Configuring Security for VXLAN EVPN Fabrics, Release 12.2.2

Table of Contents

New and Changed Information . . . 1
Understanding Security for VXLAN EVPN Fabrics . . . 2
Guidelines and Limitations . . . 2
Configuring Security on VXLAN EVPN Fabrics . . . 4
Enable the Security Groups Feature . . . 4
Navigate to the Security Page . . . 5
Import or Export Security Configurations . . . 5
Guidelines and Limitations for Importing or Exporting Security Configurations . . . 6
Configure Security Groups . . . 7
About Security Groups . . . 7
Create a Security Group . . . 7
Create a Security Contract . . . 9
Associate a Security Contract Within a VRF . . . 10
Disassociate a Security Contract from a VRF . . . 11
Create a Security Protocol . . . 11
Deploy Security Groups . . . 14
Monitor the Security Configurations . . . 14
Copyright . . . 15

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
NDFC release 12.2.2	Security for VXLAN EVPN fabrics	The ability to configure security for VXLAN EVPN fabrics is introduced.
NDFC release 12.2.2	Security for VXLAN EVPN Multi-Site fabrics	The ability to configure security for VXLAN EVPN Multi-Site fabrics is introduced.

Understanding Security for VXLAN EVPN Fabrics

In traditional data center environments, the application/workload security is often implemented at the perimeter or the north-south boundary where the users from outside of the datacenter fabric enter. This is often implemented using perimeter firewalls and other security inspection devices. However, this approach is not effective against the more recent, advanced nature of attacks, where the attack surface spans the entire datacenter including the east-west/north-south flows.

Using micro-segmentation with security groups and security group access control lists (ACLs), this feature can provide an effective solution for this problem. With micro-segmentation, organizations can provide application-specific policies that specify how the application workloads communicate, regardless of where these applications reside within the network.

Guidelines and Limitations

Following are the guidelines and limitations when configuring security for VXLAN EVPN fabrics.

- The security groups feature is supported in the following areas:
  - Only on the following family of Cisco Nexus 9000 switches:
    - FX3
    - GX
    - GX2
  - For both VXLAN EVPN standalone and Multi-Site fabrics. However, the monitoring function described in Monitor the Security Configurations is only available for VXLAN EVPN standalone fabrics or child fabrics within a VXLAN EVPN Multi-Site fabric; the monitoring function is not supported for the parent fabric of a VXLAN EVPN Multi-Site fabric.
  - Only in fabrics with an IPv4 underlay.
  - Only in fabrics where the **Overlay Mode** is set to **cli**. To determine the **Overlay Mode** setting for your fabric:
    1. Navigate to **Manage > Fabrics**.
    2. Click the button next to the appropriate fabric, then click **Actions > Edit Fabric**.
    3. Click the **Advanced** tab.
    4. Locate the **Overlay Mode** field.
    5. Change the setting to **cli**, if necessary, then click **Save**.
- The security groups feature is *not* supported in the following areas:
  - With PVLAN
  - With change control
  - If the security groups feature is enabled on a VXLAN EVPN fabric, you cannot import switches into that fabric if those switches are configured with **Preserve-Config=Yes**
- Switches must be running on NX-OS version 10.4(3)F or later.
- If you enable the security groups feature in a parent VXLAN EVPN Multi-Site fabric, only child

fabrics with the security group feature enabled will be allowed to join in this VXLAN EVPN Multi-Site fabric. In addition, all other security group functions, such as creating a security group or associating a contract, is not allowed at the child fabric level and must be configured at the parent fabric level instead.

- Security group actions are allowed for standalone VXLAN EVPN fabrics in the **Topology** window, but you cannot perform any security group actions in the **Topology** window for a VXLAN EVPN Multi-Site fabric or if the fabric is part of a VXLAN EVPN Multi-Site fabric.
- You can assign security groups to VMs if the VMM Visualizer feature is enabled in **Feature Management**. For more information, see the section "Virtual Infrastructure" in About Fabric Overview for LAN Operational Mode Setups.

Configuring Security on VXLAN EVPN Fabrics

Follow these procedures to configure security on VXLAN EVPN fabrics using security groups.

- Enable the Security Groups Feature
- Navigate to the Security Page
- Import or Export Security Configurations
- Configure Security Groups
- Create a Security Contract
- Associate a Security Contract Within a VRF
- Disassociate a Security Contract from a VRF
- Create a Security Protocol
- Deploy Security Groups
- Monitor the Security Configurations

Enable the Security Groups Feature

To enable the security groups feature on a specific VXLAN EVPN fabric:

1. Navigate to that fabric's **Edit Fabric** page.
    - If you are in the main **Fabrics** page (**Manage > Fabrics**), click the button next to the configured VXLAN EVPN fabric where you want to set up security, then click **Actions > Edit Fabric**.
    - If you are in the **Overview** page for a VXLAN EVPN fabric, click the topmost **Actions** dropdown, then choose **Edit Fabric**.

    The **Edit Fabric** for this fabric appears, with the **General Parameters** tab selected by default.
2. Click the **Security** tab.
3. Enable the security groups feature.
    - If you are in a standalone fabric, click the **Enable Security Groups** checkbox.
    - If you are in a parent VXLAN EVPN Multi-Site fabric, in the **Enable Security Groups** field, choose the **strict** option to enable the security groups feature at the parent fabric level. Only child fabrics with the security group feature enabled will be allowed to join in this VXLAN EVPN Multi-Site fabric if this is enabled at the parent fabric level.

    

    You cannot enable the security group feature in the child fabric under a VXLAN EVPN Multi-Site fabric. You can only enable the security group feature in a parent VXLAN EVPN Multi-Site fabric.
4. In the **Enable Security Groups** to enable this feature for this VXLAN EVPN fabric.
5. Click **Save**.

    The following banner message is displayed in VRFs, Networks and Security tabs:

> Security Groups feature is enabled but not yet operational. Please perform Recalculate and Deploy to operationally enable it.

All the actions in these tabs are disabled until you perform a **Recalculate and Deploy**. For security groups in the VXLAN EVPN Multi-Site fabric, perform the **Recalculate and Deploy** action on the parent fabric as well as on all the child fabrics.

When you first perform a **Recalculate and Deploy**, the following events occur:

- system routing template-security-groups will be deployed
- feature security-group deployment will result in failure, where a pop up will appear, asking you to reload the required leaf switches.

Navigate to **Manage > Inventory > Switches** and select those switches, then click **Actions > Reload**. The reload will ensure that the system routing template gets applied. You can verify this by entering these commands on the switch:

switch# show system routing mode

Configured System Routing Mode: security-groups Support

Applied System Routing Mode: Security-Groups Support

Once the switches have reloaded and the discovery status is OK, then you should be able to deploy any security group intent.

Navigate to the Security Page

1. In the main **Fabrics** page, double-click the configured VXLAN EVPN fabric where you have enabled the security groups feature, as described in Enable the Security Groups Feature.

   The **Overview** window for this VXLAN EVPN fabric appears.

2. Click the **Security** tab.

   The **Security** window appears, with the **Groups** tab selected by default and any configured security groups listed.

If you see the message Security Groups feature is disabled in this window, follow the instructions in Enable the Security Groups Feature to enable the security groups feature.

Import or Export Security Configurations

Once you have completed security configurations using the procedures provided in this article, you can then export those security configurations to a .csv file, and then import the .csv file with those configurations at a later date, if necessary.

You can export and import .csv files with security configurations in the following areas in the main **Security** page:

- **Groups**
- **Associations**
- **Contracts**
- **Protocols**

In any of these areas:

- To export a security configuration, select that configured item (for example, in **Groups**, select the configured security group), then click **Actions > Export**.

  A .csv file with that security configuration is downloaded to your system.

  

  - Exporting the default security group is not supported.
  - You can also download an empty .csv template by clicking **Actions > Export** without selecting any configured items in that page.
  - When you export a security configuration in the **Groups** area, two .csv files are exported: one .csv file that contains the IP selectors, and another .csv file that contains the network selectors.

- To import a security configuration, click the appropriate tab in the main **Security** page and click **Actions > Import**, then either drag and drop the .csv file with the security configurations that you want to import, or navigate to the appropriate area on your system and select the .csv file with the security configurations that you want to import.

  

  When importing a security configuration in the **Groups** area, you must import the IP selectors and network selectors one after another. The order that you import them does not matter.

Guidelines and Limitations for Importing or Exporting Security Configurations

- Importing a security configuration will only create a new configuration. You will not import a security configuration to update an existing configuration.
- If a security group already exists with one or more IP selectors, then importing the IP selector .csv file will not update the security group. This guideline also applies to network selectors.

  If a security group exists with IP selectors but without any existing network selectors, then importing the network selector .csv file will add the network selectors to the group and will not alter the IP selectors that were already in the security group. This guideline also applies if a security group exists with network selectors but no IP selectors and you import an IP selector .csv file.

- When importing contracts, ensure that the respective security protocols that are defined in the .csv file already exist; otherwise, those entries will not be imported.
- When importing an association .csv file, ensure that the respective source groups, destination groups, contracts, and VRFs that are defined in the .csv file already exists; otherwise, those entries will not be imported.

Configure Security Groups

The following topics provide the necessary information to configure security groups:

- About Security Groups
- Create a Security Group

About Security Groups

A security group is a security construct that has certain match criteria to define which endpoints belong to that security group, and uses contracts to define the security stance. The match criteria are called the selectors, which you will use when configuring a security group. You can configure selectors under a fabric with a variety of matching criteria to classify the endpoints that belong to the security group.

The following selector options are available when configuring a security group:

- **IP Selectors**: An IP selector classifies endpoints to a security group based on IP address or IP subnet. You can configure a host IP address to match a specific endpoint or you can configure a subnet to match multiple IP addresses within the subnet.
- **Network Selectors**: A network selector classifies endpoints to a security group based on a configured network. The network translates into a VLAN match statement in a switch, where a VLAN is configured on the switch based on the network attachment. Only Layer 3 networks are supported for network selectors.
- **VM Selectors**: A VM selector associates a security group with a virtual machine, where you assign a VM UUID or VM VNIC port to a security group, which then translates to a VRF or IP address match statement in the switch. For more information, see the section "Virtual Infrastructure" in About Fabric Overview for LAN Operational Mode Setups.

If a VM selector is marked as **Inactive** in the **Groups** page, that indicates that the VM endpoint associated with the security group no longer exists. In these cases, the VM endpoint will not be visible in the **Virtual Infrastructure** page. This can happen if the VM gets deleted or if the vCenter becomes unmanaged. To address this situation, you must explicitly remove the VMM inactive endpoints by clicking on the delete icon next to the endpoints created by the VMM by clicking **Actions > Edit** in the **Groups** page.

Create a Security Group

Rather than creating a security group from scratch, you can import already-configured security group configurations, if necessary. See Import or Export Security Configurations for more information.

1. Navigate to the **Security** page, if you're not there already.

   See Navigate to the Security Page.

2. With the **Groups** tab selected, click **Actions > Create Security Group**.

   The **Create Security Group** window appears.

3. (Optional) In the **Name** field, change the name for this security group, if necessary.

   The name for the security group in the **Name** field is automatically populated with the configured group name prefix (as shown in **Fabric Properties > Resources > Security Group Name Prefix**), concatenated with an automatically generated group ID (provided in the **Security Group Tag ID** field below). You can override this automatically generated security group name in this field, if necessary.

4. (Optional) In the **Security Group Tag ID** field, enter a tag ID for this security group, if necessary.

   Each security group has a unique tag ID, which is automatically populated from a pool; however, you can overrride the automatically-generated tag ID in this field, if necessary.

5. Determine what type of selector you want to use to create the security group.
   - To create a security group using IP selectors, go to Create a Security Group Using IP Selectors.
   - To create a security group using network selectors, go to Create a Security Group Using Network Selectors.

Create a Security Group Using IP Selectors

1. Click the **IP Selectors** tab.
2. In the **IP Selectors** area, determine how you want to add IP selectors for this security group.
   - If you want to perform a bulk add of the IP selectors for this security group, click **Bulk Add**, then enter the necessary information in the **Bulk Add** window. Enter a whitespace or comma-separated list of IPv4, IPv6, IPv4/netmask, or IPv6/prefix entries to associate with this IP selector in this case.
   - If you want to add individual IP selectors for this security group, click **+ Add IP Selector**, then make the necessary configurations.

Field	Description
Type	Select the type of IP selector that you want to use for this security group. Options are: • **Connected Endpoints**: Choose this type of IP selector to add a policy tag to an endpoint IP address or IP subnet. The tag can then be used by a tag selector to associate the endpoint IP address or IP subnet to a security group. • **External Subnets**: Choose this type of IP selector to create an IP subnet selector for a security group for networks or hosts that are learned externally and/or that are statically configured.
VRF	Select the VRF that you want to associate with this IP selector, or click **+ Create VRF** to create a new VRF for this IP selector.
IP/Mask	Enter an IPv4, IPv6, IPv4/netmask, or IPv6/prefix entry to associate with this IP selector. The IPv4/netmask or IPv6/prefix will be corrected automatically based on the provided netmask and prefix value.

Accept these updates after you have made the necessary configurations for the IP selector:

- If you performed a bulk add for the IP selector, click **Add** in the **Bulk Add** window.
- If you added an individual IP selector, click the checkbox at the end of the row. Repeat these steps to add additional individual IP selectors, if necessary.

3. Click **Create**.

Create a Security Group Using Network Selectors

1. Click the **Network Selectors** tab.
2. In the **Network Selectors** area, click **+ Add Network Selector** to add individual network selectors for this security group, then make the necessary configurations.

Field	Description
VRF	Select the VRF that you want to associate with this network selector, or click **+ Create VRF** to create a new VRF for this network selector.
Network	Select the network that you want to associate with this network selector, or click **+ Create Network** to create a new network for this network selector. If you are creating a new network for this network selector, verify that you select the correct VRF in the **Create Network** page.

3. Click the checkbox at the end of the row to accept these updates after you have made the necessary configurations for the network selector.

   Repeat these steps to add additional individual network selectors, if necessary.

4. Click **Create**.

Create a Security Contract

Rather than creating a security contract from scratch, you can import already-configured security contract configurations, if necessary. See Import or Export Security Configurations for more information.

Service contracts are logical constructs in NDFC that represent a set of Security Rules where each rule is comprised of Direction, Action, and Protocol. Contracts are associated with Security Groups within a VRF. These associated service contracts are applied to switches where the VRF is attached in the NDFC.

1. Navigate to the **Security** page, if you're not there already.

   See Navigate to the Security Page.

2. Click the **Contracts** tab.

   A table with all of the existing security contracts is displayed.

3. Click **Actions > Create Security Contract**.

The **Create Security Contract** window appears.

4. In the **Contract Name** field, enter a name for this security contract.
5. (Optional) In the **Description** field, enter a description for this security contract.
6. Below the **Rules** table, click **+ Add Rule**, then make the necessary configurations.

Field	Description
Direction	Select the direction for this rule in the security contract. Options are: • bidirectional • unidirectional
Action	Select the action for this rule in the security contract. Options are: • permit • permit log • deny • deny log
Protocol	Select a protocol for this rule in the security contract, or click **+ Create Security Protocol** to create a new security protocol for this security group. See Create a Security Protocol for more information.
Match Summary	Verify the information shown in the match summary for this rule in the security contract.

Click the checkbox at the end of the row to accept these values.

7. Click **Create**.

Associate a Security Contract Within a VRF

Rather than creating a security association from scratch, you can import already-configured security association configurations, if necessary. See Import or Export Security Configurations for more information.

1. Navigate to the **Associate Contract** page.

   You can access the same **Associate Contract** page through any of these navigation paths:

   - **Groups > Actions > Associate Contract**
   - **Associations > Actions > Create Security Association**
   - **Contracts > Actions > Associate Contract**

2. In the **Associate Contract** page, make the necessary configurations to associate a security contract with a Source Group and Destination Group within a VRF.

Field	Description

VRF	Select the VRF that you want to associate with this security contract, or click **+ Create VRF** to create a new VRF for this security contract.
Source Group	Select the source security group that you want to associate with this VRF in this security contract, or click **+ Create Security Group** to create a new source security group to associate with this VRF in this security contract. See Create a Security Group for more information.
Contract	Select the security contract that you want to associate with this VRF, or click **+ Create Security Contract** to create a new security contract for this VRF. See Create a Security Contract for more information.
Destination Group	Select the destination security group that you want to associate with this VRF in this security contract, or click **+ Create Security Group** to create a new destination security group to associate with this VRF in this security contract. See Create a Security Group for more information.

3. Click **Save**.

Disassociate a Security Contract from a VRF

Follow these procedures if you want to disassociate a security contract from a VRF for any reason:

1. Navigate to the **Security** page, if you're not there already.

   See Navigate to the Security Page.

2. Click the **Contracts** tab.
3. Click **Actions > Disassociate Contract**.

   The slide-in pane **Disassociate Contract From:** page appears.

4. Locate the row with the VRF that you want to disassociate the security contract from, then click the trashcan icon in that row.

   This action deletes the security contract association from this VRF. It does not delete the security contract or any security group.

You can also disassociate a security contract by clicking the **Associations** tab and selecting the association entries, then clicking **Actions > Delete**.

Create a Security Protocol

Rather than creating a security protocol from scratch, you can import already-configured security protocol configurations, if necessary. See Import or Export Security Configurations for more information.

1. Navigate to the **Security** page, if you're not there already.

   See Navigate to the Security Page.

2. Click the **Protocols** tab.

A table with all of the existing security protocols is displayed.

3. Click **Actions > Create Security Protocol**.

   The **Create Security Protocol** page appears.

4. In the **Name** field, enter a name for this security protocol.
5. (Optional) In the **Description** field, enter a description for this security protocol.
6. In the **Match All Traffic** field, check the box to enable this feature.
7. In the **Match Protocols** area, enter the necessary information to filter match protocols by attribute.
   a. Choose the first part of the string to use for the filter using any of these values:
      - Type
      - IP Protocol/Options
      - Source Port Range
      - Destination Port Range
      - Fragments Only
      - Stateful
      - TCP Session Rules
      - DSCP
   b. Choose the next part of the string using any of these values:
      - == (include)
      - != (doesn't include)
      - contains
      - !contains (doesn't contain)
   c. Enter a value for the final part of the string to be used to filter match protocols by attribute.
8. Click **Actions > Create Protocol Entry**.

   The slide-in pane **Create Protocol Entry** page appears.

9. Make the necessary configurations to create the security protocol entry.

Field	Description
Type	Select the type of protocol entry that you want to use with this security protocol. Options are: - IP - IPv4 - IPv6
IP Protocol/Options	Select the IP protocol or option that you want to use with this security protocol.

Fragments	This option is available only if you selected **TCP** or **UDP** in the **IP Protocol/Options** field above. Check this box to enable fragmentation functionality for this IP protocol. Fragmentation refers to the process of splitting large packets of data into smaller chunks that can fit into the network's maximum transmission unit (MTU). The receiving host then reassembles the fragments.
Stateful	This option is available only if you selected **TCP** in the **IP Protocol/Options** field above. Check this box to enable stateful functionality for this IP protocol. A process being stateful means that it keeps track of all changes or interactions that happened in the past, and a current process is performed with a context of those previous processes. In this case, TCP keeps track of areas such as the number packets to be transferred, the order of the packets and whether the receiver has received a packet or not. With the **Stateful** option selected, this information is stored as a state in TCP.
Source Port Range	This option is available only if you selected **TCP** or **UDP** in the **IP Protocol/Options** field above. Enter the source port range for this security protocol. You can enter a range in this field, such as 80-90, or a single value, such as 80.
Destination Port Range	This option is available only if you selected **TCP** or **UDP** in the **IP Protocol/Options** field above. Enter the destination port range for this security protocol. You can enter a range in this field, such as 80-90, or a single value, such as 80.
TCP Flags	This option is available only if you selected **TCP** in the **IP Protocol/Options** field above. Select the TCP flags for this security protocol. In the protocol header, TCP uses flags to manage connections and traffic flows. Options are: • **ack**: Acknowledgment. Used to acknowledge the reception of data or synchronization packets. • **est**: Established TCP connections. When this option is selected, other options cannot be selected. • **fin**: Finish. Gracefully terminate the TCP connection. • **rst**: Reset. Immediately terminate the connection and drop any in-transit data. • **syn**: Synchronization. Used to create a TCP connection.
DSCP	Enter the Differentiated Services Code Point (DSCP) for this security protocol. Valid range is 0-63.

10. Click **Add** in the **Create Protocol Entry** page.

You are returned to the **Create Security Protocol** page, with the new security protocol entry added to the table of protocol entries.

11. Click **Create** in the **Create Security Protocol** page.

    You are returned to the **Protocols** page, with the new security protocol added to the table of security protocols.

Deploy Security Groups

Once you have made all the necessary configurations for the security groups, you can now deploy them through either the **Groups** or the **Associations** pages:

- **Groups > Actions > Deploy**
- **Associations > Actions > Deploy**

Monitor the Security Configurations

The monitoring function is only available for VXLAN EVPN standalone fabrics or child fabrics within a VXLAN EVPN Multi-Site fabric; the monitoring function is not supported for the parent fabric of a VXLAN EVPN Multi-Site fabric.

The **Monitoring** screen shows changes between the point when values were previously fetched and the current values. The **Last Updated** column shows the last point when these values were resynchronized. The data is denormalized with contract direction, action, and protocol associations.

1. Navigate to the **Security** page, if you're not there already.

   See Navigate to the Security Page.

2. Click the **Monitoring** tab.

   A table with all the security contract association statistics is displayed.

3. Click **Resync** to resynchronize the table data.

   A status bar appears with the text **Resyncing Table Data**, then the resynchronized data is displayed.

Copyright