Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro

Contenido

Introducción

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

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.

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.

Actualizaciones de Microsoft

Las actualizaciones de Microsoft son parches esenciales, actualizaciones de seguridad y mejoras de las funciones que publica Microsoft para sus sistemas operativos y aplicaciones de software. Estas actualizaciones son cruciales para mantener la seguridad, la estabilidad y el rendimiento de los ordenadores y los dispositivos de red. Garantizan la protección de los sistemas frente a vulnerabilidades, la corrección de errores y la integración de nuevas funciones o mejoras en el software.

El impacto de las actualizaciones de Microsoft en los servidores proxy, como Cisco SWA, puede ser significativo. Estas actualizaciones a menudo implican la descarga de archivos grandes o numerosos archivos más pequeños, que pueden consumir un ancho de banda considerable y recursos de procesamiento en el proxy. Esto puede conllevar una congestión, un menor rendimiento de la red y un aumento de la carga en la infraestructura de proxy, lo que podría afectar a la experiencia general del usuario y a otras operaciones de red críticas.

Omitir el tráfico de Microsoft Update del proxy puede ser una forma segura y eficaz de gestionar estos retos. Puesto que las actualizaciones de Microsoft se obtienen de servidores de confianza de Microsoft, permitir que este tráfico omita el proxy puede ayudar a reducir la carga en el servidor proxy sin poner en peligro la seguridad de la red. Esto garantiza que las actualizaciones esenciales se proporcionen de forma eficaz, al tiempo que se conservan los recursos proxy para otras tareas de filtrado de contenido y seguridad. Sin embargo, es importante implementar estas configuraciones de omisión con cuidado para mantener la seguridad de la red en general y el cumplimiento de las políticas organizativas.

Omitir actualizaciones de Microsoft

Si está considerando evitar el proxy del tráfico de las actualizaciones de Microsoft, existen dos enfoques principales

1. Omisión: Esto implica configurar la red para redirigir el tráfico de modo que nunca llegue al SWA.
2. Paso a través: Esto implica configurar el SWA para que no descifre ni analice el tráfico de las actualizaciones de Microsoft, lo que le permite pasar a través del proxy sin inspección.

Omitiendo el tráfico en SWA

Para omitir el tráfico de Microsoft Updates en redes equipadas con SWA, el enfoque varía en función de la configuración de implementación de proxy:

Tipo de implementación	Evitar el tráfico
Implementación transparente	Puede redirigir el tráfico de las actualizaciones de Microsoft

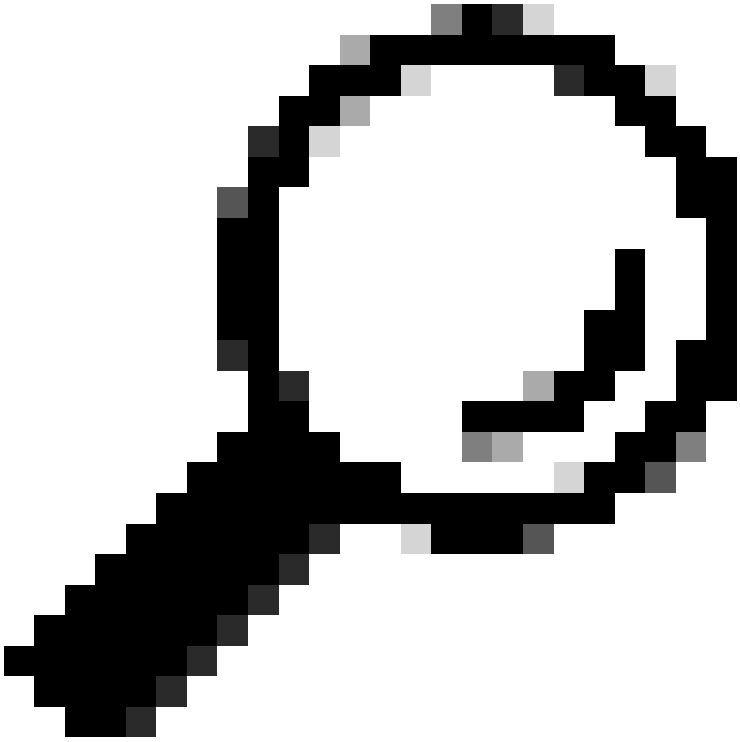
	en el router o en los switches de capa 4 que son responsables de reenviar el tráfico al servidor proxy.
	Puede configurar los parámetros de omisión directamente en la interfaz gráfica de usuario (GUI) de SWA.
Implementación explícita	Para evitar que el tráfico de Microsoft Updates llegue al SWA, debe configurar el desvío en el origen. Esto significa eximir las URL relevantes en las máquinas cliente para garantizar que el tráfico no se redirige al SWA.

Si el desvío de tráfico específico requiere un amplio rediseño de la red y no es factible, un enfoque alternativo consiste en configurar el SWA para que pase a través de ciertos tipos de tráfico. Esto se puede lograr configurando el SWA para que no descifre ni escanee el tráfico designado, lo que le permite pasar a través del proxy sin inspección. Este método garantiza que el tráfico esencial se distribuye de forma eficiente, a la vez que se minimiza el impacto en el rendimiento de la red y los recursos de proxy.

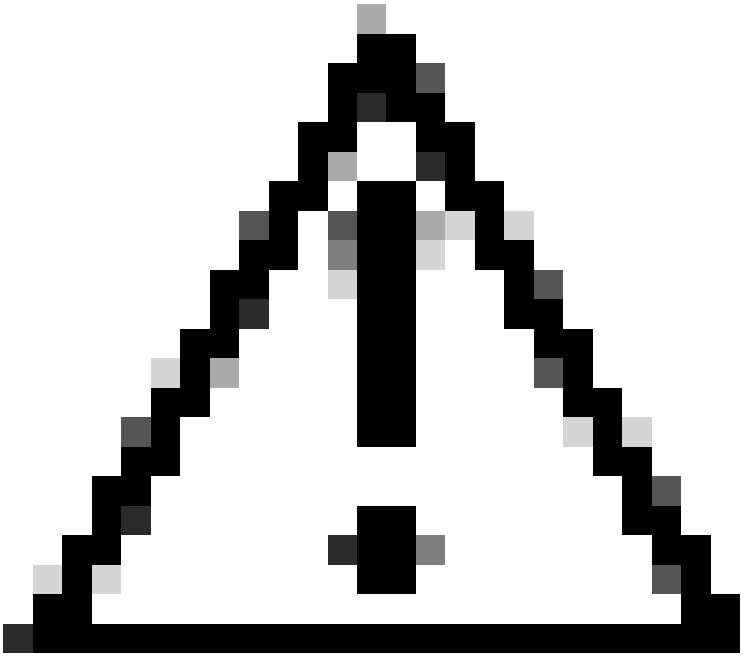
Pasos para pasar por las actualizaciones de Microsoft

Existen cuatro etapas principales para el paso a través de los tráficos de las actualizaciones de Microsoft:

Fase	Pasos
1. Crear una categoría de URL personalizada para las URL de actualizaciones de Microsoft	Paso 1.DesdeGUI, ElijaAdministrador de seguridad web y, a continuación, haga clic en Categorías de URL externas y personalizadas. Paso 2.Haga clic en Agregar categoría para agregar una categoría de URL personalizada. Paso 4.Asigne un CategoryName único. Paso 5. (Opcional) Agregar descripción. Paso 6. En Orden de la lista, elija la primera categoría que desee colocar en la parte superior. Paso 7. En la lista desplegable CategoryType, elija Local Custom Category. Paso 8. Agregue las URL de Microsoft Updates en la sección Sites.



Sugerencia: Puede comprobar la lista de actualizaciones de Microsoft desde este enlace: [Paso 2: Configuración de WSUS | Microsoft Learn]



Precaución: no copie ni pegue las direcciones URL tal y como aparecen en los documentos de Microsoft; asígneles un formato SWA adecuado. Para obtener más información, visite:

	Configuración de categorías de URL personalizadas en Secure Web Appliance - Cisco Paso 9. Enviar.
2. Cree un perfil de identificación para eximir el tráfico de Microsoft Updates de la autenticación	Paso 10.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic en Perfiles de identificación. Paso 11.Haga clic en Agregar perfil para agregar un perfil. Paso 12.Utilice la casilla de verificación Enable Identification Profile para habilitar este perfil o para deshabilitarlo rápidamente sin eliminarlo. Paso 13.Asigne un profileName único. Paso 14. (Opcional) Agregar descripción. Paso 15.En la lista desplegable Insertar arriba, elija dónde debe aparecer este perfil en la tabla. Paso 16. En la secciónMétodo de identificación de usuario, elijaExento de autenticación/identificación. Paso 17.En Definir miembros por subred, si desea pasar a través del tráfico de Microsoft para algunos usuarios específicos, introduzca las direcciones IP o las subredes correspondientes, o bien deje este campo en blanco para incluir todas las direcciones IP. Paso 18. En la sección Avanzadas, elija Categorías de URL personalizadas. Paso 19. Agregue la categoría de URL personalizado que se creó para las actualizaciones de Microsoft. Paso 20. Haga clic en Done (Listo). Paso 21. Enviar.
3. Crear una política de descifrado para pasar a través del tráfico de actualizaciones de Microsoft	Paso 2.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic enDirectiva de descifrado. Paso 23. Haga clic en Agregar política para agregar una política de descifrado. Paso 24.Utilice la casilla de verificación Enable Policy para habilitar esta directiva. Paso 25.Asignar un PolicyName único.

	Paso 26. (Opcional) Agregar descripción. Paso 27.En la lista desplegable Insertar sobre política, elija la primera política. Paso 28.Desde Perfiles de Identificación y Usuarios, elija el Perfil de Identificación que creó en los pasos anteriores. Paso 29. Enviar. Paso 30.En la página Políticas de descifrado, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de descifrado. Paso 32.SeleccionePaso a través como la acción para la categoría URL de Microsoft Updates. Paso 32. Enviar.
4. Crear una directiva de acceso para permitir el tráfico de actualizaciones de Microsoft	Paso 3.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic enDirectiva de acceso. Paso 34. Haga clic en Agregar política para agregar una política de acceso. Paso 35.Use la casilla de verificación Enable Policy para habilitar esta política. Paso 36.Asignar un PolicyName único. Paso 37. (Opcional) Agregar descripción. Paso 38.En la lista desplegable Insertar sobre política, elija la primera política. Paso 39.Desde Perfiles de Identificación y Usuarios, elija el Perfil de Identificación que creó en los pasos anteriores. Paso 40. Enviar. Paso 9. En la página Políticas de acceso, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de acceso Paso 10.Seleccione Permitir como la acción para la categoría URL personalizado creada para las actualizaciones de Microsoft. Paso 11. Enviar. Paso 12. Registrar cambios.

Información Relacionada

- 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
- Omitir autenticación en dispositivo web seguro - Cisco

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).