Entenda os novos recursos do Umbrella Dashboard

Contents

Introdução

Este documento descreve a inspeção de arquivos e o bloqueio de URLs personalizado por meio de listas de destinos no Umbrella Dashboard.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no painel do Umbrella.

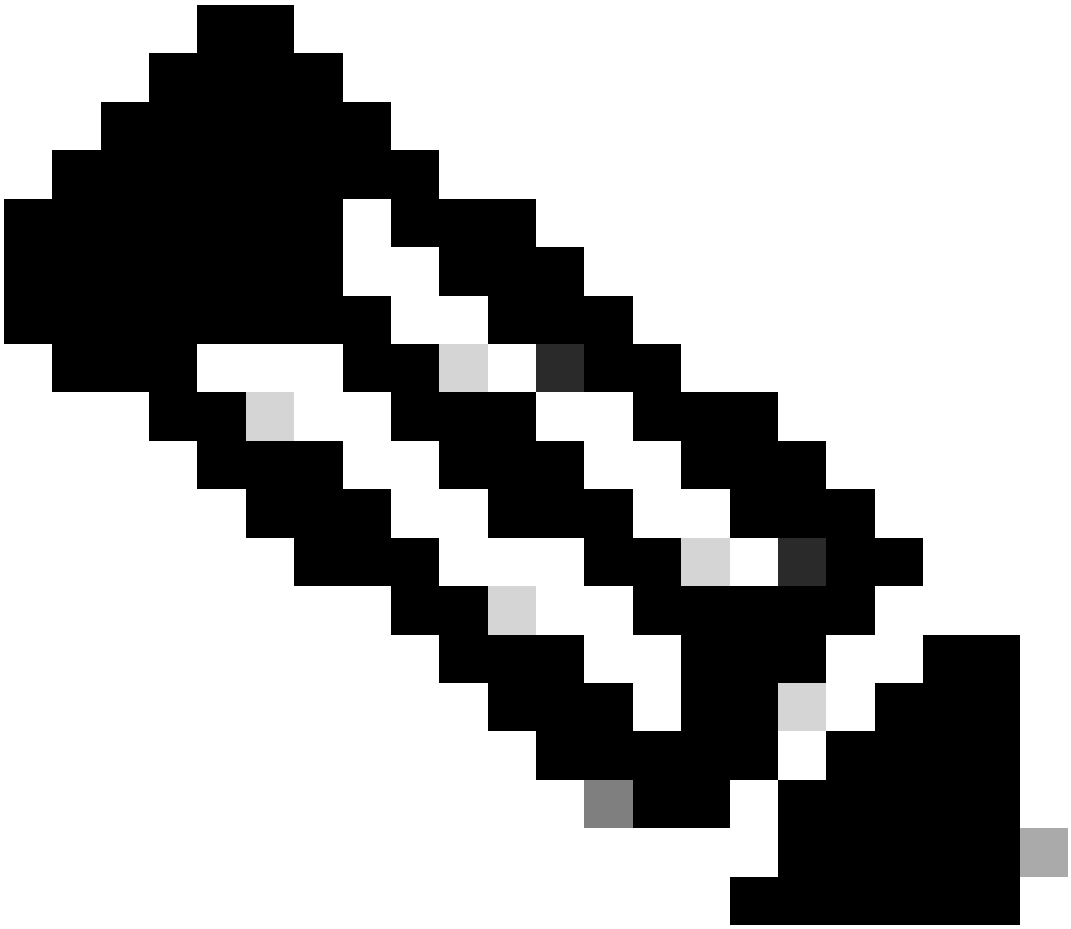
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Novos recursos

O Umbrella apresenta um novo conjunto de recursos que melhora sua funcionalidade. Com essa alteração, você pode ver dois novos recursos em seu painel agora:

- A inspeção de arquivos examina os arquivos que suas identidades baixam para ver se contêm código mal-intencionado e bloqueá-los, caso contenham.
- Os URLs bloqueados personalizados permitem bloquear seu próprio conjunto de URLs em uma lista de destinos. Isso agora lhe dá a flexibilidade de bloquear páginas específicas sem bloquear domínios inteiros.

Para ajudá-lo a aproveitar esse novo recurso, você pode usar os relatórios novos e atualizados e uma nova experiência de criação de políticas. O recurso de inspeção de arquivos é um dos vários planejados para versões futuras, criados com base no avanço da infraestrutura do Proxy inteligente para fornecer ainda mais segurança baseada em nuvem para você.



Note: Esses recursos estão sendo implementados em pequenos incrementos para nossos clientes e essas atualizações estão em disponibilidade limitada à medida que o Umbrella progride com esta versão. Se você recebeu um alerta em seu painel sobre esses recursos, você os tem. E se você quiser saber mais sobre esses recursos, entre em contato com umbrella-support@cisco.com.

O recurso de inspeção de arquivos está disponível apenas para clientes com os pacotes Umbrella Insights ou Umbrella Platform. Leia mais sobre pacotes e entre em contato com seu representante de conta da Cisco em caso de dúvidas.

Como aproveitar esses recursos

O acesso a esses novos recursos está disponível em alguns lugares: o assistente de política permite habilitar a Inspeção de Arquivos na página de resumo e, através de listas de destinos, você pode adicionar URLs personalizadas às suas listas de destinos bloqueadas. Além disso, o bloqueio de URLs personalizado também pode ser gerenciado especificamente na página de gerenciamento Listas de destinos.

No lado de relatórios, a seção de navegação de relatórios do painel Umbrella foi atualizada para que você possa localizar facilmente os relatórios novos e atualizados. Leia mais neste artigo sobre como habilitar esses recursos e confira alguns relatórios.

Inspeção de arquivo

A inspeção de arquivos é um recurso do Proxy Inteligente que amplia seu escopo e funcionalidade, adicionando a capacidade de verificar arquivos em busca de conteúdo mal-intencionado hospedado em domínios suspeitos. Um domínio suspeito não é confiável nem é conhecido por ser mal-intencionado.

Com o assistente de política do Umbrella, a inspeção de arquivos é fácil de implementar. Navegue até Policies > Policy List e expanda uma política ou selecione o ícone + (Add) para criar uma nova política. No assistente de política, certifique-se de que a Inspeção de arquivos esteja habilitada na página de resumo ou em uma nova política, selecione Inspecionar arquivos depois de habilitar o Proxy inteligente (em Configurações avançadas). Leia mais na documentação completa deste recurso.

Testando Inspeção de Arquivo

A partir de um dispositivo registrado em uma política com a Inspeção de arquivo ativada:

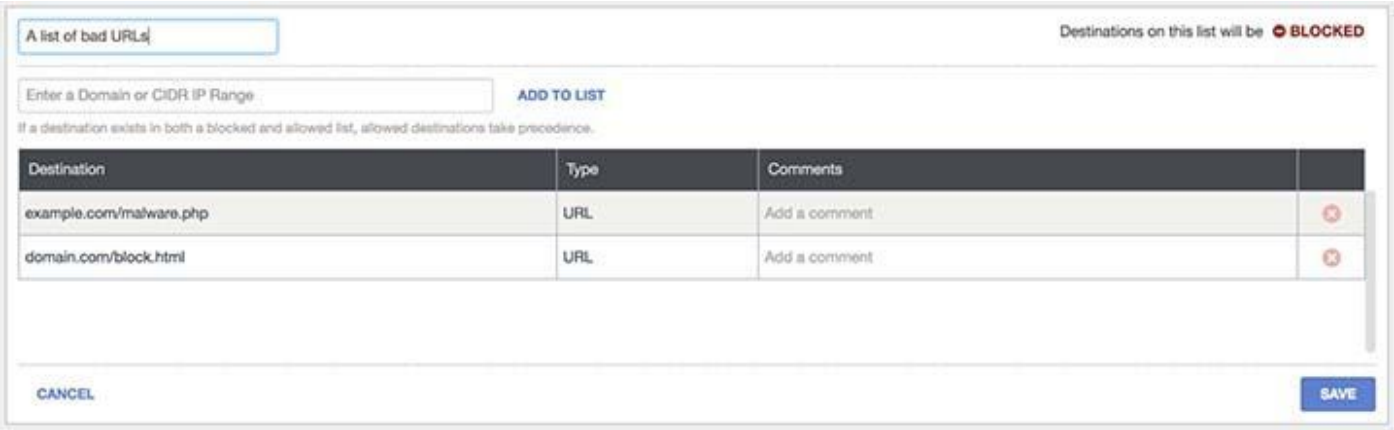
1. Navegue até http://proxy.opendnstest.com/download/eicar.com.

2. Uma página de bloqueio como esta captura de tela é exibida.

Página Bloqueada do Guarda-chuva

Habilitar URLs a serem bloqueados em suas listas de destino

Para bloquear um URL, basta inseri-lo em uma lista de destinos bloqueados ou criar uma nova lista de destinos bloqueados apenas para URLs. Para fazer isso, navegue até Policies > Destination Lists, expanda uma Destination list, adicione uma URL e selecione Save.



Lista de Destinos Bloqueados do Umbrella

Leia mais na documentação completa deste recurso.

Para que a infraestrutura do Umbrella inspecione uma URL para determinar se ela corresponde às definidas em sua lista de destinos bloqueados, você deve ter o seguinte:

- O Proxy Inteligente e a Descriptografia SSL devem ser habilitados como parte da política. Para obter mais informações, leia os documentos do Umbrella.

- A CA raiz do Cisco Umbrella deve ser instalada no(s) computador(es) usando essa política — garante que as conexões https também sejam filtradas. Para obter mais informações, leia os documentos do Umbrella.

É importante especificar uma URL corretamente para que o que está na sua política corresponda ao que o usuário está tentando acessar (e seja posteriormente bloqueado). Para obter mais informações sobre quais URLs você pode ou não usar, leia Instruções sobre lista de destino de URL personalizada.

Relatórios

A Umbrella agora tem novos e melhores relatórios:

- O Relatório de visão geral da segurança: oferece uma visão geral da atividade da rede fácil de ler por meio de gráficos e diagramas. Você pode ver rapidamente a atividade em suas identidades e em seu tráfego, ilustrando onde os problemas podem estar ocorrendo. Saiba mais sobre isso nos documentos do Umbrella.
- O Relatório de atividades de segurança: destaca eventos de segurança sinalizados, mas não necessariamente bloqueados, pela inteligência de ameaças do Umbrella. Isso inclui eventos de segurança filtrados por meio do Proxy Inteligente e da inspeção de arquivos. Saiba mais sobre isso nos documentos do Umbrella.

- Relatório de pesquisa de atividades: ajuda a encontrar o resultado de cada solicitação de DNS, URL e IP de suas várias identidades, ordenadas por data e hora decrescentes. Esse relatório pode listar todas as atividades relacionadas à segurança no Umbrella para o período de tempo selecionado e permite refinar sua pesquisa usando filtros para ver apenas o que você deseja ver. Saiba mais sobre isso nos documentos do Umbrella.

Esses relatórios também são fáceis de obter.

Enviando comentários sobre o Umbrella

A Umbrella adoraria ouvir o que você pensa sobre essas novas funcionalidades. Qualquer pergunta ou comentário que você tenha, a Umbrella quer ouvir de você! Envie seus comentários para umbrella-support@cisco.com e inclua o máximo de detalhes possível. Por exemplo, capturas de tela, o navegador que você está usando, seu SO e o cenário no qual você está usando esses recursos.

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.