



APPENDIX **A**

Configuring the Security Appliance for Use with MARS

MARS centrally aggregates logs and events from various network devices, including security appliances, which you can analyze for use in threat mitigation. MARS supports the following PIX and ASA adaptive security appliance versions: 7.0(7), 7.2(2), 7.2(3), 8.0(2), and 8.1(1).



Note

Version 8.1(1) applies to the ASA 5580 adaptive security appliance only. In addition, PIX is not supported in Version 8.1(1) or 8.1(2).

This appendix describes how to configure the security appliance and add it to MARS as a reporting device, and includes the following sections:

- [Taskflow for Configuring MARS to Monitor Security Appliances, page A-1](#)
- [Setting the Logging Severity Level for Syslog Messages, page A-2](#)
- [Syslog Messages That Are Processed by MARS, page A-2](#)
- [Configuring Specific Features, page A-5](#)
- [Configuring NSEL for MARS on the ASA 5580, page A-5](#)

Taskflow for Configuring MARS to Monitor Security Appliances

The taskflow for configuring MARS to monitor the security appliance includes the following steps:

1. Configure the security appliance to accept administrative sessions from MARS to discover settings. Configure this setting in the admin context.
2. Configure the security appliance to publish its syslog messages to MARS. Configure this setting for the admin context and for each security context defined.



Note

Each context requires a unique, routable IP address for sending syslog messages to MARS, and each context must have a unique name (usually in the *hostname.domain* name format).

3. To enable MARS to accept syslog message event data and to collect configuration settings from the security appliance, perform the following tasks:
 - Enable logging for one or more interfaces.
 - Select the logging facility and queue size.

- Specify the logging severity level as debugging (7) or indicate the desired severity level.
 - Identify the target MARS appliance, and the protocol and port pair on which it listens.
4. Within the MARS web interface, perform the following steps:
- Define the security appliance by providing the administrative connection information.
To enable administrative access to MARS on the security appliance, see [Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x with NetFlow](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
 - Define security contexts.
Events that are published by a reporting device (the security appliance) to MARS are not inspected until the reporting IP address of the security appliance is defined in the MARS web interface.
To add a PIX or ASA adaptive security appliance to monitor, see [Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x with NetFlow](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
 - Add security contexts.
To add security contexts, see [Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x with NetFlow](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
 - Add discovered contexts.
To add discovered contexts, see [Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x with NetFlow](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.
 - Edit discovered contexts.
To edit discovered contexts, see [Configuring MARS for the Cisco ASA Adaptive Security Appliances, Versions 8.1.x with NetFlow](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.

Setting the Logging Severity Level for Syslog Messages

You can change the logging severity level of the required syslog messages or turn off specific syslog messages using the **logging message** command. For more information, see the “[Configuring and Managing System Logs](#)” section on page 39-10.

Syslog Messages That Are Processed by MARS

MARS can correctly parse syslog messages at customized logging severity levels. Therefore, you can set syslog messages to a lower logging severity level (for example, logging severity level 6). By changing the logging severity level for syslog messages, you can reduce the logging load on the security appliance by 5-15%. However, the primary consumers of resources are the session detail events.

MARS processes the following syslog messages, which are required for correct sessionization. If you change the logging severity level of the security appliance, make sure that these syslog messages are generated at the new logging severity level so that the MARS appliance can receive them.

Table A-1 lists the syslog message classes, their definitions, and the ranges of syslog message numbers that are processed by MARS.

Table A-1 Syslog Message Classes and Associated Message Numbers

Class	Definition	Syslog Message Numbers
auth	User Authentication	109001-109003, 109005-109008, 109010-109014, 109016-109034, 113001, 113003-113020, 114001-114020, 611101-611104, 611301-611323
bridge	Transparent Firewall	110001
ca	PKI Certification Authority	717001-717019, 717021-717038
config	Command Interface	111001, 111003-111005, 111007-111009, 111111, 112001, 208005, 308001-308002, 504001-504002, 505001-505013, 506001
e-mail	E-mail Proxy	719001-719026
ha	High Availability (Failover)	101001-101005, 102001, 103001-103005, 104001-104004, 105001-105011, 105020-105021, 105031-105032, 105034-105040, 105042-105048, 210001-210003, 210005-210008, 210010, 210020-210022, 311001-311004, 709001-709007
ip	IP Stack	209003-209005, 215001, 313001, 313003-313005, 313008, 317001-317005, 322001-322004, 323001-323006, 324000-324007, 324300-324301, 325001-325003, 326001-326002, 326004-326017, 326019-326028, 327001-327003, 328001, 329001, 331001-331002, 332003-332004, 333001-333010, 334001-334008, 335001-335014, 408001-408003, 410001-410004, 411001-411004, 412001-412002, 413001-413004, 416001, 417001, 417004, 417006, 417008-417009, 418001, 419001-419002, 421001-421007, 422004-422006, 423001-423005, 424001-424002, 431001-431002, 450001, 507001-507002, 508001-508002, 509001
ips	Intrusion Protection Service	400000-400050, 401001-401005, 415001-415020, 420001-420003
np	Network Processor	319001-319004
npssl	NP SSL	725001-725014
ospf	OSPF Routing	318001-318009, 409001-409013, 409023, 503001, 613001-613003
rip	RIP Routing	107001-107003, 312001
rm	Resource Manager	321001-321004

Table A-1 Syslog Message Classes and Associated Message Numbers (continued)

Class (continued)	Definition	Syslog Message Numbers
session	User Session	106001-106002, 106006-106007, 106010-106027, 106100-106101, 108002-108003, 108005, 201002-201006, 201008-201013, 202001, 201005, 202011, 204001, 302001, 302003-302004, 302007-302010, 302012-302023, 302302, 303002-303005, 304001-304009, 305005-305012, 314001, 405001-405002, 405101-405107, 405201, 405300-405301, 406001-406002, 407001-407003, 500001-500004, 502101-502103, 502111-502112, 607001-607002, 608001-608005, 609001-609002, 616001, 617001-617004, 620001-620002, 621001-621003, 621006-621010, 622001, 622101-622102, 703001-703002, 710001-710006, 726001
snmp	SNMP	212001-212006
sys	System	199001-199003, 199005-199009, 211001, 211003, 216003, 217001, 218001-218004, 219002, 315004, 315011, 414001-414002, 604101-604104, 605004-605005, 606001-606004, 610001-610002, 610101, 612001-612003, 614001-614002, 615001-615002, 701001-701002, 711001-711002
vpdn	PPTP and L2TP Sessions	213001-213004, 403101-403104, 403106-403110, 403500-403507, 603101-603109
vpn	IKE and IPsec	316001, 320001, 402101-402103, 402106, 402114-402120, 402123, 404101-404102, 501101, 602101-602104, 602201-602203, 602301-602304, 702201-702212, 702301-702303, 702305, 702307, 713004, 713006, 713008-713010, 713012, 713014, 713016-713018, 713020, 713022, 713024-713037, 713039-713043, 713047-713052, 713056, 713059-713063, 713065-713066, 713068, 713072-713076, 713078, 713081-713086, 713088, 713092, 713094, 713098-713099, 713102-713105, 713107, 713109, 713112-713124, 713127-713149, 713152, 713154-713172, 713174, 713176-713179, 713182, 713184-713187, 713189-713190, 713193-713199, 713203-713206, 713208-713226, 713228-713251, 713900-713906, 714001-714007, 714011, 715001, 715004-715009, 715013, 715019-715022, 715027-715028, 715033-715042, 715044-715072, 715074-715079
vpnc	VPN Client	611101-611104, 611301-611323, 722001-722038
vpnfo	VPN Failover	720001-720073
vpnlb	VPN Load Balancing	718001-718081, 718084-718088
webvpn	Web-based VPN	716001-716056, 723001-723014, 724001-724002

Configuring Specific Features

You can configure security appliances to act as reporting devices and manual mitigation devices, because they perform multiple roles on your network. MARS can benefit from configuration of the following features:

- The built-in IDS and IPS signature matching features can be critical in detecting an attempted attack.
- The logging of accepted, as well as denied sessions, which aids in false positive analysis.
- Administrative access ensures that MARS can obtain critical data, including the following:
 - Route and ARP tables, which aid in network discovery and MAC address mapping.
 - NAT and PAT translation tables, which aid in address resolution and attack path analysis, and expose the actual instigator of attacks.
 - OS settings, from which MARS determines the correct ACLs to block detected attacks, which you can use in a management session with the security appliance.
- Implementing NSEL, in which the MARS Local Controller is configured as a NetFlow collector on the ASA 5580. When the ASA 5580 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 NSEL information in the following ways:
 - 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 according to incoming NetFlow events.
 - Use NetFlow-derived events in scheduled reports results (for example, Top N reports).

**Note**

Syslog-only anomaly detection is still supported for the ASA 5580.

Before enabling NetFlow configuration on MARS appliances, you must enable NSEL on the ASA 5580 by configuring MARS as the NetFlow collector. For information about configuring NetFlow collectors, see the “[Configuring and Using NetFlow Secure Event Logging \(NSEL\)](#)” section on page 39-31.

Configuring NSEL for MARS on the ASA 5580

The following procedure is valid only for the Cisco ASA, Version 8.1(1). The Cisco ASA, Version 8.0.x does not support NSEL.

For additional information about configuring NetFlow (NSEL) collectors for the ASA 5580, see the *Cisco ASA 5580 Implementation Note for NetFlow Collectors*, available at the following URL:

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

**Note**

The ASA 5580 interface to MARS in the following examples is configured as “cs-mars” with the ASA **name** command.

To configure NSEL for MARS on the ASA 5580, perform the following steps:

	Command	Description
Step 1	<p>configure terminal</p> <p>For example:</p> <pre>hostname# configure terminal</pre>	Enters global configuration mode from privileged EXEC mode.
Step 2	<p>ntp server ip_address [key key_id] [source interface_name] [prefer]</p> <p>For example:</p> <pre>hostname(config)# ntp server 171.68.10.80 key 1 source inside prefer</pre>	Configures an NTP server to ensure accurate time stamps. Entering this command enables better correlation between the ASA and MARS devices, because it ensures that the time on both are the same.
Step 3	<p>clear configure flow-export</p> <p>For example:</p> <pre>hostname(config)# clear configure flow-export</pre>	Clears all flow-export configurations associated with NetFlow data.
Step 4	<p>flow-export enable</p> <p>For example:</p> <pre>hostname(config)# flow-export enable</pre>	<p>For Version 8.1(1), when export of NetFlow data is enabled, the template records are sent to all configured NetFlow collectors. In addition, the device starts exporting NetFlow data events. When disabled, any pending cached NetFlow events will be removed, and the device stops exporting NetFlow events.</p> <p>For Version 8.1(2), the flow-export enable command has been deprecated. When you enter this command, flow-export actions are converted under Modular Policy Framework and the following informational message appears:</p> <pre>INFO: 'flow-export enable' command is deprecated. Converting to flow-export actions under MPF.</pre> <p>For Version 8.1(2), the no flow-export enable command is not supported. When you enter this command, the following error message appears:</p> <pre>ERROR: This command is no longer supported. Flow-export actions under MPF need to be removed to stop exporting NetFlow events.</pre>
Step 5	<p>flow-export destination interface-name ipv4-address hostname udp-port</p> <p>For example:</p> <pre>hostname(config)# flow-export destination inside cs-mars 2055</pre>	<p>Configures the ASA 5580 to export NetFlow events to a destination system (MARS).</p> <p>The example configures the ASA 5580 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.</p>

	Command	Description
Step 6	flow-export template timeout-rate <i>minutes</i> For example: <pre>hostname(config)# flow-export template timeout-rate 1</pre>	Sets the interval at which the template information is sent to NetFlow collectors. Use 1 minute for MARS.
Step 7	logging flow-export-syslogs {enable disable} For example: <pre>hostname(config)# logging flow-export-syslogs disable</pre>	Disables the redundant syslog messages. The syslog messages report the same events as the NetFlow security event logging.
Step 8	logging trap [<i>logging_list level</i>] For example: <pre>hostname(config)# logging trap informational</pre>	Sets the logging trap level to informational. You can also specify "6."
Step 9	logging host <i>interface_name</i> <i>syslog_ip</i> For example: <pre>hostname(config)# logging host cs-mars</pre>	Defines MARS as a syslog server. The example sets the logging host to the user-defined IP address of the MARS appliance using the ASA name command.
Step 10	logging enable For example: <pre>hostname(config)# clear configure flow-export cs-mars_ip</pre>	Enables logging to MARS
Step 11	exit For example: <pre>hostname(config)# exit</pre>	Logs out of global configuration mode into privileged EXEC mode.

Command	Description
<p>Step 12 show running-config [all] logging [level disabled]</p> <p>For example:</p> <pre>hostname# show running-config logging</pre>	<p>Displays the status of system logs, as follows:</p> <pre>ASA81-Single# show running-config logging 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</pre>
<p>Step 13 show running-config flow-export [destination enable template]</p> <p>For example:</p> <pre>hostname# show running-config flow-export</pre>	<p>Displays the status of flow exports, as follows:</p> <pre>ASA81-Single# show running-config flow-export 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</pre>