O endereço IP de Um ou Mais Servidores Cisco ICM NT é obstruído ou põr pela inteligência de Segurança de um sistema de Cisco FireSIGHT

ID do Documento: 117993

Atualizado em: outubro 21, 2015

Contribuído por Nazmul Rajib, engenheiro de TAC da Cisco.

Produtos Relacionados

- Centro de gerenciamento 750 de Cisco FireSIGHT
- Centro de gerenciamento 3500 de Cisco FireSIGHT
- Centro de gerenciamento 1500 de Cisco FireSIGHT
- Centro de gerenciamento de Cisco FireSIGHT

Índice

Introdução

A característica da inteligência de Segurança permite que você especifique o tráfego que pode atravessar seu baseado na rede na fonte ou no endereço IP de destino. Isto é especialmente útil se você quer pôr - negue o tráfego a e de - endereços IP de Um ou Mais Servidores Cisco ICM NT específicos, antes que o tráfego esteja sujeitado à análise por regras do controle de acesso. Isto documenta descreve como segurar encenações quando um endereço IP de Um ou Mais Servidores Cisco ICM NT está sendo obstruído ou pôr por um sistema de Cisco FireSIGHT.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento no centro de gerenciamento de Cisco FireSIGHT.

Componentes Utilizados

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

- Centro de gerenciamento de Cisco FireSIGHT
- Dispositivo de Cisco FirePOWER
- Cisco ASA com o módulo de FirePOWER (SFR)
- Versão de software 5.2 ou mais atrasado

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.

Diferença entre a alimentação da inteligência e a lista da inteligência

Há duas maneiras de usar a característica da inteligência de Segurança em um sistema de FireSIGHT:

Alimentação da inteligência de Segurança

Uma alimentação da inteligência de Segurança é uma coleção dinâmica dos endereços IP de Um ou Mais Servidores Cisco ICM NT que o centro da defesa transfere de um HTTP ou de um servidor HTTPS. Para ajudá-lo a construir listas negras, Cisco fornece a *alimentação da inteligência de Segurança*, que representa os endereços IP de Um ou Mais Servidores Cisco ICM NT determinados pela equipe de investigação da vulnerabilidade (VRT) ter uma reputação

deficiente.

Lista da inteligência de Segurança

Uma lista da inteligência de Segurança, contrastada com uma alimentação, é uma lista estática simples dos endereços IP de Um ou Mais Servidores Cisco ICM NT que você transfere arquivos pela rede manualmente a FireSIGHT o centro de gerenciamento.

O endereço IP legítimo é obstruído ou põr

Verifique se um endereço IP de Um ou Mais Servidores Cisco ICM NT está na alimentação da inteligência de Segurança

Se um endereço IP de Um ou Mais Servidores Cisco ICM NT está sendo obstruído pela lista negra da alimentação da inteligência de Segurança, você pode seguir as etapas abaixo para verificar este:

Passo 1: Alcance o CLI do dispositivo ou do módulo de serviço de FirePOWER.

Passo 2: Execute o comando seguinte. Substitua o `<IP_Address>` com o endereço IP de Um ou Mais Servidores Cisco ICM NT por que você quer procurar:

```
admin@Firepower:~$ grep <IP_Address> /var/sf/iprep_download/*.blf
```

Por exemplo, se você quer procurar pelo endereço IP 198.51.100.1, execute o comando seguinte:

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

Se este comando retorna qualquer fósforo para o endereço IP de Um ou Mais Servidores Cisco ICM NT que você forneceu, indica que o endereço IP de Um ou Mais Servidores Cisco ICM NT esta presente na lista negra da alimentação da inteligência de Segurança.

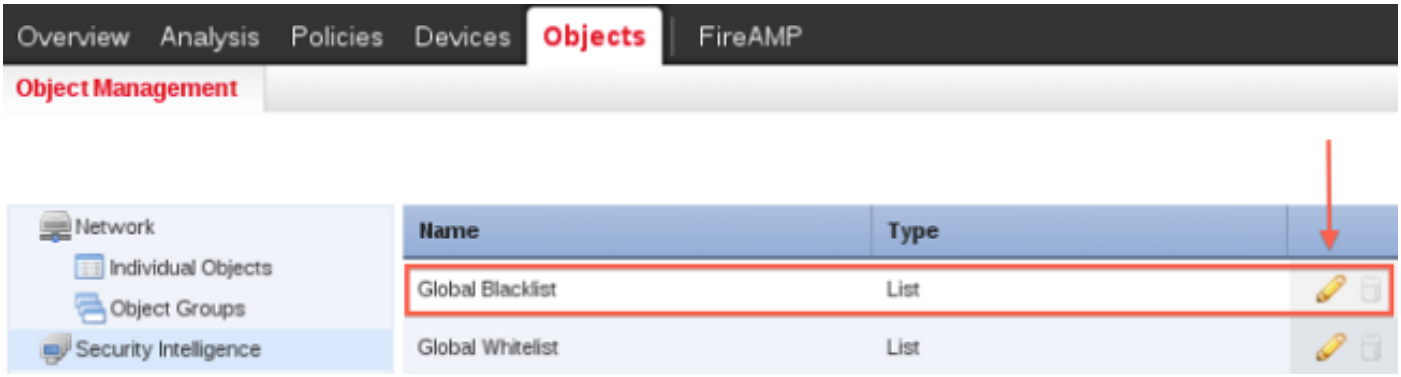
Verifique a lista negra

Para encontrar uma lista dos endereços IP de Um ou Mais Servidores Cisco ICM NT que puderam ser põr, siga as etapas abaixo:

Passo 1: Acesso à interface da WEB do centro de gerenciamento de FireSIGHT.

Passo 2: Navegue aos **objetos > à inteligência do > segurança do Gerenciamento do objeto**.

Passo 3: Clique sobre o ícone do *lápis* para abrir ou editar a **lista negra global**. Um estalo acima do indicador com uma lista de endereços IP de Um ou Mais Servidores Cisco ICM NT aparece.



Trabalho com um endereço IP de Um ou Mais Servidores Cisco ICM NT obstruído ou põr

Se um endereço IP particular é obstruído ou põr pela alimentação da inteligência de Segurança, você pode considerar algumas das seguintes opções para permiti-la.

Opção 1: Inteligência de Segurança Whitelists

Você pode whitelist um endereço IP de Um ou Mais Servidores Cisco ICM NT que seja põr pela inteligência de Segurança. Um whitelist cancela sua lista negra. O sistema de FireSIGHT avalia o tráfego com uma fonte ou um endereço IP de destino whitelisted usando regras do controle de acesso, mesmo se um endereço IP de Um ou Mais Servidores Cisco ICM NT é põr igualmente. Consequentemente, você pode usar um whitelist quando uma lista negra é ainda útil, mas é demasiado largo no espaço e obstrui incorretamente o tráfego que você quer inspecionar.

Por exemplo, se uma alimentação respeitável obstrui impropriamente seu acesso a um recurso vital mas é em geral útil a sua organização, você pode whitelist os endereços IP de Um ou Mais Servidores Cisco ICM NT impropriamente classificados somente, um pouco do que removendo a alimentação do todo da lista negra.

> **Caution**: Depois que você faz toda a mudança em uma política do controle de acesso, você deve reaplicar a política aos dispositivos gerenciado.

Opção 2: Reforce o filtro da inteligência de Segurança pela zona de Segurança

Para a granularidade adicionada, você pode reforçar a filtração da inteligência de Segurança baseada sobre se a fonte ou o endereço IP de destino em uma conexão residem em uma zona de Segurança particular.

Para estender o exemplo acima do whitelist, você poderia whitelist os endereços IP de Um ou Mais Servidores Cisco ICM NT impropriamente classificados, mas por outro lado restringir o objeto do whitelist usando uma zona de Segurança usada por aquelas em sua organização que precisam de alcançar aqueles endereços IP de Um ou Mais Servidores Cisco ICM NT. Essa maneira, somente aqueles com uma necessidade de negócio pode alcançar os endereços IP de Um ou Mais Servidores Cisco ICM NT whitelisted. Como um outro exemplo, você pôde querer usar uma alimentação da terceira do Spam para põr o tráfego em uma zona de Segurança do

servidor de e-mail.

Opção 3: Monitore, um pouco do que a lista negra

Se você não é certo se você quer pôr um endereço IP particular ou um grupo de endereços, você pode usar um ajuste do “monitor-somente”, que permita que o sistema passe a conexão de harmonização às regras do controle de acesso, mas igualmente registra o fósforo à lista negra. Note que você não pode ajustar o monitor-somente global da lista negra

Considere uma encenação onde você queira testar uma alimentação da terceira antes que você execute a obstrução usando essa alimentação. Quando você ajusta o monitor-somente da alimentação, o sistema permite as conexões que seriam obstruídas para ser analisadas mais pelo sistema, mas igualmente registra um registro de cada um daquelas conexões para sua avaliação.

Etapas para configurar a inteligência de Segurança com ajuste do “monitor-somente”:

1. Na aba da **inteligência de Segurança em uma** política do controle de acesso, clique o ícone de registro. A caixa do diálogo de opções da lista negra aparece.
2. Selecione a caixa de verificação das **conexões do log** para registrar eventos da começo--conexão quando o tráfego está conformes condições da inteligência de Segurança.
3. Especifique onde enviar eventos de conexão.
4. Clique a **APROVAÇÃO** para ajustar suas opções de registro. A aba da inteligência de Segurança aparece outra vez.
5. Click **Save**. Você deve aplicar a política do controle de acesso para que suas mudanças tomem o efeito.

Opção 4: Centro de assistência técnica da Cisco do contato

Você pode sempre contactar o centro de assistência técnica da Cisco, se:

- Você tem perguntas com as opções acima 1, 2 ou 3.
- Você quer uma pesquisa e uma análise mais adicionais em um endereço IP de Um ou Mais Servidores Cisco ICM NT que seja pôr pela inteligência de Segurança.
- Você quer uma explicação porque o endereço IP de Um ou Mais Servidores Cisco ICM NT é pôr pela inteligência de Segurança.

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: outubro 21, 2015
ID do Documento: 117993