Troubleshooting y Verificación de la Categoría de URL en CSF

Contenido

Introducción

Este documento describe cómo verificar las asignaciones de categorías de URL en Secure Firewall y FMC para asegurarse de que el dispositivo utiliza la misma clasificación de URL.

Prerequisites

Debe tener la licencia de filtrado de URL habilitada para el dispositivo, la integración de servicios en la nube en un estado correcto y una política de control de acceso que incluya filtrado de URL y se haya implementado después de configurar la condición de URL.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Filtrado de URL y búsquedas por categorías de Firepower Management Center (FMC)
- Inspección del tráfico y evaluación de políticas de Cisco Secure Firewall (CSF)
- Categorización de URL y comportamiento de reputación, basado en Talos a partir de la versión 6.5 de CSF

Componentes Utilizados

Este documento describe la funcionalidad disponible en Cisco Secure Firewall y FMC versiones 6.5 y posteriores. Los ejemplos de esta guía utilizan la versión 7.6.5.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también se puede utilizar con estos productos y versiones:

- Centro de gestión de firewall seguro (FMC)
- Firewall seguro de Cisco (CSF)
- Integración de servicios en la nube y filtrado de URL

Antecedentes

El filtrado de URL se basa en una base de datos de categorías que se evalúa durante la inspección del tráfico. El FMC almacena la información de categoría de URL para un destino y el dispositivo realiza una búsqueda en tiempo de ejecución cuando se inspecciona el tráfico. Cuando hay una discordancia entre el FMC, el dispositivo o la base de datos en la nube, los resultados de las políticas pueden parecer incoherentes incluso cuando la política de control de acceso está configurada correctamente.

Una parte importante de la verificación es confirmar que la asignación de categoría de URL es coherente en todo el FMC y el dispositivo. La búsqueda de la categoría de URL está influenciada por la configuración de integración de servicios en la nube y la caché del dispositivo. Si la configuración de actualización de caché está deshabilitada o la duración de la entrada es demasiado larga, los datos de categoría obsoletos pueden seguir en uso después de que Talos actualice la clasificación.

Arquitectura

Cuando el filtrado de URL está activado, el dispositivo comprueba primero la caché de URL local. Si la categoría aún no está presente en la caché, el dispositivo puede consultar la base de datos local o la nube de Cisco. El dispositivo utiliza su base de datos de URL local y la caché de búsqueda durante la inspección, y beakerd se comunica con Talos para descargar y actualizar los datos de filtrado de URL. En los dispositivos gestionados por FMC, el freno se ejecuta en el FMC y se encuentra en estado de espera en el CSF. Si el CSF se administra localmente, el proceso se ejecuta en el propio dispositivo.

Talos envía paquetes de bases de datos completos en varios tamaños, que se almacenan en /var/sf/cloud_download/cisco.

Estos son algunos ejemplos de cómo pueden verse los archivos de base de datos de Talos:

- cisco_uridb_large_154154243 (500 MB)
- cisco_uridb_medium_154153645 (125 MB)
- cisco_uridb_small_154153061 (33 MB)

Nota: Los archivos de la base de datos comienzan con cisco_uridb y luego se muestra el tamaño (pequeño, mediano o grande). Los tamaños pueden variar en función del hardware que se utilice.

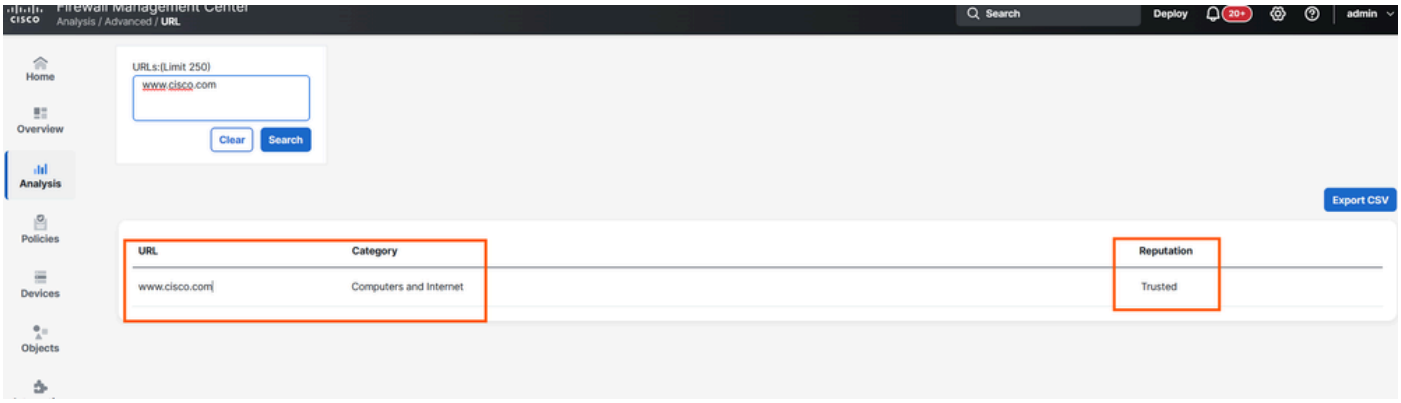
Paso 1: Buscar la categoría de URL en FMC

El FMC mantiene una base de datos de URL local que asigna los destinos de URL a sus categorías asignadas. Este es el primer paso recomendado para validar cómo se clasifica una URL.

Navegue hasta la ubicación Analysis > Advanced > URL en el FMC.

Introduzca la URL que desea investigar y revise su categoría asignada.

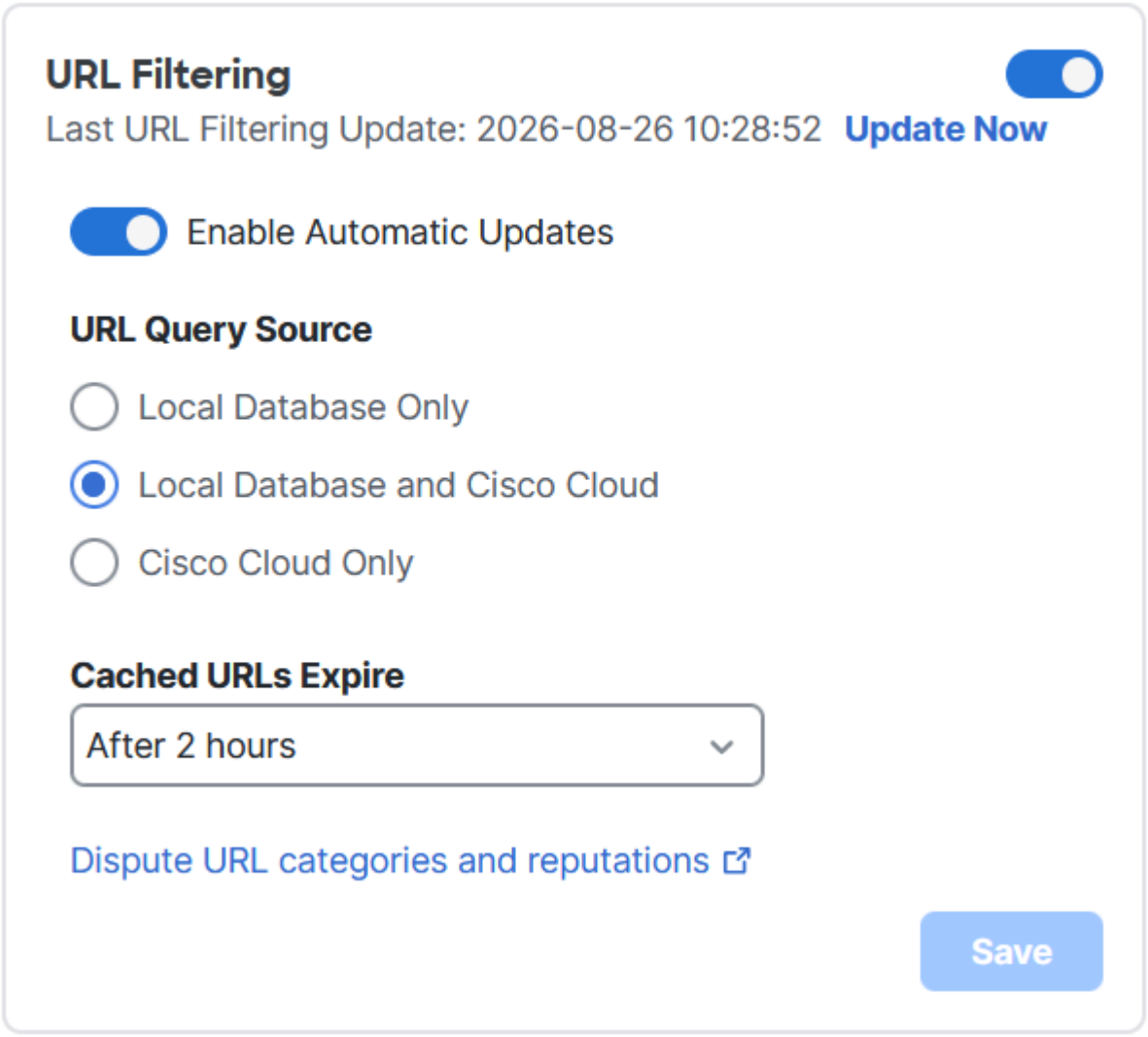
En el ejemplo que se muestra a continuación, www.cisco.com aparece en la categoría Computers and Internet (Ordenadores e Internet).



Paso 2: Revisar configuración de integración de filtrado de URL

La configuración de integración de filtrado de URL determina dónde el FMC y el dispositivo CSF generan su base de datos de categorías de URL. Cada dispositivo mantiene su propia base de datos local para la búsqueda de URL y puede consultar la nube de Cisco para obtener inteligencia de URL adicional o actualizada.

Vaya a Integration > Other Integrations > Cloud Services en FMC para revisar estos ajustes.



Verifique que la integración esté en buen estado y que la caché de búsqueda de URL esté configurada para actualizarse según el tiempo de política esperado.

⚠ Precaución: La caché de búsqueda de URL puede conservar los resultados de categoría y reputación previamente recuperados. Si la caducidad de la memoria caché está deshabilitada o configurada con una vida útil prolongada, el dispositivo puede seguir usando la información almacenada en la memoria caché después de que Talos actualice la clasificación, lo que puede hacer que el resultado del dispositivo difiera temporalmente de la búsqueda actual de FMC o Talos.

Paso 3: Confirme la categoría de URL en el dispositivo mediante el seguimiento de compatibilidad del sistema

Para verificar que el dispositivo CSF categoriza la URL de la misma manera que FMC, ejecute un

seguimiento de compatibilidad del sistema desde la CLI del dispositivo. Muestra cómo el motor de inspección de Snort evalúa el tráfico y qué categoría de URL se devuelve cuando se inspecciona la conexión.

En la CLI de FTD, ingrese el comando system support trace y responda a las indicaciones interactivas:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```

Nota: En este ejemplo, 173.37.145.84 es la dirección IP para www.cisco.com. Utilice la dirección IP de destino que corresponda a la URL que está investigando.

Ejemplo de salida:

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 20

192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90,
```

En este resultado, la dirección URL devuelve un id. de categoría de 2003. En el paso siguiente se explica cómo resolver ese valor numérico en el nombre de categoría correspondiente.

Paso 4: Convertir el número de categoría en un nombre de categoría

La búsqueda de categorías de URL en el dispositivo devuelve un ID de categoría numérica. Para asignar ese número a un nombre de categoría legible por las personas, abra el archivo aup_categories.json en el dispositivo.

Navegue hasta el directorio /var/sf/cloud_download/ en el CSF en el modo experto. Asegúrese de que se encuentra en el modo de usuario raíz.

Abra el archivo de definiciones de categoría:

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

Busque el identificador de categoría devuelto en el resultado de seguimiento. Ejemplo de entrada para la categoría 2003:

```
{
"id": 2003,
"uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
"mnemonic": "comp",
"name": "Computers and Internet",
"type": "aup_cats",
"state": "active"
}
```

Nota: Los números de ID de categoría son uniformes en todos los dispositivos CSF. La misma ID numérica se asigna al mismo nombre de categoría en cada dispositivo CSF.

Verificación

Utilice los resultados de los pasos 1 a 4 para confirmar que la asignación de categoría de URL es coherente entre la base de datos de FMC y el motor Snort del dispositivo.

En este ejemplo:

- La base de datos de FMC enumera www.cisco.com como Computers and Internet (Ordenadores e Internet).
- La CLI del dispositivo devuelve el Id. de categoría 2003, que se asigna a Equipos e Internet.

Ambas fuentes están de acuerdo, lo que confirma que la política de filtrado de URL que se está aplicando es coherente para esta URL.

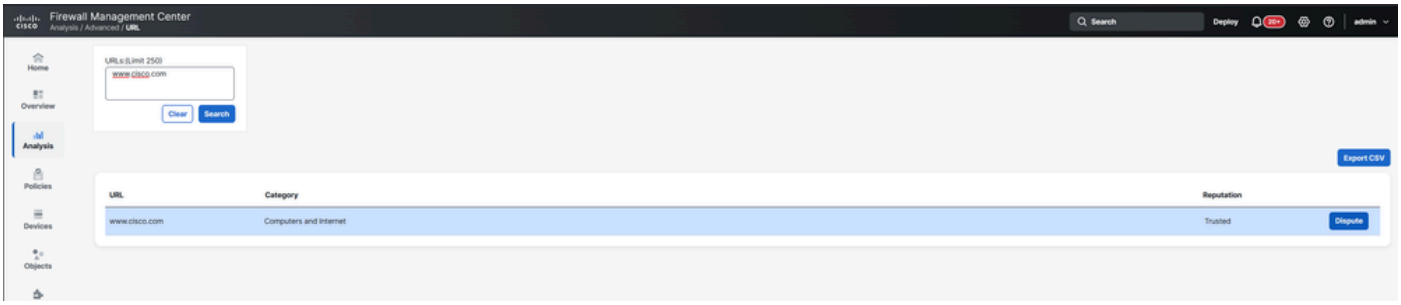
Botón de disputa

Si crees que una URL se ha clasificado en una categoría incorrecta, puedes enviar una disputa a

Talos.

Vaya a Analysis > Advanced > URL en FMC:

Escriba la URL, haga clic en Buscar, pase el cursor sobre la entrada URL y seleccione Dispute.



Esto abre la página de disputas de Talos para que la clasificación pueda ser revisada y corregida por la fuente apropiada.

Troubleshoot

Si la clasificación no coincide con las expectativas, revise estas áreas:

- Confirme que la licencia de filtrado de URL está habilitada y asignada al dispositivo.
- Verifique el estado de los servicios en la nube y la conexión con Talos.
- Inspeccione la configuración de actualización de caché y caché del dispositivo para confirmar que las entradas obsoletas no se están reutilizando.
- Compruebe si el proceso interrumpido se está ejecutando en el FMC para dispositivos gestionados por FMC.

En el caso de los dispositivos gestionados por FMC, ejecute este comando en el modo experto de FMC para confirmar que el proceso está activo:

```
pmtool status | grep beakerd
```

Nota: Si ejecuta este comando en un firewall seguro gestionado por FMC, el proceso se puede ver en estado de espera. Si Secure Firewall se administra localmente, el proceso se ve en estado de ejecución.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).