



Implementation Note for NetFlow Collectors, Version 8.1(2)

This document describes the implementation details for NetFlow collectors for the ASA 5580 adaptive security appliance, and includes the following sections:

- [Event-Driven Data Export](#)
- [Bidirectional Flows](#)
- [Template Updates](#)
- [Options Template and Data Records](#)
- [Observation Point and Observation Domain](#)
- [Flow Filtering](#)
- [Transport Protocol](#)
- [Information Model](#)
- [Command-Line Interface](#)
- [External Partner Implementation Suggestions](#)
- [Obtaining Documentation and Submitting a Service Request](#)

Event-Driven Data Export

Because the ASA 5580 device implements stateful tracking of flows, the tracked flows go through a set of state changes. NetFlow is used to export data about the status of a flow, and is triggered by the event that caused the state change. The tracked events include flow creation, flow denial (only flows denied by ACLs), and flow teardown.

The adaptive security appliance also exports syslog messages that include the same information. You can disable these syslog messages to avoid performance degradation by generating both NSEL records and syslog messages that represent the same event. For a list of redundant syslog messages, see the [Configuring and Using NetFlow Secure Event Logging \(NSEL\)](#) section in the *Cisco Security Appliance Command Line Configuration Guide*.



Bidirectional Flows

Most bidirectional flows are already assembled internally and are considered a single flow. The flow records reported by NSEL on the ASA 5580 adaptive security appliance describe both directions of the flow. The data records explicitly define the source (initiator) and destination (responder) of the connection, and you can use this information to determine the direction of flow, if required by collector applications.

Template Updates

The RFC states that templates may be sent to the user either at regular time intervals or after a set number of data records have been exported. These update intervals must be configurable. This implementation supports template updates by time interval only. Template updates based on the number of data records are not supported.

Options Template and Data Records

No options template or data records will be exported. Some fields are supported by **show** commands in the CLI. Collector applications must issue **show** commands to obtain additional information about certain fields. In addition, collectors must have unique hostnames and IP addresses; otherwise, the inspection behavior will be unpredictable. For more information, see the [Information Model](#) section and the *Cisco Security Appliance Command Line Configuration Guide*.

Observation Point and Observation Domain

The adaptive security appliance is an Observation Domain, with each interface also an Observation Point. Flows that are created through all interfaces are exported, and no option exists to limit or filter the exported data to a specific set of interfaces. Flows that are created by external devices that connect to the adaptive security appliance are also exported.

Flow Filtering

Only records for certain flows may need to be exported. For example, the adaptive security appliance can generate NSEL events for flows that match an ACE. You can use this method to restrict the number of NSEL events that are generated for NetFlow. This implementation supports the filtering of NSEL events based on traffic and event type through Modular Policy Framework, with records sent to different collectors.

For example, with two collectors, you can do the following:

- Log all flow creation events to Collector 1.
- Log all flow denied events matching ACL1 to Collector 1.
- Log all events matching ACL1 to Collector 2.

If the Modular Policy Framework is not configured for NetFlow, no NSEL events are generated. For more information, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*.

Transport Protocol

This implementation of NetFlow only supports UDP payloads.

Information Model

This section describes the data types and templates that are exported through NetFlow, and includes the following topics:

- [Data Fields](#)
- [Data Records and Templates](#)

The list of required data elements was arrived at by consolidating the data exported by syslog messages that are generated for events that results in the export of NSEL records.

Data Fields

[Table 1](#) lists the data elements that are exported from the ASA 5580 adaptive security appliance through NSEL.

The columns include the following information:

- ID—A unique name that represents the field type
- TYPE—The value assigned for this field type
- LEN—The length of the field in records exported for the selected adaptive security appliance
- DESC—A description of what the field type represents

Table 1 Data Records Exported Through NSEL

ID	TYPE	LEN	DESC
Connection ID Field			
NF_F_CONN_ID	148	4	An identifier of a unique flow for the device
Flow ID Fields (L3 IPv4)			
NF_F_SRC_ADDR_IPV4	8	4	Source IPv4 address
NF_F_DST_ADDR_IPV4	12	4	Destination IPv4 address
NF_F_PROTOCOL	4	1	IP value
Flow ID Fields (L3 IPv6)			
NF_F_SRC_ADDR_IPV6	27	16	Source IPv6 address
NF_F_DST_ADDR_IPV6	28	16	Destination IPv6 address
Flow ID Fields (L4)			
NF_F_SRC_PORT	7	2	Source port
NF_F_DST_PORT	11	2	Destination port
NF_F_ICMP_TYPE	176	1	ICMP type value
NF_F_ICMP_CODE	177	1	ICMP code value
NF_F_ICMP_TYPE_IPV6	178	1	ICMP IPv6 type value

Table 1 Data Records Exported Through NSEL (continued)

ID	TYPE	LEN	DESC
NF_F_ICMP_CODE_IPV6	179	1	ICMP IPv6 code value
Flow ID Fields (INTF)			
NF_F_SRC_INTF_ID	10	2	Ingress IFC SNMP IF index
NF_F_DST_INTF_ID	14	2	Egress IFC SNMP IF index
Mapped Flow ID Fields			
NF_F_XLATE_SRC_ADDR_IPV4	40001	4	Mapped source IPv4 address
NF_F_XLATE_DST_ADDR_IPV4	40002	4	Mapped destination IPv4 address
NF_F_SLATE_SRC_PORT	40003	2	Mapped source port
NF_F_XLATE_DST_PORT	40004	2	Mapped destination port
Status or Event Fields			
NF_F_FW_EVENT	40005	1	High-level event code. Values are as follows: <ul style="list-style-type: none"> • 0—Default (ignore) • 1—Flow created • 2—Flow deleted • 3—Flow denied
NF_F_FW_EXT_EVENT	330002	2	Extended event code. These values provide additional information about the event.
Timestamp and Statistics Fields			
NF_F_EVENT_TIME_MSEC	323	8	The time that the event occurred, which comes from IPFIX. Use 324 for time in microseconds, and 325 for time in nanoseconds. Time has been counted as milliseconds since 0000 UTC January 1, 1970.
NF_F_FLOW_BYTES	85	4	The total number of bytes of the flow
NF_F_FLOW_CREATE_TIME_MSEC	152	8	The time that the flow was created, which is included in extended flow-teardown events in which the flow-create event was not sent earlier. The flow duration can be determined with the event time for the flow-teardown and flow-create times.
ACL Fields			
NF_F_INGRESS_ACL_ID	33000	12	The input ACL that permitted or denied the flow All ACL IDs are composed of the following three, four-byte values: <ul style="list-style-type: none"> • Hash value or ID of the ACL name • Hash value, ID, or line of an ACE within the ACL • Hash value or ID of an extended ACE configuration
NF_F_EGRESS_ACL_ID	33001	12	The output ACL that permitted or denied a flow

Table 1 Data Records Exported Through NSEL (continued)

ID	TYPE	LEN	DESC
AAA Fields			
NF_F_USERNAME	40000	20	AAA username
NF_F_USERNAME_MAX	40000	65	AAA username of maximum permitted size

Event IDs Field

The Event ID field describes the event that resulted in the NSEL record. [Table 2](#) lists the values for event IDs.

Table 2 Values for Event IDs

Event ID	Description
0	Ignore—This value indicates that a field must be ignored. This value is not used in the current release.
1	Flow created—This value indicates that a new flow was created.
2	Flow deleted—This value indicates that a flow was deleted.
3	Flow denied—This value indicates that a flow was denied.

Extended Event IDs Field

The extended event ID provides additional information about a particular event. This field is specific to the ASA 5580 adaptive security appliance, and includes a product-specific field ID (33002). [Table 3](#) lists the values for extended event IDs.

Table 3 Values for Extended Event IDs

Extended Event ID	Event	Description
0	Ignore	This value indicates that the field must be ignored.
> 1000	Flow denied	Values above 1000 represent various reasons for why a flow was denied.
1001	Flow denied	A flow was denied by an ingress ACL.
1002	Flow denied	A flow was denied by an egress ACL.
1003	Flow denied	The adaptive security appliance denied an attempt to connect to the interface service. For example, this message appears with the SNMP service when the adaptive security appliance receives an SNMP request from an unauthorized SNMP management station.
1004	Flow denied	The flow was denied because the first packet on the TCP was not a TCP SYN packet.
> 2000	Flow deleted	Values above 2000 represent various reasons why a flow was terminated.

Event Time Field

Each NSEL data record has the event time field (NF_F_EVENT_TIME_MSEC), which is the time that the event occurred in milliseconds. The NetFlow packet may consist of multiple events; however, the time that the packet is sent does not represent the time that the event occurred, because the NetFlow service waits for multiple events to pack the NetFlow packet.



Note

Different events in the life of a flow may be issued in separate NetFlow packets and may arrive out-of-order at the collector. For example, the packet containing a flow teardown event may reach the collector before the packet containing a flow creation event. As a result, it is important that collector applications use the Event Time field to correlate events.

Data Records and Templates

This section describes the templates that are supported for various events and includes the following topics:

- [Templates for Flow Creation Events](#)
- [Templates for Flow Teardown Events](#)
- [Templates for Flow Denied Events, page 9](#)
- [Table 5 Templates for Extended Flow Teardown Events, page 8](#)

Templates describe the format of data records that are exported through NetFlow. Each flow event has several record formats or templates associated with it, as follows:

- There are different templates for different events.
- There are different templates for IPv4 and IPv6 flows under each event type.
- IPv6 templates do not have any xlate fields, because NAT does not support IPv6.
- The flow creation/permitted event has different templates, which are based on the size of the username field associated with the flow. Different templates are required because the size of string fields is fixed in NetFlow. Having a single template with the largest possible size for string results is a waste of bandwidth, because most strings are far shorter than the maximum value. Two types of username fields are defined, which result in two types of templates in each category.
 - Common username size for usernames that are less than 20 characters
 - Maximum username size for usernames that are up to a maximum of 65 characters
 - Each template has the Event Type and Extended Event Type fields, which can interpret or act on the event.



Note

Template definitions are sent to all collectors, and you should use these IDs and definitions to parse data records.

Templates for Flow Creation Events

Flow creation events indicate that a flow has been created by the adaptive security appliance. This event is also a log of flows that the adaptive security appliance allows. [Table 4](#) describes the templates to use for flow creation events.

Table 4 *Templates for Flow Creation Events*

Description	Fields
IPv4 flow creation event with common username size (20 chars)	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
IPv4 flow creation event with maximum username size (65 chars)	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
IPv6 flow creation with common username size	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
IPv6 flow creation with maximum username size	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Delays for Flow Creation Events

For short-lived flows, NSEL collection devices would benefit from processing a single event instead of these two events—flow-create and flow-teardown. So a configurable CLI parameter is provided to delay sending of the flow-create event. If the timer fires, the flow-create event is sent. However, if the flow is torn down before the timer expires, *only* the flow-teardown event is sent; no flow-create event is sent.

The flow-teardown event is extended and includes all information regarding the flow; no information is lost. New templates are introduced to accommodate the extended flow-teardown events.

Templates for Extended Flow Teardown Events

Table 5 describes the templates that are used for extended flow-teardown events.

Table 5 *Templates for Extended Flow Teardown Events*

Description	Fields
Extended IPv4 flow teardown with common username size (20 chars)	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
Extended IPv4 flow teardown with maximum username size (65 chars)	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Table 5 *Templates for Extended Flow Teardown Events (continued)*

Extended IPv6 flow teardown with common username size (20 chars)	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
Extended IPv6 flow teardown with maximum username size (65 chars)	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Templates for Flow Denied Events

Flow denied events indicate that a flow has been denied. [Table 6](#) describes the templates that are used for flow denied events.

Table 6 *Templates for Flow Denied Events*

Description	Fields
IPv4 flow denied	NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv4 flow denied, no xlate fields present	NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID
IPv6 flow denied	NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID

Templates for Flow Teardown Events

Flow teardown events indicate that a flow has been terminated. [Table 7](#) describes the templates that are used for flow teardown events.

Table 7 *Templates for Flow Teardown Events*

Description	Fields
IPv4 flow terminated	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV4, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV4, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES
IPv6 flow terminated	NF_F_CONN_ID, NF_F_SRC_ADDR_IPV6, NF_F_SRC_PORT, NF_F_SRC_INTF_ID, NF_F_DST_ADDR_IPV6, NF_F_DST_PORT, NF_F_DST_INTF_ID, NF_F_PROTOCOL, NF_F_ICMP_TYPE, NF_F_ICMP_CODE, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FLOW_BYTES

Command-Line Interface

For information about the commands that are used to configure the NSEL implementation on the adaptive security appliance, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*. The commands are also used to display additional information about the fields in NSEL records.

External Partner Implementation Suggestions

This section provides examples of flows that generate events and includes information about how to implement collector support for the new NSEL fields for the adaptive security appliance, and includes the following topics:

- [Example 1: Allowed Flow with PAT Interface](#)
- [Example 2: Denied Flow on Egress with PAT Interface](#)

Example 1: Allowed Flow with PAT Interface

The following example shows an allowed flow that uses the PAT interface. The output interface IP address is 209.165.200.225. The user is authenticated as User A. No ACLs are specified; however, the flow is outbound, so it is allowed by default. According to [Figure 1](#) and the description provided, a flow creation event would be issued.

Figure 1 Example of an Allowed Flow with a PAT Interface

The resulting NSEL record would include the following fields and values:

Field	Value
NF_F_CONN_ID	xxxx
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	56789
NF_F_SRC_INTF_ID	1
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	0
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	1024
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	1
NF_F_FW_EXT_EVENT	0
NF_F_EVENT_TIME_MSEC	YYYYYYYY
NF_F_FLOW_BYTES	0
NF_F_INGRESS_ACL_ID	0
NF_F_EGRESS_ACL_ID	0
NF_F_USERNAME	User A

Example 2: Denied Flow on Egress with PAT Interface

The following example shows a denied flow through an egress ACL that uses the PAT interface. The output interface IP address is 209.165.200.225. The user is authenticated as User A. An input ACL (foo) allows the flow, but an output ACL (bar) denies the flow. The input ACL (foo) is specified with an object group, as shown in the following example:

```
hostname# object-group network host_grp_1
  network-object host 209.165.200.254
  network-object host 209.165.201.1
hostname (config)# access-list foo extended permit tcp object-group host_grp_1 any eq www
```

```
hostname (config)# access-list bar extended deny tcp any any
hostname (config)# access-group foo in interface inside
hostname (config)# access-group bar out interface outside
```

According to [Figure 1](#) and the description provided, a flow denied event would be issued.

The resulting NSEL record would include the following fields and values:

Field	Value
NF_F_SRC_ADDR_IPV4	209.165.200.254
NF_F_SRC_PORT	37518
NF_F_SRC_INTF_ID	7
NF_F_DST_ADDR_IPV4	209.165.200.225
NF_F_DST_PORT	80
NF_F_DST_INTF_ID	8
NF_F_PROTOCOL	6
NF_F_ICMP_TYPE	0
NF_F_ICMP_CODE	0
NF_F_XLATE_SRC_ADDR_IPV4	209.165.201.1
NF_F_XLATE_DST_ADDR_IPV4	209.165.200.225
NF_F_XLATE_SRC_PORT	48264
NF_F_XLATE_DST_PORT	80
NF_F_FW_EVENT	3
NF_F_FW_EXT_EVENT	1002 (egress ACL)
NF_F_EVENT_TIME_MSEC	1187374131808
NF_F_INGRESS_ACL_ID	0x102154c1d0e5806e7e5ad93b
NF_F_EGRESS_ACL_ID	0x5da9bb6984434b4b00000000
NF_F_USERNAME	User A

Decoding Device Fields Through the CLI

To decode some of the field values that the adaptive security appliance populates, direct interaction with the device may be required. We recommend that you use a dynamic mechanism such as *expect* scripts to obtain the required information from the CLI of the device that issued the event.

The device supports console, Telnet, and SSH secure shell access; however, SSH is the recommended method because of performance and security. The following sections describe fields that you need to decode, based on interaction with the adaptive security appliance, and includes the following topics:

- [Interface ID Fields](#)
- [ACL ID Fields](#)
- [Event Codes](#)
- [Extended Event Codes](#)

Interface ID Fields

You can also decode the Interface ID fields using SNMP GET requests from the device interface MIB. This is the only field that has MIB support.

You may use the **show interface detail** command to obtain a list of all the interfaces on the device. This output includes a line under each interface that corresponds to the Interface ID value sent in the NetFlow fields. In the following example, the interface number is 8.

```
hostname(config)# show interface filter-outside detail
Interface GigabitEthernet4/3 "filter-outside", is up, line protocol is up
Hardware is i82571EB 4CU rev06, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
MAC address 0015.1715.59c7, MTU 1500
IP address 209.165.200.254, subnet mask 255.255.255.224
532594 packets input, 88376018 bytes, 0 no buffer
Received 3 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 L2 decode drops
675393 packets output, 53208679 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (curr/max packets): hardware (36/511) software (0/0)
output queue (curr/max packets): hardware (59/68) software (0/0)
Traffic Statistics for "filter-outside":
532594 packets input, 78636500 bytes
675393 packets output, 40866215 bytes
10837 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 0 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 8
Interface config status is active
Interface state is active
```

ACL ID Fields

The 12-byte raw ACL ID must be divided into its three constituent parts, as follows:

- The first four bytes are the ACL Name ID.
- The next four bytes are the ACL Entry ID (ACE)/Object-Group ID.
- The final four bytes are the Extended ACL Entry ID.

These individual values can be looked up in the output of the **show access-list** command from the adaptive security appliance. The ACL Name ID is at the end of the ACL first line in this output. The ACE ID is at the end of each individual ACL entry line.



Note

If you use an object-group in an access list, then the second four-byte ID is not actually the ACE ID; it is the Object-Group ID. The Extended ACE ID (the final four-byte part) refers to the actual individual ACL Entry ID. The following example shows these entries:

```
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list foo; 2 elements; name hash: 0x102154c1
access-list foo line 1 extended permit tcp object-group host_grp_1 any eq www 0xd0e5806e
access-list foo line 1 extended permit tcp host 209.165.200.254 any eq www (hitcnt=4)
0x7e5ad93b
access-list foo line 1 extended permit tcp host 209.165.201.1 any eq www (hitcnt=0)
0xe0c1846b
access-list bar; 1 elements; name hash: 0x5da9bb69
access-list bar line 1 extended deny tcp any any (hitcnt=41) 0x84434b4b
```

This example is similar to the example shown in [Example 2: Denied Flow on Egress with PAT Interface](#). In the denied flow example, the ACL IDs are divided into their constituent parts as follows:

- **NF_F_INGRESS_ACL_ID:** InAcl: 0x102154c1d0e5806e7e5ad93b
 where 0x102154c1 are the first four bytes, 0xd0e5806e are the second four bytes, and 0x7e5ad93b are the final four bytes.
- **NF_F_EGRESS_ACL_ID:** 0x5da9bb6984434b4b00000000
 where 0x5da9bb69 are the first four bytes, 0x84434b4b are the second four bytes, and 0x00000000 are the final four bytes.



Note

Each of these IDs corresponds to lines from the **show access-list** command example.

From these IDs, you can deduce that access-list *foo* was applied on the input interface, and that access-list *bar* was applied on the output interface. That information is also available through the **show run access-group** command, but the added benefit of these ACL IDs is that you can identify the individual ACE that caused the permit or deny action. Because this flow was denied on egress (determined from the extended event code), you know that the ingress ACL ID identifies the ACE line that permitted the flow and that the egress ACL ID identifies the ACE that denied the flow.

Event Codes

You must hard code event codes into the collector, because the adaptive security appliance only issues three different high-level event types (creation, teardown, and denial).

Extended Event Codes

Of the three high-level event codes, only two have extended event codes: the flow denial and flow teardown event types. For the flow denied event, the list of extended event codes in [Table 3](#) should suffice to determine the reason why the flow was denied. However, for the flow teardown event, there are too many event codes to list in this document, and the set of reasons is quite fluid.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

© 2008 Cisco Systems, Inc. All rights reserved.