Informazioni su OpenDNS FamilyShield

Sommario

Introduzione

Questo documento descrive cosa è OpenDNS FamilyShield, cosa fa e come utilizzarlo in una rete.

Panoramica

OpenDNS FamilyShield è un servizio di filtro dei contenuti basato su DNS che consente di bloccare l'accesso a siti Web comunemente classificati come contenuti per adulti utilizzando impostazioni di filtro predefinite.

Quando utilizzare FamilyShield

Utilizzare FamilyShield quando è necessario un semplice metodo basato su DNS per applicare filtri di base dei contenuti:

- Reti domestiche
- Ambienti di ufficio di piccole dimensioni
- Reti guest
- Dispositivi lab o kiosk che richiedono controlli semplificati

FamilyShield viene generalmente utilizzato quando si preferisce una configurazione rapida rispetto alla gestione di criteri di filtraggio personalizzati.

Funzionamento di FamilyShield

FamilyShield funziona utilizzando specifici indirizzi del resolver DNS. Quando un utente tenta di accedere a un dominio, le query DNS vengono risolte tramite i resolver FamilyShield. Se il dominio è classificato come limitato da FamilyShield, la risposta DNS viene bloccata o reindirizzata in base al comportamento del servizio.

Nota: Poiché è basato su DNS, controlla principalmente l'accesso in base alla risoluzione dei nomi di dominio.

Indirizzi server DNS

Configurare questi indirizzi server DNS sull'endpoint o sulle impostazioni DNS del router/DHCP:

- 208.67.222.123
- 208.67.220.123

Verifica che FamilyShield sia in uso

- Verificare che il dispositivo o la rete sia configurata per l'utilizzo degli indirizzi del server DNS FamilyShield.
- Verificare la risoluzione dei nomi per un dominio consentito noto e confermare la risoluzione normale.
- Se il filtro del contenuto non funziona, verificare che nessun altro metodo DNS abbia la precedenza sulla configurazione, ad esempio VPN DNS, browser DNS-over-HTTPS o impostazioni DNS configurate manualmente.

Limitazioni

- Il filtro basato su DNS può essere ignorato se un utente modifica le impostazioni DNS, utilizza una VPN o utilizza DNS-over-HTTPS (DoH) nel browser.
- Il filtraggio è basato sulle categorie e non equivale a una soluzione di ispezione dei contenuti proxy o firewall completa.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).