



## CHAPTER 20

# Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x and 8.2.x with NetFlow

---

Revised: October 14, 2008, OL-16778-01

## Contents

This chapter describes how to add the Cisco ASA, Versions 8.1.x or 8.2.x to the Local Controller as reporting devices, and how to configure NetFlow Security Event Logging (NSEL) between the Cisco ASA 5580, Version 8.1.x or 8.2.x and the MARS Local Controller.

Configuration procedures for firewall syslog monitoring and for adding other versions of the Cisco ASA to MARS are described in, “[Configuring Cisco Firewall Devices](#).”

This chapter contains the following sections:

- [Information About Configuring the Cisco ASA Version 8.1.x with NSEL, page 1](#)
- [Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS, page 3](#)
- [Configuring NSEL for MARS on the Cisco ASA 5580, page 10](#)
- [Additional References, page 13](#)

## Information About Configuring the Cisco ASA Version 8.1.x with NSEL

NetFlow Security Event Logging (NSEL) is an efficient logging method for high-speed environments. Before Cisco ASA Release 8.1, Cisco ASA events were exported exclusively through system log (syslog) messages and SNMP traps. NSEL can transmit much of the same syslog information in a less CPU-intensive, more secure, and more bandwidth-efficient way. NSEL is an adaptation of NetFlow version 9.

To implement NSEL, the MARS Local Controller is configured as a NetFlow collector on the Cisco ASA 5580. When the Cisco ASA is configured in multi-mode, each context can report to its own MARS Appliance—if the contexts are on separate networks. The MARS Local Controller can use the Cisco ASA NSEL information as follows:

- Create topology-aware sessionization of NetFlow events with non-NetFlow events

- Perform rule correlation and incident firing from NetFlow events
- Retrieve collected NetFlow data with queries and non-scheduled reports
- View incoming Netflow events with the Real-time Event Viewer
- Configure drop rules against incoming NetFlow events
- Use NetFlow-derived events in Scheduled reports results (For example, Top N reports)

**Note**


---

Syslog-based anomaly detection is still supported for all versions of the Cisco ASA.

---

For information on NetFlow anomaly detection on MARS, see the, *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*, [Understanding NetFlow Anomaly Detection on MARS](#).

For detailed information on NSEL, configuring the Cisco ASA Security Appliance, and descriptions of how NSEL and SYSLOG events compare, see the following publications:

- All Cisco ASA 5500 Series Adaptive Security Appliances documentation:  
[http://www.cisco.com/en/US/products/ps6120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html)
- Cisco ASA 5580 Adaptive Security Appliance Command Reference (8.1, 8.2)  
<http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/refgd.html>  
[http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd\\_ref.html](http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd_ref.html)
- Monitoring the Cisco ASA Security Appliance (8.1, 8.2):  
<http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/monitor.html#wp1099818>  
[http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor\\_syslog.html](http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_syslog.html)
- Cisco ASA 5580 Implementation Note for NetFlow Collectors (8.1 and 8.2):  
<http://www.cisco.com/en/US/docs/security/asa/asa81/netflow/netflow.html>  
<http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html>

## Taskflow for Configuring NSEL on MARS

The taskflow for configuring the Cisco ASA, Version 8.1.x and 8.2.x with MARS NetFlow Security Event Logging is as follows:

1. Identify the Cisco ASA contexts and modules on which to enable NSEL.
2. Disable syslog reporting to MARS on those devices.
3. Enable NSEL on each Cisco ASA reporting device and direct the NetFlow data to the MARS Appliance responsible for that network segment.
4. Verify that all the Cisco ASA reporting devices are defined in the MARS web interface.
5. Enable NetFlow processing in the MARS web interface.
6. Configure Networks for Traffic Anomaly Detection in the MARS web interface (if necessary)
7. Allow MARS to study traffic for a week to develop a usage baseline before it begins to generate incidents based on detected anomalies.

# Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS

## Prerequisites

The following prerequisites are required for MARS-ASA interoperability:

- MARS is permitted administrative access to ASA
- MARS is configured as a NetFlow collector for the ASA.
- MARS is configured with the same NTP server as the Cisco ASA

For details on configuring the Cisco ASA, Version 8.1.x for MARS, See the *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide, Version 8.1, Appendix F, section Configuring NSEL for MARS on the ASA 5580* at the following URL:

<http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/csmars.html>

For details on configuring the Cisco ASA, Version 8.2.x for MARS, See the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2* at the following URL:

[http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ref\\_csmars.html](http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ref_csmars.html)

Procedures for configuring administrative access on the Cisco ASA, Version 7.x and 8.0.x are also described in this guide, in the chapter, “Configuring Cisco Firewall Devices.”

See also, [Related Documents](#), page 13.

## SUMMARY STEPS

1. Navigate to Admin > System Setup > Security and Monitor Devices.
2. Select Cisco ASA, Version 8.1 or Cisco ASA, Version 8.2 from the Device Type drop-down list.
3. Complete the configuration fields on the device configuration page.
4. Click Submit.
5. Click Activate.

## DETAILED STEPS

- 
- Step 1** Navigate to **Admin > System Setup > Security and Monitor Devices**.  
The Security and Monitoring Information page appears.
- Step 2** Click **Add**.  
The Device Configuration page appears.
- Step 3** Select **Cisco ASA 8.1** or **Cisco ASA 8.2** from the Device Type drop-down list.  
The ASA 8.1 Configuration page appears, as shown in [Figure 20-1](#).

**Figure 20-1 Add the Cisco ASA, Version 8.1.X to MARS**  
(Admin > Security and Monitor Devices > Add > Device Type > ASA 8.1)

Note:  
1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.  
2. \* denotes a required field.

Device Type:

→ \*Device Name:

→ Access IP:

→ Reporting IP:

→ \* Access Type:

Login:

Password:

Enable Password:

Config Path:

File Name:

SNMP RO Community:

→ Monitor Resource Usage:

→ Secure Syslog Setting:

**Step 4** Complete the configuration fields as described in [Table 20-1](#).

**Table 20-1 Cisco ASA, Version 8.1.x and 8.2.x Configuration Fields**

ASA 8.x Device Configuration Field	Description
Device Name	Name of the Cisco ASA device.  MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and in the Security and Monitoring Device list. For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the hostname.domain format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the value specified in this field.
Access IP	ASA Administrative IP address—allows MARS to discover settings of the ASA.  The Access IP address must be reachable from MARS.
Reporting IP	The IP address of the interface that sends NetFlow data.  The Reporting IP is seen in MARS as the sender IP in an ASA syslog or netflow packet. The Reporting IP address does not have to be reachable from MARS or be the IP address of the ASA admin context (because separate NetFlow collectors can be configured from each context).

Table 20-1 Cisco ASA, Version 8.1.x and 8.2.x Configuration Fields (Continued)



ASA 8.x Device Configuration Field	Description
Access Type	<p>If you entered an address in the Access IP field, select TELNET, SSH, or FTP from the Access Type list, and continue with the procedure that matches your selection:</p> <p><b>To configure Telnet access for devices in MARS:</b></p> <ul style="list-style-type: none"> <li>In the Login field, enter the username of the administrative account to use when accessing the reporting device.</li> </ul> <p> <b>Note</b> The username field is optional for a telnet connection. It is required only when AAA is configured for the telnet access.</p> <ul style="list-style-type: none"> <li>In the Password field, enter the password associated with the username specified in the Login field.</li> <li>Enter the Cisco ASA enable password in the Enable Password field.</li> </ul> <p><b>To configure SSH access for Cisco ASA in MARS:</b></p> <ul style="list-style-type: none"> <li>From the list box to the right of the Access Type list, select 3DES, DES, or BlowFish as the encryption cipher for SSH sessions between the MARS Appliance and the reporting device.</li> <li>In the Login field, enter the username of the administrative account to use when accessing the reporting device.</li> <li>In the Password field, enter the password associated with the username specified in the Login field.</li> <li>If this device supports an enable mode, enter that password in the Enable Password field.</li> </ul> <p><b>To configure FTP access for devices in MARS:</b></p> <ul style="list-style-type: none"> <li>In the Login field, enter the username of the FTP server account to use when accessing the configuration file of the reporting device.</li> <li>In the Password field, enter the password associated with the username specified in the Login field.</li> <li>In the Config Path field, enter the path to the reporting device's configuration file residing on the FTP server. This path begins at the root of the FTP server's published folder, not at the root directory of server.</li> <li>In the File Name field, enter the name of the reporting device's configuration file residing on the FTP server.</li> </ul>
Login	See Access Type.
Password	See Access Type.

Table 20-1 Cisco ASA, Version 8.1.x and 8.2.x Configuration Fields (Continued)

ASA 8.x Device Configuration Field	Description
Enable Password	See Access Type.
Config Path	See Access Type, “To configure FTP access.”
File Name	See Access Type, “To configure FTP access.”
SNMP RO Community	<p>Optional. To enable MARS to retrieve MIB objects for this reporting device, enter the device's read-only community string in the SNMP RO Community field.</p> <p>Before you can specify the SNMP RO string, you must define an Access IP address. MARS uses the SNMP RO string to read MIBs related to the Cisco ASA's CPU usage, network usage, device anomaly data and to discover device and network settings.</p>
Monitor Resource Usage	<p>Optional. To enable MARS to monitor this device for anomalous resource usage, select Yes from the Monitor Resource Usage list.</p> <p>MARS monitors the ASA for anomalous consumption of resources, such as memory and CPU. If anomalies are detected, MARS generates an incident. Resource utilization statistics are also used to generate reports.</p>
Secure Syslog Setting: Client Authentication (not relevant to NSEL)	<p>Optional. The Cisco ASA 8.0 and 8.1 can be configured to send secure syslogs, that is, syslogs over an SSL connection.</p> <p><b>No</b>—No client authentication is necessary.</p> <p><b>Yes</b>—Perform the following tasks:</p> <ul style="list-style-type: none"> <li>• Click <b>Add Client Certificate</b>.</li> <li>• Copy and paste the certificate into the Update Client Certificate pop-up window that appears.</li> <li>• Click <b>Accept</b>.</li> </ul> <p> <b>Note</b> NSEL is transported by UDP.</p>

**Step 5** Do one of the following:

- Click **Discover** to let MARS contact the device and conduct a topology and module configuration discovery. Information about the security modules is presented on the Security and Monitoring Information page.

To edit discovered contexts, continue with Edit Discovered Security Contexts.

- Click **Next** to commit your changes and manually configure Cisco ASA modules.

For the Cisco ASA, you can add one or more security contexts or Advanced Inspection and Prevention (AIP) modules. The following sections in this guide describe how to manually add or edit Cisco ASA modules:

- [Defining a CSC SSM in MARS](#)
- [Add Security Contexts Manually](#)
- [Edit Discovered Security Contexts](#)

**Step 6** Click **Submit**.

End of the procedure, "[Adding the Cisco ASA, Version 8.1.X or 8.2.X Device to MARS](#)"

---

## What to Do Next

To enable NSEL on the MARS Appliance, go to the procedure, "[Enabling NSEL Processing on the MARS Appliance](#)"

# Enabling NSEL Processing on the MARS Appliance

This procedure is valid only for the Cisco ASA, Version 8.1.x and 8.2.x

## SUMMARY STEPS

1. Navigate to Admin > System Setup > NetFlow Config Info.
2. Complete the configuration fields on the Netflow Configuration Page.
3. Click Submit.
4. Navigate to Admin > System Setup > Networks for Traffic Anomaly Detection.
5. Configure the Networks for Traffic Anomaly Detection Page
6. Click Submit.
7. Click Activate.

## DETAILED STEPS

Before enabling NetFlow on MARS, you must enable NetFlow Security Event Logging on the Cisco ASA with MARS as the NetFlow collector. See—[Configuring NSEL for MARS on the Cisco ASA 5580](#) later in this document.

---

**Step 1** Navigate to **Admin > System Setup > NetFlow Config Info**. The NetFlow configuration page appears, as shown in [Figure 20-2](#).

Figure 20-2 NetFlow Configuration Page (Admin &gt; System Setup &gt; NetFlow Config Info)

NetFlow Configuration

Global NetFlow UDP Port:	<input type="text" value="2055"/>
Enable NetFlow Processing:	Yes <input checked="" type="radio"/> No <input type="radio"/>
Always Store IOS NetFlow Records:	Yes <input type="radio"/> No <input checked="" type="radio"/>
Always Store ASA Netflow Security Event Logs:	Yes <input type="radio"/> No <input checked="" type="radio"/>
Turn on IOS Netflow Verbose Raw Messages:	Yes <input type="radio"/> No <input checked="" type="radio"/>

Back Info Submit

- Step 2** Type the Cisco ASA NetFlow Security Event Logging port in the Global NetFlow UDP Port field. The default is 2055.



**Note** This value must match the value configured with the **ip flow-export destination** command on the ASA. Verify that you have enabled traffic on this port on all intermediate network devices between the ASA and MARS.

- Step 3** Configure **Enable NetFlow Processing**.

- **Yes**—Configures MARS to process the NetFlow logs.
- **No**—Disables the processing of NetFlow data into the MARS.

- Step 4** Configure **Always Store ASA Netflow Security Event Logs**.

- **Yes** —Enables MARS to use Cisco ASA Netflow Security Event Logs to do the following:
  - Topology-aware sessionization of NetFlow events with non-NetFlow events
  - Rule correlation and incident firing from NetFlow events
  - Retrieval of NetFlow reported data using queries and non-scheduled reports
  - View incoming Netflow events with the Real-time Event Viewer
  - Configure drop rules against incoming NetFlow events
  - Use NetFlow-derived events in Scheduled reports results (For example, Top N reports)
- **No (default)**—Configures MARS to store only anomalies. MARS detects anomalies by using two dynamically generated watermarks comparing the previous data against current data. When the data breaches the first watermark, MARS starts to save that data. When the data rises above the second watermark, MARS creates an incident.

**No** limits the use of Cisco ASA Netflow Security Event Logs to the following:

- View incoming Netflow events with the Real-time Event Viewer
- Configure drop rules against incoming NetFlow events

- Use NetFlow-derived events in Scheduled reports results (for stored incident data)

**Step 5** Click **Submit**.

If you wish to restrict traffic anomaly processing to specific networks go to [Step 6](#), otherwise go to [Step 9](#). To restrict logging, configure [drop rules](#) as needed.

**Step 6** Navigate to **Admin > System Setup > Networks for Traffic Anomaly Detection**. The Configure Networks page appears, as shown in [Figure 20-3](#).

**Figure 20-3** Networks for Traffic Anomaly Detection Page  
(Admin > System Setup > Networks for Traffic Anomaly Detection)

**Step 7** In the Configure Networks for Diagnosing Traffic Anomalies window, enter the addresses of networks you want to monitor and use the << Add button to add them.

- Specifying one or more networks causes MARS to generate NetFlow-based incidents that occur only on the specified networks. The default is to examine all data from all networks for anomalies. If the Local Controller is monitoring a specific zone (as defined by the Global Controller-Local Controller relationship), then this field should include only those networks for which this Local Controller is responsible. This interface restricts traffic anomaly processing for Cisco ASA NetFlow and Cisco IOS NetFlow.



**Note** To reduce the memory usage and increase performance of the appliance, you can configure MARS to profile hosts belonging to a set of valid networks.

**Step 8** Click **Submit** to save your changes.

**Step 9** To enable NetFlow processing by the MARS Appliance, click **Activate**.

Before MARS can start detecting anomalies based on NetFlow data, it must first develop a baseline for network behavior. It takes a full week, including the weekend, for MARS to develop a baseline. After a baseline is created, MARS can generate incidents based on NetFlow's anomaly detection.

**Step 10** Verify NetFlow configuration by observing raw messages from the Cisco ASA with the [MARS real-time event viewer](#).

End of Procedure, “[Configuring NSEL for MARS on the Cisco ASA 5580](#).”

---

## What to Do Next

To enable NSEL on a Cisco ASA, Version 8.1.x, go to the procedure, “[Configuring NSEL for MARS on the Cisco ASA 5580](#).”

# Configuring NSEL for MARS on the Cisco ASA 5580

For detailed information on configuring the Cisco ASA Security Appliance, see the section, [Related Documents](#), later in this chapter.



### Note

The Cisco ASA interface to MARS in the following examples is configured as “cs-mars” with the Cisco ASA **name** command.

---

## SUMMARY STEPS

1. configure terminal
2. ntp server
3. clear configure flow-export.
4. flow-export enable.
5. flow-export destination
6. flow-export template timeout-rate
7. logging flow-export-syslogs disable
8. logging trap 6
9. logging host
10. logging enable
11. exit
12. show running-config logging
13. show running-config flow-export

## DETAILED STEPS

	ASA Command	Explanation
Step 1	<b>configure terminal</b>  <b>Example:</b> asa# configure terminal	Enters Cisco ASA global configuration mode from privileged EXEC mode.
Step 2	<b>ntp server</b> <i>ip_address</i> [ <b>key</b> <i>key_id</i> ] [ <b>source</b> <i>interface_name</i> ] [ <b>prefer</b> ]  <b>Example:</b> asa(config)# ntp server 171.68.10.80 key 1 source inside prefer	Configure an NTP server to ensure accurate time stamps. This enables better correlation by MARS because it ensures the time on both the ASA and MARS are the same.
Step 3	<b>clear configure flow-export</b> [ <i>destination</i> ]  <b>Example:</b> asa(config)# clear configure flow-export 192.168.1.1	Clear the flow-export configurations associated with NetFlow data only for the specified IP address—in this example, previous configurations associated with the MARS IP address 192.168.1.1.
Step 4	<b>flow-export enable</b>  <b>Example:</b> asa(config)# flow-export enable	Enable export of NetFlow security event log messages.  When flow-export is enabled, the template records are sent to all configured NetFlow collectors. When disabled, any pending, cached NetFlow records are deleted from all collectors.
Step 5	<b>flow-export destination</b> <i>interface-name</i> <i>ipv4-address</i>   <i>hostname</i> <i>udp-port</i>  <b>Example:</b> asa(config)# flow-export destination inside cs-mars 2055	Configure the Cisco ASA to export the flow cache entries to a destination system (MARS).  The example configures the Cisco ASA interface on which the MARS appliance can be reached, the name associated with the IP address of the MARS appliance, and the UDP port on which MARS is listening for NetFlow traffic
Step 6	<b>flow-export template</b> <b>timeout-rate</b> <i>minutes</i>  <b>Example:</b> asa(config)# flow-export template timeout-rate 1	Set the interval at which the template information is sent to NetFlow collectors. Use 1 minute for MARS.
Step 7	<b>logging flow-export-syslogs</b> { <b>enable</b>   <b>disable</b> }  <b>Example:</b> asa(config)# logging flow-export-syslogs disable	Disable the redundant system log messages.  The syslog messages report the same events as the NetFlow security event logging.
Step 8	<b>logging trap</b> [ <i>logging_list</i>   <i>level</i> ]  <b>Example:</b> asa(config)# logging trap informational	Set the logging trap level to informational. You can also specify “6”.

	ASA Command	Explanation
Step 9	<b>logging host</b> <i>interface_name</i> <i>syslog_ip</i> <b>Example:</b> asa(config)# logging host cs-mars	Define MARS as a syslog server.  The example sets the logging host to the user-defined IP address of the CS-MARS appliance using the name command on the ASA.
Step 10	<b>logging enable</b> <b>Example:</b> asa(config)# clear configure flow-export cs-mars_ip	Enable logging to CS-MARS
Step 11	<b>exit</b> <b>Example:</b> asa(config)# exit	Log out of global configuration mode into Privileged Exec mode.
Step 12	<b>show running-config</b> [all] <b>logging</b> [level   disabled] <b>Example:</b> asa# show running-config logging	Display the status of the system logs, for example:  ASA81-Single# <b>show running-config logging</b> logging enable logging monitor debugging logging host outside 10.2.3.58 logging host outside 10.2.4.101 logging host outside 10.2.4.113 no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020
Step 13	<b>show running-config</b> <b>flow-export</b> [destination   enable   template] <b>Example:</b> asa# show running-config flow-export	Display the status of the flow exports, for example:  ASA81-Single# <b>show running-config flow-export</b> flow-export destination outside 10.2.3.226 2055 flow-export destination outside 10.2.3.42 2055 flow-export template timeout-rate 1 flow-export enable

# Additional References

The following sections provide references related to configuring the Cisco ASA Adaptive Security Appliances.

## Related Documents

Related Topic	Document Title
Understanding NetFlow Anomaly Detection on MARS	User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x: <a href="http://www.cisco.com/en/US/docs/security/security_management/c-s-mars/6.0/user/guide/combo/cfgOver.html#wp872012">http://www.cisco.com/en/US/docs/security/security_management/c-s-mars/6.0/user/guide/combo/cfgOver.html#wp872012</a>
All Cisco ASA 5500 Series Adaptive Security Appliances documentation	Cisco ASA 5500 Series Adaptive Security Appliances Support Documentation <a href="http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html">http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html</a>
Cisco ASA 5580 command line interface explanations.	Cisco ASA 5580 Adaptive Security Appliance Command Reference (8.1, 8.2) <a href="http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/refgd.html">http://www.cisco.com/en/US/docs/security/asa/asa81/command/ref/refgd.html</a> <a href="http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd_ref.html">http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/cmd_ref.html</a>
Information on Syslog, SNMP, and NetFlow monitoring for the Cisco ASA.	Monitoring the Cisco ASA Security Appliance (8.1, 8.2): <a href="http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/monitor.html#wp1099818">http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/monitor.html#wp1099818</a> <a href="http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_syslog.html">http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/monitor_syslog.html</a>
Configuring NetFlow (NSEL) Collectors for the Cisco ASA 5580	Cisco ASA 5580 Implementation Note for NetFlow Collectors (8.1, 8.2): <a href="http://www.cisco.com/en/US/docs/security/asa/asa81/netflow/netflow.html">http://www.cisco.com/en/US/docs/security/asa/asa81/netflow/netflow.html</a> <a href="http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html">http://www.cisco.com/en/US/docs/security/asa/asa82/netflow/netflow.html</a>

