ciena
Experience. Outcomes.

ANWENDUNGSNOTIZ

Die Sicherung der Cloud

Vereinfachung der Sicherheit zwischen Rechenzentren mit Verschlüsselung auf Layer 1

Die Sicherung sensibler oder unternehmenswichtiger Daten ist unerlässlich, um geistiges Eigentum und vertrauliche Daten zu schützen und kostspielige Bußgelder und Umsatzeinbußen aufgrund von Datenschutzverletzungen zu vermeiden. Es kann eine Herausforderung sein, zu bestimmen, welche Daten geschützt werden müssen und wie sie geschützt werden können. Das Design von Rechenzentren umfasst verschiedene Layer physischer Sicherheitsmaßnahmen, um ungewollten Zugang zu verhindern; Firewalls, Anti-Virus- sowie Intrusion-Detection-Systeme können zur Sicherung der Daten innerhalb des Rechenzentrums eingesetzt werden. Sobald die Daten jedoch die sicheren Grenzen des Rechenzentrums verlassen, wird ihre Sicherheit oft vernachlässigt.

Glasfasernetzwerke zur Verbindung von Rechenzentren wurden lange als nicht angreifbar angesehen, doch lässt man die Kommunikation zwischen Rechenzentren außer Acht, dann entstehen Angriffsflächen, sobald sensible Daten von einem Rechenzentrum zu Geräten oder Applikationen in einem anderen Rechenzentrum übertragen werden. Daten können über Verbindungen übertragen werden, die außerhalb der Kontrolle der eigenen Organisation liegen, und so möglicherweise an die Öffentlichkeit gelangen oder angegriffen werden.

Organisationen müssen ihre Anwendungen und Daten sowohl innerhalb des Rechenzentrums als auch bei der Übertragung schützen. Die Architektur, Implementierung und Skalierung von Sicherheitsmaßnahmen zwischen Rechenzentren kann eine Herausforderung sein. Durch die Verschlüsselung des Applikations-Layers kann die Verbindung zwischen Rechenzentren gesichert werden. Die Verschlüsselung auf dem Packet-Layer ist ebenfalls sinnvoll, jedoch können bei beiden Fällen Probleme auftreten. Eine dritte, attraktivere Option ist die Verschlüsselung von Netzwerkdaten auf dem untersten Layer – dem optischen Layer. Die Blockverschlüsselung des optischen Layers ermöglicht eine skalierbare Architektur, eine problemlose technische Umsetzung sowie einen einfachen Betrieb und bietet während der Übertragung Schutz für alle Daten, die zwischen Rechenzentren oder über die Cloud übertragen werden.

Die Sicherung der Netzwerke zwischen Rechenzentren ist von höchster Bedeutung

Eine jüngst durchgeführte Studie hat ergeben, dass ungefähr jede vierte Organisation innerhalb der nächsten 24 Monate einer weitreichenden Datenschutzverletzung zum Opfer fallen könnte.[1] Die durch solche Datenschutzverletzungen entstehenden

Die Layer 1-Verschlüsselung ermöglicht:

- Vollen Durchsatz ohne Datenstau
- Wire-Speed-Verschlüsselung mit extrem niedriger Latenzzeit für hochsichere Kommunikation zwischen Rechenzentren
- Lösungen, die einfach zu implementieren und betreiben sind und keine zusätzlichen Verschlüsselungs-anwendungen erfordern
- Flexible, protokoll-agnostische Verschlüsselung für eine Vielzahl an Services

1 Ponemon Institute, „2017 Cost of Data Breach Study", Ponemon Institute Research Report (Juni 2017), 1-2

Kosten können in Millionenhöhe liegen, denn die Opfer müssen ermittelt und benachrichtigt werden, und alle damit verbundenen Anwalts- und Gerichtskosten müssen gezahlt werden. Zusätzlich können bei einer Datenschutzverletzung weitere Kosten durch den Verlust von Umsätzen und Kunden entstehen, und der Ruf der Organisation kann geschädigt werden.

Die Rechtsvorschriften zur Erkennung und Meldung von Datenschutzverletzungen werden immer strenger. Je nach Art der übermittelten Informationen oder Datensätze gelten unterschiedliche Rechtsvorschriften bezüglich der Datenverschlüsselung. Unternehmen müssen mit erheblichen Bußgeldern rechnen, wenn sensible Daten angegriffen werden, was die Gesamtprofitabilität beeinträchtigen kann.

Neue Sicherheitskonzepte sind gefordert

Organisationen müssen bei der Wahl ihrer Sicherheitsmaßnahmen umdenken, denn Datenschutzverletzungen können und werden auftreten. Es ist nicht ratsam, davon auszugehen, dass Sicherheitsmaßnahmen einen Angreifer davon abhalten können, sich Zugriff zum Netzwerk zu verschaffen. Stattdessen sollten Unternehmen davon ausgehen, dass sich die Angreifer bereits im Netzwerk befinden oder sich in Kürze Zugriff verschaffen könnten. Unter dieser Annahme können Unternehmen Sicherheitsmaßnahmen entwickeln, die ihre Daten jederzeit schützen, anstatt zu versuchen, ein unangreifbares System zu entwickeln, oder sich um den Schutz der Daten erst dann zu kümmern, wenn Systeme schon angegriffen wurden. Organisationen können beispielsweise Daten während der Übertragung im Netzwerk verschlüsseln, sodass Angreifer die Daten nicht lesen können, selbst wenn sie sie abhören sollten.

Für einen erfolgreichen Angriff müssen ein paar wichtige Komponenten zusammenkommen. Es muss sich um ein anfälliges System handeln, das einige Schwachstellen hat, z. B. Software, die nicht auf dem neuesten Stand ist. Es muss von Interesse für den Angreifer sein, und es muss zugänglich sein. In diesem Fall kann es zu einer Datenschutzverletzung kommen, wenn ein Angreifer über die richtigen Tools und Techniken verfügt.

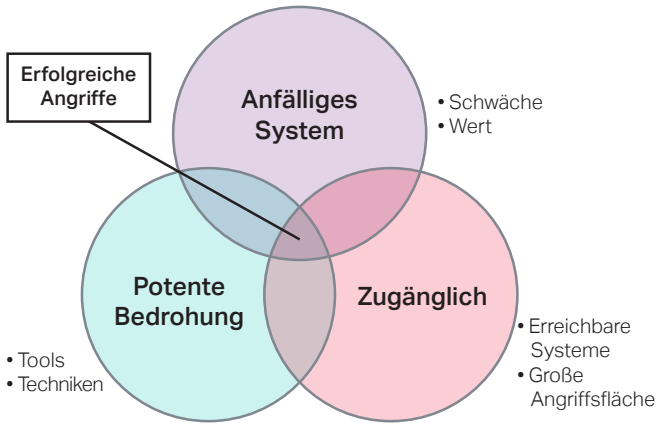

Abbildung 1. Komponenten eines erfolgreichen Angriffs

Für die Erarbeitung einer Sicherheitsstrategie sind drei Schritte erforderlich: Identifizierung der Assets, Festlegung des Zugriffs und Verstehen der Bedrohungen. Bei der Identifizierung von Assets muss festgelegt werden, welche Assets wichtig sind,z. B. Daten und vertrauliche Aufzeichnungen, und wie diese Assets geschützt werden bzw. wie darauf zugegriffen wird. Daten in einer Datenbank können sicher sein, weil die Datenbank geschützt ist; wenn diese Daten jedoch aus der Datenbank exportiert und über das Netzwerk übertragen werden, sind sie möglicherweise nicht mehr sicher. Wenn z. B. HR-Daten für das Berichtswesen nach Excel exportiert werden, werden möglicherweise Backups von Spreadsheets unverschlüsselt von Rechenzentrum zu Rechenzentrum übertragen und sind damit nicht sicher.

Netzwerkverschlüsselung als eine umfassende Sicherheitsstrategie

Der Schutz aller Daten zwischen Rechenzentren und innerhalb der Cloud als Teil einer umfassende Sicherheitsstrategie ist heute so wichtig wie nie. Es sollte nie angenommen werden, dass Teile des Netzwerks vor Hackern sicher sind, und es ist nicht ratsam, die Datensicherung während der Übertragung zu vernachlässigen. Um die Vertraulichkeit von Daten zu gewährleisten, müssen Unternehmen ein umfassendes IT-Sicherheitskonzept einführen, mit dem sich Daten in der Cloud effizient und skalierbar sichern lassen.

In der Vergangenheit stand bei IT-Organisationen in Bezug auf Sicherheit immer die räumliche Sicherheit im Vordergrund, z. B. die physische Sicherheit an den Rechenzentrumseingängen oder die Einschränkung des Zugriffs auf Server und Geräte. Firewalls, Intrusion-Prevention-Systeme, Festplattenverschlüsselung, Härtung von Anwendungen und Datenbanken, rollenbasierte Zugriffskontrollen und andere Sicherheitselemente dienen der Sicherung und Verschlüsselung wichtiger Daten. Wenn Daten jedoch außerhalb dieser sicheren Grenzen oder zwischen Rechenzentren übertragen werden, sind sie anfällig für Angriffe. Erschwerend kommt hinzu, dass Daten, die über Netzwerke Dritter oder unterschiedlicher Serviceprovider übertragen werden, nicht von einer einzigen Organisation kontrolliert werden können. Deshalb ist es schwieriger, ihre Sicherheit zu gewährleisten.

Durch Verschlüsselung können Daten während der Übertragung zwischen Rechenzentren geschützt werden, doch gibt es dafür eine Vielzahl von Lösungen, die in Betracht gezogen werden müssen. Jede Verschlüsselungslösung hat ihre Vor- und Nachteile; die beste Lösung muss leicht zu implementieren und verwalten sein, aber gleichzeitig skalierbar und effizient sein.

Sicherheit auf dem Applikations-Layer oder in der Netzwerk-Infrastruktur?

Bei der Implementierung von Verschlüsselungslösungen versuchen IT-Organisationen häufig, den Applikations-Layer zu schützen oder eine in die Netzwerkinfrastruktur integrierte Verschlüsselung zu verwenden. Für die Sicherung

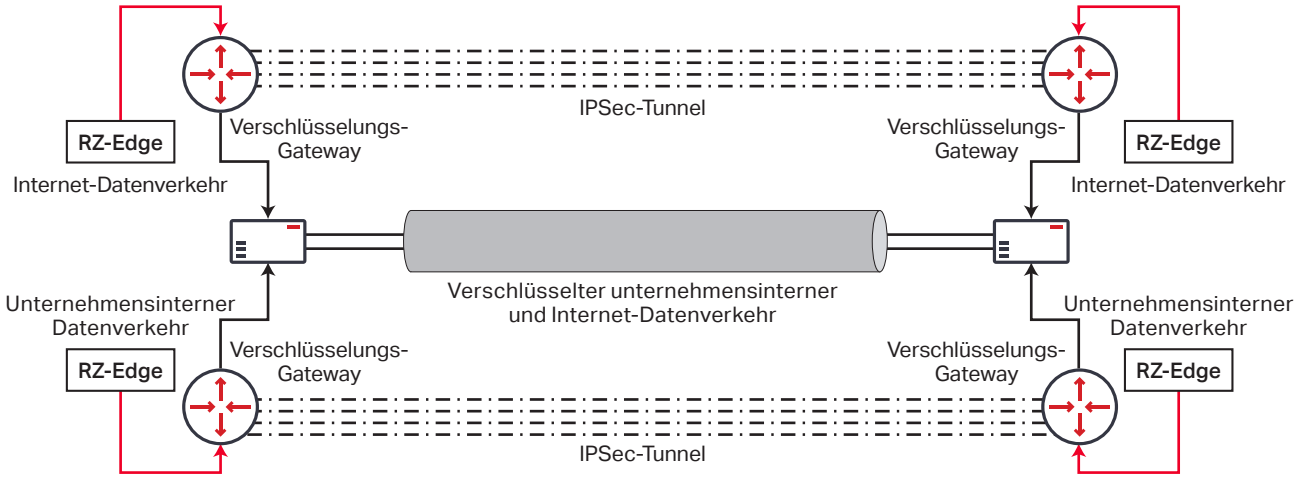

Abbildung 2. Sicherung des gesamten Datenverkehrs auf dem Packet-Layer mit verschlüsseltem Gateway (logische Ansicht)

des Applikations-Layers ist die Sicherung sowohl des Host-Computers als auch der Anwendung erforderlich: daher werden solche Sicherheitslösungen meist innerhalb von Rechenzentren implementiert. Außerdem berücksichtigen Lösungen wie z. B. Transport Layer Security (TLS) für die Sicherung der Kommunikation zwischen Anwendungen (wie z. B. Webbrowsern und E-Mail-Clients) und Servern normalerweise nicht die Kommunikation zwischen Anwendungen in der Cloud oder zwischen Rechenzentren. Der Aufbau eines gemeinsamen Frameworks für die Sicherheit zwischen Anwendungen, die auf mehrere Rechenzentren verteilt sind, kann eine Herausforderung sein; deshalb suchen Organisationen häufig nach Lösungen für die Netzwerkinfrastruktur.

Die Nutzung der Netzwerkinfrastruktur birgt eigene Probleme, und die Sicherung des Netzwerks auf dem Infrastruktur-Layer kann zu hochkomplexen Netzwerkarchitekturen führen. Der Datenfluss zwischen Rechenzentren kann sehr groß sein, und die Sicherung des kompletten Datenverkehrs von mehreren Verbindungen mit 100G und mehr kann bezüglich Betrieb, Design und Skalierung Probleme aufwerfen.

Eine mögliche Lösung ist der Einsatz verschlüsselter VPN-Gateways zur Sicherung des Verkehrs auf dem Packet-Layer (Abbildung 2). Dies erfordert die Verwendung spezialisierter, kostspieliger Gateway-Verschlüsselungsgeräte für jeden zu schützenden Link. Bei diesem Modell ist der Datenverkehr auf ein einziges Quell-/Ziel-IP-Paar begrenzt, und die äußerste IPsec-Headerinformation ist bei Pfaden mit mehreren Hops nicht für die zwischengeschalteten Router verfügbar. Diese Methode unterstützt keine Datenverkehrsschwankungen und unterbricht die Equal Cost Multi Path(ECMP)- und Link Aggregation Group(LAG)-Pfade. Außerdem ist sie nicht effizient skalierbar und erhöht die Latenzzeit. Wenn der Bandbreitenbedarf steigt und der Datenfluss immer mehr vernetzt wird, erfordern diese verschlüsselten Gateways Ports mit hohen Übertragungsraten, was zu einer drastischen Kostensteigerung führt.

Die wichtigsten Nachteilen der Verwendung von verschlüsselten VPN-Gateways zur Sicherung der Cloud sind:

- Komplexe Netzwerk-Architektur, Design und Engineering
- Notwendigkeit spezieller Skills bezüglich Betrieb und Management des Datenverkehrs zwischen Rechenzentren
- Höchst ineffiziente Skalierung
- Erhöhte Latenzzeit zwischen Rechenzentren
- Reduzierung des Paketdurchsatzes durch Verschlüsselungstechniken auf dem Packet-Layer
- Probleme beim Monitoring, der Fehlerdiagnose und anderen betrieblichen Aufgaben
- Hohe Kosten für verschlüsselte Gateway-Geräte

Wie zuvor erwähnt, sind bei zunehmendem Verkehrsfluss Ports mit höheren Übertragungsraten auf dem Verschlüsselungs-Gateway erforderlich. Diese paketbasierte Architektur lässt sich nur unzureichend skalieren, und die Verschlüsselungsgeräte sind sehr groß und teuer und haben Schwierigkeiten, den vollen Durchsatz an verschlüsselten Verbindungen zwischen Rechenzentren zu unterstützen. Um diese Probleme bei der Skalierung zu überwinden und die Kosten der speziellen verschlüsselten Gateway-Geräte bei höheren Verkehrslasten zu reduzieren, kann versucht werden, ein Verkehrsprofil zu erstellen. Ist ein solches Profil erstellt, kann der Datenverkehr nach Bedarf zwischen verschlüsselten und unverschlüsselten Pfaden, über verschlüsselte und unverschlüsselte Gateways, aufgeteilt werden (Abbildung 3). Damit soll eine Entschärfung des Skalierbarkeitsproblems erreicht werden, indem nur der zu verschlüsselnde Datenverkehr an das verschlüsselte Gateway gesendet wird; der restliche Datenverkehr wird über unverschlüsselte Gateways übertragen.

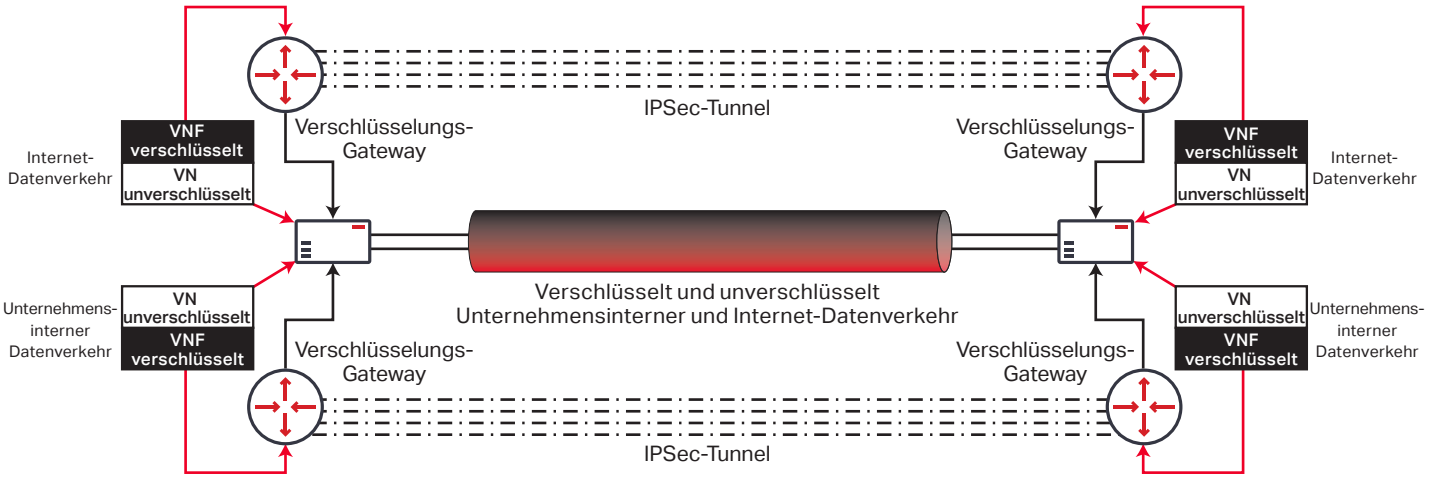

Abbildung 3. Kostenreduzierung von Verschlüsselungsgateways mit Hilfe eines Datenverkehrsprofils (logische Ansicht)

Es gibt jedoch auch Herausforderungen bei der Erstellung von Datenverkehrsprofilen. Es kann umständlich sein, genau zu bestimmen, welcher Verkehr verschlüsselt werden soll. Nur wenige Organisationen kennen ihre Daten gut genug, um sie genau zu trennen, und eine falsche Zuordnung kann dazu führen, dass sensible Daten ungeschützt bleiben. Ziele und Parameter von Anwendungen werden oft aktualisiert, und solange das Datenverkehrsprofil nicht an diese Veränderungen angepasst ist, kann es zur Übertragung von sensiblen Daten über ungeschützte Verbindungen kommen.

Zu den wichtigsten Nachteilen der Erstellung von Verkehrsprofilen mit verschlüsselten und unverschlüsselten Gateways gehören:

- Komplexe Netzwerk-Architektur, Design und Engineering
- Notwendigkeit spezieller Skills bezüglich Betrieb und Management des Datenverkehrs zwischen Rechenzentren
- Hohe Fehlerquote bei der Zuordnung des verschlüsselten/unverschlüsselten Datenverkehrs
- Anwendungsprofile und Verkehrsprofile müssen konsistent synchronisiert werden, da sich die Einsatzbereiche von Anwendungen mit der Zeit ändern
- Komplexes Design und Implementierung von Routing-Instanzen für den unverschlüsselten bzw. verschlüsselten Datenverkehr auf der Netzwerk-Hardware
- Erhöhte Latenzzeit zwischen Rechenzentren
- Reduzierter Gesamt-Paketdurchsatz aufgrund von Packet-Layer-Verschlüsselungstechniken
- Hohe Kosten für verschlüsselte Gateway-Geräte

Die Skalierung von Verkehrsprofilen dieser Art auf globaler Ebene ist extrem herausfordernd und es ist schwierig, sie langfristig zu pflegen. Die Verkehrsprofile für neue und bestehende Anwendungen und Datenquellen müssen gewissenhaft aktualisiert werden, um sicherzustellen, dass der Datenverkehr richtig gesichert ist. Die enge und konstante Zusammenarbeit von Anwendungsentwicklern, Sicherheitsingenieuren sowie System- und Netzwerkadministratoren muss gewährleistet sein, damit Verkehrsprofile erfolgreich erstellt werden können.

Beide Methoden der Packet-Layer-Verschlüsselung haben Nachteile aufgrund der komplexen Skalierbarkeit und Implementierung. Zum Glück gibt es eine neue Option zur Reduzierung der Komplexität und Verbesserung der Skalierbarkeit, nämlich die Verschlüsselung des Datenverkehrs während der Übertragung auf dem optischen Layer.

24/7-Datensicherheitslösungen

Verschlüsselung des optischen Layers: ein einfacher, sicherer Ansatz

Anstatt Ressourcen für die Erstellung von Verkehrsprofilen und die Separierung des Datenverkehrs zu verschwenden, um nur sensible Daten zu schützen, werden zunehmend Verschlüsselungslösungen für den optischen Layer in Betracht gezogen, die leicht zu implementieren sind und gleichzeitig Schutz für alle Daten bieten. Die Verschlüsselung auf Layer 1, oder dem optischen Layer, tut genau das. Sie verschlüsselt den gesamten OTN-Payload und sichert gleichzeitig alle Nachrichten, Header und Daten, die auf den oberen Layern übertragen werden (Abbildung 4).

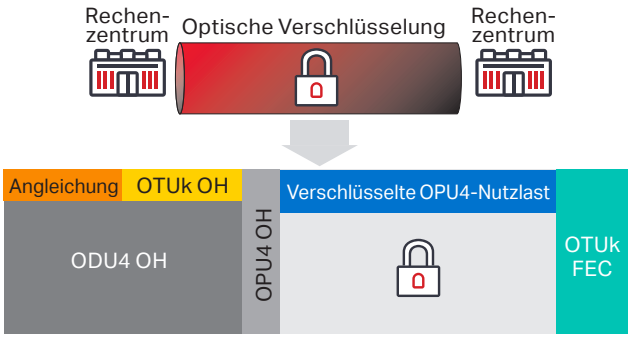

Abbildung 4. Sicherung des GESAMTEN Verkehrs mit Layer 1-Verschlüsselung

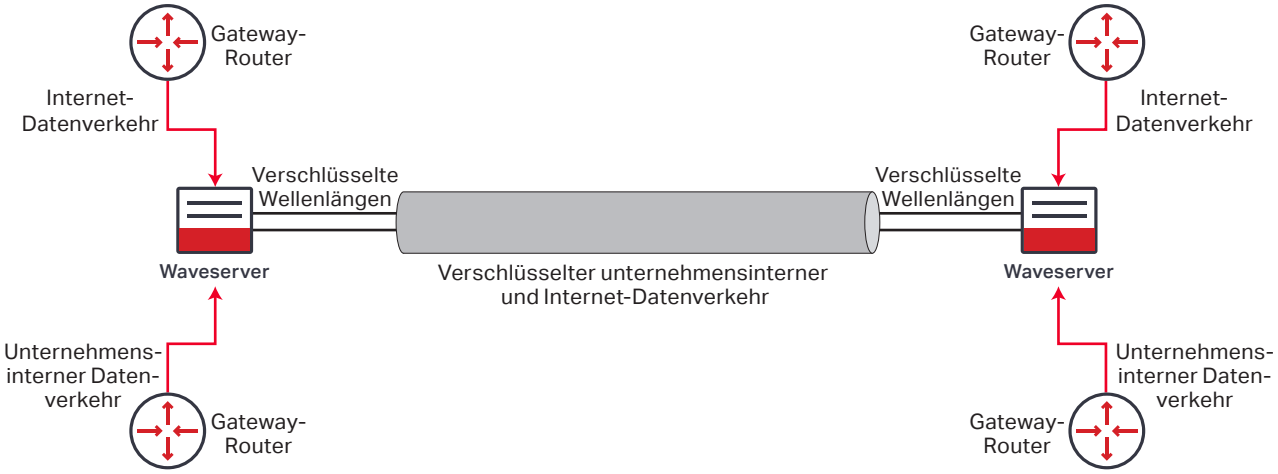

Abbildung 5. Sicherung des gesamten Verkehrs auf dem optischen Layer (logische Ansicht)

Die Verschlüsselung auf dem optischen Layer vereinfacht die Netzwerkarchitektur (Abbildung 5). Gateway-Router senden den Verkehr zur Blockverschlüsselung direkt an das Übertragungsgerät (in diesem Fall Waveserver®). Es sind keine kostspieligen Verschlüsselungsgateways erforderlich, und eine Verkehrsprofilerstellung zur Identifizierung der zu verschlüsselnden Daten ist nicht notwendig. *Der gesamte Datenverkehr, der das Rechenzentrum verlässt, wird mit Übertragungsgeschwindigkeit bei vollem Durchsatz verschlüsselt.*

Die Layer 1-Verschlüsselung bietet die folgenden Vorteile:

- **Es werden keine zusätzlichen VPNs zur Verkehrsverschlüsselung benötigt –** die Layer 1-Verschlüsselung ist eine Lösung zur Verschlüsselung des gesamten Datenverkehrs, deshalb müssen keine Verkehrsprofile erstellt werden, um verschlüsselte und unverschlüsselte VPNs zu separieren. Die gesamte Kommunikation ist sicher.
- **Vernachlässigbare Latenzzeit –** Bei der Verschlüsselung auf Layer 1 steigt die Latenzzeit um Nanosekunden bzw. Mikrosekunden, wohingegen bei Lösungen auf höheren Layers, wie beispielsweise dem IPSec- oder Applikations-Layer, die Latenzzeit um Hunderte Millisekunden steigen können.
- **Voller Durchsatz –** nur der Payload auf dem Transportlayer ist verschlüsselt, sodass der Packet-Layer-Durchsatz auf Routern und Switches nicht betroffen ist. Bei Layer 1-Verschlüsselungslösungen mit Übertragungsgeschwindigkeit wird der verschlüsselte Datenverkehr mit dem vollen Durchsatz übertragen.
- **Einfacher Aufbau, Design und Betrieb –** Layer 1-Verschlüsselungslösungen sind in die optischen Transportsysteme integriert, die für die DWDM-Übertragung im Metro- oder Langstreckennetzwerk verwendet werden; es sind keine zusätzlichen Verschlüsselungsanwendungen erforderlich.
- **Multi-Protokoll-Support –** Layer 1 bietet Support für verschiedene Datenverkehrsarten, einschließlich Ethernet, IP, SDH/SONET, Fiber Channel und mehr, und reduziert so die Anzahl der benötigten Verschlüsselungsanwendungen. Gleichzeitig werden Optionen wie IPSec besser unterstützt, die nur ein Protokoll (IP) nutzen.

Die Verschlüsselung auf Layer 1 bietet eine einfache Lösung zur Sicherung der Cloud. Sie ermöglicht die Blockverschlüsselung aller Daten während der Übertragung über den geschützten Link hinaus. Ein weiterer Vorteil der Layer 1-Verschlüsselung ist, dass sie auf dem untersten Layer alle Daten erfasst. Sicherheitsorganisationen können, falls dies aufgrund von Regelungen oder als Teil einer umfassenderen Sicherheitsstrategie erforderlich ist, nach wie vor Verschlüsselungslösungen auf dem oberen Layer entwickeln und implementieren, doch im Falle einer Kompromittierung auf dem oberen Layer sind die Daten noch immer auf dem optischen Layer verschlüsselt. Je nach Entwicklungsstand ihrer globalen Sicherheitsrichtlinien haben Organisationen die Möglichkeit, einen umfassenden Sicherheitsplan zu erstellen oder die Layer 1-Verschlüsselung als Catch-All einzusetzen.

Die Ciena WaveLogic Verschlüsselungslösung

Ciena bietet die Layer 1-Verschlüsselung an, um zu gewährleisten, dass Daten mit AES-256-Verschlüsselungsalgorithmen gesichert werden und nicht über unsichere, gefährdete Verbindungen laufen. Wenn ein Angreifer Zugriff auf das physische Medium erlangen und versuchen würde, Glasfaserverbindungen anzuzapfen, wären damit alle Daten verschlüsselt und könnten nicht ausgewertet werden.

Ciena WaveLogic Encryption ist eine einfach zu implementierende, optische Wire-Speed-Verschlüsselungslösung, die in optische Datenübertragungsgeräte integriert ist. Die Verschlüsselung muss nur einmal konfiguriert werden und ist dann immer aktiviert – so wird gewährleistet, dass alle Daten zu jeder Zeit während der Übertragung geschützt sind. So werden menschliche Fehler ausgeschlossen, die dazu führen könnten, dass sensible Daten unverschlüsselt im Netzwerk verschickt werden.

Die Lösung von Ciena umfasst eine FIPS-zertifizierte, mit AES-256 konforme Verschlüsselungs-Engine mit Unterstützung der neuesten kryptographischen Public-Key-Algorithmen, einschließlich Elliptic Curve Cryptography (ECC). WaveLogic Encryption ist für die 6500 Packet-Optical Platform und für die Waveserver-Familie von stapelbaren Interconnect-Plattformen erhältlich. Die kohärenten

WDM-Schnittstellen können für eine Vielzahl an Wire-Speed-Verschlüsselungsraten programmiert werden, einschließlich: 100G QPSK, 150G 8QAM, 200G 16QAM und Single-Carrier-400G.

Mit dem Ciena 6500 können Betreiber eine Muxponder-basierte Kartenkomplettlösung für die 10G-Verschlüsselung einsetzen oder ein 100G/200G-Leitungsmodul mit Verschlüsselung mit einer Client-Schnittstellenkarte verbinden, um die nötige Flexibilität für spezifische Datenverkehrsanforderungen zu bieten. Waveserver kann eingesetzt werden, um eine AES-256-Kapazität von bis zu 400G mit Leitungsgeschwindigkeit in nur 1HE zu unterstützen. Damit steht die nötige Flexibilität zur Verfügung, um eine Kombination von 10GE-, 40GE- und 100GE-Clients auf dem selben Gerät zu unterstützen. Waveserver Ai wurde für 100GE-Client-Schnittstellen optimiert und bietet Betreibern eine Verschlüsselungskapazität von bis zu 1,2 Tbit/s in nur einer Höheneinheit.

Die leitungsseitige Programmierbarkeit der kohärenten Transportlösungen von Ciena ermöglicht Betreibern die Optimierung der Leitungskapazität für jegliche Anwendungsanforderungen und die Sicherstellung des Datenschutzes während der Übertragung im regionalen, Metro- und Langstreckenbereich. Dies ermöglicht sichere Verbindungen zwischen Rechenzentren, unabhängig von der Distanz oder dem verwendeten photonischen Leitungssystem.

Sowohl der 6500 als auch Waveserver können eingesetzt werden, um die Cloud zu sichern, ohne komplexe Infrastruktur-lösungen auf höheren Applikationsebenen oder auf IP-Basis zu implementieren. Immer mehr sensitive Informationen werden über Glasfasernetze verbreitet, und es müssen immer mehr Gesetze und Vorschriften bezüglich Daten-sicherheit eingehalten werden. Daher gehört bei den heutigen Cloud-basierten-Netzen zur IT-Sicherheit nicht nur die Sicherheit von Servern und die Verschlüsselung gespeicherter Daten, sondern auch eine robuste Lösung für die Verschlüsselung während der Übertragung.

Mühelose Verschlüsselung.
Mehr erfahren.

Fazit

Das Erstellen eines umfassenden Sicherheitskonzepts kann eine Herausforderung darstellen – insbesondere in Bezug auf die Kommunikation zwischen Anwendungen und Rechenzentren. Organisationen ziehen oft die Netzwerkinfrastruktur in Erwägung, um Daten zwischen Rechenzentren zu sichern. Die Netzwerkverschlüsselung auf Layer 3 kann jedoch kostspielig sein und ist nur schwer skalierbar. Zum Glück steht mit der Verschlüsselung auf dem optischen Layer eine Lösung zur Verfügung, die auf unterster Ebene ansetzt und leicht implementierbar ist. Sie ist protokoll-agnostisch und unterstützt verschiedene Datenverkehrsarten. Außerdem bietet sie Wire-Speed-Verschlüsselung ohne Durchsatzeinbußen bei hoher Belastung und erhöht die Latenzzeit nur geringfügig. Mit der Verschlüsselung auf Layer 1 lassen sich Daten während der Übertragung zwischen Rechenzentren auf kosteneffiziente Weise schützen; die Ciena WaveLogic Verschlüsselungslösung kombiniert dabei ein Höchstmaß an Flexibilität und Sicherheit mit leichter Bedienbarkeit und Verwaltung. Sie unterstützt eine kosteneffiziente Wire-Speed-Verschlüsselung mit hoher Kapazität, um die Kommunikation zwischen Rechenzentren zu jeder Zeit zu sichern – egal ob über die Straße, innerhalb der Stadt, innerhalb des Landes oder über Ozeane hinweg.

Die Ciena Community
Erhalten Sie Antworten auf Ihre Fragen