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

Trademark Statement

Information Feedback

http://www.topsec.com.cn

Directory

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:

1、 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.

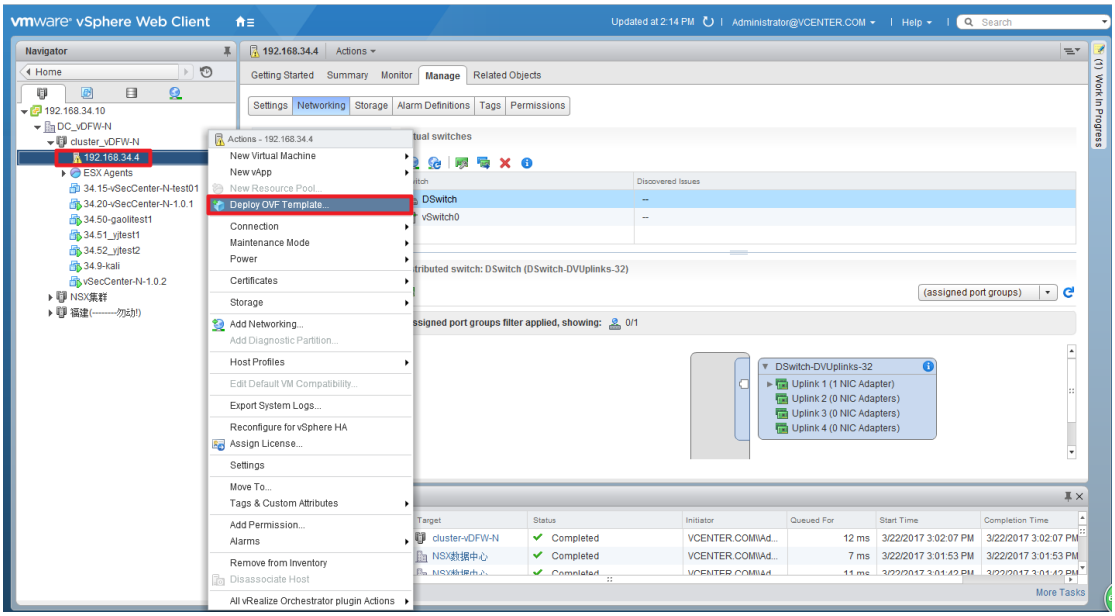

Figure 1

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

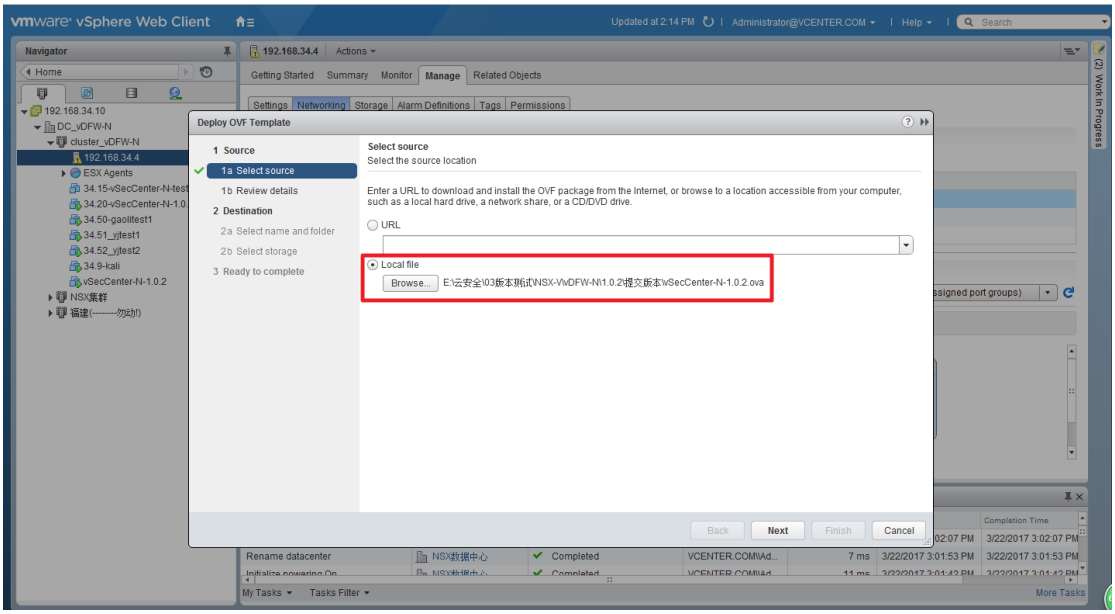

Figure 2

3、 Check the details of the OVA template and click the "Next" button, as shown in Figure 3.

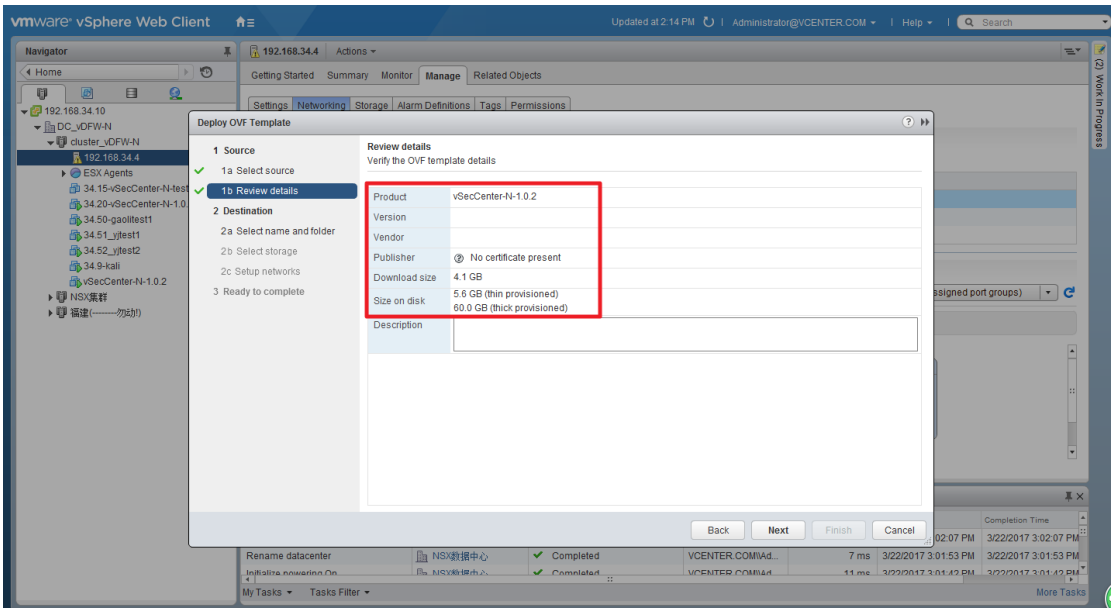

Figure 3

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

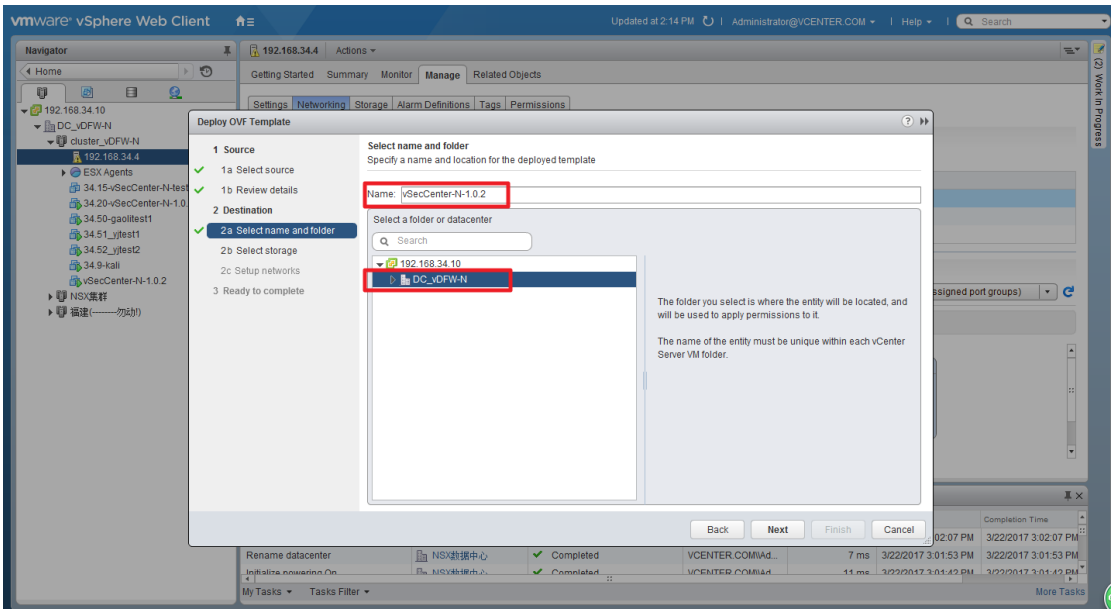

Figure 4

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

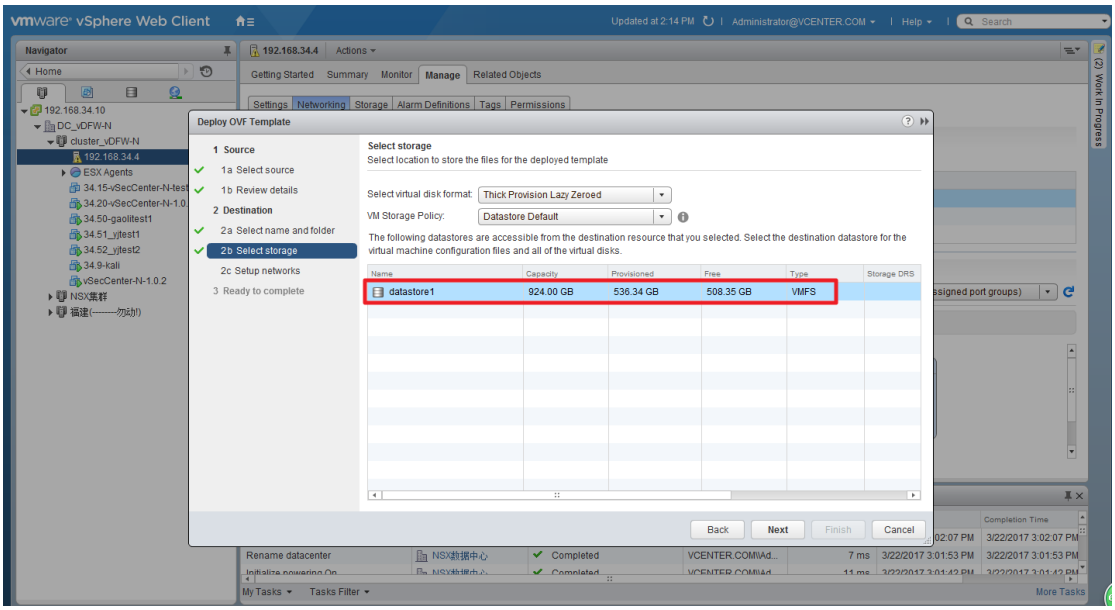

Figure 5

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

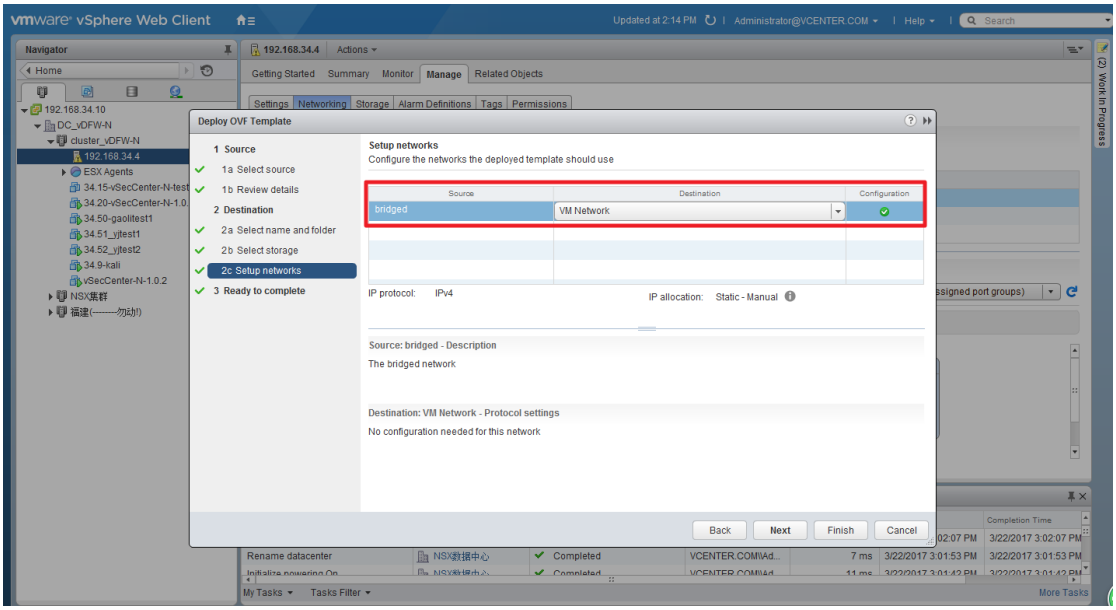

Figure 6

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.

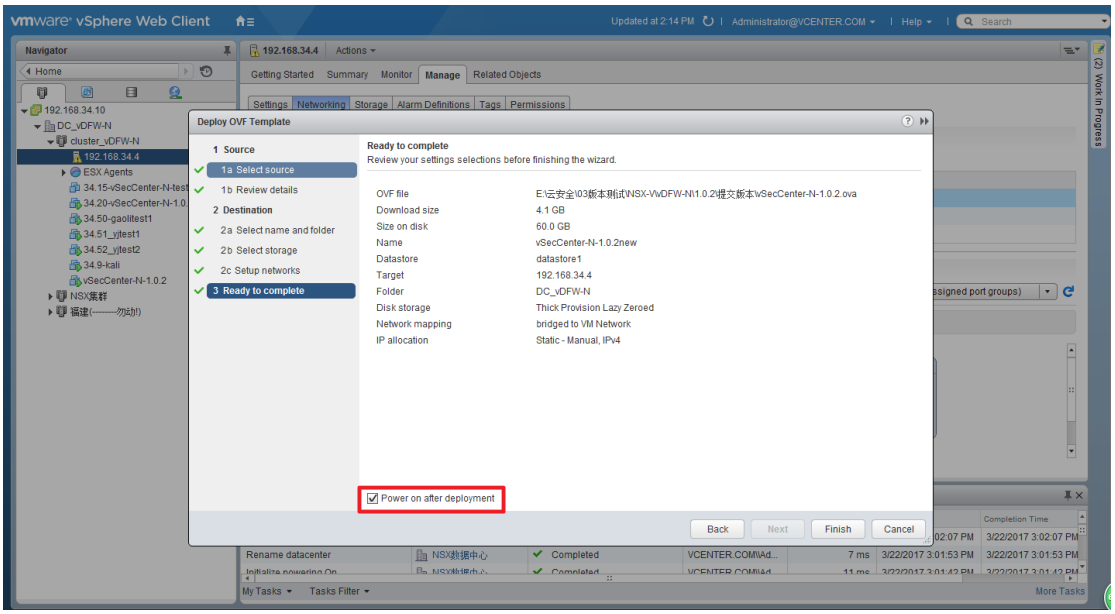

Figure 7

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:

1、 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,*** as shown in Figure 8.

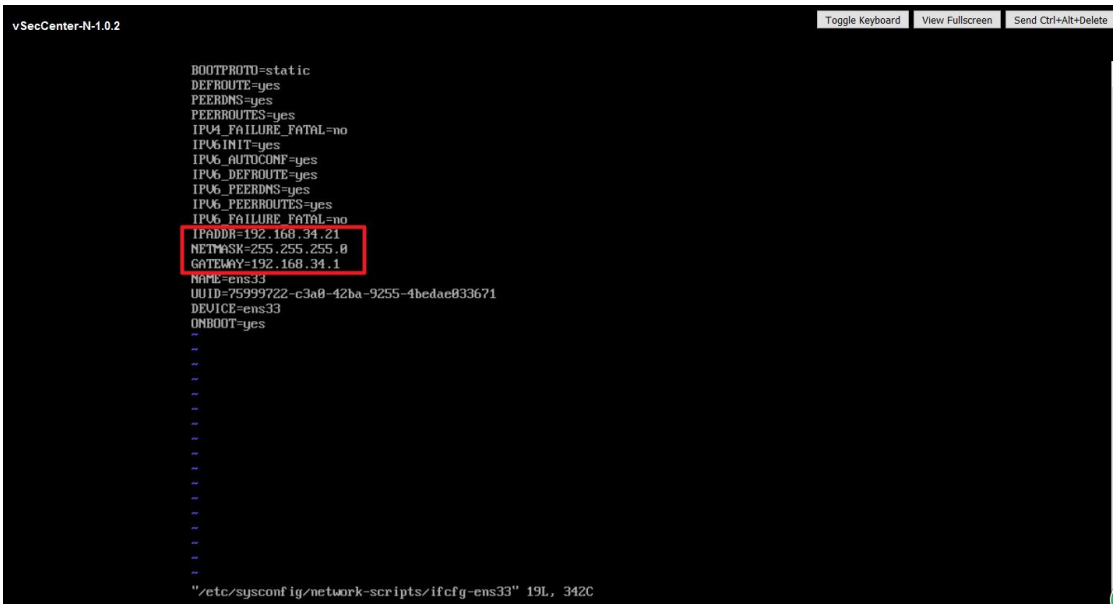

Figure 8

2、 After modifying and saving the server IP address, you need to manually restart the network card service,as shown in Figure 9.

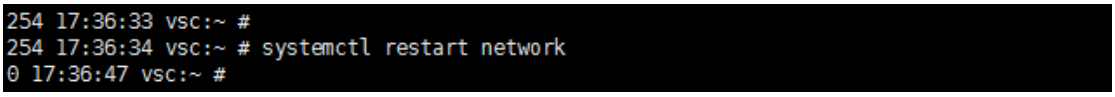

Figure 9

3、 Use *vSecCenter.sh autostart* configure service auto_start, use *vSecCenter.sh to start* start the system main service, as shown in Figure 10.

Figure 10

5.3 Login&register 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:

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

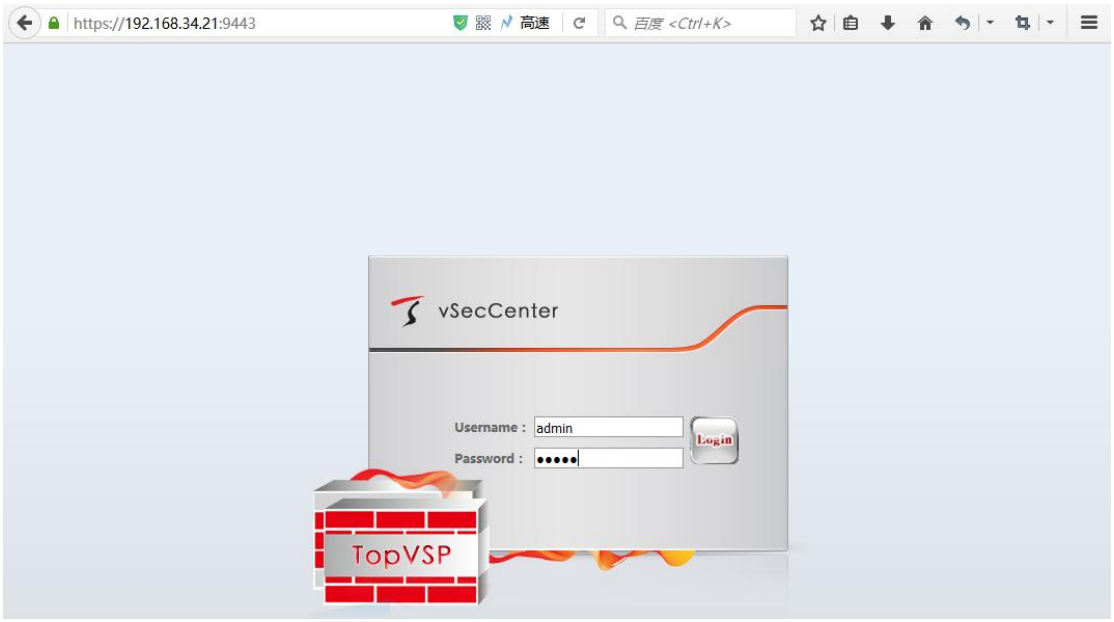

Figure 11

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.

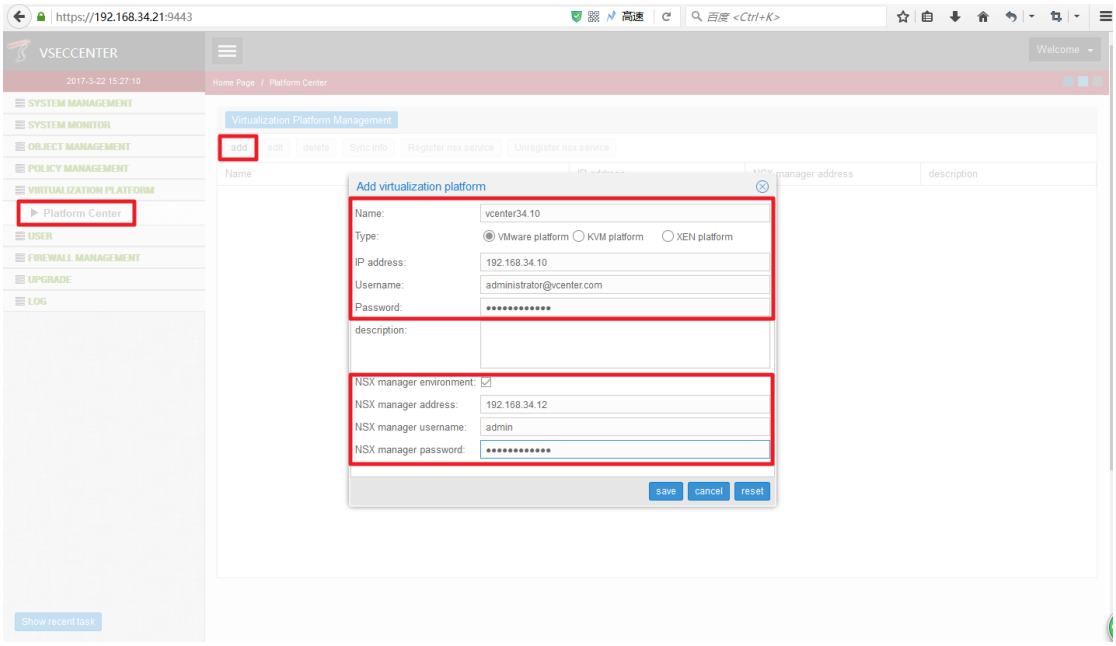

Figure 12

3、 Select the virtualization platform you just added and click the "Sync info" button, as shown in Figure 13.

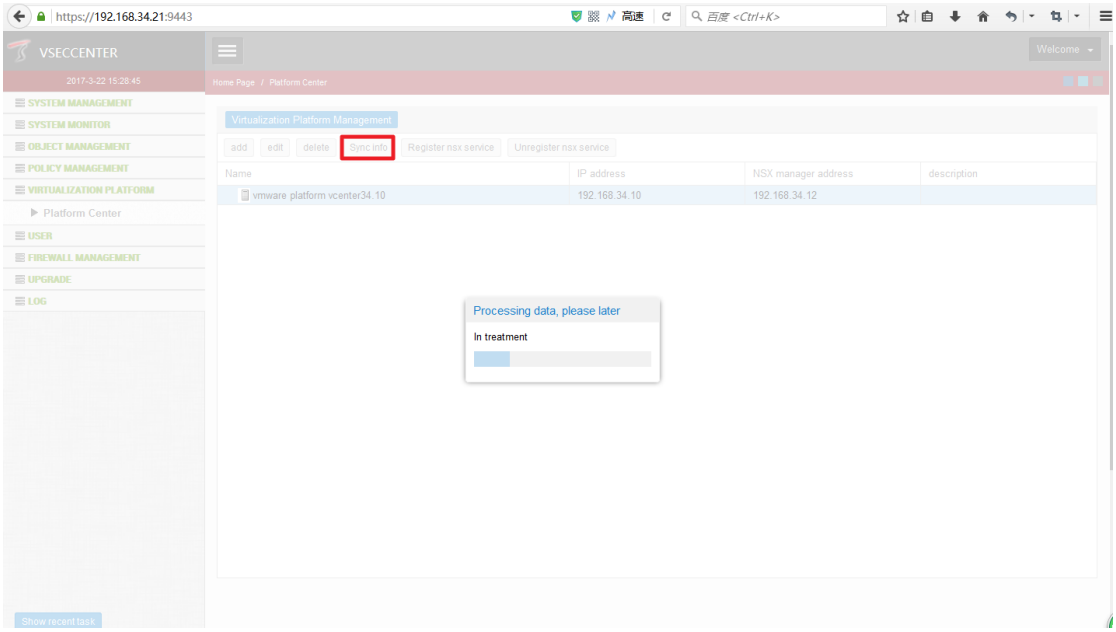

Figure 13

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

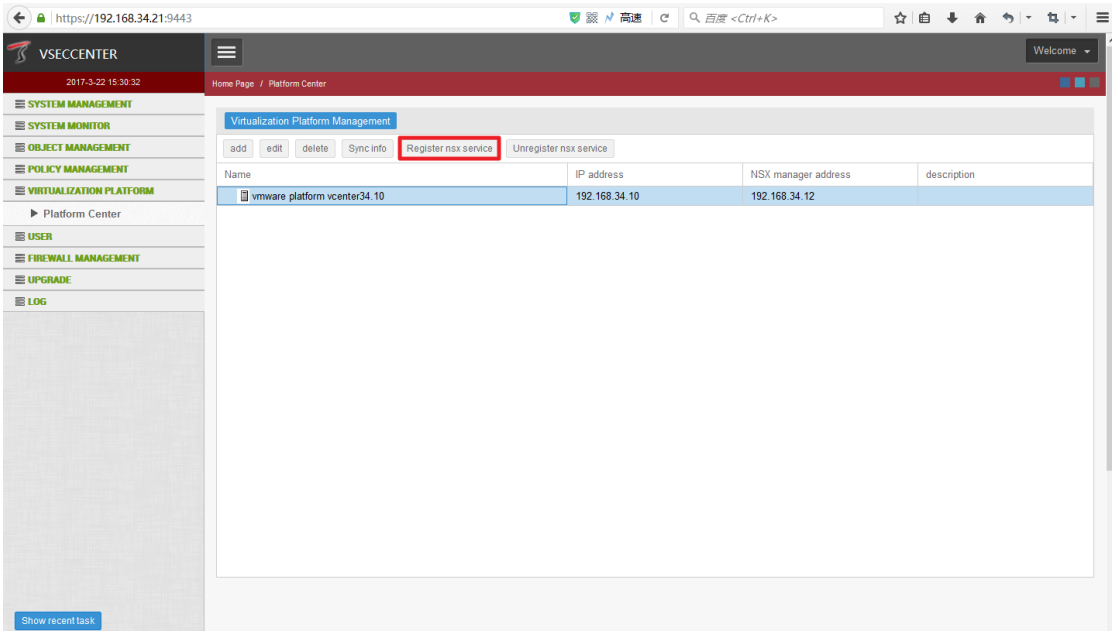

Figure 14

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.

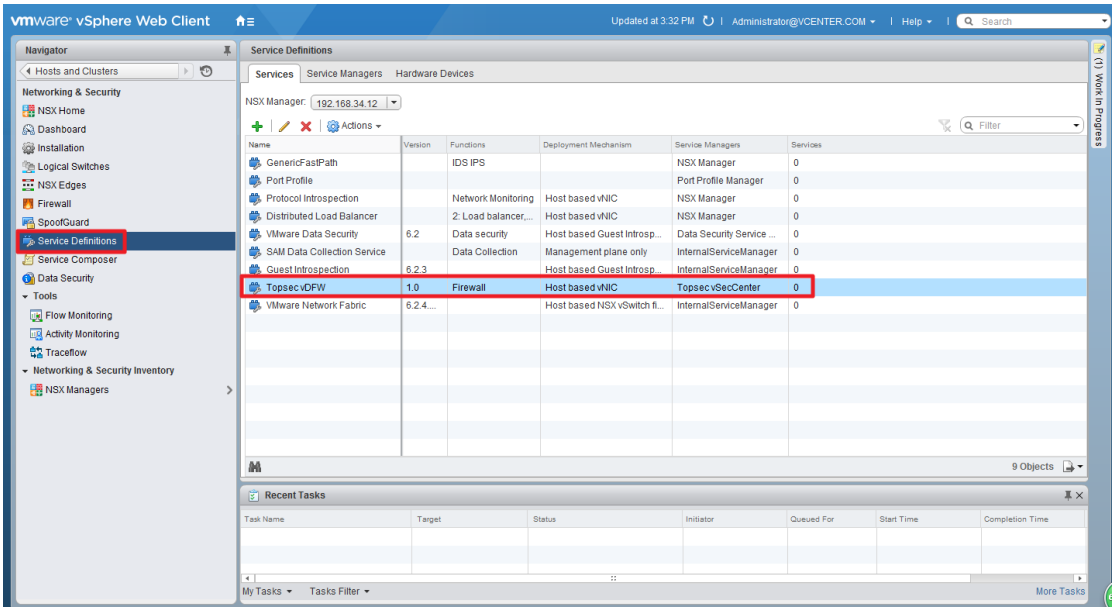

Figure 15

5.4 Deployment&Configuration of system Top-VSP

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

1、 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.

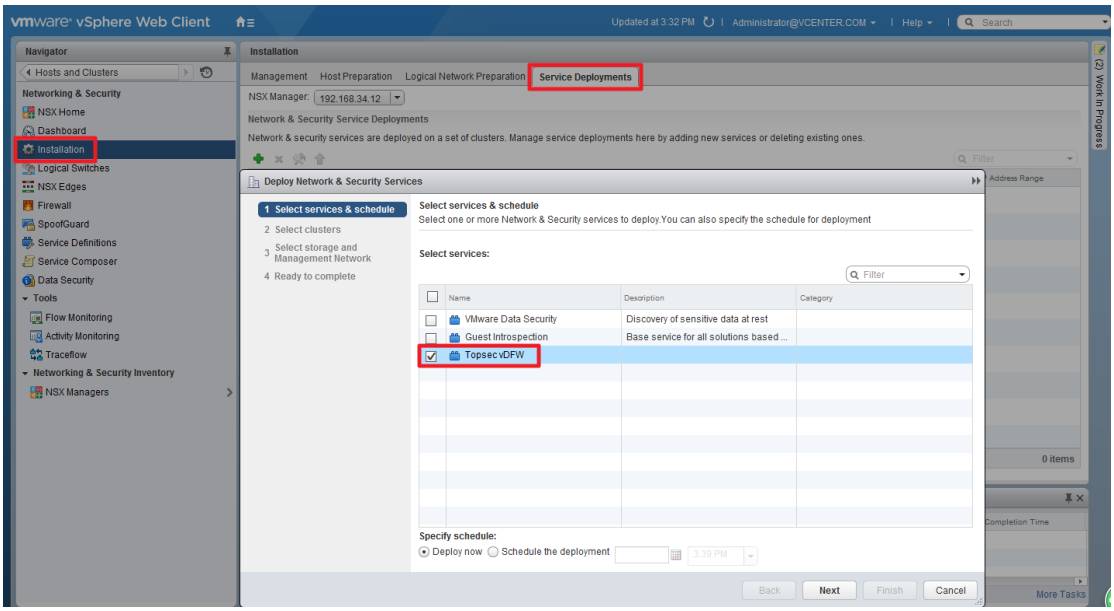

Figure 16

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

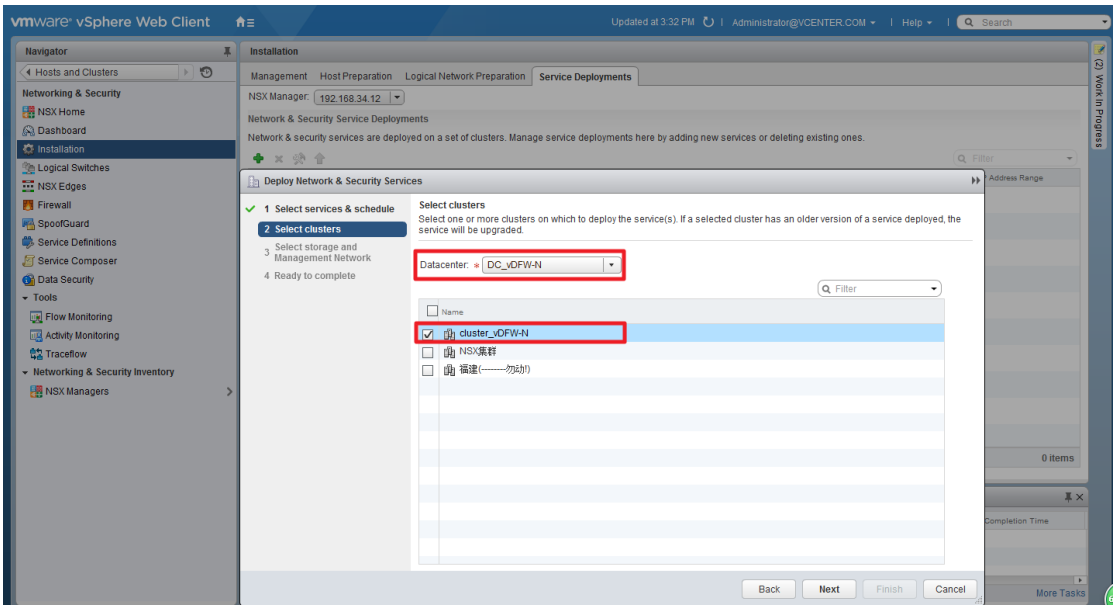

Figure 17

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.

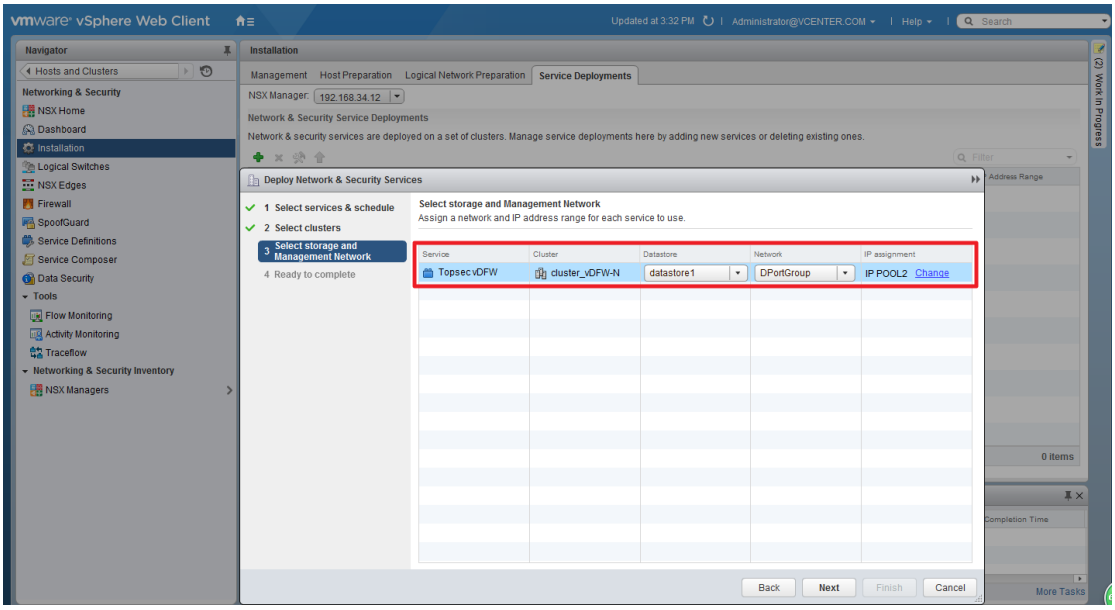

Figure 18

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

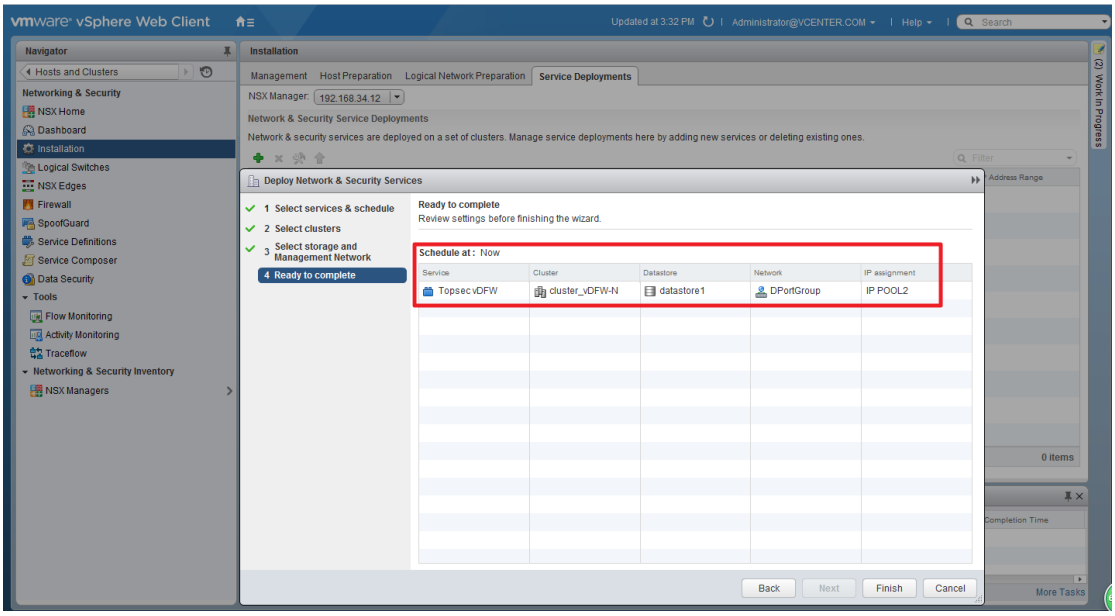

Figure 19

5、 Patiently waiting to deploy vNGFW to complete, the installation status shown as successful, as shown in Figure 20.

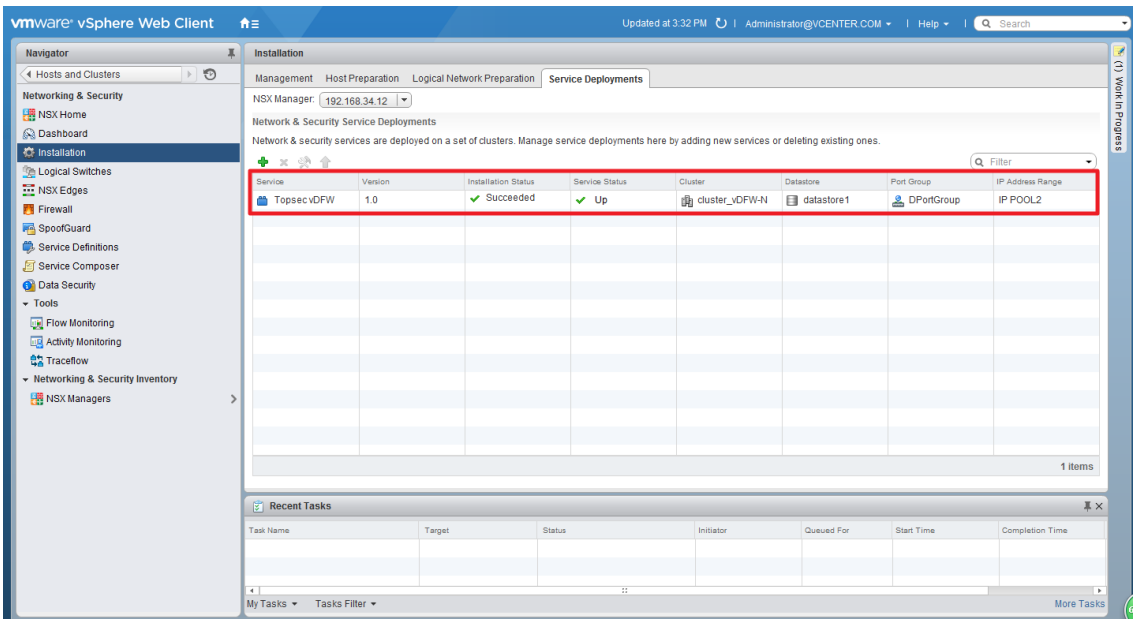

Figure 20

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.

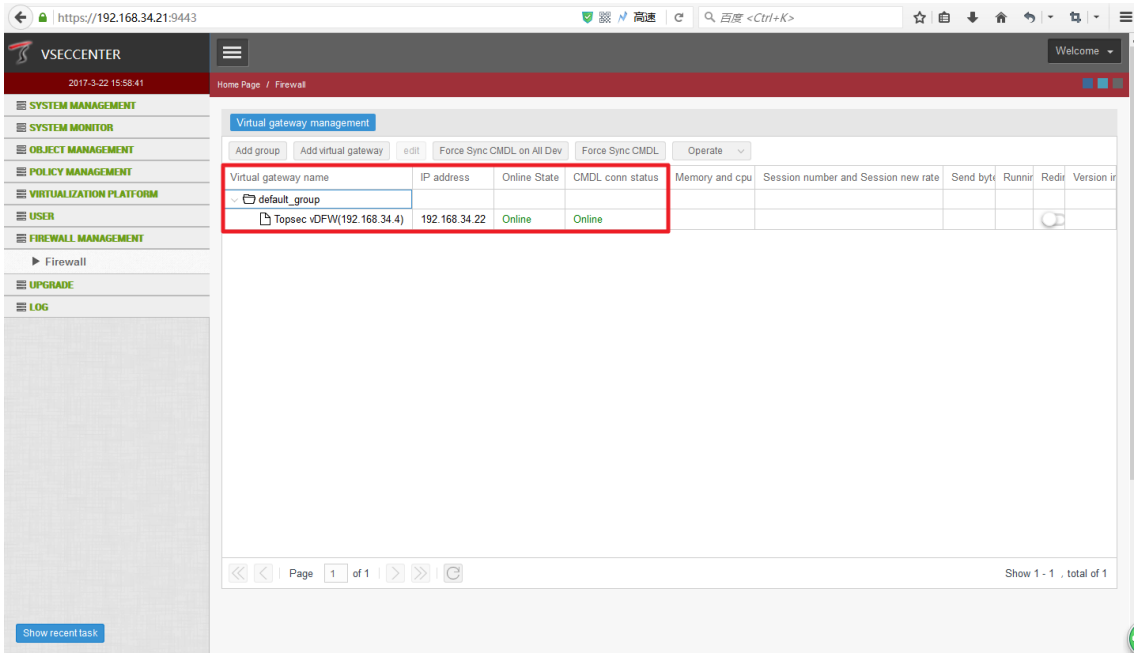

Figure 21

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:

1、 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.

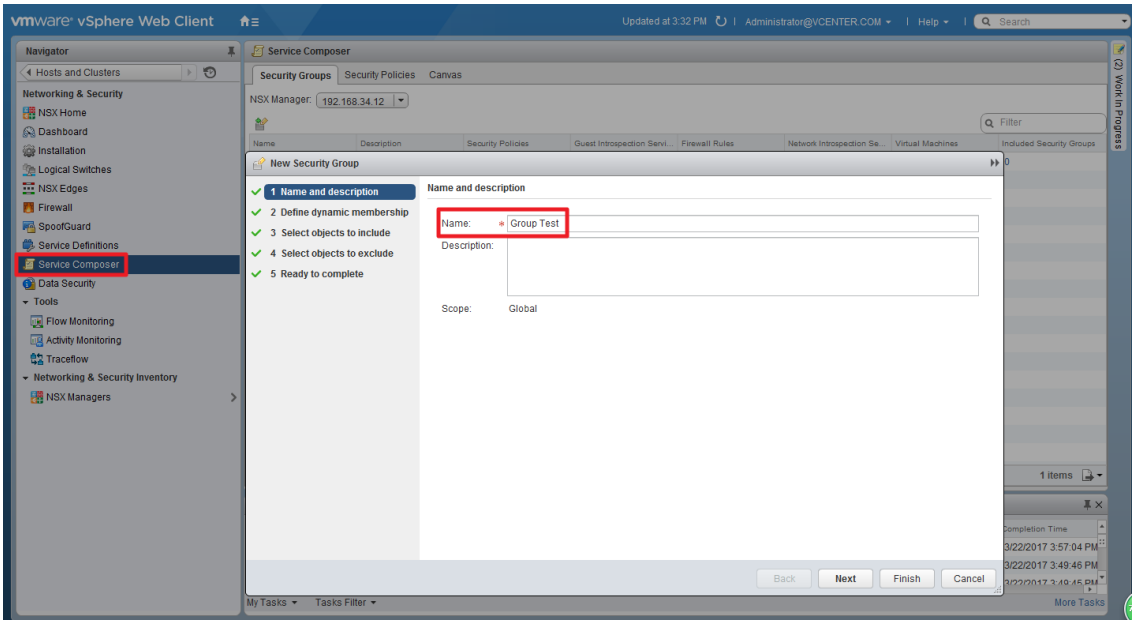

Figure 22

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.

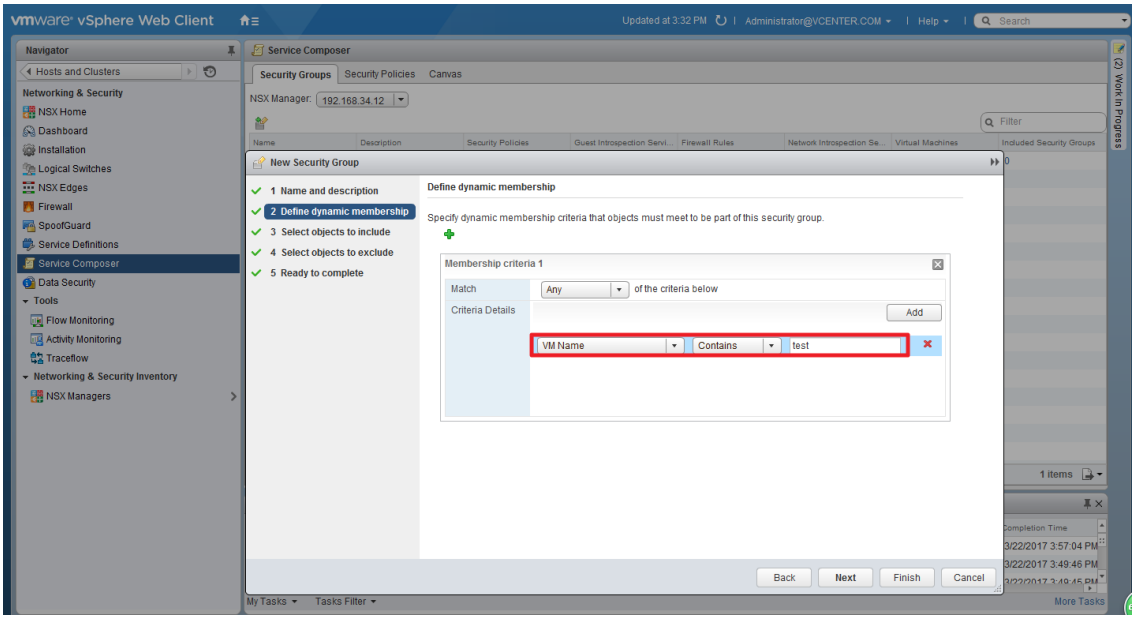

Figure 23

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.

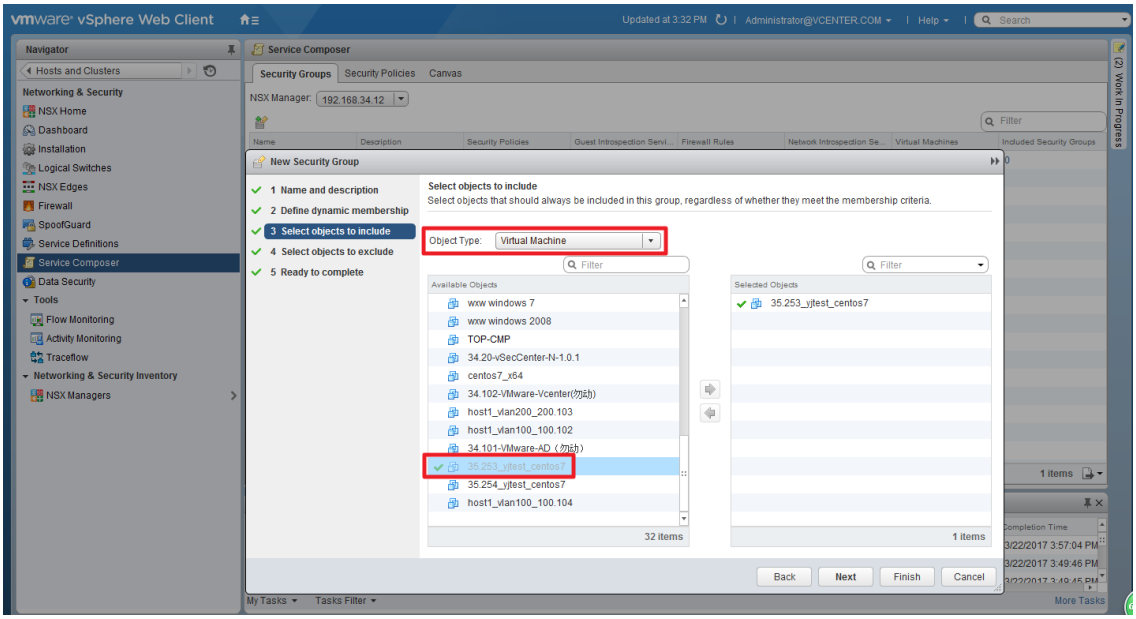

Figure 24

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.

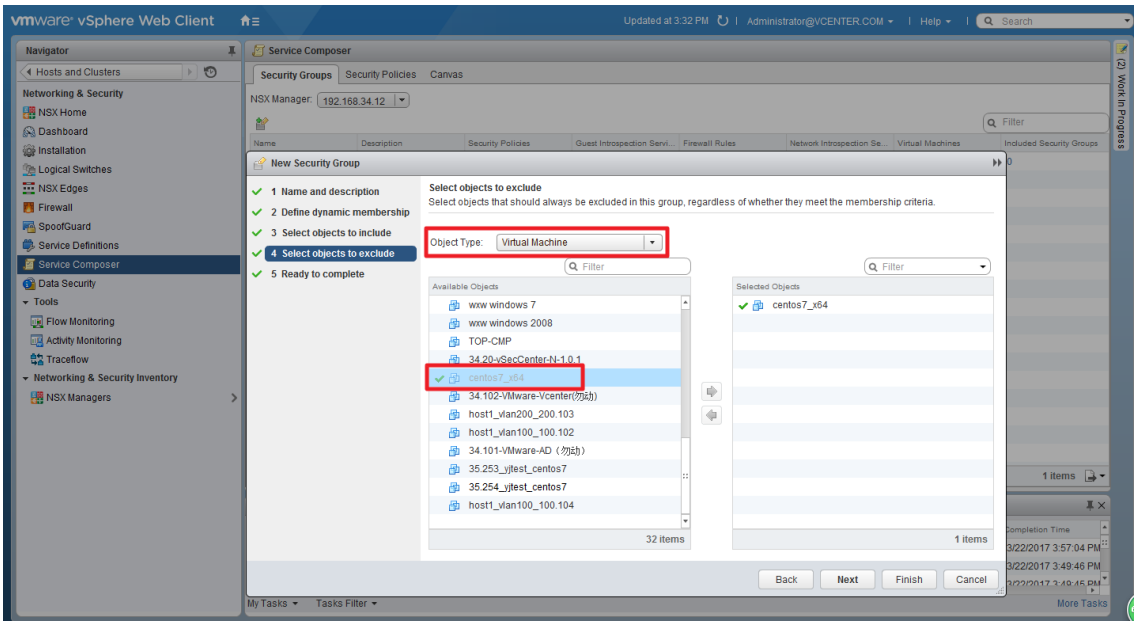

Figure 25

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

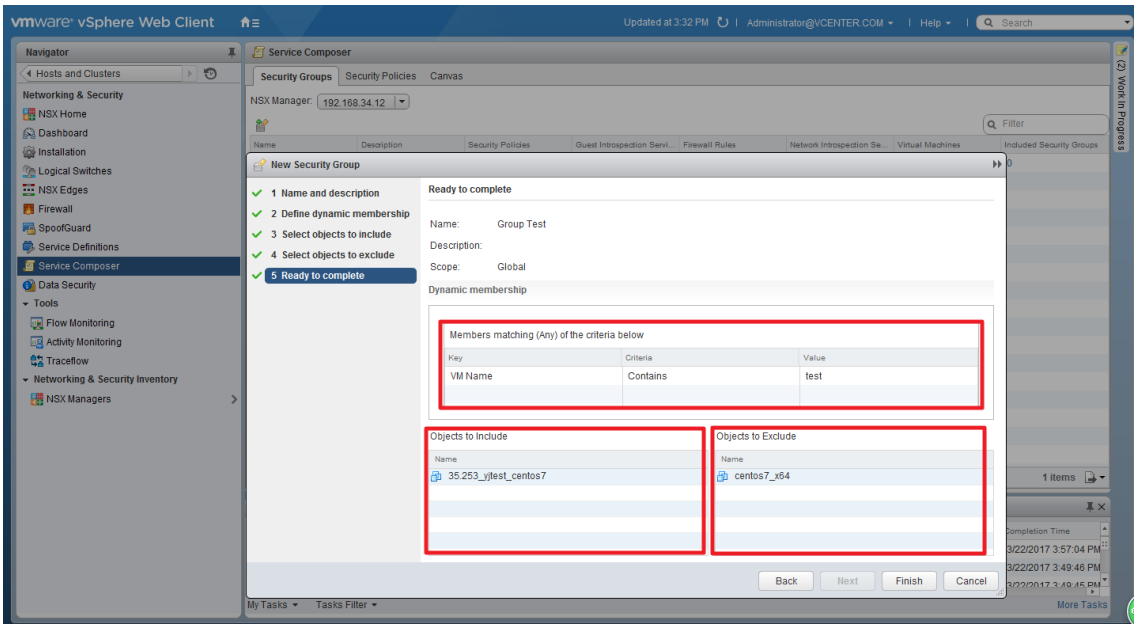

Figure 26

6、 After creating a security group, you can view the eligible objects in the security group, as shown in Figure 27.

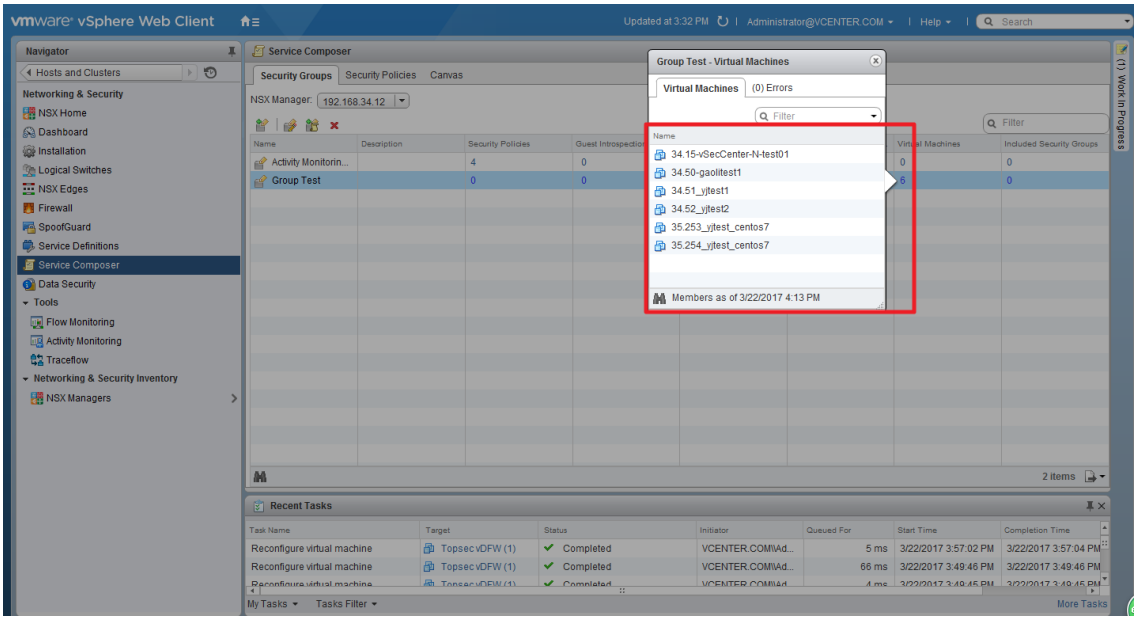

Figure 27

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.

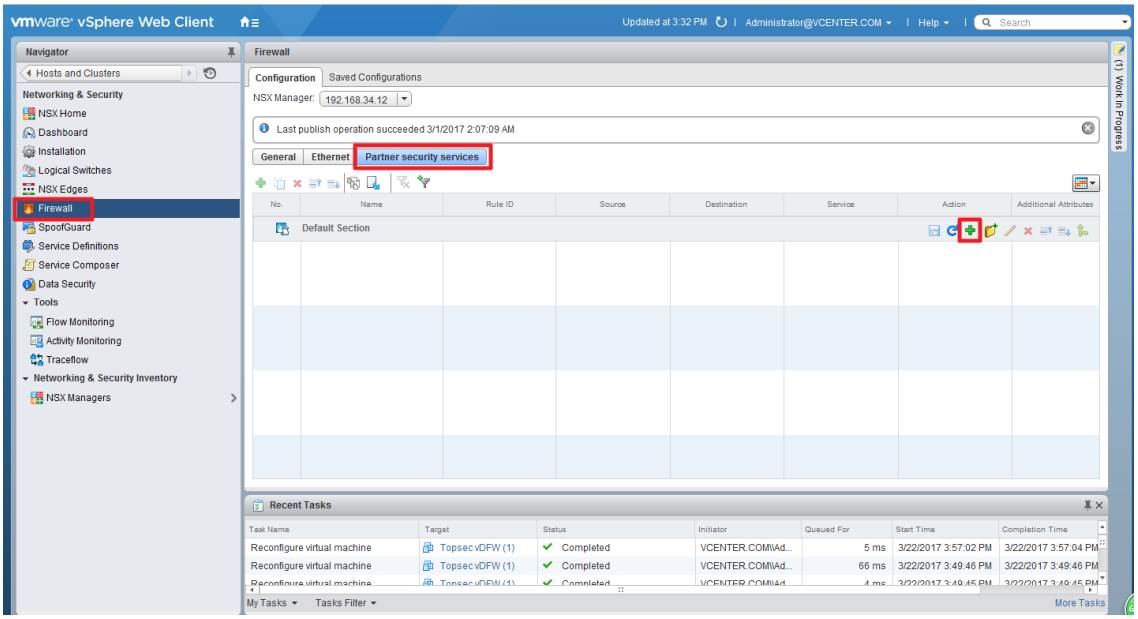

Figure 28

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

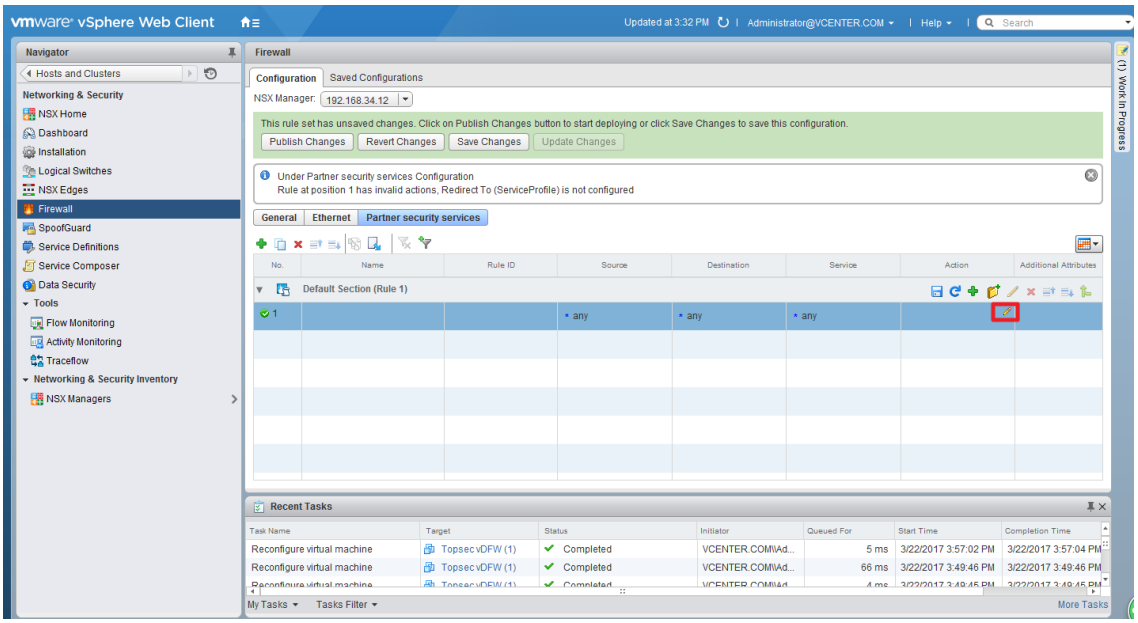

Figure 29

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.

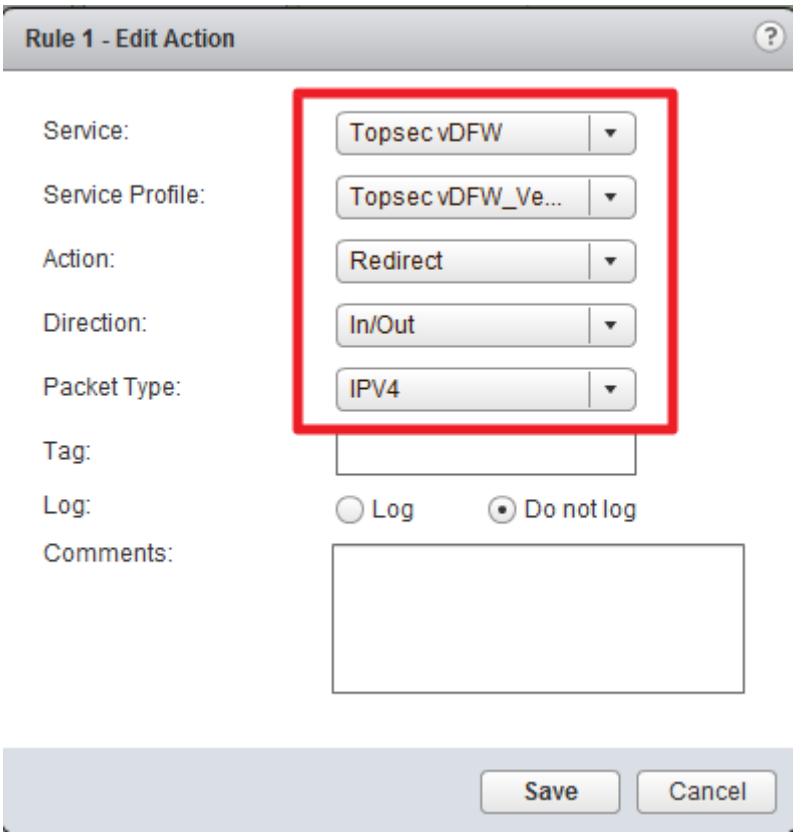

Figure 30

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.

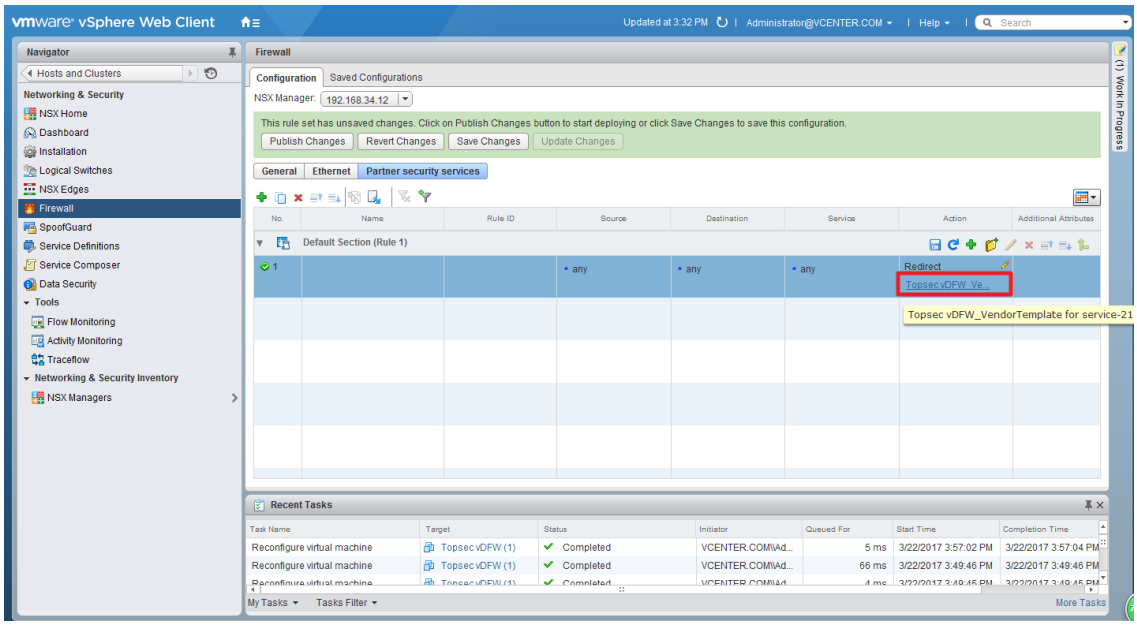

Figure 31

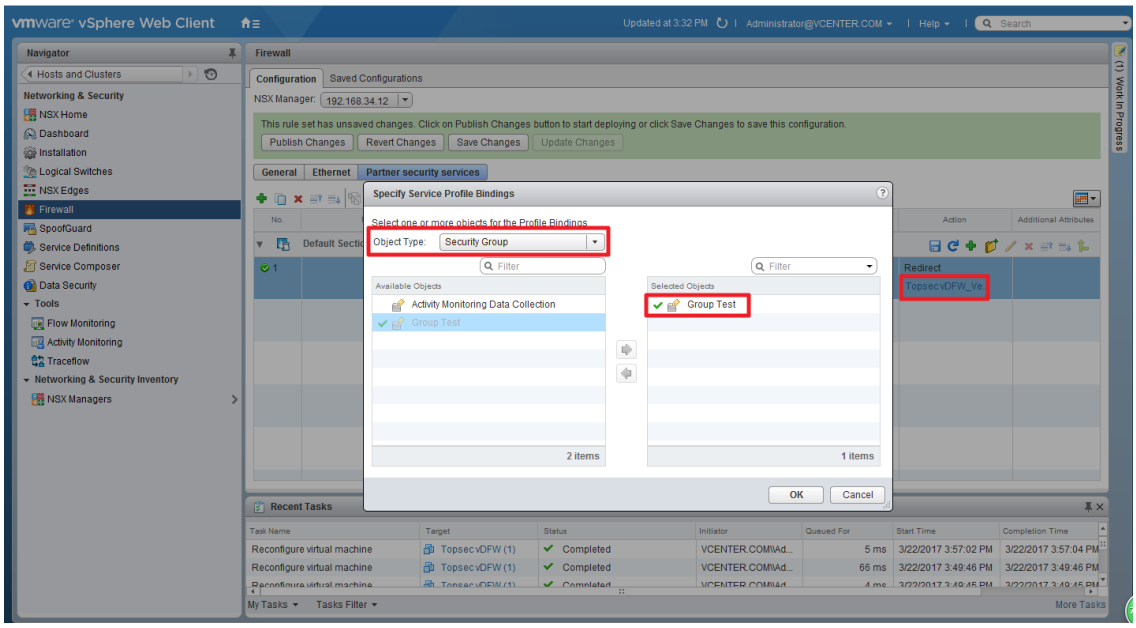

Figure 32

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

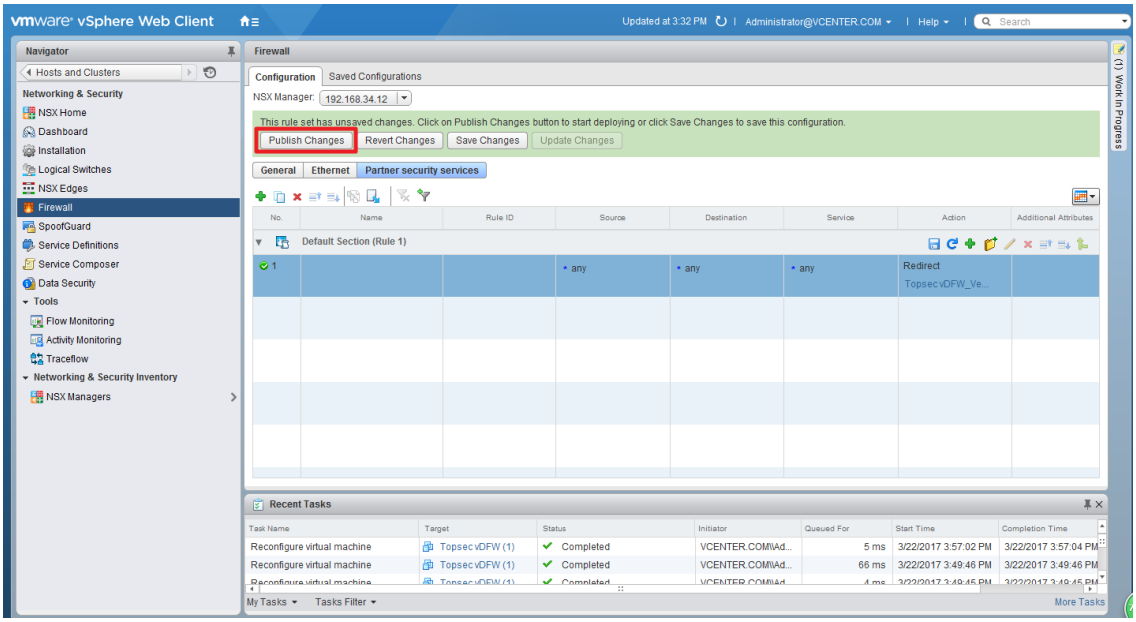

Figure 33

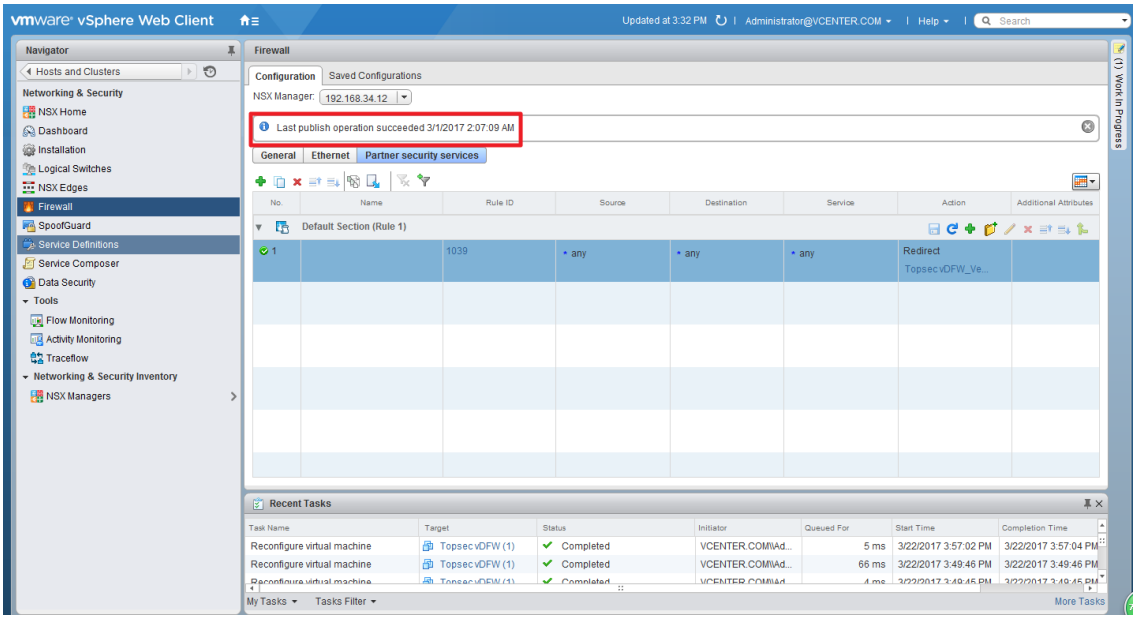

Figure 34

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.

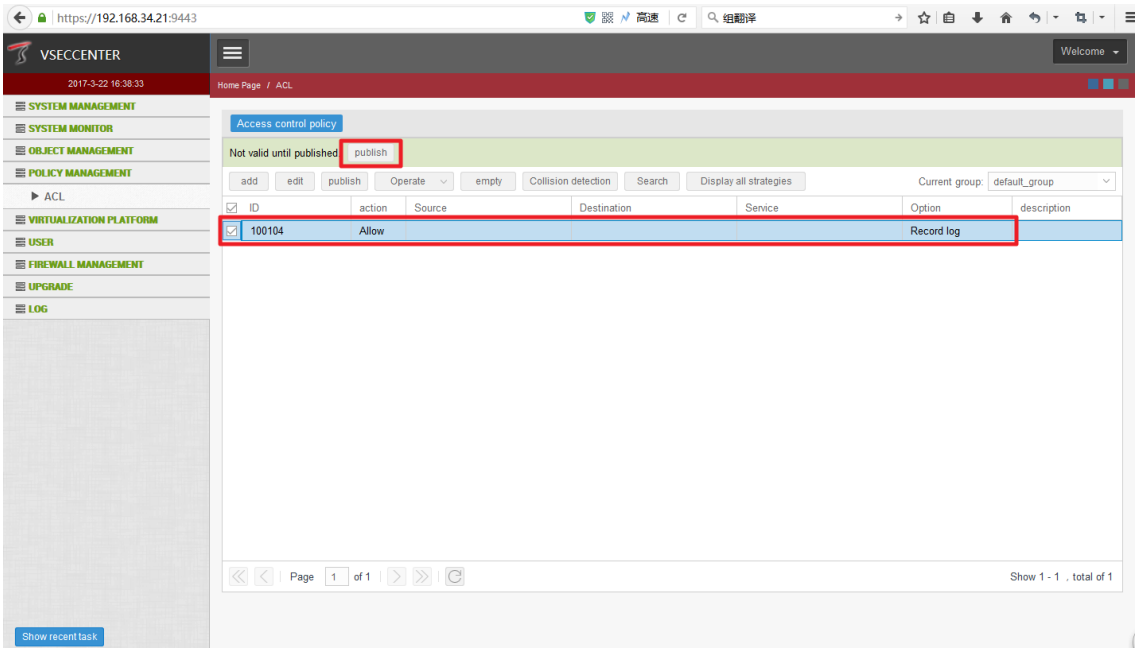

Figure 35

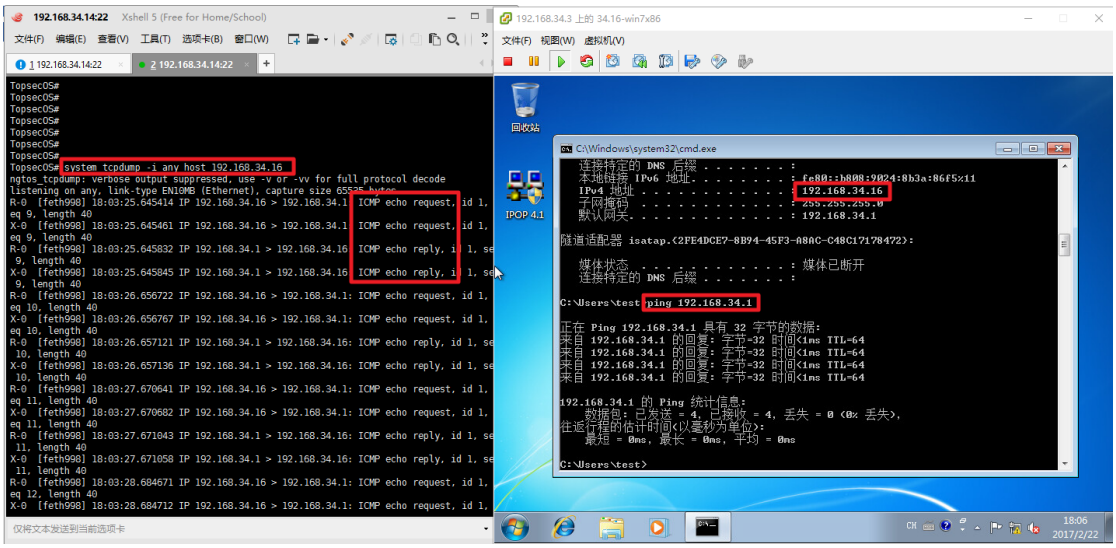

Figure 36

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.

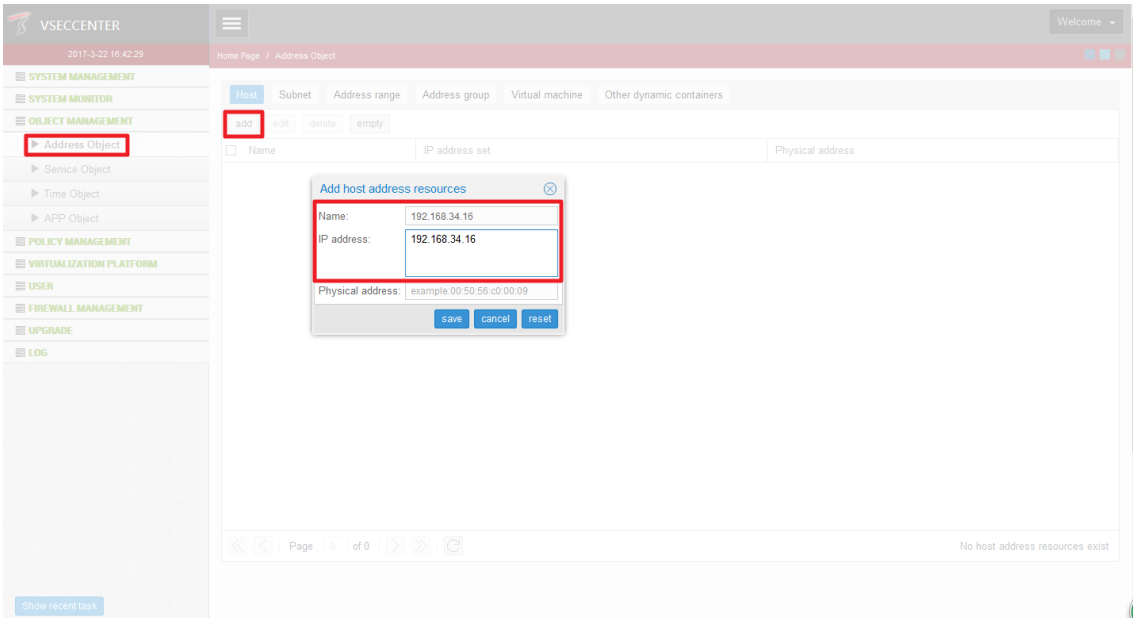

Figure 37

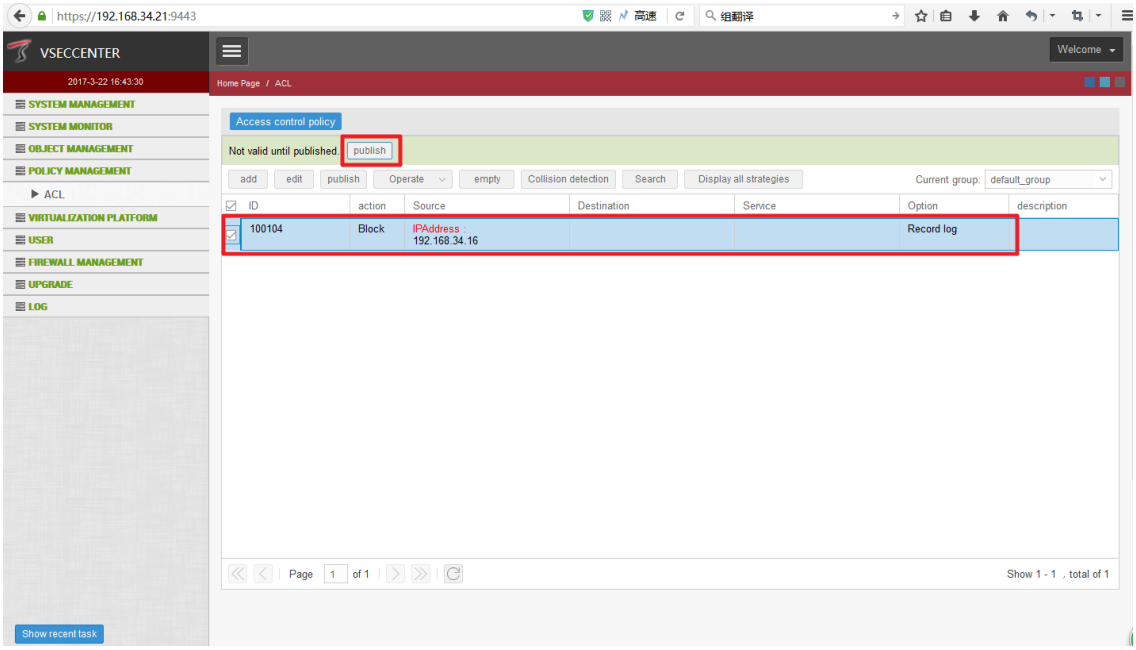

Figure 38

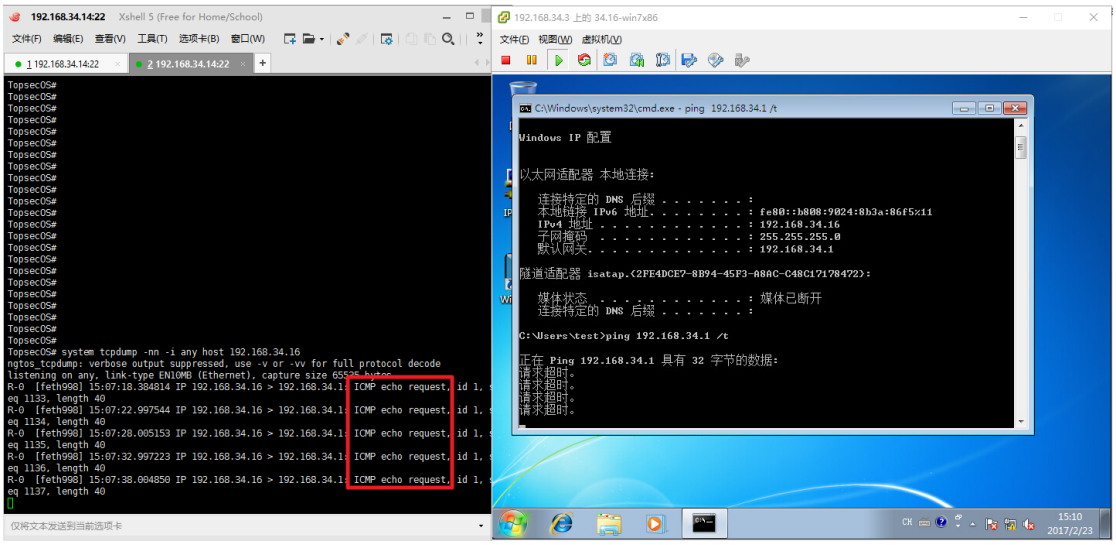

Figure 39

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.

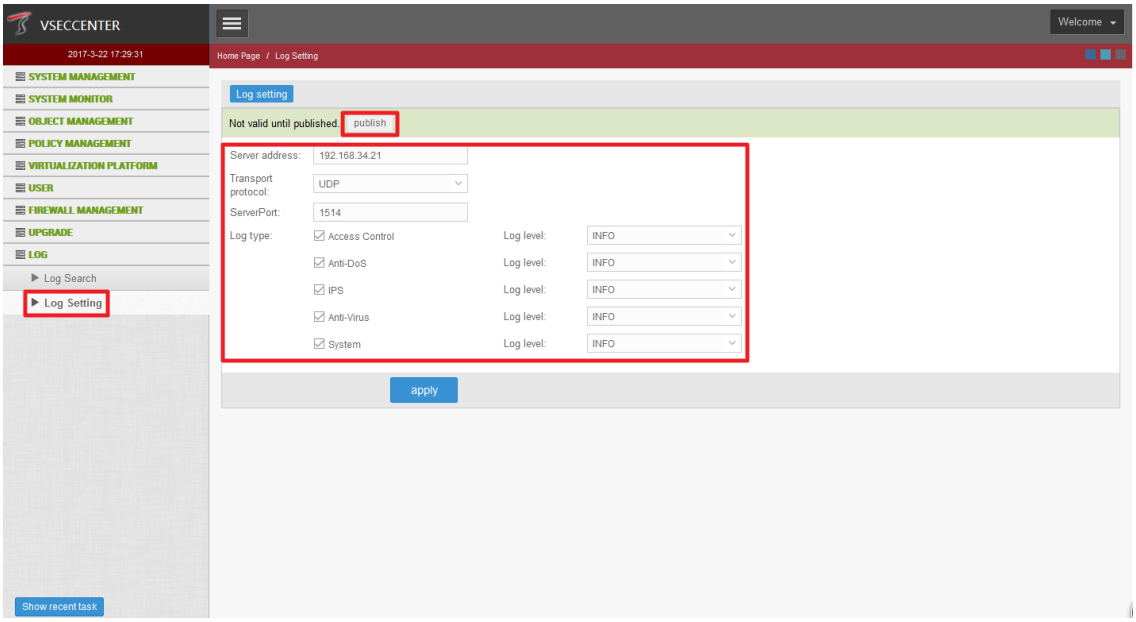

Figure 40

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.

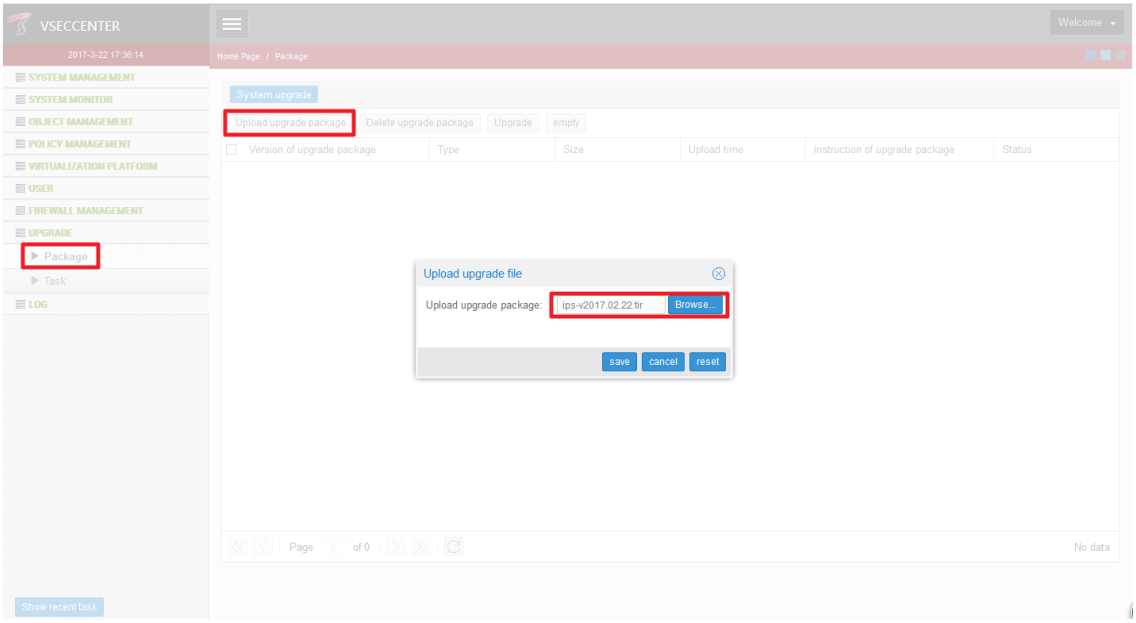

Figure 41

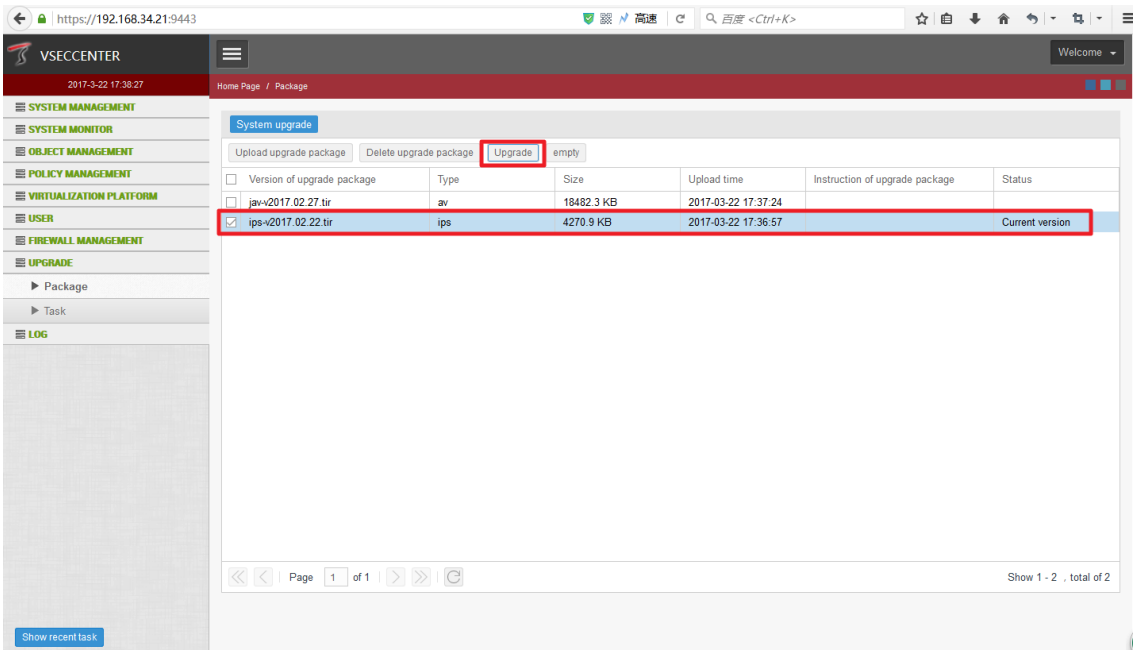

Figure 42

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.

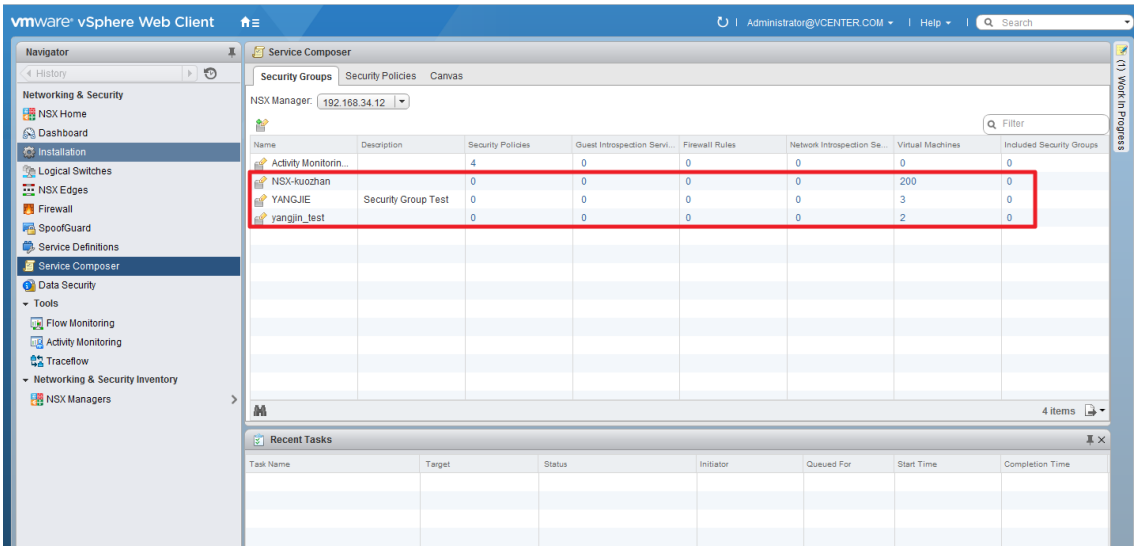

Figure 43

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 Figure 44,45.

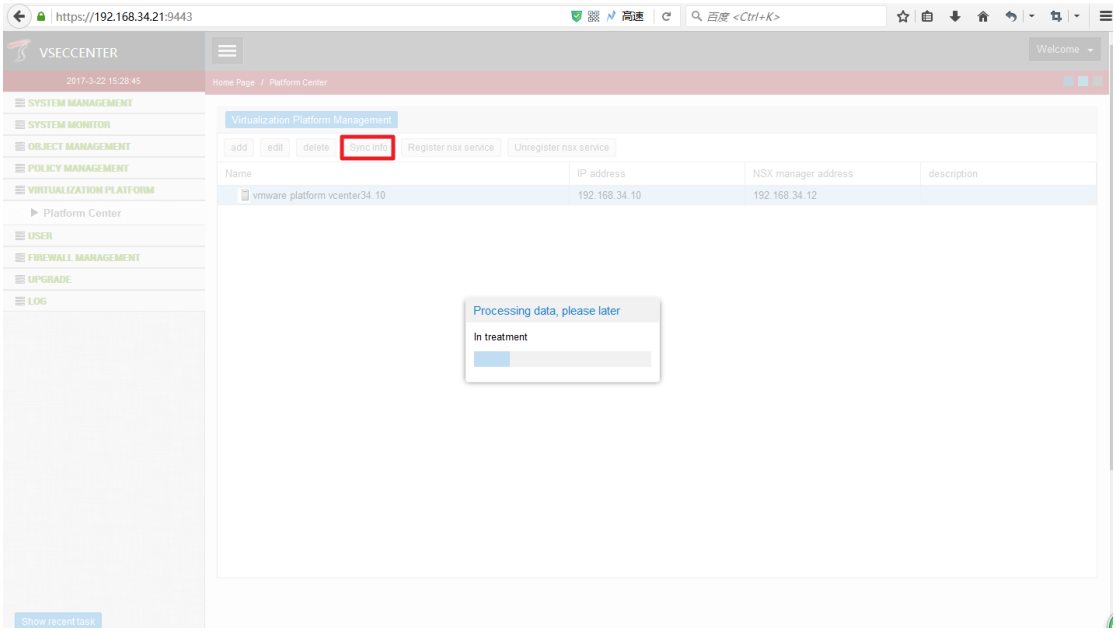

Figure 44

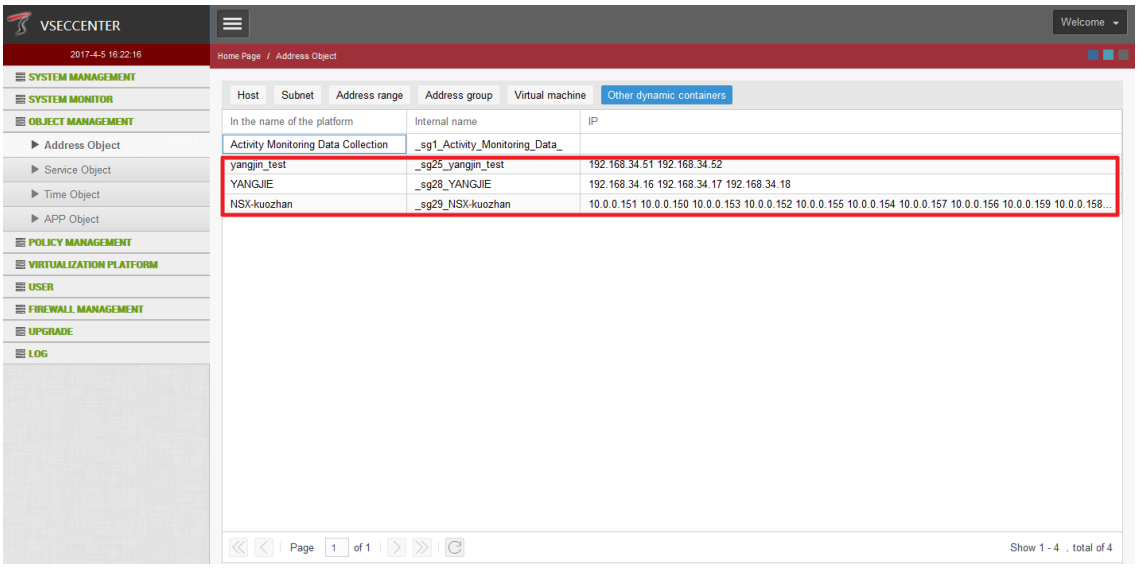

Figure 45

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.

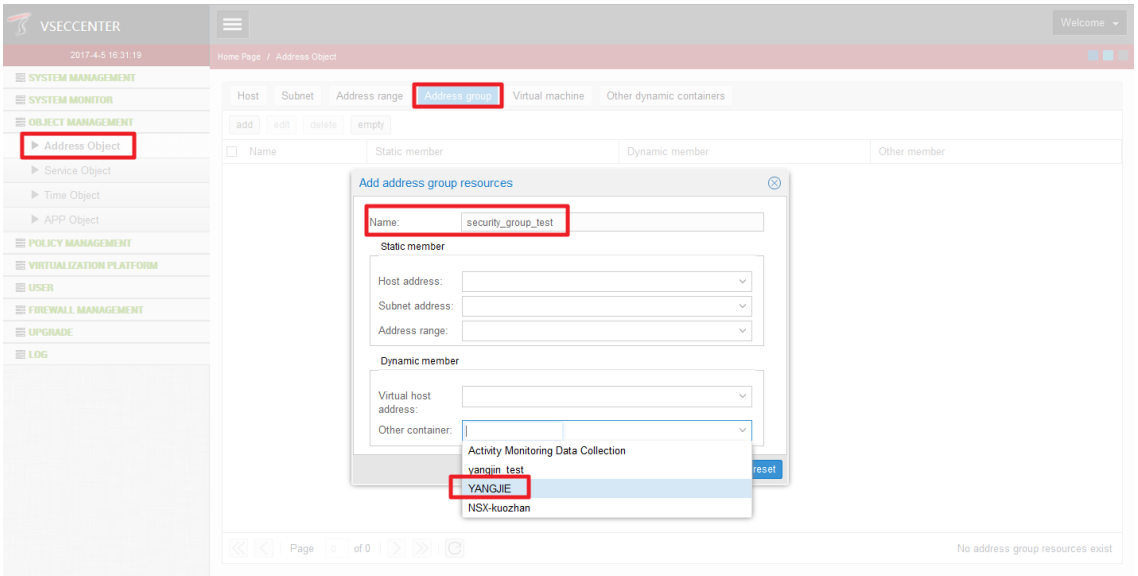

Figure 46

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

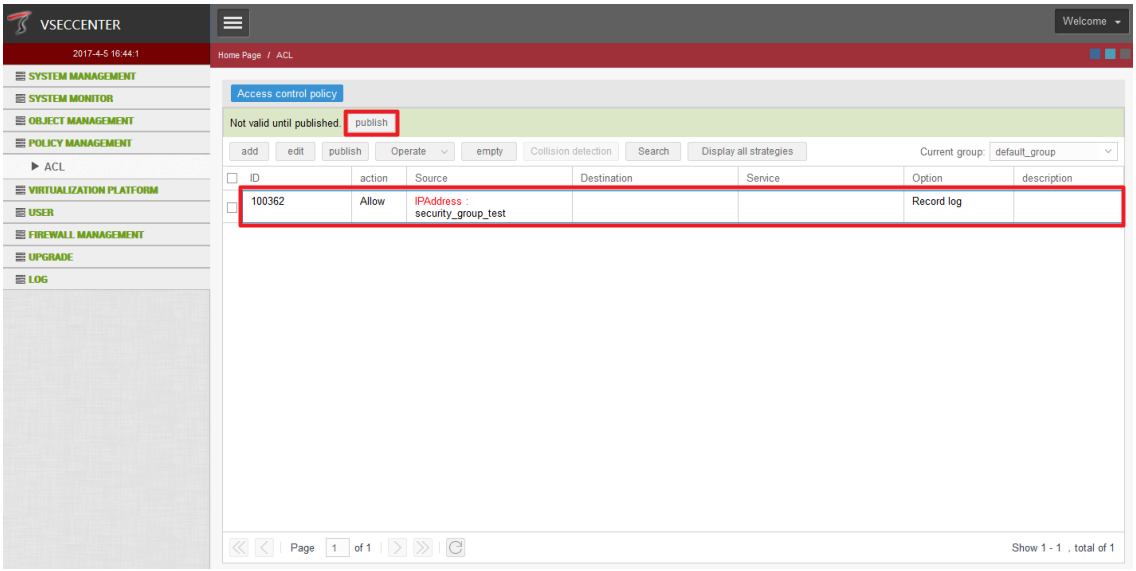

Figure 47

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.

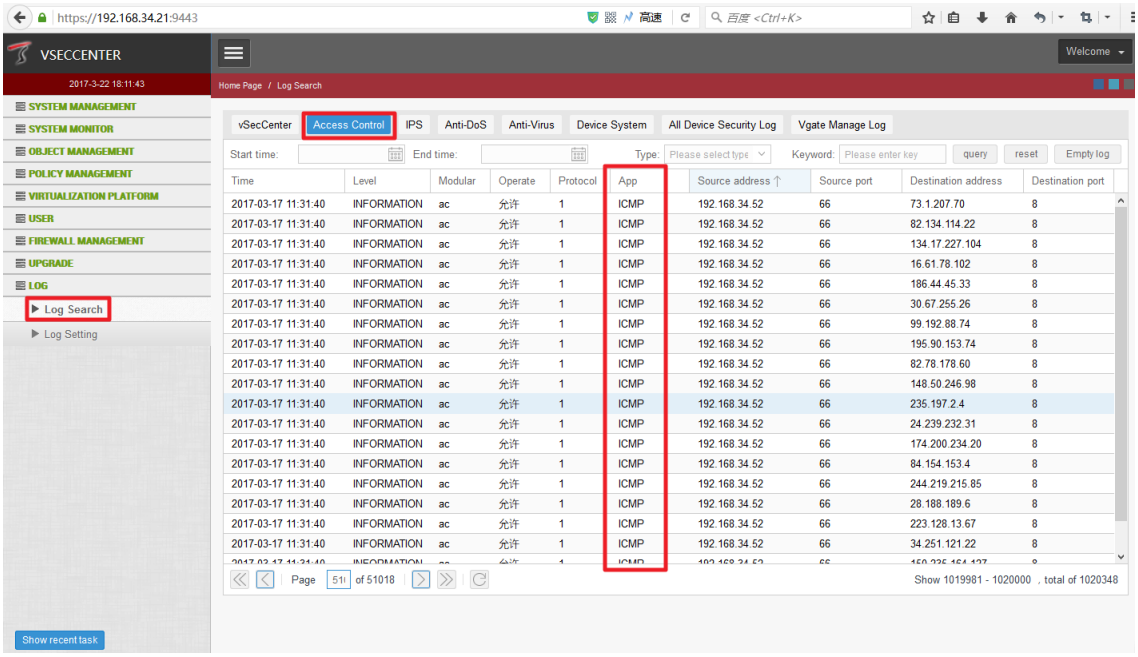

Figure 48

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.

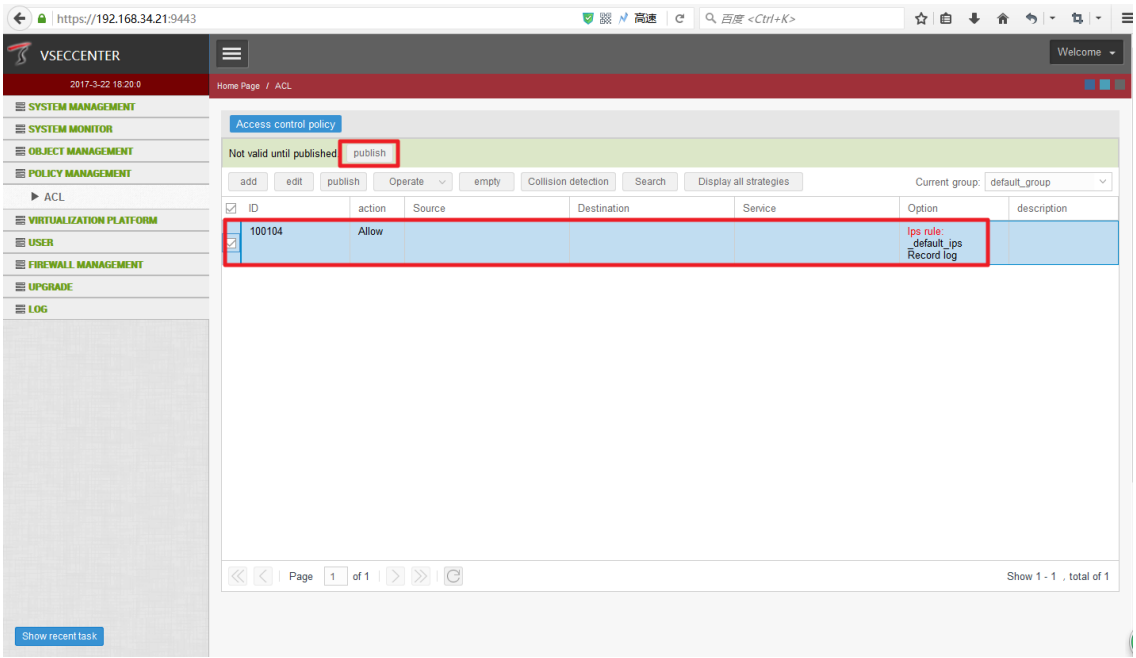

Figure 49

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.

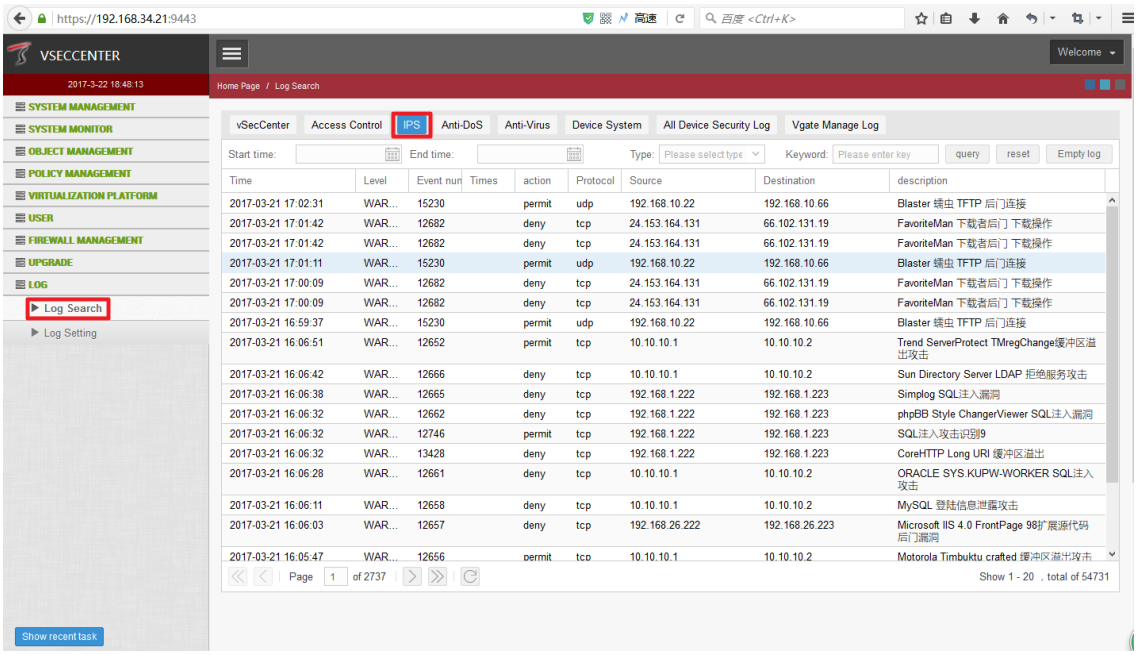

Figure 50

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.

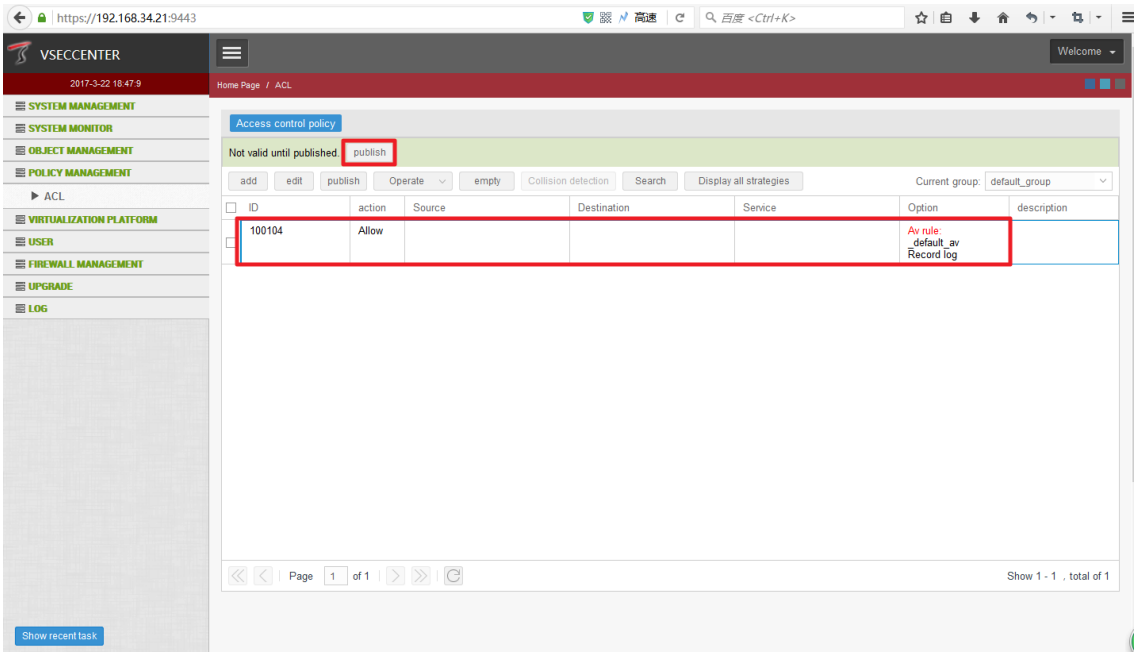

Figure 51

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.

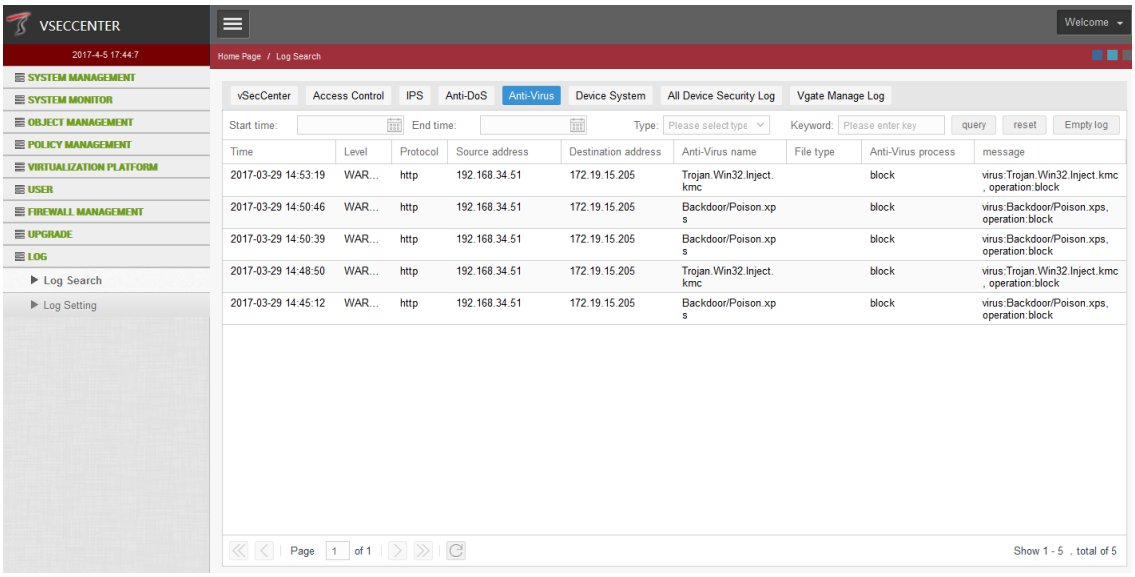

Figure 52