About Distributed Firewall

The Distributed Firewall is a hardware-assisted firewall. It supplements—but does not replace—other security features in the Cisco Application Centric Infrastructure (ACI) fabric such as Cisco Adaptive Security Virtual Appliance (ASAv) or secure zones created by Microsegmentation with Cisco ACI Virtual Edge.

No additional software is required for the Distributed Firewall to work. However, you must configure policies in the Cisco Application Policy Infrastructure Controller (APIC) to work with the Distributed Firewall.

The Distributed Firewall is supported on all Virtual Ethernet (vEth) ports but is disabled for kni-opflex, kni-ave-ctrl dpdk interfaces and for all uplink ports.

Key Features of the Distributed Firewall

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provides dynamic packet filtering (also known as stateful inspection)</td>
<td>Tracks the state of TCP and FTP connections and blocks packets unless they match a known active connection. Traffic from the Internet and internal network is filtered based on policies that you configure in the APIC GUI.</td>
</tr>
<tr>
<td>Is distributed</td>
<td>Tracks connections even if you use vMotion to move virtual machines (VMs) to other servers.</td>
</tr>
<tr>
<td>Prevents SYN-ACK attacks</td>
<td>When the provider VM initiates SYN-ACK packets, the Distributed Firewall on the provider Cisco ACI Virtual Edge drops these packets because no corresponding flow (connection) is created.</td>
</tr>
</tbody>
</table>
### Features and Description

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports TCP flow aging</td>
<td>Connections in ESTABLISHED state are maintained for 2 hours unless the per-port limit reaches the 75% threshold. Once that threshold is reached, any new connection can potentially replace the old connection (which has been inactive for at least 5 minutes). Connections in non-ESTABLISHED TCP state are retained for 5 minutes of idle or inactive time.</td>
</tr>
<tr>
<td>Is implemented at the flow level</td>
<td>Enables a flow between VMs over the TCP connection, eliminating the need to establish a TCP/IP connection for each packet.</td>
</tr>
<tr>
<td>Not dependent on any particular topology or configuration</td>
<td>Works with either Local Switching and No Local Switching modes and with either VLAN and VXLAN.</td>
</tr>
<tr>
<td>Is hardware-assisted</td>
<td>In the ACI fabric, Cisco Nexus 9000 leaf switches store the policies, avoiding impact on performance.</td>
</tr>
<tr>
<td>Bases implementation on 5-tuple values</td>
<td>Uses the source and destination IP addresses, the source and destination ports, and the protocol in implementing policies.</td>
</tr>
<tr>
<td>Is in learning mode by default</td>
<td>Facilitates upgrades. Distributed Firewall must be in learning mode if you migrate to Cisco ACI Virtual Edge from Cisco AVS if the version of Cisco AVS is earlier than Release 5.2(1)SV3(1.5). Those versions do not support Distributed Firewall.</td>
</tr>
</tbody>
</table>

---

## Benefits of Distributed Firewall

This section provides examples of how Distributed Firewall works with hardware in the Cisco ACI fabric to provide security.

### Enhanced Security for Reflexive ACLs

An administrator creates a contract using subjects and filters in the Cisco APIC between consumer and provider EPGs to allow web traffic. The administrator creates a policy in Cisco APIC to allow traffic from any source port to destination port 80.

When the policy is configured in Cisco APIC, a reflexive access control list (ACL) entry from the provider to the consumer is automatically programmed in the ACI hardware. This reflexive ACL is created to allow the reverse traffic for the time when a connection remains established. This reflexive ACL entry is necessary to allow the reverse traffic to flow.

Because of the automatic reflexive ACL creation, the leaf switch allows the provider to connect to any client port when the connection is in the established state. But this may not be desirable for some data centers. That is because an endpoint in a provider EPG may initiate a SYN attack or a port-scan to the endpoints in the consumer EPGs using its source port 80.
However, the Distributed Firewall, with the help of the physical hardware, will not allow such attack. The physical leaf hardware evaluates the packet it receives from the hypervisor against the policy ternary content addressable memory (TCAM) entry.

**Protecting Data When VMs Are Moved with VMotion**

Every packet sent or received follows the flow-based entry in the Distributed Firewall in the Cisco ACI Virtual Edge and in the physical leaf. Since the flows are directly attached to a virtual machine (VM) virtual Ethernet (vEth) interface, even when VMs are moved by VMotion to a different hypervisor host, the flows and table entries move with it to the new hypervisor.

This movement is also reported back to physical leaf. The physical leaf allows the legitimate flow to continue and prevents attacks if they occur. So even when the VM is moved to the new hosts, VM is still communicating without losing protection.

**Seamless FTP Traffic Handling**

The behavior and inter-working of the FTP protocol is different than other TCP-based protocols. For this reason, it requires special treatment in the Distributed Firewall. FTP Server (Provider) listens on the Control port (TCP port 21) and a Data port (TCP port 20). When communication begins between FTP client (Consumer) and server (Provider), the control connection is set up initially between the FTP client and server. The data connection is set up on demand (only when there is data to be exchanged) and torn down immediately after the data transfer.

Distributed Firewall supports only Active-FTP mode handling. The data connections are not tracked for the Passive-FTP mode.

Distributed Firewall allows the FTP data connection only if it matches the FTP Client IP and Port information that was received during the control connection handshake. Distributed Firewall blocks the FTP data connections if there is no corresponding control connection; this is what prevents FTP attacks.

**Distributed Firewall Configuration**

You configure Distributed Firewall by setting it to one of its three modes:

- **Enabled**—Enforces the Distributed Firewall.
- **Disabled**—Does not enforce Distributed Firewall. Use this mode only if you do not want to use the Distributed Firewall. Disabling Distributed Firewall removes all flow information on the Cisco ACI Virtual Edge.
- **Learning**—Cisco ACI Virtual Edge monitors all TCP communication and creates flows in a flow table but does not enforce the firewall. Learning is the default mode.

Distributed Firewall works with policies created in Cisco APIC; unless you create the policies, Distributed Firewall cannot work effectively.

---

**Note**

We recommend that you use vmxnet3 adapters for the VMs when using Distributed Firewall.
When Distributed Firewall is enabled on a Cisco ACI Virtual Edge VMM domain, there are restrictions on vMotion. See the section Guidelines for Using VMware vMotion with Cisco ACI Virtual Edge in this guide for more information.

### Workflow for Distributed Firewall Configuration

This section provides a high-level description of the tasks that you perform to configure Distributed Firewall.

1. Create an interface policy group to enable the firewall policy in the Cisco APIC, or, if you already have an interface policy group, make sure that it contains a firewall policy.

2. Configure a stateful policy for Distributed Firewall.
   - Follow instructions in the section Configure a Stateful Policy for Distributed Firewall Using the GUI, on page 4 in this guide.

3. Change the Distributed Firewall mode if necessary.
   - Distributed Firewall is in learning mode by default. If you have not previously enabled Distributed Firewall, follow the instructions in this guide to for changing the Distributed Firewall mode.

4. Cisco ACI Virtual Edge reports the flows that are permitted or denied by Distributed Firewall to the system log (syslog) server. You can configure parameters for the flows and view the denied flows on the syslog server. See the instructions in the section Distributed Firewall Flow Logging, on page 9 in this guide.

5. Choose which Distributed Firewall flow count statistics that you want to view.
   - Cisco ACI Virtual Edge collects Distributed Firewall flow information, but you must choose which statistics you want to know about before you can view them. See the section Distributed Firewall Flow Counts, on page 16 in this guide for instructions.

### Configure a Stateful Policy for Distributed Firewall Using the GUI

Before you can configure a Distributed Firewall policy, configure a stateful policy for Distributed Firewall.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log in to the Cisco APIC.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Choose Tenants &gt; tenant.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>In the navigation pane, expand the folder for the tenant.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Right-click the Contracts folder and then choose Create Contract.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>In the Create Contract dialog box, in the Name field, type a name for the contract.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>In the Subjects area, click the + icon.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>In the Create Contract Subject dialog box, in the Name field, type a name for the subject.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>In the Filter Chain area, click the + icon next to Filters.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Click the down arrow to display the Name drop-down filter list, and then click the + icon at the top of the Name list.</td>
</tr>
</tbody>
</table>
Step 10  In the **Create Filter** dialog box, complete the following actions:

a) In the **Name** field, type a name for the filter.

b) In the **Entries** area, click the + icon to display more fields.

c) In the **Name** field, type a name to further describe the filter.

d) From the **Ether Type** drop-down list, choose **IP**.

e) From the **IP Protocol** field, choose **tcp**.

f) Check the **Stateful** check box.

g) (Optional) In the **Source Port / Range** field, from the **To** and the **From** drop-down lists, choose **Unspecified**, the default.

h) In the **Destination Port / Range** field, from the **To** and the **From** drop-down lists, choose **http**.

i) Click **Update** and then click **Submit**.

Step 11  In the **Create Contract Subject** dialog box, in the **Filters** area, click **Update** and then click **OK**.

Step 12  In the **Create Contract** dialog box, click **Submit**.

**What to do next**

Create a Distributed Firewall policy.

---

**Configure a Stateful Policy for Distributed Firewall Using the NX-OS Style CLI**

**Procedure**

Configure a stateful policy in the Cisco APIC.

**Example:**

```
apic1(config)# tenant Tenant1
napic1(config-tenant)# access-list TCP-511 apic1
napic1 (config-tenant-acl)# match icmp
napic1 (config-tenant-acl)# match raw TCP-511 dFromPort 443 dToPort 443 etherT ip prot 6 stateful yes
napic1 (config-tenant-acl)# match raw tcp etherT ip prot 6 sFromPort 443 sToPort 443 stateful yes
napic1 (config-tenant-acl)# match raw tcp-22out dFromPort 22 dToPort 22 etherT ip prot 6 stateful yes apic1(config-tenant-acl)# match raw tcp-all etherT ip prot 6 stateful yes apic1(config-tenant-acl)# match raw tcp22-from etherT ip prot 6 sFromPort 22 sToPort 22 stateful yes apic1(config-tenant-acl)# exit apic1(config-tenant)# contract TCP511 apic1(config-tenant-contract)# subject TCP-ICMP apic1(config-tenant-contract-subj)# access-group TCP-511 both apic1(config-tenant-contract-subj)# access-group arp both apic1(config-tenant-contract-subj)#
```

**What to do next**

Create a Distributed Firewall policy.
Configure a Stateful Policy for Distributed Firewall Using the REST API

Configure a stateful policy in the Cisco APIC.

Procedure

Step 1  Log in to the Cisco APIC.
Step 2  Post the policy to https://APIC-ip-address/api/node/mo/.xml.

Example:
<pre>
<polUni>
  <infraInfra>
    <nwsFwPol name="fwpoll" mode="enabled"/>  (enabled, disabled, learning)
    <infraFuncP>
      <infraAccBndlGrp name="fw-bundle">
        <infraRsFwPol tnNwsFwPolName="fwpoll"/>
        <infraRsAttEntP tDn="uni/infra/attentp-testfw2"/>
      </infraAccBndlGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
</pre>

What to do next
Create a Distributed Firewall policy.

Create a Distributed Firewall Policy Using the GUI

You can create a Distributed Firewall policy using the Cisco APIC GUI.

Before you begin
You must have done the following:

• Created an interface policy group to enable the Distributed Firewall policy in Cisco APIC.
• Created a stateful policy for Distributed Firewall.

Procedure

Step 1  Log in to the Cisco APIC.
Step 2  Go to Fabric &gt; External Access Policies.
Step 3
In the **Policies** navigation pane, expand the **Policies** and **Interface** folders.

Step 4
Right-click the **Firewall** folder and choose **Create Firewall Policy**.

Step 5
In the **Create Firewall Policy** dialog box, in the **Name** field, type a name for the policy.

Step 6
In the **Mode** area, choose a mode.

The default mode is Learning to facilitate upgrades.

Distributed Firewall must be in Learning mode if you migrate to Cisco ACI Virtual Edge from Cisco AVS if the version of Cisco AVS is earlier than Release 5.2(1)SV3(1.5). Those versions do not support Distributed Firewall.

Otherwise, enable Distributed Firewall.

**Note**
Do not change the mode from Disabled directly to Enabled. Doing so can lead to traffic loss. Instead, from Disabled mode, change the mode to Learning, wait 5 minutes, and then change the mode to Enabled. The **Create Firewall Policy** dialog box includes a **Syslog** area. This is where you can configure the source for Distributed Firewall flow information that is sent to the syslog server. See the section **Distributed Firewall Flow Logging**, on page 9 in this guide for instructions.

Step 7
Click **Submit**.

Step 8
Associate the new policy with the VMM domain by completing the following steps:

a) Go to **Virtual Networking > Inventory**.

b) In the **Inventory** navigation pane, expand the **VMM Domains** folder and the **VMware** folder, and then choose the relevant VMM domain.

c) In the VMM domain work pane, click the **VSwitch Policies** tab.

d) In the **Properties** work pane, from the **Firewall Policy** drop-down list, choose the firewall policy that you created.

e) Click **Submit**.

---

**What to do next**
Verify that the Distributed Firewall policy is created and is in the desired state by completing the following steps:

1. Go to **Fabric > External Access Policies**.

2. In the **Policies** navigation pane, expand the **Policies, Interface**, and **Firewall** folders.

3. Choose the policy.

4. In the **Properties** work pane, verify that the policy appears and that the mode is correct.

---

### Change Distributed Firewall Policy Mode Using the GUI

Use the following procedure to change the Distributed Firewall mode.

**Note**
Enable Distributed Firewall if you migrated from Cisco AVS to Cisco ACI Virtual Edge and did not have Distributed Firewall enabled for Cisco AVS.
Before you begin
Ensure that your Distributed Firewall policy is associated with a VMM domain.

Procedure

Step 1
Log in to the Cisco APIC.

Step 2
Go to Fabric > External Access Policies.

Step 3
In the Policies navigation pane, expand the Policies, Interface, and Firewall folders.

Step 4
Click the policy that you want to modify.

Step 5
In the Properties work pane, in the Mode area, choose a mode, and then click Submit.

Note
Do not change the mode from Disabled directly to Enabled. Doing so can lead to traffic loss. Instead, from Disabled mode, change the mode to Learning, wait 5 minutes, and then change the mode to Enabled. Changing to Learning mode allows Cisco ACI Virtual Edge to add flow table entries for existing flows.

Note
The Properties work pane includes a Syslog area where you can configure the source for Distributed Firewall flow information that is sent to the syslog server. See the section Distributed Firewall Flow Logging, on page 9 in this guide for instructions.

What to do next
Verify that the Distributed Firewall is in the desired state by completing the following steps:

1. In the Policies navigation pane, choose the policy in the Firewall folder.
2. In the Properties dialog box, verify that the mode is correct.

Enable Distributed Firewall or Change Its Mode Using the NX-OS Style CLI
You can use the NX-OS style CLI to enable Distribute Firewall or change its mode.

Procedure

Enable Distributed Firewall or change its mode.

Example:
apic1# configure
apic1(config)# vmware-domain Direct-AVE2-VXLAN
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# firewall mode < any of below 3>
disabled Disabled mode
enabled Enabled mode
learning Learning mode
Distributed Firewall Flow Logging

You can view flow information for Distributed Firewall with the Cisco APIC to assist with auditing network security.

Cisco ACI Virtual Edge reports the flows that are denied and permitted by Distributed Firewall to the system log (syslog) server. When you enable Distributed Firewall, Cisco ACI Virtual Edge monitors TCP, UDP, and ICMP traffic by default. It also tracks, logs, and—depending on how you configure parameters—permits or denies TCP traffic. You can view the denied and permitted flows on the syslog server.

Configuration of Parameters for Distributed Firewall Flow Information

Cisco ACI Virtual Edge reports the flows that are denied or permitted by Distributed Firewall as well UDP and ICMP flows to the system log (syslog) server.

You configure Distributed Firewall logging in two tasks: configuring up to three syslog servers, referred to as remote destinations in the GUI, and configuring the syslog policy. You can configure the following parameters:

- Syslog server parameters
  - Enable/disable

  **Note** Distributed Firewall logging is disabled by default.

  - Permitted flows, Denied flows, or both
  - Polling interval

  You can set the interval for exporting the flows from 60 seconds to 24 hours.

  **Note** A polling interval of 125 seconds is required to send data at maximum scale. We recommend that you configure the syslog timer with a polling interval of at least 150 seconds.

  - Log severity

    You can set the severity level from 0-7.

- Syslog policy parameters
  - IP address
  - Port
  - Log severity

    You can set the severity level from 0-7.

  - Log facility
Cisco ACI Virtual Edge reports up to 250,000 denied or permitted flows to the syslog server for each polling interval. If you choose to log denied and permitted flows, Cisco ACI Virtual Edge reports up to 500,000 flows. Cisco ACI Virtual Edge also reports up to 100,000 short-lived flows—flows that are shorter than the polling interval.

Syslog messages are sent only if the syslog destination log severity is at or below the same log severity for the syslog policy. Severity levels for the syslog server and syslog policy are as follows:

- 0: Emergency
- 1: Alert
- 2: Critical
- 3: Error
- 4: Warning
- 5: Notification
- 6: Information
- 7: Debug

**Guidelines for Configuring the Syslog Server**

Follow the guidelines in this section when configuring the syslog server for Cisco ACI Virtual Edge.

- The syslog server should always be reachable from the Cisco ACI Virtual Edge host management network or Cisco ACI Virtual Edge infra port group (overlay-1 vrf of tenant infra).
  
  If the syslog server is behind the Cisco ACI Virtual Edge, bring up the VM VNIC in the infra port group.

- The syslog server should always be on a different host from Cisco ACI Virtual Edge.
  
  Sending log messages from a Cisco ACI Virtual Edge to a syslog server hosted behind the same Cisco ACI Virtual Edge is not supported.

- If the syslog server destination is a VM, make sure that vMotion is disabled on it. If the syslog server destination VM is moved to another host for any reason, make sure that the static client endpoint (CEP) is configured accordingly. See the section Configure a Static End Point Using the GUI, on page 12 in this guide.
  
  The IP for the syslog server can be obtained using DHCP (Option 61 is needed during DHCP) or static configuration. Make sure that the IP address is in the same subnet as the other EPs in infra port group (overlay-1 VRF of tenant infra).

**Distributed Firewall Flow Syslog Messages**

This section provides the formats and examples of syslog messages for distributed Firewall flows.

- Denied flows
  
  • Format

  
  <Syslog Server timestamp> < PRI - Facility*8 + Severity > <syslog version> <Host timestamp> <Host IP> <Application name (ave-dfwlog)> - AVE IP: <AVEIP> AVE Hostname <hostname> DFWLOG-DENY_FLOW - <Deny Reason> AVE UUID: <UUID>, Source IP: <Source
IP address>, Destination IP: <Destination IP address>, Source Port: <Port number>, Destination Port: <Port Number>, Source Interface: <Interface name>, Protocol: "TCP"(6), Hit-Count = <Number of Occurrences>, EPG Name: <EPG Name>, EpP DN: <EpP DN>

• Example


• Permitted flows

• Format

<Syslog server timestamp> < PRI = Facility*8 + Severity > <syslog version> <Host timestamp> <Host IP> <Application name (ave-dfwlog)> - AVE IP: <AVEIP> AVE Hostname <hostname> DFWLOG-PERMIT_FLOW -<flow status> AVE UUID: <UUID>, Source IP: <Source IP address>, Destination IP: <Destination IP address>, Source Port: <Port Number>, Destination Port: <Port Number>, Source Interface: <Interface name>, Protocol: "TCP"(6), Age = <Age in seconds>, EPG Name: <EPG Name>, EpP DN: <EpP DN>

• Example


• Short-lived permitted flows

• Format


• Example


• ICMP monitored flows

• Format

<Syslog server timestamp> < PRI = Facility*8 + Severity > <syslog version> <Host timestamp> <Host IP> <Application name (ave-dfwlog)> - AVE IP: <AVEIP> AVE Hostname <hostname> DFWLOG-ICMP_TRACKING - AVE UUID: <UUID>, Source IP: <Source IP address>, Destination IP: <Destination IP address>, Type:<ICMP type field>, Source Interface:
Configure a Static End Point Using the GUI

Procedure

Step 1 Log in to Cisco APIC.
Step 2 In the Tenant infra navigation pane, open the following folders: Application Profiles > access > Application EPGs > default.
Step 3 Right-click the Static EndPoint folder and then choose Create Static EndPoint.
Step 4 In the Create Static Endpoint dialog box, complete the following steps:
   a) In the MAC field, enter the syslog server destination's MAC address.
   b) In the Type area, choose tep.
   c) In the Path Type area, choose the appropriate path type.

   The path type determines how the leaf is connected to the syslog server destination. The leaf can be connected by port, direct port channel, or virtual port channel.

   d) If you chose Port as the Path Type, choose a node from the Node drop-down list.
   e) In the Path field, enter the appropriate path.

   The path determines the policy group where the syslog server destination is attached.
f) In the **IP Address** field, enter the syslog server destination IP address.

g) In the **Encap** field, enter the overlay-1 VLAN (vlan-xxix).

h) Click **Submit**.

**Step 5**

From the syslog server destination, ping any overlay-IP address—for example, 10.0.0.30.

This step ensures that the fabric learns the Syslog server destination IP address.

---

**Configure Parameters for Distributed Firewall Flow Information Using the GUI**

To configure parameters, you first configure the parameters for the syslog server or servers and then configure the parameters for the syslog policy. The syslog server is referred to as the *Remote Destination* in the GUI.

**Before you begin**

You must have Distributed Firewall enabled.

**Procedure**

**Step 1**

Log in to Cisco APIC.

**Step 2**

Go to **Admin > External Data Collectors**.

**Step 3**

In the **External Data Collectors** navigation pane, expand the **Monitoring Destinations** folder and then choose the **Syslog** folder.

**Step 4**

In the **Syslog** work pane, click the **ACTIONS** down arrow and then choose **Create Syslog Monitoring Destination Group**.

**Step 5**

In the **Create Syslog Monitoring Destination Group STEP 1 > Profile** dialog box, complete the following steps:

a) In the **Define Group Name and Profile** area, enter a name in the **Name** field.

b) In the **Admin State** area, make sure that **enabled** is chosen from the drop-down list.

c) Accept the defaults in the rest of the dialog box and click **NEXT**.

**Step 6**

In the **Create Syslog Monitoring Destination Group STEP 2 > Remote Destinations** dialog box, click the **+** icon.

**Step 7**

In the **Create Syslog Remote Destination** dialog box, complete the following steps:

a) In the **Host** field, enter the host IP address.

b) In the **Name** field, enter the host name.

c) In the **Admin State** area, make sure that **enabled** is chosen.

d) In the **Format** area, make sure that **aci** is chosen.

e) From the Severity drop-down list, choose a severity.

f) From the **Port** drop-down list, accept the standard port unless you are using another port.

g) From the **Forwarding Facility** drop-down list, choose a facility.

h) Ignore the **Management EPG** drop-down list and click **OK**.

**Step 8**

(Optional) In the **Create Syslog Monitoring Destination Group STEP 2 > Remote Destinations** dialog box, create up to two additional remote destinations.
**Step 9**
In the Create Syslog Monitoring Destination Group STEP 2 > Remote Destinations dialog box, click **FINISH**.
The newly created destination appears in the **Syslog** folder in the External Data Collectors navigation pane.

**Step 10**
Choose **Fabric > External Access Policies**.

**Step 11**
In the Policies navigation pane, open the Policies and Interface folders.

**Step 12**
Complete one of the following sets of steps:

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a syslog policy with a new Distributed Firewall policy</td>
<td>1. Right-click the Firewall folder and choose Create Firewall Policy.</td>
</tr>
<tr>
<td></td>
<td>2. In the Create Firewall Policy dialog box, in the Specify the Firewall Policy Properties area, type a name for the policy in the Name field.</td>
</tr>
<tr>
<td></td>
<td>3. In the Mode area, choose a mode.</td>
</tr>
<tr>
<td></td>
<td>Distributed Firewall must be in Learning mode if you migrate to Cisco ACI Virtual Edge from Cisco AVS if the version of Cisco AVS is earlier than Release 5.2(1)SV3(1.5). Those versions do not support Distributed Firewall.</td>
</tr>
<tr>
<td></td>
<td>4. In the Syslog area, make sure that enabled is chosen from the Administrative State drop-down list.</td>
</tr>
<tr>
<td></td>
<td>5. From the Included Flows area, choose Permitted flows, Denied flows, or both.</td>
</tr>
<tr>
<td></td>
<td>6. In the Polling Interval (seconds) area, choosing an interval from 60 seconds to 24 hours.</td>
</tr>
<tr>
<td></td>
<td>7. From the Log Level drop-down list, choose a severity level.</td>
</tr>
<tr>
<td></td>
<td>The logging severity level should be greater than or equal to severity level defined for the syslog server. See the section Configuration of Parameters for Distributed Firewall Flow Information, on page 9 in this guide for information about severity.</td>
</tr>
<tr>
<td></td>
<td>8. From the Dest Group drop-down list, choose the destination group that you just created.</td>
</tr>
<tr>
<td></td>
<td>9. Click Submit.</td>
</tr>
<tr>
<td></td>
<td>10. Go to the section &quot;What To Do Next&quot; and associate the new Distributed Firewall policy with a VMM domain.</td>
</tr>
</tbody>
</table>

Configure a syslog policy with an existing Distributed Firewall policy

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a syslog policy with an existing Distributed Firewall policy</td>
<td>1. Expand the Firewall folder and choose the Distributed Firewall policy that you want to modify.</td>
</tr>
<tr>
<td></td>
<td>2. In the policy work pane, change the Mode if desired.</td>
</tr>
<tr>
<td></td>
<td>Distributed Firewall must be in Learning mode if you migrate to Cisco ACI Virtual Edge from Cisco AVS if the version of Cisco AVS is earlier than Release 5.2(1)SV3(1.5). Those versions do not support Distributed Firewall.</td>
</tr>
<tr>
<td></td>
<td>3. In the Syslog area, make sure that enabled is chosen from the Administrative State drop-down list.</td>
</tr>
<tr>
<td></td>
<td>4. From the Included Flows area, choose Permitted flows, Denied flows, or both.</td>
</tr>
</tbody>
</table>
If you want to... | Then...
---|---
5. | In the **Polling Interval (seconds)** area, choosing an interval from 60 seconds to 24 hours.
6. | From the **Log Level** drop-down list, choose a severity level.
   The logging severity level should be greater than or equal to severity level defined for the syslog server. See the section **Configuration of Parameters for Distributed Firewall Flow Information**, on page 9 in this guide for information about severity.
7. | From the **Dest Group** drop-down list, choose the destination group that you just created.
8. | Click **Submit**.
9. | If you see the **Policy Usage Warning** dialog box, click **SUBMIT CHANGES**.

**What to do next**

If you configured a syslog policy with a new Distributed Firewall policy, you must associate the Distributed Firewall policy with a VMM domain.

1. | In Cisco APIC, choose **Virtual Networking > Inventory**.
2. | In the navigation pane, expand the **VMM Domains** folder and the **VMware** folder, and then choose the relevant VMM domain.
3. | In the work pane, click the **VSwitch Policy** tab under the **Policy** tab.
4. | In the **Create VSwitch Policy Container** dialog box, click **Yes**.
5. | In the work pane, from the **Firewall Policy** drop-down list, choose the policy.
6. | Click **Submit**.
7. | If you see the **Policy Usage Warning** dialog box, click **SUBMIT CHANGES**.

**Configure Parameters for Distributed Firewall Flow Information Using the NX-OS Style CLI**

**Procedure**

**Step 1**

Configure the parameters for the syslog server or servers.

**Example:**

```
apic1# configure
apic1(config)# logging server-group group name
apic1(config-logging)# server IP address severity severity level facility facility name port 1-65535 mgmtep  MgmtEp
```
You can repeat the last command for additional syslog servers; you can configure up to three syslog servers.

Step 2
Configure the parameters for the syslog source.

Example:
apic1# configure
apic1(config)# vmware-domain Direct-AVE
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# firewall mode enabled
apic1(config-vmware-ave)# firewall-logging server-group group name action-type permit, deny severity severity polling-interval 60-86400

Note: You must enter the firewall mode enabled command before you enter the firewall-logging command.

Note: For the firewall-logging command, you can enter either permit or deny. You can also enter both, separated by a comma.

Configure Parameters for Distributed Firewall Flow Information Using the REST API

Procedure

Step 1
Send an HTTP POST message to deploy the application using the XML API.

Example:
POST https://10.197.139.36/api/node/mo/uni/fabric/slgroup-Syslog-Servers.xml

Step 2
Configure the parameters for the syslog server or servers.

Example:
<syslogGroup descr="" dn="uni/fabric/slgroup-Syslog-Servers" format="aci" name="Syslog-Servers" nameAlias=""/>
<syslogRemoteDest adminState="enabled" descr="" format="aci" forwardingFacility="local7" host="10.197.139.216" name="10.197.139.216" nameAlias="" port="1514" severity="debugging">
  <fileRsARemoteHostToEpg tDn="uni/tn-mgmt/mgmtDefault/ooB-default"/>
</syslogRemoteDest>
<syslogProf adminState="enabled" descr="" name="syslog" nameAlias=""/>
<syslogFile adminState="disabled" descr="" format="aci" name="" nameAlias="" severity="information"/>
<syslogConsole adminState="disabled" descr="" format="aci" name="" nameAlias="" severity="alerts"/>
<syslogGroup>

Distributed Firewall Flow Counts

You can view Distributed Firewall flow counts with the Cisco APIC.
Cisco ACI Virtual Edge collects Distributed Firewall flow information, but you must choose which statistics you want to know about before you can view them. You can choose a sampling interval with choices ranging from 10 seconds to 1 year; however, the default is 5 minutes.

You can choose statistics and view them from two different places in Cisco APIC: one beginning with Virtual Networking and one beginning with Tenants. However, the steps for choosing and viewing statistics are the same.

When you choose statistics in Cisco APIC, you see a list of different kinds of statistics, but only nine are relevant to Distributed Firewall:

- aged connections (connections)
- created connections (connections)
- destroyed connections (connections)
- denied global input connections (connections)
- denied per port limit connections (connections)
- invalid SYN ACK packets (packets)
- invalid SYN packets (packets)
- invalid connection packets (packets)
- invalid ftp SYN packets (packets)

Choose Statistics to View for Distributed Firewall

Before you begin

You must have Distributed Firewall enabled.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Virtual Networking &gt; Inventory &gt; VMM Domains &gt; VMware &gt; VMM_name &gt; Controllers &gt; controller instance name &gt; DVS-VMM name &gt; Portgroups &gt; EPG_name &gt; Learned Point MAC address (Node).</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the Stats tab.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the tab with the check mark.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Select Stats dialog box, click the statistics that you want to view in the Available pane and then click the arrow pointing right to put them in the Selected pane.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) Choose a sampling interval.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

View Statistics for Distributed Firewall

Once you have chosen statistics for Distributed Firewall, you can view them.
Before you begin
You must have chosen statistics to view for Distributed Firewall.

Procedure

Step 1
Choose Virtual Networking > Inventory > VMware > VMM Domains > VMM_name > Controllers > controller instance name > DVS-VMM name > Portgroups > EPG_name > Learned Point MAC address (Node)

Step 2
Click the Stats tab.
The central pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper left side of the work pane.