NOTA DE APLICACIÓN

Soluciones WaveLogic Encryption

Protección de los datos en transmisión, en todo momento

La seguridad se ha convertido en un problema de fundamental importancia. El informe 2020 Data Threat de Thales[1] reveló que el 49 % de las compañías de los encuestados a nivel global ha sido víctima de una violación de seguridad en algún momento de su historia. Los sectores más afectados como cuidado de la salud, finanzas, gobierno y educación informan que las violaciones superaron el promedio.

Además de poner en peligro la información de los clientes, las violaciones de los datos impactan en los resultados de la organización. De acuerdo con un estudio global de Ponemon[2], se exponen aproximadamente 25 500 registros durante cada violación de datos y el costo de una sola violación llega a ser de millones, además de la pérdida incalculable de la confianza del cliente. Este estudio también reveló que el costo total promedio de una violación de datos en los Estados Unidos en 2019 fue de $8,19 millones. Nuevamente, esto varía según el sector; el costo por cada registro perdido en el sector del cuidado de la salud es casi el doble.

Pero mientras la amenaza de violaciones aumenta, el flujo de tráfico en la red está creciendo. Las demandas de ancho de banda siguen aumentando y necesitan una red que pueda escalar gradualmente para manejar mayores capacidades con menor complejidad operativa. Además, con la mayor sofisticación y frecuencia de las violaciones de datos, ninguna organización está inmune a la continua amenaza de ataques maliciosos para obtener información sensible y privada. Las redes de escala web actuales requieren mucho más que ancho de banda de alta capacidad: necesitan una estrategia de seguridad para proteger toda la información crítica, ya sea en transmisión o en almacenamiento, a medida que recorre el mundo atravesando distancias metro, regionales, largas o submarinas.

Diseñado para proteger las redes de alta capacidad actuales, WaveLogic™Encryption de Ciena ofrece de manera rentable una solución de cifrado de ultrabaja latencia, escalable e independiente de protocolos en la 6500 Packet-Optical Platform, ampliamente desplegada. La solución se extiende a la familia de dispositivos de transporte modulares, compactos y de alta capacidad, Waveserver® de Ciena, para aplicaciones de interconexión de centros de datos seguras y rentables. Este cifrado siempre activo combina facilidad de operación y administración para permitir una estrategia de protección de datos fácil de implementar que aprovecha

Beneficios

- Es una solución de cifrado con ultrabaja latencia y compatible con FIPS para comunicaciones de extremo a extremo transparentes y sumamente seguras
- Es una solución de cifrado escalable que incluye tecnología coherente WaveLogic programable para cifrado a velocidad de cable flexible de 100G a 400G
- Proporciona cifrado no dependiente de protocolos, y flexibilidad para el soporte de una variedad de servicios
- Utiliza funcionalidades de seguridad mejoradas, que incluyen dos conjuntos de claves distintos para funciones de cifrado de datos y autenticación, con un rápido intervalo de rotación de claves de cifrado de solo segundos
- Se integra perfectamente a las actuales infraestructuras de clave pública (PKI) empresariales a través de autenticación basada en certificados X.509
- Facilita la administración segura de la capacidad de cifrado como un servicio por parte del usuario final a través de una herramienta de gestión integrada
- Es una solución de cifrado ya probada en campo y ampliamente desplegada en el mundo en las redes de los sectores de finanzas, servicios públicos, cuidado de la salud y de organismos militares y gubernamentales

1 https://cpl.thalesgroup.com/sites/default/files/2020-04/2020-data-threat-report-global-edition-infographics.pdf
2 Estudio de Ponemon e IBM: Cost of a Data Breach 2020: https://www.ibm.com/security/data-breach

la tecnología coherente WaveLogic de Ciena líder del sector, para brindar flexibilidad y rendimiento inigualables y la primera solución de cifrado a velocidad de cable de 100G a 400G coherente del sector.

Tecnología de cifrado

El cifrado se define como el proceso de transformación de la información mediante un algoritmo que la convierte en información ilegible para cualquier persona, salvo aquellas que posean conocimientos especiales, lo que se denomina clave en criptografía. Básicamente, este proceso restringe el uso de la red al cifrar esta información, haciéndola completamente inutilizable para un intruso que intenta obtenerla, o para cualquier persona que no posea la clave correcta para descifrar el mensaje.

Hay muchas formas de cifrar datos, definidas por varios estándares que especifican los requerimientos de cifrado de los productos y claves compatibles, y establecen un proceso de certificación para los equipos de red. Existen varios algoritmos de cifrado basados en estándares, entre ellos el Advanced Encryption Standard (AES), que posee varios tamaños de claves (56, 128, 256 bits) publicados por el Instituto Nacional de Normas y Tecnología (NIST). Estos estándares son publicados como publicaciones de los Estándares Federales de Procesamiento de la Información (FIPS). Por ejemplo, el algoritmo de cifrado AES-256 fue publicado como FIPS 197. Además de las publicaciones específicas de algoritmos como FIPS 197, el NIST también publica estándares que coordinan los requerimientos de los módulos criptográficos que incluyen componentes de hardware y software en FIPS 140-2.

Existen otros marcos similares utilizados para certificar las soluciones de cifrado. Otro estándar importante es el de Criterios Comunes (CC) para la Evaluación de la Seguridad de la Tecnología de la Información, un estándar internacional (ISO/IEC 15408) para la certificación de la seguridad informática. Los Criterios Comunes son un medio para garantizar que el proceso de especificación, implementación y evaluación de un dispositivo de red, como un elemento de red en una red óptica, se ha realizado de manera estándar y rigurosa. En Alemania, la BSI que es la Oficina Federal Alemana para la Seguridad de la Información emite certificaciones de seguridad que incluyen la certificación según los Criterios Comunes. Los certificados BSI basados en los Criterios Comunes a menudo se usan como base para la certificación local, lo que ahorra tiempo y costos en el proceso de certificación. Este conjunto de estándares y procesos de certificación brinda a los proveedores de servicios y usuarios finales la garantía de que la solución de cifrado demostró conformidad con los requerimientos definidos al haber completado exitosamente las rigurosas pruebas de laboratorio y las revisiones exigidas por los estándares.

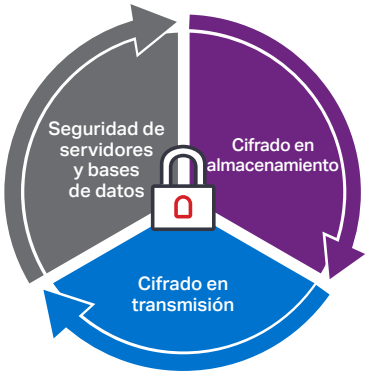

Figura 1. El cifrado de datos en transmisión es parte de una estrategia de seguridad integral

La seguridad de las redes actuales

En la actualidad el cifrado se utiliza ampliamente para proteger datos en almacenamiento y en transmisión. De acuerdo con un informe de Ponemon sobre las tendencias de cifrado, solo el 13 por ciento de quienes respondieron a nivel global no cuentan con una estrategia de cifrado.[3] Las organizaciones de cualquier tamaño en todos los sectores deben hacer todo lo posible por proteger la información almacenada en sus centros de datos contra el acceso no autorizado. El impacto y el costo de una violación de datos no pueden ser ignorados y tienen consecuencias graves para una organización, incluyendo la degradación de la reputación de una compañía, procesos judiciales, costosas multas regulatorias y alta cancelación de clientes.

Hoy en día existe una variedad de técnicas habitualmente utilizadas para proteger datos en almacenamiento para servidores, bases de datos, routers y switches a través de la administración del acceso de usuarios y comprobación de credenciales. Sin embargo, en las redes de escala web actuales, existen grandes cantidades de datos críticos en tránsito ya que las comunicaciones de elevado ancho de banda se producen más allá de las barreras del centro de datos, y atraviesan una red más grande, potencialmente global. En consecuencia, un enfoque de seguridad TI integral debe comprender una robusta solución de cifrado en transmisión como parte de su estrategia de seguridad integral, como se muestra en la Figura 1. Al cifrar los datos cuando abandonan la seguridad de la nube privada, los operadores pueden garantizar que sus datos estén protegidos contra la interceptación no autorizada a medida que atraviesan la red, cruzando distintos niveles de seguridad para llegar a su destino.

Si bien muchas organizaciones están agregando cifrado de datos en tránsito a su estrategia de seguridad, el foco tradicionalmente ha sido el cifrado de datos en transmisión en la capa 2 o superior. Aunque esto pueda llegar a ser una buena opción para algunas aplicaciones de TI de baja velocidad que no utilizan demasiados datos o que no son sensibles al tiempo, generalmente no es para

3 Informe de investigación de Ponemon y Thales e-Security: 2018 Global Encryption Trends Study; abril 2018; https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

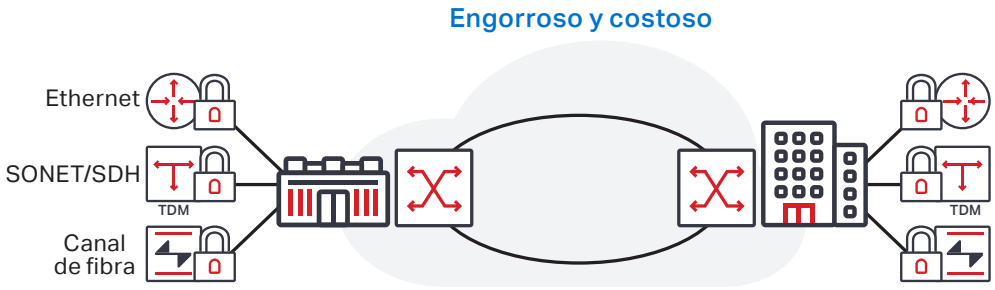

Figura 2. Encriptación tradicional y específica de protocolos implementada en una red multiservicio

toda la empresa y solo cifra datos de aplicaciones IP. Este modelo operativo para desplegar una solución de cifrado es sumamente engorroso y costoso, como lo muestra la Figura 2, ya que normalmente requiere dispositivos de cifrado independientes y específicos de un protocolo y puede generar importantes cantidades de latencia, teniendo impacto en la velocidad de tránsito de las aplicaciones y resultando en el uso ineficaz del ancho de banda. Además, la gestión de claves y autenticación de cifrado en múltiples dispositivos independientes es compleja y requiere mucha mano de obra, y la resolución de problemas de red es mucho más complicada cuando se trata de múltiples dispositivos independientes. Más aún, este enfoque deja una brecha en la estrategia de protección de los datos en tránsito de la organización. Aunque tradicionalmente, el riesgo de intrusión en cables de fibra óptica no ha sido una consideración en la estrategia de seguridad de una organización, la amenaza de infiltración en el cable óptico para acceder a la información que se transporta en el mismo es real. Los cables de fibra óptica generalmente son muy accesibles y están desprotegidos y cualquier persona con las herramientas adecuadas puede interceptar información en un cable de fibra óptica sin que se detecte, durante días, meses o incluso años. El despliegue de una solución de cifrado en la capa de transporte protege todos los datos en transmisión a cada instante, garantizando la protección de cada bit.

Data Security with Optical Encryption
Descargar la infografía ahora

WaveLogic Encryption

Como parte del enfoque de seguridad de múltiples capas de Ciena que garantiza confidencialidad, integridad y disponibilidad de los datos en la red, WaveLogic Encryption de Ciena combina tecnología de cifrado fiable, desplegada en plataformas que tienen una enorme base instalada a nivel global, con la confiabilidad demostrada de la 6500 Packet-Optical Platform líder del mercado y desplegada por más de 600 operadores en todo el mundo. Además, las capacidades de WaveLogic Encryption de Ciena se extienden a los sistemas apilables para interconexión Waveserver y Waveserver Ai de Ciena, para ofrecer hasta 1.2 Tb de capacidad de cifrado a velocidad de cable en 1RU para aplicaciones DCI rack-and-stack.

Fácil de desplegar

Con WaveLogic Encryption los operadores pueden beneficiarse con una solución que simplifica el despliegue de cifrado al integrar funcionalidad de cifrado directamente al elemento de red dentro de la red de transporte. Este enfoque reduce la complejidad de la red y elimina la necesidad de administrar distintas soluciones de cifrado para varias aplicaciones, como se muestra en la Figura 3. Esta simplificación operativa también se extiende a la gestión de la solución de cifrado, que incluye una herramienta exclusiva de administración de claves y autenticación, y fácil integración a las actuales PKI de la empresa.

Con la flexibilidad de la 6500, los clientes pueden seleccionar el tamaño de repisa óptimo que mejor se adapte a sus requerimientos de potencia, espacio y capacidad para el transporte rentable de servicios cifrados. Un beneficio clave adicional es que la solución es completamente agnóstica a protocolos, y admite una amplia variedad de clientes flexibles, entre ellos Ethernet, SONET/SDH, Canal de fibra y OTN, para el soporte de múltiples aplicaciones entre los clientes preocupados por la seguridad.

Diferenciación con cifrado 24/7

El cifrado está siempre activado en las soluciones WaveLogic Encryption de Ciena, para garantizar el más alto nivel de seguridad, ya que todo el tráfico de red está siempre cifrado. Si bien la posibilidad de encender o apagar

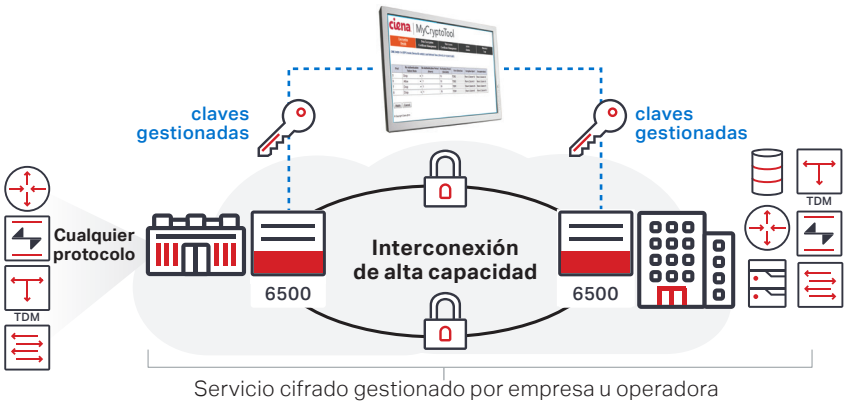

Figura 3. Solución 6500 WaveLogic Encryption de Ciena

el cifrado puede parecer una flexibilidad adicional, un simple error humano puede resultar en el envío de tráfico sensible sobre la red no cifrada. Los operadores pueden utilizar una infraestructura diferenciada que proteja todos los datos en transmisión, en todo momento, a medida que recorre el mundo a través de distancias metro, regionales, largas y submarinas. Además, los operadores pueden incrementar los ingresos y la retención de clientes mediante una oferta diferenciada de acuerdos de nivel de servicios (SLA) de alta velocidad que utilicen servicios cifrados con conectividad de ultrabaja latencia y varias opciones de protección para rutas y equipos.

Cifrado blindado

WaveLogic Encryption de Ciena es una solución validada externamente y certificada independientemente por terceros para garantizar que se implemente con algoritmos basados en estándares del sector y funcionalidades de seguridad avanzadas que incluyen Criterios Comunes y certificación FIPS. Proporciona un motor de cifrado AES-256 certificado por FIPS con mecanismos de autenticación basados en estándares (como los certificados X.509), permitiendo una perfecta integración a las PKI existentes de las empresas. Además, los componentes de hardware y software 6500 de los módulos criptográficos son compatibles con FIPS 140-2 y la certificación BSI completa bajo los Criterios Comunes para la Evaluación de Seguridad de la Tecnología de la Información, para ofrecer a los proveedores de servicios y usuarios finales la garantía de que la solución de cifrado cumple con todos los aspectos cubiertos por esta evaluación integral, incluyendo los algoritmos de cifrado, mecanismos de intercambio de claves y autenticación de usuarios.

Para mejor protección de los datos, se utilizan dos conjuntos de claves distintos e independientes para funciones de autenticación y cifrado de datos, con un rápido intervalo de rotación de claves de cifrado de segundos en lugar de minutos. Las claves de sesión de cifrado de datos AES-256 se negocian y rotan en forma autónoma cada segundo, independientemente en cada puerto de línea, sin tener impacto en el tráfico o en la velocidad de tránsito y sin la intervención del usuario. Los operadores pueden desplegar algoritmos de criptografía de claves públicas de vanguardia con soporte para Criptografía de curvas elípticas (Elliptic Curve Cryptography, ECC), que proporciona una estrategia mucho más segura que los sistemas de criptografía de claves públicas de primera generación.

Cifrado a velocidad de cable de 100G a 400G programable

Para satisfacer las necesidades de las comunicaciones de alta capacidad actuales, WaveLogic Encryption de Ciena utiliza la tecnología coherente WaveLogic líder del sector para ofrecer soluciones de cifrado de alta capacidad, flexibles y personalizables. WaveLogic 3 Extreme desarrolla las capacidades de WaveLogic 3 y brinda rendimiento extremo para todas las aplicaciones de redes coherentes a través del uso de modulaciones adicionales y una mitigación mejorada de los efectos lineales y no lineales. Esta solución de vanguardia permite modulación programable por software para ofrecer cifrado a velocidad de cable de 100G con modulación QPSK, cifrado a velocidad de cable de 150G con modulación 8QAM y cifrado a velocidad de cable de 200G con modulación 16QAM. WaveLogic Ai aprovecha el inmejorable rendimiento de WaveLogic 3 y usa un motor avanzado y optimizado para 400G que mejora considerablemente la economía del transporte: duplica la capacidad por canal, aumenta tres veces la distancia con capacidades equivalentes y cuatro veces la densidad de servicios.

En la 6500, los operadores pueden integrar un módulo de línea WaveLogic 3 Extreme con cifrado con cualquiera de las distintas interfaces clientes para desplegar con flexibilidad una solución que se adapte a sus necesidades de tráfico específicas, transporte de servicios de 10G, 40G o 100G. A medida que las demandas aumentan, con esta oferta modular de pago en función del crecimiento, puede programarse el mismo módulo de línea para transportar 200G de tráfico cifrado simplemente agregando una tarjeta cliente adicional. Además, los operadores pueden desplegar servicios cifrados de alta capacidad en toda la red utilizando la malla híbrida de paquetes y OTN de alta capacidad de la 6500, maximizando la eficiencia de los recursos de red.

En el Waveserver, los operadores aprovechan hasta 400 Gb/s de capacidad de línea de cifrado AES-256 a velocidad de cable y con certificación FIPS en solo una unidad de rack y la flexibilidad de admitir una combinación de clientes 10GE, 40GE y 100GE en el mismo dispositivo. La modulación programable permite que el Waveserver pueda optimizar su capacidad de línea de cifrado a velocidad de cable para cada aplicación o necesidad, ofreciendo dos longitudes de onda de 100 Gb/s, 150 Gb/s o 200 Gb/s. Para las aplicaciones de interconexión seguras y de ultra alta capacidad, los operadores pueden desplegar el Waveserver Ai para obtener hasta 1.2 Tb/s de capacidad cifrada en 1RU, con la posibilidad de admitir tres módulos de tráfico, cada uno de ellos capaz de ofrecer hasta 400 Gb/s de capacidad cifrada. Waveserver y Waveserver Ai proporcionan protección de datos en tránsito altamente segura y con latencia ultrabaja a través de distancias metro, regionales o de largo alcance.

Cifrado a velocidad de cable de 10G en la 6500

Los operadores pueden suministrar servicios cifrados de 10G de manera rentable utilizando el 4x10G Optical Transponder con módulo de cifrado. El módulo de una sola

High-capacity Wire-speed Encryption Modules
Descargar las especificaciones técnicas ahora

ranura proporciona 40G de capacidad de servicios cifrados a velocidad de cable a través de cuatro puertos de línea cifrados de 10G e independientes de protocolos, de manera que los clientes se benefician con diseños de redes más simples con capacidad de cifrado integrada en cualquier variante de chasis de la 6500. El módulo ofrece mayor seguridad con su diseño compatible con FIPS 140-2 de nivel 3, que brinda protección contra la manipulación física de la tarjeta mediante la puesta a cero. Esto garantiza que toda la información de seguridad crítica sea borrada cuando se detecta cualquier acceso físico no autorizado al módulo criptográfico ajustando todos los datos a cero, aun cuando la tarjeta no esté conectada a la repisa.

Administración de cifrado simplificada

Una solución de seguridad de primer nivel para la capa de transporte no sería completa sin un enfoque de administración de cifrado integrada y simplificada. La separación de la administración de cifrado de la administración de transporte permite agregar flexibilidad en una infraestructura cuyo mantenimiento está a cargo de un operador o de una empresa. En cualquier de los dos casos, es importante que el "propietario" de los datos (el usuario final) mantenga un mayor control de los parámetros de seguridad de cifrado asociados con sus datos críticos, mediante la emisión de nuevas claves o certificados requeridos por las políticas de seguridad, permaneciendo atentos a cualquier alarma y registro de seguridad de extremo a extremo.

La solución WaveLogic Encryption 6500 de Ciena incluye MyCryptoTool, una interfaz de administración de cifrado dedicada, que fue diseñada para la administración distribuida de la red que permite al usuario final o al director de seguridad administrar independientemente los parámetros

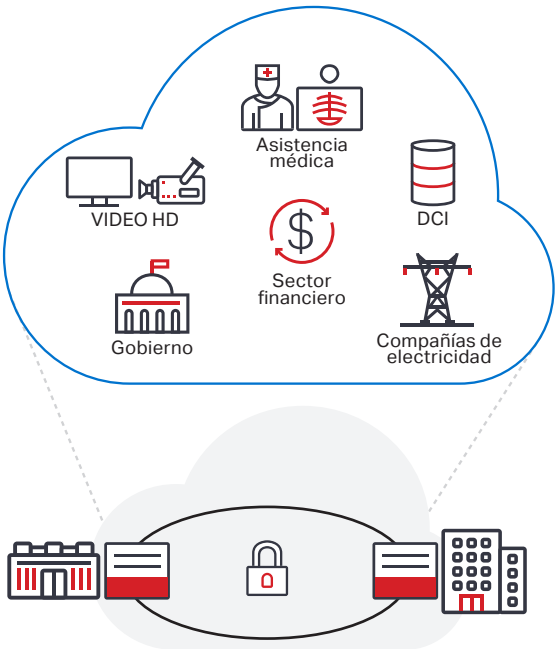

Figura 4. Ejemplos de aplicaciones clave que se benefician con WaveLogic Encryption

y alarmas de seguridad de las redes administradas por operadoras o empresas. MyCryptoTool es una interfaz fácil de usar que se conecta en forma segura con el módulo criptográfico y ofrece autenticación recíproca, limitando el acceso a personal de seguridad autorizado. Si el servicio de cifrado se adquiere a un proveedor de servicios, el proveedor gestionará los enlaces, su aprovisionamiento, administración y monitoreo de rendimiento, como con cualquier otro servicio, pero no tendrá el control o la visibilidad de los parámetros de cifrado. El mismo enfoque es válido cuando la solución de cifrado es desplegada y administrada por dos grupos diferentes dentro de la misma empresa u organismo gubernamental.

Aplicaciones principales

Las soluciones WaveLogic Encryption de Ciena están adaptadas para proteger los datos críticos en tránsito en todas las aplicaciones de alta capacidad de la actualidad. Las aplicaciones clave que se beneficiarán con estas soluciones incluyen:

- DCI empresarial para almacenamiento de alta capacidad y transporte cifrado de datos
- Gobiernos e instituciones que requieren comunicaciones certificadas, seguras y de alta velocidad entre distintas ubicaciones
- Aplicaciones para el cuidado de la salud con requisitos de baja latencia y alta calidad para una colaboración segura, eficiente y adecuada entre los participantes de la asistencia médica
- Aplicaciones de servicios gestionados
- Aplicaciones sensibles a latencia, como video de alta definición u operaciones bursátiles de alta velocidad, que requieren una solución de transporte segura y de latencia ultrabaja
- Compañías de electricidad que quieran proteger sus infraestructuras de comunicación críticas

Resumen

Como cada vez es mayor la cantidad de información confidencial que se distribuye en las redes de fibra óptica, las comunicaciones de alta capacidad de hoy deben desplegar un enfoque de seguridad de TI que comprenda no solo la seguridad de los servidores y el cifrado de datos en almacenamiento, sino también una robusta solución de cifrado en transmisión. WaveLogic Encryption de Ciena combina un alto grado de flexibilidad y seguridad con facilidad de operación y administración, para ofrecer soluciones de cifrado a velocidad de cable, escalables y rentables para proteger prácticamente todos los datos en transmisión a cada instante, ya sea que se desplacen por la calle, la ciudad o a través de fronteras o los océanos.