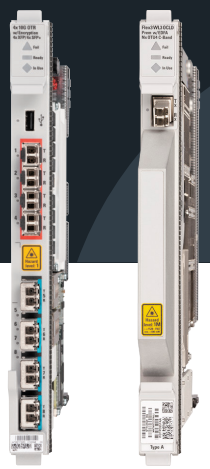
FOLHA DE DADOS

Módulos de criptografia de alto desempenho e alta capacidade

Para a 6500 Packet-Optical Platform



Projetada para garantir a confidencialidade dos dados em trânsito, a 6500 Packet-Optical Platform da Ciena possibilita, de forma econômica, uma solução de criptografia flexível, independente de protocolo, de alto desempenho 10G, 100G ou 200G, que combina facilidade de operação e administração para uma estratégia de proteção de dados simples de implementar em serviços Ethernet, Fibre Channel, SONET/SDH e OTN (Optical Transport Network).

A solução WaveLogic Encryption da Ciena combina tecnologia de criptografia comprovada, implantada em plataformas que possuem uma grande base global instalada, com a confiabilidade comprovada do 6500 líder do mercado, implementada por mais de 600 operadoras em todo o globo. As operadoras podem se beneficiar de uma solução que simplifica a implantação da criptografia integrando funcionalidade de criptografia diretamente no elemento de rede dentro da rede de transporte, reduzindo a complexidade e eliminando a necessidade de gerenciar diferentes soluções de criptografia para várias aplicações.

Uma solução altamente segura e certificada

Como parte da abordagem de segurança multicamada da Ciena que garante a confidencialidade, integridade e disponibilidade dos dados na rede, a criptografia está sempre ativada na solução WaveLogic Encryption da Ciena, que criptografa em todo momento todo o tráfego, garantindo, desta forma, o mais alto nível de segurança. Ainda que a capacidade de ativar ou desativar a criptografia possa parecer uma flexibilidade a mais, um simples erro humano pode resultar na ocorrência de tráfego sigiloso não criptografado na rede. A solução é validada externamente e certificada de forma independente por terceiros para garantir sua implementação com os algoritmos e o mecanismo AES baseado em padrões. Atendendo aos mais altos padrões de segurança reconhecidos, que incluem Critérios comuns (Common Criteria) e certificação FIPS, a solução fornece um mecanismo de criptografia AES-256 com certificação FIPS com mecanismos de autenticação baseados em padrões (como certificados X.509), permitindo simplificação operacional com integração perfeita aos PKIs corporativos existentes.

Recursos e benefícios

- Oferece uma solução de criptografia de alto desempenho e de latência ultrabaixa para comunicações ponta a ponta altamente seguras e transparentes
- Apresenta criptografia independente de protocolo, oferecendo flexibilidade para suporte a uma variedade de serviços
- Protege todos os dados em trânsito (in-fligh) essenciais por meio da solução de criptografia AES-256 com certificação FIPS
- Utiliza dois conjuntos distintos de chaves para autenticação e criptografia de dados, com um rápido intervalo de segundos para rotação de chaves de criptografia
- Integra-se totalmente às PKIs (Public Key Infrastructures) corporativas existentes usando autenticação baseada na certificação X.509
- Possibilita gerenciamento seguro do recurso Encryption-as-a-Service pelo usuário final em infraestruturas gerenciadas por operadora ou empresa através de uma ferramenta de gerenciamento integrada
- Entrega uma solução de criptografia comprovada em campo, amplamente implantada no mundo em redes financeiras, de serviços públicos, de serviços de saúde, militares e governamentais

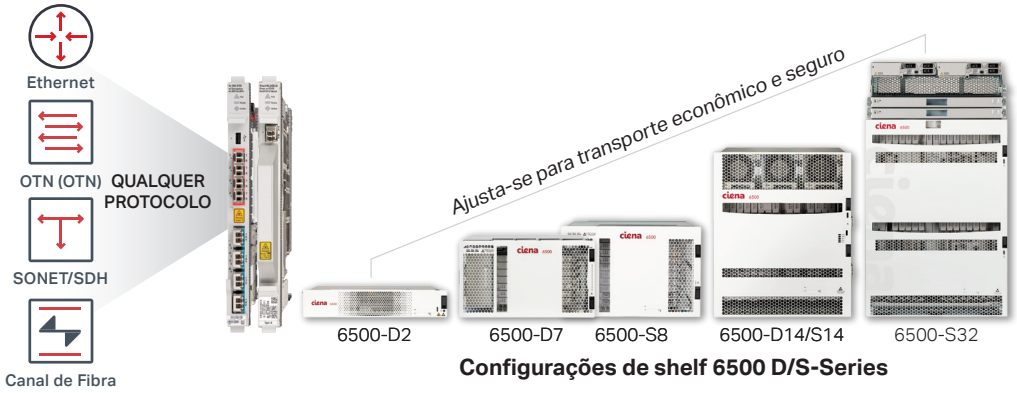


Figura 1: solução de alto desempenho e independente de protocolo WaveLogic Encryption do 6500 que acompanha os seus requisitos de rede

Flexibilidade inigualável

Com a flexibilidade do 6500, os clientes podem selecionar o tamanho ideal de shelf que atenda aos seus requisitos de capacidade, espaço e energia específicos ao local para transporte de serviços criptografados com boa relação custo-benefício. Um outro benefício importante é que a solução é totalmente independente de protocolo, possuindo uma ampla faixa de clientes flexíveis para oferecer suporte a várias aplicações de clientes preocupados com a segurança. Os clientes podem implantar serviços diferenciados com conectividade de latência ultrabaixa e várias opções de proteção de caminho/equipamento.

Teste de criptografia e certificação
Faça o download do informativo

Criptografia Ironclad

Para maior proteção de dados, dois diferentes conjuntos de chaves independentes são usados para autenticação e criptografia de dados, com um intervalo rápido de rotação de chaves de criptografia de segundos em vez de minutos. As chaves de sessão de criptografia de dados AES-256 são negociadas e rotacionadas de forma autônoma a cada segundo, independentemente, em cada porta de linha, sem afetar o tráfego ou o rendimento e sem intervenção do usuário. As operadoras podem implantar a nova geração de algoritmos de criptografia de chave pública com suporte para ECC (Elliptic Curve Cryptography), o que possibilita uma estratégia significativamente mais segura que os sistemas de criptografia de chaves públicas de primeira geração.

Figura 2. Módulo 4x10G OTR com criptografia

Criptografia de alto desempenho 10G

As operadoras podem, de forma econômica, oferecer serviços criptografados de 10G utilizando o módulo 4x10G OTR (Optical Transponder) de slot único com criptografia que permite 40G de capacidade de serviço criptografado de alto desempenho por meio de quatro diferentes portas de linha criptografadas e independentes de protocolo. O módulo compatível com FIPS 140-2 Nível 3 oferece maior proteção para informações essenciais contra sabotagem física por meio da "zeroização"; todos os dados são ajustados para zero no momento em que é detectada qualquer sabotagem física do módulo criptográfico, mesmo quando a placa não está conectada no shelf.

WaveLogic Encryption 100G ou 200G programável

A solução WaveLogic Encryption da Ciena aproveita a tecnologia coerente WaveLogic líder de mercado, possibilitando uma solução de criptografia personalizável, de alta capacidade e flexível por meio do novo módulo de linha WL3 (WaveLogic 3) Extreme. O WL3 Extreme conta com os recursos do WL3 e permite desempenho extremo para todas as aplicações de rede coerentes com o uso de modulações adicionais e minimização aprimorada de

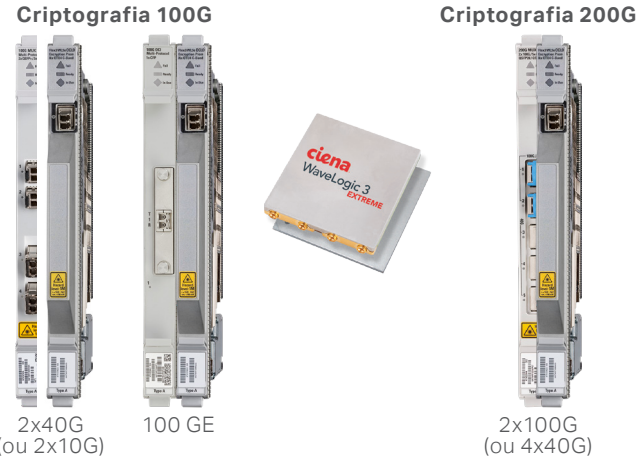


Figura 3. Exemplos de criptografia de alto desempenho 100G ou 200G com o módulo de linha WL3 Extreme

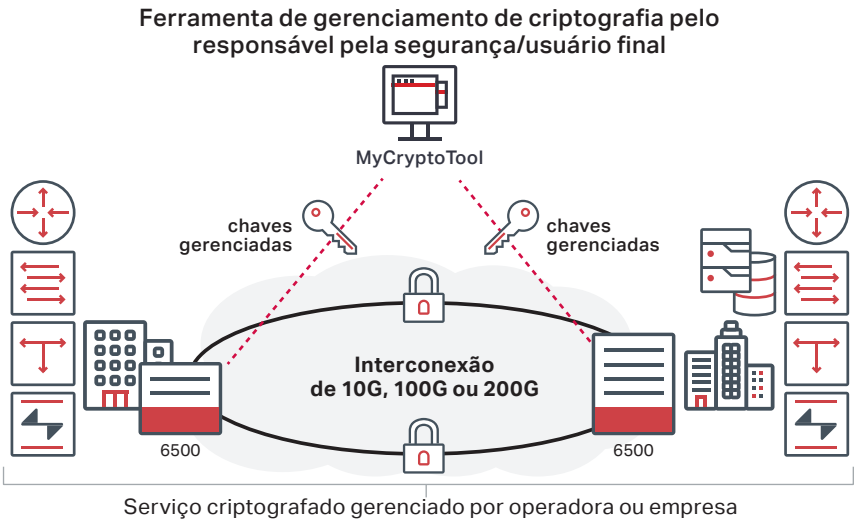


Figura 4. A interface dedicada de gerenciamento de criptografia MyCryptoTool

Segurança de dados com criptografia óptica
Faça download agora do infográfico

deficiências lineares e não lineares. Essa solução de ponta atende a todos os requisitos de infraestrutura, de aplicações metropolitanas até longa distância, e proporciona modulação programável por software para ativar tanto a criptografia de 100G com modulação QPSK quanto a criptografia de 200G com modulação 16QAM, a primeira do setor.

Integrando esse módulo de linha WL3 Extreme com qualquer uma das várias interfaces de cliente, as operadoras têm a flexibilidade de implantar uma solução ajustada para atender a necessidades de tráfego específicas, seja de transporte de serviço de 10G, 40G ou 100G. À medida que a demanda crescer, o mesmo módulo de linha WL3 Extreme poderá ser programado para transportar 200G de tráfego criptografado simplesmente adicionando uma placa de cliente. Além disso, as operadoras poderão implantar serviços criptografados de alta capacidade na rede, utilizando a malha híbrida pacote/OTN de alta capacidade do 6500, maximizando a eficiência dos recursos da rede.

Simplificação do gerenciamento de criptografia

A solução WaveLogic Encryption da Ciena inclui a MyCryptoTool, uma interface dedicada de gerenciamento de criptografia projetada para gerenciamento distribuído da rede que permite que o usuário final/diretor de segurança gerencie de forma independente os parâmetros e os alarmes de segurança dos serviços de 10G, 100G e 200G gerenciados por empresa ou operadora. A MyCryptoTool é uma interface intuitiva que se conecta com segurança ao módulo criptográfico e permite autenticação mútua, limitando o acesso à equipe de segurança autorizada.

A solução WaveLogic Encryption combina uma alto nível de flexibilidade e segurança com facilidade de operação e administração para permitir uma solução de criptografia de latência ultrabaixa, de 10G/100G/200G, independente de protocolo e econômica, para proteger praticamente todos os aplicativos de comunicação em escala Web.

Solução de criptografia de alto desempenho - Nota sobre a aplicação
Faça o download

Informações técnicas

Pacote de circuitos	4x10G OTR com criptografia	Módulo de linha WaveLogic 3 Extreme com criptografia
Requisitos do sistema	Opera em qualquer chassi 6500 S/D-Series	Opera em qualquer chassi 6500 S/D-Series, exceto o 6500-D2
Formato de porta **Interfaces do cliente compatíveis**	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 linha compatíveis	OTU2 OTU2e	Coerente de 100G (QPSK); 1 x OTU4 Coerente de 200G (16QAM); 2xOTU4
Opções de proteção	Proteção de linha 1+1 Proteção de cliente e equipamento 1+1	Proteção de linha 1+1 Proteção de cliente e equipamento 1+1
Modos FEC	Conformidade com G.709 RS-8 FEC, UFEC e OFF	FEC suave
Características ambientais Temperatura operacional Umidade relativa Altitude	 +5 °C a +40 °C (+41 °F a +104 °F) -5 °C a + 55 °C (+ 23 °F a + 131 °F) a curto prazo - para 6500-D2/D7/S8/D14/S14 -5 °C a +50 °C (+23 °F a +122 °F) curto prazo – para 6500-S32 5% a 85% (sem condensação) 13.000 pés; 4.000 metros	
Características físicas	28,8 cm (A) x 2,5 cm (L) x 23,7 cm (P) 11,34 pol. (A) x 0,99 pol. (L) x 9,34 pol. (P)	
Funcionalidades de segurança	• Solução de criptografia AES-256 com certificação NIST para criptografia de dados • Algoritmos ECC (Elliptic Curve Cryptography) • Negociação de chaves seguras Diffie-Hellman (incluindo Elliptic Curve) • Suporte à certificação X.509 para autenticação • Suporte a CRL (Certificate Revocation List) • Rotação de chaves AES-256 a cada segundo sem interrupção • Interface mutuamente autenticada e com proteção TLS para gerenciamento de criptografia • Suporte a autenticação do Radius • TACACS + AAA • Suporte a SNMPv3	
	• Certificação RSA de 2.048 bits • Certificações Elliptic Curve	• Certificações Elliptic Curve
Certificações	• Certificação para Critérios comuns (CC) do Perfil de proteção colaborativa de dispositivos de rede (NDCPP) • BSI (Escritório Federal Alemão de Segurança da Informação) • FIPS 140-2 Nível 3 – Certificado no. 2379, no. 2635 • FIPS 197 – AES–256 – Certificado no. 2963, no. 2964, no. 3599, no. 3600 • GDPS, IBM • EMC, Brocade	• Certificação para Critérios comuns (CC) do Perfil de proteção colaborativa de dispositivos de rede (NDCPP) • BSI (Escritório Federal Alemão de Segurança da Informação) • FIPS 140-2 Nível 2 – Certificado no. 2697, no. 2843 • FIPS 197 – AES–256 – Certificado no. 3601, no. 3602, no. 4231, no. 4232, no. 5241 • GDPS, IBM • EMC, Brocade

Entre em contato com a Ciena