# Configurar a política da intrusão e a configuração da assinatura no módulo da potência de fogo (o Gerenciamento da Em-caixa)

## Índice



## Introdução

Este documento descrevem a funcionalidade do sistema de detecção do Intrusion Prevention System (IPS) /Intrusion (IDS) do módulo da potência de fogo e os elementos da vária política da intrusão que fazem uma política da detecção no módulo da potência de fogo.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

* Conhecimento do Firewall adaptável da ferramenta de segurança (ASA), Security Device Manager adaptável (ASDM).

* Conhecimento do dispositivo da potência de fogo.

## Componentes Utilizados

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

Versão de software running 5.4.1 dos módulos da potência de fogo ASA (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) e mais alto.

Versão de software running 6.0.0 do módulo da potência de fogo ASA (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) e mais alto.

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 sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

# Informações de Apoio

A potência de fogo IDS/IPS é projetada examinar o tráfego de rede e identificar todos os testes padrões maliciosos (ou assinaturas) que indicarem um ataque da rede/sistema. O módulo da potência de fogo funciona no modo IDS se a serviço-política do ASA está configurada especificamente no modo de monitor (promíscuo) mais, ele trabalha no modo Inline.

A potência de fogo IPS/IDS é uma aproximação assinatura-baseada da detecção. FirePOWERmodule no modo IDS gerencie um alerta quando a assinatura combina o tráfego malicioso, visto que o módulo da potência de fogo no modo IPS gerencie o tráfego malicioso do alerta e do bloco.

> Nota: Assegure-se de que o módulo da potência de fogo deva ter **proteger a** licença configurar esta funcionalidade. Para verificar a licença, navegue a **licença da configuração > da potência de fogo ASA a configuração >.**

# Configuração

## Etapa 1. Configurar a política da intrusão

### Etapa 1.1. Crie a política da intrusão

Para configurar a política da intrusão, entre ao Security Device Manager adaptável (ASDM) e termine estas etapas:

Etapa 1. Navegue à **configuração da configuração > da potência de fogo ASA > às políticas > à política da intrusão > à política da intrusão**.

Etapa 2. Clique a **política da criação**.

Etapa 3. Dê entrada com o **nome da** política da intrusão.

Etapa 4. Incorpore a **descrição da** política da intrusão (opcional).

Etapa 5. Especifique a **gota quando** opção **Inline**.

Etapa 6. Selecione a **política baixa da** lista de gota para baixo.

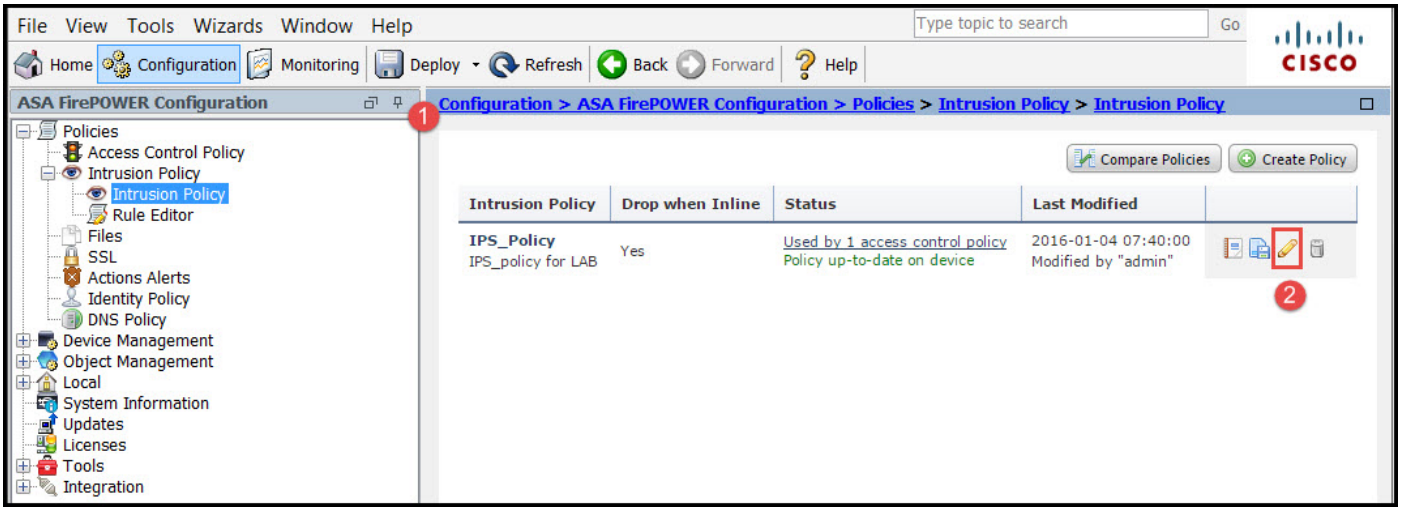
Etapa 7. O clique **cria a política** para terminar a criação da política da intrusão.

> Dica: Deixe cair quando a opção Inline for crucial em determinadas encenações quando o sensor estiver configurado no modo Inline e se exigir para não deixar cair o tráfego mesmo que combine uma assinatura que tenha uma ação de queda.

Você pode observar que a política está configurada, contudo, não está aplicada a nenhum dispositivo.

### Etapa 1.2. Altere a política da intrusão

Para alterar a política da intrusão, para navegar à **configuração da configuração > da potência de fogo ASA > às políticas > à política da intrusão > à política da intrusão** e a seleto **edite a** opção.



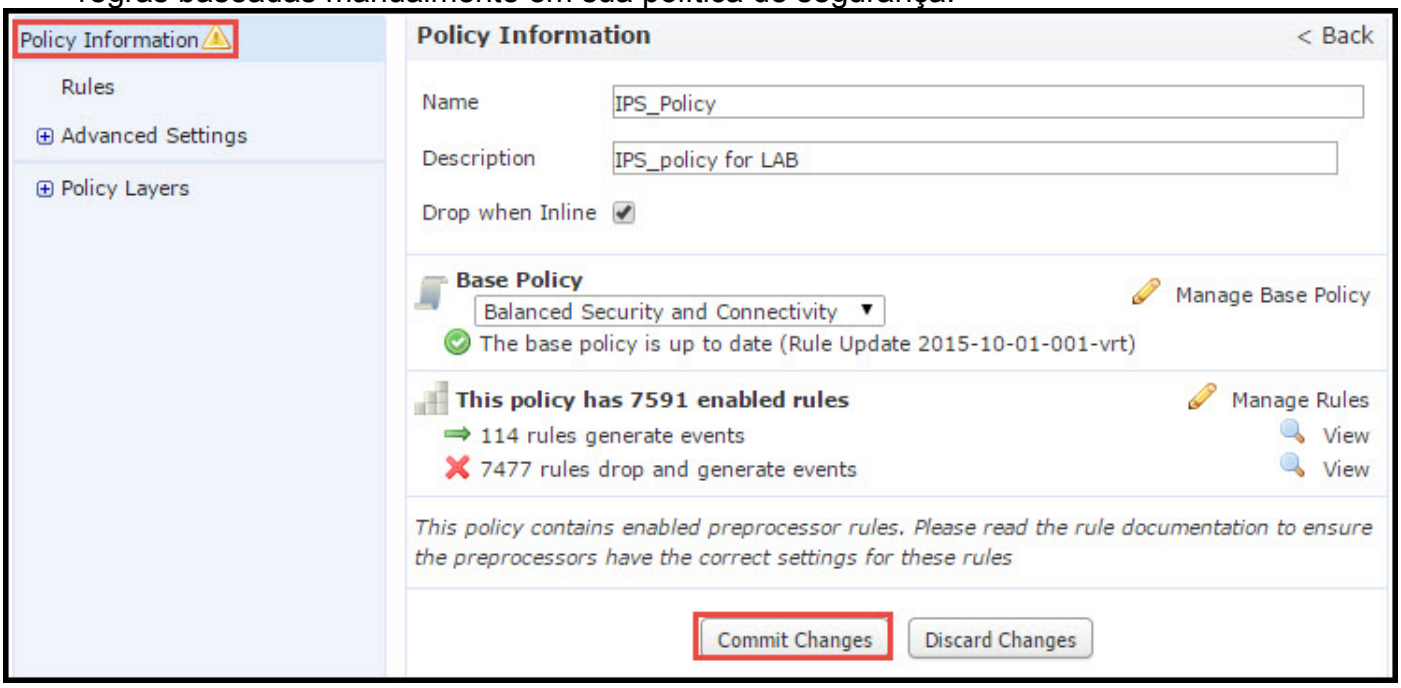

### Etapa 1.3. Altere a política baixa

A página do Gerenciamento de políticas da intrusão der a opção para mudar a gota baixa da política quando Inline/opção da salvaguarda e do descarte.

A política baixa contém algum sistema-forneceu as políticas, que são políticas incorporados.

1. Segurança e Conectividade equilibradas: É uma política ótima em termos da Segurança e da Conectividade. Esta política tem ao redor 7500 regras permitidas, algumas delas gerenciem somente eventos visto que outro gerenciem eventos assim como deixam cair o tráfego.
2. Segurança sobre a Conectividade: Se sua preferência é Segurança então você pode escolher a Segurança sobre a política de conectividade, que aumenta o número de regras permitidas.

3. Conectividade sobre a Segurança: Se sua preferência é Conectividade um pouco do que Segurança então você pode escolher a Conectividade sobre a política de segurança que reduzirá o número de regras permitidas.
4. Detecção máxima - Selecione esta política para obter a detecção máxima.
5. Nenhum Active da regra - Esta opção desabilita todas as regras. Você precisa de permitir as regras baseadas manualmente em sua política de segurança.




### Etapa 1.4. Assinatura que filtra com opção da barra do filtro

Navegue à opção das **regras no** painel navegacional e a página do Gerenciamento da regra publica-se. Há uns milhares da regra no base de dados da regra. A barra do filtro fornece uma boa opção do Engine de busca para procurar eficazmente a regra.

Você pode introduzir toda a palavra-chave na barra do filtro e o sistema agarra os resultados para você. Se há uma exigência encontrar a assinatura para a vulnerabilidade heartbleed do secure sockets layer (SSL), você pode procurar a palavra-chave heartbleed na barra do filtro e buscará a assinatura para a vulnerabilidade heartbleed.

> Dica: Se as palavras-chaves múltiplas são usadas na barra do filtro então o sistema combina-as que usam-se E a lógica para criar um composto procura.

Você pode igualmente procurar as regras usando o ID de assinatura (SID), o gerador ID (GID), categoria: dos etc.

As regras são divididas eficazmente em formas múltiplas tais como baseado em vulnerabilidades de Microsoft das classificações da categoria/em específico da plataforma sem-fins de Microsoft. Tal associação das regras ajuda o cliente a obter a assinatura direita em uma maneira fácil e a ajudar o cliente a ajustar eficazmente as assinaturas.

Você pode igualmente procurar com número CVE para encontrar as regras que as cobrem. Você pode usar o **CVE da** sintaxe**: <cve-number>.**

### Etapa 1.5. Configurar o estado da regra

Navegue à opção das **regras no** painel navegacional e a página do Gerenciamento da regra publica-se. Selecione as regras e escolha o **estado da regra da** opção configurar o estado das regras. Há três estados que podem ser configurados para uma regra:

1. **Gerencia eventos:** Esta opção gerencie eventos quando a regra combina o tráfego.

2. **Deixe cair e gerencia eventos:** Esta opção gerencie eventos e tráfego da gota quando a regra combina o tráfego.

3. **Desabilitado:** Esta opção desabilita a regra.

### Etapa 1.6. O filtro do evento configura

A importância de um evento da intrusão pode ser baseada na frequência de ocorrência, ou na fonte ou no endereço IP de destino. Em alguns casos, você não pode importar-se com um evento até que ocorra um determinado número de vezes. Por exemplo, você não pôde ser referido se alguém tenta entrar a um server até que falhem um determinado número de vezes. Em outros casos, você pôde somente precisar de ver algumas ocorrências da batida da regra para verificar se há um problema difundido.

Há duas maneiras por que você pode conseguir este:

1. Ponto inicial do evento.

2. Supressão do evento.

### Ponto inicial do evento

Você pode ajustar os pontos iniciais que ditam como um evento é indicado frequentemente, com base no número de ocorrências. Você pode configurar o limiar pelo evento e pela política.

Etapas para configurar o ponto inicial do evento:

Etapa 1. Selecione as **regras** para que você quer configurar o ponto inicial do evento.

Etapa 2. Clique a **filtração do evento**.

Etapa 3. Clique o **ponto inicial**.

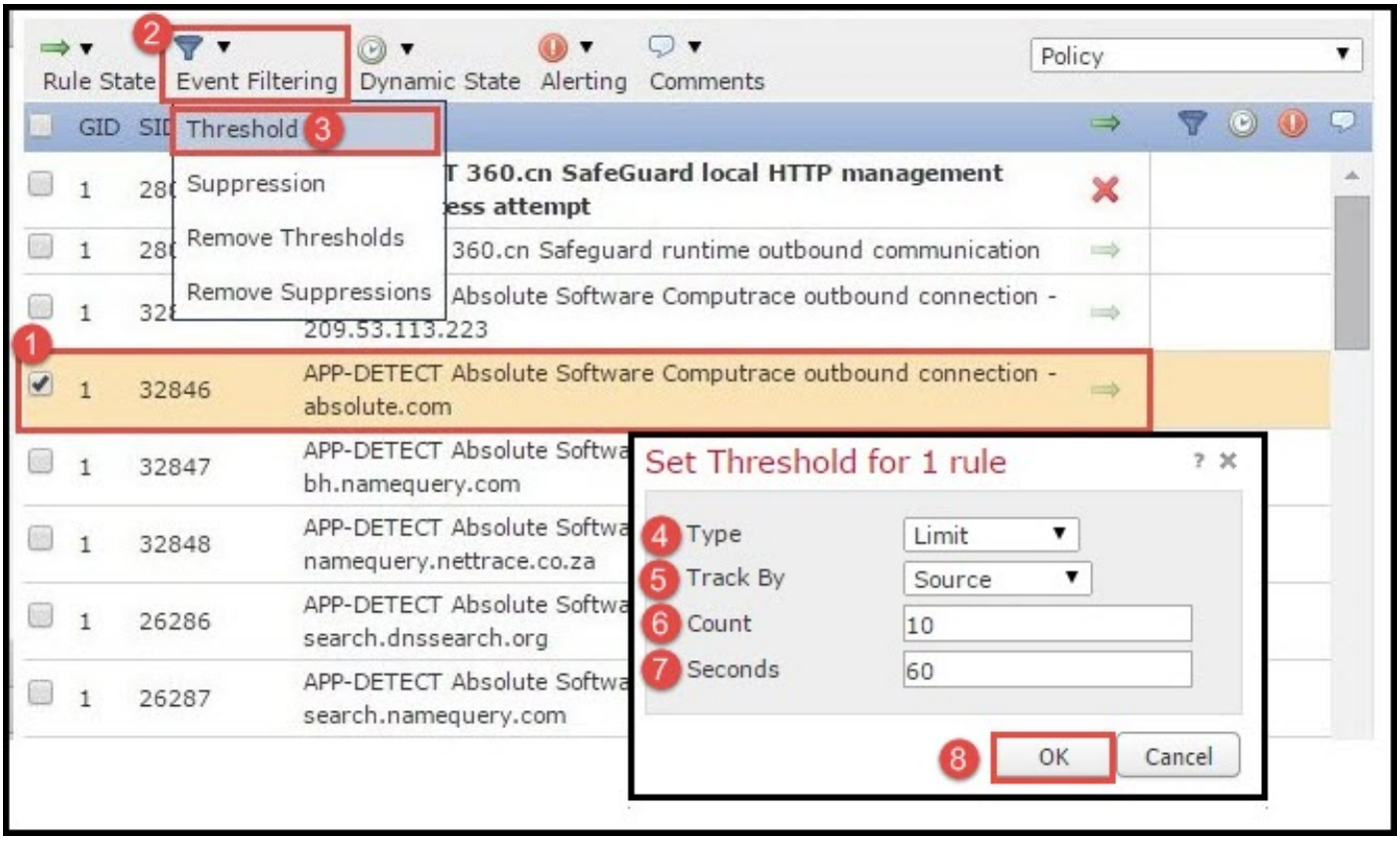
Etapa 4. Selecione o **tipo da** lista de gota para baixo. (Limite ou ponto inicial ou ambos).

Etapa 5. Selecione como você quer seguir da **trilha pela** caixa da gota. (Fonte ou destino).

Etapa 6. Incorpore a **contagem dos** eventos para encontrar o ponto inicial.

Etapa 7. Incorpore os **segundos** para decorrer antes das restaurações da contagem.

Etapa 8. **APROVAÇÃO do** clique a terminar.




Depois que um filtro do evento é adicionado a uma regra, você deve poder ver um ícone do filtro ao lado da indicação da regra, que mostra que há uma filtração do evento permitida para esta regra.

**Supressão do evento**

As notificações especificadas dos eventos podem ser suprimidas com base no endereço IP de origem/destino ou pela regra.

**Nota:** Quando você adicionar a supressão do evento para uma regra. A inspeção da assinatura trabalha como normalmente mas o sistema não gerencie os eventos se o tráfego combina a assinatura. Se você especifica uma fonte/destino específicos então os eventos não aparecem somente para a fonte/destino específicos para esta regra. Se você escolhe suprimir a regra completa então o sistema não gerencie nenhum evento para esta regra.

Etapas para configurar o ponto inicial do evento:

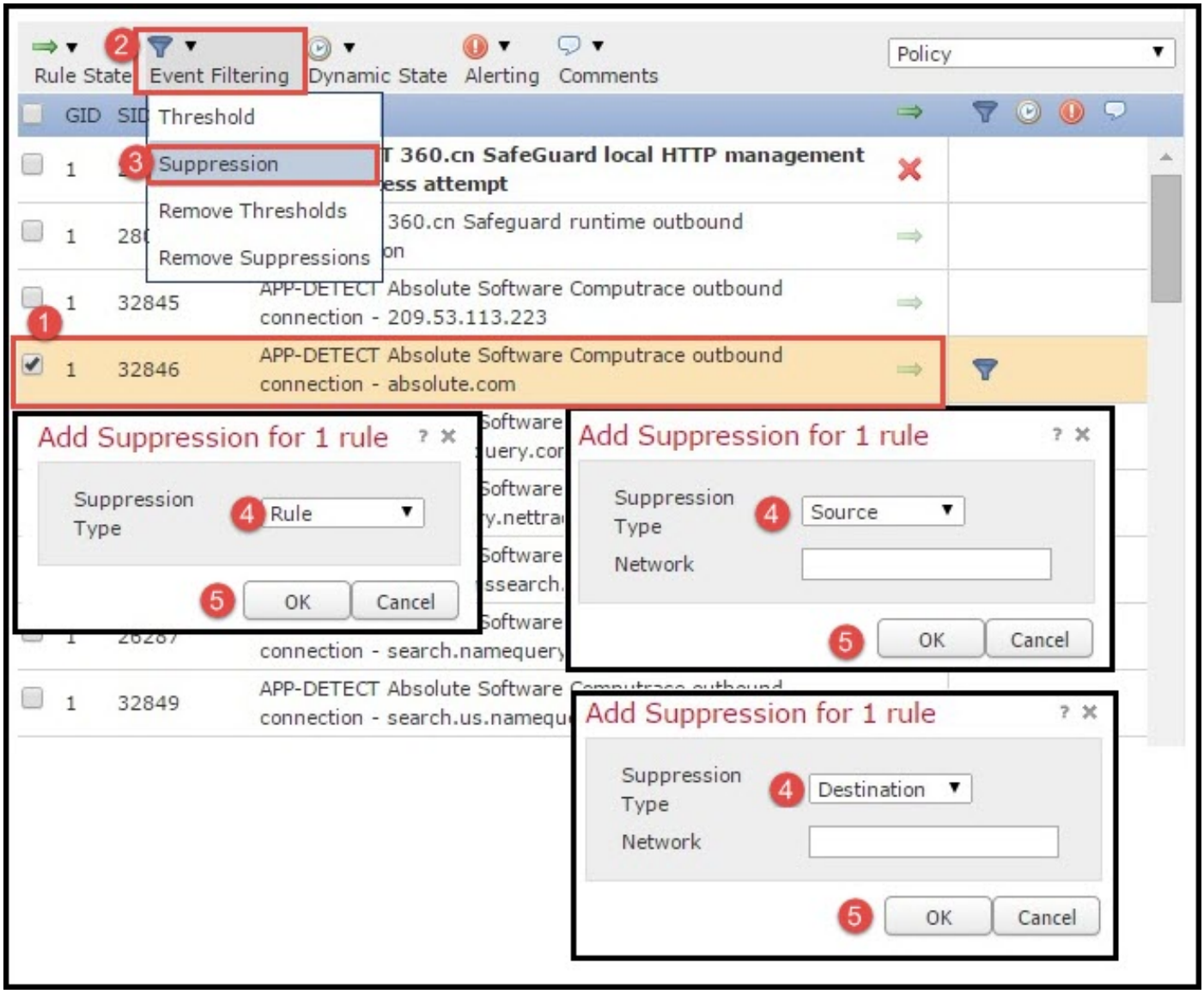
Etapa 1. Selecione as **regras** para que você quer configurar o ponto inicial do evento.

Etapa 2. **Filtração do evento do** clique.

Etapa 3. **Supressão do** clique.

**Tipo da supressão da** etapa 4.Select de gota da lista para baixo. (Regra ou fonte ou destino).

Etapa 5. **APROVAÇÃO do** clique a terminar.




Depois que o filtro do evento é adicionado a esta regra, você deve poder ver um ícone do filtro com a contagem dois ao lado da indicação da regra, que mostra que há dois filtros do evento permitidos para esta regra.

### Etapa 1.7. Configurar o estado dinâmico

Éuma característica onde nós podemos mudar o estado de uma regra se a condição especificada combina.

Supõe uma encenação do ataque de força bruta para rachar a senha. Se uma assinatura detecta a tentativa da falha da senha e a ação da regra são gerar um evento. O sistema mantém-se em gerar o alerta para a tentativa da falha da senha. Para esta situação, você pode usar o **estado dinâmico** onde uma ação de **eventos Generate** pode ser mudada **para deixar cair e gerar eventos** para obstruir o ataque de força bruta.

Navegue à opção das **regras no** painel navegacional e a página do Gerenciamento da regra publica-se. Selecione a regra para que você quer permitir o estado dinâmico e escolher o **> Add dinâmico do estado das** opções um **estado da regra da Taxa-base.**

Para configurar o estado com base em taxa da regra:

1. Selecione as **regras** para que você quer configurar o ponto inicial do evento.

2. Clique o **estado dinâmico**.
3. Clique o **estado com base em taxa da regra adicionar**.
4. Selecione como você quer seguir o estado da regra da **trilha pela** caixa da gota. (**Regra ou fonte ou destino**).
5. Incorpore a **rede**. Você pode especificar um único endereço IP de Um ou Mais Servidores Cisco ICM NT, o bloco de endereço, a variável, ou uma lista separada - da vírgula que seja compreendida de toda a combinação destes.
6. Incorpore a **contagem dos** eventos e o timestamp aos segundos.
7. Selecione o **estado novo,** você querem definir para a regra.
8. Incorpore o **intervalo** depois do qual o estado da regra é revertido.
9. **APROVAÇÃO do** clique a terminar.

## Etapa 2. Configurar a política da análise de rede (SESTA) & os conjuntos variáveis (opcionais)

### Configurar a política da análise de rede

A política do acesso de rede é sabida igualmente como preprocessors. O preprocessor faz a remontagem do pacote e normaliza o tráfego. Ajuda a identificar anomalias da camada de rede e do protocolo de camada de transporte na identificação de opções impróprias do encabeçamento.

A SESTA faz o defragmentation de datagramas IP, fornece a inspeção stateful TCP e a remontagem do córrego e somas de verificação da validação. O preprocessor normaliza o tráfego, valida e verifica o padrão de protocolo.

Cada preprocessor tem seu próprio número GID. Representa que preprocessor foi provocado pelo pacote.

Para configurar a política da análise de rede, navegue à **configuração da configuração > da potência de fogo ASA > às políticas > à política do controle de acesso > avançou > política da análise de rede e da intrusão**

A política da análise de rede padrão é Segurança e a Conectividade equilibradas que é política recomendada ótima. Há outras três mais políticas fornecidas sistema da SESTA que podem ser selecionadas da lista de drop-down.

Selecione a lista da **política da análise de rede da** opção para criar a política feita sob encomenda da SESTA.

### Configurar conjuntos variáveis

Os conjuntos variáveis são usados em regras da intrusão para identificar os endereços de rementente e destinatário e as portas. As regras são mais eficazes quando as variáveis refletem seu ambiente de rede mais exatamente. A variável joga um papel importante no ajuste de desempenho.

Os conjuntos variáveis têm sido configurados já com opção padrão (/porta da rede). Adicionar conjuntos variáveis novos se você quer mudar a configuração padrão.

Para configurar os conjuntos variáveis, navegue à **configuração da configuração > da potência de fogo ASA > ao Gerenciamento > ao conjunto variável do objeto**. A opção seleta **adiciona o**

**conjunto variável** para adicionar conjuntos variáveis novos. Dê entrada com o **nome dos** conjuntos variáveis e especifique a **descrição.**

Se qualquer aplicativo feito sob encomenda trabalha em uma porta específica a seguir define o número de porta no campo de número de porta. Configurar o parâmetro de rede.

**$Home_NET** especificam a rede interna.

**$External_NET** especificam a rede externa.

## Passo 3: Configurar o controle de acesso para incluir conjuntos variáveis da SESTA da política da intrusão

Navegue à **configuração da configuração > da potência de fogo ASA > às políticas > à política do controle de acesso.** Você precisa de terminar estas etapas:

1. Edite a regra da política de acesso onde você quer atribuir a política da intrusão.
2. Escolha a aba da **inspeção.**
3. Escolha a **política da intrusão da** lista de gota para baixo e escolha os **conjuntos variáveis** de deixam cair para baixo a lista
4. Clique em Salvar.

Desde que uma política da intrusão é adicionada a esta regra da política de acesso. Você pode ver o ícone do protetor na cor dourada que indica que a política da intrusão está permitida.

**A potência de fogo da loja ASA do** clique **muda** para salvar as mudanças.

## Etapa 4. Distribua a política do controle de acesso

Agora, você deve distribuir a política do controle de acesso. Antes que você aplique a política, você verá uma política do controle de acesso da indicação expirado no dispositivo. Para distribuir as mudanças ao sensor:

1. O clique **distribui**.
2. O clique **distribui mudanças da potência de fogo**.
3. O clique **distribui na** janela pop-up.

Nota: Na versão 5.4.x, para aplicar a política de acesso ao sensor, você precisa de clicar aplica mudanças da potência de fogo ASA

Nota: Navegue à **monitoração > monitoração da potência de fogo ASA > estado da tarefa.** Assegure-se de que a tarefa deva terminar para aplicar a alteração de configuração.

## Etapa 5. Monitore eventos da intrusão

Para ver os eventos da intrusão gerados pelo módulo da potência de fogo, navegue à **monitoração > monitoração da potência de fogo ASA > tempo real Eventing.**

# Verificar

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

# Troubleshooting

Etapa 1. Assegure-se de que o estado da regra de regras esteja configurado apropriadamente.

Etapa 2. Assegure-se de que a política correta IPS esteja incluída em regras do acesso.

Etapa 3. Assegure-se de que os grupos das variáveis estejam configurados corretamente. Se os conjuntos variáveis não são configurados corretamente então as assinaturas não combinarão o tráfego.

Etapa 4. Assegure-se de que a distribuição de política do controle de acesso termine com sucesso.

Etapa 5. Monitore os eventos de conexão e os eventos da intrusão para verificar se o fluxo de tráfego está batendo a regra correta ou não.

## Informações Relacionadas

- **Guia de início rápido do módulo da potência de fogo de Cisco ASA**
- **Suporte Técnico e Documentação - Cisco Systems**