



ConnectGuard™ Schutz für Ethernet Netze

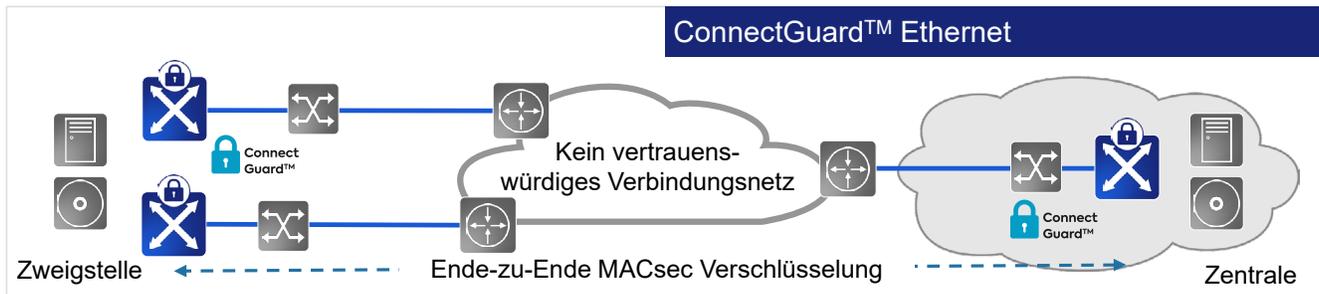
Schutz von Ethernet-Verbindungen mit quantensicherer Verschlüsselung

Wesentliche Vorteile

- **Quantensichere Ethernet Verbindungen**
Schutz von Carrier Ethernet-Verbindungen durch quantensichere AES 256-Verschlüsselung und quantensichere Algorithmen für den Schlüsselaustausch
- **Höchste Leistung und niedrigste Latenz**
Verschlüsselung der Ethernet Verkehre auf Layer 2 mit sehr geringer Latenz bei vollem Durchsatz
- **Ende-zu-Ende Schutz**
Anwendbar auf einzelne Verbindungen oder den gesamten Verkehr einer Schnittstelle über bestehende Carrier Ethernet Netze
- **Benutzerfreundlichkeit**
Automatisierte, sichere Authentifizierung der Netzelemente ohne aufwändige, manuelle Konfiguration
- **Integration in Public-Key-Infrastruktur (PKI)**
SCEP-basierter, automatisierter Zugriff auf Zertifikate vermeidet fehlerhafte Bedienung
- **Leistungsfähige Ensemble Management Suite**
Netzmanagement unterstützt separate Schlüsselverwaltung durch dedizierte Bevollmächtigte („Segregation of duties“)

Immer mehr sensible Daten und geschäftskritische Anwendungen werden in der Cloud verarbeitet und dafür täglich mehrfach über nicht-vertrauenswürdige Netze übertragen. Unternehmen, Behörden und kritische Infrastrukturen müssen ihre Netze schützen, um Angriffe auf ihre sensiblen Informationen zu verhindern. Mit ConnectGuard™ Ethernet werden Layer 2 Ethernet Verbindungen ohne nennenswerten Durchsatzverlust zuverlässig authentisiert und verschlüsselt. Diese äußerst latenzarme Sicherheitslösung ist darauf ausgelegt, auch zukünftigen Bedrohungen durch Quantencomputer zu widerstehen.

ConnectGuard™ Schutz für Ethernet Netze



Wie schützt ConnectGuard™ Ethernet-Verschlüsselung vor Quanten-Angriffen?

Der IEEE 802.1AE MACsec-Standard schützt die Vertraulichkeit und Integrität von Netzwerk-Verbindungen durch Authentisierung und Verschlüsselung der Ethernet-Verbindungen zwischen benachbarten Knoten. ConnectGuard™ Ethernet erweitert den MACsec-Standard um einen Ende-zu-Ende Schutz und hebt so die Beschränkungen einer segmentweisen Verschlüsselung auf. Dieser Schutz kann auch in bestehenden Carrier Ethernet-Netzen eingesetzt werden da die Struktur der Ethernet-Frames den Spezifikationen des IEEE802.1AE Standards entspricht. Die Krypto-agile Implementierung bietet ein hohes Maß von Flexibilität und ermöglicht ein Upgrade von etablierten Schlüsselaustausch-Algorithmen mit neuen, quantensicheren Verfahren.

Die ConnectGuard™ Lösungen von Adva Network Security

Die innovativen ConnectGuard™ Sicherheitslösungen schützen die Bitübertragungsschicht (Layer 1) und die Sicherungsschicht (Layer 2) des Verbindungsnetzes. Mit ConnectGuard™ können optische Kanäle in Echtzeit komplett verschlüsselt werden. Wenn Punkt-zu-Punkt oder Punkt-zu-Mehrpunkt Verbindungen im Carrier Ethernet-Netz geschützt werden sollen, ist ConnectGuard™ Ethernet mit äußerst geringer Latenz und sehr hohem Durchsatz die optimale Lösung. Die ConnectGuard™ Technologie bietet einem umfassenden Schutz, da nicht nur die Daten der Anwender, sondern auch die Netzsteuerung und das Netzmanagement vor Angriffen geschützt werden.

Vermeidung von Cyber-Risiken

In unserer global vernetzten Welt sind Cyberangriffe zu einem immer größeren Risiko für Diensteanbieter, Betreiber kritischer Infrastrukturen und Behörden geworden. Die Übertragung von Daten über nicht-vertrauenswürdige, öffentliche Netze muss gegen Lauschangriffe und Manipulationen geschützt werden. Eine zuverlässige Verschlüsselungstechnik schützt sensiblen Datenverkehr und stellt die Verfügbarkeit von Prozessen und Diensten mit nationaler Bedeutung sicher. In vielen Anwendungsfällen werden damit auch regulatorische Anforderungen zum Schutz kritischer Infrastrukturen erfüllt.

Die Kosten für Schäden durch Cyberangriffe haben in den letzten Jahren enorm zugenommen. Dabei werden Unternehmen nicht nur durch entgangene Einnahmen, Aufwendung für Instandsetzung und Geldstrafen geschädigt, sie haben auch immaterielle Kosten für gestohlenen geistiges Eigentum oder Imageverlust zu verkraften.

Unsere ConnectGuard™ Ethernet Sicherheitstechnologie bietet einen robusten Schutz für Netze und die darüber übertragenen Daten. Mit der MACsec Ende-zu-Ende Verschlüsselung können Verbindungen über unsichere Netze zuverlässig und effizient geschützt werden. Obwohl Quantencomputer heute noch nicht in der Lage sind, einen geschützten Schlüsselaustausch zu kompromittieren, sollten Verschlüsselungsgeräte mit quantensicheren Algorithmen erweitert werden können. Diese Krypto-agilität für neue Algorithmen wird von ConnectGuard™ Ethernet unterstützt.

Schutz von Ethernet-Verbindungen mit quantensicherer Verschlüsselung

Unsere ConnectGuard™ Ethernet-Technologie wurde in Übereinstimmung mit international anerkannten Sicherheitsstandards wie BSI, Common Criteria und dem Federal Information Processing Standard (FIPS) entwickelt.

Vollständige Integration in die PKI

ConnectGuard™ kann über standardisierte Schnittstellen einfach und sicher in bestehende Public Key Infrastrukturen (PKI) integriert werden, um Zertifikate für Anwender und Geräte zu beziehen. Ein hohes Maß an Automatisierung vereinfacht komplexe und zeitaufwändige Aufgaben wie beispielsweise die gegenseitige Authentisierung, die Erzeugung temporärer Schlüssel zum Schutz aktiver Sessions und die Aktivierung geschützter Verbindungen.

Damit liefert ConnectGuard™ einen wesentlichen Beitrag zur betrieblichen Sicherheit bei Minimierung der operativen Kosten.

Vorteilhafte Eigenschaften

- Hardwarebasierte MACsec-Verschlüsselung mit IEEE 802.1AE standardisiertem Frame-Format
- Geschützte Ende-zu-Ende Verbindungen über bestehende, nicht vertrauenswürdige Ethernet Netze
- Physische Gerätesicherheit für die sichere Speicherung von kryptografischen Schlüsseln und Erkennung von Manipulationsversuchen
- Minimaler Overhead von lediglich 24 Bytes zur Maximierung des Durchsatzes und Minimierung der Latenz
- Verschlüsselte 1Gbit/s- und 10Gbit/s-Schnittstellen im Netzabschluss mit optionalem Server für virtualisierte Netzfunktionen
- Passwort-geschützte Protokolle für den Schlüsselaustausch zur Verhinderung vor Man-in-the-Middle-Angriffen
- Quantensicherer Verschlüsselung nach IEEE 802.1AE-2006 mit GCM-AES-128 und IEEE 802.1AEbn-2011 mit GCM-AES-256

Ethernet sicher machen

Ethernet ist die am häufigsten verwendete Schnittstellen- und Switching-Technologie in öffentlichen und privaten Netzen. In den letzten Jahren wurden hohe Investitionen in den Auf- und Ausbau von Ethernet-Netzen getätigt. Die meisten Netze sind jedoch nicht in der Lage, die Daten kryptografisch zu schützen und gelten als nicht vertrauenswürdig.

Mit ConnectGuard™ Ethernet können diese nicht vertrauenswürdigen Netze in wirtschaftlicher Weise abgesichert werden. Für jede einzelne Verbindungen kann entschieden werden, ob ein Schutz notwendig ist und ob eine Verschlüsselung aktiviert werden soll. ConnectGuard™ Ethernet ist in 1Gbit/s bis 10Gbit/s Netzabschluss- und Aggregationsprodukten verfügbar und schützt auch Endgeräte mit integriertem Server, der für das Hosting von virtualisierten Netzfunktionen verwendet werden kann. Unsere ConnectGuard™ Ethernet-Technologie wird erfolgreich bei großen Kommunikationsdienstleistern sowie bei Betreibern kritischer Infrastrukturen eingesetzt. Ein FSP 150 Produkt für den sicheren Netzzugang wurde vom BSI für die Übertragung von klassifizierten Daten bis VS-NfD zugelassen.



„ConnectGuard™-Verschlüsselung ermöglicht quantensichere Verbindungen selbst über nicht vertrauenswürdige Netze“

