NOTA DE APLICACIÓN

# Protección de la infraestructura crítica

## Cifrado de red para las compañías de electricidad

La ciberseguridad plantea problemas que serán cada vez más frecuentes, complejos y desafiantes. Según Michael Mullen, expresidente del Estado Mayor Conjunto de Estados Unidos, "La amenaza cibernética es la mayor amenaza existencial" porque "una amenaza cibernética, puede atacar, no teóricamente sino de hecho, nuestra infraestructura y nuestros sistemas financieros."[1]

Las compañías de energía enfrentan mayores desafíos cibernéticos ya que se consideran infraestructura nacional crítica, que se define como "tan vital para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un efecto debilitante en la seguridad, la seguridad económica nacional o la salud pública".[2]

Para ilustrar los desafíos cibernéticos actuales que enfrentan las compañías de electricidad, una encuesta de Unisys junto con el Ponemon Institute del año 2014 mostró que casi un 70 por ciento de los proveedores de infraestructura crítica encuestados—compañías de servicios públicos responsables de la electricidad, el agua y otras funciones críticas del mundo—han reportado por lo menos una violación de seguridad que resultó en la pérdida de información confidencial o la interrupción de sus operaciones en los últimos 12 meses.[3]

La seguridad y la privacidad son esenciales para establecer y mantener la confianza pública en las redes eléctricas nacionales. El cifrado, una de las herramientas clave en el kit de herramientas de ciberseguridad, hace que la información sea ilegible para cualquier persona, excepto para aquellos que poseen la clave correcta para descifrar el mensaje.

La mayoría de las organizaciones protegen los datos estáticos, resguardando servidores, bases de datos, enrutadores y conmutadores mediante la administración del acceso y las credenciales de los usuarios. Sin embargo, en las redes de las compañías de servicios eléctricos de la actualidad, se transmiten grandes cantidades de datos críticos como comunicaciones de alto ancho de banda más allá de las paredes de la subestación o del centro de datos de la empresa de servicios eléctricos, atravesando redes regionales y nacionales. En consecuencia, un enfoque de seguridad TI integral debe comprender una robusta solución de cifrado en transmisión como parte de su estrategia de seguridad global. Al cifrar los datos cuando abandonan la seguridad de la nube privada, las compañías de servicios eléctricos pueden garantizar que sus datos estén protegidos contra la interceptación no autorizada a medida que atraviesan la red, cruzando distintos niveles de seguridad hasta llegar a su destino.

1 CNN: "Admiral Michael Mullen: Farewell and thank you" por Micah Zenko, 11 de noviembre de 2011; http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/
2 Cornell University Law School, Legal Information Institute: U.S. Code 5195c – Critical infrastructures protection; http://globalpublicsquare.blogs.cnn.com/2011/09/29/admiral-michael-mullen-farewell-and-thank-you/
3 Ponemon Institute: "Unisys Survey Reveals Nearly 70 Percent of Critical Infrastructure Providers Have Been Breached in the Past Year", 10 de julio de 2014; http://www.unisys.com/offerings/security-solutions/News%20Release/Unisys-Survey-Reveals-Critical-Infrastructure-Providers-Breached

### Beneficios

- Protege los datos activos de la empresa de energía contra la violación de datos y mantiene los sistemas críticos seguros
- Protege su valorada reputación y evita costosas multas, exposición en los medios y cancelación de clientes al cumplir con las expectativas de protección de la información
- Cumple con los requerimientos de seguridad NERC-CIP para la industria de servicios eléctricos

### Por qué los directores de Tecnología de la Información (CIO) de las compañías de servicios eléctricos no realizan el cifrado de datos activos

Muchos CIO de empresas de electricidad no son plenamente conscientes de que una vez que los datos salen de la subestación o centro de datos, están básicamente fuera de su control. Con todos los esfuerzos para restringir datos estáticos con firewalls, software antivirus y detección de intrusiones, los delincuentes cibernéticos están dirigiendo su atención a la interceptación de los datos en tránsito cuando se transmiten en la red. Las firmas de seguridad cibernética denuncian la existencia de un mayor número de incidentes informáticos focalizados en las redes internas y corporativas.

Otra razón de la falta de atención al cifrado de datos activos es que muchos CIO creen que las redes de fibra óptica son por naturaleza inmunes a las violaciones. La realidad es que un hacker de nivel intermedio que cuente con equipos y software económicos puede interceptar los datos de la compañía de electricidad durante días, meses o incluso años sin ser detectado. Cualquier persona con acceso a Internet puede comprar fácilmente en línea una herramienta de acoplamiento de fibra y, después de ver algunos videos de YouTube que lo guían a través del proceso de tapping, puede aprender rápidamente cómo robar datos confidenciales de un cable de fibra óptica. En YouTube hay una gran cantidad de videos que muestran la facilidad con la que los hackers pueden violar una red de fibra. Un solo hilo de fibra puede transportar enormes cantidades de datos y, dado que los cables de fibra óptica son sorprendentemente accesibles, se han convertido en objetivos valiosos para los atacantes.

Hacking an Optical Fiber Line in Minutes **Ver el video**

Una razón más por la que los CIO de las compañías de servicios eléctricos se han mostrado reacios a implementar el cifrado de datos activos es la preocupación por la disminución del rendimiento y el costo de la red. En un sector donde los márgenes se reducen y la latencia de red puede significar la diferencia entre contener o propagar un corte de energía, su preocupación es comprensible, aunque infundada. Estas preocupaciones pueden surgir de la experiencia con soluciones de cifrado de red de capa 2 y superior. Por ejemplo, los dispositivos de cifrado de capa 3 están diseñados para el cifrado IPSec (cifrado estándar de Internet). IPSec utiliza un proceso que "crea túneles" en el paquete IP original para cifrar una "cabecera" de IP. Sin embargo, los túneles pueden producir un aumento en la sobrecarga y la complejidad, y posteriormente, en la velocidad de rendimiento y procesamiento de la red.

### La solución ideal de cifrado de red para datos activos

El cifrado de red, ya sea como parte de una red óptica privada o suministrado como un servicio gestionado por un proveedor de servicios, debe considerar algunos puntos clave:

**Cumplimiento de normas.** Las empresas de servicios eléctricos son muy conscientes de las regulaciones que pueden aplicarse a las aplicaciones que llevan sus redes. La industria de servicios públicos estableció una serie de especificaciones de seguridad bajo las normas de North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP). Estas incluyen todo, desde la protección de activos físicos hasta la seguridad de su cadena de suministro y activos de TI. La solución elegida debe cumplir con los requerimientos de NERC-CIP para la industria de servicios públicos.

**Latencia.** Las especificaciones de latencia en el mercado de los servicios de distribución eléctrica son más estrictas que en otros mercados verticales, ya que se debe actuar sobre una subida de tensión con un retraso de menos de 10 ms para evitar propagar un corte de energía. Las soluciones de cifrado de vanguardia satisfacen los requisitos de las compañías de electricidad al ofrecer latencias basadas en hardware del orden de varios microsegundos.

**Administración.** Ya sea que la compañía de electricidad o un proveedor de servicios administre los enlaces cifrados, el "propietario" de los datos—la compañía de electricidad—debe mantener el control de las claves de cifrado, emitir nuevas claves cuando sea necesario y tener visibilidad de las alarmas e informes de seguridad asociados con sus enlaces encriptados. Esto se logra separando la administración de la red de la gestión de las claves de cifrado. Si el servicio encriptado se adquiere de un proveedor de servicios, este gestionará los enlaces y su aprovisionamiento, administración y monitoreo del rendimiento, pero no controlará la distribución ni el mantenimiento de las claves. Dependiendo de las políticas de seguridad de la empresa de electricidad, la distribución de las claves se puede realizar manual o automáticamente a través de túneles encriptados y seguros.

Un enfoque de seguridad global debe abarcar no solo los "datos estáticos", incluidos los datos almacenados en bases de datos, archivos y sistemas de almacenamiento, sino también el cifrado de "datos activos" para garantizar que los datos estén protegidos contra detecciones no autorizadas cuando atraviesan la red. Las sofisticadas técnicas actuales de encriptación de "datos activos" pueden camuflar el tráfico para que no se pueda leer ni manipular, e incluso pueden disfrazar el hecho mismo de que existe tráfico desplazándose por la red.

### Cifrado de datos activos en la capa óptica

El cifrado de datos activos en la capa óptica aborda todos estos problemas y muchos más. Si bien es cierto que tecnologías como seguridad de la capa de transporte (TLS) y capa de conexión segura (SSL) se utilizan cada vez más para proteger las conexiones a servidores, la única forma de proteger toda la información en el enlace de comunicaciones que ingresa y sale de una ubicación es cifrar todo en la capa física. Esto es particularmente cierto cuando se considera la cantidad de "metadatos" generados por varios servicios en una red que no está necesariamente encriptada, incluso

cuando se utiliza el cifrado de la capa de aplicación, como TLS / SSL. Las direcciones IP y MAC, los tipos de protocolo en uso y otra información de red se intercambian sin codificar, incluso cuando los datos de usuario reales están cifrados. Estos metadatos pueden ser utilizados por los adversarios para mapear una red y planificar ataques, incluso sin acceso a los datos cifrados de la capa de aplicación. Un enfoque de cifrado masivo de capa 1 hace que todos los datos y metadatos de la compañía de electricidad sean indescifrables para cualquier hacker que tenga acceso a la fibra.

**Aplicaciones y casos de uso de cifrado de claves para las compañías eléctricas:**

**(1) Comunicaciones en la línea eléctrica**

a. Teleprotección
b. SCADA

**(2) Interconexión de centro de datos**

a. Prevención y recuperación ante desastres
b. Consolidación y optimización del centro de datos
c. Movilidad de la carga de trabajo

**(3) Transporte de video**

a. Videovigilancia

## Solución WaveLogic Encryption de Ciena

WaveLogic Encryption brinda soluciones de cifrado óptico wire-speed, de latencia muy baja y fácil de implementar, que se integran directamente a la red de transporte. Gracias a su enfoque "configure y despreocúpese" el cifrado está siempre activo, lo cual asegura el más alto nivel de seguridad y elimina los errores humanos que pueden resultar en el envío de datos confidenciales a través de la red no encriptada. Como se ilustra en la figura 1, WaveLogic Encryption garantiza que todos los datos y metadatos críticos de la compañía de electricidad que viajan a través de la red estén siempre seguros.

La solución está validada externamente y certificada independientemente por terceros para garantizar que se implemente con algoritmos basados en estándares del sector y funcionalidades de seguridad avanzadas. Proporciona un motor de cifrado AES-256 con certificación FIPS y mecanismos de autenticación basados en estándares (como los certificados X.509), que permite una integración sin problemas a las PKI empresariales existentes, así como soporte para los últimos algoritmos de criptografía de clave pública, incluyendo criptografía de curvas elípticas (ECC). Además, los componentes de hardware y software de los módulos criptográficos son compatibles con FIPS 140-2, ofreciendo 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.

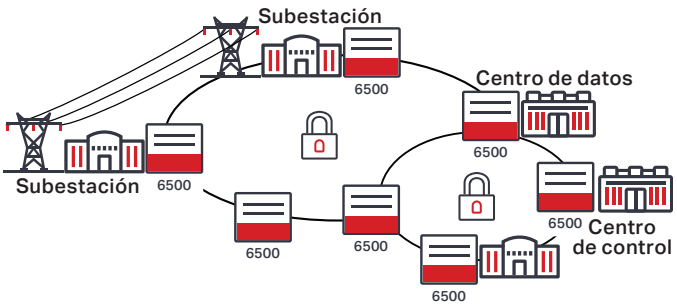


*Figura 1. WaveLogic Encryption de Ciena*

La solución WaveLogic Encryption de Ciena permite a las compañías de electricidad:

- Converger sin problemas las redes OT/IT de la compañía de electricidad y cumplir con los requerimientos de conformidad sobre una única infraestructura convergente y sumamente segura
- Cumplir con los requisitos NERC-CIP de protección de las redes de la compañía de servicios eléctricos a través de cifrado certificado por FIPS de todos sus datos activos durante las 24 hs, los siete días de la semana
- Aprovechar las ofertas de banda ancha flexibles con cifrado wire-speed de 10G, 100G o 200G sin impacto en el rendimiento de las aplicaciones de la compañía de energía
- Beneficiarse de un enfoque de gestión del cifrado simple e integrado que separa la administración de cifrado de la administración de transporte. Esto permite al equipo de redes de la compañía de electricidad administrar la red mientras el equipo de seguridad mantiene el control total de los parámetros de seguridad de cifrado asociados con sus datos críticos, generando nuevas claves o certificados según lo requieran sus políticas de seguridad

**WaveLogic Encryption Solution**
**Descargar la nota de aplicación**

El cifrado de datos estáticos y activos no es mutuamente exclusivo. Ambos se implementan normalmente de forma conjunta y se complementan entre sí como parte de una estrategia de seguridad integral. Al implementar una estrategia de seguridad de datos en múltiples niveles y en profundidad, las compañías de electricidad deben comprender los requerimientos del caso de uso, la aplicación y el cumplimiento. También deben asegurarse de que el software o la tecnología que hayan elegido cumpla con el más alto nivel de estándares y algoritmos de cifrado. La solución WaveLogic Encryption de Ciena combina un alto grado de flexibilidad y seguridad, con la facilidad de operación y administración, para crear una solución de cifrado wire-speed rentable y de alta capacidad para el mercado de los servicios eléctricos.

**Visite la Comunidad de Ciena**
Obtenga respuestas a sus preguntas