Cómo bloquear aplicaciones desconocidas en un dispositivo web seguro

Contenido

Introducción

Este documento describe varios métodos para bloquear aplicaciones desconocidas en Cisco Secure Web Appliance.

Métodos para bloquear aplicaciones desconocidas

Puede utilizar cualquiera de estos métodos solo o en combinación.

> **Nota:** Este artículo sobre Base de conocimiento hace referencia a software que no es mantenido ni soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para obtener asistencia adicional, comuníquese con el proveedor de software.

Bloquear aplicaciones basadas en cadenas de agentes de usuario

La primera defensa es utilizar cadenas de agente de usuario para bloquear aplicaciones desconocidas.

- Agregue el agente de usuario en **Web Security Manager** > **Access Policies** > **Protocols and User Agents** columna <para la política de acceso requerida>.
- Agregue la cadena de agente de usuario en **Block Custom User Agents** (uno por línea).

Nota: Puede utilizar los enlaces proporcionados en Referencia para buscar agentes de usuario.

Bloquear aplicaciones basadas en controles de visibilidad de aplicaciones

Si los controles de visibilidad de la aplicación (AVC) están habilitados (en **GUI > Security Services > Web Reputation and Anti-Malware**), a continuación, puede bloquear el acceso en función de tipos de aplicaciones como Proxies, Compartir archivos, Utilidades de Internet, etc. Puede hacer esto en **Web Security Manager > Access Policies > Applications** columna <para la política de acceso requerida>.

Bloquear aplicaciones basadas en el tipo MIME

Si el agente de usuario no existe, puede intentar agregar el tipo MIME (Extensiones multipropósito de correo de Internet):

- Agregar tipos MIME en **Web Security Manager** > **Web Access Policies** > **Objects** columna <para la política de acceso requerida>.
- Agregue el tipo de objeto/MIME en el **Block Custom MIME Types** (una por línea). Por ejemplo, para bloquear las aplicaciones BitTorrent, introduzca application/x-bittorrent.

Nota: Puede utilizar los enlaces proporcionados en Referencia para buscar tipos MIME.

Bloquear categorías de URL en políticas de acceso

Asegúrese de que las categorías como Evitar filtros, Actividades ilegales, Descargas ilegales, etc. se bloqueen en las políticas de acceso. Si algunas aplicaciones utilizan URL o direcciones IP conocidas para sus conexiones, puede bloquear sus categorías de URL predefinidas asociadas o configurarlas en una categoría de URL personalizada bloqueada mediante su dirección IP, nombre de dominio completo (FQDN) o un regex que coincida con los dominios. Puede hacer esto en **Web Security Manager > Access Policies > URL Categories** columna.

Restricción de la Configuración de Puertos HTTP CONNECT en la Política de Acceso

Algunas aplicaciones pueden utilizar el método HTTP CONNECT para conectarse a diferentes puertos. Sólo permita los puertos conocidos o los puertos específicos que se necesitan en su entorno en los dominios de configuración de puertos HTTP CONNECT:

- HTTP CONNECT se puede configurar en **Web Security Manager** > **Access Policies** > **Protocols and User Agents** columna <para la política de acceso requerida>.
- Agregar puertos permitidos en **HTTP CONNECT Ports**.

Block Access for Specific IP Addresses (Bloquear acceso para direcciones IP específicas)

Para las aplicaciones en las que sólo conoce las direcciones IP de destino a las que se está accediendo, puede utilizar la función Monitor de tráfico L4 para bloquear el acceso para esas direcciones IP específicas. Puede agregar las IP de destino en **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses.**

Cómo encontrar el agente de usuario o tipo MIME que utiliza una

aplicación

Si no sabe qué tipo de agente de usuario o MIME están utilizando determinadas aplicaciones, puede realizar cualquiera de estos pasos para encontrar esta información:

- Ejecute una captura de paquetes con WireShark (Ethernet) en el equipo del cliente y filtre el protocolo 'http'.
- Ejecute la captura en Secure Web Appliance (en **Support and Help** > **Packet Capture**), filtrado en la dirección IP del cliente.

Referencia

> **Nota:** Los sitios web externos enumerados aquí se proporcionan únicamente como referencia. Los enlaces y el contenido no están controlados por Cisco y están sujetos a cambios.

Lista de agentes de usuario

User Agent String.Com (en useragentstring.com)

Lista de tipos MIME

- Tipos MIME comunes (en mozilla.org)
- Tipos MIME: Lista completa de tipos MIME (en w3cub.com)
- La lista completa de tipos MIME (en sitepoint.com)