TECHNOLOGY WHITE PAPER

Optical Network Encryption – a New Key to Data Security

Authors:
Dr. Michael Ritter and Christian Illmer,
ADVA Optical Networking

Data security is not a single feature, but rather an increasingly important set of technologies, used to safeguard private data sent across both public and private networks. The proliferation of data requiring protection – whether internal corporate data or records containing information on customers or other associates – means there is more data at risk of being compromised than ever before.

This, in conjunction with the increasing cost of a data breach, measured in both hard-dollar terms like legal settlements and soft costs such as loss of customer loyalty, makes the intelligent use of data protection technologies increasingly necessary for organizations of all sizes.

According to studies from the SANS Institute, data theft through interception is on the increase and set to rise even more dramatically in the upcoming years. Despite a reputation for being more secure than standard wiring or airwaves, the truth is that fiber cabling is just as vulnerable to technical hacks.

The misconception about fiber's security is largely due to the lack of public reports on fiber hacks – but they still happen. Several years ago, three main Deutsche Telekom trunk lines were breached at Frankfurt Airport in Germany. In the United States, an illegal eavesdropping device was discovered hooked into Verizon's optical network. Other international incidents include optical taps found on police networks in the Netherlands and Germany, and on the networks of pharmaceutical giants in the U.K. and France. Reports on these high-profile fiber intrusions offered few details. For the most part, hacks typically go unreported, and often undetected.

Unique issues must be considered when including data security aspects into data backup and disaster recovery solutions. These specific issues need to be understood and integrated into an organization's broader business continuity plans.

The Business Need

Since the days of the Roman army, military organizations have tried to protect intelligence information. Today, enterprises of all sizes manage intelligence information. Any business that has a product or service for sale handles and stores personal customer information – from names and addresses to more sensitive information like social security numbers, bank account and credit card numbers.

For most companies, the amount of information they retain has grown steadily over the years, and the need for privacy of that information has also evolved.

Unfortunately, many companies have failed to recognize that as the amount of information they retain has grown, so has the risk to which they are exposed. Consider the example of a bank and the full breadth of customer information that it maintains. Detailed information on customer accounts and transactions is potentially far more valuable and vulnerable than an armored car full of cash.

... the wide-scale adoption of cloud computing applications for processing, hosting and especially data storage increases the amount of sensitive data sent across networks.

Additionally, the wide-scale adoption of cloud computing applications for processing, hosting and especially data storage increases the amount of sensitive data sent across networks. Traditionally stored and processed in company-owned private data centers, personal and business-critical information is now more frequently than ever before transported across shared network resources connecting company facilities with the locations of cloud computing resources.

The costs associated with data loss can be almost unimaginably high. Any loss of data exposes a company to severe damage to its customer relationships and can create a huge distraction to running the business. It establishes potential legal liability for subsequent losses experienced by customers, infringes regulatory compliance and virtually guarantees significant damage to the company's reputation.

Protecting Data from Theft

Over the years, several approaches have evolved to protect valuable enterprise data from theft and tampering. In addition to the actual security aspect, there are other important factors like cost and feasibility that determine the success of a data-protection solution.

The most simple one from a technology standpoint is physical protection, even though it can be difficult to implement or simply not practical in some cases. Hindering unauthorized access to the fiber plant by choosing routes where the fiber optic cable is buried into the ground rather than mounted on poles or installed in subway tunnels can increase security significantly. This option is, however, not generally available since most of the pre-existing fiber plant was built with no special emphasis on security. The absence of secured access to manholes and patch points constitutes additional risk that is difficult to mitigate.

Fiber optic intrusion detection systems monitor the optical fiber strand for both signal degradation and intrusion disturbances that could indicate fiber damage or physical intrusion. These systems are far more sensitive to subtle intrusion attempts than devices that rely upon power measurement alone. The preparation of the cable and fiber for tapping will cause power and distribution transients that the optical filters and receiver detect and amplify. The result is analyzed and

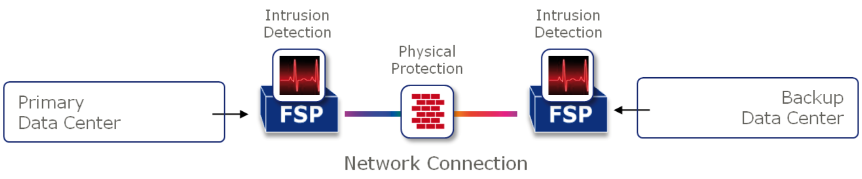


Figure 1: Data protection approaches

used to identify signal patterns of intrusion attempts. Alarms are issued upon verification of an intrusion signature.

Advanced implementations allow maximum sensitivity to intrusion-attempt signatures while minimizing the probability of false alarm events. The design objective is to identify intrusion attempts while the attack is still at the outer layer of the cable structure. This allows for the rapid location and interception of any intruder before data is compromised.

Both physical protection and intrusion detection are useful tools that lower the risk of data theft through interception. They cannot, however, actually prevent such attempts, which is why powerful encryption implementations are still considered the best option for guaranteeing ultimate security. Encrypting data is the most powerful technological method to safeguard business-critical data in transit over fiber network infrastructure.

Both physical protection and intrusion detection are useful tools that lower the risk of data theft through interception. They cannot, however, actually prevent such attempts, which is why powerful encryption implementations are still considered the best option for guaranteeing ultimate security.

Encryption Implementation Alternatives

As a general term, cryptography is used to guard crucial or sensitive information from unauthorized access. Encryption, one implementation of crypto-graphy, is the conversion of data into a seemingly incomprehensible mixture of characters that, when viewed, cannot be read as simple text. The algorithm used to encrypt data is called a cipher, while unencrypted data is called plain text.

Data encryption can be integrated into an existing workflow in a variety of different ways, each with its own advantages and disadvantages. There are three basic ways to approach the process of implementing data encryption on a network:

- **File system encryption on a server**
  File system encryption is probably the easiest method to implement – the tools needed are often already included with server operating systems. This type of encryption, however, requires heavy computing power on the server, which often makes it impractical for high-performance applications. Additionally, server file system encryption does not allow for centralized management. It must be implemented on a per-server basis, and is managed only with respect to that system.

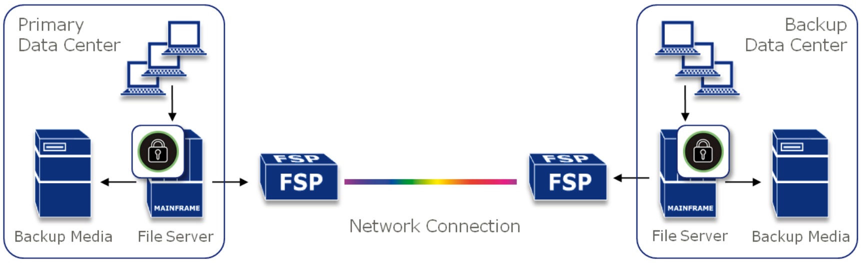


Figure 2: File system encryption

- **Backup device encryption**
  The most commonly used method of encryption takes place on the backup media – either on the server driving the tape backup device or on the tape drive itself. When implemented on the tape server, encryption can dramatically reduce the performance of the backup system, since a large portion of the server's CPU resources are diverted to perform the encryption. While using a tape drive that provides its own encryption processing can help alleviate the overall load on the tape server, this approach does not secure the original data when transferred across the network to remote locations and is therefore not applicable for protecting against network interception.

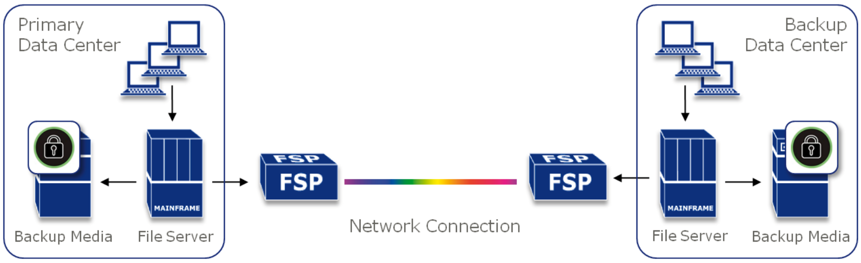


Figure 3: Backup device encryption

- **On-the-fly encryption**
  On-the-fly encryption is a method typically performed by a hardware appliance and is relatively simple to implement. The appliance normally has two network connections, with plain text coming in through the client interface and encrypted text leaving via the network side. These systems encrypt data as it passes through the device. Encryption appliances can be set up in between a company's primary and backup data center to provide encryption of the data that is about to be transferred securely to the remote location. In-line devices provide wire-speed encryption, meaning that the servers and backup devices can operate at their own natural throughput, as if there was no encryption being performed.

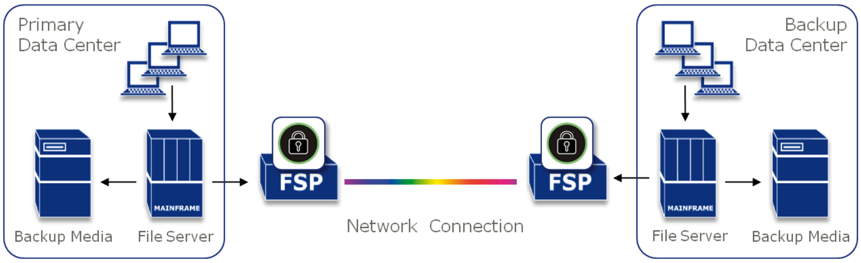


Figure 4: On-the-fly encryption

Implementing On-the-Fly Encryption

On-the-fly encryption can be implemented on different layers of the OSI protocol stack, with the lower three layers being preferred – i.e., physical, data link and network layers. Encryption on the lowest possible layer has the additional benefit of safeguarding information exchanged on all protocol layers above it. Current implementations typically perform security measures at Layer 3, utilizing Internet Protocol Security (IPsec), a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec encryption can add more than 60% of information to an IP packet flow. This increase in bandwidth is considered to be an acceptable burden for predictable traffic consisting of large packets. IP traffic, however, is inherently bursty and consists of many small packets that slow down the communication flow, thus creating considerable strain to network devices and their compute resources.

The increased importance of data security has caused a paradigm shift, focusing on encryption implementations at lower layers of the OSI protocol stack ...

The increased importance of data security has caused a paradigm shift, focusing on encryption imple-mentations at lower layers of the OSI protocol stack, the physical layer in particular. At this lowest layer, data rate and block size are more constant and predictable, allowing lowest latency while guar-anteeing wire-speed data throughput without any loss in performance. These characteristics are vital to enterprise applications for data backup, protection and disaster recovery, which require the highest network performance and efficiency.

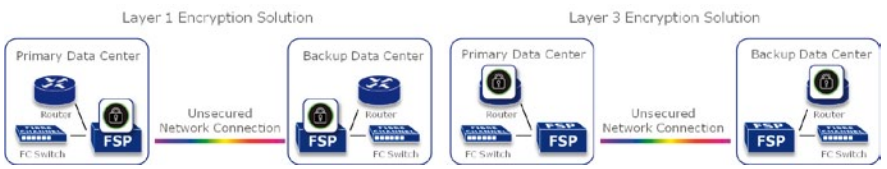


Figure 5: Encryption implementation on Layer 1 vs. Layer 3

In addition to performance considerations, key management plays an important role in any en-cryption scenario. After all, locks have little value if everyone has a key. The encryption of data itself is straightforward, while the answer to the question of how to generate, store and securely distribute the required encryption keys is a bigger challenge. Keys are the central element of every encryption solution, and any third-party access to or knowledge of the actual keys used renders the whole solution useless.

Before an exchange of data can start, an authentication process is needed to make sure that only the entitled parties are able to participate in the communication. Following this initial authentication process, each automatically generated key is derived in a secure way using established technologies such as real random number generators or highly sophisti-cated software algorithms. The distribution of keys between the parties should be achieved following accredited methods like asymmetric key exchange according to Diffie-Hellman, which is explained in a later section of this paper. Internal keys should be stored only during their usage – if at all – and should be discarded immediately after a new key has been generated. Protection measures must be imple-mented, including shielding and destruction of keys in case of tampering attempts.

Encryption Methods

The symmetric-key encryption standard Advanced Encryption Standard (AES) announced by the National Institute of Standards and Technology (NIST) and adopted by the U.S. government is the de facto industry standard for encryption. AES is based on a design principle known as a Substitution Permutation Network and is therefore fast to implement in both software and hardware solutions.

The introduction of AES has its roots in a competition held in the mid 1990s for the best new encryption method. Out of the five algorithms that made it into the final round, AES had the best relation between performance and security. It is generally regarded as the best method for data encryption, while the only known attack against AES consists of testing all coding possibilities (brute-force attack).

AES is a set of algorithms specifically designed to resist the most sophisticated methods of code breaking used by attackers. Hackers employ a wide variety of cryptographic attacks, including timing analysis – i.e., looking for correlations between a plain text and the time taken to encrypt it – and power analysis – i.e., looking for variations in the processing power requirements for encrypting different plain texts. Yet they still find it challenging to penetrate AES block ciphers.

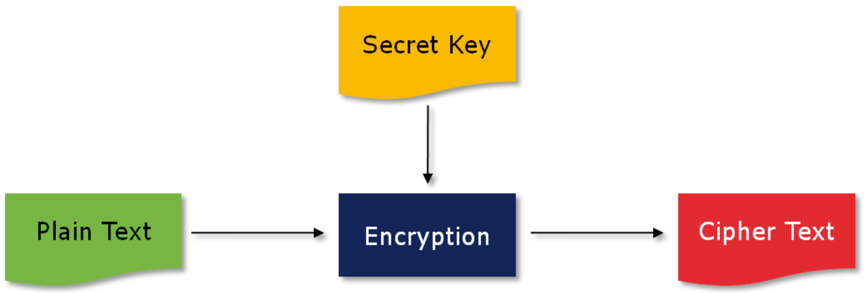


Figure 6: Encryption of a data block

In AES, the encryption block takes 128 bits of plain text data and transforms them into 128 bits of cipher text output. The block is controlled by a secret key, which can have the length of 128, 192 or 256 bits. At the moment, a key length of 128 bits is sufficient, since a brute-force attack would require 2127 trials, far too many to be carried out in a practical amount of time, even by the most advanced computing system. The encrypted data block can be decrypted with the inverse encryption function using the same secret key. Encryption and decryption are separate functions.

Besides the pure mathematical transformation, the application of this algorithm on the actual data stream creates another challenge. The most basic way of encrypting a data stream on the physical layer would be to divide the incoming data into blocks of 128-bit length and to encrypt the data to be transmitted

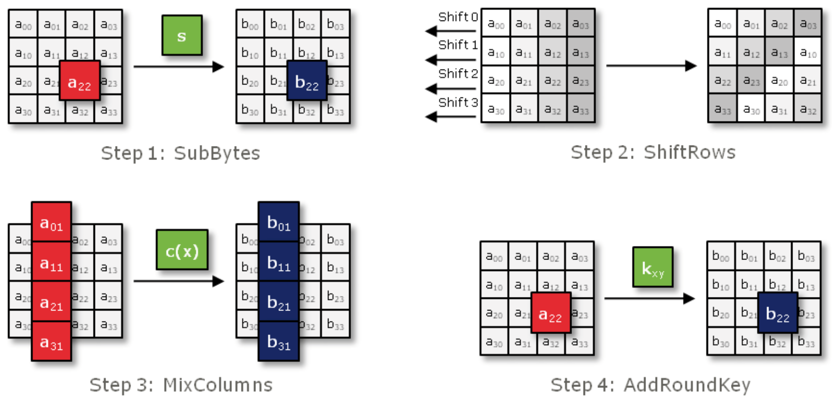
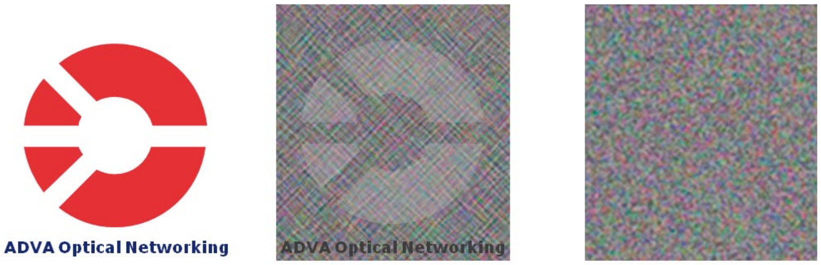


Figure 7: AES transformation principles

block by block. This mode is called Electronic Codebook (ECB). Since every block of data is independent and the AES encryption algorithm is not altering, ECB has the drawback that structures larger than 128 bit can be detected in the encrypted cipher text. In the example illustrated in Figure 8, a picture with eight bits per pixel is encoded using ECB. Even though the pixels are encrypted, the overall structure of the data, which extends over several blocks, can still be recognized.

As demonstrated by this example, a correlation between individual blocks is desirable to add more security to the cipher text. The most popular correlated encryption modes are the Cipher Block Chaining (CBC), Cipher Feedback (CFB) and Counter (CTR) modes. In CBC mode, the plain text is divided into blocks of 128-bit length as with CBM. An exclusive disjunction (XOR) operation with the previously encrypted block data is then added to introduce correlation. CFB is similar to CBC, except that the plain text is added using XOR only after the encryption process.



Original

Encrypted with ECB

Expected

Figure 8: ECB mode encryption

A general problem with feedback modes is the error propagation that occurs in cases of bit errors. Since the blocks are correlated, a single bit failure in the first data block will cause the entire data in the following data block to become invalid. This error propagation has a direct impact on the bit-error rate, since a single bit error results in 129 bit errors in the decrypted text.

In order to overcome the error multiplication problem, CTR mode has been introduced. Instead of encrypting the data, a counter is instead encrypted. To arrive at the cipher text, the data is then added to the result using the same XOR operation. In CTR mode, the cipher text is therefore independent of the previous data block. CTR also allows pre-calculation of the encryption key stream. The data encryption itself is performed by a simple XOR operation and permits lowest-latency implementation.

Keys and Key Management

Successful implementation of an encryption solution requires hierarchical levels of security that must be established to guarantee secure data transmission. Each security level comes with its own setup procedures and dedicated keys that serve a specific purpose.

Successful implementation of an encryption solution requires hierarchical levels of security that must be established to guarantee secure data transmission.

- **Authentication Key**
  The authentication process is the very first step required to establish secure data transmission. Its purpose is to make sure that only the entitled parties participate in a communication process, which is designed to derive a secret session key to be used for encryption. In order to authen-ticate each party, an authentication key is generated and distributed to the participants. Only those devices that have the proper authentication key can participate in the key-exchange process.

- **Public Key (Diffie-Hellman)**
  The most common method for generating a secret-session key and to exchange it between two parties is the Diffie-Hellman algorithm. As part of this algorithm, each party – in this example, **A**lice and **B**ob – generates a public key, which is typically a random integer number, and sends it to the other side. In the case of two parties, two integer numbers ‘g’ and ‘p’ are generated.

- **Private Key (Diffie-Hellman)**
  In addition, each party also generates a private key (integer numbers ‘a’ and ‘b’), which are only known locally and are not sent over the link. The result of the term $A = (g^a \bmod p)$ is sent from Alice to Bob, and the result from $B = (g^b \bmod p)$ is sent from Bob to Alice.

- **Shared Secret Key (Diffie-Hellman)**
  After each party has received the data from its counterpart, it computes the shared secret key K. Alice computes $K = ((g^b)^a \bmod p)$, whereas Bob computes $K = ((g^a)^b \bmod p)$. Both computations deliver the same result, which is the shared secret key. Since there is no inverse operation for the mod operation, an attacker cannot calculate the shared secret key if he has no knowledge of ‘a’ or ‘b’. A mandatory requirement is that the number ‘p’, which is used for the mod operation, must be a large enough prime number. In order to guarantee a certain level of security, asymmetric key exchange methods like Diffie-Hellman use a key length of at least 1024 bits, if not even 2048 bits.

- **Session Key**
  The session key is the final key that is used to encrypt and decrypt the

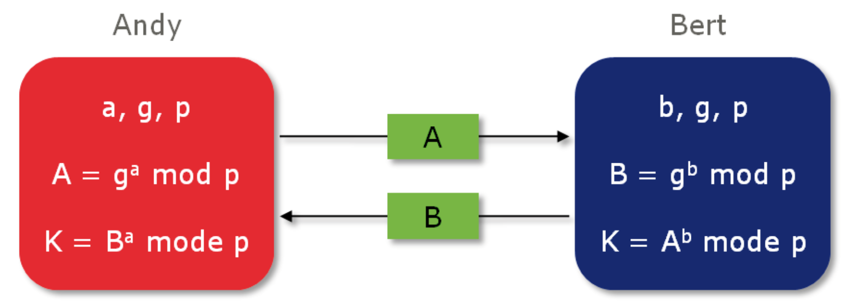


Figure 9: Diffie-Hellman key exchange

transmitted data for a given period of time. It is derived from the shared secret key of the Diffie-Hellman key exchange process. Typically, if AES 256 is used, the length of the session key is 256-bit. Since the encryption with the same session key at both ends – symmetric key operation – could be broken into through a brute force attack over a long period of time, it is highly recommended that the session key be changed in periodic intervals of less than one hour.

Data Center Connectivity – a Case Study for Encryption at Work

From a disaster recovery and business continuity perspective, it is imperative to have data backed up and stored offsite, preferably in a location geographically far away. The historical approach to offsite backup – using removable media such as disks or tapes – is rapidly being supplanted by disc mirroring technology, utilizing the fiber network to achieve highest performance and shortest recovery times. But in either case, the data must be encrypted before it leaves a site.

Figure 10 shows a typical application scenario for synchronous disc mirroring as deployed in the financial industry. Wavelength Division Multiplexing (WDM) technology is used to interconnect the primary and backup data centers. The deployment of WDM technology assures efficiency in fiber usage combined with lowest transmission latency and bandwidth scalability. Up to several Terabytes can be transported between the two locations – just enough to satisfy the high-performance requirements of disaster recovery solutions.

The network connection in this example is typically of a private character and can either be provided by a managed service provider or maintained by the financial institution itself by means of leasing fiber from a local fiber provider.

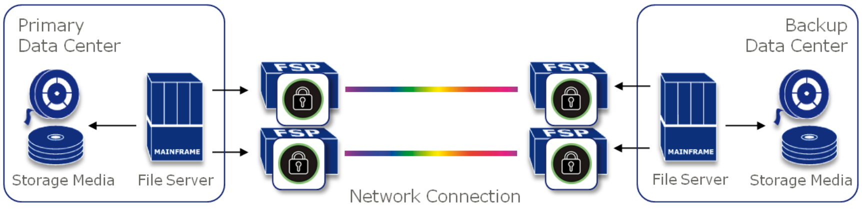


Figure 10: Data center interconnection for disaster recovery

In either case, data sent over the remote link is preferably encrypted in order to protect all private and sensitive data from theft. Some countries such as Switzerland have even made the encryption of data before remote transport a regulatory requirement.

Due to the performance-critical nature of this application, on-the-fly encryption built on top of a high-performance optical networking solution is considered the most suitable solution for data backup, protection and disaster recovery.

Due to the performance-critical nature of this application, on-the-fly encryption built on top of a high-performance optical networking solution is considered the most suitable solution for data backup, protection and disaster recovery.

Encryption in Managed Service Environments

Traditionally, on-the-fly encryption solutions have been deployed by enterprises operating both their own transport network infrastructure and data center equipment. However, now that managed service providers are starting to offer encryption services on top of their standard connectivity portfolios, they must also manage the encryption function implemented as an integral part of the transport solution. Yet not all responsibilities lay with the service provider: the managed service provider is in charge of operating his network and meeting service level agreements, but all security-relevant functions generally remain under the control of the enterprise customer leasing the managed service. The challenge is to completely separate the security management domain from management of the connectivity domain.

Managed service providers must restrict their customers from having access to their network elements so there can be no service reconfiguration or manipulation. At the same time, service providers must still grant secure access to the security management domain of the system. Because they are maintained by the enterprise customer, the service provider should not be granted the right to change or overrule any security-relevant settings or even have access to any of the secret keys.

Figure 11 illustrates the separation of the management domains between the service provider and the managed service customer. By means of a specific customer portal not accessible to the service provider itself, the system provides access to the key exchange mechanism for configuring and controlling the encryption function.

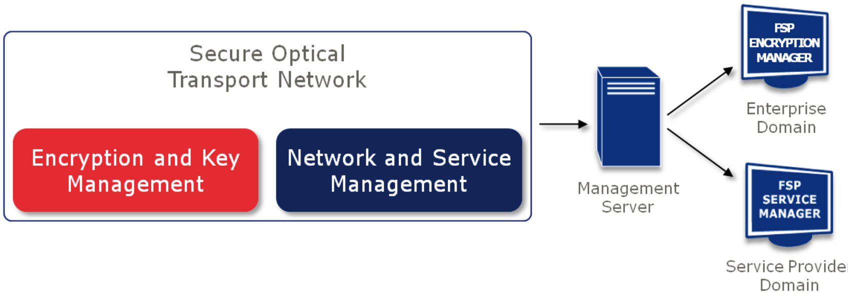


Figure 11: Separation of management domains

Another challenge in implementing an encryption solution is finding the right balance between maintaining maximum security levels and operational ease-of-use. For example, the operations department may want the option to temporarily operate on-the-fly encryption in a non-encrypted fashion in order to troubleshoot any potential errors. But the security department may want to simultaneously impose the requirement on the system design that an encryption solution only be used in encryption mode.

A Tailored Solution for Managed Services

Security for optical transport networks is becoming an important means to safeguard private data sent across networks. The threat of data theft and espionage is real, and recent advancements in technology increase the likelihood that hackers will successfully gain access to business-critical information. But the protection mechanisms have also developed, creating new opportunities for managed service providers to enhance their services in a simple manner and add encryption functionality to their portfolios.

With its scalable optical transport solution, the FSP 3000, ADVA Optical Networking offers a widely deployed best-of-breed Wavelength Division Multiplexing (WDM) platform that enables the secure interconnection of data center facilities.

With its scalable optical transport solution, the FSP 3000, ADVA Optical Networking offers a widely deployed best-of-breed Wavelength Division Multi-plexing (WDM) platform that enables the secure interconnection of data center facilities. Superior transmission performance at the lowest latency is guaranteed by:

- Transmission interfaces from 10Mbit/s to 100Gbit/s to ensure support of all future protocols and applications;
- Multi-protocol support, including Ethernet, Fibre Channel and SONET/SDH;
- Integrated electrical multiplexing technology for maximum wavelength utilization;
- Transparent wavelength conversion for data transfer at lowest possible latency;
- Built-in redundancy and protection concepts, allowing the achievement of regulatory compliance with regard to data safety and integrity; and
- Single-span distances up to 200km, eliminating the need for mid-span application sites.

Through the recent addition of high-performance encryption functionality, the FSP 3000 has become a tailored solution allowing enterprises and managed service providers to successfully deploy encrypted high-bandwidth transport services over an optical network. The main characteristics of the encryption implementation are:

- Data encryption on the transmission layer, guaranteeing lowest latency and highest throughput;
- Integrated solution, allowing for ease of use and lowest complexity;
- Application of AES encryption technology and Diffie-Hellman key exchange, offering highest security;

- Separate management domains for management of both the transport equipment and security;
- Protection against interference of the managed service provider with the security management domain; and
- Maintenance of the guidelines outlined in international encryption standards, including FIPS 140-2 Level 2 or Level 3.

A joint solution of the FSP 3000 and the FSP Service Manager provides for automated provisioning and simplified network operations. The combined solution provides a comprehensive set of features for cost-effective and secure data center interconnection. It offers strict separation of the management domain for the transmission and encryption layers, implemented by means of virtual server technology. The virtual server concept allows secure access to the individual management domains as required in the case of a managed service provider scenario.

Figure 12: The FSP 3000 5TCE-module with optional line side encryption

About ADVA Optical Networking

ADVA Optical Networking is a global provider of intelligent telecommunications infrastructure solutions. With software-automated Optical+Ethernet transmission technology, the Company builds the foundation for high-speed, next-generation networks. The Company's FSP product family adds scalability and intelligence to customers' networks while removing complexity and cost. Thanks to reliable performance for more than 15 years, the Company has become a trusted partner for more than 250 carriers and 10,000 enterprises across the globe.

Products

FSP 3000

ADVA Optical Networking's scalable optical transport solution is a modular WDM system specifically designed to maximize the bandwidth and service flexibility of access, metro and core networks. The unique optical layer design supports WDM-PON, CWDM and DWDM technology, including 100Gbit/s line speeds with colorless, directionless and contentionless ROADMs. RAYcontrol™, our integrated, industry-leading multi-layer GMPLS control plane, guarantees operational simplicity, even in complex meshed-network topologies. Thanks to OTN, Ethernet and low-latency aggregation, the FSP 3000 represents a highly versatile and cost-effective solution for packet optical transport.

FSP 150

ADVA Optical Networking's family of intelligent Ethernet access products provides devices for Carrier Ethernet service demarcation, extension and aggregation. It supports delivery of intelligent Ethernet services both in-region and out-of-region. Incorporating an MEF-certified UNI and the latest OAM and advanced Etherjack™ demarcation capabilities, the FSP 150 products enable delivery of SLA-based services with full end-to-end assurance. Its comprehensive Syncjack™ technology for timing distribution, monitoring and timing service assurance opens new revenue opportunities from the delivery of synchronization services.

ADVA Optical Networking
North America, Inc.
5755 Peachtree Industrial Blvd.
Norcross, Georgia 30092
USA

ADVA Optical Networking SE
Campus Martinsried
Fraunhoferstrasse 9 a
82152 Martinsried / Munich
Germany

ADVA Optical Networking
Singapore Pte. Ltd.
25 International Business Park
#05-106 German Centre
Singapore 609916

For more information visit us at www.advaoptical.com

ADVA™
Optical Networking

Version 07 / 2012