

External Alerting for Intrusion Events

The following topics describe how to configure external alerting for intrusion events:

- External alerts for intrusion events, on page 1
- License requirements for external alerting for intrusion events, on page 2
- Requirements for configuring external alerting for intrusion events, on page 2
- Configure SNMP alerting for intrusion events, on page 2
- Configure syslog alerting for intrusion events, on page 4
- Configure email alerting for intrusion events, on page 6

External alerts for intrusion events

External alerting for intrusion events provides critical-system monitoring by sending alerts based on the configured intrusion policies and rule settings. It supports sending external alerts using multiple external notification methods and operates independently of alert responses.

External alerting methods

- Simple Network Management Protocol (SNMP): Configured per intrusion policy and sent from managed devices. SNMP alerting can be enabled for individual intrusion rules.
- Syslog: Configured per intrusion policy and sent from managed devices. Enabling syslog alerting in an intrusion policy activates it for every rule in the policy.
- Email: Configured across all intrusion policies and sent from the Secure Firewall Management Center. You can enable email alerts per intrusion rule, as well as limit their length and frequency.

If you configure intrusion event suppression or thresholding, the system may not generate an intrusion event each time a rule triggers and you might receive fewer alerts.

Note The Secure Firewall Management Center also uses SNMP , email, and syslog *alert responses* to send different types of external alerts. For more information, refer to Configuring external alerts with alert responses. The system does not use alert responses to send alerts based on individual intrusion events.

Related Topics

Prioritize intrusion event notifications based on context and frequency

License requirements for external alerting for intrusion events

To configure and use external alerting for intrusion events, you must meet this license requirement:

Threat Defense License

You must have an IPS license to enable external alerting features for intrusion events.

Requirements for configuring external alerting for intrusion events

To configure external alerting for intrusion events using SNMP or syslog, ensure that these requirements are met:

Model support

All device models are supported.

Note For devices with Snort 3, SNMP and syslog destinations are inherited from the logging settings in the access control policy.

Supported domains

Any

User roles

- Administrator
- Intrusion Admin

Configure SNMP alerting for intrusion events

Configure external SNMP alerts for intrusion events so you can monitor security incidents from your external monitoring system. Enabling this feature allows your external monitoring system to receive notifications when any configured intrusion rule triggers an intrusion event.

The managed device sends alerts when specific intrusion events occur.

Note

- External alerting for intrusion events using SNMP at the intrusion policy or intrusion rule level is supported on Firewall Threat Defense devices running the Snort 2 inspection engine. On devices using Snort 3, SNMP trap destination is inherited from the logging settings in the access control policy.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Intrusion**.

Step 2 Click **Snort 2 Version**, and in the intrusion policy editor's navigation pane, click **Advanced Settings**.

Step 3 Enable **SNMP Alerting**, then click **Edit** next to **SNMP Alerting**.

A message appears at the bottom of the page, identifying the intrusion policy layer that contains the configuration.

Step 4 Choose the **Trap Type**.

Step 5 Choose an **SNMP Version**, then specify configuration options as described in Intrusion SNMP alert configuration options, on page 3.

Step 6 In the navigation pane, click **Rules**.

Step 7 Choose the rules for which you want to enable SNMP alerts. Then, from the **Alerting** drop-down list, choose **Add SNMP Alert**.

Step 8 To save changes you made in this policy since the last policy commit, choose **Policy Information**, then click **Commit Changes**.

If you leave the policy editor without committing, unsaved changes are discarded when you edit a different policy.

What to do next

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Intrusion SNMP alert configuration options

If your network management system requires a management information base file (MIB), you can obtain it from the Secure Firewall Management Center at `/etc/sf/DCEALERT.MIB`.

SNMP v2 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, choose **as Binary**. Otherwise, choose **as String**. For example, HP OpenView requires **as String**.
Trap Server	The server that will receive SNMP trap notifications. You can specify a single IP address or hostname.
Community String	The community name.

SNMP v3 options

Managed devices encode SNMPv3 alerts with an Engine ID value. To decode the alerts, your SNMP server requires this value, which is the hexadecimal version of the sending device's management interface IP address, appended with "01."

For example, if the device sending the SNMP alert has a management interface IP address of 172.16.1.50, the Engine ID value is 0xAC10013201.

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, choose **as Binary**. Otherwise, choose **as String**. For example, HP OpenView requires **as String**.
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. SNMP v3 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.
Private Password	The SNMP key for privacy. SNMP v3 uses the Data Encryption Standard (DES) block cipher to encrypt this password. When you enter an SNMP v3 password, the password displays in plain text during initial configuration but is saved in encrypted format. If you specify a private password, privacy is enabled, and you must also specify an authentication password.
User Name	Your SNMP user name.

Configure syslog alerting for intrusion events

Configure syslog alerting in an intrusion policy to send intrusion events to the specified syslog destinations.

After you enable syslog alerting in an intrusion policy, the system sends all intrusion events to the syslog, either on the managed device itself or to external hosts. If you specify an external host, syslog alerts are sent from the managed device.



Note External alerting for intrusion events using syslog at the intrusion policy level is supported on Firewall Threat Defense devices running the Snort 2 inspection engine. For devices with Snort 3, syslog destination is inherited from the logging settings in the access control policy.

Procedure

Step 1 Choose **Policies** > **Access Control heading** > **Intrusion**.

Step 2 Click **Snort 2 Version**, and in the intrusion policy editor's navigation pane, click **Advanced Settings**.

Step 3 Enable **Syslog Alerting**, then click **Edit** next to **Syslog Alerting**.

A message appears at the bottom of the page, identifying the intrusion policy layer that contains the configuration.

The **Syslog Alerting** page is added under **Advanced Settings**.

Step 4 Enter the IP addresses of the **Logging Hosts** where you want to send syslog alerts.

If you leave this field blank, the details of the logging hosts will be taken from logging settings in the associated access control policy.

Step 5 Choose the **Facility** and **Severity** levels as described in Facility and severity values for intrusion syslog alerts, on page 5.

Step 6 To save changes you made in this policy since the last policy commit, choose **Policy Information**, then click **Commit Changes**.

If you leave the policy editor without committing, unsaved changes are discarded when you edit a different policy.

What to do next

- Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Facility and severity values for intrusion syslog alerts

Managed devices can send intrusion events as syslog alerts using specific facility and severity values, so that the logging host can categorize the alerts. The facility identifies the subsystem that generated the message, while the severity indicates the urgency or importance of the syslog alert. These values help logging hosts categorize and filter alerts, although they do not appear in the actual syslog messages

Choose values that make sense based on your environment. Local configuration files (such as **syslog.conf** on UNIX-based logging hosts) may indicate which facilities are saved to which log files.

Syslog alert 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.
CONSOLE	An alert message.

Facility	Description
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.

Syslog alert severities

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.

Configure email alerting for intrusion events

Enabling email alerting for intrusion events allows the Secure Firewall Management Center to send email notifications when intrusion events occur, providing timely awareness of potential security threats across your network infrastructure.

Before you begin

- Configure your mail host to receive email alerts. For more information, refer to Configure a mail relay host and notification address.
- Ensure the Secure Firewall Management Center can reverse-resolve its own IP address, as some mail servers may perform reverse DNS lookups to verify the sender's identity.

Procedure

Step 1 Choose **Policies** > **Actions** > **Alerts**.

Step 2 Click **Intrusion Email**.

Step 3 Choose alerting options, including the intrusion rules or rule groups for which you want to alert, as described in Intrusion email alert options, on page 7.

Step 4 Click **Save**.

Intrusion email alert options

Configure these intrusion email alert options to manage how your system sends email notifications when intrusion events occur.

On/Off

Enable or disable intrusion email alerts.

Note When you enable this option, alerts are sent for all rules. Select individual rules to limit alerting.

From/To addresses

Specify the email sender and one or more recipients. Use commas to separate multiple recipients.

Max alerts and frequency

Set the maximum number of email alerts (**Max Alerts**) that the Secure Firewall Management Center will send per time interval (**Frequency**).

Coalesce alerts

Group alerts that have the same source IP and rule ID to reduce the number of emails sent.

Summary output

Enable brief alerts suitable for text-limited devices. Brief alerts contain:

- Timestamp
- Protocol

- Source and destination IPs and ports
- Message
- The number of intrusion events generated against the same source IP

Example: `2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

If you enable **Summary Output**, also consider enabling **Coalesce Alerts**. You may also want to lower **Max Alerts** to avoid exceeding text-message limits.

Time zone

The time zone for alert timestamps.

Email alerting on specific rules configuration

Choose rules to set email alerts for those specific events.