Configurar o módulo de abertura de FirePOWER para eventos do tráfego do sistema usando ASDM (o Gerenciamento da Em-caixa)

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Configurando um destino de emissor
Etapa 1. Configuração de servidor de SYSLOG
Configuração do servidor da etapa 2.SNMP
Configuração para enviar os eventos do tráfego
Permita o registro externo para eventos de conexão
Permita o registro externo para eventos da intrusão
Permita o registro externo para a inteligência de Segurança da Segurança Intelligence/URL da Segurança IP Intelligence/DNS
Permita o registro externo para eventos SSL
Configuração para enviar os eventos do sistema
Permita o registro externo para eventos do sistema
Verificar
Troubleshooting
Informações Relacionadas
Cisco relacionado apoia discussões da comunidade

Introdução

Este documento descreve eventos do tráfego do sistema do módulo de FirePOWER e o vário método de enviar estes eventos a um servidor de logging externo.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firewall ASA (ferramenta de segurança adaptável), ASDM (Security Device Manager adaptável).
- Conhecimento do dispositivo de FirePOWER.

- Syslog, conhecimento do protocolo de SNMP.

Componentes Utilizados

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

- Versão de software running 5.4.1 dos módulos ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) e acima.
- Versão de software running 6.0.0 do módulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) e acima.
- ASDM 7.5(1) e acima.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Tipo de eventos

Os eventos do módulo de FirePOWER podem ser categorizados em dois tipos: -

1. Eventos do tráfego (eventos de conexão/eventos da intrusão/eventos inteligência de Segurança Events/SSL/eventos do malware/arquivo).
2. Eventos do sistema (eventos do operating system (OS) de FirePOWER).

Configurar

Configurando um destino de emissor

Etapa 1. Configuração de servidor de SYSLOG

Para configurar um servidor de SYSLOG para eventos do tráfego, para navegar à **configuração > à configuração ASA FirePOWER > às políticas > aos alertas das ações** e para clicar o menu suspenso do **alerta da criação** e para escolher a opção **cria o alerta do Syslog.** Incorpore os valores para o servidor de SYSLOG.

Nome: Especifique o nome que identifica excepcionalmente o servidor de SYSLOG.

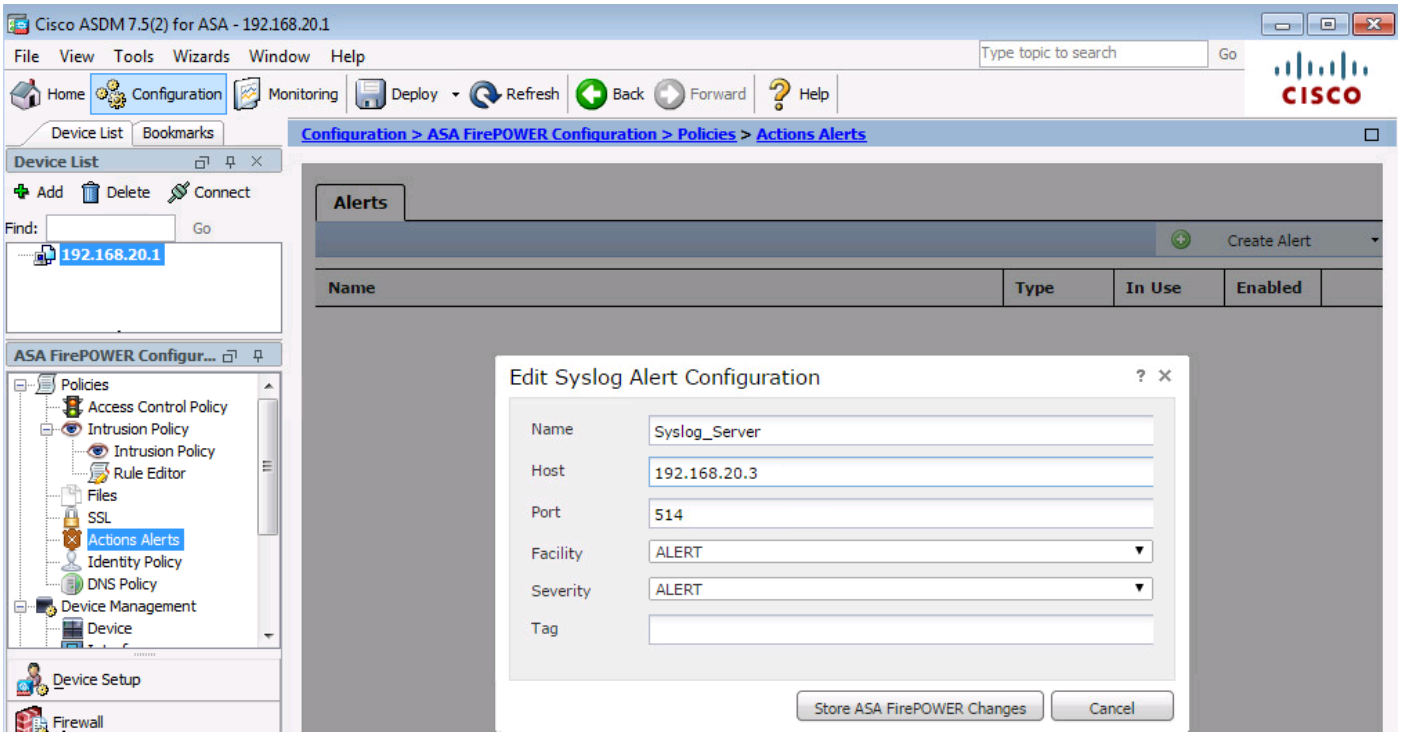
Host: Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT/hostname do servidor de SYSLOG.

Porta: Especifique o número de porta de servidor de SYSLOG.

Facilidade: Selecione toda a facilidade que for configurada em seu servidor de SYSLOG.

Severidade: Selecione toda a severidade que for configurada em seu servidor de SYSLOG.

Etiqueta: Especifique o nome da etiqueta que você quer aparecer com o mensagem do syslog.



Configuração do servidor da etapa 2.SNMP

Para configurar um server da armadilha de SNMP para eventos do tráfego, para navegar à **configuração ASDM > à configuração ASA FirePOWER > às políticas > aos alertas das ações** e para clicar o menu suspenso do **alerta da criação** e para escolher a opção **cria o alerta SNMP.**

Nome: Especifique o nome que identifica excepcionalmente o server da armadilha de SNMP.

Server da armadilha: Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT/hostname do server da armadilha de SNMP.

Versão: Suportes de módulo SNMP v1/v2/v3 de FirePOWER. Selecione a versão de SNMP do menu de gota para baixo.

String de comunidade: Se você seleciona v1 ou v2 na opção da **versão**, especifique o nome de comunidade SNMP.

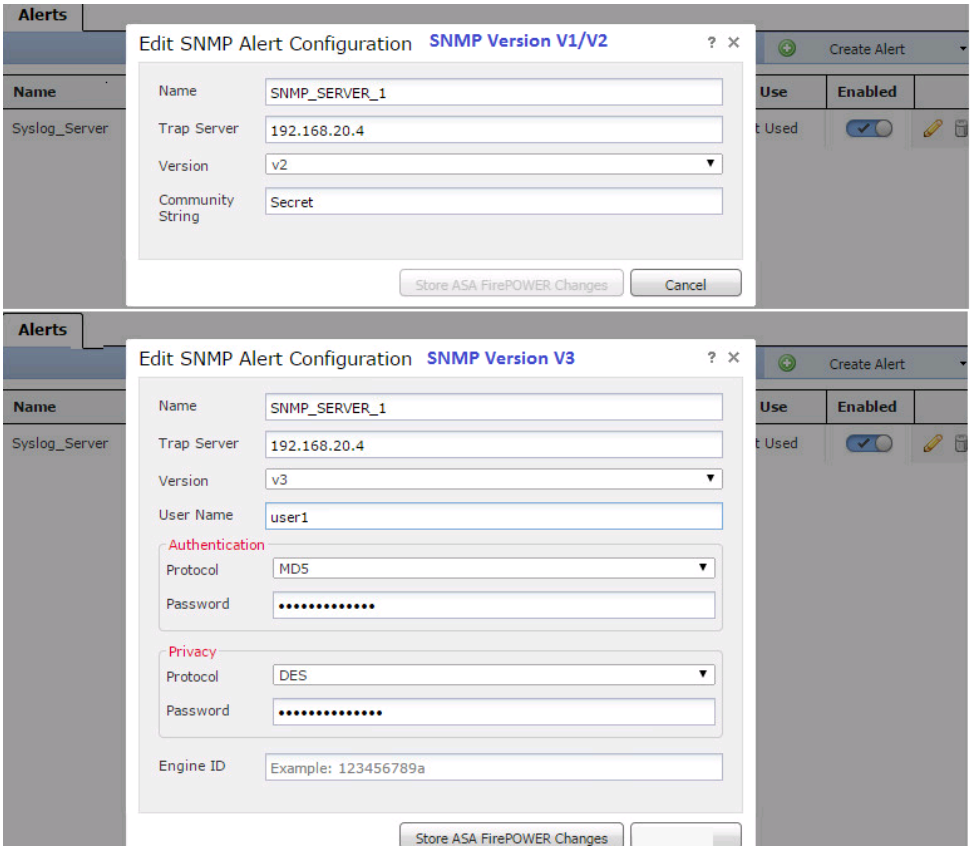
Nome de usuário: Se você seleciona v3 na opção da **versão**, o sistema alerta o campo de **nome de usuário**. Especifique o username.

Autenticação: Esta opção é parte de uma configuração SNMP v3. Fornece a autenticação baseada na mistura

algoritmo usando algoritmos MD5 ou SHA. **No protocolo** deixe cair para baixo o menu selecionam o algoritmo de hash & entram-no

senha na **opção de senha**. Se você não quer usar esta característica, a seguir não selecione **nenhuns** opção.

Privacidade: Esta opção é parte de uma configuração SNMP v3. Fornece a criptografia usando o algoritmo de DES. No menu da gota do **protocolo** selecione a opção como **DES&** incorporam a senha ao campo de **senha**. Se você não quer usar recursos de criptografia de dados, a seguir não escolha **nenhuns** opção.



Configuração para enviar os eventos do tráfego

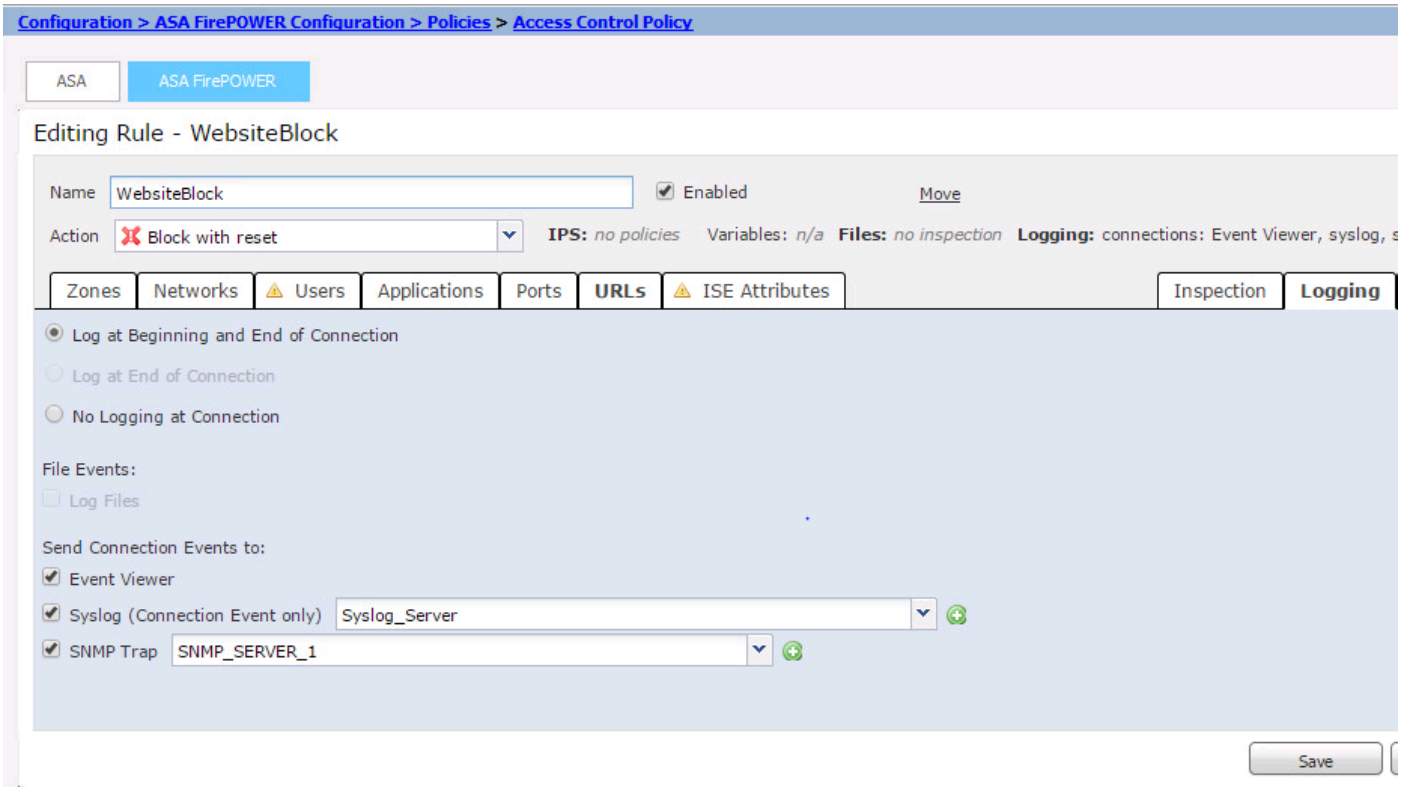
Permita o registro externo para eventos de conexão

Os eventos de conexão são gerados quando o tráfego bate uma regra do acesso com o registro permitido. A fim permitir o registro externo para eventos de conexão, navegue a **(configuração ASDM > configuração ASA FirePOWER > políticas > política do controle de acesso)** editam a **regra do acesso** e navegam à **opção de registro**.

Selecione o **log da** opção de registro no **começo e a extremidade da conexão** ou **registre-os na extremidade da conexão**. Navegue **para enviar eventos de conexão à** opção e para especificar onde enviar eventos.

A fim enviar eventos a um servidor syslog externo, a um **Syslog** seleto, e selecionar então uma resposta do alerta do Syslog da lista de drop-down. Opcionalmente, você pode adicionar uma resposta do alerta do Syslog clicando o **ícone** adicionar.

Para enviar eventos de conexão a um server da armadilha de SNMP, a uma **armadilha de SNMP** seleta, e selecionar então uma resposta do alerta SNMP da lista de drop-down. Opcionalmente, você pode adicionar uma resposta do alerta SNMP clicando o **ícone** adicionar.



Permita o registro externo para eventos da intrusão

Os eventos da intrusão estão gerados quando uma assinatura (regras do snort) combina algum tráfego malicioso. A fim permitir o registro externo para eventos da intrusão, navegue à **política da configuração ASDM > da configuração ASA FirePOWER > da intrusão de Policies> > à política da intrusão.** Crie uma política nova da intrusão ou edite a intrusão existente Policy.Navigate a **ajuste avançado > respostas externos.**

A fim enviar eventos da intrusão a um servidor SNMP externo, a opção **permitida** seleta no **SNMP que alerta** e clicar então a opção da **edição**.

Tipo de armadilha: O tipo de armadilha é usado para os endereços IP de Um ou Mais Servidores Cisco ICM NT que aparecem nos alertas. Se seu sistema de gerenciamento de rede rende corretamente o tipo de endereço INET_IPV4, a seguir você pode selecionar como o binário. Se não, selecione como a corda.

Versão de SNMP: Selecione o botão de rádio da **versão 2** ou da **versão 3**.

Opção SNMP v2

Server da armadilha: Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT/hostname do server da armadilha de SNMP, segundo as indicações desta imagem.

String de comunidade: Especifique o nome da comunidade.

Opção SNMP v3

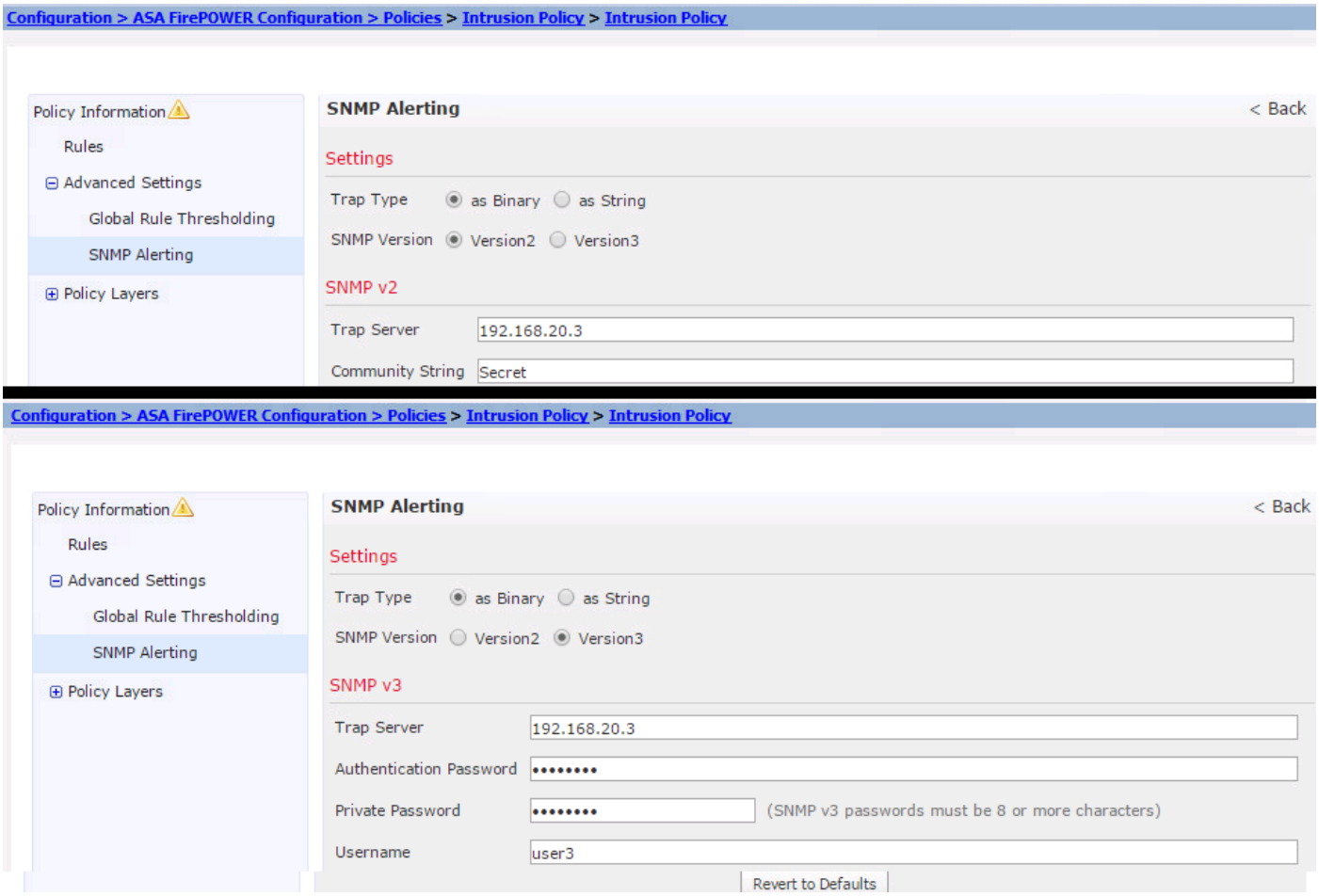
Server da armadilha: Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT/hostname do server da armadilha de SNMP, segundo as indicações desta imagem.

Senha de autenticação: Specifypassword exigiu para a autenticação. O SNMP v3 usa a função de

mistura para autenticar a senha.

Senha privada: Especifique a senha para a criptografia. O SNMP v3 usa a cifra de bloco do Data Encryption Standard (DES) para cifrar esta senha.

Nome de usuário: Especifique o username.



A fim enviar eventos da intrusão a um servidor syslog externo, a opção seleta **permitida no Syslog que alerta** então clica a opção da **edição**, segundo as indicações desta imagem.

Logging host: Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT/hostname do servidor de SYSLOG.

Facilidade: Selecione toda a facilidade que for configurada em seu servidor de SYSLOG.

Severidade: Selecione toda a severidade que for configurada em seu servidor de SYSLOG.

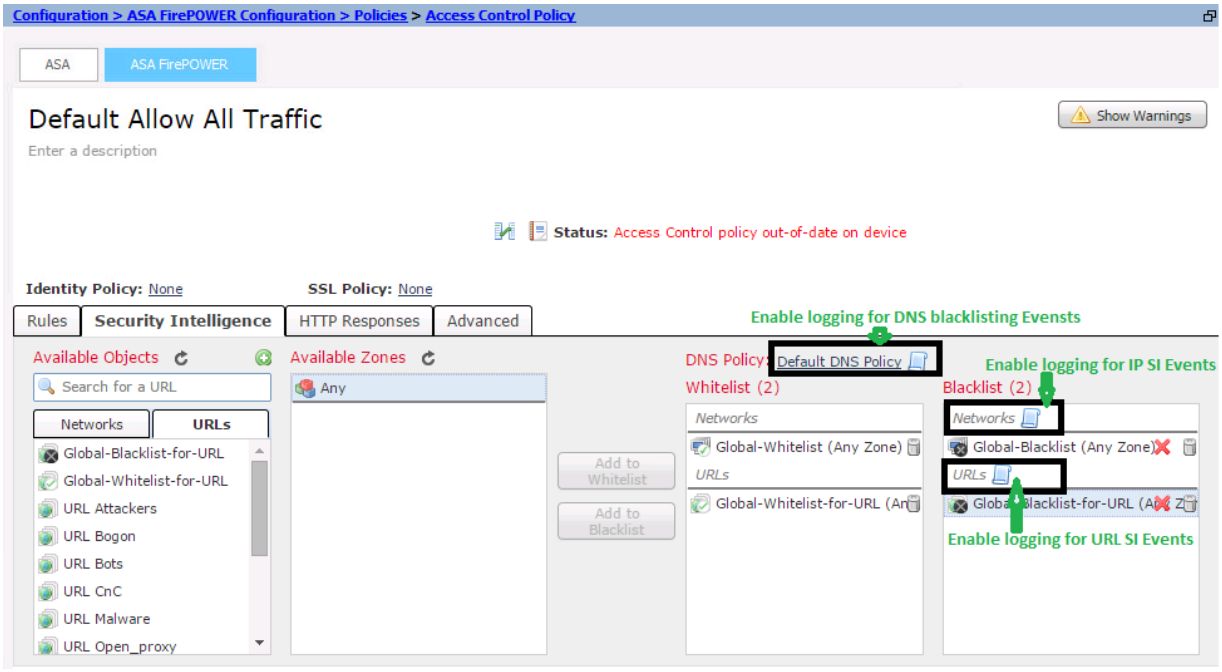
Permita o registro externo para a inteligência de Segurança da Segurança Intelligence/URL da Segurança IP Intelligence/DNS

Os eventos da **inteligência de Segurança da Segurança Intelligence/URL da Segurança IP Intelligence/DNS** são gerados quando o tráfego combina todo o base de dados do endereço IP de Um ou Mais Servidores Cisco ICM NT/da inteligência Segurança do Domain Name /URL. A fim permitir o registro externo para eventos da inteligência de Segurança IP URL/DNS, navegue a **(configuração ASDM > configuração ASA FirePOWER > políticas > a inteligência do > segurança da política do controle de acesso)**,

Clique o **ícone** segundo as indicações da imagem para permitir o registro para a inteligência de Segurança IP/DNS/URL. Clicar o ícone alerta uma caixa de diálogo para permitir o registro e a opção para enviar os eventos ao servidor interno.

A fim enviar eventos a um servidor syslog externo, a um **Syslog** seleto, e selecionar então uma resposta do alerta do Syslog da lista de drop-down. Opcionalmente, você pode adicionar uma resposta do alerta do Syslog clicando o ícone adicionar.

A fim enviar eventos de conexão a um server da armadilha de SNMP, a uma **armadilha de SNMP** seleta, e selecionar então uma resposta do alerta SNMP da lista de drop-down. Opcionalmente, você pode adicionar uma resposta do alerta SNMP clicando o ícone adicionar.



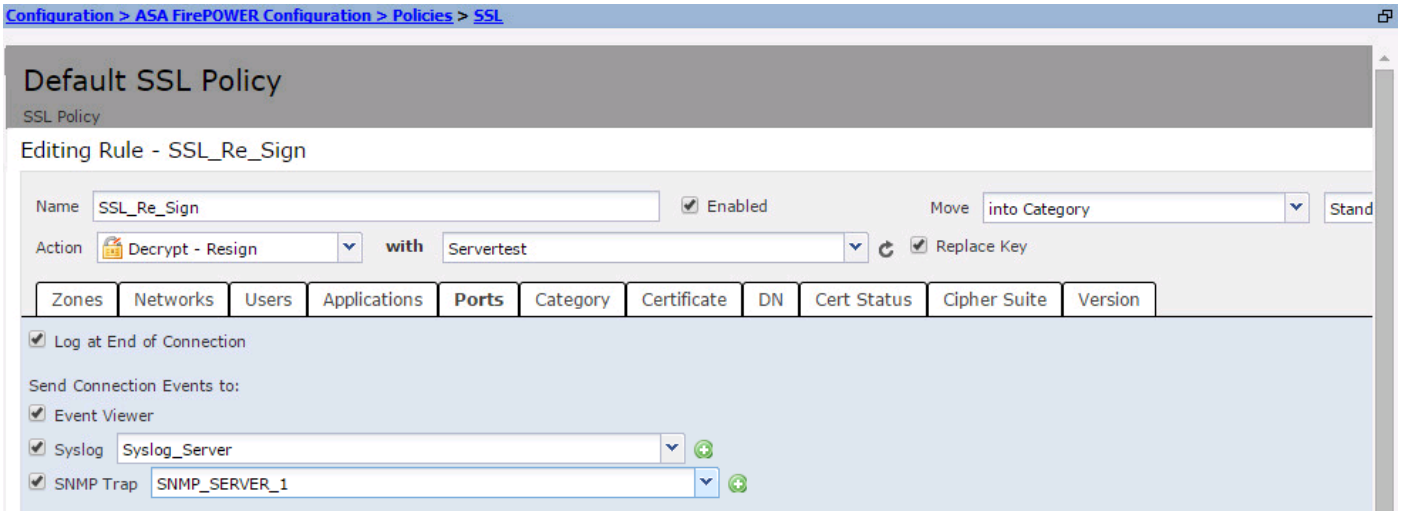
Permita o registro externo para eventos SSL

Os eventos SSL são gerados quando o tráfego combina toda a regra na política SSL, em que registrar está permitido. A fim permitir o registro externo para o tráfego SSL, navegue à **configuração ASDM > à configuração > às políticas > ao SSL ASA FirePOWER.** Edite a existência ou crie uma regra nova e navegue à **opção de registro**. Selecione o **log no fim da opção de conexão**.

Navegue então **para enviar eventos de conexão a** e para especificar onde enviar os eventos.

Para enviar eventos a um servidor syslog externo, a um **Syslog** seleto, e selecionar então uma resposta do alerta do Syslog da lista de drop-down. Opcionalmente, você pode adicionar uma resposta do alerta do Syslog clicando o ícone adicionar.

Para enviar eventos de conexão a um server da armadilha de SNMP, a uma **armadilha de SNMP** seleta, e selecionar então uma resposta do alerta SNMP da lista de drop-down. Opcionalmente, você pode adicionar uma resposta do alerta SNMP clicando o ícone adicionar.



Configuração para enviar os eventos do sistema

Permita o registro externo para eventos do sistema

Os eventos do sistema mostram o estado do sistema operacional de FirePOWER. O SNMP Manager pode ser usado para votar estes eventos de sistemas.

Para configurar o servidor SNMP a fim votar eventos do sistema do módulo de FirePOWER, você precisa de configurar uma política de sistema que faça a informações disponíveis em firePOWER MIB (Management Information Base) que podem ser votados pelo servidor SNMP.

Navegue à **configuração ASDM > à configuração > ao Local > à política de sistema ASA FirePOWER** e clique o **SNMP**.

Versão de SNMP: Suportes de módulo SNMP v1/v2/v3 de FirePOWER. Especifique a versão de SNMP.

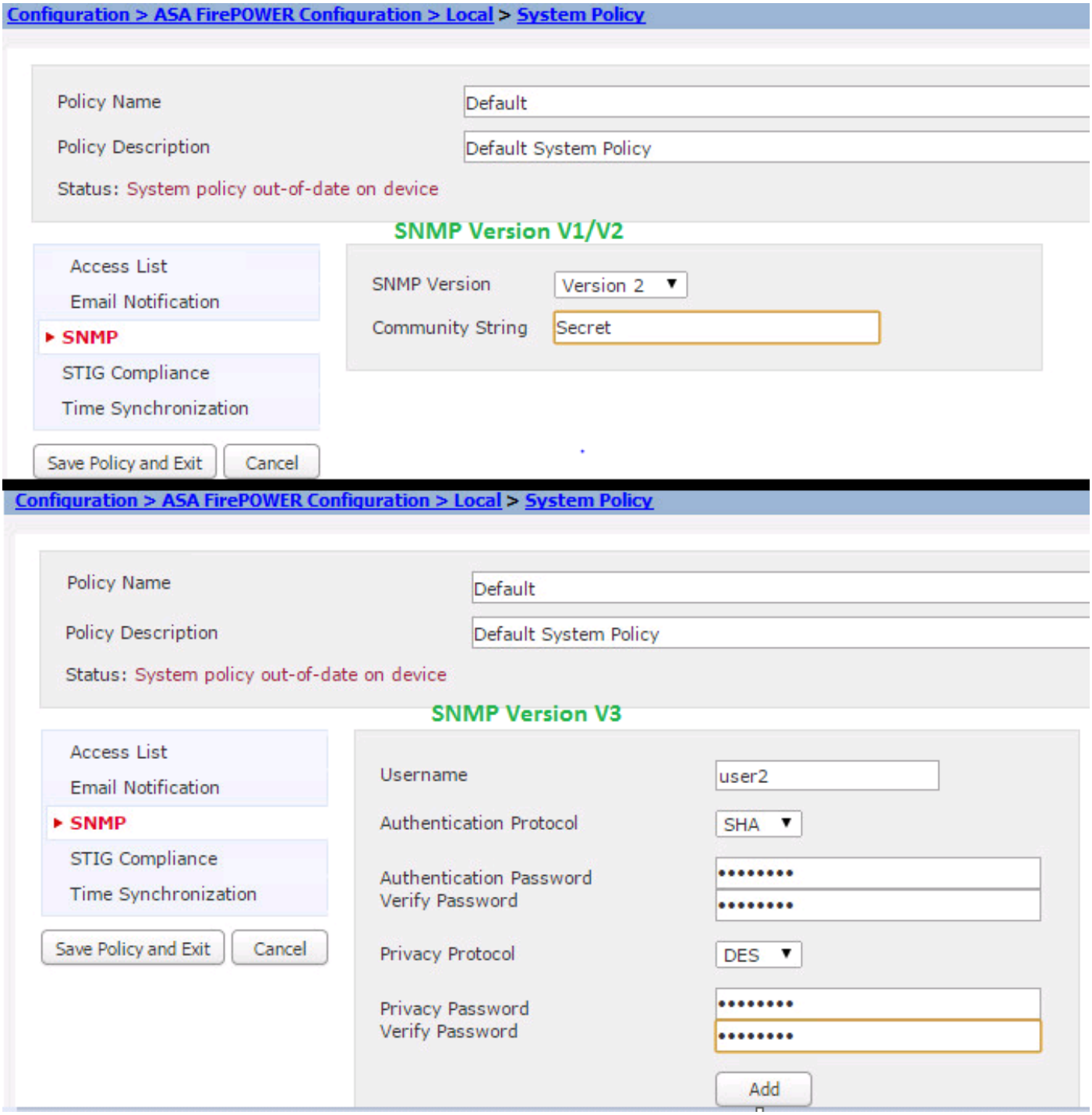
String de comunidade: Se você seleciona **v1/ v2 na** opção da versão de SNMP, datilografe o nome de comunidade SNMP no campo do string de comunidade.

Nome de usuário: Se você seleciona a opção **v3 na** opção da versão. Clique o botão do **usuário adicionar** e especifique o **username no** campo de nome de usuário.

Autenticação: Esta opção é parte de uma configuração SNMP v3. Fornece a autenticação baseada no código de autenticação de mensagens picado usando algoritmos MD5 ou SHA. Escolha o **protocolo** para o algoritmo de hash & incorpore a senha

no campo de **senha**. Se você não quer usar a característica de autenticação a seguir não seleciona **nenhuns** opção.

Privacidade: Esta opção é parte de uma configuração SNMP v3. Fornece a criptografia usando o algoritmo DES/AES. Selecione o protocolo para a criptografia & incorpore a senha ao campo de **senha**. Se você não quer recursos de criptografia de dados a seguir não escolhe **nenhuns** opção.



Note: Um Management Information Base (MIB) é um levantamento de informação que seja organizado hierarquicamente. O arquivo MIB (DCEALERT.MIB) para o módulo de FirePOWER está disponível na localização de diretório (/etc/sf/DCEALERT.MIB) que pode ser buscada desta localização de diretório.

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems