O endereço IP está bloqueado ou na lista negra pela inteligência de segurança de um sistema Cisco FireSIGHT

Contents

Introduction

O recurso Security Intelligence permite especificar o tráfego que pode atravessar a rede com base no endereço IP de origem ou de destino. Isso é especialmente útil se você quiser fazer uma lista negra - negar tráfego para e de - endereços IP específicos, antes que o tráfego seja submetido a análise pelas regras de controle de acesso. Este documento descreve como lidar com situações em que um endereço IP está sendo bloqueado ou listado em negrito por um Cisco FireSIGHT System.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre o Cisco FireSIGHT Management Center.

Componentes Utilizados

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

- Cisco FireSIGHT Management Center
- Cisco Firepower Appliance

- Módulo Cisco ASA com Firepower (SFR)
- Versão do software 5.2 ou posterior

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.

Diferença entre o feed de inteligência e a lista de inteligência

Há duas maneiras de usar o recurso de inteligência de segurança em um sistema FireSIGHT:

Feed de inteligência de segurança

Um feed de Inteligência de Segurança é uma coleção dinâmica de endereços IP que o Centro de Defesa faz o download de um servidor HTTP ou HTTPS. Para ajudá-lo a criar listas negras, a Cisco fornece o *Security Intelligence Feed*, que representa endereços IP determinados pela Equipe de Pesquisa de Vulnerabilidade (VRT) para ter uma reputação ruim.

Lista de inteligência de segurança

Uma lista de inteligência de segurança, ao contrário de um feed, é uma lista estática simples de endereços IP que você carrega manualmente no FireSIGHT Management Center.

O endereço IP legítimo está bloqueado ou na lista negra

Verifique se um endereço IP está no feed Security Intelligence

Se um endereço IP estiver sendo bloqueado pela lista negra do Security Intelligence Feed, você pode seguir as etapas abaixo para verificar isso:

Passo 1: Acesse o CLI do dispositivo Firepower ou módulo de serviço.

Passo 2: Execute o seguinte comando. Substitua **<IP_Address>** pelo endereço IP que você deseja procurar:

```
admin@Firepower:~$ grep
```

Por exemplo, se desejar pesquisar o endereço IP 198.51.100.1, execute o seguinte comando:

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

Se esse comando retornar qualquer correspondência para o endereço IP que você forneceu, ele indica que o endereço IP está presente na lista negra do Security Intelligence Feed.

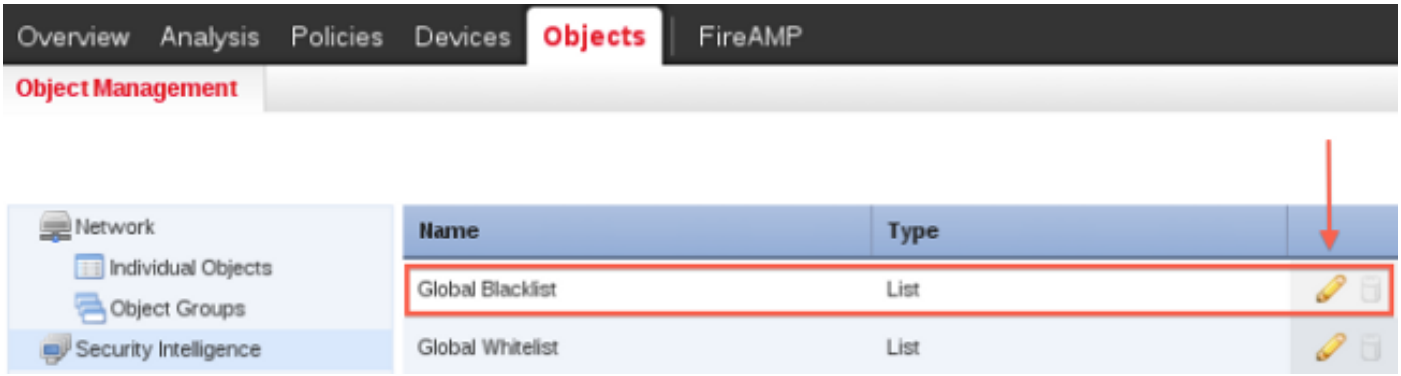
Verifique a lista negra

Para encontrar uma lista dos endereços IP que podem estar na lista negra, siga as etapas abaixo:

Passo 1: Acesso à interface da Web do FireSIGHT Management Center.

Passo 2: Navegue até **Objects > Object Management > Security Intelligence**.

Passo 3: Clique no ícone *do lápis* para abrir ou editar a **lista negra global**. Uma janela pop-up com uma lista de endereços IP é exibida.



Trabalhe com um endereço IP bloqueado ou com lista negra

Se um determinado endereço IP for bloqueado ou listado na lista negra pelo Security Intelligence Feed, você poderá considerar qualquer uma das seguintes opções para permitir isso.

Opção 1: Listas brancas de inteligência de segurança

Você pode fazer uma lista branca de um endereço IP que está na lista negra da Security Intelligence. Uma lista branca substitui sua lista negra. O sistema FireSIGHT avalia o tráfego com um endereço IP de origem ou de destino listado em branco usando regras de controle de acesso, mesmo se um endereço IP também estiver na lista negra. Portanto, você pode usar uma lista branca quando uma lista negra ainda é útil, mas tem um escopo muito amplo e bloqueia incorretamente o tráfego que você deseja inspecionar.

Por exemplo, se um feed respeitável bloquear incorretamente seu acesso a um recurso vital, mas for útil para sua organização, você poderá listar somente os endereços IP classificados incorretamente, em vez de remover todo o feed da lista negra.

> **Caution**: Depois de fazer qualquer alteração em uma política de controle de acesso, você deve reaplicar a política aos dispositivos gerenciados.

Opção 2: Aplique o filtro de inteligência de segurança por zona de segurança

Para obter granularidade adicional, você pode aplicar a filtragem de inteligência de segurança com base no endereço IP de origem ou de destino em uma conexão que reside em uma determinada zona de segurança.

Para estender o exemplo da lista branca acima, você pode listar os endereços IP classificados

incorretamente, mas depois restringir o objeto da lista branca usando uma zona de segurança usada por aqueles na sua organização que precisam acessar esses endereços IP. Dessa forma, somente aqueles com uma necessidade de negócios podem acessar os endereços IP da lista branca. Como outro exemplo, talvez você queira usar um feed de spam de terceiros para listar o tráfego em uma zona de segurança de servidor de e-mail.

Opção 3: Monitorar, em vez de lista negra

Se você não tiver certeza se deseja colocar uma lista negra em um determinado endereço IP ou conjunto de endereços, poderá usar uma configuração "somente monitor", que permite que o sistema passe a conexão correspondente às regras de controle de acesso, mas também registre a correspondência na lista negra. Observe que não é possível definir a lista negra global como somente monitoramento

Considere um cenário em que você deseja testar um feed de terceiros antes de implementar o bloqueio usando esse feed. Quando você define o feed como somente monitoramento, o sistema permite que conexões que teriam sido bloqueadas sejam analisadas pelo sistema, mas também registra um registro de cada uma dessas conexões para sua avaliação.

Etapas para configurar a inteligência de segurança com a configuração "somente monitor":

1. Na guia **Security Intelligence** em uma política de controle de acesso, clique no ícone de registro. A caixa de diálogo Opções da lista negra é exibida.
2. Marque a caixa de seleção **Log Connections** para registrar eventos de início de conexão quando o tráfego atender às condições de Security Intelligence.
3. Especifique para onde enviar eventos de ligação.
4. Clique em **OK** para definir as opções de registro. A guia Security Intelligence é exibida novamente.
5. Click **Save**. Você deve aplicar a política de controle de acesso para que as alterações entrem em vigor.

Opção 4: Entre em contato com o Centro de assistência técnica da Cisco

Você pode sempre entrar em contato com o Cisco Technical Assistance Center se:

- Você tem dúvidas sobre as opções 1, 2 ou 3 acima.
- Você deseja mais pesquisas e análises sobre um endereço IP que esteja na lista negra da Security Intelligence.
- Você quer uma explicação do motivo pelo qual o endereço IP está na lista negra da Security Intelligence.