Cisco Secure Firewall ASA NetFlow Implementation Guide

Last Modified: 2022-05-31

Cisco Secure Firewall ASA NetFlow Implementation Guide

This guide describes how to configure NetFlow Secure Event Logging (NSEL), how to handle events and syslog messages through NSEL, and how to use NetFlow collectors.

About NSEL

The Secure Firewall ASA supports NetFlow Version 9 services. 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.

Netflow data cannot be manually extracted from ASA device and manually sent to the collector. The 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, flow-denied (excluding those flows that are denied by EtherType ACLs), and flow-update. The ASA implementation of NSEL generates periodic NSEL events, called 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 is not available in Version 9.0(1). It is available in Versions 8.4(5), and 9.1(2) and later.

The ASA 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.

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

Syslog Messages and NSEL Events

The following table 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 corresponding syslog messages redundant. For better 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 Disable and Reenable NetFlow-related Syslog Messages.

Table 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.

NSEL Collectors

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.

Bidirectional Flows

Most bidirectional flows are already assembled internally and are considered a single flow. The flow records reported by NSEL on the ASAs 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. In addition, some NSEL records include two byte counter fields, NF_F_FWD_FLOW_DELTA_BYTES and NF_F_REV_FLOW_DELTA_BYTES, which provide direction-specific traffic data.

Template Updates

RFC 3954, Cisco Systems NetFlow Services Export Version 9, 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.

Observation Point and Observation Domain

The ASA 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. Flow that are created by external devices that connect to the ASA are also exported.

Flow Filtering

Only records for certain flows may need to be exported, For example, the ASA 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.

Data Fields

The following table lists the data elements that are exported from the ASAs through NSEL. 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.

Note NetFlow uses IFC SNMP IF index to report the interface which is based on vpifNum. But, vpifnum does not have a valid value for identity interfaces. Hence, from ASA version 8.0, for exported NetFlow records, interface identity number is displayed as 65535.

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 ASA
- DESC—A description of what the field type represents

Table 2: 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

ID	TYPE	LEN	DESC
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
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 (L3 IPv4)			
NF_F_XLATE_SRC_ADDR_IPV4	225	4	Post NAT Source IPv4 Address
NF_F_XLATE_DST_ADDR_IPV4	226	4	Post NAT Destination IPv4 Address
NF_F_XLATE_SRC_PORT	227	2	Post NATT Source Transport Port
NF_F_XLATE_DST_PORT	228	2	Post NATT Destination Transport Port
Mapped Flow ID Fields (L3 IPv6)			
NF_F_XLATE_SRC_ADDR_IPV6	281	16	Post NAT Source IPv6 Address
NF_F_XLATE_DST_ADDR_IPV6	282	16	Post NAT Destination IPv6 Address
Status or Event Fields			
NF_F_FW_EVENT	233	1	High-level event code. Values are as follows: • 0—Default (ignore) • 1—Flow created • 2—Flow deleted • 3—Flow denied • 4—Flow alert • 5—Flow update
NF_F_FW_EXT_EVENT	33002	2	Extended event code. These values provide additional information about the event.
Timestamp and Statistics Fields			

ID	TYPE	LEN	DESC
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_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.
NF_F_FWD_FLOW_DELTA_BYTES	231	4	The delta number of bytes from source to destination.
NF_F_REV_FLOW_DELTA_BYTES	232	4	The delta number of bytes from destination to source.
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: • 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
AAA Fields			
NF_F_USERNAME	40000	20	AAA username
NF_F_USERNAME_MAX	40000	65	AAA username of maximum permitted size

Event ID Field

The Event ID field describes the event that resulted in the NSEL record. The following table lists the values for event IDs.

Table 3: Values for Event IDs

Event ID	Description
0	Ignore—This value indicates that a field must be ignored and 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.
5	Flow updated—This value indicates that a flow timer went off or a flow was torn down.

Extended Event ID Field

The extended event ID provides additional information about a particular event. This field includes a product-specific field ID (33002). The following table lists the values for extended event IDs.

Table 4: 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	Possible reasons include the following: • An attempt to connect to the ASA interface was denied. • The ICMP packet to the device was denied. • The ICMPv6 packet to the device was denied.
1004	Flow denied	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.

Flow Deleted Extended Event IDs (2000+)

The following table explains the various flow deleted extended event IDs, whose values are 2000 and above.

Table 5: Flow Deleted Extended Event IDs (2000+)

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2001	NP_FLOW_TUNNEL_TORN_DOWN Tunnel has been torn down. This counter will increment when the appliance receives a packet associated with an established flow whose IPSec security association is in the process of being deleted. **Recommendation:** This is a normal condition when the IPSec tunnel is torn down for any reason.	None
2002	NP_FLOW_NO_IPV6_IPSEC IPSec over IPv6 unsupported. This counter will increment when the appliance receives an IPSec ESP packet, IPSec NAT-T ESP packet or an IPSec over UDP ESP packet encapsulated in an IP version 6 header. The appliance does not currently support any IPSec sessions encapsulated in IP version 6. **Recommendation:** None	None
2003	NP_FLOW_TUNNEL_PENDING Tunnel being brought up or torn down. This counter will increment when the appliance receives a packet matching an entry in the security policy database (i.e. crypto map) but the security association is in the process of being negotiated; its not complete yet. This counter will also increment when the appliance receives a packet matching an entry in the security policy database but the security association has been or is in the process of being deleted. The difference between this indication and the 'Tunnel has been torn down' indication is that the 'Tunnel has been torn down' indication is for established flows. **Recommendation:** This is a normal condition when the IPSec tunnel is in the process of being negotiated or deleted.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2004	NP_FLOW_NEED_IKE Need to start IKE negotiation. This counter will increment when the appliance receives a packet that requires encryption but has no established IPSec security association. This is generally a normal condition for LAN-to-LAN IPSec configurations. This indication will cause the appliance to begin ISAKMP negotiations with the destination peer. **Recommendation:** If you have configured IPSec LAN-to-LAN on your appliance, this indication is normal and does not indicate a problem. However, if this counter increments rapidly it may indicate a crypto configuration error or network error preventing the ISAKMP negotiation from completing. Verify that you can communicate with the destination peer and verify your crypto configuration using the **show running-config** command.	None
2005	NP_FLOW_VPN_HANDLE_ERROR VPN handle error. This counter is incremented when the appliance is unable to create a VPN handle because the VPN handle already exists. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of VPN-based applications, then this may be caused by a software defect. Use the following commands to gather more information about this counter and contact the Cisco TAC to investigate the issue further. **capture** *name***type asp-drop vpn-handle-error** **show asp table classify crypto** **show asp table vpn-context detail**	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2006	NP_FLOW_VPN_HANDLE_NOT_FOUND VPN handle not found. This counter is incremented when a datagram hits an encrypt or decrypt operation, and no VPN handle is found for the flow the datagram is on. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of VPN-based applications, then this may be caused by a software defect. Use the following commands to gather more information about this counter and contact the Cisco TAC to investigate the issue further. **capture** *name***vpn-handle-not-found** **show asp table classify crypto** **show asp table vpn-context detail**	None
2007	NP_FLOW_IPSEC_SPOOF_DETECT IPSec spoof packet detected. This counter will increment when the appliance receives a packet which should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the appliance but was received unencrypted. This is a security issue. **Recommendation:** Analyze your network traffic to determine the source of the spoofed IPSec traffic.	402117
2008	NP_FLOW_IPSEC_SP_DETUNNEL_FAIL IPsec detunnel processing failed. This counter will increment when a clear text flow fails IPSec tunnel flow processing. **Recommendation:** Use the **show asp drop** command to look at more specific packet drops.	None
2009	NP_FLOW_SVC_SPOOF_DETECT SVC spoof packet detected. This counter will increment when the security appliance receives a packet which should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established SVC connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation:** Analyze your network traffic to determine the source of the spoofed SVC traffic.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2010	NP_FLOW_SOCKET_SVC_FAILOVER An SVC socket connection is being disconnected on the standby unit. This counter is incremented for each new SVC socket connection that is disconnected when the active unit is transitioning into standby state as part of a failover transition. This is part of a normal cleanup of a SVC connection when the current device is transitioning from active to standby. Existing SVC connections on the device are no longer valid and need to be removed. **Recommendation:** None.	None
2011	NP_FLOW_SOCKET_SVC_CONN_REPLACE SVC replacement connection established. This counter is incremented when an SVC connection is replaced by a new connection. **Recommendation:** None. This may indicate that users are having difficulty maintaining connections to the ASA. Users should evaluate the quality of their home network and Internet connection.	722032
2012	NP_FLOW_VPN_SELECTOR_MISMATCH IPSec VPN inner policy selector mismatch detected. This counter is incremented when an IPSec packet is received with an inner IP header that does not match the configured policy for the tunnel. **Recommendation:** Verify that the crypto ACLs for the tunnel are correct and that all acceptable packets are included in the tunnel identity. Verify that the box is not under attack if this message is repeatedly seen.	402116
2013	NP_DROP_FLOW_VPN_EXPIRED Expired VPN context. This counter will increment when the security appliance receives a packet that requires encryption or decryption, and the ASP VPN context required to perform the operation is no longer valid. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2014	NP_DROP_FLOW_VPN_OVERLAP_CONFLICT VPN Network Overlap Conflict. When a packet is decrypted the inner packet is examined against the crypto map configuration. If the packet matches a different crypto map entry than the one it was received on it will be dropped and this counter will increment. A common cause for this is two crypto map entries containing similar/overlapping address spaces. **Recommendation:** Check your VPN configuration for overlapping networks. Verify the order of your crypto maps and use of 'deny' rules in ACLs.	None
2015	NP_DROP_FLOW_VPN_LOCK_ERR IPSec locking error. This counter is incremented when VPN flow cannot be created due to an internal locking error. **Recommendation:** This condition should never be encountered during normal operation and may indicate a software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC) if this error occurs.	None
2016	NP_DROP_FLOW_VPN_RECLASSIFY_FAILED The flow could not be reclassified according to existing VPN policies. When VPN policies change, flows that no longer match those policies are freed as packets arrive for those flows. **Recommendation:** None. This counter is informational and the behavior expected.	None
2017	NP_DROP_FLOW_VPN_MISSING_DECRYPT The flow could not be created because its decryption policy was not available. A VPN flow creation was attempted before its decryption policy was fully initialized. This is a transient condition and will be resolved once the decryption policy completes its installation. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a traffic disruption, then this may be caused by a misconfiguration or a software defect. Use the following commands to gather more information about this counter and contact the Cisco TAC to investigate the issue further. **capture** *name***type asp-drop vpn-missing-decrypt** **show asp table classify** **show asp drop** **show tech-support**	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2018	NP_DROP_FLOW_VPN_BAD_DECRYPT_RULE The flow could not be created because a wrong decryption policy was hit. This is a transient condition when clustering is enabled and vpn-mode is set to distributed. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a traffic disruption, then this may be caused by a misconfiguration or a software defect. Use the following commands to gather more information about this counter and contact the Cisco TAC to investigate the issue further. **show asp drop** **show tech-support**	None
2019	NP_DROP_FLOW_VPN_INVALID_ENCRYPTION_PACKET The flow is dropped because encryption flag was not set. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a traffic disruption, then this may be caused by a misconfiguration or a software defect. Use the following commands to gather more information about this counter and contact the Cisco TAC to investigate the issue further. **show asp drop** **show tech-support**	None
2020	NP_FLOW_OUT_OF_MEMORY No memory to complete flow. This counter is incremented when the appliance is unable to create a flow because of insufficient memory. **Recommendation:** Verify that the appliance is not under attack by checking the current connections. Also verify if the configured timeout values are too large resulting in idle flows residing in memory longer. Check the free memory available by issuing **show memory**. If free memory is low, issue the command **show processes memory** to determine which processes are utilizing most of the memory.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2021	NP_FLOW_PARENT_CLOSED Parent flow is closed. When the parent flow of a subordinating flow is closed, the subordinating flow is also closed. For example, an FTP data flow (subordinating flow) will be closed with this specific reason when its control flow (parent flow) is terminated. This reason is also given when a secondary flow (pin-hole) is closed by its controlling application. For example, when the BYE messaged is received, the SIP inspection engine (controlling application) will close the corresponding SIP RTP flows (secondary flow). **Recommendation:** None.	None
2022	NP_FLOW_CLOSED_BY_FIXUP Flow closed by inspection. This reason is given for closing a flow due to an error detected during application inspection. For example, if an error is detected during inspecting an H323 message, the corresponding H323 flow is closed with this reason. **Recommendation:** None.	None
2023	NP_FLOW_FO_PRIMARY_CLOSED Failover primary closed. Standby unit received a flow delete message from the active unit and terminated the flow. **Recommendation:** If the appliance is running stateful failover, then this counter should increment for every replicated connection that is torn down on the standby appliance.	302014, 302016, 302018
2024	NP_FLOW_FO_STANDBY Flow closed by failover standby. If a through-the-box packet arrives at an appliance or context that is in a Standby state, and a flow is created, the packet is dropped and the flow removed. This counter will increment each time a flow is removed in this manner. **Recommendation:** This counter should never be incrementing on the Active appliance or context. However, it is normal to see it increment on the Standby appliance or context.	302014, 302016, 302018

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2025	NP_FLOW_FO_REP_ERR Standby flow replication error. Standby unit failed to replicate a flow. **Recommendation:** If appliance is processing VPN traffic, then this counter could be constantly increasing on the standby unit because the flow could be replicated before the IKE SA info. No action is required in this case. If the appliance is not processing VPN traffic, then this indicate a software defect. Use the **debug fover fail** command on the standby unit, collect the debug output, and report the problem to Cisco TAC.	302014, 302016, 302018
2026	NP_FLOW_LOOPBACK Flow is a loopback. This reason is given for closing a flow due to the following conditions: 1) when U-turn traffic is present on the flow, and, 2) **same-security-traffic permit intra-interface** is not configured. **Recommendation:** To allow U-turn traffic on an interface, configure the interface with **same-security-traffic permit intra-interface**.	None
2027	NP_FLOW_ACL_DROP Flow is denied by access rule. This counter is incremented when a drop rule is hit by the packet and flow creation is denied. This rule could be a default rule created when the box comes up, when various features are turned on or off, when an ACL is applied to interface or any other feature. Apart from default rule drops, a flow could be denied because of: • ACL configured on an interface • ACL configured for AAA and AAA denied the user. • Through-the-box traffic arriving at a management-only interface. • Unencrypted traffic arriving on an IPsec-enabled interface. • Implicitly deny **ip any any** at the end of an ACL. **Recommendation:** Look for syslog messages related to packet and flow drops.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2028	NP_FLOW_ACL_DROP_RECLASSIFY Flow is denied by access rule after reclassification. This counter is incremented when a drop rule is hit by the packet during reclassification of ACL rules. **Recommendation:** Look for syslog messages related to packet and flow drops.	None
2029	NP_FLOW_PINHOLE_TIMEOUT Pinhole timeout. This counter is incremented to report that the appliance opened a secondary flow, but no packets passed through this flow within the timeout interval, and hence it was removed. An example of a secondary flow is the FTP data channel that is created after successful negotiation on the FTP control channel. **Recommendation:** None.	None
2030	NP_FLOW_HOST_REMOVED Host is removed. Flow removed in response to **clear local-host** command. This is an information counter. **Recommendation:** None.	302014, 302016, 302018, 302021, 305010, 305012, 609002
2031	NP_FLOW_XLATE_REMOVED Xlate Clear. Flow removed in response to a **clear xlate** or **clear local-host** command. This is an information counter. **Recommendation:** None.	302014, 302016, 302018, 302021, 305010, 305012, 609002
2032	NP_FLOW_TIMEOUT Connection timeout. This counter is incremented when a flow is closed because of the expiration of its inactivity timer. **Recommendation:** None.	302014, 302016, 302018, 302021
2033	NP_FLOW_CONN_LIMIT_EXCEEDED Connection limit exceeded. This reason is given for closing a flow when the connection limit has been exceeded. The connection limit is configured using the **set connection conn-max** command. **Recommendation:** None.	201011

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2034	NP_FLOW_TCP_FINS TCP FINs. This reason is given for closing a TCP flow when TCP FIN packets are received. This counter will increment for each TCP connection that is terminated normally with FINs. **Recommendation:** None.	302014
2035	NP_FLOW_SYN_TIMEOUT SYN Timeout. This reason is given for closing a TCP flow due to expiry of the embryonic connection timer. **Recommendation:** If these are valid sessions that take longer to establish a connection, increase the embryonic timeout.	302014
2036	NP_FLOW_FIN_TIMEOUT FIN Timeout. This reason is given for closing a TCP flow due to expiry of the half-closed connection timer. **Recommendation:** If these are valid sessions that take longer to close a TCP flow, increase the half-closed timeout.	302014
2037	NP_FLOW_RESET_IN TCP Reset-I. This reason is given for closing an outbound flow (from a low-security interface to a same- or high-security interface) when a TCP reset is received on the flow. **Recommendation:** None.	302014
2038	NP_FLOW_RESET_OUT TCP Reset-O. This reason is given for closing an inbound flow (from a high-security interface to low-security interface) when a TCP reset is received on the flow. **Recommendation:** None.	302014
2039	NP_FLOW_RESET_APPLIANCE TCP Reset-APPLIANCE. This reason is given for closing a flow when a TCP reset is generated by the appliance. **Recommendation:** None.	302014

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2040	NP_FLOW_RECURSE Close recursive flow. A flow was recursively freed. This reason applies to pair flows, multicast subordinate flows, and syslog flows to prevent syslogs being issued for each of these subordinate flows. **Recommendation:** None.	None
2041	NP_FLOW_PROXY_SERVER_NOT_RESPOND TCP intercept, no response from server. SYN retransmission timeout after trying three times, once every second. Server unreachable, tearing down connection. **Recommendation:** Check if the server is reachable from the ASA.	None
2042	NP_FLOW_PROXY_UNEXPECTED TCP intercept unexpected state. Logic error in TCP intercept module, this should never happen. **Recommendation:** This indicates memory corruption or some other logic error in the TCP intercept module.	None
2043	NP_FLOW_TCPNORM_REXMIT_BAD TCP bad retransmission. This reason is given for closing a TCP flow when the check-retranmission feature is enabled and the TCP endpoint sent a retransmission with different data from the original packet. **Recommendation:** The TCP endpoint might be attacking by sending different data in TCP retransmits. Please use the packet capture feature to learn more about the origin of the packet.	302014
2044	NP_FLOW_TCPNORM_WIN_VARIATION TCP unexpected window size variation. This reason is given for closing a TCP flow when the window size advertized by the TCP endpoint is drastically changed without accepting that much data. **Recommendation:** In order to allow this connection, use the window-variation configuration under tcp-map.	302014

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2045	NP_FLOW_TCPNORM_INVALID_SYN TCP invalid SYN. This reason is given for closing a TCP flow when the SYN packet is invalid. **Recommendation:** The SYN packet could be invalid for a number of reasons, like invalid checksum or invalid TCP header. Please use the packet capture feature to understand why the SYN packet is invalid. If you would like to allow these connections, use the tcp-map configurations to bypass checks.	302014
2046	NP_FLOW_SCTP_DROP_INIT_0_TAG SCTP INIT contains 0 value initiate tag. This counter is incremented and the flow is dropped when an SCTP INIT chunk contains 0 value initiate tag. **Recommendation:** None.	None
2047	NP_FLOW_SCTP_DROP_INITACK_0_TAG SCTP INIT ACK contains 0 value initiate tag. This counter is incremented and the flow is dropped when an SCTP INIT ACK chunk contains 0 value initiate tag. **Recommendation:** None.	None
2048	NP_FLOW_SCTP_DROP_INIT_0_STREAM_CNT SCTP INIT contains 0 value inbound/outbound stream count. This counter is incremented and the packet is dropped when an SCTP INIT chunk contains 0 value inbound/outbound stream count. **Recommendation:** None.	None
2049	NP_FLOW_SCTP_DROP_INIT_TIMEOUT SCTP INIT timed out (not receiving INIT ACK). This counter is incremented and the flow is dropped when an SCTP INIT chunk timeout count reaches the limit. **Recommendation:** This drop can happen in a scenarios like when the receiver of the INIT chunk is not responding INIT ACK or there could be a redundant path between the client and server where the INIT goes in one path and the INIT ACK comes in another path. If this error occurs in large numbers, please use packet capture to help isolate the issue.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2050	NP_FLOW_SCTP_DROP_COOKIE_TIMEOUT SCTP cookie timed out. This counter is incremented and the flow is dropped when the SCTP cookie state (after received INIT ACK or COOKIE ECHO) timeout count reaches the limit. **Recommendation:** None.	None
2051	NP_FLOW_SCTP_DROP_ENDPOINT_ABORT SCTP received ABORT from endpoint. This counter is incremented and the flow is dropped when the SCTP ABORT chunk is received. **Recommendation:** None.	None
2052	NP_FLOW_SCTP_DROP_INITACK_0_STREAM_CNT SCTP INIT ACK contains 0 value inbound/outbound stream count. This counter is incremented and the packet is dropped when an SCTP INIT ACK chunk contains 0 value inbound/outbound stream count. **Recommendation:** None.	None
2053	NP_FLOW_SCTP_DROP_SHUTDOWN_TIMEOUT SCTP SHUTDOWN timed out (not receiving SHUTDOWN ACK). This counter is incremented and the flow is dropped when the SCTP SHUTDOWN timeout count reaches the limit. **Recommendation:** None.	None
2054	NP_FLOW_MCAST_INTRF_REMOVED Multicast interface removed. An output interface has been removed from the multicast entry, or all output interfaces have been removed from the multicast entry. **Recommendation:** No action required if you simply removed an interface. If you remove all output interfaces, verify that there are no longer any receivers for this group.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2055	NP_FLOW_MCAST_ENTRY_REMOVED Multicast entry removed. One of the following: • A packet has arrived that matches a multicast flow, but the multicast service is no longer enabled, or was re-enabled after the flow was built. **Recommendation:** Reenable multicast if it is disabled. • The multicast entry has been deleted so the flow is being cleaned up, but the packet will be reinjected into the data path. **Recommendation:** No action required.	None
2056	NP_FLOW_KILLED_BY_TCP_INTERCEPT Flow terminated by TCP Intercept. TCP intercept would tear down a connection if this is the first SYN, a connection is created for the SYN, and TCP intercept replied with a SYN cookie, or after seeing a valid ACK from the client, when TCP intercept sends a SYN to the server, the server replies with a RST. **Recommendation:** TCP intercept normally does not create a connection for the first SYN, except when there are nailed rules or the packet comes over a VPN tunnel or the next hop gateway address to reach the client is not resolved. So for the first SYN this indicates that a connection got created. When TCP intercept receives a RST from server, its likely the corresponding port is closed on the server.	None
2057	NP_FLOW_AUDIT_FAILURE Audit failure. A flow was freed after matching an **ip audit** signature that had reset as the associated action. **Recommendation:** If removing the flow is not the desired outcome of matching this signature, then remove the reset action from the **ip audit** command.	None
2058	NP_FLOW_CX_REQUEST Flow terminated by CXSC. This reason is given for terminating a flow as requested by the CXSC module. **Recommendation:** Check syslogs and alerts on the CXSC module.	429002

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2059	NP_FLOW_CX_FAIL_CLOSE CXSC fail-close. This reason is given for terminating a flow since the CXSC card is down and the fail-close option was used with the CXSC action. **Recommendation:** Check and bring up the CXSC module.	429001
2060	NP_FLOW_CX_BAD_HDL Flow terminated by ASA due to bad handle from CX. Since the handle received from CX is invalid, the flow is dropped. **Recommendation:** Check syslogs and alerts on the CXSC module.	421004
2061	NP_FLOW_RESET_BY_CX Flow reset by CXSC. This reason is given for terminating a TCP flow as requested by the CXSC module. **Recommendation:** Check syslogs and alerts on the CXSC module.	429003
2062	NP_FLOW_SFR_REQUEST Flow terminated by SFR. This reason is given for terminating a flow as requested by the ASA FirePOWER module. **Recommendation:** Check syslogs and alerts on the ASA FirePOWER module.	434002
2063	NP_FLOW_SFR_FAIL_CLOSE SFR fail-close. This reason is given for terminating a flow because the ASA FirePOWER module is down and the fail-close option was used with the SFR action. **Recommendation:** Check and bring up the ASA FirePOWER module.	434001
2064	NP_FLOW_SFR_BAD_HDL Flow terminated by ASA due to bad handle from SFR. Since the handle received from ASA FirePOWER is invalid, dropping flow. **Recommendation:** Check syslogs and alerts on the ASA FirePOWER module.	421004

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2065	NP_FLOW_RESET_BY_SFR Flow reset by SFR. This reason is given for terminating a TCP flow as requested by the ASA FirePOWER module. **Recommendation:** Check syslogs and alerts on the ASA FirePOWER module.	434003
2066	NP_FLOW_SNORT_FLOW_DROP Flow terminated by SNORT. This reason is given for terminating a flow as requested by the Snort module. **Recommendation:** Review Snort policies for any such rule denying the flow.	None
2067	NP_FLOW_IDS_REQUEST Flow terminated by IPS. This reason is given for terminating a flow as requested by IPS module. **Recommendation:** Check syslogs and alerts on the IPS module.	420002
2068	NP_FLOW_IDS_FAIL_CLOSE IPS fail-close. This reason is given for terminating a flow because the IPS module is down and the fail-close option was used with the IPS inspection. **Recommendation:** Check and bring up the IPS module.	420001
2069	NP_FLOW_IDS_LICENSE_FAIL_CLOSE IPS module license disabled. This reason is given for terminating a flow when the IPS module license is disabled and the fail-close option was used in IPS inspection. **Recommendation:** Please apply an activiation key that has the IPS Module License enabled.	420008

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2070	NP_FLOW_REINJECT_PUNT Flow terminated by punt action. This counter is incremented when a packet is punted to the exception-path for processing by one of the enhanced services such as inspection or AAA, and the servicing routine, having detected a violation in the traffic flowing on the flow, requests that the flow be dropped. The flow is immediately dropped. **Recommendation:** Please watch for syslogs issued by the servicing routine for more information. Flow drop terminates the corresponding connection.	None
2071	NP_FLOW_SHUNNED Flow shunned. This counter will increment when a packet is received that has a source IP address that matches a host in the shun database. When a **shun** command is applied, it will be incremented for each existing flow that matches the **shun** command. **Recommendation:** None.	401004
2072	NP_FLOW_HOSTLIMIT Flow host limit. **Recommendation:** None.	None.
2073	NP_FLOW_NAT_FAILED NAT failed. Failed to create an xlate to translate an IP or transport header. **Recommendation:** If NAT is not wanted, disable the NAT commands. Otherwise, configure a NAT rule for the dropped flow.	305005, 305006, 305009, 305010, 305011, 305012
2074	NP_FLOW_NAT_RPF_FAILED NAT reverse path failed. Rejected attempt to connect to a translated host using the translated host's real address. **Recommendation:** When not on the same interface as the host undergoing NAT, use the mapped address instead of the real address to connect to the host. Also, enable the appropriate inspect command if the application embeds IP address.	305005

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2075	NP_FLOW_INSPECT_FAIL Inspection failure. This counter will increment when the appliance fails to enable protocol inspection carried out by the NP for the connection. The cause could be memory allocation failure, or for ICMP error message, the appliance not being able to find any established connection related to the frame embedded in the ICMP error message. **Recommendation:** Check system memory usage. For ICMP error message, if the cause is an attack, you can deny the host using the ACLs.	313004
2076	NP_FLOW_NO_INSPECT Failed to allocate inspection. This counter will increment when the security appliance fails to allocate a run-time inspection data structure upon connection creation. The connection will be dropped. **Recommendation:** This error condition is caused when the security appliance runs out of system memory. Please check the current available free memory by executing the **show memory** command.	None
2077	NP_FLOW_RESET_BY_IDS Flow reset by IPS. This reason is given for terminating a TCP flow as requested by the IPS module. **Recommendation:** Check syslogs and alerts on the IPS module.	420003

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2078	NP_FLOW_RECLAIMED Non-tcp/udp flow reclaimed for new request. This counter is incremented when a reclaimable flow is removed to make room for a new flow. This occurs only when the number of flows through the appliance equals the maximum number permitted by the software imposed limit, and a new flow request is received. When this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels permitted by the appliance, then the oldest reclaimable flow is removed to make room for the new flow. All flows except the following are deemed to be reclaimable: • TCP, UDP, GRE and Failover flows • ICMP flows if ICMP stateful inspection is enabled • ESP flows to the appliance **Recommendation:** No action is required if this counter is incrementing slowly. If this counter is incrementing rapidly, it could mean that the appliance is under attack and the appliance is spending more time reclaiming and rebuilding flows.	302021
2079	NP_FLOW_NON_TCP_SYN non-syn TCP. This reason is given for terminating a TCP flow when the first packet is not a SYN packet. **Recommendation:** None.	None
2080	NP_FLOW_RM_XLATE_LIMIT RM xlate limit reached. This counter is incremented when the maximum number of xlates for a context or the system has been reached and a new connection is attempted. **Recommendation:** Use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and denied counts and adjust resource limits if desired.	321001
2081	NP_FLOW_RM_HOST_LIMIT RM host limit reached. This counter is incremented when the maximum number of hosts for a context or the system has been reached and a new connection is attempted. **Recommendation:** Use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and denied counts and adjust resource limits if desired.	321001

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2082	NP_FLOW_RM_INSPECT_RATE_LIMIT RM inspect rate limit reached. This counter is incremented when the maximum inspection rate for a context or the system has been reached and a new connection is attempted. **Recommendation:** Use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and denied counts and adjust resource limits if desired.	321002
2083	NP_FLOW_TCPMOD_CONNECT_CLASHED TCP module port collision between client and server. A self-sourced TCP connection uses a port that conflicted with an existing listen server's port. **Recommendation:** If non-zero, this counter indicates a system-consistency check has failed. Please contact the TAC.	None
2084	NP_FLOW_SSM_APP_REQUEST Flow terminated by service module. This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when the application running on the SSM requests the security appliance to terminate a connection. **Recommendation:** You can obtain more information by querying the incident report or system messages generated by the SSM itself. Please consult the documentation that comes with the SSM for instructions.	None
2085	NP_FLOW_SSM_APP_FAIL Service module failed. This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when a connection that is being inspected by the SSM is terminated because the SSM has failed. **Recommendation:** The card manager process running in the security appliance control plane issued system messages and CLI warning to inform you of the failure. Please consult the documentation that comes with the SSM to trouble shoot the SSM failure.	421001

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2086	NP_FLOW_SSM_APP_INCOMPETENT Service module incompetent. This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when a connection is supposed to be inspected by the SSM, but the SSM is not able to inspect it. This counter is reserved for future use: it should always be 0. **Recommendation:** None.	None
2087	NP_FLOW_SSL_BAD_RECORD SSL bad record detected. This counter is incremented for each unknown SSL record type received from the remote peer. Any unknown record type received from the peer is treated as a fatal error and the SSL connections that encounter this error must be terminated. **Recommendation:** It is not normal to see this counter increment at any time. If this counter is incremented, it usually means that the SSL protocol state is out of sync with the client software. The most likely cause of this problem is a software defect in the client software. Contact the Cisco TAC with the client software or web browser version and provide a network trace of the SSL data exchange to troubleshoot this problem.	None
2088	NP_FLOW_SSL_HANDSHAKE_FAILED SSL handshake failed. This counter is incremented when the TCP connection is dropped because the SSL handshake failed. **Recommendation:** This is to indicate that the TCP connection is dropped because the SSL handshake failed. If the problem cannot be resolved based on the syslog information generated by the handshake failure condition, please include the related syslog information when contacting the Cisco TAC.	725006, 725014
2089	NP_FLOW_DTLS_HELLO_CLOSE DTLS hello close. This counter is incremented when the UDP connection is dropped after the DTLS client hello message processing is finished. This does not indicate an error. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2090	NP_FLOW_SSL_MALLOC_ERROR SSL malloc error. This counter is incremented for each malloc failure that occurs in the SSL lib. This is to indicate that SSL encountered a low memory condition where it cannot allocate a memory buffer or packet block. **Recommendation:** Check the security appliance memory and packet block condition and contact Cisco TAC.	None
2091	NP_FLOW_DROP_SEND_CTM_ERROR CTM crypto request error. This counter is incremented each time CTM cannot accept our crypto request. This usually means the crypto hardware request queue is full. **Recommendation:** Issue the **show crypto protocol statistics ssl** command and contact the Cisco TAC.	None
2092	NP_FLOW_DROP_SSL_DECRYPT_ERROR SSL record decryption failed. This counter is incremented when a decryption error occurs during SSL data receive. This usually means that there is a bug in the SSL code of the ASA or peer, or an attacker may be modifying the data stream. The SSL connection has been closed. **Recommendation:** Investigate the SSL data streams to and from your ASA. If there is no attacker, then this indicates a software error that should be reported to the Cisco TAC.	None
2093	NP_FLOW_SOCKET_NOT_ACCEPTED A new socket connection was not accepted. This counter is incremented for each new socket connection that is not accepted by the security appliance. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of socket-based applications, then this may be caused by a software defect. Contact the Cisco TAC to investigate the issue further.	None
2094	NP_FLOW_SOCKET_FAILURE NP socket failure. This is a general counter for critical socket processing errors. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2095	NP_FLOW_SOCKET_RELAY_FAILURE NP socket relay failure. This is a general counter for socket relay processing errors. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of socket-based applications, then this may be caused by a software defect. Contact the Cisco TAC to investigate the issue further.	None
2096	NP_FLOW_SOCKET_DATA_MOVE_FAILED NP socket data movement failure. This counter is incremented for socket data movement errors. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None
2097	NP_FLOW_SOCKET_NEW_CONN_FAILED NP socket new connection failure. This counter is incremented for new socket connection failures. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None
2098	NP_FLOW_SOCKET_TRANSP_CLOSED NP socket transport closed. This counter is incremented when the transport attached to the socket is abruptly closed. **Recommendation:** It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of socket-based applications, then this may be caused by a software defect. Contact the Cisco TAC to investigate the issue further.	None
2099	NP_FLOW_SOCKET_BLK_CONV_FAILED NP socket block conversion failure. This counter is incremented for socket block conversion failures. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2100	NP_FLOW_SSL_ALERT SSL received close alert. This counter is incremented each time the security appliance receives a close alert from the remote client. This indicates that the client has notified us they are going to drop the connection. It is part of the normal disconnect process. **Recommendation:** None.	725007
2101	NP_FLOW_CHILDREN_LIMIT Max per-flow children limit exceeded. The number of children flows associated with one parent flow exceeds the internal limit of 200. **Recommendation:** This message indicates either a misbehaving application or an active attempt to exhaust the firewall memory. Use the **set connection per-client-max** command to further fine tune the limit. For FTP, additionally enable the **strict** option in **inspect ftp**.	210005
2102	NP_FLOW_TRACER_DROP packet-tracer traced flow drop. This counter is internally used by packet-tracer for flow freed once tracing is complete. **Recommendation:** None.	None
2103	NP_FLOW_SP_LOOPING_ADDRESS looping-address. This counter is incremented when the source and destination addresses in a flow are the same. SIP flows where address privacy is enabled are excluded, as it is normal for those flows to have the same source and destination address. **Recommendation:** There are two possible conditions when this counter will increment. One is when the appliance receives a packet with the source address equal to the destination. This represents a type of DoS attack. The second is when the NAT configuration of the appliance NATs a source address to equal that of the destination. Examine syslog message 106017 to determine what IP address is causing the counter to increment, then enable packet captures to capture the offending packet, and perform additional analysis.	106017
2104	NP_FLOW_FP_DROP_NO_ADJACENCY No valid adjacency. This counter will increment when the security appliance receives a packet on an existing flow that no longer has a valid output adjacency. This can occur if the next hop is no longer reachable or if a routing change has occurred, typically in a dynamic routing environment. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2105	NP_FLOW_MIDPATH_SERVICE_FAILURE NP midpath service failure. This is a general counter for critical midpath service errors. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None
2106	NP_FLOW_MIDPATH_CP_EVENT_FAILURE NP midpath CP event failure. This is a counter for critical midpath events that could not be sent to the CP. **Recommendation:** This indicates that a software error should be reported to the Cisco TAC.	None
2107	NP_FLOW_CONTEXT_REMOVED NP virtual context removed. This counter is incremented when the virtual context with which the flow is going to be associated has been removed. This could happen in a multi-core environment when one CPU core is in the process of destroying the virtual context, and another CPU core tries to create a flow in the context. **Recommendation:** None.	None
2108	NP_FLOW_FAILOVER_IDLE_TIMEOUT Flow removed from standby unit due to idle timeout. A flow is considered idle if the standby unit no longer receives periodic updates from the active unit, which is supposed to happen to at fixed internal when flow is alive. This counter is incremented when the flow is removed from standby unit. **Recommendation:** None.	None
2109	NP_FLOW_L4TM_BLACKLIST Flow matched dynamic-filter blacklist. A flow matched a dynamic-filter blacklist or greylist entry with a threat-level higher than the threat-level threshold configured to drop traffic. **Recommendation:** Use the internal IP address to trace the infected host. Take remediation steps to remove the infection.	None
2110	NP_FLOW_ASA_TEARDOWN ASA requested flow to be torn down. ASA requested the flow to be removed. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2111	NP_FLOW_PDTS_PUNT_DROP No. of segments queued to an inspector reached limit. For this flow, the number of packets queued to the inspector reached the limit. Thus, terminating the flow. **Recommendation:** None.	None
2112	NP_FLOW_DROP_PDTS_RULE_META_FAILED PDTS rule-meta allocation failed. This counter is incremented when rule-meta allocation failed, thus terminating the flow. **Recommendation:** None.	None
2113	NP_FLOW_TCP_FULL_PROXY_REQD Full TCP proxy is required, but not available in monitor-only mode. This flow requires full TCP proxy, but this feature is not available in monitor-only mode. **Recommendation:** None.	None
2114	NP_FLOW_ROUTE_CHANGE Flow terminated due to route change. When the system adds a lower cost (better metric) route, incoming packets that match the new route will cause their existing connection to be torn down after the user configured timeout (floating-conn) value. Subsequent packets will rebuild the connection out the interface with the better metric. **Recommendation:** To prevent the addition of lower cost routes from affecting active flows, the floating-conn configuration timeout value can be set to 0:0:0.	None
2115	NP_FLOW_SVC_SELECTOR_MISMATCH SVC VPN inner policy selector mismatch detected. This counter is incremented when an SVC packet is received with an inner IP header that does not match the policy for the tunnel. **Recommendation:** None.	None
2116	NP_FLOW_VPATH_LICENSE_FAILURE Flow terminated due to vPath license failure. The flow is dropped due to licensing failure for ASA 1000V. **Recommendation:** Check Nexus 1000V and verify that there are sufficient ASA 1000V licenses installed to support all ASA 1000V virtual machines in use.	4450002

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2117	NP_FLOW_SVC_CONN_TIMER_CB_FAIL SVC connection timer callback failure. This condition occurs when there is a failed attempt to place an event on the async lock queue for that connection. **Recommendation:** None.	None
2118	NP_FLOW_SVC_UDP_CONN_TIMER_CB_FAIL SVC UDP connection timer callback failure. This condition occurs when there is a failed attempt to place an event on the async lock queue for that connection. **Recommendation:** None.	None
2119	NP_FLOW_NAT64_OR_NAT46_CONVERSION_FAIL IPv6 to IPv4 or vice-verse conversion failure. This condition occurs when there is a failure in conversion of IPv6 traffic to IPv4 or vice-verse. **Recommendation:** None.	None
2120	NP_FLOW_CLUSTER_CFLOW_CLU_OWNER_CLOSED Cluster flow with CLU closed on owner. Director/backup unit received a cluster flow clu delete message from the owner unit and terminated the flow. This counter should increment for every replicated CLU that is torn down on the owner unit. **Recommendation:** None.	None
2121	NP_FLOW_CLUSTER_CFLOW_STALE_CLU_CLOSED Cluster flow with CLU removed due to stale owner. A cluster flow was removed because it has stale owner information. Stale information can happen due to missing CLU_DELETE as normally this is not a reliable message. **Recommendation:** None.	None
2122	NP_FLOW_CLUSTER_CFLOW_CLU_TIMEOUT Cluster flow with CLU removed from due to idle timeout. A cluster flow with CLU is considered idle if director/backup unit no longer receives periodic updates from owner, which is supposed to happen at fixed intervals when a flow is alive. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2123	NP_FLOW_CLUSTER_REDIRECT Flow matched a cluster redirect classify rule. A stub forwarding flow will thereafter forward packets to the cluster unit that owns the flow. This counter is informational and the behavior is expected. The packet was forwarded to the owner over the Cluster Control Link. **Recommendation:** None.	None
2124	NP_FLOW_CLUSTER_DROP_ON_SLAVE Flow matched a cluster drop-on-slave classify rule. This is for cases that the packets from a level-3 subnet are seen by all units and only the master unit needs to process them. This counter is informational and the behavior expected. **Recommendation:** None.	None
2125	NP_FLOW_CLUSTER_DIR_CHANGE The flow director changed due to a cluster join event. A new unit joined the cluster and is now the director for the flow. The old director/backup has removed its flow and the flow owner will update the new director. This counter is informational and the behavior expected. **Recommendation:** None.	None
2126	NP_FLOW_CLUSTER_MCAST_OWNER_CHANGE The multicast flow owner changed due to a cluster join or leave event. The flow gets created on a new owner unit. This counter is informational and the behavior expected. **Recommendation:** None.	None
2127	NP_FLOW_CLUSTER_CONVERT_TO_DIR_OR_BAK Forwarding or redirect flow converted to director or backup flow. Forwarding or redirect flow is removed, so that director or backup flow can be created. This counter is informational and the behavior expected. **Recommendation:** None.	None
2128	NP_FLOW_CLUSTER_MOBILITY_OWNER_REMOVED Flow mobility has old owner removed. Flow mobility moved this flow to another unit. The old owner will be removed. This counter is informational and the behavior expected. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2129	NP_FLOW_CLUSTER_MOBILITY_FWDER_REMOVED Flow mobility has old forwarder removed. Flow mobility moved this flow to another unit. This old forwarder will be removed because its turning into a backup. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2130	NP_FLOW_CLUSTER_MOBILITY_BACKUP_REMOVED Flow mobility has backup removed. Flow mobility moved this flow to another unit. This backup will be removed because the new owner and director are on difference nodes. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2131	NP_FLOW_CLUSTER_MOBILITY_OWNER_2_DIR Flow mobility has old owner/director changed to director only. Flow mobility moved this flow to another unit. This unit used to be both owner and director, now will host director flow only. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2132	NP_FLOW_SCANSAFE_SERVER_NOT_REACHABLE Scansafe server is not configured or the cloud is down. Either the scansafe server IP is not specified in the scansafe \ general options or the scansafe server is not reachable. **Recommendation:** Cloud Web Security is no longer supported.	None
2133	NP_FLOW_REMOVED_BY_CLU_ADD_FORCE Another owner overrides me, and I will become a director later. Another unit owns the flow, and asks me to delete my flow in order to create a director flow in its place later. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2134	NP_FLOW_REMOVED_BY_CLU_FWD_FORCE Another owner overrides me, and I will become a forwarder later. Another unit owns the flow, and asks me to delete my flow in order to create a forwarder flow in its place later. This counter is informational and the behavior is expected. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2135	NP_FLOW_REMOVED_DIRECTOR_CLOSED The flow is removed and the director is closed. **Recommendation:** None.	None
2136	NP_FLOW_PINHOLE_MASTER_CHANGE Master only pinhole flow removed at bulk sync due to master change. This counter is informational and the behavior is expected. **Recommendation:** None.	302014
2137	NP_FLOW_PARENT_OWNER_LEFT Flow removed at bulk sync because parent flow is gone. Flow is removed during bulk sync because the parent flow's owner has left the cluster. This counter is informational and the behavior is expected. **Recommendation:** None.	302014
2138	NP_FLOW_CLUSTER_CTP_PUNT_CHANNEL_MISSING Flow removed at bulk sync because CTP punt channel is missing. Flow is removed during bulk sync because CTP punt channel is missing in cluster restored flow. **Recommendation:** The cluster master may have just left the cluster. And there might be packet drops on the Cluster Control Link.	302014
2139	NP_FLOW_DROP_INVALID_VNID Invalid VXLAN segment-id. This counter is incremented when the security appliance sees an invalid VXLAN segment-id attached to a flow. **Recommendation:** None.	None
2140	NP_FLOW_DROP_NO_VALID_NVE_IFC No valid NVE interface. This counter is incremented when the security appliance fails to identify the NVE interface of a VNI interface for a flow. **Recommendation:** Verify that the NVE is configured for all interfaces.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2141	NP_FLOW_DROP_INVALID_PEER_NVE Invalid peer NVE. This counter is incremented when the security appliance fails to get the IP and MAC address of a peer NVE for a flow. **Recommendation:** Verify that the peer NVE is configured or learned for the NVE.	None
2142	NP_FLOW_DROP_VXLAN_ENCAP_ERROR Fail to encap with VXLAN. This counter is incremented when the security appliance fails to encapsulate a packet with VXLAN for a flow. **Recommendation:** None.	None
2143	NP_FLOW_DROP_NO_ROUTE_TO_PEER_NVE No route to peer NVE. This counter is incremented when the security appliance fails to locate the next hop to the peer NVE. **Recommendation:** Verify the peer NVE is reachable through the source-interface.	None
2144	NP_FLOW_DROP_INVALID_VNI_MCAST_IP Invalid Multicast IP on VNI interface. This counter is incremented when the security appliance fails to get the multicast group IP from the VNI interface. **Recommendation:** Verify that in the absence of a configured peer NVE, the VNI interface has a valid multicast group IP configured on it.	None
2145	NP_FLOW_DROP_MISSING_PEER_VTEP_IP Peer VTEP IP not found. This counter is incremented when the security appliance fails to find the peer VTEP IP for an inner destination IP for VXLAN encapsulation. **Recommendation:** Verify that in **show arp vtep-mapping**, **show mac-address-table vtep-mapping**, **show ipv6 neighbor vtep-mapping** output, the VTEP IP is present for the desired remote inner host.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2146	NP_FLOW_IFC_ZN_CHG Interface experienced a zone change. This reason is given for terminating a flow because the parent interface has joined or left a zone. **Recommendation:** None.	302014, 302016, 302018, 302021, 302304
2147	NP_FLOW_DROP_PDTS_SNORT_INFO_MISSING Snort inspected flow missing pdts snort info. This reason is given for terminating a flow because the connection lacks Snort related structure. **Recommendation:** None.	None
2148	NP_FLOW_IFC_VRF_CHG Interface experienced a VRF change. This reason is given for terminating a flow because the parent interface has moved from one VRF to another. **Recommendation:** None.	None
2149	NP_FLOW_CLEAN_FOR_VPN_STUB Clean up for creation of a new VPN stub. This reason is given for tearing down a conflicting connection in preparation for a new VPN stub connection. **Recommendation:** None.	None
2150	NP_FLOW_CLUSTER_CFLOW_ISAKMP_OWNER_CLOSED Cluster flow closed on ISAKMP owner. Director/backup unit received an ISAKMP redirected packet from a forwarding unit and terminated the flow. This counter should increment for every cflow torn down by ISAKMP redirected packet on the ISAKMP owner unit. **Recommendation:** None.	None
2151	NP_FLOW_UNABLE_TO_ASSOCIATE_VPN_CONTEXT VPN context association failure. This counter is increased whenever the system fails to associate the VPN context with a cluster flow. **Recommendation:** None.	None

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2152	NP_FLOW_DROP_IKE_PKT_BAD_SPI Flow removed for IKE packet with corrupted or expired SPI. This counter is incremented and the flow is dropped when the IKE packet in this flow gets dropped due to corrupted or expired SPI. **Recommendation:** Check the syslog message to get more information about the origin of the packet. This situation can be normal and transient. If the drops persist, call TAC to investigate further.	753001
2153	NP_FLOW_TEAR_CONN_RETRANSMIT_TIMEOUT Maximum retries of retransmission exceeded. The connection was torn down because the TCP packet exceeded maximum retries of retransmission, no reply from peer, tearing down connection. **Recommendation:** None.	302014
2154	NP_FLOW_PROBE_TEAR_CONN_MAX_RETRANSMITS Probe maximum retries of retransmission exceeded. The connection was torn down because the TCP packet exceeded maximum probe retries of retransmission, no reply from peer, tearing down connection. **Recommendation:** None.	302014
2155	NP_FLOW_PROBE_TEAR_CONN_RETRANSMIT_TIMEOUT Probe maximum retransmission time elapsed. The connection was torn down because the maximum probing time for TCP packet has elapsed, no reply from peer, tearing down connection. **Recommendation:** None.	302014
2156	NP_FLOW_PROBE_TEAR_CONN_RST Probe received RST. The connection was torn down because the probe connection received RST from server, tearing down connection. **Recommendation:** None.	302014
2157	NP_FLOW_PROBE_TEAR_CONN_FIN Probe received FIN. The connection was torn down because the probe connection received FIN from server, tearing down connection. **Recommendation:** None.	302014

Extended Event ID	ENUM Value, Description, and Recommendation	Syslog IDs
2158	NP_FLOW_PROBE_TEAR_CONN_COMPLETE Probe completed. The connection was torn down because the probe connection is successful, tearing down connection. **Recommendation:** None.	302014
2159	NP_FLOW_CLU_REMOVED_DUP_OWNER Duplicated owner flow detected, and I will become a director later. Another unit owns the flow, so I need to delete my flow in order to create a director flow in its place later. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2160	NP_FLOW_CLU_REMOVED_DUP_OWNER_BY_DIR Duplicated owner flow removed by director. Another unit owns the flow, so director deleted the flow on this unit. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2161	NP_FLOW_CLU_REMOVED_STALE_STUB Stale stub flow removed by owner. This is a stale stub flow, so owner deleted the flow on this unit. This counter is informational and the behavior is expected. **Recommendation:** None.	None
2162	NP_FLOW_INVALID_MAP_ADDR_PORT Invalid MAP address/port combination. A packet with an address that matches a MAP (Mapping of Address and Port) domain Basic Mapping Rule has inconsistent encoding or the port number used is not within the allotted range. **Recommendation:** Check MAP BR and CE configurations to ensure they are consistent within the same MAP domain. Note that this can also be caused by a rouge MAP CE that maliciously tries to use an unallotted port.	305019, 305020

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

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

- There are different templates for different events.
- There are different templates for IPv4 and IPv6 flows under each event type.
- There are different templates for IPV44, IPV46, IPV64, and IPV66 flows under each event type.
- The flow creation 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.

  – A common username size for usernames that are less than 20 characters

  – A 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.
- The flow denied and flow deletion events have IPV46 and IPV64 templates in which the destination IP address has been translated by a NAT rule, but the source IP address has not been translated by a NAT rule; this results in different IP versions between the source and destination IP addresses. The source and destination NAT rules are not applied at the same time (the destination NAT rule is applied first), so it is possible for a NetFlow record to be generated before both NAT rules are applied or when only one NAT rule is available.

  These partial NAT translation templates are not needed for flow creation and delayed flow creation events because both source and destination IP addresses need to be the same IP version for a flow to be created.

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 ASA. This event is also a log of flows that the ASA allows. The following table describes the templates to use for flow creation events.

Table 6: Templates for Flow Creation Events

Description	Fields
IPv44 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_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
IPv44 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_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Description	Fields
IPv66 flow creation 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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
IPv66 flow creation 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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Description	Fields
IPv46 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_IPV6, NF_F_XLATE_DST_ADDR_IPV6, 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_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
IPv46 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_IPV6, NF_F_XLATE_DST_ADDR_IPV6, 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_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Description	Fields
IPv64 flow creation 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_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
IPv64 flow creation 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_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_FLOW_CREATE_TIME_MSEC, 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

The following table describes the templates that are used for extended flow-teardown events.

Table 7: Templates for Extended Flow Teardown Events

Description	Fields
Extended IPv44 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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
Extended IPv44 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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX

Description	Fields
Extended IPv66 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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
Extended IPv66 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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
Extended IPv46 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_IPV6, NF_F_XLATE_DST_ADDR_IPV6, 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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME

Description	Fields
Extended IPv46 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_IPV6, NF_F_XLATE_DST_ADDR_IPV6, 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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME_MAX
Extended IPv64 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_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC, NF_F_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID, NF_F_USERNAME
Extended IPv64 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_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_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. The following table describes the templates that are used for flow denied events.

Table 8: Templates for Flow Denied Events

Description	Fields
IPv44 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
IPv66 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_IPV6, NF_F_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_ICMP_CODE_IPV6, 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, no xlate fields present	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_INGRESS_ACL_ID, NF_F_EGRESS_ACL_ID

Description	Fields
IPv46 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_IPV6, NF_F_XLATE_DST_ADDR_IPV6, 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
IPv46 flow denied, no source translation	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_IPV6, 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
IPv64 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_IPV6, NF_F_ICMP_CODE_IPV6, NF_F_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_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
IPv64 flow denied, no source translation	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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_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

Templates for Flow Teardown Events

Flow teardown events indicate that a flow has been terminated. The following table describes the templates that are used for flow teardown events.

Table 9: Templates for Flow Teardown Events

Description	Fields
IPv44 flow teardown	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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv66 flow teardown	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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV6, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC

Description	Fields
IPv46 flow teardown	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_IPV6, NF_F_XLATE_DST_ADDR_IPV6, 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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv46 flow teardown, no source translation	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_IPV6, 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_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC
IPv64 flow teardown	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_XLATE_SRC_ADDR_IPV4, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC

Description	Fields
IPv64 flow teardown, no source translation	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_XLATE_SRC_ADDR_IPV6, NF_F_XLATE_DST_ADDR_IPV4, NF_F_XLATE_SRC_PORT, NF_F_XLATE_DEST_PORT, NF_F_FW_EVENT, NF_F_FW_EXT_EVENT, NF_F_EVENT_TIME_MSEC, NF_F_FWD_FLOW_DELTA_BYTES, NF_F_REV_FLOW_DELTA_BYTES, NF_F_FLOW_CREATE_TIME_MSEC

Templates for Flow Update Events

Flow update events indicate that a flow update timer has gone off for a flow or a flow was torn down. This event functions as a periodic byte counter for flow traffic. Flow update events also use the same templates as flow teardown events, excluding those for partial NAT translation. The NF_F_FWD_FLOW_DELTA_BYTES and NF_F_REV_FLOW_DELTA_BYTES fields contain the byte counts since the last timer interval. The NF_F_FW_EXT_EVENT field is not used and is ignored in flow update records. See Table 8 for the templates that are used for flow teardown events.

Flow Update (at timer) and Flow Update (at teardown) Events

The ASA sets flow update timers for flows passing through it, and when the timers goes off, NSEL issues flow update (at timer) records. If there is no activity on the flow for the configured time interval, no flow update (at timer) records are sent for that interval. A flow update (at teardown) record is sent with a flow teardown record to capture the traffic in the last time interval. No flow update (at teardown) record is sent if there is no traffic on the flow for the last interval. In addition, no flow update (at teardown) record is sent for short-lived flows (that is, if teardown occurs before the first flow update (at timer) event occurs).

The flow update timer is not set nor is it ever set again if at the time of flow creation, no flow update collectors are configured or if during a flow update event, the flow update collectors are removed. Under these conditions, no flow update (at timer) event or flow update (at teardown) event is seen again.

Flow Update Records and Failover

An attempt to keep flow update records consistent before and after failover is made. After failover occurs, all flow update records are based on the last update from the previously active ASA. This update occurs every 15 seconds as long as traffic is flowing. Inaccuracies may appear in flow update records if failover pairs are brought up at different times, or if failover occurs before the active ASA has a chance to send a periodic update to the standby ASA.

Flow Update Events and Clustering

One major divergence occurs in how flow update events interact with failover and how they interact with clustering. In clustering, before ownership change, the flow director has a stub flow copy of the original flow, which would not have the active refresh timer set. Only after the original flow owner goes down will a full

flow copy be generated with the active refresh timer set. This means it is highly likely that a noticeable time offset will occur between when the flow update timer goes off on the original flow owner and when the flow update timer goes off on the new flow owner.

After flow ownership changes in a cluster, all flow-update records are based on the last update that the flow director received. Flow information is updated every 15 seconds as long as there is traffic. Maintenance of up-to-date flow information uses the same methods as those provided for failover.

NetFlow and Failover

NetFlow data records and templates are only sent from the active (primary) ASA in an active-standby failover pair. The standby (secondary) ASA does not send any NetFlow-related information. However, after failover, the secondary ASA starts to send templates and NetFlow records for any replicated or new flows. The source IP address for each NetFlow collector connection is the same between the two ASAs, but the source port varies. This means that the NetFlow collectors are capable of differentiating packets sent from the primary unit and the secondary unit.

In an active-active failover pair, both ASAs may send NetFlow data records and templates simultaneously. Only the active unit per context sends the NetFlow packets, but the standby unit does not; much like in active-standby scenarios. The source IP address for each NetFlow collector connection is the same for an ASA context and its copy, but the source port varies.

Each ASA node (context) in the failover pair establishes its own connection to the NetFlow collector(s) and advertises its templates independently. The collector uses the source IP address and source port of the packet to differentiate between the NetFlow exporters.

NetFlow and Clustering

NetFlow is supported on both management and regular data interfaces; however, we recommend that you use management interfaces. When the NetFlow collector connection is configured on management-only interfaces, each ASA in the cluster uses its own per-unit source IP address and source port to send NetFlow packets. NetFlow may be used with both data interfaces in layer 2 mode and layer 3 mode. For data interfaces in layer 2 mode, each ASA in the cluster has the same source IP address, but the source port is different. Although layer 2 mode is designed to make a cluster appear as a single device, a NetFlow collector can differentiate between the different nodes in the cluster. For data interfaces in layer 3 mode, NetFlow operates the same way as management-only interfaces do.

Each ASA node in the cluster establishes its own connection to the NetFlow collector(s) and advertises its templates independently. The collector uses the source IP address and source port of the packet to differentiate between the NetFlow exporters.

Decoding Device Fields Through the CLI

To decode some of the field values that the ASA 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.

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.

```
ciscoasa(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 ASA. 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:

```
ciscoasa(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, on page 66. 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 and Extended Event Codes

You must hard code event codes into the collector, because the ASA only issues four different high-level event types (creation, teardown, denial, and update).

Of the four high-level event codes, only two have extended event codes: the flow denial and flow teardown event types. The flow denied and flow teardown extended event codes are explained in Extended Event ID Field, on page 7.

Guidelines for NSEL

Supported Features

- IPv6 for the **class-map**, **match access-list**, and **match any** commands.
- UDP payloads only.

Additional Guidelines

- 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.
- You must use the threat detection feature to view bandwidth usage for NetFlow records (not available in real-time).
- Make sure that you assign unique IP address and hostnames throughout the NetFlow configuration.
- For more implementation details, see the following articles:
  – https://supportforums.cisco.com/docs/DOC-6113
  – https://supportforums.cisco.com/docs/DOC-6114

Configure NSEL Collectors (CLI)

You must have at least one configured collector before you can use NSEL, and you must configure NSEL collectors before you can configure filters via Modular Policy Framework.

To configure an NSEL collector, perform the following steps:

Procedure

Step 1 Add an NSEL collector to which NetFlow packets may be sent.

flow-export destination *interface-name ipv4-address | hostname udp-port*

Example:

```
ciscoasa(config)# flow-export destination inside 209.165.200.225 2002
```

The **destination** keyword indicates that a NSEL collector is being configured. The *interface-name* argument is the name of the ASA and ASA Services Module 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.

Step 2 Repeat the first step to configure more collectors.

Configure Flow-Export Actions Through Modular Policy Framework

To configure flow-export actions through Modular Policy Framework, perform the following steps:

Procedure

Step 1 Define the class map that identifies traffic for which NSEL events need to be exported.

class-map *flow_export_class*

Example:

```
ciscoasa(config-pmap)# class-map flow_export_class
```

The *flow_export_class* argument is the name of the class map.

Step 2 Choose one of the following options:

- Configure the ACL to match specific traffic.

  match access-list *flow_export_acl*

Example:

```
ciscoasa(config-cmap)# match access-list flow_export_acl
```

The *flow_export_acl* argument is the name of the ACL.

- Match any traffic.

match any

Example:

```
ciscoasa(config-cmap)# match any
```

Step 3 Define the policy map to apply flow-export actions to the defined classes.

policy-map *flow_export_policy*

Example:

```
ciscoasa(config)# policy-map flow_export_policy
```

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 remaining inspection policies are deactivated.

Alternatively, enter the **class flow_export_class** command after the **policy-map global_policy** command to insert a NetFlow class in the existing policy.

See the firewall configuration guide or more information about creating or modifying the Modular Policy Framework.

Step 4 Define the class to apply flow-export actions.

class *flow_export_class*

Example:

```
ciscoasa(config-pmap)# class flow_export_class
```

The *flow_export_class* argument is the name of the class.

Step 5 Configure a flow-export action.

flow-export event-type *event-type* **destination** *flow_export_host1* [*flow_export_host2*]

Example:

```
ciscoasa(config-pmap-c)# flow-export event-type all destination 209.165.200.230
```

The **event_type** keyword is the name of the supported event being filtered. The **destination** keyword is the IP address of the configured collector. The flow_export_host argument is the IP address of a host.

Step 6 Add the service policy globally.

service-policy *flow_export_policy* **global**

Example:

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

The *flow_export_policy* argument is the name of the policy map.

Configure Template Timeout Intervals

To configure template timeout intervals, perform the following steps:

Procedure

Specify the interval at which template records are sent to all configured output destinations.

flow-export template timeout-rate *minutes*

Example:

```
ciscoasa(config)# flow-export template timeout-rate 15
```

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.

Change the Time Interval for Sending Flow-Update Events to a Collector

To change the time interval for sending flow-update events to a collector, perform the following steps:

Procedure

Configure NetFlow parameters for active connections.

flow-export active refresh-interval *value*

Example:

```
ciscoasa(config)# flow-export active refresh-interval 30
```

The *value* argument specifies the time interval between flow-update events in minutes. Valid values are from 1 - 60 minutes. The default value is 1 minute.

If you have already configured the **flow-export delay flow-create** command, and you then configure the flow-export active refresh-interval command with an interval value that is not at least 5 seconds more than the delay value, the following warning message appears at the console:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

If you have already configured the flow-export active refresh-interval command, and you then configure the **flow-export delay flow-create** command with a delay value that is not at least 5 seconds less than the interval value, the following warning message appears at the console:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
appear before flow-creation events.
```

Delay the Sending of Flow-Create Events

To delay the sending of flow-create events, perform the following steps:

Procedure

Delay the sending of a flow-create event by the specified number of seconds.

flow-export delay flow-create *seconds*

Example:

```
ciscoasa(config)# flow-export delay flow-create 10
```

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.

Disable and Reenable NetFlow-related Syslog Messages

To disable and reenable NetFlow-related syslog messages, perform the following steps:

Procedure

Step 1 Disable syslog messages that have become redundant because of NSEL.

logging flow-export-syslogs disable

Example:

```
ciscoasa(config)# logging flow-export-syslogs disable
```

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 Reenable syslog messages individually, where *xxxxxx* is the specified syslog message that you want to reenable.

logging message*xxxxxx*

Example:

```
ciscoasa(config)# logging message 302013
```

Step 3 Reenable all NSEL events at the same time.

logging flow-export-syslogs enable

Example:

```
ciscoasa(config)# logging flow-export-syslogs enable
```

Reset Runtime Counters

To reset runtime counters, perform the following steps:

Procedure

Reset all runtime counters for NSEL to zero.

clear flow-export counters

Example:

```
ciscoasa# clear flow-export counters
```

Enable NetFlow (ASDM)

To enable NetFlow, perform the following steps:

Procedure

Step 1 Choose **Configuration** > **Device Management** > **Logging** > **NetFlow**.

Step 2 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 3 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 4 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 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,

Step 5 Specify the collectors to which NetFlow packets will be sent. You can configure a maximum of five collectors. Click **Add** to display the **Add NetFlow Collector** dialog box to configure a collector, 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**.

Repeat these steps to create additional collectors.

Step 6 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. Check the **Disable redundant syslog messages** check box to disable all redundant syslog messages. Click **Show Redundant Syslog Messages** to display the redundant syslog messages and their status.

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.

Choose **Configuration** > **Device Management** > **Logging** > **Syslog Setup** to disable individual redundant syslog messages.

Step 7 Click **Apply** to save your changes, or click **Reset** to enter new settings.

Match NetFlow Events to Configured Collectors

To match a NetFlow event with any configured collector, perform the following steps:

Procedure

Step 1 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**. See the firewall configuration guide for more information about service policy rules.

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 Click the **NetFlow** tab in the **Rule Actions** screen.

Step 4 Click **Add** to display the **Add Flow Event** dialog box and specify flow events, 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) and later.

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

c. Click **Manage** to display the **Manage NetFlow Collectors** dialog box, in which you can add, edit or delete collectors, or configure other NetFlow settings (for example, syslog messages). Click **OK** to close

the **Manage NetFlow Collectors** dialog box and return to the **Add Flow Event** dialog box. See Step 5 of Enable NetFlow (ASDM), for more information about configuring collectors.

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

Step 6 Click **Finish** to exit the wizard.

Step 7 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.

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. See Syslog Messages and NSEL Events, for more information.

You can monitor NSEL using the following commands:

Procedure

	Command or Action	Purpose
Step 1	In Adaptive Security Device Manager (ASDM), choose **Tools** > **Command Line Interface** to enter the commands.	• **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 flow-export** Shows the currently configured NetFlow commands. • **show running-config logging** Shows disabled syslog messages, which are redundant syslog messages because they export the same information through NetFlow.

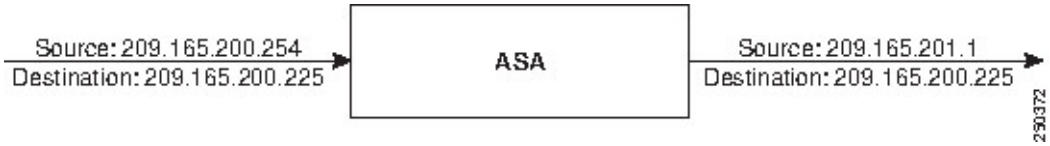
Examples for NSEL (CLI)

The following examples show flows that generate events and include information about how to implement collector support for NSEL fields in the ASA.

Example 1: Allowed Flow with PAT Interface

This 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 the following figure 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_INGRESS_ACL_ID	0
NF_F_EGRESS_ACL_ID	0

Field	Value
NF_F_USERNAME	User A

Example 2: Denied Flow on Egress with PAT Interface

This 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:

```
ciscoasa# object-group network host_grp_1
 network-object host 209.165.200.254
 network-object host 209.165.201.1
ciscoasa(config)# access-list foo extended permit tcp
object-group host_grp_1 any eq www
ciscoasa(config)# access-list bar extended deny tcp any any
ciscoasa(config)# access-group foo in interface inside
ciscoasa(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

Field	Value
NF_F_INGRESS_ACL_ID	0x102154c1d0e5806e7e5ad93b
NF_F_EGRESS_ACL_ID	0x5da9bb6984434b4b00000000
NF_F_USERNAME	User A

Example 3: Filtering NSEL Events

These examples show how to filter NSEL events, with the specified collectors already configured:

- **flow-export destination inside 209.165.200.2055**
- **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:

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

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

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

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

Note You must enter the following command:

```
ciscoasa(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:

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

History for NSEL

Table 10: 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 commands: **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**. We introduced the following screen: Configuration > Device Management > Logging >NetFlow.

Feature Name	Platform Releases	Feature Information
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. We modified the following commands: **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. We introduced the following command: **flow-export delay flow-create**. We modified the following screen: Configuration > Firewall > Service Policy Rules.
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	9.0(1)	A new NetFlow error counter, source port allocation failure, has been added. We modified the following command: **show flow-export counters**. **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 introduced the following command: **flow-export active refresh-interval**. We modified the following command: **flow-export event-type**. 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.