Cómo configurar los parámetros de paso a través adicionales del dispositivo de seguridad web para la aplicación Webex

Introducción

Este documento describe cómo configurar las políticas de omisión de Secure Web Appliance (SWA/WSA) para garantizar la funcionalidad adecuada de la aplicación Cisco Webex en condiciones especiales de implementación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Sistema operativo asíncrono para Secure Web Appliance 14.x o superior.
- Acceso de usuario de administración a la interfaz gráfica de usuario (GUI) de Secure Web Appliance.
- Administración Acceso de usuario a la interfaz de línea de comandos (CLI) de Secure Web Appliance.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Problema

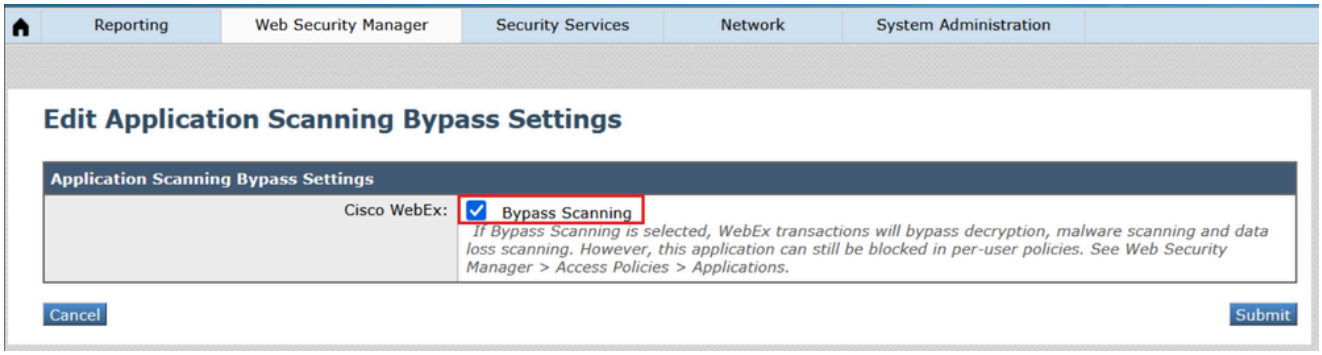
De acuerdo con la documentación pública de Webex sobre Requisitos de red para los servicios de Webex, el servidor proxy debe configurarse para permitir que el tráfico de señalización de Webex acceda a los dominios/URL enumerados en el documento. El dispositivo web seguro cumple los requisitos de la mayoría de los entornos activando la casilla de verificación Omisión de la aplicación Webex en la configuración de omisión; sin embargo, es posible que se requieran algunas configuraciones adicionales en el dispositivo web seguro para evitar la interrupción del servicio en la aplicación Webex. Los siguientes pasos se recomiendan para estos escenarios de caso:

Omisión de Webex Application Scanning

La función Cisco Webex: Omitir análisis es el primer paso para permitir que el tráfico de la aplicación Webex pase sin filtrar a través del dispositivo web seguro. Debe habilitarse en todos los entornos y escenarios de implementación en los que los usuarios de aplicaciones móviles o de escritorio de Webex hayan procesado el tráfico web a través del dispositivo web seguro.

Pasos para habilitar la omisión del escaneo de aplicaciones Webex:

1. En la GUI de WSA, vaya a Web Security Manager > Bypass Settings > Edit Application Bypass Settings.
2. Active la casilla de verificación de "Cisco WebEx".



1_wsa_bypass_scanning_settings

3. Enviar y registrar cambios

Cuando esta configuración está habilitada, no omite el tráfico transparente como cabría esperar una vez que el FQDN se agrega a la lista de omisión en el dispositivo web seguro. En su lugar, el tráfico de la aplicación Webex se sigue procesando a través del dispositivo web seguro, pero se transmitirá durante el descifrado con la etiqueta de decisión "PASSTHRU_AVC". A continuación se muestra un ejemplo de cómo esto podría mostrarse en los registros de acceso:

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

Consideraciones para entornos únicos

Existen algunos escenarios en los que se requieren configuraciones adicionales para que la aplicación Webex funcione cuando el tráfico se proxy a través del dispositivo web seguro.

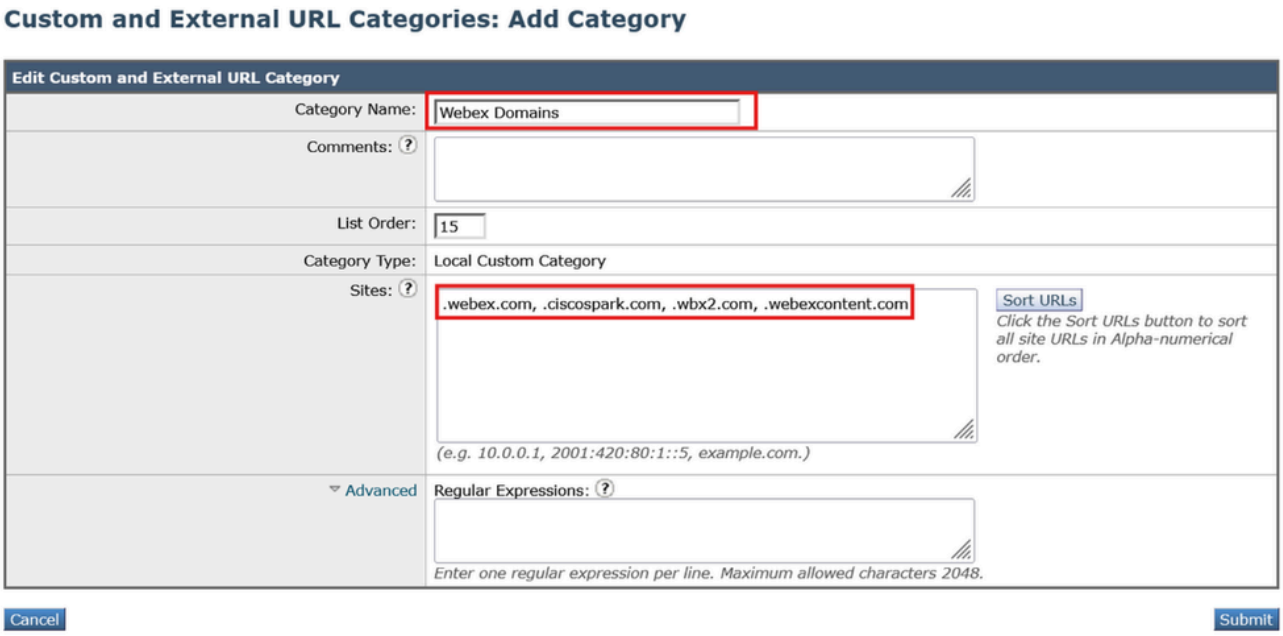
Escenario 1: Los dominios Webex deben estar exentos de autenticación

Esto es especialmente evidente en entornos en los que los sustitutos IP no están habilitados en el perfil de identificación y se utiliza la redirección transparente. De acuerdo con la documentación existente, la aplicación Webex es capaz de autenticar NTLMSSP en estaciones de trabajo unidas al dominio donde el proxy está definido explícitamente. De lo contrario, se recomienda configurar una categoría personalizada para los dominios Webex y eximirlos de la autenticación.

Pasos para eximir de la autenticación a los dominios Webex:

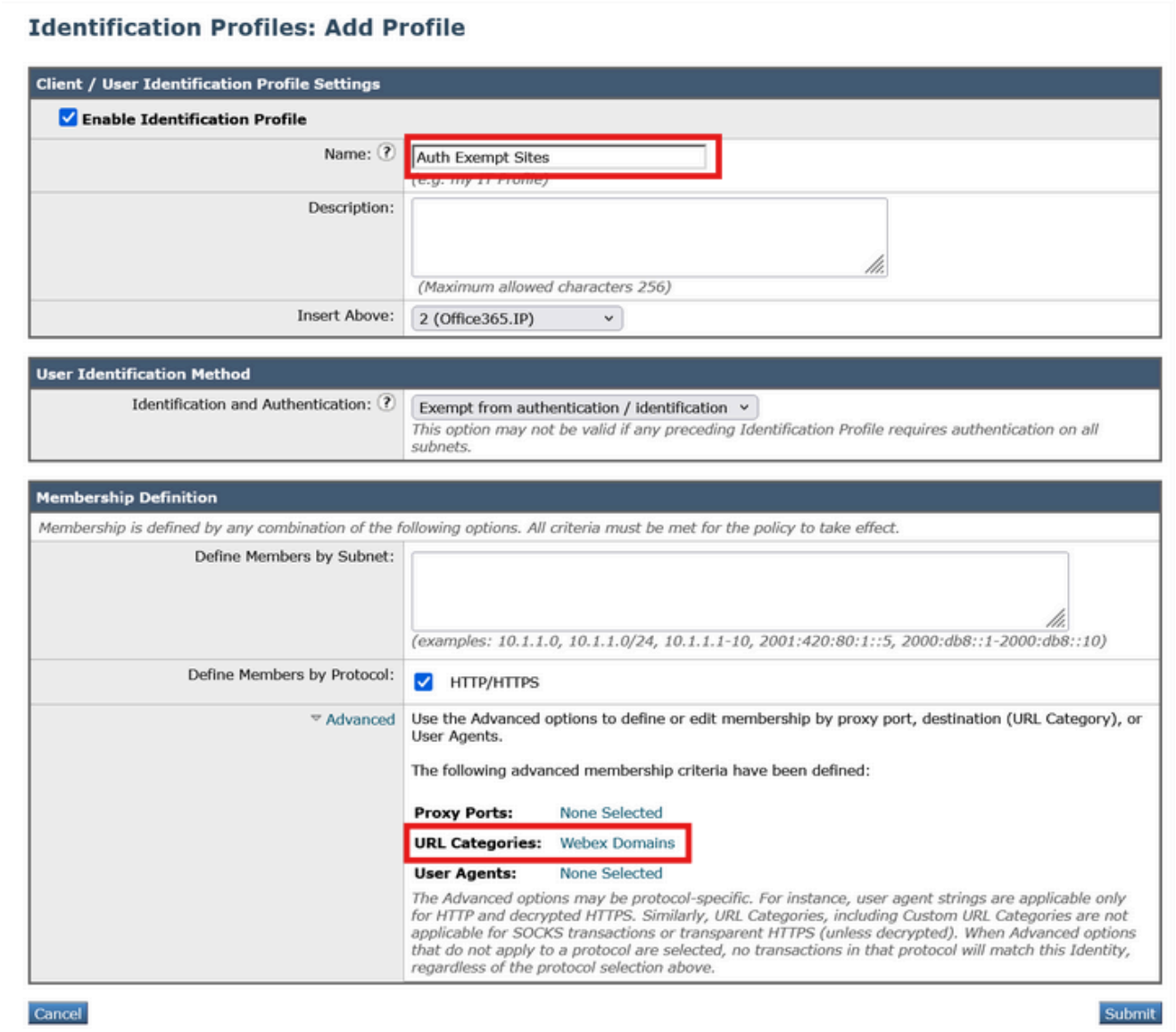
1. En la GUI de WSA, navegue hasta Administrador de seguridad web > Categorías de URL externas y personalizadas > Agregar categoría.
2. Dé un nombre a la nueva categoría y coloque los siguientes dominios en la sección Sitios:

   ```
   .webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
   ```



2_wsa_custom_url_category

3. Haga clic en Submit (Enviar). A continuación, vaya a Web Security Manager > Identification Profiles > Add Identification Profile
4. Asigne un nombre al nuevo perfil y, en la sección Avanzado para Categorías de URL, seleccione la nueva categoría que se creó en el paso #2



3_wsa_id_profile

5. Asegúrese de que la Identificación y Autenticación en el nuevo perfil esté configurada como Exento de autenticación / identificación
6. Enviar y registrar cambios.

Escenario 2: Los dominios de contenido de Webex no se respetan completamente para la omisión del descifrado.

Hay algunos subdominios relacionados con webexcontent.com que no pasan automáticamente por el descifrado cuando se habilita la omisión del escaneo de aplicaciones Webex. La aplicación Webex confía en el contenido servido de estos dominios cuando se descifra, siempre y cuando el certificado de descifrado del dispositivo web seguro ya se agregue al almacén de certificados raíz de confianza del dispositivo o esté firmado de otro modo por una autoridad de certificación interna que ya es de confianza para el dispositivo que ejecuta la aplicación Webex. Sin embargo, si el dispositivo no está gestionado y el certificado de descifrado del dispositivo web seguro no es de confianza, estos dominios deben configurarse para pasar a través del descifrado.

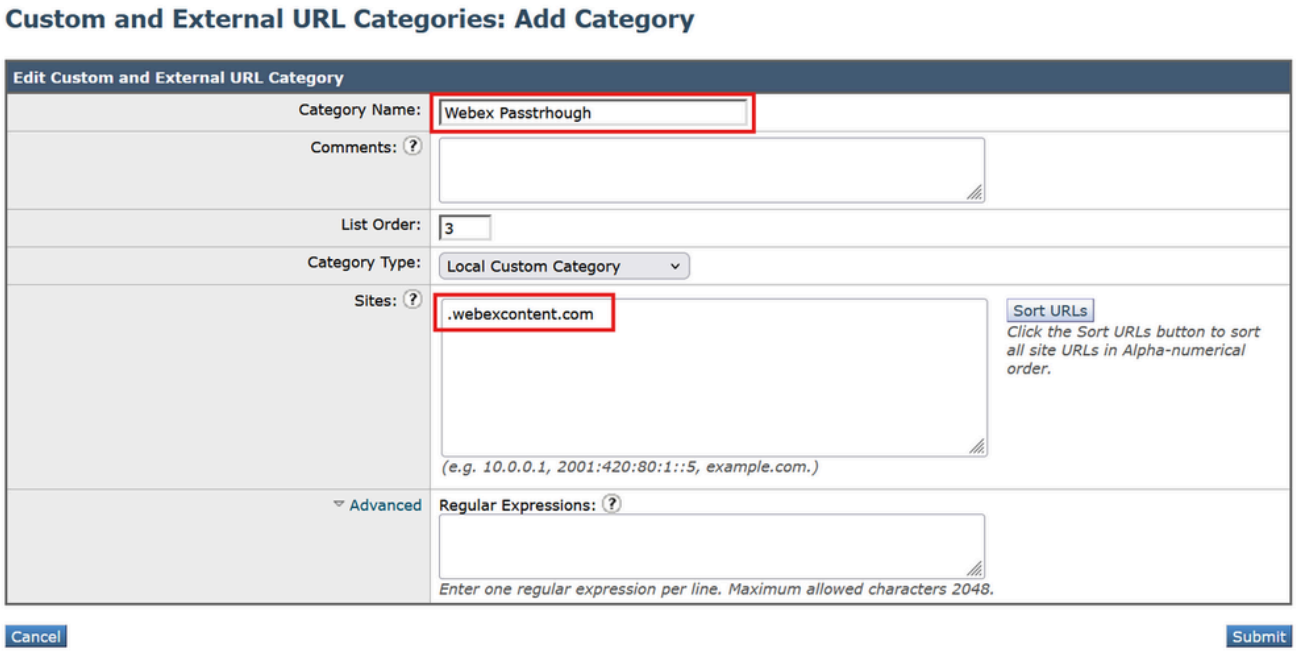
Cuando existe una implementación de redirección transparente y hay más de un SWA a lo largo

de la suplantación de IP de cliente que se utiliza para los grupos de redirección, el tráfico se puede configurar para redirigir al dispositivo web seguro en función de la IP de destino, y de manera similar el tráfico de retorno de los servidores web se configura para redirigir de nuevo a través del dispositivo web seguro en función de la dirección de origen. Cuando el dispositivo web seguro está configurado para establecer conexiones con el servidor web mediante la IP que resuelve mediante la búsqueda de DNS, el tráfico de retorno se puede redirigir inadvertidamente a un dispositivo web seguro diferente y, posteriormente, descartarse. Este problema afecta no solo a Webex, sino también a otras aplicaciones de transmisión de vídeo, debido al uso de direcciones IP rotativas en los servidores web.

Pasos para configurar el paso a través en el descifrado para todos los dominios Webex:

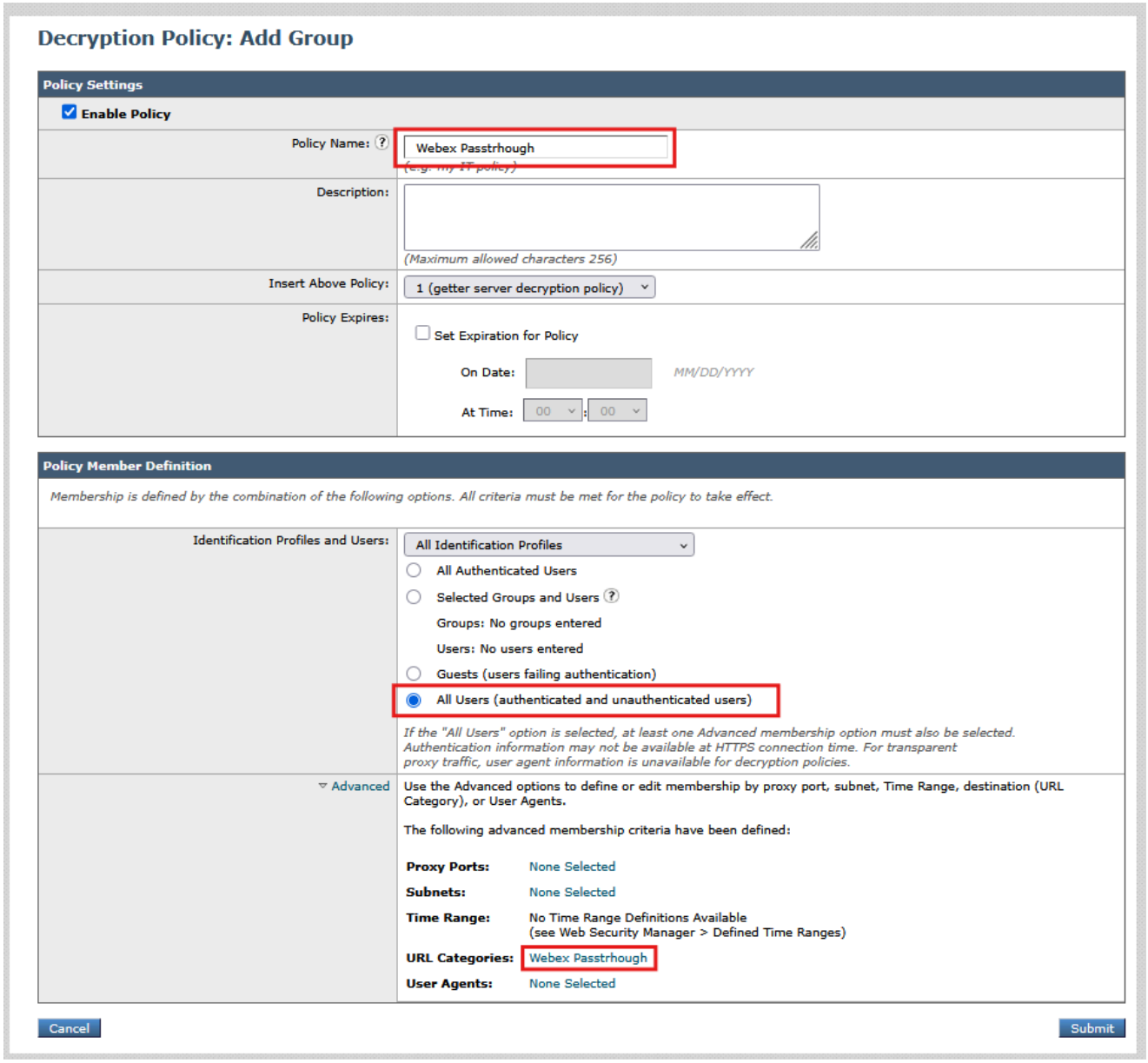
1. Asegúrese de que la opción Omisión del escaneo de aplicaciones Webex esté habilitada de acuerdo con las instrucciones anteriores.
2. En la GUI de WSA, navegue hasta Administrador de seguridad web > Categorías de URL externas y personalizadas > Agregar categoría.
3. Dé un nombre a la nueva categoría y coloque el siguiente dominio en la sección Sitios:

```
.webexcontent.com
```



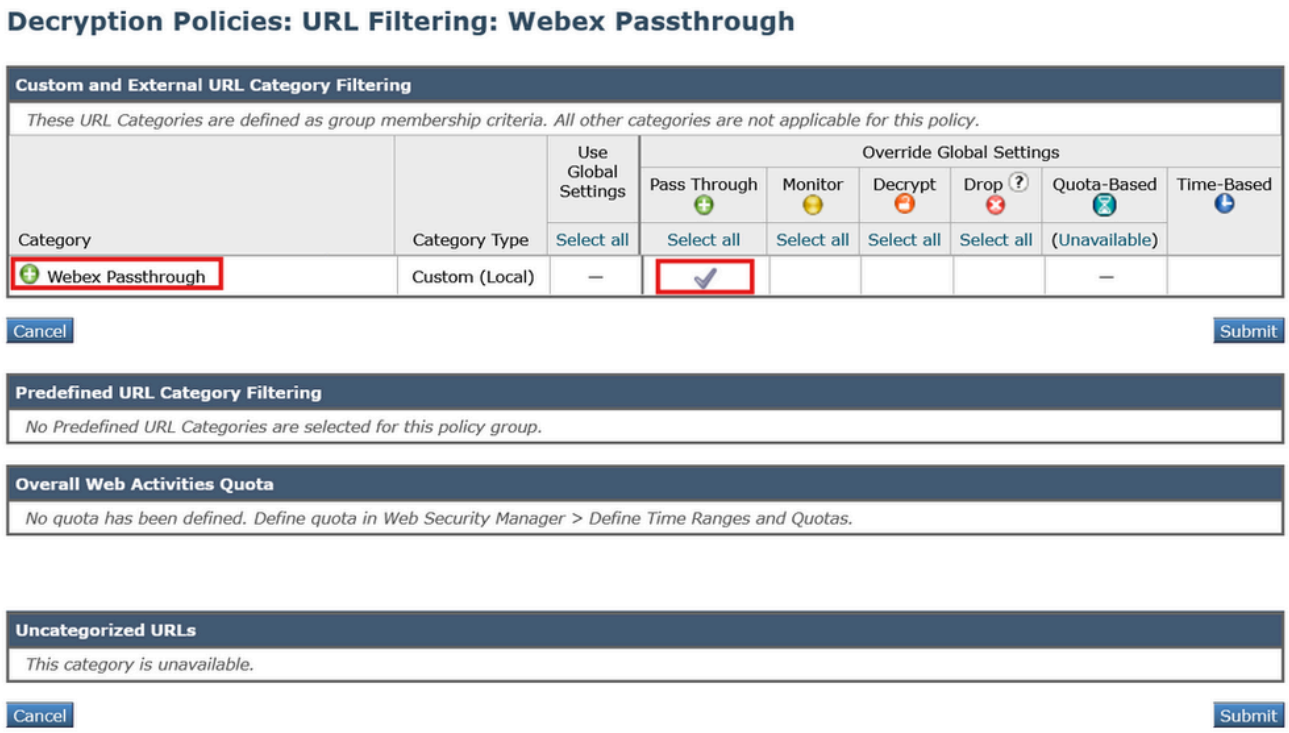
4_wsa_url_category

4. Haga clic en Submit (Enviar). Ahora, navegue hasta Administrador de seguridad web > Políticas de descifrado > Agregar política
5. Dé un nombre a la nueva política, establezca Perfiles de identificación y usuarios en "Todos los usuarios", y en la sección Avanzadas para Categorías de URL, seleccione la nueva categoría que se creó en el paso #3



5_wsa_decryption_policy

6. Haga clic en Submit (Enviar). A continuación, haga clic en la sección Filtrado de URL y establezca la categoría personalizada que se creó en el paso #3 en "Paso a través".



6_wsa_url_filters

7. Enviar y registrar los cambios.

Si se implementan varios dispositivos web seguros para la redirección transparente y se habilita la suplantación de IP de cliente, hay dos soluciones para esto:

1. Establezca los servicios WCCP de salida y devolución para equilibrar la carga según la dirección del cliente en lugar de la dirección del servidor.
2. En la CLI de WSA, establezca advanced proxyconfig > DNS > "Find web server by" para utilizar siempre la dirección IP proporcionada por el cliente en las conexiones al servidor web (opciones 2 y 3). Puede encontrar más información sobre esta configuración en la sección DNS de la guía de prácticas recomendadas de uso de dispositivos web seguros.

Verificación

Cuando se complete la configuración de paso a través, el tráfico de Webex se procesará en los registros de acceso como Paso a través según las políticas:

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

Revise y supervise la aplicación webex; si se informa de alguna lentitud o interrupción del servicio, revise los registros de acceso una vez más y valide que todo el tráfico de WebEx se procesa correctamente.

Información Relacionada

- Requisitos de red para los servicios Webex
- Uso de las prácticas recomendadas de Secure Web Appliance

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).