Configurar o IP que põr ao usar a inteligência do Cisco Security com ASDM (o Gerenciamento da Em-caixa)

Índice

Introdução

Este documento descrever a reputação da inteligência/endereço IP de Um ou Mais Servidores Cisco ICM NT do Cisco Security e a configuração do IP que põr (obstrução) quando alimentação feita sob encomenda/auto da utilização do baixo endereço IP de Um ou Mais Servidores Cisco ICM NT da reputação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firewall ASA (ferramenta de segurança adaptável), ASDM (Security Device Manager adaptável)
- Conhecimento do dispositivo da potência de fogo

Nota: A filtração da inteligência de Segurança exige uma licença da proteção.

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 acima
- 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 acima

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.

Informações de Apoio

A inteligência do Cisco Security compreende de diversas coleções regularmente actualizadas dos endereços IP de Um ou Mais Servidores Cisco ICM NT que são determinados ter uma reputação deficiente pela equipe de Cisco TALOS. A equipe de Cisco TALOS determina a baixa reputação se alguma atividade mal-intencionada é originada daqueles endereços IP de Um ou Mais Servidores Cisco ICM NT tais como os Spam, o malware, os ataques etc. do phishing.

A alimentação da inteligência de Segurança IP de Cisco segue o base de dados dos atacantes, Bogon, bot, CnC, Dga, ExploitKit, malware, Open_proxy, Open_relay, phishing, resposta, Spam, suspeito. O módulo da potência de fogo fornece a opção para criar a alimentação feita sob encomenda do baixo endereço IP de Um ou Mais Servidores Cisco ICM NT da reputação.

Vista geral da alimentação da inteligência de Segurança

Está aqui um pouco mais de informação sobre o tipo de coleções do endereço IP de Um ou Mais Servidores Cisco ICM NT que podem ser classificadas como categorias diferentes na inteligência de Segurança.

Atacantes: Coleção dos endereços IP de Um ou Mais Servidores Cisco ICM NT que continuamente estão fazendo a varredura para vulnerabilidades ou estão tentando explorar outros sistemas.

Malware: Coleção dos endereços IP de Um ou Mais Servidores Cisco ICM NT que estão tentando propagar o malware ou estão atacando ativamente qualquer um que os visita.

Phishing: Coleção dos anfitriões que estão tentando ativamente enganar utilizadores finais na informação confidencial entrando como nomes de usuário e senha.

Spam: Coleção dos anfitriões que foram identificados como a fonte de enviar mensagens de Email do Spam.

Bot: A coleção dos anfitriões que estão participando ativamente como parte de um botnet, e está sendo controlada por um controlador conhecido da rede do bot.

CnC: Coleção dos anfitriões que foram identificados como os server de controlo para um Botnet conhecido.

OpenProxy: Coleção dos anfitriões que são sabidos para executar proxys da Web abertos e para oferecer serviços anônimos da navegação na web.

OpenRelay: A coleção dos anfitriões que são sabidos para oferecer o email anônimo que retransmite serviços usou-se por atacantes do Spam e do phishing.

TorExitNode: Coleção dos anfitriões que são sabidos para oferecer serviços de nó da saída para a rede de Anonymizer do Tor.

Bogon: A coleção dos endereços IP de Um ou Mais Servidores Cisco ICM NT que não são atribuídos mas estão enviando o tráfego.

Suspeito: Coleção dos endereços IP de Um ou Mais Servidores Cisco ICM NT que estão indicando a atividade suspeita e estão sob a investigação ativa.

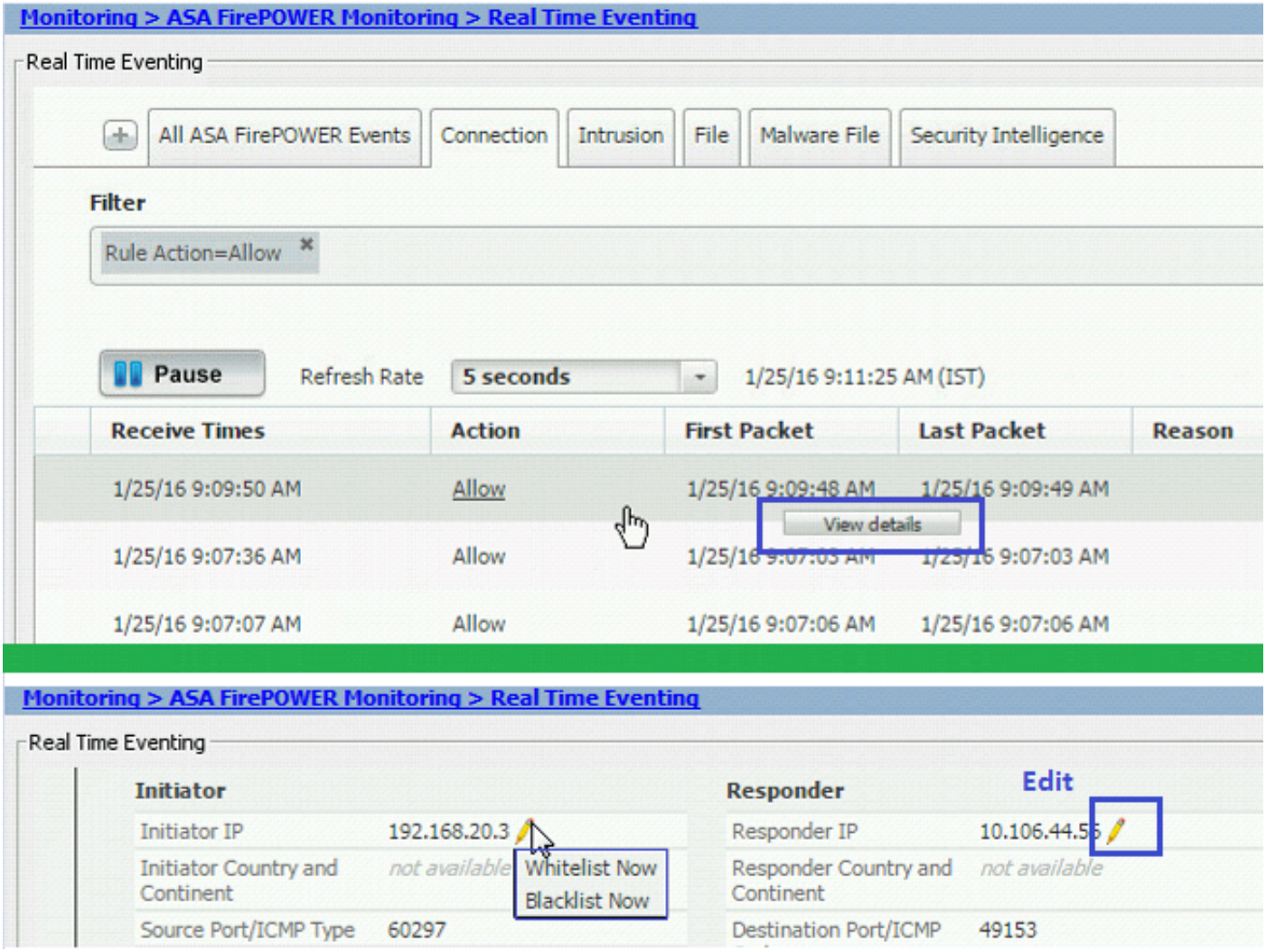
Resposta: Coleção dos endereços IP de Um ou Mais Servidores Cisco ICM NT que foram observados repetidamente contratados no comportamento suspeito ou malicioso.

Adicionar manualmente a Global-lista negra dos endereços IP de Um ou Mais Servidores Cisco ICM NT e o Global-WHITELIST

O módulo da potência de fogo permite que você adicione determinada Global-lista negra dos endereços IP de Um ou Mais Servidores Cisco ICM NT quando você sabe que são parte de alguma atividade mal-intencionada. Os endereços IP de Um ou Mais Servidores Cisco ICM NT podem igualmente ser adicionados ao Global-WHITELIST, se você quer permitir o tráfego a determinados endereços IP de Um ou Mais Servidores Cisco ICM NT que estão obstruídos por endereços IP de Um ou Mais Servidores Cisco ICM NT da lista negra. Se você adiciona qualquer Global-lista negra do endereço IP de Um ou Mais Servidores Cisco ICM NT/WHITELIST, toma o efeito imediatamente sem a necessidade de aplicar a política.

A fim adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT a Global-Blacklist/Global-WHITELIST, navegue à **monitoração > monitoração da potência de fogo ASA > tempo real Eventing**, paire o rato em eventos de conexão e selecione **detalhes da vista**.

Você pode adicionar a fonte ou o endereço IP de destino ao Global-Blacklist/Global-WHITELIST. Clique sobre o **botão Edit** e **agora** seleto de **Whitelist/lista negra agora** para adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT à lista respectiva, segundo as indicações da imagem.



A fim verificar que a fonte ou o endereço IP de destino estão adicionados ao Global-Blacklist/Global-WHITELIST, navegue à **inteligência do > segurança da configuração da configuração > da potência de fogo ASA > do Gerenciamento do objeto > Network Lists e alimente** e editem **Global-Blacklist/Whitelist global**. Você pode igualmente usar o botão Delete Button para remover todo o endereço IP de Um ou Mais Servidores Cisco ICM NT da lista.

Crie a lista feita sob encomenda de endereço IP de Um ou Mais Servidores Cisco ICM NT da lista negra

A potência de fogo permite que você crie a lista feita sob encomenda da rede/endereços IP de Um ou Mais Servidores Cisco ICM NT que pode ser usada em pôr (obstrução). Há a opção três para fazer isto:

1. Você pode escrever os endereços IP de Um ou Mais Servidores Cisco ICM NT a um arquivo de texto (um endereço IP de Um ou Mais Servidores Cisco ICM NT pela linha) e pode transferir arquivos pela rede o arquivo ao módulo da potência de fogo. A fim transferir arquivos pela rede o arquivo, navegue à **inteligência do > segurança da configuração da configuração > da potência de fogo ASA > do Gerenciamento do objeto > Network Lists e às alimentações** e clique então **adicionam listes de redes e alimentações** **Nome:** Especifique o nome da lista feita sob encomenda. **Digite:** Selecione a **lista da** lista de drop-down. **Lista da transferência de arquivo pela rede:** Escolha **consultam** para encontrar o arquivo de texto em seu sistema. Selecione a **transferência de arquivo pela rede**

da opção para transferir arquivos pela rede o arquivo.

2. Você pode usar todo o base de dados da terceira IP para a lista feita sob encomenda para que o módulo da potência de fogo contacta o server da terceira parte para buscar a lista de endereço IP. A fim configurar isto, navegue à **inteligência do > segurança da configuração da configuração > da potência de fogo ASA > do Gerenciamento do objeto > Network Lists e às alimentações** e clique então **adicionam listes de redes e alimentações**

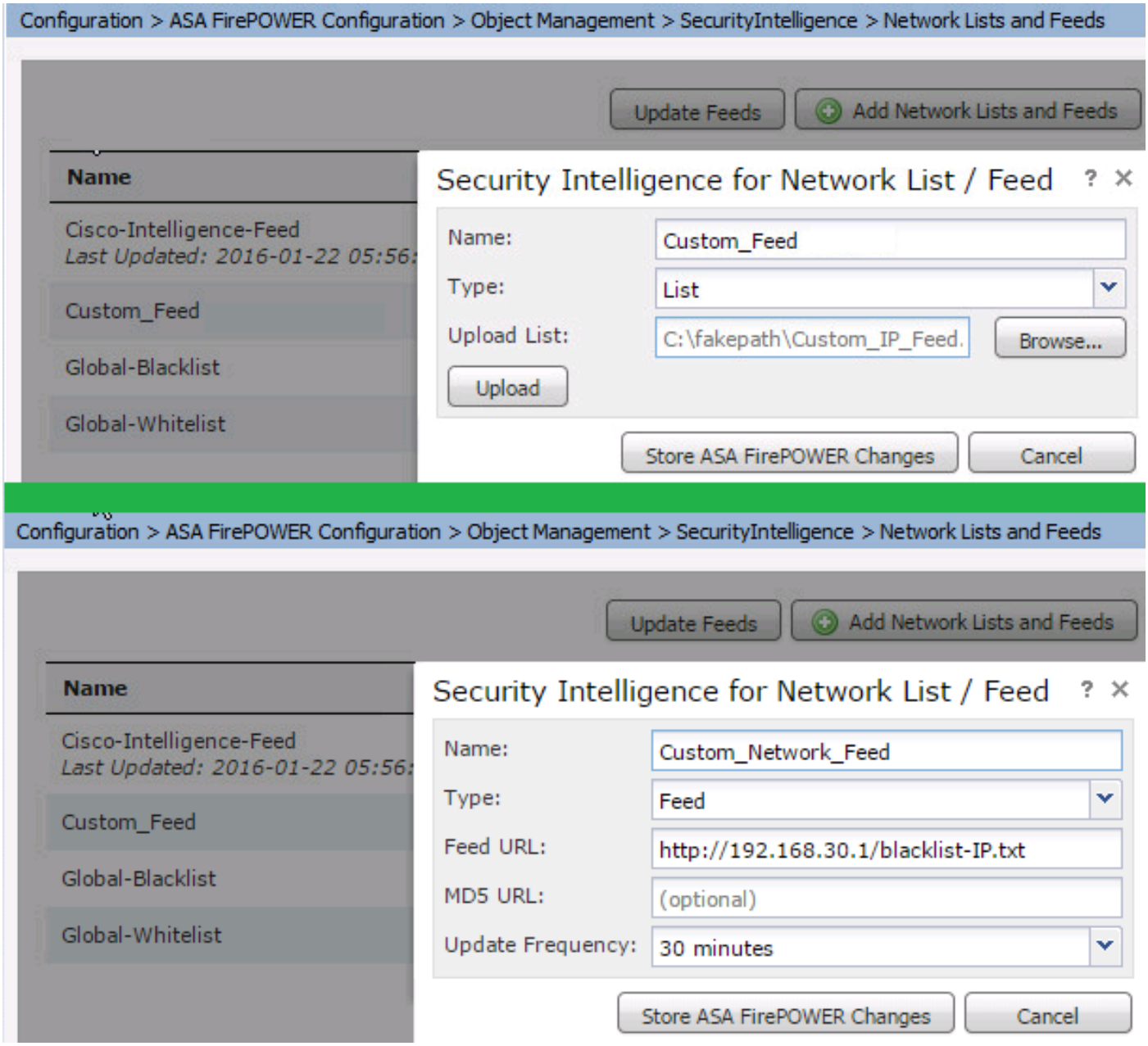
Nome: Especifique o nome da alimentação feita sob encomenda.

Digite: Alimentação seleta da opção da lista de drop-down.

Alimentação URL: Especifique a URL do server a que o módulo da potência de fogo deve conectar e transfira a alimentação.

MD5 URL: Especifique o valor de hash para validar o trajeto da alimentação URL.

Frequência da atualização: Especifique o intervalo de tempo em que o sistema conecta ao server da alimentação URL.



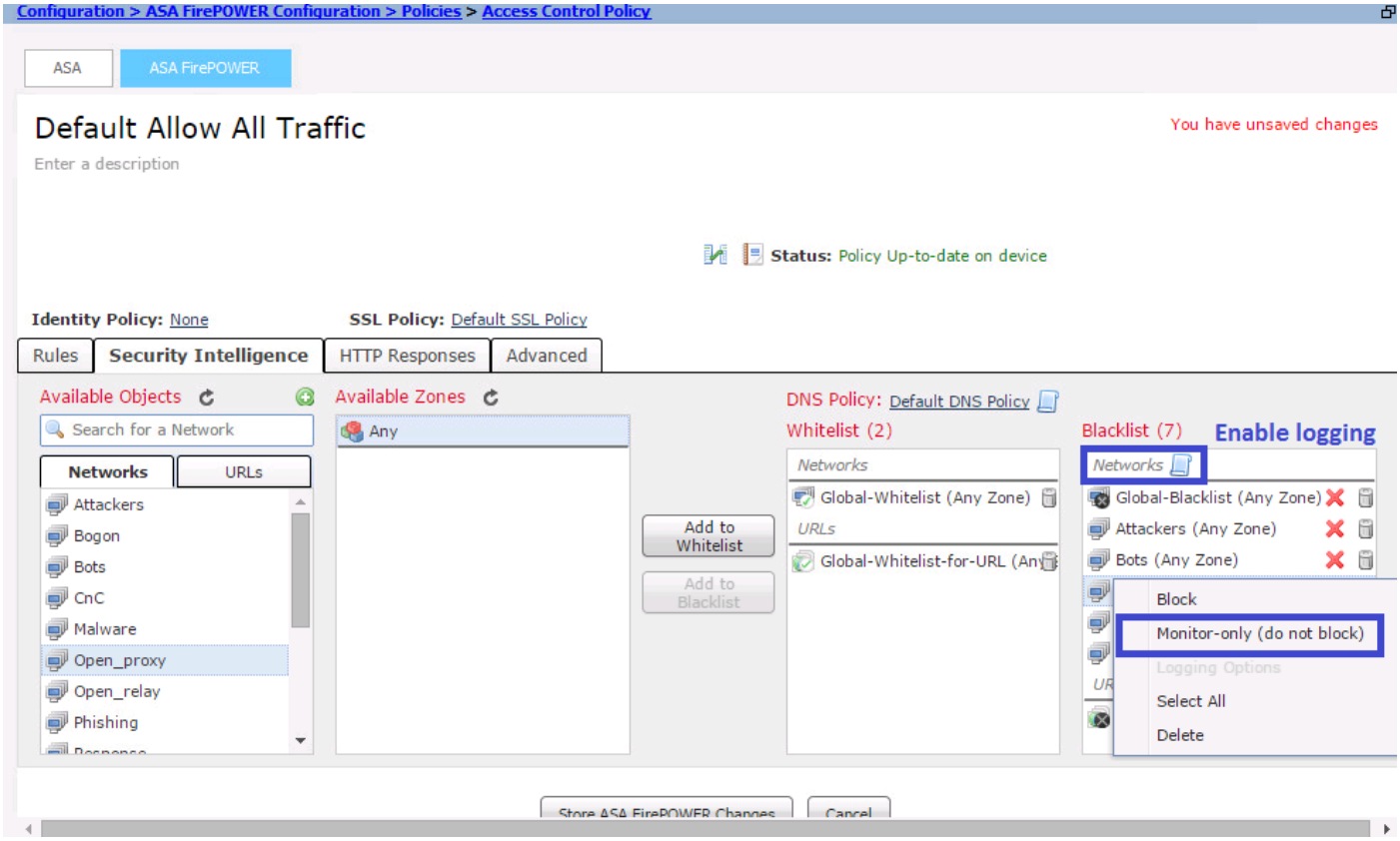
Configurar a inteligência de Segurança

A fim configurar a inteligência de Segurança, navegue à **configuração da configuração > da potência de fogo ASA > às políticas > à política do controle de acesso,** selecionam a aba da **inteligência de Segurança**.

Escolha a alimentação do objeto disponível da rede, movimento à reservar da coluna da **lista negra Whitelist**//bloco a conexão ao endereço IP de Um ou Mais Servidores Cisco ICM NT malicioso.

Você pode clicar o ícone e permitir o registro como especificado na imagem.

Se você apenas quer gerar o evento para conexões IP maliciosas em vez de obstruir a conexão, a seguir clicar com o botão direito na alimentação, escolhem o **monitor-somente (não faz o bloco)**, segundo as indicações da imagem:

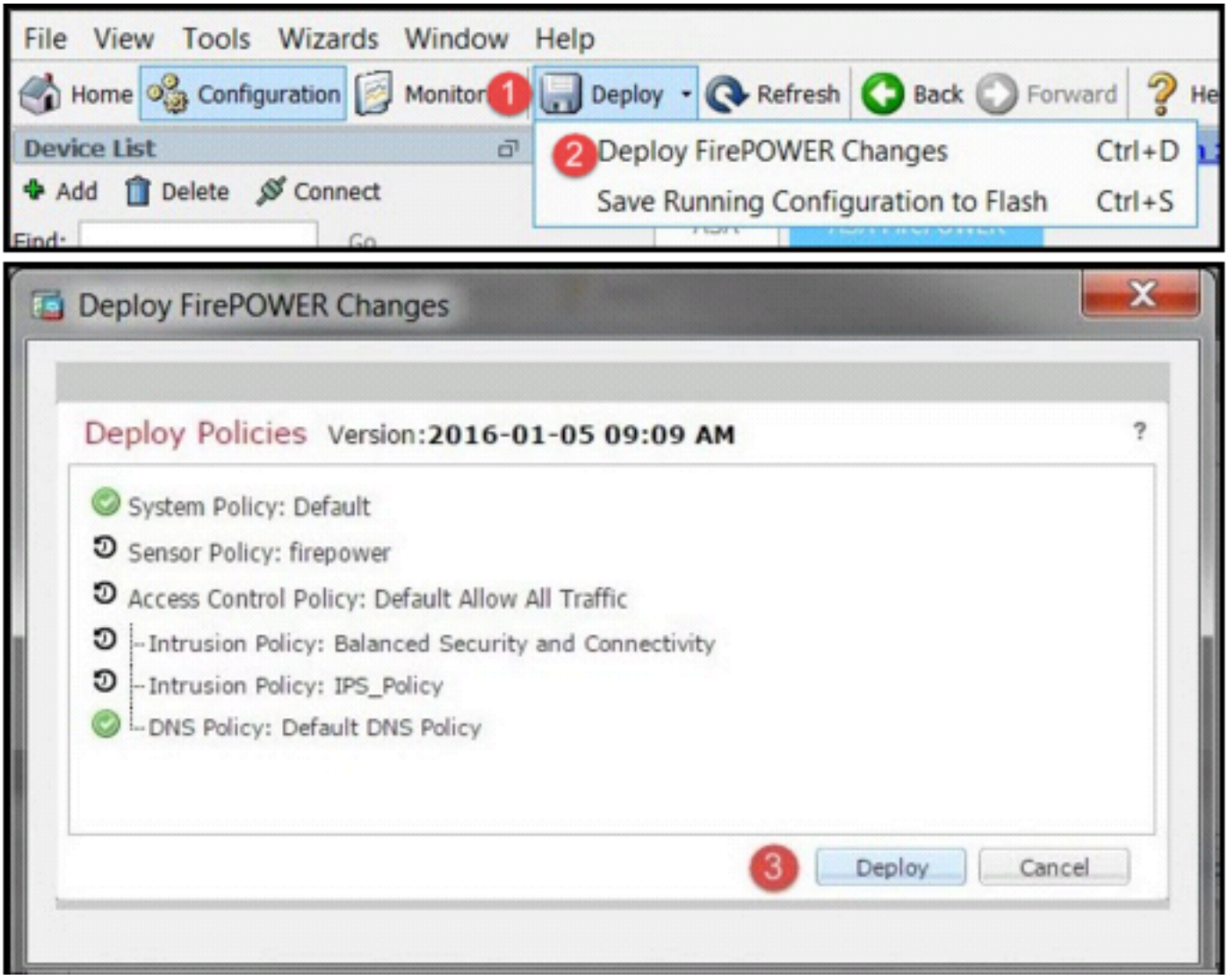


Escolha mudanças da potência de fogo da loja ASA da opção salvar as alterações de política AC.

Distribua a política do controle de acesso

Para que as mudanças tomem o efeito, você deve distribuir a política do controle de acesso. Antes que você aplique a política, veja uma indicação que se a política do controle de acesso seja expirado no dispositivo ou não.

Para distribuir as mudanças ao sensor, o clique **distribui** e escolhe **distribui mudanças da potência de fogo** a seguir seleciona-as **distribui na** janela pop-up para distribuir as mudanças.

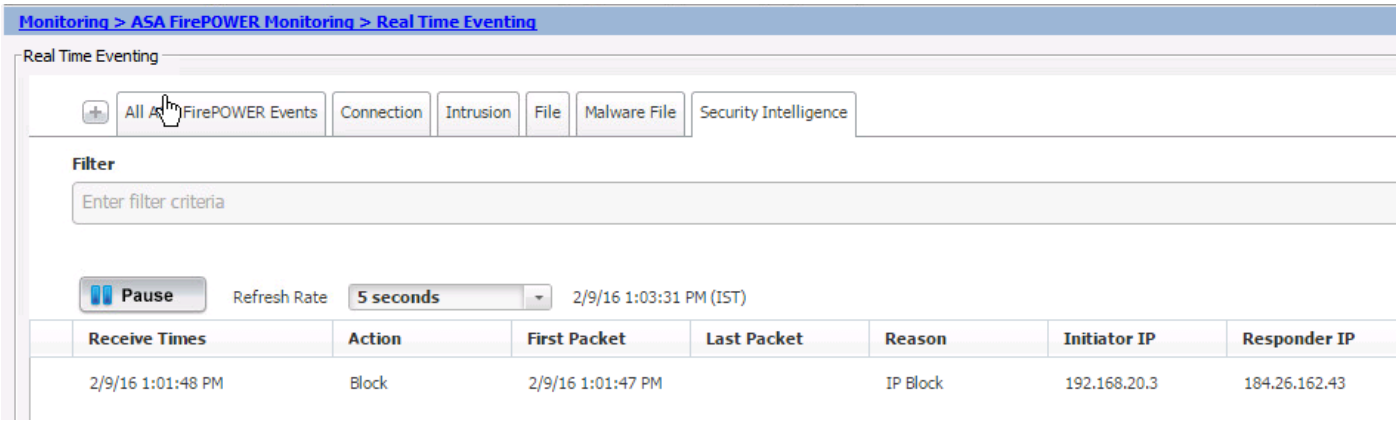


Nota: Na versão 5.4.x, para aplicar a política de acesso ao sensor, você precisa de clicar **aplica mudanças da potência de fogo ASA**

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

Monitoração dos eventos de inteligência de Segurança

A fim ver a inteligência de Segurança pelo módulo da potência de fogo, navegue à **monitoração > monitoração da potência de fogo ASA > tempo real Eventing**. Selecione a aba da **inteligência de Segurança**. Isto aparecerá os eventos segundo as indicações da imagem:

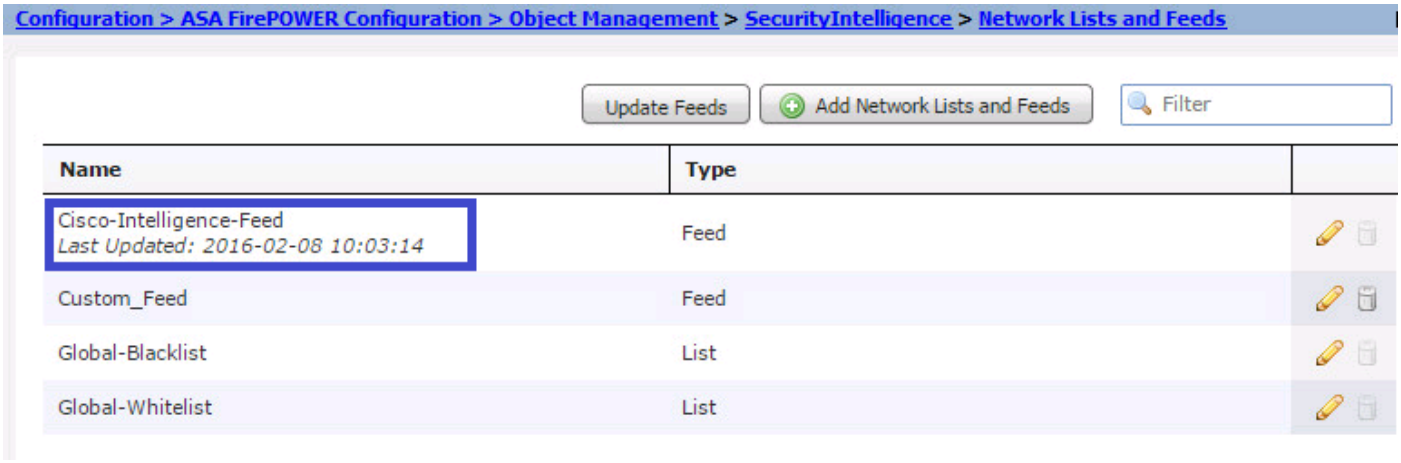


Verificar

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

Troubleshooting

A fim assegurar-se de que as alimentações da inteligência de Segurança sejam atualizadas, navegue à **inteligência do > segurança da configuração da configuração > da potência de fogo ASA > do Gerenciamento do objeto > Network Lists e alimente** e verifiquem o tempo em que a alimentação foi atualizada por último. Você pode escolher o botão Edit ajustar a frequência da atualização da alimentação.



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

Monitore a inteligência de Segurança ver se o tráfego está obstruindo ou não.

Informações Relacionadas

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