Comprendre la catégorie de contenu Internet Watch Foundation

Table des matières

Introduction

Ce document décrit la catégorie de filtrage de contenu Internet Watch Foundation (IWF) dans Cisco Umbrella.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Dans le cadre de l'engagement de Cisco Umbrella à fournir la meilleure sécurité et le meilleur filtrage Internet possible, cet article présente une catégorie de filtrage de contenu à Umbrella : Internet Watch Foundation (IWF).

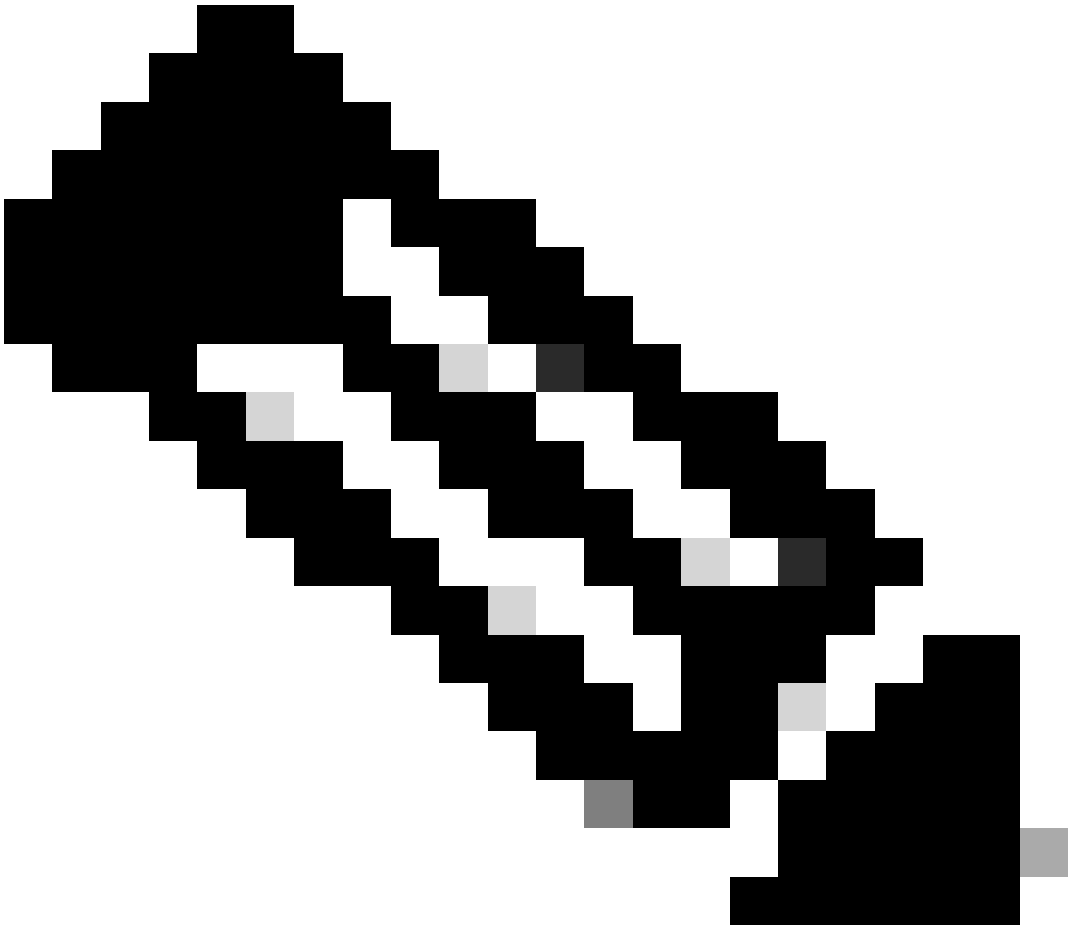
L'IWF est une organisation caritative basée au Royaume-Uni dont la mission est l'élimination des images d'abus sexuels d'enfants en ligne. L'IWF tient à jour une liste de pages web bloquées afin d'empêcher les internautes de trouver accidentellement du contenu pédopornographique. Ils

fournissent aux partenaires une liste d'URL précise et à jour pour permettre le blocage du contenu sur les abus sexuels commis contre des enfants. Umbrella adopte sa liste comme une catégorie qui peut être bloquée dans Umbrella. En savoir plus sur le travail de l'IWF.

Activer la catégorie IWF

La liste de l'IWF comprend à la fois les domaines et les URL. Cela signifie que certaines entrées de la liste peuvent simplement être bloquées à l'aide de notre technologie de liste de blocage basée sur DNS standard, alors que les blocs spécifiques à l'URL nécessitent que le proxy intelligent d'Umbrella soit activé. Afin de bloquer tous les sites contenus dans la catégorie de contenu IWF, vous devez activer le proxy intelligent dans vos politiques.

Le proxy intelligent est expliqué dans la documentation Umbrella. Il permet essentiellement de filtrer certaines URL, comme déterminé par notre proxy basé sur le cloud. En fournissant sélectivement et intelligemment un proxy à certains trafics, Umbrella peut facilement filtrer la liste d'URL à partir de l'IWF sans ralentir ou bloquer la vitesse de votre Internet.



Remarque : Le proxy intelligent et la catégorie de contenu IWF ne sont disponibles que pour les clients disposant de certains packages Umbrella. La catégorie de contenu IWF et le proxy intelligent sont également disponibles pour les fournisseurs de services Internet proposant le package « Umbrella for MSPs » à leurs clients, ainsi que pour tous les utilisateurs actuels du package Wi-Fi invité/point d'accès sécurisé (itinérance/succursale/WLAN). Si la catégorie Internet Watch Foundation (IWF) n'apparaît pas dans vos paramètres de catégorie, contactez votre gestionnaire de compte pour obtenir cette fonctionnalité supplémentaire.

Configurer Internet Watch Foundation en tant que catégorie de contenu à bloquer

Pour configurer IWF en tant que catégorie de contenu à bloquer :

1. Activez le proxy intelligent d'Umbrella dans vos politiques. Le proxy intelligent est la capacité d'Umbrella à intercepter et à transmettre par proxy des requêtes de fichiers malveillants intégrés dans certains domaines dits « gris ».

- Pour obtenir des instructions sur la façon d'activer le proxy intelligent, reportez-vous à la documentation de Enable the Intelligent Proxy.

2. Accédez à Policies > Management > DNS Policies > Category Settings.

3. Dans la liste des catégories à bloquer, sélectionnez Internet Watch Foundation et enregistrez votre mise à jour.

Tester la catégorie IWF et afficher les rapports

1. Umbrella a configuré un domaine de test pour vous permettre de vous assurer que vous avez correctement configuré vos stratégies pour les identités pertinentes qui peuvent avoir les URL sur la liste IWF bloquées. Le domaine de test est http://proxy.opendnstest.com/iwf.htm.

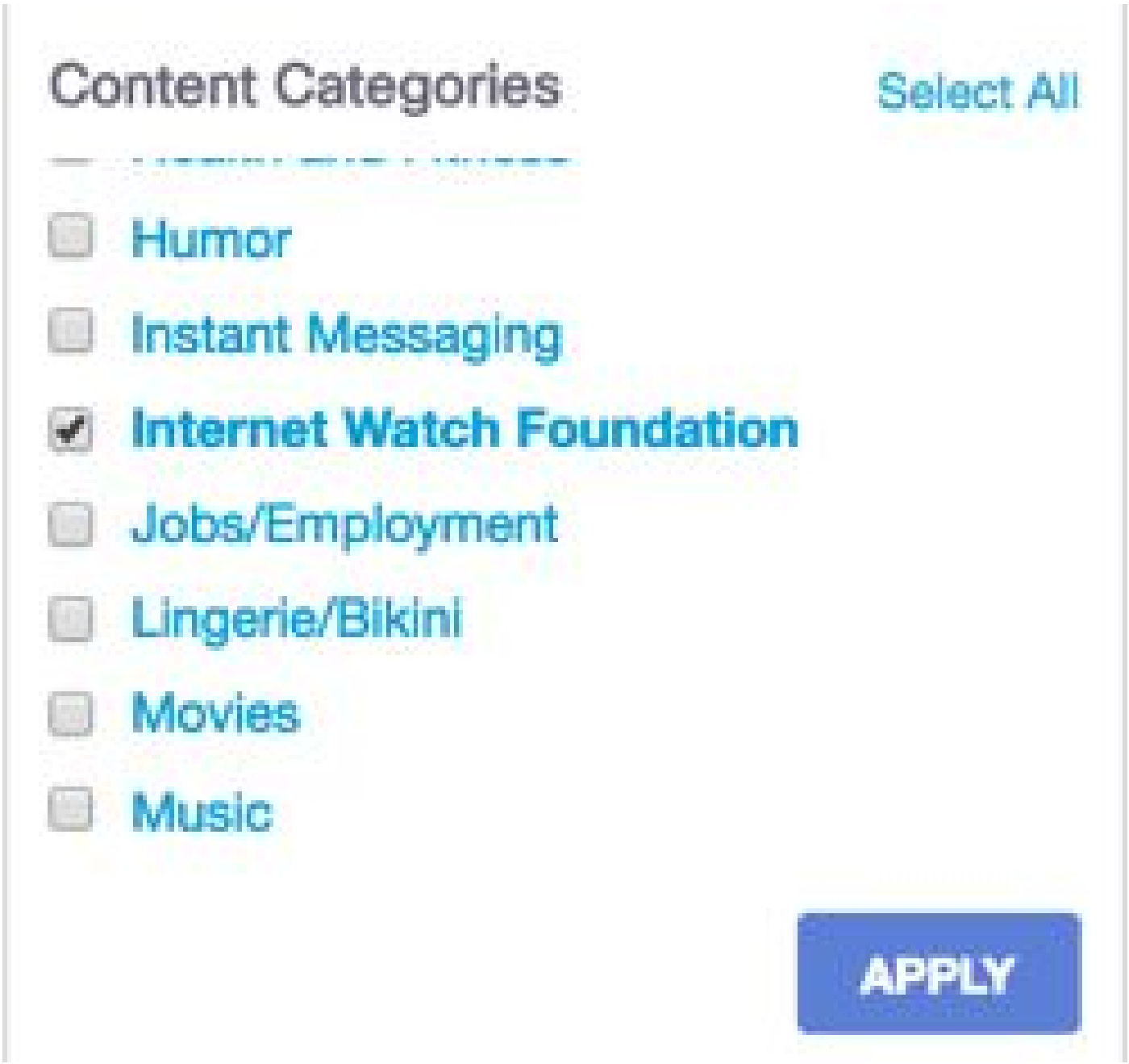
- Si vos identités et stratégies sont correctement configurées, vous pouvez recevoir une page de blocage comme vous le pouvez pour tout autre bloc de catégorie de contenu. L'apparence de la page de blocage peut varier selon votre configuration.

2. Si vous ne voyez pas de page de blocage, vérifiez que l'identité que vous testez avec est correctement appliquée à la stratégie appropriée.

- Si vous voyez une page indiquant que vous n'utilisez pas le proxy intelligent, vérifiez vos stratégies pour vous assurer que le proxy intelligent est activé.
- S'il est activé mais que la catégorie de contenu IWF n'est pas définie pour bloquer, vous pouvez recevoir une page affichant le texte « IWF ». Dans ce cas, vérifiez que la catégorie de contenu est activée dans vos stratégies.

3. Une fois que vous l'avez testé et que vous souhaitez consulter vos rapports, appliquez un filtre

par rapport à une recherche dans le rapport Recherche d'activité :



115014821466

4. Vos résultats peuvent montrer toutes les tentatives faites contre notre page de test dans les résultats.

5. Si vous ne voyez pas la page de blocage appropriée lors du test, ou si les résultats de vos tests n'apparaissent pas dans votre recherche, veuillez contacter l'assistance Cisco Umbrella.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.