

Advanced Access Control settings for Network Analysis and Intrusion Policies

This chapter describes how to configure advanced settings for network analysis and intrusion policies.

- Advanced access control settings for network analysis and intrusion policies, on page 1
- Advanced access control settings for network analysis and intrusion policies, on page 1
- Requirements and prerequisites for advanced access control settings for network analysis and intrusion policies, on page 2
- Inspection of packets that pass before traffic is identified, on page 2
- Advanced settings for network analysis policies, on page 4

Advanced access control settings for network analysis and intrusion policies

Advanced access control settings are intrusion detection and prevention configurations that

- require specific expertise to configure,
- typically require little or no modification, and
- are not common to every deployment.

Version compatibility

Advanced access control settings for network analysis and intrusion policies

Advanced access control settings are intrusion detection and prevention configurations that

- require specific expertise to configure,
- typically require little or no modification, and
- are not common to every deployment.

Version compatibility

Requirements and prerequisites for advanced access control settings for network analysis and intrusion policies

This reference provides the system requirements, software prerequisites, and configuration dependencies needed to implement advanced access control settings for network analysis and intrusion detection policies in Cisco Secure Firewall environments.

Model support

Any.

Supported domains

Any

User roles

- Administrator
- Access Admin
- Network Admin

Inspection of packets that pass before traffic is identified

Inspection of packets that pass before traffic is identified is a network security process that

- allows a few packets to pass initially for connection establishment and traffic identification,
- enables features like URL filtering, application detection, rate limiting, and Intelligent Application Bypass to function properly, and
- requires explicit configuration in access control policies to inspect, prevent, and generate events for these initial packets.

Configuration requirements

You must explicitly configure your access control policy to inspect these packets, prevent them from reaching their destination, and generate any events.

As soon as 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.

Best practices for handling packets that pass before traffic identification

The default action specified for an access control policy is NOT applied to these packets.

Use these guidelines to choose a value for the **Intrusion Policy used before Access Control rule is determined** setting in the Advanced settings of the access control policy.

- You can choose a system-created or custom intrusion policy. For example, you can choose **Balanced Security and Connectivity**.
- For performance reasons, unless you have good reason to do otherwise, this setting should match the default action set for your access control policy.
- If your system does NOT perform intrusion inspection (for example, in a discovery-only deployment), select **No Rules Active**. The system will NOT inspect these initial packets, and they will be allowed to pass.
- By default, this setting uses the default variable set. Ensure that this is suitable for your purposes. For information, see Variable sets.
- The network analysis policy associated with the first matching network analysis rule preprocesses traffic for the policy you select. If there are no network analysis rules, or none match, the default network analysis policy is used.

Specify a policy to handle packets that pass before traffic identification

This task explains how to specify the system's behavior for network traffic during the period before traffic identification is complete.

Note This setting is sometimes referred to as the *default intrusion policy*. (This is distinct from the default action for an access control policy.)

Before you begin

Review best practices for these settings. See Best practices for handling packets that pass before traffic identification, on page 2.

Follow these steps to specify a policy to handle packets that pass before traffic identification:

Procedure

Step 1 In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the **Network Analysis and Intrusion Policies** section.

If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 2 Select an intrusion policy from the **Intrusion Policy used before Access Control rule is determined** drop-down list.

If you choose a user-created policy, you can click **Edit** (✎) to edit the policy in a new window. You cannot edit system-provided policies.

Step 3 Optionally, select a different variable set from the **Intrusion Policy Variable Set** drop-down list. You can also select **Edit** (✎) next to the variable set to create and edit variable sets. If you do not change the variable set, the system uses a default set.

Step 4 Click **OK**.

Step 5 Click **Save** to save the policy.

What to do next

- Deploy configuration changes.

Advanced settings for network analysis policies

A *network analysis policy* is a traffic preprocessing configuration that governs how traffic is decoded and preprocessed so that it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.

Advanced configuration concepts

This traffic preprocessing occurs after Security Intelligence matching and traffic decryption, but before intrusion policies inspect packets in detail. By default, the system-provided Balanced Security and Connectivity network analysis policy is the default network analysis 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. If you are an advanced user with a complex deployment, 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, networks, or VLANs.

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

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.

Set the default network analysis policy

Setting a default network analysis policy establishes the baseline preprocessing behavior for network traffic analysis within your access control policy.

You can choose a system- or user-created 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 web 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.

Procedure

Step 1 In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the Network Analysis and Intrusion Policies section.

If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 2 From the **Default Network Analysis Policy** drop-down list, select a default network analysis policy.

If you choose a user-created policy, you can click **Edit** (✎) to edit the policy in a new window. You cannot edit system-provided policies.

Step 3 Click **OK**.

Step 4 Click **Save** to save the policy.

What to do next

- Deploy configuration changes.

Network analysis rules

A network analysis rule is a preprocessing configuration component that

- tailors preprocessing configurations to network traffic within access control policy advanced settings,
- matches packets in top-down order by ascending rule number, starting at 1, and
- preprocesses traffic according to the first rule where all conditions match.

Network analysis rule conditions and matching

You can add zone, network, and VLAN tag conditions to a rule. 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.

Network analysis policy rule conditions

Network analysis policy rule conditions are configuration parameters that enable you to fine-tune your network analysis policy to target the users and networks you want to control.

Security zone rule conditions

A security zone rule condition is a network traffic control mechanism that

- segments your network to help you manage, classify, and decrypt traffic flow by grouping interfaces across multiple devices,
- controls or decrypts traffic by its source and destination security zones, and
- requires all interfaces in a zone to be of the same type (all inline, passive, switched, or routed).

Zone condition traffic matching

If you add both source and destination zones to a zone condition, matching traffic must originate from an interface in one of the source zones and leave through an interface in one of the destination zones.

All zones used in a zone condition must be of the same type. Because devices deployed passively do not transmit traffic, you cannot use a zone with passive interfaces as a destination zone.

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.

Tip Constraining rules by zone is one of the best ways to improve system performance. If a rule does not apply to traffic through any of device's interfaces, that rule does not affect that device's performance.

Network rule conditions

A network condition is a traffic matching criterion that

- matches traffic for rate limiting based on source and destination IP addresses using inner packet headers,
- enables administrators to specify exact IP addresses or blocks for granular policy enforcement, and
- can be built using predefined network objects or by manually entering IP addresses or address blocks.

Network rule condition restrictions

Minimize the number of matching criteria whenever possible, especially those for security zones, network objects, and port objects. When you specify multiple criteria, the system must match against *every* combination of the contents of the criteria you specify.



Note You *cannot* use FQDN network objects in identity rules.

VLAN tag rule conditions

VLAN tags rule conditions are filtering mechanisms that

- control VLAN-tagged traffic, including Q-in-Q (stacked VLAN) traffic
- use the innermost VLAN tag to filter VLAN traffic, with the exception of prefilter policy which uses the outermost VLAN tag, and
- apply only to inline sets and do not match traffic on firewall interfaces.

VLAN tag rule conditions configuration details



Note VLAN tags in access rules only apply to inline sets. Access rules with VLAN tags do not match traffic on firewall interfaces.

The system uses the innermost VLAN tag to filter VLAN traffic, with the exception of the prefilter policy, which uses the outermost VLAN tag in its rules.

Note this Q-in-Q support:

- Firewall Threat Defense on Firepower 4100/9300—Does not support Q-in-Q (supports only one VLAN tag).
- Firewall Threat Defense on all other models:
  - Inline sets and passive interfaces—Supports Q-in-Q, up to 2 VLAN tags.
  - Firewall interfaces—Does not support Q-in-Q (supports only one VLAN tag).

You can use predefined objects to build VLAN conditions, or manually enter any VLAN tag from 1 to 4094. Use a hyphen to specify a range of VLAN tags.

In a cluster, if you encounter problems with VLAN matching, edit the access control policy advanced options, Transport/Network Preprocessor Settings, and select the **Ignore the VLAN header when tracking connections** option.

Configure network analysis rules

Network analysis rules allow you to specify which network analysis policy should preprocess traffic that matches specific conditions, providing granular control over traffic inspection before intrusion detection.

Network analysis rules are configured within the advanced settings of an access control policy. You can create custom rules to apply different network analysis policies based on traffic conditions such as source, destination, ports, or applications.

Before you begin

Follow these steps to configure network analysis rules:

Procedure

Step 1 In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the Network Analysis and Intrusion Policies section.

If **View** (👁) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Tip Click **Network Analysis Policy List** to view and edit existing custom network analysis policies.

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

Step 3 Click **Add Rule**.

Step 4 Configure the rule's conditions by clicking the conditions you want to add.

Step 5 Click **Network Analysis** and choose the **Network Analysis Policy** you want to use to preprocess the traffic matching this rule.

Click **Edit** (✎) to edit a custom policy in a new window. You cannot edit system-provided policies.

Step 6 Click **Add**.

What to do next

- Deploy configuration changes.

Manage network analysis rules

Network analysis rules allow you to control how traffic preprocessing occurs by defining specific conditions and configurations that determine traffic handling methods.

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.

Procedure

Step 1 In the access control policy editor, click **Advanced**, then click **Edit** (✎) next to the Intrusion and Network Analysis Policies section.

If **View** ( ) appears instead, settings are inherited from an ancestor policy, or you do not have permission to modify the settings.If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

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

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 **Edit** ( ) 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 **Delete** ( ) next to the rule.

Tip Right-click a rule to display a context menu that lets you cut, copy, paste, edit, delete, or add new network analysis rules.

Step 4 Click **OK**.

Step 5 Click **Save** to save the policy.

What to do next

- Deploy configuration changes.