Aplique Umbrella DNS y evite el desvío con reglas de firewall

Contenido

Introducción

En este documento se describe cómo evitar la omisión de DNS y aplicar las protecciones de Umbrella DNS mediante reglas de firewall y políticas de red.

Prerequisites

- Firewall de red
- Privilegios de acceso del firewall
- Conocimiento de la configuración del firewall

Aplicación de Umbrella DNS: método más común

La mayoría de los routers y firewalls le permiten aplicar todo el tráfico DNS a través del puerto 53, lo que requiere que todos los dispositivos de red utilicen la configuración DNS definida en el router, que debe apuntar a los servidores Umbrella DNS.

El enfoque preferido es reenviar todas las solicitudes DNS de direcciones IP que no sean de Umbrella a las direcciones IP de Umbrella DNS que se muestran a continuación. Este método reenvía las solicitudes DNS de forma transparente e impide que la configuración manual de DNS simplemente falle.

Como alternativa, puede crear una regla de firewall para permitir DNS (TCP/UDP) solo a los

servidores Umbrella DNS y bloquear el resto del tráfico DNS a cualquier otra dirección IP.

Ejemplo de regla de firewall

1. Agregue esta regla al firewall perimetral:
    - Permitir TCP/UDP entrante y saliente hacia **208.67.222.222** o **208.67.220.220** en el puerto 53.
    - Bloquear TCP/UDP entrante y saliente a todas las direcciones IP del puerto 53.

La regla de permiso para Umbrella DNS tiene prioridad sobre la regla de bloqueo. Se permiten solicitudes DNS a Umbrella, mientras que el resto de solicitudes DNS se bloquean.

En función de la interfaz de configuración del firewall, configure una regla independiente para cada protocolo o una única regla que cubra TCP y UDP. Aplique la regla en el dispositivo de extremo de la red. También puede aplicar una regla similar a los firewalls de software en las estaciones de trabajo, como el firewall incorporado en Windows o macOS.

Si utiliza el cliente de itinerancia y la directiva de grupo de Active Directory, consulte la documentación sobre el bloqueo del cliente de itinerancia empresarial mediante la directiva de grupo.

Aplicación contra DNS sobre HTTPS (DoH)

Configuración recomendada

1. En Umbrella, habilite las categorías Proxy / AnonymizerandDoH / DoTcontent.
2. Bloquee las direcciones IP de los proveedores de DoH conocidos en su firewall.

Detalles y antecedentes

Umbrella admite eluse-application-dns.netdominio, según lo define Mozilla, para evitar que Firefox habilite DoH de forma predeterminada. Para obtener información sobre Firefox y DoH, consulte la documentación relacionada.

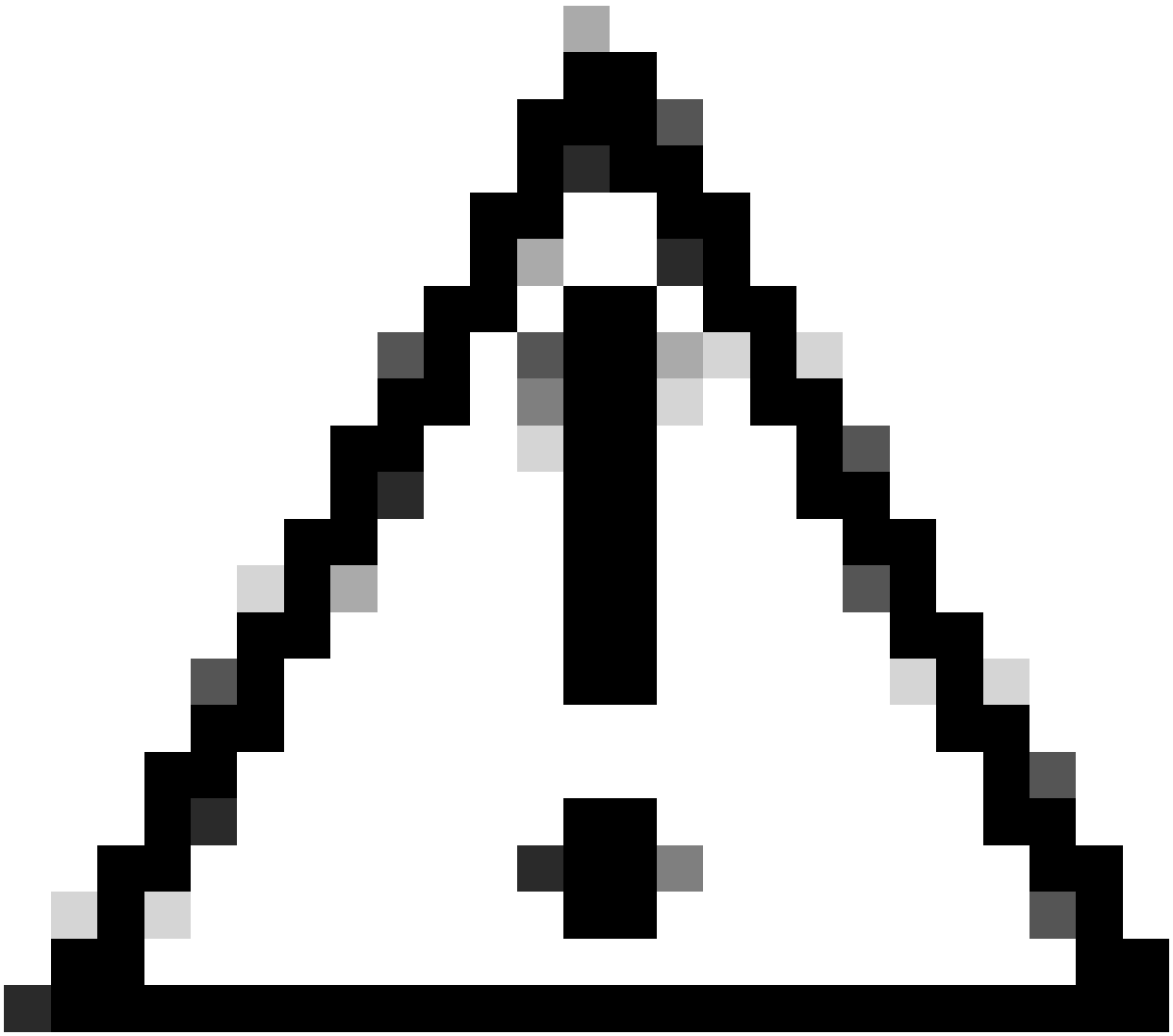
Incluso después de bloquear proveedores DNS alternativos, DNS se puede omitir con DoH. Una resolución DNS local traduce las solicitudes DNS a HTTPS y las envía a un terminal mediante JSON o POST/GET. Este tráfico normalmente evita la inspección de DNS.

Debido a que DoH se puede utilizar para omitir Umbrella, Umbrella incluye servidores DoH conocidos en la categoría de contenido Proxy / Anonymizer. Este mecanismo tiene algunas limitaciones:

- No puede bloquear proveedores de DoH completamente nuevos que aún no se conocen.
- No puede bloquear el DoH utilizado directamente a través de la dirección IP.

Para dirigirse a los nuevos proveedores de DoH, monitoree las actualizaciones y bloquee los dominios recién vistos para obtener una mejor cobertura.

Para DoH a través de la dirección IP, los escenarios son limitados. Firefox con CloudFlare es un ejemplo destacado.



Precaución: No agregue dominios del switch de eliminación de Mozilla a la lista de bloqueo. El bloqueo de estos dominios da como resultado un registro A para bloquear páginas, y Firefox lo trata como válido y actualiza automáticamente su uso de DoH.

Aplicación contra DNS sobre TLS (DoT)

Incluso después de bloquear proveedores DNS alternativos y DoH, DNS se puede omitir sobre TLS, que utiliza RFC7858 en el puerto 853. Por ejemplo, CloudFlare es un proveedor DoT.

Ejemplo de aplicación

- Bloquee las direcciones1.1.1.1IP y1.0.0.1en el puerto 853 (CloudFlare).

Renuncia de soporte de firewall

Este documento ayuda a los administradores de red a aplicar Umbrella DNS. Cisco Umbrella Support no proporciona asistencia con configuraciones de firewall o router individuales, ya que cada dispositivo tiene una interfaz de configuración única. Consulte la documentación del router o del firewall o póngase en contacto con el fabricante del dispositivo para confirmar si estas configuraciones son posibles.

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).