APPLIKATIONSSCHRIFT

WaveLogic Encryption-Lösungen

Permanente Sicherung aller Daten während der Übertragung

Sicherheit wird immer mehr zur Chefsache. Ein Thales Data Threat Report aus dem Jahr 2020[1] ergab, dass 49 % der weltweit befragten Unternehmen im Verlauf ihrer Unternehmensgeschichte bereits einmal Opfer eines Angriffs geworden sind. Bei besonders betroffenen Branchen, wie beispielsweise im Gesundheitswesen, bei Finanzdienstleistern, Behörden und im Bildungssektor, lagen die Werte sogar noch weit höher.

Angriffe stellen nicht nur eine Gefahr für die Daten der Kunden dar, sondern auch für den Unternehmensgewinn. Nach einer weltweiten Ponemon-Studie[2] sind bei jedem erfolgreichen Angriff etwa 25.500 Datensätze betroffen. Damit liegen die Kosten für einen einzigen Angriff im Millionenbereich, ganz abgesehen vom Vertrauensverlust der Kunden, der sich nicht in Zahlen fassen lässt. Die Studie ergab weiterhin, dass sich die durchschnittlichen Kosten einer Datensicherheitsverletzung im Jahr 2019 in den USA auf 8,19 Millionen USD beliefen. Diese Angaben variieren jedoch je nach Branche. Im Gesundheitswesen sind die Kosten pro verlorenem Datensatz fast doppelt so hoch.

Gleichzeitig mit der steigenden Zahl der Angriffe ist aber auch eine Zunahme des Datenverkehrs zu beobachten. Die Nachfrage nach Bandbreite nimmt weiter zu; dafür sind Netze erforderlich, die leicht zu skalieren sind, damit die höhere Kapazität mit einem geringeren Betriebsaufwand gemanagt werden kann. Allgemein gilt, dass keine Organisation gegen die allgegenwärtige Gefahr von kriminellen Attacken auf ihre sensitiven privaten Daten gefeit ist, denn die Angriffe werden immer häufiger und raffinierter. Die heutigen Hochkapazitätsnetze erfordern nicht nur Bandbreiten mit hoher Kapazität, sondern benötigen auch ein Sicherheitskonzept, um wichtige Daten sowohl bei der Speicherung als auch bei der Übertragung zu schützen – und dies weltweit in allen Metro-, Langstrecken-, regionalen und submarinen Netzen.

Die Ciena WaveLogic™ Encryption-Lösung wurde speziell für die heutigen Hochkapazitätsnetze entwickelt und ermöglicht eine skalierbare, protokollagnostische Verschlüsselung mit extrem niedrigen Latenzzeiten auf der verbreiteten 6500 Packet-Optical Platform. Die Lösung schließt auch die Waveserver®-Produktreihe von Ciena ein, die kompakte, modulare Transportgeräte mit hoher Kapazität für die Unterstützung kosteneffizienter und sicherer Data Center Interconnect (DCI)-Anwendungen umfasst. Die Verschlüsselung ist dauerhaft aktiviert und ermöglicht durch die einfache Bedienung und Administration die schnelle Implementierung von Datenschutzkonzepten, bei denen die branchenführende kohärente

Vorteile

- FIPS-konforme Verschlüsselungslösung mit extrem niedriger Latenzzeit, für hochsichere und transparente Kommunikation über die gesamte Übertragungsstrecke
- Skalierbare Lösung mit der kohärenten programmierbaren WaveLogic-Technologie für eine flexible Wire-Speed-Verschlüsselung mit 100G bis 400G
- Protokollagnostische Verschlüsselung mit Flexibilität für die Unterstützung einer Vielzahl von Services
- Erweiterte Sicherheitsfunktionen, u. a. zwei unterschiedliche Schlüsselsätze für die Authentifizierung und die Datenverschlüsselung, mit einer schnellen Schlüsselrotation im Sekundenbereich
- Nahtlose Integration in vorhandene Unternehmens-PKIs mit X.509-Authentifizierung auf Zertifikat-Basis
- Sicheres Management durch den Endbenutzer mithilfe des integrierten Management-Tools und damit Möglichkeit der Unterstützung von Encryption-as-a-Service
- In der Praxis erprobte Verschlüsselungslösung, die bereits weltweit in Netzen in den Bereichen Finanzdienstleistung, Rechts- und Gesundheitswesen, Militär und Behörden eingesetzt wird

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

WaveLogic-Technologie von Ciena zum Einsatz kommt. Das Ergebnis ist die branchenweit erste kohärente Wire-Speed-Verschlüsselungslösung für 100G bis 400G mit konkurrenzloser Flexibilität und Leistung.

Verschlüsselungstechnologie

Unter Verschlüsselung versteht man den Vorgang der Umwandlung von Informationen mit Hilfe eines Algorithmus, um sie für alle unlesbar zu machen, die über kein Spezialwissen verfügen; bei der Kryptografie wird dieses Wissen als Schlüssel bezeichnet. Bei diesem Vorgang wird im Grunde der Zugang zum Netz durch die Verschlüsselung der Daten gesperrt, sodass für Eindringlinge oder andere, die nicht im Besitz des richtigen Schlüssels sind, keine sinnvollen Informationen verfügbar sind.

Es gibt unterschiedliche Verschlüsselungsmethoden; diese sind in verschiedenen Standards definiert, welche die Verschlüsselungsanforderungen für konforme Produkte und Schlüssel sowie den Zertifizierungsprozess für Netzgeräte festlegen. Es gibt mehrere unterschiedliche standardisierte Verschlüsselungsalgorithmen; dazu gehört der Advanced Encryption Standard (AES) mit unterschiedlichen Schlüssellängen (56, 128 und 256 Bit), der vom National Institute of Standards and Technology (NIST) publiziert wird. Diese Standards werden in Form von U.S. Federal Information Processing Standard (FIPS)-Publikationen veröffentlicht. Beispielsweise wurde der AES-256 Verschlüsselungsalgorithmus als FIPS 197 veröffentlicht. NIST veröffentlicht aber nicht nur algorithmusbezogene Publikationen wie FIPS 197, sondern auch Standards, in denen die Anforderungen für kryptografische Module festgelegt werden, die aus Hard- und Softwarekomponenten bestehen, wie beispielsweise FIPS 140-2.

Es gibt weitere ähnliche Frameworks, die für die Zertifizierung von Verschlüsselungslösungen herangezogen werden. Eine weitere wichtige Norm ist Common Criteria (CC) for Information Technology Security Evaluation, ein internationaler Standard (ISO/IEC 15408) für die Computersicherheitszertifizierung. Mit Common Criteria wird die stringente Spezifikation, Implementierung und Bewertung aller Netzwerkelemente in einem optischen Netzwerk gewährleistet. In Deutschland vergibt das Bundesamt für Informationssicherheit (BSI) Sicherheitszertifikate, einschließlich einer Zertifizierung gemäß Common Criteria. BSI-Zertifikate gemäß Common Criteria werden häufig als Grundlage für lokale Zertifizierungen verwendet. So lässt sich bei der Zertifizierung Zeit und Geld sparen. Mit diesen Standards und Zertifizierungsprozessen haben Serviceprovider und Endbenutzer die Sicherheit, dass ihre Verschlüsselungslösung den definierten Anforderungen entspricht, wenn sie die strikten erforderlichen Labortests und Überprüfungen bestanden hat, die von den Standards gefordert werden.

Abbildung 1: Die Datenverschlüsselung während der Übertragung als Teil einer umfassenden Sicherheitsstrategie

Schutz der Netze von heute

Verschlüsselung wird mittlerweile im großen Stil zur Datensicherung eingesetzt, sowohl bei der Datenspeicherung als auch während der Übertragung. Laut einem Ponemon-Bericht zu Trends bei der Verschlüsselung setzen nur 13 Prozent der Umfrageteilnehmer keine Verschlüsselung ein.[3] Organisationen müssen unabhängig von ihrer Größe und Branche große Anstrengungen unternehmen, um die in ihren Rechenzentren gespeicherten Daten vor nicht autorisierten Zugriffen zu schützen. Die Auswirkungen und Kosten von Angriffen lassen sich nicht ignorieren; die Konsequenzen für Unternehmen werden immer schwerwiegender, sei es durch den entstandenen Imageschaden, durch Strafverfolgung, Geldstrafen oder den Verlust von Kunden.

Es gibt eine Reihe von häufig eingesetzten Techniken zum Schutz gespeicherter Daten, die für Server, Datenbanken, Router und Switches verfügbar sind und den Benutzerzugriff auf diese Geräte verwalten. Allerdings befinden sich auch in den heutigen Web-Scale-Netzen große Datenmengen, die über Rechenzentrumsgrenzen hinweg in großen, möglicherweise weltweiten Netzen mit hoher Bandbreite übertragen werden. Zu einem umfassenden IT-Sicherheitskonzept gehört daher auch eine zuverlässige Verschlüsselungslösung der Daten während der Übertragung. Dies ist in Abbildung 1 dargestellt. Durch die Verschlüsselung von Daten, welche die Sicherheit der privaten Cloud verlassen, können Betreiber gewährleisten, dass die Daten während der Übertragung über das Netz mit seinen unterschiedlich gesicherten Bereichen bis zum Erreichen des Ziels vor nicht autorisierten Zugriffen geschützt sind.

Zwar haben auch heute schon viele Unternehmen die Verschlüsselung während der Übertragung in ihre Sicherheitsstrategie integriert, aber der Schwerpunkt liegt dabei normalerweise bei der Verschlüsselung auf Layer 2 und höher. Dies kann zwar eine gute Lösung für IT-Applikationen mit niedriger Bandbreite sein, bei denen die Übertragungszeiten keine große Rolle spielen, aber oft ist dies keine unternehmensweite Lösung, und die Verschlüsselung ist nur für IP-Applikationsdaten möglich. Wie in Abbildung 2 dargestellt, kann dieses Modell für Verschlüsselungslösungen ziemlich umständlich und teuer sein. Typischerweise werden dafür protokollspezifische Standalone-Verschlüsselungsgeräte

3 e-Security-Forschungsbericht von Ponemon, Thales: 2018 Global Encryption Trends Study; April 2018; https://go.ncipher.com/rs/104-QOX-775/images/2018-nCipher-Ponemon-Global-Encryption-Trends-Study-ar.pdf

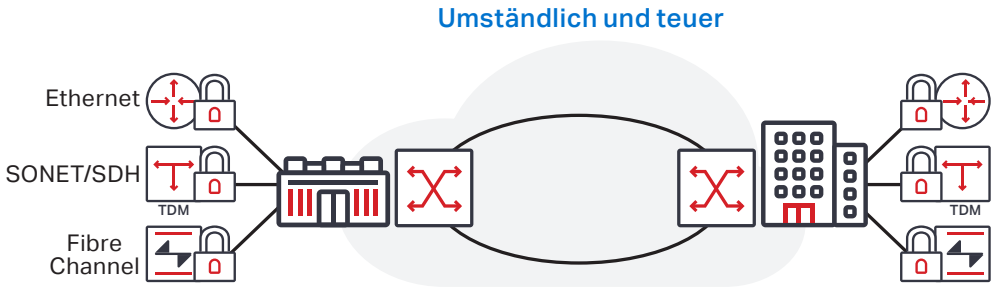

Abbildung 2: Herkömmliche protokollspezifische Verschlüsselung in einem Multiservice-Netz

benötigt, welche die Latenzzeit deutlich erhöhen können und damit den Durchsatz der Applikation beeinträchtigen und eine ineffiziente Bandbreitennutzung zur Folge haben. Außerdem ist das Management der Schlüssel und der Authentifizierung auf einer Vielzahl von Geräten nicht nur komplex und arbeitsintensiv, sondern es kompliziert auch die End-to-End-Fehlersuche in Netzen, wenn viele unabhängige Geräte eingesetzt werden. Auch entsteht hierbei eine Lücke beim Schutz von Daten während der Übertragung. Zwar wurde in der Vergangenheit das Risiko des Eindringens in Glasfaserkabel bei der Sicherheitsstrategie oft vernachlässigt, aber die Gefahr, dass optische Kabel infiltriert werden, um auf die Daten zuzugreifen, ist real. Glasfaserkabel sind häufig leicht zugänglich und kaum geschützt, und jeder, der über die nötigen Werkzeuge verfügt, kann ein Glasfaserkabel anzapfen und über Tage, Monate oder sogar Jahre Daten abgreifen, ohne entdeckt zu werden. Die Implementierung einer Verschlüsselungslösung auf dem Transport-Layer schützt alle Daten während der Übertragung und garantiert, dass jedes Bit sicher ist.

Data Security with Optical Encryption Infografik jetzt herunterladen

WaveLogic Encryption

Ciena WaveLogic Encryption ist Teil des Multi-Layer-Sicherheitsansatzes von Ciena, der die Vertraulichkeit, Integrität und Verfügbarkeit der Daten im Netzwerk sicherstellt. Es handelt sich um eine Kombination bewährter, weltweit implementierter Verschlüsselungstechnologien mit der zuverlässigen, marktführenden 6500 Packet-Optical Platform, die bereits von mehr als 600 globalen Betreibern eingesetzt wird. Außerdem schließen die Möglichkeiten der Ciena WaveLogic Encryption auch das Ciena Waveserver-System sowie das Waveserver Ai Stackable Interconnect-System ein, die eine Verschlüsselung mit Leitungsgeschwindigkeit für eine Kapazität von bis zu 1,2 Tbit in nur 1HE und damit einfache Rack-and-Stack-DCI-Applikationen ermöglichen.

Einfache Implementierung

Mit WaveLogic Encryption profitieren Betreiber von einer einfachen Implementierung, da die Verschlüsselungs-funktionalität direkt in die Netzwerkkomponenten im Transportnetz integriert wird. Durch diesen Ansatz reduziert sich die Komplexität von Netzen, denn es müssen keine unterschiedlichen Verschlüsselungslösungen für verschiedene Applikationen verwaltet werden, wie in Abbildung 3 dargestellt ist. Der einfache Betrieb betrifft auch das Management der Verschlüsselungslösung, die ein spezifisches Tool für die Authentifizierung und das Schlüsselmanagement beinhaltet, sowie die problemlose Integration in vorhandene Unternehmens-PKIs.

Mit der flexiblen 6500 Plattform können Kunden die optimale Bauform für ihre individuellen Anforderungen in Bezug auf Kapazität, Platz- und Energiebedarf wählen, wodurch eine kosteneffiziente Übertragung verschlüsselter Daten gewährleistet ist. Die Lösung ist völlig protokollagnostisch – ein zusätzlicher Vorteil, da hierdurch eine Vielzahl flexibler Clients wie beispielsweise Ethernet, SDH/SONET, Glasfaser und OTN unterstützt werden können, um unterschiedliche Applikationen bei sicherheitsbewussten Kunden zu implementieren.

Differenzierung durch Verschlüsselung rund um die Uhr

Bei den Ciena WaveLogic Encryption-Lösungen ist die Verschlüsselung ständig aktiviert. Damit wird ein höchstmöglicher Sicherheitsstandard erreicht, denn der gesamte Datenverkehr ist immer verschlüsselt. Zwar mag die

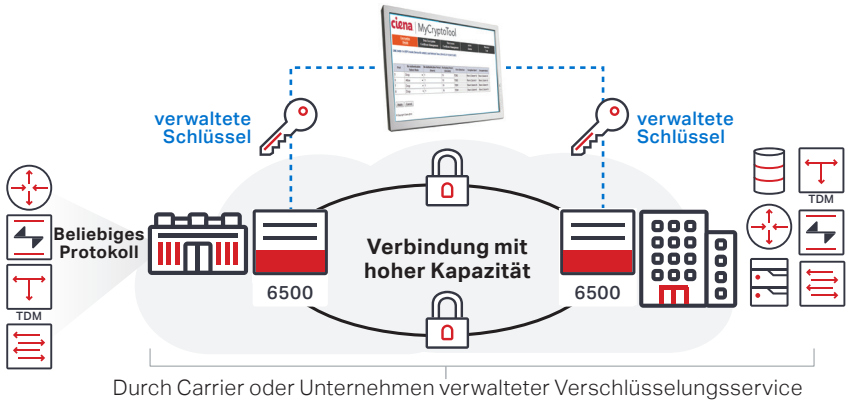

Abbildung 3: Die Ciena 6500 WaveLogic Encryption-Lösung

Fähigkeit zum Ein- oder Ausschalten der Verschlüsselung zusätzliche Flexibilität bieten, aber ein einfacher menschlicher Fehler kann dann dazu führen, dass sensibler Datenverkehr unverschlüsselt über das Netz übertragen wird. Für Betreiber steht damit eine differenzierte Infrastruktur zur Verfügung, bei der alle Daten während der Übertragung ständig geschützt sind, egal ob im regionalen, submarinen, im Metro- oder im Langstreckenbereich. Außerdem können verschiedene Abstufungen von Service Level Agreements (SLAs) mit verschlüsselten Services mit extrem niedriger Latenzzeit und unterschiedlichen Schutzoptionen für Pfade und Geräte definiert werden, wodurch die Umsätze gesteigert und die Kundenbindung verbessert werden können.

Robuste Verschlüsselung

Die Ciena WaveLogic Encryption-Lösung wird von externen Institutionen validiert und zertifiziert, um sicherzustellen, dass sie mit standardisierten Algorithmen und Sicherheitsfunktionen implementiert wird. Dazu gehört auch eine Zertifizierung nach Common Criteria und FIPS. Die Kombination aus einer FIPS-zertifizierten AES-256-Verschlüsselungs-Engine mit standardisierten Authentifizierungsmechanismen (wie beispielsweise X.509-Zertifikate) ermöglicht eine nahtlose Integration in vorhandene PKIs des Unternehmens. Außerdem sind die Hard- und Softwarekomponenten der kryptografischen Module der 6500-Plattform mit FIPS 140-2 konform und verfügen über eine vollständige BSI-Zertifizierung gemäß Common Criteria for Information Technology Security Evaluation. Serviceprovider und Endbenutzer können also sicher sein, dass ihre Verschlüsselungslösung in allen Aspekten einer umfassenden Überprüfung genügt, einschließlich Verschlüsselungsalgorithmen, Schlüsselaustausch-mechanismen und Benutzerauthentifizierung.

Zwei getrennte und voneinander unabhängige Schlüssel für die Authentifizierung und die Datenverschlüsselung bieten zusätzlichen Schutz. Das Rotationsintervall der Schlüssel ist äußerst kurz und beträgt nur wenige Sekunden. Die AES-256-Datensitzungsschlüssel werden autonom ausgehandelt sowie sekündlich für jede Leitungsschnittstelle der Karte unabhängig voneinander aktualisiert, ohne dass Datenverkehr oder Durchsatz hiervon beeinträchtigt werden oder der Benutzer eingreifen muss. Betreiber können damit die neueste Generation von Public-Key-Verschlüsselungsalgorithmen implementieren, welche auch Elliptic Curve Cryptography (ECC) unterstützen. Damit ist eine gegenüber den Verschlüsselungssystemen der ersten Generation erheblich bessere Sicherung möglich.

Programmierbare Wire-Speed-Verschlüsselung mit 100G bis 400G

Um die Anforderungen der Hochkapazitätskommunikation zu erfüllen, setzt Ciena WaveLogic Encryption die branchen-führende kohärente WaveLogic-Technologie ein, um flexible, individuell anpassbare Verschlüsselungslösungen mit hoher Kapazität zu implementieren. WaveLogic 3 Extreme basiert auf den Funktionen von WaveLogic 3 und zeichnet sich durch eine herausragende Leistung bei sämtlichen kohärenten Netzapplikationen aus. Möglich wird dies durch zusätzliche Modulationen sowie durch eine verbesserte Kompensation linearer und nichtlinearer Fehler. Die technologisch führende Lösung ermöglicht die Programmierung der Modulation durch Software. Damit wird die 100G-Wire-Speed-Verschlüsselung mit QPSK-Modulation, die 150G-Wire-Speed-Verschlüsselung mit 8QAM-Modulation und die 200G-Wire-Speed-Verschlüsselung mit 16QAM-Modulation unterstützt. WaveLogic Ai basiert auf der branchenführenden Leistung von WaveLogic 3 und nutzt eine weiterentwickelte, für 400G optimierte Engine, um eine signifikante Verbesserung der Rentabilität bei der Datenübertragung zu erzielen: Verdoppelung der Kapazität pro Kanal, Verdreifachung der Entfernung bei gleicher Kapazität und Vervierfachung der Servicedichte.

Beim 6500 kann der Betreiber ein WaveLogic 3 Extreme-Leitungsmodul mit Verschlüsselung in unterschiedliche Client-Schnittstellen integrieren, um flexible Lösungen zu implementieren, welche die jeweiligen Datenverkehrs-anforderungen unterstützen – egal, ob die Übertragungs-services 10G, 40G oder 100G erfordern. Die Lizenzkosten der modularen Lösung sind nutzungsabhängig. Bei wachsenden Anforderungen kann das gleiche Leitungsmodul so programmiert werden, dass eine verschlüsselte Datenübertragung mit 200G ermöglicht wird – einfach durch Hinzufügen einer weiteren Client-Karte. Weiterhin besteht die Möglichkeit, verschlüsselte Services mit hoher Kapazität mithilfe der Hybrid-Packet-/OTN-Fabric des 6500 zu implementieren – damit können Netzressourcen äußerst effizient genutzt werden.

Bei Waveserver stehen für den Betreiber bis zu 400 Gbit/s an FIPS-zertifizierter, gemäß AES-256 mit Leitungsgeschwindigkeit verschlüsselter Kapazität in nur 1HE zur Verfügung, sowie die Flexibilität, um Clients mit 10GE, 40GE und 100GE mit dem gleichen Gerät zu unterstützen. Aufgrund der programmierbaren Modulation kann mit Waveserver die Kapazität der Verschlüsselung mit Leitungsgeschwindigkeit für jede Applikation und Anforderung optimiert werden. So können zwei Wellenlängen mit 100 Gbit/s, 150 Gbit/s oder 200 Gbit/s kombiniert werden. Für die Unterstützung sicherer Interconnect-Applikationen mit extrem hoher Kapazität kann Waveserver Ai implementiert werden, um eine Verschlüsselungskapazität von bis zu 1,2 Tbit/s in nur 1HE zu ermöglichen. Damit wird es möglich, drei Datenverkehrsmodule mit einer Verschlüsselungskapazität von jeweils bis zu 400 Gbit/s zu unterstützen. Waveserver und Waveserver Ai ermöglichen den hochsicheren Schutz der Daten während der Übertragung mit extrem niedrigen Latenzzeiten für Metro-, regionale und Langstreckenverbindungen.

6500 Wire-Speed-Verschlüsselung mit 10G

Verschlüsselte 10G-Services können mit dem 4x10G Optical Transponder mit Verschlüsselungsmodul kostengünstig implementiert werden. Das Modul benötigt einen Steckplatz

Wire-Speed-Verschlüsselungsmodule mit hoher Kapazität
Datenblatt jetzt herunterladen

und bietet eine Verschlüsselungskapazität von 40G über vier getrennte, protokollunabhängige 10G-Leitungsports. Kunden können damit ihr Netzwerkdesign vereinfachen, denn die integrierte Verschlüsselung ist in allen Chassisvarianten des 6500 einsetzbar. Mit einem Design, das FIPS 140-2 Level 3 entspricht, bietet das Modul verbesserte Sicherheit und Schutz gegen physische Manipulationen der Karte, denn die Schlüssel können mit Nullen überschrieben werden, wenn eine Manipulation erkannt wird. Damit kann sichergestellt werden, dass alle kritischen Informationen gelöscht werden, wenn eine physische Manipulation des Verschlüsselungsmoduls erkannt wird. Dies wird auch im nicht eingebauten Zustand sichergestellt.

Verschlüsselungsmanagement leicht gemacht

Eine branchenführende Transport-Layer-Security-Lösung wäre nicht vollständig ohne ein einfaches, integriertes Verschlüsselungsmanagement. Die Trennung des Verschlüsselungsmanagements vom Datenübertragungsmanagement bietet zusätzliche Flexibilität für Infrastrukturen, die entweder von einem Betreiber oder Unternehmen verwaltet werden können. In beiden Fällen ist es wichtig, dass der „Eigentümer" der Daten – der Endbenutzer – die vollständige Kontrolle über die Verschlüsselungsparameter seiner wichtigen Daten behält und neue Schlüssel oder Zertifikate entsprechend den eigenen Sicherheitsrichtlinien vergeben kann, sowie gleichzeitig auf alle Sicherheitsalarme und Aufzeichnungen für den gesamten Übertragungsweg zugreifen kann.

Zur Ciena 6500 WaveLogic Encryption-Lösung gehört auch MyCryptoTool, eine Benutzerschnittstelle für das Verschlüsselungsmanagement, die speziell für das verteilte Management von Netzen entwickelt wurde. Damit besteht die Möglichkeit zur unabhängigen Verwaltung von Sicherheitsparametern und Alarmen – sowohl durch den Carrier als auch durch den Unternehmenskunden. MyCryptoTool ist eine benutzerfreundliche Schnittstelle, welche eine sichere Verbindung zum kryptografischen Modul herstellt und gegenseitige Authentifizierung bietet, wodurch der Zugriff auf autorisiertes Sicherheitspersonal beschränkt wird. Im Fall, dass der verschlüsselte Service von einem Serviceprovider erworben wird, verwaltet der Provider die Links und deren Bereitstellung, Verwaltung und Leistungsüberwachung wie bei jedem anderen Service, er hat jedoch keine Kontrolle über die Verschlüsselungsparameter. Der gleiche Ansatz gilt auch, wenn die Verschlüsselungslösung von zwei unterschiedlichen Gruppen im selben Unternehmen oder derselben Behörde implementiert und verwaltet wird.

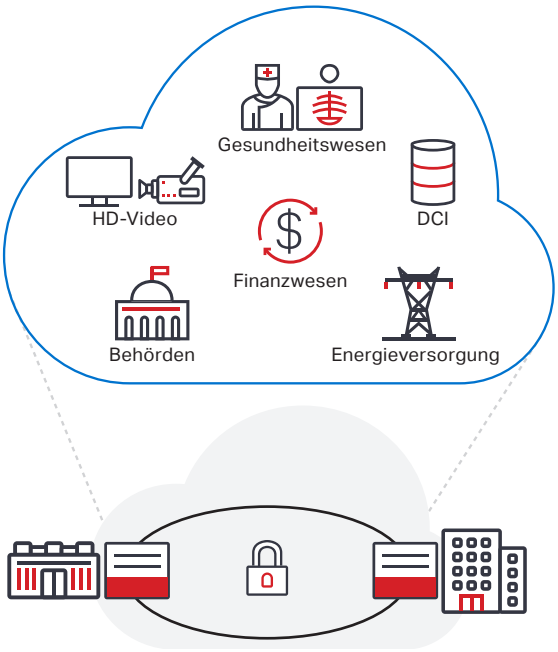

Abbildung 4: Beispiele für wichtige WaveLogic Encryption-Applikationen

Hauptapplikationen

Die Ciena WaveLogic-Verschlüsselungslösungen wurden speziell zum Schutz wichtiger Daten während der Übertragung für die heutigen Applikationen mit hoher Kapazität entwickelt. Zu den wichtigsten Applikationen, bei denen diese Lösungen von Nutzen sind, gehören:

- Unternehmens-DCI für die Speicherung und die verschlüsselte Übertragung großer Datenmengen
- Behörden und Institutionen, die eine zertifizierte und sichere Hochgeschwindigkeitskommunikation zwischen Standorten benötigen
- Applikationen im Gesundheitswesen, die auf qualitativ hochwertige Datenübertragung mit niedriger Latenzzeit angewiesen sind, um eine sichere, effiziente und schnelle Zusammenarbeit zwischen unterschiedlichen Funktionen zu ermöglichen
- Managed-Service-Applikationen
- Latenzzeitsensitive Applikationen, wie beispielsweise HD-Video oder High-Speed-Trading, die eine sichere Transportlösung mit extrem niedriger Latenzzeit benötigen
- Energieversorger, die ihre wichtigen Kommunikationsinfrastrukturen schützen wollen

Zusammenfassung

Da immer mehr sensitive Informationen über Glasfasernetze verbreitet werden, gehört bei den heutigen Hochkapazitätsnetzen 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. In der Ciena WaveLogic Encryption-Lösung wurden hohe Flexibilität und Sicherheit mit einfachem Betrieb kombiniert. Dies ermöglicht die Implementierung von kosteneffizienten und skalierbaren Wire-Speed-Verschlüsselungslösungen für die ständige Sicherung praktisch aller Daten während der Übertragung, egal ob diese nur über die Straße, innerhalb der Stadt oder über Landesgrenzen hinweg stattfindet.

War dieser Inhalt hilfreich? Ja Nein

Ciena behält sich das Recht vor, die hier beschriebenen Produkte oder Angaben jederzeit ohne Vorankündigung zu ändern. Ciena und das Ciena Logo sind Warenzeichen oder eingetragene Warenzeichen der Ciena Corporation in den USA und anderen Ländern. Eine vollständige Liste der Warenzeichen von Ciena finden Sie unter www.ciena.com. Warenzeichen Dritter sind das Eigentum der jeweiligen Inhaber und implizieren keine Partnerschaft zwischen Ciena und einem anderen Unternehmen. Copyright © 2020 Ciena® Corporation. Alle Rechte vorbehalten. Beim vorliegenden Text handelt es sich um die Übersetzung eines englischen Dokuments. Bei Abweichungen ist die englische Fassung maßgebend. AN107_de_DE 11.2020