ciena
Experience. Outcomes.

APPLICATION NOTE

Securing the Cloud

Simplifying security between data centers with Layer 1 encryption

Safeguarding sensitive or mission-critical data is essential to protect intellectual property and confidential records and avoid costly fines and loss of revenue due to data breaches. Determining which data to protect and how to protect it can be challenging. The physical design of the data center incorporates multiple layers of physical security measures to restrict unwanted access, and firewalls, anti-virus, and intrusion detection techniques may be used to secure data within the center. However, once information leaves the safe confines of the data center, its security is often neglected.

The fiber networks that interconnect data centers often have been thought of as impervious to attack, but ignoring inter-data center communications creates vulnerability when sensitive data is sent from one center to a device or application in another center. Data may traverse links outside of the organization's control, and thus be at risk of exposure and compromise.

Organizations need to keep their applications and information secure inside the data center and as it travels between centers. Inter-data center security can be difficult to architect, implement, and scale. Application layer encryption can secure interconnections between data centers. Packet layer encryption also can help, but each type has its own set of challenges. A third, more attractive 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 operation while offering protection for all in-flight data passing between data centers or through the cloud.

Securing the networks between data centers is critical

A recent 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

Layer 1 encryption enables:

- Full-rate throughput without traffic congestion
- Ultra-low-latency, wire-speed encryption for highly secure inter-data-center communications
- Solutions that are simple-to-deploy and operate, without requiring additional encryption appliances
- Flexible, protocol-agnostic encryption for a variety of services

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

place, further costs may be incurred through lost revenue and customers, and damage to the organization's reputation.

Legislation increasingly is 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. Companies can face heavy regulatory fines if sensitive data is compromised, which can affect a company's overall profitability.

Formulating a new security mindset

When considering security, organizations should adopt a new mindset—one that assumes a breach can and will happen. It is not advisable to assume defenses will keep an adversary out of the network. Instead, companies should assume attackers are already in, or will be soon. By adopting an assumed breach mentality, companies can design defenses to always protect their data, rather than trying to design an impervious system or worry about protecting the data once a system is compromised. For example, organizations can encrypt data in transit across the network, so attackers cannot read the data in flight, even if they can capture it.

A successful attack requires a few key components to come together at the same time. There must be a vulnerable system that contains some weakness, such as software that has not been patched. It must have value to the attacker, and it must be accessible. In this case, if an attacker is armed with the proper tools and techniques, a breach may occur.

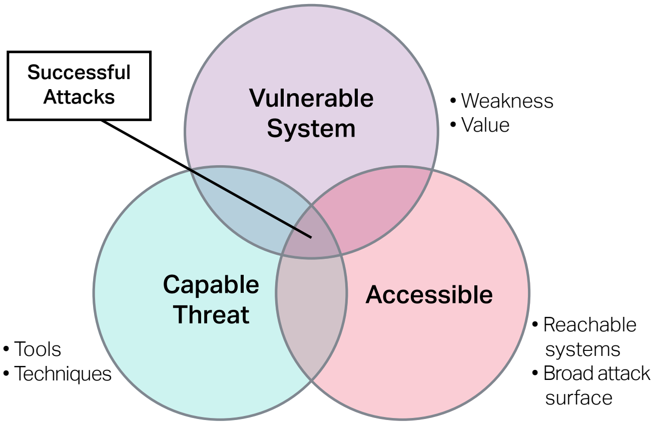

Figure 1. Components of a successful attack

To formulate a defense strategy, organizations must perform three steps: Identify assets, determine access, and understand threats. When identifying assets, organizations must know which assets are important, such as data and confidential records, and how those assets are protected and accessed. Data within a database may be secure due to protections that have been applied to the database, but if that data is exported from the database and then moves within the network, it may no longer be secure. For example, if HR exports data to Excel for reporting, backups of the spreadsheet that move unencrypted from one data center to another are not secure.

Adding network encryption for a comprehensive security strategy

As part of a comprehensive security strategy, protecting all data between data centers, including the cloud, has never been more important. No part of the network should be assumed to be impervious to hacking, and neglecting in-flight data is not advisable. To ensure data confidentiality, companies must adopt a comprehensive IT security approach that includes an efficient and scalable way to secure data transiting the cloud.

Traditionally, IT organizations have associated security with on-premises security, which includes elements such as physical security at the data center entry points and restricted access to servers and equipment. Firewalls, intrusion prevention systems, full disk encryption, application and database hardening, role-based access controls, and other security elements secure and encrypt critical data repositories. However, when data moves outside these secure walls or is in flight between data centers, it is vulnerable to attacks and breaches. Further compounding the problem, data traversing third-party networks or multiple service provider networks may not be under a single organization's full control, so ensuring its security becomes more challenging.

Encryption can be used to protect in-flight data as it transits between data centers, but there are a variety of solutions to consider. Each encryption solution comes with its own benefits and challenges, and the best solution must be easy to deploy and manage, highly scalable, and efficient.

Application layer or network infrastructure security?

When implementing an encryption solution, IT organizations commonly either try to protect the application layer or use encryption built into the network infrastructure. Application layer security requires securing both the host device and the application, so most application layer security frameworks are contained within the data center. Also, solutions such as Transport Layer Security (TLS), which secures communications between applications (such as Web browsers or email

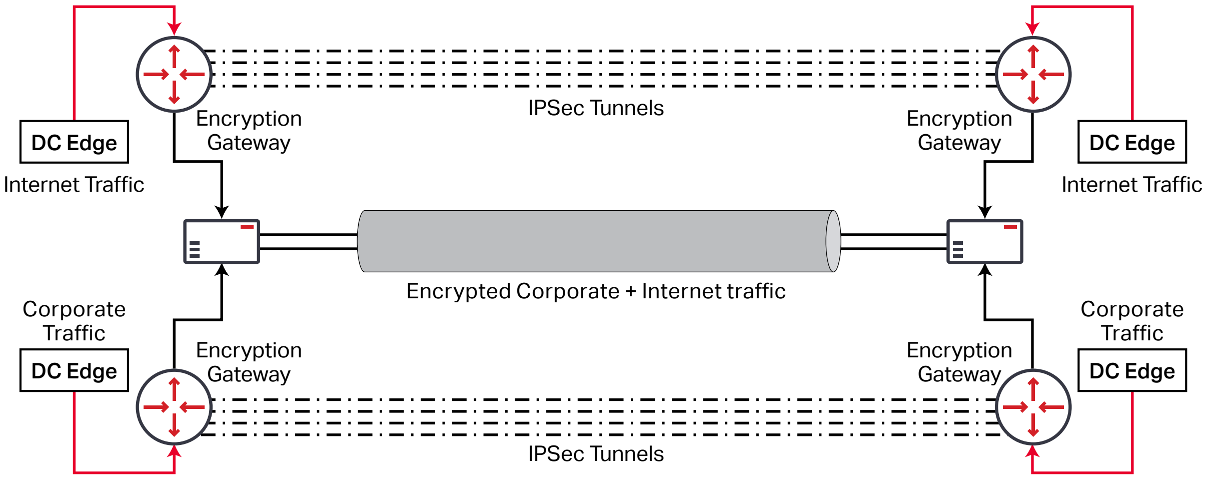

Figure 2. Securing all traffic at the packet layer with an overlay (logical view)

clients) and servers, do not typically address application-to-application security for communications through the cloud or between data centers. Building a common framework for application-to-application security across multiple data centers can be challenging, so organizations frequently look to the network infrastructure for the solution.

Using the network infrastructure introduces its own set of challenges and securing the network at the infrastructure layer can result in a highly complex network architecture. Traffic flows between data centers are very large, and securing all traffic across multiple 100G+ connections can be operationally cumbersome and difficult to architect and scale.

One option is to use an overlay of encrypted VPN gateways to secure traffic at the packet layer (Figure 2). This requires use of specialized, higher-cost encryption gateway equipment on each link that requires protection. This model limits traffic to a single source/destination IP pair, and the outermost IPsec header information is not available to intermediate routers for multi-hop paths. This overlay method does not allow for traffic variability, and breaks Equal Cost Multi-Path (ECMP) and Link Aggregation Group (LAG) paths. Furthermore, it does not scale efficiently and increases latency. As bandwidth requirements increase and data flows become more meshed, higher-rate ports are required on the encrypted gateways, dramatically increasing costs.

The key drawbacks of using an overlay of encrypted VPN gateways to secure the cloud include:

- Complex network architecture, design, and engineering
- Specialized skills required for operating and managing inter-data center traffic
- Highly inefficient to scale
- Introduces additional latency between data centers
- Packet layer encryption techniques reduce overall packet throughput
- Monitoring, troubleshooting, and other operational challenges
- High cost of encrypted gateway equipment

As previously mentioned, as traffic flows increase, higher-rate ports are required on the encryption gateway. This packet-based architecture scales poorly, and the encryption devices become very large, very costly, and have difficulty providing full-throughput on the encrypted links between data centers. To overcome this scalability challenge and reduce the cost of the specialized encrypted gateway equipment at higher traffic loads, organizations may attempt to profile their traffic. Once profiled, traffic can be split between encrypted and non-encrypted paths through encrypted or non-encrypted gateways as required (Figure 3). This attempts to alleviate scalability issues on the encrypted gateway by sending traffic requiring encryption to the encrypted gateway and offloading all other traffic to non-encrypted gateways.

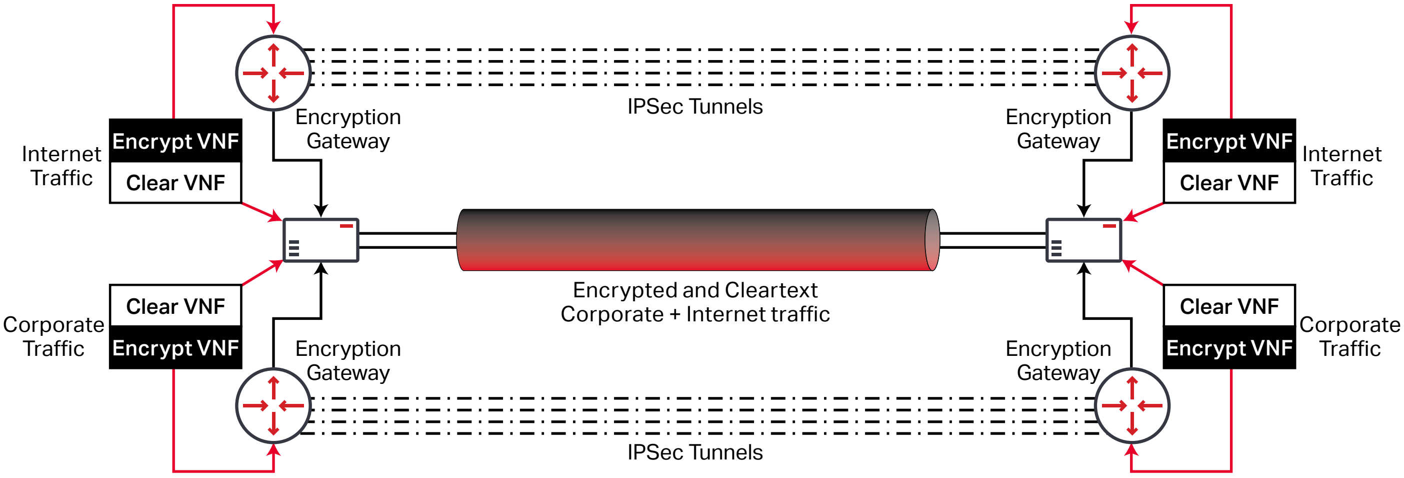

Figure 3. Traffic profiling to reduce cost of the encryption gateway (logical view)

However, there are challenges that come along with traffic profiling, as well. Accurately determining whether traffic should be encrypted can be cumbersome. Few organizations know their own data well enough to accurately separate it, and incorrectly identifying traffic could leave sensitive data unprotected. Application purposes and parameters are often updated, and unless the traffic profile is kept in sync with these changes, it could lead to transmission of sensitive data via unprotected routes.

The key drawbacks of using traffic profiling with encrypted and non-encrypted gateways include:

- Complex network architecture, design, and engineering
- Specialized skills required for operating and managing inter-data center traffic
- High error-rate in profiling traffic as encrypted vs. non-encrypted
- Application profiles and traffic profiles must be consistent and in sync as application uses change over time
- Complex to design and implement Normal/Clear and Encrypted routing instances on the network hardware
- Introduces additional latency between data centers
- Packet layer encryption techniques reduce overall packet throughput
- High cost of encrypted gateway equipment

Scaling traffic profiling of this nature to a global level is extremely challenging, and it is difficult to maintain over time. The traffic profiles for new and existing applications and data sources must be diligently updated to ensure traffic is properly secured. Tight and constant integration between application developers, security engineers, and system and network administrators must be ensured for traffic profiling to succeed.

Both methods of packet layer encryption have their drawbacks with respect to scalability and implementation complexity. Fortunately, a new option exists to reduce complexity and improve scalability by encrypting in-flight traffic at the optical layer.

24/7 data security solutions →

Optical layer encryption: A simple, secure approach

Instead of spending resources to profile and segregate traffic to protect only sensitive data, organizations are increasingly looking to the optical layer for encryption solutions that are easy to implement while offering protection for all data. Encryption at Layer 1, or the optical layer, does just that. It encrypts the entire OTN payload, securing all the messaging, headers, and data from upper layer communications (Figure 4).

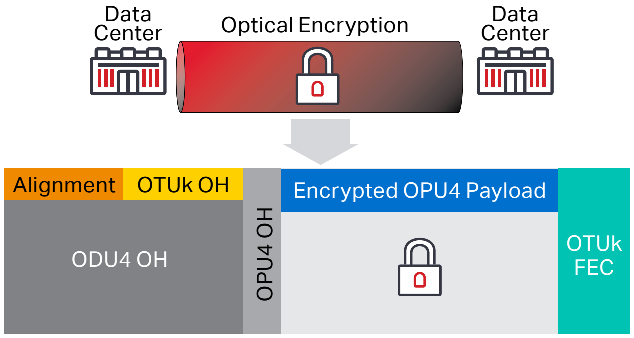

Figure 4. Securing ALL traffic with Layer 1 encryption

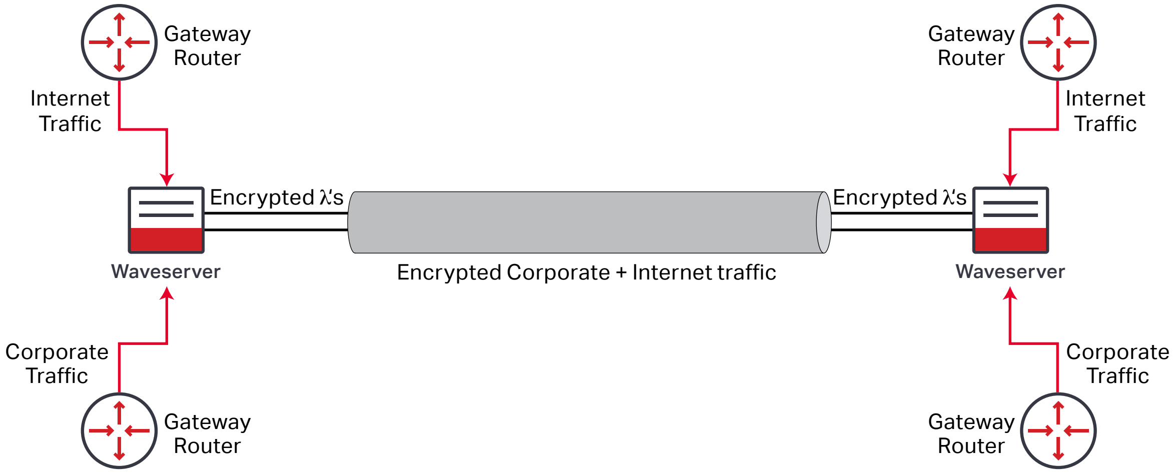

Figure 5. Securing all traffic at the optical layer (logical view)

Encryption at the optical layer simplifies the network architecture (Figure 5). Gateway routers send traffic directly to the transport device (in this case, Waveserver®) for bulk encryption. Expensive encryption gateways are not required, and no traffic profiling is needed to identify which traffic must be encrypted. *All traffic that leaves the data center is encrypted at wire speed with full throughput.*

Layer 1 encryption provides the following benefits:

- **No additional VPN requirements to encrypt traffic—** 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. All communications are secure.
- **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.
- **Full throughput—**Only the transport layer payload is encrypted, so packet layer throughput on routers and switches is unaffected. Layer 1 wire-speed encryption solutions offer full-rate throughput when traffic is encrypted.
- **Simple to build, design, and operate—**Layer 1 encryption solutions are built into the same optical transport systems used to provide DWDM transmission across the metro or the long-haul network; no additional encryption appliances are required.
- **Multi-protocol support—**Layer 1 provides support for multiple types of traffic, including Ethernet, IP, SONET/SDH, Fibre Channel, and more, reducing the number of different encryption appliances required and increasing protocol support over options like IPSec, which is limited to a single protocol (IP).

Moving to Layer 1 encryption provides a simple solution to secure the cloud. It enables bulk encryption for all in-flight data passing across the protected link. Another advantage of Layer 1 encryption is that it can be used as a catch-all at the bottom layer. Security organizations can still develop and engineer upper-layer encryption solutions 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 Layer 1 encryption as a catch-all, depending on where they are in developing their global security policy.

Ciena's WaveLogic Encryption solution

Ciena offers Layer 1 encryption to ensure data is secured with AES-256 encryption algorithms instead of flowing across unsecure, exposed links. Furthermore, if an adversary were to gain access to the physical medium and attempt to tap the fiber, all data would be encrypted and unusable.

Ciena's WaveLogic Encryption provides a simple-to-implement, wire-speed optical encryption solution integrated into optical transport networking equipment. With its set-and-forget approach, encryption is always on, ensuring all data is protected in flight all the time. This eliminates any human error that could result in sensitive data being sent over the network unencrypted.

Ciena's solution provides a FIPS-certified AES-256 encryption engine with support for the latest public key cryptography algorithms, including Elliptic Curve Cryptography (ECC). WaveLogic Encryption is available on Ciena's 6500 Packet-Optical Platform and Ciena's Waveserver family of stackable interconnect platforms, utilizing coherent WDM interfaces that can be programmed to provide wire-speed encryption at a variety of line rates, including: 100G QPSK, 150G 8QAM, 200G 16QAM, and single-carrier 400G.

With Ciena's 6500, operators can utilize an all-in-one muxponder-based card solution for 10G encryption, or pair a 100G/200G line module with encryption to a client interface card, giving the flexibility to meet specific traffic needs. Operators can utilize Waveserver to deploy up to 400G of AES-256 wire-speed encrypted capacity in just 1RU, with the flexibility to support a mix of 10GE, 40GE, and 100GE clients on the same device. With Waveserver Ai, which is optimized for 100GE client interfaces, operators can deploy up to 1.2T of encrypted capacity in a single rack unit.

Line-side programmability built into Ciena's coherent transport 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. This enables secure connectivity between data centers regardless of the distance or underlying photonic line system being used.

Both the 6500 and Waveserver can be deployed to secure the cloud without the complexity associated with higher-level application or IP-based infrastructure solutions. As increasingly more sensitive information gets distributed across fiber-optic networks and more legislation and regulations require data security, today's cloud-based communications must deploy an IT security approach that encompasses not just server security and at-rest encryption, but also a robust in-flight encryption solution.

Effortless encryption. Learn more.

Conclusion

Rolling out a comprehensive security plan can be challenging—especially when considering application-to-application communications between data centers. Organizations often look to the network infrastructure to provide a means to secure data passing between data centers. However, providing network encryption at Layer 3 can be costly and difficult to scale. Fortunately, optical layer encryption provides first-level defense and is simple to implement. It is protocol-agnostic, and can support a variety of traffic types. It provides wire-speed encryption without decreases in throughput under heavy loads, and it introduces almost no additional latency. Layer 1 encryption provides a cost-effective way to protect in-flight data as it passes between data centers, and Ciena's WaveLogic Encryption solution combines a high degree of flexibility and security, with ease of operation and administration. It enables cost-effective, high-capacity, wire-speed encryption to secure communications between data centers all the time—across the street, city, country, or ocean.

The Ciena Community
Get answers to your questions