

Compreender a categoria de conteúdo Internet Watch Foundation

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Habilitar a Categoria IWF](#)

[Configurar a Base de Monitoramento da Internet como uma Categoria de Conteúdo para Bloqueio](#)

[Testar a categoria IWF e exibir relatórios](#)

Introdução

Este documento descreve a categoria de filtragem de conteúdo da Internet Watch Foundation (IWF) no Cisco Umbrella.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

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

Como parte do compromisso da Cisco Umbrella em fornecer a melhor segurança e filtragem possíveis da Internet, este artigo introduz uma categoria de filtragem de conteúdo para a Umbrella: Internet Watch Foundation (IWF).

A IWF é uma organização de caridade com sede no Reino Unido, cuja missão é a eliminação de imagens de abuso sexual infantil on-line. O IWF mantém uma lista de páginas da Web

bloqueadas para evitar que os usuários da Internet encontrem acidentalmente conteúdo de abuso sexual infantil. Eles fornecem aos parceiros uma lista de URLs precisa e atual para permitir o bloqueio de conteúdo de abuso sexual infantil. A Umbrella está adotando sua lista como uma categoria que pode ser bloqueada no Umbrella. [Leia mais sobre o trabalho que a IWF está fazendo.](#)

Habilitar a Categoria IWF

A lista do IWF é composta de domínios e URLs. Isso significa que algumas entradas na lista podem simplesmente ser bloqueadas usando nossa tecnologia padrão de lista de bloqueio baseada em DNS, enquanto os blocos específicos de URL exigem que o proxy inteligente do Umbrella esteja habilitado. Para bloquear todos os sites contidos na categoria de conteúdo IWF, você deve habilitar o proxy inteligente em suas políticas.

O proxy inteligente é explicado na [documentação do Umbrella](#). Essencialmente, ele permite a capacidade de filtrar determinados URLs conforme determinado pelo nosso proxy baseado em nuvem. Usando proxy seletivo e inteligente para determinado tráfego, o Umbrella é capaz de filtrar facilmente a lista de URLs do IWF sem diminuir ou congestionar a velocidade da sua Internet.



Note: O proxy inteligente e a categoria de conteúdo IWF estão disponíveis apenas para clientes com [determinados pacotes Umbrella](#). A categoria de conteúdo IWF e o Intelligent Proxy também estão disponíveis para MSPs que fornecem o pacote "Umbrella for MSPs" para seus clientes e para qualquer usuário atual do pacote de hotspots Wi-Fi/Secure para convidados (Roaming/branch/WLAN). Se você não vir a categoria Internet Watch Foundation (IWF) listada em suas configurações de categoria, entre em contato com seu gerente de conta para obter esse recurso adicional.

Configurar a Base de Monitoramento da Internet como uma Categoria de Conteúdo para Bloqueio

Para configurar o IWF como uma categoria de conteúdo para bloqueio:

1. Habilite o proxy inteligente do Umbrella em suas políticas. O proxy inteligente é a capacidade do Umbrella de interceptar e enviar solicitações de proxy para arquivos mal-intencionados incorporados dentro de certos domínios chamados "cinza".

- Para obter instruções sobre como ativar o proxy inteligente, consulte a documentação de [Ativar o proxy inteligente](#).

2. Navegue até Políticas > Management > DNS Políticas > Category Settings.

3. Na lista de Categorias a serem Bloqueadas, selecione Internet Watch Foundation e salve sua atualização.

Testar a categoria IWF e exibir relatórios

1. O Umbrella configurou um domínio de teste para permitir que você assegure que configurou corretamente suas políticas para as identidades relevantes que podem ter as URLs na lista IWF bloqueadas. O domínio de teste é <http://proxy.opendnstest.com/iwf.htm>.

- Se suas identidades e políticas estiverem configuradas corretamente, você poderá receber uma página de bloqueio da mesma forma que pode para qualquer outro bloco de categoria de conteúdo. A aparência da página de bloqueio pode variar com base na sua configuração.

2. Se você não vir uma página de bloqueio, verifique se a identidade com a qual você está testando está corretamente aplicada à política apropriada.

- Se você vir uma página indicando que não está usando o proxy inteligente, verifique suas políticas para garantir que o proxy inteligente esteja ativado.
- Se ela estiver ativada, mas a categoria de conteúdo IWF não estiver definida para bloqueio, você poderá receber uma página mostrando o texto "IWF". Nesse caso, verifique se a categoria de conteúdo está habilitada em suas políticas.

3. Depois de testá-lo e de fazer check-out dos relatórios, aplique um filtro em uma pesquisa no relatório Pesquisa de Atividade:

Content Categories

Select All

- Humor
- Instant Messaging
- Internet Watch Foundation
- Jobs/Employment
- Lingerie/Bikini
- Movies
- Music

APPLY

115014821466

4. Seus resultados podem mostrar quaisquer tentativas feitas contra nossa página de teste nos resultados.
5. Se você não estiver vendo a página de bloqueio apropriada ao testar ou se os resultados dos testes não estiverem aparecendo na pesquisa, entre em [contato com o Suporte do Cisco Umbrella](#).

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.