NOTA SOBRE O APLICATIVO

Soluções WaveLogic Encryption

Proteção de dados em trânsito, o tempo todo.

A segurança é um problema que está exigindo maior atenção. Um Relatório sobre ameaças de dados feito pela Thales em 2020[1] revelou que 49% das empresas globais participantes foram vítimas de uma violação em algum momento de sua história. A maioria dos setores pesquisados, como serviços de saúde, finanças, governo e educação, relatou violações muito acima da média.

Além de ameaçarem as informações do cliente, as violações de dados impactam os resultados financeiros das organizações. De acordo com um estudo global realizado pela Ponemon[2], cerca de 25.500 registros são expostos durante cada violação de dados, colocando o custo de uma única violação na casa de milhões, além da incalculável perda de confiança do cliente. Este estudo também revelou que o custo total médio de uma violação de dados nos EUA em 2019 foi de US $ 8,19 milhões. Novamente, isso varia de acordo com o setor; o custo por registro perdido no setor de saúde é quase o dobro.

Porém, mesmo com a ameaça crescente das violações, o fluxo de tráfego na rede vem crescendo. As demandas por largura de banda continuam crescendo, exigindo uma rede que se ajuste apropriadamente para suportar capacidades mais altas com menos complexidade operacional. Além disso, com a crescente sofisticação e frequência das violações de dados, nenhuma organização está imune à constante ameaça de ataques mal-intencionados para coleta de informações privadas e sigilosas. As redes de hoje precisam de muito mais que largura de banda de alta capacidade: elas precisam de uma estratégia de segurança para proteção de todos os dados críticos, tanto em repouso como em trânsito, à medida que percorrem o globo cruzando distâncias metropolitanas, regionais, longas e submarinas.

Projetada para proteger as redes de alta capacidade de hoje, a solução WaveLogic™ Encryption da Ciena inclui, na amplamente implantada 6500 Packet-Optical Platform, uma solução econômica de criptografia de latência ultrabaixa, alta capacidade e independente de protocolo. As soluções se estendem à família Waveserver® da Ciena de dispositivos de transporte modulares compactos e de alta capacidade, que permitem aplicações de interconexão de data center (DCI) seguras e econômicas. Essa criptografia always-on combina facilidade de operação e administração para possibilitar uma estratégia de proteção de dados simples de implementar e que

Benefícios

- Oferece uma solução de criptografia compatível com FIPS e de latência ultrabaixa para comunicações de ponta a ponta altamente seguras e transparentes
- Escala com tecnologia coerente WaveLogic programável para criptografia flexível de 100G a 400G de alto desempenho
- Apresenta criptografia independente de protocolo, oferecendo flexibilidade para suporte a uma variedade de serviços
- Utiliza recursos de segurança aprimorados, incluindo 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 através de uma ferramenta de gerenciamento integrada
- Entrega uma solução de criptografia comprovada em campo, amplamente implantada no mundo em redes financeiras, legais, de serviços de saúde, militares e governamentais

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

utiliza a tecnologia coerente e líder do setor WaveLogic da Ciena para oferecer flexibilidade e desempenho incomparáveis. É a primeira solução do setor para criptografia coerente de alto desempenho de 100G a 400G.

Tecnologia de criptografia

A criptografia é definida como o processo de transformação de informações por meio de algoritmo visando torná-las ilegíveis a todos os que não possuam o conhecimento especial, a chamada chave de criptografia. Essencialmente, esse processo bloqueia a rede criptografando esses dados de forma que não possam ser usados por um invasor que os intercepte ou por qualquer pessoa que não tenha a chave correta para decifrar a mensagem.

Existem muitas maneiras de criptografar dados, definidas por vários padrões que especificam os requisitos de criptografia para suporte de produtos e chaves, e que estabelecem um processo de certificação para o equipamento da rede. Há diversos algoritmos de criptografia baseados em padrões, incluindo o AES (Advanced Encryption Standard), que possui vários tamanhos de chaves (de 56, 128 e 256 bits) publicados pelo NIST (National Institute of Standards and Technology). Estas normas são divulgadas como publicações do Federal Information Processing Standard (FIPS) dos EUA. Por exemplo, o algoritmo de criptografia AES-256 foi publicado como FIPS 197. Além das publicações com algoritmos específicos, como o FIPS 197, o NIST também publica no FIPS 140-2 os padrões que coordenam os requisitos para módulos de criptografia que incluem componentes de hardware e software.

Existem outras estruturas semelhantes usadas para certificar soluções de criptografia. Outro padrão importante é o Common Criteria (CC) para Avaliação de Segurança de Tecnologia da Informação, que é um padrão internacional (ISO/IEC 15408) para certificação de segurança da computação. O Common Criteria fornece um meio de garantir que o processo de especificação, implementação e avaliação de um dispositivo de rede, como um elemento de rede em uma rede óptica, seja conduzido de maneira rigorosa e padronizada. Na Alemanha, o BSI, Departamento Federal de Segurança de Informações da Alemanha, emite certificados de segurança que incluem a certificação Common Criteria. Os certificados do BSI baseados em Common Criteria normalmente são usados como base para a certificação local, o que economiza tempo e dinheiro no processo de certificação. Este conjunto de padrões e processos de certificação dá aos provedores de serviços e usuários finais a garantia de que a solução de criptografia está em conformidade com os requisitos definidos, tendo completado com êxito os rigorosos testes de laboratório e revisões exigidos pelos padrões normatizados.

Figura 1. A criptografia de dados em trânsito faz parte de uma estratégia holística de segurança

Proteção das redes de hoje

A criptografia é usada amplamente hoje em dia para proteger dados em repouso e em trânsito (in-flight). De acordo com um relatório da Ponemon sobre tendências de criptografia, somente 13% dos entrevistados globais não possuíam estratégia de criptografia.[3] Organizações de todos os tamanhos e setores devem envidar grandes esforços para a proteção das informações armazenadas em seus data centers contra acessos não autorizados. O impacto e o custo de uma violação de dados não podem ser ignorados e apresentam consequências cada vez mais graves para uma organização, incluindo perda de reputação da empresa, processo criminal, multas altas por descumprimento da lei e alta rotatividade de clientes.

Hoje existe uma série de técnicas usadas frequentemente para proteger dados em repouso em servidores, bancos de dados, roteadores e switches seguros por meio de gerenciamento de acesso e credenciamento de usuário. No entanto, nas atuais redes em escala Web, grandes volumes de dados essenciais estão em trânsito, tendo em vista que as comunicações de alta largura de banda ocorrem além das paredes do data center, atravessando uma rede maior, provavelmente internacional. Uma abordagem de segurança de TI abrangente deve, portanto, incluir uma solução robusta de criptografia de dados em trânsito (in-flight) como parte de sua estratégia holística de segurança, como mostra a Figura 1. Criptografando os dados quando eles deixam a segurança da nuvem privada, as operadoras podem assegurar que esses dados ficarão protegidos de interceptação não autorizada ao atravessar a rede, cruzando níveis de segurança variáveis até atingirem seu destino.

Ainda que muitas organizações estejam incluindo a criptografia de dados em trânsito em sua estratégia de segurança, o foco tradicionalmente para esses dados tem sido na criptografia na Camada 2 ou superior. Apesar de esta ser uma boa opção para algumas aplicações de TI de baixa velocidade que não usam muitos dados nem são urgentes, muitas vezes ela não é usada em toda a empresa e só é usada em dados de aplicações IP. Esse modelo operacional para implantação de uma solução de criptografia é muito

3 Ponemon, relatório de pesquisa da Thales e-Security: 2018 Global Encryption Trends Study; Abril de 2018; https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

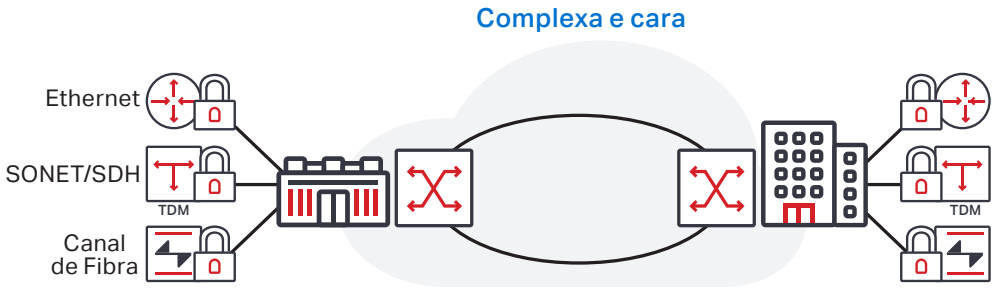

Figura 2. Criptografia tradicional de protocolo específico implantada em uma rede multisserviço

complexo e caro, como mostra a Figura 2, pois geralmente requer dispositivos de criptografia independentes de protocolo e podem contribuir com quantidade significativa de latência, impactando o rendimento da aplicação e resultando no uso ineficiente da largura de banda. Além disso, o gerenciamento e a autenticação de chaves de criptografia em vários dispositivos independentes são complexos e trabalhosos, e a solução de problemas de rede de ponta a ponta é mais complicada em muitos dispositivos independentes. Essa abordagem cria ainda uma lacuna na estratégia de proteção de dados em trânsito da organização. Apesar de, tradicionalmente, o risco da invasão de cabos de fibra óptica não ser levado em conta na estratégia de segurança das empresas, é real a ameaça de infiltração de cabos ópticos para acesso dos dados que estão sendo transportados. Os cabos de fibra óptica normalmente ficam desprotegidos e podem ser acessados com facilidade; qualquer pessoa com as ferramentas certas pode ter acesso a um cabo de fibra óptica e coletar dados sem que essa violação seja detectada por dias, meses ou mesmo anos. A implementação de uma solução de criptografia da camada de transporte protege constantemente todos os dados em trânsito, garantindo a segurança de cada bit.

Data Security with Optical Encryption
Faça download agora do infográfico

WaveLogic Encryption

Como parte da abordagem de segurança multicamada da Ciena que garante a confidencialidade, integridade e disponibilidade dos dados na rede, a solução WaveLogic Encryption da Ciena combina a tecnologia de criptografia comprovada implantada em plataformas que possuem uma grande base global instalada com a confiabilidade comprovada da plataforma líder de mercado 6500 Packet-Optical Platform, implantada por mais de 600 operadoras em todo o mundo. Além disso, as capacidades da solução WaveLogic Encryption da Ciena se estendem ao sistema de interconexão empilhável Waveserver e Waveserver Ai da Ciena, permitindo 1,2Tb de capacidade de criptografia de alto desempenho em 1RU para aplicações DCI de rack e pilha simples.

Fácil de implementar

Com WaveLogic Encryption, as operadoras podem se beneficiar de uma solução que simplifica a implantação da criptografia integrando essa funcionalidade diretamente no elemento de rede dentro da rede de transporte. Essa abordagem reduz a complexidade da rede e elimina a necessidade de gerenciamento de diferentes soluções de criptografia para várias aplicações, como mostra a Figura 3. Essa simplificação operacional também se estende ao gerenciamento da solução de criptografia, incluindo uma ferramenta dedicada de autenticação e gerenciamento de chaves, e à fácil integração em PKIs corporativos.

A flexibilidade da plataforma 6500 permite que os clientes selecionem o tamanho ideal de shelf para melhor atender aos seus requisitos de capacidade, espaço e energia específicos ao local para transporte de serviços criptografados com boa relação custo-benefício.
Um benefício-chave adicional é que a solução é totalmente independente de protocolo, oferecendo suporte a uma ampla faixa de clientes flexíveis, incluindo Ethernet, SONET/SDH, Fibre Channel e OTN, para atender a várias aplicações de clientes preocupados com a segurança.

Diferenciação com a criptografia em tempo integral

A criptografia sempre está ativa nas soluções WaveLogic Encryption da Ciena, garantindo o mais alto nível de segurança, visto que o tráfego de rede está sempre

Figura 3. Solução 6500 WaveLogic Encryption da Ciena

criptografado. 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. As operadoras podem utilizar uma infraestrutura diferenciada que proteja constantemente todos os dados em trânsito, tendo em vista que eles percorrem o globo cruzando distâncias metropolitanas, regionais, longas e submarinas. Além disso, as operadoras podem aumentar as receitas e a retenção de clientes oferecendo contratos de nível de licença (SLAs) de alta velocidade utilizando serviços criptografados com conectividade de latência ultrabaixa e diversas opções de proteção de caminho/equipamento.

Criptografia Ironclad

A solução WaveLogic Encryption da Ciena é validada externamente e certificada de forma independente por terceiros a fim de garantir sua implementação com algoritmos padrão do setor e recursos avançados de segurança que incluem Common Criteria e certificação FIPS. Ela apresenta um mecanismo de criptografia AES-256 com certificação FIPS e autenticação baseada em padrões (como certificações X.509), possibilitando integração total em PKIs corporativos existentes. Além disso, os componentes de hardware e software 6500 dos módulos de criptografia são compatíveis com o FIPS 140-2 e certificação BSI completa sob Common Criteria para Avaliação de Segurança de Tecnologia da Informação, oferecendo aos provedores de serviços e usuários finais a garantia de que a solução de criptografia está em conformidade com todos os aspectos abordados por essa avaliação abrangente, incluindo algoritmos de criptografia, mecanismos de troca de chaves e autenticação de usuário.

Para oferecer maior proteção de dados, dois conjuntos de chaves independentes diferentes 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.

Criptografia de alto desempenho de 100G ou 400G programável

Para atender às atuais necessidades das comunicações de alta capacidade, a solução WaveLogic Encryption da Ciena utiliza a tecnologia coerente WaveLogic, líder do setor, para permitir soluções de criptografia personalizáveis, flexíveis e de alta capacidade. O WaveLogic 3 Extreme conta com os recursos do WaveLogic 3 e fornece desempenho extremo para todas as aplicações de rede coerentes com o uso de modulações adicionais e minimização aprimorada de deficiências lineares e não lineares. Essa solução de ponta apresenta modulação programável por software para ativar criptografia de alto desempenho de 100G com modulação QPSK, criptografia de alto desempenho de 150G con 8QAM e criptografia de alto desempenho de 200G com modulação 16QAM. O WaveLogic Ai tem como base o melhor desempenho da classe do WaveLogic 3 e utiliza um avançado motor de 400G, otimizado para melhorar significativamente a economia de transporte: duplica a capacidade por canal, aumenta em três vezes a distância com capacidade equivalente, e quatro vezes a densidade de serviço.

No 6500, as operadoras podem integrar um módulo de linha WaveLogic 3 Extreme com criptografia, junto com qualquer uma das várias interfaces de cliente, para implementar, de forma flexível, uma solução ajustada para atender suas necessidades de tráfego específicas, sejam de serviço de transporte de 10G, 40G ou 100G. À medida que as demandas aumentam, com essa oferta modular de pagamento conforme o crescimento, o mesmo módulo de linha pode ser programado para transportar 200G de tráfego criptografado com a simples inclusão de um placa de cliente adicional. 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.

No Waveserver, as operadoras aproveitam até 400 Gb/s de capacidade de linha de criptografia de alto desempenho AES-256 certificada FIPS em apenas 1RU e a flexibilidade para suportar um mix de 10GE, 40GE e 100GE clientes no mesmo dispositivo. A modulação programável permite que o Waveserver otimize sua capacidade de linha de criptografia de alto desempenho para cada aplicação/necessidade, permitindo comprimentos de onda de 100 Gb/s, 150 Gb/s ou 200 Gb/s. Para lidar com aplicativos de interconexão seguros de altíssima capacidade, as operadoras podem implantar o Waveserver Ai para habilitar até 1,2 Tb/s de capacidade criptografada em 1RU, com a capacidade de suportar três módulos de tráfego, cada um deles oferecendo até 400 Gb/s de capacidade criptografada. O Waveserver e o Waveserver Ai fornecem proteção de dados em trânsito altamente segura e com latência ultrabaixa em todas as distâncias metropolitanas, regionais ou longas.

Criptografia de alto desempenho de 10G do 6500

As operadoras podem fornecer serviços criptografados 10G com boa relação custo-benefício utilizando o módulo 4x10G Optical Transponder com criptografia. O módulo de slot único fornece 40G de capacidade de serviço criptografado

High-capacity Wire-speed Encryption Modules
Faça download agora da folha de dados

de alto desempenho via quatro diferentes portas de linha criptografadas 10G independentes de protocolo para que os clientes possam se beneficiar de projetos de rede mais simples com recurso de criptografia integrado em qualquer versão de chassi do 6500. O módulo oferece maior segurança com seu design compatível com FIPS 140-2 Nível 3, permitindo proteção contra sabotagem da placa, com suporte para zeroização. Isso assegura que, se for detectada alguma sabotagem física no módulo criptográfico, todas as informações essenciais de segurança serão removidas zerando-se todos os dados, mesmo se a placa não estiver conectada à prateleira.

Simplificação do gerenciamento de criptografia

A melhor solução de segurança da camada de transporte não estaria completa sem uma abordagem simplificada de gerenciamento de criptografia integrado. A separação do gerenciamento de criptografia do gerenciamento de transporte oferece flexibilidade adicional em uma infraestrutura mantida pela operadora ou pela empresa. Nos dois casos, é importante que o "proprietário" dos dados (o usuário final) mantenha total controle dos parâmetros de segurança de criptografia associados aos dados essenciais, emitindo novas chaves ou certificados conforme exigido por suas políticas de segurança, permanecendo informado sobre quaisquer alarmes de segurança e registros de ponta a ponta.

A solução 6500 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/responsável pela segurança gerencie de forma independente os parâmetros e os alarmes de segurança das redes gerenciadas por operadora ou por empresa. A MyCryptoTool é uma interface simples de usar que se conecta com segurança ao módulo criptográfico e permite autenticação mútua, limitando o acesso à equipe de segurança autorizada. Caso o serviço criptografado seja adquirido por meio de um provedor de serviços, o provedor gerenciará os links, seu provisionamento, administração e monitoramento de desempenho como em qualquer outro serviço, mas não terá controle ou visibilidade dos parâmetros de criptografia. A mesma abordagem é válida quando a solução de criptografia é implantada e gerenciada por dois diferentes grupos dentro da mesma empresa ou órgão do governo.

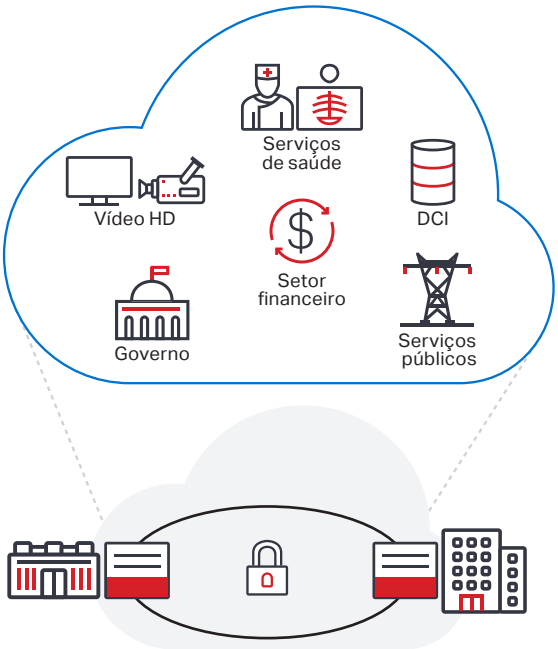

Figura 4. Exemplos de importantes aplicações da solução WaveLogic Encryption

Principais aplicações

As soluções WaveLogic Encryption da Ciena foram elaboradas para proteger dados em trânsito críticos em todas as aplicações de alta capacidade existentes. As principais aplicações que se beneficiam dessas soluções incluem:

- DCI corporativa para armazenamento de alta capacidade e transporte criptografado de dados
- Governos e instituições que requerem comunicações de alta velocidade, certificadas e seguras entre locais diferentes
- Aplicações de serviços de saúde com requisitos de alta qualidade e baixa latência para colaboração segura, eficiente e oportuna entre participantes dos serviços de saúde
- Aplicações de serviços gerenciados
- Aplicações sensíveis à latência, como vídeo de alta definição ou negociação rápida, que requerem uma solução de transporte de latência ultrabaixa
- Serviços públicos que desejam proteger suas infraestruturas de comunicação essenciais

Resumo

Com o aumento contínuo de informações sigilosas sendo distribuídas entre as redes de fibra óptica, as atuais comunicações devem implantar uma abordagem de segurança de TI que inclua não apenas segurança de servidor e criptografia em repouso, mas também uma solução robusta de criptografia em trânsito. A solução WaveLogic Encryption da Ciena combina um alto grau de flexibilidade e segurança com facilidade de operação e administração, permitindo soluções de criptografia de alta capacidade e alto desempenho para proteger, o tempo todo, todos os dados em trânsito, estejam eles cruzando a rua, a cidade, as fronteiras ou os oceanos.