ciena
Experience. Outcomes.

NOTE D'APPLICATION

Sécuriser le cloud

Simplifier la sécurité entre les data centers grâce au chiffrement de couche 1

Il est fondamental de protéger les données sensibles ou critiques afin de préserver la propriété intellectuelle et les dossiers confidentiels, et d'éviter des amendes coûteuses et la perte de revenu liées à la violation des données. Il est parfois difficile de déterminer les données qui doivent être protégées et la manière de les protéger. La conception physique du data center prévoit plusieurs couches de mécanismes physiques de sécurité pour empêcher tout accès non souhaité. Par ailleurs, pare-feu, anti-virus et techniques de détection d'intrusion peuvent être utilisés pour sécuriser les données à l'intérieur du data center. En revanche, une fois que les informations ont quitté l'enceinte sécurisée du data center, on se soucie souvent peu de les protéger.

Les réseaux de fibre optique qui relient les data centers ont souvent été considérés comme inattaquables, mais le fait d'ignorer les communications entre data centers rend les données sensibles vulnérables, en particulier lorsque celles-ci sont envoyées d'un data center vers une application ou un appareil situés dans un autre centre. Les données peuvent traverser des liaisons échappant au contrôle de l'organisation et ainsi risquer d'être exposées et compromises.

Les organisations doivent préserver la sécurité de leurs applications et informations à l'intérieur de leur data center et pendant leur acheminement d'un data center à l'autre. Il peut s'avérer difficile de concevoir, mettre en œuvre et faire évoluer la sécurité entre les data centers. Un chiffrement au niveau de la couche d'application permet de sécuriser les interconnexions de data centers. Un chiffrement au niveau de la couche paquet peut lui aussi s'avérer utile, mais chaque type présente son lot de difficultés. Une troisième option, plus séduisante, consiste à chiffrer les données de réseau au niveau de la couche la plus basse du réseau : la couche optique. Le chiffrement de masse au niveau de la couche optique offre évolutivité architecturale, simplicité de conception et facilité de fonctionnement, tout en protégeant l'ensemble des données en transit dans le cloud ou entre les data centers.

Il est fondamental de sécuriser les réseaux entre les data centers

Selon une étude récente, une organisation sur quatre pourrait être confrontée à une violation massive de ses données au cours des 24 prochains mois[1]. Les coûts associés à ces violations peuvent se chiffrer en millions de dollars, car les victimes doivent être identifiées et avisées et qu'il convient d'acquitter l'ensemble des frais juridiques et réglementaires associés. De plus, lorsqu'une violation a lieu, des

1 Ponemon Institute, « 2017 Cost of Data Breach Study » (Étude 2017 sur le coût de la violation des données), rapport de recherche du Ponemon Institute (juin 2017), 1-2

Le chiffrement de couche 1 offre :

- Un plein débit sans congestion du trafic.
- Un délai de transit extrêmement faible, un chiffrement hautes performances pour des communications hautement sécurisées entre les data centers.
- Des solutions faciles à déployer et à exploiter, n'impliquant l'utilisation d'aucun autre dispositif de chiffrement.
- Un chiffrement flexible, indépendant du protocole pour une multitude de services.

coûts supplémentaires peuvent être engendrés par la perte de revenus ou de clients et par l'atteinte à la réputation de l'organisation.

La législation exige de plus en plus des mesures plus strictes d'identification et de notification en cas de brèche dans la sécurité. Selon le type de données ou de dossiers transférés, certaines réglementations peuvent exiger le chiffrement des données. Les entreprises s'exposent à être condamnées à payer de lourdes amendes administratives si des données sensibles ont été compromises, ce qui peut porter préjudice à la rentabilité générale de l'organisation.

Adopter un nouvel état d'esprit en matière de sécurité

En matière de sécurité, un changement de mentalité est nécessaire au sein des organisations : il faut partir du principe qu'une violation peut se produire et qu'elle se produira. Il ne faut pas présumer que les mécanismes de défense mis en place suffiront à maintenir hors du réseau toutes les menaces. Les entreprises doivent au contraire accepter la réalité : les attaques ont déjà eu lieu ou sont imminentes. En acceptant cet état de fait, les entreprises peuvent concevoir des moyens de défense qui leur permettront de protéger leurs données en toute circonstance plutôt que d'essayer de créer un système imperméable ou de se préoccuper de la protection des données une fois le système compromis. Les organisations peuvent par exemple chiffrer les données en transit dans le réseau, de sorte qu'il soit impossible aux personnes attaquant le réseau de lire les données à la volée, même si elles parviennent à les saisir.

Pour qu'une attaque réussisse, quelques facteurs déterminants doivent être réunis. Il faut un système vulnérable présentant certaines faiblesses, par exemple un logiciel qui n'a pas été mis à jour. Le système doit avoir une certaine valeur pour l'auteur de l'attaque et il doit être accessible. Dans ce cas, si l'auteur de l'attaque dispose des outils et techniques adéquats, une violation est plausible.

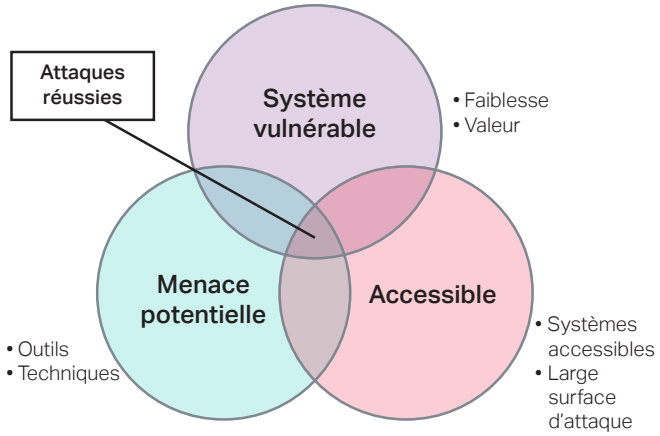

Figure 1. Composants d'une attaque réussie

Les organisations articuleront leur stratégie de défense autour de trois axes : identifier leurs actifs, déterminer l'accès et comprendre les menaces pesant sur eux. Concernant l'identification des actifs, les organisations doivent pouvoir déterminer ceux qui sont importants, notamment les données et dossiers confidentiels, et la manière dont ils sont protégés et accessibles. Les données présentes dans une base de données peuvent être sécurisées au moyen des protections appliquées à la base de données, mais si ces données sont exportées depuis la base, puis déplacées d'un endroit à l'autre dans le réseau, il est possible qu'elles ne soient plus sécurisées. Par exemple, si un service RH exporte des données dans Excel pour établir des rapports, les copies de sauvegarde de la feuille de calcul déplacées sans être chiffrées d'un data center vers un autre ne sont pas sécurisées.

Ajouter un chiffrement réseau pour une stratégie de sécurité globale

Dans le cadre d'une stratégie de sécurité globale, la protection de l'ensemble des données entre les data centers, y compris le cloud, n'a jamais été aussi essentielle. Aucune portion du réseau n'est à l'abri des pirates informatiques, et il convient de tenir compte des données en transit. Pour assurer la confidentialité des données, les entreprises doivent adopter une approche globale de la sécurité au niveau informatique, prévoyant des moyens efficaces et évolutifs pour sécuriser les données qui transitent par le cloud.

Généralement, les organisations TIC ont associé la sécurité à la sécurité sur site, ce qui inclut des éléments tels que la sécurité physique aux points d'entrée du data center et un accès restreint aux serveurs et équipements. Les pare-feu, les systèmes de prévention des intrusions, le chiffrement complet du disque, le renforcement des applications et bases de données, les contrôles d'accès basés sur les rôles et d'autres éléments de sécurité protègent et chiffrent les référentiels de données critiques. Toutefois, lorsque les données quittent ces enceintes sécurisées ou transitent entre les data centers, elles sont exposées aux attaques et aux violations. Le problème est encore aggravé par le fait que les données qui traversent des réseaux tiers ou plusieurs réseaux de prestataires de services ne sont pas toujours sous le contrôle d'une seule et même organisation, de sorte qu'il devient encore plus difficile d'en assurer la sécurité.

Un chiffrement peut être utilisé pour protéger les données en transit entre les data centers, mais les solutions à envisager sont nombreuses. Chaque solution de chiffrement comporte son lot d'avantages et de difficultés, et la solution la meilleure doit être une solution facile à déployer et à gérer, évolutive et efficace.

Sécurité de la couche d'application ou de l'infrastructure réseau ?

Lorsqu'elles mettent en œuvre une solution de chiffrement, les organisations TIC ont pour habitude d'essayer de protéger la couche applicative ou d'utiliser un dispositif de chiffrement intégré à l'infrastructure réseau. La sécurité de la couche applicative implique de protéger à la fois l'appareil

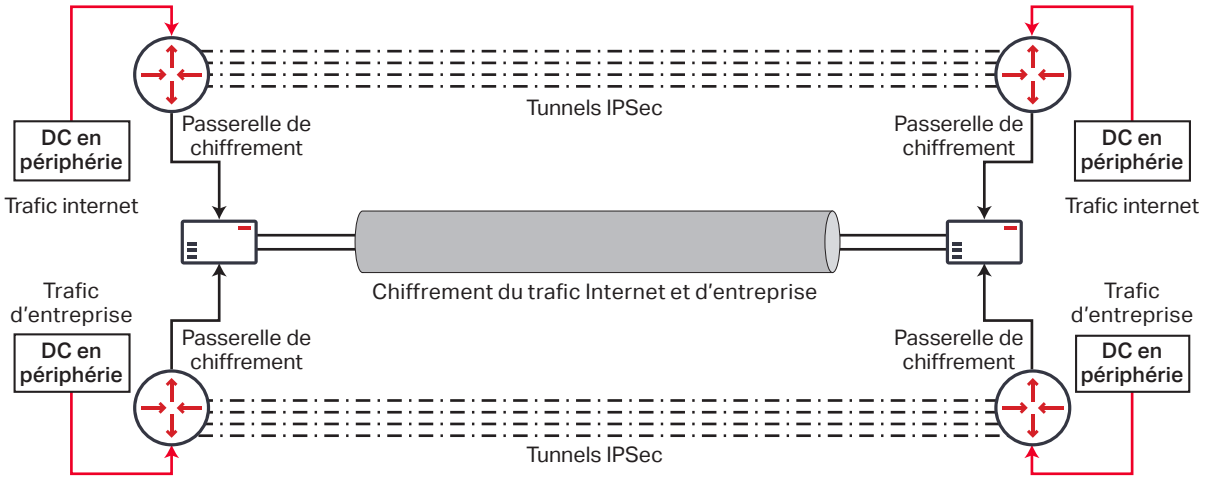

Figure 2. Sécurisation de l'ensemble du trafic au niveau de la couche paquet avec superposition (vue logique)

hôte et l'application, c'est pourquoi la plupart des cadres de sécurité de la couche applicative se trouvent dans le data center. De plus, des solutions, telles que la TLS (Transport Layer Security) qui sécurise les communications entre applications (p. ex. : navigateurs Web ou clients e-mail) et serveurs, ne sont généralement pas conçues pour assurer la sécurité entre les applications dans le cadre des communications via le cloud ou entre data centers. Il peut être difficile de mettre en place un cadre commun de sécurité entre applications à l'échelle de plusieurs data centers, c'est pourquoi les organisations envisagent souvent une solution au niveau de l'infrastructure réseau.

L'utilisation de l'infrastructure réseau induit son propre lot de difficultés et la protection du réseau au niveau de la couche d'infrastructure peut contribuer à une architecture réseau particulièrement complexe. Le trafic entre les data centers est très dense, et la sécurisation de l'ensemble du trafic résultant de multiples connexions 100G+ peut s'avérer fastidieuse d'un point de vue opérationnel et difficile à concevoir et à faire évoluer.

L'une des options possibles consiste à recourir à une superposition de passerelles VPN chiffrées pour sécuriser le trafic au niveau de la couche paquet (cf. figure 2). La démarche nécessite l'utilisation d'un équipement plus coûteux de passerelles de chiffrement sur chaque liaison à protéger. Ce modèle limite le trafic à une seule paire d'IP source/destination, et les informations d'en-tête IPsec externe ne sont pas accessibles aux routeurs intermédiaires pour les trajets multi-sauts. Cette méthode de superposition ne permet pas la variabilité du trafic et rompt les trajets ECMP (Equal Cost Multi-Path) et LAG (Link Aggregation Group). De plus, elle ne peut pas évoluer efficacement et elle augmente le délai de transit. À mesure que les exigences en bande passante augmentent et que les flux de données sont de plus en plus maillés, des ports à débit supérieur sont nécessaires sur les passerelles chiffrées, ce qui fait grimper sensiblement la facture.

Parmi les inconvénients majeurs liés à une superposition de passerelles VPN chiffrées pour sécuriser le cloud, citons :

- La complexité de l'architecture, de la conception et de l'ingénierie réseau.
- Les compétences particulières requises pour exploiter et gérer le trafic entre les data centers.
- Une évolutivité très inefficace.
- L'introduction d'un délai de transit supplémentaire entre les data centers.
- Des techniques de chiffrement au niveau de la couche paquet réduisant le débit global des paquets.
- Les difficultés liées à la surveillance, au dépannage et aux opérations.
- Le coût élevé des équipements de passerelles chiffrées.

Comme mentionné précédemment, à mesure que les flux de trafic augmentent, des ports de débit supérieur sont nécessaires sur la passerelle de chiffrement. Cette architecture en paquets évolue difficilement et les appareils de chiffrement deviennent très imposants, très couteux et peinent à fournir un plein débit au niveau des liaisons chiffrées entre les data centers. Pour surmonter ce défi d'évolutivité et réduire le coût des équipements spécialisés de passerelle chiffrée en cas de trafic plus dense, les organisations peuvent tenter d'établir le profil de leur trafic. Une fois le profil établi, le trafic peut être scindé en chemins chiffrés et non chiffrés sur des passerelles elles-mêmes chiffrées ou non, selon les besoins (cf. figure 3). L'objectif est d'atténuer les problèmes d'évolutivité sur la passerelle chiffrée en envoyant le trafic exigeant un chiffrement vers la passerelle chiffrée et en déchargeant le reste du trafic vers des passerelles non chiffrées.

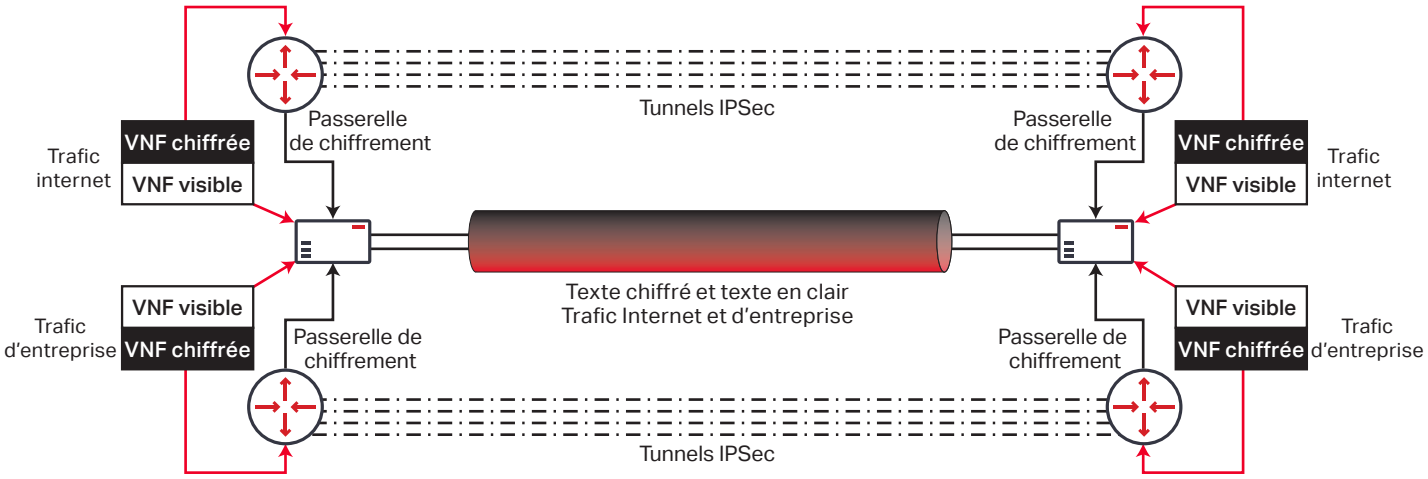

Figure 3. Profilage du trafic pour réduire les coûts de la passerelle de chiffrement (vue logique)

Toutefois, le profilage du trafic suscite lui aussi certaines difficultés. Il est parfois fastidieux de déterminer précisément si le trafic doit être chiffré. Peu d'organisations connaissent leurs propres données suffisamment bien pour les distinguer de manière précise, et si elles ne parviennent pas à identifier correctement le trafic, certaines données sensibles peuvent ne pas être protégées. Les objectifs et paramètres des applications sont souvent mis à jour, et à moins que le profil du trafic soit synchronisé en permanence en fonction de ces modifications, il est possible que des données sensibles soient transmises par des trajets non protégés.

Les inconvénients principaux d'un profilage du trafic selon des passerelles chiffrées et non chiffrées sont notamment :

- La complexité de l'architecture, de la conception et de l'ingénierie réseau.
- Les compétences particulières requises pour exploiter et gérer le trafic entre les data centers.
- Le taux d'erreur élevé (entre chiffré/non chiffré) dans le profilage du trafic.
- Les profils d'applications et de trafic doivent être cohérents et synchronisés, à mesure que l'usage des applications évolue au fil du temps.
- Des instances de routage normal/en clair et chiffré difficiles à concevoir et à mettre en place dans le matériel du réseau.
- L'introduction d'un délai de transit supplémentaire entre les data centers.
- Des techniques de chiffrement au niveau de la couche paquet réduisant le débit global des paquets.
- Le coût élevé des équipements de passerelles chiffrées.

Il est extrêmement difficile de faire évoluer un profilage du trafic à cette nature à un niveau global et de le maintenir à long terme. Les profils de trafic pour les applications nouvelles et existantes et les sources de données doivent être soigneusement mis à jour pour assurer au trafic une sécurité adéquate. Une collaboration étroite et constante entre les développeurs d'applications, ingénieurs sécurité et administrateurs réseau et système doit être assurée pour permettre un profilage efficace du trafic.

Les deux méthodes de chiffrement de la couche paquet présentent certains inconvénients en matière d'évolutivité et de complexité de mise en œuvre. Il existe heureusement une nouvelle option permettant de réduire la complexité et d'améliorer l'évolutivité en chiffrant le trafic en transit au niveau de la couche optique.

Solutions de sécurité des données 24/7

Chiffrement de la couche optique : une approche simple et sûre

Au lieu d'investir des ressources pour profiler et répartir le trafic afin de protéger seulement les données sensibles, les organisations s'intéressent de plus en plus à la couche optique pour trouver des solutions de chiffrement faciles à mettre en place et protégeant toutes les données. C'est exactement ce que réalise le chiffrement au niveau de la couche 1 ou couche optique. Il s'agit d'un chiffrement de l'intégralité de la charge OTN, qui protège l'ensemble des messages, en-têtes et données issus des communications de la couche supérieure (cf. figure 4).

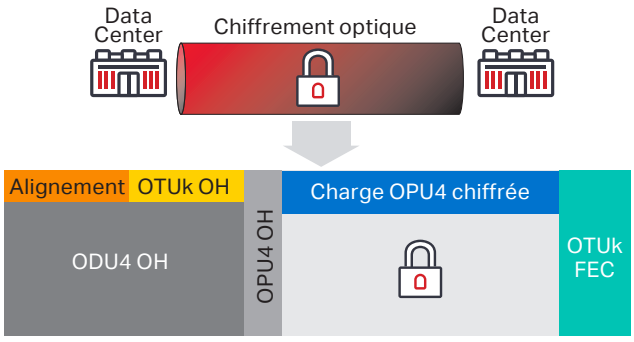

Figure 4. Sécurité de TOUT le trafic assuré par chiffrement en couche 1

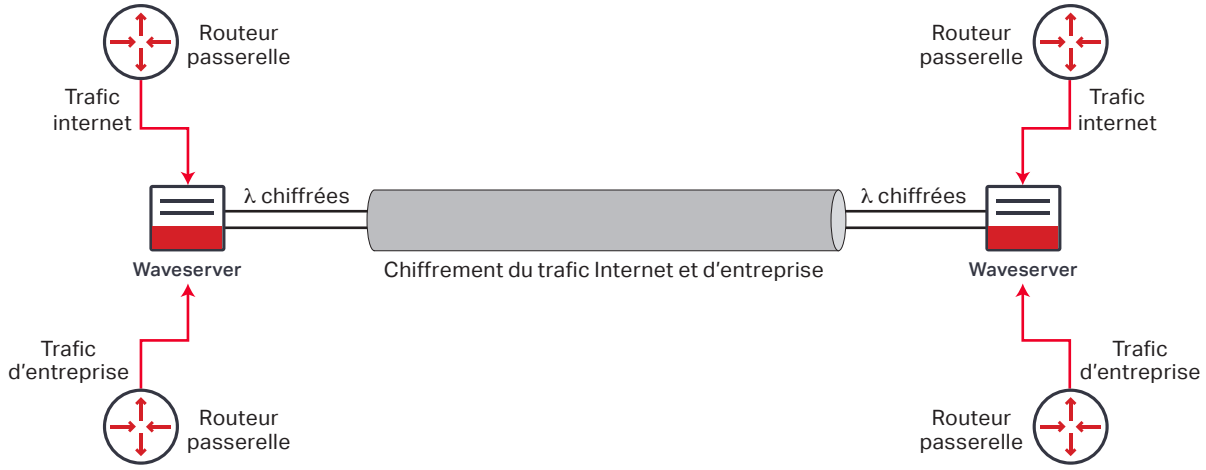

Figure 5. Sécurisation de l'ensemble du trafic au niveau de la couche optique (vue logique)

Le chiffrement au niveau de la couche optique simplifie l'architecture réseau (cf figure 5). Les routeurs de la passerelle envoient le trafic directement à l'appareil de transport (dans ce cas, Waveserver®) pour effectuer un chiffrement de masse. Il n'est pas nécessaire d'investir dans des passerelles de chiffrement coûteuses, et aucun profilage n'est requis pour identifier le trafic à chiffrer. *Tout le trafic qui sort du data center est chiffré à grande vitesse et à plein débit.*

Le chiffrement de couche 1 présente les avantages suivants :

- **Aucune exigence VPN supplémentaire pour chiffrer le trafic —** Comme le chiffrement de couche 1 permet de chiffrer tout le trafic, il n'est pas nécessaire d'établir un profil du trafic avant de le répartir entre VPN chiffrés ou non chiffrés. Toutes les communications sont sûres.
- **Délai de transit négligeable —** Le chiffrement en couche 1 ajoute quelques nanosecondes, voire des microsecondes au délai de transit, tandis que des solutions de couche supérieure telles que l'IPsec ou le chiffrement en couche applicative peuvent lui rajouter des centaines de millisecondes.
- **Plein débit —** Seule la charge de la couche transport est chiffrée, le débit de la couche paquet sur les routeurs et les commutateurs n'est donc pas affecté. Les solutions de chiffrement hautes performances en couche 1 fonctionnent à plein débit lorsque le trafic est chiffré.
- **Simplicité de conception, de construction et d'exploitation —** Les solutions de chiffrement de couche 1 sont mises en place dans les mêmes systèmes de transport optique que ceux utilisés pour assurer la transmission DWDM dans un réseau métropolitain ou à longue portée : aucun appareil de chiffrement supplémentaire n'est requis.
- **Prise en charge de divers protocoles —** La couche 1 peut prendre en charge divers types de trafic, dont Ethernet, IP, SONET/SDH, Fibre Channel et d'autres, réduisant ainsi le nombre et la variété de dispositifs de chiffrement nécessaires et permettant une meilleure prise en charge du nombre de protocoles par rapport à des options telles que IPSec, limité à un seul protocole (IP).

Le passage au chiffrement de couche 1 offre une solution simple pour sécuriser le cloud. Le système permet de chiffrer en masse toutes les données en transit sur la liaison protégée. Le chiffrement de couche 1 présente par ailleurs l'avantage de pouvoir être utilisé comme solution universelle au niveau de la couche inférieure. Les organisations spécialisées dans la sécurité peuvent toujours développer et concevoir des solutions de chiffrement en couche supérieure pour se plier à certaines réglementations ou dans le cadre d'un plan de sécurité plus global si cela est nécessaire ou souhaitable, mais si un risque apparaît sur une couche supérieure, les données seront toujours chiffrées au niveau de la couche optique. Les organisations ont la possibilité de concevoir comme solution universelle soit un plan global soit un verrou de sécurité pour le chiffrement de couche 1, selon le stade d'avancement de leur politique globale de sécurité.

Solution WaveLogic Encryption de Ciena

Ciena offre un chiffrement de couche 1 pour assurer la sécurité des données au moyen d'algorithmes de chiffrement AES-256 au lieu de les faire transiter sur des liaisons non sécurisées et exposées. De plus, même si une personne malveillante avait accès au support physique et tentait de détourner la fibre, l'ensemble des données seraient chiffrées et inutilisables.

WaveLogic Encryption de Ciena offre une solution de chiffrement optique hautes performances, simple à mettre en œuvre et intégrée aux équipements transport optique. Grâce à son approche à réglage unique, le chiffrement est actif en permanence, ce qui assure la protection permanente des données en transit. On évite ainsi toute erreur humaine qui pourrait entraîner l'envoi de données sensibles non chiffrées dans le réseau.

La solution de Ciena offre un moteur de chiffrement AES-256 certifié FIPS, avec la prise en charge des plus récents algorithmes d'encodage à clé publique, y compris ECC (encodage de courbes elliptiques). WaveLogic Encryption est disponible sur le système 6500 Packet-Optical Platform et

sur la gamme Waveserver de plates-formes d'interconnexion empilables de Ciena, qui utilisent des interfaces WDM cohérentes pouvant être programmées pour fournir un chiffrement hautes performances à diverses fréquences de ligne telles que : 100G QPSK, 150G 8QAM, 200G 16QAM, et 400G à simple porteuse.

Avec le 6500 de Ciena, les opérateurs peuvent utiliser une solution tout-en-un par carte à transpondeur multiplexé pour le chiffrement 10G, ou combiner un module de ligne 100G/200G à un chiffrement par carte d'interface client, afin de fournir la flexibilité nécessaire pour satisfaire à des besoins spécifiques en matière de trafic. Les opérateurs peuvent utiliser Waveserver pour déployer jusqu'à 400G de capacité de chiffrement AES-256 hautes performances en format 1RU, avec la flexibilité nécessaire pour prendre en charge un mélange de clients 10GE, 40GE et 100GE sur le même appareil. Avec Waveserver Ai, optimisé pour les interfaces client 100GE, les opérateurs peuvent déployer jusqu'à 1,2 T de capacité de chiffrement dans une seule unité de rack.

La capacité de programmation côté ligne intégrée au transport cohérent de Ciena permet aux opérateurs d'optimiser la capacité de ligne pour toutes les exigences d'application et d'assurer la protection des données en transit, dans un contexte métropolitain, régional ou longue portée. Cela permet de relier en toute sécurité les data centers, indépendamment de la distance ou du système de ligne photonique sous-jacent utilisé.

Le 6500 et Waveserver peuvent tous deux être déployés pour sécuriser le cloud sans la complexité associée aux solutions d'infrastructure sur IP ou par application de niveau supérieur. Comme les informations sensibles sont de plus en plus nombreuses à être distribuées sur les réseaux à fibre optique et que de plus en plus de lois et réglementations exigent la sécurité des données, les communications sur le cloud d'aujourd'hui doivent déployer une approche de sécurité informatique qui englobe non seulement la sécurité du serveur et le chiffrement au repos, mais aussi une solution robuste de chiffrement à la volée.

Un chiffrement sans effort. En savoir plus.

Conclusion

Déployer un plan de sécurité global représente souvent un réel défi, en particulier en ce qui concerne les communications d'une application à une autre entre data centers. Les organisations considèrent souvent l'infrastructure réseau pour sécuriser les données transitant entre les data centers. Toutefois, un chiffrement réseau de couche 3 peut être coûteux et difficile à faire évoluer. Le chiffrement de la couche optique offre heureusement une défense de premier niveau. Il est également simple à mettre en œuvre. Il est indépendant du protocole et peut prendre en charge divers types de trafics. Il assure un chiffrement hautes performances sans toutefois réduire le débit en cas de trafic intense, et n'introduit pratiquement aucun délai de transit supplémentaire. Le chiffrement de couche 1 constitue un moyen de protection rentable des données en transit entre des data centers, et la solution WaveLogic Encryption de Ciena allie un haut niveau de flexibilité et de sécurité à une simplicité de fonctionnement et d'administration. Cette solution assure un chiffrement hautes performances de capacité supérieure économique, garantissant à tout moment la sécurité des communications entre les data centers, lors de leur traversée de la rue, de la ville, du pays ou des océans.

La Communauté Ciena
Trouvez les réponses à vos questions