Preguntas frecuentes sobre la puntuación de reputación en la Web (WBRS) y el motor de categorización web (FAQ)

Contenido

Puntuación de reputación en la Web (WBRS) y Preguntas frecuentes sobre el motor de categorización web (FAQ).

En este artículo se describen las preguntas más frecuentes sobre la puntuación de reputación en la Web (WBRS) y la función de categorización con Cisco Web Security Appliance (WSA).

¿Qué significa la puntuación de reputación en la Web?

Web Reputation Filters asigna una puntuación de reputación basada en Web (WBRS) a una URL para determinar la probabilidad de que contenga malware basado en URL. El dispositivo de

seguridad web utiliza puntuaciones de reputación web para identificar y detener los ataques de malware antes de que se produzcan. Puede utilizar los filtros de reputación web con las políticas de acceso, descifrado y seguridad de datos de Cisco.

¿Qué significa la categorización web?

Los sitios web de Internet son categorías basadas en el comportamiento y el propósito de estos sitios web, para facilitar a los administradores de los proxies, hemos agregado cada URL de sitio web a una categoría predefinida, donde se puede identificar por motivos de seguridad y generación de informes. los sitios web que no pertenecen a una de las categorías predefinidas, se denominan sitios web no categorizados, que pueden ser debido a la creación de nuevos sitios web y a la falta de datos/tráfico suficientes para determinar su categoría. y esto cambia según el tiempo.

¿Cómo se encuentra la puntuación de reputación en los registros de acceso?

Cada solicitud que realice a través de Cisco Web Security Appliance (WSA) debe tener una puntuación de reputación basada en Web (WBRS) y una categoría de URL adjuntas. y una de las maneras de verlo es a través de los registros de acceso, a continuación se muestra el ejemplo: la puntuación de reputación basada en Web (WBRS) es (-1.4) y la categoría de URL es: Ordenadores e Internet.

Referencia de texto para la captura de pantalla anterior.

1563214694.033 117 xx.xx.xx.xx TCP_MISS/302 1116 GET https://example.com - DIRECT/example.com text/html
DEFAULT_CASE_12-DefaultGroup-DefaultGroup-NONE-NONE-NONE-DefaultGroup-NONE ,0,"-",0,0,0,-,"-",-,-,-,"-","-,-,-,"-","-",-,-,IW_comp,-,"-","-","Unknown","Unknown","-","-",76.31,0,-,"Unknown","-",-,"-","-",-,-,"-",-> -

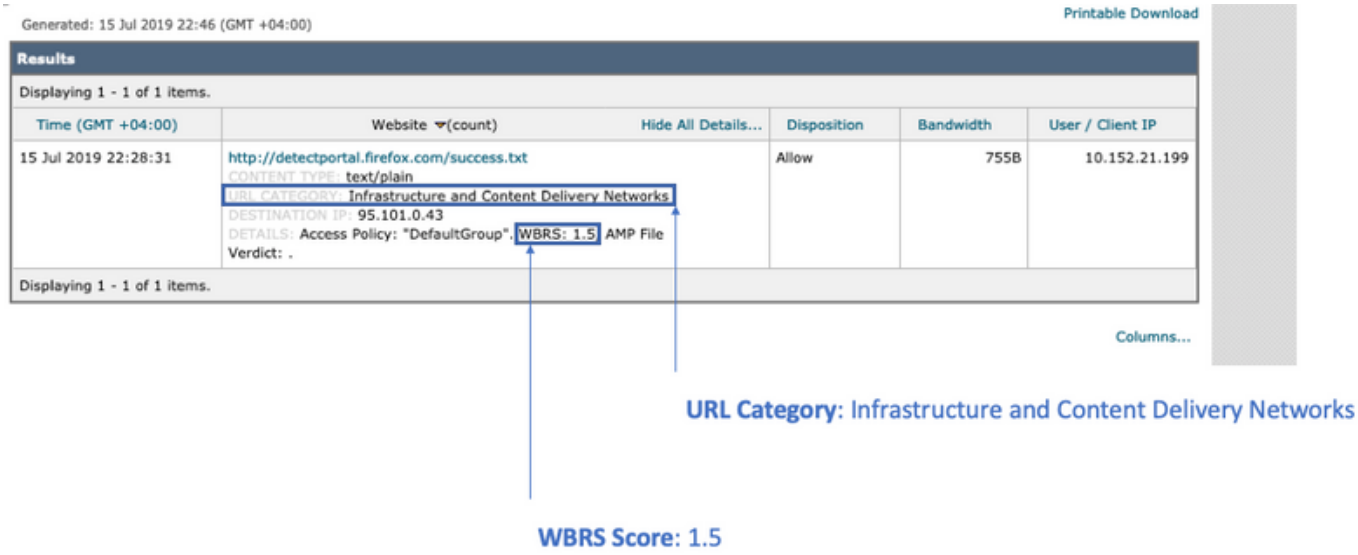
Notas:

- Los registros de acceso se pueden ver desde la interfaz de línea de comandos (CLI) o descargarse mediante el método FTP (protocolo de transferencia de archivos) en la IP de la interfaz de administración. (asegúrese de que FTP esté habilitado en la interfaz).
- Lista completa de abreviaturas de categorías: https://www.cisco.com/c/en/us/td/docs/security/wsa/wsa11-7/user_guide/b_WSA_UserGuide_11_7/b_WSA_UserGuide_11_7_chapter_01001.html#con_1208638

¿Cómo se encuentra la puntuación de reputación en mis

informes?

1. Vaya a la **GUI** de Cisco Web Security Appliance (WSA) -> **Reporting** -> **Web Tracking**.
2. Busque el **dominio** que busca.
3. En la página **Resultados**, haga clic en el enlace necesario y se mostrarán más detalles como se muestra a continuación.



¿Dónde comprueba los registros de actualizaciones de la puntuación de reputación basada en Web (WBRS)?

Los registros de actualizaciones de la puntuación de reputación basada en Web (WBRS) se pueden encontrar en los registros updater_logs; puede descargar estos registros mediante el inicio de sesión del protocolo de transferencia de archivos (FTP) en la interfaz de administración. o mediante la interfaz de línea de comandos (CLI).

Para ver registros mediante terminal:

1. Abra **Terminal**.
2. Escriba la **cola de** comando.
3. Elija el **número de registros** (varía según la versión y el número de registros configurados).
4. Se mostrarán los registros.

```
WSA.local (SERVICE)> tail

Currently configured logs:
1. "xx.xx.xx.xx" Type: "Configuration Logs" Retrieval: FTP Push - Host
xx.xx.xx.xx
2. "Splunk" Type: "Access Logs" Retrieval: FTP Poll
3. "accesslogs" Type: "Access Logs" Retrieval: FTP Push - Host xx.xx.xx.xx
4. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
5. "archiveinspect_logs" Type: "ArchiveInspect Logs" Retrieval: FTP Poll
....
43. "uds_logs" Type: "UDS Logs" Retrieval: FTP Poll
44. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
45. "upgrade_logs" Type: "Upgrade Logs" Retrieval: FTP Poll
46. "wbnp_logs" Type: "WBNP Logs" Retrieval: FTP Poll
```

```
47. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
48. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
49. "webtapd_logs" Type: "Webtapd Logs" Retrieval: FTP Poll
50. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval: FTP
Poll
Enter the number of the log you wish to tail.
[]> 44

Press Ctrl-C to stop scrolling, then `q` to quit.
Mon Jul 15 19:24:04 2019 Info: mcafee updating the client manifest
Mon Jul 15 19:24:04 2019 Info: mcafee update completed
Mon Jul 15 19:24:04 2019 Info: mcafee waiting for new updates
Mon Jul 15 19:36:43 2019 Info: wbrs preserving wbrs for upgrades
Mon Jul 15 19:36:43 2019 Info: wbrs done with wbrs update
Mon Jul 15 19:36:43 2019 Info: wbrs verifying applied files
Mon Jul 15 19:36:58 2019 Info: wbrs Starting heath monitoring
Mon Jul 15 19:36:58 2019 Info: wbrs Initiating health check
Mon Jul 15 19:36:59 2019 Info: wbrs Healthy
Mon Jul 15 19:37:14 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:15 2019 Info: wbrs Healthy
Mon Jul 15 19:37:30 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:31 2019 Info: wbrs Healthy
Mon Jul 15 19:37:46 2019 Info: wbrs Initiating health check
Mon Jul 15 19:37:47 2019 Info: wbrs Healthy
Mon Jul 15 19:38:02 2019 Info: wbrs updating the client manifest
Mon Jul 15 19:38:02 2019 Info: wbrs update completed
Mon Jul 15 19:38:03 2019 Info: wbrs waiting for new updates
Mon Jul 15 20:30:23 2019 Info: Starting scheduled release notification fetch
Mon Jul 15 20:30:24 2019 Info: Scheduled next release notification fetch to occur at Mon Jul 15
23:30:24 2019
Mon Jul 15 23:30:24 2019 Info: Starting scheduled release notification fetch
Mon Jul 15 23:30:25 2019 Info: Scheduled next release notification fetch to occur at Tue Jul 16
02:30:25 2019
```

¿Cómo verifica si tiene conectividad con Puntuación de reputación basada en Web (WBRS) actualiza los servidores?

Para asegurarse de que su dispositivo de seguridad Cisco Web Security Appliance (WSA) pueda obtener las nuevas actualizaciones. compruebe que dispone de conectividad con los servidores de actualización de Cisco en los siguientes puertos de protocolo de control de transmisión (TCP) 80 y 443:

```
wsa.local (SERVICE)> telnet updates.ironport.com 80
Trying xx.xx.xx.xx...
Connected to updates.ironport.com.
Escape character is '^]'.

wsa.calo (SERVICE)> telnet upgrades.ironport.com 80
Trying xx.xx.xx.xx...
Connected to upgrades.ironport.com.
Escape character is '^]'.
```

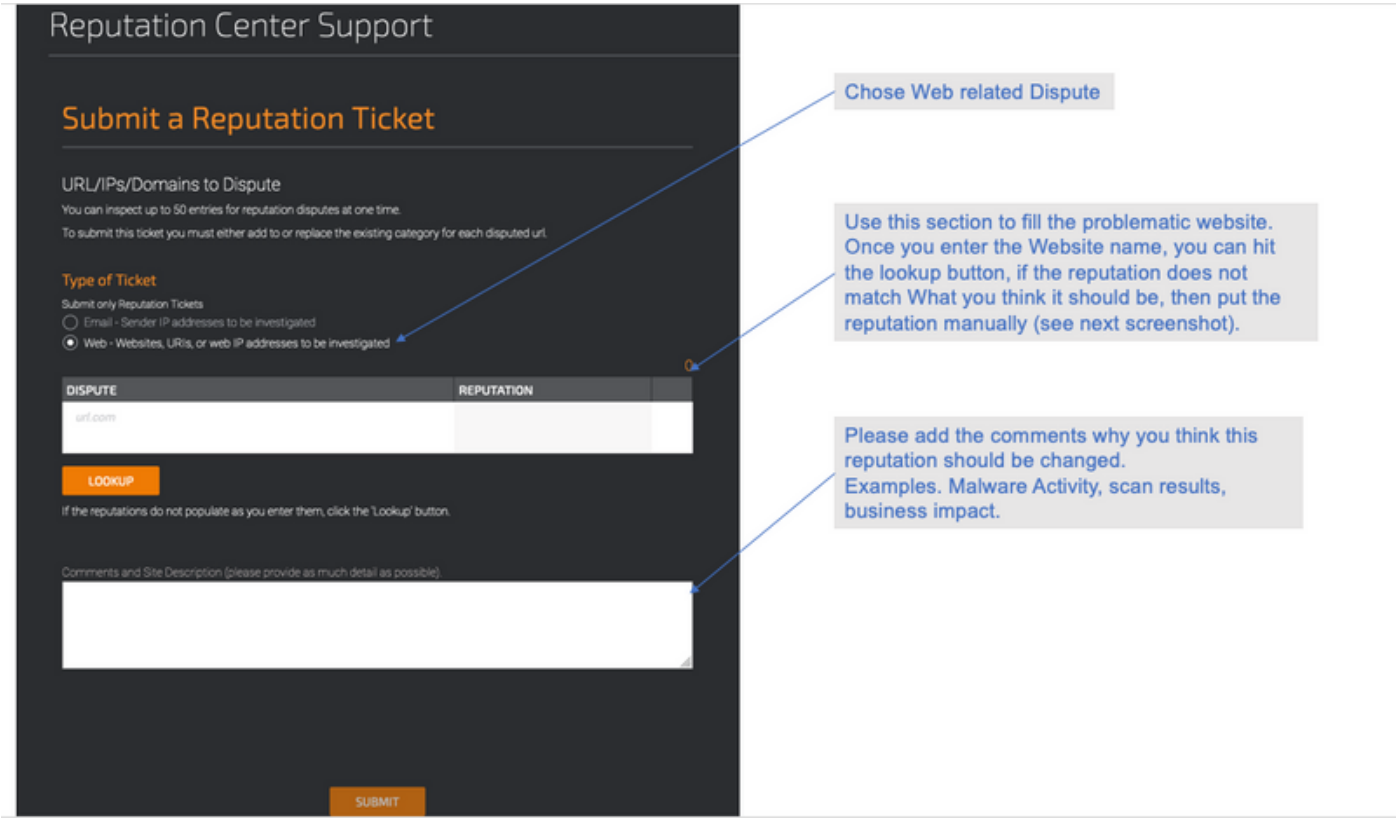
Nota: Si tiene algún proxy upstream, realice las pruebas anteriores a través de su proxy upstream.

¿Cómo archiva una disputa para la categorización web?

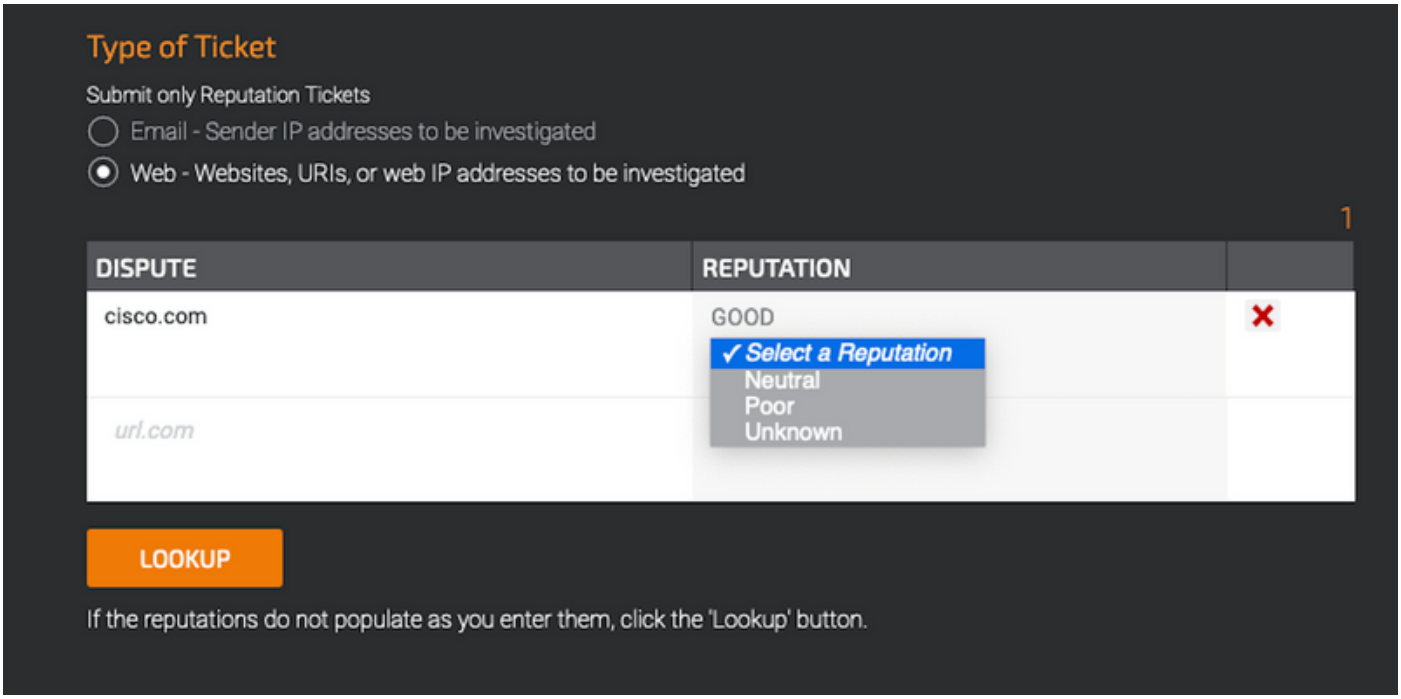
Después de comprobar que tanto Cisco Web Security Appliance (WSA) como Cisco TALOS tienen la misma puntuación de reputación, pero todavía cree que este no es un resultado válido, es necesario solucionarlo enviando una disputa al equipo de Cisco TALOS.

Esto se puede hacer mediante el siguiente enlace:
https://talosintelligence.com/reputation_center/support

Para **enviar** la **disputa**, siga estas instrucciones.



Resultados tras acceder a Búsqueda y la opción para cambiar manualmente la puntuación.



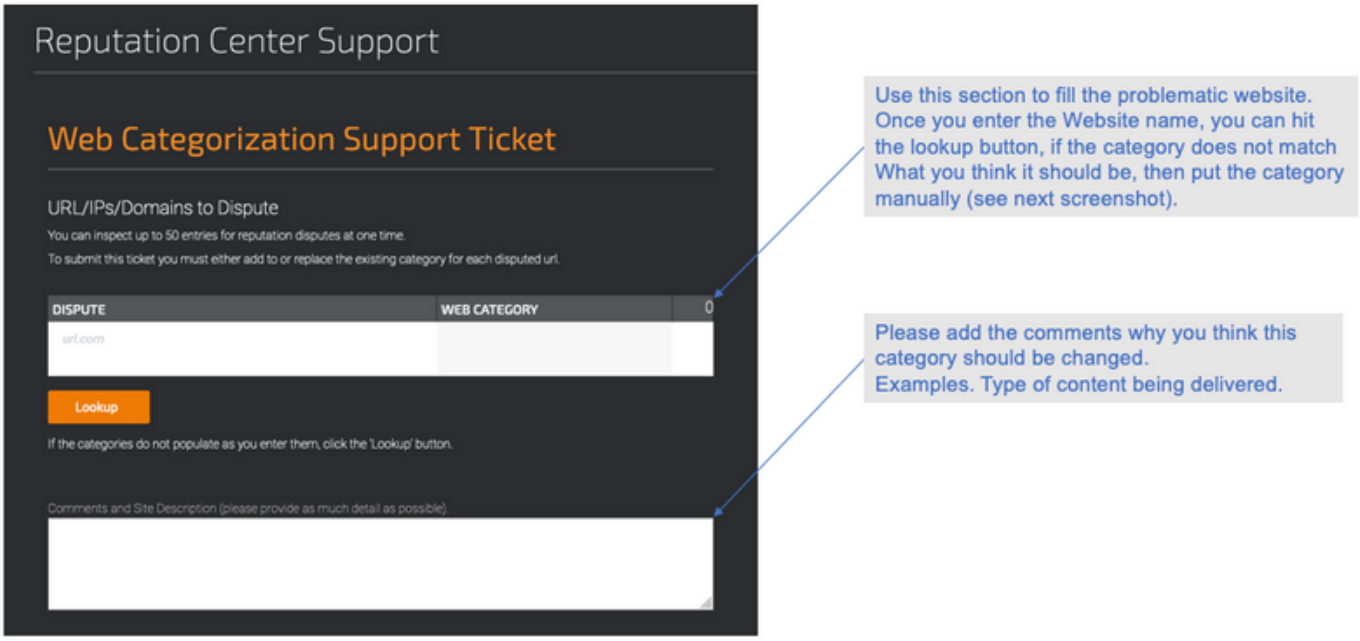
Nota: Los envíos de Cisco TALOS pueden tardar algún tiempo en reflejarse en la base de datos, si el problema es urgente, siempre puede crear un **WHITELIST** o **BLOCKLIST**, como solución temporal hasta que el problema se solucione desde el motor de Cisco. para ello, puede comprobar esta sección (Cómo escribir la lista blanca o la URL de la lista negra).

¿Cómo archiva la disputa por la puntuación de Web Reputation?

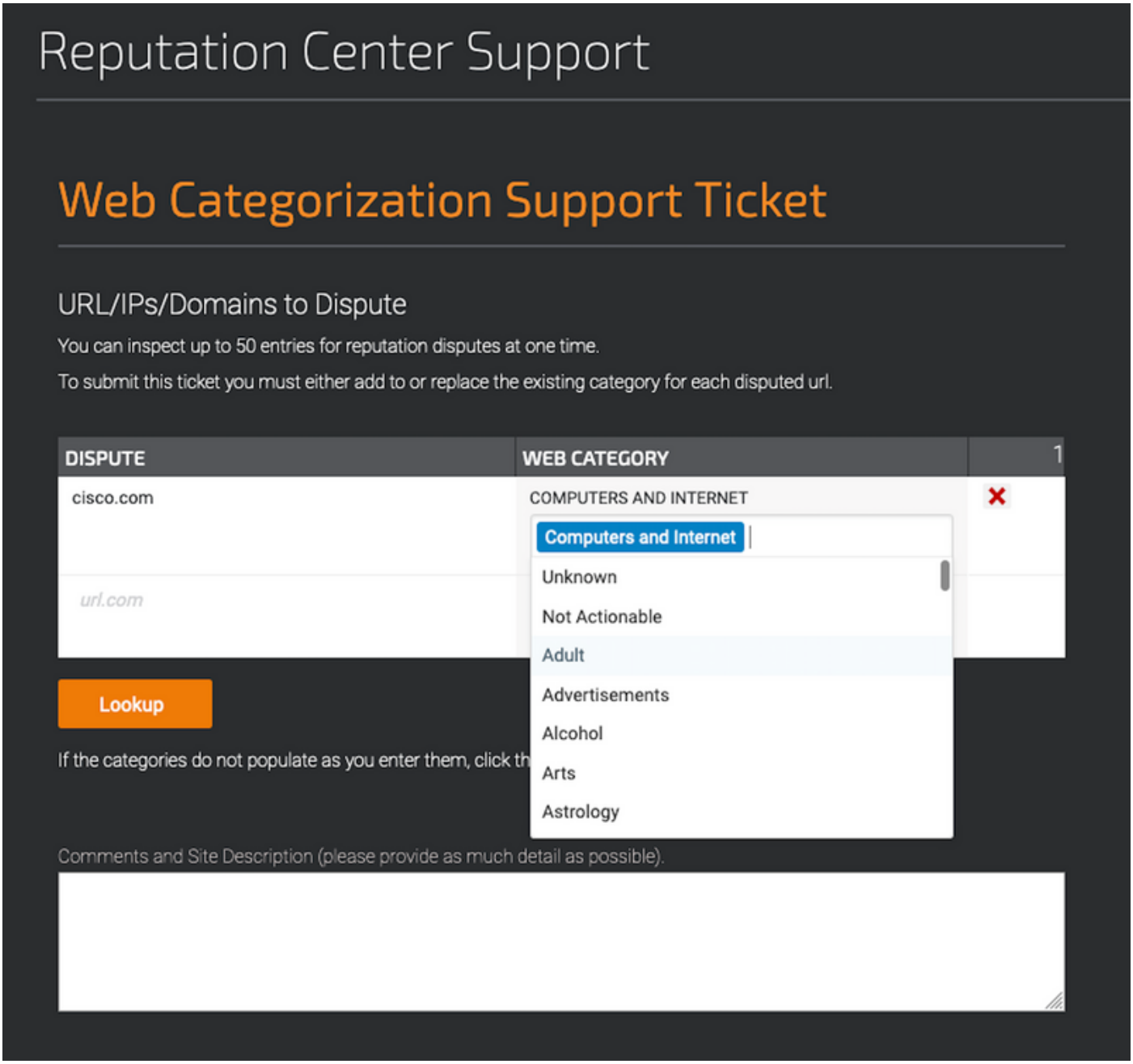
Después de comprobar que tanto Cisco Web Security Appliance (WSA) como Cisco TALOS cuentan con la misma categorización, pero todavía cree que no se trata de un resultado válido, esto debe solucionarse enviando una disputa al equipo de Cisco TALOS.

Vaya a la página de envío de categorización en el sitio web de TALOS: https://talosintelligence.com/reputation_center/support#categorization

Para **enviar** la **disputa**, siga estas instrucciones.



Para actualizar la Categoría, elija en el menú **desplegable** lo que considere conveniente para el sitio web, y asegúrese de seguir las pautas de comentarios.



Se ha presentado una disputa, pero la puntuación o categoría no se está actualizando en Cisco Web Security Appliance (WSA) o Cisco TALOS.

En caso de que haya presentado un caso con Cisco TALOS y la reputación/puntuación no se haya actualizado en un plazo de 3-4 días. puede comprobar la configuración de las actualizaciones y asegurarse de que dispone de disponibilidad para el servidor de la actualización de Cisco. si todos estos pasos fueron correctos, puede continuar y abrir un ticket con el TAC de Cisco, y el ingeniero de Cisco le ayudará en el seguimiento con el equipo de Cisco TALOS.

> **Nota:** puede aplicar la solución WHITELIST/BLOCKLIST para aplicar la acción necesaria hasta que el equipo de Cisco TALOS actualice la categoría/reputación.

Dispositivo de seguridad Cisco Web Security Appliance

(WSA) mostrando resultados diferentes a los de Cisco TALOS, ¿cómo solucionar esto?

La base de datos puede estar obsoleta en el dispositivo de seguridad Cisco Web Security Appliance (WSA) debido a varias razones, principalmente la comunicación con nuestros servidores de actualizaciones. Siga estos pasos para verificar que dispone de servidores de actualización y conectividad correctos.

1. Compruebe que dispone de conectividad para los servidores de actualización de Cisco en los puertos 80 y 443:

```
wsa.local (SERVICE)> telnet updates.ironport.com 80
Trying xx.xx.xx.xx...
Connected to updates.ironport.com.
Escape character is '^]'.

wsa.calo (SERVICE)> telnet upgrades.ironport.com 80
Trying xx.xx.xx.xx...
Connected to upgrades.ironport.com.
Escape character is '^]'.
```

2. Si tiene algún proxy upstream, asegúrese de que el proxy upstream se asegure de realizar las pruebas anteriores a través de su proxy upstream.

3. Si la conectividad está bien y todavía ve la diferencia, fuerce las actualizaciones manualmente: **actualización** desde la CLI o desde la **GUI->Servicios de seguridad -> Protección frente a malware -> actualización**.

Espere unos minutos y, si no funciona, compruebe el paso siguiente.

4. En este momento, deberá comprobar el archivo updater_logs: **terminal** abierto**: CLI->tail-> (elija el número de archivo de registro updater_logs.)** esto hará que los registros de actualización muestren sólo las líneas nuevas.

Las líneas de registro deben comenzar con esta línea "**Comando remoto recibido para indicar una actualización manual**":

```
Mon Jul 15 19:14:12 2019 Info: Received remote command to signal a manual
update
Mon Jul 15 19:14:12 2019 Info: Starting manual update
Mon Jul 15 19:14:12 2019 Info: Acquired server manifest, starting update 342
Mon Jul 15 19:14:12 2019 Info: wbrs beginning download of remote file
"http://updates.ironport.com/wbrs/3.0.0/ip/default/1563201291.inc"
Mon Jul 15 19:14:12 2019 Info: wbrs released download lock
Mon Jul 15 19:14:13 2019 Info: wbrs successfully downloaded file
"wbrs/3.0.0/ip/default/1563201291.inc"
Mon Jul 15 19:14:13 2019 Info: wbrs started applying files
Mon Jul 15 19:14:13 2019 Info: wbrs started applying files
Mon Jul 15 19:14:13 2019 Info: wbrs applying component updates
Mon Jul 15 19:14:13 2019 Info: Server manifest specified an update for mcafee
Mon Jul 15 19:14:13 2019 Info: mcafee was signalled to start a new update
Mon Jul 15 19:14:13 2019 Info: mcafee processing files from the server manifest
Mon Jul 15 19:14:13 2019 Info: mcafee started downloading files
Mon Jul 15 19:14:13 2019 Info: mcafee waiting on download lock
```

5. Compruebe si hay algún mensaje "**Crítico/Advertencia**", los registros de actualización son

errores legibles por humanos y muy probablemente le guiarán dónde está el problema.

6. Si no hubo respuesta, puede continuar y abrir una entrada con el soporte de Cisco con los resultados de los pasos anteriores, y estarán encantados de ayudarle.

¿Cómo se calculan las puntuaciones de reputación en la Web?

Algunos de los parámetros que se están considerando al asignar una puntuación a un sitio web específico:

- Datos de categorización de URL
- Presencia de código descargable
- Presencia de contratos de licencia de usuario final (EULA) largos y confusos
- Volumen global y cambios en el volumen
- Información del propietario de la red
- Historial de una URL
- Antigüedad de una URL
- Presencia en cualquier lista de bloqueo
- Presencia en cualquier lista permitida
- Tipos de URL de dominios populares
- Información del registrador de dominios
- información de dirección IP

¿Cuál es el rango de puntuación para cada categoría de reputación (buena, neutral, pobre)?

Rangos de reputación en la Web y sus acciones asociadas:

Políticas de acceso:

Puntuación	Acción	Descripción	Ejemplo:
-10 a -6.0 (Pobre)	Bloqueo	Mal sitio. La solicitud está bloqueada, y no más análisis de malware ocurre.	• URL descarga información sin. • permiso de usuario. • Auge repentino del volumen de URL. • URL es un tipo de dominio popular.
-5.9 a 5.9 (Neutra)	Análisis	Sitio indeterminado. La solicitud es pasado al motor DVS para análisis de malware adicional. El motor DVS escanea la solicitud y contenido de respuesta del servidor.	• URL creada recientemente que tiene un • dirección IP dinámica y contiene • contenido descargable. • Dirección IP del propietario de red que tiene • puntuación de reputación web positiva
6.0 a 10.0 (Bien)	Permiso	Buen sitio. Se permite la solicitud. No se requiere análisis de malware.	• La URL no contiene contenido descargable. • Dominio de gran volumen y reputación con u historial largo.

			• Dominio presente en varias listas de permitid • No hay enlaces a URL con una reputación deficiente.

Políticas de descifrado:

Puntuación	Acción	Descripción
-10 a -9.0 (Pobre)	Desplegar	Mal sitio. La solicitud se elimina sin que se envíe un aviso al usuario final. Uso este entorno con precaución.
-8.9 a 5.9 (Neutra)	Descifrar	Sitio indeterminado. La solicitud está permitida, pero la conexión está descifrada y las políticas de acceso se aplican al tráfico descifrado.
6.0 a 10.0 (Bien)	Paso	Buen sitio. La solicitud se transmite sin inspección ni descifrado.

Políticas de seguridad de datos de Cisco:

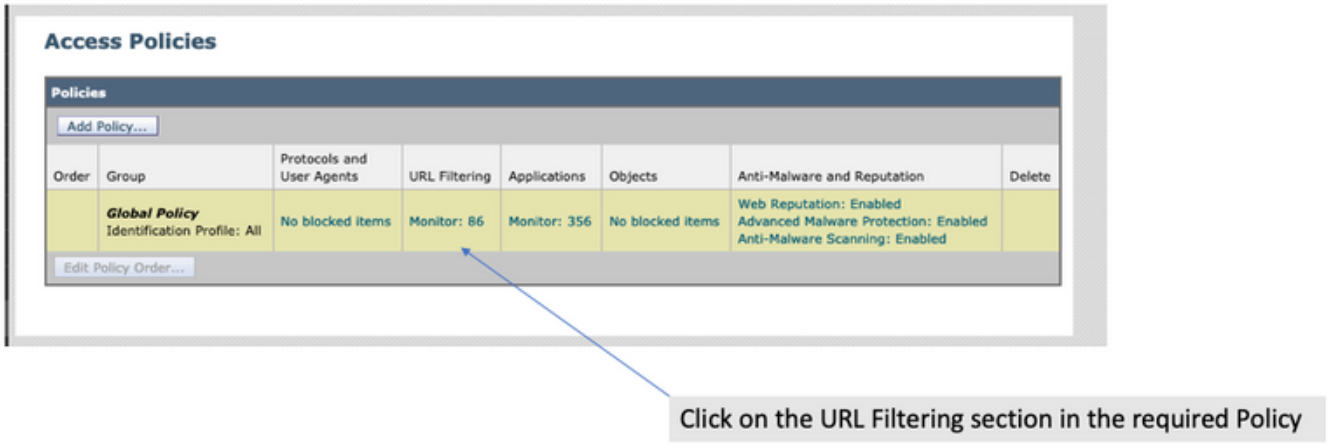
Puntuación	Acción	Descripción
-10 a -6.0 (Pobre)	Bloqueo	Mal sitio. La transacción está bloqueada y no se realiza ninguna exploración adicional.
-5.9 a 0.0 (Neutra)	Monitor	La transacción no se bloqueará en función de Web Reputation y continuará con las comprobacion contenido (tamaño y tipo de archivo). Nota Los sitios sin puntuación se monitorean.

¿Qué significa un sitio web sin categorías?

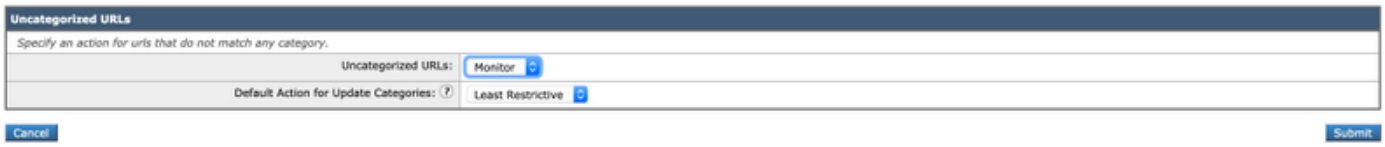
Las URL no categorizadas son las que la base de datos de Cisco no tiene suficiente información para confirmar su categoría. por lo general sitios web creados recientemente.

¿Cómo bloquea las URL no categorizadas?

1. Vaya a la política de acceso deseada: **Administrador de seguridad web -> Políticas de acceso**.



2. Desplácese hacia abajo hasta la sección URLs no categorizadas.



3. Elija una de las acciones deseadas, **Monitor**, **Block** o **Warn**.

4. **Enviar** y **Registrar** cambios.

¿Con qué frecuencia se actualiza la base de datos?

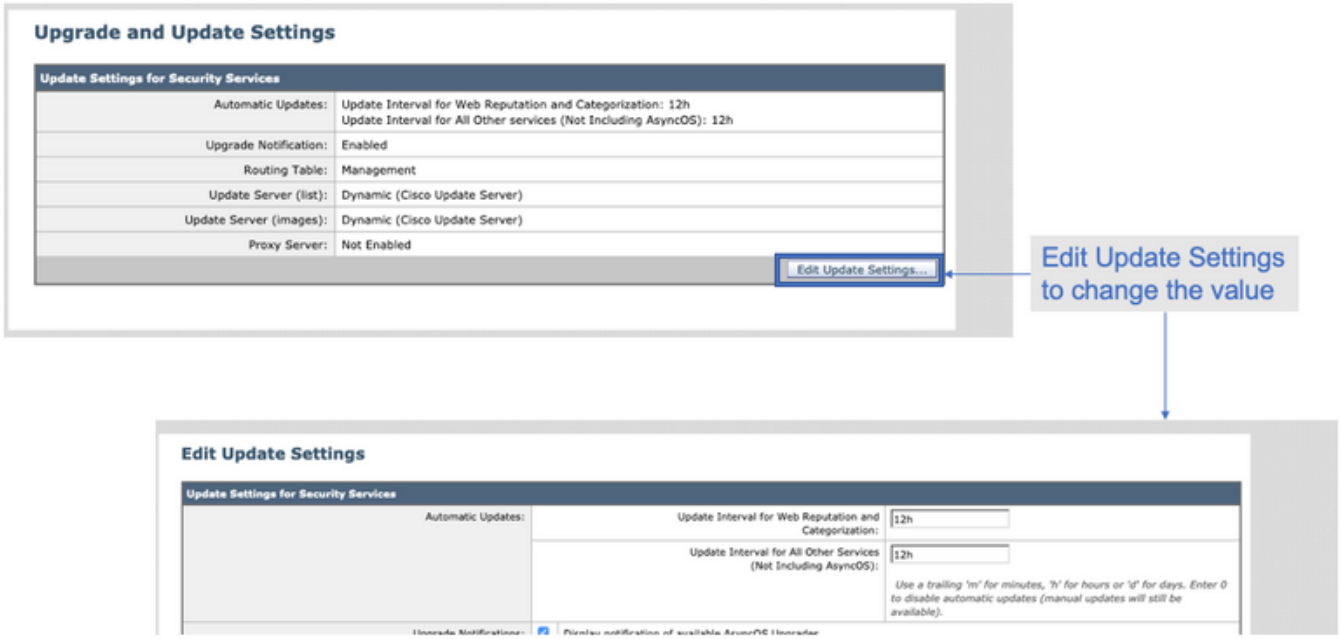
La frecuencia de comprobación de las actualizaciones se puede actualizar mediante el siguiente comando desde CLI: **updateconfig**

```
WSA.local (SERVICE)> updateconfig

Service (images): Update URL:

-------------------------------------------------------------------------------
Webroot Cisco Servers
Web Reputation Filters Cisco Servers
L4 Traffic Monitor Cisco Servers
Cisco Web Usage Controls Cisco Servers
McAfee Cisco Servers
Sophos Anti-Virus definitions Cisco Servers
Timezone rules Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:

-------------------------------------------------------------------------------
Webroot Cisco Servers
Web Reputation Filters Cisco Servers
L4 Traffic Monitor Cisco Servers
Cisco Web Usage Controls Cisco Servers
McAfee Cisco Servers
Sophos Anti-Virus definitions Cisco Servers
Timezone rules Cisco Servers
HTTPS Proxy Certificate Lists Cisco Servers
```

```
Cisco AsyncOS upgrades Cisco Servers

Update interval for Web Reputation and Categorization: 12h
Update interval for all other services: 12h

Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
The following services will use this routing table:
- Webroot
- Web Reputation Filters
- L4 Traffic Monitor
- Cisco Web Usage Controls
- McAfee
- Sophos Anti-Virus definitions
- Timezone rules
- HTTPS Proxy Certificate Lists
- Cisco AsyncOS upgrades

Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]>
```

> **Nota:** el valor anterior muestra la frecuencia con la que buscamos actualizaciones, pero no la frecuencia con la que lanzamos nuevas actualizaciones para la reputación y otros servicios. las actualizaciones pueden estar disponibles en cualquier momento.

O desde la GUI: **Administración del sistema -> Configuración de actualización y actualización.**



¿Cómo se muestra una lista blanca o una lista negra de URL?

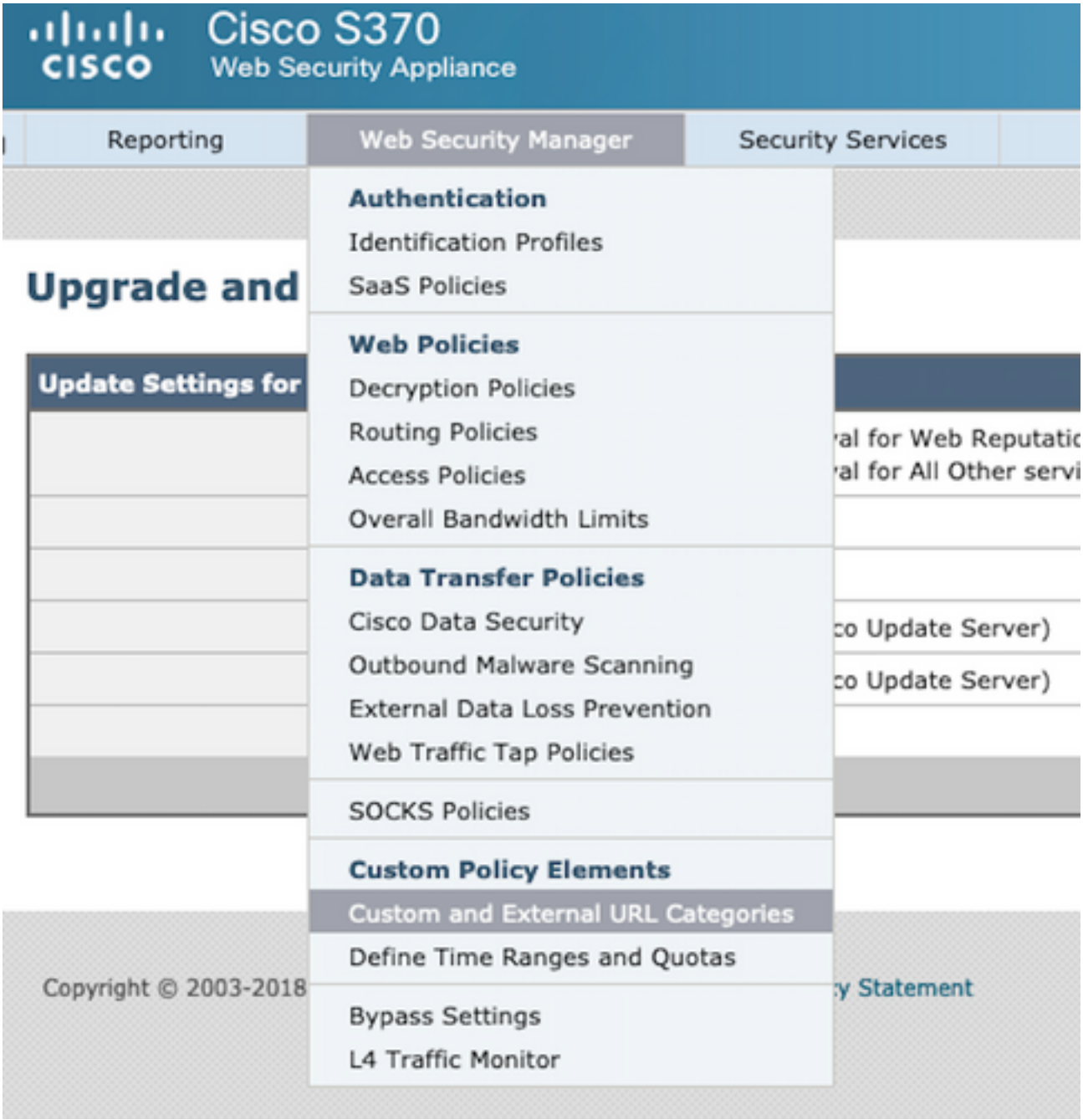
A veces, las actualizaciones de URL de Cisco TALOS toman tiempo, ya sea por falta de información suficiente. o no hay forma de cambiar la reputación, ya que el sitio web aún no ha

demostrado el cambio en el comportamiento malicioso. en este punto, puede agregar esta URL a una categoría de URL personalizada que permita/bloquee sus políticas de acceso o que se transfiera/descarte en su política de descifrado, y que garantice que la URL se entrega sin que el dispositivo de seguridad Cisco Web Security Appliance (WSA) o el bloque verifiquen el escaneo o el filtrado de URL.

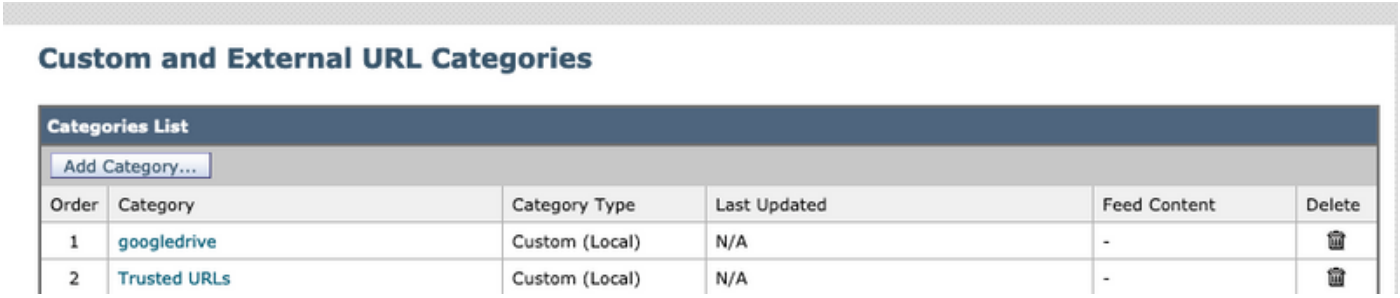
para la lista blanca/negra de una URL, siga estos pasos:

1. Agregar URL en la categoría de URL personalizada.

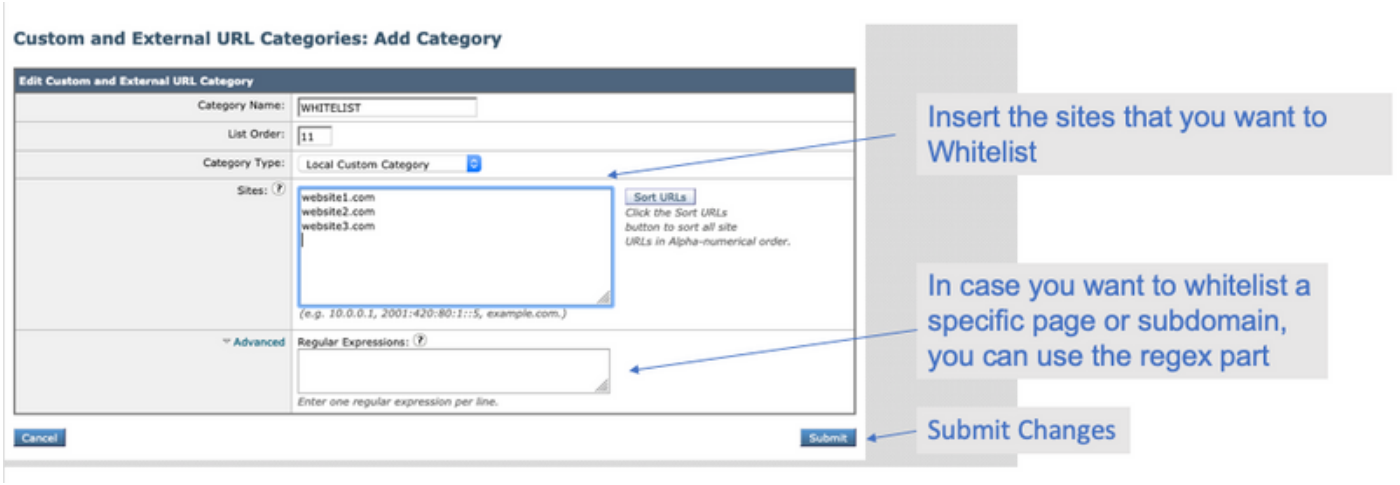
Desde la GUI vaya a **Web Security Manager -> Categoría de URL personalizada y externa**.



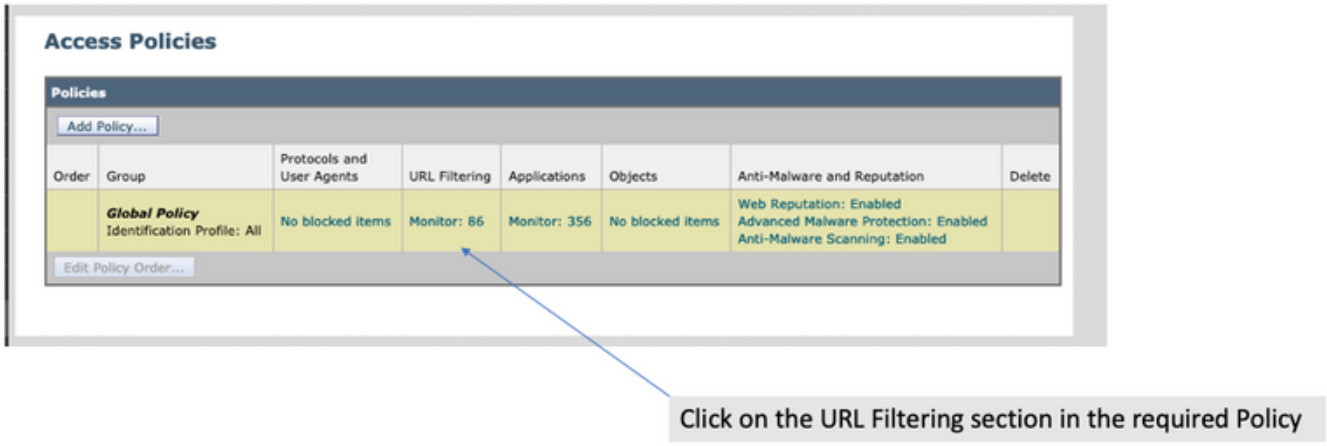
2. Haga clic en **Agregar categoría**:



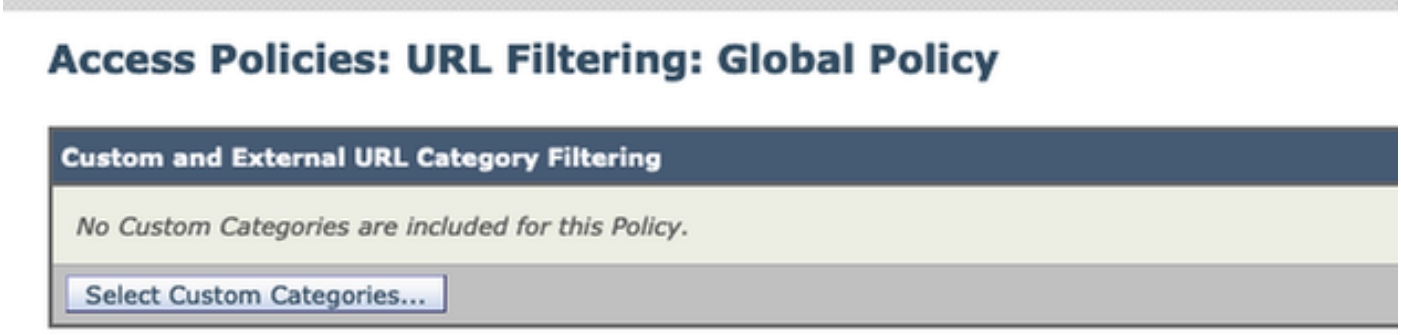
3. Agregue los sitios web similares a las capturas de pantalla siguientes:



4. Vaya al filtrado de URL en la política de acceso necesaria (**Web Security Manager -> Access Policies -> URL Filtering**).



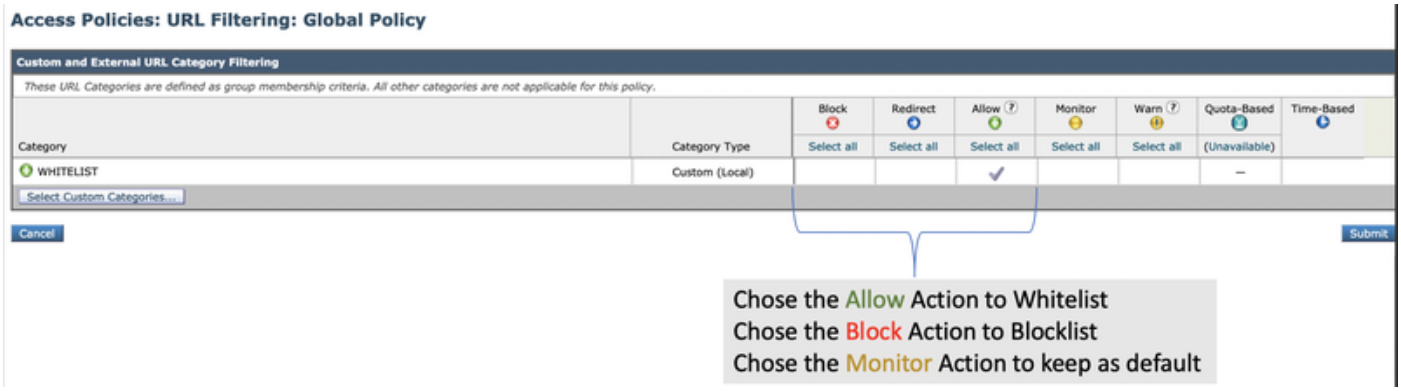
5. Seleccione el **WHITELIST o BLACKLIST** que acabamos de crear e insértelo en la política.



6. Incluya la categoría de política en la configuración de filtrado de URL de política como se

muestra a continuación.

7. Defina la acción, Block to Blocklist (Bloquear a lista de bloqueo), Allow to Whitelist (Permitir a lista blanca). y si desea que la URL pase por los motores de escaneo, mantenga la Acción como Monitor.



8. **Enviar** y **Registrar** cambios.