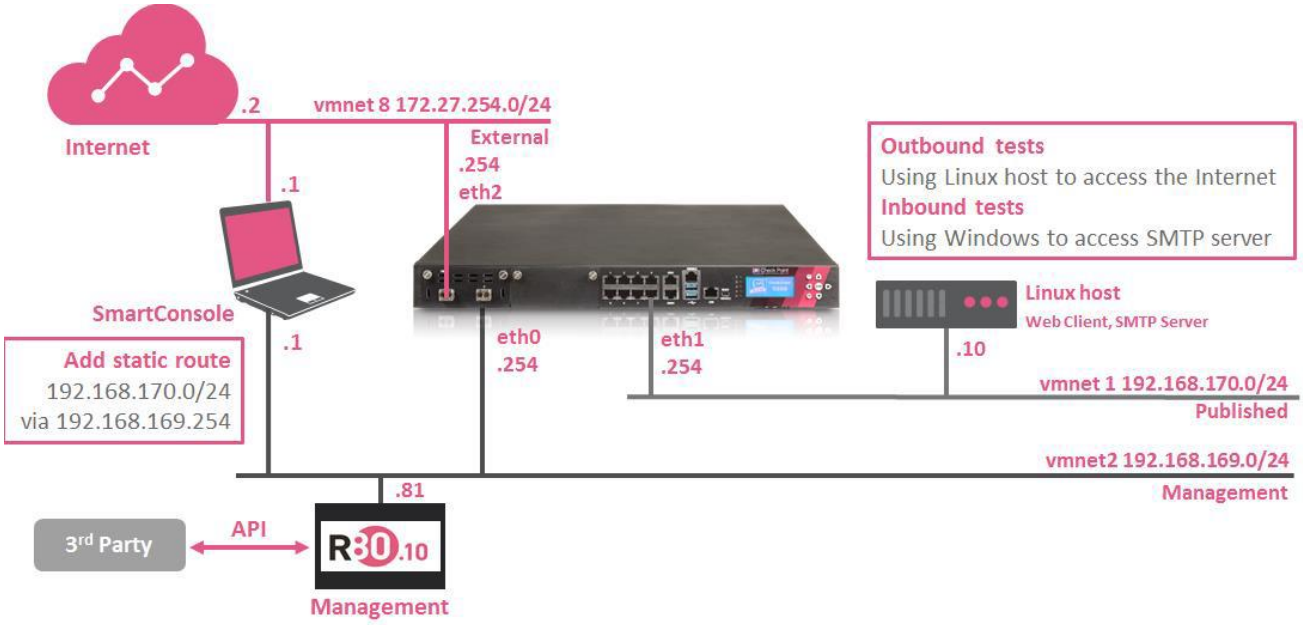
Local VM edition, May 2018

R80.10 Training Lab Guide

目錄

Lab network diagram



Lab 需求以及確認

你的電腦需要以下的硬體規格來執行virtual machines。

Lab中的虛擬機使用以下的帳號密碼

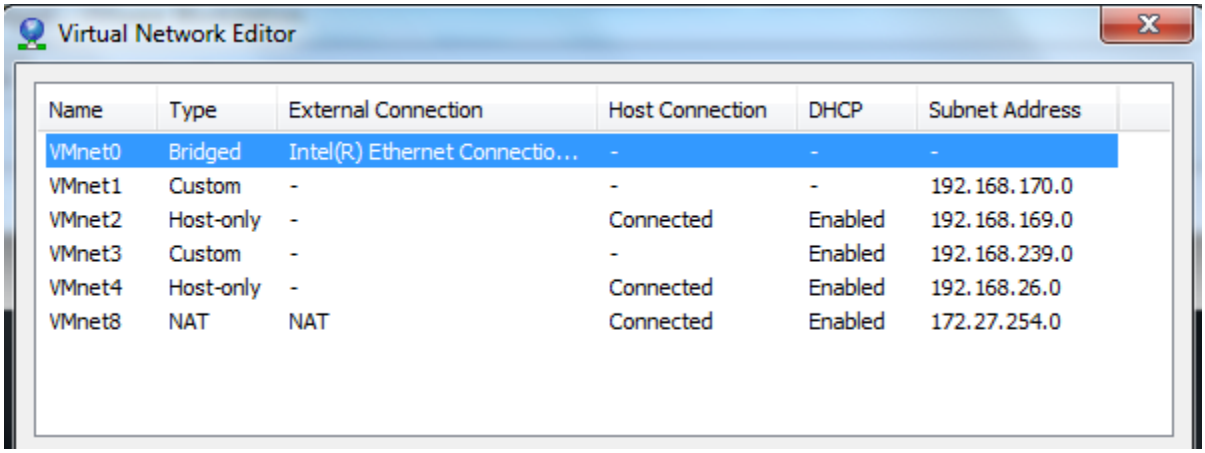
- 4 Core / 16 GB RAM
- Administrative UserID/password on management server and gateway: admin/vpn123.
- Gaia expert level password: vpn123
- Linux user/password: peter/vpn123
- Root authorization on Linux: vpn123

在你的電腦上應該具備以下的軟體：

- VMware workstation 10 or later (all virtual machines are based on vmware workstation 10)
- A scp program i.e. winscp
- A ssh terminal program i.e. putty
- Notepad++ editor
- Lightweight email client like Thunderbird portable
- Google Chrome Browser does work best with Gaia WebUI

VMware networking configuration

請確認你的 VM Network 與下圖完全相同：



Memory, CPU 與 disk 需求

管理主機至少須具備以下的硬體規格要求：

1. CPU 4 Core
2. RAM 8 GB
3. 100 GB disk space.

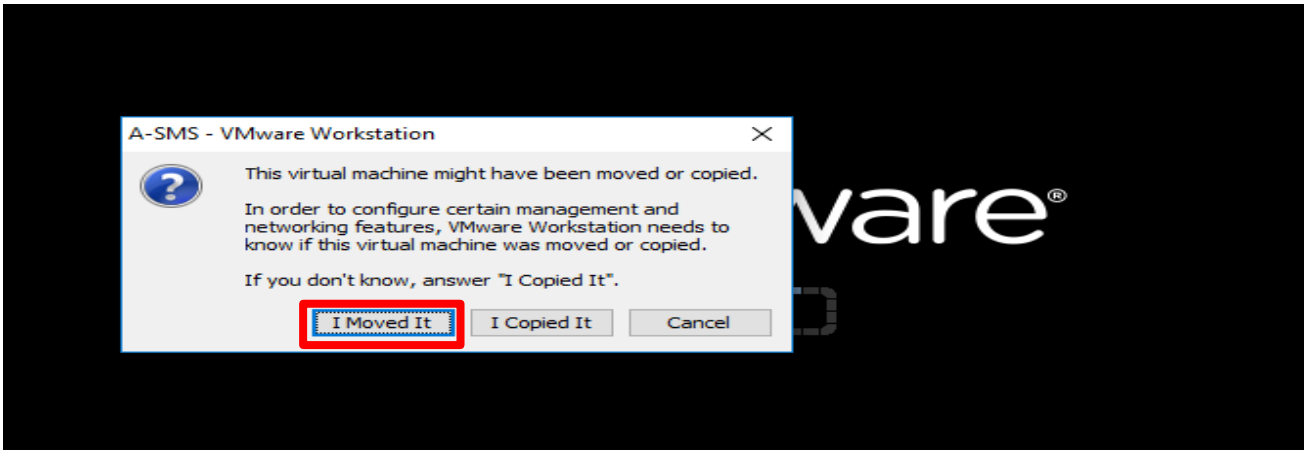
安全閘道至少須具備以下的硬體規格要求：

1. CPU 4 Core
2. RAM 4 GB
3. 50 GB disk space.

請確認你的 VM 主機是否為相同的硬體配置。

開啟 VM 時請注意：

第一次開啟 VM 主機，**請選擇「I Moved It」**。如果選擇其它選項，VM 網卡需做調整：



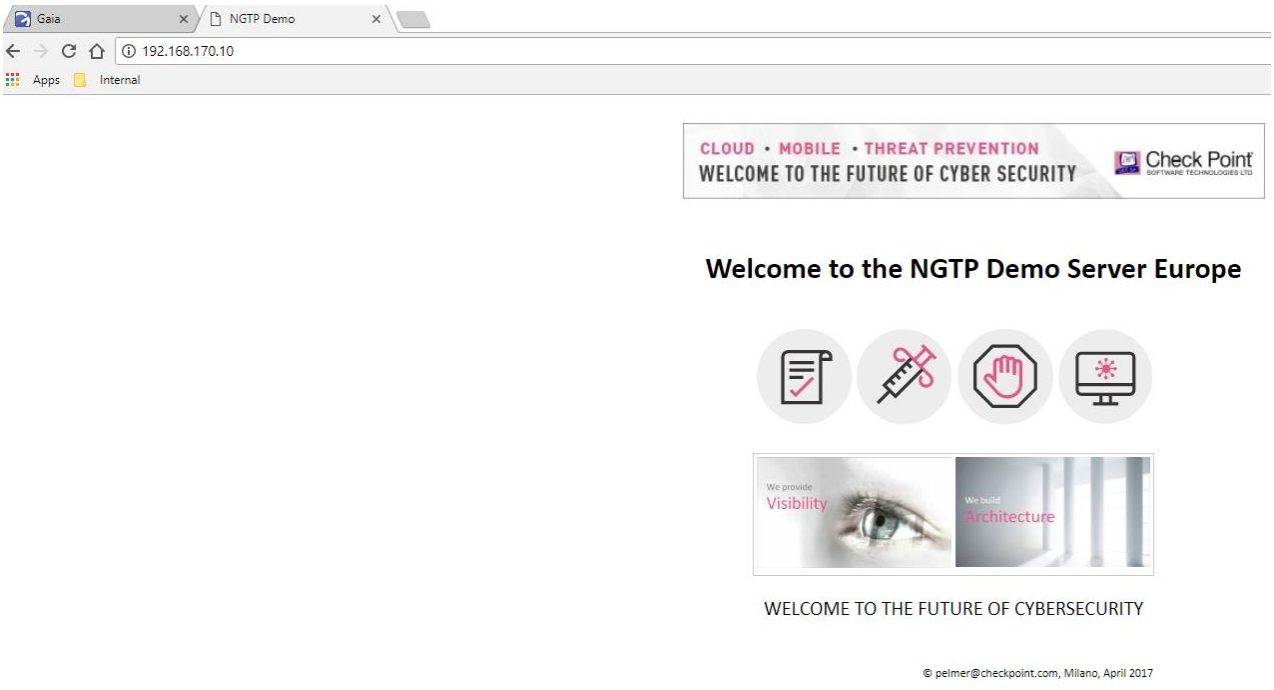
確認 Windows 主機與各個 VM 之間的連線是否正常

- **Gateway** 的 GAiA Portal 是 TCP 4434 Port，Management Server 則是 TCP 443 Port。

- Gateway 與 Management 都應該可以連線到 Internet 上。

```
mgmt> ping tw.yahoo.com
PING atsv2-fp.wgl.b.yahoo.com (87.248.98.7) 56(84) bytes of data.
64 bytes from media-router-fp1.prod1.media.vip.ir2.yahoo.com (87.248.98.7): icmp
_seq=1 ttl=127 time=324 ms
64 bytes from media-router-fp1.prod1.media.vip.ir2.yahoo.com (87.248.98.7): icmp
_seq=2 ttl=127 time=328 ms

--- atsv2-fp.wgl.b.yahoo.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 324.675/326.368/328.061/1.693 ms

mgmt>
```

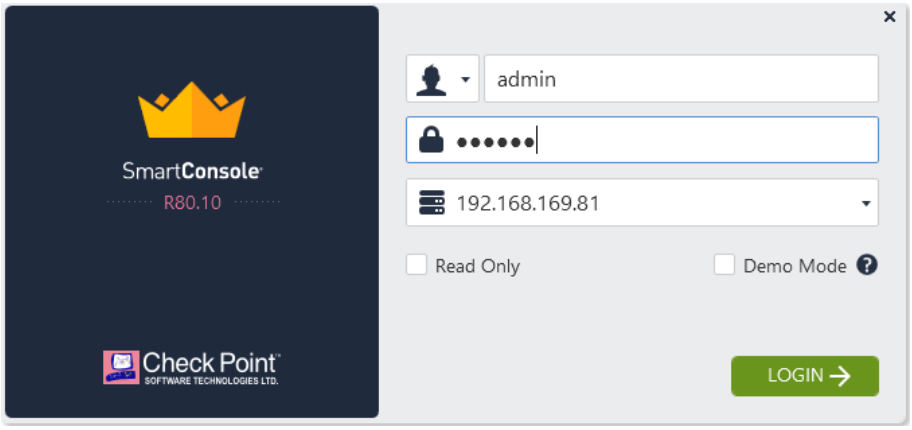
- Windows 主機應該可以連線到 Linux Web+ Mail Server：



- Gateway應該可以Ping到 web+mailserver 192.168.170.10

```
gwR8010> ping 172.27.254.1
PING 172.27.254.1 (172.27.254.1) 56(84) bytes of data.
64 bytes from 172.27.254.1: icmp_seq=1 ttl=128 time=4.97 ms
64 bytes from 172.27.254.1: icmp_seq=2 ttl=128 time=0.343 ms
64 bytes from 172.27.254.1: icmp_seq=3 ttl=128 time=0.373 ms

--- 172.27.254.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.343/1.896/4.974/2.176 ms

gwR8010> ping 192.168.170.10
PING 192.168.170.10 (192.168.170.10) 56(84) bytes of data.
64 bytes from 192.168.170.10: icmp_seq=1 ttl=64 time=2.27 ms
64 bytes from 192.168.170.10: icmp_seq=2 ttl=64 time=0.576 ms
```

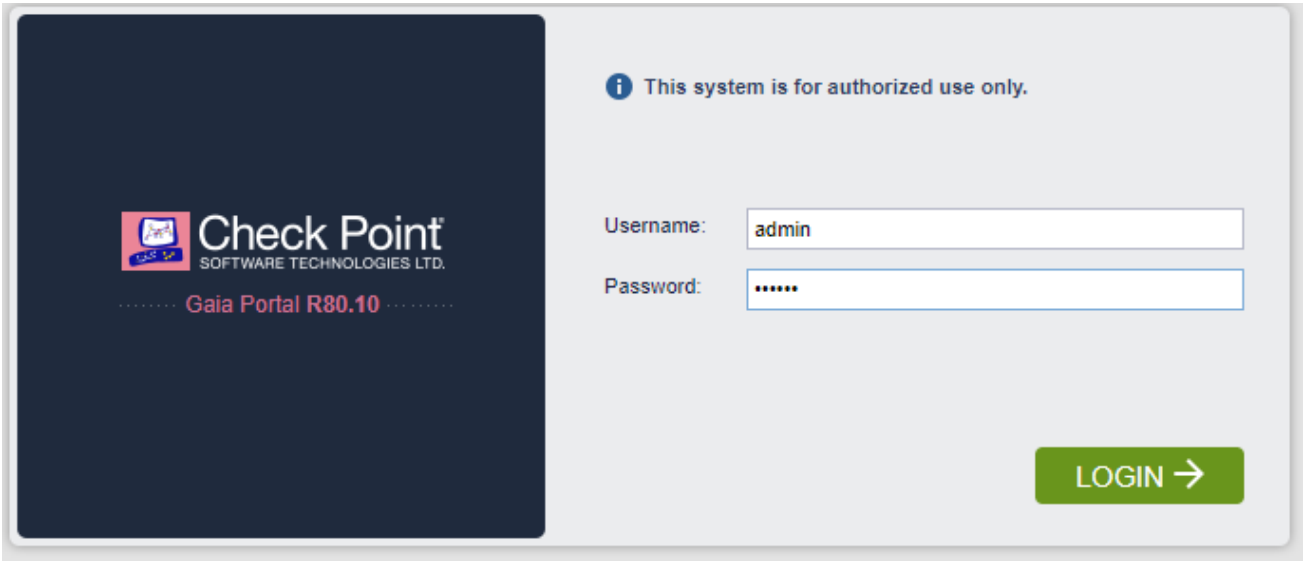
- Windows主機上的R80.10 SmartConsole應該可以成功登入SMS管理主機：



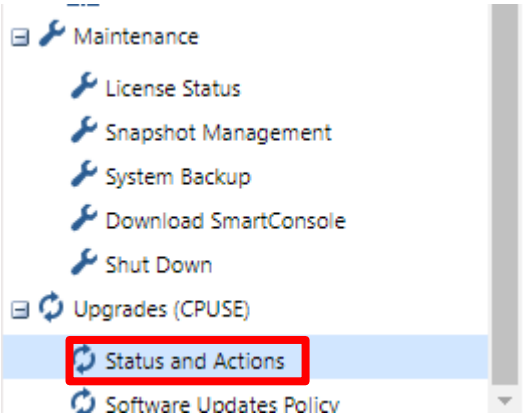
Lab 0: 準備 Lab 使用的 Check Point 管理主機以及 Security Gateway

在管理主機以及 Security Gateway 上安裝 Jumbo hotfix file

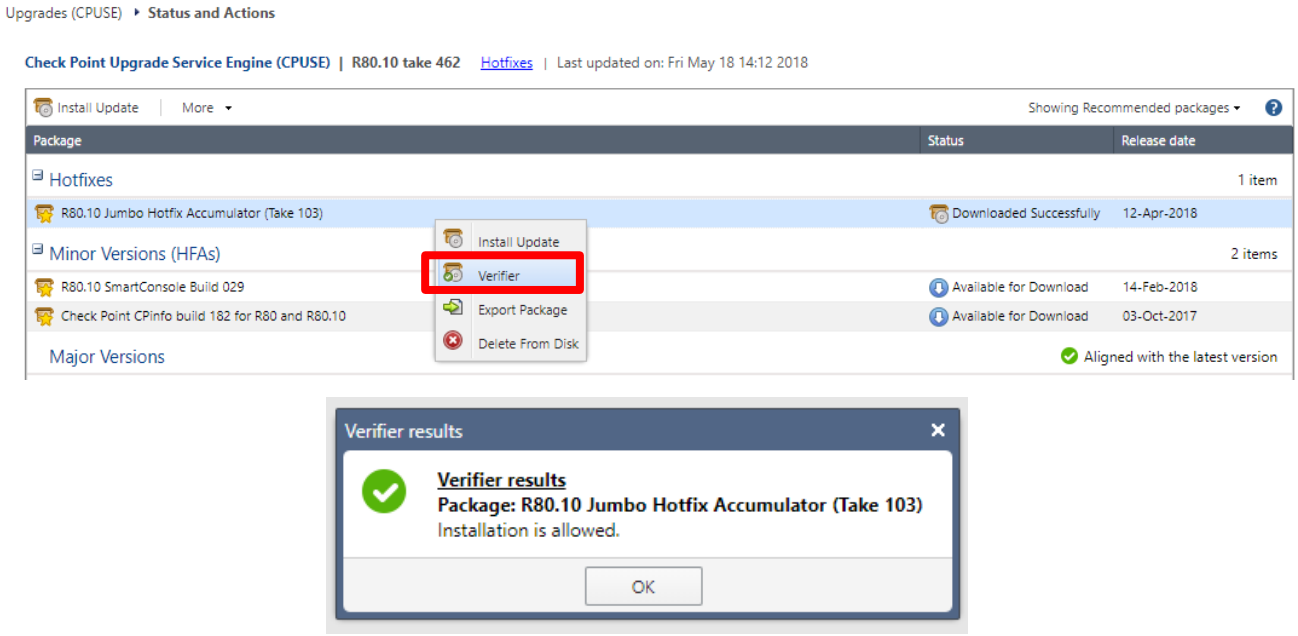
開啟並登入管理主機 SMS 以及 Gateway 上的 WebUI 介面 admin / vpn123：



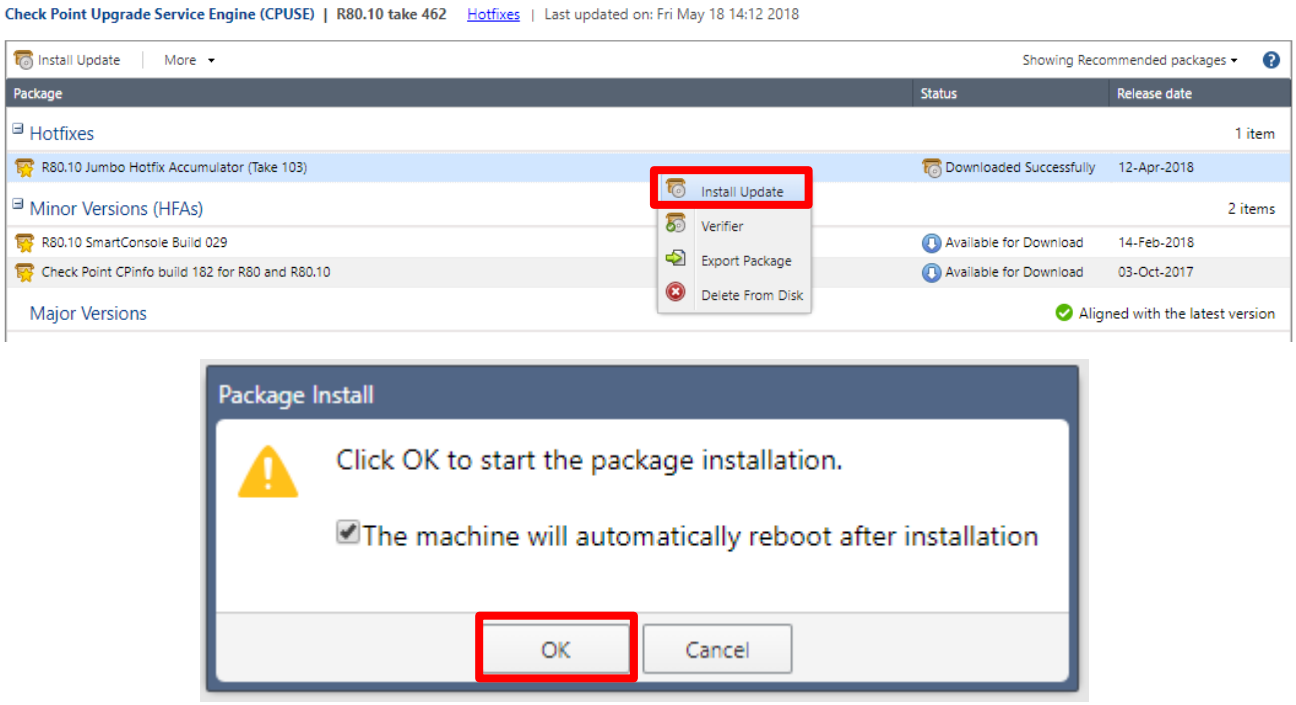
切換選項至「Upgrades(CPUSE) >> Status and Action」：



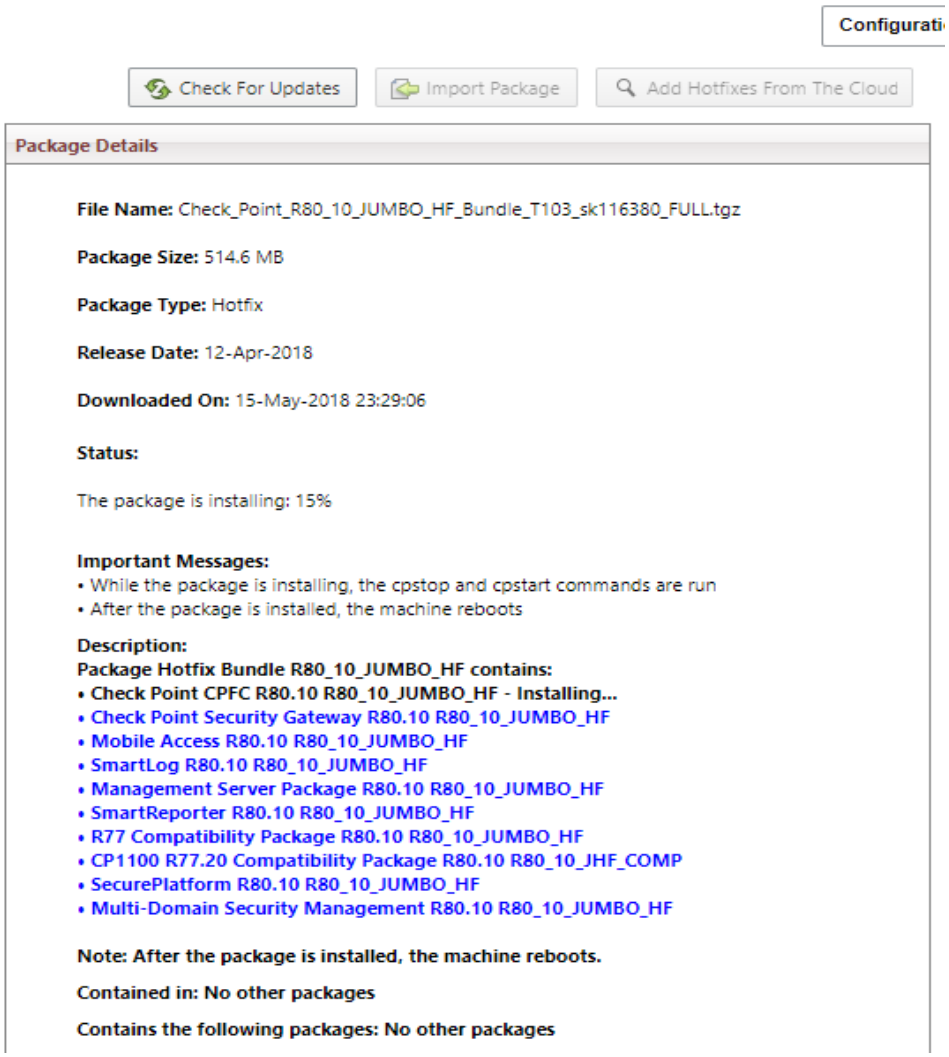
在 R80.10 Jumbo Hotfix Accumulator (Take 103)上方按右鍵 >>「Verifier」，成功的話會出現如下圖：

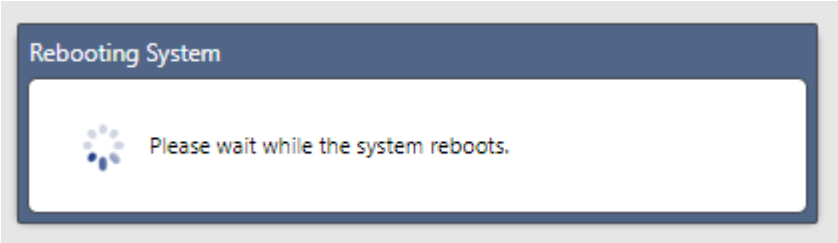


在 R80.10 Jumbo Hotfix Accumulator (Take 103)上方按右鍵 >>「Install Update」，隨後會出現如下圖提示需要重新開機：



在畫面右邊會顯示目前的安裝進度 >>「Install Update」，隨後會出現如下圖提示重新開機：





重新開機完成後即會顯示完成安裝。

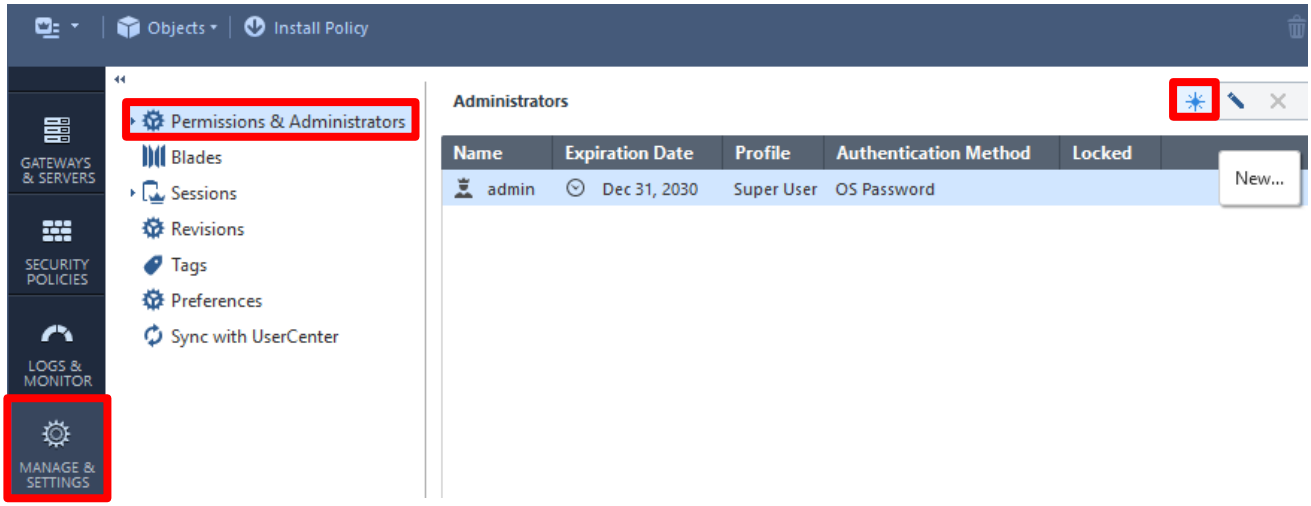
使用 API 的 scripts 自動建立防火牆物件、服務及規則

接下來我們要建立 Lab 中會使用到的物件、服務以及防火牆規則。在 R80.10 中你可以透過 API 介面(Web, CLI)連線到管理主機自動建立 Policy Packages 以及相關的物件規則。

請參照以下的 Lab Guide 來一步步建立這些設定。

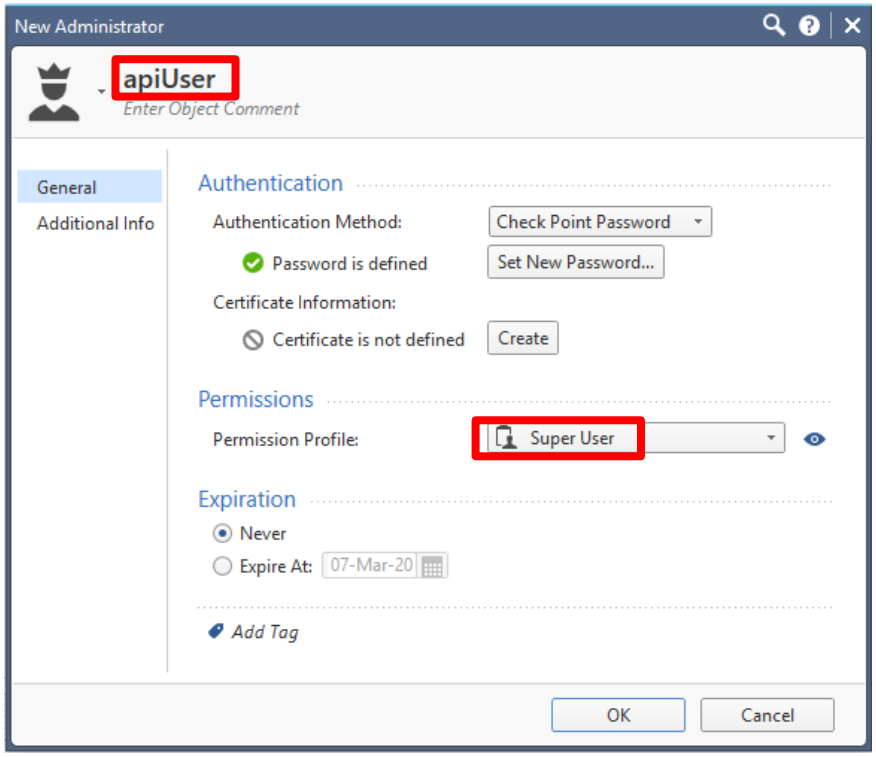
建立 API 要使用的 api 帳號

登入 SmartConsole，並切換至「Manage & Settings」頁籤，點選「New…」建立 API User：



輸入帳號名稱為「**apiUser**」、Permissions Profile 為「Super User」：

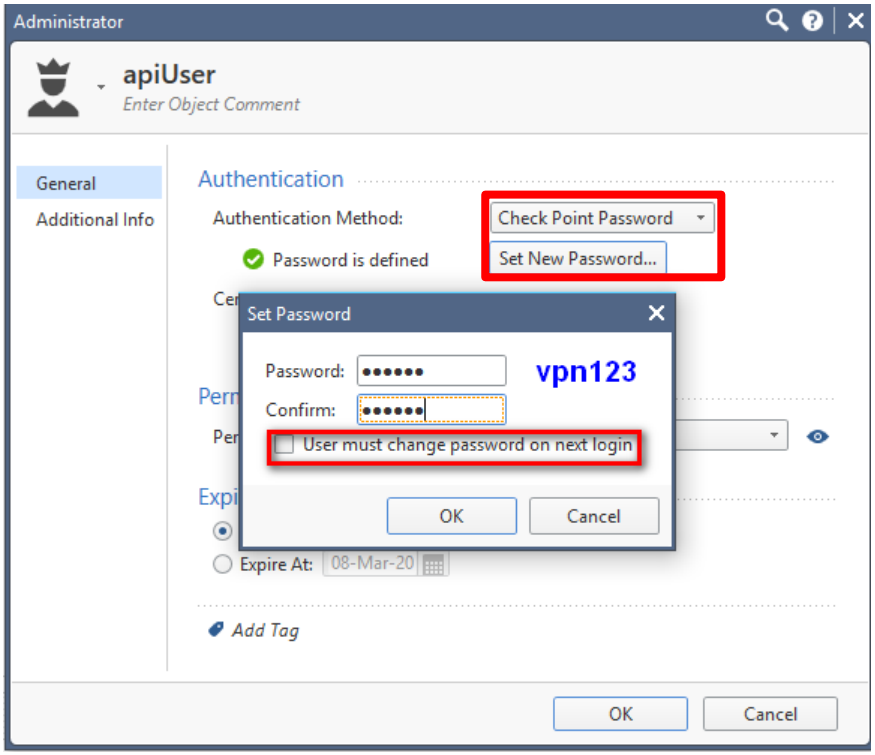
請注意帳號大小寫必須完全相同，後面執行 Script 才不會有錯誤



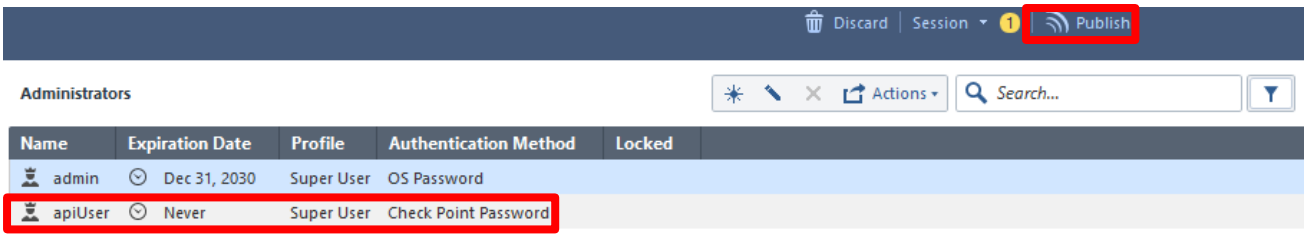
選擇 Authentication Method 為「Check Point Password」並點選「Set New Password…」設定密碼，

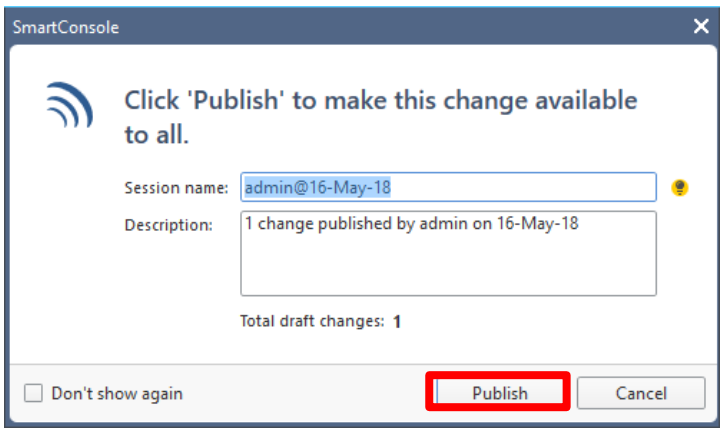
密碼請輸入「**vpn123**」並**取消勾選**「User must change password on next login」，完成後點選 OK >> OK：

請注意密碼大小寫必須完全相同，並**取消勾選**該選項，後面執行 Script 才不會有錯誤

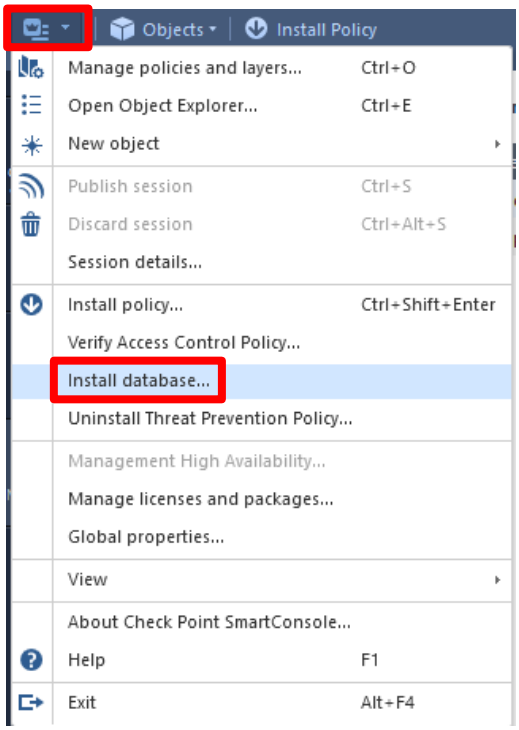


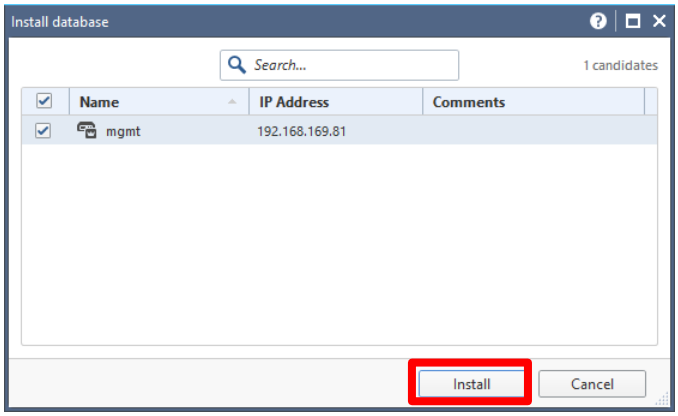
剛建立的 api 使用者會出現在下方，點選上方的「Publish」將設定儲存於 SMS 上



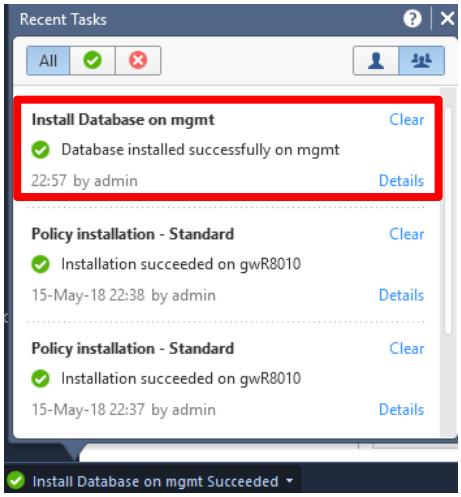


至左上角的下拉式選單選擇「Install database」將剛剛在 SMS 上做的設定生效：



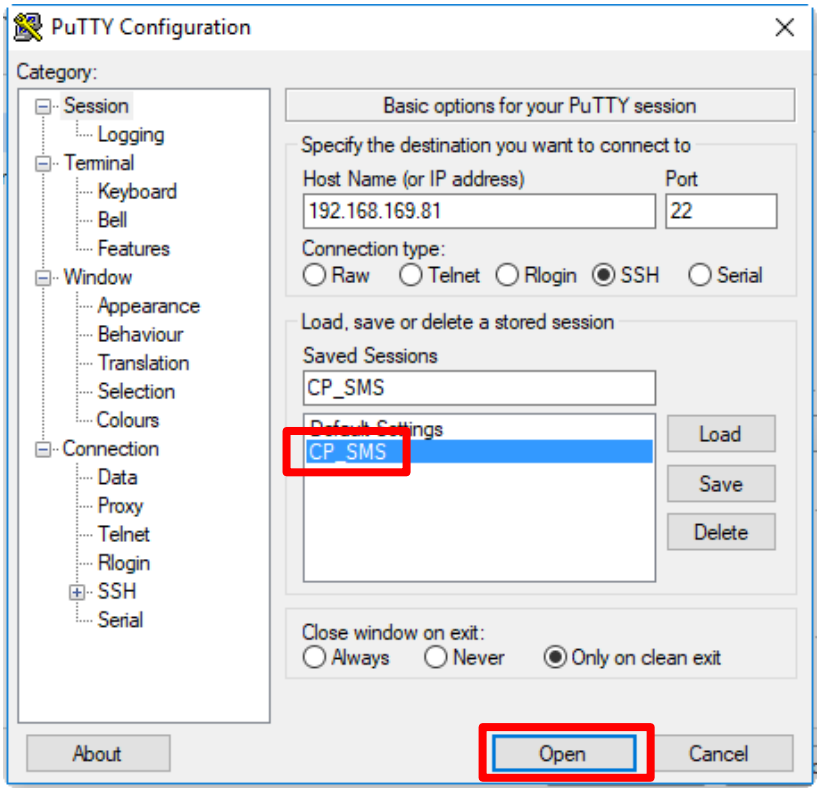


待左下角的任務選單出現「Database installed successfully on mgmt」就代表完成設定：



執行 scripts

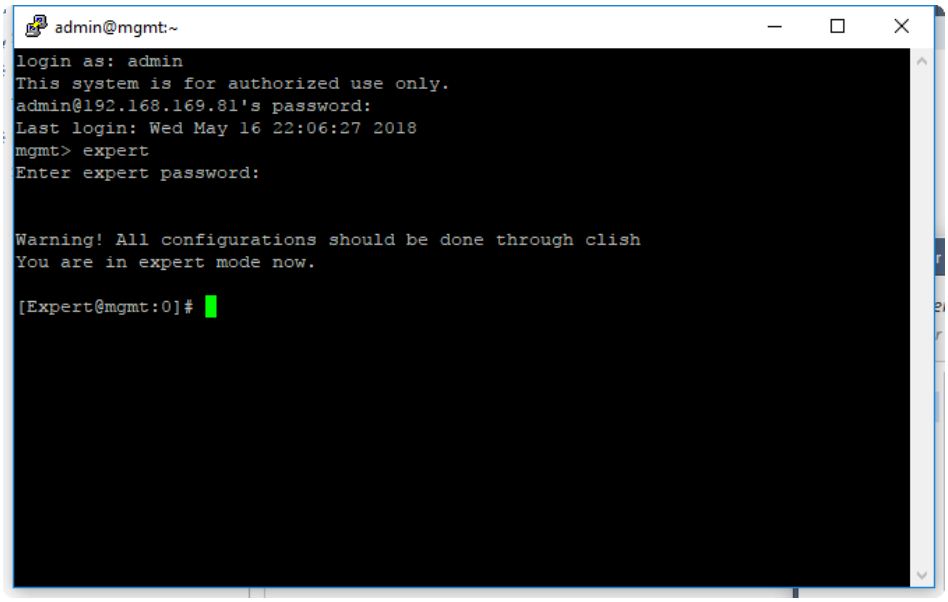
使用R80.10 Training資料夾中的putty登入SMS管理主機，並進入Expert模式：



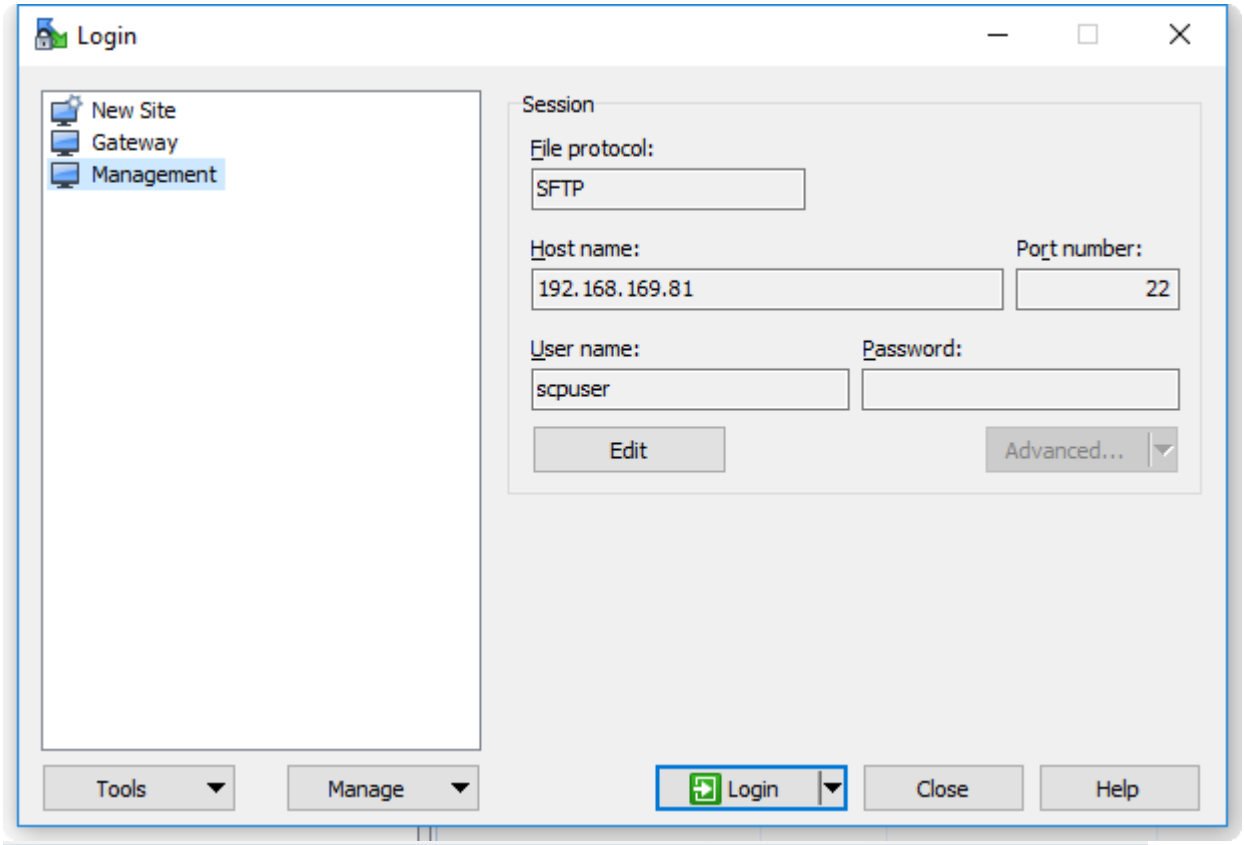
mgmt> **expert**
Enter expert password:

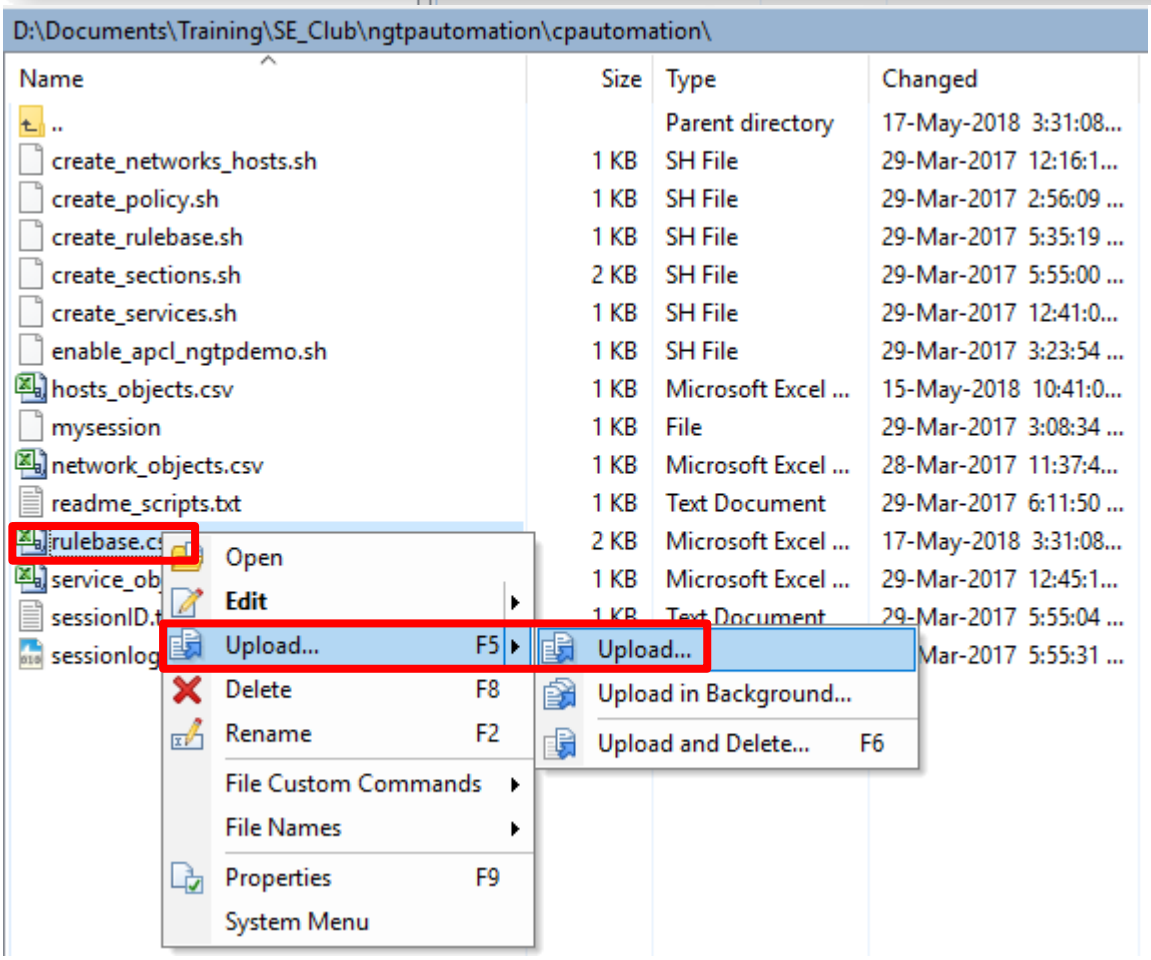
Warning! All configurations should be done through clish
You are in expert mode now.

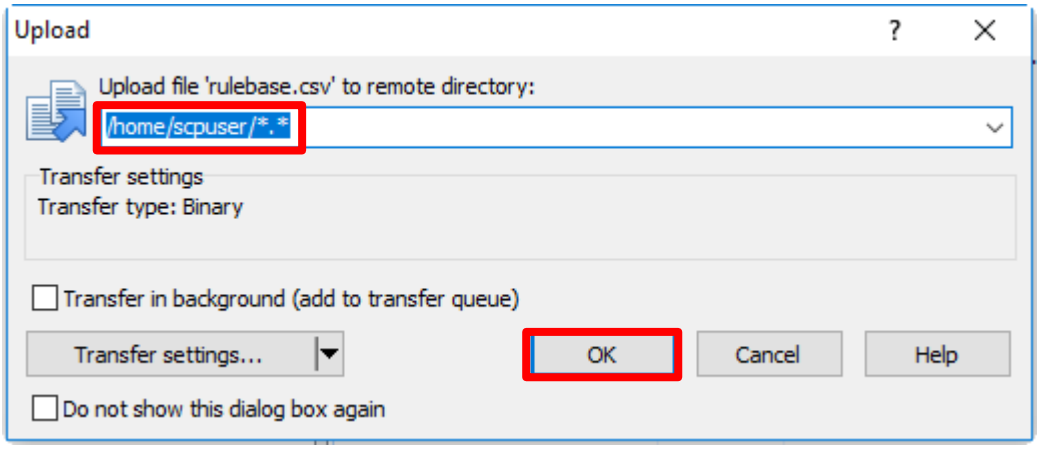
[Expert@mgmt:0]#



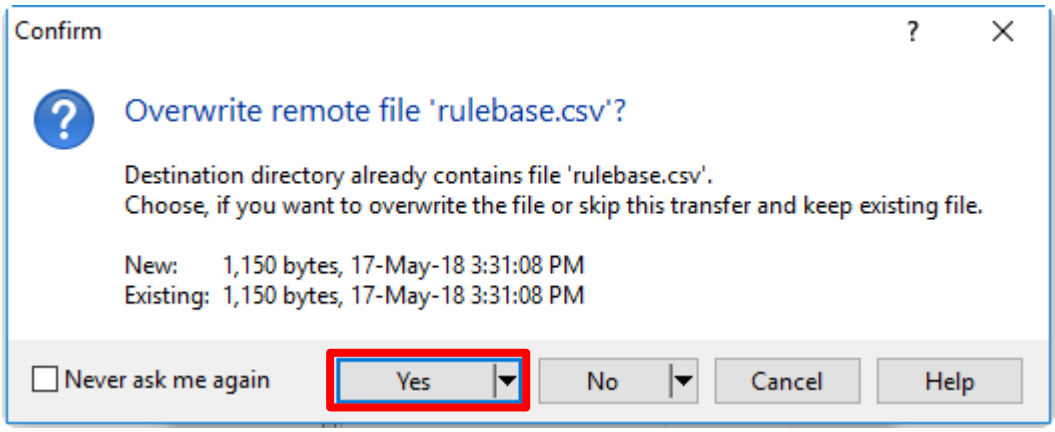
請開啟WinSCP並連到CP_SMS身上，上傳「**rulebase.csv**」至SMS管理主機：







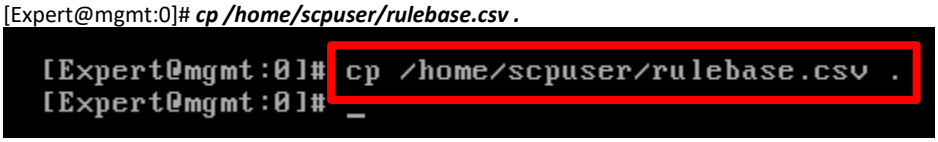
選擇「Yes」覆蓋原本的rulebase.csv檔案：



覆蓋完成之後，使用以下的指令將「rulebase.csv」複製至當前的目錄：

請注意指令最後有一個符號「.」

[Expert@mgmt:0]# ***cp /home/scpuser/rulebase.csv .***

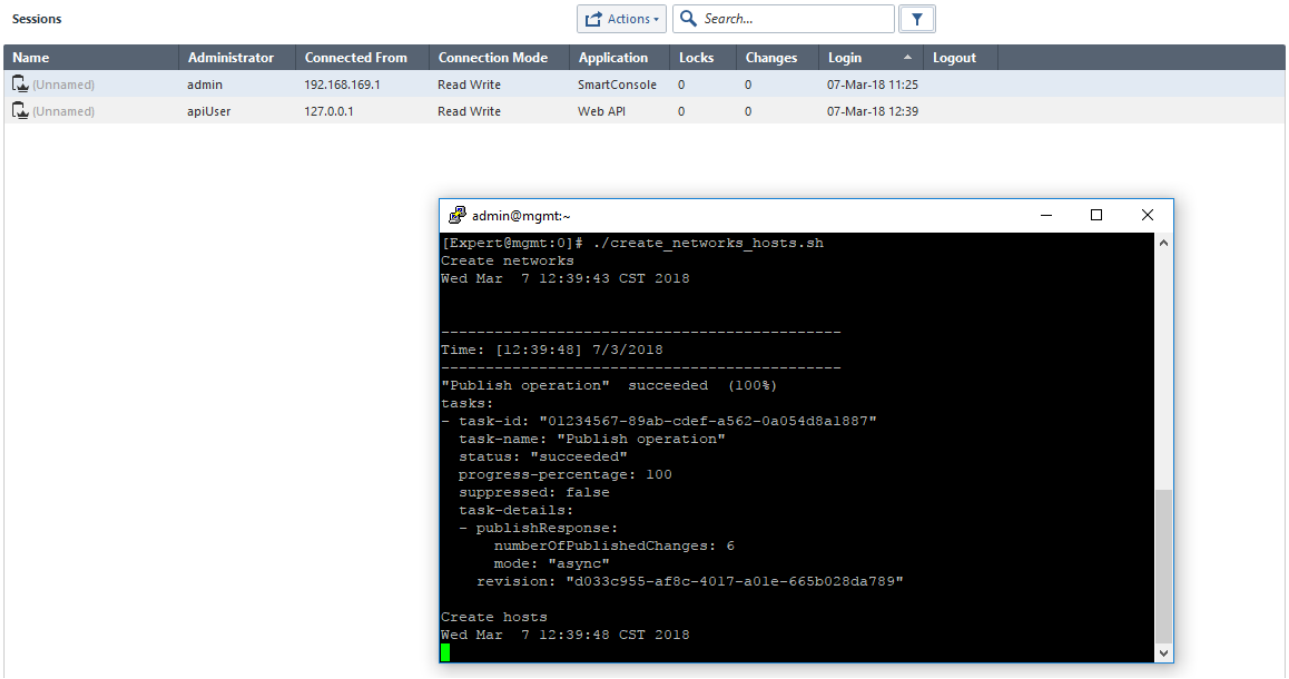


請依照以下的順序執行Script：

[Expert@mgmt:0]# **./create_networks_hosts.sh**

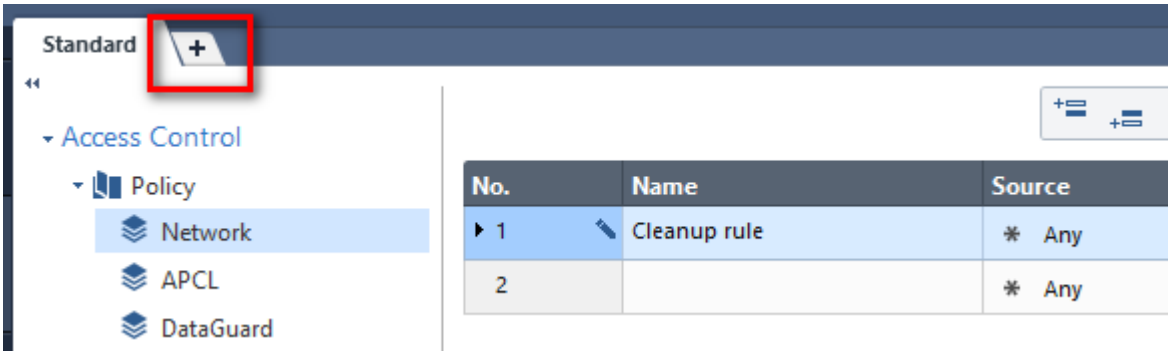
Running order:

1. create_networks_hosts.sh
2. create_services.sh
3. create_policy.sh
4. enable_apcl_ngtpdemo.sh
5. create_rulebase.sh
6. create_sections.sh

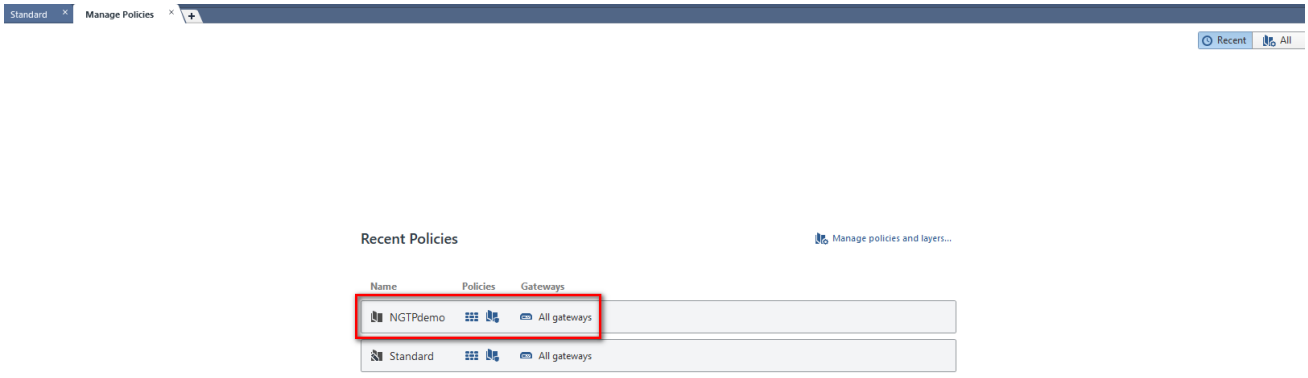


開啟匯入的 Policy Package

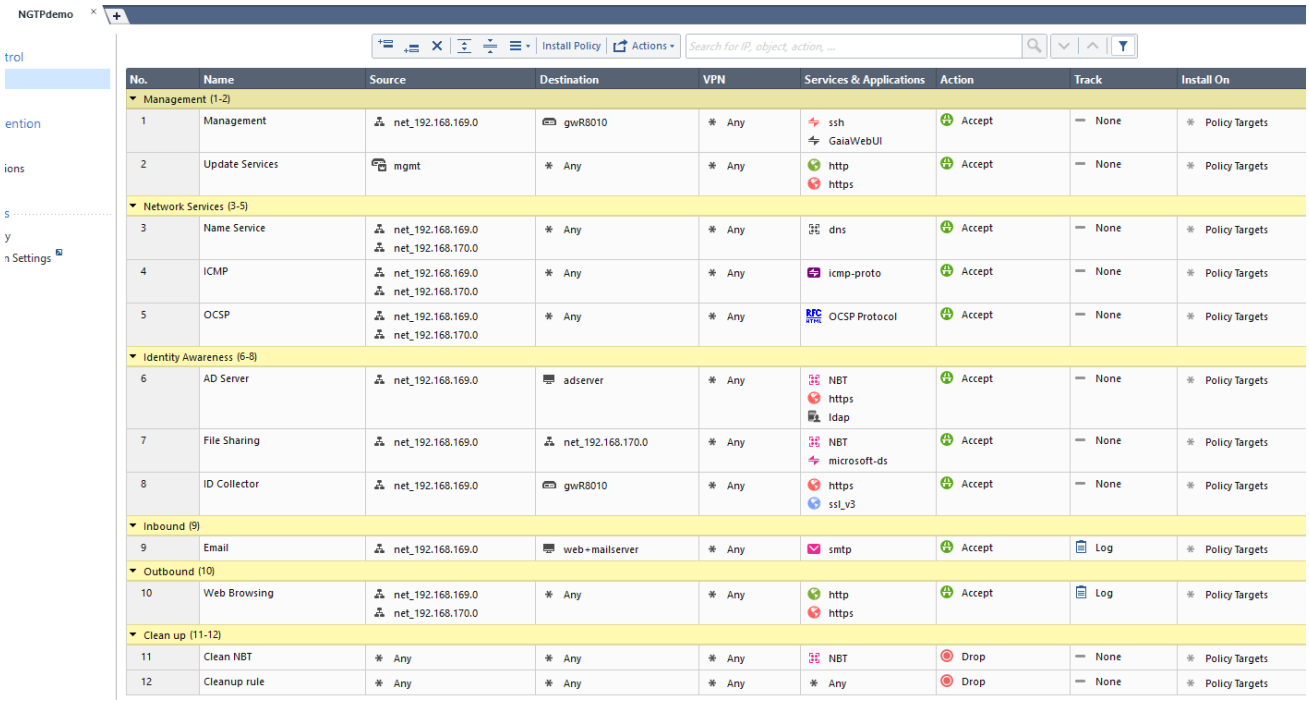
執行完成 6 個 Script 之後，回到 SmartConsole 的 Policy 頁籤，點選「+」號開啟新的分頁：



你會看見剛剛透過 API 自動建立的 Policy Package「NGTPdemo」，點擊 Policy Package 打開：



確認 Policy Package「NGTPdemo」的內容與下圖完全相同（**共有 12 條規則**）：



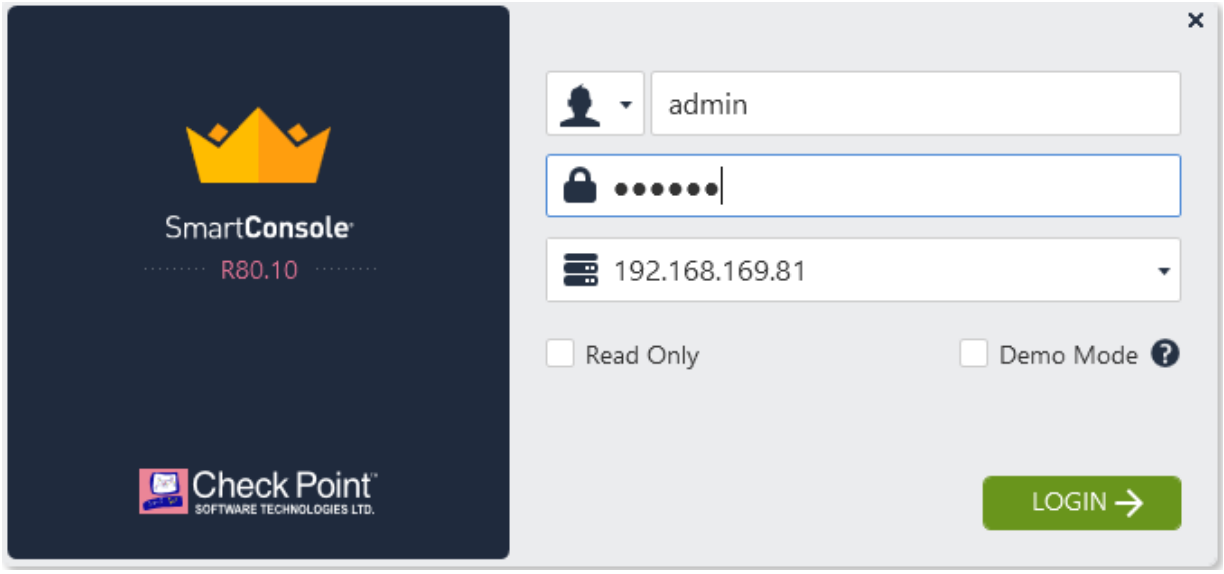
Lab 1: 體驗 R80.10 Unified Rule Base

啟用 APCL, URLF, IPS 以及 NAT 功能並設定規則

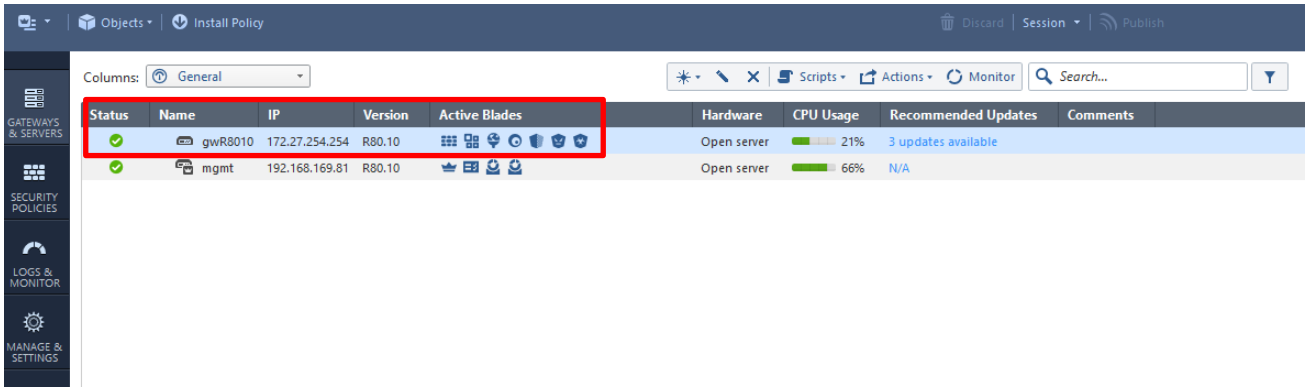
使用 R80.10 SmartConsole 登入 Management Server :

IP : 192.168.169.81

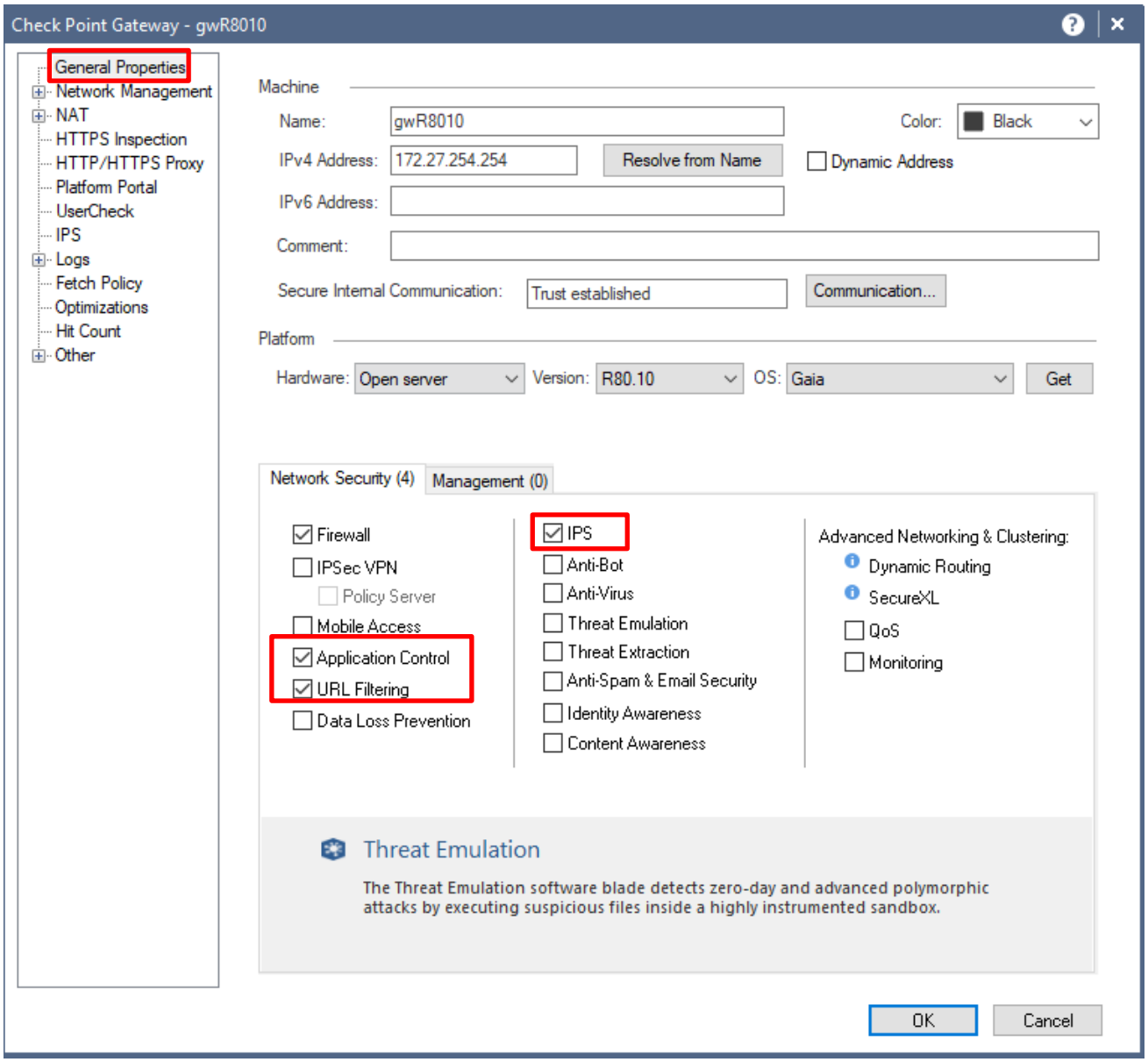
帳號密碼：admin / vpn123



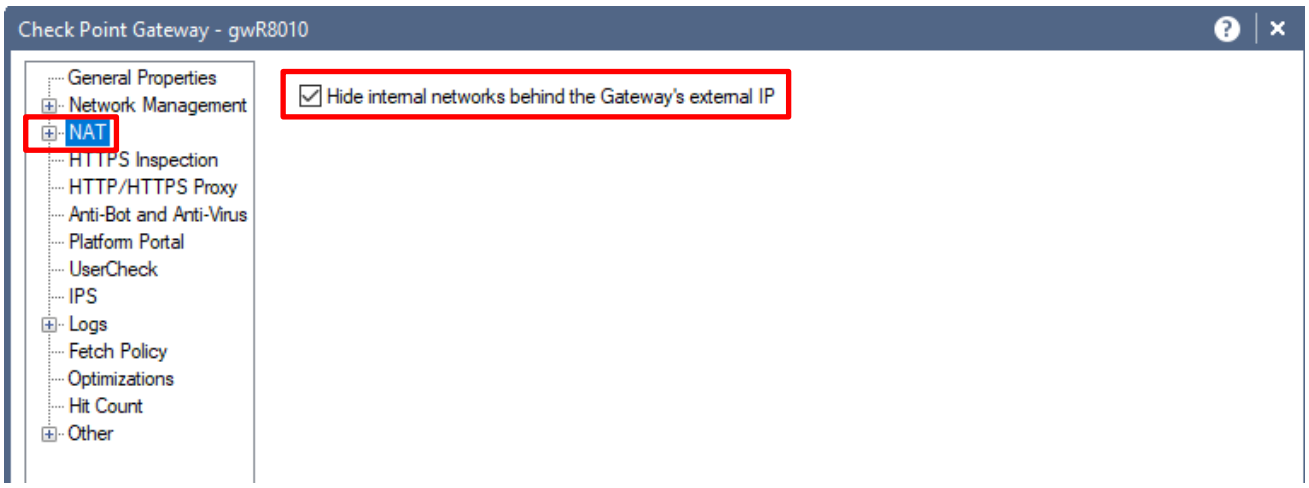
雙擊點選 Gateway 啟用 APCL, URFL, IPS :



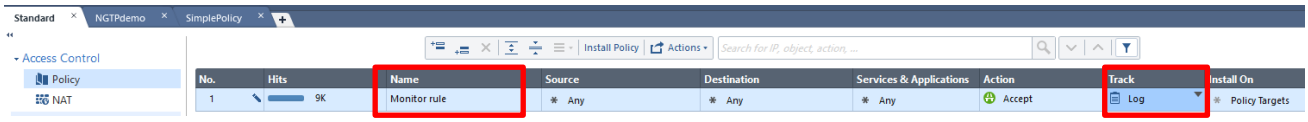
雙擊點選 Gateway 啟用 APCL, URFL, IPS :



切換到 NAT 的頁籤，勾選「Hide internal networks behind the Gateway's external IP」

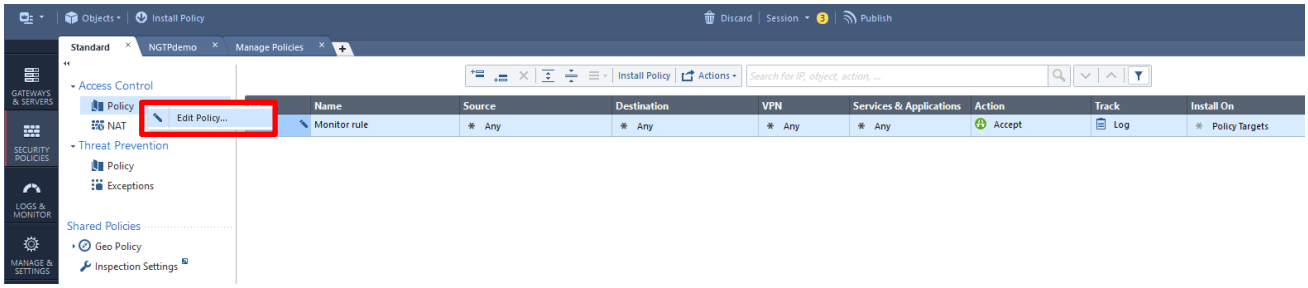


在 Standard Policy Package 中修改預設規則的 Name 為「Monitor rule」並調整 Track 欄位為「Log」：

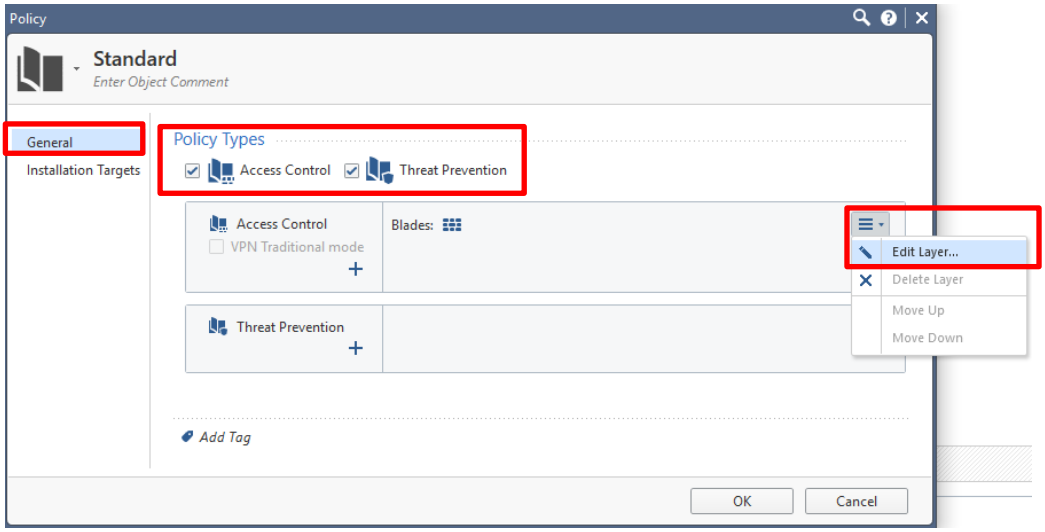


在規則上開啟 Firewall, APCL&URL 功能：

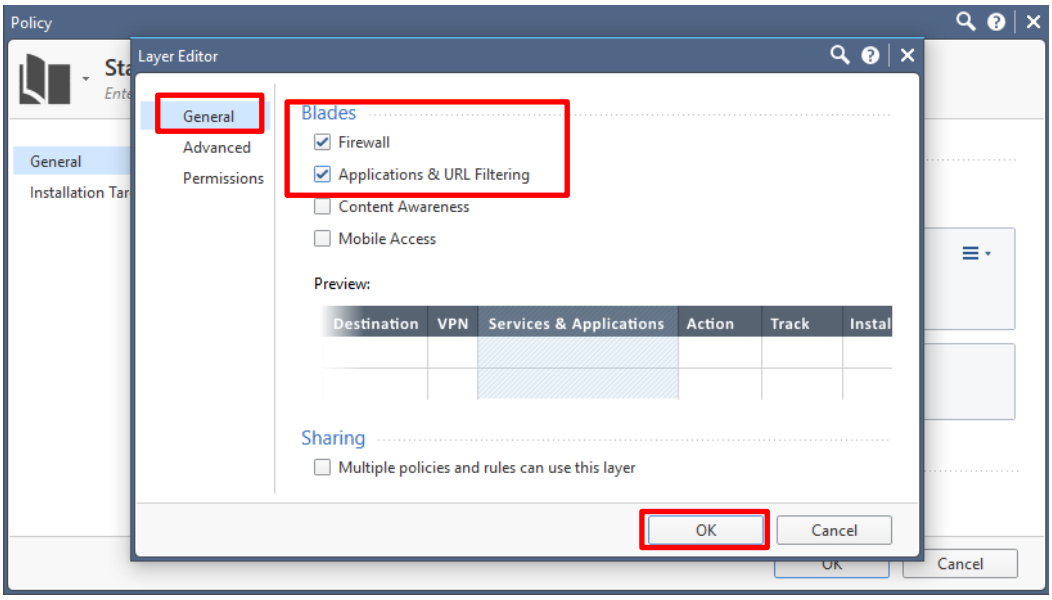
Access Control >> Policy 按右鍵「Edit Policy…」



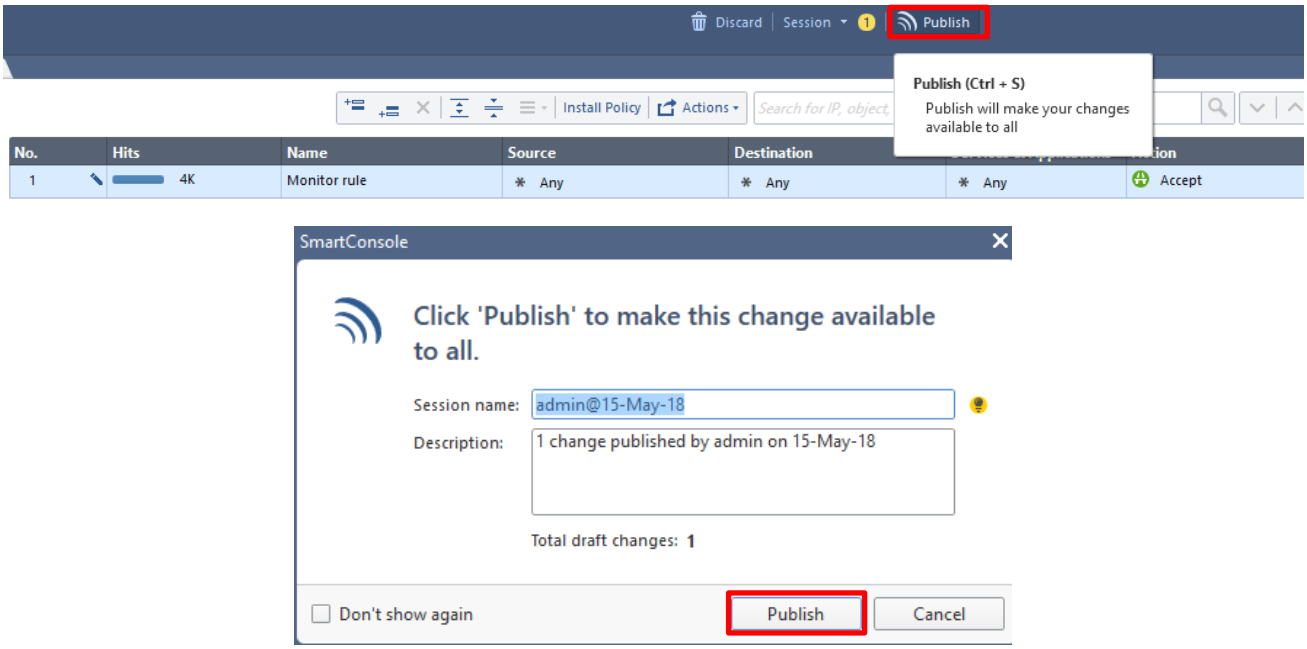
在 Access Control >> Policy 點選右邊下拉式選單「Edit Layer…」



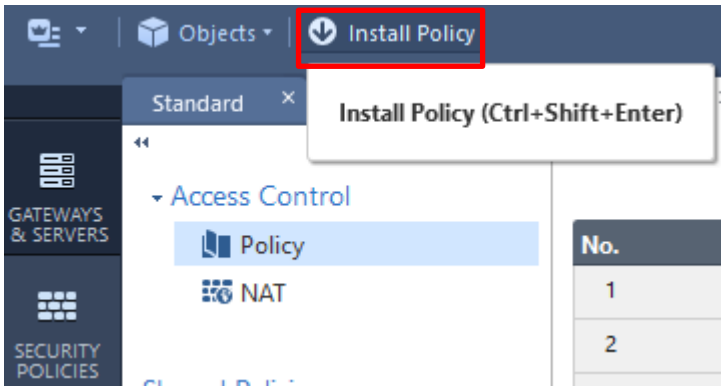
在 Blades 勾選「Firewall, Applications & URL Filtering」再點選 OK 確認。

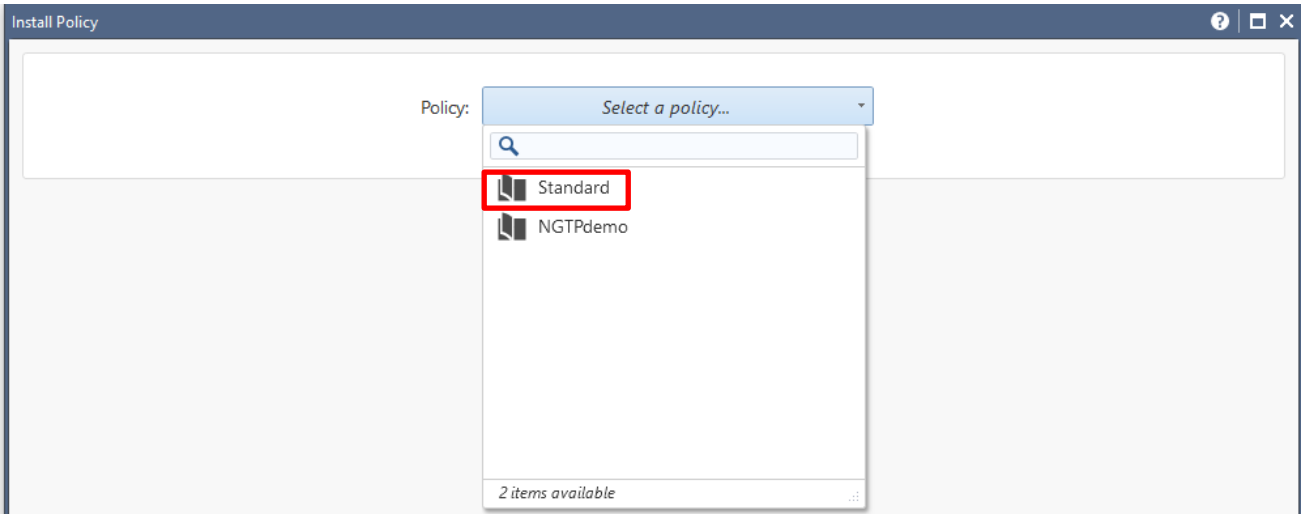


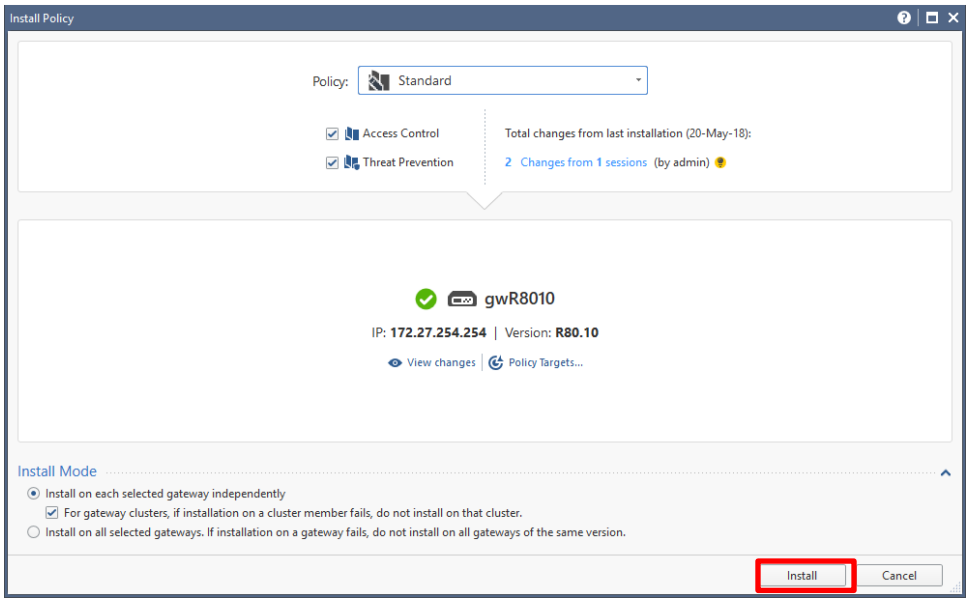
將設定進行「Publish」，儲存於 SMS 管理主機：



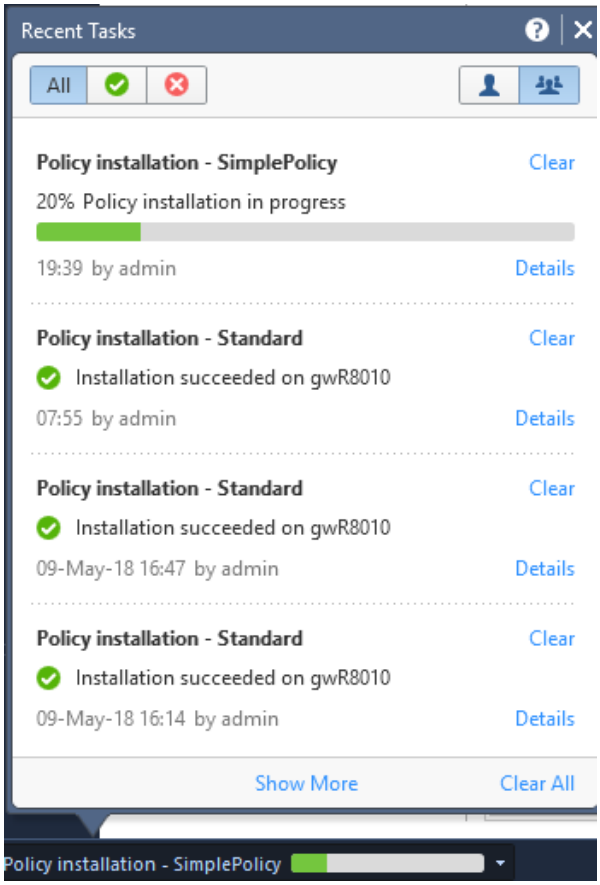
「Publish」執行完成之後點選上方的「Install Policy」將 Policy Package 從管理主機派送至 Gateway：

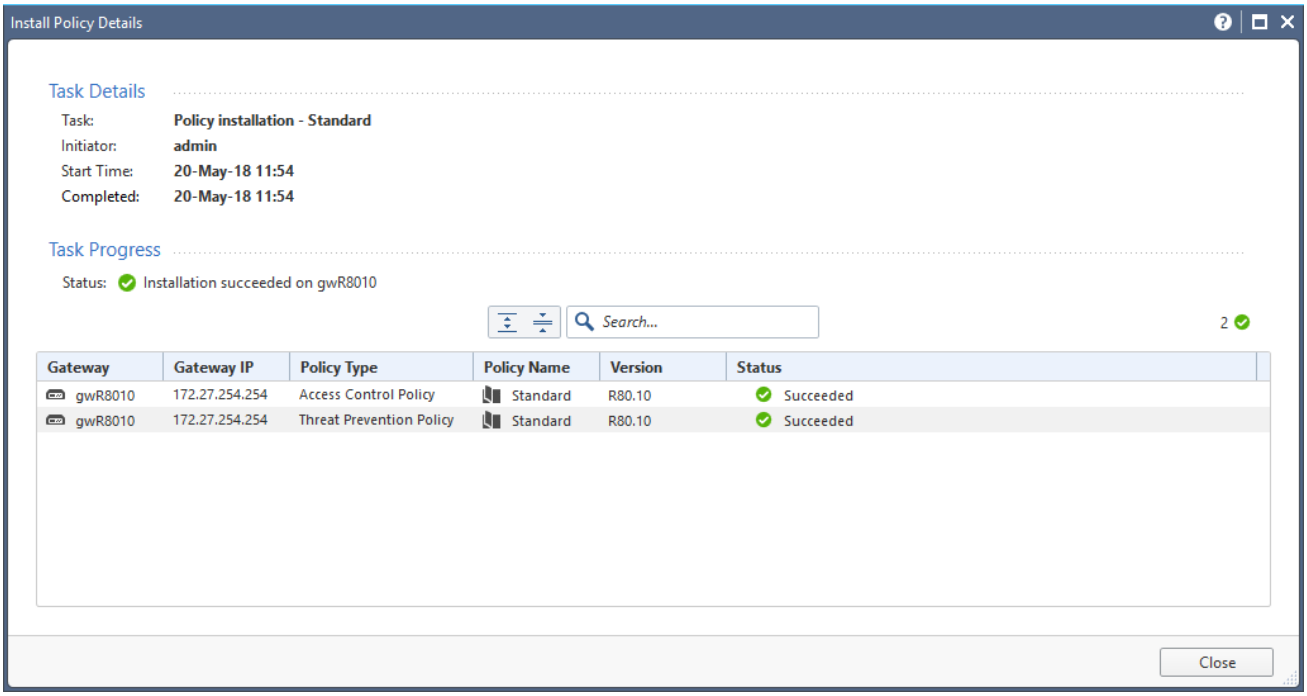






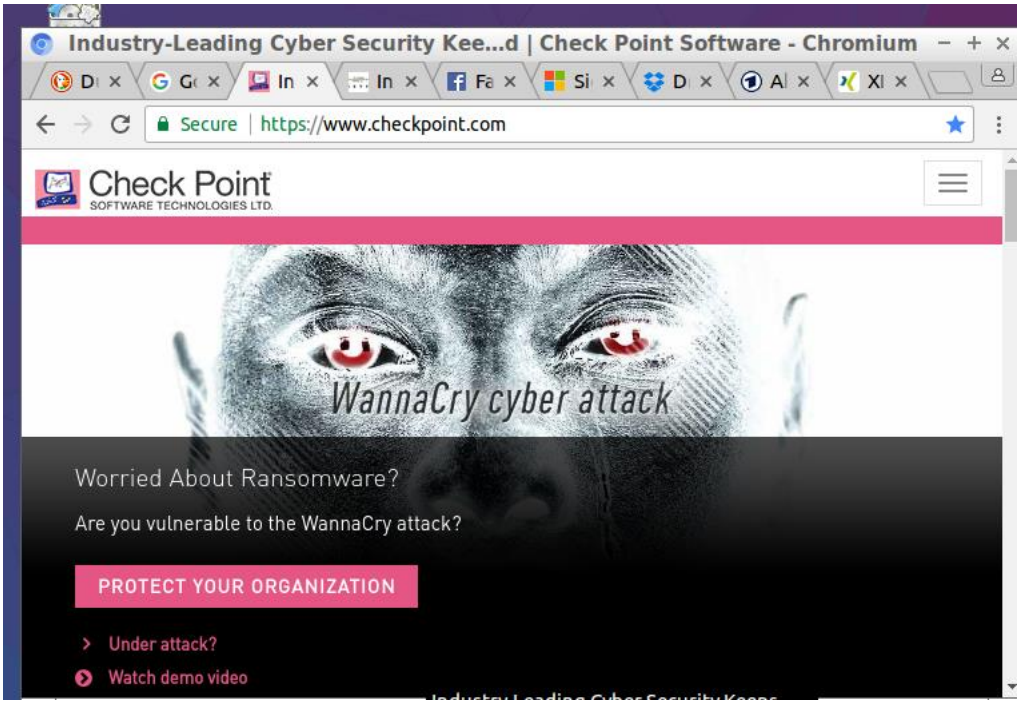
等待 installation progress 結束即完成 Policy 規則的派送：



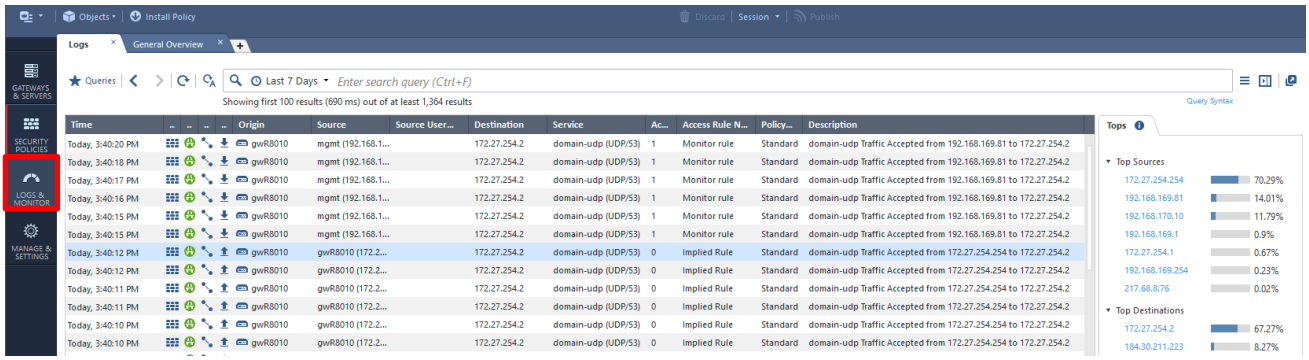


登入 Linux 虛擬機並開啟 Web Browser 內的所有我的最愛連結

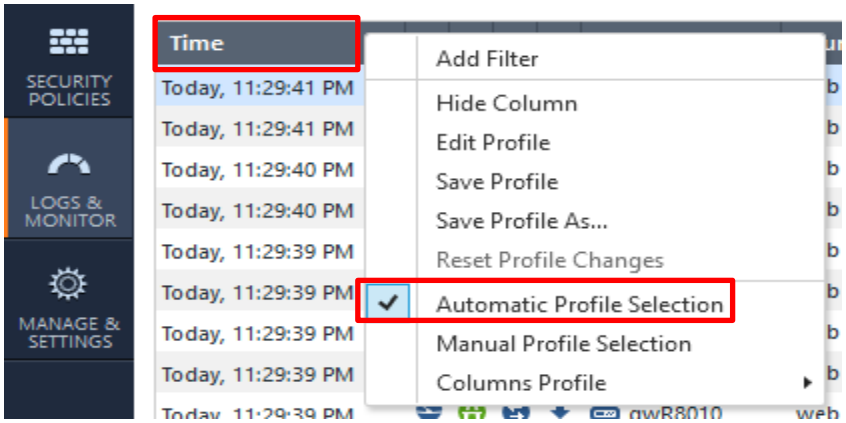
確認瀏覽器內「我的最愛」這些網頁，看看這些網頁是否都能夠開啟：



登入 R80.10 SmartConsole 並切換到 Log&Monitor 頁籤

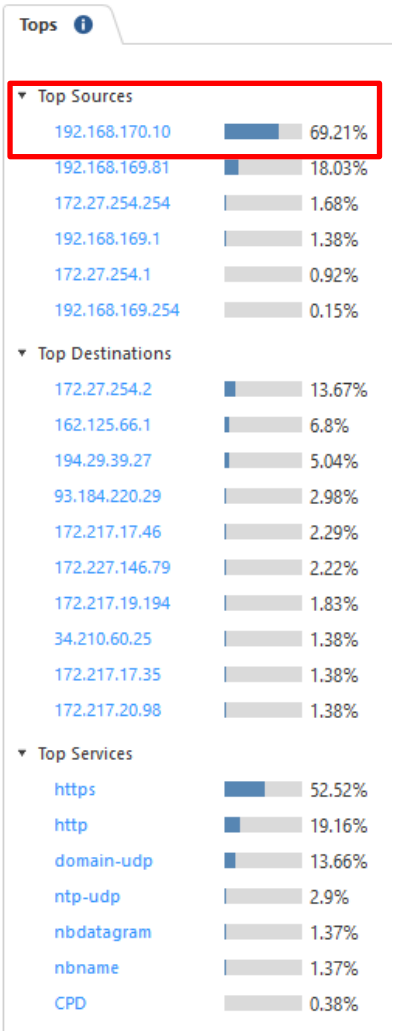


在上方灰色欄位處按右鍵並選擇「Automatic Profile Selection」：

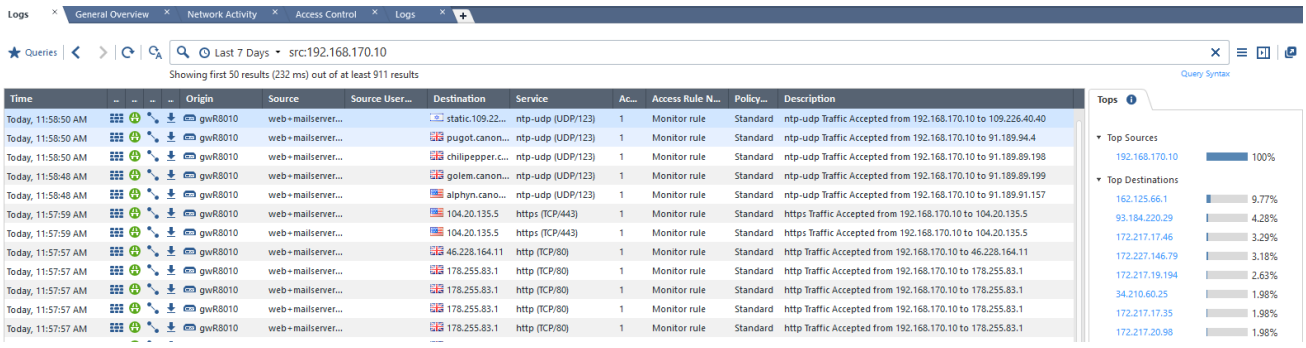


展開右邊的 Tops 選項，觀察一下你看到哪些 IP 與 Services 服務?

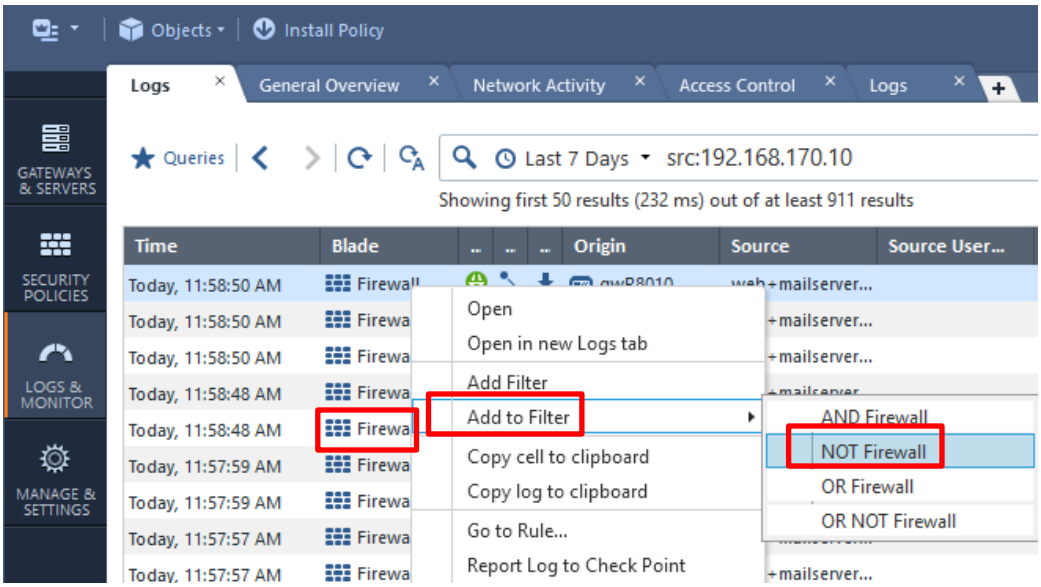
然後嘗試點選一下 Linux 主機的 IP (192.168.170.10)



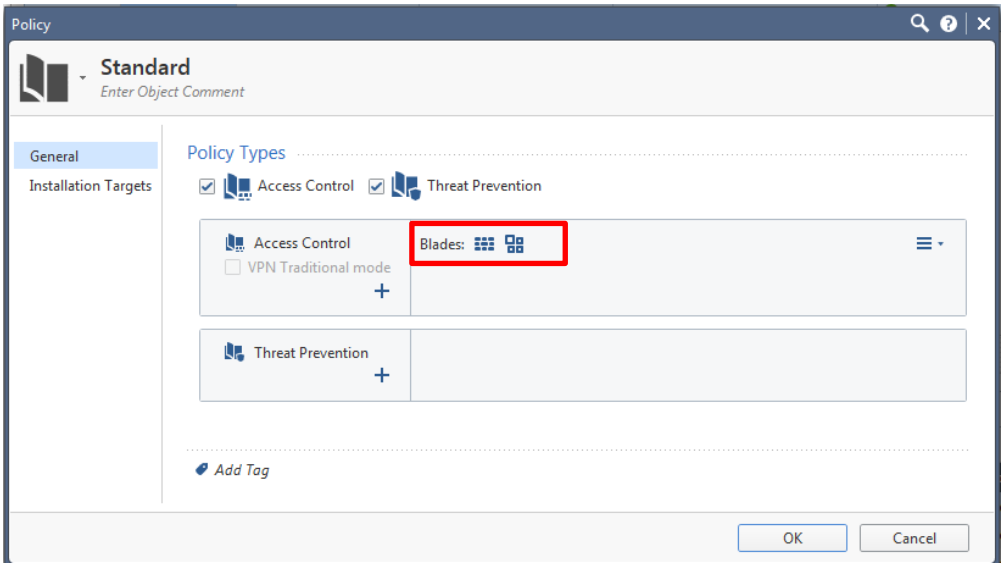
有看到任何跟應用程式(APCL)或網頁(URL)相關的 Log 嗎?



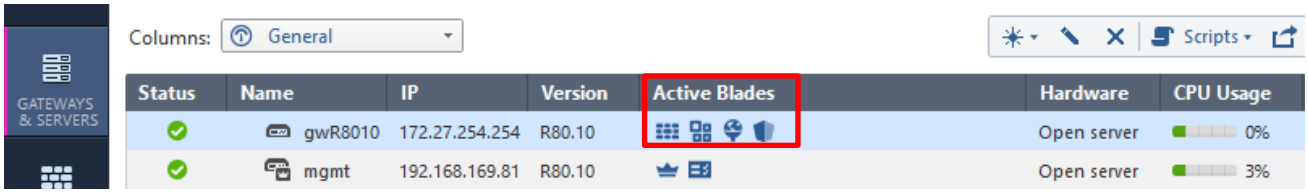
試著將 Firewall Log 排除之後再找看看(在 Blade 欄位點選 Firewall 之後按右鍵)：



確認一下 APCL & URLF Blades 功能是否已經啟用在你的 Policy Layer 裡面了?



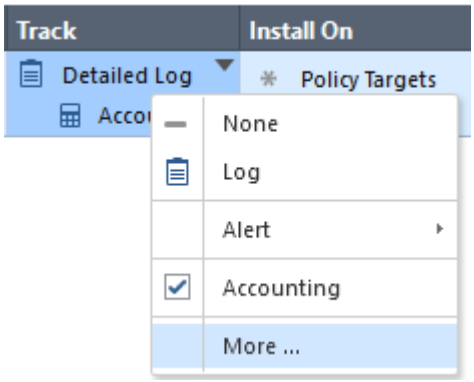
確認一下 APCL & URLF Blades 在 Gateway 上是否已經有開啟了?



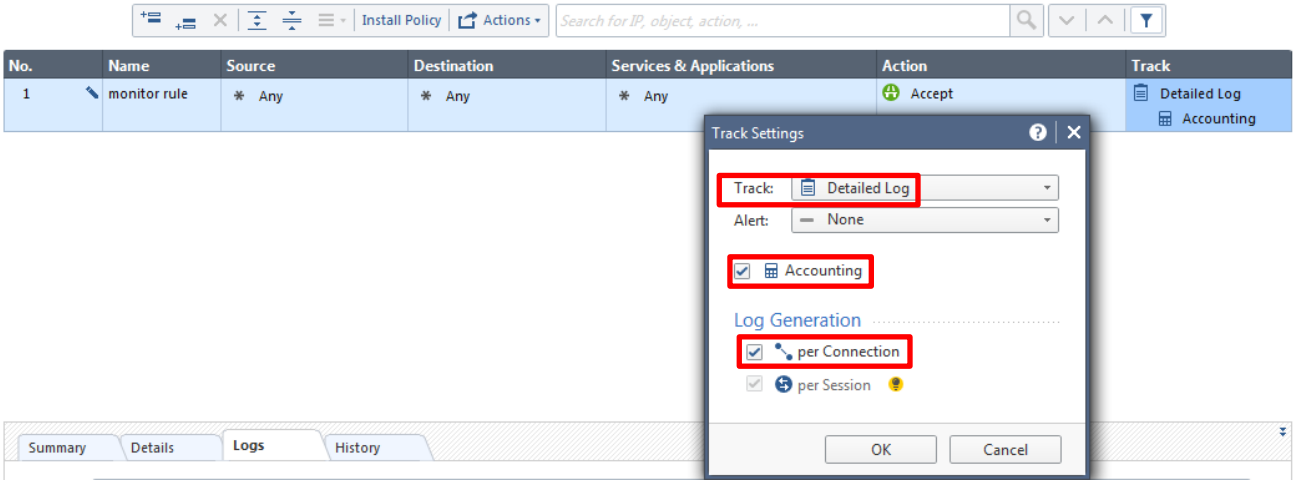
如果上述設定都確認過了，思考一下為何沒有 APCL & URLF Log?

更改規則的 Log 設定並且 install policy

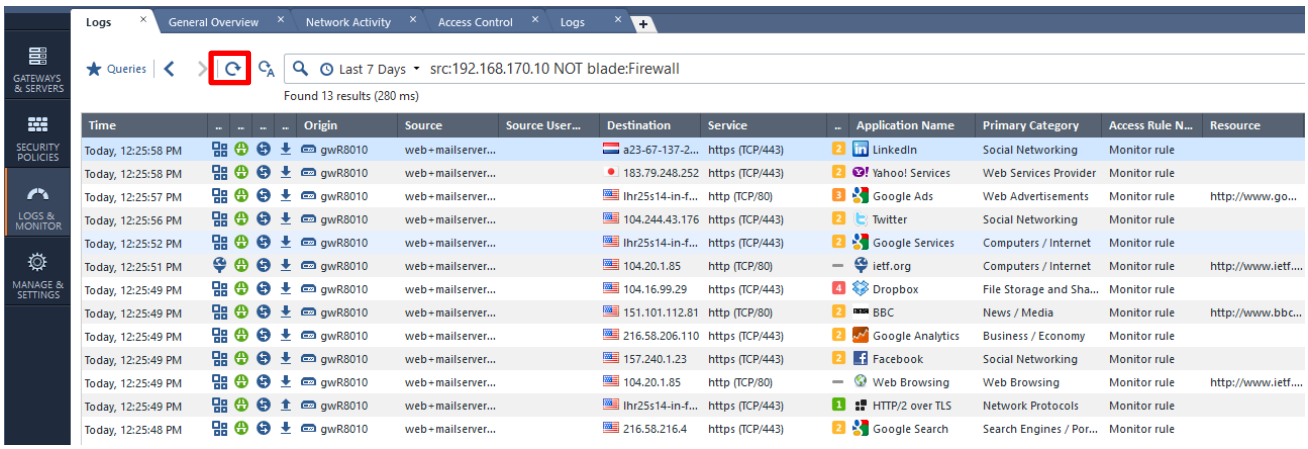
在 Track 欄位上按右鍵選擇「More…」：



更改 Log 的設定為「Detailed Log」並勾選 Accounting 以及「per Connection」：



重新整理一下 Linux 主機的瀏覽器以及 Log view，現在你能看到 APCL & URLF Log 了嗎?



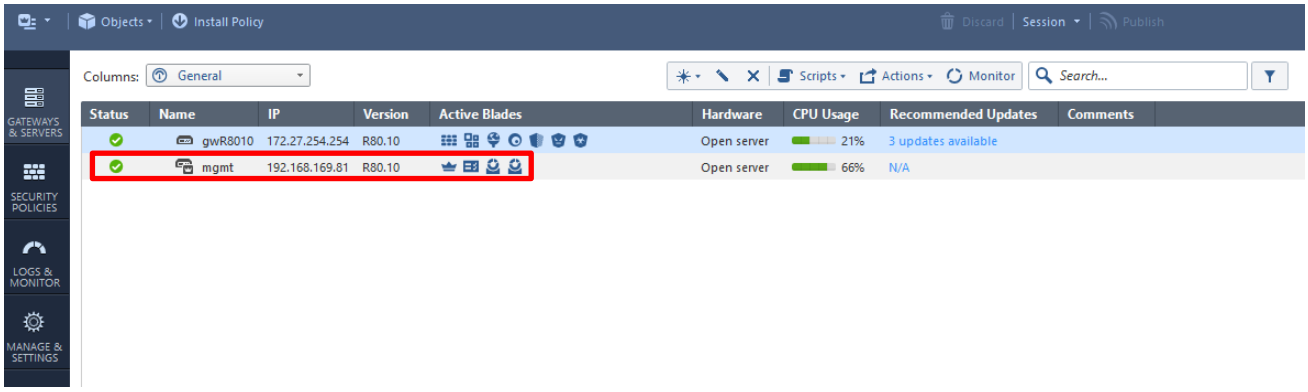
如果可以看到 APCL & URLF Log，思考一下為何同一條規則調整 Log 設定後顯示的內容不同?

比較一下 HTTP 和 HTTPS 的 Log 有什麼差別?

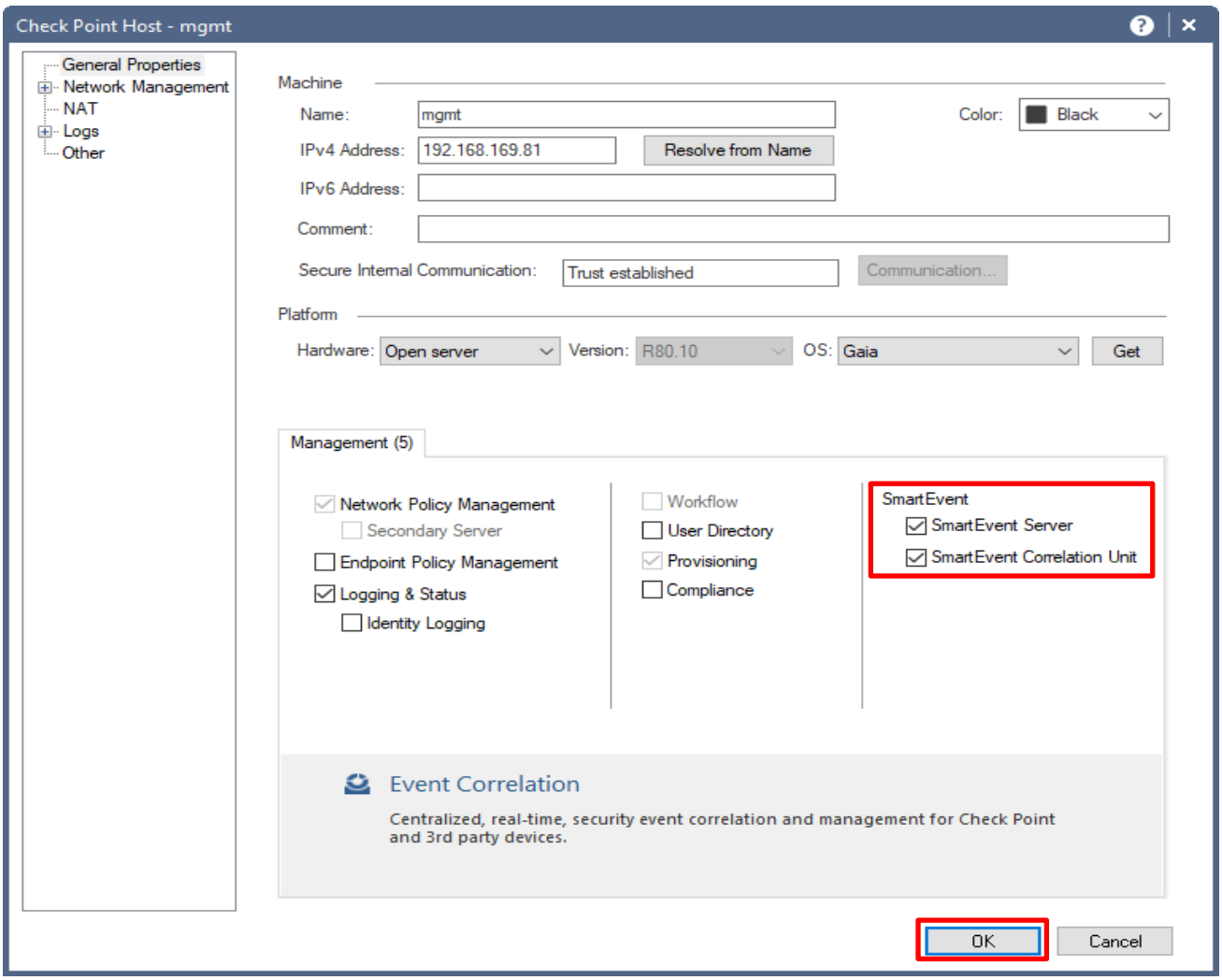
使用 Logs & Monitor 來產生 APCL & URLF 使用報表

依照以下的做法來開啟 SmartEvent 報表功能：

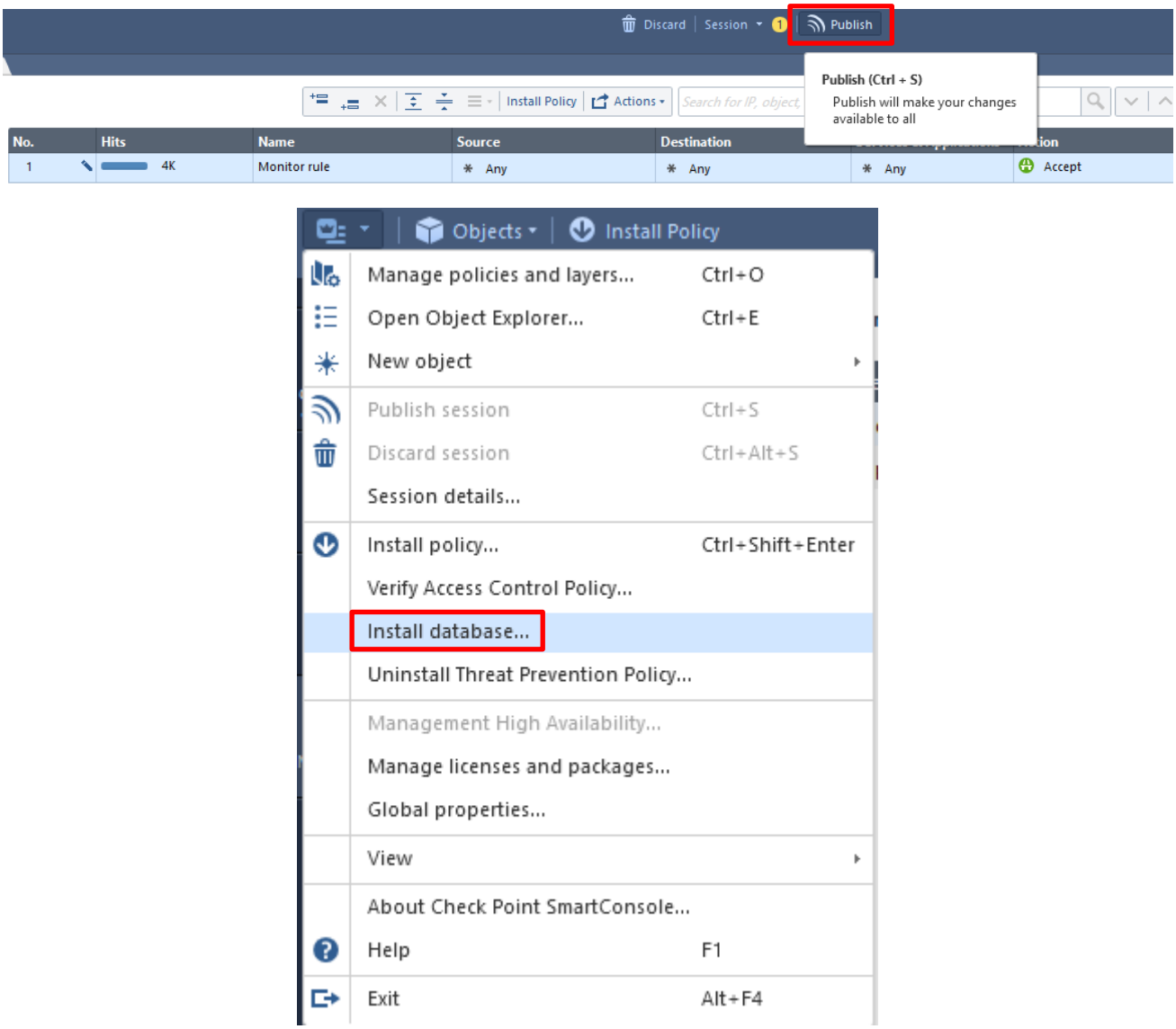
- 在管理主機 SMS 上啟用 SmartEvent and the Correlation Unit 功能
  - 切換到 Gateway & Servers 頁籤，在 mgmt 物件上連點 2 下開啟 SMS 管理主機物件



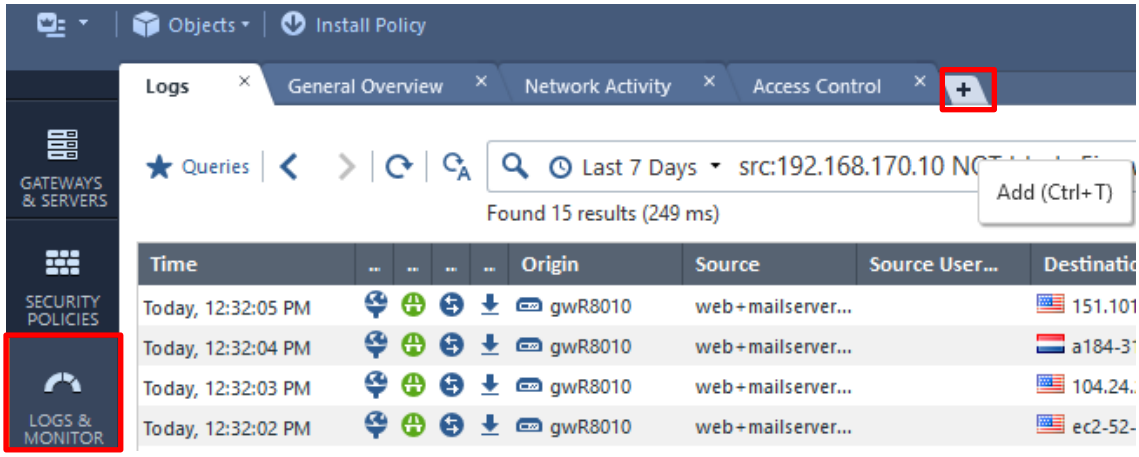
  - 在 mgmt 物件中勾選「SmartEvent Server」以及「SmartEvent Correlation Unit」並點選 OK。



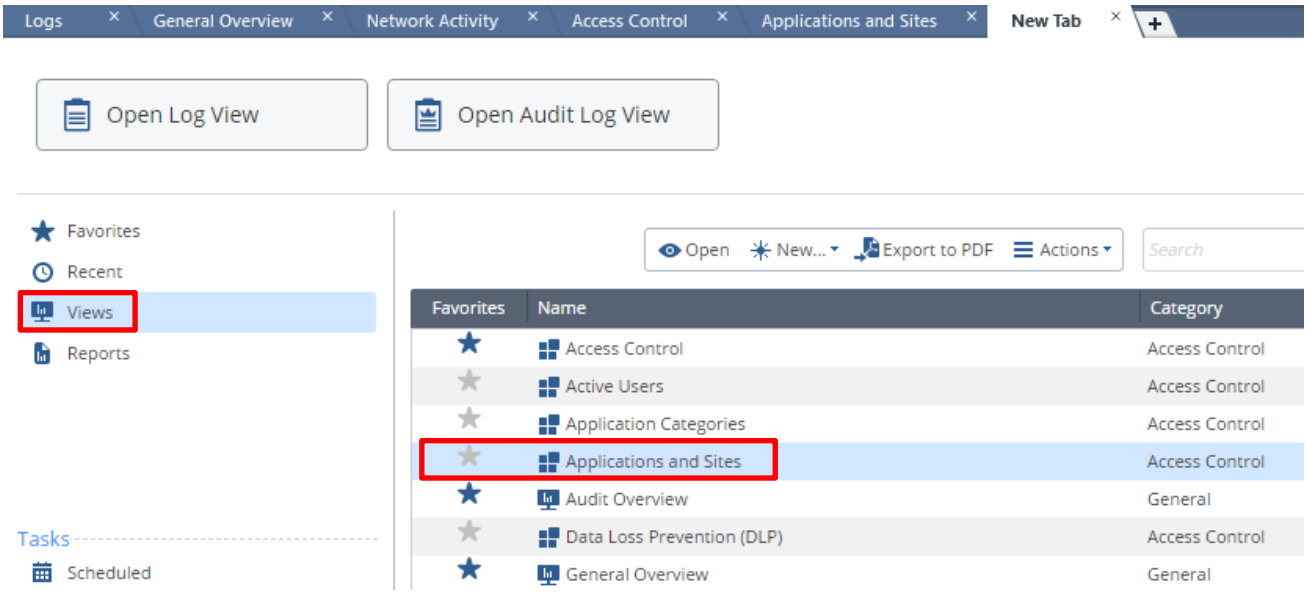
- 將設定「Publish」並且「Install Database」



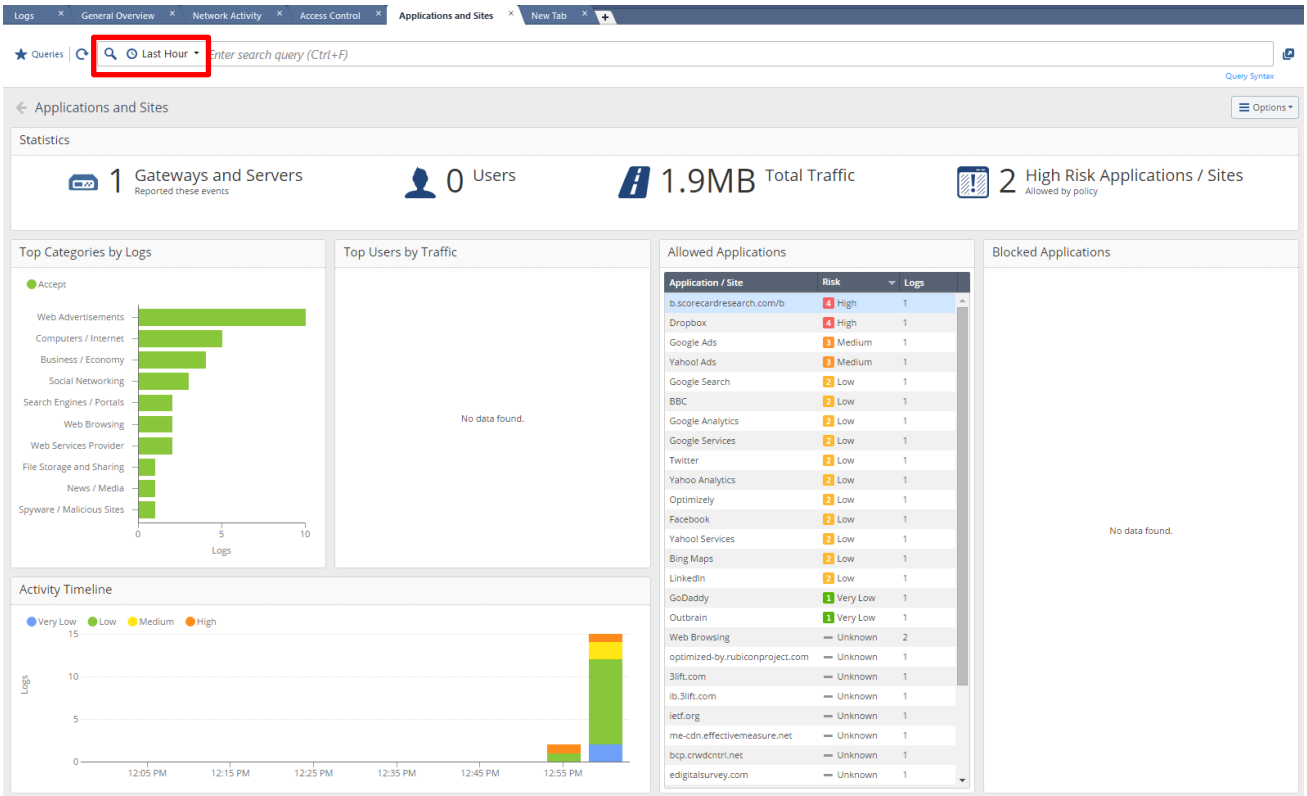
- 檢視 Views：Applications and Sites
  - 待 Install database 結束，切換到 Logs & Monitor > 頁籤，點選右上角的「+」開啟新分頁。



- 點選左邊「Views」頁籤，再連點 2 下選擇右邊「Applications and Sites」

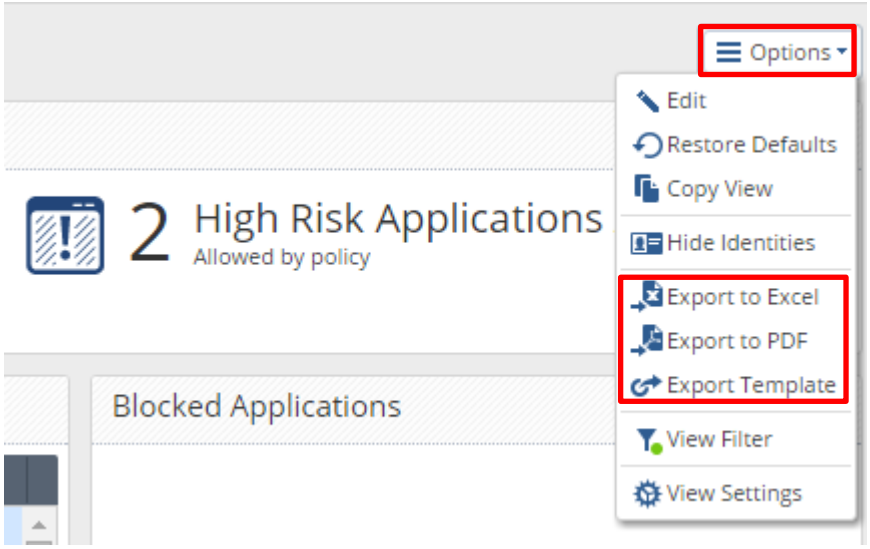


- 切換上方時間到“Last Hour”並重整報表，會看到如下圖的畫面

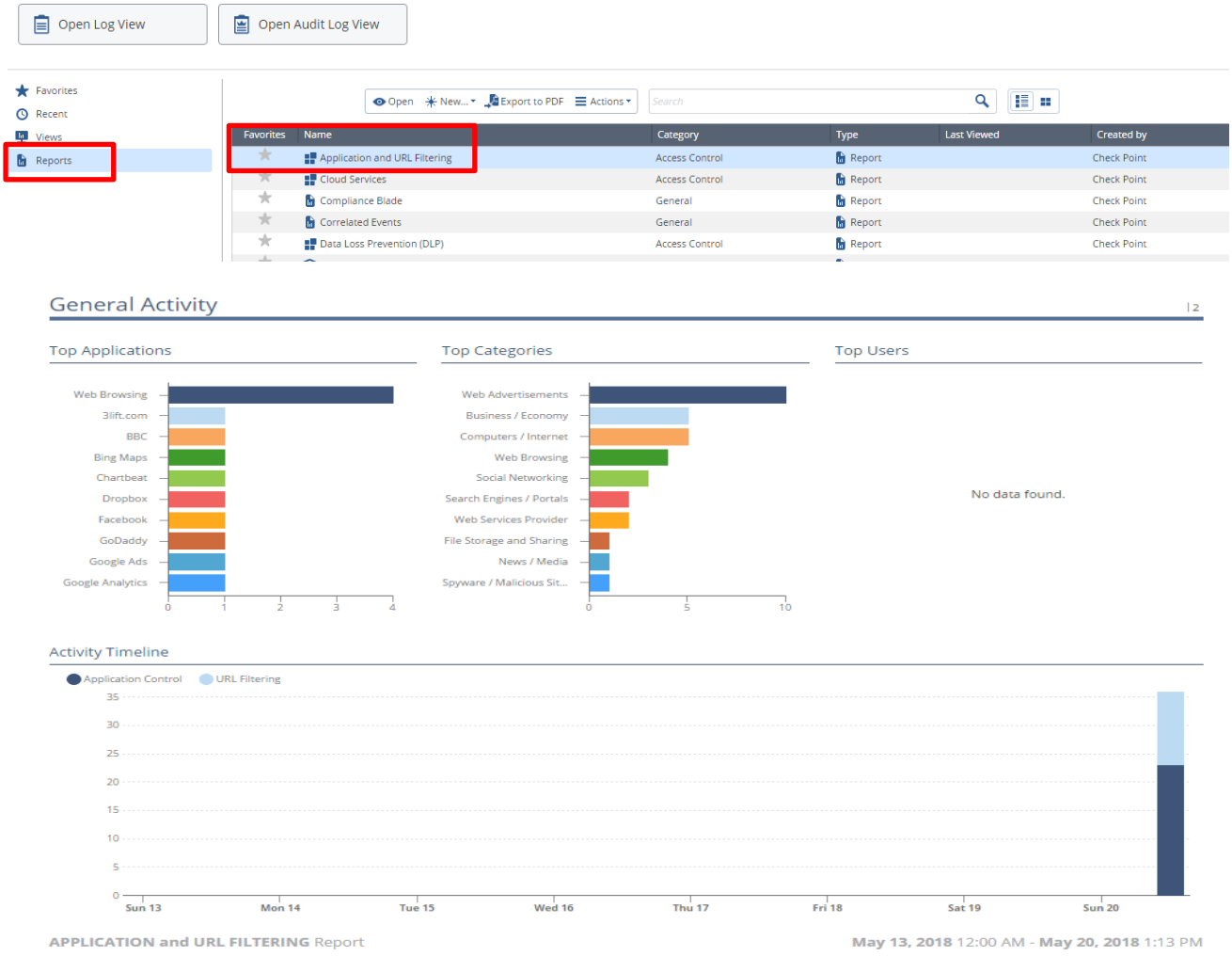


Generate a report

在剛剛的畫面右上角點選「Options」可以進行 Views 的編輯或是匯出成 Excel, PDF：



或是開啟新分頁切換到「Reports」頁籤，選擇預設的範例報表或是自訂報表：



觀察 gateway 狀態

使用桌面 R80.10 Training 資料夾中的 Putty 連線一個 SSH session 到 gateway 上並執行「cpview」：

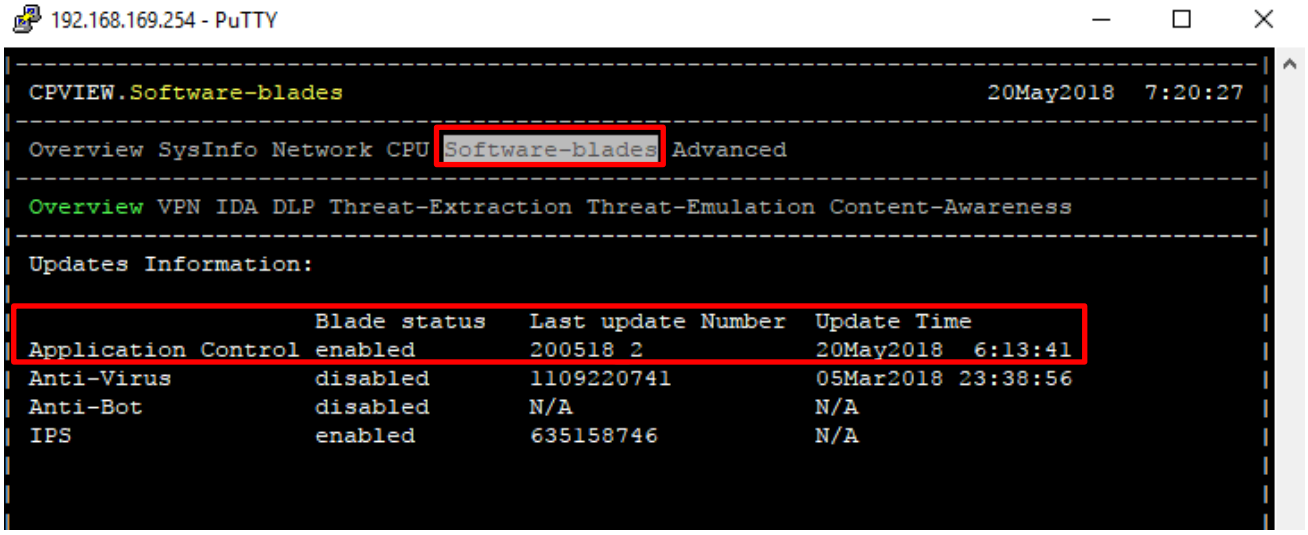
192.168.169.254 - PuTTY

```
login as: admin
This system is for authorized use only.
admin@192.168.169.254's password:
Last login: Sat May 19 18:44:37 2018
gwr8010> cpview
```

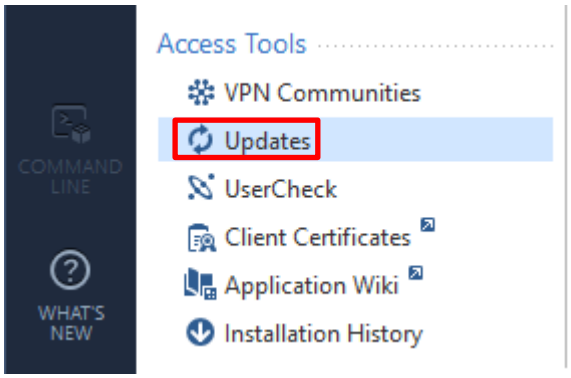
192.168.169.254 - PuTTY

```
CPVIEW.Overview
Overview SysInfo Network CPU Software-blades Advanced
CPU:

Num of CPUs:      4

       CPU      Used
         0        1%
         1        1%
         3        1%
Memory:

            Total MB   Used MB   Free MB
Physical       3,809     1,212     2,596
FW Kernel      3,047       337     2,710
Swap           3,067         0     3,067
Network:

Bits/sec                            134K
Packets/sec                          15
Connections/sec                       0
Concurrent connections               14
Disk space (top 3 used partitions):

Partition  Total MB   Used MB   Free MB
/            14,878     4,755     9,355
/boot           288        23       250
/var/log     13,887       951    12,218
Events:

# of monitored daemons crashes since last cpstart         0
```

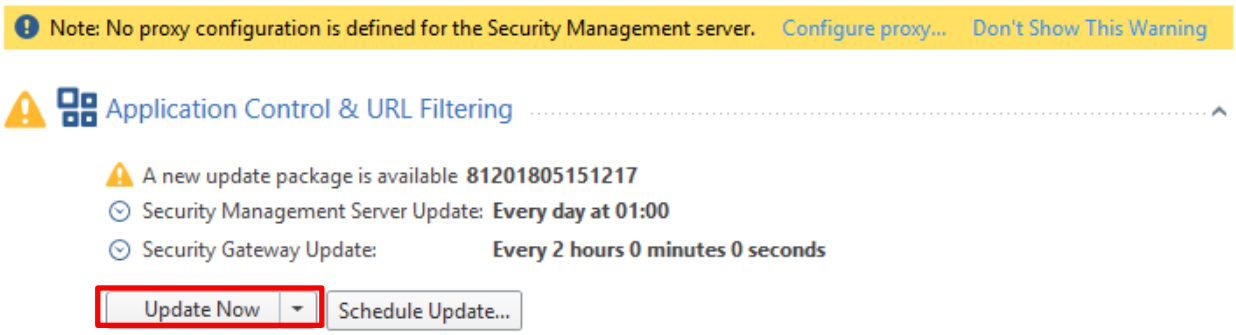

使用鍵盤的方向鍵切換 View 到「Software-blades」頁籤，檢視有開啟哪些功能以及是否有 Update：



如果尚未 Update，可以回到 SmartConsole，切換到 Security Policy 頁籤，點選左下角的 Access Tools 中的「Updates」選項：



點選 Application Control & URL Filtering 中的「Update Now」即可進行更新，初次更新約 5-8 分鐘：

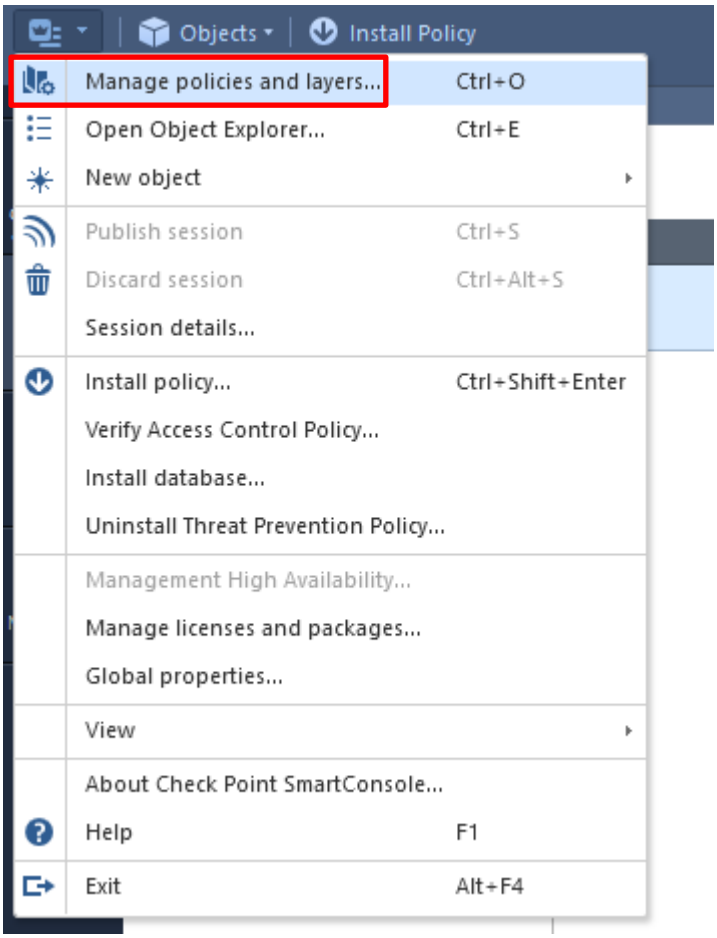


Lab 2: 了解 Content Awareness 以及 Inline Layer 的運作

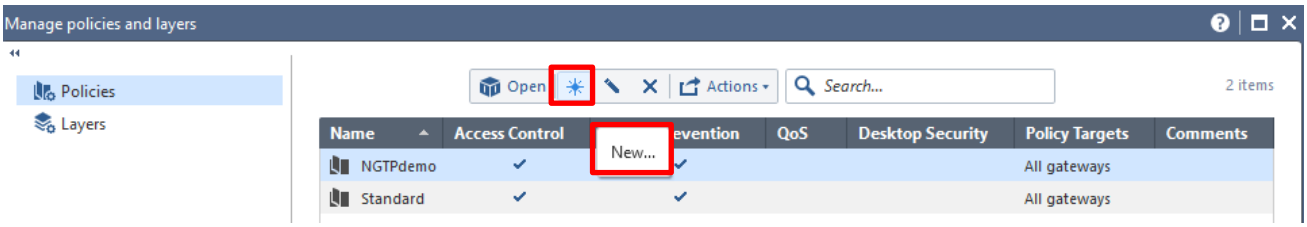
目標先建立一個新的 Policy Package「SimplePolicy」如下圖所示：

No.	Name	Source	Destination	Services & Applicat...	Content	Action	Track
1	Management	net_192.168.169.0	gwR8010	ssh	Any	Accept	None
2	ICMP	net_192.168.169.0	net_192.168.170.0	icmp-proto	Any	Accept	Log
3	DNS	Any	dnsserver OpenDNS	dns	Any	Accept	None
4	Parrent rule for web server	Any	web+mailserver	Web Browsing	Any	WebServerPolicyLayer	N/A
4.1	Credit Card Numbers	Any	web+mailserver	Web Browsing	Download Traffic PCI - Credit Card Numbers	Drop Content Management	Detailed Log Accounting
4.2	Documents	Any	web+mailserver	Web Browsing	Download Traffic Document File	Accept	Detailed Log Accounting
4.3	Spreadsheets	Any	web+mailserver	Web Browsing	Download Traffic Spreadsheet or CSV File	Accept	Detailed Log Accounting
4.4	Cleanup rule	Any	Any	Any	Any	Accept	Log
5	SMTP	net_192.168.169.0	web+mailserver	smtp	Any	Accept	Log
6	Cleanup rule	Any	Any	Any	Any	Drop	Log

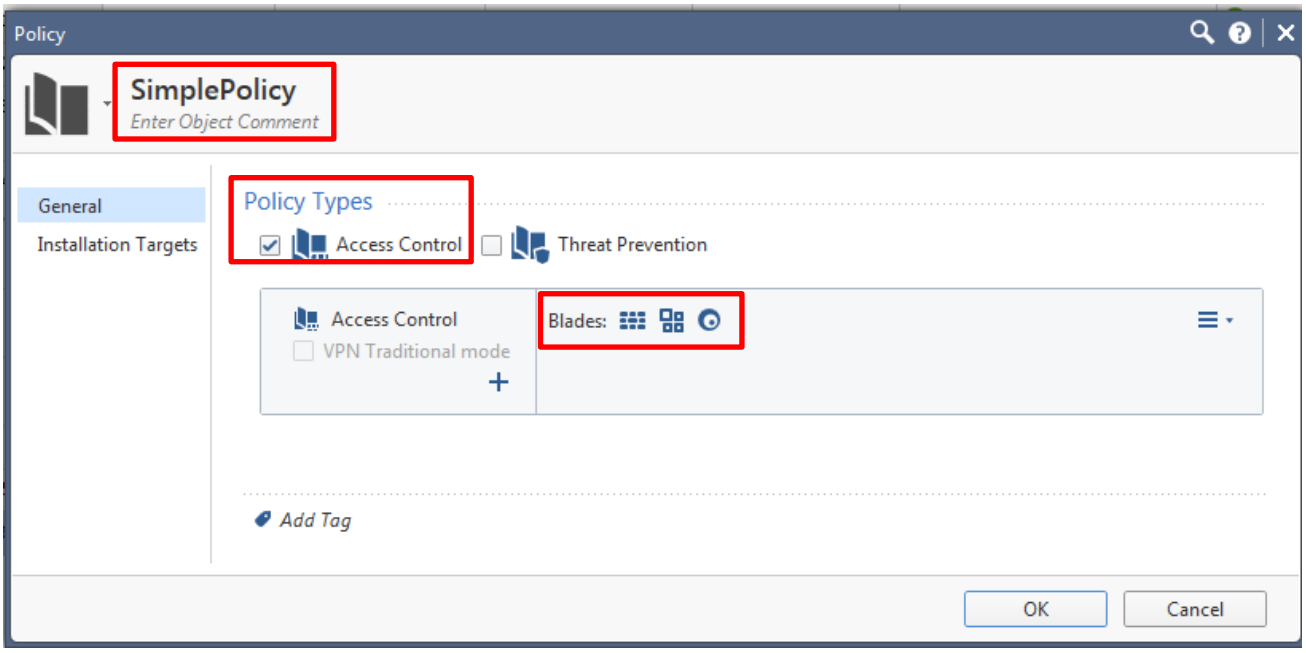
點選左上角下拉式選單中的「Manage policies and layers…」：

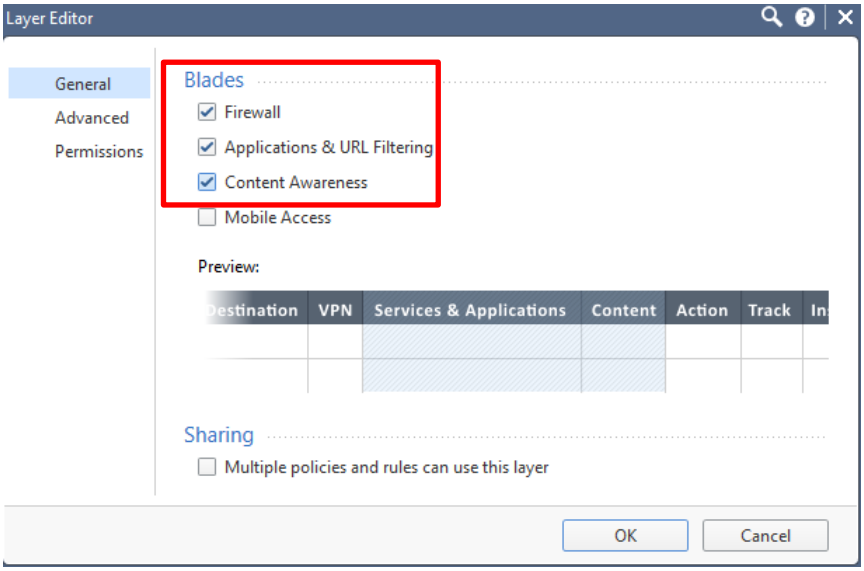


點選「New」建立新的 Policy Package：



Policy 名稱為「SimplePolicy」、只勾選「Access Control」並勾選啟用「Firewall」、「Applications & URL Filtering」以及「Content Awareness」：

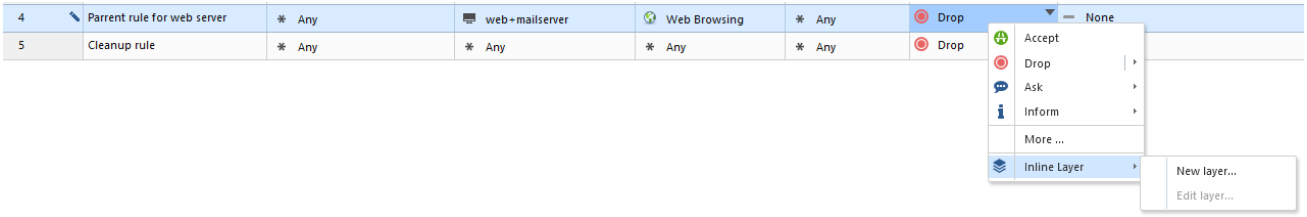




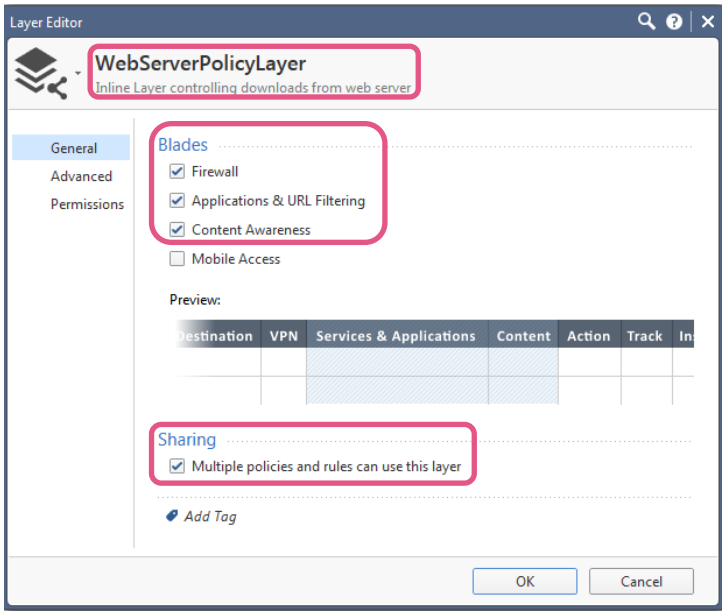
接下來依照 Lab-1 一開始的附圖新增規則。

建立 Rule 4 的 Inline Layer 規則

先建立 Inline Layer 會套用到的父規則;在第 4 條規則設定完「Name」、「Source」、「Destination」以及「Services & Applications」欄位之後，在「Action」欄位點選「Inline Layer」>「New layer…」

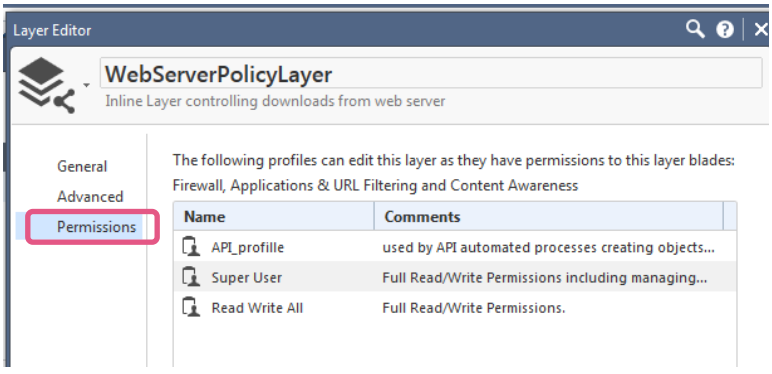


將 Inline Layer 命名為「WebServerPolicyLayer」以及啟用「Firewall」、「Applications & URL Filtering」和「Content Awareness」並勾選「multiple policies can use this layer」，勾選該選項之後在其它 Policy Package 就可以重覆使用該 Inline Layer。



在 Permissions 的欄位可以設定 Inline Layer 的讀取權限：

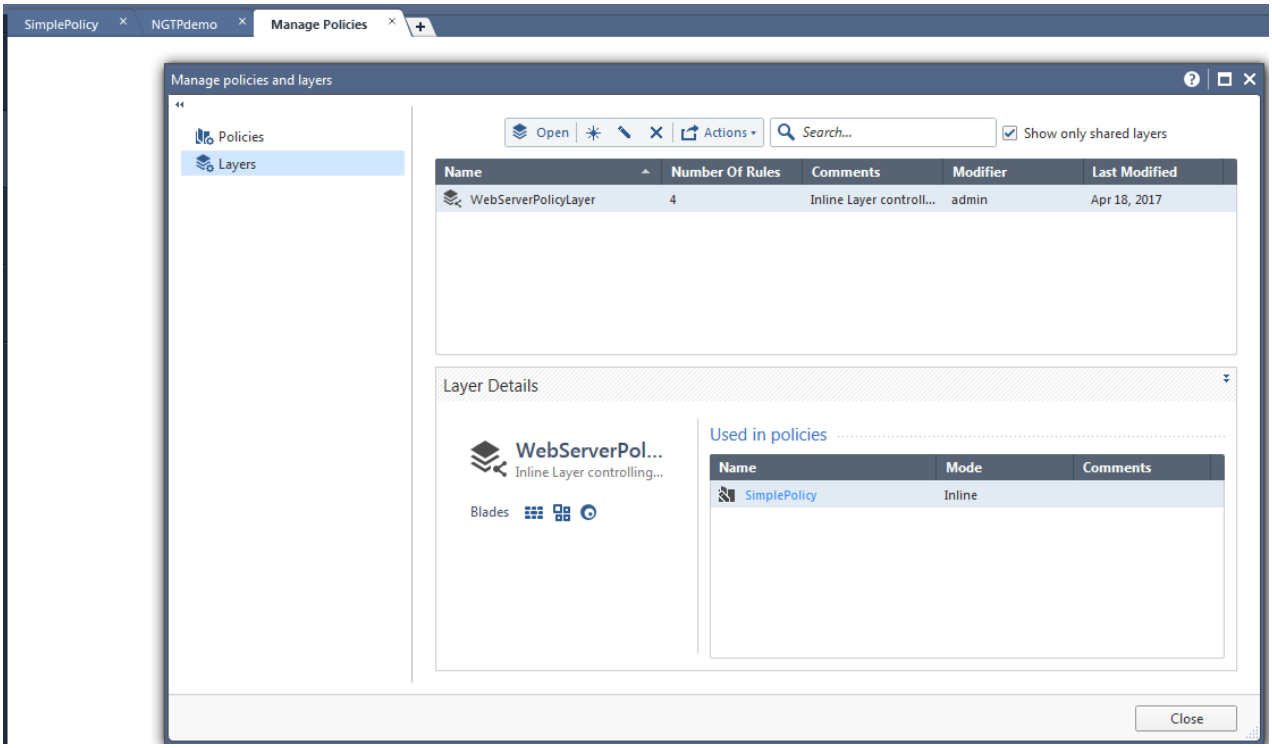
Option Lab：嘗試建立一個新的 User Profile 以及 User 帳號，設定只能編輯該 Inline Layer 而不能更改整個 Policy Layer，並使用該 User 登入看看畫面有什麼不一樣：



完成後的 Inline Layer Policies 如下圖：

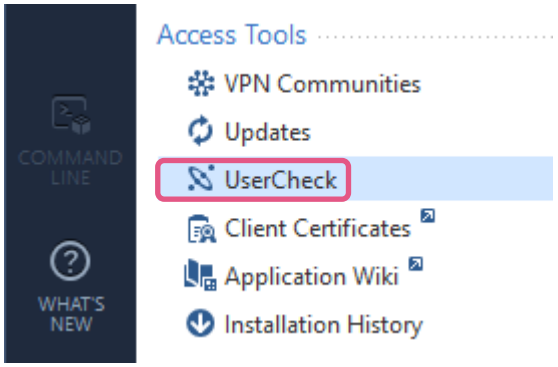
4	Parrent rule for web server	Any	web+mailserver	Web Browsing	Any	WebServerPolicyLaye	N/A
4.1	Creadit Card Numbers	Any	web+mailserver	Any	Download Traffic PCI - Credit Card Numbers	Drop Blocked Messa...	Detailed Log Accounting
4.2	Documents	Any	web+mailserver	Any	Download Traffic Document File	Accept	Detailed Log Accounting
4.3	Spreadsheets	Any	web+mailserver	Any	Download Traffic Spreadsheet or CSV File	Accept	Detailed Log Accounting
4.4	Cleanup rule	Any	Any	Any	Any	Accept	Log

完成之後可以在 Manage Policies 頁面看到剛剛新增的 Inline Layer Policies：

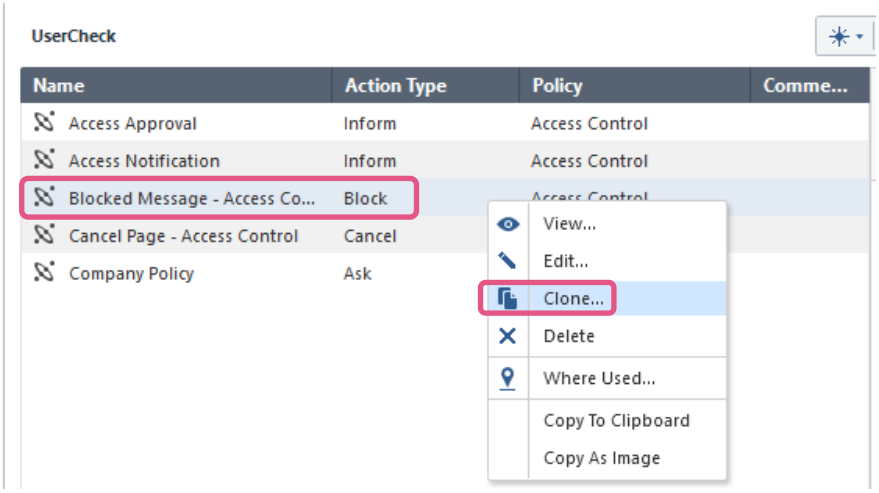


建立 Content Awareness 的阻檔頁面

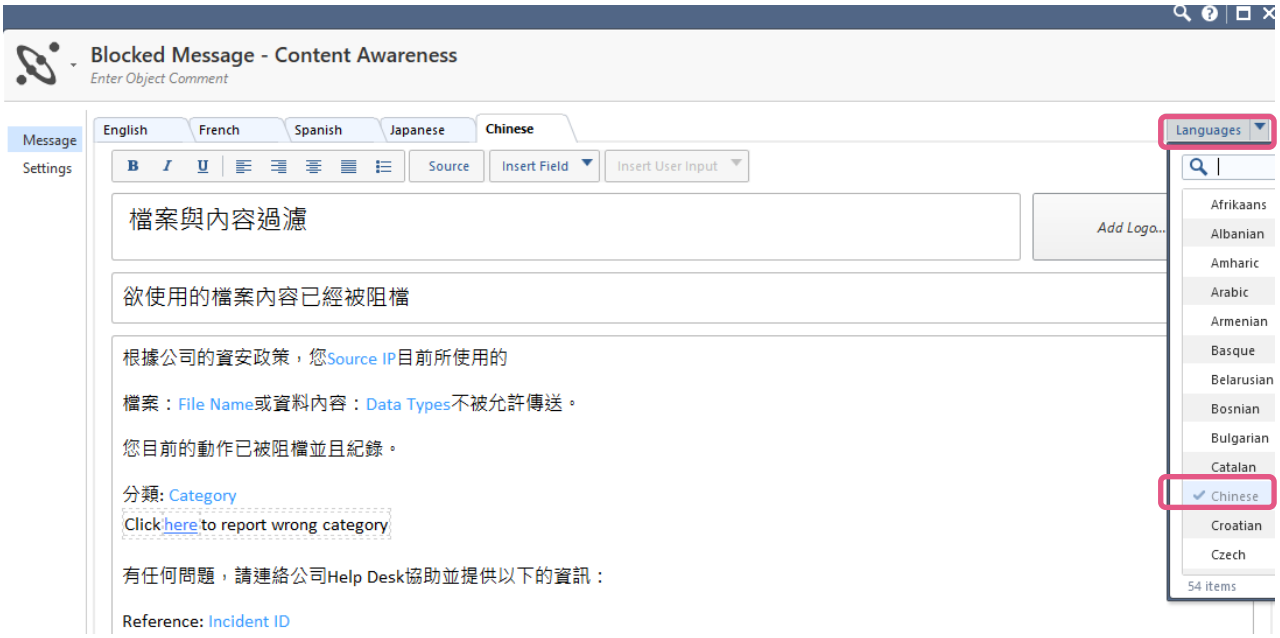
在 Security Policies 頁籤左下角 Access Tools 點選「UserCheck」：



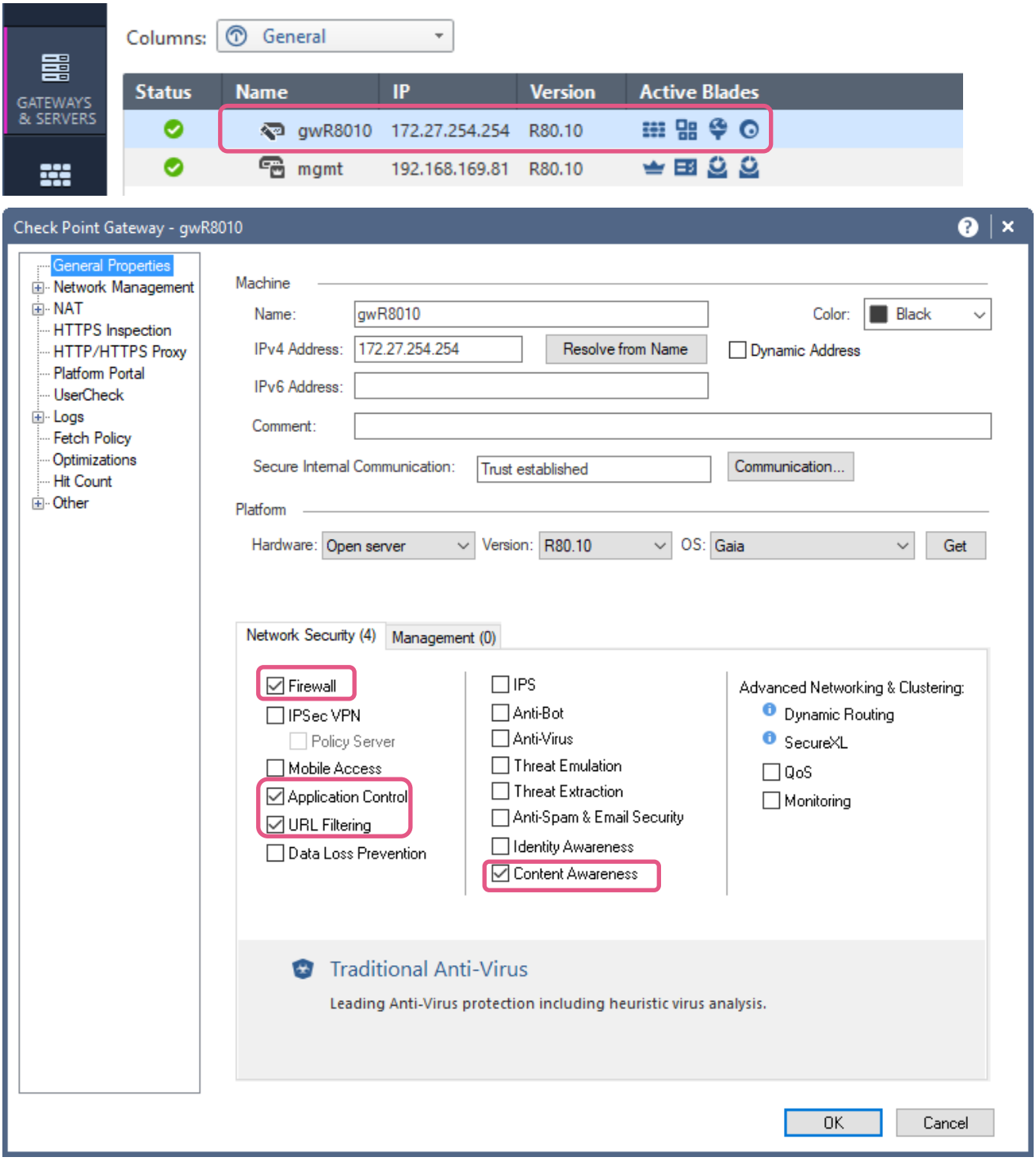
點選「Blocked Message」選項然後按右鍵選擇「Clone…」：



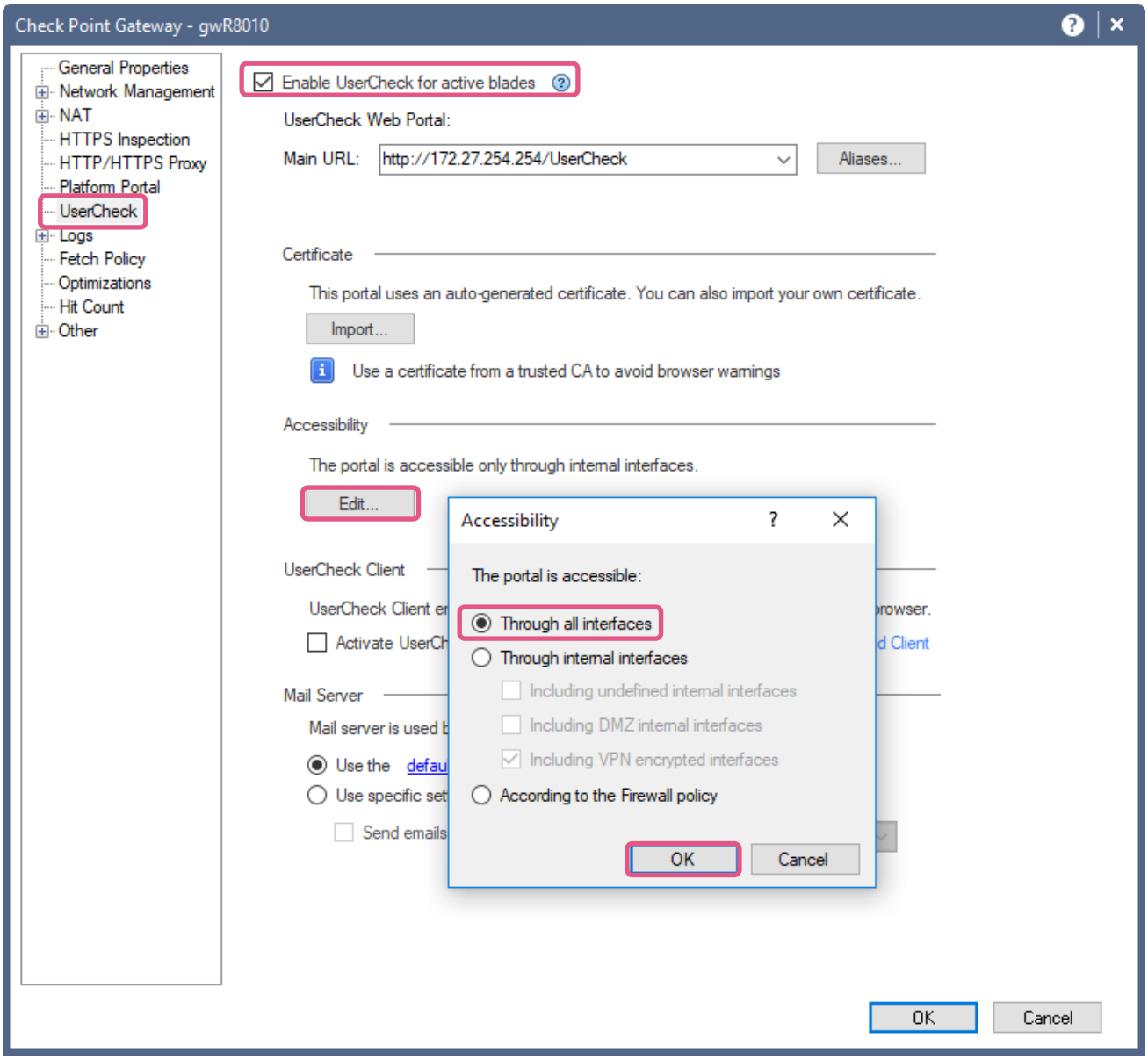
點選右上角的「Language」選項新增中文頁面，然後自訂阻檔頁面的訊息：



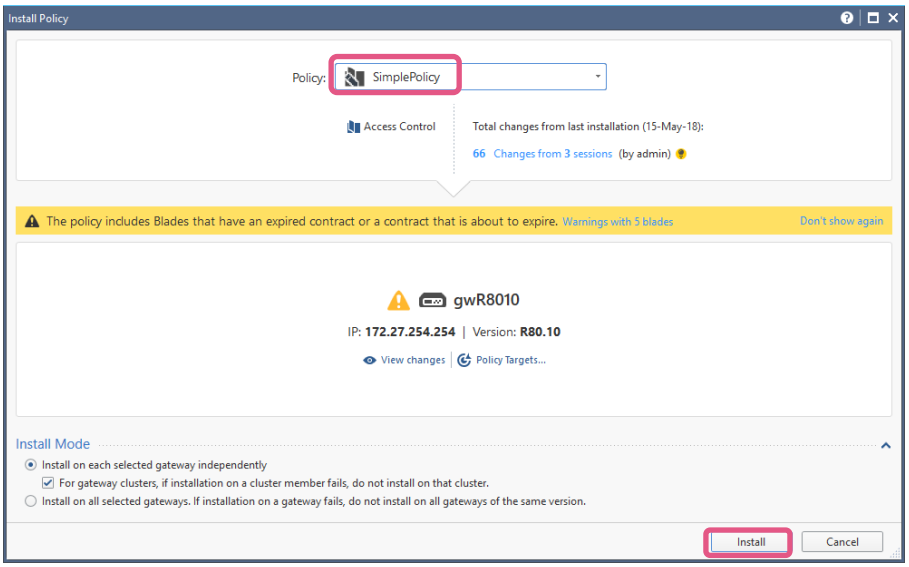
Policy 設定完成之後記得回到 Gateway & Server 頁籤，點擊 Gateway 物件之後啟用「Content Awareness」功能：



再切換至 UserCheck 頁籤，確認勾選「Enable UserCheck for active blades」，再點選 Accessibility 的「Edit…」選項，設定選項為「Through all interfaces」：

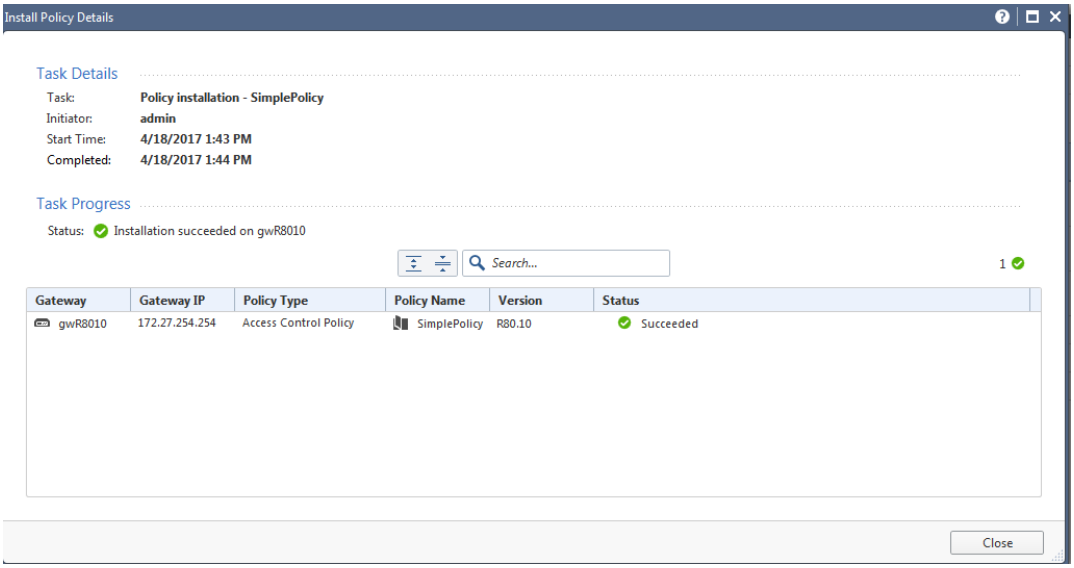


設定完成之後，點選「Publish」並「Install Policy」：



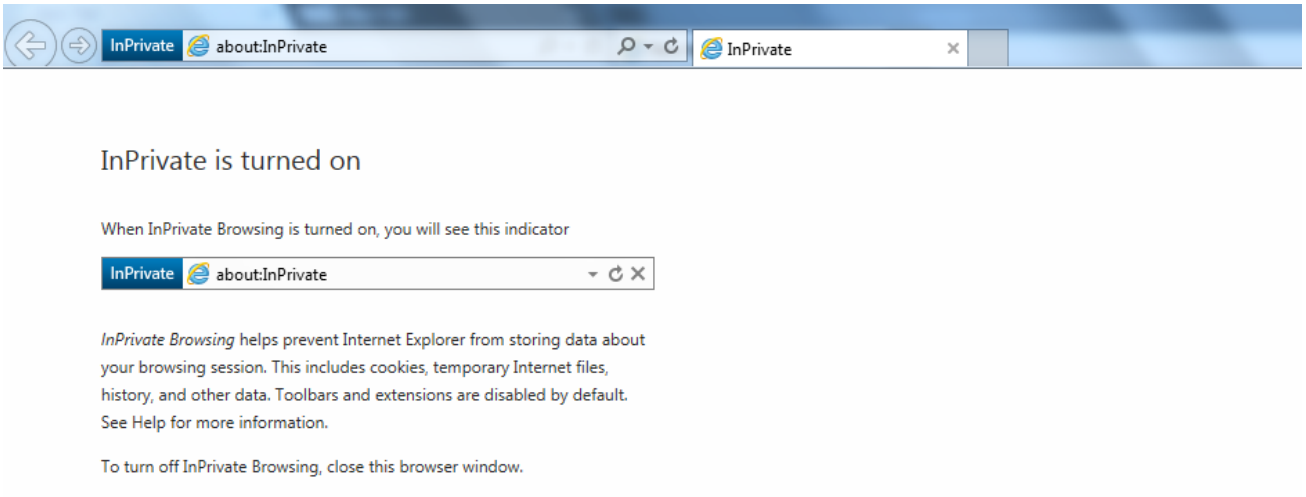
如果欲派送的 Policy 與之前派送給 Gateway 的是不同的 Policy Package，會出現如下提示訊息，點選「Install」繼續派送：

等待 Policy 成功完成派送之後，即可繼續進行 Lab 測試：

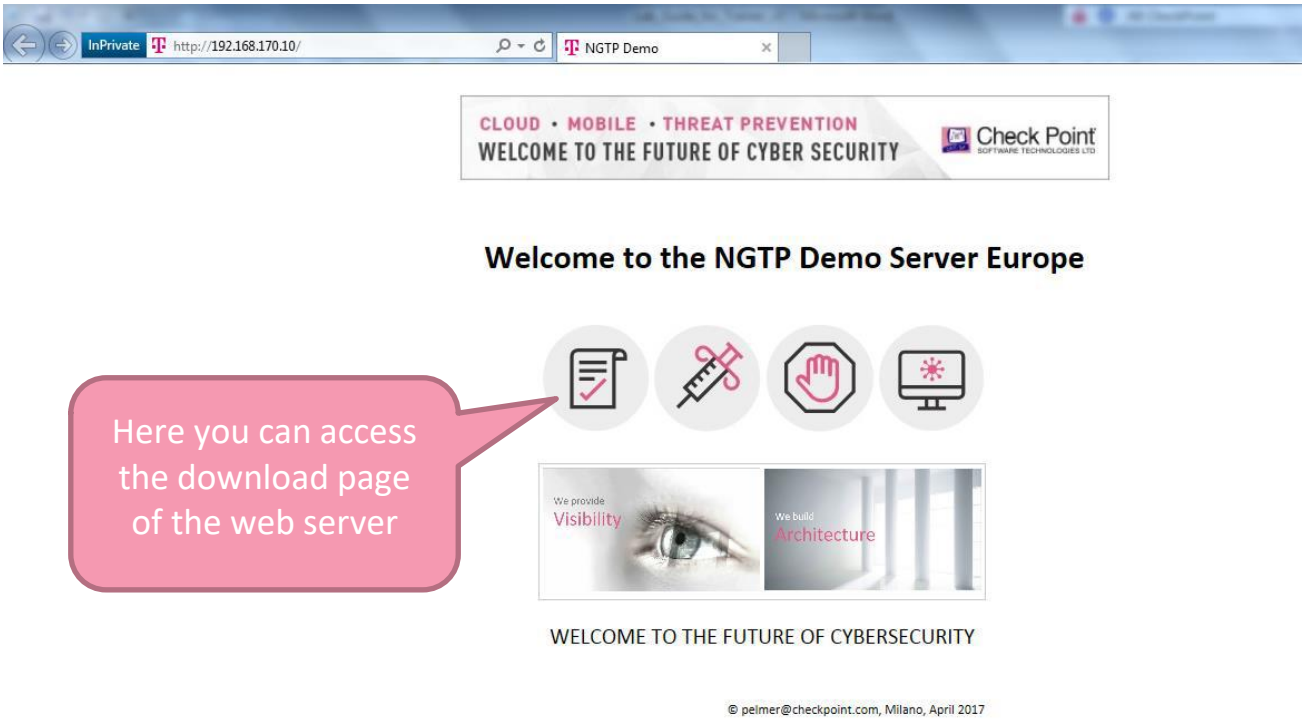


使用瀏覽器的 private mode 開啟 Web Server 網頁進行測試

為了避免因為瀏覽器 cache 的問題影響 Lab 進行，建議使用瀏覽器的 private mode 連線到 Web Server。以下是使用 IE 的範例 (Google Chrome 請使用 Ctrl + Shift + N 開啟)

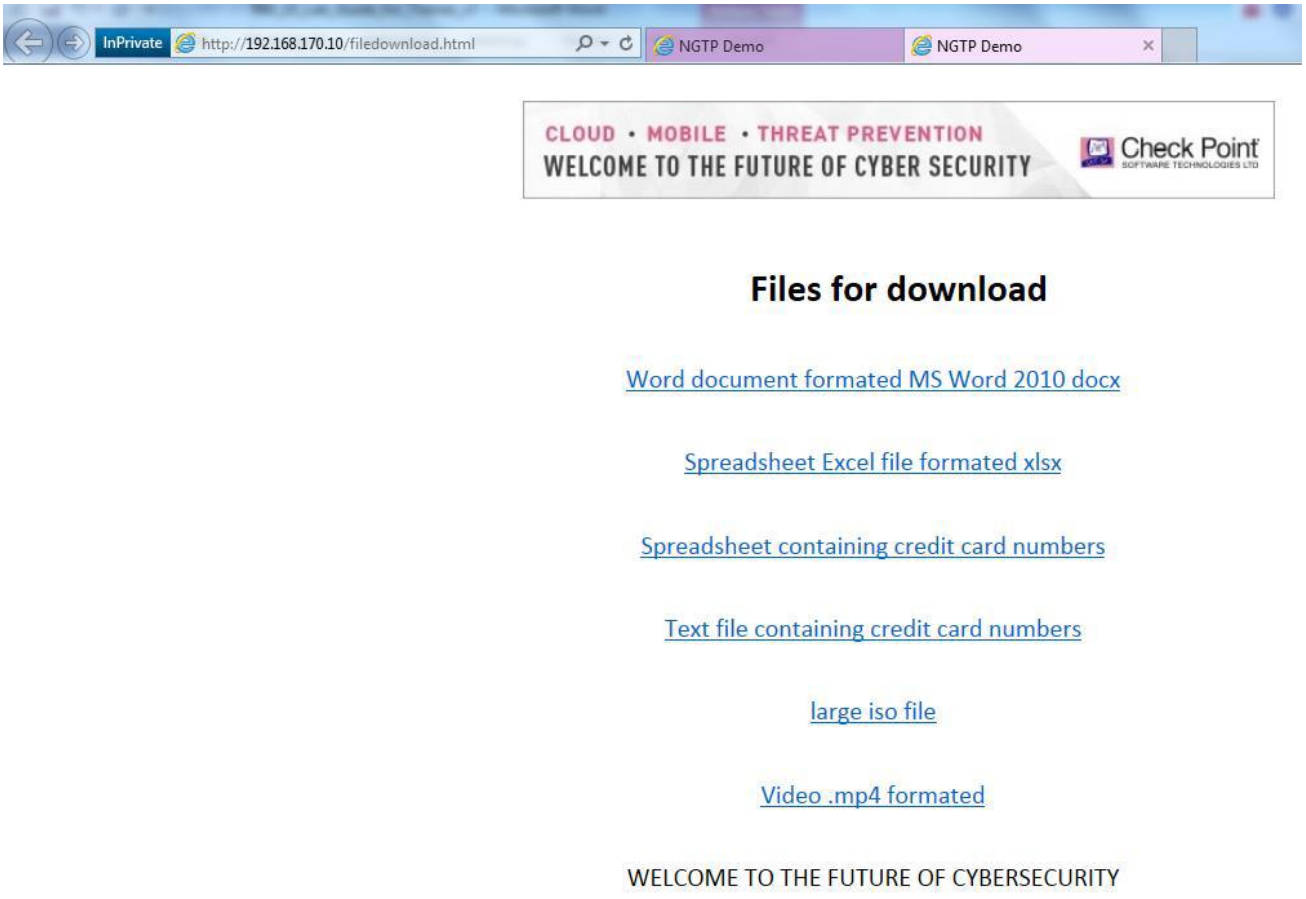


連線到 Web Server 進行測試

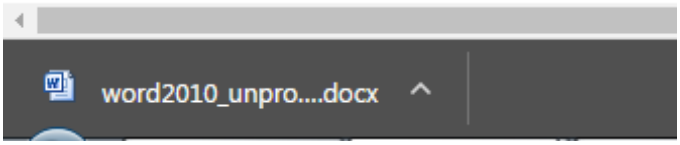


嘗試從 Web Server 下載 Word、Excel、TXT 等各個檔案並產生相關的 Log

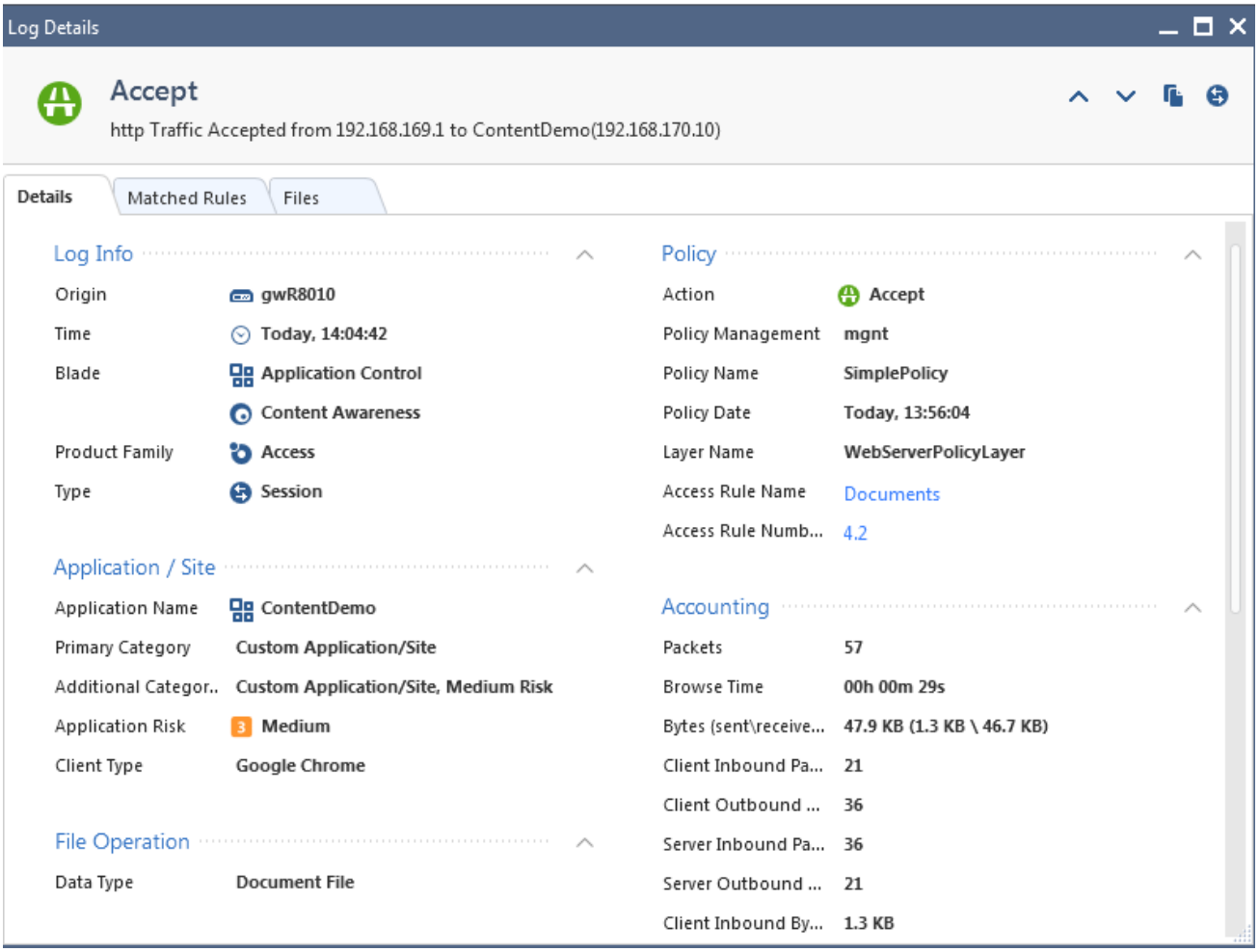
P.S : Spreadsheet containing credit card numbers 檔案異常，請測試其它檔案。



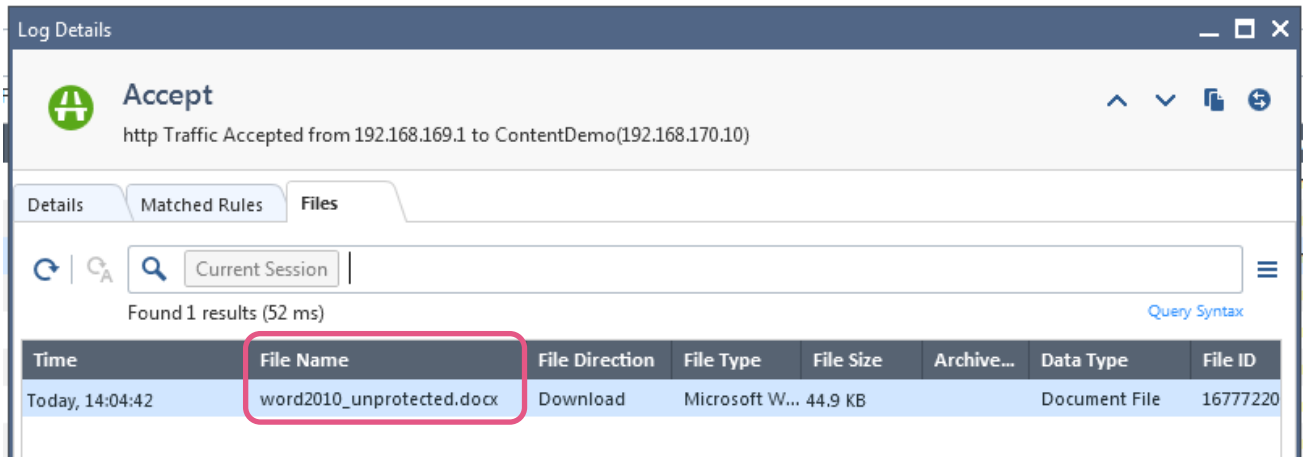
根據 Policy，Word 文件可以被正常的下載：



切換至 Log 頁面檢視該筆下載的 Log：



注意到檔案名稱會顯示在 Log Details 的「Files」頁籤中：

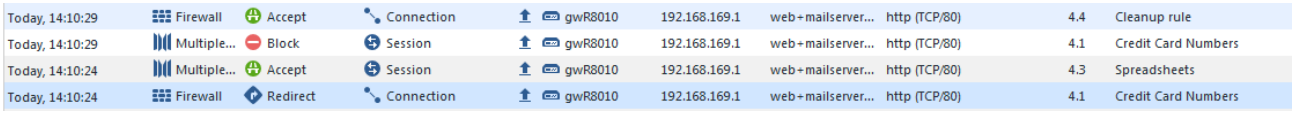


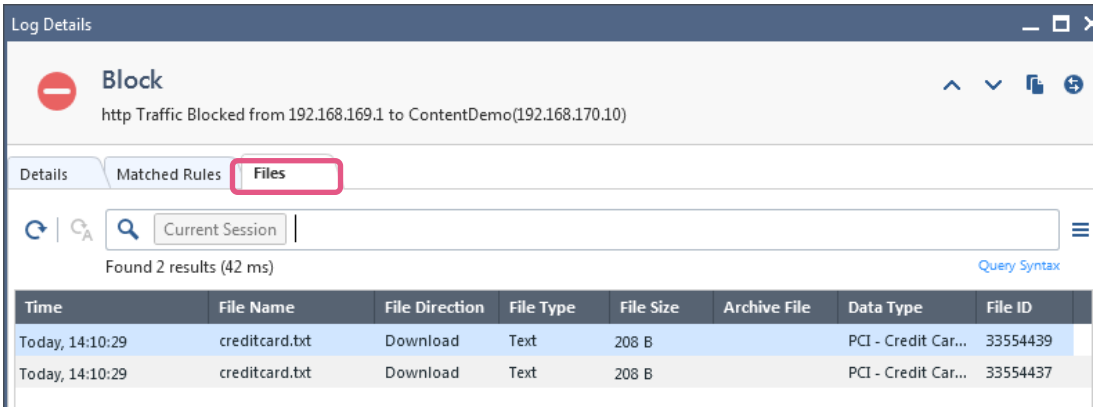
下載包含信用卡資料的 Text 檔測試

當企圖下載包含信用卡資料的 Text 檔案時，你會看到剛剛我們自訂以下的阻檔訊息：

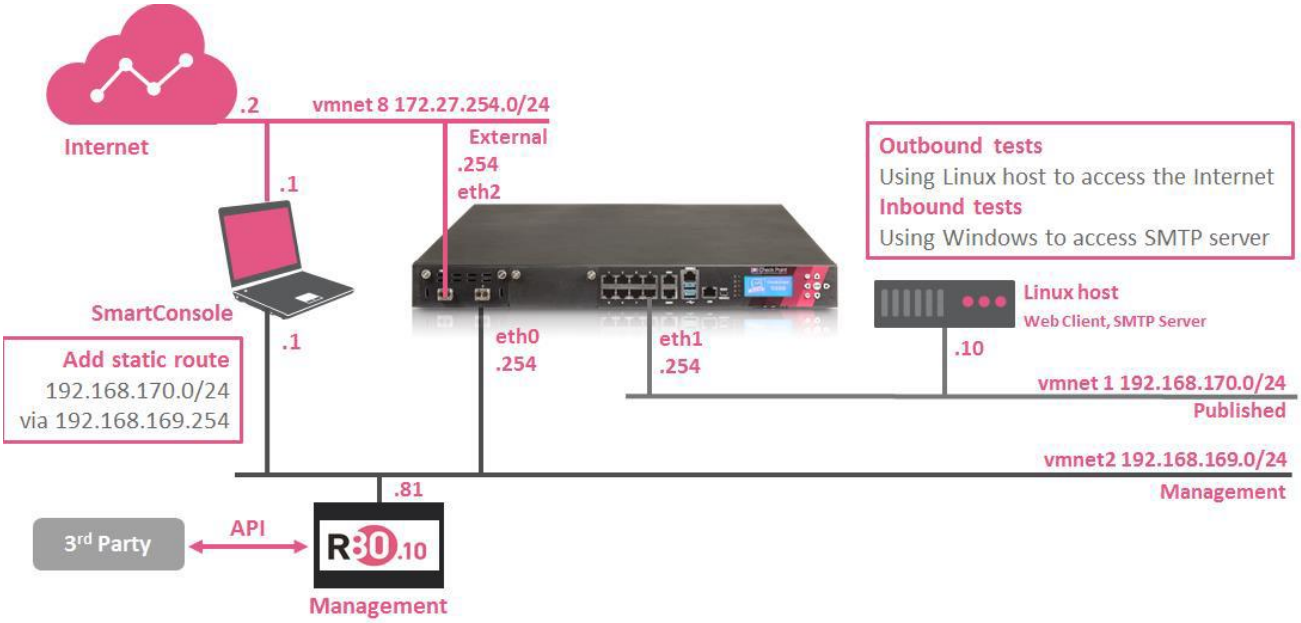
你的阻檔訊息跟上述圖片顯示的相同或是類似嗎?

產生相關的 Log 檔案



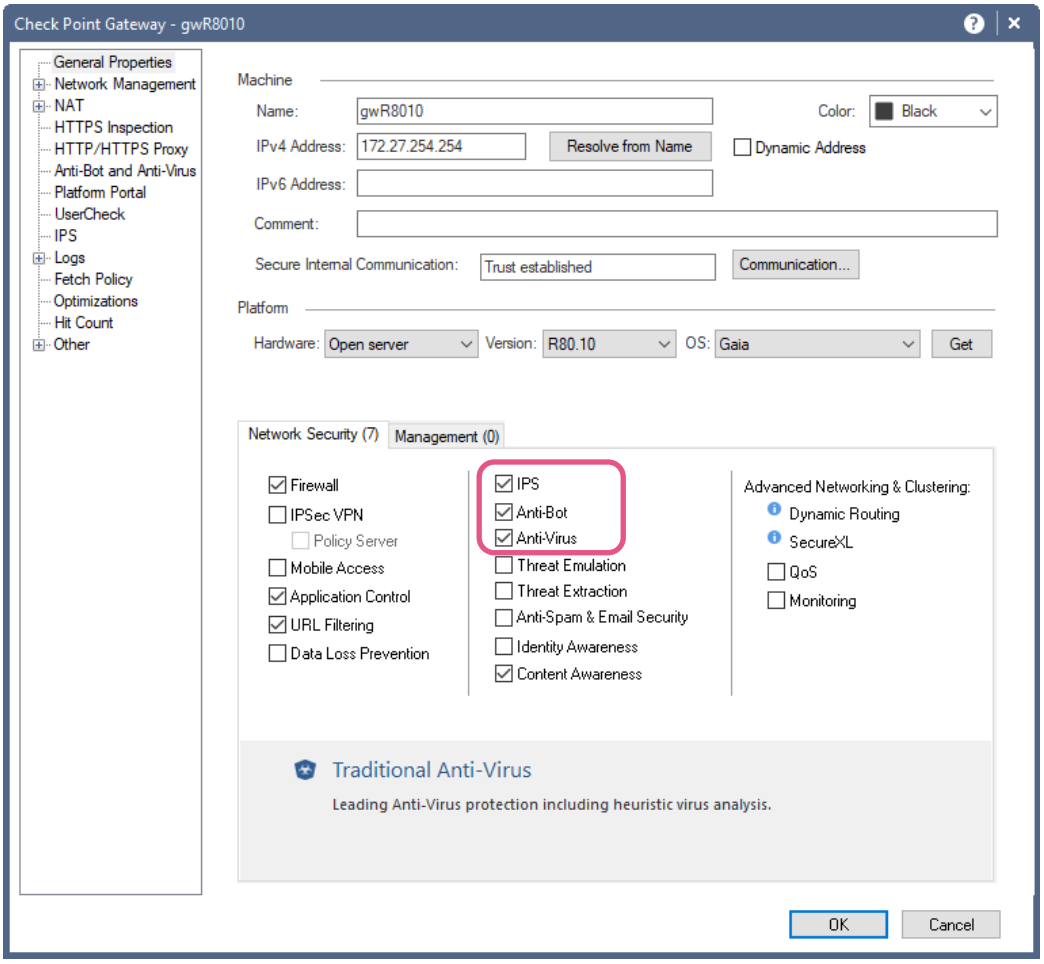


Lab 3: Threat Prevention

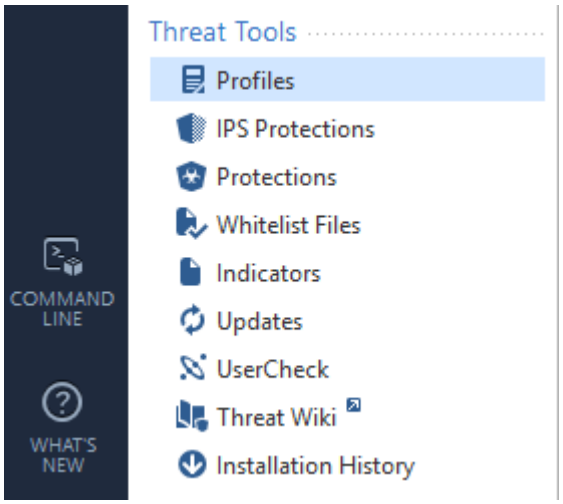


設定 Gateway 啟用 Threat Prevention 功能

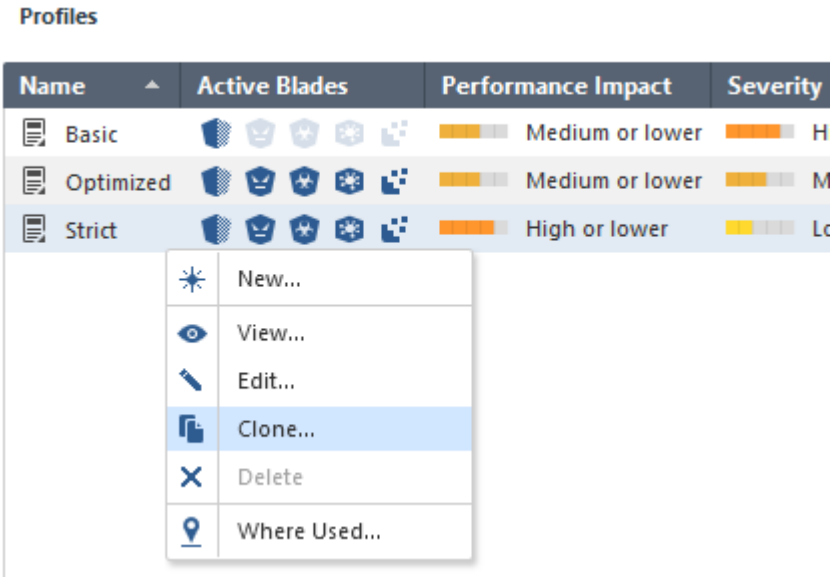
至 Gateways & Servers 頁籤，點選 Gateway 勾選 IPS、Anti-Bot 以及 Anti-Virus 功能：



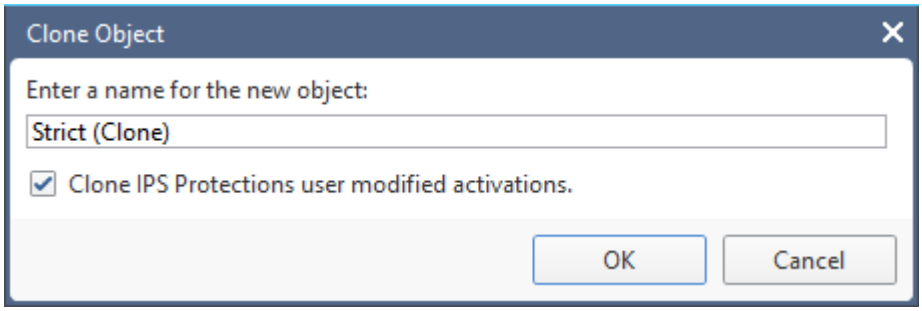
點選 Threat Prevention >> Policy，然後在左下角的 Threat Tools 點選「Profile」：



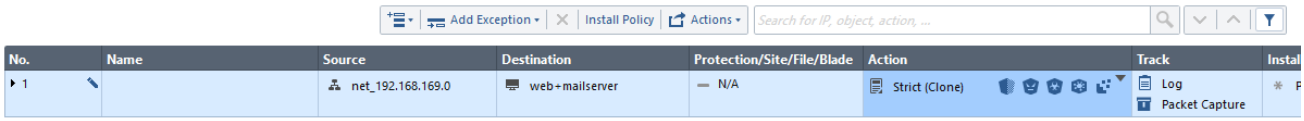
接下來在右邊的 Profile 中點選「Strick」然後按右鍵「Clone」：



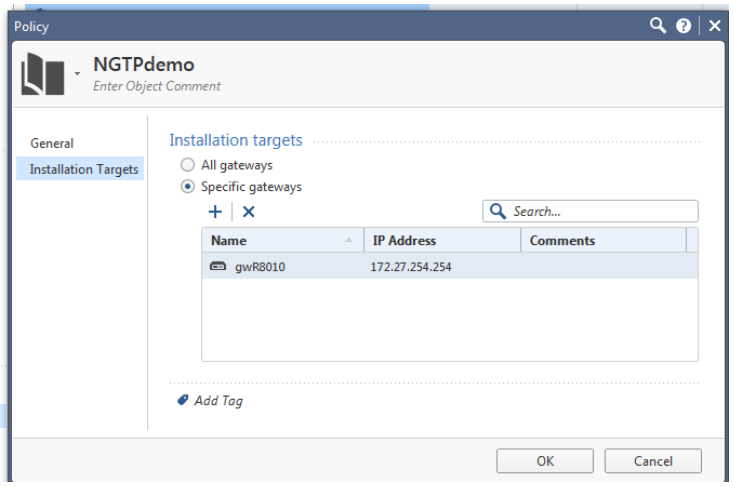
按 OK 進行複製：

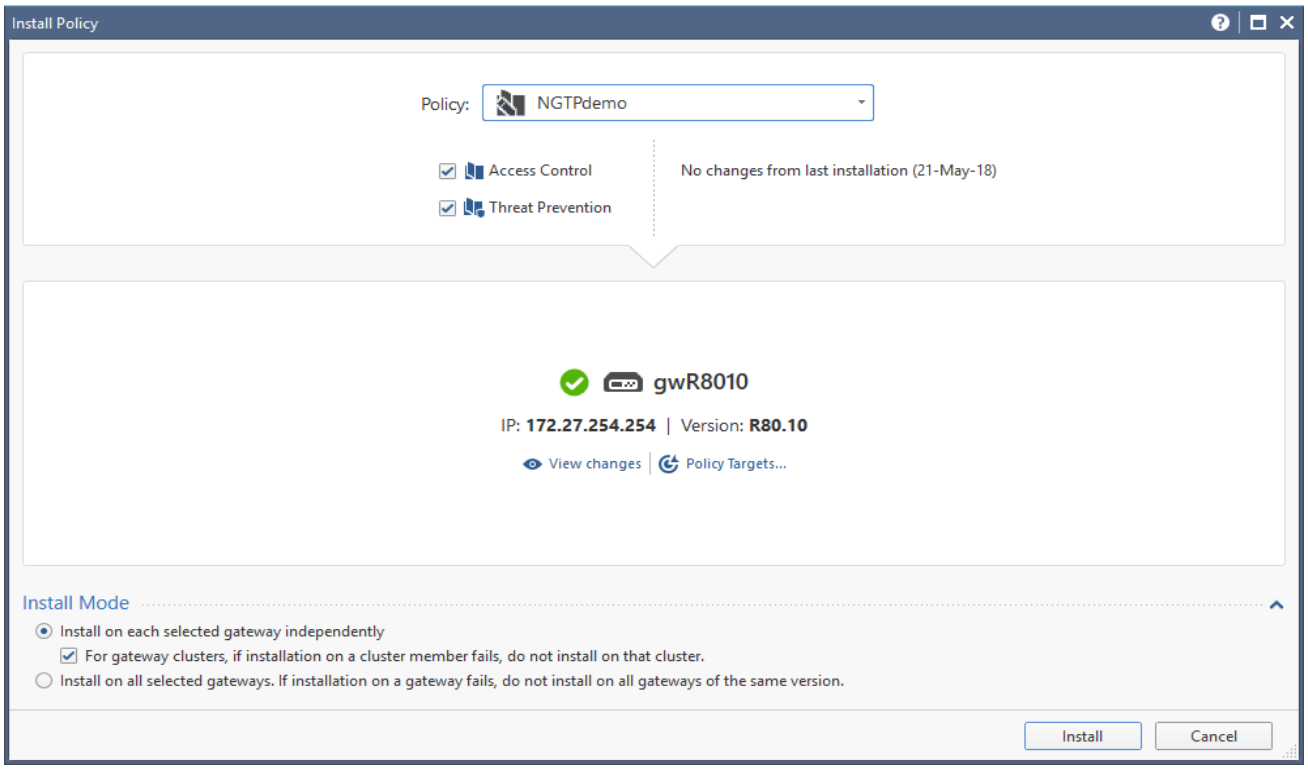


設定 Threat Prevention Policy 如下圖：



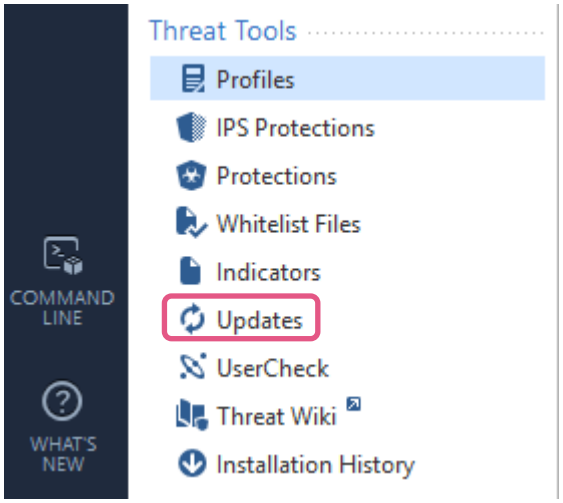
設定完成後，進行 Publish 以及 Install Policy，確定派送 NGTPdemo Policy Package 至正確的 Gateway 上



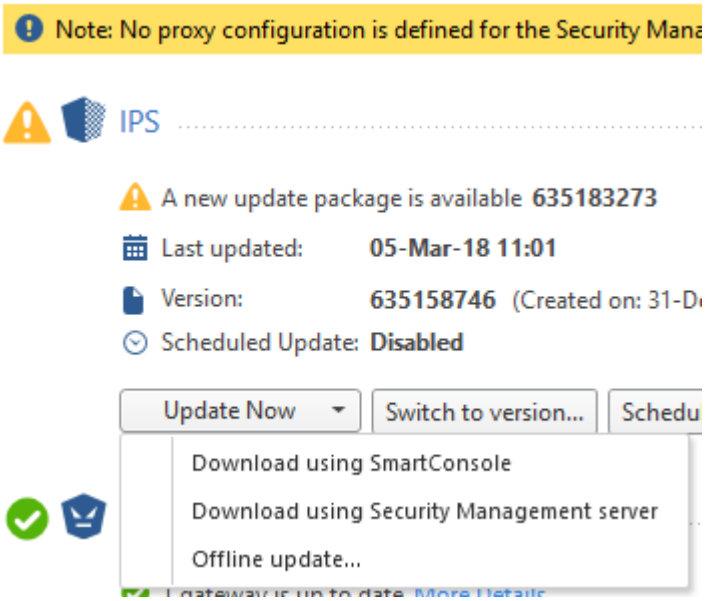


初次更新 Threat Prevention

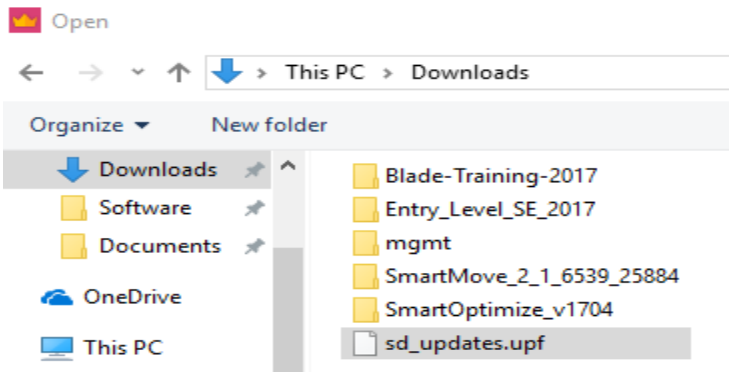
在左下角 Threat Tools 中點擊 Updates：



Anti-Bot 與 Anti-Virus 會自動進行更新，IPS 的部份請點選「Update Now」旁邊的下拉式箭頭，然後選擇「Offline update…」：

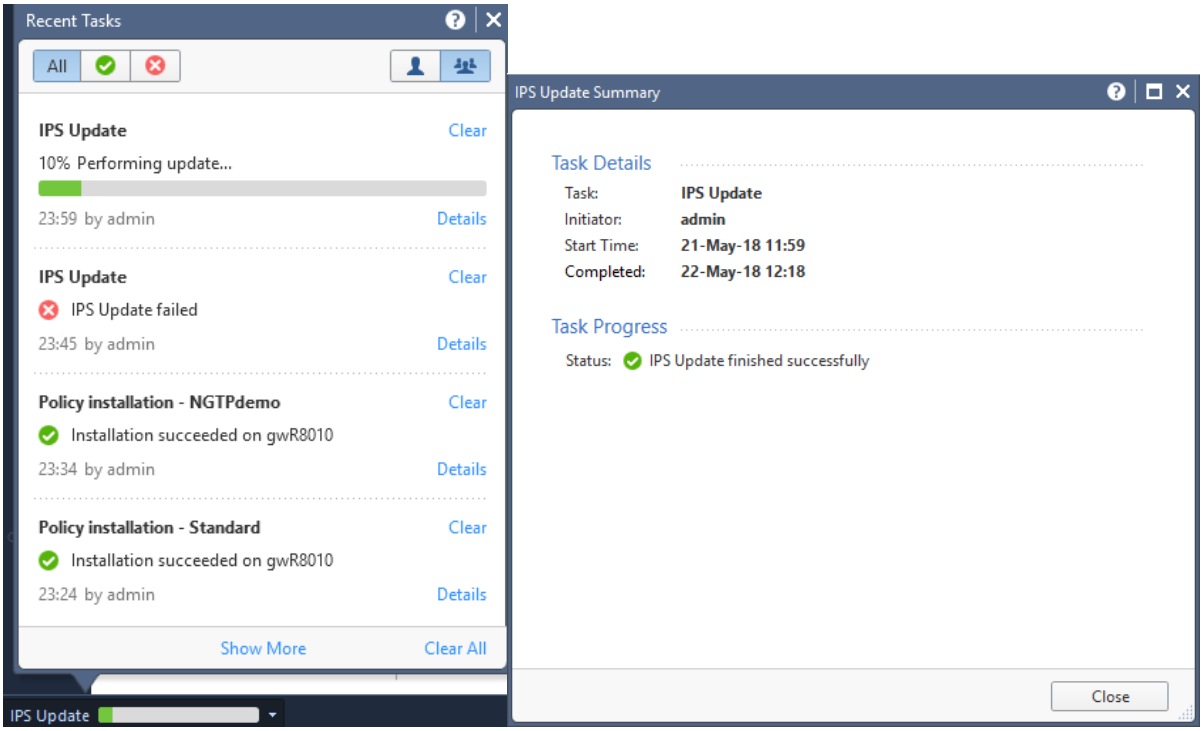


選擇 IPS offline update file「sd_updates.upf」：

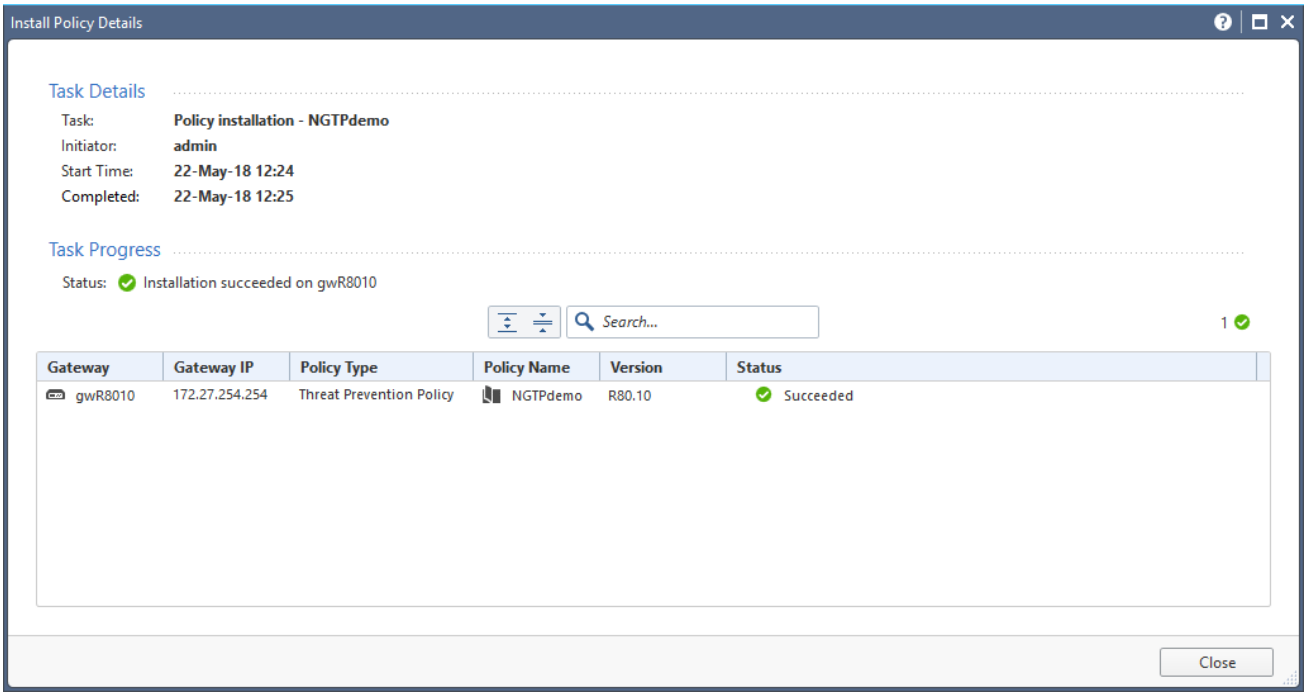


畫面左下角的 Recent Tasks 會顯示 IPS 更新的進度條，等待 IPS 更新完成：

P.S 初次更新 IPS 整個過程約需要 **20 分鐘**!! Take a Coffee time~



更新完成之後，請再一次的 Install Policy：

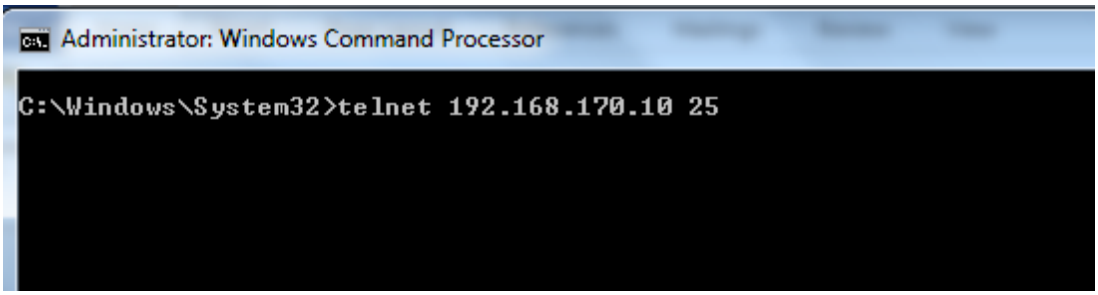


測試 IPS 的防釣魚郵件防禦功能

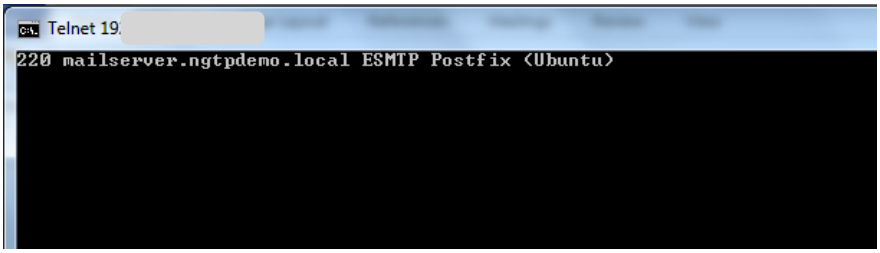
接下來我們會嘗試發送一封釣魚郵件至 Linux Mail 主機上.

從 Windows 系統上開啟 CLI 介面

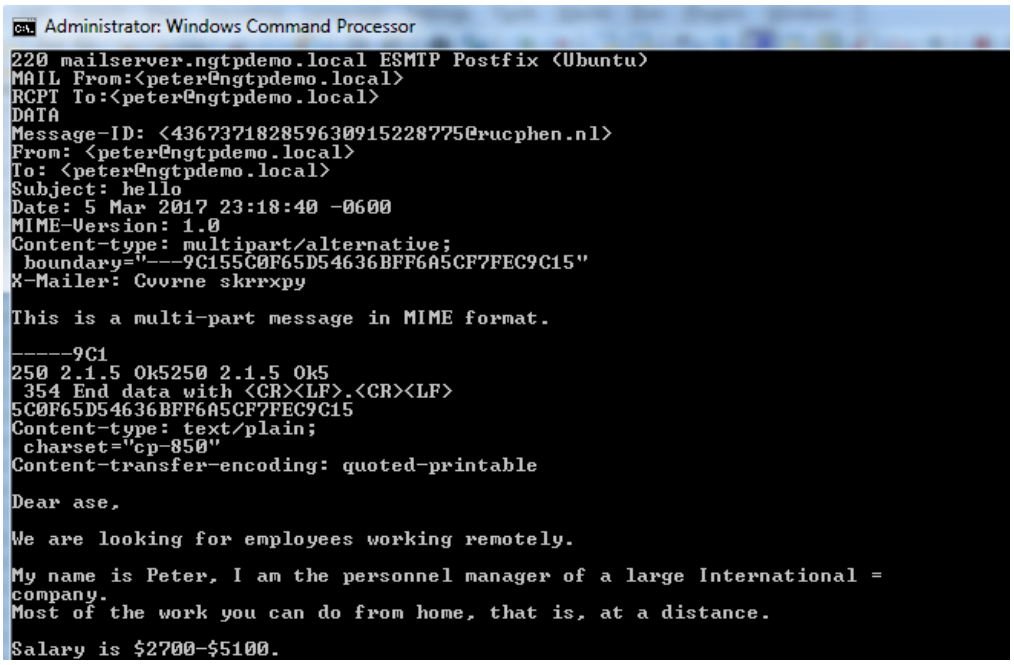
開啟 CMD 介面並嘗試使用 Telnet 到 192.168.170.10 的 Linux Mail Server 上的 Port 25。



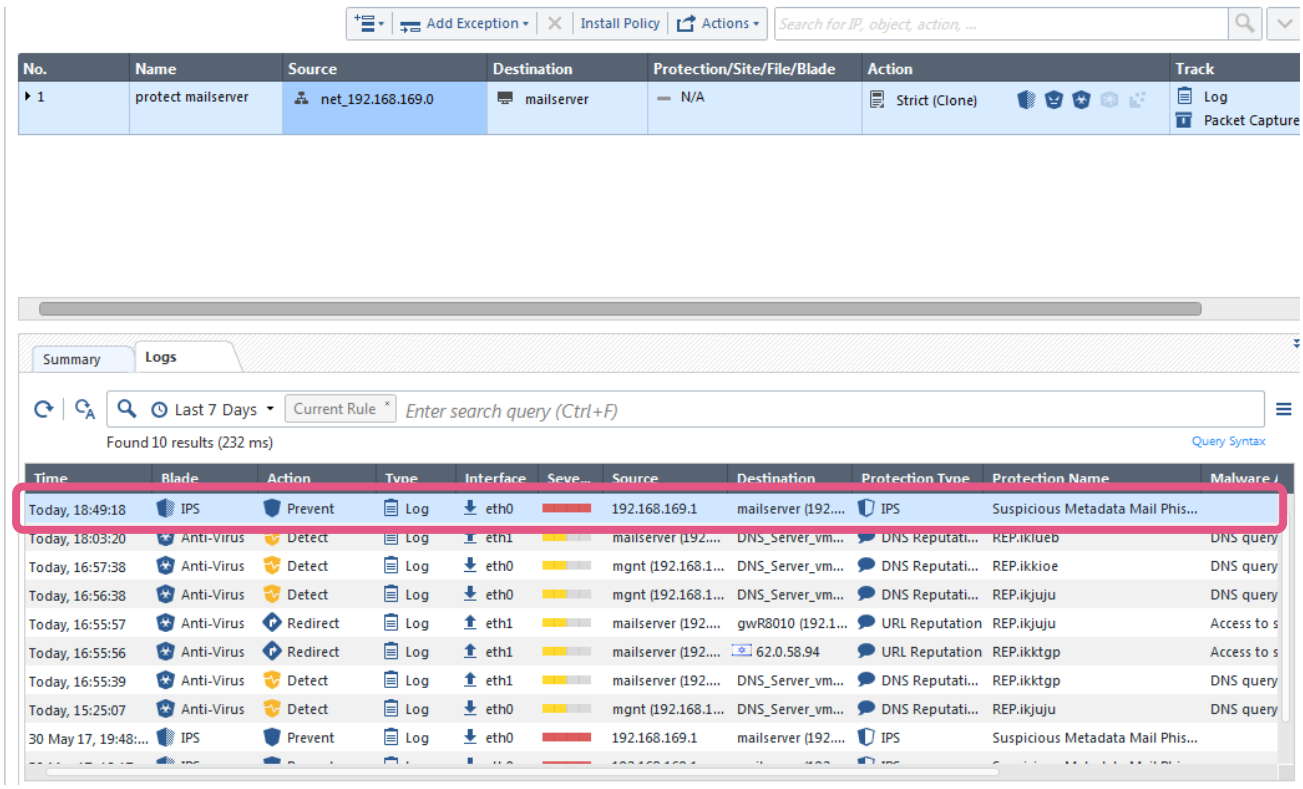
可以看到 Connection 成功的建立了



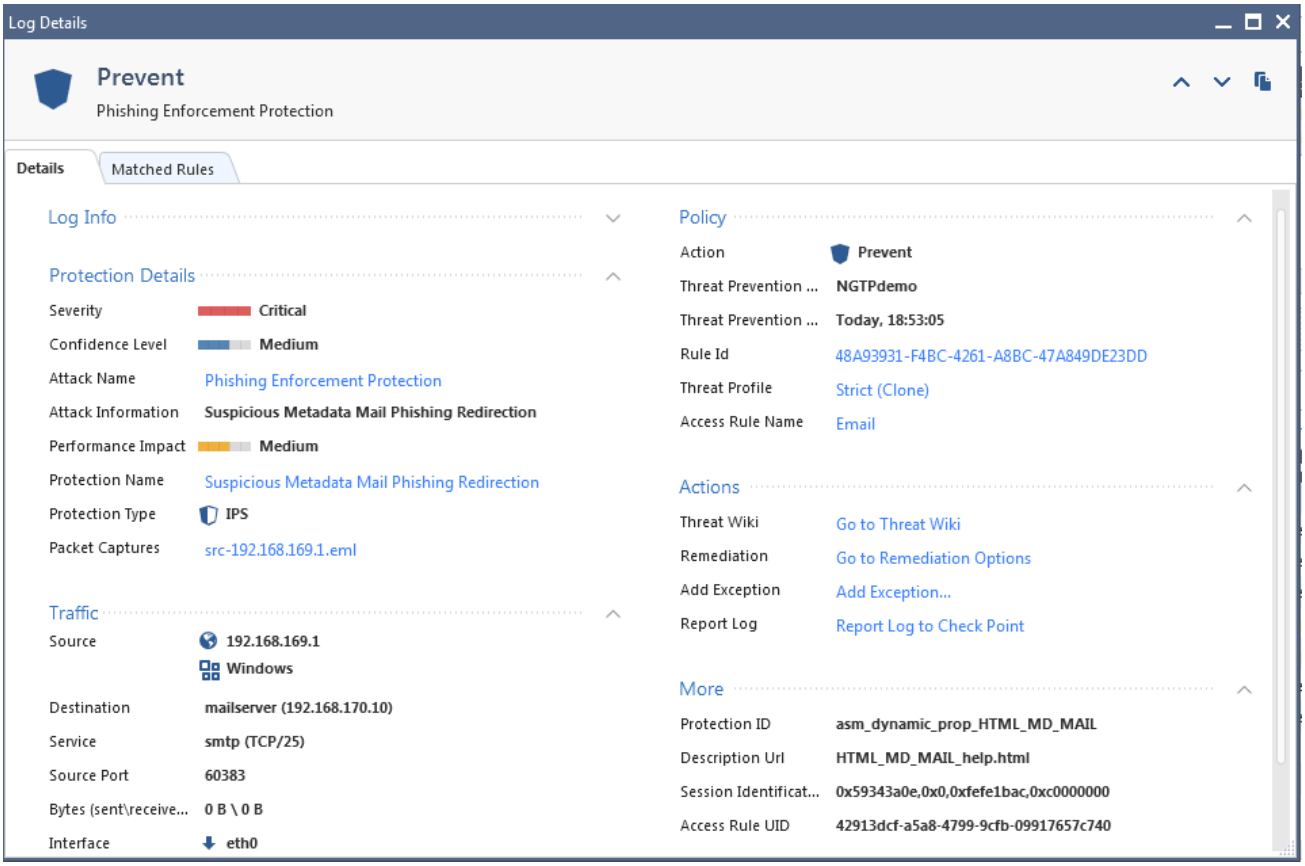
開啟 PhishingSample text 範例郵件，並將所有的內容複製起來貼到 CMD 視窗中。



顯示 Log 訊息，可以發現一筆阻檔的紀錄：

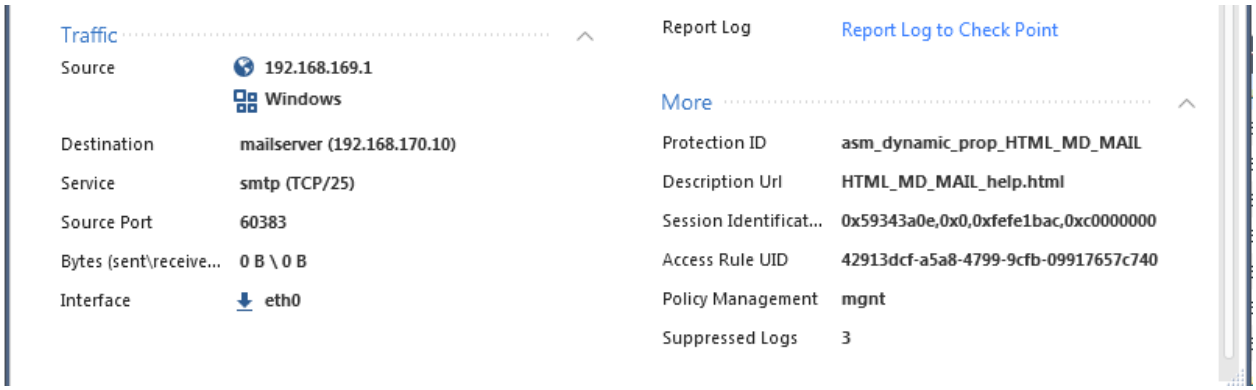


檢視 IPS 的 Log Details



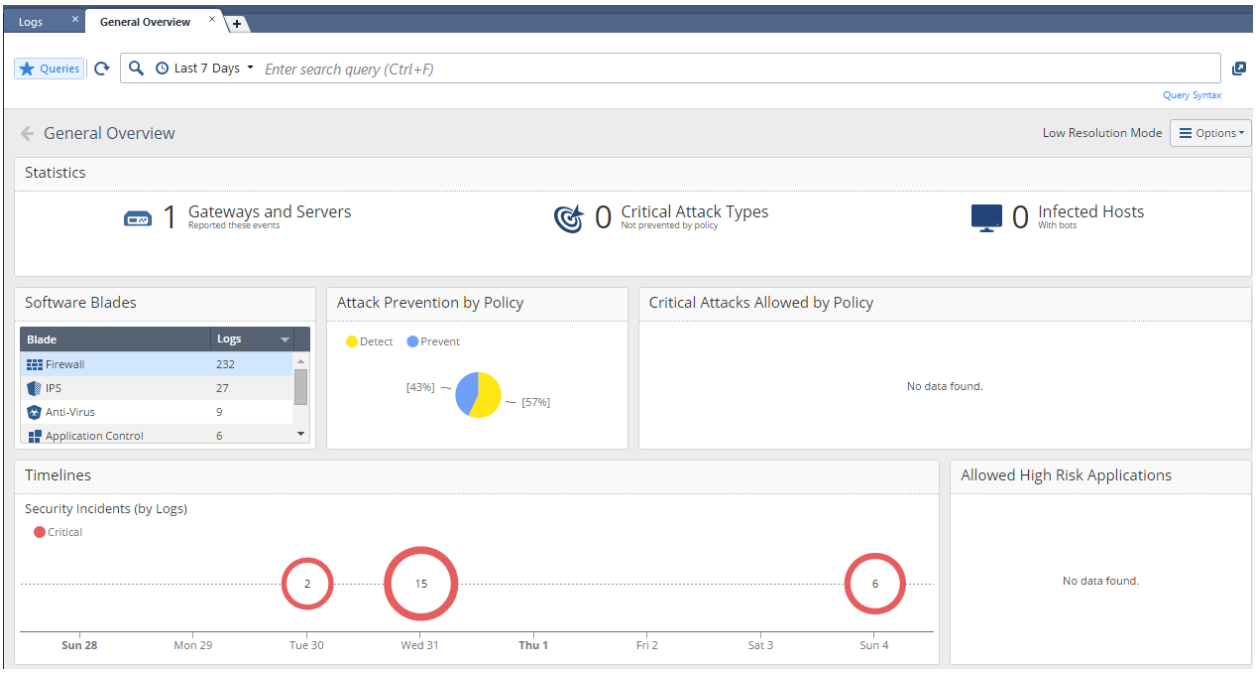
嘗試發送多筆的 Phishing Mail 之後再檢視 Log.

Scroll down verifying if there are suppressed log messages.

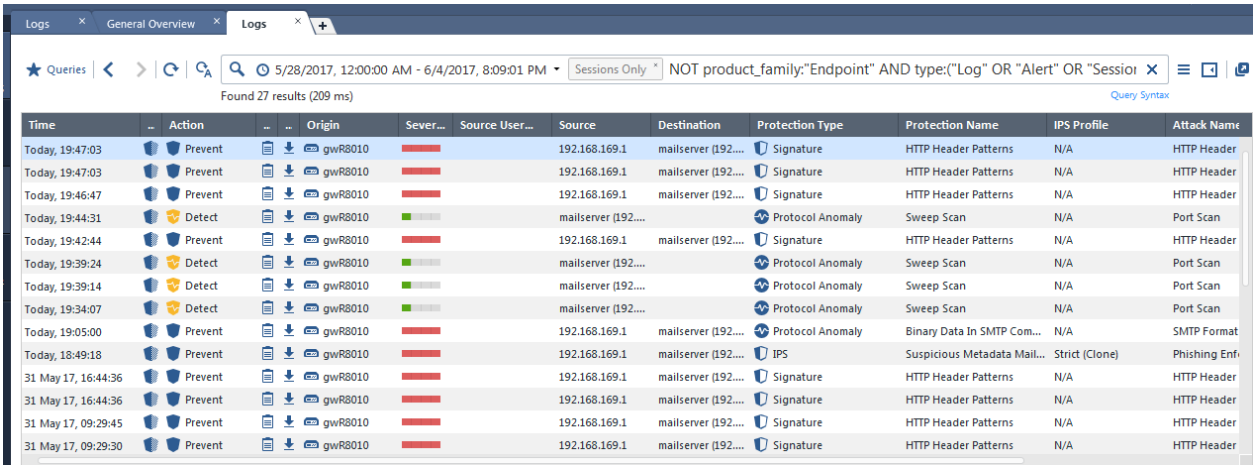


Lab 4: 使用 SmartEvent 報表功能

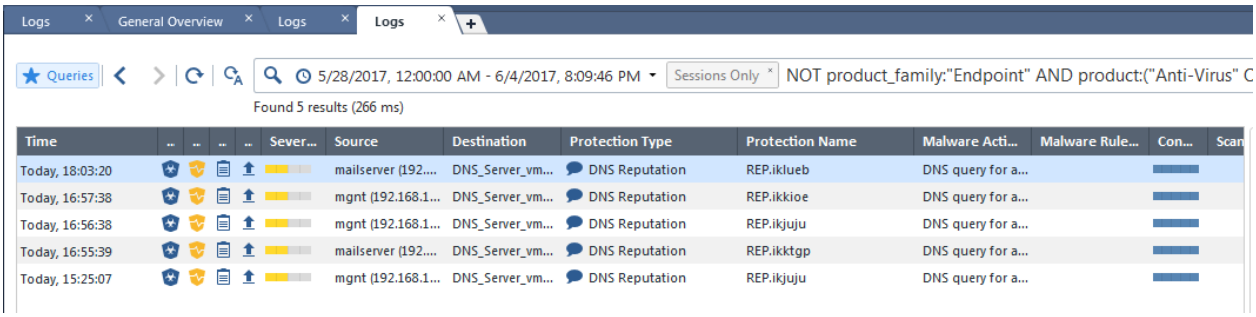
開啟 Logs & Monitor > General 頁籤



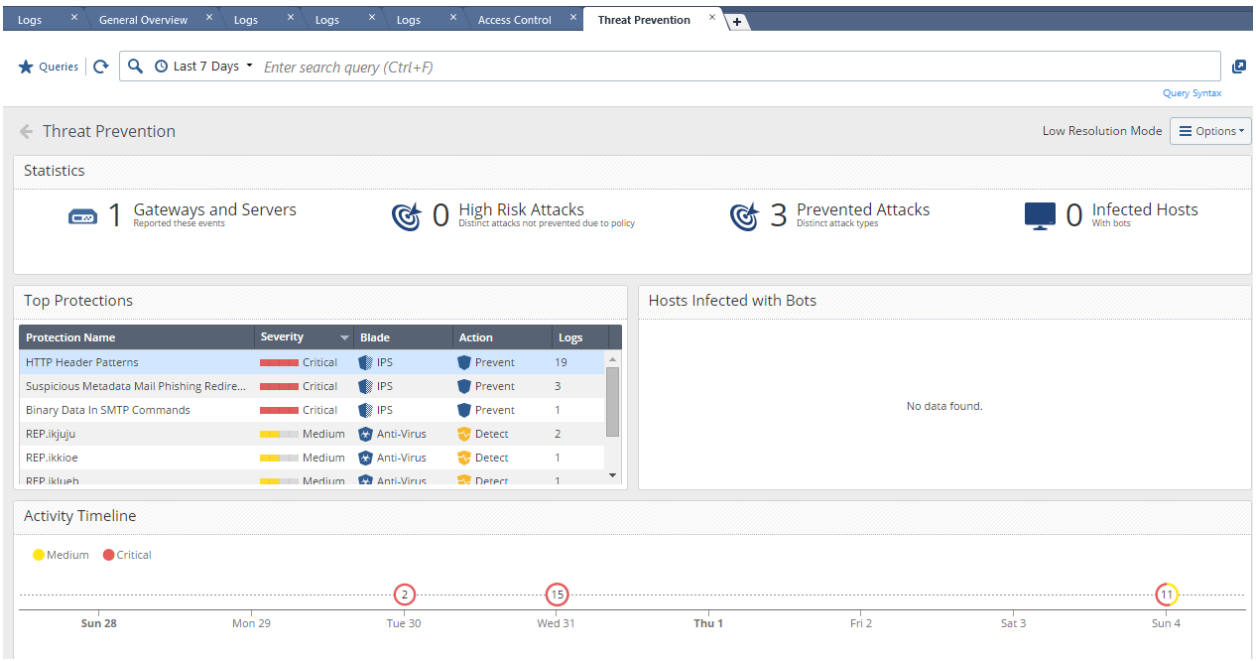
點擊 IPS 事件



檢視 IPS 事件中被 Detect 的事件



開啟 Threat Prevention view



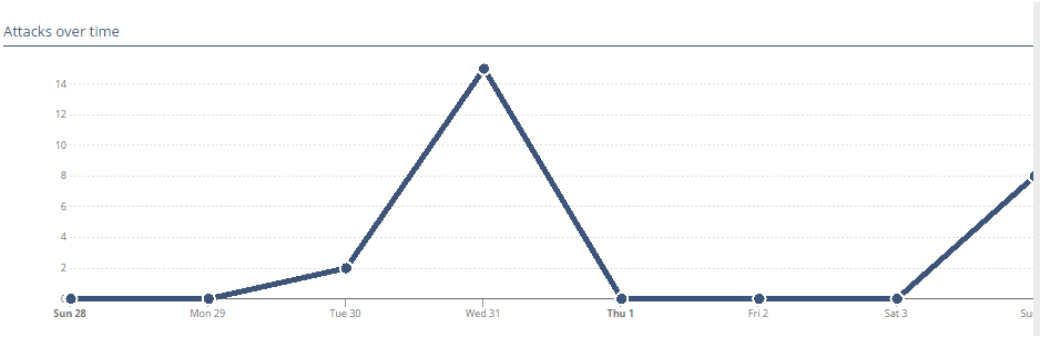
產生一份關於 Threat Prevention 的攻擊報表

報表應該會包含以下的內容

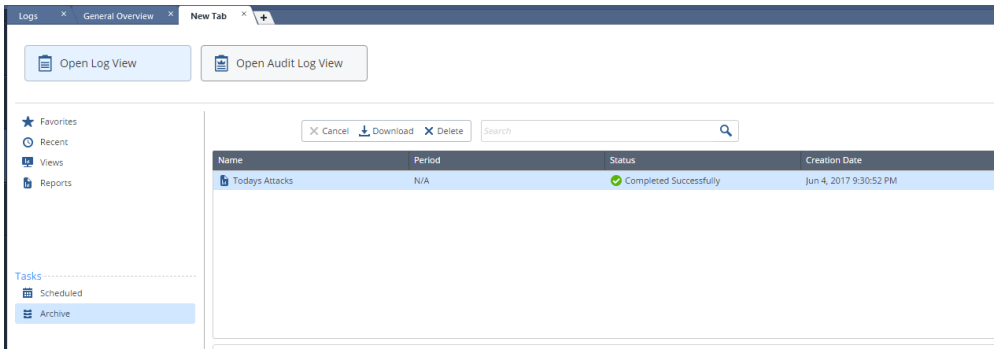
- 攻擊來源、目的以及對應到的攻擊特徵
- 攻擊 Mail Server 的 Timeline

Attacks by destination

Destination	Blade	Protection Name
mailserver (192.168.170.10)	Anti-Virus IPS	Binary Data In SMTP Commands HTTP Header Patterns REP.ikjuju Suspicious Metadata Mail Phishing Redirection
DNS_Server_vmware (172.27.254.2)	Anti-Virus	REP.ikjuju REP.ikkioe REP.ikktgp REP.iklueb
0.0.0.0	IPS	Sweep Scan
a23-214-49-228.deploy.static.akamaitechnologies.com (23.214.49.228)	Anti-Bot	Check Point - Testing Bot
gwR8010 (192.168.170.254)	Anti-Virus	REP.ikjuju

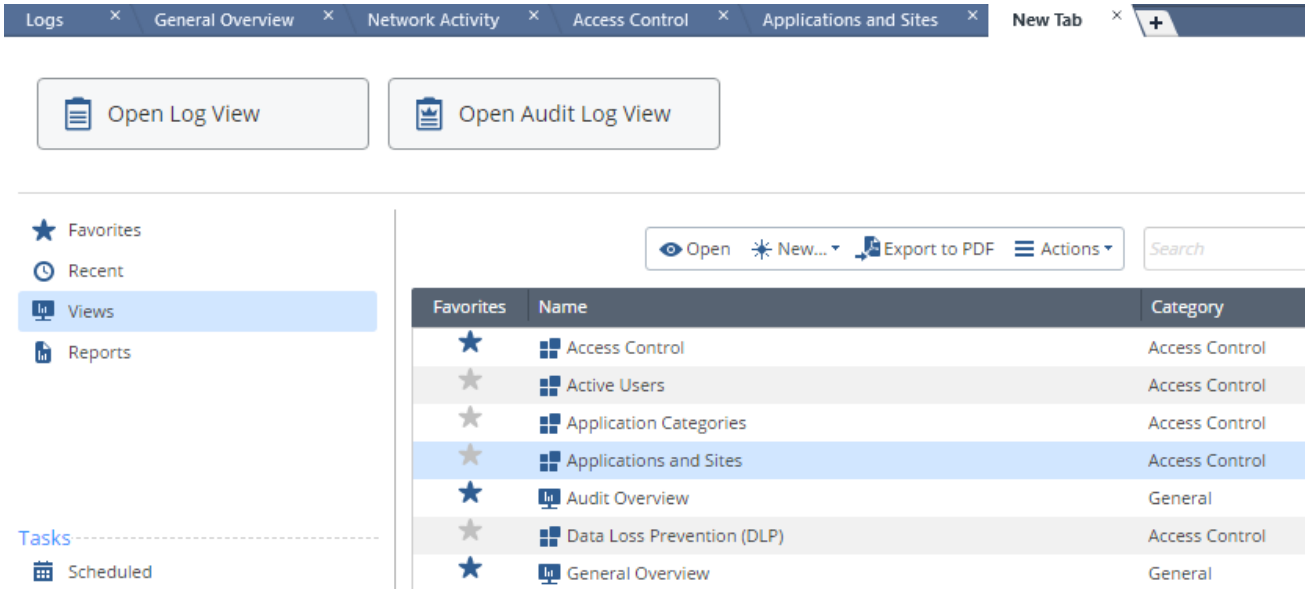


嘗試產生報表並且下載至 Windows 電腦上：

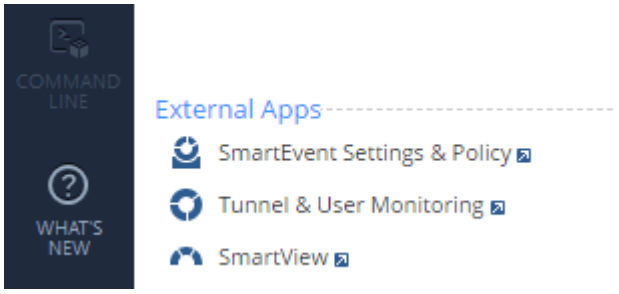


開啟 SmartView 功能

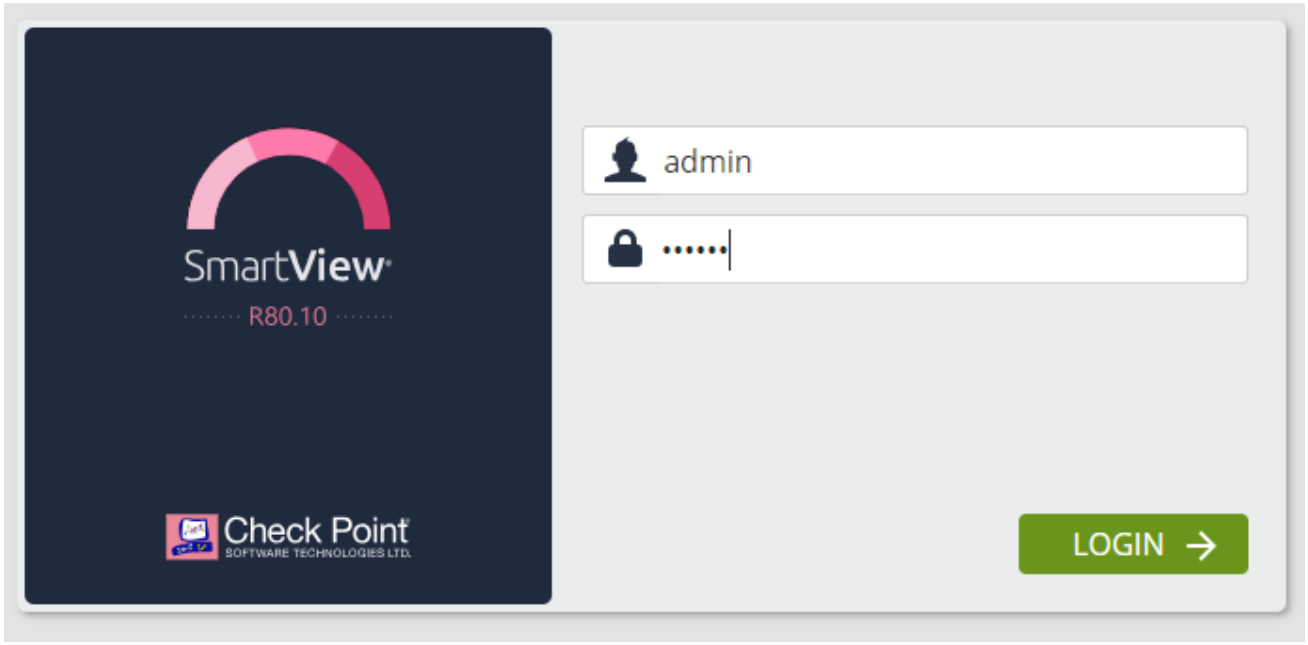
在 Log & Monitor 頁籤點選右上角「+」開新分頁：



在左下角 External Apps 中點擊「SmartView」：



自動開啟瀏覽器，輸入 SmartConsole 的帳號密碼：



透過 SmartView 功能使用瀏覽器來檢視報表：