CONTRA LA ATACO DDOS EN NTP

Para quién es este documento:

• Ingenieros de redes y sistemas, administradores de redes y sistemas;

• Directores/gestores de infraestructura TI.

Introducción Muchas empresas no consideran el servicio de tiempo de red como un componente clave de sus infraestructuras críticas. En la práctica, a menudo se pasa por alto completamente. Como resultado, el arquitecto de red o ingeniero generalmente opta por una alternativa simple: utiliza un servidor o conmutador de red como fuente de reloj de red y sincroniza estas fuentes con servidores de tiempo en Internet utilizando el protocolo de tiempo de red NTP/PTP. Estos protocolos permiten que las computadoras y dispositivos sincronicen sus relojes del sistema con una fuente de tiempo de referencia. NTP es esencial para varias aplicaciones y servicios que dependen de un tiempo sincronizado, como seguridad de red, autenticación y registro de datos.

¿Es realmente "NTP a través de Internet" un método seguro para resolver las necesidades de sincronización de tiempo de red? NTP a través de Internet: ¿qué tan seguro es? NTP, uno de los protocolos de tiempo más antiguos utilizados en Internet, es el estándar para sincronizar relojes entre computadoras en una red de paquetes. Según informes sobre el estado global de la seguridad de Internet (hasta 2023), el protocolo NTP es el segundo protocolo más común afectado por ataques DDoS. Solo en un año, el número de ataques DDoS contra el protocolo aumentó en un 16%.

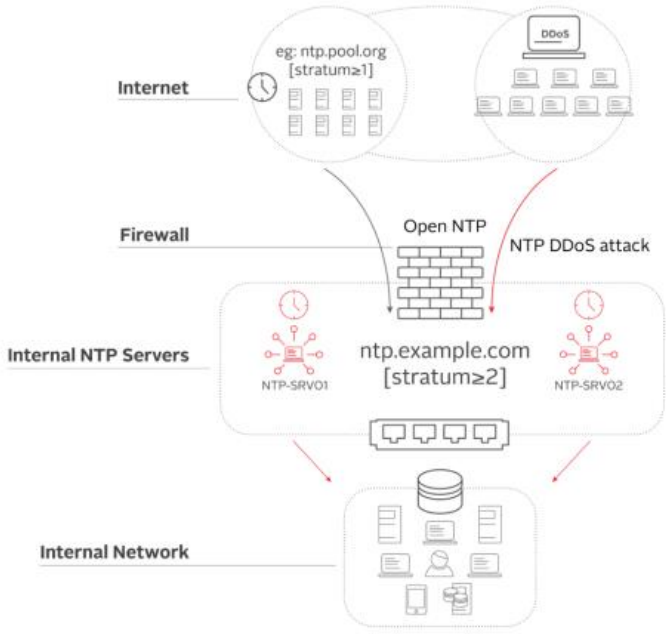

Figura 1: Sincronización corporativa típica utilizando NTP a través de Internet.

En la Figura 1 se muestra cómo funciona una configuración típica de NTP a través de Internet en una infraestructura. Consiste en un grupo público de servidores NTP (nivel NTP 1) que se usa como referencia por los servidores internos de tiempo para obtener el tiempo. Este

enfoque requiere una conexión entre Internet y los servidores internos de tiempo a través de un firewall, lo que abre acceso a la red y crea una vulnerabilidad que los hackers pueden usar para penetrar en todo su sistema. En las redes que usan este método, la infraestructura de sincronización puede no solo volverse vulnerable a ciberataques, sino que también la calidad del tiempo estará en riesgo en términos de precisión.

La mejor solución: su propio servidor NTP/PTP Stratum 1 Si utiliza Internet como fuente de tiempo de red, lamentablemente, confiar en que su firewall - incluso un firewall de nueva generación con funciones IDS (sistema de detección de intrusiones) o IPS (sistema de prevención de intrusiones) - lo protegerá de ataques DDoS, no es suficiente. ¿Cómo puede mitigar las consecuencias de los ataques DDoS al servicio de tiempo? El dicho "una cadena es tan fuerte como su eslabón más débil" no podría ser más cierto en el caso de los ataques DDoS. En las soluciones Shiwa/Qantum recomendamos a nuestros clientes una solución muy efectiva y sencilla: eliminar el eslabón más débil de la cadena. Es decir, no dependa de Internet para el tiempo operativo en su red.

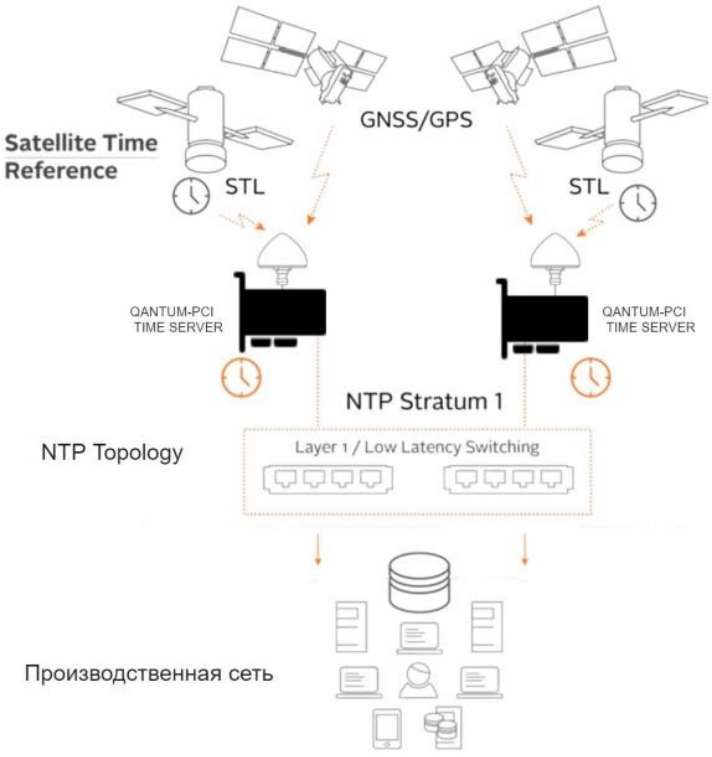

Figura 2 - Infraestructura de sincronización resistente típica para una empresa con servidores de tiempo Qantum/SHIWA

En la Figura 2 se muestra cómo una empresa puede eliminar el "eslabón más débil" creando su propia infraestructura de sincronización de red resistente y redundante dentro de la compañía, utilizando servidores de tiempo Qantum PCIe o SHIWA Time+ (para entornos seguros, con soporte para conciliación de tiempo mediante registros distribuidos (blockchain)).

Cada uno de estos servidores de tiempo recibe señales de tiempo a través del Sistema de Navegación Satelital Global (GNSS). Luego, el tiempo con precisión hasta nanosegundos se

distribuye por la red. Si se utiliza NTP/PTP como protocolo preferido, el servidor funcionará en el nivel 1 y distribuirá un tiempo seguro por el resto de su red sin necesidad de conexión a Internet.

Otros beneficios de la sincronización interna Además de reducir el riesgo de ataques DDoS, los servidores de tiempo SHIWA/Qantum ofrecen varios otros beneficios, incluyendo:

1. Alta disponibilidad – cada servidor de tiempo puede utilizar múltiples GNSS para vincularse al tiempo. En caso de que la señal GNSS no esté disponible, los servidores de tiempo contienen un generador de reserva de alta estabilidad que puede mantener un tiempo preciso durante varios días o incluso meses usando tecnología de reloj atómico.
2. Protección de la señal de radiofrecuencia – la protección contra interferencias, suplantación y protección de la señal están integradas en los servidores de tiempo. En nuestras soluciones, aplicamos protección contra interferencias en los sistemas de antenas.
3. Alta integridad, tiempo rastreable UTC - amenazas complejas pueden falsificar señales GNSS. En este caso, la tecnología SHIWA Time+ está lista para ayudar. Como señal alternativa cifrada que utiliza una potente autenticación a través de un registro distribuido, para confirmar que tiene el valor verdadero de UTC.
4. Opciones adicionales – además de la compatibilidad completa con NTP/PTP, los servidores de tiempo admiten numerosos protocolos y opciones de extensiones para distribuir el tiempo.

Conclusión En el entorno informativo moderno lleno de amenazas, es demasiado fácil bloquear o falsificar una red, causando cualquier cosa desde pequeños errores hasta un caos extremo en infraestructuras críticas. La dependencia de NTP a través de Internet conlleva riesgos inherentes que se pueden reducir fácilmente utilizando su propio servidor NTP/PTP Stratum 1, que garantizará una alta integridad del tiempo rastreable según UTC. Agregar software de protección contra interferencias y falsificación de datos proporcionará aún mayor nivel de alta disponibilidad y seguridad. La verdadera pregunta que debe hacerse es: ¿puede su empresa permitirse el riesgo de un ataque DDoS? Si la respuesta es negativa, actualizar a un servidor NTP Stratum 1 debe ser obligatorio.