JUNIPER NETWORKS | Engineering Simplicity

Security Director

VMware NSX Integration with Juniper Connected Security

Published
2025-09-18

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

YEAR 2000 NOTICE

END USER LICENSE AGREEMENT

Table of Contents

About this guide

Use this guide to understand how Juniper Networks vSRX Virtual Services Gateway integrates in VMware NSX environment as an advanced security service with Junos Space Security Director as its security manager. Policy Enforcer integrates with the VMware NSX solution to deliver an advanced next-generation firewall feature set that uses vSRX for VMware microsegmentation deployments.

1
PART

VMWare NSX Integration

CHAPTER 1

NSX Managers

IN THIS CHAPTER

About the NSX Managers Page

IN THIS SECTION

To access this page, click Security Director > Devices > NSX Managers.

Use the NSX Managers page to discover the NSX Manager and perform service registration of the vSRX VM with the NSX Manager. The NSX Manager is added as a device in the Security Director and its inventory is synchronized with Security Director.

When you add an NSX Manager in Security Director, the NSX Management RESTful API configures Policy Enforcer as a system log server in NSX Manager. The system log server handler runs in the Policy Enforcer virtual machine. On receiving the security group membership changes from system log, the system log service handler parses the system log and extracts the changed security group details. The security policies with rules having the modified security groups (dynamic address groups) as source or destination addresses are filtered and the perimeter firewall devices assigned to those policies are obtained. A remote procedure call (RPC) is sent to those perimeter firewall devices to update the dynamic address groups. The perimeter firewall devices then obtains and update the IP address feeds from Policy Enforcer.

Before you Begin

1. Install the Policy Enforcer Release OVA image.

   a. After the installation is complete, log in to the Policy Enforcer VM through SSH. Run the service commands to verify the status of the following services:

   ```
   service nsxmicro status
   service  sd_event_listener status
   service nsx_callback_listener status
   service  ssh_listener status
   ```

   b. If services are stopped, initiate the services again by running the following commands:

   ```
   service nsxmicro start
   service  sd_event_listener start
   service nsx_callback_listener start
   service  ssh_listener start
   ```

2. Select **Security Director** > **Administration** > **Policy Enforcer** > **Settings**, and add Policy Enforcer to Security Director. For more information, see Identifying the Policy Enforcer Virtual Machine In Security Director.

3. Download the SSH Key. Copy the vSRX OVA file to the Policy Enforcer VM along with the downloaded SSH key. See Download the SSH Key File.

4. Obtain the vSRX license key before adding the NSX Manager to the Security Director.

Tasks You Can Perform

You can perform the following tasks from this page:

- Download the SSH Key. See Download the SSH Key File.

- Add the NSX Manager. See *Add the NSX Manager*.

- Register security services. See *Registering Security Services*.

- Synchronize the NSX inventory.

Field Descriptions

Table 1 on page 4 provides guidelines on using the fields on the NSX Managers page.

Table 1: Fields on the NSX Managers Page

Field	Description
Hostname/IP Address	Specifies the hostname or the IPv4 address of the NSX Manager.
Name	Specifies the name of the NSX Manager.
Associated vCenter	Specifies the hostname or the IP address of the vCenter associated with the NSX Manager that is automatically fetched by Security Director.
Associated vCenter Status	Specifies the connection status of an associated vCenter.
Service Manager Registration Status	Specifies the registration status of the security services.
Services	Specifies the service definition of a selected NSX Manager. Click **View** to view the service definition.
Port	Specifies the port number of the NSX Manager.

Table 1: Fields on the NSX Managers Page *(Continued)*

Field	Description
Username	Specifies the username of the NSX Manager. The user must have the administrator privileges to access the NSX Manager.
Connection Status	Specifies the connection status of the NSX Manager.

About the Security Groups Page

IN THIS SECTION

- Tasks You Can Perform | **5**
- Field Descriptions | **6**

To access this page, select Security Director > Monitor > NSX Inventory > Security Groups.

Use the Security Groups page to view a list of security groups obtained from NSX and the corresponding dynamic address groups created by Security Director.

The security groups updates are automatically synchronized by Security Director.

Tasks You Can Perform

You can perform the following task from this page:

- View members of the security group.

Field Descriptions

provides guidelines on using the fields on the Security Groups page.

Table 2: Fields on the Security Groups Page

Field	Description
NSX Manager	Specifies the name of the NSX Manager from which the corresponding security group is obtained.
Name	Specifies the name of the security group.
Members	Click **View** to view the list of VMs belonging to a security group. If the vCenter is associated with the NSX Manager, the members list shows the VM names with IPv4 and IPv6 addresses.
DAG Name	Specifies the name of a dynamic address group created for each security group. The dynamic address group name is created in the format *<NSX Manager name>-<security group name>*.
Definition	Specifies the definition of a security group.

RELATED DOCUMENTATION

About the NSX Managers Page

About the vCenter Servers Page

IN THIS SECTION

To access this page, select Security Director > Devices > vCenter Servers.

VMWare NSX Manager is always associated to a vCenter Server. Based on the NSX Manager discovered by Security Director, the NSX service automatically fetches the associated vCenter server hostname. The NSX service uses the specific vCenter credentials provided by the user at the time of adding the NSX Manager, to connect to vCenter and obtain any required inventory from it.

Use the vCenter Servers page to view details of an associated vCenter Server.

Tasks You Can Perform

You can perform the following task from this page:

- Synchronize any changes to the inventory objects in vCenter with the vCenter database.

Field Descriptions

Table 3 on page 7 provides guidelines on using the fields on the vCenter Servers page.

Table 3: Fields on the vCenter Servers Page

Field	Description
Host Name	Specifies the hostname of the associated vCenter Server.
Port	Specifies the port number of the vCenter server.
Connection Status	Specifies the connection status of NSX Manager and associated vCenter server.

RELATED DOCUMENTATION

About the NSX Managers Page

Add the NSX Manager

Registering Security Services

About the Virtual Machines Page

To access this page, select Security Director > Monitor > vCenter Server Inventory > Virtual Machines.

Use the Virtual Machines page to view the complete list of VMs that are dynamically fetched by the associated vCenter.

Tasks You Can Perform

You can perform the following tasks from this page:

- View security groups associated with each VM.

- View a list of vNICs for each VM and the network that each of vNIC is linked to.

Field Descriptions

Table 4 on page 8 provides guidelines on using the fields on the Virtual Machines page.

Table 4: Fields on the Virtual Machines Page

Field	Description
VM Name	Specifies the name of the VM.
vCenter	Specifies the vCenter details.
OS on VM	Specifies the operating system on each VM. For example: Red Hat, CentOS, and so on.
Security Groups	Click **View** to view a list of security groups associated with each VM.

Table 4: Fields on the Virtual Machines Page *(Continued)*

Field	Description
Network Details	Click **View** to view a list of vNICs for each VM with their corresponding IPv4 and IPv6 addresses.
State	Specifies whether the VM is switched on or off.
Status	Specifies whether the VM is connected to the ESXi host or not.

RELATED DOCUMENTATION

About the NSX Managers Page

Before You Deploy vSRX in VMware NSX Environment

Before you begin deploying the vSRX Virtual Services Gateway as an advanced security service in VMware NSX:

- Download the **.ovf** file of the vSRX software image from Juniper Networks website and save it to the Policy Enforcer. The vSRX OVF URL automatically appears in the Register Security Service page of the Security Director when you register the vSRX virtual machine (VM) as a Juniper security service on the NSX Manager.

- Obtain the Juniper SDSN for NSX license key (see *Juniper Connected Security for VMware NSX Licensing*).

- Install two or more VMware ESXi hosts. See the VMware documentation for details.

- Install the VMware vCenter Server on a Windows VM or physical server, or deploy the VMware vCenter Server Appliance. Connect to the vCenter Server from the vSphere Web Client. See the VMware documentation for details.

- Create a vSphere distributed switch (VDS) in the vSphere environment, add each ESXi host to a common VDS, and then configure the ESXi hosts in a vSphere cluster. For each host cluster that will participate in NSX, all hosts within the cluster must be attached to a common VDS. See the VMware documentation for details.

- Deploy VMs on each ESXi host by using the vSphere Web Client. See the VMware documentation for details.

- Install the VMware NSX Manager in your vCenter Server environment by using the vSphere Web Client. The NSX Manager is the centralized network management component of NSX, and is installed as a virtual appliance on any ESXi host in your vCenter Server environment. It provides an aggregated system view. See the VMware documentation for details.

> **NOTE**: Ensure that NSX Manager is configured in single vCenter Mode and not in multiple vCenter mode. See the VMware documentation for details.

> **NOTE**: Juniper Networks devices require a license to activate the feature. To understand more about VMWare NSX Licensing, see, Licenses for Network Management. Please refer to the Licensing Guide for general information about License Management.

Table 5 on page 10 lists the system software requirement specifications for the components of a vSRX, Security Director, and VMware NSX integration.

Table 5: System Software Specifications for vSRX in VMware NSX Environment

Component	Specification
VMware ESXi Server	6.0 Update 3 or later
VMware vCenter Server	6.3.1 or later
VMware NSX for vSphere	6.3.1 or later **NOTE**: For sites that are running vSphere 6.5, vSphere 6.5a is the minimum supported version with NSX for vSphere 6.3.0.
VMware NSX Manager	6.3.1 or later
Linux Kernel	3.10.x or later
Junos Space Security Director	17.1 or later

Table 5: System Software Specifications for vSRX in VMware NSX Environment *(Continued)*

Component	Specification
Junos Space Policy Enforcer	17.1 or later
vSRX	Junos OS Release vSRX 15.1X49-D101 or later
Memory	4 GB
Disk space	16 GB (IDE or SCSI drives)
vCPUs	2 vCPUs
vNICs	A single vNIC for management traffic. Network traffic is forwarded to the vSRX over a Virtual Machine Communication Interface (VMCI) communication channel by the ESXi hypervisor. **NOTE**: VMCI is not a network interface (NIC) but a VMWare-proprietary device for Host to Guest Communication.

RELATED DOCUMENTATION

vSphere Installation and Setup

Understanding Juniper Connected Security for VMware NSX Integration

IN THIS SECTION

This section presents an overview of how Juniper Networks vSRX Virtual Services Gateway integrates in the VMware NSX environment as an advanced security service with Junos Space Security Director as its security manager.

VMware NSX Overview

VMware NSX is VMware's network virtualization platform for the software-defined data center (SDDC). Similar in concept to server virtualization, network virtualization decouples network functions from physical devices. With VMware NSX, existing networks are immediately ready to deploy a software-defined data center. This enables data center operators to create, provision, and manage their networks with greater agility and operational efficiency. VMware NSX is completely managed by the VMware vCenter Server through the VMware vSphere Web Client.

The VMware NSX network virtualization platform is security orientated. The NSX Distributed Firewall (DFW) on all ESXi hosts to provide a set of kernel-based Layer 2 (L2) through Layer 4 (L4) stateful firewall features inside the ESXi hypervisor to deliver segmentation within each virtual network. Every virtual machine (VM) running in a VMware NSX environment can be protected with a full stateful firewall at a granular level. DFW operates at the vNIC of each individual VM.

VMware NSX, however, does not provide advanced L4 through L7 security services which are critical to provide complete protection in a SDDC environment. Environments that require advanced, application-level network security capabilities can leverage VMware NSX to distribute, enable, and enforce advanced network security services in a virtualized network context.

You can add the vSRX Virtual Services Gateway as a partner security service in the VMware NSX environment. The vSRX security service is managed by the Junos Space Security Director and VMware NSX Manager to deliver a complete and integrated virtual security solution for your SDDC environment. The vSRX provides advanced security services, including intrusion detection and prevention (IDP), and application control and visibility services through AppSecure.

DFW implements a stateful *traffic steering* mechanism that identifies what traffic should be sent to the vSRX VM. The protected VMs and the security service vSRX VM run on the same physical ESXi host.

vSRX Integration with NSX Manager and Junos Space Security Director

To deploy the advanced security features of the vSRX Virtual Services Gateway in the VMware NSX environment, the Junos Space Security Director, vSRX, and NSX Manager operate together as a joint solution to fully automate the provisioning and deployment of the vSRX to protect applications and data from advanced cyberattacks.

Integration of the vSRX VM in the VMware NSX environment involves use with the following management software:

- Junos Space Security Director—The centralized security management platform responsible for service registration and configuration of each vSRX instance. The Security Director provides you with the

ability to manage a distributed network of virtualized and physical firewalls from a single location. The Security Director functions as the management interface between the NSX Manager and the vSRX Services Gateway. Security Director manages the firewall policies on all vSRX instances.

- NSX Manager—The centralized network management component of VMware NSX. The NSX Manager provides integration with the VMware vCenter Server, which enables you to manage the VMware NSX environment through VMware vCenter. All VMware NSX operations and configuration is done through VMware vCenter, which communicates with the NSX Manager through Representational State Transfer (REST) APIs to delegate tasks to the responsible owner. The NSX Manager is always associated with a VMware vCenter Server.

The NSX Manager is added as a registered device in the Security Director and communication is bidirectionally synchronized by the Junos Space Policy Enforcer between the two management platforms. All shared objects (such as security groups) are synchronized between the NSX Manager and Security Director. This includes the IP addresses of all VMs in ESXi hosts, including the vSRX agent VMs. The Security Director creates an address group for each security group synchronized from the NSX Manager, along with the addresses of each member of the security group. The security groups discovered from the NSX Manager are mapped to dynamic address groups (DAG) in the Security Director. The Policy Enforcer retains the mapping of all IP addresses between security groups and dynamic address groups.

The vSRX Services Gateway is deployed as a partner service appliance in the VMware NSX environment. vSRX agent VMs are deployed for each ESXi host in a cluster. You use security policies to direct all VM traffic in an ESXi host through the vSRX VM (the Juniper security service) for L4 through L7 advanced security analysis.

High-Level Workflow

provides a high-level workflow of how the NSX Manager, Security Director, and vSRX interact to deploy vSRX as a security service in the VMware NSX environment.

Figure 1: vSRX, Security Director, and VMware NSX Integration Workflow
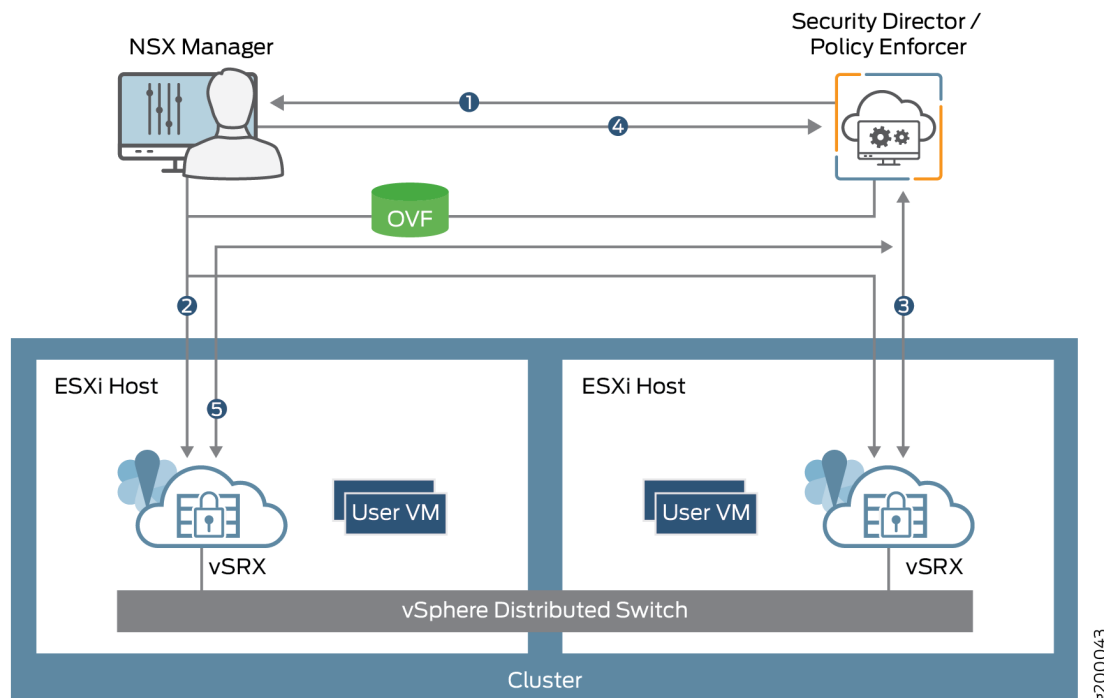
1. The Junos Space Security Director initiates communication with the NSX Manager. The Security Director discovers, registers, and adds the NSX Manager as a device in its database. The Security Director also deploys the vSRX instance from the **.ovf** file and registers it as a security service. The NSX Manager and its inventory of shared objects (for example, security groups) and addresses are then synchronized with the Security Director. The registration process uses the Policy Enforcer to enable bidirectional communication between the Security Director and the NSX Manager.

2. The NSX Manager deploys the registered vSRX instance as a Juniper security service for each ESXi host in a vSphere cluster. The deployment is based on the vSRX **.ovf** file. Whenever an ESXi host is added to a vSphere cluster, NSX Manager creates a vSRX agent VM in the new ESXi host. The same process occurs if an ESXi host is removed from a vSphere cluster.

3. After the vSRX agent VM is provisioned as a security service on each ESXi host in a vSphere cluster, NSX Manager notifies Security Director by using REST API callbacks. The Security Director pushes the initial boot configurations and Junos OS configuration policies to each vSRX agent VM to support the NSX security group. The Security Director is aware of the NSX security groups and corresponding address groups, and all deployed vSRX agent VMs are automatically discovered (one per ESXi host).

   Security policies redirect relevant network traffic originating from the VMs in a specific security group in the ESXi hosts in a vSphere cluster to the Juniper security service vSRX agent VM in each ESXi host for further analysis.

4. The vCenter Server and the NSX Manager continue to send real-time updates on changes in the virtual environment to Security Director.

5. The Security Director dynamically synchronizes the object database to all vSRX agent VMs deployed in ESXi clusters. Security groups discovered from NSX Manager are mapped to a dynamic address group (DAG) in Security Director. The Security Director manages the firewall policies on the vSRX agent VMs. Using the Security Director, you create advanced security service policies (for example, an application firewall policy or an IPS policy) and push those policies to each vSRX agent VM in an ESXi host.

RELATED DOCUMENTATION

NSX

VMware NSX Data Sheet

Junos Space Security Director

vSRX

Add the NSX Manager

Use the Add NSX Manager page to add the NSX Manager in to the Security Director database. Based on the NSX details provided, the Security Director automatically fetches the associated VMware vCenter Server hostname from NSX.

To add a NSX Manager:

1. Select **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Click the add icon (+).

   The Add NSX Manager page appears.

3. Complete the configuration by using the guidelines in Table 6 on page 16.

4. Click **Finish** to complete the configuration.

   After adding the NSX Manager, you must register the vSRX VM as a Juniper security service with the NSX Manager. See *Registering Security Services*.

Table 6: Fields on the Add NSX Manager Page

Field	Description
Name	Enter the name of the NSX manager.
Host	Enter the IPv4 address of the NSX manager.
Port	Enter the port number of the NSX Manager. The NSX Manager and Security Director use SSL to communicate on TCP port 443.
Username	Enter the username of the NSX Manager to allow Security Director to authenticate the communication.
Password	Enter the password of the NSX Manager to allow Security Director to authenticate the communication.
Description	Enter a description about the NSX Manager; you can use a maximum of 255 characters.
SSL Certificate	View the SSL certificate required to authenticate the NSX Manager.
Accept SSL Certificate	Select this option to accept the SSL certificate. This is a mandatory field.
Type	Select an option: NSX-V or NSX-T. VMware NSX-T is the latest generation of VMware's network virtualization product series. NSX-T is the successor to NSX-V. NSX-T supports third-party Hypervisors and next generation overlay encapsulation protocols such as Generic Network Virtualization Encapsulation (Geneve).

Table 6: Fields on the Add NSX Manager Page *(Continued)*

Field	Description
Firewall Type	Select the type of perimeter firewall for your datacenter. • East-West Firewall—vSRX is spawned in each ESX server of VMware NSX for the east-west traffic. This provides east-west security for members of the security groups within a datacenter. • North-South Firewall—Perimeter firewall for the north-south traffic. This provides a consistent north-south security for members of the security groups, if the members move across datacenters. You can select both the types or any one of the firewall types. **NOTE**: Firewall Type is applicable only if you select the Type as NSX-V.

Service Manager Registration

Field	Description
SD Username	Enter the username of Security Director to allow the NSX Manager to authenticate its communication with Security Director.
SD Password	Enter the password of Security Director to allow the NSX Manager to authenticate its communication with Security Director.
License Key	Enter the license key of vSRX VM.

Associated vCenter - vCenter Server

Field	Description
	To add multiple vCenter servers: Click the + icon. The Associate vCenter page is displayed.
Host	Enter the IPv4 address of the VMware vCenter Server.
Port	Enter the port number of the VMware vCenter Server. Default: 443

Table 6: Fields on the Add NSX Manager Page *(Continued)*

Field	Description
Username	Enter the username of the VMware vCenter Server. Security Director uses these credentials to discover the vCenter server and fetch the VM inventory details.
Password	Enter the password of the VMware vCenter Server. Security Director uses these credentials to discover the vCenter Server and fetch the VM inventory details.
SSL Certificate	View the SSL certificate required to authenticate the vCenter Server.
Accept SSL Certificate	Select this option to accept the SSL certificate. This is a mandatory field.

RELATED DOCUMENTATION

About the NSX Managers Page

Deleting the NSX Manager

Before You Begin

Before you delete the NSX Manager, perform the following steps:

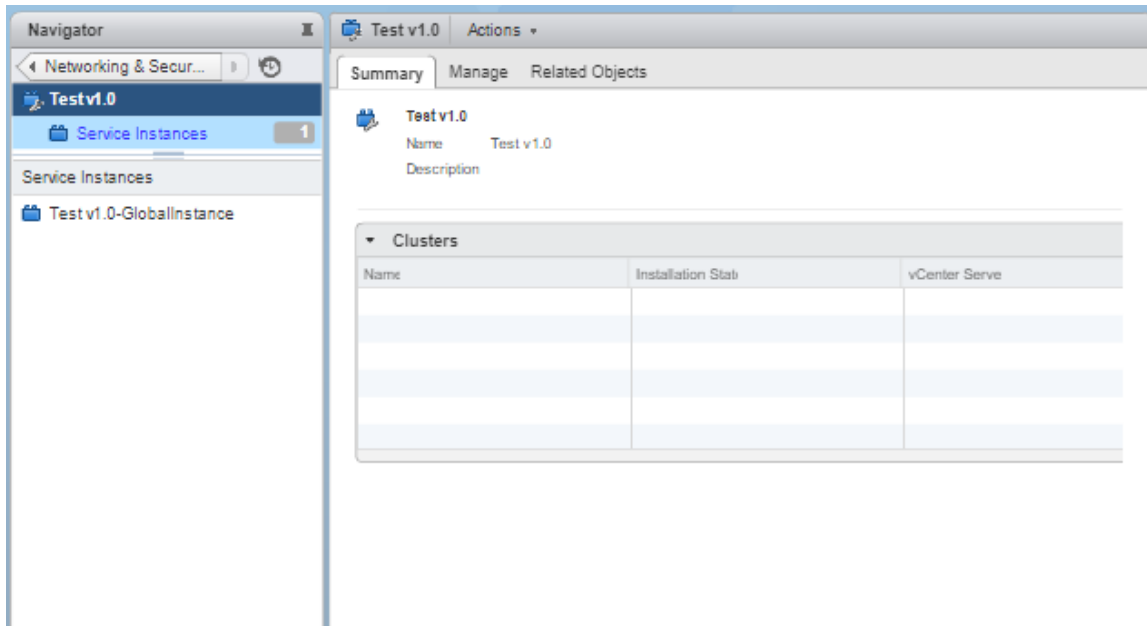1. Unbind all bindings of network object from a service profile in VMWare vCenter Server.

   - Log in to the vSphere Web Client through the VMware vCenter Server.

   - Select **Networking & Security** > **Service Definitions**.

     The Service Definitions page appears.

   - Double-click on the Juniper service.

     The respective service page appears, as shown in .

Figure 2: Service Instances Page

- In the left pane, click on the global instance > Service Profiles > Juniper Vendor Template.

  The Juniper Networks Template page for the selected service appears.

- Select the template and from the Actions list, select **Apply to Objects**.

  The Apply to Network Objects page appears.

- Remove the object associated with a service profile by moving the object listed under Selected Objects column to Available Objects column.

2. Delete the redirect policy in VMWare vCenter Server.

   - Select **Networking & Security** > **Service Composer**.

     The Service Composer page appears.

   - In the Security Policies tab, right-click the security policy and select **Delete**.

     The security policy along with corresponding firewall rules are deleted.

3. Delete the deployed services in VMWare vCenter Server.

   - Select **Networking & Security** > **Installation**.

     The Installation page appears.

   - In the Service Deployments tab, right-click on the service name and select **Delete**.

The deployed service is deleted.

4. Deregister the service definition in VMWare vCenter Server.

- Select **Networking & Security** > **Service Definitions**.

  The Service Definitions page appears.

- Double-click on the Juniper service.

  The respective service page appears.

- In the left pane, click on the global instance > Service Profiles > Juniper Vendor Template.

  The Juniper Networks Template page for the selected service appears.

- In the Related Object tab, right-click on the template and click **Delete**.

- Select **Service Definitions** in the left pane.

  The Service Definitions page appears.

- In the Service tab, right-click on the service and click **Delete**.

  The Remove service definition pop-up message appears to confirm the delete operation. Enable the Delete service manager option and click **Yes**.

Use the Delete NSX Manager option to delete the NSX Manager from the Security Director inventory. Along with NSX Manager, the associated vCenter server is also deleted.

To delete the NSX Manager:

1. Select **Devices** > **NSX Managers**.

   The NSX Manager page appears.

2. Select the NSX Manager that you want to delete.

3. From the More list, or right-click menu, select **Delete NSX Manager**.

   A confirmation message appears to confirm the deletion.

   > ⓘ **NOTE**: You cannot delete NSX Manager if the security service is already deployed in NSX.

4. Click **Yes** to confirm the deletion.

   The NSX Manager and its associated vCenter server are deleted from the Security Director inventory.

> **NOTE**: You cannot delete a NSX Manager if there is a NSX Secure Fabric. You must first delete the Secure Fabric. See *Editing or Deleting a Secure Fabric*.

RELATED DOCUMENTATION

Understanding Juniper Connected Security for VMware NSX Integration **| 11**

Before You Deploy vSRX in VMware NSX Environment **| 9**

Download the SSH Key File

About the NSX Managers Page

Add the NSX Manager

Registering Security Services

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment **| 27**

View Network Details of a Virtual Machine

Use the View Network Details page to view the network details of a virtual machine(VM) such as name of the virtual Network Interface Card (NIC) or the network adapter and the IPv4 and IPv6 addresses of each NIC.

To view the network details:

1. Select **Monitor** > **vCenter Server Inventory** > **Virtual Machines**.

   The Virtual Machines page appears.

2. In the Network Details column, click **View**.

   The View Network Details page appears. Table 7 on page 21 provides the guidelines on using the fields on this page.

Table 7: Fields on the View Networks Details Page

Field	Description
Virtual Machine	Specifies the IP address of the VM.
vNIC	Specifies the name of a vNIC or network adapter.

Table 7: Fields on the View Networks Details Page *(Continued)*

Field	Description
IPv4	Specifies the IPv4 address of a vNIC.
IPv6	Specifies the IPv6 address of a vNIC.

RELATED DOCUMENTATION

About the NSX Managers Page

Registering Security Services

Use the Register Security Service page in Security Director to register a Juniper security service on a specific NSX Manager. After registering the security service from Security Director, log in to the vCenter server and deploy the service from NSX.

To register the Juniper security service:

1. Select **Devices** > **NSX Managers**.

   The NSX Managers page appears.
2. Select the NSX Manager for which service needs to be registered.
3. From the More list or right-click menu, select **Register Security Service**.

   The Register Security Service page appears.
4. Complete the configuration by using the guidelines in .
5. Click **Register** to complete the registration.

   A confirmation message appears to indicate if registration is successful or not.

Table 8: Fields on the Register Security Service Page

Field	Description
Service Name	Enter the name for the Juniper Security Service.

Table 8: Fields on the Register Security Service Page *(Continued)*

Field	Description
vSRX OVF URL	The vSRX OVF image that you have copied to the Policy Enforcer VM is listed here. Select the vSRX OVF image from the list.
vSRX Root Password	Enter the root password of the vSRX instance. The same root password is set for all the vSRX VMs deployed in NSX.
Confirm Password	Enter the root password of the vSRX instance for confirmation.
Firewall Type	Select East-West or North-South from the list. The default firewall type is East-West. East-West—vSRX is spawned in each ESX server of VMware NSX-T for the east-west traffic. This provides east-west security for members of the security groups within a datacenter. North-South—It is the perimeter firewall for the north-south traffic. This provides a consistent north-south security for members of the security groups, if the members move across datacenters. **NOTE**: The Firewall Type field is applicable only if the NSX Manager type is NSX-T.

RELATED DOCUMENTATION

About the NSX Managers Page

Delete NSX Manager Services

You can delete NSX Manager services from Security Director. Before deleting a service, you must ensure that the service is not deployed in NSX through the vCenter plugin. If the service that you are trying to delete is already deployed in vCenter, you will see an error message. To delete the registered security service, you must first delete the vSRX Virtual Firewall virtual machines.

To delete a NSX Manager service from Security Director:

1. Select **Security Director**>**Devices**>**NSX Managers**.

   The NSX Managers page appears.

2. Select the NSX Manager for which you want to delete the service definition, and in the Services column click **View**.

   The Services Definition page appears listing the registered security services.

3. Select the service that you want to delete, right click and select **Delete Service**.

   If the selected service is already deployed in NSX, an error message is shown to delete the running vSRX Virtual Firewall virtual machines to delete the registered security service.

   To delete the vSRX Virtual Firewall virtual machines from the VMware vCenter Server:

   a. Log in to the vSphere Web Client through the VMware vCenter Server.

   b. Select **Networking & Security**>**Installation and Upgrade**>**Service Deployment**.

   c. Select the service and click **DELETE**.

      The vSRX Virtual Firewall virtual machines are deleted.

   d. Go to **Security Director** and repeat the procedure from Step 1.

4. If the selected service is not deployed in NSX, Security Director deletes the service successfully.

RELATED DOCUMENTATION

About the NSX Managers Page

VMware vSphere Documentation

View Members of a Security Group

Use the View Members page to view the list of VMs belonging to a security group.

To view the list of virtual machines:

1. Select **Monitor** > **NSX Inventory** > **Security Groups**.

   The Security Groups page appears.

2. In the Members column, click **View**.

   The View Members page appears. describes the fields on this page.

Table 9: Fields on the View Members Page

Field	Description
Security Group	Specifies the name of the security group.
VM Name	Specifies the name of the VM that belongs to the security group.
IP Address	Specifies the IPv4 address of the VM.
IPv6 Address	Specifies the IPv6 address of the VM.

About the NSX Managers Page

Downloading the SSH Key File

You must copy the vSRX OVA image to the Policy Enforcer virtual machine (VM) before adding the NSX Manager.

Use the Upload Image page to download the SSH key file and copy the vSRX OVA file to the Policy Enforcer VM by using the SFTP command with the downloaded SSH key. You must perform this as a first step before adding the NSX Manager.

To download the SSH key:

1. Select **Security Director** > **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Click **Download SSH Key**.

   The Download SSH Key page appears.

3. Click **Download SSH Key**.

   The SSH key is downloaded and saved in your local drive.

Copying vSRX OVA Image File to Policy Enforcer from Linux Machines

To copy the vSRX OVA file to a Policy Enforcer VM from a Linux machine:

1. Copy the downloaded SSH key file to the same directory where the vSRX OVA image file is saved.

2. Navigate to the directory path where vSRX OVA and SSH key files are located.

3. Run the `chmod 600 <<SSHKEYFILE>>` command to change the permission of the SSH key file.

4. Run the following commands:

   - `sftp -o "IdentityFile=<<SSHKEYFILE>>" nsxmicro@<<pe_ipaddress>>`

   - `cd publish`

   - `put <<VSRX OVA FILE>>`

     The vSRX OVA file will be copied to the Policy Enforcer VM after sometime.

5. After the vSRX OVA file is copied, you can add the NSX Manager and register its services in the Security Director.

Copying vSRX OVA Image File to Policy Enforcer from MAC Machines

To copy the vSRX OVA file to a Policy Enforcer VM from a MAC machine:

1. Copy the downloaded SSH key file to the same directory where the vSRX OVA image file is saved.

2. Navigate to the directory path where vSRX OVA and SSH key files are located.

3. Run the `chmod 600 <<SSHKEYFILE>>` command to change the permission of the SSH key file.

4. Run the following commands:

   - `sftp -i sshkey nsxmicro@<pe_ip>`

   - `cd publish`

   - `put *<<VSRX OVA FILE>>`

     The vSRX OVA file will be copied to the Policy Enforcer VM after sometime.

5. After the vSRX OVA file is copied, you can add the NSX Manager and register its services in the Security Director.

RELATED DOCUMENTATION

About the NSX Managers Page

View Security Groups of a Virtual Machine

Use the Security Groups page to view the list of security groups assigned to a virtual machine (VM).

To view the list of security groups:

1. Select **Monitor** > **vCenter Server Inventory** > **Virtual Machines**.

   The Virtual Machines page appears.
2. In the Security Groups column, click **View**.

   The Security Groups page appears. describes fields on this page.

Table 10: Fields on the Security Groups Page

Field	Description
Virtual Machine	Specifies the IP address of the VM.
Security Group	Specifies the name of the security group to which a VM belongs.

RELATED DOCUMENTATION

About the NSX Managers Page

Deploying the vSRX as an Advanced Security Service in a VMware NSX Environment

IN THIS SECTION

Use the following procedures to deploy the vSRX as an advanced security service virtual machine (VM) in the VMware NSX environment. The vSRX VM is deployed in conjunction with Juniper Networks Junos Space Security Director and VMware NSX Manager. In each procedure you are instructed whether to perform the steps in the NSX Manager (from the VMware vCenter Server) or in the vSphere cluster. For example, you create the security group using the NSX Manager, but the discovery of devices happens in the vSphere cluster.

The deployment steps are performed in the following sequence :

Creating a Security Group (VMware vCenter Server)

You create a security group by using the NSX Manager from the VMware vCenter Server. Each security group is a logical collection of objects from your vSphere inventory. These objects include VMs that you want to be members in the same security group and to which you will apply the vSRX as a Juniper security service. You can apply an advanced security service policy to all the objects contained in a security group.

To create a security group from the VMware vCenter Server:

1. Log in to the vSphere Web Client through the VMware vCenter Server.
2. From the vSphere Web Client, click **Hosts and Clusters** to view hosts and clusters in the vSphere Web Client inventory. From the Summary tab, you can verify the vSphere cluster and the VMs associated as part of this cluster. All VMs are part of the VXLAN network and can communicate over this VLAN.
3. From the vSphere Web Client, click **Networking & Security** and then click **Service Composer**. The Service Composer appears. From the Service Composer, click the **Security Groups** tab.
4. Click the **Add Security Group** icon to create a new security group that contains the specific VMs you want as members of the same group, as shown in .

Figure 3: Create a New Security Group Page

5. Type a name and description for the security group and then click **Next**.

6. On the Define dynamic membership page, define the criteria that an object must meet for it to be added to the security group you are creating. You can define a dynamic group membership criteria for the VMs that are to be part of each security group. For example, VM membership in a security group can be tagged by name. You define the exact membership criteria that you want to use to group VMs. Group membership is associated dynamically at runtime.

   Click **Next**.

7. On the Select objects to include page, select the tab for the resources you want to include in this security group. Click **Next**.

8. On the Select objects to exclude page, select the tab for the resources you want to exclude from this security group. Click **Next**.

9. Click **Finish** to complete creating the security group.

Discovering the NSX Manager and Registering vSRX as a Security Service in vSphere cluster

You use the Junos Space vSphere cluster to discover the NSX Manager and perform service registration of the vSRX VM with the NSX Manager. The NSX Manager is added as a device in the Security Director, and its inventory is synchronized with the Security Director.

> **NOTE**: Ensure that SNMP is disabled in the Security Director while performing device discovery for the vSRX agent VM. If SNMP is enabled in Security Director, the vSRX agent VM discovery operation fails.

To discover the NSX Manager from the Security Director:

1. Select **Security Director** > **Devices** > **NSX Managers**.

   The NSX Managers page appears.

2. Click the **Add icon (+)** to add the NSX Manager to the Security Director.

   The Add NSX Manager page appears, as shown in Figure 4 on page 30.

Figure 4: Add NSX Manager Page

3. In the NSX Manager section, enter the following information:

   - Name—Enter the name of the NSX Manager.

   - Host—Enter the IP address of the NSX Manager.

   - Port—Enter the port number of the NSX Manager. The NSX Manager and Security Director use SSL to communicate on TCP port 443.

- Username, Password—Enter the username and password of the NSX Manager that are required for communication to be authenticated by the Security Director.

- Description—Enter a description for the NSX Manager you are to add to the Security Director.

- SSL Certificate—View the SSL certificate to authenticate the NSX Manager and select the Accept SSL Certificate option to accept the SSL certificate.

  This is a mandatory field to discover the NSX Manager. The SSL Certificate field appears once you enter the NSX details.

4. Click **Next**.

5. In the Service Manager Registration section, enter the following details about the Security Director:

   - SD Username, SD Password—Enter the username and password of Security Director to allow the NSX Manager to authenticate communication to the Security Director.

   - License Key—Enter the license key for the previously procured Juniper SDSN for NSX license. See Juniper Connected Security for VMware NSX Integration for background details.

6. Click **Next**.
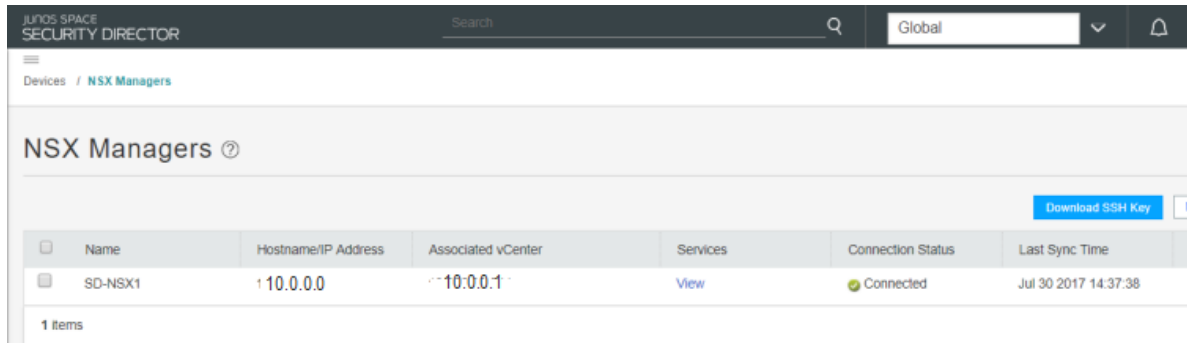
7. In the vCenter Server section, provide the following details about the vCenter Server:

   - Host—Enter the IP address of the VMWare vCenter Server.

   - Port—Enter the port number of the VMWare vCenter Server. By default, 443 is used.

   - Username, Password—Enter the username and password of the VMware vCenter Server. Security Director uses these credentials to discover the vCenter Server and fetch the VM inventory details.

   - SSL Certificate—View the SSL certificate to authenticate the vCenter Server and select the Accept SSL Certificate option to accept the SSL certificate. To discover the vCenter Server, it is mandatory to accept the certificate.

8. Click **Finish**.

   The Summary page of configuration changes appears. Click **OK** to add the NSX Manager. When you return to the NSX Managers page, you will see the discovered NSX Manager listed, as shown in .

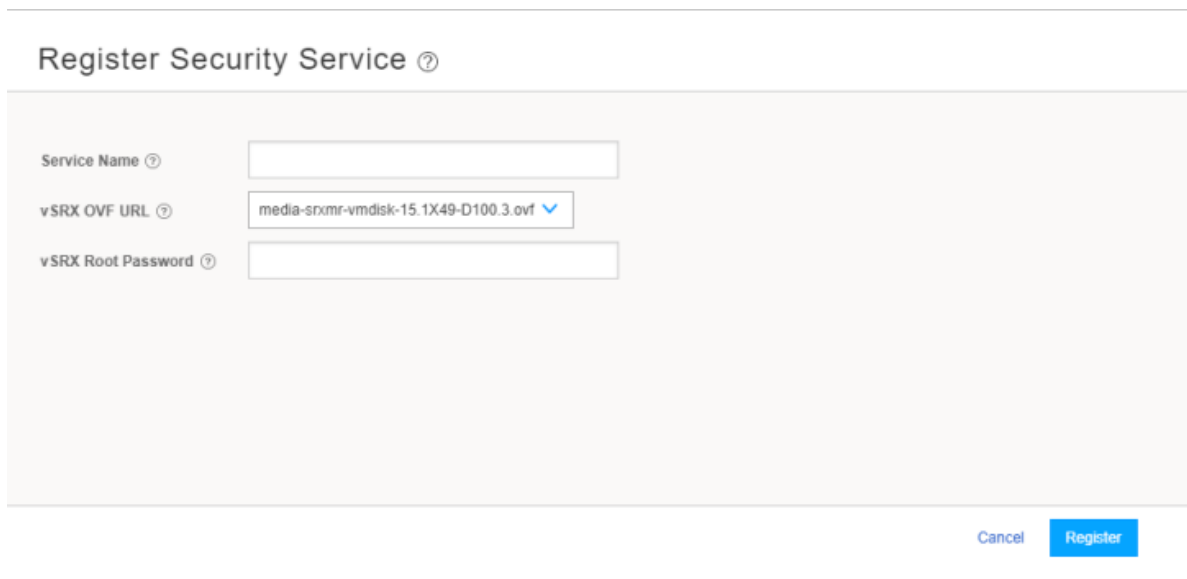**Figure 5: NSX Managers Page**

After adding the NSX Manager, you must register the vSRX VM as a Juniper security service with the NSX Manager.

To register the vSRX instance as a Juniper security service:

1. Select the NSX Manager for which service needs to be registered, right-click or from the More list, select **Register Security Service**.

    The Register Security Service page appears, as shown in .

Figure 6: Register Security Service Page

2. In the Service Name field, enter the name of the Juniper security service.

3. From the vSRX OVF URL list, select the available vSRX OVF image that you copied to the Policy Enforcer machine.

4. In the vSRX Root Password field, enter the root password of the vSRX instance. The same root password will be set for all the vSRX instances deployed in NSX.

5. In the Description field, enter a description.
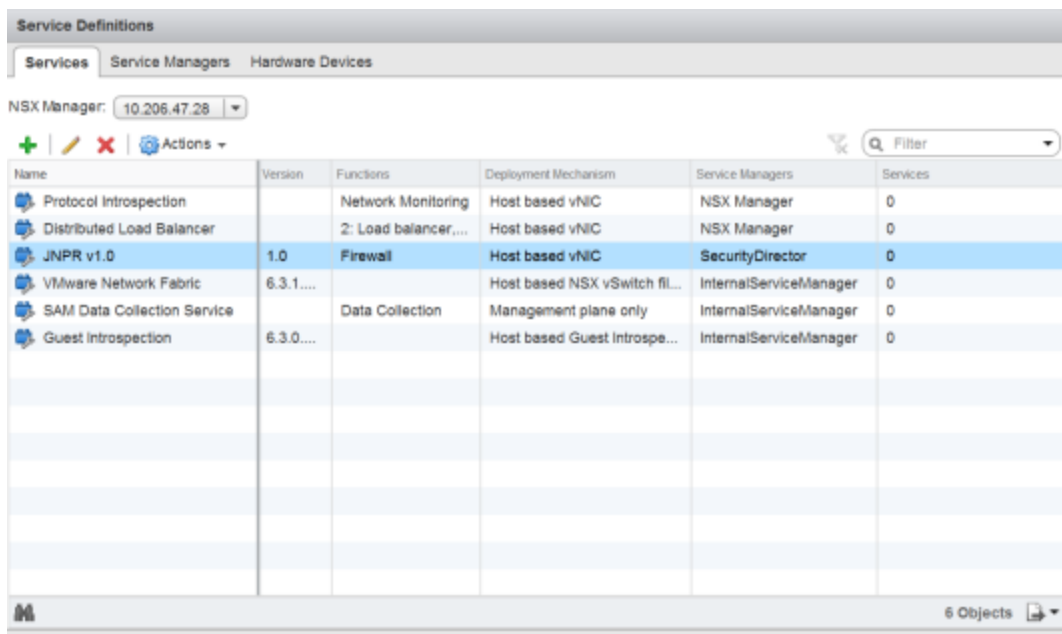
6. Click **Register**.

   A confirmation message indicates whether the registration is successful or not.

The vSRX instance registered as a new service in the vSphere Web Client environment. The vSRX is added as a network service that can be deployed by the NSX Manager.

In the vSphere Web Client, verify the following:

- Click **Networking & Security** and then click **Service Definitions**. Click the **Services** tab and verify that *<service-name>* v1.0 is listed in the table (the newly registered vSRX VM) along with the Security Director as the Service Manager, as shown in Figure 7 on page 33.

Figure 7: Service Definitions Page

- Click the **Service Managers** tab and verify that the Security Director is listed with a status of **In Service**, as shown in Figure 8 on page 34.

Figure 8: vSphere Web Client Service Manager Page

The NSX Manager and its inventory are now synchronized with the Security Director. All shared objects (such as security groups) are synchronized between the NSX Manager and Security Director. The shared objects include the IP addresses of all VMs in ESXi hosts, including the vSRX agent VMs. Security Director creates a dynamic address group(DAG) for each security group synchronized from the NSX Manager, along with the addresses of each member of the security group.

After you register a Juniper security service in the NSX Manager, the NSX Manager uses the vSRX agent VM to communicate the service status. The NSX Manager transmits messages to the Security Director when any changes or activities are happening in the NSX Manager that are related to the Juniper security service.

Deploying vSRX as a Security Service on a vSphere Cluster (VMware vCenter Server)

The next step is to deploy the Juniper security service on a vSphere cluster. You perform this action as a new service deployment, selecting the Juniper security service and the specific vSphere cluster on which you want the vSRX agent VM deployed.

Before you deploy the vSRX agent VM as a security service on the vSphere cluster, you must create a static IP pool with a primary DNS for the vSRX. To create the static IP pool:

Create a static IP pool with a primary DNS for the vSRX. This is a mandatory step before you deploy the vSRX agent VM.

1. From the vSphere Web Client, select **Networking & Security** and then **NSX Managers**.
2. In the Navigator column, select the name of the NSX Manager and click **Manage** > **Grouping Objects** > **IP Pools**.

3. Click the **Add icon (+)** to add the static IP pool.

   The Add Static IP Pool page appears, as shown in .

   Figure 9: Add Static IP Pool Page

4. In the Name field, provide a name for the IP pool.
5. In the Gateway field, provide a default gateway IP address.
6. In the Prefix Length field, provide a prefix length of the DNS.
7. Provide the primary and secondary DNS and the DNS suffix . This is a mandatory field.
8. In the Static IP Pool field, provide the IP address ranges to be included in the pool.
9. Click **OK**.

   A new IP pool is created for the vSRX to be deployed.

To deploy the vSRX agent VM as a security service for a vSphere cluster:

1. From the vSphere Web Client, click **Networking & Security** and then click **Installation**.

   The Installation page appears.

2. Click the **Service Deployments** tab and then click the **New Service Deployment (+)** icon. The Deploy Network & Security Services page appears, as shown in .

Figure 10: Deploy Network and Security Services Page

3. From the Select services & schedule page, select *<service-name>* v1.0 as the service to deploy and then click **Next**.

4. From the Select clusters page, select the data center and one or more clusters on which the vSRX agent VM is to be deployed, and then click **Next**.

5. From the Select storage and Management Network page:

   • Select the datastore on which to allocate shared storage for the vSRX agent VM, as shown in . ESXi hosts should be configured so that they can access shared storage. If you select **Specified on-host**, ensure that the datastore for the ESXi host is specified in the **Agent VM Settings** of the ESXi host in the cluster. See the VMware documentation for details.

Figure 11: Select Storage and Management Network Page

- Select the network that you intend to use for traffic to the vSRX agent VM. If you select **Specified on-host**, ensure that the network to be used is specified in the **Agent VM Settings > Network** property of the ESXi host in the cluster. See the VMware documentation for details.

  ⓘ **NOTE**: The datastore and network must be configured for each ESXi host in the cluster.

  For IP assignment, you can choose an IP pool to assign a range of IP addresses from a selected static IP pool or create a new static IP pool.

6. Click **Next** to access the Ready to complete page, and then click **Finish** to publish the changes and deploy the vSRX agent VM security services to the specified cluster. From the Service Deployments tab, you will see that the Juniper security service has been successfully deployed on the selected vSphere cluster.

7. From the vSphere Web Client, click **Hosts and Clusters** and verify that vSRX agent VMs are listed as *service-name* v1.0 in the vSphere Web Client inventory and created for each ESXi host in the vSphere cluster.

  ⓘ **NOTE**: *service-name* is the name provided at the time of service registration.

8. The Security Director automatically discovers all the deployed vSRX VM agents by using the device-initiated discovery. A new firewall and IPS group policies are created and all devices are assigned to these group policies.

> ℹ **NOTE**: The Security Director creates predefined IPS policies with a single IPS template. You can either add more IPS templates or convert the predefined IPS policies to custom IPS policies.

When you add an ESXi host in the vSphere cluster, NSX Manager automatically detects that the new ESXi host and adds the Juniper security service vSRX agent VM for it.

Verifying vSRX Agent VM Deployment in Security Director

In the Security Director, based on the NSX Manager discovery, NSX security groups are automatically synchronized with Security Director. For each service group in NSX Manager, Security Director creates a corresponding dynamic address group.

To verify that the vSRX agent VMs have been properly deployed:

1. Select **Security Director** > **Devices** > **NSX Managers**.

   The NSX Managers page appears with the discovered NSX Manager and the vSRX instance registered as a new service in the vSphere Web Client environment.

2. Select **Security Director** > **Monitor** > **NSX Inventory** > **Security Groups**.

   The Security Groups page appears listing all the security groups obtained from NSX and the corresponding dynamic address groups created by the Security Director, as shown in .

Figure 12: Security Groups Page

3. Select **Security Director** > **Monitor** > **vCenter Server Inventory** > **Virtual Machines**.

The Virtual Machines page appears, listing the VMs that are dynamically fetched by the associated vCenter, as shown in . You can view the security groups associated with each VM. Also, you can view security groups associated with each VM.

Figure 13: Virtual Machines Page

Automatic Creation of Security Policy in the NSX Environment to Direct Traffic Through the vSRX Agent VMs (VMware vCenter Server)

After you deploy vSRX agent VM security services to the ESXi hosts in a vSphere cluster, security policies are automatically created to redirect any network traffic originating from the VMs in a specific security group to the Juniper security service vSRX agent VM residing in the ESXi host for further analysis.

To direct the traffic to the vSRX agent VMs in each ESXi host by using the automatically created security policies:

1. In the Security Director, install the IPS signature to all the vSRX VM agents.
2. On the Firewall and IPS Policies page, add new rules to the automatically created firewall or IPS policies with respective dynamic address groups, as shown in . You can also use the application firewalls in the firewall rules.

Figure 14: Firewall Policy Rules Page
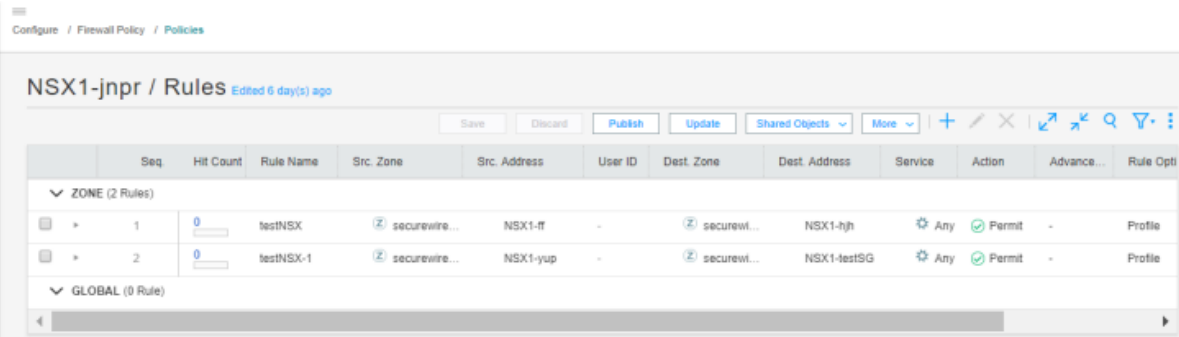
3. After creating policy rules, publish and update the firewall and IPS policies.

4. After the firewall and IPS policies are successfully updated in the Security Director, log in to the vSphere Web Client to verify the security policies in NSX Manager.

   Select **Network & Security** > **NSX Managers**, and the Navigator column, select the NSX Manager name. The security policies are automatically created in NSX Manager by Security Director, as shown .

Figure 15: NSX Security Groups Page
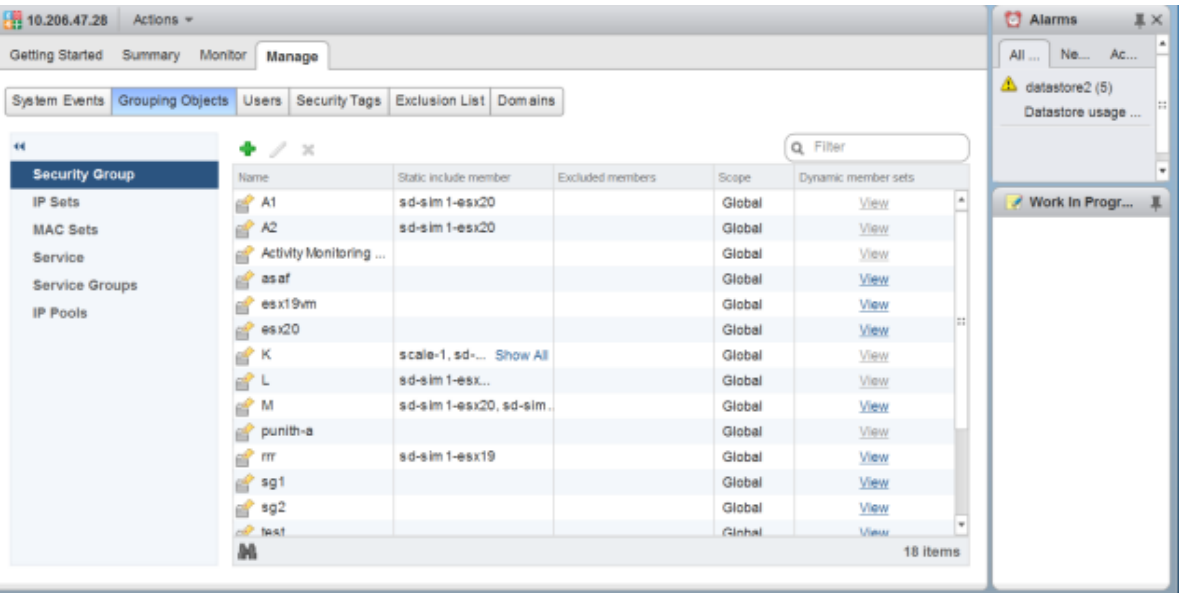
5. From the vSphere Web Client, select **Networking & Security** and then select **Firewall**.

   The Firewall page appears.

6. In the right pane, select the Partner Security Services tab to view the complete list of automatically created security policies from the Security Director, as shown in .
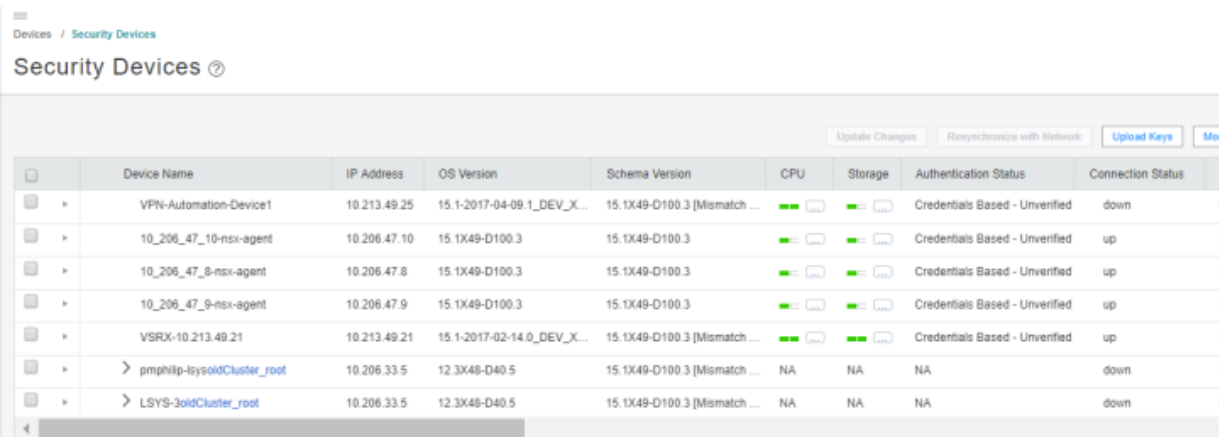
Figure 16: Firewall Page
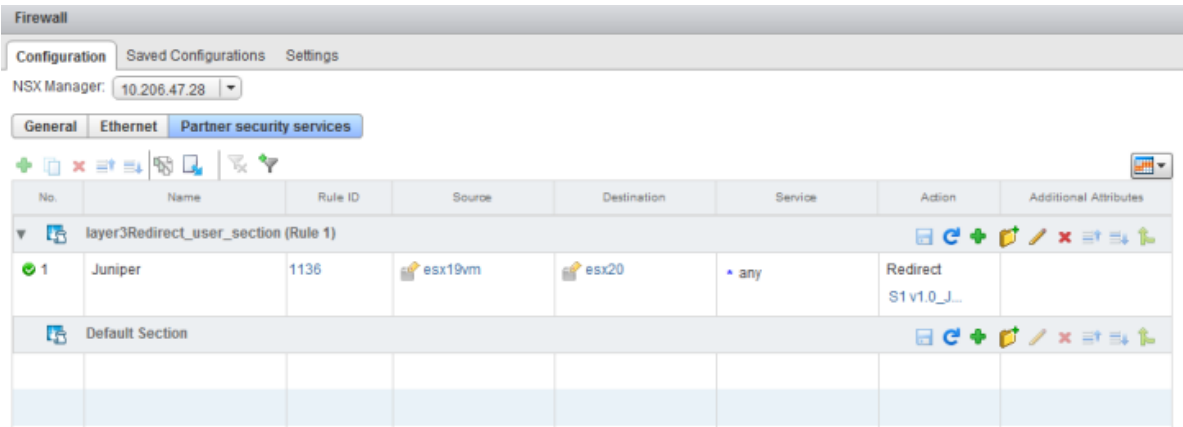
7. The corresponding traffic now goes through the vSRX VM agent.

When you return to **Security Director > Devices > Security Devices**, you can view the active configuration for the vSRX agent VMs, as shown in .

Figure 17: Security Devices Page

The NSX Manager is aware of the security groups that the Juniper security service monitors. If any changes occur in the security group, the NSX Manager notifies the Security Director about those changes. If membership changes, the NSX Manager notifies the Security Director of the changes and the Security Director updates its database based on the new membership.

RELATED DOCUMENTATION

Junos Space Security Director

Implementing Threat Policy on VMWare NSX

VMWare NSX Integration with Policy Enforcer and ATP Appliance Cloud Overview

Juniper Networks Advanced Threat Prevention Cloud (ATP Appliance Cloud) identifies the infected virtual machines (VMs) running on VMWare NSX and tags these VMs as infected. This is based on a malware file exchange from the infected VMs and/or based on the Command and Control communication with known botnet sites on the internet.

Based on this identification of infected or compromised hosts, you can take one of the following actions:

- Enable additional security features such as Layer-7 Application Firewall and Intrusion Prevention (IPS) leveraging vSRX

- Enforce Layer-2 to Layer-4 controls using NSX Distributed Firewall

- Leverage NSX integration with Host-Based security vendors (https://www.vmware.com/products/nsx/technology-partners.html) to take host-based security actions such as running antivirus or anti malware features on the infected VMs.

Policy Enforcer provides a set of Connector APIs for the third-party adaptors. The NSX Connector integrates with the Policy Enforcer using these APIs to enable enforcement of the infected hosts policy on Secure Fabric. For NSX connectors, the NSX Manager , its associated vCenter, and an edge firewall form the Secure Fabric.

The following topology shows how NSX Manager and the edge firewall create a Secure Fabric to use with Policy Enforcer.

Figure 18: Topology of NSX Integration with Policy Enforcer
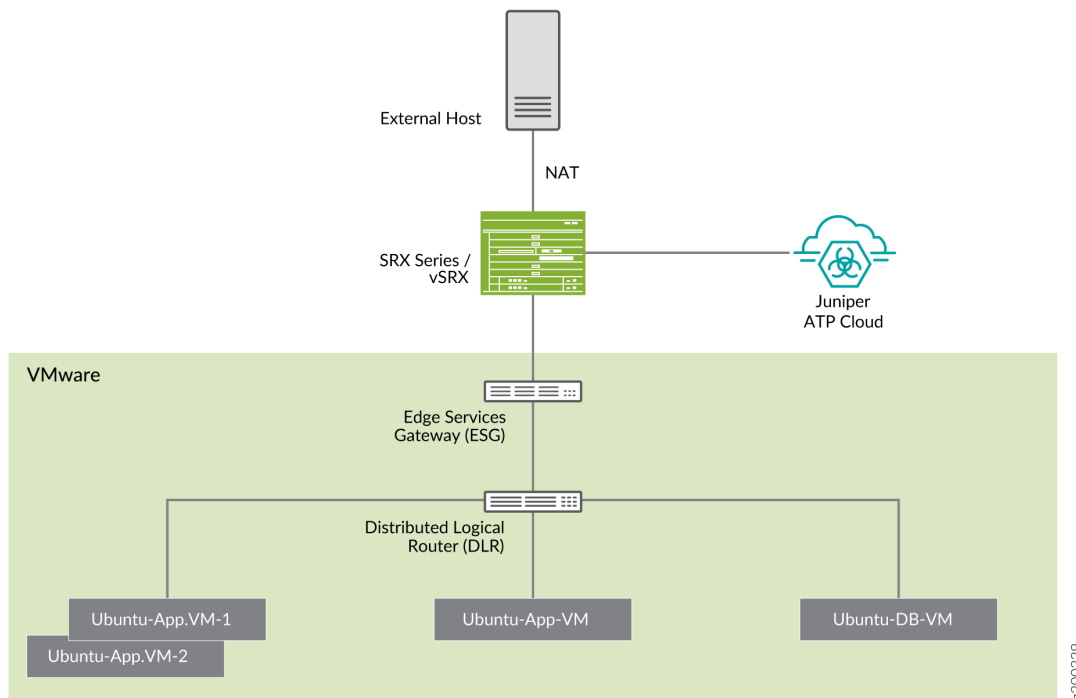
Within the NSX Manager, the virtual machines (VM) connect to logical networks, shown as green and yellow colour logical networks, as shown in . The logical switches connect to each other using a Distributed Logical Router(DLR). To form the Secure Fabric, configure the edge service gateway (ESG) to point to SRX Series Firewalls or vSRX as the gateway for the networks hosted on NSX. This is implemented by establishing IBGP session between ESG and vSRX or SRX Series Firewall. This ensures that all the north-south traffic passes through the vSRX edge firewall. The vSRX edge gateway is enrolled with ATP Appliance Cloud for the traffic inspection.

If NAT services are required, it must be configured on the vSRX and not on the ESG. Configure NAT services using the following CLI commands.

```
set security nat source rule-set trust-to-untrust from zone trust

set security nat source rule-set trust-to-untrust to zone untrust

set security nat source rule-set trust-to-untrust rule snat-rule match source-address 0.0.0.0/0

set security nat source rule-set trust-to-untrust rule snat-rule then source-nat interface
```
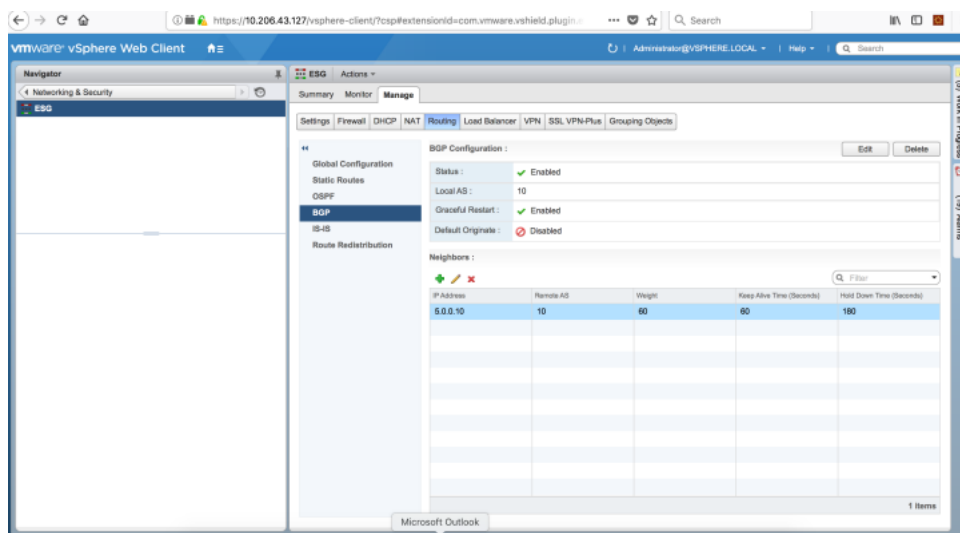
To establish a BGP session, use the following configuration commands:

```
set routing-options autonomous-system 10

set protocols bgp group nsx neighbor 5.0.0.2 peer-as 10
```

You can view the BGP configuration in VMWare vCenter Server, as shown in .

Figure 19: VMWare vCenter BGP Configuration

> **NOTE**: You can register the NSX Manager with Security Director only when the Policy Enforcer is configured. The NSX micro service is bundled with the Policy Enforcer VM. However, the NSX micro service is packaged as a standalone rpm, so that the NSX micro service upgrade and patches can be performed independent of the Policy Enforcer VM.

Implementation of Infected Hosts Policy Overview for VMware NSX

The vSRX or SRX Series Firewalls running as an edge firewall is enrolled to send all the suspected traffic to ATP Appliance Cloud.

The following steps explain the high-level workflow:

- If an infection is detected, ATP Appliance Cloud notifies the Policy Enforcer about the infected IP addresses

- If the infected IP address belongs to Secure Fabric associated with the NSX domain, Policy Enforcer calls the NSX plugin APIs to notify the NSX Connector about the list of infected IP addresses

- NSX service will then retrieve the VM corresponding to the IP addresses sent and then calls the NSX API to tag to an appropriate VM with a security tag, SDSN_BLOCK.

You can then create a policy to block the infected hosts using the SDSN_BLOCK tag by creating VMWare Distributed Firewall (DFW) rules. The block policy consists of two rules for ingress block and egress block. The ingress block rule applies to any traffic originating from a security group composed of VMs tagged with a block tag to any destination. Similarly, the egress block rule applies to any traffic destined to security group composed of VMs tagged with block tag from any source.

The creation of security groups associated with the SDSN_BLOCK tag, creation of ingress and egress block rules, and the action to take on the matching packets must be configured by the VMWare administrators. The NSX Connector will simply apply the SDSN_BLOCK tag on the infected VM.

Registering NSX Micro Service as Policy Enforcer Connector Instance Overview

The integration of each NSX manager discovered in Security Director with Policy Enforcer is triggered automatically.

The automatic registration of a connector instance involves the following steps:

1. Discovering the NSX Manager in Security Director. This triggers an auto creation of the Policy Enforcer connector instance.

2. Secure Fabric is created to manage the discovered NSX Manager.

3. Creation of threat prevention policy requires the knowledge of ATP Appliance Cloud realm and the edge firewall device. These are taken as inputs from the user.

Before You Begin

IN THIS SECTION

- Infected Hosts Workflow in VMware vCenter Server | **46**

Before you begin to configure NSX with Policy Enforcer, configure the infected hosts workflow in VMWare vCenter Server.

Infected Hosts Workflow in VMware vCenter Server

To block the infected hosts:

1. Log in to the vSphere Web Client through the VMware vCenter Server.
2. From the vSphere Web Client, click **Networking & Security** and then click **NSX Managers**.

   Under the Manage section, click **Security Tags** column head and create SDSN_BLOCK security tag for NSX, as shown in .

Figure 20: SDSN_BLOCK Security Tag
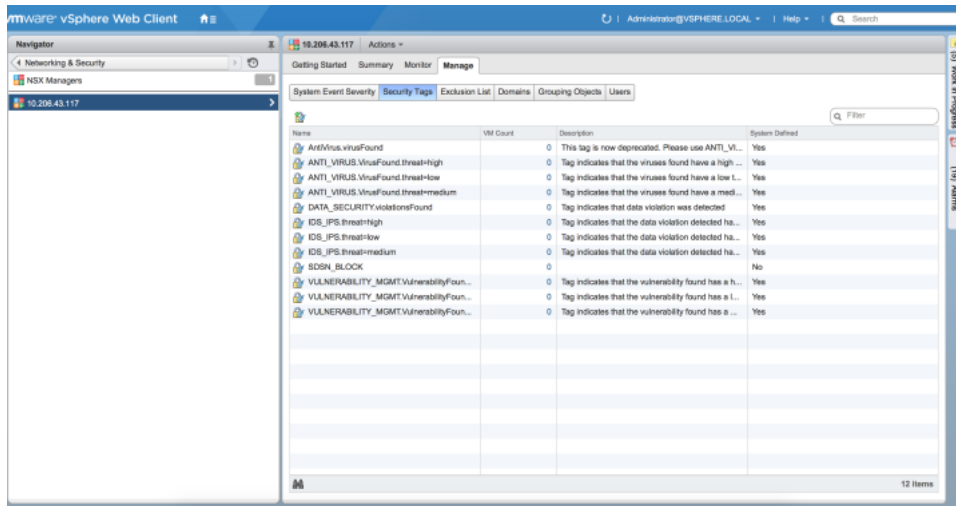
The feed for the infected hosts will be triggered by ATP Appliance Cloud down to Policy Enforcer. When there is a trigger, the SDSN_BLOCK tag is attached to the VM. Click on the VM Count column to see the VM details attached to the tag.

3. Select **Networking & Security** and then click **Service Composer**.

   The Service Composer page appears. From the Service Composer, click the **Security Groups** tab. The security administrator can create the security group based on the security tag.

4. Click the **New Security Group** icon to create a new security group.

5. Enter a name and description for the security group and then click **Next**.

6. On the Define dynamic membership page, define the criteria that an object must meet for it to be added to the security group you are creating.

   In the Criteria Details row, select **Security Tag** from the list and provide the SDSN_BLOCK tag name, as shown in .

Figure 21: Define Dynamic Membership Page

Click **Next**.

7. In the Ready to Complete page, verify the parameters and click **Finish**.

   In the Service Composer page, under the Security Groups tab, you can see that the security group has been created and the VM with the security tag is assigned to the security group.

Configuring VMware NSX with Policy Enforcer

The following steps explain configuring VMWare NSX with Policy Enforcer:

1. Add the NSX Manager to the Security Director database, as shown in . To know more about adding a NSX Manager, see *Add the NSX Manager*.

Figure 22: Adding NSX Manager Page

2. After discovering the NSX Manager in Security Director, use the Guided Setup workflow to configure the following parameters:

   - Secure Fabric

   - Policy Enforcement Group (PEG)

   - ATP Appliance Cloud Realm

   - Threat policies for the following threat types:

     - Command and Control (C&C) Server
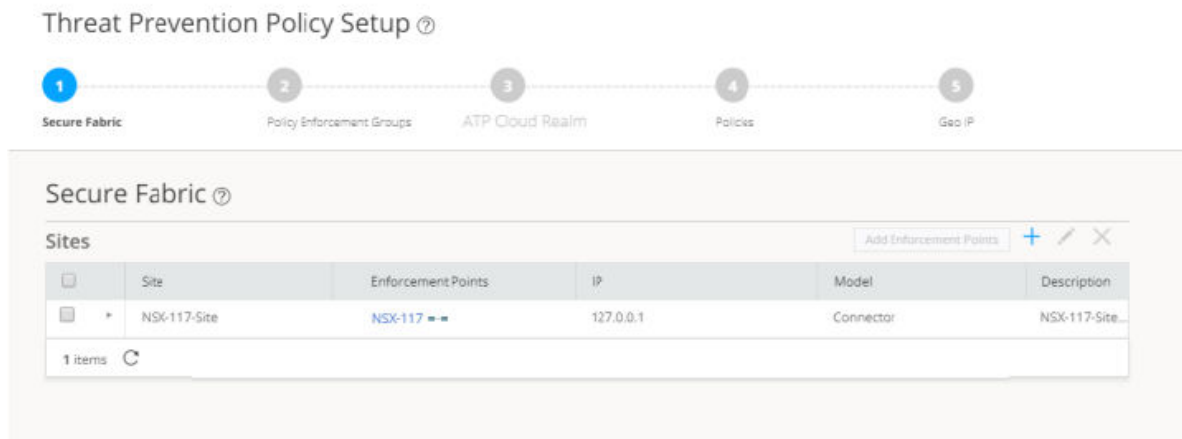
     - Infected Hosts

     - Malware

3. Select **Configuration** > **Guided Setup** > **Threat Prevention**.

   The Threat Prevention Policy Setup page appears.

4. Click **Stat Setup**.

   The Threat Prevention Policy Setup page appears, as shown in Figure 23 on page 50. Some of the resources are already configured as you discover the NSX Manager.

Figure 23: Guided Setup Page

5. In the Secure Fabric page, the site is already created. For that site, one enforcement point is also added.

    To create a secure fabric site in Policy Enforcer for NSX based environment, you require two parts : NSX Manager and edge firewall. In the Add Enforcement Points page, add vSRX, as shown in the topology, as a edge firewall. Select the vSRX device listed under the Available column and move it to the Selected column. You now have two enforcement points within the Secure Fabric.

    Click **Next**.

6. In the Policy Enforcement Groups page, the policy enforcement group is already created based on the Location Group Type. The location points to the Secure Fabric site created for NSX.

    Click. **Next**.

7. In the ATP Cloud Realm page, associate the Secure Fabric with ATP Cloud realm.

    If the ATP Cloud realm is already created, click **Assign Sites** in the Sites Assigned column and chose the Secure Fabric site. The ATP Cloud realm and Secure Fabric are now associated.

    Click. **Next**.

8. In the Policies page, create a threat prevention policy by choosing the profile types depending on the type of threat prevention this policy provides (C&C Server, Infected Host, Malware) and an action for the profile. The DDoS profile is not supported by the NSX Connector. Once configured, you apply policies to PEGs.

    Click **Assign groups** in the Policy Enforcement Group column to associate the policy enforcement group with the policy.

    Security Director takes the snapshot of the firewall by performing the rule analysis and threat remediation rules are pushed into the edge firewall.

    Click **Finish**.

> **NOTE**: The GeoIP feeds are not used with the NSX Connectors.

9. The last page is a summary of the items you have configured using quick setup. Click **OK** to be taken to the Policies page under Configure > Threat Prevention > Policies and your policy is listed there.

Example: Creating a Firewall Rule in VMWare vCenter Server Using SDSN_BLOCK Tag

The following example shows the firewall rule creation using the SDSN_BLOCK security tag:

1. Log in to the vSphere Web Client through the VMware vCenter Server.

2. Select **Networking & Security** and then click **Service Composer**.

   The Service Composer page appears.

3. Select **Security Policies** tab in the Service Composer page.

   Create a security policy to block the traffic coming from the infected hosts.

4. Select the **Create Security Policy** icon.

   The New Security Policy page appears.

5. Enter a name and description for the security policy, and click **Next**.

6. Select the **Firewall Rules** option from the left pane.

   The Firewall Rules page appears.

7. Select the New Firewall Rule icon (+) to create a new firewall rule.

   The New Firewall Rule page appears.

8. Enter the name of the firewall rule.

9. In the Action field, select the **Block** option.

10. In the Source field, click **Change** and select the security group.

11. In the Destination field, click **Change** and select the security group to add as Any.

    Click **Ok**. Figure 24 on page 52 shows a sample firewall rule configuration.

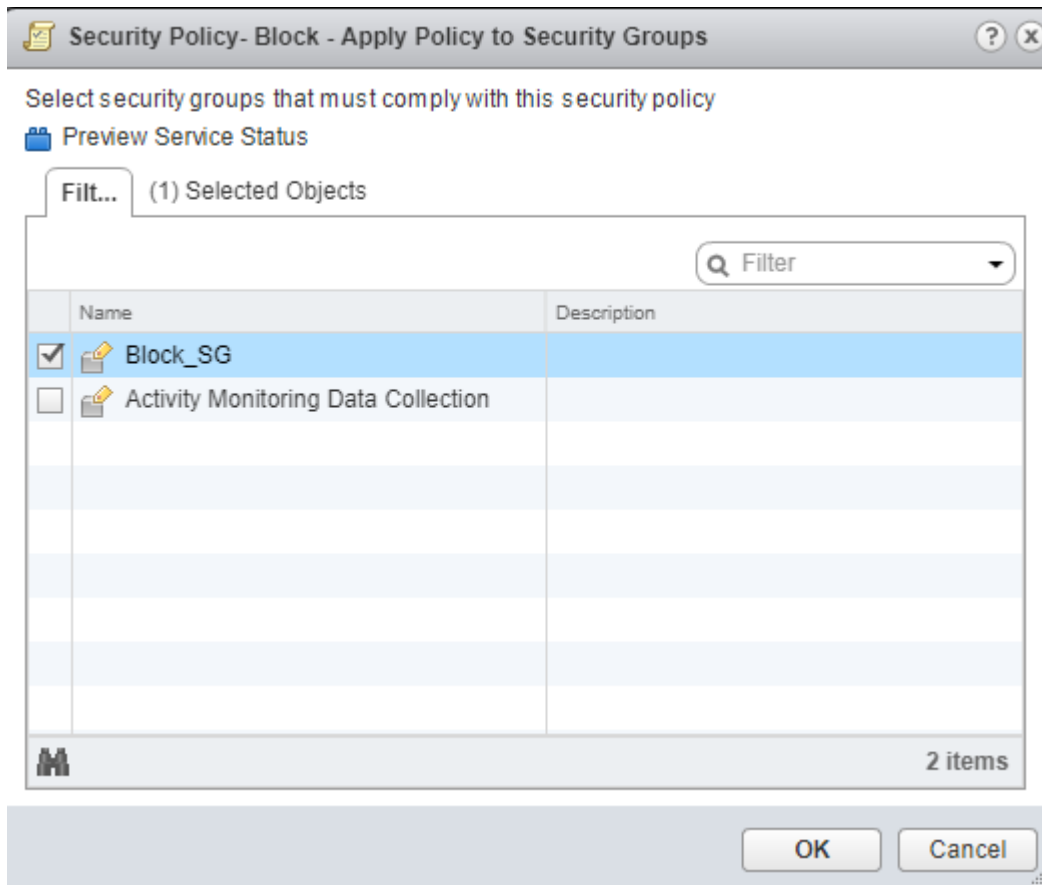**Figure 24: New Firewall Rule Page**

12. Click **Finish**.

    A new policy is created. You can apply this policy to the security group.

13. In the Security Policies page, right-click on the policy name and select **Apply Policy**.

    The Apply Policy to Security Groups page appears, as shown in Figure 25 on page 53.

Figure 25: Apply Policy to SG Page

14. Select the security group that you have created and assign to a policy.

    Security administrator is now able to block the traffic coming from the infected hosts.