

Configurar uma regra de aprovação em um sistema Cisco Firepower

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Criar uma regra de aprovação](#)

[Habilitar uma regra de aprovação](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve uma regra de passagem, como criá-la e como ativá-la em uma política de invasão.

Você pode criar regras de passagem para impedir que os pacotes que atendem aos critérios definidos na regra de passagem acionem a regra de alerta em situações específicas, em vez de desativar a regra de alerta. Por padrão, as regras de passagem substituem as regras de alerta. Um sistema Firepower compara pacotes com as condições especificadas em cada regra e, se os dados do pacote corresponderem a todas as condições especificadas em uma regra, a regra é disparada. Se uma regra for uma regra de alerta, ela gerará um evento de invasão. Se for uma regra de passagem, ela ignora o tráfego.

Por exemplo, você pode desejar que uma regra que procure tentativas de fazer login em um servidor FTP como o usuário "anonymous" permaneça ativo. No entanto, se sua rede tiver um ou mais servidores FTP anônimos legítimos, você poderá gravar e ativar uma regra de passagem que especifique que, para esses servidores específicos, os usuários anônimos não disparam a regra original.

Caution: Quando uma regra original na qual a regra de aprovação é baseada recebe uma revisão, a regra de aprovação não é atualizada automaticamente. Portanto, as regras de aprovação podem ser difíceis de manter.

Note: Se você habilitar o recurso Supressão para uma regra, ele suprime as notificações de evento para essa regra. No entanto, a regra ainda é avaliada. Por exemplo, se você suprime uma regra de queda, os pacotes que correspondem à regra são silenciosamente descartados.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Configurar

Criar uma regra de aprovação

1. Navegue até **Objetos > Regras de intrusão**. A lista de categorias de regras é exibida.
2. Localize a categoria de regra associada à regra que deseja filtrar. Use o ícone de seta para expandir a categoria de regra das listas de categorias e localizar a regra para a qual deseja criar uma regra de aprovação. Como alternativa, você pode usar a caixa de pesquisa de regra.
3. Depois de encontrar a regra desejada, clique no ícone do lápis ao lado dela para editar a regra.
4. Ao editar uma regra, faça o seguinte: Clique no botão **Editar** que corresponde à regra. Na lista suspensa **Ação**, escolha **passar**. Altere o campo **IPs de origem** e o campo **IPs de destino** para os hosts ou redes sobre os quais você não deseja que a regra seja alertada. Clique em **Salvar como novo**.

Edit Rule 3:13921:5


[\(View Documentation, Rule Comment\)](#)

Message	IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling me		
Classification	Attempted Administrator Privilege Gain ▼		
	Edit Classifications		
Action	pass ▼		
Protocol	tcp ▼		
Direction	Directional ▼		
Source IPs	any	Source Port	any
Destination IPs	\$HOME_NET	Destination Port	143

Detection Options

reference	
<input type="text" value="url,secunia.com/advisories/24596"/>	
reference	
<input type="text" value="bugtraq,23058"/>	
reference	
<input type="text" value="cve,2007-1578"/>	
metadata	
<input type="text" value="engine shared, soid 3 13921, service imap"/>	
ack ▼ <input type="button" value="Add Option"/>	<input type="button" value="Save As New"/>

5. Observe o número de ID da nova regra. Por exemplo, 1000000.

 **Success** ✕
Successfully created new rule "IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling memory corruption attempt"

Edit Rule 3:1000000:1 [\(View Documentation, Rule Comment\)](#)

Message:

Classification: ▼
[Edit Classifications](#)

Action: ▼

Protocol: ▼

Direction: ▼

Source IPs: Source Port:

Destination IPs: Destination Port:

Detection Options

reference

reference

reference

metadata

▼

Habilitar uma regra de aprovação

Você precisa ativar sua nova regra na política de invasão apropriada para transmitir o tráfego nos endereços de origem ou destino que você especificou. Siga estas etapas para ativar uma regra de passagem:

1. Modificar a política de intrusão ativa: Navegue até **Políticas > Controle de acesso > Invasão**. Clique em **Editar** ao lado da política de intrusão ativa.
2. Adicione a nova regra à lista de regras: Clique em **Regras** no painel do lado esquerdo. Digite a ID da regra anotada anteriormente na caixa de filtro. Marque a caixa de seleção Regras e

altere o Estado da regra para **Gerar eventos**. Clique em **Policy Information (Informações da política)** no painel à esquerda. Clique em **Confirmar alterações**.

3. Clique em **Implantar** para implantar as alterações no dispositivo.

Verificar

Você deve monitorar os novos eventos por algum tempo para garantir que nenhum evento seja gerado para essa regra específica para o endereço IP de origem ou de destino definido.

Troubleshoot

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