



# 'Crypto WDM Surprise!'

Ari Salomaa, ADVA Finland  
@Trex, June 9, 2014



# Security & Encryption in Optical Transmission

Ari Salomaa, ADVA Finland  
@Trex, June 9, 2014

# Why?



When you transport information optically from A to B and you want it to be safe and secure...

**How valuable is your information to you?**

**What is the damage and cost to you  
IF the information ends up in the wrong  
hands?**

in Industry, Finance, Government, Healthcare, ...



# Top 3 IT Security Issues in 2014

Cyber Attacks Continue [3]



“Within the next couple of years, we will experience an increasing number of cyber attacks resulting in militaristic and economic damage.”

“As governments worry about the scale of the cyber security threat, we can **expect to see more national standards emerge**, and greater pressure for “voluntary” compliance.”

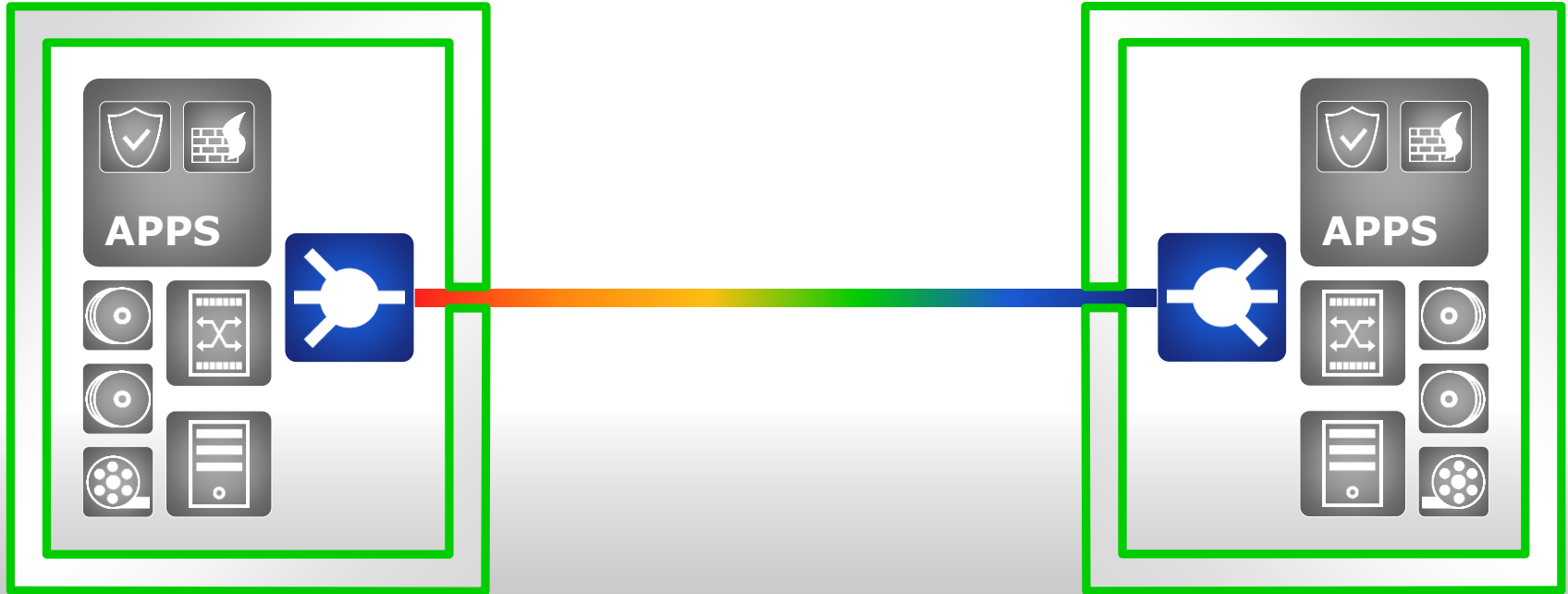
“On the back of emerging standards we will see the **cyber insurance market develop** and begin to provide market incentives for compliance, whether that is a willingness to insure or reduce premiums. **Non-compliance** will also **lead to a legal debate over liability for incidents.**”



[3] Jarno Limnell, director of cyber security at Stonesoft.

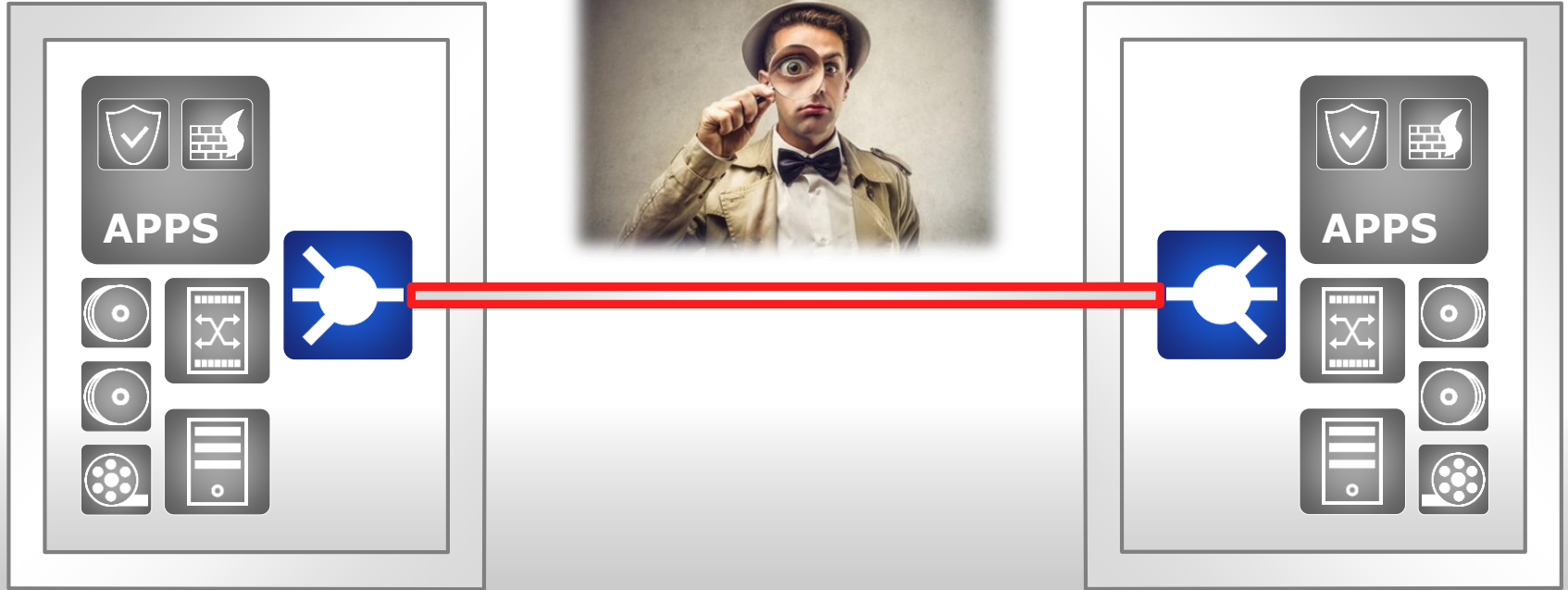
# Data Center Environment & Security

Physical Access , Hardware, Software, ...



# Data Center Environment & Security

...and what about the Fiber Connection?



# Fiber Optic Networks

## Tapping Possibilities



Street cabinet

**Where**  
to get access?



Splice boxes / cassettes  
(Outdoor / Inhouse)



Y-Bridge for  
service activities



Fiber Coupling device

**How**  
to get access?



**There are multiple ways to access fiber**

# Optical Transmission Security





# Optical Security Topics



## Physical Layer Monitoring

Power Tracking  
Intrusion Detection  
Optical Time-Domain Reflectometer (OTDR)  
Access Line Monitoring (ALM)



## Encryption

AES-256  
Authentication  
Diffie-Hellman



## Security-Hardened Software

RADIUS  
Secure Shell  
SNMPv3



**A complete and integrated solution helps to manage it all**

# Physical Layer Monitoring



## **Fiber Cut:**

Detection through software-adjustable switching thresholds



## **Fiber Degredation:**

Alarm generation through adjustable fiber attenuation thresholds



## **Long Term Effects:**

Long term fiber performance information monitoring  
Intrusion detection through correlation of typical power signatures



## **Fault Location Detection:**

In-service OTDR measurement or Access Link Monitoring (ALM)  
to locate fiber problems and possible fiber taps

# Encryption

What is the Key for high performance encryption?



- Compliance with encryption standards
- Speed - Low Latency
- Highest level of security
- Encryption on the lowest possible layer
- 100% Throughput
- No Jitter
- Role Based Management (Multi Tenant Management for Carriers)
- Total Cost of Implementation



**Security solution has to meet application requirements**

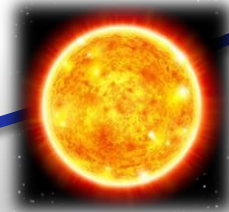
# Encryption Basics



# Encryption Basics

## Key Lengths – Magnitude

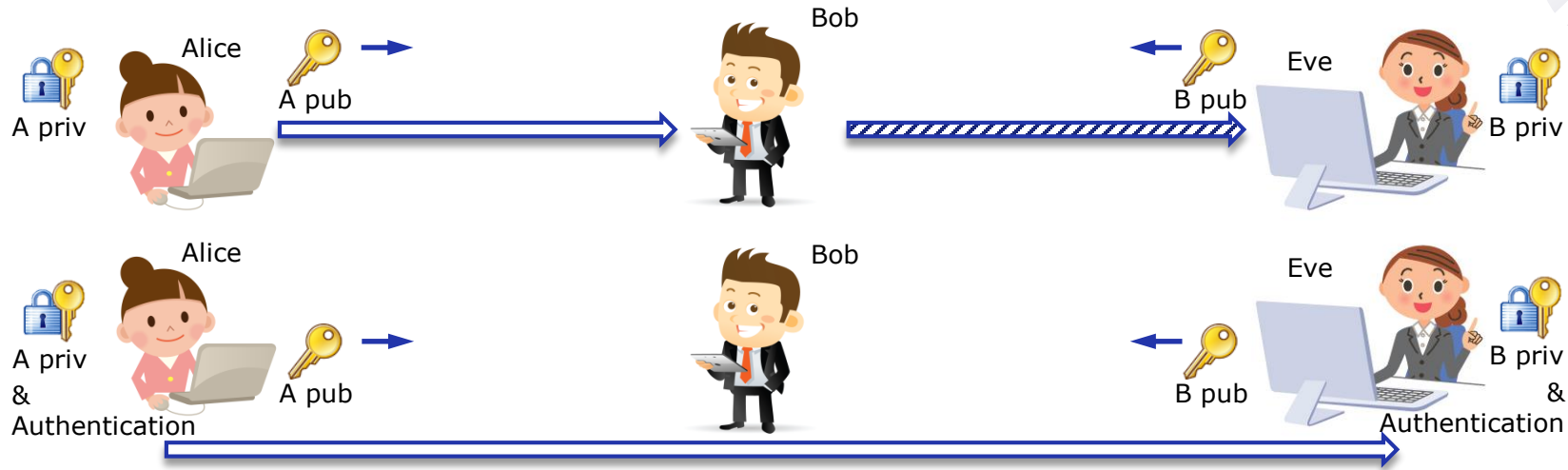
Number of grains in 1 m <sup>3</sup> sand from the beach	<b>2<sup>40</sup></b>
Number of atoms in a human body	<b>2<sup>92</sup></b>
Number of atoms in the earth	<b>2<sup>165</sup></b>
Number of atoms in the sun	<b>2<sup>189</sup></b>
Number of atoms in the Milky Way	<b>2<sup>226</sup></b>
Number of atoms in the universe	<b>2<sup>259</sup></b>



**AES**  
**256**



# Basic Cryptographic Goals



## Confidentiality (privacy) - "Encryption"

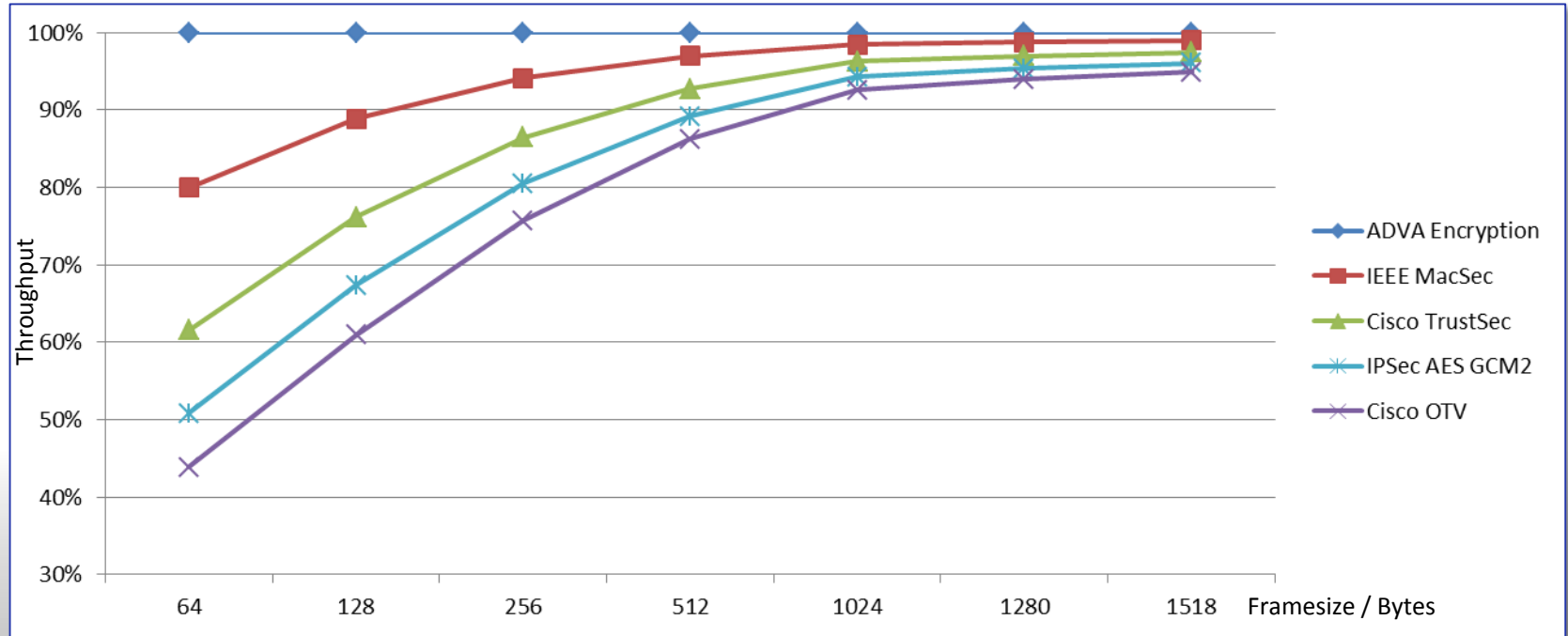
- Bob cannot understand message from Alice.
- Diffie Hellman Key Agreement/Exchange is arbitrated in the background.
- Bob could try to manipulate key exchange to Eve.

## Solution: Authenticity - "Authentication"

- Alice and Bob can be sure that they are really connected.

# Encryption Performance

## Comparison of Maximum Throughput

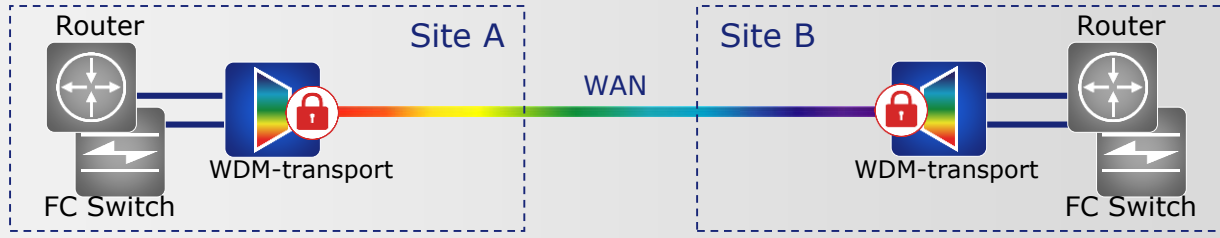


# Optical transmission security

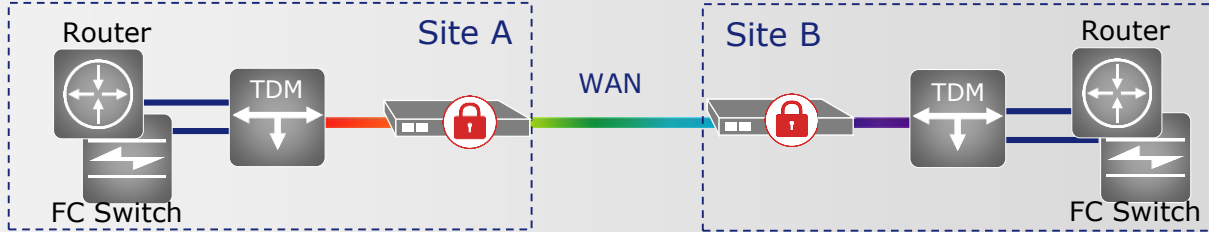
## Speed of Encryption



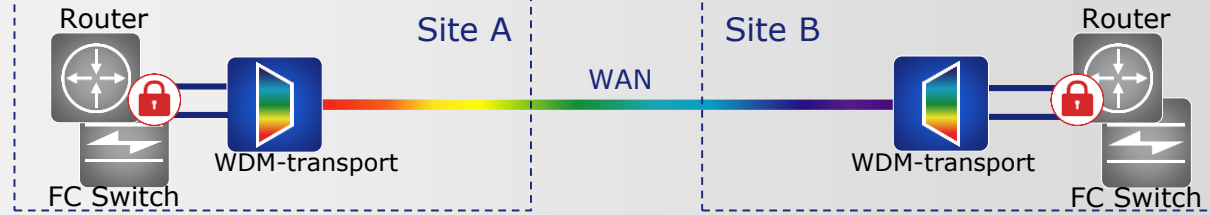
### xWDM based Encryption



### Appliance based Encryption



### Ipssec / MacSec Encryption





# Encryption Solution Integrated in Optical Transmission platform



# ADVA FSP 3000 Encryption Highlights



## Protection Building Blocks

- Authentication via initial authentication key to protect from “man in the middle” attacks
- AES256 encryption to offer maximum data security
- Diffie Hellman (DH) key exchange for secure encryption key generation
- New encryption key every 1min/10mins for additional security
- Key lifetime configurable
- Lowest latency (100ns) while providing 100% throughput

# Layer 1 Encryption Solution Suite



100GbE		AES 100G Encryption	100G
40GbE		40G	
FC 16G		5G – 15G	
FC 10G			
10GbE			
STM-64/OC-192		1G – 5G	
FC 8G			
IB 5G			
FC 4G			
STM-16/OC-48			
FC 2G			
FC 1G			
GbE			



# Encryption over OTN Networks

## 1GbE & 10GbE Services



FSP Network &  
Crypto Manager



Site A

Site B

LAN

LAN

OTN Network  
Carrier Managed Service

1-8G FC  
n\*1GbE,  
10GbE

1-8G FC  
n\*1GbE,  
10GbE

STM-64c  
OTU-2e

STM-64c  
OTU-2e

5TCE-PCN+AES10G

5TCE-PCN+AES10G

# Encryption Management & Operations

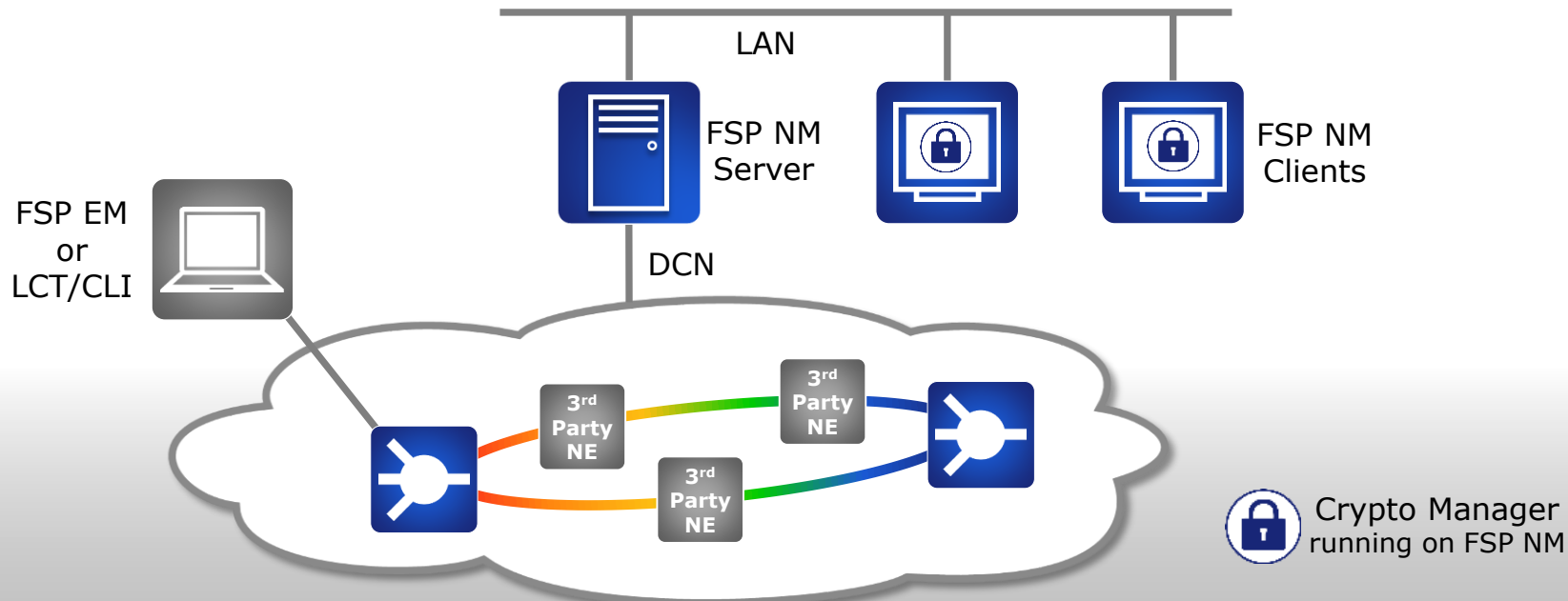


# Data Center Networks

## Encryption Management for Private Networks



Scenario 1 - User of encryption is the operator of equipment

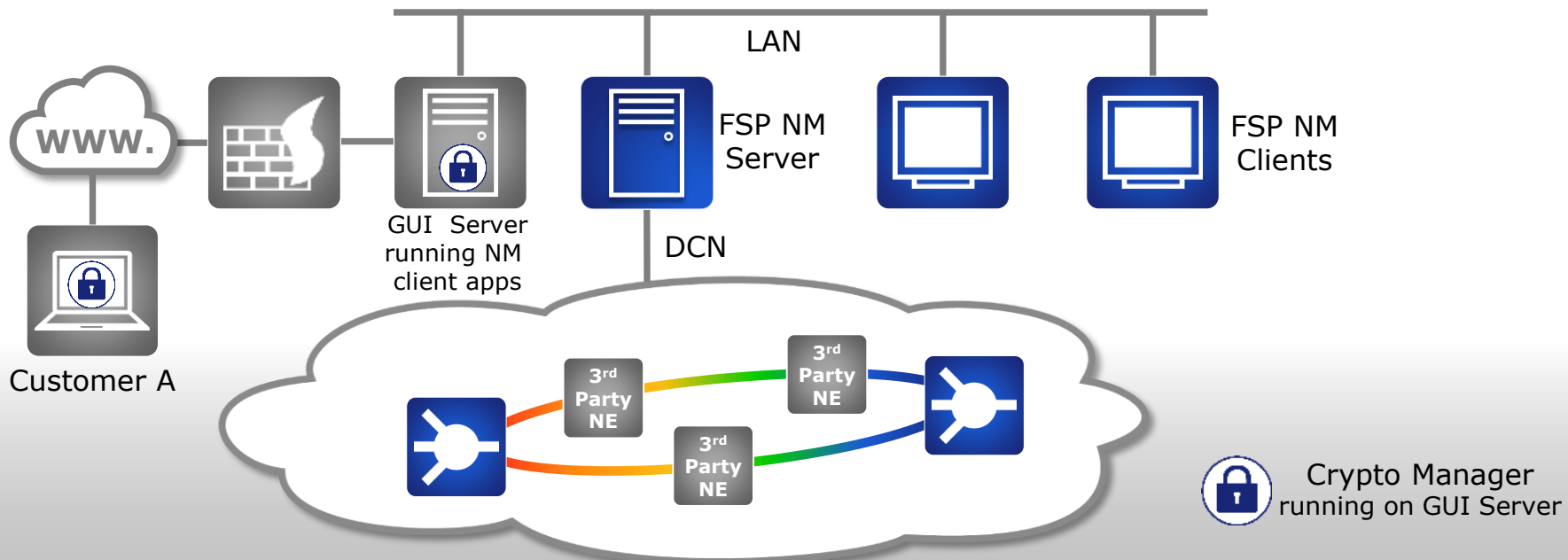



# Data Center Networks

## Encryption Management for Private Networks

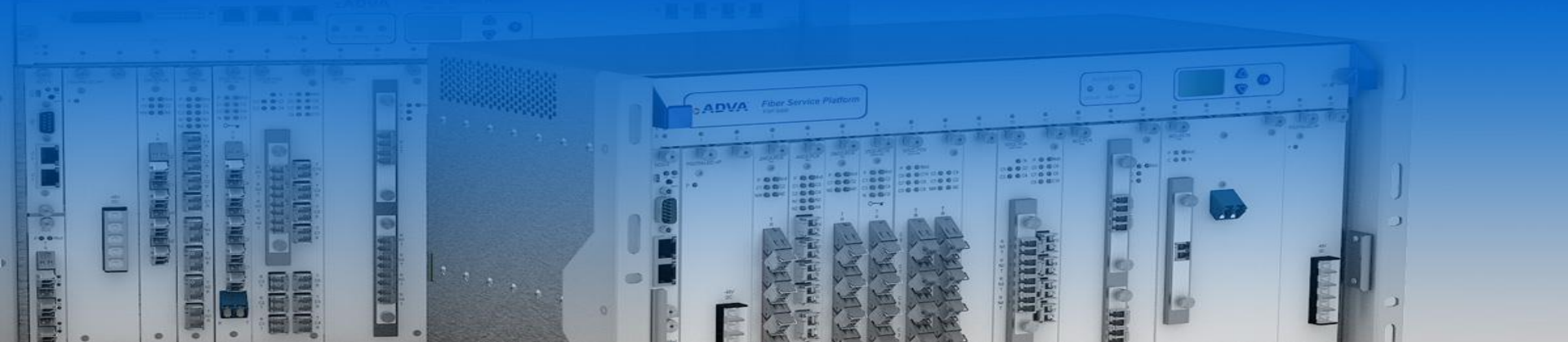


### Scenario 2 - Encryption user does not own the network



 Crypto Manager running on GUI Server

# Summary





# Optical Transmission Security with Encryption

## Summary

### Encryption Solution

- Enables compliance with laws and regulations
- Effective security and protection for all information
- High bandwidth & 100% encrypted throughput
- Low-latency performance
- Superior scalability and agility on Layer 1
- Encryption for both own enterprise networks and through operator managed service



**A complete and integrated solution leveraging advanced technology**

# Why?



**How valuable is your information to you?**

**What is the cost to you IF the information end up in the wrong hands?**

Industry, Finance, Government, Healthcare, ...



***Easy insurance: Encrypt your Optical transmission!***



# Thank You

[asalomaa@advaoptical.com](mailto:asalomaa@advaoptical.com)



**IMPORTANT NOTICE**

The content of this presentation is strictly confidential. ADVA Optical Networking is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.

The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA Optical Networking shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.

Copyright © for the entire content of this presentation: ADVA Optical Networking.