Configuring Firewall Policies

This article provides procedures for configuring firewall policies on XE SD-WAN Routers. You provision firewall policies to direct traffic between two zones, which are referred to as a source zone and a destination zone. Each zone consists of one or more VPNs in the overlay network.

In vManage NMS, you configure firewall policies from the Configuration ► Security screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the XE SD-WAN Router.

Configuration Components

For firewall policies, you configure zones and a policy to apply to those zones.

Each zone consists of one or more VPNs in the overlay network. You define a source zone, which identifies the VPNs from which data traffic originates, and a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered (ordered) sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken and policy evaluation on that packet stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the policy sequences, you define a default action to be taken on the packet.

The following figure illustrates the configuration components for firewall policies:

To create a firewall policy, you include the following components in the configuration for a XE SD-WAN Router:
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match portion of the zone-based firewall configuration.</td>
<td>Configuration ► Security ► Custom Options ► Lists ► Data Prefix</td>
<td>policy lists policy zone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Custom Options ► Lists ► Zones</td>
<td></td>
</tr>
<tr>
<td>Numbered sequences of match–action pairs</td>
<td>Sequences establish the order in which the policy components are applied.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule</td>
<td>policy zone-based-policy sequence</td>
</tr>
<tr>
<td>L3/4 Match parameters</td>
<td>Conditions that packets must match to be considered for a data policy.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule ► Match</td>
<td>policy zone-based-policy sequence match</td>
</tr>
<tr>
<td>Actions</td>
<td>Whether to accept or reject matching packets, and how to process matching items.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy ► Sequence Rule ► Action</td>
<td>policy zone-based-policy sequence action</td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy</td>
<td>policy zone-based-policy default-action</td>
</tr>
<tr>
<td>Apply firewall policy to a zone pair</td>
<td>For a firewall policy to take effect, you include it in the definition of a zone pair.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Apply Policy</td>
<td>policy zone-pair</td>
</tr>
</tbody>
</table>
To create an application firewall policy, you include the following components in the configuration for a XE SD-WAN Router:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists</td>
<td>Groupings of related items that you reference in the match portion of the firewall policy configuration.</td>
<td>Configuration ► Security ► Custom Options ► Lists ► Application</td>
<td>policy lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Custom Options ► Lists ► Zones</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Sequence Rule</td>
<td></td>
</tr>
<tr>
<td>Numbered sequences of</td>
<td>Sequences establish the order in which the policy components are applied.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>match–action pairs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Match parameters</td>
<td>Conditions that packets must match to be considered for a security policy.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► Sequence Rule ► Match ► Application/Application Family List</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► Sequence Rule ► Actions ▶ Inspect</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>For a sequence that contains an application or application family list, packets can be inspected. Matching applications are blocked/denied.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► Sequence Rule ► Actions ▶ Inspect</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► Sequence Rule ► Actions ▶ Inspect</td>
<td></td>
</tr>
<tr>
<td>Default action</td>
<td>Action to take if a packet matches none of the match parameters in any of the sequences. By default, nonmatching packets are dropped.</td>
<td>Configuration ► Security ► Add Security Policy ► &lt;Scenario&gt; ► Add Firewall Policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► Sequence Rule ► Actions ▶ Inspect</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration ► Security ► Add Security Policy ► Sequence Rule ► Actions ▶ Inspect</td>
<td></td>
</tr>
</tbody>
</table>
### General vManage Configuration Procedure

To configure firewall policies, use the vManage policy configuration wizard. The wizard is a UI policy builder that lets you configure policy components:

- **Create Lists**—Create lists that group together related items and that you call in the match condition of a firewall policy.
- **Firewall Policy**—Define the match and action conditions of the firewall policy.
- **Apply Configuration**—Define zone pairs.

You must configure all these components to create a firewall policy. If you are modifying an existing firewall, you can skip a component by clicking the Next button at the bottom of the screen. To return to a component, click the Back button at the bottom of the screen.

#### Step 1: Create Lists

To create lists:

1. In vManage NMS, select the Configure ➤ Security screen.
2. In the Title bar, click the Custom Options drop-down.
4. Select the list type to create. The following table describes the lists you can create for firewall policies.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>vManage Configuration</th>
<th>CLI Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply firewall policy to a zone pair</td>
<td>For a firewall policy to take effect, you include it in the definition of a zone pair.</td>
<td>Configuration ➤ Security ➤ Add Security Policy ➤ &lt;Scenario&gt; ➤ Apply Policy</td>
<td>policy zone-pair</td>
</tr>
</tbody>
</table>

---


Created on: Sat, 01 Jun 2019 03:58:13 GMT

Generated by: Anonymous
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Application | 1. In the left pane, click Application.  
2. Click New Application List.  
3. Enter a name for the list.  
4. Select individual applications or application families.  
5. Click Add. |
| Data Prefix | 1. In the left pane, click Data Prefix.  
2. Click New Data Prefix List.  
3. Enter a name for the list.  
4. Enter one or more IP prefixes.  
5. Click Add. |
| Zones | 1. In the left pane, click Zones.  
2. Click New Zone List.  
3. Enter a name for the zone list.  
4. In the Add VPN field, enter the number or numbers of the VPN in the zone. Separate numbers with commas.  
5. Click Add. |

4. To edit, copy, or delete an existing list, click the Edit, Copy, or Trash Bin icon in the Action column.

**Step 2: Start the Policy Configuration Wizard**

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Security screen.  
2. Click Add Security Policy.

The Add Security Policy configuration wizard opens, and various use-case scenarios display.

**Step 3: Select a Use-Case Scenario**

In Add Security Policy, select a policy based on use-case scenarios, or build your own custom policy.

1. Select a security policy use-case scenario. The following table describes the use-case scenarios.
• Compliance – Applies application firewall and intrusion prevention.
• Guest Access – Applies application firewall and URL filtering.
• Direct Cloud Access – Applies application firewall, URL filtering, and DNS Umbrella security.
• Direct Internet Access – Applies application firewall, intrusion prevention, URL filtering, and DNS Umbrella security.
• Custom – Build your own security policy by combining various security policy blocks.

2. Click Proceed to add a firewall policy in the wizard.

---

**Step 4: Configure Firewall Policy**

1. Click the Add Firewall Policy drop-down.

2. To create a new firewall policy:
   1. Select Create New.
   2. Enter a name and description for the policy.

3. To import an existing zone-based firewall policy:
   1. Select Copy from Existing. The Copy from Existing Firewall Policy dialog box appears.
   2. From the Policy drop-down, select the policy to copy.
   3. In the Policy Name field, accept the default name (policy_name_copy) or enter a new name.
   4. In the Policy Description field, enter a description.
   5. Click Copy.
   6. To modify the policy, click the More Actions icon to at the far right of the policy and select Edit. Go to Step 4.

   Otherwise, click Next to move to the next security block in the configuration wizard.

4. In the left pane, click Sequence Rule to create a single sequence in the firewall policy. The Match tab is selected by default.

5. Click a match condition:
   • Source Data Prefix
   • Source Port
   • Destination Data Prefix
   • Destination Port
• Protocol

• Application/Application Family List

You can select and configure more than one match condition in a sequence.

6. Enter the values for the match condition.

   **Note:** If you selected an Application or Application Family List, you must select at least one other match condition.

7. Click the Actions tab.

8. Enter the action or actions to take if the traffic matches.

   **Note:** If a match condition contains an Application or Application Family List, the action must be Inspect. This inspect action is a Layer 4 action. The action for a specific application is block/deny.

9. Click Save Match and Actions to save match-action pair.

10. Repeat Steps 4 through 9 to add match–action pairs to the firewall policy.

11. To rearrange match–action pairs in the policy, drag them to the desired position.

12. To edit, copy, or delete a sequence rule, in the right pane, click the edit, copy, or delete icon to the right of the sequence rule.

13. If no packets match any of the policy sequence rules, the default action is to drop the packets. To change the default action:

    1. Click the Pencil icon.

    2. Change the default action to Inspect or Pass.

    3. Click Save Match and Actions.

---

**Step 5: Apply Policy to a Zone Pair**

1. At the top of the page, click Apply Zone-Pairs.

2. In the Source Zone field, select the zone that is the source of the data packets.

3. In the Destination Zone field, select the zone that is the destination of the data packets.

You can select the same zone for both source and destination. However, if the packet's source and destination use the same physical interface (resulting in U-turn traffic), a firewall session is not created and traffic passes.

4. Click the plus (+) icon to add zone pairs.

5. Click Save.

6. At the bottom of the page, click Save Firewall Policy to save the policy.
7. To edit or delete a firewall policy, in the right pane, click the More Actions icon to the far right of the policy and select the desired option.

8. Click Next to configure the next security block in the wizard.

   • Intrusion Prevention

   • URL Filtering

   • DNS Security

---

**Policy Summary**

1. Enter a name for the security policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

2. Enter a description for the security policy. This field is mandatory.

3. If you configured an application firewall policy, uncheck the "Bypass firewall policy and allow all Internet traffic to/from VPN 0" checkbox in the Additional Security Policy Settings area.

4. Click Save Policy to save the security policy.

---

**Apply a Security Policy to an XE SD-WAN Router**

1. In vManage NMS, select the Configuration ► Templates screen.

2. If you are creating a new device template:
   1. In the Device tab, click Create Template.
   2. From the Create Template drop-down, select From Feature Template.
   3. From the Device Model drop-down, select one of the XE SD-WAN Router.
   4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
   5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

3. If you are editing an existing device template:
   1. In the Device tab, click the More Actions icon to the right of the desired template, and click the pencil icon.
   2. Click the Additional Templates tab. The screen scrolls to the Additional Templates section.
   3. From the Policy drop-down, select the name of a policy that you have configured.
4. Click the Additional Templates tab located directly beneath the Description field. The screen scrolls to the Additional Templates section.

5. From the Security Policy drop-down, select the name of the security policy you configured in the above procedure.

6. Click Create (for a new template) or Update (for an existing template).

Additional Information

Enterprise Firewall with Application Awareness
Configuring Unified Threat Defense