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

## Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Informações de Apoio Configurar Configurando um destino de saída Etapa 1. Configuração do Servidor Syslog Etapa 2. Configuração do servidor SNMP Configuração para enviar os eventos de tráfego Habilitar registro externo para eventos de conexão Habilitar registro externo para eventos de intrusão Habilitar registro externo para inteligência de segurança IP/inteligência de segurança DNS/inteligência de segurança de URL Habilitar registro externo para eventos SSL Configuração para enviar os eventos do sistema Habilitar registro externo para eventos do sistema Verificar Troubleshoot Informações Relacionadas Discussões relacionadas da comunidade de suporte da Cisco

## 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.

| 📴 Cisco ASDM 7.5(2) for ASA - 192.16 | 8.20.1                   |                 |   |                    |        |                |
|--------------------------------------|--------------------------|-----------------|---|--------------------|--------|----------------|
| File View Tools Wizards Wind         | ow Help                  |                 |   | Type topic to sear | ch     | Go             |
| Home 🍇 Configuration 🔯 Mor           | nitoring 🗐 Deploy 👻 🤇    | Refresh 🔇 Ba    | ick 🔘 Forward 🦓 Help                    |                    |        | CISCO          |
| Device List Bookmarks                | Configuration > ASA Fire | POWER Configura | tion > Policies > <u>Actions Alerts</u> |                    |        |                |
| Device List 🗇 🕂 🗙                    |                          |                 |   |                    |        |                |
| 🕈 Add 📋 Delete 🚿 Connect             | Alerts                   |                 |   |                    |        |                |
| Find: Go                             |                          |                 |   |                    | 0      | Create Alert 🔹 |
|                                      | Name                     |                 |   | Туре               | In Use | Enabled        |
|                                      | -                        |                 |   |                    |        |                |
| ASA FirePOWER Configur 🗗 🗜           |                          |                 |   |                    | -      |                |
| Policies                             |                          | Edit Syslog     | Alert Configuration                     |                    | ? ×    |                |
| Access Control Policy                |                          | Name            | Syslog Server                           |                    | _      |                |
|                                      |                          |                 | Systeg_Server                           |                    | - 1    |                |
| Rule Editor                          |                          | Host            | 192.168.20.3                            |                    | - 18   |                |
| SSL                                  |                          | Port            | 514                                     |                    |        |                |
| Actions Alerts                       |                          | Facility        | ALERT                                   |                    | •      |                |
| DNS Policy                           |                          | Severity        | AI FRT                                  |                    | T      |                |
| Device Management                    |                          | Sevency         |   |                    | _      |                |
| Device                               |                          | Tag             |   |                    | _      |                |
| A Device Setup                       |                          |                 |   |                    |        |                |
| Firewall                             |                          |                 | Store ASA FirePOW                       | ER Changes Ca      | ancel  |                |

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.

| Alerts        |                     |                                      |        |        |              |   |
|---------------|---------------------|--------------------------------------|--------|--------|--------------|---|
|               | Edit SNMP AI        | ert Configuration SNMP Version V1/V2 | ? ×    | 0      | Create Alert |   |
| Name          | Name                | SNMP_SERVER_1                        |        | Use    | Enabled      |   |
| Syslog_Server | Trap Server         | 192.168.20.4                         |        | t Used |              | 8 |
|               | Version             | v2                                   | •      |        |              |   |
|               | Community<br>String | Secret                               |        |        |              |   |
|               |                     |                                      |        |        |              |   |
|               |                     | Store ASA FirePOWER Changes          | Cancel | J      |              |   |
| Alerts        |                     |                                      |        |        |              |   |
|               | Edit SNMP A         | ert Configuration SNMP Version V3    | ? ×    |        | Create Alert |   |
| Name          | Name                | SNMP_SERVER_1                        |        | Use    | Enabled      |   |
| Syslog_Server | Trap Server         | 192.168.20.4                         |        | t Used |              | 8 |
|               | Version             | v3                                   | •      |        |              |   |
|               | User Name           | user1                                |        |        |              |   |
|               | Authenticatio       | n                                    |        |        |              |   |
|               | Protocol            | MD5                                  | •      |        |              |   |
|               | Password            | •••••                                |        |        |              |   |
|               | Privacy             |                                      |        |        |              |   |
|               | Protocol            | DES                                  | Ŧ      |        |              |   |
|               | Password            | •••••                                |        |        |              |   |
|               | Engine ID           | Example: 123456789a                  |        |        |              |   |
|               |                     |                                      |        |        |              |   |
|               |                     | Store ASA FirePOWER Changes          |        |        |              |   |

#### 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.

| ASA ASA FirePOWER<br>Editing Rule - WebsiteBlock Name WebsiteBlock  Name WebsiteBlock  IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer, syslog,   |
|---|
| Editing Rule - WebsiteBlock          Name       WebsiteBlock       Image: Comparison of the set of the |
| Name     WebsiteBlock     Move       Action     X Block with reset     IPS: no policies     Variables: n/a     Files: no inspection     Logging: connections: Event Viewer, syslog,   |
| Action X Block with reset   IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer, syslog,  |
|   |
| Zones Networks 🛦 Users Applications Ports URLs 🛦 ISE Attributes Inspection Logging  |
| Log at Beginning and End of Connection  |
| O Log at End of Connection  |
| O 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   |
|   |
|   |
| Save  |

#### 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.

| nfiguration > ASA FirePOWER Confi     | figuration > Policies > Intrusion Policy > Intrusion Policy  |      |
|---------------------------------------|--|------|
|                                       |  |      |
| Policy Information 🖄                  | SNMP Alerting  | < Ba |
| Rules                                 | Settings   |      |
| <ul> <li>Advanced Settings</li> </ul> | Trap Type () as Binary () as String  |      |
| Global Rule Thresholding              | SNMP Version   Version  Versio |      |
| SNMP Alerting                         | SNMP v2  |      |
| Policy Layers                         | Tran Server 192 168 20 3   |      |
|                                       | Community String Count   |      |
|                                       | Community String Secret  |      |
| Policy Information                    | SNMP Alerting  | < E  |
| Rules                                 | Settings   |      |
| Global Rule Thresholding              | Trap Type 💿 as Binary 🔘 as String  |      |
| SNMP Alerting                         | SNMP Version O Version2   Version3   |      |
| Policy Layers                         | SNMP v3  |      |
|                                       | Trap Server 192.168.20.3   |      |
|                                       | Authentication Password  |      |
|                                       | Private Password (SNMP v3 passwords must be 8 or more characters)  |      |
|                                       | Username user3   |      |
|                                       |  |      |

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.

| Configuration > ASA FirePOWER Config | <u>guration &gt; Policies</u> > <u>Intrusion Policy</u> > <u>Intrusion Policy</u>                               |        |
|--------------------------------------|---|--------|
| Policy Information                   | Syslog Alerting   | < Back |
| Rules                                | Settings  |        |
| Global Rule Thresholding             | Logging Hosts       192.168.20.3       (Single IP address or comma-separated list)         Facility       ALERT |        |
| SNMP Alerting<br>Syslog Alerting     | Priority EMERG T  |        |
| Policy Layers                        | Revert to Defaults  |        |

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.

| Configuration > ASA FirePOWER Config                       | <u>uration &gt; Policies &gt; A</u> | ccess Control I | Policy              |   | đ  |
|--|-------------------------------------|-----------------|---------------------|---|--|
| ASA ASA FirePOWER  |                                     |                 |                     |   |  |
| Default Allow All Tra                                      | offic                               |                 |                     |   | Show Warnings                                    |
|  |                                     |                 | Status: Access Co   | ntrol policy out-of-date on device  |  |
| Identity Policy: None                                      | SSL Policy: None                    |                 |                     |   |  |
| Rules Security Intelligence                                | HTTP Responses                      | Advanced        |                     | Enable logging for DNS  | blacklisting Evensts                             |
| Available Objects C C<br>Search for a URL<br>Networks URLs | Available Zones 🖒                   |                 |                     | DNS Policy Default DNS Policy<br>Whitelist (2) Networks Clobal Whitelist (Any Topo) | Enable logging for IP SI Events<br>Blacklist (2) |
| Global-Blacklist-for-URL                                   |                                     |                 | Add to              | URLs  |  |
| Global-Whitelist-for-URL                                   |                                     |                 | whitelist           | Global-Whitelist-for-URL (An  | 🙀 Globa Blacklist-for-URL (A💢 Z                  |
| URL Bogon  |                                     |                 | Add to<br>Blacklist |   | Enable logging for LIRI SI Events                |
| JURL Bots  |                                     |                 |                     |   |  |
| JURL CnC   |                                     |                 |                     |   |  |
| 🗑 URL Malware  |                                     |                 |                     |   |  |
| 🗑 URL Open_proxy 🔻   |                                     |                 |                     |   |  |

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.

| Configuration > ASA FirePOWER Configuration > Policies > SSL                                     | Ð |
|--|---|
| Default SSL Policy<br>SSL Policy   | Î |
| Editing Rule - SSL_Re_Sign   |   |
| Name SSL_Re_Sign   Move into Category   Stan   | d |
| Action 🛗 Decrypt - Resign 🔹 with Servertest 🔹 🕑 C Replace Key                                    |   |
| Zones Networks Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version |   |
| ✓ Log at End of Connection   |   |
| Send Connection Events to:   |   |
| ✓ Event Viewer   |   |
| Syslog_Server  |   |
| SNMP Trap SNMP_SERVER_1  |   |

#### 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.

| Delian News   | D.C. H   |   |
|---|--|---|
| Policy Name   | Default  |   |
| Policy Description  | Default System   | m Policy  |
| Status: System policy out-of-   | date on device   |   |
|   | SNMP Version V1  | /V2   |
| Access List   | enner i  |   |
| Email Notification  | SNMP Version Ver   | rsion 2   |
| SNMP  | Community String Sec   | cret  |
| STIG Compliance   |  |   |
| Time Synchronization  |  |   |
|   |  |   |
| ave Policy and Exit Cancel  |  |   |
|   | )  |   |
| iquration > ASA FirePOWER (   | configuration > Local > System   | n Policy  |
| iquration > ASA FirePOWER (   | <u>Configuration &gt; Local</u> > <u>Systen</u>  | n Policy  |
| iquration > ASA FirePOWER (   | Configuration > Local > System   | n Policy  |
| iquration > ASA FirePOWER (<br>Policy Name  | Configuration > Local > System   | n Policy  |
| iquration > ASA FirePOWER (<br>Policy Name<br>Policy Description  | Default System   | n Policy<br>em Policy   |
| iguration > ASA FirePOWER (<br>Policy Name<br>Policy Description<br>Status: System policy out-of-   | Default<br>Default System  | n Policy<br>em Policy   |
| iguration > ASA FirePOWER (<br>Policy Name<br>Policy Description<br>Status: System policy out-of  | Default<br>Default<br>Default Syste<br>date on device<br>SNMP Version  | n Policy<br>em Policy   |
| iguration > ASA FirePOWER (<br>Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List   | Default<br>Default<br>Default Syste<br>date on device<br>SNMP Version  | n Policy  |
| iquration > ASA FirePOWER (<br>Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List<br>Email Notification   | Default<br>Default<br>Default Syste<br>Odate on device<br>SNMP Version<br>Username   | n Policy<br>em Policy<br>n V3<br>user2                                  |
| Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List<br>Email Notification  | Default<br>Default System<br>-date on device<br>SNMP Version<br>Username<br>Authentication Protocol  | n Policy<br>em Policy<br>NV3<br>user2<br>SHA ▼                          |
| Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List<br>Email Notification<br>STIG Compliance   | Default<br>Default<br>Default Syste<br>date on device<br>SNMP Version<br>Username<br>Authentication Protocol   | n Policy<br>em Policy<br>I V3<br>User2<br>SHA T                         |
| Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List<br>Email Notification<br>STIG Compliance<br>Time Synchronization   | -date on device<br>Username<br>Authentication Protocol<br>Verify Password  | n Policy<br>em Policy<br>I V3<br>User2<br>SHA V<br>d                    |
| Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List<br>Email Notification<br>SNMP<br>STIG Compliance<br>Time Synchronization   | -date on device<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Output<br>Outpu | n Policy<br>em Policy<br>NV3<br>user2<br>SHA ▼<br>d<br>••••••••         |
| iquration > ASA FirePOWER (         Policy Name         Policy Description         Status: System policy out-of         Access List         Email Notification         STIG Compliance         Time Synchronization         Save Policy and Exit         Cancel | Image: Second system         Default         Default System         Image: Operation system         Image: Operat  | n Policy<br>em Policy<br>I V3<br>user2<br>SHA ▼<br>SHA ▼<br>DES ▼       |
| Policy Name<br>Policy Description<br>Status: System policy out-of<br>Access List<br>Email Notification<br>STIG Compliance<br>Time Synchronization<br>Save Policy and Exit Cancel  | -date on device<br>SNMP Version<br>Username<br>Authentication Protocol<br>Verify Password<br>Privacy Protocol<br>Privacy Password  | em Policy em Policy User2 SHA  DES  L L L L L L L L L L L L L L L L L L |

**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

<u>Suporte Técnico e Documentação - Cisco Systems</u>