OpenDNS FamilyShield verstehen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, was OpenDNS FamilyShield ist, was es tut und wie es in einem Netzwerk verwendet wird.

Überblick

OpenDNS FamilyShield ist ein DNS-basierter Content-Filter-Service, der mithilfe vordefinierter Filtereinstellungen den Zugriff auf Websites blockiert, die in der Regel als jugendgefährdende Inhalte kategorisiert werden.

Verwendung von FamilyShield

Verwenden Sie FamilyShield, wenn Sie eine einfache DNS-basierte Methode zum Anwenden einer grundlegenden Inhaltsfilterung benötigen:

- Heimnetzwerke
- Kleine Büroumgebungen
- Gastnetzwerke
- Labor- oder Kiosk-Geräte, die vereinfachte Kontrollen erfordern

FamilyShield wird in der Regel dann verwendet, wenn eine schnelle Einrichtung gegenüber der Verwaltung benutzerdefinierter Filterrichtlinien bevorzugt wird.

Funktionsweise von FamilyShield

FamilyShield verwendet bestimmte DNS-Resolver-Adressen. Wenn ein Benutzer versucht, auf eine Domäne zuzugreifen, werden DNS-Abfragen über die FamilyShield-Resolver aufgelöst. Wenn die Domäne als durch FamilyShield eingeschränkt kategorisiert wird, wird die DNS-Antwort aufgrund des Dienstverhaltens blockiert oder umgeleitet.

Anmerkung: Da dies DNS-basiert ist, wird der Zugriff primär anhand der Auflösung von Domänennamen gesteuert.

DNS-Serveradressen

Konfigurieren Sie die folgenden DNS-Serveradressen auf dem Endpunkt oder auf den Router-/DHCP-DNS-Einstellungen:

- 208.67.222.123
- 208.67.220.123

Überprüfen Sie, ob FamilyShield verwendet wird.

- Überprüfen Sie, ob das Gerät oder das Netzwerk für die Verwendung der FamilyShield-DNS-Serveradressen konfiguriert ist.
- Testen der Namensauflösung für eine bekannte zulässige Domäne und Bestätigen der normalen Auflösung
- Wenn die Inhaltsfilterung nicht funktioniert, stellen Sie sicher, dass die Konfiguration nicht von einer anderen DNS-Methode überschrieben wird (z. B. VPN DNS, Browser-DNS-over-HTTPS oder manuell konfigurierte DNS-Einstellungen).

Einschränkungen

- Die DNS-basierte Filterung kann umgangen werden, wenn ein Benutzer DNS-Einstellungen ändert, ein VPN verwendet oder DNS-over-HTTPS (DoH) im Browser verwendet.
- Das Filterverhalten ist kategoriebasiert und unterscheidet sich von einer Vollproxy- oder Firewall-Inhaltsüberprüfungslösung.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.