Understand the Internet Watch Foundation Content Category

Contents

Introduction

This document describes the Internet Watch Foundation (IWF) content filtering category in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on 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. If your network is live, ensure that you understand the potential impact of any command.

Overview

As part of Cisco Umbrella's commitment to providing the best possible Internet security and filtering, this article introduces a category of content filtering to Umbrella: the Internet Watch Foundation (IWF).

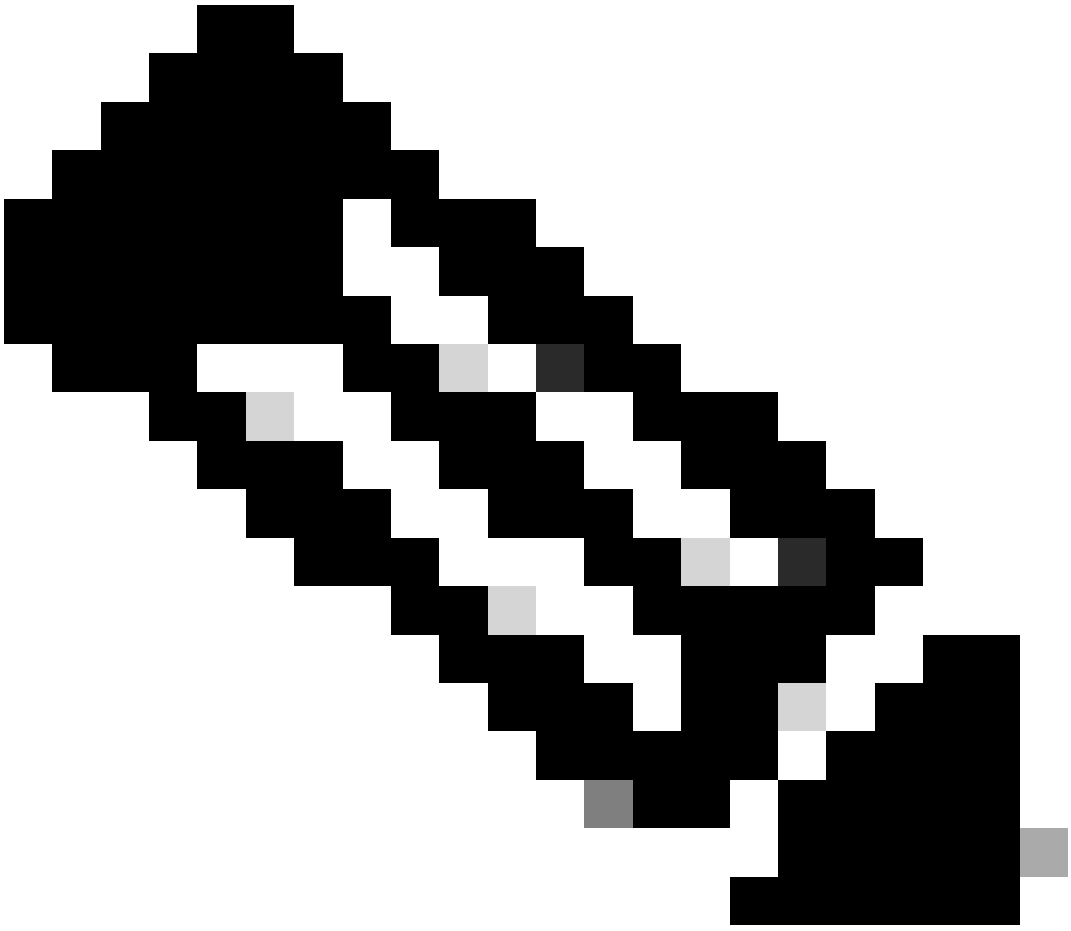
The IWF is a UK-based charitable organization whose mission is the elimination of child sexual abuse images online. The IWF maintains a list of blocked web pages to prevent internet users from accidentally finding child sexual abuse content. They supply partners with an accurate and current URL list to enable blocking of child sexual abuse content. Umbrella is adopting their list as a category that can be blocked in Umbrella. Read more about the work the IWF is doing.

Enable the IWF Category

The IWF's list is comprised of both domains and URLs. This means that some entries on the list can simply

be blocked using our standard DNS-based block list technology, whereas the URL-specific blocks requires that Umbrella's intelligent proxy is enabled. In order to block all the sites contained within the IWF content category, you are required to enable the intelligent proxy within your policies.

The intelligent proxy is explained in the Umbrella documentation. Essentially, it enables the ability to filter certain URLs as determined by our cloud-based proxy. By selectively and intelligently proxying certain traffic, Umbrella is able to easily filter the URL list from the IWF without slowing down or bottlenecking the speed of your Internet.



Note: The intelligent proxy and the IWF content category are only available to customers with certain Umbrella packages. The IWF content category and the Intelligent Proxy are also available to MSPs providing the "Umbrella for MSPs" package to their customers, and for any current Guest Wi-Fi/Secure hotspot package users (Roaming/branch/WLAN). If you do not see the Internet Watch Foundation (IWF) category listed in your Category Settings, please contact your account manager for this additional feature.

Configure the Internet Watch Foundation as a Content Category for Blocking

To set up IWF as a content category for blocking:

1. Enable Umbrella's intelligent proxy in your policies. The intelligent proxy is the ability for Umbrella to intercept and proxy requests for malicious files embedded within certain so-called "grey" domains.

- For instructions on how to enable the intelligent proxy, see the documentation for Enable the Intelligent Proxy.

2. Navigate to **Policies > Management> DNS Policies > Category Settings.**

3. In the list of **Categories to Block**, select **Internet Watch Foundation** and save your update.

Test the IWF Category and View Reports

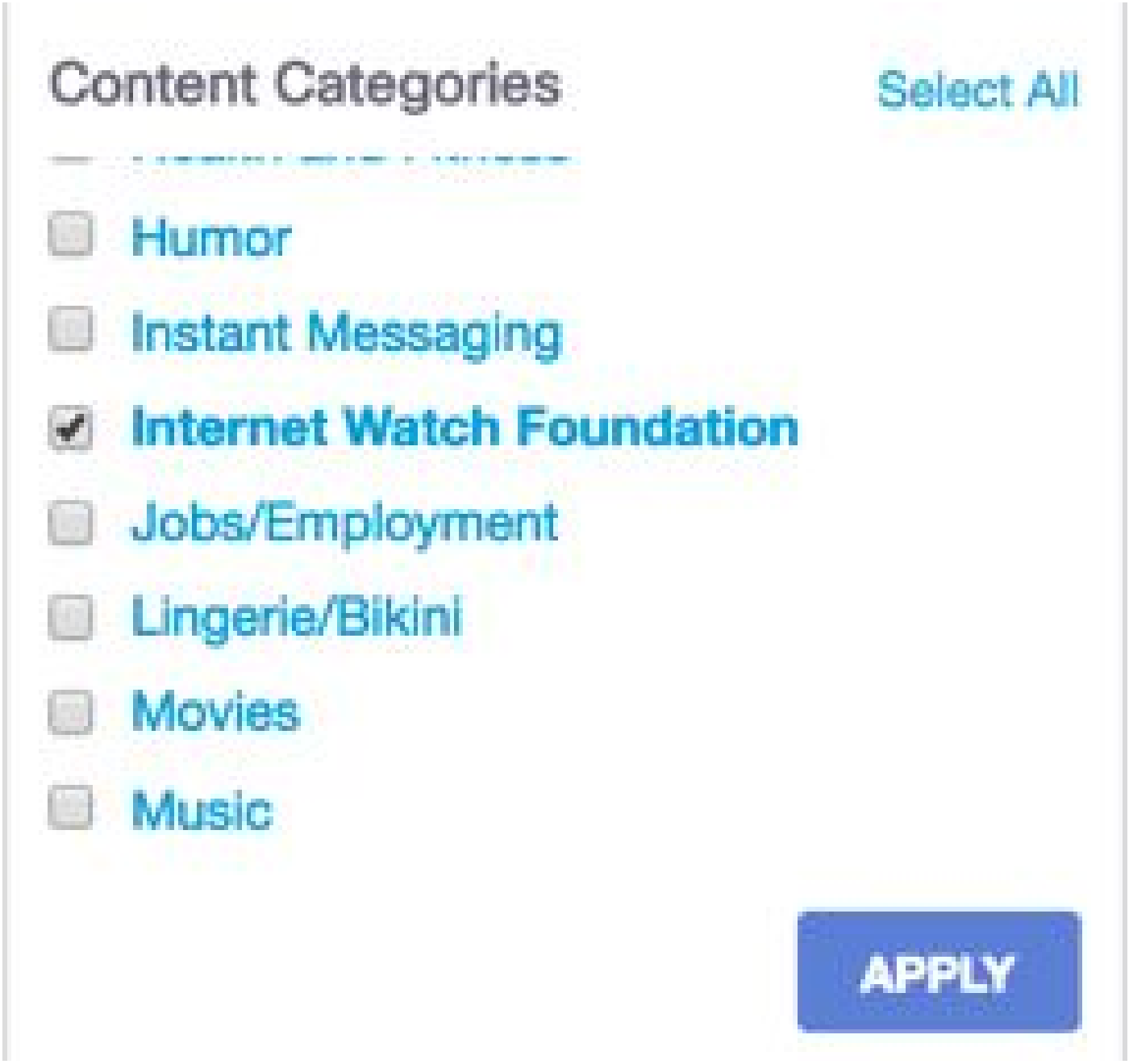
1. Umbrella set up a test domain to allow you to ensure that you have correctly configured your policies for the relevant identities that can have the URLs on the IWF list blocked. The test domain is http://proxy.opendnstest.com/iwf.htm.

- If your identities and policies are correctly configured, you can receive a block page as you can for any other content category block. The block page appearance can vary based on your configuration.

2. If you do not see a block page, check to ensure that the identity that you are testing with is correctly applied to the appropriate policy.

- If you see a page indicating you are not using the intelligent proxy, check your policies to ensure the intelligent proxy is enabled.
- If it is enabled but the IWF content category is not set to block, you can receive a page showing the text "IWF." In that case, please check to ensure the content category is enabled in your policies.

3. Once you tested it and you would like to check out your reports, apply a filter against a search in the **Activity Search** report:



115014821466

4. Your results can show any attempts made against our test page in the results.

5. If you are not seeing the appropriate block page when testing, or if the results of your tests are not appearing in your search, please contact Cisco Umbrella Support.