Sponsored Content

FCW

Protect Data in Transit: A Forward-Thinking Approach

Applying optical encryption to in-flight data can help ensure greater data security.

Agencies have long accepted the importance of data encryption to their cybersecurity efforts. But they might not realize the particular advantages of high-speed encryption, especially when performed at the optical layer.

Relying on encryption at the network layer (Layer 3) has some shortcomings. It can add significant latency and complexity to the network. This is especially true as agencies today require high-availability, time-sensitive communications and applications requiring low latency, such as high-definition video. That's where optical encryption enters the picture.

Federal regulations require data to be encrypted when in transit, whether moving across external or private networks. In most cases, that means complying with the requirements of a number of federal regulations. The tactical approach agencies take to encrypting data in transit depends on several factors—including the type of data they're protecting, internal agency requirements, and how long agencies' data security technologies have been place.

The technologies available for encrypting data in transit have come a long way, but the rapid increase in data rate has not been matched by encryption solutions. Optical encryption solves that problem. Today, more organizations are taking advantage of optical encryption. Performed at the transport layer (Layer 1), optical encryption involves encrypting data packets directly in the path of optical modems. That means data in transit is encrypted as it moves over optical waves across fiber-optic cables. This method works with all protocols, packets, frame sizes, and data types.

Because the encryption takes place at the optical layer inside the modem, all IP packet header information is also encrypted. This helps ensure no sensitive information is left unencrypted. In some cases, the packet header information, which includes who is reading the data and where, is more important than the actual contents of the data. This is different from encryption techniques at other layers.

Lagarto Filmy/ Shutterstock.com

"There has been a more recent focus on data-at-rest encryption strategies because there's a belief that data-in-flight has been solved when in fact it hasn't," says Rob McLaughlin, director of DoD/Special Programs at Ciena. "The legacy approaches to data-in-flight encryption either cannot keep up with the increases in network speeds nor can they offer lower latency required of new applications. That's where optical encryption embedded in the modems brings value."

A BETTER ENCRYPTION APPROACH

Unlike encryption at other layers, which requires adding hardware to the network, optical encryption is part of the modem, which means agencies don't need additional equipment. This improves

availability while drastically reducing latency, complexity, and cost.

Because data is encrypted in the modem, the encryption function does not increase the processing time (latency) at each encryption site. Other technologies do increase latency. In most cases, it travels at line speed in bandwidths from 10 Gbps to 200 Gbps. So when the modem increases speed, so does the encryption. Ciena's optical encryption technology, WaveLogic Encryption, provides wire-speed encryption with 100 percent throughput, contrary to higher layer encryption solutions that can waste a significant amount of bandwidth on encryption overhead.

Besides high availability, strong scalability and ultra-low latency, optical encryption solutions are often less expensive than encryption options that work at higher layers of the network. Not only does optical encryption eliminate additional hardware, but also the maintenance and personnel that go along with that hardware.

Not only does optical encryption eliminate additional hardware, but also the maintenance and personnel that go along with that hardware.

Cybersecurity by the Numbers

16 | The number of cyber-incidents considered "major" by federal agency heads, out of nearly 31,000 incidents

46 | The average amount of days it takes to resolve a cyberattack

50 | The percentage of attacks that will use SSL/TLS encryption to avoid detection

300 | The percentage of increased ransomware attacks nationwide in 2016 over 2015

1,300 | The percentage of increased cyberattacks in federal agencies over the past ten years

4,868 | The number of federal cyberattacks, out of nearly 31,000, reported as web-based or web application-based attacks

21,155 | The average cost of a data breach, per day

3.1 billion | The proposed federal budget for cybersecurity and modernizing IT

Reducing latency also speeds data transport, thus increasing productivity. And faster speeds help better meet service level agreement (SLA) requirements.

Optical encryption is especially useful for latency-sensitive applications, such as high-definition video, which requires a secure, ultra-low latency transport solution. "You can't get lower latency than inside the application specific integrated circuit (ASIC) of a modem," says Kimball. This benefits all applications where high-definition video is important, from telehealth and disaster relief to surveillance and video from drones.

Encryption at layer 1 also more easily accommodates the high speeds and large data sets that other technologies often can't. Any agency working with large data sets can benefit. For example, the amount of data resulting from large research projects, such as those run in high performance computing (HPC) environments, can overwhelm traditional security methods.

Applications requiring secure collaboration and data sharing between participants also benefit from optical encryption. Whether used in videoconferencing, virtual meetings or secure file-sharing, sensitive data must be encrypted before it is shared.

Agencies that routinely transport encrypted data between different locations also are excellent candidates for optical encryption. One example is data sent overseas. Any data leaving our nation's borders must be encrypted and optical encryption techniques work as well on submarine links as terrestrial links. It's also an effective and secure method for transporting Personally Identifiable Information.

THE OPTICAL ENCRYPTION SOLUTION

With benefits like ultra-low latency and high availability, optical encryption makes a lot of sense for agencies wanting to upgrade their data-in-transit

encryption. The first step is looking to NSA guidance on what's acceptable and what isn't, says Shawn Carroll, director of engineering at CenturyLink Federal Solutions.

The next step is narrowing down potential solutions. When looking for an optical encryption solution, agencies need to find one with 24/7, always-on encryption. While some might view the ability to turn off encryption as a benefit, it's extremely dangerous and truly gives cyber thieves the keys to the kingdom. An encryption solution that is software selectable is worse than no encryption at all (since a clever hacker can make you believe you are encrypting, when in fact you are not).

It's also important that the solution use two separate sets of keys for data encryption and authentication. For example, with WaveLogic Encryption, the crypto-management tool is a distinct, separate policy from normal network management. That way, security management can be completely separate from the network management function—which is a security best practice.

Encryption keys should also rotate as fast as possible. Ideally, that means keys should rotate as quickly as once every second, independently, and on each line port. This should not affect traffic or throughput, and should not require user intervention.

Optical encryption should also use the highest available security cryptography algorithms. The most important are Elliptic Curve Cryptography (ECC) algorithms, which many believe is more secure than older public key cryptography systems. The solution should also use a FIPS-certified AES-256 encryption engine and be certified for FIPS 140-2 level 2 or higher.

As the demands for secure data in transit encryption evolve, optical encryption will keep pace.

As the federal government continues to adopt new technologies and deal with new types of data, it must find ways to ensure data in transit continues to be secure and fully encrypted. The rise of internet-connected sensors in everything from HVAC and lighting systems to supply chain components, for example, presents a huge and growing security challenge for government. Encrypting data collected by these sensors at layer 1—the deepest layer possible—is an effective way to control this rapidly growing and vulnerable data.

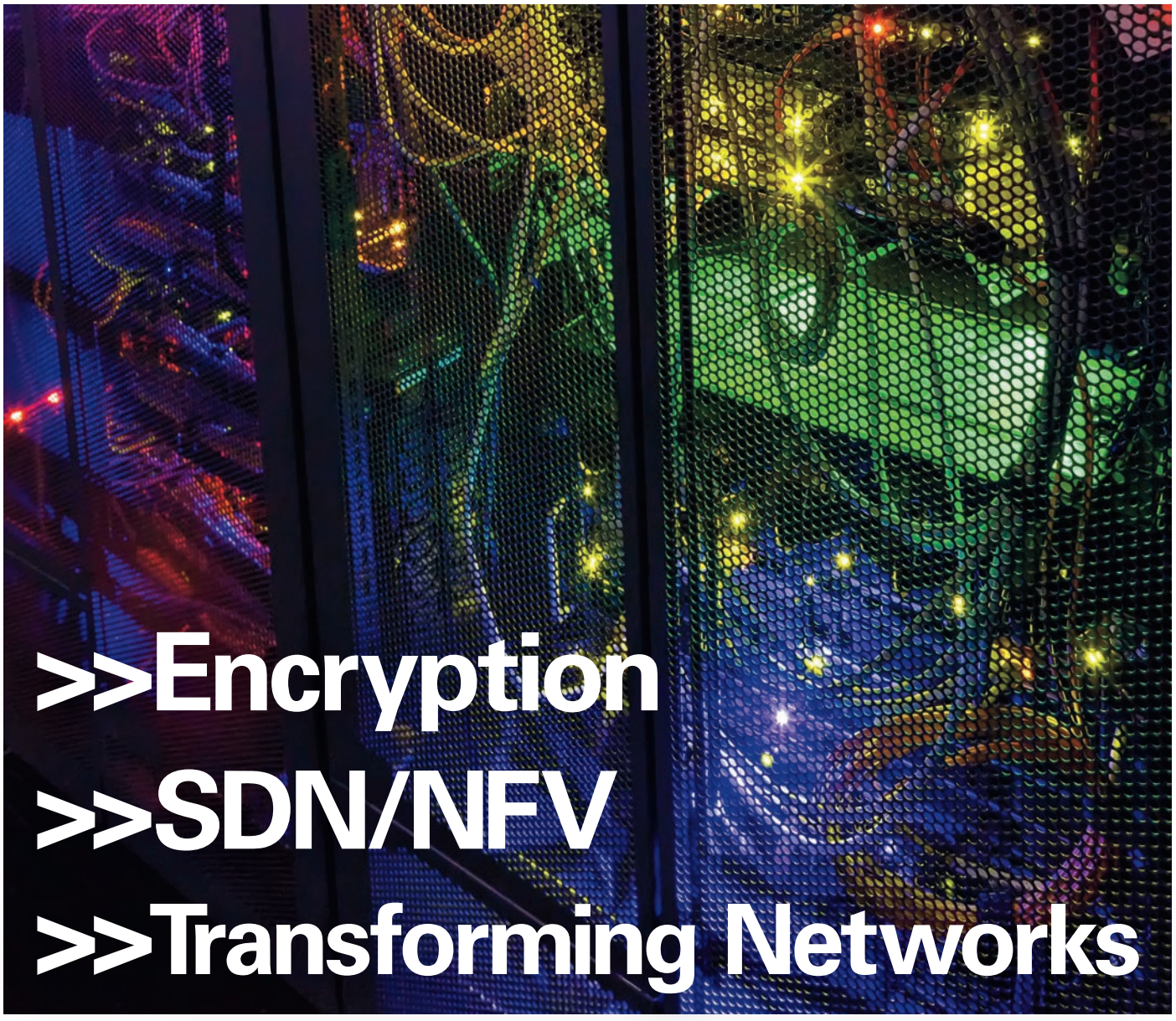
As the demands for secure data in transit encryption continue to evolve, optical encryption technology will keep pace. CenturyLink's Carroll expects products in this category to mature across the board. He also expects more widespread adoption, especially when using optical encryption in conjunction with other encryption methods at other layers. Optical encryption technology is already fairly entrenched in the financial and healthcare markets. Government agencies will catch up as vendors earn required certifications.

Encryption as a Service

As agencies look for ways to reduce costs and ensure application availability and scalability, many are moving from traditional on-premises applications to hosted solutions. It's happening with everything from productivity tools to entire platforms and infrastructures. A Deltek report recently found that federal agencies' use of cloud services will more than double between fiscal 2016 and fiscal 2021.

The "as-a-service" trend even extends to encryption. With the Encryption-as-a-Service (EaaS) model, agencies rely on the encryption technology of a chosen provider for all data encryption needs via the cloud. That means agencies don't have to deploy and manage equipment. More importantly, it also means no downtime or scalability issues. And that is critical. Any amount of downtime can expose agencies to breaches.

When considering Encryption-as-a-Service, make sure your agency retains full control over your encryption security parameters and security keys. One way to do that is using a service that provides a dedicated portal or console that includes easy-to-use management tools. The service should also allow credentialed users to access the portal on any device, from any location.



SOLUTIONS THAT CONNECT THE FEDERAL GOVERNMENT TO THE POWER OF THE DIGITAL WORLD.

Modernizing federal networks requires transformation. Federal agencies' changing mission priorities require a shift in communication network architecture. But economic realities demand these network services in an environment of flat, or even shrinking budgets. Learn how agencies can meet these transformation challenges while balancing budgets and crucial mission needs. **www.TransformingNetworks.com**

ciena
Experience. Outcomes.

CenturyLink®