



## CHAPTER 39

# Monitoring the Adaptive Security Appliance

---

This chapter describes how to monitor the adaptive security appliance, and includes the following sections:

- [Using SNMP, page 39-1](#)
- [Configuring and Managing System Logs, page 39-11](#)
- [Configuring and Using NetFlow Secure Event Logging \(NSEL\), page 39-31](#)

## Using SNMP

This section describes how to use SNMP, and includes the following topics:

- [SNMP Overview, page 39-1](#)
- [Enabling SNMP, page 39-9](#)
- [Differences in SNMP Traffic Statistics Output, page 39-10](#)

## SNMP Overview

The adaptive security appliance provides support for network monitoring using SNMP V1 and V2c. The adaptive security appliance supports traps and SNMP read access, but does not support SNMP write access.

You can configure the adaptive security appliance to send traps (event notifications) to an NMS, or you can use the NMS to browse the MIBs on the adaptive security appliance. MIBs are a collection of definitions, and the adaptive security appliance maintains a database of values for each definition. Browsing a MIB entails issuing an SNMP get request from the NMS. Use CiscoWorks for Windows or any other SNMP V1 or V2c, MIB-II-compliant browser to receive SNMP traps and browse a MIB.

[Table 39-1](#) lists supported MIBs and traps for the adaptive security appliance and, in multiple mode, for each context. You can download Cisco MIBs from the following website:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

After you download the MIBs, compile them for your NMS.



### Note

In software Versions 7.2(1), 8.0(2), and later, the SNMP information refreshes about every five seconds. As a result, we recommend that you wait for at least five seconds between consecutive polls.

---

Table 39-1 SNMP MIB and Trap Support

MIB or Trap Support	Description
SNMP core traps	<p>The adaptive security appliance sends the following SNMP core traps:</p> <ul style="list-style-type: none"> <li>• authentication—An SNMP request fails, because the NMS did not authenticate with the correct community string.</li> <li>• linkup—An interface has transitioned to the “up” state.</li> <li>• linkdown—An interface is down, for example, if you removed the <b>nameif</b> command.</li> <li>• coldstart—The adaptive security appliance is running after a reload.</li> </ul>
IF-MIB	<p>The security appliance supports browsing of the following tables:</p> <ul style="list-style-type: none"> <li>• ifXTable, which includes a central lookup for speed of new interface cards.</li> </ul> <p>The following example lists the supported objects:</p> <pre> IF-MIB::ifName.1 = Ge7/0 IF-MIB::ifInMulticastPkts.1 = Counter32: 0 IF-MIB::ifInBroadcastPkts.1 = Counter32: 0 IF-MIB::ifOutMulticastPkts.1 = Counter32: 0 IF-MIB::ifOutBroadcastPkts.1 = Counter32: 0 IF-MIB::ifHCInOctets.1 = Counter64: 231678 IF-MIB::ifHCInUcastPkts.1 = Counter64: 963 IF-MIB::ifHCInMulticastPkts.1 = Counter64: 0 IF-MIB::ifHCInBroadcastPkts.1 = Counter64: 0 IF-MIB::ifHCOutOctets.1 = Counter64: 27251 IF-MIB::ifHCOutUcastPkts.1 = Counter64: 325 IF-MIB::ifHCOutMulticastPkts.1 = Counter64: 0 IF-MIB::ifHCOutBroadcastPkts.1 = Counter64: 0 IF-MIB::ifLinkUpDownTrapEnable.1 = enabled(1) IF-MIB::ifHighSpeed.1 = Gauge32: 10000 (supports 10GE interfaces) IF-MIB::ifPromiscuousMode.1 = false(2) IF-MIB::ifConnectorPresent.1 = true(1) IF-MIB::ifAlias.1 = IF-MIB::ifCounterDiscontinuityTime.1 = Timeticks: (0) 0:00:00.00 </pre> <p>To display equivalent information through the CLI, enter the <b>show interface</b> command.</p>

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
RFC1213-MIB	<p>The security appliance supports browsing of the following table:</p> <ul style="list-style-type: none"> <li>• ip.ipAddrTable</li> <li>• ifTable</li> </ul> <p>The following example lists the supported objects:</p> <pre>RFC1213-MIB::ifNumber.0 = 1 RFC1213-MIB::ifIndex.1 = 1 RFC1213-MIB::ifDescr.1 = "Adaptive Security Appliance 'mgmt' interface" RFC1213-MIB::ifType.1 = ethernet-csmacd(6) RFC1213-MIB::ifMtu.1 = 1500 RFC1213-MIB::ifSpeed.1 = Gauge32: 4294967295 RFC1213-MIB::ifPhysAddress.1 = Hex: 00 15 17 15 AB 08 RFC1213-MIB::ifAdminStatus.1 = up(1) RFC1213-MIB::ifOperStatus.1 = up(1) RFC1213-MIB::ifLastChange.1 = Timeticks: (200) 0:00:02.00 RFC1213-MIB::ifInOctets.1 = Counter32: 231678 RFC1213-MIB::ifInUcastPkts.1 = Counter32: 963 RFC1213-MIB::ifInNUcastPkts.1 = Counter32: 0 RFC1213-MIB::ifInDiscards.1 = Counter32: 630 RFC1213-MIB::ifInErrors.1 = Counter32: 0 RFC1213-MIB::ifOutOctets.1 = Counter32: 27251 RFC1213-MIB::ifOutUcastPkts.1 = Counter32: 325 RFC1213-MIB::ifOutNUcastPkts.1 = Counter32: 0 RFC1213-MIB::ifOutDiscards.1 = Counter32: 0 RFC1213-MIB::ifOutErrors.1 = Counter32: 0 RFC1213-MIB::ifOutQLen.1 = Gauge32: 6 RFC1213-MIB::ifSpecific.1 = OID: SNMPv2-SMI::zeroDotZero</pre> <ul style="list-style-type: none"> <li>• system</li> </ul> <p>The following example lists the supported objects:</p> <pre>RFC1213-MIB::sysDescr.0 = "Cisco Adaptive Security Appliance Version 8.1(0)15" RFC1213-MIB::sysObjectID.0 = OID: CISCO-PRODUCTS-MIB::ciscoASA5580 RFC1213-MIB::sysUpTime.0 = Timeticks: (390500) 1:05:05.00 RFC1213-MIB::sysContact.0 = "username@example.com" RFC1213-MIB::sysName.0 = "sw8-5580" RFC1213-MIB::sysLocation.0 = "YourCity, YourState" RFC1213-MIB::sysServices.0 = 4</pre> <p>To display equivalent information through the CLI, enter the <b>show version</b> command.</p>
SNMPv2-MIB	<p>The adaptive security appliance supports browsing of the following:</p> <ul style="list-style-type: none"> <li>• snmp</li> </ul>

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
ENTITY-MIB	<p>The adaptive security appliance supports browsing of the following groups and tables:</p> <ul style="list-style-type: none"> <li>• entPhysicalTable</li> <li>• entLogicalTable</li> </ul> <p>The following example lists the supported objects:</p> <pre> ENTITY-MIB::entPhysicalDescr.1 = ASA 5580 Series SPE40 or SPE20 ENTITY-MIB::entPhysicalDescr.2 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.3 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.4 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.5 = ASA 5580 Series CPU ENTITY-MIB::entPhysicalDescr.6 = ASA 5580 4 port GE Fiber Interface Card ENTITY-MIB::entPhysicalDescr.7 = ASA 5580 4 port GE Copper Interface Card ENTITY-MIB::entPhysicalDescr.8 = ASA 5580 2 port 10GE SR Fiber Interface Card ENTITY-MIB::entPhysicalVendorType.1 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevChassisASA5580 ENTITY-MIB::entPhysicalVendorType.2 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.3 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.4 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.5 = OID: 0.0 ENTITY-MIB::entPhysicalVendorType.6 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevModuleASA5580Pm4x1geFi ENTITY-MIB::entPhysicalVendorType.7 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevModuleASA5580Pm4x1geCu ENTITY-MIB::entPhysicalVendorType.8 = OID: CISCO-ENTITY-VENDORTYPE-OID-MIB::cevModuleASA5580Pm2x10geFi ENTITY-MIB::entPhysicalContainedIn.1 = 0 ENTITY-MIB::entPhysicalContainedIn.2 = 1 ENTITY-MIB::entPhysicalContainedIn.3 = 1 ENTITY-MIB::entPhysicalContainedIn.4 = 1 ENTITY-MIB::entPhysicalContainedIn.5 = 1 ENTITY-MIB::entPhysicalContainedIn.6 = 1 ENTITY-MIB::entPhysicalContainedIn.7 = 1 ENTITY-MIB::entPhysicalContainedIn.8 = 1 ENTITY-MIB::entPhysicalClass.1 = chassis(3) ENTITY-MIB::entPhysicalClass.2 = cpu(12) ENTITY-MIB::entPhysicalClass.3 = cpu(12) ENTITY-MIB::entPhysicalClass.4 = cpu(12) ENTITY-MIB::entPhysicalClass.5 = cpu(12) ENTITY-MIB::entPhysicalClass.6 = module(9) ENTITY-MIB::entPhysicalClass.7 = module(9) ENTITY-MIB::entPhysicalClass.8 = module(9) ENTITY-MIB::entPhysicalParentRelPos.1 = 0 ENTITY-MIB::entPhysicalParentRelPos.2 = 0 ENTITY-MIB::entPhysicalParentRelPos.3 = 1 ENTITY-MIB::entPhysicalParentRelPos.4 = 2 ENTITY-MIB::entPhysicalParentRelPos.5 = 3 ENTITY-MIB::entPhysicalParentRelPos.6 = 0 ENTITY-MIB::entPhysicalParentRelPos.7 = 0 ENTITY-MIB::entPhysicalParentRelPos.8 = 0 ENTITY-MIB::entPhysicalName.1 = Chassis ENTITY-MIB::entPhysicalName.2 = 0 ENTITY-MIB::entPhysicalName.3 = 1 ENTITY-MIB::entPhysicalName.4 = 2 </pre>

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
ENTITY-MIB (continued)	ENTITY-MIB::entPhysicalName.5 = 3 ENTITY-MIB::entPhysicalName.6 = slot 4 ENTITY-MIB::entPhysicalName.7 = slot 5 ENTITY-MIB::entPhysicalName.8 = slot 7 ENTITY-MIB::entPhysicalHardwareRev.1 = V01 ENTITY-MIB::entPhysicalHardwareRev.2 = ENTITY-MIB::entPhysicalHardwareRev.3 = ENTITY-MIB::entPhysicalHardwareRev.4 = ENTITY-MIB::entPhysicalHardwareRev.5 = ENTITY-MIB::entPhysicalHardwareRev.6 = D5618404 ENTITY-MIB::entPhysicalHardwareRev.7 = D4577407 ENTITY-MIB::entPhysicalHardwareRev.8 = D7555203 ENTITY-MIB::entPhysicalFirmwareRev.1 = 1.1(0)4 ENTITY-MIB::entPhysicalFirmwareRev.2 = ENTITY-MIB::entPhysicalFirmwareRev.3 = ENTITY-MIB::entPhysicalFirmwareRev.4 = ENTITY-MIB::entPhysicalFirmwareRev.5 = ENTITY-MIB::entPhysicalFirmwareRev.6 = ENTITY-MIB::entPhysicalFirmwareRev.7 = ENTITY-MIB::entPhysicalFirmwareRev.8 = ENTITY-MIB::entPhysicalSoftwareRev.1 = 8.1(0)1 ENTITY-MIB::entPhysicalSoftwareRev.2 = ENTITY-MIB::entPhysicalSoftwareRev.3 = ENTITY-MIB::entPhysicalSoftwareRev.4 = ENTITY-MIB::entPhysicalSoftwareRev.5 = ENTITY-MIB::entPhysicalSoftwareRev.6 = ENTITY-MIB::entPhysicalSoftwareRev.7 = ENTITY-MIB::entPhysicalSoftwareRev.8 = ENTITY-MIB::entPhysicalSerialNum.1 = JAB12345678 ENTITY-MIB::entPhysicalSerialNum.2 = ENTITY-MIB::entPhysicalSerialNum.3 = ENTITY-MIB::entPhysicalSerialNum.4 = ENTITY-MIB::entPhysicalSoftwareRev.5 = ENTITY-MIB::entPhysicalSerialNum.6 = 001517154451 ENTITY-MIB::entPhysicalSerialNum.7 = 0015171559DC ENTITY-MIB::entPhysicalSerialNum.8 = 0015171D9752 ENTITY-MIB::entPhysicalMfgName.1 = Cisco Systems Inc. ENTITY-MIB::entPhysicalMfgName.2 = ENTITY-MIB::entPhysicalMfgName.3 = ENTITY-MIB::entPhysicalMfgName.4 = ENTITY-MIB::entPhysicalMfgName.5 = ENTITY-MIB::entPhysicalMfgName.6 = ENTITY-MIB::entPhysicalMfgName.7 = ENTITY-MIB::entPhysicalMfgName.8 = ENTITY-MIB::entPhysicalMfgName.9 = ENTITY-MIB::entPhysicalModelName.1 = ASA5580-SPE40 or SPE20 ENTITY-MIB::entPhysicalModelName.2 = ENTITY-MIB::entPhysicalModelName.3 = ENTITY-MIB::entPhysicalModelName.4 = ENTITY-MIB::entPhysicalModelName.5 = ENTITY-MIB::entPhysicalModelName.6 = ASA5580-4GE-FI ENTITY-MIB::entPhysicalModelName.7 = ASA5580-4GE-CU ENTITY-MIB::entPhysicalModelName.8 = ASA5580-2X10GE-SR ENTITY-MIB::entPhysicalAlias.1 = ENTITY-MIB::entPhysicalAlias.2 = ENTITY-MIB::entPhysicalAlias.3 = ENTITY-MIB::entPhysicalAlias.4 = ENTITY-MIB::entPhysicalAlias.5 = ENTITY-MIB::entPhysicalAlias.6 = ENTITY-MIB::entPhysicalAlias.7 =

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
ENTITY-MIB (continued)	<p>ENTITY-MIB::entPhysicalAlias.8 =            ENTITY-MIB::entPhysicalAssetID.1 =            ENTITY-MIB::entPhysicalAssetID.2 =            ENTITY-MIB::entPhysicalAssetID.3 =            ENTITY-MIB::entPhysicalAssetID.8 =            ENTITY-MIB::entPhysicalIsFRU.1 = false(2)            ENTITY-MIB::entPhysicalIsFRU.2 = false(2)            ENTITY-MIB::entPhysicalIsFRU.4 = false(2)            ENTITY-MIB::entPhysicalIsFRU.5 = false(2)            ENTITY-MIB::entPhysicalIsFRU.6 = true(1)            ENTITY-MIB::entPhysicalIsFRU.7 = true(1)            ENTITY-MIB::entPhysicalIsFRU.8 = true(1)</p> <p>To display equivalent information through the CLI, enter the <b>show controller</b> and <b>show inventory</b> commands.</p> <p>The adaptive security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• config-change</li> <li>• fru-insert</li> <li>• fru-remove</li> </ul>
CISCO-IPSEC-FLOW-MONITOR-MIB	<p>The adaptive security appliance supports browsing of the MIB.</p> <p>The adaptive security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• start</li> <li>• stop</li> </ul>
CISCO-REMOTE-ACCESS-MONITOR-MIB	<p>The adaptive security appliance supports browsing of the MIB.</p> <p>The adaptive security appliance supports browsing of the following traps:</p> <ul style="list-style-type: none"> <li>• session-threshold-exceeded</li> </ul>
CISCO-CRYPTO-ACCELERATOR-MIB	<p>The adaptive security appliance supports browsing of the MIB.</p>
ALTIGA-GLOBAL-REG	<p>The adaptive security appliance supports browsing of the MIB.</p>
CISCO-FIREWALL-MIB	<p>The adaptive security appliance supports browsing of the following groups:</p> <ul style="list-style-type: none"> <li>• cfwSystem</li> </ul> <p>The information in cfwSystem.cfwStatus, which relates to failover status, applies to the entire device and not only a single context.</p>

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
CISCO-MEMORY-POOL-MIB	<p>The adaptive security appliance supports browsing of the following table:</p> <ul style="list-style-type: none"> <li>• <code>ciscoMemoryPoolTable</code>—The memory usage described in this table applies only to the adaptive security appliance general-purpose processor, and not to the network processors. Multiple rows are present; the first row (with index .1) reflects system memory usage. Subsequent rows (dynamic, starting with index .6) reflect optimizations made that are associated with the ASA 5580 hardware.</li> </ul> <p>The following example lists the supported objects:</p> <pre> CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.1 = System memory CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.6 = DMA ALT1 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.7 = DMA CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolName.8 = Global Shared CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.1 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.6 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.7 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolAlternate.8 = 0 CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.1 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.6 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.7 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolValid.8 = true(1) CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.1 = Gauge32: 102805792 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.6 = Gauge32: 32012672 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.7 = Gauge32: 32012672 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolUsed.8 = Gauge32: 38752248 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.1 = Gauge32: 1432686304 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.6 = Gauge32: 198862416 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.7 = Gauge32: 198862416 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolFree.8 = Gauge32: 229683208 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.1 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.6 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.7 = Gauge32: 0 bytes CISCO-MEMORY-POOL-MIB::ciscoMemoryPoolLargestFree.8 = Gauge32: 0 bytes </pre> <p>To display equivalent information through the CLI, enter the <b>show memory detail</b> command.</p>

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
CISCO-PROCESS- MIB	<p>The adaptive security appliance supports browsing of the following table:</p> <ul style="list-style-type: none"> <li>• <b>cpmCPUTotalTable</b>—This table includes the starting and ending number of CPU cores, which are set during initialization and remain until the next reboot. Multiple rows are present; the first row (with index .1) reflects the system CPU usage. Subsequent rows (with index .2 through .5 or .2 through .9) reflect per-core CPU usage. The last row (with index .6 or .10) reflects aggregate system CPU usage. The <b>PhysicalIndex</b> object maps to a corresponding row in the ENTITY-MIB.</li> </ul> <p>The following example lists the supported objects:</p> <pre> CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.1 = 1 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.2 = 2 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.3 = 3 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.4 = 4 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.5 = 5 CISCO-PROCESS-MIB::cpmCPUTotalPhysicalIndex.6 = 1 CISCO-PROCESS-MIB::cpmCPUTotal5sec.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5sec.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal5sec.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal5sec.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5sec.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5sec.6 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal1min.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal1min.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal1min.6 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.1 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.2 = Gauge32: 100 CISCO-PROCESS-MIB::cpmCPUTotal5min.3 = Gauge32: 0 CISCO-PROCESS-MIB::cpmCPUTotal5min.4 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.5 = Gauge32: 50 CISCO-PROCESS-MIB::cpmCPUTotal5min.6 = Gauge32: 50 </pre> <p>The first row in <b>cpmCPUTotalTable</b> reflects the system CPU usage in single security context mode, or the security context CPU usage in multiple mode. The last row in <b>cpmCPUTotalTable</b> always reflects the system CPU usage. In single mode, this value is identical to the first row. In multiple mode, this row is only available through the admin context and represents the aggregate system CPU usage, which is equivalent to entering the <b>show cpu usage core_id</b> command. All rows in-between the first and last reflect the per-core CPU usage. They are only present for multi-CPU systems and only available in single mode or the admin context in multiple mode.</p> <p><b>Note</b> The adaptive security appliance implements the legal values for these objects, which range from 1 through 100. The adaptive security appliance returns valid data for the MIB, although the data does not match the CLI output.</p>

Table 39-1 SNMP MIB and Trap Support (continued)

MIB or Trap Support	Description
CISCO-SYSLOG-MIB	The adaptive security appliance supports the following trap: <ul style="list-style-type: none"> <li>clogMessageGenerated</li> </ul> You cannot browse this MIB.
CISCO-UNIFIED-FIREWALL-MIB	The adaptive security appliance supports browsing of the following tables: <ul style="list-style-type: none"> <li>cuFwConnectionGlobals</li> <li>cufwUrFilterGlobals</li> <li>cufwUrFilterServers</li> </ul>

## Enabling SNMP

The SNMP agent that runs on the adaptive security appliance performs two functions:

- Replies to SNMP requests from NMSs.
- Sends traps (event notifications) to NMSs.

To enable the SNMP agent and identify an NMS that can connect to the adaptive security appliance, perform the following steps:

- Step 1** Ensure that the SNMP server on the adaptive security appliance is enabled by entering the following command:

```
hostname(config)# snmp-server enable
```

The SNMP server is enabled by default.

- Step 2** To identify the IP address of the NMS that can connect to the adaptive security appliance, enter the following command:

```
hostname(config)# snmp-server host interface_name ip_address [trap | poll] [community text] [version 1 | 2c] [udp-port port]
```

where *interface\_name* is the name of the NMS and *ip\_address* is the IP address of the NMS.

Specify **trap** or **poll** if you want to limit the NMS to receiving traps only or browsing (polling) only. By default, the NMS can use both functions.

SNMP traps are sent on UDP port 162 by default. You can change the port number using the **udp-port** keyword.

- Step 3** To specify the community string, enter the following command:

```
hostname(config)# snmp-server community key
```

The SNMP community string is a shared secret between the adaptive security appliance and the NMS. The key is a case-sensitive value up to 32 characters long. Spaces are not permitted.

- Step 4** (Optional) To set the SNMP server location or contact information, enter the following command:

```
hostname(config)# snmp-server {contact | location} text
```

where *text* defines the SNMP server location or lists contact information.

- Step 5** To enable the adaptive security appliance to send traps to the NMS, enter the following command:

```
hostname(config)# snmp-server enable traps [all | syslog | snmp [trap] [...] |
entity [trap] [...] | ipsec [trap] [...] | remote-access [trap]]
```

Enter this command for each feature type to enable individual traps or sets of traps, or enter the **all** keyword to enable all traps.

The default configuration has all SNMP core traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart**). You can disable these traps using the **no** form of this command with the **snmp** keyword. However, use the **clear configure snmp-server** command to restore the default enabling of SNMP traps.

If you enter this command and do not specify a trap type, then the default is the syslog trap. (The default SNMP traps continue to be enabled along with the syslog trap.)

**Step 6** To enable syslog messages to be sent as traps to the NMS, enter the following command:

```
hostname(config)# logging history level
```

where *level* defines the logging severity level.

You must also enable syslog traps using the **snmp-server enable traps** command.

**Step 7** To enable logging, so that system messages are generated and can then be sent to an NMS, enter the following command:

```
hostname(config)# logging enable
```

---

The following example sets the adaptive security appliance to receive requests from host 192.168.3.2 on the inside interface:

```
hostname(config)# snmp-server host 192.168.3.2
hostname(config)# snmp-server location building 42
hostname(config)# snmp-server contact system administrator
hostname(config)# snmp-server community ohwhatakeyisthee
```

## Differences in SNMP Traffic Statistics Output

For the ASA 5580, differences may appear in the physical interface statistics output and the logical interface statistics output between the **show interface** command and **show traffic** command.

## Interface Types and Examples

The interface types that produce SNMP traffic statistics include the following:

- Logical—Statistics collected by the software driver, which are a subset of physical statistics.
- Physical—Statistics collected by the hardware driver. Each physical named interface has a set of logical and physical statistics associated with it. Each physical interface may have more than one VLAN interface associated with it. VLAN interfaces only have logical statistics. For a physical interface that has multiple VLAN interfaces associated with it, be aware of the following:




---

**Note** For a physical interface that has multiple VLAN interfaces associated with it, note that SNMP counters for ifInOctets and ifOutOctets OIDs match the aggregate traffic counters for that physical interface.

---

- VLAN-only—SNMP uses logical statistics for ifInOctets and ifOutOctets.

The examples in [Table 39-2](#) show the differences in SNMP traffic statistics.

**Table 39-2** *SNMP Traffic Statistics for Physical and VLAN Interfaces*

Example 1	Example 2
<p>The following example shows the difference in physical and logical output statistics for the <b>show interface</b> command and the <b>show traffic</b> command.</p> <pre>hostname#show interface GigabitEthernet3/2 interface GigabitEthernet3/2   description fullt-mgmt   nameif mgmt   security-level 10   ip address 10.7.14.201 255.255.255.0   management-only  hostname#show traffic (Condensed output)  Physical Statistics GigabitEthernet3/2:   received (in 121.760 secs)     36 packets      3428 bytes     0 pkts/sec      28 bytes/sec  Logical Statistics mgmt:   received (in 117.780 secs)     36 packets      2780 bytes     0 pkts/sec      23 bytes/sec</pre> <p>The following examples show the SNMP output statistics for the management interface and the physical interface. The ifInOctets value is close to the physical statistics output that appears in the <b>show traffic</b> command output, but not to the logical statistics output.</p> <p>ifIndex of the mgmt interface:</p> <pre>IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface</pre> <p>ifInOctets that corresponds to the physical interface statistics:</p> <pre>IF-MIB::ifInOctets.6 = Counter32:3246</pre>	<p>The following example shows output statistics for a VLAN-only interface for the <b>show interface</b> command and the <b>show traffic</b> command. The example shows that the statistics are close to the output that appears for the <b>show traffic</b> command:</p> <pre>hostname# show interface GigabitEthernet0/0.100 interface GigabitEthernet0/0.100   vlan 100   nameif inside   security-level 100   ip address 47.7.1.101 255.255.255.0 standby   47.7.1.102  hostname#show traffic inside   received (in 9921.450 secs)     1977 packets      126528 bytes     0 pkts/sec        12 bytes/sec   transmitted (in 9921.450 secs)     1978 packets      126556 bytes     0 pkts/sec        12 bytes/sec</pre> <p>ifIndex of VLAN inside:</p> <pre>IF-MIB::ifDescr.9 = Adaptive Security Appliance 'inside' interface IF-MIB::ifInOctets.9 = Counter32: 126318</pre>

## Configuring and Managing System Logs



### Note

This section does not apply to the system logging functionality and configuration through UDP for NetFlow. For more information, see [Configuring and Using NetFlow Secure Event Logging \(NSEL\)](#), page 39-31.

This section describes the logging functionality and configuration, as well as the syslog message format, options, and variables. It includes the following topics:

- [System Logging Overview, page 39-12](#)
- [Enabling and Disabling System Logging, page 39-13](#)

## System Logging Overview

The adaptive security appliance system logs provide you with information for monitoring and troubleshooting the adaptive security appliance. With the system logging feature, you can do the following:

- Specify which syslog messages should be logged.
- Disable or change the severity level of a syslog message.
- Specify one or more locations where syslog messages should be sent, including an internal buffer, one or more syslog servers, ASDM, an SNMP management station, specified e-mail addresses, or to Telnet and SSH sessions.
- Configure and manage syslog messages in groups, such as by severity level or class of message.
- Specify whether a rate-limit is applied to syslog message generation.
- Specify what happens to the contents of the internal buffer when the buffer becomes full: overwrite the buffer, send the buffer contents to an FTP server, or save the contents to internal flash memory.

You can choose to send all syslog messages, or subsets of syslog messages, to any or all output locations. You can filter syslog messages by locations, by the severity of the syslog message, the class of the syslog message, or by creating a customized message list.

## System Logging in Multiple Context Mode

Each security context includes its own system logging configuration and generates its own syslog messages. If you log in to the system or admin context, and then change to another context, syslog messages you view in your session are only those that are related to the current context.

Syslog messages that are generated in the system execution space, including failover messages, are viewed in the admin context along with messages generated in the admin context. You cannot configure system logging or view any system logging information in the system execution space.

You can configure the adaptive security appliance to include the context name with each syslog message, which helps you differentiate context messages that are sent to a single syslog server. This feature also helps you to determine which messages are from the admin context and which are from the system; messages that originate in the system execution space use a device ID of *system*, and messages that originate in the admin context use the name of the admin context as the device ID. For more information about enabling logging device IDs, see the [“Including the Device ID in Syslog Messages”](#) section on page 39-26.

## Enabling and Disabling System Logging

This section describes how to enable and disable system logging on the adaptive security appliance and includes the following topics:

- [Enabling System Logging to All Configured Output Destinations](#), page 39-13
- [Disabling System Logging to All Configured Output Destinations](#), page 39-13
- [Viewing the System Log Configuration](#), page 39-13

### Enabling System Logging to All Configured Output Destinations

The following command enables system logging; however, you must also specify at least one output destination so that you can view or save the logged messages. If you do not specify an output destination, the adaptive security appliance does not save syslog messages generated when events occur.

For more information about configuring system log output destinations, see the “[Configuring System Log Output Destinations](#)” section on page 39-14.

To enable system logging, enter the following command:

```
hostname(config)# logging enable
```

### Disabling System Logging to All Configured Output Destinations

To disable all system logging to all configured system log output destinations, enter the following command:

```
hostname(config)# no logging enable
```

### Viewing the System Log Configuration

To view the running system log configuration, enter the following command:

```
hostname(config)# show logging
```

The following is sample output from the **show logging** command:

```
Syslog logging: enabled
  Facility: 16
  Timestamp logging: disabled
  Standby logging: disabled
  Deny Conn when Queue Full: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled
  Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.2.3
  History logging: disabled
  Device ID: 'inside' interface IP address "10.1.1.1"
  Mail logging: disabled
  ASDM logging: disabled
```

## Configuring System Log Output Destinations

This section describes how to specify where the adaptive security appliance should save or send the syslog messages that are generated, and includes the following topics:

- [Sending Syslog Messages to a Syslog Server, page 39-14](#)
- [Sending Syslog Messages to the Console Port, page 39-15](#)
- [Sending Syslog Messages to an E-mail Address, page 39-16](#)
- [Sending Syslog Messages to ASDM, page 39-17](#)
- [Sending Syslog Messages to a Telnet or SSH Session, page 39-19](#)
- [Sending Syslog Messages to the Log Buffer, page 39-20](#)

### Sending Syslog Messages to a Syslog Server

This section describes how to configure the adaptive security appliance to send syslog messages to a syslog server.

Configuring the adaptive security appliance to send syslog messages to a syslog server enables you to archive logs, limited only by the available disk space on the server, and to manipulate log data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

To view syslog messages generated by the adaptive security appliance, you must specify a syslog message output destination. If you enable system logging without specifying a syslog message output destination, the adaptive security appliance generates messages, but does not save them to a location from which you can view them.

The syslog server must run a server program called “syslogd.” Windows (except for Windows 95 and Windows 98) provides a syslog server as part of its operating system. For Windows 95 and Windows 98, you must obtain a syslogd server from another vendor.



#### Note

To start system logging to a syslog server that you define in this procedure, be sure to enable system logging for all output locations. See the [“Enabling System Logging to All Configured Output Destinations”](#) section on page 39-13. To disable system logging, see the [“Disabling System Logging to All Configured Output Destinations”](#) section on page 39-13.

To configure the adaptive security appliance to send syslog messages to a syslog server, perform the following steps:

**Step 1** To designate a syslog server to receive the syslog messages, enter the following command:

```
hostname(config)# logging host interface_name ip_address [tcp[/port] | udp[/port]]
[format emblem]
```

where the **format emblem** keyword enables EMBLEM format logging for the syslog server (UDP only).

The *interface\_name* argument specifies the interface through which you access the syslog server.

The *ip\_address* argument specifies the IP address of the syslog server.

The `tcp[/port]` or `udp[/port]` argument specifies that the adaptive security appliance should use TCP or UDP to send syslog messages to the syslog server. The default protocol is UDP. You can configure the adaptive security appliance to send data to a syslog server using either UDP or TCP, but not both. If you specify TCP, the adaptive security appliance discovers when the syslog server fails and discontinues sending syslog messages. If you specify UDP, the adaptive security appliance continues to send syslog messages, regardless of whether the syslog server is operational. The `port` argument specifies the port that the syslog server listens to for syslog messages. Valid port values are 1025 through 65535, for either protocol. The default UDP port is 514. The default TCP port is 1470.

For example:

```
hostname(config)# logging host dmz1 192.168.1.5
```

If you want to designate more than one syslog server as an output destination, enter a new command for each syslog server.

- Step 2** To specify which syslog messages should be sent to the syslog server, enter the following command:

```
hostname(config)# logging trap {severity_level | message_list}
```

where the `severity_level` argument specifies the severity levels of syslog messages to be sent to the syslog server. You can specify the severity level number (0 through 7) or name. For severity level descriptions, see the [“Severity Levels” section on page 39-31](#). For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, 1, and 0.

The `message_list` argument specifies a customized message list that identifies the syslog messages to send to the syslog server. For information about creating custom message lists, see the [“Filtering Syslog Messages with Custom Message Lists” section on page 39-24](#).

The following example specifies that the adaptive security appliance should send to the syslog server all syslog messages with a severity level of 3 (errors) and higher. The adaptive security appliance will send syslog messages with the severity levels of 3, 2, and 1.

```
hostname(config)# logging trap errors
```

- Step 3** (Optional) If needed, to continue TCP logging when the syslog server is down, enter the following command:

```
hostname(config)# logging permit-hostdown
```

- Step 4** (Optional) If needed, set the logging facility to a value other than its default of 20 by entering the following command:

```
hostname(config)# logging facility number
```

Most UNIX systems expect the syslog messages to arrive at facility 20.

---

## Sending Syslog Messages to the Console Port

This section describes how to configure the adaptive security appliance to send syslog messages to the console port.



### Note

To start system logging to the console port as defined in this procedure, be sure to enable system logging for all output locations. See the [“Enabling System Logging to All Configured Output Destinations” section on page 39-13](#). To disable logging, see the [“Disabling System Logging to All Configured Output Destinations” section on page 39-13](#).

To specify which syslog messages should be sent to the console port, enter the following command:

```
hostname(config)# logging console {severity_level | message_list}
```

where the *severity\_level* argument specifies the severity levels of messages to be sent to the console port. You can specify the severity level number (0 through 7) or name. For severity level descriptions, see the “Severity Levels” section on page 39-31. For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for levels 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the syslog messages to send to the console port. For information about creating custom message lists, see the “Filtering Syslog Messages with Custom Message Lists” section on page 39-24.

The following example specifies that the adaptive security appliance should send to the syslog server all syslog messages with a severity level of 3 (errors) and higher. The adaptive security appliance will send messages with the severity levels of 3, 2, and 1.

```
hostname(config)# logging console errors
```

## Sending Syslog Messages to an E-mail Address

You can configure the adaptive security appliance to send some or all syslog messages to an e-mail address. When sent by e-mail, a syslog message appears in the subject line of the e-mail message. For this reason, we recommend configuring this option to notify administrators of syslog messages with high severity levels, such as critical, alert, and emergency.



### Note

To start system logging to an e-mail address you define in this procedure, be sure to enable logging for all output locations. See the “Enabling System Logging to All Configured Output Destinations” section on page 39-13. To disable logging, see the “Disabling System Logging to All Configured Output Destinations” section on page 39-13.

To designate an e-mail address as an output destination, perform the following steps:

**Step 1** To specify the syslog messages to be sent to one or more e-mail addresses, enter the following command:

```
hostname(config)# logging mail {severity_level | message_list}
```

where the *severity\_level* argument specifies the severity levels of syslog messages to be sent to the e-mail address. You can specify the severity level number (0 through 7) or name. For severity level names, see the “Severity Levels” section on page 39-31. For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the syslog messages to send to the e-mail address. For information about creating custom message lists, see the “Filtering Syslog Messages with Custom Message Lists” section on page 39-24.

The following example uses a *message\_list* with the name “high-priority,” previously configured with the **logging list** command:

```
hostname(config)# logging mail high-priority
```

**Step 2** To specify the source e-mail address to be used when sending syslog messages to an e-mail address, enter the following command:

```
hostname(config)# logging from-address email_address
```

For example:

```
hostname(config)# logging from-address xxx-001@example.com
```

- Step 3** Specify the recipient e-mail address to be used when sending syslog messages to an e-mail destination. You can configure up to five recipient addresses. You must enter each recipient separately.

To specify a recipient address, enter the following command:

```
hostname(config)# logging recipient-address e-mail_address [severity_level]
```

If a severity level is not specified, the default severity level is used (error condition, severity level 3).

For example:

```
hostname(config)# logging recipient-address admin@example.com
```

- Step 4** To specify the SMTP server to be used when sending syslog messages to an e-mail destination, enter the following command:

```
hostname(config)# smtp-server ip_address
```

For example:

```
hostname(config)# smtp-server 10.1.1.1
```

---

## Sending Syslog Messages to ASDM

You can configure the adaptive security appliance to send syslog messages to ASDM. The adaptive security appliance sets aside a buffer area for syslog messages waiting to be sent to ASDM and saves messages in the buffer as they occur. The ASDM log buffer is a different buffer than the internal log buffer. For information about the internal log buffer, see the [“Sending Syslog Messages to the Log Buffer”](#) section on page 39-20.

When the ASDM log buffer is full, the adaptive security appliance deletes the oldest syslog message to make room in the buffer for new syslog messages. To control the number of syslog messages retained in the ASDM log buffer, you can change the size of the buffer.

This section includes the following topics:

- [Configuring System Logging for ASDM, page 39-17](#)
- [Configuring Secure System Logging, page 39-18](#)
- [Clearing the ASDM Log Buffer, page 39-19](#)

## Configuring System Logging for ASDM



### Note

To start system logging to ASDM as defined in this procedure, be sure to enable system logging for all output locations. See the [“Enabling System Logging to All Configured Output Destinations”](#) section on page 39-13. To disable logging, see the [“Disabling System Logging to All Configured Output Destinations”](#) section on page 39-13.

---

To specify ASDM as an output destination, perform the following steps:

**Step 1** To specify which syslog messages should go to ASDM, enter the following command:

```
hostname(config)# logging asdm {severity_level | message_list}
```

where the *severity\_level* argument specifies the severity levels of syslog messages to be sent to ASDM. You can specify the severity level number (0 through 7) or name. For severity level names, see the “Severity Levels” section on page 39-31. For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, 1, and 0.

The *message\_list* argument specifies a customized message list that identifies the syslog messages to send to ASDM. For information about creating custom message lists, see the “Filtering Syslog Messages with Custom Message Lists” section on page 39-24.

The following example shows how to enable logging and send syslog messages of severity levels 0, 1, and 2 to the ASDM log buffer:

```
hostname(config)# logging asdm 2
```

**Step 2** To specify the number of syslog messages retained in the ASDM log buffer, enter the following command:

```
hostname(config)# logging asdm-buffer-size num_of_msgs
```

where *num\_of\_msgs* specifies the number of syslog messages that the adaptive security appliance retains in the ASDM log buffer.

The following example shows how to set the ASDM log buffer size to 200 syslog messages:

```
hostname(config)# logging asdm-buffer-size 200
```

## Configuring Secure System Logging



### Note

You must use TCP only. Secure system logging does not support UDP; an error occurs if you try to use this protocol.

To enable secure system logging, enter the following command:

```
hostname(config)# logging host interface_name syslog_ip [tcp/port | udp/port] [format emblem] [secure]
```

where the *interface\_name* argument specifies the interface on which the syslog server resides, the *syslog\_ip* argument specifies the IP address of the syslog server, and the *port* argument specifies the port (TCP or UDP) that the syslog server listens to for syslog messages.

The **tcp** keyword specifies that the adaptive security appliance should use TCP to send syslog messages to the syslog server. The **udp** keyword specifies that the adaptive security appliance should use UDP to send syslog messages to the syslog server. The **format emblem** keyword enables EMBLEM format logging for the syslog server. The **secure** keyword specifies that the connection to the remote logging host should use SSL/TLS for TCP only.

The following example shows how to set up secure system logging:

```
hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure
```

## Clearing the ASDM Log Buffer

To erase the current contents of the ASDM log buffer, enter the following command:

```
hostname(config)# clear logging asdm
```

## Sending Syslog Messages to a Telnet or SSH Session

Viewing syslog messages in a Telnet or SSH session requires two steps:

1. Specify which syslog messages should be sent to Telnet or SSH sessions.
2. View syslog messages in the current session.

This section includes the following topics:

- [Configuring System Logging for Telnet and SSH Sessions, page 39-19](#)
- [Viewing Syslog Messages in the Current Session, page 39-19](#)

## Configuring System Logging for Telnet and SSH Sessions



### Note

To start system logging to a Telnet or SSH session as defined in this procedure, be sure to enable logging for all output locations. See the [“Enabling System Logging to All Configured Output Destinations” section on page 39-13](#). To disable logging, see the [“Disabling System Logging to All Configured Output Destinations” section on page 39-13](#).

To specify which syslog messages should be sent to Telnet or SSH sessions, enter the following command:

```
hostname(config)# logging monitor {severity_level | message_list}
```

where the *severity\_level* argument specifies the severity levels of syslog messages to be sent to the session. You can specify the severity level number (0 through 7) or name. For severity level names, see the [“Severity Levels” section on page 39-31](#). For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, 1, and 0.

The *message\_list* argument specifies a custom message list that identifies the syslog messages to send to the session. For information about creating custom message lists, see the [“Filtering Syslog Messages with Custom Message Lists” section on page 39-24](#).

## Viewing Syslog Messages in the Current Session

To view syslog messages in the current session, perform the following steps:

- Step 1** After you log in to the adaptive security appliance, enable system logging to the current session by entering the following command:

```
hostname# terminal monitor
```

This command enables system logging only for the current session. If you log out, and then log in again, you need to reenter this command.

- Step 2** To disable system logging to the current session, enter the following command:

```
hostname(config)# terminal no monitor
```

## Sending Syslog Messages to the Log Buffer

If configured as an output destination, the log buffer serves as a temporary storage location for syslog messages. New syslog messages are appended to the end of the listing. When the buffer is full, that is, when the buffer wraps, old messages are overwritten as new messages are generated, unless you configure the adaptive security appliance to save the full buffer to another location.

This section includes the following topics:

- [Enabling the Log Buffer as an Output Destination, page 39-20](#)
- [Viewing the Log Buffer, page 39-21](#)
- [Automatically Saving the Full Log Buffer to Flash Memory, page 39-21](#)
- [Automatically Saving the Full Log Buffer to an FTP Server, page 39-21](#)
- [Saving the Current Contents of the Log Buffer to Internal Flash Memory, page 39-22](#)
- [Clearing the Contents of the Log Buffer, page 39-22](#)

### Enabling the Log Buffer as an Output Destination



#### Note

To start system logging to the buffer as defined in this procedure, be sure to enable system logging for all output locations. See the [“Enabling System Logging to All Configured Output Destinations” section on page 39-13](#). To disable logging, see the [“Disabling System Logging to All Configured Output Destinations” section on page 39-13](#).

To enable the log buffer as a syslog message output destination, enter the following command:

```
hostname(config)# logging buffered {severity_level | message_list}
```

where the *severity\_level* argument specifies the severity levels of messages to be sent to the buffer. You can specify the severity level number (0 through 7) or name. For severity level names, see the [“Severity Levels” section on page 39-31](#). For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, 1, and 0.

The *message\_list* argument specifies a custom message list that identifies the syslog messages to send to the buffer. For information about creating custom message lists, see the [“Filtering Syslog Messages with Custom Message Lists” section on page 39-24](#).

For example, to specify that messages with severity levels 1 and 2 should be saved in the log buffer, enter one of the following commands:

```
hostname(config)# logging buffered critical
```

or

```
hostname(config)# logging buffered level 2
```

For the *message\_list* option, specify the name of a message list containing criteria for selecting messages to be saved in the log buffer.

```
hostname(config)# logging buffered notif-list
```

## Viewing the Log Buffer

To view the log buffer, enter the following command:

```
hostname(config)# show logging
```

## Changing the Log Buffer Size

By default, the log buffer size is 4 KB. To change the size of the log buffer, enter the following command:

```
hostname(config)# logging buffer-size bytes
```

where the *bytes* argument sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the adaptive security appliance uses 8 KB of memory for the log buffer.

The following example specifies that the adaptive security appliance uses 16 KB of memory for the log buffer:

```
hostname(config)# logging buffer-size 16384
```

## Automatically Saving the Full Log Buffer to Flash Memory

Unless configured otherwise, the adaptive security appliance sends messages to the log buffer on a continuing basis, overwriting old messages when the buffer is full. If you want to keep a history of logs, you can configure the adaptive security appliance to send the buffer contents to another output location each time the buffer fills. Buffer contents can be saved either to internal flash memory or to an FTP server.

When saving the buffer content to another location, the adaptive security appliance creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

While the adaptive security appliance writes the log buffer contents to internal flash memory or an FTP server, the adaptive security appliance continues saving new messages to the log buffer.

To specify that messages in the log buffer should be saved to internal flash memory each time the buffer wraps, enter the following command:

```
hostname(config)# logging flash-bufferwrap
```

## Automatically Saving the Full Log Buffer to an FTP Server

See the [“Saving the Current Contents of the Log Buffer to Internal Flash Memory”](#) section for more information about saving the buffer.

To specify that messages in the log buffer should be saved to an FTP server each time the buffer wraps, perform the following steps:

- 
- Step 1** To enable the adaptive security appliance to send the log buffer contents to an FTP server every time the buffer wraps, enter the following command:
- ```
hostname(config)# logging ftp-bufferwrap
```
- Step 2** To identify the FTP server, entering the following command:

```
hostname(config)# logging ftp-server server path username password
```

where the *server* argument specifies the IP address of the external FTP server.

The *path* argument specifies the directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory.

The *username* argument specifies a username that is valid for logging into the FTP server.

The *password* argument specifies the password for the username specified.

For example:

```
hostname(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
```

---

### Saving the Current Contents of the Log Buffer to Internal Flash Memory

At any time, you can save the contents of the buffer to internal flash memory. To save the current contents of the log buffer to internal flash memory, enter the following command:

```
hostname(config)# logging savelog savefile
```

For example, the following example saves the contents of the log buffer to internal flash memory using the filename, latest-logfile.txt:

```
hostname(config)# logging savelog latest-logfile.txt
```

### Clearing the Contents of the Log Buffer

To erase the contents of the log buffer, enter the following command:

```
hostname(config)# clear logging buffer
```

## Filtering Syslog Messages

This section describes how to specify which syslog messages should go to output destinations, and includes the following topics:

- [Message Filtering Overview, page 39-22](#)
- [Filtering Syslog Messages by Class, page 39-23](#)
- [Filtering Syslog Messages with Custom Message Lists, page 39-24](#)

### Message Filtering Overview

You can filter generated syslog messages so that only certain syslog messages are sent to a particular output destination. For example, you could configure the adaptive security appliance to send all syslog messages to one output destination and to send a subset of those syslog messages to a different output destination.

Specifically, you can configure the adaptive security appliance so that syslog messages are directed to an output destination according to the following criteria:

- Syslog message ID number
- Syslog message severity level

- Syslog message class (equivalent to a functional area of the adaptive security appliance)

You customize these criteria by creating a message list that you can specify when you set the output destination in the [“Configuring System Log Output Destinations”](#) section on page 39-14. Alternatively, you can configure the adaptive security appliance to send a particular message class to each type of output destination independently of the syslog message list.

For example, you could configure the adaptive security appliance to send to the internal log buffer all syslog messages with severity levels of 1, 2 and 3, send all syslog messages in the “ha” class to a particular syslog server, or create a list of messages that you define as “high-priority” that are sent to an e-mail address to notify system administrators of a possible problem.

## Filtering Syslog Messages by Class

The syslog message class provides a method of categorizing syslog messages by type, equivalent to a feature or function of the adaptive security appliance. For example, the “vpnc” class denotes the VPN client.

This section includes the following topics:

- [Message Class Overview, page 39-23](#)
- [Sending All Syslog Messages in a Class to a Specified Output Destination, page 39-23](#)

### Message Class Overview

With logging classes, you can specify an output location for an entire category of syslog messages with a single command.

You can use syslog message classes in two ways:

- Issue the **logging class** command to specify an output location for an entire category of syslog messages.
- Create a message list using the **logging list** command that specifies the message class. See the [“Filtering Syslog Messages with Custom Message Lists”](#) section on page 39-24 for this method.

All syslog messages in a particular class share the same initial three digits in their syslog message ID numbers. For example, all syslog message IDs that begin with the digits 611 are associated with the vpnc (VPN client) class. Syslog messages associated with the VPN client feature range from 611101 to 611323.

In addition, most of the ISAKMP syslog messages have a common set of prepended objects to help identify the tunnel. These objects precede the descriptive text of a syslog message when available. If the object is not known at the time the syslog message is generated, the specific “*heading = value*” combination will not be displayed.

The objects will be prepended as follows:

“Group = *groupname*, Username = *user*, IP = *IP\_address*, ...”

Where the group identifies the tunnel-group, the username is the username from the local database or AAA server, and the IP address is the public IP address of the remote access client or L2L peer.

### Sending All Syslog Messages in a Class to a Specified Output Destination

When you configure all messages in a class to go to a type of output destination, this configuration overrides the configuration in the specific output destination command. For example, if you specify that messages at level 7 should go to the log buffer, and you also specify that ha class messages at level 3 should go to the buffer, then the latter configuration takes precedence.

To configure the adaptive security appliance to send an entire syslog message class to a configured output destination, enter the following command:

```
hostname(config)# logging class message_class {buffered | console | history | mail |
monitor | trap} [severity_level]
```

where the *message\_class* argument specifies a class of syslog messages to be sent to the specified output destination. For a list of syslog message classes, see the *Cisco ASA 5580 Adaptive Security Appliance System Log Messages Guide*.

The **buffered**, **history**, **mail**, **monitor**, and **trap** keywords specify the output destination to which syslog messages in this class should be sent. The **history** keyword enables SNMP logging. The **monitor** keyword enables Telnet and SSH logging. The **trap** keyword enables syslog server logging. Select one destination per command line entry. If you want to specify that a class should go to more than one destination, enter a new command for each output destination.

The *severity\_level* argument further restricts the syslog messages to be sent to the output destination by specifying a severity level. For more information about message severity levels, see the “[Severity Levels](#)” section on page 39-31.

The following example specifies that all syslog messages related to the class *ha* (high availability, also known as failover) with a severity level of 1 (alerts) should be sent to the internal logging buffer.

```
hostname(config)# logging class ha buffered alerts
```

## Filtering Syslog Messages with Custom Message Lists

Creating a custom message list is a flexible way to exercise fine control over which syslog messages are sent to which output destination. In a custom syslog message list, you specify groups of syslog messages using any or all of the following criteria: severity level, message IDs, ranges of syslog message IDs, or message class.

For example, message lists can be used to do the following:

- Select syslog messages with severity levels of 1 and 2 and send them to one or more e-mail addresses.
- Select all syslog messages associated with a message class (such as “ha”) and save them to the internal buffer.

A message list can include multiple criteria for selecting messages. However, you must add each message selection criteria with a new command entry. It is possible to create a message list containing overlapping message selection criteria. If two criteria in a message list select the same message, the message is logged only once.

To create a customized list that the adaptive security appliance can use to select messages to be saved in the log buffer, perform the following steps:

---

**Step 1** Create a message list containing criteria for selecting messages by entering the following command:

```
hostname(config)# logging list name {level level [class message_class] |
message start_id[-end_id]}
```

where the *name* argument specifies the name of the list. Do not use the names of severity levels as the name of a customized message list. Prohibited names include “emergencies,” “alert,” “critical,” “error,” “warning,” “notification,” “informational,” and “debugging.” Similarly, do not use the first three characters of these words at the beginning of a filename. For example, do not use a filename that starts with the characters “err.”

The **level** *level* argument specifies the severity level. You can specify the severity level number (0 through 7) or name. For severity level names, see the “Severity Levels” section on page 39-31. For example, if you set the level to 3, then the adaptive security appliance sends syslog messages for severity levels 3, 2, 1, and 0.

The **class** *message\_class* argument specifies a particular message class. For a list of class names, see the *Cisco ASA 5580 Adaptive Security Appliance System Log Messages Guide*.

The **message** *start\_id[-end\_id]* argument specifies an individual syslog message number or a range of numbers.

The following example creates a message list named `notif-list` that specifies messages with a severity level of 3 or higher should be saved in the log buffer:

```
hostname(config)# logging list notif-list level 3
```

**Step 2** (Optional) If you want to add more criteria for message selection to the list, enter the same command as in the previous step, specifying the name of the existing message list and the additional criterion. Enter a new command for each criterion you want to add to the list.

The following example adds criteria to the message list—a range of message ID numbers and the `ha` message class (high availability or failover):

```
hostname(config)# logging list notif-list 104024-105999
hostname(config)# logging list notif-list level critical
hostname(config)# logging list notif-list level warning class ha
```

The preceding example states that syslog messages that match the criteria specified will be sent to the output destination. The specified criteria for syslog messages to be included in the list are the following:

- Syslog message IDs that fall in the range of 104024 to 105999
- All syslog messages with critical level or higher (emergency, alert, or critical)
- All `ha` class syslog messages with warning level or higher (emergency, alert, critical, error, or warning)

A syslog message is logged if it satisfies any of these conditions. If a syslog message satisfies more than one of the conditions, the message is logged only once.

## Customizing the Log Configuration

This section describes other options for fine tuning the logging configuration, and includes the following topics:

- [Configuring the System Logging Queue, page 39-26](#)
- [Including the Date and Time in Syslog Messages, page 39-26](#)
- [Including the Device ID in Syslog Messages, page 39-26](#)
- [Generating Syslog Messages in EMBLEM Format, page 39-27](#)
- [Disabling a Syslog Message, page 39-27](#)
- [Changing the Severity Level of a Syslog Message, page 39-28](#)
- [Limiting the Rate of Syslog Message Generation, page 39-29](#)
- [Changing the Amount of Internal Flash Memory Available for System Logs, page 39-29](#)

## Configuring the System Logging Queue

The adaptive security appliance has a fixed number of blocks in memory that can be allocated for buffering syslog messages while they are waiting to be sent to the configured output destination. The number of blocks required depends on the length of the system logging queue and the number of syslog servers specified.

To specify the number of syslog messages that the adaptive security appliance can hold in its queue before sending them to the configured output destination, enter the following command:

```
hostname(config)# logging queue message_count
```

where the *message\_count* variable specifies the number of syslog messages that can remain in the syslog message queue while awaiting processing. The default is 512 syslog messages. A setting of 0 (zero) indicates unlimited syslog messages, that is, the queue size is limited only by block memory availability.

To view the queue and queue statistics, enter the following command:

```
hostname(config)# show logging queue
```

## Including the Date and Time in Syslog Messages

To specify that syslog messages should include the date and time that the syslog messages was generated, enter the following command:

```
hostname(config)# logging timestamp
```

## Including the Device ID in Syslog Messages

To configure the adaptive security appliance to include a device ID in non-EMBLEM-format syslog messages, enter the following command:

```
hostname(config)# logging device-id {context-name | hostname | ipaddress interface_name | string text}
```

You can specify only one type of device ID for the syslog messages.

The **context-name** keyword indicates that the name of the current context should be used as the device ID (applies to multiple context mode only). If you enable the logging device ID for the admin context in multiple context mode, messages that originate in the system execution space use a device ID of **system**, and messages that originate in the admin context use the name of the admin context as the device ID.

The **hostname** keyword specifies that the hostname of the adaptive security appliance should be used as the device ID.

The **ipaddress interface\_name** argument specifies that the IP address of the interface specified as *interface\_name* should be used as the device ID. If you use the **ipaddress** keyword, the device ID becomes the specified adaptive security appliance interface IP address, regardless of the interface from which the syslog message is sent. This keyword provides a single, consistent device ID for all syslog messages that are sent from the device.

The **string text** argument specifies that the text string should be used as the device ID. The string can contain as many as 16 characters. You cannot use blank spaces or any of the following characters:

- & (ampersand)
- ' (single quote)
- " (double quote)

- < (less than)
- > (greater than)
- ? (question mark)

**Note**

If enabled, the device ID does not appear in EMBLEM-formatted syslog messages or SNMP traps.

The following example enables the logging device ID for the adaptive security appliance:

```
hostname(config)# logging device-id hostname
```

The following example enables the logging device ID for a security context on the adaptive security appliance:

```
hostname(config)# logging device-id context-name
```

## Generating Syslog Messages in EMBLEM Format

To use the EMBLEM format for syslog messages sent to destinations other than a syslog server, enter the following command:

```
hostname(config)# logging emblem
```

To use the EMBLEM format for syslog messages sent to a syslog server over UDP, specify the **format emblem** option when you configure the syslog server as an output destination. Enter the following command:

```
hostname(config)# logging host interface_name ip_address {tcp[/port] | udp[/port]}  
[format emblem]
```

where the *interface\_name* and *ip\_address* specifies the syslog server to receive the syslog messages, **tcp[/port]** and **udp[/port]** indicate the protocol and port that should be used, and **format emblem** enables EMBLEM formatting for messages sent to the syslog server.

The adaptive security appliance can send syslog messages using either the UDP or TCP protocol; however, you can enable the EMBLEM format only for messages sent over UDP. The default protocol and port are UDP and 514.

For example:

```
hostname(config)# logging host interface_1 209.165.201.1 udp format emblem
```

For more information about syslog servers, see the [“Sending Syslog Messages to a Syslog Server” section on page 39-14](#).

## Disabling a Syslog Message

To prevent the adaptive security appliance from generating a particular syslog message, enter the following command:

```
hostname(config)# no logging message message_number
```

where *message\_number* is the specific syslog message number that you want to stop generating.

For example:

```
hostname(config)# no logging message 113019
```

To reenable a disabled syslog message, enter the following command:

```
hostname(config)# logging message message_number
```

where *message\_number* is the specific syslog message number that you want to reenable.

For example:

```
hostname(config)# logging message 113019
```

To see a list of disabled syslog messages, enter the following command:

```
hostname(config)# show logging message
```

To reenable logging of all disabled syslog messages, enter the following command:

```
hostname(config)# clear config logging disabled
```

## Changing the Severity Level of a Syslog Message

To specify the logging level of a syslog message, enter the following command:

```
hostname(config)# logging message message_ID level severity_level
```

where *message\_ID* is the specific syslog message number, and *severity\_level* is the assigned severity level (0 - 7) of the syslog message.

The following example modifies the severity level of syslog message 113019 from 4 (warnings) to 5 (notifications):

```
hostname(config)# logging message 113019 level 5
```

To reset the logging level of a syslog message to its default level, enter the following command:

```
hostname(config)# no logging message message_ID level current_severity_level
```

where *message\_ID* is the specific syslog message number, and *current\_severity\_level* is the existing severity level (0 - 7) of the syslog message.

The following example modifies the severity level of syslog message 113019 to its default value of 4 (warnings):

```
hostname(config)# no logging message 113019 level 5
```

To see the severity level of a specific message, enter the following command:

```
hostname(config)# show logging message message_ID
```

where *message\_ID* is the specific syslog message number.

To see a list of syslog messages with modified severity levels, enter the following command:

```
hostname(config)# show logging message
```

To reset the severity level of all modified syslog messages to their default values, enter the following command:

```
hostname(config)# clear configure logging level
```

The following example shows the use of the **logging message** command to control both whether a syslog message is enabled and the severity level of the syslog message:

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

```
hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

## Limiting the Rate of Syslog Message Generation

The logging rate-limit determines the rate at which syslog messages are generated. You can specify the rate at which syslog messages are generated by applying a specified severity level (1 through 7) to a set of messages or to an individual message within a specified time period.

To limit the logging rate-limit, enter the following command:

```
hostname(config)# logging rate-limit
```

To show the disallowed system log messages, enter the following command:

```
hostname(config)# show logging rate-limit
```

To show the current logging rate-limit setting, enter the following command:

```
hostname(config)# show running-config logging rate-limit
```

To reset the logging rate-limit to the default value, enter the following command:

```
hostname(config)# clear running-config logging rate-limit
```

To reset the logging rate-limit, enter the following command:

```
hostname(config)# clear configure logging rate-limit
```

## Changing the Amount of Internal Flash Memory Available for System Logs

You can have the adaptive security appliance save the contents of the log buffer to internal flash memory in two ways:

- Configure system logging so that the contents of the log buffer are saved to internal flash memory each time the buffer wraps
- Enter a command instructing the adaptive security appliance to save the current contents of the log buffer to internal flash memory immediately

By default, the adaptive security appliance can use up to 1 MB of internal flash memory for system log data. The default minimum amount of internal flash memory that must be free for the adaptive security appliance to save system log data is 3 MB.

If saving a log file to internal flash memory would cause the amount of free internal flash memory to fall below the configured minimum limit, the adaptive security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the adaptive security appliance does not save the new log file.

To modify settings for the amount of internal flash memory available for system logs, perform the following steps:

- Step 1** To specify the maximum amount of internal flash memory available for saving log files, enter the following command:

```
hostname(config)# logging flash-maximum-allocation kbytes
```

where *kbytes* specifies the maximum amount of internal flash memory in kilobytes, which can be used for saving log files.

The following example sets the maximum amount of internal flash memory that can be used for log files to approximately 1.2 MB:

```
hostname(config)# logging flash-maximum-allocation 1200
```

- Step 2** To specify the minimum amount of internal flash memory that must be free for the adaptive security appliance to save a log file, enter the following command:

```
hostname(config)# logging flash-minimum-free kbytes
```

where *kbytes* specifies the minimum amount of internal flash memory in kilobytes, which must be available before the adaptive security appliance saves a new log file.

The following example specifies that the minimum amount of free internal flash memory must be 4000 KB before the adaptive security appliance can save a new log file:

```
hostname(config)# logging flash-minimum-free 4000
```

## Understanding Syslog Messages

This section describes the contents of syslog messages generated by the adaptive security appliance. It includes the following topics:

- [Syslog Message Format, page 39-30](#)
- [Severity Levels, page 39-31](#)

## Syslog Message Format

Syslog messages begin with a percent sign (%) and are structured as follows:

```
%ASA Level Message_number: Message_text
```

Field descriptions are as follows:

|                |                                                                                                                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ASA            | Identifies the syslog message facility code for messages generated by the adaptive security appliance. This value is always ASA.                                                                 |
| Level          | 1-7. The level reflects the severity of the condition described by the syslog message. The lower the number, the more severe the condition. See <a href="#">Table 39-3</a> for more information. |
| Message_number | A unique six-digit number that identifies the syslog message.                                                                                                                                    |
| Message_text   | A text string describing the condition. This portion of the syslog message sometimes includes IP addresses, port numbers, or usernames.                                                          |

## Severity Levels

[Table 39-3](#) lists the syslog message severity levels.

**Table 39-3 Syslog Message Severity Levels**

| Severity Level | Level Keyword        | Description                         |
|----------------|----------------------|-------------------------------------|
| 0              | <b>emergencies</b>   | System is unusable.                 |
| 1              | <b>alert</b>         | Immediate action is needed.         |
| 2              | <b>critical</b>      | Critical conditions.                |
| 3              | <b>error</b>         | Error conditions.                   |
| 4              | <b>warning</b>       | Warning conditions.                 |
| 5              | <b>notification</b>  | Normal, but significant conditions. |
| 6              | <b>informational</b> | Informational messages only.        |
| 7              | <b>debugging</b>     | Debugging messages only.            |



### Note

The adaptive security appliance does not generate syslog messages with a severity level of 0 (emergencies). This level is provided in the **logging** command for compatibility with the UNIX system log feature, but is not used by the adaptive security appliance.

# Configuring and Using NetFlow Secure Event Logging (NSEL)

NSEL is a security logging mechanism that is built on NetFlow Version 9 technology. This section describes event and syslog message handling through NSEL, and includes the following topics:

- [About NetFlow Secure Event Logging, page 39-32](#)
- [Using NSEL and Syslog Messages, page 39-32](#)
- [Configuring NSEL Collectors, page 39-33](#)
- [Filtering NSEL Events, page 39-34](#)
- [Configuring Template Timeout Intervals, page 39-36](#)
- [Delaying Flow-Create Events, page 39-37](#)

- [Disabling and Reenabling NetFlow-related Syslog Messages, page 39-37](#)
- [Displaying NetFlow-related Syslog Messages, page 39-38](#)
- [Clearing Runtime Counters, page 39-38](#)
- [Displaying Runtime Counters, page 39-38](#)

For more information about NSEL-related commands and configuration, see the *Cisco ASA 5580 Adaptive Security Appliance Command Reference*.

## About NetFlow Secure Event Logging

The adaptive security appliance supports NetFlow Version 9 services. For more information about NetFlow services, see RFC 3954.

The adaptive security appliance implementation of NSEL is a stateful, IP flow tracking method that exports only those records that indicate significant events in a flow. In stateful flow tracking, tracked flows go through a series of state changes. NSEL events are used to export data about flow status, and are triggered by the event that caused the state change.

The significant events that are tracked include flow creation, flow teardown, and flow denial (excluding those flows that are denied by EtherType ACLs). Each NSEL record has an event ID and an extended event ID field, which describes the flow event.

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

- Keeps track of **flow-create**, **flow-teardown**, and **flow-dened** events, and generates appropriate NSEL data records.
- Defines and exports templates that describe the progression of a flow. Templates describe the format of the data records that are exported through NetFlow. Each event has several record formats or templates associated with it.
- Tracks configured NSEL collectors and delivers templates and data records to these configured NSEL collectors through NetFlow over UDP only.
- Sends template information periodically to NSEL collectors. Collectors receive template definitions, normally before receiving flow records.
- Filters NSEL events based on the traffic and event type through Modular Policy Framework, and then sends records to different collectors. Traffic is matched based on the order in which classes are configured. The supported event types are flow-create, flow-denied, flow-teardown, and all.
- Delays the export of flow-create events. If the **flow-export delay flow-create** 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.

For details about the adaptive security appliance implementation of NSEL, see the *Implementation Note for NetFlow Collectors*.

## Using NSEL and Syslog Messages

[Table 39-4](#) 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). For more information about syslog messages, see the *Cisco ASA 5580 Adaptive Security Appliance System Log Messages Guide*.

**Note**

Enabling NetFlow to export flow information makes the syslog messages listed in [Table 39-4](#) redundant. In the interest of performance, we recommend that you disable redundant syslog messages, because the same information is exported through NetFlow. You can enable or disable individual syslog messages by following the procedure in the “[Disabling and Reenabling NetFlow-related Syslog Messages](#)” section on [page 39-37](#).

**Table 39-4 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).<br>3—Flow was denied (if the ACL denied the flow). | 0—If the ACL allowed the flow.<br>1001—Flow was denied by the ingress ACL.<br>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 <b>access-group</b> command. | 3—Flow was denied.                                                                                   | 1001—Flow was denied by the ingress ACL.<br>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.<br>> 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.                                                             |

## Configuring NSEL Collectors

**Note**

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

To configure an NSEL collector to which NetFlow packets are sent, enter the following command:

```
hostname (config)# flow-export destination interface-name ipv4-address/hostname udp-port
```

where the **destination** keyword indicates that a NSEL collector is being configured, *interface-name* is the name of the adaptive security appliance interface through which the collector is reached, *ipv4-address* is the IP address of the machine running the collector application, *hostname* is the

destination IP address or name of the collector, and *udp-port* is the UDP port number to which NetFlow packets are sent. You can configure a maximum of five destinations. After a destination is configured, template records are automatically sent to all configured NSEL collectors.

For example:

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

## Filtering NSEL Events

NSEL events can be filtered based on traffic and event-type, and records can be sent to different collectors.

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

- Log all flow-denied events that match access-list 1 to collector 1.
- Log all flow-create events to collector 1.
- Log all flow-teardown events to collector 2.

NSEL collectors must be configured before you can configure filters via Modular Policy Framework.



### Note

If you previously configured flow-export actions in Version 8.1(1) using the **flow-export enable** command, and you upgrade to a later version, then your configuration will be automatically converted to the new Modular Policy Framework **flow-export event-type** command. For more information, see the 8.1(2) release notes.

## Configuring Flow-Export Actions

You can configure flow-export actions using Modular Policy Framework to export NSEL events. Traffic is matched based on the order in which classes are configured. After a match is found, no other classes are checked.

The supported event types are **flow-create**, **flow-denied**, **flow-teardown**, and **all**, which includes the three previously listed event types.

A flow-export destination is uniquely identified by its IP address.

To export NSEL events, you must define all classes with flow-export actions by performing the following steps:

- Step 1** Define the class map that identifies traffic for which NSEL events need to be exported by entering the following command:

```
hostname (config)# class-map flow_export_class
```

where *flow\_export\_class* is the name of the class map.

Configure the access-list to match specific traffic by entering the following command:

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

where *flow\_export\_acl* is the name of the access-list.

Alternatively, any traffic can be matched by entering the following command:

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



**Note** 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.

**Step 2** Define the policy map to apply flow-export actions to the classes defined by entering the following command:

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

where *flow\_export\_policy* is the name of the policy map.

Define the class to apply flow-export actions by entering the following command:

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

where *flow\_export\_class* is the name of the class.

Configure a flow-export action by entering the following command:

```
hostname (config-pmap-c)# flow-export event-type event-type destination flow_export_host1  
[flow_export_host2]
```

where **event\_type** is the name of the supported event being filtered and *flow\_export\_host* is the IP address of the collector.

**Step 3** Attach the service policy globally by entering the following command:

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

The following examples show four filtering scenarios for NSEL events, with these collectors already configured:

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

## Scenario 1

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

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

## Scenario 2

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

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

## Scenario 3

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

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



### Note

You must enter the following command:

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

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

## Scenario 4

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

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

## Configuring Template Timeout Intervals

To specify the interval at which template records are sent to all configured destinations, enter the following command:

```
hostname (config)# flow-export template timeout-rate minutes
```

where **template** indicates the template-specific configurations, **timeout-rate** specifies the time before templates are resent, and *minutes* specifies the time interval in minutes at which the templates are resent. The default value is 30 minutes.

For example:

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

## Delaying Flow-Create Events

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

```
hostname (config)# flow-export delay flow-create seconds
```

where *seconds* 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.

For example:

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

## Disabling and Reenabling NetFlow-related Syslog Messages

Although the adaptive security appliance supports both NSEL and syslog messages, we recommend that you disable all syslog messages that are also represented by NSEL events to avoid redundancy and maintain performance.

**Note**

---

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

---

To disable syslog messages that have become redundant because of NSEL, perform the following steps:

**Step 1** Enter the following command:

```
hostname (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** To display the disabled syslog messages, enter the following command:

```
hostname (config)# show running-config logging
```

```
no logging message xxxxx1  
no logging message xxxxx2
```

where *xxxxx1* and *xxxxx2* are redundant syslog messages because they are also captured by NSEL.

- Step 3** After you have disabled the redundant syslog messages, you can reenble them individually with the **logging message xxxxxx** command, where *xxxxxx* is the specified syslog message that you want to reenble.
- Step 4** To reenble all NSEL events at the same time, enter the **logging flow-export syslogs enable** command.

## Displaying NetFlow-related Syslog Messages

To list all syslog messages that are captured by NSEL events, enter the following command:

```
hostname# show logging flow-export-syslogs
```

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

For a list of specific features that have been implemented for the adaptive security appliance, see the [“Supported Platforms and Feature Licenses”](#) section on page A-1.

## Clearing Runtime Counters

To reset all runtime counters for NSEL to zero, enter the following command:

```
hostname# clear flow-export counters
```

## Displaying Runtime Counters

Runtime counters include statistical data and error data. To show runtime counters for NSEL, enter the following command:

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

```
destination: inside 209.165.200.225 2055
```

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