Configuring NetFlow Secure Event Logging (NSEL)

This chapter describes how to configure NSEL, a security logging mechanism that is built on NetFlow Version 9 technology, and how to handle events and syslog messages through NSEL.

This chapter includes the following sections:

- Information About NSEL, page 43-1
- Licensing Requirements for NSEL, page 43-4
- Prerequisites for NSEL, page 43-4
- Guidelines and Limitations, page 43-4
- Configuring NSEL, page 43-5
- Monitoring NSEL, page 43-7
- Where to Go Next, page 43-7
- Additional References, page 43-7
- Feature History for NSEL, page 43-8

Information About NSEL

This section includes the following topics:

- Using NSEL and Syslog Messages, page 43-2
- Using NSEL in Clustering, page 43-3

The ASA and ASASM support NetFlow Version 9 services. For more information about NetFlow services, see the "RFCs" section on page 43-8.

The ASA and ASASM implementations of NSEL provide 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. NSEL events are used to export data about flow status and are triggered by the event that caused the state change.

The significant events that are tracked include flow-create, flow-teardown, and flow-denied (excluding those flows that are denied by EtherType ACLs). In addition, the ASA and ASASM implementation of NSEL generates periodic NSEL events, flow-update events, to provide periodic byte counters over the duration of the flow. These events are usually time-driven, which makes them more in line with traditional NetFlow; however, they may also be triggered by state changes in the flow.

Note The flow-update event feature is not available in Version 9.0(1). It is available in Versions 8.4(5) and 9.1(2).

Each NSEL record has an event ID and an extended event ID field, which describes the flow event.

The ASA and ASASM implementations of NSEL provide the following major functions:

- Tracks flow-create, flow-teardown, and flow-denied events, and generates appropriate NSEL data records.
- Triggers flow-update events and generates appropriate NSEL data records.
- Defines and exports templates that describe the progression of a flow. Templates describe the format of the data records that are exported through NetFlow. Each event has several record formats or templates associated with it.
- Tracks configured NSEL collectors and delivers templates and data records to these configured NSEL collectors through NetFlow over UDP only.
- Sends template information periodically to NSEL collectors. Collectors receive template definitions, normally before receiving flow records.
- Filters NSEL events based on the traffic and event type through Modular Policy Framework, then sends records to different collectors. Traffic is matched based on the order in which classes are configured. After a match is found, no other classes are checked. The supported event types are flow-create, flow-denied, flow-teardown, flow-update, and all. Records can be sent to different collectors. For example, with two collectors, you can do the following:
  - Log all flow-denied events that match ACL 1 to collector 1.
  - Log all flow-create events to collector 1.
  - Log all flow-teardown events to collector 2.
  - Log all flow-update events to collector 1.
- Delays the export of flow-create events.

Using NSEL and Syslog Messages

Table 43-1 lists the syslog messages that have an equivalent NSEL event, event ID, and extended event ID. The extended event ID provides more detail about the event (for example, which ACL—ingress or egress—has denied a flow).

Note Enabling NetFlow to export flow information makes the syslog messages that are listed in Table 43-1 redundant. In the interest of performance, we recommend that you disable redundant syslog messages, because the same information is exported through NetFlow.

Table 43-1 Syslog Messages and Equivalent NSEL Events

Syslog Message	Description	NSEL Event ID	NSEL Extended Event ID
106100	Generated whenever an 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.
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.

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

Using NSEL in Clustering

Each ASA establishes its own connection to the collector(s). The fields in the header of the export packet include the system up time and UNIX time (synchronized across the cluster). These fields are all local to an individual ASA. The NSEL collector uses the combination of the source IP address and source port of the packet to separate different exporters.

Each ASA manages and advertises its template independently. Because the ASA supports in-cluster upgrades, different units may run different image versions at a certain point in time. As a result, the template that each ASA supports may be different.

Note Clustering is available on the ASA 5580 and 5585-X only. For more information about clustering, see Chapter 10, “Configuring a Cluster of ASAs.”

Licensing Requirements for NSEL

Model	License Requirement
All models	Base License.

Prerequisites for NSEL

NSEL has the following prerequisites:

- IP address and hostname assignments must be unique throughout the NetFlow configuration.
- You must have at least one configured collector before you can use NSEL.
- You must configure NSEL collectors before you can configure filters via Modular Policy Framework.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall mode.

IPv6 Guidelines

Supports IPv6 for the **class-map**, **match access-list**, and **match any** commands.

Additional Guidelines and Limitations

- If you have previously configured flow-export actions using the **flow-export enable** command, and you upgrade to a later version, then your configuration is automatically converted to the new Modular Policy Framework **flow-export event-type** command, which is described under the **policy-map** command.
- If you have previously configured flow-export actions using the **flow-export event-type all** command, and you upgrade to a later version, NSEL automatically begins issuing flow-update records when necessary.
- Flow-export actions are not supported in interface-based policies. You can configure flow-export actions in a class-map only with the **match access-list**, **match any**, or **class-default** commands. You can only apply flow-export actions in a global service policy.
- To view bandwidth usage for NetFlow records (not available in real-time), you must use the threat detection feature.
- Only the ASA 5580 and 5585-X support clustering.

Configuring NSEL

This section describes how to configure NSEL and includes the following topics:

- Using NetFlow, page 43-5
- Matching NetFlow Events to Configured Collectors, page 43-6

Using NetFlow

The NetFlow pane lets you enable the transmission of data about a flow of packets. To access this pane, choose **Configuration > Device Management > Logging > NetFlow**.

Note IP address and hostname assignments should be unique throughout the NetFlow configuration.

To use NetFlow, perform the following steps:

Step 1 Enter the template timeout rate, which is the interval (in minutes) at which template records are sent to all configured collectors. The default value is 30 minutes.

Step 2 Enter the flow update interval, which specifies the time interval between flow-update events in minutes. Valid values are from 1 - 60 minutes. The default value is 1 minute.

Step 3 To delay the export of flow-creation events and process a single flow-teardown event instead of a flow-creation event and a flow-teardown event, check the **Delay export of flow creation events for short-lived flows** check box, then enter the number of seconds for the delay in the Delay By field.

Step 4 Specify the collector(s) to which NetFlow packets will be sent. You can configure a maximum of five collectors. To configure a collector, click **Add** to display the Add NetFlow Collector dialog box, and perform the following steps:

a. Choose the interface to which NetFlow packets will be sent from the drop-down list.

b. Enter the IP address or hostname and the UDP port number in the associated fields.

c. Click **OK**.

Step 5 To configure more collectors, repeat Step 4 for each additional collector.

Step 6 To change collector configuration details, select a collector and click **Edit**. To remove a configured collector, select it and click **Delete**.

Step 7 When NetFlow is enabled, certain syslog messages become redundant. To maintain system performance, we recommend that you disable all redundant syslog messages, because the same information is exported through NetFlow. To disable all redundant syslog messages, check the **Disable redundant syslog messages** check box. To display the redundant syslog messages and their status, click **Show Redundant Syslog Messages**.

The Redundant Syslog Messages dialog box appears. The Syslog ID field displays the redundant syslog message numbers. The Disabled field indicates whether or not the specified syslog message is disabled. Click **OK** to close this dialog box.

To disable individual redundant syslog messages, choose **Configuration > Device Management > Logging > Syslog Setup**.

Step 8 Click **Apply** to save your changes. Click **Reset** to enter new settings.

What to Do Next

See the "Matching NetFlow Events to Configured Collectors" section on page 43-6.

Matching NetFlow Events to Configured Collectors

After you configure NetFlow collectors, you can match a NetFlow event with any of these configured collectors.

To specify which NetFlow events should be sent to which collector, perform the following steps:

Step 1 In the ASDM main application window, choose **Configuration > Firewall > Service Policy Rules**.

Step 2 To add a service policy rule, perform the following steps:

a. Click **Add** to display the Add Service Policy Rule Wizard. For more information about service policy rules, see the firewall configuration guide.

b. Click the **Global - applies to all interfaces** radio button to apply the rule to the global policy. Click **Next**.

c. Check the **Source and Destination IP Address (uses ACL)** check box or the **Any traffic** check box as traffic match criteria, or click the **Use class-default as traffic class** radio button. Click **Next** to continue to the Rule Actions screen.

Note NetFlow actions are available only for global service policy rules and are applicable only to the class-default traffic class and to traffic classes with traffic match criteria of "Source and Destination IP Address (uses ACL)" or "Any traffic."

Step 3 In the Rule Actions screen, click the **NetFlow** tab.

Step 4 To specify flow events, click **Add** to display the Add Flow Event dialog box, then perform the following steps:

a. Choose the flow event type from the drop-down list. Available events are created, torn down, denied, updated, or all.

Note The flow-update event is not available in Version 9.0(1). It is available in Versions 8.4(5) and 9.1(2).

b. Choose collectors to which you want events sent by checking the corresponding check boxes in the Send column.

c. To add, edit or delete collectors, or to configure other NetFlow settings (for example, syslog messages), click **Manage** to display the Manage NetFlow Collectors dialog box. Click **OK** to close the Manage NetFlow Collectors dialog box and return to the Add Flow Event dialog box. For more information about configuring collectors, see Step 4 of the "Using NetFlow" section on page 43-5.

Step 5 Click **OK** to close the Add Flow Event dialog box and return to the NetFlow tab.

Step 6 To change flow event entries, select an entry from the list, and click **Edit**. To remove flow event entries, select an entry from the list, and click **Delete**.

Step 7 Click **Finish** to exit the wizard.

Step 8 To edit a NetFlow service policy rule, perform the following steps:

a. Select it in the Service Policy Rules table, and click **Edit**.

b. Click the **Rule Actions** tab, then click the **NetFlow** tab.

What to Do Next

See the "Monitoring NSEL" section on page 43-7.

Monitoring NSEL

You can use syslog messages to help troubleshoot errors or monitor system usage and performance.You can view real-time syslog messages that have been saved in the log buffer in a separate window, which include an explanation of the message, details about the message, and recommended actions to take, if necessary, to resolve an error. For more information, see the "Using NSEL and Syslog Messages" section on page 43-2.

To monitor NSEL, see the following pane:

Path	Purpose
Tools > Command Line Interface Enter the **show flow-export counters** command, then click **Send**.	Shows runtime counters, including statistical data and error data, for NSEL.
Tools > Command Line Interface Type **show logging flow-export-syslogs**, then press **Send**.	Lists all syslog messages that are captured by NSEL events.
Tools > Command Line Interface Enter the **show running-config flow-export** command, then click **Send**.	Shows the currently configured NetFlow commands.
Tools > Command Line Interface Enter the **show running-config logging** command, then click **Send**.	Shows disabled syslog messages, which are redundant syslog messages, because they export the same information through NetFlow.

Where to Go Next

To configure the syslog server, see Chapter 41, "Configuring Logging."

Additional References

For additional information related to implementing NSEL, see the following sections:

- Related Documents, page 43-8
- RFCs, page 43-8

Related Documents

Related Topic	Document Title
Using NSEL and Syslog Messages, page 43-2	*syslog messages guide*
Information about the implementation of NSEL on the ASA and ASA Services Module	*Cisco ASA 5500 Series Implementation Note for NetFlow Collectors* See the following article at https://supportforums.cisco.com/docs/DOC-6113.
Configuring NetFlow on the ASA and ASA Services Module using ASDM	See the following article at https://supportforums.cisco.com/docs/DOC-6114.

RFCs

RFC	Title
3954	Cisco Systems NetFlow Services Export Version 9

Feature History for NSEL

Table 43-2 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 43-2 Feature History for NSEL

Feature Name	Platform Releases	Feature Information
NetFlow	8.1(1)	The NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. NetFlow Version 9 services are used to export information about the progression of a flow from start to finish. The NetFlow implementation exports records that indicate significant events in the life of a flow. This implementation is different from traditional NetFlow, which exports data about flows at regular intervals. The NetFlow module also exports records about flows that are denied by ACLs. You can configure an ASA 5580 to send the following events using NetFlow: flow create, flow teardown, and flow denied (only flows denied by ACLs are reported). We introduced the following screen: Configuration > Device Management > Logging > NetFlow.
NetFlow Filtering	8.1(2)	You can filter NetFlow events based on traffic and event type, then send records to different collectors. For example, you can log all flow-create events to one collector, and log flow-denied events to a different collector. For short-lived flows, NetFlow collectors benefit from processing a single event instead of two events: flow create and flow teardown. You can configure a delay before sending the flow-create event. If the flow is torn down before the timer expires, only the flow teardown event is sent. The teardown event includes all information regarding the flow; no loss of information occurs. We modified the following screen: Configuration > Firewall > Service Policy Rules.

Table 43-2 Feature History for NSEL (continued)

Feature Name	Platform Releases	Feature Information
NSEL	8.2(1)	The NetFlow feature has been ported to all available models of ASAs.
Clustering	9.0(1)	The NetFlow feature supports clustering.
NSEL		A new NetFlow error counter, source port allocation failure, has been added. **Note** The flow-update event feature is not available in Version 9.0(1).
NSEL	9.1(2)	Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent. We modified the following screens: Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard - Rule Actions > NetFlow > Add Flow Event Configuration > Device Management > Logging > NetFlow.