Configurar o registro no módulo Firepower para eventos de tráfego/sistema usando ASDM (On-Box Management, gerenciamento integrado)

Contents

Introduction

Este documento descreve os eventos de tráfego/sistema do módulo Firepower e vários métodos de envio desses eventos para um servidor de registro externo.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager).
- Firepower appliance Knowledge.

- Syslog, conhecimento do protocolo SNMP.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Módulos ASA Firepower (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) executando a versão de software 5.4.1 e superior.
- Módulo ASA Firepower (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) executando a versão de software 6.0.0 e superior.
- ASDM 7.5(1) e superior.

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.

Informações de Apoio

Tipo de eventos

Os eventos do módulo Firepower podem ser classificados em dois tipos:-

1. Eventos de tráfego (eventos de conexão/eventos de intrusão/eventos de inteligência de segurança/eventos SSL/malware/eventos de arquivo).
2. Eventos do sistema (eventos do sistema operacional (SO) Firepower).

Configurar

Configurando um destino de saída

Etapa 1. Configuração do Servidor Syslog

Para configurar um Servidor Syslog para eventos de tráfego, navegue para **Configuração > Configuração do ASA Firepower > Políticas > Alertas de Ações** e clique no menu suspenso **Criar alerta** e escolha a opção **Criar alerta de syslog.** Insira os valores para o servidor Syslog.

Nome: especifique o nome que identifica exclusivamente o servidor Syslog.

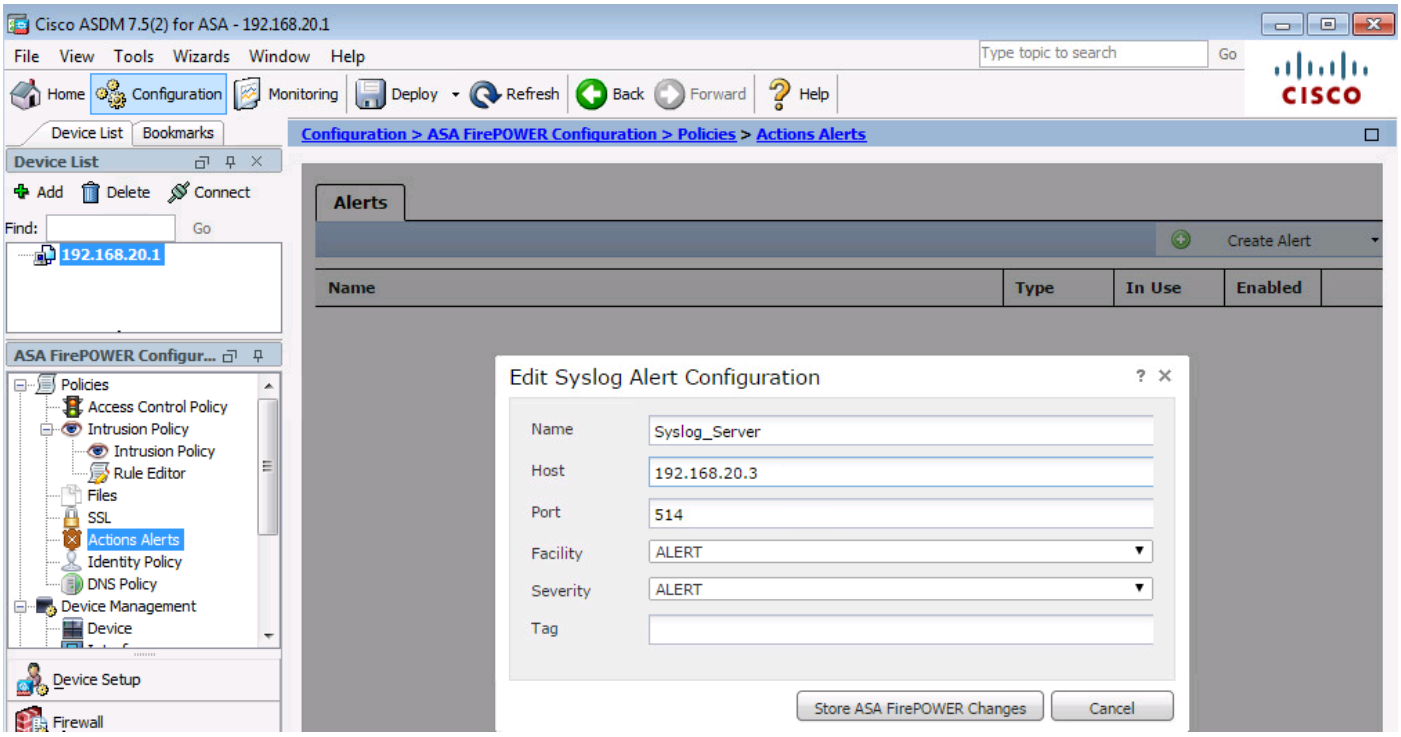
Host: especifique o endereço IP/nome de host do servidor Syslog.

Porta: especifique o número da porta do servidor Syslog.

Instalação: Selecione qualquer recurso configurado no servidor Syslog.

Gravidade: selecione qualquer Gravidade configurada no servidor Syslog.

Tag: Especifique o nome da tag que pretende apresentar com a mensagem Syslog.



Etapa 2.Configuração do servidor SNMP

Para configurar um servidor Trap SNMP para eventos de tráfego, navegue para **Configuração do ASDM > Configuração do ASA Firepower > Políticas > Alertas de ações** e clique no menu suspenso **Criar alerta** e escolha a opção **Criar alerta SNMP.**

Nome: especifique o nome que identifica exclusivamente o servidor Trap SNMP.

Servidor Trap: especifique o endereço IP/nome de host do servidor de trap SNMP.

Versão: O módulo Firepower suporta SNMP v1/v2/v3. Selecione a versão SNMP no menu suspenso.

Sequência de caracteres da comunidade: Se você selecionar v1 ou v2 na opção **Version**, especifique o nome da comunidade SNMP.

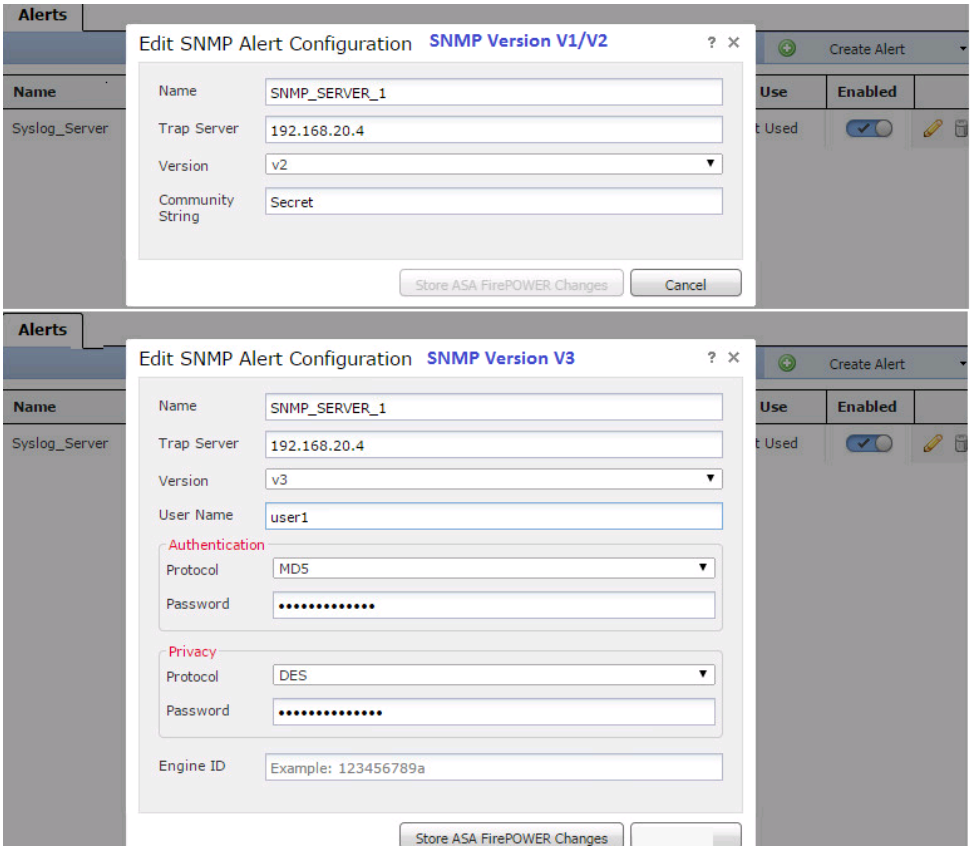
Nome de usuário: Se você selecionar v3 na opção **Versão**, o sistema solicitará o campo **Nome de usuário**. Especifique o nome de usuário.

Autenticação: esta opção faz parte da configuração do SNMP v3. Ele fornece autenticação baseada no Hash

algoritmo usando algoritmos MD5 ou SHA. No menu suspenso **Protocolo**, selecione o algoritmo de hash e digite

senha na opção **Senha**. Se não quiser usar esse recurso, selecione a opção **Nenhum**.

Privacidade: Esta opção faz parte da configuração do SNMP v3. Ele fornece criptografia usando o algoritmo DES. No menu suspenso **Protocolo**, selecione a opção **DES** e insira a senha no campo **Senha**. Se não quiser usar o recurso de criptografia de dados, escolha **Nenhuma** opção.



Configuração para enviar os eventos de tráfego

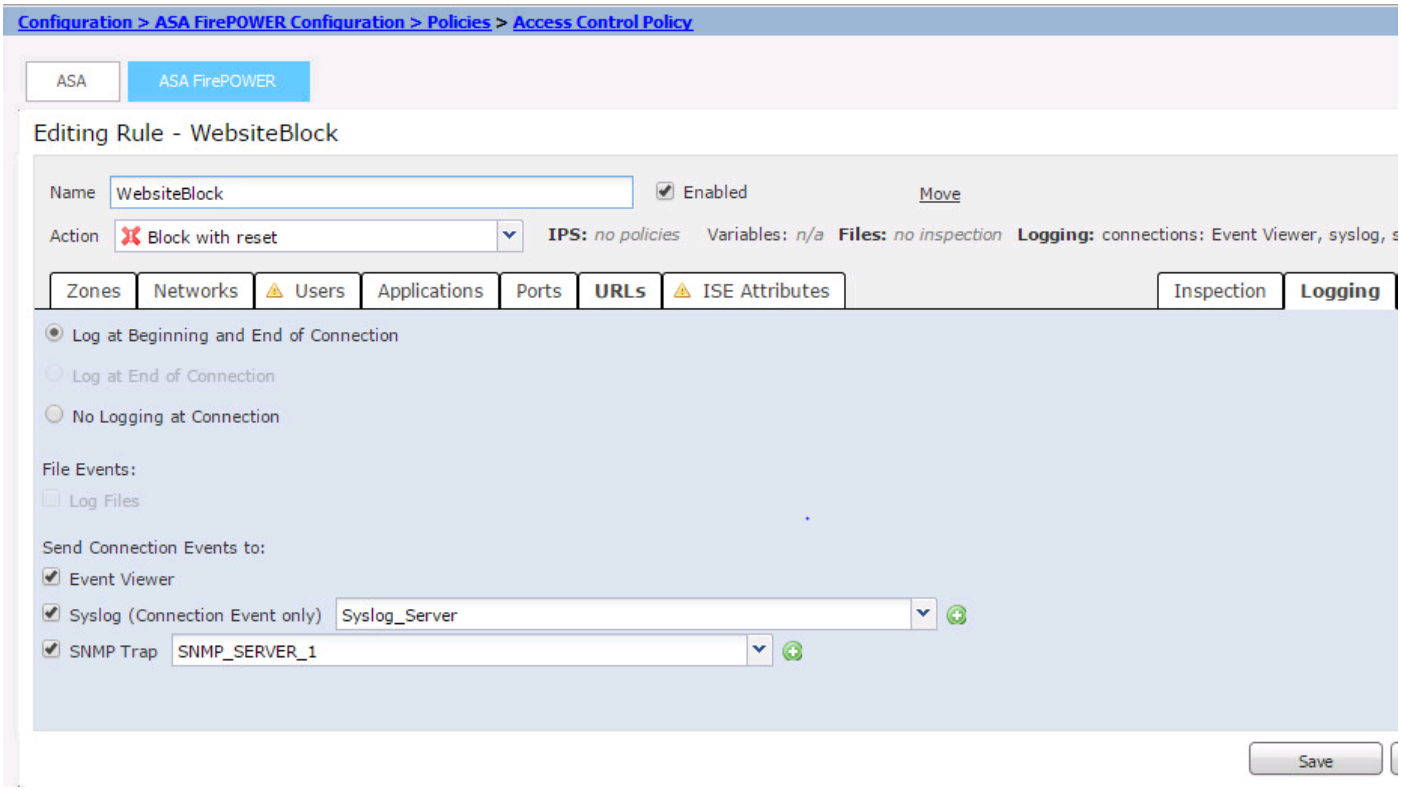
Habilitar registro externo para eventos de conexão

Os eventos de conexão são gerados quando o tráfego atinge uma regra de acesso com o registro ativado. Para habilitar o registro externo para eventos de conexão, navegue para **(Configuração do ASDM > Configuração do ASA Firepower > Políticas > Política de controle de acesso)** edite a **regra de acesso** e navegue para a opção de **registro.**

Selecione a opção de registro **log no início e no fim da conexão** ou **log no fim da conexão**. Navegue até a opção **Enviar eventos de conexão para** e especifique para onde enviar eventos.

Para enviar eventos para um servidor Syslog externo, selecione **Syslog** e selecione uma resposta de alerta Syslog na lista suspensa. Opcionalmente, você pode adicionar uma resposta de alerta de Syslog clicando no **ícone** adicionar.

Para enviar eventos de conexão a um servidor de interceptação SNMP, selecione **Trap SNMP** e selecione uma resposta de alerta SNMP na lista suspensa. Opcionalmente, você pode adicionar uma resposta de alerta SNMP clicando no **ícone** adicionar.



Habilitar registro externo para eventos de intrusão

Os eventos de intrusão são são gerados quando uma assinatura (regras de snort) corresponde a algum tráfego mal-intencionado. Para ativar o registro externo para eventos de intrusão, navegue para **Configuração do ASDM > Configuração do ASA Firepower > Políticas> Política de intrusão > Política de intrusão.** Crie uma nova política de intrusão ou edite a política de intrusão existente.Navegue até **Configuração avançada > Respostas externas.**

Para enviar eventos de intrusão a um servidor SNMP externo, selecione **Enabled** option em **SNMP Alerting** e clique na opção **Edit**.

Tipo de armadilha: O tipo de armadilha é usado para endereços IP que aparecem nos alertas. Se o seu sistema de gerenciamento de rede retornar corretamente o tipo de endereço INET_IPV4, você poderá selecionar como Binário. Caso contrário, selecione String.

Versão SNMP: Selecione **Versão 2** or **Versão 3** botão de opção.

opção SNMP v2

Servidor Trap: Especifique o endereço IP/nome de host do servidor Trap SNMP, como mostrado nesta imagem.

String de comunidade: Especifique o nome da comunidade.

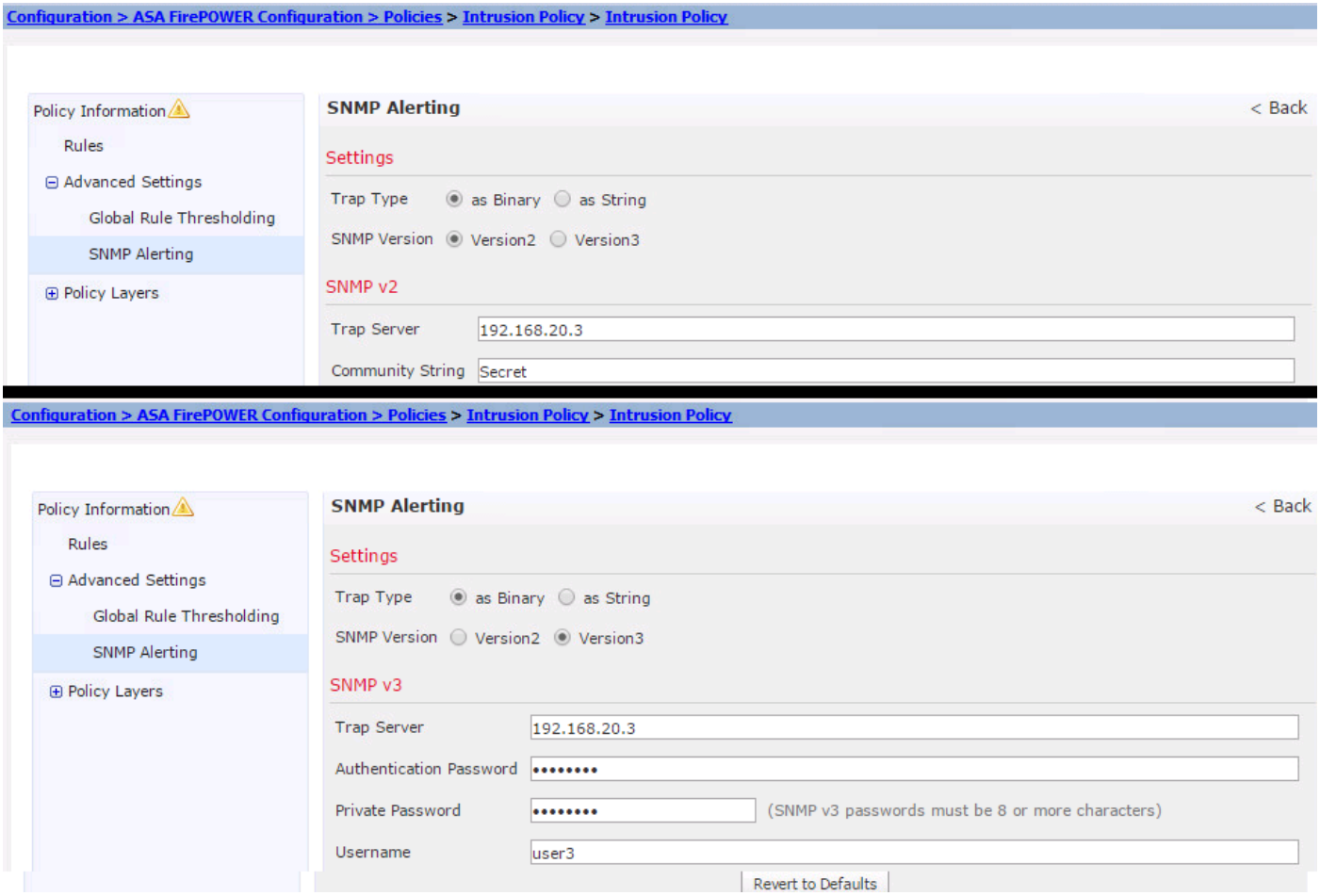
Opção SNMP v3

Servidor Trap: Especifique o endereço IP/nome de host do servidor Trap SNMP, como mostrado nesta imagem.

Senha de autenticação: Especificarsenha necessária para autenticação. O SNMP v3 usa a função hash para autenticar a senha.

Senha Privada: Especificar senha para criptografia. O SNMP v3 usa cifra de bloco Data Encryption Standard (DES) para criptografar essa senha.

User Name: Especifique o nome de usuário.



Para enviar eventos de intrusão a um servidor Syslog externo, selecione a opção **Habilitado** no **Syslog Alerta** em seguida, clique no botão **Editar** , como mostrado nesta imagem.

Host de registro: Especifique o endereço IP/nome de host do servidor Syslog.

Recurso: Selecionar qualquer recurso que está configurado no servidor Syslog.

Severity: Selecione qualquer Gravidade configurada no servidor Syslog.

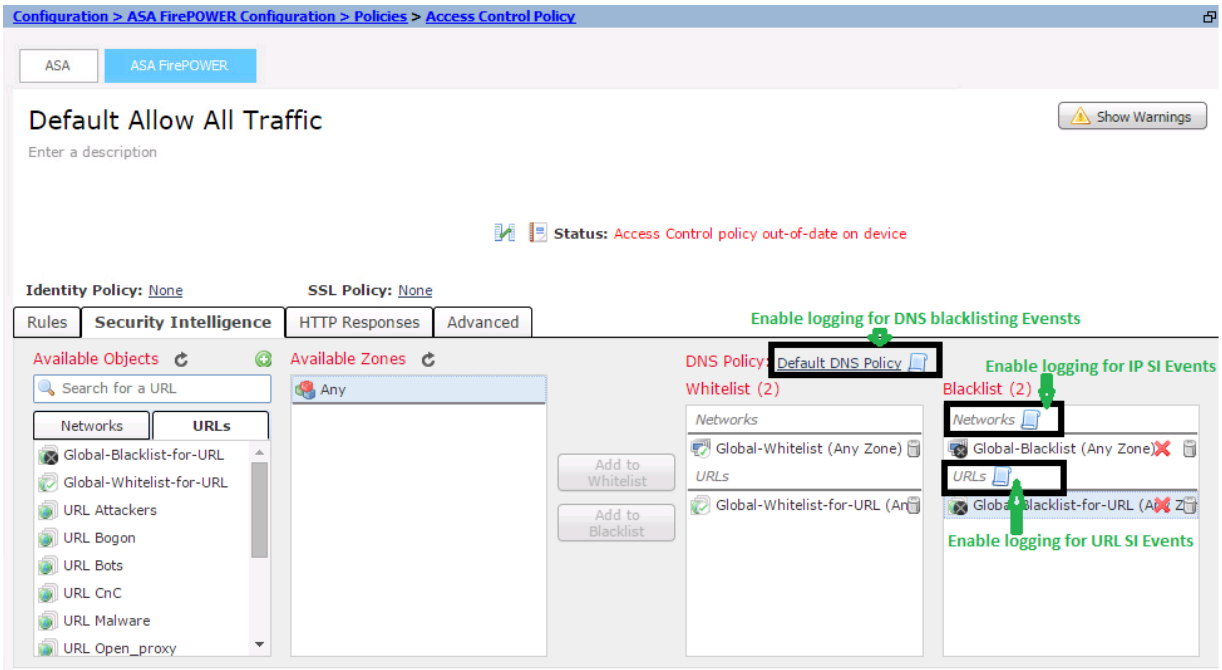
Habilitar registro externo para inteligência de segurança IP/inteligência de segurança DNS/inteligência de segurança de URL

Os eventos **de inteligência de segurança IP/inteligência de segurança DNS/URL** são gerados quando o tráfego corresponde a qualquer banco de dados de inteligência de segurança de endereço IP/nome de domínio/URL. Para ativar o registro externo para Eventos de Inteligência de Segurança IP/ URL/DNS, navegue para **(Configuração do ASDM > Configuração do ASA Firepower > Políticas > Política de Controle de Acesso > Inteligência de Segurança)**,

Clique no **ícone** como mostrado na imagem para ativar o registro para IP/DNS/URL Security Intelligence. Clicar no ícone solicita uma caixa de diálogo para ativar o registro e a opção para enviar os eventos para o servidor externo.

Para enviar eventos para um servidor Syslog externo, selecione **Syslog** e selecione uma resposta de alerta Syslog na lista suspensa. Opcionalmente, você pode adicionar uma resposta de alerta de Syslog clicando no ícone de adição.

Para enviar eventos de conexão a um servidor de interceptação SNMP, selecione **Trap SNMP** e selecione uma resposta de alerta SNMP na lista suspensa. Opcionalmente, você pode adicionar uma resposta de alerta SNMP clicando no ícone adicionar.



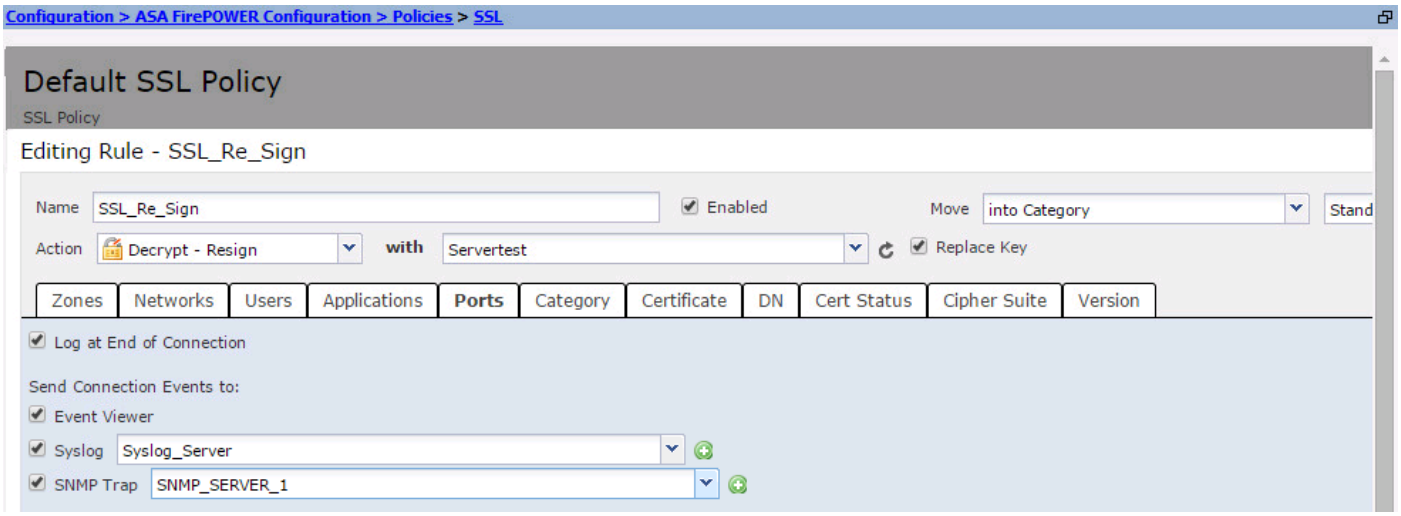
Habilitar registro externo para eventos SSL

Os eventos SSL são gerados quando o tráfego corresponde a qualquer regra na política SSL, na qual o registro está ativado. Para habilitar o registro externo para tráfego SSL, navegue para **Configuração do ASDM > Configuração do ASA Firepower > Políticas > SSL.** Edite a regra existente ou crie uma nova regra e navegue para a opção **registro**.Selecione a opção **registro no fim da ligação**.

Em seguida, navegue para **Enviar eventos de conexão** e especifique para onde enviar os eventos.

Para enviar eventos para um servidor Syslog externo, selecione **Syslog** e selecione uma resposta de alerta Syslog na lista suspensa. Opcionalmente, você pode adicionar uma resposta de alerta de Syslog clicando no ícone de adição.

Para enviar eventos de conexão a um servidor de interceptação SNMP, selecione **Trap SNMP** e selecione uma resposta de alerta SNMP na lista suspensa. Opcionalmente, você pode adicionar uma resposta de alerta SNMP clicando no ícone adicionar.



Configuração para enviar os eventos do sistema

Habilitar registro externo para eventos do sistema

Os eventos do sistema mostram o status do sistema operacional Firepower. O gerenciador SNMP pode ser usado para pesquisar esses eventos de sistemas.

Para configurar o servidor SNMP para pesquisar eventos do sistema a partir do módulo Firepower, você precisa configurar uma política do sistema que disponibilize as informações em firepower MIB (Management Information Base), que pode ser pesquisado pelo servidor SNMP.

Navegue até **Configuração do ASDM > Configuração do ASA Firepower > Local > Política do sistema** e clique no **SNMP**.

Versão SNMP: O módulo Firepower suporta SNMP v1/v2/v3. Especifique a versão SNMP.

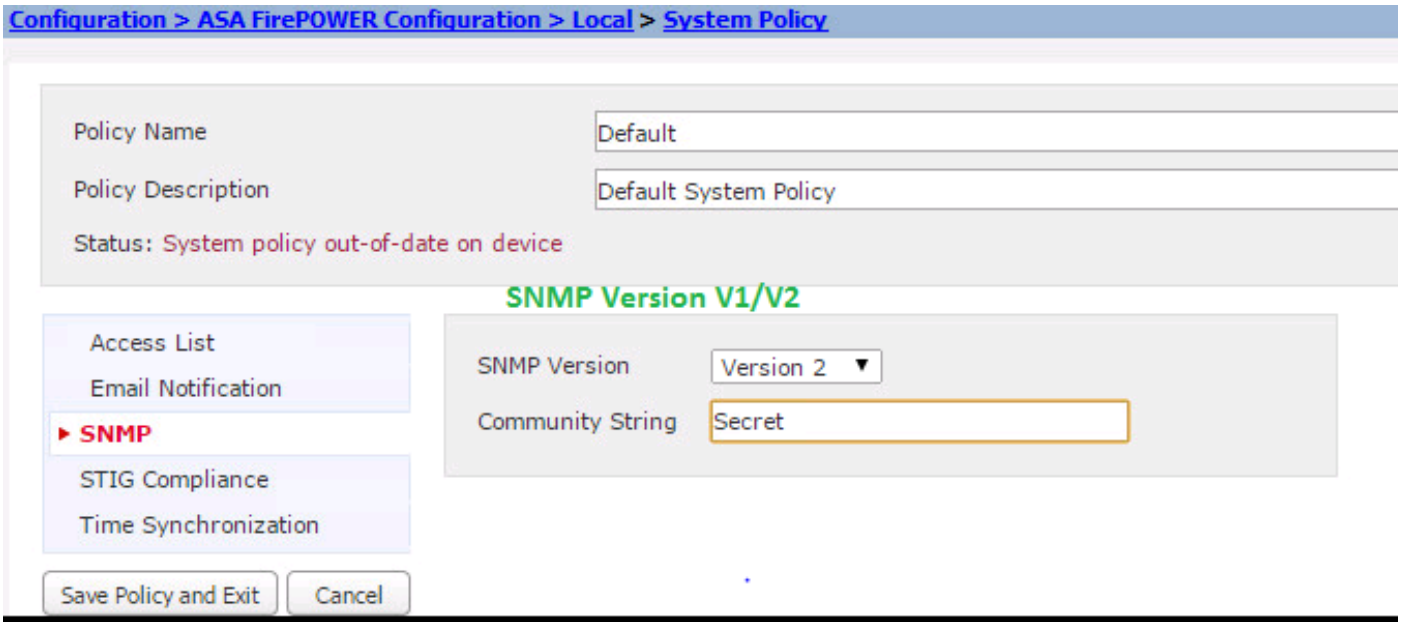
Sequência de caracteres da comunidade: Se você selecionar **v1/ v2** na opção de versão SNMP, digite o nome da comunidade SNMP no campo Community String.

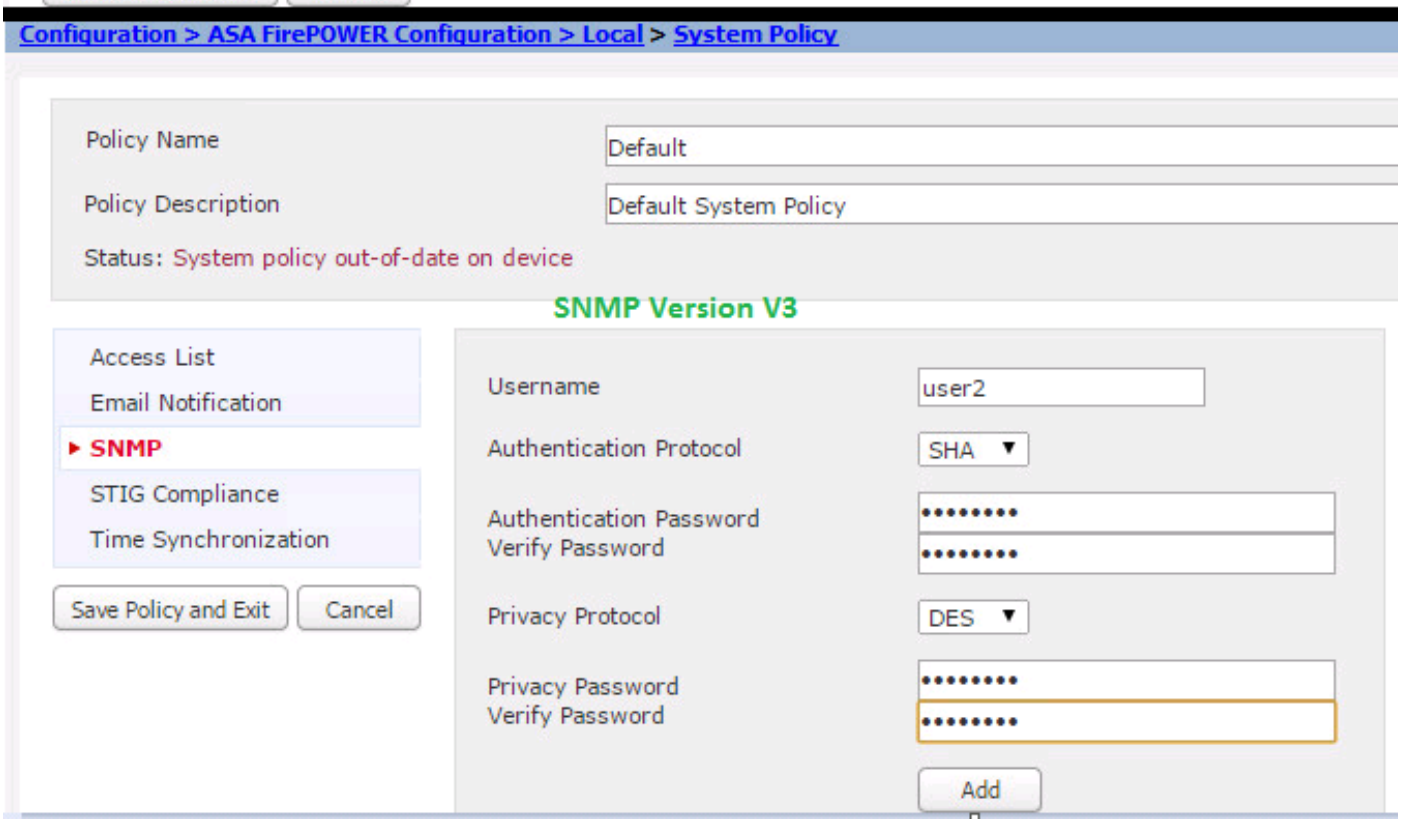
Nome de usuário: Se você selecionar a opção **v3** na versão. Clique no botão **Adicionar usuário** e especifique o **nome de usuário** no campo nome de usuário.

Autenticação: esta opção faz parte da configuração do SNMP v3. Ele fornece autenticação baseada no Hash Message Authentication Code usando algoritmos MD5 ou SHA. Escolha **Protocolo** para algoritmo de hash e digite a senha

no campo **Senha**. Se não quiser usar o recurso de autenticação, selecione a opção **Nenhum**.

Privacidade: Esta opção faz parte da configuração do SNMP v3. Ele fornece criptografia usando o algoritmo DES/AES. Selecione o protocolo para criptografia e insira a senha no campo **Senha**. Se você não quiser o recurso de criptografia de dados, escolha **Nenhuma** opção.





Nota: MIB (management information base, base de informações de gerenciamento) é uma coleção de informações organizada hierarquicamente. O arquivo MIB (DCEALERT.MIB) para o módulo Firepower está disponível no local do diretório (/etc/sf/DCEALERT.MIB) que pode ser buscado nesse local do diretório.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems