# Zone-Based Firewall Logging Export Using NetFlow

Zone-based firewalls support the logging of messages to an external collector using NetFlow Version 9 export format. NetFlow Version 9 export format uses templates to define the format of data that is exported. Template records are sent to the collector along with data records, and the collector interprets these records by using the structural information available in the template.

This module describes the various firewall logging counters and how to configure NetFlow Version 9 flow exporter for firewall message logging.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

# Restrictions for Zone-Based Firewall Logging Export Using NetFlow

The following features are not supported:

- NetFlow-based logging of pass events
- Layer 7 inspection events
- IPFIX and NetFlow Version 5
- Export of records to multiple collectors
- IPv6 events

# Information About Zone-Based Firewall Logging Export Using NetFlow

## NetFlow Version 9 Logging Overview

Log messages help the monitoring or managing system to report, analyze, and correlate various events for network administrators. With the introduction of the Zone-Based Firewall Logging Export Using NetFlow feature, firewalls also support the export of record templates and events in Cisco NetFlow Version 9 export format.

Zone-based firewalls export some events (audits and alerts) to an external collector using NetFlow Version 9 export format. NetFlow is a Cisco proprietary network protocol that collects IP traffic to gather flow information, events, and statistics on a device and exports this information to a collector device as NetFlow records. The basic output of NetFlow is a flow record. The latest NetFlow flow-record format is NetFlow Version 9. NetFlow Version 9 format uses templates to define the format of the data that is exported. As template records are sent to an external collector along with data records, the collector can interpret the data records using the structural information available in templates.

NetFlow Version 9 records provide the following features:

- Provides templates to format logging events that help collectors to consume and interpret data based on templates.
- Data is binary-coded and easy to encode and decode (parse).
- Scales better than traditional syslogs and provides better logging performance on the device and the management station.

For more information about NetFlow Version 9, see *RFC 3954*.

**Note** An external collector application is required to parse templates and interpret the logged data for reporting and display.

# Firewall Logging Events

Zone-based firewalls export the following event types by using NetFlow Version 9 export format:

- Audit Events—Start Audit Record and Stop Audit Record. Logs messages when sessions are created and deleted.
- Drop Events—Packet Drop notifications. Logs messages when the following events are dropped—unknown protocols, unseen flows, Out-of-Order (OoO) packets, and so on.
- Alert Events—TCP Half Open Alert, Half Open Session Alert, Maximum-Open sessions. Logs TCP half-open alert messages when the TCP half-open alert threshold values exceed the configured limit.

# NetFlow Version 9 Start Audit Records

This template describes the format of data records associated with Start Audit events. Records are generated when a firewall creates a new IPv4-to-IPv4 session. A record is created for every new flow that the firewall creates. The Start Record event is similar to the firewall syslog message (SESS_AUDIT_TRAIL_START).

***Table 1: NetFlow Version 9 Start Audit Records***

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_SRC_ADDR_IPV4 | 8 | 4 | Source IPv4 address. |
| FW_DST_ADDR_IPV4 | 12 | 4 | Destination IPv4 address. |
| FW_SRC_PORT | 7 | 2 | Source port. |
| FW_DST_PORT | 11 | 2 | Destination port. |
| FW_PROTOCOL | 4 | 1 | Internet Protocol value. Valid values are the following:<br>• 0—Unknown<br>• 0x01—Layer 4 Internet Control Message Protocol (ICMP)<br>• 0x06—Layer 4 TCP<br>• 0x11—Layer 4 UDP |
| FW_ICMP_TYPE | 176 | 1 | ICMP type value that is set only for ICMP packets (for all other packets the value is zero). |
| FW_ICMP_CODE | 177 | 1 | ICMP code value.<br>**Note** This field is not supported by Cisco IOS zone-based firewalls. The value of this field is zero. |

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_EVENT | 233 | 1 | Indicates a firewall event. Valid values are the following:<br>• 0—Ignore (invalid)<br>• 1—Flow created<br>• 2—Flow deleted<br>• 3—Flow denied<br>• 4—Flow alert<br>• 5—Flow update |
| FW_IPV4_IDENT | 54 | 4 | IPv4 ID. The value of the ID field in IPv4 packet. If no fragment header is available, the value is zero. |
| FW_TCP_SEQ | 184 | 4 | TCP sequence number. |
| FW_TCP_ACK | 185 | 4 | TCP acknowledgment sequence number. This value is zero for session creation. |
| FW_TCP_FLAGS | 6 | 1 | TCP flags. |
| FW_EVENT_TIME_MSEC | 323 | 8 | Time, in milliseconds, (time since 0000 hours Consolidated Universal Time [UTC] January 1, 1970) when the event occurred. |
| FW_INITIATOR_OCTETS | 231 | 8 | Size of the Layer 4 payload (in bytes) sent by the initiator. |
| FW_RESPONDER_OCTETS | 232 | 8 | Size of the Layer 4 payload (in bytes) arrived from the responder. This value is zero for session creation. |
| FW_EXT_EVENT | 35001 | 2 | Firewall feature extended event code. The values are defined in Table 8. |
| FW_L7_PROTOCOL_ID | 95 | 4 | Layer 7 protocol ID. This field is specified as per RFC 6758. This field consists of two parts:<br>• 1-byte of Classification Engine ID<br>• 3-bytes of Selector ID |
| FW_XLATE_SRC_ADDR_IPV4 | 225 | 4 | Translated source IPv4 address. |
| FW_XLATE_DST_ADDR_IPV4 | 226 | 4 | Translated destination IPv4 address. |

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_XLATE_SRC_PORT | 227 | 2 | Translated source port. |
| FW_XLATE_DST_PORT | 228 | 2 | Translated destination port. |
| FW_SRC_INTF_ID | 10 | 2 | Source interface ifIndex. |
| FW_DST_INTF_ID | 14 | 2 | Destination interface ifIndex. |
| FW_SRC_VRF_ID | 234 | 4 | Ingress virtual routing and forwarding (VRF) ID. This value is zero if there is no VRF configuration on the source interface. |
| FW_DST_VRF_ID | 235 | 4 | Egress VRF ID. This value is zero if there is no VRF configuration on the destination interface. |
| FLOW_CLASS -or- FW_CLASS_ID | 51 | 4 | Class map ID (numeric representation of the class-map name) associated with this flow. |
| FW_ZONEPAIR_ID | 35007 | 4 | Zone pair ID (numeric representation of zone-pair name) associated with this flow. |
| FW_CTS_SRC_SGT | 34000 | 2 | Source security group tag (SGT) (if a match on SGT) for this flow. |

# NetFlow Version 9 Stop Audit Records

This template describes the format of data records associated with the Stop Audit event. This record is generated when a firewall deletes an existing IPv4-to-IPv4 session. This record is generated for every flow that is deleted or terminated by a firewall. This event is similar to the firewall syslog message (SESS_AUDIT_TRAIL).

**Note** The export of this event is not rate limited.

***Table 2: NetFlow Version 9 Stop Audit Records***

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_SRC_ADDR_IPV4 | 8 | 4 | Source IPv4 address. |
| FW_DST_ADDR_IPV4 | 12 | 4 | Destination IPv4 address. |
| FW_SRC_PORT | 7 | 2 | Source port. |

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_DST_PORT | 11 | 2 | Destination port. |
| FW_PROTOCOL | 4 | 1 | Internet Protocol value. Valid values are the following:<br>• 0—Unknown<br>• 0x01—Layer 4 Internet Control Message Protocol (ICMP)<br>• 0x06—Layer 4 TCP<br>• 0x11—Layer 4 UDP |
| FW_ICMP_TYPE | 176 | 1 | ICMP type value. The value is set only for ICMP packets; the value of all other packets is zero. |
| FW_ICMP_CODE | 177 | 1 | ICMP code value.<br>**Note** This field is not supported by Cisco IOS zone-based firewalls. The value of this field is zero. |
| FW_EVENT | 233 | 1 | Indicates a firewall event. Valid values are the following:<br>• 0—Ignore (invalid)<br>• 1—Flow created<br>• 2—Flow deleted<br>• 3—Flow denied<br>• 4—Flow alert<br>• 5—Flow update |
| FW_IPV4_IDENT | 54 | 4 | IPv4 identification. This value is zero for a Stop Audit event. |
| FW_TCP_SEQ | 184 | 4 | TCP sequence number. |
| FW_TCP_ACK | 185 | 4 | TCP acknowledgment sequence number. |
| FW_TCP_FLAGS | 6 | 1 | TCP flags. |
| FW_EVENT_TIME_MSEC | 323 | 8 | Time, in milliseconds, (time since 0000 hours Consolidated Universal Time [UTC] January 1, 1970) when the event occurred. |

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_INITIATOR_OCTETS | 231 | 8 | Size of the Layer 4 payload (in bytes) sent by the initiator. |
| FW_RESPONDER_OCTETS | 232 | 8 | Size of the Layer 4 payload (in bytes) arrived from the responder. |
| FW_EXT_EVENT | 35001 | 2 | Firewall feature extended event code. The values are defined in Table 8. |
| FW_L7_PROTOCOL_ID | 95 | 4 | Layer 7 protocol ID as specified in RFC 6758. This ID consists of two parts:<br>• 1-byte of Classification Engine ID<br>• 3-bytes of Selector ID |
| FW_XLATE_SRC_ADDR_IPV4 | 225 | 4 | Translated source IPv4 address. |
| FW_XLATE_DST_ADDR_IPV4 | 226 | 4 | Translated destination IPv4 address. |
| FW_XLATE_SRC_PORT | 227 | 2 | Translated source port. |
| FW_XLATE_DST_PORT | 228 | 2 | Translated destination port. |
| FW_SRC_INTF_ID | 10 | 2 | Source interface ifIndex. |
| FW_DST_INTF_ID | 14 | 2 | Destination interface ifIndex. |
| FW_SRC_VRF_ID | 234 | 4 | Ingress virtual routing and forwarding (VRF) ID. This value is zero if there is no VRF configuration on the source interface. |
| FW_DST_VRF_ID | 235 | 4 | Egress VRF ID. This value is zero if there is no VRF configuration on the destination interface. |
| FLOW_CLASS or<br>FW_CLASS_ID | 51 | 4 | Class map ID associated with this flow. |
| FW_ZONEPAIR_ID | 35007 | 4 | Zone pair ID associated with this flow. |
| FW_CTS_SRC_SGT | 34000 | 2 | Source security group tag (SGT) (if a match on SGT) for this flow. |

# NetFlow Version 9 Flow-Denied Records

This template describes the format of the data records associated with a flow-denied event. This record is generated when a firewall denies an IPv4-to-IPv4 flow or packet. This record is generated for every flow that is denied or packet that is dropped by the firewall. The FW_EXT_EVENT specifies the reason for the flow drop or denial. This event matches the syslog message DROP_PKT.

***Table 3: NetFlow Version 9 Flow-Denied Records***

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_SRC_ADDR_IPV4 | 8 | 4 | Source IPv4 address. |
| FW_DST_ADDR_IPV4 | 12 | 4 | Destination IPv4 address. |
| FW_SRC_PORT | 7 | 2 | Source port. |
| FW_DST_PORT | 11 | 2 | Destination port. |
| FW_PROTOCOL | 4 | 1 | Internet Protocol value. Valid values are the following:<br>• 0—Unknown<br>• 0x01—Layer 4 Internet Control Message Protocol (ICMP)<br>• 0x06—Layer 4 TCP<br>• 0x11—Layer 4 UDP |
| FW_ICMP_TYPE | 176 | 1 | ICMP type value that is set only for ICMP packets (for all other packets the value is zero). |
| FW_ICMP_CODE | 177 | 1 | ICMP code value.<br>**Note** This field is not supported by Cisco IOS zone-based firewalls. The value of this field is zero. |

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_EVENT | 233 | 1 | Indicates a firewall event. Valid values are the following:<br>• 0—Ignore (invalid)<br>• 1—Flow created<br>• 2—Flow deleted<br>• 3—Flow denied<br>• 4—Flow alert<br>• 5—Flow update |
| FW_IPV4_IDENT | 54 | 4 | IPv4 ID. The value of the ID field in an IPv4 packet. If no fragment header is available, the value is zero. |
| FW_TCP_SEQ | 184 | 4 | TCP sequence number. |
| FW_TCP_ACK | 185 | 4 | TCP acknowledgment sequence number. This value is zero for session creation. |
| FW_TCP_FLAGS | 6 | 1 | TCP flags. |
| FW_EVENT_TIME_MSEC | 323 | 8 | Time, in milliseconds, (time since 0000 hours Consolidated Universal Time [UTC] January 1, 1970) when the event occurred. |
| FW_INITIATOR_OCTETS | 231 | 8 | Size of the Layer 4 payload (in bytes) sent by the initiator. |
| FW_RESPONDER_OCTETS | 232 | 8 | Size of the Layer 4 payload (in bytes) arrived from the responder. This value is zero for session creation. |
| FW_EXT_EVENT | 35001 | 2 | Firewall feature extended event code. The values are defined in Table 8. |

| Field IDs | Type | Length | Description |
|---|---|---|---|
| FW_L7_PROTOCOL_ID | 95 | 4 | Layer 7 protocol ID. This field is specified as per RFC 6758. This field consists of two parts:<br>• 1-byte of Classification Engine ID<br>• 3-bytes of Selector ID |
| FW_XLATE_SRC_ADDR_IPV4 | 225 | 4 | Translated source IPv4 address. |
| FW_XLATE_DST_ADDR_IPV4 | 226 | 4 | Translated destination IPv4 address. |
| FW_XLATE_SRC_PORT | 227 | 2 | Translated source port. |
| FW_XLATE_DST_PORT | 228 | 2 | Translated destination port. |
| FW_SRC_INTF_ID | 10 | 2 | Source interface ifIndex. |
| FW_DST_INTF_ID | 14 | 2 | Destination interface ifIndex. |
| FW_SRC_VRF_ID | 234 | 4 | Ingress virtual routing and forwarding (VRF) ID. This value is zero if there is no VRF configuration on the source interface. |
| FW_DST_VRF_ID | 235 | 4 | Egress VRF ID. This value is zero if there is no VRF configuration on the destination interface. |
| FLOW_CLASS or FW_CLASS_ID | 51 | 4 | Class map ID (numeric representation of the class-map name) associated with this flow. |
| FW_ZONEPAIR_ID | 35007 | 4 | Zone pair ID (numeric representation of zone-pair name) associated with this flow. |
| FW_CTS_SRC_SGT | 34000 | 2 | Source security group tag (SGT) (if a match on SGT) for this flow. |

# TCP Half-Open Alert Records

Zone-based firewalls provide protection for hosts against denial-of-service (DoS) attacks such as TCP SYN-flood attack. The threshold values to detect this event can be set using the following commands:

```
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp max-incomplete host 100
```

or

```
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# tcp max-incomplete host 100 block-time 10
```

When the threshold values exceed the configured limit, the information for this event is exported as TCP Half-Open Alert Record. A TCP session that has not yet reached the established state is called a half-open session. The two scenarios that trigger the export of this record are the following:

- TCP maximum-incomplete value is configured, and block time is not configured. When the maximum number of half-open sessions that reach a host exceeds the configured limit, the firewall generates NetFlow logs with the FW_EXT_EVENT set to FW_EXT_ALERT_HOST_TCP_ALERT_ON. This event is similar to firewall syslog message ID HOST_TCP_ALERT_ON.
- TCP maximum-incomplete value and block time are configured:
  - When the maximum number of half-open sessions that reach a host exceeds the configured limit, the firewall blocks all subsequent TCP connection requests. After the configured blocking interval expires, TCP connection requests are allowed. NetFlow logs FW_EXT_EVENT that is set to FW_EXT_ALERT_BLOCK_HOST and FW_BLACKOUT_SECS (indicates the blocking interval in seconds). This event is similar to the syslog message ID BLOCK_HOST.
  - When the blocking interval expires and the firewall allows further connections to the host, NetFlow logs FW_EXT_EVENT that is set to FW_EXT_ALERT_UNBLOCK_HOST and FW_BLACKOUT_SECS. This event is similar to the syslog message ID UNBLOCK_HOST.

**Note** The export of this event is not rate limited.

***Table 4: TCP Half-Open Alert Records***

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| FW_DST_ADDR_IPV4 | 12 | 4 | 0 to 3 | Destination IPv4 address. |
| FW_PROTOCOL | 4 | 1 | 4 | Internet Protocol value or ID. |
| FW_EVENT | 233 | 1 | 5 | High level event code. A value is 4 indicates a flow alert. |

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| FW_EXT_EVENT | 35001 | 2 | 6 to 7 | Extended firewall event code. Valid values are the following:<br>• 0x1E—FW_EXT_ALERT_UNBLOCK_HOST<br>• 0x1F—FW_EXT_ALERT_HOST_TCP_ALERT_ON<br>• 0x20—FW_EXT_ALERT_BLOCK_HOST |
| FW_EVENT_TIME_MSEC | 323 | 8 | 8 to 15 | Time, in milliseconds, (time since 0000 hours Consolidated Universal Time [UTC] January 1, 1970) when the event occurred. |
| FW_HALFOPEN_CNT | 35012 | 4 | 16 to 19 | Number of half-open TCP sessions. |
| FW_BLACKOUT_SECS | 35004 | 4 | 20 to 23 | Time duration, in seconds, when a destination is blacked out or unavailable. |
| FW_DST_INTF_ID | 14 | 2 | 24 to 26 | SNMP ifIndex of the egress interface. |
| FW_DST_VRF_ID | 235 | 4 | 27 to 30 | Unique ID of the destination virtual routing and forwarding (VRF) instance. |
| FLOW_CLASS or FW_CLASS_ID | 51 | 4 | 31 to 34 | Class map ID associated with this flow. |
| FW_ZONEPAIR_ID | 35007 | 4 | 35 to 38 | Zone pair ID associated with this flow. |

# Half-Open Session Alert Records

This template describes the format of data records for Half Open Session Alert. This record is generated when the number of existing half-open sessions exceed the configured high limit value or drop below the low bound value. The export of this event is not rate limited.

Use the following commands to configure the half-open session limit:

```
Device(config)# parameter-map type inspect param-name
Device(config-profile)# max-incomplete high 20000
Device(config-profile)# max-incomplete low 10000
```

*Table 5: Half-Open Session Alert Records*

| Field ID | Type | Length | Description |
|---|---|---|---|
| FW_EVENT | 233 | 1 | High level event code. A value of 4 indicates Flow Alert. |
| FW_EXT_EVENT | 35001 | 2 | Extended Firewall event code. Valid values are the following:<br>• 0x21—FW_EXT_SESS_RATE_ALERT_ON<br>• 0x22—FW_EXT_SESS_RATE_ALERT_OFF |
| FW_EVENT_TIME_MSEC | 323 | 8 | Time, in milliseconds, (time since 0000 hours Consolidated Universal Time [UTC] January 1, 1970) when the event occurred. |
| FW_EVENT_LEVEL | 33003 | 1 | Extended firewall event code. Valid values are the following:<br>• 0x01—Per box<br>• 0x02—Virtual routing and forwarding (VRF)<br>• 0x03—Zone<br>• 0x04—Class map<br>• Other values are undefined |
| FW_EVENT_LEVEL_ID | 33004 | 4 | Defines the identifier for the FW_EVENT_LEVEL event. Valid values are the following:<br>• 0x02—VRF_ID.<br>• 0x03—ZONE_ID.<br>• 0x04—CLASS_ID.<br>• In all other cases and if FW_EVENT_LEVEL is not present the field ID is zero. |
| FW_CONFIGURED_VALUE | 33005 | 4 | Specifies the configured half-open session high-limit value or low-bound value. |

# Maximum Session Alert Records

This template describes the format of data records for the Maximum Session Alert event. This record is generated when the number of firewall sessions exceed the configured limit. The export of this event is not rate limited and is generated when sessions exceed the configured limit. Use the following commands to configure the maximum limit for firewall sessions:

```
Device (config)# parameter-map type inspect param-map
Device(config-profile)# sessions maximum 20000
```

***Table 6: Maximum Session Alert Records***

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| FW_EVENT | 233 | 1 | 0 | High level event code. A value of 4 indicates flow alert. |
| FW_EXT_EVENT | 35001 | 2 | 1 to 2 | Extended firewall event code. A value of 0x23 indicates FW_EXT_L4_SESSION_LIMIT. |
| FW_EVENT_TIME_MSEC | 323 | 8 | 3 to 10 | Time, in milliseconds, (time since 0000 hours Consolidated Universal Time [UTC] 4 January 1, 1970) when the event occurred. |
| FW_MAX_SESSIONS | 35008 | 4 | 11 to 14 | Maximum sessions allowed for this zone pair or class ID. |
| FW_ZONEPAIR_ID | 35007 | 4 | 15 to 18 | Zone pair ID associated with this flow. |
| FLOW_CLASS or FW_CLASS_ID | 51 | 4 | 19 to 22 | Class map ID associated with this flow. |

# NetFlow Version 9 Option Template Records

This template provides information about the data that is exported as part of data records. For example, a data record exports the Interface-ID field, which is a numerical representation of the interface. To obtain the corresponding name on the device, the device exports option template data records that consists of the Interface-ID-to-Interface-Name value mapping. Option template data records are exported periodically based on the configured option template timeout value.

### Protocol ID-to-Name Mapping

The protocol ID-to-name mapping is obtained by exporting the inspect-protocol-table option template and enabling the **debug policy-firewall exporter** command.

The following is sample output from the **debug policy-firewall exporter** command. In the following output, protocol ID is 6xxyyzz where xxyyzz is the 3-byte protocol ID in hexadecimal notation.

```
FW-EXPORT: Sent Opt Rec Protocol Id:(6000001) <--> Name:(ftp)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000002) <--> Name:(telnet)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000003) <--> Name:(smtp)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000004) <--> Name:(http)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000005) <--> Name:(tacacs)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000006) <--> Name:(dns)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000007) <--> Name:(sql-net)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000008) <--> Name:(https)
FW-EXPORT: Sent Opt Rec Protocol Id:(6000009) <--> Name:(tftp)
FW-EXPORT: Sent Opt Rec Protocol Id:(600000A) <--> Name:(gopher)
FW-EXPORT: Sent Opt Rec Protocol Id:(600000B) <--> Name:(finger)
FW-EXPORT: Sent Opt Rec Protocol Id:(600000C) <--> Name:(kerberos)
FW-EXPORT: Sent Opt Rec Protocol Id:(600000D) <--> Name:(pop2)
FW-EXPORT: Sent Opt Rec Protocol Id:(600000E) <--> Name:(pop3)
!
!
!
```

### VRF Name Options Record

NetFlow Version 9 supports the export of the vrf-table option template. The external collectors must correlate the virtual routing and forwarding (VRF) IDs in the firewall records with the VRF names specified in vrf-table option records received from the exporter.

The following is a sample output from the **show flow exporter templates** command:

```
Device# show flow exporter templates

Flow Exporter tfoo
  Client: Option options vrf-id-name-table
  Exporter Format: NetFlow Version 9
  Template ID    : 256
  Source ID      : 0
  Record Size    : 40
  Template layout
 _____________________________________________________________________
|                 Field                   |  Type | Offset |  Size  |
---------------------------------------------------------------------
| v9-scope system                         |     1 |      0 |      4 |
| routing vrf input                       |   234 |      4 |      4 |
| routing vrf name                        |   236 |      8 |     32 |
---------------------------------------------------------------------
```

### Interface ID-to-Name Mapping

There is no option template to export interface ID-to-name mapping. External collectors must query the ifIndex MIB via Simple Network Management Protocol (SNMP) to correlate SRC_IF_INDEX and DST_IF_INDEX to the interface description or name.

## Class-Name Option Records

This template describes the format of option templates that map FW_CLASS_ID to a class name.

*Table 7: Class-Name Options Records*

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| v9-scope-system | 1 | 4 | 0 to 3 | Provides information about the NetFlow process to which the option record refers. Valid values are the following:<br>• 0x0001—System<br>• 0x0002—Interface<br>• 0x0003—Line card<br>• 0x0004—NetFlow cache<br>• 0x0005—Template |
| FLOW_CLASS or FW_CLASS_ID | 51 | 4 | 4 to 7 | Class map ID on the device. |
| FW_CLASS_NAME | 100 | 64 | 8 to 71 | Name of the class. |

## Firewall Extended Event Records

The following table describes the FW_EXT_EVENT_ID fields associated with the logging of drop events. The firewall extended event records map extended-event IDs to names.

*Table 8: Firewall Extended Event Records*

| Value | FW_EXT_EVENT_ID | Description |
|---|---|---|
| 0 | INSP_L4_NO_ERROR | No specific extended event. |
| 1 | INSP_L4_INVAL_HLEN | Invalid Layer 4 header length. |
| 2 | INSP_L4_C3PL_LOOKUP_FAIL | Policy match failure. |
| 3 | INSP_L4_POLICE_RATE_LIMIT | Police rate limiting |
| 4 | INSP_L4_SESSION_LIMIT | Session limit exceeded. |
| 5 | INSP_L4_ICMP_INVAL_RET | Invalid return packet. |
| 6 | INSP_L4_ICMP_INVAL_DEST | Invalid destination address for unreachable or time-exceeded packets. |
| 7 | INSP_L4_UDP_DISA_BIDIR | Bidirectional traffic disabled. |
| 8 | INSP_L4_SYN_INVAL_FLDATA | Synchronize (SYN) packet with data or with push (PSH) or urgent (URG) flags. |

| Value | FW_EXT_EVENT_ID | Description |
|---|---|---|
| 9 | INSP_L4_INVALID_CONN_SEG | Segment does not match any TCP connection. |
| 10 | INSP_L4_INVALID_SEG | Invalid TCP segment. |
| 11 | INSP_L4_INVALID_SEQ | Invalid TCP sequence number. |
| 12 | INSP_L4_INVALID_ACK | Invalid TCP acknowledgment (ACK) or no ACK. |
| 13 | INSP_L4_INVALID_FLAGS | Invalid TCP flags. |
| 14 | INSP_L4_INVALID_CHKSM | Invalid TCP checksum. |
| 15 | INSP_L4_SYN_IN_WIN | SYN inside current window. A SYN packet is seen within the window of an already established TCP connection. |
| 16 | INSP_L4_RST_IN_WIN | Reset (RST) inside current window. An RST packet is seen within the window of an already established TCP connection. |
| 17 | INSP_L4_OOO_SEG | Out-of-Order (OoO) segment. |
| 18 | INSP_L4_OOO_INVALID_FLAGS | OoO segment with invalid flag. |
| 19 | INSP_L4_RETRANS_SEG | Retransmitted segment. |
| 20 | INSP_L4_RETRANS_INVALID_FLAGS | Retransmitted segment with invalid flag. |
| 21 | INSP_L4_STRAY_SEQ | Stray TCP segment. |
| 22 | INSP_L4_INTERNAL_ERR | Firewall internal error. |
| 23 | INSP_L4_INVALID_WINDOW_SCALE | Invalid window scale option. |
| 24 | INSP_L4_INVALID_TCP_OPTION | Invalid TCP option. |
| 25 | INSP_UNKNOWN_ERR | Unknown error. |
| 26 | INSP_L4_C3PL_LOOKUP_FAIL_NO_ZONE_PAIR | Lookup failure because zone pairs are not available between zones. |
| 27 | INSP_L4_C3PL_LKP_FAIL_ZONE_TO_NONZONE | Lookup failure because only one interface is the member of a zone and other interface is not a member of any zone. |
| 28 | INSP_L4_C3PL_LOOKUP_FAIL_NO_POLICY | Policy not present in the zone pair. |
| 29 | INSP_L4_DROP_CONFIGURED | Drop action configured in a policy map. |

| Value | FW_EXT_EVENT_ID | Description |
|---|---|---|
| 30 | FW_EXT_ALERT_UNBLOCK_HOST | Blocking of TCP attempts to a specified host is removed. |
| 31 | FW_EXT_ALERT_HOST_TCP_ALERT_ON | Maximum incomplete host limit of half-open TCP connections exceeded.<br>**Note** Once this message is sent to the host, the traffic from that host can be blocked by sending the FW_EXT_ALERT_BLOCK_HOST message for the time period configured. |
| 32 | FW_EXT_ALERT_BLOCK_HOST | Maximum incomplete host threshold of half-open TCP connections exceeded. |
| 33 | FW_EXT_SESS_RATE_ALERT_ON | Exceeded either the maximum incomplete high threshold of half-open connections or the new connection initiation rate ID. |
| 34 | FW_EXT_SESS_RATE_ALERT_OFF | Either the number of half-open connections or the new connection initiation rate is below the maximum incomplete low threshold. |
| 35 | FW_EXT_MAX_SESS_LIMIT | Number of established sessions has crossed the configured threshold. |

## Firewall Extended Event-Named Option Records

This template describes the format of option templates that map FW_EXT_EVENT to an event name or a description

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| v9-scope-system | 1 | 4 | 0 to 3 | This field provides information about the NetFlow process to which the options record refers. Valid values are the following:<br>• 0x0001—System<br>• 0x0002—Interface<br>• 0x0003—Line card<br>• 0x0004—NetFlow cache<br>• 0x0005—Template |
| FW_EXT_EVENT | 35001 | 2 | 4 to 5 | Extended event code. |

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| FW_EXT_EVENT_DESC | 35010 | 64 | 6 to 69 | Description of the extended event. |

### Extended Event ID-to-Name Mapping

The extended event ID-to-name mapping records are obtained by exporting the inspect-ext-event-table option template and enabling the **debug policy-firewall exporter** command.

The following is sample output from the **debug policy-firewall exporter** command:

```
*Dec 20 05:24:50.917: FW-EXPORT: Sent Optional Record Ext Event id:(0x0) <--> Name:(NO_ERROR)
*Dec 20 05:24:50.917: FW-EXPORT: Sent Optional Record Ext Event id:(0x1) <-->
Name:(INVALID_HEADER_LENGTH)
*Dec 20 05:24:50.917: FW-EXPORT: Sent Optional Record Ext Event id:(0x2) <-->
Name:(POLICY_MATCH_FAILURE)
*Dec 20 05:24:50.917: FW-EXPORT: Sent Optional Record Ext Event id:(0x3) <-->
Name:(POLICE_RATE_LIMITING)
*Dec 20 05:24:50.917: FW-EXPORT: Sent Optional Record Ext Event id:(0x4) <-->
Name:(SESSION_LIMITING)
*Dec 20 05:24:50.917: FW-EXPORT: Sent Optional Record Ext Event id:(0x5) <-->
Name:(INVALID_RETURN_PACKET)
!
!
!
```

## Protocol-Name Option Records

This template describes the format of option templates that map the FW_PROTOCOL_ID to the protocol name. As per RFC 6759, the protocol ID or application ID (that is, the IANA Flow Field Type 95) is represented as a 4-byte number with the following two parts:

- 1-byte of Classification Engine ID. For NetFlow logging this value is always equal to 6, which specifies that this value is user defined.
- 3-bytes of Selector ID. This value represents the actual protocol ID or application ID as defined by the device.

**Note** All values are not exported; only protocols that the zone-based firewall supports are exported.

*Table 9: Protocol-Name Option Records*

| Field IDs | Type | Length | Offset | Description |
|---|---|---|---|---|
| v9-scope-system | 1 | 4 | 0 to 3 | This field refers to the NetFlow process to which the options record refers.<br>Valid values are the following:<br>• 0x0001—System<br>• 0x0002—Interface<br>• 0x0003—Line card<br>• 0x0004—NetFlow cache<br>• 0x0005—Template |
| FW_L7_PROTOCOL_ID | 95 | 4 | 4 to 7 | Layer 7 protocol ID as specified in RFC 6758. The ID consists of the following two parts:<br>• 1-byte of Classification Engine ID<br>• 3-bytes of Selector ID |
| FLOW_FIELD_L7_PROTOCOL_NAME | 96 | 64 | 8 to 72 | Specifies the name of the protocol or application. |

## Zone-Pair Name Option Records

This template describes the format of option templates that map FW_ZONEPAIR_ID event to a zone-pair name configured on the device.

*Table 10: Zone-Pair Name Options Records*

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| v9-scope-system | 1 | 4 | 0 to 3 | This field provides information about the NetFlow process to which the options record refers. Valid values are the following:<br>• 0x0001—System<br>• 0x0002—Interface<br>• 0x0003—Line card<br>• 0x0004—NetFlow cache<br>• 0x0005—Template |

| Field ID | Type | Length | Offset | Description |
|---|---|---|---|---|
| FW_ZONEPAIR_ID | 35007 | 4 | 4 to 7 | Zone-pair ID configured on the device. |
| FW_ZONEPAIR_NAME | 35009 | 64 | 8 to 71 | Name of the zone pair that corresponds to the zone-pair ID. |

# How to Configure Zone-Based Firewall Logging Export Using NetFlow

Perform the following tasks to configure zone-based firewall logging export using NetFlow:

1. Define a flow exporter and option templates.
2. Attach the flow exporter to a global parameter map.

## Defining a Flow Exporter and Option Templates

In this task you define the flow exporter and then the option templates. You must attach the flow exporter to a parameter map.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *name*
4. **export-protocol netflow-v9**
5. **destination** {*ipv4-address* | *ipv6-address*} [**vrf** *vrf-name*]
6. **transport udp** *port-number*
7. **option inspect-class-table** [**timeout** *timeout-value*]
8. **option inspect-protocol-table** [**timeout** *timeout-value*]
9. **option inspect-ext-event-table** [**timeout** *timeout-value*]
10. **option zone-pair-table** [**timeout** *timeout-value*]
11. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **flow exporter** *name*<br><br>**Example:**<br>`Device(config)# flow exporter v9-flow` | Creates or modifies a Flexible NetFlow flow exporter and enters flow exporter configuration mode. |
| **Step 4** | **export-protocol netflow-v9**<br><br>**Example:**<br>`Device(config-flow-exporter)# export-protocol netflow-v9` | Configures the export protocol for a Flexible NetFlow flow exporter. |
| **Step 5** | **destination** {*ipv4-address* \| *ipv6-address*} [**vrf** *vrf-name*]<br><br>**Example:**<br>`Device(config-flow-exporter)# destination 10.1.1.1` | Configures an export destination for a Flexible NetFlow flow exporter. |
| **Step 6** | **transport udp** *port-number*<br><br>**Example:**<br>`Device(config-flow-exporter)# transport udp 200` | Specifies UDP as the transport protocol for a flow exporter. |
| **Step 7** | **option inspect-class-table** [**timeout** *timeout-value*]<br><br>**Example:**<br>`Device(config-flow-exporter)# option inspect-class-table timeout 2000` | Configures a policy-firewall class table for a flow exporter. |
| **Step 8** | **option inspect-protocol-table** [**timeout** *timeout-value*]<br><br>**Example:**<br>`Device(config-flow-exporter)# option inspect-protocol-table timeout 3000` | Configures a policy-firewall inspect protocol table for a flow exporter. |
| **Step 9** | **option inspect-ext-event-table** [**timeout** *timeout-value*]<br><br>**Example:**<br>`Device(config-flow-exporter)# option inspect-ext-event-table timeout 1200` | Configures a policy-firewall extended event table for a flow exporter. |
| **Step 10** | **option zone-pair-table** [**timeout** *timeout-value*]<br><br>**Example:**<br>`Device(config-flow-exporter)# option zone-pair-table timeout 2500` | Configures a policy-firewall zone-pair table for a flow exporter. |
| **Step 11** | **end**<br><br>**Example:**<br>`Device(config-flow-exporter)# end` | Exits flow exporter configuration mode and returns to privileged EXEC mode. |

# Attaching a Flow Exporter to a Global Parameter Map

You must attach the NetFlow flow exporter (v9-flow) that you configured to a global parameter map. You cannot attach a flow exporter to a default or user-defined parameter map.

**Note** After attaching the flow exporter to a global parameter map, you can configure the **audit-trail** command for a default or user-defined parameter map; log messages will be exported.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **exporter** *exporter-name*
5. **alert** {**on** | **off**}
6. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **parameter-map type inspect global**<br><br>**Example:**<br>`Device(config)# parameter-map type inspect global` | Configures an inspect-type global parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action and enters parameter-map type inspect configuration mode. |
| **Step 4** | **exporter** *exporter-name*<br><br>**Example:**<br>`Device(config-profile)# exporter v9-flow` | Configures a flow exporter.<br>• The flow exporters that you previously configured are listed as options for this command. In this example, you can see v9-flow as an option. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **alert** {**on** \| **off**}<br><br>**Example:**<br>`Device(config-profile)# alert on` | Enables or disables the console display of stateful packet inspection alert messages. |
| **Step 6** | **end**<br><br>**Example:**<br>`Device(config-profile)# end` | Exits parameter-map type inspect configuration mode and returns to global configuration mode. |

# Verifying Zone-Based Firewall Logging Export Using NetFlow

Use the following commands to troubleshoot your configuration:

## SUMMARY STEPS

1. **enable**
2. **debug policy-firewall exporter**
3. **show parameter-map type inspect global**
4. **show flow exporter** *exporter-name* [**statistics** | **templates**]
5. **show flow exporter** {**templates** | **statistics** | **export-ids netflow-v9**}
6. **show running-config flow exporter export-ids netflow-v9**

## DETAILED STEPS

**Step 1** **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

**Example:**
```
Device> enable
```

**Step 2** **debug policy-firewall exporter**
Enables logging of firewall NetFlow Version 9 messages.

**Example:**
```
Device# debug policy-firewall exporter
```

**Step 3** **show parameter-map type inspect global**
Displays global inspect type parameter map values.

**Example:**

```
Device# show parameter-map type inspect global

alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets disabled
  log summary disabled
  max-incomplete low 18000
  max-incomplete high 20000
  one-minute low 2147483647
  one-minute high 2147483647
  tcp reset-PSH disabled
  exporter v9-flow
```

**Step 4** **show flow exporter** *exporter-name* [**statistics** | **templates**]

Displays the status and statistics for the Flexible NetFlow user-configured flow exporter.

**Example:**

```
Device# show flow exporter v9-flow

Flow Exporter v9-flow:
  Description:              User defined
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.1.1.1
    Source IP address:      10.4.5.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            0
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Not Used
```

**Step 5** **show flow exporter** {**templates** | **statistics** | **export-ids netflow-v9**}

Displays flow exporter statistics.

**Example:**

```
Device# show flow exporter statistics

Flow Exporter netflow-v9:
  Packet send statistics (last cleared 00:02:27 ago):
    Successfully sent:         0                     (0 bytes)
    No FIB:                    13                    (16010 bytes)

  Client send statistics:
    Client: Option Start audit v4 (session creation)
      Records added:           0
      Bytes added:             0

    Client: Option Stop audit v4 (session deletion)
      Records added:           0
      Bytes added:             0

    Client: Option Drop audit v4 (Pak drop)
      Records added:           0
      Bytes added:             0

    Client: Option Alert TCP halfopen
      Records added:           0
      Bytes added:             0
```

```
Client: Option Alert halfopen
  Records added:           0
  Bytes added:             0

Client: Option Alert max session
  Records added:           0
  Bytes added:             0

Client: Option Template for FW class-id
  Records added:           2
    - failed to send:      2
  Bytes added:             136
    - failed to send:      136

Client: Option Template for FW protocol-id
  Records added:           172
    - failed to send:      172
  Bytes added:             11696
    - failed to send:      11696

Client: Option Template for FW Extended Event
  Records added:           36
    - failed to send:      36
  Bytes added:             2376
```

**Step 6** **show running-config flow exporter export-ids netflow-v9**
Displays flow exporter configuration.

**Example:**
```
Device# show running-config flow exporter export-ids netflow-v9
```

# Configuration Examples for Zone-Based Firewall Logging Export Using NetFlow

## Example: Defining a Flow Exporter and Option Templates

```
Device# configure terminal
Device(config)# flow exporter v9-flow
Device(config-flow-exporter)# export-protocol netflow-v9
Device(config-flow-exporter)# destination 10.1.1.1
Device(config-flow-exporter)# transport udp 200
Device(config-flow-exporter)# option inspect-class-table timeout 2000
Device(config-flow-exporter)# option inspect-protocol-table timeout 3000
Device(config-flow-exporter)# option inspect-ext-event-table timeout 1200
Device(config-flow-exporter)# option zone-pair-table timeout 2500
Device(config-flow-exporter)# end
```

## Example: Attaching a Flow Exporter to a Global Parameter Map

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# exporter v9-flow
Device(config-profile)# alert on
```

```
Device(config-profile)# end
```

# Additional References for Zone-Based Firewall Logging Export Using NetFlow

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Firewall commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |
| Flexible NetFlow commands | Cisco IOS Flexible NetFlow Command Reference |

### Standards and RFCs

| Standard/RFC | Title |
|---|---|
| RFC 792 | Internet Control Message Protocol |
| RFC 3954 | Cisco Systems NetFlow Services Export Version 9 |
| RFC 6758 | Tunneling of SMTP Message Transfer Priorities |

### MIBs

| MIB | MIBs Link |
|---|---|
| ifIndex | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/support |

# Feature Information for Zone-Based Firewall Logging Export Using NetFlow

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

***Table 11: Feature Information for Zone-Based Firewall Logging Export Using NetFlow***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Zone-Based Firewall Logging Export Using NetFlow | 15.4(2)T | Zone-based firewalls support the logging of messages to an external collector using NetFlow Version 9 export format. NetFlow version 9 export format uses templates to define the format of data that is exported. Template records are sent to collector along with data records, the collector interprets these records by using the structural information available in template.<br>The following commands were introduced or modified by this feature: **debug policy-firewall exporter**, **option (FlexibleNetFlow)**, and **show flow internal**. |