APPLICATION NOTE

Simplifying Security between Data Centers with Optical-layer Encryption

Waveserver® Ai

Cloud services' growth depends on secure connectivity. Safeguarding sensitive and mission-critical data is essential to protect intellectual property and confidential records, and app-to-app communications between Data Centers (DCs) may require encryption as well. To avoid costly fines and loss of revenue due to data breaches, Data Center Interconnect (DCI) networks must be secured. Although the fiber networks that interconnect DCs have often been thought of as impervious to attack, ignoring inter-DC communications creates a vulnerability when sensitive data is sent from one DC to a device or application in another DC. Furthermore, data may traverse links outside of the organization's control, and thus be at risk of exposure and compromise.

Inter-DC data security can be difficult to architect, implement, and scale. Application- or packet-layer encryption can be used to secure interconnections between DCs, but each has its own set of challenges. A third option is to encrypt network data at the lowest networking layer—the optical layer. Bulk optical-layer encryption enables architecture scalability, engineering simplicity, and ease of operations while offering protection for all in-flight data passing between DCs or through the cloud.

Securing the networks between DCs is critical

A recent research study found that roughly one in four organizations could experience a large-scale data breach within the next 24 months.[1] Costs related to breaches can scale up to millions of dollars, as victims must be identified and notified, and all associated legal and regulatory fees must be paid. Additionally, once a breach takes place, further costs may be incurred through lost revenue, lost customers, and damage to the business' reputation or brand.

Legislation is increasingly requiring more stringent identification and notification for security breaches. Depending on the type of data or records being transported, regulations may require encryption of the data. Heavy regulatory fines can be levied against companies if sensitive data is compromised, which can affect a company's overall profitability.

A comprehensive IT security approach that includes an efficient and scalable way to secure cloud networking data must be adopted to ensure data confidentiality, so data is protected from attacks and breaches while in flight between DCs. But traffic flows between DCs can be very large and securing all traffic across multiple 100G+ connections can be difficult to architect and scale, as well as operationally cumbersome. Encryption at the optical layer provides a solution that is easy to deploy and manage, highly scalable, and efficient.

Optical-layer encryption—A simple, secure approach

The optical layer provides encryption solutions that are easy to implement, while offering protection for all data. It encrypts the entire Optical Transport Network (OTN) payload to secure all the messaging, headers, and data carried within upper-layer communications. It simplifies the network architecture, allowing gateway routers to send traffic directly to the transport device—in this case, Waveserver Ai—for bulk encryption without requiring expensive encryption gateways or additional encryption appliances. All traffic that leaves the DC is encrypted at wire speed with full throughput. Optical-layer encryption on Waveserver Ai provides several benefits, summarized in Figure 1.

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

Key benefits	Description
Full throughput	Only the transport-layer payload is encrypted, so packet-layer throughput on routers and switches is unaffected. Waveserver Ai offers wire-speed encryption with full-rate throughput when traffic is encrypted.
Simple to build, design, and operate	Layer 1 encryption is built directly into the Waveserver Ai platform, used to provide DWDM transmission across the metro or the long-haul network; no additional encryption appliances are required.
Negligible latency	Performing encryption at Layer 1 adds nanoseconds to microseconds of latency, whereas higher layer solutions such as IPsec or application-layer encryption can add 100s of milliseconds of latency.
Certified for encryption applications	Waveserver Ai is not designed simply for FIPS compliance. It provides FIPS 140-2 Level 2-certified encryption, having undergone certification testing and verification.
No additional VPN requirements or encryption appliances required	Since Layer 1 encryption provides a solution to encrypt all traffic, there is no need to profile traffic to send to encrypted or non-encrypted VPNs, and no specialized encryption appliances are required.

Figure 1. Benefits of optical-layer encryption

Moving to optical-layer encryption provides a simple solution to secure the cloud. Upper-layer encryption solutions can still be used for regulations or as part of a more comprehensive security plan, if required or desired; but if an upper layer compromise occurs, the data will still be encrypted at the optical layer. Organizations have the option to engineer a comprehensive security plan, or bolt on optical-layer encryption with Waveserver Ai as a catch-all, depending on where they are in the development of their global security policy.

Waveserver Ai
Simple. Scalable. Secure.

Waveserver Ai applications for optical-layer encryption

Wire-speed encryption is increasingly becoming table stakes for secure DC communication. Internet Content Providers (ICPs) and Global Content Networks (GCNs) benefit from Waveserver Ai's wire-speed encryption solution, which offers the fastest connectivity speeds, supporting up to 400G of encrypted data transmission per wavelength.

Financial networks can use low-latency optical encryption to seamlessly interconnect resources, transferring trades and data records while meeting compliance requirements by using Waveserver Ai's encryption capabilities as part of a highly secure network. Customer confidence is ensured by deploying a FIPS-certified solution that will safeguard financial data 24/7. Networks built with encryption on Waveserver Ai can be used to avoid damage to company reputation and costly sanctions due to security breaches.

Along with providing the highest-quality care, healthcare providers must securely transport patient data between locations. Nearly 90 percent of healthcare providers have been hit by data breaches in the past two years, so safeguarding data is extremely important. Using optical-layer encryption on Waveserver Ai provides a means to keep patient information secure from data breaches and protects the provider's valued reputation, while reducing patient churn by meeting expectations for information protection. Optical-layer encryption complies with HIPAA requirements for protecting healthcare information through FIPS-certified encryption of all in-flight data, all the time. By protecting against security breaches, negative public media exposure is limited, and costly fines can be avoided. Waveserver Ai enables efficient and secure collaboration between healthcare stakeholders.

Optical-layer encryption on Waveserver Ai

Ciena offers optical-layer encryption to ensure data is secured between DCs instead of flowing across unsecure, exposed links. If an adversary were to gain access to the physical medium and attempt to tap the fiber, all data would be encrypted and unusable. Waveserver Ai provides a simple-to-implement, wire-speed optical encryption solution that is always on, ensuring data is protected all the time to eliminate any human error that could result in sensitive data being sent over the network unencrypted.

Waveserver Ai utilizes a FIPS-certified AES-256 encryption engine supporting the latest public key cryptography algorithms, including Elliptic Curve Cryptography (ECC). Optical-layer encryption is available on the 1x400G module, with encryption that offers a single WaveLogic™ Ai coherent interface and four QSFP28 client 100G ports. Each Waveserver Ai chassis can support up to three encryption modules, so network operators can deploy up to 1.2T of encrypted capacity in a single rack unit (Figure 2).

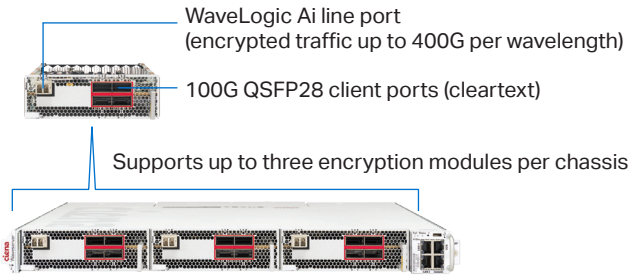

Figure 2. Waveserver Ai equipped with encryption modules

Line-side programmability built into Waveserver Ai enables operators to optimize line capacity for any application's requirements, and to secure in-flight data protection across metro, regional, or long-haul distances. The single coherent WDM interface supports wire-speed encryption at a variety of line rates, including 100G to 400G in 100G increments (in 56Gbaud mode) and 100G or 200G in 35Gbaud mode (for compatibility with existing 50GHz grid networks). Waveserver Ai ensures secure connectivity between DCs, regardless of the distance or underlying photonic line system being used.

The Waveserver Ai platform has been designed for use in the most secure networks and is FIPS 140-2 Level 2-certified. The encryption algorithm used by Waveserver Ai is FIPS 197-certified. The National Institute of Standards and Technology (NIST) developed FIPS standards and guidelines for information processing to provide information assurance and interoperability. Waveserver Ai meets FIPS Level 2 security requirements, including the basic requirements for an encryption module, and utilizing tamper-evident seals that must be broken to obtain access to security information within the module. Additionally, Waveserver Ai is certified for Common Criteria (CC), an international standard for security certification. Many vendors design products to the FIPS and CC standards, but few go through the third-party certification process to guarantee the products are compliant. Waveserver Ai has been through the certification process for both FIPS and CC and is suitable for any optical-layer encryption deployment, including government applications.

Waveserver Ai
Get the data sheet

Waveserver Ai provides several additional security features beyond encryption to ensure the security of the platform, as detailed in Figure 3.

Feature	Description
Authentication support	Gives operators the choice to utilize Pre-Shared Key (PSK) or X.509 certificates to authenticate data path encryption peers
Key rotation	Provides fast key rotation, every 10 seconds, further reducing the likelihood that a key can be compromised; session keys are stored in volatile memory, so they will not be retained if power is lost to the unit
Secure boot	Supports secure boot to perform digital signature validation on the software load
Secure erase	Supports secure erase to securely, permanently erase configuration data from non-volatile storage; all user information is destroyed as part of a secure erase, and the Waveserver Ai is reset to its factory default state
RADSec	Supports RADIUS Security (RADSec) to securely transport RADIUS authentication requests over TCP using TLS (Transport Layer Security)
SNMPv3	Supports SNMPv3 to enhance security by authenticating and encrypting data communications between the Waveserver Ai and an SNMP-based management system or notification receiver

Figure 3. Additional security features available on Waveserver Ai

A comprehensive security plan must include a robust, in-flight encryption solution

As increasingly more sensitive information is distributed across fiber-optic networks and more legislation and regulations require data security, cloud-based communications must deploy an IT security approach that encompasses a robust in-flight encryption solution. Optical layer encryption on Waveserver Ai provides first-level defense for communications between DCs that is simple to implement. It enables wire-speed encryption without decreases in throughput under heavy load and introduces almost no additional latency. Ciena's Waveserver Ai combines a high degree of flexibility and security, with ease of operation and administration. It provides FIPS- and CC-certified encryption, enabling its use in government encryption applications. Waveserver Ai enables cost-effective, high-capacity, wire-speed encryption to secure communications between DCs all the time—across the street, the city, the country, or the ocean.

Are you doing everything you can to protect your data?

Visit the Ciena Community
Get answers to your questions