# Gerente de dispositivo de sistema 5.1 da prevenção de intrusão - Assinatura do acordo

## Índice



## Introdução

O Intrusion Prevention System (IPS) 5.1 contém sobre 1000 assinaturas incorporados do padrão. Você não pode rebatizar ou suprimir de assinaturas da lista de assinaturas incorporados, mas você pode aposentar-se assinaturas para removê-las do motor de detecção. Você pode mais tarde ativar assinaturas aposentadas. Contudo, este processo exige os motores de detecção reconstruir sua configuração, que toma o tempo e poderia atrasar o processamento do tráfego. Você pode ajustar assinaturas incorporados quando você ajusta diversos parâmetros da assinatura. As assinaturas incorporados que foram alteradas são chamadas *assinaturas ajustadas*.

Este documento ilustra as etapas para usar-se a fim ajustar a assinatura usando o gerenciador de dispositivo IPS (IDM). O IDM é um com base na Web, o aplicativo de java que o permite de configurar e controlar seu sensor. O servidor de Web para o IDM reside no sensor. Você pode alcançá-lo com os navegadores da Web do internet explorer, do Netscape, ou do Mozilla.

**Nota:** Você pode criar as assinaturas, que são chamadas *assinaturas feitas sob encomenda*. A assinatura feita sob encomenda ID começa em 60000. Você pode configurar-los para diversas coisas, tais como a harmonização das cordas em conexões de UDP, o seguimento de inundações da rede, e as varreduras. Cada assinatura é criada usando um Engine de assinatura projetado especificamente para o tipo de tráfego que é monitorado.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

## Componentes Utilizados

A informação neste documento é baseada no gerenciador de dispositivo 5.x do Sistema de prevenção de intrusões da Cisco.

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.

## Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Informações de Apoio

A fim configurar um sensor para monitorar o tráfego de rede para uma assinatura particular, você deve permitir a assinatura. À revelia, as assinaturas as mais críticas são permitidas quando você instala a atualização de assinatura. Quando um ataque é detectado que combine uma assinatura permitida, o sensor gerencie um alerta, que seja armazenado na loja do evento do sensor. Os alertas, assim como outros eventos, podem ser recuperados da loja do evento por clientes com base na Web. À revelia, o sensor registra todos os alertas informativos ou mais altamente.

Algumas assinaturas têm subassinaturas. Isto é, a assinatura é dividida em subcategorias. Quando você configura uma subassinatura, as mudanças feitas aos parâmetros de uma subassinatura aplicam-se somente a essa subassinatura. Por exemplo, se você edita a subassinatura 1 da assinatura 3050 e muda a severidade, a mudança da severidade aplica-se somente à subassinatura 1 e não à 3050 2, 3050 3, e 3050 4.

# Assinaturas do acordo

A + o ícone indicam que mais opções estão disponíveis para este parâmetro. Clique **+** ícone para expandir a seção e para ver os parâmetros remanescente.

Um ícone verde indica que o parâmetro usa atualmente o valor padrão. Clique o ícone verde para mudá-lo ao vermelho, que ativa o campo do parâmetro assim que você pode editar o valor.

## Procedimento Passo a Passo

Termine estas etapas a fim ajustar assinaturas:

1. Entre ao IDM usando uma conta com privilégios do administrador ou do operador.
2. Escolha a **configuração > a definição da assinatura > a configuração da assinatura**.A placa da configuração da assinatura aparece.
3. A fim encontrar uma assinatura, escolha uma opção de classificação do **seleto pela** lista.Por exemplo, se você procura por uma assinatura da inundação UDP, escolha o **protocolo L2/L3/L4** e então as **inundações UDP**.A placa da configuração da assinatura refresca e indica somente aquelas assinaturas que combinam seus critérios de classificação.

4. A fim ajustar uma assinatura existente, selecione a assinatura e termine estas etapas:O clique **edita** para abrir a caixa de diálogo da assinatura da edição.Reveja os valores de parâmetro e mude o valor de todo o parâmetro que você quiser ajustar.**Nota:** A fim escolher mais de uma ação do evento, mantenha a chave **CTRL**.Sob o estado, escolha **sim** permitir a assinatura.**Nota:** A assinatura deve ser permitida para que o sensor detecte ativamente o ataque especificado pela assinatura.Sob o estado, especifique se esta assinatura é aposentada. Clique **não** para ativar a assinatura. Isto coloca a assinatura no motor.**Nota:** Uma assinatura deve ser ativada para que o sensor detecte ativamente o ataque especificado pela assinatura.**Nota:** Clique o **cancelamento** a fim desabotoar suas mudanças e fechar a caixa de diálogo da assinatura da edição.Clique em **OK**.A assinatura editada aparece agora na lista com o tipo grupo ao ajustado.**Nota:** Se você quer desabotoar suas mudanças, clique a **restauração**.
5. O clique **aplica-se** para aplicar suas mudanças e para salvar a configuração revisada.

## Informações Relacionadas

- Cisco Intrusion Prevention System
- Suporte Técnico e Documentação - Cisco Systems