DATA CENTER CONNECT SECURITY

A COMPREHENSIVE APPROACH TO PREVENTING, DETECTING AND MITIGATING DATA SECURITY RISKS

STRATEGIC WHITE PAPER

Facing increased security threats and new regulations, enterprises must develop a comprehensive IT security program to address real-time data transfers between data centers. Essential requirements include physical-layer encryption of in-flight[1] data – which can encrypt local area network (LAN), storage area network (SAN) and High Performance Computing (HPC) application data traffic – as well as encryption key management for the security of mission-critical data. The Alcatel-Lucent 1830 Photonic Service Switch (PSS), a best-of-breed wavelength division multiplexing (WDM) platform, along with the Alcatel-Lucent 1830 Key Management Tool (KMT), delivers these requirements to demanding enterprises today. This compelling solution for data center interconnection is capable of encrypting application data in less than 1 µsec, a latency equivalent to only 200 meters of fiber. It also provides today's most comprehensive key management solution to support the automated rotation of encryption keys with end-user control.

[1] In-flight data refers to data traversing a network.

TABLE OF CONTENTS

1 CHALLENGES TO MULTI-SITE DATA CENTER SECURITY

In a world filled with electronic security threats, data centers are at continuous risk. Traditionally, these threats have arisen from malware or hobbyist hackers, but increasingly, criminal organizations are also directly targeting the enterprise. In most cases, the motivation is profit from selling intellectual property or financial information — or even extortion. The Symantec™ Norton™ Cybercrime Report 2011 states: "The global cost of cybercrime is greater than the combined effect on the global economy of trafficking in marijuana, heroin and cocaine."[2]

Many security threats to data centers are internal and perpetrated by legitimate users, usually employees behaving inappropriately. The insider threat is not limited to breaking into network devices. For less than $1,000, a knowledgeable intruder can easily purchase the hardware necessary to eavesdrop on an optical fiber, a capability that was once thought to be impossible. The tap works by bending the optical fiber until it leaks light. The light pulses leaking from the cable can then be detected by an optical photo detector clipped around the optical fiber, without interfering with passing network traffic. This kind of attack is very challenging to discover and can be performed by anyone with physical access to corporate premises.

Recently, virtualization technologies for computing and storage have allowed data center administrators to share resources across multiple data centers. This approach delivers IT services much more efficiently and has the potential to dramatically increase the volume of data traversing an inter-data center network. With this rapid growth in data center connect (DCC) traffic, enterprises must find effective ways to secure the transport of this critical data.

2 CUSTOMER REQUIREMENTS

Multi-site data center security must go beyond technical countermeasures, such as antivirus and firewalls, used inside the data center. A more systematic and holistic approach is needed, including a comprehensive and coordinated counterattack. To enable security across the inter-data center network, the following three approaches to dealing with the threat of information theft can be blended:

- Prevention
- Detection
- Mitigation

[2] Source: Symantec Corp., maker of Norton antivirus software.

Prevention — Infrastructure system security, managed user access and privileged-user access controls are required to prevent misuse of information by legitimate data center users, as well as external hackers. Data center administrators must deploy network equipment from vendors that facilitate the implementation and management of such security practices.

Detection — Embedded security monitoring technology must be deployed in network devices to expose intrusions even when traffic traversing the DCC network is undisturbed. Optical intrusion detection (OID) mechanisms are effective for detecting intrusion on fiber-optic cables and immediately alerting the security administrator of potential security breaches.

Mitigation — Encryption of data is the most effective method of mitigating security breaches. This algorithmic process transforms data into unreadable cryptographic text, so stolen data is rendered useless to an intruder. Encryption is no longer an exotic mechanism whose use is limited to secret organizations: it is now a common tool used for security in normal business workflows. For example, the Payment Card Industry Data Security Standard[3] (PCI DSS), the essential process for protecting credit card payments, uses encryption for data storage and transfer.

Many companies encrypt data at rest[4] and then move the encrypted data between data centers. This manual process may include tape backups and tedious transport of backups using armored vehicles. Often used for disaster recovery, this process has proven to be very difficult to manage and delivers higher-than-expected costs. In addition, data-at-rest encryption does not support the multi-protocol, real-time communications between data centers that enterprises now need to provide business continuity and protect dynamic mission-critical data.

2.1 Secure Layer 1 traffic encryption

Physical-layer encryption is the most effective method for securing in-flight data transmitted between a local and a remote enterprise data center. It provides encryption with transparent connectivity to support all upper-layer Open Systems Interconnection (OSI) protocols and applications, including data mirroring, Virtual Machine (VM) mobility and storage virtualization — all with ultra-low latency and high bandwidth to meet today's enterprise requirements. Layer 1 (L1) encryption also lowers the total cost of ownership (TCO) for data center interconnection by allowing the convergence of LAN, SAN and HPC traffic onto a single L1 physical medium and by significantly simplifying management of the secure network infrastructure. With increasing demand for data center interconnection worldwide, enterprises can build secure, scalable, high-performance private cloud interconnects, based on L1 encrypted links over fiber using DWDM technology. The fiber can be owned (private builds) or leased from service providers.
While encryption in the higher layers of the OSI network stack can be effective in certain situations, it is complex and costly — resulting in high CPU utilization and increased latency and overhead in the underlying data and application flow. It can also suffer from problems with compatibility between OSI network layers.

[3] Source: Payment Card Industry Data Security Standards Council, *PCI DSS v2.0*, October 2010.
[4] Data at rest refers to data stored in computers.

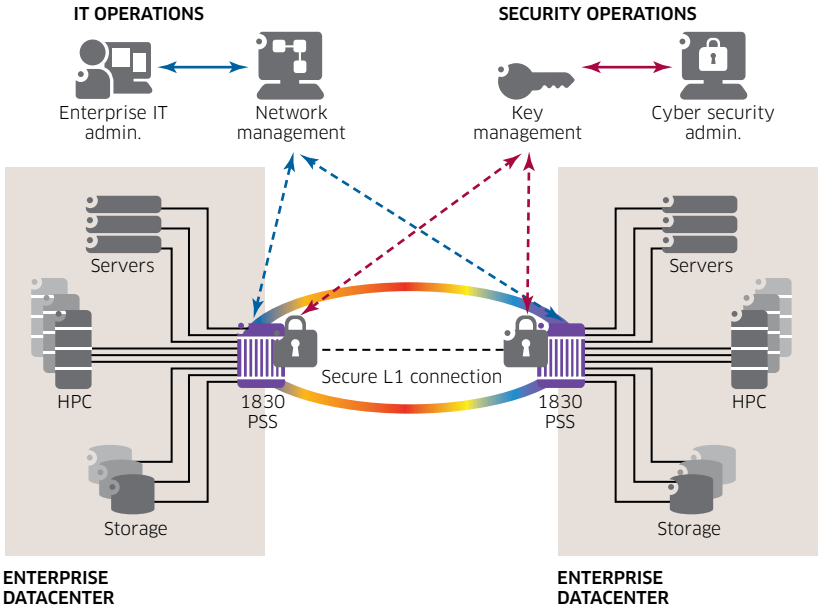
2.2 Managing encryption keys

Mismanagement of encryption keys, required to enable encrypted data transport, can deny system access to authorized clients or even cause inter-data center traffic interruption, which could affect critical enterprise business applications. Often, complex key management is implemented using manual processes which introduce enterprise security vulnerabilities and risk. Ultimately, data center administrators require a secure, encrypted DCC solution with comprehensive management of associated encryption keys over their entire life cycle.

3 SECURING DCC WITH THE ALCATEL-LUCENT 1830 PHOTONIC SERVICE SWITCH

As shown in Figure 1, the Alcatel-Lucent 1830 Photonic Service Switch (PSS) provides the prevention, detection and mitigation capabilities enterprises need to establish and deploy effective data center security practices.

Figure 1. Secure L1 data center connect



3.1 Preventing security attacks

To reduce the attack surface and, therefore, the security risk, the Alcatel-Lucent 1830 PSS can function in “secure mode”, which provides a hardened device configuration with the following configuration settings:

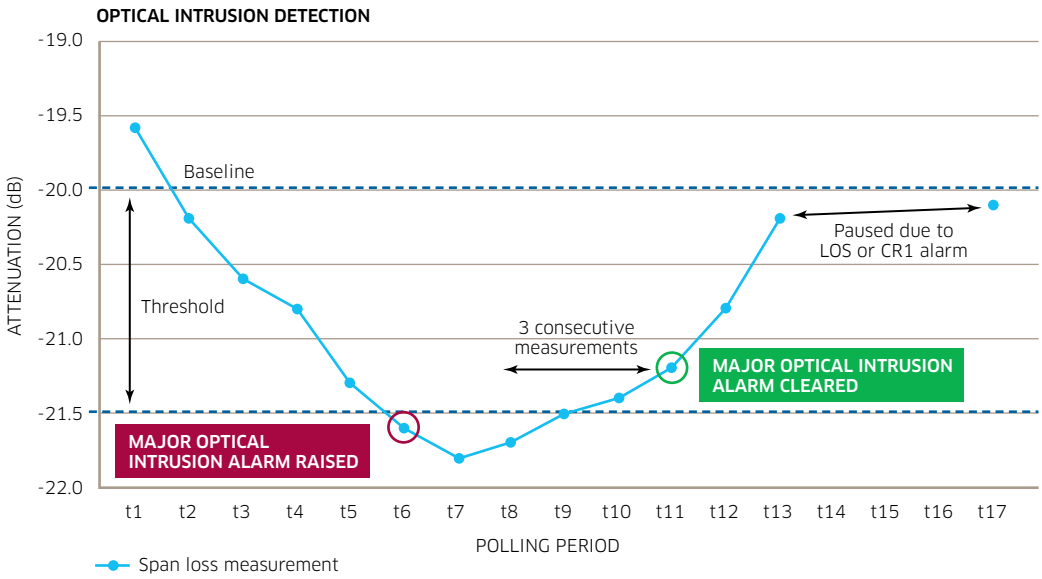
- Only the essential logical and physical ports needed to manage the system are open.
- Software debug functions are disabled.
- Services of the embedded OS are disabled, as well as any interactive OS access.
- Only secure network element management protocols, such as Secure Sockets Layer (SSL) and SNMPv3, are supported.

General security risks can also be related to inadequate security policies or human factors. To reduce these risks, enterprises must adopt systematic approaches to risk management, such as ISO/IEC 27001[5] (for ISMS), or auditing frameworks such as Statement of Auditing Standards No. 70 (SAS 70).[6] Enterprise security processes can rely on well-designed security controls that properly ensure the confidentiality, integrity and availability required of products used in the data center. To promote these crucial principles, the Alcatel-Lucent coordinated approach to data center security is based on the requirements of security best practices and security frameworks widely used in data center environments.

3.2 Detection of security breaches

The Alcatel-Lucent 1830 PSS provides several security mechanisms to ensure the integrity of data communication services across the DCC network — and of the DWDM equipment itself. Comprehensive security logs allow an administrator to detect non-authorized changes to the device configuration, complemented by real-time alarms to detect optical intrusion. The optical intrusion detection (OID) capability constantly checks the status of each optical fiber by monitoring for changes in optical loss. First, a threshold value is set up, ranging from 1.0 dB to 3.0 dB, with steps of 0.5 dB. Then, if the optical loss changes beyond the configured level, an alarm identifies a possible optical intrusion, as shown in Figure 2.

Figure 2. Optical Intrusion Detection (OID)



[5] ISO/IEC, ISO/IEC 27001: *Information technology — Security techniques — Information security management systems — Requirements.*
[6] Auditing Standards Board of the American Institute of Certified Public Accountants, SAS 70: *Service Organizations*, April, 1992.

3.3 Reducing the risks associated with stolen data

To perform symmetric Layer 1 encryption, the Alcatel-Lucent 1830 PSS implements the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES)7 block encryption/decryption algorithm (cipher). This cipher encrypts rapidly and is extremely difficult to break when large encryption key sizes are implemented. It's called symmetric because the same pre-shared keys are used for encryption and decryption of the blocks at each end of the circuit.

The Alcatel-Lucent 1830 PSS uses integrated hardware and large, robust 256-bit AES keys to encrypt data flows and transport information securely. Working at a 10-Gb/s line rate, its L1 encryption hardware introduces less than 1µsec latency (equivalent to approximately 200 meters of fiber) into the end-to-end data stream.

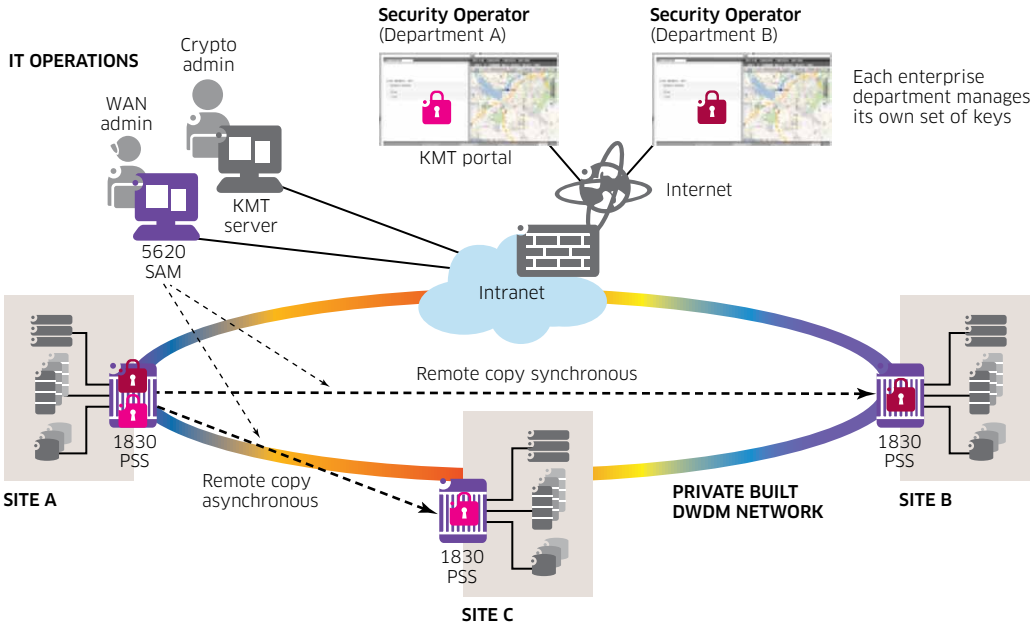
The Alcatel-Lucent 1830 PSS encryption module was designed and tested using FIPS 1402 standards8, including detailed requirements for strong cryptographic algorithms and physical device protection from NIST.

4 MANAGING DWDM ENCRYPTION WITH THE ALCATEL-LUCENT 1830 KEY MANAGEMENT TOOL

The Alcatel-Lucent 1830 Key Management Tool (KMT) is a secure, scalable solution for managing keys across both simple and complex encryption deployments for inter-data center connections. It helps manage the cryptographic life cycle of each encrypted wavelength service — the keys generated to perform the encryption — as well as encryption key expiration, rotation and destruction. These operations are all essential to encrypted inter-data center communication.

Figure 3 shows a secure enterprise L1 inter-data center configuration, using the 1830 KMT to manage the shared symmetric encryption keys.

Figure 3. Alcatel-Lucent 1830 Key Management Tool for encrypted L1 encrypted L1 DCC

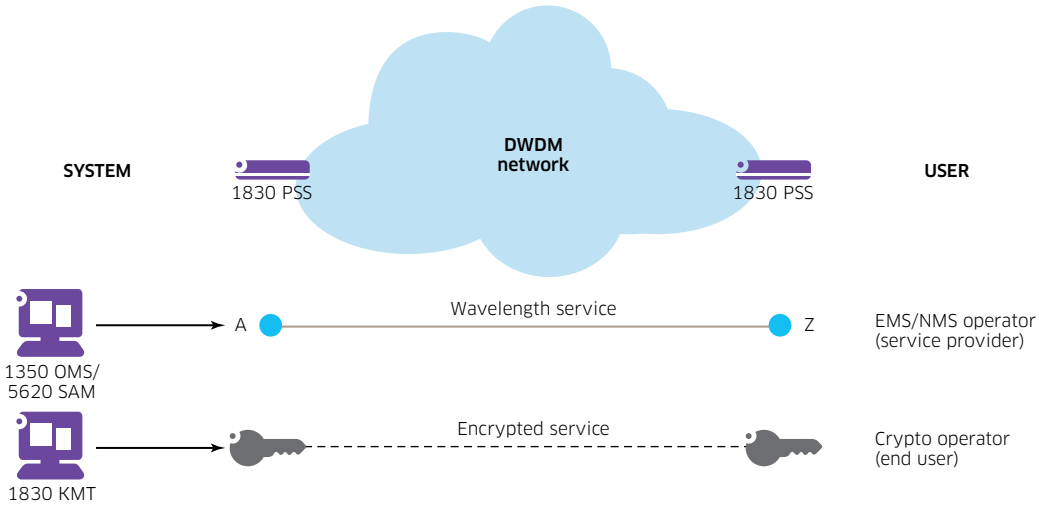


With the Alcatel-Lucent 1830 KMT, an enterprise IT organization can offer managed infrastructure services to its internal customers and stakeholders, while allowing them to keep full ownership and control of their own cryptographic keys and encryption parameters. This tool also provides critical support when unique encryption keys must be used between each sender-and-receiver pair within the enterprise, and these keys are rotated frequently as part of encryption security best practices.

4.1 Role-based, compliant authentication and authorization

Role-based Access Control (RBAC) authorization mechanisms grant permissions to perform certain operations in a computer system, based on the user's role in the organization. The Alcatel-Lucent 1830 KMT supports a Federal Information Processing Standard (FIPS)-compliant RBAC authorization mechanism that provides separation of IT security duties for device management, as well as the underlying encryption services offered by the device, as shown in Figure 4.

Figure 4. Alcatel-Lucent 1830 KMT FIPS-compliant RBAC authorization mechanism



- FIPS 140-3 Level 2 compliance requires standalone software tool for cryptographic functions.
- 1830 KMT fits service provider/ enterprise model that requires separate network and security management/monitoring modules.
  - ¬ Separate groups are responsible for security ("crypto" officer) and network devices (network administrator).
  - ¬ Alcatel-Lucent 1350 Optical Management System (OMS) or 5620 Service Aware Manager (SAM) manages wavelength service.
  - ¬ 1830 KMT manages crypto aspects of wavelength service.

To provide centralized authentication and authorization profiles for an enterprise, the Alcatel-Lucent 1830 PSS uses a standard Remote Authentication Dial-In User Service (RADIUS) interface, which supports third-party integration of corporate identity management systems (IDMS) and multifactor authentication systems.

5 CONCLUSION

As enterprises consolidate their data center assets and invest in next-generation private and public cloud infrastructure, a comprehensive IT security program is required. The ideal approach to data center interconnection meets strict requirements for latency and security, as well as operations, administration and maintenance (OA&M). It also combines prevention, detection and mitigation methods to create a comprehensive response to security threats and to regulation. Physical layer encryption offers security for all in-flight data types, including LAN, SAN and HPC applications between remote data center locations.

The Alcatel-Lucent Optical Data Center Connect solution delivers the scalability, versatility, and security required for next-generation private and public cloud transport, across metro and long-haul distances. It supports high-speed optical WDM connectivity between data centers and, unlike other alternatives, it enables enterprises to deploy high-bandwidth and low-latency encrypted wavelength services with end-user key control. This FIPS-compliant solution satisfies enterprise DCC security requirements without compromising the low, predictable latency required by most mission-critical applications. With operations in more than 130 countries and one of the most experienced global services and support organizations in the industry, Alcatel-Lucent is a local partner with global reach. Visit the Alcatel-Lucent web site at www.alcatel-lucent.com.

6 ACRONYMS

1350 OMS	Alcatel-Lucent 1350 Optical Management System
1830 PSS	Alcatel-Lucent 1830 Photonic Service Switch
1830 KMT	Alcatel-Lucent 1830 Key Management Tool
5620 SAM	Alcatel-Lucent 5620 Service Aware Manager
AES	Advanced Encryption Standard
BCP	Business continuity plan
CPU	Central processing unit
DCC	Data Center Connect
DSS	Data Security Standard
DWDM	Dense Wavelength Division Multiplexing
E-SNCP	Extended Sub-Network Connection Protection
FC	Fibre Channel
FIPS	Federal Information Processing Standard
GMPLS	Generalized MPLS
HPC	High Performance Computing
ISMS	Information security management system
IT	Information technology
KMT	Alcatel-Lucent Key Management Tool
L1	Layer 1
LAN	Local area network
MPLS	Multi-Protocol Label Switching
NAS	Network-attached storage
NE	Network element
NIST	National Institute of Standards and Technology
OA&M	Operations, administration and maintenance
OID	Optical intrusion detection
OLP	Optical Line Protection
OMSP	Optical Multiplex Section Protection
OS	Operating system
OSI	Open Systems Interconnection
PCI	Payment Card Industry
QoE	Quality of Experience
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service

RBAC	Role-Based Access Control
SAN	Storage area network
SAS 70	Statement of Auditing Standards No. 70
SLA	Service Level Agreement
SNMPv3	Simple Network Management Protocol version 3
SSL	Secure Sockets Layer
T-ROADM	Tunable and Reconfigurable Optical Add-Drop Multiplexer
TCO	Total cost of ownership
VM	Virtual Machine
WAN	Wide area network
WUI	Web user interface

7 REFERENCES

1. Alcatel-Lucent 1830 PSS: www.alcatel-lucent.com/1830
2. Alcatel-Lucent 100G: www.alcatel-lucent.com/100g-coherent/index.html
3. Auditing Standards Board of the American Institute of Certified Public Accountants. SAS 70: Service Organizations. April 1992 http://sas70.com/sas70_overview.html
4. InfiniBand Trade Association. The InfiniBand Architecture. http://www.infinibandta.org/content/pages.php?pg=technology_download
5. ISO/IEC. ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements. http://www.iso27001security.com/html/27001.html
6. National Institute of Standards and Technology. FIPS Publication 140-2: Security Requirements for Cryptographic Modules. May 25, 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
7. National Institute of Standards and Technology. FIPS Publication 197: Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
8. Payment Card Industry Data Security Standards Council. PCI DSS v2.0. October 2010. www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0
9. Symantec – Norton. Norton Cybercrime Report 2011. http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/