Configuring External Alerting for Intrusion Rules

While the ASA FirePOWER module provides various views of intrusion events within the user interface, some enterprises prefer to define external intrusion event notification to facilitate constant monitoring of critical systems. You can enable logging to syslog facilities or send event data to an SNMP trap server.

Within each intrusion policy, you can specify intrusion event notification limits, set up intrusion event notification to external logging facilities, and configure external responses to intrusion events.

Tip Some analysts prefer not to receive multiple alerts for the same intrusion event, but want to control how often they are notified of a given intrusion event occurrence. See Filtering Intrusion Event Notification Per Policy, page 21-20 for more information.

There is another type of alerting you can perform in the ASA FirePOWER module, outside of your intrusion policies. You can configure SNMP and syslog alert responses for other types of events, including connection events logged by specific access control rules. For more information, see Configuring External Alerting, page 29-1.

See the following sections for more information on external intrusion event notification:

- Using SNMP Responses, page 30-1 describes the options you can configure to send event data to specified SNMP trap servers and provides the procedure for specifying the SNMP alerting options.
- Using Syslog Responses, page 30-4 describes the options you can configure to send event data to an external syslog and provides the procedure for specifying the syslog alerting options.

Using SNMP Responses

License: Protection

An *SNMP trap* is a network management notification. You can configure the device to send intrusion event notifications as SNMP traps, also known as *SNMP alerts*. Each SNMP alert includes:

- the name of the server generating the trap
- the IP address of the device that detected it
- the name of the device that detected it
- the event data

You can set a variety of SNMP alerting parameters. Available parameters vary depending on the version of SNMP you use. For details on enabling and disabling SNMP alerting, see Configuring Advanced Settings in an Intrusion Policy, page 20-6.

Tip If your network management system requires a management information base file (MIB), you can obtain it from the ASA FirePOWER module at `/etc/sf/DCEALERT.MIB`.

SNMPv2 Options

For SNMPv2, you can specify the options described in the following table.

Table 30-1 SNMPv2 Options

Option	Description
Trap Type	The trap type to use for IP addresses that appear in the alerts. If your network management system correctly renders the INET_IPV4 address type, then you can select **as Binary**. Otherwise, select **as String**. For example, HP Openview requires the string type.
Trap Server	The server that will receive SNMP traps notification. You can specify a single IP address or hostname.
Community String	The community name.

Note SNMPv2 only supports read-only communities.

SNMPv3 Options

For SNMPv3, you can specify the options described in the following table.

Note When using SNMPv3, the appliance uses an Engine ID value to encode the message. Your SNMP server requires this value to decode the message. Currently, this Engine ID value will always be the hexadecimal version of the appliance's IP address with `01` at the end of the string. For example, if the appliance sending the SNMP alert has an IP address of `172.16.1.50`, the Engine ID is `0xAC10013201` or, if the appliance has an IP address of `10.1.1.77`, `0x0a01014D01` is used as the Engine ID.

Table 30-2 SNMPv3 Options

Option	Description
Trap Type	The trap type to use for IP addresses that appear in the alerts. If your network management system correctly renders the INET_IPV4 address type, then you can select **as Binary**. Otherwise, select **as String**. For example, HP Openview requires the string type.
Trap Server	The server that will receive SNMP traps notification. You can specify a single IP address or hostname.
Authentication Password	The password required for authentication. SNMPv3 uses either the Message Digest 5 (MD5) hash function or the Secure Hash Algorithm (SHA) hash function to encrypt this password, depending on configuration. If you specify an authentication password, authentication is enabled.

Table 30-2 SNMPv3 Options (continued)

Option	Description
Private Password	The SNMP key for privacy. SNMPv3 uses the Data Encryption Standard (DES) block cipher to encrypt this password. If you specify a private password, privacy is enabled. If you specify a private password, you must also specify an authentication password.
User Name	Your SNMP user name.

Note SNMPv3 only supports read-only users and encryption with AES128.

For information about configuring SNMP Alerting, see Configuring SNMP Responses, page 30-3.

Configuring SNMP Responses

License: Protection

You can configure SNMP alerting in an intrusion policy. After you apply the policy as part of an access control policy, the system notifies you of any intrusion events it detects via SNMP trap. For more details on SNMP alerting, see Using SNMP Responses, page 30-1.

To configure SNMP alerting options:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**.

The Intrusion Policy page appears.

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

If you have unsaved changes in another policy, click **OK** to discard those changes and continue. See Resolving Conflicts and Committing Policy Changes, page 12-15 for information on saving unsaved changes in another policy.

The Policy Information page appears.

Step 3 Click **Advanced Settings** in the navigation panel on the left.

The Advanced Settings page appears.

Step 4 You have two choices, depending on whether **SNMP Alerting** under External Responses is enabled:

- If the configuration is enabled, click **Edit**.
- If the configuration is disabled, click **Enabled**, then click **Edit**.

The SNMP Alerting page appears.

A message at the bottom of the page identifies the intrusion policy layer that contains the configuration. See Using Layers in a Network Analysis or Intrusion Policy, page 13-1 for more information.

Step 5 Specify the trap type format that you want to use for IP addresses that appear in the alerts, **as Binary** or **as String**.

Note If your network management system correctly renders the INET_IPV4 address type, then you can use the **as Binary** option. Otherwise, use the **as String** option. For example, HP OpenView requires the **as String** option.

Step 6 Select either SNMPv2 or SNMPv3:

- To configure SNMPv2, enter the IP address and the community name of the trap server you want to use in the corresponding fields. See SNMPv2 Options, page 30-2.
- To configure SNMPv3, enter the IP address of the trap server you want to use, an authentication password, a private password, and a user name in the corresponding fields. See SNMPv3 Options, page 30-2 for more information.

Note You must select SNMPv2 **or** SNMPv3. SNMPv2 only supports read-only communities and SNMPv3 only supports read-only users.

Note When you enter an SNMPv3 password, the password displays in plain text during initial configuration but is saved in encrypted format.

Step 7 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. See Resolving Conflicts and Committing Policy Changes, page 12-15 for more information.

Using Syslog Responses

License: Protection

The system log, or *syslog,* is the standard logging mechanism for network event logging. You can send *syslog alerts*, which are intrusion event notifications, to the syslog on an appliance. The syslog allows you to categorize information in the syslog by priority and facility. The *priority* reflects the severity of the alert and the *facility* indicates the subsystem that generated the alert. Facilities and priorities are not displayed in the actual message that appears in syslog, but are instead used to tell the system that receives the syslog message how to categorize it.

Syslog alerts contain the following information:

- date and time of alert generation
- event message
- event data
- generator ID of the triggering event
- Snort ID of the triggering event
- revision

In an intrusion policy, you can turn on syslog alerting and specify the syslog priority and facility associated with intrusion event notifications in the syslog. When you apply the intrusion policy as part of an access control policy, the system then sends syslog alerts for the intrusion events it detects to the

syslog facility on the local host or on the logging host specified in the policy. The host receiving the alerts uses the facility and priority information you set when configuring syslog alerting to categorize the alerts.

The following table lists the facilities you can select when configuring syslog alerting. Be sure to configure a facility that makes sense based on the configuration of the remote syslog server you use. The `syslog.conf` file located on the remote system (if you are logging syslog messages to a UNIX- or Linux-based system) indicates which facilities are saved to which log files on the server.

Table 30-3 Available Syslog Facilities

Facility	Description
AUTH	A message associated with security and authorization.
AUTHPRIV	A restricted access message associated with security and authorization. On many systems, these messages are forwarded to a secure file.
CRON	A message generated by the clock daemon.
DAEMON	A message generated by a system daemon.
FTP	A message generated by the FTP daemon.
KERN	A message generated by the kernel. On many systems, these messages are printed to the console when they appear.
LOCAL0-LOCAL7	A message generated by an internal process.
LPR	A message generated by the printing subsystem.
MAIL	A message generated by a mail system.
NEWS	A message generated by the network news subsystem.
SYSLOG	A message generated by the syslog daemon.
USER	A message generated by a user-level process.
UUCP	A message generated by the UUCP subsystem.

Select one of the following standard syslog priority levels to display on all notifications generated by this alert:

Table 30-4 Syslog Priority Levels

Level	Description
EMERG	A panic condition broadcast to all users
ALERT	A condition that should be corrected immediately
CRIT	A critical condition
ERR	An error condition
WARNING	Warning messages
NOTICE	Conditions that are not error conditions, but require attention
INFO	Informational messages
DEBUG	Messages that contain debug information

For more detailed information about how syslog works and how to configure it, refer to the documentation that accompanies your system. If you are logging to a UNIX- or Linux-based system's syslog, the `syslog.conf` man file (type `man syslog.conf` at the command line) and syslog man file (type `man syslog` at the command line) provide information about how syslog works and how to configure it.

Configuring Syslog Responses

License: Protection

You can configure syslog alerting in an intrusion policy. After you apply the policy as part of an access control policy, the system notifies you of any intrusion events it detects via the syslog. For more information on syslog alerting, see Using Syslog Responses, page 30-4.

To configure syslog alerting options:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies> Intrusion Policy**.

The Intrusion Policy page appears.

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

If you have unsaved changes in another policy, click **OK** to discard those changes and continue. See Resolving Conflicts and Committing Policy Changes, page 12-15 for information on saving unsaved changes in another policy.

The Policy Information page appears.

Step 3 Click **Advanced Settings** in the navigation panel on the left.

The Advanced Settings page appears.

Step 4 You have two choices, depending on whether **Syslog Alerting** under External Responses is enabled:

- If the configuration is enabled, click **Edit**.
- If the configuration is disabled, click **Enabled**, then click **Edit**.

The Syslog Alerting page appears.

A message at the bottom of the page identifies the intrusion policy layer that contains the configuration. See Using Layers in a Network Analysis or Intrusion Policy, page 13-1 for more information.

Step 5 Optionally, in the **Logging Hosts** field, enter the remote access IP address you want to specify as logging host. Separate multiple hosts with commas.

Step 6 Select facility and priority levels from the drop-down lists.

See Using Syslog Responses, page 30-4 for details on facility and priority options.

Step 7 Save your policy, continue editing, discard your changes, revert to the default configuration settings in the base policy, or exit while leaving your changes in the system cache. See Resolving Conflicts and Committing Policy Changes, page 12-15 for more information.