Adva NETWORK SECURITY

Solution Brief

ConnectGuard™ security for Ethernet networks

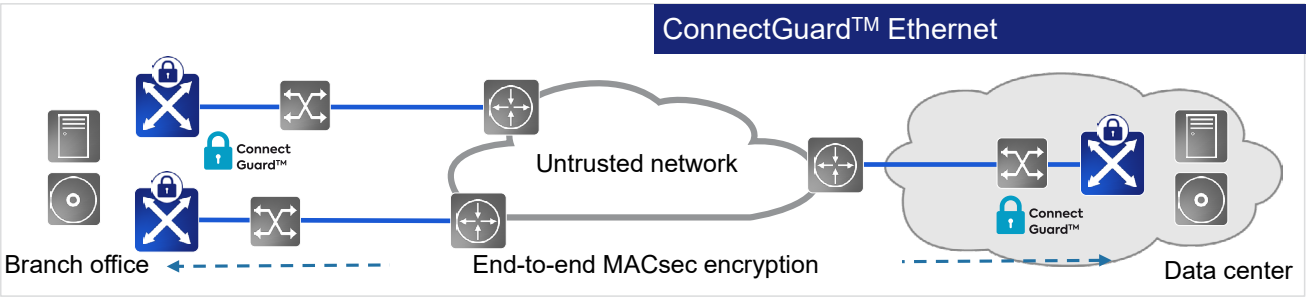
Protecting Ethernet connections with quantum-safe encryption at Layer 2

Highlights

- **Quantum-safe confidentiality and integrity**
  Protecting Carrier Ethernet services with quantum-safe AES 256 encryption and post-quantum key exchange
- **Highest performance and lowest latency**
  Encryption of Ethernet traffic with line-rate performance for highest throughput
- **End-to-end protection**
  Applicable on individual links as well as securing end-to-end connections
- **Ease of use**
  Automated, secure authentication of devices eliminates need for manual configuration
- **Full integration into standard public key infrastructure (PKI)**
  SCEP-based automated certificate handling for highest security avoiding manual interaction
- **Sophisticated Ensemble Controller management**
  Sophisticated assignment of security associations and separated key management for end-user control

With more and more sensitive data and mission-critical applications moving into the cloud, service providers, enterprises and governments are becoming increasingly concerned about untrusted connectivity networks. They need way to protect their operations from malicious attacks. With ConnectGuard™ Ethernet encryption, connections can made highly secure without impacting performance and latency, even with the emerging threat posed by quantum computers.

ConnectGuard™ security for Ethernet networks



What make ConnectGuard™ Ethernet encryption quantum safe?

Specified by IEEE, 802.1AE MACsec is a method for protecting the confidentiality and integrity of Ethernet connections. This standard specifies a technique for securing links between nodes, decrypting incoming and encrypting outgoing traffic. ConnectGuard™ Ethernet uses the MACsec standard and resolves the limitation of hop-by-hop encryption by using unencrypted tags for end-to-end security over legacy Ethernet networks. It performs IEEE 802.1AE standard-based frame format with optional VLAN tag bypass. With crypto-agility, post-quantum algorithms can be applied to secure the key exchange against quantum attacks.

ConnectGuard™ solution suite

Our innovative ConnectGuard™ security solutions provide protection across all network layers. Our ConnectGuard™ Optical encrypts high-bitrate optical traffic at line-rate, while ConnectGuard™ Ethernet secures Ethernet P2P and Ethernet LAN connections with best performance and lowest latency. By securing both data and control traffic, ConnectGuard™ Ethernet protects edge compute nodes from network attacks.

ConnectGuard™ makes any network connection secure. With our common Ensemble Controller management suite including Ensemble Packet Director, security associations and credentials can easily be managed even in heterogeneous scenarios.

Responding to cybersecurity risk

In our globally connected world, cyberattacks have become an ever-increasing risk for service providers, enterprises and governments. Data transported over public networks must be protected to meet privacy and integrity requirements and to ensure compliance with existing and emerging regulation.

When mission-critical and personal data is transported over untrusted networks, security breaches can be extremely harmful. The damage caused includes not only lost revenues, liabilities and fines but also the intangible cost of stolen intellectual property or ruined credibility. This amounts to far more than the investment required to secure connectivity networks.

Our ConnectGuard™ Ethernet provides a secure and robust solution to protect data transported over untrusted networks. It can be applied in point-to-point as well as in multi-point scenarios. Cryto-agility enables operators to upgrade with the latest, quatum-safe algorithms.

Our ConnectGuard™ Ethernet solution is developed in compliance with most stringent security standards, such as the US Federal Information Processing Standard (FIPS), Common Criteria as well as national regulations.

Protecting Ethernet connections with quantum-safe encryption at Layer 2

Full integration into PKI

Public key infrastructure (PKI) reduces security risks associated with business processes. It safeguards electronic data in strategic areas, such as healthcare, finance, or national security. Just like our ConnectGuard™ for optical networks, our ConnectGuard™ Ethernet technology has been engineered to work in this environment, where an efficient and secure interworking with third-party solutions is required. Automated processes for complex and time-consuming tasks such as mutual authentication, key rotation and service provisioning, make the operation of FSP 150 encrypted connectivity simple. This significantly reduces complexity and minimizes operational costs.

High-level specifications

- Hardware-based MACsec encryption with IEEE 802.1AE standard-based frame format and optional VLAN tag bypass
- Peer-to-peer Ethernet connection encryption over MACsec-agnostic networks
- Physical device security for secure storage of key materials with tamper detection and response circuitry
- Minimum overhead (24 bytes) to maximize throughput and minimize delay
- Secure 1GbE and 10Gbit/s interfaces with demarcation devices and edge compute nodes
- Password-authenticated Diffie-Hellman and post-quantum key exchange protocol securing against man-in-the-middle attacks
- Quantum-safe encryption standard IEEE 802.1AE-2006-compliant GCM-AES-128 and IEEE 802.1AEbn-2011-compliant GCM-AES-256 NIST-approved cyphers

Making Ethernet secure

Ethernet is the most widely used interface and switching technology in public and private networks. In recent years, a huge amount of investment has gone into building Ethernet networks. However, security has not been designed into most current installations.

ConnectGuard™ Ethernet leverages this installed base and adds security in the most cost-efficient way. On a per-connection basis, a service provider can decide to offer connectivity as a conventional or higher-value secured bandwidth service. ConnectGuard™ Ethernet is applied with our 1Gbit/s to 10Gbit/s demarcation and edge aggregation products as well as our edge compute nodes responding to the specific security needs of virtual networks.

Our ConnectGuard™ Ethernet has been successfully applied with major communication service providers as well as operators of critical infrastructure. A FSP 150 secure network access device has been approved by the German Federal Office of Information Security (BSI) for the transport of classified data up to VS-NfD.

Connect Guard™

"ConnectGuard™ encryption turns an untrusted network into a quantum-safe platform for even mission-critical communication"

Adva NETWORK SECURITY