Contents

Introduction

This document describes Firepower module’s system/ traffic events and various method of sending these events to an external logging server.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of ASA (Adaptive Security Appliance) firewall, ASDM (Adaptive Security Device Manager).
- Firepower appliance Knowledge.
- Syslog, SNMP protocol knowledge.

Components Used

The information in this document is based on these software and hardware versions:

- ASA Firepower modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) running software version 5.4.1 and above
- ASA Firepower module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) running software version 6.0.0 and above.
- ASDM 7.5(1) and above.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Type of Events

Firepower Module events can be categorized in two types:-

1. Traffic Events (Connection events/Intrusion Events/Security Intelligence Events/SSL Events/Malware/File Events).
2. System Events (Firepower Operating System (OS) events).

Configure

Configuring an Output Destination

Step 1. Syslog Server Configuration

To configure a Syslog Server for traffic events, Navigate to **Configuration > ASA Firepower Configuration > Policies > Actions Alerts** and click the **Create Alert** drop-down menu and choose option **Create Syslog Alert.** Enter the values for the Syslog server.

Name: Specify the name which uniquely identifies the Syslog server.

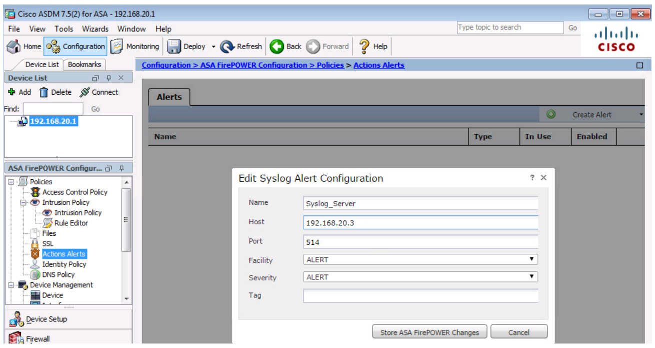
Host: Specify the IP address/hostname of Syslog server.

Port: Specify the port number of Syslog server.

Facility: Select any facility that is configured on your Syslog server.

Severity: Select any Severity that is configured on your Syslog server.

Tag: Specify tag name that you want to appear with the Syslog message.



Name: Syslog_Server
Host: 192.168.20.3
Port: 514
Facility: ALERT
Severity: ALERT
Tag:

Step 2.

To configure an SNMP Trap server for traffic events, **ASDM Configuration > ASA Firepower Configuration > Policies > Actions Alerts** and click the **Create Alert** drop-down menu and choose option **Create SNMP Alert.**

Name: Specify the name which uniquely identifies the SNMP Trap server.

Trap Server: Specify IP address/hostname of SNMP trap server.

Version: Firepower Module supports SNMP v1/v2/v3. Select the SNMP version from the drop down menu.

Community string: If you select**Version** option, Specify the SNMP community name.

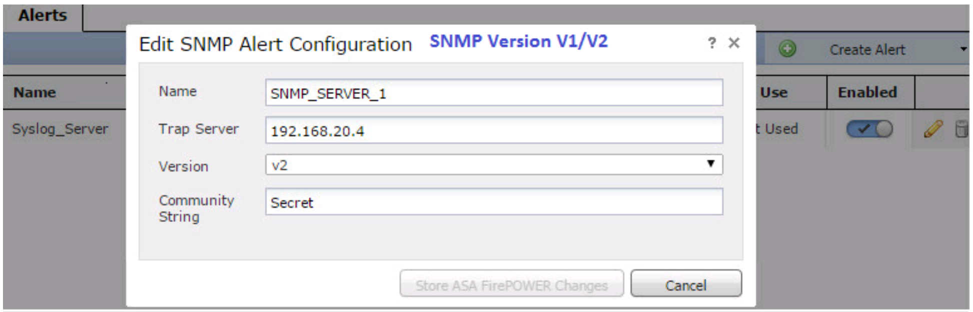
Username: If you select v3 in **Version** option, the system prompts **User Name** field. Specify the username.

Authentication: This option is a part of SNMP v3 configuration. It provides authentication based on the Hash

algorithm using either MD5 or SHA algorithms. In **Protocol** drop down menu select the hash algorithm & enter

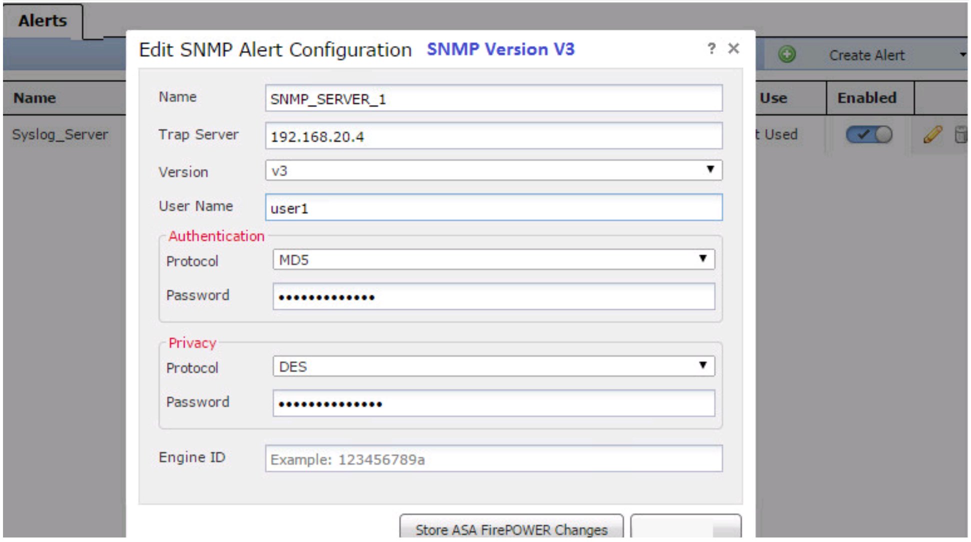
password in **Password** option. If you do not want to use this feature, then select **None** option.

Privacy: This option is a part of SNMP v3 configuration. It provides encryption using DES algorithm. In **Protocol** drop menu select the option as **DES**& enter password in **Password** field. If you do not want to use data encryption feature, then choose **None** option.



Edit SNMP Alert Configuration SNMP Version V1/V2

Name: SNMP_SERVER_1
Trap Server: 192.168.20.4
Version: v2
Community String: Secret



Edit SNMP Alert Configuration SNMP Version V3

Name: SNMP_SERVER_1
Trap Server: 192.168.20.4
Version: v3
User Name: user1
Authentication
Protocol: MD5
Password: •••••••••••••
Privacy
Protocol: DES
Password: ••••••••••••••
Engine ID: Example: 123456789a

Configuration for sending the Traffic Events

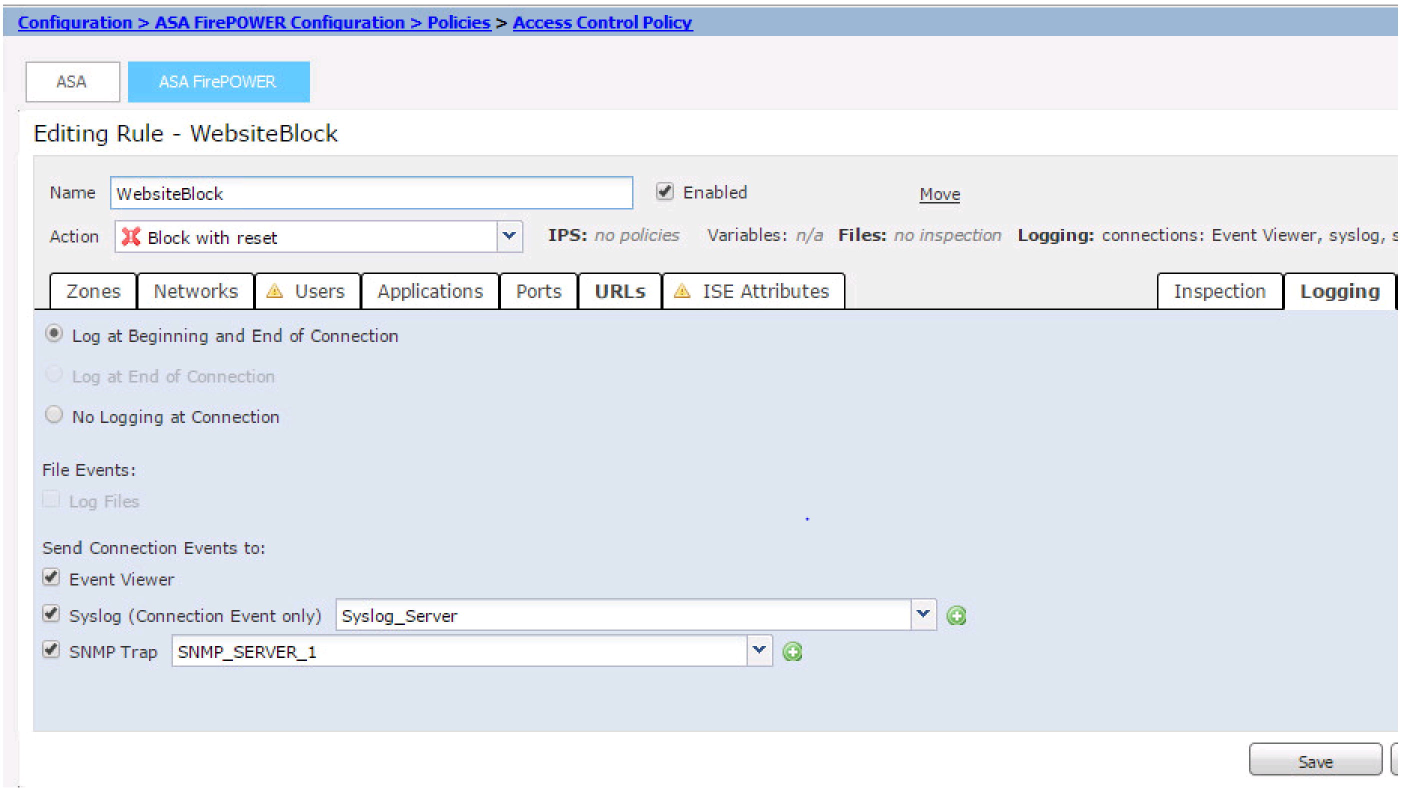
Enable external logging for Connection Events

Connection Events are generated when traffic hits an access rule with logging enabled. In order to enable the external logging for connection events, navigate to **(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy)** edit the **access rule** and navigate to **logging** option.

Select the logging option either **log at Beginning and End of Connection** or **log at End of Connection**. Navigate to **Send Connection Events to** option and specify where to send events.

In order to send events to an external Syslog server, select **Syslog**, and then select a Syslog alert response from the drop-down list. Optionally, you can add a Syslog alert response by clicking the add **icon**.

To send connection events to an SNMP trap server, select **SNMP Trap**, and then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add **icon**.



Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

Editing Rule - WebsiteBlock

Name: WebsiteBlock ☑ Enabled

Action: Block with reset

IPS: *no policies* Variables: *n/a* **Files:** *no inspection* **Logging:** connections: Event Viewer, syslog, s

● Log at Beginning and End of Connection

○ Log at End of Connection

○ No Logging at Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

☑ Syslog (Connection Event only) Syslog_Server

☑ SNMP Trap SNMP_SERVER_1

Enable external logging for Intrusion Events

Intrusion events are generated when a signature (snort rules) matches some malicious traffic. **ASDM Configuration > ASA Firepower Configuration > Policies> Intrusion Policy > Intrusion Policy.** Either create a new Intrusion policy or edit existing Intrusion Policy. **Advanced Setting** > **External Responses.**

In order to send intrusion events to an external SNMP server, select **Enabled** option in **SNMP Alerting** and then click the **Edit** option.

Trap Type: The trap type is used for IP addresses that appear in the alerts. If your network management system correctly renders the INET_IPV4 address type, then you can select as Binary. Otherwise, select as String.

SNMP Version: Select either **Version 2** or **Version 3** radio button.

SNMP v2 option

Trap Server: Specify the IP address/hostname of SNMP Trap server, as shown in this image.

Community String: Specify the community name.

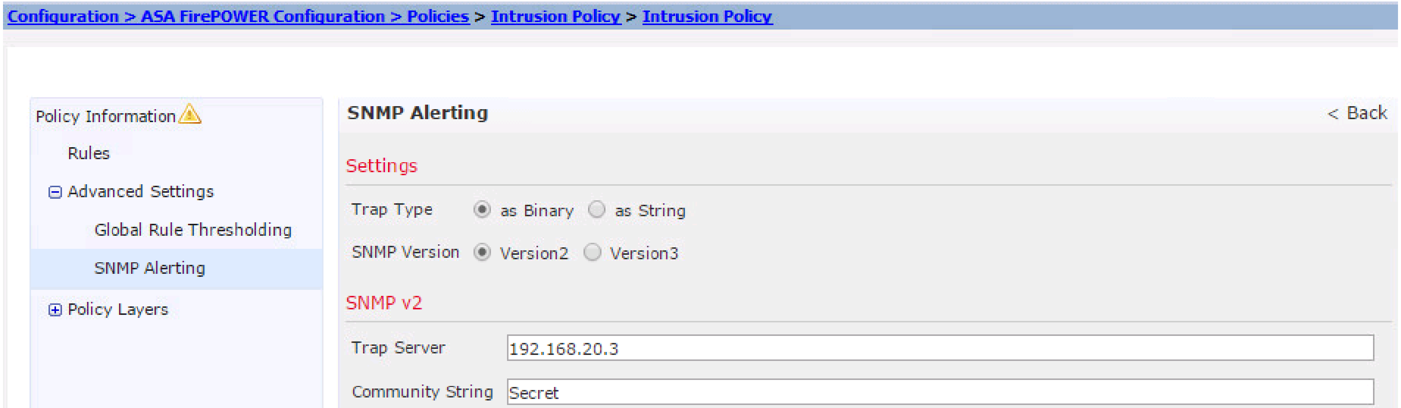
SNMP v3 Option

Trap Server: Specify the IP address/hostname of SNMP Trap server, as shown in this image.

Authentication Password: Specify password.

Private Password: Specify password for encryption. SNMP v3 uses Data Encryption Standard (DES) block cipher to encrypt this password.

User Name: Specify the Username.



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

SNMP Alerting

< Back

Settings

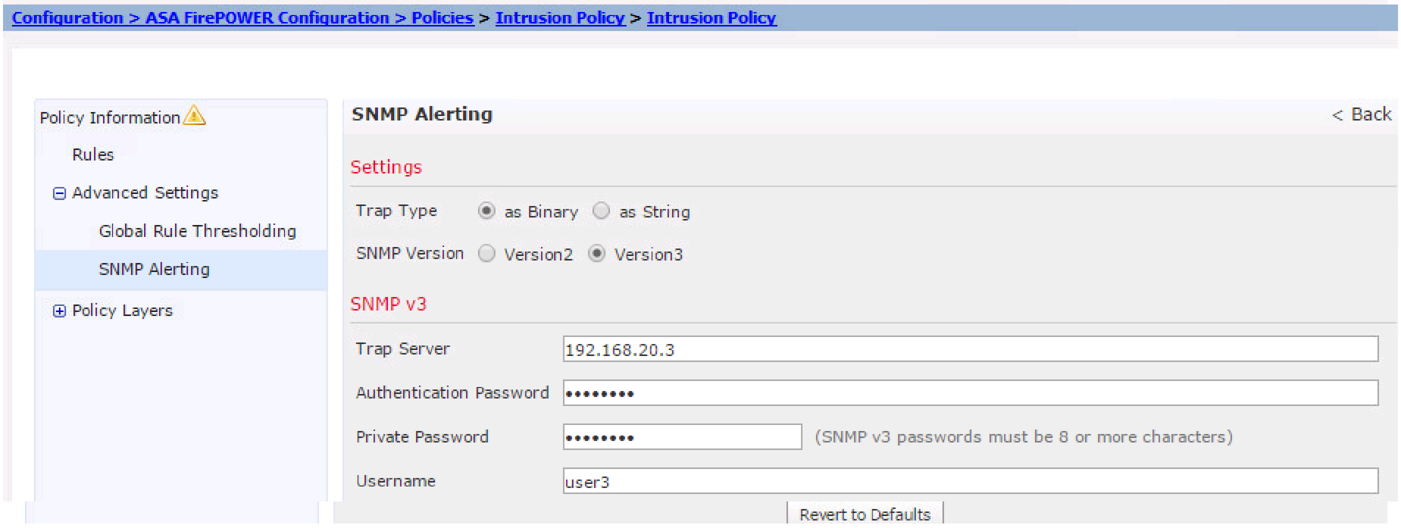
Trap Type ● as Binary ○ as String

SNMP Version ● Version2 ○ Version3

SNMP v2

Trap Server: 192.168.20.3

Community String: Secret



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

SNMP Alerting

< Back

Settings

Trap Type ● as Binary ○ as String

SNMP Version ○ Version2 ● Version3

SNMP v3

Trap Server: 192.168.20.3

Authentication Password: ••••••••

Private Password: •••••••• (SNMP v3 passwords must be 8 or more characters)

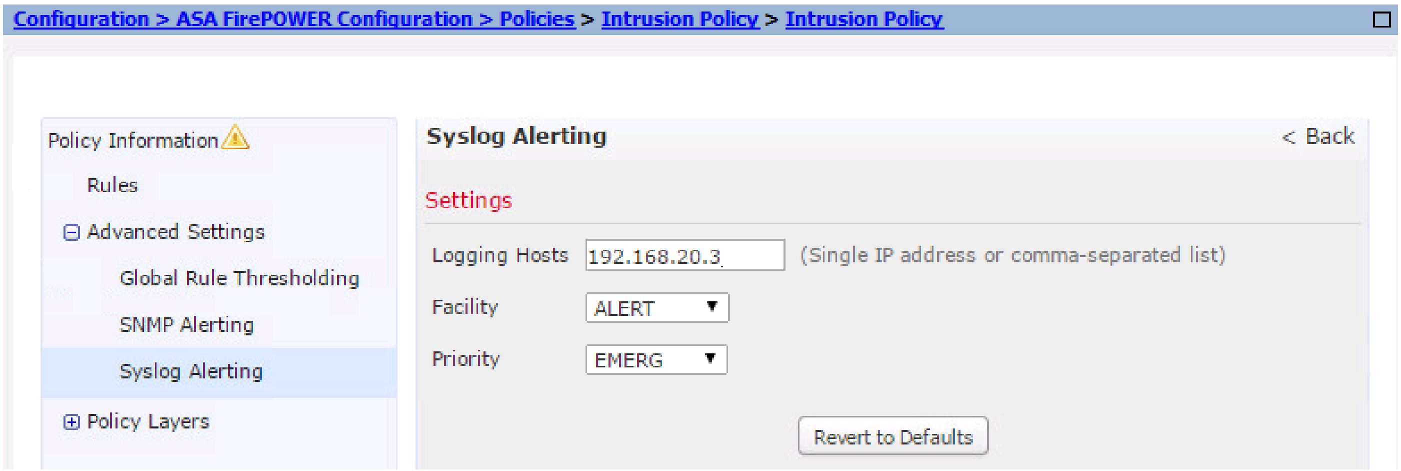
Username: user3

In order to send intrusion events to an external Syslog server, select option **Enabled** in **Syslog** then click the **Edit** option, as shown in this image.

Logging Host: Specify the IP address/hostname of Syslog server.

Facility: Select any facility that is configured on your Syslog server.

Severity: Select any Severity that is configured on your Syslog server.



Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

Syslog Alerting

Settings

Logging Hosts: 192.168.20.3 (Single IP address or comma-separated list)

Facility: ALERT

Priority: EMERG

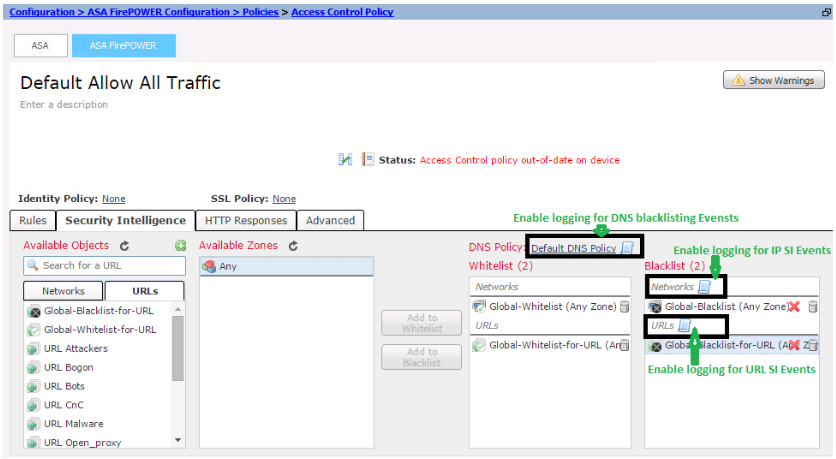
Enable external logging for IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence

IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence events are generated when traffic matches any IP address/domain name/URL Security Intelligence database. In order to enable the external logging for IP/ URL/DNS Security Intelligence Events, navigate to **(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy > Security Intelligence)**,

Click the **icon** as shown in the image to enable the logging for IP/DNS/URL Security Intelligence. Clicking the icon prompts a dialog box to enable logging and option to send the events to the external server.

In order to send events to an external Syslog server, select **Syslog**, and then select a Syslog alert response from the drop-down list. Optionally, you can add a Syslog alert response by clicking the add icon.

In order to send connection events to an SNMP trap server, select **SNMP Trap**, and then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add icon.



Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

Default Allow All Traffic

Enter a description

Status: Access Control policy out-of-date on device

Identity Policy: None

SSL Policy: None

DNS Policy: Default DNS Policy

Whitelist (2)

Networks: Global-Whitelist (Any Zone)

URLs: Global-Whitelist-for-URL (An

Blacklist (2)

Networks: Global-Blacklist (Any Zone)

URLs: Global-Blacklist-for-URL (Any Z

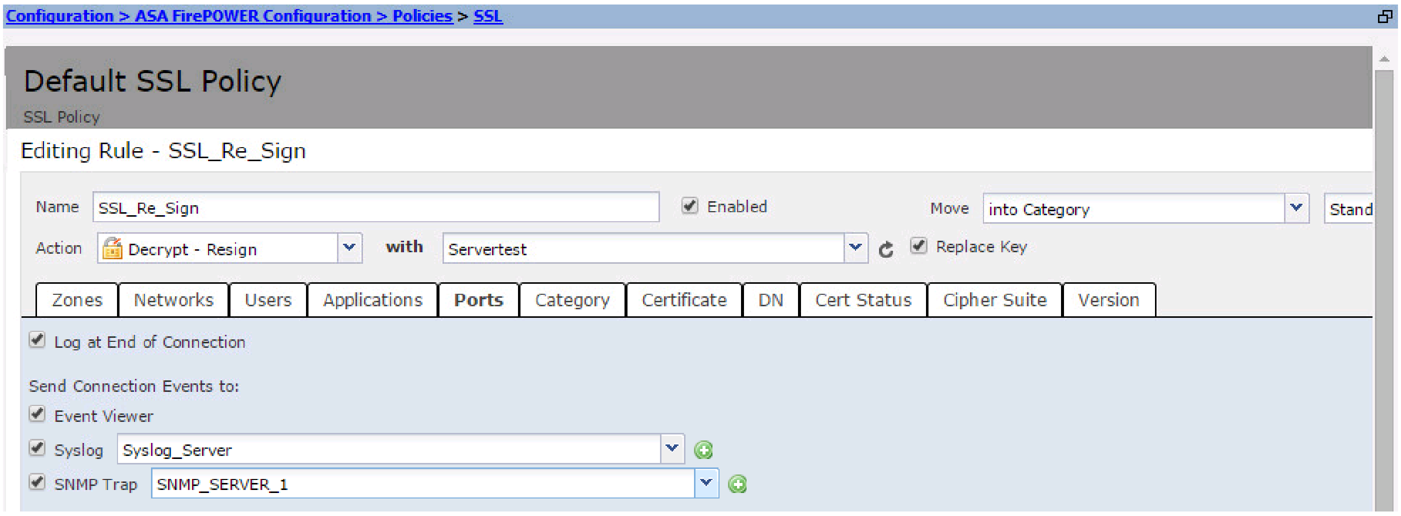
Enable external logging for SSL events

SSL events are generated when traffic matches any rule in SSL policy, in which logging is enabled. In order to enable the external logging for SSL traffic, navigate to **ASDM Configuration > ASA Firepower Configuration > Policies > SSL.** Edit the existing or create a new rule and navigate to **logging** option.Select **log at End of Connection** option.

Then navigate to **Send Connection Events to** and specify where to send the events.

To send events to an external Syslog server, select **Syslog**, and then select a Syslog alert response from the drop-down list. Optionally, you can add a Syslog alert response by clicking the add icon.

To send connection events to an SNMP trap server, select **SNMP Trap**, and then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add icon.



Editing Rule - SSL_Re_Sign

Name SSL_Re_Sign ☑ Enabled Move into Category Stand

Action Decrypt - Resign with Servertest ☑ Replace Key

☑ Log at End of Connection

Send Connection Events to:

☑ Event Viewer

☑ Syslog Syslog_Server

☑ SNMP Trap SNMP_SERVER_1

Configuration for sending the System Events

Enable external logging for system events

System events show the status of Firepower Operating System. SNMP manager can be used to poll these systems events.

To configure SNMP server in order to poll system events from Firepower Module, you need to configure a System Policy which makes the information available in firepower MIB (Management Information Base) which can be polled by the SNMP server.

Navigate to **ASDM Configuration > ASA Firepower Configuration > Local > System Policy** and click the **SNMP**.

SNMP Version: Firepower Module supports SNMP v1/v2/v3. Specify the SNMP version.

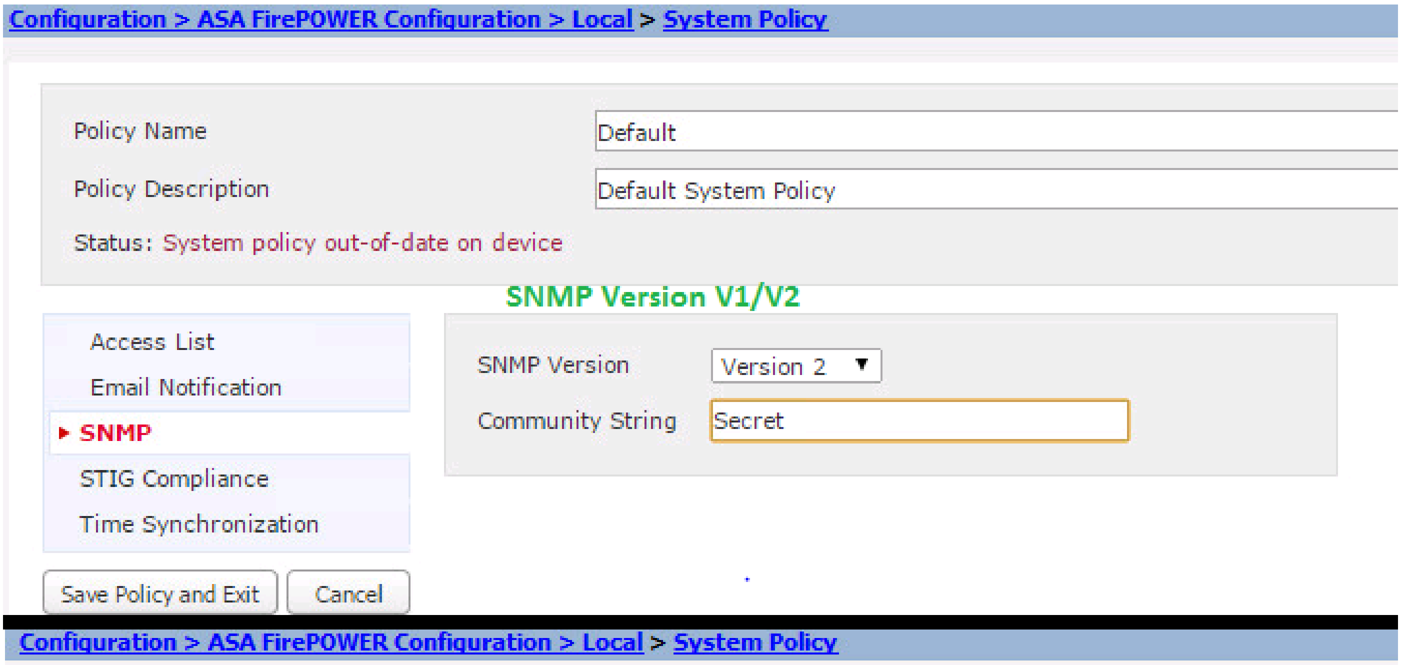
Community string: If you select **v1** in SNMP version option, type the SNMP community name in the Community String field.

Username: If you select the **v3** option in version option. Click the **Add User** button and specify the **Username** in the username field.

Authentication: This option is a part of SNMP v3 configuration. It provides authentication based on the Hashed Message Authentication Code using MD5 or SHA algorithms. Choose **Protocol** for hash algorithm & enter password

in **Password** field. If you do not want to use authentication feature then select **None** option.

Privacy: This option is a part of SNMP v3 configuration. It provides encryption using DES/AES algorithm. Select protocol **Password** field. If you do not want data encryption feature then choose **None** option.



Configuration > ASA FirePOWER Configuration > Local > System Policy

Policy Name: Default

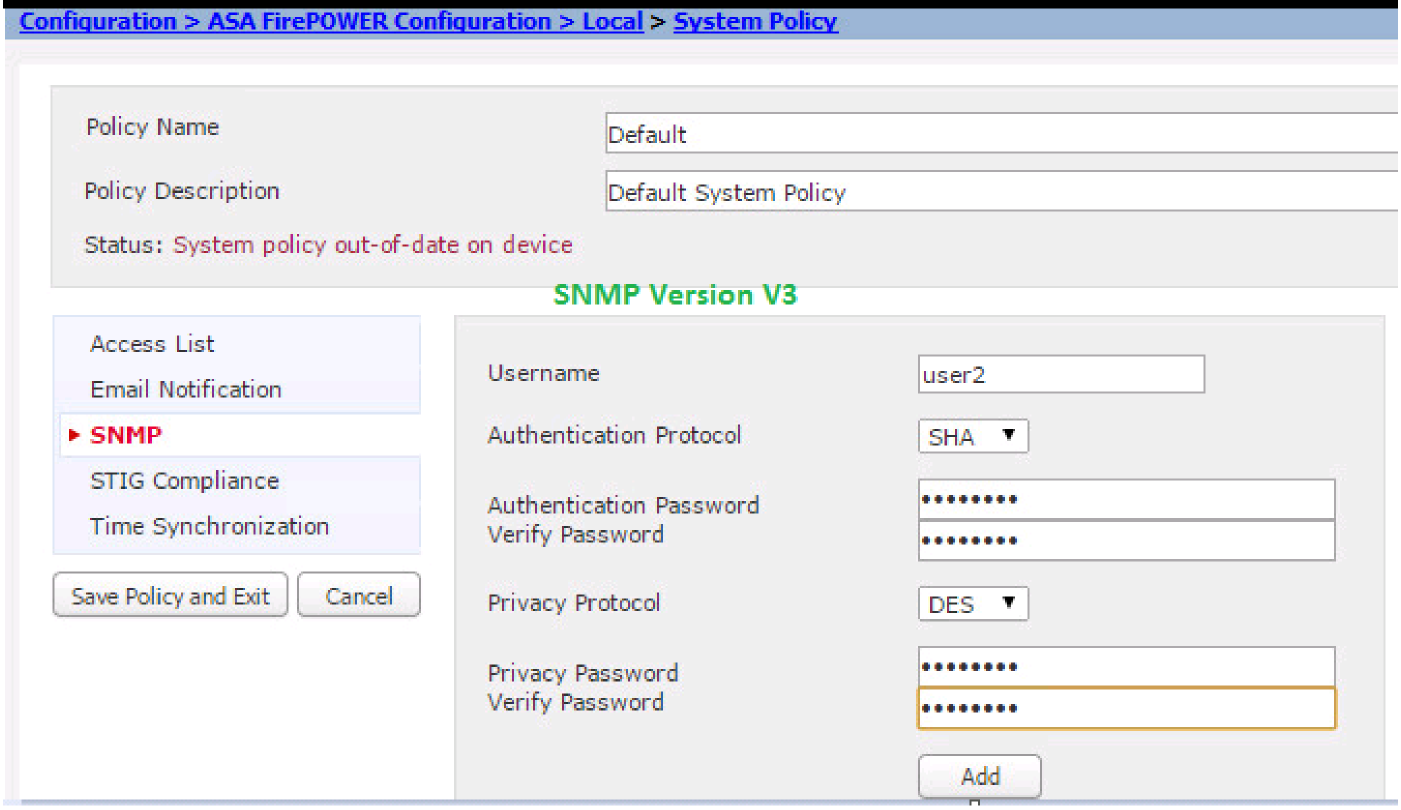
Policy Description: Default System Policy

Status: System policy out-of-date on device

SNMP Version V1/V2

SNMP Version: Version 2

Community String: Secret



Configuration > ASA FirePOWER Configuration > Local > System Policy

Policy Name: Default

Policy Description: Default System Policy

Status: System policy out-of-date on device

SNMP Version V3

Username: user2

Authentication Protocol: SHA

Authentication Password: ••••••••

Verify Password: ••••••••

Privacy Protocol: DES

Privacy Password: ••••••••

Verify Password: ••••••••

Note: A management information base (MIB)is a collection of information that is organized hierarchically. MIB file (DCEALERT.MIB) for Firepower Module is available at directory location (/etc/sf/DCEALERT.MIB) which can be fetched from this directory location.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation - Cisco Systems**