Forcepoint

Next Generation Firewall

NGFW 6.5.5.21305.nsx.1
and other compatible versions

How to deploy NGFW using NSX-V

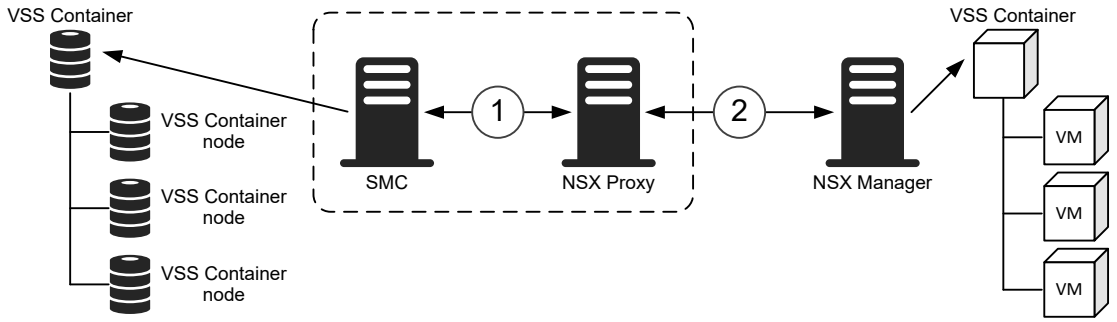
Revision B

Contents

Introduction

NSX-V coordinates services between a software-defined data center (SDDC) and Forcepoint Next Generation Firewall (Forcepoint NGFW). Integrating NSX-V with Forcepoint NGFW makes it possible to quickly deploy security services throughout the SDDC.

Integrating NSX-V with Forcepoint NGFW provides a transparent mapping service between Forcepoint NGFW and vSphere.



1. Through the NSX Proxy, the NSX-V Manager automatically creates objects, such as VSS Containers, VSS Container nodes, and other objects in the Security Management Center (SMC) component of Forcepoint NGFW.

   VSS Containers and VSS Container nodes are specialized types of NGFW Engine. Each VSS Container in the SMC represents a VSS container that has been deployed to a hypervisor. Each VSS Container node represents a virtual machine that has been deployed in a VSS container.

2. Through the NSX Proxy, the NSX-V Manager dynamically maps the policy to be uploaded to the virtual machines.

Before deploying Forcepoint NGFW Engines in the Firewall/VPN role on the virtualization platform with NSX-V, make sure that the following requirements are met.

- The NGFW Engine version must be a specific version intended for deployment using NSX-V, such as NGFW 6.5.5. 21305.nsx.1 or another NGFW Engine version for NSX-V available at https://support.forcepoint.com/Downloads.

- The NSX-V version must be 6.3 or higher.
- The SMC must be installed on the Linux operating system.
- The SMC version must be 6.5.0 or higher.
- 256-bit security strength is recommended between the Management Server and NGFW Engines.
- The IP address of the Management Server and the control IP addresses of the NGFW Engines must be IPv4 addresses.
- You must have enough NGFW Engine licenses for all VSS Container nodes.

This document focuses on the SMC administrator as the main audience. The workflow and tasks that are typically performed by a VMware administrator are labeled separately.

For general requirements and installation instructions, see the *Forcepoint Next Generation Firewall Installation Guide* and *Forcepoint Next Generation Firewall Product Guide*

Configuration overview

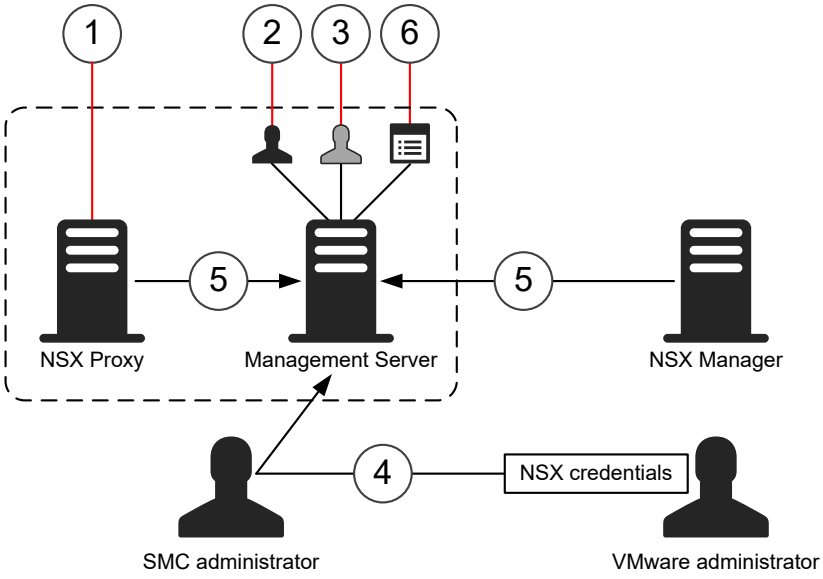
There are several steps in integrating NSX-V with the Forcepoint NGFW.

Note

This document focuses on the SMC administrator as the main audience. The workflow and tasks that are typically performed by a VMware administrator are labeled separately. For detailed information about vSphere and NSX-V, see third-party documentation for vSphere and NSX-V.

To integrate NSX-V with the Forcepoint NGFW, you must complete the following general steps:

1) The SMC administrator prepares for NSX-V integration in the SMC.



1. The SMC administrator installs and starts the NSX Proxy on the Management Server.
2. The SMC administrator creates an Administrator account with the NSX role for the VMware administrator.
3. The SMC administrator enables the SMC API and creates an API Client element to allow the NSX Proxy to connect to the Management Server.
4. The VMware administrator provides the NSX-V user name and password to the SMC administrator.

   The SMC administrator adds the NSX-V credentials to the Management Server to allow the SMC to communicate with NSX-V.
5. The SMC administrator adds the IP address of the NSX-V Manager and the listening IP address of the NSX Proxy to the Management Server.
6. The SMC administrator creates policies for VSS Containers and VSS Context Firewalls.

Note

You can complete most of the preparations in the Management Client component of the SMC.

2) In the NSX Proxy web interface, the SMC administrator configures NSX-V for use with the Forcepoint NGFW.

3) In vSphere, the VMware administrator configure NSX-V integration and assigns a Security Policy to each Security Group.

4) In the Management Client component of the SMC, SMC administrator verifies that the VSS Container and the VSS Context Firewalls have been automatically created in the SMC, then installs the Layer 2 Firewall Policies on the VSS Context Firewalls.

Objects and object names for NSX-V integration

When the workflow is divided between an SMC administrator and a VMware administrator, the objects used in the NSX-V integration and the names of the objects must be planned carefully and used consistently.

Some objects are shared between several components. They are combined in several ways, so we recommend keeping the names short and descriptive, and the intended usage as obvious as possible.

Two types of policies are shared between the components:

- In the Management Client, the SMC administrator creates two types of policy elements: a Firewall Policy for the VSS Container and a Layer 2 Firewall Policy for the VSS Context Firewalls.
- In the NSX Proxy web interface, the Firewall Policy that the SMC administrator has created is used as the VSS Container Policy for the NSX Proxy service.
- In vSphere, the Layer 2 Firewall Policy that the SMC administrator has created is used as the Security Policy for the Security Group.

Also objects that represent the firewall engines that are run on a virtualization are shared between the SMC, the NSX Proxy, and the vSphere platform.

CAUTION

Make sure to select names that are unique. Objects with the same name might cause mapping issues or be difficult for other administrators to use. After implementing the names of the objects in the SDDC, changing the names of these objects might cause mapping errors.

Object naming structures

Object	Description	Naming structure
Service	In the NSX Proxy web interface and vSphere, the Service represents the VSS Context Firewall engine image that is uploaded to the NSX Proxy.	*FPNGFW <VSS Container name>* NSX-V automatically creates the service name in vSphere when the VSS Container is built.
VSS Container Policy	In the NSX Proxy, the VSS Container Policy represents a networking policy that contains traffic intercept rules that NSX-V maps to a Forcepoint NGFW Firewall Policy.	*FPNGFW <Firewall Policy name>* The policy is automatically added to the list of available VSS Container Policies for Services in the NSX Proxy web interface shortly after a Firewall Policy is created in the Management Client.

Object	Description	Naming structure
Security Group	On the VMware virtualization platform, a Security Group is a group of virtual machines. In the SMC, a Security Group element corresponds to a group of firewalls that are available as the source or destination in policy rules. NSX-V creates and dynamically maintains these elements in the SMC. They are not configurable by SMC administrators.	The VMware administrator enters this name. **Important** The length of the Security Group name must not exceed 120 characters. We recommend that Security Group names be 75 characters or less. NSX-V automatically creates the Security Group element in the SMC when a Security Group is bound to a Security Policy.
Security Policy	On the VMware virtualization platform, a Security Policy represents a networking policy that contains traffic intercept rules that NSX-V maps to a Forcepoint NGFW Firewall Policy.	The SMC administrator enters this name in the Management Client. **Important** The length of the policy name must not exceed 120 characters. We recommend that policy names be 75 characters or less.
VSS Container	A specialized type of NGFW Engine. NSX-V creates a VSS Container in the SMC to represent a VSS container that has been deployed to a hypervisor.	*<VSS Container name>-<VSSID>* NSX-V automatically creates the virtual security system ID (VSSID) when the VSS Container is built. VSS Containers are numbered sequentially.
VSS Container node	A specialized type of NGFW Engine. NSX-V creates VSS Container nodes in the SMC for each virtual machine within the VSS Context Firewall engine image.	*<VSS Container name>-<VSSID>-<appliance instance ID >* NSX-V automatically creates the appliance instance ID when an engine is created.
VSS Context Firewall	A specialized type of NGFW Engine in the Layer 2 Firewall role. VSS Context Firewalls are deployed on the virtual machines.	*FPNGFW <VSS Container name>-<Layer 2 Firewall Policy name>-<VSSID>* NSX-V automatically creates the VSS Context Firewall in the SMC when a Security Group is bound to a Security Policy.

VSS Context Firewall deployment considerations

A secure SDDC requires careful planning of the network environment and the product requirements.

Network deployment options

Before making any changes, consider these key decisions about your environment.

Select the SMC

You can upgrade an existing SMC for NSX-V integration or you can install a dedicated SMC for performance or security reasons. A dedicated SMC requires its own licenses.

Important

If SMC is in an HA configuration, the IP address of the NSX Proxy must be updated if the active Management Server changes.

Plan network communication

We recommend that you do not use NAT policies between SMC, the NSX Server, the virtualization system, and the engines. If NAT must be used, you might need to create a custom Firewall Policy rule for the VSS Container.

Determine the security requirements

A Security Policy can be applied to more than one Security Group, but each Security Group can have only one Security Policy. When you plan Security Policies and Security Groups, there are two management strategies to choose from. See the following table that compares the strategies. Consider which security services the firewall supplies and which Security Groups need those services. A Security Group contains virtual machines with the same needs. It might be useful to create a Security Group that has restricted security. If you suspect that a firewall might be compromised, you can move the firewall to this Security Group.

Tip

You can have up to 126 different Security Policies.

Designing the security environment

Benefits	Drawbacks
Few Security Policies applied to Security Groups of many virtual machines	

Benefits	Drawbacks
■ Applies a consistent policy to a greater number of virtual machines ■ Less setup for the security administrator ■ Reduces maintenance for the security administrator	■ Policy must be broadly applicable
Many Security Policies with a few virtual machines in each Security Group	
■ Granular application of policy in an SDDC	■ Policy updates could require changes to multiple policies ■ More setup for the security administrator ■ Requires more maintenance by the security administrator

Unsupported features

When you deploy firewalls on the virtualization platform with NSX-V automation, some features are not available.

Engine type	Features not supported	Features managed by the virtualization platform or NSX-V
VSS Container	■ Clustering ■ Tester	■ Changing engine state ■ Domains — All VSS Containers are in the Shared Domain ■ Interfaces
VSS Context Firewall	■ ARP entries ■ DSCP ■ Zones — Only internal and external zones are supported ■ URL Filtering	■ Changing engine state ■ Quality of Service

Preparing the SMC for NSX-V integration

The SMC administrator must prepare the SMC for integration with NSX-V and enable NSX-V to access the SMC through an SMC API client.

Note

We recommend that the SMC and the NSX Proxy are installed on the same management network as vSphere.

These tasks are done by the SMC administrator.

The configuration consists of the following general steps:

1) Install and start the NSX service on the Management Server.

2) Create administrator accounts for NSX-V integration in the SMC.

3) Configure the SMC API to allow communications between NSX-V and the SMC using the SMC API.

4) Enable NSX-V integration for the Management Server to allow the Management Server to communicate with NSX-V.

5) Create policies for VSS Containers and VSS Context Firewalls.

Install or upgrade the SMC for NSX-V integration

Enable NSX-V integration when you install or upgrade the SMC.

Before you begin

You must have licenses for the SMC server components and NGFW Engine licenses for all VSS Container nodes. To obtain licenses, go to the License Center at https://stonesoftlicenses.forcepoint.com.

Note

This document explains the high-level steps for installing or upgrading the SMC. For detailed instructions, see the *Forcepoint Next Generation Firewall Installation Guide* available at https://support.forcepoint.com.

Steps

1) Download the SMC software from https://support.forcepoint.com.

2) Log on as root, then run setup.sh the start the **Installation Wizard** to install or upgrade the SMC components.

3) On the Management Server page of the **Installation Wizard**, select **Install NSX Service on the Management Server** to install the NSX Proxy.

4) Install or upgrade the other SMC components as described in the *Forcepoint Next Generation Firewall Installation Guide*.

5) If you installed the SMC instead of upgrading it, install the licenses for the SMC servers, then install the NGFW Engines licenses for the VSS Container nodes.

Create an administrator role for license management

In the SMC, you must create an Administrator Role element that has permissions for license management.

Note

This document explains the high-level steps for creating administrator roles in the SMC. For detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide* available at https://support.forcepoint.com.

Steps

1) Select **Configuration**, then browse to **Administration**.
2) Right-click **Access Rights** , then select **New** > **Administrator Role**.
3) In the **Name** field, enter `LICENSE`.
4) From the **Administrative Rights** group of permissions, select **Manage Licenses**.
5) Click **OK**.

Create administrator accounts for NSX-V integration

In the SMC, you must create an administrator account for the VMware administrator who configures the NSX Proxy in the NSX Proxy web interface.

Before you begin

Create an administrator role for license management.

CAUTION

Select only the minimum necessary permissions for each Administrator account.

Note

This document explains the high-level steps for creating administrator accounts in the SMC. For detailed instructions, see the *Forcepoint Next Generation Firewall Product Guide* available at https://support.forcepoint.com.

Steps

1) Select **Configuration**, then browse to **Administration**.

2) Right-click **Access Rights** , then select **New** > **Administrator**.

3) From the **Type** drop-down list, select **Local** to store the administrator account on the Management Server.

4) In the **Name** field, enter a unique name.
The VMware administrator uses this user name to log on to the Management Client or to the NSX Proxy web interface.

5) To authenticate administrator logons using a user name and password on the Management Server, configure these options.
   a) From the **Authentication** drop-down list, select **Local Username and Password**.
   b) In the **Password** fields, enter and confirm the password.

Note

The SMC administrator must provide the user name and password to the VMware administrator. The VMware administrator must log on to the Management Client and change the password before logging on to the NSX Proxy web user interface for the first time.

Tip

To change your own password, select ☰ **Menu** > **System Tools** > **Password** > **Change Password** in the Management Client.

6) On the **Permissions** tab, add the NSX administrator role and define the granted elements.
   a) Make sure that **Restricted Permissions** is selected.
   b) Click **Add Role**.
   A new Administrator Role appears in the list.
   c) Click the **Role** cell, then select **NSX Role** as the administrator role.
   The NSX Role is a predefined Administrator Role in the SMC. It allows the VMware administrator to view and manage granted elements in the SMC, to upload and refresh policies on the granted engines and to send commands to the granted engines.

Tip

To view permissions for the **NSX Role**, click the **Role** cell, select **Select**, right-click **NSX Role**, then select **Properties**.

   d) Right-click the **Granted Elements** cell for the role, then select **Edit Granted Elements**.
   The **Select Elements** dialog box opens.
   e) To select the elements to which the rights granted by the administrator role apply, click **Set to ALL** or select individual elements in the left pane, then click **Add**.
   f) Click **OK**.

7) On the **Permissions** tab, add the LICENSE administrator role and define the granted elements.
   a) Make sure that **Restricted Permissions** is selected.
   b) Click **Add Role**.
      A new Administrator Role appears in the list.
   c) Click the **Role** cell, then select **LICENSE** as the administrator role.
   d) Right-click the **Granted Elements** cell for the role, then select **Edit Granted Elements**.
      The **Select Elements** dialog box opens.
   e) To select the elements to which the rights granted by the administrator role apply, click **Set to ALL** or select individual elements in the left pane, then click **Add**.
   f) Click **OK**.
8) Click **OK** to save the Administrator element.

Enable NSX-V integration for the Management Server

You must enable NSX-V integration on the Management Server to allow communications between the NSX Server and the Management Server.

Steps

1) In the Management Client, select **Home**.
2) Browse to **Others** > **Management Server**.
3) Right-click the Management Server, then select **Properties**.
4) On the **Integration** tab, enable NSX-V integration and enter the credentials that allow the VMware administrator to manage firewalls in the NSX Proxy web interface.
   a) Click **Add**, then select **NSX** as the integration type.
      A new row appears in the list.
   b) Click the **IP Address** cell for the NSX-V integration, then enter the IP address of the NSX-V Manager.
   c) Click the **Port** cell, then enter the listening port of NSX Proxy server.
   d) Click the **Listening IP Address** cell, then enter the IP address that the NSX Proxy server uses in communications with the Management Server and the SMC API.

e) Click the **Username** cell then, select the user name of the VMware administrator.

The user name of the VMware administrator is added in the **Username** cell, and the password of the VMware administrator is added in **Password** cell.

Note

The user name and the password are not editable on the **Integration** tab. If necessary, you can modify the user name and change the password in the Administrator element that represents the account for the VMware administrator.

5) Click the **Administrator** cell, then select the Administrator element that represents the account that the VMware administrator uses to log on to the NSX Proxy web interface.

6) Make sure that the checkbox in the **Enabled** cell is selected.

Tip

If you need to disable the VMware administrator's access to the NSX Proxy web interface, deselect the checkbox in the **Enabled** cell.

7) Click **OK**.

Configure SMC API

The Application Programming Interface (API) of SMC allows external applications to connect with the SMC.

Note

If there is a firewall between SMC and the other applications, make sure that there is an Access rule to allow communication.

The SMC API can be used to run actions remotely using an external application or script. For more information about using SMC API, see the *Forcepoint NGFW SMC API Reference Guide*.

Create TLS credentials for SMC API Clients

If you want to use encrypted connections, the SMC API Client needs TLS credentials to connect with the Management Server.

Note

You can import the existing private key and certificate if they are available.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Configuration**.

2) Browse to **Administration** > **Certificates** > **TLS Credentials**.

3) Right-click **TLS Credentials**, then select **New TLS Credentials**.

4) Complete the certificate request details.
   a) In the **Name** field, enter the IP address or domain name of SMC.
   b) Complete the remaining fields as needed.
   c) Click **Next**.

5) Select **Self Sign**.

6) Click **Finish**.

Result

The TLS Credentials element is added to **Administration** > **Certificates** > **TLS Credentials**. The **State** column shows that the certificate has been signed.

Enable SMC API

To allow other applications to connect using the SMC API, enable SMC API on the Management Server.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Home**.

2) Browse to **Others** > **Management Server**.

3) Right-click the Management Server, then select **Properties**.

4) Click the **SMC API** tab, then select **Enable**.

5) (Optional) In the **Host Name** field, enter the name that the SMC API service uses.

Note

API requests are served only if the API request is made to this host name. To allow API requests to any host name, leave this field blank.

6) Make sure that the listening port is set to the default of 8082 on the Management Server.

7) If the Management Server has several IP addresses and you want to restrict access to one, enter the IP address in the **Listen Only on Address** field.

8) If you want to use encrypted connections, click **Select**, then select the TLS Credentials element.

9) Click **OK**.

Create an API Client element for NSX-V integration

External applications use API clients to connect to SMC. You must create an API Client element to allow the NSX Proxy server to connect to the Management Server.

Before you begin

SMC API must be enabled for the Management Server.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) Select **Configuration**, then browse to **Administration**.
2) Browse to **Access Rights**.
3) Right-click **Access Rights** , then select **New** > **API Client**.
4) In the **Name** field, enter a unique name for the API Client.
5) Use the initial authentication key or click **Generate Authentication Key** to generate a new one.

   Important

   This key appears only once, so be sure to record it. The API Client uses the authentication key to log on to SMC API.

6) On the **Permissions** tab, select **Unrestricted Permissions** to define the permissions for actions in the SMC API.
   - Select **Unrestricted Permissions** to allow the API Client to manage all elements and perform all actions without restrictions in the SMC API.
7) Click **OK**.

Create the policies in the Management Client

Create the policies for the VSS Container and VSS Context Firewalls.

Before you begin

Each VSS Containers node and VSS Context Firewall requires a separate license.

In the Management Client, check that you have licenses for all the VSS Container nodes and VSS Context Firewalls. The elements for the VSS Container Nodes and VSS Context Firewalls are automatically created when you deploy the engine image in the NSX Proxy web interface and the licenses are automatically bound to the VSS Container Nodes and VSS Context Firewalls. If you do no have enough licenses, you cannot install the policies on the VSS Container nodes and VSS Context Firewalls.

You must create two sets of policies:

- A Firewall Policy for the VSS Container
- As many Layer 2 Firewall Policies for VSS Context Firewalls as are needed for your environment

Create a Firewall Policy for the VSS Container

Create a Firewall Policy to install on the VSS Container.

Note

We recommend that you use a unique naming format for the Firewall Policies that you create in the Management Client. Make sure that you name the Firewall Policies in the Management Client in a way that allows you to quickly identify the policies that you want to use for the VSS Containers

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Configuration**.

2) Right-click **Policies**, then select **New** > **Firewall Policy**.

3) In the **Name** field, enter a name for the element.

4) Select the Default Firewall Template Policy element as the template policy to base this policy on.
   The Default Firewall Template Policy includes rules that allow the VSS Container and VSS Container nodes to connect to NSX-V. The automatic rule allows inbound and outbound TCP connections on port 8090.

5) Click **OK**.
   The policy opens in the **Policy Editing** view.

6) (Optional) Add other rules according to your environment.

7) Click **Save**.

Create Layer 2 Firewall Policies for VSS Context Firewalls

Create a Layer 2 Firewall Policy for each VSS Context Firewall based on your network needs.

Note

NSX-V maps each Layer 2 Firewall Policy to a list of Security Policies in vSphere, including existing Layer 2 Firewall Policies. We recommend that you use a unique naming format for the Layer 2 Firewall Policies that you create in the Management Client. Make sure that you name the Layer 2 Firewall Policies in the Management Client in a way that allows you to quickly identify the policies that you want to use for the VSS Context Firewalls that NSX-V coordinates.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) Select **Configuration**.

2) Right-click **Policies**, then select **New** > **Layer 2 Firewall Policy**.

3) In the **Name** field, enter a name for the element.

4) Select the Template Policy element that you want to base this policy on.

5) Click **OK**.
   The policy opens in the **Policy Editing** view.

6) Configure the rules as needed.
   Consider carefully the choice for connection tracking. The choice can cause a traffic interruption if a virtual machine is moved from one hypervisor to another. Decide whether tighter security (Strict connection tracking) or preservation of the session (Loose connection tracking) is more important.

   Note

   You cannot use Security Group elements in Access rules.

7) Click **Save**.

Configuring NSX-V integration in the NSX Proxy

You must configure NSX-V integration for use with the Forcepoint NGFW in the NSX Proxy web interface.

Configure NSX-V for use with Forcepoint NGFW in the NSX Proxy web interface

You must register the SMC with NSX-V and upload the Forcepoint NGFW engine image for the VSS Container to the image catalog in the NSX Proxy web interface.

Before you begin

These tasks are done by the SMC administrator.

Before you start configuring the NSX-V for use with the Forcepoint NGFW, the following tasks must have been completed:

- The NSX service has been installed on the Management Server.
- The SMC API has been configured in the Management Client component of the SMC.

Make sure that you have the following information available:

- the Management Server's IP address and the listening port for the Management Server
- the authentication key for the API client
- the IP address of the NSX Server and the listening port for the NSX Server

Steps

1) Go to https://support.forcepoint.com/Downloads, enter your logon credentials, then navigate to the appropriate product and version.

2) Download the Forcepoint NGFW engine image for the VSS Container.

3) Open a command prompt, open a connection to a Management Server CLI, then change to the sgadmin user (for example, by using the sudo command).

4) Install the virtual environment for the NSX Proxy service.

   a) (Recommended) To create a copy of your configuration, enter the following command:

   ```
   cp -rp nsx nsx-production
   ```

   The <SMC installation directory>/usr/local/forcepoint/smc/data/plugins/nsx directory is overwritten when you upgrade the SMC. Creating a copy of your configuration allows you to restore the configuration after you upgrade the SMC.

b) Locate the README.md file in the <SMC installation directory>/usr/local/forcepoint/smc/data/plugins/nsx directory.

c) Run the installation commands listed in the README.md file.

5) On the command line of the Management Server, enter the following commands to start the NSX Proxy service:

```
. nsxproxy_venv/bin/activate
cd /usr/local/forcepoint/smc/data/plugins/nsx
python server.py --smc_address <Management_Server_IP_address> --smc_apikey
 <API_key_of_API_client> --nsx_address <NSX-V_server_IP_address>
```

Tip

Use `--help` to see information about all the available options.

6) (Only before logging on to the NSX Proxy web interface for the first time) Change the password for the account that you use for logging on to the NSX Proxy web interface.

a) Log on to the Management Client with the user name and the password that the SMC administrator provided.

b) In the Management Client, select ☰ **Menu** > **System Tools** > **Password** > **Change Password**.

c) In the **Old Password** field, enter your current password.

d) In the **New Password** field, enter your new password.

e) In the **Confirm Password** field, enter the new password again, then click **OK**.

7) Log on to the NSX Proxy web interface.
Use the user name and the password of the VMware administrator account that was created in the SMC.

8) On the **Images** tab, upload the Forcepoint NGFW .zip file that you want to use as the VSS Container image.
The image is added to the list of available Forcepoint NGFW images.

9) On the **Managers** tab, create a service that represents the VSS Container Firewall in NSX-V.

- When you create the service, select the Firewall Policy that you created in the Management Client component of the SMC as the VSS Container Policy.

  Note

  The NSX Proxy service automatically provides a list of the available Firewall Policies in Forcepoint NGFW through the SMC API.

- In the **Version** list, select the VSS Context Firewall engine image that you want to use.

Result

Forcepoint NGFW has been integrated with NSX-V.

Configuring NSX-V integration in vSphere

You must finalize the NSX-V integration with Forcepoint NGFW in vSphere.

These tasks are done by the VMware administrator.

To configure the NSX-V integration in vSphere, you must complete the following general steps:

1) Create a Forcepoint NGFW deployment for NSX-V.

2) Create the Security Groups and Security Policies, then assign a Security Policy to each Security Group.

Create a Forcepoint NGFW deployment for NSX-V in vSphere

You must create a Forcepoint NGFW deployment for NSX-V in vSphere.

Before you begin

You have created a service for the Forcepoint NGFW VSS Container in the NSX Proxy web interface.

Steps

1) Log on to vSphere.

2) Browse to **Home** > **Networking & Security**.

3) Select **Service Definitions**, then make sure that the service for the Forcepoint NGFW VSS Container is included in the list of services.

4) Select **Installation and Upgrades**, then install the Forcepoint NGFW VSS Container image on the cluster of virtual machines that are used as the VSS Container nodes.

   a) Select the service.

   b) Select the cluster of virtual machines.

   c) As several virtual machines share the same data storage, select a shared data storage in the **Datastore** list.

CAUTION

DHCP is not supported in vSphere when you integrate NSX-V with Forcepoint NGFW.

d) In the **IP assignment** column, click **Change**, select **Use IP Pool**, then create a new IP pool or select an existing IP pool in the list.

e) Click **Finish** to start the installation.

Result

- The Forcepoint NGFW VSS Container image is installed on the ESX hosts.
- After the installation of the VSS Container image is complete, elements for the VSS Container and VSS Container nodes are automatically created in the SMC. Ask the SMC administrator to verify that the elements become available in the Management Client.

Verify SMC elements in the Management Client

Confirm that a VSS Container and VSS Container nodes are present in the Management Client after the Forcepoint NGFW image has been deployed on the virtual machines.

Note

This task is done by the SMC administrator.

The VSS Container shows up immediately after the Forcepoint NGFW image has been deployed on the virtual machines. The VSS Container nodes appear within a few minutes.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Configuration**.

2) Double-click the VSS Container.

3) In the navigation pane on the left, click **VSS Container Nodes** and verify that they appear as expected.

Result

- An initial configuration is automatically transferred to the VSS Container nodes.
- The Firewall Policy that was selected for the NSX Proxy service in the NSX Proxy web interface is automatically installed on the VSS Container nodes.

Assign a Security Policy to each Security Group in vSphere

Create the Security Groups and associate a Security Policy and traffic intercept rules for each VSS Context Firewall.

Note

You can apply a Security Policy to more than one Security Group, but each Security Group can have only one Security Policy.

Steps

1) In vSphere, create the Security Group.

2) Configure the Security Policy, including rules to intercept the applicable inbound and outbound traffic.
   - Use Network Introspection Services in the Security Policy. Make sure that **Redirect to service** is selected in the Network Introspection Service.
   - When you create the Network Introspection Services, you also the select the Layer 2 Firewall Policies for the VSS Context Firewalls.
   - Create a separate Network Introspection Service for inbound and outbound traffic. For inbound traffic, select **Any** as the Source and **Policy's Security Group** as the Destination. For outbound traffic, select **Policy's Security Group** as the Source and **Any** as the Destination.

3) Assign a Security Policy to the Security Group.

Result

- NSX-V creates a Security Group element and VSS Context Firewall in the SMC to represent the binding of the Security Group and Security Policy. Traffic now passes to the VSS Context Firewall. However, the Layer 2 Firewall Policy is not applied to the VSS Context Firewall until the Firewall Policy on the VSS Container is refreshed.
- If there are enough unbound licenses in the SMC, licenses are automatically bound to the VSS Container and the VSS Context Firewalls.

Refresh the VSS Container Firewall Policy

By default, the NSX proxy refreshes the Firewall Policies on the VSS Containers automatically. If necessary, the SMC administrator can manually refresh the Firewall Policy on the VSS Container to upload the Layer 2 Firewall Policy to the VSS Context Firewalls.

Note

This task is done by the SMC administrator.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Configuration**.
2) Right-click the VSS Container, then select **Current Policy** > **Refresh on VSS Container and VSS Context Firewalls**.
3) Click **OK**.
4) Review the policy upload history.
   If the policy upload to a node failed, work with the network administrator to determine the cause.

Result

The rules are enforced against traffic in the SDDC.

Maintenance for NSX-V associated elements

Using NSX-V to manage engines and policies requires some processes that are different than the normal Forcepoint NGFW workflow.

Filter logs by virtual machine

You can filter log data to review events for the virtual identifier (VM ID). A VM ID is assigned in the virtualization platform to each virtual machine.

When the network administrator sends you the VM ID, you can use it to review the logs related only that virtual machine. Alternatively, if you notice a particular VM ID sending suspicious traffic, you can send the VM ID to the network administrator for investigation.

You can report traffic patterns to the network administrator that might indicate that a virtual machine is compromised. The virtual machine can be shut down or quarantined until the issue is resolved.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Logs**.
2) Create the log filter.
   a) In the **Query** pane, verify that **Security Engine** is selected from the drop-down list.
   b) On the **Filter** tab, select **Select** from the **New** drop-down list.

c) In the **Select Filter** dialog box, browse to **Fields** > **All Fields** > **Virtual Machine ID**.

d) Click **Select**.
An entry called **Virtual Machine ID** appears in the **Query** pane.

3) Define the filter properties

a) Right-click **Virtual Machine ID**, then select **Properties**.

b) From the **Comparison** drop-down, select **in**.

c) (Optional) In the **String** field, enter the specific VM ID.

d) Click **Add**.

e) Click **Apply**.

4) (Optional) Restrict the time range.

a) Select the time parameter from the drop-down list.

b) Select the start and end date.

5) Click **Apply**.

Troubleshoot engines deployed with NSX-V

A VSS Container node can display a failure for various reasons, such as failure to install policy, network connectivity loss, lack of licensing, or the policy being out of synchronization.

In the Management Client, check the VSS Container node color for status. You can also check the audit entries for failed policy upload entries.

Steps

1) In the Management Client, verify that all VSS Container nodes have been licensed.

2) Try refreshing the VSS Container policy.
If you are trying to upload a policy when NSX-V is performing an automated task, there might be a conflict. Waiting a few moments and trying the refresh again is likely to resolve the issue.

3) (Network administrator) Check for and resolve any networking issues.

4) In the NSX Proxy web user interface, update the existing Service and refresh the VSS Container policy.

5) In the Management Client, refresh the VSS Container policy.

Delete policies used in a virtualization system

To prevent a Firewall or Layer 2 Firewall Policy from being available in vSphere, you must permanently delete the policy.

Steps

1) (Network administrator) In vSphere, disassociate the policy from any Security Groups.

2) In the Management Client, make sure that there are no object references to the policy.

3) Move the policy to the Trash.
   a) Right-click the policy, then select **Delete**.
   b) Click **Yes**.

4) Delete the policy from the Trash.

   Important

   If the policy is not permanently deleted, it is still available in vSphere.

   a) Select **Menu** > **View** > **Panels** > **Trash**.
   b) Right-click the policy, then select **Delete**.
   c) Click **Yes**.
   The policy is deleted.

Delete obsolete Security Group elements

When Security Groups are deleted from vSphere but still referenced in the SMC, the Security Group element remains in SMC. We recommend periodically cleaning up the list of Security Group elements.

Security Groups that are obsolete are noted with a changed icon:

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, select **Configuration**.

2) Browse to **Network Elements** > **Security Groups**.

3) Right-click obsolete Security Groups, then select **Delete**.

Tip

You can select multiple Security Groups with **Ctrl** and **Shift**.

A confirmation dialog opens showing any references to the Security Group.

4) Click **Open References** to remove any references.

5) Delete the Security Group.

Upgrade VSS Context Firewall engines

To upgrade VSS Container Firewall engines, you must first upgrade the engine image in the Service definition in the NSX Proxy web interface, then upgrade the VSS Context Firewalls in vSphere.

When you upgrade the VSS Container Firewall engines, the configuration of the VSS Context Firewalls does not change. The Security Policy and Security Group assignments also remain unchanged.

Steps

1) (SMC administrator) Provide the upgraded engine image to the VMware administrator.

2) (VMware administrator) In the NSX Proxy web interface, upgrade the engine image in the Service.
   a) Switch to the **Managers** tab, then click the name of the Service.
   b) Click **Upgrade**, then select the engine image that you want to upload.
   c) Click **OK**.

3) In vSphere, upgrade the VSS Context Firewalls.
   a) Browse to **Home** > **Networking & Security**.
   b) Select **Service Definitions**.
   c) Select **Installation and Upgrades**.
   d) Switch to the **Service Deployments** tab.
   e) Select the Service to be upgraded, the click **Upgrade**.

CAUTION

When the engine image is upgraded in vSphere, the Service stops working for the duration of the upgrade.

The VSS Container Firewalls are upgraded, then the NSX Proxy automatically refreshes the Firewall Policy on the VSS Container and the Layer 2 Firewall Policy on the VSS Context Firewalls.

4) (SMC administrator) When the VMware administrator informs you that the Service definition has been updated and the VSS Context Firewalls have been upgraded, verify that the Firewall Policy on the VSS Container and the Layer 2 Firewall Policy on the VSS Context Firewalls have been refreshed.

Note

By default, the NSX Proxy refreshes the Firewall Policies on the VSS Containers automatically. If necessary, you can manually refresh the Firewall Policy on the VSS Container to upload the Layer 2 Firewall Policy to the VSS Context Firewalls.

Restore an SMC backup

Restoring an SMC backup requires coordination between the SMC administrator and the VMware administrator to ensure that SMC and NSX-V are synchronized and error free.

Before you begin

Create an SMC backup.

Tip

We recommend that you back up the Management Server frequently to make sure that a recent backup is always available.

These high-level tasks describe the restoration process for engines deployed with NSX-V.

Steps

1) Restore the SMC backup.

2) Remove any Security Group elements that are not associated with a VSS Container.

Important

If there are Security Group elements without a VSS Container, they can cause synchronization job failures in NSX-V.

3) (VMware administrator) If the SMC backup was restored because the SMC has stopped working correctly, refresh the Service definition in the NSX Proxy web interface.

   a) Switch to the **Managers** tab, then click **Sync Service**.

   b) Select the Service, then click the Refresh icon (blue arrow) in the top right corner of the **Deployments** dialog box.

4) (VMware administrator) Resolve any errors or job failures.

5) (SMC administrator) Check the Firewall Policy for the VSS Container and the Layer 2 Firewall Policy for the VSS Context Firewalls for any rule changes made since the SMC backup was created.

Note

By default, the NSX Proxy refreshes the Firewall Policies on the VSS Containers automatically. If necessary, you can manually refresh the Firewall Policy on the VSS Container to upload the Layer 2 Firewall Policy to the VSS Context Firewalls.

Examples of using VSS Context Firewalls in virtual networks

NSX-V handles the initial provisioning of security services to network components, then the day-to-day operations are similar to normal firewall administration.

These examples highlight possible use cases.

Example: Securing east-west traffic

Controlling traffic within the SDDC, or even protecting one virtual machine from another, can be done within a single policy shared with multiple Security Groups.

Your company uses various virtual machines as their front-end web servers, back-end business logic servers, database servers, and promotional email servers to support an external website. The site allows customers to receive data about services the company provides and for the company to send emails with more information and offers. These virtual machines are in groups based on their services, but might exist within the same hypervisor. For example, a hypervisor with access to the Internet might contain an email sender and a front-end web server. They want strict control over what systems are able to send data, such as emails, to outside the network but allow the virtual machines to communicate within the network as needed.

Use these high-level steps to control what traffic is allowed or blocked on each port, based on the virtual machine grouping.

1) Create a Layer 2 Firewall Policy without rules.

2) (Network administrator) Create a Security Group for each group of virtual machines: Web Server, Back-End, Database, and Email. These groups correspond to Security Group elements in the SMC.

3) (Network administrator) Associate the four Security Groups with the empty Security Policy.
Four Security Group elements appear in the SMC.

4) Fill the empty Layer 2 Firewall Policy with the following rules and using the Security Group elements as the Source or Destination:

   a) Allow web traffic from External to Web Server.

   b) Allow back-end traffic from Web Server to Back-End.

   c) Allow database traffic from Back-end to Database.

d) Allow email-triggering traffic from Back-End to Email.

e) Allow email from Email to External.

f) Discard all.

5) Refresh the policy to apply it to all firewalls protecting those groups.

This policy allows these separate groups of virtual machines to be protected from each other within a single policy, regardless of what hypervisor they exist on. Any traffic not defined by the groups is denied and external exposure is limited.

Example: Moving virtual machines to a different Security Group

Moving virtual machines to new hosts can be done with minimal disruption because the security service is associated with the virtual machine, regardless of the networking changes.

The virtual machine was previously deployed within Security Group A. The group has a normal policy allowing inbound and outbound connections. An alert indicates that a particular virtual machine might be compromised. To protect company data while the incident is investigated, the affected virtual machine is moved to Security Group B with a more restrictive policy that only allows incoming SSH connections and enhanced logging to gather forensic data.

Use these high-level tasks to move virtual machines to a different Security Group, which automatically uses the Security Policy associated with the new group.

1) Notify the network administrator to move the virtual machine to Security Group B.

2) Take steps to address the issue.

3) Notify the network administrator to move the virtual machine back to Security Group A.

After the cause of the attack is addressed, the virtual machine is returned to a normal policy.

Example: Dynamically updating security services

When the Layer 2 Firewall Policy is updated and the policy refreshed in the SMC, it results in an update to every virtual machine in every VSS Context Firewall associated with that Layer 2 Firewall Policy. These simultaneous updates allow for a consistent application of changes with minimal time investment.

The internal site-specific database servers are on virtual machines that were previously deployed and grouped. Your company is adding a module on the database that requires a security update to allow traffic on a specific port.

Use these high-level tasks to reconfigure groups and policies, which means that changing needs can be met quickly.

1) Update the Layer 2 Firewall Policy.

2) Refresh the VSS Container policy in the Management Client.

The database servers now have a current Security Policy.

Example: Deploying network components to existing Security Group

Any new components added to a Security Group are protected under the established Security Policy and the associated VSS Context Firewall.

You have already set up and configured the policies needed for your environment. Later, an extra ESXi server is needed to add capacity for the growing network.

Use these high-level tasks to add a VSS Context Firewall to a new ESXi server in a VMware cluster.

1) (Network administrator) Create an ESXi host to add to the VMware cluster, which adds it to the Security Group and the associated Security Policy. The ESXi host is now included in the existing Security Group in SMC.

2) You receive notification from the network administrator that there has been a change.

3) Refresh the VSS Container policy in the Management Client.

The added ESXi server enforces the established Security Policy.

Example: Phased implementation of policy changes

Virtual machines can be assigned to different Security Groups as needed to apply a change in policy.

You need to make a major policy change to production firewalls that receive live traffic. In this group of firewalls and hosts, there are some that are less critical for day-to-day operations. You want to test policy changes on live traffic to verify that rule changes do not have a negative impact.

Use these high-level tasks to test a new policy in a phased approach before applying the policy to all VSS Context Firewalls in a Security Group.

1) Make a copy of the existing Layer 2 Firewall Policy with a new name and make any necessary changes.

2) (Network administrator) Create a test Security Group with only a few virtual machines in it.

3) (Network administrator) Associate the new Security Policy with the new test Security Group.
A new Security Group element is created in SMC.

4) Refresh the policy to apply it to the test group.

5) Testing of the new policy is completed and any necessary adjustments are made.

6) (Network administrator) Associate the Security Policy with the production Security Group.

7) (Network administrator) Move the test virtual machines back to the production group.

8) Refresh the policy to apply it to all production firewalls in the group.

The test policy is verified on a select group of virtual machines and has a greater chance of success when these changes are applied to the entire group.

Published 14 September 2020