

# OpenDNS FamilyShield 이해

## 목차

---

- [소개](#)
  - [개요](#)
  - [FamilyShield 사용 시기](#)
  - [FamilyShield 작동 방식](#)
  - [DNS 서버 주소](#)
  - [FamilyShield가 사용 중인지 확인](#)
  - [제한 사항](#)
- 

## 소개

이 문서에서는 OpenDNS FamilyShield의 정의, 기능, 네트워크에서 이를 사용하는 방법에 대해 설명합니다.

## 개요

OpenDNS FamilyShield는 미리 정의된 필터링 설정을 사용하여 성인 콘텐츠로 일반적으로 분류되는 웹 사이트에 대한 액세스를 차단하는 DNS 기반 콘텐츠 필터링 서비스입니다.

## FamilyShield 사용 시기

기본 콘텐츠 필터링을 적용하는 간단한 DNS 기반 방법이 필요한 경우 FamilyShield를 사용합니다.

- 홈 네트워크
- 소규모 사무실 환경
- 게스트 네트워크
- 간소화된 제어가 필요한 랩 또는 키오스크 장치

FamilyShield는 일반적으로 사용자 지정 필터링 정책 관리보다 빠른 설정을 선호할 때 사용됩니다.

## FamilyShield 작동 방식

FamilyShield는 특정 DNS 확인자 주소를 사용하여 작동합니다. 사용자가 도메인에 액세스하려고 하면 DNS 쿼리는 FamilyShield 확인자를 통해 확인됩니다. 도메인이 FamilyShield에 의해 제한되는 것으로 분류되면 DNS 응답은 서비스 동작에 따라 차단되거나 리디렉션됩니다.



참고: DNS 기반이므로, 기본적으로 도메인 이름 확인에 의한 액세스를 제어합니다.

---

## DNS 서버 주소

엔드포인트 또는 라우터/DHCP DNS 설정에서 다음 DNS 서버 주소를 구성합니다.

- 208.67.222.123
- 208.67.220.123

## FamilyShield가 사용 중인지 확인

- 디바이스 또는 네트워크가 FamilyShield DNS 서버 주소를 사용하도록 구성되었는지 확인합니다.
- 알려진 허용 도메인에 대한 이름 확인을 테스트하고 정상 확인을 확인합니다.
- 콘텐츠 필터링이 작동하지 않는 경우 다른 DNS 방법이 컨피그레이션을 재정의하지 않는지 확인합니다(예: VPN DNS, 브라우저 DNS-over-HTTPS 또는 수동으로 구성된 DNS 설정).

## 제한 사항

- 사용자가 브라우저에서 DNS 설정을 변경하거나, VPN을 사용하거나, DNS-over-HTTPS(DoH)를 사용하는 경우 DNS 기반 필터링을 우회할 수 있습니다.
- 필터링 동작은 카테고리 기반이며 전체 프록시 또는 방화벽 콘텐츠 검사 솔루션과 동일하지 않습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.