Top-VSP V1.02 User Manual



TOPSEC[®]

HuaKong Building ,No.1, Shangdi East Road, Haidian District, Beijing 100085 Phone: +8610-82776666 Fax: +8610-82776677 Service Hotline: +8610-8008105119 http://www.topsec.com.cn

Copyright Notice

All contents and formats in this manual are the property of Beijing Topsec Company (hereinafter referred to as Topsec) and may not be copied, copied, translated or arbitrarily by any person without the permission of the Company.

All rights reserved Do not reprint ©2017 Topsec Company

Trademark Statement

The product names mentioned in this manual are for identification purposes only. The registered trademarks of the other companies involved in the manual or the copyright are the property of the trademark registrants and are not listed in a separate manner.

TOPSEC® Company.

Information Feedback

http://www.topsec.com.cn



Directory

1	PR	EFACE	1
	1.1	DOCUMENT PURPOSE	1
	1.2	READER OBJECT	1
	1.3	NAME INTERPRETATION	1
	1.4	CONVENTIONS	`2
	1.5	TECHNICAL SERVICE SYSTEM	3
2	SY	STEM INTRODUCTION	4
3	CC	ONFIGURATION REQUIREMENTS	5
4	PR	EPARATION	5
5	DE	PLOYMENT&CONFIGURATION OF SYSTEM TOP-VSP	6
	5.1	DEPLOY VSECCENTER-N SYSTEM	6
	5.2	CONFIGURE THS VSECCENTER-N SYSTEM	9
	5.3	LOGIN®ISTER NSX SERVICE	11
	5.4	DEPLOYMENT&CONFIGURATION OF SYSTEM TOP-VSP	14
	5.5	CONFIGURE SECURITY GROUP AND REDIRECTION	17
	5.6	VALIDATION OF REDIRECTION RESULTS	24
6	CC	ONFIGURE MANAGEMENT OF TOP-VSP SYSTEM	27
	6.1	LOG SETTINGS	
	6.2	UPGRADE MANAGEMENT	
7	AC	CCESS CONTROL POLICY	
	7.1	ACCESS CONTROL POLICY AND APPLICATION IDENTIFICATION	
	7.2	POLICY WITH IPS	
	7.3	POLICY WITH AV	



1 Preface

This manual focuses on the preparation and configuration of the environment and the management and application of the system for Top-VSP. By reading this document, users can understand the main functions of Topsec cloud security system, and according to the actual application environment to install and configure Topsec cloud security system.

1.1 Document purpose

This document describes how to deploy and configure the system. By reading this document, users can correctly complete the deployment and configuration of the system, combined with the use of the system to provide a variety of security control methods to effectively manage and protect the virtual cloud platform in a variety of virtual machine systems to achieve efficient and reliable security protection and unified management.

1.2 Reader object

This deployment manual applies to system administrators and network administrators who have basic network knowledge and VMware-related basics to read and use.

1.3 Name interpretation

VMware vSphere: It is the industry's leading and most reliable virtualization platform. VSphere separates the application and the operating system from the underlying hardware, and the application is no longer limited by the underlying operating system. VSphere allows a physical server to allow multiple different operating systems at the same time, and can run multiple different applications, rather than a server can only run an operating system, a single server as a resource pool Management, greatly improving the utilization of hardware servers. VMware NSX: NSX is part of the VMware software definition data center and is a virtualized network and security software product. NSX is an independent hypervisor cloud management network virtualization platform and NSX offers a complete 2-7 layer network virtualization service.

Top-VSP: Top-Vsp is a short description for Topsec cloud security protection system, it is researched and developed independently by Beijing Topsec company, it is for enterprise-class virtualized cloud platform users , it provides a set of access control 、 intrusion detection 、 intrusion prevention 、 traffic monitoring 、 stream-based virus protection and secure migration awareness and other functions in one of the cloud security protection system for VMware NSX. vSecCenter-N: VSecCenter-N is part of the Top-VSP system, which manages all deployed vNGFWs, provides centralized management of security policies, centralized monitoring of network traffic, centralized collection of alarms and logs, and provision of virtual machine security policy stand by. vNGFW: VNGFW is part of the Top-VSP system. The vNGFW is deployed as a stand-alone virtual machine on each virtualized physical server, which obtains all network traffic through the network redirection function of VMware NSX, including the

access to the virtual machine and Network traffic between virtual machines. And it provides virtual machine security monitoring and protection for each virtualized physical service, providing security functions such as virtual machine access control, intrusion detection, intrusion prevention, malicious code detection, traffic monitoring, alarm log and so on.

1.4 Conventions

This document follows the following conventions. The description of the graphical interface operation is as follows:



'' indicates the button.

() indicates the selection.

Click (select) a menu item with the following conventions:

Click(select) Advanced Management> Special Objects> Users.

The prompts, warnings, illustrations, and examples of the documents appear on the part of the user who needs special attention during the installation and configuration of the cloud security system. Please make sure that the user is aware of the possible operation results.

1.5 Technical service system

Topsec provides remote product consulting services for all of its security products, and a wide range of users and partners can access online documentation, troubleshooting, and more.

Company's main page

http://www.topsec.com.cn/

Online technical information

http://www.topsec.com.cn/support/down.asp

Security solution

http://www.topsec.com.cn/jjfa/index.htm

Technical support center

http://www.topsec.com.cn/support/support.asp

Topsec national security service hotline 800-810-5119

2 System introduction

Topsec cloud security system (Top-VSP) is a set of access control, intrusion detection, intrusion prevention, traffic monitoring, and traffic control based on VMware NSX, which is developed by Beijing Topsec Company for enterprise virtual cloud platform users. Streaming virus protection and secure migration awareness in one cloud security system, usually packaged OVA template provided, and allows users to use vSphere Web Client vNGFW in the form of a virtual machine to install and deploy.

The system is suitable for the procurement and use of VMware NSX cloud management network virtualization business and units such as government, military agencies network management, public security, confidentiality, judicial and other national authorized network security supervision departments, finance, telecommunications, electricity, insurance, Customs, commodity inspection, schools, military and other industries network management center, and large and medium-sized enterprise network management center.



3 Configuration requirements

The Top-VSP is composed of vSecCenter-N and vNGFW. The corresponding system configuration requirements are as follows:

vSecCenter-N:

- ➢ CPU:1 x 2 core
- ≻ RAM: 3GB
- ➢ Dard disk: 60GB

vNGFW:

- ➢ CPU:1 x 4 core
- ≻ RAM: 8GB
- ➢ Hard disk: 10GB

4 Preparation

Before deploying and using the Top-VSP system, you need to prepare for the previous phase:

- VMware NSX needs to provide a built-in VMware vCenter server environment, including the AD domain server and DNS server and the vSphere Web Client, where VMware vCenter server needs to provide a 6.0 environment;
- After you complete the VMware vCenter server environment, you need to configure it, including: adding licenses, creating datacenters, creating clusters, adding ESXi hosts, and roles and permissions assignments. If multiple ESXi hosts are added to the cluster, configuration to add shared storage and distributed virtual switches;
- The NSX Manager management plane needs to be successfully deployed, with the NSX Manager version 6.2.4;
- > You need to register the NSX Manager to vCenter;
- > You need to add the license for "NSX for vSphere";



You need to install vSphere Installation Bundles (VIBs) on top of the ESXi host's hypervisor.

5 Deployment&Configuration of system Top-VSP

5.1 Deploy vSecCenter-N system

The vSecCenter-N system is typically provided with a packaged OVA template and allows users to deploy vSecCenter-N as a virtual machine using the vSphere Web Client. The installation steps are as follows:

 Log in to the vCenter home page through the vSphere Web Client, install the OVA template as usual, right-click the ESXi host you want to deploy, and choose to deploy from the OVF template, as shown in Figure 1.

vmware [®] vSphere Web Clien	t ≜		Update	d at 2:14 PM 👌 I Administrate	or@VCENTER.COM -	l Help + I 🔍	Search	•
Navigator	I92.168.34.4 Actions -						=* 6	2
(Home	D Getting Started Summary Monito	Manage Related O	biects				3	V (P)
Image: Constraint of the state of	Settings Networking Storage Ali Settings Networking Storage Ali Actions - 192,168,34.4 New Virtual Machine New Kasource Pool. Connection Maintenance Mode Power	arm Definitions Tags P tual switches 2 @ I @ X tion 2 DSwitch 1 vSwitch0 4 tributed switch: DSwitch	ermissions)	scorvered Issues 			estina a secondaria	Nork In Progress
VSecCenter-N-1.0.2	Certificates					(assigned po	rt groups) 🔻 😋	
▶ 9 (NSA集群 ▶ 9 福建(勿zh!)	Storage							
	Add Networking Add Diagnostic Partition	ssigned port groups filte	er applied, showing: 🚢 0/1					
	Host Profiles	•			Switch-DVUplinks-32	6	-	
	Edit Default VM Compatibility				Uplink 1 (1 NIC Ada	pter)		
	Export System Logs				Uplink 2 (0 NIC Ada) Uplink 3 (0 NIC Ada)	pters) pters)		
	Reconfigure for vSphere HA				Uplink 4 (0 NIC Ada	pters)	•	
	Settings							
	Move To Tags & Custom Attributes						≭ ×	
	Add Permission	Target	Status	Initiator	Queued For	Start Time	Completion Time	
	Alarms	Cluster-vDFW-N	 Completed 	VCENTER.COMIAd	12 ms	3/22/2017 3:02:07 PM	3/22/2017 3:02:07 PM	
	Remove from Inventory Disassociate Host	Ba NSX約48中心 超 NSX約48中心	Completed	VCENTER COMILA	7 ms 11 ms	3/22/2017 3:01:53 PM	3/22/2017 3:01:53 PM	
	All vRealize Orchestrator plugin Actions						More Tasks	

Figure 1

 Select the OVA file for vSecCenter-N from the local folder and click the "Next" button, as shown in Figure 2.



vmware [®] vSphere Web Cli	ient ≜ ≘		Updated a	it 2:14 PM 💍 i Administrator@VC	CENTER.COM - I He	lp - I 🔍	Search	
Navigator	Getting Started Summ. Settings Networking Started Summ.	ns • ary Monitor <mark>Manage</mark> Related Ot Storage Alarm Definitions Tags Pr	ojects ermissions					(2) Work In I
	Deploy OVF Template Source D Review details D Breview details D Select name and folder 2b Select atorage 3 Ready to complete	Select source Select the source location Enter a URL to download and install as a clocal hard drive, a networf URL ① URL ① Local file Browse E1元安全103版本期	the OVF package from the Inter share, or a ODOVD drive.	tel, or browse to a location accessib	(?	>> ssigned pr	rtgroups) - C	Progress
	Rename datacenter	In NSX数据中心 In NSX数据中心	Completed	VCENTER.COMIAd	7 ms 3/22/20	17 3:01:53 PM	3/22/2017 3:02:07 P 3/22/2017 3:01:53 F 3/22/2017 3:01:42 F 3/22/2017 3:01:42 F	PM PM asks

Figure 2

 3_{\sim} Check the details of the OVA template and click the "Next" button, as shown in Figure 3.

vmware [,] vSphere Web Cli									🗸 I 🔍 S	arch		•
Navigator	Ŧ	192.168.34.4 Action	s *								=*	
(Home)	•	Getting Started Summa	ry Monitor Man	age Related Objects								(2) W
												Vork II
▼ 🚱 192.168.34.10	Deploy OVE	Settings Networking S F Template	torage Alarm Defir	hitions Tags Permis	SIONS	 		(? H	5			1 Pro
	1 Sour	ce elect source	Review details Verify the OVF tem	plate details								Iress
a 34.15-vSecCenter-N-test	1b Review details	Product	vSecCenter-N-102									
34.20-vSecCenter-N-1.0.	2 Desti	ination	Version	V0000011011111012								
34.51_yjtest1	2a Se	elect name and folder	Vendor									
34.52_yjtest2	2b Se	elect storage	Publisher	② No certificate pre	sent							
vSecCenter-N-1.0.2	2c Se	tup networks	Download size	4.1 GB								
▶ 間 NSX集群	3 Read	ly to complete	Size on disk	5.6 GB (thin provision 60.0 GB (thick provision	ied) ioned)				ssigned port	roups) -] G	
▶ 110 1101年(*********/JG/J:)			Description									
											-	
									-			
									J			
						Back	Next	Cancel	c	pmpletion Time	A	
		Description data sector	R 10	and the state of t	Constants of				02:07 PM	/22/2017 3:02:	07 PM	
		Rename datacenter	B NS	■2%提供中心	Completed Completed	VCENTER COMM	40 / 14 11	ms 3/22/2017	3:01:53 PM 3 3:01:42 PM 3	/22/2017 3:01: /22/2017 3:01	12 PM	
	7	∢ My Tasks ▼ Tasks Filter	•							Mor	e Tasks	1
						 					_	- (



- 4. Select the installation location for vSecCenter-N and click the 'Next button', as shown in Figure
 - 4.



vmware [®] vSphere Web Cli	ent n ≘		Updated at 2:14 PM 🚺 Administrator@VCENTER.COM 🗸 Help 🗸 🔍 Search	F
Navigator	Getting Started Summa Setting Networking S	ns + ary Monitor Manage Related Objects Storace Alarm Definitions Taos Permissions		📉 (2) Work In
	Deploy OVF Template 1 Source 1 a Select source 2 Ib Review details 2 Destination 2 a Select name and folder 2 b Select storage 2 c Selup networks 3 Ready to complete	Select name and folder Specify a name and location for the deployed template Name: VSecCenter-N-10.2 Select a folder or datacenter Q Search → Q 192:183.34.10 ▷ ■ DO_XOFV-N	The folder you select is where the entity will be located, and will be used to apply permissions to it. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name of the entity must be unique within each vCenter Server VM folder. The name	Progress
	Rename datacenter	Ba NSX對接中心 Ba NSX對接由心 ▼ Completed	Back Next Finish Cancel Completion Time Cancel VCENTER COMMAL 7 ms 3/22/2017 3 0/2 0 PM 3/22/2017 3 0/3 2 PM 3/22/2017 3 0/3 2 PM VCENTER COMMAL 7 ms 3/22/2017 3 0/3 PM 3/22/2017 3 0/3 PM 3/22/2017 3 0/3 PM VCENTER COMMAL 11 ms 3/22/2017 3 0/3 PM 3/22/2017 3 0/3 PM 3/2/2017 3 0/3 PM VCENTER COMMAL 11 ms 3/22/2017 3 0/3 PM 3/2/2017 3 0/3 PM 3/2/2017 3 0/3 PM	

Figure 4

5. Select the disk deployment mode, select the disk location, click the "next" button, as shown in

Figure 5.

vmware [,] vSphere Web Cl	ient n ≘							l Q Search	
Navigator	I92.168.34.4 Action	1S 🔻							
(Home	Getting Started Summa	ary Monitor Manage Related	1 Objects						(2) W
	Cottings Networking S	Norago Alarm Definitions Tage	Permissions						ork in
♥ 201 192.168.34.10 ♥ 201 DC_VDFW-N	Deploy OVF Template	Storage Alarm Delinitions Tags	[T ennissions]				?⊮]	Prog
	Source 1a Select source 1b Review details 2 Destination 2a Select name and folder	Select storage Select location to store the files f Select virtual disk format: Thick VM Storage Policy: Data The following datastores are as	or the deployed templa Provision Lazy Zeroer store Default cessible for the dest	d v ination resource that	1 at you selected. Select	the destination data	astore for the		ess
34.9-kali	2c Setup networks	Virtual machine configuration file	Canacity	Disks.	Free	Type	Storene DRS		
	3 Ready to complete	datastore1	924.00 GB	536.34 GB	508.35 GB	VMFS	otoroge orto	ssigned port groups)	- C
▶ 🦉 福建(初始))		4	5						*
					Back	lext Finish	Cancel	02:07 PM 3/22/2017 3:0	2:07 PM
	Rename datacenter	<u>同</u> NSX数据中心 Banex新增出人	Completed Completed		VCENTER.COMIAd	7	ms 3/22/2017 3	01:53 PM 3/22/2017 3:0	1:53 PM
	My Tasks 👻 Tasks Filter	•						M	ore Tasks

Figure 5

6. Set the network for vSecCenter-N and click the "Next" button, as shown in Figure 6.



vmware [®] vSphere Web Clien	nt † ≣		Updated at 2:	14 PM 👌 I Administrator@VC	CENTER.COM 👻 Help	🔹 I 🔍 Search	•
Navigator	I 192.168.34.4 Action	IS ¥				E*	
Home N	Cotting Staded Summa	ny Manifer Manage Related Object	te.				(2)
	Getting Started Summa	wanage Related Object	10				Wort
	Settings Networking S	torage Alarm Definitions Tags Perm	issions				ŝ
▼ En DC vDFW-N	eploy OVF Template				?)	••	rog
✓ III cluster_vDFW-N	4. Courses	Setup networks					S S B.
<u>5</u> 192.168.34.4	1 Source	Configure the networks the deployed ter	mplate should use				
► C ESX Agents	1a Select source						
34.15-VSecCenter-N-test √ 34.20-ySecCenter-N-1.0	1b Review details	Source		Destination	Configuration		
m 34.50-gaolitest1	2 Destination	bridged	VM Network		▼ Ø		
34.51_yjtest1	2a Select name and folder					'	
🖧 34.52_yjtest2 🗸	2b Select storage						
34.9-kali	2c Setup networks						
NSX11214	3 Ready to complete	IP protocol: IPv4	IP all	ocation: Static Manual 🖨		ssigned port groups) 🔻 😋 .	
▶ 唧 福津(勿动!)			1 01	ocatori. Otale manual g			
		Source: bridged - Description					
		The bridged network				H I	
						line in the second s	
		Destination: VM Network - Protocol set	ttings				
		No configuration needed for this networ	к				
						Completion Time	
				Back Next	Finish Cancel	02:07 PM 3/22/2017 3:02:07 PM	
	Rename datacenter	In NSX数据中心	 Completed 	VCENTER.COMIVAd	7 ms 3/22/2017	7 3:01:53 PM 3/22/2017 3:01:53 PM	
	Initialize nowering On	Ba MSX#HEM.2.	Completed	VCENTER COMINAN	11 me 3/22/2017	7 3-01-42 PM 3/22/2017 3-01-42 PM	
	My Tasks 👻 Tasks Filter	*				More Tasks	1

Figure 6

7、 Check "Power on after deployment", click "Finish" button, so vSecCenter-N installation is complete, waiting for power and initialization completed, as shown in Figure 7.

188.34.4 Actions - y Started Summary Monitor Manage Related as Networking Storage Atam Definitions Tags tet Ready to complete Review your settings selections b tails OVF file Download size Size on diak	Objects Permissions effore finishing the wizard. E 记录安全的名称本明成WSK-WoDFW-N110.2增支版本Video 4.108 50.0m	⊙ ₩	2 Work in Fragress
Started Summary Monitor Manage Related Storage Alarm Definitions Tags te Ready to complete Review your settings selections b datas OVF file Download size Size on diak	Objects Permissions efore finishing the wizard. E 公式安全的名称本例成WSK-WoDFW-IN10.2現文版本Weet 4 10 8 50 cm	Center-№-1.0.2.ova	2) Work In Progress
rape Name Datastore Datastore Target Polder Disk storage Nework mapping	uo oo oo VaseConter-N-1.0.2new datastore1 192:168.34.4 DC_vCPV-N Thick:Provision Lazy Zeroed bridged to WiteWork	ssign	ied port groups) 🔹 😋
IP allocation I	Back N Completed VCENTER COMMA VCENTER COMMA	ext Finish Cancel 02:0 . 7ms 3022017.3.01.5 .11me 3022017.3.01.4	Image: Completion Time Image: Completion Time<
e (and folder pe pe bits wave. kits kits kits kits Folder Disk storage Network mapping IP allocation Power on atter deployment kitscenter Missiklight-b Missiklight-b Missiklight-b Missiklight-b Missiklight-b Missiklight-b Missiklight-b Missiklight-b Missiklight-b Missiklight-b	and folder pe Size of foldsk ou u u b pe U Size of foldsk ou u b b pe U Size of foldsk ou u b b pe U Size of foldsk ou u b b Datastore datastore i Target 122 f63 34 4 Folder DC_vOFW-N Disk storage Thick Provision Lazy Zeroed Network mapping biological U Size - Manual, IPv4 I allocation Static - Manual, IPv4 I allocation Static - Manual, IPv4 I allocation VCENTER COMMAL measure Completed VCENTER COMMAL I Datasts Filter - VCENTER COMMAL	and tolder State of lask: bold Ge 2e Datastore datastore 1 Target 112:168.34.4 Folder DC_XOFW-N Disk storage Thick Provision Laz Zeroed Network mapping bridget to VIN Network IP allocation Static - Manual, IP-4 Eatacenter Back Next Finish Cance 02 Rest Finish Cance 02 Disk storage Completed VCENTER COMMAL 7 ns 32220173.01.5 - Tasks Filter -

Figure 7

5.2 Configure the vSecCenter-N system

After the deployment of the vSecCenter-N virtual machine, you need to configure the network, including modifying the IP address of the server, enabling the



service from the startup and opening the main service. The specific steps are as follows:

 Open the vSecCenter-N virtual machine console, login(root/Topsec1!) and then modify and save the server IP address through vi /etc/sysconfig/network-scripts/ifcfg-ens33, a s shown in Figure 8.

vSecCenter-N-1.0.2	Toggle Keyboard	View Fullscreen	Send Ctrl+Alt+Delete
BOOTPROTD=static DEFROUTE:yes PEERBOITS:yes IPU4,FAILURE_FATAL=no IPU6,UINT=yes IPU6,DEFROUTE:yes IPU6_DEFROUTE:yes IPU6_PEERBOITS:yes IPU6_FAILURE_FATAL:I NETMOSK=225.255.0 GATEWAY=192.160.34.21 NETMOSK=225.255.40 GATEWAY=192.160.34.21 NETMOSK=255.255.40 GATEWAY=192.160.34.21 NETMOSK=255.255.40 GATEWAY=192.160.34.21 NETD=979722-c3a0-42ba-9255-4bedae0033671 DEVICE=ens33 ONBOOT=yes -			
-			
"/etc/sysconfig/network-scripts/ifcfg-ens33" 19L, 342C			

Figure 8

 $2\,{\scriptstyle \sim}\,$ After modifying and saving the server IP address, you need to manually restart the ne

twork card service, as shown in Figure 9.



Figure 9

3. Use vSecCenter.sh autostart configure service auto_start, use vSecCenter.sh to start start

the system main service, as shown in Figure 10.

0 11:03:03 vsc:~ #
0 11:03:04 vsc:~ # vseccenter.sh autostart
<pre>ln -s '/usr/lib/systemd/system/topsecredis.service' '/etc/systemd/system/multi-user.target.wants/topsecredis.service'</pre>
ln -s '/usr/lib/systemd/system/cmdland.service' '/etc/systemd/system/multi-user.target.wants/cmdland.service'
<pre>ln -s '/usr/lib/systemd/system/postgresql.service' '/etc/systemd/system/multi-user.target.wants/postgresql.service'</pre>
<pre>ln -s '/usr/lib/systemd/system/topsecnginx.service' '/etc/systemd/system/multi-user.target.wants/topsecnginx.service'</pre>
<pre>ln -s '/usr/lib/systemd/system/topsecuwsgi.service' '/etc/systemd/system/multi-user.target.wants/topsecuwsgi.service'</pre>
<pre>ln -s '/usr/lib/systemd/system/tplogcollector.service' '/etc/systemd/system/multi-user.target.wants/tplogcollector.service'</pre>
<pre>ln -s '/usr/lib/systemd/system/tplogparser.service' '/etc/systemd/system/multi-user.target.wants/tplogparser.service'</pre>
<pre>ln -s '/usr/lib/systemd/system/tpftpserver.service' '/etc/systemd/system/multi-user.target.wants/tpftpserver.service'</pre>
ln -s '/usr/lib/systemd/system/celeryworker.service' '/etc/systemd/system/multi-user.target.wants/celeryworker.service'
<pre>ln -s '/usr/lib/systemd/system/celerybeat.service' '/etc/systemd/system/multi-user.target.wants/celerybeat.service'</pre>
ln -s '/usr/lib/systemd/system/ntpd.service' '/etc/systemd/system/multi-user.target.wants/ntpd.service'
<pre>ln -s '/usr/lib/systemd/system/supervisord.service' '/etc/systemd/system/multi-user.target.wants/supervisord.service'</pre>
0 11:03:14 vsc:~ # vseccenter.sh start
0 11:03:31 vsc:~ #
0 11:03:34 vsc:~ #
0 11:03:34 vsc:~ #

Figure 10

5.3 Login®ister NSX service

After deployment and configuration of the vSecCenter-N is complete, you can log in to the vSecCenter-N system for configuration, including adding the virtualization platform and registering the NSX service. The steps are as follows:

Open the browser, it is recommended to use Firefox or Chrome, enter the vSecCenter-N IP address: <u>https://192.168.34.21:9443</u>, user name/password is admin / admin, as shown in Figure 11.

← ▲ https://192.168.34.21:9443	V 隠速 V 高速 C Q, 百度 <ctrl+k></ctrl+k>	☆ 自 ♣ ☆ ち * ┺ * ☰
	3 vSecCenter	-
	Username : admin Login Password : •••••	



2. After the success of the login, click the Virtualization Platform> Platform Center in the left menu bar, and then click the "Add" button. Enter the correct information about the vCenter and NSX Manager platform respectively in the Add Virtualization Platform interface, and then click "Save" Button, as shown in Figure 12.



← ▲ https://192.168.34.21:9443			🦁 器 📌 高速 🛛 C 🛛 Q 百度 <ctr< th=""><th>'l+K></th><th>☆ 自 ↓ 合</th><th>•)- u - ≡</th></ctr<>	'l+K>	☆ 自 ↓ 合	•)- u - ≡
SYSTEM MANAGEMENT						
SYSTEM MONITOR	Virtualization Platform Ma	inagement				
CONTRACT	add edit delete					
POLICY MANAGEMENT	Name			manager address		
VIRTUALIZATION PLATFORM		Add virtualization platform	n	\otimes		
Platform Center		Name:	vcenter34.10			
USER		Туре:	VMware platform KVM platform XEN platform			
E FIREWALL MANAGEMENT		IP address:	192.168.34.10			
E UPGRADE		Username:	administrator@vcenter.com			
≣ LOG		Password:	•••••			
		description:				
		NOV				
		NCV manager eddroses	400 460 04 40			
		NOX manager address.	192.100.34.12			
		NOX manager username.	admin			
		NSA manager password:	*****	_		
			save cancel res	et		
Show recent task						1
						(



 $3\,{}_{\sim}\,$ Select the virtualization platform you just added and click the "Sync info" button, as shown in

Figure 13.

← ▲ https://192.168.34.21:9443		▼ 謎 📌 高速 🛛 🤆 🤇 百度。	cCtrl+K> ✿	▲ 슈 카 - 빅 - 북
SYSTEM MANAGEMENT				
SYSTEM MONITOR	Virtualization Platform Management			
CONTRACT	add edit delete Sync info Register nsx service Unregister			
POLICY MANAGEMENT	Name	IP address	NSX manager address	
VIRTUALIZATION PLATFORM	vmware platform vcenter34.10	192.168.34.10	192.168.34.12	
Platform Center				
USER				
FIREWALL MANAGEMENT				
E UPGRADE				
E 106	Processing data,	please later		
	In treatment			
Show recent task				



4. After the synchronization information is successful, click the "Register nsx service" button to register the NSX service, as shown in Figure 14.



← ● https://192.168.34.21:9443		V 器 / 高速 C Q 百度 < C	Ctr/+K> ✿	ፅ ∔ กิ	•5 • 12 • ≣
	=				Welcome 👻
2017-3-22 15:30:32	Home Page / Platform Center				
SYSTEM MANAGEMENT					
SYSTEM MONITOR	Virtualization Platform Management				
OBJECT MANAGEMENT	add edit delete Sync info Register nsx service Unregister n	sx service			
POLICY MANAGEMENT	Name	IP address	NSX manager address	description	
VIRTUALIZATION PLATFORM	vmware platform vcenter34.10	192.168.34.10	192.168.34.12		
Platform Center		4			
≣ USER					
E FIREWALL MANAGEMENT					
E UPGRADE					
≣ LOG					
Show recent task					



5. After logging in to the NSX service, log in to the vCenter home page through the vSphere Web Client, click the "Network & Security" option, click the "Service Definition" option in the left toolbar, switch the "Services" tab, confirm the success of the NSX service registration ,as shown in Figure 15.

vmware [®] vSphere Web Client	nt≡			Updated at 3	32 PM 🚺 I Administrato	or@VCENTER.COM	✓ I Help ✓ I	Q Search	-
Navigator 📮	Service Definitions								
Hosts and Clusters	Services Service Managers	Hardware I	Devices						3
Networking & Security		le la							
🚟 NSX Home	NSA manager. 192.168.34.12								nPr
🖓 Dashboard	🕂 🖌 🗶 🖓 Actions 🗸							Q Filter	- ge
installation	Name	Version	Functions	Deployment Mechanism	Service Managers	Services			ss
Sector States	🖏 GenericFastPath		IDS IPS		NSX Manager	0			
NSX Edges	🖏 Port Profile				Port Profile Manager	0			
Firewall	Protocol Introspection		Network Monitoring	Host based vNIC	NSX Manager	0			
R SpoofGuard	🖏 Distributed Load Balancer		2: Load balancer,	Host based vNIC	NSX Manager	0			
	🖏 VMware Data Security	6.2	Data security	Host based Guest Introsp	Data Security Service	0			
Service Composer	SAM Data Collection Service		Data Collection	Management plane only	InternalServiceManager	0			
Data Security	🔲 Guest Introspection	6.2.3		Host based Guest Introsp	InternalServiceManager	0			
✓ Tools	🖏 Topsec vDFW	1.0	Firewall	Host based vNIC	Topsec vSecCenter	0			
Flow Monitoring	S VMware Network Fabric	6.2.4		Host based NSX vSwitch fi	InternalServiceManager	0			
Activity Monitoring									
the Traceflow									_
Networking & Security Inventory									
RNSX Managers									
	44							9 Objects	3 -
								0.0010000	-
	🕄 Recent Tasks							1	# ×
	Task Name	Target	4	Status	Initiator	Queued For	Start Time	Completion Time	
	(
	My Tasks 👻 Tasks Filter 👻							More Ta	asks

Figure 15

5.4 Deployment&Configuration of system Top-VSP

After successfully registering the service, proceed to deploy the vNGFW operation, as follows:

 Log in to the vCenter home page through the vSphere Web Client, click the "Network & Security" option, click the "Installation" option on the left side of the toolbar, switch the "Service Deployments" tab, click the "+" button,select the registered NSX service "Topsec vDFW" in the "Deploy Network & Security Services" interface, click the "Next" button, as shown in Figure 16.

Navigator	Installation				
🖣 Hosts and Clusters 💿 🕥	Management Host Preparation	_oglcal Network Preparation Service Deploy	ments		
Networking & Security	NSX Manager: 192.168.34.12				
🛃 NSX Home	Network & Security Service Deploym	ients			
🖓 Dashboard	Network & security services are deplo	yed on a set of clusters. Manage service deploy	ments here by adding new services or dele	ting existing ones.	
C Installation	▲ ± ⊕ ☆				Q Filter
State Logical Switches	En Doploy Natural's & Socurity Sond				Address Range
NSX Edges	Deploy Network & Security Servi	ces			
Firewall	1 Select services & schedule	Select services & schedule Select one or more Network & Security service	ces to deploy You can also specify the scher	dule for deployment	
SpootGuard	2 Select clusters				
Service Definitions	3 Select storage and Management Network	Select services:			
Service Composer	4 Ready to complete			Q Filter	•
Tools		Name	Description	Category	
Elow Monitoring		Muture Data Security	Discovery of sensitive data at rest		
Activity Monitoring		Guest Introspection	Base service for all solutions based		
the Traceflow		Topsec vDFW			
Networking & Security Inventory					
🞆 NSX Managers	>				
					0.itoms
					0 items
					÷ *
		Specify schedule:			Completion Time
		Deploy now Schedule the deployment	it 3:39 PM 🚽		
				Next Finish	Cancel

Figure 16

- 2. Select the corresponding data center and cluster, click the "Next" button, as shown in Figure
 - 17.



Navigator I	Installation			
Hosts and Clusters	Management Host Preparation L	ogical Network Preparation Service Deployments		(2) V
Networking & Security	NSX Manager 102 169 24 12			Vork
NSX Home	Natural: 8 Canucity Camica Danlaum	auta		In Pr
🙉 Dashboard	Network & security service beployin	ento ad an e eat of cluetare. Menega canica danloymente hara by editing new canicas or delating avisting ones		ogre
🔅 Installation	A second second services are deploy	eu on a set of clusters, manage service deproyments nere by adding new services of defening existing ones.		SS
🀏 Logical Switches	• × % T			
I NSX Edges	Deploy Network & Security Service	ies	Address Range	
10 Firewall	 1 Select services & schedule 	Select clusters		
🜇 SpoofGuard	2 Select clusters	Select one or more clusters on which to deploy the service(s). If a selected cluster has an older version of a service deployed, service will be upgraded.	the	
🌼 Service Definitions	3 Select storage and			
Service Composer	Management Network	Datacenter: * DC_vDFW-N 🔹		
😘 Data Security	4 Ready to complete	Q Filter 🔹		
- Tools				
Flow Monitoring				
Activity Monitoring		V 期 Custel_VDFW-IN		
Hatwarking & Convitu Inventory		□ B1 (NOA, Ref =		
Networking & security inventory		EN MAGEN SCHOOL		
anagers >				
			0 i	tems
				¥×
			Completion Time	
		Back Next Finish Ca	ncel Mor	e Tasks



3. Then select the data storage, network and change the IP allocation mode, here need to pay attention to two aspects: on the one hand, select the network can only choose a distributed virtual switch, it needs to add configuration in advance; the other hand, if the selected cluster contains Multiple ESXi hosts, then the data storage needs to choose shared storage, also need to add the configuration in advance. Then click the "Next" button, as shown in Figure 18.

vmware [®] vSphere Web Client	fh≡				dministrator@VCENTER.C		Q Search -			
Navigator	Installation									
Hosts and Clusters	Management Host Preparation L	ogical Network Preparati	on Service Deployments				22			
Networking & Security	NSX Manager: 192 168 34 12						Vork			
Home NSX Home	Notwork & Socurity Soprice Deployme	onte					P			
🔊 Dashboard	Network & security services are deploy	unk a security service ophysitems of the service defloyments here by adding new services or deletion existing ones								
🔅 Installation		unk a security services are deproyed on a securit custors, manage service deprogramments rere by adding new services on dereining example in the security services are deprogramments and the security services are deprogramments and the security services are deprogramments and the security services are deprogramments								
🀏 Logical Switches										
🔜 NSX Edges	Deploy Network & Security Servic	es					Madress Range			
📕 Firewall	✓ 1 Select services & schedule	Select storage and Ma	anagement Network							
🖷 SpoolGuard	✓ 2 Select clusters	Assign a network and I	P address range for each se	ervice to use.			-			
Service Definitions	3 Select storage and	Que las	01-11-1	Detector	Madamad	10				
Service Composer	Management Network	At Tapage (DEW)	cluster	detectore	DRedOreure	IP assignment	_			
① Data Security	4 Ready to complete	Topsec vor w	Dg custer_vDFW-N	datastore i	DPongroup +	J IPPOOL2 Change				
✓ Tools										
Elow Monitoring										
Activity Monitoring										
Traceflow										
Networking & Security Inventory										
MSX Managers >										
							0 items			
							∓ ×			
							Completion Time			
					Back Next	Finish Can	Cel More Tasks			

Figure 18

 Please check if the settings are correct after successful loading. Click "Finish" button, as shown in Figure 19.



vmware [®] vSphere Web Client	Ħ≡		Upd	ated at 3:32 PM 💍	Administrator@VCENTER.	COM + I Help +		arch
Navigator	Installation							
Hosts and Clusters	Management Host Preparation L	ogical Network Preparati	on Service Deployments					8
Networking & Security	NSX Manager: 192 168 34 12							lork l
INSX Home	Network & Security Service Deploym	onte						P
🖓 Dashboard	Network & security service services	vention a set of clusters. M	anare senice denloyments	e here by adding new se	nices or deleting existing a	nac		ogre
🔅 Installation	• · · · · ·							
🌸 Logical Switches	T A XY T						(Q PIILEI	
III NSX Edges	Deploy Network & Security Service	ces					>> ~~	odress Hange
📕 Firewall	✓ 1 Select services & schedule	Ready to complete						
🖷 SpoofGuard	✓ 2 Select clusters	Review settings before	finishing the wizard.					
is Service Definitions	Select storage and	Sebedule et a blew						
Service Composer	Management Network	Schedule at . Now						
🕥 Data Security	4 Ready to complete	Service	cluster	Datastore	DRadCraue	IP assignment		
▼ Tools		TOPSEC VDPW	In cluster_vDPW-I4	G datastore i	E DPolitGroup	IF FOOL2		
🙀 Flow Monitoring								
Activity Monitoring								
\$월 Traceflow								
 Networking & Security Inventory 								
🔣 NSX Managers >								
								0 items
								IX
								+ ^
							Co	mpletion Time
							_	
					Back Next	Finish	ancel	More Tasks

Figure 19

5. Patiently waiting to deploy vNGFW to complete, the installation status shown as successful, as

shown in Figure 20.

vmware [®] vSphere Web Client	h≣			Update	ed at 3:32 PM 🚺 I Admini	strator@VCENTER.C	OM ▼ I Help ▼ I (Q Search -
Navigator I	Installation							
📢 Hosts and Clusters 🗼 🧐	Management Host	Preparation Logical	Network Preparation	Service Deployments				A 6.
Networking & Security	NSX Manager: 102 1	69 34 12						Vork
INSX Home	Notwork & Coourity C	anice Depleumente						In Pr
🛞 Dashboard	Network & Security S	ervice Deployments				a datakan salakan sa		ogre
🔅 Installation	Network & security ser	vices are deployed on	a set of clusters, manag	e service deployments n	lere by adding new services (in deleting existing on	15. C	s
(1) Logical Switches	+ × % 1						le	2 , Filter
NSX Edges	Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Firewall	Topsec vDFW	1.0	 Succeeded 	✓ Up	Cluster_vDFW-N	datastore1	DPortGroup	IP POOL2
R SpoofGuard								
Service Definitions								
Service Composer								
Data Security								
▼ Tools								
🕞 Flow Monitoring								
Activity Monitoring								
traceflow								
Networking & Security Inventory								
R NSX Managers								
, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,								
								1 items
	👸 Recent Tasks							
	Task Name	Targe	t	itatus	Initiator	Queued For	Start Time	Completion Time
	4							•
	My Tasks 🔻 🛛 Tasks F	ilter 🔻						More Tasks

Figure 20

6. Log in to vSecCenter-N to view the corresponding vNGFW. The online status of the vNGFW and the status of the CMDL connection are online, as shown in Figure 21.



← ▲ https://192.168.34.21:9443				💙 🎎 📈 高速	C Q 百度 <	Ctrl+K> ✿	≜ ∔	â	•) -	t , -	≡
🚿 VSECCENTER	=								W	/elcome 👻	
2017-3-22 15:58:41	Home Page / Firewall										
SYSTEM MANAGEMENT											
SYSTEM MONITOR	Virtual gateway management										
OBJECT MANAGEMENT	Add group Add virtual gateway ed	tit Force Sync C	CMDL on All Dev	Force Sync CMDL	Operate 🗸						1
POLICY MANAGEMENT	Virtual gateway name	IP address	Online State	CMDL conn status	Memory and cpu	Session number and Session new rate	e Send by	te Run	nir Redi	Version i	r
VIRTUALIZATION PLATFORM	✓										
I USER	Topsec vDFW(192.168.34.4)	192.168.34.22	Online	Online					O		
FIREWALL MANAGEMENT											1
► Firewall											
E UPGRADE											
≣ L0G											
	Page 1 of 1	» G						Sho	w 1 - 1 ,	total of 1	
Show recent task											6

Figure 21

5.5 Configure security group and redirection

After the deployment and configuration of vNGFW, the configuration of the security group and traffic redirection is performed. The detail steps are as follows:

Log in to the vCenter home page through the vSphere Web Client, click the "Network & security" option, click the "Service Composer" option on the left side of the toolbar, switch the "Security Groups" tab, click the "New Security Group" option, enter the security group name "Group Test ", click the" Next "button, as shown in Figure 22.



vmware [,] vSphere Web Client	n	Q Search -
Navigator 👢	🖉 Service Composer	
Hosts and Clusters	Security Groups Security Policies Canvas	(2) ×
Networking & Security	NSX Manager (and aso by an internet)	lork l
🔠 NSX Home	192.100.34.12	n Pr
🚱 Dashboard		Q Filler
@ Installation	Name Description Security Policies Guest Introspection Servi Firewall Rules Network Introspection Se Virtual Machines	Included Security Groups
🎡 Logical Switches	eff New Security Group	>> 0
III NSX Edges	1 Name and description Name and description	
👩 Firewall	2 Define dynamic membership	
n SpoolGuard	V 3 Select objects to include Name: * Group Test	
Service Definitions	A Select objects to exclude Description:	
/ 🗃 Service Composer	5 Ready to complete	
😰 Data Security		
- Tools	Scope: Global	
🔜 Flow Monitoring		
Activity Monitoring		
Carlow Carlow		
Networking & Security Inventory		
NSX Managers >		
		1 items 📑 🗧
		I ×
		Completing Time
		3/22/2017 3:57:04 PM
		3/22/2017 3:49:46 PM
	Back Next Finish Can	cel 3/22/2017 2:40:45 PM
	My Tasks + Tasks Filter +	More Tasks

Figure 22

2. Defining dynamic membership You can specify the dynamic membership criteria that you must meet as a member of the security group for the object. Here you can choose the relationship between the determination entity, the satisfaction criteria, and the membership conditions. Here we choose the virtual machine name to include "Test", as shown in Figure 23.

vmware [®] vSphere Web Client	h≡	Updated at 3:32 PM 👌 Administrator@VCENTER.COM - Help -	Q Search -
Navigator	Service Composer	Canuas	22
Networking & Security RNX Home Cashboard Ristallation Listal Contense	NSX Manager: 192.168.34.12 Name Description P New Security Group	Security Policies Guest Introspection Servi Piewall Rules Network Introspection Se. Virtual Machines	Q Filter Induded Security Groups
Euglian Switches NSX Edges Firewall SolofGuard Service Definitions	1 Name and description 2 Define dynamic membership 3 Select objects to include	Define dynamic membership Specify dynamic membership criteria that objects must meet to be part of this security group.	
Sendes Composer Sata Security Tools Cols Co	 Seecorpeter vector Seedy to complete 	Membership criteria 1 Match Any of the criteria below Criteria Details VM Name Contains test X	
			1 items • • • • • • • • • • • • • • • • • • •
	My Tasks 👻 Tasks Filter 👻	Back Next Finish Car	Cel 3/22/2017 3:40:45 PM* More Tasks



3. When you select an object to include, it will always be included in the strategy, whether or not it meets the membership criteria, as shown in Figure 24.



Navigator	🛙 🖉 Service Composer					
📢 Hosts and Clusters 🕑 🧐	Security Groups Security Policies	Canvas				2
Hosts and Clusters Hosts and Clusters Hosts and Clusters Hosts and Clusters Nork days Nork Home Dashboard Installation Logical Switches Toolg Firewall Source Definitions Gende Composer Data Security Tools Cuby Monitoring Cuby Monitoring Cuby Monitoring Cuby Monitoring Katuby Monitoring Matching Security Inventory Mix Managers	Security Groups Security Policies NSX Manager: 192168.34.12 Temperature New Security Group Internet New Security	Canvas Security Policies Quest Interspection Servit P Select objects to include Select objects to include Select objects that should always be included in this group, r Object Type: Virtual Machine 	egardles	ter Votual Machines ss of whether they meet the membership orteria. ↓ Filter Selected Objects ↓ @ 35.253_yjtest_centos7	•	2) WKR In Property Induced Security Groups 0
		35.254_ytest_centos7 host1_vtan100_100.104 v		1	items	Tompletion Time
	My Tasks + Tasks Filter +	SZ REINS		Back Next Finish C	ancel	3/22/2017 3:57:04 PM ³³ 3/22/2017 3:49:46 PM 3/22/2017 3:49:45 PM 3/22/2017 3:49:45 PM

Figure 24

4. When you select an object to exclude, it will always be excluded from the policy, whether or

not it meets the membership criteria, as shown in Figure 25.

avigator	I Service Composer					
Hosts and Clusters	Security Groups Security Policie	es Canvas				
tworking & Security	NSX Manager: 192 168 34 12					
NSX Home	•					Co Eillor
Dashboard						(a rinei
Installation	Name Description	Security Policies Guest Intros	action Servi Firewall F	Rules Network Introsp	ection Se Virtual Machines	Included Security Group
Logical Switches	New Security Group					** 0
NSX Edges	 1 Name and description 	Select objects to exclude				
Firewall	2 Define dynamic membershir	Select objects that should always be exclude	1 in this group, regard	lless of whether they meet the	membership criteria.	
SpoofGuard	3 Select objects to include					
Service Definitions		Object Type: Virtual Machine				
Service Composer		Q Filter			Q Filter	•
Data Security	 5 Ready to complete 	Available Objects		Selected Objects		
ools		wxw windows 7	-	🗸 🔂 centos7_x64		
Flow Monitoring		wxw windows 2008				
Activity Monitoring		B TOP-CMP				
Traceflow		A 34.20-vSecCenter-N-1.0.1				
etworking & Security Inventory		✓ 🗗 centos7_x64				
NSX Managers	>	🔮 34.102-VMware-Vcenter(勿动)				
		host1_vlan200_200.103	4			
		host1_vlan100_100.102				
		🗿 34.101-VMware-AD (勿助)				
		35.253_yjtest_centos7				1 items
		35.254_yjtest_centos7				
		host1_vlan100_100.104				
			•			Completion Time
			32 items		10	3/22/2017 3:57:04 F
						3/22/2017 3:49:46 F
				Back	ext Finish Ca	Incel 2/99/9017 3-40-45 P

Figure 25

 Check the new security group configuration is correct, click the "Finish" button, as shown in Figure 26.



vmware [®] vSphere Web Client 1	ħ≡		Updated at 3:32 PI	M 🖸 I Administrator@VCENTER.COM	🕶 Help 🕶 🤇	Search -
Navigator	Service Composer					
📢 Hosts and Clusters 💿 🖲	Security Groups Security Policies	Canvas				(2) <
Networking & Security						Vork
RSX Home	140X mailagel. 192.168.34.12					In Pr
🚱 Dashboard	ľ				le	Q Filter
🙀 Installation	Name Description	Security Policies Gues	t Introspection Servi Firew.	all Rules Network Introspection Se	Virtual Machines	Included Security Groups
🂁 Logical Switches	e New Security Group					•• U
	 1 Name and description 	Ready to complete				
10 Firewall	 2 Define dynamic membership 					
Page SpoofGuard	 3 Select objects to include 	Name: Group Test				
Service Definitions	✓ 4 Select objects to exclude	Description:				
🧧 Service Composer	✓ 5 Ready to complete	Scope: Global				
🚺 Data Security		Dynamic membership				
Flow Monitoring		Members matching (Any) of the cr	iteria below			
Activity Monitoring		Key	Critoria	Malua		
Naturation 9. Constitutions form		VMName	Contains	test		
Networking & security inventory						
C Nox managers						
		Objects to Include		Objects to Exclude		
		Name		Name		
		35.253_yjtest_centos7		centos7_x64		1 items 🔒 🗸
				-		
						Completion Time
						3/22/2017 3:57:04 PM
				Back Next	Finish Cancel	3/22/2017 3:49:46 PM
	My Tasks 🔻 Tasks Filter 💌		_		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	More Tasks
						Store rusts

Figure 26

6. After creating a security group, you can view the eligible objects in the security group, as

shown in Figure 27.

vmware [®] vSphere Web Client	ħ≡							· I Help → I 🔍	Search	
Navigator	Service Composer				Course To at 11		0			
Hosts and Clusters	Security Groups S	ecurity Policies Canva	s		Group rest - vi	rtual machines				A C
Networking & Security	NSX Manager 400 46	0.04.40			Virtual Machi	nes (0) Errors				/ork
🛃 NSX Home	140X manager. 192.16	8.34.12 *				Q Filter	-			In Pr
💫 Dashboard	1 1 1 1 1 1 1 X				Name			<u> </u>		ogre
@ Installation	Name	Description	Security Policies	Guest Introspection	👼 34.15-vSec0	Center-N-test01		Virtual Machines	Included Security Groups	ss
3 Logical Switches	Activity Monitorin		4	0	A 34.50-gaolit	est1		0	0	
NSX Edges	e Group Test		0	0	A 34.51_yjtest	1		>6	0	
Firewall					A 34.52_yjtest	2				
ra SpoofGuard					🔂 35.253_yjte:	st_centos7				
Service Definitions					🗿 35.254_yjte:	st_centos7				
🧧 Service Composer										
🛐 Data Security										
					Members as	s of 3/22/2017 4:	13 PM			
👧 Flow Monitoring										
Activity Monitoring										
Carlow Carlow										
✓ Networking & Security Inventory										
🗱 NSX Managers >										
	M								2 items 🔒 🗸	
	Recent Tasks								I ×	
	Task Name	Target		Status	Initiate	or	Queued For	Start Time	Completion Time	
	Reconfigure virtual mad	chine 🔂 Top	sec vDFW (1)	 Completed 	VCE	VTER.COMINAd	5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM	
	Reconfigure virtual mad	chine 🔂 Top	sec vDFW (1)	 Completed 	VCE	VTER.COMINAd	66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM	
	Reconfigure virtual mag	hine 🕅 Tor	SAC VOEW (1)	Completed	VCE		/ me	3/22/2017 3-/10-/15 PM	3/22/2017 3-/0-//5 PM	
	My Tasks 👻 Tasks Fi	ilter 👻							More Tasks	



7. Next we configure the traffic redirection, press left toolbar to switch the "Firewall" option,
 Click the "Configure" tab, then switch to the "Partner security services" tab, click the "Add
 Rule" button, as shown in Figure 28.



vmware [®] vSphere Web Client	ft≣			Updated	l at 3:32 PM 💍 I Administral	or@VCENTER.COM -	- I Help - I 🔍	Search	
Navigator	Firewall								
🖣 Hosts and Clusters 💿 🕥	Configuration	Saved Configurations							
Networking & Security	NSX Manager:	192.168.34.12							Örk
👭 NSX Home		(nPr
🚱 Dashboard	1 Last pub	lish operation succeede	d 3/1/2017 2:07:09 AM					8	gre
installation	General E	thernet Partner seco	urity services						SS
m Logical Switches								_	
NSX Edges	• 🛛 × 🗉	* =+ % L	Y						
Firewall	No.	Name	Rule ID	Source	Destination	Service	Action	Additional Attributes	
Not Spool Guard	📑 Del	fault Section					🛛 🖯 🖶 🔁	/ x =t =. 1	
Service Definitions									
Service Composer									
🛐 Data Security									
👿 Flow Monitoring									
Activity Monitoring									
Carlow Traceflow									
 Networking & Security Inventory 									
RSX Managers									
	👸 Recent Ta	sks						I.>	Į.
	Task Name		Target	Status	Initiator	Queued For	Start Time	Completion Time	-
	Reconfigure vir	tual machine	Dopsec vDFW (1)	 Completed 	VCENTER.COM\\Ad	5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM	
	Reconfigure vir	tual machine	Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad	66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM	
	Reconfigure vir	tual machine	TonsecyDEW (1)	✓ Completed	VCENTER COMMAN	4 ms	3/22/2017 3:40:45 PM	3/99/2017 3-40-45 PM	•
	My Tasks 👻	Tasks Filter 🔻						More Task	s

Figure 28

8、 Click Modify on the new rule, as shown in Figure 29.

vmware [®] vSphere Web Client	nt≣			Updated	at 3:32 PM 🖸 I Administr	ator@VCENTER.COM -	🗧 l Help 👻 l 🔍	Search				
Navigator I	Firewall											
- Hosts and Clusters	Configura	tion Saved Configurations						2				
Networking & Security	NSX Mana	K Manager: 192.168.34.12 *										
NSX Home	This rule	s rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.										
S Dashboard	Publist	Changes Revert Changes	Save Changes	Update Changes				gress				
(ge installation												
NSX Edges	Unde Rule	r Partner security services Cont at position 1 has invalid actions	Iguration Redirect To (Service)	Profile) is not configured				8				
Firewall		at position i nuo intana actiona	, redirect to (octifice	Tome) is not comigated								
SpoofGuard	General	Ethernet Partner securit	y services									
Service Definitions	🔶 🗈 🗴	: = = 1 😵 🖳 🕺 🦞						-				
Service Composer	No.	Name	Rule ID	Source	Destination	Service	Action	Additional Attributes				
1 Data Security	v 📑	Default Section (Rule 1)					🗟 C 🕈 💋	/ × =+ =+ ⊱				
Tools	⊘1			* anv	* anv	* anv		7				
Flow Monitoring							_					
Pt Traceflow												
Networking & Security Inventory												
H NSX Managers												
	😨 Recen	t Tasks						1×				
	Task Name	Та	rget	Status	Initiator	Queued For	Start Time	Completion Time				
	Reconfigur	e virtual machine 🏻 🎒	Topsec vDFW (1)	 Completed 	VCENTER.COM\Ad	5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM				
	Reconfigur	e virtual machine 🏻 🖞	Topsec vDFW (1)	 Completed 	VCENTER.COM\Ad	66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM				
	Reconfigur	a virtual machina 🛛 🖓	TonsecyDEW (1)	Completed ;;	VCENTER COMILLA	/ me	3/22/2017 3:40:45 PM	3/99/9017 3:40:45 PM				
	My Tasks 🔻	Tasks Filter 🔻						More Tasks				



9. In the rule edit operation interface, [Service]select the NSX service "Topsec vDFW", [Service Profile] select the "Topsec vDFW_VendorTem.....",[Action] select the "Redirect",[Direction] select the "In/Out", [Packet Type] select the "IPV4",and then click "Save" button, as shown in Figure 30.



Rule 1 - Edit Action	?
Service:	Topsec vDFW 🔹
Service Profile:	Topsec vDFW_Ve 🔹
Action:	Redirect 🔹
Direction:	In/Out 🔹
Packet Type:	IPV4 🔹
Tag:	
Log:	🔵 Log 💿 Do not log
Comments:	
	Save Cancel
	E: 20



10. To return to the previous page, click "Topsec vDFW_VendorTemplate for service-21" on the newly added rule and select and add the previously configured security group "Group Test" in the "Specify Service Profile Binding" interface. Click "OK" Button, as shown in Figure 31, 32.

vmware [®] vSphere Web Client	ft≣			Updated	at 3:32 PM 🖸 I Administr	ator@VCENTER.COM +	r I Help マ I 🔍	Search -		
Navigator	Firewall							Z		
Hosts and Clusters	Configura	tion Saved Configurations	•					U N		
Networking & Security	NSX Mana	Iger: 192.168.34.12						fork i		
NSX Home	This rule	In set has upgruid dynamics. Olick on Bulklich Changes hutter to start dealering or click Saus Changes to saus this configuration.								
🔊 Dashboard	Publis	h Changes Revert Chan	nes Save Changes	Update Changes	a ouve onlinges to sure this	sonnguration.		gres		
installation										
2 Logical Switches	General	Ethernet Partner sec	urity services							
I NSX Edges	• • • •	• = = 18 🖬 😵	7					-		
Firewall	No.	Name	Rule ID	Source	Destination	Service	Action	Additional Attributes		
SpootGuard	- Fb.	Default Section (Rule 1)						A		
	1 43									
Data Security	01			 any 	 any 	 any 	Redirect	ʻ		
Tools							TOPSECVORW Ve			
Elow Monitoring							Topsec vDFW_Ver	ndorTemplate for service-21		
Activity Monitoring										
traceflow										
 Networking & Security Inventory 										
H NSX Managers										
-										
		4 T 1 -								
	s Recen	IL TASKS						**		
	Task Name		Target	Status	Initiator	Queued For	Start Time	Completion Time		
	Reconfigur	re virtual machine	Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad.	. 5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM		
	Reconfigur	re virtual machine	DE Topsec VDFW (1)	Completed	VCENTER.COM/Ad.	. 66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM		
	4	Toole Filter -	and concerning of the		W HATCHE COMMAN	. A me	STOTIC CAUCIE PM	Mare Tasks		
	My Tasks •	r asks ⊨iner ▼						More Tasks		

Figure 31



vmware [®] vSphere Web Client	ŧ≡		Upda	ated at 3:32 PM 💍 I Administrate	or@VCENTER.COM +	I Heip ≠ I 🔍	Search •
Navigator	Firewall						
Hosts and Clusters	Configuration Saved Co	onfigurations					(1) V
Networking & Security	NSX Manager: 192 168 3	4 12 🔍					Vork
🔡 NSX Home	102.100.0						Pr
🚱 Dashboard	Rublish Changes	Pevert Changes	Lindate Changes	r click save changes to save this co	niigurauon.		ogres
installation	T dollari citaligea	Cave Changes					
💯 Logical Switches	General Ethernet P	Partner security services					
INSX Edges	🔶 🗈 x 🖃 💷 😵	Specify Service Profile Bindings			?		
👹 Firewall	No	Caladana ar mara shiada fartha Dr	file Diadiana			Action	Additional Attributes
Page SpoofGuard	- Default Castle	Object Type: Requirity Crown	ante Bindinds				
Service Definitions	▼ La Delauit Secuc	Object type. Security Group				🛛 C 🕈 👂	/ × =* =+ %-
I Service Composer	© 1	Q Filter		Q Filter	•	Redirect	
1 Data Security		Available Objects		Selected Objects			
Tools		Activity Monitoring Data Colle	ection	🗸 🔐 Group Test			
Flow Monitoring		Group Test					
At Transferre			цþ.				
- Notworking & Security Inventory			4				
Networking & security inventory							
C INOX Mallagets							
			2 items		1 items		
					1 1101110		
				0	K Cancel		
	😰 Recent Tasks						
	Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time
	Reconfigure virtual machine	e 📅 Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad	5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM
	Reconfigure virtual machine	Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad	66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM
	Reconfigure virtual machine	TonsecuDEW (1)	Completed ::	VCENTER COMILAR	/ me	3/22/2017 3:40:45 PM	3/22/2017 3:40:45 PM
	My Tasks 🔻 Tasks Filter	•					More Tasks

Figure 32

11、 Click the "Publish Changes" button to complete the rule release, as shown in Figure 33,34.

vmware [®] vSphere Web Client	nt≣			Updated	at 3:32 PM 💍 I Administr	ator@VCENTER.COM -	I Help → I 🔍	Search -			
Navigator	Firewall							.			
🖣 Hosts and Clusters 🕨 🔊	Configura	tion Saved Configurations						A (C)			
Networking & Security	NSX Mana	ager: 192168.34.12 V									
INSX Home	This rule	set has unsaved channes. Cl	ick on Publish Changes	button to start deploying or cli	k Save Channes to save this	configuration		Pro			
🖓 Dashboard	Publis	h Changes Revert Change	s Save Changes	Update Changes		ooningaraaton.		gres			
installation											
2 Logical Switches	General	Ethernet Partner secur	ity services								
NSX Edges	+ 🗅 🗴										
Pirewall	No.	Name	Rule ID	Source	Destination	Service	Action	Additional Attributes			
Service Definitions	v 🖪	Default Section (Rule 1)					🗟 C 🕈 💋	/ x =t =, %			
Service Composer	© 1			* anv	• anv	• anv	Redirect				
🚯 Data Security				uny	uny	0.1	Topsec vDFW_Ve				
👿 Flow Monitoring											
Activity Monitoring											
Sa Traceflow											
Networking & Security Inventory											
NSX Managers											
	_										
	🔋 Recen	t Tasks						# ×			
	Task Name	1	arget	Status	Initiator	Queued For	Start Time	Completion Time			
	Reconfigur	e virtual machine	Topsec vDFW (1)	 Completed 	VCENTER.COM\Ad	5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM			
	Reconfigur	re virtual machine	Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad	66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM			
	Reconfigur	e virtual machine	Tonsecy/DEW (1)	Completed ::	VCENTER COMMAN	/ me	3/22/2017 3-40-45 PM	3/99/9017 3-40-45 PM			
	My Tasks •	Tasks Filter 👻						More Tasks			

Figure 33



vmware [®] vSphere Web Client	ŧ≡			Update	ed at 3:32 PM 💍 I Administr	ator@VCENTER.COM +	l Help 👻 l 🔍	Search	•
Navigator 🖡	Firewall								
Hosts and Clusters	Configura	tion Saved Configurations							13
Networking & Security	NSX Mana	Der: 102 160 24 12							Vork
RNSX Home		182.100.54.12							In Pr
💫 Dashboard	1 Last	publish operation succeeded	3/1/2017 2:07:09 AM					8	ogre
@ Installation	General	Ethernet Partner secu	rity services						ss
🌆 Logical Switches	Gonora								
NSX Edges	+ 🗆 >	• ≣† ≣↓ 1% L <u>4</u> % 1	7						i i
👸 Firewall	No.	Name	Rule ID	Source	Destination	Service	Action	Additional Attributes	
Magazara SpoolGuard	v 🖪	Default Section (Rule 1)					🖯 C 🕈 💋	/ × =t =, %	
🛸 Service Definitions	🙁 1		1039	• anv	* anv	• anv	Redirect		
Service Composer							TopsecvDFW_Ve		
🙆 Data Security									
Flow Monitoring									
a Activity Monitoring									
Carlow Carlow									
Networking & Security Inventory									
MSX Managers >									
	😰 Recen	t Tasks						بة	<
	Task Name		Target	Status	Initiator	Queued For	Start Time	Completion Time	-
	Reconfigur	e virtual machine	🛐 Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad.	5 ms	3/22/2017 3:57:02 PM	3/22/2017 3:57:04 PM	-
	Reconfigur	e virtual machine	🔂 Topsec vDFW (1)	 Completed 	VCENTER.COM\\Ad.	66 ms	3/22/2017 3:49:46 PM	3/22/2017 3:49:46 PM	
	Reconfigur	e virtual machine	TonsecyDEW (1)	Completed ::	VCENTER COMMAN	/ me	3/22/2017 3-40-45 PM	3/99/9017 3-40-45 PM	-
	My Tasks 🔻	Tasks Filter 👻						More Task	s

Figure 34

5.6 Validation of redirection results

At this point, we have completed the deployment and configuration of vSecCenter-N and vNGFW, and now provide two simple ways to verify the success of traffic redirection, as follows:

Method 1: Log in to the vSecCenter-N system, enter the POLICY MANAGEMENT > ACL interface, configure one such access control strategy: [Action] select "Allow", [Source] select the default "any", [Destination] select the default "any", [Service] default is empty, [Options] select the log "Record log", and successfully issued a strategy to vNGFW. SSH login vNGFW (superman / talent), the use of tcpdump for the re-testing of the test machine for capturing, and then use the test machine for ping operation, in the vNGFW can catch ICMP echo request and ICMP echo reply packet to prove traffic The orientation is successful, as shown in Figure 35, 36.



← ▲ https://192.168.34.21:9443			😺 🎇 📌 高速 🛛 🤆 🔍 🖗	且翻译	→ ☆ 自 ♣ 斋	•)- ম∣- ≣
77 VSECCENTER						Welcome 👻
2017-3-22 16:38:33	Home Page / ACL					
SYSTEM MANAGEMENT						
SYSTEM MONITOR	Access control policy					
B OBJECT MANAGEMENT	Not valid until published	publish				
POLICY MANAGEMENT	add edit pub	lish Operate v empty	Collision detection Search Displa	av all strategies	Current group: defa	ult group
► ACL		antian Cause	Destination	Contine	Ortice	description
VIRTUALIZATION PLATFORM	100104	Allerer	Destination	Service	Option Descent las	description
USER	100104	Allow			Record log	
E FIREWALL MANAGEMENT						
E UPGRADE						
≣ L06						
	C Page 1	of 1 > >> C			:	Show 1 - 1 , total of 1
Show recent task						

Figure 35





Method 2: Log in to the vSecCenter-N system, add the redirected test machine IP address as the host address object, configure such access control policy: [Action] Select "Block", [Source] select the host address "34.16" [Destination] default "any", [Service] Select the predefined service "ICMP", [Option] Select the log "Record log", and successfully issue the policy to vNGFW, and then use the redirected test machine to ping, Found that can not ping, and vNGFW can only be caught on the ICMP echo request to prove that the flow of data redirects success, as shown in Figure 37, 38, 39.



7 VSECCENTER						
SYSTEM MANAGEMENT	_					
SYSTEM MONITOR	Host Subne	et Address range	Address group Virtual mach	ine Other dynamic containers		
BOBJECT MANAGEMENT	add edit					
Address Object	Name		IP address set		Physical address	
Service Object						
Time Object		Add host addres	ss resources 🛛 🛞			
APP Object		Name:	192.168.34.16			
POLICY MANAGEMENT		IP address:	192.168.34.16			
VIRTUALIZATION PLATFORM						
USER		Physical address:	example:00:50:56:c0:00:09			
FIREWALL MANAGEMENT			save cancel reset			
E UPGRADE						
■ L06						
	Reg	je 0 of 0 📄				No host address resources exist

Figure 37

← ▲ https://192.168.34.21:9443			🦁 認 📌 高速	연 🤇 组翻译	→ ☆ 自 ♣ 徻	•)- ¤ - ≡
7 VSECCENTER						Welcome 👻
2017-3-22 16:43:30	Home Page / ACL					
SYSTEM MANAGEMENT						
SYSTEM MONITOR	Access control policy					
B OBJECT MANAGEMENT	Not valid until published.	publish				
POLICY MANAGEMENT	add edit pub	lish Operate V emp	Collision detection Search	Display all strategies	Current group: default	group
► ACL			Destination		Outlos group. deidale	group
E VIRTUALIZATION PLATFORM		action Source	Destination	Service	Option d	escription
≣ USER	100104	Block 192.168.34.16			Record log	
E FIREWALL MANAGEMENT						
E UPGRADE						
≣ L06						
	Page 1	of 1 > >> C			Sho	ow 1 - 1 , total of 1
Show recent task						4
Chow recent date						1

Figure 38





6 Configure management of Top-VSP system

Next, the basic configuration management of the Top-VSP system is briefly introduced, including log settings and upgrade management.

6.1 Log settings

After the successful deployment of vNGFW, in order to ensure the normal reception and display of logs, we need to make log settings and delivery operations on the vSecCenter-N system, as follows:

Log in vSecCenter-N system, enter LOG > Log Settings interface, [Server address] fill in "vSecCenter-N system IP address", [Transport Portocol] select "UDP", [ServerPort] fill in "1514", [Log Type] Select the full type, [Log Level] are selected "INFO", and then click "apply" button, then the system will prompt to release after the entry into force, click the "publish" button, as shown in Figure 40.



T VSECCENTER	Ξ				
2017-3-22 17:29:31	Home Page / Log Set	ting			
SYSTEM MANAGEMENT					
SYSTEM MONITOR	Log setting				
B OBJECT MANAGEMENT	Not valid until pu	blished. publish			
POLICY MANAGEMENT	Server address:	192 168 34 21			
VIRTUALIZATION PLATFORM	Transport	102.100.34.21			
E USER	protocol:	UDP			
E FIREWALL MANAGEMENT	ServerPort:	1514			
E UPGRADE	Log type:	Access Control	Log level:	INFO	~
🔤 LOG		Anti-DoS	Log level:	INFO	~
▶ Log Search			l og level:	INFO	~
Log Setting			Les levels		
		Anti-Virus	Log level:	INFO	×
		System	Log level:	INFO	~
		apply			
Show recent task					

Figure 40

6.2 Upgrade management

After the successful deployment of vNGFW, you need to upgrade the IPS, AV and AI rule base on the vSecCenter-N system to ensure the correctness and accuracy of the detection. The specific steps are as follows:

Log in to the vSecCenter-N system, go to the **Upgrade > Package** interface, click the "Upload Upgrade Package" button. In the Upload Upgrade File window, select the corresponding rule base and click the "Save" button, then select the Upload Upgrade the package and click the "Upgrade" button, suggesting that the upgrade is successful, you can view the upgrade list of the status bar shows the "current version", as shown in Figure 41, 42.



77 VSECCENTER						Welcome 👻
SYSTEM MANAGEMENT						
SYSTEM MONITOR	System upgrade					
OBJECT MANAGEMENT	Upload upgrade package Delete upgrade pack					
POLICY MANAGEMENT	Version of upgrade package Typ	e				
VIRTUALIZATION PLATFORM						
E USER						
FIREWALL MANAGEMENT						
▶ Package						
► Task	Uploa	d upgrade file		\otimes		
2106	Uploa	d upgrade package:	ips-v2017.02.22.tir save cano	Browse el reset		
	🔣 🤇 Page 0 of 0 🔪 💓 🤇					No data



← ● https://192.168.34.21:9443			💙 🎇 📈 高速	C Q 百度 <ctrl+k></ctrl+k>	☆自◀	k n n - 14 -
WSECCENTER						Welcom
2017-3-22 17:38:27	Home Page / Package					
SYSTEM MANAGEMENT						
SYSTEM MONITOR	System upgrade					
OBJECT MANAGEMENT	Upload upgrade package De	lete upgrade package Upgrad	e empty			
POLICY MANAGEMENT	Version of upgrade package	Туре	Size	Upload time	Instruction of upgrade package	Status
VIRTUALIZATION PLATFORM	jav-v2017.02.27.tir	av	18482.3 KB	2017-03-22 17:37:24		
E USER	ips-v2017.02.22.tir	ips	4270.9 KB	2017-03-22 17:36:57		Current version
E FIREWALL MANAGEMENT						
E UPGRADE						
Package						
▶ Task						
≣ L0G						
	Rege 1 of 1	> » C				Show 1 - 2 , total o
	Page 1 of 1	> » C				Show 1 - 2 , total c

Figure 42

7 Access Control Policy

7.1 Access Control Policy and Application Identification

1. Use the vSphere Web Client login to vCenter, click the "Network & Security" option, the left side of the toolbar



Click on the "Service Composer" option, you can view the security group has been created configuration, as shown in Figure 43.

vmware [®] vSphere Web Client	fh≣				ن ا 🖒	strator@VCENTER.COM	• Help • (Q Search	
Navigator I	🖉 Service Composer								
History	Security Groups Se	curity Policies Canvas	3						(1) M
Networking & Security	NSX Manager. 192 165	34.12							Ork
RSX Home								C Eilter	Pro
S Dashboard		Description	Consulty Dellates	Current Industry and Inc. Count	Circural During	Network Internet in Co.	Midual Manhless	Laduded Consult	gres
installation	Activity Monitorin	Description	Security Policies	Ouest Introspection Servi	Pirewall Rules	Network Introspection Se	Virtual Machines		y Groups o
mail: Switches	NSX-kuozban		4	0	0	0	200	0	
NSX Edges	YANG IF	Security Group Test	0	0	0	0	3	0	
Firewall	av vangiin test		0	0	0	0	2	0	
Page SpoofGuard									
Service Definitions									
🧧 Service Composer									
① Data Security									
+ Tools									
Flow Monitoring									
Activity Monitoring									_
Carlow Traceflow									
Networking & Security Inventory									_
NSX Managers	M6							4 iter	ns 📑 🗝
	😨 Recent Tasks								Ψ×
	Task Name	Target		Status	Initiator	Queued For	Start Time	Completion Tim	e

Figure 43

2. Log in to the vSecCenter-N system and enter the VIRTUALIZATION PLATFORM> Platform Center interface. Select the VMware platform you added before. Click the "Sync info" button. After the synchronization is successful, go to the OBJECT MANAGEMENT> Address Object interface and click the "Other Dynamic Containers" option , You can view the synchronization information exactly the same as the security configuration information in the VMware NSX environment, as shown in



← ▲ https://192.168.34.21:9443		▼ 蹨 〃 高速 c ♀ <i>百度</i> <	Ctrl+K>)自 🖡 🏠 🍤 🐂 🖬 -	≡
2017-3-22 15:28:45					
SYSTEM MANAGEMENT					
SYSTEM MONITOR	Virtualization Platform Management				
CONTRACT MANAGEMENT	add edit delete Sync info Register nsx service Unregister n				
POLICY MANAGEMENT	Name				
VIRTUALIZATION PLATFORM	vmware platform vcenter34.10	192.168.34.10	192.168.34.12		
Platform Center					11
≣ USER					
E FIREWALL MANAGEMENT					
E UPGRADE					
≣ LOG	Processing data, p	lease later			
	In treatment				
	in reachent				
Show recent task					(

Figure 44



T VSECCENTER	=		Welcome 👻
2017-4-5 16:22:16	Home Page / Address Object		
SYSTEM MANAGEMENT			
SYSTEM MONITOR	Host Subnet Address range	Address group Virtual machin	e Other dynamic containers
B OBJECT MANAGEMENT	In the name of the platform	Internal name	IP
Address Object	Activity Monitoring Data Collection	_sg1_Activity_Monitoring_Data_	
Service Object	yangjin_test	_sg25_yangjin_test	192.168.34.51 192.168.34.52
Time Object	YANGJIE	_sg28_YANGJIE	192.168.34.16 192.168.34.17 192.168.34.18
	NSX-kuozhan	_sg29_NSX-kuozhan	10.0.0.151 10.0.0.150 10.0.0.153 10.0.0.152 10.0.0.155 10.0.0.154 10.0.0.157 10.0.0.156 10.0.0.159 10.0.0.158
APP Object			
E POLICY MANAGEMENT			
VIRTUALIZATION PLATFORM			
≣ USER			
E FIREWALL MANAGEMENT			
E UPGRADE			
≝ L0G			
		»C	Show 1 - 4 , total of 4

Figure 45

3. Log in vSecCenter-N system, enter the **OBJECT MANAGEMENT > Address Object** interface, select "Address group" option, click "add" button, in the pop-up window, enter the [name] is "security_group_test", [Other container] come over the security group "YANGJIE" and click the "Save" button, as shown in Figure 46.

	=	
SYSTEM MANAGEMENT		
SYSTEM MONITOR	Host Subnet Address range Address group Virtual machine Other dynamic containers	
B OBJECT MANAGEMENT		
Address Object	Name Static member Dynamic member	
Service Object		
Time Object	Had address group resources	
APP Object	Name: security_group_test	
POLICY MANAGEMENT	Static member	
VIRTUALIZATION PLATFORM		
≣ USER	Host address:	
FIREWALL MANAGEMENT	Subnet address:	
UPGRADE	Address range:	
E LOG	Dynamic member	
	Virtual host address: Other container Activity Monitoring Data Collection yangin test YANGJIE NSX-kuozhan	
	🔣 🤇 Page 0 of 0 📡 💓 🖸	No address group resources exist

Figure 46

4. Log in vSecCenter-N system, enter the POLICY MANAGEMENT > ACL interface, configure such access control policy: [Action] select "Allow", [Source] select the "security_group_test", [Destination] select the default "any" [Service] default is empty, [Option] select the log "Record Log", and successfully issued a strategy to vNGFW, as shown in Figure 47



77 VSECCENTER	E	=										Welcome 👻
2017-4-5 16:44:1	Home	e Page / ACL										
SYSTEM MANAGEMENT			_									
SYSTEM MONITOR		Access control p	policy									
B OBJECT MANAGEMENT	N	lot valid until publ	ished.	publish								
E POLICY MANAGEMENT		add edit	publis	sh Or	ierate 🗸	empty Collisio	n detection	Search	Display	all strategies	Current group: de	fault group
► ACL		1 10		action	Source		Dectinati	00		Sanina	Ontion	description
VIRTUALIZATION PLATFORM		100262	_	Allow	IDAddroom		Destinati	on		Gennice	Benerd leg	description
≣ USER		100302		Allow	security_	group_test					Record log	
E FIREWALL MANAGEMENT												
UPGRADE												
≣ LOG												
		K A Page	1	of 1 >	\gg	71						Show 1 - 1 , total of 1

Figure 47

After logging in to the vSecCenter-N system, enter the LOG > Log Search interface and click the "Access Control" tab to check the access control and application identification detection. After logging on using the virtualized test virtual machine in the security group "security_group_test" The result log, where "allowed" is denoted as "permit" and "deny" is denoted as "deny", as shown in Figure 48.

VSECCENTER											Welcom
2017-3-22 18:11:43	Home Page / Log Search										
SYSTEM MANAGEMENT			_	_		_					
SYSTEM MONITOR	vSecCenter Acce	ess Control IPS	Anti-DoS	Anti-Vin	is Device	e System	All Device Security Log	Vgate Manage Log			
OBJECT MANAGEMENT	Start time:	End	time:			Type:	Please select type \vee	Keyword: Please enter	key query	reset	Empty Io
POLICY MANAGEMENT	Time	Level	Modular	Operate	Protocol	App	Source address ↑	Source port	Destination address	Destina	tion por
VIRTUALIZATION PLATFORM	2017-03-17 11:31:40	INFORMATION	90	4-ite	1	ICMP	192 168 34 52	66	73 1 207 70	8	tion poi
USER	2017-03-17 11:31:40	INFORMATION	ac	分许	1	ICMP	192.168.34.52	66	82,134,114,22	8	
FIREWALL MANAGEMENT	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	134.17.227.104	8	
UPGRADE	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	16.61.78.102	8	
LOG	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	186.44.45.33	8	
▶ Log Search	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	30.67.255.26	8	
N Las Catting	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	99.192.88.74	8	
 Log Setting 	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	195.90.153.74	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	82.78.178.60	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	148.50.246.98	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	235.197.2.4	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	24.239.232.31	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	174.200.234.20	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	84.154.153.4	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	244.219.215.85	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	28.188.189.6	8	
	2017-03-17 11:31:40	INFORMATION	ac	允许	1	ICMP	192.168.34.52	66	223.128.13.67	8	
	2017-03-17 11:31:40	INFORMATION	ас	允许	1	ICMP	192.168.34.52	66	34.251.121.22	8	
	2017 02 17 11-21-40	INFORMATION		<u>4</u> 377	4	ICMD	100 100 04 00	cc	100 000 101 107	0	
	Reference Page	511 of 51018 >	» C				-		Show 1019981 - 10	20000 , total	of 10

Figure 48



7.2 Policy with IPS

Log in to the vSecCenter-N system and enter the POLOCY MANAGEMENT > ACL interface to configure the access control policy: [Action] select "Allow", [Source] select default "any", [Destination] select default "any", [Service]Default is empty, [Option] IPS rule select "_default_ips", [Option] select "Record Log", and successfully issued a strategy to vNGFW, as shown in Figure 49.

← ● https://192.168.34.21:9443					😺 🎇 📝 高速	c < 百	度 <ctrl+k></ctrl+k>	r	1 自 🖡	⋒ _ 5 -	tu - ⊟
										1	Welcome 👻
2017-3-22 18:20:0	Home Page / ACL										
SYSTEM MANAGEMENT											_
SYSTEM MONITOR	Access control p	policy									
B OBJECT MANAGEMENT	Not valid until publ	ished publish	1								
E POLICY MANAGEMENT	tibe bbc	nublich (nerate v emi	oby Collision de	tection Search	Dienlay	all strategies	C	urrant group:	infoult group	
► ACL			- citi			Diopidy				reladi _ group	
VIRTUALIZATION PLATFORM		action	Source		Destination		Service	Opt	tion	descriptio	on
≣ USER	100104	Allow						lps _de	rule: efault_ips		
E FIREWALL MANAGEMENT								Rec	cord log		
E UPGRADE											
≣ LOG											
	Reference Page	1 of 1	> > C							Show 1 - 1	, total of 1
Show recent task											

Figure 49

After using a redirected test virtual machine to launch an attack that can hit an IPS rule, log in to the vSecCenter-N system, go to the LOG > Log Search interface, and click the IPS tab to check the test result of the IPS attack, as shown in Figure 50.



← ● https://192.168.34.21:9443				V 88	☆ 高速 ♂ ♀ 百度	<ctrl+k></ctrl+k>	☆ 自 ♣ 合 与 * 年 *
77 VSECCENTER	Ξ						Welcome
2017-3-22 18:48:13	Home Page / Log Search						
SYSTEM MANAGEMENT							
SYSTEM MONITOR	vSecCenter Access	s Control IPS	Anti-DoS Anti-Viru	s Device Sy	stem All Device Security	Log Vgate Manage Log	
B OBJECT MANAGEMENT	Start time:	End t	ime:	(100) (100) (100)	Type: Please select type	Keyword: Please ent	ter key query reset Empty log
POLICY MANAGEMENT	Time	Loval Eva	at nun Timos actis	n Protocol	Source	Dectination	description
VIRTUALIZATION PLATFORM	0047 02 04 47 02 24	Level Lve	action action	in Protocor	300/CE	Destination	Blacker tech TETD (5/2)/6/16
E USER	2017-03-21 17:02:31	WAR 152	o perm	nt uap	192.166.10.22	192.100.10.00	Diaster 瑞虫 IFIP 后门 庄按
	2017-03-21 17:01:42	WAR 126	52 deny	tcp	24.153.164.131	66.102.131.19	FavoriteMan 下载省后门 下载操作
	2017-03-21 17:01:42	WAR 120	oz deny	tcp	24.153.104.131	402.402.131.19	Pavonteivian 下载合向门 下载操作
	2017-03-21 17:00:09	WAR 152	su perm	in uap	24 152 164 121	192.100.10.00	Diaster 瑞士 IFTP 后门 建按
e LOG	2017-03-21 17:00:09	WAR 120	oz deny	tcp	24.153.164.131	66,102,131,19	FavoriteMan 下载合向]下载保作
Log Search	- 2017-03-21 16-59-37	WAR 120	30 porr	icp vit ude	24.155.104.151	192 168 10 66	Pavonteiman P载音后门 P载保TF Blactor 標由 TETP 戶门连接
Log Setting	2017-03-21 16:06:51	WAR 126	50 perm	iit tcp	10.10.10.1	10.10.10.2	Trend ServerProtect TMregChange缓冲区溢 出攻击
	2017-03-21 16:06:42	WAR 126	56 deny	tcp	10.10.10.1	10.10.10.2	Sun Directory Server LDAP 拒绝服务攻击
	2017-03-21 16:06:38	WAR 126	65 deny	tcp	192.168.1.222	192.168.1.223	Simplog SQL注入漏洞
	2017-03-21 16:06:32	WAR 126	62 deny	tcp	192.168.1.222	192.168.1.223	phpBB Style ChangerViewer SQL注入漏洞
	2017-03-21 16:06:32	WAR 127	46 perm	nit tcp	192.168.1.222	192.168.1.223	SQL注入攻击识别9
	2017-03-21 16:06:32	WAR 134	28 deny	tcp	192.168.1.222	192.168.1.223	CoreHTTP Long URI 缓冲区溢出
	2017-03-21 16:06:28	WAR 126	61 deny	tcp	10.10.10.1	10.10.10.2	ORACLE SYS.KUPW-WORKER SQL $注 $ 入 攻击
	2017-03-21 16:06:11	WAR 126	58 deny	tcp	10.10.10.1	10.10.10.2	MySQL 登陆信息泄露攻击
	2017-03-21 16:06:03	WAR 126	57 deny	tcp	192.168.26.222	192.168.26.223	Microsoft IIS 4.0 FrontPage 98扩展源代码 后门漏洞
	2017-03-21 16:05:47	WAR 126	56 perm	nit top	10.10.10.1	10.10.10.2	Motorola Timbuktu crafted 缓冲区溢出攻击
	🔍 < 🛛 Page 1	of 2737	» I C				Show 1 - 20 , total of 5473

Figure 50

7.3 Policy with AV

Log in to the vSecCenter-N system and enter the POLOCY MANAGEMENT > ACL interface to configure the access control policy: [Action] select "Allow", [Source] select default "any", [Destination] select default "any", [Service]Default is empty, [Option] Av rule select "_default_av", [Option] select "Record Log", and successfully issued a strategy to vNGFW, as shown in Figure 51.



← ▲ https://192.168.34.21:9443				😺 🎇 📌 高速 🛛 C	옥 百	ī度 <ctrl+k></ctrl+k>	☆ 自 ♣ 徻	• •।• ম।• ≡
	=							Welcome 👻
2017-3-22 18:47:9	Home Page / ACL							
SYSTEM MANAGEMENT								
SYSTEM MONITOR	Access control policy							
B OBJECT MANAGEMENT	Not valid until published.	publish						
POLICY MANAGEMENT	add edit publ	ish Oper	rate v empty Collision	detection Search	Display	all strategies	Current group: def:	ault group
► ACL			0	Destination	a repres	Ourier	Outine	decodation
VIRTUALIZATION PLATFORM		action	Source	Destination		Service	Option	description
≣ USER		Allow					_default_av	
FIREWALL MANAGEMENT							Record log	
I UPGRADE								
≣ L06								
	C Page 1	of 1 >	» C					Show 1 - 1 , total of 1
Chaussesset lands								
Show recent task								

Figure 51

After logging the virtual machine virus file download operation, log in to the vSecCenter-N system and go to the LOG > Log Search interface. Click the "Malicious code detection log" tab to check the malicious code detection result log, where "warning" is "Warning", as shown in Figure 52.

T VSECCENTER								Welcome 👻						
2017-4-5 17:44:7	Home Page / Log Search													
SYSTEM MANAGEMENT														
SYSTEM MONITOR	vSecCenter	Access Control	IPS	Anti-DoS Anti-Virus	Device System	All Device Security Log	Vgate Manage Log							
B OBJECT MANAGEMENT	Start time:		End ti	me:	Type:	Please select type \vee	Keyword: Please enter key	query reset Emptylog						
E POLICY MANAGEMENT	Time	Level	Protocol	Source address	Destination address	Anti-Virus name	File type Anti-Virus process	message						
VIRTUALIZATION PLATFORM	2017-03-29 14	53:19 WAR	http	192 168 34 51	172 19 15 205	Trojan Win32 Inject	block	virus:Trojan Win32 Inject kmc						
≣ USER						kmc		, operation:block						
E FIREWALL MANAGEMENT	2017-03-29 14	50:46 WAR	http	192.168.34.51	172.19.15.205	Backdoor/Poison.xp s	block	virus:Backdoor/Poison.xps, operation:block						
E UPGRADE	2017-03-29 14	50:39 WAR	http	192.168.34.51	172.19.15.205	Backdoor/Poison.xp	block	virus:Backdoor/Poison.xps,						
≣ L0 6	2017 02 20 14	49-50 10/40		100 169 24 51	170 10 16 006	S	blash.	operation:block						
▶ Log Search	2017-03-29 14	40.00 VVAR	nup	132.100.34.51	172.19.15.205	kmc	DIOCK	, operation:block						
Log Setting	2017-03-29 14	45:12 WAR	http	192.168.34.51	172.19.15.205	Backdoor/Poison.xp s	block	virus:Backdoor/Poison.xps, operation:block						
		age 1 of 1		C				Show 1 - 5 , total of 5						

Figure 52