SNIA NSF | NETWORKING STORAGE

Storage Networking Security Series: Securing Data in Transit

Live Webcast

October 28, 2020

10:00 am PT

Today's Presenters

Alex McDonald
Moderator
Independent Consultant
Vice Chair SNIA NSF

Claudio DeSanti
Dell Technologies

Ariel Kit
NVIDIA

Cesar Obediente
Cisco

Brandon Hoff
Broadcom

SNIA-At-A-Glance

SNIA-at-a-Glance

185
industry leading organizations

2,000
active contributing members

50,000
IT end users & storage pros worldwide

Learn more: **snia.org/technical** **@SNIA**

Technologies We Cover

- Ethernet
- iSCSI
- NVMe-oF
- InfiniBand
- Fibre Channel, FCoE
- Hyperconverged (HCI)
- Storage protocols (block, file, object)
- Virtualized storage
- Software-defined storage

SNIA NSF | NETWORKING STORAGE

SNIA Legal Notice

- The material contained in this presentation is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

- Storage networks security framework
- Data-in-motion security
- Private and public cloud
- Securing data in the datacenter

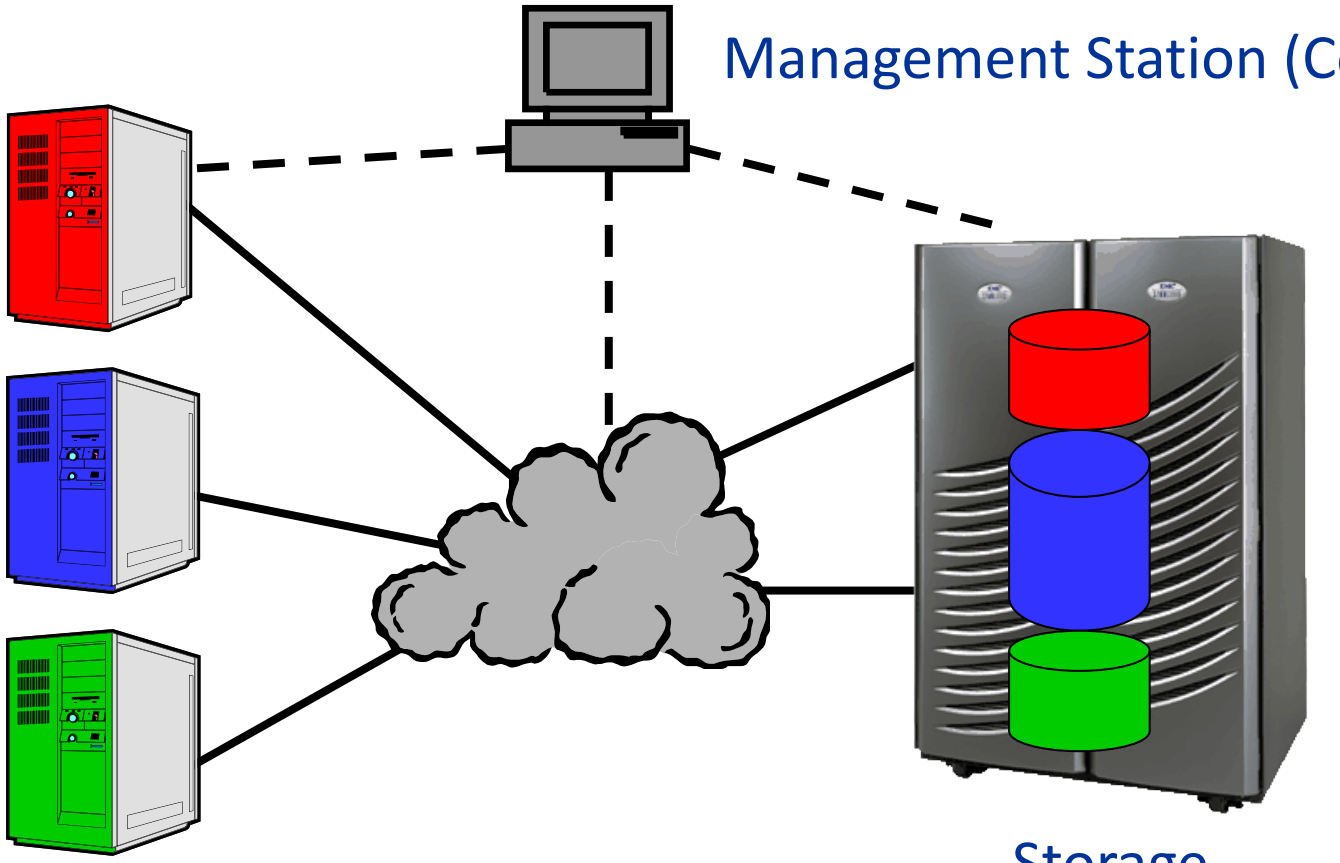
Storage Networks Security Framework

Threats Analysis

Claudio DeSanti

Dell Technologies

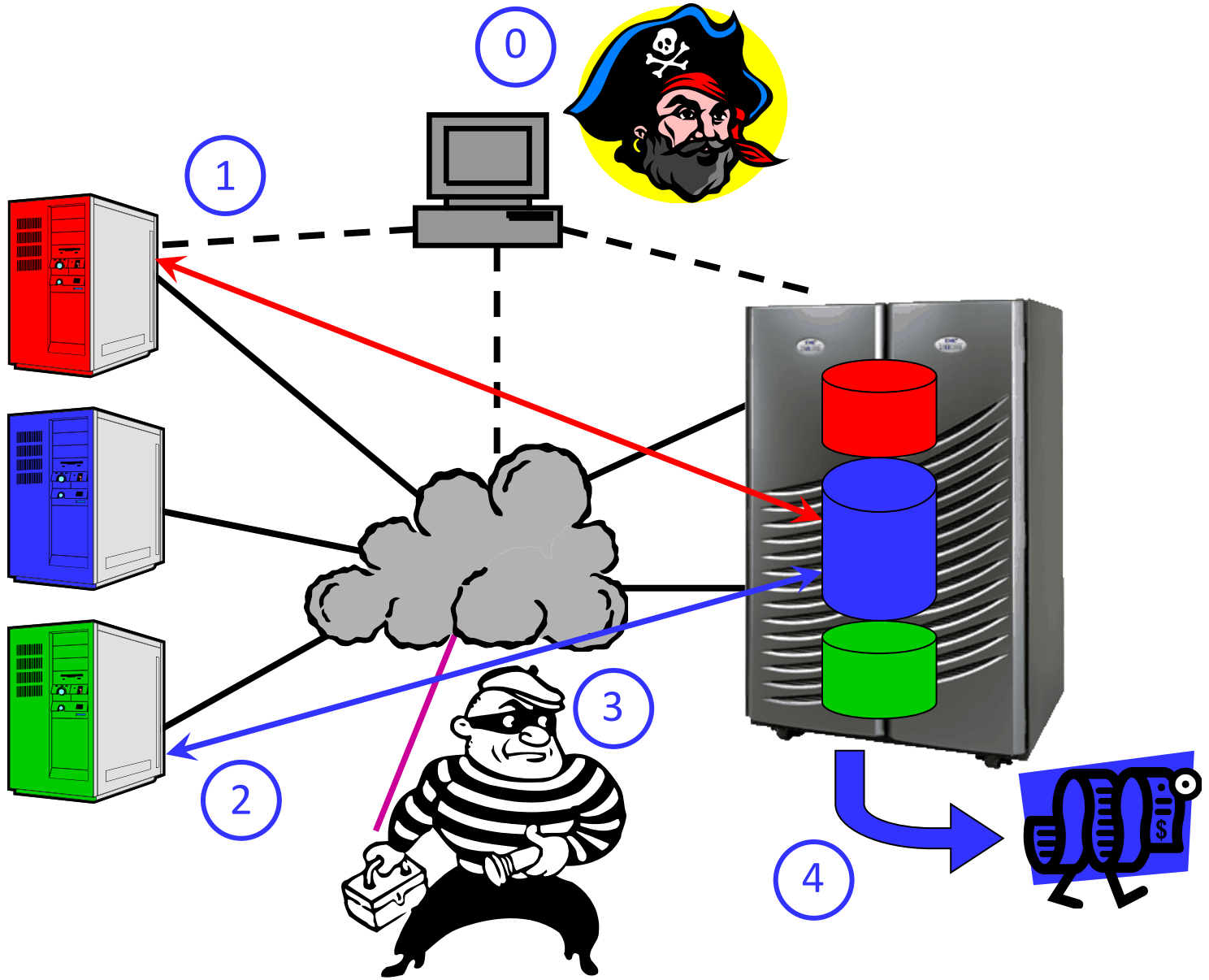
Storage Area Network (SAN) Example



Images credit: David Black

Security Threats

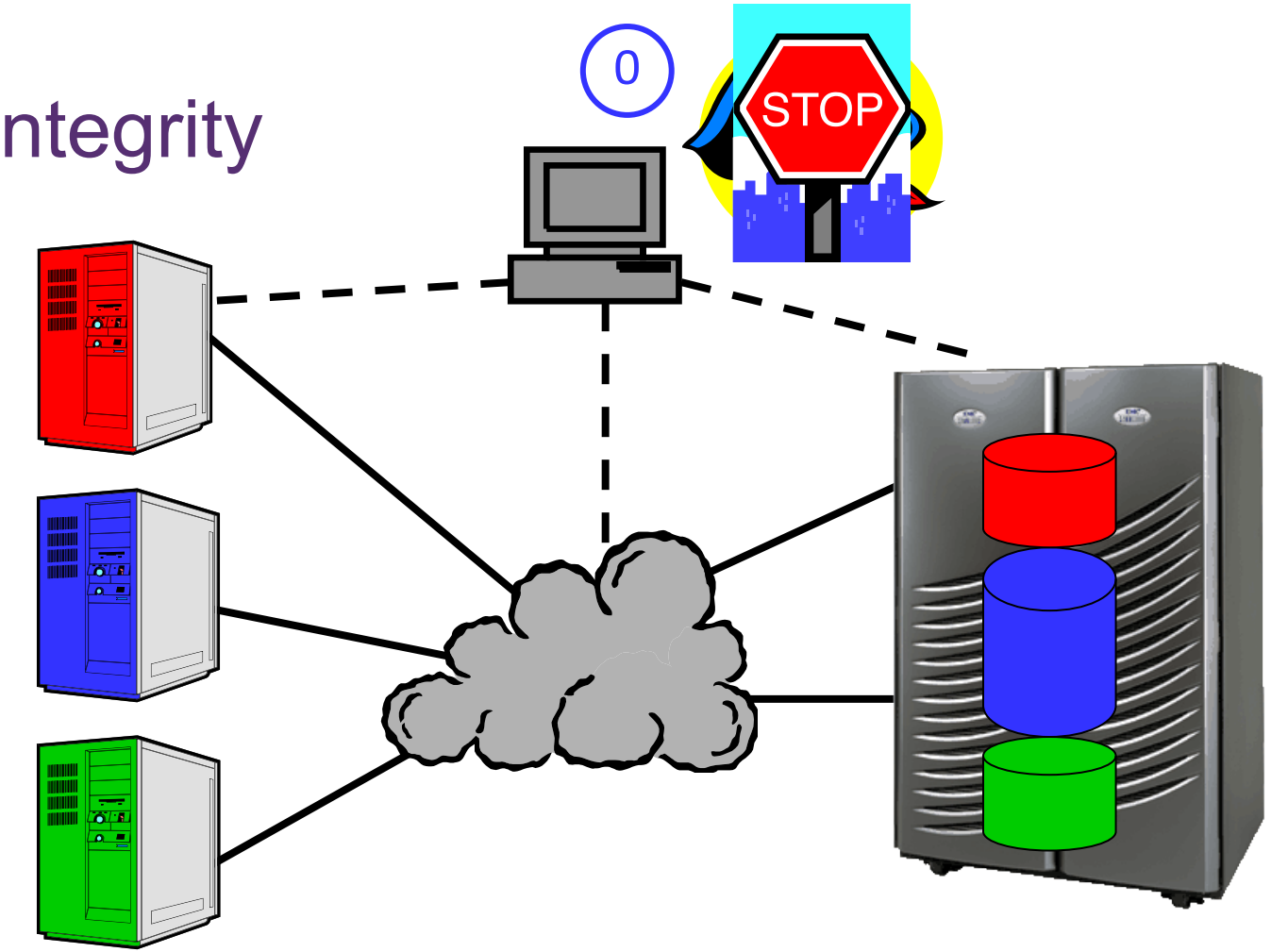
0) Management & System Integrity
1) Uncontrolled Storage Access
2) Impersonation (Spoofing)
3) Communication Access
   - Eavesdrop
   - Inject/Modify
4) External Access
   - Media Theft
   - Other Access



Security Threat 0: Management & System Integrity

0) Management & System Integrity

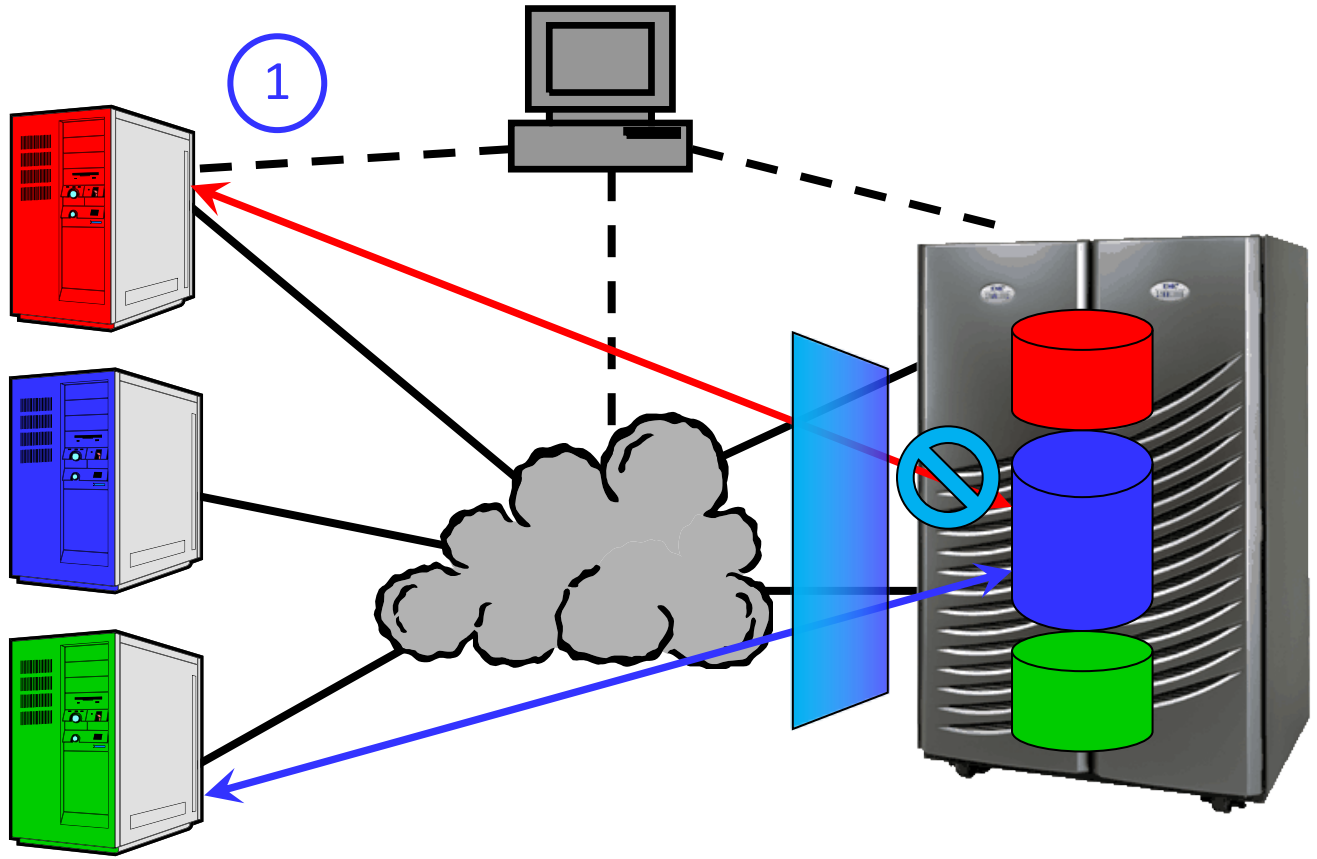
- Countermeasures: Management Security
  - Authentication & Authorization
  - Logging and Anomaly Detection
  - Secure Channels
- Countermeasures: System Integrity
  - Hardware/software/firmware integrity checks and assurance
  - Preferably anchored to hardware root of trust



Security Threat 1: Access Control

1) Uncontrolled Storage Access

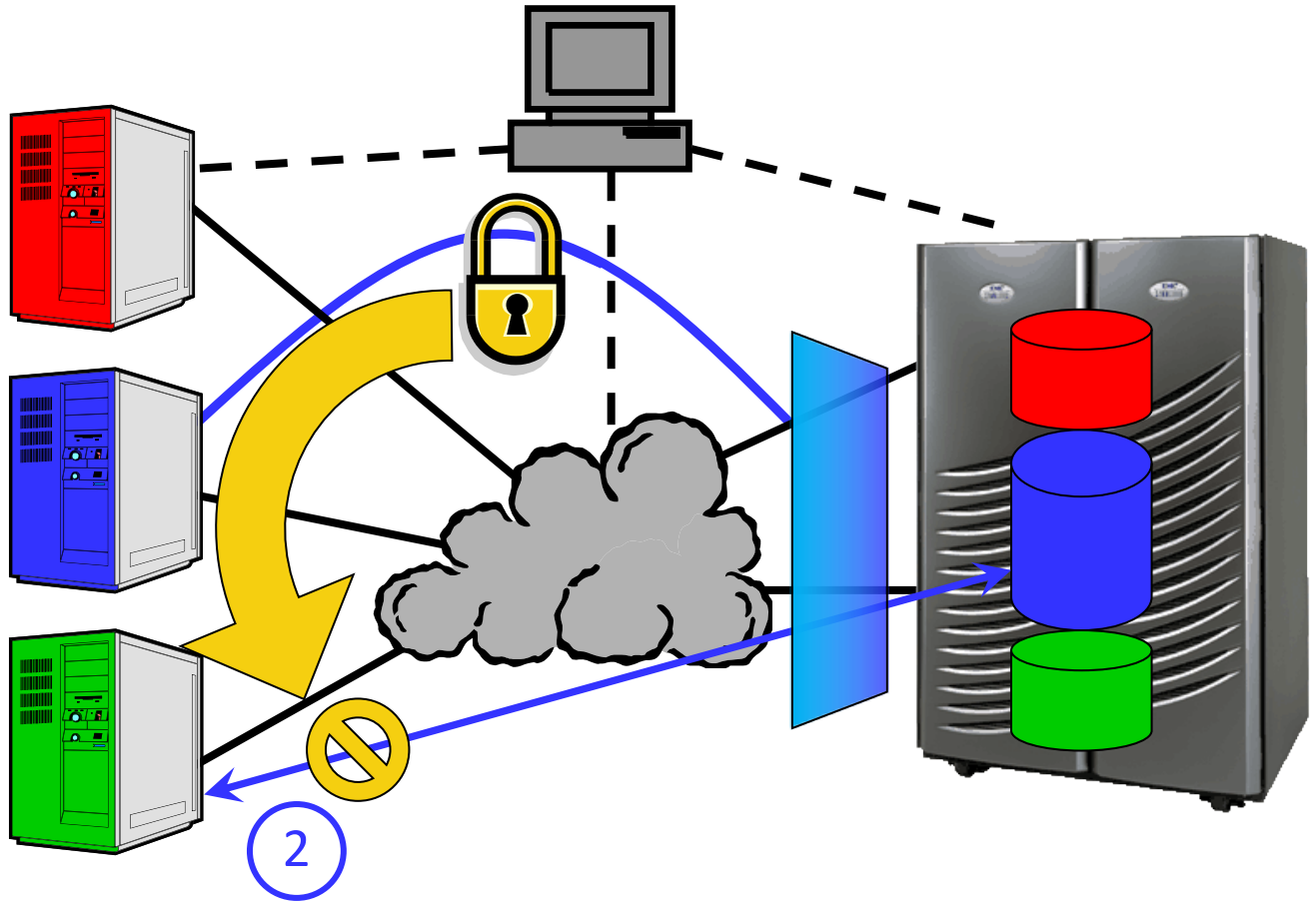
- Countermeasure: Storage Access Control
  - E.g., FC zoning, SCSI LUN masking, NVMe Namespace mapping
- Does not prevent impersonation



Security Threat 2: Impersonation

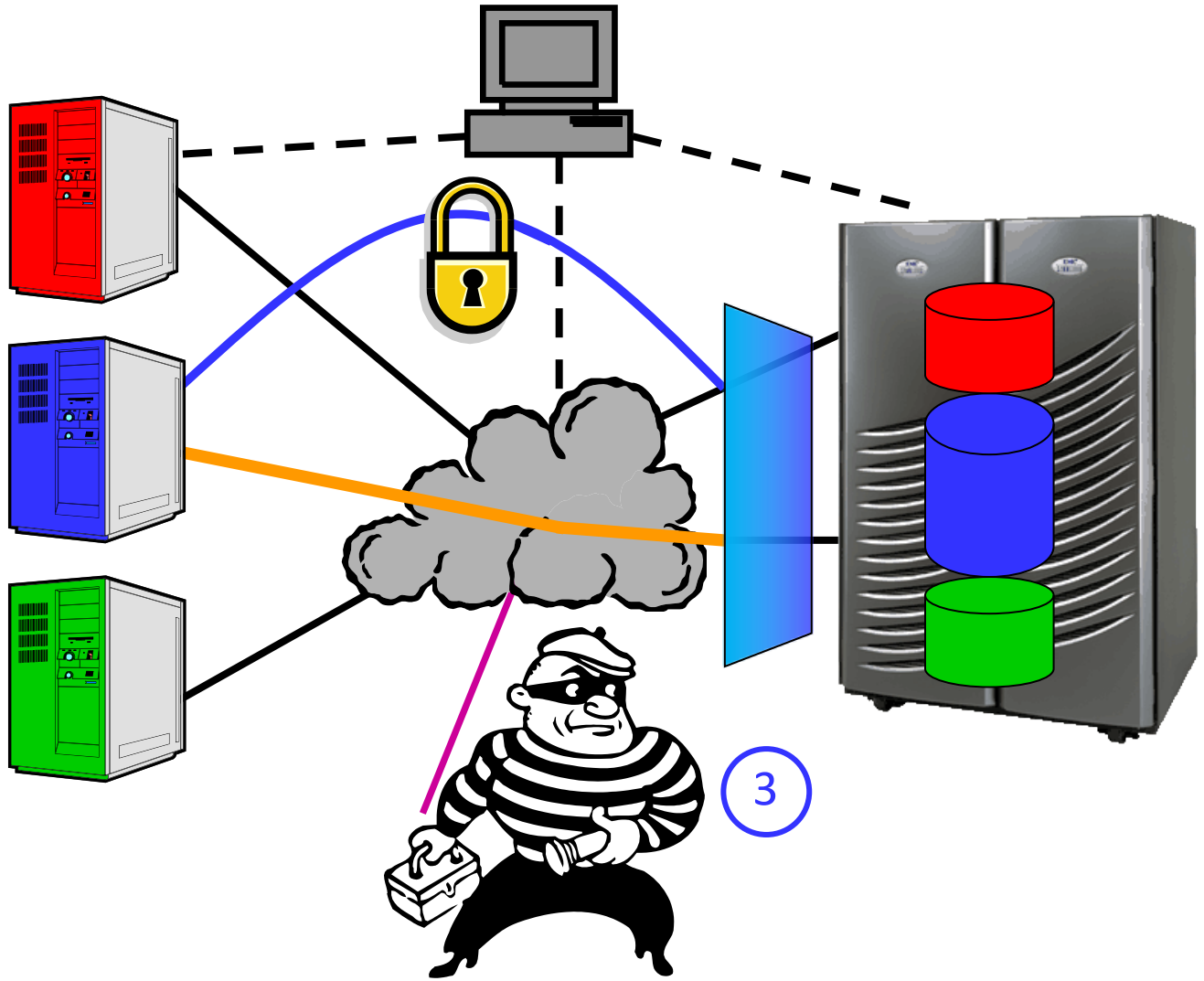
2) Impersonation (Spoofing)

- Countermeasure: Authentication
  - Proof of identity



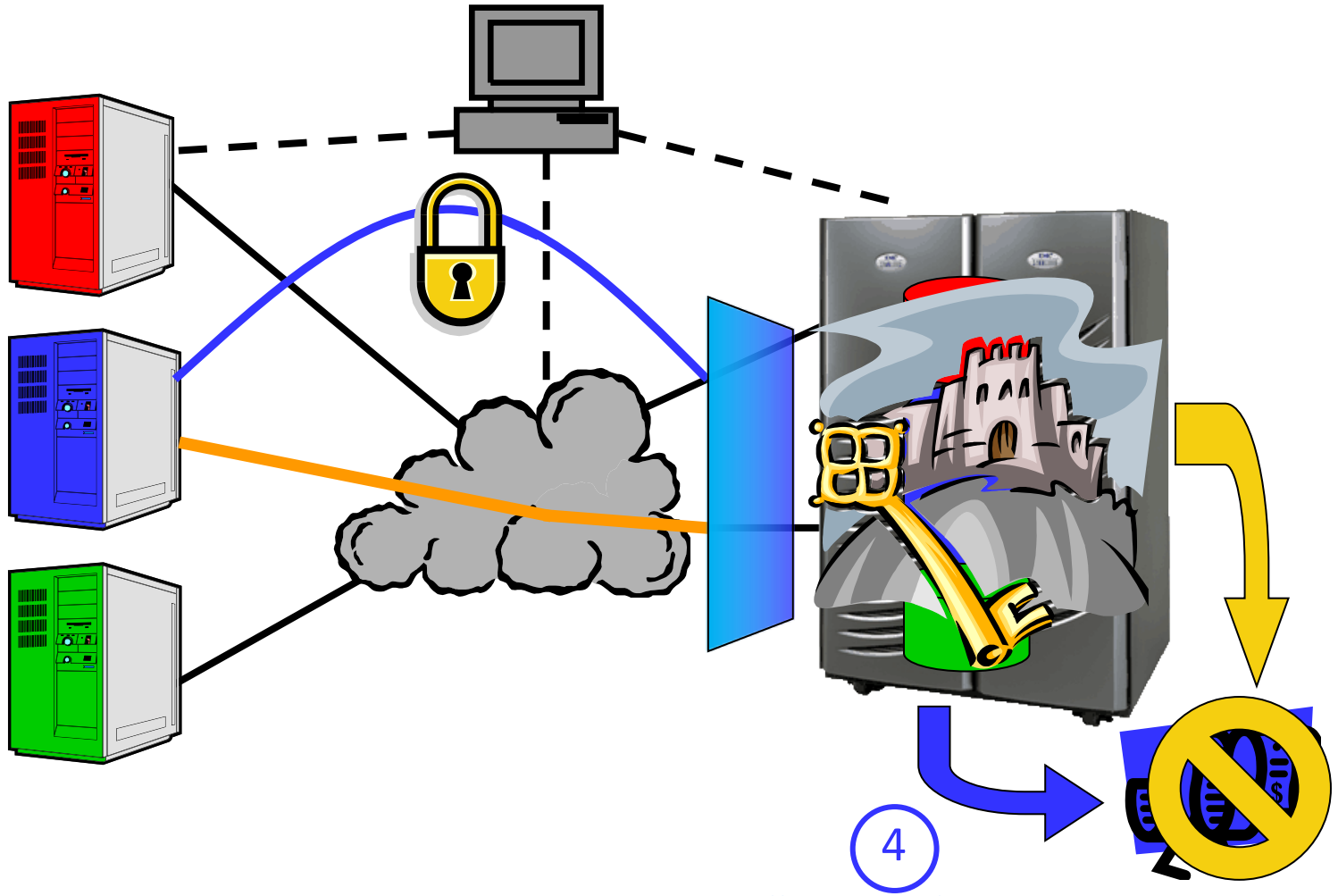
Security Threat 3: Communication

3) Communication Access
   - Eavesdrop
   - Inject/Modify
- Countermeasure: Secure Channel (data in flight)
   - Confidentiality
   - Cryptographic Integrity



Security Threat 4: Stored Data

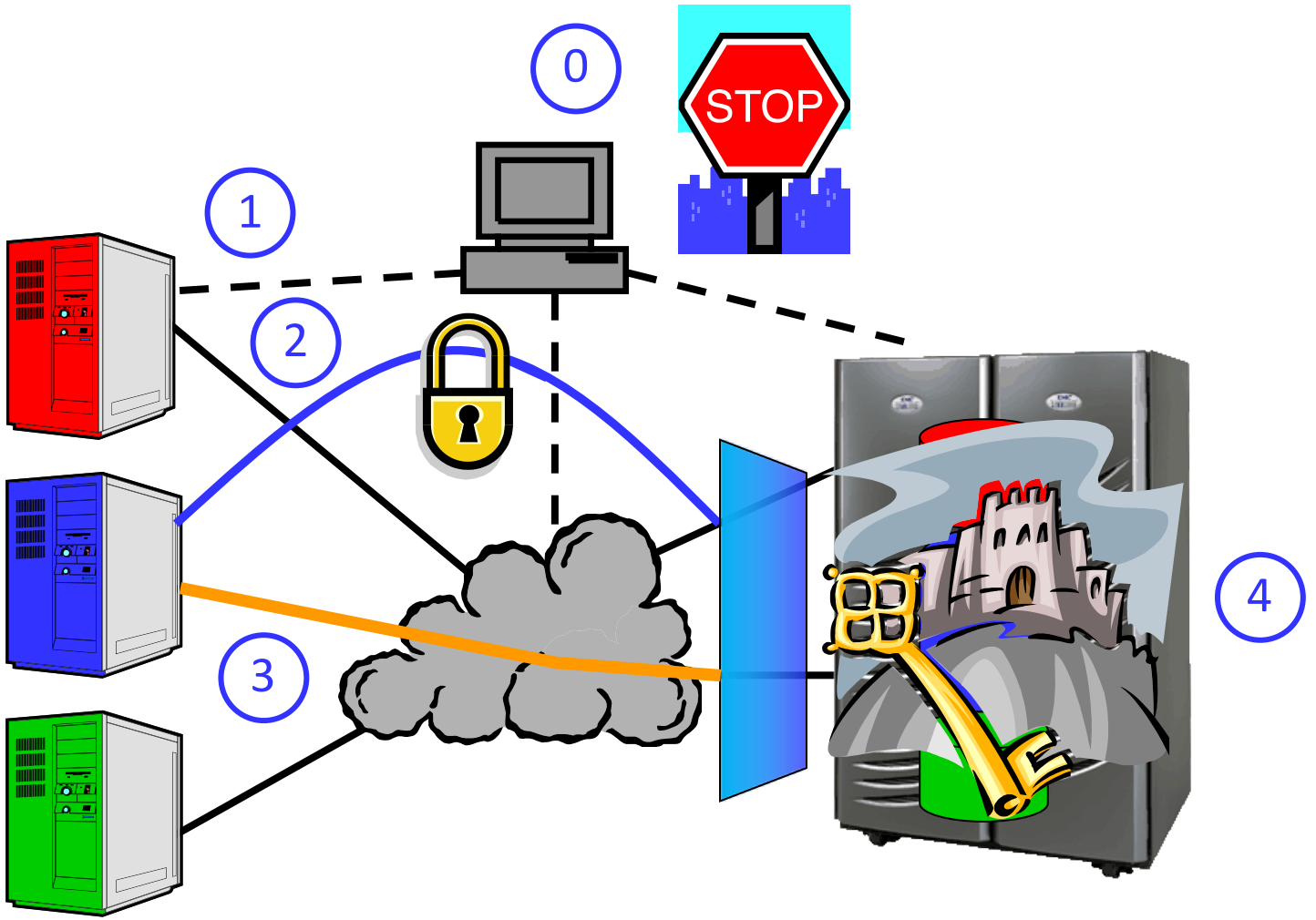
4) External Access
   - Media Theft
   - Other Access
- Countermeasure: Stored Data Encryption (data at rest)*
   - Application, server OS, VM guest OS
   - Hypervisor
   - Storage drives (SEDs)



*Storage Networking Security Series: Protecting Data at Rest https://www.snia.org/educational-library/storage-networking-security-series-protecting-data-rest-2020

Storage Networking Security Review

0) Management & System Integrity
1) Storage Access Control
2) Authentication (proof of identity)
3) Secure Channel (data in flight)
   - Confidentiality
   - Cryptographic Integrity
4) Stored Data (data at rest) Encryption*



*Storage Networking Security Series: Encryption 101 https://www.snia.org/educational-library/storage-networking-security-series-%E2%80%93-encryption-101-2020

SAN Protocols: Security Mechanisms Comparison

	Fibre Channel	iSCSI	NVMe over Fabrics/IP
Access control (1)	Zoning LUN masking	Network reachability LUN masking	Network reachability Namespace mapping
Authentication (2)	DH-CHAP FCAP FCPAP FC-EAP	CHAP SRP	DH-HMAC-CHAP
Secure Channel (3)	**FC ESP_Header**	**IPsec**	**TLS** (1.2 defined, 1.3 in progress)

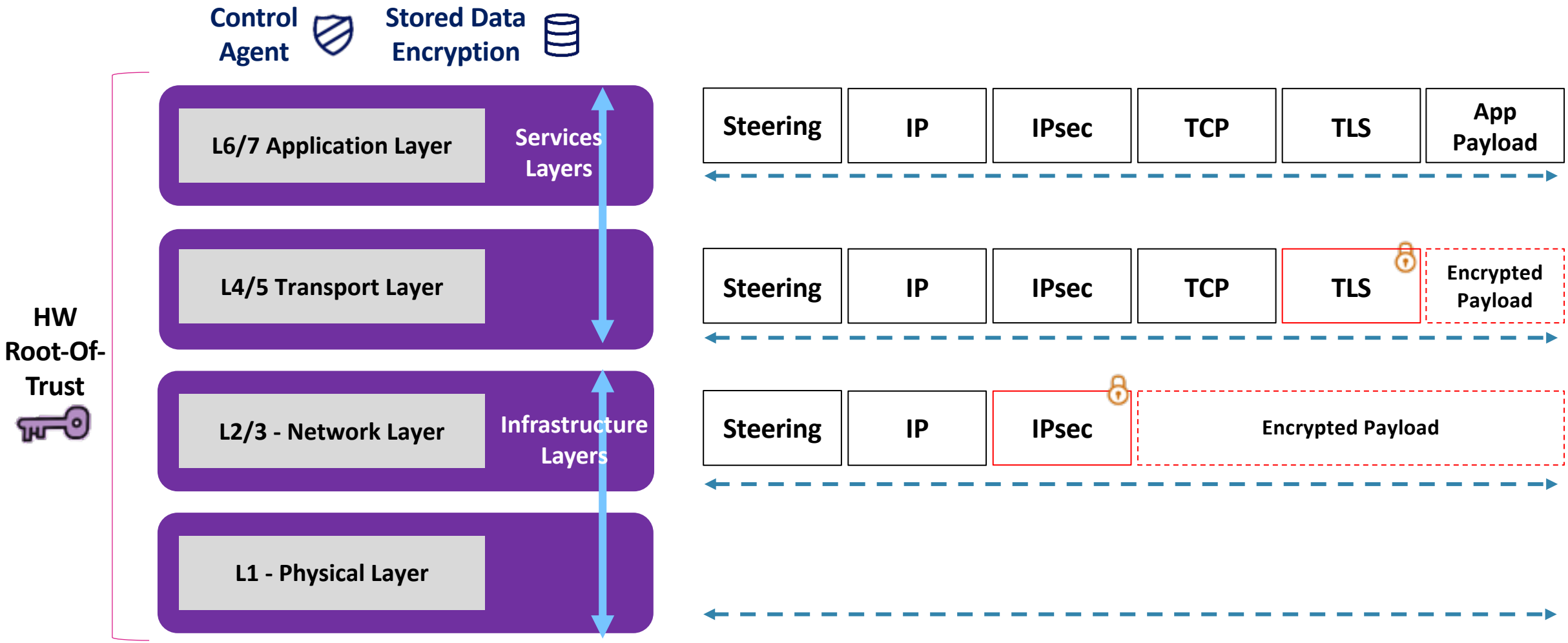
Data-in-Motion Security

Encryption Technologies

Ariel Kit

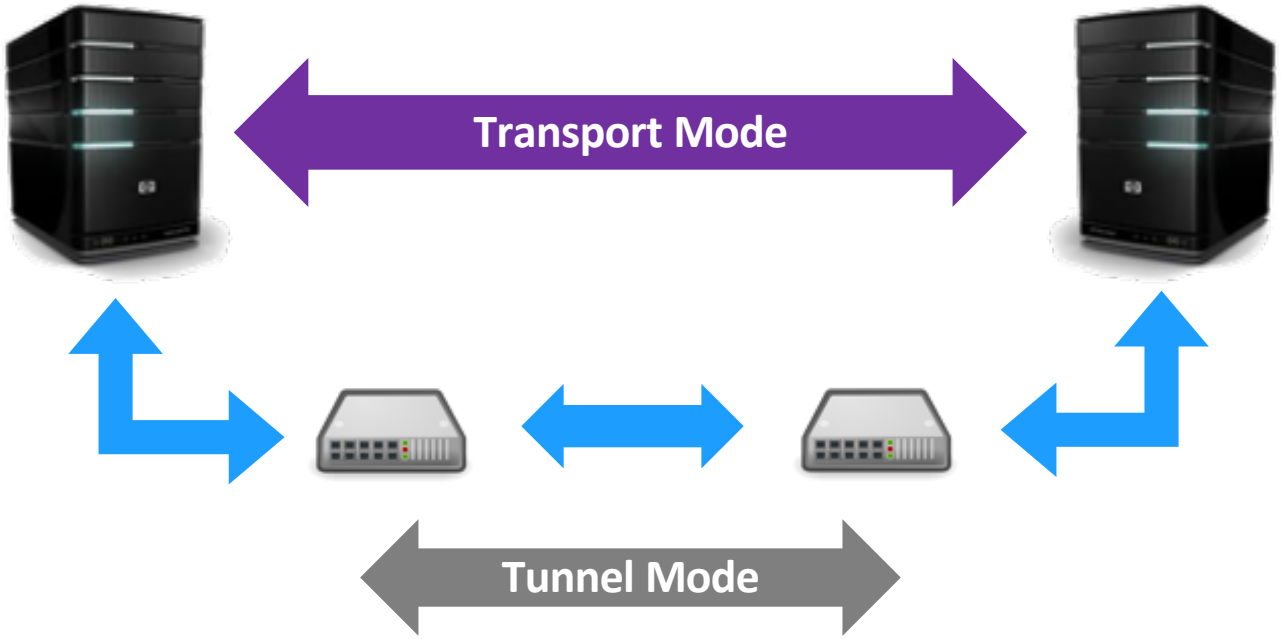
NVIDIA

Security in Different Layers (OSI)



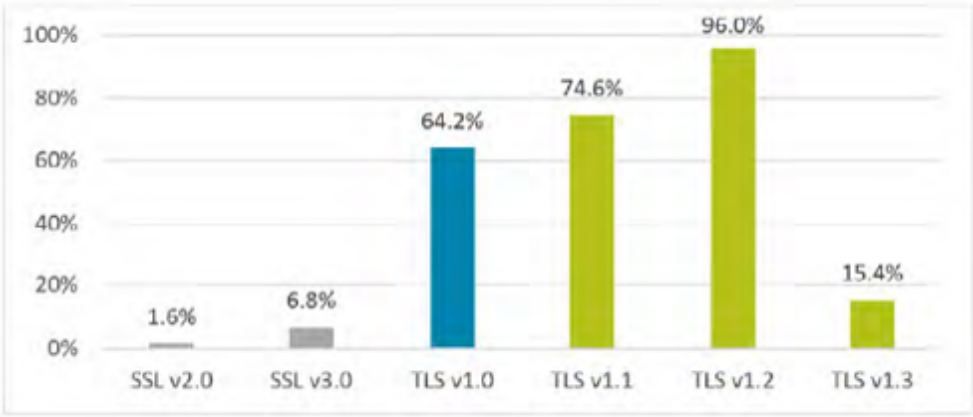
IPsec

- Generic encryption and authentication of any IP packet
- 2 IP protocols
  - AH - Authentication Headers
  - ESP - Encapsulating Security Payload
- 2 modes of operation
  - Tunnel – between IPsec gateways (VPN)
  - Transport – end-to-end communication
- Implementations
  - Site-to-site or edge-to-site (VPN)
  - OS\Server level encryption (Kernel IPsec)



Transport Layer Security (TLS)

- Privacy and data integrity between applications or micro-services
- Connection security/privacy by symmetric cryptography
- Identity and session keys negotiated using asymmetric cryptography
- Versions
  - 1.2 – widely deployed
  - 1.3 – better performance, more secure
- Implementations
  - Web applications (HTTPS)
  - Client/server application communication



SSL/TLS protocol support across world's most popular sites

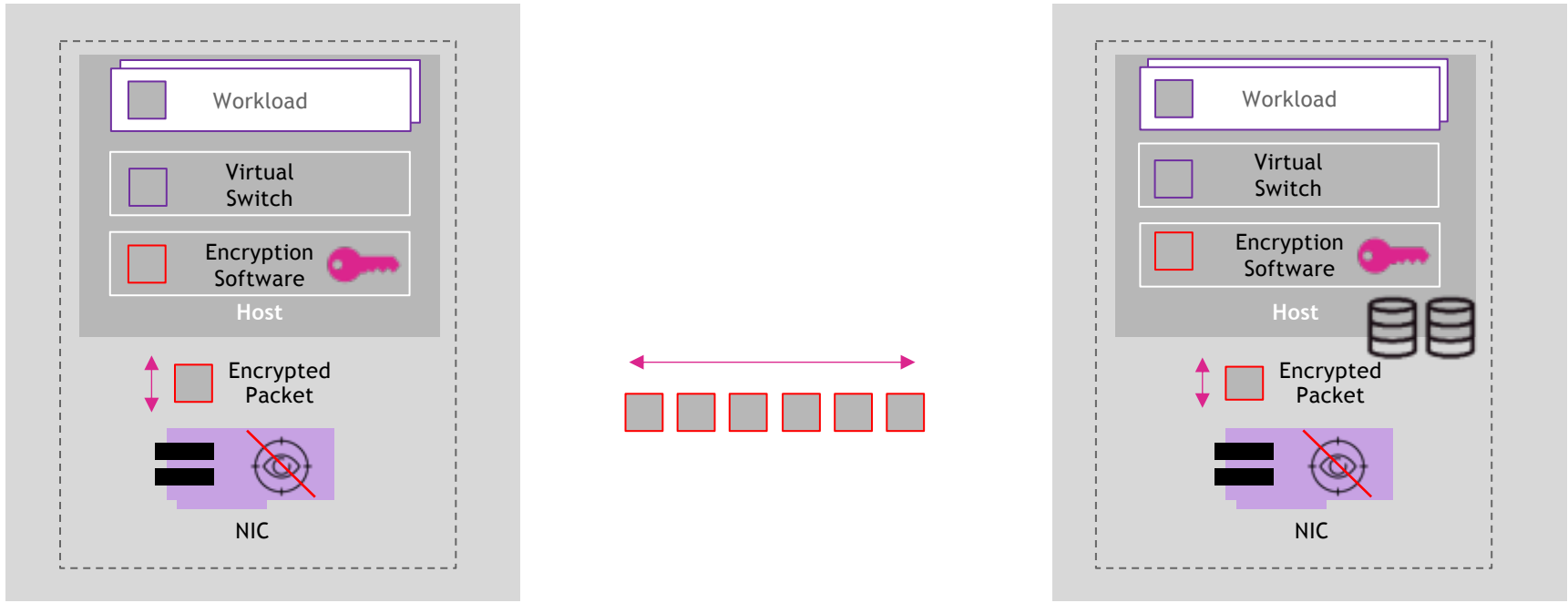
IPsec or TLS?

- Web 2.0 content and application based (SaaS)?
  - TLS is more popular as it is done at the application level to protect the content
- Infrastructure or cloud provider (IaaS)?
  - IPsec protects the communication between sites or servers and widely used to protect the north-south channels (application un-aware)
- East-west encryption?
  - IPsec and TLS are relevant, depends on the deployment and customer preferences including existing solutions. TLS is widely used for service mesh
- RoCE encryption?
  - IPsec is the only option as it can be fully implemented in hardware
- Transparent encryption for legacy and bare metal?
  - IPsec implementation can be hidden to the server OS and applications which also match regulatory requirements for data confidentially

To summarize:

- IPsec is used for applications that don't natively support any kind of protection
- TLS is used when the application is aware to the type of protection

Data Confidentiality Performance Challenges



Plaintext Packet

Encrypted Packet

Crypto is complex and compute hungry

Encrypted headers blind the network devices

NIC hardware accelerators become useless

Private and Public Cloud

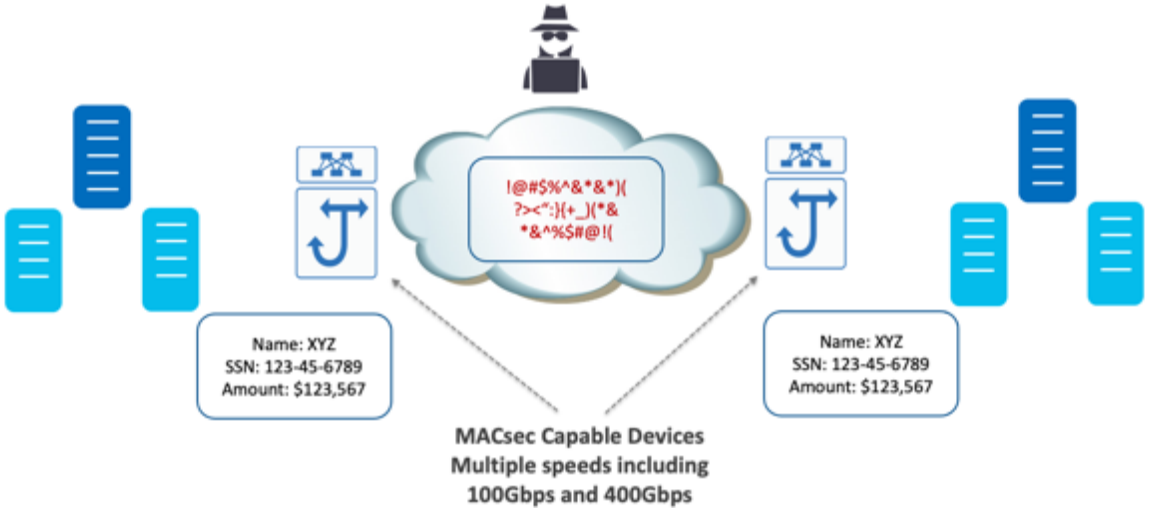
Data in-flight Network Encryption

Cesar Obediente

Cisco

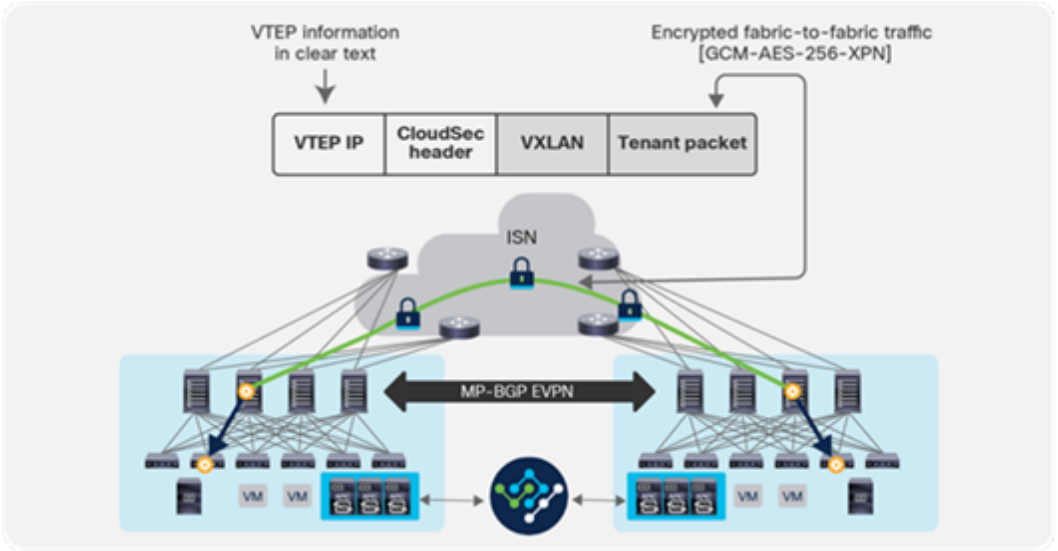
MAC Security - IEEE802.1AE

- Provides confidentiality, replay protection, and data integrity on Ethernet links between nodes
- Enabled on Point-to-Point Ethernet Link
  - Packets are decrypted on ingress port
  - Packets are in the clear in the device
  - Packets are encrypted on egress port
- Can co-exist with other security protocols:
  - IP Security (IPSec)
  - Secure Socket Layer (SSL)



Cloud Security Encryption

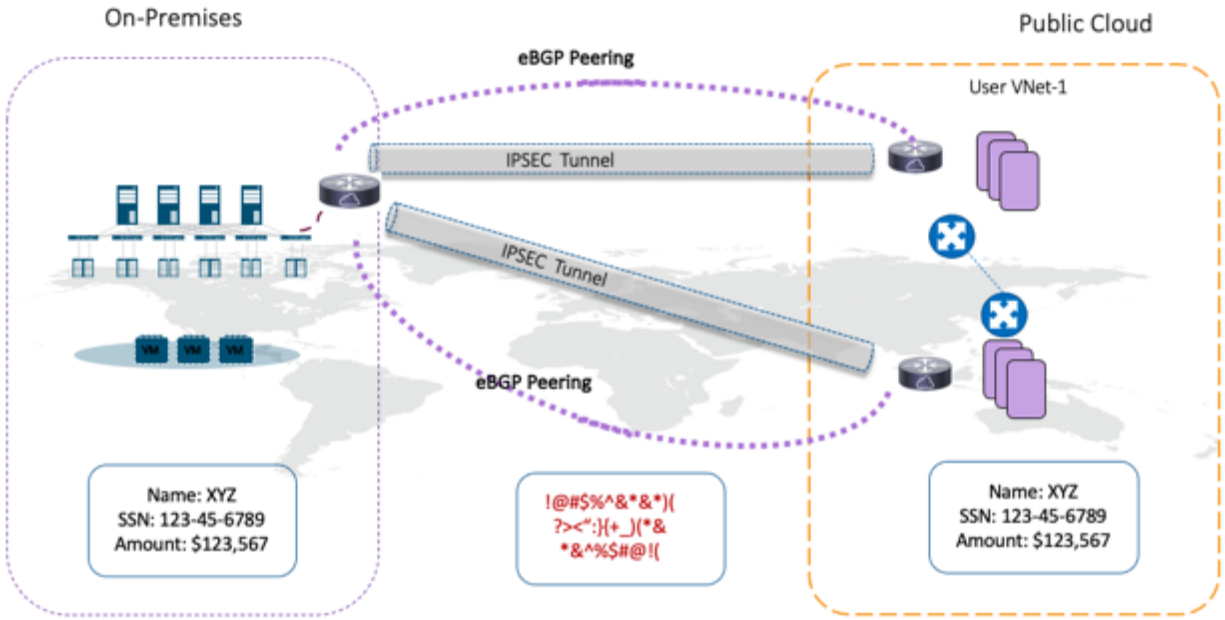
- Cloud security provides transport and encryption for VXLAN technology - “multi-hop MACsec”
- Cloud security offers secure tunnel between authorized VXLAN EVPN endpoints
- Cloud security leverages BGP to do the key exchange



Cloud Security - Multiple Data Centers
MacSec – Point-to-Point

Site-to-Site IPSec VPN

- Provides encryption to all the traffic over the Internet
- Maintain a permanent encrypted connection between the sites
- Protocols
  - AH - Authentication Headers
  - ESP - Encapsulating Security Payload
- Modes of operation
  - Tunnel
  - Transport



Fibre Channel
Securing Data in the Datacenter

Brandon Hoff

Broadcom

FC-SP-2: What and Why?

- **Why?** : Need to transition SANs from **Authorization and segmentation** based FC security to **authentication and encryption** based security!

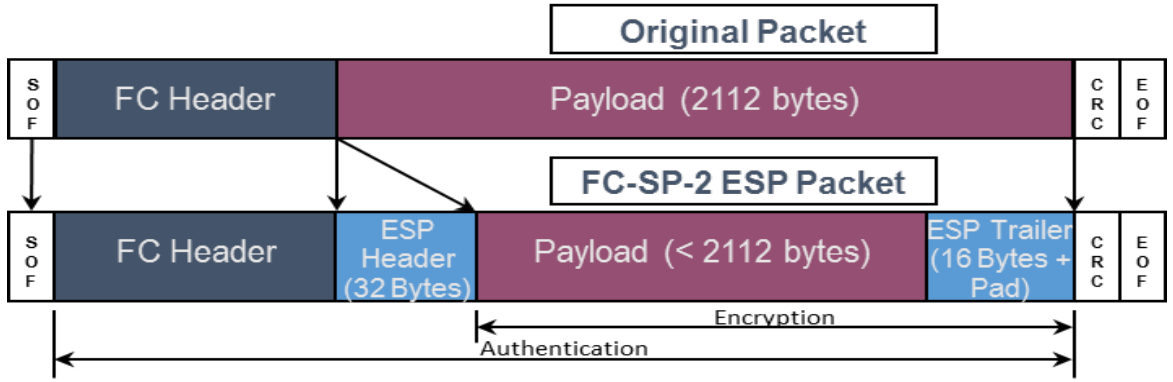
- **What?** FC-SP-2 is a ANSI/INCITS standard (2012) that defines protocols to –
  - **Authenticate** Fibre Channel entities
  - **Setup** session **encryption keys**
  - Negotiate parameters to ensure per **frame integrity and confidentiality**
  - Define and **distribute security policies** over FC

- Designed to protect against several classes of threats

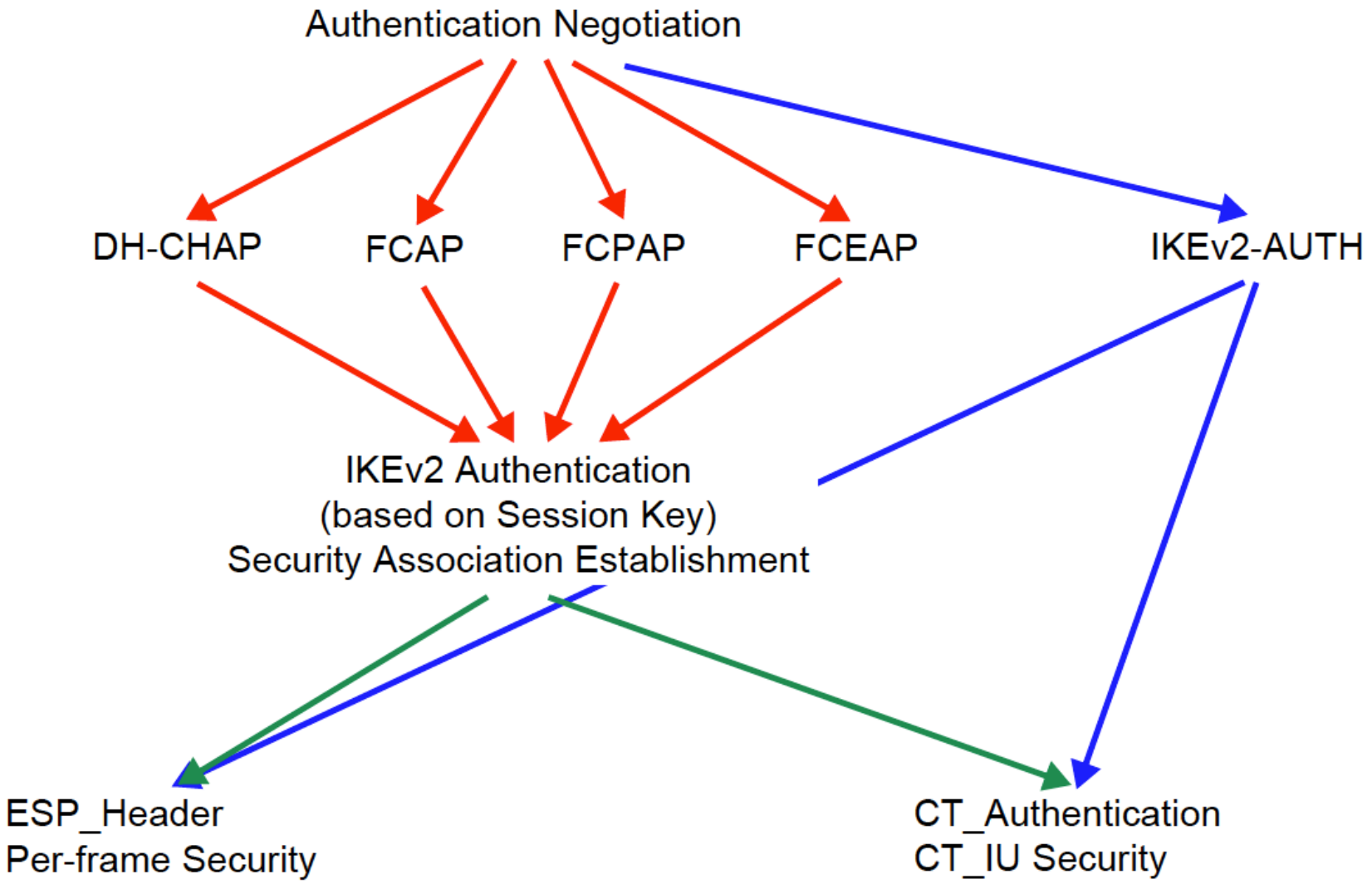
FCIA Webinar: "Fibre Channel and Security"
https://www.brighttalk.com/webcast/14967/363593

FC-SP-2 *ESP_header*

- *ESP_header* (optional) is a layer 2 security protocol that provides
  - Origin authentication, Integrity, Anti-replay protection, Confidentially
- Encapsulating Security Payload (ESP) is defined in RFC 4303
- FC-FS-3 defines optional headers for Fibre Channel, FC-SP defines how to use ESP in Fibre Channel
- Similar protections exist for CT_Authentication



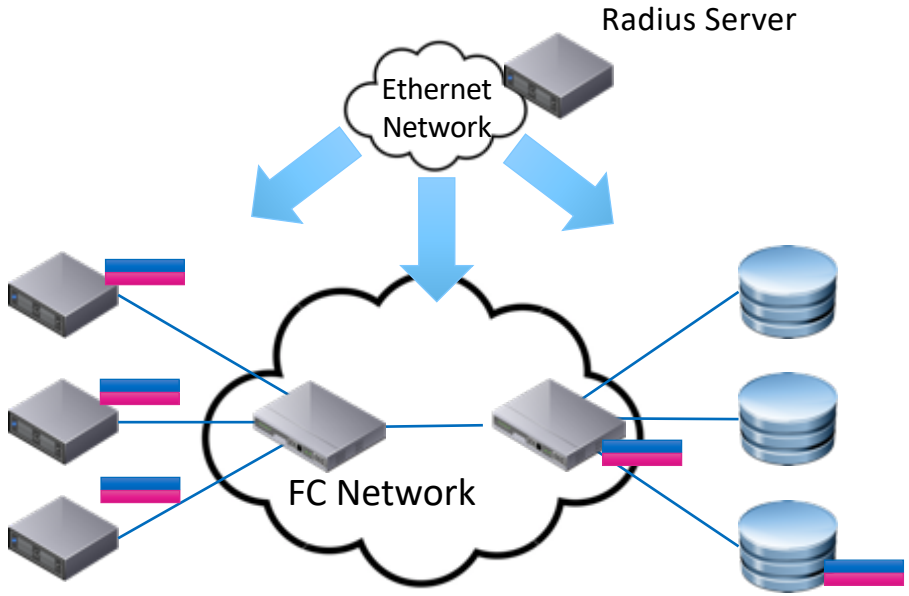
Authentication Protocols and SAs



Managing Secrets, Passwords, and Certs

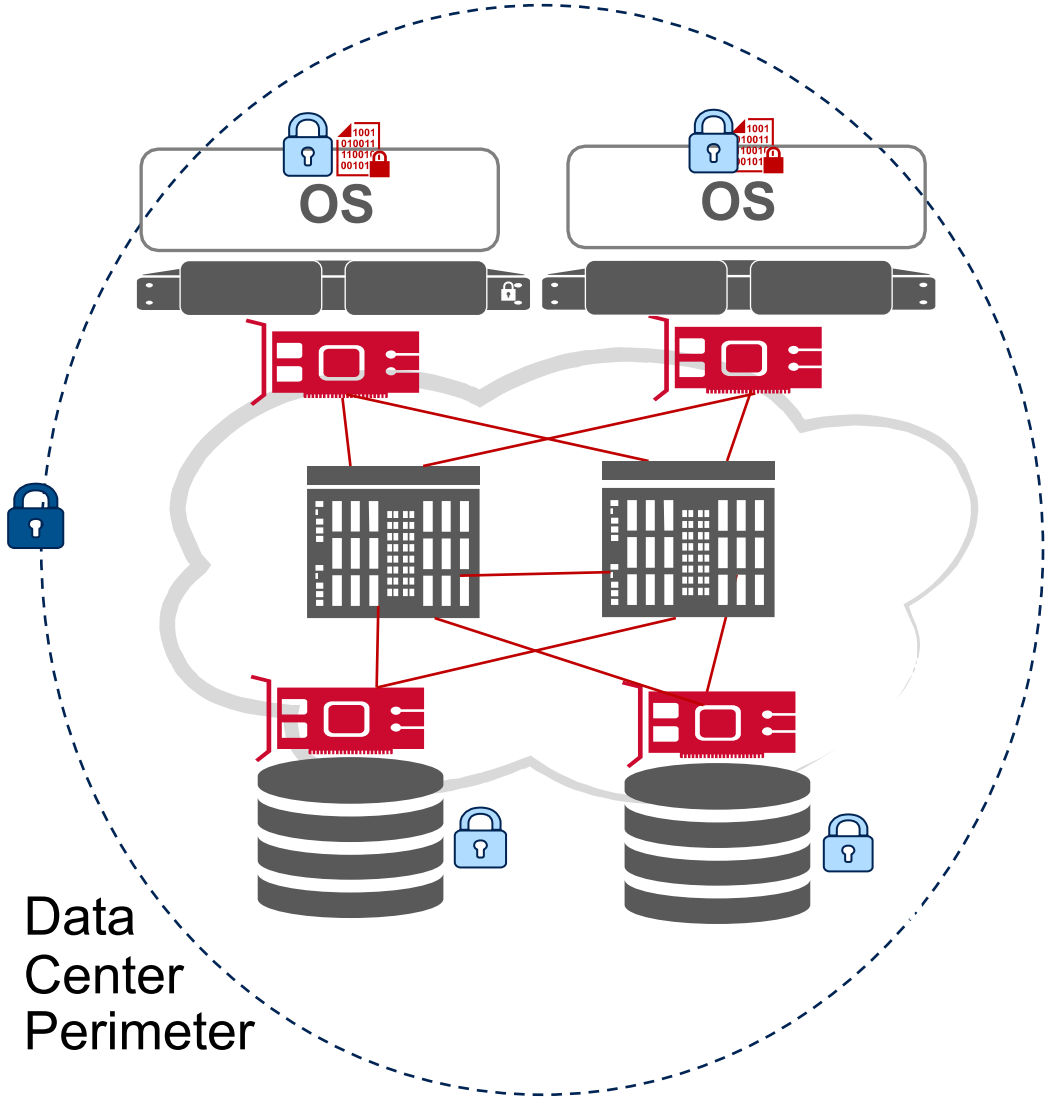
- For mutual authentication, each device needs to know the credentials of
  - The adjacent device
  - End nodes for end-to-end
- Manual configuration becomes difficult
  - 50,000 or more credentials are possible in large environments
- Options for managing credentials
  - RADIUS
  - KMIP
  - Public Certificate Authority
  - Internal Certificate Authority
- Unfortunately, not supported in any open systems operating system

Sharing the credentials of one device



DH-CHAP Credentials: Name Secret

Fibre Channel SAN Threat Mitigation

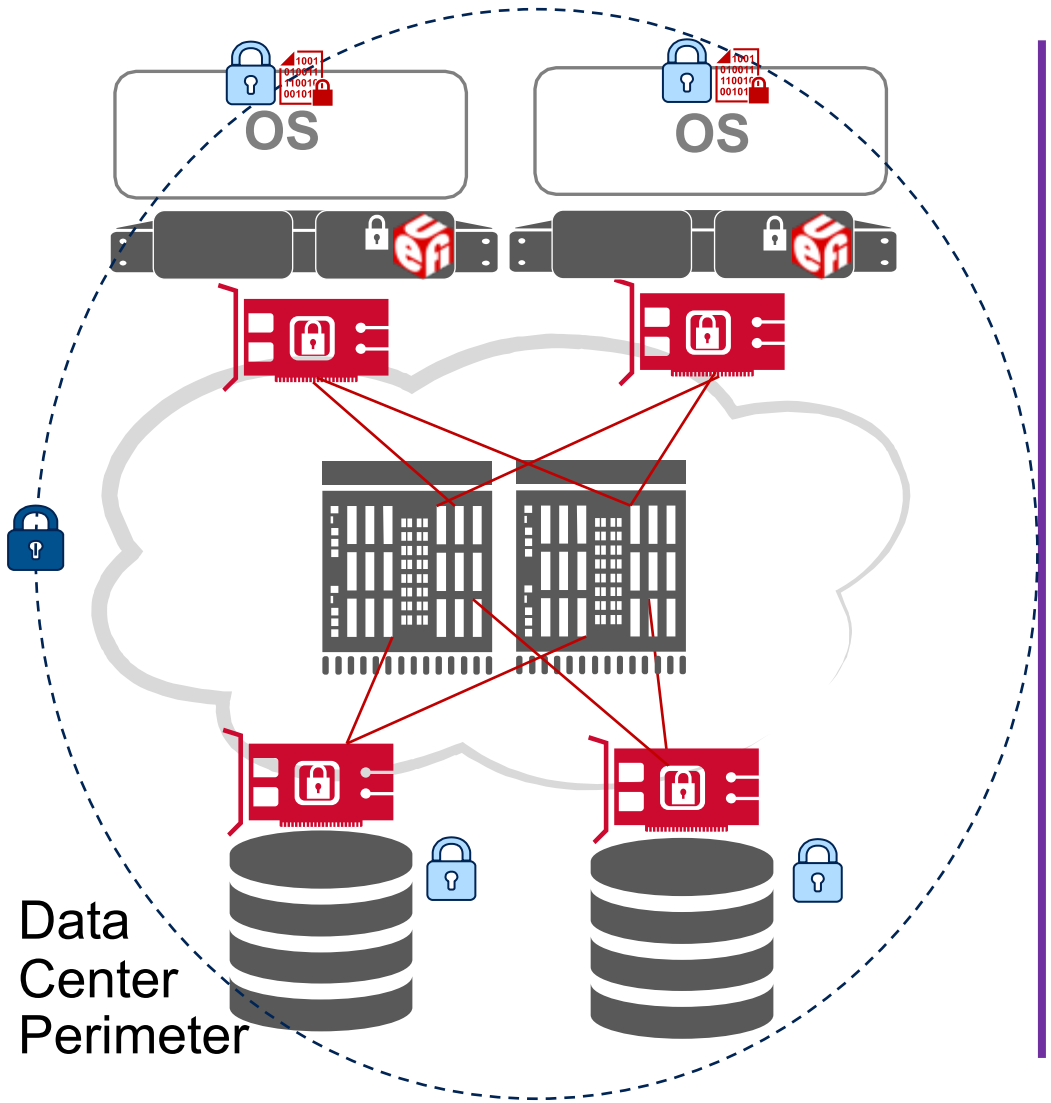


“Outside Job” Threats

“Inside Job” Threats

Unlikely Threats

Full Fibre Channel Storage Security Stack



Digitally Signed Drivers

Integrated with OS security guidelines/best practices.

Secure UEFI Fibre Channel Boot

Digitally signed boot image that is validated by the server prior to system boot. Supported by all major server OEMs.

Digitally Signed Firmware Upgrade

Firmware images digitally signed by the vendor. Signature check and validation before firmware update.

Secure User Interfaces

User ACLs, RBAC, SSL, etc.

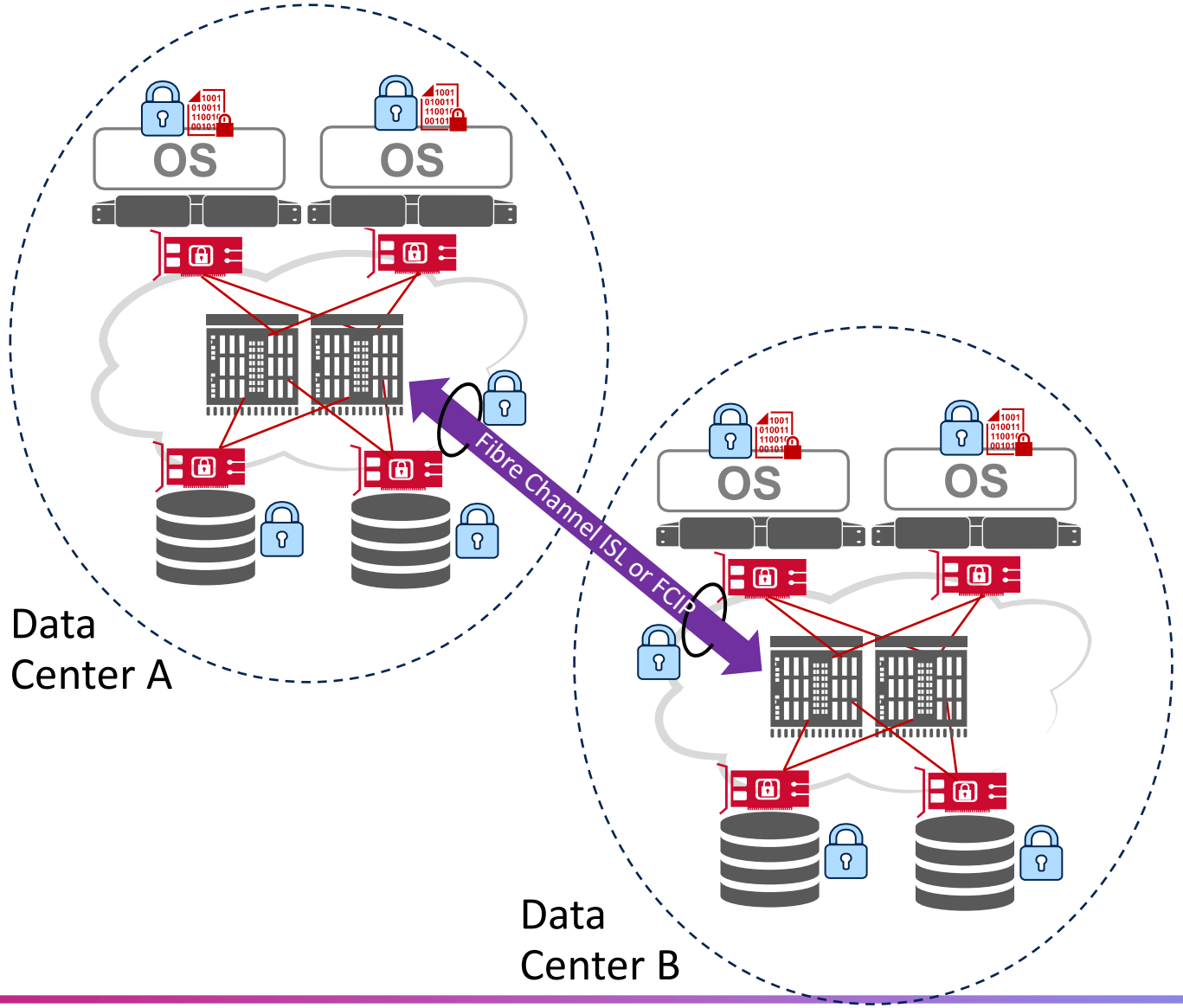
Fabric based Authorization and Authentication

Zoning, FC-SP Authentication, LUN Masking

Digitally signed software stack for the array

Extends security features to the storage array.

Best Practices for Encryption in Fibre Channel SANs



Data At Rest Encryption

Encrypt in the storage system to protect data on SSDs and Hard Disks when they are taken out of the array.

Data In Flight Encryption

Encrypt data in flight when it leaves the secure boundary of the data center. Usually for site-to-site Fibre Channel links (ISLs) or FCIP.

Minimize Cost and Risk

Avoid the cost and complexity of data in flight encryption inside the data center. No commercially available options.

Summary

- We've discussed
  - Storage networks security framework
  - Data-in-motion security
  - Private and public cloud
  - Securing data in the datacenter
- Ensuring data is secure requires more than just a lock & key when it's stored; it needs *in-transit security*
  - Secure data is possible, even if it's eavesdropped, intercepted, copied or hacked on private or public networks
  - Essential on an insecure & unreliable edge

More SNIA Security Resources

- Storage Networking Security Webcast Series: On-demand at the SNIA Educational Library: snia.org/educational-library
  - Understanding Storage Security and Threats
  - Protecting Data at Rest
  - Encryption 101
  - Key Management 101
  - Security & Privacy Regulations
  - Applied Cryptography
- Follow us on Twitter @SNIANSF for dates and times of others planned:
  - Securing the Protocol
  - Securing the System: Hardening Methods
- SNIA TLS Specification for Storage Systems

After this Webcast

- Please rate this webcast and provide us with your feedback
- This webcast and a copy of the slides will be available at the SNIA Educational Library https://www.snia.org/educational-library
- A Q&A from this webcast, including answers to questions we couldn't get to today, will be posted on our blog at https://sniansfblog.org/
- Follow us on Twitter @SNIANSF

Thank You

