Configurazione della registrazione in Firepower Module per eventi di sistema/traffico tramite ASDM (gestione integrata)

Sommario

Introduzione

In questo documento vengono descritti gli eventi relativi al traffico e al sistema del modulo Firepower e diversi metodi per inviare tali eventi a un server di registrazione esterno.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager).
- Conoscenza dell'appliance Firepower.

- Syslog, conoscenza del protocollo SNMP.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA Firepower Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 5.4.1 e successive.
- ASA Firepower module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive.
- ASDM 7.5(1) e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Tipo di eventi

Gli eventi del modulo Firepower possono essere classificati in due categorie:

1. Eventi traffico (eventi connessione/eventi intrusione/eventi di Security Intelligence/eventi SSL/malware/eventi file).
2. Eventi di sistema (eventi del sistema operativo Firepower).

Configurazione

Configurazione di una destinazione di output

Passaggio 1. Configurazione del server Syslog

Per configurare un server Syslog per gli eventi del traffico, selezionare **Configurazione > Configurazione di ASA Firepower > Criteri > Avvisi azioni** e fare clic sul menu a discesa **Crea avviso** e scegliere l'opzione **Crea avviso syslog.** Immettere i valori per il server Syslog.

Nome: Specificare il nome che identifica in modo univoco il server Syslog.

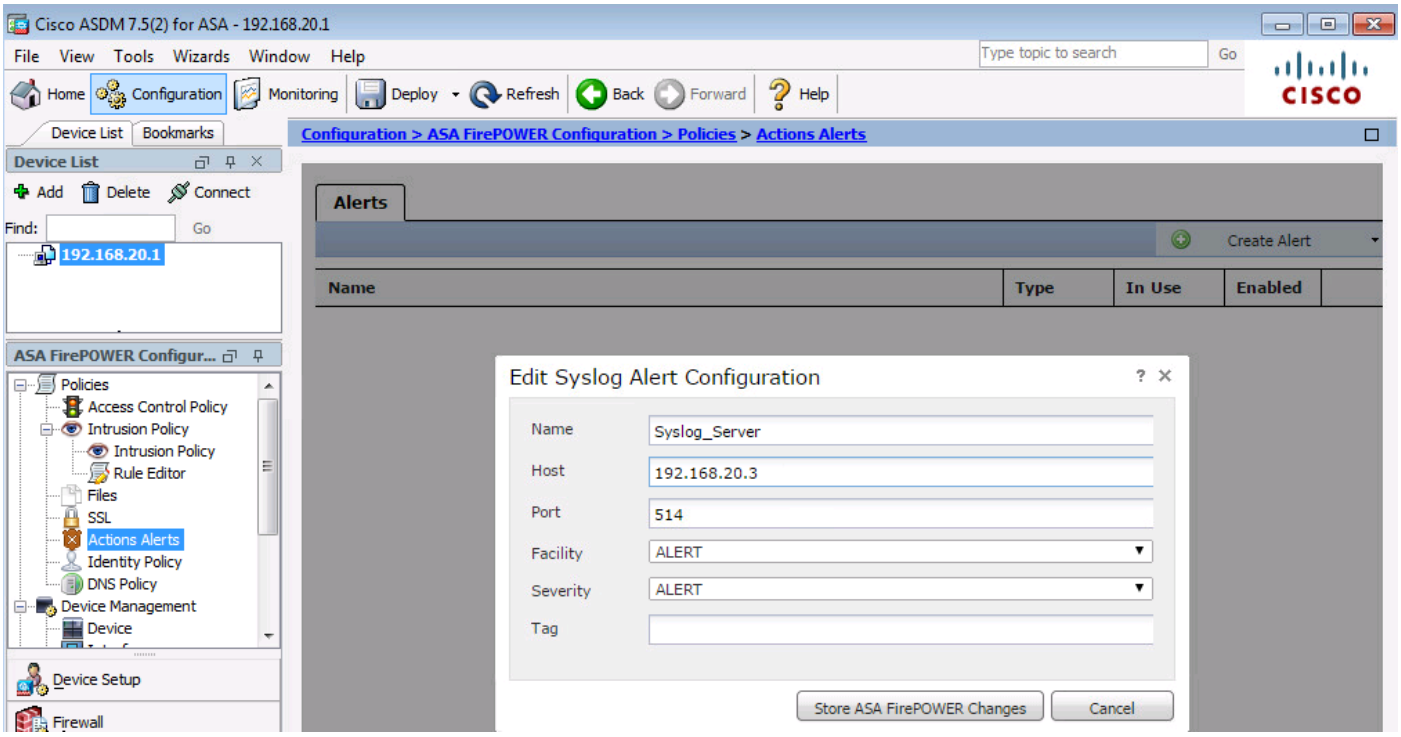
Host: specificare l'indirizzo IP o il nome host del server Syslog.

Port: Specificare il numero di porta del server Syslog.

Struttura: Selezionare una struttura configurata sul server Syslog.

Gravità: Selezionare qualsiasi gravità configurata sul server Syslog.

Contrassegno: Specificare il nome del tag da visualizzare con il messaggio Syslog.



Passaggio 2.Configurazione server SNMP

Per configurare un server Trap SNMP per gli eventi di traffico, selezionare **Configurazione ASDM > Configurazione ASA Firepower > Criteri > Azioni** e fare clic sul menu a discesa **Crea avviso** e scegliere l'opzione **Crea avviso SNMP.**

Nome: Specificare il nome che identifica in modo univoco il server Trap SNMP.

Server trap: Specificare l'indirizzo IP o il nome host del server trap SNMP.

Version: Firepower Module supporta SNMP v1/v2/v3. Selezionare la versione SNMP dal menu a discesa.

Stringa della community: Se si seleziona v1 o v2 in **Versione**, specificare il nome della community SNMP.

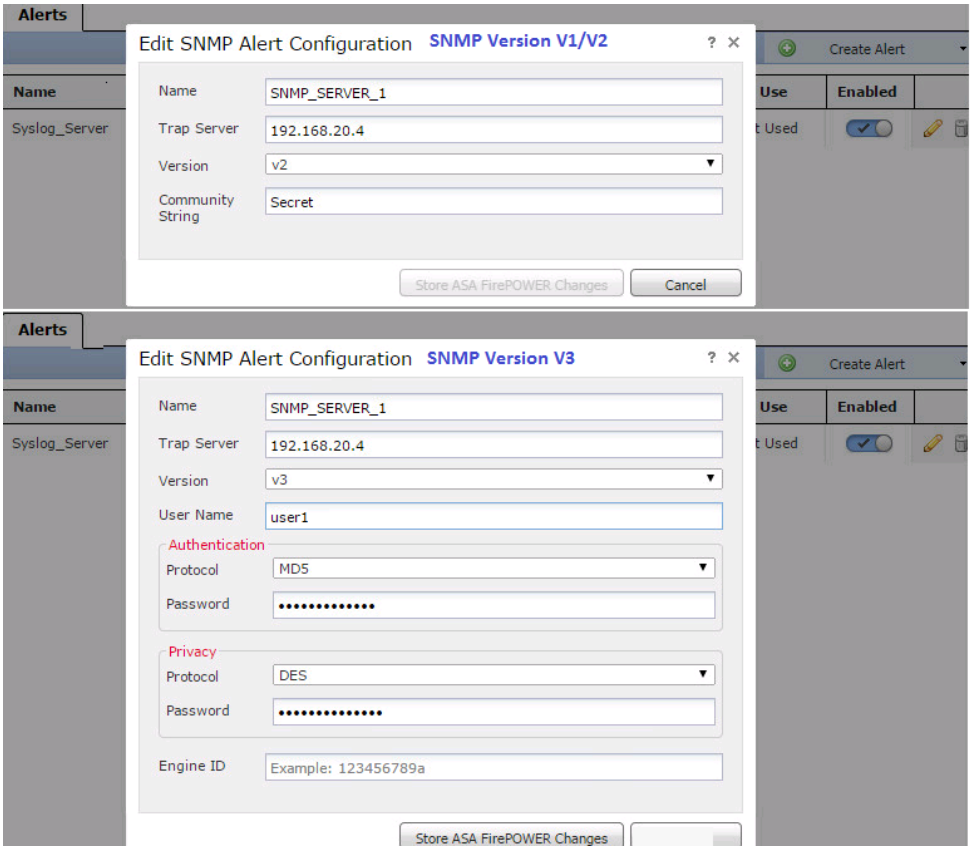
Username: Se si seleziona v3 nell'opzione **Versione**, il sistema visualizza il campo **Nome utente**. Specificare il nome utente.

Autenticazione: Questa opzione fa parte della configurazione di SNMP v3. Fornisce l'autenticazione basata sull'hash

utilizzando l'algoritmo MD5 o SHA. Nel menu a discesa **Protocollo** selezionare l'algoritmo hash & immettere

password nell'opzione **Password**. Se non si desidera utilizzare questa funzione, selezionare l'opzione **Nessuno**.

Privacy: Questa opzione fa parte della configurazione di SNMP v3. Fornisce la crittografia utilizzando l'algoritmo DES. Nel menu a discesa **Protocol** selezionare l'opzione **DES**& enter password in **Password** field. Se non si desidera utilizzare la funzione di crittografia dei dati, scegliere l'opzione **Nessuno**.



Configurazione per l'invio degli eventi traffico

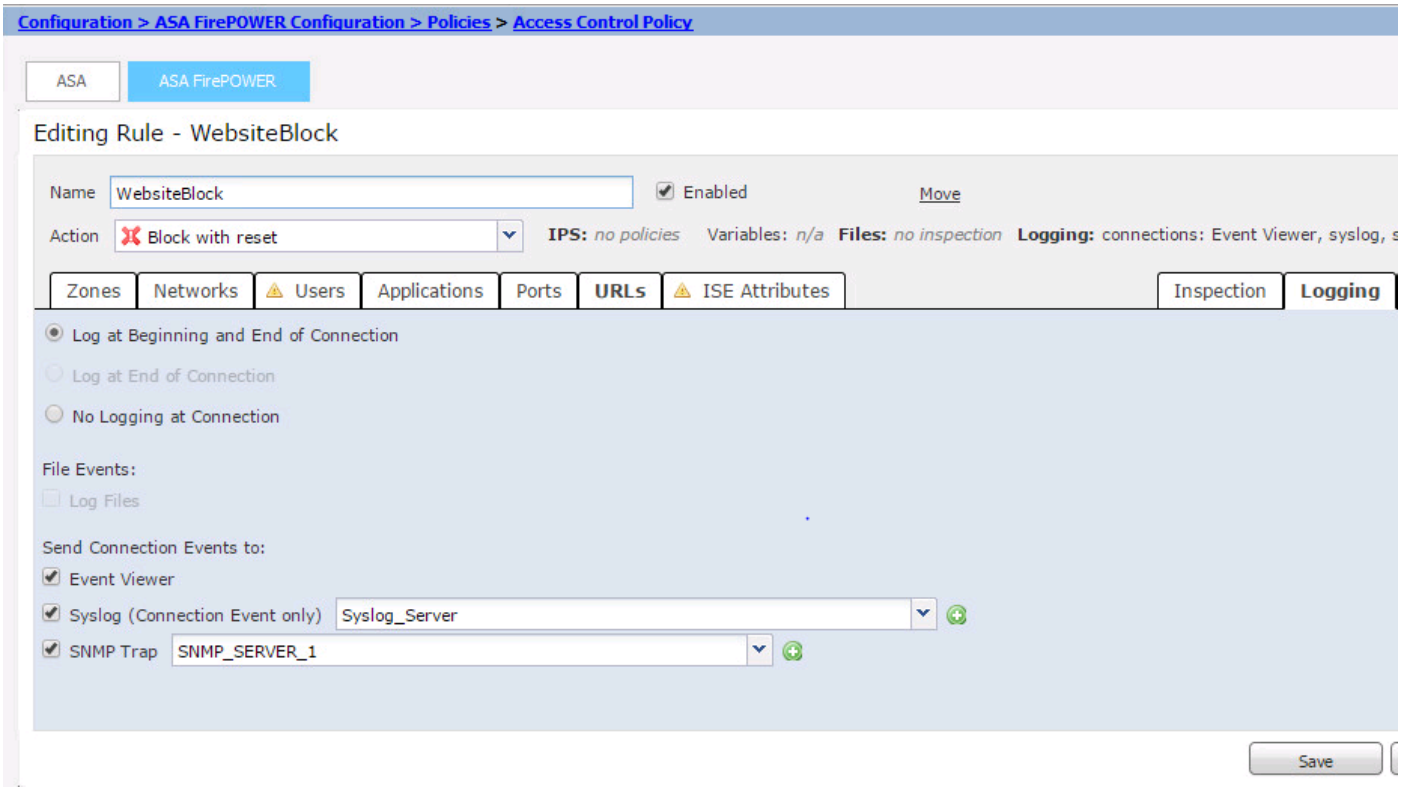
Attiva registrazione esterna per eventi di connessione

Gli eventi di connessione vengono generati quando il traffico raggiunge una regola di accesso con la registrazione attivata. Per abilitare la registrazione esterna per gli eventi di connessione, selezionare **(Configurazione ASDM > Configurazione ASA Firepower > Criteri > Criteri di controllo di accesso) per** modificare la **regola di accesso** e passare all'opzione di **registrazione**.

Selezionare l'opzione di registrazione **Registra all'inizio e alla fine della connessione** o **Registra alla fine della connessione**. Passare all'opzione **Invia eventi connessione a** e specificare la posizione in cui inviare gli eventi.

Per inviare eventi a un server Syslog esterno, selezionare **Syslog**, quindi selezionare una risposta all'avviso Syslog dall'elenco a discesa. Facoltativamente, è possibile aggiungere una risposta all'avviso Syslog facendo clic sull'**icona di** aggiunta.

Per inviare eventi di connessione a un server trap SNMP, selezionare **Trap SNMP**, quindi selezionare una risposta all'avviso SNMP dall'elenco a discesa. Facoltativamente, è possibile aggiungere una risposta all'avviso SNMP facendo clic sull'**icona di** aggiunta.



Abilita registrazione esterna per eventi di intrusione

Gli eventi di intrusione vengono generati quando una firma (regole di snort) corrisponde a del traffico dannoso. Per abilitare la registrazione esterna degli eventi di intrusione, selezionare **Configurazione ASDM > Configurazione ASA Firepower > Criteri > Criteri intrusione > Criteri intrusione.** Creare un nuovo criterio di intrusione o modificare il criterio esistente.Passare a **Impostazioni avanzate > Risposte esterne.**

Per inviare eventi di intrusione a un server SNMP esterno, selezionare l'opzione **Enabled** (Attivato) in **SNMP Alerting** (Avvisi SNMP) e fare clic sull'opzione **Edit** (Modifica).

Tipo di trap: Il tipo di trap viene utilizzato per gli indirizzi IP visualizzati negli avvisi. Se il sistema di gestione della rete esegue correttamente il rendering del tipo di indirizzo INET_IPV4, è possibile selezionare Binario. In caso contrario, selezionare come stringa.

Versione SNMP: Selezionare una delle opzioni **Versione 2** o **Versione 3** pulsante di opzione.

SNMP v2, opzione

Server trap: Specificare l'indirizzo IP o il nome host del server Trap SNMP, come mostrato nell'immagine.

Stringa della community: Specificare il nome della community.

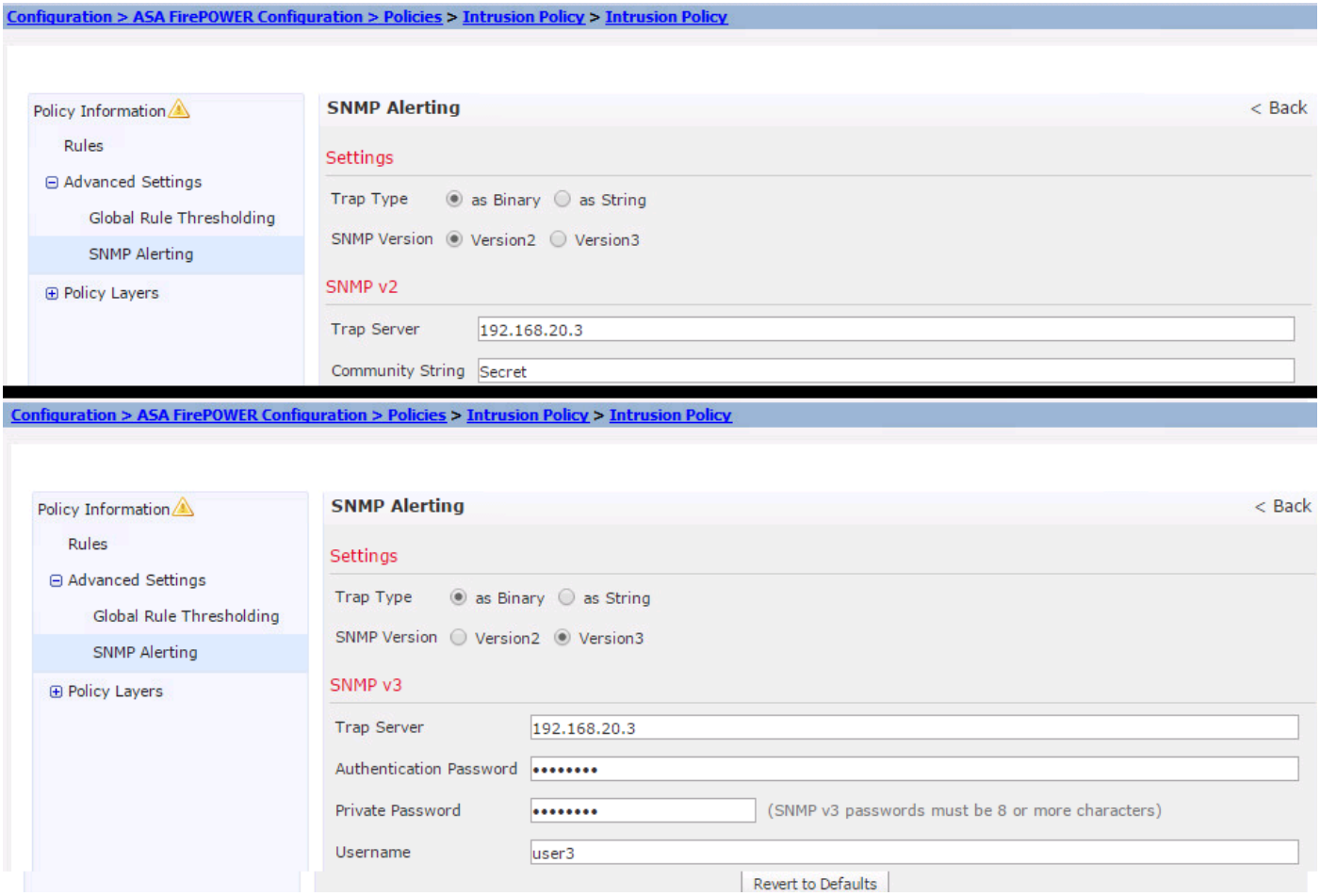
Opzione SNMP v3

Server trap: Specificare l'indirizzo IP o il nome host del server Trap SNMP, come mostrato nell'immagine.

Password di autenticazione: Specificarepassword necessaria per l'autenticazione. SNMP v3 utilizza la funzione hash per autenticare la password.

Password privata: specificare la password per la crittografia. Per crittografare la password, SNMP v3 utilizza la cifratura a blocchi DES (Data Encryption Standard).

Nome utente: Specificare il nome utente.



Per inviare eventi di intrusione a un server Syslog esterno, selezionare l'opzione **Attivato** in **Syslog Avvisi** quindi fare clic sul pulsante **Modifica** come mostrato nell'immagine.

Host di registrazione: Specificare l'indirizzo IP o il nome host del server Syslog.

Struttura: Seleziona una struttura configurata sul server Syslog.

Gravità: Selezionare qualsiasi gravità configurata sul server Syslog.

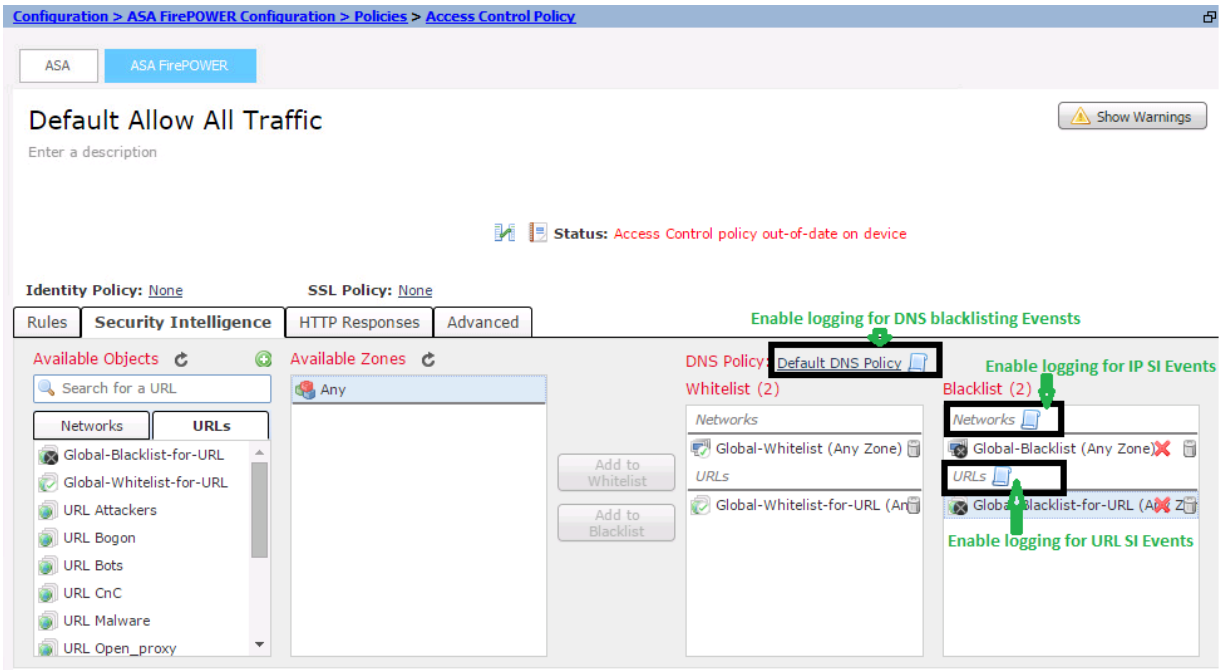
Abilita registrazione esterna per Intelligence sicurezza IP/Intelligence sicurezza DNS/Intelligence sicurezza URL

Gli eventi di **IP Security Intelligence/DNS Security Intelligence/URL Security Intelligence** vengono generati quando il traffico corrisponde a qualsiasi indirizzo IP/nome di dominio/database URL Security Intelligence. Per abilitare la registrazione esterna degli eventi di intelligence per la sicurezza IP/URL/DNS, selezionare **(Configurazione ASDM > Configurazione ASA Firepower > Criteri > Criteri di controllo di accesso > Security Intelligence)**,

Fare clic sull'**icona** come mostrato nell'immagine per abilitare la registrazione per la funzionalità di intelligence IP/DNS/URL. Se si fa clic sull'icona, viene visualizzata una finestra di dialogo che consente di attivare la registrazione e l'opzione per l'invio degli eventi al server esterno.

Per inviare eventi a un server Syslog esterno, selezionare **Syslog**, quindi selezionare una risposta all'avviso Syslog dall'elenco a discesa. Facoltativamente, è possibile aggiungere una risposta all'avviso Syslog facendo clic sull'icona di aggiunta.

Per inviare eventi di connessione a un server trap SNMP, selezionare **Trap SNMP**, quindi selezionare una risposta all'avviso SNMP dall'elenco a discesa. Facoltativamente, è possibile aggiungere una risposta all'avviso SNMP facendo clic sull'icona di aggiunta.



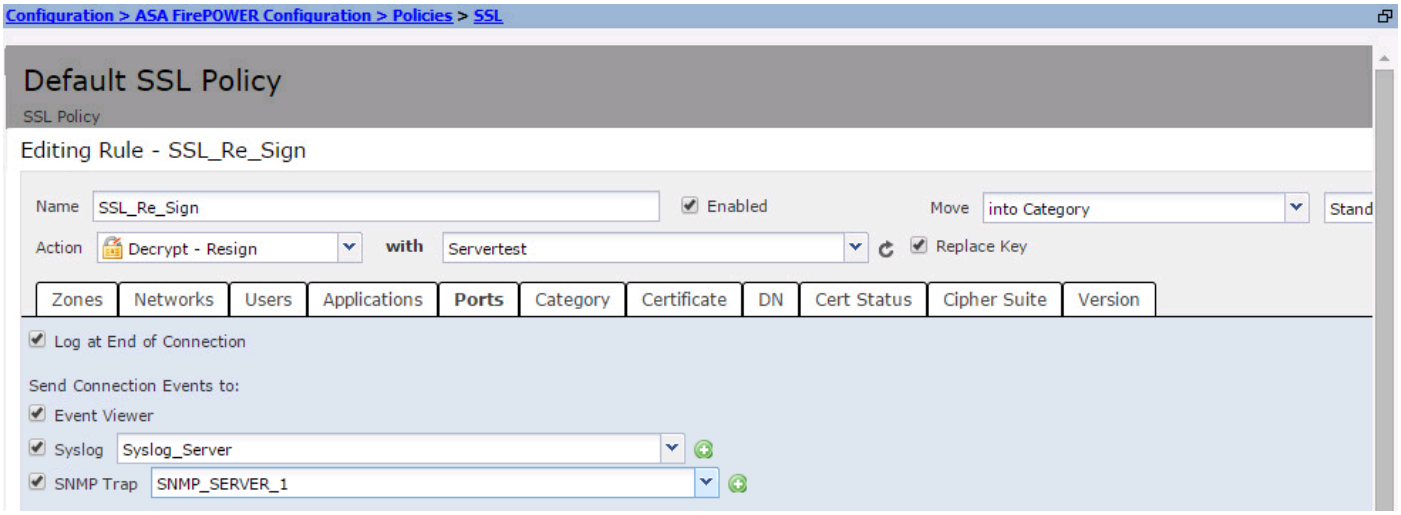
Abilita registrazione esterna per eventi SSL

Gli **eventi SSL** vengono generati quando il traffico corrisponde a una qualsiasi regola del criterio SSL in cui è attivata la registrazione. Per abilitare la registrazione esterna per il traffico SSL, selezionare **Configurazione ASDM > Configurazione ASA Firepower > Criteri > SSL.** Modificare la regola esistente o crearne una nuova e selezionare l'opzione di **registrazione**.Selezionare l'opzione **Registra alla fine della connessione**.

Passare quindi a **Invia eventi connessione a** e specificare la destinazione degli eventi.

Per inviare eventi a un server Syslog esterno, selezionare **Syslog**, quindi selezionare una risposta all'avviso Syslog dall'elenco a discesa. Facoltativamente, è possibile aggiungere una risposta all'avviso Syslog facendo clic sull'icona di aggiunta.

Per inviare eventi di connessione a un server trap SNMP, selezionare **Trap SNMP**, quindi selezionare una risposta all'avviso SNMP dall'elenco a discesa. Facoltativamente, è possibile aggiungere una risposta all'avviso SNMP facendo clic sull'icona di aggiunta.



Configurazione per l'invio degli eventi di sistema

Abilita registrazione esterna per eventi di sistema

Gli eventi di sistema mostrano lo stato del sistema operativo Firepower. È possibile utilizzare SNMP Manager per eseguire il polling di questi eventi di sistema.

Per configurare il server SNMP in modo da eseguire il polling degli eventi di sistema dal modulo Firepower, è necessario configurare un criterio di sistema che renda le informazioni disponibili nel MIB (Management Information Base) di firepower che può essere sottoposto a polling dal server SNMP.

Selezionare **ASDM Configuration > ASA Firepower Configuration > Local > System Policy** e fare clic su **SNMP**.

Versione SNMP: Firepower Module supporta SNMP v1/v2/v3. Specificare la versione SNMP.

Stringa della community: Se si seleziona l'opzione **v1/ v2** in versione SNMP, digitare il nome della community SNMP nel campo Stringa della community.

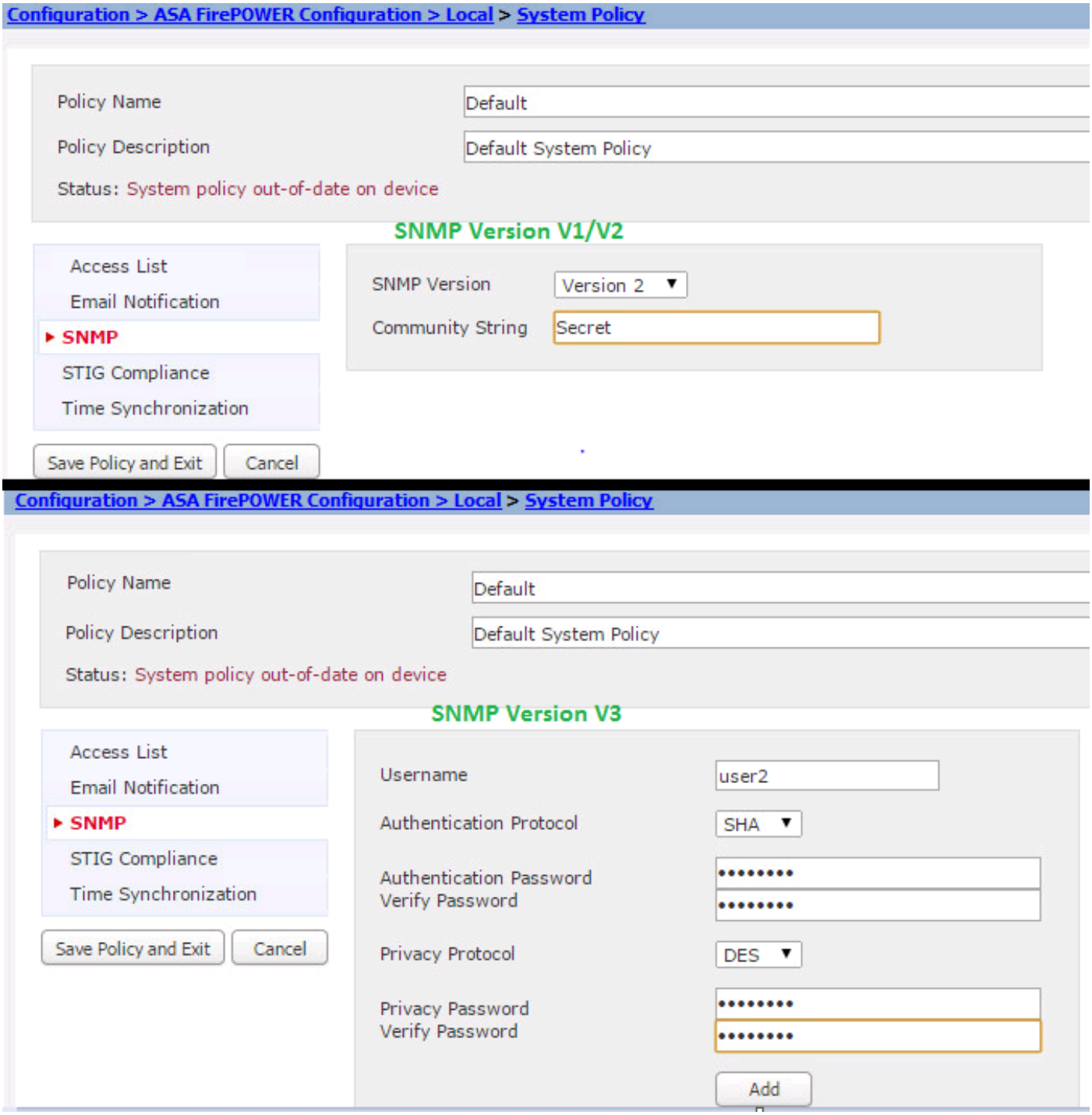
Username: Se si seleziona l'opzione v3 in versione, Fare clic sul pulsante **Add User** (Aggiungi utente) e specificare il **nome utente** nel campo username (Nome utente).

Autenticazione: Questa opzione fa parte della configurazione di SNMP v3. Fornisce l'autenticazione basata sul codice di autenticazione del messaggio con hash utilizzando gli algoritmi MD5 o SHA. Scegli **protocollo** per algoritmo hash e immetti password

nel campo **Password**. Se non si desidera utilizzare la funzione di autenticazione, selezionare

l'opzione **Nessuno**.

Privacy: Questa opzione fa parte della configurazione di SNMP v3. Fornisce la crittografia utilizzando l'algoritmo DES/AES. Selezionare il protocollo per la crittografia e immettere la password nel campo **Password**. Se non si desidera la funzione di crittografia dei dati, scegliere **Nessuna** opzione.



Nota: MIB (Management Information Base) è una raccolta di informazioni organizzata in modo gerarchico. Il file MIB (DECEALERT.MIB) per Firepower Module è disponibile nella directory (/etc/sf/DCEALERT.MIB) che può essere recuperata da questa directory.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems