Secure Logging Analytics (SaaS) for ASA Devices

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

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.

With the **Logging Analytics and Detection** package (formerly **Firewall Analytics and Logging** package), the system can apply Secure Cloud Analytics dynamic entity modeling to your FTD events, and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your FTD events and your network traffic, and generates observations and alerts. You can cross-launch from Security Cloud Control to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.

How ASA Events are Displayed in the Security Cloud Control Events Viewer

Syslog events and NSEL events are generated when logging is enabled on the ASA, and network traffic matches access control rule criteria. After the events are stored in the Cisco cloud, you can view them in Security Cloud Control.

You can install multiple Secure Event Connectors (SECs) and send events generated by a rule, on any device, to any of the SECs as if it were a syslog server. The SEC then forwards the event to the Cisco cloud. Do not forward the same events to all of your SECs. You will be duplicating the events sent to the Cisco cloud and needlessly inflate your daily ingest rate.

How Syslog and NSEL Events are Sent from an ASA to the Cisco Cloud by way of the Secure Event Connector

With the basic **Logging and Troubleshooting** license, this is how an ASA event reaches the Cisco cloud:

1. You onboard your ASA to Security Cloud Control using username and password.
2. You configure the ASA to forward syslog and NSEL events to any one of your SECs as if they were syslog servers and enable logging on the device.
3. The SEC forwards the events to the Cisco cloud where the events are stored.
4. Security Cloud Control displays events from the Cisco cloud in its Events Viewer based on the filters you set.

With the **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license, the following also occur:

1. Cisco Secure Cloud Analytics applies analytics to the ASA syslog events stored in the Cisco cloud.
2. Generated observations and alerts are accessible from the Secure Cloud Analytics portal associated with your Security Cloud Control portal.
3. From the Security Cloud Control portal, you can cross-launch your Secure Cloud Analytics portal to review these observations and alerts.

Componets Used in the Solution

Secure Device Connector (SDC)-The SDC connects Security Cloud Control to your ASAs. The login credentials for the ASA are stored on the SDC.

Secure Event Connector (SEC)-The SEC is an application that receives events from your ASAs and forwards them to the Cisco cloud. Once in the Cisco cloud, you can view the events on Security Cloud Control's Event Logging page or analyze them with Secure Cloud Analytics. Depending on your environment, the SEC is installed on a Secure Device Connector, if you have one; or on its own Security Cloud Control Connector virtual machine that you maintain in your network. See About Secure Event Connectors for more information.

Adaptive Security Appliance (ASA)-The ASA provides advanced stateful firewall and VPN concentrator functionality as well as integrated services with add-on modules. The ASA includes many advanced features, such as multiple security contexts (similar to virtualized firewalls), clustering (combining multiple firewalls into a single firewall), transparent (Layer 2) firewall or routed (Layer 3) firewall operation, advanced inspection engines, IPsec VPN, SSL VPN, and clientless SSL VPN support, and many more features.

Secure Cloud Analytics applies dynamic entity modeling to ASA events, generating detections based on this information. This provides a deeper analysis of telemetry gathered from your network, allowing you to identify trends and examine anomalous behavior in your network traffic. You would make use of this service if you have a **Logging Analytics and Detection** or **Total Network Analytics and Monitoring** license.

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 the Security Analytics and Logging License table.
- **Adaptive Security Appliance (ASA)**. Base license or higher.

Security Analytics and Logging Licensing

In order to implement Security Analytics and Logging (SaaS), you need to purchase one of these licenses:

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Logging and Troubleshooting	• View ASA events and event detail within Security Cloud Control, both as a live feed and as a historical view	• 1 year • 3 years • 5 years	• Security Cloud Control • An on-premises ASA deployment running software version 9.6 or greater. • Deployment of one or more SECs to pass ASA events to the Cisco cloud.
Logging Analytics and Detection (formerly **Firewall Analytics and Monitoring**)	**Logging and Troubleshooting** functionality, plus: • Apply dynamic entity modeling and behavioral analytics to your events. • Open alerts in Secure Cloud Analytics based on event data, cross-launching from the Security Cloud Control event viewer.	• 1 year • 3 years • 5 years	• Security Cloud Control • An on-premises ASA deployment running software version 9.6 or greater • Deployment of one or more SECs to pass ASA events to the Cisco cloud. • A newly provisioned or existing Cisco Secure Cloud Analytics portal.

License Name	Provided Functionality	Available License Durations	Functionality Prerequisites
Total Network Analytics and Monitoring	**Logging Analytics and Detection**, plus: • Apply dynamic entity modeling and behavioral analytics to ASA events, on-premises network traffic, and cloud-based network traffic • Open alerts in Cisco Secure Cloud Analytics based on the combination of ASA event data, on-premises network traffic flow data collected by Cisco Secure Cloud Analytics sensors, and cloud-based network traffic passed to Cisco Secure Cloud Analytics, cross-launching from the Security Cloud Control event viewer.	• 1 year • 3 years • 5 years	• Security Cloud Control • An on-premises ASA deployment running software version 9.6 or greater • Deployment of one or more SECs to pass events to the Cisco cloud. • Deployment of at least one Cisco Secure Cloud Analytics sensor version 4.1 or greater to pass network traffic flow data to the cloud OR integrating Cisco Secure Cloud Analytics with a cloud-based deployment, to pass network traffic flow data to Cisco Secure Cloud Analytics. • A newly provisioned or existing Cisco Secure Cloud Analytics portal.

Data Plans

You need to buy a data plan that reflects the number of events the Cisco cloud receives from your on-boarded ASAs on a daily basis. This is called your "daily ingest rate." You can use the Logging Volume Estimator Tool to estimate your daily ingest rate and as that rate changes you can update your data plan.

Data plans are available in 1 GB daily volumes increments, and in 1, 3 or 5 year terms. See the Secure Logging Analytics (SaaS) Ordering Guide for information about data plans.

Note If you have a Security Analytics and Logging license and data plan, then obtain a different license at a later date, that alone does not require you to obtain a different data plan. If your network traffic throughput changes and you obtain a different data plan, that alone does not require you to obtain a different Security Analytics and Logging license.

30-day Free Trial

You can request a 30-day risk-free trial by logging in to Security Cloud Control and navigating **Events & Logs** > **Events** > **Event Logging** tab. On completion of the 30-day trial, you can order the desired event data volume to continue the service from Cisco Commerce Workspace (CCW), by following the instructions in the Secure Logging Analytics (SaaS) ordering guide.

Next Step

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

Implementing Secure Logging Analytics (SaaS) for ASA Devices

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.

Workflow to Implement Cisco Security Analytics and Logging (SaaS) and Send Events through the Secure Event Connector to the Cisco Cloud

1. Be sure to review "Before you Begin" above to make sure your environment is properly configured.
2. Onboard ASA Device to Security Cloud Control using username and password.
3. Send ASA Syslog Events to the Cisco Cloud.
4. Configuring NSEL for ASA Devices Using a Security Cloud Control Macro.
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.
6. If you have a **Firewall Analytics and Monitoring** or **Total Network Analytics and Monitoring** license, continue with the next section, **Analyzing Events with Cisco Secure Cloud Analytics**.

Reviewing Cisco Secure Cloud Analytics Alerts by Cross-launching from Security Cloud Control

With a **Firewall Analytics and Monitoring** or **Total Network Analytics and Monitoring** license, you can cross-launch from Security Cloud Control to Secure Cloud Analytics to review the alerts generated by FTD events.

Review these articles for more information:

Troubleshooting Secure Event Connector Issues

Use these troubleshooting topics to gather status and logging information about

- Troubleshooting Secure Event Connector Onboarding Failures
- Event Logging Troubleshooting Log Files
- Use Health Check to Learn the State of your Secure Event Connector

Workflows

Troubleshooting Using Security and Analytics Logging Events describes using the events generated from Cisco Security Analytics and Logging to determine why a user can't access a network resource.

Send ASA Syslog Events to the Cisco Cloud using a Security Cloud Control Macro

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.

Security Cloud Control's Macro tool allows you to assemble a list of CLI commands, turn elements of the command syntax into parameters, and then save the list of commands so that it can be used more than once. Macros can also be run on more than one device at a time.

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

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.

Creating an ASA Security Analytics and Logging (SaaS) Macro

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.

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. 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 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.

Example

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.

What to do next

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.

Send ASA Syslog Events to the Cisco Cloud Using the Command Line Interface

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.

Limitations on Supported ASA Commands

Security Cloud Control does not yet support these syslog commands or message formats:

- EMBLEM format for syslogs
- Secure Syslogs

Security Cloud Control Command Line Interface for ASA

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

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. You are now ready to enter the commands described below at the prompt.

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.

Forward ASA Syslog Events to the Secure Event Connector

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.

Send ASA Syslog Events to the Cisco Cloud Using CLI

Procedure

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

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.

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 Event Storage 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
```

Related Infromation:

- Install a Secure Event Connector on an SDC Virtual Machine
- Install Second or Subsequent SECs for your Tenant

Create a Custom Event List

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 the following three criteria:

- Event Class
- Severity
- Message ID

To create a custom event list to send to a specific logging destination (for example, a syslog server or a Secure Event Connector), perform the following steps:

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 the following:

  - 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
```

Include the Device ID in Non-EMBLEM Format Syslog Messages

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
```

NetFlow Secure Event Logging (NSEL) for ASA Devices

Basic syslog messages from the ASA lack much of the data that Secure Cloud Analytics needs to determine if events reported by the ASA indicate a threat. Netflow Secure Event Logging (NSEL) provides the Secure Cloud Analytics with that data.

"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 Security Cloud Control 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).

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
```

Before you Begin

Gather the following information:

- Read about macros in Security Cloud Control configuration guide if you have never worked with a Security Cloud Control Macro before.
- 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

Workflow

Follow this workflow to configure NSEL for ASA devices by using a Security Cloud Control macro. You need to follow each step:

1. Open the Configuring NSEL Macro , on page 18.
2. Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC, on page 18.
3. Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC, on page 19.
4. Define a Policy-Map for NSEL Events, on page 20.
5. Disable Redundant Syslog Messages, on page 21.
6. Review and Send the Macro, on page 22.

What to do next

Begin the workflow above by going to Open the Configuring NSEL Macro , on page 18.

Open the Configuring NSEL Macro

Before you begin

This is first part in a longer workflow, see Configuring NSEL for ASA Devices by Using a Security Cloud Control Macro, on page 16 before getting started.

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 ★ Macros 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**.

What to do next

Continue to Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC, on page 18.

Define the Destination of NSEL Messages and the Interval at Which They Are Sent to the SEC

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 Security Cloud Control 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.

What to do next

Continue to Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC, on page 19.

Create a Class-Map that Defines which NSEL Events Will Be Sent to the SEC

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 Security Cloud Control 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.

What to do next

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

Define a Policy-Map for NSEL Events

The 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 Security Cloud Control 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.

What to do next

Continue to, Disable Redundant Syslog Messages, on page 21.

Disable Redundant Syslog Messages

These instructions refer to this section of the macro. You do not need to modify the command.

logging flow-export-syslogs disable

Enabling NetFlow to export flow information makes the syslog messages in the following table redundant. In the interest of performance, we recommend that you disable redundant syslog messages, because the same information is exported through NetFlow.

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.

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
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.
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.

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.

Review and Send the Macro

Before you begin

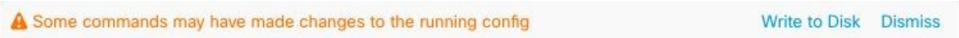
This is part of a larger workflow. See Configuring NSEL for ASA Devices by Using a Security Cloud Control Macro, on page 16, before getting started.

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.



⚠ Some commands may have made changes to the running config

- 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 descried in Configuring NSEL for ASA Devices by Using a Security Cloud Control Macro, on page 16.

Delete NetFlow Secure Event Logging (NSEL) Configuration from an ASA

This procedure explains how to DELETE the NetFlow Secure Event Logging (NSEL) Configuration on an ASA, which 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.

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

```
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}}
```

Open the DELETE-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 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 ★ Macros 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**.

Enter the Values in the Macro to Complete the No Commands

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.

Determine the Name of an ASA Global Policy

To determine the name of the ASA's global policy, follow this procedure:

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

Troubleshooting NSEL Data Flows

Once you have configured Netflow Secure Event Logging (NSEL) , use these procedures to verify that NSEL events are being sent from your ASA to the Cisco Cloud and that the Cisco Cloud is receiving them.

Note that once your ASA is configured to send NSEL events to the Secure Event Connector (SEC) and then on to the Cisco Cloud, 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.

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.

Perform these tasks:

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

Verify that NSEL Events are Being Sent to the SEC

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.

If there are no errors and packets are being sent, skip to Verify that NetFlow Packets are Being Received by the Cisco Cloud below.

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

- 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 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.

Verify that NetFlow Packets are Being Received by the Cisco Cloud

Before you Begin

Verify that NSEL events are being sent from the ASA.

Check for Live NSEL Events

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.

Check for Historical NSEL Events

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.

Parsed ASA Syslog Events

Parsed syslog events contain more event attributes than other syslog events and let you search on any specific parsed field. The SEC forwards all ASA events you specify to the Cisco cloud but only the syslog messages in the table below 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.

Syslog ID	Syslog Category	Purpose of syslog messge
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
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