

QUANTUM SPARK 1530 系列 Quick Setup Guide





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:該設備啟用之日起計二年

預設 IP 及 帳密 LAN IP Address: https://192.168.1.1 User Name: admin (預設) Password: (自行填入)



目 錄

第一章 安裝及設定 Quantum Spark 防火牆

1. 認識Check Point Quantum Spark 防火牆	ŀ
2. Quantum Spark 1530 產品外觀	ł
3. 安裝 Quantum Spark 1530 設備)
4.所需環境介紹	}
4-1. 電腦端設定	}
4-2. 瀏覽器設定)
5. 開始設定 Quantum Spark 防火牆之前 19)
5-1. 進行線上註冊)
5-2. 回復出廠預設值 (Factory reset))

第二章 開始設定 Quantum Spark 防火牆

1. 設定內部網路組態
2. 設定外部網路組態
2-1. 固定制 IP 客戶
2-2. 非固定制 IP 客戶 (PPPoE)
2-3. DHCP制客戶
3. 設定 DNS/NTP 伺服器位址
4. 設定防火牆開啟相關服務
5. 設定IPS/Application Control/URL Filtering/Anti-Bot/AV&AM
6. IP-Mac Binding

第三章 建立企業網站服務

1. 設定 Web (網頁) 伺服器	40
2. 設定 Mail (郵件) 伺服器	45
3. 設定對外服務伺服器	50
4. 設定開啟 BitTorrent 服務	54

第四章 線路 Fail-over 設定

第五章 VPN 連線設定

1. IPsec VPN (Site-to-Site) 設定	64
2. SSL VPN 設定	71
2-1. SSL VPN 設定 步驟	71
2-2. SSL VPN 用戶端登入	72



第六章 網路頻寬管理

1. 頻寬管理 (客戶可應用於網路語音/視訊會議)	
1-1. 依政策作頻寬管理	
1-2. 依 IP (per-ip) 作頻寬管理	

第七章 系統備份設定

1.	更新系統韌體	85
2.	設定檔備份及上傳	91
	2-1. 備份設定檔	91
	備份設定檔操作路徑: Device > Setup > Operations	92
	2-2. 上傳設定檔	93

第八章 遠端管理防火牆設定

1. 手機APP管理平台	 76
2. SMP Portal雲端管理平台	 01



第一章 安裝及設定 Quantum Spark 防火牆

1-1. 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 1530 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 1530 優勢

- 提供 SandBlast 多合一次世代威脅防護 (SNBT):應用多層保護防堵複雜的網路威脅-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)。
- 共 6 個 1G 乙太網路連接埠:提供 5 個 Internal Port、1 個 WAN port。
- 內建 R80.20.15 (992001653) 版本。
- 可支援中控式管理(管理機需另購)和雲端式管理。

1-2. Quantum Spark 1530 產品外觀





- 1. USB Port3.0:用於軟體下載
- Internal (Port1-5): Gigabit Ethernet 提供連接內部網路使用, WAN Port 提供 ISP 線路使用, 預設 IP: 192. 168. 0.1: 4434
- 3. Console Port:提供 CONSOLE 管理介面, Speed: 115200
- 4. Power DC12V: 電源線接孔
- 5. Factory Default:持續長壓至 Port LED 熄滅,約為 12 秒,可將設備還原為其出廠預設值
- 6. Power Button:按下以開啟或關閉硬體設備



• 側面面板



1. 防盜插槽:在此插入防盜線。使用 Kensington 和 Sunbox TL-623M 纜線作為參考

• 燈號說明

管理 LED	$ \mathbf{\widehat{v}} $	 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:關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,將會從重試指令碼推出。	持續紅色



網路 LED (網路孔)

網路 LED 每個連接 [;]	(RJ45 WAN 和 LAN 連接埠)。 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

1-3. 安裝 Quantum Spark 1530 設備

[請注意] 請避免將 Check Point-1530 的 Internal Port 連接到現有網路上, Checkpoint-1530 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-1530 的 WAN Port。



- 3. 請使用內附的電源變壓器 (12V / 3.0A) 連接至 Check Point-1530 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。





1-4. 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:

- 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 1530。
- 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-1530 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)。

1-4-1. 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。

1-4-1-1. 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-1530 DHCP Server 獲得正確 IP。

- 步驟一:確定電腦的網路埠正確連接到 CheckPoint-1530 的WAN網路埠
- 步驟二:請確定 CheckPoint-1530 的燈號顯示正常 (POWER恆亮), CheckPoint-1530 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

्रि अज्ञास्टर स					
Google Chrome 整 網路和共用中心				-)	×
← → ↑ 壁 か 20年 Mozila Firefox World of Tarks	会 → 規則也利用的利用 → 利用电机用用中心 快信/包括本的/網路留訊/包括/ 地信化用中的網路 開點 = 私人網路 期夏/用於私花 型度/用於私花 型度/目的地域或用数 私花度/但· 品物式 VPN 違用 和前式 / PPN 連續 新算/中國/規模 = 或数/	2 建绿 平均描述: 研究研究 中omeGroup: 建型造工 重要: ¥ 乙大成的 1・或品之的由最成分为和。	v 0 (6)	發盤 新会	4
語参照 HoneGroup Windows 防火纜 網探網路編選					
# P O C 🗧 🗮 🌒 💷					ヘ 炉 🔩 🗐 📟 中 上牛 1 2016/

步驟六:點選乙太網路

資 務回收篇							
Google Chrome	·圣 网络地址			-		×	
	← → ↑ ▲ 2 > 控制合 > 網路和網路網路 > 網路後線 > 組合管理 -	v õ	搜尋網路	連線 夏:	• 💷	م 0	
Mozilla Firefox	Z.x1003 HSR 3 Realtel PCIe GBE Family Contro						
World of Tenks							
	1 個項目						
= ਨ 🗆 🗧 🛤 (Ê 🥹 💷					~ 1	豆 🕼 🗊 💷 中 上午 11:28 2016/7/12



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)

a Ber		
Google Chrome	9.7+05.10 V	- D X
← → ∨ 个 ♥ 2 対応の対応的 総合管理 ▼ 停用症症病院範囲 診断症	1976年) ↓ 2 大利用用 人名	く 5 振春 網路進線 戶 計 11 2
Mozile Firefox GPResitek PCIe GBE Family Contro	建编方式: 💇 Resitek:PCIe GBE Family Controller	
World of Tonks	総定(C) 這個連線使用下列項目(O):	
	図 全 Central of Matter Sharing for Microsoft Networks 図 実 Rela and Printer Sharing for Microsoft Networks 図 えのが自然電話 図 え 利暇利心道印象定葉4 委 (TCP/IPv4)	
	→ Microsoft Network Adapter 多工器通知協定 → Microsoft LDP 通訊協定知動程式	
	安裝(N)	
	讓您的電腦能夠存取 Microsoft 網際上的資源。	
1. 保護目 三編款1. 保護日	補定 取消	100 MI
# P 💷 🤮 🗮 🖨 🧶 💻		ヘ 見 4 同 画 中 片1130 2016//12

步驟八:請選擇自動取得IP位址 (0) → 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

a Hist		
Google Internation		- 🗆 X
小 ジン 控制合 > 規築和相関網路 > 1	2 7-64885.5F36	~ ひ 将最適的体体 の
	¥ 2,538,8 198 ×	Ere CI O
	網路功能	B- • 11 🖉
Mozilo Frefox Zzstigio 1960 3 Resitai Pole GBE Family Contro	塘 闲照细道田康定第4版 (TCP/IPv4) - 内容	
	一般 其他說定	
ET Mondul of	5 均果在的網路支援边頂功能,您可以取得自動描述的 IP 設定。否则, 位必須 時時期指未成管理具正確的 IP 設定。	_
Tenka		
	● 回動取得 ₽ 位堆(O)	
	○使用下列的 IP 位址(S):	
	P位比O:	
	子網路進業(U):	
	9000 M (20):	
	● 自動取得 DNS 伺服器位 並(B)	
	○ 使用下列的 DNS 伺服器位址(E):	
	·俄用 DNS 伺服器(P):	
	第治 DNS 伺服器(A):	
1 保障目 已编取1 希項目	□ 结束時確認設定(L) 連路(V)	1
	20.00	
	W.C. R.A	
📰 🔑 🗔 🖼 🥥 🛄		^ 🖫 🖣 💭 💷 🔮 2016/7/12



步驟十一:請點選詳細資料

般		
連線		
IPv4 連線能力		網際網路
IPv6 連線能力	:	無網路存取
媒體狀態:		已啟用
連線時間:		02:05:50
速度:		1.0 Gbps
活動 ————		
活動	己傳送 ——	
活動	已傳送 —— 20,910,331	一 己接收
活動 位元組: ◆内容(P)	已傳送 —— 20,910,331 ��停用(D)	一 己接收 511,213,700

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。





1-4-1-2. 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-1530 DHCP Server 獲得正確 IP。

步驟一:確定電腦的網路埠正確連接到 CheckPoint-1530 的WAN網路埠

步驟二:請確定CheckPoint-1530的燈號顯示正常 (POWER恆亮), CheckPoint-1530 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+l, 會顯示下圖

■ 赤統				
書牙與裝置		Wi-Fi 建築、管理已知感路、計量付置感路	開啟 🛑 >	
🗢 網路和網際網路				
🥖 個人化		VPN 系後、建築、管理		
📑 應用程式				
💄 ¶EB	((†))	行動熱點 共用的約個問題問題語建築		
6 時間與語言				
☞ 遊戲	₽	预备(模式 件止無疎通問		
★ 協助工具		Prove		
🖤 隱私權與安全性	8	Froxy 美用於 Wi-fi 及乙大網路建線的 Proxy 何重語		
🥏 Windows Update		粉饮 品立我试察阿察路接续		
	₽	/ 推現/創設設定 豊富作有側部分子 卡·劉治重政		

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

網路和網際網路 > 進階網路設定		
VMware Virtual Ethernet Adapter VMnet1 VMware Virtual Ethernet Adapter for VMnet1	停用	
C. 乙太網路 Forlinet Virtual Ethemet Adapter (NDIS 6.30)	停用	
C. 乙太纲路 3 Check Point Virtual Network Adapter For Endpoint VPN Client	停用	
C	啟用	
C 乙太絕路 2 Kaspersky Socurity Data Escort Adapter	停用	
建多规定		
建销共用设定 紧更累固定条和时用动定		
數據使用量		
硼糖及溃疡内容		
續路 重設 或所其與說介质 + 重說為原論說定		
相關 認定		
更多網路介面卡選項		
Windows防火满		

步驟七:點選乙太網路

2 網路連線			-			×
🔶 🛶 🔹 🛉 🙀 > 控制合 > 網路和網際網路 > 網路連線 >	~ ひ 提	录 網路連線				P
組合管理 ▼			-	•		0
乙六時時 網路 3 Realtek PCIe GBE Family Contro						
使項目					B	



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(0)→請選擇自動取得DNS 伺服器位址(B)

然後點選確定

股	其他設定					
ロ果()間#	您的網路支援這項功能,您 網路系統管理員正確的 IP 認	可以取得自重 注:	加措派的) IP 設定	「不見	,您必須
0	自動取得 IP 位址(O)					
0	使用下列的 IP 位址(S):					
IP	位址(I):					
子	網路遠罩(U):		÷			
預	設閘道(D):		-			
0	自動取得 DNS 伺服器位址((B)				
0	使用下列的 DNS 伺服器位:	址(E):				
慣	用 DNS 伺服器(P):					
其	他 DNS 伺服器(A):		*	.*)		
	結束時確認設定(L)				<u>1</u>	階(V)

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

10.4 油油台出土.		· · · · · · · · · · · · · · · · · · ·	吃大雨
IFV4 建脉胎力.		無調味調	路左取
揮體狀能·			二的田
連線時間:		00:	:01:32
速度:		1.0	Gbps
詳細資料(E)			
詳細資料(E,		.	己接收
詳細資料(E	已傳送 ——	-	∃接收 1,508

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1-4-2章節設定瀏覽器。



1-4-2. 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。

1-4-2-1. 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

自動設定會取	代手動設定。要確保使用手動設定,請停用自動設定。
🔽 自動偵測詞	段定(A)
🗌 使用自動詞	设定指令碼(S)
位址(R)	
Proxy 伺服器	
□ ^{為您的 LA} (X)	N 使用 Proxy 伺服器 (這些設定將不會套用到撥號或 VPN 連線)
位址(E);	連接埠(T); 80 進階(C)
☑ 近端維]址不使用 Proxy 伺服器(B)

都不要勾選→確定後請點選<mark>確定</mark>,→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-1530,接下來請跳至 1-5-1 進入預設 Web 設定畫面。



1-4-2-2. 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)

連線設定		×
設定存取網際網路的代理伺服器 ● 不使用 Proxy (Y) ● 自動偵測此網路的 Proxy 設定 (W)		
○ 使用系統 Proxy 設定 (U)		_
○ 手動設定 Proxy (<u>M</u>)		_
HTTP Proxy (X)		0
_ 也針對 HTTPS 連線使用此代理伺服器 (S)		
HTTPS Proxy (H)	埠 (<u>O</u>)	0
		<u> </u>
○ SOCKS V4 (K) ● SOCKS V5 (V)		
	重新載	λ (F)
	確定	取消

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-1530,接下來請跳至 1-5-1 進入預設 Web 設定畫面。



1-4-2-3. 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:

9	設定	Q、搜尋設定	D
•	你與 Google	齨 你的 <u>瀏覽器是由貴機構所管理</u>	
â	自動填入	系統	
•	隱私權和安全性	Google Chrome 關閉時繼續執行背景應用程式	
æ	外觀	在可用時使用硬體加速	
۹	搜尋引擎	開啟電腦的 Proxy 設定	2
□	預設瀏覽器		
ሳ	起始畫面		
₿	語言		
₹	下載		
Ť	無障礙設定		
4	系統		
Ð	重設與清理		

步驟二:再選取開啟電腦的Proxy設定

設定	
命 首頁	Proxy
尋找設定 ク 網路和網際網路	針對乙太網路或 Wi-Fi 連線使用 Proxy 伺阪器。這些設定不會套用到 VPN 連線。
④ 狀態	自動傾測設定
<i>(i</i> , Wi-Fi	使用設定指令碼 開閉
記 乙太網路	指令碼位址
☆ 撥號	
% VPN	
97 元朝(1933 (19) 行動熱點	手動 Proxy 設定 針對乙太網路或 Wi-Fi 連線使用 Proxy 伺服器。這些設定不會套用到
Proxy	VPN 連線。 使用 Proxy 伺服器
and the second se	
	位址 連接單
	不要為開頭為下列項目的位址使用 Proxy 伺服器。請使用分號 () 來分陽 每個項目。

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-1530,接下來請跳至 1-5-1 進入預設 Web 設定畫面。



1-5. 開始設定 Quantum Spark 防火牆

1-5-1. 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 1530 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"



1-5-2. 透過精靈設定 CheckPoint-1530

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)。

CHECK POINT 1500 APPLIANCE WIZARD		❸ English 日本語
O f #100.00		
Welcome to the Check Point First Time Configurati	1500 Applian on Wizard	ce
You are just a few steps away from using your ne	w Check Point 1500 Ap	opliance!
	a Daala Mau	
Fetch settings from Zero Touch	< Back Nex	t> Quit



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。

CHECK POINT 1500 APPL	IANCE WIZARD		? Help	
Authentication Details				
Change the default admi	nistrator name and set the passw	ord:		
Administrator name:	admin			
Password:		Password strength:	ong	
Confirm password:				
Enforce password cor	nplexity on administrators			
It is strongly recommended to use both uppercase and lowercase characters as well as one of the following characters in the password: 1@#\$%^&*0=+:;				
Help us improve product experience by sending data to Check Point				
Step 1 of 9 Authenticatio	n	< Back	Next > Quit	

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。

CHECK POINT 1500 APPLIANCE WIZARD					
Appliance Date an	Appliance Date and Time Settings				
O Set time manually					
Date:	Thursday, June 23, 2022	苗			
Time:	3 : 18 PM 🔻				
Time zone:	(GMT+08:00) Taipei	-			
Use Network Time Pre	otocol (NTP)				
First NTP server:	ntp.checkpoint.com				
Second NTP server:	ntp2.checkpoint.com				
Time zone:	(GMT+08:00) Taipei	•			
Step 2 of 9 Date and Tim	e Settings <	Back	Next > Quit		



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。

CHECK POINT 1500	APPLIANCE WIZARD			🥐 Help
Appliance Nan	ne			Point"
Of Back				
Appliance Name:	Gateway-ID-7F9C9FF6			
Domain name:	Field is not mandatory			
	Example: mycompany.com			
Step 3 of 9 Appliand	ce Name	< Back	Next >	Quit



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。

CHECK POINT 1500 APPLIANCE WIZARD	? Help
Security Policy Management	Check Point SOFTWARE TECHNOLOGIES LTD.
Choose how to manage security settings	
Local management I want to manage the security policy of the device using the local web application	
Central management I am using a Management Server that will manage this	s device
Step 4 of 9 Security Policy Management < Back	Next > Quit

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。

CHECK POINT

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)

CHECK POINT 1500 APPLIA	NCE WIZARD	7 Help	•
Internet Connection	ı		
• Configure Internet conr	nection now		
Connection type:	DHCP	•	
Configure Internet conr	ection later		
Step 5 of 9 Internet Conne	ction	< Back Next > Quit	

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。

CHECK POINT 1500 AF	PPLIANCE WIZARD			0	Help
Local Network					ogies LTD.
LAN Settings					
✓ Enable switch on	LAN ports			1 2 3 5	5 WAN
Network name:	LAN Switch		[
IP address:	192.168.1.1				1
Subnet mask:	255.255.255.0				
DHCP Settings			LAN	I switch	
DHCP Server:	Enabled 🔹		Tr	affic between LAN por inspected	ts is not
DHCP range:	192.168.1.1	: 192.168.1.254			<u> </u>
The device IP address	is automatically exclu	ded from the DHCP	range		–
Exclusion range:	not mandatory	: not mandatory			
Step 6 of 9 LAN			< Back	Next > Q	uit

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。

CHECK POINT 1500 APPLIANCE WIZARD	🝞 Help
Administrator Access	
Select the sources from which to allow administrator access	
✓ LAN ✓ VPN Internet	
Access from the above sources is allowed from	
O Any IP address	
O Specified IP addresses only	
 Specified IP addresses from the Internet and any IP address from other sources 	
* New × Delete	
No Items Found	
Step 7 of 9 Administrator Access < Back	Next > Quit



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。

CHECK POINT 1500 APPLIANCE WIZARD					
Software Blades Activation					
Select the Softw	vare Blades you wis	h to activate			
ACCESS CONTR	0L		VPN		
v		√ []=	v 🦚		
Firewall	Applications & URL Filtering	User Awareness	Remote Access	Site To Site VPN	
THREAT PREVEN	ITION ·····				
v ()	v 🗞	✓ ¥	v 😫	\checkmark	
Intrusion Prevention (IPS)	Anti-Virus	Anti-Bot	Threat Emulation	Anti-Spam	
Step 9 of 9 Soft	ware Blades Activation	on	< Back	Next > Quit	

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」。

The First Time Configu	ration Wizard has completed
Administrator name:	admin
System time:	Friday, April 29, 2022 02:07 PM
Appliance name:	Gateway-ID-7F9C9FF6 (1550 Appliance)
Internet:	Connected
License:	Obtained
Local network:	192.168.100.253 / 255.255.255.0
	DHCP server is disabled
	🛕 A secondary IP address was set on LAN1 Switch 🕕
Security policy mode:	Locally managed
Active Software Blades:	Firewall, Application Control, URL Filtering, User Awareness, Remote Access, Site To Site VPN, Intrusion Prevention (IPS), Anti-Virus, Anti-Bot, Threat Emulation, Anti-Spam



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

Check Po 1530 Ap	vint pliance		wadmin E+ Log Out ? Help / Support Q Search
Номе	 Overview 	System System INFORMATION	Help NETWORK Internet connections
DEVICE DEVICE ACCESS POLICY	Security Dashboard Security Management Cloud Services License Site Map	Check Point 1530 Appliance Wersion:: R80.20.15 (992001653) Name: Gateway-ID-7FB0DCB6 MAC: 00:1C:7F:B0.DC:B6 Wednesday, December 14th, 2022 02:22:59 PM (GMT-08:00) Taipei System is up for 0 days, 22 hours, 42 minutes and 13 seconds	Connection type: DHCP Interface: WAN IPv4 address: 10.10.150.104/24
THREAT PREVENTION VPN USERS & OBJECTS	Notifications Active Devices Monitoring Reports • Troubleshooting Tools Support	NOTIFICATIONS Notifications page Image: New device detected Informative Event 11:40:44 14 Dec 2022 (192.168.99.99) connects to your network (LANS) for the first time. Informative Event 11:38:55 14 Dec 2022 (192.168.200.1) connects to your network (LAN1) for the first time. Informative Event 11:38:55 14 Dec 2022 (192.168.200.1) connects to your network (LAN1) for the first time. Informative Event 11:38:35 14 Dec 2022 (172.161.1) connects to your network (LAN2) for the first time. Informative Event 11:38:35 14 Dec 2022	WATCHTOWER MOBILE APP WATCHTOWER WATCHTO
LOGS & MONITORING		NETWORK ACTIVITY Packet Rate (packets per second)	Reports Monitoring Throughput (Kbps)

1-5-2-1. 設定外部連線 (單條寬頻網路)

1-5-2-1-1. 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

CHECK POINT 1500 APPLIANCE WIZARD					? Help
Internet Connection					Point"
• Configure Internet conne					
Connection type:	Static IP		•		
IP address:	10.10.150.99			3-4-5	WAN
Subnet mask:	255.255.255.0				-
Default gateway:	10.10.150.254				
First DNS server:	8.8.8.8				J
Second DNS server:					
		Connec	t		
O Configure Internet connection later					
🕏 WAN link is up					
Step 5 of 9 Internet Connect	ion		< Back	Next >	Quit



1-5-2-1-2. 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 DHCP,點擊 Connect 測試,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

CHECK POINT 1500 APPLIANCE WIZARD	? Help
Internet Connection	
 Configure Internet connection now Connection type: PPPoE ISP login user name: ISP login password: Connect Configure Internet connection later 	
Step 5 of 9 Internet Connection <	Back Next > Quit

1-5-2-1-3. DHCP 制客戶

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

CHECK POINT 1500 APPLIAN	CE WIZARD		Help
Internet Connection			
• Configure Internet conne	ction now		
Connection type:	DHCP	-	
Configure Internet conne	Connection later	ct	- 3 - 4 - 5 WAN
Connected [IP: 10.10.150.	106]		
Step 5 of 9 Internet Connect	ion	< Back	Next > Quit

第二章 開始設定 Quantum Spark 防火牆

2-1. 設定內部網路組態

貴客戶請登入 Check Point 1530,點選 DEVICE → Local Network → 選取 LAN1 按 Edit ,進入下一步驟

Check P 1530 Ap	oint opliance			🛥 adn	nin 🗗 Log Out ? Help / Supp	ort Q Search
		Local Network: Configure and mana	age local interfaces, switches, bridges, bonds and VLANs			Help
HOME	Network Internet	Type to filter Q 🗧	New 🔻 🧪 Edit 🗙 Delete 🗮 Enable 🛛 Disj	olay: Networks 🔻		
	Local Network	Name	Local IPv4 address	Subnet mask	MAC Address	Status
DEVICE	Hotspot	🗼 LAN1	192.168.1.1	255.255.255.0	00:1c:7f:b0:dc:b7	3 1 Gbps/Full duplex
	Routing	🗼 LAN2			00:1c:7f:b0:dc:b7	Cable disconnected
:::	MAC Filtering	🗼 LAN3			00:1c:7f:b0:dc:b7	O Disabled
ACCESS POLICY	DNS	🗼 LAN4			00:1c:7f:b0:dc:b7	⊘ Disabled
6	Proxy	🗼 LAN5			00:1c:7f:b0:dc:b7	Cable disconnected
THREAT	 System 					
PREVENTION	System Operations					
22.0	Administrators					
VPN	Administrator Access					
	Device Details					
	Date and Time					
OBJECTS	DDNS & Device Access					
~	Tools					
LOGS &	Certificates					
MONITORIN	Installed Certificates					
	Internal Certificate					
	• Advanced					
	Painternet connected					🚱 Up to date 🛛 O 2:28 PM

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)

Configuration Advanced	DHCPv4 Settings			
Interface Configuration				
······································				
Assigned to:	Separate network	•		
Local IPv4 address:	192.168.1.1			
Subnet mask:	255.255.255.0			
Use hotspot when connecting t	o network			
DUCD 4 Server				~
DHCFV4 Server				
 Enabled 				
IP address range:	192.168.1.110	-	192.168.1.210	
The device IP address is automatic	cally excluded from the DHC	P range		
IP addresses exclude range:		-		
Relay				
ODisabled				
Obiabled				



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 CheckPoint 1530 系統 (例如: https://192.168.1.254)

EDIT LAN1	×
Configuration Advanced	DHCPv4 Settings
DNS Server Settings (For DHCPv4)	
 Auto - use the DNS configuration 	on of the device
O Use the following IP addresses:	
First DNS server:	
Second DNS server:	
Third DNS server:	
Default Gateway	~
 Use this gateway's IP address a 	is the default gateway
O Use the following IP address:	
WINS	· · · · · · · · · · · · · · · · · · ·
 Use the WINS servers configure 	ed for the internet connection
Use the following WINS servers	
First:	
Second:	
Lease	~ *
	✓ Apply × Cancel

2-2. 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。



2-2-1. 固定制 IP 客戶

貴客戶請登入 CheckPoint1530,點選 DEVICE → Internet → 按 Edit,進入下一步驟



請注意:系統預設值為 DHCP

	INECTION				
Configuration	Connecti	on Monitoring	Advanced		
Internet Configu	ration				
Connection nam	ne:	Internet1			
Interface:		WAN		•	
Connection type	2:	DHCP		•	
Use connect	ion as VLAN				



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

Configuration	Connection Monitoring Advanced	
nternet Configura	ation	~ ~
Connection name	: Internet1	
Interface:	WAN 👻	
Connection type:	Static IP 🗸	
IP address:	10.10.150.104	
Subnet mask:	255.255.255.0	
Default gateway:	10.10.150.254	
Use connectio	n as VLAN	
ONS Server Settin	gs	~
First DNS server:	168.95.1.1	
Second DNS serve	er: 8.8.8.8	
Third DNS server:	Field is not mandatory	



2-2-2. 非固定制 IP 客戶 (PPPoE)

貴客戶請登入CheckPoint1530,點選 DEVICE → Internet → 按 Edit,進入下一步驟



請注意:系統預設值為 DHCP

DIT INTERNET CON	INECTION				
Configuration	Connectio	on Monitoring	Advanced		
Internet Configu	ration				
Connection nan	ne:	Internet1			
Interface:		WAN		•	
Connection type	2:	DHCP		•	
Use connect	ion as VLAN				



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

Configuration	Connec	tion Monitoring	Advanced		
Internet Configu	ration				~
Connection nam	e:	Internet1			
Interface:		WAN		•	
Connection type	:	PPPoE		•	
ISP login user na	me:				
ISP login passwo	rd:				
		Show			
Use connecti	on as VLAN				



2-2-3. DHCP 制客戶

貴客戶請登入CheckPoint1530,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

×
nitoring Advanced
~
rnet1
V -
P 🔹
✓ Apply × Cancel


2-3. 設定 DNS/NTP 伺服器位址

貴客戶請登入CheckPoint1530,點選 DEVICE → DNS → 按 Configure,手動設定DNS IP

Check Po 1530 Ap	pint pliance	, second s	🛶 admin					
		Configure DNS and Domain settings for the device						
6	 Network 	IPv4 DNS						
HOME	Internet	IPv4 DNS Servers						
_	Local Network							
	Hotspot	Configure DNS servers These settimes will be applied as all laterant compactions						
DEVICE	Routing	mese secongs will be applied on all internet connections						
:::	MAC Filtering	First DNS server:						
ACCESS	DNS	Second DNS server:						
	Proxy	Third DNS server:						
	 System 	Use DNS servers configured for the active Internet connection(s)						
PREVENTION	N System Operations IPv4 DNS Proxv							
2 0.	Administrators							
VPN	Administrator Access	Relay DNS requests from internal network clients to the DNS servers defined above						
	Device Details	✓ Resolve Network Objects						
	Date and Time	Use network objects as a hosts list to translate names to their IP addresses						
OBJECTS	DDNS & Device Access							
0	Tools	Domain Name						
LOGS &	Certificates	Domain name: e.g. MyCompany.com						
MONITORING	Installed Certificates							
	Internal Certificate	e Apply - M Cascal						
	 Advanced 	▼ Appiy × Cancel						
	Salnternet connected							

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

1530 App	pliance	DNG Configure DNC and Dama	in settings for the devise		admin 🗳		
ð	• Network	DN3. Compute DNS and Doma	in settings for the device				
HOME	Internet	IPV4 DINS					
_	Local Network	IPv4 DNS Servers					
-	Hotspot	O Configure DNS servers					
DEVICE	Routing	These settings will be ap	olied on all Internet connecti	ons			
	MAC Filtering						
ACCESS	DNS						
POLICY	Dave						
Ô	Proxy						
THREAT	 System 	 Use DNS servers configu 	red for the active internet co	nnection(s)			
EVENTION	System Operations	Connection Name	First DNS Server	Second DNS Server	Third DNS Server		
220	Administrators	Internet1	168.95.1.1	8.8.8.8			
VPN	Administrator Access						
	Device Details	IPv4 DNS Proxy					
22	Date and Time	 Enable DNS proxy 					
JSERS & DBJECTS	DDNS & Device Access	Relay DNS requests from	internal network clients to t	he DNS servers defined above			
~	Tools	Resolve Network Objects					
065.8	 Certificates 	Use network objects a	as a hosts list to translate na	mes to their IP addresses			
NITORING	Installed Certificates	Domain Name					
	Internal Certificate	Domain wante					
	internar certificate			🗸 Apply	× Cancel		
	 Advanced 						

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

Check Poi 1530 App	int oliance					Y	🖬 admin 🛛				
	<	Date and Time	: Configu	ring c	device's d	ate and time manually or using NTP					
	 Network 	Connect Contern Times We describe: Describes 14th 2020 02:05:01 DM (CMT: 00:00) Tyles I									
HOME	Internet	Adjust Date ar	d Time	ember 140, 2022 03.03.51 Hw (Gwi 1 00.00) Taiper							
	Local Network	Aujust Date al	Aujust Date and Time								
-	Hotspot	Set date a	• Set date and time manually								
DEVICE	Routing	Date:	Wedne	esday,	Decemb	er 14th, 🗰					
:::	MAC Filtering	Time:	03 :	04	PM 🔻						
ACCESS POLICY	DNS	🔵 Set date a	nd time u	using	a Networ	k Time Protocol (NTP) server					
~	Proxy	NTP serve				ntp.checkpoint.com					
	• System	NTP serve									
PREVENTION	System Operations										
10-0	Administrators										
VPN	Administrator Access	NTP authentication									
	Device Details										
2 <u>2</u>	Date and Time										
USERS & OBJECTS	DDNS & Device Access	Time Zone									
~	Tools	Local time zo	ne:		GMT+08	00) Taipei					
LOGS &	 Certificates 		Cocar ume zone. (GMT+08								
MONITORING	Installed Certificates	✓ Automatic	any dujus	st clot	LK TOF GAY	nghi saying changes					
	Internal Certificate										
	Advanced					✓ Apply × Cancel					
	lnternet connected										

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

Check Poi 1530 App	int Diance			🛶 adm				
і номе	Network Internet	 Current System Adjust Date and 	Date and Time: Configuring device's date and time manually or using NTP Current System Time: Wednesday, December 14th, 2022 03:07:16 PM (GMT+08:00) Talpei Adjust Date and Time					
DEVICE	Local Network Hotspot Routing	O Set date and Date:	 ○ Set date and time manually Date: Wednesday, December 14th,					
ACCESS POLICY	MAC Filtering DNS Proxy	Set date and NTP server:	d time using a Networ	rk Time Protocol (NTP) server				
THREAT PREVENTION	System System Operations	NTP server:	rval (minutes):	Intp2.checkpoint.com				
VPN	Administrators Administrator Access	NTP aut	hentication					
USERS & OBJECTS	Date and Time DDNS & Device Access	Shared S	Secret identifier:					
LOGS & MONITORING	Tools Certificates Installed Certificates	Local time zone	e: (GMT+08: Ily adjust clock for day	:00) Taipel				
	Internal Certificate			✓ Apply X Cancel				

完成後按 Apply 完成時間設定



2-4. 設定防火牆開啟相關服務

貴客戶請登入 CheckPoint1530,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



2-5. 設定 IPS/Application Control/URL Filtering/Anti-Bot/AV&AM

貴客戶請登入 CheckPoint1530,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

Check Po 1530 Ap	oint opliance		🛥 admin [
	<	Threat Prevention Blade Control: Configure IPS and malware policy	
``	 Threat Prevention 	•¥• O	
HOME	Blade Control	Vinfected devices More details	
	Exceptions	Threat Prevention (Powered by SandBlast Cloud)	
DEVICE	Infected Devices	ON IPS Out of date	
	 Protections 	ON Anti-Virus 📀 Up to date	
::::	IPS Protections	Anti-Bot Q Up to date	
ACCESS POLICY	Engine Settings		
	 Anti-Spam 	Inreat Emulation	
THREAT	Blade Control	Schedule updates	
PREVENTION	Exceptions	Policy	
22.0		O Stalet	
VPN		O strict	
A .		Recommended	
		○ Custom	
OBJECTS		Tracking options:	
\sim		Protection Activation	
LOGS & MONITORING			
		High confidence: Vrevent	
		✓ Apply 🗙 Cancel	

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

Check Po 1530 Ap	pint pliance				🍟 adm	iin E+ Log_Out ?) E	ielp / Support Q	Search	
П НОМЕ	 Threat Prevention Blade Control 	IPS Protections: Monitor protections	ctions list and manually configu	re specific protections to ove	erride general policy			📇 Print 🕑	Help
	Exceptions	Protection	Protection Type	Category	Action	Severity	Confidence L	Performance Imp	
-	Infected Devices	SYN Attack	Server/Client Protection	ТСР	Inactive	High	High	Critical	^
DEVICE	 Protections 	Sequence Verifier	Server Anomaly	TCP	Thactive 🖤	High	Mediu	Low	
===	IPS Protections	LAND	Server/Client Protection	Denial of Service	Prevent	Medium	Mediu	Very-low	
ACCESS	Engine Settings	Ping of Death	Server/Client Protection	Denial of Service	Prevent	🛑 Medium	Mediu	Very-low	
POLICI	 Anti-Spam 	Small PMTU	Server/Client Anomaly	TCP	That ive	High	High	Critical	
Ô	Blade Control Exceptions	Teardrop	Server/Client Anomaly	Denial of Service	Thactive 🖤	High	Mediu	Very-low	
THREAT PREVENTION		Max Ping Size	Server/Client Anomaly	IP and ICMP	Prevent	Medium	High	Very-low	
		Non-TCP Flooding	Server/Client Anomaly	Denial of Service	That ive	High	Mediu	Low	
2000 - C		Network Quota	Server/Client Anomaly	IP and ICMP	Inactive	High	Mediu	Critical	
VPN		Dynamic Ports	Server/Client Anomaly	Network Security	Inactive	Medium	High	Very-low	
22		Inbound DNS Request	Server Protection	Cache Poisoning	Inactive	High	Low	Critical	
USERS &		Mismatched Replies	Server/Client Protection	Cache Poisoning	Inactive	High	Mediu	Critical	
OBJECTS		Scrambling	Server/Client Protection	Cache Poisoning	Inactive	High	Mediu	Critical	
\sim		Non Compliant DNS	Server/Client Anomaly	DNS	Inactive	Critical	Medium	Low	
LOGS & MONITORING		Unknown Resource Record	Server/Client Anomaly	DNS	Inactive	Medium	Low	Low	
		DNS Data Overflow	Server/Client Protection	DNS	Inactive	Critical	Mediu	Low	-
		≪ < Page 1 of 2 >	>					1-50 0	of 64
	Salnternet connected					🕹 Upgr	ade available 🛛 😵	Up to date 🛛 🛇 03:16	5 PM

2-6. 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

Check Poin 1530 Appli	it iance					🕁 admin 🗗 Log C
і номе	 Users Management User Awareness 	Network Objects: Create a	and edit network objects that Q 🔆 New 🖍 Edit	will be used in the device's feat	ure configuration	
	Users	Object Name	-	Type Domain / IP Ac	ldresses	
-	Administrators	PC2	EDIT NETWORK OBJ	ECT	×	
DEVICE	Authentication Servers					
343	 Network Resources 		Type:	Single IP	*	
ACCESS POLICY	Servers		IPv4 address:	192.168.1.2		
	Applications & URLs		Object name:	PC2		
U THREAT	Services		✓ Allow DNS server	r to resolve this object name		
PREVENTION	Service Groups		✓ Exclude from DH	ICP service		
250	Network Objects		Reserve IP ad	dress in DHCP service for MAC		
VPN	Network Object Groups		MAC address	·		
			MAC address			
OBJECTS				Apply	× Cancel	
0						
LOGS & MONITORING						
0	Internet connected					
10	internet connected					

設定完成後按 Apply 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。

3-1. 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。



Port 對應方式 (外部 IP Port 對應到內部 IP Port, 此設定會將所有連線到外部 IP Port 轉到內部 IP Port)

架構圖如下:





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

NEW SERVER WIZ	ARD STEP 1: SERVER TYPE	×
✓ Web Server	HTTP (80, 8080), HTTPS (443)	
Mail Server	. /	
DNS Server		
FTP Server	EDIT WEB SERVER PORTS ×	
Citrix Server	✓ HTTP 80, 8080	
PPTP Server	✓ HTTPS 443	
Other Server		
	✓ Apply × Cancel	
Cancel	Back	Next



設定網頁伺服器內容:

NEW SERVER W	VIZARD STEP 2: SERVER DEFINITIONS	×
Name:	WebServer	
IP address:	172.16.1.100	\equiv
Comments:	web server	
 Allow DNS s Exclude from Reserve 	erver to resolve this object name m DHCP service IP address in DHCP service for MAC	
MAC add	dress:	Back Next

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:

NEW SERVER WIZARD STEP 3: ACCESS		×
This server is accessible from the following zones:		
All zones (including the Internet)		
Only trusted zones (my organization)		
V LAN		
Remote Access VPN users		
✓ Remote VPN sites		
O Manually configure access policy to this server		
Ping to this server		
✓ Allow access to the server using ICMP (ping)		
Logging traffic to this server		
✓ Log blocked connections		
Log accepted connections		
Cancel	Back	Next

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

O 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:

NEW SERVER WIZARD STEP 4: NAT	×
NAT Settings	
Hide Behind Gateway (Port Forwarding)	
Traffic to the gateway's external IP address on the specified ports will be forwarded to this server	
• Static NAT: 210.243.191.65	
Traffic to the specified IP address and ports will be forwarded to this server	
\checkmark Hide outgoing traffic from the server behind this IP address	
🔘 No NAT	
The server's IP address is accessible from the Internet	
Redirect from port:	
Port translation is only available for a single-port server	
Advanced	
\checkmark Force translated traffic to return to the gateway	
Allow access from internal networks to the external IP address of the server via local switch	
Cancel Back Finish	

O 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)

- O No NAT
- \rightarrow \pm NAT

Redirect from port : [____]

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

Check Po 1500 Ap	oint pliance					🛥 admin 🗗 Log Out 📀 Hel	A Search
номе	Firewall Blade Control	Servers Definition and A	CCCESS: Access permissions and NAT for Q ★ New ✓ Edit × Dei	server objects			🚔 Print 🚱 Help
	Policy	Name My PC	Server Type	IP Address	Ports	Public IP Address	Comments BitTorrent access
DEVICE	NAT	WebServer	😼 Web Server	172.16.1.100	TCP: 80, 443,8080	210.243.191.65	web server
ACCESS POLICY IHREAT PREVENTION VPN USERS & OBJECTS & LOGS & MONITORING	User Awareness Blade Control QoS Blade Control Policy SSL Inspection Policy Exceptions Advanced	MailSever	👪 Mai Server	172-19-1.200	TCP: 25, 110,143	210.245.191.65	



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。

Check P 1500 Ap	oint opliance							<u>ा</u>	🖬 admin 🗗 Log Out 🧿 Help / Support 🔍 Search	
HOME	 Frewall Blade Control Policy Servers NAT User Awareness 	NAT: Conf Outgoing ON NAT Rule	figure NAT (Network Ar Traffic Hide internal networ S v Server (forwarding	idress Translation) for ou ks behind the Gateway's rule)	tgoing traffic and forw	arding NAT rules for inc	oming traffic			Help
POLICY	Blade Control	* New No.	Criginal Source	elete Enable Original Destinati	Original Service	Translated Sourc	Translated Destin	Translated Servic	Comment	
0 THREAT	Blade Control	▼ Auto	o Generated Forwardi	ng Rules						
PREVENTION	Policy	1	* Any	210.243.191.65	🔀 Custom, ICMP	* This Gateway	My_PC	 Original 	Generated forwarding rule: My_PC Servers page	
24-0	 SSL Inspection 	2	My_PC	* Any	* Any	210.243.191.65	 Original 	 Original 	Generoted forwarding rule: My_PC Servers page	
VPN	Policy	3	* Any	210.243.191.65	🕃 Web, ICMP	 This Gateway 	R WebServer	 Original 	Generated forwarding rule: WebServer Servers page	
	Exceptions	4	Row WebServer	* Any	· Any	210.243.191.65	 Original 	 Original 	Generated forwarding rule: WebServer Servers page	
22	Advanced	5	· Any	210.243.191.65	🕃 Mail, ICMP	 This Gateway 	Ra MailServer	 Original 	Generated forwarding rule: MailServer Servers page	
OBJECTS		6	RailServer	· Any	· Any	210.243.191.65	 Original 	 Original 	Generated forwarding rule: MailServer Servers page	
LOGS & MONITORIN		4								•

3-2. 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。





Port 對應方式 (外部 IP Port 對應到內部 IP Port ,此設定會將所有連線到外部 IP Port 轉到內部 IP Port) 架構圖如下:

USB 3.0 1 2/Sync 3 4	5 WAN
	CONSOLE CONSOLE
Mail Server : 172.16.1.200	WAN: 210.243.191.65
Default Gateway : 172.16.1.1	Default Gateway : 210.243.191.1
	對應到Mail Server: 172.16.1.200

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

NEW SERVER WIZARD STE	P 1: SERVER TYPE		×
Web Server			
Mail Server SMTP (25), IMAP (143), PC	DP3 (110) Edit	
DNS Server		Ĥ	
FTP Server	EDIT MAIL SE	RVER PORTS X	1 I.
Citrix Server			
PPTP Server	SMTP	25	
Other Server	✓ POP3	110	
	✓ IMAP	143	
			_
		✓ Apply X Cancel	
Cancel		Back	Next



設定郵件伺服器內容:

NEW SERVER V	VIZARD STEP 2: SERVER DEFINITIONS	
Name:	MailServer	
IP address:	172.16.1.200	\equiv
Comments: ✓ Allow DNS :	server to resolve this object name	
Reserve	IP address in DHCP service for MAC [®]	
Consul		Deels Neut

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:

NEW SERVER WIZARD STEP 3: ACCESS	×
This server is accessible from the following zones:	
All zones (including the Internet)	
Only trusted zones (my organization)	
✓ LAN	
Remote Access VPN users	
✓ Remote VPN sites	
O Manually configure access policy to this server	
Ping to this server	
✓ Allow access to the server using ICMP (ping)	
Logging traffic to this server	
✓ Log blocked connections	
Log accepted connections	
Cancel Back Next	

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

O 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:

NEW SERVER WI	ZARD STEP 4: NAT	×
NAT Settings		
O Hide Behind	Gateway (Port Forwarding)	
Traffic to the this server	gateway's external IP address on the specified ports will be forwarded	d to
• Static NAT:	210.243.191.65	
Traffic to the	specified IP address and ports will be forwarded to this server	
No NAT The server's	IP address is accessible from the Internet	
 Port translat 	ion is only available for a single-port server	
Advanced		
✓ Force transla	ited traffic to return to the gateway	
Allow access switch	from internal networks to the external IP address of the server via loc	al
Cancel	Back Fin	iish

O 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)

- O No NAT
- \rightarrow \pm NAT
 - Redirect from port : [_____]

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

Check P 1500 Ap	oint opliance					🛥 admin 🗗 <u>Log Out</u> 🥐 <u>Hel</u>	g/Support Q Search
номе	 Firewall Blade Control 	Servers Definition and A Type to filter	CCCESS: Access permissions and NAT for Q ★ New ✓ Edit ★ Del	server objects ete			🚔 Print 🕢 Help
	Policy	Name	Server Type	IP Address	Ports	Public IP Address	Comments
	Servers	My_PC	Custom Server	172.16.1.10	TCP: 6881-6889	210.243.191.65	BitTorrent access
DEVICE	NAT	WebServer	R Web Server	172.16.1.100	TCP: 80, 443,8080	210.243.191.65	-
	User Awareness	MallServer	Ra Mail Server	172.16.1.200	TCP: 25, 110,143	210.243.191.65	
ACCESS	Blade Control						_
THREAT PREVENTION VPN USERS & OBJECTS LOGS & MONITORING	QoS Blade Control Policy SSL Inspection Policy Exceptions Advanced						



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。

Check P 1500 Ap	oint ppliance							1	admin E+ Log Out ? Help / Support Q. Search	
HOME BOUCE	 Firewall Blade Control Policy Servers NAT 	 NAT: Co Outgoir ON NAT Ru 	nfigure NAT (Network A ng Traffic] Hide internal networ les	ddress Translation) for ou ks behind the Gateway's	utgoing traffic and forw	varding NAT rules for inc	oming traffic			Help
ACCESS POLICY	 ✓ User Awareness Blade Control 	∎ Ne	ew Server (forwarding w 🔹 🧨 Edit 🗙 D	rule) Hide NAT rule:	5					
	✓ QoS Blade Control	No.	Original Source	Original Destinati	Original Service	Translated Sourc	Translated Destin	Translated Servic	Comment	
8 5 0	SSL Inspection Bolicy	2	My_PC	* Any 210.243.191.65	* Any Web, ICMP	 This Gateway 210.243.191.65 This Gateway 	Original WebServer	 Original Original 	Generated forwarding rule: My_PC Servers page Generated forwarding rule: My_PC Servers page Generated forwarding rule: WebServer Servers page	
USERS & OBJECTS	Exceptions Advanced	4 5 6	 WebServer Any MailServer 	 Any 210.243.191.65 Any 	* Any Mail, ICMP * Any	 210.243.191.65 This Gateway 210.243.191.65 	 Original MailServer Original 	 Original Original Original 	Generated farwarding rule: WebServer Servers page Generated forwarding rule: MailServer Servers page Generated forwarding rule: MailServer Servers page	
LOGS & MONITORIN	¢	-								•

3-3. 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。

eck Point 00 Appliance							wadmin E+ Log Out ⑦ Help / Support Q Search
Firewall Blade Control	Firewall A Outgoing * New	cccess Policy g access to the Internet → → ∠ Edit × Delete	≡ Enable [≘ Clone ♦	Customize Messages			6
Servers	No.	Source	Destination	Application / Service	Action	Log	Comment
CE NAT	▼ Auto	o Generated Rules					
User Awareness	1	* Any	() Internet	🔀 Undesired applications	Block	E Log	Standard default policy is configured in Firewall blade control page
	2	* 6.00	() Internet	+ Anv	🕀 Accept	- None	Standard default policy is configured in Firewall blade control page
Blade Control		# Cuty	U macrice				
SS Blade Control CV Blade Control AT Blade Control	3 Incoming	Finternal and VPN traffic	Enable CE Clone				
CY Blade Control QOS AT Blade Control TION Policy	3 Incoming	Edit X Delete	Enable C Cone	Service	Action	Log	Comment
CY Blade Control QOS AT HON Policy • SSL Inspection	3 Incoming * New No. • Auto	 J. Internal and VPN traffic - Edit × Delete Source Generated Rules 	Enable C Cone	Service	Action	Log	Comment
Blade Control QOS Blade Control Policy SSL Inspection Policy	3 Incoming * New No. • Auto 1	 Any Internal and VPN traffic - Edit X Delete Source o Generated Rules Any 	Enable (E Clone Destination	Service # Custom, ICMP	Action () Accept	Log — None	Comment Generated rule: Access policy for My_PC Servers page
Blade Control QoS Blade Control Policy SSL Inspection Policy Exceptions	3 Incoming * New No. • Auto 1 2	Internal and VPN traffic Edit X Delete Source o Generated Rules Any Any	Enable (E Clone Destination My_PC R_WebServer	Service # Custom, ICMP # Web, ICMP	Action Accept Accept	Log — None — None	Comment Generated rule: Access policy for My_PC Servers page Generated rule: Access policy for WebServer Servers page
SSC Blade Control CQOS AT AT Flade Control Policy SSL Inspection Policy Exceptions Advanced	3 Incoming * New No. 1 2 3	 Any Edit × Delete Source Generated Rules Any Any Any 		Service Custon, ICMP H Web, ICMP H Mail, ICMP	Action Accept Accept Accept Accept	Log - None - None - None	Comment Generated rule: Access policy for My_PC Servers page Generated rule: Access policy for WebServer Servers page Generated rule: Access policy for MaliServer Servers page
Blade Control QoS Blade Control Policy SSL Inspection Policy Exceptions Advanced	3 Incoming * New No. • Aut 1 2 3 4	 Ary Internal and VPN traffic - Edit × Delete Source Generated Rules Any Any Any LAN networks 		Service Custom, ICMP H Web, ICMP H Mail, ICMP * Any	Action Accept Accept Accept Accept Accept Accept	Log - None - None - None - None	Comment Generated rule: Access policy for My_PC [Servers page Generated rule: Access policy for WebServer Servers page Generated rule: Access policy for MailServer Servers page Default policy is configured in Firewall blade control page



Port 對應方式 (外部 IP Port 對應到內部 IP Port ,此設定會將所有連線到外部 IP Port 轉到內部 IP Port) 架構圖如下:



WAN: 210.243.191.65 Default Gateway: 210.243.191.1 取210.243.191.66 對應到MyPC: 172.16.1.50

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)

Check Pr 1500 Ap	pint ppliance						🛥 adm	in E+ Log Out ③ Help / Support
HOME DEVICE	Firewall Blade Control Policy Servers NAT	 Firewall Access Po Outgoing access t * New * No. Source * Auto General 	icy o the Internet Edit X Delete 🗮 Enabl e Des ted Rules	e 🔚 Clone 🔕 Custo stination	mize Messages Application / Service Acti	on Log	Comn	nent.
ACCESS POLICY	User Awareness Blade Control	1 * 2 *	ADD RULE: INCOMING, INTERN	IAL AND VPN TRAFFIC	destination on any service is accepted a	nd logged	×	d default policy is configured in Firewa d default policy is configured in Firewa
THREAT PREVENTION	Policy	Incoming, Inter	Source * Any	Destination * Any	Service * Any	Action Accept	Log	
VPN	SSL Inspection IP address Policy IP range Networ Exceptions Advanced	x set: 210.243.191.66 210.243.191.66/x.x.x 210.243.191.66/x.x.x <i>TER when done</i> 3 4 4	210.243.191.66 Search or type a new IP address Filter: Networks Users AD	(e.g. 10.0.1) Updatable objects	AM * - 09 : 00 AM *	✓ Apply	X Cancel	d rule: Access policy for My_PC Serv d rule: Access policy for WebServer d rule: Access policy for WebServer bolicy is configured in Firewall bilder of policy is configured in Firewall bilder
LOGS & MONITORING		3 44	Any source except	Import • New •			wg. Ucrau	n porteg in consegure diff in events builder o



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

Source	Destination	Application / Service	Action	Log (Comment
ienerated Rules					
* ADD RULE: INCOMING, IN	TERNAL AND VPN TRAFFIC				× d default po
*	Fraffic from 210.243.191.66	to any destination on any service	is accepted and logged		d default po
nter Source	Destination	Service	Action	Log	
210.243.191.66	* Any	* Any	() Ассер	t 🖹 Log	
Sol Write a comment	Search or type a new	domain or IP address (e.g. 10.0.0.1)	Q		nt
* Apply only during this t	ime: Filter: Networks Us	ers AD Updatable objects	*		d rule: Acce
* Match only for encrypt	ed traff				d rule: Acce
*	All identified use	ers	Network Object	5	ed rule: Acce
÷	Blocked_hosts	×	Network Object Group	pply X Can	cel policy is cor
* Any	* An Blocked_infecte	d_hosts	Domain	Log [Default policy is cor
	🜲 LAN networks		Local user		
	Any destination	except Import	N -		



於 New Network object 中的 [type] 選擇 Single IP

Туре:	Single IP	Single IP
IPv4 address:	172.16.1.50	Single IP
IPv6 address:		IP Range
Object name:	МуРС	IPv6 Range
✓ Allow DNS serv	er to resolve this object name	Network
✓ Exclude from D	HCP service	IPv6 Network
Reserve IP a	address in DHCP service for MAC	Domain Name
MAC addres	55:	Device

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[apply]確認

Source	Destination	Service	Action	Log
P 210.243.191.66	🖳 МуРС	* Any	H Accept	E Log
Vrite a comment				
Apply only during this tir Match only for encrypted	me: 09 : 09	00 AM 🔻 - 09 : 00 A	M	



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

Check Pe 1500 Ap	pint pliance								admin 🗗 Log Out ? Help / Support 🔍 Search	
HOME DEVICE	Firewall Blade Control Policy Servers NAT User Awareness	< NAT: Co Outgoi ON NAT RL	onfigure NAT (Network A ng Traffic Hide internal networ Iles ew Server (forwarding	dress Translation) for our the Gateway's rule)	itgoing traffic and forw external IP address	varding NAT rules for inc	oming traffic			Help
ACCESS	Blade Control	* No	ew 👻 🧨 Edit 🗙 D	elete 🗮 Enable						
THREAT PREVENTION	 QoS Blade Control Policy 	No. • A 1	Original Source uto Generated Forwardi Any	Original Destinati ing Rules	Original Service	Translated Sourc This Gateway	Translated Destin	Translated Servic Original	Comment Generated forwarding rule: My_PC Servers page Generated forwarding rule: My_PC Servers page	
VPN	SSL Inspection Policy Eventions	3	Any WebServer	* Any 	Any Web, ICMP Any	 This Gateway 210.243.191.65 	Original WebServer Original	Original Original	Generated forwarding rule: WebServer Servers page Generated forwarding rule: WebServer Servers page Generated forwarding rule: WebServer Servers page	
LOGS & MONITORING	Advanced	5	• Any	210.243.191.65 * Any	 Mail, ICMP Any 	 This Gateway 210.243,191.65 	 MailServer Original 	 Original Original 	Generated forwarding rule: MailServer Servers page Generated forwarding rule: MailServer Servers page	•

3-4. 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。

Se Quantur 1500 Ap	m Spark opliance	🛥 admin 🗗 Log <u>Out</u> 🥐 Help / Sup
∧ 2 Маноме	Firewall Blade Control Policy Sepuers	NAT: Configure NAT (Network Address Translation) for outgoing traffic and forwarding NAT rules for incoming traffic Outgoing Traffic N Hide internal networks behind the Gateway's external IP address
DEVICE ACCESS POLICY	VoIP Smart Accel	NAT Rules New Server (forwarding rule) View NAT rules
THREAT PREVENTION VPN	Blade Control COS Blade Control Policy SSL Inspection	



Port 對應方式 (外部 IP Port 對應到內部 IP Port ,此設定會將所有連線到外部 IP Port 轉到內部 IP Port) 架構圖如下:

USB 3.0 1 3 3 4	5 WAN
	CONSOLE CONSOLE
IMy_PC : 172.16.1.10	WAN: 210.243.191.65
IDefault Gateway : 172.16.1.1	Default Gateway : 210.243.191.1
	對應到My PC: 172.16.1.10

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

NEW SERVER WIZARI	STEP 1: SERVER TYPE		×
Web Server			
Mail Server			
DNS Server			
FTP Server			
Citrix Server			
PPTP Server			
✓ Other Server			
Protocol:	TCP		
TCP ports:	6881-6889		
Enter port numbe For example: 1,3,	ers and/or port ranges separated by comma 5-8,15	s	
Cancel		Back	Next

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:	My_PC	_	
IP address:	172.16.1.10	=	
Comments:	BitTorrent access		
			.
Allow DNS s Exclude from Reserve	erver to resolve this object name n DHCP service IP address in DHCP service for MAC		
Allow DNS s Exclude from Reserve MAC add	erver to resolve this object name n DHCP service IP address in DHCP service for MAC Iress:		

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:

NEW SERVER WIZARD STEP 3: ACCESS		×
This server is accessible from the following zones:		
• All zones (including the Internet)		
Only trusted zones (my organization)		
✓ LAN		
Remote Access VPN users		
✓ Remote VPN sites		
O Manually configure access policy to this server		
Ping to this server		
✓ Allow access to the server using ICMP (ping)		
Logging traffic to this server		
✓ Log blocked connections		
Log accepted connections		
Cancel	Back	Next

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

O 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:

NEW SERVER WIZARD STEP 4: NAT ×
NAT Settings
 Hide Behind Gateway (Port Forwarding) Traffic to the gateway's external IP address on the specified ports will be forwarded to this server
 Static NAT: 210.243.191.65 Traffic to the specified IP address and ports will be forwarded to this server Hide outgoing traffic from the server behind this IP address
 No NAT The server's IP address is accessible from the Internet
 Redirect from port: Port translation is only available for a single-port server
Advanced
Force translated traffic to return to the gateway
Allow access from internal networks to the external IP address of the server via local switch
Cancel Back Finish

網路地址轉換設置:

O 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)

- O No NAT
- $\rightarrow \texttt{mNAT}$

Redirect from port : [____]



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

Check Point 1500 Appli	t ance					🛥 admin 🗗 Log Out 🧿 He	p/Support Q Search
НОМЕ	 Firewall Blade Control 	Servers Definition and Ar	Q ★ New ✓ Edit × Dei	server objects			🚔 Print 🕑 Help
	Policy	Name	Sonior Tipo	ID Addrose	Deste	Dublic ID Addrose	Commente
DEVICE	Servers	My_PC	Custom Server	172.16.1.10	TCP: 6881-6889	210.243.191.65	BitTorrent access
DEVICE	NAT	WebServer	Web Server	172.16.1.100	TCP: 80, 443,8080	210.243.191.65	
ACCESS PROVENTION THREAT PROVENTION VPN 44 USERS & OBJECTS LOGS & MONITORING	User Awareness Blade Control QoS Blade Control Policy SSL Inspection Policy Exceptions Advanced	MallServer	R Mai Server	172.16.1.200	TCP: 25, 110,143	210.243,191.65	

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。

Check P 1500 Ap	oint opliance									🛥 admin 🗗 Log Out 🕐 Help / Support 🔍 Search	
HOME BEVICE	 Firewall Blade Control Policy Servers NAT 	¢	NAT: Confi Outgoing ON	igure NAT (Network Ad Traffic Hide Internal network	idress Translation) for ou is behind the Gateway's	itgoing traffic and forw external IP address	arding NAT rules for inc	oming traffic			🛛 Help
ACCESS POLICY	User Awareness Blade Control		New * New	Server (forwarding r	elete						
	✓ QoS Blade Control		No. • Auto	Original Source Generated Forwardin	Original Destinati	Original Service	Translated Sourc	Translated Destin	Translated Servic	Comment	_
VPN	SSL Inspection Policy		2	My_PC	 Any 210.243.191.65 	Any Web, ICMP	210.243.191.65 This Gateway	Original	Original Original	Generated forwarding rule: My_PC Servers page Generated forwarding rule: My_PC Servers page Generated forwarding rule: WebServer Servers page	
JUSERS &	Exceptions Advanced		4	WebServer Any	 Any 210.243.191.65 	* Any	 210.243.191.65 This Gateway 	Original MailServer	 Original Original 	Generated forwarding rule: WebServer Servers page Generated forwarding rule: MailServer Servers page	
LOGS & MONITORING			4	Re MailServer	 Arry 	• Any	210.243.191.65	• Original	• Ongiñal	oeneratea jonwarang runc. Maitserver servers page	,



第四章 線路 Fail-over 設定

4-1. 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:

Check Po 1550 Ap	int pliance	
і Номе	 Network Internet 	Internet: Manage one or more Internet connections Status: Connected DHCP WAN 192 168 100 12/24 00:06:40
DEVICE	Local Network Hotspot Routing	0% failures, 8.4ms latency Connection monitoring Edit Delete
ACCESS POLICY	MAC Filtering DNS Proxy	Add an Internet connection
THREAT PREVENTION	 System System Operations 	
VPN	Administrators Administrator Access	



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。

EW INTERNET CON	ECTION				
Configuration	Connection Mon	toring	Advanced		
Internet Configu	ition				~
Connection nam	: Inter	net2			
Interface:	LANS			•	
Connection type	DHC	>		•	
Use connecti	n as VLAN				

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)

Check Po 1550 Ap	pliance					🛥 admin 🗗 Log Out ? Help / Suj
	<	Internet: Manage one or more internet	connections			
ò	 Network 	Multiple Internet	connections			
HOME	Internet					
_	Local Network	High Availability mo	de Configure			
DEVICE	Hotspot					
DEFICE	Routing	* New 🖌 Edit 🗙 Delete 🔳	Disable 🧥 Connection M	onitoring		
	MAC Filtering	Name	Interface	Туре	Status	IP Address
ACCESS POLICY	DNS	Internet1 (primary, active)	WAN	DHCP	Onnected	192.168.100.12
~	Proxy				Failures: 0% Latency: 5.6ms	
	 System 	Internet2	LAN5	DHCP	Onnected	192.168.20.12
PREVENTION	System Operations				Failures: 0% Latency: 6.6ms	
20-0	Administrators					
VPN	Administrator Access					
	Device Details					
22	Date and Time					
USERS & OBJECTS	DDNS & Device Access					
~	Tools					
LOGS &	Certificates					
MONITORING	Installed Certificates					
	Internal Certificate					
	 Advanced 					
	High Availability					
	Advanced Settings					



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)

Check Pe 1550 Ap	oint opliance				Mir adr
HOME	 Network Internet 	Internet: Manage one or more Internet Multiple Internet	connections		
DEVICE	Local Network Hotspot Routing	High Availability mo	ie Configure Enable ^ Connection Mo	nitoring	
	MAC Filtering	Name	Interface	Туре	Status
ACCESS POLICY	DNS	Internet1 (primary, active)	WAN	DHCP	S Connected
Ô	Proxy				Failures: 0% Latency: 8.2ms
	 System 	Internet2	LAN5	MULTIPLE INTERI	Connected NET CONNECTIONS X Latency: 7.7ms
VPN	System Operations Administrators Administrator Access Device Details Date and Time			ISP Redundancy High Availab	y Ility mode
OBJECTS OBJECTS LOGS & MONITORING	DDNS & Device Access Tools • Certificates Installed Certificates			~	Apply × Cancel
	Internal Certificate				

步驟五: 選取 Load Balancing (負載模式) 模式,會顯示下圖

Check Po 1550 App	int pliance			
	<	Internet: Manage one or more Internet connection	ons	
	 Network 	Multiple Internet connec	tions	
HOME	Internet	Real Multiple Internet connec	uons	
	Local Network	Load Balancing mode Confi	gure	
	Hotspot			
DEVICE	Routing	★ New ✓ Edit × Delete	Connection Monitoria	ng
:::	MAC Filtering	Name	Interface	Туре
ACCESS POLICY	DNS	Internet1 (primary, active)	WAN	DHCP
~	Proxy			
	▪ System	Internet2 (active)	LAN5	DHCP
PREVENTION	System Operations			
24-0	Administrators			
VPN	Administrator Access			
	Device Details			
22	Date and Time			
OBJECTS	DDNS & Device Access			
	Tools			



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

Configuration	Connection I	Monitoring	Advanced		
Port Settings					~
QoS Settings					~~~~
ISP Redundancy					~
 Route traffic t In order to ro 	through this con ute traffic throu	nection by de gh this conne	fault ction you need to	add specific route	s through it
High Availabi	lity				
Upon failure according to	e of the primary o the selected pr	Internet conn iority	ection, traffic will	be routed	
Priority:	1	(The hi	gher the value, the	e lower its priority	
Load Balanci	ng				
Traffic will b	e distributed au	tomatically ad	cording to the co	nfigured load bala	ncing weights
Weight:	30	(75% of	f the total weight)		
NAT Settings					~
DHCP Settings					····· v

設定完成後按 Apply 完成設定



第五章 VPN 連線設定

5-1. 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)

網路架構圖示:



A點設定:

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

<	VPN Sites: Configure remote VPN sites
 Remote Access 	
Blade Control	Type to filter Q ★ New ➤ Edit X Delete ≡ Enable/Disable ✓ Test
Remote Access Users	Site Name
Connected Remote Users	VPNA
Authentication Servers	
Advanced	
✓ Site to Site	
Blade Control	
VPN Sites	
Community	
VPN Tunnels	
Advanced	
 Certificates 	
Trusted CAs	
Installed Certificates	
Internal Certificate	

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)。

Type to filter 🛛 🔍 米 New	🖌 Edit 🗙 Delete 🗮 Disable 🔉	🟒 Test		
Site Name	NEW VPN SITE			×
No VPN sites were found. Add a new V				
	Remote Site Encryption A	dvanced		.
	Site name:	VPNA		1
	Connection type:	Host nar	ne or IP address 🔻	
	IP address	192.168.	200.1	
	Behind static NAT			
	O Host name			
	Authentication		~	Н
	• Pre-shared secret			
	Password:			Н
	Confirm:			
	○ Certificate			Н
	Match certificate by DN			
	Remote Site Encryption Domain		~	1
	Encryption domain:	Define r	emote network topology manually	
	🔆 New 🗙 Remove 🛛 🔩 Select.			
	Object Name	Addroscos		
			✓ Apply × Cancel	



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。

Pre-shared secret	
Password:	••••••
Confirm:	
Certificate	
Match certificate by DN	
emote Site Encryption Domain	
emote Site Encryption Domair	Define remote network topology manually
emote Site Encryption Domain ncryption domain: * New X Remove 🔩	Define remote network topology manually
emote Site Encryption Domain ncryption domain: * New × Remove • * Object Name	Define remote network topology manually
Remote Site Encryption Domain incryption domain: * New X Remove Object Name No items were found	Define remote network topology manually
emote Site Encryption Domain ncryption domain: * New X Remove Object Name No items were found xclude networks	Define remote network topology manually
Remote Site Encryption Domain Encryption domain: <u>* New</u> × Remove E _k S Object Name No items were found Exclude networks	Define remote network topology manually

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 Apply 繼續。

NEW NETWORK OBJE	ст	×	NEW NETWORK OBJE	ЕСТ	×
Type: Network address: Subnet mask: Object name:	Network 192.168.1.0 255.255.255.0 CP2_LAN1 CP2_LAN1		Type: Network address: Subnet mask: Object name:	Network 192.168.2.0 255.255.255.0 CP2_LAN2 CP2_LAN2	
	 Apply 	× Cancel		✓ Apply 🗙 Car	ncel



新增後按 Apply 完成。

Authentication	······
• Pre-shared secret	
Password:	
Confirm:	
Certificate	
Match certificate by DN	
Remote Site Encryption Domain	~
Encryption domain:	Define remote network topology manually
Ӿ New 🗙 Remove 🛛 🔩 Selec	:t
Object Name	IP Addresses
CP_LAN	192.168.1.0/255.255.255.0
CP2_LAN3	192.168.2.0/255.255.255.0
Exclude networks	· · · · · · · · · · · · · · · · · · ·
	✓ Apply × Cancel

B點設定:

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

<	VPN Sites: Configure remote VPN sites
 Remote Access 	
Blade Control	Type to filter Q 🔆 New 🖍 Edit X Delete 🗮 Enable/Disable 🛃 Test
Remote Access Users	Site Name
Connected Remote Users	VPNA
Authentication Servers	
Advanced	
 Site to Site 	
Blade Control	
VPN Sites	
Community	
VPN Tunnels	
Advanced	
Certificates	
Trusted CAs	
Installed Certificates	
Internal Certificate	

在 Site Name 中,命名此 VPN Site 的名稱。在 IP Address 中輸入對端設備的 IP:172.16.1.1 (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)

Type to filter Q * New	🛚 🇪 Edit 🗙 Delete 🗮 Disable	∠ Test
Site Name	NEW VPN SITE	×
No VPN sites were found. Add a new V		
	Remote Site Encryption	Advanced
	Site name:	VPNA
	Connection type:	Host name or IP address 🔹
	IP address	172.16.1.1
	Behind static NAT	
	◯ Host name	
	Authentication	^
	• Pre-shared secret	
	Password:	
	Confirm:	
	O Certificate	_
	Match certificate by DN	
	Remote Site Encryption Domain	······
	Encryption domain:	Define remote network topology manually
	🔆 New 🗙 Remove 📑 Select	
	Object Name	▼ Addraccoc
		✓ Apply X Cancel



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。

Authentication	^
Pre-shared secret	
Password:	
Confirm:	
Certificate	
Match certificate by DN	
Remote Site Encryption Domain	····· .
Remote Site Encryption Domain	Define remote network topology manually
Remote Site Encryption Domain Encryption domain:	Define remote network topology manually
Remote Site Encryption Domain Encryption domain: * New X Remove S S Object Name	elect IP Addresses
Remote Site Encryption Domain Encryption domain: * New X Remove S Object Name No items were found	Define remote network topology manually elect IP Addresses
Remote Site Encryption Domain Encryption domain: X New X Remove X Object Name No items were found X clude networks	Define remote network topology manually elect IP Addresses
Remote Site Encryption Domain Encryption domain:	Define remote network topology manually elect IP Addresses

將要存取的對端子網10.10.10.0/24及10.10.11.0/24(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 Apply 繼續。

NEW NETWORK OBJECT		×	NEW NETWORK OBJECT		×
Type: Network address: Subnet mask: Object name:	Network 10.10.10.0 255.255.255.0 CP1_LAN1		Type: Network address: Subnet mask: Object name:	Network • 10.10.11.0 255.255.255.0 CP1_LAN2 CP1_LAN2	
	✓ Apply ×	Cancel		✓ Apply × Ca	ancel



新增後按 Apply 完成。

Confirm:	••••••			
Certificate				
Match certificate by D	۷			
emote Site Encryption Do	main ······			
ncryption domain:	Define remote network topology manually			
★ New X Remove	Ex Select			
Object Name	IP Addresses			
CP1_LAN2 10.10.11.0/255.255.255.0				
CP2_LAN 🔓 10.10.10.0/255.255.255.0				

確認可以從 B 點 ping 到 A 點 LAN

C:\Users\May Chen>ipconfig
Windows IP 設定
乙太網路卡 乙太網路:
連線特定 DNS 尾碼
ⅠⅠ. 命令提示字元
C:\Users\May Chen>ping 10.10.10.1
Ping 10.10.10.1 (使用 32 位元組的資料): 回覆自 10.10.10.1: 位元組=32 時間=7ms TTL=63 回覆自 10.10.10.1: 位元組=32 時間=2ms TTL=63 回覆自 10.10.10.1: 位元組=32 時間=2ms TTL=63
10.10.10.1 的 Ping 統計資料: 封包: 已傳送 = 3,已收到 = 3,已遺失 = 0 (0% 遺失), 大約的來回時間 (毫秒): 最小值 = 2ms,最大值 = 7ms,平均 = 3ms Control-C AC
C:\Users\May Chen>ping 10.10.11.1
?ing 10.10.11.1 (使用 32 位元組的資料): 回覆自 10.10.11.1: 位元組=32 時間=7ms TTL=63 回覆自 10.10.11.1: 位元組=32 時間=2ms TTL=63 回覆自 10.10.11.1: 位元組=32 時間=2ms TTL=63
10.10.11.1 的 Ping 統計資料: 封包: 已傳送 = 3,已收到 = 3,已遺失 = 0 (0% 遺失), 大約的來回時間 (毫秒):



5-2. SSL VPN 設定

5-2-1. 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。

NEW LOCAL USER			×			
Remote Access	SSL VPN Bookmarks					
User name:	User01					
Password:						
Confirm:						
Email:	Field is not mandatory					
Phone number:	Field is not mandatory					
Comments:	Field is not mandatory					
Temporary user						
Remote Access permissions						
		🗸 Apply	× Cancel			

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。


5-2-2. SSL-VPN 用戶端登入

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:

\leftarrow C	▲ 不安全 https://210.243
	SSL Network Extender
	Check Point SSL Network Extender requires the download of an ActiveX / Java control to your browser. The entire process will take approximately 1 minute, depending on your connection speed. If a security box appears, you must click Ves to approve the security certificate to initiate the download of the required ActiveX / Java control. Check Point SSL Network Extender will be displayed upon the completion of the ActiveX / Java control download and automatic installation. SSL Network Extender Login - 個人 - Microsoft Ed – X M 不安全 https://210.243 / extender.html A ^N ab SSL Network Extender
	Please enter your user name and password User Name: Password: Click for using SecurID © 2017 Check Point Software Technologies Ltd. OK Cancel

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

S ^{Quantus} 1500 Ap	n Spark opliance				wadmin E+ Log_Out ? Help / Support Q Search
-	<	Advanced Settings: Manage very advanced settings of the device			📇 Print 🚱 He
a	 Network 	A Changing these advanced settings can be harmful to the stability, security and perf	formance of the appliance		
HOME	Internet	443 K Fdit Restore Defaults			
_	Local Network		7	14-1	Description
DEVICE	Hotspot	Autobute Name	Туре	value	Description
	Routing	VPN Remote Access - Remote Access port	port	443	Select the port to which Remote Access clients connect, and SSL VPN Network extender portal uses
:::	MAC Filtering	VPN Remote Access - Reserve port 443 for port forwarding	bool	false	Reserving port 443 for port forwarding (port 443 will not be used for Remote Access and SSL VPN Network extender)
ACCESS POLICY	DNS				
\$	Proxy				
THREAT	 System 				
PREVENTION	System Operations				
220	Administrators				
VPN	Administrator Access				
	Device Details				
22	Date and Time				
OBJECTS	DDNS & Device Access				
~	Tools				
LOGS &	 Certificates 				
MONITORING	Installed Certificates				
	Internal Certificate				
	 Advanced 				
	High Availability				
	Advanced Settings				



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

VPN REMOTE ACCESS		×
Select the port to which remote and SSL VPN Network extended	e access clients connect, r portal uses	
Remote Access Port: 1144	3	
Reserve port 443 for port fo	orwarding	
Restore Defaults	🗸 Apply	× Cancel

5-3. Check Point Remote VPN 設定

5-3-1. 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 Check Point VPN clients 選項打 勾。

Se Quantur 1500 Ap	n Spark opliance	
	<	VPN Remote Access Control
*	 Remote Access 	
HOME	Blade Control	On Remote Access On Access On Access
	Remote Access Users	Static IP for Remote Access: 210.243.191.65
	Connected Remote Users	O Off
DEVICE	Authentication Servers	 Allow traffic from Remote Access users
:+:	Advanced	✓ Log traffic from Remote Access users
ACCESS POLICY	 Site to Site 	Require users to confirm their identity using two-factor authentication Configure
~	Blade Control	VPN Remote Access users can connect via:
THREAT	VPN Sites	Check Point VPN clients
PREVENTION	Community	Connecting laptops/desktops with Check Point's VPN client software How to connect
22.0	VPN Tunnels	Mobile client
VPN	Advanced	Enable VPN remote access mobile clients to connect via Check Point Mobile VPN client How to connect
	 Certificates 	SSL VPN Manage SSL VPN Bookmarks Certificate authentication
22	Trusted CAs	Enable VPN remote access clients to connect via SSE VPN How to connect
OBJECTS	Installed Certificates	WINDOWS VPN Client L2TP pre-shared key Enable VPN remote access clients to connect via native VPN client (L2TP) How to connect
0	Internal Certificate	
LOGS &		
MONTORING		



5-3-2. 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。

PRODUCTS	SOLUTIONS SUPPORT & SERVICES	PARTNERS RESOURCES	Contect Us Support Center Sign In Blog Q 🔀
Windows and Mac	Android and iOS	Browser	Linder Attack Connact
Remote Access Clien Windows and Mac	t for every line and the second secon		
VPN Client VPN Auto-Connect Multi-Factor Authentication Support Secure Hotspot Registration Compliance Scanning Central Management	-	A characterize (a second seco	-
VIEW DATASHEET Remote Access for Windows 7, 8.1, 10 and 11)	lows	DOWNLOAD	

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。

PRODUCTS	SOLUTION	SUPPORT & SERVICES	PARTNERS	RESOURCES
Support Center > Search F	lesults > Download Details			
Search Support Center		٩		
Downloa	ad Details			
Downtot				
E86.50 Check Point R	emote Access VPN Clients for Wind	lows		
My Favorites				Download
Details				
File Name	E86.50_CheckPointVPN.msi			
Product	Check Point Mobile, SecuRemote, E	ndpoint Security VPN		
Version	E86			
Minor Version	E86.50			
OS	Windows			
Build Number				
Show more details 🗸				
Having problems downloar	ling the file? Click here for help.			
Download Agre	ement			
PLEASE READ TH BY CLICKING ON	IS AGREEMENT CAREFULLY. THE "DOWNLOAD" BUTTON, YOU EXPRESSI	LY AGREE TO BE BOUND BY THE TERMS AND COND	DITIONS OF THIS DOWNLOAD AGRE	EMENT.
This Software Download	Agreement ("Agreement") is between you	(either as an individual or company) and		
Check Point Software Te	chnologies Ltd. ("Check Point"), for the so	oftware and documentation provided by		
this Agreement ("Softw	are"].			



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。

🖟 Check Point VPN Installation Wizar	d		_		\times
Client Products Choose a product to install		0	СНЕ	СК РО	
Endpoint Security VPN Enterprise Grade Remote Access Cl Security Features (Recommended for	ient, including basi or SecureClient rep	c Endpoint blacement).			
Check Point Mobile Enterprise Grade Remote Access Cl	ient.				
O SecuRemote Basic Remote Access Client.					
	Back	Nevt		Cance	
	Duck	NEXI		Carrot	

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。



Help



等待設定完成後再點 Next 進到下一步。

😚 Site Wizard	×
Resolving Site Name	
Please wait while the Site Name is being resolved	
This may take several minutes, depending on the speed of your network connection.	

Back	Next	Cancel	Help

若有創建多個 Site的VPN 的話,選擇欲連線的 VPN Site。

😚 Check Point End	point Security	- 🗆 ×
Endpoint	Security	SOFTWARE TECHNOLOGIES LTD.
Site: Authentication	210.243.191.65 ▼ Tead-VFN 220.128 210.243 (Rew Site)	I.
Please provide a user r Username:	name and password to authenticate	9
Password:		<u> </u>
Connect	Cancel Help	
elected Login Option: V	/PN Client	Change Login Option Setting

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

	point security	- U X
Endpoint	Security [.]	SOFTWARE TECHNOLOGIES LTD.
Site:	210.243.	
Authentication		
Please provide a user r Username:	name and password to authenticate	
Please provide a user i Username: Password:	name and password to authenticate kevin ••••••••••	
Please provide a user r Username: Password: Connect	ame and password to authenticate kevin ••••••••• Cancel Help	



5-4. L2TP VPN 設定

5-4-1. 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。

		Windows VPN Client	L2TP pre-shared key		
~	Ŧ	Enable VPN remote access clie	nts to connect via native	VPN client (L2TP)	How to connect

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。

WINDOWS VPN CLIENT (L2TP) SETTINGS					
L2TP pre-shared key	abc12345				
		V OK	× Cancel		



5-4-2. L2TP VPN 客戶端設定

進到 Windows 的 VPN 中,點選新增 VPN 連線。

設定	
命 首頁	VPN
マック マック マック マック マック マック マック マンジョン マンシン マンジョン マンシン マンジョン マンシン マンジョン マンシン マンシン マンシン マンシン マンシン マンシン マンシン マン	→ 新増 VPN 連線
網路和網際網路	
角	進階選項
	允許計量付費網路上的 VPN
n Wi-Fi	● 開啟
臣 乙太網路	漫遊時允許 VPN
☆ ☆	, 一,
% VPN	
(l) 行動熱點	
Proxy	

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。

新增 VPN 連線			
VPN 提供者			
Windows (內建)	~		
連線名稱			
CP_L21P			
伺服器名稱或位址			
210.243.			
VPN 類型			
L2TP/IPsec (使用預先共用金鑰)	~		
••••••			
登入資訊的類型			
使用者名稱與密碼	~		
使用者名稱 (選擇性)			
kevin			
<u>家</u> 碼 (羅擇性)			
•••••			
•••••			
●●●●●●●●			
●●●●●●●			



點選右邊變更介面卡選項。

		—	٥	×
VPN				
	相關設定			
+ 新増 VPN 連線	變更介面卡選項			
oxo CP_L2TP				
允許計量付費網路上的 VPN	來自網站的說明			
na n				
滑遊時允許 VPN				
	取得協助			
	🛓 提供意見反應			

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。

■ CP_L2TP 内容 ×
一般 選項 安全性 網路功能 共用
VPN 類型(T):
使用 IPsec 的第二層通道通訊協定 (L2TP/IPSec) V
遭階設定(S) 資料加密(D):
可省略加密 (即使沒有加密也要連線) 🛛 🗸 🗸
驗證 ○ 使用可延伸的驗證通訊協定 (EAP)(E) ───────────────────────────────────
 ✓ 未加密的密碼 (PAP)(U) ✓ Challenge Handshake 驗證通訊協定 (CHAP)(H) ✓ Microsoft CHAP Version 2 (MS-CHAP v2) □ 自動使用我的 Windows 登入名稱及密碼 (及網域,如果 有的話)(A)
確定 取消



回到 VPN 中,點選連線後顯示已連線代表已成功建立 L2TP VPN。

設定	
☆ 首頁	VPN
尋找設定 の	+ 新増 VPN 連線
網路和網際網路	
₿ 狀態	CF_L2TF 已連線
na Wi-Fi	進階選項 中斷連線
空 乙太網路	進階選項
♀ 撥號	公許計量付费網路上的 VPN
∞ VPN	
✤ 飛航模式	漫遊時允許 VPN
(ゆ) 行動熱點	
Proxy	



第六章 網路頻寬管理

6-1. 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)

6-1-1. 依政策作頻寬管理

I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。

G ^{• Quantu} 1500 Aj	m Spark opliance						🖬 admin 🗗 Log Out 💽 Help / Support 🔍 Search
номе	Firewall Blade Control	Firewall Access Policy Outgoing access to the Internet * New * Edit × Del	ete 🗮 Disable 👍 Gione Ö Customize Messages				9 H
CE DEVICE	Servers	No. Source Auto Generated Rules	Destination	Application / Service	Action	Log	Comment
ACCESS POLICY	VoIP Smart Accel	1 * Any 2 * Any	🚱 Internet	Undesired applicationsAny	C Blos	ept – None	Standard default policy is configured in Firewall blade control page Standard default policy is configured in Firewall blade control page
THREAT PREVENTION	User Awareness Blade Control QoS	Incoming, Internal and VPN traf	ADD RULE: OUTGOING ACCESS TO THE INTERNET Traffic from VPN Remote Access to LAN r	networks of FTP Protocol is accepted	d and logged	×	
VPN	Blade Control Policy	Auto Generated Rules Mo. Source Auto Generated Rules Mo. Source	Source Destination Source Access LAN networks	Application / Service	Action Accept	Log	Comment Generated rule: Access policy is configured in Remote Access page
USERS & OBJECTS	SSL inspection Policy Exceptions	2 VPN Sites 3 LAN networks 4 Any	Write a comment Apply only during this time: 09	AM • - 09 : 00 AM •			Generated rule: Access policy is configured in VPN Site to Site page Default policy is configured in Firewall blade control page Default policy is configured in Firewall blade control page
LOGS & MONITORIN	Advanced		Limit download traffic of applications to: 10240 Kbp Limit upload traffic of applications to: 5120 Kbp	25			
					✓ Apply	X Cancel	

完成後如下圖。

Firewall A	irewall Access Policy								
Outgoing access to the Internet									
+ New ▼ 🖍 Edit 🗙 Delete Ξ Disable (Ξ Clone 🎯 Customize Messages									
No.	Source	Destination	Application / Service	Action	Log	Comment			
▼ Man	ual Rules								
1	🗱 VPN Remote Access	LAN networks	FTP Protocol	Accept	E Log				
▼ Auto	Generated Rules								
2	* Any	🚱 Internet	😭 Undesired applications	🖨 Block	🗐 Log	Standard default policy is configured in Firewall blade control page			
3	* Any	Internet	* Any	🔁 Accept	— None	Standard default policy is configured in Firewall blade control page			
3	* Any	() Internet	* Any	Accept	— None	Standard default policy is configured in Firewall blade			



6-1-2. 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

G ^{• Quantus} 1500 Ap	m Spark opliance						wadmin E+ Log Out 🕐 Help / Support Q. Search
номе	 Firewall Blade Control 	Firewall Access Policy Outgoing access to the Internet New Control C		•			
DEVICE	Servers	No. Source Auto Generated Rules	Destination	Application / Service	Action	Log	Comment
ACCESS POLICY	VoIP Smart Accel • User Awareness	1 * Any 2 * Any 3 * Any	Internet Winternet ADD RULE: OUTGOING ACCESS TO THE INTERNET	¥ Undesired applications	Block Gons GAccept	E Log	Standard default policy is configured in Firewall blade control page Generated rate: Limit konstantific consuming applications to undefined Standard default policy is configured in Firewall blade control page
THREAT PREVENTION	Blade Control • QoS Blade Control	No. Source	Traffic from 192.168.1	125 to the Internet of YouTube is accepted and k Application / Service	Action Log		Comment
VPN	Policy • SSL Inspection Policy Exceptions	Auto Generated Rules Auto Generated Rules WPN Remote Acco Average VPN Sites Auto According to the second se	gl 192.168.1.125 write a comment Apply only during this time:	9 : 00 AM v - 09 : 00 AM v	Accept		Generated rule Access policy is configured in Remote Access page Generated rule Access policy is configured in VPN SRE to Site page Default policy is configured in Frewall blade control page
LOGS & MONITORING	Advanced	4 * Any	Imit upload traffic of applications to: Imit upload traffic of applications to:	ingen 2044 kbps	✓ Apply :	c Cancel	Default policy is configured in Firewall blade control page

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。

EDIT RULE: OUTGOING ACCESS TO THE INTERNET									
	Traffic from 192.1	68.1.125 to the Inte	ernet of YouTube is accepted	and logged					
Source	Destination		Application / Service	Action	Log				
🖳 192.168.1.125	🚱 Internet		You You Tube	🕀 Accept	🖹 Log				
Write a comment			youtube		×				
	1		Common Categories Cu	stom Applications	Services				
Apply only during this t	ime:	09 : 00 A	YouTube						
 Limit download traffic of 	of applications to:	42949 Kbps							
 Limit upload traffic of a 	pplications to:	42949 Kbps							
						Tance			
			Any application / servic	e except	New 🔻				



完成後如下圖。

S ^{Quantu} 1500 Ap	m Spark ppliance							🛥 admin 🗗 Log Out ? Help / Support	
а номе	 Firewall Blade Control 	Firewall Ac Outgoing	access Policy	r를 Clone : 혀 Customize Messages					
DEVICE	Policy Servers NAT	No.	Source ual Rules	Destination	Application / Service	Action	Log	Comment	
ACCESS POLICY	VoIP Smart Accel	1 • Auto	🖳 192.168.1.125 Generated Rules	Internet	🚜 YouTube	😗 Accept	🗐 Log		
	 User Awareness Blade Control 	2 3 4	* Any * Any * Any	Internet Internet Internet	Indesired applications If Bandwidth consuming applications Any	Block Accept Accept	Log	Standard default policy is configured in Fire Generated rule: Limit bandwidth consuming Standard default policy is configured in Fire	
VPN	QoS Blade Control Policy	Incoming, Internal and VPN traffic							
USERS &	SSL Inspection Policy	No.	Source Generated Rules	Destination	Service	Action	Log	Comment	
OBJECTS	Exceptions Advanced	1	🕸 VPN Remote Access	* Any * Any	* Any * Any	AcceptAccept	E Log	Generated rule: Access policy is configured in Generated rule: Access policy is configured in	
LOGS & MONITORIN	d	3	 LAN networks * Any 	* Any * Any	* Any * Any	Accept Block	- None	Default policy is configured in Firewall blade Default policy is configured in Firewall blade	

第七章 系統備份設定

7-1. 更新系統韌體

開啟瀏覽器,輸入 https://ip address:4434,登入 Quantum Spark 1530 首頁









點選 DEVICE \rightarrow Manual Upgarde

Check Poi 1530 App	int pliance		🖬 admin E+ Log Out 😗 Help / Support 🔍 Search	
		System Operations: Manage your fir	mware version and backup your appliance	🕜 Help
ò	 Network 	Appliance		~
HOME	Internet	Delast	O houth and hour	
	Local Network	Repoot	Repoor the appliance	
DEVICE	Hotspot	Default Settings	Restore factory default settings but keep the current firmware version	
	Routing	Factory Defaults	Revert to the factory default image and settings.	
===	MAC Filtering		The factory firmware version is R80.20.15 (992001653)	
ACCESS POLICY	DNS	Firmware Upgrade		~
\$	Proxy	The current firmware version is R80).20.15 (992001653)	
THREAT	- System	🔹 🚺 A new firmware version is availa	ble: 1500_R80.20.40_992002691. Upgrade Now More Information	
PREVENTION	System Operations	Configure automatic upgrades		
24.0	Administrators	Manual Upgrade	Revert to Previous Image	
VPN	Administrator Access	Backup and Restore System Settin	ne	~
	Device Details	Periodic backup is OFF Settings	5*	
22	Date and Time	Create Backup File	Restore	
OBJECTS	DDNS & Device Access	a ave been print		
~	Tools			
LOGS &	Certificates			
MONITORING	Installed Certificates			
	Internal Certificate			
	 Advanced 			
	High Availability			
< →	Advanced Settings			
(Connected		🛓 Upgrade available 🛭 Update pending 🛇	02:38 PM

點選 Check Point Download Center

SOFTWARE UPGRADE WIZARD	×
Welcome to the Check Point 1530 Appliance Upgrade Wizard	
The Check Point 1530 Appliance Upgrade Wizard helps you upgrade the appliance to the latest software.	
You can download the latest software from the Check Point Download Center.	
Cancel Help < Back	Next >



選擇韌體版本

💆 СНЕСК РС	DINT	PRODUCTS	SOLUTION	SUPPORT & SERVICES	PARTNERS	RESOURCES	Q
pport Center > Downloads	& Documenta	ation - Quantum > 15	00				
earch Support Center				Q			
1500							
1500							
Home	Downlo	ads Do	ocuments				
	(53)		(92)				
Model	Down	loads					
All	Showin	g 1 to 20 of 53 entries				Show 20 🗸 entries	
1500							
Version	1. CF	ieck Point 1500 App	liance package R80	0.20.01 build 992000872 for R80 Sr	nartUpdate		
A11	2. Ch	ieck Point 1500 App	liance package R80	0.20.01 build 992000899 for R80 Sr	nartUpdate		
	3. Ch	ieck Point 1500 App	liance package R80	0.20.02 build 992000936 for R80.20	SmartUpdate		
R80 (EUL)	4. Ch	ieck Point 1500 App	liance package R80	0.20.05 build 992001134 for R80.20	SmartUpdate		
Os	5. CH	ieck Point 1500 App	liance package R80	0.20.05 build 992001169 for R80.20	SmartUpdate		
		eck Point 1500 Apr	liance package R80	0.20.05 build 992001208 for R80.20	SmartUpdate		
All	6. Ch	IEEK FOILT 1500 App					
All Gaia	6. CH	eck Point 1500 App	liance package R80	0.20.10 build 992001433 for R80.20	SmartUpdate		

點擊 Download ,等待下載完成





點選 Next

SOFTWARE UPGRADE WIZARD	×
Welcome to the Check Point 1530 Appliance Upgrade Wizard	
The Check Point 1530 Appliance Upgrade Wizard helps you upgrade the appliance to the latest software.	
You can download the latest software from the Check Point Download Center.	
Cancel Help < Back Nex	xt >

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

SOFTWARE UPGRAD	EWIZARD			×
Upload Softwar	re			
Click Browse to lo Software file nam fw1_vx_dep_R80_	ocate the software file to upload. tes end with an .img extension. For example: .992000668_20.img.			
Software file:	fw1_vx_dep_R81_10_00_996000558.im	Browse		
Upload				
Cancel He	lp		< Back	Next >
.	0			
SOFTWARE UPGRAD	E WIZARD			×
Upload Softwar	re			
Click Browse to lo Software file nam fw1_vx_dep_R80_	ocate the software file to upload. nes end with an .img extension. For example: .992000668_20.img.			
Software file:	Select an image file	Browse		
Upload				
Upload progress:	: 🕑 Upload finished			
		and and		
			and and a second	
Cancel He	p		< Back	Next >



確認版本資訊無誤後點選Next

SOFTWARE UPGRADE WIZARD	×
Upgrade Settings	
Version Information The current software version is R80.20.15 (992001653) [Oct 27 2020] You are about to upgrade the appliance to software version R81.10 (996000558). Click 'Next' to start the upgrade. This process may take few minutes.	
Cancel Help < Back	vext >

等待更新(約3分鐘)

SOFTWARE UPGRADE WIZARD	×
Upgrading	
Performing step 1/2	
2%	
) Initializing upgrade process Installing new image	
Cancel Help	



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

SOFTWARE UPGRADE WIZARD							
Upgrading							
Performing step 2/2							
100%							
Initializing upgrade process							
Installing new image							
Upgrade complete.							
Please wait while the appliance reboots. Please do not pull out the power cable. Appliance will be up in about 246 seconds							
In the unlikely event that the appliance fails to boot properly, resetting the power to the appliance will cause it to fully restore your current image. Once the appliance is up it is recommended to clear the browser's cache.							
Download Log Files							
Cancel Help							
·							
🗳 User name							
Password							
QUANTUM SPARK Save user name SECURITY APPLIANCE							

登入Quantum Spark 1530首頁,確認設備版本正確,完成

Se Quantum Spark 1530 Appliance	w admin E- Log Out 😗 Help / Support 🔍 Search						
	We recommend you enforce password complexity for administrator passwords in Device > System > Administrators > Security Settings Dismiss						
HOME System	System						
Security Dashboard DEVICE Cloud Services Cloud Services License ACCTSS POLICY Monitoring	SYSTEM INFORMATION Quantum Spark 1530 Appliane Wersion: R81.10 (996000558) Name: Gateway-02-75CA0-40 MAC: 00:1C:7F:9C-40:40 Wednesday, December 7th, 2022 02:50:46 PM (GMT+08:00) Taipei System is up for 0 days, 0 hours, 4 minutes and 45 seconds	NETWORK Internet connections Connection type: DHCP Interface: WAN IPv4 address: 172.16.1.110/24					
Notifications Notific	NOTIFICATIONS Notifications page Image: New firmware available Image:	WATCHTOWER MOBILE APP Get security alerts to your mobile! Enhance your Check Point network security with the ability to monitor your network and quickly mitigate security threats on the go with your mobile phone PAIR YOUR MOBILE DEVICE					
	NETWORK ACTIVITY Packet Rate (packets per second)	Reports Monitoring Throughput (Kbps)					



7-2. 設定檔備份及上傳

7-2-1. 手動設定檔備份

開啟 Quantum Spark 1530 GUI \rightarrow DEVICE \rightarrow System \rightarrow System Operations \rightarrow Backup and Restore System Settings \rightarrow Create Backup File

Check P 1530 Ap	oint opliance			🖬 adr	min E+ Log_Out ? Help / Support Q Search	
<u>~</u>	Hotspot	<	System Operations: Manage your firm	ware version and backup your applianc	e	Help
HOME	Routing		Appliance			~
	MAC Filtering		Reboot	Reboot the appliance		
	DNS		Default Settings	Restore factory default settings but kee	p the current firmware version	
Devici	Proxy	L	Factory Defaults	Revert to the factory default image and	settings.	
ACCES! POLICY	System Operations	L	Firmware Upgrade	The factory firmware version is Roo.20.	(2010)2020	~
Ô	Administrators Administrator Access	L	The current firmware version is R80 .	20.15 (992001653)		
THREA PREVENTI	Device Details		Configure automatic upgrades	DW		
	Date and Time		Manual Upgrade	Revert to Previous Image		
VPN	DDNS & Device Access	L		1		<u>_</u>
	Tools		Backup and Restore System Setting	S		~ ~ ~
22	 Certificates 		Create Daskup File	Destava		
USERS a	Installed Certificates		Create Backup File	Restore		
	Internal Certificate					
	Advanced	-				
	Sa Internet connected					🛇 01:40 PM

7-2-1-2 Create Backup \rightarrow Download Backup \rightarrow Finished

BACKUP SETTINGS ×	BACKUP SETTINGS ×
Backup Settings	Backup Settings
Use file encryption	Use file encryption
Set password:	Set password:
Confirm password:	Confirm password:
Comment:	Comment:
Backup File Contents	Backup File Contents
✓ Backup system settings	✓ Backup system settings
Create Backup Cancel Help	Download Backup Cancel Help Click the Download button to save the backup file



7-2-2. 排程設定檔備份

開啟Quantum Spark 1530 GUI \rightarrow DEVICE \rightarrow System \rightarrow System Operations \rightarrow Backup and Restore System Settings \rightarrow 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 1530 登入帳號密碼)

PERIODIC BACKUP SETTINGS			×
Enable scheduled backups	N.		^
File Storage			
Backup server path:	\\192.168.17	1.3\QS-1530-ba	ckup-dei
Username:	admin		
Password:	•••••		
File Encryption			
Use file encryption			
Password:			
Confirm:			
	Show		
Schedule Periodic Backup			
Daily			
Time of day:	01:00 - 02:00		•
O Weekly			-
		🗸 Apply	× Cancel



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

PERIODIC BACKUP SETTINGS		×
 Enable scheduled backups 		4
File Storage		
Backup server path:	\\192.168.171.3\QS-1530-backup-der	
Username:	admin	
Password:		1
File Encryption		1
Use file encryption		1
Password: Confirm:	Show	
Schedule Periodic Backup		
Daily Time of day:	01:00 - 02:00	
у меекіу	Apply X Car	L .

7-2-3. 上傳/還原設定檔

開啟 Quantum Spark 1530 GUI \rightarrow DEVICE \rightarrow System \rightarrow System Operations \rightarrow Backup and Restore System Settings \rightarrow Restore

Check P 1530 Ap	oint ppliance	admin E• Log_Out ⑦ Help / Support Q Search	
А	Hotspot Routing	System Operations: Manage your firmware version and backup your appliance Appliance	Help
	MAC Filtering	Reboot Reboot the appliance	
DEVICE	DNS Proxy	Default Settings Restore factory default settings but keep the current firmware version Factory Defaults Revert to the factory default image and settings. The factory firmware version is DB0.20.15 (002.001.552)	
ACCESS POLICY	System Operations Administrators	Firmware Upgrade	~
THREA' PREVENTI	Administrator Access Device Details	The current firmware version is R80.20.15 (992001653) Firmware is up to date Check now Configure automatic upgrades	
VPN	Date and Time DDNS & Device Access	Manual Upgrade Revert to Previous Image Backup and Restore System Setting	~
	Certificates Installed Certificates	Periodic backup is OFF Settings Create Backup File Restore	
	Internal Certificate • Advanced		
	Salinternet connected		🛇 01:40 PM



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 1530 GUI → 登入 →完成

RESTORE SETTINGS				×		
Upload Settings	File					
Settings file:	Gateway-ID-7F90	A040-demo_R81	- Browse			
Upload File	Close					
RESTORE SETTINGS				×		
File Information						
Backup saved on Firmware version Date: Created by: Policy:	appliance: Gat : R81 Dec adn Incl	eway-ID-7F9CA040- .10_996000558 .08, 2022 01:05:42 F nin uded in backup (loc	demo PM ally managed)			
Restore	Close					
	4					
RESTORE SETTI	NGS					
Are you reboot t	sure you wan he appliance.	t to restore setti	ngs? This will	override	your current	setting







第八章 遠端管理防火牆設定

8-1. 手機 APP 管理平台

開啟 Quantum Spark 1530 GUI \rightarrow HOME \rightarrow System \rightarrow PAIR YOUR MOBILE DEVICE

Check P 1530 Ap	oint opliance	🖬 admin QS-1530-demo	b.jlead_com_tw E+ Log_Out ? Help / Support Q S	earch
ò	< Overview	System		Help
HOME DEVICE	System Security Dashboard Security Management Cloud Services License Site Map • Monitoring	SYSTEM INFORMATION Check Point 1530 Appliance Wersion: R80.20.15 (992001653) Name: Gateway-ID-7F9CA040-SMP MAC: 00:1C:7F:9C:A0:40 Wednesday, December 7th, 2022 11:17:26 AM (GMT+08:00) Talpel System is up for 0 days, 1 hour, 45 minutes and 12 seconds	NETWORK In Connection type: DHCP Interface: WAN IP 172.16.1.110/24	/4 address:
THREAT PREVENTION VPN USERS & OBJECTS	Notifications Active Devices Monitoring Reports • Troubleshooting Tools Support	NOTIFICATIONS Notifications page	WATCHTOWER MOBILE APP	mobile! : network security your network and nreats on the go NEVICE
LOGS & MONITORIN		NETWORK ACTIVITY Packet Rate (packets per second)	Re Throughput (Kbps)	ports Monitoring

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

CONNECT MOBILE DEVICE ×	CONNECT MOBILE DEVICE ×
Generate a new one-time use QR code to connect the Check Point WatchTower mobile app with the gateway. Select administrator: admin Generate	Generate a new one-time use QR code to connect the Check Point WatchTower mobile app with the gateway. Select administrator: admin r Generate
	CONFIRM Inis operation will allow access to the gateway from mobile devices. Are you sure you want to continue? Yes



CONNECT MOBILE DE	/ICE			×	CONNECT MOBILE DEVICE	×
Generate Select adn	a new one-time use C WatchTower mobile inistrator: admin	R code to connect app with the gates	the Check Point way. Generate		Generate a new one-time use QR code to connect the Check Point WatchTower mobile app with the gateway. Select administrator: admin Generate	
Establ	shing a connection three	ugh Reach-My-De	vice service	•	Scan QR code with Check Point WatchTower Expires at 15:53	

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



1 2 100% 📰

٢



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 1530 QR Code (1.2 產生的 QR Code) → 輸入 Check Point Quantum Spark 1530 登入帳號密碼 → Connect → Finished







8-2. 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

	A Domain	
	Luser name	
-	Password	o
QUANTUM SPARK		
SECURITY MANAGEMENT PORTAL	Save user name	
And both a many advantant mental fait the many advantant advantation and faith of the second advantation of the		
	New Domain Request	
		LOGIN

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)

NEW SERVICE DOMAIN REQUEST	×	NEW SERVICE DOMAIN REQUEST	×
Service Domain Name:	-		
Domain's Goal: Select a do	main goal 🗸 🗸	Service Domain Name:	jlead.com.tw
Country: Select a cou	untry ~	Domain's Goal:	Select a domain goal
Expected number of Category		Country:	Demo/Poc Production
Expected number of Galeways:		Expected number of Gateways:	Other
Service Domain Administrator:		Service Domain Administrator:	
First Name:		First Name:	
Last Name:		Last Name:	
Email:		Emailt	
User Center Account:		Lindi.	
Prerequisites for Net	w Service Domain	User Center Account:	
		Prerequi	isites for New Service Domain
我不是機器人 reCAPTCHA 隱私權 - 條款		我不是機器人 reC. 5.1	APTCHA 1.修款
	 Finish × Cancel 		✓ Finish X Cancel



NEW SERVICE DOMAIN REQUEST		×
Service Domain Name:	jlead.com.tw	
Domain's Goal:	Select a domain goal	~
Country:	Tuvalu	~
	Sudan	
Expected number of Gateways:	Suriname	
Service Domain Administrator:	Svalbard and Jan Mayen Sweden	
	Switzerland	
First Name:	Syrian Arab Republic	
Last Name:	Tajikistan	_
	Tanzania, United Republic of	f
Email:	Timor-Leste	
User Center Account:	Тодо	
	Tokelau	
Prereq	Trinidad and Tobago	
	Tunisia	
- 我不是機器人 ref	Turkmenistan	
[[書表]	Turks and Caicos Islands	
l	Tuvalu	ncel

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)

NEW SERVICE DOMAIN REQUEST		×
Service Domain Name:		
Domain's Goal:	Select a domain goal	~
Country:	Select a country	~
Expected number of Gateways:		
Service Domain Administrator:		
First Name:		
Last Name:		
Email:		
User Center Account:		
Prer	requisites for New Service Don	nain
我不是機器人	reCAPTCHA 香私權 - 條款	
	✓ Finish	Cancel



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:_00D209OX500672eVPVM:ref]
CP Check Point Support <support@checkpoint.com> 收件者 田TS-Group</support@checkpoint.com>
③ 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。
53 約部件翻譯為:繁體中文 (繁體) 一律不翻譯自:英文 翻譯裏好設定
ا الله الله الله الله الله الله الله ال
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: //
La User name
OUANTUM SPARK
SECURITY MANAGEMENT PORTAL
New Domain Request

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

Sign In	
To continue to User	Center/PartnerMAP
User <mark>N</mark> ame (Email)	
Password	V
	Forgot Your Password
	Sign In



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

S	Check Point PartnerMap	SALES & KNOWLEDGE	MARKETING	Free Dem	Contact Us Suppo	rt Center Blog We HECK POINT	elcome Sigr Q
	My Accounts		My Info		My Partner Profile		
	Product Conton						
	My Accounts		My Certifications		Partner Dashboard		
	Track Orders (New)		My Subscriptions				
			Notifications				
	Tools						
	Accounts, Products a	nd Orders					
	Sync License Informa	tion Tool					
	Download Contract Fi	le					
		Rattine Crieck Paint	to provide any cardiad	n Information In The Charle Point (or liver who purchased p	enductfol on my hierail	
		Talinos Chuck Phili	to provide my contact	Contempolaria de Creck Ponte	árthur who più chasad p	mbuctfol on my henall	
		Talinov Crouch Pount	ta provide ny condar		arthur who parchased p	rratuat (a) (an my behad)	
		Talinoi Couch Puni	ta provide diversitat	Conference for the Direct Point of	n finn ann gur fhanair g	ort Center Blog	Welcome:
G	Check Point DartnarMan				Contact Us Supp	ort Center Blog	Welcome:
¢	• Check Point Partner Map	SALES & KNOWLEDG	e Marketing	Free Dem CUSTOMER ACQUISITIONS	10 Contact Us Supp 5 SUPPORT MY	ort Center Blog CHECK POINT	Welcome:
•	Check Point PartnerMap	SALES & KNOWLEDG	e Marketing	Free Den CUSTOMER ACQUISITIONS	 Contact Us Supp SUPPORT MY 	ort Center Blog CHECK POINT	Welcome: 4
S My U	Check Point PartnerMap	SALES & KNOWLEDG	e marketing	Free Den CUSTOMER ACQUISITIONS	10 Contact Us Supp 5 SUPPORT MY	ort Center Blog CHECK POINT	Welcome:
My U Q Fil	Check Point PartnerMap CAccounts Iter as you type	SALES & KNOWLEDG	E MARKETING	Free Den CUSTOMER ACQUISITIONS	Contact Us Supp S SUPPORT MY	ort Center Blog CHECK POINT	Welcome:
My U a Fit	Check Point PartnerMap IC Accounts Iter as you type g 2 of 2 Accounts I Active I	SALES & KNOWLEDG	E MARKETING		Contact Us Supp S SUPPORT MY	ort Center Blog CHECK POINT Create Accor	Welcome:
S My U Q Fit	Check Point PartnerMap CAccounts Iter as you type g 2 of 2 Accounts I Active I D Company	SALES & KNOWLEDG Filters: Only Active Account Name Account Nam	E MARKETING	Endeemediate is the black is based in Free Dem CUSTOMER ACQUISITIONS U Name ↑ Country	Contact Us Supp S SUPPORT MY C ID # of Products	ort Center Blog CHECK POINT Create Accor Renewal Date	Welcome:
My U Q Fit Showing	Check Point PartnerMap CAccounts ter as you type g 2 of 2 Accounts Active ID Compan INFORMATION (1)	SALES & KNOWLEDG Filters: Only Active Account y Name Account Name	E MARKETING	Free Dert CUSTOMER ACQUISITIONS	Contact Us Supp S SUPPORT MY C ID # of Products	ort Center Blog CHECK POINT Create Accor Renewal Date	Welcome:
My U Q Fit Showing V	Check Point PartnerMap CAccounts Iter as you type g 2 of 2 Accounts I Active I ID Compan INFORMATION (1)	SALES & KNOWLEDG Filters: Only Active Account y Name Account Nam HEORMATION	E MARKETING	Free Dem CUSTOMER ACQUISITIONS	Contact Us Supp SUPPORT MY CID # of Products	ort Center Blog CHECK POINT Create Accor Renewal Date	Welcome: [] : unt I Transformed I Transform
My U Q Fil Showing V I	Check Point PartnerMap IC Accounts Iter as you type g 2 of 2 Accounts Active ID Company ID Company XXXXXXX IM INFORMATION (1) XXXXXXXX IM INFORMATION (1) XXXXXXX XXXXX XXXXX XXXX XXXXXX XXXX	SALES & KNOWLEDG Filters: Only Active Account y Name Account Name HFORMATION	E MARKETING	Free Dert CUSTOMER ACQUISITIONS	C ID # of Products 27	ort Center Blog CHECK POINT Create Accor Renewal Date 31-Jul-2023	Welcome: [1]
My U a Fil bhowing - - - - - - - - - - - - -	Check Point PartnerMap UC Accounts Iter as you type g 2 of 2 Accounts I Active I ID Compan Compa	SALES & KNOWLEDG Filters: Only Active Account y Name Account Nam IFORMATION Pany customer [1]	E MARKETING	Free Den CUSTOMER ACQUISITIONS Name ↑ Country	C Contact Us Supp S SUPPORT MY # of Products 27	ort Center Blog CHECK POINT Create Accor Renewal Date 31-Jul-2023	Welcome: [1]



SMP (Security Management Portal) 納管Quantum Spark 1530

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

	A Domain	
	Luser name	
	Password	O
SECURITY MANAGEMENT PORTAL	Save user name	
	New Domain Request	1 🔪
		LOGIN

點選 HOME \rightarrow Plans \rightarrow New



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

CREATE NEW PLAN X	CREATE NEW PLAN X	
Name SMP-demo-QS-1530 Description manager from cloud	Supply the following services: Store gateway logs Send periodic reports Firmware upgrades Dynamic DNS Send cloud notifications Periodic backup can be configured after the Plan is created.	



CREATE NEW PLAN	×
Activate the following Security Software Blades:	^
✓ Firewall	
✓ Application Control and URL Filtering	
▼ IPS	
✓ Traditional Anti-Virus	
✓ Anti-Spam	
QoS	
Remote Access VPN	
✓ Site to Site VPN	
✓ User Awareness	
✓ Anti-Virus	
✓ Anti-Bot	
By default, Security Software Blades are remotely managed. Changing this configuration is possible only after the plan is created.	Ŧ
G Back Finish x C	ancel







點選 HOME → Gateways → New

Security Management Portal	▲ (Super User) 🕄 HELP 🗘 LOGOUT Search for Gateways 🔎
	★ New
Materia Gateways	Status Name Description Human Readable Address Access Gateway MAC Address License
Plans Users	
Communities Service Domain	No items found
Settings Roles	
Custom Images	
Gateway Logs System Logs	
Activity Logs	
Gateways: 🔮 0 Connected	connected 🖥 0 Plans 07 December 10:52:53 GMT +08:00

選擇Type → Name (自訂義欲管理設備名稱) → Finsh → 複製 Activation key 備用 (Quantum Spark 1530 join SMP 時 必須資料)

CREATE NEW GATEWAY		×
Туре	Small Office Appliance 🗸	
Name	QS-1530-demo 🚱 Generate	
Description	manager from cloud	
 Managed by SMP 		
Plan	SMP-demo-QS-1530	
Registration key	CF7PcSQY @Generate	
Owner ID	Y Search	₩ New
	✓ Finish	× Cancel

 \checkmark




💠 Quantum Spark Security Management Portal	1 🔺	p (Super User) Image: HELP Image: HeLP Search for Gateways
 ✓ Gatev ∧ Home QS-1530-de 	way Edit lemo	Access Gateway Delete Gateway Actions •
Map Search Gateways General Plans - Y Location Users 2 Owner	Description Enabled Gateway type r Reported Firmware	manager from cloud
Communities Status ◆ Service Domain Settings ,	et Monitoring Managed by SMP Plan [®] es Settings ity Software MAC address [®] es Last connected IP address Registration key [®]	SMP-demo-QS-1530 Change Plan SGO Remote management
A Logs , Setup Gateway Logs System Logs Activity Logs 	Activation key	smp-beta.checkpoint.com&QS-1530-demo.jlead_com_tw&CF7P
∧ Cyber Views		Cancel Save
Gateways: 🔇 0 Connected 🚯 0 Disconnected	h 1 Plans	08 December 10:14:01 GMT +08:00

登入Quantum Spark 1530 \rightarrow HOME \rightarrow Cloud Services \rightarrow Configure

Se Quantum 1530 Ap	n Spark pliance	wradmin E- Log.Out 🍞 Help / Support 🔍 Search	
	<	Cloud Services: Configure a Cloud Services provider that can handle your security policy and supply a variety of services	🕑 Help
ĥ	 Overview 	Cloud Services	
HOME	System	Cloud Services	
	Security Dashboard		
	Security Management	Configure	
DEVICE	Cloud Services	Managed Security Blades	
I#1	License		
ACCESS POLICY	Site Map	Firewall Applications User QoS IPS Anti-Virus Anti-Bot Threat Anti-Spann Remote Site To Site	
~	 Monitoring 	& URL Awareness Emulation Access VPN	
THREAT	Notifications	rince ing	
PREVENTION	Active Devices	Available Services	
25.	Monitoring	Reports Reports Firmware Upgrades Firmware Upgra	
VPN	Reports		
	 Troubleshooting 	Logs O Periodic Backup	
22	Tools	 Store security and system ridgs in coursiseffers Periodically backup the applance's securitys 	
USERS & OBJECTS	Support	P Dynamic DNS	
~		Bill" Assign a persistent domain name e.g. my gateway domain.com	
LOGS &			
MONITORING			
		Apply x Canel	
4 F	A	· pppy realised	



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

 Activation key: 	ւթ-beta.checkpoint.com&QS-1530-demo.jlead_com_tw&CF7PcSQY
Activation details:	
Service Center:	smp-beta.checkpoint.com
Gateway ID:	QS-1530-demo.jlead_com_tw
Registration key:	CF7PcSQY











\$	Quantum Spark Security Management Portal			2	(Super User)	😯	HELP	🗈 LOGOUT	Search for Gateways	Q
	<									0
٨	Home	Status	Sessions							
	Overview	Gateways			Show All	_				
	Мар	G Connected		1	Show					
	Gateways	Not connected	4	0	Show					
	Plans	© Disabled	<i>•</i>	0	Show					
	Users									
	Communities	Plans								
٨	Service Domain	Plans		1	Show					
	Settings	Users								
	Roles	S Logged In		1						
	Custom Images									
٨	Logs	Service Center Na	me:	jlead_com_tw						
	Gateway Logs									
	System Logs									
	Activity Logs		Refresh	Generate Report						
^	Cyber Views									
	· · · · · · · · · · · · · · · · · · ·		al							
Gat	eways: 👽 1 Connected 🛛 🚯 0 D	isconnected 1 1	Plans			_			07 Decembe	er 11:04:43 GMT +08:00







