

# Support Doc

# **1** Troubleshooting (logs, procedures and techniques)

# Troubleshooting commands (show/debug/GUI), example of command output and what to look for

An SVM has two connection-status fields on the service manager (*the first one 'Online State' is hidden since vDFW-N-1.0.6*). Each status field stands for a channel of communication. One channel is for special configuration and the other is for all other communications between the service manager and the SVM.

SYSTEM MANAGEMENT	-	_					
E SYSTEM MONITOR	Virtual gateway management						
S OBJECT MANAGEMENT	Add group Add virtual gat	teway edit Forces	Sync CMDL on All De	V Force Sync CMDL			
E POLICY MANAGEMENT	Virtual gateway name	IP address Online State		CMDL conn status			
E VIRTUALIZATION PLATFORM							
₿ USER	172.19.15.170	172.19.15.170	Online	Online			
S FIREWALL MANAGEMENT	172.19.15.171	172.19.15.171	Online	Online			
▶ Firewall							
E UP GRADE							
≣ LOG							

Detail of the two fileds:

1. An SVM listens on tcp port 4000 to receive special configuration from the service manager. The special configuration mainly contains the address of the service manager. It's in case that the address of the service manager is changed when the SVM is running.

2. The service manager runs a Redis server to publish policies and settings, and send messages to SVMs. The service manager checks the client list of the Redis server to see whether an SVM is online for every N (N=10 in vDFW-N-1.0.6) seconds.

To resolve:

If ererything is OK, both fields should be "online". If the second status (CMDL) 北京天融信公司



shows "offline", user can select that device and click the button "Force Sync CMDL" and wait the status to become "online".

User can check the result of the last configuration publishment. Every SVM is expected to do things and write result to the Redis server. The result of a SVM should be OK if it works fine, otherwise there will be an error message.

SYSTEM MANAGEMENT										_
System Overview	Backup and re	covery \	View service status	Tasks	Result of Publis	hment				
System Configuration	Action Type:	Update co	nfig ~	check						
System Maintaining	Mission ID:	4			Publish Time:	2017-02-16 0	00:03:01	Result Key:	result.update_cfg.1.4	
SYSTEM MONITOR	Dotail	Courrent	vorsion': 14' Instahl: "	'aompioto	ofa': "evetope ad	min auth policy	s of maxinum same admin on	ing 10 nevetors as	Imin auth policy set	4
E OBJECT MANAGEMENT	Detail.	login-type	gin-type webui maxnum-login 10insystem admin-auth-policy set login-type ssh maxnum-login 10insystem admin-auth-policy set login-type telnet							
POLICY MANAGEMENT		delete all	login Tolnnetwork inte	ile tune in	eleav profile clear	heldofing schoo	dulo cloan/adofino group, con	ing clean/adofine	convice clean/ndofine	•
E VIRTUALIZATION PLATFORM	Device IP						Result			
≣ USER	172.19.15.171						ок			
FIREWALL MANAGEMENT	172.19.15.170						ок			
E UP GRADE										
≣ L0G										

Troubleshoot if the traffic is being redirected from ESXi.

Show slots under vnics:

#### # summarize-dvfilter

There should be a slot with number >= 4 under the protected vnic. This command

also shows the filter name.



The filter name can also be listed with this command:

*# vsipioctl getfilters* 

-	天融信
_	TOPSEC_

天融信安全技术 高品质保证

Beijing Topsec

Filter Name	:	nic-18361993-eth0-serviceinstance-39.4
VM UUID		50 02 a5 5a 0f f2 d8 d4-0a 8d 85 c5 67 e8 f0 1a
VNIC Index		0
Service Profile		serviceprofile-37
Filter Hash		63839
Flow Collection Flags		
L2 Pass Flows		0n
L2 Drop Flows		0n
L3 Drop Flows		0n
L3 Inactive Flows		0n
L3 Active Flows		0n
All Flows		Off
Global override		0n

Show rules of a filter:

# vsipioctl getrules -f <FILTER\_NAME>



Troubleshoot if the traffic is being redirected from SVM.

Login to the firewall management console in SVM:

#/tos/bin/login

username: superman

password: talent

Then call *system tcpdump* to capture packets. This will show only the redirected packets.

Tops	sec0S# syst	em tcpdump -nn -i	any host 172.19.1	L5.180 -q				
ngto	ngtos tcpdump: verbose output suppressed, use -v or -vv for full protocol decode							
list	ening on a	n <mark>y, link-type EN1</mark>	0MB (Ethernet), ca	apture size 65535	bytes			
R-0	[feth998]	02:08:15.484348	IP 192.168.32.36 >	> 172.19.15.180: I	CMP echo request, id 3	30743, seq 1, length 64		
X - 0	[feth998]	02:08:15.484485	IP 192.168.32.36 >	> 172.19.15.180: I	CMP echo request, id 3	30743, seq 1, length 64		
R-0	[feth998]	02:08:15.485082	IP 172.19.15.180 >	192.168.32.36: I	CMP echo reply, id 307	743, seq 1, length 64		
X - 0	[feth998]	02:08:15.485113	IP 172.19.15.180 >	192.168.32.36: I	CMP echo reply, id 307	743. sea 1. lenath 64		

Troubleshoot if the traffic is being redirected from the service manager.

User can check logs to see whether the access control policy worked.

Configure log settings of SVMs. Check the Access Control and set its level to INFO:

了天融信 TOPSEC			天融信安全技术 Bei,	き 商品质保证 jing Topsec	_
SYSTEM MANAGEMENT					
a SYSTEM MONITOR	Log setting				
B OBJECT MANAGEMENT	Not valid until pul	blished. publish			
E POLICY MANAGEMENT					
SVIRTUALIZATION PLATFORM	Server address:	192.168.32.40			
≣ USER	Transport protocol:	UDP ~			
FIREWALL MANAGEMENT	ServerPort:	1514			
E UP GRADE	Log type:	🖂 Access Control	Log level:	INFO	$\sim$
E LOG		🗹 Anti-DoS	Log level:	INFO	$\sim$
Log Search		IPS	Log level:	INFO	$\sim$
Log Setting		Anti-Virus	Log level:	INFO	$\sim$
		🗹 System	Log level:	INFO	$\sim$
		apply			

Turn on the log recording in the access control policy:

SYSTEM MANAGEMENT		Add access control p	olicy					$\otimes$
SYSTEM MONITOR	Acce	Essential information	Source	Destination	Service	Advanced security	Advanced opt	tions
B OBJECT MANAGEMENT	add					,		
POLICY MANAGEMENT		Time configuration						
► ACL								
VIRTUALIZATION PLATFORM		Single time:					~	
<b>USER</b>		Multiple time:					~	
FIREWALL MANAGEMENT		Logi	Record				~	ר
UP GRADE		Log.	Record					J
≣ LOG		Connection options:	Common	connection			$\sim$	
		Maximum number of ac	tive connectio	ons: P	lease enter[0-	21 47 48 36 47]		
						_		
						• • • • • • • • • • • • • • • • • • •	save close	reset

Generate network traffic matching the access control policy, the SVM will send logs to the service manager. User can check SVM logs on web-UI of the service manager:

了天殿	信 EC						天融	信安全技术	高品质例	截正
								Beijir	ng Topsec	
SYSTEM MANAGEMENT										
SYSTEM MONITOR	vSecCenter Acc	ess Control IPS	Anti-DoS	Anti-Virus	Device	System V	/gate Manage Log			
E OBJECT MANAGEMENT	Start time:	End :	time:		000	Type: Ple	ase select type \vee	Keyword: Please enter H	cey query re	iset Empty log
E POLICY MANAGEMENT	Time	Level	Modular	Operate	Protocol	App	Source address	Source port	Destination address	Destination port
VIRTUALIZATION PLATFORM	2017-07-05 23:27:02	INFORMATION	ac	拒绝	6	unknown	192,168,32,36	57366	172.19.15.180	22
≣ USER	2017-07-05 23:26:48	INFORMATION	ac	拒绝	6	unknown	192.168.32.36	57364	172.19.15.180	22
E FIREWALL MANAGEMENT										
E UP GRADE										
≣ LOG										
▶ Log Search										
Log Setting										

# 2 Steps to collect logs from partner SVM

Where to find the log for each component?

#### Service Manager Log

/var/www/vSecCenter/logs/\*.log

/var/log/redis/\*.log

#### SVM Log

Common logs of the firewall will be sent to the service manager. User can browse logs of both the service manager and the SVMs on UI of the service manager.

## **3** Steps to upgrade from previous partner solution

## versions

#### Upgrade procedure, upgrade path, impact to data plane traffic

#### Upgrade SVM

Upload firewall upgrading package to the service manager, then publish the package to SVMs.

When upgrading, the firewall processes in the SVM will restart, and the firewall policies won't work during that time. Currently, the default failure policy is fail-open, so the data plane traffic will bypass.

#### **Upgrade Service Manager**

1. Login to the service manager's terminal.



- 2. Stop the services.
- 3. Upgrade with RPM packages provided by Topsec.
- 4. Start the services.

# 4 Sample problematic scenarios and how to address

them

# 4.1 Most common misconfigurations

#### Forget to set the services to be auto-started.

The services in the service manager is not auto-started by default. Administrator can execute **vseccenter.sh autostart** to let it start after booting.

#### Forget to publish changes.

User should click "publish" button to publish firewall policies and settings to the SVMs. Otherwise they will not be valid.

## 4.2 Troubleshoot a sample error

Troubleshoot a Sample Error

Published access control policy, but it doesn't work. Check the result of the publishment, find that one SVM didn't response:

SYSTEM MANAGEMENT									
System Overview	Backup and re	covery View service	ce status Tasks	Result of Publis	shment				
System Configuration	Action Type:	Update config	Check						
System Maintaining	Mission ID:	5		Publish Time:	2017-07-05 1	6:48:06	Result Key:	result.update_cfg.1.5	
SYSTEM MONITOR									~
E OBJECT MANAGEMENT	Detail:	{'current_version': '5 login-type webui ma	xnum-login 10\nsyste	e_ctg:: "system ac em admin-auth-poli	cy set login-type	e set maxnum-same-a e ssh maxnum-login	admin-online 10\nsystem ad 10\nsystem admin-auth-pol	icy set login-type telnet	
POLICY MANAGEMENT		delete all'pipe event	et clean rule, tupo i	pelaav profile cloa	andofino sobod	hulo cloan/ndofino ar	oup convice clean/ndefine	convice clean/ndofine	~
E VIRTUALIZATION PLATFORM	Device IP					Result			
≣ USER	172 19 15 170					ок			
S FIREWALL MANAGEMENT	172.19.15.171								
E UP GRADE									
≣ LOG									

Check status of the SVM, find that this SVM is 'Offline Offline':

了 天 融信				天融	官安全技术	高品质保证	
<i>,</i>					Beijing	Topsec	
言 SYSTEM MANAGEMENT							
SYSTEM MONITOR	Virtual gateway management						
冒 OBJECT MANAGEMENT	Add group Add virtual gatewa	uy edit	Force Sync CMDL	on All Dev	Force Sync CMDL	Operate $\lor$	Refresh
E POLICY MANAGEMENT	Virtual gateway name	IP addres	s	Online Stat	e	CMDL conn statu	IS
VIRTUALIZATION PLATFORM							
를 USER	171	172.19.15.	171	Offline		Offline	
FIREWALL MANAGEMENT	170	172.19.15.	170	Online		Online	
Firewall							
= UP GRADE							
클 LOG							

The first 'Offline' means that the TCP port 4000 is closed on the SVM. So login to the SVM's console, look for a process named 'tp\_agent', but not found:



'tp\_agent' is the process which listens on TCP port 4000, so start it manually



About 20 seconds later, the first status becomes 'Online', and the CMDL status is still 'Offline':

SYSTEM MANAGEMENT					
E SYSTEM MONITOR	Virtual gateway management				
B OBJECT MANAGEMENT	Add group Add virtual gatewa	y edit Force Sync CMDI	on All Dev Force Sync CMDL	Operate v Refresh	
POLICY MANAGEMENT	Virtual gateway name	IP address	Online State	CMDL conn status	
VIRTUALIZATION PLATFORM	√  ☐ default_group				
음 USER	171	172.19.15.171	Online	Offline	
FIREWALL MANAGEMENT	170	172.19.15.170	Online	Online	
► Firewall					
E UP GRADE					
클 LOG					

Just wait, or click the 'Force Sync CMDL' button above the SVM list. After about 30 seconds, the CMDL status becomes 'Online':



Beijing Topsec

SYSTEM MANAGEMENT								
E SYSTEM MONITOR	Virtual gateway management							
E OBJECT MANAGEMENT	Add group Add virtual gatewa	ay edit Force Sync CMDI	L on All Dev Force Sync CMDL	Operate $\vee$ Refresh				
POLICY MANAGEMENT	Virtual gateway name	IP address	Online State	CMDL conn status				
VIRTUALIZATION PLATFORM	default group							
E USER	171	172.19.15.171	Online	Online				
FIREWALL MANAGEMENT	170	172.19.15.170	Online	Online				
Firewall								
= UPGRADE								

# 5 Best practices

## Demo of the product

## Home Page

≣ LOG

🗊 VSECCENTER										Welcome
2017-6-19 14:54:46	Home Page /	System Overview								
SYSTEM MANAGEMENT			system state				Alarm	information		
System Overview		Virtual gateway	install 2 virtual gateways,		Time		Event type	Level	Information	
System Configuration		status:	2 virtual gateway Online							
System Maintaining		Software version:	N-1.0.4							
SYSTEM MONITOR		system time:	2017-06-19 14:54:45							
B OBJECT MANAGEMENT										
POLICY MANAGEMENT										
VIRTUALIZATION PLATFORM										
= USER										
FIREWALL MANAGEMENT			Attack trend graph				Malici	ous code trer	nd chart	
E UP GRADE						d)				
E LOG	Attack number	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	65 AT 40 AT	-16 14:14:00 tack number: 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	05.09.200 of malicious cod	<sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup> <sup>42</sup>	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	45 21, 12 40 40 40 40 40 40 40 40 40 40 40 40 40	o o o o o o o o o o o o o o o o o o o

#### Add NSX Information



天融信安全技术 高品质保证

Beijing Topsec

SYSTEM MANAGEMENT					
SYSTEM MONITOR	Virtuali				
OBJECT MANAGEMENT	add	edit delete			
POLICY MANAGEMENT	Name				
VIRTUALIZATION PLATFORM		Add virtualizati	on platfo	orm	
▶ Platform Center		*Name:		nsx	
E USER		*NSX manager ad	ldress:	172.19.15.111	
FIREWALL MANAGEMENT		*NSX manager us	ername:	admin	
E UP GRADE		*NSX manager pa	ssword:	•••••	
E LOG		vCenter Address		Please enter the IP address	s of the platform
		vCenter Usernam	e:		
		vCenter Passwor	d:		
		description:			
				_	
				sav	e cancel reset

## Register Service

SYSTEM MANAGEMENT									
SYSTEM MONITOR	Virtualization Platform Management								
OBJECT MANAGEMENT	add edit delete Sync info Register nsx service Unregister nsx service								
E POLICY MANAGEMENT	Name	NSX manager address	vCenter Address	Service ID	Service Manager ID				
E VIRTUALIZATION PLATFORM	vmware platform nsx	172.19.15.111		service-45	servicemanager-57				
Platform Center		-							
豊 USER									
S FIREWALL MANAGEMENT									
E UP GRADE									
≣ LOG									

Check Service on NSX



Beijing Topsec

Navigator I	Service Definitions	Service Definitions									
Hosts and Clusters	Services Service Managers H	ervices Service Managers Hardware Devices									
Networking & Security											
tome NSX Home	NSA Manager. 172.19.15.111 ▼	A Manager. 172.19.15.111									
🚱 Dashboard	🕂 🖌 🗶 🛛 🍪 Actions 🗸										
🙀 Installation	Name	Version	Functions	Deployment Mechanism	Service Managers	Services					
🋬 Logical Switches	🖏 GenericFastPath		IDS IPS		NSX Manager	0					
NSX Edges	뿾 Port Profile				Port Profile Manager	0					
Firewall	Protocol Introspection		Network Monitoring	Host based vNIC	NSX Manager	0					
ra SpoofGuard	뿾 Distributed Load Balancer		2: Load balancer,	Host based vNIC	NSX Manager	0					
Service Definitions	뿾 VMware Data Security	6.2	Data security	Host based Guest Introsp	Data Security Service	0					
Service Composer	🛱 Topsec vDFW	1.0	Firewall	Host based vNIC	Topsec vSecCenter	0					
Data Security	SAM Data Collection Service		Data Collection	Management plane only	InternalServiceManager	0					
	🧊 Topsec vDFW ming	1.0	Firewall	Host based vNIC	Topsec vSecCenter mi	0					
Elow Manitoring	뿾 Guest Introspection	6.2.3		Host based Guest Introsp	InternalServiceManager	0					
Activity Menitoring	🤀 VMware Network Fabric	6.2.4		Host based NSX vSwitch fi	InternalServiceManager	0					
Networking & Security Inventory											
🔠 NSX Managers >											

## Deploy SVM on NSX UI

🖣 Home 🕑 🕑	Management Host Preparation Log	ical Network Prepar	ation Service D	eployments							
Networking & Security	SX Manager: 172.19.15.111 V										
🔠 NSX Home	Network & Security Service Deployment	work & Security Service Deployments									
🚱 Dashboard	Network & security services are deployed	work & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.									
🔅 Installation											
💁 Logical Switches		Manlan	Installation Contra	Consider Otatus	Cluster	Detectors	Dent Cours	ID Address Desers			
NSX Edges	Service	Version	Succeeded	Service Status	Cluster	Datastore	Port Group	IP Address Range			
Firewall	TopsecvDFvv	1.0	♦ Oucceeded	✓ Up	W vCluster-1	nts_109	avPortGro	VNGFW_test			
K SpoofGuard											

## **Check Firewall Status**

SYSTEM MANAGEMENT										
SYSTEM MONITOR	Virtual gateway management									
B OBJECT MANAGEMENT	Add group Add virtual gateway edit Force Sync CMDL on All Dev Force Sync CMDL Operate V Refresh									
POLICY MANAGEMENT	Virtual gateway name	IP address	Online State	CMDL conn status						
VIRTUALIZATION PLATFORM	✓  ☐ default_group									
E USEB	Topsec_vDFW(172.19.15.173)	172.19.15.173	Online	Online						
FIREWALL MANAGEMENT	Topsec_vDFW(172.19.15.172)	172.19.15.172	Online	Online						
Firewall										
E UP GRADE										
E LOG										

Configure Redirection Policy on NSX UI



天融信安全技术 高品质保证

Beijing Topsec

Navigator I	Firewall								
Hosts and Clusters	Configura	Configuration Saved Configurations							
Networking & Security	NSX Mana	SX Manager. 172 19 15 111							
🚟 NSX Home									
💫 Dashboard	1 Last	publish operation succ	eeded 6/26/20	017 11:02:57 PM					
@ Installation	General	General Ethernet Dartner security services							
🏠 Logical Switches			-						
NSX Edges	• 🗇 3	< ≣1 ≣↓ 183 🗳	% <b>Y</b>						
👸 Firewall	No.	Name	Rule ID	Source	Destination	Service	Action		
No SpoofGuard	v 🖪	test (Rule 1)					🗟 😅 🕈 💋		
🜼 Service Definitions	€ 1	test rule	1144	* 201	* 207	* 201	Redirect		
🖉 Service Composer				any	any	any	Topsec vDFW_VendorTemplate for servic		
🚳 Data Security		Default Section							
	45	Default Section					🚽 C 🕈 💋		
🙀 Flow Monitoring									
Activity Monitoring									
traceflow									
<ul> <li>Networking &amp; Security Inventory</li> </ul>									
🔠 NSX Managers >									

#### Synchronize Information (Security Groups) from NSX

SYSTEM MANAGEMENT			
SYSTEM MONITOR	Virtualization Platform Management		
OBJECT MANAGEMENT	add edit delete Sync info Register nsx	service Unregister nsx ser	/ice
E POLICY MANAGEMENT	Name	NSX manager address	vCente
VIRTUALIZATION PLATFORM	vmware platform nsx	172.19.15.111	
Platform Center		-	

#### **Check Security Groups**



## Add Security Group to Address Group

大開信 TOPSEC			天融信安全技术	卡 商品质保证
-			Bei	ijing Topsec
SYSTEM MANAGEMENT				
SYSTEM MONITOR	Host	Subnet Address rang	ge 🔄 Address group 🔵 Virtual ma	chine Other dynamic contai
🛓 OBJECT MANAGEMENT	add e	Add address group	resources	$\otimes$
Address Object	Name	·····		<u> </u>
Service Object		Name:	g1	
▶ Time Object		Static member		
APP Object		Heat address:		
POLICY MANAGEMENT		Post address.		
VIRTUALIZATION PLATFORM		Subnet address:		
		Address range:		~
E FIREWALL MANAGEMENT		Dynamic member		
UPGRADE		Virtual bost		
E LOG		address:		
		Other container:	sg_test ×	~
				save cancel reset

## Configure Access Control Policy

SYSTEM MANAGEMENT	_	Add access control p	olicy			$\otimes$
SYSTEM MONITOR	Access	Essential information	Source De	estination Service	Advanced security	Advanced options
	Not valid	Destination address				
POLICY MANAGEMENT	add					
	D ID	Host address:				~
		Subnet address:				~
FIREWALL MANAGEMENT		Address range:				~
<b>UPGRADE</b>		Address group:	g1 ×			~
E LOG						
	-				_	
					s	ave close reset

### Publish to SVMs



Beijing Topsec

SYSTEM MANAGEMENT									
SYSTEM MONITOR	Access control policy								
OBJECT MANAGEMENT	Not valid until published. (publish)								
POLICY MANAGEMENT	add edit publ	add edit nublish Onerate empty Collision detection Search Display all strategies							
► ACL				Destroy	0				
VIRTUALIZATION PLATFORM		action	Source	Destination	Service				
= USER	100007	Block		IPAddress : g1	SSH				
FIREWALL MANAGEMENT					·				
≣ UP GRADE									
E LOG									

## Check Firewall Logs

l

SYSTEM MANAGEMENT									
SYSTEM MONITOR	vSecCenter Ac	ccess Control	IPS	Anti-DoS Anti-Virus	Device System	All Device Security Log	Vgate Manage	e Log	
B OBJECT MANAGEMENT	Start time:	[	End tin	ne:	Type: F	Please select type \vee	Keyword: Plea	ase enter key qu	ery reset Emptylog
E POLICY MANAGEMENT	Time	Level	Protocol	Source address	Destination address	Anti-Virus name	File type	Anti-Virus process	message
E 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
E USER	2017-03-29 14:50:46	WAR	http	192.168.34.51	172.19.15.205	Backdoor/Poison.xp		block	virus:Backdoor/Poison.xps,
I UPGRADE	2017-03-29 14:50:39	WAR	http	192.168.34.51	172.19.15.205	s Backdoor/Poison.xp		block	operation:block virus:Backdoor/Poison.xps,
a LOG	0047.00.00.44.40.50	14/4 D	har -	100 100 01 51	470 40 45 005	S		M. d.	operation:block
▶ Log Search	2017-03-29 14:46:50	VVAR	nttp	192.168.34.51	172.19.15.205	kmc		DIOCK	, operation:block
Log Setting	2017-03-29 14:45:12	2 WAR	http	192.168.34.51	172.19.15.205	Backdoor/Poison.xp s		block	virus:Backdoor/Poison.xps, operation:block