Omitir el tráfico en el dispositivo web seguro

Contenido

Introducción

En este documento se describen los pasos para omitir el tráfico en el dispositivo web seguro (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.
- Protocolos básicos de red y proxy

Cisco recomienda tener instaladas estas herramientas:

- SWA físico o virtual

- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA

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.

Diferentes tipos de bypass

En SWA, hay tres conceptos diferentes para evitar que un tráfico llegue al SWA, lo que depende de la implementación de proxy (implementación explícita o transparente), o de que el SWA lo analice y lo analice. A continuación se ofrece una breve descripción general de estos tres conceptos:

- Omitir: Parámetro que impide que el tráfico llegue al SWA, lo que reduce la utilización de la tarjeta de interfaz de red (NIC) y elimina la necesidad de una sesión entre el usuario y el dispositivo.
- Paso a través: Esta configuración evita que el SWA descifre el tráfico HTTPS. A pesar de esto, el SWA sigue facilitando dos sesiones distintas: uno entre el cliente y el SWA, y un segundo entre el SWA y el servidor web.
- Permiso: Parámetro de la directiva de acceso en el que el tráfico HTTP o descifrado omite la inspección por parte de los motores SWA internos, como AMP, Sophos, WebRoot y el filtro de aplicación. En este caso, todavía hay dos sesiones en uso en el SWA.

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP	✓	✗	GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP	✓	✗	WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP	✗	✓	From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP	✗	✓	From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP	✓	✓	GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP	✓	✓	GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

Imagen - Gráfico comparativo

Procedimientos de derivación SWA por tipo de implementación

Los procedimientos de omisión varían en función del modelo de implementación de proxy. A continuación se ofrece una breve descripción general de cada tipo:

- Implementación explícita: Los clientes se configuran manualmente para dirigir el tráfico al proxy.
- Implementación transparente: La infraestructura de red redirige el tráfico al proxy de forma automática, por lo que no requiere configuración por parte del cliente.

Omitir el tráfico en la implementación explícita

Para omitir el tráfico en la implementación explícita, debe configurar el cliente para que no reenvíe la solicitud web para las URL deseadas al SWA. Como se muestra en este diagrama de red, parte del tráfico va directamente al firewall o a la puerta de enlace predeterminada para omitir el SWA (ruta número 2).

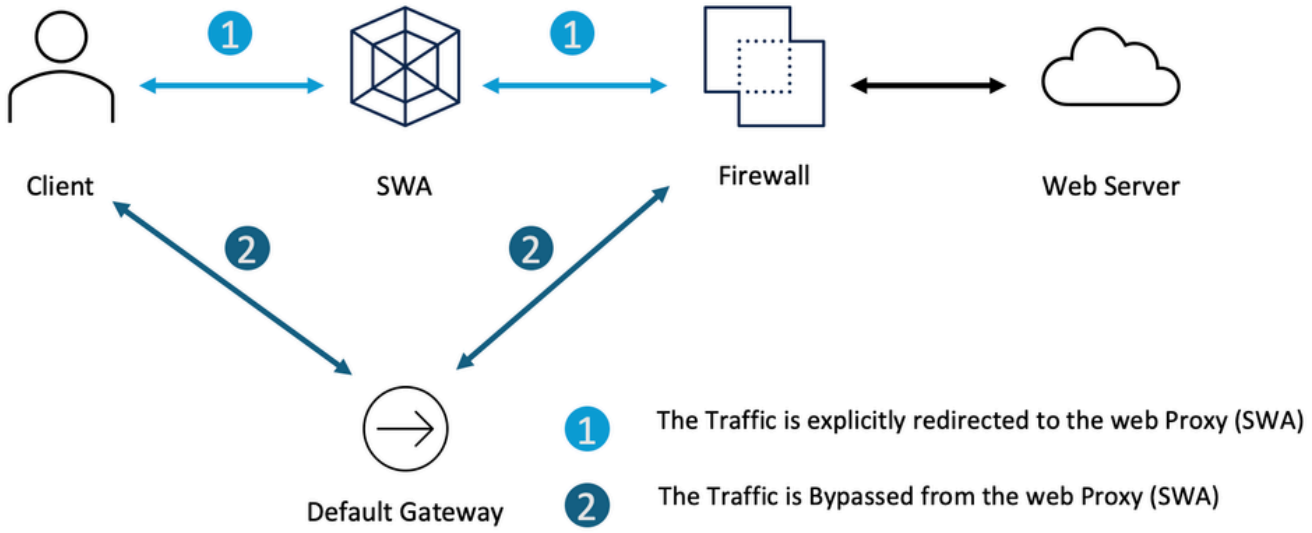


Imagen: omisión del tráfico en la implementación explícita

Dependiendo de la implementación de proxy explícita, puede eximir algunas URL para redirigirlas al SWA.

Configuración de proxy explícito	Pasos para excluir las URL del acceso al SWA

Configuración de archivo PAC	Dependiendo de cómo haya configurado el archivo PAC, puede definir la lista de excepciones y establecer la acción en DIRECT.
	
	A continuación se muestran algunos ejemplos para evitar que la dirección IP privada llegue al SWA
	
	`var resolved_ip = dnsResolve(host);`
	`if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||`
	`isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||`
	`isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||`
	`isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`
	`return "DIRECT";`
	
	Este es un ejemplo para evitar que el tráfico a www.cisco.com redirija el SWA
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	Este ejemplo es para evitar que todos los subdominios de cisco.com redireccionen

	el SWA `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` Nota: Dado que el archivo PAC no es un producto de Cisco, la información se proporciona como cortesía para su comodidad. Para obtener asistencia adicional, comuníquese con el proveedor de software.
Configuración del navegador (Microsoft Edge, Internet Explorer, Google Chrome)	Paso 1. En el menú Inicio, escriba "Opciones de Internet" y pulse Intro Paso 2. Vaya a la pestaña Conexiones y haga clic en Configuración de LAN Paso 3. Haga clic en el botón Paso 4. Defina las URL que desee en la sección Excepciones.

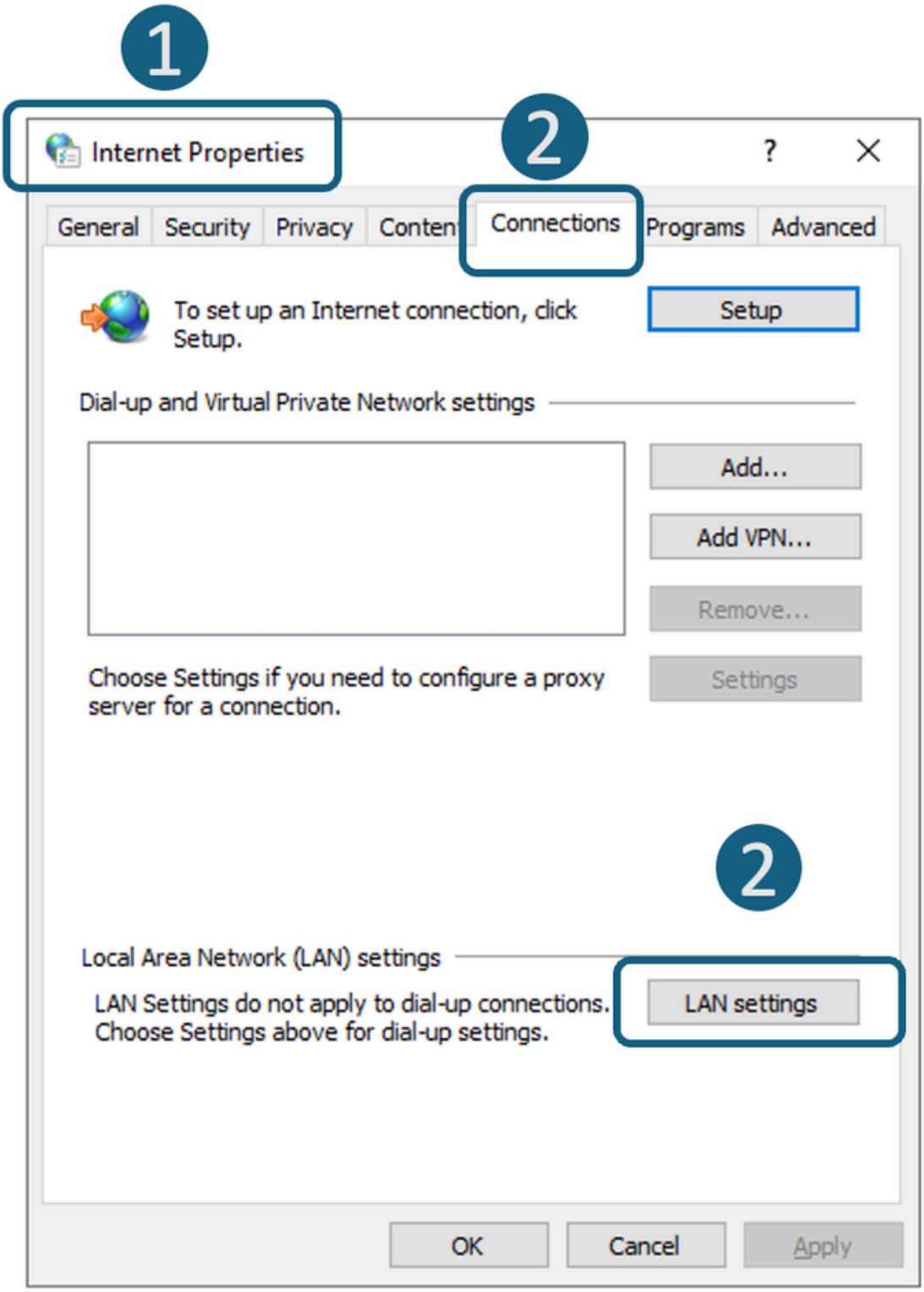


Imagen: acceda a Configuración de LAN

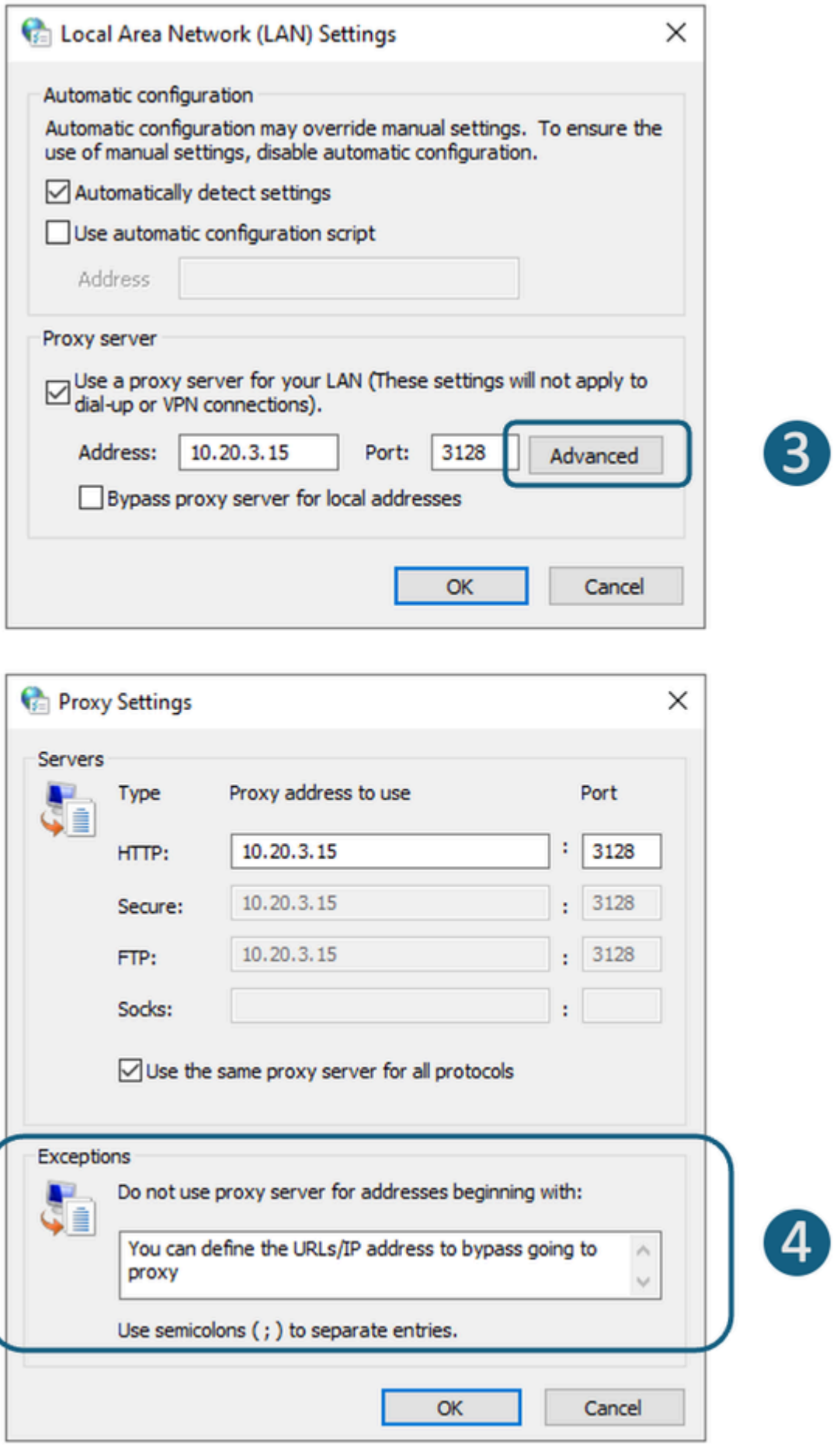
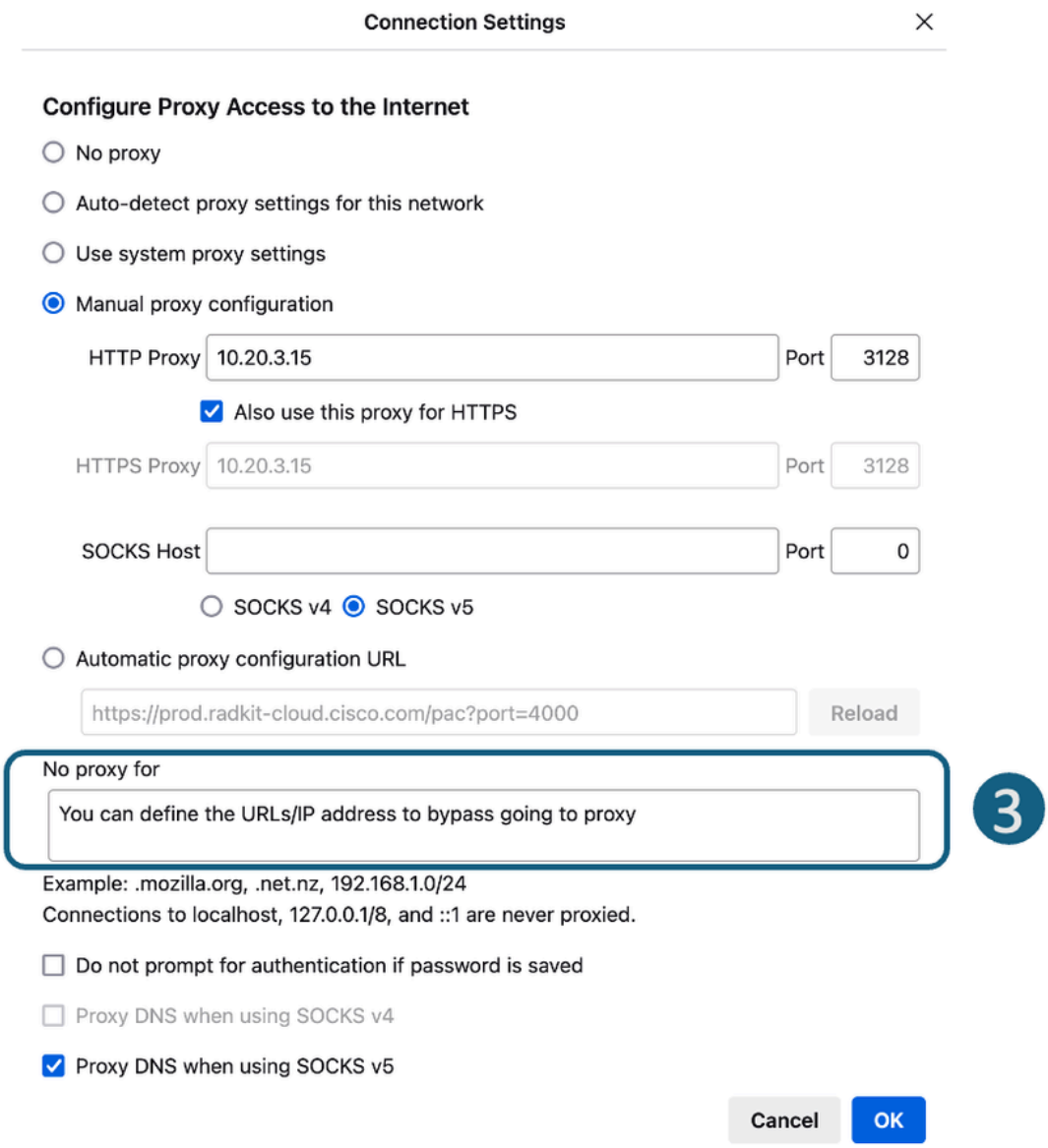
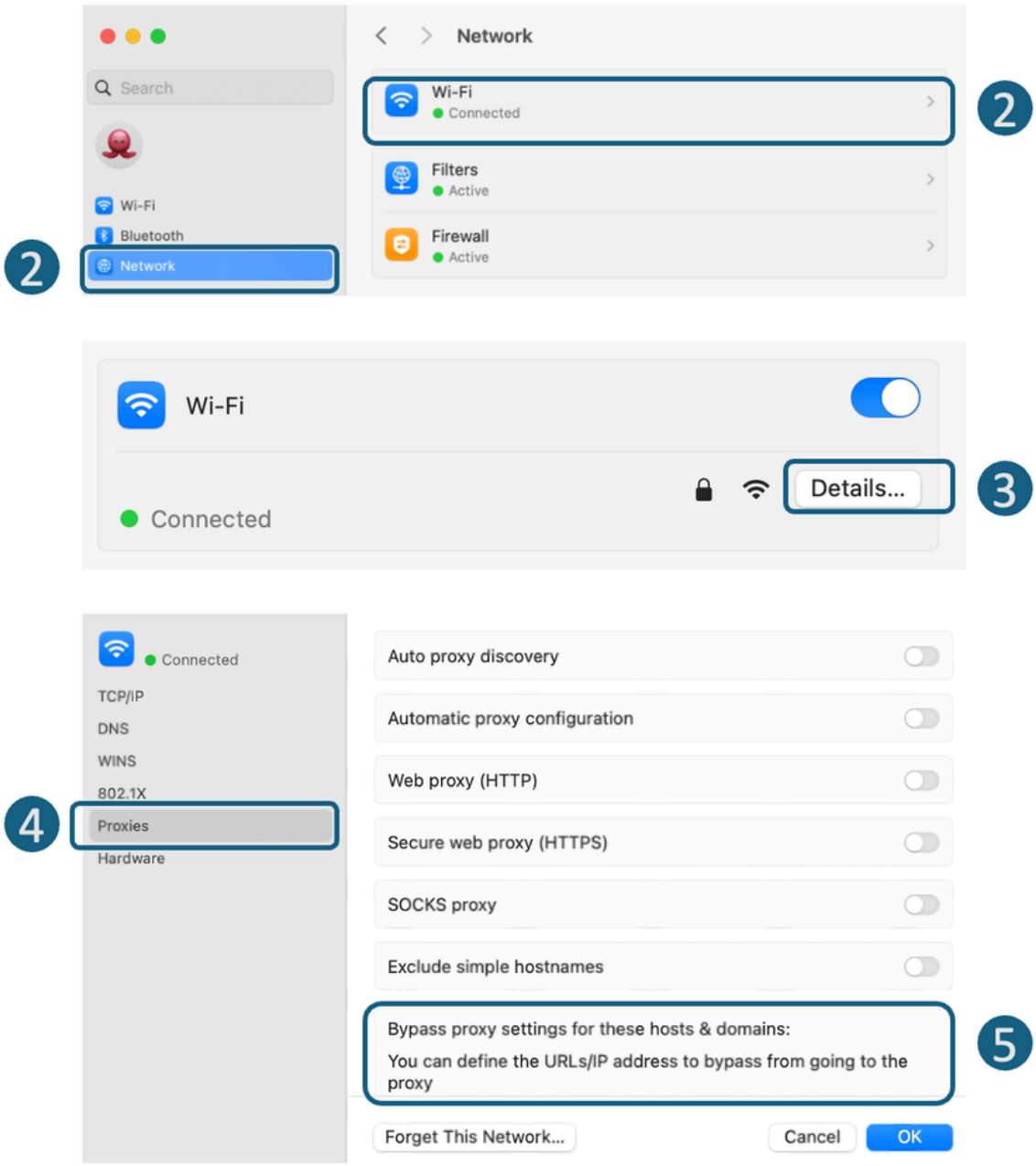


Imagen: defina las excepciones

Configuración del explorador (Mozilla FireFox)	Paso 1. En la esquina superior derecha, haga clic en el menú de tres barras y seleccione Configuración. Paso 2. En la barra de búsqueda, escriba proxy. Paso 3. Defina las URL deseadas en la sección Sin Proxy para.  Imagen - Definición de las excepciones en Fire Fox
Configuración del navegador (Apple Safari)	Paso 1. En la esquina superior izquierda, haga clic en el icono de Apple y elija System Settings (Configuración del sistema). Paso 2. En el panel izquierdo, navegue hasta Red y seleccione la interfaz de red que está utilizando para acceder a Internet.

	Paso 3. Haga clic en Detalles. Paso 4. En el panel izquierdo, seleccione Proxies. Paso 5. Defina las URL deseadas en la sección Omitir configuración de proxy.  Imagen - Definición de las excepciones en Fire Fox
Configuración de directiva de grupo	Dependiendo de cómo haya configurado la directiva de grupo para insertar la configuración de proxy, puede definir la lista de excepciones.

Omitir el tráfico en una implementación transparente

Puede omitir el tráfico en una implementación transparente utilizando el router WCCP o la configuración de omisión SWA. El desvío de SWA actúa en la capa 3, dirigiendo el tráfico a la puerta de enlace predeterminada y omitiendo el dispositivo por completo, lo que impide el procesamiento y la creación de sesiones independientes.

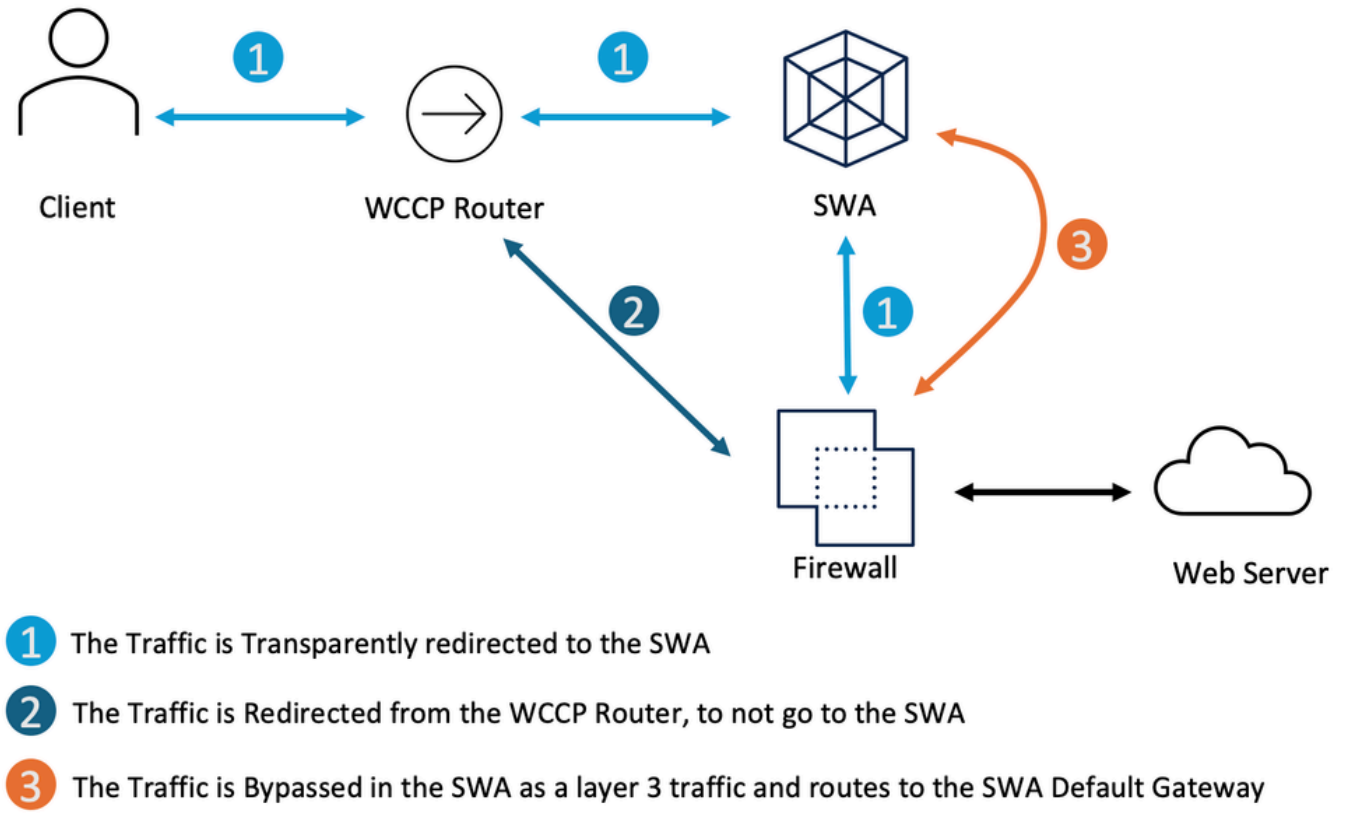
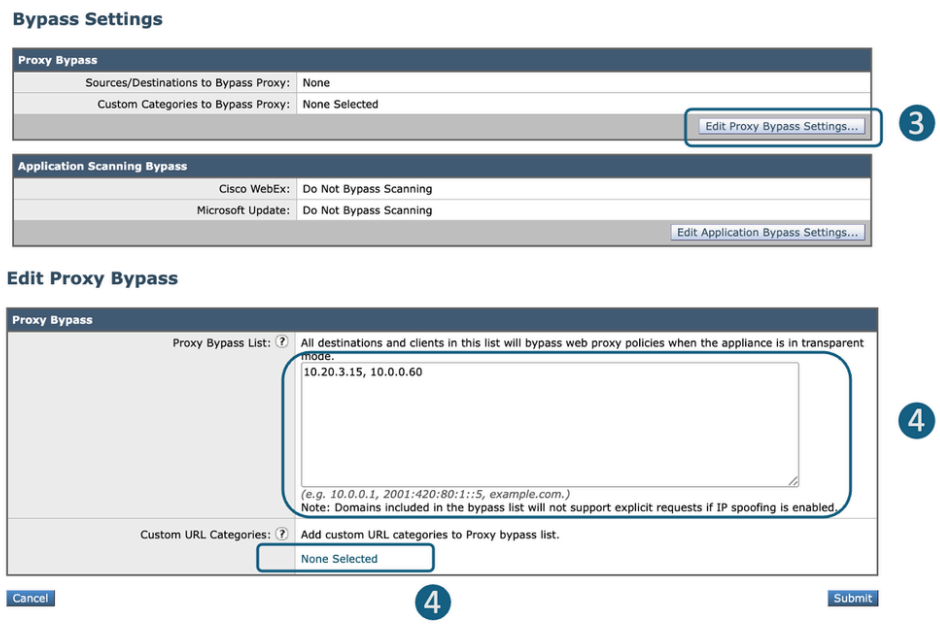


Imagen: omisión del tráfico en una implementación transparente

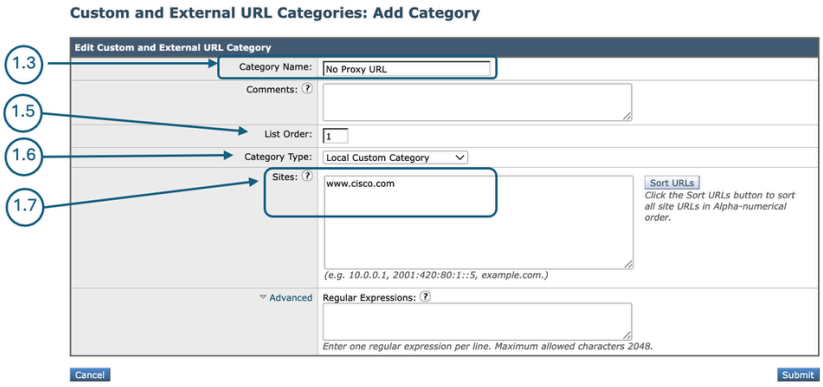
Omitiendo el tráfico Implementación de proxy transparente	Pasos para evitar que el tráfico llegue al SWA
Configuración de derivación SWA	Paso 1. En GUI, elija Web Security Manager. Paso 2. Seleccione Bypass Settings. Paso 3. Haga clic en Editar configuración de omisión de proxy. Paso 4. Puede introducir la URL, la dirección IP o agregar una categoría de URL personalizado a la lista. Paso 5. Envíe y confirme los cambios.

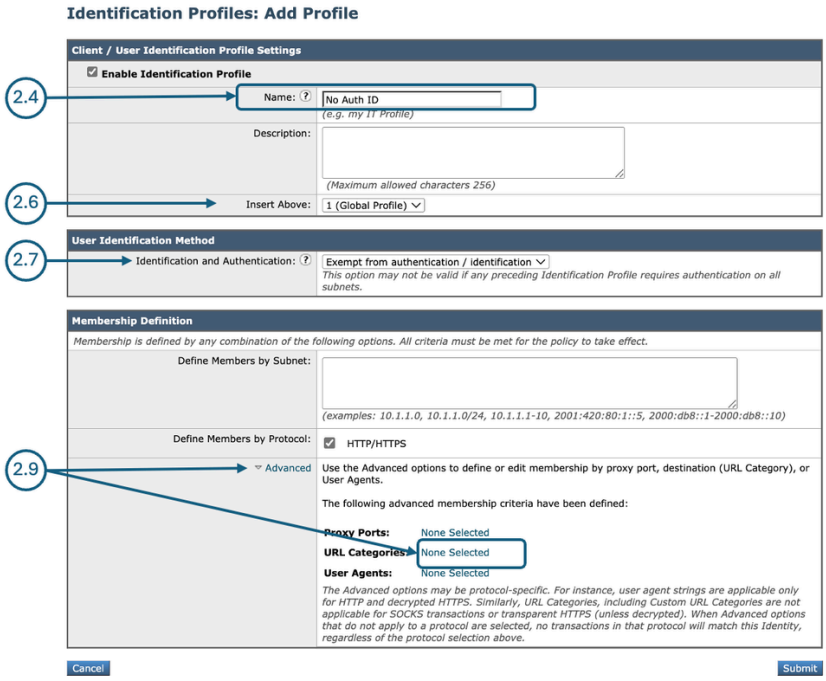
	 Imagen - Configuración de los parámetros de omisión Consejo: El tráfico que se omite con esta configuración no se registra en los registros de acceso y se puede ver en Bypass_Logs.
Redirección del tráfico desde el router WCCP/PBR	Puede configurar la dirección IP de origen o de destino en el WCCP o en el router basado en políticas (PBR) para no redirigir algunos tráficos al SWA.

Configuración del paso a través y autorización del tráfico en SWA

Si el tráfico está llegando al SWA y con el fin de reducir la carga en el SWA a debido a las preocupaciones de privacidad, no desea que el tráfico de algunas URL sean inspeccionadas por el SWA, utilice estos pasos.

Pasos	Pasos
Paso 1. Cree una categoría de URL personalizada para las URL.	Paso 1.1.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic en Categorías de URL externas y personalizadas. Paso 1.2.Haga clic en Agregar categoría para agregar una categoría de URL personalizada.

	Paso 1.3.Asignar un CategoryName único. Paso 1.4. (Opcional) Agregar descripción. Paso 1.5. En Orden de la lista, elija la primera categoría que desee colocar en la parte superior. Paso 1.6. En la lista desplegable Tipo de categoría, elija Categoría personalizada local. Paso 1.7. Agregue las URL deseadas en la sección Sitios. Paso 1.8. Enviar.  Imagen: creación de una categoría de URL personalizada
Paso 2. Cree un perfil de identificación para eximir el tráfico de la autenticación.	Paso 2.1.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic en Perfiles de identificación. Paso 2.2.Haga clic en Agregar perfil para agregar un perfil. Paso 2.3.Utilice la casilla de verificación Enable Identification Profile para habilitar este perfil o para deshabilitarlo rápidamente sin eliminarlo. Paso 2.4.Asignar un profileName único. Paso 2.5. (Opcional) Agregar descripción. Paso 2.6.En la lista desplegable Insertar arriba, elija dónde debe aparecer este perfil en la tabla. Paso 2.7. En la sección Método de identificación de usuario, elijaExento de autenticación/ identificación. Paso 2.8.En el campo Define Members by Subnet, deje este campo en blanco para incluir todas las direcciones IP del cliente a menos que desee pasar a través del tráfico para una dirección IP determinada. Paso 2.9. En la sección Avanzado, elija Categorías de URL personalizadas.

	 Imagen - Agregar perfil de identificación Paso 2.10. Agregue la Categoría de URL Personalizada que se creó en el Paso 1. Paso 2.11. Haga clic en Finalizado. Paso 2.12. Enviar.
Paso 3. Crear una política de descifrado para pasar a través del tráfico.	Paso 3.1.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic enDirectiva de descifrado. Paso 3.2. Haga clic en Agregar Política para agregar una Política de Descifrado. Paso 3.3.Use la casilla de verificación Enable Policy para habilitar esta política. Paso 3.4.Asignar un único PolicyName. Paso 3.5. (Opcional) Agregar descripción. Paso 3.6.En la lista desplegable Insertar sobre política, elija la primera política. Paso 3.7.Desde Perfiles de Identificación y Usuarios, elija el Perfil de Identificación que creó en el Paso 2. Paso 3.8. Enviar.

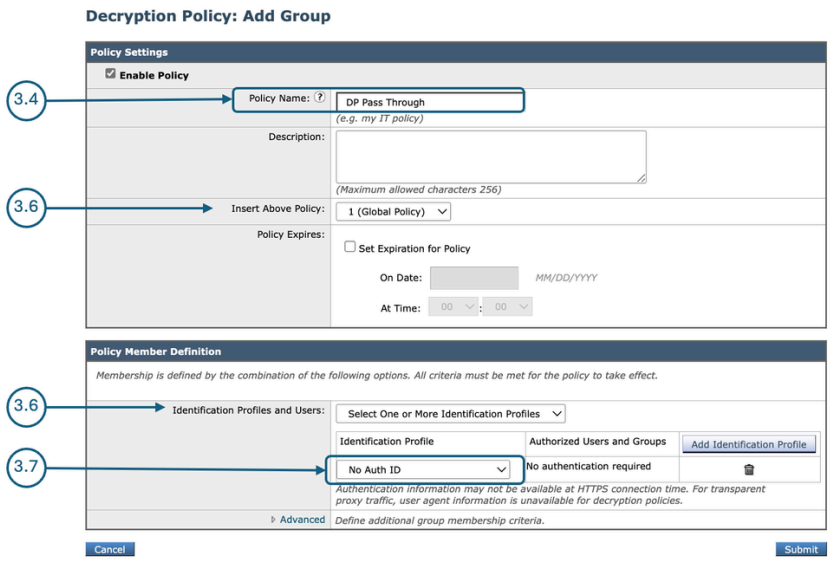
<table>
<tr>
<td></td>
<td>


Imagen - Crear una política de descifrado

Paso 3.9.En la página Políticas de descifrado, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de descifrado.

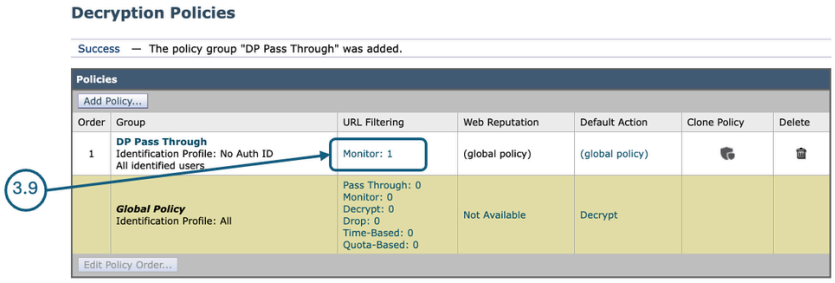


Imagen - Seleccionar filtrado de URL

Paso 3.10.SelectPassThrough es la acción para la categoría de URL creada en el Paso 1.

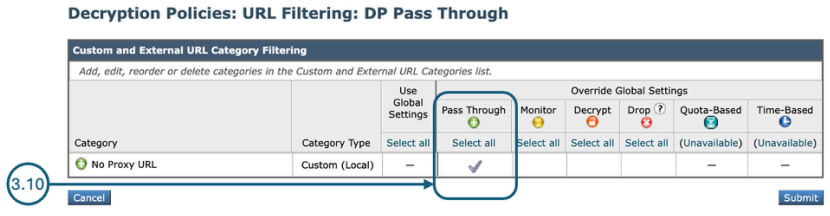


Imagen: establezca la acción para pasar a través de

Paso 3.11. Enviar.</td>
</tr>
<tr>
<td>Paso 4. Crear una directiva de acceso para permitir el tráfico de Microsoft Updates.</td>
<td>Paso 4.1.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic enDirectiva de acceso.</td>
</tr>
</table>

Paso 4.2. Haga clic en Agregar Política para agregar una Política de Acceso.

Paso 4.3.Use la casilla de verificación Enable Policy para habilitar esta política.
Paso 4.4.Asignar un único PolicyName.
Paso 4.5. (Opcional) Agregar descripción.
Paso 4.6.En la lista desplegable Insertar sobre política, elija la primera política.

Paso 4.7.Desde Perfiles de Identificación y Usuarios, elija el Perfil de Identificación que creó en el Paso 2.

Paso 4.8. Enviar.

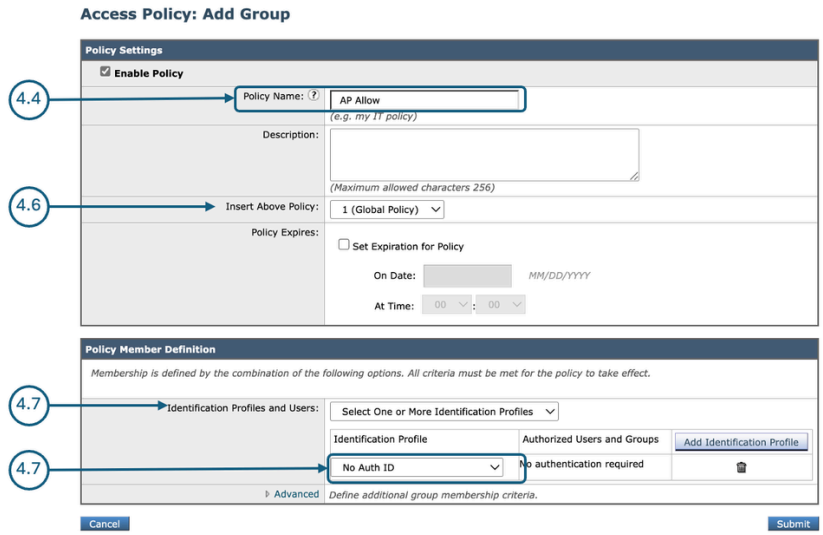


Imagen - Crear política de acceso

Paso 4.9. En la página Access Policies, en URL Filtering, haga clic en el enlace asociado a esta nueva política de acceso.

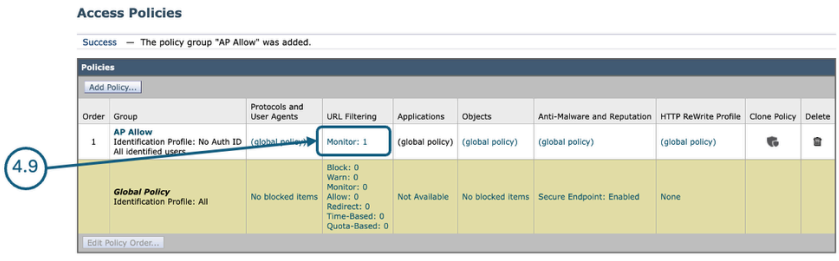
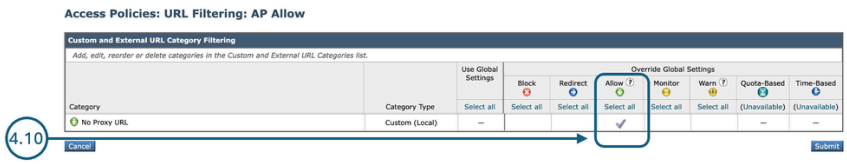


Imagen - Seleccionar filtrado de URL

Paso 4.10.Seleccione Permitir como la acción para la categoría de URL personalizado creada para la categoría de URL creada en el Paso 1.

	 Imagen: establezca la acción en Permitir Paso 4.11. Enviar. Paso 4.12. Realice los cambios.

Información Relacionada

- Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro
- Omitir autenticación en dispositivo web seguro - Cisco
- Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - GD(General Deployment) - Clasificación de usuarios finales para la aplicación de políticas [Cisco Secure Web Appliance] - Cisco
- Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco
- Cómo eximir el tráfico de Office 365 de la autenticación y el descifrado en Cisco Web Security Appliance (WSA): Cisco
- Uso de las prácticas recomendadas de los dispositivos web seguros: Cisco
- Bloqueo del tráfico en el dispositivo web seguro
- Bloquear la carga de tráfico en el dispositivo web seguro
- Bloquear la descarga de archivos ejecutables en SWA

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).