

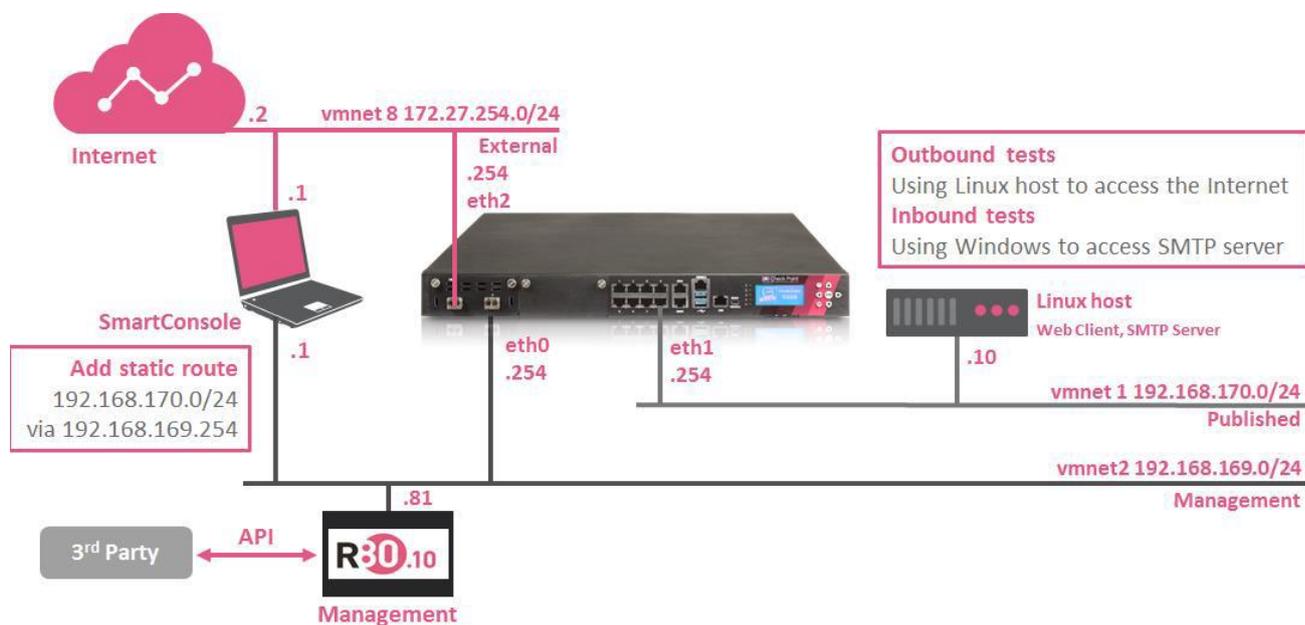
Local VM edition, May 2018

R80.10 Training Lab Guide

目錄

R80.10 Training Lab Guide	1
Lab network diagram.....	2
Lab 需求以及確認.....	2
Lab 0: 準備 Lab 使用的 Check Point 管理主機以及 Security Gateway	6
在管理主機以及 Security Gateway 上安裝 Jumbo hotfix file	6
使用 API 的 scripts 自動建立防火牆物件、服務及規則.....	9
Lab 1: 體驗 R80.10 Unified Rule Base.....	17
啟用 APCL, URLF, IPS 以及 NAT 功能並設定規則.....	17
使用 Logs & Monitor 來產生 APCL & URLF 使用報表	28
觀察 gateway 狀態.....	32
Lab 2: 了解 Content Awareness 以及 Inline Layer 的運作.....	34
目標先建立一個新的 Policy Package 「SimplePolicy」如下圖所示：	34
建立 Rule 4 的 Inline Layer 規則.....	36
建立 Content Awareness 的阻檔頁面.....	38
使用瀏覽器的 private mode 開啟 Web Server 網頁進行測試.....	42
Lab 3: Threat Prevention	46
設定 Gateway 啟用 Threat Prevention 功能.....	46
初次更新 Threat Prevention	49
測試 IPS 的防釣魚郵件防禦功能.....	51
Lab 4: 使用 SmartEvent 報表功能	54
產生一份關於 Threat Prevention 的攻擊報表	56
開啟 SmartView 功能.....	57

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

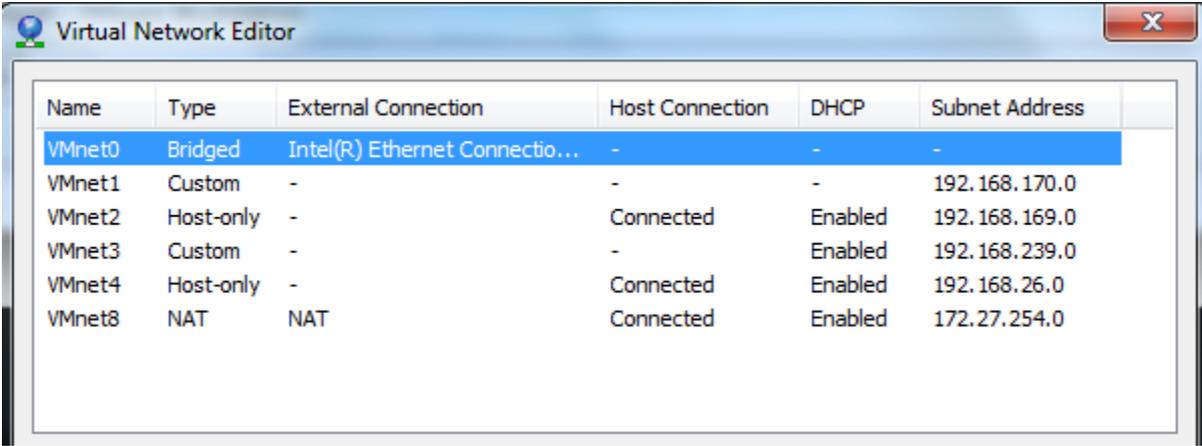
- 4 Core / 16 GB RAM
- Administrative UserID/password on management server and gateway: admin/vpn123.
- Gaia expert level password: vpn123
- Linux user/password: peter/vpn123
- Root authorization on Linux: vpn123

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：



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Intel(R) Ethernet Connectio...	-	-	-
VMnet1	Custom	-	-	-	192.168.170.0
VMnet2	Host-only	-	Connected	Enabled	192.168.169.0
VMnet3	Custom	-	-	Enabled	192.168.239.0
VMnet4	Host-only	-	Connected	Enabled	192.168.26.0
VMnet8	NAT	NAT	Connected	Enabled	172.27.254.0

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.

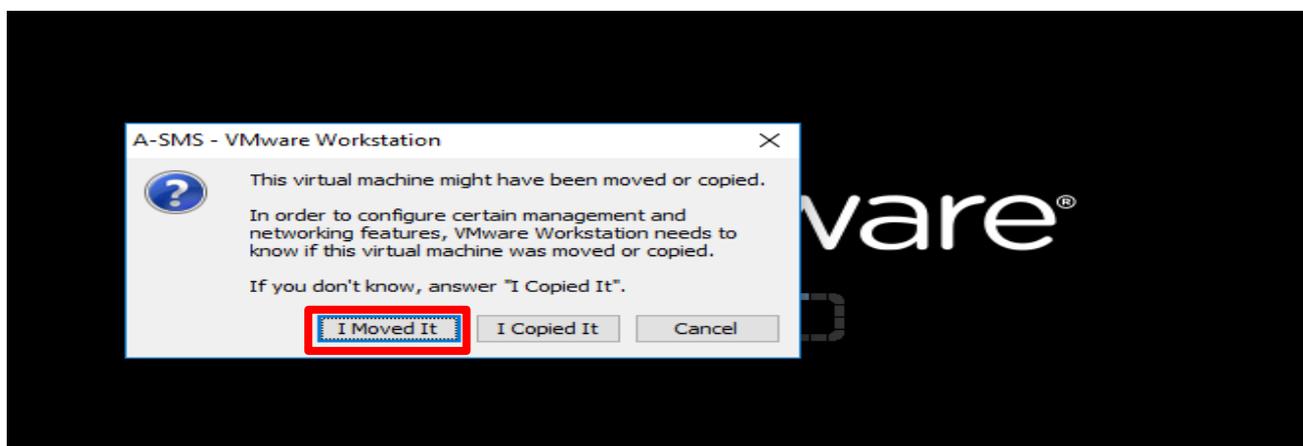
安全閘道至少須具備以下的硬體規格要求：

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。

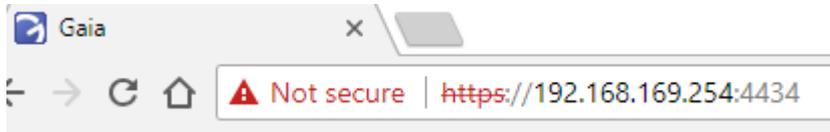
開啟 VM 時請注意：

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 。

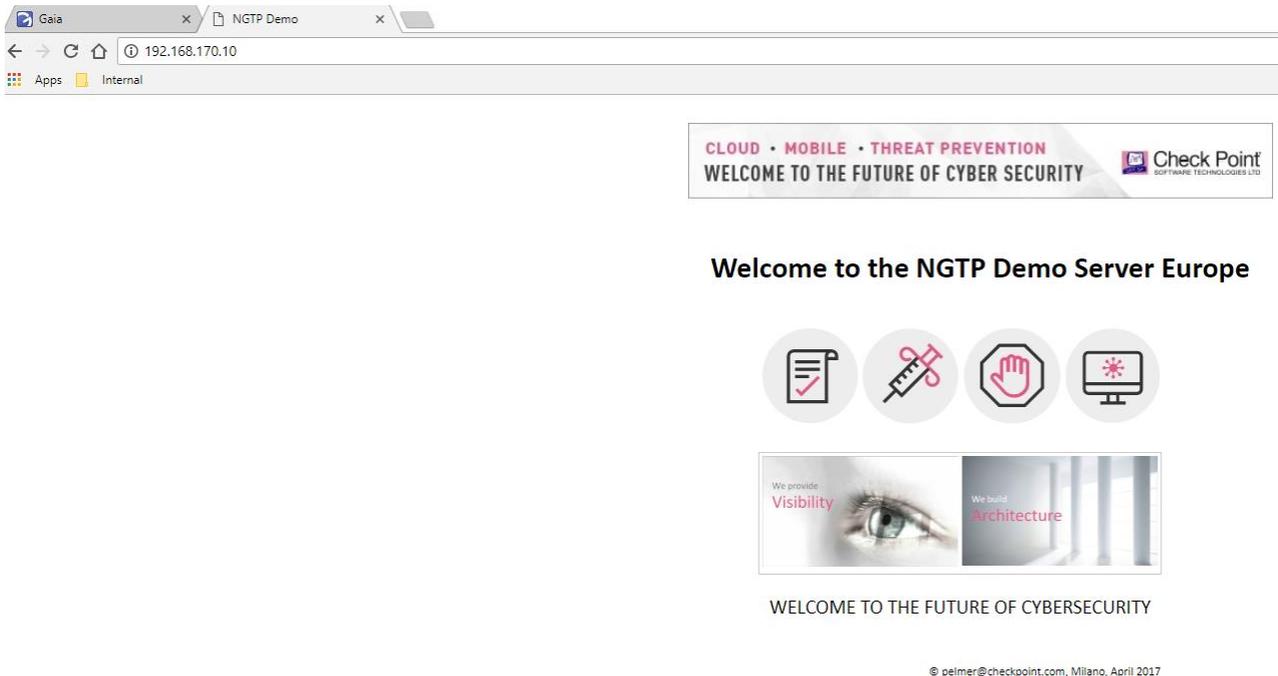


- Gateway 與 Management 都應該可以連線到 Internet 上。

```
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.prodl.media.vip.ir2.yahoo.com (87.248.98.7): icmp
_seq=1 ttl=127 time=324 ms
64 bytes from media-router-fp1.prodl.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 ：



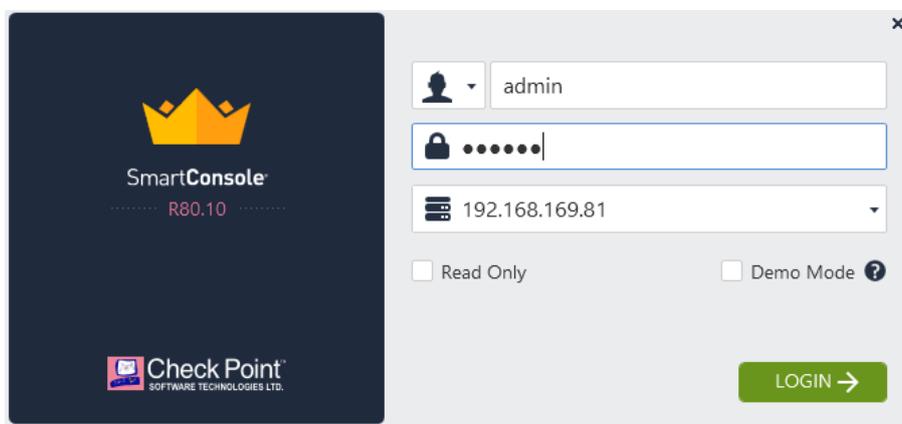
- Gateway應該可以Ping到 web+mailserver 192.168.170.10

```
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
```

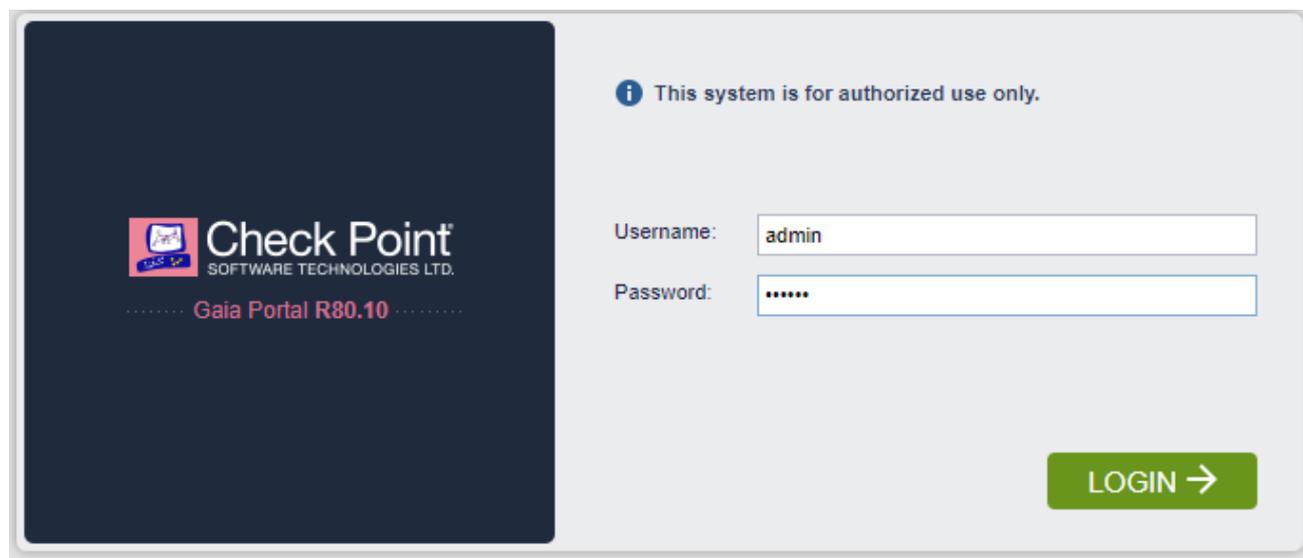
- Windows主機上的R80.10 SmartConsole應該可以成功登入SMS管理主機：



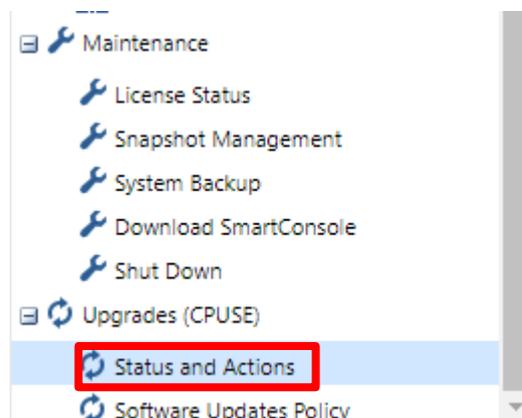
Lab 0: 準備 Lab 使用的 Check Point 管理主機以及 Security Gateway

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 :



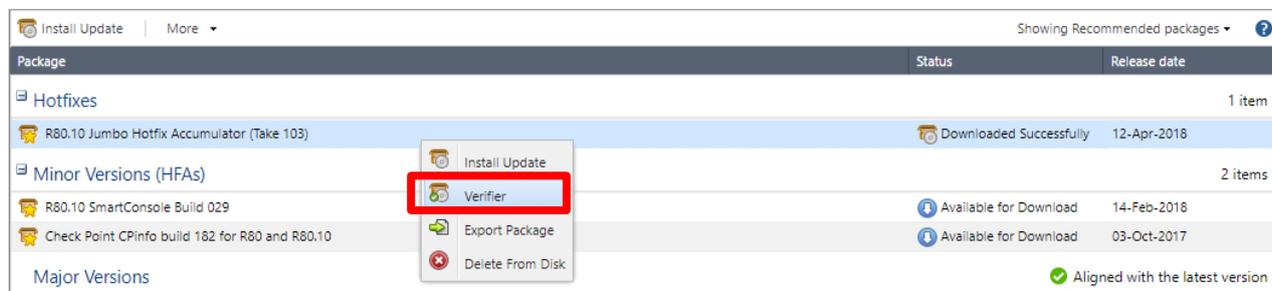
切換選項至「Upgrades(CPUSE) >> Status and Action」：



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

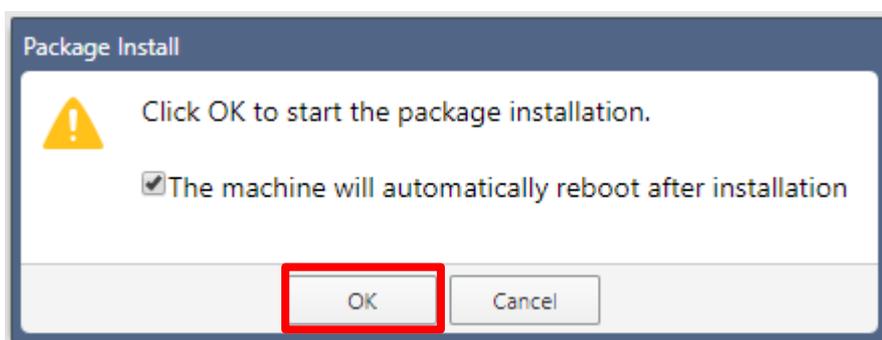
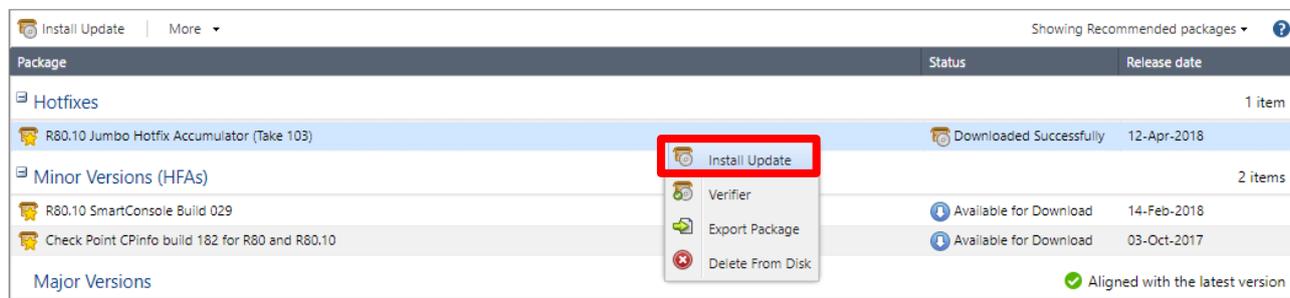
Upgrades (CPUSE) > Status and Actions

Check Point Upgrade Service Engine (CPUSE) | R80.10 take 462 [Hotfixes](#) | Last updated on: Fri May 18 14:12 2018



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：

Check Point Upgrade Service Engine (CPUSE) | R80.10 take 462 [Hotfixes](#) | Last updated on: Fri May 18 14:12 2018



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：

Configurati

Check For Updates Import Package Add Hotfixes From The Cloud

Package Details

File Name: Check_Point_R80_10_JUMBO_HF_Bundle_T103_sk116380_FULL.tgz

Package Size: 514.6 MB

Package Type: Hotfix

Release Date: 12-Apr-2018

Downloaded On: 15-May-2018 23:29:06

Status:

The package is installing: 15%

Important Messages:

- While the package is installing, the cpstop and cpstart commands are run
- After the package is installed, the machine reboots

Description:

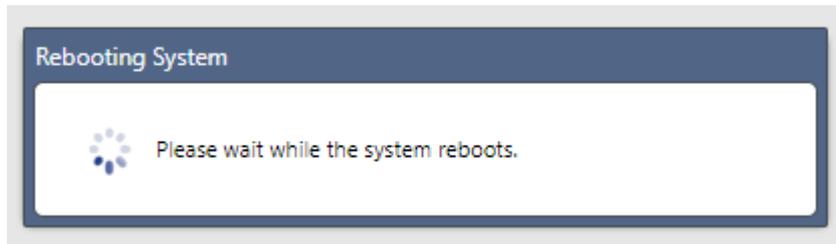
Package Hotfix Bundle R80_10_JUMBO_HF contains:

- Check Point CPFC R80.10 R80_10_JUMBO_HF - Installing...
- Check Point Security Gateway R80.10 R80_10_JUMBO_HF
- Mobile Access R80.10 R80_10_JUMBO_HF
- SmartLog R80.10 R80_10_JUMBO_HF
- Management Server Package R80.10 R80_10_JUMBO_HF
- SmartReporter R80.10 R80_10_JUMBO_HF
- R77 Compatibility Package R80.10 R80_10_JUMBO_HF
- CP1100 R77.20 Compatibility Package R80.10 R80_10_JHF_COMP
- SecurePlatform R80.10 R80_10_JUMBO_HF
- Multi-Domain Security Management R80.10 R80_10_JUMBO_HF

Note: After the package is installed, the machine reboots.

Contained in: No other packages

Contains the following packages: No other packages



重新開機完成後即會顯示完成安裝。

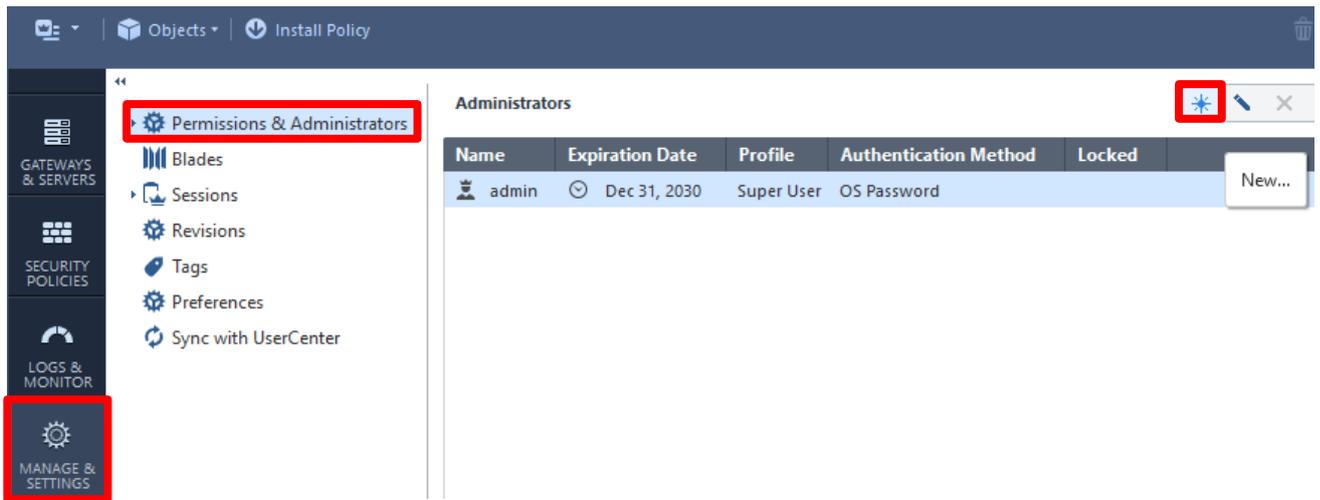
使用 API 的 scripts 自動建立防火牆物件、服務及規則

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。

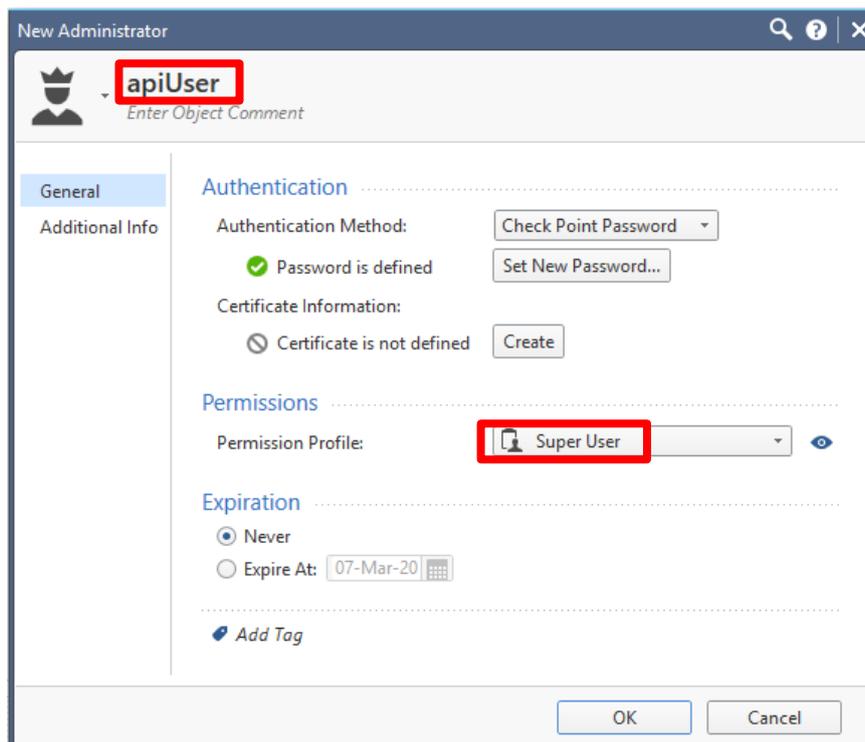
建立 API 要使用的 api 帳號

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

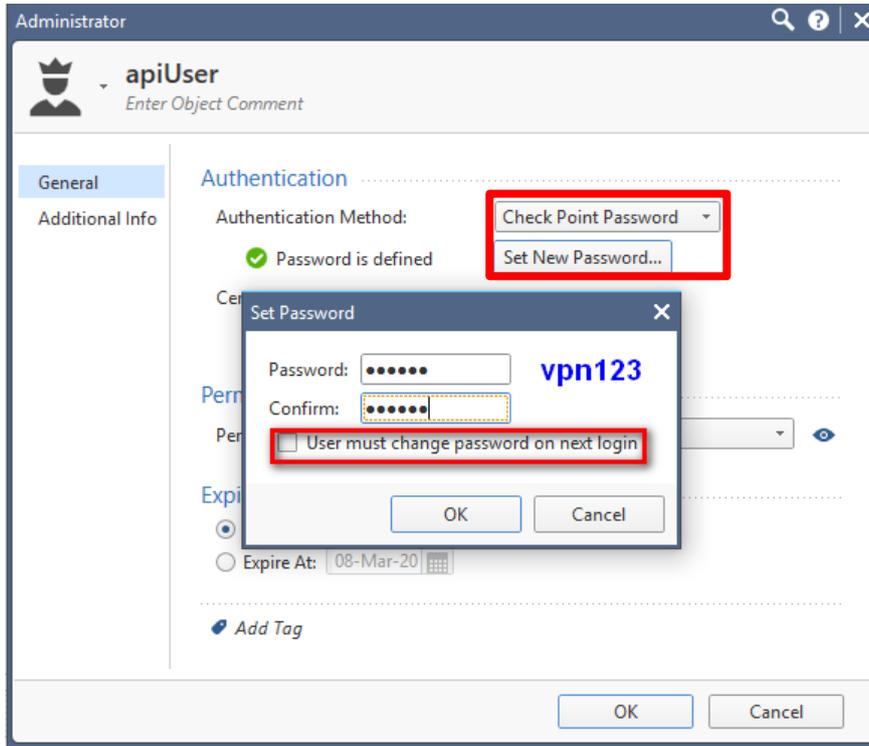


輸入帳號名稱為「apiUser」、Permissions Profile 為「Super User」：

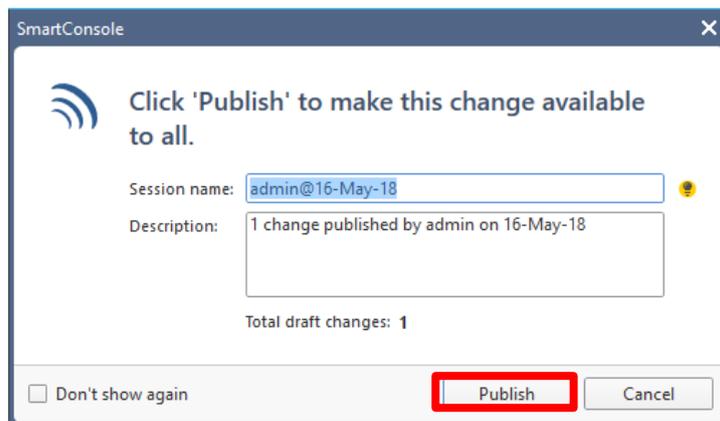
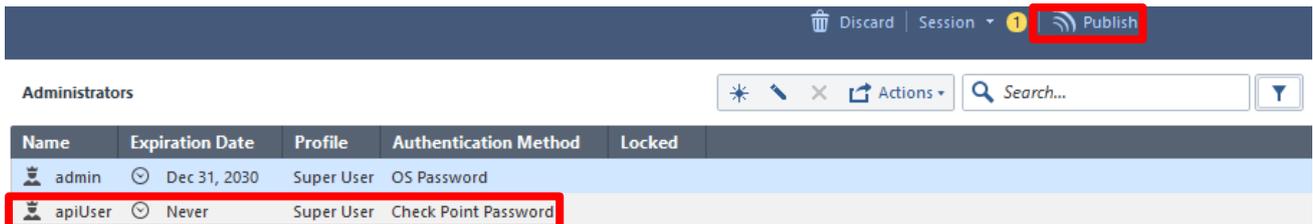
請注意帳號大小寫必須完全相同，後面執行 Script 才不會有錯誤



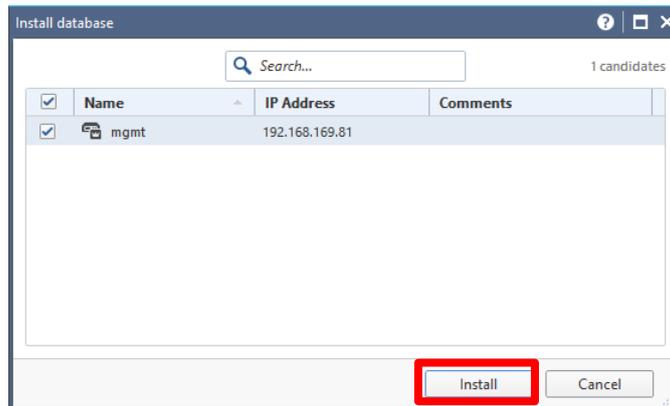
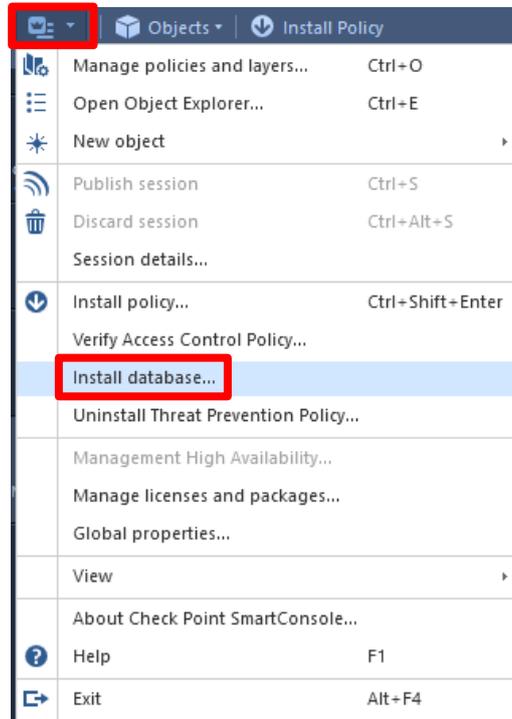
選擇 Authentication Method 為「Check Point Password」並點選「Set New Password...」設定密碼，
 密碼請輸入「vpn123」並取消勾選「User must change password on next login」，完成後點選 OK >> OK：
 請注意密碼大小寫必須完全相同，並取消勾選該選項，後面執行 Script 才不會有錯誤



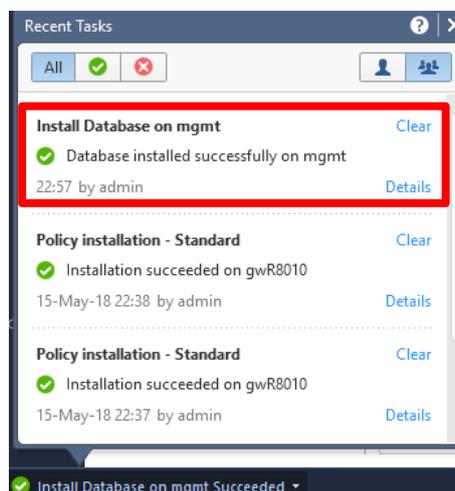
剛建立的 api 使用者會出現在下方，點選上方的「Publish」將設定儲存於 SMS 上



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：

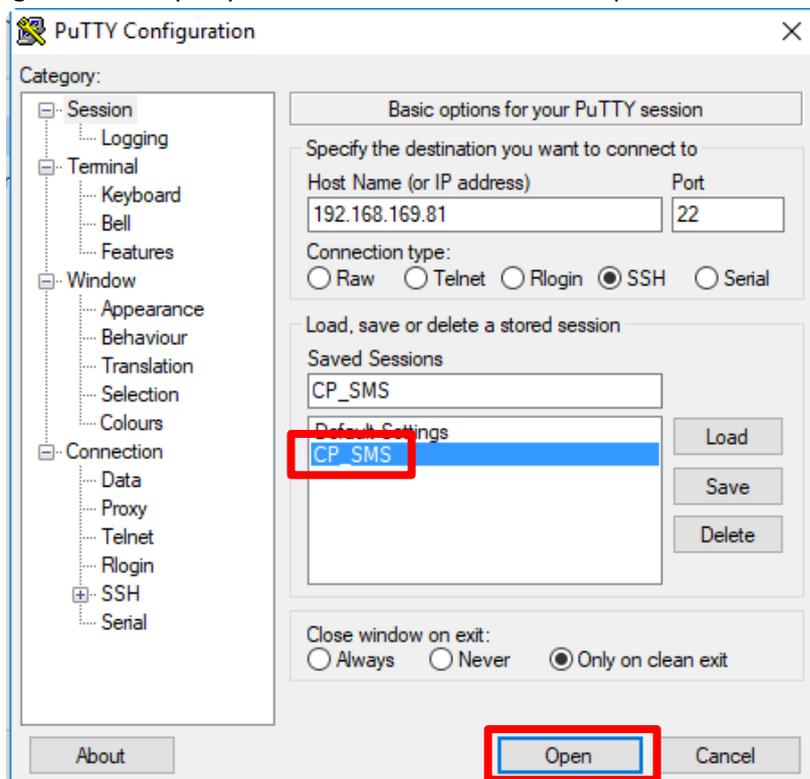


待左下角的任務選單出現「Database installed successfully on mgmt」就代表完成設定：



執行 scripts

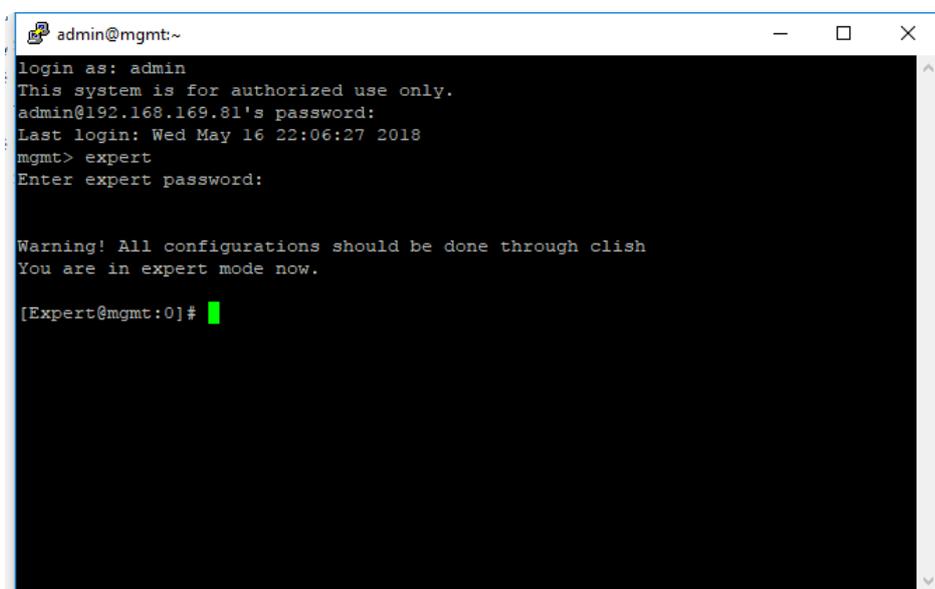
使用R80.10 Training資料夾中的putty登入SMS管理主機，並進入Expert模式：



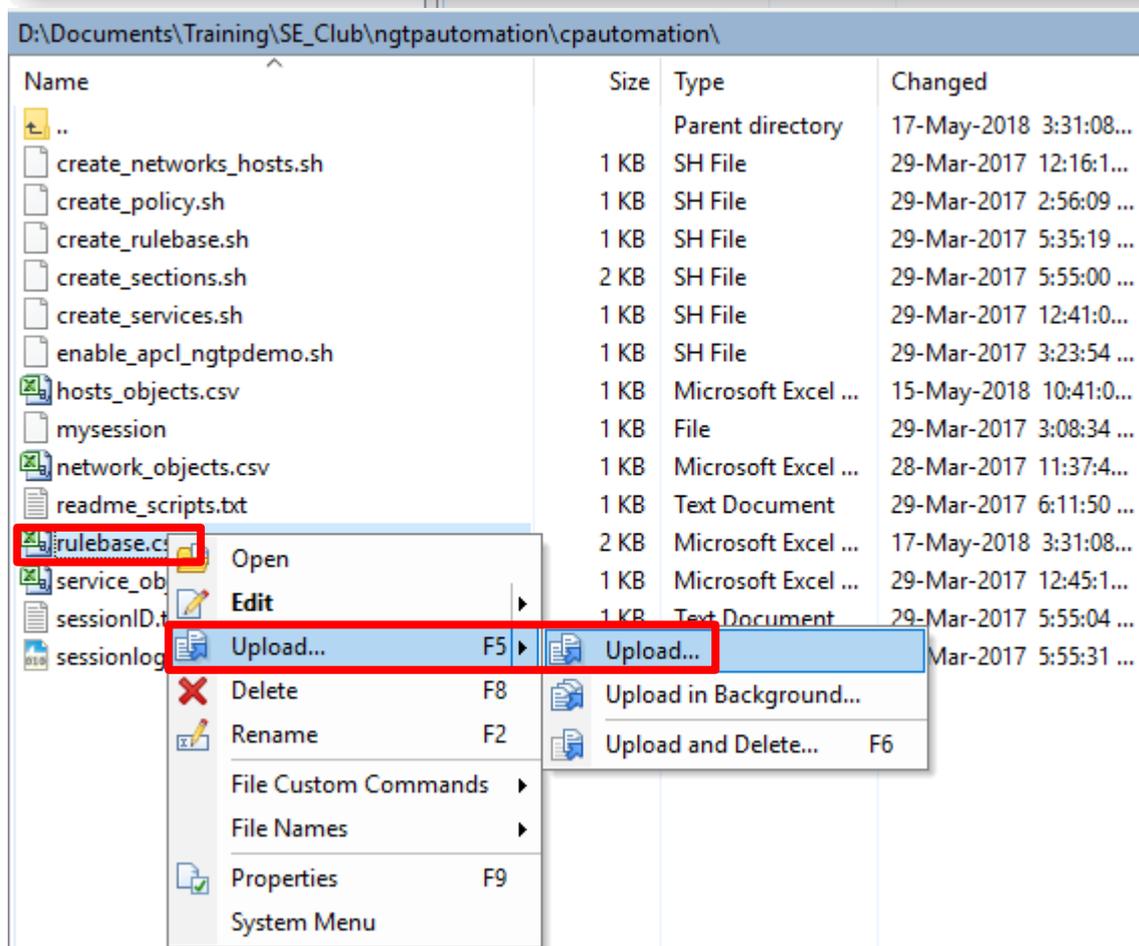
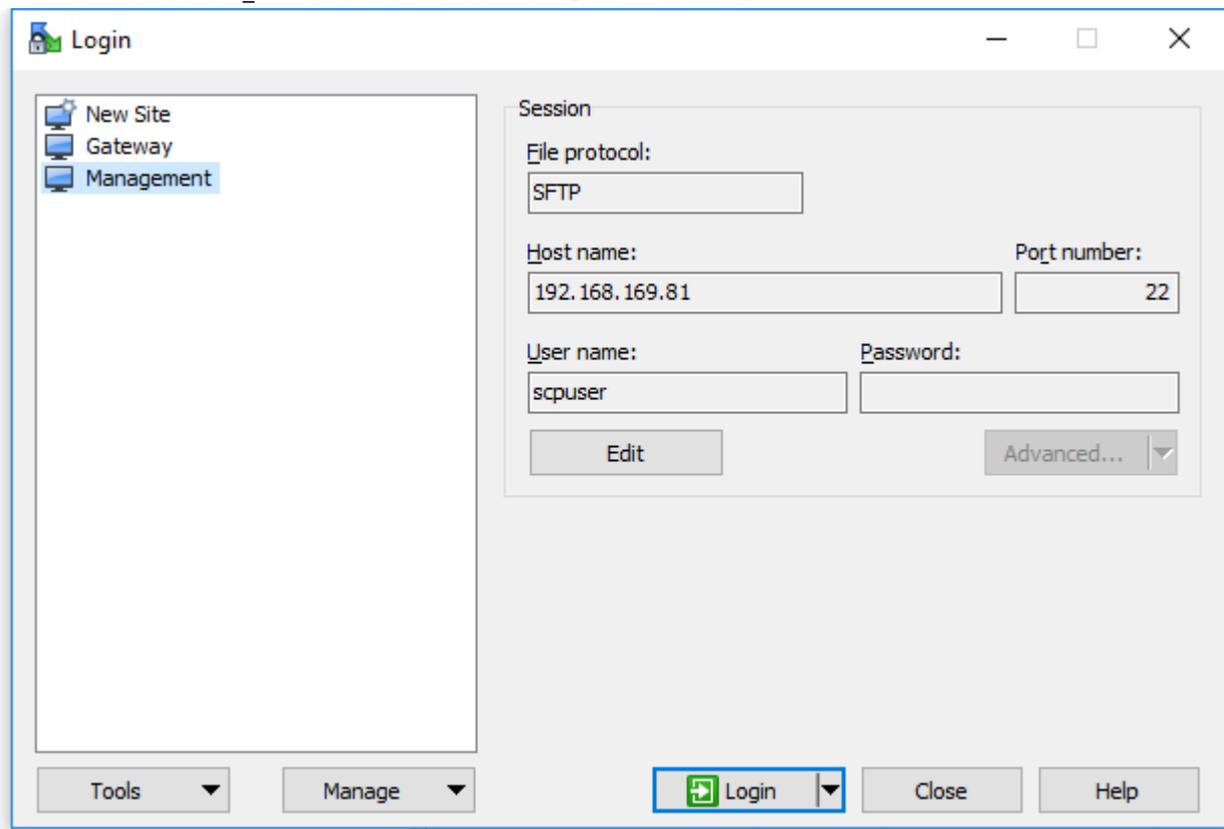
```
mgmt> expert
Enter expert password:
```

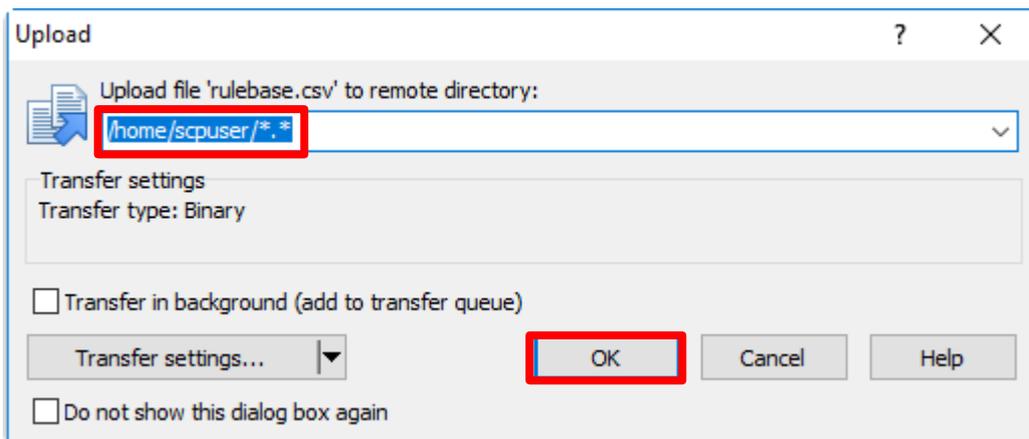
```
Warning! All configurations should be done through clish
You are in expert mode now.
```

```
[Expert@mgmt:0]#
```

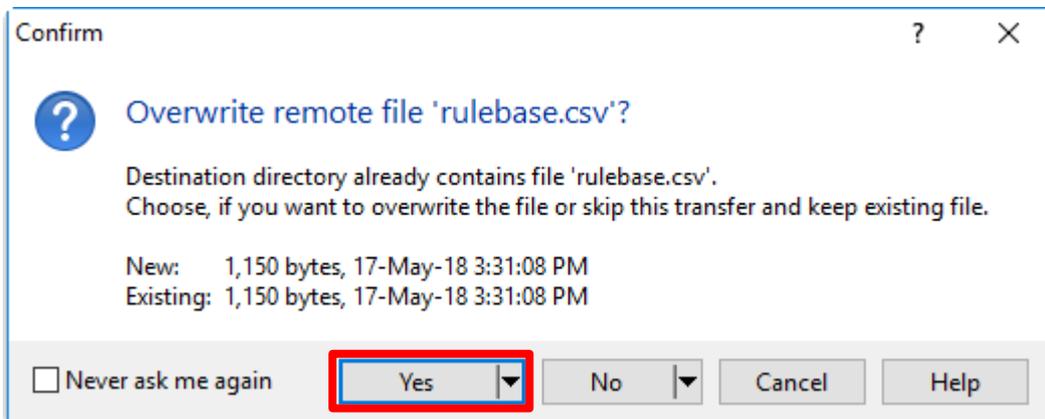


請開啟WinSCP並連到CP_SMS身上，上傳「rulebase.csv」至SMS管理主機：





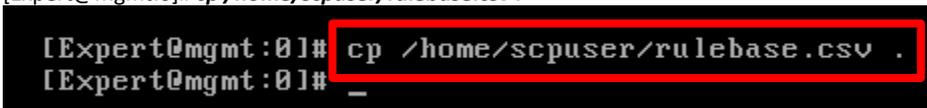
選擇「Yes」覆蓋原本的rulebase.csv檔案：



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 :

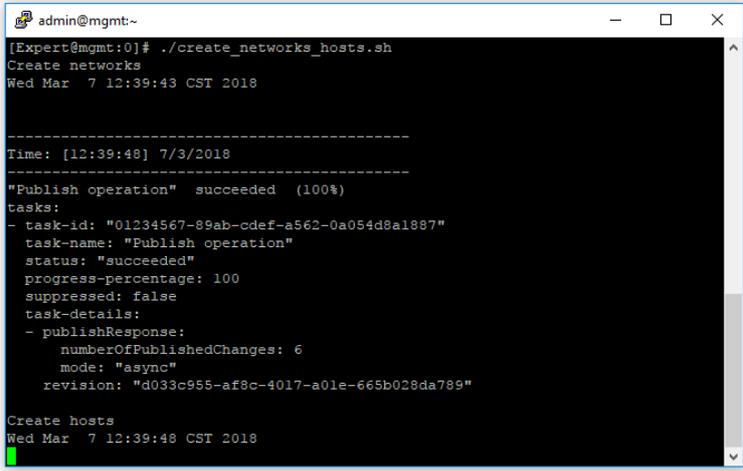
```
[Expert@mgmt:0]# ./create_networks_hosts.sh
```

Running order:

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

Sessions

Name	Administrator	Connected From	Connection Mode	Application	Locks	Changes	Login	Logout
(Unnamed)	admin	192.168.169.1	Read Write	SmartConsole	0	0	07-Mar-18 11:25	
(Unnamed)	apiUser	127.0.0.1	Read Write	Web API	0	0	07-Mar-18 12:39	



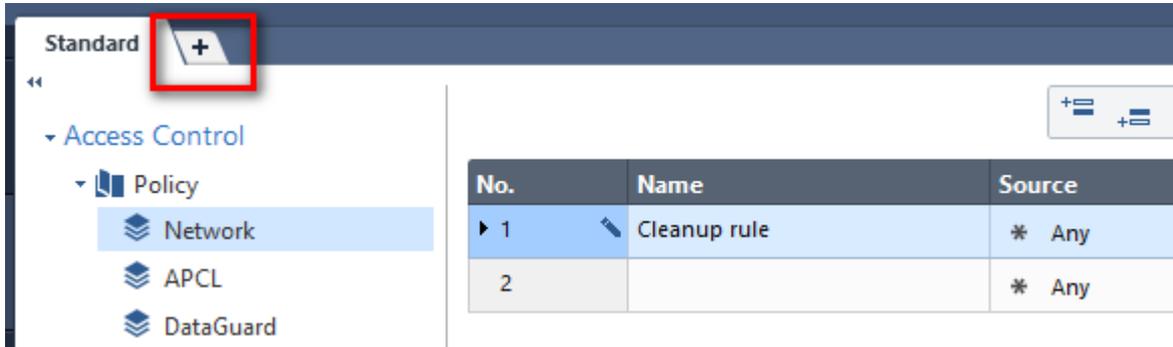
```
admin@mgmt:~
[Expert@mgmt:0]# ./create_networks_hosts.sh
Create networks
Wed Mar 7 12:39:43 CST 2018

-----
Time: [12:39:48] 7/3/2018
-----
"Publish operation" succeeded (100%)
tasks:
- task-id: "01234567-89ab-cdef-a562-0a054d8a1887"
  task-name: "Publish operation"
  status: "succeeded"
  progress-percentage: 100
  suppressed: false
  task-details:
  - publishResponse:
    numberOfPublishedChanges: 6
    mode: "async"
    revision: "d033c955-af8c-4017-a01e-665b028da789"

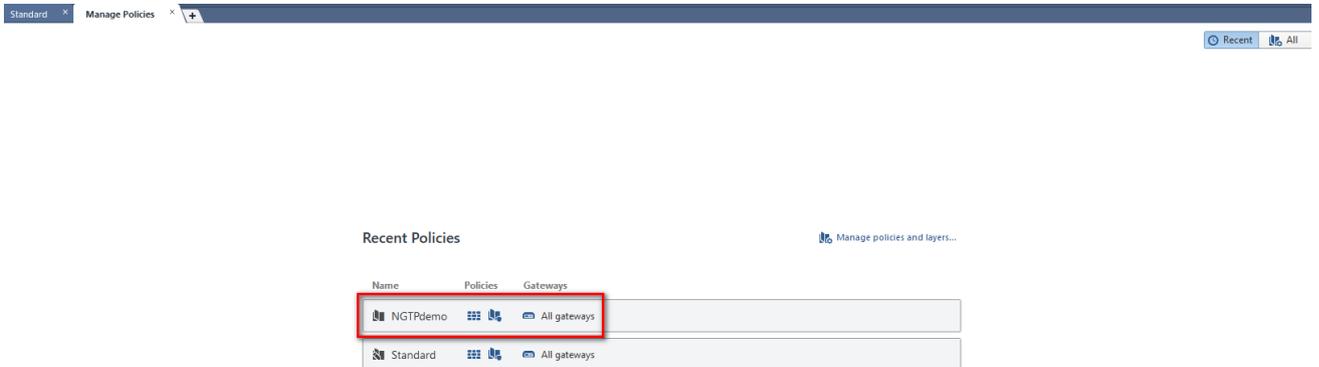
Create hosts
Wed Mar 7 12:39:48 CST 2018
```

開啟匯入的 Policy Package

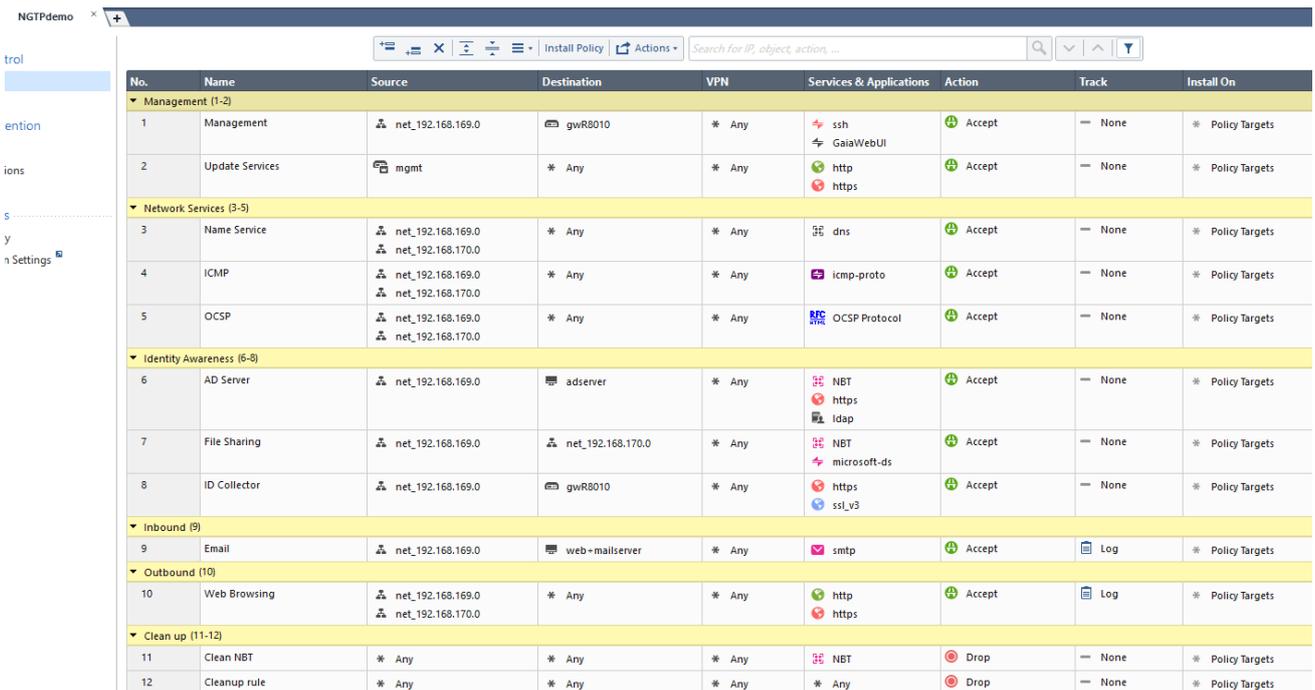
執行完成 6 個 Script 之後，回到 SmartConsole 的 Policy 頁籤，點選「+」號開啟新的分頁：



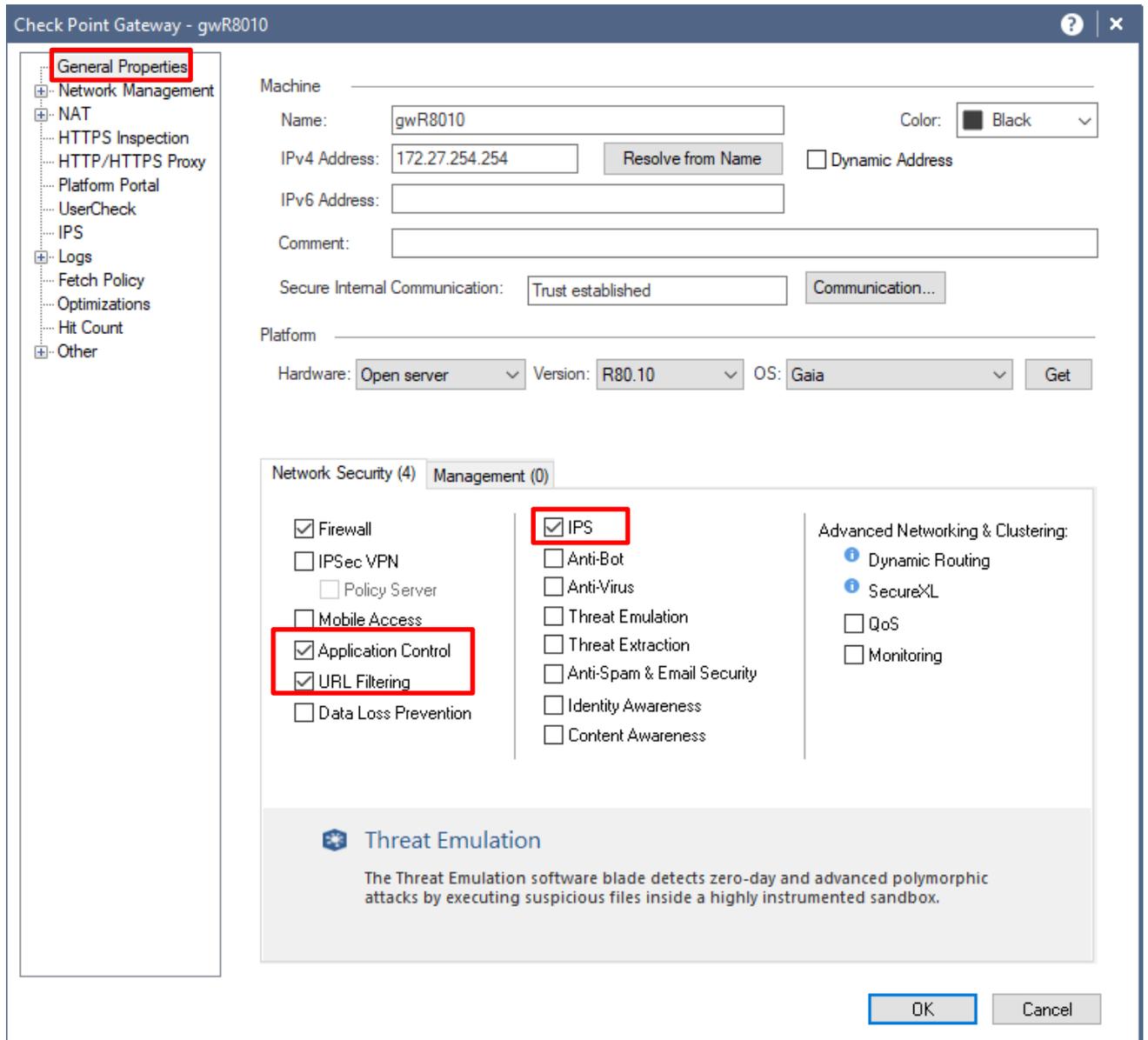
你會看見剛剛透過 API 自動建立的 Policy Package 「NGTPdemo」，點擊 Policy Package 打開：



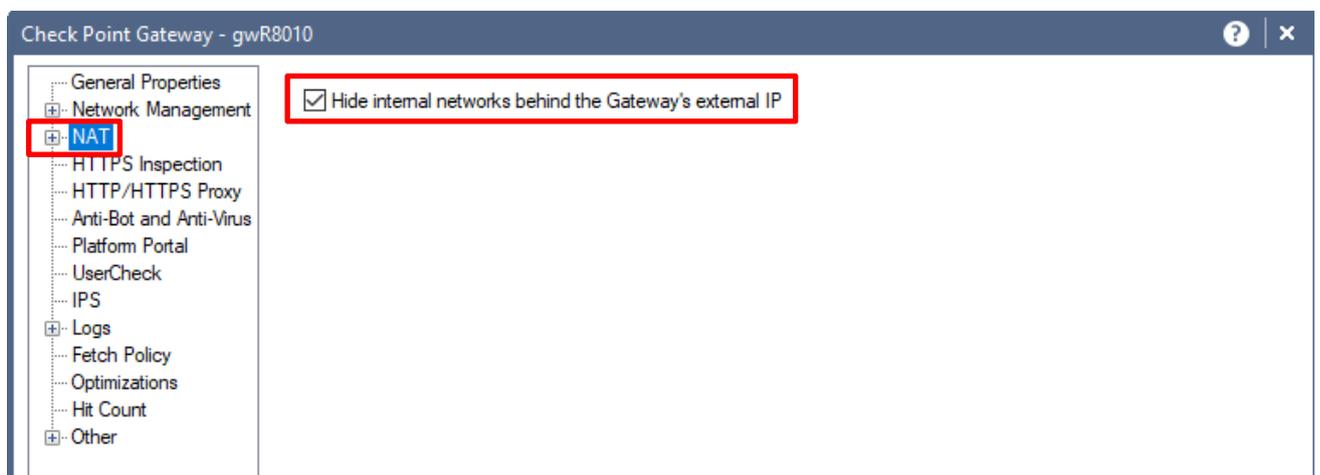
確認 Policy Package 「NGTPdemo」的內容與下圖完全相同（共有 12 條規則）：



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」

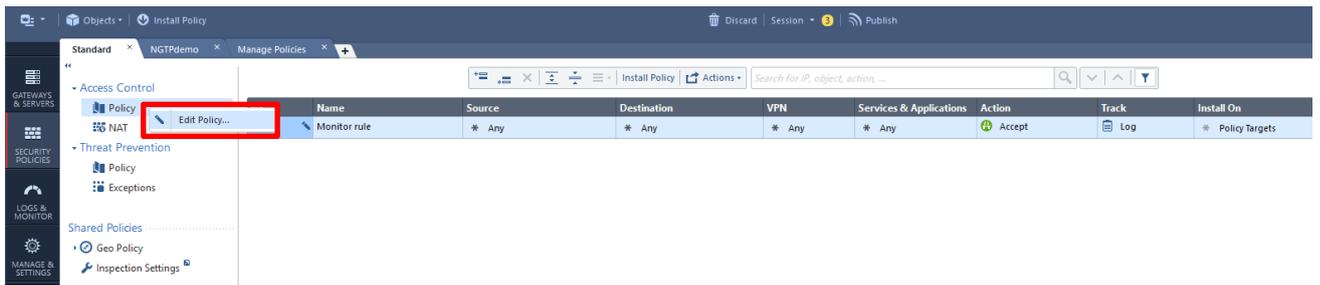


在 Standard Policy Package 中修改預設規則的 Name 為「Monitor rule」並調整 Track 欄位為「Log」：

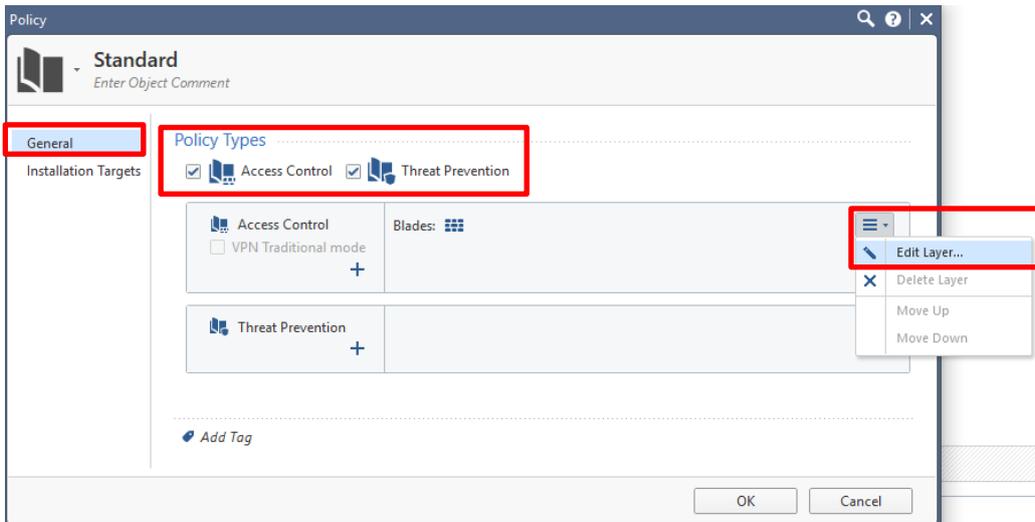


在規則上開啟 Firewall, APCL&URL 功能：

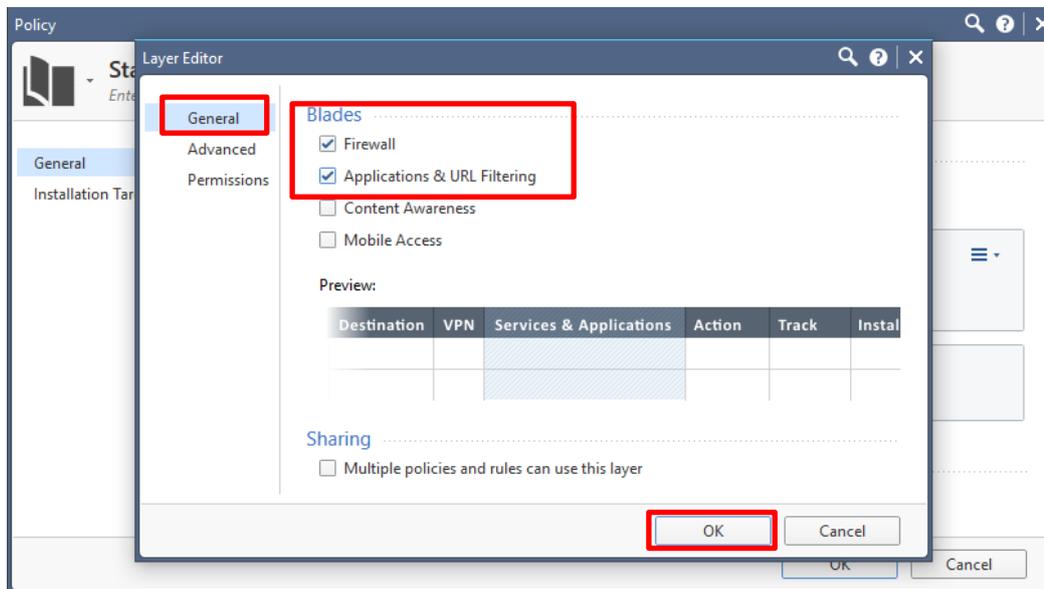
Access Control >> Policy 按右鍵「Edit Policy...」



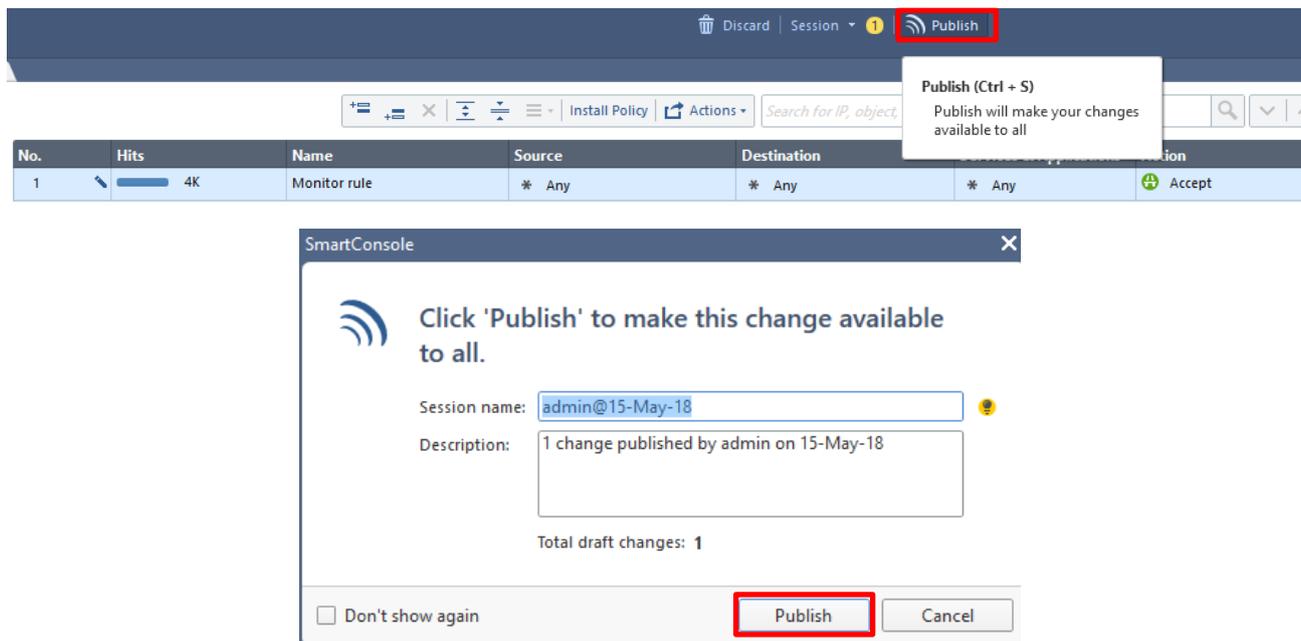
在 Access Control >> Policy 點選右邊下拉式選單「Edit Layer...」



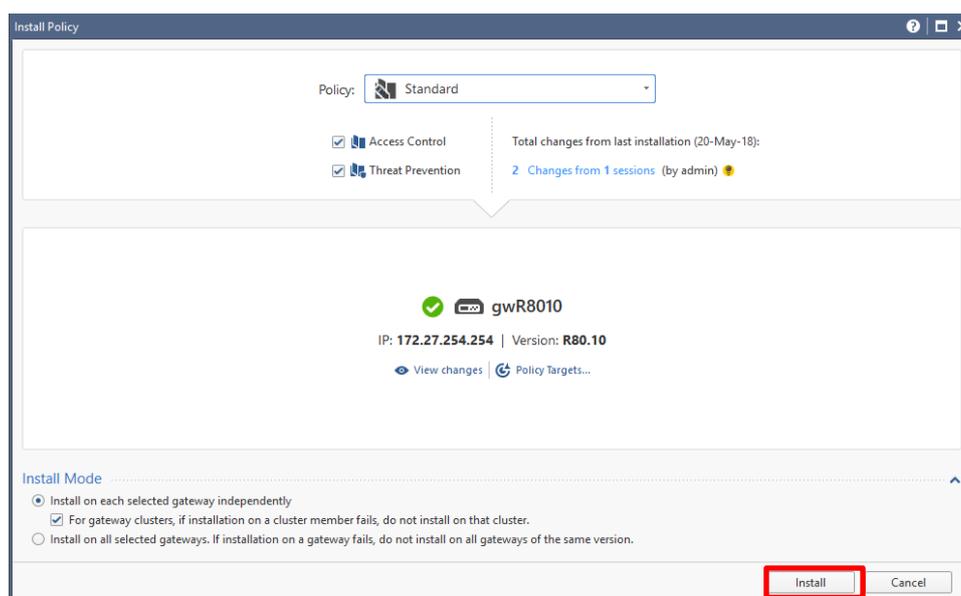
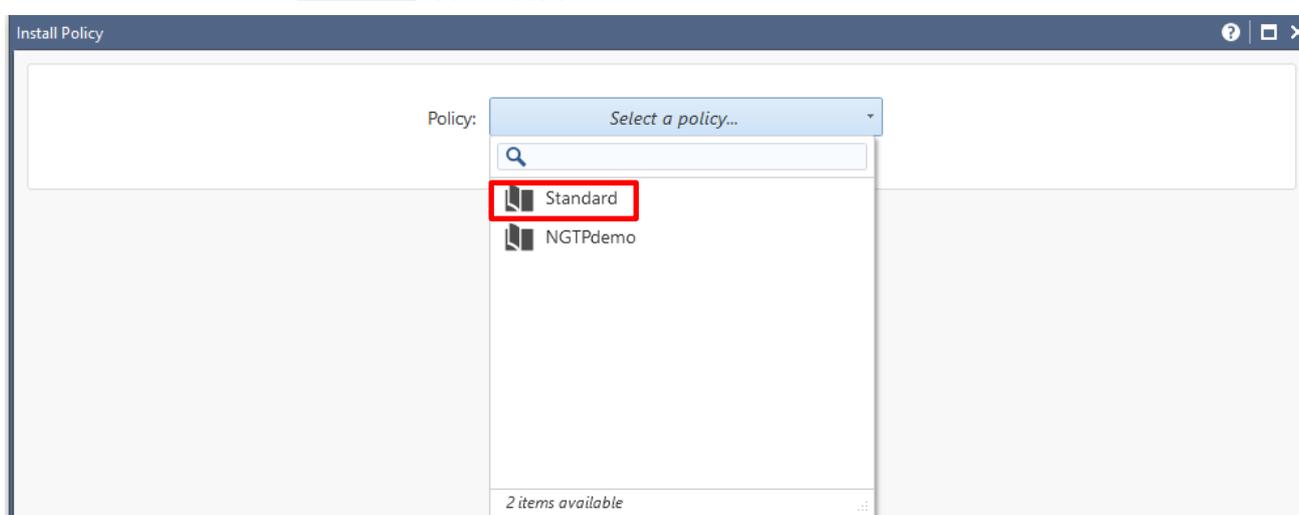
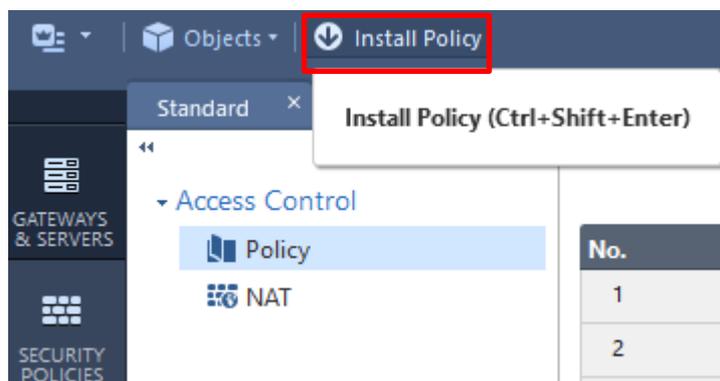
在 Blades 勾選「Firewall, Applications & URL Filtering」再點選 OK 確認。



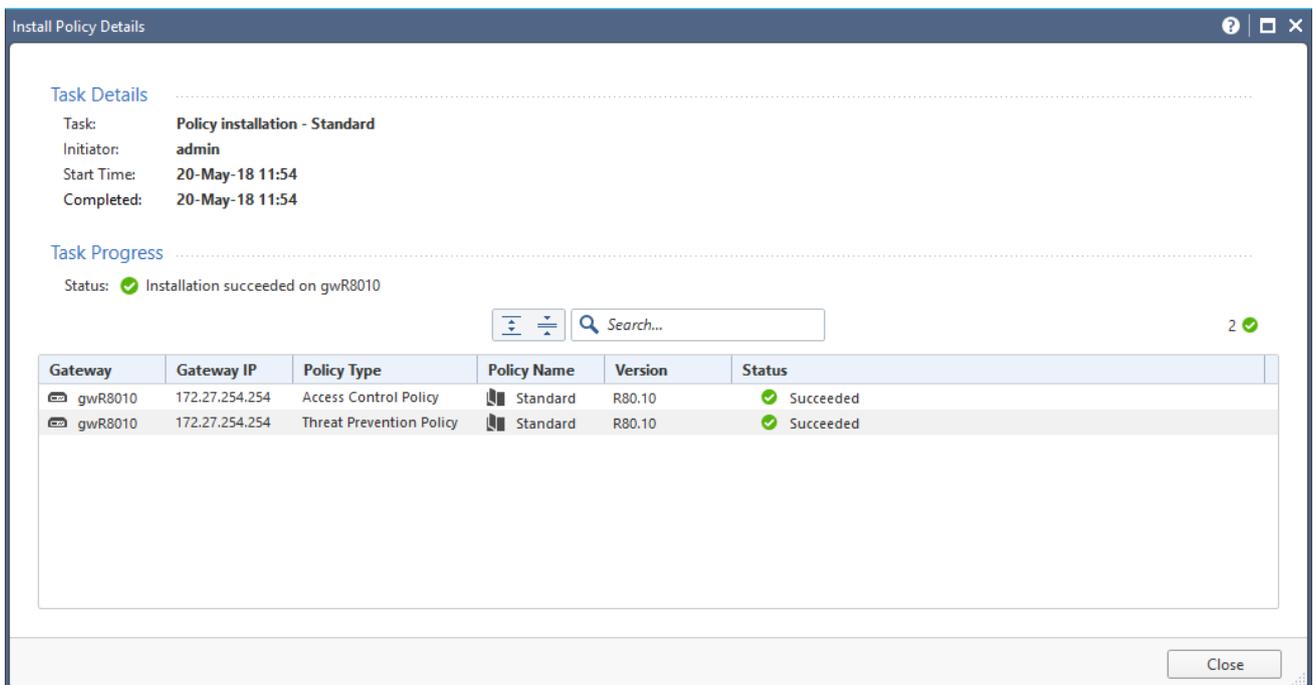
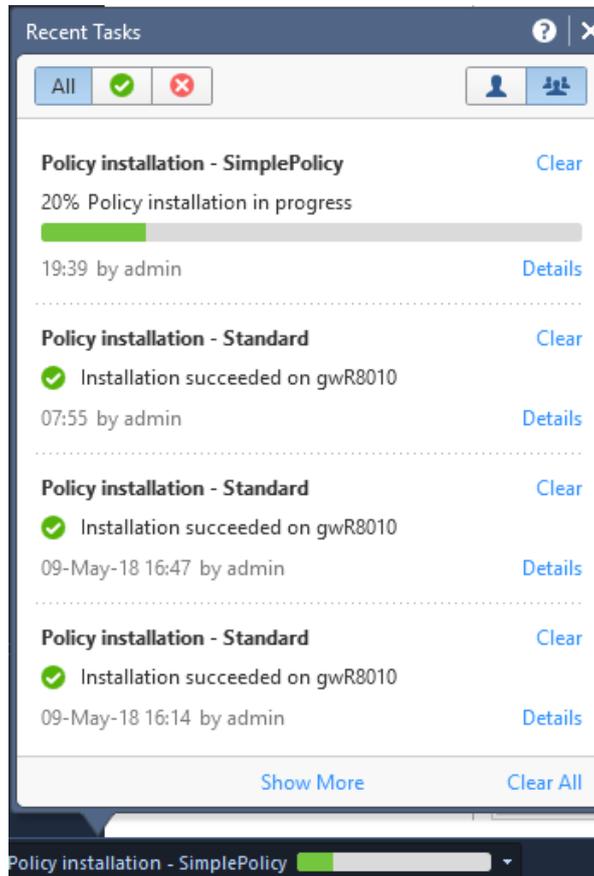
將設定進行「Publish」，儲存於 SMS 管理主機：



「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：

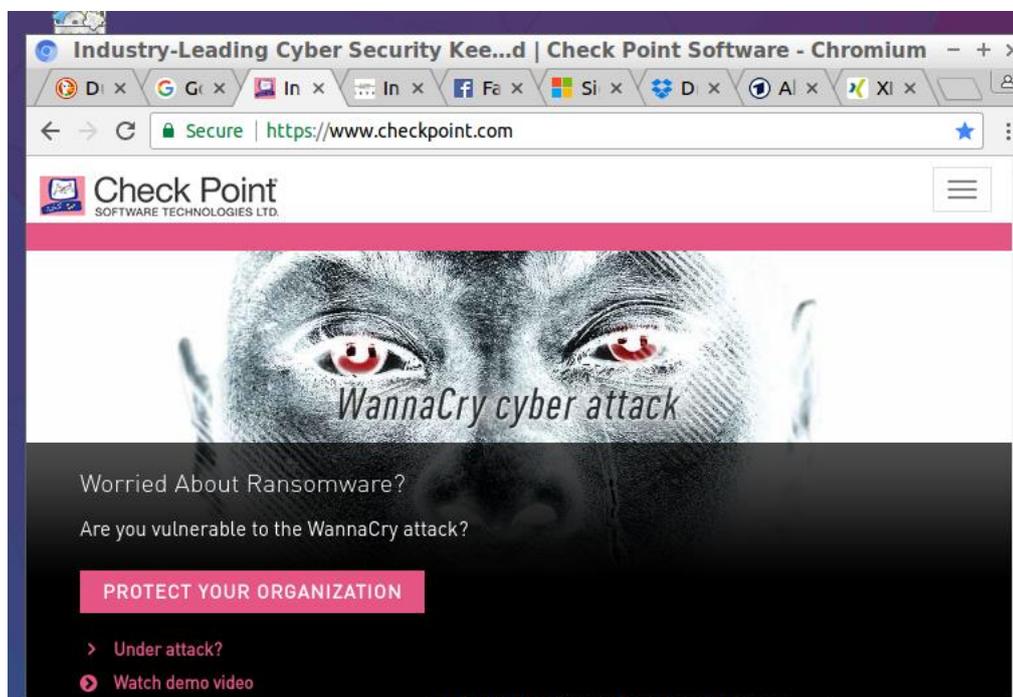


等待 installation progress 結束即完成 Policy 規則的派送：



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

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 3:40:20 PM	gwR8010	mgmt (192.168.1...		172.27.254.2	domain-udp (UDP/53)	1	Monitor rule	Standard	domain-udp Traffic Accepted from 192.168.169.81 to 172.27.254.2
Today, 3:40:18 PM	gwR8010	mgmt (192.168.1...		172.27.254.2	domain-udp (UDP/53)	1	Monitor rule	Standard	domain-udp Traffic Accepted from 192.168.169.81 to 172.27.254.2
Today, 3:40:17 PM	gwR8010	mgmt (192.168.1...		172.27.254.2	domain-udp (UDP/53)	1	Monitor rule	Standard	domain-udp Traffic Accepted from 192.168.169.81 to 172.27.254.2
Today, 3:40:16 PM	gwR8010	mgmt (192.168.1...		172.27.254.2	domain-udp (UDP/53)	1	Monitor rule	Standard	domain-udp Traffic Accepted from 192.168.169.81 to 172.27.254.2
Today, 3:40:15 PM	gwR8010	mgmt (192.168.1...		172.27.254.2	domain-udp (UDP/53)	1	Monitor rule	Standard	domain-udp Traffic Accepted from 192.168.169.81 to 172.27.254.2
Today, 3:40:12 PM	gwR8010 (172.2...	gwR8010 (172.2...		172.27.254.2	domain-udp (UDP/53)	0	Implied Rule	Standard	domain-udp Traffic Accepted from 172.27.254.254 to 172.27.254.2
Today, 3:40:12 PM	gwR8010 (172.2...	gwR8010 (172.2...		172.27.254.2	domain-udp (UDP/53)	0	Implied Rule	Standard	domain-udp Traffic Accepted from 172.27.254.254 to 172.27.254.2
Today, 3:40:11 PM	gwR8010 (172.2...	gwR8010 (172.2...		172.27.254.2	domain-udp (UDP/53)	0	Implied Rule	Standard	domain-udp Traffic Accepted from 172.27.254.254 to 172.27.254.2
Today, 3:40:10 PM	gwR8010 (172.2...	gwR8010 (172.2...		172.27.254.2	domain-udp (UDP/53)	0	Implied Rule	Standard	domain-udp Traffic Accepted from 172.27.254.254 to 172.27.254.2
Today, 3:40:10 PM	gwR8010 (172.2...	gwR8010 (172.2...		172.27.254.2	domain-udp (UDP/53)	0	Implied Rule	Standard	domain-udp Traffic Accepted from 172.27.254.254 to 172.27.254.2

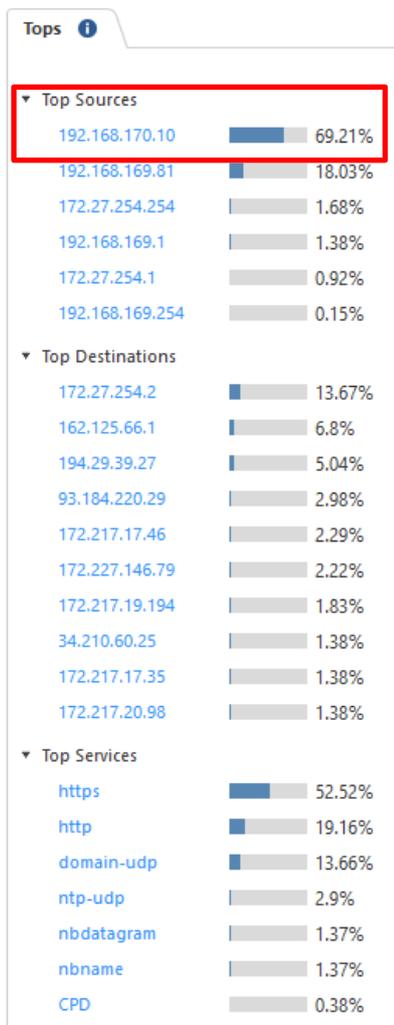
在上方灰色欄位處按右鍵並選擇「Automatic Profile Selection」：

Time

- Add Filter
- Hide Column
- Edit Profile
- Save Profile
- Save Profile As...
- Reset Profile Changes
- Automatic Profile Selection
- Manual Profile Selection
- Columns Profile

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?

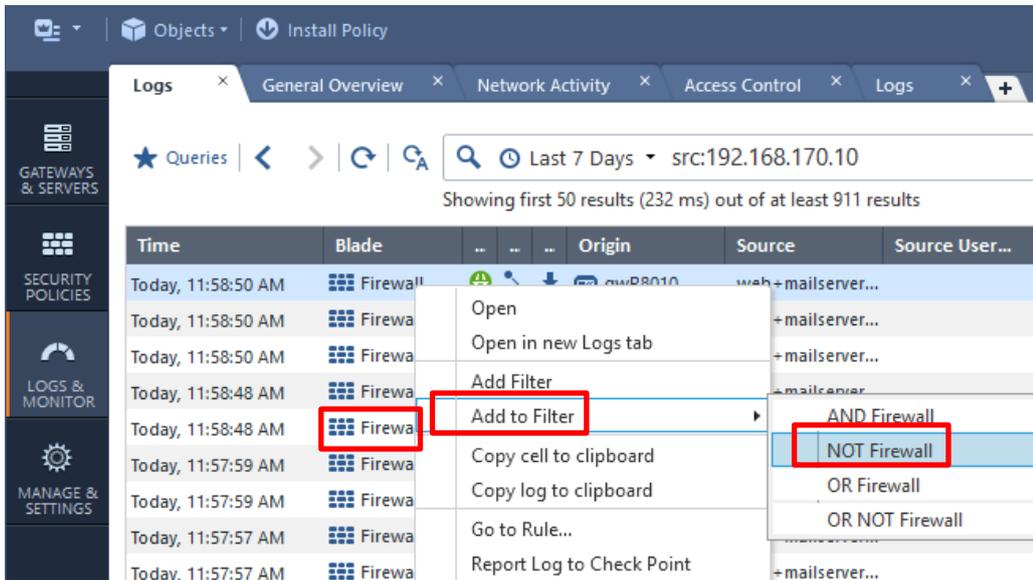
★ Queries | < > | 192.168.170.10 | Last 7 Days | src:192.168.170.10 | Showing first 50 results (232 ms) out of at least 911 results

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 11:58:50 AM	gwR8010	web-mailserver...		static.109.22...	ntp-udp (UDP/123)	1	Monitor rule	Standard	ntp-udp Traffic Accepted from 192.168.170.10 to 109.226.40.40
Today, 11:58:50 AM	gwR8010	web-mailserver...		pugot.canon...	ntp-udp (UDP/123)	1	Monitor rule	Standard	ntp-udp Traffic Accepted from 192.168.170.10 to 91.189.94.4
Today, 11:58:50 AM	gwR8010	web-mailserver...		chilipepper.c...	ntp-udp (UDP/123)	1	Monitor rule	Standard	ntp-udp Traffic Accepted from 192.168.170.10 to 91.189.89.198
Today, 11:58:48 AM	gwR8010	web-mailserver...		golem.canon...	ntp-udp (UDP/123)	1	Monitor rule	Standard	ntp-udp Traffic Accepted from 192.168.170.10 to 91.189.89.199
Today, 11:58:48 AM	gwR8010	web-mailserver...		alphyn.canon...	ntp-udp (UDP/123)	1	Monitor rule	Standard	ntp-udp Traffic Accepted from 192.168.170.10 to 91.189.91.157
Today, 11:57:59 AM	gwR8010	web-mailserver...		104.20.135.5	https (TCP/443)	1	Monitor rule	Standard	https Traffic Accepted from 192.168.170.10 to 104.20.135.5
Today, 11:57:59 AM	gwR8010	web-mailserver...		104.20.135.5	https (TCP/443)	1	Monitor rule	Standard	https Traffic Accepted from 192.168.170.10 to 104.20.135.5
Today, 11:57:57 AM	gwR8010	web-mailserver...		46.228.164.11	http (TCP/80)	1	Monitor rule	Standard	http Traffic Accepted from 192.168.170.10 to 46.228.164.11
Today, 11:57:57 AM	gwR8010	web-mailserver...		178.255.83.1	http (TCP/80)	1	Monitor rule	Standard	http Traffic Accepted from 192.168.170.10 to 178.255.83.1
Today, 11:57:57 AM	gwR8010	web-mailserver...		178.255.83.1	http (TCP/80)	1	Monitor rule	Standard	http Traffic Accepted from 192.168.170.10 to 178.255.83.1
Today, 11:57:57 AM	gwR8010	web-mailserver...		178.255.83.1	http (TCP/80)	1	Monitor rule	Standard	http Traffic Accepted from 192.168.170.10 to 178.255.83.1

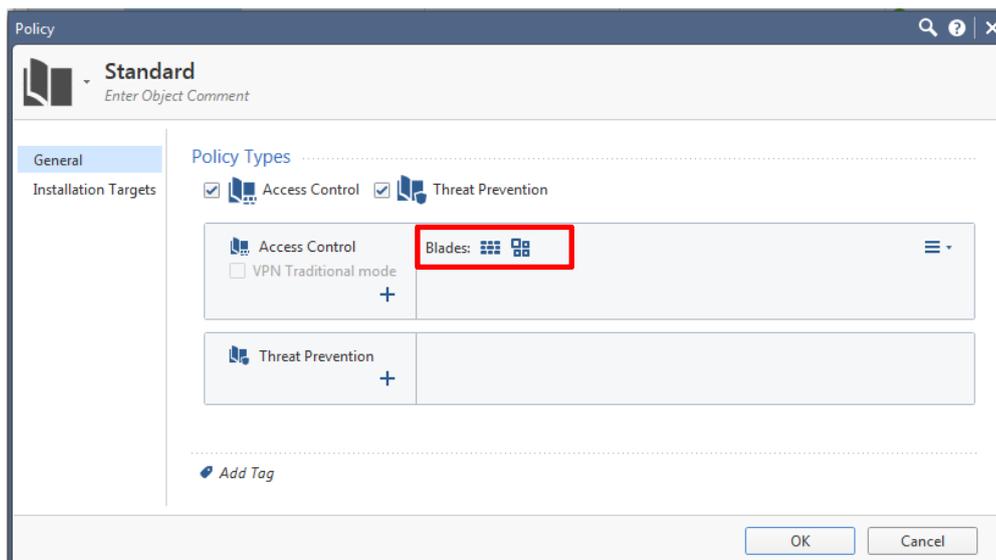
Tops

- Top Sources**
 - 192.168.170.10 100%
- Top Destinations**
 - 162.125.66.1 9.77%
 - 93.184.220.29 4.28%
 - 172.217.17.46 3.29%
 - 172.227.146.79 3.18%
 - 172.217.19.194 2.63%
 - 34.210.60.25 1.98%
 - 172.217.17.35 1.98%
 - 172.217.20.98 1.98%

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？



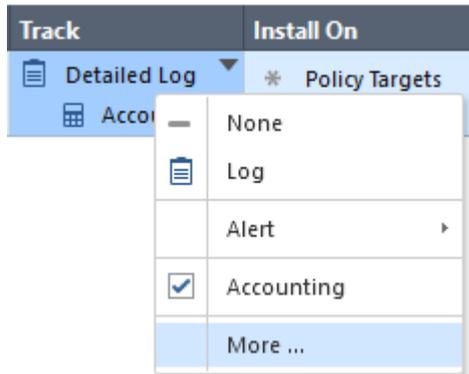
確認一下 APCL & URLF Blades 在 Gateway 上是否已經有開啟了？



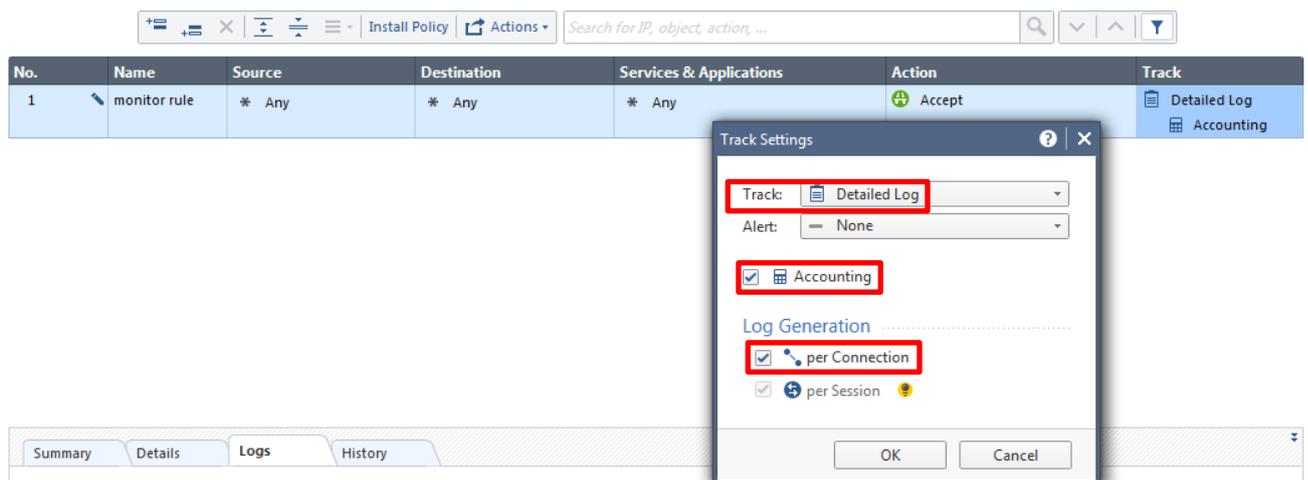
如果上述設定都確認過了，思考一下為何沒有 APCL & URLF Log？

更改規則的 Log 設定並且 install policy

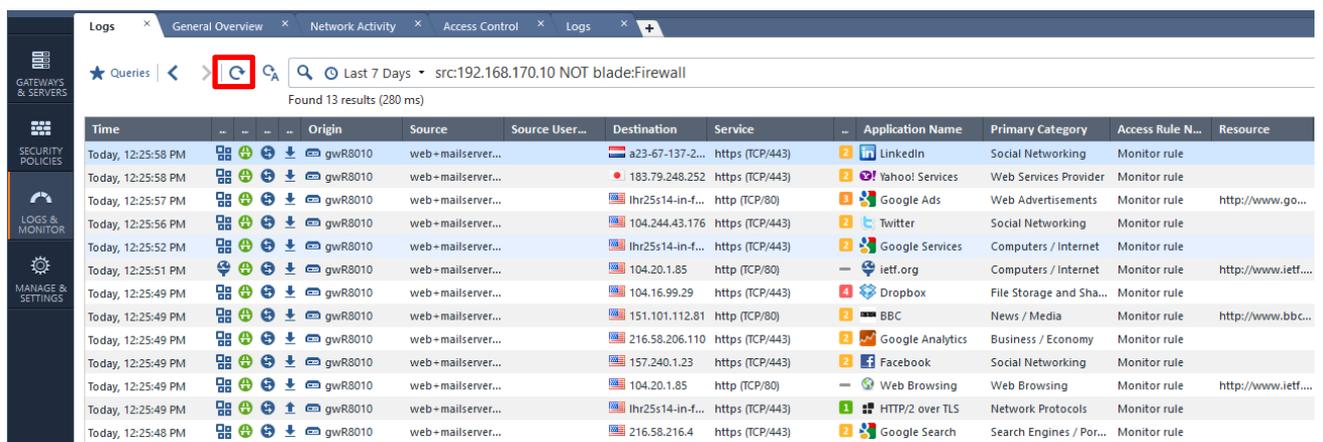
在 Track 欄位上按右鍵選擇「More...」：



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？



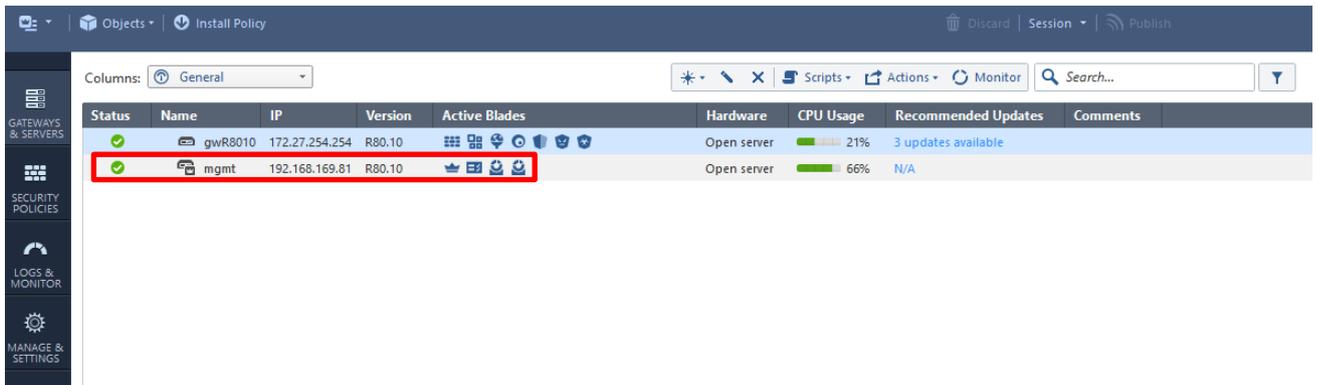
如果可以看到 APCL & URLF Log，思考一下為何同一條規則調整 Log 設定後顯示的內容不同？

比較一下 HTTP 和 HTTPS 的 Log 有什麼差別？

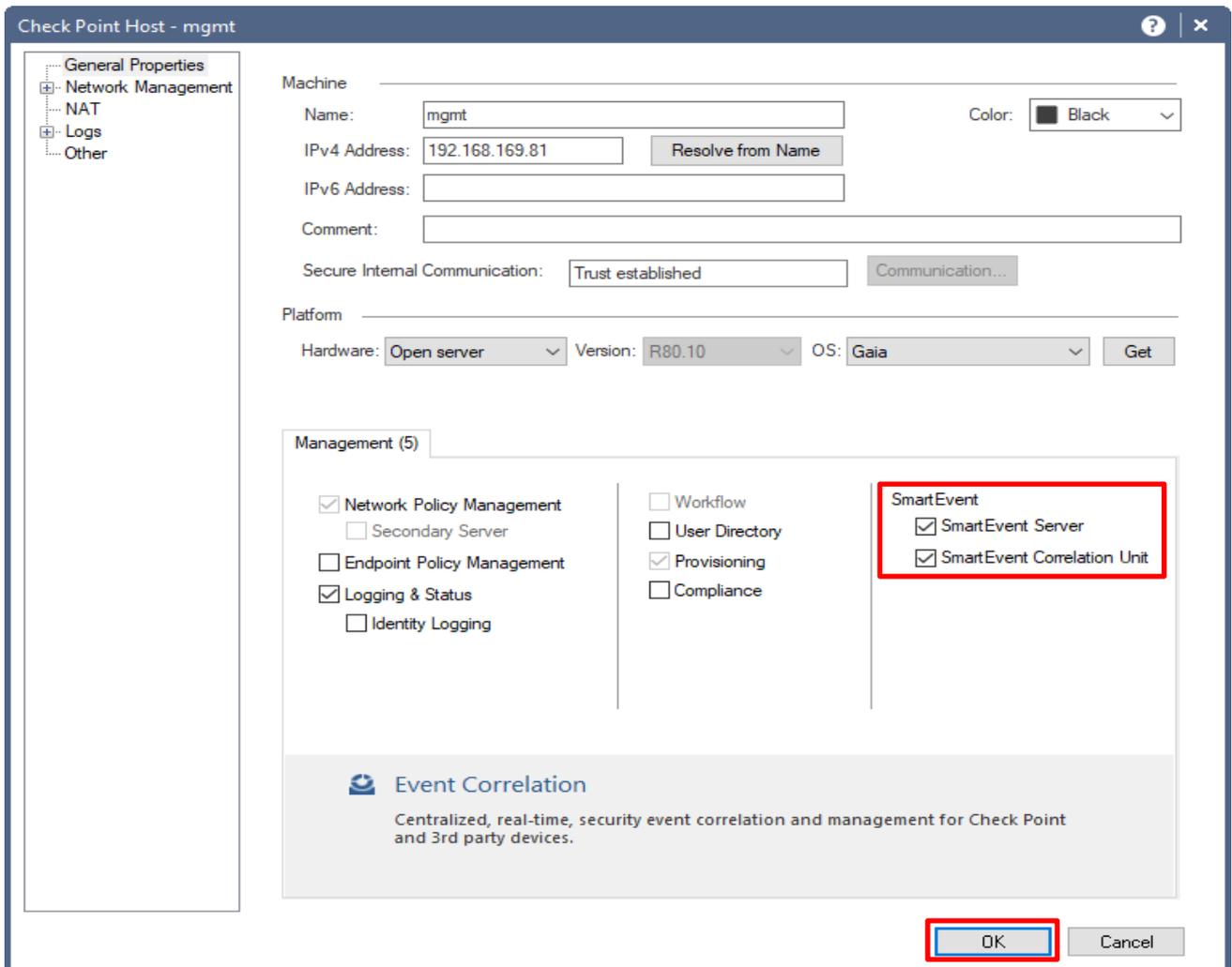
使用 Logs & Monitor 來產生 APCL & URLF 使用報表

依照以下的做法來開啟 SmartEvent 報表功能：

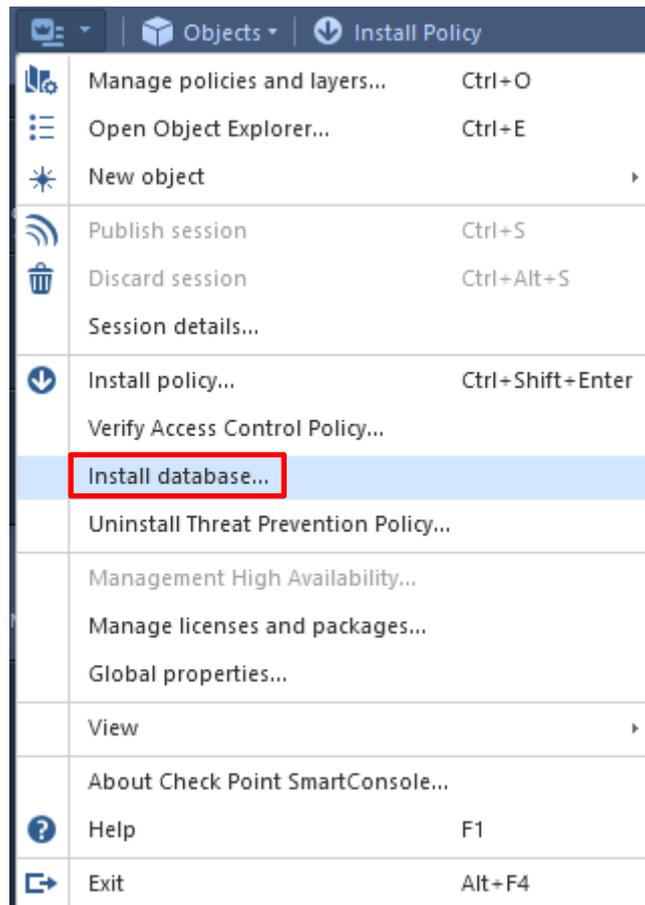
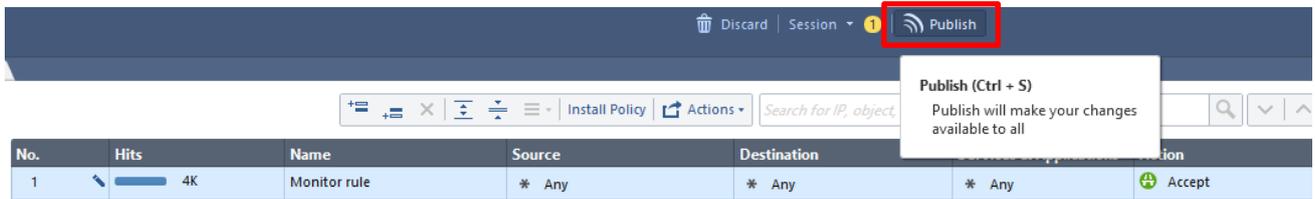
- 在管理主機 SMS 上啟用 SmartEvent and the Correlation Unit 功能
 - 切換到 Gateway & Servers 頁籤，在 mgmt 物件上連點 2 下開啟 SMS 管理主機物件



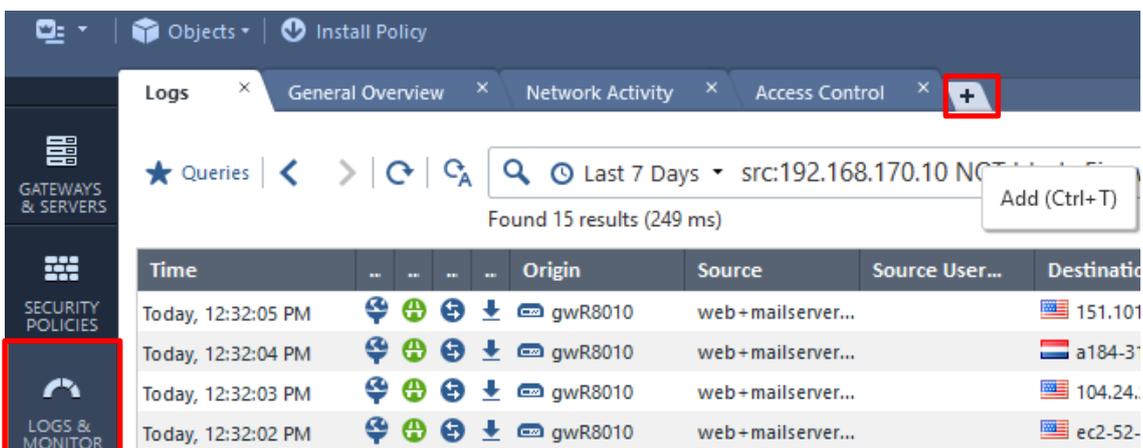
- 在 mgmt 物件中勾選「SmartEvent Server」以及「SmartEvent Correlation Unit」並點選 OK。



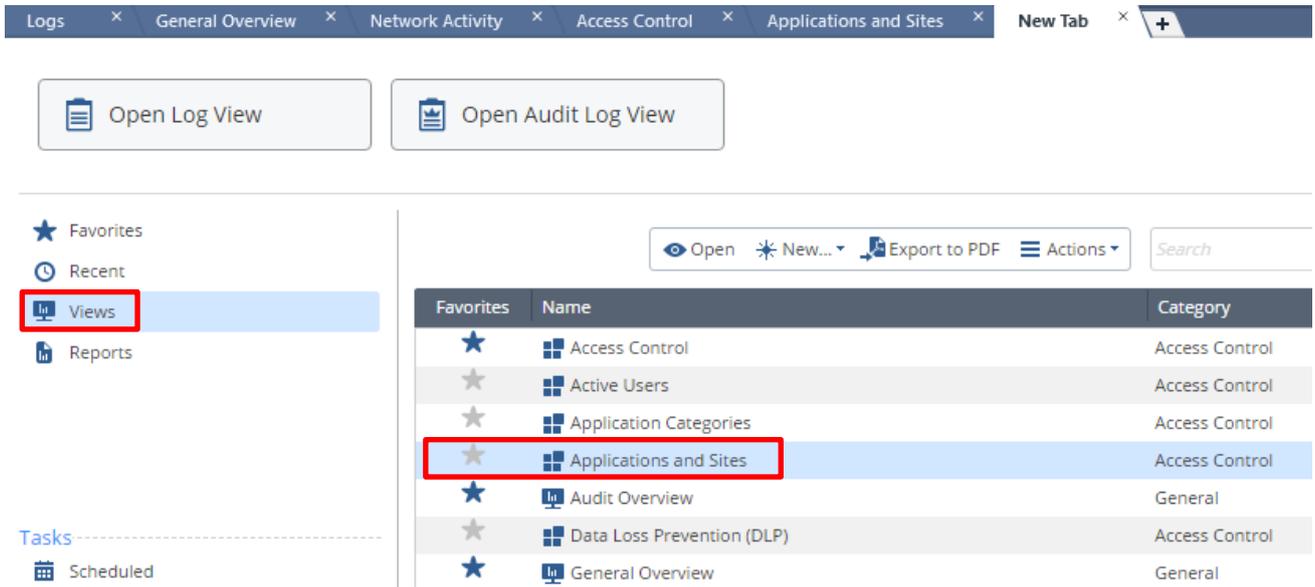
- 將設定「Publish」並且「Install Database」



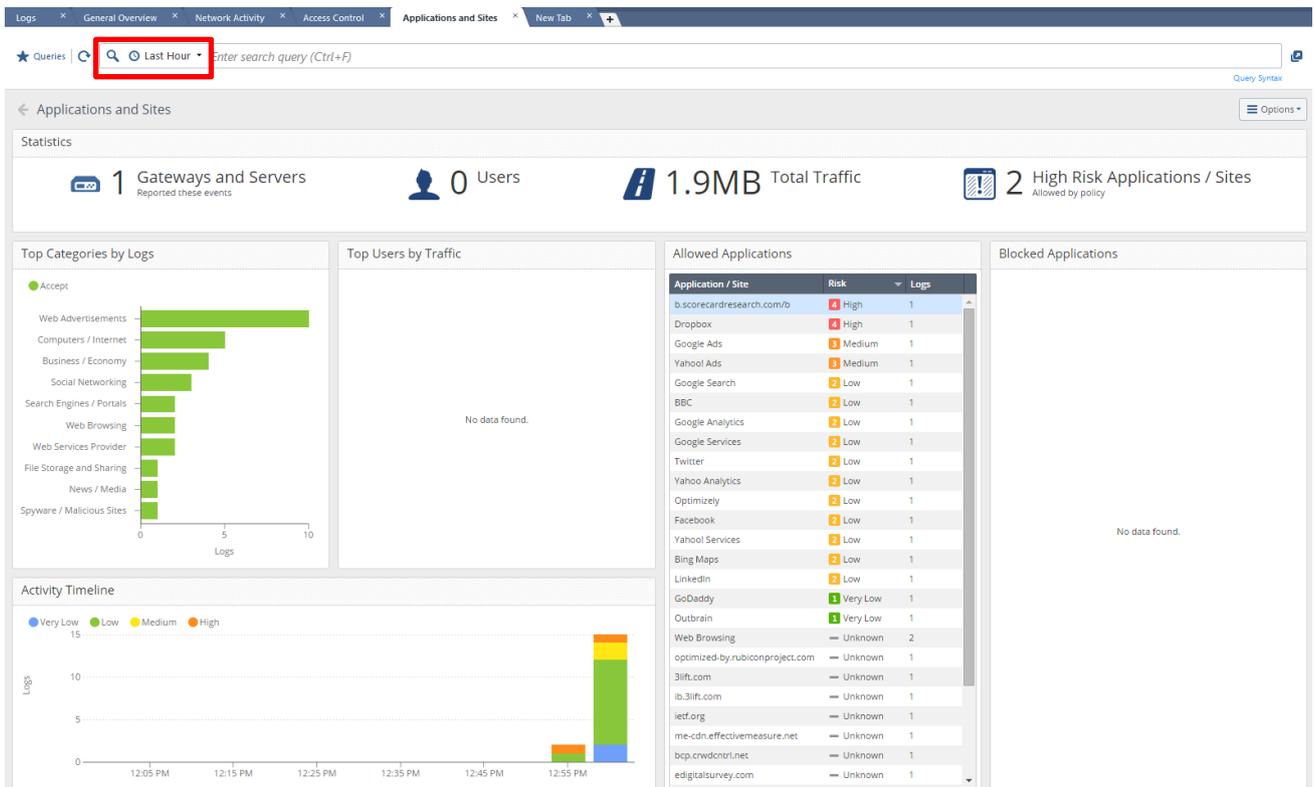
- 檢視 Views : Applications and Sites
 - 待 Install database 結束，切換到 Logs & Monitor > 頁籤，點選右上角的「+」開啟新分頁。



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

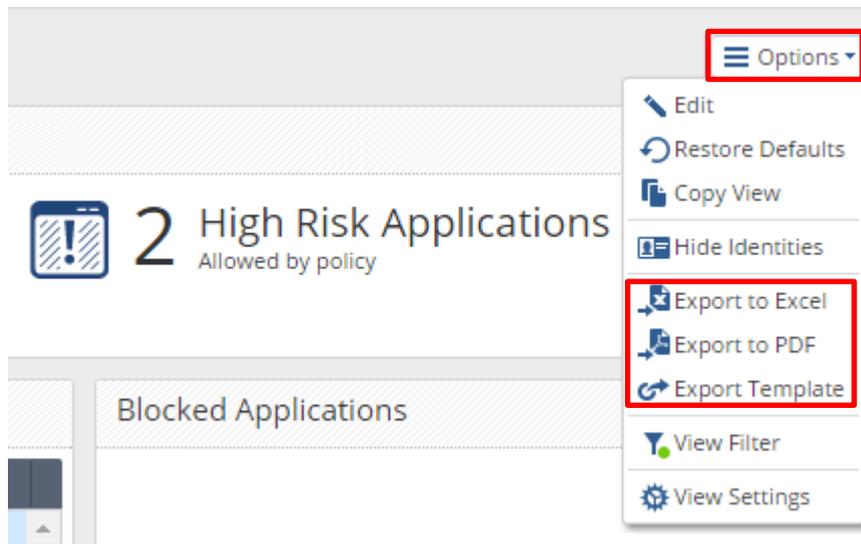


- 切換上方時間到“Last Hour” 並重整報表，會看到如下圖的畫面

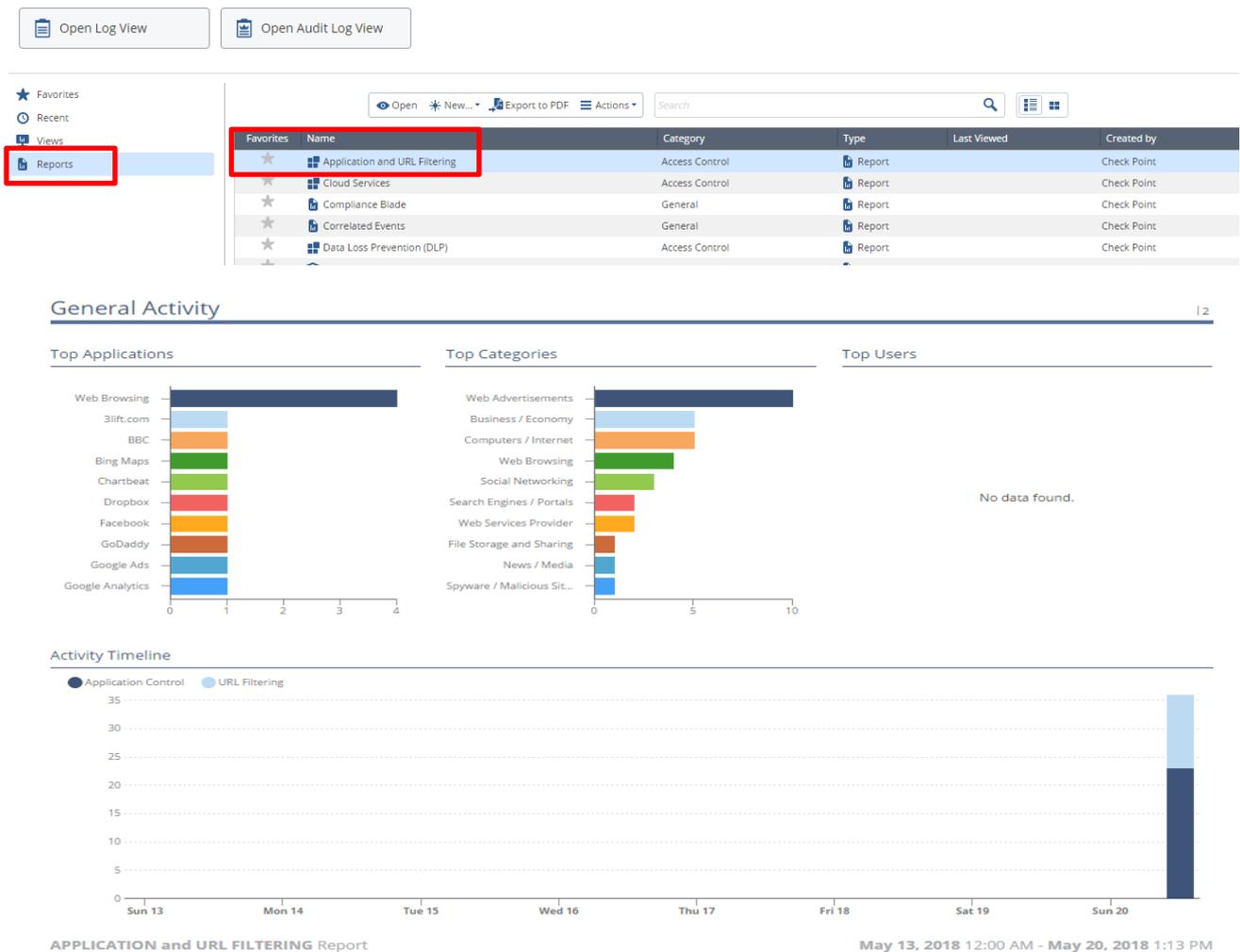


Generate a report

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

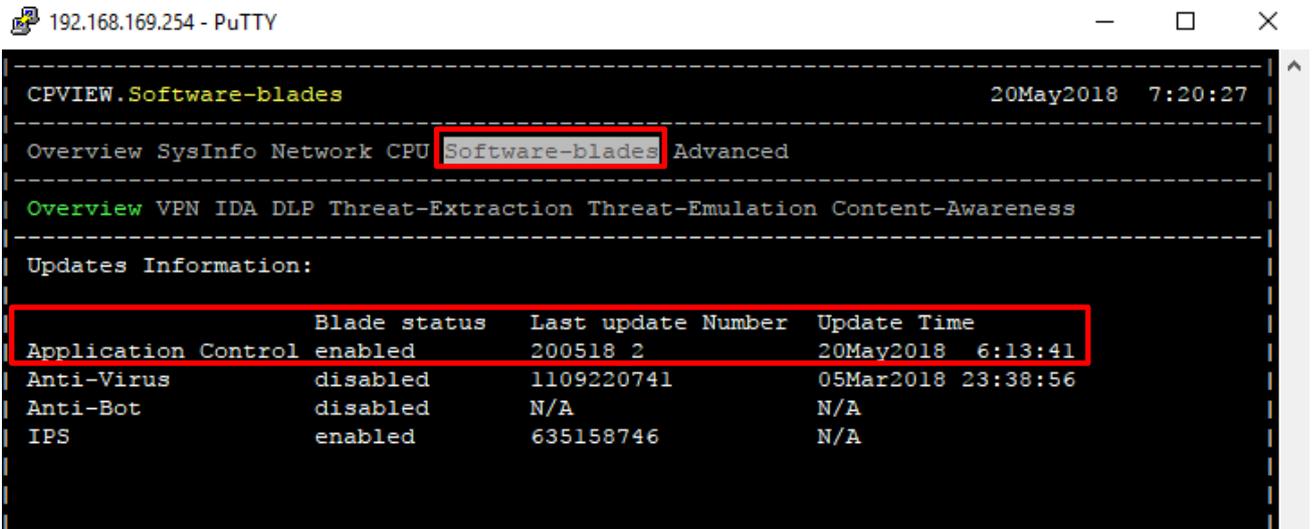
使用桌面 R80.10 Training 資料夾中的 Putty 連線一個 SSH session 到 gateway 上並執行「cpview」：

```
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
```

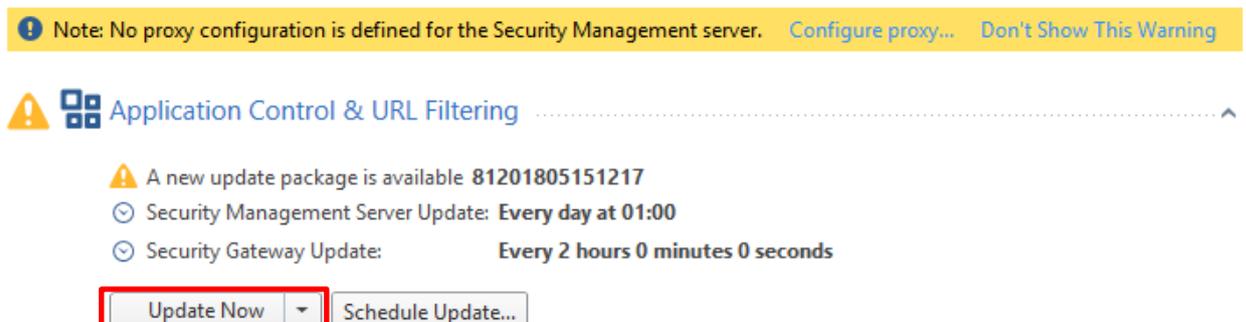
使用鍵盤的方向鍵切換 View 到「Software-blades」頁籤，檢視有開啟哪些功能以及是否有 Update：



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：

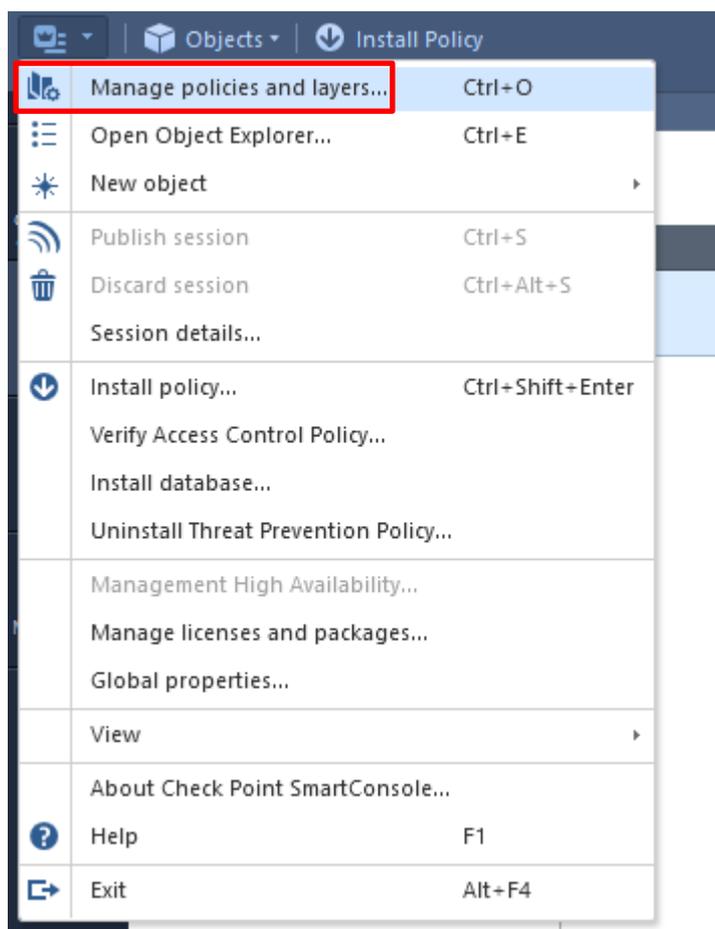


Lab 2: 了解 Content Awareness 以及 Inline Layer 的運作

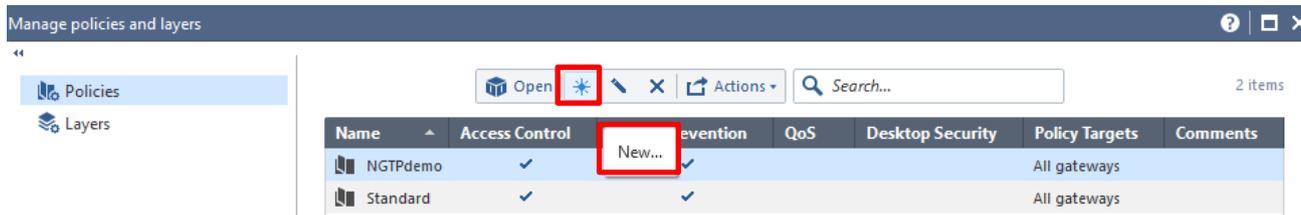
目標先建立一個新的 Policy Package 「SimplePolicy」 如下圖所示：

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	Parent 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

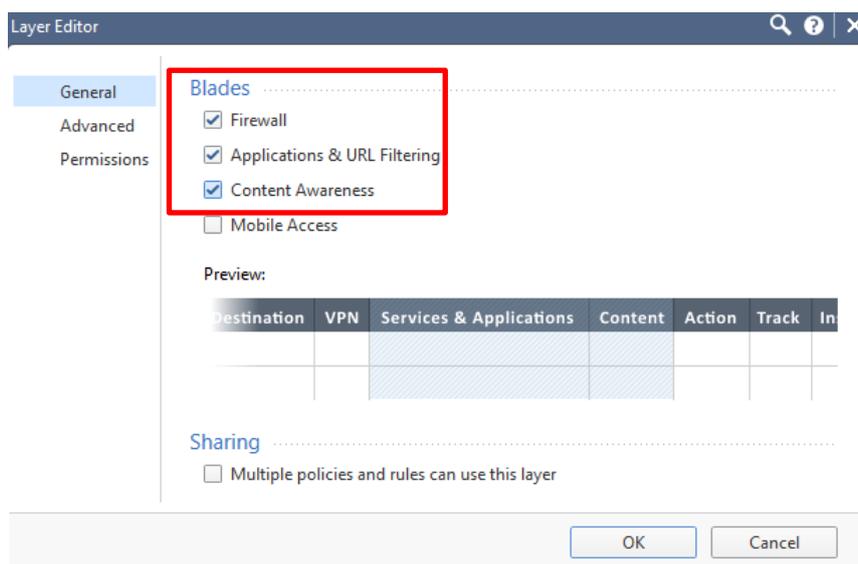
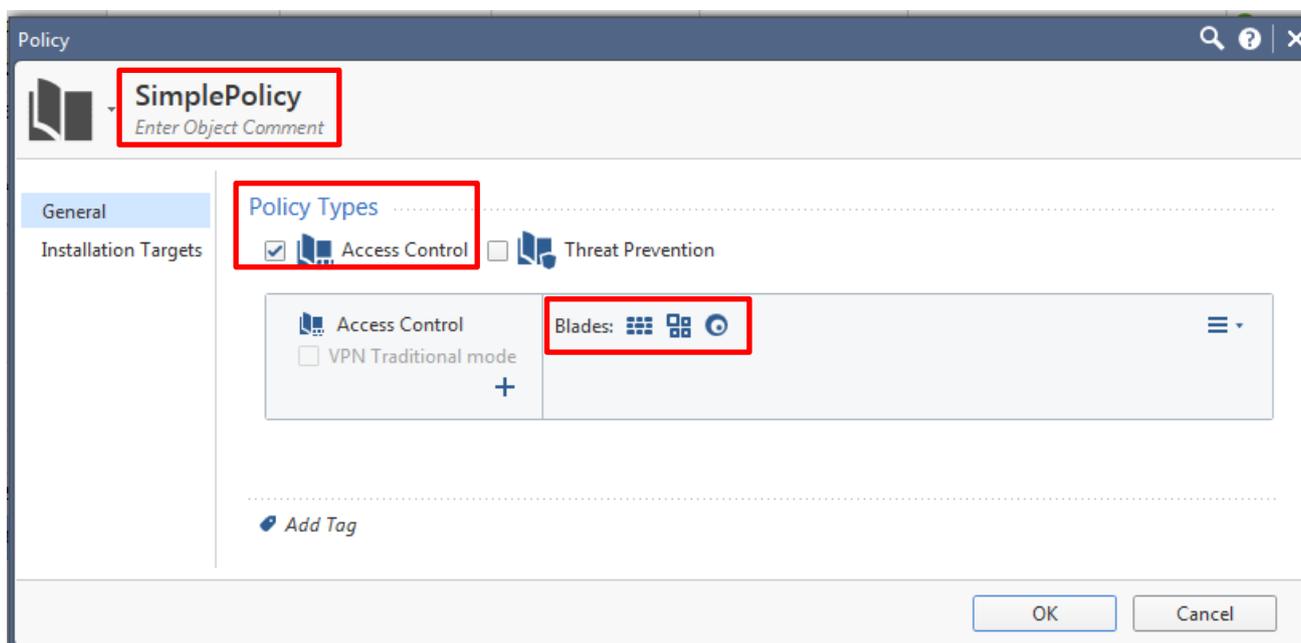
點選左上角下拉式選單中的「Manage policies and layers...」：



點選「New」建立新的 Policy Package ：



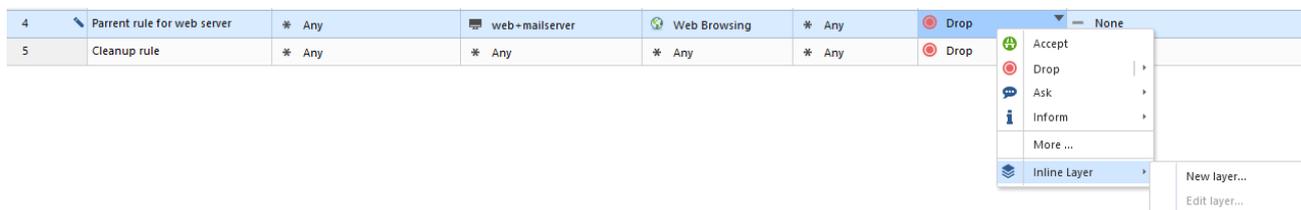
Policy 名稱為「SimplePolicy」、只勾選「Access Control」並勾選啟用「Firewall」、「Applications & URL Filtering」以及「Content Awareness」：



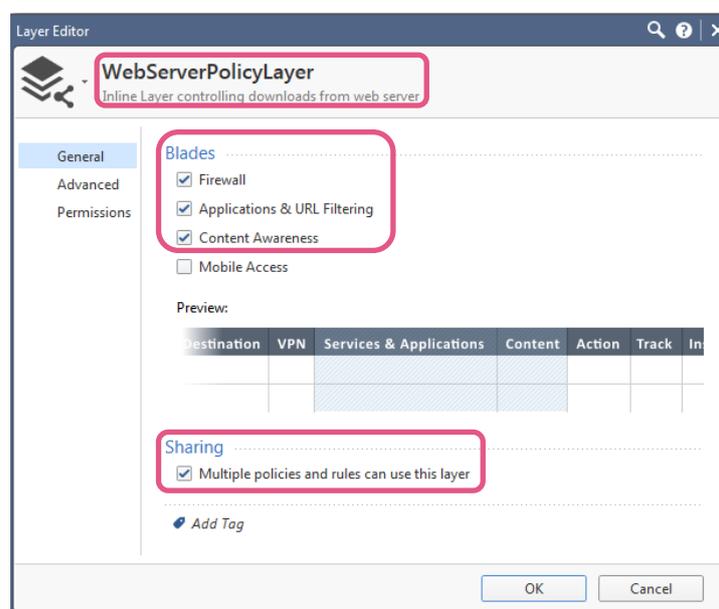
接下來依照 Lab-1 一開始的附圖新增規則。

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：

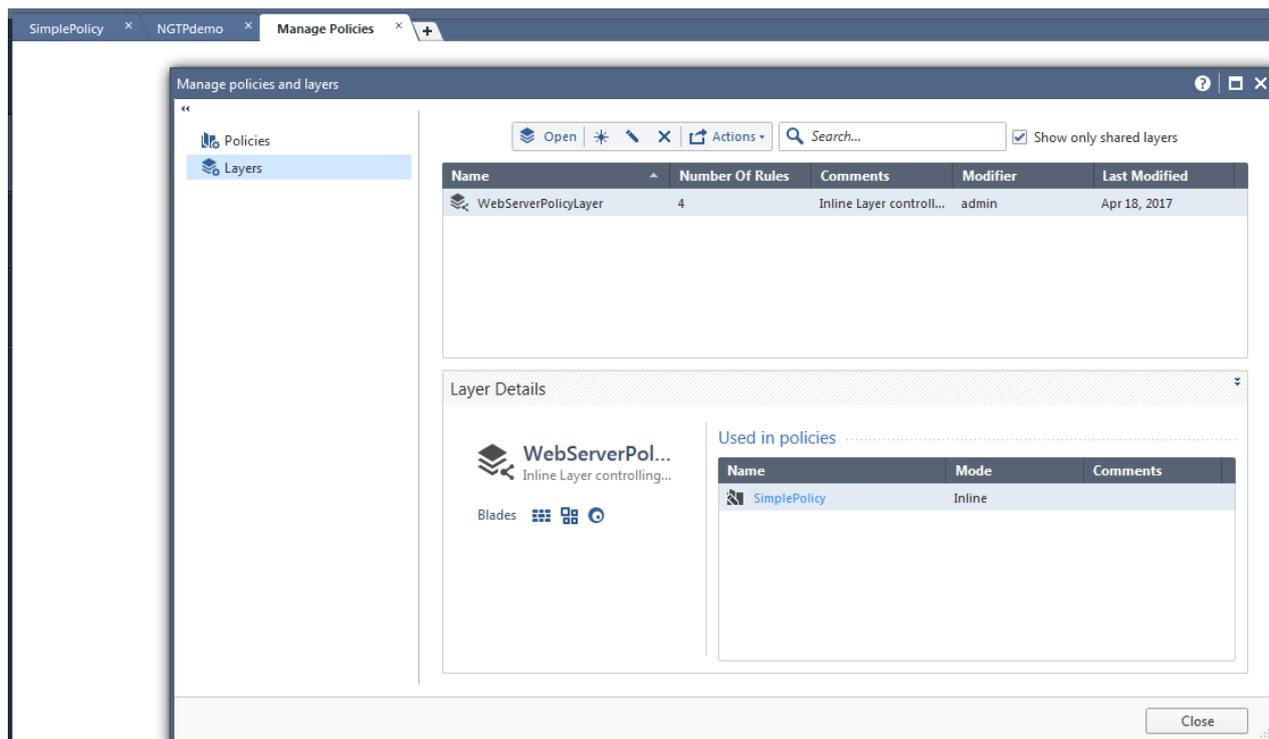
Option Lab：嘗試建立一個新的 User Profile 以及 User 帳號，設定只能編輯該 Inline Layer 而不能更改整個 Policy Layer，並使用該 User 登入看看畫面有什麼不一樣：



完成後的 Inline Layer Policies 如下圖：

4	Parent rule for web server	* Any	web-mailserver	Web Browsing	* Any	WebServerPolicyLaye	N/A
4.1	Credit 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：

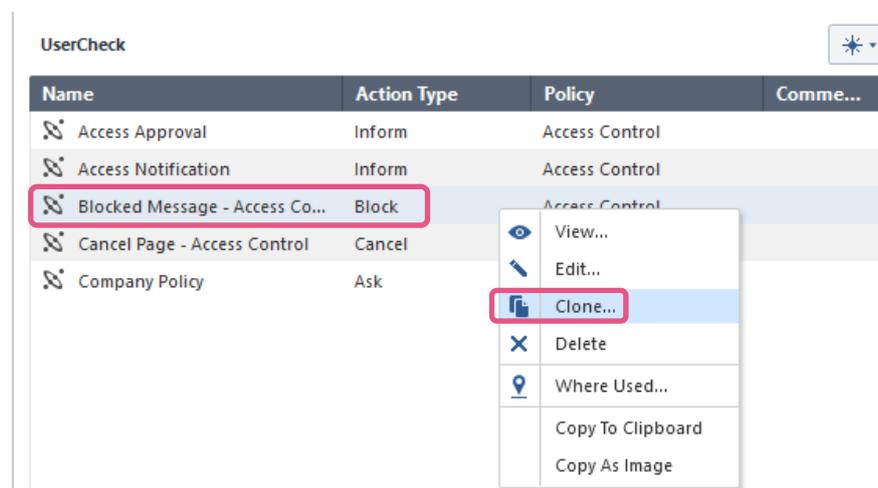


建立 Content Awareness 的阻檔頁面

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：

The screenshot shows the Check Point Gateway & Servers interface. At the top, a table lists gateways. The gateway 'gwR8010' is highlighted, and its configuration window is open below.

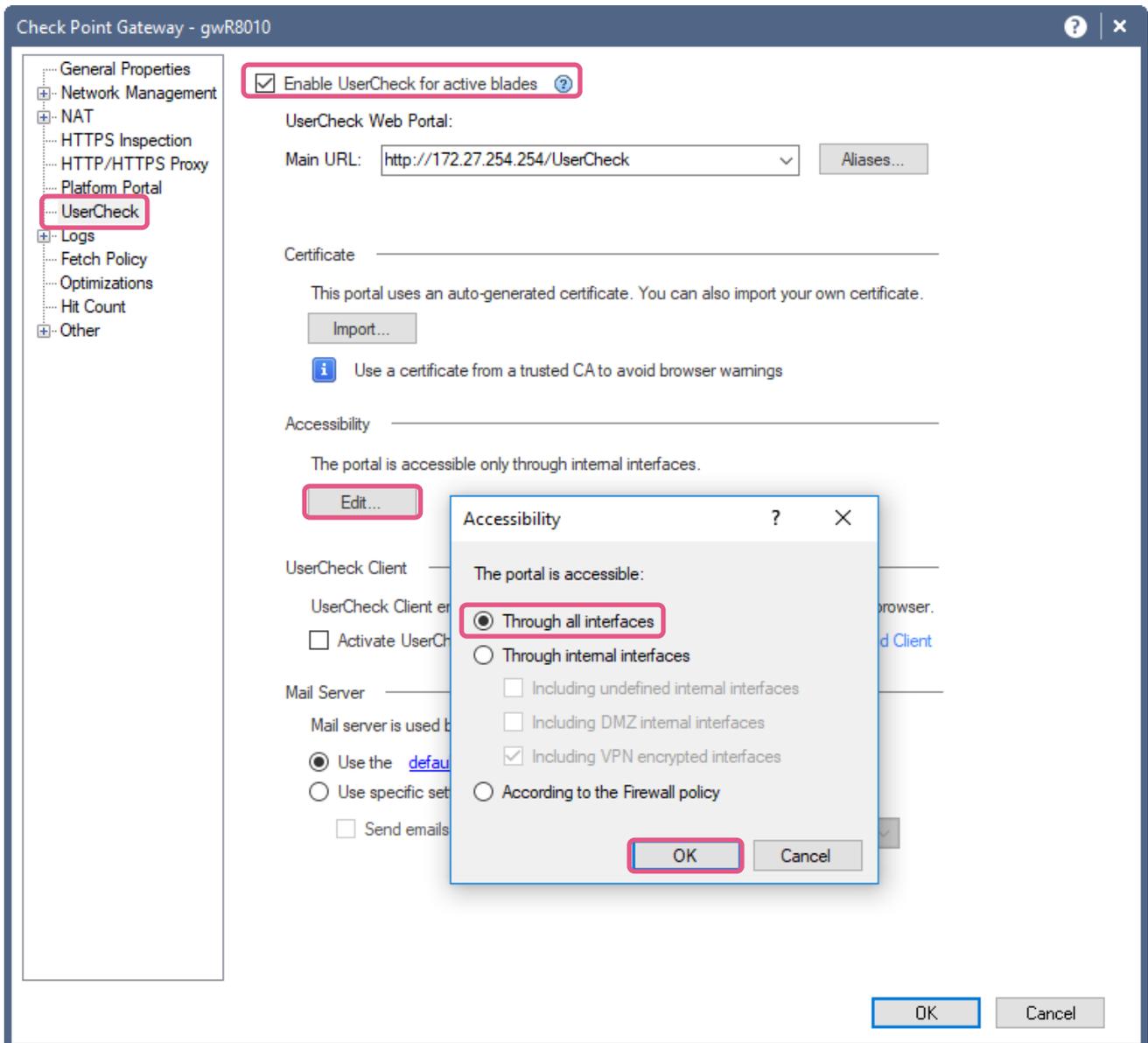
Status	Name	IP	Version	Active Blades
✓	gwR8010	172.27.254.254	R80.10	[Grid] [Grid] [Lightbulb] [Refresh]
✓	mgmt	192.168.169.81	R80.10	[Crown] [List] [Refresh] [Refresh]

The configuration window for 'gwR8010' shows the following settings:

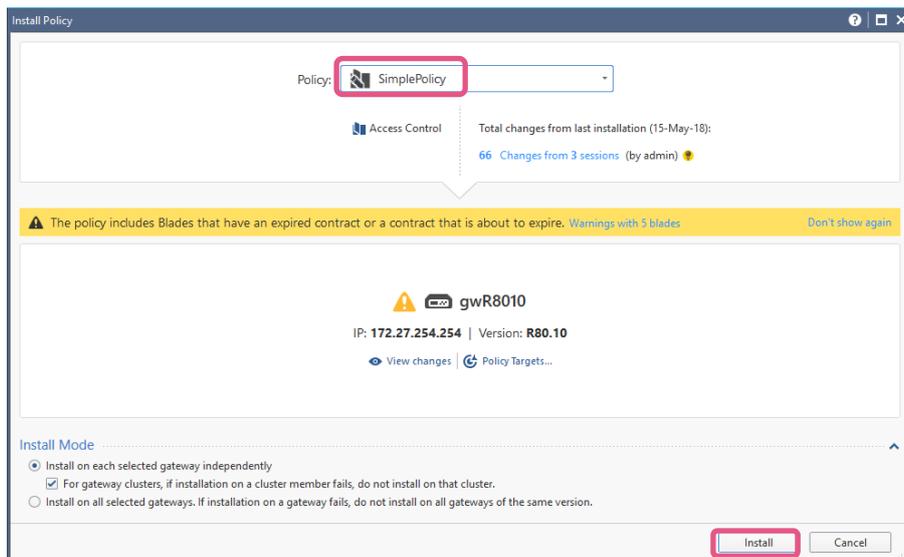
- Machine:** Name: gwR8010, Color: Black, IPv4 Address: 172.27.254.254, IPv6 Address: (empty), Comment: (empty), Secure Internal Communication: Trust established.
- Platform:** Hardware: Open server, Version: R80.10, OS: Gaia.
- Network Security (4):**
 - Firewall
 - IPSec VPN
 - Mobile Access
 - Application Control
 - URL Filtering
 - Data Loss Prevention
 - IPS
 - Anti-Bot
 - Anti-Virus
 - Threat Emulation
 - Threat Extraction
 - Anti-Spam & Email Security
 - Identity Awareness
 - Content Awareness
- Advanced Networking & Clustering:**
 - Dynamic Routing
 - SecureXL
 - QoS
 - Monitoring

At the bottom, there is a section for 'Traditional Anti-Virus' with the text: 'Leading Anti-Virus protection including heuristic virus analysis.'

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」：



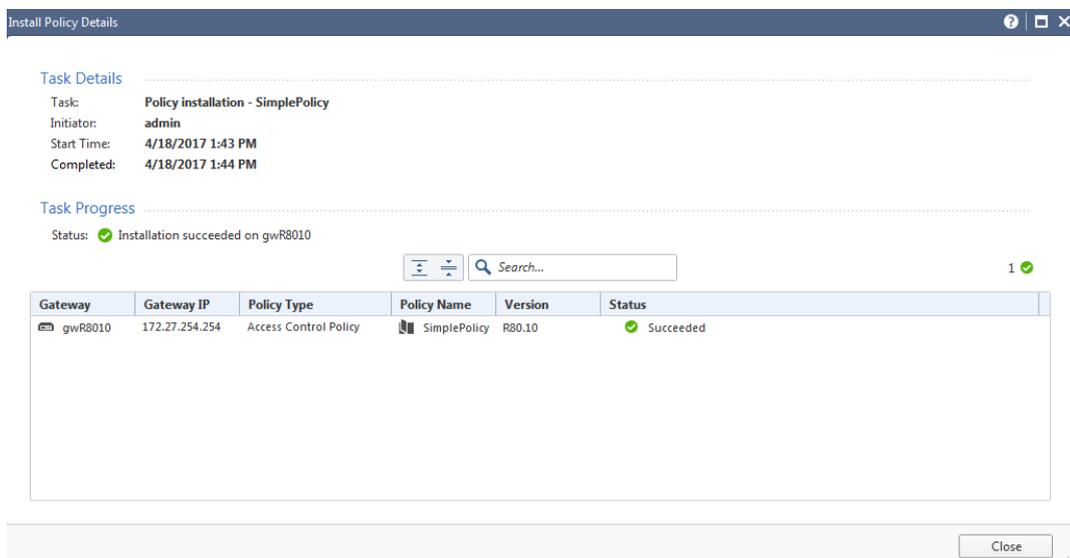
設定完成之後，點選「Publish」並「Install Policy」：



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：

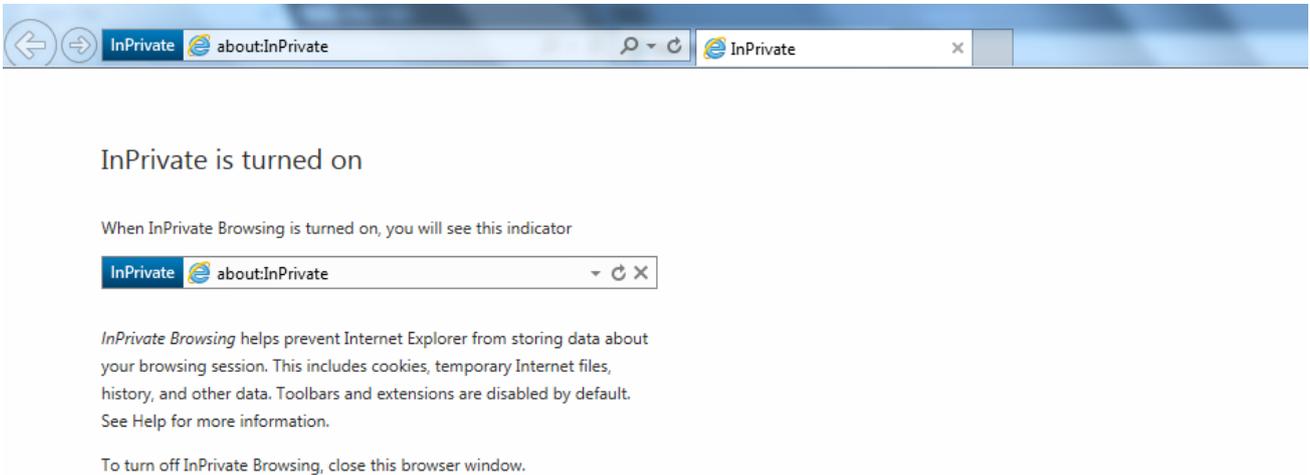


等待 Policy 成功完成派送之後，即可繼續進行 Lab 測試：

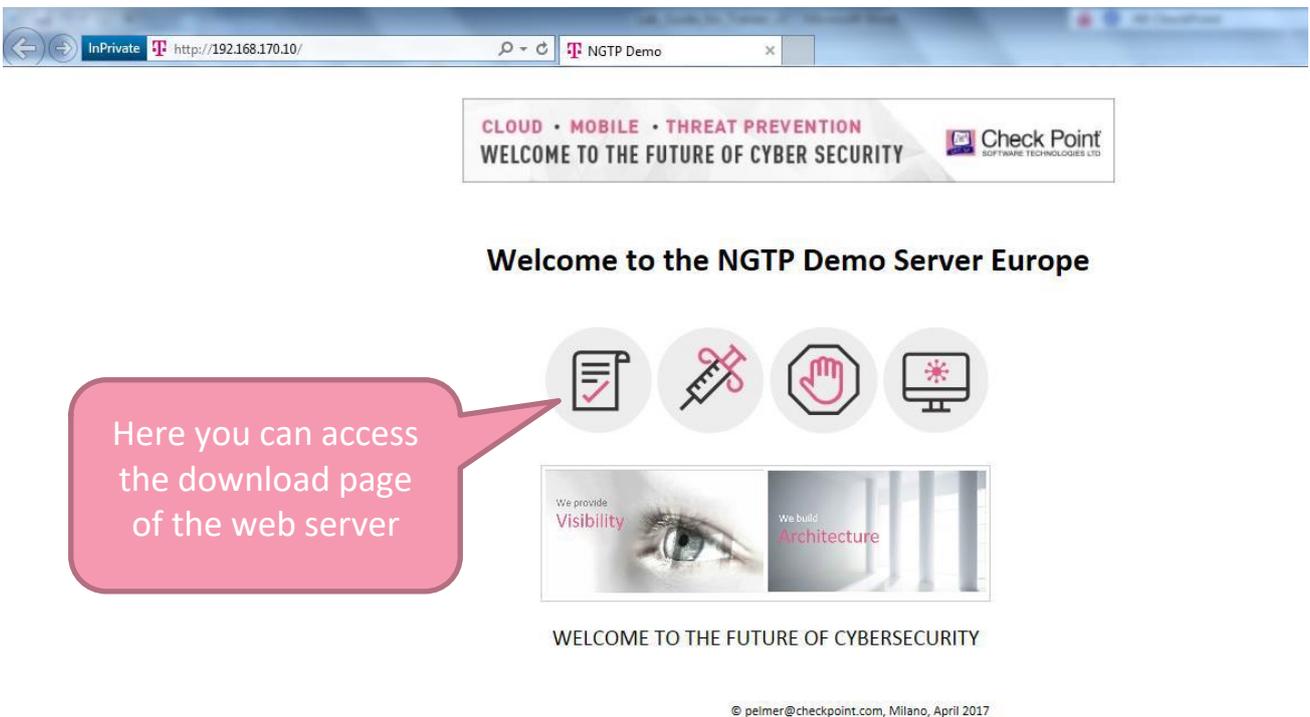


使用瀏覽器的 private mode 開啟 Web Server 網頁進行測試

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)

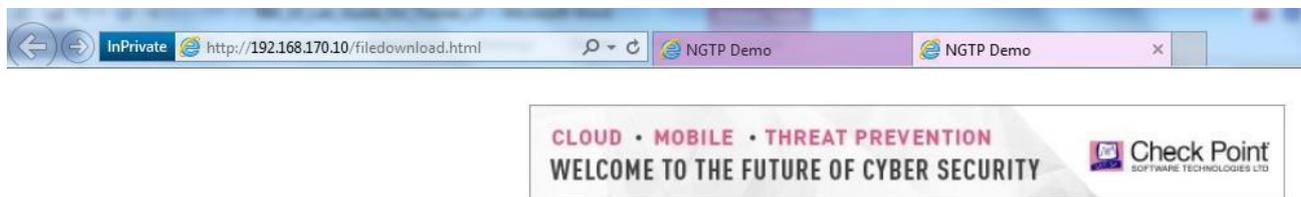


連線到 Web Server 進行測試

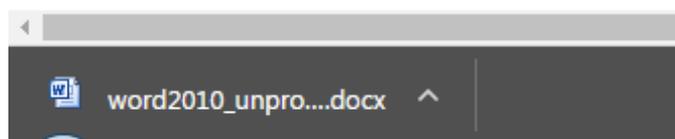


嘗試從 Web Server 下載 Word、Excel、TXT 等各個檔案並產生相關的 Log

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：

Log Details
Accept
http Traffic Accepted from 192.168.169.1 to ContentDemo(192.168.170.10)

Details | Matched Rules | Files

Log Info

- Origin: gwR8010
- Time: Today, 14:04:42
- Blade: Application Control, Content Awareness
- Product Family: Access
- Type: Session

Application / Site

- Application Name: ContentDemo
- Primary Category: Custom Application/Site
- Additional Categor...: Custom Application/Site, Medium Risk
- Application Risk: Medium
- Client Type: Google Chrome

File Operation

- Data Type: Document File

Policy

- Action: Accept
- Policy Management: mgnt
- Policy Name: SimplePolicy
- Policy Date: Today, 13:56:04
- Layer Name: WebServerPolicyLayer
- Access Rule Name: Documents
- Access Rule Numb...: 4.2

Accounting

- Packets: 57
- Browse Time: 00h 00m 29s
- Bytes (sent\receive...): 47.9 KB (1.3 KB \ 46.7 KB)
- Client Inbound Pa...: 21
- Client Outbound ...: 36
- Server Inbound Pa...: 36
- Server Outbound ...: 21
- Client Inbound By...: 1.3 KB

注意到檔案名稱會顯示在 Log Details 的「Files」頁籤中：

Log Details
Accept
http Traffic Accepted from 192.168.169.1 to ContentDemo(192.168.170.10)

Details | Matched Rules | **Files**

Current Session | Found 1 results (52 ms) | Query Syntax

Time	File Name	File Direction	File Type	File Size	Archive...	Data Type	File ID
Today, 14:04:42	word2010_unprotected.docx	Download	Microsoft W...	44.9 KB		Document File	16777220

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：



欲使用的檔案內容已經被阻檔

根據公司的資安政策，您192.168.169.1目前所使用的檔案：creditcard.txt 資料內容：PCI - Credit Card Numbers 不被允許傳送。

您目前的動作已被阻檔並且紀錄。

分類: General
Click [here](#) to report wrong category

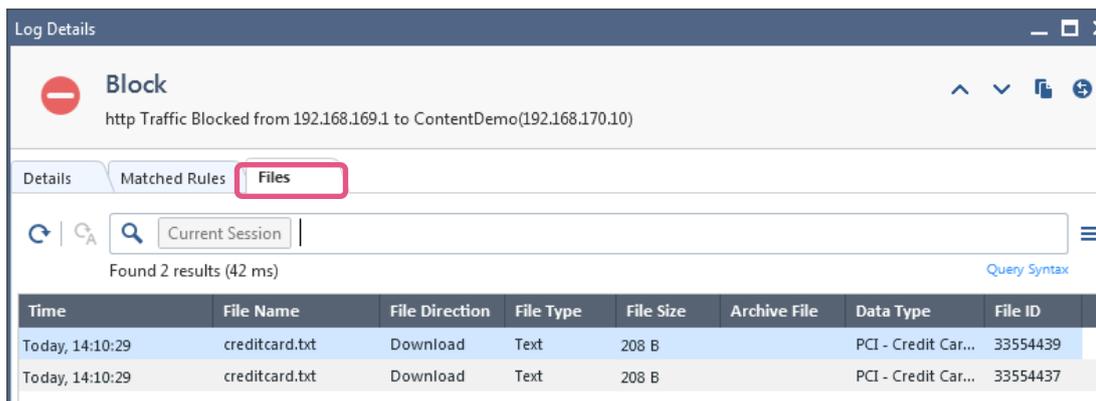
有任何問題，請連絡公司Help Desk協助並提供以下的資訊：

Reference: 5E231B02

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

Time	Action	Source	Destination	Port	Category
Today, 14:10:29	Accept	192.168.169.1	web-mailserver...	http (TCP/80)	Cleanup rule
Today, 14:10:29	Block	192.168.169.1	web-mailserver...	http (TCP/80)	Credit Card Numbers
Today, 14:10:24	Accept	192.168.169.1	web-mailserver...	http (TCP/80)	Spreadsheets
Today, 14:10:24	Redirect	192.168.169.1	web-mailserver...	http (TCP/80)	Credit Card Numbers



Log Details

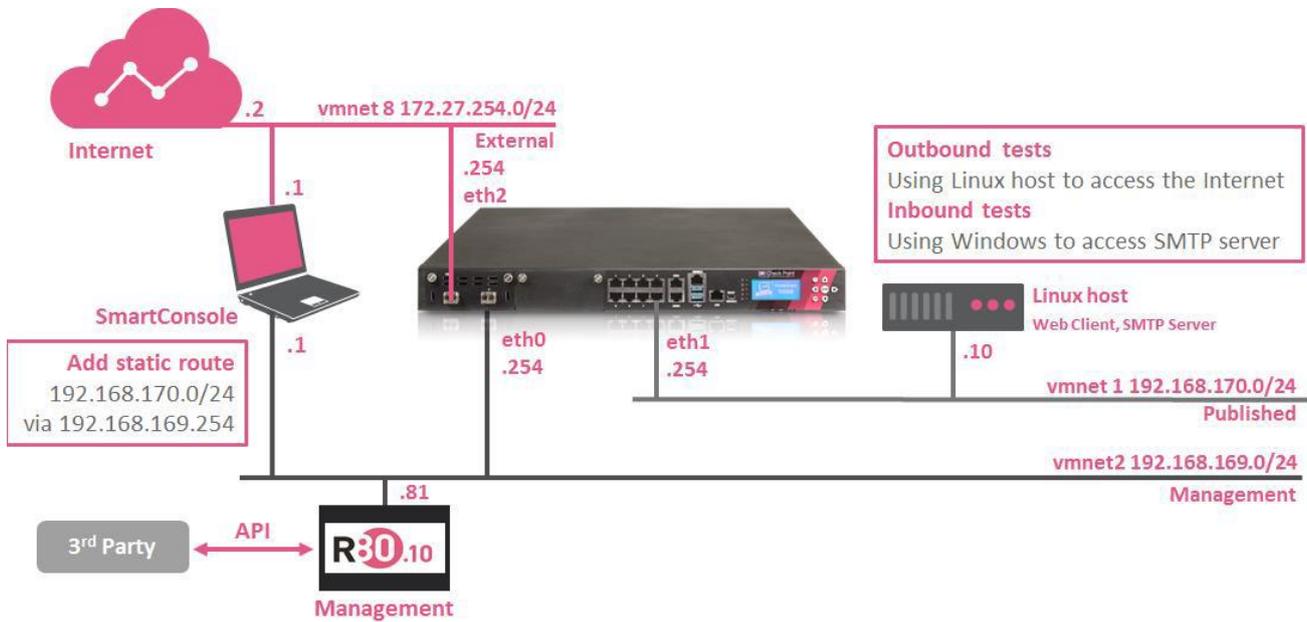
Block
http Traffic Blocked from 192.168.169.1 to ContentDemo(192.168.170.10)

Details | Matched Rules | **Files**

Current Session | Found 2 results (42 ms) | Query Syntax

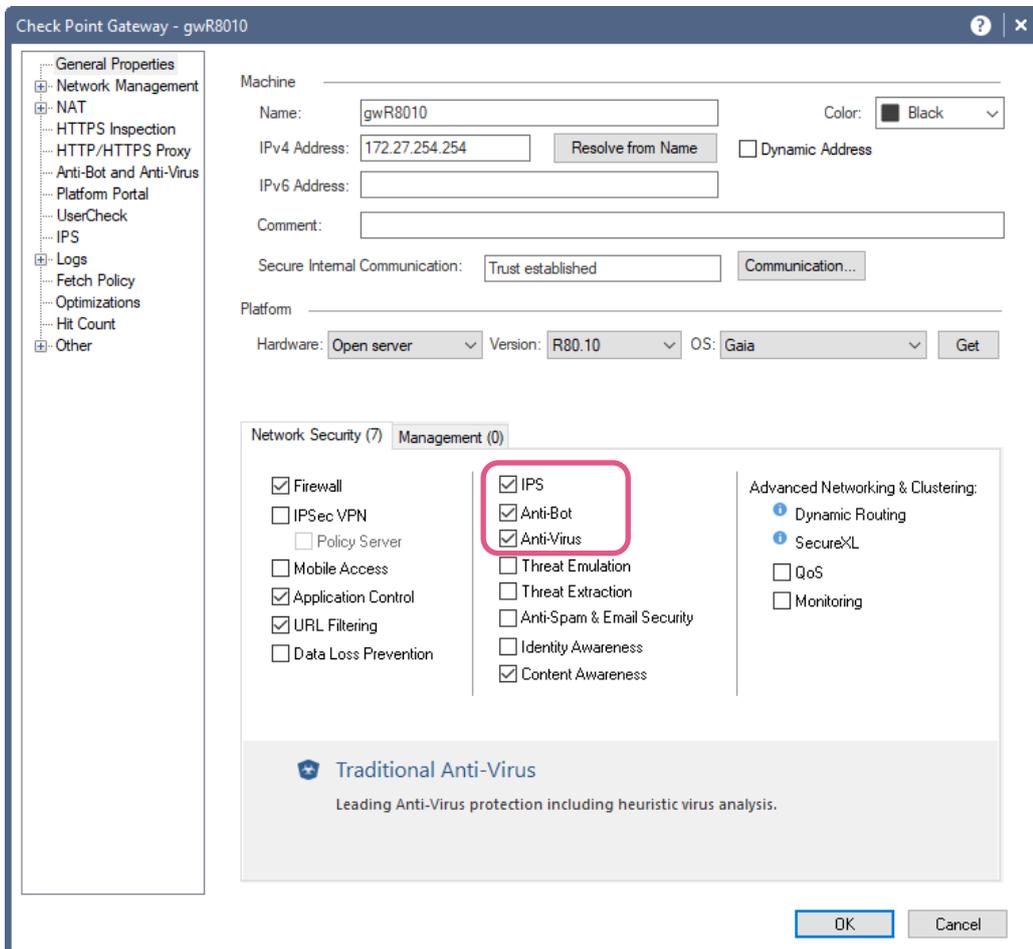
Time	File Name	File Direction	File Type	File Size	Archive File	Data Type	File ID
Today, 14:10:29	creditcard.txt	Download	Text	208 B		PCI - Credit Car...	33554439
Today, 14:10:29	creditcard.txt	Download	Text	208 B		PCI - Credit Car...	33554437

Lab 3: Threat Prevention

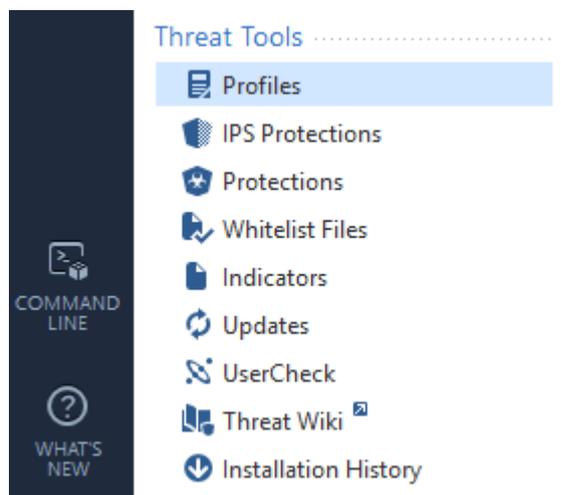


設定 Gateway 啟用 Threat Prevention 功能

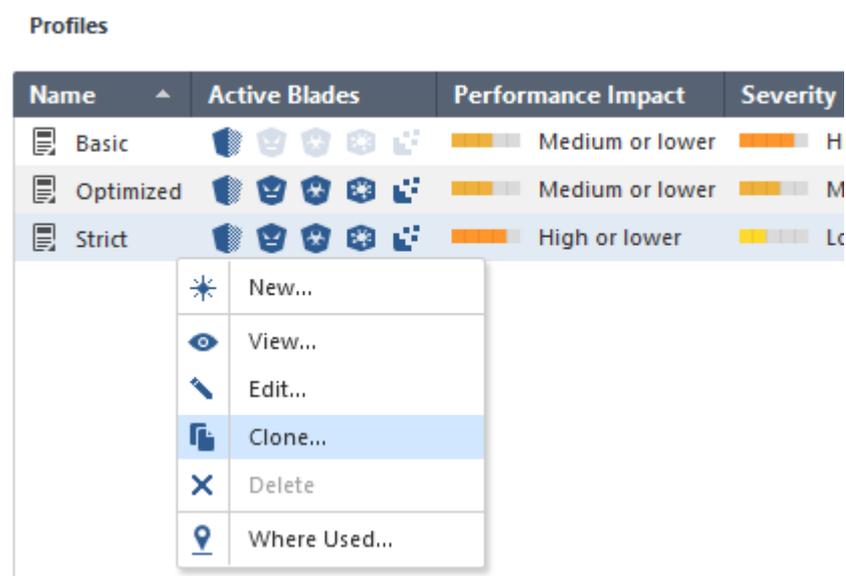
至 Gateways & Servers 頁籤，點選 Gateway 勾選 IPS、Anti-Bot 以及 Anti-Virus 功能：



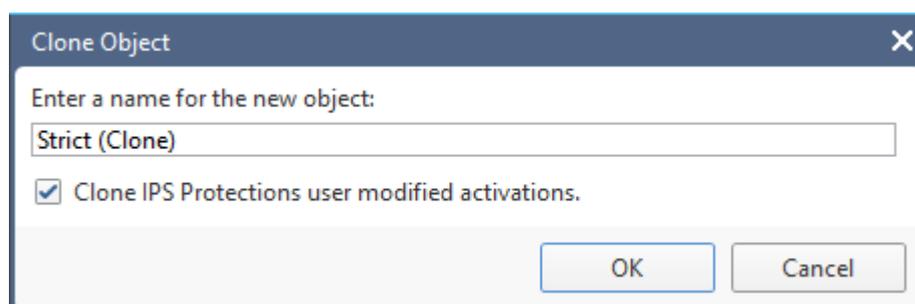
點選 Threat Prevention >> Policy，然後在左下角的 Threat Tools 點選「Profile」：



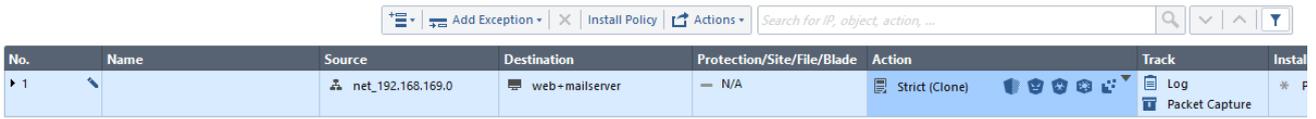
接下來在右邊的 Profile 中點選「Strict」然後按右鍵「Clone」：



按 OK 進行複製：

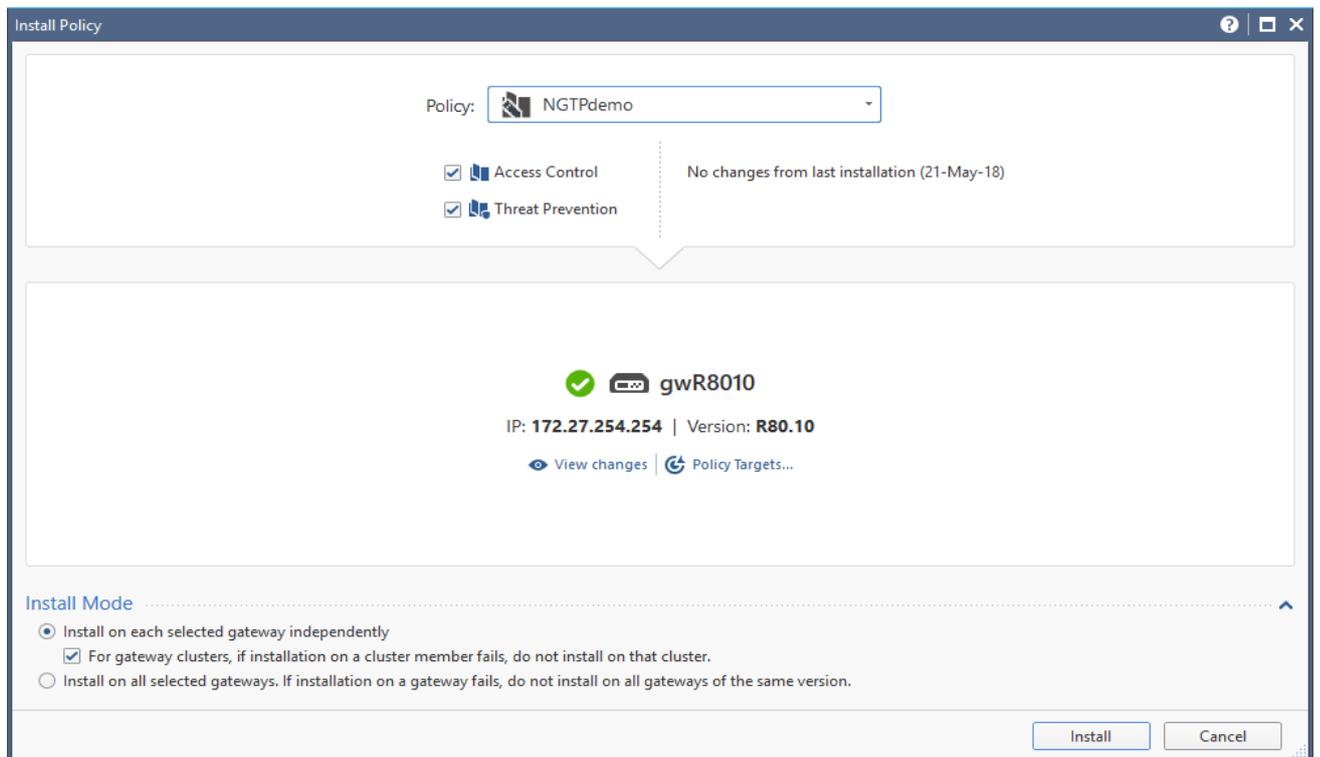
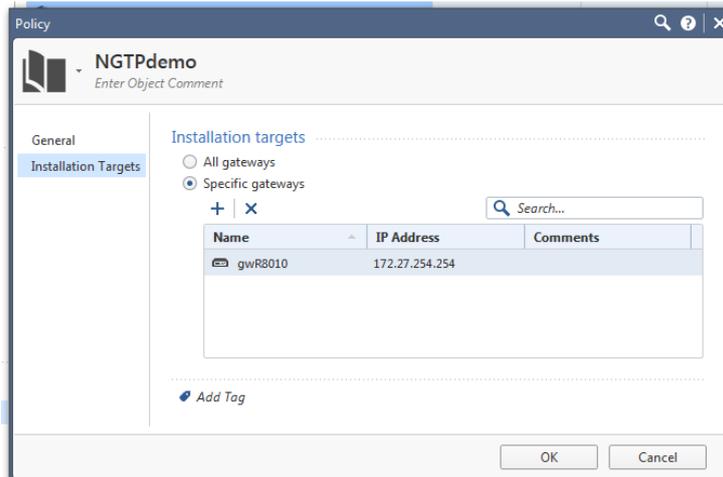


設定 Threat Prevention Policy 如下圖：



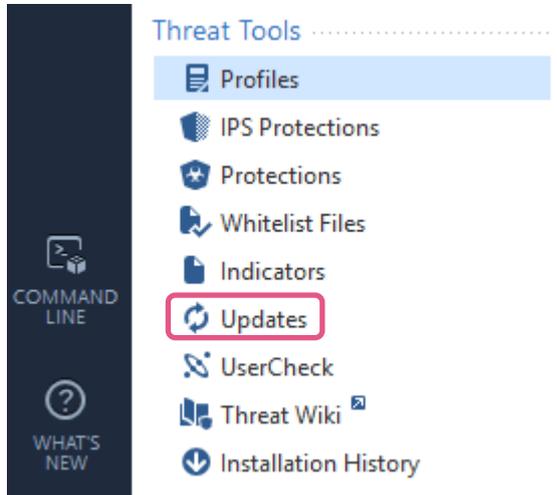
No.	Name	Source	Destination	Protection/Site/File/Blade	Action	Track	Instal
1		net_192.168.169.0	web+mailserver	N/A	Strict (Clone)	Log Packet Capture	*

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

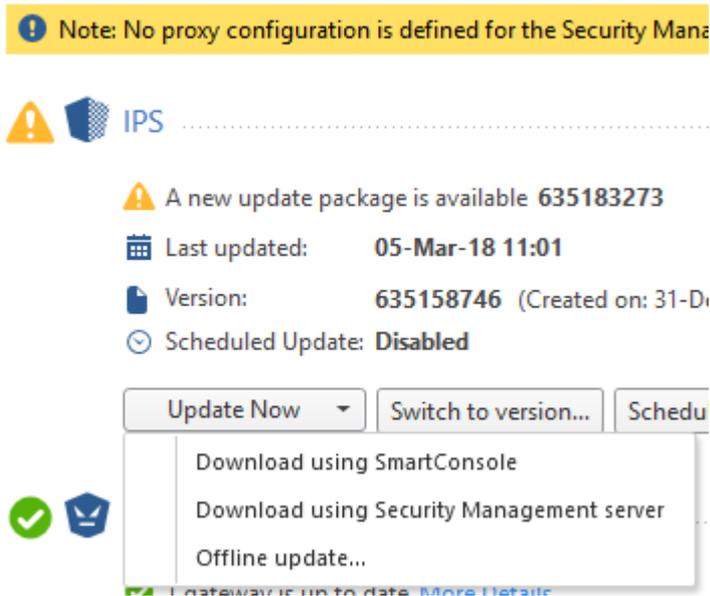


初次更新 Threat Prevention

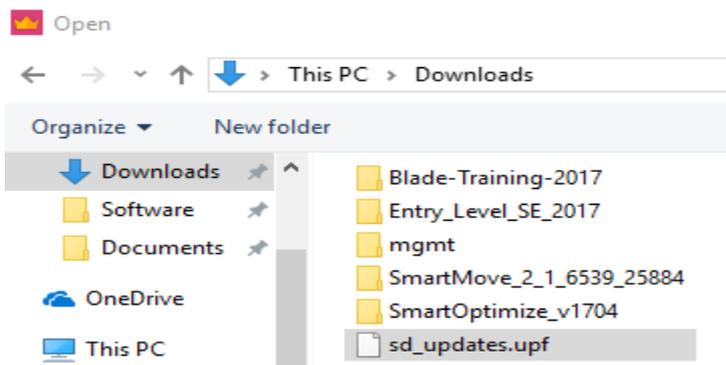
在左下角 Threat Tools 中點擊 Updates :



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...」：

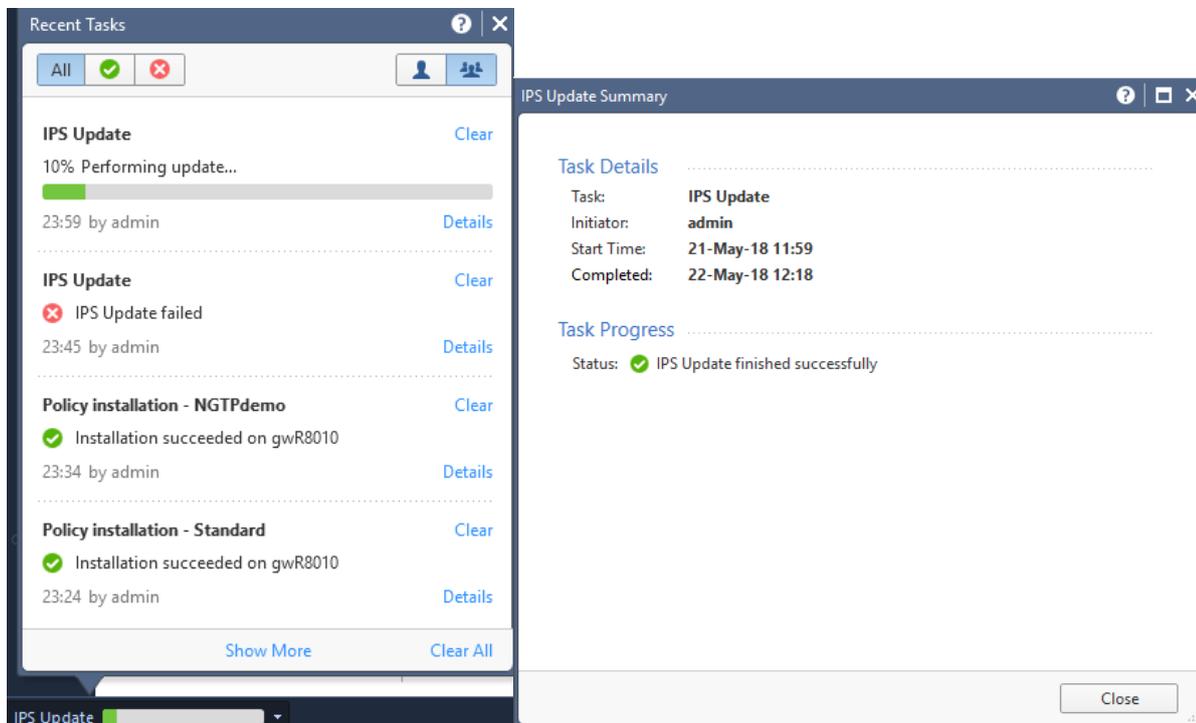


選擇 IPS offline update file 「sd_updates.upf」：

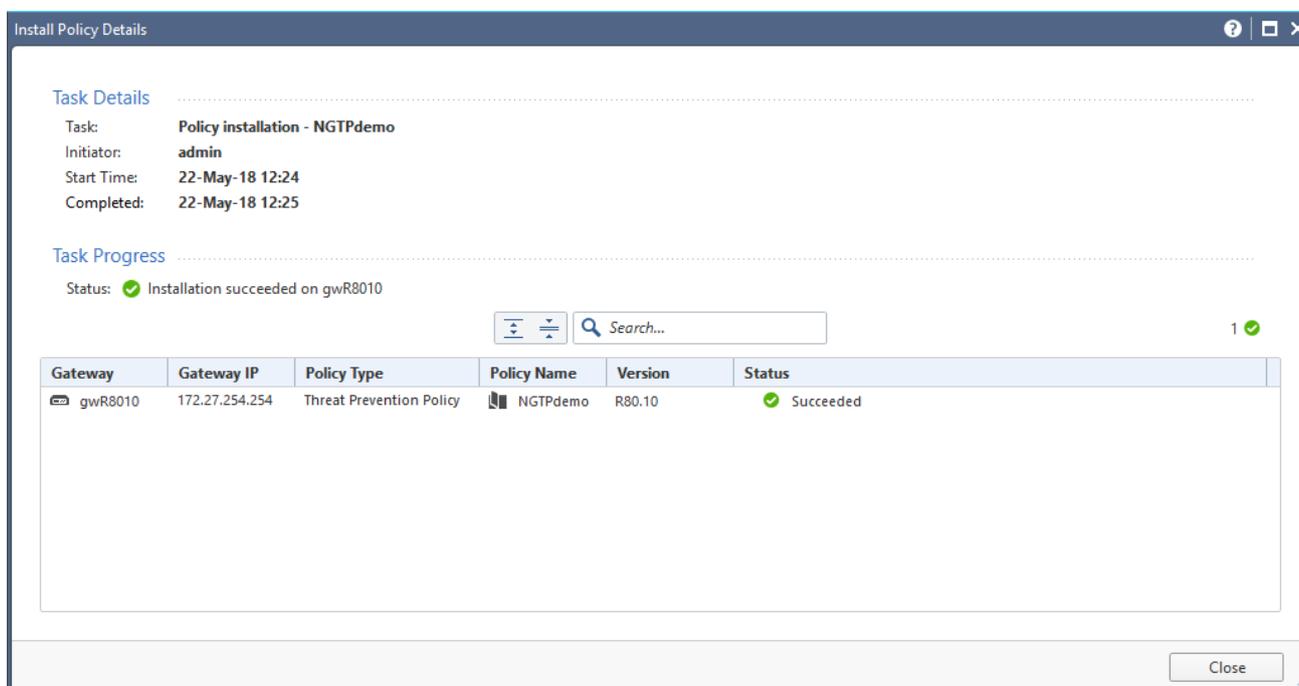


畫面左下角的 Recent Tasks 會顯示 IPS 更新的進度條，等待 IPS 更新完成：

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：

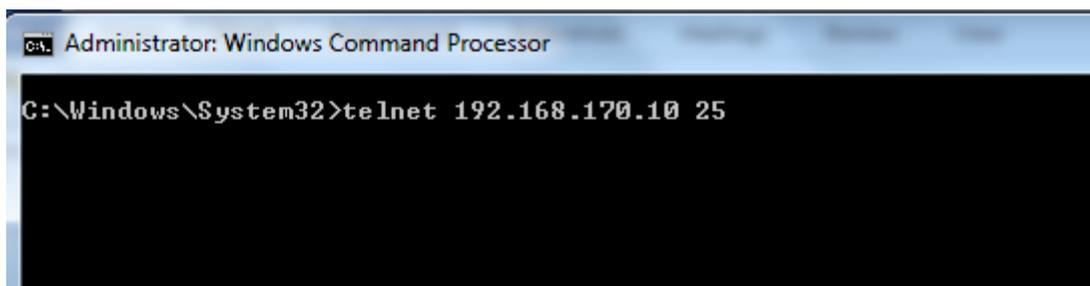


測試 IPS 的防釣魚郵件防禦功能

接下來我們會嘗試發送一封釣魚郵件至 Linux Mail 主機上。

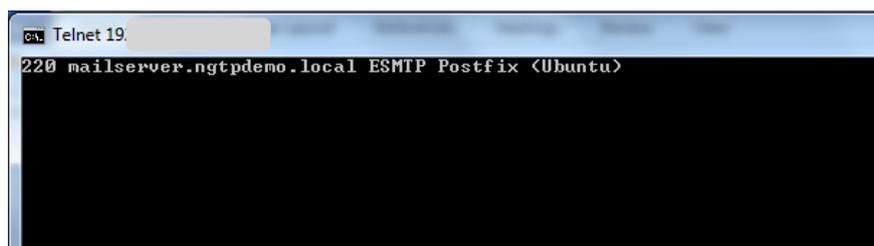
從 Windows 系統上開啟 CLI 介面

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



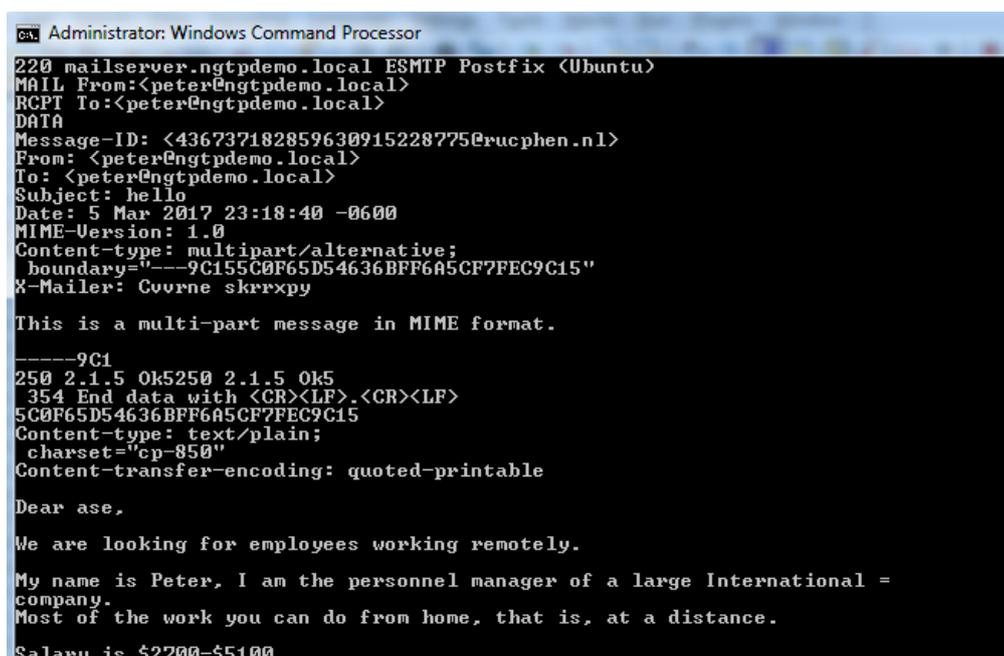
```
Administrator: Windows Command Processor
C:\Windows\System32>telnet 192.168.170.10 25
```

可以看到 Connection 成功的建立了



```
Telnet 19
220 mailserver.ngttdemo.local SMTP Postfix (Ubuntu)
```

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。



```
Administrator: Windows Command Processor
220 mailserver.ngttdemo.local SMTP Postfix (Ubuntu)
MAIL From:<peter@ngttdemo.local>
RCPT To:<peter@ngttdemo.local>
DATA
Message-ID: <436737182859630915228775@rucphen.nl>
From: <peter@ngttdemo.local>
To: <peter@ngttdemo.local>
Subject: hello
Date: 5 Mar 2017 23:18:40 -0600
MIME-Version: 1.0
Content-type: multipart/alternative;
  boundary="---9C155C0F65D54636BFF6A5CF7FEC9C15"
X-Mailer: Covrne skrrxpy

This is a multi-part message in MIME format.

-----9C1
250 2.1.5 Ok5250 2.1.5 Ok5
 354 End data with <CR><LF>.<CR><LF>
5C0F65D54636BFF6A5CF7FEC9C15
Content-type: text/plain;
  charset="cp-850"
Content-transfer-encoding: quoted-printable

Dear ase,

We are looking for employees working remotely.

My name is Peter, I am the personnel manager of a large International =
company.
Most of the work you can do from home, that is, at a distance.

Salary is $2700-$5100.
```

顯示 Log 訊息，可以發現一筆阻檔的紀錄：

No.	Name	Source	Destination	Protection/Site/File/Blade	Action	Track
1	protect mailserver	net_192.168.169.0	mailserver	N/A	Strict (Clone)	Log Packet Capture

Time	Blade	Action	Type	Interface	Seve...	Source	Destination	Protection Type	Protection Name	Malware
Today, 18:49:18	IPS	Prevent	Log	eth0	Critical	192.168.169.1	mailserver (192....	IPS	Suspicious Metadata Mail Phis...	
Today, 18:03:20	Anti-Virus	Detect	Log	eth1	Medium	mailserver (192....	DNS_Server_vm...	DNS Reputati...	REP.iklueb	DNS query
Today, 16:57:38	Anti-Virus	Detect	Log	eth0	Medium	mgnt (192.168.1...	DNS_Server_vm...	DNS Reputati...	REP.ikkioe	DNS query
Today, 16:56:38	Anti-Virus	Detect	Log	eth0	Medium	mgnt (192.168.1...	DNS_Server_vm...	DNS Reputati...	REP.ikjuju	DNS query
Today, 16:55:57	Anti-Virus	Redirect	Log	eth1	Medium	mailserver (192....	gwR8010 (192.1...	URL Reputation	REP.ikjuju	Access to s
Today, 16:55:56	Anti-Virus	Redirect	Log	eth1	Medium	mailserver (192....	62.0.58.94	URL Reputation	REP.iktgpp	Access to s
Today, 16:55:39	Anti-Virus	Detect	Log	eth1	Medium	mailserver (192....	DNS_Server_vm...	DNS Reputati...	REP.iktgpp	DNS query
Today, 15:25:07	Anti-Virus	Detect	Log	eth0	Medium	mgnt (192.168.1...	DNS_Server_vm...	DNS Reputati...	REP.ikjuju	DNS query
30 May 17, 19:48:...	IPS	Prevent	Log	eth0	Critical	192.168.169.1	mailserver (192....	IPS	Suspicious Metadata Mail Phis...	

檢視 IPS 的 Log Details

Prevent
Phishing Enforcement Protection

Details | Matched Rules

Log Info

- Severity: Critical
- Confidence Level: Medium
- Attack Name: Phishing Enforcement Protection
- Attack Information: Suspicious Metadata Mail Phishing Redirection
- Performance Impact: Medium
- Protection Name: Suspicious Metadata Mail Phishing Redirection
- Protection Type: IPS
- Packet Captures: src-192.168.169.1.eml

Traffic

- Source: 192.168.169.1 (Windows)
- Destination: mailserver (192.168.170.10)
- Service: smtp (TCP/25)
- Source Port: 60383
- Bytes (sent/receive...): 0 B \ 0 B
- Interface: eth0

Policy

- Action: Prevent
- Threat Prevention ...: NGTpdemo
- Threat Prevention ...: Today, 18:53:05
- Rule Id: 48A93931-F4BC-4261-A8BC-47A849DE23DD
- Threat Profile: Strict (Clone)
- Access Rule Name: Email

Actions

- Threat Wiki: [Go to Threat Wiki](#)
- Remediation: [Go to Remediation Options](#)
- Add Exception: [Add Exception...](#)
- Report Log: [Report Log to Check Point](#)

More

- Protection ID: asm_dynamic_prop_HTML_MD_MAIL
- Description Url: [HTML_MD_MAIL_help.html](#)
- Session Identificat...: 0x59343a0e,0x0,0xfefe1bac,0xc0000000
- Access Rule UID: 42913dcf-a5a8-4799-9cfb-09917657c740

嘗試發送多筆的 **Phishing Mail** 之後再檢視 Log.

Scroll down verifying if there are suppressed log messages.

The screenshot displays a network log entry with two main sections: Traffic and Report Log.

Traffic

Source	192.168.169.1 Windows
Destination	mailserver (192.168.170.10)
Service	smtp (TCP/25)
Source Port	60383
Bytes (sent\receive...)	0 B \ 0 B
Interface	eth0

Report Log

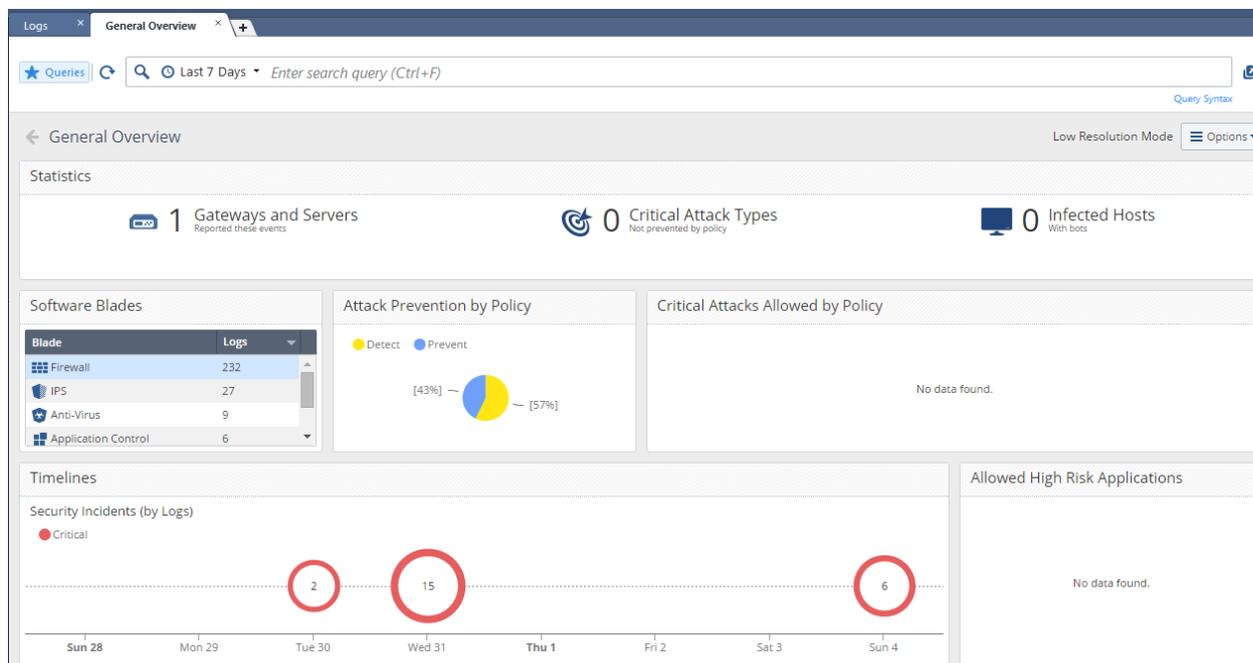
[Report Log to Check Point](#)

More

Protection ID	asm_dynamic_prop_HTML_MD_MAIL
Description Url	HTML_MD_MAIL_help.html
Session Identificat...	0x59343a0e,0x0,0xfefe1bac,0xc0000000
Access Rule UID	42913dcf-a5a8-4799-9cfb-09917657c740
Policy Management	mgnt
Suppressed Logs	3

Lab 4: 使用 SmartEvent 報表功能

開啟 Logs & Monitor > General 頁籤



點擊 IPS 事件

Logs

Found 27 results (209 ms)

Time	Action	Origin	Sever...	Source User...	Source	Destination	Protection Type	Protection Name	IPS Profile	Attack Name
Today, 19:47:03	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
Today, 19:47:03	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
Today, 19:46:47	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
Today, 19:44:31	Detect	gwR8010	Medium		mailserver (192...	mailserver (192...	Protocol Anomaly	Sweep Scan	N/A	Port Scan
Today, 19:42:44	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
Today, 19:39:24	Detect	gwR8010	Medium		mailserver (192...	mailserver (192...	Protocol Anomaly	Sweep Scan	N/A	Port Scan
Today, 19:39:14	Detect	gwR8010	Medium		mailserver (192...	mailserver (192...	Protocol Anomaly	Sweep Scan	N/A	Port Scan
Today, 19:34:07	Detect	gwR8010	Medium		mailserver (192...	mailserver (192...	Protocol Anomaly	Sweep Scan	N/A	Port Scan
Today, 19:05:00	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Protocol Anomaly	Binary Data In SMTP Com...	N/A	SMTP Format
Today, 18:49:18	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	IPS	Suspicious Metadata Mail...	Strict (Clone)	Phishing Enf...
31 May 17, 16:44:36	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
31 May 17, 16:44:36	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
31 May 17, 09:29:45	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header
31 May 17, 09:29:30	Prevent	gwR8010	High		192.168.169.1	mailserver (192...	Signature	HTTP Header Patterns	N/A	HTTP Header

檢視 IPS 事件中被 Detect 的事件

Found 5 results (266 ms)

Time	Severity	Source	Destination	Protection Type	Protection Name	Malware Acti...	Malware Rule...	Con...	Scan
Today, 18:03:20	Medium	mailserver (192...	DNS_Server_vm...	DNS Reputation	REP.iklueb	DNS query for a...			
Today, 16:57:38	Medium	mgnt (192.168.1...	DNS_Server_vm...	DNS Reputation	REP.ikkioe	DNS query for a...			
Today, 16:56:38	Medium	mgnt (192.168.1...	DNS_Server_vm...	DNS Reputation	REP.ikjuju	DNS query for a...			
Today, 16:55:39	Medium	mailserver (192...	DNS_Server_vm...	DNS Reputation	REP.ikktgp	DNS query for a...			
Today, 15:25:07	Medium	mgnt (192.168.1...	DNS_Server_vm...	DNS Reputation	REP.ikjuju	DNS query for a...			

開啟 Threat Prevention view

Threat Prevention

Statistics

- 1 Gateways and Servers (Reported these events)
- 0 High Risk Attacks (Distinct attacks not prevented due to policy)
- 3 Prevented Attacks (Distinct attack types)
- 0 Infected Hosts (With bots)

Top Protections

Protection Name	Severity	Blade	Action	Logs
HTTP Header Patterns	Critical	IPS	Prevent	19
Suspicious Metadata Mail Phishing Redire...	Critical	IPS	Prevent	3
Binary Data In SMTP Commands	Critical	IPS	Prevent	1
REP.ikjuju	Medium	Anti-Virus	Detect	2
REP.ikkioe	Medium	Anti-Virus	Detect	1
REP.iklueb	Medium	Anti-Virus	Detect	1

Hosts Infected with Bots

No data found.

Activity Timeline

● Medium ● Critical

Sun 28 Mon 29 Tue 30 Wed 31 Thu 1 Fri 2 Sat 3 Sun 4

Event counts: Tue 30 (2), Wed 31 (15), Sun 4 (11)

產生一份關於 Threat Prevention 的攻擊報表

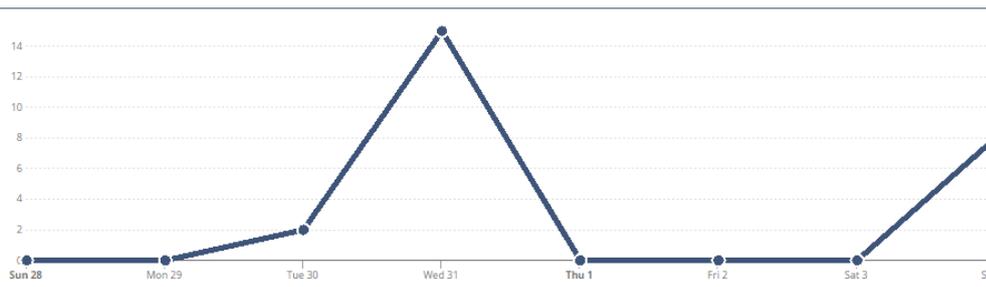
報表應該會包含以下的內容

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

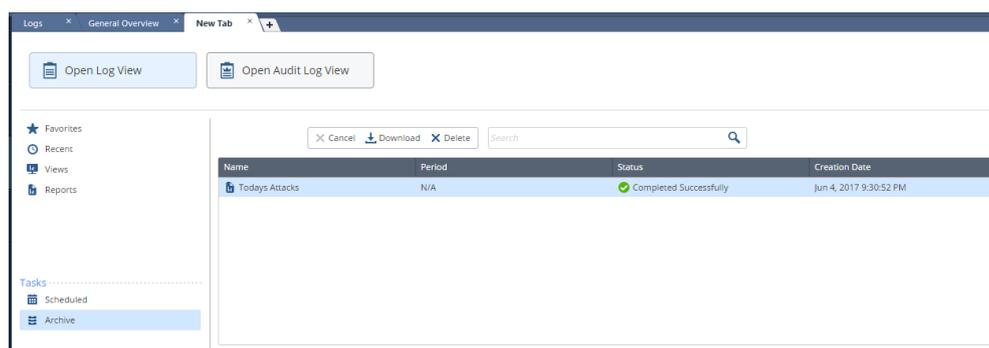
Attacks by destination

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

Attacks over time

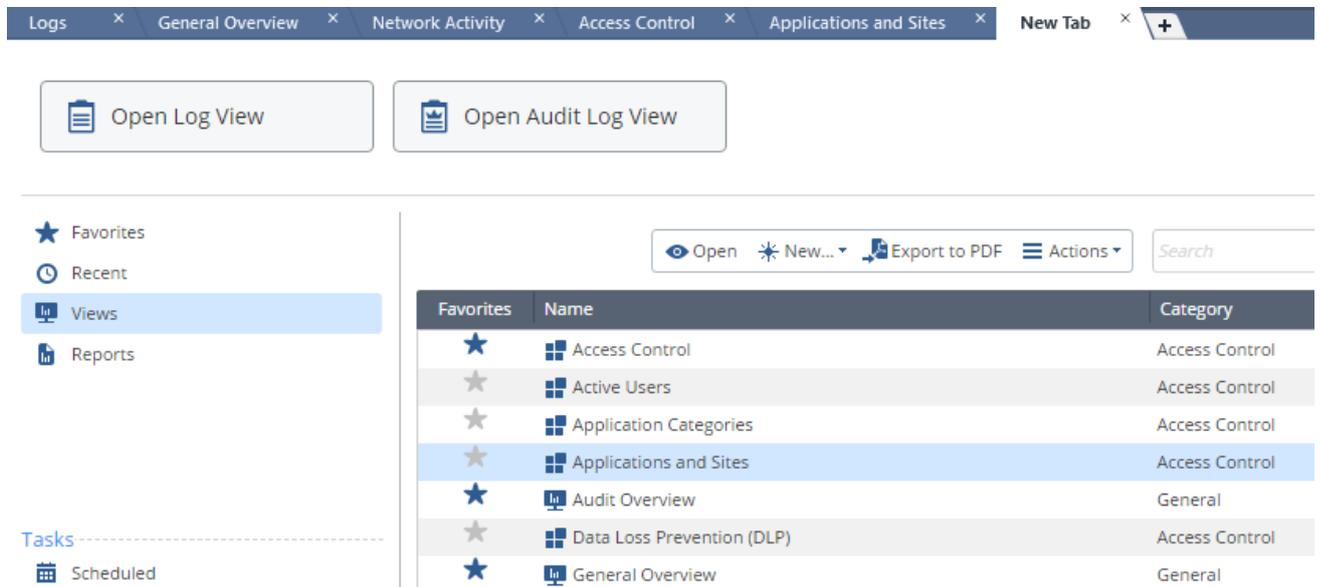


嘗試產生報表並且下載至 Windows 電腦上：



開啟 SmartView 功能

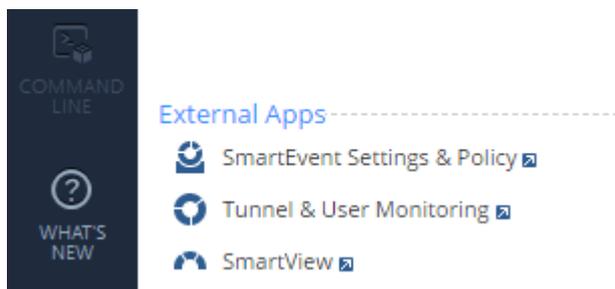
在 Log & Monitor 頁籤點選右上角「+」開新分頁：



The screenshot shows the SmartConsole interface with the Log & Monitor page. At the top, there are several tabs: Logs, General Overview, Network Activity, Access Control, Applications and Sites, and a new tab labeled 'New Tab'. Below the tabs are two buttons: 'Open Log View' and 'Open Audit Log View'. The main content area is divided into a left sidebar and a main table. The sidebar has sections for Favorites, Recent, Views, Reports, and Tasks. The main table has a search bar and a table of favorites.

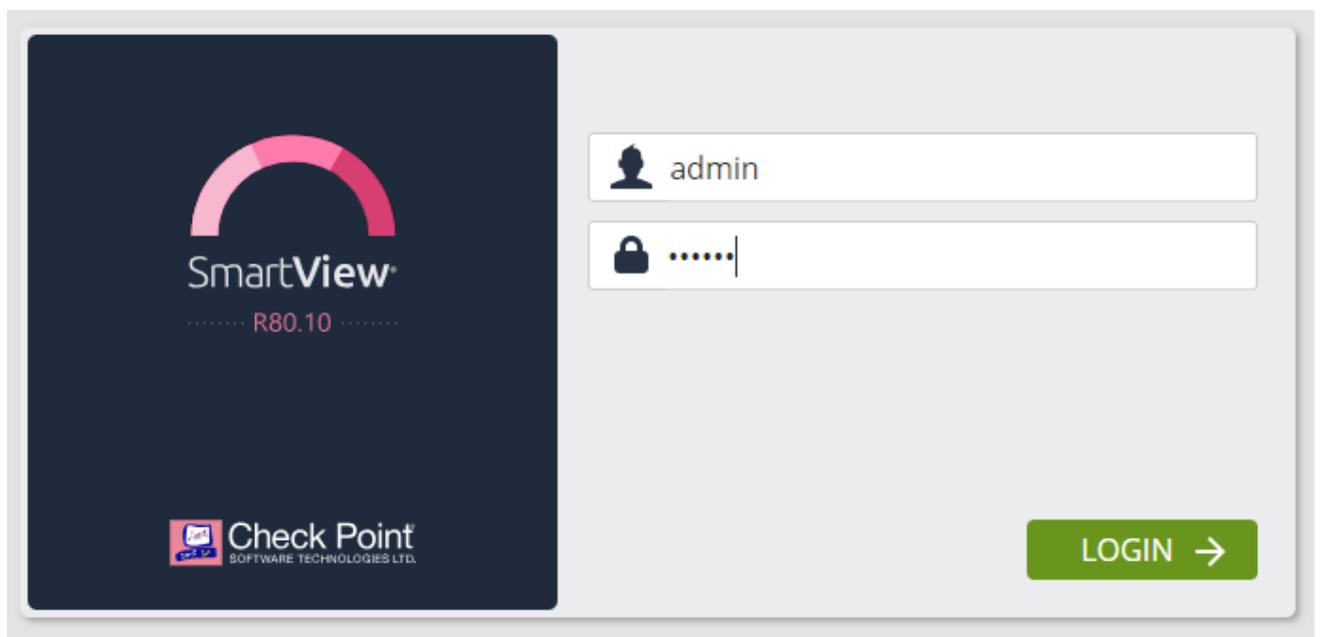
Favorites	Name	Category
★	Access Control	Access Control
★	Active Users	Access Control
★	Application Categories	Access Control
★	Applications and Sites	Access Control
★	Audit Overview	General
★	Data Loss Prevention (DLP)	Access Control
★	General Overview	General

在左下角 External Apps 中點擊「SmartView」：



The screenshot shows the 'External Apps' section in the SmartConsole interface. On the left, there is a dark sidebar with 'COMMAND LINE' and 'WHAT'S NEW' buttons. The main area is titled 'External Apps' and contains three items: 'SmartEvent Settings & Policy', 'Tunnel & User Monitoring', and 'SmartView'.

自動開啟瀏覽器，輸入 SmartConsole 的帳號密碼：



The screenshot shows the SmartView login page. On the left, there is a dark blue box with the SmartView logo and 'R80.10' text. Below the logo is the Check Point logo and 'SOFTWARE TECHNOLOGIES LTD.' text. On the right, there are two input fields: the first for the username 'admin' and the second for the password, which is masked with dots. A green 'LOGIN' button with a right arrow is located at the bottom right.

透過 SmartView 功能使用瀏覽器來檢視報表：

