Solution Brief

ConnectGuard™ Schutz für optische Netze

Zuverlässiger Schutz auf Layer 1 mit quantensicherer Verschlüsselung

Wesentliche Vorteile

- **Beliebige Protokolle, jede Geschwindigkeit Transparente Hardware-Verschlüsselung mit minimaler Latenzzeit bei vollem Durchsatz**
- **Gleichzeitiger Schutz aller Netzschichten Verschlüsselung auf unterem Layer schützt alle darüber liegenden Netzschichten**
- **Zertifiziert und zugelassen Common Criteria und FIPS Zertifzierzierung; BSI-Zulassung für Verschlussachen bis „VS-V" und „NATO confidential"**
- **Quantensichere Verschlüsselung Diffie-Hellman in Kombination mit quantensicherer innovativer cEliece-Kryptographie**
- **Vollständige Integration in Standard-PKI SCEP-basierte Automatisierung oder manueller Betrieb**
- **Ensemble Controller management suite Getrennte Schlüsseldomänen für Betreiber/Anwender**

Mit der Zunahme von Cloud-basierten Anwendungen verlassen immer mehr Daten die Perimeter-geschützten Unternehmensgrenzen. Damit sind sensible Daten zunehmend durch Cyberangriffe gefährdet. Unsere ConnectGuard™ Layer 1-Verschlüsselung, die auf der FSP 3000-Plattform verfügbar ist, sichert Daten bei der Übertragung über nicht vertrauenswürdige Netze mit minimalem betrieblichen Aufwand und einem Höchstmaß an Zuverlässigkeit.

ConnectGuard™ Schutz für optische Netze

Quantensichere Übertragung zwischen Datenzentren und in Weitverkehrsnetzen kritscher Infrastrukturen

Warum Verschlüsselung auf Layer 1?

Verschlüsselung ist der effektivste Weg, um die Kommunikation über nicht vertrauenswürdige Netze vor unberechtigtem Zugriff zu schützen. Darüber hinaus schützt die Verschlüsselung auf Layer 1 die Daten auf allen darüber liegenden Netzschichten, da alle höheren Schichten die Dienste der darunter liegenden Schicht nutzen. Da jedes auf Layer 1 transportierte Bit verschlüsselt wird, sind alle Daten einschließlich des Management- und Steuerungsverkehrs geschützt.

ConnectGuard™ Sicherheitslösung

Unsere innovative optische Verschlüsselungstechnologie ConnectGuard™ ist auch auf der FSP 3000 Plattform verfügbar. Ohne zusätzliche Hardware wird die Übertragung mit niedrigsten Kosten und höchster betrieblicher Einfachheit geschützt. Mit sehr geringer Latenzzeit bei vollem Durchsatz ist unsere optische Verschlüsselung ConnectGuard™ protokollunabhängig. Sie verschlüsselt jede Art von Diensten wie beispielsweise Ethernet, Fiber Channel oder OTN mit 100 Gbit/s und mehr.

Die ConnectGuard™ optische Verschlüsselung verwendet den Advanced Encryption Standard und einen 256-Bit-Schlüssel (AES-256), um Daten auf dem Übertragungsweg zu schützen. Der Diffie-Hellman-Algorithmus erzeugt im Minutentakt neue Sitzungsschlüssel. Innovative physische Schutzmechanismen und eine strikte Trennung der Schlüsselverwaltung sichern die Konformität der Lösung mit den strengsten gesetzlichen Vorschriften.

Einhaltung gesetzlicher Anforderungen

Die General Data Protection Regulation (GDPR) und andere gesetzliche Vorschriften verlangen von immer mehr Branchen wie dem Finanzsektor, dem Gesundheitswesen, Regierungsbehörden und militärischen Einrichtungen ein Höchstmaß an Sicherheit bei der Übertragung sensibler Daten zwischen Rechenzentren für die Notfallwiederherstellung und die Aufrechterhaltung von Geschäftsabläufen. Die FSP 3000 Plattform mit ConnectGuard™ optischer Verschlüsselung entspricht den strengsten Sicherheitsstandards, wie beispielsweise dem US Federal Information Processing Standard FIPS 140-2, der vom National Institute of Standards and Technology (NIST) herausgegeben wurde (Zertifikatsnummer #3952).

Die FSP 3000 Plattform mit ConnectGuard™ Verschlüsselung wurde auch von staatlichen Institutionen wie dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Übertragung von Verschlusssachen zugelassen. Derzeit ist die FSP 3000 das einzige DWDM-System, das vom BSI für den Transport von in Deutschland als vertraulich eingestuften Daten bis zur Stufe “VS-V” zugelassen ist. Die Zulassung erlaubt auch den Einsatz von ADVA FSP 3000-Geräten für die Übertragung klassifizierter Daten in EU- und NATO-Staaten.

Zuverlässiger Schutz auf Layer 1 mit quantensicherer Verschlüsselung

Vollständige PKI-Integration

Eine Public Key Infrastruktur (PKI) schützt vor Sicherheitsrisiken in strategischen Bereichen wie dem Gesundheitswesen, dem Finanzwesen oder dem Militär. Unsere FSP 3000 ConnectGuard™ Technologie nutzt das Simple Certificate Enrollment Protocol (SCEP), um sich in bestehende PKI-Systeme zu integrieren und die erforderlichen Zertifikate zu erhalten. Automatisierte Prozesse für komplexe und zeitaufwändige Aufgaben wie gegenseitige Authentifizierung, Schlüsselrotation oder Servicebereitstellung machen den Betrieb unserer verschlüsselten FSP3000-Verbindungen einfach. Dadurch werden die betriebliche Komplexität und die Betriebskosten erheblich reduziert.

Vorteilhafte Eigenschaften

- Hardware-basierte Layer 1-Verschlüsselung
- Advanced Encryption Standard mit 256-Bit Schlüssellänge (AES-256)
- Diffie-Hellman 2048/3072/4096 Bit mit automatischem Schlüsselaustausch in jeder Minute
- Konfigurierbare ODU Overhead Bytes
- FIPS (-F) zertifizierte und BSI-zugelassene Varianten der Kanalkarten
- Automatisierte Authentifizierung zwischen Transponder-Modulen oder Ports
- Schlüsselrotation während der X.509 Lebensdauer
- Automatisierte Zertifikatsregistrierung (SCEP) oder manueller Betrieb
- Management System stellt sichere Dienste bereit
- Sicherheit der Webserver mit X.509-Zertifikaten

Zukunftsfähig und quantensicher

Das Aufkommen von Quantencomputern mit extrem hoher Rechenleistung stellt eine große Gefahr für die Datensicherheit dar. Es werden neue quantensichere Techniken benötigt: PQC und QKD. Die Post-Quanten-Kryptografie (PQC) verwendet Algorithmen, die von Quantencomputern nicht gebrochen werden können. Die Quantenschlüsselverteilung (QKD) nutzt die Quantenphysik, um Informationen zu sichern. Beide Methoden werden von FSP 3000 unterstützt.

Quantencomputer befinden sich noch in der Entwicklung. Sie stellen jedoch bereits heute ein Problem dar. Daten, die mit herkömmlichen Algorithmen verschlüsselt wurden, könnten gespeichert und zu einem späteren Zeitpunkt entschlüsselt werden. Netzbetreiber und Unternehmen sollten jetzt damit beginnen, ihre Sicherheitsmaßnahmen anzupassen.

Im Juli 2021 brachte ADVA die erste kommerzielle Lösung auf den Markt, die durch PQC gesicherte Dienste anbietet. Diese quantensichere Lösung wurde nach Empfehlungen führender Sicherheitsbehörden entwickelt und basiert auf einem hybriden Schlüsselaustauschsystem, das PQC-Algorithmen mit klassischen Verschlüsselungsmethoden kombiniert. Mit Krypto-Agilität können per Software-Update zukünftige Schutzalgorithmen verwendet werden. Damit bietet diese Lösung einen robusten und zuverlässigen Netzschutz.

Connect Guard™

„Unsere ConnectGuard™ Sicherheitstechnologie erfüllt die strengsten regulatorischen Anforderungen“

Adva NETWORK SECURITY

Für weitere Informationen besuchen Sie bitte www.advasecurity.com