SECURE SOLUTIONS FOR DATA CENTER CONNECT

TECHNOLOGY WHITE PAPER

Responding to increasing security threats and regulation, enterprises face a range of challenges in providing a comprehensive IT security program. Organizations are now shifting to the real-time transfer of data between data centers, and implementing on-the-fly data encryption with key management for security. Physical Layer encryption is the preferred method for securing data across the data center connect (DCC) WAN, deployed across optical fiber and DWDM for converged LAN and SAN traffic. Optical DWDM solutions enable the highest throughput for DCC at the lowest TCO.

The Alcatel-Lucent 1830 Photonic Service Switch (PSS) is a best-of-breed DWDM platform, and the integrated physical layer encryption lowers data center security risks and increases data confidentiality, integrity and availability.

TABLE OF CONTENTS

1. INTRODUCTION TO DATA CENTER SECURITY

In the face of a world filled with security threats, companies are recognizing that their data centers are at continuous risk. Security threats to the data center arise not just from traditional malware or hobbyist hackers, but increasingly from criminal organizations that are directly targeting the enterprise. In most cases, the motivation is monetary 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."[1]

Data center security is not just about technical countermeasures such as antivirus and firewalls, but a much more systematic and holistic approach to enterprise-wide security. Enterprises must establish comprehensive IT security programs that include information security management systems (ISMSs) to achieve corporate or regulatory compliance.

2. DATA CENTER CHALLENGES

Although data center operators and service providers recognize the importance of security, their first priority in recent years has focused on the addition of servers, storage and software to cope with new anywhere/anytime business requirements. These application and computing resources have been clustered across distributed geographic locations for the more efficient delivery of IT services. In addition, enterprises in all sectors have been forced to deal with a deluge of data, managing massive sets of information that they need to collect, filter, aggregate, correlate encrypt and store. The processing of such large, distributed data sets — so called "big data" — requires low latency and high bandwidth from the hardware and networks used to connect data centers and end users.

Technologies such as virtualization have the potential to dramatically increase the amounts of data traversing a network. Moving Virtual Machines (VMs) dynamically across a metro or long-haul WAN from one host or storage cluster to another can result in application delays and congestion. Such activity over large geographic distances can also result in a loss of revenue from underperformance on Service Level Agreements (SLAs) or failure to meet business continuity plan (BCP) requirements.

For distributed resources to work effectively, applications require secure, real-time communication. With rapid growth in traffic, sensitivity to transmission latency poses an increasing challenge in applications that rely heavily on storage area networks (SANs), virtualization and BCP. Applications such as data replication, as well as the mirroring of real-time/mission-critical applications, also require scalable bandwidth, Quality of Service (QoS), and ultra-low latency from a secure data center connect (DCC) solution.

[1] *Symantec Norton Cybercrime Report 2011*. 1 *Symantec Norton Cybercrime Report 2011*.

3. SECURE DCC

Encryption is the algorithmic process of transforming data into unreadable cryptographic text. Encryption is no longer an exotic mechanism whose use is limited to secret organizations: it is a common tool used as part of normal business workflows for security. For example, the Payment Card Industry Data Security Standard[2] (PCI DSS) is the essential process for protecting credit card payments, using encryption for data storage and transfer.

Many companies are continuing to use offline encryption to move data between data centers, requiring a manual process that may include tape backups and transport using armored vehicles. Deployed frequently for disaster recovery, the cost of this process has proven to be higher than expected, and offline encryption does not support the required real-time communications between data centers. Companies are now shifting to the real-time transfer of data between data centers, with on-the-fly encryption for security in this always-on world.

3.1 Layer 1 encryption

While encryption in the higher layers of the Open Systems Interconnection (OSI) network stack can be effective in certain situations, such encryption can be complex — resulting in high CPU utilization, increased latency and overhead — and can suffer from problems with compatibility between OSI network layers. Layer 1 (L1) physical layer encryption is therefore the preferred method for securing data across the DCC WAN. Using dedicated hardware, L1 encryption can closely couple any higher-layer data flow with its transmission medium: typically over an optical fiber with Dense Wavelength Division Multiplexing (DWDM) to maximize the data center interconnection capacity and DCC performance.

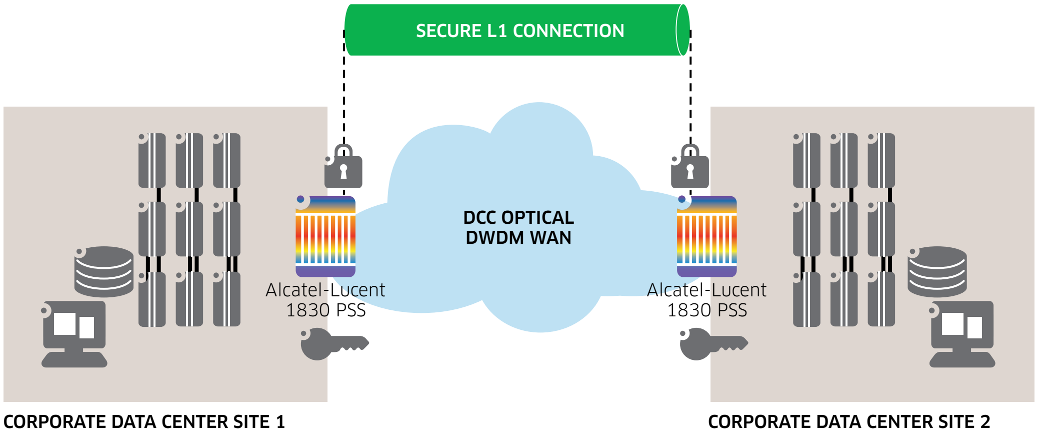
Optical fiber was once considered secure on its own because of the inherent difficulty of tapping into glass media and reading light signals. However, new technologies that tap into the fiber and read the data flow are now available. L1 encryption provides protection against this new threat, along with transparent connectivity to support all upper-layer protocols and applications, including firewalls, all with ultra-low latency and high bandwidth. L1 encryption also supports lowering the DCC total cost of ownership (TCO) by allowing the convergence of LAN and SAN traffic onto L1 media. With increasing demand from data centers worldwide, service providers are increasing the availability of dark fiber and/or leased wavelength services to accommodate these L1 encrypted links across the DCC WAN.

[2] Payment Card Industry Data Security Standards Council, *PCI DSS v2.0*, October 2010.

3.2 Managing encryption keys

Supporting a secure, encrypted DCC solution also requires the management of associated encryption keys over their life cycle — a process that is complex and that may introduce other security vulnerabilities and risks. For example, a single mismanagement of encryption keys may deny system access to authorized clients or even cause a DCC traffic interruption.

Figure 1. Secure L1 DCC



4. OPTICAL DWDM WITH THE ALCATEL-LUCENT 1830 PHOTONIC SERVICE SWITCH

Optical DWDM transport is the leading technology to meet DCC requirements for the transport and delivery of new virtual services. Optical DWDM is the only solution that enables:

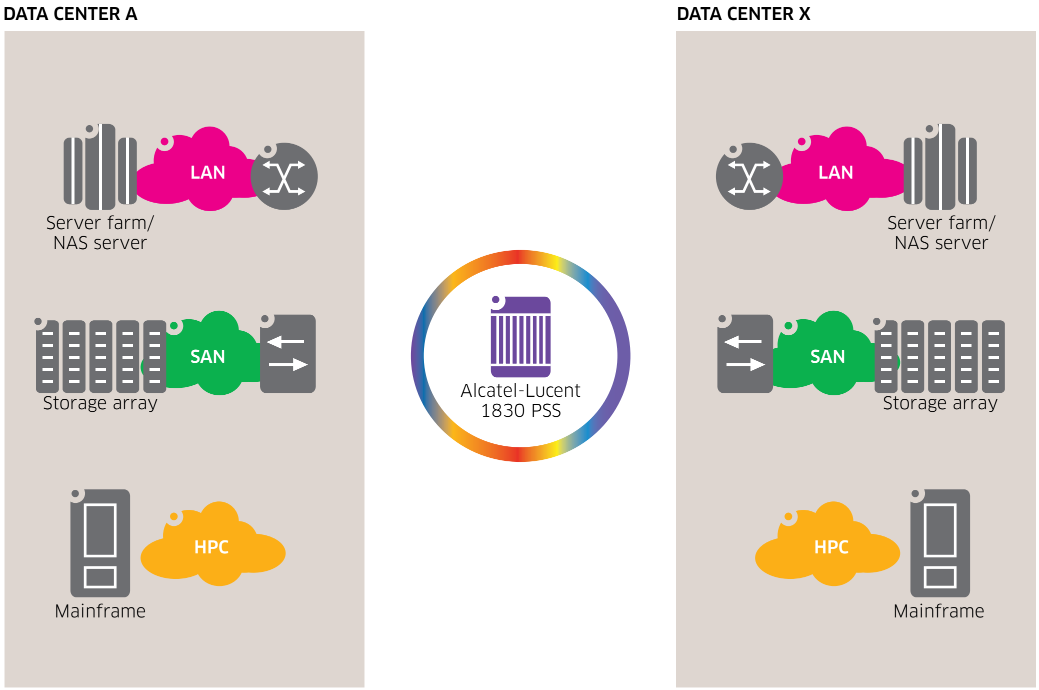
- Full network flexibility and adaptability at speeds of 100G and beyond
- Quick service turn-up to meet changing bandwidth requirements
- Ultra-low latency connectivity
- Transport-grade reliability for protocol-independent data

Ultimately, optical DWDM solutions enable the highest throughput for DCC at the lowest TCO for service providers.

4.1 100G coherent transport on a single carrier

Alcatel-Lucent is a worldwide leader in optical transport. Leveraging years of innovative Alcatel-Lucent Bell Labs research and internal development, the Alcatel-Lucent 1830 Photonic Service Switch (PSS) is the industry's first DWDM platform to deliver 100G coherent transport on a single carrier. The Alcatel-Lucent 1830 PSS is a scalable optical DWDM platform that supports data center aggregation for Ethernet, Fibre Channel (FC) and InfiniBand®[3] data sources, as shown in Figure 2. Services can then be dynamically and flexibly transported over metro and long-haul spans using Tunable and Reconfigurable Optical Add-Drop Multiplexers (T-ROADMs) for optical wavelengths.

Figure 2. DCC with the Alcatel-Lucent 1830 PSS



4.2 Optimized DCC across metro and long-haul networks

The communication capabilities of the Alcatel-Lucent 1830 PSS are further enhanced with a complete Ethernet feature set that supports L2 services over the optical infrastructure and a Generalized Multi-Protocol Label Switching (GMPLS) control plane that enables the automated setup, provisioning and restoration of services. In addition, built-in encryption addresses secure communications for mission-critical applications over public and private/hybrid clouds. The Alcatel-Lucent 1830 PSS provides the features required to optimize DCC across metro and long-haul networks.

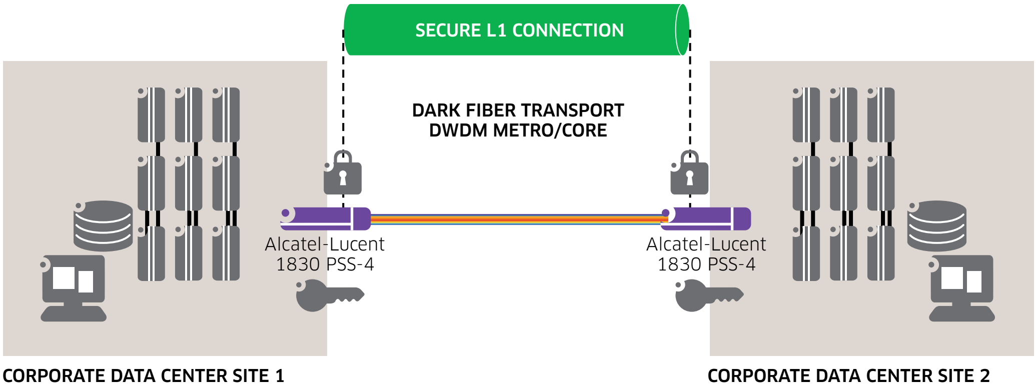
Integrated L1 hardware for on-the-fly encryption enhances the capabilities of the Alcatel-Lucent 1830 PSS by providing strong and transparent DCC encryption. This integration decreases TCO by enabling security on the same network element (NE) that performs the DWDM and T-ROADM roles.

[3] InfiniBand Trade Association, *The InfiniBand Architecture*.

5. SECURE DCC WITH THE ALCATEL-LUCENT 1830 PSS

The Alcatel-Lucent Secure Data Center Connect Solution is designed to address both enterprise and service provider requirements. In its simplest point-to-point configuration, a secure L1 DCC can be configured with a pair of Alcatel-Lucent 1830 PSS platforms connected to an owned or leased dark fiber as the physical media between data center sites, as shown in Figure 3.

Figure 3. Dark fiber for secure encrypted L1 transport



DWDM wavelength and encryption services can be provisioned for this configuration using the Alcatel-Lucent 1830 PSS web user interface (WUI) and a Simple Network Management Protocol version 3 (SNMPv3) graphical tool that supports user-friendly management of the integrated transport and encryption devices. Working at a 10G line rate, the L1 encryption hardware in the Alcatel-Lucent 1830 PSS introduces less than 10µs latency to the end-to-end data stream.

5.1 Centralized, compliant authentication and authorization

Role-Based Access Control (RBAC) authorization mechanisms provide a Federal Information Processing Standard (FIPS)-compliant separation of duties for both the element management and the encryption services. With a standard Remote Authentication Dial-In User Service (RADIUS) interface, the Alcatel-Lucent 1830 PSS can support third-party integration of corporate identity management systems and multifactor authentication systems, providing for centralized authentication and authorization profiles.

5.2 Network and key management

For the complex security scenarios inherent in a service provider infrastructure model, Alcatel-Lucent offers a network management system suite and the Alcatel-Lucent Key Management Tool (KMT). The Alcatel-Lucent KMT is a secure, scalable application that supports management of the cryptographic life cycle of each wavelength service — the keys generated to perform the encryption — as well as the management of encryption key expiration, rotation and destruction.

The Alcatel-Lucent KMT enables a service provider to offer managed infrastructure services to customers while allowing them to keep ownership and control of the cryptographic keys and encryption parameters for the services they are using. The Alcatel-Lucent KMT is necessary to support the complexity and scalability in these scenarios: unique encryption keys must be used between each sender and receiver, and these keys are frequently rotated as part of encryption security best practices.

6. MANAGING RISK FOR SECURE DCC WITH THE ALCATEL-LUCENT 1830 PSS

Security threats refer to both physical and logical dangers that, if an incident occurs, can adversely impact data center operations. DCC transport risks arise from the uncertainty that vulnerabilities could be exploited and result in the likelihood of damage and/or removal of sensitive data or assets. To reduce the attack surface, and therefore the security risk, the Alcatel-Lucent 1830 PSS can be enabled to function in secure mode, which provides a hardened device configuration with these 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 NE management protocols such as Secure Sockets Layer (SSL) and SNMPv3 are supported

General risks can also be related to inadequate security policies or human factors. To reduce these risks, many services providers are adopting systematic approaches to risk management, such as ISO/IEC 27001[4] (for ISMS) or auditing frameworks such as Statement of Auditing Standards No. 70 (SAS 70).[5] Services provider processes often rely on well-designed security controls that properly ensure the confidentiality, integrity and availability (CIA) that is required on products used in the data center. The Alcatel-Lucent Secure Data Center Connect Solution supports the CIA principle with several security features based on the requirements of security best practices and common security frameworks used in data center environments.

6.1 Data confidentiality

The Alcatel-Lucent 1830 PSS implements the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES)[6] block cipher to perform symmetric Layer 1 encryption. This cipher can encrypt data very quickly, and it is extremely difficult to break when large key sizes are used. The Alcatel-Lucent 1830 PSS uses integrated hardware and robust 256-bit AES keys to encrypt data flows and deliver securely transported information. Because encryption and decryption of the blocks is done using the same key in the devices and keys, the algorithm is called symmetric.

The Alcatel-Lucent 1830 PSS encryption module was designed and tested using FIPS 1402 standards[7], including detailed requirements for strong cryptographic algorithms and physical device protection from NIST.

[4] ISO/IEC, ISO/IEC 27001: *Information technology — Security techniques — Information security management systems — Requirements*
[5] Auditing Standards Board of the American Institute of Certified Public Accountants, SAS 70: *Service Organizations*, April 1992
[6] National Institute of Standards and Technology, FIPS Publication 197: *Announcing the Advanced Encryption Standard (AES)*
[7] National Institute of Standards and Technology, FIPS Publication 140-2: *Security Requirements for Cryptographic Modules*, May 25, 2001

6.2 Data integrity

Data integrity means detecting and avoiding unauthorized access or data modification. The Alcatel-Lucent 1830 PSS provides several security mechanisms to ensure the integrity of data communication services across the DCC and for the equipment itself. Comprehensive security logs allow an administrator to detect non-authorized changes to the device configuration, complemented by real-time intrusion prevention alarms. The optical intrusion detection (OID) capability constantly checks the status of each optical fiber by monitoring for changes in optical loss. A threshold value (from 1.0 dB to 3.0 dB, with steps of 0.5 dB) can be set up to raise an alarm for a possible optical intrusion when the optical loss changes beyond the configured level.

6.3 Data availability

Availability ensures that the DCC service is operating regardless of failures or disruptions in the network. Optical technologies provide the highest level of availability for DCC operations and are therefore considered as the most reliable infrastructure for supporting BCPs and disaster recovery plans. The Alcatel-Lucent 1830 PSS offers complete hardware redundancy as well as diverse optical DWDM protection schemes such as Y-cables, Extended Sub-Network Connection Protection (E-SNCP), Optical Multiplex Section Protection (OMSP) and Optical Line Protection (OLP). These mechanisms provide fault recovery from fiber, amplifier or Reconfigurable Optical Add-Drop Multiplexer (ROADM) failures.

7. CONCLUSION

The undisputable trend toward virtual and distributed applications and data presents opportunities and challenges for service providers. DCC delivers the end-user Quality of Experience (QoE), scalability and flexibility required for virtual computing and storage across metro and long-haul transport infrastructures. Ideal approaches for data center interconnection must meet strict requirements for latency, operations, administration and maintenance (OA&M) and security. In particular, data center security aspects such as data encryption and key management are important elements of an organization's response to security threats and regulation.

These DCC security challenges can best be addressed with the Alcatel-Lucent Secure Data Center Connect Solution, designed to flexibly support the full range of DCC requirements. The Alcatel-Lucent Secure Data Center Connect Solution supports high-speed optical DWDM connectivity between data centers and enables service providers to deploy high-bandwidth and low-latency encrypted services. This infrastructure delivers the fixed and predictable latency required for DCC, without traffic loss and with high reliability.

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.

8. ACRONYMS

1830 PSS	Alcatel-Lucent 1830 Photonic Service Switch
AES	Advanced Encryption Standard
BCP	business continuity plan
CIA	confidentiality, integrity and availability
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

9. REFERENCES

1. Alcatel-Lucent 1830 PSS: www.alcatel-lucent.com/1830
2. Alcatel-Lucent 100G: www.alcatel-lucent.com/100g
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/

Alcatel·Lucent