Getting Started with Network Analysis Policies

Network analysis policies govern many traffic preprocessing options, and are invoked by advanced settings in your access control policy. Network analysis-related preprocessing occurs after Security Intelligence blacklisting and SSL decryption, but before intrusion or file inspection begins.

By default, the system uses the *Balanced Security and Connectivity* network analysis policy to preprocess all traffic handled by an access control policy. However, you can choose a different default network analysis policy to perform this preprocessing. For your convenience, the system provides a choice of several non-modifiable network analysis policies, which are tuned for a specific balance of security and connectivity by the Cisco Vulnerability Research Team (VRT). You can also replace this default policy with a custom network analysis policy with custom preprocessing settings.

Tip System-provided intrusion and network analysis policies are similarly named but contain different configurations. For example, the 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. Understanding Network Analysis and Intrusion Policies, page 23-1 provides an overview of how network analysis and intrusion policies work together to examine your traffic, as well as some basics on using the navigation panel, resolving conflicts, and committing changes.

You can also tailor traffic preprocessing options to specific security zones, networks, and VLANs by creating multiple custom network analysis policies, then assigning them to preprocess different traffic. (Note that ASA FirePOWER devices cannot restrict preprocessing by VLAN.)

Note Tailoring preprocessing, especially using multiple custom network analysis policies, is an **advanced** task. Because preprocessing and intrusion inspection are so closely related, the network analysis and intrusion policies examining a single packet **must** complement each other. The system does **not** coordinate the policies for you. For more information, see Limitations of Custom Policies, page 23-12.

This chapter explains how to create a simple custom network analysis policy. This chapter also contains basic information on managing network analysis policies: editing, comparing, and so on. For more information, see:

- Comparing Two Network Analysis Policies or Revisions, page 26-9

Creating a Custom Network Analysis Policy

License: Protection

When you create a new network analysis policy you must give it a unique name, specify a base policy, and choose an *inline mode*.

The base policy defines the network analysis policy's default settings. Modifying a setting in the new policy overrides—but does not change—the settings in the base policy. You can use either a system-provided or custom policy as your base policy. For more information, see Understanding the Base Layer, page 24-2.

The network analysis policy's inline mode allows preprocessors to modify (normalize) and drop traffic to minimize the chances of attackers evading detection. Note that in passive deployments, the system cannot affect traffic flow regardless of the inline mode. For more information, see Allowing Preprocessors to Affect Traffic in Inline Deployments, page 26-5.

To create a network analysis policy:

Access: Admin/Intrusion Admin

Step 1 Select **Policies > Access Control** to display the Access Control Policy page, then click **Network Analysis Policy**.

The Network Analysis Policy page appears.

You can create and edit network analysis as well as intrusion policies if your FireSIGHT System user account's role is restricted to Intrusion Policy or Modify Intrusion Policy. To access the Network Analysis Policy page, select **Policies > Intrusion**, then click **Network Analysis Policy**. For more information, see Managing Custom User Roles, page 61-53.

Step 2 Click **Create Policy**.

If you have unsaved changes in another policy, click **Cancel** when prompted to return to the Network Analysis Policy page. See Resolving Conflicts and Committing Policy Changes, page 23-16 for information on saving unsaved changes in another policy.

The Create Network Analysis Policy pop-up window appears.

Step 3 Give the policy a unique **Name** and, optionally, a **Description**.

Step 4 Specify the initial **Base Policy**.

You can use either a system-provided or custom policy as your base policy.

Step 5 Specify whether you want to allow preprocessors to affect traffic in an inline deployment:

- To allow preprocessors to affect traffic, enable **Inline Mode**.
- To prevent preprocessors from affecting traffic, disable **Inline Mode**.

Step 6 Create the policy:

- Click **Create Policy** to create the new policy and return to the Network Analysis Policy page. The new policy has the same settings as its base policy.
- Click **Create and Edit Policy** to create the policy and open it for editing in the advanced network analysis policy editor; see Editing Network Analysis Policies, page 26-3.

Managing Network Analysis Policies

License: Protection

On the Network Analysis Policy page (**Policies > Access Control**, then click **Network Analysis Policy**) you can view your current custom network analysis policies, along with the following information:

- the time and date the policy was last modified (in local time) and the user who modified it
- whether the **Inline Mode** setting is enabled, which allows preprocessors to affect traffic
- which access control policies and devices are using the network analysis policy to preprocess traffic
- whether a policy has unsaved changes, as well as information about who (if anyone) is currently editing the policy

In addition to custom policies that you create, the system provides two custom policies: Initial Inline Policy and Initial Passive Policy. These two network analysis policies use the Balanced Security and Connectivity network analysis policy as their base. The only difference between them is their inline mode, which allows preprocessors to affect traffic in the inline policy and disables it in the passive policy. You can edit and use these system-provided custom policies.

Options on the Network Analysis Policy page allow you to take the actions in the following table.

Table 26-1 Network Analysis Policy Management Actions

To...	You can...	See...
create a new network analysis policy	click **Create Policy**.	Creating a Custom Network Analysis Policy, page 26-2.
edit an existing network analysis policy	click the edit icon ( ).	Editing Network Analysis Policies, page 26-3.
view a PDF report that lists the current configuration settings in a network analysis policy	click the report icon ( ).	Generating a Report of Current Network Analysis Settings, page 26-8
compare the settings of two network analysis policies or two revisions of the same policy	click **Compare Policies**.	Comparing Two Network Analysis Policies or Revisions, page 26-9.
delete a network analysis policy	click the delete icon ( ), then confirm that you want to delete the policy. You cannot delete a network analysis policy if an access control policy references it.	

Note that you can create and edit network analysis as well as intrusion policies if your FireSIGHT System user account's role is restricted to Intrusion Policy or Modify Intrusion Policy. To access the Network Analysis Policy page, select **Policies > Intrusion**, then click **Network Analysis Policy**. For more information, see Managing Custom User Roles, page 61-53.

Editing Network Analysis Policies

License: Protection

When you create a new network analysis policy, it has the same settings as its base policy. The following table lists the most common actions you can take to tailor the new policy to your needs:

Table 26-2 Network Analysis Policy Editing Actions

To...	You can...	See...
allow preprocessors to modify or drop traffic	select the **Inline Mode** check box on the Policy Information page.	Allowing Preprocessors to Affect Traffic in Inline Deployments, page 26-5
change the base policy	select a base policy from the **Base Policy** drop-down list on the Policy Information page.	Changing the Base Policy, page 24-4
view the settings in the base policy	click **Manage Base Policy** on the Policy Information page.	Understanding the Base Layer, page 24-2
enable, disable, or edit the settings for a preprocessor	click **Settings** in the navigation panel.	Configuring Preprocessors in a Network Analysis Policy, page 26-6
manage policy layers	click **Policy Layers** in the navigation panel.	Using Layers in a Network Analysis or Intrusion Policy, page 24-1

When tailoring a network analysis policy, especially when disabling preprocessors, keep in mind that some preprocessors and intrusion rules require that traffic first be decoded or preprocessed in a certain way. If you disable a required preprocessor, the system automatically uses it with its current settings, although the preprocessor remains disabled in the network analysis policy web interface.

Note Because preprocessing and intrusion inspection are so closely related, the network analysis and intrusion policies examining a single packet **must** complement each other. Tailoring preprocessing, especially using multiple custom network analysis policies, is an **advanced** task. For more information, see Limitations of Custom Policies, page 23-12.

The system caches one network analysis policy per user. While editing a network analysis policy, if you select any menu or other path to another page, your changes stay in the system cache even if you leave the page. In addition to the actions you can perform in the table above, Understanding Network Analysis and Intrusion Policies, page 23-1 provides information on using the navigation panel, resolving conflicts, and committing changes.

To edit a network analysis policy:

Access: Admin/Intrusion Admin

Step 1 Select **Policies > Access Control** to display the Access Control Policy page, then click **Network Analysis Policy**.

The Network Analysis Policy page appears.

Step 2 Click the edit icon ( ) next to the network analysis policy you want to configure.

The network analysis policy editor appears, focused on the Policy Information page and with a navigation panel on the left.

Step 3 Edit your policy. Take any of the actions summarized above.

Step 4 Save your policy, continue editing, discard your changes, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Allowing Preprocessors to Affect Traffic in Inline Deployments

License: Protection

In an inline deployment, some preprocessors can modify and block traffic. For example:

- The inline normalization preprocessor normalizes packets to prepare them for analysis by other preprocessors and the intrusion rules engine. You can also use the preprocessor's **Allow These TCP Options** and **Block Unrecoverable TCP Header Anomalies** options to block certain packets. For more information, see Normalizing Inline Traffic, page 29-6.
- The system can drop packets with invalid checksums; see Verifying Checksums, page 29-5.
- The system can drop packets matching rate-based attack prevention settings; see Preventing Rate-Based Attacks, page 34-9.

For a preprocessor configured in the network analysis policy to affect traffic, you must enable and correctly configure the preprocessor, as well as correctly deploy managed devices inline, that is, with inline interface sets. Finally, you must enable the network analysis policy's **Inline Mode** setting.

If you want to assess how your configuration would function in an inline deployment without actually modifying traffic, you can disable inline mode. In passive deployments or inline deployments in tap mode, the system cannot affect traffic regardless of the inline mode.

Note that disabling inline mode can affect intrusion event performance statistics graphs. With inline mode enabled in an inline deployment, the Intrusion Event Performance page (**Overview > Summary > Intrusion Event Performance**) displays graphs that represent normalized and blocked packets. If you disable inline mode, or in a passive deployment, many of the graphs display data about the traffic the system would have normalized or dropped. For more information, see Generating Intrusion Event Performance Statistics Graphs, page 41-5.

Tip In an inline deployment, Cisco recommends that you enable inline mode and configure the inline normalization preprocessor with the **Normalize TCP Payload** option enabled. In a passive deployment,Cisco recommends you configure adaptive profiles.

To allow preprocessors to affect traffic in an inline deployment:

Access: Admin/Intrusion Admin

Step 1 Select **Policies > Access Control** to display the Access Control Policy page, then click **Network Analysis Policy**.

The Network Analysis Policy page appears.

Step 2 Click the edit icon ( ) next to the policy you want to edit.

The Policy Information page appears.

Step 3 Specify whether you want to allow preprocessors to affect traffic:

- To allow preprocessors to affect traffic, enable **Inline Mode**.

- To prevent preprocessors from affecting traffic, disable **Inline Mode**.

Step 4 Save your policy, continue editing, discard your changes, or exit while leaving your changes in the system cache. For more information, see Resolving Conflicts and Committing Policy Changes, page 23-16.

Configuring Preprocessors in a Network Analysis Policy

License: Protection

Preprocessors prepare traffic to be further inspected by normalizing traffic and identifying protocol anomalies. Preprocessors can generate preprocessor events (see Reading Preprocessor Events, page 41-38) when packets trigger preprocessor options that you configure. The base policy for your network analysis policy determines which preprocessors are enabled by default and the default configuration for each.

When you select **Settings** in the navigation panel of a network analysis policy, the policy lists its preprocessors by type. On the Settings page, you can enable or disable preprocessors in your network analysis policy, as well as access preprocessor configuration pages.

A preprocessor must be enabled for you to configure it. When you enable a preprocessor, a sublink to the configuration page for the preprocessor appears beneath the **Settings** link in the navigation panel, and an **Edit** link to the configuration page appears next to the preprocessor on the Settings page.

Tip To revert a preprocessor's configuration to the settings in the base policy, click **Revert to Defaults** on a preprocessor configuration page. When prompted, confirm that you want to revert.

When you disable a preprocessor, the sublink and **Edit** link no longer appear, but your configurations are retained. Note that to perform their particular analysis, many preprocessors and intrusion rules require that traffic first be decoded or preprocessed in a certain way. If you disable a required preprocessor, the system automatically uses it with its current settings, although the preprocessor remains disabled in the network analysis policy web interface.

Note In most cases, preprocessors require specific expertise to configure and typically require little or no modification. Tailoring preprocessing, especially using multiple custom network analysis policies, is an **advanced** task. Because preprocessing and intrusion inspection are so closely related, the network analysis and intrusion policies examining a single packet **must** complement each other. For more information, see Limitations of Custom Policies, page 23-12.

Modifying a preprocessor configuration requires an understanding of the configuration and its potential impact on your network. The following sections provide links to specific configuration details for each preprocessor.

Application Layer Preprocessors

Application-layer protocol decoders normalize specific types of packet data into formats that the intrusion rules engine can analyze.

Table 26-3 Application Layer Preprocessor Settings

For information on...	See...
DCE/RPC Configuration	Decoding DCE/RPC Traffic, page 27-2
DNS Configuration	Detecting Exploits in DNS Name Server Responses, page 27-14
FTP and Telnet Configuration	Decoding FTP and Telnet Traffic, page 27-18
HTTP Configuration	Decoding HTTP Traffic, page 27-30
Sun RPC Configuration	Using the Sun RPC Preprocessor, page 27-44
SIP Configuration	Decoding the Session Initiation Protocol, page 27-46
GTP Command Channel Configuration	Configuring the GTP Command Channel, page 27-51
IMAP Configuration	Decoding IMAP Traffic, page 27-52
POP Configuration	Decoding POP Traffic, page 27-55
SMTP Configuration	Decoding SMTP Traffic, page 27-58
SSH Configuration	Detecting Exploits Using the SSH Preprocessor, page 27-65
SSL Configuration	Using the SSL Preprocessor, page 27-69

SCADA Preprocessors

The Modbus and DNP3 preprocessors detect traffic anomalies and provide data to the intrusion rules engine for inspection.

Table 26-4 SCADA Preprocessor Settings

For information on...	See...
Modbus Configuration	Configuring the Modbus Preprocessor, page 28-1
DNP3 Configuration	Configuring the DNP3 Preprocessor, page 28-3

Transport/Network Layer Preprocessors

Network and transport layers preprocessors detect exploits at the network and transport layers. Before packets are sent to preprocessors, the packet decoder converts packet headers and payloads into a format that can be easily used by the preprocessors and the intrusion rules engine; it also detects various anomalous behaviors in packet headers.

Table 26-5 Transport and Network Layer Preprocessor Settings

For information on...	See...
Checksum Verification	Verifying Checksums, page 29-5
Inline Normalization	Normalizing Inline Traffic, page 29-6
IP Defragmentation	Defragmenting IP Packets, page 29-11
Packet Decoding	Understanding Packet Decoding, page 29-16

Table 26-5 Transport and Network Layer Preprocessor Settings (continued)

For information on...	See...
TCP Stream Configuration	Using TCP Stream Preprocessing, page 29-20
UDP Stream Configuration	Using UDP Stream Preprocessing, page 29-32

Note that some advanced transport and network preprocessor settings apply globally to all networks, zones, and VLANs where you apply your access control policy. You configure these advanced settings in an access control policy rather than in a network analysis policy; see Configuring Advanced Transport/Network Settings, page 29-2.

Specific Threat Detection

The Back Orifice preprocessor analyzes UDP traffic for the Back Orifice magic cookie. The portscan detector can be configured to report scan activity. Rate-based attack prevention can help you protect your network against SYN floods and an extreme number of simultaneous connections designed to overwhelm your network.

Table 26-6 Specific Threat Detection Settings

For information on...	See...
Back Orifice Detection	Detecting Back Orifice, page 34-1
Portscan Detection	Detecting Portscans, page 34-2
Rate-Based Attack Prevention	Preventing Rate-Based Attacks, page 34-9

Note that you configure the sensitive data preprocessor, which detects sensitive data such as credit card numbers and Social Security numbers in ASCII text, in intrusion policies. For more information, see Detecting Sensitive Data, page 34-19.

Generating a Report of Current Network Analysis Settings

License: Protection

A network analysis policy report is a record of the policy configuration at a specific point in time. The system combines the settings in the base policy with the settings of the policy layers, and makes no distinction between which settings originated in the base policy or policy layer.

You can use the report, which contains the following information, for auditing purposes or to inspect the current configuration.

Table 26-7 Network Analysis Policy Report Sections

Section	Description
Policy Information	Provides the name and description of the policy, the name of the user who last modified the policy, and the date and time the policy was last modified. Also indicates whether inline normalization can be enabled, the current rule update version, and whether the base policy is locked to the current rule update.
Settings	Lists all enabled preprocessor settings and their configurations.

You can also generate a comparison report that compares two network analysis policies, or two revisions of the same policy. For more information, see Comparing Two Network Analysis Policies or Revisions, page 26-9.

To view a network analysis policy report:

Access: Admin/Intrusion Admin

Step 1 Select **Policies > Access Control** to display the Access Control Policy page, then click **Network Analysis Policy**.

The Network Analysis Policy page appears.

Step 2 Click the report icon () next to the policy for which you want to generate a report. Remember to commit any changes before you generate a network analysis policy report; only committed changes appear in the report.

The system generates the report. Depending on your browser settings, the report may appear in a pop-up window, or you may be prompted to save the report to your computer.

Comparing Two Network Analysis Policies or Revisions

License: Protection

To review policy changes for compliance with your organization's standards or to optimize system performance, you can examine the differences between two network analysis policies. You can compare any two network analysis policies or two revisions of the same network analysis policy. Optionally, after you compare, you can then generate a PDF report to record the differences between the two policies or policy revisions.

There are two tools you can use to compare network analysis policies or policy revisions:

- The comparison view displays only the differences between two network analysis policies or network analysis policy revisions in a side-by-side format; the name of each policy or policy revision appears in the title bar on the left and right sides of the comparison view.

  You can use this to view and navigate both policy revisions on the web interface, with their differences highlighted.

- The comparison report creates a record of only the differences between two network analysis policies or network analysis policy revisions in a format similar to the network analysis policy report, but in PDF format.

  You can use this to save, copy, print and share your policy comparisons for further examination.

For more information on understanding and using the policy comparison tools, see:

- Using the Network Analysis Policy Comparison View, page 26-9
- Using the Network Analysis Policy Comparison Report, page 26-10

Using the Network Analysis Policy Comparison View

License: Protection

The comparison view displays both policies or policy revisions in a side-by-side format, with each policy or policy revision identified by name in the title bar on the left and right sides of the comparison view. The time of last modification and the last user to modify are displayed with the policy name.

Differences between the two policies are highlighted:

- Blue indicates that the highlighted setting is different in the two policies, and the difference is noted in red text.
- Green indicates that the highlighted setting appears in one policy but not the other.

You can perform any of the actions in the following table.

Table 26-8 Network Analysis Policy Comparison View Actions

To...	You can...
navigate individually through changes	click **Previous** or **Next** above the title bar. The double-arrow icon ( ) centered between the left and right sides moves, and the **Difference** number adjusts to identify which difference you are viewing.
determine which layer contains the configuration for a specific preprocessor	hover your pointer over the advanced configuration icon ( ) next to the configuration you want to view. The window displays the name of the layer that contains the preprocessor configuration.
generate a new policy comparison view	click **New Comparison**. The **Select Comparison** window appears. See Using the Network Analysis Policy Comparison Report, page 26-10 for more information.
generate a policy comparison report	click **Comparison Report**. The policy comparison report creates a PDF document that lists only the differences between the two policies or policy revisions.

Using the Network Analysis Policy Comparison Report

License: Protection

A network analysis policy comparison report is a record of all differences between two network analysis policies or two revisions of the same network analysis policy identified by the network analysis policy comparison view, presented as a PDF. You can use this report to further examine the differences between two network analysis policy configurations and to save and disseminate your findings.

You can generate a network analysis policy comparison report from the comparison view for any policies to which you have access. Remember to save any changes before you generate a policy report; only saved changes appear in the report.

The format of the policy comparison report is the same as the policy report with one exception: the policy report contains all configurations in the policy, and the policy comparison report lists only those configurations that differ between the policies. A network analysis policy comparison report contains the sections described in Table 26-7 on page 26-8.

Tip You can use a similar procedure to compare SSL, access control, intrusion, file, system, or health policies.

To compare two network analysis policies or policy revisions:

Access: Admin/Intrusion Admin

Step 1 Select **Policies > Access Control** to display the Access Control Policy page, then click **Network Analysis Policy**.

The Network Analysis Policy page appears.

Step 2 Click **Compare Policies**.

The Select Comparison window appears.

Step 3 From the **Compare Against** drop-down list, select the type of comparison you want to make:

- To compare two different policies, select **Other Policy**.

  The page refreshes and the Policy A and Policy B drop-down lists appear.
- To compare two revisions of the same policy, select **Other Revision.**

  The page refreshes and the Policy, Revision A, and Revision B drop-down lists appear.

Step 4 Depending on the comparison type you selected, you have the following choices:

- If you are comparing two different policies, select the policies you want to compare from the Policy A and Policy B drop-down lists.
- If you are comparing two revision of the same policy, select the Policy, then select the timestamped revisions you want to compare from the Revision A and Revision B drop-down lists.

Step 5 Click **OK** to display the policy comparison view.

The comparison view appears.

Step 6 Optionally, click **Comparison Report** to generate the network analysis policy comparison report.

The network analysis policy comparison report appears. Depending on your browser settings, the report may appear in a pop-up window, or you may be prompted to save the report to your computer.