

Monitor Secure Firewall ASA Events

This chapter covers information on how to share events from your Secure Firewall ASA and view them in Security Cloud Control.

- About Security Analytics and Logging (SAL SaaS) for ASA devices, on page 1
- Implement secure logging analytics (SaaS) for ASA devices, on page 4
- Send ASA syslog events to the Cisco Cloud using a Security Cloud Control macro, on page 5
- Requirement: send ASA syslog events to the Cisco cloud using the command line interface, on page 8
- NetFlow secure event logging (NSEL) for ASA devices, on page 15
- Parsed ASA syslog events, on page 30

About Security Analytics and Logging (SAL SaaS) for ASA devices

Security Analytics and Logging (SaaS) allows you to capture all syslog events and Netflow Secure Event Logging (NSEL) from your ASA and view them in one place in Security Cloud Control .

The events are stored in the Cisco cloud and viewable from the Event Logging page in Security Cloud Control where you can filter and review them to gain a clear understanding of what security rules are triggering in your network. The **Logging and Troubleshooting** package gives you these capabilities.

Licensing

To configure this solution you need the following accounts and licenses:

- Security Cloud Control : You must have a Security Cloud Control tenant.
- **Secure Device Connector** : There is no separate license for a Secure Device Connector.
- **Secure Event Connector** : There is no separate license for a Secure Event Connector.
- **Secure Logging Analytics (SaaS)** : See Security Analytics and Logging licenses .
- **Adaptive Security Appliance (ASA)** : Base license or higher.

Next step

Go to Implementing Secure Logging Analytics (SaaS) for ASA Devices

A Security Analytics and Logging is a service that captures syslog events and Netflow Secure Event Logging, stores events in the Cisco cloud, and provides filtering and review capabilities.

- captures syslog events and Netflow Secure Event Logging
- stores events in the Cisco cloud, and, and
- provides filtering and review capabilities.

How ASA events are displayed in Security Cloud Control

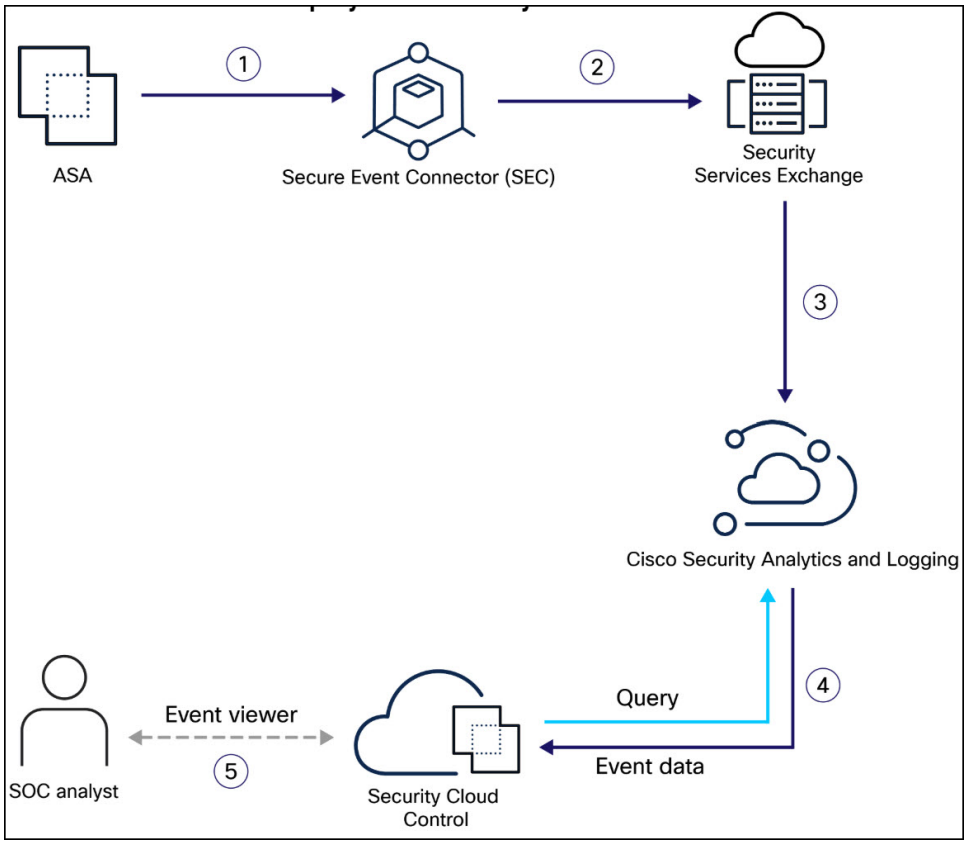
Summary

The key components involved in displaying ASA events in Security Cloud Control are:

- ASA devices: Generate and forward syslog and NSEL events when logging is enabled and network traffic matches access control rule criteria
- Secure Event Connectors: Receive events from ASA devices and forward them to Security Services Exchange
- Security Services Exchange: Aggregates event data from all devices, converts it to JSON format, and sends it for storage
- Security Analytics and Logging: Processes and enriches event data for use by Security Cloud Control
- Security Cloud Control: Stores event data and provides SOC analysts with relevant information

Workflow

Figure 1: How ASA events are displayed in security cloud control



These stages describe how ASA events are processed and displayed in Security Cloud Control:

1. You configure the ASA to forward syslog and NSEL events to any one of your Secure Event Connectors as if they were syslog servers and enable logging on the device.

   Syslog events and NSEL events are generated when logging is enabled on the ASA, and network traffic matches access control rule criteria. The ASA device forwards the syslog and NSEL events to the configured Secure Event Connector.

2. The Secure Event Connector forwards the events to Security Services Exchange.
3. Security Services Exchange aggregates the event data from all the ASA devices, converts it to JSON format, and sends it to Security Analytics and Logging for storage.
4. Security Analytics and Logging process the event data using various services to classify and enrich it for use by the Security Cloud Control.
5. Security Cloud Control stores the event data in the cloud data store. Security Cloud Control queries the stored data to provide SOC analysts with the relevant information.

Implement secure logging analytics (SaaS) for ASA devices

Implement Secure Logging Analytics (SaaS) to send ASA device events to the Cisco cloud for security analysis and monitoring.

Use this workflow to set up secure logging analytics for ASA devices, enabling cloud-based security monitoring and analysis capabilities.

Before you begin

- Review Secure Logging Analytics (SaaS) for ASA devices to learn about:
  - How events are sent to the Cisco cloud
  - Applications in the solution
  - Licenses you need
  - Data plan you need
- You have contacted your managed service provider or Security Cloud Control Sales representative to create a Security Cloud Control tenant.
- You have installed one or more SECs for your tenant and you can send events from any ASA to any SEC onboarded to your tenant.

Follow these steps to implement Cisco Security Analytics and Logging (SaaS) and send events through the Secure Event Connector to the Cisco Cloud:

Procedure

Step 1 Be sure to review "Before you Begin" above to make sure your environment is properly configured.

Step 2 Onboard ASA device to Security Cloud Control Firewall Management using username and password.

Step 3 Send ASA Syslog Events to the Cisco Cloud.

Step 4 Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.

Step 5 Confirm events are visible in Security Cloud Control.

From the navigation bar, select **Events & Logs** > **Events** > **Event Logging**. Click the **Live** tab to view live events.

You have successfully implemented Secure Logging Analytics (SaaS) for your ASA devices. Events are now being sent to the Cisco cloud for analysis and monitoring. If you have the appropriate licenses, you can also access Secure Cloud Analytics for advanced security monitoring and alerting capabilities.

What to do next

For troubleshooting and monitoring:

- Troubleshooting Secure Event Connector Onboarding Failures

- Event Logging Troubleshooting Log Files
- Use Health Check to Learn the State of your Secure Event Connector
- Troubleshooting Using Security and Analytics Logging Events

Send ASA syslog events to the Cisco Cloud using a Security Cloud Control macro

A Security Cloud Control macro is a configuration tool that

- allows you to assemble a list of CLI commands and turn elements of the command syntax into parameters
- can be saved and used more than once, and
- can be run on multiple devices at the same time to configure all your ASAs to send events to the Cisco cloud.

Macro benefits

Using proven macros promotes configuration consistencies between devices and prevents syntax errors that can occur when using the command line interface.

You can configure all your ASAs to send events to the Cisco cloud by creating a Security Cloud Control macro that uses all the commands described in Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface and running that macro on all your ASA in the same batch.

Before you read further, review macros in Security Cloud Control configuration guide so that you understand the mechanics of using macros. This article will only describe assembling the final macro.

Create an ASA security analytics and logging (SaaS) macro

This task helps you create a reusable macro that automates the configuration of ASA logging to send syslog events to a Secure Event Connector (SEC) in the Cisco cloud. The macro allows you to define parameters that can be customized each time you run it, making it easy to deploy consistent logging configurations across multiple ASA devices.

There are two types of formatting you'll see in the following procedure, ASA CLI commands and macro formatting. The ASA CLI commands are written to follow ASA syntax conventions. See Use command line interface for more information about using the CLI in Security Cloud Control.

Before you begin, open Send ASA Syslog Events to the Cisco Cloud in a separate window and read it in parallel with this procedure so you can read the command descriptions as you create your macros.

Before you begin

Note If a logging config is already in place on the ASA, running the macro from Security Cloud Control will *not* first clear out all of the existing logging config. Rather, the settings defined in the Security Cloud Control macro will merge into whatever might already be in place.

Procedure

Step 1 Open a plain text editor and create a list of commands you are going to turn into a macro, based on the instructions and options below. Security Cloud Control will execute the commands in the order they are written in the macro. Some command will have values that you turn into {{parameters}} that you will fill in when it comes time to run the macro.

Step 2 **Configure the** ASA **to send messages to an SEC as if it were a syslog server.**

Use the **logging host** command to specify the SEC as the syslog server you send messages to. You can send events to any one of the SECs you have onboarded to your tenant.

The **logging host** command specifies a TCP or UDP port to send events to. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging to determine what ports you should use.

logging host*interface_nameSEC_IP_address* { **TCP/port** | **UDP/port** }

Turn this command into one of two different macros depending on what protocol you use to send syslog events to the SEC:

logging host {{interface_name}} {{SEC_ip_address}} TCP/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} UDP/{{port)_number}}

(Optional) If you use TCP, you can add this command to your list of commands in your macro. It does not need any parameters.

logging permit-hostdown

Step 3 **Specify which syslog messages should be sent to the syslog server.**

Use the **logging trap** command to specify which syslog messages should be sent to the syslog server:

logging trap { *severity_level* | *message_list* }

If you want to define the events sent to the SEC by severity level, turn the command into this macro:

logging trap {{severity_level}}

If you only want to send events to the SEC that are part of a message list, turn the command into this macro:

logging trap {{message_list_name}}

If you chose the **logging trap message_list** command in the previous step, you need to define the syslogs in your message list. Open Create a Custom Event List so you can read the command descriptions as you create the macro. Start with this command:

logging list*name* { **level***level* [**class***message_class*] | **message***start_id* [*-end_id*] }

And break it down into these variations:

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

In the last variation, the message parameter {{syslog_range_or_number}} could be entered as a single syslog ID, 106023, or a range, 302013-302018. Use one or more of the command variations in as many lines as you

like to create your message list. Keep in mind that, in a single macro, all parameters with the same name will use the same value you enter. Security Cloud Control will not run a macro with empty parameters.

Important
The **logging list** command has to come before the **logging trap** command in your macro. You define the list first and then the **logging trap** command can use it. See the sample macro below.

Step 4 **(Optional) Add the syslog timestamp.** Add this command if you want to add the date and time to the message that the syslog message originated on the ASA. The timestamp value is displayed in the **SyslogTimestamp** field. Add this command to your list of commands, it will not need any parameters:

logging timestamp

Note
Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. This is a sample output with RFC 5424 format:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
 from src interface :src IP/src port to dest IP/dest port
```

Step 5 **(Optional) Include a device ID in non-EMBLEM format syslog messages.** Open Include the Device ID in Non-EMBLEM Format Syslog Messages so you can read the command descriptions as you create the macro. This is the CLI command you will base your macro on:

logging device-ID {**cluster-ID** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text*}

And break it down into these variations:

logging device-ID cluster-ID

logging device-ID context-name

logging device-ID hostname

logging device-ID ipaddress {{interface_name}} **system**

logging device-ID string {{text_16_char_or_less}}

Step 6 **Enable logging**. Add this command to your macro as it is. It does not have any parameters:

logging enable

Step 7 **Do not add write memory** to the last line of the macro. Add the **show running-config logging** command instead to review the results of the logging commands you entered before committing them to the ASA's startup config.

show running-config logging

Step 8 After you are confident your configuration changes were made, you can create a separate macro for the **write memory** command or use Security Cloud Control's Bulk Command Line Interface tool to issue the command to all the devices you configured using your macro.

write memory

Step 9 **(Optional) Enable logging on access control rule "permit" events.** This step in the described in the Send ASA Syslog Events to the Cisco Cloud procedure but it is not included in this macro. It is performed in the Security Cloud Control GUI instead.

Step 10 Save the macro.

You have successfully created an ASA Security Analytics and Logging macro that can be run to configure multiple ASA devices with consistent logging settings. The macro includes commands for specifying the SEC as a syslog server, defining which messages to send, and enabling logging functionality.

Here is a sample of a list of commands combined into a single macro:

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

Note There are several logging list commands to add different specific syslog IDs or ranges. The {{syslog_range_or_number_X}} parameter requires a number or some other differentiator, otherwise their values will all be the same when the macro is filled in. Also keep in mind that Security Cloud Control will not run a macro if not all the parameters are given a value, so only include the commands in the macro you want to execute. We do want all the syslog IDs contained in the same list so event_list_name stays the same for in each line.

Run the Macro

After you have created and saved the ASA Security Analytics and Logging Macro, run the macro to send ASA syslog events to the Cisco cloud.

Requirement: send ASA syslog events to the Cisco cloud using the command line interface

Limitations on supported ASA commands

This procedure explains how to forward ASA syslog events to a Secure Event Connector (SEC) and then enable logging. These procedures explain only what is needed to complete that workflow. For a broader discussion of all the ways you can configure logging on the ASA, see the Monitoring chapter of either ASDM1: Cisco ASA Series General Operations ASDM Configuration Guide or CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide.

- Security Cloud Control does not yet support EMBLEM format for syslogs.
- Security Cloud Control does not yet support Secure Syslogs.

Security Cloud Control Command Line Interface for ASA

Access the command line interface to configure ASA devices directly through Security Cloud Control.

For all the tasks in this procedure, you will be working on the Security Cloud Control's command line interface for ASA.

Procedure

Step 1 From the left navigation bar, click **InventorySecurity Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the ASA for which you want to enable logging.

Step 4 In the Device Actions pane on the right, click **>_ Command Line Interface**.

Step 5 Click the **Command Line Interface** tab.

After entering every command, you will click **Send**. Because Security Cloud Control's CLI Interface is a direct connection to the ASA, the command is written to the device's running configuration immediately. For changes to be written to the ASA's startup configuration, you need to issue the `write memory` command in addition.

You are now ready to enter commands at the command line interface prompt.

Forward ASA syslog events to the secure event connector

This task enables ASA syslog event forwarding to Secure Event Connectors for centralized logging and monitoring.

To forward ASA syslog events to one of the Secure Event Connectors (SECs) you have onboarded and then enable logging, you need complete these tasks in the procedure that follows.

Procedure

Step 1 Configure the ASA to send messages to the SEC as if it were a syslog server.

Step 2 Decide what severity level of all logs, or what list of syslog events, you want to send to the SEC.

Step 3 Enable logging.

Step 4 Save the changes to the ASA's startup config.

ASA syslog events are now forwarded to the configured Secure Event Connector with logging enabled and changes saved to startup configuration.

Send ASA syslog events to the Cisco cloud using CLI

This task configures the ASA to forward syslog events to the Cisco cloud for security analytics and logging purposes through the Secure Event Connector.

When sending syslog events from the ASA to the Cisco cloud, you forward them to the SEC as if it were an external syslog server, and it forwards the messages to the Cisco cloud.

Procedure

Step 1 Configure the ASA to send messages to the SEC as if it were a syslog server

To send syslog messages to the SEC, perform the following steps:

a. Configure the ASA to send messages, using TCP or UDP, to the SEC as if it were a syslog server. The SEC can use an IPv4 or IPv6 addresss. You will be sending events to either a TCP or UDP port. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging to determine what ports you should use.

Here is an example of the **logging host** command syntax:

logging host *interface_name SEC_IP_address* [[**TCP/port**] | [**UDP/port**]]

Examples:

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- The **interface_name** argument specifies the ASA interface from which messages are sent to the syslog server. It is a "best practice" to send the syslog messages to the SDC over the same ASA interface already in use for communication with the SDC.
- The **SEC_IP_address** argument should contain the IP address of the VM on which the SEC is installed.
- The **TCP/port** or **UDP/port** keyword-argument pair specifies that syslog messages should be sent using either TCP protocol and relevant port, or the UDP protocol and relevant port. You can configure the ASA to send data to a syslog server using either UDP or TCP, but not both. The default protocol is UDP if you do not specify a protocol.

  If you specify TCP, the ASA will discover syslog server failures and as a security protection, new connections through the ASA are blocked. To allow new connections regardless of connectivity to a TCP syslog server, see step b. If you specify UDP, the ASA continues to allow new connections whether or not the syslog server is operational. Valid port values

  Note
  If you want to send ASA messages to two separate syslog servers, you can run a second logging host command with the appropriate interface, IP address, protocol and port of the other syslog server.

b. (Optional) If you send events to the SEC over TCP, and if either the SEC is down or the log queue on the ASA is full, then new connections are blocked. New connections are allowed again after the syslog server is back up and the log queue is no longer full. To allow new connections regardless of connectivity to a TCP syslog server, disable the feature to block new connections when a TCP-connected syslog server is down using this command:

logging permit-hostdown

Example:

```
 > logging permit-hostdown
```

Step 2 Specify which syslog messages should be sent to the syslog server with the following command:

logging trap { severity_level | message_list }

Examples:

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

You can specify the severity level number (1 through 7) or name. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

The message_list argument is replaced with the name of a custom event list, if you have created one. When specifying a custom event list, you only send the syslog messages that are in that list to the Secure Event Connector. In the example above, asa_syslogs_to_cloud is the name of the event list.

Using a message_list could save you money by tightly defining which syslog messages are sent to the Cisco cloud.

See Create a Custom Event List to create a message_list. See Security Analytics and Logging licenses for more information about data ingest and storage costs.

Step 3 (Optional) Add the syslog timestamp

Add the date and time that the syslog message originated on the ASA to the message using the logging timestamp command. The timestamp value is displayed in the **SyslogTimestamp** field.

Example:

```
> logging timestamp
```

Note
Beginning with version 9.10(1), ASA provides the option to enable timestamp as per RFC 5424 in eventing syslogs. When this option is enabled, all timestamp of syslog messages would be displaying the time as per RFC 5424 format. Following is a sample output with RFC 5424 format:

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
 from src interface :src IP/src port to dest IP/dest port.
```

Step 4 (Optional) Include a device ID in non-EMBLEM format syslog messages

A device ID is an identifier you can insert in a syslog message that will help you easily distinguish all syslog messages sent from a particular ASA. See Include the Device ID in Non-EMBLEM Format Syslog Messages for instructions.

Step 5 (Optional) Enable logging on access control rule "permit" events

When an access control rule denies access to a resource, the event is automatically logged. If you also want to log events generated when an access control rule allows access to a resource, you need to turn on logging for the access control rule and configure a severity type.

See Log Rule Activity for instructions on how to turn on logging for an individual network access control rule.

Note
Enabling logging on access control rule "permit" events will use-up more of your purchased data plan as it is based on your daily ingest rate of events.

Step 6 Enable logging

At the command prompt, type logging enable. On the ASA, logging is enabled for the entire device, not for individual rules.

Example:

```
> logging enable
```

Note
At this time, Security Cloud Control does not support enabling secure logging.

Step 7 Save your Changes to the Startup Config

At the command prompt, type write memory. On the ASA, logging is enabled for the entire device, not for individual rules.

Example:

```
> write memory
```

The ASA is now configured to send syslog events to the Cisco cloud through the Secure Event Connector. Logging is enabled and messages will be forwarded according to your specified configuration.

Create a custom event list

Create a custom event list to filter and send specific ASA syslog events to logging destinations such as syslog servers or Secure Event Connectors in the Cisco Cloud.

Create a custom event list when you are sending ASA syslog events to the Cisco Cloud using one of these methods:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Send ASA Syslog Events to the Cisco Cloud using a Security Cloud Control Macro

You can create an event list, also referred to as a message_list, based on these three criteria:

- Event Class
- Severity
- Message ID

Before you begin

Follow these steps to create a custom event list to send to a specific logging destination:

Procedure

Step 1 From the left navigation bar, click **InventorySecurity Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate tab and select the ASA whose syslog messages you want to include in a custom event list.

Step 4 In the **Device Actions** pane, click **>_ Command Line Interface.**

Step 5 Use this command syntax to issue the **logging list** command to the ASA:

logging list *name* { **level** *level* [**class** *message_class*] | **message** *start_id* [*-end_id*] }

The *name* argument specifies the name of the list. The **level** *level* keyword and argument pair specify the severity level. The **class** *message_class* keyword-argument pair specify a particular message class. The **message** *start_id* [*-end_id*] keyword-argument pair specify an individual syslog message number or a range of numbers.

Note
Do not use the names of severity levels as the name of a syslog message list. Prohibited names include emergencies, alert, critical, error, warning, notification, informational, and debugging. Similarly, do not use the first three characters of these words at the beginning of an event list name. For example, do not use an event list name that starts with the characters "err."

- **Add syslog messages to the event list based on severity**. For example, if you set the severity level to 3, then the ASA sends syslog messages for severity levels 3, 2, and 1.

  Example:

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- **Add syslog messages based on other criteria to the event list**:

  Enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion that you want to add to the list. For example, you can specify criteria for syslog messages to be included in the list as follows:

  - Syslog message IDs that fall into the range of 302013-302018.
  - All syslog messages with the critical severity level or higher (emergency, alert, or critical).
  - All HA class syslog messages with the warning severity level or higher (emergency, alert, critical, error, or warning).

    Example:

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    Note
    A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

Step 6 **Save your Changes to the Startup Config**

At the command prompt, type **write memory**.

Example:

```
> write memory
```

The custom event list is created and saved to the ASA startup configuration. The ASA will now filter and send syslog messages to the Cisco Cloud based on your specified criteria.

Include the device ID in Non-EMBLEM format syslog messages

Configure the ASA to include a device identifier in non-EMBLEM-format syslog messages to ensure proper identification and tracking in the Event Logging page's SensorID field.

You can configure the ASA to include a device ID in non-EMBLEM-format syslog messages. You can specify only one type of device ID for syslog messages. This procedure is referred to by these procedures:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Send ASA Syslog Events to the Cisco Cloud using a Security Cloud Control Macro

This device identifier will be reflected in the SensorID field of a syslog event displayed on the Event Logging page.

Procedure

Step 1 Select the ASA whose syslog messages you want to assign a device-ID to.

Step 2 In the Device Actions pane, click **>_ Command Line Interface.**

Step 3 Use this command syntax to issue the **logging device-ID** commands to the device.

logging device-ID { **cluster-ID** | **context-name** | **hostname** | **ipaddress***interface_name* [**system**] | **string***text* }

Example:

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

Note
In an ASA cluster, always use the primary unit IP address for the selected interface.

The **cluster-ID** keyword specifies the unique name in the boot configuration of an individual ASA unit in the cluster as the device ID.

The **hostname** keyword specifies that the hostname of the ASA should be used as the device ID.

The **ipaddress** *interface_name* keyword-argument pair specifies that the interface IP address specified as *interface_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified ASA interface IP address, regardless of the interface from which the syslog message is sent. In the cluster environment, the **system** keyword dictates that the device ID becomes the system IP address on the interface. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device.

The **string** *text* keyword-argument pair specifies that the text string should be used as the device ID. The string can include as many as 16 characters.

You cannot use blank spaces or any of the following characters:

- & (ampersand)

- ' (single quote)
- " (double quote)
- < (less than)
- > (greater than)
- ? (question mark)

Step 4 **Save your Changes to the Startup Config**

At the command prompt, type **write memory**.

Example:

```
> write memory
```

The ASA is now configured to include the specified device ID in non-EMBLEM-format syslog messages, which will appear in the SensorID field on the Event Logging page.

NetFlow secure event logging (NSEL) for ASA devices

NetFlow Secure Event Logging (NSEL) is a stateful IP flow tracking method that

- provides Security Analytics and Logging with granular data that basic syslog messages from the ASA lack
- exports only those records that indicate significant events in a flow, and
- supports NetFlow Version 9 services on Cisco ASA devices.

Flow characteristics and implementation details

A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flows are highly granular; for example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, etc.[1]

The Cisco ASA supports NetFlow Version 9 services. The ASA implementation of NSEL provides a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes.

This documentation describes a straight forward approach to configuring NetFlow for your ASAs using a Security Cloud Control macro. The Cisco ASA NetFlow Implementation Guide provides an extremely detailed discussion of configuring NetFlow on the ASA and you may find it a valuable resource to accompany this content.

What to do Next

Go to Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.

Related Articles

- Configuring NSEL for ASA Devices Using a Security Cloud Control Macro

- Delete NetFlow Secure Event Logging (NSEL) Configuration from an ASA
- Determine the Name of an ASA Global Policy

1. ("Cisco Systems NetFlow Services Export Version 9." Internet Engineering Task Force, Network Working Group, Request for Comments: 3954, October 2004, B. Claise, Ed. https://www.ietf.org/rfc/rfc3954.txt)

Configuring NSEL for ASA devices by using a CDO macro

ASAs report detailed connection event data using Netflow Secure Event Logging (NSEL). You can apply Secure Cloud Analytics to this connection event data, which includes bidirectional flow statistics. This procedure describes how to configure NSEL on an ASA device and send those NSEL events to a flow collector. In this case, the flow collector is a Secure Event Connector (SEC).

Summary

The key components involved in configuring NSEL for ASA devices are:

- **ASA device**: Reports detailed connection event data using NSEL
- **Secure Event Connector (SEC)**: Acts as the flow collector that receives NSEL events
- **CDO macro**: Automates the configuration process for NSEL settings
- **Flow-export destination**: Defines where NSEL events are sent
- **Class-map**: Defines which NSEL events will be sent to the SEC
- **Policy-map**: Applies the flow-export configuration to specific traffic classes

Workflow

These are the stages of configuring NSEL for ASA devices by using a Security Cloud Control macro:

1. Before beginning the configuration process, gather the required information including the IPv4 address of the SEC, the ASA interface, the UDP port number, and the global policy name.
   - IPv4 address of the SEC that will receive data from the ASA
   - Interface on the ASA that will send data to the SEC
   - UDP port number used to forward NetFlow events. See Finding your device's TCP, UDP, and NSEL port used for secure logging analytics (SaaS).
   - Determine the name of an ASA global policy, on page 24
2. Execute the configuration workflow by following each step in sequence to properly configure NSEL using the CDO macro.
   - Open the configuring NSEL macro, on page 17.
   - Define the destination of NSEL messages and the interval at which they are sent to the SEC, on page 18.
   - Create a Class-Map that defines which NSEL events will be sent to the SEC, on page 19.
   - Define a Policy-Map for NSEL events, on page 20.

- Recommendation: disable redundant syslog messages when using NetFlow, on page 21.
- Review and send the macro, on page 22.

This procedure refers to this macro, **Configure NSEL**:

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

Here is an example of the Configure NSEL macro with all the default values filled in, a generic name for the class-map, and the class map added to the global_policy, When you are done with these procedures, your macro will resemble this:

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

Open the configuring NSEL macro

This task allows you to access the Configuring NSEL macro to configure NetFlow Secure Event Logging on ASA devices.

This is the first part in a longer workflow for configuring NSEL on ASA devices using CDO macros.

Before you begin

This is first part in a longer workflow, see Configuring NSEL for ASA devices by using a CDO macro, on page 16 before getting started.

Follow these steps to open the Configuring NSEL macro:

Procedure

Step 1 On the **InventorySecurity Devices** page, click the **Devices** tab.

Step 2 Click the appropriate device type tab and select the ASA(s) on which you want to configure NetFlow Secure Event Logging (NSEL).

Step 3 In the **Device Actions** pane, click **Command Line Interface**.

Step 4 Click the Macro star  to show the list of available macros.

Step 5 From the list of macros, select **Configuring NSEL**.

Step 6 Under the Macro box, click **View Parameters**.

Continue to Define the destination of NSEL messages and the interval at which they are sent to the SEC, on page 18.

The Configuring NSEL macro parameters are displayed, allowing you to proceed with configuring NSEL settings for the selected ASA devices.

Define the destination of NSEL messages and the interval at which they are sent to the SEC

This task configures the destination SEC collector and timing intervals for NSEL message transmission from ASA devices.

NSEL messages can be sent to any one of the SECs you have onboarded to your tenant. These instructions refer to this section of the macro:

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA devices by using a CDO macro, on page 16 before getting started.

Procedure

Step 1 The **flow-export destination** command defines the collector to which the NetFlow packets are sent. In this case, you are sending them to an SEC. Fill in the fields for these parameters:

- **{{interface}}**-Enter the name of the interface on the ASA from which the NetFlow events are sent.
- **{{SEC_IPv4_address}}**-Enter the IPv4 address of the SEC. The SEC functions as the flow collector.
- **{{SEC_NetFlow_port}}**-Enter the UDP port number on the SEC to which NetFlow packets are sent.

Step 2 The **flow-export template timeout-rate** command specifies the interval at which template records are sent to all configured output destinations.

- **{{timeout_rate_in_mins}}**-Enter the number of minutes before templates are resent. **We recommend using a value of 60 minutes**. The SEC does not process the templates. A large number reduces traffic to the SEC.

Step 3 The **flow-export delay flow-create** command delays the sending of flow-create events by the specified number of seconds. This value matches the recommended Active Timeout value and reduces the number of flow

events exported from the ASA. At that rate, expect NSEL events to first appear in Security Cloud Control at the close of a connection or within 55 seconds of the creation of the connection, whichever happens earlier. If this command is not configured, there is no delay, and the flow-create event is exported as soon as the flow is created.

- **{{delay_flow_create_rate_in_secs}}**-Enter the number of seconds delay between sending flow-create events. **We recommend using a value of 55 seconds**.

Step 4 The **flow-export active refresh-interval** command defines the frequency that status updates for long-lived flows will be sent from ASA. Valid values are from 1-60 minutes. In the Flow Update Interval field, configuring the **flow-export active refresh-interval** to be at least 5 seconds more than the **flow-export delay flow-create** interval prevents flow-update events from appearing before flow-creation events.

- **{{refresh_interval_in_mins}}-We recommend using a value of 1 minute**. Valid values are from 1-60 minutes.

Continue to Create a Class-Map that defines which NSEL events will be sent to the SEC, on page 19

The NSEL message destination and timing parameters are configured for transmission to the specified SEC collector.

Create a Class-Map that defines which NSEL events will be sent to the SEC

Create a class-map that identifies NSEL traffic for export to the SEC and define the matching criteria for traffic classification.

The following commands in the macro group all NSEL events in a class and then export that class to the Secure Event Connector (SEC). These instructions refer to this section of the macro:

class-map {{flow_export_class_name}}

match {{add_this_traffic_to_class_map}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA devices by using a CDO macro, on page 16 before getting started.

Procedure

Step 1 The **class-map** command names the class map that identifies NSEL traffic that will be exported to the SEC.

- **{{flow-export-class-name}}**-Enter a name for your class map. The name may be up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot re-use a name already used by another type of class map.

Step 2 Identify the traffic that is going to be associated with (matched with) your class-map. Choose one of these options for the value of **{{add_this_traffic_to_class_map}}:**

- Enter **any** in the **{{add_this_traffic_to_class_map}}** field. This monitors all traffic types for NSEL traffic. **We recommend using the value "any".**

- Enter **access-list *name-of-access-list*** in the **{{add_this_traffic_to_class_map}}** field. This associates all the traffic associated with an access-list that you have created. See Configure Flow-Export Actions Through Modular Policy Framework in the Cisco ASA NetFlow Implementation Guide for more information.

Continue to Define a Policy-Map for NSEL events, on page 20.

You have created a class-map that defines which NSEL events will be sent to the SEC and specified the traffic matching criteria.

Define a Policy-Map for NSEL events

Create a policy-map that assigns NetFlow export actions to the class and associates the class with a new policy map for managing NSEL events.

This task assigns NetFlow export actions to the class you created in the previous task, and the class to a new policy map. These instructions refer to this section of the macro:

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA devices by using a CDO macro, on page 16 before getting started.

Procedure

Step 1 The **policy-map** command creates a policy-map. In the next task, you associate this policy map with the global policy.

- **{{global_policy_map_name}}**-Enter a name for the policy map. **We recommend using the name of the firewall's existing global policy if there is one**. The default name for the global policy is **global_policy**. See Determine the Name of an ASA Global Policy. If you create a new policy map and apply it globally according to Configure Flow-Export Actions Through Modular Policy Framework in Cisco ASA NetFlow Implementation Guide, the remaining inspection policies are deactivated.

Step 2 The **class** command inherits the name of the class-map you created in Create a Class-Map that defines which NSEL events will be sent to the SEC, on page 19.

Step 3 The **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} command defines which event types should be sent to flow collector, (in this case the SEC).

- **{{event-type}}**-The event_type keyword is the name of the supported event being filtered. **We recommend using the value "all"**.
- **{{SEC_IPv4_address}}**-This is the IPv4 address of the SEC. Its value is inherited from the value you entered in Define the destination of NSEL messages and the interval at which they are sent to the SEC, on page 18.

Continue to Recommendation: disable redundant syslog messages when using NetFlow, on page 21.

The policy-map is created with NetFlow export actions assigned to the specified class for managing NSEL events.

Recommendation: disable redundant syslog messages when using NetFlow

When NetFlow is enabled to export flow information, disable redundant syslog messages for improved performance. The same information is exported through NetFlow, making these syslog messages unnecessary.

Enabling NetFlow to export flow information makes certain syslog messages redundant because the same information is exported through NetFlow. Disabling these messages improves performance.

The macro includes the command **logging flow-export-syslogs disable** to disable redundant syslog messages. You do not need to modify this command.

If you do not want to disable redundant syslog messages, you can edit this macro and delete only this line from it:

logging flow-export-syslogs disable

You can later enable or disable individual syslog messages by following the procedure in the Disabling and Reenabling NetFlow-related Syslog Messages.

Note When NSEL and syslog messages are both enabled, there is no guarantee of chronological ordering between the two logging types.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
106100	Generated whenever an access control rule (ACL) is encountered.	1-Flow was created (if the ACL allowed the flow). 3-Flow was denied (if the ACL denied the flow).	0-If the ACL allowed the flow. 1001-Flow was denied by the ingress ACL. 1002-Flow was denied by the egress ACL.
106015	A TCP flow was denied because the first packet was not a SYN packet.	3-Flow was denied.	1004-Flow was denied because the first packet was not a TCP SYN packet.
106023	When a flow was denied by an ACL attached to an interface through the **access-group** command.	3-Flow was denied.	1001-Flow was denied by the ingress ACL. 1002-Flow was denied by the egress ACL.
302013, 302015, 302017, 302020	TCP, UDP, GRE, and ICMP connection creation.	1-Flow was created.	0-Ignore.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
302014, 302016, 302018, 302021	TCP, UDP, GRE, and ICMP connection teardown.	2-Flow was deleted.	0-Ignore. > 2000-Flow was torn down.
313001	An ICMP packet to the device was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.
313008	An ICMP v6 packet to the device was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.
710003	An attempt to connect to the device interface was denied.	3-Flow was denied.	1003-To-the-box flow was denied because of configuration.

Review and send the macro

Review and send macro commands to the ASA device to complete the NSEL configuration workflow.

This task is performed after filling in the macro fields as part of configuring NSEL for ASA devices using a CDO macro.

Before you begin

This is part of a larger workflow. See Configuring NSEL for ASA devices by using a CDO macro, on page 16, before getting started.

Follow these steps to review and send the macro:

Procedure

Step 1 After filling in the fields of the macro, click **Review** to review the commands before they are sent to the ASA.

Step 2 If you are satisfied with your responses to the commands, click **Send**.

Step 3 After you send the command, you may see the message, "Some commands may have made changes to the running config" along with two links.



- Clicking **Write to Disk** saves the changes made by this command, and any other changes in the running-configuration, to the device's startup configuration.
- Clicking **Dismiss** dismisses the message.

You have finished the workflow described in Configuring NSEL for ASA devices by using a CDO macro, on page 16.

DELETE NetFlow secure event logging (NSEL) configuration from an ASA

This task removes the NetFlow Secure Event Logging (NSEL) configuration from an ASA device, which reverses the configuration that specifies the Secure Event Connector (SEC) as the NSEL flow collector.

This procedure reverses the macro described in Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.

Procedure

Use the **DELETE NSEL** macro to remove the NetFlow configuration.

Example:

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

The NetFlow Secure Event Logging (NSEL) configuration is removed from the ASA device.

Open the DELETE-NSEL macro

This task enables you to access and prepare the DELETE-NSEL macro for removing NetFlow Secure Event Logging (NSEL) configuration from ASA devices.

Use this task when you need to DELETE the NetFlow Secure Event Logging configuration from one or more ASA devices using the command line interface and macro functionality.

Procedure

Step 1 On the **InventorySecurity Devices** page, click the **Devices** tab.

Step 2 Click the appropriate device type tab and select the ASA(s) on which you want to DELETE the configuration of NetFlow Secure Event Logging (NSEL).

Step 3 In the **Device Actions** pane, click **Command Line Interface**.

Step 4 Click the Macros star  to show the list of available macros.

Step 5 In the list of macros, select **DELETE-NSEL**.

Step 6 Under the Macro box, click **View Parameters**.

The DELETE-NSEL macro is now open and ready for parameter configuration before execution.

Enter the values in the macro to complete the no commands

Remove NetFlow policy-map configurations by completing the "no" form of commands with appropriate macro values.

The ASA CLI uses the "no" form of a command to delete it. Fill in the fields in the macro to complete the "no" form of the command:

Procedure

Step 1 policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}**-Enter the value of the policy-map name.

Step 2 no class {{flow_export_class_name}}

- **{{flow_export_class_name}}**-Enter the value of the class-map name.

Step 3 no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}**-The value of the class-map name is inherited from the step above.

Step 4 no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}**-Enter the name of the interface on the ASA from which the NetFlow events were sent.
- **{{IPv4_address}}**-Enter the IPv4 address of the SEC. The SEC functions as the flow collector.
- **{{NetFlow_port}}**-Enter the UDP port number on the SEC to which NetFlow packets were sent.

Step 5 no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}**-Enter the flow-export template timeout-rate.

Step 6 no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}**-Enter the flow-export delay flow-create rate.

Step 7 no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}**-Enter the flow-export active refresh-interval interval.

The NetFlow policy-map configuration is removed from the ASA device after completing all the "no" commands with the appropriate macro values.

Determine the name of an ASA global policy

This task enables you to identify the specific name assigned to an ASA's global policy configuration.

You may need to determine the name of an ASA's global policy when troubleshooting or configuring security policies on your device.

Before you begin

Follow these steps to determine the name of an ASA global policy:

Procedure

Step 1 From the **InventorySecurity Devices** page, select the device for which you want to find the name of the global policy.

Step 2 In the Device Actions pane, select **>_Command Reference**.

Step 3 In the Command Line Interface window, at the prompt, type:

show running-config service-policy

In the output of the example below, global_policy is the name of the global policy.

Example:

>**show running-config service-policy**

service-policy global_policy global

The command output displays the global policy name in the service-policy configuration line.

Troubleshooting NSEL data flows

Troubleshooting NSEL data flows is a verification process that

- verifies that NSEL events are being sent from your ASA to the Cisco Cloud
- confirms that the Cisco Cloud is receiving NSEL events, and
- uses flow-export counters and capture commands to diagnose data flow issues.

NSEL data flow verification requirements

Once you have configured Netflow Secure Event Logging (NSEL), data does not flow immediately. It could take a few minutes for the first NSEL packets to arrive assuming there is NSEL-related traffic being generated on the ASA.

This verification process involves these tasks:

- Verify that NetFlow Packets are Being Sent to the SEC
- Verify that NetFlow Packets are Being Received by the Cisco Cloud

Note This workflow shows you a straight-forward use of the "flow-export counters" command and "capture" commands to Troubleshoot NSEL Data Flows. See "Packet Captures" CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide and "Monitoring NSEL" in the Cisco ASA NetFlow Implementation Guide for a more detailed discussion of the usage of these commands.

Verify that NSEL events are being sent to the SEC

This task verifies that NSEL events are successfully being transmitted from ASA devices to the SEC for security event monitoring.

Use one of two commands to verify that NSEL packets are being sent to the SEC:

- flow-export counters
- capture

Use the "flow-export counters" Command to Check for flow-export Packets Being Sent and for NSEL errors

- Make sure you have configured your ASA to send NSEL events to the SEC. See Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.
- The SEC IP address is the flow collector address for NSEL events. If you have onboarded more than one SEC to your tenant, be sure you are using the correct IP address.
- Find the UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging.
- Our recommended interface on the ASA from which to send NSEL events is the management interface; your interface may be different.

Use the command line interface in Security Cloud Control to send these commands to the ASAs that you have configured for NSEL.

Procedure

Step 1 In the navigation pane, click **InventorySecurity Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device tab and select the ASA you configured to send NSEL events to the SEC.

Step 4 In the **Device Actions** pane on the right, click **Command Line Interface**.

Step 5 Reset the flow export counters by running the **clear flow-export counters** command. This resets the clear export flow counters to zero so that you can easily tell if new events are coming in.

example:

>**clear flow-export counters**

Done!

Step 6 Run the show flow-export counters command to see the destination of the NSEL packets, how many packets were sent and any errors:

example:

>show flow-export counters

destination: management 209.165.200.225 10425

Statistics:

packets sent 25000

Errors:

block allocation errors 0

invalid interface 0

template send failure 0

no route to collector 0

source port allocation 0

In the output above, the destination line shows the interface on the ASA from which NSEL events are sent, the IP address of the SEC, port 10425 of the SEC. It also shows packets sent of 25000.

Error descriptions:

- **block allocation errors**-If you receive a block allocation error, the ASA did not allocate memory to the flow-exporter.
  - Recovery action: Call Cisco Technical Assistance Center (TAC).
- **invalid interface**-Indicates that you are trying to send NSEL events to the SEC but the interface you've defined for flow export isn't configured to do so.
  - Recovery action: Review the interface you chose when configuring NSEL. We recommend using the management interface, your interface may be different.
- **template send failure**-The template you had to define NSEL was not parsed correctly.
  - Recovery action: Contact Security Cloud Control support.
- **no route to collector**-Indicates there is no network route from the ASA to the SEC.
  - Recovery actions:
    - Make sure that the IP address you used for the SEC when you configured NSEL is correct.
    - Make sure the SEC's status is Active and it has sent a recent heartbeat. See SDC is Unreachable.
    - Make sure the Secure Device Connector's status is Active and it has sent a recent heartbeat.
- **source port allocation**-May indicate that there is a bad port on your ASA.

Use the "capture" command to capture NSEL packets sent from the ASA to the SEC

This task captures NSEL packets to verify that your ASA is successfully sending NSEL events to the SEC.

Use the command line interface in Security Cloud Control to send these commands to the ASAs that you have configured for NSEL.

Before you begin

- Make sure you have configured your ASA to send NSEL events to the SEC. See Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.

- The SEC IP address is the flow collector address for NSEL events. If you have onboarded more than one SEC to your tenant be sure you are using the correct IP address.
- Find the UDP port number used to forward NetFlow events. See Finding Your Device's TCP, UDP, and NSEL Port Used for Cisco Security Analytics and Logging.
- Our recommended interface on the ASA from which to send NSEL events is the management interface; your interface may be different.

Follow these steps to capture NSEL packets sent from the ASA to the SEC:

Procedure

Step 1 In the navigation pane, click **InventorySecurity Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab and select the ASA you configured to send NSEL events to the SEC.

Step 4 In the **Device Actions** pane on the right, click **Command Line Interface**.

Step 5 In the command window, run this **capture** command:

>**capture***capture_name***interface***interface_name* **match UDP any host** *IP_of_SEC***eq***NetFlow_port*

Where

- *capture_name* is the name of the packet capture.
- *interface_name* is the name of the interface from which NSEL packets leave the ASA.
- *IP_of_SEC* is the IP address of the SEC VM.
- *NetFlow_port* is the port to which NSEL events are sent.

This starts the packet capture.

Step 6 Run the **show capture** command to view the captured packets:

> show capture*capture_name*

Where *capture_name* is the name of the packet capture you defined in the previous step.

Here is an example of the output showing the time of the capture, the IP address from which the packet was sent, the IP address, and the port the packet was sent to. In this example, 192.168.25.4 is the IP address of the SEC and port 10425 is the port on the SEC that receives NSEL events.

6 packets captured

```
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: UDP 476

2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: UDP 248

3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: UDP 1436

4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: UDP 1276

5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: UDP 112

6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: UDP 196
```

Step 7 Run the **capture stop** command to manually stop the packet capture:

> **capture** *capture_name***stop**

Where *capture_name* is the name of the packet capture you defined in the previous step.

The packet capture shows NSEL packets being sent from the ASA to the SEC, confirming that NSEL events are successfully transmitted to the configured destination.

Check for live NSEL events

This task allows you to verify that NSEL events are being properly received and processed by the Cisco Cloud system.

Check for both live and historical events. This procedure will filter for NSEL events that the Cisco Cloud has received within the last hour.

Procedure

Step 1 In the left pane, choose **Events & Logs** > **Events** > **Event Logging**.

Step 2 Click the **Live** tab.

Step 3 Pin-open the event filter.

Step 4 In the ASA Events section, make sure **NetFlow** is checked.

Step 5 In the Sensor ID field, enter the IP address of the ASA you configured to send NSEL events.

Step 6 At the bottom of the filter, make sure that **Include NetFlow Events** is checked.

The system displays live NSEL events from the specified ASA device, confirming that events are being successfully received and processed.

Check for historical NSEL events

Filter for NSEL events that the Cisco Cloud has received within a specific time-frame to verify event receipt and troubleshoot connectivity issues.

This procedure will filter for NSEL events that the Cisco Cloud has received within the time-frame you specify.

Procedure

Step 1 In the left pane, choose **Events & Logs** > **Events** > **Event Logging**.

Step 2 Click the **Historical** tab.

Step 3 Pin-open the event filter.

Step 4 In the ASA Events section, make sure **NetFlow** is checked.

Step 5 Set the Start time far enough back in time to check if Security Cloud Control ever did receive NSEL events.

Step 6 In the Sensor ID field, enter the IP address of the ASA you configured to send NSEL events.

Step 7 At the bottom of the filter, make sure that **Include NetFlow events** is checked.

The historical event filter displays NSEL events received from the specified ASA within your configured time-frame, confirming successful event transmission to Cisco Cloud.

Parsed ASA syslog events

Parsed ASA syslog events are specialized syslog messages that

- contain more event attributes than other syslog events
- let you search on any specific parsed field, and
- are forwarded by the SEC to the Cisco cloud with italicized EventTypes for identification.

Parsed syslog event processing

The SEC forwards all ASA events you specify to the Cisco cloud but only specific syslog messages are parsed. All parsed Syslogs events are shown with their EvenTypes italicised to help you identify.

For detailed explanations of syslogs see, Cisco ASA Series Syslog Messages.

Syslog ID	Syslog Category	Purpose of syslog messge
106015	Firewall	Represents out of state TCP Deny
106023	Firewall	A real IP packet was denied by the ACL. This message appears even if you do not have the **log** option enabled for an ACL.
106100	Access Lists/User Session	Packet was permitted or denied by an ACL.
113019	User Authentication	Critical AnyConnect
302013, 302015, 302017, 302020	User Session	Connection start and end syslogs for TCP, UDP, GRE, and ICMP connection creation.
302014, 302016, 302018, 302021	User Session	Connection start and end syslogs for TCP, UDP, GRE, and ICMP connection creation.
302020 - 302021	User Session	ICMP session establishment and teardown.
305006	User Session/NAT and PAT	NAT connection failure
305011-305014	User Session/NAT and PAT	NAT Build/Teardown related
313001, 313008	IP Stack	Represents denied connections to the box.
414004	System	Critical AnyConnect

Syslog ID	Syslog Category	Purpose of syslog messge
609001 - 609002	Firewall	A network state container was reserved/removed for host **ip-address** connected to a zone.
710002,710004 710005	User Session	To the box connections failures
710003	User Session	Represents denied connections to the box.
746012, 746013	User Session	Critical AnyConnect

Related information:

- Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface
- Filtering Events in the Event Logging Page