Bloquear la descarga de archivos ejecutables en SWA

Contenido

Introducción

Este documento describe el proceso de configuración de Secure Web Appliance (SWA) para bloquear la descarga de archivos ejecutables.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

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

Antes de comenzar

Cisco SWA puede bloquear de forma eficaz la descarga de archivos ejecutables inspeccionando el tipo de contenido web MIME (Extensiones multipropósito de correo de Internet). Al identificar

tipos de archivos como application/x-msdownload, application/x-msi y otros tipos MIME relacionados, SWA aplica políticas que impiden que el ejecutable se entregue a los usuarios. Además de la detección de tipo MIME, SWA puede aprovechar el filtrado de extensiones de archivos, el análisis basado en la reputación y las reglas de políticas personalizadas para reforzar aún más la protección frente a descargas no deseadas o arriesgadas. Estas funciones ayudan a las organizaciones a mantener un entorno de navegación seguro y reducir el riesgo de infecciones de malware.

Consejo: SWA no puede identificar el tipo MIME del archivo, a menos que se descifre el tráfico.

---

application/octet-stream es un tipo MIME genérico utilizado para indicar que un archivo contiene datos binarios. No especifica la naturaleza del archivo, por lo que se puede utilizar para cualquier archivo que no se ajuste a un tipo MIME más específico. Este tipo se suele asignar a archivos ejecutables, instaladores y otros archivos que no son de texto cuando el servidor Web no puede determinar un tipo más preciso.

Configuration Steps

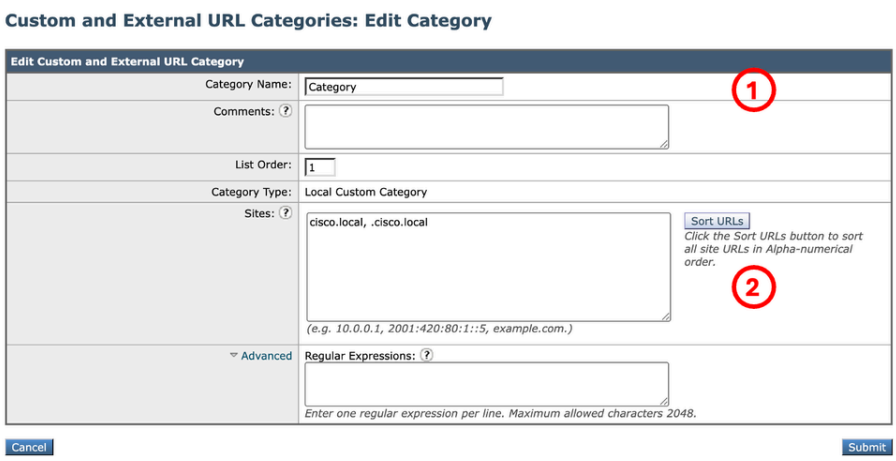
Paso 1.Cree una categoría de URL personalizada para el sitio web.	Paso 1.1.Desde la GUI vaya aWeb Security Manager y elijaCategorías de URL externas y personalizadas. Paso 1.2.Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada. Paso 1.3.EnterName para la nueva categoría. Paso 1.4.Defina el dominio y/o los subdominios del sitio web que está intentando bloquear el tráfico de carga (en este ejemplo es cisco.local y todos sus subdominios). Paso 1.5.Envíe los cambios. 

	Imagen - Crear categoría de URL personalizada Consejo: Para obtener más información sobre cómo configurar categorías de URL personalizadas, visite: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Paso 2.Descifrar el tráfico para la URL	Precaución: El descifrado de un gran número de URL puede reducir el rendimiento. Paso 2.1. Desde la GUI, vaya aAdministrador de seguridad web y elijaPolíticas de descifrado Paso 2.2.Haga clic en Agregar directiva. Paso 2.3.EnterName para la nueva política. Paso 2.4.(Opcional) Seleccione el perfil de identificación al que necesita que se aplique esta política. Consejo: (Opcional) Si desea aplicar la política para todos los usuarios, incluso si no están autenticados, elija Todos los usuarios (usuarios autenticados y no autenticados). Paso 2.5.Desde la sección Definición de miembro de política, haga clic en los enlaces URL para agregar la categoría de URL personalizado. Paso 2.6.Seleccione la categoría de URL que se creó enPaso 1. Paso 2.7.Haga clic en Enviar.

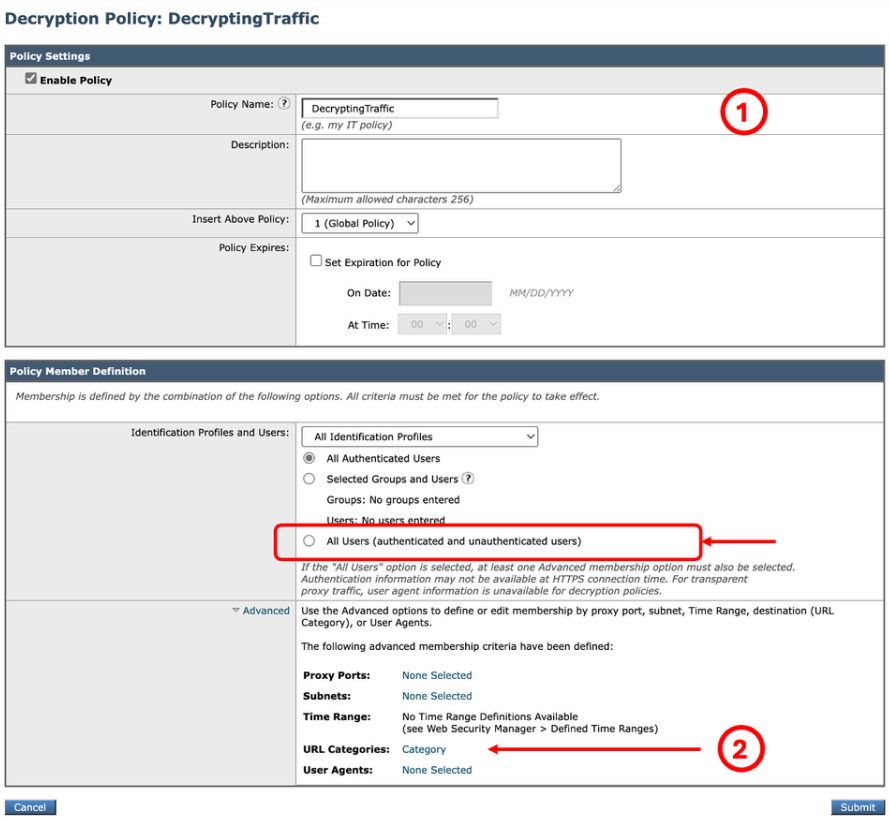


Imagen - Crear una política de descifrado

Paso 2.8.En la página Políticas de descifrado, haga clic en el enlace de Filtrado de URL para la nueva política.

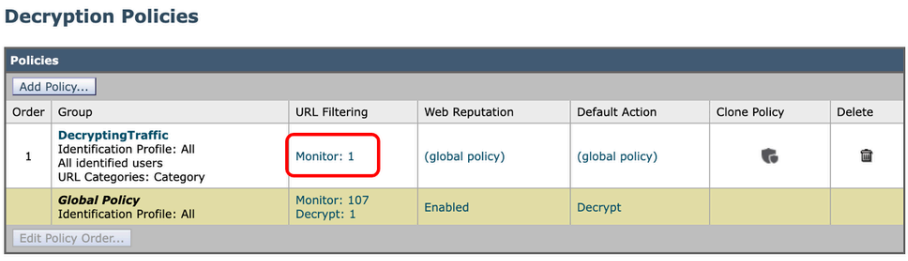


Imagen: seleccione el filtrado de URL

Paso 2.9.ChooseDecrypt como la acción para Custom URL Category.

Paso 2.10.Haga clic en Enviar.

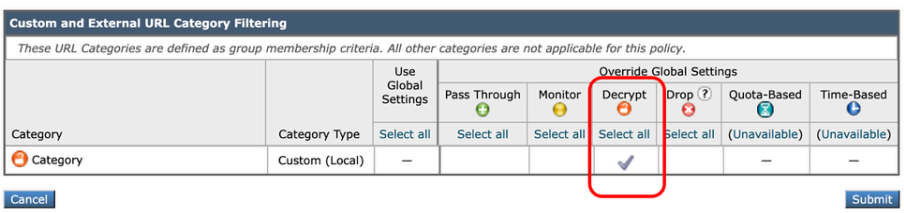
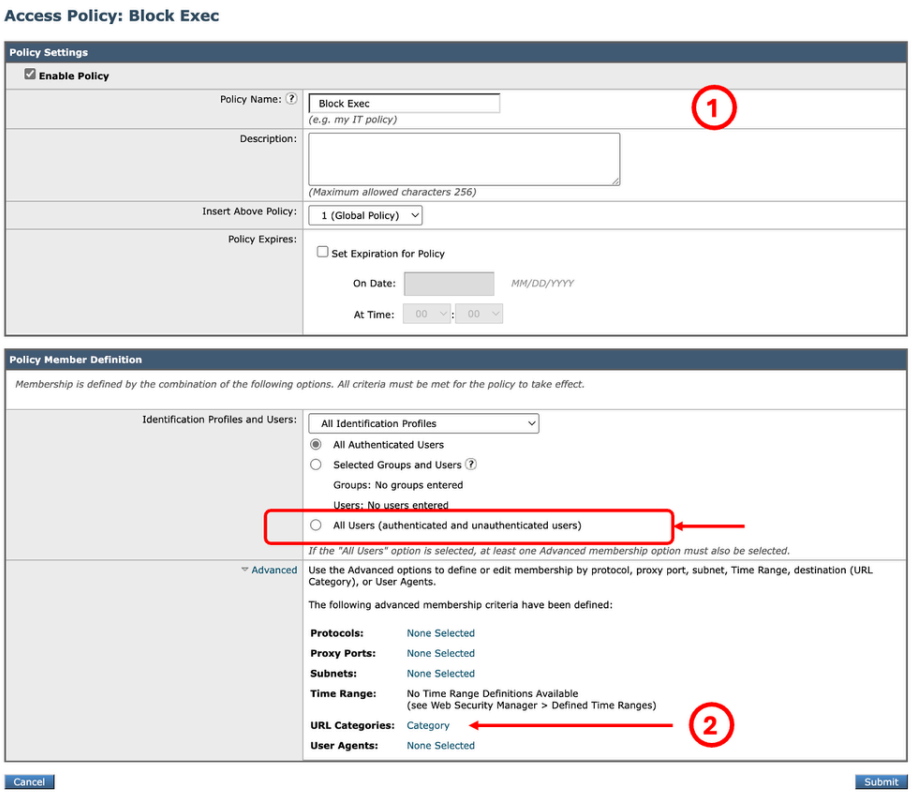


	Imagen - Establecer descifrado como acción
Paso 3.Bloquear los archivos ejecutables	Paso 3.1.En la GUI, vaya aAdministrador de seguridad web y elijaDirectivas de acceso. Paso 3.2.Haga clic en Agregar directiva. Paso 3.3.EnterName para la nueva política. Paso 3.4.(Opcional) Seleccione el perfil de identificación al que necesita que se aplique esta política. Consejo: (Opcional) Si desea aplicar la política para todos los usuarios, incluso si no están autenticados, elija Todos los usuarios (usuarios autenticados y no autenticados). Paso 3.5.Desde la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado. Paso 3.6.Seleccione la categoría de URL que se creó enPaso 1. Paso 3.7.Haga clic en Enviar.  Imagen - Política de acceso

Consejo: A efectos de generación de informes, es mejor elegir un nombre que no sea el mismo que el de cualquier otra política de acceso o descifrado.

Paso 3.8.En la página Políticas de acceso, asegúrese de que la acción Filtrado de URL está establecida en Monitor.

Paso 3.9. En la página Directivas de InAccess, haga clic en el enlace de Objetos para la nueva directiva.

Imagen: seleccione los objetos

Imagen: seleccione el filtrado de URL

Paso 3.10. En el menú desplegable, seleccione Definir configuración de bloqueo de objetos personalizados.

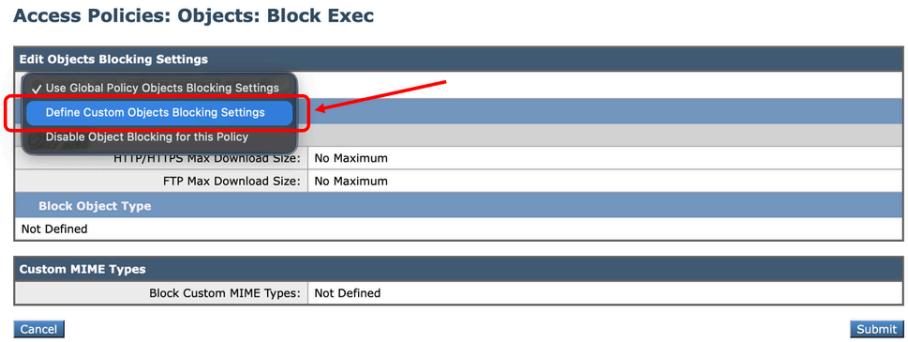


Imagen - Definir objetos personalizados

Paso 3.11.Haga clic en Código ejecutable para seleccionar los tipos de objetos que desea bloquear.

Paso 3.12.Haga clic en Instaladores para seleccionar los tipos de objetos que desea bloquear.

Paso 3.13. Además puede introducir los tipos MIME de los archivos que desea bloquear en la sección Tipos MIME personalizados.

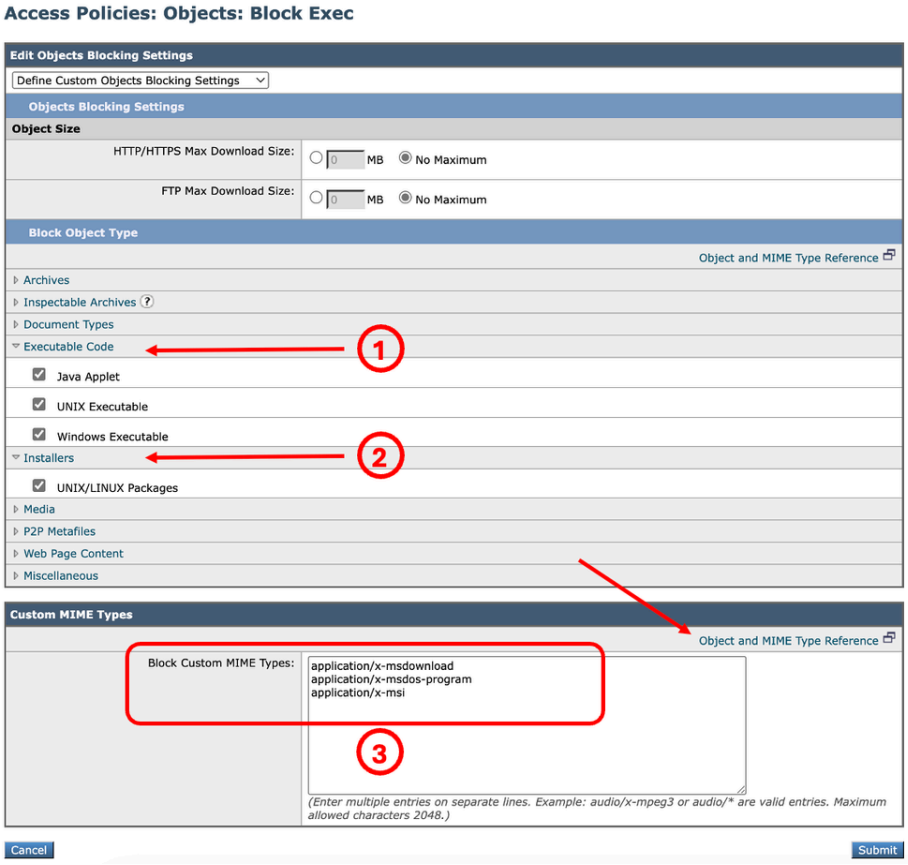


Imagen - Configuración de objetos para bloquear

Consejo: Para ver la lista de tipos MIME, haga clic en Referencia de tipo MIME y objeto.

Paso 3.14.Enviar.

Paso 3.15.Registrar cambios.

Validación del bloqueo de extensiones de archivo

En este ejemplo, cuando un usuario intenta descargar un archivo ejecutable, se muestra esta página de advertencia:

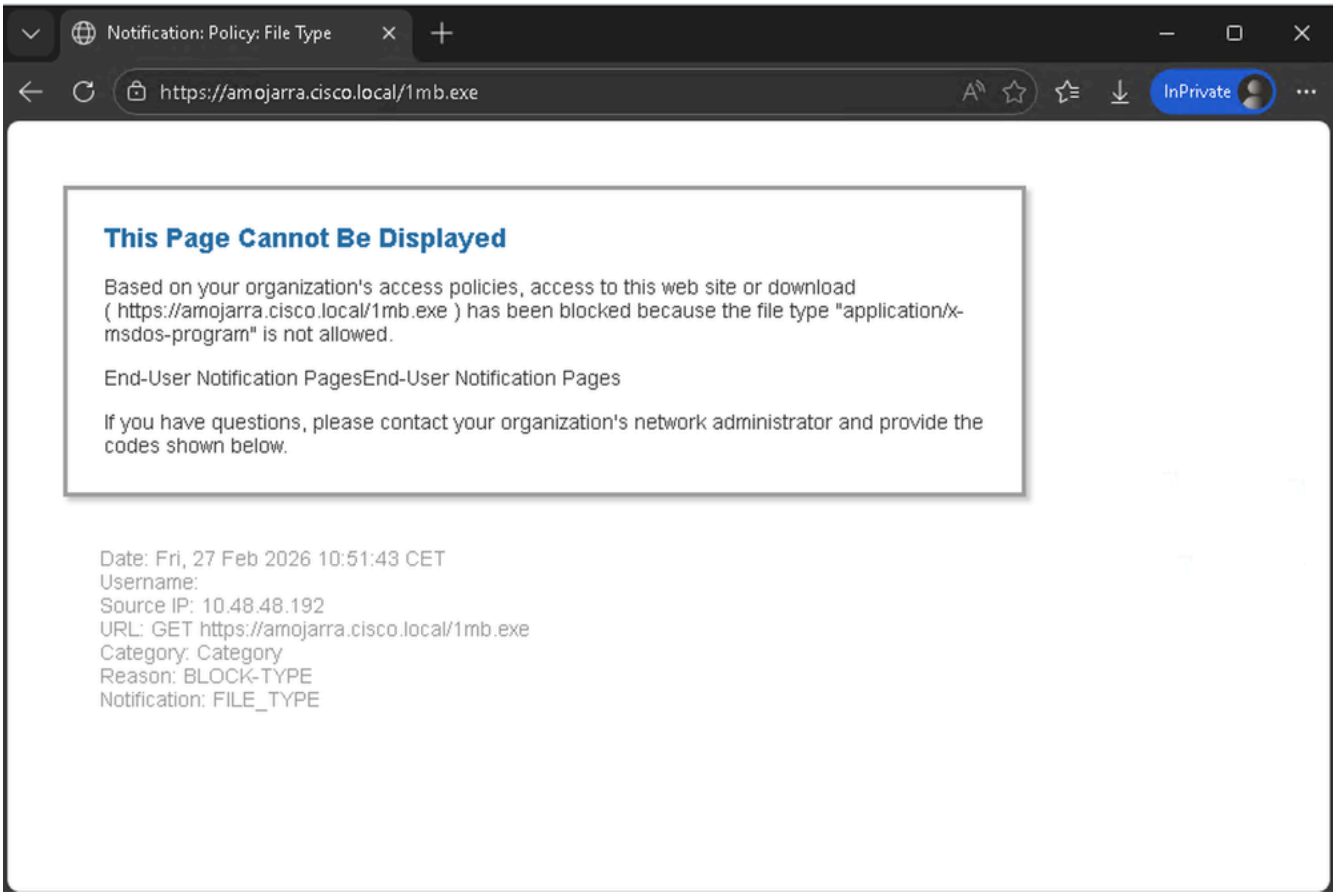


Imagen - Página de notificación de bloqueo

Consejo: Para configurar la página de notificación de usuario final (EUN), en la GUI, navegue hasta Servicios de seguridad y haga clic en Notificación de usuario final y modifique la sección Páginas de notificación de usuario final.

En los registros de acceso, puede ver dos líneas de registro relacionadas con el tráfico.

La primera línea del registro está relacionada con la política de descifrado (Nombre: DecryptingTraffic) que descifra el tráfico. La acción es DECRYPT_CUSTOMCAT

La segunda línea del registro de acceso está relacionada con la política de acceso (nombre: Block_Exec) que hemos creado en el paso 1.3. La acción es BLOCK_ADMIN_FILE_TYPE

Política	Registro de acceso
Política de descifrado	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-,"-,-,-,-,-",-,-,-,-,-,"-,-,-",-",-",-,-,-",-",-",-",-",-",-",-",-","-",-",-",1.71,0,-","-",-",-,"-,-,-,"-,-"-,-,-> -

Política de acceso	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-LAB_Access-NONE <"C_Cate",ns,0,"-",-,0,0,-,"-,-,-,-,"-,-,-,-,"-,"-",-,-,-,"nc",-,"-",-,"-,"-,"-,"-,"-,"-",00,0,-,"Desconocido","-,-,"-,-",-,-,-"-,-"-,-,-"-,-> -

Información Relacionada

- Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance
- Guía de instalación de Cisco Secure Email and Web Virtual Appliance
- Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco
- Uso de las prácticas recomendadas de Secure Web Appliance
- Configuración del firewall para el dispositivo web seguro
- Configurar certificado de descifrado en dispositivo web seguro
- Configuración y solución de problemas de SNMP en SWA
- Configuración de registros de inserción de SCP en un dispositivo web seguro con Microsoft Server
- Habilitar canal/vídeo específico de YouTube y bloquear el resto de YouTube en SWA
- Comprensión del formato de registro de acceso HTTPS en el dispositivo web seguro
- Acceder a registros de appliances web seguros
- Omitir autenticación en dispositivo web seguro
- Bloqueo del tráfico en el dispositivo web seguro
- Omitir tráfico de actualizaciones de Microsoft en dispositivo web seguro

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).