HOJA DE DATOS

Fortalecer la ciberseguridad federal con DNS cifrado

Implementar el DNS cifrado de conformidad con la Orden Ejecutiva de la Casa Blanca

RESUMEN

En unas directrices recientes, la Casa Blanca emitió una Orden Ejecutiva integral destinada a fortalecer y promover la ciberseguridad del país. Dicha Orden Ejecutiva tiene por objeto mejorar la ciberseguridad a través de la rendición de cuentas de los proveedores de software y servicios en la nube, el refuerzo de los sistemas federales de comunicaciones y gestión de la identidad, y la promoción del uso de tecnologías emergentes en todos los departamentos y agencias ejecutivos. Entre las medidas clave introducidas destaca la exigencia de protocolos de DNS cifrados, que garanticen la confidencialidad y la integridad del tráfico del DNS. Se reconoce el DNS como control de seguridad de primera línea y se resalta su importancia en la estrategia de defensa en profundidad de la ciberseguridad.

En línea con las recientes disposiciones federales de ciberseguridad, Advanced DNS Protection (ADP) de Infoblox ofrece un sólido soporte para el tráfico del DNS cifrado, que garantiza la confidencialidad y la integridad de las comunicaciones del DNS. Esta capacidad es esencial para las agencias federales que tratan de mejorar sus medidas de ciberseguridad y de cumplir la reciente orden ejecutiva de la Casa Blanca sobre el DNS cifrado.

Las soluciones de Infoblox son completas, escalables y fáciles de implementar, lo que posibilita una transición fluida al DNS cifrado con una interrupción mínima. Es importante destacar que más de 15 agencias federales civiles de EE. UU. están utilizando el cifrado del DNS de Infoblox, incluido en Advanced DNS Protection. Esta adopción las ayuda a avanzar en la política de seguridad, al habilitar el cifrado del DNS en apoyo de sus iniciativas de confianza cero.

DESAFÍOS DE LA AGENCIA

El DNS cifrado requiere recursos informáticos adicionales, especialmente en los servidores del DNS, ya que exige proceder al cifrado y descifrado al enviar y recibir mensajes del DNS. Las agencias deben anticiparse y asegurar que sus servidores del DNS cuentan con recursos suficientes para gestionar la carga de consultas antes de iniciar cualquier implementación generalizada del DNS cifrado. Si el DNS cifrado no se implementa adecuadamente, se podrían dañar todas las redes y aplicaciones, y perjudicar a los usuarios.

El DNS cifrado también puede dificultar la resolución de problemas, ya que el personal de TI que utiliza herramientas de resolución de problemas de red no tendrá acceso inmediato al contenido de las consultas o respuestas del DNS. Como es lógico, el contenido de las consultas y respuestas del DNS seguirá estando disponible para el personal de TI en los propios servidores de nombres, que habrán efectuado el descifrado necesario.

PRESTACIONES CLAVE

Respalda los mandatos de ciberseguridad
Garantiza el cumplimiento de las últimas directrices federales de ciberseguridad.

Admite el tráfico del DNS cifrado
Es compatible con DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT) para ofrecer comunicaciones del DNS seguras y autenticadas.

Protección avanzada contra amenazas
Define y mantiene bloques de direcciones y ámbitos de enrutamiento para NIOS e inquilinos en la nube.

Registro de consultas de alta velocidad
Captura y registra el tráfico del DNS en tiempo real sin sacrificar significativamente el rendimiento.

Escalable y fiable
Garantiza una gestión eficiente de grandes volúmenes de tráfico del DNS y DHCP con una escalabilidad y fiabilidad excepcionales.

Para superar estos retos y garantizar la ciberresiliencia, las agencias deben limitar la coexistencia de múltiples servicios críticos en un solo sistema. Dado el aumento de los requisitos computacionales, esta separación de funciones proporcionará la mayor resiliencia posible. La infraestructura que aloja el servicio del DNS debe estar dedicada a esa tarea y reforzada para este fin, a fin de reducir la superficie de ataque y garantizar que el servicio del DNS disponga de los recursos del sistema adecuados. La infraestructura debe incluir suficiente capacidad para elementos del servicio del DNS, como son el registro, el soporte de protocolos del DNS cifrados y el DNS protector, cuando sea aplicable. Puede ser más fácil lograrlo con servicios del DNS diseñados específicamente, ya sea como servicio o mediante dispositivos virtuales o físicos.

ADVANCED DNS PROTECTION DE INFOBLOX

Como líder en soluciones del DNS seguras, Infoblox se encuentra en una posición única para ayudar a las agencias federales a cumplir estos nuevos requisitos. Advanced DNS Protection (ADP) de Infoblox es un complemento de suscripción de software adecuado para diversos dispositivos de hardware y software de Infoblox Trinzic. Es compatible con protocolos del DNS cifrados, como DNS sobre HTTPS (DoH) y DNS sobre TLS (DoT), lo que lo convierte en adecuado tanto para entornos in situ como en la nube. Además, ADP es una solución de seguridad integral diseñada para proteger la infraestructura del DNS frente a una amplia gama de amenazas, incluidos los ataques DDoS, el malware y la exfiltración de datos. Permite a las agencias salvaguardar la integridad del DNS y prevenir los ataques DDoS tanto externos como internos contra el DNS en entornos in situ, privados y de nube pública.

Soporte de tráfico del DNS cifrado

- DNS sobre HTTPS (DoH): ADP es compatible con DoH, que ejecuta el tráfico del DNS sobre HTTPS, aprovechando la amplia adopción y la seguridad de HTTPS para proteger las consultas y respuestas del DNS.
- DNS sobre TLS (DoT): ADP también es compatible con DoT, que utiliza la seguridad de la capa de transporte (TLS) para cifrar el tráfico del DNS. Este protocolo garantiza que las comunicaciones con el DNS sean seguras y estén autenticadas.

Protección contra amenazas avanzadas

ADP proporciona inteligencia avanzada sobre amenazas, mitigación automatizada de amenazas y visibilidad en tiempo real del tráfico del DNS, lo que garantiza la integridad y la disponibilidad de los servicios del DNS.

- Supervisa, detecta y detiene continuamente todo tipo de ataques al DNS, incluidos volumétricos y no volumétricos, como los exploits y el secuestro del DNS, al tiempo que responde a las consultas legítimas.
- Mantiene la integridad del DNS, que puede verse comprometida por los ataques de secuestro del DNS.
- ADP de Infoblox utiliza la tecnología Threat Adapt™ para actualizar automáticamente la protección contra amenazas emergentes, utilizando análisis e investigación independientes, al tiempo que se adapta a los cambios en la configuración del DNS.

Registro de consultas y respuestas de alta velocidad

ADP incluye registro de consultas y respuestas del DNS de alta velocidad, lo cual es esencial para capturar y analizar el tráfico del DNS en tiempo real. Está diseñado para ser rápido y ligero, por lo que proporciona un método rápido y flexible para capturar y registrar el tráfico del DNS sin sacrificar el rendimiento.

- A diferencia del registro de consultas y respuestas con uso intensivo de E/S, dnstap funciona de forma asíncrona, lo que permite un registro de consultas de alta velocidad con una pérdida mínima de rendimiento.
- Utiliza dnstap para almacenar en búfer la información directamente desde el servidor del DNS en un formato de registro estructurado binario flexible y, a continuación, transmite estos datos a un servidor receptor.
- Las agencias pueden aprovechar las herramientas de big data para analizar estos datos (e incluso combinarlos con otras fuentes) para así crear una imagen completa de los patrones de uso de la red.

Escalabilidad y fiabilidad

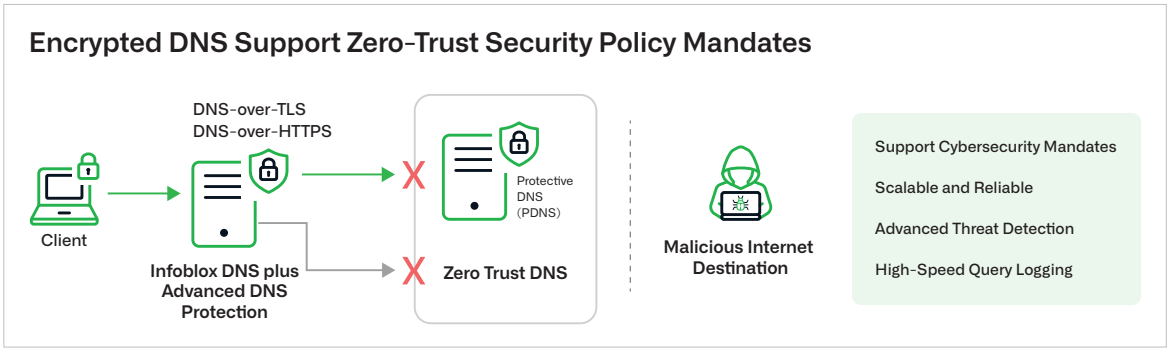
Los últimos dispositivos Trinzic de Infoblox están diseñados para ofrecer una escalabilidad y fiabilidad excepcionales, lo que los convierte en ideales para las agencias federales que cuentan con requisitos de red exigentes.

- Se han ideado para satisfacer las futuras demandas de red y aprovechan las últimas innovaciones de Infoblox en avances de red y seguridad.
- La mejora del 50 % en el rendimiento de las consultas al DNS por segundo (QPS) y las concesiones de DHCP por segundo (LPS) garantiza una gestión eficiente de grandes volúmenes de tráfico del DNS y DHCP.
- Es más fácil de implementar y gestionar en arquitecturas distribuidas, lo que garantiza la resiliencia y la escalabilidad de la red.
- Incluye funcionalidades con licencia previa para la API Cloud Platform (CP) de Infoblox, compatibilidad con zonas de políticas de respuesta del cortafuegos del DNS (DFW) y equilibrio de carga global de servidores integrado con DNS Traffic Control (DTC).

Para obtener más información sobre cómo puede Infoblox ayudar a su organización a implementar el DNS cifrado, contacte con el equipo de Infoblox en scsprogram@infobloxfederal.com o con los representantes de su cuenta directamente.

Opciones de implementación

- ADP es escalable, fácil de implementar y ayuda a las agencias a mejorar su postura de ciberseguridad, al proteger su infraestructura del DNS. Las agencias pueden implementar servidores del DNS de Infoblox con la función ADP habilitada para implementar la compatibilidad con el tráfico del DNS cifrado.
- Esta implementación puede tener lugar in situ, en la nube o en un entorno híbrido, lo que proporciona flexibilidad para atender las diferentes necesidades operativas.



LLAMADA A LA ACCIÓN

Se insta a las agencias federales a dar prioridad a la seguridad DNS mediante la adopción de Advanced DNS Protection (ADP) de Infoblox en respuesta a la reciente Orden Ejecutiva de la Casa Blanca. Esta norma exige el uso de protocolos del DNS cifrados, reconociendo el DNS como un control de seguridad de primera línea esencial. Al implementar ADP, las agencias pueden garantizar la confidencialidad e integridad de su tráfico del DNS, protegiéndose contra posibles ciberamenazas. Las soluciones completas y escalables de Infoblox son compatibles con DNS sobre HTTPS y DNS sobre TLS, lo que hace que la transición al DNS cifrado sea fluida y eficaz.

Infoblox une redes y seguridad para ofrecer un rendimiento y una protección inigualables. Con la confianza de empresas Fortune 100 e innovadores emergentes, proporcionamos visibilidad y control en tiempo real sobre quién y qué se conecta a su red, para que su organización funcione más rápido y detenga antes las amenazas.

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

+1.408.986.4000
www.infoblox.com/es

© 2025 Infoblox, Inc. Todos los derechos reservados. El logotipo de Infoblox y otras marcas que aparecen en el presente documento son propiedad de Infoblox, Inc. Todas las demás marcas son propiedad de sus respectivos titulares.

Versión: 20250203v1