

# 了解OpenDNS系列Shield

## 目录

---

[简介](#)

[概述](#)

[何时使用FamilyShield](#)

[FamilyShield的工作原理](#)

[DNS 服务器地址](#)

[验证FamilyShield是否正在使用](#)

[限制](#)

---

## 简介

本文档介绍OpenDNS FamilyShield是什么、它执行什么以及在网络中如何使用它。

## 概述

OpenDNS FamilyShield是一种基于DNS的内容过滤服务，通过使用预定义的过滤设置来帮助阻止对通常归类为成人内容的网站的访问。

## 何时使用FamilyShield

当需要基于DNS的简单方法应用基本内容过滤时，请使用FamilyShield:

- 家庭网络
- 小型办公室环境
- 访客网络
- 需要简化控制的实验室或终端机设备

FamilyShield通常用于快速设置优先于管理自定义过滤策略。

## FamilyShield的工作原理

FamilyShield使用特定的DNS解析器地址工作。当用户尝试访问域时，DNS查询通过FamilyShield解析器进行解析。如果域被归类为FamilyShield限制，DNS响应会根据服务行为被阻止或重定向。



注意：由于这是基于DNS的，因此它主要通过域名解析来控制访问。

---

## DNS 服务器地址

在终端或路由器/DHCP DNS设置上配置以下DNS服务器地址：

- 208.67.222.123
- 208.67.220.123

## 验证FamilyShield是否正在使用

- 检验设备或网络是否配置为使用FamilyShield DNS服务器地址。
- 测试已知允许域的名称解析并确认正常解析。
- 如果内容过滤似乎不起作用，请验证没有其他DNS方法覆盖配置（例如，VPN DNS、浏览器DNS-over-HTTPS或手动配置的DNS设置）。

## 限制

- 如果用户在浏览器中更改DNS设置、使用VPN或使用DNS-over-HTTPS(DoH)，则可以绕过基于DNS的过滤。
- 过滤行为基于类别，与完全代理或防火墙内容检测解决方案不同。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。