



# Check Point SG1570

## R80.20.35



咨询订购:400-010-8885、 8008106669@b.qq.com





一、安	装及设定	6
<u> </u>	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
Ξ、	初始设定 SG1570	8
1.	进入连线设定页面	
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.	设定內部网络 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
<u> </u>	联网下载更新版本	15
二、	手动更新版本	16
≡ ∙ w	/eb 管理功能說明	
<u> </u>	页面說明	17
1.	显示登入者 ID 与登出(Log Out)	17
2.	主功能标签17	

#### Check Point SOFTWARE TECHNOLOGIES LTD.

3.		次功能目录	17	
4.		內容		17
5.		显示当前设备状态,包含 Internet、Status、Device Time		17
Ξ、	н	ome 目录		18
1.		Overview 总览		
-	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	
4	2-1.	Active Computers		22
2	2-2.	Monitoring		23
-	2-3.	Reports		24
3.		Troubleshooting	29	
3	3-1.	Tools		29
	3-2.	Support		31
Ξ·	D	evice 設定		32
1.		Network	32	
	1-1.	Internet	••••••	
-	1-2.	Local Network	••••••	
-	1-3.	Hotspot		
-	1-4.	Routing		41
-	1-5.	DNS		42
-	1-6.	Proxy		43
2.		System	43	
2	2-1.	System Operations		43
4	2-2.	Administrators		44
2	2-3.	Administrator Access		44
4	2-4.	Device Details		45
4	2-5.	Date and Time		45
4	2-6.	DDNS & Device Access		45

SOFTWARE TECHNOLOGIES LTD

	SOFT			
	2-7.	Tools		46
	3.	Advanced	46	
	3-1.	High Availability		46
	3-2.	Advanced Settings		48
四、	A	ccess 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、	Т	hreat Prevention 設定		56
	1.	Threat Prevention		
	1-1.	Blade Control		
	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、	· v	PN 設定		66
	1.	Remote Access		
	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

SOFTW		
2-3.	Community	73
2-4.	VPN Tunnels	73
2-5.	Advanced	73
3. C	ertificates	74
3-1.	Trusted	74
3-2.	Installed Certificates	74
3-3.	Internal Certificate	74
七、 Us	ers & Objects 設定	75
1. U	lser Management	75
1-1.	User Awareness	75
1-2.	Users	75
1-3.	Administrators	75
1-4.	Authentication Servers	76
2. N	letwork 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、 Log	gs & Monitoring	
1. L	ogs	81
2-1.	Security Logs	81
2-2.	System Logs	83
2-3.	External Log Servers	83
2. S	tatus	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. D	Viagnostics	85

Check Point SOFTWARE TECHNOLOGIES LTD.

3-1.	Tools	.86
3-2.	SNMP	.86

四、	复出厂设定配置与备份	86
<u> </u>	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
Ξ.	备份及恢复	89
1.	备份	89
2.	计划备份	92
3.	恢复	93



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

← 设置		-	٥	×
命 主页	以太网			
直找设置の	日本192 ChinaNet+TYm-5G 可と1940 更改造配器追頭	٦		
网络和 Internet	· · · · · · · · · · · · · · · · · · ·			
<b>●</b> 状态	网络和共享中心			
// WLAN	Windows 防火墙			
<b></b>	Q 获取帮助		60	-
♀ 拨号	2 提供反馈		8 50%	%
% VPN				
♪ 飞行模式				
(中) 移动热点				
⊕ 代理				

点选网络连接 · 点击属性



以太网 ChinaN Intel(R)	<u>et eTV∞ EC</u>	
- incol(ry	↓ 状态(U)	
	-V(B(C))	
	诊断(I)	
	➡ 桥接(G)	
	创建快捷方式(S)	
	💡 删除(D)	
	▼ 里叩名(IVI)	
	💡 属性(R)	

请选择网络通信协议第4版(TCP/IPv4)点击属性

٢	Intel(R) Etherne	et Connection (6) I219-V	/	
			配置	ť( <u>C</u> )
比连接	接使用下列项目( <u>O</u> )	:		
v	Microsoft 网络	客户端		^
🗹 🤰	VMware Bridge	Protocol		
🗹 📜	Microsoft 网络的	的文件和打印机共享		
모 速	QoS 数据包计划	程序		
<ul> <li></li> </ul>	Internet 协议版	本 4 (TCP/IPv4)		
	Microsoft 网络	<b>适配器多路传送器协议</b>		- 1
v 🚽	Microsoft LLDP	协议驱动程序		
v 🚽	Internet 协议版	本 6 (TCP/IPv6)		~
<				>
	安装( <u>N</u> )	卸载( <u>U</u> )	属性	E( <u>R</u> )
描述				
传转 于7	諭控制协议/Intern 在不同的相互连接的	et 协议。该协议是默认的 的网络上通信。	广域网络协	议, 用

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。



Internet 协议版本 4 (TCP/IPv4) 属性		×
常规		
如果网络支持此功能,则可以获取自动指 系统管理员处获得适当的 IP 设置。	派的 IP 设置。否则,你需要从网络	
○ 自动获得 IP 地址( <u>O</u> )		
● 使用下面的 IP 地址( <u>S</u> ):		
IP 地址( <u>l</u> ):	192.168.1.10	
子网掩码( <u>U</u> ):	255 . 255 . 255 . 0	
默认网关( <u>D</u> ):	192.168.1.1	
○ 自动获得 DNS 服务器地址(B)		
● 使用下面的 DNS 服务器地址( <u>E</u> ):		
首选 DNS 服务器( <u>P</u> ):		
备用 DNS 服务器( <u>A</u> ):	· · ·	
□退出时验证设置(L)	高级(⊻)	
	确定取消	

## 二、初始设定 SG1570

#### 1. 进入连线设定界面

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

🖸 🛛 🚱 360导航_一个主页,整个世界 🛛 🗙 360核编安全管理系统	× 🕃 生态理念 生态架构 音频经销度 🛛 🗙 隐私错误	×	+								-	٥	×
← → Ĉ බ ▲ 不安全   [+++++++++++++++++++++++++++++++++++				î	۲	<i>i</i>	۲	G	£_≡	Ē	ø		
	Δ												
	你的连接不是专用连接												
	攻击者可能试图从 192.168.1.1 窃取你的信息(例如, 密码、消息或信用卡)。												
	NET:ERR_CERT_AUTHORITY_INVALID												
	隐藏高级		返回										
	LI服务部元去证明已是192.198.1.1; 初的计算机的解释系统不信任它的安全证 是由配置错误或者有攻击者截获你的连接而导致的。	C-12.	1X PJ RE										
	继续访问 192.168.1.1 (不安全)												
										49	3%		
										( 0.4	IK/s		



2. 开始初始设定

<b>-</b>		
1500 Ap	oliance	
on Wizaro	ł	
w Check Point	1500 Appliance	
< Back	Next >	Quit
	<b>1500 App</b> on Wizard w Check Point	<b>1500 Appliance</b> on Wizard w Check Point 1500 Appliance! < Back Next >

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

CHECK POINT 1500 APPLIANCE	? Help			
Authentication Details	Check Point			
Change the default administrate	or name and set the passwo	ord:		
Administrator name: adm	in			
Password:				
Confirm password:				
Enforce password complexit	y on administrators			
It is strongly recommended to a as well as one of the following o	use both uppercase and low haracters in the password:	ercase character:  @#\$%^&*()=+:	5	
$\fbox$ Help us improve product experience by sending data to Check Point				
Step 1 of 9   Authentication < Back Next > Quit				



#### 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 APPL	? Help		
Appliance Date an	Appliance Date and Time Settings		
• Set time manually			
Date:	Monday, October 18, 2021	<b></b>	
Time:	11 : 10 AM 🕶		
Time zone:	(GMT+08:00) Beijing Chongqing Hong Kong U	•	
Use Network Time Pro	otocol (NTP)		
First NTP server:	ntp.checkpoint.com		
Second NTP server:	ntp2.checkpoint.com		
Time zone: (GMT+08:00) Beijing Chongqing Hong Kong U 💌			
Step 2 of 9   Date and Tim	e Settings < Back	Next > Quit	

#### 5. 设定设备主机名(Appliance Name)

CHECK POINT 1500	APPLIANCE WIZARD		? Help
Appliance Nar	ne		Check Point DOFTWARE TECHNOLOGIES LTD.
<b>9 8</b> 2609			
Appliance Name:	Gateway-ID-7FAE41EF		
Domain name:	Field is not mandatory		
	Example: mycompany.com		
Step 3 of 9   Applian	ce Name	< Back	Next > Quit

确认后点击" Next>" 进行下一步進行下一步



#### 6. 选择防火墙的管理方式

#### 选择 Local management · 确认后点击" Next>" 进行下一步進行下一步

若为单台防火墙设备建议采用Local,可不用另外安裝管理软件

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

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

#### 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

Internet Connection	
Configure Internet connection now     Connection type: Static IP     IP address:     Subnet mask:     Default gateway:	
First DNS server: Second DNS server: O Configure Internet connection later	Connect
WAN link is up	

Check Point

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)

CHECK POINT 1500	APPLIANCE WIZARD	? Help
Local Network		
LAN Settings	on LAN ports	2 — 4 LAN 6 — 8
Network name:	LAN1	
IP address:	172.16.1.1	
Subnet mask:	255.255.255.0	
DHCP Settings		Local T network
DHCP Server:	Disabled 🔹	Traffic between LAN ports undergoes firewall inspection
Step 6 of 9   LAN		< Back Next > Quit

#### 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







#### 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

CHECK POINT 1500 APPLIANCE WIZARD	? Help
Appliance Registration	
Click 'Activate License' to check registration status. An Internet connection must be configured and connected. MAC Address: 00:1C:7F:AE:41:EF Registration Key: F32D-F600-CB47-D913 Activate License Offline Set proxy	evalue
Step 8 of 9   Activation < Back	Next > Quit

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。

CHECK POINT 1500 AP	PLIANCE WIZARD			
The First Time Configu	ration Wizard has completed			
Administrator name: System time: Appliance name:	admin Monday, October 18, 2021 11:17 AM Nantian-FWSMB (1500 Appliance)			
Internet: License:	A Not configured			
Local network:	192.168.1.1 / 255.255.255.0 DHCP server is enabled			
Security policy mode:	Locally managed			
Active Software Blades:	Firewall, Remote Access, Site To Site VPN			
		< Back	Finish	



## 二、升级 R80.20.35

## 一、联网下载更新版本

通过 Device>System Operations>Firmware Upgrade>Check now

	<	System Operations: Manage your firmware version and backup your appliance			
	<ul> <li>Overview</li> </ul>	Appliance			
HOME	System	Appliance			
	Security Dashboard	Reboot	Reboot the appliance		
	Security Management	Default Settings	Restore factory default settings but kee	ep the current firmware version	
DEVICE	Cloud Services	Factory Defaults	Revert to the factory default image and	l settings.	
:::	License		The factory firmware version is R80.20.	.10 (992001203)	
ACCESS POLICY	Site Map	Firmware Upgrade		1	
~	<ul> <li>Monitoring</li> </ul>	The current firmware version is R8	0.20.10 (992001203)		
	Notifications	Firmware is up to date   Check	now		
PREVENTION	Active Devices	Configure automatic upgrades			
24-0	Monitoring	Manual Upgrade	Revert to Previous Image		
●●~ VPN	Reports	Rackup and Restore System Settir	arc	J	
	<ul> <li>Troubleshooting</li> </ul>	Deviedis backup is OFF   Cettings	163		
<u>22</u>	Tools	Grante Declare Sile	Destaur		
USERS & OBJECTS	Support	Create Backup File	Restore		
LOGS & MONITORING					

若有新版本可更新时,会提示新版的信息,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

	Check Poi	nt s LTD.		
	<	System Operations: Manage your firm	ware version and backup your appliar	nce
	<ul> <li>Overview</li> </ul>	Appliance		
HOME	System			
	Security Dashboard	Reboot	Reboot the appliance	
	Security Management	Default Settings	Restore factory default settings but ke	eep the current firmware version
DEVICE	Cloud Services	Factory Defaults	Revert to the factory default image ar	nd settings.
===	License	,	The factory firmware version is R80.2	0.10 (992001203)
ACCESS POLICY	Site Map	Firmware Ungrade		
~	<ul> <li>Monitoring</li> </ul>	The current firmware version is <b>R80</b>	20 10 (992001203)	
	Notifications	Firmware is up to date   Check no	W	
PREVENTION	Active Devices	Configure automatic upgrades		
•• -	Monitoring	Manual Upgrade	Revert to Previous Image	
VPN	Reports			
	<ul> <li>Troubleshooting</li> </ul>	Backup and Restore System Setting	5	
<u>2ع</u>	Tools	Periodic backup is OFF   Settings		
USERS & OBJECTS	Support	Create Backup File	Restore	
00,2215	Support			
~				
LOGS & MONITORING				

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。

SOFTWARE UPGRADE WIZARD	×
Upload Software	
Click <b>Browse</b> to locate the software file to upload. Software file names end with an .img extension. For example: fw1_vx_dep_R80_992000668_20.img.	
Software file: fw1_vx_dep_R80_20_35_992002467.im Browse	
Upload	
Cancel Help < Back	√ext >

更新完成后会回到登入页面,此时为新版本的登入页面,输入账号密码密即可登入



## 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. 內容
- 5. 显示当前设备状态,包含 Internet、Status、Device Time

Check Poin VNF Appli	nt iance			l	<b>₩admin   E+ Log Out   ? Help</b> / Support Q Search
2	3<	System	4		🕑 Help
6	<ul> <li>Overview</li> </ul>	VNF Appliance	Name: SMB-1	Connectio	on type: Static IP   Interface: WAN   IPv4 address: 192.168.1.20/24
HOME	System		MAC: 00:0C:29:9D:09:EC		
	Security Dashboard		Thursday, November 11th, 2021 08:36:00 PM (GMT+08:00) Beijing Chongging Hong Ko		
DEVICE	Security Management		System is up for 0 days, 3 hours, 3 minutes and 28 seconds		
	Cloud Services				
	License	NOTIFICATIONS	Notifications page	WATCHTOWER	MOBILE APP
ACCESS POLICY	Site Map	ပံ Security gateway is u	up 1) Informative Event 17:34:08 11 Nov 2021		NEW
	<ul> <li>Monitoring</li> </ul>	Security gateway is up.	Reboot initiated by expert at 22:13 Wednesday November 10,		Get security alerts to your mobile!
THREAT	Notifications	(1) Security gateway is I	In Informative Event 21:10:04 10 Nov 2021	Enhance your Check Point network security with	Enhance your Check Point network security with the ability to
PREVENTION	Active Devices	Security gateway is up.	Reboot initiated by expert at 15:21 Wednesday November 10,	WATCH TOWER	go with your mobile phone
22.0	Monitoring	2021.			
VPN	Reports	C Security gateway is u	μp 🚯 Informative Event 14:35:29 10 Nov 2021 🗣		PAIR YOUR MOBILE DEVICE
	<ul> <li>Troubleshooting</li> </ul>				
	Tools	NETWORK ACTIVITY			Reports   Monitoring
OBJECTS	Support	Packet Rate (packets pe	er second)	Throughput (Kl	ibps)
$\sim$		38-		66-	
LOGS & MONITORIN(					
		23-		39	
		7		12-	
e	Internet connected		5		😌 Update available 🛛 🛇 08:36 PM



## 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 图素

Check Point VNF Appliance		wadmin   E+ Log.Out   2 Help / Support Q Search
Coverview     System     Security Dashboard     Security Management     Cloud Services	System Check Point VNF Appliance Check Dint VN	Internet connected     Connection type: Static IP   Interface: WAN   IPv4 address: 192.168.1.20/24
CERSE POLICE POLICE POLICE POLICE SITE Map Monitoring Notifications Active Devices Monitoring VPN Reports	NOTIFICATIONS     Notifications page <sup>©</sup> Security gateway is up. Reboot initiated by expert at 22:13 Wednesday November 10, 2021. <sup>©</sup> Security gateway is up. Reboot initiated by expert at 15:21 Wednesday November 10, 2021. <sup>©</sup> Security gateway is up. Reboot initiated by expert at 15:21 Wednesday November 10, 2021. <sup>©</sup> Security gateway is up. Reboot initiated by expert at 15:21 Wednesday November 10, 2021. <sup>©</sup> Security gateway is up. Reboot initiated by expert at 15:21 Wednesday November 10, 2021.	WATCHTOWER MOBILE APP
Troubleshooting     Tools     Support	NETWORK ACTIVITY Packet Rate (packets per second) 45 28 11	Reports   Monitoring
Sainternet connected		😌 Update available 🛛 O8:42 PM

- 1-2. Security Dashboard
  - A. 查看当前防火墙功能,并可透过图示开尖(\_\_\_\_\_\_关闭或启用\_\_\_\_)功能
  - B. 点击齿轮 <sup>•</sup> 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 山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



*	<ul> <li>Overview</li> </ul>	Security Dashboard: C	ontrol and monitor Softwa	re Blades configurations	and status	
HOME	System	44.94	19.92	<u> </u>		
	Security Dashboard					
-	Security Management				V	
DEVICE	Cloud Services		ıl. 🗘 📃 💴	II. ¢	OFF 🗘 .lı	
===	License	Firewall	Applications & URL Filtering	User Awareness	QoS	
ACCESS POLICY	Site Map					
<b>@</b>	<ul> <li>Monitoring</li> </ul>					
THREAT	Active Computers		69	A		
PREVENTION	Monitoring	ON O .h	II. ¢	ON 🗘 .lı	OFF 🗘 .lı	ON O.II
24-	Reports	Intrusion Prevention (IPS)	Anti-Virus	Anti-Bot	Threat Emulation	Anti-Spam
VPN	<ul> <li>Troubleshooting</li> </ul>					
<b>1</b> .	Tools	194	194			
USERS & OBJECTS	Support		100 m			
~		II. Ø	ON 🗘 .lı			
LOGS & MONITORING		Remote Access	Site To Site VPN			

1-3. Security Management

查看及变更防火墙的管理方式

Local 管理与防火墙一体,可不用另外安装管理软件 A.

Β. Central 管理与防火墙分开,需另装管理服务器來管理单(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

Æ	Z	Cloud Serv	ices							
		Configure	2							
Manage	ed Security Blade	es								
Firewall	Applications & URL Filtering	User Awareness	QoS	IPS	Anti-Virus	Anti-Bot	Threat Emulation	Anti-Spam	Remote Access	
Availab	le Services									
	Reports Receive periodic	network and see	curity reports b	iy mail	¢ F	irmware Up rmware upgrad	ogrades es management			
	Logs Store security and	d system logs in	cloud servers		Ð 🖁	eriodic Back	<b>ckup</b> up the appliance	's settings		
(WEW)	Dynamic DN Assign a persiste e.g. my-gateway.	<b>IS</b> nt domain name domain.com								
<										>
					X Ca	ncel				
Config	jure Cloud Servi	ices					×			
Activate	e connection to a	Cloud Service	es using:							
Acti	ivation key:									
Acti	ivation details:									
Ser	vice Center:	https://sm	bcloudmgmt	.checkpoint.c	om/SMC/se	vices/SMP				
Gat	eway ID:									
Reg	gistration key:									
🚹 The	e activation details	s are supplied	by your Clou	ıd Services p	rovider					
					✓ A	pply 🥋 🗙	Cancel			



#### 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
III 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
1PS	🚔 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	菺 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:
Select an activation file
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

Device	III Access Policy	Threat Prevention	
Network	Firewall	Threat Prevention	
Internet	Access Policy Control	Threat Prevention Blade Control	
Local Network	Firewall Access Policy	Threat Prevention Policy	
Hotspot	Servers Definition and Access	Exceptions	
Routing	NAT	Infected Hosts	
DNS	User Awareness	Protections	
Proxy	User Awareness	IPS Protections	
System	QoS	Threat Prevention Engine Settings	
System Operations	Quality of Service Control	Anti Sanan	
Administrators	Quality of Service Policy	Anti-Spam	
Administrator Access		Anti-Spam Control	
Device Details		Anti-Spam Exceptions	
Date and Time			
DDNS & Device Access			
Tools			
Advanced			
High Availability			
Advanced Settings			

#### 2. Monitoring

#### 2-1. Active Computers

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

Туре	to filter	Q 🛞 Save as 🔻	Y Filter - ■ Details	× Revoke Certificate C Refresh	=
	Object Name	IP/MAC Address	Device/User Name	Services	Interface
1	NB05	192.168.1.5 b8:ca:3a:ce:e8:fa		I➡ WebUI, UDP:1900, UDP:5355, Net	∔ LAN1

Help



## 2-2. Monitoring

## 监控目前网络、安全防护的状态

Check Point VNF Appliance		wadmin   E→ Log Out   ? Help / Support Q Search
VVF Appliance     VVF Appliance     VVF Appliance     VVF View     System     Security Dashboard     Security Management     Cloud Services     License     ACCESS     POLICY     VVF     VVF     VVF     VVF     VVF     Reports     VVF     Reports     TurkeAt     Security Devices     Security	Monitoring   Refresh Current Connections: ** 0 VPN Tunnels   TActive Device   ** 31 Connections NETWORK Last hour * Bandwidth Usage Applications   Categories   Sites   Users Total traffic: OB Traffic Total   Received   Sent 0.58	Top Bandwidth Consuming No Data   Top application No Data   Top category No Data   Top site N/A   Top user Identity Awareness is inactive OB Total Traffic OB Received
Troubleshooting     Tools     Users & Support     Locs &     MONITORING	O INFECTED DEVICES     O HIGH RISK APPLICATIONS     Detected in last month     O O High/Critical Infected Devices	<ul> <li>OB Sent</li> <li>Security Events</li> <li>Detected since reboot</li> <li>O Anti-Bot Events</li> <li>O Anti-Virus Events</li> </ul>
California Connected		😲 Update available 🛛 🛇 09:46 PM



#### 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。

orts : Monthly  Weekly  Daily  Hourly no report: October 13th, 2021 09:00am / Nove	mber 12th, 2021 09:00am		
Anti-Bot 283 Events <sup>1</sup> S64 Events <sup>2</sup>	IPS 3 Incidents <sup>3</sup>	Threat Emulation 0 Malicious files 1000 Files scanned	
op Bandwidth Consuming	Bandwidth Usage b	y Applications	
High Bandwidth   Top category 42.4GB(24.9%) Bandwidth			
youtube.com   Top site 29.2GB(17.2%) Bandwidth	Total traffic:		
John A   Top user 26.7GB(15.7%) Bandwidth	170GB Top 5 Apps: 78.3GB		
130GB			
10GB Total Sent	<ul> <li>17% YouTube</li> <li>13% Gmail</li> <li>9.2% SSL Protocom</li> </ul>	<ul> <li>4% Facebook</li> <li>3.7% Wikipedia</li> <li>\$3.1% Other</li> </ul>	
7 INFECTED DEVICES Detected in last month	15 high risk ap	PLICATIONS	
5 High/Critical infected Devices     4 Infected/Compromised Servers	Most used hi WinMX World DroidVPN, mo	<b>gh risk applications:</b> , eMule, 3proxy.com, ore	
A Recently active infected devices	John A, Tim R, more	h <b>igh risk applications:</b> Dan B, Jill F, Beth D, Jeffie M,	



2021/11/12 上午9:39

3

#### NETWORK USAGE









#### 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**

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
0	TeamViewer		28.1KB(7.8%)		16.5KB	11.5KB
in	LinkedIn	-	21KB(5.8%)		17KB	4KB
	LINE		13.8KB(3.8%)	•	6.66KB	7.11KB
0	Server Message Block (SMB)		12.2KB(3.4%)	•	3.14KB	9.03KB
	Kerberos Protocol	-	10.3KB(2.8%)	•	3.79KB	6.49KB
27	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 1				
All top applications		232				
Gateway   877 20 40   00:1C:7F:7C:CD:1D   © 2016 Check Point Software Technologies   td						

4



#### **TOP SITES**

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

	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

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

5



#### **TOP CATEGORIES**

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

			in August Stil, 2017	ourly report: August 9th, 2017 09:25a
		ons	ications by sess	op potentially high-risk appl
width	Bandwie	Sessions	Risk	Application
В	22.9KB	6		TeamViewer
B	22.9KB	6	RISK	TeamViewer

6



### 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

То	ols: Various Tools used to di	agnos	e problems with the ap	pliance					
Α	Monitor System Resource	System Resources Display CPU usage, memory usage and processes							
В	Show Routing Table		ble of the gate	le of the gateway					
С	C Test Cloud Services Ports Verify that the appliance could connect to Cloud Services								
D	Generate CPInfo File								
E Pir	ng or Trace an IP Address								
Ho	ost name or IP address:			Ping	Traceroute				
<b>F</b> Pe	rform a DNS Lookup								
Ho	ost name or IP address:			Lookup					
GPa	Gacket Capture								
Se	lect network:	All Int	terfaces 🔻	Start	Download File				

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

1						
CPU Usage History			Memory Usage His	tory		
100% 90%			1000MB			
80% - 70% -			800MB -			
60% - 50% -			600MB -			
40% - 30% -			400MB -		/	
			200MB -			
20% -						
20% 10% 0%	CDU: 7% 1%	<u> </u>	0B		EMB	
20% 10% 0% Current usage per Disk Usage C Ref	·CPU: 7% 1%	<u> </u>	0B Current men	nory usage: 383.	.5MB	
20% 10% 0% Current usage per Disk Usage C Ref Filesystem	°CPU: 7% 1% resh	Used	0B Current men	nory usage: 383. Use%	.5MB Mounted On	
20% 10% 0% Current usage per Disk Usage C Ref Filesystem tmpfs	• CPU: 7% 1% resh Size 20.0MB	Used 704.0KB	0B Current men Available 19.3MB	nory usage: 383. Use% 3%	.5MB Mounted On /tmp	•
20% 10% 0% Current usage per Disk Usage C Ref Filesystem tmpfs tmpfs	CPU: 7% 1% resh Size 20.0MB 40.0MB	Used 704.0KB 14.6MB	0B Current men Available 19.3MB 25.4MB	nory usage: 383. Use% 3% 36%	.5MB Mounted On /tmp /fwtmp	
20% 10% 0% Current usage per Disk Usage C Ref Filesystem tmpfs tmpfs ubi2_0	CPU: 7% 1% resh Size 20.0MB 40.0MB 65.6MB	Used 704.0KB 14.6MB 468.0KB	0B Current men Available 19.3MB 25.4MB 61.8MB	usage: 383. Use% 3% 36% 1%	.5MB Mounted On /tmp /fwtmp /logs	
20% 10% 0% Current usage per Disk Usage C Ref Filesystem tmpfs tmpfs ubi2_0 ubi3_0	CPU: 7% 1% resh 20.0MB 40.0MB 65.6MB 259.8MB	Used 704.0KB 14.6MB 468.0KB 109.0MB	0B Current men 25.4MB 61.8MB 146.1MB	nory usage: 383 Use% 3% 36% 1% 43%	.5MB Mounted On /tmp /fwtmp /logs /storage	
20% 20% Current usage per Disk Usage C Ref Filesystem tmpfs tmpfs ubi2_0 ubi3_0 ubi1_0	CPU: 7% 1% resh 20.0MB 40.0MB 65.6MB 259.8MB 159.4MB	Used 704.0KB 14.6MB 468.0KB 109.0MB 111.7MB	0B Current men 25.4MB 61.8MB 146.1MB 47.7MB	Use% Use% 3% 36% 1% 43% 70%	.5MB Mounted On /tmp /fwtmp /logs /storage /pfrm2.0	
20% 20% Current usage per Disk Usage C Ref Filesystem tmpfs tmpfs ubi2_0 ubi3_0 ubi1_0 tmpfs	CPU: 7% 1% resh 20.0MB 40.0MB 65.6MB 259.8MB 159.4MB 14.0MB	Used 704.0KB 14.6MB 468.0KB 109.0MB 111.7MB 60.0KB	0B Current men 25.4MB 61.8MB 146.1MB 47.7MB 13.9MB	Use% Use% 3% 36% 1% 43% 70% 0%	.5MB Mounted On /tmp /fwtmp /logs /storage /pfrm2.0 /tmp/log/local	

Close



#### B. Show Routing table 查看目前路由的状况

Command Out	put					
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   ++	*
++	
TCP   18191   Unreachable         Policy/Configuration           TCP   18210   Unreachable         Management Connection           TCP   18264   Unreachable         CA's CRL download           TCP   443   Open smbmgmtservice.checkpoint.com         Web services (initial connection, upgr                     report	f: 1 Ya: T
4	)
Close	

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



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





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



➤ Stop 停止抓包记录 Stop Download File →

⊳	点击 Download File 下载对应抓包文件
	Packet Capture

r denet capture			
Select network:	All Interfaces 🔹	Start	Download File
File exists since: Friday, Nover Capture file is ready for do	nber 12th, 2021 10:30:31 AM ownload	(GMT+08:00)	

#### 3-2. Support

G.

查看各種 support 方式

CI	NECK POIR	nt LTD.
	Support: How can we help?	
	Whether you have an urger	nt problem or a simple question, we're here to help you by Web or phone.
	Contact Technical Suppor	t
	Occal guide is the a	ppliance's help files repository.
	<ul> <li>Service Request Tool</li> <li>Live Chat provides</li> <li>Our Worldwide Tech</li> <li>Americas: +1 (97</li> </ul>	is your online resource for submitting, updating and tracking service requests. online support for quick questions about Check Point products and services. nical Assistance Centers are available to assist you 24x7 (select option #4): 2) 444 6600 / +1 (888) 361 5030 / +1 (613) 271-7950
	EMEA: +972 3 61	1 5100
	Australia: 1 800	805 793
	China: +86 1084	181958
	<b>Japan</b> : +81 345 8	81 101
	New Zealand: 08	300 443 601
	UK: 0808 101 73	99
	Other Countries	: +972 3 611 5100
	Official support site	
	Download a local m	anual in PDF format
	S Download Windows	s driver for a USB-C console socket
	Product Information for S	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

设定 Internet · 若想配置多个 Internet 线路可点击 Add an Internet

#### connection 进行设定



Heck Poil TWARE TECHNOLOGIES	nt LTD.			
New Internet Conne	ection			×
Α		в	С	
Configuration	Connecti	on Monitoring	Advanced	
Internet Config	guration			
Connection name	):	Internet2		
Interface name:		DMZ	•	
Connection type:		DHCP	-	
Use connection	on as VLAN			

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

New Internet Connec	ction			×
Configuration	Connection Monitoring		Advanced	
Internet Config	uration			
Connection name:		Internet2		
Interface name:		DMZ	•	
Connection type:		DHCP	-	
Use connection	i as VLAN			

- 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

New Internet Connec	ction				×
Configuration	Connection Mo	nitoring Adva	anced		
<ul> <li>Connection Magnetical</li> <li>Automatical</li> <li>Select this a</li> <li>gateway and</li> <li>Monitor conselect this a</li> </ul>	Differing Ily detect loss of con option to detect conr id expecting respons nection state by ser option to detect conr	nectivity to the defau lectivity loss by send les inding probe packets t nectivity loss by using	It gateway ing ARP req o one or mo i more metho	uests (pinging) to the default re servers on the Internet ods and servers	
Connection	probing method:	Probe DNS serve Ping addresses Probe DNS serve	rs 🗸 🔻		



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: 00:1C:7F:7C:CD:1F

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 throug In order to route tra	gh this connection affic through this	on by default connection you need to add specific routes through it
High Availability Upon failure of the the selected priorit	primary Internet	t connection, traffic will be routed according to
Priority:	2	(The higher the value, the lower its priority)
Load Balancing		
Traffic will be distri	buted automatic	ally according to the configured load balancing weights
Weight:	10	(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.



Internet: Manage one or n	nore Internet con	nections		
Multiple	e Internet coi	nnections	Multiple Internet Connections	×
High Ava	ilability mode   Co	onfigure	ISP Redundancy <ul> <li>High Availability mode</li> </ul>	
			Load Balancing mode	
* New New Kdit X	Delete E	nable		
Name	Interface	Туре		
Internet1 (primary)	WAN	Static IP		
Internet2	DMZ	DHCP	<ul> <li>Apply</li> <li>X Cal</li> </ul>	ncel

#### 1-2. Local Network

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

ocal Network: Configure and manage local interfaces, switches, bridges and VLANs					Help	
🔆 New 👻 💊 Edit	× Delete Enable					
L Switch		Local IPv4 address	Subnet mask	MAC Address	Status	
💥 Bridge		192.168.1.1	255.255.255.0	00:1c:7f:7c:cd:1e		
VIAN					3 1 Gbps/Full d	
					Cable discon	
					O Disabled	
∔ LAN2					O Disabled	

A Switch : 可將多个 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 🖌 Apply 即完成设定。
Check Point SOFTWARE TECHNOLOGIES LTD. (DHCP 可自行決定是否使用)

w Switch			
Configuration	Advanced	DHCPv4 Settings	
Switch Configura	tion		
□ Name			
Interferen Confere			
nterrace Configu	ration		
Assigned to:		Separate network	•
Local IPv4 address	s:	192.168.200.1	
Subnet mask:		255.255.255.0	
Use Hotspot wł	nen connecting to net	work	
A-DHCPv4-Serv	er		
C Enabled			
IP address	range:	192.168.200.1	- 192.168.200.254
IP address	es exclude range:		-
Relay			
Disabled			
Disableu			

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 ✓ Apply 即完成设定。



(DHCP	可自行決定是否使用	)
-------	-----------	---

NOW	Hudao
INCW	Diluuc

Configuration	Advanced	DHCPv4 Settings				
Bridge Configurat	ion					
🔲 Name						
LAN1 Switch						
DMZ						
LAN2						
LAN5					~	
Enable Spannin	g Tree Protocol					
Interface Configur	ation					
Name:		br0				
Local IPv4 address	:	192.168.220.1				
Subnet mask:		255.255.255.0				
Use Hotspot wh	en connecting to n	etwork				
	er					
Enabled						
IP address	range:	192.168.220.1	-	192.168.220.254		
IP address	es exclude range:		-			
Relay						
DHCP serv						
Secondary	DHCP server IP a					
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 ✓ Apply 完成设定 (DHCP 可自行決定是否使用)



# New VLAN Configuration DHCPv4 Settings VLAN Settings VLAN ID: Interface Configuration Assigned to: Local IPv4 address: 192.168.100.1

Subnet mask:	255.255.255.0	
Use Hotspot when connecting to ne	etwork	
- DHCPv4 Server		
Enabled		
IP address range:	192.168.100.1	- 192.168.100.254
IP addresses exclude range:		-
Relay		
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 ✓ Apply 完成 设 定。

New VTI	
Configuration	
VPN Tunnel Settings	
VPN Tunnel ID:	2
Peer:	RemoteSite
O 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 页面做確认,使用者需同意页面中的內容点击" OK" 后连接才会建立,预设 timeout 時間为 240 分钟,超过则需重新確认。

	Hotspot: Configure guest access and hotspot Browser-Based Authentication
	Hotspot
A	One network interface is defined for Hotspot   Configure in Local Network
в	() No network objects are excluded from Hotspot   No source exceptions   No destination exceptions (advanced)
	Access
с	Require authentication
	Allow access to all users
	Allow access to a specific group: ManagerGroup
D	Session timeout: 240 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 完成設定

🛞 New 👻 💽 Edit 🙀 Delete 📄 Disable				
Name	Local IPv4 address	Subnet mask	MAC Address	Status
✓	192.168.1.1	255.255.255.0	00:1c:7f:7c:cd:1e	
🕂 LAN1				🔇 1 Gbps/Ful
🛓 LAN3				Cable disc
F D147				O Disabled

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

Help



Edit LAN1 Switch				
Configuration	Advanced	DHCPv4 Settings		
Switch Configurat	tion			
Name				
LAN1				^
LAN2				
LAN3				
LAN5				~
Interface Configu	ration			
Assigned to:		Separate network	•	
Local IPv4 address: 192.168.1.1				
Subnet mask: 255.255.255.0				
Use Hotspot when connecting to network				

B. 设定例外·点击來源" No source exceptions" 或目的" No destination exceptions" 后可勾选例外物件进行設定,或点击 New 即可新增 Network Object(設定方法可參考<u>二、七、User & objects 设定 2-5</u> Network Objects)→确定后点击 Apply 完成設定。

11	-	£	-	- 4	
н	O	$\mathbf{IS}$	D	OI	
	~	~~	~	~	

<ul> <li>One network interface is defined for Hotspot   Configure in Local Network</li> <li>No network objects are excluded from Hotspot No source exceptions   No destination exceptions (advanced)</li> </ul>						
Hot	spot Source Network-Objects Exceptions		×			
Туре	Type to filter Q * New					
	Object Name	Туре				
	TestLanGroup					
	ManageLan	👬 Network				
	Lan223	🖳 IP Range				
$\checkmark$	Network224	📩 Network				
$\checkmark$	ManagerIP	🖳 Single IP				
	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。(使用者组請参考<u>二、七、User</u> &objects 1-2 Users 设定)

Access Require authentication Allow access to all users Allow access to a specific group: ManagerGroup D. 设定超时 timeout 时间 240 minutes Session timeout: 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 My Company Hotspot Portal title: Welcome to My Company Hotspot - You have to agree this Portal message: terms before connect to internet. Terms of use 1.Your connection will be logged. 2.You cannot connet to malware website Settings Redirect the user to a URL after authentication http(s)://

Displayed Logo						
	Check F	Point <sup>™</sup>				
Upload	🔛 Use Default					
		~	Apply	× Cancel		

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



My Company Hotspot		
	My Company Hotspot Welcome to My Company Hotspot - You have to agree this terms before connect to internet. Username: Password: I agree with the following terms and conditions	

#### 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	New Routing Rule						
Traffic from <mark>any source</mark> to <b>any destination</b> that belongs to <mark>any service</mark> should be routed through <mark>next hop</mark>							
Destination Source Service Next Hop							
Any		Any	💥 Any	N/A			
Comment:	Write a comment						
Metric:	0 [0-100]						
配置范例如下·配置完成后点击 Apply 即设定完成。							
Tert	(f	4- 402 400 242 0 that halve are					
l rai	Traffic from any source to 192.168.212.0 that belongs to any service should be routed through 192.168.212.254						
Destination	Destination Source Service Next Hop						
192.168.212	192.168.212.0/24 Any * Any 192.168.212.254						
Comment:	Write a comment						
Metric:	0 [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

Check Point SOFTWARE TECHNOLOGIES LTD.			
C. 设定 Domain Name(	不设定也可)		
DNS: Configure DNS and Domai	n settings for the device		
-^-IPv4 DNS			
IPv4 DNS Servers			
<ul> <li>Configure DNS servers</li> <li>These settings will be ap</li> </ul>	plied on all Internet conr	nections	
First DNS Server:	8.8.8.8		
Second DNS Server:			
Third DNS Server:			
O Use DNS servers configu	ured for the active Intern	et connection(s)	
IPv4 DNS Proxy			
Enable DNS proxy			
Relay DNS requests from	n internal network clients	to the DNS serv	ers defined above
Resolve Network Obj	ects		
Use network objects a	as a hosts list to transla	te names to thei	r IP addresses
Domain Name			
Domain name: e.g. MyC	Company.com		
		<ul> <li>Apply</li> </ul>	× Cancel

#### 1-6. Proxy

Å

#### 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)、还原成预设定值(維持目前版本 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 設定)、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

A	Admin、仅能配置网络 Networking Admin					
A	Administrators: Configure administrators for the device					
G	No RAD	IUS servers exist	RADIUS configuration			
1	ype to filt	er	Q \star New 🚿 Edit 🗙 Delete 🏘 Security Settings			
		Name	Administrator Role			
	1	admin	🛥 Super Admin			
	2	ReadOnly	TRead-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

elect the sources fro	n which to allow ad	ministrator acc	ess	
🔽 LAN 🔽 VP	N 🗌 Internet			
ccess from the above	e sources is allowed	l from		
Any IP address				
Specified IP addr	esses only			
O Specified IP addr	esses from the Intern	et and any IP a	ddress from ot	her sources
ccess ports				
Web port (HTTPS):	4434			
SSH Port:	22			
			Apply	V Cancel

2-4. Device Details Device Details: Configure device's name and details

设定设备主机名

Appliance name:

Gateway

#### 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:	Tuesday, August 2	gust 29th, 2017 🛱			
Time:	11 : 41 AM	•			
Set date and time using a Network Time Protocol (NTP) server					
Primary N	TP server:	ntp.checkpoint.com			
Secondary	NTP server:	ntp2.checkpoint.com			
Update Inte	erval (minutes):	30			
NTP au	Ithentication				
	Secret:				
	Secret identifier:				
Time Zone					
Local time zon	ne: (GM	T+08:00) Taipei 🗸			

#### 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:	DynDns	-	
User name:			
Password:			
Host name:		0	Your routable host name, as defined in your DDN

#### **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,提供工具測試

#### 3. Advanced

#### 3-1. High Availability

可將两台设备做 HA,点击 Configure Cluster 开始设定

Step1.決定当前设备为主要设备还是次要



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 設定用与同步兩台设备的接口信息(预设是 LAN2)



New Cluster Wizard	Step 2: SIC Setti	ngs	×
Secure Internal Comm This will be used for es	nunication tablishing the initial	trust with the other member	
Password:	•••••		
Confirm:	•••••		
- Advanced			
Sync Interface			
Sync interface:		LAN2 -	
Sync IP address:		10.231.149.1	]
Sync IP subnet:		255.255.255.0	]
Other member syn	IP address:	10.231.149.2	

#### 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: Gatew	ay Interfaces (1 out of 6)	>
LAN4		
Enable High Availability on Interfac	e	
Cluster IP address:	192.168.223.4,172.16.90.1	
Subnet mask:	255.255.255.0,255.255.258	
Primary physical IP address:		
Conordani physical ID address;		

#### Step4 Finish 完成設定

igh A	vailability: Clu	ster between two appliances
	Enable	O This gateway (Primary Member)
		O Peer Gateway Reinitialize Trust
		This gateway is active   Peer gateway is not defined   View diagnostics
$\bigcirc$	Disable	Reset Cluster Configuration Force Member Down

#### List of Configured Interfaces

in 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	

Help



3-2. Advanced Settings

#### 查看設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

Type to filter Q Sectore Defaults					
Attribute Name	Туре	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 I	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

預設允许所有对外流量、允许內部所有流量,阻挡(block)由外部進入的流量

C. Firewall Policy>off 关闭

#### 允许所有流量通过

	Strict	Firewall Policy
		Allow traffic to the Internet on all services
$\odot$	Standard	😛 Allow traffic between internal networks
		Block incoming traffic
	Off	I No servers are configured   Add a server

- D. Applications & URL Filtering>On 启动应用及 URL 过滤功能
- E. Applications & URL Filtering>URL Filtering only 仅启用用 URL 过滤功能
- F. Applications & URL Filtering>Off 不启用应用与URL 过滤功能

Check Point

G. 设定 Applications & URL Filtering 预设值

> 可依需求勾選預設阻擋的群組,包含 security risk categories、 inappropriate content、 file sharing applications或自訂項 目 (other undesired applications)。

۲	On	Applications & URL Filtering 🕑 Up to date					
	URL Filtering only	<ul> <li>Block security risk categories</li> </ul>					
		Block file sharing applications					
	Off	Block inappropriate content					
		Block other undesired applications					
		Limit bandwidth consuming applications	Download:	100000	Kbps		
			Upload:	10000	Kbps		

➤ 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。

	plication / Category	Туре	
	Adds other software	Category	<u>^</u>
	AIM		
	Alcohol & Tobacco	Category	
•	Allows remote connect	Category	
	Allows remote control	Category	
a	Amazon		
•	Anonymizer	Category	
	Ares		
•	Art / Culture	Category	_

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

EC T	CK POIN	TD.				
•	On	Applications & URL Filtering 🕑 Up to o	date			
	URL Filtering only	<ul> <li>Block security risk categories</li> <li>Block file sharing applications</li> </ul>				
	Off	Block inappropriate content     Block other undesired applications				
		Limit bandwidth consuming applications	Download:	100000	Kbps	
			Upload:	10000	Kbps	

➤ 勾选 Enable User Awareness 可开启用户访问控制,详细说明参考<u></u>, Access Policy>2 User Awareness。

> 勾选是否记录 允许(allowed)或阻挡(blocked)的流量。

Tracking:	✓ Log All   blocked traffic
	Log All - allowed traffic

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) 、服務 (Service)、动作(Action)、记录(Log)、点击 Apply 即设定完成。
```

ADD RULE: OUTGOING A	ACCESS TO THE INTERN	IET			×
	Traffic from <mark>any source</mark>	to the Internet of a	any application / service is bl	ocked and logged	
Source	Destination		Application / Service	Action	Log
* Any	🚱 Internet		* Any	😑 Block	🖹 Log
Write a comment					
Apply only during this	s time:	09 : 00 A	M 🔻 - 09 : 00 AM	•	
Limit download traffi	c of applications to:	1000 Kbps			
Limit upload traffic o	f applications to:	100 Kbps			
				<ul> <li>Apply</li> </ul>	y X Cancel

当有设定 Application 時,在 Action 的部分可选择阻挡(Block)、放行(Accept)、 確认后放行(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) Check Poinť RE TECHNOLOGIES LTD ADD RULE: OUTGOING ACCESS TO THE INTERNET Traffic from any source to the Internet of Alcohol & Tobacco is blocked and logged is configured in Fire Source Destination Application / Service Action Log 🚱 Internet Alcohol & Tobacco 😑 Block \* Any 🖹 Log 😑 Block Write a comment... Accept Apply only during this time: 09 : 00 AM 🔻 - 09 : 00 AM 🔻 🗩 Ask Limit download traffic of applications to: 1000 Kbps i Accept and Inform Limit upload traffic of applications to: 100 Kbps i Block and Inform Apply × Cancel

> 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、Block and Inform 页面与上传 Logo 图片(Customize)





Customize Messages

Ask	Accept a	nd Inform	Block and Inform	Customize		
Message Content						
Title:		MY Compan	y Application Control			
Subject:		Are you sure	to access?			
Body:		Access to \$a only. Category: \$c Reference: \$	application_name is inten :ategory. 6incident_id	ded for work-rela	ted use	
Optional keywords						
Ignore te	ext:	I will use this	s site or application for wo	ork-related use or	nly	
User	must enter a	reason				
Message	e Settings					
Fallback action:		Block			-	
Frequen	cy:	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。

ſ	Servers Definition and Access: Access permissions and NAT for server objects						
	Type to filter						
	Name Server Type		IP Address	Ports	Public IP Address	Comments	
	MailServer1	Rail Server	192.168.10.2	TCP: 25, 110,143			

#### 1-4. NAT

#### 启用 NAT 与设定 NAT rules

NAT: Confi	igure NAT (Network Add	ress Translation) for ou	tgoing traffic and forwa	arding NAT rules for inco	oming traffic		
Outgoing	Traffic						
ON	Hide internal networks	behind the Gateway's e	external IP address				
NAT Rules	5						
New	Server (forwarding ru	le)   Hide NAT rules					
<u>∗</u> New	▼ 📝 Edit 🗙 Dele	ete 🔳 Enable					
No.	Original Source	Original Destinati	Original Service	Translated Sourc	Translated Destin	Translated Servic	Comment
<ul> <li>Man</li> </ul>	ual NAT Rules						
1	嚞 lan-30	* Any	* Any	🚆 FW-out (hide)	* Original	* Original	
•							

#### 2. User Awareness>Blade Control

Use 2-	er Av 1	wareness: Incorp	oorate users into access policy and	l display users	in security logs
(		On	User Awareness		
			Configuration wizard	2-2	
		Off	Ų		
Pol	licy	configuration			
~			ctory Queries	Configure	2-3
	4	NO ACTIVE DIrecto	ry Server denned		
~	Use	Browser-Ba	sed Authentication	Configure	2-4

- 2-1. 启用或关闭用戶访问控制,可基于用戶账号來做限制并 LOG 记录
  - ▶ 启用后在 log 中的 User 一栏可看到 用户账号



ecurity Logs: M	onitor Che	ck Point security logs	, created by	the applian	ce				He
Enter search quer	y	👂 🥏 Refre	sh 🥐 Qu	iery Syntax	i View De	tails 🔀 Cl	ear 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.googlesyndication.com
Today 10:39:18		Application	WAN	G 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			×						
N	ethods for identifying users Comparison Active Directory Compared Seamless detection via your lease the seam	Queries local AD server								
	Browser-Based Authentication Users are required to enter their credentials in a portal									
2-3. 启	用 AD server 识別用	月戶身分(Active Directory	Queries) , Ź	习选后可点击						
С	onfigure 设定 AD s	erver 配置信息								
E	Active Direc	tory Queries	Configure							
	A No Active Directo	ry Server defined								
	Active Directory Queries			×						
	Use existing Active Director	y servers								
	Define a new Active Directo	ory 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)來识別用戶身分,当用戶开 启浏览器尝试登入受保护的网站时,需要先登入验证身分后才可继续
  - ▶ 启用 Browser-Based Authentication 后开启受保护网站,会显示 Login 页面。



Network Login		Check Point " Software Technologies LTD.
	Network Access Login In order to connect to the network, please enter your credentials Username Password Log In	

▶ 登入后可查看規定(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 Plicy 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

۲	On	QoS QoS options are not selected for the configured Internet connection Internet connections
	Off	No manual QoS rules configured
QoS [	Default Po	licy
🗸 En	sure low la	atency for delay sensitive services (e.g. VoIP)
Gu	arantee	20 % of the bandwidth to VPN traffic - on all services
Lir	nit bandw	dth consuming applications

#### 3-2. Policy

配置	QoS Poli	су											
🕕 Blade is	stade is not active (QoS). Dismiss												
Quality of	uality of Service Policy: Manage bandwidth by configuring Quality of Service (QoS) policy rules												
<ol> <li>Limit ba</li> <li>Limit lo</li> <li>★ New</li> </ol>	Elmit bandwidth consuming applications is disabled     Limit low latency traffic to 20% of bandwidth     * New ▼												
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。





#### 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

Policy			
◯ Strict			
Recommended			
Custom			
Tracking options:	🖹 Log 🔻		
Protection Activation			
High confidence:	Prevent		
Medium confidence:	Prevent		
Low confidence:	😵 Detect		
Severity:	Medium or above		
Performance impact:	Medium or lower		
		<ul> <li>Apply</li> </ul>	× Cancel

- ➤ 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



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 Pre	reat Prevention Exceptions										
<b>∦</b> New	🔆 New 🔻 🎤 Edit 🗙 Delete 🛱 Whitelists ▼										
No.	Source	Destination	Protection	Service	Action	Log	Comment				
Add threa	at prevention exception										

#### 1-3. Infected Hosts

查看受感染的主机

Infected Hosts: Display	infected h	osts and serve	ers in	the interna	al networks			
🔆 0 infected	hosts							
Type to filter	Q	C Refresh	T	Filter -	* Add Protection Exc	ception	Ex View I	Host Logs
Object Name	IP/MAC	Address	Dev	ice/Us	Incident Type	Se	verity	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

Type to filter Q	🧨 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	Trevent	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

调整特定策略的防护动作 PROTECTION SETTINGS: SQL INJECTION ★ General Protection Configuration Override IPS policy action: Prevent Detect Inactive Track: 
Log 
✓ Apply ★ Cancel

#### 2-2. Engine Settings

Check Point OFTWARE TECHNOLOGIES LTD.

进阶设定扫描引擎,可依具实际需求进行调整

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 Detece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

Bypass under load
✓ Bypass under load   Configure
Bypass under load tracking: 📄 Log 🔹
范例:当设备 CPU 高于 90%时停止 IPS · 低与 70%时启用 IPS
GATEWAY LOAD THRESHOLDS ×
IPS inspection is disabled if resource usage exceeds the High threshold. (1) It is re-enabled when usage falls below the Low threshold. (2) CPU Usage
Low: 70 - High: 90 - X
Low: 70 ♦ % High: 90 ♦ %
IPS is activated/deactivated when a threshold is crossed for over 10 seconds
✓ Apply × Cancel

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

· ^· Anti-Virus·

Protected scope

- Scan incoming files from External and DMZ ▼ interfaces
- Scan both incoming and outgoing files



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
- O 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):

Viruses:

According to policy	•
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)

	Anti-Virus User Me	essage	
Scanned protocols			
HTTP (on any port)	Ask Bloc	k Customize	
Mail (SMTP and POP3)	Message Conter	nt	~
FTP	Title:	Check Point Anti-Virus	
File types policy	Subject:	Are you sure?	
Process file types known to con	Body:	The site you are trying to access is classified as	
O Process all file types		malicious. Malware activity: Sactivity	
O Process specific file types famili		URL: \$original_url.	
Policy overrides		Reference: \$incident_id. Press OK to continue.	
URLs with malware (HTTP):			
Viruses:		Optional keywords	
Customize Anti-Virus user message	Ignore text:	Ignore warning	
- Anti-Bot			
Policy overrides	User must en	ter a reason	
Malicious activity:	Message Setting	le	
Reputation domains:	Fallback action:	Block 👻	
Penutation IPs:	Frequency	Once a day	

H. 设定 Anti-Bot 策略已覆蓋 Threat Prevention 中常规定义的 policy,若无特

#### 殊需求可不用调整

According to policy
According to policy -
According to policy -
According to policy
According to policy -

- 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來的流量如 External and DMZ, 或选择扫描所有出入文件 Scan both incoming and outgoing files
  - A-Threat Emulation

Protected scope

- Scan incoming files from External and DMZ ▼ interfaces
- 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. Threat Emulation File Types Type to filter 🛕 🔨 Edit Restore Defaults bz2 Bypass Bz2 archive Cab archive cab Bypass CSV Bypass Comma-se Edit File Type × Microsoft V doc Inspect docn Word mac Bypass Extension cab docx Microsoft V Inspect Action: O Inspect • Bypass dot Word templ Cab archive Description: Word macr dotm Bypass dotx Word tem Bypass exe Executabl Apply X Cancel Bypass Gz archive qz hwp Hangul Word Processor file Bypass Java archive file jar Bypass Adobe Acrobat document

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
- O 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



#### 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

Allow List		Block List			
Type to filter Q * New	🔨 Edit 🗙 Delete	Type to filter	Q <del>米</del> New	🔨 Edit 🛛 🗙 I	Delete
Sender / Domain / IP Address		Sender / Domain / IP Address	S		
192.168.223.70		Add a new Sender / Domain	/ IP Address		
Block the Following:	×				
Block the Following:	×				
IP address     Sender / Domain					
✓ Apply × Cancel					
✓ Apply × Cancel					

### 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

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	

Help



VPN Remote Access users can connect via:



# 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





New Connection	0	About	+	Site List	About
	-		Device-w	vide VPN	
Your Network	Capsule Cl	oud	O Ch	p <b>1400</b> .70.121, NB07	(j)
Manual C	onnection				
Server Name or IP	9 Address				
Display Name					
Cre	eate				
If this information is not contact your syst	available to you tem administrate	u please or			
ancel Lo	gin	About	Site List	0	Abou
Conne 10.2.7	ect to: 0.121				
NB07					
Password				CONNECTE	D
			0	0:00:1	9
Con	nect			Time Left: 07:59:41	
				User NB07	
				Site	
				10.2.70.121	
				Disconnect	

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

SSL Netwo	rk Extender		
Please enter v			
	our user name and pas	sword	d of an ActiveX / Java
User Name: Password:			ending on your conne he security certificate
User Name: Password:	Click for using SecurID		ending on your co he security certific h the completion c

B-4. Windows VPN Client 通过电脑建立 VPN 连接



1-2. Remote Access Users

200

设定允许访问的用户者



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

() No authentication servers are defined. Add Active Directory / RADIUS server

Type to fi	lter 🛛 🗙 Add 🚽 🔨 Edit	X Delete S Edit Permissions	
	Name	Remote Access	Comments
1	NB07	Ser permissions	
1	NB04	Ser permissions	
1	NB01	Ser permissions	
44	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 p	ermissions	

B. 点击Edit Permissions 给与现有用户的使用权限

Edit Re	mote Access Permissions	×
Selected (	3):	
Users X	RemoteUse1 × NB07 ×	
Filter: Use	rs  Active Directory	
51	Name	
⊻ 4	NB07	
∠ ∔	RemoteUse1	
	vpnuser	
	📀 Apply 🖉 Car	ncel



#### 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

Onice wode - Anocate IP addresses	5		
Office Mode Network:	172.16.10.0	A	
Office Mode Subnet:	255.255.255.0		
Route Internet traffic from connect Local encryption domain is defined a	ted clients through this gateway utomatically according to topology	в	
DNS servers for Remote Access use	s:	Configure manually	1
DNS servers for Remote Access use Office mode first DNS for clients: Office mode second DNS for clients:	This gateway Field is not mandatory	Configure manually	
DNS servers for Remote Access use Office mode first DNS for clients: Office mode second DNS for clients: Office mode third DNS for clients:	s: This gateway Field is not mandatory Field is not mandatory	Configure manually	с
DNS servers for Remote Access use Office mode first DNS for clients: Office mode second DNS for clients: Office mode third DNS for clients: DNS domain name:	s: This gateway Field is not mandatory Field is not mandatory Same as DNS domain name	Configure manually Configure manually	с
DNS servers for Remote Access use Office mode first DNS for clients: Office mode second DNS for clients: Office mode third DNS for clients: DNS domain name: SSL VPN Bookmarks	s: This gateway Field is not mandatory Field is not mandatory Same as DNS domain name	Configure manually Configure manually	с
DNS servers for Remote Access use Office mode first DNS for clients: Office mode second DNS for clients: Office mode third DNS for clients: DNS domain name: SSL VPN Bookmarks Type to filter Q	s: This gateway Field is not mandatory Field is not mandatory Same as DNS domain name * New * Edit × Delete	Configure manually	С

- 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





- 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 A	dvanced					
Site name:	RemoteVPN	^				
Connection type:	Host name or IP addres	55 🗸				
IP address	10.2.70.103					
Behind static NAT						
🔵 Host name						
Authentication						
Preshared secret						
Password:	•••••					
Confirm:	•••••					
○ Certificate						
Match certificate by DN						
Remote Site Encryption I	Domain					
Encryption domain:	Define remote network	topology manually 🗸 🗸				
Remove Select						
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 Encryptic	on Advanced					
Encryption settings:	Default (N	Default (Most compatible)				
IKE (Phase 1)						
Encryption:	3DES, AES	-128, AES-256	-			
Authentication:	MD5, SHA	1, SHA256	-			
Diffie-Hellman group suppor	Group 2 (1	1024 bit), Group 14 (2048 bit)	-			
Renegotiate every:	1440 r	minutes (24 hours)				
IPSec (Phase 2)						
Encryption:	3DES, AES	-128, AES-256	-			
Authentication:	MD5, SHA	1, SHA256	~			
Enable Perfect Forward Secrecy (better security, affects performance)						
Diffie-Hellman group sup	oort: Group 2 (1	1024 bit)	-			
Renegotiate every:	3600 s	seconds (60 minutes)				
			🗸 App	ly ×	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:		$\nabla$					
Initiate VPN tunnel using this gateway's identifier							
		~					
Additional Certificate Matching -							
Remote site certificate should be issued by:		Any Trusted CA 🔹					
	*	-	•				
		🗸 At	oply 🗙 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	Q 米 New	🔨 Edit	× Delete	🚍 Disable 🏑 Test	
Site Name				Host Name / IP Address	
RemoteSite				192.168.220.100	
RemoteLan				172.16.90.3	
Testing conne	ection to Rem	oteLan	l.		>

#### 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 Q C Refresh							
From		Site Name	Peer Address	Status			
No VPN tunnels foun	d						

#### 2-5. Advanced配置連接 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 automatic	ally according to topology				
Link selection					
Outgoing interface selection:					
<ul> <li>According to the routing table</li> </ul>					
<ul> <li>Route based probing</li> </ul>					
Source IP address selection:					
<ul> <li>Automatically chosen according to outg</li> </ul>	going interface				
O Manually configured:					
Tunnel health monitoring:					
Tunnel health monitoring method:	Tunnel test (Check Point Proprietary) 🔹				
Use DPD (Dead Peer Detection) responder mode					
Encryption Method					
IKEv2 global gateway ID: 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 米 Add	🔨 Edit	× Delete	👉 Export	🆄 Sign a Request
Trusted CA				E:	xpiration
Internal CA				W	ved 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						
Type to filter Q * New Signing F	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

可查看內部 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 CA Certificate 可导出自签证书。

Internal Certificate: Disp	play the appliance Internal CA certifica	ate and Internal VPN certificate				
Reinitialize Certifica	tes 👌 Replace Internal CA	<ul> <li>Export Internal CA Certificate</li> </ul>	🆄 Sign a Request			
Internal CA Certificate						
🕕 The internal CA cert	ificate is the certification which authe	enticates the internal CA to sign on the int	ernal certificates			
Certificate:	O=00:1C:7F:24:C5:BBmos57g					
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	2					
🕕 The internal VPN ce	rtificate is the certificate used for this	appliance to authenticate itself on VPN b	ased certificate configuration			
Certificate:	CN=00:1C:7F:24:C5:BB VPN Certifica	te,O=00:1C:7F:24:C5:BBmos57g				
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 O	SAG HIVE SUDS BELL JULY TIME				

# 七、Users & Objects 設定

# 1. User Management

1-1. User Awareness

参考四-2 User Awareness 设定

#### 1-2. Users

#### 点击 New 新增用户/用户组

Users: Create and edit permission	ns for users and groups
Type to filter Q	★ New ▼ ✓ Edit × Delete
Name	1 Local user
No users defined. Add a new us	🙅 Users Group



Users: Create and edit permissions for users and groups						
Type to f	ilter	Q	New 👻	🔨 Edit	× Delete	
	Name				Remote Access	Comments
1	NB07				Ser permissions	
1	NB04				Ser permissions	
1	NB01				Ser permissions	
	ManagerGroup				Scoup permissions	

#### 1-3. Administrators

与<u>三、2-2 Administrators</u>相同

1-4. Authentication Servers

新增认证服务器 RADIUS Servers 或 AD Server

> 新 增AD server



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

Neck Point WARE TECHNOLOGIES LTD.			
New Active Directory	Domain		×
Domain:	nico.com		
IPv4 address:	192.168.223.60		
User name:	administrator		
Password:	••••••		
User DN:		Discover	
Use user groups from	a specific branch only		
	New Active Directory I Domain: IPv4 address: User name: Password: User DN: Use user groups from	New Active Directory Domain         Domain:       nico.com         IPv4 address:       192.168.223.60         User name:       administrator         Password:       •••••••         User DN:       □         Use user groups from specific branch only	New Active Directory Domain   Domain:   nico.com   IPv4 address:   192.168.223.60   User name:   administrator   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

Application Management: Define custom applications and application groups 📲 Check Point AppWiki | 💄 Print | 🕑 Help Configure applications default policy in the Applications Blade Control page Filter by: Common | Custom | Categories | All Type to filter Q \star New 👻 × Delete 🔨 Edit 🗇 URL Name \*sysage.com.tw Application, URL Application Adds other software 88 Applications Group AIM ts File Transfer, Supports video/webcam, Logs IM, Encrypts communications, Instant Chat,.  $\mathcal{R}$ Alcohol & Tobacco Allows remote connect Allows remote control Encrypts communications, Share links, SSL Protocol, Low Risk, Media Sharing a Amazon Anonymizer 2 范例 新增 URL



#### 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 se				ervice objects	📑 Print	Help
Туре	to filter	Q 米 New 🔦 Edit	× Delete			
	Name	Туре	IP Pr	Destination Ports	Comments	
Q <sub>+</sub>	HTTP	🗲 TCP	6	80, 3128, 8080	Hypertext Transfer Protocol	~
Q <sub>+</sub>	FTP	👉 TCP	6	21	File Transfer Protocol	
Q <sub>+</sub>	PPTP_TCP	🗲 TCP	6	1723	Point-to-Point Tunneling Protocol, extension of PPP	
Ø <sub>+</sub>	SNMP	<b>⇐</b> UDP	17	161	Simple Network Management Protocol	
Q_	TFTP	← UDP	17	69	Trivial File Transfer Protocol	
Ø <sub>+</sub>	SSH	🗲 TCP	6	22	Secure shell, encrypted and authenticated rsh	
Q.	TELNET	🗲 TCP	6	23	Telnet Protocol	
Q.	SMTP	🗲 TCP	6	25	Simple Mail Transfer Protocol	
Q.	IMAP	🗲 TCP	6	143	Interactive Mail Access Protocol	

#### 2-4. Service Groups

#### 配置或新增 Service 組

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

Type t	to filter Q 🗶 New	🔨 Edit 🗙 Delete	
	Name	Туре	Comments
<b>O</b> <sub>+</sub>	DNS	🕃 Group	Domain Name system services
Q_	Mail	🕃 Group	Mail protocols
Q_	NetBios	🕃 Group	Network Basic Input-Output System
Q_	Web	🕃 Group	Web protocols
Ø,	Any_TCP_UDP	🕃 Group	Any TCP-UDP services
Q,	Delay_Sensitive_Services	🕃 Group	Delay sensitive services
Q.	Guaranteed_Bandwidth_Services	Croup	Guaranteed Bandwidth Services
Q.	VoIP	🕃 Group	VoIP Protocols
Q.	SIP	🕃 Group	Session Initialization Protocols, used in VoIP
G	NewGroup	🕃 Group	



新增 Service Group

New Service G	roup				×
Name:	NewGroup				
Comments:					
Type to filter	Q	🔆 New	× Remove	E Select.	
Services		C	Comments	<b>V</b> :	
No items were f	ound				

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

Sel	ect Services		×
*	New		
	Services	Comments	
$\checkmark$	HTTP	Hypertext Transfer Protocol	~
	FTP	File Transfer Protocol	
	PPTP_TCP	Point-to-Point Tunneling Protocol, extension of P	
$\checkmark$	SNMP	Simple Network Management Protocol	
	TFTP	Trivial File Transfer Protocol	
$\checkmark$	SSH	Secure shell, encrypted and authenticated rsh	
	TELNET	Telnet Protocol	
	SMTP	Simple Mail Transfer Protocol	
	IMAP	Interactive Mail Access Protocol	
	POP3	Post Office Protocol - Version 3	
	NNTP	Network News Transfer Protocol	
	DNS_UDP	Domain Name System Queries	~
Sele HT1	rcted items (3):		
		✓ Apply × Cance	el l

点击 Apply 后完成设定



New Service G	Group	×
Name: Comments:	NewGroup	
Type to filter	Q * New X Remove	
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

letwork Objects: Create and edit network objects that will be used in the device's feature configuration					
Type to filter	Q 🔆 New 💊 Edit 🗙 Delete				
Object Name	Туре	IP Addresses			
ManageLan	🚑 Network	192.168.1.0/255.255.255.0			
Lan223	🜉 IP Range	192.168.223.1-192.168.223.10			
Network224	A 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			
Туре:	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	Ӿ New	🔨 Edit	× Delete		
Name				Туре	Comments	
TestLanGroup				💽 Group	0	

#### 点击 New 可进行网络对象组的配置

New Network O	bject Group	×
Name:	NewGroup	
Comments:		
Type to filter	Q ★ New X Remove	-

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

Sele	elect Network Objects					
<u></u> ∦ №	lew					
	Network Objects					
	ManageLan					
	Lan223					
$\checkmark$	Network224					
$\checkmark$	ManagerIP					
	NB05					
	NetworkObject172					



# 八、 Logs & Monitoring

# 1. Logs

# 2-1. Security Logs

# 查看通过 Firewall 的日志

Security Logs: Monitor	r Che	ck Point secu	rity logs, create	ed by the applia	ance			Help
А			В	С	D	E	F	
Enter search query		Q CI	Refresh 🕐	Query Syntax	Ex View Details	× Clear Logs	🏟 Options 👻	
Time U.	E	Blade	Interface	Action	Source	Destination	Stop local logging	Rule
Today 17:03:24	:	Firewall	WAN	🔂 Accept	10.2.70.239	239.255.255	Eject SD card safely	Default policy (Incoming/
Today 17:03:05		Firewall	WAN	Accept	10.2.70.239	10.2.70.255	NetBIOSDatagram	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		× Q C	Refresh ?	Query Synta:	x 🔤 View Deta	ails 🗙 Clear Lo	gs 🔅 Options 🕶	
Time	U	Blade	Interface	Action	Source	Destination	Service	Rule
Today 17:02:48	<mark>N</mark>	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)
T 1 4704 50			1 4 4 14		400 400 4 5	40.0.05.0		DEFE FOR S

#### B. 更新 Log

#### 点击Refresh实时刷新日志数据

User:NB07	× c	Refrest	h 🕜 Quer	y Syntax ≣ <sub>w</sub>	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 (Out
Today 17:06:41	NB07	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Out
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	168.61.146.25	HTTPS	Default policy (Out
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Out
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	23.101.30.126	HTTPS	Default policy (Out
Today 17:06:27	NB07	Firewall	LAN1	Accept	192.168.1.5	10.2.25.2	DNS_UDP	Default policy (Out
T- J 47.00.07	ND07	and Firewood	LANIA	A	403 400 4 5	403 409 4 355	Napioonata	Defende en Enn /les

#### C. 选择对应日志点击后查看详细日志

Check Point SOFTWARE TECHNOLOGIES LTD.

Log Details					×
Accepted on rule Defail	ult policy (Outgoing)			< Prev	> Next
Log Info		More			-
Time	Today 17:06:41	Description	Accepted on rule Defau	lt	
Blade	Firewall		policy (Outgoing)		
Product Family	Network	Inzone	Internal		
Туре	E Log	Out-Zone	External		
Deller		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 Rul	e 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
--------------	---	------

Securit	Security Logs: Monitor Check Point security logs, created by the appliance							
Enter	search que	ry <b>Q</b>	<b>○</b> Refres	h 🕜 Query	Syntax 🔤 View Details	🗙 Clear Logs 🛱 O	ptions 🔻	
Time		Blade	Interface	Action	Source	Destination	Service	Rule
Today	y 11:11:34	Firewall	WAN	🖲 Drop	192.168.30.1	192.168.30.255	NetBIOSDatag	
Today	y 11:07:44	Firewall	WAN	🖲 Drop	192.168.30.1	192.168.30.255	NetBIOSName	
Today	y 11:07:44	Firewall	WAN	🖲 Drop	192.168.30.1	192.168.30.255	NetBIOSName	
Today	y 11:03:11	🗳 URL Fi						
Today	y 11:03:06	Applic						

#### E.查看選項

# 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 syst	System Logs: Monitor system logs, created by the appliance				
C Refresh X Clear Logs → Download Full Log File					
Time	Туре	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 Serv	/er:				
Management Server IP address:	0.0.0.0				
SIC Name: 🛛					
Set SIC one-time password:					
Confirm:					
Log server uses different IP address					
	✓ Apply X Cancel				

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



Ovelan Center			
Syslog Server			*
Name:	KiwiLog		
IP address:	192.168.1.4		
Port:	514		
Enable log server	ver		
Forwarded logs:			
System logs	s		
Security log	S		
System and	Security Logs		
		<ul> <li>Apply</li> </ul>	× Cancel

# 范例: Syslog Server 收到 防火墙发送的系统日志

😫 Kiwi Syslo	🖞 Kiwi Syslog Service Manager (14 Day evaluation - Version 9.6)							
File Edit	View Mar	nage Help						
🔒 🕗 🔜 💩 🚳 🗞 Display 01 💌 14 Days left in evaluation 🗾 Boy Now								
Date	Time	Priority	Hostname	Message A				
08-22-2017	17:56:57	System0.Notice	192.168.1.1	Aug 22 17:55:52+08:00 192.168.1.1 Action="drop" UUid="{0x0.0x0.0x0.0x0.0x0]" 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.Notice	192.168.1.1	Aug 22 17:55:47+08:00 192.168.1.1 Action="drop" UUid="{0x0.0x0.0x0.0x0.0x0}" 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.Notice	192.168.1.1	Aug 22 17:55:44:08:00 192.168.11 Action="drop" Ultid="{0x0.0x0.0x0.0x0}" inzone="External" outzone="Local" src="10.2.70.136" dst="255.255.255.255.255" 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.Notice	192.168.1.1	Aug 22 17:55:44:08:00 192:163:11 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="VPI-1 & FireVall-II" service="177500" s_port="17500"				
08-22-2017	17:56:49	System0.Notice	192.168.1.1	Aug 22 17:55:44:08:00 192:168:11 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="17:1500" s_port="17:500"				

# 2. Status

#### 3-1. Active Computers

与<u>三>一、Monitoring>2-1.Active Computers</u>相同

#### 3-2. Infected Hosts

与<u>三>四、Access Policy</u> 設定>1-3.Infected Hosts 相同

3-3. VPN Tunnels

与<u>三>六、VPN 設定>2-4.VPN Tunnels</u>相同

3-4. Connections



# 查看通过 firewall 的连接通信

Connections: View all active connections

Print | 3 Help

Type to filter	ype to filter Q C Refresh					
Protocol	Source Address	Source Port	Destination Address	Destination Port		
UDP	10.2.70.121	50002	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 <u>三>二、Home>2-2.Monitoring</u> 相同

#### 3-6. Reports

与 <u>=> 、Home>2-3.Reports</u>相同

# 3. Diagnostics



3-1. Tools

与三>二、Home>3-1.Tools 相同

#### 3-2. SNMP

点击 🔤 一 开启或关闭 SNMP · 点击" Configure..." 设定是否启用 SNMP traps

SNMP ON SNMP	: Monitor the device's status u SNMP Version: v1/v2 v3 Users <sup>©</sup> lew <sup>•</sup> Edit × Delete	sing SNMP 2/v3   SNMP Traps are e	nabled   Configure		Help
User	Name	Security Level			
Nov	3 users defined. Add SNMP v	3 User			
SNMP	<b>Traps Receivers <sup>©</sup></b> lew <b>\</b> Edit <b>X</b> Delete				
IP A	ddress	SNMP Version	Community Name	SNMP v3 User	
No r	eceivers defined. Add SNMP t	raps receiver			
SNMP	Traps <sup>©</sup>				
N E	dit				
	Event Name	Monitored Object	Value	Trap OID	Description
0	Interface disconnected	Interface link status		1.3.6.1.4.1.2620.1.200	Either network cable was
0	Interface unassigned	Interface IP address		1.3.6.1.4.1.2620.1.200	Interface IP address rem
0	High memory utilization	Memory utilization	> 90 %	1.3.6.1.4.1.2620.1.200	Memory utilization excee
0	Low disk space	Free disk space	<= 10 %	1.3.6.1.4.1.2620.1.200	Disk partition free space
0	LE LODUL CE LE	OBUL CELLE		4 3 6 4 4 4 3 6 3 4 3 6 9	000 100

# 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.進入 CONSOLE 重設

#### 1. 使用 WEB UI 介面

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



Check Po VNF App	pint pliance	
	<	System Operations: Manage your firmware version and backup your appliance
ò	Local Network	Appliance
HOME	Hotspot	Deheat the appliance
	Routing	Reboot Reboot the appliance
	MAC Filtering	Default Settings Restore factory default settings but keep the current firmware version
	DNS	Factory Defaults Revert to the factory default image and settings.
:::	Proxy	The factory firmware version is R80.20.10 (992001203)
ACCESS POLICY	• System	Firmware Upgrade
â	System Operations	The current firmware version is R80.20.10 (992001203)
THREAT	Administrators	A Could not connect to Check Point Upgrade Service. Check Internet connection   Try again
PREVENTION	Administrator Access	Configure automatic upgrades
22.0	Device Details	Manual Upgrade Revert to Previous Image
VPN	Date and Time	Backup and Restore System Settings
	DDNS & Device Access	Periodic backup is OFF   Settings
USERS &	Tools	Create Backup File Restore
OBJECTS	<ul> <li>Certificates</li> </ul>	
~	Installed Certificates	
LOGS & MONITORING	Internal Certificate	

#### 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

-		 	11 111		
RESET	2/Sync — 4 — 6 — 8 1 — 3 — 5 — 7	WAN	USB 3.0	CONSOLE	Power DC 12V



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:



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



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 se t 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

Check Po VNF App	bint bliance	
		System Operations: Manage your firmware version and backup your appliance
<b>```</b>	<ul> <li>Network</li> </ul>	
HOME	Internet	Арриансе
	Local Network	Reboot Reboot the appliance
	Hotspot	Default Settings Restore factory default settings but keep the current firmware version
DEVICE	Routing	Factory Defaults Revert to the factory default image and settings.
:::	MAC Filtering	The factory firmware version is R80.20.10 (992001203)
ACCESS POLICY	DNS	Eirmware Ungrade
~	Proxy	The current firmware version is <b>R80 20 10 (992001203)</b>
THREAT	<ul> <li>System</li> </ul>	Could not connect to Check Point Upgrade Service. Check Internet connection   Try again
PREVENTION	System Operations	Configure automatic upgrades
24-0	Administrators	Manual Upgrade Revert to Previous Image
VPN	Administrator Access	Backup and Restore System Settings
	Device Details	Periodic hackun is OFE   Settings
	Date and Time	Create Backup File Restore
OBJECTS	DDNS & Device Access	

输入 Comment-选择Create Backup



BACKUP SETTINGS					
Backup Settings					
Use file encryption					
Set password:					
Confirm password:					
Comment:	0322				
Backup File Content	S				
✓ Backup system settings					
Create Backup	Cancel	Help			

# 选择 Download Backup

BACKUP SETTINGS		×
Backup Settings		
Use file encryption		
Set password:		
Confirm password:		
Comment:	0322	
Backup File Content	S	
✓ Backup system settir	ngs	
Download Backup	Cancel	Help
Click the Download but	ton to save the bac	kup file



Do you want to open or save Gateway-ID-7F7AD148\_R77.20.31\_990170952\_2017-Mar-22-11\_42\_37.zip from 192.168.1.1?

Open

Save 

Cancel

# 2. 计划备份

Check Po VNF App	vint oliance			
		System Operations: Manage your firmware version and backup your appliance		
8	<ul> <li>Network</li> </ul>	Appliance		
HOME	Internet	Аррнансе		
	Local Network	Reboot Reboot the appliance		
	Hotspot	Default Settings Restore factory default settings but keep the current firmware version		
DEVICE	Routing	Factory Defaults Revert to the factory default image and settings.		
:::	MAC Filtering	The factory firmware version is R80.20.10 (992001203)		
ACCESS POLICY	DNS	Firmware Upgrade		
~	Proxy	The current firmware version is <b>R80 20 10 (992001203</b> )		
	<ul> <li>▼ System</li> </ul>	Could not connect to Check Point Upgrade Service. Check Internet connection   Try again		
PREVENTION	System Operations	Configure automatic upgrades		
24-0	Administrators	Manual Upgrade Revert to Previous Image		
VPN	Administrator Access	Backup and Restore System Settings		
	Device Details	Deriodis backup is OEE   Settings		
<u>2</u> 2	Date and Time	Create Backup File Restore		
USERS &		Ci cate backup nie Restore		

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	
O Weekly	
Monthly	
Day of month:	1st 🗸
Time of day:	00:00 - 01:00
	Apply O Cancel



#### 3. 恢复

Check Po VNF App	liance			
		System Operations: Manage your firmware version and backup your appliance		
	<ul> <li>Network</li> </ul>	A		
HOME	Internet	Appliance		
	Local Network	Reboot	Reboot the appliance	
	Hotspot	Default Settings	Restore factory default settings but keep the cur	rent firmware version
DEVICE	Routing	Factory Defaults	Revert to the factory default image and settings.	
:::	MAC Filtering		The factory firmware version is R80.20.10 (99200	01203)
ACCESS POLICY	DNS	Firmware Upgrade		
Â	Proxy	The current firmware version is R80	.20.10 (992001203)	
THREAT PREVENTION	<ul> <li>System</li> </ul>	🛕 Could not connect to Check Poir	t Upgrade Service. Check Internet connection   T	ry again
	System Operations	Configure automatic upgrades		
24-0	Administrators	Manual Upgrade	Revert to Previous Image	
● <b>↓</b> ● VPN	Administrator Access	Backup and Restore System Setting	25	
	Device Details	Periodic backup is OFF   Settings		
USERS &	Date and Time	Create Backup File	Restore	
OBIECTS	DDNS & Device Access			

# 选择 Restore 恢复配置→选择上传配置文件

Restore Setti	ngs	×		
Upload Settings File				
Settings file:	Select a settings file Browse			
Upload File	Close			
Restore Sett	lings	×		
Upload Setti	ings File			
Settings file:	Gateway-ID-7F7AD148_R77.20.31_99017			
Settings file:	Gateway-ID-7F7AD148_R77.20.31_99017 Browse			



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

Rebooting...

Please wait while the appliance reboots...

Appliance will be up in about 251 seconds