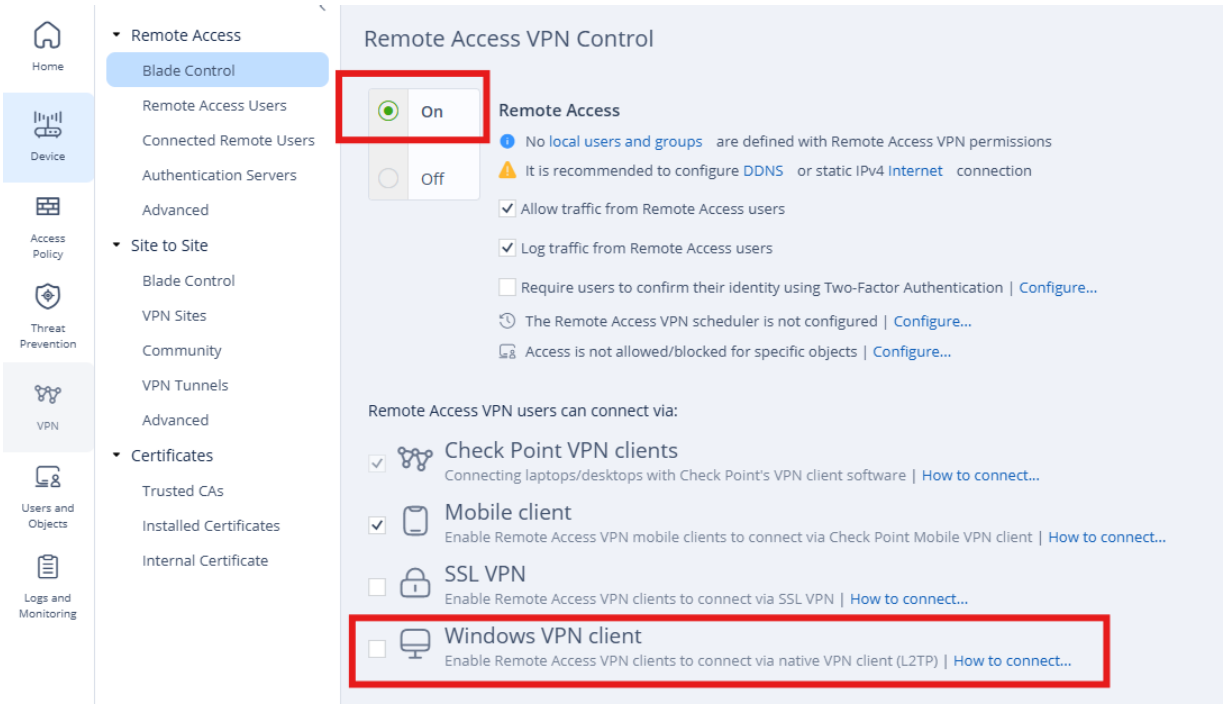
若有創建多個 Site 的 VPN 的話，選擇欲連線的 VPN Site。



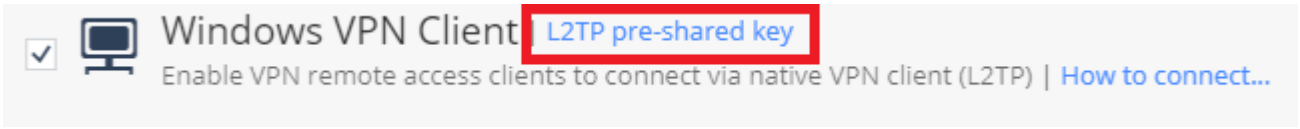
輸入自行設定的 Username 以及 Password，完成後點 Connect 連線。

L2TP VPN 設定

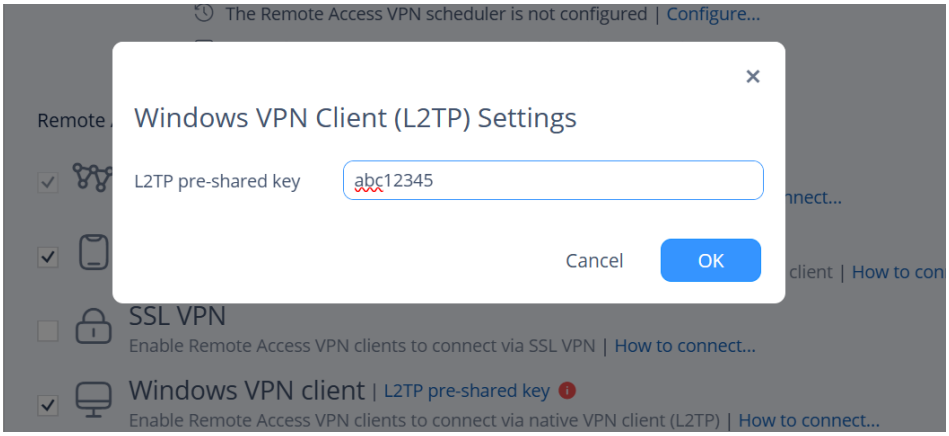
i. L2TP VPN 設定



登入 CheckPoint 防火牆後，於左邊功能欄位點選 VPN，再到 Remote Access > Blade Control 底下，將 Remote Access 功能選擇 On 啟用，再將 VPN Remote Access users can connect via: 底下的 Windows VPN Client 選項打勾。



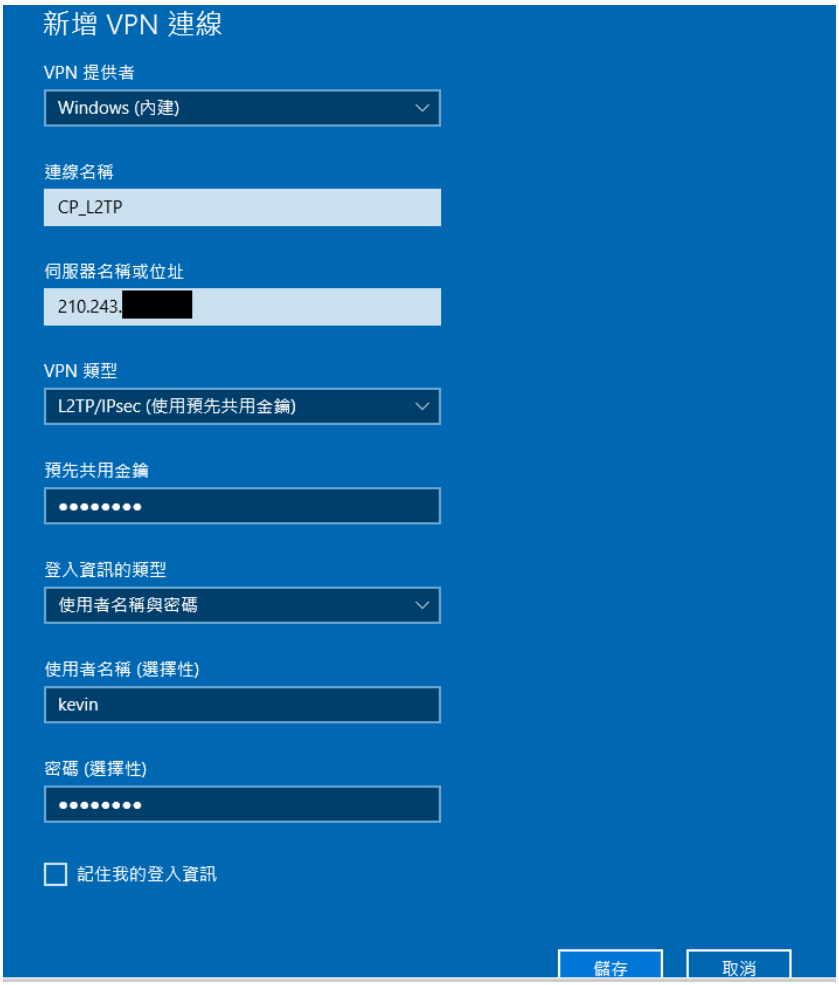
點選 L2TP pre-shared key 進去，設定一組共享密碼。



設定共享密碼 abc12345(此為範例，請貴客戶依實際狀況輸入)，完成後按 OK 結束。

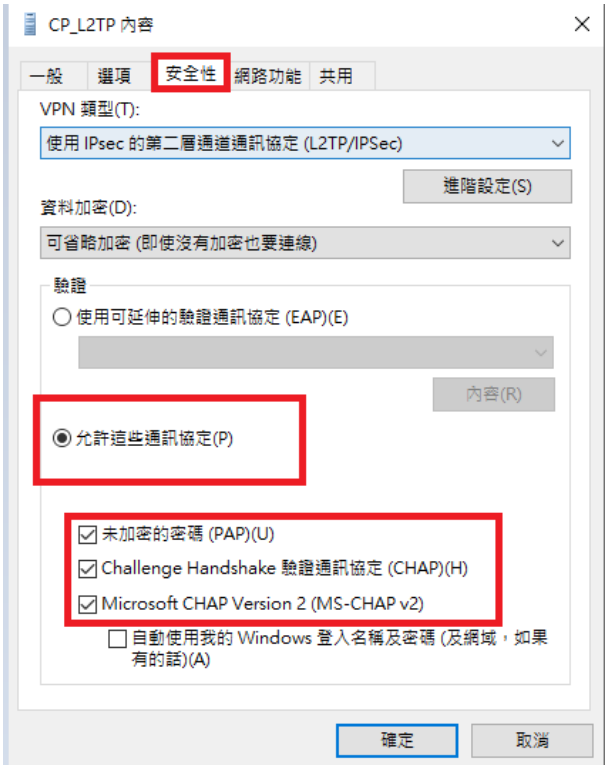
ii. L2TP VPN 客戶端設定

進到 Windows 的 VPN 中，點選新增 VPN 連線。

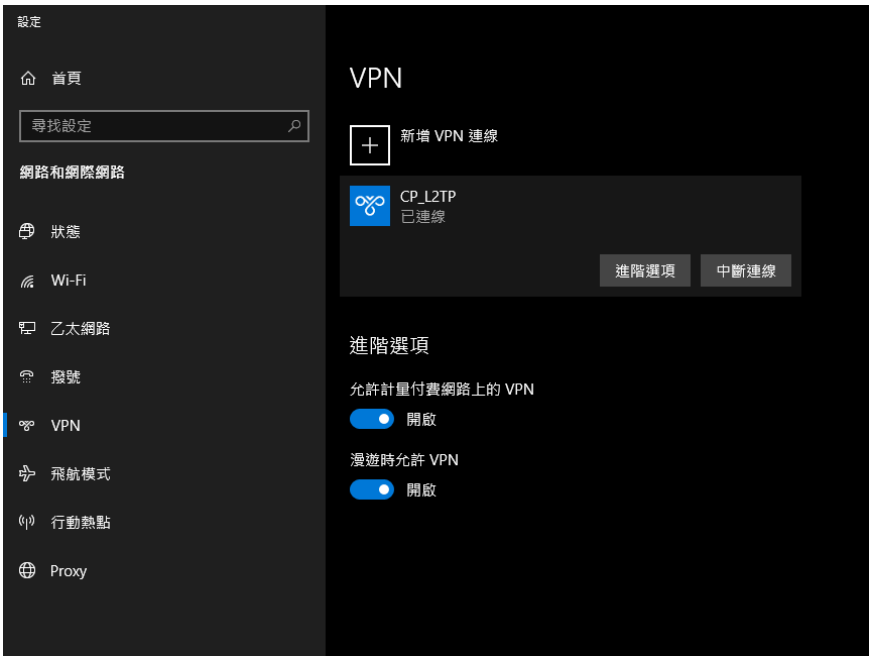


輸入 VPN Site 連線名稱、IP 位址、防火牆上設定的共用金鑰: abc12345(此為範例，請貴客戶依實際狀況輸入)、使用者名稱及密碼，並將 VPN 類型選擇 L2TP/IPsec(使用預先共用金鑰)，設定完後按儲存。

點選右邊變更介面卡選項。



到安全性，勾選允許這些通訊協定，並將底下未加密的密碼(PAP)(U)、Challenge Handshake 驗證通訊協定(CHAP)(H)、Microsoft CHAP Version2(MS-CHAP v2)的選項打勾後按確定。



回到 VPN 中，點選連線後顯示已連線代表已成功建立 L2TP VPN。

第六章 網路頻寬管理

1. 頻寬管理 (貴客戶可應用於網路語音/視訊會議/限制使用者流量及連線數)

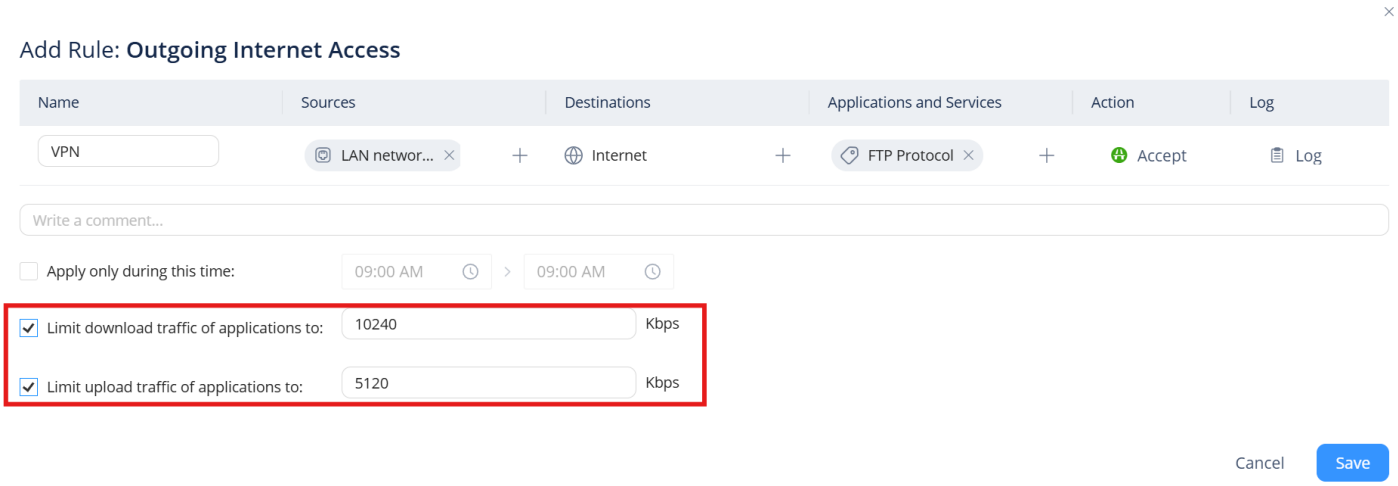
i. 依政策作頻寬管理

本範例以限制 VPN 流量對內部網路的 FTP 傳輸限制下載 10Mbps /上傳 5Mbps。

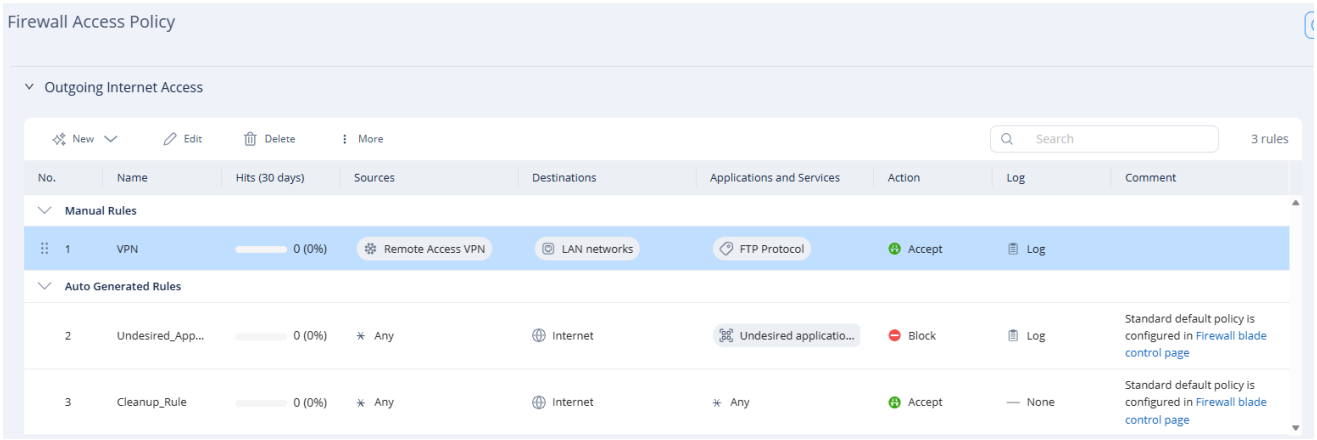
單位以 1Mbps = 1024Kbps 做計算

計算後下載流量為：10,240 kbps

計算後上傳流量為：5,120 kbps



到 ACCESS POLICY > Policy，點選 New 來新建一條具有 Rate Limiting 的規則，將 Limit download traffic of application to 及 Limit upload traffic of applications to 打勾，並在 Limit download traffic of application to 後的空格輸入 10240、於 Limit upload traffic of application to 後的空格輸入 5120，完成後點選 Apply。



完成後如上圖。

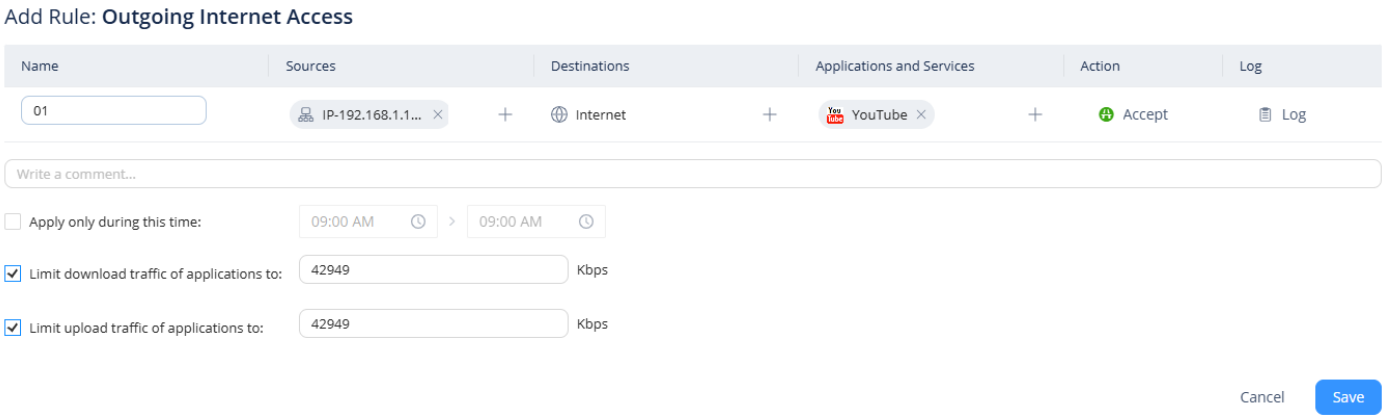
ii. 依 IP (per-ip) 作頻寬管理

本範例以限制內部特定 IP: 192.168.1.125 上 Youtube 的流量限制下載 5MBps /上傳 5MBps。

單位以 1Mbps = 1024Kbps 做計算

計算後下載流量約為：42,949 kbps

計算後上傳流量為：42,949 kbps

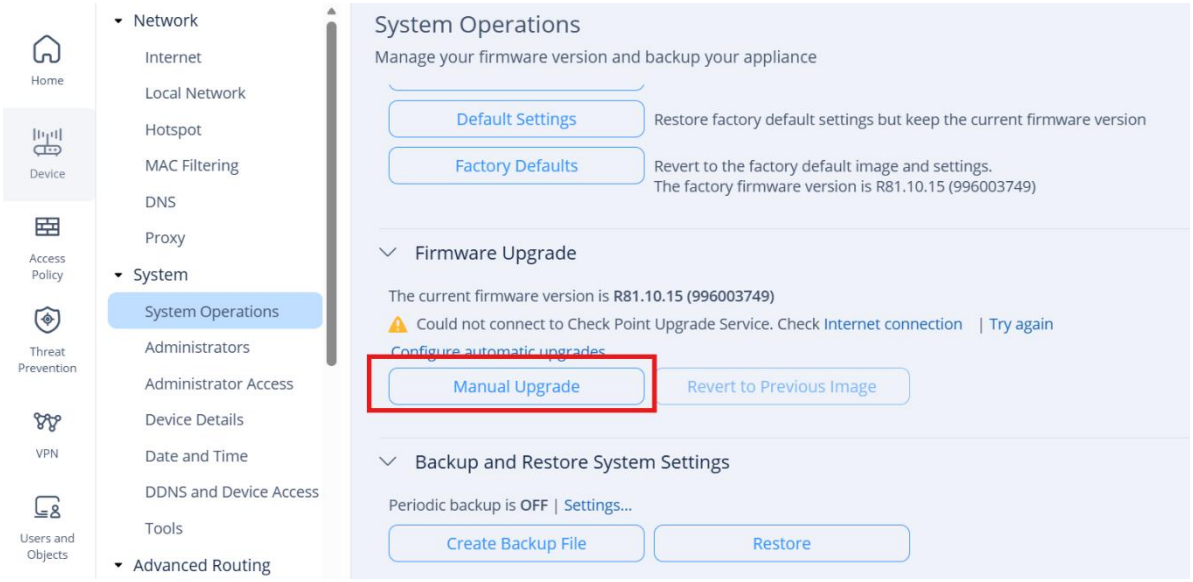


到 ACCESS POLICY > Policy，點選 New 來新建一條具有 Rate Limiting 的規則，點選 Source 輸入 192.168.1.125，再點選 Application/Service 輸入 Youtube 並選擇該物件，然後將 Limit download traffic of application to 及 Limit upload traffic of applications to 打勾，並在 Limit download traffic of application to 後的空格輸入 42949、於 Limit upload traffic of application to 後的空格輸入 42949，完成後點選 Apply。

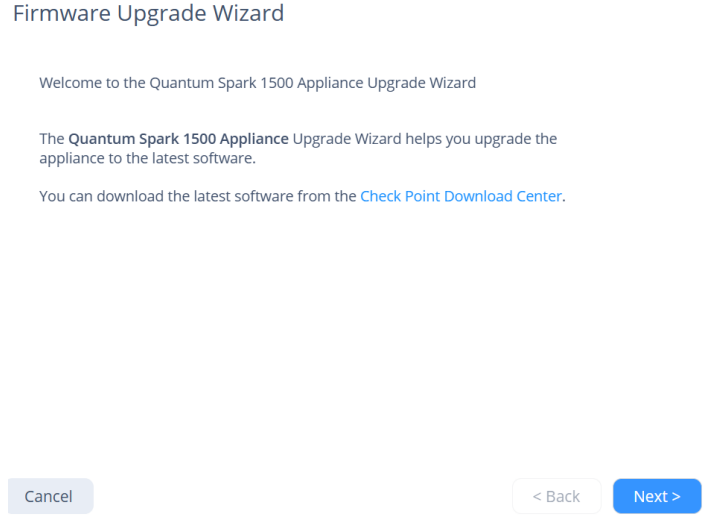
第七章 系統備份設定

1. 更新系統韌體

開啟瀏覽器，輸入 https://ip address:4434，登入 Quantum Spark 2530 首頁

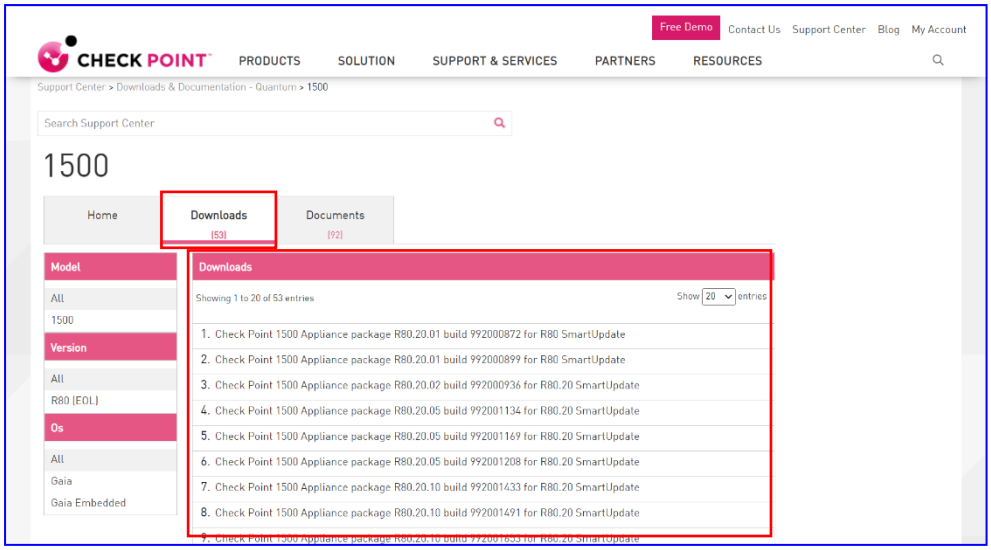


點選 DEVICE → Manual Upgarde

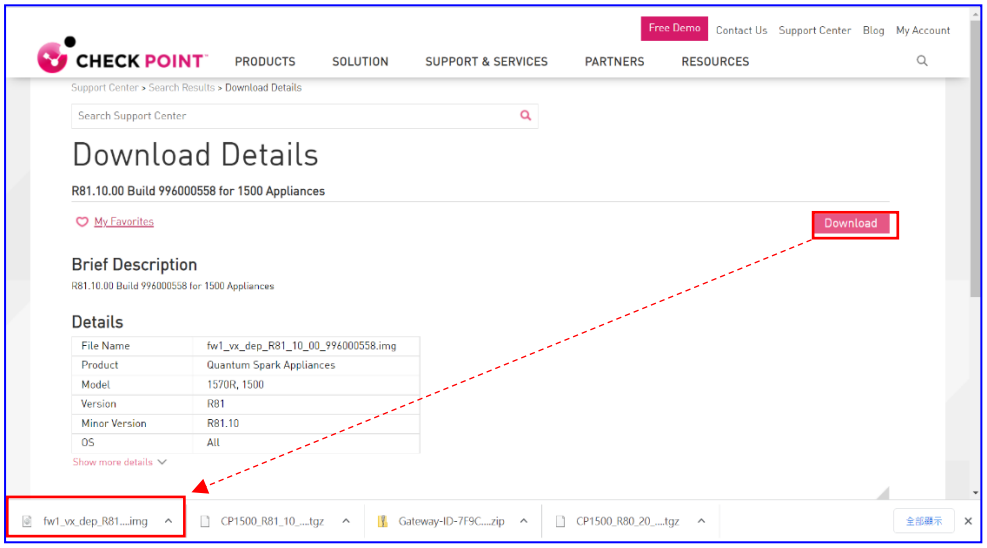


點選 Check Point Download Center

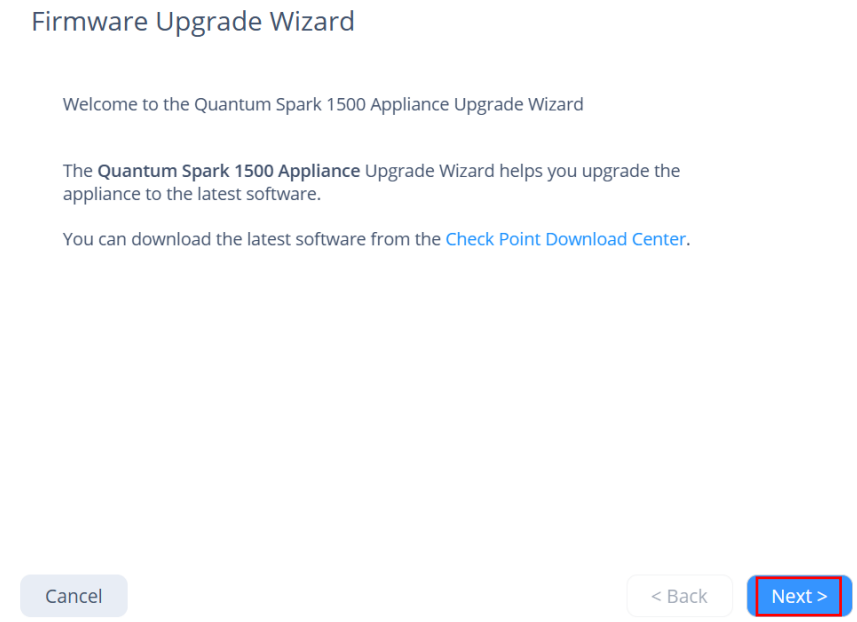
選擇韌體版本



點擊 Download，等待下載完成

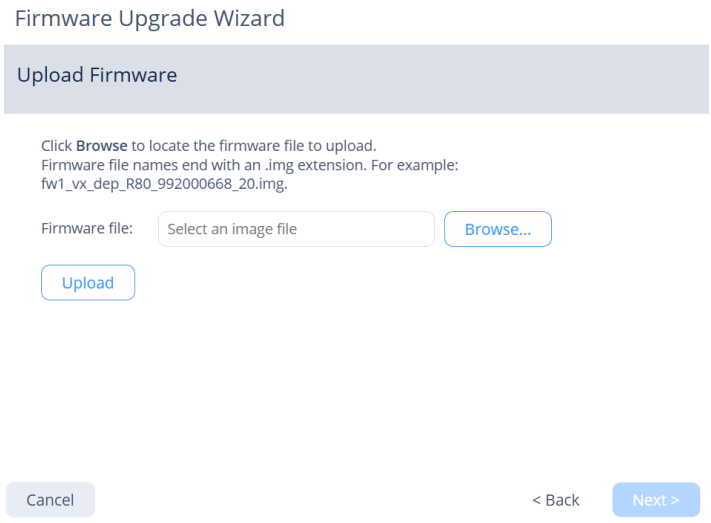


點選 Next

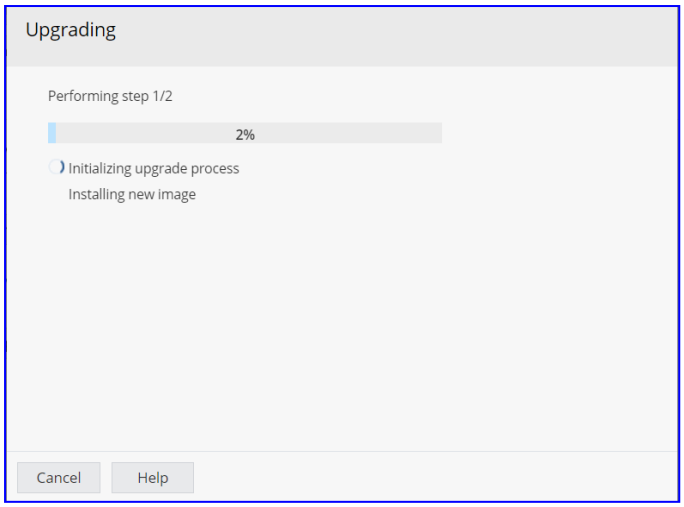


點選 Browe，載入欲更新韌體 → Upload → Upload finished → Next

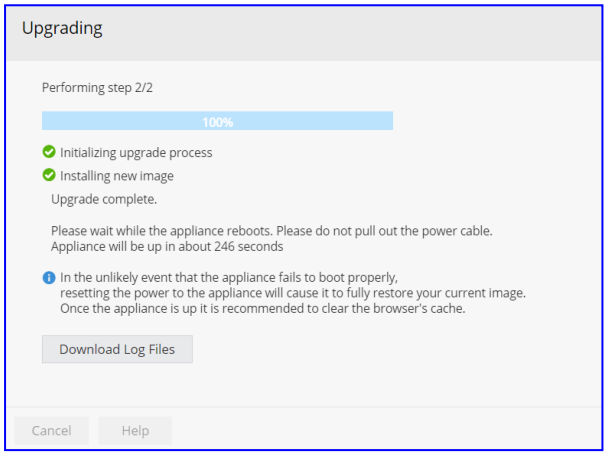
確認版本資訊無誤後點選 Next

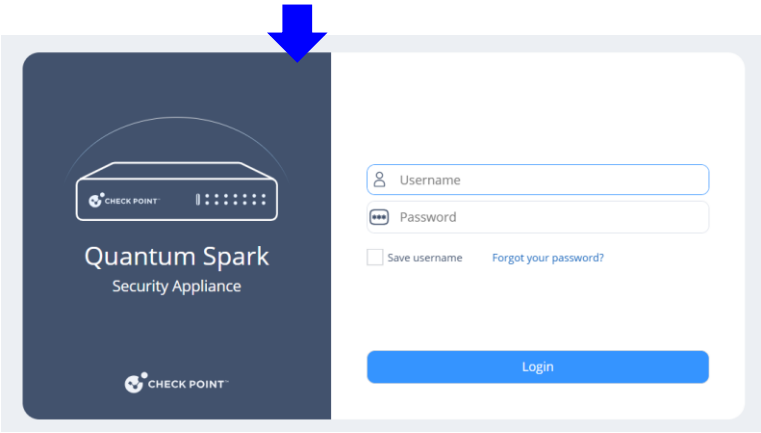


等待更新（約 3 分鐘）



更新完成後，需等待 300 秒，系統自動重啟返回登入頁面 → 輸入帳號密碼



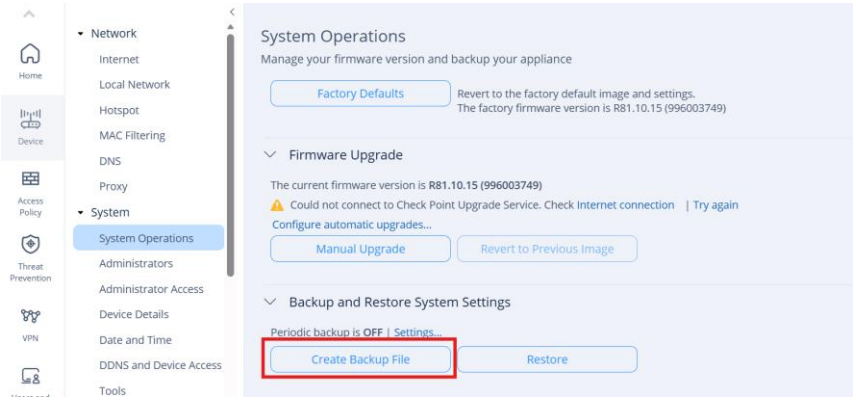


登入 Quantum Spark 2530 首頁，確認設備版本正確，完成

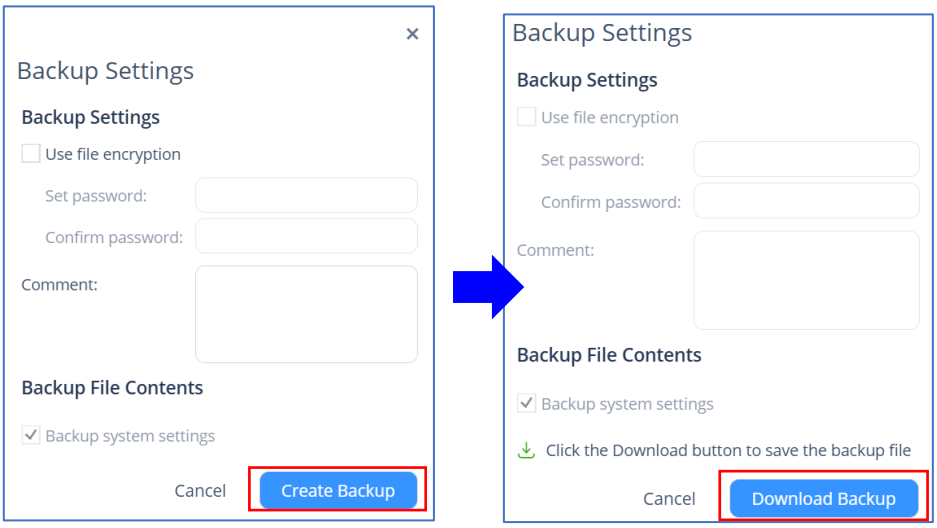
2. 設定檔備份及上傳

i. 手動設定檔備份

開啟 Quantum Spark 2530 GUI → DEVICE → System → System Operations → Backup and Restore System Settings → Create Backup File

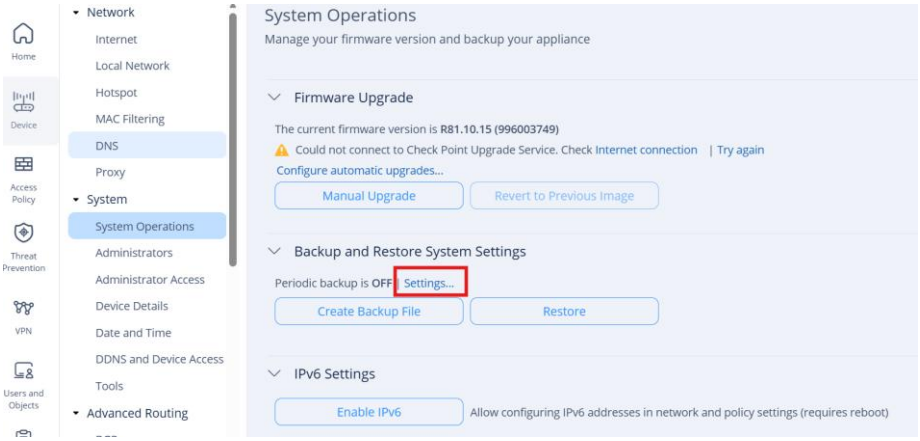


2-1-2 Create Backup → Download Backup → Finished



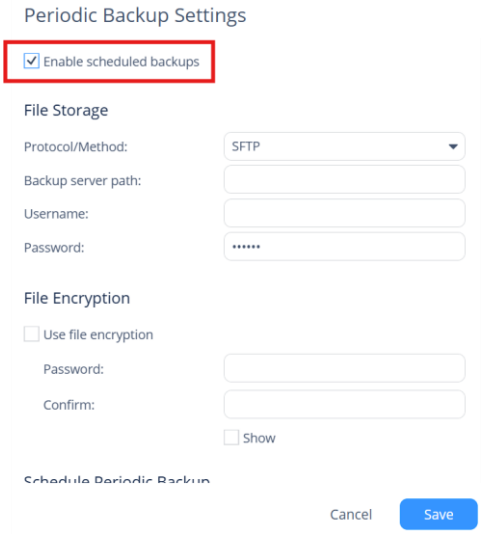
ii. 排程設定檔備份

開啟 Quantum Spark 2530 GUI → DEVICE → System → System Operations → Backup and Restore System Settings → Settings



Enable scheduled backups，依照下列步驟進行，如下圖所示

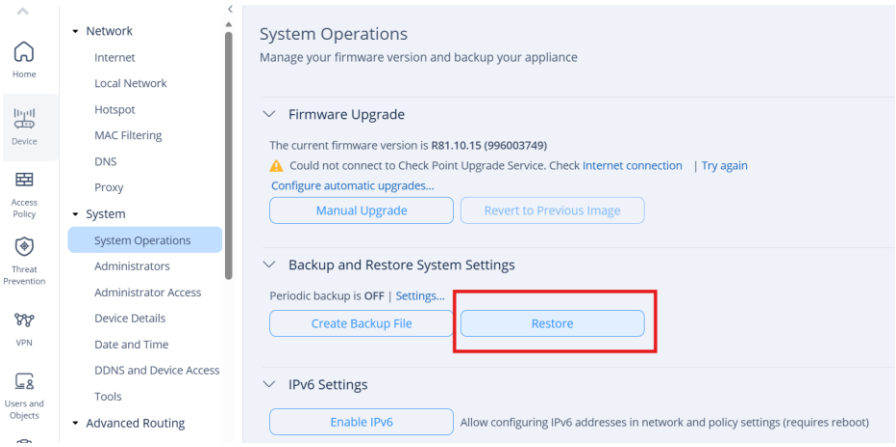
File Storage，輸入備份路徑（Backup server path）、Username and password（Quantum Spark 2530 登入帳號密碼）



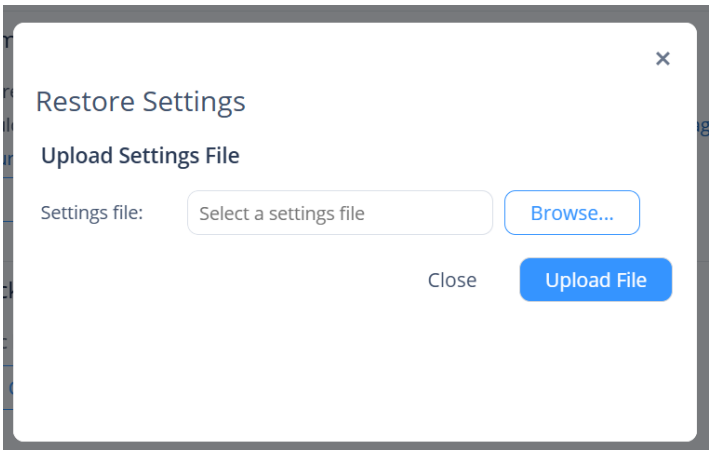
Schedule Periodic Backup，依照需求選擇排程備份時間 → Save

iii. 上傳/還原設定檔

開啟 Quantum Spark 2530 GUI → DEVICE → System → System Operations → Backup and Restore System Settings → Restore



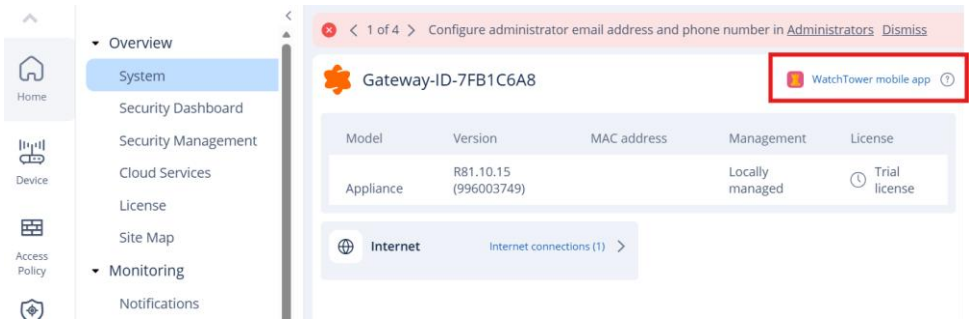
點選 Browse → 選擇欲還原的設定備份檔 → Upload File → Restore → OK（確認是否還原） REBOOTING（等待 260 秒）→ OK（SESSION TIMEOUT）→ OK（SESSION TIMEOUT）→REBOOTING（等待 81 秒）→ Quantum Spark 2530 GUI → 登入 → 完成



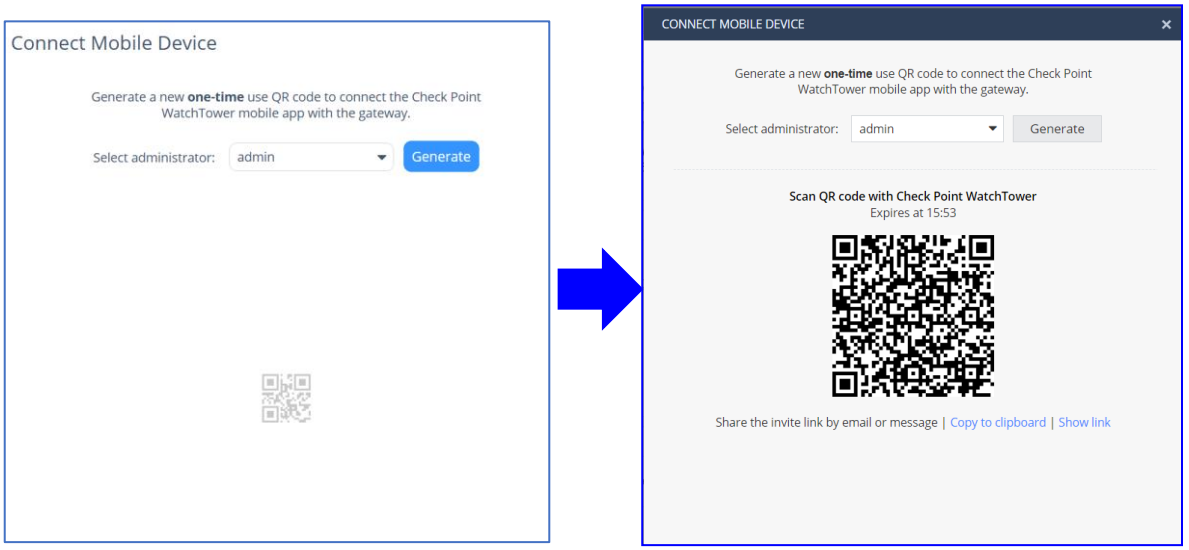
第八章 遠端管理防火牆設定

1. 手機 APP 管理平台

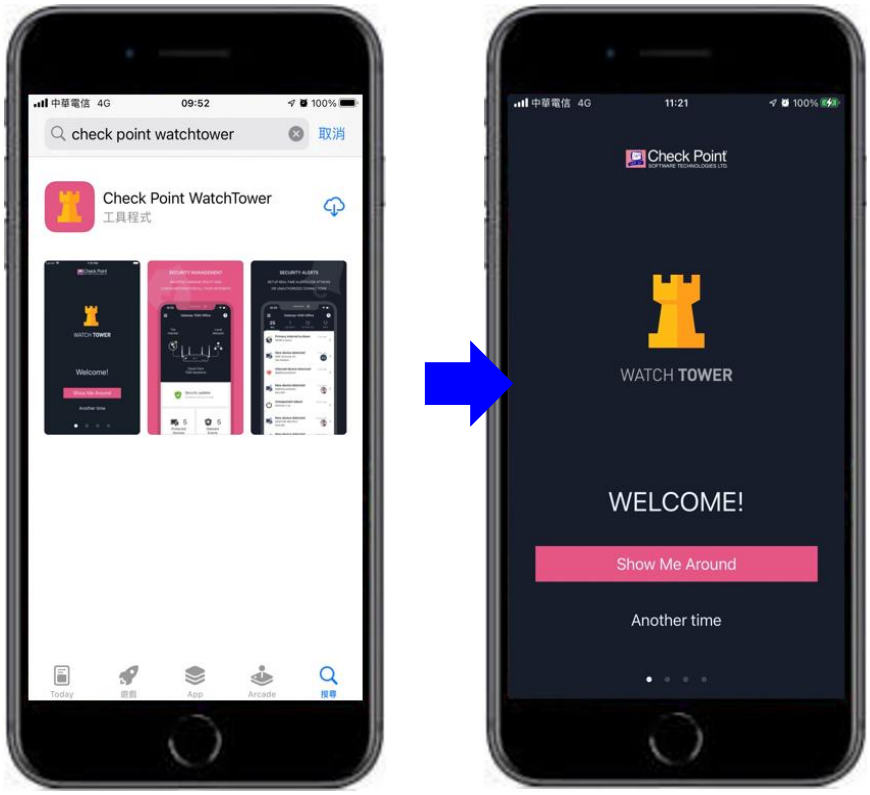
開啟 Quantum Spark 2530 GUI → HOME → System → PAIR YOUR MOBILE DEVICE



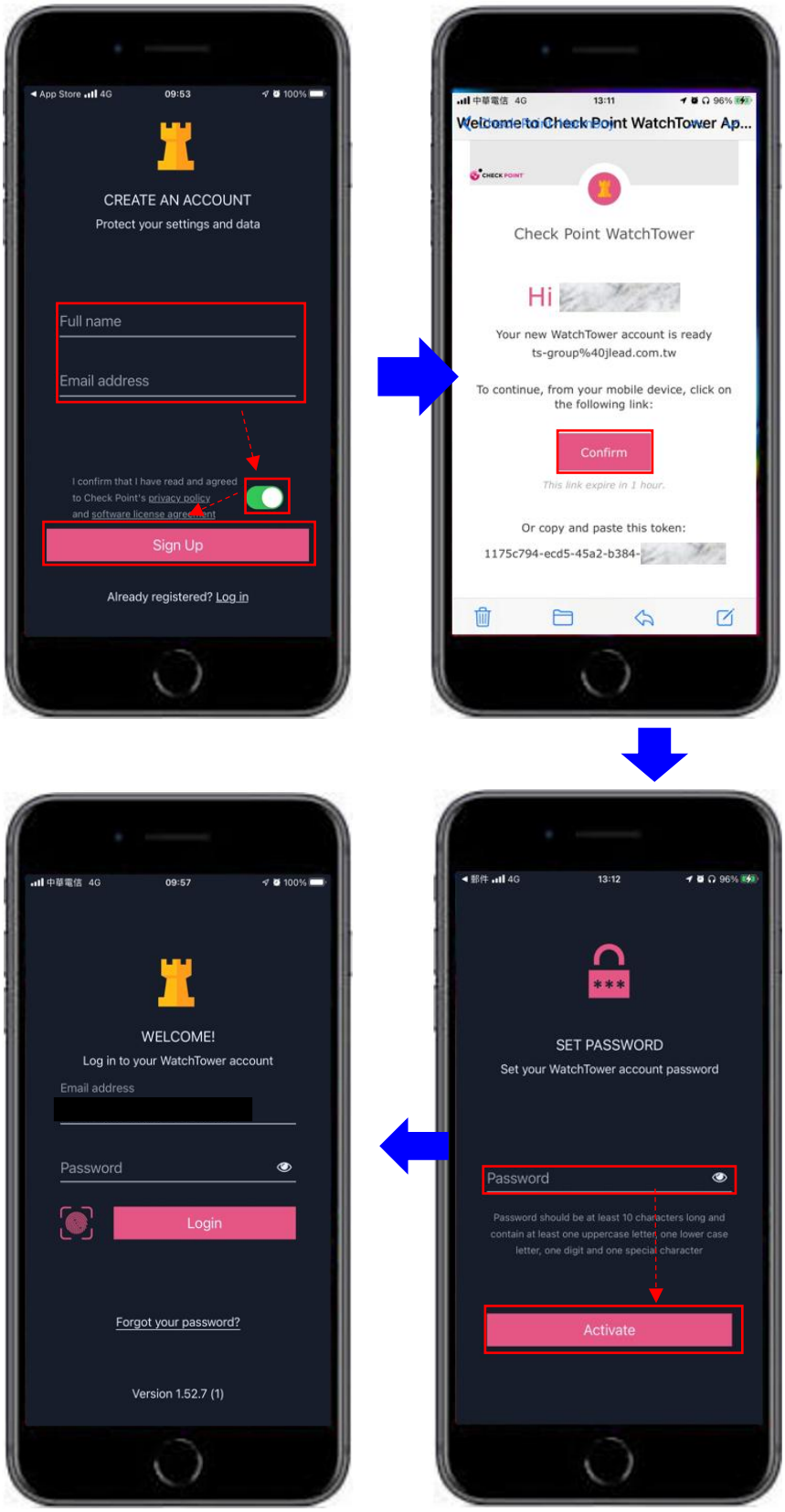
Generate → Yes (確認允許與行動裝置連接) → 等待產生 QR Code



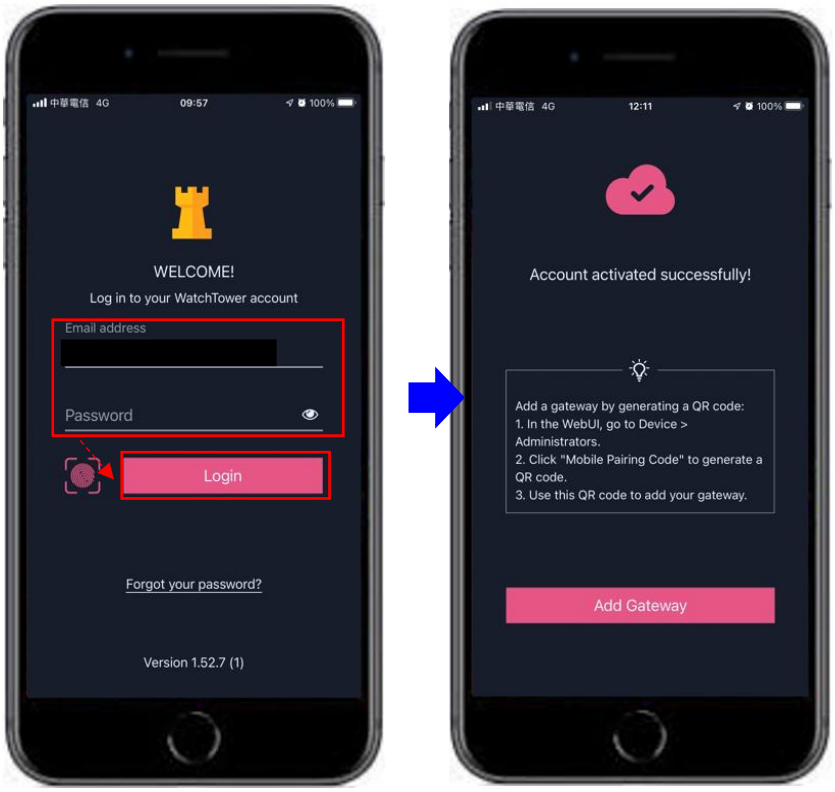
使用行動裝置下載 Check Point WatchTower (iOS App Store / Android Google Play) → 開啟 Check Point WatchTower 工具程式 → Another time



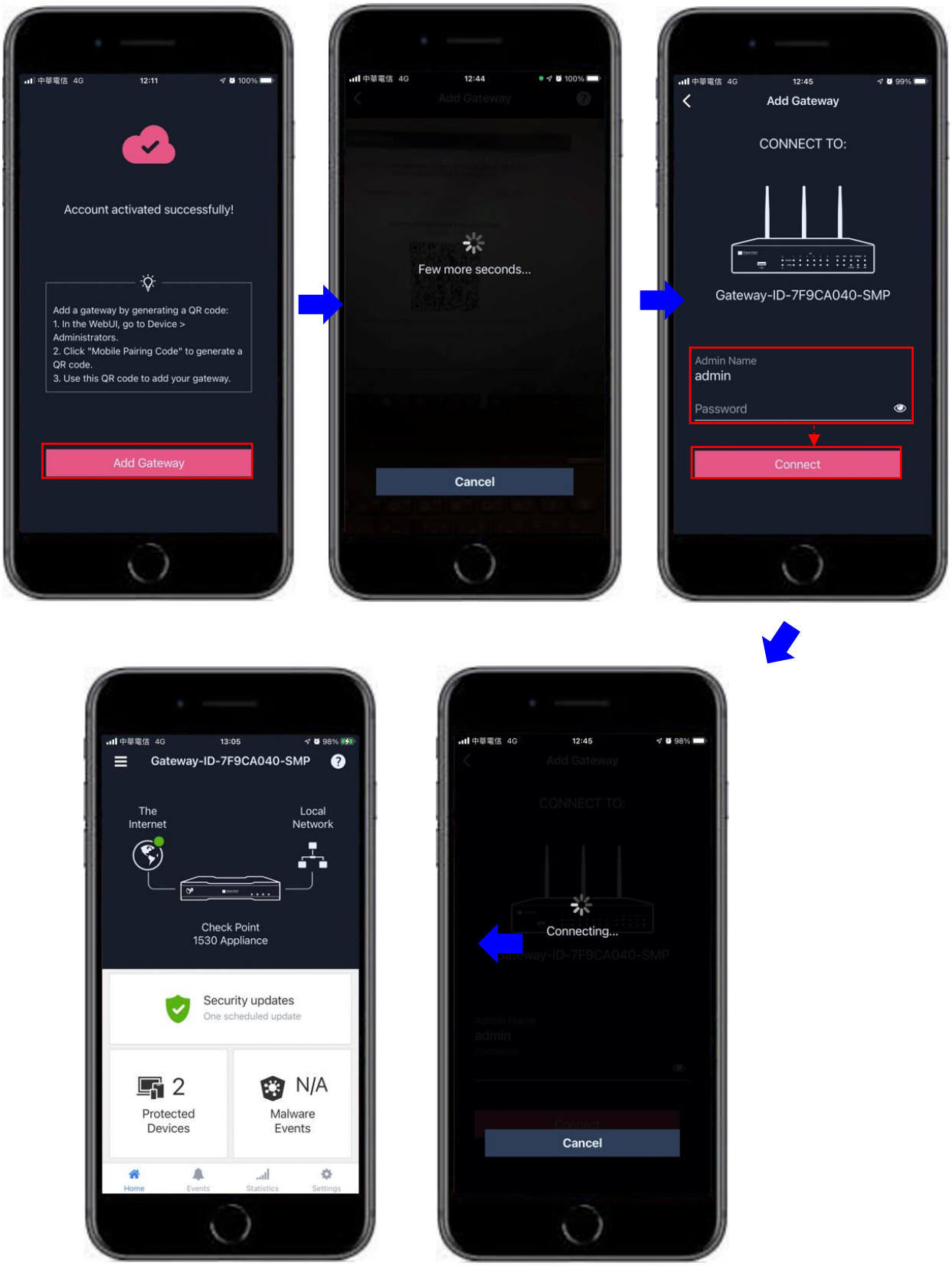
首次登入請建立帳戶，帳號名稱 → 郵件信箱 → 開啟 privacy policy（預設關閉）→ Sign Up → 請至郵件信箱收取驗證信件（請使用行動裝置開啟驗證郵件） → Confirm → 啟用帳號 → 設定密碼 → Activate（完成）



開啟並登入 Check Point WatchTower App



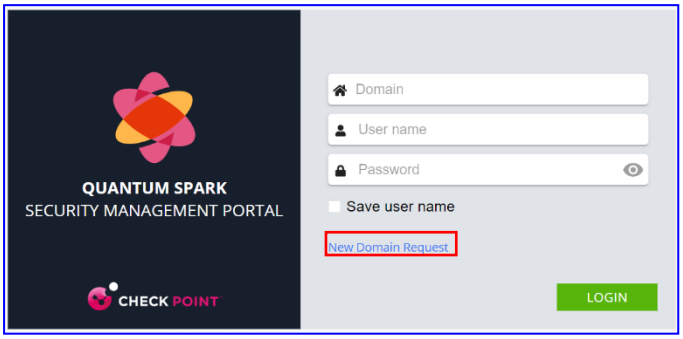
點擊 Add Gateway → 掃描欲加入的 Check Point Quantum Spark 2530 QR Code (1.2 產生的 QR Code) → 輸入 Check Point Quantum Spark 2530 登入帳號密碼 → Connect → Finished



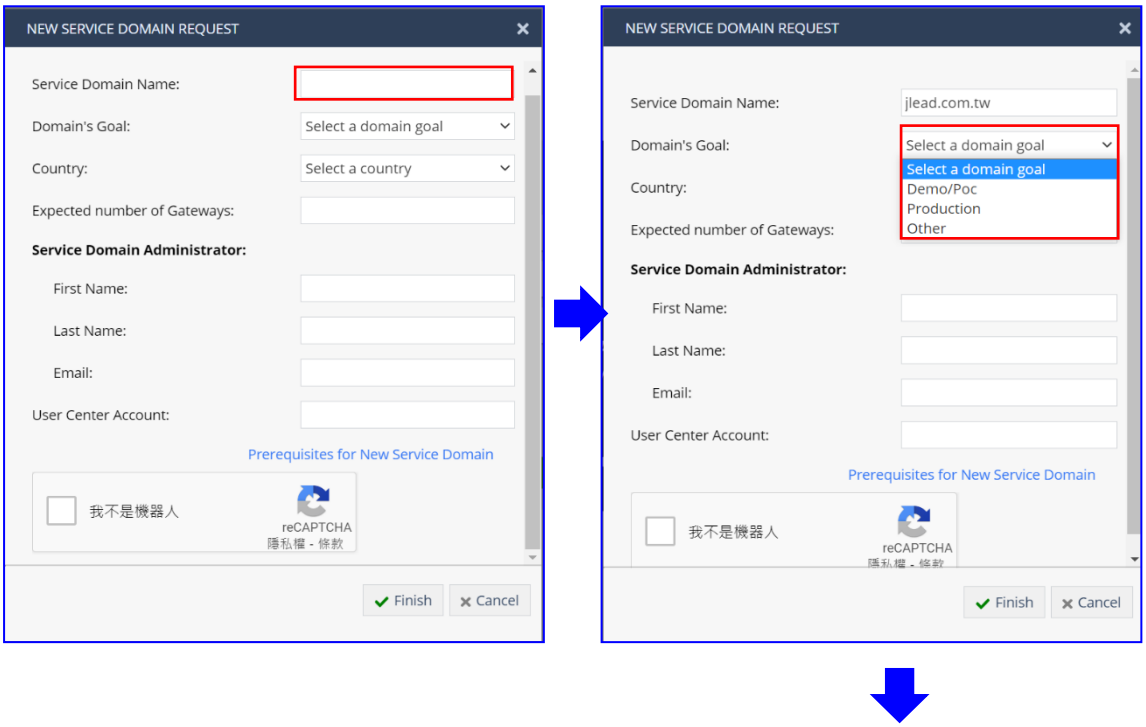
2. SMP Portal 雲端管理平台

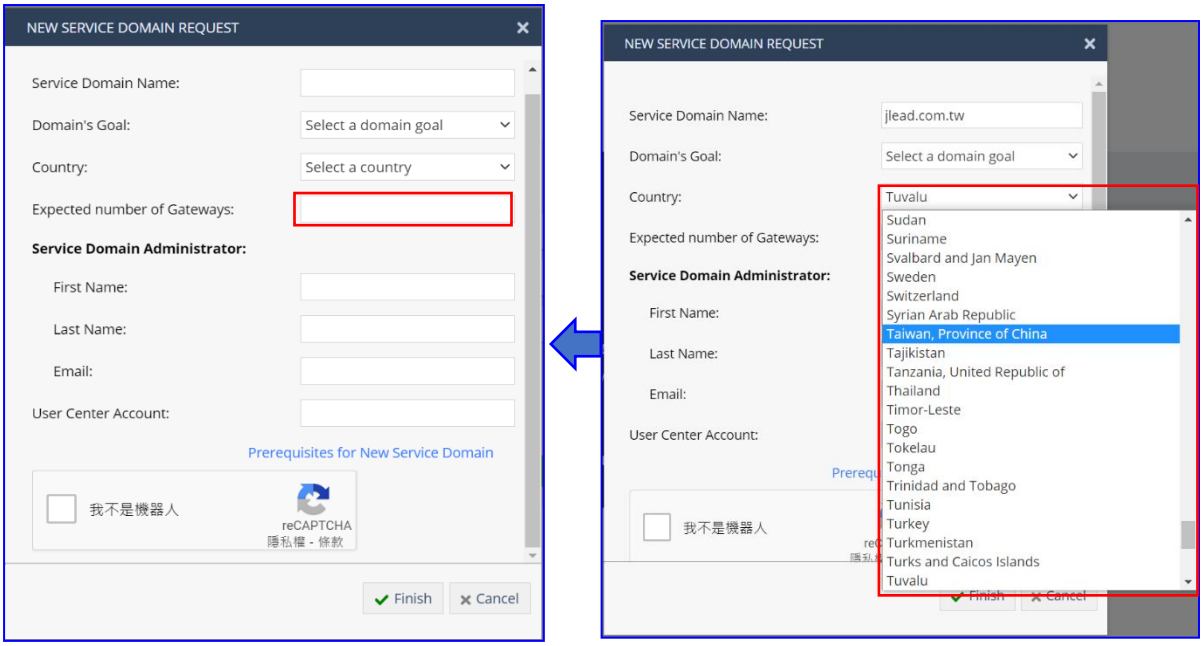
註冊 SMP（Security Management Portal）

開啟瀏覽器 → https://smp1.portal.checkpoint.com/ → New Domain Request

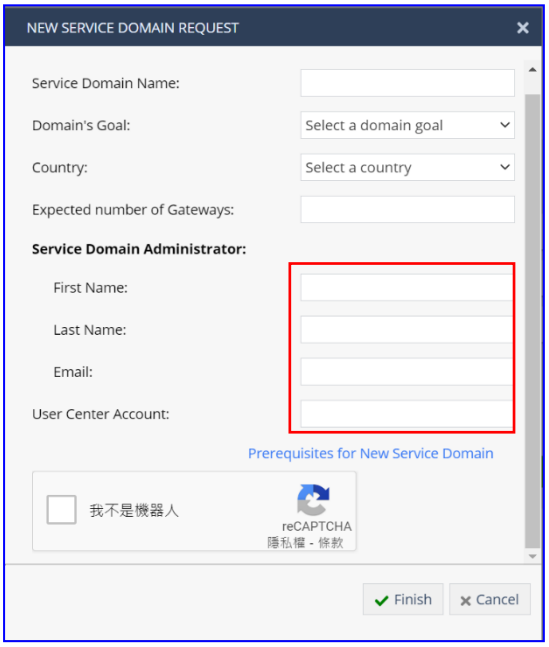


Service Domain Name（輸入公司 Domain）→ Domain’ s Goal（選擇使用目的）→ County（選擇國家）→ Expected number of Gateways（輸入欲管理的防火牆數量）

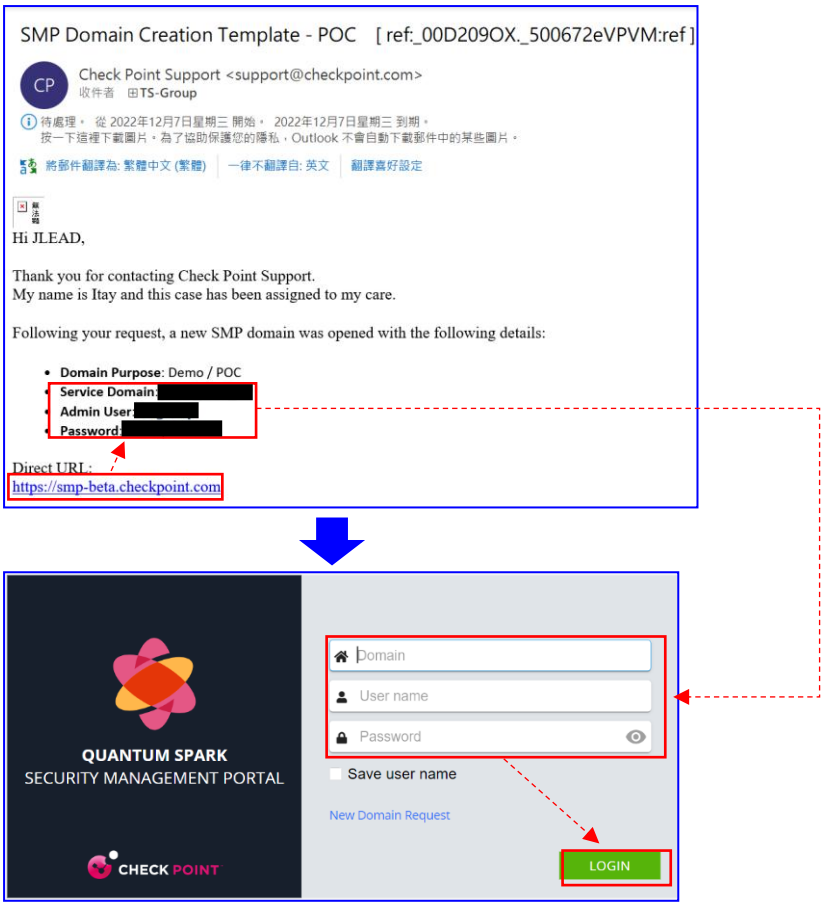




Service Domain Administrator → First Name → Last Name → Email (建議使用公司當初所購買時提供之 Email 申請) → User Center Account (UC ID 查找請參照 2.1.5、2.1.6 步驟)

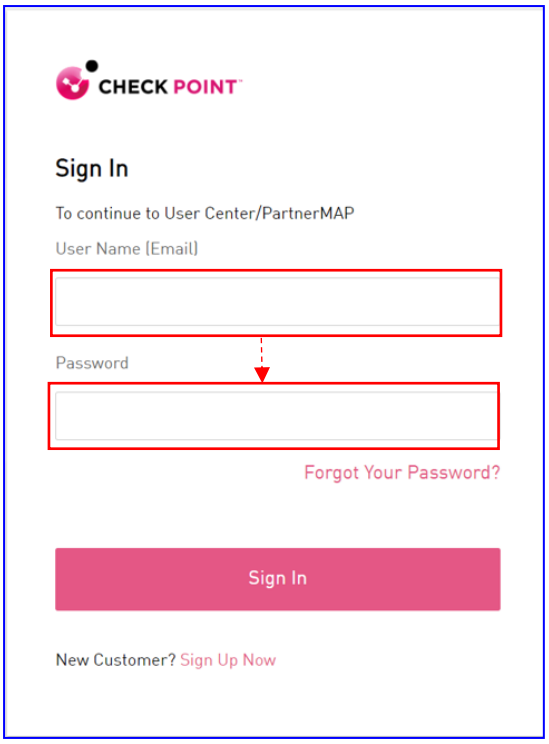


開啟註冊成功信件 → 點擊 Direct URL → 輸入 Domain (註冊時使用網域)、User Name、Password → Login (完成登入)

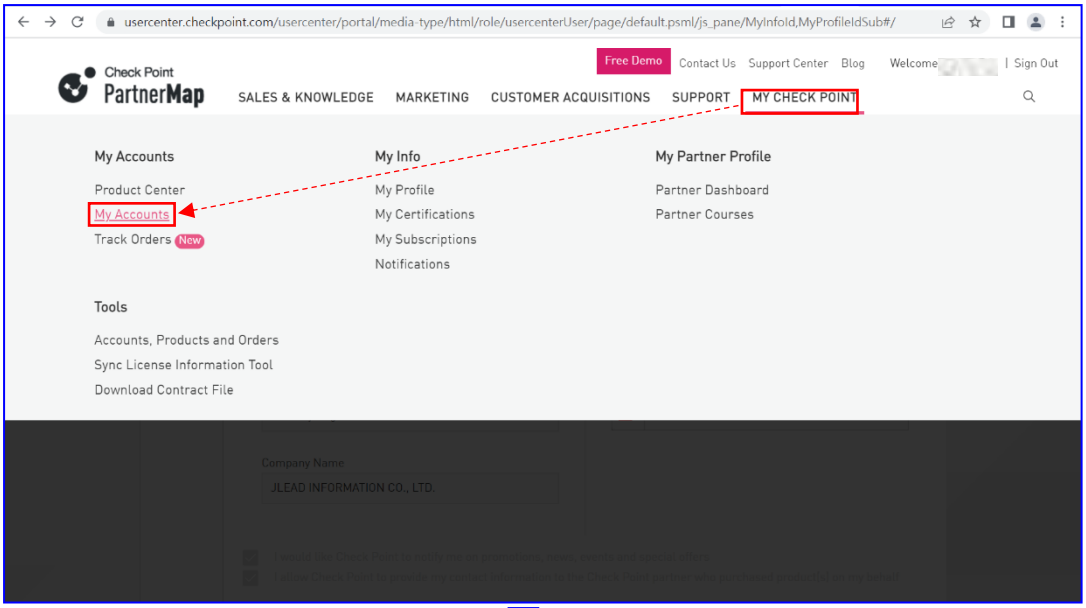

SMP Domain Creation Template - POC [ref:_00D209OX._500672eVPVM:ref]
Check Point Support <support@checkpoint.com>
收件者 TS-Group
待處理。 從 2022年12月7日星期三 開始。 2022年12月7日星期三 到期。
按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。
將郵件翻譯為: 繁體中文 (繁體)
一律不翻譯自: 英文
翻譯喜好設定
Hi JLEAD,
Thank you for contacting Check Point Support.
My name is Itay and this case has been assigned to my care.
Following your request, a new SMP domain was opened with the following details:
Domain Purpose: Demo / POC
Service Domain:
Admin User:
Password:
Direct URL:
https://smp-beta.checkpoint.com

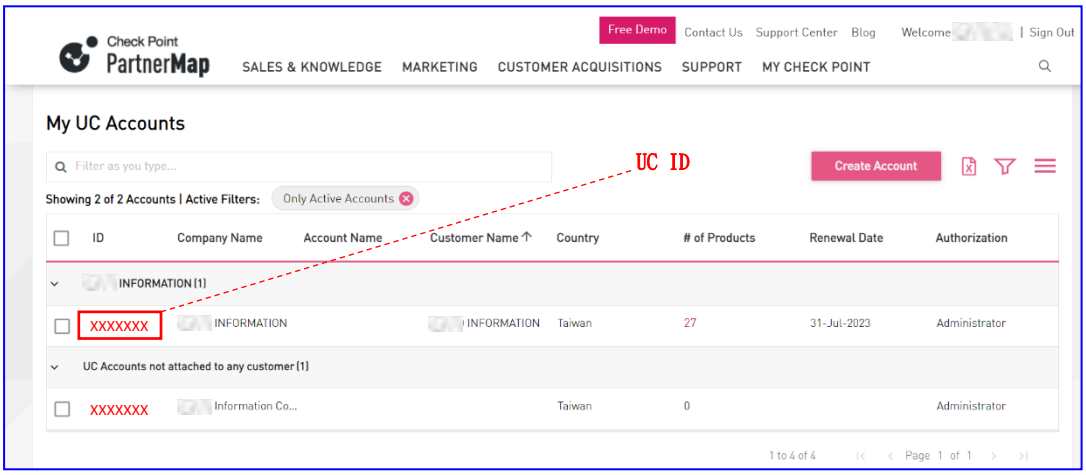
QUANTUM SPARK
SECURITY MANAGEMENT PORTAL
CHECK POINT
Domain
User name
Password
Save user name
New Domain Request
LOGIN

開啟瀏覽器，輸入 https://accounts.checkpoint.com/，輸入帳號密碼登入



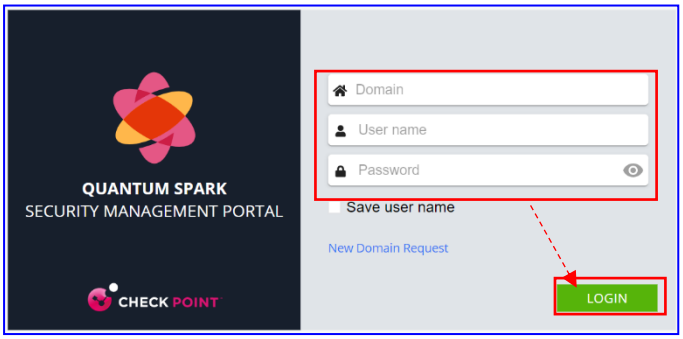
點選 MY CHECK POINT → My Accounts，即可看到公司所屬 UC ID



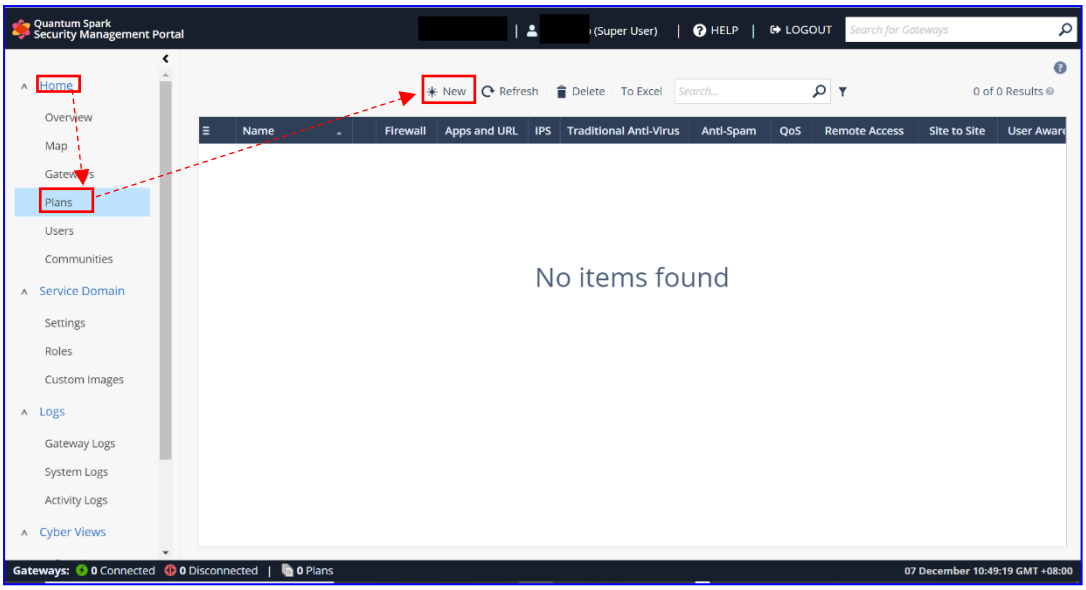


SMP（Security Management Portal）納管 Quantum Spark 2530

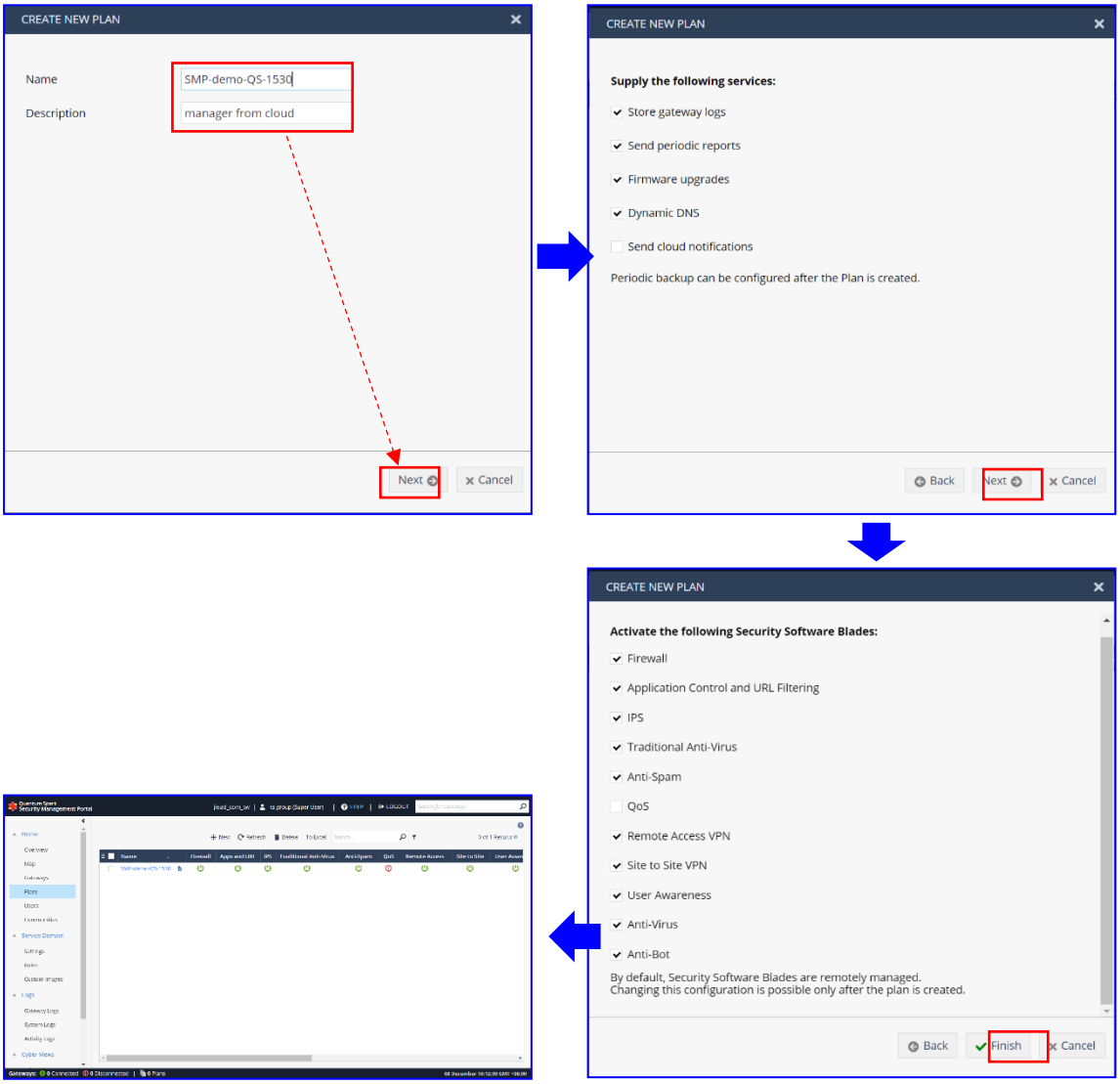
開啟瀏覽器 → https://smp1.portal.checkpoint.com/login → 輸入 Doamin、User name and Password 登入



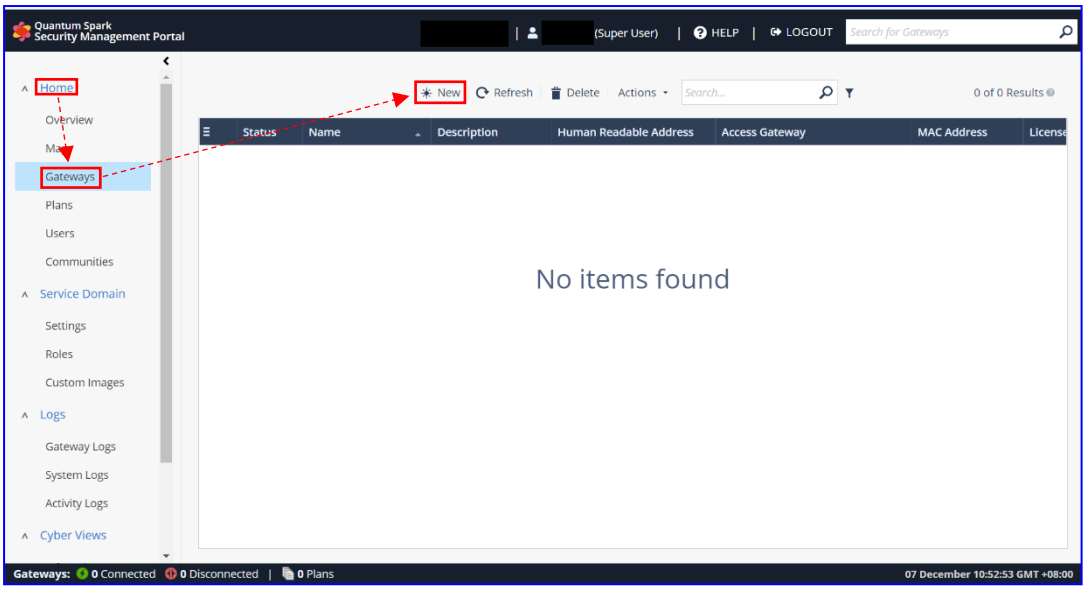
點選 HOME → Plans → New



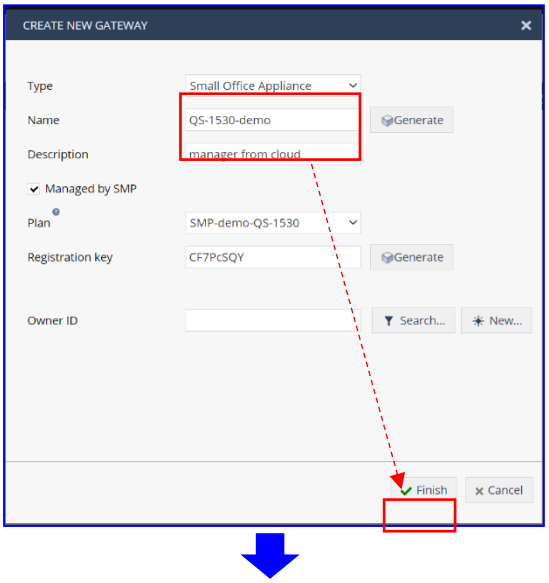
輸入 Plans 名稱 (敘述可填可不填) → Next → Next → Finsh

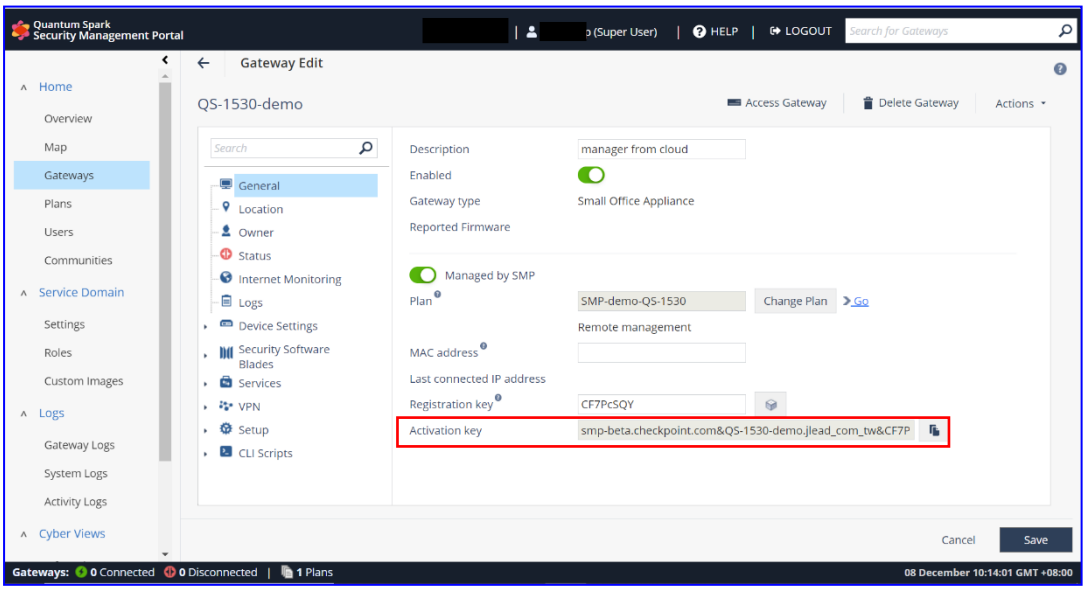


點選 HOME → Gateways → New

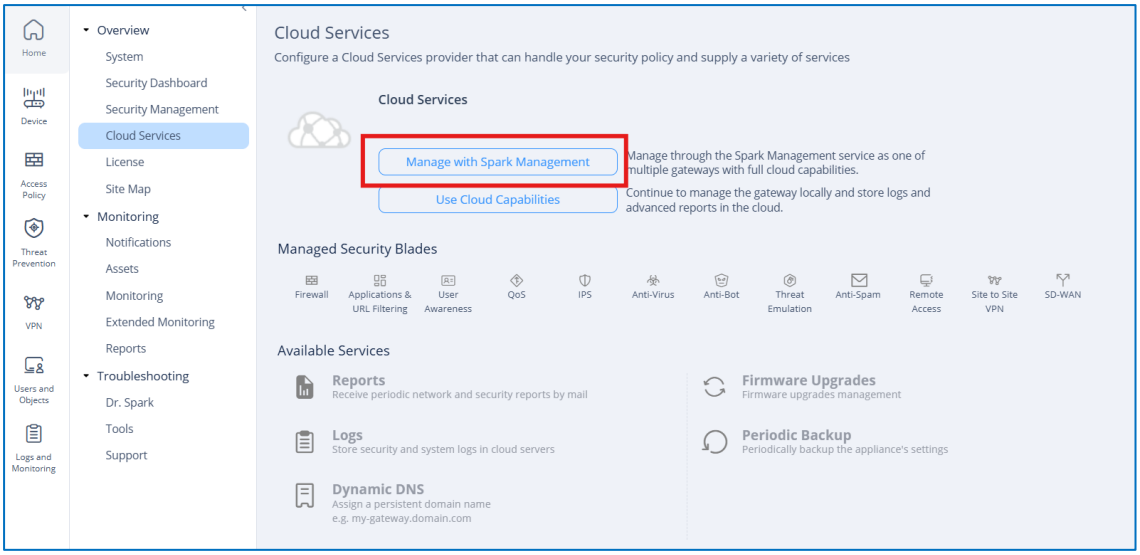


選擇 Type → Name (自訂義欲管理設備名稱) → Finsh → 複製 Activation key 備用 (Quantum Spark 2530 join SMP 時必須資料)

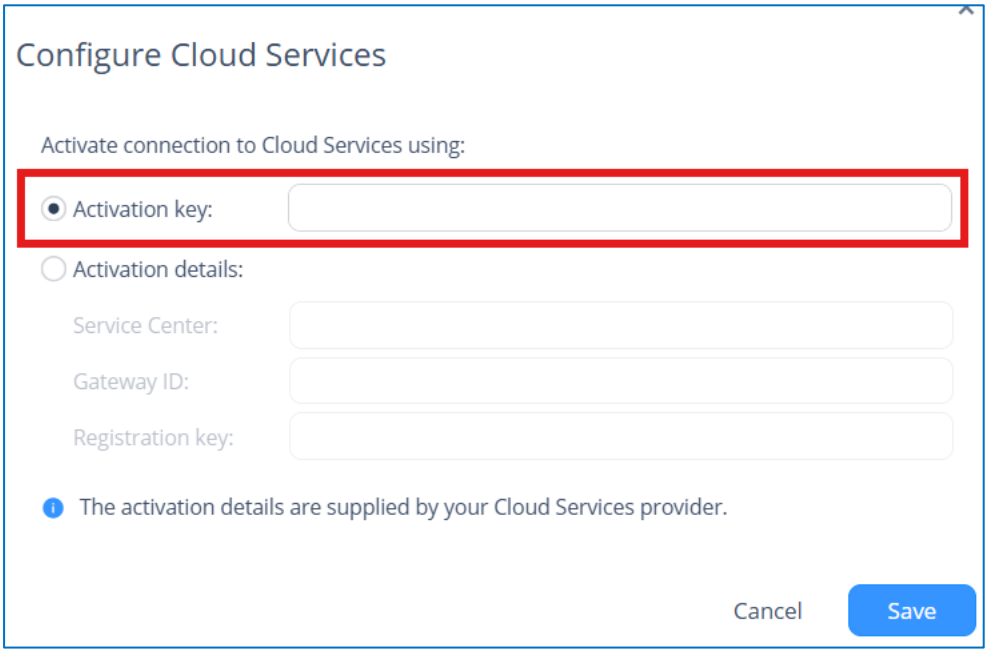


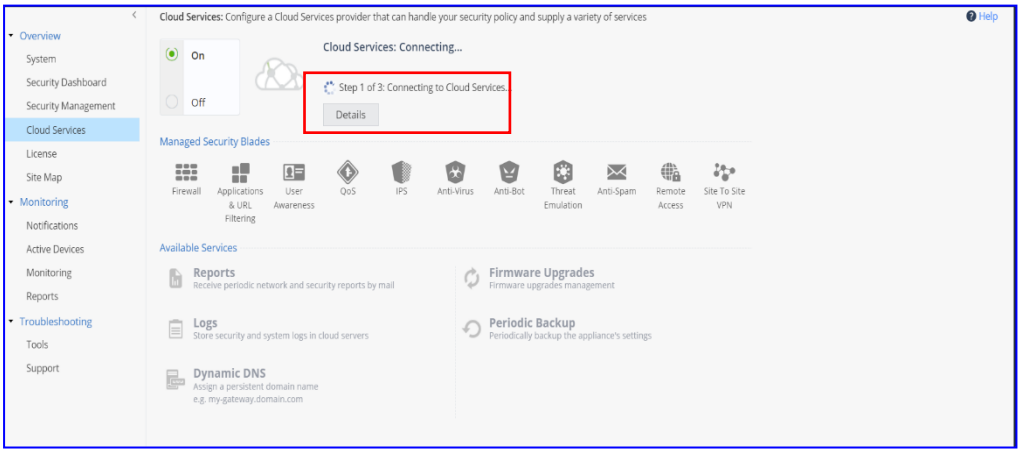


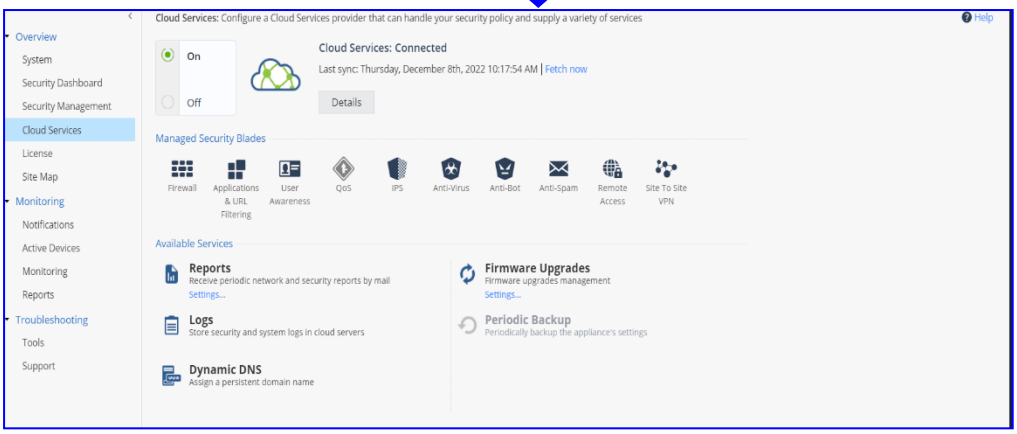
登入 Quantum Spark 2530 → HOME → Cloud Services → Manage with Spark Management

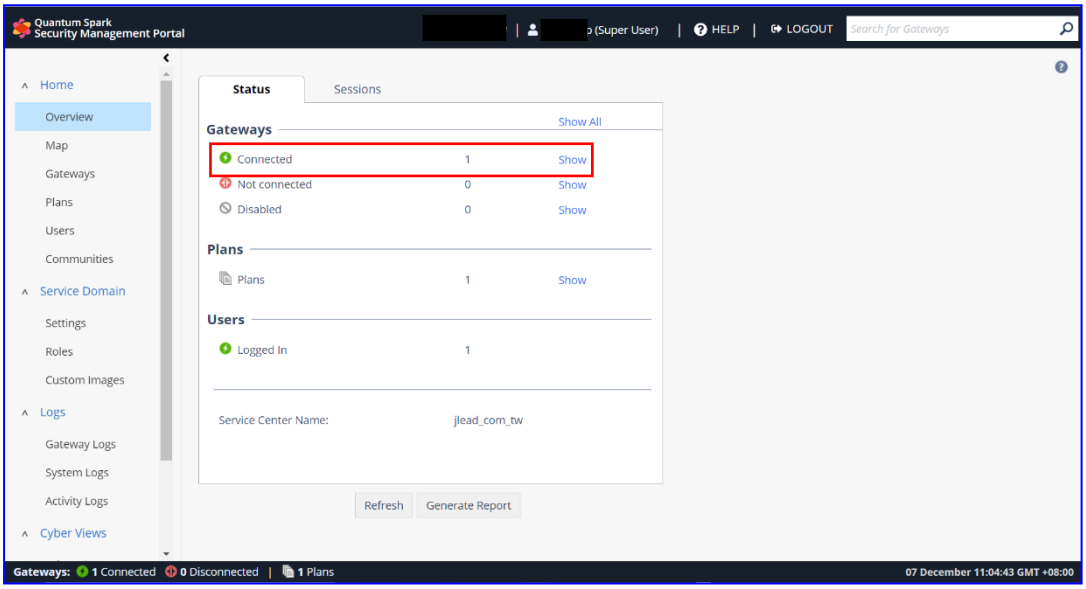


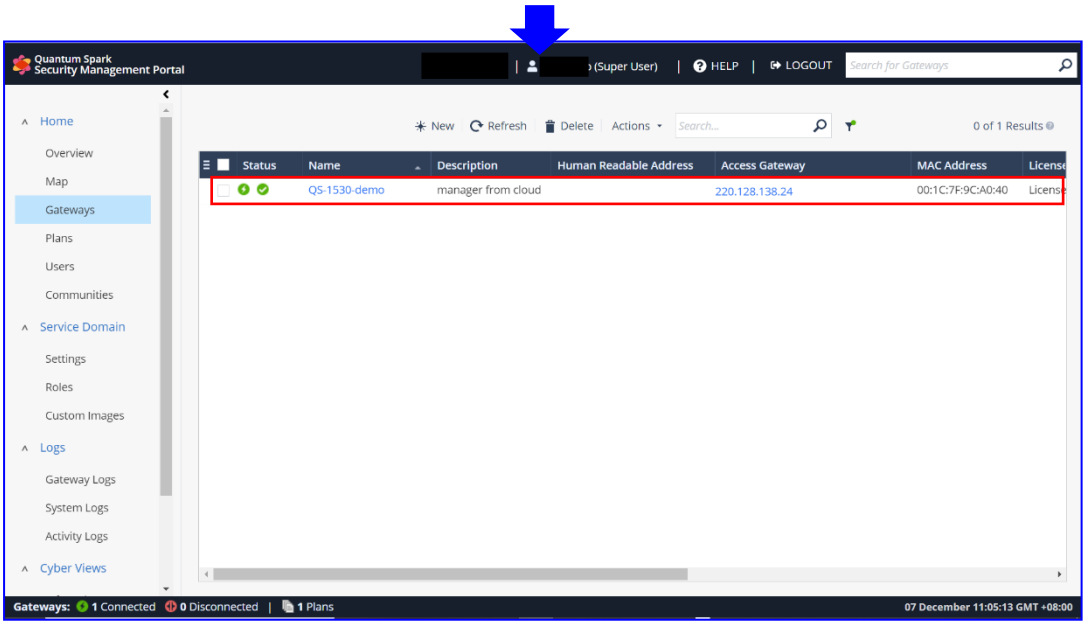
貼上 Activation key → Save → Cloud Services: Connecting（等待連線） → Cloud Services: Connected（完成連線）






Cloud Services: Configure a Cloud Services provider that can handle your security policy and supply a variety of services
Help
Overview
System
Security Dashboard
Security Management
Cloud Services
License
Site Map
Monitoring
Notifications
Active Devices
Monitoring
Reports
Troubleshooting
Tools
Support
On
Off
Cloud Services: Connected
Last sync: Thursday, December 8th, 2022 10:17:54 AM | Fetch now
Details
Managed Security Blades
Firewall
Applications & URL Filtering
User Awareness
QoS
IPS
Anti-Virus
Anti-Bot
Anti-Spam
Remote Access
Site To Site VPN
Available Services
Reports
Receive periodic network and security reports by mail
Settings...
Logs
Store security and system logs in cloud servers
Dynamic DNS
Assign a persistent domain name
Firmware Upgrades
Firmware upgrades management
Settings...
Periodic Backup
Periodically backup the appliance's settings


Quantum Spark
Security Management Portal
[redacted] | [redacted] (Super User) | HELP | LOGOUT
Search for Gateways
Home
Overview
Map
Gateways
Plans
Users
Communities
Service Domain
Settings
Roles
Custom Images
Logs
Gateway Logs
System Logs
Activity Logs
Cyber Views
Status
Sessions
Gateways
Show All
Connected 1 Show
Not connected 0 Show
Disabled 0 Show
Plans
Plans 1 Show
Users
Logged In 1
Service Center Name: jlead_com_tw
Refresh
Generate Report
Gateways: 1 Connected 0 Disconnected | 1 Plans
07 December 11:04:43 GMT +08:00


Quantum Spark
Security Management Portal
[redacted] | [redacted] (Super User) | HELP | LOGOUT
Search for Gateways
Home
Overview
Map
Gateways
Plans
Users
Communities
Service Domain
Settings
Roles
Custom Images
Logs
Gateway Logs
System Logs
Activity Logs
Cyber Views
New
Refresh
Delete
Actions
Search...
0 of 1 Results
Status
Name
Description
Human Readable Address
Access Gateway
MAC Address
License
QS-1530-demo
manager from cloud
220.128.138.24
00:1C:7F:9C:A0:40
Gateways: 1 Connected 0 Disconnected | 1 Plans
07 December 11:05:13 GMT +08:00