Configurar solicitud de intervalo para tráfico de Microsoft Update en SWA

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Solicitud de intervalo

Solicitud de rango en el entorno proxy

Habilitación de solicitudes de intervalo para actualizaciones de Microsoft

Pasos para habilitar la solicitud de intervalo sólo para actualizaciones de Microsoft

- Paso 1. Activar la Solicitud de Rango
- Paso 2. Crear una categoría de URL personalizada para las URL de Microsoft Updates
- Paso 3. (Opcional) Crear un perfil de identificación para eximir el tráfico de Microsoft Updates de la autenticación
- Paso 4. (Opcional) Crear una directiva de descifrado para pasar el tráfico de actualizaciones de Microsoft
- Paso 5. Crear una directiva de acceso para permitir la solicitud de intervalo para el tráfico de actualizaciones de Microsoft

Modificación de los registros de acceso

Verificación

Información Relacionada

Introducción

Este documento describe los pasos para permitir que el tráfico de actualizaciones de Microsoft utilice la solicitud de rango 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.

Solicitud de intervalo

Una solicitud de intervalo es una característica del protocolo HTTP que permite a un cliente (como un explorador Web o un administrador de descargas) solicitar sólo una parte específica de un archivo desde un servidor, en lugar de descargar todo el archivo a la vez. Esto resulta especialmente útil para reanudar descargas interrumpidas, transmitir archivos multimedia o acceder a archivos de gran tamaño de forma eficaz. El cliente especifica el rango de bytes deseado en el encabezado Range de la solicitud HTTP, y el servidor responde con un código de estado de contenido parcial 206 si admite solicitudes de rango, entregando sólo el segmento solicitado del archivo.

Este mecanismo mejora el rendimiento y la experiencia del usuario en varios escenarios. Por ejemplo, en la transmisión de vídeo, las solicitudes de alcance permiten a los reproductores captar solo los segmentos necesarios para la reproducción, lo que reduce el uso de ancho de banda y mejora la capacidad de respuesta. Del mismo modo, los administradores de descargas utilizan solicitudes de intervalo para dividir un archivo en fragmentos y descargarlos en paralelo, lo que acelera el proceso. Las solicitudes de rango también desempeñan un papel clave en el almacenamiento en caché y los sistemas proxy, permitiendo las actualizaciones parciales y reduciendo las transferencias de datos redundantes.

Solicitud de rango en el entorno proxy

En un entorno proxy, las solicitudes de intervalo desempeñan un papel crucial a la hora de optimizar el uso del ancho de banda y mejorar la eficacia de la entrega de contenido. Cuando las solicitudes de rango están habilitadas, el servidor proxy puede obtener sólo los segmentos de bytes requeridos del servidor de origen y almacenarlos localmente en la memoria caché. Esto permite a los clientes solicitar contenido parcial, como segmentos específicos de un vídeo o un archivo de gran tamaño, y recibirlo rápidamente de la caché de proxy si está disponible. También permite descargas paralelas y capacidades de reanudación, que son especialmente beneficiosas en entornos con ancho de banda limitado o latencia alta.

Sin embargo, cuando las solicitudes de rango están inhabilitadas, el proxy debe obtener el archivo completo del servidor de origen incluso si el cliente sólo necesita una pequeña parte. Esto conlleva una transferencia de datos innecesaria, una mayor carga en los servidores proxy y de origen, y tiempos de respuesta más lentos para los clientes. También evita estrategias de almacenamiento en caché eficaces, ya que el proxy no puede almacenar ni suministrar contenido

parcial. En escenarios de transmisión, esto puede ocasionar retrasos en el almacenamiento en búfer o una experiencia de usuario degradada. La deshabilitación de las solicitudes de intervalo se puede realizar por motivos de seguridad o de políticas, pero a menudo se produce a costa del rendimiento y la flexibilidad.

Por ejemplo, supongamos que 10 usuarios intentan descargar 1 MB de un archivo de 100 MB a través de un servidor proxy.

Solicitudes de intervalo desactivadas:

Cuando las solicitudes de rango están inhabilitadas, el proxy no puede obtener solamente el segmento de 1MB que cada usuario necesita. En su lugar, debe descargar el archivo completo de 100 MB del servidor de origen para cada solicitud. Esto da como resultado:

Tráfico total desde el origen al proxy: 10 × 100 MB = 1000 MB (1 GB)

Solo 10 MB de esos datos son usados por los clientes.

Los 990 MB restantes se desperdician, lo que provoca un uso ineficiente del ancho de banda y un aumento de la carga en los servidores proxy y de origen.

Solicitudes de intervalo habilitadas:

Con las solicitudes de intervalo activadas, el proxy obtiene sólo los 1 MB solicitados por usuario:

Tráfico total desde el origen al proxy: 10 × 1 MB = 10 MB

El proxy puede almacenar en caché estos segmentos y servirlos a otros usuarios si es necesario.

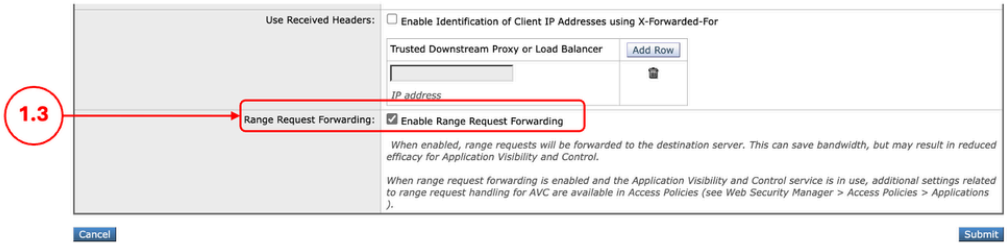
Esto se traduce en un tráfico 90 veces menor, tiempos de respuesta más rápidos y una utilización de los recursos significativamente mejor.

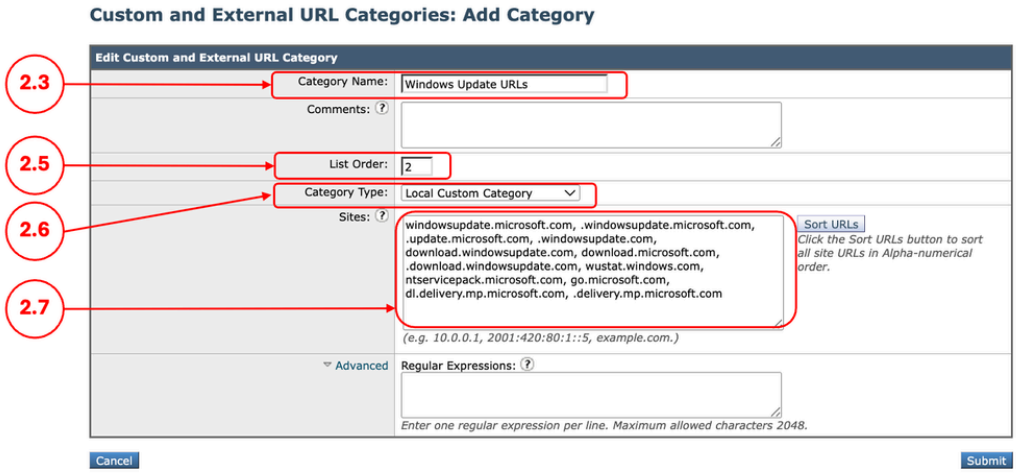
Habilitación de solicitudes de intervalo para actualizaciones de Microsoft

Aunque las solicitudes de intervalo mejoran el rendimiento, dificultan el análisis de seguridad y la aplicación de políticas en entornos SWA, ya que estos sistemas no pueden inspeccionar completamente el contenido parcial. Este artículo limita el uso de solicitudes de intervalo exclusivamente al tráfico de Microsoft Update.

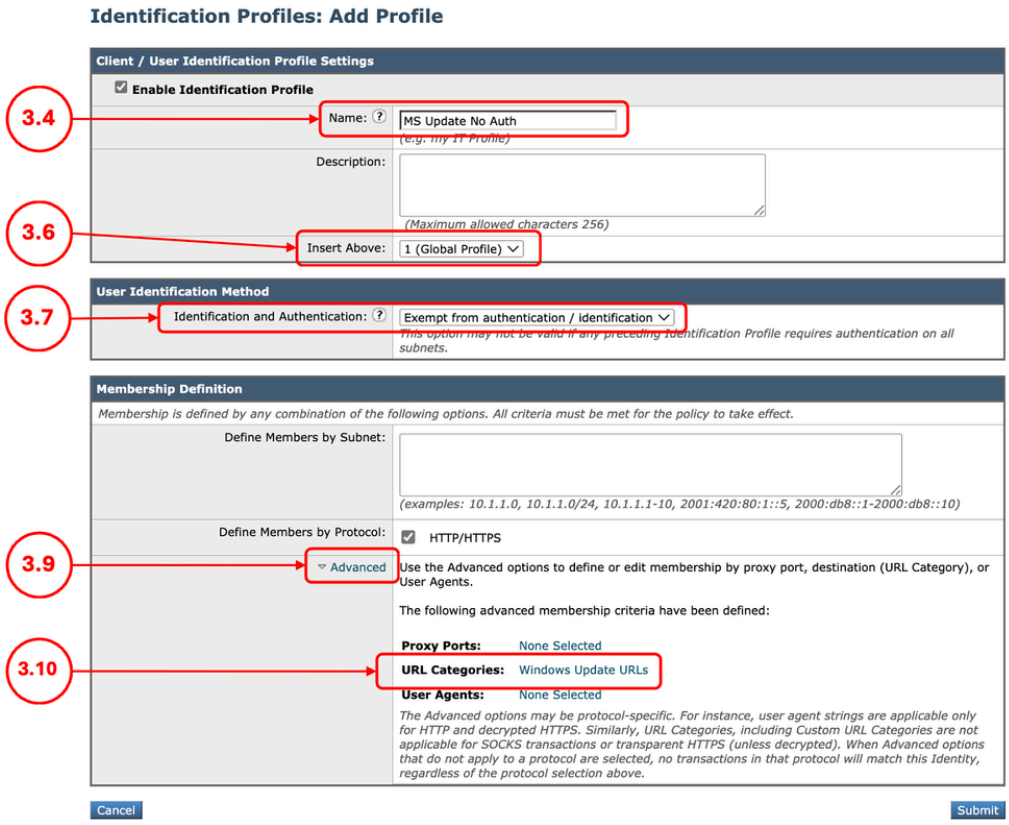
⚠ Precaución: la habilitación del reenvío de solicitudes de intervalo puede interferir con la eficacia de la visibilidad y el control de aplicaciones (AVC) basados en políticas y poner en peligro la seguridad.

Pasos para habilitar la solicitud de intervalo sólo para actualizaciones de Microsoft

Paso 1. Activar la Solicitud de Rango	Paso 1.1. Desde GUI, haga clic en Servicios de seguridad y elija Proxy Web. Paso 1.2. Haga clic en Editar configuración. Paso 1.3. Active la casilla de verificación Enable Range Request Forwarding. Paso 1.4. Haga clic en Enviar.  Imagen - Habilitar reenvío de solicitud de rango
Paso 2. Crear una categoría de URL personalizada para las URL de Microsoft Updates	Paso 2.1.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic en Categorías de URL externas y personalizadas. Paso 2.2.Haga clic en Agregar categoría para agregar una categoría de URL personalizada. Paso 2.3.Asignar un CategoryName único. Paso 2.4. (Opcional) Agregar descripción. Paso 2.5. En Orden de la lista, elija la primera categoría que desee colocar en la parte superior. Paso 2.6. En la lista desplegable Tipo de categoría, elija Categoría personalizada local. Paso 2.7. Agregue las URL de Microsoft Updates en la Sección Sites. Consejo: Puede consultar la lista de actualizaciones de Microsoft desde este enlace: Paso 2: Configuración de WSUS | Microsoft Learn Precaución: No copie/pegue las URL como están en los

	documentos de Microsoft; formatéelos correctamente como formato SWA. Para obtener más información, visite: Configure Custom URL Categories in Secure Web Appliance - Cisco
	
	Aquí tiene un ejemplo:
	
	`http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com`
	`http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com`
	
	Paso 2.8. Haga clic en Enviar.
	
	 
	
	Imagen: creación de una categoría de URL personalizada

Paso 3. (Opcional) Crear un perfil de identificación para eximir el tráfico de Microsoft Updates de la autenticación Nota: Esta acción es para reducir la carga de autenticación en el SWA para el tráfico a las actualizaciones	Paso 3.1.DesdeGUI, Elija Web Security Manager y haga clic en Perfiles de identificación. Paso 3.2.Haga clic en Agregar perfil para agregar un perfil. Paso 3.3.Asegúrese de que la casilla de verificación Enable Identification Profile está activada. Paso 3.4.Asignar un profileName único. Paso 3.5. (Opcional) Agregar descripción. Paso 3.6.En la lista desplegable Insertar arriba, elija dónde debe aparecer este perfil en la tabla. Paso 3.7. En la sección Método de identificación de usuario, elijaExento de autenticación/ identificación. Paso 3.8.En Define Members by Subnet (Definir miembros por subred), si desea transferir tráfico de Microsoft para algunos usuarios específicos, introduzca las direcciones IP o las subredes correspondientes, o bien

de Microsoft.	deje este campo en blanco para incluir todas las direcciones IP. Paso 3.9. En la sección Advanced, elija Custom URL Categories. Paso 3.10. Agregue la Categoría de URL personalizado que se creó para las actualizaciones de Microsoft. Paso 3.11. Haga clic en Finalizado. Paso 3.12. Haga clic en Enviar.  Imagen - Crear perfil de identificación
Paso 4. (Opcional) Crear una directiva de descifrado para pasar el tráfico de actualizaciones de Microsoft Nota: Microsoft Updates utiliza HTTP y el tráfico HTTPS para insertar los	Paso 4.1.DesdeGUI, ElegirAdministrador de seguridad web y, a continuación, haga clic enDirectiva de descifrado. Paso 4.2. Haga clic en Agregar política para agregar una política de descifrado. Paso 4.3.Asignar un único PolicyName. Paso 4.4. (Opcional) Agregar descripción. Paso 4.5.En la lista desplegable Insertar sobre política, elija la primera política. Paso 4.6.Desde Perfiles de Identificación y Usuarios, elija Seleccionar Uno o Más Perfiles de Identificación.

enlaces de actualizaciones. Esta acción es para reducir la carga de descifrado en el SWA.

Paso 4.7. Seleccione el perfil de identificación que creó en el paso 3 y vaya al paso 4.11.

Paso 4.8. Si no ha creado ningún perfil de ID para las actualizaciones de Windows, en la sección Avanzadas, elija Categorías de URL personalizadas.

Paso 4.9. Agregue la Categoría de URL personalizado que se creó para las actualizaciones de Microsoft en el Paso 2.

Paso 4.10. Haga clic en Finalizado.

Paso 4.11. Haga clic en Enviar.

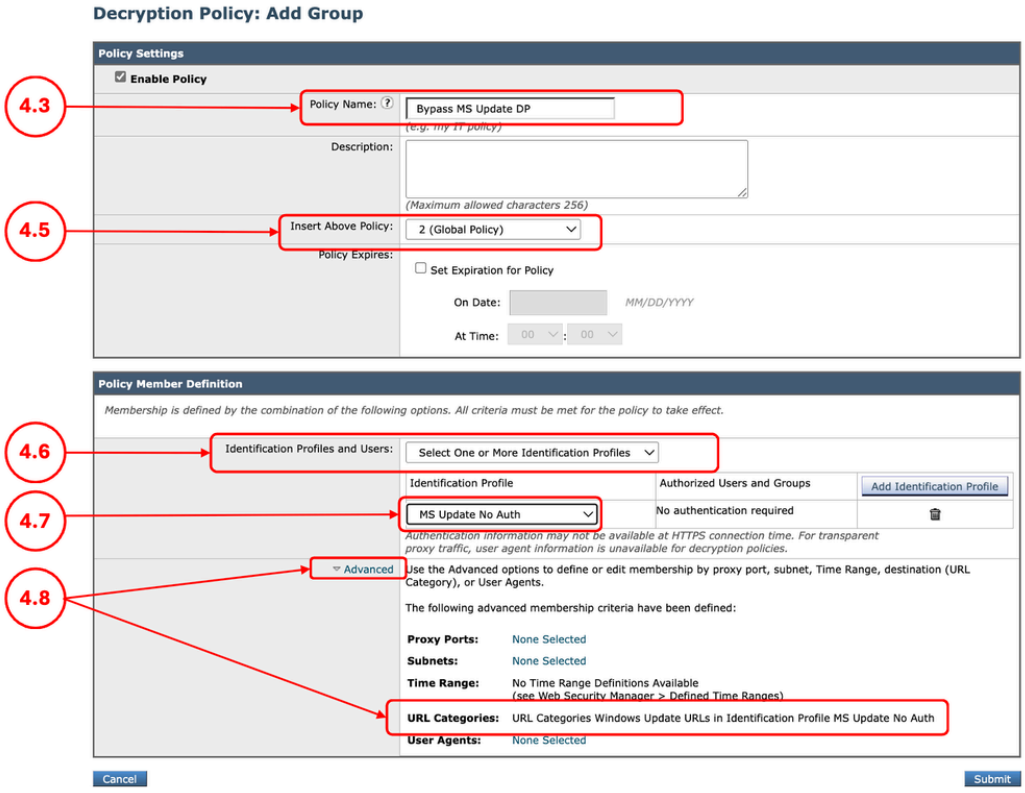
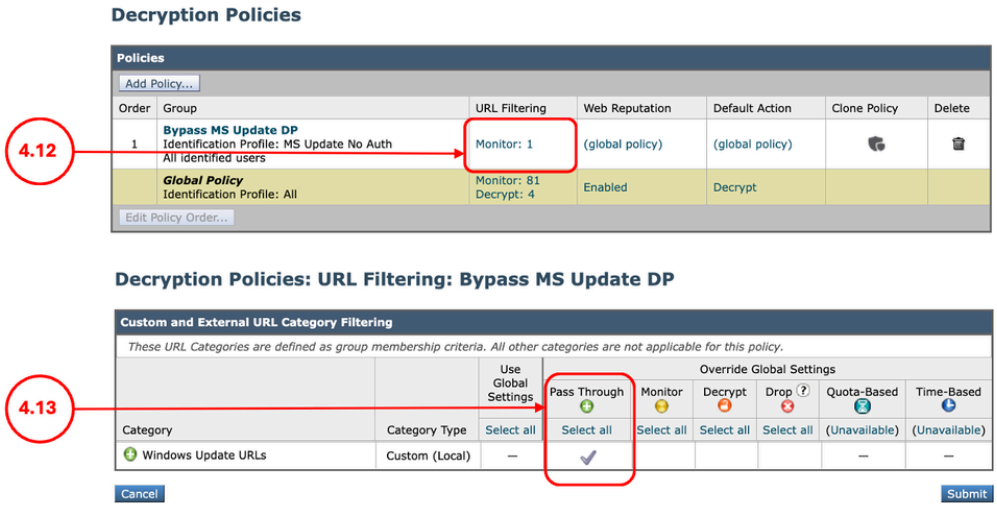


Imagen - Crear una política de descifrado

Paso 4.12.En la página Políticas de descifrado, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de descifrado.

Paso 4.13.SelectPassThrough como la acción para la categoría URL de Microsoft Updates.

	 Imagen: establezca el paso a través de acción para la categoría de URL Paso 4.12. Haga clic en Enviar.
Paso 5. Crear una directiva de acceso para permitir la solicitud de intervalo para el tráfico de actualizaciones de Microsoft	Paso 5.1.DesdeGUI, haga clic enAdministrador de seguridad web y elijaDirectiva de acceso. Paso 5.2. Haga clic en Agregar Política para agregar una Política de Acceso. Paso 5.3.Asignar un único PolicyName. Paso 5.4. (Opcional) Agregar descripción. Paso 5.5.En la lista desplegable Insertar sobre política, elija la primera política. Paso 5.6.Desde Perfiles de Identificación y Usuarios, elija Seleccionar Uno o Más Perfiles de Identificación. Paso 5.7. Seleccione el perfil de identificación que creó en el paso 3 y vaya directamente al paso 5.11. Paso 5.8. Si no ha creado ningún perfil de ID para las actualizaciones de Windows, en la sección Avanzadas, elija Categorías de URL personalizadas. Paso 5.9. Agregue la Categoría de URL personalizado que se creó para las actualizaciones de Microsoft en el Paso 2. Paso 5.10. Haga clic en Finalizado. Paso 5.11. Enviar.

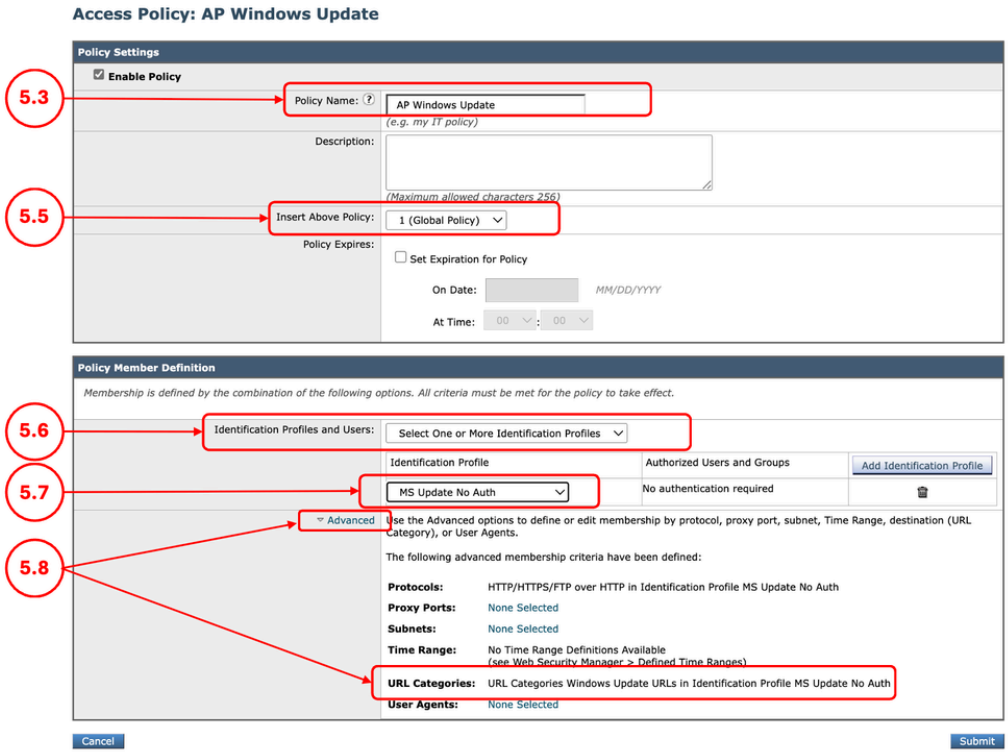


Imagen: creación de la política de acceso

Paso 5.12. En la página Políticas de acceso, en Filtrado de URL, haga clic en el enlace asociado a esta nueva política de acceso

Paso 5.13.Seleccione Permitir como la acción para la categoría URL personalizado creada para las actualizaciones de Microsoft.

Paso 5.14. Haga clic en Enviar.

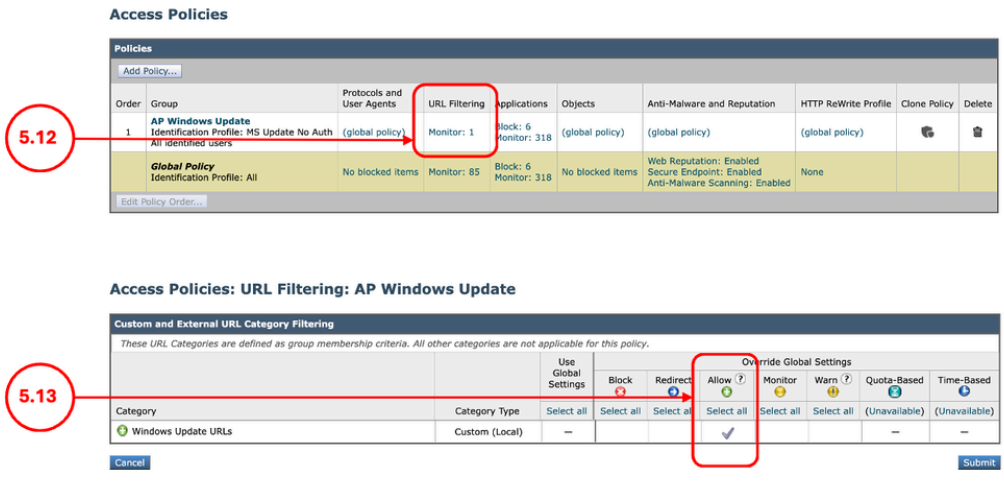


Imagen: establezca la acción Permitir para la categoría de URL

Paso 5.15. En la página Access Policies, en Applications, haga clic en el enlace asociado con esta nueva política de acceso

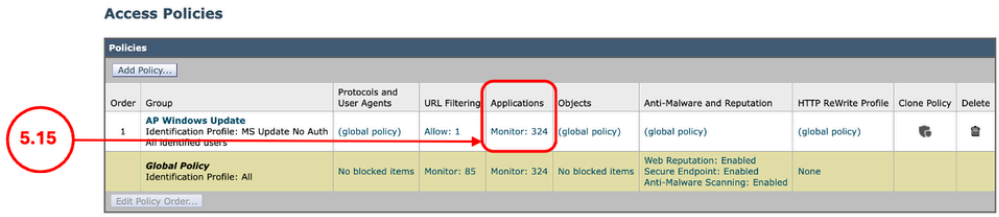


Imagen - Editar visibilidad y control de la aplicación

Paso 5.16. En la sección Editar configuración de aplicaciones, seleccione Definir configuración personalizada de aplicaciones.

Paso 5.17. En la sección Configuración de aplicaciones, haga clic en Editar todo para la aplicación Juegos y establezca la acción en Bloquear.

Paso 5.18. Hagan clic en Aplicar.

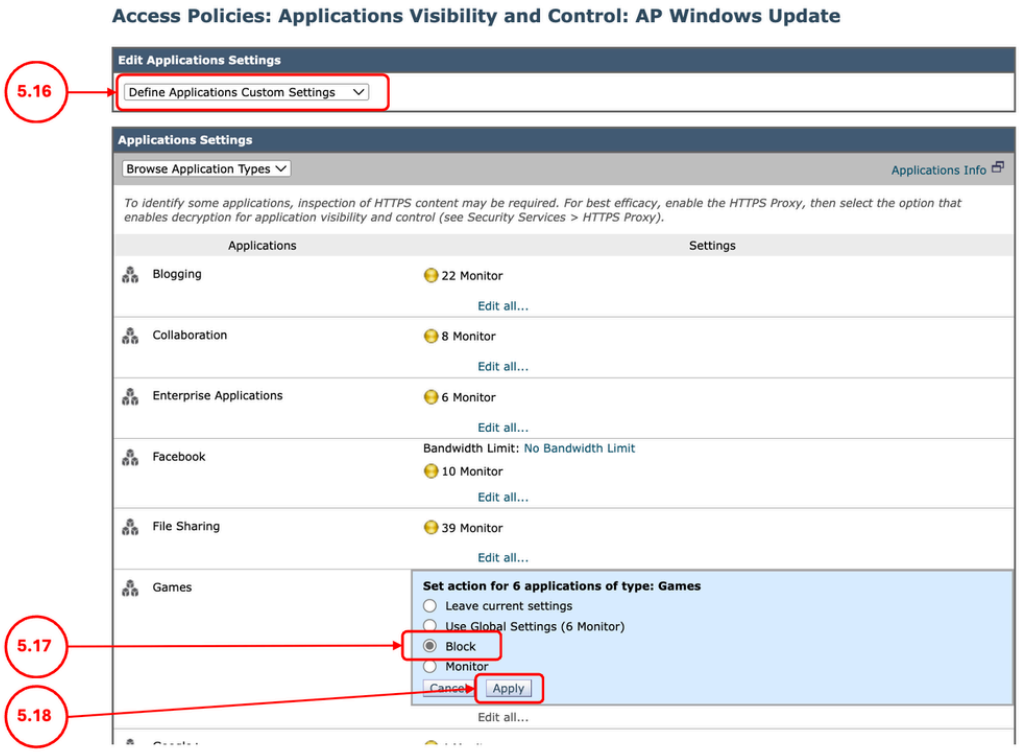


Imagen - Establecer una acción de aplicación en Bloquear

Paso 5.19. Desplácese hacia abajo hasta la sección Configuración de solicitudes de rango para la política, asegúrese de que Reenviar solicitudes de rango está seleccionado,

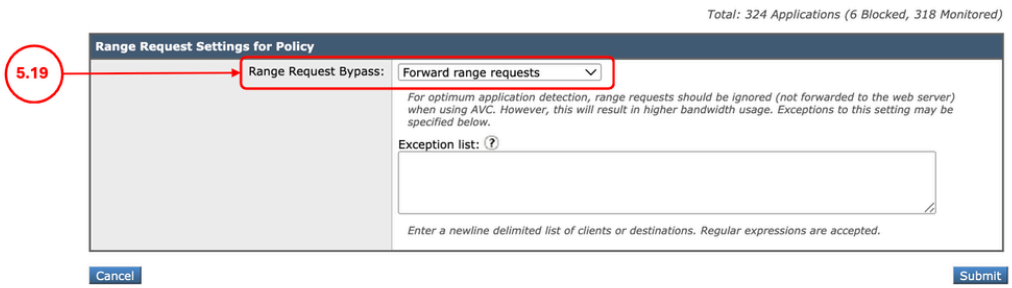


Imagen - Configuración de solicitud de rango para política

Paso 5.20. Enviar.

Paso 5.21. En la página Access Policies, en Applications, haga clic en el enlace asociado a la política global.

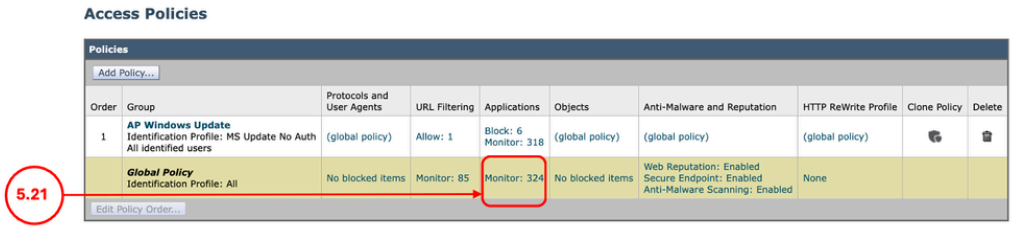


Imagen - Configuración de aplicación de política de acceso predeterminada

Paso 5.22. Desplácese hacia abajo hasta la sección Configuración de solicitud de rango para la política, asegúrese de que No reenviar solicitudes de rango está seleccionado,

Paso 5.23. Registrar cambios.

Modificación de los registros de acceso

Para tener más visibilidad de las solicitudes de rango de los registros de acceso, puede agregar estos campos personalizados:

[Intervalo de clientes = %<Intervalo:]	Muestra el intervalo solicitado por el cliente (bytes)
[content= %>Longitud del contenido:]	Muestra el tamaño del contenido descargado (bytes)

Para obtener más información sobre cómo agregar un campo personalizado a los registros de acceso SWA, visite este enlace: Configure Performance Parameter in Access Logs

Verificación

Utilice este comando CURL para enviar una solicitud de rango al SWA:

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

En el resultado del CURL, puede ver que la respuesta HTTP es HTTP/1.1.206:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

En Access Logs (Registros de acceso) puede ver que la acción es TCP_CLIENT_REFRESH_MISS/2006:

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

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
- Configurar el parámetro de rendimiento en registros de acceso
- 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).