CHAPTER 73

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.

The chapter includes the following sections:

Information About NSEL

The adaptive security appliance supports NetFlow Version 9 services. For more information about NetFlow services, see RFCs, page 73-11.

The adaptive security appliance implementation of NSEL is 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). Each NSEL record has an event ID and an extended event ID field, which describes the flow event.

The adaptive security appliance implementation of NSEL provides the following major functions:

- Keeps track of flow-create, flow-teardown, and flow-denied 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, and 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, 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 access-list 1 to collector 1.
  - Log all flow-create events to collector 1.
  - Log all flow-teardown events to collector 2.
- Delays the export of flow-create events.

Using NSEL and Syslog Messages

Table 73-1 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 73-1 redundant. In the interest of performance, we recommend that you disable redundant syslog messages, because the same information is exported through NetFlow. You can enable or disable individual syslog messages by following the procedure in the "Disabling and Reenabling NetFlow-related Syslog Messages" section on page 73-7.

Table 73-1 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.

Table 73-1 Syslog Messages and Equivalent NSEL Events (continued)

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.

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

Licensing Requirements for NSEL

The following table shows the licensing requirements for this feature:

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 modes.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

IPv6 Guidelines

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

Additional Guidelines and Limitations

- If you previously configured flow-export actions using the **flow-export enable** command, and you upgrade to a later version, then your configuration will be automatically converted to the new Modular Policy Framework **flow-export event-type** command, described under the **policy-map** command. For more information, see the *Release Notes for the Cisco ASA 5500 Series* for Version 8.1(2).
- 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.

Configuring NSEL

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

Configuring NSEL Collectors

To configure NSEL collectors, enter the following command:

Command	Purpose
flow-export destination *interface-name ipv4-address|hostname udp-port* **Example:** `hostname (config)# flow-export destination inside 209.165.200.225 2002`	Adds, edits, or deletes an NSEL collector to which NetFlow packets are sent. The **destination** keyword indicates that a NSEL collector is being configured. The *interface-name* argument is the name of the adaptive security appliance interface through which the collector is reached. The *ipv4-address* argument is the IP address of the machine running the collector application. The *hostname* argument is the destination IP address or name of the collector. The *udp-port* argument is the UDP port number to which NetFlow packets are sent. You can configure a maximum of five collectors. After a collector is configured, template records are automatically sent to all configured NSEL collectors. **Note** Make sure that collector applications use the Event Time field to correlate events.

What to Do Next

See the "Configuring Flow-Export Actions Through Modular Policy Framework" section on page 73-5.

Configuring Flow-Export Actions Through Modular Policy Framework

To export NSEL events by defining all classes with flow-export actions, enter the following commands:

	Command	Purpose
Step 1	**class-map** *flow_export_class* **Example:** `hostname (config-pmap)# class-map flow_export_class`	Defines the class map that identifies traffic for which NSEL events need to be exported. The *flow_export_class* argument is the name of the class map.
Step 2	Choose one of the following options:	
	match access-list *flow_export_acl* **Example:** `hostname (config-cmap)# match access-list flow_export_acl`	Configures the access list to match specific traffic. The *flow_export_acl* argument is the name of the access list.
	match any **Example:** `hostname (config-cmap)# match any`	Matches any traffic.
Step 3	**policy-map** *flow_export_policy* **Example:** `hostname(config)# policy-map flow_export_policy`	Defines the policy map to apply flow-export actions to the defined classes. The *flow_export_policy* argument is the name of the policy map. If you create a new policy map and apply it globally according to Step 6, the rest of the inspection policies will be deactivated. Alternatively, to insert a NetFlow class in the existing policy, enter the **class flow_export_class** command after the **policy-map global_policy** command. For more information about creating or modifying Modular Policy Framework, see Chapter 30, "Configuring a Service Policy Using the Modular Policy Framework.".
Step 4	**class** *flow_export_class* **Example:** `hostname (config-pmap)# class flow_export_class`	Defines the class to apply flow-export actions. The *flow_export_class* argument is the name of the class.

	Command	Purpose
Step 5	**flow-export event-type** *event-type* **destination** *flow_export_host1 [flow_export_host2]* **Example:** `hostname (config-pmap-c)# flow-export event-type all destination 209.165.200.230`	Configures a flow-export action. The **event_type** keyword is the name of the supported event being filtered. The *flow_export_host* argument is the IP address of a host. The **destination** keyword is the IP address of the configured collector.
Step 6	**service-policy** *flow_export_policy* **global** **Example:** `hostname (config)# service-policy flow_export_policy global`	Adds or edits the service policy globally. The *flow_export_policy* argument is the name of the policy map.

What to Do Next

See the "Configuring Template Timeout Intervals" section on page 73-6.

Configuring Template Timeout Intervals

To configure template timeout intervals, enter the following command:

Command	Purpose
flow-export template timeout-rate *minutes* **Example:** `hostname (config)# flow-export template timeout-rate 15`	Specifies the interval at which template records are sent to all configured output destinations. The **template** keyword indicates the template-specific configurations. The **timeout-rate** keyword specifies the time before templates are resent. The *minutes* argument specifies the time interval in minutes at which the templates are resent. The default value is 30 minutes.

What to Do Next

See the "Delaying Flow-Create Events" section on page 73-7.

Delaying Flow-Create Events

To delay the sending of flow-create events, enter the following command:

Command	Purpose
flow-export delay flow-create *seconds* **Example:** `hostname (config)# flow-export delay flow-create 10`	Delays the sending of a flow-create event by the specified number of seconds. The *seconds* argument indicates the amount of time allowed for the delay in seconds. If this command is not configured, there is no delay, and the flow-create event is exported as soon as the flow is created. If the flow is torn down before the configured delay, the flow-create event is not sent; an extended flow teardown event is sent instead.

What to Do Next

See the "Disabling and Reenabling NetFlow-related Syslog Messages" section on page 73-7.

Disabling and Reenabling NetFlow-related Syslog Messages

To disable and reenable NetFlow-related syslog messages, enter the following commands:

	Command	Purpose
Step 1	**logging flow-export syslogs disable** **Example:** `hostname(config)# logging flow-export syslogs disable`	Disables syslog messages that have become redundant because of NSEL. **Note** Although you execute this command in global configuration mode, it is not stored in the configuration. Only the **no logging message xxxxxx** commands are stored in the configuration.
Step 2	**logging message** *xxxxxx* **Example:** `hostname(config)# logging message 302013`	Reenables syslog messages individually, where *xxxxxx* is the specified syslog message that you want to reenable.
Step 3	**logging flow-export syslogs enable** **Example:** `hostname(config)# logging flow-export syslogs enable`	Reenables all NSEL events at the same time.

What to Do Next

See the "Clearing Runtime Counters" section on page 73-8.

Clearing Runtime Counters

To reset runtime counters, enter the following command:

Command	Purpose
clear flow-export counters **Example:** `hostname# clear flow-export counters`	Resets all runtime counters for NSEL to zero.

What to Do Next

See the "Monitoring NSEL" section on page 73-8.

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 73-2.

NSEL Monitoring Commands

To monitor NSEL, enter the following command:

Command	Purpose
show flow-export counters	Shows runtime counters, including statistical data and error data, for NSEL.
show logging flow-export-syslogs	Lists all syslog messages that are captured by NSEL events.
show running-config logging	Shows disabled syslog messages, which are redundant syslog messages, because they export the same information through NetFlow.

Examples

```
hostname (config)# show flow-export counters

destination: inside 209.165.200.225 2055

Statistics:
```

```
    packets sent                250
Errors:
    block allocation errors       0
    invalid interface             0
    template send failure         0

hostname# show logging flow-export-syslogs

Syslog ID       Type                          Status
302013          Flow Created                  Enabled
302015          Flow Created                  Enabled
302017          Flow Created                  Enabled
302020          Flow Created                  Enabled
302014          Flow Deleted                  Enabled
302016          Flow Deleted                  Enabled
302018          Flow Deleted                  Enabled
302021          Flow Deleted                  Enabled
106015          Flow Denied                   Enabled
106023          Flow Denied                   Enabled
313001          Flow Denied                   Enabled
313008          Flow Denied                   Enabled
710003          Flow Denied                   Enabled
106100          Flow Created/Denied           Enabled


hostname (config)# show running-config logging

no logging message 313008
no logging message 313001
```

Configuration Examples for NSEL

The following examples show how to filter NSEL events, with these collectors already configured:

- **flow-export destination inside 209.165.200.230**
- **flow-export destination outside 209.165.201.29 2055**
- **flow-export destination outside 209.165.201.27 2055**

Log all events between hosts 209.165.200.224 and hosts 209.165.201.224 to 209.165.200.230, and log all other events to 209.165.201.29:

```
hostname (config)# access-list flow_export_acl permit ip host 209.165.200.224 host
209.165.201.224
hostname (config)# class-map flow_export_class
hostname (config-cmap)# match access-list flow_export_acl
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class flow_export_class
hostname (config-pmap-c)# flow-export event-type all destination 209.165.200.230
hostname (config-pmap)# class class-default
hostname (config-pmap-c)# flow-export event-type all destination 209.165.201.29
hostname (config)# service-policy flow_export_policy global
```

Log flow-create events to 209.165.200.230, flow-teardown events to 209.165.201.29, and flow-denied events to 209.165.201.27:

```
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class class-default
hostname (config-pmap-c)# flow-export event-type flow-creation destination 209.165.200.230
hostname (config-pmap-c)# flow-export event-type flow-teardown destination 209.165.201.29
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
```

```
hostname (config)# service-policy flow_export_policy global
```

Log flow-create events between hosts 209.165.200.224 and 209.165.200.230 to 209.165.201.29, and log all flow-denied events to 209.165.201.27:

```
hostname (config)# access-list flow_export_acl permit ip host 209.165.200.224 host
209.165.200.230
hostname (config)# class-map flow_export_class
hostname (config)# match access-list flow_export_acl
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class flow_export_class
hostname (config-pmap-c)# flow-export event-type flow-creation destination 209.165.200.29
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
hostname (config-pmap)# class class-default
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
hostname (config)# service-policy flow_export_policy global
```

Note You must enter the following command:

```
hostname (config-pmap-c)# flow-export event-type flow-denied destination 209.165.201.27
```

for *flow_export_acl*, because traffic is not checked after the first match, and you must explicitly define the action to log flow-denied events that match *flow_export_acl*.

Log all traffic except traffic between hosts 209.165.201.27 and 209.165.201.50 to 209.165.201.27:

```
hostname (config)# access-list flow_export_acl deny ip host 209.165.201.30 host
209.165.201.50
hostname (config)# access-list flow_export_acl permit ip any any
hostname (config)# class-map flow_export_class
hostname (config-cmap)# match access-list flow_export_acl
hostname (config)# policy-map flow_export_policy
hostname (config-pmap)# class flow_export_class
hostname (config-pmap-c)# flow-export event-type all destination 209.165.201.27
hostname (config)# service-policy flow_export_policy global
```

Where to Go Next

To configure the syslog server, see Chapter 72, “Configuring Logging.”

Additional References

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

Related Documents

Related Topic	Document Title
Using NSEL and Syslog Messages, page 73-2	*Cisco ASA 5500 Series System Log Messages*
Information about the implementation of NSEL on the adaptive security appliance	*Cisco ASA 5500 Series Implementation Note for NetFlow Collectors*

RFCs

RFC	Title
3954	Cisco Systems NetFlow Services Export Version 9

Feature History for NSEL

Table 73-2 lists each feature change and the platform release in which it was implemented..

Table 73-2 Feature History for NSEL

Feature Name	Platform Releases	Feature Information
NetFlow	8.1(1)	The NetFlow feature enhances the adaptive security appliance 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 access lists. 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). The following commands were introduced: **clear flow-export counters, flow-export enable, flow-export destination, flow-export template timeout-rate, logging flow-export syslogs enable, logging flow-export syslogs disable, show flow-export counters, show logging flow-export-syslogs**.
NetFlow Filtering	8.1(2)	You can filter NetFlow events based on traffic and event-type, and 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. The following commands were modified: **class, class-map, flow-export event-type destination, match access-list, policy-map, service-policy**. 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. The following command was introduced: **flow-export delay flow-create**.
NSEL	8.2(1)	The NetFlow feature has been ported to all ASA 5500 series adaptive security appliances.