Configurar Umbrella com Blade de Software Anti-Boot Check Point

Contents

Introdução

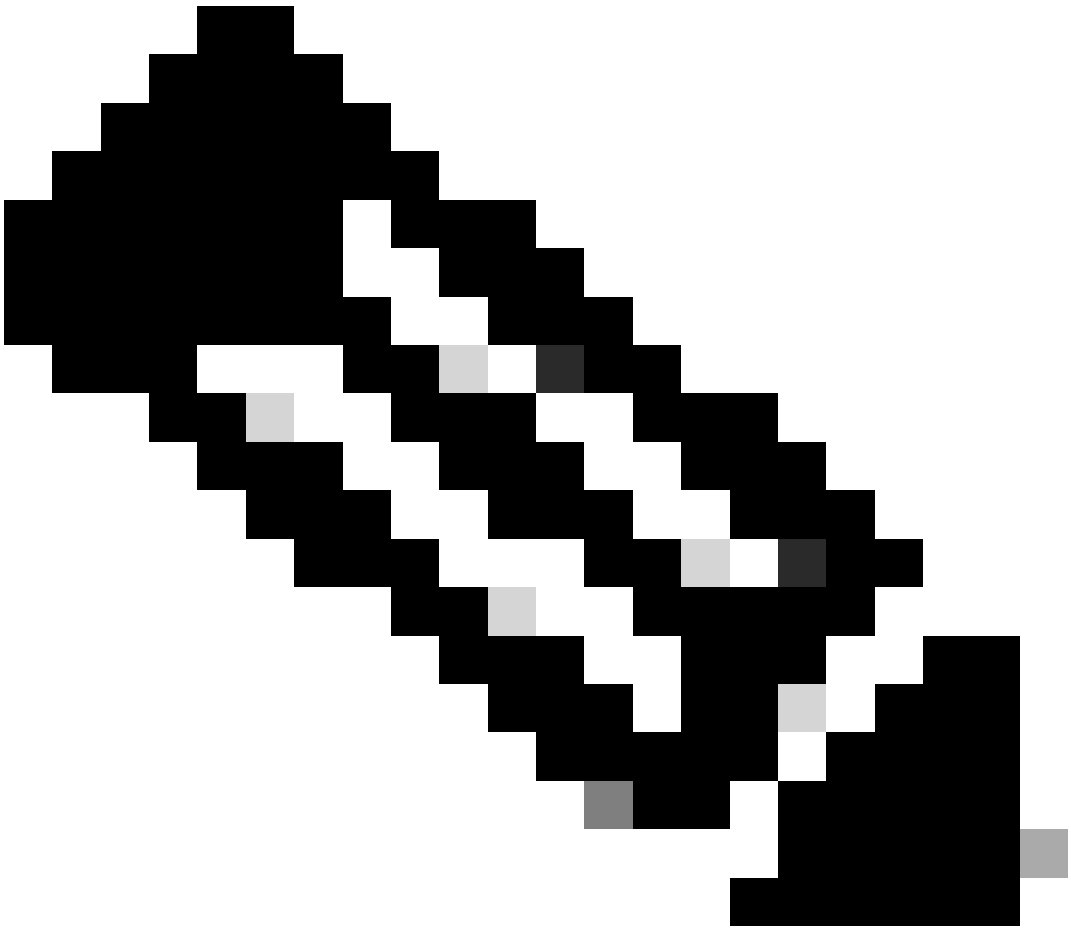
Este documento descreve como integrar o Cisco Umbrella com o Blade de Software Anti-Boot da Check Point.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Um dispositivo Check Point com lâmina de software antiboot
- Check Point versão de software R80.40 ou superior
- Certifique-se de que o dispositivo Check Point possa fazer solicitações HTTP de saída para "https://s-platform.api.opendns.com".
- Um pacote Cisco Umbrella como DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage
- Direitos administrativos do Cisco Umbrella Dashboard



Note: A integração do Check Point é incluída somente em pacotes Cisco Umbrella como DNS Essentials, DNS Advantage, SIG Essentials ou SIG Advantage. Se você não tiver um desses pacotes e quiser ter a integração do Check Point, entre em contato com seu Gerente de Contas do Cisco Umbrella. Se você tiver o pacote Cisco Umbrella correto, mas não vir o Check Point como uma integração para seu painel, entre em contato com o Suporte do Cisco Umbrella.

Componentes Utilizados

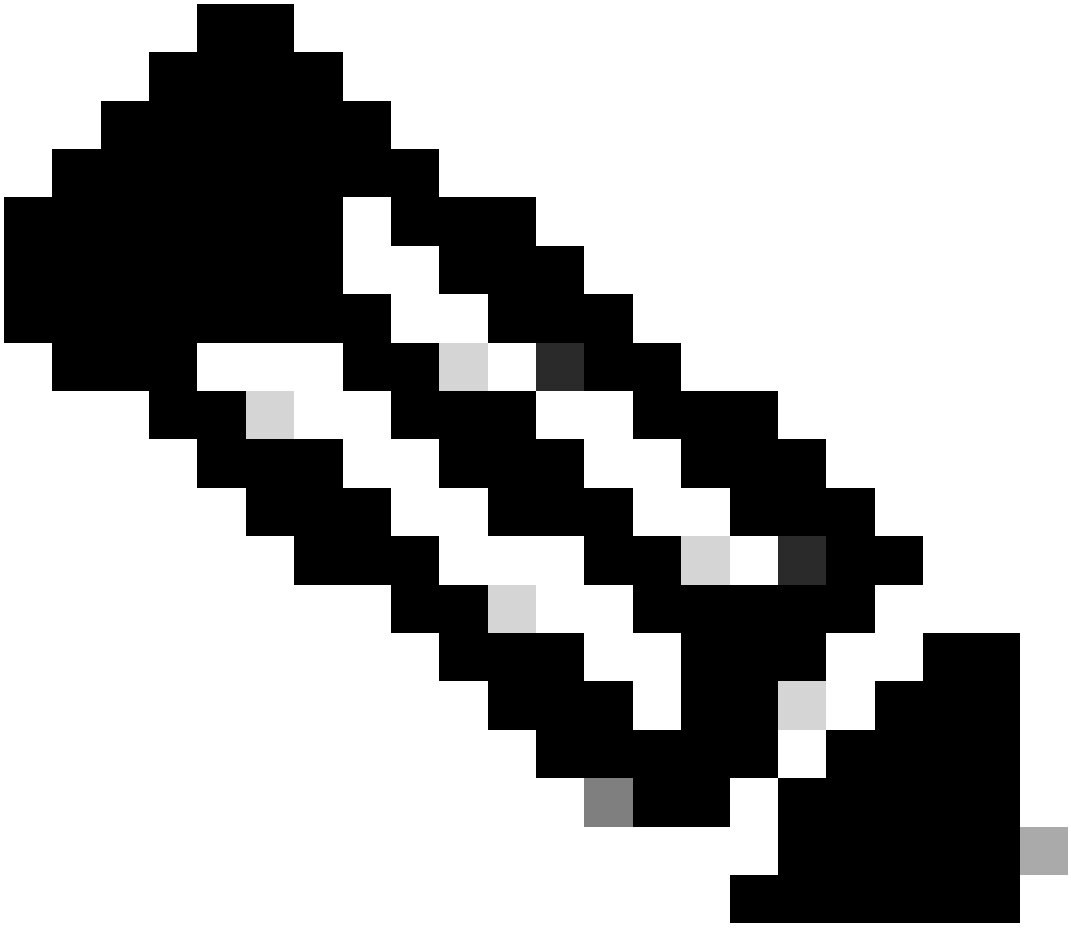
As informações neste documento são baseadas no Cisco Umbrella.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

A integração do Cisco Umbrella com o Blade de software anti-boot da Check Point permite que um dispositivo da Check Point envie seus alertas do Blade de software anti-boot para o Cisco Umbrella quando o Blade descobre ameaças no tráfego de rede que inspeciona. Os alertas recebidos pelo Cisco Umbrella criam uma lista de bloqueio que pode proteger notebooks, tablets e telefones em roaming em redes não protegidas pelo Blade de Software Anti-Boot da Check Point.

Este artigo fornece instruções para configurar um dispositivo Check Point para enviar alertas de Blade de software antiboot para o Cisco Umbrella.



Note: Esta integração foi descontinuada pela Check Point na versão R81.20 depois que foi inicialmente lançado em R80.40.

Funcionalidade

A integração do Cisco Umbrella com o dispositivo Blade de software antiboot da Check Point envia as ameaças encontradas (por exemplo, domínios que hospedam malware, comandos e controles para botnets ou sites de phishing) para o Cisco Umbrella para aplicação global.

Em seguida, o Cisco Umbrella valida a ameaça para garantir que ela possa ser adicionada a uma política. Se as informações do Blade do software de antiinicialização Check Point forem confirmadas como uma ameaça, o endereço do domínio será adicionado à lista de destino do Check Point como parte de uma configuração de segurança que pode ser aplicada a qualquer política do Cisco Umbrella. Essa política é aplicada imediatamente a todas as solicitações feitas de dispositivos atribuídos a essa política.

No futuro, o Cisco Umbrella analisa automaticamente os alertas do Check Point e adiciona sites

mal-intencionados à lista de destino do Check Point. Isso estende a proteção do Check Point a todos os usuários e dispositivos remotos e fornece outra camada de aplicação à sua rede corporativa.

Configuration Steps

A configuração da integração envolve estas etapas:

1. Habilite a integração no Cisco Umbrella para gerar um token de API com um script personalizado.
2. Implante o token de API e o script personalizado no dispositivo Check Point.
3. Criar/Editar um alerta de Ponto de Verificação para postar neste novo script.
4. Definir eventos do Check Point para serem bloqueados no Cisco Umbrella.

Evitar interrupções de serviço

Para evitar interrupções de serviço indesejadas, o Cisco Umbrella recomenda adicionar nomes de domínio de missão crítica que nunca podem ser bloqueados (por exemplo, google.com ou salesforce.com) à Lista de Permissões Global (ou outras listas de destino, de acordo com sua política) antes de configurar a integração.

Os domínios de missão crítica podem incluir:

- A página inicial da sua organização
- Domínios que representam os serviços que você fornece e que podem ter registros internos e externos. Por exemplo, "mail.myservicedomain.com" e "portal.myotherservicedomain.com".
- Os aplicativos baseados em nuvem menos conhecidos dos quais você depende não podem ser incluídos na validação automática de domínio do Cisco Umbrella. Por exemplo, "localcloudservice.com".

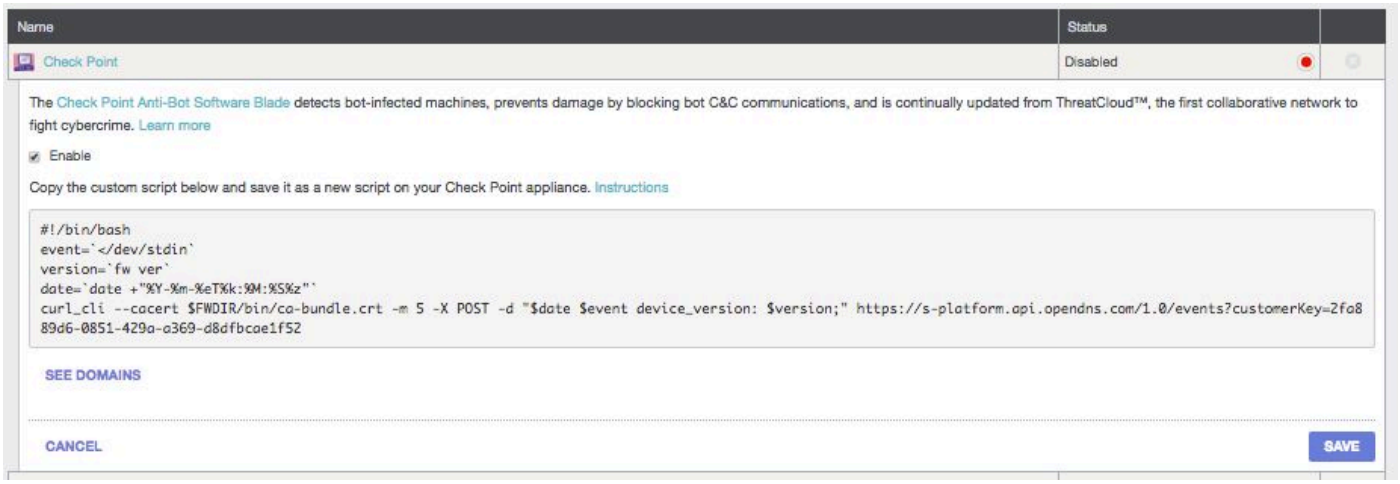
Esses domínios devem ser adicionados à Lista de permissões global, que se encontra em Políticas > Listas de destino no Cisco Umbrella.

Passo 1: Geração de script Umbrella e token API

1. Efetue login no Cisco Umbrella Dashboard como Administrador.

2. Navegue até Policies > Policy Components > Integrations e selecione Check Point na tabela para expandi-la.

3. Selecione a opção Ativar.



4. Copie o script inteiro, começando pela linha com:

```
#!/bin/bash
```

Você pode usar o script em etapas posteriores.

5. Selecione Salvar para ativar a integração.

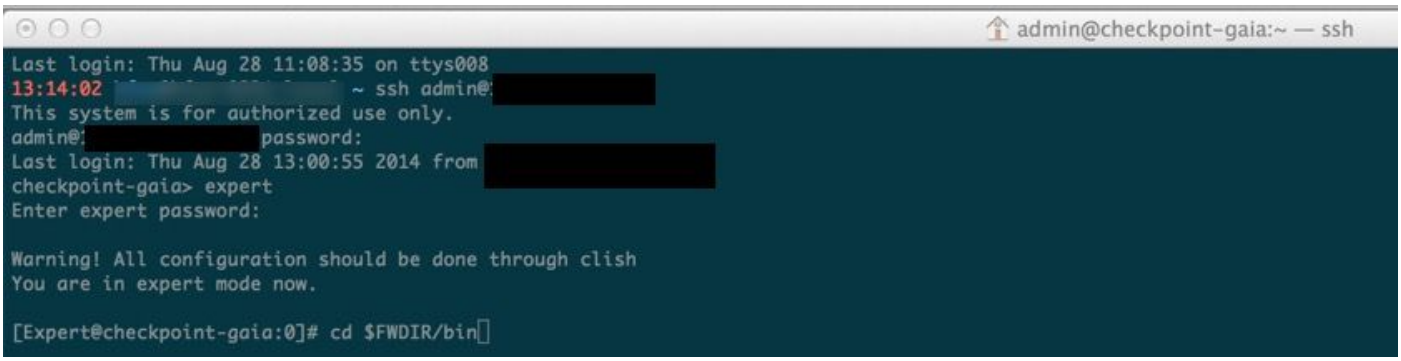
Passo 2: Implante o script personalizado no dispositivo Check Point

As próximas etapas são instalar o script personalizado do Cisco Umbrella em seu dispositivo Check Point e habilitá-lo no SmartDashboard.

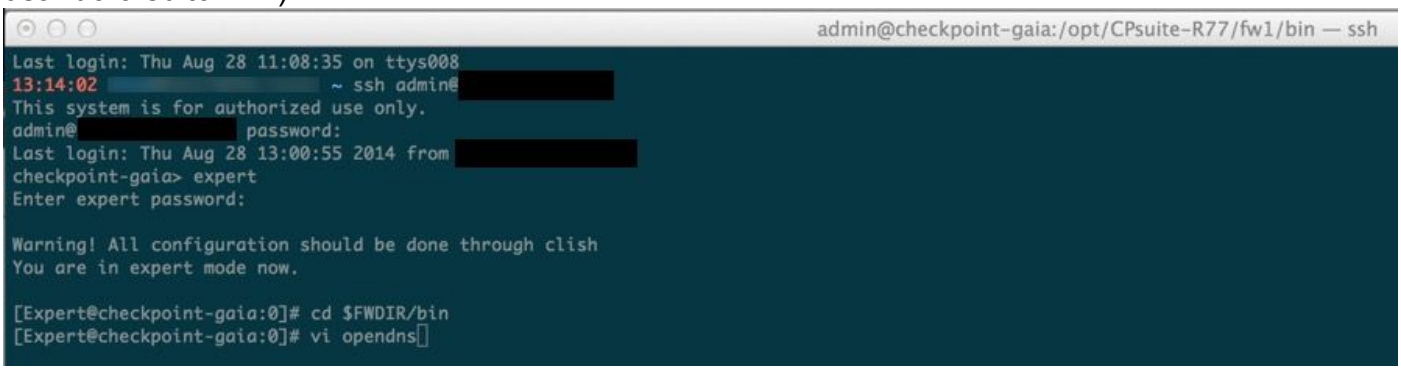
1. Para instalar o script personalizado, use SSH no Check Point Appliance como um administrador:

2. Em seguida, inicie o "Modo Especialista" digitando "expert" na linha de comando:

3. Altere o diretório de trabalho para `$FWDIR/bin`:

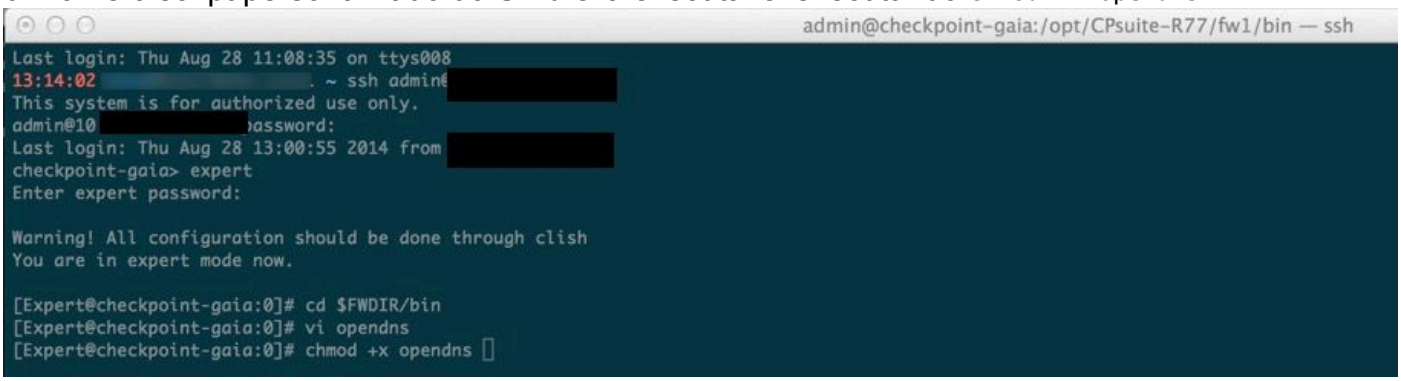


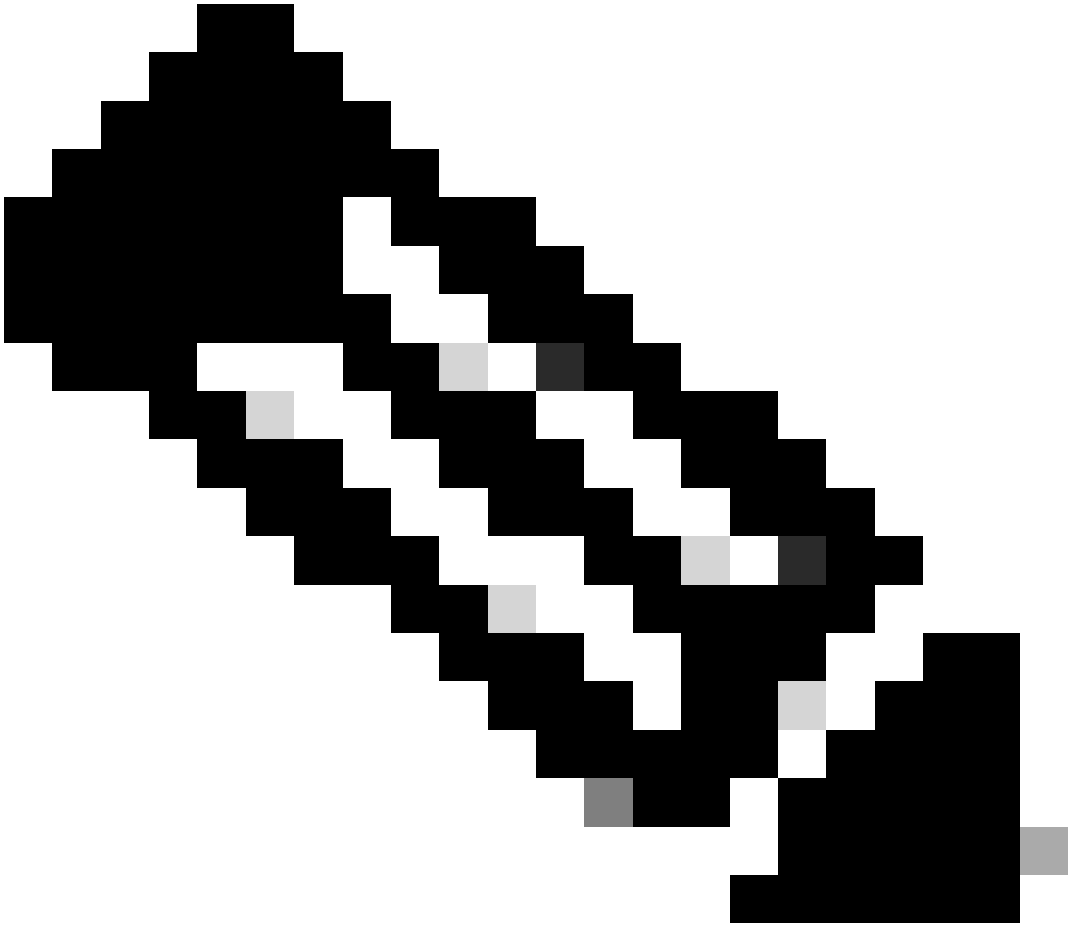
4. Abra um novo arquivo chamado "opendns" usando um editor de texto (como no exemplo aqui usando o editor "vi"):



5. Cole o script do Cisco Umbrella no arquivo, salve o arquivo e saia do editor:

6. Torne o script personalizado do Umbrella executável executando `chmod +x opendns` :



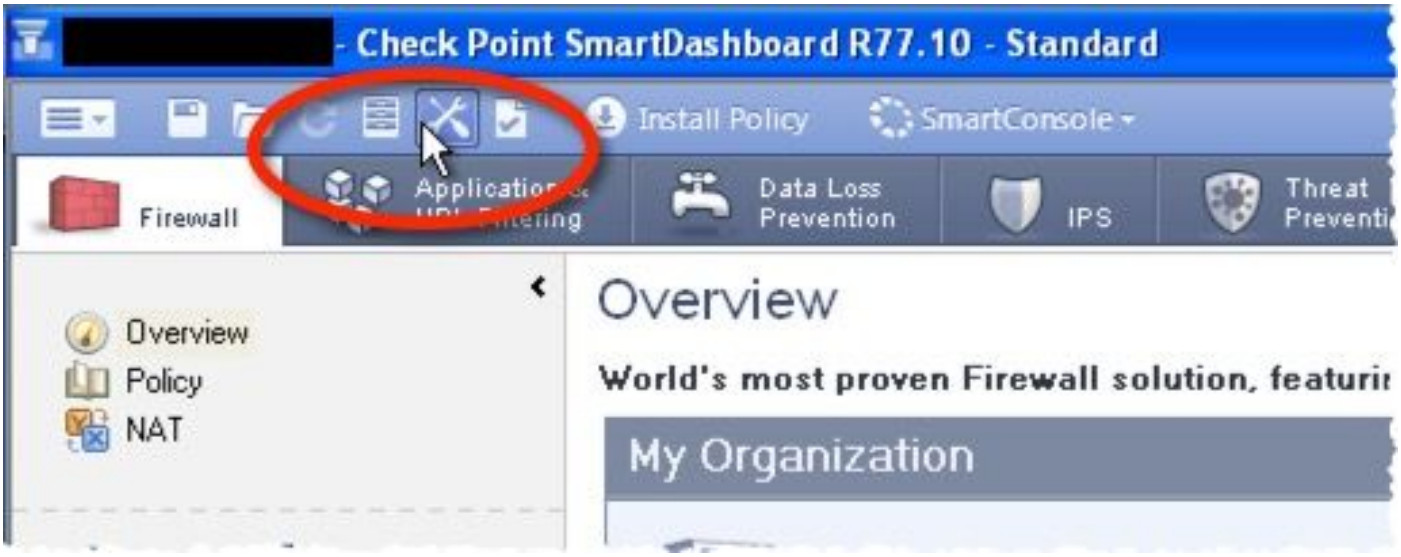


Note: Se você atualizar ou alterar versões de Blade, repita essas etapas nessa nova versão.

Etapa 3. Criar ou editar um alerta de ponto de verificação para postar no novo script

1. Ative o SmartDashboard para publicar o novo script fazendo login e iniciando o SmartDashboard:

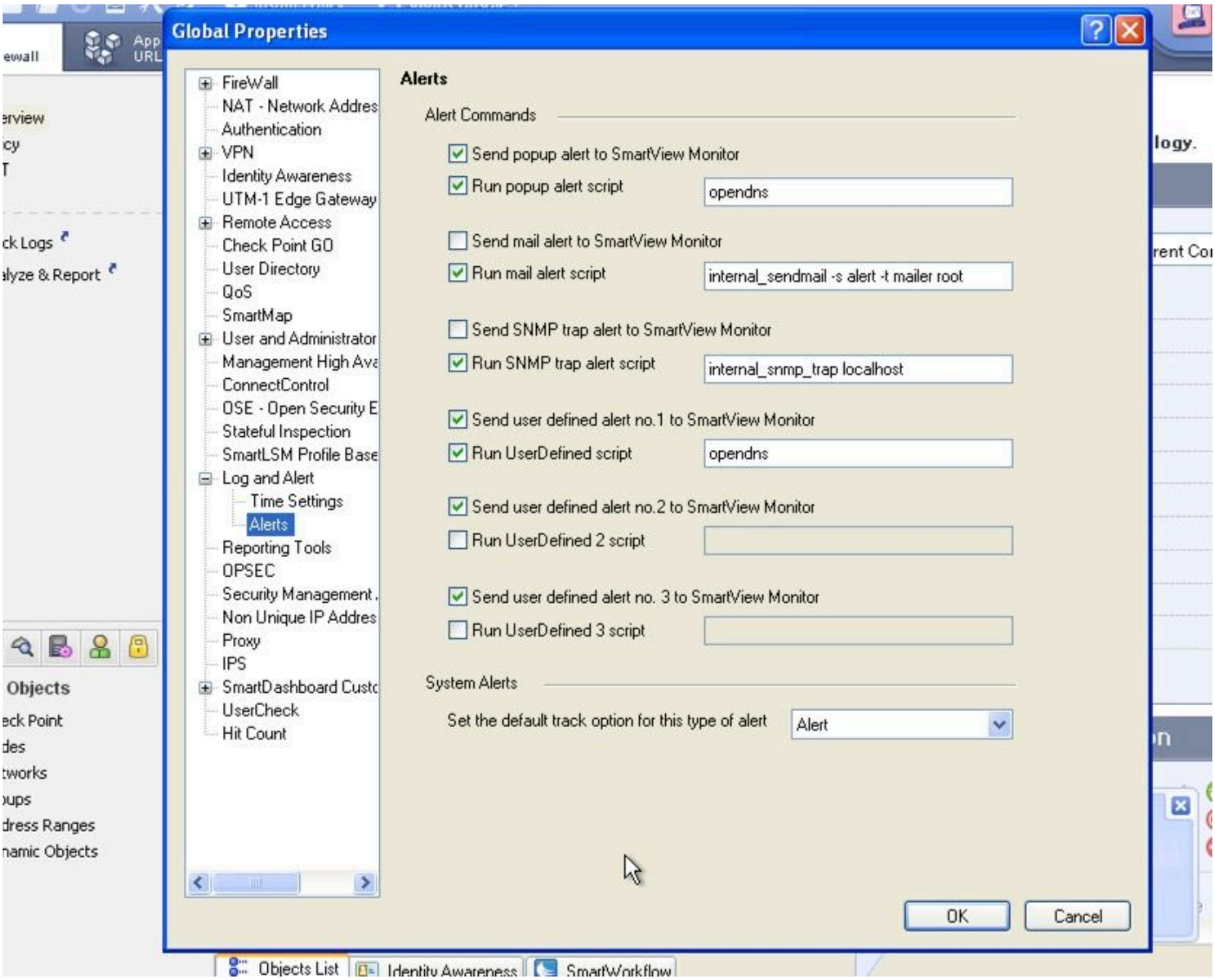
2. Abrir Propriedades Globais:



3. Em Propriedades Globais, abra Log e Alerta > Alertas e conclua estas etapas:

- Selecione Send popup alertscript e Run UserDefined script.
- Defina "aberturas" nos campos de script para ambos.

4. Selecione OK. No SmartDashboard, salve e instale a política atualizada.



Passo 4: Testando os eventos do ponto de verificação de integração e configuração a serem bloqueados

Primeiro, gere um evento de blade de teste anti-bot para ser exibido no Cisco Umbrella Dashboard:

1. Carregue este URL em seu navegador a partir de qualquer dispositivo na rede protegido pelo seu Check Point:

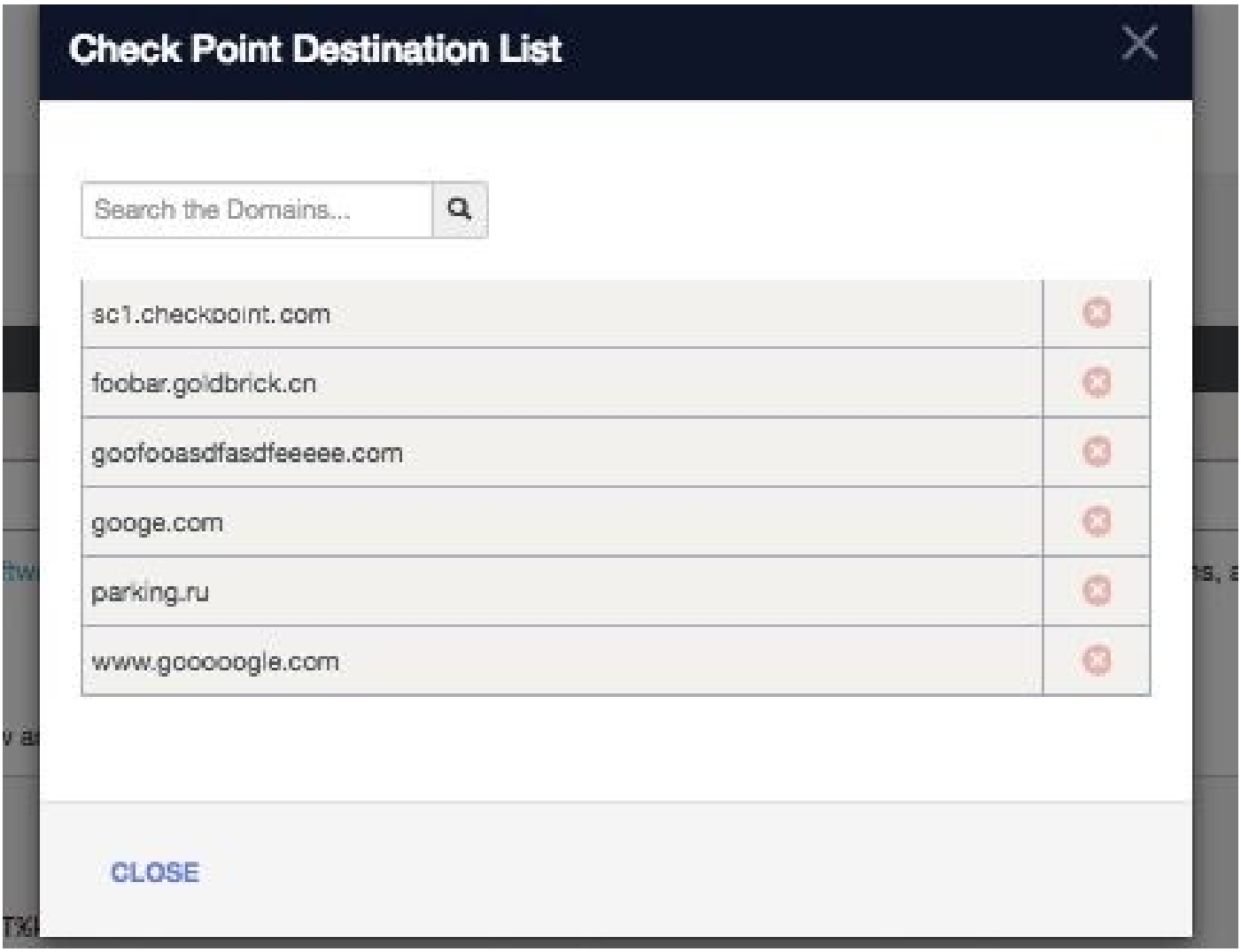
```
"http://sc1.checkpoint.com/za/images/threatwiki/pages/TestAntiBotBlade.html"
```

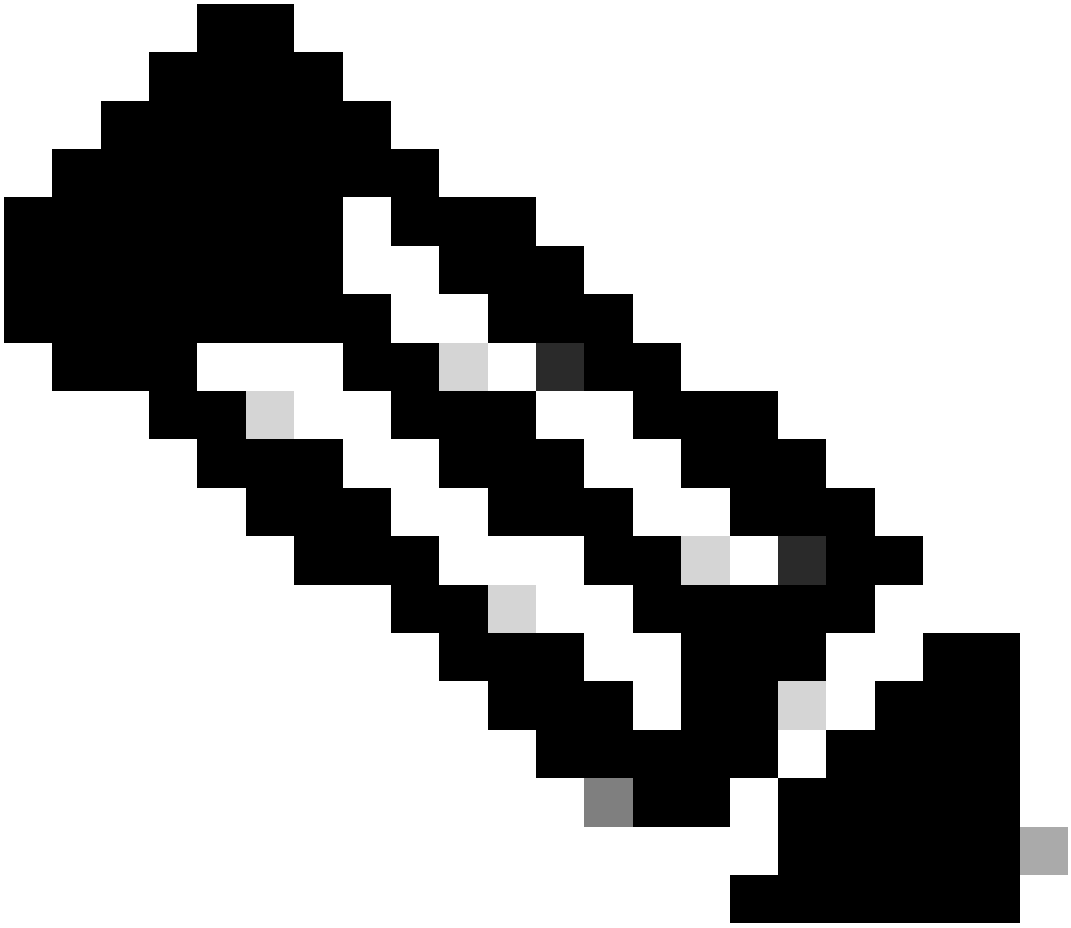
2. Efetue login no painel do Cisco Umbrella como administrador.

3. Navegue até Policies > Policy Components > Integrations e selecione Check Point na tabela para expandi-la.

4. Selecione Ver Domínios. Isso abre uma janela que exibe a lista de destino do ponto de

verificação que pode incluir "sc1.checkpoint.com". A partir desse ponto, uma lista pesquisável começa a ser preenchida e a crescer.



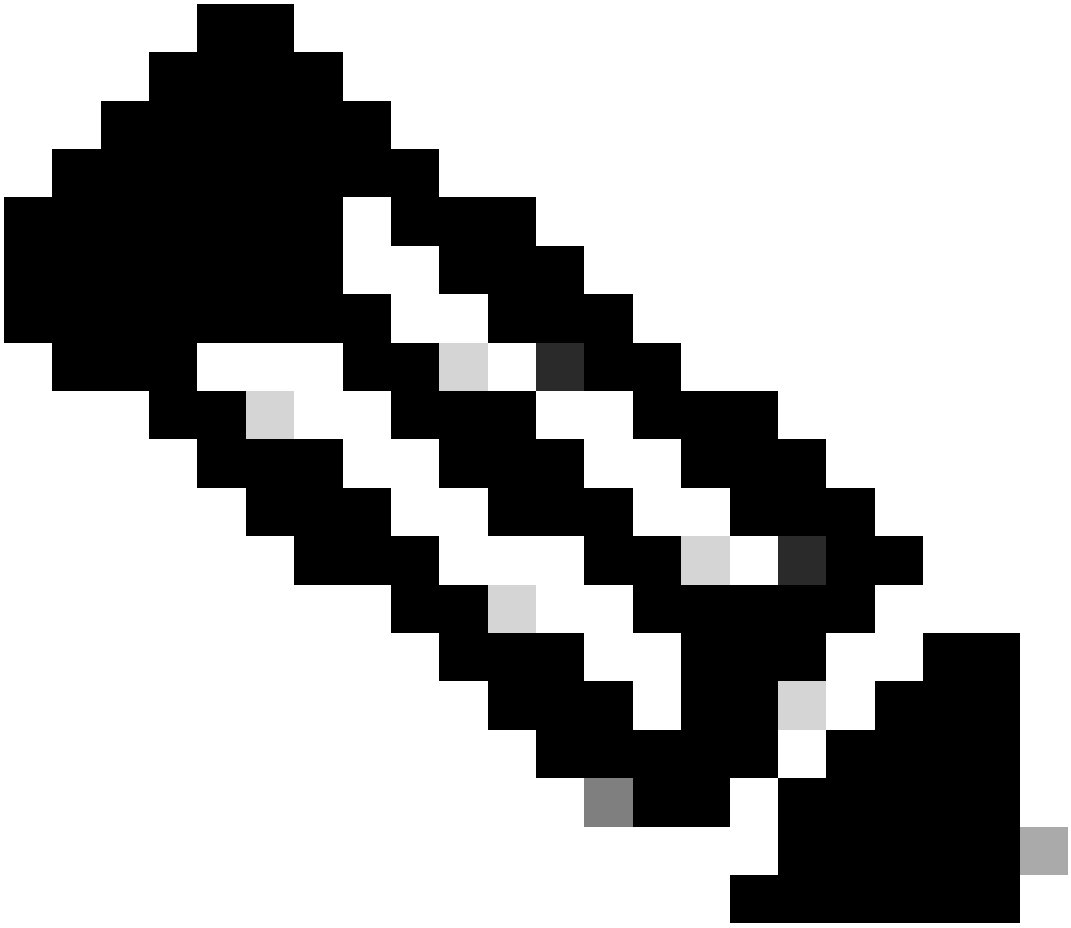


Note: Você também pode alterar essa lista de destinos se houver um domínio exibido aqui no qual você não deseja aplicar a política. Selecione o ícone Excluir para remover o domínio.

Observação de eventos adicionados à categoria de segurança Ponto de verificação em "Modo de auditoria"

A próxima etapa é observar e auditar os eventos adicionados à sua nova categoria de segurança Ponto de verificação.

Os eventos do seu dispositivo Check Point começam a preencher uma lista de destinos específica que pode ser aplicada a políticas como uma categoria de segurança Check Point. Por padrão, a lista de destino e a categoria de segurança estão no "modo de auditoria" e não são aplicadas a nenhuma política e não podem resultar em nenhuma alteração nas políticas atuais do Cisco Umbrella.



Note: O "modo de auditoria" pode ser ativado por quanto tempo for necessário, com base no perfil de implantação e na configuração da rede.

Revisar lista de destinos

Você pode rever a Lista de destinos de pontos de verificação a qualquer momento no Cisco Umbrella:

1. Navegue até Policies > Policy Components > Integrations.

2. Expanda Check Point na tabela e selecione See Domains.

Revisar Configurações de Segurança para uma Política

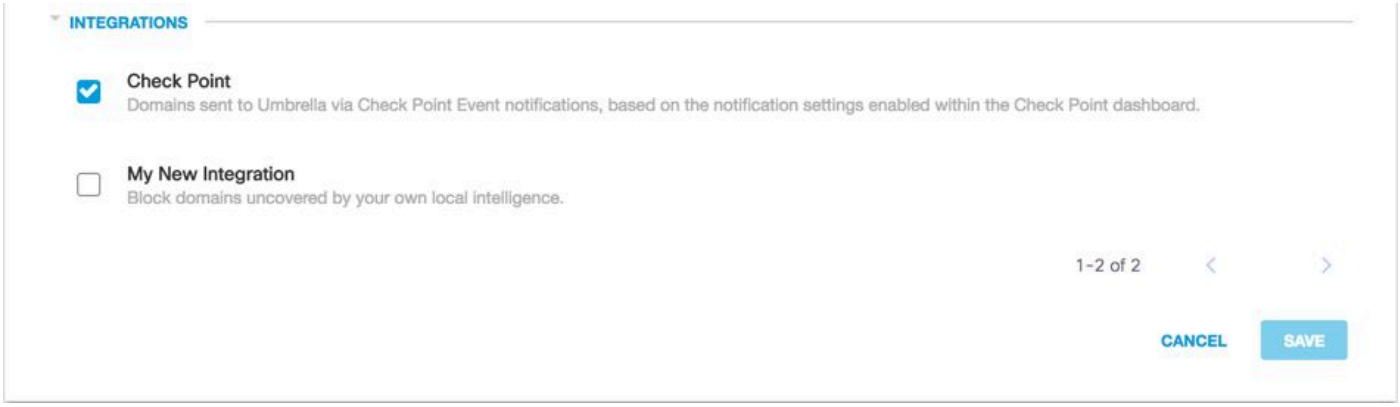
Você pode revisar as configurações de segurança que podem ser ativadas para uma política a qualquer momento no Cisco Umbrella:

1. Navegue até Policies > Policy Components > Security Settings.

2. Selecione uma configuração de segurança na tabela para expandi-la.

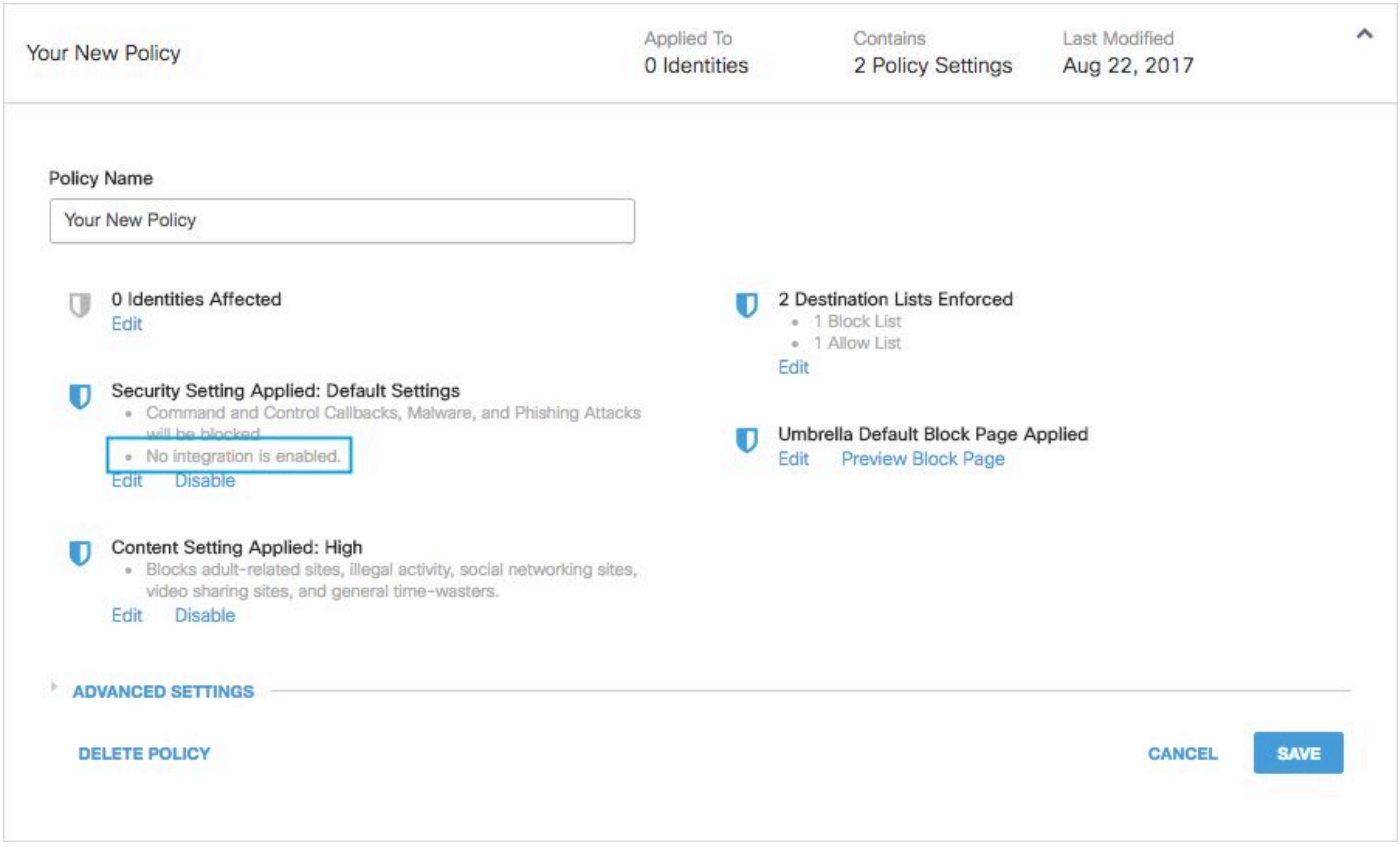
3. Role até a seção Integrações e expanda a seção para exibir a integração do Check Point.

4. Selecione a opção para a integração Check Point e, em seguida, selecione Save.



115013984226

Você também pode revisar as informações de integração através da página Resumo das configurações de segurança:



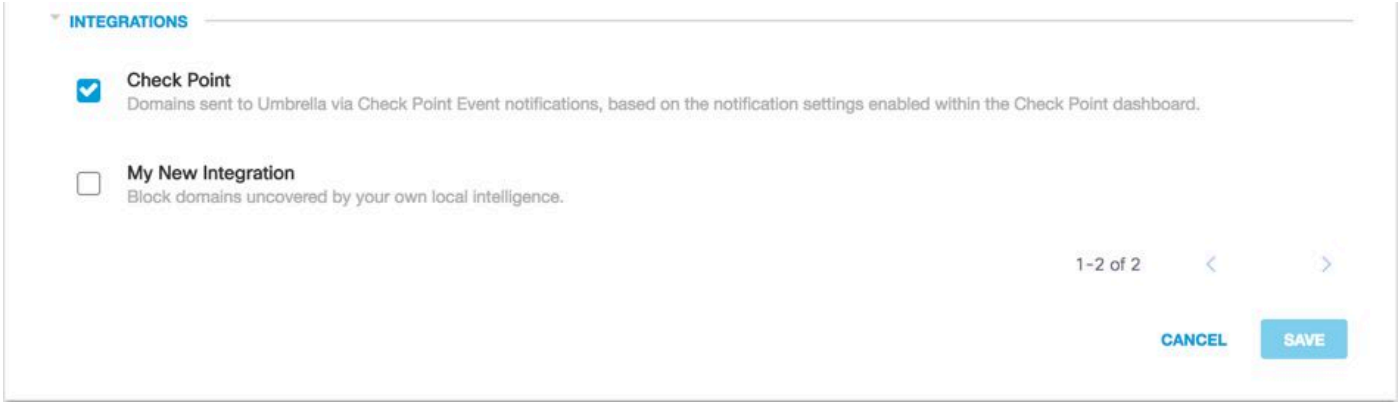
19916943300244

Aplicação das configurações de segurança do Check Point no "modo de bloqueio" a uma política para clientes gerenciados

Quando estiver pronto para que essas ameaças de segurança adicionais sejam aplicadas pelos clientes gerenciados pelo Cisco Umbrella, altere a configuração de segurança em uma política existente ou crie uma nova política que fique acima da sua política padrão para garantir que ela seja aplicada primeiro:

1. Certifique-se de que a integração do Check Point ainda esteja habilitada como foi feito na seção anterior. Navegue até Policies > Policy Components > Security Settings e abra a configuração relevante.

2. Em Integrations, verifique se a opção Check Point está selecionada. Caso contrário, selecione a opção e selecione Salvar.



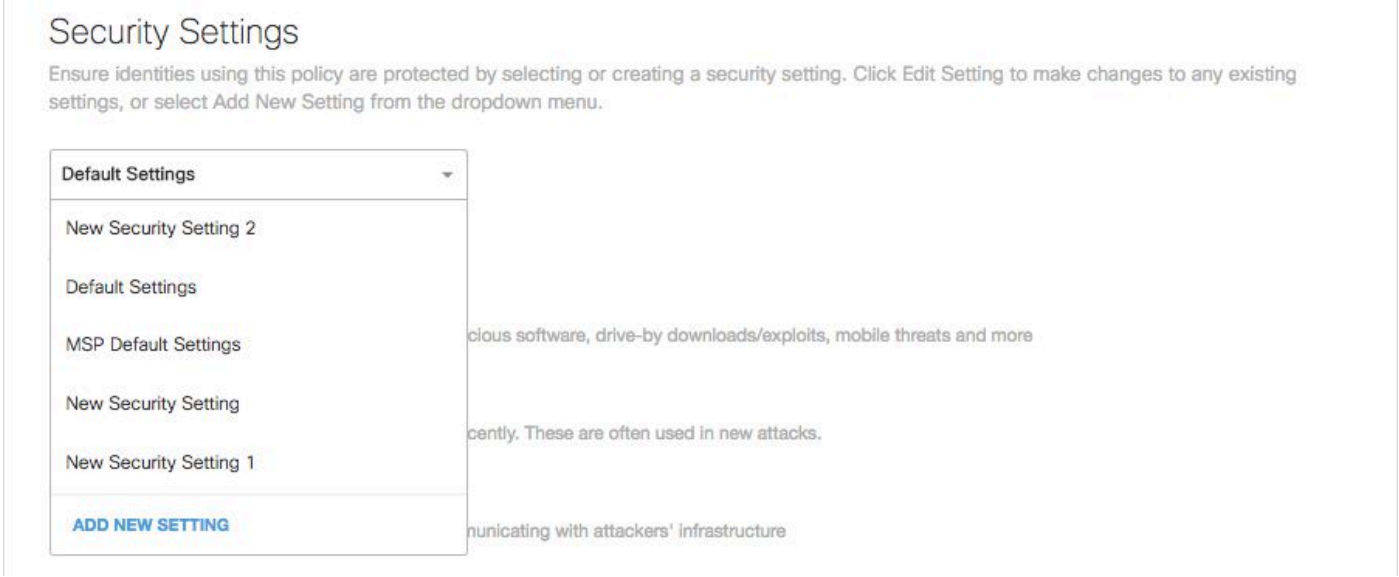
115013984226

Em seguida, no assistente Cisco Umbrella Policy, adicione esta configuração de segurança a uma política que você esteja editando:

1. Navegue até uma política: Policies > DNS Policies ou Policies > Web Policy.

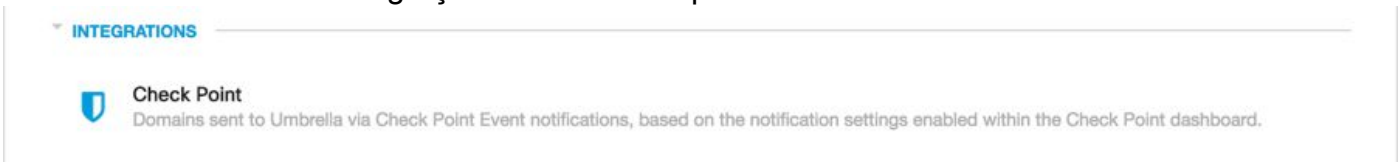
2. Expanda uma diretiva e, em Security Setting Applied (DNS Policies) ou Security Settings (Web Policy), selecione Edit.

3. No menu suspenso Configurações de segurança, selecione uma configuração de segurança que inclua a configuração Ponto de verificação.



19916943316884

O ícone de escudo em Integrações é atualizado para azul.



115014149783

4. Selecione Set & Return (DNS Policies) ou Save (Web Policy).

Os domínios de Ponto de Verificação contidos na configuração de segurança para Ponto de Verificação podem ser bloqueados para essas identidades usando a política.

Relatórios dentro do Umbrella para eventos de ponto de verificação

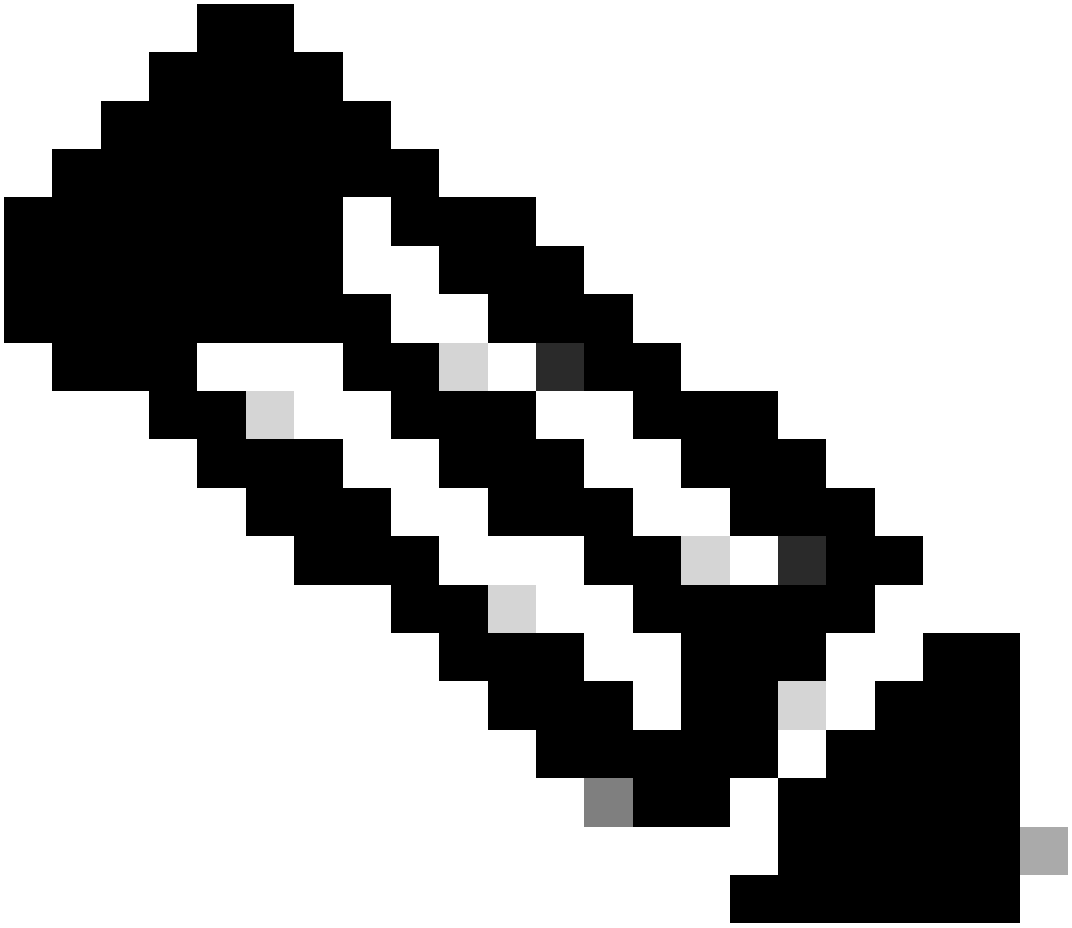
Relatórios sobre eventos de segurança do Check Point

A Lista de destino do ponto de verificação é uma das categorias de segurança disponíveis para relatórios. A maioria ou todos os relatórios usam as Categorias de segurança como um filtro. Por exemplo, você pode filtrar as categorias de segurança para mostrar apenas a atividade relacionada ao Ponto de Verificação:

1. Navegue até Relatórios > Relatórios Principais > Pesquisa de Atividade.

2. Em Categorias de Segurança, selecione Ponto de Verificação para filtrar o relatório para mostrar apenas a categoria de segurança do Ponto de Verificação.

115014197623



Note: Se a integração do Check Point estiver desativada, ela não poderá aparecer no filtro Categorias de segurança.

3. Selecione Aplicar para ver a atividade relacionada ao Ponto de Verificação para o período selecionado no relatório.

Relatando quando os domínios foram adicionados à lista de destino do ponto de verificação

O log de auditoria do Cisco Umbrella Admin inclui eventos do dispositivo Check Point à medida que adiciona domínios à lista de destino. Esses domínios parecem ter sido adicionados por um rótulo "Check Point account", na coluna User do log de auditoria.

Para localizar o log de Auditoria do Umbrella Admin, navegue para Relatórios > Log de Auditoria do Administrador.

Para gerar relatórios sobre quando um domínio foi adicionado, filtre para incluir apenas alterações

de Ponto de verificação aplicando um filtro Filtrar por Identidades e Configurações para a Lista de Bloqueios de Pontos de Verificação.

Depois de executar o relatório, você poderá ver uma lista de domínios adicionados à lista de destino do Ponto de verificação.

Lidando com detecções indesejadas ou falsos positivos

Gerenciando uma lista de permissões para detecção indesejada

Embora seja improvável, é possível que os domínios adicionados automaticamente pelo seu dispositivo Check Point possam disparar um bloqueio indesejado que possa fazer com que seus usuários sejam impedidos de acessar sites específicos. Em uma situação como essa, o Cisco Umbrella recomenda adicionar o(s) domínio(s) a uma lista de permissão, que tem precedência sobre todos os outros tipos de listas de bloqueio, incluindo Configurações de segurança. Uma lista de permissão tem precedência sobre uma lista de bloqueio quando um domínio está presente em ambos.

Há duas razões pelas quais esta abordagem é preferida:

- Primeiro, caso o dispositivo Check Point fosse readicionar o domínio novamente após sua remoção, a lista de permissões protege contra isso, causando mais problemas.
- Em segundo lugar, a lista de permissão mostra um registro histórico de domínios problemáticos para análises ou relatórios de auditoria posteriores.

Por padrão, há uma Lista de Permissões Global que é aplicada a todas as políticas. Adicionar um domínio à Lista de Permissões Global resulta na permissão do domínio em todas as políticas.

Se a Configuração de segurança do Check Point no modo Bloquear for aplicada apenas a um subconjunto de suas identidades gerenciadas do Cisco Umbrella (por exemplo, ela só é aplicada a computadores móveis e dispositivos móveis em roaming), você poderá criar uma lista de permissões específica para essas identidades ou políticas.

Para criar uma lista de permissões:

1. Navegue até Policies > Destination Lists e selecione o ícone Add.

2. Selecione Permitir e adicione seu domínio à lista.

3. Selecione Salvar.

Depois que a lista for salva, você poderá adicioná-la a uma política existente que abranja os clientes que foram afetados pelo bloqueio indesejado.

Excluindo domínios da lista de destinos de pontos de verificação

Ao lado de cada nome de domínio na lista de destino do Ponto de verificação, há um ícone Excluir. A exclusão de domínios permite limpar a lista de destinos do Check Point em caso de detecção indesejada.

No entanto, a exclusão não será permanente se o dispositivo Check Point reenviar o domínio para o Cisco Umbrella.

Para excluir um domínio:

1. Navegue até Configurações > Integrações e selecione Check Point para expandi-lo.

2. Selecione Ver Domínios.

3. Procure o nome de domínio que deseja deletar.

4. Selecione o ícone Deletar.

5. Selecione Fechar.

6. Selecione Salvar.

Se ocorrer uma detecção indesejada ou um falso positivo, o Cisco Umbrella recomenda a criação imediata de uma lista de permissões no Cisco Umbrella e, em seguida, a correção do falso positivo no Check Point Appliance. Posteriormente, você poderá remover o domínio da lista de destinos do Ponto de verificação.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.