Konfigurieren der Protokollierung im FirePOWER-Modul für System-/Datenverkehrsereignisse mithilfe von ASDM (integriertes Management)

Inhalt

Einführung

In diesem Dokument werden die System-/Datenverkehrsereignisse des FirePOWER-Moduls sowie die verschiedenen Methoden zum Senden dieser Ereignisse an einen externen Protokollierungsserver beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis der ASA (Adaptive Security Appliance)-Firewall, ASDM (Adaptive Security Device

Manager).
- Kenntnisse der FirePOWER-Appliance.
- Syslog, SNMP-Protokoll-Kenntnisse.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 5.4.1 und höher.
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 und höher.
- ASDM 7.5(1) und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Ereignistyp

FirePOWER-Modulereignisse können in zwei Kategorien eingeteilt werden:

1. Datenverkehrsereignisse (Verbindungsereignisse/Angriffsversuche/Sicherheitsinformationsereignisse/SSL-Ereignisse/Malware/Dateiereignisse).
2. Systemereignisse (FirePOWER-Betriebssystemereignisse).

Konfigurieren

Konfigurieren eines Ausgabeziels

Schritt 1: Syslog-Serverkonfiguration

Um einen Syslog-Server für Datenverkehrsereignisse zu konfigurieren, navigieren Sie zu **Konfiguration > ASA-Firepower-Konfiguration > Richtlinien > Aktionswarnungen** und klicken Sie auf das Dropdown-Menü **Create Alert** (Warnmeldung erstellen), und wählen Sie die Option **Syslog Alert erstellen aus.** Geben Sie die Werte für den Syslog-Server ein.

Name: Geben Sie den Namen an, der den Syslog-Server eindeutig identifiziert.

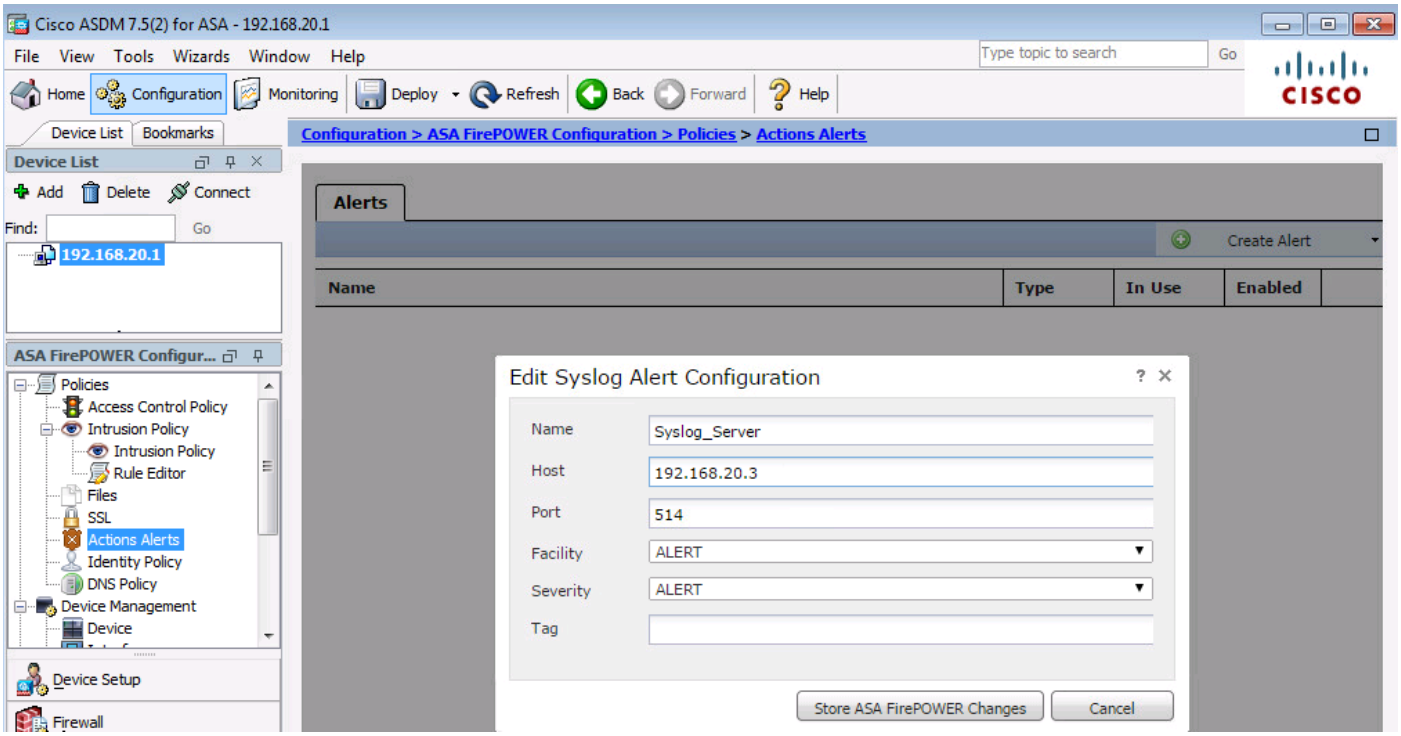
Host: Geben Sie die IP-Adresse/den Hostnamen des Syslog-Servers an.

Port: Geben Sie die Portnummer des Syslog-Servers an.

Einrichtung: Wählen Sie eine beliebige Einrichtung, die auf Ihrem Syslog-Server konfiguriert ist.

Schweregrad: Wählen Sie einen beliebigen Schweregrad aus, der auf Ihrem Syslog-Server konfiguriert ist.

Tag: Geben Sie den Tagnamen an, der zusammen mit der Syslog-Meldung angezeigt werden soll.



Schritt 2:SNMP-Serverkonfiguration

Um einen SNMP-Trap-Server für Datenverkehrsereignisse zu konfigurieren, navigieren Sie zu **ASDM Configuration > ASA FirePOWER Configuration > Policies > Actions Alerts (ASDM-Konfiguration > ASA FirePOWER-Konfiguration > Aktionswarnungen),** und klicken Sie auf das Dropdown-Menü **Create Alert (Warnmeldung erstellen)** und wählen die Option **SNMP Alert erstellen.**

Name: Geben Sie den Namen an, der den SNMP-Trap-Server eindeutig identifiziert.

Trap Server: Geben Sie die IP-Adresse/den Hostnamen des SNMP-Trap-Servers an.

Version: Das FirePOWER-Modul unterstützt SNMP v1/v2/v3. Wählen Sie die SNMP-Version aus dem Dropdown-Menü aus.

Community String: Wenn Sie die Option v1 oder v2 in **Version** auswählen, geben Sie den SNMP-Community-Namen an.

Benutzername: Wenn Sie die Option v3 in **Version** auswählen, fordert das System das Feld **Benutzername** auf. Geben Sie den Benutzernamen an.

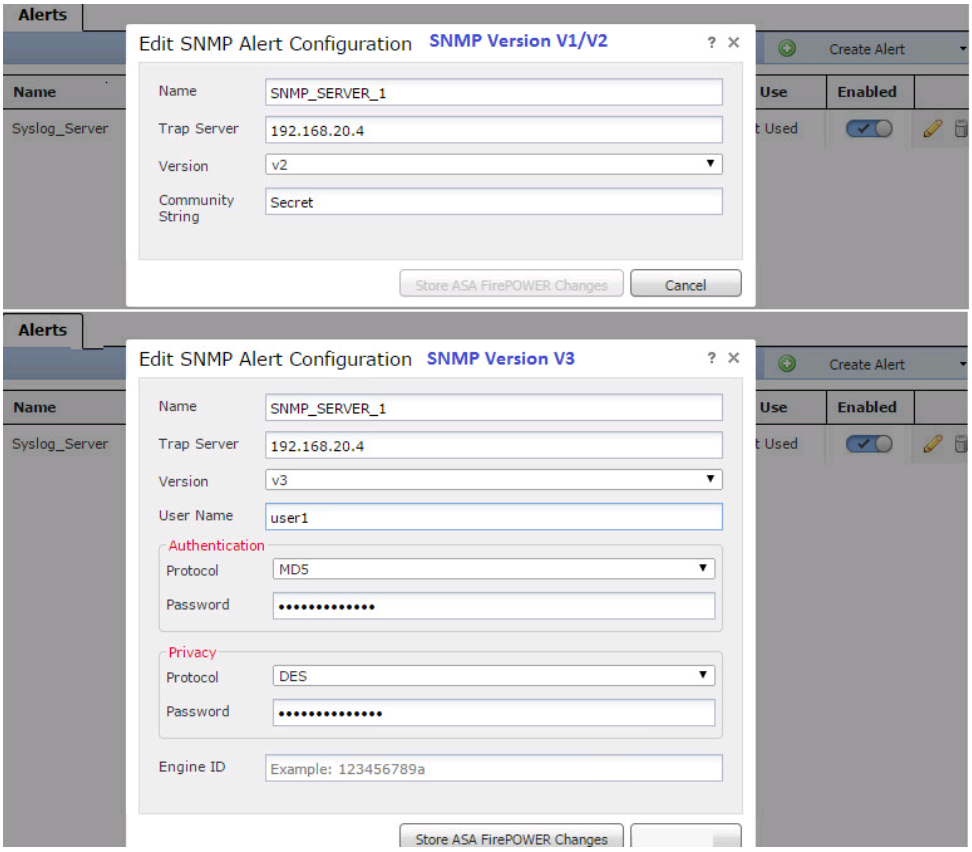
Authentifizierung: Diese Option ist Teil der SNMP v3-Konfiguration. Er stellt eine Authentifizierung basierend auf dem Hash bereit.

Algorithmen, die entweder MD5- oder SHA-Algorithmen verwenden. Wählen Sie im Dropdown-Menü **Protokoll** den Hash-Algorithmus aus, und geben Sie Folgendes ein:

Option "Kennwort in **Kennwort**". Wenn Sie diese Funktion nicht verwenden möchten, wählen Sie

die Option **Keine**.

Datenschutz: Diese Option ist Teil der SNMP v3-Konfiguration. Er stellt Verschlüsselung mithilfe des DES-Algorithmus bereit. Wählen Sie im **Protokoll-**Dropdown-Menü die Option **DES** und geben Sie das Kennwort in das Feld **Kennwort ein**. Wenn Sie die Datenverschlüsselungsfunktion nicht verwenden möchten, wählen Sie die Option **Keine**.



Konfiguration zum Senden von Datenverkehrsereignissen

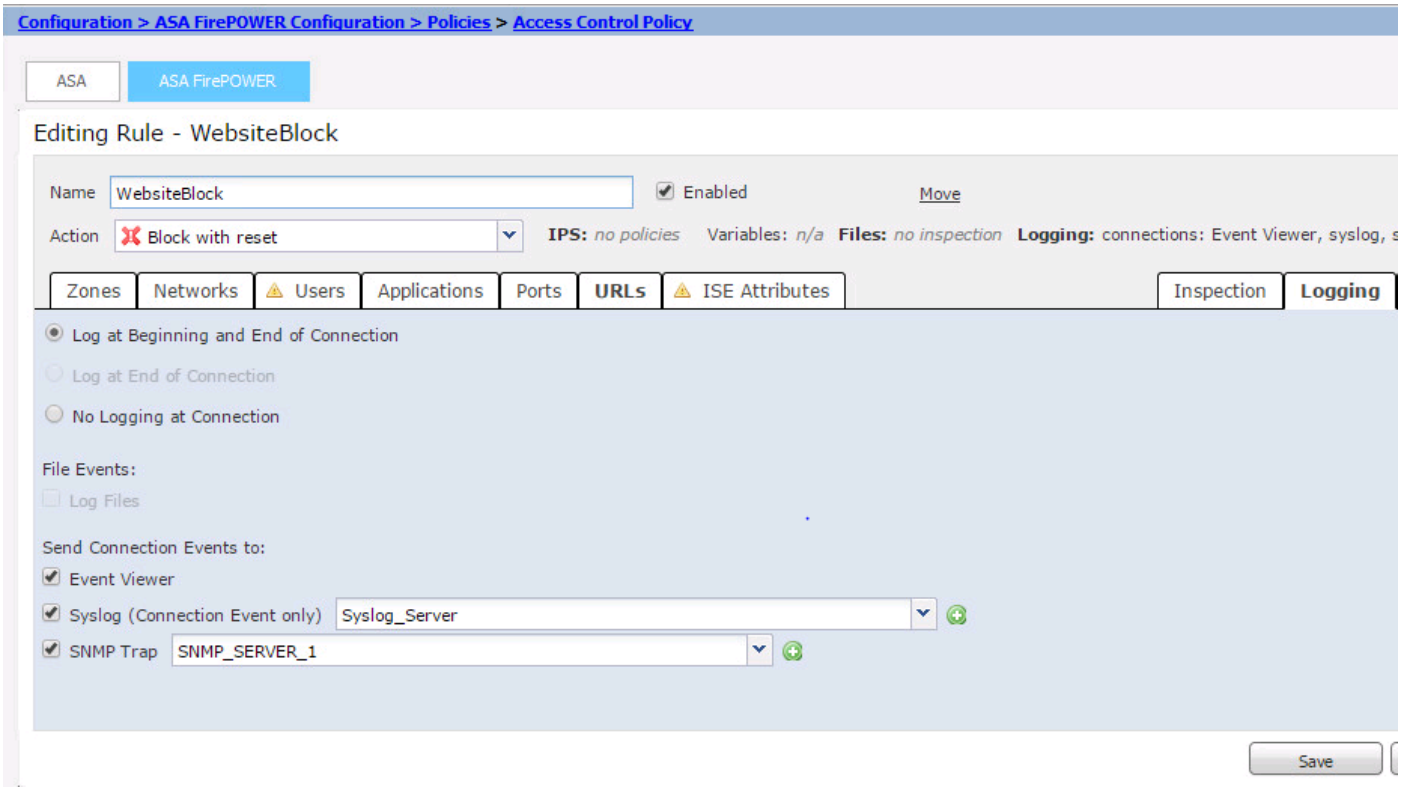
Aktivieren der externen Protokollierung für Verbindungsereignisse

Verbindungsereignisse werden generiert, wenn Datenverkehr auf eine Zugriffsregel trifft, bei der die Protokollierung aktiviert ist. Um die externe Protokollierung für Verbindungsereignisse zu aktivieren, navigieren Sie zu **(ASDM Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy),** bearbeiten Sie die **Zugriffsregel** und navigieren Sie zur **Protokollierungsoption**.

Wählen Sie die Protokollierungsoption entweder **bei "Beginning and End of Connection" (Beginn und Ende der Verbindung) aus** oder **melden Sie sich bei "End of Connection" (Ende der Verbindung)**. Navigieren Sie zu Option **Verbindungsereignisse an senden**, und geben Sie an, wo Ereignisse gesendet werden sollen.

Um Ereignisse an einen externen Syslog-Server zu senden, wählen Sie **Syslog aus**, und wählen Sie dann eine Syslog-Warnmeldung aus der Dropdown-Liste aus. Optional können Sie eine Syslog-Warnmeldung hinzufügen, indem Sie auf das **Symbol** Hinzufügen klicken.

Um Verbindungsereignisse an einen SNMP-Trap-Server zu senden, wählen Sie **SNMP Trap** und dann eine SNMP-Warnmeldung aus der Dropdown-Liste aus. Optional können Sie eine SNMP-Warnmeldung hinzufügen, indem Sie auf das **Symbol** Hinzufügen klicken.



Externe Protokollierung für Angriffsversuche aktivieren

Angriffsereignisse werden generiert, wenn eine Signatur (Snort-Regeln) mit schädlichem Datenverkehr übereinstimmt. Um die externe Protokollierung von Angriffsversuchen zu aktivieren, navigieren Sie zu **ASDM Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy (ASDM-Konfiguration > ASA FirePOWER-Konfiguration > Richtlinien für Sicherheitsrisiken > Intrusion Policy (Angriffsrichtlinie).** Erstellen Sie entweder eine neue Intrusion Policy, oder bearbeiten Sie vorhandene Intrusion Policy.Navigieren Sie zu **Erweiterte Einstellungen > Externe Antworten.**

Um Intrusion Events an einen externen SNMP-Server zu senden, wählen Sie in **SNMP Alerting** die Option **Enabled (Aktiviert)** aus, und klicken Sie dann auf die Option **Edit (Bearbeiten)**.

Trap-Typ: Der Trap-Typ wird für IP-Adressen verwendet, die in den Warnungen angezeigt werden. Wenn Ihr Netzwerkmanagementsystem den Adresstyp INET_IPV4 korrekt wiedergibt, können Sie als Binär auswählen. Wählen Sie andernfalls String aus.

SNMP-Version: Wählen Sie **Version 2** oder **Version 3** ein.

SNMP v2-Option

Trap-Server: Geben Sie die IP-Adresse/den Hostnamen des SNMP-Trap-Servers an, wie in diesem Bild gezeigt.

Community-String: Geben Sie den Community-Namen an.

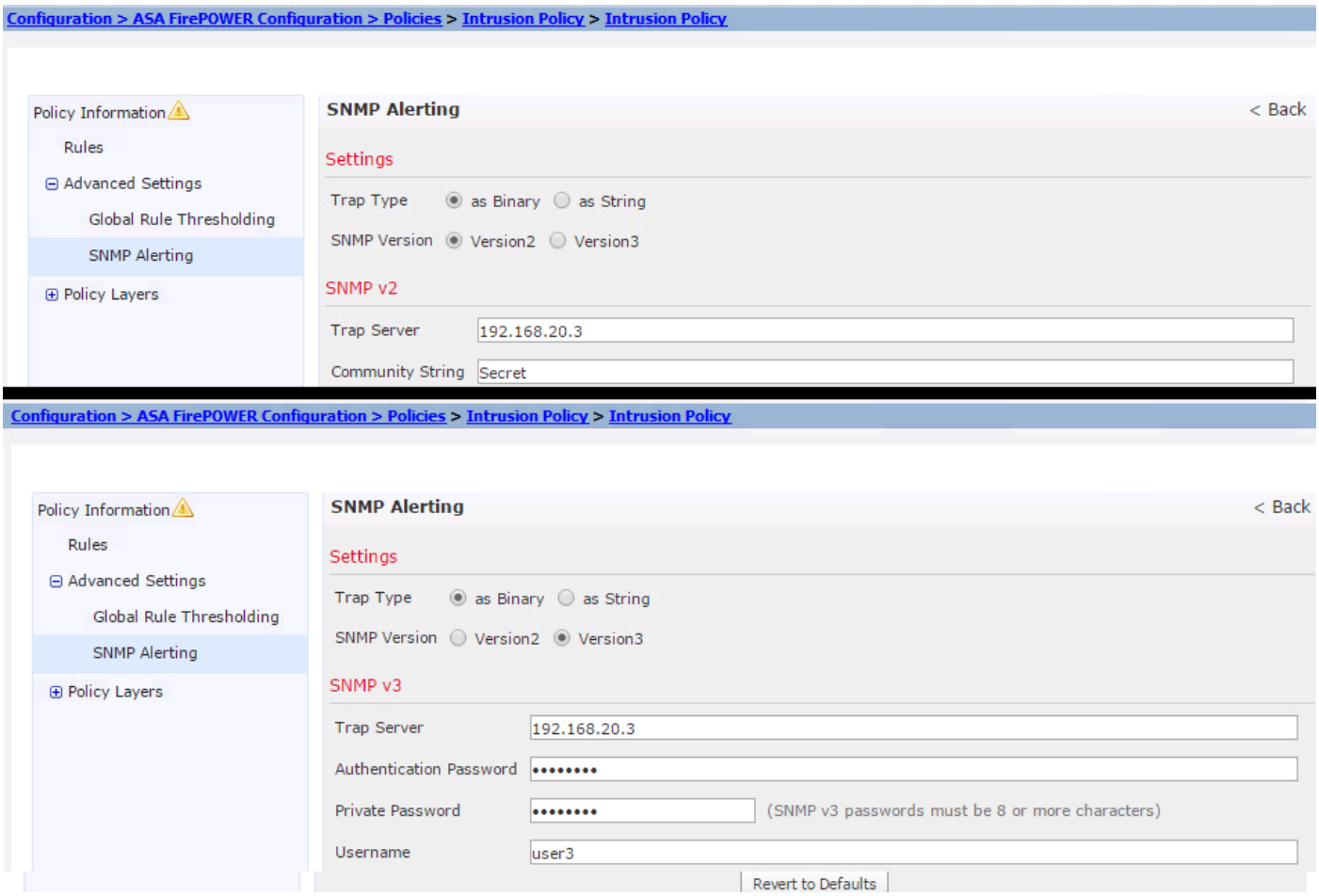
SNMP v3-Option

Trap-Server: Geben Sie die IP-Adresse/den Hostnamen des SNMP-Trap-Servers an, wie in diesem Bild gezeigt.

Authentifizierungskennwort: FestlegenKennwort für die Authentifizierung erforderlich. SNMP v3 verwendet die Hash-Funktion zur Authentifizierung des Kennworts.

Privates Kennwort: Geben Sie das Kennwort für die Verschlüsselung an. SNMP v3 verwendet zur Verschlüsselung dieses Kennworts den DES-Blockcode (Data Encryption Standard).

Benutzername: Geben Sie den Benutzernamen an.



Wählen Sie Option aus, um Intrusion Events an einen externen Syslog-Server zu senden. **Aktiviert** in **Syslog Warnung** und anschließend auf **Bearbeiten** wie in diesem Bild gezeigt.

Protokollierungshost: Geben Sie die IP-Adresse/den Hostnamen des Syslog-Servers an.

Einrichtung: Einrichtung auswählen die auf Ihrem Syslog-Server konfiguriert wurde.

Schweregrad: Wählen Sie einen beliebigen Schweregrad aus, der auf Ihrem Syslog-Server konfiguriert ist.

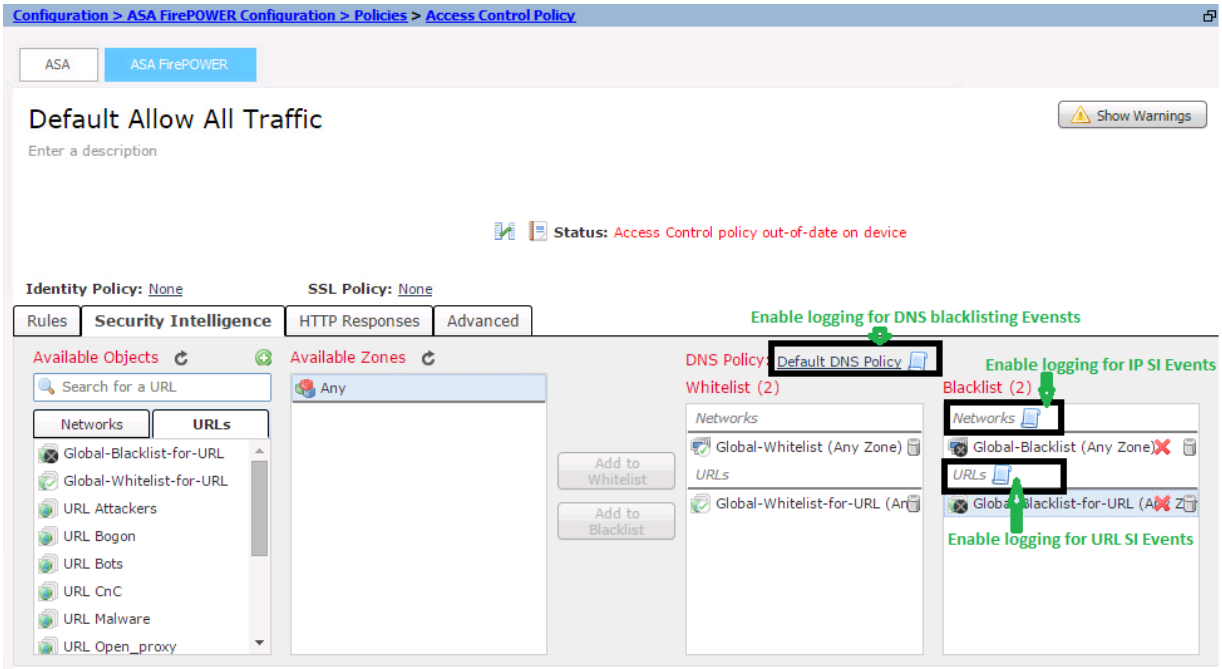
Externe Protokollierung für IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence aktivieren

IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence-Ereignisse werden generiert, wenn der Datenverkehr einer IP-Adresse/Domänenname/URL Security Intelligence-Datenbank entspricht. Um die externe Protokollierung für IP-/URL-/DNS-Sicherheitsereignisse zu aktivieren, navigieren Sie zu **(ASDM-Konfiguration > ASA FirePOWER Configuration > Policies > Access Control Policy > Security Intelligence)**,

Klicken Sie auf das **Symbol**, wie im Bild gezeigt, um die Protokollierung für IP/DNS/URL-Sicherheitsintelligenz zu aktivieren. Durch Klicken auf das Symbol wird ein Dialogfeld angezeigt, in dem die Protokollierung und die Option zum Senden der Ereignisse an den externen Server aktiviert werden.

Um Ereignisse an einen externen Syslog-Server zu senden, wählen Sie **Syslog aus**, und wählen Sie dann eine Syslog-Warnmeldung aus der Dropdown-Liste aus. Optional können Sie eine Syslog-Warnmeldung hinzufügen, indem Sie auf das Symbol Add (Hinzufügen) klicken.

Um Verbindungsereignisse an einen SNMP-Trap-Server zu senden, wählen Sie **SNMP Trap aus**, und wählen Sie dann eine SNMP-Warnmeldung aus der Dropdown-Liste aus. Optional können Sie eine SNMP-Warnmeldung hinzufügen, indem Sie auf das Symbol Add (Hinzufügen) klicken.



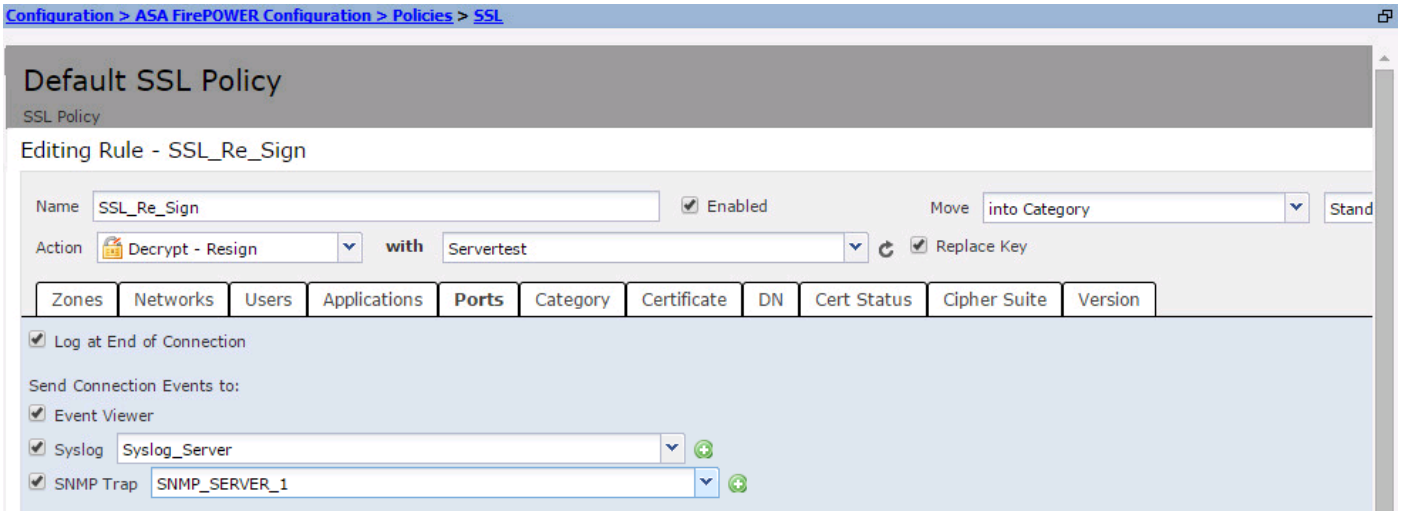
Externe Protokollierung für SSL-Ereignisse aktivieren

SSL-Ereignisse werden generiert, wenn der Datenverkehr mit einer beliebigen Regel in einer SSL-Richtlinie übereinstimmt, in der die Protokollierung aktiviert ist. Um die externe Protokollierung für SSL-Datenverkehr zu aktivieren, navigieren Sie zu **ASDM Configuration > ASA FirePOWER Configuration > Policies > SSL.** Bearbeiten Sie die vorhandene Regel oder erstellen Sie eine neue Regel, und navigieren Sie zur **Protokollierungsoption**.Wählen Sie die Option **Protokoll bei Verbindungsende** aus.

Navigieren Sie anschließend zu **Verbindungsereignisse senden,** und geben Sie an, an welche Stelle die Ereignisse gesendet werden sollen.

Um Ereignisse an einen externen Syslog-Server zu senden, wählen Sie **Syslog aus**, und wählen Sie dann eine Syslog-Warnmeldung aus der Dropdown-Liste aus. Optional können Sie eine Syslog-Warnmeldung hinzufügen, indem Sie auf das Symbol Add (Hinzufügen) klicken.

Um Verbindungsereignisse an einen SNMP-Trap-Server zu senden, wählen Sie **SNMP Trap** und dann eine SNMP-Warnmeldung aus der Dropdown-Liste aus. Optional können Sie eine SNMP-Warnmeldung hinzufügen, indem Sie auf das Symbol Add (Hinzufügen) klicken.



Konfiguration zum Senden von Systemereignissen

Externe Protokollierung für Systemereignisse aktivieren

Systemereignisse zeigen den Status des FirePOWER-Betriebssystems an. Mit dem SNMP-Manager können diese Systemereignisse abgefragt werden.

Um den SNMP-Server zu konfigurieren, um Systemereignisse vom FirePOWER-Modul abzurufen, müssen Sie eine Systemrichtlinie konfigurieren, die die Informationen in der Firewall-MIB (Management Information Base) bereitstellt, die vom SNMP-Server abgefragt werden kann.

Navigieren Sie zu **ASDM Configuration > ASA FirePOWER Configuration > Local > System Policy** und klicken Sie auf **SNMP**.

SNMP-Version: Das FirePOWER-Modul unterstützt SNMP v1/v2/v3. Geben Sie die SNMP-Version an.

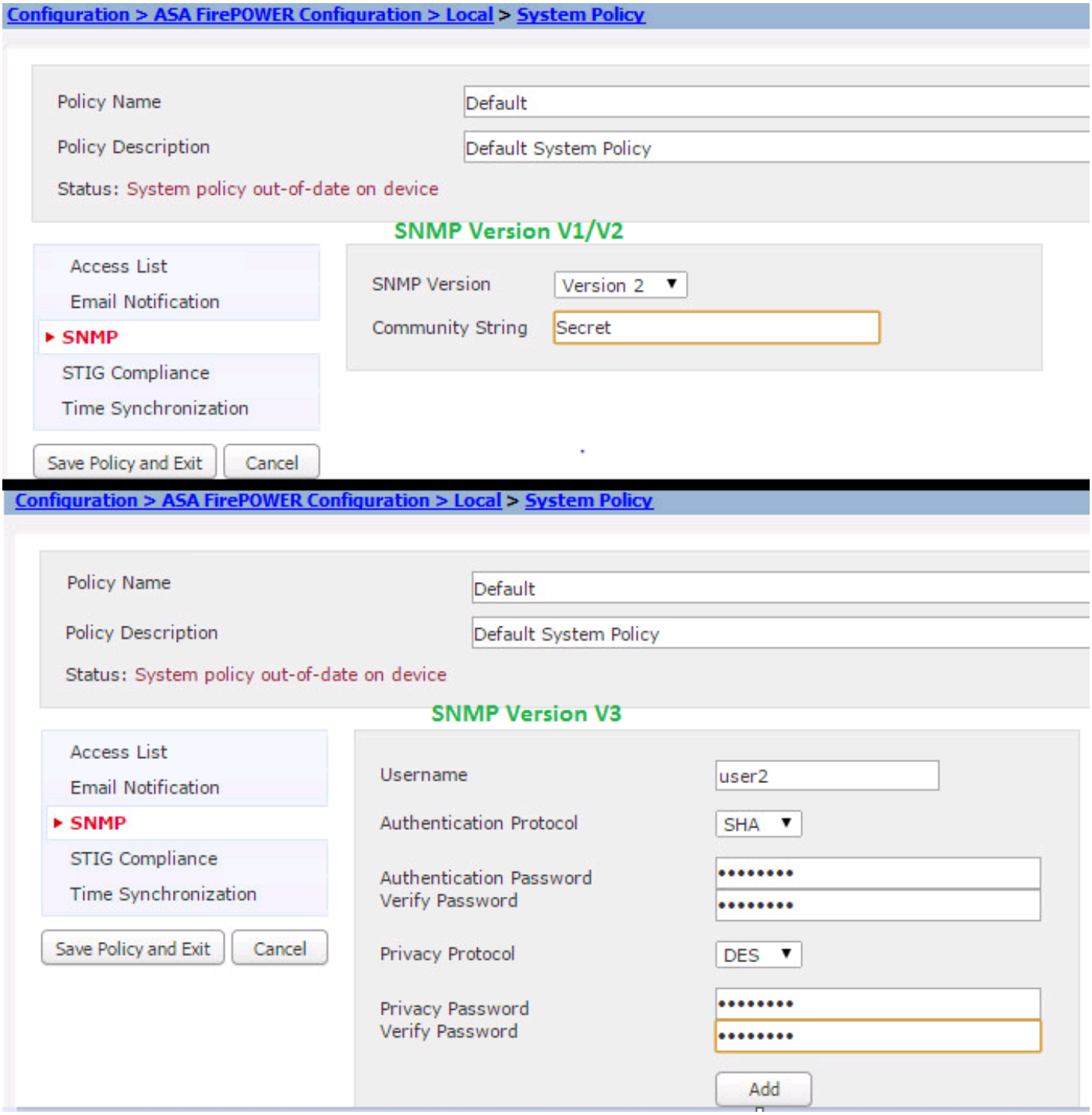
Community-String: Wenn Sie in der Option SNMP-Version **v1/v2** auswählen, geben Sie den SNMP-Community-Namen in das Feld Community String ein.

Benutzername: Wenn Sie die Option **v3** in Version auswählen. Klicken Sie auf die Schaltfläche **Benutzer hinzufügen**, und geben Sie den **Benutzernamen** im Feld Benutzername an.

Authentifizierung: Diese Option ist Teil der SNMP v3-Konfiguration. Sie stellt eine Authentifizierung auf der Grundlage des Hashed Message Authentication Code mit MD5- oder SHA-Algorithmen bereit. **Protokoll** für Hash-Algorithmus auswählen und Kennwort eingeben

im Feld **Kennwort**. Wenn Sie die Authentifizierungsfunktion nicht verwenden möchten, wählen Sie die Option **Keine**.

Datenschutz: Diese Option ist Teil der SNMP v3-Konfiguration. Er stellt Verschlüsselung mithilfe des DES/AES-Algorithmus bereit. Wählen Sie das Protokoll für die Verschlüsselung aus, und geben Sie das Kennwort in das Feld **Kennwort ein**. Wenn Sie keine Datenverschlüsselungsfunktion wünschen, wählen Sie die Option **Keine**.



Hinweis: Eine Management Information Base (MIB) ist eine Sammlung von Informationen, die hierarchisch organisiert ist. MIB-Datei (DCEALERT.MIB) für das FirePOWER-Modul ist am Verzeichnisspeicherort (/etc/sf/DCEALERT.MIB) verfügbar, der von diesem Verzeichnisspeicherort abgerufen werden kann.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems