目錄:

→ 、	架構圖 & Lab 架設步驟:2
<u> </u>	Enviroment and Prepare :
三、	Depoly one AD Server \circ
四、	安裝 vCenter 6.5 版本:4
略	
五 、	建立 Datacenter、Cluster、virtual Distributed Switch。4
略	4
六、	Deploy one NSX Manager \circ 4
と、	CheckPoint :
八、	設定 vCenter 新增 Service。14
九、	Configuring NSX redirect traffic to the Security Gateway Virual Edition :
+ 、	驗證:





LAB 架設流程:

- 1. 準備 AD Windows2012 並設定好各主機 DSN 解析。
- 2. 安裝設定兩台 ESXi 5.5 版本以上。
- 3. 安裝設定 vCenter 6.5 版本。
- 4. vCenter 納管兩台 ESXi。
- 5. 設定 Distribution Switch。
- 6. 設定 iSCSI Storage 主機,並設定 vCenter 的兩台 ESXI 共用 iSCSI Storage。
- 7. 安裝設定 NSX 6.3 版本,整合 vCenter & NSX。
- 8. 發布 NSX Controller、設定 NSX Host Preparation、Logical Network Preparation。
- 9. 安裝 CHP SMS, install 最新 jumbo hotfix、Check_Point_R80.10_vSEC_Service_Hotfix4_FULL。

10. 啟動 vsec。

- 11. 連線 SmartConsole 新增 DataCenter 物件 vCenter、NSX。
- 12. 透過 ssh 連到 SMS 設定 vsec_config 的 nsx 參數,在 vCenter 設定 NSX 的 Service Deploymemts。
- 13. 等待 vSEC Service deployment(vSEC Firewall)佈署完成,登入 SMS 調整 Cluster 物件。
- 14. 修改 policy 後 install policy。
- 15. 回到 vCenter 設定 Service Composer。
- 16. 打開 Client 測試連線。

\Box > Enviroment and Prepare :

- 1. AD Windows 2012 $\,^\circ$
- 2. VMWare vCenter (version 6.5.0.12000 Appliance) File : VMware-VCSA-all-6.5.0-7119157.iso •
- VMWare NSX Manager (version 6.3.5-7119875 Appliacne)
 File : upgrae from 6.2.2 version , VMware-NSX-Manager-upgrade-bundle-6.3.5-7119875.tar.gz
- 4. ESXi (version 5.5 u3) and 2 appliance with cluster \circ
- 5. CheckPoint SMS R80.10 $\,^{\rm o}$ Recommand $\,$ RAM 16GB $\,^{\rm o}$

File :

- (i) Check_Point_R80.10_T421_Gaia.iso •
- (ii) Check_Point_R80.10_vSEC_Service_Hotfix4_FULL.tgz (vSEC patch)
- (iii) Check_Point_Security_Gateway_R77_30_vSEC_for_NSX_v4_OVF.tgz (vSEC Firewall)

Network	VLAN	Network / Mask	Gateway	Related Network Interfaces
Management Network / vMotion Network / VXLAN Network	230	192.168.230.0/24	192.168.230.254	Mgmt Cluster Host Management Kernel / VC / NSX Manager / Controllers / VM or Physical Machines on Physical Network

Component	Hostname	IP Address	Gateway	Note
AD/DNS	ad.9fdemolab.com	192.168.230.10	192.168.230.254	
vCenter	vc65.9fdemolab.com	192.168.230.18	192.168.230.254	
NSX Manager IP	nsx.9fdemolab.com	192.168.230.19	192.168.230.254	
NSX Controller IP	-	192.168.230.31-40	192.168.230.254	
CheckPoint vSEC		102 169 220 56 60	102 169 220 254	
Service		192.108.230.30-00	192.108.230.234	
ChecPoint SMS		192.168.230.51	192.168.230.254	R80.10
ESXi-16	esxi-16.9fdemolab.com	192.168.230.16	192.168.230.254	
	esxi-17.9fdemolab.com	192.168.230.17	192.168.230.254	
				include AD 🕥
ESXi		192.168.230.15	192.168.230.254	vCenter NSX
				CHP SMS

略

四、安裝 vCenter 6.5 版本:

略

五、建立 Datacenter、Cluster、virtual Distributed Switch。

略

- 六、Deploy one NSX Manager \circ
 - 1. NSX Deployment •

略

- 2. 設定 NSX Manager。
 - a. 開啟瀏覽器 <u>https://<NSX manager IP></u> or <u>https://nsx.9fdemolab.com</u>,帳號:admin,密碼: P@ssw0rd。



b. 點擊『Manage Appliance Settings』, 點選『NSX Management Service』, 於 Lookup Service, 點 擊『Edit』。

VMware NSX Manager X +		_ _ ×	
🛞 🕐 🔍 https://normenager.sysage.vm.lab/index.html Ø väphere Web Client 🔳 Wilvere Appliance	C Q 277 ☆ 自	↓ ☆ © ⊇	Whware NSX Manager
NSX Manager Virtual Appliance Management	in 172 186.131 Name naxmanagar	Version: 6.2.2 Build 3604007	Volver Web Client Volvare Applance P. 172.168.131 Verson: 62.2.84d 3064007 Nover maxmanager Volver adma Summary Manage
Week Summary Manage Applance Settings Manage vCenter Registration	Download Tech Support Log Backup & Restore Upgrade		SETTINGS Lookup Service Edit General For X-Entre resions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Manageme Network Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly. SSC. Conficutes Lookup Service: Backups & Restore
			Upgrade COMPORTS COMPORTS CONFORMENTS CONFORMENTS Connecting to a Confert Server enables NSX Management Service to display the VMware Initiastructure Inventory. HTTPS pot (43) needs to be post of communication between NSX Management Service, ESX and VC. For a full its of pots required, see section 'Client and User Access' Chapter Preparing for Installation' In the NSX Installation and Upgrade Oxide'.
			If your/Center server is hosted by a XCenter Sarver Applance, please easure that appropriate CPU and memory reservation is given to this applie VM. After successful configuration of VCenter on NSX Manager, you need to log out of any active client sessions on VSphere Web Client and log ba in to enable NSX user interface components. VCenter Server:

 c. NSX Manager 連結 vCenter PSC(SSO): Lookup Service IP: 192.168.230.18 or vc65.9fdemolab.com, Lookup Service Port: 7444,帳號:<u>administrator@9fdemolab.com</u>, 密碼: P@ssw0rd,點擊『Yes』。

Lookup Service URL		×
For vCenter versions 5.5 and abov administrator credentials to registe recommended to set the NTP serve	e, you may configure Lookup Service and provide the SSO r NSX Management Service as a solution user. It is also er for SSO configuration to work correctly.	
Lookup Service Host:	vc65.9fdemolab.com	
Lookup Service Port:	7444	
	Enter port 443 for vSphere 6.0, for vSphere 5.5 use 7444.	
Lookup Service URL:	https://vc65.9fdemolab.com:7444/lookupservice/sdk	
SSO Administrator User Name:	administrator@9fdemolab.com	
Password:		
	OK Cance	əl

d. Lookup Service 設定完成,於 vCenter Server 點擊『Edit』, NSX Manager 連結 vCenter Server : vCenter Server : 192.168.230.18 or vc65.9fdemolab.com, vCenter User Name :

administrator@9fdemolab.com,Password:P@ssw0rd,點擊『Yes』。

vCenter Server		×		
Connecting to a vCenter s	erver enables NSX Management Service to display the VM	ware		
Infrastructure inventory. H	TTPS port (443) needs to be opened for communication be	tween NSX		
Management Service, ES	K and VC. For a full list of ports required, see section 'Clien	t and User		
Access' of Chapter 'Prepa	ring for Installation' in the 'NSX Installation and Upgrade Gu	iide'.		
If your vCenter server is h	osted by a vCenter Server Appliance, please ensure that a	opropriate		
CPU and memory reserva	tion is given to this appliance VM. After successful configur	ation of		
vCenter on NSX Manager	you need to log out of any active client sessions on vSphe	re Web Client		
and log back in to enable I	NSX user interface components.			
vCenter Server:	vc65.0fdemolah.com			
···O · ·······························	Yoo, Jacinolab.com			
vCenter User Name.	administrator@9fdemolab.com			
Password:				
Modify plugin script	download location			
	OK	Cancel		
設定完成。				
vmware [.]			IP: 192.168.230.19	Version: 6.3.5 Build 7119
NSX			Name: nsx	User admin

	Summary	Mana	age				
SE	TTINGS		Lookup Service URL			Unconfigure	Edit
G	eneral etwork		For vCenter versions 5.5 a Management Service as a	and above, you solution user.	u may configure Lookup Service and provide the SSO administrator creder . It is also recommended to set the NTP server for SSO configuration to we	ntials to register NS. ork correctly.	x
s	SL Certificates		Lookup Service URL:	h	https://vc65.9fdemolab.com:7444/lookupservice/sdk		
в	ackups & Rest	ore	SSO Administrator User	Name: a	administrator@9fdemolab.com		
U	pgrade		Status:	9	🔍 Connected 💋		
CO	MPONENTS						
N	SX Manageme	nt	vCenter Server				Edit
			Connecting to a vCenter si opened for communication of Chapter 'Preparing for Ir If your vCenter server is ho appliance VM. After succes	erver enables between NS3 nstallation' in t osted by a vC4 ssful configura	NSX Management Service to display the VMware Infrastructure inventory X Management Service, ESX and VC. For a full list of ports required, see the 'NSX Installation and Upgrade Guide'. enter Server Appliance, please ensure that appropriate CPU and memory ation of vCenter on NSX Manager, you need to log out of any active client	. HTTPS port (443) section 'Client and U reservation is given sessions on vSpher	needs to be Jser Access' to this re Web
			Client and log back in to er	nable NSX us	er interface components.		
			vCenter Server:	vc65.9fdem	nolab.com		

vCenter Server:	vc65.9fdemolab.com
vCenter User Name:	administrator@9fdemolab.com
Status:	🞈 Connected - Last successful inventory update was on Tue, 05 Dec 2017 08:07:16 GMT 🧲

f. 匯入 NSX License。

從 Home > administration > Licensing > Licenses 中匯入。

3. 發佈 NSX Controller。

e.

a. 採用 vSphere Web Client,登入 vCenter。<u>https://vc65.9fdemolab.com/vsphere-client</u> or <u>https://192.168.230.18/vsphere-client</u>,帳號:administrator@9fdemolab.com 密碼: P@ssw0rd。

) 🕘 🎯 https://192.1	68 🔎 👻 憑證 ぐ	🧭 vSphere Web Client	× 👩 VMware NSX Manager Virtu	- □ ☆☆
vm ware [,]				
User name:	example@domai	n.local	VMware [®] vCenter [®] Single	Sign-On
Password:	Use Windows s	ession authentication		

b. 點選『Networking & Security』,新增 Controller(將 Controller 部署在 Management Cluster 下的 ESXi)。

ØvSphere Web Client ×	+						- 0 X	vmw	are vSphere Web Cli	ent nt≣	O I Adminis	trator@VSPHERELOCAL + I #	湖• (Q	
🐑 🖬 🔍 🔒 https://vcenter6u2.sys	age-vm.lab/vsphere-	lient/?csp#exten	iorld%i C	Q. <u>#</u> #	\$	⊕ ↓ ☆	⊚ ⊠ ≡	14958	25 ¥	Installation				
🖗 vSphere Web Client 🏧 VMware App	pliance							< 8	e 🖻 🕤	Management Host P	reparation Logical Network I	Preparation Service Deployments	i	
Ministry VSphere Web Clive SFR2 a C110000 b SFR3 b C110000 b C1100000 b	Int filler	20008x	DI Admonistra ED Admonistra Admon	Regentreficie Los	(ж) (дой) - 	C. MA	. 0 10 AB 10 AB		In Home setublic of the security CR Home estilation ogical Switches CR Edges invali poofGuard ence Detribuns ence Composer lata Security	NSX Managers Actions NSC Manager 172.16.8.131	IF Address 172 16 8 131	<center< th=""><th>Q 21285 Veson 6223804967</th><th>• 1 御夜日</th></center<>	Q 21285 Veson 6223804967	• 1 御夜日
VRealize Orchestrator > Networking & Security > Statestrate >	Hybrid Cloud Manager	vRealize Orchestrator	Networking & Security				10 m		Flow Monitoring Activity Monitoring Traceflow	NSX Controller notes	NSX Managar St	tatua Pasas	Q. 31535 Software Venion	•
 工作 ZEEDEE 事件 希臘 	ジェルション		vRealize Operations Manager	1955. 1955.1952.	上記味器站存在 资9]	BURGERA	0 BUDIO	- Ne	tworking & Security Inventory NSX Managers					
☐ Bitsation d	7.00019 20 7.0 2 2.0407.5	alia Refere	<mark>2</mark> 1918	5PMMXMI										0 個項目
		_	_	_	_	Sh (T) LA (Sh TD and a damage	

c. 選擇要部署的 ESXi,及其網路和 datastore, Connected To:點選 Select,點選 DPoortGroup230。

		Select Network ?
Add Controller	?	Select network for Controller. Object Type: Distributed Port Group
Name:	* NSX-Controller	Selected: A DPortGroup 230
NSX Manager: Datacenter:	* 192.168.230.19 * Datacenter	Available Objects
Cluster/Resource P	ool: * 9FDemoLAB Cluster	 ✓ A DPortGroup 230 ▲ DPortGroup 70
Host:		 vxw-vmknicPg-dvs-81-230-36f4f819-934b-4cc7-b77 DPortGroup 210
Folder Connected To:	Select Remove	
IP Pool:	* Select	
		4 items 🕒 Copy ▾
	OK Cancel	OK Cancel

d. Connected To: Mgmt Management Network,IP Pool: 點選 Select,新增 IP Pool 提供 Controller 所需 IP 位址範圍,點選 New IP Pool...。

dd Controller			?	Select IP Pool	(1
				Select an IP Pool for controller IP allo	ocation.
Name:	*	NSX-Controller		Selected:	
NSX Manager:	*	192.168.230.19	•	(Q , Filter
Datacenter:	*	Datacenter	•	Available Objects	
Cluster/Resource Pool:	*	9FDemoLAB Cluster	•	NSX-Controller-Pool	
Datastore:	*	datastore16	•	() vSEC_Firewall	
Host:			•		
Folder			•		
Connected To:	*	DPortGroup 230 Change	Remove		
IP Pool:	*		Select		
					2 items ∎Copy +
				New IP Pool	
		ОК	Cancel		OK Cancel

e. 新增 IP Pool 並輸入 Controller IP 資訊,點選該 IP Pool。

Add Static IP	Pool	Select IP Pool (?)
Name: Gateway: Prefix Length: Primary DNS: Secondary DNS:	 NSX-Controller-Pool 192.168.230.254 A gateway can be any IPv4 or IPv6 address. 24 192.168.230.10 	Select an IP Pool for controller IP allocation. Selected: Available Objects (SX-Controller-Pool (VSEC_Firewall
Static IP Pool:	* 192.168.230.31-192.168.230.40 for example 192.168.1.2-192.168.1.100 or abcd:87:87::10-abcd:87:87::20	2 items টি Copy → New IP Pool
	OK Cancel	OK Cancel

f. 密碼: PAssw0rd123!

Add Controller		?	Add Controller				?
Name:	* NSX-Controller	_	NSX Manager:	*	172.16.8.131	•	
NSX Manager:	* 192.168.230.19	•	Datacenter:	*	Datacenter	•	
Datacenter:	* Datacenter	•	Cluster/Resource Pool:	*	Management Cluster	•)	
Cluster/Resource Pool:	* 9FDemoLAB Cluster	•	Datastore:	*	datastore-Mgmt-1	•	
Datastore:	* HDS-FC-Storage	•	Host:		mgmt-1.sysage-vm.lab	•	
Host:		•	Folder			•	
Folder		•	Connected To:	*	Mgmt Management Change	F	Remove
Connected To:	* DPortGroup 230 Chan	ge Remove	IP Pool:	*	NSX-Controller-Pool		Select
IP Pool:	* NSX-Controller-Pool	Select	Password:	*	****		
			Confirm password:	*	*****		
	ОК	Cancel			確定		取消

g. 依照 b~f步驟建立第 2 個 NSX Controller。

vmware [®] vSphere Web Cli	ent n ≘		c	J Administrator@9FDEMOLAB	.COM - I Help - I 🤇	Q Search
Navigator I	Installation					
Back	Management Host Preparatio	on Logical Network Preparati	ion Service Deployments			2) W
Networking & Security						fork
👯 NSX Home	NSX Managers					n Pro
🖓 Dashboard	🔯 Actions				(🕈 Filter 🔹 🖣
🔅 Installation	NSX Manager	IP Address		vCenter	Version	ö
羷 Logical Switches	192.168.230.19	192.168.230.19		192.168.230.18	6.3.5.7119875	
NSX Edges						9
👸 Firewall						Rece
Regional Spool Guard						ntia
Service Definitions						sks
Service Composer						1 items
▼ Tools						
How Monitoring	NSX Controller nodes					् र
Endpoint Monitoring	💠 🗙 📋 🍪 Actions				(۲ Filter •
 Networking & Security Inventory 	Name	Controller Node	NSX Manager	Status	Peers	Software Ve
👭 NSX Managers 🔰	NSX-Controller-2	192.168.230.32	192.168.230.19	 Connected 		6.3.707
		controller-2		🔥 Disk Alert		2
	NSX-Controller	192.168.230.31	192.168.230.19	 Connected 		6.3.707
		controller-1				9
						larm
						8
						2 items

h. 安裝至此 vCenter 中會有 1 台 AD、1 台 vCenter、1 台 NSX Manager、2 台 NSX Controller。



- 4. Host Preparation :
 - a. 於 Cluster (9FDemoLAB Cluster) 中點擊安裝。備註: NSX Manger/vCenter/ESXi 間的名稱解析 (正反解)及校時,都需正常。(此部分抓圖不是本次 LAB 的圖)(NSX License 需先匯入)



b. 點擊『是』。

· 導覽器	Installation						
 (1首頁) 	Management Host Preparati	on Logical Network Preparatio	n Service Deployments				
Networking & Security NSX Home Installation	NSX Manager: 172.16.8.131	•					
Sector States	NSX Component Installation on Hosts						
NSX Edges	Actions						
Firewall	Clusters & Hosts	Installation Status	Firewall	VXLAN			
SpoofGuard	Management Cluster	Not Installed	Not Configured	Not Configured			
Service Composer	mgmt-1 eve and um lab Compute Clu	ister - Install					
 Tools 	Compute C Are you sur	e you want to continue with the in	stall? figured	Not Configured			
👿 Flow Monitoring	Comp-4.	是否					
Retivity Monitoring	comp-3.sysage-vm.lab						
😫 Traceflow							
 Networking & Security Inventory 							
🖁 NSX Managers 💦 🔪							

c. 等待安裝完成。

導覧器 耳	Installation				
	Management Host Preparatio	n Logical Network Preparatio	n Service Deployments		
Networking & Security					
🔡 NSX Home	NSX Manager: 172.16.8.131	•			
🔅 Installation		11			
🆄 Logical Switches	NSX Component installation on	Hosts			
NSX Edges	Actions				
👸 Firewall	Clusters & Hosts	Installation Status	Firewall	VXLAN	
🖷 SpoofGuard	▼ 🛱 Management Cluster	Not Installed	Not Configured	Not Configured	
Service Definitions	mgmt-1.sysage-vm.lab				
Service Composer	momt-2 sysage-ym lab				
Data Security	▼ IBCompute Cluster	**: Installing	e Linknown		
+ 100IS		<pre>spinstaning</pre>			
Levi Flow Monitoring	Comp-4.sysage-vm.lab	In Progress	Not Configured		
	Comp-3.sysage-vm.lab	1 In Progress	Not Configured		
Networking & Security Inventory					
NSX Managers					
· · · ·					
		·			
芬 覽器 耳	Installation				
導號器 I (1首頁) ③	Installation Management Host Preparation	on Logical Network Preparatio	n Service Deployments		
導致器 Image: Constraint of the second secon	Installation Management Host Preparation	on Logical Network Preparatio	n Service Deployments		
· 導致器 ↓ ◆ 首頁 >> ⑦ Networking & Security 優 NSX Home	Installation Management Host Preparatie NSX Manager: 172.16.8.131	on Logical Network Preparatio	n Service Deployments		
· 補稅器 平 ◆ 首頁 ● ⑦ Networking & Security 操 NSX Home 意 Installation	Installation Management Host Preparation NSX Manager: 172.16.8.131 NSX Component Installation on	n Logical Network Preparatio	n Service Deployments		
· 著號器 単 ・ 首頁) ⑦ Networking & Security 課 NSX Home 意 Installation 像 Logical Switches ■	Installation Management Host Preparation NSX Manager: 172.16.8.131 NSX Component Installation on	Logical Network Preparatic Hosts	n Service Deployments		
	Installation Management Host Preparation NSX Manager: 172.16.8.131 NSX Component Installation on Actions	Logical Network Preparatio Hosts	n Service Deployments		
· · · · · · · · · ·	Installation Management Host Preparation NSX Manager: 172.16.8.131 NSX Component Installation on Actions Cluster & Hosts	n Logical Network Preparatio	n Service Deployments	VZLAN	
·	Installation Management Host Preparation NSX Manager: 172.16.8.131 NSX Component Installation on	n Logical Network Preparatio	n Service Deployments Firewall Not Configured	VXLAN Not Configured	
	Installation Management Host Preparative NSX Manager: 172.16.8.131 NSX Component Installation on Actions Cluster & Hosts Tig Management Cluster Impmt-1.sysage-ym.lab	n Logical Network Preparatio	n Service Deployments Firewall Not Configured	VXLAN Not Configured	
導致器 其 ◆ 首頁 ▶ ⑦ Networking & Security ● ● Institution ● ● Logical Switches ● ● NSX Edges ● ● Firewall ● ● SportGuard ● ● Service Definitions ● ● Data Security ●	Installation Management Host Preparative NSX Manager: 172.16.8.131 NSX Component Installation on Actions Clusters & Hots	n Logical Network Preparatio	n Service Deployments Firewall Not Configured	VXLAN Not Configured	
·	Installation Management Host Preparative NSX Manager: 172.16.8.131 NSX Component Installation on		n Service Deployments	VXLAN Not Configured	
· 補充 · 甘百 · 七百 · 七百 · 七百 · · · · · · · · · · · · · · · · · · ·	Installation Management Host Preparativ NSX Manager: 172.16.8.131 NSX Component Installation on		n Service Deployments	VXLAN Not Configured Not Configured	
·	Installation Management Host Preparativ NSX Manager: 172.16.8.131 NSX Component Installation on		n Service Deployments	VXLAN Not Configured Not Configured	
	Installation Management Host Preparation NSX Manager: 172.16.8.131 NSX Component Installation on	Installetion Status Not Installed	n Service Deployments	VXLAN Not Configured Not Configured	
研究器 単 ● 首页 ・ NExtvorking & Security ・ ● NSX Home ・ ● Logical Switches ・ ● Logical Switches ・ ● Service Composer ● ● Data Security ・ ● Tools ● ● Flow Monitoring ● ● Coldital Security ・ ● Tools ● ● Toreeflow ・ ● Networking & Security Inventory	Installation Management Host Preparativ NSX Manager: 172.16.8.131 NSX Component Installation on Actions Cluster & Hods ▼ ∰Management Cluster	n Logical Network Preparation	rirevall Firevall Vt Configured Finabled Finabled Finabled	VXLAN Not Configured Not Configured	

d. 點擊『Configure VXLAN』, 點選 Use IP Pool, 並點擊 New IP Pool, 點擊 OK。

導覽器 I	Installation			
	Management Host Preparati	on Logical Network Preparatio	n Service Deployments	
Networking & Security	NSX Manager: 172.16.8.131	•		
Logical Switches	NSX Component Installation on	Hosts		
NSX Edges	🔯 Actions			
7 Firewall	Clusters & Hosts	Installation Status	Firewall	VXLAN
SpoofGuard	▼ 🛍 Management Cluster	Not Installed	Not Configured	Not Configured
Service Definitions	mgmt-1.sysage-vm.lab			
Service Composer	mgmt-2.sysage-vm.lab			
Tools	Gompute Cluster	✔ 6.2.2	 Enabled 	Not Configured
🙀 Flow Monitoring	comp-4.sysage-vm.lab	✔ 6.2.2	✓Enabled	orce Sync Services
Activity Monitoring	comp-3.sysage-vm.lab	✓ 6.2.2	✓ Enabled C	hange IP Detection Type
😫 Traceflow		•	C	hange Locale ID
 Networking & Security Inventory 				onfigure VXLAN
🚦 NSX Managers 🔋 🔰			U	ninstall
Compute Cluster - Configu	ure VXLAN Networking	?	**	
Switch:	* vDS-Comp	•		
VLAN:	* 0			
MTU:	* 1600			
VMKNic IP Addressing:	* O Use DHCP			
	Use IP Pool N	SX-Controller 🔹		
VMKNic Teaming Policy:	* Fail Over	SX-Controller-Pool		
VTEP:	* 1	W IF F 001		
		OK Cancel)	

此部分我選擇前面步驟設定好的 NSX-Controller-Pool

e. 完成。



- 5. 設定 Logical Network Preparation:
 - a. 切換到 Logical Network Preparation,可看到第 4 步驟設定的 VXLAN IP,此 VXLAN IP 其實是 VMKernl Port。



- \pm 、 CheckPoint :
 - 登入 CHP SMS 的 WebUI(安裝省略),透過 CPUSE 安裝最新的 jumbo hotfix 和 Check_Point_R80.10_vSEC_Service_Hotfix4_FULL.tgz。(License & Contract 請先申請並匯入)



2. 使用 ssh 或 console 登入 SMS, 並進入 expert mode, 輸入指令 vsec on 啟動 vsec 功能。



3. 登入 CHP SMS 的 SmartConsole,新增物件 Data Center > NSX 和 vCenter。



 把檔案 Check_Point_Security_Gateway_R77_30_vSEC_for_NSX_v4_OVF.tgz 解壓縮後的所有檔案, 傳送到 SMS 的\$FWDIR/VE/jetty/ve 中。



5. 接著輸入指令 vsec_config, 選擇 1.VMware Configuratin, 確認 Service Manager IP 是 SMS IP, 請 URL 中的 ovf 檔名,與上一步驟傳送的檔名一致,輸入 y 並按 Enter。



6. 輸入 y 確定要 register a new service, 並選擇 1.nsx。

```
Below are the defaults that will be used for this vSEC Manager Server:
      Service Manager IP Address: 192.168.230.51
      URL of OVF: https://192.168.230.51:443/ve/Security_Gateway_R77_30VSEC.ovf
   Do you accept the default values? (y/n: y to accept, n to change) [y]:
   Service Manager thumbprint has been updated for nsx.
   Would you want to register a new service now?
    (y/n) [y]:
   The following NSX Managers are configured in SmartConsole. Select NSX manager:
      1. nsx
          Back
   Selected option: 1
7. 選擇 1.admin, 並輸入 SMS 所屬 admin 密碼。
   Please Choose an administrator from the list below.
   This administrator will be used by the NSX for authentication
       1.
            admin
       2.
            Back
   Selected option: 1
   Please enter the password of the administrator you chose
   Password:
    Creating new Service: Check Point vSEC Service
    Creating new Service: Check Point vSEC Service
   Updating Service Profile Failure Policy for service: Check Point vSEC Service
    Service registration completed successfully.
    Service deployment is now available via vSphere Web Client under Networking & Se
    curity -> Installation -> Service Deployments.
    ****************************
         vSEC VMware Service Manager Menu
           Change Global Configuration
           Licensing
           Register Service
           Manage Registered Services
           Reload Data Center Servers list
           Check Connection
      6.
           Back
      7.
    Selected option:
```

8. 設定完畢後,可檢視設定,選擇 4. Manager Registered Services > 1. Show Services > 1. nsx。



9. 設定完畢跳出 vsec_config 設定。

- 八、設定 vCenter 新增 Service。
 - 1. 登入 vCenter,切换到 Networking & Security > Installtion > Service Deployments 中,新增一

Service $\,^\circ$

Navigator	Installation		
A Back	Management Host Preparati	on Logical Network Preparation	Service Deployments
Networking & Security	NSX Manager: 192.168.230.1	9 -	
👯 NSX Home	EAM Status: 🔟 Up		
🚱 Dashboard	Network & Security Service De	niovmonts	
🔅 Installation	Network & security service be	deployments	ne service deployments here by
n Logical Switches	Interwork & security services are	deployed on a set of dusters, mana	ge service deproyments here by
NSX Edges	T K K T		
Firewall	New service deployment	Installation Status	Service Status G
Network Spool Guard			
🖐 Service Definitions			
Service Composer			
- Tools			
🙀 Flow Monitoring			
😫 Traceflow			
📷 Endpoint Monitoring			
 Networking & Security Inventory 	r		
🔠 NSX Managers	>		

2. 可在選項中看到第七步驟完成後產生的 Servce " CheckPoint vSEC Service", 勾選後點選 Next。

Deploy Network & Security Servic	es				•	٢.
1 Select services & schedule	Selec Selec	t services & schedule t one or more Network & Security services	to deploy.You can also specify the sch	edule for dep	loyment	
3 Select storage and Management Network	Selec	t services:				
4 Ready to complete					Q Filter -	
		Name	Description	Category		
	\checkmark	Check Point vSEC Service	Check Point vSEC Service			
		Guest Introspection	Base service for all solutions based.			
	Spec	ify schedule:				
	• D	eploy now 🔘 Schedule the deployment	4:01 PM 👻			
			Back	Next	t Finish Cancel	
						1

3. 選擇要套用的 Cluster 後點選 Next,接者選擇要使用的 share storage "HDS-FC-Storage",以及要 使用的 Network "DPortGroup 230", IP assignment 點選 change。

Deploy Network & Security Service	es					
 1 Select services & schedule 2 Select clusters 	Select clusters Select one or more of service will be upgra	dusters on which to deploy the service(s). If ded.				
3 Select storage and Management Network 4 Ready to complete	Datacenter: * Data	acenter -				
	V Name					
	9FDemoL	BCluster				
Deploy Network &	Security Servi	ces				
 1 Select services 2 Select clusters 	& schedule	Select storage and Mana Assign a network and IP a	gement Network ddress range for each ser	vice to use.		
3 Select storage a Management Ne	nd twork	Service	Cluster	Datastore	Network	IP assignment

4. 此部分可以新增一組 DHCP pool,本範例選擇之前建立的 NSX-Controller-Pool,點選 OK。

						Q Filter	
1	lame	1 🔺	IP Range	Prefix Length	Gateway		Used / Total
	NSX-Controller-		192.168.230.31-19	24	192.16	8.230.254	<u>4/10</u>

5. 設定完畢後點選 Next。

 1 Select services & schedule 2 Select elustere 	Select storage and Mana Assign a network and IP a	agement Network address range for each se	rvice to use.		
3 Select storage and	Service	Cluster	Datastore	Network	IP assignment
A Ready to complete	Check Point vSEC	n 9FDemoLAB Clus	HDS-FC-Storage	DPortGroup 230	NSX-Controller-Pool Ct

6. 確認設定參數都沒有問題後,點選 Finish。

Select services & schedule Select clusters	Ready to complete Review settings before finishing the wizard.							
3 Select storage and Management Network 4 Ready to complete	Schedule at: Now							
	Service	Cluster	Datastore	Network	IP assignment			
	Check Point vSEC	및 9FDemoLAB Cluster	HDS-FC-Storage	DPortGroup 230	NSX-Controller-Pool			

7. 當 vCenter 和 NSX 開始連線到 CHP SMS 讀取 ovf 檔,並開始佈署 vSEC Service 時,請關閉 SmartConsole,避免影響運作,此時可從 vCenter 上看到每台 ESXi 都會佈建一台 Check Point vSEC Service。此步驟需要花費超過 30 分鐘以上。

Navigator	Check Point vSEC Service	r (1) 🔮 👂 🔳 1	0 (A I 0	Actions +			
A Back	Getting Started Summary	Monitor Configure	Permission	s Snapshots	Datastores	Networks	Update Manager
	Pewmed On	Check Point vSEC Guest OS Oth Compatibility: ESX Managed By: vSp Deta VMware Tools: Run DNS Name: serv P Addresses: 192 Hoat: 192	Service (1) tr 2.6.x Linux (6 15.0 and later (1 here ESX Agent is ining, version: 10 e info iceinstance-3-a 168.230.36 168.230.17	4-bit) /M version 8) Manager 277 (Current) 153d6			
9F_DemoLA8 - AD_Win201	VM Hardware			NSX Endpoint M	lonitoring		
9F_DemoLAB - NSX-Manag AB - VCenter ann	Security Tags		- V	Intual Machine Dat	a Collection	O Disat	bled
CHP - VSEC SMS	Security tags can not be ap	plied to a service virtual i	nachine.	lobal Data Collect	ion	✓ Enab	led



8. 等到 Service Deploy,ents 中佈建狀態顯示成功,但 status 顯示 Down,且 Error Description 顯示 vSEC GW didn't run First Time Wizard。打開 SmartConsole,可看到新的 Clueter 物件與對應的 Firewall。

vintuale vopriere web client	ΠΞ	/					
· 莽覽器 - 耳	Installation						
▲ 上一頁 ▶	Management	Host Preparation	Logical Network	Preparation	Service Deployments		
Networking & Security	Service Status			,	x		
				Q	篩躍器		
🚱 Dashboard	Host	Installation Status	Status	Error Id	Error Description	e by adding new services or dele	ting existing
S Installation	192.168.210.1	 Succeeded 	🔥 Warning		vSEC GW has		
Logical Switches	192.168.210.1	🗸 Succeeded	🔔 Warning		vSEC GW has	Service Status	Cluster
Firewall					VSEC	GW has Initial Policy	
SpoofGuard					Pleas	e install policy from Managem	ient
Service Definitions					Serve	er Smart Console, make sure t valid managing license.	the Server
Service Composer					Last	Update:[12/21/17.11:02:41]	
✓ Tools							
🙀 Flow Monitoring	M				2 個項目 🗋 複製 🚽		
Columns: Col	Version 0.52 R77.30 0.36 R77.30 0.55 R77.30 0.51 R80.10	Active Blades Active Blades Cluster Propet General Properties Cluster Members Starty Configure Ad Party Configure Ad Party Configure Ad Party Configure Added A Configure Added	Scripts - CP Hardware CP rites - Check_Point Gateway (Name Serv Ky	Actions - O J Usage Rr LySEC Service- Juster members U ceinstance-3-af7 ceinstance-3-af5	Monitor Q Search ecommended Updates Datacenter-9FDemoLAB_C ist: IPv4 Address IP 324 192 168 230 3d5 192 168 230	Comments luster 16 Address	

9. 確認 cluster member 是否和 SMS sync 正常,Cluster 物件的 General Properties 中,修改 Cluster 物件 IP、Version 版本、取消勾選 IPSecVPN、ClusterXL,在 3rd Party Configuration 中取消勾選 Hide Cluster Member's outgoing traffic behind the Cluster's IP Address。

Cotorio Churton Document	La Charle Daint of CC Service OF Demot AP Determine New Cluster	Gateway Cluster Properties - Check_Point_vSEC_Service-Datacenter-SFDernoLAB_Cluster	2 ×
Contract Proposition Cutater Members	Machine Machine Machine Disck_Part_USEC_Service-9F_DemoLAB-Datacents IP-6 Address: Comment: Planform Hardware: vySEC for NSX Version: R77.30 V 05: Gala Network: Security (3) Prevail Bisce VRN Advanced Hetmorking & Clustering: Advanced Hetmorking & Clustering: Optimula Disce VRN Advanced Hetmorking & Clustering: Advanced Hetmorking & Clustering: Optimula Disce VRN Advanced Hetmorking Content Amareness	Curter Mode El Bark/Conformer El Bark/Conformer	
	Mobile Access Integrated Mobile Access that provides efficient and secure remote access connectivity for both managed and unmanaged clients.		
< :	DK Cancel	< >> 0K	Cancel

10. 到 Topology,關閉每個介面中 Topology 的 Anti-Spoofing,到 Platform Portal 修改 Main URL。

...

	nfiguration		~							
Topology	arvice	<pre>JF_DemoLAB-Datace</pre>	nter-New_Cluster	serviceinstance-3-91 192.168.230.38 (eth)	aff3 serviceinsta D) 192.168.23	nce-3-9104b6 0.39 (eth0)	Network Type Private			
HTTPS Inspe	ection			1.1.1.1 (eth 1)	1.1.1.1 (eth	1)	1st Sync			
···· Platform Porta	al									
Identity Awan Identity Awan	reness									
Fetch Policy	<						>			
Optimizations Hit Count	\$									
							Interface	e Properties		?
dit Topology							_ Genera	a Topology		
	Network Objecti	re 📼 Check_Point	v 📾 serviceinstan	c 📾 serviceinstanc	Topology					
Name	Private		Get Topology eth0	Get Topology eth0		-	Торо	olog)		
IPv4 Address			192.168.230.38	192.168.230.39	External	-	() Ext	xternal (leads out to the Internet)		
Net Mask	1		255.255.255.0	255.255.255.0			0	terrel des dete des la sel seture 12		
IPv6 Address							OInt	nternal (leads to the local network)		
Prefix length						-	IP	P Addresses behind this interface:		
Name Rv4 Address	1st Sync	\leq	eth1	etri1	Internal	-		○ Not Defined		
Nat Maek	1		255.255.255.0	255.255.255.0		-		Network defined by the interface ID a	and Nat Mask	
I CLININGN			_	-		-		O Network defined by the interface in a	and Net Wask	
Pv6 Address					1					
IPv6 Address Prefix length							Anti-S	Specific: Specific: Interface leads to DMZ		View
IPv6 Address Prefix length				1		1	Anti-S	Specific:	topolog	View
Pv6 Address Pv6 Address Prefix length	Get Conv t		8			Show Net Mask	Anti-S Per Ar	Specific: Interface leads to DMZ Spoofing erform Anti-Spoofing based on interface inti-Spoofing action is set Prevent Dotation device device form	topolog	View
Prefix length Add network	Get Copy to	pology to cluster interfac	es	<u> </u>		Show Net Mask	Anti-S	Specific: Interface leads to DMZ Spoofing erform Anti-Spoofing based on interface inti-Spoofing ection is set Prevent Don't check packets from: Don't check packets from:	topology v	View
New Address Prefix length Add network Edit Remove	Get Copy to	pology to cluster interfac		ОК	Cancel	Show Net Mask	Anti-5 Per Ar	Specific: Spoofing efform Anti-Spoofing based on interface inti-Spoofing ection is set Prevent On't check packets from: poof Tracking: None Output Don't check packets from:	topolog:	View
Not Indak Prefix length Add network Edt Remove Juster Properties -	Get Copy Is	pology to cluster interfac	es -Datacenter-New_	OK	Cancel	Show Net Mask	Anti-S Pe Ar	Specific: Spoofing From Anti-Spoofing based on interface inti-Spoofing action is set Prevent On't check packets from: Don't check packets from:	topolog;	View
Add network Add network Edt Remove uster Properties I Properties	Get Copy to Check_Point_vSEC_ Platform Administrat	pology to cluster interface	es -Datacenter-New_	OK	Cancel	Show Net Mask Help	Anti-S Pee Ar Sp	Specific: Spoofing Spoofing solution Spoofing based on interface on interface solution Spoofing action is set Prevent Don't check packets from: Don	topolog	View
Add network Refine any constraints Add network Edt Remove ster Properties - Properties Network	Get Copy tr Check, Point_vSEC_ Platform Administrat Main URL: https	pology to cluster interfac iervice=9F_DemoLAE an Web Portal: //192.168.230.6/	-Datacenter-New_	OK Cluste	Cancel	Show Net Mask	Anti-S Pee Ar	Specific: Spoofing From Anti-Spoofing based on interface Spoofing etion is set Prevent On't check packets from: Spoof Tracking: None Sog	topolog:	View
Add network Prefix length Add network Edit Remove uster Properties - Properties Properties Verofigration gr	Get Copy tr Check_Point_vSEC_ Platform Administrat Main URL: https	pology to cluster interfact iervice-9F_DemoLAE on Web Portal: //192.168.230.6/	-Datacenter-New_	OK Cluste V Alaser	Cancel	Show Net Mask	Anti-S Pee Ar	Specific: Spoofing From Anti-Spoofing based on interface Spoofing etion is set Prevent On't check packets from: Spoof Tracking: None Sog	topolog;	View
Add network Prefix length Add network Edt Remove uster Properties I Properties ty Configuration gy S Inspection	Get Copy to Check_Point_vSEC_ Platform Administrat Main URL: https Certificate	pology to cluster interface	-Datacenter-New_	OK Cluste V Akaser	Cancel	Show Net Mask	Anti-5 Pee Ar	Specific: Spoofing From Anti-Spoofing based on interface NRE-Spoofing ection is set Prevent On't check packets from: poof Trecking: None Gog	topolog:	View
Add network Prefix length Add network Edt Remove uster Properties - al Properties - si Reporties - y Configuration gy Si hapector Si h	Get Copy to Check Point, vSEC Platform Administrat Man URL: https Certificate — This portal uses	pology to cluster interfac iervice-9F_DemoLAB on Web Portal: //192.168.230.6/	es -Datacenter-New_	OK Cluste V Aliases	Cancel	Show Net Mask Help	Anti-S Pe Ar	Specific: Spoofing From Anti-Spoofing based on interface inti-Spoofing action is set Prevent On't check packets from: Don't check packets from:	topolog;	View
Add network Prefix length Add network Edt Remove uster Properties - U Configuration 9' S respection 9' S respection Protal Advances	Get Copy to Check_Point_vSEC Platform Administrat Man URL: https Certificate This portal uses inport.	pology to cluster interfact iervice: 9F_DermoLAE on Web Portal: //192.168.230.6/	es -Datacenter-New_ ficale. You can also	OK Cluste V Aliases	Cancel	Show Net Mask Help	Anti-S Pe Arr	Specific: Speci	topology v Alert	View
Add network Edt Remove Juster Properties - al Properties Members by Configuration gy S Inspection (HTTPS Proxy n Postal /Awareness Policy	Get Copy to Check_Point_vSEC_ Platform Administrat Main URL: https Certificate This portal uses Import	pology to cluster interfac ienvice-9F_DemoLAE on Web Portal: //192.158.230.6/ an auto-generated cert	es -Datacenter-New_ ficate. You can also	OK Cluste Alasee Import your own certif	Cancel	Show Net Mask Help	Anti-S Pe An	Specific: Spoofing Spoofing Spoofing Specific: Spoofing Specific: Spoofing Specific: Spoofing Specific Specifi	topolog v Alert	View
Add network Profix length Add network Edt Remove uster Properties Add network Singection (HTTPS Proxy n Portal Progenties Policy ations ant	Get Copy to Check, Point_vSEC Platform Administrat Man URL: https Certificate This portal uses Import Use a cert	pology to cluster interfac ienvice-9F_DemoLAE an Web Portal: //192.168.230.6/ an auto-generated cert ficate from a trusted C	es -Datacenter-New_ ficate. You can also A to avoid browser w	OK Clust Clust impot your own cetif amings	Cancel	Show Net Mask	Anti-S Pe Ar	 Specific:	topolog 	View
Add network Prefix length Add network Edt Remove uster Properties ty Configuration gy S Inspection HTTPS Provy n Portal Awareness Policy tations art	Get Copy to Check_Point_vSEC Platiom Administrat Main URL: https Cettficate This portal uses Impot Use a cet Accessibility	pology to cluster interfac service-9F_DermoLAE an Web Portal: //152.168.230.6/ an auto generated cert ficate from a trusted C	es -Datacenter-New_ ficate. You can also Ato avoid browser w	Cluste Cluste Import your own certif amings	Cancel	Show Net Mask	Anti-S Pee Ar	Specific: Spoofing offing off	topolog;	View
Add network Prefix length Add network Edt Remove ster Properties I Properties Wembers ty Configuration GY S Inspection HTTPS Proxy n Portal Awareness Policy adions int	Get Copy to Check_Point_vSEC_ Platform Administrat Man URL: https Certificate This portal uses import Cetablity — The potal is ac	pology to cluster interface envice-9F_DemoLAE on Web Portal: //192.168.230.6/ an auto-generated cert ficate from a trusted C	es -Datacenter-New_ ficate. You can also A to avoid browser w faces.	OK Cluste Aliaser import your own certifi amings	Cancel	Show Net Mask Help	Anti-S Pe Ar	 ○ Specific:	topolog;	View

11. 到 SECURITY POLICIES > Access Control > Policy 中,修改預設 policy Action 為 Accept、Tack 為 log, 然後 Install policy, 等待 install policy 完成。

Q: *	Gbjects • 🔮 Install Policy	2						Check Point [®] Smart Console	- 7
88	Standard +		≝ ₌ ×∣≣ ÷ ≡	🗄 - Install Policy 📫 Actions -	Search for IP, obje	ect, action,	٩,	~ ^ Y	
& SERVERS	Policy	No. 1	Source * Any	Destination * Any	VPN * Any	Services & Applications * Any	Action Accept	Track	Install On * Policy
	Threat Prevention Im Policy Exceptions						1		



12. $匯人 gateway license & contract \circ$

🖀 192.168.230.5 - Check Point SmartUpdate							-	o)	×
	x x x x x	G #					Chec	k Point	
Package Management Licenses & Contracts							Sma	птораа	
Machines	IPv4 Address	IPv6 Address	Version	State	SKU	Description	Expiration) Has (Con
□-□ 192.168.230.5									
🖕 🖷 sms:8010	192.168.230.5								
			Software Bla		CPSM-C-U CPSB-NPM CP	Security Management container to manage Unlimi.	18Jan2018	Yes	
CPSM-C-U CPSB-NPM CPSB-EPM CPSB-LOGS CP			Software Bla		CPSM-C-U CPSB-NPM CP	Security Management container to manage Unlimi.	18Jan2018	Yes	
- 📾 serviceinstance-3-91aff3	192.168.230.38					Trial Period	15 3Jan20	18	
CPSG-C-8-U CPSB-FW CPSB-VPN CPSB-IPSA CPS			Software Bla		CPSG-C-8-U CPSB-FW CP	Security Gateway Container for Security Gateway	18Jan2018	Yes	
- 📾 serviceinstance-3-9104b6	192.168.230.39					Trial Period	15 3Jan20	18	
			Software Bla		CPSG-C-8-U CPSB-FW CP	Security Gateway Container for Security Gateway.	18Jan2018	Yes	

13. 回到 vCenter 檢查 NSX 佈署的 service deployment 可以看到都變成 OK。

vmware [®] vSphere Web Client	n≘				
· 導覽器 ■	Installation				
	Management Host Preparati	on Logical Network Preparati	on Service Deployments		
Networking & Security	NSX Manager: 192.168.210.13	35 🔍			
🛃 NSX Home	Network & Security Service De	ployments			
💫 Dashboard	Network & security services are	deployed on a set of clusters. M	anage service deployments her	e by adding new service	s or deletii
🔅 Installation	4 y 3h 🔺				
🋬 Logical Switches					
NSX Edges	Service	Version	Installation Status	Service Status	
🛃 Firewall	Check Point vSEC Servi	R77.30VSEC	 ancreaned 	✔ Up	

- 九、Configuring NSX redirect traffic to the Security Gateway Virual Edition:
 - 回到 vCenter Web Client,到 Home > Networking \$ Security > Service Composer > Security Groups, 點選 New Security Group。



2. 設定 name



3. 設定套用的 membership 條件。

e New Security Group			**
 1 Name and description 	Define dynamic membe	rship	
2 Define dynamic membership	Specify dynamic memb	rship criteria that objects must meet to be part of this security group.	
 3 Select objects to include 	+		
 4 Select objects to exclude 	Membership criteri	a1 🛛	
 5 Ready to complete 			
	Match	Any of the criteria below	
	Criteria Details	Add	
		With Name	
		Deale Haut Fision O	Incal

4. Select objects to include 選擇所要保護的 cluster, Select objects to exclude 不選擇,直接點 Next。

🔗 New Security Group							ÞI
 1 Name and description 2 Define dynamic membership 	Select objects Select objects	to include that should always be included ir	this group, re	egardles	s of whether they meet the r	nembership criteria.	
 2 Define dynamic membership 3 Select objects to include 4 Select objects to exclude 5 Ready to complete 	Object Type: Available Objec	Cluster Q Filter ds Cluster		•	Selected Objects	Q Filter	•
		1 items	Copy 🗸			1 items 🖺 C	ору 🗸
					Back	ext Finish Ca	ancel
		- Viiiware vobinere ob	4001	113 127	20/2011 10.41.0 12/20	22011 10.41.1 1 102.100	230.10
Yew Security Group							H
 1 Name and description 	Select objects Select objects	to exclude that should always be excluded in	n this aroup, re	edardles	s of whether they meet the	membership criteria.	

 1 Name and description 	Select objects Select objects	to exclude that should al	lways be excluded ir	n this group, r	egardies	s of whether they n	neet the memb	ership criteria.	
 2 Define dynamic membership 									
✓ 3 Select objects to include	Object Type:	Cluster		•					
4 Select objects to exclude			(a ===						
 5 Ready to complete 		+	Q Filter)			C	L Filter	· ·
	Available Objet	75 Olivetee				Selected Objects			
	igi New	Cluster							
			1 itome	Copy -				0 itoms	Copy -
			1 Items	- Cobl .				o itemis	Coopy .
						Васк	Next	Finish	Cancel

5. 確認設定資訊無誤後點 Finish。

🔗 New Security Group							**
 1 Name and description 2 Define dynamic membership 3 Select objects to include 4 Select objects to exclude 5 Ready to complete 	Ready to com Name: Description: Scope: Dynamic men Members Key VM Nam	plete vSEC Security Group vSEC Security Group Global mbership s matching (Any) of the criteria e	below Criteria Contains		Value NSX - Win7		
	Objects to Inc Name 태 New Clus	ster		Objects to Exclude Name			
				Back	Next	Finish	Cancel

6. 確認要測試的主機在此 Security Group 中。

vmware [,] vSphere Web	Cli	ent f i≣					Updated at 10:32 AM
Navigator	X	Service Composer					
(Back)		Security Groups Security F	Policies Canvas				
Networking & Security		NSX Manager: 192.168.230.1	9 💌			vSEC. Security Group - Virtual Machines	×
Dashboard Installation		Synchronization Status 🛞	tion errors or warnings.			Virtual Machines (0) Errors	AM
Logical Switches		11 1 af 118 ×				Q Filter	
Firewall		Name Activity Monitoring Data	Description	Security Policies 4	Cur 0	Airmin n/a	Virtual Ma 0
SpectGuard		er vSEC Security Group	VSEC Security Group	0	0	NSX - Win NSX - Win7 01	2
 Service Composer Tools 							
Flow Monitoring							
Endpoint Monitoring Networking & Security Inventor	ry					Members as of 12/20/2017 11:24 AM 31	tems 🔒 Export

7. 切換到 Security Policied,點選 Create Security Policy。



8. 設定 Security Policy Name。

T New Security Policy		(?)
1 Name and description		
 2 Guest Introspection Services 	Name:	VSEC Security Policy
✓ 3 Firewall Rules	Description:	vSEC Security Policy
✓ 4 Network Introspection Services		
 5 Ready to complete 	🗌 Inherit securi	ty policy
	Parent policy:	*
	 Advanced op 	tions
		Back Navt Einich Cancel
		Back Next Finish Cancer

9. 接著直接跳到 Network Introspection Serevices , 點選 Add Network Introspection Service。

Vew Security Policy						
 1 Name and description 	Network Introspection Services					
✓ 2 Guest Introspection Services						
✓ 3 Firewall Rules						
4 Network Introspection Services	Add Network Introspection Service					
 5 Ready to complete 						

10. 新增第 1 條 Service,檢查從虛擬機對外的 traffic,設定 Name、Description, Service Name 選擇 前面設定 for CheckPoint vSEC 的 Serice, Profile 選擇前面設定的 vSEC Profile, Sourcec 為 Policy's Security Group, Destination 確定為 any,點選 OK。

	ntrospection Service	
Name:	From vSEC	
Description:	From vSEC Security Grou	qu
		_
Action:	 Redirect to service 	
	 Do not redirect 	
Service Name:	Check Point vSEC Servio	CB 🔹
Profile:	Check Point vSEC Service	ce_Template_of_NSX (IDS IPS, Firewall)
Source:	Policy's Security Groups	Change
oburde.	Negate source	onange
Destination:	Any	Change
	Negate destination	
 Either soul Current se gets applie 	rce or destination selection (lection will apply to "Outgoin ad to specified Destination.	or both) must be "Policy's Security Groups". g" traffic from the security groups where this policy
i Either sour Current se gets applie Service:	rce or destination selection (lection will apply to "Outgoin ad to specified Destination. Any	or both) must be "Policy's Security Groups". g" traffic from the security groups where this policy Change
 Either sou. Current se gets applie Service: State: 	rce or destination selection (lection will apply to "Outgoin ed to specified Destination. Any Enabled 	or both) must be "Policy's Security Groups". g" traffic from the security groups where this policy Change
 Either sou. Current se gets applie Service: State: 	rce or destination selection (lection will apply to "Cutgoin ed to specified Destination. Any Enabled Disabled	or both) must be "Policy's Security Groups". g" traffic from the security groups where this policy Change
 Either sou. Current se gets applie Service: State: Log: 	rce or destination selection (lection will apply to "Outgoin ed to specified Destination. Any	or both) must be "Policy's Security Groups". g" traffic from the security groups where this policy Change
 Either sou. Current se gets applie Service: State: Log: 	cce or destination selection (lection will apply to "Outgoin ad to specified Destination. Any Enabled Disabled Log O not log	or both) must be "Policy's Security Groups". g" traffic from the security groups where this policy Change

11. 新增第 2 條 Service 檢查外部 traffic 到虛擬機,設定 Name、Description, Service Name 選擇前面設定 for CheckPoint vSEC 的 Serice, Profile 選擇前面設定的 vSEC Profile, Sourcec 為 any, Destination 確定為 Policy's Security Group,點選 OK。

	[•
Name:	To vSEC	
Description:	To vSEC Security Group	
Action:		
ACTON.	 Do not redirect 	
Service Name:	Check Point vSEC Service	•
Profile:	Check Point vSEC Service	_Template_of_NSX (IDS IPS, Firewall)
Source:	Any Negate source	Change
Destination:	Policy's Security Groups	Change
	Negate destination	
i Either sour Current sei	ce or destination selection (or lection will apply to "Outgoing" d to specified Destination.	both) must be "Policy's Security Groups". "traffic from the security groups where this policy
gets applie	4	Change
Service:	Any	
Service: State:	 Enabled 	
Service: State:	 Enabled Disabled 	
gets appre Service: State: Log:	Any • Enabled Disabled Log	

12. 確認 Service 是否正確,點 Finish。

I New Security Policy								
 1 Name and description 	Network Introspection Services							
2 Guest Introspection Services 3 Firewall Rules	+ /	=t =4 ~ O ×	Q Filter	•				
Network Introspection	No.	Name	Source	Destination	Service	Action		
⁴ Services	😨 1	From vSEC	😭 Policy's S	* Any	* Any	Redirect to C		
 5 Ready to complete 	© 2	To vSEC	* Any	😰 Policy's S	* Any	Redirect to C		
	0.0				2 itoma 🕞 E			
	am				z items	sport - estopy +		
				Back	Next Fir	nish Cancel		

13. 點選剛剛新增的 Security Policy 再點選 Apply Security Policy, 勾選要套用的 vSEC Security Group, 點選 OK。

vmware [®] vSphere Web Client					
Navigator I	Service Composer				
A Back	Security Groups Security Policies Canvas				
Networking & Security	NSX Manager: 192.168.230.19				
Home NSX Home	Synchronization Status				
S Dashboard	There are no synchronization errors or warnings				
instanation 🏤 Logical Switches					
NSX Edges	Global Settings:				
👩 Firewall	Firewall Rules Applied To: Distributed Firewall				
🌇 SpoofGuard					
🖏 Service Definitions	🖅 🎜 🌠 🚉 🎌 🎇 Actions 🗸				
Service Composer	Rank Name Apply Security Policy	Description			
▼ 100IS ■ Elow Monitoring	1 SEC Security Policy	vSEC Security Policy			
SEC Security Policy - Apply Policy to Sec	curity Groups ? 💌				
Select security groups that must comply with t	nis security policy				
Filter (1) Selected Objects					
Name	Description				
🗹 鹶 vSEC Security Group	vSEC Security Group				
Activity Monitoring Data Collection					
M	2 items 🕒 Copy 🗸				
	OK Cancel				

14. 等待套用完成。



- 十、驗證:
 - 1. 設定 Policy 不允許第1、2台 Win7 不能 ping AD,但能存取其他資源。

⊡ : ▼	😚 Objects 🛛 🔮 Install Policy	💼 Discard Session → 🔊 Publish					Check Point Smart Console	
	Standard +							
GATEWAYS	** • Access Control		= <u>+</u> × <u>≥</u> =	- Install Policy Actions -	Search for IP, obje	ct, action,	Q	~ ^ T
& SERVERS	💵 Policy	No.	Source	Destination	VPN	Services & Applications	Action	Track
SECURITY	• Threat Prevention	1	 host_192.168.230.41 host_192.168.230.42 	🖶 AD	* Any	😝 icmp-proto	Drop	🗐 Log
POLICIES	🚺 Policy	2	* Any	* Any	* Any	* Any	Accept	Log

2. 從 Win 7(192.168.230.41)不可 ping AD(192.168.230.10),但能存取 AD 的 http,且能 ping 到 Win7(192.168.230.42)。



3. 從 Win 7(192.168.230.42)不可 ping AD(192.168.230.10),但能存取 AD 的 http,且能 ping 到 Win7(192.168.230.41)。



4. 啟動 Application Control & URL Filter Blades,並設定阻擋 facebook,驗證是否能阻擋成功。



Log Details			_ 🗆 ×
Prevent Prevented			~ ~ i i
Log Info	~	Policy	· · · ·
Origin	🚌 serviceinstance-3-9104b6	Action	Prevent
Time	Today, PM 02:40:51	Scope	host_192.168.230.41 (192.168.230.41)
Blade	😵 Anti-Virus	Rule Id	45AD6DC8-FD8C-4B36-8A64-EA3554
Product Family	Threat		
Туре	📄 Log	Actions	~
		Threat Wiki	Go to Threat Wiki
Protection Details	~	Remediation	Go to Remediation Options
Severity	Medium	Add Exception	Add Exception
Confidence Level	High	Report Log	Report Log to Check Point
Malware Action	Malicious file/exploit download		
Protection Name	EICAR-Test-File	More	~
Protection Type	Signature	Id	c0a8e627-0100-00c0-5a3a-05f200000
Packet Captures	src-192.168.230.41.eml	Marker	@A@@B@1513699200@C@2399
Resource	http://www.eicar.org/download/eicar.com	Log Server Origin	smsr8010 (192.168.230.5)
	more	Id Generated By In	false
Scan Result	Intected	First	false
		Sequencenum	2147483647
File	· · · · · · · · · · · · · · · · · · ·	Client Type	Firefox
File Name	eicar.com	Session Identificati	0x5a3a05f2,0x1,0x27e6a8c0,0xc00000
ніе Туре	Command	Ticket ID	5A3A05F2-0-C0A8E629-C0000001
File MD5	44d88612tea8a8t36de82e1278abb02t	Protection ID	0407D7DC6
		Suppressed Logs	2