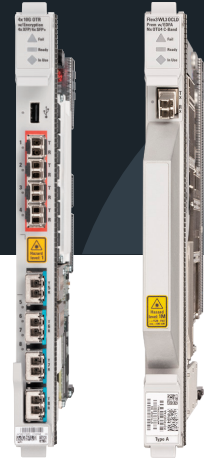


Módulos de cifrado a velocidad de cable de alta capacidad

Para la 6500 Packet-Optical Platform



Diseñada para garantizar la confidencialidad de los datos activos, la 6500 Packet-Optical Platform de Ciena ofrece una solución de cifrado a velocidad de cable rentable, agnóstica a protocolos y de 10G, 100G o 200G que combina facilidad de operación y administración para posibilitar una estrategia de protección de datos sencilla de implementar para servicios Ethernet, Canal de fibra, SONET/SDH, y red de transporte óptico (Optical Transport Network, OTN).

La solución 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 plataforma 6500 líder del mercado, desplegada por más de 600 operadores en todo el mundo. 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, reduciendo la complejidad de la red y eliminando la necesidad de administrar distintas soluciones de cifrado para varias aplicaciones.

Una solución certificada y sumamente segura

Como parte del enfoque de seguridad en múltiples capas de Ciena que garantiza la confidencialidad, integridad y disponibilidad de los datos en la red, el cifrado está siempre activo con la solución WaveLogic Encryption de Ciena, garantizando así el más alto nivel de seguridad, ya que el tráfico está siempre encriptado. Si bien la posibilidad de encender o apagar el cifrado puede parecer una flexibilidad adicional, un simple error humano puede resultar en el envío de tráfico sensible sobre la red no cifrada. La solución está validada externamente y certificada independientemente por terceros para garantizar que se implemente con el motor AES y algoritmos basados en estándares. La solución cumple con estándares de seguridad reconocidos, que incluyen los Criterios comunes y la certificación de FIPS, y también ofrece un motor de cifrado AES-256 certificado por FIPS con mecanismos de autenticación basados en estándares (como los certificados X.509) que simplifican las operaciones con perfecta integración a las PKI actuales de la empresa.

Funciones y beneficios

- Es una solución de cifrado a velocidad de cable con latencia ultrabaja para comunicaciones de extremo a extremo transparentes y sumamente seguras
- Proporciona cifrado no dependiente de protocolos, y flexibilidad para el soporte de una variedad de servicios
- Asegura todos los datos críticos en transmisión a través de una solución de cifrado AES256 (Advanced Encryption Standards) conforme con FIPS
- Utiliza dos conjuntos de claves distintos para funciones de cifrado de datos y autenticación, con un intervalo rápido de rotación de claves de cifrado de solo segundos
- Se integra perfectamente a las infraestructuras de clave pública (PKI) empresariales usando autenticación basada en certificados X.509
- Facilita la administración segura de la capacidad de cifrado como un servicio por parte del usuario final en infraestructuras gestionadas por operadoras o empresas 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

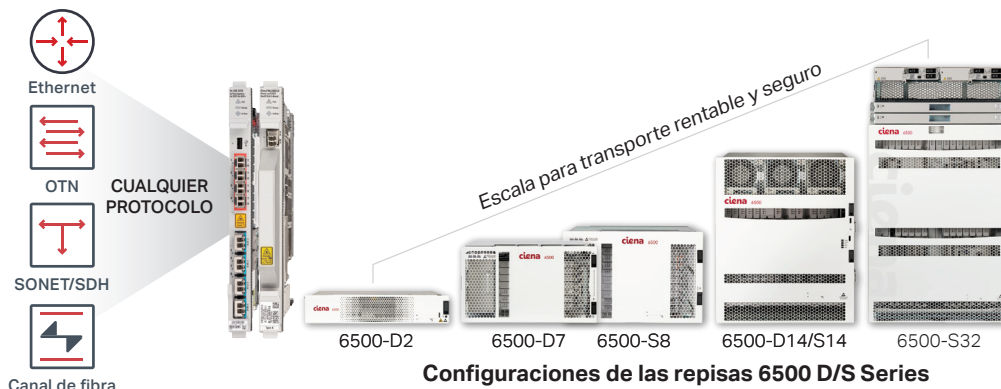



Figura 1: Solución WaveLogic Encryption para la 6500 de cifrado a velocidad de cable e independiente de protocolos que escala para cumplir con los requerimientos de su red

Flexibilidad inigualable

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 para el soporte de múltiples aplicaciones entre los clientes preocupados por la seguridad. Los clientes pueden desplegar servicios diferenciados con conectividad de latencia ultrabaja y varias opciones de protección de rutas y equipos.

Prueba y certificación de cifrado
 Descargar el Infobrief 

Cifrado blindado

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 transmisión, 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.



Figura 2. Módulo 4x10G OTR con cifrado

Cifrado a velocidad de cable de 10G

Los operadores pueden ofrecer servicios cifrados de 10 G en forma rentable, utilizando el módulo 4x10G Optical Transponder (OTR) con cifrado de una sola ranura que proporciona 40G de capacidad de servicios cifrados a velocidad de cable a través de cuatro puertos de línea distintos, cifrados e independientes de protocolos. Este módulo compatible con FIPS 140-2 de nivel 3 brinda mayor protección de la información crítica contra la manipulación física mediante la puesta a cero; todos los datos se ajustan en cero en el momento en que se detecta cualquier acceso físico no autorizado al módulo criptográfico, aún cuando la tarjeta no esté conectada a la repisa.

WaveLogic Encryption programable de 100G o 200G

La solución WaveLogic Encryption de Ciena aprovecha la tecnología coherente WaveLogic líder en el sector para ofrecer una solución de cifrado de alta capacidad, flexible y adaptable a través del nuevo módulo de línea WaveLogic 3 (WL3) Extreme. WL3 Extreme emplea las capacidades de WL3 y proporciona rendimiento extremo para todas las aplicaciones de la red coherente a través del uso de modulaciones adicionales y mayor mitigación de los

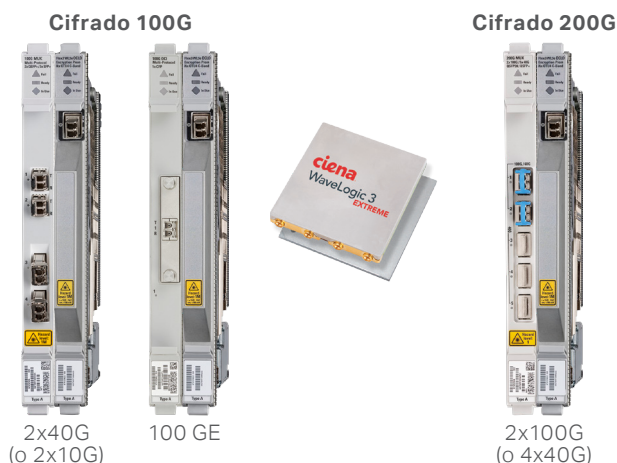


Figura 3. Ejemplos de cifrado a velocidad de cable de 100G o 200G con módulo de línea WL3 Extreme

Herramienta de administración de cifrado para usuario final/director de seguridad

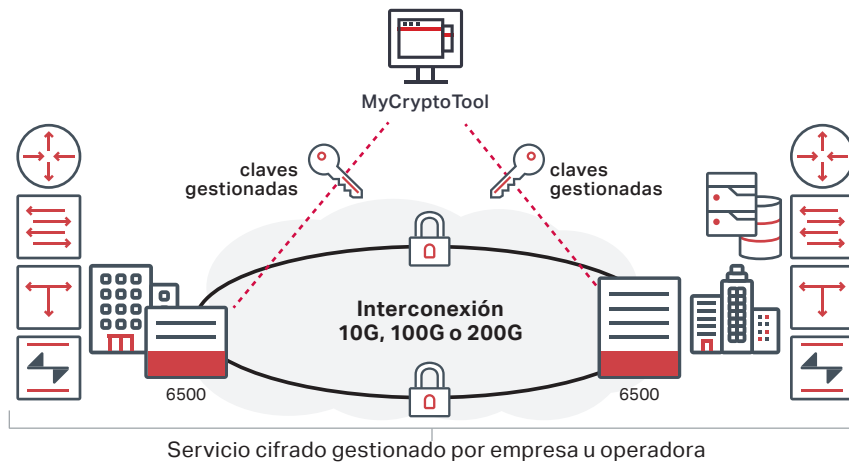


Figura 4. MyCryptoTool interfaz dedicada para la administración de cifrado

Seguridad de los datos con cifrado óptico
Descargar la infografía ahora



deterioros lineales y no lineales. Esta solución de vanguardia aborda todos los requerimientos de infraestructura, desde largas distancias hasta metropolitanas y proporciona modulación programable por software para ofrecer cifrado de 100G con modulación QPSK y cifrado de 200G con modulación 16QAM—la primera en el sector.

Al integrar este módulo de línea WL3 Extreme con cualquiera de las distintas interfaces cliente, los operadores tienen la flexibilidad de desplegar una solución que se adapte a sus necesidades de tráfico específicas, ya sea transporte de servicios de 10G, 40G o 100G. A medida que las demandas aumentan, el mismo módulo de línea WL3 Extreme puede programarse 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, con la maximización de la eficiencia de los recursos de red.

Administración de cifrado simplificada

La solución WaveLogic Encryption 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/director de seguridad administrar independientemente los parámetros y alarmas de seguridad de los servicios 10G, 100G o 200G gestionados 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.

La solución WaveLogic Encryption de Ciena combina un alto grado de flexibilidad y seguridad con facilidad de operación y administración para ofrecer una solución de cifrado rentable, agnóstica a protocolos, de 10G/100G/200G y latencia ultrabaja para obtener prácticamente todas las aplicaciones de comunicaciones de escala web de la actualidad.

Cifrado a velocidad de cable
Nota de aplicación para la solución
Descargar ahora



Información técnica

Tarjeta de servicios	4x10G OTR con cifrado	Módulo de línea WaveLogic 3 Extreme con cifrado
Requisitos del sistema	Opera en cualquier chasis de 6500 S/D Series	Opera en cualquier chasis de 6500 S/D-Series con excepción de 6500-D2
Formato de puerto Interfaces de cliente compatibles	OC-192/STM-64 10GbE LAN, 10GbE WAN FC400, FC800, FC1200 OTU2/OTU2e	OC-192/STM-64 10GbE LAN, 10GbE WAN, 40GbE, 100GbE FC800, FC1200 OTU2, OTU2e, OTU3, OTU4, ODU-Flex
Interfaces de línea compatibles	OTU2 OTU2e	100G coherentes (QPSK); 1xOTU4 200G coherentes (16QAM); 2xOTU4
Opciones de protección	Protección de línea 1+1 Protección de cliente y equipos 1+1	Protección de línea 1+1 Protección de cliente y equipos 1+1
Modos FEC	RS-8 FEC, UFEC y OFF que cumplen con G.709	Soft FEC
Características ambientales Temperatura de funcionamiento Humedad relativa Altitud	+41 °F a +104 °F (+5 °C a +40 °C); +23 °F a +131 °F (-5 °C a +55 °C) corto plazo – para 6500-D2/D7/S8/D14/S14 +23 °F a +122 °F (-5 °C a +50 °C) corto plazo – para 6500-S32 5% a 85% (sin condensación) 13 000 ft; 4000 m	
Características físicas	11.34 in (H) x 0.99 in (W) x 9.34 in (D) 288 mm (al.) x 25 mm (an.) x 237 mm (pr.)	
Características de seguridad	<ul style="list-style-type: none"> • Solución de cifrado AES-256 certificado por NIST para cifrado de datos • Algoritmos de criptografía de curvas elípticas (Elliptic Curve Cryptography, ECC) • Intercambio de claves seguro Diffie-Hellman (incluye curva elíptica) • Soporte para autenticación con certificados X.509 • Soporte para Lista de Revocación de Certificados (Certificate Revocation List, CRL) • Rotación de claves AES-256 sin errores cada segundo • Interfaz protegida por TLS y mutuamente autenticada para la administración del cifrado • Soporte de autenticación RADIUS • TACACS+AAA • Soporte SNMPv3 	
	<ul style="list-style-type: none"> • Certificados 2048-bit RSA • Certificados de curvas elípticas 	<ul style="list-style-type: none"> • Certificados de curvas elípticas
Certificaciones	<ul style="list-style-type: none"> • Criterios comunes para el perfil de protección de dispositivos de red • BSI (Oficina federal alemana para la seguridad de la información) • FIPS 140-2 Nivel 3 – Certificado #2379, #2635 • FIPS 197 – AES-256 – Certificado #2963, #2964, #3599, #3600 • IBM GDPS • EMC, Brocade 	<ul style="list-style-type: none"> • Criterios comunes para el perfil de protección de dispositivos de red • BSI (Oficina federal alemana para la seguridad de la información) • FIPS 140-2 Nivel 2 – Certificado #2697, #2843 • FIPS 197 – AES-256 – #3601, #3602, #4231, #4232, #5241 • IBM GDPS • EMC, Brocade

Conéctese con Ciena ahora

