Controlling Traffic with Network-Based Rules

Access control rules within *access control policies* exert granular control over network traffic logging and handling. Network-based conditions allow you to manage which traffic can traverse your network, using one or more of the following criteria:

- source and destination security zones
- source and destination IP addresses or geographical locations
- a packet's innermost VLAN tag
- source and destination port, which also includes transport layer protocol and ICMP code options

You can combine network-based conditions with each other and with other types of conditions to create an access control rule. These access control rules can be simple or complex, matching and inspecting traffic using multiple conditions. For detailed information on access control rules, see Tuning Traffic Flow Using Access Control Rules, page 14-1.

Note Hardware-based fast-path rules, Security Intelligence-based traffic filtering, and some decoding and preprocessing occur **before** network traffic is evaluated by access control rules. You can also configure the *SSL inspection* feature to block or decrypt encrypted traffic before access control rules evaluate it.

While you can perform most network-based access control using any FireSIGHT System appliance and any license, geolocation-based access control requires a FireSIGHT license and is not supported on many Series 2 appliances, nor on Cisco NGIPS for Blue Coat X-Series. Also, ASA FirePOWER devices do not support access control by VLAN.

Table 15-1 License and Model Requirements for Network-Based Access Control Rules

Requirement	VLAN Tag	Geolocation Control	All Other Network-Based Control
license	Any	FireSIGHT	Any
devices	Any except ASA FirePOWER	Series 3 virtual ASA FirePOWER	Any
Defense Centers	Any	Any except DC500	Any

For information on building network-based access control rules, see:

- Controlling Traffic by Security Zone, page 15-2
- Controlling Traffic by Network or Geographical Location, page 15-3

Controlling Traffic by Security Zone

License: Any

Zone conditions in access control rules allow you to control traffic by its source and destination security zones. A *security zone* is a grouping of one or more interfaces, which may be located across multiple devices. An option you choose during a device's initial setup, called its *detection mode*, determines how the system initially configures the device's interfaces, and whether those interfaces belong to a security zone.

As a simple example, when you register device with an **Inline** detection mode, the Defense Center creates two zones: Internal and External, and assigns the first pair of interfaces on the device to those zones. Hosts connected to the network on the Internal side represent your protected assets.

To extend this scenario, you could deploy additional identically configured devices—managed by the same Defense Center—to protect similar resources in several different locations. Like the first device, each of these devices protects the assets in its Internal security zone.

Tip You are not required to group all internal (or external) interfaces into a single zone. Choose the grouping that makes sense for your deployment and security policies. For more information on creating zones, see Working with Security Zones, page 3-39.

In this deployment, you may decide that although you want these hosts to have unrestricted access to the Internet, you nevertheless want to protect them by inspecting incoming traffic for intrusions and malware.

To accomplish this using access control, configure an access control rule with a zone condition where the **Destination Zone** is set to **Internal**. This simple access control rule matches traffic that leaves the device from any interface in the Internal zone.

To ensure that the system inspects matching traffic for intrusions and malware, choose a rule action of **Allow**, then associate this rule with an intrusion and a file policy. For more information, see Using Rule Actions to Determine Traffic Handling and Inspection, page 14-7 and Controlling Traffic Using Intrusion and File Policies, page 18-1.

If you want to build a more complex rule, you can add a maximum of 50 zones to each of the **Source Zones** and **Destination Zones** in a single zone condition:

- To match traffic *leaving* the device from an interface in the zone, add that zone to the **Destination Zones**.

  Because devices deployed passively do not transmit traffic, you cannot use a zone comprised of passive interfaces in a **Destination Zone** condition.
- To match traffic *entering* the device from an interface in the zone, add that zone to the **Source Zones**.
- If you add both source and destination zone conditions to a rule, matching traffic must originate from one of the specified source zones **and** egress through one of the destination zones.

Note that just as all interfaces in a zone must be of the same type (all inline, all passive, all switched, or all routed), all zones used in a zone condition for an access control rule must be of the same type. That is, you cannot write a single rule that matches traffic to or from zones of different types.

When building a zone condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon and see Troubleshooting Access Control Policies and Rules, page 12-22.

To control traffic by zone:

Access: Admin/Access Admin/Network Admin

Step 1 In the access control policy that targets the devices where you want to control traffic by zone, create a new access control rule or edit an existing rule.

For detailed instructions, see Creating and Editing Access Control Rules, page 14-2.

Step 2 In the rule editor, select the Zones tab.

The Zones tab appears.

Step 3 Find and select the zones you want to add from the **Available Zones**.

To search for zones to add, click the **Search by name** prompt above the **Available Zones** list, then type a zone name. The list updates as you type to display matching zones.

Click to select a zone. To select multiple zones, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination** to add the selected zones to the appropriate list.

You can also drag and drop selected zones.

Step 5 Save or continue editing the rule.

You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Controlling Traffic by Network or Geographical Location

License: feature dependent

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

Network conditions in access control rules allow you to control traffic by its source and destination IP address. You can either:

- explicitly specify the source and destination IP addresses for the traffic you want to control, or
- use the geolocation feature, which associates IP addresses with geographical locations, to control traffic based on its source or destination country or continent

When you build a network-based access control rule condition, you can manually specify IP address and geographical locations. Alternately, you can configure network conditions with network and geolocation *objects*, which are reusable and associate a name with one or more IP addresses, address blocks, countries, continents, and so on.

Tip After you create a network or geolocation object, you can use it not only to build access control rules, but also to represent IP addresses in various other places in the system's web interface. You can create these objects using the object manager; you can also create network objects on-the-fly while you are configuring access control rules. For more information, see Managing Reusable Objects, page 3-1.

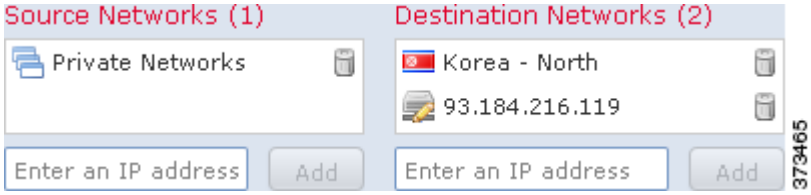
Note that if you want to write rules to control traffic by geographical location, to ensure you are using up-to-date geolocation data to filter your traffic, Cisco **strongly** recommends you regularly update the geolocation database (GeoDB) on your Defense Center; see Updating the Geolocation Database, page 66-27.

Additionally, note that while you can perform simple IP address-based access control using any FireSIGHT System appliance and any license, geolocation-based access control requires a FireSIGHT license and is not supported on many Series 2 appliances, nor on Cisco NGIPS for Blue Coat X-Series.

Table 15-2 License and Model Requirements for Network Conditions

Requirement	Geolocation Control	IP Address Control
license	FireSIGHT	Any
devices	Series 3, virtual, ASA FirePOWER	Any
Defense Centers	Any except DC500	Any

The following graphic shows the network condition for an access control rule that blocks connections originating from your internal network and attempting to access resources either in North Korea or on 93.184.216.119 (example.com).



In this example, a network object group called Private Networks (that comprises the IPv4 and IPv6 Private Networks network objects, not shown) represents your internal networks. The example also manually specifies the example.com IP address, and uses a system-provided North Korea geolocation object to represent North Korea IP addresses.

You can add a maximum of 50 items to each of the **Source Networks** and **Destination Networks** in a single network condition, and you can mix network and geolocation-based configurations:

- To match traffic *from* an IP address or geographical location, configure the **Source Networks**.
- To match traffic *to* an IP address or geographical location, configure the **Destination Networks**.

If you add both source and destination network conditions to a rule, matching traffic must originate from one of the specified IP addresses **and** be destined for one of the destination IP addresses.

When building a network condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon and see Troubleshooting Access Control Policies and Rules, page 12-22.

To control traffic by network or geographical location:

Access: Admin/Access Admin/Network Admin

Step 1 In the access control policy that targets the devices where you want to control traffic by network, create a new access control rule or edit an existing rule.

For detailed instructions, see Creating and Editing Access Control Rules, page 14-2.

Step 2 In the rule editor, select the Networks tab.

The Networks tab appears.

Step 3 Find and select the networks you want to add from the **Available Networks**, as follows:

- Click the Networks tab to display network objects and groups to add; click the Geolocation tab to display geolocation objects.
- To add a network object on the fly, which you can then add to the condition, click the add icon ( ) above the **Available Networks** list; see Working with Network Objects, page 3-4.
- To search for network or geolocation objects to add, select the appropriate tab, click the **Search by name or value** prompt above the **Available Networks** list, then type an object name or the value of one of the object's components. The list updates as you type to display matching objects.

To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination** to add the selected objects to the appropriate list.

You can also drag and drop selected objects.

Step 5 Add any source or destination IP addresses or address blocks that you want to specify manually.

Click the **Enter an IP address** prompt below the **Source Networks** or **Destination Networks** list; then type an IP address or address block and click **Add**.

Step 6 Save or continue editing the rule.

You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Controlling VLAN Traffic

License: Any

Supported Devices: Any except ASA FirePOWER

VLAN conditions in access control rules allow you to control VLAN-tagged traffic. The system uses the innermost VLAN tag to identify a packet by VLAN.

When you build a VLAN-based access control rule condition, you can manually specify VLAN tags. Alternately, you can configure VLAN conditions with VLAN tag *objects*, which are reusable and associate a name with one or more VLAN tags.

Tip After you create a VLAN tag object, you can use it not only to build access control rules, but also to represent VLAN tags in various other places in the system's web interface. You can create VLAN tag objects either using the object manager or on-the-fly while you are configuring access control rules. For more information, see Working with VLAN Tag Objects, page 3-13.

The following graphic shows a VLAN tag condition for an access control rule that matches traffic on public-facing VLANs (represented by a VLAN tag object group), as well as the manually added VLAN 42.

You can add a maximum of 50 items to the **Selected VLAN Tags** in a single VLAN tag condition. When building a VLAN tag condition, warning icons indicate invalid configurations. For details, hover your pointer over the icon and see Troubleshooting Access Control Policies and Rules, page 12-22.

To control traffic by VLAN tag:

Access: Admin/Access Admin/Network Admin

Step 1 In the access control policy that targets the devices where you want to control traffic by VLAN tag, create a new access control rule or edit an existing rule.

For detailed instructions, see Creating and Editing Access Control Rules, page 14-2.

Step 2 In the rule editor, select the VLAN Tags tab.

The VLAN Tags tab appears.

Step 3 Find and select the VLANs you want to add from the **Available VLAN Tags**, as follows:

- To add a VLAN tag object on the fly, which you can then add to the condition, click the add icon ( ) above the Available VLAN Tags list; see Working with VLAN Tag Objects, page 3-13.
- To search for VLAN tag objects and groups to add, click the **Search by name or value** prompt above the **Available VLAN Tags** list, then type either the name of the object, or the value of a VLAN tag in the object. The list updates as you type to display matching objects.

To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Rule** or to add the selected objects to the **Selected VLAN Tags** list.

You can also drag and drop selected objects.

Step 5 Add any VLAN tags that you want to specify manually.

Click the **Enter a VLAN Tag** prompt below the **Selected VLAN Tags** list; then type a VLAN tag or range and click **Add**. You can specify any VLAN tag from 1 to 4094; use a hyphen to specify a range of VLAN tags.

Step 6 Save or continue editing the rule.

You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Controlling Traffic by Port and ICMP Codes

License: Any

Network conditions in access control rules allow you to control traffic by its source and destination port. In this context, "port" refers to one of the following:

- For TCP and UDP, you can control traffic based on the transport layer protocol. The system represents this configuration using the protocol number in parentheses, plus an optional associated port or port range. For example: TCP(6)/22.
- For ICMP and ICMPv6 (IPv6-ICMP), you can control traffic based on its Internet layer protocol plus an optional type and code. For example: ICMP(1):3:3.
- You can control traffic using other protocols that do not use ports.

When you build a port-based access control rule condition, you can manually specify ports. Alternately, you can configure port conditions with port *objects*, which are reusable and associate a name with one or more ports.

Tip After you create a port object, you can use it not only to build access control rules, but also to represent ports in various other places in the system's web interface. You can create port objects either using the object manager or on-the-fly while you are configuring access control rules. For more information, see Working with Port Objects, page 3-11.

You can add a maximum of 50 items to each of the **Selected Source Ports** and **Selected Destination Ports** lists in a single network condition:

- To match traffic *from* a port, configure the **Selected Source Ports**.

  If you add only source ports to a condition, you can add ports that use different transport protocols. For example, you can add both DNS over TCP and DNS over UDP as source port conditions in a single access control rule.

- To match traffic *to* a port, configure the **Selected Destination Ports**.

  If you add only destination ports to a condition, you can add ports that use different transport protocols.

- To match traffic both originating from specific **Selected Source Ports** *and* destined for specific **Selected Destination Ports**, configure both.

  If you add both source and destination ports to a condition, you can only add ports that share a single transport protocol (TCP or UDP). For example, if you add DNS over TCP as a source port, you can add Yahoo Messenger Voice Chat (TCP) as a destination port but not Yahoo Messenger Voice Chat (UDP).

Keep the following points in mind when building a port condition:

- When you add a destination ICMP port with the type set to 0 or a destination ICMPv6 port with the type set to 129, the access control rule only matches unsolicited echo replies. ICMP echo replies sent in response to ICMP echo requests are ignored. For a rule to match on any ICMP echo, use ICMP type 8 or ICMPv6 type 128.
- When you use the GRE (47) protocol as a destination port condition, you can only add other network-based conditions to the access control rule, that is, zone, network, and VLAN tag conditions. You cannot save the rule if you add reputation or user-based conditions.

When building a port condition, warning icons indicate invalid configurations. For example, you can use the object manager to edit in-use port objects so that the rules that use those object groups become invalid. For details, hover your pointer over the icon and see Troubleshooting Access Control Policies and Rules, page 12-22.

To control traffic by port:

Access: Admin/Access Admin/Network Admin

Step 1 In the access control policy that targets the devices where you want to control traffic by port, create a new access control rule or edit an existing rule.

For detailed instructions, see Creating and Editing Access Control Rules, page 14-2.

Step 2 In the rule editor, select the Ports tab.

The Ports tab appears.

Step 3 Find and select the ports you want to add from the **Available Ports**, as follows:

- To add a port object on the fly, which you can then add to the condition, click the add icon ( ) above the Available Ports list; see Working with Port Objects, page 3-11.
- To search for port objects and groups to add, click the **Search by name or value** prompt above the **Available Ports** list, then type either the name of the object, or the value of a port in the object. The list updates as you type to display matching objects. For example, if you type 80, the Defense Center displays the Cisco-provided HTTP port object.

  To select an object, click it. To select multiple objects, use the Shift and Ctrl keys, or right-click and then select **Select All**.

Step 4 Click **Add to Source** or **Add to Destination** to add the selected objects to the appropriate list.

You can also drag and drop selected objects.

Step 5 Add any source or destination ports that you want to specify manually.

- For source ports, select either **TCP** or **UDP** from the **Protocol** drop-down list under the **Selected Source Ports** list. Then, enter a **Port**. You can specify a single port with a value from 0 to 65535.
- For destination ports, select a protocol (including **All** for all protocols) from the **Protocol** drop down list under the **Selected Destination Ports** list. You can also type the number of an unassigned protocol that does not appear in the list.

  If you select **ICMP** or **IPv6-ICMP**, a pop-up window appears where you can select a type and a related code. For more information on ICMP types and codes, see http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml and http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml.

  If you do not want to specify a protocol, or optionally if you specified TCP or UDP, enter a **Port**. You can specify a single port with a value from 0 to 65535.

Click **Add**. Note that the Defense Center will not add a port to a rule condition that results in an invalid configuration.

Step 6 Save or continue editing the rule.

You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.