

Customizing Traffic Preprocessing

Many of the advanced settings in an access control policy govern intrusion detection and prevention configurations that require specific expertise to configure. Advanced settings typically require little or no modification and are not common to every deployment.

This chapter explains how to set the following preferences:

- Setting the Default Intrusion Policy for Access Control, page 14-1 explains how to change the access control policy's default intrusion policy, which is used to initially inspect traffic before the system can determine exactly how to inspect that traffic
- Customizing Preprocessing with Network Analysis Policies, page 14-2 explains how to tailor certain traffic preprocessing options to specific security zones, and networks by assigning custom network analysis policies to preprocess matching traffic.

Other chapters describe policy-wide preprocessing and performance options for access control policies. For more information, see:

- Configuring Advanced Transport/Network Settings, page 18-1
- Tuning Preprocessing in Passive Deployments, page 19-1
- Tuning Intrusion Prevention Performance, page 10-6
- Tuning File and Malware Inspection Performance and Storage, page 10-16

Setting the Default Intrusion Policy for Access Control

License: Any

Each access control policy uses its *default intrusion policy* to initially inspect traffic before the system can determine exactly how to inspect that traffic. This is needed because sometimes the system must process the first few packets in a connection, **allowing them to pass**, before it can decide which access control rule (if any) will handle the traffic. However, so that these packets do not reach their destination uninspected, you can use an intrusion policy—called the default intrusion policy—to inspect them and generate intrusion events.

A default intrusion policy is especially useful when performing application control and URL filtering, because the system cannot identify applications or filter URLs before a connection is fully established between the client and the server. For example, if a packet matches all the other conditions in an access control rule with an application or URL condition, it and subsequent packets are allowed to pass until the connection is established and application or URL identification is complete, usually 3 to 5 packets.

The system inspects these allowed packets with the default intrusion policy, which can generate events and, if placed inline, block malicious traffic. After the system identifies the access control rule or default action that should handle the connection, the remaining packets in the connection are handled and inspected accordingly.

When you create an access control policy, its default intrusion policy depends on the default action you **first** chose. Initial default intrusion policies for access control are as follows:

- Balanced Security and Connectivity (a system-provided policy) is the default intrusion policy for an access control policy where you first chose the **Intrusion Prevention** default action.
- No Rules Active is the default intrusion policy for an access control policy where you first chose the **Block all traffic** default action. Although choosing this option disables intrusion inspection on the allowed packets described above, it can improve performance if you are not interested in intrusion data.

Note If you are not performing intrusion inspection, keep the No Rules Active policy as your default intrusion policy. For more information, see Troubleshooting Access Control Policies and Rules, page 4-12.

Note that if you change your default action after you create the access control policy, the default intrusion policy does **not** automatically change. To change it manually, use the access control policy's advanced options.

To change an access control policy's default intrusion policy:

Step 1 In the access control policy where you want to change the default intrusion policy, select the **Advanced** tab, then click the edit icon ( ) next to the Network Analysis and Intrusion Policies section.

The Network and Analysis Policies dialog box appears.

Step 2 From the **Intrusion Policy used before Access Control rule is determined** drop-down list, select a default intrusion policy. You can choose a system- or user-created policy.

Note that if you choose a user-created policy, you can click an edit icon ( ) to edit the policy in a new window. You cannot edit system-provided policies.

Caution Do **not** use `Experimental Policy 1` unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

Step 3 Click **OK** to save your changes.

You must apply the access control policy for your changes to take effect.

Customizing Preprocessing with Network Analysis Policies

License: Any

Network analysis policies govern how traffic is decoded and preprocessed so that it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt. This traffic preprocessing occurs after Security Intelligence blacklisting, but before intrusion policies inspect packets in detail. By default, the system-provided Balanced Security and Connectivity network analysis policy applies to *all* traffic handled by an access control policy.

Tip The system-provided Balanced Security and Connectivity network analysis policy and the Balanced Security and Connectivity intrusion policy work together and can both be updated in intrusion rule updates. However, the network analysis policy governs mostly preprocessing options, whereas the intrusion policy governs mostly intrusion rules.

A simple way to tune preprocessing is to create and use a custom network analysis policy as the default; see Creating a Custom Network Analysis Policy, page 15-2. Tuning options available vary by preprocessor.

For advanced users with complex deployments, you can create multiple network analysis policies, each tailored to preprocess traffic differently. Then, you can configure the system to use those policies to govern the preprocessing of traffic using different security zones or networks.

To accomplish this, you add custom *network analysis rules* to your access control policy. Each rule has:

- a set of rule conditions that identifies the specific traffic you want to preprocess
- an associated network analysis policy that you want to use to preprocess traffic that meets all the rules' conditions

When it is time for the system to preprocess traffic, it matches packets to network analysis rules in top-down order by rule number. Traffic that does not match any network analysis rules is preprocessed by the default network analysis policy.

Note If you disable a preprocessor but the system needs to evaluate preprocessed packets against an enabled intrusion or preprocessor rule, the system automatically enables and uses the preprocessor although it remains disabled in the network analysis policy interface. Tailoring preprocessing, especially using multiple custom network analysis policies, is an **advanced** task. Because preprocessing and intrusion inspection are so closely related, you **must** be careful that you allow the network analysis and intrusion policies examining a single packet to complement each other. For more information, see Limitations of Custom Policies, page 12-11.

For more information, see the following sections:

- Setting the Default Network Analysis Policy for Access Control, page 14-3
- Specifying Traffic to Preprocess Using Network Analysis Rules, page 14-4
- Managing Network Analysis Rules, page 14-7

Setting the Default Network Analysis Policy for Access Control

License: Any

By default, the system-provided Balanced Security and Connectivity network analysis policy applies to all traffic handled by an access control policy. If you add network analysis rules to tailor traffic preprocessing options, the default network analysis policy preprocesses all traffic not handled by those rules.

An access control policy's advanced settings allow you to change this default policy.

To change an access control policy's default network analysis policy:

Step 1 In the access control policy where you want to change the default network analysis policy, select the **Advanced** tab, then click the edit icon ( ) next to the Network Analysis and Intrusion Policies section.

The Network and Analysis Policies dialog box appears.

Step 2 From the **Default Network Analysis Policy** drop-down list, select a default network analysis policy. You can choose a system- or user-created policy.

Note that if you choose a user-created policy, you can click an edit icon ( ) to edit the policy in a new window. You cannot edit system-provided policies.

Caution Do **not** use `Experimental Policy 1` unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

Step 3 Click **OK** to save your changes,.

You must apply the access control policy for your changes to take effect.

Specifying Traffic to Preprocess Using Network Analysis Rules

License: Any

Within your access control policy's advanced settings, you can use network analysis rules to tailor preprocessing configurations to network traffic. Similar to access control rules, network analysis rules are numbered, starting at 1.

When it is time for the system to preprocess traffic, it matches packets to network analysis rules in top-down order by ascending rule number, and preprocesses traffic according to the first rule where all the rule's conditions match. The conditions you can add to a rule are described in the following table.

Table 14-1 Network Analysis Rule Condition Types

This Condition...	Matches Traffic...	Details
Zones	entering or leaving a device via an interface in a specific security zone	A security zone is a logical grouping of one or more interfaces according to your deployment and security policies. To build a zone condition, see Preprocessing Traffic Per Zone, page 14-5.
Networks	by its source or destination IP address	You can explicitly specify IP addresses. To build a network condition, see Preprocessing Traffic Per Network, page 14-6.

If you do not configure a particular condition for a rule, the system does not match traffic based on that criterion. For example, a rule with a network condition but no zone condition evaluates traffic based on its source or destination IP address, regardless of its ingress or egress interface. Traffic that does not match any network analysis rules is preprocessed by the default network analysis policy.

To add a custom network analysis rule:

Step 1 In the access control policy where you want to create custom preprocessing configurations, select the **Advanced** tab, then click the edit icon ( ) next to the Intrusion and Network Analysis Policies section.

The Network and Analysis Policies dialog box appears. If you have not added any custom network analysis rules, the module interface indicates that you have **No Custom Rules**, otherwise it displays how many you have configured.

Tip Click **Network Analysis Policy List** to display the Network Analysis Policy page in a new window. Use this page to view and edit your custom network analysis policies; see Managing Network Analysis Policies, page 15-3

Step 2 Next to **Network Analysis Rules**, click the statement that indicates how many custom rules you have.

The dialog box expands to show the custom rules, if any.

Step 3 Click **Add Rule**.

The network analysis rule editor appears.

Step 4 Build your rule's conditions. You can restrict NAP preprocessing using the following criteria:

- Preprocessing Traffic Per Zone, page 14-5
- Preprocessing Traffic Per Network, page 14-6

Step 5 Associate a network analysis policy with the rule by clicking the **Network Analysis** tab and choosing a policy from the **Network Analysis Policy** drop-down list.

The system uses the network analysis policy you choose to preprocess traffic that meets all the rule's conditions. Note that if you choose a user-created policy, you can click an edit icon ( ) to edit the policy in a new window. You cannot edit system-provided policies.

Caution Do **not** use `Experimental Policy 1` unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

Step 6 Click **Add**.

The rule is added after any other rules. To change the rule's evaluation order, see Managing Network Analysis Rules, page 14-7.

Preprocessing Traffic Per Zone

License: Any

Zone conditions in network analysis rules allow you to preprocess traffic by its source and destination security zones. A security zone is a grouping of one or more interfaces. For more information on creating zones, see Working with Security Zones, page 2-33.

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 **Destination Zones**. Note that 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 **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.

Warning icons ( ) indicate invalid configurations, such as zones that contain no interfaces. For details, see Troubleshooting Access Control Policies and Rules, page 4-12.

To preprocess traffic by zone:

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

For detailed instructions, see Specifying Traffic to Preprocess Using Network Analysis Rules, page 14-4.

Step 2 In the network analysis 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 Deploying Configuration Changes, page 4-11.

Preprocessing Traffic Per Network

License: Any

Network conditions in network analysis rules allow you to preprocess traffic by its source and destination IP address. You can manually specify the source and destination IP addresses for the traffic you want to preprocess, or you can configure network conditions with network objects, which are reusable and associate a name with one or more IP addresses and address blocks.

Tip After you create a network object, you can use it not only to build network analysis rules, but also to represent IP addresses in various other places in the system's module interface. You can create these objects using the object manager; you can also create network objects on-the-fly while you are configuring network analysis rules. For more information, see Working with Network Objects, page 2-3.

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

- To match traffic from an IP address, configure **Source Networks**.
- To match traffic to an IP address, configure **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, see Troubleshooting Access Control Policies and Rules, page 4-12.

To preprocess traffic by network:

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

For detailed instructions, see Specifying Traffic to Preprocess Using Network Analysis Rules, page 14-4.

Step 2 In the network analysis 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:

- 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 2-3.
- To search for networks to add, 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 Deploying Configuration Changes, page 4-11.

Managing Network Analysis Rules

License: Any

A network analysis rule is simply a set of configurations and conditions that specifies how you preprocess traffic that matches those qualifications. You create and edit network analysis rules in the advanced options in an existing access control policy. Each rule belongs to only one policy.

To edit a custom network analysis rule:

Step 1 In the access control policy where you want to change your custom preprocessing configurations, select the **Advanced** tab, then click the edit icon ( ) next to the Intrusion and Network Analysis Policies section.

The Network and Analysis Policies dialog box appears. If you have not added any custom network analysis rules, the module interface indicates that you have **No Custom Rules**; otherwise, it displays how many you have configured.

Step 2 Next to **Network Analysis Rules**, click the statement that indicates how many custom rules you have.

The dialog box expands to show the custom rules, if any.

Step 3 Edit your custom rules. You have the following options:

- To edit a rule's conditions, or change the network analysis policy invoked by the rule, click the edit icon ( ) next to the rule.
- To change a rule's order of evaluation, click and drag the rule to the correct location. To select multiple rules, use the Shift and Ctrl keys.
- To delete a rule, click the delete icon ( ) next to the rule.

Step 4 Click **OK** to save your changes.

You must apply the access control policy for your changes to take effect; see Deploying Configuration Changes, page 4-11.