OpenDNS FamilyShield begrijpen

Inhoud

Inleiding

In dit document wordt beschreven wat OpenDNS FamilyShield is, wat het doet en hoe het op een netwerk kan worden gebruikt.

Overzicht

OpenDNS FamilyShield is een op DNS gebaseerde contentfilterservice die helpt bij het blokkeren van toegang tot websites die gewoonlijk worden gecategoriseerd als inhoud voor volwassenen door vooraf gedefinieerde filterinstellingen te gebruiken.

Wanneer gebruik je FamilyShield

Gebruik FamilyShield wanneer u een eenvoudige DNS-gebaseerde manier nodig hebt om basisinhoudfilters toe te passen:

- Thuisnetwerken
- Kleine kantooromgevingen
- Gastnetwerken
- Laboratorium- of kioskapparaten die vereenvoudigde bedieningselementen vereisen

FamilyShield wordt meestal gebruikt wanneer een snelle installatie de voorkeur heeft boven het beheren van aangepast filterbeleid.

Hoe werkt FamilyShield

FamilyShield werkt met behulp van specifieke DNS-resolver-adressen. Wanneer een gebruiker probeert toegang te krijgen tot een domein, worden DNS-query's opgelost via de FamilyShield-resolvers. Als het domein is gecategoriseerd als beperkt door FamilyShield, wordt de DNS-reactie geblokkeerd of omgeleid op basis van het servicegedrag.

Opmerking: omdat dit op DNS is gebaseerd, wordt de toegang voornamelijk bepaald door de resolutie van de domeinnaam.

DNS-serveradressen

Configureer deze DNS-serveradressen op het eindpunt of op de DNS-instellingen van de router/DHCP:

- 208.67.222.123
- 208.67.220.123

Controleer of FamilyShield in gebruik is

- Controleer of het apparaat of netwerk is geconfigureerd voor het gebruik van de FamilyShield DNS-serveradressen.
- Test de naamresolutie voor een bekend toegestaan domein en bevestig de normale resolutie.
- Als het filteren van inhoud niet lijkt te werken, controleer dan of geen andere DNS-methode de configuratie overschrijft (bijvoorbeeld VPN DNS, browser DNS-over-HTTPS of handmatig geconfigureerde DNS-instellingen).

Beperkingen

- DNS-gebaseerde filtering kan worden omzeild als een gebruiker DNS-instellingen wijzigt, een VPN gebruikt of DNS-over-HTTPS (DoH) in de browser gebruikt.
- Filtergedrag is op categorieën gebaseerd en is niet hetzelfde als een volledige proxy- of firewall-inhoudsinspectieoplossing.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.