How PCS Raised the Standard in Securing Law Enforcement Networks

The need for data security over WAN links and augmented segmentation has increased dramatically due to the ever-expanding litany of security threats. It is readily evident that owning your own dark fiber infrastructure is no longer a guarantee for data security. In reaction to this ongoing security threat, the federal government issued new mandatory federal encryption standards for all government agencies. This new set of standards has provided government agencies, like law enforcement, with a prevalent need to stay compliant while juggling the cost and complexity of implementing new infrastructure a difficult problem to solve. Facing this stark new reality, one of the largest Sheriff's Departments in Florida came to PCS for help. The Sheriff's Department was looking for a cost-effective solution that required minimal downtime to implement. Minimizing impact when deploying new technology is key when critical Public Safety related services could potentially be affected. PCS' team of network and security certified engineers sought out the support of two manufacturers who utilized their combination of technology to deliver a robust solution that satisfied our Customer's CJII's FIPS 140-2 encryption requirements, while simultaneously providing them an automated fabric based hyper-segmented solution from Core to Edge.

INDUSTRY

State and Local Government

LOCATION

Florida

TECHNOLOGY PARTNERS

PacketLight

Extreme Networks

The New Wave of Encryption Standards: *Is your CJI Data Encrypted as Per FDLE Requirements?*

Encryption is considered a key technology essential to protecting sensitive data. However, the various number of algorithms and capabilities out on the market for providing encryption lacked one thing: tangible standards. Luckily, the U.S Federal Government identified this issue in the technology market and set forth important security metrics vendors must use for encryption before selling into government agencies. The use of this standard is mandatory for these agencies and is enforced according to the Federal Information Security Management Act (FISMA) of 2002.

What is FIPS 140-2?

Federal Information Processing Standard 140-2 (FIPS 140-2) is a U.S. government information technology security benchmark for validating the effectiveness of cryptographic hardware, software, and firmware solutions. This standard applies to all federal departments and agencies and dictates that all cryptography modules used by these agencies must be FIPS 140-2 certified.

CJIS and FIPS 140-2

5.10.1.2.1 Encryption for CJI in Transit
The Criminal Justice Information Services (CJIS) Security Policy states:

> *"When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI."*
>
> ***- U.S Department of Justice, 2018***

Simplify with Technology

Extreme Connect Beyond the Network

PacketLight Networks

QUICK TIPS:

The NSA's Recommendation:

- Limit access to important systems
- Segment networks and data
- Implement application whitelisting

"A well segmented network means that if a breach occurs, it can be contained…the difference between a contained and uncontained breach is the difference between an incident and a catastrophe."

- Rob Joyce, Chief of Tailored Access Operations
US National Security Agency

Simplify with Technology

Extreme Connect Beyond the Network

PacketLight NETWORKS

THE PACKETLIGHT AND EXTREME NETWORKS SOLUTION

The key to accurately securing data is to extend the encryption from the end-user to the end-system the user is accessing. To achieve this, PCS relied on Extreme Networks and PacketLight Networks to hyper-segment the Sheriff's Departments network while also adding FIPS 140-2 level security on packets traversing through the WAN. With hyper-segmentation, organizations can establish borders to defend against unauthorized lateral movement, reduce their attack profile, deliver highly effective breach isolation, improve the effectiveness of anomaly scanning, and greatly improve the value of specialist security appliances.

PacketLight Networks provides the Federal Information Processing Standard (FIPS) 140-2 Level 2 validation for its state-of-the-art fiber optic networking Layer-1 encryption solutions, awarded by the National Institute of Standards and Technology (NIST).
The encryption solution ensures high-security level of the fiber infrastructure by combining cryptographic protection of the service data flow, firewall, secured management protocols, password-protected role-based user authentication, and optical link power level monitoring. The solution resolves three major concerns in optical link security:

- Confidentiality - preventing disclosure of information to unauthorized parties
- Data integrity - ensuring that the message has not been altered
- Authentication - validating that the parties involved are who they claim to be

Optical link security provides network administrators with the tools to identify fiber tapping by detecting unexplained degradation of the link power. This has made Layer-1 (the physical layer) security a key part of a total cyber-security solution.

The solution performs GCM-AES-256 encryption on Layer-1 of the client signal, supporting full bandwidth of the 1/10/40/100G services. It is compliant with NIST FIPS 140-2 standards and NSA Suite B requirements for GbE/10/40/100Gb Ethernet, as well as 4/8/10/16/32G FC, STM64/OC-192 SONET/SDH, and OTU2/3/4.

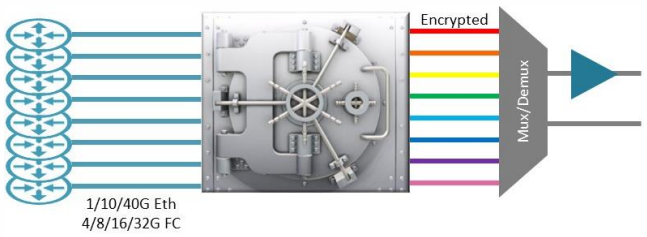

Figure 1: Encryption Mechanism

Extreme Networks augments the security and resiliency by supplanting legacy protocols. Hyper segmentation delivers scale-out service separation and seamlessly traverses the entire organization, from device to data center. With hyper-segmentation, organizations can:

- establish borders to defend against unauthorized lateral movement
- reduce their attack profile
- deliver highly effective breach isolation
- improve the effectiveness of anomaly scanning
- greatly improve the value of specialist security appliances.