Comprender por qué las consultas de dominios internos no están registradas en Umbrella Insights

Contenido

Introducción

Este documento describe por qué no se registran las consultas de Dominios internos.

Overview

Cuando se utiliza Umbrella Insights, que incluye el dispositivo virtual (VA), todas las estaciones de trabajo deben tener únicamente la configuración de servidor DNS que apunte a los VA. Los dispositivos virtuales deben configurarse para utilizar los servidores DNS internos existentes. El panel le permite introducir una lista de 'Dominios internos' para que cuando el cliente realice una consulta DNS de un recurso interno, el VA reenvíe la solicitud a uno de los servidores DNS internos. Ocasionalmente se nos pregunta por qué ninguna de estas solicitudes internas aparece en el registro.

Explicación

Como se ha descrito anteriormente, las solicitudes de DNS internas recibidas por el VA se reenvían a uno de los servidores DNS internos configurados en el VA durante la configuración. Estos se pueden ver en la consola. Si todo está bien, el servidor DNS interno emite una respuesta y el VA retransmite esto al cliente.

Cuando el cliente realiza una solicitud DNS para un recurso que NO está en la lista de dominios internos, lo reenvía a las direcciones IP de difusión ilimitada de Umbrella. Esta solicitud incluye datos adicionales en la consulta DNS a nuestros resolvers, lo que permite que la solicitud esté vinculada a un origen. El origen podría ser, por ejemplo, un hash de ID de usuario, una IP de origen o una serie de otros factores de identificación que se incluyen en este paquete DNS extendido. Estos datos adicionales se pueden ver al ejecutar una consulta DNS específica desde una línea de comandos:

```
nslookup -server=208.67.222.222 -type=txt debug.opendns.com.
```

El registro real de solicitudes DNS tiene lugar en nuestros resolvers. El registro se basa en esta información única que se anexa al paquete DNS. El VA no registra las solicitudes DNS que reenvía. Es ante todo un servidor DNS recursivo. Una vez que nuestros resolvers públicos reciben una consulta DNS, utilizan los datos extendidos enviados con la consulta real para identificar el origen, aplicar la política apropiada y registrar la información de la solicitud y si se permitió o se bloqueó, que luego se muestra en el panel. Como las consultas DNS internas nunca ven nuestros resolvers, el registro de ellos no es posible.

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).

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).