Compreender o OpenDNS FamilyShield

Contents

Introdução

Este documento descreve o que é o OpenDNS FamilyShield, o que ele faz e como usá-lo em uma rede.

Overview

O OpenDNS FamilyShield é um serviço de filtragem de conteúdo baseado em DNS que ajuda a bloquear o acesso a sites comumente categorizados como conteúdo adulto, usando configurações de filtragem predefinidas.

Quando usar o FamilyShield

Use o FamilyShield quando precisar de uma forma simples baseada em DNS para aplicar a filtragem básica de conteúdo:

- Redes domésticas
- Ambientes de pequenos escritórios
- Redes de convidados
- Dispositivos de laboratório ou quiosque que exigem controles simplificados

O FamilyShield é normalmente usado quando uma configuração rápida é preferível ao gerenciamento de políticas personalizadas de filtragem.

Como funciona o FamilyShield

O FamilyShield funciona utilizando endereços de resolvedor DNS específicos. Quando um usuário tenta acessar um domínio, as consultas de DNS são resolvidas através dos resolvedores do FamilyShield. Se o domínio for classificado como restrito pelo FamilyShield, a resposta do DNS será bloqueada ou redirecionada com base no comportamento do serviço.

Note: Como é baseado em DNS, ele controla principalmente o acesso por resolução de nome de domínio.

Endereços de Servidor DNS

Configure estes endereços de servidor DNS no endpoint ou nas configurações DNS do roteador/DHCP:

- 208.67.222.123
- 208.67.220.123

Verifique se o FamilyShield está em uso

- Verifique se o dispositivo ou a rede está configurada para usar os endereços de servidor DNS do FamilyShield.
- Teste a resolução de nomes para um domínio permitido conhecido e confirme a resolução normal.
- Se a filtragem de conteúdo não parecer funcionar, verifique se nenhum outro método DNS substitui a configuração (por exemplo, DNS da VPN, DNS do navegador sobre HTTPS ou configurações DNS definidas manualmente).

Limitações

- A filtragem baseada em DNS pode ser ignorada se um usuário alterar as configurações DNS, usar uma VPN ou usar DNS sobre HTTPS (DoH) no navegador.
- O comportamento de filtragem é baseado em categoria e não é o mesmo que uma solução completa de inspeção de conteúdo de proxy ou firewall.

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.