

Configurar a lista negra de IP ao usar a inteligência de segurança da Cisco por meio do ASDM (On-Box Management, gerenciamento integrado)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Resumo do feed de inteligência de segurança](#)

[Adicionar manualmente endereços IP à lista negra global e à lista branca global](#)

[Crie a lista personalizada de endereços IP da lista negra](#)

[Configurar a inteligência de segurança](#)

[Implante a política de controle de acesso](#)

[Monitoramento de eventos da inteligência de segurança](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a reputação do Cisco Security Intelligence/IP Address e a configuração da lista negra de IP (Blocking) ao usar a alimentação personalizada/automática de endereço IP de baixa reputação.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conhecimento do dispositivo FirePOWER

Note: A filtragem de Inteligência de Segurança requer uma licença de Proteção.

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 555-X) executando a versão de software 6.0.0 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

O Cisco Security Intelligence consiste em várias coleções regularmente atualizadas de endereços IP que são determinados como tendo uma reputação ruim pela equipe do Cisco TALOS. A equipe do Cisco TALOS determina a baixa reputação se qualquer atividade mal-intencionada for originada desses endereços IP, como spam, malware, ataques de phishing, etc.

O feed do Cisco IP Security Intelligence rastreia o banco de dados de invasores, Bogon, Bots, CnC, Dga, ExploitKit, Malware, Open_proxy, Open_relay, Phishing, Response, Spam, Suspeito. O módulo Firepower oferece a opção de criar o feed personalizado de endereço IP de baixa reputação.

Resumo do feed de inteligência de segurança

Aqui estão mais algumas informações sobre o tipo de coleções de endereços IP que podem ser classificadas como categorias diferentes na Inteligência de segurança.

Invasores: Coleta de endereços IP que estão continuamente procurando vulnerabilidades ou tentando explorar outros sistemas.

Malware: Coleta de endereços IP que estão tentando propagar malware ou estão atacando ativamente qualquer um que os visita.

Phishing: Coleção de hosts que estão tentando ativamente enganar os usuários finais para que eles digitem informações confidenciais, como nomes de usuário e senhas.

Spam: Coleção de hosts que foram identificados como a origem do envio de mensagens de e-mail de spam.

Bots: Coleção de hosts que estão participando ativamente como parte de um botnet e estão sendo controlados por um controlador bot net conhecido.

CnC: Coleção de hosts que foram identificados como os servidores de controle de uma botnet conhecida.

OpenProxy: Coleção de hosts conhecidos por executar os Open Web Proxies e oferecer serviços anônimos de navegação na Web.

OpenRelay: Coleção de hosts conhecidos por oferecer serviços de retransmissão de e-mail

anônimos usados por invasores de spam e phishing.

TorExitNode: Coleção de hosts conhecidos por oferecer serviços de nó de saída para a rede Tor Anonymizer.

Bogon: Coleta de endereços IP que não estão alocados, mas estão enviando tráfego.

Suspeito: Coleta de endereços IP que estão exibindo atividade suspeita e estão sob investigação ativa.

Resposta: Coleta de endereços IP que foram repetidamente observados envolvidos no comportamento suspeito ou mal-intencionado.

Adicionar manualmente endereços IP à lista negra global e à lista branca global

O módulo Firepower permite adicionar determinados endereços IP à lista negra global quando você sabe que eles fazem parte de alguma atividade mal-intencionada. Os endereços IP também podem ser adicionados à lista branca global se você quiser permitir o tráfego para determinados endereços IP bloqueados por endereços IP da lista negra. Se você adicionar algum endereço IP à lista negra global/lista branca global, ele entrará em vigor imediatamente sem a necessidade de aplicar a política.

Para adicionar o endereço IP à lista negra global/ lista branca global, navegue para **Monitoring > ASA FirePOWER Monitoring > Real Time Event**, passe o mouse sobre os eventos da conexão e selecione **View Details**.

Você pode adicionar o endereço IP origem ou destino à lista negra global/ lista branca global. Clique no botão **Editar** e selecione **Whitelist Now/Blacklist Now** para adicionar o endereço IP à respectiva lista, como mostrado na imagem.

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

+ All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter
Rule Action=Allow *

Pause Refresh Rate 5 seconds 1/25/16 9:11:25 AM (IST)

Receive Times	Action	First Packet	Last Packet	Reason
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	1/25/16 9:07:03 AM	1/25/16 9:07:03 AM	
1/25/16 9:07:07 AM	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Initiator		Responder		Edit
Initiator IP	192.168.20.3	Responder IP	10.106.44.55	
Initiator Country and Continent	not available	Responder Country and Continent	not available	
Source Port/ICMP Type	60297	Destination Port/ICMP	49153	

Whitelist Now
Blacklist Now

Para verificar se o endereço IP origem ou destino é adicionado à lista global-negra/ lista branca global, navegue para **Configuração > Configuração do ASA Firepower > Gerenciamento de objetos > Inteligência de segurança > Listas de rede e feeds** e edite lista negra global/ lista branca global. Você também pode usar o botão excluir para remover qualquer endereço IP da lista.

Crie a lista personalizada de endereços IP da lista negra

O Firepower permite criar uma lista de endereços IP/de rede personalizada que pode ser usada na lista negra (bloqueio). Há três opções para fazer isso:

1. Você pode gravar os endereços IP em um arquivo de texto (um endereço IP por linha) e carregar o arquivo no Firepower Module. Para carregar o arquivo, navegue até **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** e clique em **Add Network Lists and Feeds** Nome: Especifique o nome da lista Personalizada. Digite: Selecione **Lista** na lista suspensa. Carregar lista: Escolha **Procurar** para localizar o arquivo de texto no sistema. Selecione a opção **Upload** para carregar o arquivo.
2. Você pode usar qualquer banco de dados IP de terceiros para a lista personalizada para a qual o módulo Firepower entra em contato com o servidor de terceiros para buscar a lista de endereços IP. Para configurar isso, navegue até **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** e clique em **Add Network Lists and Feeds**

Nome: Especifique o nome do feed personalizado.

Digite: Selecione a opção **Feed** na lista suspensa.

URL do feed: Especifique o URL do servidor ao qual o módulo Firepower deve se conectar e baixar o feed.

URL MD5: Especifique o valor de hash para validar o caminho da URL do feed.

Frequência de atualização: Especifique o intervalo de tempo no qual o sistema se conecta ao servidor de feed de URL.

The image displays two screenshots of the ASA FirePOWER configuration interface, specifically the 'Security Intelligence for Network List / Feed' dialog box. The top screenshot shows the configuration for a 'List' type feed. The 'Name' field is set to 'Custom_Feed', the 'Type' is 'List', and the 'Upload List' field contains the path 'C:\fakepath\Custom_IP_Feed.'. The bottom screenshot shows the configuration for a 'Feed' type feed. The 'Name' field is set to 'Custom_Network_Feed', the 'Type' is 'Feed', the 'Feed URL' is 'http://192.168.30.1/blacklist-IP.txt', the 'MD5 URL' is '(optional)', and the 'Update Frequency' is set to '30 minutes'. Both screenshots show a list of existing feeds on the left, including 'Cisco-Intelligence-Feed', 'Custom_Feed', 'Global-Blacklist', and 'Global-Whitelist'. The interface includes buttons for 'Update Feeds', 'Add Network Lists and Feeds', 'Upload', 'Browse...', 'Store ASA FirePOWER Changes', and 'Cancel'.

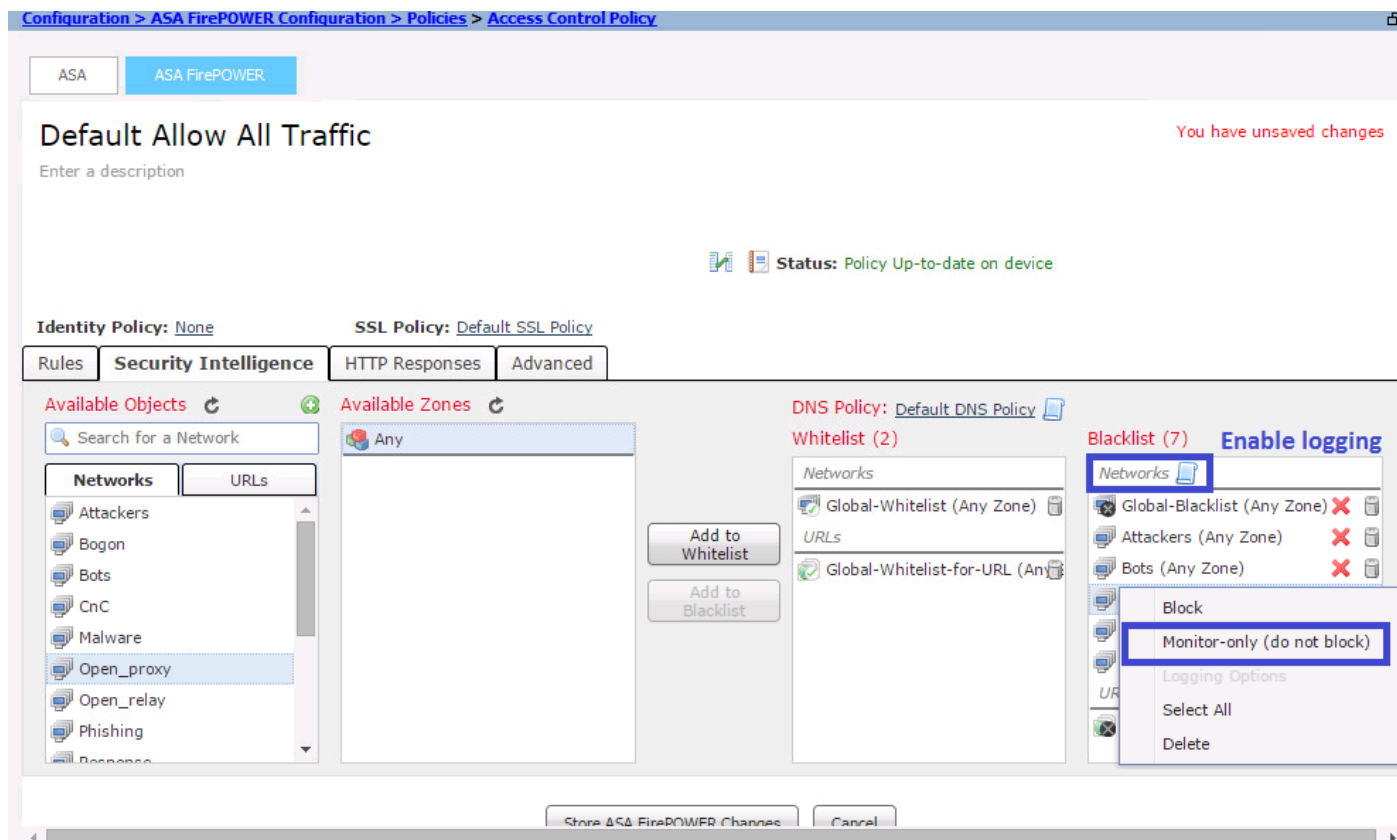
Configurar a inteligência de segurança

Para configurar a inteligência de segurança, navegue para **Configuração > Configuração do ASA Firepower > Políticas > Política de controle de acesso**, selecione a guia **Inteligência de segurança**.

Escolha o feed da coluna Network Available Object (Objeto disponível na rede), vá para **Whitelist/Blacklist** para permitir/bloquear a conexão com o endereço IP mal-intencionado.

Você pode clicar no ícone e ativar o registro conforme especificado na imagem.

Se você apenas quiser gerar o evento para conexões IP mal-intencionadas em vez de bloquear a conexão, clique com o botão direito do mouse no feed, escolha **Monitor-only (não bloquear)**, como mostrado na imagem:

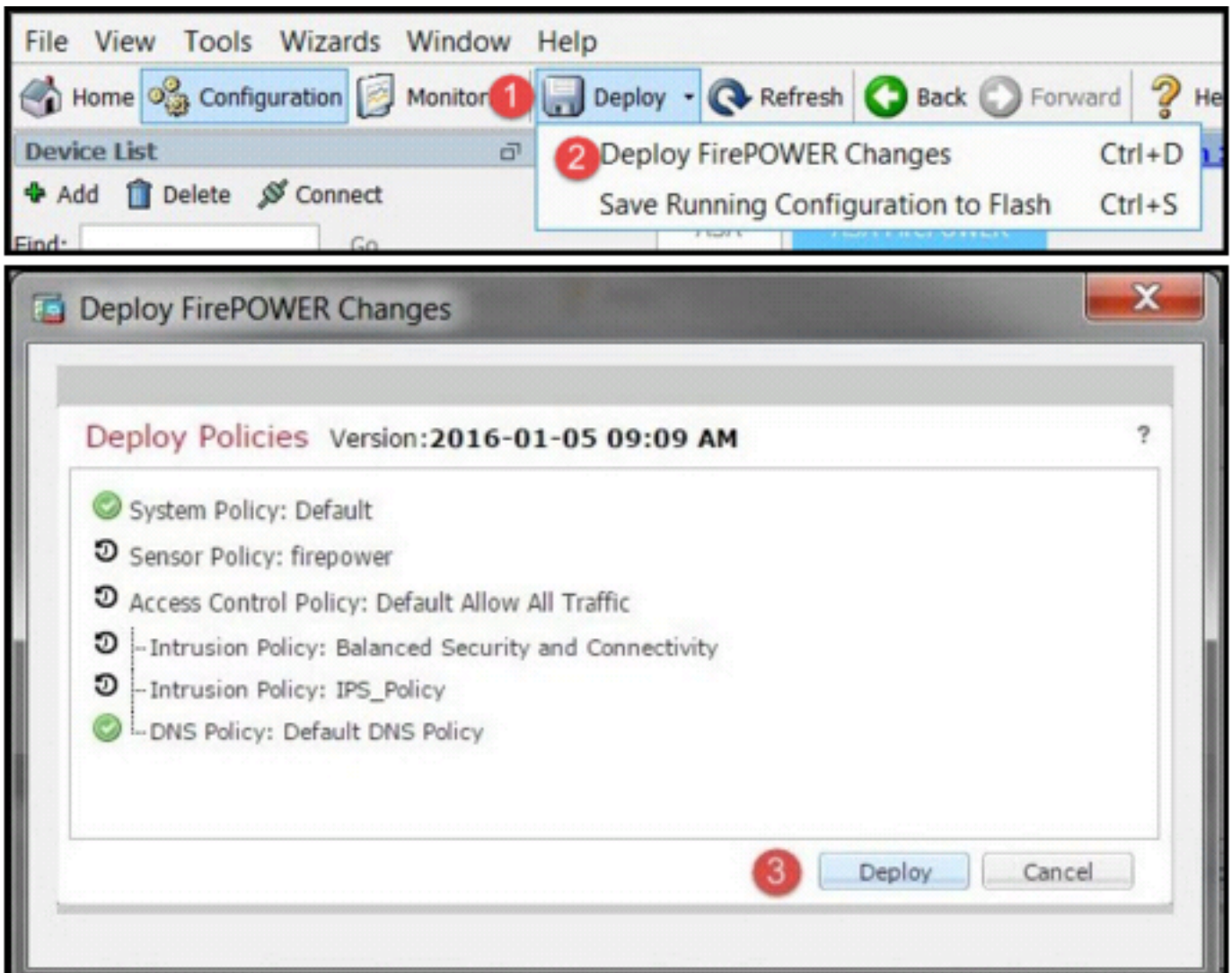


Escolha a opção Store ASA Firepower Changes para salvar as alterações da política de CA.

Implante a política de controle de acesso

Para que as alterações entrem em vigor, você deve implantar a política de controle de acesso. Antes de aplicar a política, consulte uma indicação de que a Política de controle de acesso está desatualizada no dispositivo ou não.

Para implantar as alterações no sensor, clique em **Implantar** e escolha **Implantar alterações do FirePOWER** e selecione **Implantar** na janela pop-up para implantar as alterações.

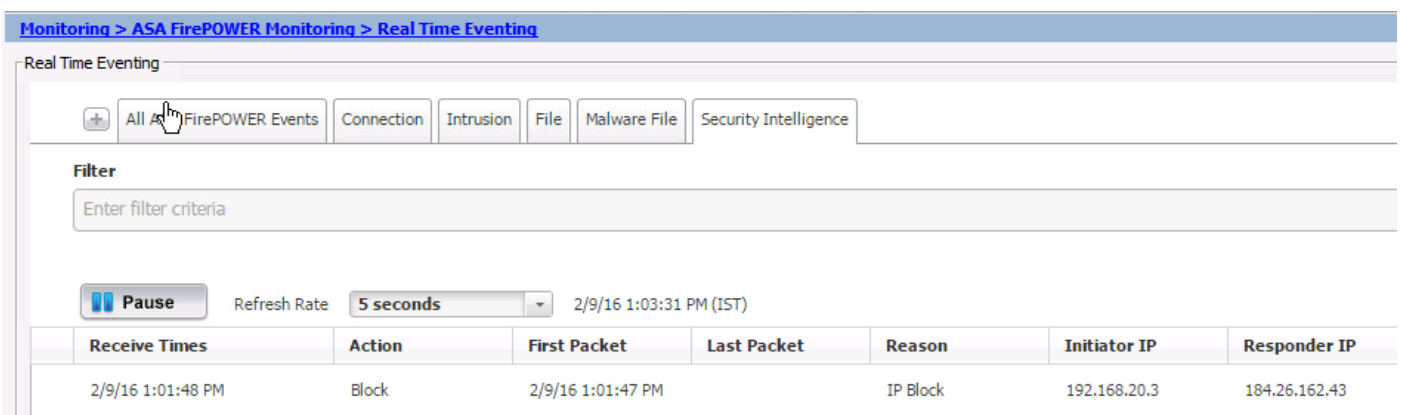


Nota: Na versão 5.4.x, para aplicar a política de acesso ao sensor, clique em **Aplicar alterações do ASA FirePOWER**

Note: Navegue até **Monitoring > ASA Firepower Monitoring > Task Status**. Verifique se a tarefa deve ser concluída para aplicar as alterações de configuração.

Monitoramento de eventos da inteligência de segurança

Para ver a inteligência de segurança pelo módulo Firepower, navegue para **Monitoring > ASA Firepower Monitoring > Real Time Eventing**. Selecione a guia **Security Intelligence**. Isso mostrará os eventos como mostrado na imagem:

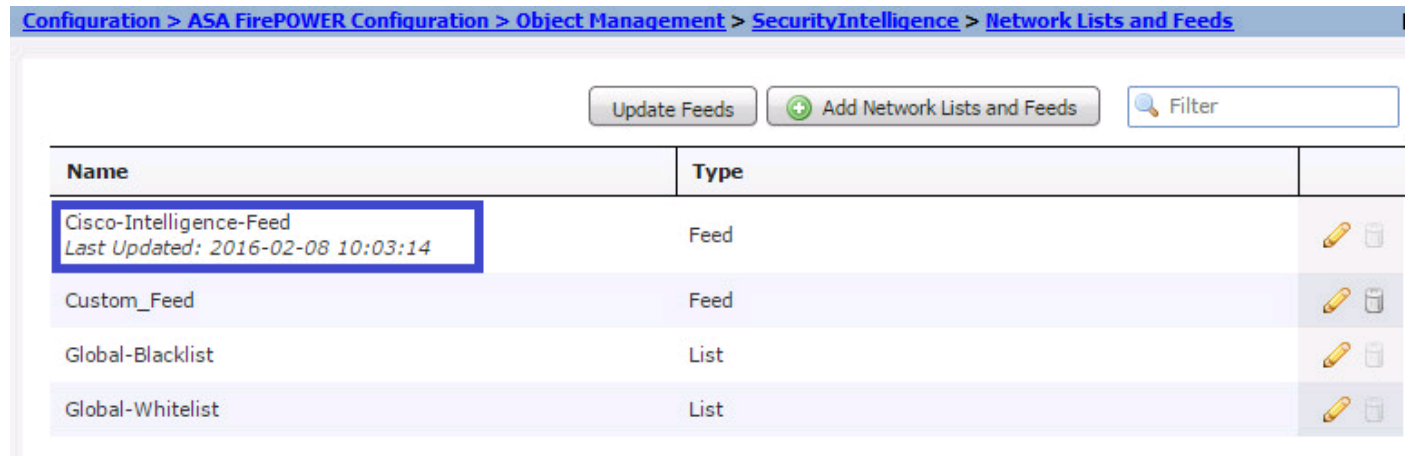


Verificar









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

Troubleshoot

Para garantir que os feeds de inteligência de segurança estejam atualizados, navegue para **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** e verifique a hora em que o feed foi atualizado pela última vez. Você pode escolher o botão Editar para definir a frequência da atualização do feed.



The screenshot shows the 'Network Lists and Feeds' configuration page. At the top, there is a breadcrumb trail: [Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds](#). Below the breadcrumb, there are three buttons: 'Update Feeds', 'Add Network Lists and Feeds', and a search box labeled 'Filter'. The main content is a table with the following data:

Name	Type	
Cisco-Intelligence-Feed <i>Last Updated: 2016-02-08 10:03:14</i>	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

Verifique se a implantação da política de controle de acesso foi concluída com êxito.

Monitore a inteligência de segurança para ver se o tráfego está bloqueando ou não.

Informações Relacionadas

- [Guia de início rápido do módulo Cisco ASA FirePOWER](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)