

# Internet Watch Foundation 콘텐츠 범주 이해

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[IWF 범주 활성화](#)

[Internet Watch Foundation을 차단을 위한 콘텐츠 범주로 구성](#)

[IWF 범주 테스트 및 보고서 보기](#)

---

## 소개

이 문서에서는 Cisco Umbrella의 IWF(Internet Watch Foundation) 콘텐츠 필터링 카테고리에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 Cisco Umbrella를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 개요

최상의 인터넷 보안 및 필터링을 제공하기 위한 Cisco Umbrella의 노력의 일환으로, 이 문서에서는 Umbrella에 대한 콘텐츠 필터링 카테고리를 소개합니다. IWF(Internet Watch Foundation)에 대해 설명합니다.

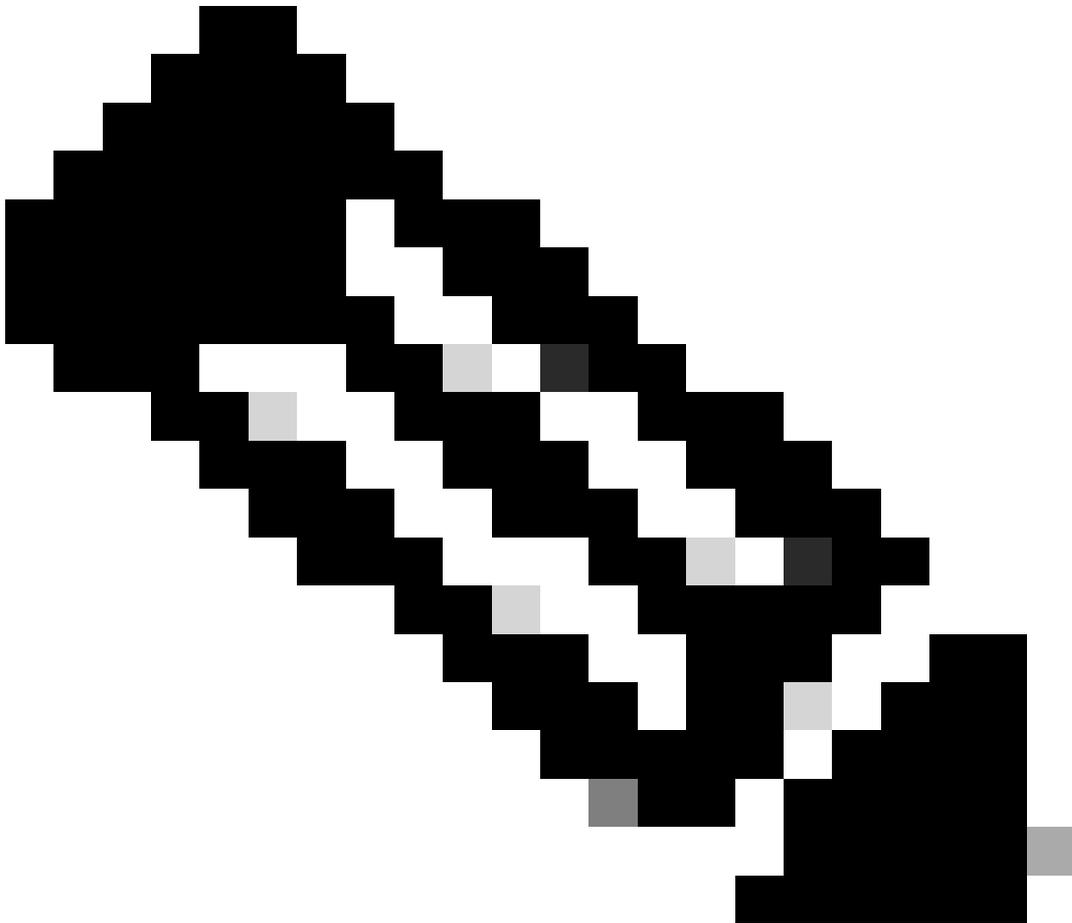
IWF는 영국에 본부를 둔 자선 단체로, 이 단체의 임무는 온라인 아동 성학대 이미지 제거이다. IWF는 인터넷 사용자가 실수로 아동 성학대 콘텐츠를 발견하지 못하도록 차단한 웹 페이지 목록을 유지 관리하고 있다. 아동 성학대 콘텐츠 차단이 가능하도록 파트너에게 정확한 최신 URL 리스트를 제공한다. Umbrella는 Umbrella에서 차단 가능한 범주로 목록을 채택하고 있습니다. [IWF의 작업에 대해 자세히 알아보십시오.](#)

## IWF 범주 활성화

IWF의 목록은 도메인과 URL로 구성됩니다. 즉, 목록의 일부 항목은 표준 DNS 기반 차단 목록 기술을 사용하여 간단히 차단할 수 있는 반면, URL 전용 차단에서는 Umbrella의 지능형 프록시가 활성화되어 있어야 합니다. IWF 콘텐츠 카테고리에 포함된 모든 사이트를 차단하려면 정책 내에서 지능형 프록시를 활성화해야 합니다.

지능형 프록시는 Umbrella 설명서에 [설명되어 있습니다](#). 기본적으로 이 프록시를 사용하면 클라우드 기반 프록시에서 결정한 특정 URL을 필터링할 수 있습니다. Umbrella는 특정 트래픽을 선택적으로 지능적으로 프록시함으로써 인터넷 속도를 늦추거나 병목 현상을 일으키지 않고 IWF에서 URL 목록을 쉽게 필터링할 수 있습니다.

---



참고: 지능형 프록시 및 IWF 콘텐츠 카테고리는 [특정 Umbrella](#) 패키지를 보유한 고객만 사용할 수 [있습니다](#). IWF 콘텐츠 카테고리 및 지능형 프록시는 고객에게 "MSP용 Umbrella" 패키지를 제공하는 MSP 및 현재 게스트 Wi-Fi/보안 핫스팟 패키지 사용자(로밍/브랜치/WLAN)에게도 제공됩니다. 범주 설정에 IWF(Internet Watch Foundation) 범주가 표시되지 않으면 계정 관리자에게 이 추가 기능에 대해 문의하십시오.

---

# Internet Watch Foundation을 차단을 위한 콘텐츠 범주로 구성

IWF를 차단을 위한 콘텐츠 카테고리로 설정하려면

1. 정책에서 Umbrella의 지능형 프록시를 사용하도록 설정합니다. 지능형 프록시는 Umbrella가 특정 "회색" 도메인 내에 포함된 악성 파일에 대한 요청을 가로채고 프록시하는 기능입니다.

- 지능형 프록시를 활성화하는 방법에 대한 자세한 내용은 지능형 프록시 활성화 [설명서를 참조 하십시오](#).

2. Policies(정책) > Management(관리) > DNS Policies(DNS 정책) > Category Settings(범주 설정)로 이동합니다.

3. 차단할 범주 목록에서 Internet Watch Foundation을 선택하고 업데이트를 저장합니다.

## IWF 범주 테스트 및 보고서 보기

1. Umbrella는 IWF 목록의 URL을 차단할 수 있는 관련 ID에 대한 정책을 올바르게 구성했는지 확인할 수 있도록 테스트 도메인을 설정합니다. 테스트 도메인은

<http://proxy.opendnstest.com/iwf.htm>입니다.

- ID 및 정책이 올바르게 구성된 경우 다른 콘텐츠 범주 블록에 대해 가능한 차단 페이지를 받을 수 있습니다. 차단 페이지 모양은 컨피그레이션에 따라 달라질 수 있습니다.

2. 차단 페이지가 표시되지 않으면 테스트할 ID가 적절한 정책에 올바르게 적용되었는지 확인합니다.

- 지능형 프록시를 사용하고 있지 않음을 나타내는 페이지가 표시되면 정책을 확인하여 지능형 프록시가 활성화되어 있는지 확인합니다.
- 활성화되었지만 IWF 콘텐츠 범주가 차단으로 설정되지 않은 경우 "IWF" 텍스트가 표시된 페이지를 수신할 수 있습니다. 이 경우 콘텐츠 범주가 정책에서 활성화되어 있는지 확인하십시오.

3. 보고서를 테스트한 후 보고서를 체크 아웃하려면 활동 검색 보고서의 검색에 대해 필터를 적용합니다.

## Content Categories

Select All

- Humor
- Instant Messaging
- Internet Watch Foundation
- Jobs/Employment
- Lingerie/Bikini
- Movies
- Music

APPLY

115014821466

4. 결과에 테스트 페이지에 대한 모든 시도가 표시될 수 있습니다.
5. 테스트할 때 적절한 차단 페이지가 표시되지 않거나 검색 결과가 표시되지 않으면 [Cisco Umbrella Support](#)에 [문의하십시오](#).

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.