

De Content Categorie van de Internet Watch Foundation begrijpen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[De IWF-categorie inschakelen](#)

[Configureer de Internet Watch Foundation als een inhoudscategorie voor blokkeren](#)

[Test de IWF-categorie en bekijk rapporten](#)

Inleiding

In dit document wordt de categorie voor het filteren van inhoud van de Internet Watch Foundation (IWF) beschreven in Cisco Umbrella.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Als onderdeel van Cisco Umbrella's inzet om de best mogelijke internetbeveiliging en -filtering te bieden, introduceert dit artikel een categorie inhoudfilters voor Umbrella: de Internet Watch Foundation (IWF).

De IWF is een in het Verenigd Koninkrijk gevestigde liefdadigheidsorganisatie die zich inzet voor de eliminatie van afbeeldingen van seksueel misbruik van kinderen online. De IWF onderhoudt

een lijst met geblokkeerde webpagina's om te voorkomen dat internetgebruikers per ongeluk inhoud over seksueel misbruik van kinderen vinden. Ze bieden partners een nauwkeurige en actuele URL-lijst om inhoud over seksueel misbruik van kinderen te blokkeren. Umbrella neemt hun lijst over als een categorie die kan worden geblokkeerd in Umbrella. [Lees hier meer over het werk dat de IWF doet.](#)

De IWF-categorie inschakelen

De lijst van de IWF bestaat uit zowel domeinen als URL's. Dit betekent dat sommige items op de lijst eenvoudig kunnen worden geblokkeerd met behulp van onze standaard DNS-gebaseerde blokkijsttechnologie, terwijl de URL-specifieke blokken vereisen dat de intelligente proxy van Umbrella is ingeschakeld. Om alle sites in de IWF-inhoudscategorie te blokkeren, moet u de intelligente proxy inschakelen in uw beleid.

De intelligente proxy wordt uitgelegd in [de Umbrella documentatie](#). In wezen maakt het de mogelijkheid om bepaalde URL's te filteren zoals bepaald door onze cloud-gebaseerde proxy. Door selectief en intelligent proxy bepaald verkeer, Umbrella is in staat om gemakkelijk te filteren de URL-lijst van de IWF zonder het vertragen of bottlenecking van de snelheid van uw internet.



Opmerking: de intelligente proxy en de IWF-inhoudscategorie zijn alleen beschikbaar voor klanten met [bepaalde Umbrella-pakketten](#). De IWF-inhoudscategorie en de Intelligente proxy zijn ook beschikbaar voor MSP's die het pakket "Paraplu voor MSP's" aan hun klanten leveren, en voor alle huidige gebruikers van het Guest Wi-Fi/Secure-hotspotpakket (Roaming/branch/WLAN). Als de categorie Internet Watch Foundation (IWF) niet wordt weergegeven in de rubriekinstellingen, neemt u contact op met uw accountmanager voor deze extra functie.

Configureer de Internet Watch Foundation als een inhoudscategorie voor blokkeren

IWF instellen als een inhoudscategorie voor blokkeren:

1. Schakel de intelligente proxy van Umbrella in uw beleid in. De intelligente proxy is de mogelijkheid voor Umbrella om te onderscheppen en proxy verzoeken voor kwaadaardige bestanden ingebed in bepaalde zogenaamde "grijze" domeinen.

- Zie de documentatie voor het inschakelen van de intelligente proxy voor instructies over het inschakelen [van de intelligente proxy](#).

2. Navigeer naar Beleid > Beheer > DNS-beleid > Categorieinstellingen.

3. Selecteer Internet Watch Foundation in de lijst met te blokkeren categorieën en sla uw update op.

Test de IWF-categorie en bekijk rapporten

1. Umbrella stelt een testdomein in zodat u kunt controleren of u uw beleid correct hebt geconfigureerd voor de relevante identiteiten waarvoor de URL's op de IWF-lijst kunnen worden geblokkeerd. Het testdomein is <http://proxy.opendnstest.com/iwf.htm>.

- Als uw identiteiten en beleidsregels correct zijn geconfigureerd, kunt u een blokpagina ontvangen, zoals u kunt voor elk ander blok voor inhoudscategorieën. Het uiterlijk van de blokpagina kan variëren op basis van uw configuratie.

2. Als u geen blokpagina ziet, controleert u of de identiteit waarmee u test correct wordt toegepast op het juiste beleid.

- Als u een pagina ziet die aangeeft dat u de intelligente proxy niet gebruikt, controleert u uw beleid om ervoor te zorgen dat de intelligente proxy is ingeschakeld.
- Als deze optie is ingeschakeld, maar de inhoudscategorie van de IWF niet is ingesteld op blokkeren, kunt u een pagina ontvangen met de tekst "IWF". Controleer in dat geval of de inhoudscategorie is ingeschakeld in uw beleid.

3. Nadat u het hebt getest en u uw rapporten wilt bekijken, past u een filter toe tegen een zoekopdracht in het rapport Activiteit zoeken:

Content Categories

Select All

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

APPLY

115014821466

4. Uw resultaten kunnen alle pogingen tonen die tegen onze testpagina in de resultaten worden ondernomen.
5. Als u tijdens het testen niet de juiste blokpagina ziet of als de resultaten van uw tests niet in uw zoekopdracht worden weergegeven, [neemt u contact op met Cisco Umbrella Support](#).

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.