



Check Point®
SOFTWARE TECHNOLOGIES LTD.



Check Point SG1570

R80.20.35

配置手册

目录

一、 安装及设定	6
一、 设定环境配置	6
1. 连接设备	6
2. 调整电脑网卡 TCP/IP 设定	6
二、 初始设定 SG1570	8
1. 进入连线设定页面	8
2. 开始初始设定	9
3. 设定管理员账号(Administrator name)以及密码>Password)	9
4. 设定日期(Date)/时间(Time)/时区(Time Zone).....	10
5. 设定主机名(Appliance Name)	10
6. 选择防火墙管理方式	11
7. 设定 WAN 网络连接.....	11
8. 设定内部网络 Local Network	12
9. 设定管理员连接方式	12
10. 启用 License.....	13
11. 启用 Check Point 功能刀片	14
12. 完成设定	14
二、 升级 R80.20.35	15
一、 联网下载更新版本	15
二、 手动更新版本	16
三、 Web 管理功能说明	17
一、 页面说明	17
1. 显示登入者 ID 与登出(Log Out).....	17
2. 主功能标签.....	17



3.	次功能目录.....	17
4.	内容.....	17
5.	显示当前设备状态，包含 Internet、Status、Device Time	17
二、	Home 目录.....	18
1.	Overview 总览.....	18
1-1.	System.....	18
1-2.	Security Dashboard.....	18
1-3.	Security Management.....	19
1-4.	Cloud Services.....	20
1-5.	License.....	21
1-6.	Site Map.....	22
2.	Monitoring.....	22
2-1.	Active Computers.....	22
2-2.	Monitoring.....	23
2-3.	Reports.....	24
3.	Troubleshooting.....	29
3-1.	Tools.....	29
3-2.	Support	31
三、	Device 設定	32
1.	Network.....	32
1-1.	Internet.....	32
1-2.	Local Network.....	34
1-3.	Hotspot	38
1-4.	Routing.....	41
1-5.	DNS.....	42
1-6.	Proxy	43
2.	System.....	43
2-1.	System Operations	43
2-2.	Administrators.....	44
2-3.	Administrator Access.....	44
2-4.	Device Details	45
2-5.	Date and Time	45
2-6.	DDNS & Device Access.....	45



2-7. Tools.....	46
3. Advanced.....	46
3-1. High Availability.....	46
3-2. Advanced Settings.....	48
四、 Access Policy 設定.....	48
1. Firewall.....	48
1-1. Blade Control.....	48
1-2. Policy.....	50
1-3. Servers.....	53
1-4. NAT.....	53
2. User Awareness>Blade Control.....	53
3. QoS.....	55
五、 Threat Prevention 設定.....	56
1. Threat Prevention.....	56
1-1. Blade Control.....	56
1-2. Exceptions.....	59
1-3. Infected Hosts.....	59
2. Protections.....	59
2-1. IPS Protections.....	59
2-2. Engine Settings.....	60
3. Anti-Spam.....	65
3-1. Blade Control.....	65
3-2. Exceptions.....	65
六、 VPN 設定.....	66
1. Remote Access.....	66
1-1. Blade Control.....	66
1-2. Remote Access Users.....	68
1-3. Authentication Servers.....	70
1-4. Advanced.....	70
2. Site to Site.....	70
2-1. Blade Control.....	70
2-2. VPN Sites.....	71



2-3.	Community.....	73
2-4.	VPN Tunnels.....	73
2-5.	Advanced	73
3.	Certificates.....	74
3-1.	Trusted	74
3-2.	Installed Certificates.....	74
3-3.	Internal Certificate	74
七、	Users & Objects 設定.....	75
1.	User Management.....	75
1-1.	User Awareness.....	75
1-2.	Users.....	75
1-3.	Administrators.....	75
1-4.	Authentication Servers.....	76
2.	Network Resources	76
2-1.	Servers	76
2-2.	Applications & URLs	77
2-3.	Services	77
2-4.	Service Groups	77
2-5.	Network Objects.....	80
2-6.	Network Object Groups.....	80
八、	Logs & Monitoring.....	81
1.	Logs.....	81
2-1.	Security Logs.....	81
2-2.	System Logs	83
2-3.	External Log Servers.....	83
2.	Status.....	85
3-1.	Active Computers.....	85
3-2.	Infected Hosts	85
3-3.	VPN Tunnels.....	85
3-4.	Connections	85
3-5.	Monitoring.....	85
3-6.	Reports.....	85
3.	Diagnostics.....	85



3-1. Tools.....	86
3-2. SNMP.....	86
四、恢复出厂设定配置与备份	86
一、恢复原厂预设的方式.....	86
1. 使用 WEB UI 介面	86
2. 按背面 Factory Default 按钮.....	87
3. 进入 CONSOLE 重设	88
二、备份及恢复	89
1. 备份	89
2. 计划备份	92
3. 恢复.....	93

一、安装及设定

一、设定环境配置

1. 连接设备

请使用网线连接至SG1570防火墙的LAN1来进行设定

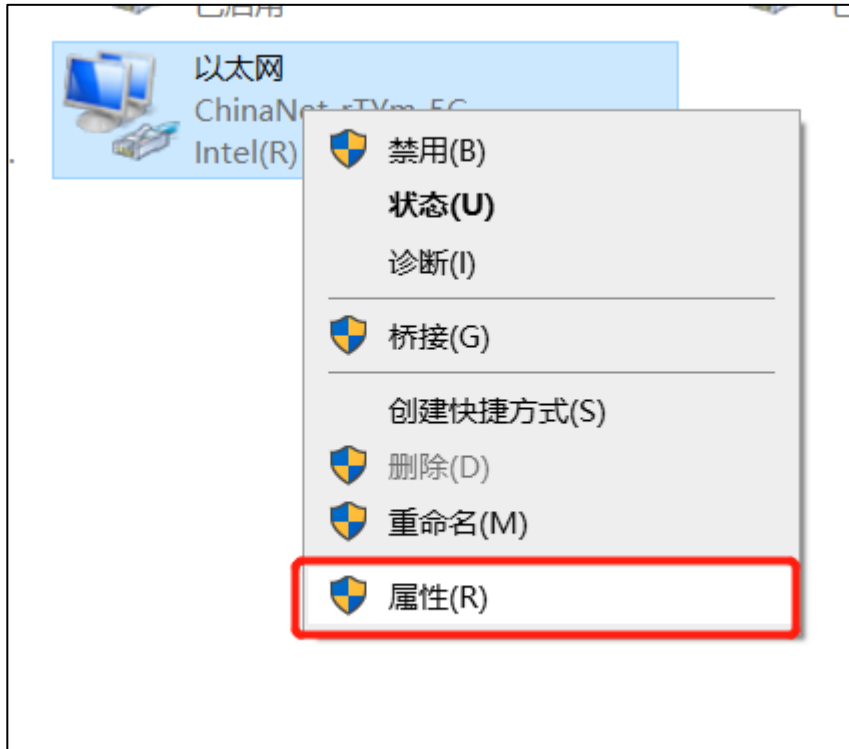


2. 调整电脑区域网络 TCP/IP 设定

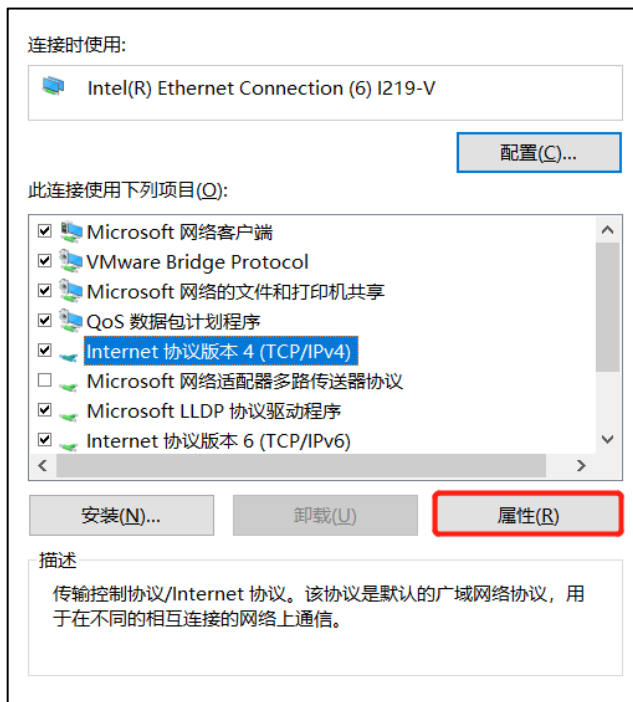
开启电脑控制台→网络和Internet→以太网，点击更改适配器选项



点选网络连接，点击属性



请选择网络通信协议第4版(TCP/IPv4)点击属性



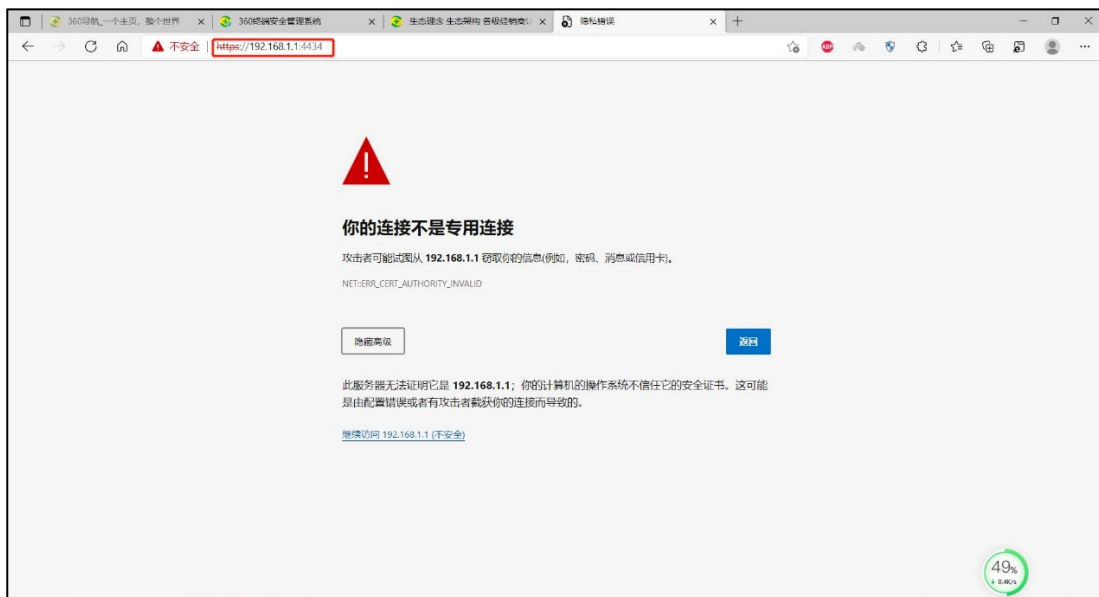
设定ip地址为192.168.1.X子网掩码是255.255.255.0，设定完点击确定。



二、初始设定 SG1570

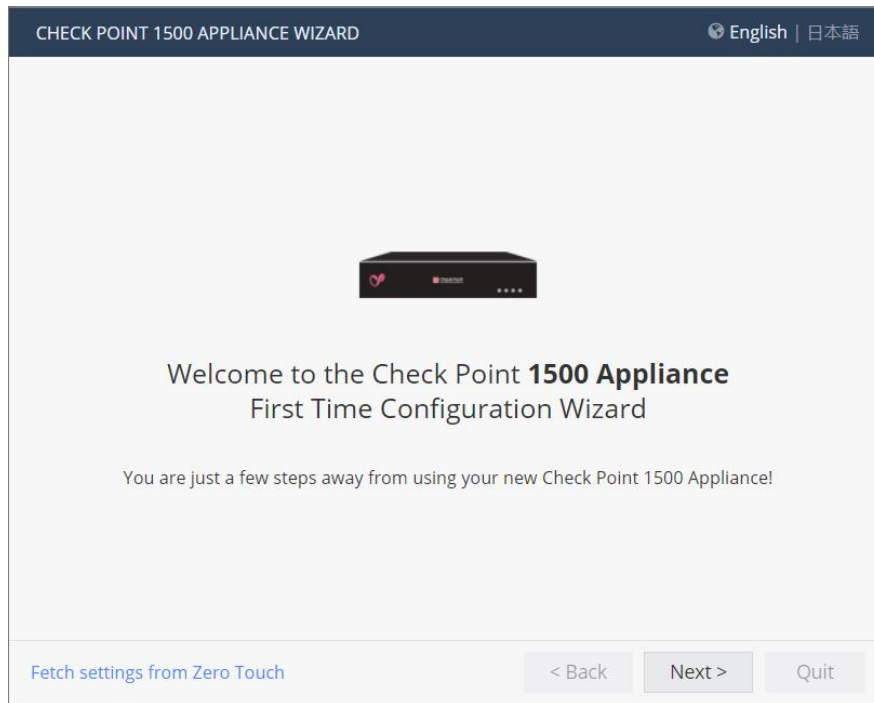
1. 进入连线设定界面

开启电脑浏览器输入 <https://192.168.1.1:4434/> 点击后 **Continue to this website** 进入设定



2. 开始初始设定

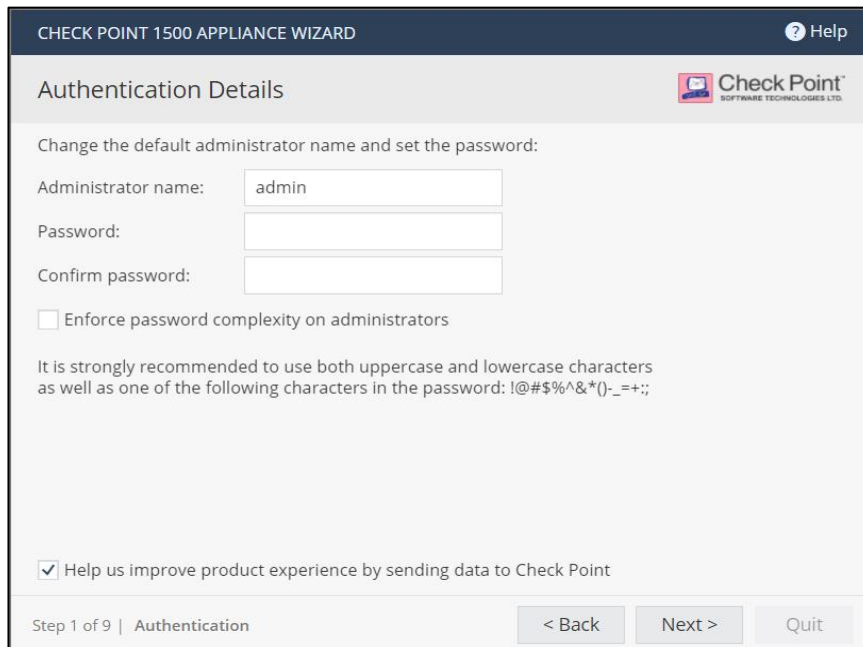
进入首次设定页面，点击“Next>”进行下一步



3. 设定管理员账号(Administrator name)以及密码>Password)

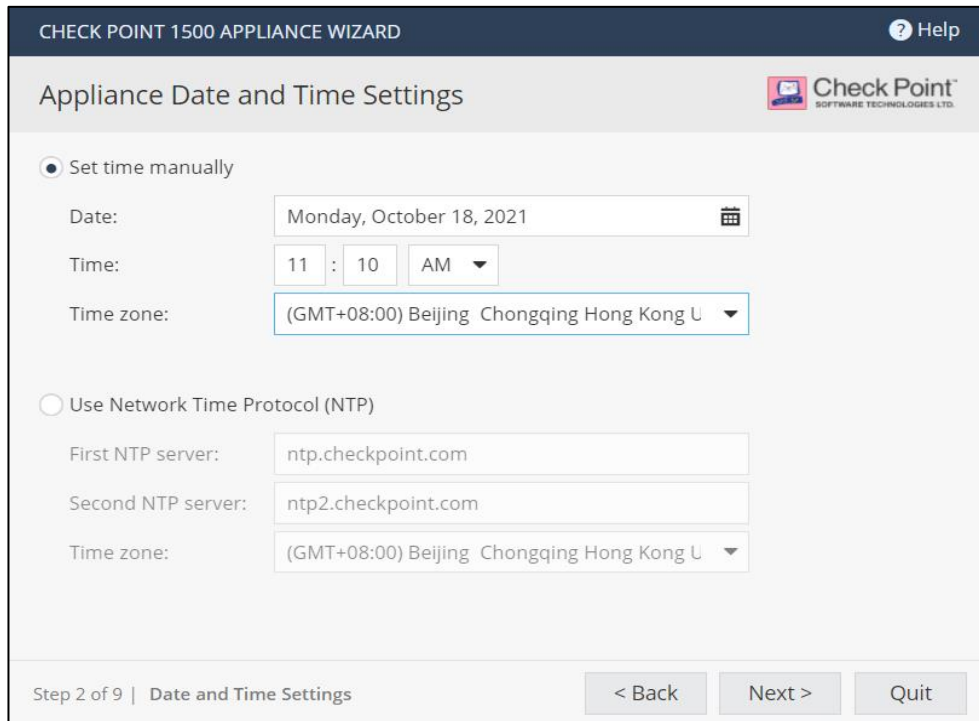
确认后点击“Next>”进行下一步。

补充：勾选 Enforce password complexity on administrators，可设定密码逾期时间



4. 设定日期(Date)/时间(Time)/时区(Time Zone)

确认后点击“ Next> ” 进行下一步



CHECK POINT 1500 APPLIANCE WIZARD Help

Appliance Date and Time Settings

Set time manually

Date:

Time: :

Time zone:

Use Network Time Protocol (NTP)

First NTP server:

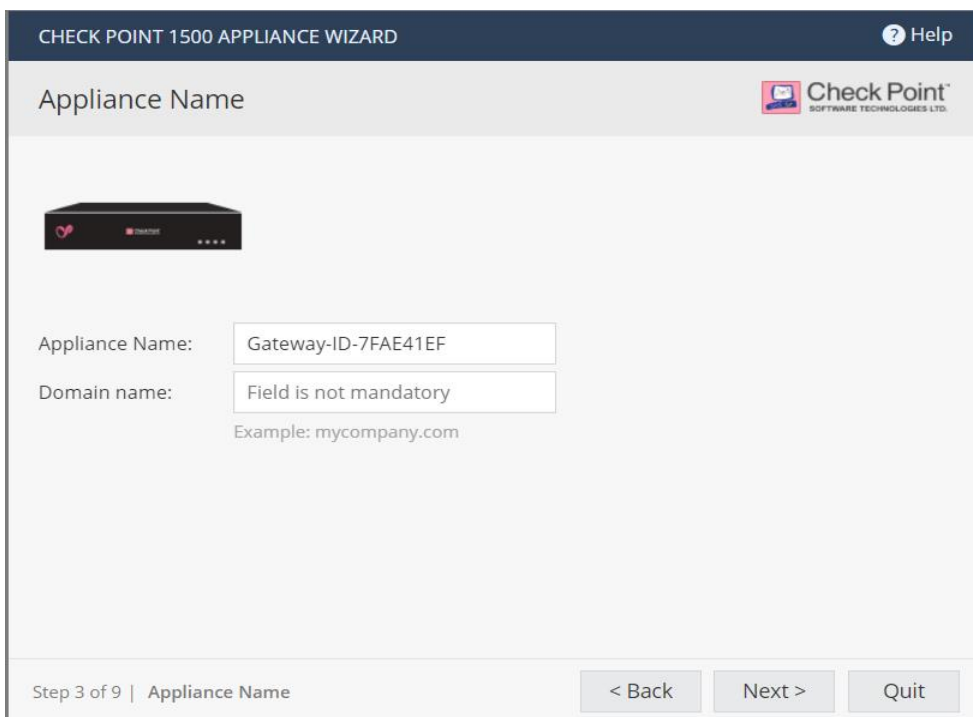
Second NTP server:

Time zone:

Step 2 of 9 | Date and Time Settings < Back Next > Quit


5. 设定设备主机名(Appliance Name)

确认后点击“ Next> ” 进行下一步进行下一步



CHECK POINT 1500 APPLIANCE WIZARD Help

Appliance Name



Appliance Name:

Domain name:

Example: mycompany.com

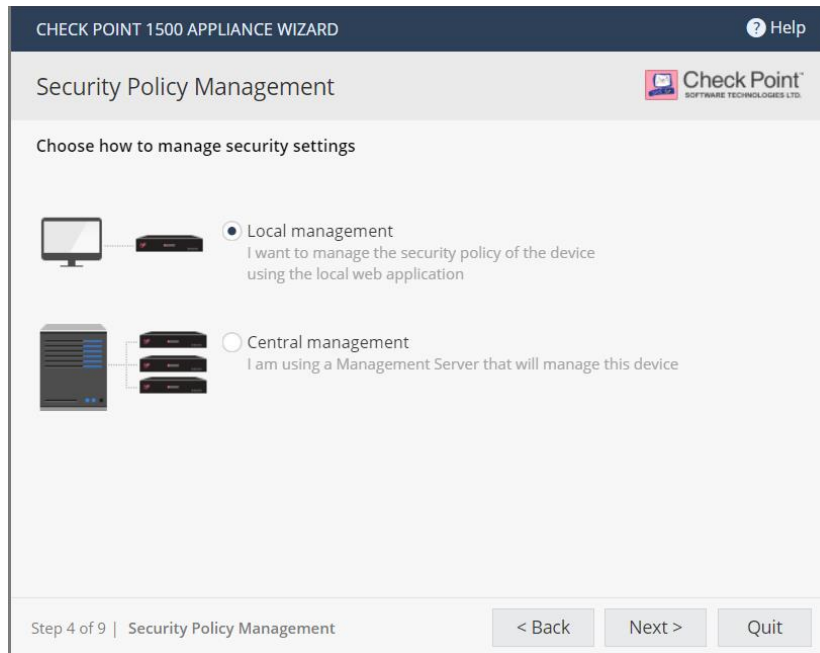
Step 3 of 9 | Appliance Name < Back Next > Quit

6. 选择防火墙的管理方式

选择 Local management，确认后点击“Next>”进行下一步进行下一步

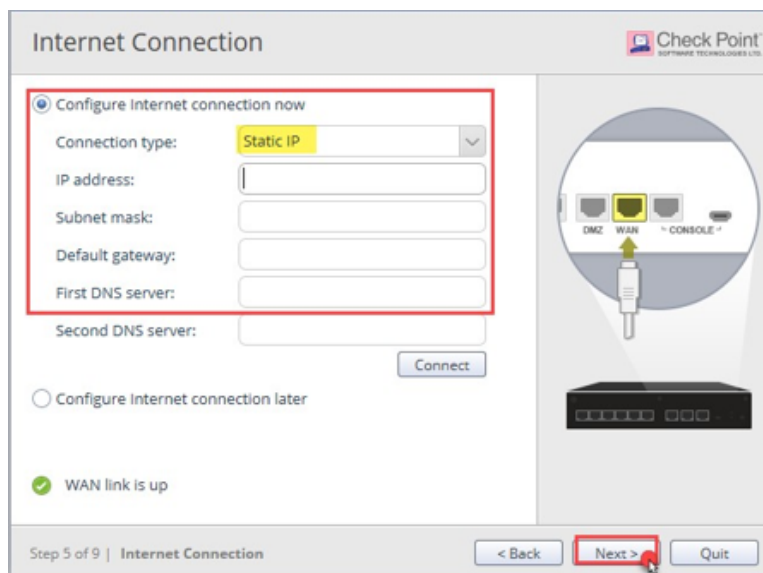
若为单台防火墙设备建议采用Local，可不用另外安装管理软件

若需要管理多台防火墙则建议采用 Central，需要另安装管理服务器来管理多台防火墙设备



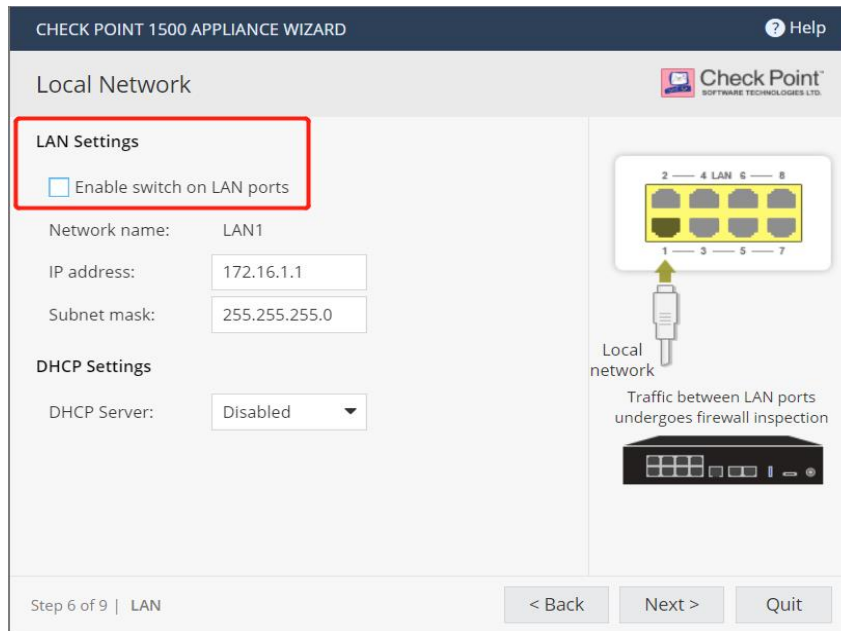
7. 设定 WAN 网络连接

建议连线方式(Connetione type)使用 Static ip，填入设定的 IP、Subnet Mask、Default gateway，，确认后点击“Next>”进行下一步



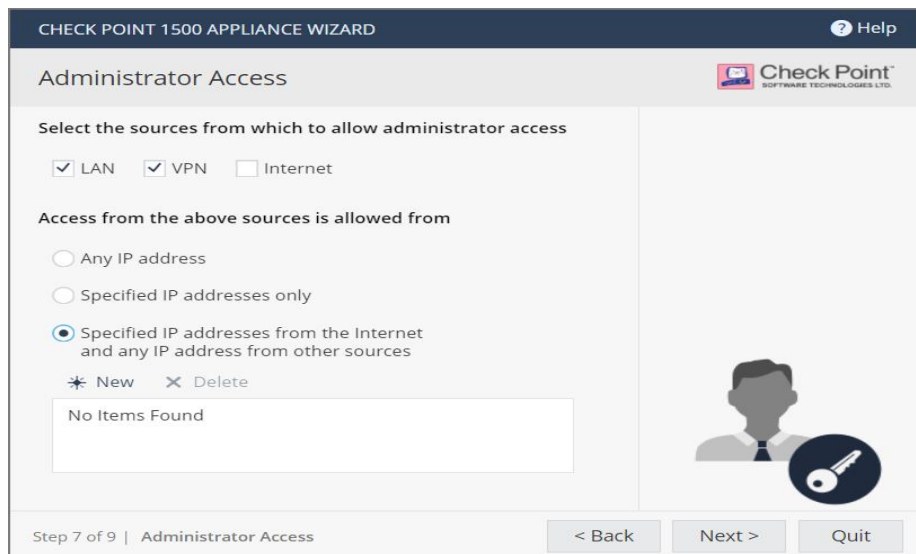
8. 设定内部网络连线 Local Network

输入 IP address 、 Subnet mask 、 DHCP Settings 若无使用选择 Disable ，确认后点击“ Next> ”进行下一步(初始设定完成后可再调整 Local Network)



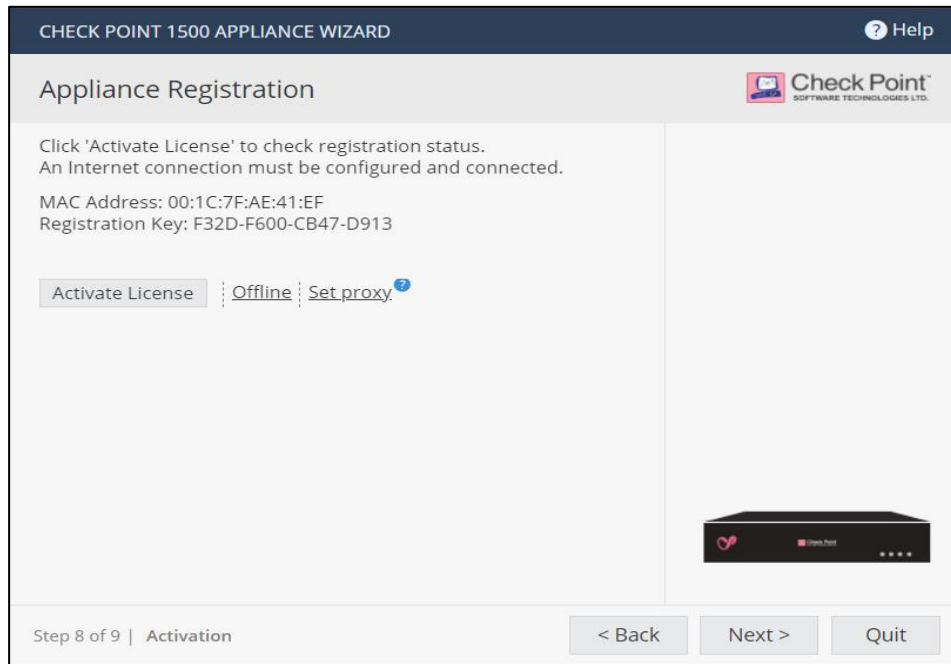
9. 设定管理员连接方式

可依公司需求进行设定任何 IP(Any IP Address) 、 特定 IP(Specified IP addresses only) 、 特定 Internet IP 以及任何来源位置(Specified IP addresses from the Internet and any IP address from other sources) 确认后点击“ Next> ”进行下一步。



10. 激活许可License

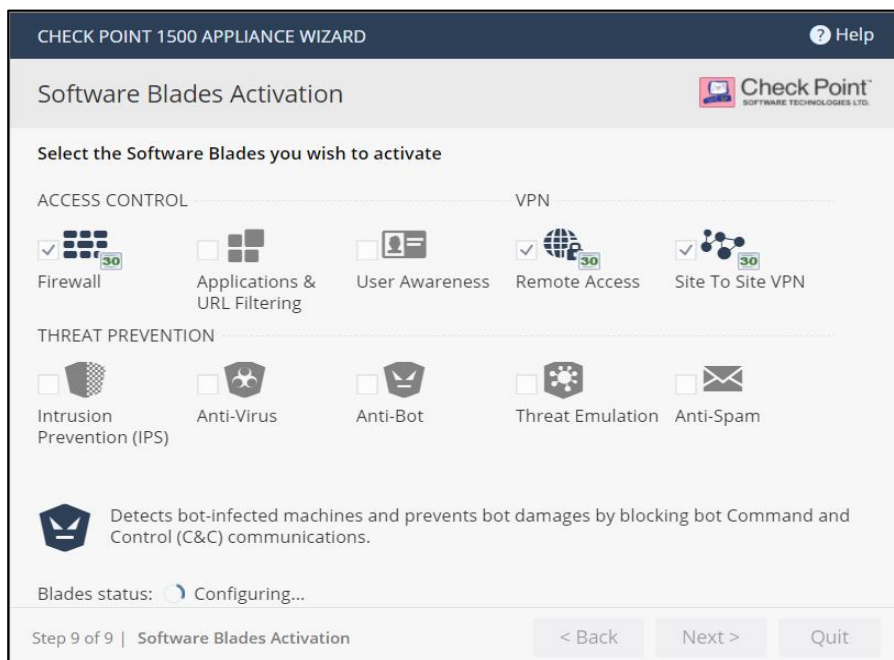
License 建议后期在 Device 设定时再启用，点击“ Next>” 进行下一步



点击后跳出 License 未启用的警告，请点击 OK 确认即可。

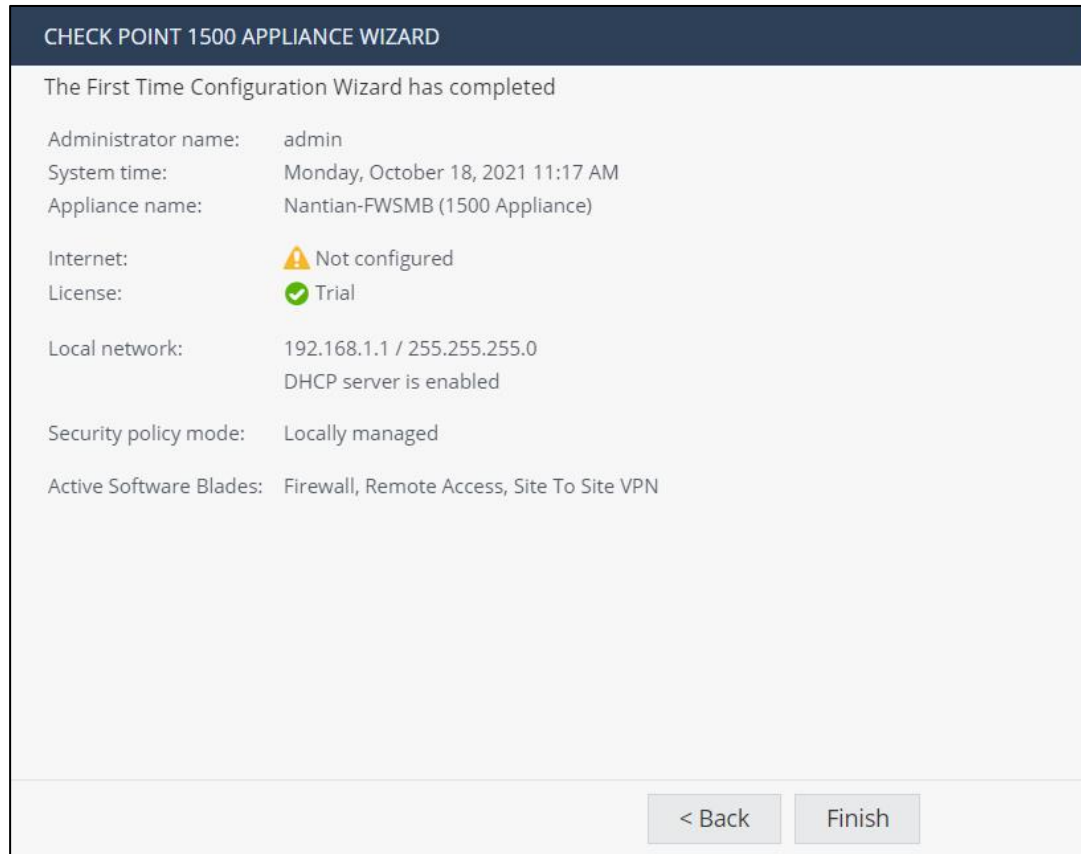
11. 启用防火墙功能刀片

勾选需要使用的功能后，点击“ Next>” 进行下一步。



12. 完成设定

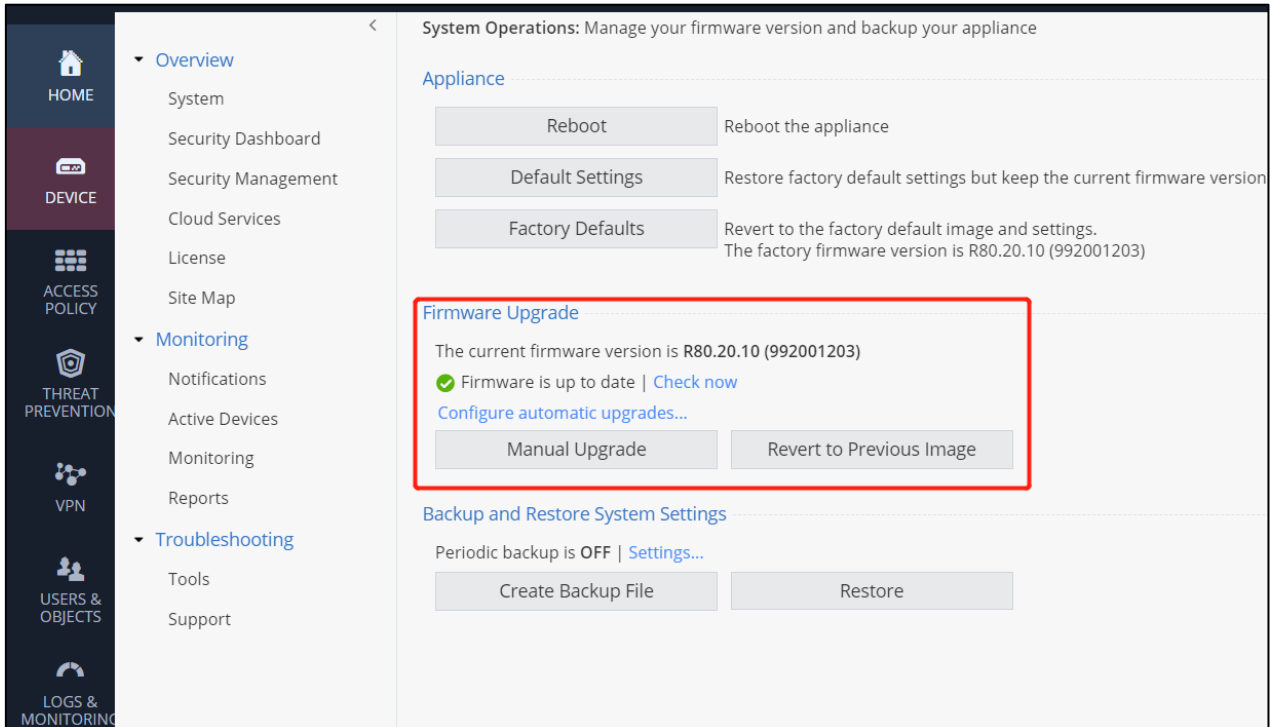
确认设备信息后点击 **Finish** 完成设定，设定完成后进入 Web UI 介面。



二、升级 R80.20.35

一、联网下载更新版本

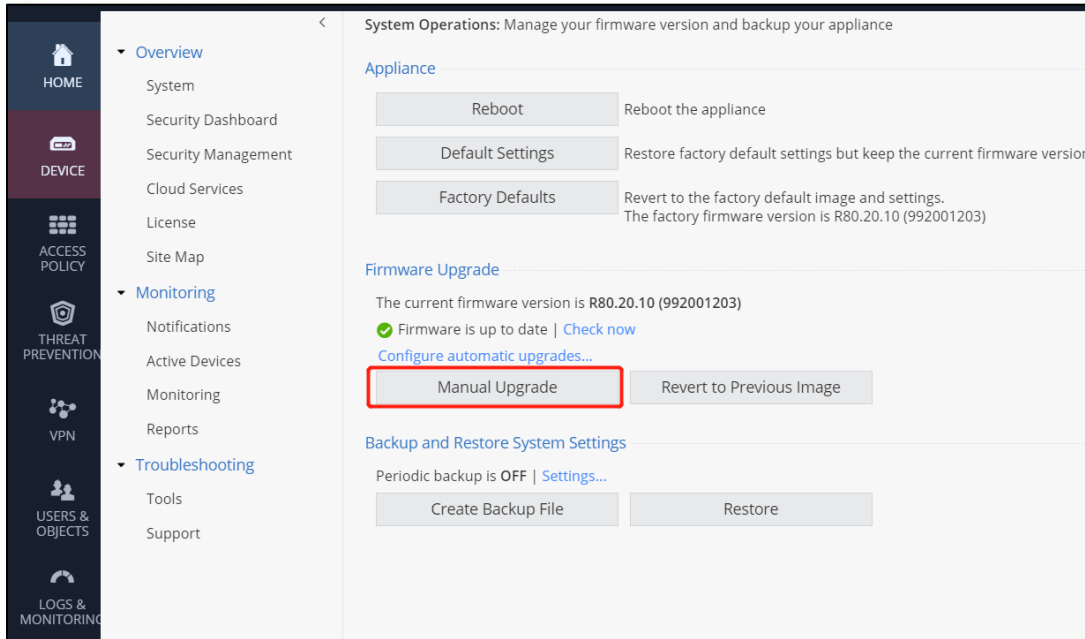
通过 Device>System Operations>Firmware Upgrade>Check now



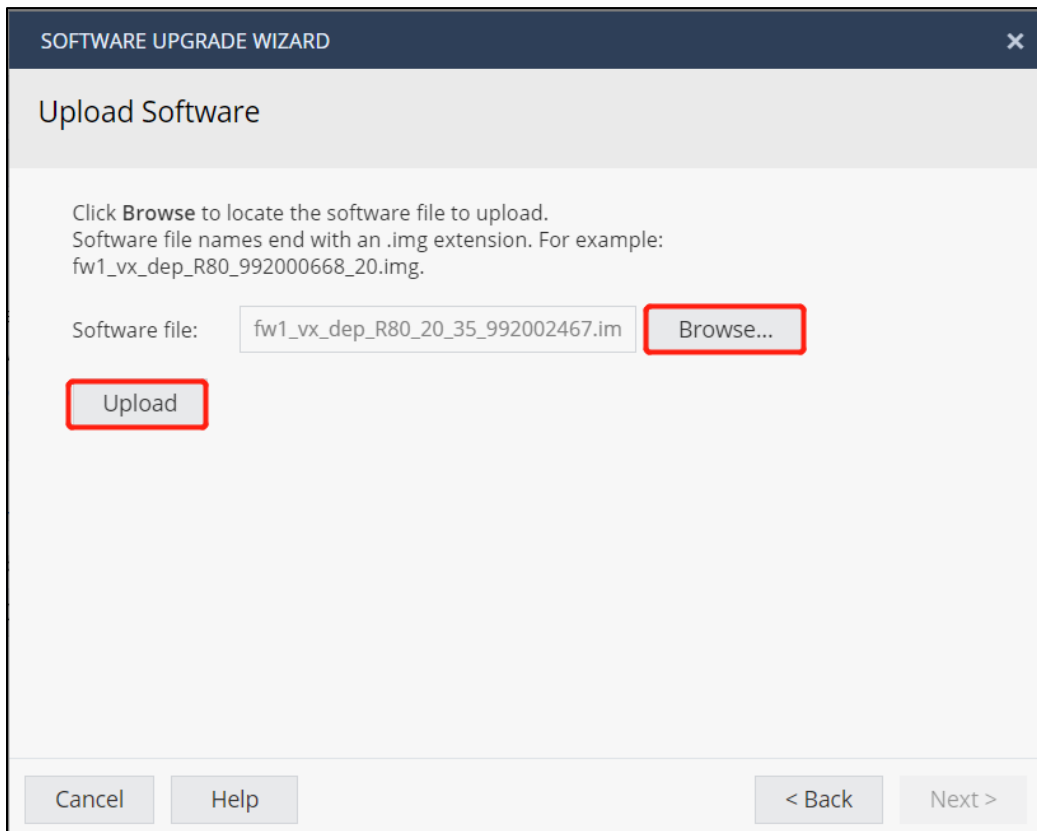
若有新版本可更新时，会提示新版的的信息，点击Upgrade Now 即可开始更新

二、手动更新版本

使用CheckPoint账号下载对应的版本，点击Manual Upgrade，进行下一步



点击**Browse**选择下载的新版本文件，再点击**Upload**上传入设备进行更新。

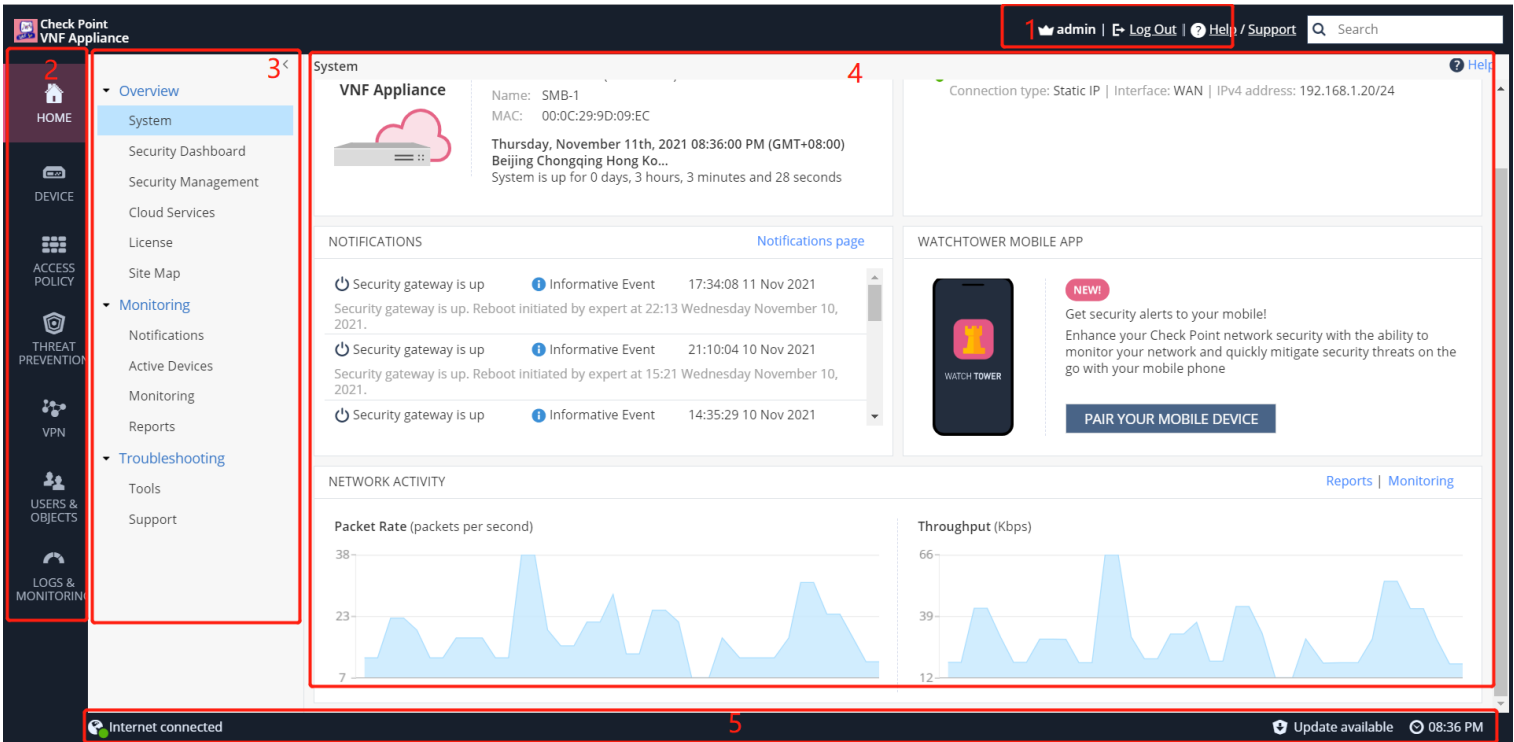


更新完成后会回到登入页面，此时为新版本的登入页面，输入账号密码即可登入

三、Web 管理功能说明

一、界面说明

1. 显示登入人员及登出(Log Out)
2. 主功能标签
3. 次功能目录
4. 内容
5. 显示当前设备状态，包含 Internet、Status、Device Time



The screenshot displays the Check Point VNF Appliance web management interface. Key elements include:

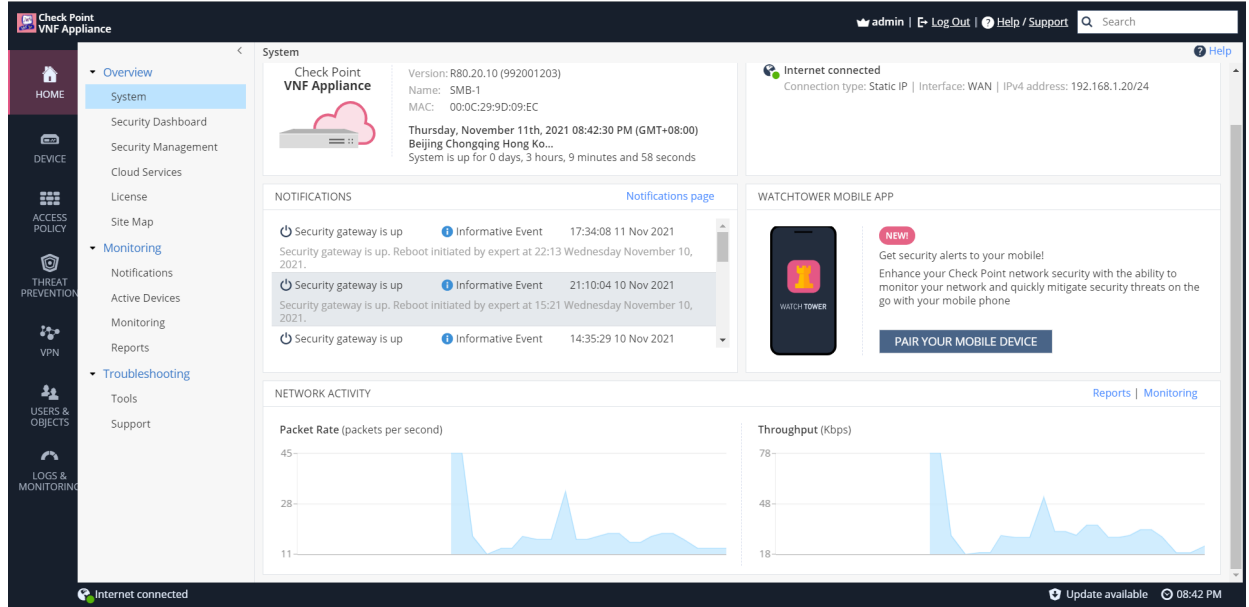
- Top Bar:** User 'admin' and 'Log Out' button.
- Left Sidebar:** Navigation menu with icons for Overview, Device, Access Policy, Threat Prevention, VPN, Users & Objects, and Logs & Monitoring.
- Main Content Area:**
 - System Overview:** Shows VNF Appliance details: Name: SMB-1, MAC: 00:0C:29:9D:09:EC, Status: Thursday, November 11th, 2021 08:36:00 PM (GMT+08:00), Beijing Chongqing Hong Ko... System is up for 0 days, 3 hours, 3 minutes and 28 seconds.
 - Notifications:** Lists security gateway events, including 'Security gateway is up' and 'Reboot initiated by expert'.
 - WATCHTOWER MOBILE APP:** Promotes the mobile app with a 'PAIR YOUR MOBILE DEVICE' button.
 - NETWORK ACTIVITY:** Contains two line graphs: 'Packet Rate (packets per second)' and 'Throughput (Kbps)'.
- Status Bar:** Shows 'Internet connected' and 'Update available'.

二、Home 目录



1. Overview 总览

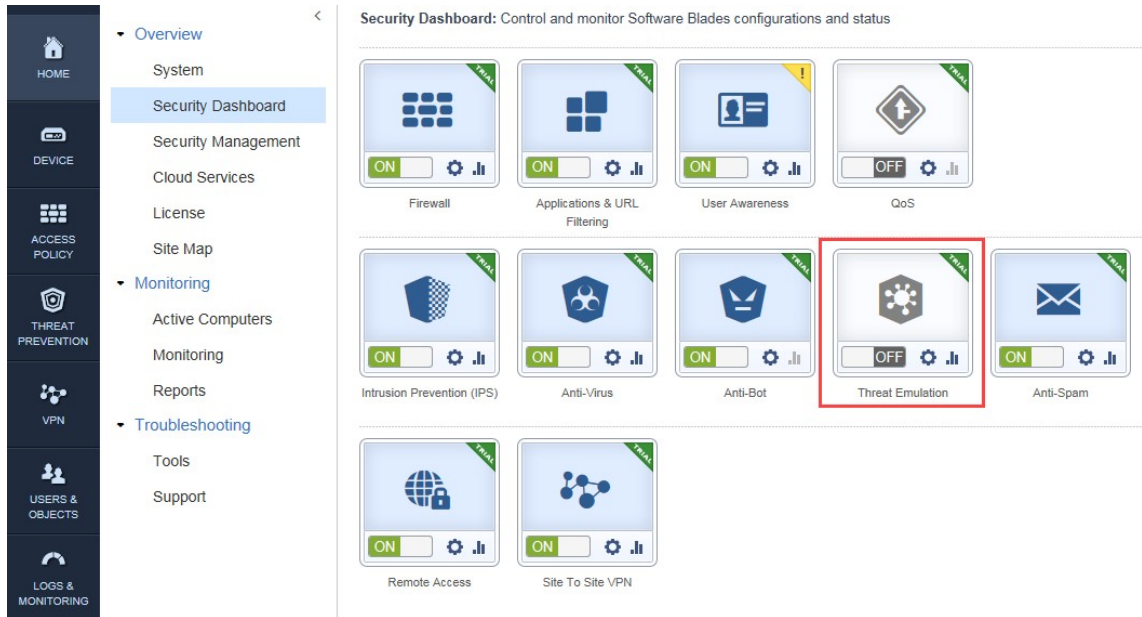
1-1. System

显示当前系统信息，包含版本、主机名、MAC、日期时间、网络速率及吞吐量
图表



1-2. Security Dashboard

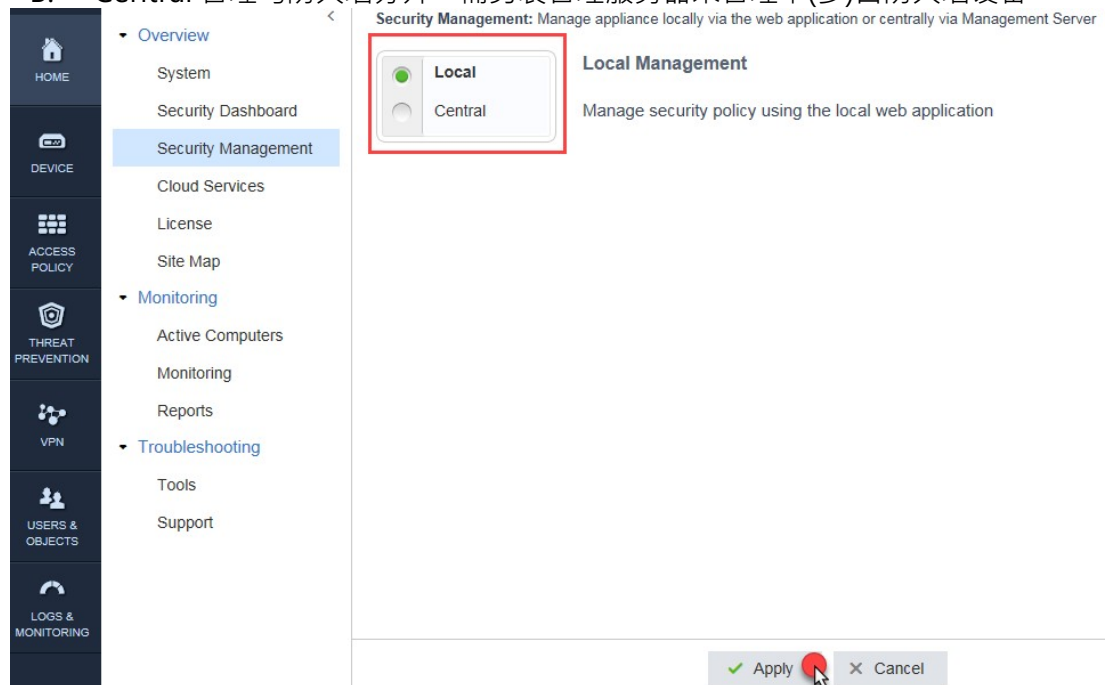
- A. 查看当前防火墙功能，并可透过图示开关(OFF 关闭或启用 ON)功能
- B. 点击齿轮  图示可进行该功能设定(功能设定也在各功能标签中进行设定)
- C. 点击图表  图示可查看该功能当前状态
- D. 目前SMB各版本均支持“Threat Emulation”的 blade



1-3. Security Management

查看及变更防火墙的管理方式

- A. Local 管理与防火墙一体，可不用另外安装管理软件
- B. Central 管理与防火墙分开，需另装管理服务器来管理单(多)台防火墙设备




1-4. Cloud Services

设定云端管理服务，Cloud Services 可透过 Web 來管理、设定、监控防火墙。

补充：Try License 需請原厂提供

Cloud Services: Configure a Cloud Services provider that can handle your security policy and supply a variety of services [? Help](#)

Cloud Services



[Configure](#)

Managed Security Blades

- Firewall
- Applications & URL Filtering
- User Awareness
- QoS
- IPS
- Anti-Virus
- Anti-Bot
- Threat Emulation
- Anti-Spam
- Remote Access

Available Services

- Reports**
Receive periodic network and security reports by mail
- Logs**
Store security and system logs in cloud servers
- Dynamic DNS**
Assign a persistent domain name
e.g. my-gateway.domain.com
- Firmware Upgrades**
Firmware upgrades management
- Periodic Backup**
Periodically backup the appliance's settings

< | >

Configure Cloud Services

Activate connection to a Cloud Services using:

Activation key:

Activation details:

Service Center:

Gateway ID:























Registration key:

The activation details are supplied by your Cloud Services provider

1-5. License

查看、管理与启用防火墙各功能 License，点击 Offline 可上传 License 文件

License: View, manage and activate your license

Software Blade	Expiration	Service
 Firewall	 Trial (24 days left)	CPSB-FW
 Application Control	 Trial (24 days left)	CPSB-APCL
 URL Filtering	 Trial (24 days left)	CPSB-URLF
 Identity Awareness	 Trial (24 days left)	CPSB-IA
 Advanced Networking	 Trial (24 days left)	CPSB-ADNC
 IPS	 Trial (24 days left)	CPSB-IPS
 Anti-Virus	 Trial (24 days left)	CPSB-AV
 Anti-Bot	 Trial (24 days left)	CPSB-ABOT
 Threat Emulation	 Trial (24 days left)	CPSB-TE
 Anti-Spam	 Trial (24 days left)	CPSB-ASPM
 IPSec VPN	 Trial (24 days left)	CPSB-VPN

Appliance activation is required:

[Activate License](#) | [Offline](#) | [Set proxy](#)

Import Activation File

Activation file:

[Browse...](#)

Download an activation file from your [Check Point User Center account](#) under 'My Products'.

[Close](#)

[Import](#)

1-6. Site Map

查看 Web UI 各功能链接

Site Map: Navigation map of the web application ? Help

<p>Device</p> <p>Network</p> <ul style="list-style-type: none"> Internet Local Network Hotspot Routing DNS Proxy <p>System</p> <ul style="list-style-type: none"> System Operations Administrators Administrator Access Device Details Date and Time DDNS & Device Access Tools <p>Advanced</p> <ul style="list-style-type: none"> High Availability Advanced Settings 	<p>Access Policy</p> <p>Firewall</p> <ul style="list-style-type: none"> Access Policy Control Firewall Access Policy Servers Definition and Access NAT <p>User Awareness</p> <ul style="list-style-type: none"> User Awareness <p>QoS</p> <ul style="list-style-type: none"> Quality of Service Control Quality of Service Policy 	<p>Threat Prevention</p> <p>Threat Prevention</p> <ul style="list-style-type: none"> Threat Prevention Blade Control Threat Prevention Policy Exceptions Infected Hosts <p>Protections</p> <ul style="list-style-type: none"> IPS Protections Threat Prevention Engine Settings <p>Anti-Spam</p> <ul style="list-style-type: none"> Anti-Spam Control Anti-Spam Exceptions
---	--	---

2. Monitoring

2-1. Active Computers

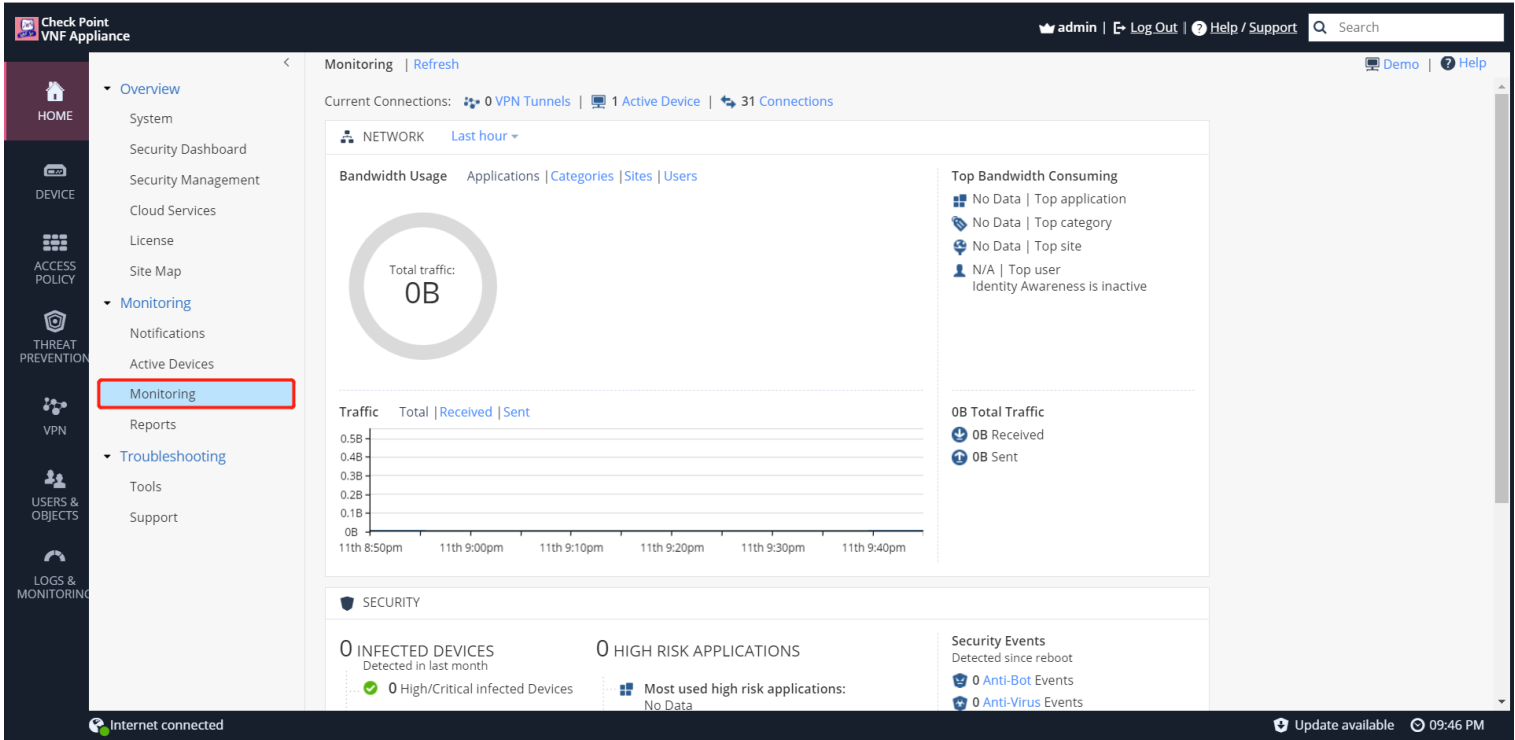
查看连接中的客户端信息(IP、MAC、Services、Interface)

Active Computers: Display devices in the internal networks Print | ? Help


	Object Name	IP/MAC Address	Device/User Name	Services	Interface
🖨️	NB05	192.168.1.5 b8:ca:3a:ce:e8:fa		➔ WebUI, UDP:1900, UDP:5355, Net...	📌 LAN1...

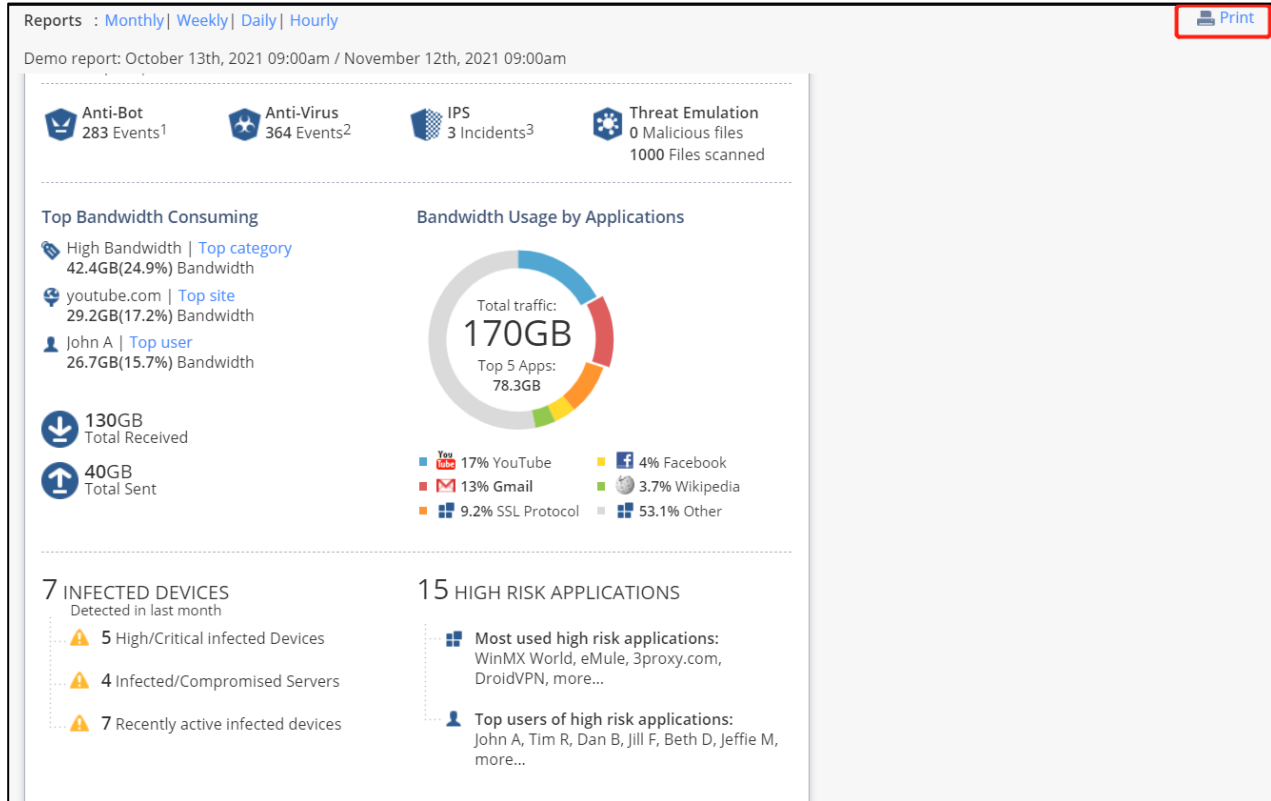
2-2. Monitoring

监控目前网络、安全防护的状态



2-3. Reports

查看当前通过防火墙的网络与防护状态并以图表显示，可点击右上方 Print 图示  Print 打印出本页面中的报表信息。

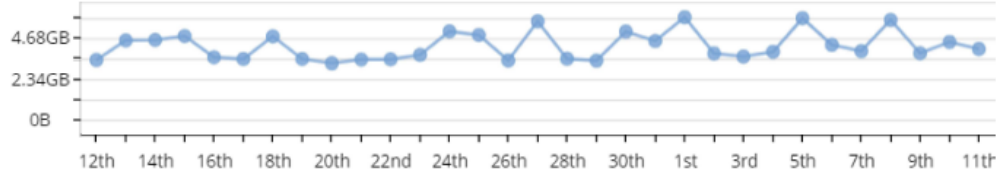


NETWORK USAGE

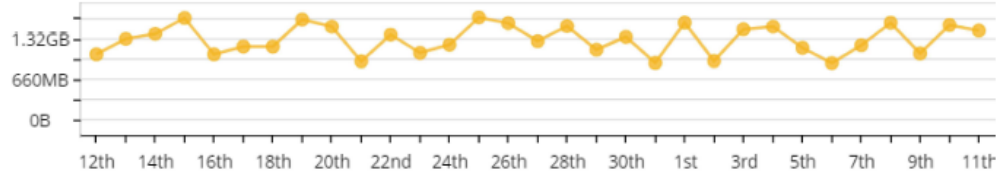
13

Demo report: October 13th, 2021 09:00am / November 12th, 2021 09:00am

Received traffic



Sent traffic



Bandwidth usage

Date	Bandwidth	Received	Sent
Oct 12th	4.42GB	3.38GB	1.04GB
Oct 13th	5.8GB	4.51GB	1.3GB
Oct 14th	5.92GB	4.54GB	1.38GB
Oct 15th	6.4GB	4.76GB	1.64GB
Oct 16th	4.58GB	3.54GB	1.04GB
Oct 17th	4.61GB	3.44GB	1.17GB
Oct 18th	5.91GB	4.74GB	1.17GB
Oct 19th	5.05GB	3.44GB	1.61GB
Oct 20th	4.7GB	3.2GB	1.5GB
Oct 21st	4.34GB	3.41GB	929MB
Oct 22nd	4.79GB	3.42GB	1.37GB
Oct 23rd	4.74GB	3.68GB	1.07GB
Oct 24th	6.23GB	5.03GB	1.2GB
Oct 25th	6.46GB	4.82GB	1.65GB
Oct 26th	4.91GB	3.36GB	1.55GB
Oct 27th	6.87GB	5.61GB	1.26GB
Oct 28th	4.96GB	3.45GB	1.51GB
Oct 29th	4.47GB	3.35GB	1.12GB
Oct 30th	6.35GB	5.02GB	1.33GB
Oct 31st	5.38GB	4.48GB	902MB
Nov 1st	7.41GB	5.84GB	1.56GB
Nov 2nd	4.69GB	3.76GB	934MB
Nov 3rd	5.03GB	3.58GB	1.45GB
Nov 4th	5.35GB	3.85GB	1.5GB
Nov 5th	6.93GB	5.78GB	1.15GB
Nov 6th	5.15GB	4.26GB	899MB



TOP APPLICATIONS

| 4

Hourly report: August 9th, 2017 09:25am / August 9th, 2017 10:25am

Top applications by bandwidth

Application	Risk	Bandwidth	Received	Sent
MSN-web		116KB(32%)	87KB	29KB
Google Services		44.3KB(12%)	21.7KB	22.6KB
DNS Protocol		33.4KB(9.2%)	21.9KB	11.5KB
LDAP-search		28.2KB(7.8%)	14.3KB	13.9KB
TeamViewer		28.1KB(7.8%)	16.5KB	11.5KB
LinkedIn		21KB(5.8%)	17KB	4KB
LINE		13.8KB(3.8%)	6.66KB	7.11KB
Server Message Block (SMB)		12.2KB(3.4%)	3.14KB	9.03KB
Kerberos Protocol		10.3KB(2.8%)	3.79KB	6.49KB
Microsoft Account		6.7KB(1.9%)	5.15KB	1.55KB
All top applications		314KB(87%)	197KB	117KB

Top applications by sessions

Application	Risk	Sessions
DNS Protocol		140
LDAP-search		58
Google Services		8
MSN-web		8
TeamViewer		6
Kerberos Protocol		4
LinkedIn		3
Server Message Block (SMB)		2
Teredo Protocol		2
Microsoft Account		1
All top applications		232

Gateway | R77.20.40 | 00:1C:7F:7C:CD:1D | © 2016 Check Point Software Technologies Ltd.



TOP SITES

| 5

Hourly report: August 9th, 2017 09:25am / August 9th, 2017 10:25am

Top sites by bandwidth

Site	Bandwidth	Received	Sent
10.2.70.1	233KB(64%)	163KB	70.2KB
a248.e.akamai.net	212KB(58%)	192KB	19.1KB
sysage.com.tw	85KB(23%)	52.5KB	32.5KB
bing.com	67.6KB(19%)	58.6KB	9KB
10.2.25.249	33.2KB(9.2%)	28.1KB	5.1KB
adnxs.com	8.41KB(2.3%)	4.88KB	3.53KB
bizographics.com	7.47KB(2.1%)	6.05KB	1.42KB
officeapps.live.com	5.67KB(1.6%)	4.47KB	1.19KB
All top sites	652KB(180%)	510KB	142KB

Top sites by sessions

Site	Sessions
10.2.70.1	7
a248.e.akamai.net	6
bing.com	4
sysage.com.tw	4
10.2.25.249	1
adnxs.com	1
bizographics.com	1
officeapps.live.com	1
All top sites	25



TOP CATEGORIES

| 6

Hourly report: August 9th, 2017 09:25am / August 9th, 2017 10:25am

Top categories by bandwidth

Category	Bandwidth	Received	Sent
Computers / Internet	297KB(82%)	245KB	51.6KB
Uncategorized	266KB(74%)	191KB	75.3KB
Search Engines / Portals	73.3KB(20%)	63.1KB	10.2KB
Inactive Sites	8.41KB(2.3%)	4.88KB	3.53KB
Business / Economy	7.47KB(2.1%)	6.05KB	1.42KB
All top categories	652KB(180%)	510KB	142KB

Top categories by sessions

Category	Sessions
Computers / Internet	10
Uncategorized	8
Search Engines / Portals	5
Business / Economy	1

Hourly report: August 9th, 2017 09:25am / August 9th, 2017 10:25am

SECURITY EVENTS

| 7

Hourly report: August 9th, 2017 09:25am / August 9th, 2017 10:25am

Top potentially high-risk applications by sessions

Application	Risk	Sessions	Bandwidth
TeamViewer		6	22.9KB

Top users of potentially high-risk applications by sessions

No Data

3. Troubleshooting

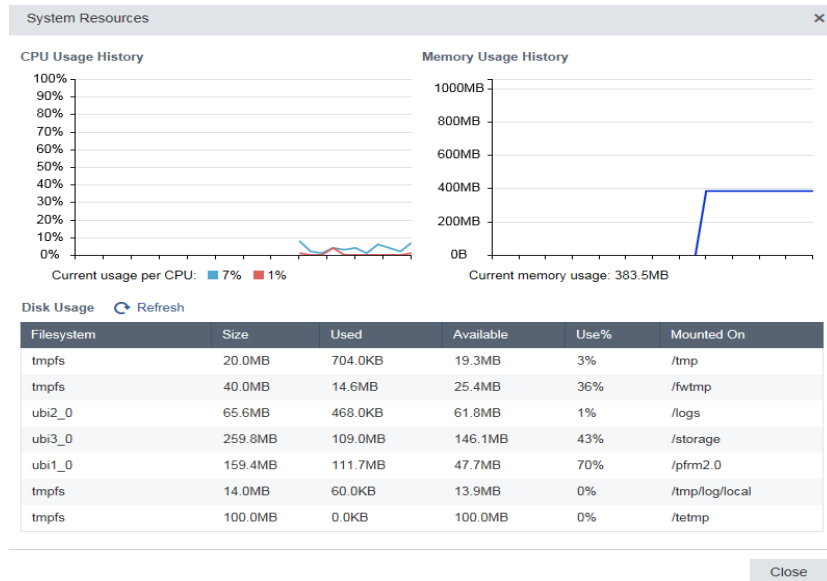
3-1. Tools

提供常用的测试工具让管理员验证或检查时使用

Tools: Various Tools used to diagnose problems with the appliance

- A** **Monitor System Resources** Display CPU usage, memory usage and processes
- B** **Show Routing Table** Display the routing table of the gateway
- C** **Test Cloud Services Ports** Verify that the appliance could connect to Cloud Services
- D** **Generate CInfo File**
- E** **Ping or Trace an IP Address**
 Host name or IP address:
- F** **Perform a DNS Lookup**
 Host name or IP address:
- G** **Packet Capture**
 Select network:

A. Monitor System Resources 查看目前 CPU 与RAM 使用状况



B. Show Routing table 查看目前路由的状况

Command Output

Source	Destination	Service Gateway	Metric	Interface	Origin
Any	default	Any 10.2.70.254	102	wan	static-route
Any	10.2.70.0/24	Any NA	0	wan	connected-route
Any	192.168.1.0/24	Any NA	0	lan	connected-route
Any	192.168.223.0/24	Any NA	0	LAN5Sw	connected-route

C. Test Cloud Services Ports 测试云端服务是否可正常连接

补充：因目前无启用云端服务，因此显示 Unreachable

CLOUD SERVICES PORTS TEST

```

+-----+
| Cloud Services Connectivity Test |
+-----+

+-----+-----+-----+-----+
| Pro | Port | State | Description |
+-----+-----+-----+-----+
| TCP | 18191 | Unreachable | Policy/Configuration f | |
| TCP | 18210 | Unreachable | Management Connection |
| TCP | 18264 | Unreachable | CA's CRL download |
| TCP | 443 | Open | smbmgmtservice.checkpoint.com | Web services (initial connection, upgrad |
| | | | report |
+-----+-----+-----+-----+
  
```

Close

D. Generate CPInfo File 收集并下载 CPInfo 日志文件

Generate CPInfo File Generating CPInfo file: 5% complete

Download CPInfo File Click the Download button to save CPInfo file

E. Ping or Trace an IP Address 输入 IP 或 Host name 即可测试

Ping or Trace an IP Address

Host name or IP address: Ping Traceroute

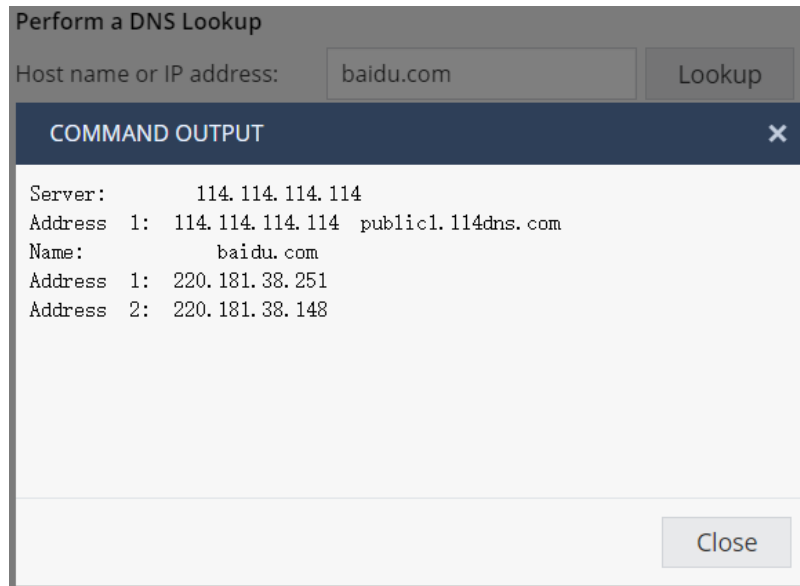
COMMAND OUTPUT

```

PING www.baidu.com (180.101.49.11): 56 data bytes
64 bytes from 180.101.49.11: seq=0 ttl=53 time=9.343 ms
64 bytes from 180.101.49.11: seq=1 ttl=53 time=8.314 ms
--- www.baidu.com ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 8.314/8.828/9.343 ms
  
```

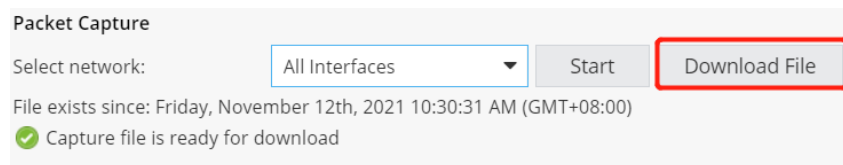
Close

F. Perform a DNS Lookup 输入 IP 或 Host name 进行测试



G. Packet Capture 抓包的界面：

- > 按下 Start 开始抓包记录 →
- > Stop 停止抓包记录 →
- > 点击 Download File 下载对应抓包文件



3-2. Support

查看各種 support 方式



Support: How can we help?

Whether you have an urgent problem or a simple question, we're here to help you by Web or phone.

Contact Technical Support

- [Local guide](#) is the appliance's help files repository.
- [Service Request Tool](#) is your online resource for submitting, updating and tracking service requests.
- [Live Chat](#) provides online support for quick questions about Check Point products and services.
- Our Worldwide Technical Assistance Centers are available to assist you 24x7 (select option #4):
 - Americas: +1 (972) 444 6600 / +1 (888) 361 5030 / +1 (613) 271-7950
 - EMEA: +972 3 611 5100
 - Australia: 1 800 805 793
 - China: +86 1084181958
 - Japan: +81 345 881 101
 - New Zealand: 0800 443 601
 - UK: 0808 101 7399
 - Other Countries: +972 3 611 5100
- [Official support site](#)
- [Download](#) a local manual in PDF format
- [Download](#) Windows driver for a USB-C console socket

Product Information for Support

Appliance: Check Point VNF (SMB-1)
Security Management: Locally managed
Version (Firmware): R80.20.10 (992001203)
MAC Address: 00:0C:29:9D:09:EC

More: [License](#) | [Security Dashboard](#) | [System](#)


三、 Device 設定

1. Network

1-1. Internet

設定 Internet，若想配置多个 Internet 线路可点击 Add an Internet connection 进行设定

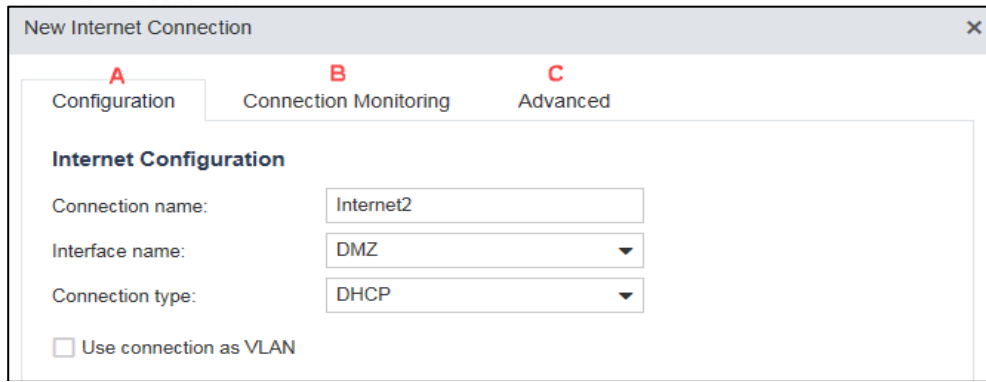
Internet: Manage one or more Internet connections



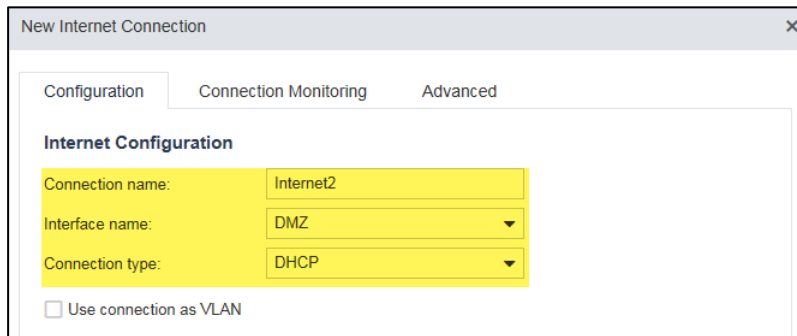
Status: Connected
Static IP | WAN | 192.168.1.20/24 | 11:28:58
6.67% failures, 7.8ms latency | [Connection monitoring...](#)

[Edit](#) [Delete](#) [Disable](#)

[Add an Internet connection...](#)



A配置Internet 的名称 (Connecting name)、选择对应的接口 (Interface name)、连接类型 (Connection type)



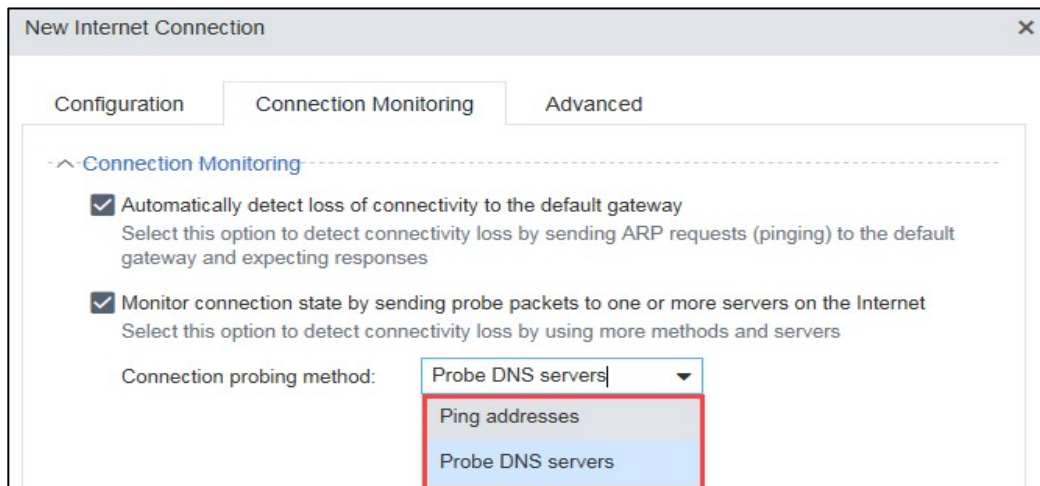
B. Connection Monitoring 选择连接状态的监控方式

B-1. Automatically detect loss of connectivity to the default gateway

Advanced · 使用 **ping default gateway** 来确认网络连接是否正常

B-2. Monitor connection state by sending probe packets to one or more servers on the Internet

· 提供探测 **DNS servers** 或是 **ping 其他 server** 的方式来确认网络连接是否正常





C. Advanced 连接设定(若无特殊需求可采用预设值即可)

C-1. Port Setting 设定MTU、MAC address clone、Disable auto negotiation

Port Settings

Use custom MTU value

MAC address clone:

Use default MAC address 00:1C:7F:7C:CD:1F

Override default MAC address:

Disable auto negotiation

C-2. QoS Settings 启用上传、下载带宽限制

QoS Settings

Enable QoS (download)

Enable QoS (upload)

C-3. ISP Redundancy 设定 HA 的优先级(priority)、Load Balancing 的权重 (Weight)

ISP Redundancy

Route traffic through this connection by default
In order to route traffic through this connection you need to add specific routes through it

High Availability
Upon failure of the primary Internet connection, traffic will be routed according to the selected priority

Priority: (The higher the value, the lower its priority)

Load Balancing
Traffic will be distributed automatically according to the configured load balancing weights

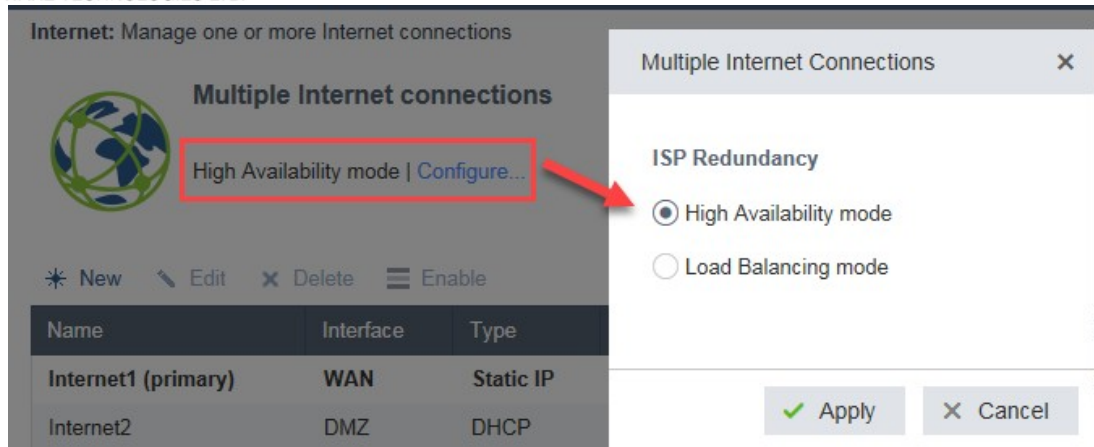
Weight: (50% of the total weight)

C-4. NAT Settings

NAT Settings

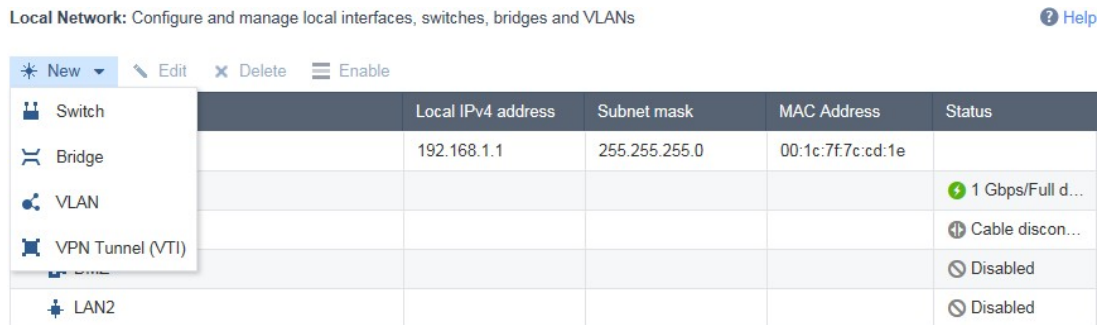
Do not hide internal networks behind this Internet connection

D. 当设定多条 Internet 时可针对多条 Internet 做 High Availability or Load Balancing.



1-2. Local Network

查看与设定 Local Network，点击 New 即可新增 switch、Bridge、VLAN、VPN Tunnel。



A **Switch**：可将多个 Port 绑定成同 VLAN (port based VLANs)，同一个 LAN Switch 的使用同一个 MAC Address，且同 LAN Switch 间的流量不会进行检查或监控。

设定：勾选设定的界面并设定 IP 信息后点击  即完成设定。



(DHCP 可自行決定是否使用)

New Switch

Configuration Advanced DHCPv4 Settings

Switch Configuration

<input type="checkbox"/>	Name
<input type="checkbox"/>	LAN2
<input checked="" type="checkbox"/>	LAN5
<input checked="" type="checkbox"/>	LAN6

Interface Configuration

Assigned to:

Local IPv4 address:

Subnet mask:

Use Hotspot when connecting to network

^ DHCPv4 Server

Enabled

IP address range: -
The device IP address is automatically excluded from the DHCP range

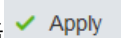
IP addresses exclude range: -

Relay

DHCP server IP address:

Secondary DHCP server IP address:

Disabled

B. Bridge：可將多个接口設定成同一个 Bridge，通过的流量会进行监控或检查。
设定：勾选设定的界面并设定 IP 信息后点击  即完成设定。



(DHCP 可自行決定是否使用)

New Bridge

Configuration Advanced DHCPv4 Settings

Bridge Configuration

- Name
- LAN1 Switch
- DMZ
- LAN2
- LAN5

Enable Spanning Tree Protocol

Interface Configuration

Name:

Local IPv4 address:

Subnet mask:

Use Hotspot when connecting to network

DHCPv4 Server

Enabled

IP address range: -
The device IP address is automatically excluded from the DHCP range

IP addresses exclude range: -

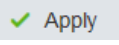
Relay

DHCP server IP address:

Secondary DHCP server IP address:

Disabled

C VLAN : tag based VLANs · 仅设定在 DMZ 或 Lan 的接口中

设定：输入 VLAN ID→勾选需要配置的接口→输入 IP 信息→点击  完成设定

(DHCP 可自行決定是否使用)



New VLAN

Configuration DHCPv4 Settings

VLAN Settings

VLAN ID: 10

Interface Configuration

Assigned to: LAN2

Local IPv4 address: 192.168.100.1

Subnet mask: 255.255.255.0

Use Hotspot when connecting to network

~^~ DHCPv4 Server ~^~

Enabled

IP address range: 192.168.100.1 - 192.168.100.254
The device IP address is automatically excluded from the DHCP range

IP addresses exclude range: [] - []

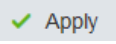
Relay

DHCP server IP address: []

Secondary DHCP server IP address: []

Disabled

D. VPN Tunnel(VTI) : 设定 Route based VPN。

设定：设入 VPN Tunnel ID→输入 VPN 站的名称→有编号 VTI 需设定 Local 与 Remote IP；未编号 VTI 可指定 WAN 接口做为代理接口→点  完成设定。

New VTI

Configuration

VPN Tunnel Settings

VPN Tunnel ID: 2

Peer: RemoteSite

Numbered VTI

Local IPv4 address: []

Remote IP address: []

Unnumbered VTI

Local interface: Internet1

1-3. Hotspot

当管理员启用 Hotspot 功能后，使用者会先连接到 Checkpoint 页面做确认，使用者需同意页面中的内容点击“OK”后连接才会建立，预设 timeout 时间为 240 分钟，超过则需重新确认。

Hotspot: Configure guest access and hotspot Browser-Based Authentication

Hotspot

A ⓘ One network interface is defined for Hotspot | [Configure in Local Network](#)

B ⓘ No network objects are excluded from Hotspot | [No source exceptions...](#) | [No destination exceptions \(advanced\)...](#)

Access

C Require authentication

Allow access to all users

Allow access to a specific group:

D Session timeout: minutes

E [Customize Hotspot portal...](#)

A. 设定启用 Hotspot Lan 页面，点击后会引导至 Local Network 页面，选择需要设定接口点击 Edit→勾选“Use Hotspot when connecting to network”后点击 Apply 完成设定

Local Network: Configure and manage local interfaces, switches, bridges and VLANs ? Help

* New Edit Delete Disable

Name	Local IPv4 address	Subnet mask	MAC Address	Status
LAN1 Switch	192.168.1.1	255.255.255.0	00:1c:7f:7c:cd:1e	
LAN1				1 Gbps/Ful...
LAN3				Cable disc...
DMZ				Disabled

Edit LAN1 Switch

Configuration Advanced DHCPv4 Settings

Switch Configuration

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	LAN1
<input type="checkbox"/>	LAN2
<input checked="" type="checkbox"/>	LAN3
<input type="checkbox"/>	LAN5

Interface Configuration

Assigned to:

Local IPv4 address:

Subnet mask:

Use Hotspot when connecting to network

- B. 设定例外，点击来源“ No source exceptions” 或目的“ No destination exceptions” 后可勾选例外物件进行设定，或点击 New 即可新增 Network Object(设定方法可参考 [二、七、User & Objects 设定 2-5 Network Objects](#))→确定后点击 Apply 完成设定。

Hotspot

- One network interface is defined for Hotspot | [Configure in Local Network](#)
- No network objects are excluded from Hotspot | [No source exceptions...](#) | [No destination exceptions \(advanced\)...](#)

Hotspot Source Network-Objects Exceptions

Type to filter

<input type="checkbox"/>	Object Name	Type
<input type="checkbox"/>	TestLanGroup	
<input type="checkbox"/>	ManageLan	Network
<input type="checkbox"/>	Lan223	IP Range
<input checked="" type="checkbox"/>	Network224	Network
<input checked="" type="checkbox"/>	ManagerIP	Single IP
<input type="checkbox"/>	NB05	Single IP

- C. 设定是否需要身分认证，勾选后可选择所有使用者皆可连线至 internet 或指有特定使用者组才可连线至 Internet。（使用者组请参考 [二、七、User &objects 1-2 Users](#) 设定)

Access

Require authentication

Allow access to all users

Allow access to a specific group:

- D. 设定超时 timeout 时间

Session timeout: minutes

- E. 设定 Hotspot 页面，可自定页面名称与信息，确认后点击 Apply 完成设定

Hotspot Customization ×

Portal Appearance

Portal title:


Portal message:

Terms of use

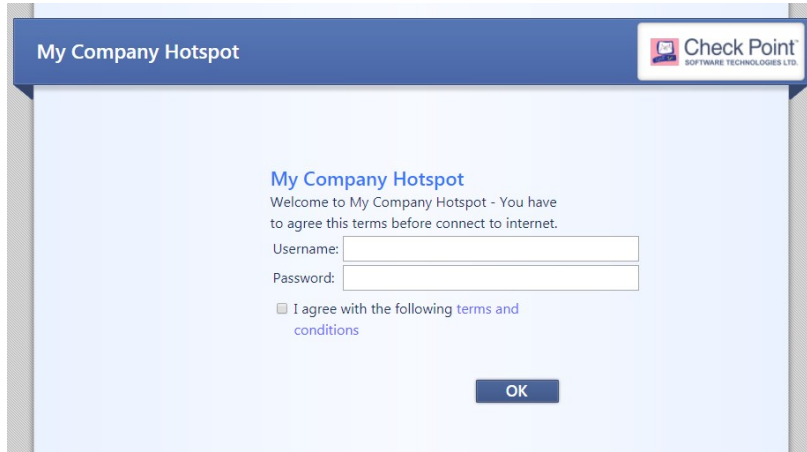
Settings

Redirect the user to a URL after authentication

Displayed Logo

 **Check Point**
SOFTWARE TECHNOLOGIES LTD.

- F. 设定完成后，当使用者连线至 internet 时会先看到 Hotspot 页面，确认后即可正常浏览。



1-4. Routing

新增路由配置信息，点击 **New** 可新增新的路由，点击下图黄标处进行配置

New Routing Rule ✕

Traffic from **any source** to **any destination** that belongs to **any service** should be routed through **next hop**

Destination	Source	Service	Next Hop
Any	Any	* Any	N/A

Comment:

Metric: [0-100]

配置范例如下，配置完成后点击 **Apply** 即设定完成。

New Routing Rule ✕

Traffic from **any source** to **192.168.212.0** that belongs to **any service** should be routed through **192.168.212.254**

Destination	Source	Service	Next Hop
192.168.212.0/24	Any	* Any	192.168.212.254

Comment:

Metric: [0-100]

1-5. DNS

- A. 指定 DNS server(Configure DNS servers)或使用 Internet 所设定的 DNS(Use DNS servers configured for the active Internet connection(s))
- B. 设定是否启用 DNS Proxy



C. 设定 Domain Name(不设定也可)

DNS: Configure DNS and Domain settings for the device

IPv4 DNS

IPv4 DNS Servers

Configure DNS servers

These settings will be applied on all Internet connections

First DNS Server:

Second DNS Server:

Third DNS Server:

Use DNS servers configured for the active Internet connection(s)

IPv4 DNS Proxy

Enable DNS proxy

Relay DNS requests from internal network clients to the DNS servers defined above

Resolve Network Objects

Use network objects as a **hosts list** to translate names to their IP addresses

Domain Name

Domain name:

Apply

Cancel

1-6. Proxy

设定是否使用 Proxy

Proxy: Configure proxy settings for connecting with Check Point update and license servers

Use a proxy server

Host name or IP address:

Port:

2. System

2-1. System Operations

重启设备(Reboot)、还原成预设值(维持目前版本 Default Settings)、还原成出厂设定(Factory Defaults)

Appliance

- Reboot** Reboot the appliance
- Default Settings** Restore factory default settings but keep the current firmware version
- Factory Defaults** Revert to the factory default image and settings. The factory firmware version is R80.20.10 (992001203)

版本更新→手动更新 或还原至前一版本

Firmware Upgrade

The current firmware version is R80.20.10 (992001203)

✔ Firmware is up to date | [Check now](#)

[Configure automatic upgrades...](#)

Manual Upgrade **Revert to Previous Image**

备份与还原系统设定→可设定定期备份机制(点击 **Settings** 设定)、手动备份 (Create Backup File)、依备份还原(Restore)

Backup and Restore System Settings

Periodic backup is OFF **Settings...**

Create Backup File **Restore**

2-2. Administrators

新增管理员账号并赋权限：最高权限 Super Admin、仅能查看 Read-Only Admin、仅能配置网络 Networking Admin

Administrators: Configure administrators for the device [Print](#) | [Help](#)

No RADIUS servers exist | RADIUS configuration...

Type to filter **New** Edit Delete Security Settings

Name	Administrator Role
1 admin	Super Admin
2 ReadOnly	Read-Only Admin
3 NetworkOnly	Networking Admin

2-3. Administrator Access

设定管理员连线方式



Administrator Access: Web (HTTPS) and SSH access for administrators

Select the sources from which to allow administrator access

LAN VPN Internet

Access from the above sources is allowed from

Any IP address
 Specified IP addresses only
 Specified IP addresses from the Internet and any IP address from other sources

Access ports

Web port (HTTPS):

SSH Port:

2-4. Device Details

Device Details: Configure device's name and details

设定设备主机名

Appliance name:

2-5. Date and Time

设定设备时间与时区

Date and Time: Configuring device's date and time manually or using NTP

Current System Time: Tuesday, August 29th, 2017 11:42:03 AM (GMT+08:00) Taipei

Adjust Date and Time

Set date and time manually

Date:

Time: :

Set date and time using a Network Time Protocol (NTP) server

Primary NTP server:

Secondary NTP server:

Update Interval (minutes):

NTP authentication

Shared Secret:

Shared Secret identifier:

Time Zone

Local time zone:

Automatically adjust clock for daylight saving changes

2-6. DDNS & Device Access



设定是否使用 DDNS

DDNS & Device Access: Configure a persistent domain name for the device

DDNS

Connect to the appliance by name from the Internet (DDNS):

Provider:

User name:

Password:

Host name:

Your routable host name, as defined in your DDNS account

Reach My Device

[Register](#) to allow connections to the appliance when it is unreachable from the Internet.

2-7. Tools

与 [二>二、Home>3.Troubleshooting>3-1Tools](#) 相同，提供工具测试

3. Advanced

3-1. High Availability

可将两台设备做 HA，点击 [Configure Cluster](#) 开始设定

Step1. 决定当前设备为主要设备还是次要

New Cluster Wizard Step 1: Gateway Priority ✕

Gateway Priority

Configure as primary member
This appliance is the first to be configured

Configure as secondary member
Primary member has already been configured and this gateway will connect to it

Step2. 设定设备间通信加密密码，[Advanced](#) 设定用与同步两台设备的接口信息(预设是 LAN2)



New Cluster Wizard Step 2: SIC Settings

Secure Internal Communication

This will be used for establishing the initial trust with the other member

Password:

Confirm:

Advanced

Sync Interface

Sync interface:

Sync IP address:

Sync IP subnet:

Other member sync IP address:

Step3 依序设定接口界面是否启用 HA，若设定的 port down 时即启用 HA

New Cluster Wizard Step 3: Gateway Interfaces (1 out of 6)

LAN4

Enable High Availability on Interface

Cluster IP address:

Subnet mask:

Primary physical IP address:

Secondary physical IP address:

Monitor interface state (fail over when interface is down)

Step4 Finish 完成设定

High Availability: Cluster between two appliances

[Help](#)

Enable

Disable

+ This gateway (Primary Member)

+ Peer Gateway [Reinitialize Trust](#)

This gateway is active | Peer gateway is not defined | [View diagnostics...](#)

[Reset Cluster Configuration](#) [Force Member Down](#)

List of Configured Interfaces

[Edit](#)

Name	Status	IP Address	Member IP Address
LAN1	Monitored	192.168.1.1/24	
LAN2	Sync		Primary: 10.231.149.1, Secondary: 10.231.149.2
LAN4	Monitored	192.168.223.4/24	
LAN6	Monitored	172.16.90.1/24	
LAN5:2	Monitored	192.168.2.254/24	
LAN5:3	Monitored	192.168.3.254/24	
Internet1	Monitored	10.2.70.121/24	

3-2. Advanced Settings

查看设备预设的进阶设定内容，点击 **Edit** 可进行编辑

Advanced Settings: Manage very advanced settings of the device

[Print](#) | [Help](#)

⚠ Changing these advanced settings can be harmful to the stability, security and performance of the appliance

Attribute Name	Type	Value	Description
Reach My Device - Ignore SSL certificate	bool	false	Ignore SSL certificate when running Reach My Device
Reach My Device - Server address	url	smbrelay...	Indicates the address of the remote server that allows administrati...
Internet - Reset Sierra USB on LSI error	bool	true	Indicates whether Sierra type USB modems will be reset when the...
Cluster - Use virtual MAC	bool	false	Indicates if a virtual MAC address will be used by all cluster memb...
Threat Prevention Anti-Virus policy - Priority scanning	bool	true	Scan according to security and performance priorities for maximu...
Threat Prevention Anti-Virus policy - File scan size l...	int	0	Indicates the size limit (in KB) of a file scanned by the Anti-Virus e...
Threat Prevention Anti-Virus policy - MIME maximu...	int	7	Indicates the maximum number of levels in nested MIME content t...

四、Access Policy 設定

1. Firewall

1-1. Blade Control

A. Firewall Policy > **Strict** 严谨模式

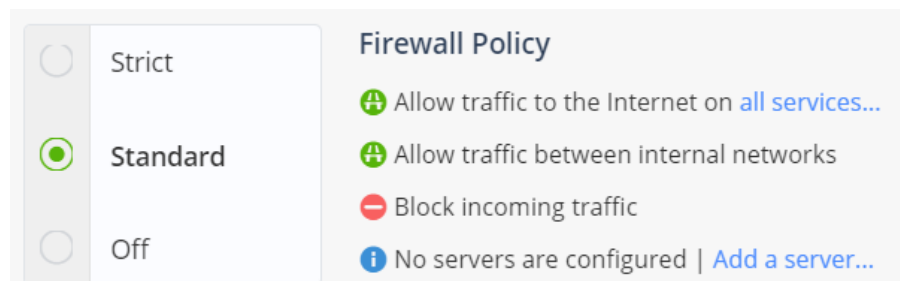
预设 **block 所有流量**，欲放行的流量需要 Firewall > Policy 设定

B. Firewall Policy > **Standard** 标准模式

预设 **允许所有对外流量、允许内部所有流量**，**阻挡(block)**由外部进入的流量

C. Firewall Policy > **off** 关闭

允许所有流量通过



D. Applications & URL Filtering > **On** 启动应用及 URL 过滤功能

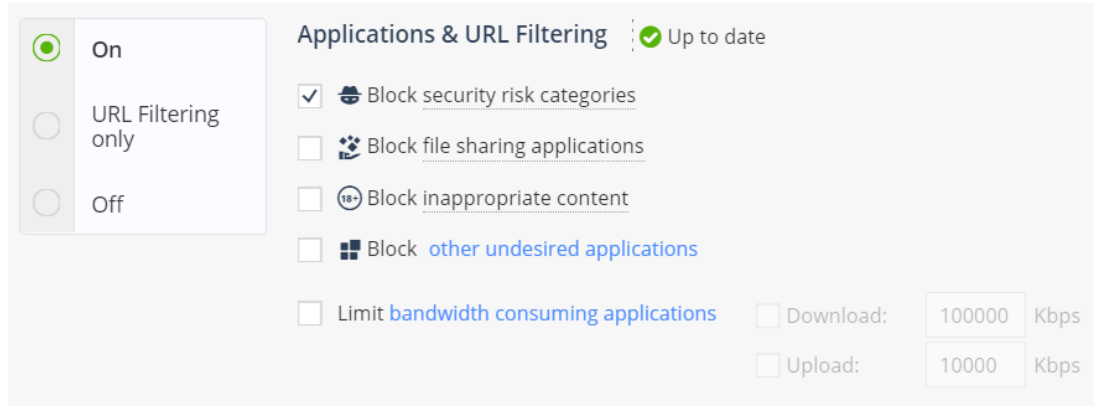
E. Applications & URL Filtering > **URL Filtering only** 仅启用 URL 过滤功能


F. Applications & URL Filtering > **Off** 不启用应用与 URL 过滤功能

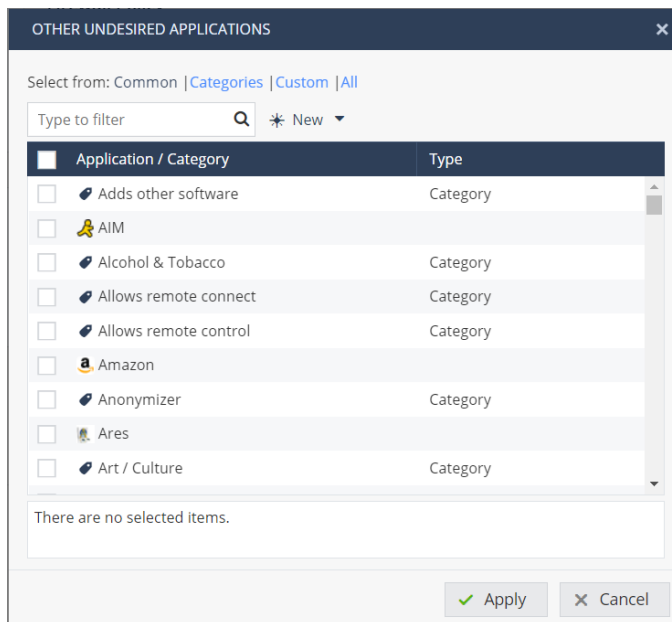


G. 设定 Applications & URL Filtering 预设值

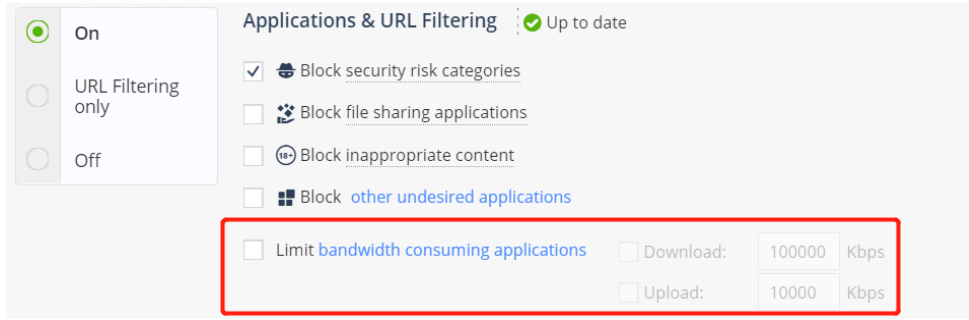
- 可依需求勾选预设阻挡的群组，包含 security risk categories、inappropriate content、file sharing applications 或自订项目 (other undesired applications)。



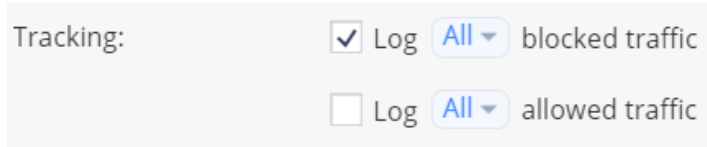
- 点击  可查看该项目阻挡的分类项目，预设类别不可编辑，需要了解细项可以点击 [Check Point AppWiki](#) 查询。



- 勾选 Limit bandwidth consuming applications 可针对设定的应用或URL 限制上传下载带宽



- 勾选 Enable User Awareness 可开启用户访问控制，详细说明参考 [二>四、Access Policy>2 User Awareness](#)。
- 勾选是否记录 允许(allowed)或阻挡(blocked)的流量。

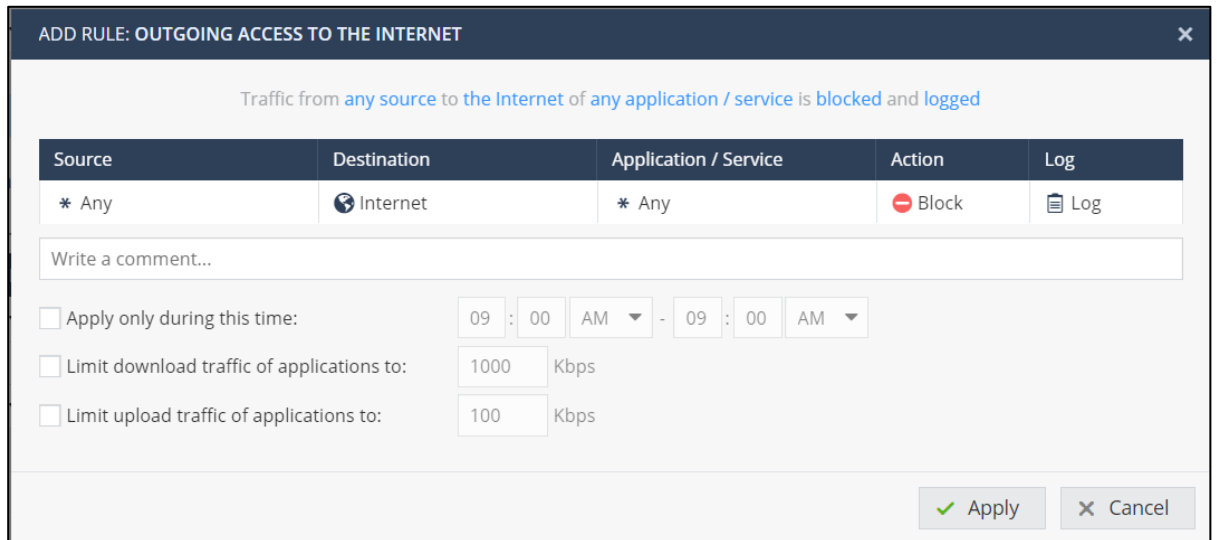


1-2. Policy

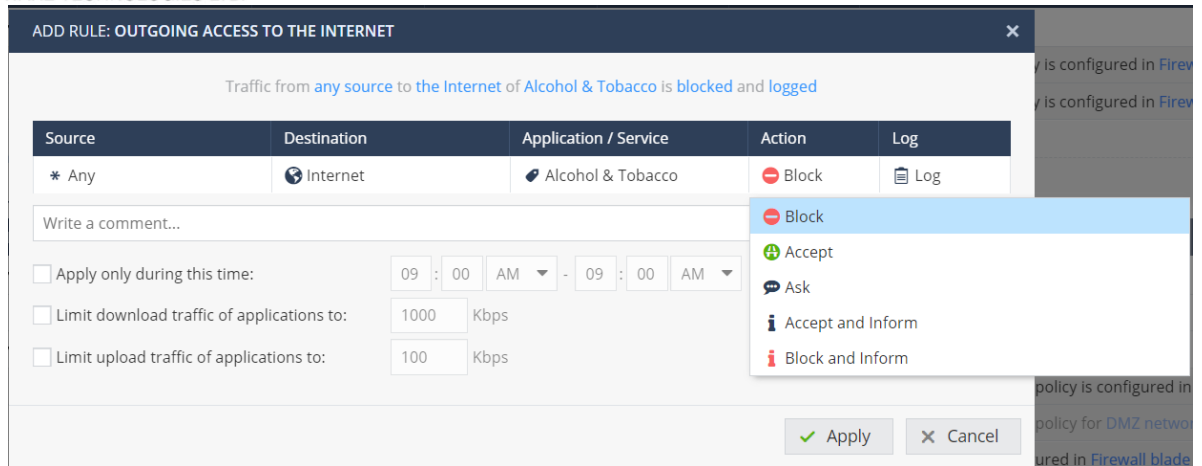
查看与设定 Firewall Policy

- 点击New 新增 Policy

选择来源 (source)、目的 (Destination)、应用 (Application)、服务 (Service)、动作(Action)、记录(Log)，点击 Apply 即设定完成。



当有设定 Application 時，在 Action 的部分可选择阻挡(Block)、放行(Accept)、确认后放行(Ask)、显示 inform 页面确认后放行(Accept and inform)、显示 inform 页面并阻挡(Block and inform)



- 选择 Edit 修改、Delete 删除、Disable 停用 Policy、Clone 复制所选择 policy 进行设定



- Customize Messages 可自定 Ask、Accept and Inform 页面与上传 Logo 图片(Customize)



以 Ask 为例，可输入页面标题、主题、内容，并设定如果确认失败的操作(Accept or Block)以及询问频率 (once a day、once a week、once a month)



Ask Accept and Inform Block and Inform Customize

Message Content

Title: MY Company Application Control

Subject: Are you sure to access?

Body: Access to \$application_name is intended for work-related use only.
Category: \$category.
Reference: \$incident_id

Optional keywords...

Ignore text: I will use this site or application for work-related use only

User must enter a reason

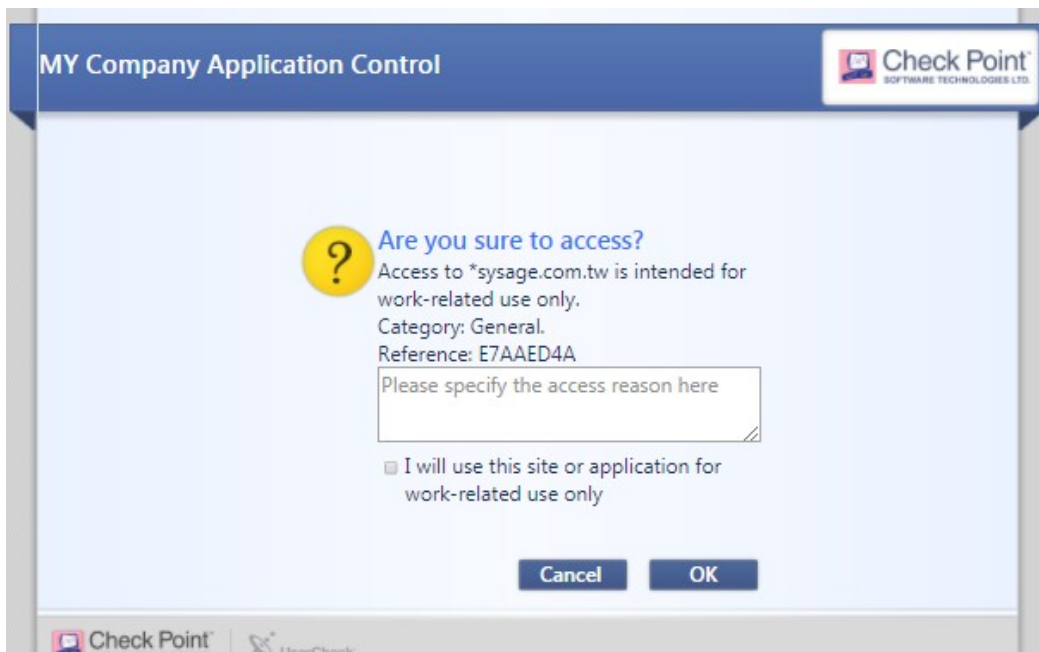
Message Settings

Fallback action: Block

Frequency: Once a day

✓ Apply ✕ Cancel

范例：Ask 页面



1-3. Servers

查看与设定 server 对象，此对象可用于 Policy 或其他设定中被选取。

Servers Definition and Access: Access permissions and NAT for server objects Print | Help

Search: [Type to filter] [New] [Edit] [Delete]

Name	Server Type	IP Address	Ports	Public IP Address	Comments
MailServer1	Mail Server	192.168.10.2	TCP: 25, 110, 143		

1-4. NAT

启用 NAT 与设定 NAT rules

NAT: Configure NAT (Network Address Translation) for outgoing traffic and forwarding NAT rules for incoming traffic

Outgoing Traffic

ON Hide internal networks behind the Gateway's external IP address

NAT Rules

[New Server (forwarding rule)] | Hide NAT rules

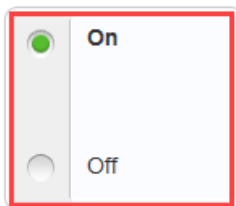
[New] [Edit] [Delete] [Enable]

No.	Original Source	Original Destinati...	Original Service	Translated Sourc...	Translated Destin...	Translated Servic...	Comment
Manual NAT Rules							
1	lan-30	* Any	* Any	FW-out (hide)	* Original	* Original	

2. User Awareness > Blade Control

User Awareness: Incorporate users into access policy and display users in security logs

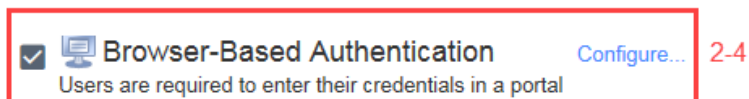
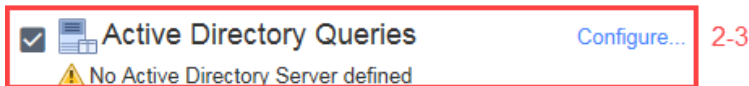
2-1



User Awareness

[Configuration wizard...](#) 2-2

Policy configuration



2-1. 启用或关闭用户访问控制，可基于用户账号来做限制并 LOG 记录

➢ 启用后在 log 中的 User 一栏可看到用户账号

Security Logs: Monitor Check Point security logs, created by the appliance

Enter search query... Refresh Query Syntax View Details Clear Logs Options

Time	User	Blade	Interface	Action	Source	Destination	Service	Rule	Description
Today 10:43:21	NB07	Identity Awa...		Log...	192.168...				Session Expiration: Session...
Today 10:41:17	NB07	Identity Awa...		Log in	192.168...				Successful Login: User and...
Today 10:44:41		URL Filtering	WAN	Allow	192.168...	216.58.2...	HTTPS	3 (Outgoing)	tpc.google syndication.com...
Today 10:39:18		Application...	WAN	Allow	192.168...	216.58.2...	HTTPS	3 (Outgoing)	Google Calendar was allowed
Today 10:11:43	NB07	Identity Awa...		Log...	192.168...				Session Expiration: Session...
Today 10:11:37	NB07	Firewall	LAN3	Acce...	192.168...	192.168...	TCP/6690	Default poli...	Accepted on rule Default po...

2-2. 点击 Configuration wizard 可进入引导设定，configuration 勾选设定也可

User Awareness Wizard

Methods for identifying users

Active Directory Queries
Seamless detection via your local AD server

Browser-Based Authentication
Users are required to enter their credentials in a portal

2-3. 启用 AD server 识别用户身份(Active Directory Queries)，勾选后可点击 Configure 设定 AD server 配置信息

Active Directory Queries [Configure...](#)

No Active Directory Server defined

Active Directory Queries

Use existing Active Directory servers

Define a new Active Directory server

Domain: nico.com

IPv4 address: 192.168.223.60

User name: administrator

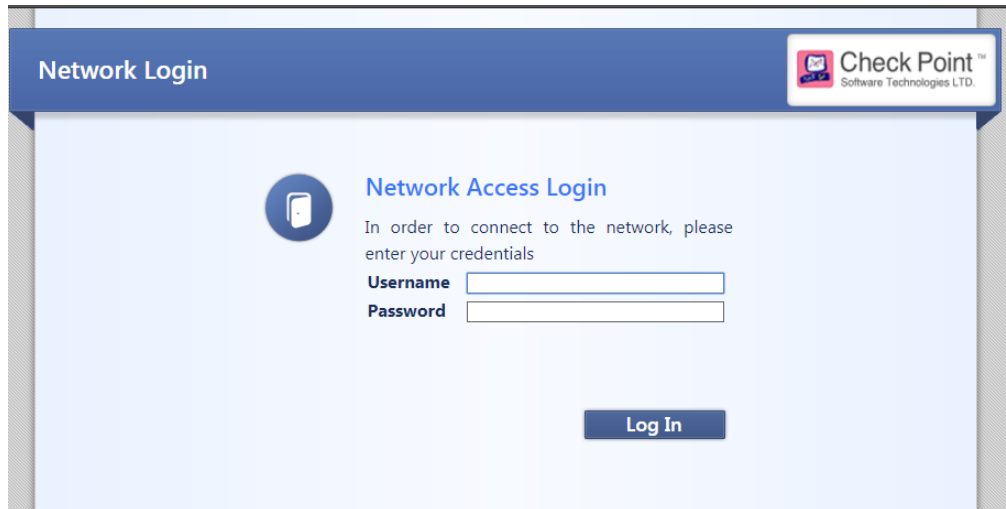
Password:

User DN: [Discover](#)

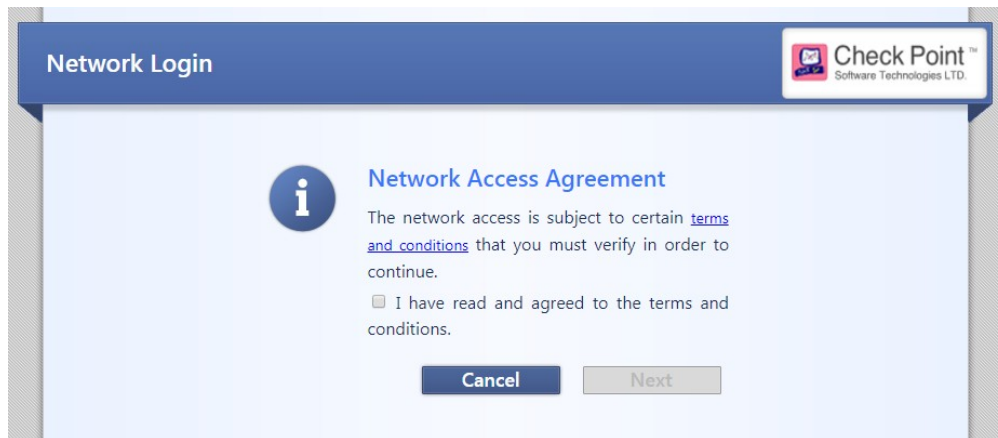
Use user groups from specific branch only

2-4. 启用浏览器登入(Browser-Based Authentication)来识别用户身份，当用户开启浏览器尝试登入受保护的网站时，需要先登入验证身份后方可继续

➤ 启用 Browser-Based Authentication 后开启受保护网站，会显示 Login 页面。



➤ 登入后可查看规定(terms and conditions) · 同意后点击 Next 即可正常浏览页面





3. QoS

3-1. Blade Control

- A. 启用或关闭 QoS 功能
- B. QoS 预设 Policy 设定(QoS Default Policy)
 - B-1. 确保敏感性低延迟服务的带宽
(Ensure low latency for delay sensitive services)
 - B-2. 确保所有 VPN\service 的带宽
(Guarantee % of the bandwidth to VPN traffic on all services)
 - B-3. 限制特定应用服务的带宽
(Limit bandwidth consuming applications)

Quality of Service Control: Manage bandwidth by configuring Quality of Service (QoS) policy

On QoS
 Off


 QoS options are not selected for the configured Internet connection | [Internet connections](#)
 No manual QoS rules configured


QoS Default Policy



Ensure low latency for [delay sensitive services](#) (e.g. VoIP)
 Guarantee % of the bandwidth to [VPN traffic](#) on [all services](#)
 Limit [bandwidth consuming applications](#)

3-2. Policy


配置 QoS Policy

 Blade is not active (QoS). [Dismiss](#)

Quality of Service Policy: Manage bandwidth by configuring Quality of Service (QoS) policy rules  Help

 Limit [bandwidth consuming applications](#) is disabled
 Limit low latency traffic to 20% of bandwidth

* New Edit Delete Enable


No.	Source	Destination	Service	Guarantee/Limit	Weight	Track	Comment
1	* Any	* Any	 Delay sensitiv...	Latency: low	10	— None	Note: Ensure low latency for Delay Sensitive Services (
2	* Any	* Any	* Any (encrypted)	20% / -	10	— None	Note: Guarantee bandwidth for all services
3	* Any	* Any	* Any	- / -	10	— None	Note: Default QoS policy

五、Threat Prevention 设定




1. Threat Prevention

1-1. Blade Control

启用或关闭 IPS、Anti-Bot、Anti-Virus、Threat Emulation 功能，点击 Edit 可做详细设置。

 **0** infected devices [More details](#)

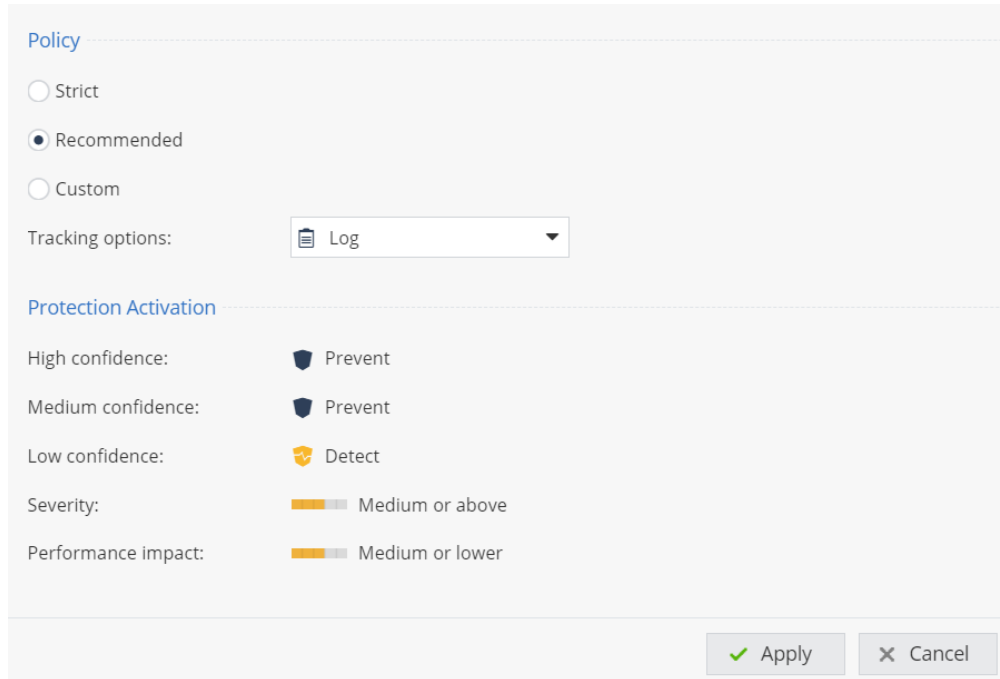
Threat Prevention (Powered by SandBlast Cloud)

ON IPS  Updating...
 ON Anti-Virus  Update available
 ON Anti-Bot  Update available
 OFF Threat Emulation

[Schedule](#) updates

A. Edit IPS

选择IPS 的防御机制，有 Strict(严谨安全防御)、预设选项 Typical(提供安全与性能最佳效果)、Custom(自定义)三中

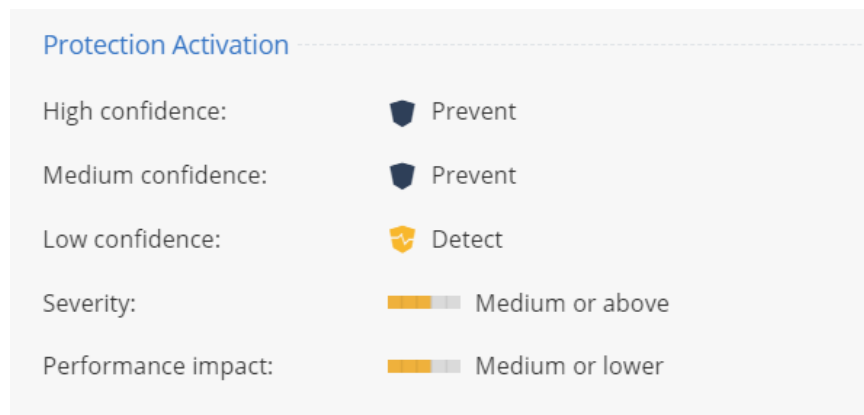


The screenshot shows the 'Edit IPS' configuration page. Under the 'Policy' section, three radio buttons are present: 'Strict', 'Recommended' (which is selected), and 'Custom'. Below this is a 'Tracking options' dropdown menu set to 'Log'. The 'Protection Activation' section contains several settings: 'High confidence' is set to 'Prevent' (shield icon); 'Medium confidence' is set to 'Prevent' (shield icon); 'Low confidence' is set to 'Detect' (shield with checkmark icon); 'Severity' is set to 'Medium or above' (yellow bar); and 'Performance impact' is set to 'Medium or lower' (yellow bar). At the bottom right, there are 'Apply' and 'Cancel' buttons.

- > Severity –严重等级.
- > Confidence-level –信任等级
- > Performance impact – 启用此 IPS 防护时性能影响程度


IPS 所设定的列表可在后续 [Threat Protection>Protect>IPS Protections](#) 查看



B. Edit Anti-Bot& Edit Anti-Virus& Threat Emulation







This screenshot is a zoomed-in view of the 'Protection Activation' section from the previous image. It shows the same settings: High confidence: Prevent; Medium confidence: Prevent; Low confidence: Detect; Severity: Medium or above; Performance impact: Medium or lower.

1-2. Exceptions

例外设定，可针对特定条件设定例外不阻挡，点击  **New** 即可新增设定。

Threat Prevention Policy Exceptions: Configure exceptions for specific traffic so it is not blocked by Threat Prevention protections  | 

Threat Prevention Exceptions

 New  Edit  Delete  Whitelists






No.	Source	Destination	Protection	Service	Action	Log	Comment
Add threat prevention exception							

1-3. Infected Hosts

查看受感染的主机

Infected Hosts: Display infected hosts and servers in the internal networks


 **0** infected hosts



Type to filter   Refresh  Filter  Add Protection Exception  View Host Logs



Object Name	IP/MAC Address	Device/Us...	Incident Type	Severity	Protection...
No items were found					





































































2. Protections

2-1. IPS Protections

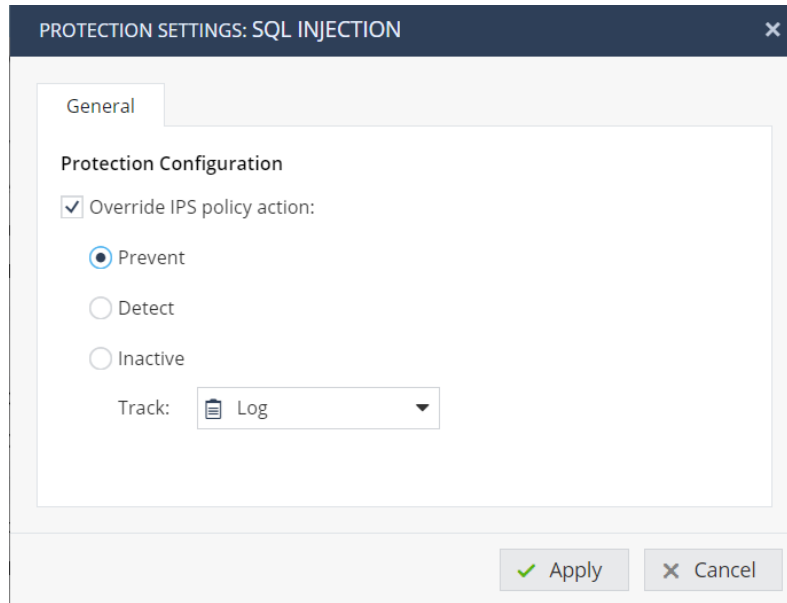
查看 IPS Protections 列表，可针对特定 policy 点击  **Edit** 单独调整该策略的执行动作

IPS Protections: Monitor protections list and manually configure specific protections to override general policy  Print |  Help

Type to filter   Edit

Protection	Protection Type	Category	Action	Severity	Confidence Le...	Performance Imp...
SYN Attack	Server/Client Protection	TCP	 Inactive	 High	 High	 Critical
Sequence Verifier	Server Anomaly	TCP	 Inactive	 High	 Mediu...	 Low
LAND	Server/Client Protection	Denial of Service	 Prevent	 Medium	 Mediu...	 Very-low
Ping of Death	Server/Client Protection	Denial of Service	 Prevent	 Medium	 Mediu...	 Very-low
Small PMTU	Server/Client Anomaly	TCP	 Inactive	 High	 High	 Critical
Teardrop	Server/Client Anomaly	Denial of Service	 Inactive	 High	 Mediu...	 Very-low
Max Ping Size	Server/Client Anomaly	IP and ICMP	 Prevent	 Medium	 High	 Very-low
Non-TCP Flooding	Server/Client Anomaly	Denial of Service	 Inactive	 High	 Mediu...	 Low
Network Quota	Server/Client Anomaly	IP and ICMP	 Inactive	 High	 Mediu...	 Critical
Dynamic Ports	Server/Client Anomaly	Network Security	 Inactive	 Medium	 High	 Very-low
Inbound DNS Request	Server Protection	Cache Poisoning	 Inactive	 High	 Low	 Critical
Mismatched Replies	Server/Client Protection	Cache Poisoning	 Inactive	 High	 Mediu...	 Critical
Scrambling	Server/Client Protection	Cache Poisoning	 Inactive	 High	 Mediu...	 Critical
Non Compliant DNS	Server/Client Anomaly	DNS	 Inactive	 Critical	 Medium	 Low
Unknown Resource Record	Server/Client Anomaly	DNS	 Inactive	 Medium	 Low	 Low
DNS Data Overflow	Server/Client Protection	DNS	 Inactive	 Critical	 Mediu...	 Low
DNS Maximum Request Len...	Server/Client Anomaly	DNS	 Inactive	 Low	 Mediu...	 Low

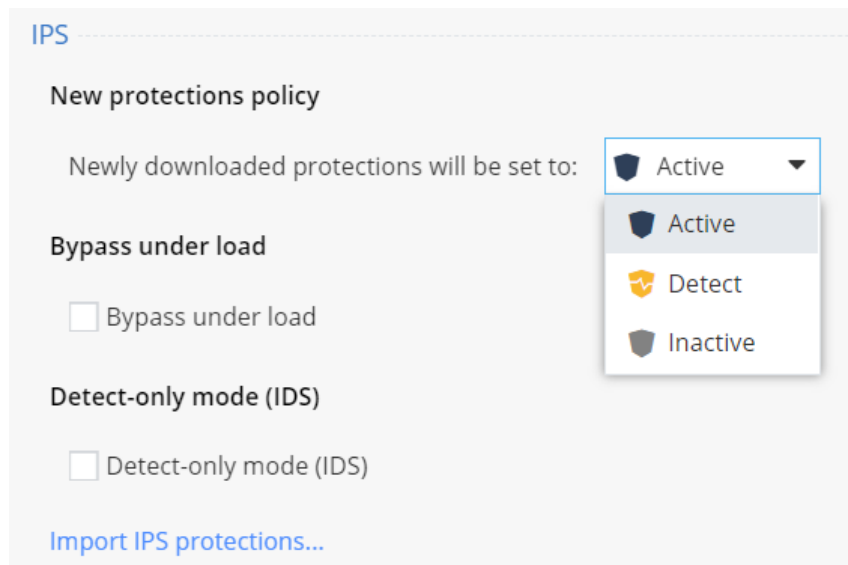
« < Page 1 of 242 > » 1-50 of 12071



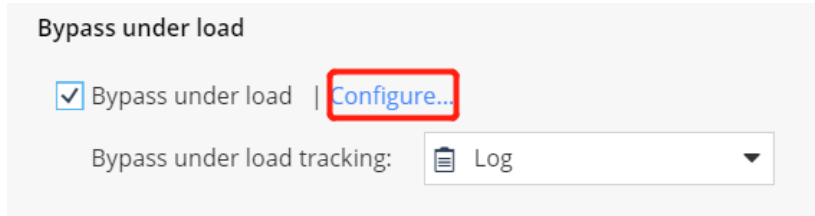
2-2. Engine Settings

进阶设定扫描引擎，可依实际需求进行调整

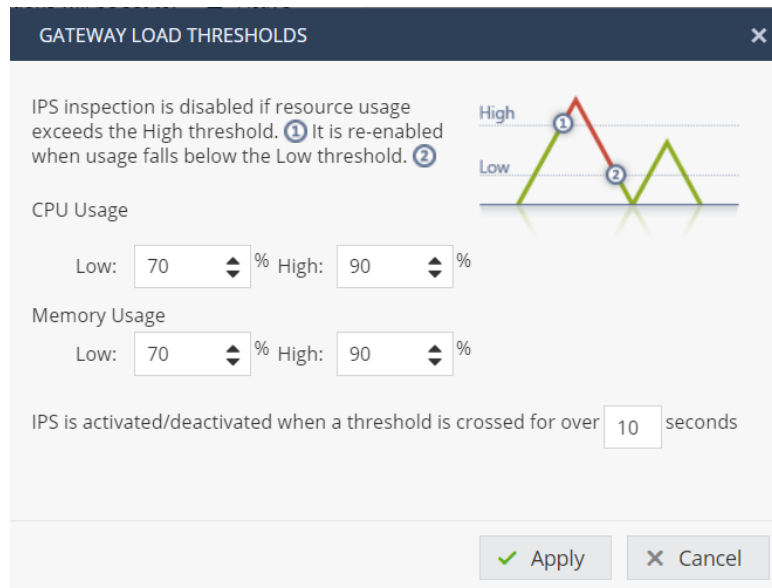
- A. 设定 IPS 新策略：指定IPS新更新的策略条目的执行动作，默认是Active，另有 Detecte和Inactive。



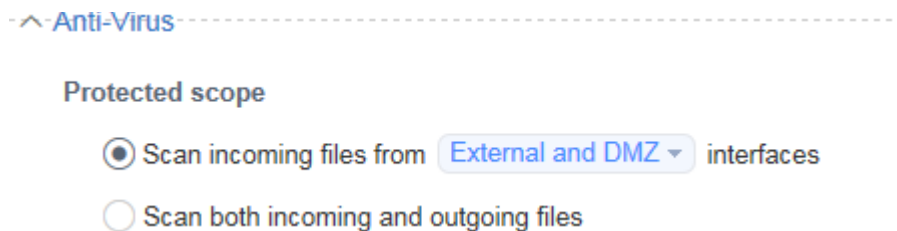
- B. 设定当前设备负载超过限制时不进行检查，勾选后即会显示 Configure，可点击进行设定



范例：当设备 CPU 高于 90%时停止 IPS，低与 70%时启用 IPS



- C. 设定 **Anti-Virus** 防护范围，预设为扫描从外部接口进入如 External and DMZ





D. 设定 **Anti-Virus** 扫描协议 Http、Mail、FTP

Scanned protocols

- HTTP (on any port)
- Mail (SMTP and POP3)
- FTP

E. 设定 **Anti-Virus** 文件类型处理方式：处理已知的病毒文件类型(Process file types known to contain malware)、处理所有文件类型(Process all file types)、自定义文件类型处理方式(Process specific file types families)

File types policy

- Process file types known to contain malware
- Process all file types
- Process specific file types families | [Configure...](#)

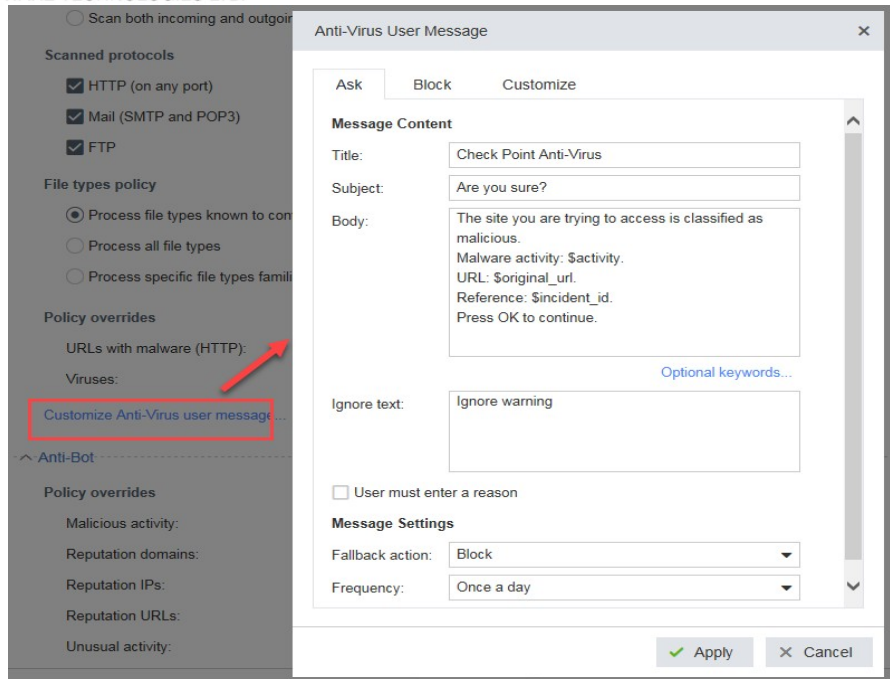
F. 设定 **Anti-Virus** 策略已覆盖 Threat Prevention 中常规定义的 policy，若无特殊需求可不用调整

Policy overrides

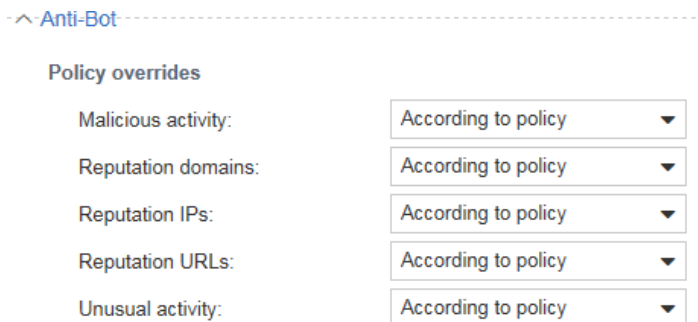
URLs with malware (HTTP):	<input type="text" value="According to policy"/>
Viruses:	<input type="text" value="According to policy"/>

G. 设定 **Anti-Virus** 的 Ask、Block 页面信息，与设定 Access Policy 时的 Ask 页面设定方法相同

以 Ask 为例，可输入页面标题、主题、内容，并设定若确认失败时的动作(Accept or Block)与询问频率 (once a day、once a week、once a month)

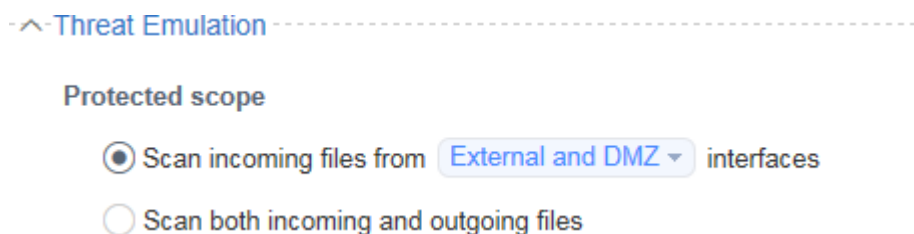


H. 设定 **Anti-Bot** 策略已覆盖 Threat Prevention 中常规定义的 policy，若无特殊需求可不用调整



I. 设定 **Anti-bot** 的 Ask、Block 页面信息，与 G 设定 Anti-virus 设定方法相同

J. 设定 **Threat Emulation** 的防护范围，预设为扫描外部接口进来的流量如 External and DMZ，或选择扫描所有出入文件 Scan both incoming and outgoing files



K. 选择 **Threat Emulation** 扫描协议，有 HTTP、Mail(SMTP)

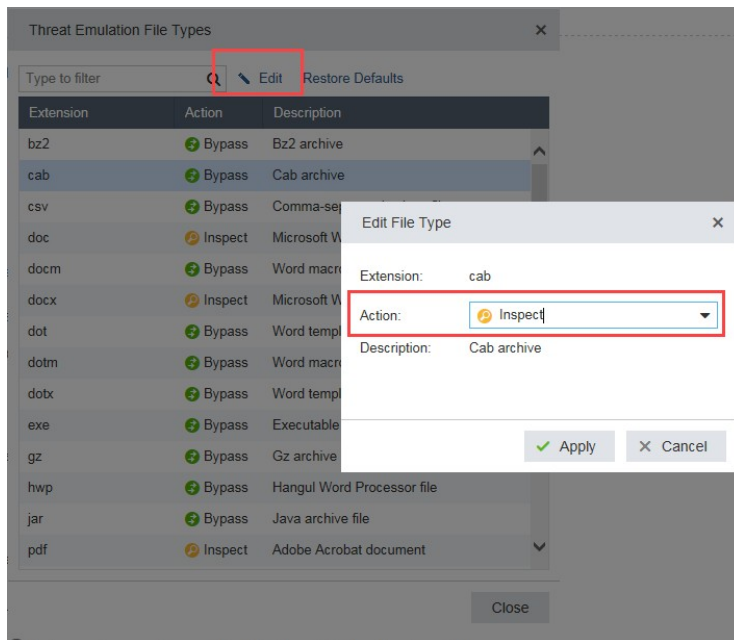
Scanned protocols

- HTTP (on any port)
- Mail (SMTP)

L. 设定 **Threat Emulation** 分析的文件类型，点击 **Configure** 进行设定

File types policy

Process specific file types families | **Configure**



M. 选择需 **Threat Emulation** 扫描时，该文件的处理模式：

Background 当文件仍在分析时此文件会下载完成(预设)；

Hold 当文件仍在分析時此文件会被 block，直到分析完成确认没问题时才会完成下载。

HTTP connection emulation handling mode

- Background - connections are allowed until emulation handling is complete
- Hold - connections are blocked until emulation handling is complete

3. Anti-Spam

3-1. Blade Control

启用或关闭 Anti-Spam 功能



Anti-Spam Control

On
 Off
 Anti-Spam

Detect-only mode

3-2. Exceptions

手动建立允许或阻挡名单，点击 NEW 可使用 ip 或 domain 設定

Anti-Spam Exceptions: Manually configure IP addresses and email addresses to be exempt from inspection or blocked

[Help](#)

Allow List	Block List
Type to filter <input type="text"/> <input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	Type to filter <input type="text"/> <input type="button" value="New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
Sender / Domain / IP Address	Sender / Domain / IP Address
192.168.223.70	Add a new Sender / Domain / IP Address

Block the Following:

IP address

Sender / Domain

六、VPN 設定

1. Remote Access

1-1. Blade Control

- A. 启用或关闭 Remote Access 功能
- B. 选择连接 VPN Remote Access 方式

On
 Off
 Remote Access
A

No local users and groups are defined with VPN Remote Access permissions

Static IP for Remote Access:





Allow traffic from Remote Access users

Log traffic from Remote Access users

Require users to confirm their identity using two-factor authentication | [Configure...](#)



VPN Remote Access users can connect via:

-  **Check Point VPN clients**
Connecting laptops/desktops with Check Point's VPN client software | [How to connect...](#)
-  **Mobile client**
Enable VPN remote access mobile clients to connect via Check Point Mobile VPN client | [How to connect...](#)
-  **SSL VPN**
Enable VPN remote access clients to connect via SSL VPN | [How to connect...](#)
-  **Windows VPN Client**
Enable VPN remote access clients to connect via native VPN client (L2TP) | [How to connect...](#)

B

B-1. Check Point VPN clients 使用在电脑的客户端连接VPN (預設勾選)

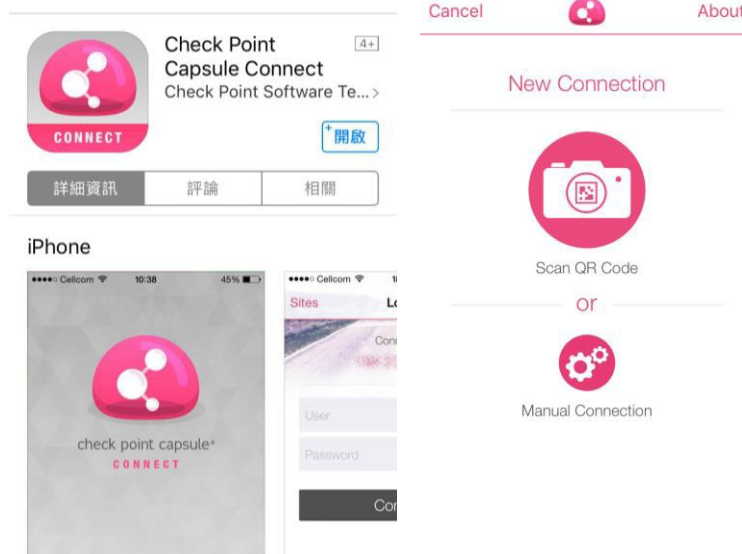
B-2. Mobile client 通过手机 app 连接 VPN

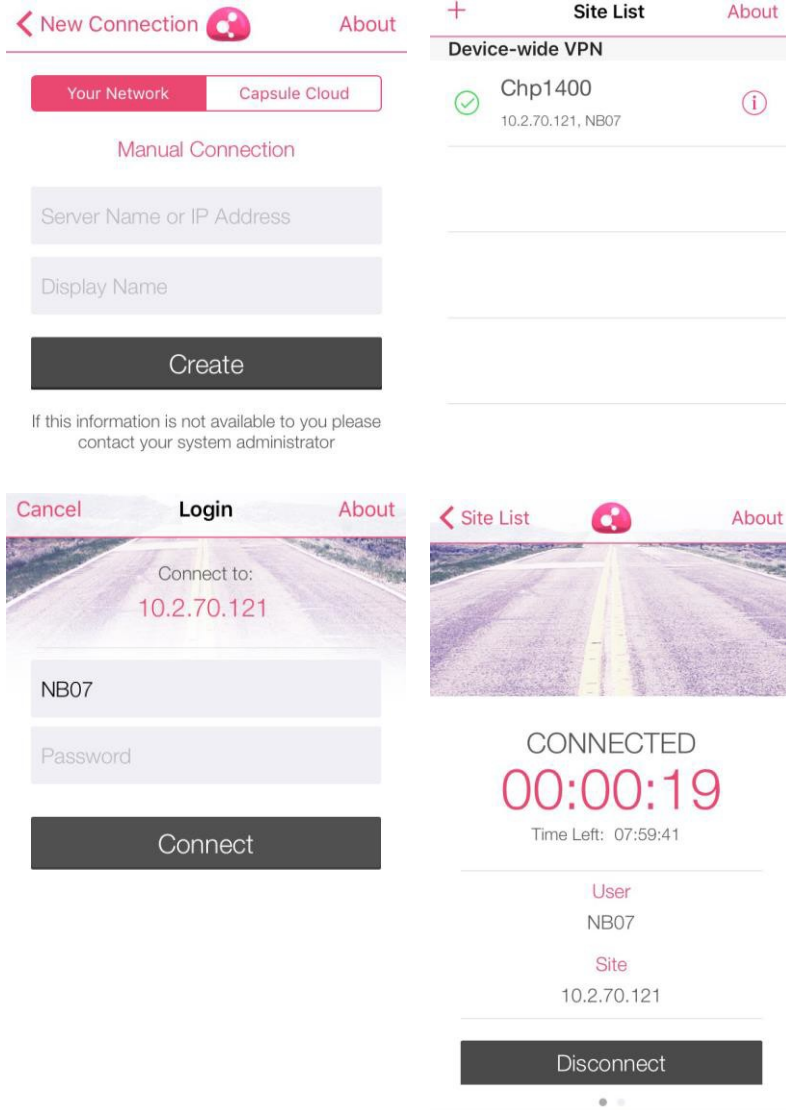
Step1. 预先下载 Check Point Capsule Connect APP (下图以 IOS 为例)

Step2. 设定连接

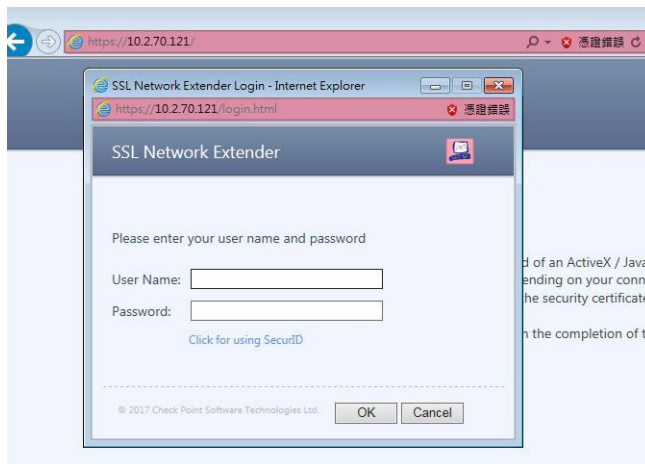
Step3. 输入需要的账号密码

Step4. 连接成功

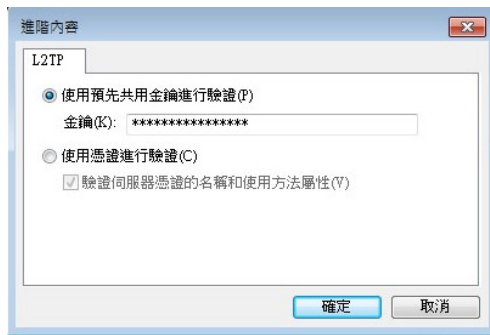
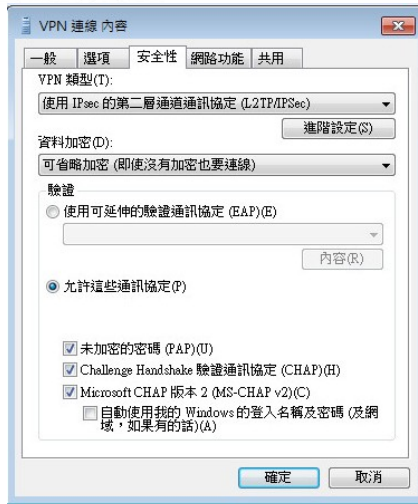




B-3. SSL VPN 通过 Browse SSL VPN 连接，输入账号密码进行连接



B-4. Windows VPN Client 通过电脑建立 VPN 连接



1-2. Remote Access Users

设定允许访问的用户者

Remote Access Users: Configure remote access permissions for users and groups

i No authentication servers are defined. Add [Active Directory](#) / [RADIUS](#) server

Type to filter

	Name	Remote Access	Comments
	NB07	User permissions	
	NB04	User permissions	
	NB01	User permissions	
	ManagerGroup	Group permissions	

A. 设定允许 Remote Access 的用户，点击 Add 可新增

New Local User ✕

Remote Access SSL VPN Bookmarks

User name:

Password:

Confirm:

Comments:

Temporary user

Remote Access permissions

B. 点击Edit Permissions 给与现有用户的使用权限

Edit Remote Access Permissions ✕

Selected (3):

Users RemoteUse1 NB07

Filter: Users | [Active Directory](#)

Type to filter

	Name
<input checked="" type="checkbox"/>	NB07
<input checked="" type="checkbox"/>	RemoteUse1
<input type="checkbox"/>	vpnuser

1-3. Authentication Servers

与 [二>七、Users&Objects>1-4 Authentication Servers](#) 相同

1-4. Advanced

Remote Access Advanced Settings: Configure additional advanced options for VPN remote access users

Office Mode - Allocate IP addresses from the following network:

Office Mode Network: A

Office Mode Subnet:

Route Internet traffic from connected clients through this gateway B

Local encryption domain is defined [automatically according to topology...](#)

DNS servers for Remote Access users:

Office mode first DNS for clients: [Configure manually](#) C

Office mode second DNS for clients:

Office mode third DNS for clients:

DNS domain name: [Configure manually](#)

SSL VPN Bookmarks

Type to filter Q * New ✎ Edit ✕ Delete

Label	Type	URL
No items were found		

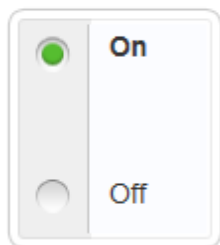
- A. 设定连接 VPN 后访问的网段
- B. 是否允许Client 通过 gateway 连接到 Internet
- C. 设定连接 VPN 的 DNS Server

2. Site to Site

2-1. Blade Control

启用或关闭 Site to Site VPN 功能

Site to Site VPN Control



Site to Site VPN

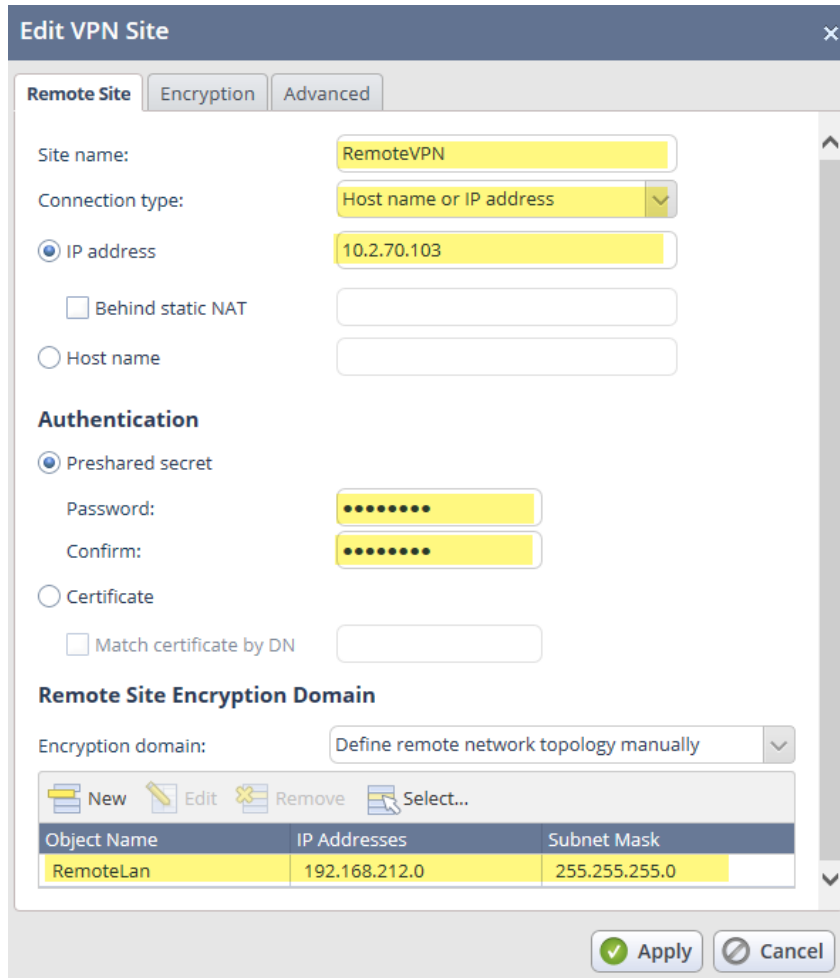
- i One VPN Site defined | [VPN Sites](#)
- Allow traffic from remote sites (by default)
- Log remote sites traffic (by default)

2-2. VPN Sites

A. 点击 New 建立或 Edit 编辑 VPN Site

B. 依次输入 Site Name、Connection Type、Authentication、选取 Remote Site Encryption Domain

> Remote Site Encryption Domain 可点击 New 新增如 RemoteLan (范例)· 若已有对应配置的话可点击 Select 选取即可



Edit VPN Site

Remote Site | Encryption | Advanced

Site name: RemoteVPN

Connection type: Host name or IP address

IP address: 10.2.70.103

Behind static NAT

Host name

Authentication

Preshared secret

Password: [REDACTED]

Confirm: [REDACTED]

Certificate

Match certificate by DN

Remote Site Encryption Domain

Encryption domain: Define remote network topology manually

Object Name	IP Addresses	Subnet Mask
RemoteLan	192.168.212.0	255.255.255.0

Apply Cancel

C. 切换到 Encryption 页面确认加密方式，需要与连接的 VPN sites 相同



NEW VPN SITE

Remote Site Encryption Advanced

Encryption settings: Default (Most compatible)

IKE (Phase 1)

Encryption: 3DES, AES-128, AES-256

Authentication: MD5, SHA1, SHA256

Diffie-Hellman group support: Group 2 (1024 bit), Group 14 (2048 bit)

Renegotiate every: 1440 minutes (24 hours)

IPSec (Phase 2)

Encryption: 3DES, AES-128, AES-256

Authentication: MD5, SHA1, SHA256

Enable Perfect Forward Secrecy (better security, affects performance)

Diffie-Hellman group support: Group 2 (1024 bit)

Renegotiate every: 3600 seconds (60 minutes)

Apply Cancel

D. 切换到 Advanced 页面确认高级设定

NEW VPN SITE

Remote Site Encryption Advanced

Settings

Remote gateway is a Check Point Security Gateway

Enable Permanent VPN Tunnels

Disable NAT for this site
Connections opened to this site will use the original IP addresses, even if hide NAT is defined.

Allow traffic to the internet from remote site through this gateway

Encryption method

Encryption method: IKEv1

Enable aggressive mode for IKEv1

Use Diffie-Hellman group:

Initiate VPN tunnel using this gateway's identifier

Gateway ID:

Type: Domain name

Additional Certificate Matching

Remote site certificate should be issued by: Any Trusted CA

Apply Cancel



E. 建立完成后可点击 Test 确认隧道是否建立成功

VPN Sites: Configure remote VPN sites

Type to filter

Site Name	Host Name / IP Address
RemoteSite	192.168.220.100
Remotelan	172.16.90.3

Testing connection to Remotelan

Testing VPN site tunnel...

2-3. VPN Tunnels

查看已建立 VPN 的状态

VPN Tunnels: Monitor all VPN tunnels

Type to filter

From	Site Name	Peer Address	Status
No VPN tunnels found			

2-5. Advanced配置连接 VPN 的傳出與來源介面達到最佳路徑，預設值是由設備自行決定

Site to Site VPN Advanced Settings: Configure additional advanced options for Site to Site VPN

Local encryption domain is defined [automatically according to topology...](#)

Link selection

Outgoing interface selection:

- According to the routing table
- Route based probing

Source IP address selection:

- Automatically chosen according to outgoing interface
- Manually configured:

Tunnel health monitoring:

Tunnel health monitoring method:

Use DPD (Dead Peer Detection) responder mode

Encryption Method

IKEv2 global gateway ID:

3. Certificates

3-1. Trusted

管理信任的认证，可点击 **Add** 新增外部证书文件(.crt)，配置当前设备的认证

Trusted CAs: Manage trusted certificate authorities

Type to filter	Q	* Add	Edit	Delete	Export	Sign a Request
Trusted CA	Expiration					
Internal CA	Wed Aug 12 18:39:06 2037					

3-2. Installed Certificates

管理已安装证书，可建立新的认证或导出.p12，.pfx 憑證

Installed Certificates: Create and manage appliance certificates

Print | Help

Type to filter	Q	* New Signing Request	Details...	Delete	Export	Upload Signed Certificate	☰
Installed Certificate	Expiration	Status					
Default Certificate	Wed Aug 17 18:39:17 2022	Verified					

3-3. Internal Certificate

可查看内部 Site to Site VPN 与设备初始化时设备内部所使用的自签证书信息，

点击 [Export Internal CA Certificate](#) 可导出自签证书。



Internal Certificate: Display the appliance Internal CA certificate and Internal VPN certificate

Reinitialize Certificates Replace Internal CA Export Internal CA Certificate Sign a Request

Internal CA Certificate

i The internal CA certificate is the certification which authenticates the internal CA to sign on the internal certificates

Certificate: O=00:1C:7F:24:C5:BB..mos57g
Not valid before: Friday, December 3rd, 2021 06:12:58 AM
Not valid after: Friday, January 1st, 2038 11:14:07 AM
Fingerprint: FAT DEAN OVAL CARD POT CUNY SUNK QUOD FLAM AUTO ASKS REEF

Internal VPN Certificate

i The internal VPN certificate is the certificate used for this appliance to authenticate itself on VPN based certificate configurations

Certificate: CN=00:1C:7F:24:C5:BB VPN Certificate,O=00:1C:7F:24:C5:BB..mos57g
Not valid before: Friday, December 3rd, 2021 06:13:06 AM
Not valid after: Tuesday, December 3rd, 2024 06:13:06 AM
Fingerprint: CALL HUGO WINK GIN BURT CASK GAG HIVE SUDS BELL JULY TIME
CRL Distribution: http://my.firewall:18264/ICA_CRL1.crl

七、Users & Objects 設定

1. User Management

1-1. User Awareness

参考[四-2 User Awareness](#) 設定

1-2. Users

点击 New 新增用户/用户组

Users: Create and edit permissions for users and groups









Type to filter

Name
No users defined. Add a new user

- Local user
- Users Group

Users: Create and edit permissions for users and groups

Type to filter * New

	Name	Remote Access	Comments
	NB07	 User permissions	
	NB04	 User permissions	
	NB01	 User permissions	
	ManagerGroup	 Group permissions	

1-3. Administrators

与 [三、2-2 Administrators](#) 相同

1-4. Authentication Servers

新增认证服务器 RADIUS Servers 或 AD Server

> 新增AD server

Step1. 点击 New 或 Add 配置 AD server 服务器

Authentication Servers: Create and edit authentication services that will be used in user definition

RADIUS Servers

No RADIUS servers exist | [Configure...](#)

 Remote access [permissions for RADIUS users](#) are disabled

Active Directory

Type to filter * **New**

Domain	Server IP	User Name
Add new AD Domain		


Step2. 输入 AD server 的配置 > Discover User DN > Apply

New Active Directory Domain ✕

Domain:

IPv4 address:

User name:

Password: 

User DN:

Use user groups from specific branch only

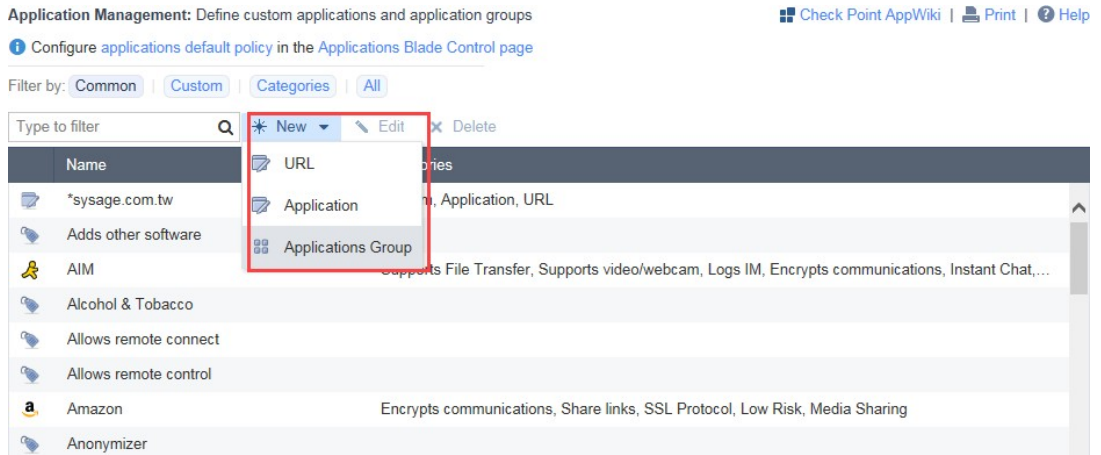
2. Network Resources

2-1. Servers

与三>四、[Access Policy 设定](#)>1-3 Servers 相同

2-2. Applications & URLs

查看现有配置或点击 **New** 可新增自定义项目



范例 新增 URL

New URL
✕

http(s):// ✕

✔ Apply
✕ Cancel

2-3. Services

查看现有配置或点击 **New** 可新增自定义条目、**Edit** 编辑、**Delete** 删除自定义条目

Services: Change system services' configuration and create/edit new service objects Print | Help

Type to filter ✱ New ✎ Edit ✕ Delete

	Name	Type	IP Pr...	Destination Ports	Comments
	HTTP	↔ TCP	6	80, 3128, 8080	Hypertext Transfer Protocol
	FTP	↔ TCP	6	21	File Transfer Protocol
	PPTP_TCP	↔ TCP	6	1723	Point-to-Point Tunneling Protocol, extension of PPP
	SNMP	↔ UDP	17	161	Simple Network Management Protocol
	TFTP	↔ UDP	17	69	Trivial File Transfer Protocol
	SSH	↔ TCP	6	22	Secure shell, encrypted and authenticated rsh
	TELNET	↔ TCP	6	23	Telnet Protocol
	SMTP	↔ TCP	6	25	Simple Mail Transfer Protocol
	IMAP	↔ TCP	6	143	Interactive Mail Access Protocol

2-4. Service Groups

配置或新增 Service 组

Service Groups: Change system service groups' configuration and create/edit new service groups

Type to filter ✱ New ✎ Edit ✕ Delete

	Name	Type	Comments
	DNS	Group	Domain Name system services
	Mail	Group	Mail protocols
	NetBios	Group	Network Basic Input-Output System
	Web	Group	Web protocols
	Any_TCP_UDP	Group	Any TCP-UDP services
	Delay_Sensitive_Services	Group	Delay sensitive services
	Guaranteed_Bandwidth_Services	Group	Guaranteed Bandwidth Services
	VoIP	Group	VoIP Protocols
	SIP	Group	Session Initialization Protocols, used in VoIP
	NewGroup	Group	



新增 Service Group

New Service Group

Name:

Comments:

Type to filter

Services	Comments
No items were found	

点击select 可勾选当前的 service，或是使用 New 新增 service

Select Services

Services	Comments
<input checked="" type="checkbox"/>	HTTP Hypertext Transfer Protocol
<input type="checkbox"/>	FTP File Transfer Protocol
<input type="checkbox"/>	PPTP_TCP Point-to-Point Tunneling Protocol, extension of P...
<input checked="" type="checkbox"/>	SNMP Simple Network Management Protocol
<input type="checkbox"/>	TFTP Trivial File Transfer Protocol
<input checked="" type="checkbox"/>	SSH Secure shell, encrypted and authenticated rsh
<input type="checkbox"/>	TELNET Telnet Protocol
<input type="checkbox"/>	SMTP Simple Mail Transfer Protocol
<input type="checkbox"/>	IMAP Interactive Mail Access Protocol
<input type="checkbox"/>	POP3 Post Office Protocol - Version 3
<input type="checkbox"/>	NNTP Network News Transfer Protocol
<input type="checkbox"/>	DNS_UDP Domain Name System Queries

Selected items (3):

点击 Apply 后完成设定

✕
New Service Group

Name:

Comments:

Type to filter 🔍 ✳️ New ✕ Remove 📄 Select..

Services	Comments
HTTP	Hypertext Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure shell, encrypted and authenticated rsh

✔️ Apply ✕ Cancel

2-5. Network Objects

查看、新增、编辑、删除网络对象，建立的对象可供做 policy 或其他设定时使用

Network Objects: Create and edit network objects that will be used in the device's feature configuration 🖨️ Print | 🆘 Help

Type to filter 🔍 ✳️ New ✎ Edit ✕ Delete

Object Name	Type	IP Addresses
ManageLan	🌐 Network	192.168.1.0/255.255.255.0
Lan223	🌐 IP Range	192.168.223.1-192.168.223.10
Network224	🌐 Network	192.168.221.0/255.255.255.0
ManagerIP	🌐 Single IP	192.168.1.4

点击New 新增，可选择网段(Network)、单一 IP(Single IP) 或是 IP 范围(IP Range)，输入后点击 Apply 完成设定

✕
New Network Object

Type:

Network ▼

Network address:

Single IP

Subnet mask:

IP Range

Object name:

Network

2-6. Network Object Groups



查看、新增、編輯、刪除網路物件群組

Network Object Groups: Create and edit network objects groups that will be used in the device's feature configuration

Type to filter Q * New Edit Delete

Name	Type	Comments
TestLanGroup	Group	

点击 New 可进行网络对象组的配置

New Network Object Group ×

Name:

Comments:

Type to filter Q * New Remove Select...

点击 Select 可勾选现有 Network Object 对象或点击 New 新增 Network Object 并加入此 Group

Select Network Objects ×

* New

<input type="checkbox"/>	Network Objects
<input type="checkbox"/>	ManageLan
<input type="checkbox"/>	Lan223
<input checked="" type="checkbox"/>	Network224
<input checked="" type="checkbox"/>	ManagerIP
<input type="checkbox"/>	NB05
<input type="checkbox"/>	NetworkObject172

八、Logs & Monitoring

1. Logs

2-1. Security Logs

查看通过 Firewall 的日志

Security Logs: Monitor Check Point security logs, created by the appliance ? Help

Enter search query... Refresh Query Syntax View Details Clear Logs Options

Time	U...	Blade	Interface	Action	Source	Destination	Service	Rule
Today 17:03:24		Firewall	WAN	Accept	10.2.70.239	239.255.255...	Stop local logging	Default policy (Incoming/...
Today 17:03:05		Firewall	WAN	Accept	10.2.70.239	10.2.70.255	Eject SD card safely	Default policy (Incoming/...
Today 17:02:59		Firewall	WAN	Accept	10.2.70.136	10.2.70.255	NetBIOSDatagram	Default policy (Incoming/...
Today 17:02:48	N...	Firewall	LAN1	Accept	192.168.1.5	216.58.200.2...	HTTPS	Default policy (Outgoing)
Today 17:02:48	N...	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)
Today 17:02:48		Firewall	WAN	Accept	10.2.70.90	255.255.255...	UDP/5246	Default policy (Incoming/...

A. 输入关键字段或相关条件进行搜索

Security Logs: Monitor Check Point security logs, created by the appliance ? Help

DNS Refresh Query Syntax View Details Clear Logs Options

Time	U...	Blade	Interface	Action	Source	Destination	Service	Rule
Today 17:02:48	N...	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)
Today 17:02:38	N...	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)
Today 17:01:59	N...	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)

B. 更新 Log

点击Refresh实时刷新日志数据

User:NB07 Refresh Query Syntax View Details Clear Logs Options

Time	User	Blade	Interface	Action	Source	Destination	Service	Rule
Today 17:06:42	NB07	Firewall	LAN1	Accept	192.168.1.5	216.58.200.46	HTTPS	Default policy (Outgoing)
Today 17:06:41	NB07	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	168.61.146.25	HTTPS	Default policy (Outgoing)
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	23.101.30.126	HTTPS	Default policy (Outgoing)
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Outgoing)

C. 选择对应日志点击后查看详细日志

Log Details

Accepted on rule Default policy (Outgoing) < Prev > Next

Log Info		More	
Time	Today 17:06:41	Description	Accepted on rule Default policy (Outgoing)
Blade	Firewall	Inzone	Internal
Product Family	Network	Out-Zone	External
Type	Log	Service ID	DNS_UDP
Policy		Session ID	61baa884
Action	Accept	XlateDPort	0
Rule	Default policy (Outgoing)	XlateDst	0.0.0.0
Traffic		XlateSport	12124
Source	192.168.1.5	XlateSrc	10.2.70.121
Destination	10.2.25.2	NAT Rule Number	0
Service	UDP/53	NAT Additional Rule N...	0
Interface Direction	inbound		
Protocol	17		
Destination Port	53		
Source Port	64584		
Service Name	DNS_UDP		
Source User Name	NB07		

D. 清除日志

点击Clear logs，清楚日志

Security Logs: Monitor Check Point security logs, created by the appliance

Enter search query... Refresh Query Syntax View Details **Clear Logs** Options

Time	Blade	Interface	Action	Source	Destination	Service	Rule
Today 11:11:34	Firewall	WAN	Drop	192.168.30.1	192.168.30.255	NetBIOSDatag...	
Today 11:07:44	Firewall	WAN	Drop	192.168.30.1	192.168.30.255	NetBIOSName	
Today 11:07:44	Firewall	WAN	Drop	192.168.30.1	192.168.30.255	NetBIOSName	
Today 11:03:11	URL Fi...						
Today 11:03:06	Applic...						

E. 查看选项

Options > Stop local logging 停止本地记录，再点击一次可恢复

2-2. System Logs

查看系统日志

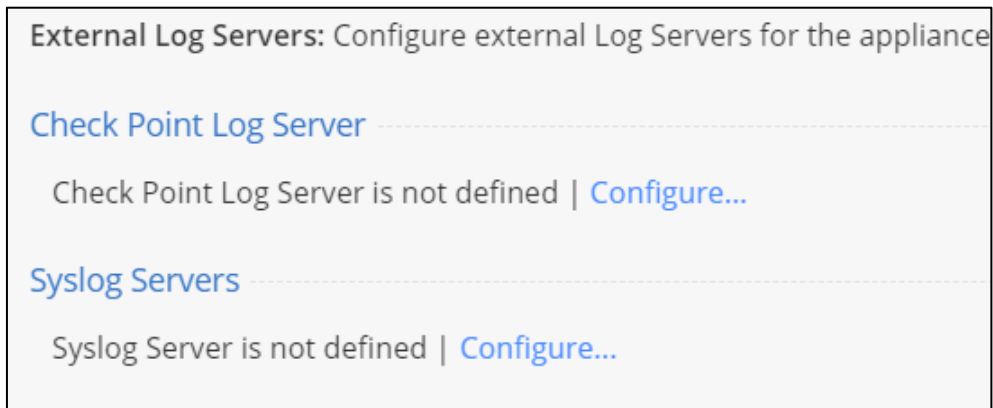
System Logs: Monitor system logs, created by the appliance

Refresh Clear Logs Download Full Log File

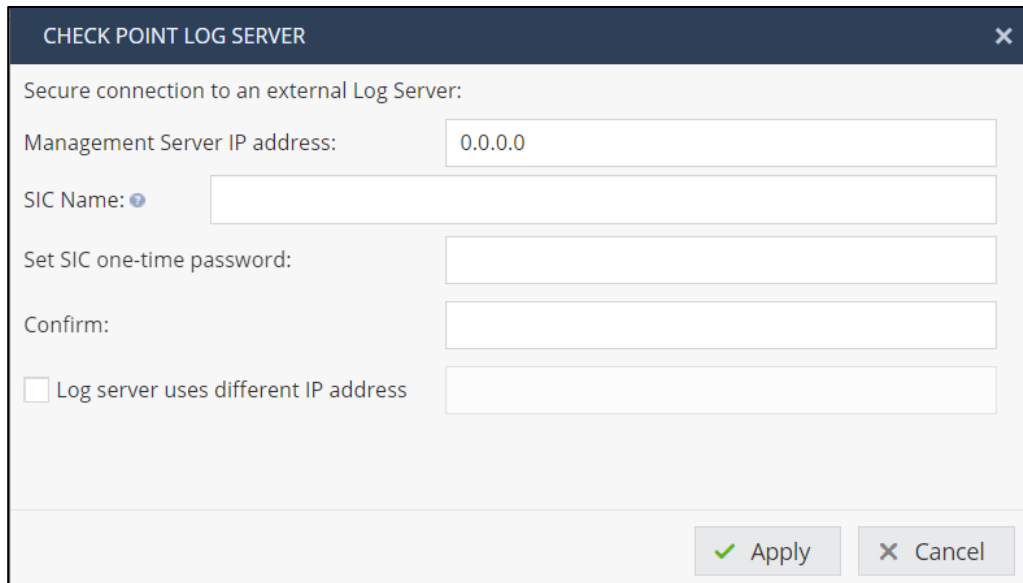
Time	Type	Details
11:20:40 05 Dec 2021	Info	[AUDIT] [Inteface: WEB] 'admin' updated logs configuration
11:20:38 05 Dec 2021	Info	[AUDIT] [Inteface: WEB] 'admin' updated logs configuration
11:19:42 05 Dec 2021	Info	[AUDIT] [Inteface: WEB] 'admin' updated logs configuration
11:19:37 05 Dec 2021	Info	[AUDIT] [Inteface: WEB] 'admin' updated logs configuration

2-3. External Log Servers

配置外部 Log Server，可配置为另一台 Check Point Server 或 Syslog Server



- A. Check Point Log Server：点击 Configure→输入另一台 Check point 管理设备的 IP、SIC 名称、SIC 密码后点击 Apply 确认



CHECK POINT LOG SERVER

Secure connection to an external Log Server:

Management Server IP address:

SIC Name:

Set SIC one-time password:

Confirm:

Log server uses different IP address

- B. Syslog Servers 点击 Configure→输入Server 配置→选择要传送的 Log 类型，确认后按下 Apply 即完成配置

Syslog Server ✕

Name:

IP address:

Port:

Enable log server

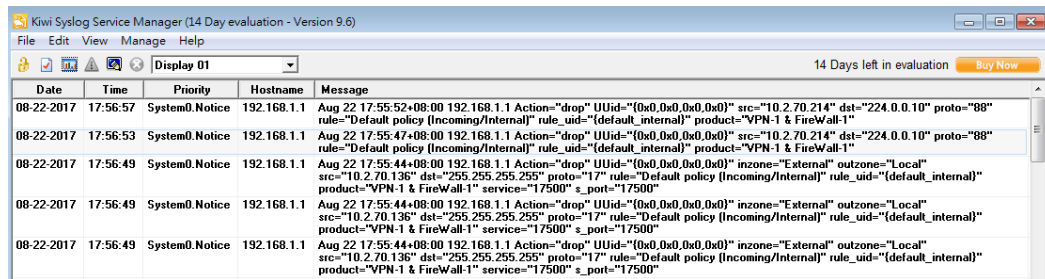
Forwarded logs:

System logs

Security logs

System and Security Logs

范例：Syslog Server 收到 防火墙发送的系统日志



Date	Time	Priority	Hostname	Message
08-22-2017	17:56:57	System0.Notic	192.168.1.1	Aug 22 17:55:52+08:00 192.168.1.1 Action="drop" Uuid="(0x0,0x0,0x0,0x0)" src="10.2.70.214" dst="224.0.0.10" proto="88" rule="Default policy (Incoming/Internal)" rule_uid="(default_internal)" product="VPN-1 & FireWall-1"
08-22-2017	17:56:53	System0.Notic	192.168.1.1	Aug 22 17:55:47+08:00 192.168.1.1 Action="drop" Uuid="(0x0,0x0,0x0,0x0)" src="10.2.70.214" dst="224.0.0.10" proto="88" rule="Default policy (Incoming/Internal)" rule_uid="(default_internal)" product="VPN-1 & FireWall-1"
08-22-2017	17:56:49	System0.Notic	192.168.1.1	Aug 22 17:55:44+08:00 192.168.1.1 Action="drop" Uuid="(0x0,0x0,0x0,0x0)" inzone="External" outzone="Local" src="10.2.70.136" dst="255.255.255.255" proto="17" rule="Default policy (Incoming/Internal)" rule_uid="(default_internal)" product="VPN-1 & FireWall-1" service="17500" s_port="17500"
08-22-2017	17:56:49	System0.Notic	192.168.1.1	Aug 22 17:55:44+08:00 192.168.1.1 Action="drop" Uuid="(0x0,0x0,0x0,0x0)" inzone="External" outzone="Local" src="10.2.70.136" dst="255.255.255.255" proto="17" rule="Default policy (Incoming/Internal)" rule_uid="(default_internal)" product="VPN-1 & FireWall-1" service="17500" s_port="17500"
08-22-2017	17:56:49	System0.Notic	192.168.1.1	Aug 22 17:55:44+08:00 192.168.1.1 Action="drop" Uuid="(0x0,0x0,0x0,0x0)" inzone="External" outzone="Local" src="10.2.70.136" dst="255.255.255.255" proto="17" rule="Default policy (Incoming/Internal)" rule_uid="(default_internal)" product="VPN-1 & FireWall-1" service="17500" s_port="17500"

2. Status

3-1. Active Computers

与 [三 > 一、Monitoring > 2-1.Active Computers](#) 相同

3-2. Infected Hosts

与 [三 > 四、Access Policy 設定 > 1-3.Infected Hosts](#) 相同

3-3. VPN Tunnels

与 [三 > 六、VPN 設定 > 2-4.VPN Tunnels](#) 相同

3-4. Connections



查看通过 firewall 的连接通信

Connections: View all active connections

Print | Help

Type to filter

Protocol	Source Address	Source Port	Destination Address	Destination Port
UDP	10.2.70.121	50002	8.8.8.8	53
TCP	192.168.1.5	50347	216.58.200.46	443
UDP	10.2.70.136	17500	255.255.255.255	17500
TCP	10.2.70.121	48217	103.243.111.213	80

3-5. Monitoring

与 [三>二、Home>2-2.Monitoring](#) 相同

3-6. Reports

与 [三>二、Home>2-3.Reports](#) 相同

3. Diagnostics

3-1. Tools

与 [三>二、Home>3-1.Tools](#) 相同

3-2. SNMP

点击 开启或关闭 SNMP，点击“Configure...” 设定是否启用 SNMP traps

SNMP: Monitor the device's status using SNMP Help

SNMP Version: v1/v2/v3 | SNMP Traps are enabled | [Configure...](#)

SNMP v3 Users

[New](#) [Edit](#) [Delete](#)

User Name	Security Level
No v3 users defined. Add SNMP v3 User	

SNMP Traps Receivers

[New](#) [Edit](#) [Delete](#)

IP Address	SNMP Version	Community Name	SNMP v3 User
No receivers defined. Add SNMP traps receiver			

SNMP Traps

[Edit](#)

	Event Name	Monitored Object	Value	Trap OID	Description
<input checked="" type="checkbox"/>	Interface disconnected	Interface link status		1.3.6.1.4.1.2620.1.200...	Either network cable was...
<input checked="" type="checkbox"/>	Interface unassigned	Interface IP address		1.3.6.1.4.1.2620.1.200...	Interface IP address rem...
<input checked="" type="checkbox"/>	High memory utilization	Memory utilization	> 90 %	1.3.6.1.4.1.2620.1.200...	Memory utilization excee...
<input checked="" type="checkbox"/>	Low disk space	Free disk space	<= 10 %	1.3.6.1.4.1.2620.1.200...	Disk partition free space...

四、恢复出厂预设置与备份

一、恢复出厂预设值方式

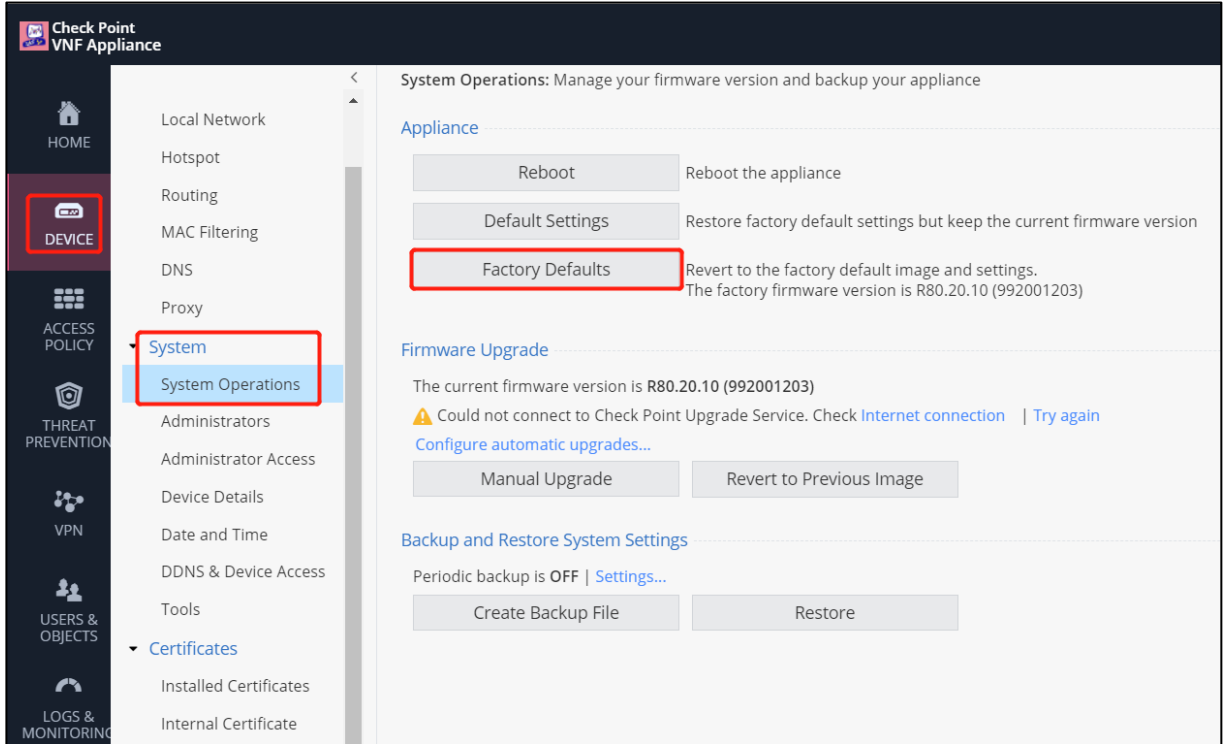
方式 1.使用 WEB UI 页面

方式 2.按背面 Factory Default

方式 3.进入 CONSOLE 重设

1. 使用 WEB UI 介面

登录 WEB UI-依次选择 Device→System-System Operations→Factory Defaults



点击 OK



等待約 2 分鐘後，即可完成原廠預設值。

2. 按背面 Factory Default 鈕



按住 Factory Default 按钮 12 秒，当设备前面的 Power and Notice LEDs 亮紅灯时，放开 Factory Default 按钮，等到 Power 亮绿灯后，即完成恢复原厂配置。

3. 进入 CONSOLE 重设

使用随盒附的 USB CONSOLE 线，插入 CONSOLE PORT，**Baud Rate 设为 115200**，将 FW 插上电源，输入 Ctrl-C，即可出現 Boot Menu:

```
al_eth0, al_eth1 [PRIME], al_eth2, al_eth3
device 0 offset 0x300000, size 0x3fd00000
do_nand: set partition base address to=300000
Trying to read nand: 262144 bytes from offset 3145728
Read nand: 262144 bytes from nand
blob magic: a5a51234
blob crc: 458ae674
Verifying CRC for settings area... Done

***** Hit 'Ctrl + C' for boot menu *****

Setting bootaddr to 0x8000200
Enabling network ports...
Done.

Welcome to Gaia Embedded Boot Menu :

  1. Start in normal Mode
  2. Start in debug Mode
  3. Start in maintenance Mode
  4. Restore to Factory Defaults (local)
  5. Install/Update Image from Network
  6. Restart Boot-Loader
  7. Run Hardware diagnostics
  8. Upload preset configuration file

Please enter your selection (press ENTER to finish) : █
```

选择 4. Restore to Factory Defaults (local)，按 Y，即可恢复原厂预设，并可查看页面是否恢复完成。

```
Starting kernel ...

Uncompressing Linux... done, booting the kernel.
INIT: version 2.88 booting

Booting Check Point RD-6281-A User Space...
INIT: Entering runlevel: 3
.....
----- This is a first boot -----
.....
----- First boot done -----

System Started...
Running predefined CLI commands
Appliance was not configured yet - Checking Zero Touch service...

Gateway-ID-7F7AD148 login: █
```

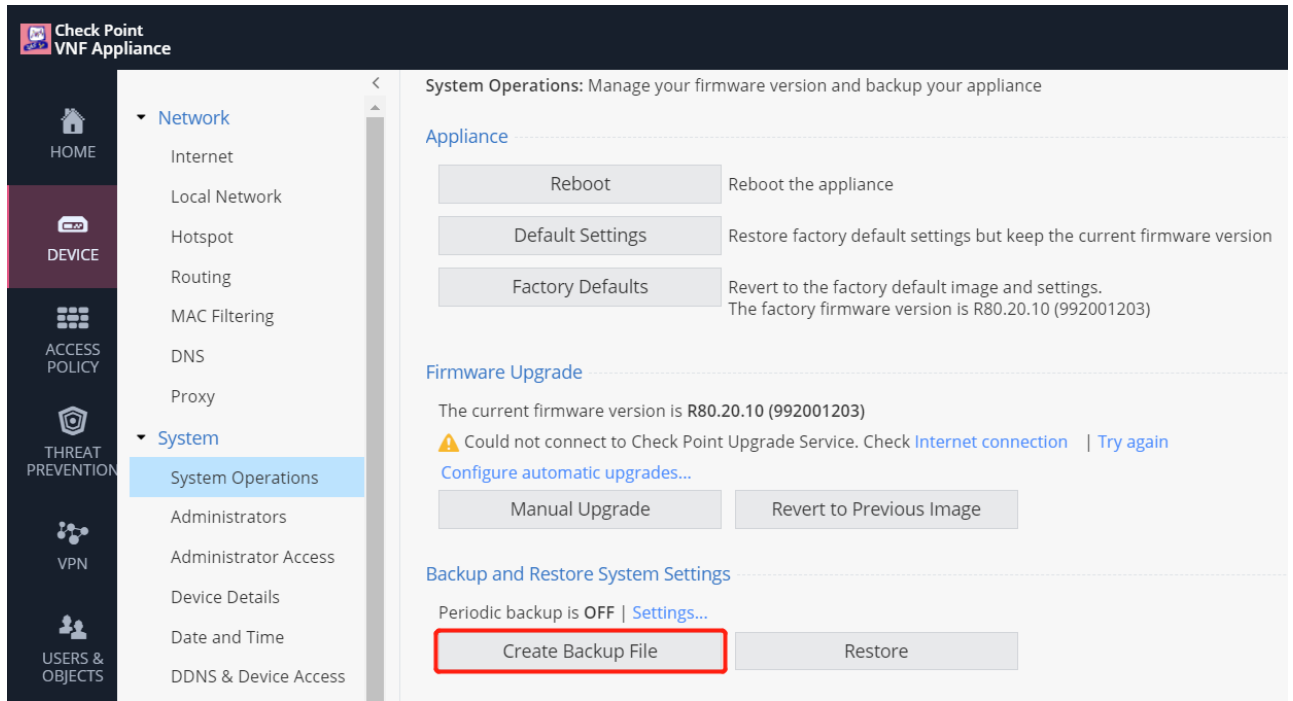
登入预设账号 admin/admin，确认完成恢复

```
Gateway-ID-7F7AD148 login: admin
Password:
> Welcome to CLISH. The First Time Configuration wizard was not completed yet
> NOTE: The First Time Configuration wizard may delete or override some of the settings you see in CLISH
> To disable the First Time Configuration wizard (and USB automatic configuration) please run "set property first-time-wizard off"
Gateway-ID-7F7AD148>
```

二、备份及恢复配置设定

1. 备份

选择 Device>System>System Operations>Create Backup File



输入 Comment-选择Create Backup



BACKUP SETTINGS [X]

Backup Settings

Use file encryption

Set password:

Confirm password:

Comment:

Backup File Contents

Backup system settings

选择 Download Backup

BACKUP SETTINGS [X]

Backup Settings

Use file encryption

Set password:

Confirm password:

Comment:

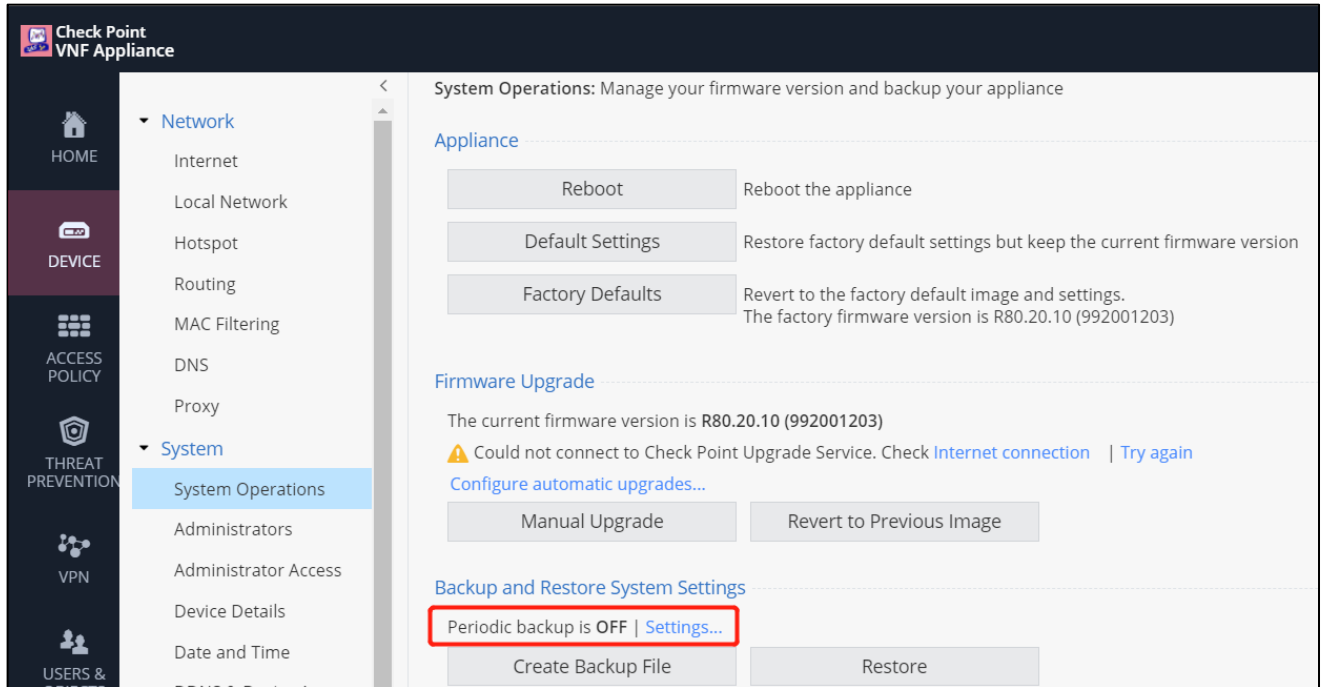
Backup File Contents

Backup system settings

Click the Download button to save the backup file



2. 计划备份



选择 Settings，输入 File Storage 路径及 username/Password，选择计划备份的备份频率、日期、时间



Periodic Backup Settings ×

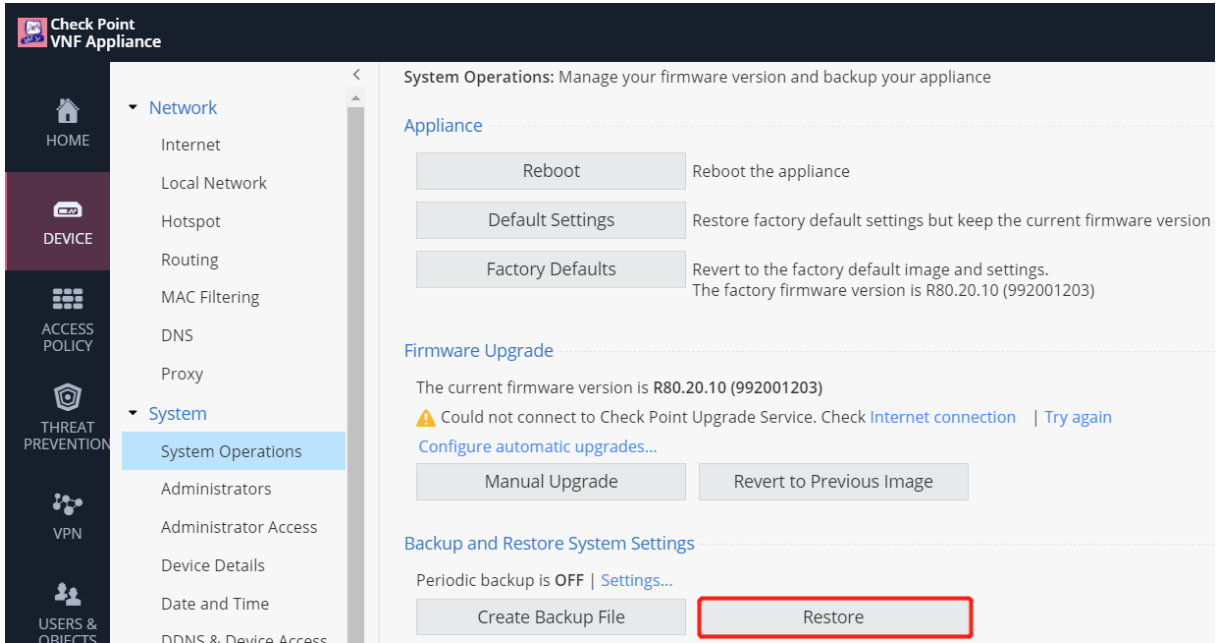
Enable scheduled backups

File Storage
Backup server path:
Username:
Password:

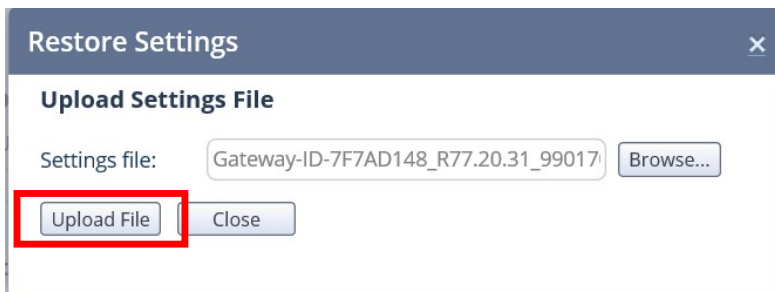
File Encryption
 Use file encryption
Password:
Confirm:
 Show

Schedule Periodic Backup
 Daily
 Weekly
 Monthly
Day of month:
Time of day:

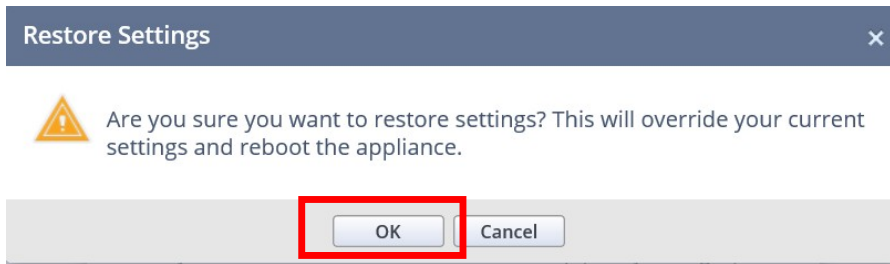
3. 恢复



选择 Restore 恢复配置→选择上传配置文件



确认恢复的信息→确认恢复，即可按 OK



等待数分钟后，完成恢复配置→重新整理页面即出现登录页面

