TSTC

ICT en Security Trainingen

The Layer oft Forgotten

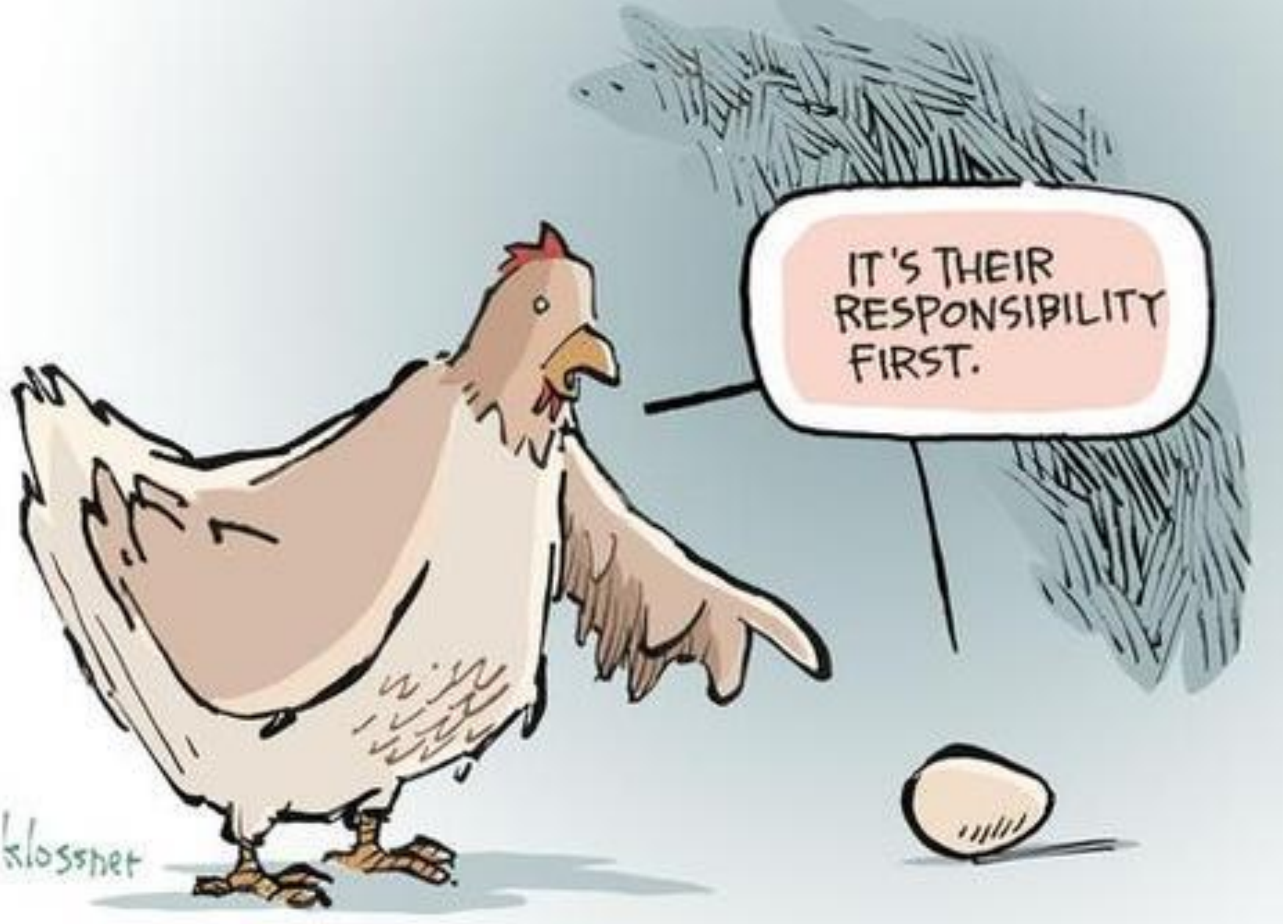
When discussing cloud we often forget about the virtual layer!

Who is talking?

- Duane Anderson, RAZR Technologies, LLC.
- Just a guy from Iowa! We grow corn not potatoes or buckeyes! (Not Idaho or Ohio)
- Security Consultant and Instructor
    - Global Reach - 33 Countries
- Works with all Sizes of Companies
- Currently spending time in virtualization and cloud
- Certifications: CCSP, VCP, CASP, Security+, CPTE, CPTC, CDFE, CISSO, CEH and others.

What are we covering today?

- What is the common reaction to cloud computing?
- Security provided by the CSP?
- What is stated in the Agreements?
- Why does the virtual layer matter?
- What should we do in the end?
- Continuing Education



Cloud Security Explained

Common Reaction’s

1. NO WAY, it is not secure!

2. It will save us money, so lets go!

I MIGRATED OUR NORTHERN DATA CENTER TO THE CLOUD.
Dilbert.com DilbertCartoonist@gmail.com
BUT THE CLOUD STOPPED WORKING AND I CAN'T FIND THE PHONE NUMBER FOR OUR CLOUD GUY.
SO . . . WHATEVER.
7-5-13 ©2013 Scott Adams, Inc./Dist. by Universal Uclick
YOU LOST OUR DATA CENTER?
THAT'S ONE WAY TO LOOK AT IT.

What security is provided?

- They are all different! Let’s take a look!
    - Microsoft
    - Amazon
    - Internap

Microsoft Azure Security

- Office 365 and Azure
  - Encrypts data in transit
  - Encrypts data at rest
- Much more available – this is not complete

- https://azure.microsoft.com/en-us/support/trust-center/

Amazon AWS Security

- AWS offers you the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features.
  - Data encryption capabilities
  - Key Management services
  - HSM available
- AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.
- Encrypts data in transit

- https://aws.amazon.com/security/

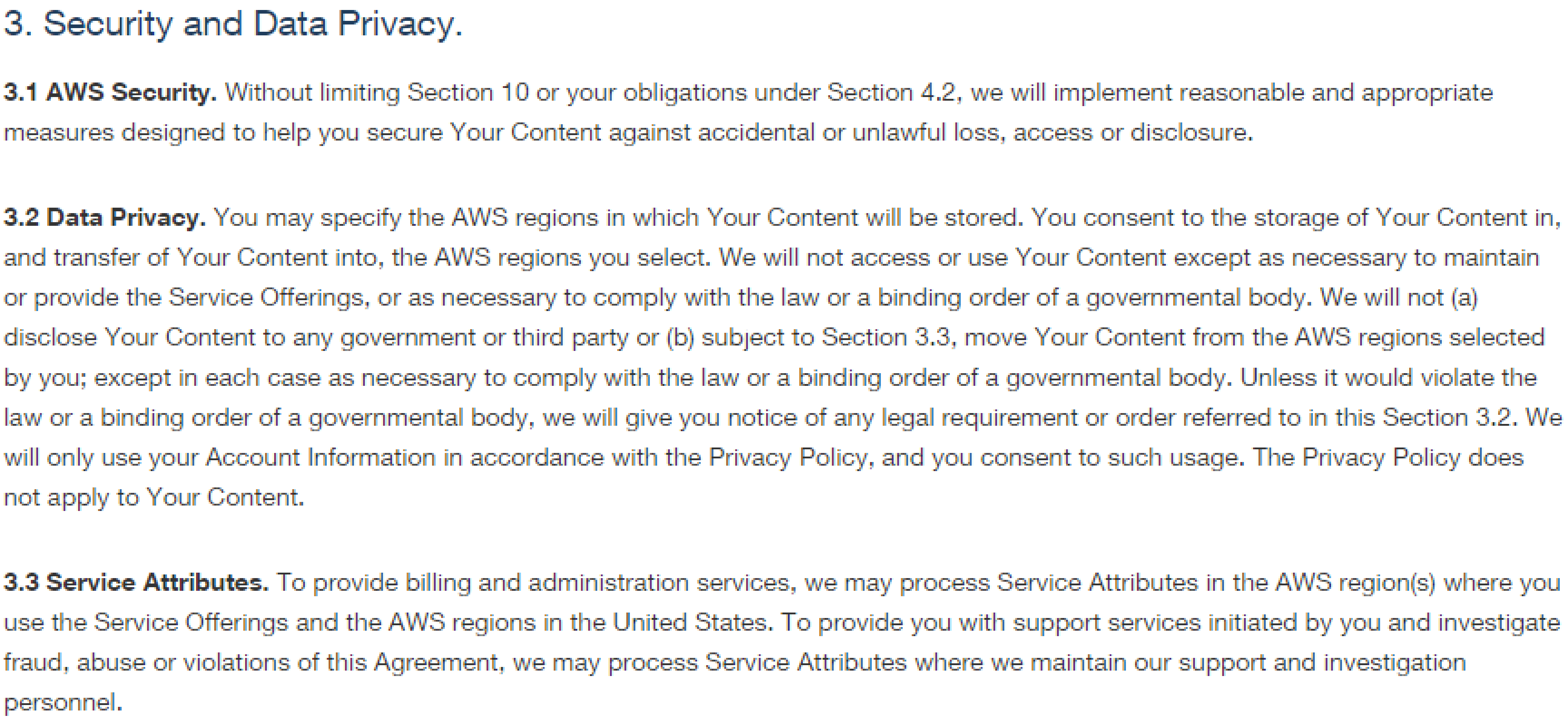
Internap Private Cloud Data Security

- Full Isolation
- Automation is utilized
  - IDS
  - Monitoring
- Dynamically configured firewall
- Access Control

- Compliance Standards
  - Payment Card Industry and Data Security Standards (PCI DSS)
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)

How about the agreements?

- They are even less detailed!



3. Security and Data Privacy.

3.1 AWS Security. Without limiting Section 10 or your obligations under Section 4.2, we will implement reasonable and appropriate measures designed to help you secure Your Content against accidental or unlawful loss, access or disclosure.

3.2 Data Privacy. You may specify the AWS regions in which Your Content will be stored. You consent to the storage of Your Content in, and transfer of Your Content into, the AWS regions you select. We will not access or use Your Content except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body. We will not (a) disclose Your Content to any government or third party or (b) subject to Section 3.3, move Your Content from the AWS regions selected by you; except in each case as necessary to comply with the law or a binding order of a governmental body. Unless it would violate the law or a binding order of a governmental body, we will give you notice of any legal requirement or order referred to in this Section 3.2. We will only use your Account Information in accordance with the Privacy Policy, and you consent to such usage. The Privacy Policy does not apply to Your Content.

3.3 Service Attributes. To provide billing and administration services, we may process Service Attributes in the AWS region(s) where you use the Service Offerings and the AWS regions in the United States. To provide you with support services initiated by you and investigate fraud, abuse or violations of this Agreement, we may process Service Attributes where we maintain our support and investigation personnel.

Why does the virtual layer matter?

- What are the top cloud security risks?
  - https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf
- Is that really everything?
  - VMware vSphere Hardening Guide has over 70 specific vulnerabilities!
  - And another 85 moved to the general documentation!

  - What about Azure, Amazon and other cloud providers?

The Treacherous 12!

- Data Breaches
- Insufficient Identity, Credential and Access Management
- Insecure Interfaces and APIs
- System Vulnerabilities
- Account Hijacking
- Malicious Insiders
- Advanced Persistent Threats
- Data Loss
- Insufficient Due Diligence
- Abuse and Nefarious Use of Cloud Services
- Denial of Service
- Shared Technology Issue

Areas of Concern
The short list!

- Privileged Accounts
  - What can an administrator actually access?

Privileged Account

- Can they view your desktop?
- Can a user get access to a privileged account?
- Can a read only user do more than read?

Areas of Concern
The short list!

- Privileged Accounts
  - What can an administrator actually access?
- Networking – Management Environment
  - Is my data actually separate like they say?

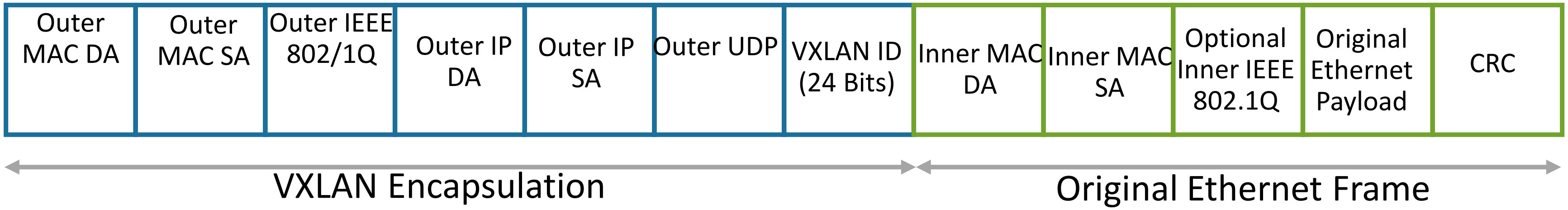
Networking

- How does traffic flow?
- Can my traffic be sniffed by the CSP?

VXLAN

- Used by Microsoft Server 2016 and VMware NSX

- Uses User Datagram Protocol (UDP) encapsulation
- Enables the network to stretch across multiple clusters and Layer 3 segments of the datacenter.
- Scales to 16 million segments
- Utilizes a Distributed Switch as its core networking.

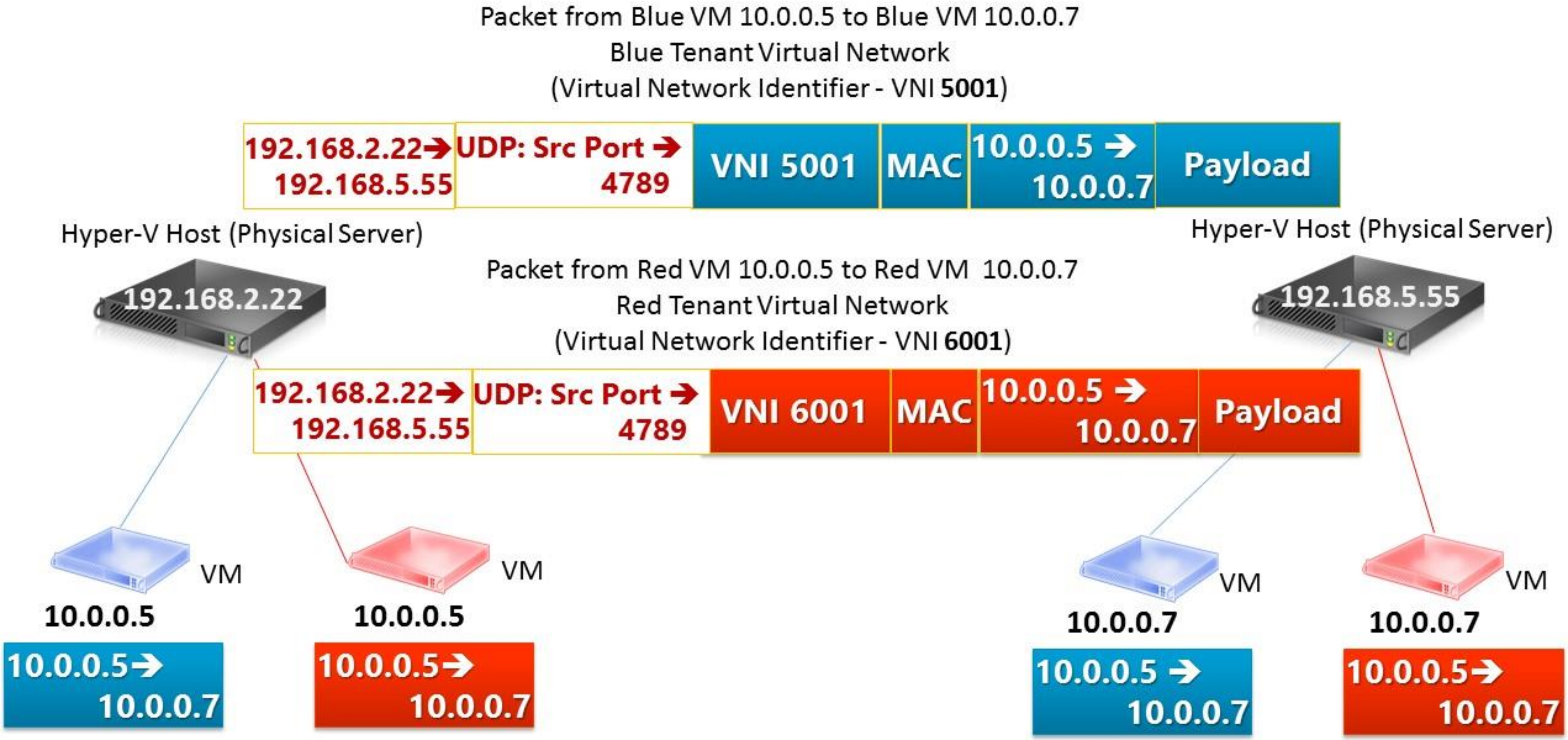


Outer MAC DA	Outer MAC SA	Outer IEEE 802/1Q	Outer IP DA	Outer IP SA	Outer UDP	VXLAN ID (24 Bits)	Inner MAC DA	Inner MAC SA	Optional Inner IEEE 802.1Q	Original Ethernet Payload	CRC

VXLAN Encapsulation

Original Ethernet Frame

VXLAN

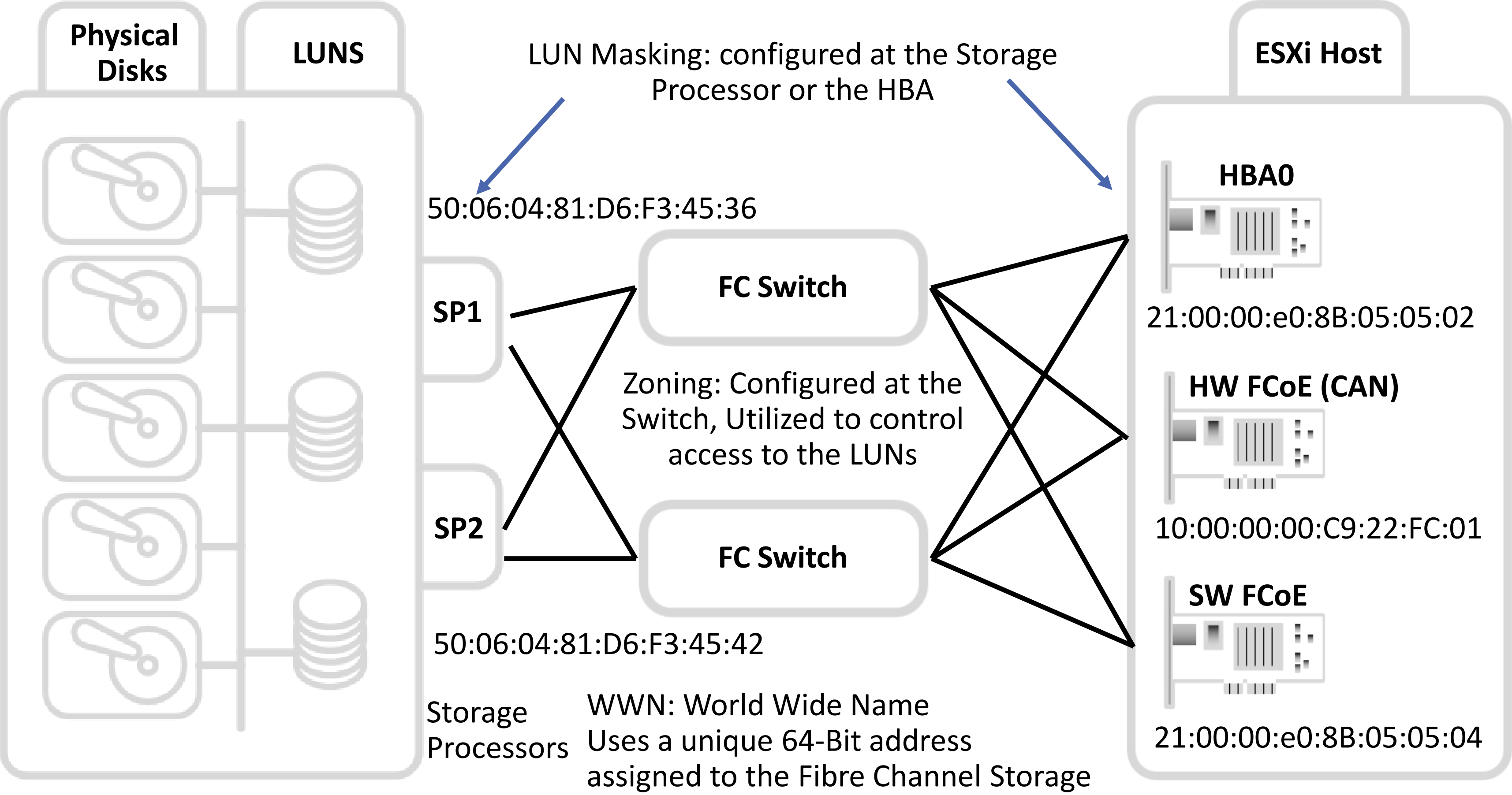


https://blogs.technet.microsoft.com/networking/2016/10/26/network-virtualization-with-ws2016-sdn/

Areas of Concern
The short list!

- Privileged Accounts
  - What can an administrator actually access?
- Networking – Management Environment
  - Is my data actually separate like they say?
- Data in Transit
  - From where to where?

Fibre Channel Environment



LUN Masking: configured at the Storage Processor or the HBA

Zoning: Configured at the Switch, Utilized to control access to the LUNs

WWN: World Wide Name
Uses a unique 64-Bit address assigned to the Fibre Channel Storage Processors or HBAs
FCoE: The IPs are assigned to the Vmkernel ports that the FCoE utilize

Areas of Concern
The short list!

- Privileged Accounts
  - What can an administrator actually access?
- Networking – Management Environment
  - Is my data actually separate like they say?
- Data in Transit
  - From where to where?
- Other hypervisor specific concerns!
  - Specific security risks; API issues, account management issues

Do we or don’t we?

- Depends on Data in question!
- Data Classification!
    - Secret
    - Confidential
    - Company Confidential
    - Public
- How the data is being used!
- Your requirements around that data being used!

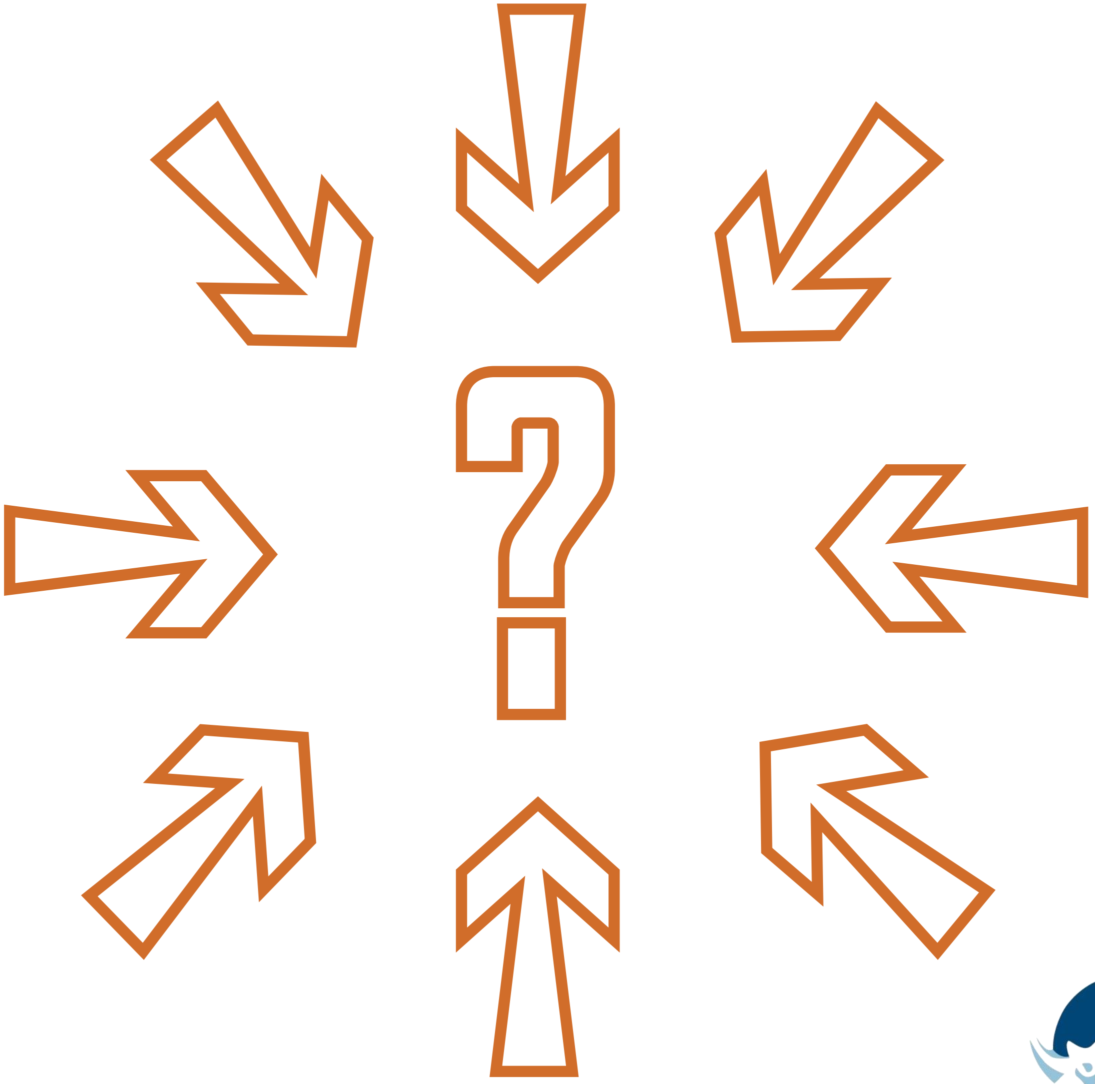
Continuing Education

- Fast growing security certification:
  - ISC2 – CCSP – Certified Cloud Security Professional
- What we teach
  - Items needed for the certification
  - Items needed for the real world
  - Hands on labs covering IaaS Private Cloud, IaaS Public Cloud and SaaS
- Only TSTC provides additional real world implementations and discussions beyond the lecture associated with the CCSP exam preparation!
- Come visit us at booth E148

TSTC

ICT en Security Trainingen

Questions



ICT en Security Trainingen