

Securing Networks with
Cisco FTD

Chapter 19

System Logging

(Syslog)

Mohsen Kheradmand

Syslog

- You can use logging for real-time alerting as well as for auditing purposes
- The Internet Engineering Task Force (IETF) standardizes system logging (syslog) in RFC 5424
- Secure Firewall supports sending syslog messages to third-party syslog servers and SIEM tools
- The FMC or the FTD can send logs to the syslog server separately , but it's better to choose one of these
- Syslog messages can be sent over TCP or UDP (TCP is more reliable but has more overhead due to the multiple connections)

RFC	Description
RFC 5424	The Syslog Protocol
RFC 5426	Transmission of Syslog Messages over UDP
RFC 6587	Transmission of Syslog Messages over TCP
RFC 5425	Transport Layer Security (TLS) Transport Mapping for Syslog

Syslog Security Levels

- Each syslog message is associated with a severity level
- A severity level indicates the significance of a message.

Severity Level (0–7)	Messages That Describe...
EMERG	An emergency condition where the system is unusable
ALERT	A condition where an action must be taken immediately to fix the issue
CRIT	A critical condition that indicates a failure in the primary system
ERR	An error condition
WARNING NOTICE	A warning condition
INFO	A condition that does not indicate an error but may require special attention
DEBUG	Debug-level information to help the developers of an application or system

Facility of Syslog message

- The IETF uses the term facility to refer to various subsystems

KERN : Kernel

USER : User-level process

MAIL : Mail system

DAEMON : System daemon

AUTH : Security/authentication subsystem

SYSLOG : System logging daemon (syslogd)

LPR : Line printer subsystem

NEWS : Network news subsystem

UUCP : Unix-to-Unix copy subsystem

CRON : Clock/scheduling daemon (Used by Syslog server running on a Linux OS)

AUTHPRIV : Security/authentication system

FTP : FTP daemon

NTP : NTP subsystem

AUDIT : Audit subsystem (Security log audit)

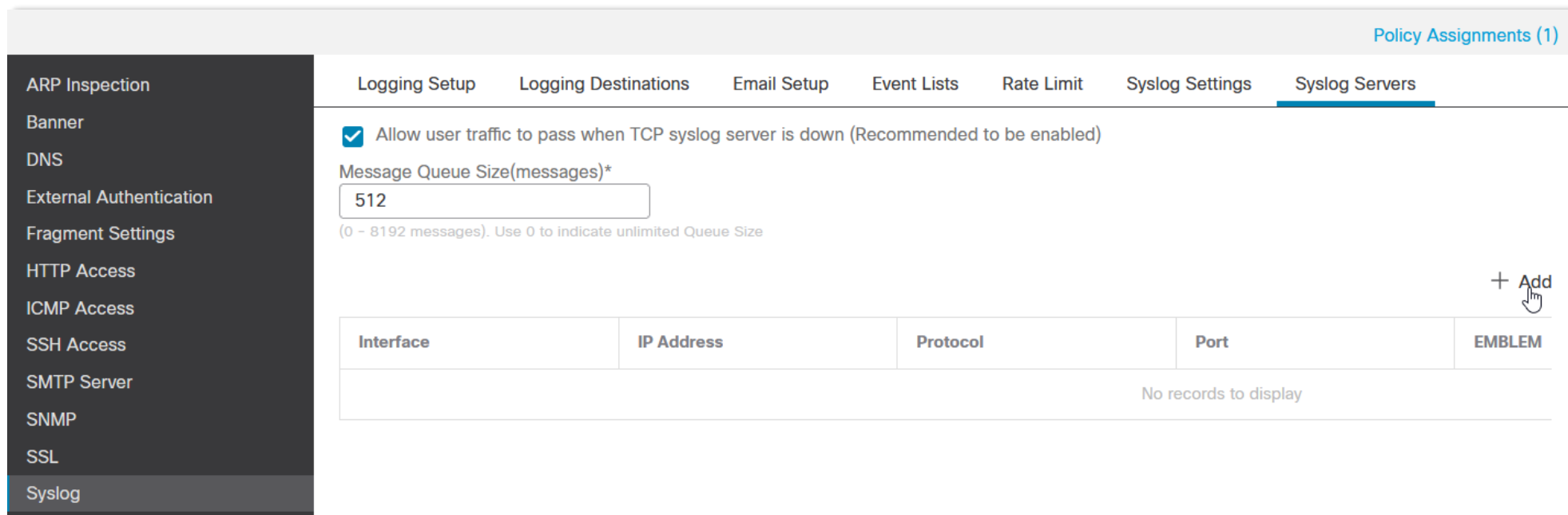
ALERT : Alerting subsystem (Console)

CLOCK : Clock/scheduling daemon (Used by Syslog server running on Windows OS)

LOCAL0–LOCAL7 : Locally defined facilities

Best Practices for Logging

- If your syslog server uses TCP, enable the **Allow User Traffic to Pass When TCP Syslog Server Is Down** option.
- It enables the traffic flow to continue in case of any issues with the syslog server



The screenshot shows the Mikrotik WinBox interface for configuring Syslog Servers. On the left is a sidebar menu with various system settings. The main panel has tabs for different logging-related settings, with 'Syslog Servers' currently selected. In this tab, there is a checkbox for 'Allow user traffic to pass when TCP syslog server is down' which is checked. Below this is a text input field for 'Message Queue Size(messages)*' with the value '512'. A table below the input field is empty, with columns for 'Interface', 'IP Address', 'Protocol', 'Port', and 'EMBLEM'. A '+ Add' button is located to the right of the table. The text 'No records to display' is shown at the bottom of the table area.

Policy Assignments (1)

ARP Inspection
Banner
DNS
External Authentication
Fragment Settings
HTTP Access
ICMP Access
SSH Access
SMTP Server
SNMP
SSL
Syslog

Logging Setup Logging Destinations Email Setup Event Lists Rate Limit Syslog Settings **Syslog Servers**

☒ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)*
512
(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

+ Add

Interface	IP Address	Protocol	Port	EMBLEM
No records to display				

- To prevent a syslog server from crashing, you can enable rate limiting for certain types of syslog messages
- Syslog over TCP can introduce overhead in a large deployment. In this case , syslog over UDP can improve performance.

Syslog configuration

- You can configure a Syslog server like Kiwi and configure address and port on it
- The default port for syslog servers is UDP port **514** or TCP port **1470**

The image shows the 'Kiwi Syslog Server Setup' window. The left sidebar contains a tree view with categories like 'Custom file formats', 'DNS Resolution', 'Alarms', and 'Inputs'. The 'Inputs' category is expanded, and 'UDP' is selected. The main area displays the 'UDP' configuration options, including a checkbox for 'Listen for UDP Syslog messages', a text field for 'UDP Port (1 - 65535)' set to '514', and a dropdown for 'Data encoding' set to 'System'. A title 'Protocol and Port Setup on Syslog Server GUI' is visible. Overlaid on this is a smaller 'Add Syslog Server' dialog. It has a text field for 'IP Address*' set to '10.1.1.100', radio buttons for 'Protocol' with 'UDP' selected, and a text field for 'Port' set to '514'. It also includes checkboxes for 'Log Messages in Cisco EMBLEM format(UDP only)' and 'Enable secure syslog.', and a 'Reachable By:' section with radio buttons for 'Device Management Interface' (selected) and 'Security Zones or Named Interface'. At the bottom, there are lists for 'Available Zones' (containing 'INSIDE_ZONE' and 'OUTSIDE_ZONE') and 'Selected Zones/Interfaces', with a search bar and an 'Add' button.

Sending Syslog from Threat Defense

Platform settings

- By using the platform settings policy, you can deploy different logging configurations to different threat defense devices
 - The platform settings policy allows you to configure many device-specific options in one place and then deploy them to one or more threat defense devices as needed.
- ❑ For example:
- You can add a custom banner to appear during a threat defense login
 - Allow the hosts that can communicate with a threat defense over SSH, HTTPS, and ICMP protocols
 - Define how the threat defense device will synchronize time with its management center or an NTP server
 - Provide health monitoring status over the simple network management protocol (SNMP)
 - Send security events and system messages to an external syslog server
 - And other configurations and settings

Sending Syslog from Threat Defense

Platform settings

Firepower Management Center
 Devices / Platform Settings

Overview
 Analysis
 Policies
 Devices
 Objects
 AMP
 Intelligence

Deploy
 ?
 ?
 admin

Platform Settings

New Policy

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

FTD1

Add to Policy

Selected Devices

FTD1

Cancel

Save

Object Management
 New Policy
 Firepower Settings
 Threat Defense Settings

- Devices > Platform Settings
- New Policy
- Threat Defense Settings
- Type a name
- Add the FTD to selected
- Click save

Sending Syslog from Threat Defense

- Click syslog
- Enable logging

The screenshot displays the Cisco Firepower Management Center (FMC) interface. At the top, the navigation bar includes the Cisco logo, the title "Firepower Management Center", and the breadcrumb "Devices / Platform Settings Editor". The main navigation tabs are Overview, Analysis, Policies, Devices (selected), Objects, AMP, and Intelligence. Below this, the "PL-Policy1" configuration page is shown with a sub-header "Enter Description". A left-hand sidebar lists various configuration categories, with "Syslog" highlighted and a mouse cursor pointing at it. The main content area for the "Syslog" configuration is divided into several tabs: Logging Setup (selected), Logging Destinations, Email Setup, Event Lists, Rate Limit, Syslog Settings, and Syslog Servers. Under the "Logging Setup" tab, the "Basic Logging Settings" section includes: "Enable Logging" (checked), "Enable Logging on the failover standby unit" (unchecked), "Send syslogs in EMBLEM format" (unchecked), and "Send debug messages as syslogs" (unchecked). The "Memory Size of the Internal Buffer" is set to 4096 (4096-52428800 Bytes). The "VPN Logging Settings" section includes "Enable Logging to FMC" (checked). The "Logging Level" is set to "errors". The "Specify FTP Server Information" section includes "FTP Server Buffer Wran" (unchecked).

Sending Syslog from Threat Defense

- Click Syslog Servers tab
- Click Add

The screenshot shows the Threat Defense configuration interface. On the left, a sidebar menu lists various configuration options, with 'Syslog' highlighted. The main area displays the 'Syslog Servers' tab. A modal dialog titled 'Add Syslog Server' is open, showing the following fields and options:

- IP Address***: 192.168.10.245
- Protocol**: ☐ TCP, ☒ UDP
- Port**: 514 (with a note: (514 or 1025-65535))
- Log Messages in Cisco EMBLEM format(UDP only)**: ☒
- Enable secure syslog.**: ☐
- Reachable By:**
 - ☒ Device Management Interface (Applicable on FTD v6.3.0 and above)
 - ☐ Security Zones or Named Interface
- Available Zones**: DMZ, Inside-LAN, Internet
- Selected Zones/Interfaces**: (Empty)
- Interface Name**: (Empty)

Buttons at the bottom of the dialog include 'Cancel' and 'OK'. On the right side of the main interface, there is a '+ Add' button and an 'EMBLEM' button.

- Enter the syslog server IP address, transport protocol, and port number.
- If syslog server is in management network select Device Management Interface
- If not , select other source interface to send logs through that
- Click Ok

Enable Logging on Access Control Policy

Policies

Access Control Policy

Select the policy

Click Logging tab

Select these items as you see :

The screenshot shows the Cisco FMC Policy Editor interface. The top navigation bar includes tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, Intelligence, and Deploy. The main header displays 'AC Policy' with buttons for 'Show Warnings', 'Analyze Hit Counts', 'Save', and 'Cancel'. Below the header, there are tabs for Rules, Security Intelligence, HTTP Responses, Logging (selected), and Advanced. The 'Logging' tab is active, showing 'Default Syslog Settings'. The text indicates that the following configuration will be used for all syslog destinations in this AC policy. The settings include: 'Send using specific syslog alert' (unchecked), 'Syslog Alert' (dropdown menu), 'Use the syslog settings configured in the FTD Platform Settings policy deployed on the device' (checked), 'Syslog Severity' (dropdown menu set to 'ALERT'), 'IPS Settings' (checked), 'Send Syslog messages for IPS events' (checked), 'Default syslog settings configured above are used for syslog destinations for IPS events' (text), 'Show Overrides' (link), 'File and Malware Settings' (checked), 'Send Syslog messages for File and Malware events' (checked), 'Default syslog settings configured above are used for syslog destinations for File and Malware events' (text), and 'Show Overrides' (link).

Sending Syslog from Management Center

Create Syslog Alerts

Policies > Actions > Alert

Create Alert

Create Syslog Alert

The screenshot shows the Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and a breadcrumb trail 'Policies / Actions / Alerts / Alerts'. Below this, there are tabs for 'Overview', 'Analysis', and 'Policies'. The 'Policies' tab is active, and within it, the 'Alerts' sub-tab is selected. A table with the following headers is visible: 'Alerts', 'Impact Flag Alerts', 'Discovery Event Alerts', and 'Advanced Malware Protection Alerts'. The 'Alerts' column is highlighted. Below the table, there is a form with a 'Name' label and an empty input field.

Enter a name for this Alert

Enter Syslog server Address

Select Port , Facility and Severity and the click Ok

The screenshot shows the 'Edit Syslog Alert Configuration' dialog box. It has a title bar with a question mark icon. The form contains the following fields: 'Name' (text input with 'FMC-Syslog'), 'Host' (text input with '192.168.10.245'), 'Port' (text input with '514'), 'Facility' (dropdown menu with 'ALERT' selected), 'Severity' (dropdown menu with 'ALERT' selected), and 'Tag' (text input). At the bottom right, there are 'Cancel' and 'Save' buttons.

The screenshot shows a 'Create Alert' dropdown menu. The menu is open, showing three options: 'Create Email Alert', 'Create SNMP Alert', and 'Create Syslog Alert'. The 'Create Syslog Alert' option is highlighted with a mouse cursor.

Sending Syslog from Management Center

Impact Flag Alerts

- You can choose the types of events for which you want to receive alerts on the syslog server
- Select Syslog Server
- Optional : select Email address to send Alerts
- Optional : configure SNMP to send alerts as a Trap
- Select Impact Level to send Logs
- Click Save

Alerts

Impact Flag Alerts

Discovery Event Alerts

Advanced Malware Protection Alerts

Intrusion Email

Alerts

Select alert responses to use for Impact Flag alerts. You must click Save after you make your selections.

Syslog

FMC-Syslog

Email

None

SNMP

None

Impact Flag Configuration

Check boxes below to cause Intrusion Events with the associated Impact Flag to generate alerts.

Impact Flag	Syslog Notification	Email Notification	SNMP Notification
☐ Unknown	☒	☐	☐
☐ Unknown Target	☒	☐	☐
☒ Currently Not Vulnerable	☒	☐	☐
☒ Potentially Vulnerable	☒	☐	☐
☒ Vulnerable	☒	☐	☐

Save

Sending Syslog from Management Center

Discovery Event Alerts

- To trigger these alerts, the FMC requires an active Network Discovery policy
- Select Syslog server , (Email or SNMP)
- Select event type for which to generate alerts
- Click Save

Alerts

Impact Flag Alerts

Discovery Event Alerts

Advanced Malware Protection Alerts

Intrusion Email

Alerts

Select alert responses to use for discovery event alerts. You must click Save after you make your selections.

Syslog

FMC-Syslog

Email

None

SNMP

None

Events Configuration

Select the event types for which you want to generate alerts.

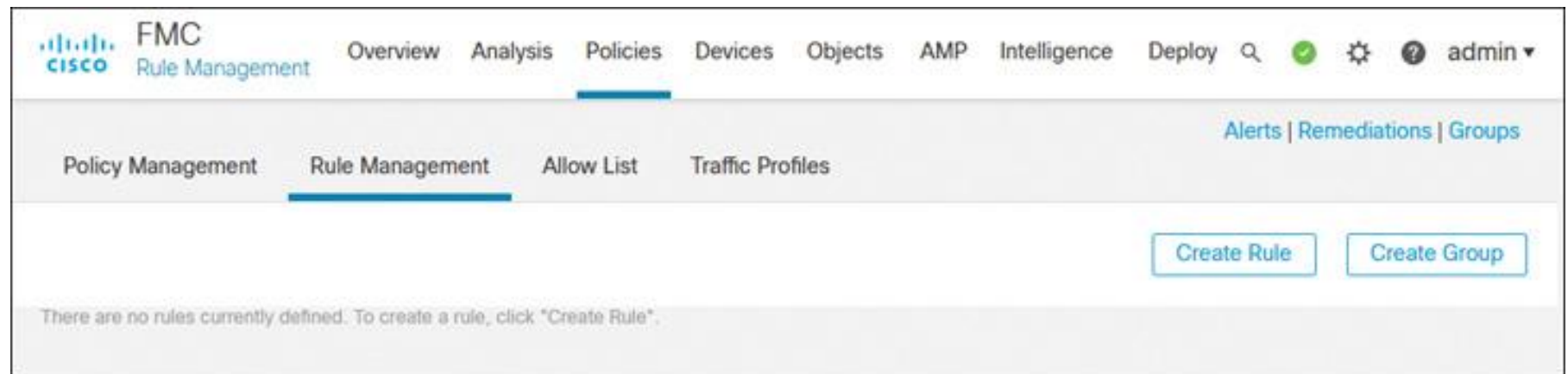
Event	Syslog Notification	Email Notification	SNMP Notification
Add Client	☒	☐	☐
Add Host	☒	☐	☐
Add Port	☒	☐	☐
Add Protocol	☐	☐	☐
Add Scan Result	☐	☐	☐
Additional MAC Detected for Host	☒	☐	☐
Client Timeout	☐	☐	☐
Client Update	☒	☐	☐
Delete Client	☒	☐	☐
Delete Host/Network	☒	☐	☐
Delete Port	☒	☐	☐

Correlate Events to Send Syslog Alerts

- Correlation policy: produce syslog events under the specific set of conditions in logging
- You can create correlation rules based on discovery events, intrusion events, file events, connection events, and a variety of other conditions

1) Create a rule :

- Policies > Correlation
- Rule Management tab
- Create Rule



Correlate Events to Send Syslog Alerts

- Enter a name for rule
- Optional : description
- Optional : Rule group
- Select the type of event
- Click Add Condition
- Add your conditions to take effect
- Click Save

Policy Management
Rule Management
Allow List
Traffic Profiles

Rule Information
Add Connection Tracker
Add User Qualification
Add Host Profile Qualification

Rule Name
Intrusion-Egress-Logs

Rule Description

Rule Group
Ungrouped

Select the type of event for this rule

If
an intrusion event occurs
and it meets the following conditions:

Add condition
Add complex condition

AND

Egress Interface
is
FTD1 / outside

Egress Security Zone
is
Internet

Protocol
is
TCP

Rule Options
Add Inactive Period

Snooze
If this rule generates an event, snooze for
0
hours

Inactive Periods
There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

Cancel
Save

Correlate Events to Send Syslog Alerts

2) Create a Policy

- Click Policy Management tab
- Type a name for the Policy
- Click Add rule
- Select the Rules (you have creates)

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy

Policy Management Rule Management Allow List Traffic Profiles

Cancel Save

Correlation Policy Information

Policy Name

Policy Description

Default Priority

Policy Rules

No Rules Currently Active

Available Rules

Select the rules you wish to add to this policy, then click "Add".

▼ Ungrouped Rules

☒ Intrusion-Egress-Logs

▼ Allow List Rules

☐ Default Allow List

Cancel Add

Add Rules

Correlate Events to Send Syslog Alerts

- 3) Assign policy to Syslog server
- Click Responses (next to the policy name)
 - Move the preconfigured syslog alert to the Assigned Responses creates)
 - Click update and then click Save

Policy Management

Rule Management

Allow List

Traffic Profiles

Cancel

Save

You have 1 rule

Correlation Policy Information

Policy Name

Custom-Policy

Policy Description

Default Priority

None

Policy Rules

Add Rules

Rule	Responses	Priority	
Intrusion-Egress-Logs	This rule does not have any responses.	Default	

Responses for Intrusion-Egress-Logs

Assigned Responses

FMC-Syslog

Unassigned Responses

Cancel

Update

Correlate Events to Send Syslog Alerts

4) Activate the Policy

- Make sure to activate it

[Alerts](#) | [Remediations](#) | [Groups](#)

[Policy Management](#) | [Rule Management](#) | [Allow List](#) | [Traffic Profiles](#)

Create Policy

Success
Activated Policy: Custom-Policy

Name	Sort by
Custom-Policy	State

Monitoring

To View the syslog messages of the FMC

➤ Monitoring > Syslog

