ABC de la seguridad de DNS, DHCP e IPAM

Incluye técnicas de defensa efectivas que los analistas de seguridad pueden usar

ManageEngine
Log360

Índice

Capítulo 1

¿Qué es DDI?

Temas abordados:

- Sistema de nombres de dominio (DNS)
- Protocolo de configuración dinámica de host
- (DHCP) Gestión de direcciones IP (IPAM)

En 2009, Gartner utilizó por primera vez el término DDI cuando publicó el primer informe MarketScope.1 Aunque el término DDI puede parecer raro, usted podrá reconocerlo como la integración de DNS, DHCP y IPAM.

- El **sistema de nombres de dominio (DNS)** es un protocolo que resuelve nombres de sitios web a sus correspondientes direcciones IP.

- El **protocolo de configuración dinámica de host (DHCP)** es un protocolo de red en el que el servidor DHCP asigna automáticamente direcciones de protocolo de internet (IP) y otros parámetros de configuración de red a dispositivos en la red de IP.

- La **gestión de direcciones IP (IPAM)** es un sistema para gestionar espacios de direcciones IP en una red con la ayuda de DNS y DHCP.

DNS, DHCP e IPAM son componentes esenciales para el funcionamiento de la red de la empresa. Desde diagnosticar problemas de red hasta reducir inactividades, identificar violaciones de red y evitar ataques cibernéticos, la seguridad de DDI se ha vuelto un elemento vital en el manual de seguridad informática de cualquier organización.

En este Ebook, abordaremos cada uno de estos componentes en detalle.

Capítulo 2

Sistema de nombre de dominio (DNS) - El resolutor

Temas abordados:

- 2.1 ¿Qué es el DNS?
- 2.2 ¿Cómo funciona el DNS?
- 2.3 Amenazas al DNS
    - 2.3.1 Denegación del servicio distribuida (DDoS)
    - 2.3.2 Envenenamiento del caché del DNS
    - 2.3.3 Tunelización del DNS

2.1 ¿Qué es el DNS?

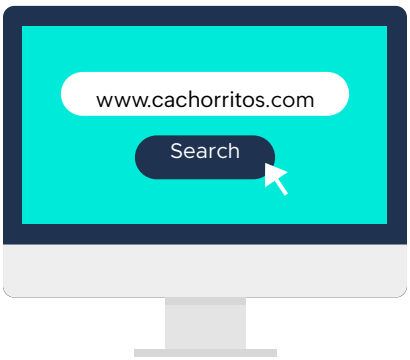
Así como los seres humanos identifican cosas, lugares y a otros seres humanos por nombre, en el reino de la red, los equipos y otros dispositivos de red se identifican entre sí mediante sus direcciones IP. No obstante, es difícil para nosotros recordar la dirección IP de cada sitio web en el que navegamos. Aquí es donde el DNS viene al rescate. Puede considerarlo como la aplicación de contactos en su smartphone que enumera los nombres de las personas con sus números de teléfono, ID de correo electrónico y otros detalles. El DNS da una lista de todos los sitios web con sus correspondientes direcciones IP. En resumen, el DNS es un traductor que convierte nombres de dominio legibles para seres humanos en direcciones IP numéricas entendibles para equipos.

2.2 ¿Cómo funciona el DNS?

Usted tiene un día no tan bueno y conoce el sitio web que lo alegrará, «www.cachorritos.com». Sigamos el rastro de cómo los videos de perritos tiernos terminan en la pantalla de su equipo o dispositivo móvil. Los siguientes son los pasos involucrados en convertir un nombre de dominio en una dirección IP:

PASO 1

Usted abre su navegador y escribe «www.cachorritos.com». Primero, su navegador y sistema operativo buscarán su caché para recuperar la dirección IP del sitio web.



Si se encuentra la dirección IP en el caché, el navegador llega directamente a «cachorritos.com» al remitirse al sitio. Se encontrará la dirección IP en el caché si ha visitado este sitio web antes, pues los detalles aún están almacenados allí. Si no se encuentra la dirección IP en el caché, se da el Paso 2

PASO 2

Se envía la consulta de «www.cachorritos.com» al servidor de resolución. El servidor de resolución verifica su memoria caché para buscar la dirección IP de la consulta recibida. Si se encuentra la dirección IP, se devuelve el valor al equipo cliente, es decir, su equipo.

Definición: El **resolutor de DNS**, también conocido como **recursor de DNS**, es un servidor responsable de hacer solicitudes adicionales para identificar la dirección IP del nombre de dominio solicitado por el cliente.

Los resolutores se ubican con los prestadores de servicios de internet (ISP) o redes institucionales.

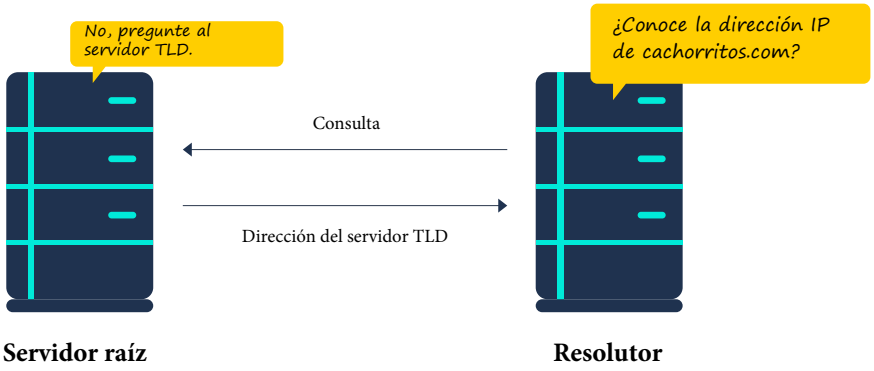
Nota:
Antes de proceder, necesita saber que la resolución de la dirección IP sucede de derecha a izquierda. La jerarquía de dominios desciende y se vuelve más específica al moverse de derecha a izquierda, es decir, la etiqueta de la izquierda es una subdivisión de la de la derecha.

Si no se encuentra la dirección IP en el caché de resolución, la consulta se redirecciona al servidor raíz.

PASO 3

El servido principal no contiene la dirección IP de «cachorritos.com», pero redirecciona el resolutor al servidor de dominio de máximo nivel, o servidor TLD, del dominio .com.

Definición: Los s**ervidores raíz** forman el nivel más alto de la jerarquía del DNS. Hay 13 servidores raíz distribuidos por el mundo que una organización sin ánimo de lucro, llamada Internet Corporation for Assigned Names and Numbers (ICANN), gestiona.

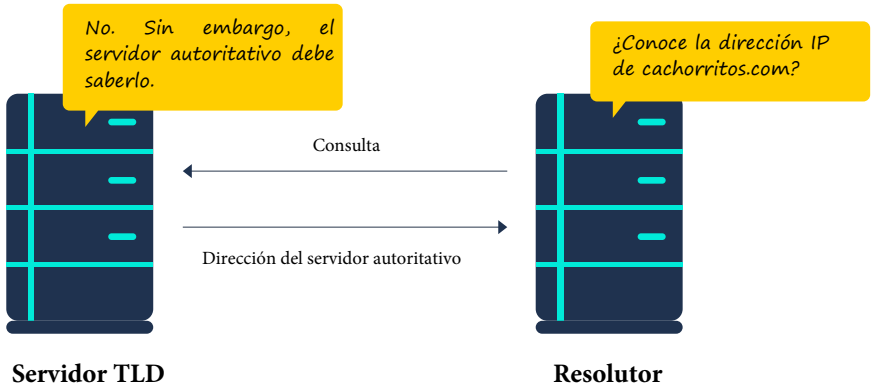


www.cachorritos.com

PASO 4

El servidor TLD contiene la información de dirección para el dominio de nivel superior «.com» del cual «cachorritos.com» es parte. El servidor TLD dirige el resolutor al servidor de nombre autoritativo del dominio de cachorritos.com, que es el destino final.

Definición: El **servidor de nombre del dominio de nivel superior (TLD)** contiene la información para dominios de nivel superior, tales como .com, .net, .gov, etc. Internet Assigned Numbers Authority (IANA), que es una subdivisión de ICANN, gestiona los servidores de nombre TLD.

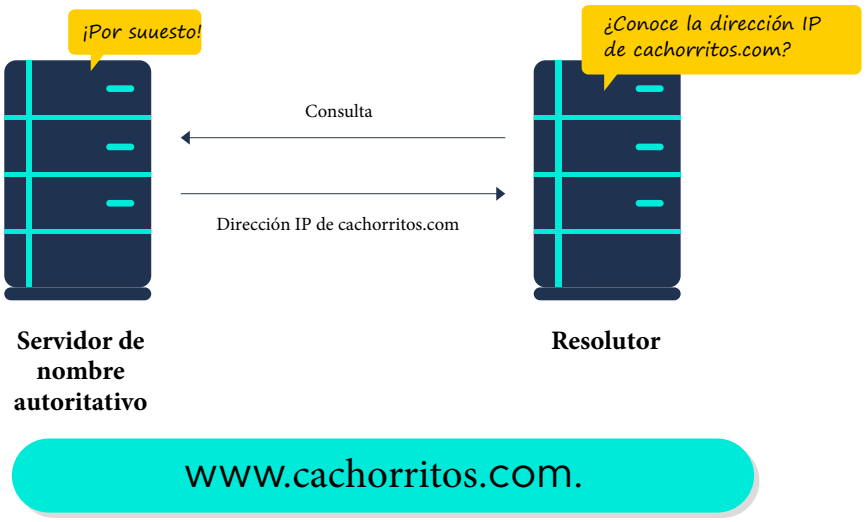


www.cachorritos.com.

PASO 5

El servidor TLD contiene la información de dirección para el dominio de nivel superior «.com» del cual «cachorritos.com» es parte. El servidor TLD dirige el resolutor al servidor de nombre autoritativo del dominio de cachorrritos.com, que es el destino final.

Definición: El **servidor de nombre del dominio de nivel superior (TLD)** contiene la información para dominios de nivel superior, tales como .com, .net, .gov, etc. Internet Assigned Numbers Authority (IANA), que es una subdivisión de ICANN, gestiona los servidores de nombre TLD.



PASO 6

El resolutor devuelve la dirección IP de «cachorritos.com» a su equipo. Utilizando esta información, su equipo ahora puede llegar a «cachorritos.com».

¡Ahora puede dedicarse a mirar videos de perritos y sentirse mejor!

2.3 Amenazas al DNS

En las secciones previas, hemos visto cómo funciona el DNS en detalle. Sin el DNS, la internet de fácil acceso, como la conocemos hoy, no existiría. El DNS es un componente crucial de cualquier red que se conecta a la internet para comunicarse con redes externas. La criticidad de las operaciones del DNS, junto con el hecho de que no se puede bloquear por completo, lo hace uno de los objetivos favoritos de los atacantes cibernéticos.

Estadística: De acuerdo con el informe Global DNS Threat de IDC, 82 por ciento de las organizaciones en el mundo han enfrentado un ataque de DNS en 2019.2

Ahora abordaremos algunos de los tipos prevalentes de ataques de DNS.

2.3.1 Denegación del servicio distribuida (DDoS)

El DDoS es un tipo de ataque cibernético en el que el atacante satura un dispositivo o una red con tráfico masivo, lo que lo hace inutilizable para los usuarios previstos. El DDoS no es una amenaza específica al DNS. No obstante, el DNS es particularmente vulnerable a los ataques de DDoS y puede formar un punto de estrangulamiento lógico en una red, ya que todos los dispositivos conectados a su red deben interactuar con él para contactar a la internet.

Ataque de amplificación del DNS

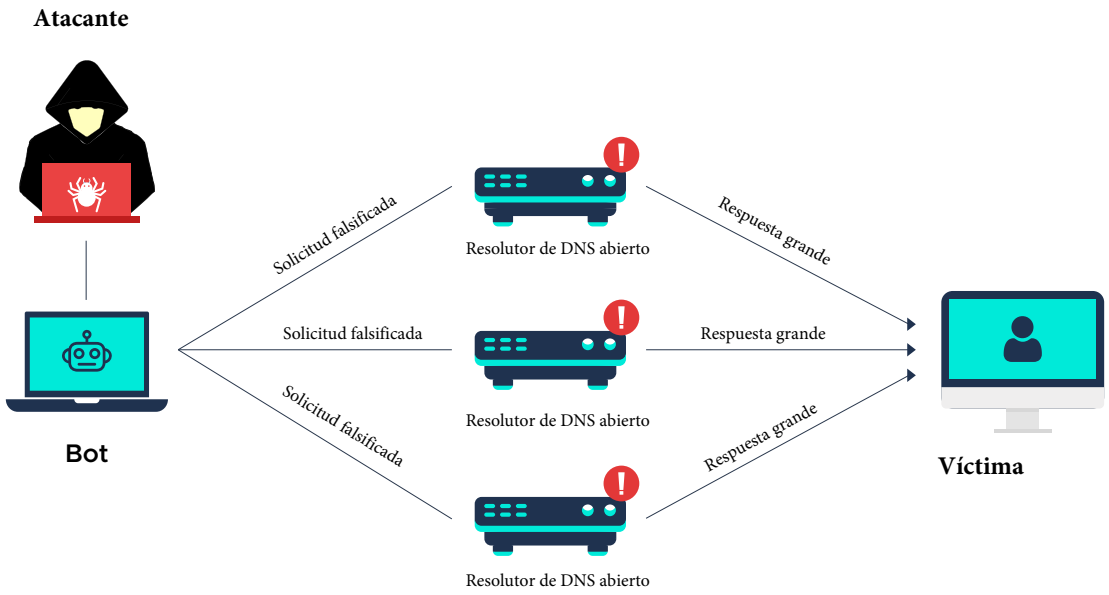
El ataque de amplificación del DNS es un tipo de ataque de DDoS que explota la forma en que el DNS funciona. Los atacantes utilizan resolutores de DNS abiertos y técnicas de suplantación de IP para saturar a sus víctimas con cargas de alto volumen. Los resolutores de DNS abiertos dan una resolución recursiva del nombre para cualquier cliente.

Así es cómo se desarrolla un ataque de amplificación del DNS:

- Los atacantes envían una solicitud de DNS con una dirección IP falsa, que apunta a la IP objetivo, a un resolutor de DNS abierto.

- Con el fin de amplificar el tamaño de la respuesta desde el resolutor, la solicitud incluye argumentos con «ANY». Mientras que una consulta no maliciosa de DNS solo solicitaría la dirección IP de un sitio web, una consulta que incluye el argumento «ANY» devuelve información sobre todo el dominio, como subdominios, alias, servidores de correo, etc., aumentando el tamaño de la carga hasta 50 veces con respecto a la respuesta original.

- Una vez el resolutor recibe la solicitud, envía la carga amplificada a la dirección IP falsificada, lo que satura la red objetivo, resultando en un ataque de denegación del servicio.



2.3.2 Envenenamiento del caché del DNS

En la Sección 2.2 «¿Cómo funciona el DNS?», vimos que el resolutor de DNS primero verifica su propio caché para encontrar la dirección IP del dominio que un cliente ha solicitado. Los atacantes pueden manipular los resolutores de DNS con información de caché falsa. El hecho de registrar información falsa en un caché de DNS se conoce como envenenamiento del caché del DNS o suplantación del DNS. Esto hace que el resolutor devuelva direcciones IP incorrectas a los clientes y, a su vez, los dirija a sitios web maliciosos.

Estos son los pasos involucrados en el envenenamiento del caché del DNS:

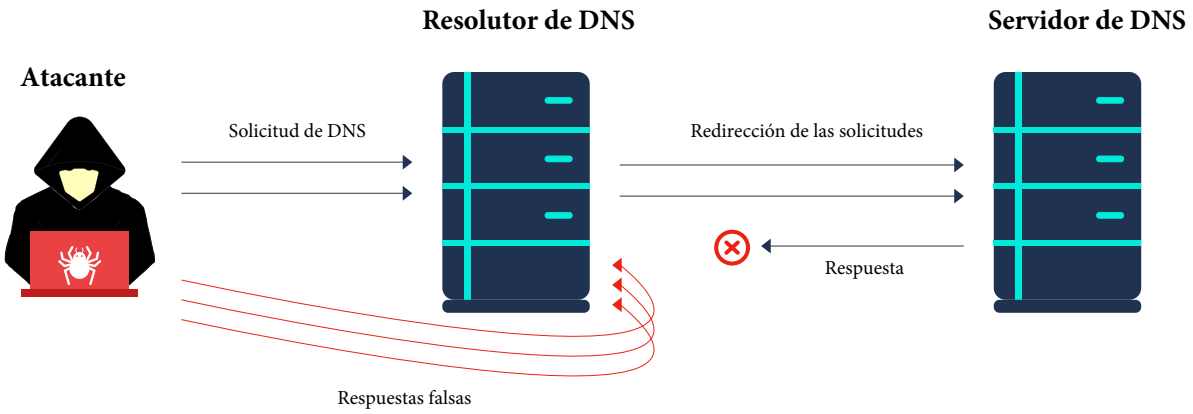
- Los atacantes envían una consulta de DNS a un resolutor de DNS, que redirige la solicitud a un servidor raíz, luego al TLD y a los servidores de nombre autoritativo.

- El atacante imita el servidor de nombre autoritativo y bombardea al resolutor con respuestas falsas que no apuntan al sitio web original. Ya que el DNS utiliza el protocolo de datagramas de usuario (UDP), no hay mecanismos para verificar la identidad del remitente. El resolutor, sin conocer la respuesta envenenada, almacena el valor en su caché.

Definición: **El protocolo de datagramas de usuario (UDP)** es un protocolo de comunicación que se utiliza en conexiones de poca tolerancia. Tiene poca latencia y permite una transferencia más rápida de datos al eliminar el proceso de establecer y verificar conexiones entre el remitente y el destinatario.

- Ahora, cuando un usuario legítimo consulta este resolutor de DNS, se devuelve del caché una respuesta falsa que dirige al usuario a un sitio web malicioso.

- Ya que el resolutor de DNS por lo general no tiene la capacidad de verificar la autenticidad de los datos en su caché, el valor envenenado permanece hasta que el tiempo de vida (TTL) expire o se elimine manualmente la entrada.



Nota:
Para que el ataque de envenenamiento del caché del DNS sea exitoso, el atacante debe conocer o adivinar varios factores:

- Las consultas del DNS que no se almacenan en el caché del resolutor, por lo que se redirigen al servidor de nombre autoritativo.
- El servidor de nombre autoritativo al que se redirige la consulta.
- El número de puerto utilizado por el resolutor de DNS y el número de ID de la solicitud, de forma que se pueda enviar la respuesta falsa al resolutor de DNS objetivo y su caché envenenado.

2.3.3 Tunelización del DNS

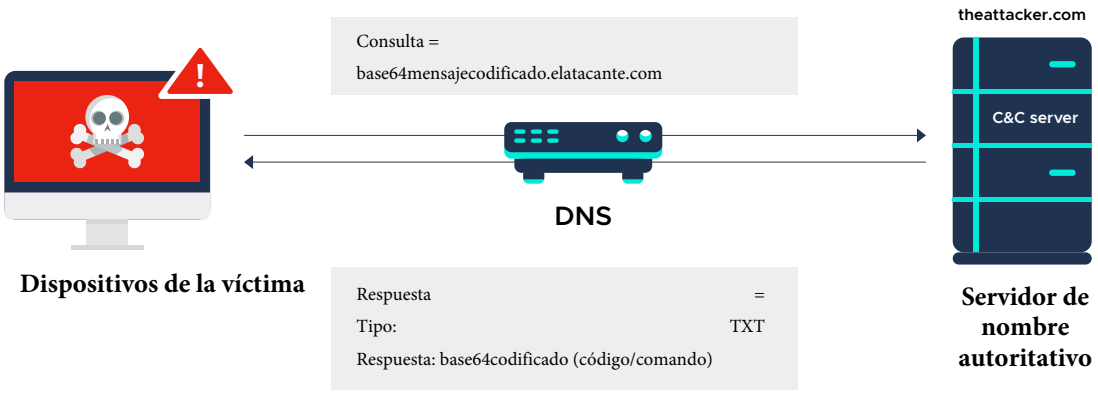
De forma similar al envenenamiento del caché del DNS, la tunelización del DNS también abusa del protocolo de DNS para realizar actividades maliciosas. La tunelización del DNS es el proceso de esconder datos en las consultas y respuestas del DNS. Los atacantes utilizan la tunelización del DNS para establecer una conexión de comando y control con un dispositivo ya comprometido en una red para ejecutar comandos o robar datos.

Los siguientes son los pasos involucrados en el ataque de tunelización del DNS:

- Los atacantes registran un dominio (por ejemplo, elatacante.com), y establecen un servidor de comando y control (C&C) que actúa como el servidor de nombre autoritativo para «elatacante.com».

- El malware en un dispositivo comprometido envía un mensaje codificado (base64mensajecodificado.elatacante.com) en forma de una consulta de DNS a «elatacante.com», que el resolutor de DNS dirige al servidor de C&C de «elatacante.com".

- El servidor de C&C regresa un registro TXT al dispositivo de la víctima. El registro TXT puede contener comandos o códigos que la carga maliciosa debe ejecutar. La tunelización del DNS establecida ayuda a intercambiar información no detectada a lo largo del perímetro.



Capítulo 3

Protocolo de configuración dinámica de host - El asignador

Temas abordados

- 3.1 ¿Qué es el DHCP?
- 3.2 ¿Cómo funciona el DHCP?
- 3.3. Amenazas al DHCP
    - 3.3.1 Inanición del DHCP
    - 3.3.2 Suplantación del DHCP

3.1 ¿Qué es el DHCP?

Sabemos que para cualquier equipo o dispositivo que se debe identificar en una red, este requiere una dirección IP. Las direcciones IP se pueden asignar a dispositivos de dos formas: estática o dinámica. En la asignación estática de direcciones IP, el usuario debe ingresar manualmente una dirección IP única y otras propiedades de red para cada dispositivo.

No obstante, esto no es práctico en redes que contienen varios dispositivos. Aquí es donde el DHCP entra en juego. El DHCP es un protocolo para la gestión de redes que asigna automáticamente direcciones IP a dispositivos de red junto con una máscara de subred, gateway predeterminado y servidor de DNS preferido.

Definición: **El servidor de DHCP** es un servidor de red que utiliza el protocolo DHCP para automatizar la asignación de direcciones IP y otros parámetros de red a clientes del DHCP.

El **cliente del DHCP** es cualquier dispositivo conectado a una red que utiliza el protocolo DHCP para obtener parámetros de red de un servidor de DHCP.

En resumen, cuando se añade un dispositivo a una red, envía una solicitud a una dirección IP. Luego, el servidor de DHCP responde con una dirección IP y una vez que el nuevo dispositivo acepta a oferta, el servidor de DHCP confirma y la asigna al dispositivo. Demos una mirada detallada al funcionamiento del DHCP.

Nota:
Se debe tener cuidado para garantizar que a cada dispositivo en una red se le asigna una dirección IP local única con el fin de evitar un conflicto de IP. Esto es similar a por qué dos casas no deben tener la misma dirección física.

Nota:
Para la asignación dinámica de direcciones IP, hay dos requisitos básicos:

- Los dispositivos en la red deben ejecutar un cliente de DHCP.
- Al menos un servidor de DHCP debe estar presente en la red. Generalmente, los routers tienen un servidor de DHCP integrado.

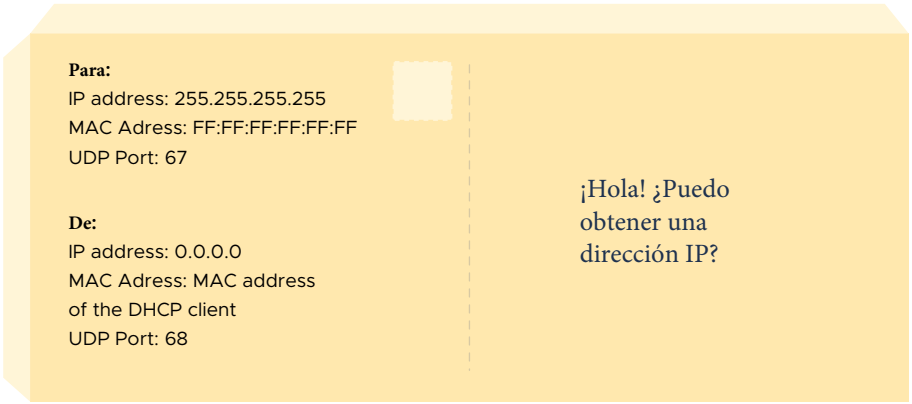
3.2 ¿Cómo funciona el DHCP?

El DHCP sigue un proceso de cuatro pasos llamado DORA por su sigla en inglés (Descubrimiento-Oferta-Solicitud-Reconocimiento).

PASO 1

Descubrimiento del DHCP

El cliente del DHCP comunica un mensaje de descubrimiento del DHCP a todos los dispositivos en la red, ya que no conoce la ubicación del servidor de DHCP.



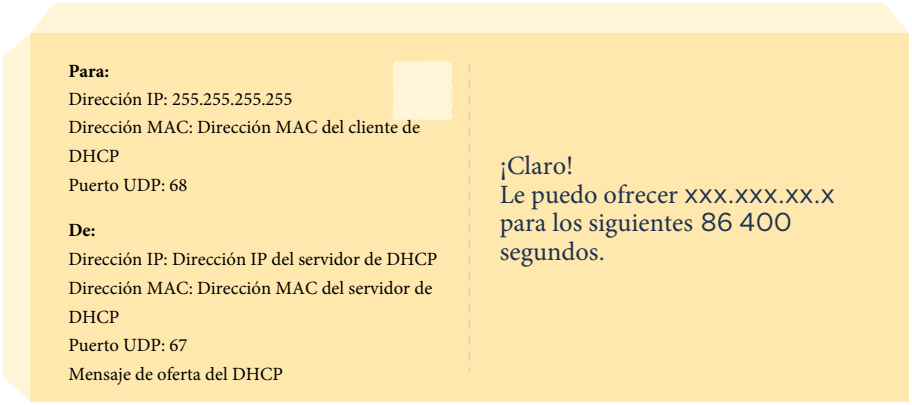
Mensaje de descubrimiento del DHCP

- La dirección IP del destinatario es 255.255.255.255 ya que es un mensaje de comunicación.
- La dirección MAC del destinatario es FF:FF:FF:FF:FF:FF ya que el servidor de DHCP es aún desconocido.
- La IP del remitente es 0.0.0.0 ya que aún no se le ha asignado una dirección IP.
- Se reserva el puerto UDP 67 a servidores de DHCP, y el puerto 68 se reserva a clientes de DHCP.

PASO 2

Oferta del DHCP

El servidor del DHCP recibe el mensaje de descubrimiento y responde con una oferta.



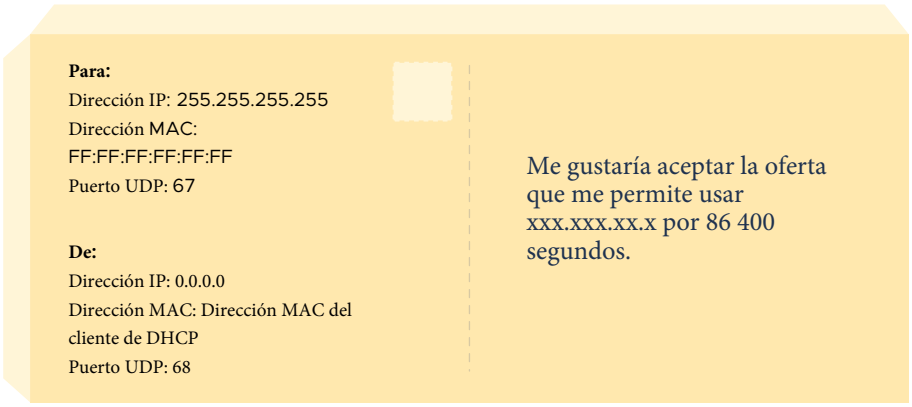
Mensaje de oferta de DHCP

- La dirección IP del destinatario es 255.255.255.255 ya que el cliente aún no tiene una dirección IP.

PASO 3

Solicitud del DHCP

Por ahora, el cliente de DHCP habría recibido ofertas de al menos un servidor de DHCP. El cliente envía un mensaje de solicitud de DHCP en el que especifica la dirección IP preferida.



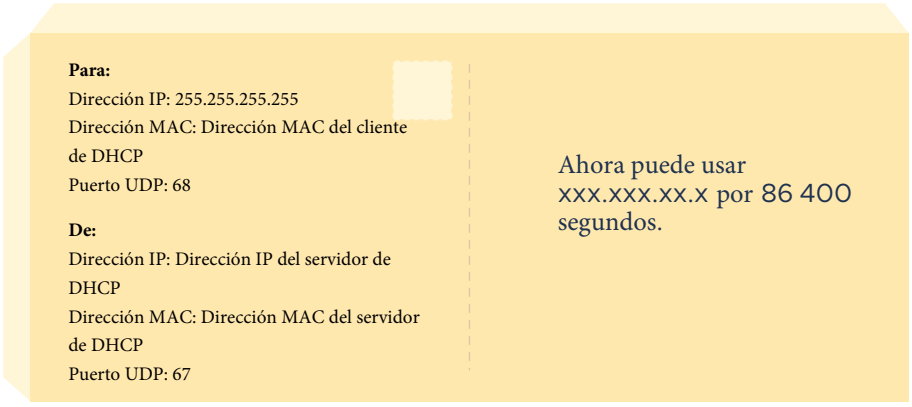
Mensaje de solicitud del DHCP

- La dirección IP del destinatario es 255.255.255.255 ya que habría recibido ofertas de más de un servidor de DHCP en la red. Se envía el mensaje para informar a otros servidores de DHCP sobre la liberación de la dirección IP ofrecida a sus pools disponibles de nuevo.

PASO 4

Reconocimiento del DHCP

Mediante el mensaje de reconocimiento del DHCP, también denominado «ACK», el servidor de DHCP confirma al cliente que puede empezar a usar la dirección IP por el periodo especificado de tiempo y que se ha reservado la dirección.



Mensaje de reconocimiento del DHCP.

Una vez que se completa este proceso de cuatro pasos, el cliente puede empezar a utilizar la nueva dirección IP.

3.3 Amenazas al DHCP

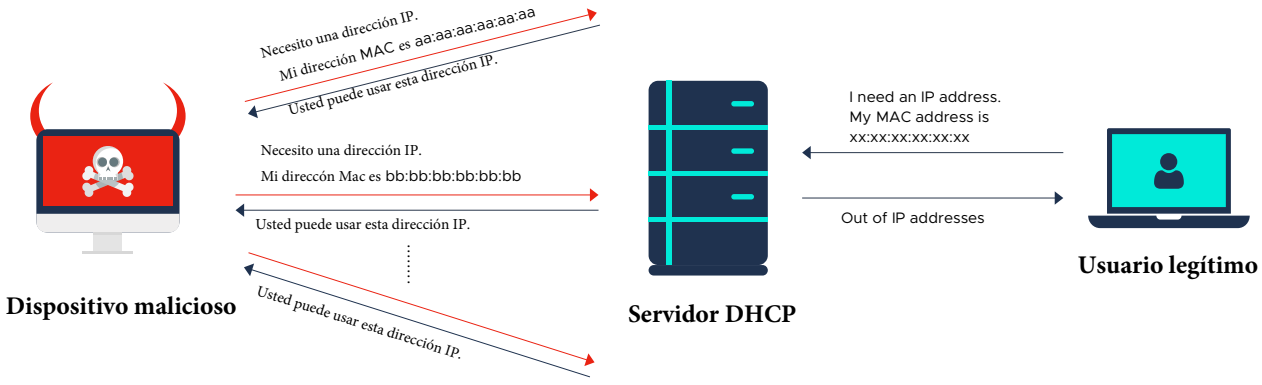
El DHCP es uno de los protocolos más utilizados para configurar hosts. A un cliente de DHCP también se le denomina un host. Similar al DNS, el DHCP también utiliza UDP como un protocolo de transporte. El hecho de que el DHCP no emplee ningún mecanismo de autenticación para verificar la integridad de los mensajes intercambiados entre clientes y servidores lo hace fácil de explotar.

3.3.1 Inanición del DHCP

Los servidores de DHCP tienen un pool de direcciones IP que prestan a hosts por un periodo especificado de tiempo. Un ataque de inanición de DHCP puede darse mediante un ataque de denegación del servicio (DoS) en el DHCP. En este ataque, el atacante inunda el servidor de DHCP con un gran número de solicitudes. Ya que el servidor no tiene mecanismos para distinguir solicitudes legítimas de maliciosas, podría distribuir direcciones IP a hosts maliciosos, agotando el pool de direcciones IP y así denegando el servicio para usuarios legítimos de la red.

He aquí los pasos involucrados en el ataque de inanición del DHCP:

- Un cliente malicioso obtiene acceso no autorizado a una red y envía varios mensajes de descubrimiento de DHCP utilizando direcciones MAC falsas.
- El servidor, a su vez, envía ofertas de DHCP, a las cuales el cliente malicioso responde con mensajes de solicitud del DHCP.
- Luego, el servidor confirma la solicitud y da reconocimiento, reservando direcciones IP para los clientes maliciosos. Las direcciones IP en el pool de direcciones en el servidor se usan rápidamente, y los clientes legítimos de la red son incapaces de acceder al servidor.



3.3.2 Suplantación del DHCP

Un ataque de suplantación del DHCP es un tipo de ataque de hombre en el medio. Este ataque generalmente sigue a un ataque de inanición. Aquí, el atacante se hace pasar por un servidor de DHCP y responde a los clientes con direcciones IP falsas y configuraciones de red erróneas, como servidor de DNS y gateway predeterminado. El atacante puede ahora manipular paquetes de datos e interceptar información de los usuarios antes de redirigirlo al gateway real o dirigir a los clientes a servidores DNS falsos y lanzar ataques de phishing.

Los siguientes son los pasos involucrados en un ataque de suplantación del DHCP:

- Un cliente envía un mensaje de descubrimiento del DHCP.
- El servidor de DCHP se queda sin direcciones IP debido al ataque de inanición de DNS y es incapaz de procesar la solicitud del cliente.
- Un dispositivo malicioso que se hace pasar por un servidor de DHCP devuelve un mensaje de oferta al cliente.
- El cliente la acepta y el servidor de DHCP falso le asigna una dirección IP y otros parámetros de configuración de la red. El cliente ahora se vuelve una víctima, ya que el servidor malicioso intercepta toda la información de la víctima, incluyendo contraseñas y otros datos sensibles.

Capítulo 4

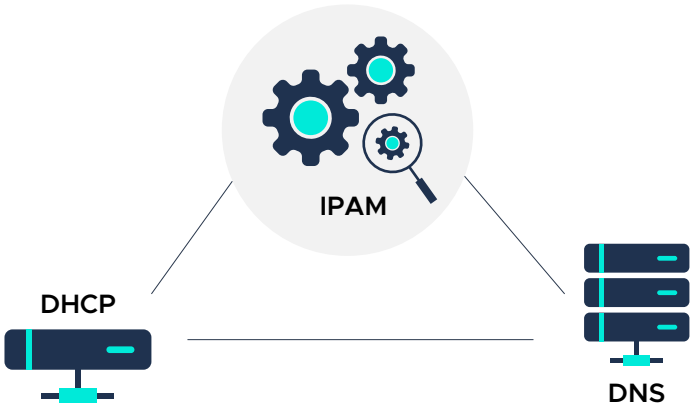
Gestión de direcciones IP (IPAM) - El administrador

Temas abordados:

- 4.1 ¿Qué IPAM?
- 4.2 ¿La IPAM es esencial?

4.1 ¿Qué es IPAM?

La gestión de direcciones IP (IPAM) es una metodología para planear, implementar, monitorear y gestionar las direcciones IP de la red. LA IPAM involucra servicios de gestión como DHCP y DNS, que están involucrados en la asignación y resolución de direcciones IP para garantizar que el inventario de direcciones IP asignables permanece actualizado y es exacto.



La IPAM puede considerarse un repositorio de toda la información relacionada con direcciones IP que pertenecen a una red, como:

- Direcciones IP disponibles para asignación.
- Estado de cada dirección IP.
- Nombre del host asociado con cada dirección IP.
- Especificaciones de hardware asociadas con cada dirección IP.
- Detalles sobre las subredes en uso.

4.2 ¿La IPAM es esencial?

Hay un mito popular que dice que, a diferencia del DNS y el DHCP, que son componentes obligatorios para cualquier dispositivo conectado a la red para la comunicación, una solución para la IPAM no es realmente indispensable; las viejas hojas de cálculo pueden hacer el trabajo.

Utilizar hojas de cálculo para la gestión de espacios de direcciones IP es solo una solución temporal y no un método eficiente. Veamos por qué.

- Explosión de dispositivos habilitados con direcciones IP - en el mundo de hoy, los panoramas de red de las organizaciones se han vuelto más complejos y dinámicos debido al aumento en el uso de dispositivos de internet de las cosas (IoT) y de políticas de traiga su propio dispositivo (BYOD). El número de dispositivos habilitados con IP conectados a una red ha aumentado muchísimo. En dicha situación, es irreal usar hojas de cálculo y documentos para controlar la información como direcciones IP, subredes, redes de área local virtuales (VLAN) y dispositivos conectados.

- Conflictos en la asignación de direcciones IP - Gestionar manualmente direcciones IP requiere que los administradores de TI actualicen la hoja de cálculo cada vez que se asigna una nueva IP, se desaprovisiona un dispositivo o se identifica un cambio en el estado de las direcciones IP. En las redes gestionadas por varios administradores de TI, se pueden generar errores de sincronización e incongruencias en los datos. Se puede asignar la misma dirección IP a distintos dispositivos, creando varios usos de la dirección. Esto hará que ningún dispositivo esté disponible.

- Interrupción de la red - Cuando las hojas de cálculo no se actualizan adecuadamente, resolver problemas se vuelve muy complicado, ya que se deben considerar diversos factores como conflictos en las direcciones IP, fallas de seguridad y disparidades de puertos. Este proceso puede ser tedioso y puede conllevar a interrupciones temporales de la red.

Estadística: De acuerdo con un estudio realizado por Ponemon Institute en 2016, el costo promedio de la inactividad de la red es de aproximadamente **$9000** por minuto.3

- **Postura de cumplimiento y seguridad** - Claramente, almacenar toda la información en una sola hoja de cálculo es tedioso, además de que los administradores de TI encuentran con frecuencia que da poca, si alguna, información procesable. Además, una hoja de cálculo no ayuda a defenderse ante fallas de seguridad. En su lugar es vulnerable a manipulaciones y sabotaje. Además, ciertas regulaciones de cumplimiento obligan a tener logs e informes detallados sobre la asignación detallada de IP; se hace tedioso procesar esto manualmente.

Formular e implementar una estrategia adecuada de IPAM no es obligatorio, pero es esencial para mejorar la eficiencia, seguridad y visibilidad de su red.

Capítulo 5

La defensa del DDI

Temas abordados:

- 5.1 Medidas para proteger las infraestructuras del DNS, DHCP e IPAM 5.2
- 5.2. ¿Cómo puede ayudar Log360?

5.1 Medidas para proteger las infraestructuras de DNS, DHCP e IPAM

En los capítulos anteriores exploramos en detalle qué es DDI y por qué debe tenerlo en cuenta. Ahora es momento de abordar algunas de las mejores prácticas para controlar los ataques a DDI y mantener su red activa y en ejecución.

- Actualice las contraseñas de la cuenta de *DNS* periódicamente. *E*sto puede evitar que usuarios no autorizados accedan a las cuentas con contraseñas maliciosas o antiguas que aún retengan.

- *P*ermita la autenticación multi factor para todas las cuentas de registro y cuentas de hosts de *DNS*.
- *G*arantice que se modifican la contraseña y nombre de usuario de los dispositivos de red, como routers, con respecto a los ajustes de fábrica.

- *N*o se deben compartir contraseñas con otros, no se deben almacenar o transmitir como texto plano o reutilizarse en los servicios.

- *L*a aleatorización es la clave para evitar el envenenamiento del caché. *U*tilice un puerto fuente, una *ID* de consulta aleatorios y letras en mayúscula o minúscula en los nombres de los dominios.

- *G*arantice que los registros de zona del *DNS* tienen firma de la extensión de seguridad del sistema de nombres de dominio (*DNSSEC*) y que sus resolutores de *DNS* realizan la validación de *DNSSEC*.

- *A*juste los servidores de *DNS* para ejecutar solo servicios que se requieran. *E*jecute el servidor resolutor y el de nombre autoritativo en servidores separados para limitar el tamaño del vector de ataque.

- *I*mplemente *DHCP* snooping para evitar un ataque de denegación del servicio en el *DHCP* y ataques de suplantación. *DHCP* snooping es una función de seguridad de nivel *2* que permite que los switches descarten el tráfico de *DHCP* no autorizado.

- *P*ermita el registro de datos cuando sea posible, de forma que se pueda auditar cualquier actividad.
- *A*udite regularmente los logs recopilados para identificar signos de ataques y tome medidas correctivas.
- *E*mplee análisis y detección de amenazas de comportamiento en tiempo real para ayudar a evitar ataques en su inicio antes de que se haga mucho daño

*S*i leer esta lista no exhaustiva de mejores prácticas de *DDI* lo deja agotado, ¡no se preocupe!
*L*ea sobre cómo *M*anage*E*ngine *Log360* puede hacer la mayoría del trabajo pesado por usted.

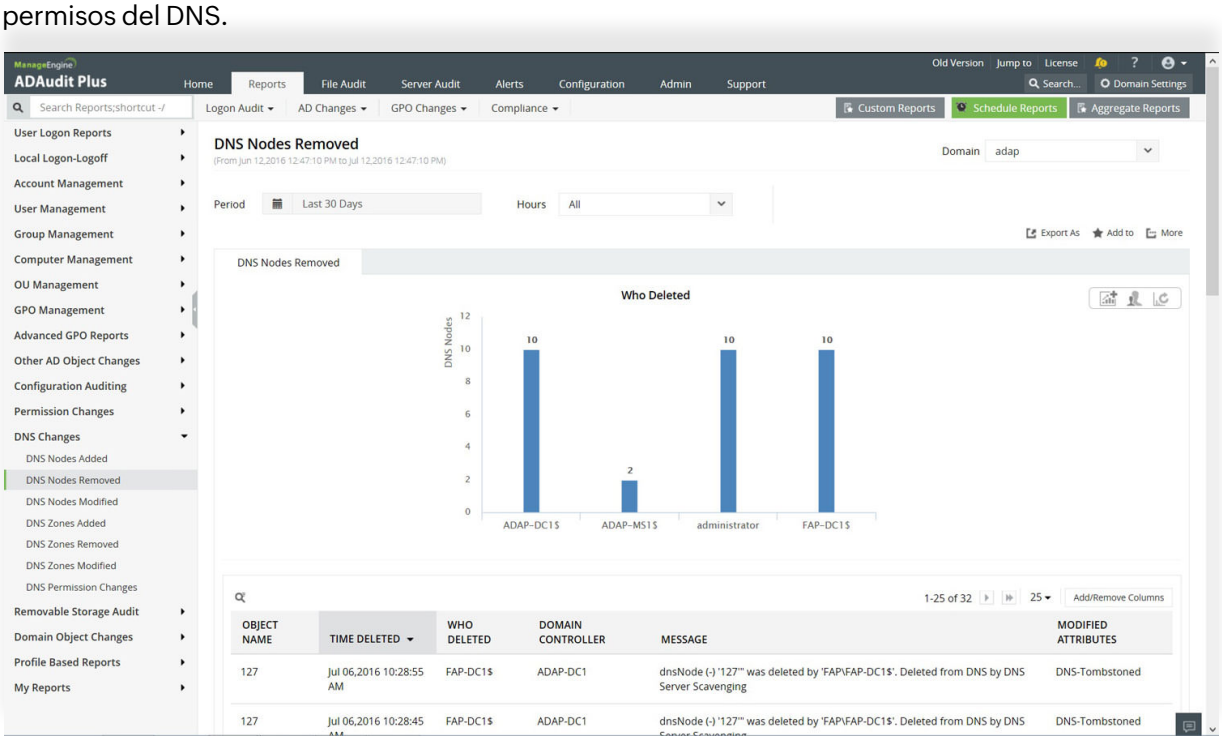
5.2 ¿Cómo puede ayudar Log360?

Log360 es una solución integral para la gestión de eventos e información de seguridad (SIEM) que le ayuda a combatir amenazas y ataques de seguridad, incluyendo los descritos en este e-book. Con su análisis detallado de logs, funciones de auditorías de Active Directory, análisis de comportamiento dirigido por machine learning, correlación en tiempo real, análisis forense y gestión de incidentes, Log360 puede ayudarle a detectar ataques en tiempo real y a bloquear y contener ataques cibernéticos.

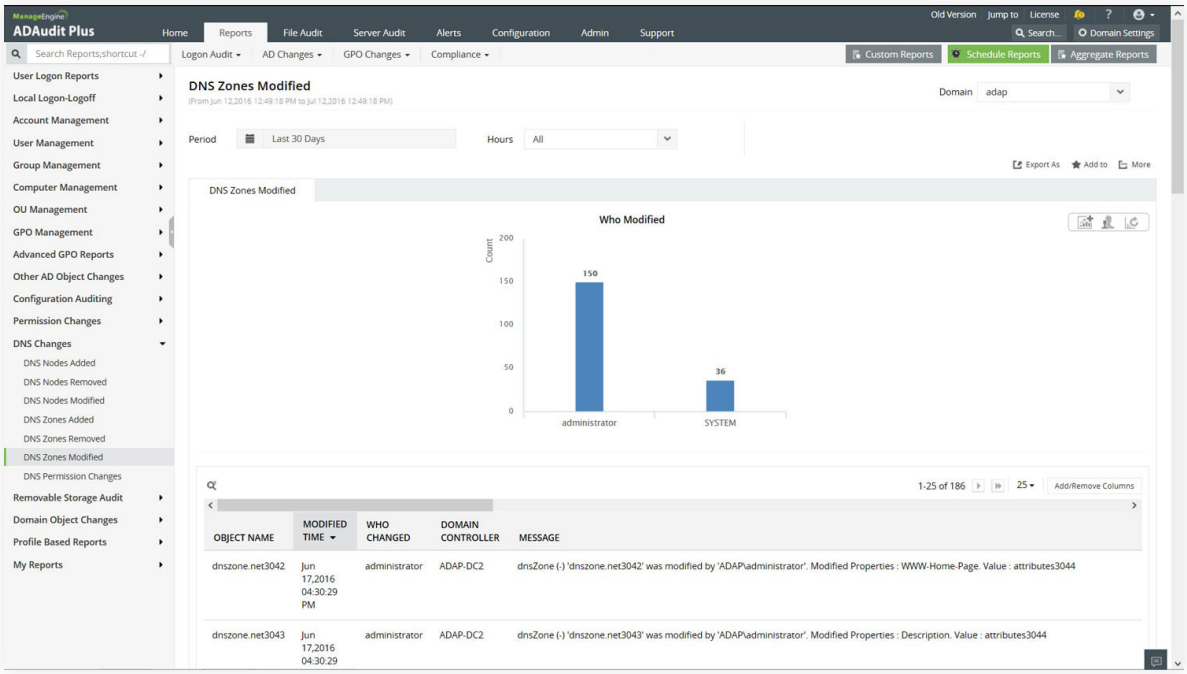
Demos un vistazo a algunas de las funciones de Log360 que pueden ayudarle a identificar y frustrar los ataques de DDI.

Auditoría de DNS

Log360 permite la auditoría en tiempo real de DNS y da una vista clara sobre los cambios realizados en el DNS. También genera informes de seguridad detallados sobre los nodos y zonas de DNS que se han modificado o eliminado, y las zonas añadidas junto con cambios cruciales en permisos del DNS.



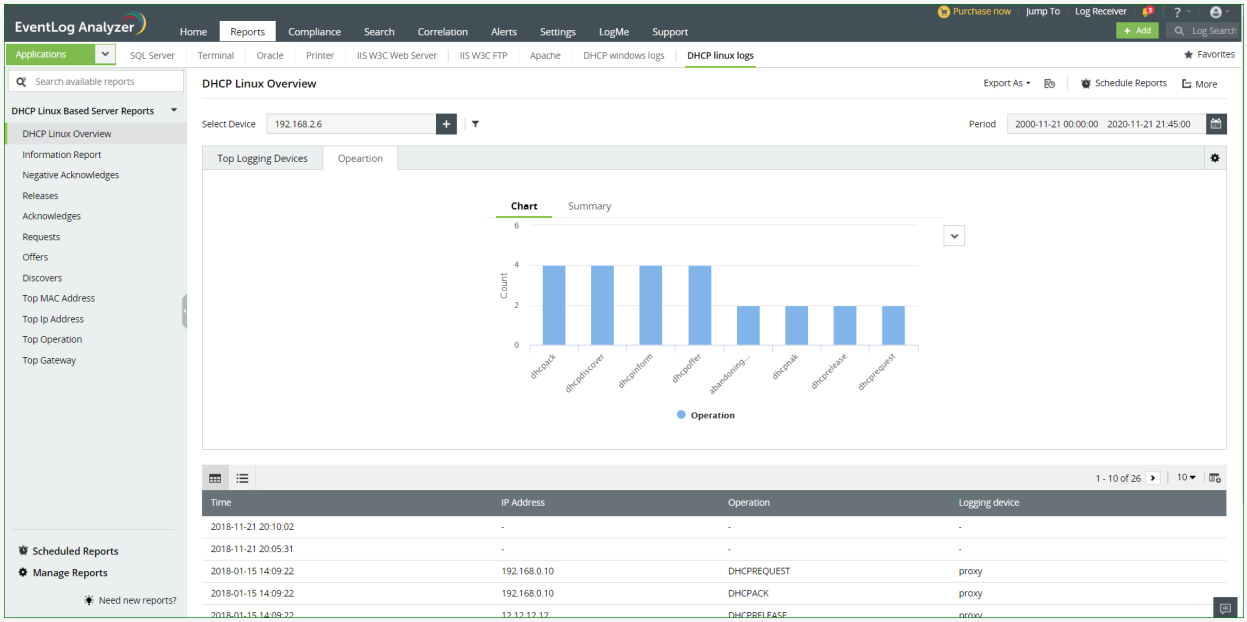
Informe de Log360 que indica la eliminación de nodos de DNS.



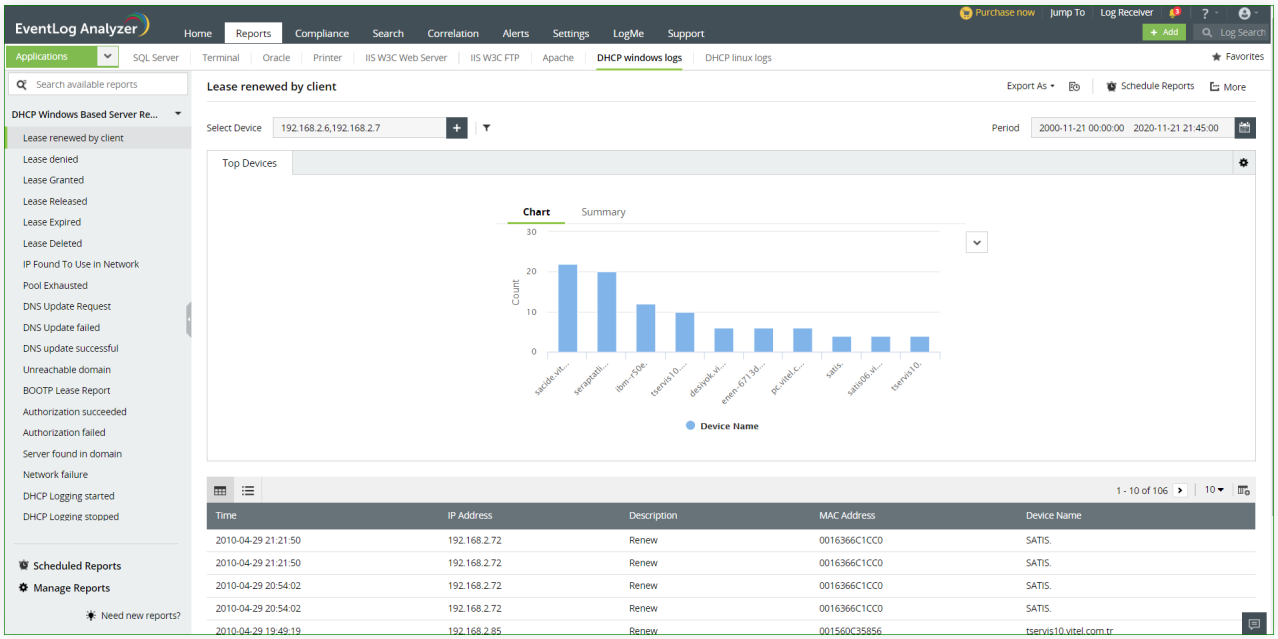
Informe de Log360 que indica las modificaciones de la zona de DNS junto con información sobre quién hizo el cambio y cuándo.

Auditoría de DHCP

Al analizar los logs del servidor de DHCP, Log360 es capaz de dar información sobre solicitudes para direcciones IP y los correspondientes reconocimientos, otorgamientos correctos y fallidos, y agotamientos del pool de direcciones IP en el servidor de DHCP.



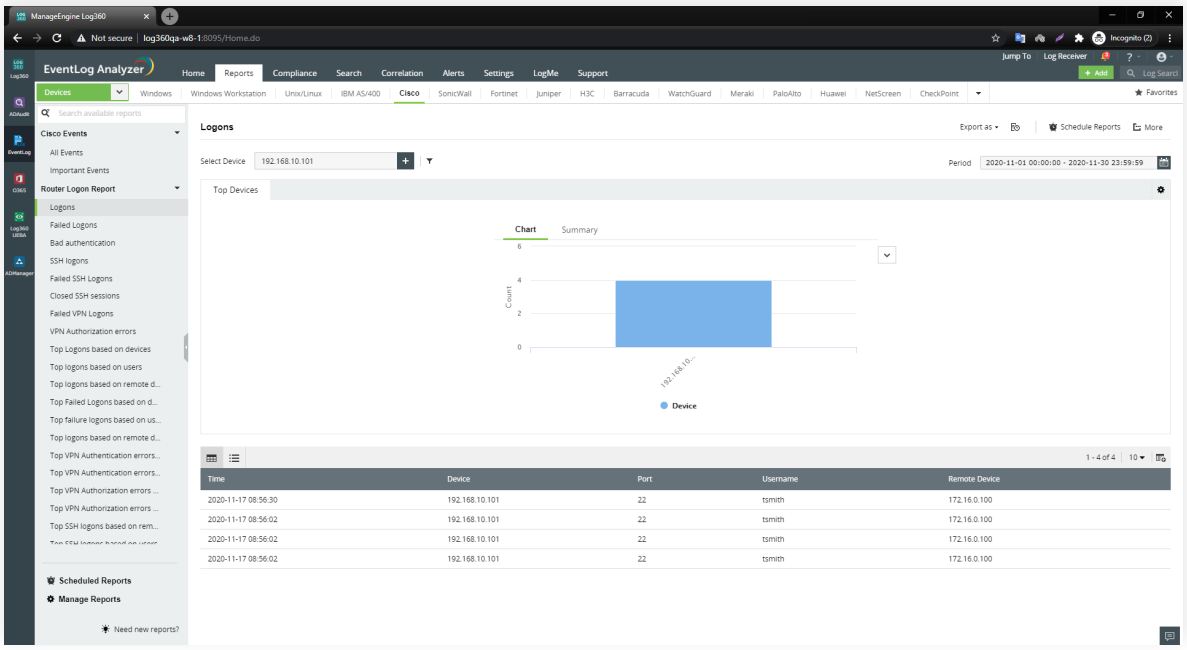
Informe de resumen general del DHCP Linux que resume todos los eventos de logs del DHCP.



Informe que enumera todos los arrendamientos de dirección IP renovados por los clientes.

Auditoría de routers

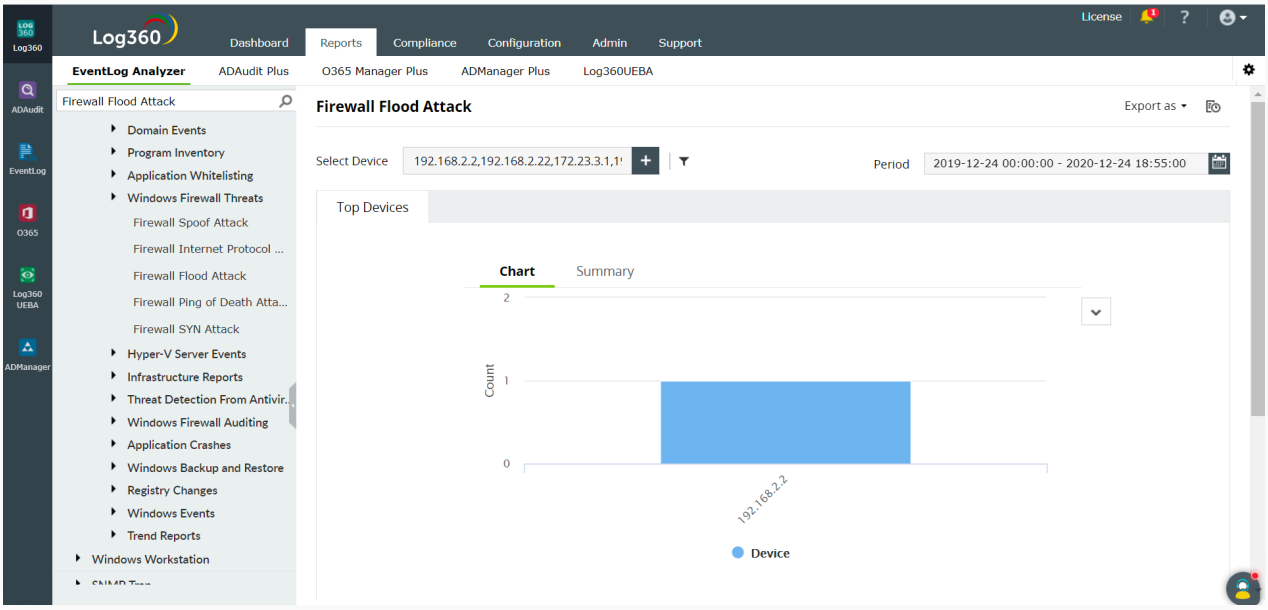
*C*on las cantidades masivas de tráfico que pasan a través de los routers regularmente, monitorear la actividad de los routers puede ser desafiante. *P*ero auditar routers y otros dispositivos de red es muy fácil con *Log360*. *A*naliza su red y descubre routers y otros dispositivos de syslog que pueden añadirse para el monitoreo. *C*on las alertas en tiempo real de *Log360* usted puede detectar actividades sospechosas instantáneamente, y los informes de logs de routers predefinidos le dan información sobre la actividad de la red.

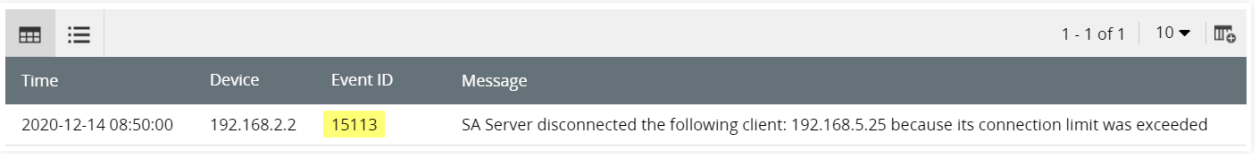


Informe que detalla los inicios de sesión en el router.

Monitoreo de firewall

*L*os firewalls actúan como un regulador de su tráfico de red, garantizando que solo partes de confianza accedan a los recursos y protegiendo sus hosts de ataques de red. *C*ontrolar los cambios hechos en las reglas de firewall, configuraciones y ajustes puede ayudarlo a garantizar que se configura adecuadamente para combatir ataques de inundación, de *SYN*, de suplantación, de medio-análisis y de ping de la muerte.

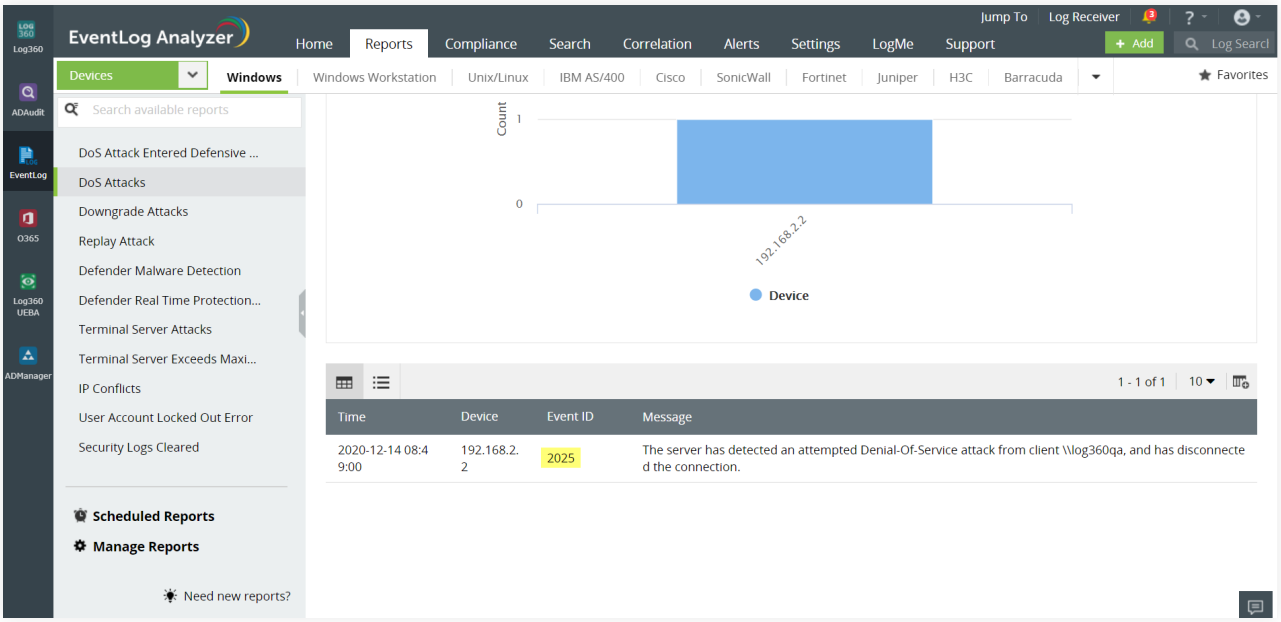




Informe que indica un ataque de inundación en un firewall.

Detectar ataques de DoS

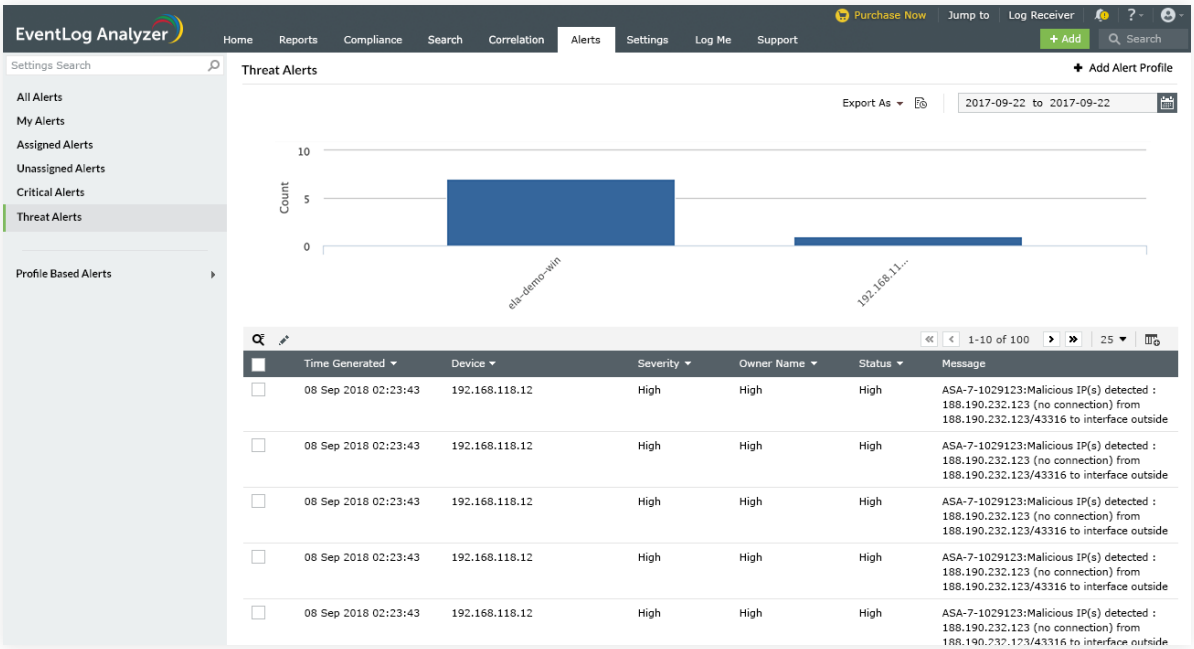
Log360 audita los datos de log de sus dispositivos de seguridad de la red, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). La solución detecta instantáneamente los ataques de DoS y lo alerta en tiempo real. Log360 también le ayuda a supervisar la actividad del servidor web cuando una IP específica sigue enviando solicitudes repetidas de conexión, un indicio de un ataque de DoS.



Log360 detecting a DoS attempt and preventing the onset of an attack.

Análisis avanzado de amenazas

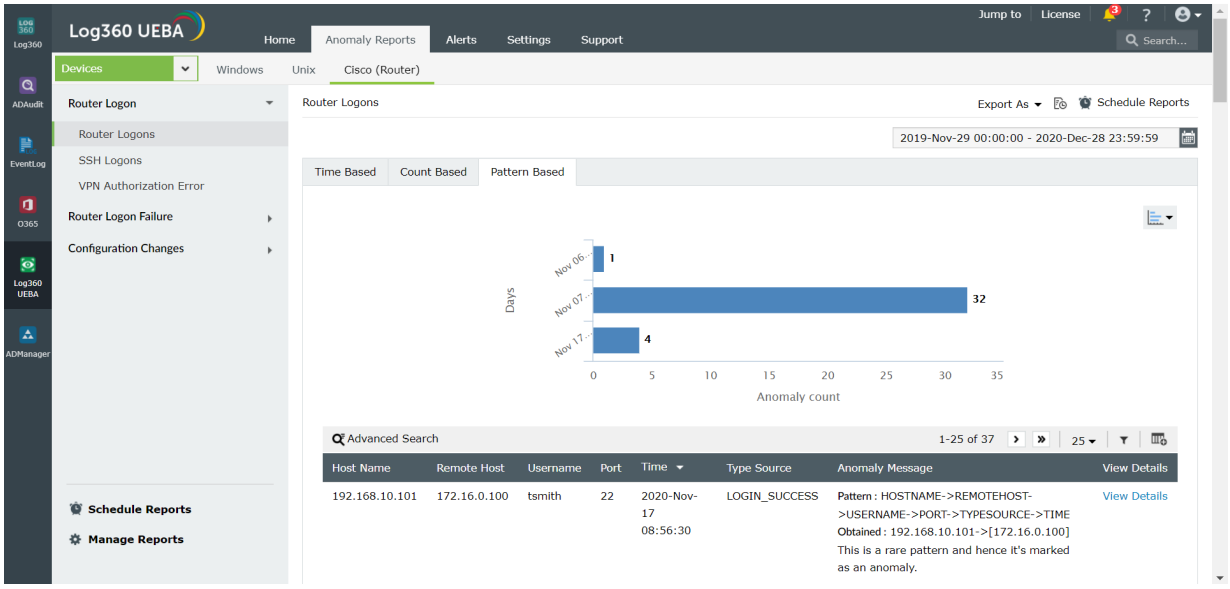
El módulo de inteligencia de amenazas de Log360 ayuda a detectar cualquier comunicación con varias fuentes maliciosas externas conocidas y tiene integrada la base de datos Global Threat Intelligence Database que aloja más de 600 millones de direcciones IP maliciosas. Esta base de datos se actualiza dinámicamente de manera regular, y Log360 correlaciona instantáneamente estos datos con los detalles de tráfico entrante y saliente para detectar tráfico malicioso en su red en tiempo real. La solución también es compatible con fuentes contra amenazas en formatos STIX, TAXII y OTX. Log360 puede equiparse fácilmente con el add-on de análisis de amenazas avanzadas, que da información más detallada sobre actores hostiles, como geolocalización del actor atacante, categoría de la amenaza, puntuación de reputación de la fuente maliciosa y más.



Log360 muestra el tráfico de direcciones IP maliciosas.

Análisis del comportamiento de los usuarios y entidades (UEBA)

Log360 utiliza machine learning para identificar los patrones de comportamiento de los usuarios y entidades en una red, lo que le permite crear un comportamiento de referencia. Luego, se compara toda actividad realizada por los usuarios y entidades con respecto a la referencia para detectar anomalías que podrían indicar un posible problema.



Informe que muestra inicios de sesión sospechosos en el router

Además de los numerosos informes arriba mencionados, Log360 ofrece más de 400 informes out-of-the-box que pueden ayudarle a supervisar las actividades de los usuarios y entidades a lo largo de su organización y realizar análisis forenses en un instante cuando surge la necesidad. Desde ayudar a cumplir las regulaciones estrictas de las normas de cumplimiento, como HIPAA, GDPR, etc., a permitirle crear alertas personalizadas basadas en sus necesidades, Log360 es una solución integral.

References

1 *R*ick *R*umbarger. "*N*etwork complexity: *T*hree trends that are contributing to a 'perfect storm' ". https://www.circleid.com/posts/*20100923*_network_complexity_three_trends_contributing_to_a_perfect_storm/

2 *V*irendra *S*oni. "*A*verage cost per *DNS* attack is now whopping $*1.07* million: *R*eport". https://www.dailyhostnews.com/average-cost-per-dns-attack-is-*1-07*-million

3 *P*onemon *I*nstitute *LLC*. "*C*ost of *D*ata *C*entre *O*utages". http://files.server-rack-online.com/*2016-C*ost-of-*D*ata-*C*enter-*O*utages.pdf