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