Experience. Outcomes.

NOTA SOBRE O APLICATIVO

Proteção de nuvem

Simplificação da segurança entre data centers com a criptografia de Camada 1

A proteção de dados confidenciais ou estratégicos é essencial para resguardar a propriedade intelectual e os registros sigilosos, além de evitar multas caras e perdas de receita resultantes de violações de dados. Mas é um desafio identificar quais dados devem ser protegidos e como fazê-lo. O design físico do data center incorpora várias camadas de medidas de segurança física para restringir acessos indesejados. Além disso, é possível usar firewalls, programas antivírus e técnicas de detecção de invasão para proteger os dados dentro do data center. No entanto, depois que as informações saem desse ambiente protegido, a segurança geralmente é negligenciada.

As redes de fibras que interconectam os data centers sempre foram consideradas imunes a ataques, sem se levar em conta que as comunicações entre data centers geram vulnerabilidade quando os dados confidenciais são enviados de um data center para um dispositivo ou aplicativo em outro data center. Os dados podem atravessar links fora do controle da organização, portanto, eles correm o risco de serem expostos e comprometidos.

As organizações precisam manter os aplicativos e as informações em segurança dentro do data center e enquanto eles trafegam entre data centers. Pode ser difícil projetar, implementar e dimensionar a segurança entre data centers. A criptografia da camada de aplicativos pode proteger as interconexões entre data centers. A criptografia da camada de pacotes também pode ajudar, mas cada tipo tem suas dificuldades próprias. Uma terceira opção mais atrativa é criptografar os dados da rede na camada de redes mais baixa: a camada ótica. A criptografia em massa da camada ótica proporciona escalabilidade de arquitetura e simplicidade de engenharia, além de facilitar a operação e, ao mesmo tempo, oferecer proteção a todos os dados em trânsito (in-flight) que passam entre data centers ou pela nuvem.

É fundamental proteger as redes entre data centers

Um estudo recente revelou que cerca de uma em quatro organizações pode vir a sofrer uma violação de dados de grande escala nos próximos 24 meses.[1] Os custos relacionados a isso podem chegar a milhões de dólares, pois as vítimas precisam ser identificadas e notificadas. Além disso, todas as multas legais e regulatórias devem ser pagas. Depois da violação, ainda pode haver outros custos decorrentes

A criptografia de camada 1 permite:

- Rendimento completo sem congestão do tráfego
- Latência ultrabaixa, criptografia de alto desempenho para comunicações entre data centers altamente seguras
- Soluções simples de implantar e operar, sem exigir dispositivos de criptografia adicionais
- Criptografia flexível, independente de protocolo, para uma variedade de serviços

1 Ponemon Institute, "2017 Cost of Data Breach Study" (Estudo do custo da violação de dados em 2017), Relatório de pesquisa do Ponemon Institute (junho de 2017), 1-2

da perda de receita e clientes e dos danos à reputação da organização.

A legislação está cada vez mais rigorosa em relação à identificação e à notificação em casos de violações de segurança. Dependendo dos tipos de dados ou registros transportados, a criptografia pode ser exigida por lei. As empresas estão sujeitas a multas regulatórias pesadas quando os dados confidenciais são comprometidos, o que pode afetar a lucratividade geral do negócio.

Formulação de uma nova mentalidade sobre segurança

Ao considerar a segurança, as organizações devem adotar uma nova mentalidade, presumindo que a violação pode e vai ocorrer. Não convém supor que as defesas manterão os adversários do lado de fora da rede. Na verdade, as empresas devem assumir que os invasores já entraram ou entrarão nela em breve. Assumindo a ideia de que a violação é uma possibilidade real, as empresas poderão criar defesas para proteger os dados sempre, em vez de tentar projetar um sistema invulnerável ou se preocupar em proteger os dados depois que o sistema tiver sido comprometido. Por exemplo, as organizações podem criptografar os dados em trânsito na rede, assim, os invasores não conseguem ler dados in-flight, mesmo que possam capturá-los.

Para que o ataque seja eficiente, é necessário que alguns componentes estejam presentes ao mesmo tempo. Deve haver um sistema vulnerável com alguma fragilidade, como um software sem patches. Ele deve ter valor para o invasor e ser acessível. Nesse caso, se o invasor estiver munido das ferramentas e das técnicas certas, poderá ocorrer uma violação.

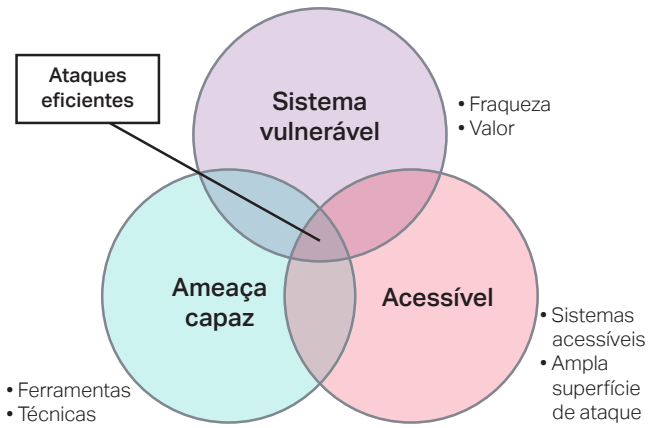

Figura 1. Componentes de um ataque eficiente

Para formular uma estratégia de defesa, as organizações devem seguir três etapas: identificar os ativos, definir o acesso e entender as ameaças. Ao identificar os ativos, as organizações devem saber quais deles são importantes (como dados e arquivos confidenciais) e como eles são protegidos e acessados. Os dados dentro do banco de dados podem estar seguros graças às proteções aplicadas nele, mas se esses dados forem exportados do banco de dados e migrados dentro da rede, talvez eles não estejam mais protegidos. Por exemplo, se o RH exportar dados para o Excel ao gerar relatórios, os backups da planilha que migram não criptografados de um data center para outro não estão seguros.

Adição de criptografia de rede para uma estratégia de segurança abrangente

Como parte de uma estratégia de segurança abrangente, nunca foi tão importante proteger todos os dados entre data centers, incluindo a nuvem. Nenhuma parte da rede deveria ser considerada invulnerável a invasões, e não se deve negligenciar os dados em trânsito. Para garantir a confidencialidade dos dados, as empresas devem adotar uma abordagem de segurança de TI ampla, que tenha um modo eficiente e escalável de proteger os dados em trânsito na nuvem.

Tradicionalmente, as organizações de TI associam segurança à segurança no local, que inclui elementos como segurança física nos pontos de entrada do data center e acesso restrito a servidores e equipamentos. Firewalls, sistemas de prevenção contra invasão, criptografia de disco cheio, proteção de aplicativos e bancos de dados, controles de acesso baseados em função e outros elementos de segurança protegem e criptografam os repositórios de dados essenciais. No entanto, quando os dados vão além dessas paredes seguras ou estão trafegando entre data centers, eles ficam vulneráveis a ataques e violações. Para complicar ainda mais, os dados que atravessam redes de terceiros ou de vários provedores de serviços talvez não estejam sob controle total de uma única organização, logo, é mais difícil garantir que eles estejam seguros.

A criptografia pode ser usada para proteger dados in-flight que transitam entre data centers, mas há uma variedade de soluções a serem consideradas. Cada solução de criptografia tem seus próprios benefícios e desafios, e a melhor solução deve ser fácil de implantar e gerenciar, além de altamente escalável e eficiente.

Segurança da camada de aplicativos ou da infraestrutura de rede?

Ao implementar uma solução de criptografia, as organizações de TI geralmente tentam proteger a camada de aplicativos ou usar a criptografia incorporada à infraestrutura de rede. A segurança da camada de aplicativos requer a proteção do dispositivo de host e do aplicativo. Por isso, a maioria das estruturas de segurança da camada de aplicativos fica dentro do data center. Além disso, soluções como o protocolo TLS (Transport Layer Security), que protege as comunicações entre aplicativos (como navegadores da

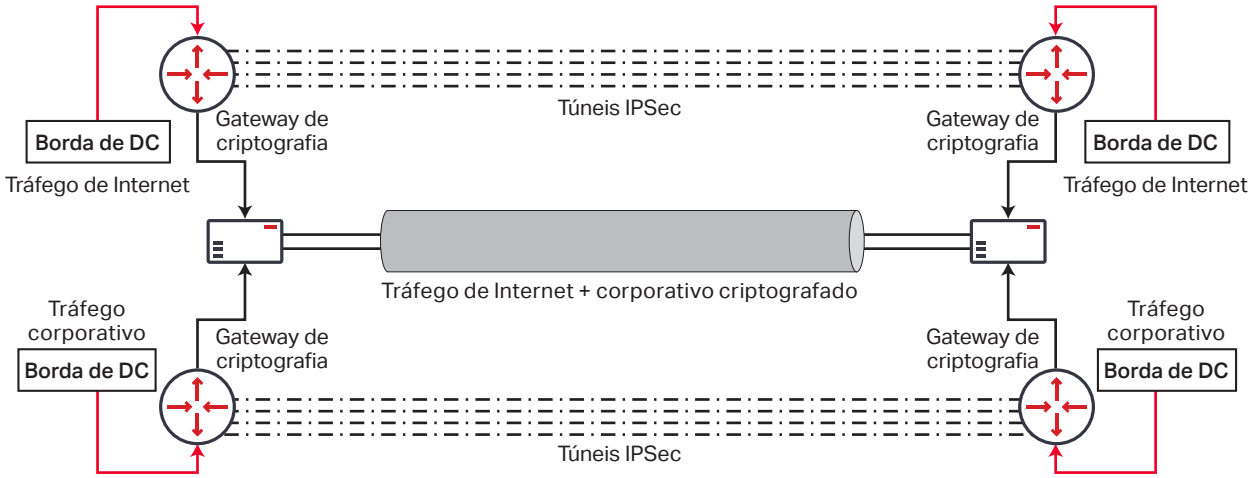

Figura 2. Proteção de todo o tráfego na camada de pacotes com um overlay (visão lógica)

Web ou clientes de e-mail) e servidores, normalmente não lidam com a segurança de aplicativo para aplicativo nas comunicações pela nuvem ou entre data centers. Como é complicado criar uma estrutura comum para segurança de aplicativo para aplicativo entre vários data centers, as organizações costumam recorrer à infraestrutura de rede como solução.

O uso da infraestrutura de rede introduz dificuldades próprias, e a proteção da rede na camada de infraestrutura pode resultar em uma arquitetura de rede altamente complexa. Os fluxos de tráfego entre data centers são muito grandes, logo, a proteção de todo o tráfego entre várias conexões de 100G+ pode ser complexa em termos operacionais, difícil de projetar e dimensionar.

Uma opção é usar um overlay de gateways de VPN criptografados para proteger todo o tráfego na camada de pacotes (Figura 2). Esse procedimento requer equipamentos de gateway de criptografia especializados de alto custo em cada link que precisa de proteção. Esse modelo limita o tráfego a um único par de IP de origem/destino, e as informações do cabeçalho IPsec mais externo não estão disponíveis para os roteadores intermediários em caminhos de nós múltiplos. Esse método de overlay não permite a variabilidade de tráfego e interrompe os caminhos de ECMP (Equal Cost Multi-Path) e LAG (Link Aggregation Group). Além disso, ele não dimensiona com eficiência e aumenta a latência. À medida que os requisitos de largura de banda aumentam e os fluxos de dados ficam mais entrelaçados na malha, portas com taxas mais altas são necessárias nos gateways criptografados, o que leva a um aumento de custos substancial.

As principais desvantagens de usar um overlay de gateways de VPN criptografados para proteger a nuvem são:

- Arquitetura, design e engenharia de rede complexos
- Requer habilidades especializadas para operação e gerenciamento de tráfego entre data centers
- Muito difícil de dimensionar
- Introduz latência adicional entre data centers
- Técnicas de criptografia de camada de pacotes reduzem o rendimento de pacotes geral
- Monitoramento, solução de problemas e outros desafios operacionais
- Alto custo dos equipamentos de gateway criptografados

Como mencionado antes, à medida que o tráfego aumenta, portas de taxa mais alta são necessárias no gateway de criptografia. É difícil dimensionar esta arquitetura baseada em pacotes, e os dispositivos de criptografia se tornam muito grandes, caros e têm dificuldade em fornecer rendimento total nos links criptografados entre data centers. Para superar este desafio de escalabilidade e reduzir o custo dos equipamentos de gateway criptografados especializados com cargas de tráfego maiores, as organizações podem tentar criar o perfil do tráfego. Depois disso, é possível dividir o tráfego entre caminhos criptografados e não criptografados por gateways criptografados ou não criptografados conforme necessário (Figura 3). Essa é uma tentativa de reduzir problemas de escalabilidade no gateway criptografado enviando o tráfego que requer criptografia para o gateway criptografado e descarregando o tráfego restante para outros gateways não criptografados.

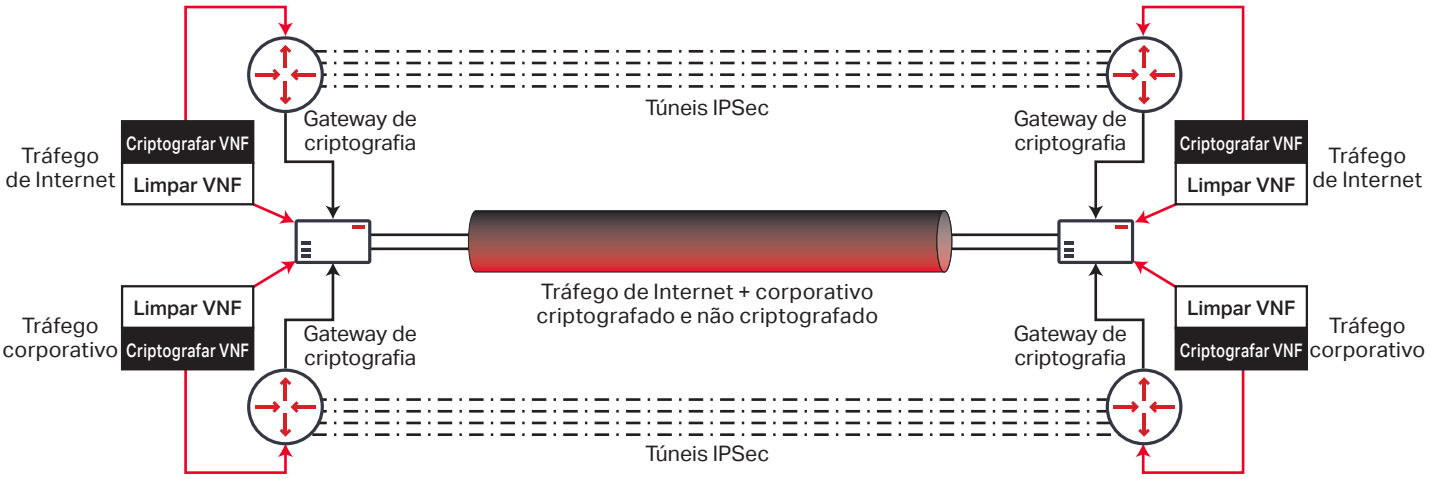

Figura 3. Criação de perfil de tráfego para reduzir o custo do gateway de criptografia (visão lógica)

No entanto, a criação de perfil do tráfego também tem desafios. Pode ser complicado identificar com precisão se o tráfego deve ser criptografado. Poucas organizações conhecem seus próprios dados tão bem a ponto de separá-los, e identificar o tráfego incorretamente pode deixar dados confidenciais desprotegidos. Os propósitos e os parâmetros dos aplicativos são atualizados com frequência. Se o perfil do tráfego não for mantido em sincronia com essas mudanças, isso pode levar à transmissão de dados confidenciais pelas rotas não protegidas.

As principais desvantagens de usar a criação de perfil de tráfego com gateways criptografados e não criptografados são:

- Arquitetura, design e engenharia de rede complexos
- Requer habilidades especializadas para operação e gerenciamento de tráfego entre data centers
- Alta taxa de erros na criação de perfil de tráfego como criptografado versus não criptografado
- Os perfis de aplicativos e os perfis de tráfego devem ser consistentes e estar em sincronia conforme os usos do aplicativo mudam com o tempo
- É complexo projetar e implementar instâncias de roteamento Normal/Não criptografado e Criptografado no hardware da rede
- Introduz latência adicional entre data centers
- Técnicas de criptografia de camada de pacotes reduzem o rendimento de pacotes geral
- Alto custo dos equipamentos de gateway criptografados

É um enorme desafio dimensionar uma criação de perfil de tráfego dessa natureza para um nível global, assim como é difícil fazer a manutenção. Os perfis de tráfego para aplicativos e fontes de dados novos e existentes devem ser atualizados com diligência, para garantir a proteção do tráfego. A integração estreita e constante entre desenvolvedores de aplicativos, engenheiros de segurança e administradores de sistema e rede devem ser garantidos para que a criação do perfil de tráfego tenha êxito.

Os dois métodos de criptografia da camada de pacotes têm suas desvantagens em relação a escalabilidade e complexidade de implementação. Felizmente, existe uma nova opção para reduzir a complexidade e melhorar a escalabilidade criptografando o tráfego in-flight na camada ótica.

Soluções de segurança de dados 24/7

Criptografia da camada ótica: uma abordagem simples

Em vez de gastar recursos para criar perfis e segregar o tráfego para proteger somente dados confidenciais, as organizações estão cada vez mais recorrendo à camada ótica para soluções de criptografia que são fáceis de implementar e, ao mesmo tempo, oferecem proteção para todos os dados. A criptografia na Camada 1 ou na camada ótica faz justamente isso. Ela criptografa toda a carga útil de OTN, protegendo todas as mensagens, cabeçalhos e dados das comunicações da camada superior (Figura 4).

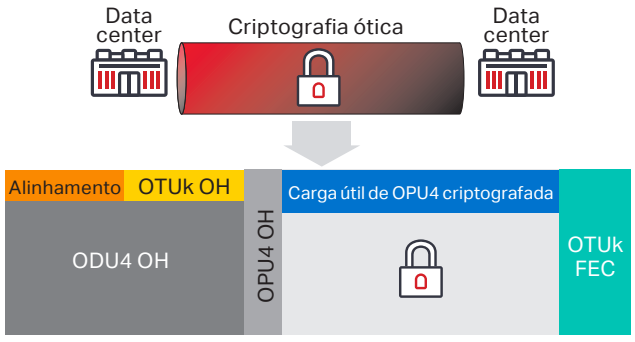

Figura 4. Proteção de TODO o tráfego com a criptografia de Camada 1

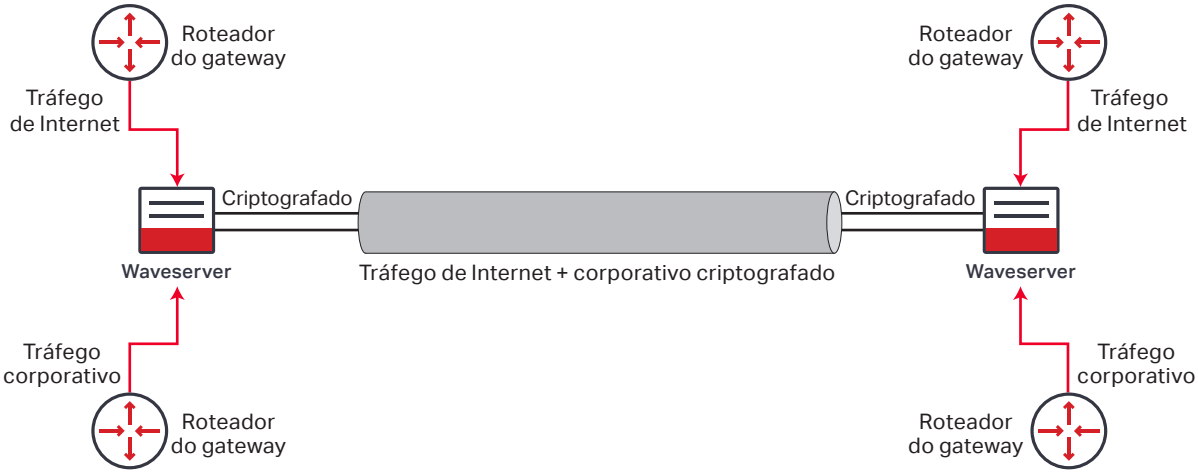

Figura 5. Proteção de todo o tráfego na camada ótica (visão lógica)

A criptografia na camada ótica simplifica a arquitetura de rede (Figura 5). Os roteadores de gateway enviam o tráfego diretamente ao dispositivo de transporte (nesse caso, o Waveserver®) para criptografia em massa. Os gateways de criptografia caros não são necessários, e não é necessário criar perfil de tráfego para identificar qual tráfego deve ser criptografado. *Todo o tráfego que sai do data center passa por criptografia de alto desempenho com rendimento total.*

A criptografia de Camada 1 oferece estes benefícios:

- **Nenhum requisito adicional de VPN para criptografar o tráfego:** como a criptografia de Camada 1 fornece uma solução para criptografar todo o tráfego, não há necessidade de criar o perfil do tráfego para enviar VPNs criptografadas e não criptografadas. Todas as comunicações são seguras.
- **Latência:** a execução da criptografia na Camada 1 adiciona nanossegundos a microssegundos de latência, enquanto as soluções de camadas mais altas, como IPsec ou criptografia de camada de aplicativo, podem adicionar centenas de milissegundos de latência.
- **Rendimento total:** somente a carga útil da camada de transporte é criptografada, então o rendimento da camada de pacotes nas rotas e nos switches não é afetado. As soluções de criptografia de alto desempenho de Camada 1 oferecem rendimento completo quando o tráfego é criptografado.
- **Simples de criar, projetar e operar:** as soluções de criptografia de Camada 1 são criadas nos mesmos sistemas de transporte ótico usados para transmissão de DWDM na rede metropolitana ou de longa distância. Nenhum dispositivo de criptografia adicional é necessário.
- **Suporte multiprotocolo:** a Camada 1 oferece suporte a vários tipos de tráfego, incluindo Ethernet, IP, SONET/SDH, Fibre Channel e muito mais, reduzindo o número de dispositivos de criptografia necessários e aumentando o suporte a protocolo em relação a opções como o IPSec, que é limitado a um único protocolo (IP).

A migração para a criptografia da Camada 1 é uma solução simples para proteger a nuvem. Ela permite a criptografia em massa de todos os dados in-flight que passam pelo link protegido. A criptografia de Camada 1 tem outra vantagem: ela pode ser usada como depósito (catch-all) na camada inferior. As organizações de segurança ainda podem desenvolver e projetar soluções de criptografia da camada superior para regulamentações ou como parte de um plano de segurança mais abrangente se necessário ou desejado. Mas se houver comprometimento da camada superior, os dados ainda serão criptografados na camada ótica. As organizações têm a opção de projetar um plano de segurança abrangente ou inserir a criptografia de Camada 1 como catch-all, dependendo de onde elas estejam desenvolvendo sua política de segurança global.

Solução WaveLogic Encryption da Ciena

A Ciena oferece criptografia de Camada 1 para garantir que os dados fiquem protegidos com algoritmos de criptografia AES-256, em vez de transitarem desprotegidos e expostos entre links. Além disso, se um adversário obtiver acesso ao meio físico e tentar tocar na fibra, todos os dados serão criptografados e ficarão inutilizáveis.

O WaveLogic Encryption da Ciena é uma solução de criptografia ótica de alto desempenho, simples de implementar, integrada aos equipamentos de redes de transporte ótico. Com a abordagem "configure e esqueça", a criptografia está sempre ativa, garantindo que todos os dados em trânsito sejam protegidos, o tempo todo. Isso elimina qualquer erro humano que possa levar ao envio de dados confidenciais pela rede não criptografada.

A solução da Ciena oferece um mecanismo de criptografia AES-256 certificado pela FIPS, com suporte aos algoritmos de criptografia de chave pública mais recentes, como o ECC (Elliptic Curve Cryptography). O WaveLogic Encryption está disponível na Plataforma de Pacotes Óticos 6500 da Ciena e na família Waveserver da Ciena de plataformas interconectadas empilháveis, utilizando interfaces WDM

coerentes que podem ser programadas para fornecer criptografia de alto desempenho em uma variedade de taxas de linha, como: QPSK de 100G, 8QAM de 150G, 16QAM de 200G e portadora única 400G.

Com o Ciena 6500, as operadoras podem utilizar uma solução de placa baseada em muxponder completa para criptografia de 10G ou um par de módulo de linha 100G/200G com criptografia para uma placa de interface de cliente, tendo flexibilidade para atender a necessidades de tráfego específicas. As operadoras podem utilizar o Waveserver para implantar até 400G de capacidade de criptografia de alto desempenho de AES-256 em apenas 1 RU, com a flexibilidade de suporte a uma variedade de clientes de 10GE, 40GE e 100GE no mesmo dispositivo. Com o Waveserver Ai, que é otimizado para interfaces de cliente de 100GE, as operadoras podem implantar até 1,2 TB de capacidade criptografada em uma única unidade de rack.

A programabilidade de linha incorporada no transporte coerente da Ciena permite que as operadoras otimizem a capacidade de linha para os requisitos de qualquer aplicativo e para proteger os dados in-flight nas redes metropolitanas, regionais ou de longa distância. Isso permite proteger a conectividade entre data centers, seja qual for a distância ou o sistema de linha fotônico subjacente em uso.

O 6500 e o Waveserver podem ser implantados para proteger a nuvem sem a complexidade associada a soluções de aplicativos de nível mais alto ou de infraestrutura baseada em IP. Conforme mais informações sigilosas são distribuídas entre as redes de fibra ótica e mais leis e regulamentações exigem a segurança de dados, as comunicações atuais baseadas na nuvem devem implantar uma abordagem de segurança de TI que inclua não apenas segurança de servidor e criptografia em repouso, mas também uma solução avançada de criptografia in-flight.

Criptografia sem esforço. Saiba mais.

Conclusão

A implementação de um plano de segurança abrangente pode ser difícil, principalmente ao considerar as comunicações de aplicativo para aplicativo entre data centers. As organizações geralmente buscam a infraestrutura de rede para fornecer um meio de proteger os dados que passam entre data centers. No entanto, o fornecimento de criptografia de rede na Camada 3 pode ser caro e difícil de dimensionar. Felizmente, a criptografia da camada ótica oferece uma defesa de primeiro nível e é simples de implementar. Ela é independente de protocolo e comporta uma variedade de tipos de tráfego. Ela oferece criptografia de alto desempenho sem redução de rendimento sob cargas pesadas e não introduz quase nenhuma latência adicional. A criptografia da Camada 1 é uma maneira econômica de proteger dados em trânsito conforme eles trafegam entre data centers, e a solução WaveLogic Encryptionn da Ciena concilia alto grau de flexibilidade e segurança com facilidade de operação e administração. Ela permite a criptografia de alto desempenho, alta capacidade e econômica para proteger as comunicações entre os data centers o tempo todo, na rua, na cidade, no país ou no oceano.

Faça suas perguntas na Comunidade da Ciena