NOTAS DE LA SOLUCIÓN

RESOLVER RETOS IMPREVISTOS CON DOT Y DOH

RESUMEN

Proteger su infraestructura del DNS es más importante que nunca: más del 90% de los incidentes de malware y más de la mitad de todos los ataques de ransomware y robo de datos utilizan el DNS como vector.

¿Sabe cuál es la buena noticia? Dos nuevas tecnologías en evolución, diseñadas para mejorar la privacidad del DNS, están logrando avances significativos.

¿Y la mala? Estas tecnologías dirigen los servidores y las aplicaciones a resolutores del DNS externos, lo que permite a los dispositivos suscriptores eludir los mecanismos del DNS tradicionales y acceder a servicios del DNS que quedan fuera de su control, exponiendo a la empresa a posibles riesgos de seguridad. Y estos cambios están produciéndose ahora mismo.

Infoblox ofrece a las organizaciones soluciones que resuelven estos retos de privacidad del DNS. La capacidad de bloquear el acceso a los resolutores del DNS externos y proporcionar resolución del DNS cifrada interna permite a las organizaciones mantener el control sobre el DNS.

MARGEN DE MEJORA

El concepto de apertura ha sido una característica fundamental de internet desde sus inicios. Aunque los usuarios transmiten información confidencial, como números de tarjetas de crédito, correos electrónicos y contraseñas, entre sus navegadores web y los sitios web utilizando el protocolo seguro HTTPS, las solicitudes iniciales de direcciones de internet y las respuestas posteriores para localizar los sitios web se transmiten como texto sin cifrar. Como resultado, el DNS ha sufrido tradicionalmente lo que describimos como un problema de seguridad de «último kilómetro». Las comunicaciones entre un cliente del DNS y el servidor del DNS local casi nunca se cifran y, por lo tanto, están sujetas a suplantación de identidad, interceptación, secuestro y otros problemas. Aunque se han efectuado mejoras en el pasado para incorporar una mayor seguridad de extremo a extremo, el último tramo de la comunicación con el navegador web seguía expuesto a la suplantación de identidad.

INTRODUCCIÓN DE DOT Y DOH

Los grupos industriales que trabajan en el seno del Grupo de Trabajo de Ingeniería de Internet (IETF) han propuesto dos mecanismos para abordar estas cuestiones, que cifran la comunicación del DNS entre el resolutor stub de su sistema operativo o una aplicación local y el resolutor del DNS recursivo. Uno se conoce como DNS sobre TLS (seguridad de la capa de transporte) o DoT, y el otro como DNS sobre HTTPS o DoH. Aunque DoT y DoH se diseñaron para abordar los problemas de privacidad del DNS, también introducen cambios significativos en el comportamiento del DNS en cuanto al funcionamiento de los navegadores y las aplicaciones. Estos cambios crean una complejidad adicional y consecuencias no deseadas para la seguridad de la red, y afectan directamente a la prestación de servicios de seguridad y filtrado de contenidos por parte de las empresas. DoT y DoH pueden dirigir los servidores y las aplicaciones a resolutores DNS externos, lo que permite a los dispositivos cliente eludir los mecanismos del DNS tradicionales y acceder a servicios del DNS fuera de su control, exponiendo a la empresa a posibles riesgos de seguridad. Un ejemplo claro: la Agencia de Seguridad Nacional estadounidense (NSA) publicó recientemente una guía en la que recomienda a las organizaciones que alojen sus propios resolutores DoH y eviten enviar tráfico del DNS interno a resolutores externos de terceros.

DNS SOBRE TLS (DOT)

DoT es un estándar del IETF que utiliza el protocolo de control de transmisión (TCP) común como protocolo de conexión para superponer el cifrado y la autenticación TLS entre un cliente y un servidor del DNS. Habitualmente funciona a nivel del sistema operativo y se comunica a través del puerto TCP 853. Este puerto se utiliza para todo el tráfico del DNS cifrado y los administradores de red están muy familiarizados con él. El tráfico de DNS sobre TLS se cifra, pero su uso de un puerto bien conocido facilita a los administradores de red la supervisión y el control del DNS cifrado cuando se produce. DoT es también un estándar maduro, respaldado por los actores tradicionales de la industria del DNS.

DNS SOBRE HTTPS (DOH)

DoH, respaldado por Apple, Microsoft, la Fundación Mozilla y Chromium Projects, es el otro protocolo de seguridad del IETF que aborda la seguridad de las comunicaciones entre clientes y servidores del DNS. Aprovecha la extensión del protocolo de seguridad HTTPS para proporcionar cifrado y autenticación entre un cliente y un servidor del DNS.

Un problema potencial del DoH es que utiliza el mismo puerto TCP (443) que todo el tráfico HTTPS. Puede resultar difícil solucionar los problemas del DNS relacionados con DoH debido a la imposibilidad de distinguir las solicitudes del DNS basadas en DoH de las solicitudes HTTPS estándar. Por ejemplo, si un administrador de red utiliza la supervisión del DNS para bloquear las solicitudes al DNS de dominios maliciosos conocidos, no verá esas solicitudes en HTTPS. Por lo tanto, ese tráfico malicioso pasará desapercibido.

Además, DoH se implementa a menudo en la capa de aplicaciones en lugar de en el sistema operativo, lo que introduce la posibilidad de que el tráfico del navegador eluda los controles del DNS empresariales. Eludir los controles del DNS podría dificultar la capacidad del equipo de asistencia para mantener los niveles de rendimiento, seguridad, escala y fiabilidad de la red que las empresas exigen al DNS.

RETOS EMPRESARIALES DE DOT Y DOH

Los administradores de redes y seguridad confían en el DNS como elemento importante del plano de control de la red para garantizar acceso rápido a las aplicaciones y mantener a los usuarios a salvo del malware y otras amenazas de internet. Entre los retos más importantes a los que pueden enfrentarse los equipos de redes y seguridad debido a los nuevos estándares DoT y DoH se incluyen:

- **DNS centralizado:** El control externo del DNS puede permitir a los clientes utilizar resolutores del DNS centralizados controlados por terceros y no proporcionados por el departamento de TI, lo que introduce riesgos y dificulta la gestión y la seguridad de los recursos de red.
- **Elusión de los controles empresariales:** DoH introduce específicamente la posibilidad de que cientos de aplicaciones y sitios web, cada uno con su propia configuración DoH, eludan los controles del DNS. Además de complicar la supervisión de exploits como el secuestro del DNS, DoH también hace posible eludir los filtros de contenido empresarial, como contenido para adultos, juegos, streaming y malware.
- **Exposición a la exfiltración de datos y a la proliferación de malware:** si no se controla, el DoH puede aumentar la exposición a la exfiltración de datos y a la proliferación de malware, ya que puede abrir puertas traseras a redes protegidas. Los ciberdelincuentes suelen utilizar el DNS como puerta trasera para obtener y exportar información comercial sensible y para propagar malware a través de comunicaciones de comando y control (C&C) con dispositivos. La solicitud DNS DoH está cifrada y, por lo tanto, es invisible para terceros, incluido el software de ciberseguridad que puede basarse en la supervisión pasiva del DNS para bloquear las solicitudes a dominios maliciosos conocidos. Normalmente, los equipos de seguridad pueden detener estos ataques de forma eficaz utilizando inteligencia sobre amenazas en la infraestructura DNS interna, combinada con análisis basados en inteligencia artificial y aprendizaje automático. Dado que el DoH elude estas medidas de seguridad del DNS, existe un nuevo riesgo de que las empresas se vean expuestas a estos y otros filtros basados en el DNS.

  Por ejemplo, las versiones recientes del malware PsiXBot utilizan DoH para cifrar las comunicaciones maliciosas, lo que le permite ocultarse en el tráfico HTTPS normal e instalar malware que puede robar datos o añadir a la víctima a una botnet.

- **Aumento de la sobrecarga/disminución del rendimiento del servidor del DNS:** DoT y DoH aumentan la carga que cada consulta al DNS impone al servidor del DNS y pueden afectar a la calidad de la experiencia del usuario. El DNS tradicional se basa en el protocolo de datagramas de usuario e introduce una sobrecarga mínima. Tanto DoT como DoH se ejecutan sobre TCP, que consume más recursos en un servidor del DNS. Además, tanto DoT como DoH requieren que el servidor del DNS descifre la consulta y cifre la respuesta, lo que aumenta aún más su sobrecarga. Los administradores de servidores del DNS deben prever que con DoH y DoT sus servidores solo podrán gestionar una fracción de las consultas tradicionales al DNS que antes gestionaban.

NAVEGADORES Y SISTEMAS OPERATIVOS DIFERENTES

Planes de implementación

Numerosos proveedores de DNS recursivos públicos, como Google DNS, Cloudflare y Quad9, incluyen DoT y DoH como parte de sus ofertas. Muchos clientes de sistemas operativos deben activar DoT (aunque muchos clientes de Android están configurados para utilizar DoT de forma predeterminada). Sin embargo, con DoH, los navegadores web como Chromium y Mozilla requieren sus propios métodos para que los clientes se conecten.

Chromium

La implementación de DoH en Chromium afecta a todos los navegadores basados en el proyecto Chromium, incluidos Google Chrome, Microsoft Edge y Opera. Chromium se configura de forma predeterminada en un modo automático que comprueba una lista compatible de resolutores configurados por el sistema operativo para ver si DoH está disponible y, a continuación, utiliza el resolutor configurado para DoH solo si está disponible. También está previsto que observe la configuración DoT del cliente del sistema operativo en Android y actuar de forma controlable y predecible. Para la mayoría de los clientes de Infoblox, los cambios de Chromium posiblemente no requieran cambiar el resolutor ni la red.

Mozilla

Mozilla ofrece Cloudflare como resolutor recursivo de confianza predeterminado que utiliza DoH. Mozilla intentará detectar y desactivar el uso de DoH cuando lo considere necesario. Lamentablemente, los métodos utilizados en una degradación elegante de la resolución del DNS tradicional aún no se han probado y es posible que no se adapten a todas las situaciones. Es posible que algunas empresas no tengan control total sobre los navegadores instalados en su organización.

Por ejemplo, puede resultar difícil garantizar el cumplimiento de las preferencias de la empresa en cuanto a la configuración del navegador en dispositivos BYOD, el teletrabajo y otros escenarios móviles. Del mismo modo, los proveedores de servicios de comunicaciones con usuarios finales diversos tendrán aún menos influencia sobre la configuración de los navegadores en los dispositivos de red.

Apple

Las versiones recientemente lanzadas de iOS y macOS de Apple son compatibles con los protocolos DoT y DoH. Esta configuración se puede aplicar de forma selectiva, desde todo el sistema operativo a través de perfiles MDM o extensiones de red, hasta aplicaciones individuales o solicitudes de red seleccionadas de aplicaciones.

Según Apple, hay tres formas de habilitar el DNS cifrado. Una opción puede aplicar la configuración del DNS cifrado en todo el sistema, donde los usuarios o administradores pueden elegir un único servidor del DNS cifrado como resolutor predeterminado para todas las aplicaciones del sistema operativo. Los desarrolladores pueden crear aplicaciones de extensión de red que configuren el sistema operativo para utilizar ese servidor, o pueden enviarse perfiles MDM a los clientes, que configuren los ajustes del DNS cifrado. Si no se utiliza esta opción, las otras dos se activan de modo automático y el propietario del dispositivo no puede desactivarlas directamente.

La segunda opción es para los propietarios de dominios. Pueden configurar ajustes a nivel de dominio que indican la existencia de un resolutor cifrado para el dominio. Si se detectan y verifican estos ajustes, el tráfico DNS de ese dominio se redirige al resolutor cifrado proporcionado por el dominio.

La última opción es el DNS cifrado en la capa de aplicaciones. En ella, los desarrolladores pueden crear aplicaciones que permitan a las aplicaciones utilizar DoT y DoH directamente desde aplicaciones individuales. Esta opción significa que los desarrolladores pueden seleccionar un servidor específico para algunas o todas las conexiones de sus aplicaciones cuando el sistema operativo no está configurado.

Apple tiene previsto advertir a los usuarios con un mensaje específico en caso de que una red concreta bloquee las comunicaciones del DNS cifrado en la red mediante una política. Las redes específicas se marcarán visualmente con una advertencia de privacidad, y las aplicaciones configuradas para utilizar resolutores DoH específicos no se comunicarán correctamente.

Microsoft

Microsoft anunció su intención de admitir DoH en 2019 y ha adoptado DoH en el cliente DNS de Windows, con la opción de admitir DoT en futuras versiones. Microsoft diseñó su enfoque bajo la premisa de que los usuarios no precisen conocimientos especializados para utilizar DoH, al tiempo que permite a los administradores de red mantener el control mediante el degradado hacia el protocolo del DNS tradicional.

Una vez configurado, el cliente del DNS funcionará en «modo oportunista», lo que significa que intentará utilizar el protocolo DoH en lugar del DNS tradicional. Sin embargo, el cliente puede configurarse para recurrir al DNS convencional si los protocolos DoH no están disponibles o no responden. Los resolutores DoH de confianza iniciales serían Cloudflare, Google y Quad9.

INFOBLOX RESUELVE LOS RETOS DE DOT Y DOH

Como líder del sector en servicios de red seguros y gestionados en la nube, Infoblox sostiene que eludir la infraestructura del DNS interna existente aumenta la complejidad operativa. Estas nuevas opciones de privacidad del DNS apenas están empezando a desarrollarse. Las organizaciones deben tomar medidas ahora para reducir los riesgos que plantean estas tecnologías. Como mínimo, un excelente punto de partida es bloquear el tráfico del DNS directo —incluidos DoT y DoH— entre las direcciones IP internas y los servidores del DNS en internet (Figura 1). Este paso garantizará que los usuarios finales utilicen la infraestructura del DNS interna de la empresa, lo que permitirá al equipo de TI aplicar una política de resolución del DNS exhaustiva y solucionar problemas. Infoblox ofrece a las organizaciones soluciones que resuelven estos retos de privacidad del DNS. La capacidad de bloquear el acceso a los resolutores del DNS externos y proporcionar resolución del DNS cifrada interna permite a las organizaciones mantener el control sobre el DNS.

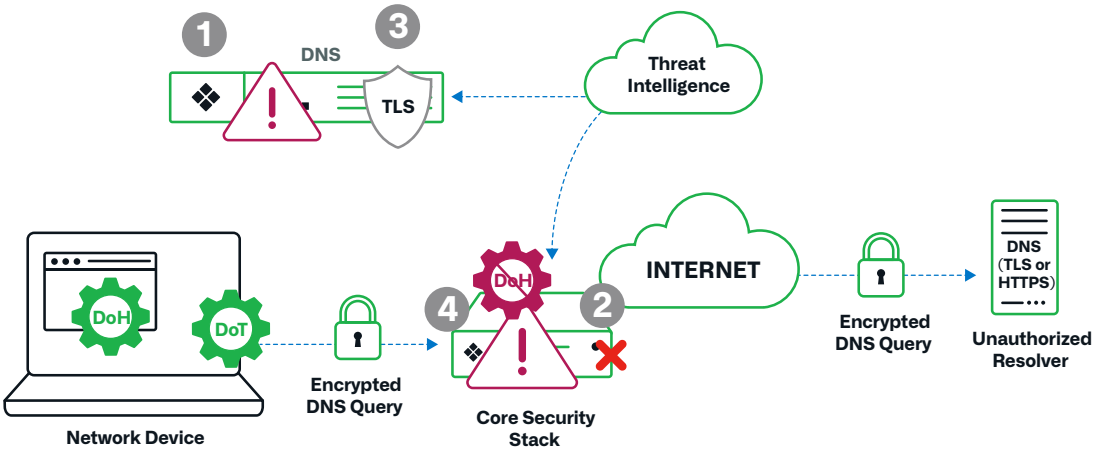

Figura 1: Las prácticas recomendadas de DoT/DoH protegen a sus usuarios y dispositivos

Bloqueo de la resolución de dominios DoH

BloxOne® Threat Defense, una solución de seguridad híbrida fundamental de Infoblox, utiliza el DNS como primera línea de defensa. Bloquea la resolución de dominios DoH y facilita una transición fluida al DNS interno existente. Estas capacidades ayudan a prevenir el uso indebido de DoH y a mitigar el riesgo.

BloxOne Threat Defense incluye varias funciones que ayudan a gestionar DoH:

- Las fuentes de información sobre amenazas de políticas para DoH proporcionan a los administradores de red la capacidad de controlar el método de acceso DNS utilizado para detectar y mitigar amenazas mediante la desactivación de las políticas de seguridad basadas en DoH. Los navegadores volverán sin problemas al DNS gestionado por la organización sin interrumpir la actividad del usuario.
- Se ha añadido una fuente de políticas DoH para IP y dominios DoH conocidos a Threat Intelligence Data Exchange, la plataforma de agregación y distribución de inteligencia sobre amenazas de Infoblox. Otras herramientas de seguridad, como los NGFW, pueden utilizar esta fuente de datos y la inteligencia relacionada para bloquear el tráfico DoH hacia servidores externos.
- Los usuarios pueden revisar los dominios y las IP relacionados con DoH en Dossier, la herramienta de investigación de amenazas de Infoblox.

Estas capacidades están disponibles con todos los niveles de suscripción de BloxOne Threat Defense.

DNS cifrado de Infoblox

Network Identity Operating System (NIOS) es el sistema operativo de identidad de red de Infoblox que impulsa los servicios de red básicos para garantizar el funcionamiento ininterrumpido de la infraestructura de red.

Encrypted DNS de Infoblox es una función de NIOS que proporciona un cifrado eficiente, a la vez que ofrece los mejores servicios del DNS de Infoblox. Las capacidades de lanzamiento incluyen la compatibilidad con DoH y DoT.

Encrypted DNS de Infoblox ofrece un enfoque único para cifrar el tráfico del DNS. A diferencia de los métodos que dependen de equilibradores de carga o del sobreaprovisionamiento, Encrypted DNS de Infoblox se ejecuta como un único servicio para todas sus necesidades en el DNS. Nuestras funciones estándar, que incluyen protección avanzada del DNS y aceleración de la caché del DNS, están disponibles en el mismo servicio del DNS, altamente escalable.

CONCLUSIÓN

Infoblox se compromete a ayudar a sus clientes a mantener el rendimiento, la seguridad, la escalabilidad y la fiabilidad que exigen las redes empresariales modernas. Estos cambios se están produciendo en este mismo momento, ya que las recientes actualizaciones de los navegadores y las nuevas versiones de los sistemas operativos implementan estos cambios en las redes actuales. Si bien resolver el problema del «último kilómetro» es esencial y merece el esfuerzo, también reconocemos que las empresas deben mantener la visibilidad y el control sobre su tráfico del DNS. Importantes organismos de seguridad, como la NSA, recomiendan que las organizaciones tomen medidas para reducir los riesgos que plantean estas tecnologías. Los clientes pueden aprovechar las soluciones de Infoblox para mantener el control de su DNS y mitigar problemas imprevistos derivados de las nuevas iniciativas de privacidad del DNS. Para obtener más información, visite la comunidad de Infoblox y descubra estas tecnologías en constante evolución y las soluciones de Infoblox.

Sede corporativa
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054 (EE. UU.)

+1.408.986.4000
www.infoblox.com/es

Versión: 20230919v1