NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Project 2016-02
CIP Modifications

Webinar on Standard Drafting Team Considerations for the Use of **Virtualization in the CIP Environment**
July 19, 2017

RELIABILITY | ACCOUNTABILITY

Agenda

- Opening Remarks and Introduction of Presenters
- Standard Drafting Team
- Administrative Items
  - Antitrust and Disclaimers
  - Webinar Format
- Storage Virtualization
- Questions and Answers

Administrative Items

- NERC Antitrust Guidelines
  - It is NERC’s policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.
- Notice of Open Meeting
  - Participants are reminded that this webinar is public. Notice of the webinar was posted on the NERC website and the access number was widely distributed. Speakers on the call should keep in mind that the listening audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

CIP Standard Drafting Team

	Name	Entity
Co-Chair	Christine Hasha	Electric Reliability Council of Texas
Co-Chair	David Revill	Georgia System Operations Corporation
Members	Steven Brain	Dominion
	Jay Cribb	Southern Company
	Jennifer Flandermeyer	Kansas City Power and Light
	Tom Foster	PJM Interconnection
	Richard Kinas	Orlando Utilities Commission
	Forrest Krigbaum	Bonneville Power Administration
	Philippe Labrosse	Hydro-Quebec TransEnergie
	Mark Riley	Associated Electric Cooperative, Inc.

Virtualization Webinar : Purpose

- Purpose of this presentation:
  - To inform and educate industry stakeholders to help them participate in the discussions around virtualization
  - To improve feedback on comment forms
  - To validate concepts that the SDT has developed with real-world use cases

**Note: The examples and use cases shown here are for discussion purposes only, and are not intended to be guidance for implementing any CIP compliance program

Virtualization Webinar Recap

- Webinar #1
  - Virtualization Overview
  - Logical Isolation / Management Plane Isolation
  - Introduction of Centralized Management System (CMS)
  - Network Topology
- Webinar #2
  - Hypervisors (Templates, VM Mobility, Resource Scheduler, etc.)
  - Multi-Tenancy (Tenants, Underlay Networks, etc.)
  - Introduced ESZ Concept (Logical Separation)
- Webinar #3
  - Storage

Webinar 3 - Storage Summary

Storage

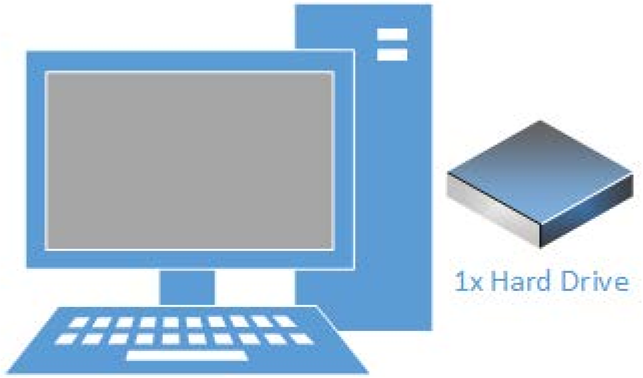
- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection

Storage Definitions

- **Redundant Array of Independent Disks(RAID) –** a technology used to prevent the loss of data from the failure of an independent disk
- **Storage Processor** – the server built into the storage array for providing access to the shared storage
- **Storage Array –** Generally referred to as the combination of disks and the storage processor
- **Host BUS Adapter(HBA) –** Used to provide servers access to a storage array network
- **Storage Network –** Provides transport between the components of a storage system
- **Storage Area Network –** Collection of HBA, Storage Processors, Storage Arrays and disks

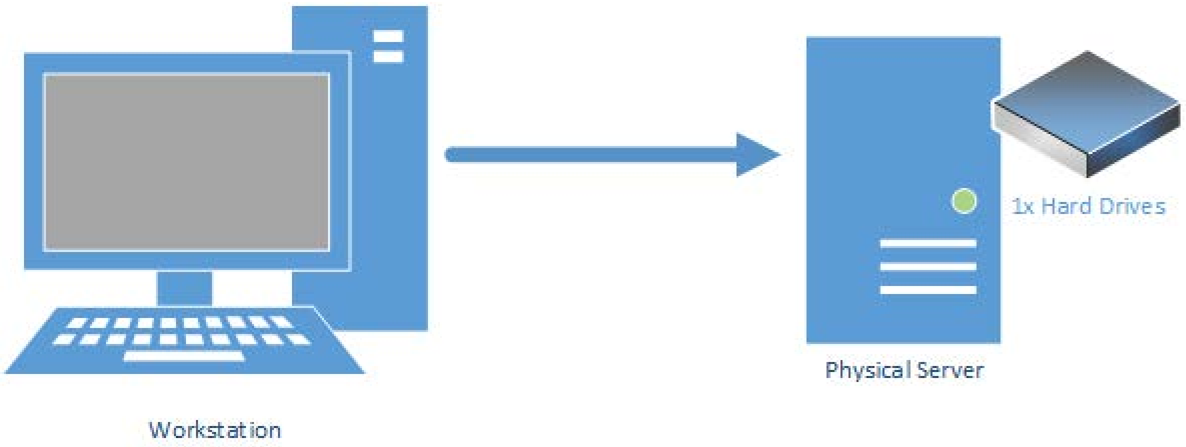
Evolution of Storage Solutions (1 of 8)

- The Personal Computer
  - Difficult to share data between users
  - Failure results in the total loss of data



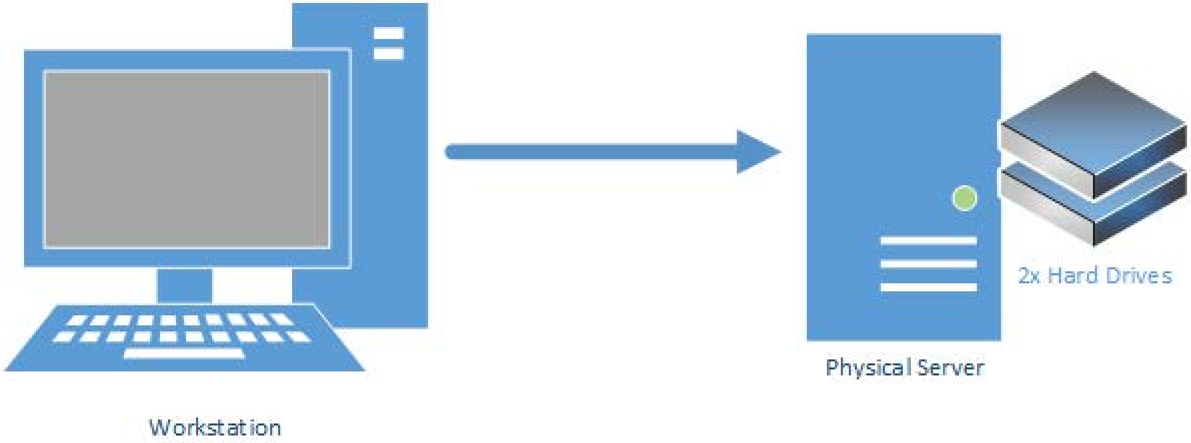
Evolution of Storage Solutions (2 of 8)

- Server Model
  - Easy to share data
  - Single drive failure still results in the total loss of data



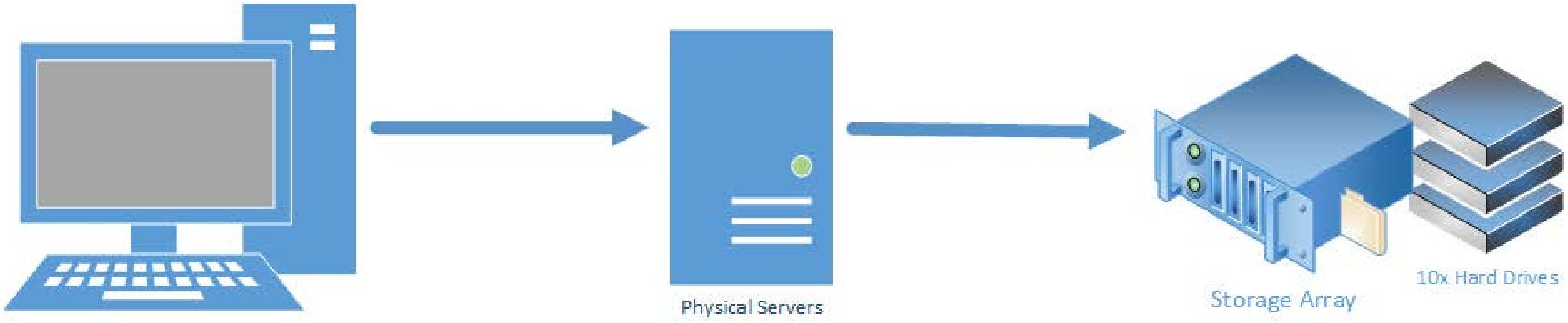
Evolution of Storage Solutions (3 of 8)

- Server w/ RAID
  - Redundancy allows a single drive to fail without the loss of data
  - Wastes 30-50% of storage
  - Servers have a limited number of slots for drives



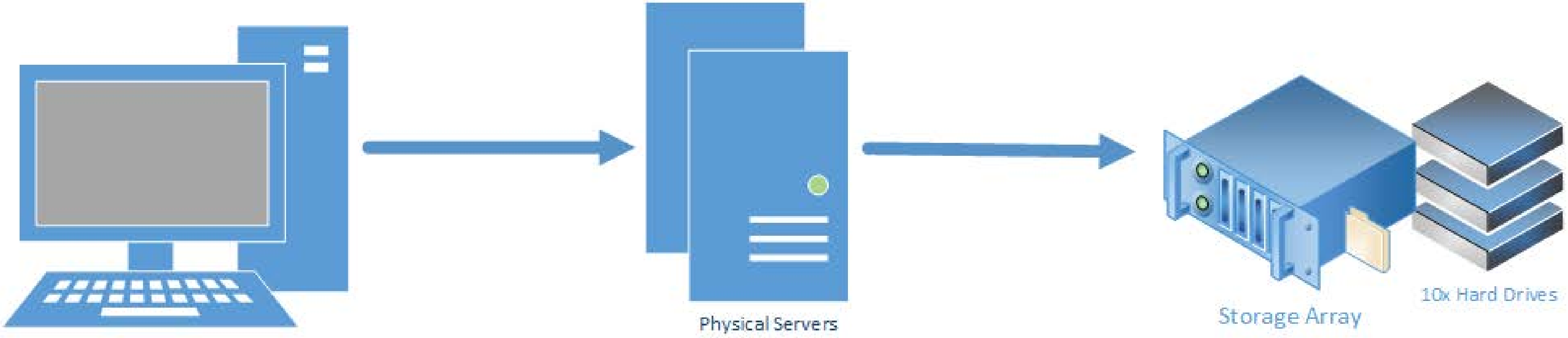
Evolution of Storage Solutions (4 of 8)

- Server with Direct Attached Storage
  - Wastes ~30% of storage
  - Each server has drives to manage and maintain
  - Server Hardware failure results in total outage to applications
  - Applications are installed directly to the physical server



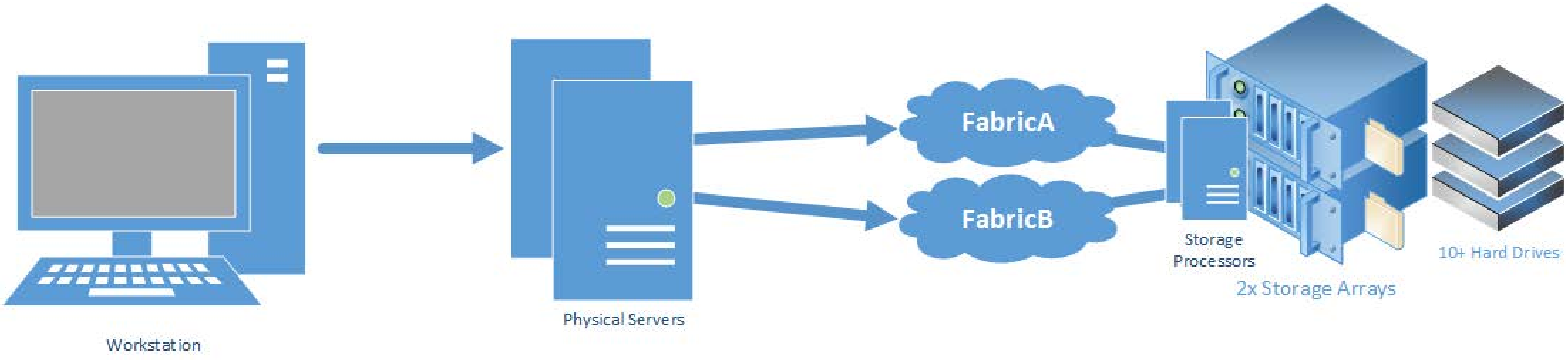
Evolution of Storage Solutions (5 of 8)

- Redundant Servers with Direct Attached Storage
  - Since the Data exists outside of the servers, multiple servers can be used to support the application
  - Direct Attached Storage Array is now the single point of failure
  - Complex Environment – Experts only
  - Limited Application Support
  - Cabling Distance VERY limited



Evolution of Storage Solutions (6 of 8)

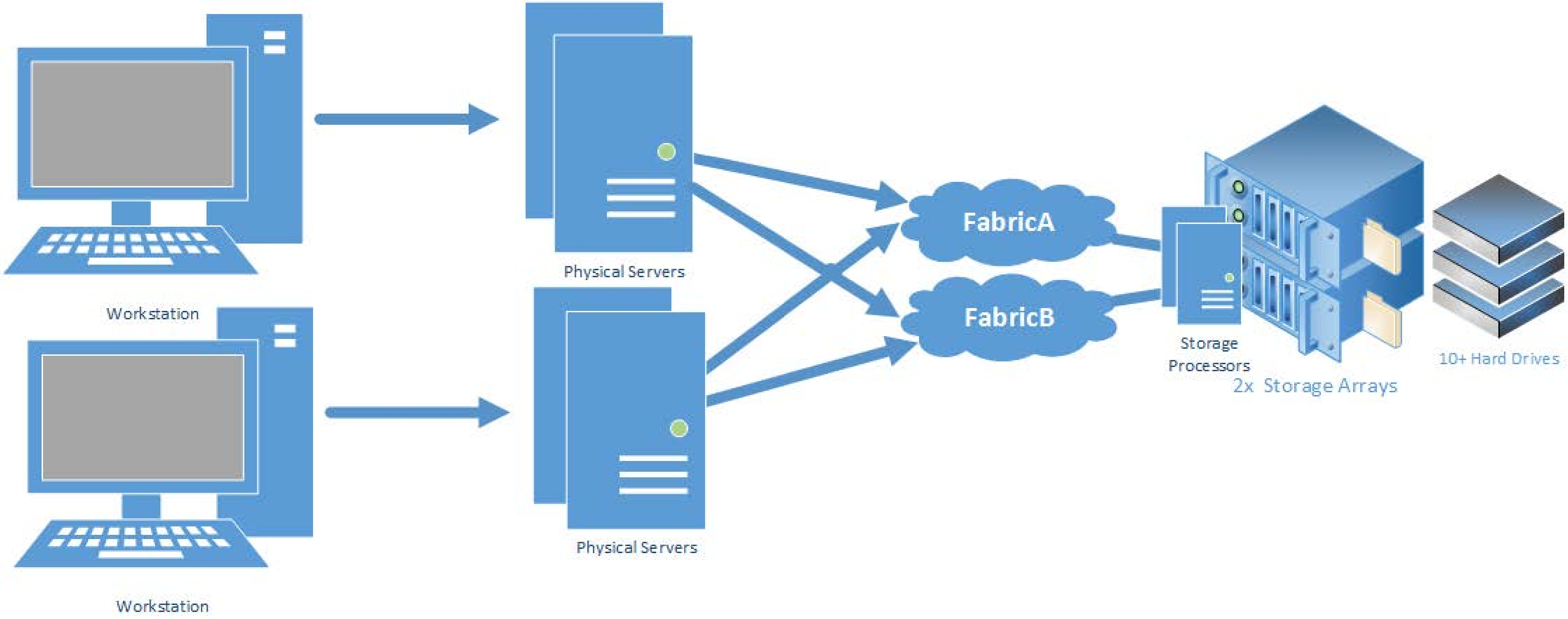
- Storage Area Network
  - The Storage Area Network is made up of HBA’s, Storage Networks, Storage Processors, and Disks
  - Storage Networks are a separate component from the Storage Array
  - Storage Arrays need a front end to talk to servers across the storage network(Commonly called Storage Processors)
  - Addresses the cabling limitations of direct attached storage
  - Provides Redundancy to all components
  - Complex Environment – Experts only
  - Limited Application Support



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

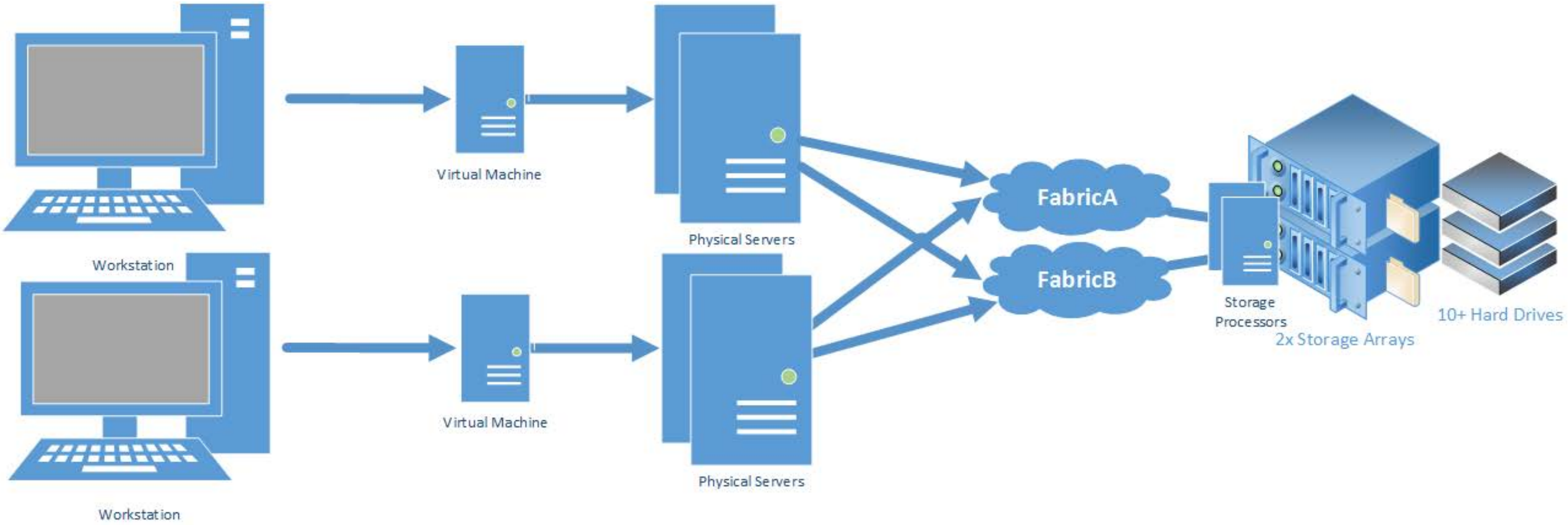
Evolution of Storage Solutions (6 of 8)

- Multi-Instance Storage Area Networks
  - Provides Redundancy to all components
  - Supports Multiple Tenants at a physical level
  - Complex Environment – Experts only
  - Limited Application Support



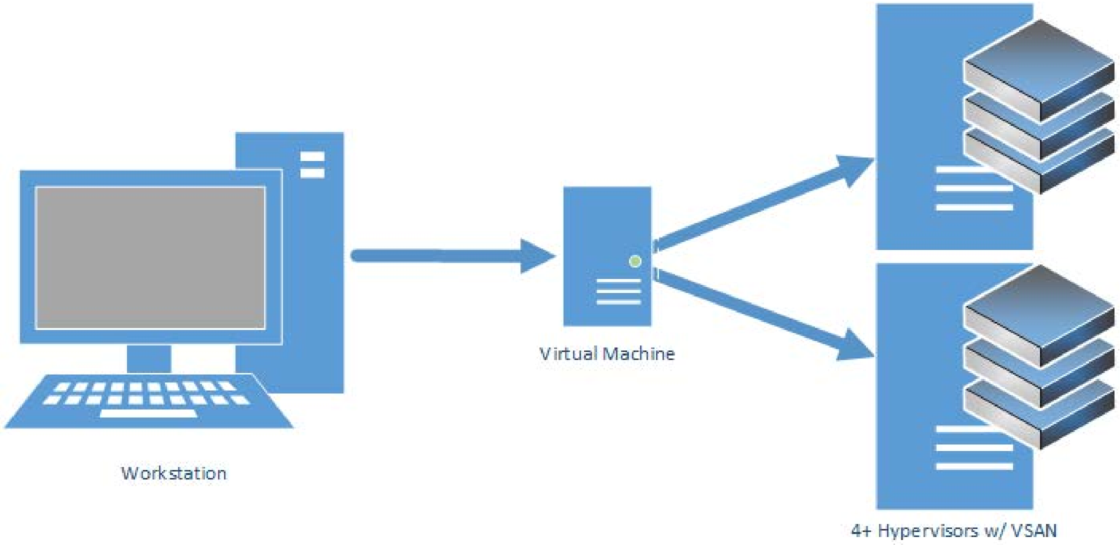
Evolution of Storage Solutions (7 of 8)

- Storage Area Network w/ Hypervisor
  - Current Technology
  - Complex Backend Environment
  - Applications are moved to virtual machines
  - Applications no longer need to understand the storage infrastructure to be redundant
  - Since the complex hardware environment is abstracted from the users it can be replaced without impacting users.



Evolution of Storage Solutions (8 of 8)

- Fully Virtualized SAN
  - New Technology <2 years old
  - Backend storage system is simplified dramatically
  - This type of Storage Area Network is entirely software controlled
  - Consistent and simplified hardware profile
  - Significantly reduced software footprint
  - Transition Issues : Some implementations emulate the old constructs that are very complex, Others use simplified models that are very easy to administer



Evolution of Storage Solutions

- Evolution Wrap-up
  - Each Iteration of Storage Technology tried to fix a major problem from the previous generation
  - Utilities are generally using multiple iterations of storage technology
  - Storage Networks were added later and are separate from the Storage Array
  - Hypervisors were built to abstract applications from backend systems
  - Datacenter Storage Systems are designed for Multi-Instance environments from the ground up. (Even before Hypervisors were implemented)

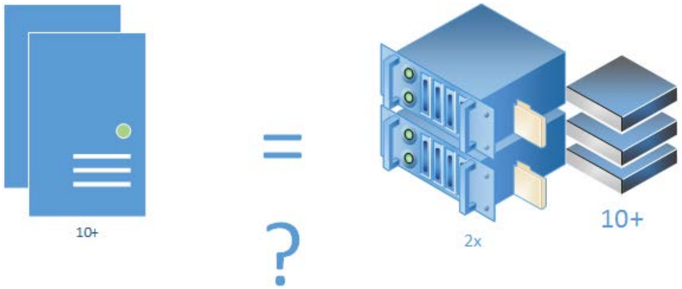
Webinar 3 - Storage Summary

Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection

Storage and Hypervisor Similarity

- Server and Storage Virtualization Similarities
  - They both service application workloads for user consumption
  - Both operate invisible to the users
  - Both typically have dedicated management planes and operate out of band from the production systems
  - Both are built from the ground up to service multi-instance environments
  - ESZ’s can be applied to logically separate both



ESZ Concept

- The SDT is considering the creation of a construct called an Electronic Security Zone to describe controls used to separate Tenants with logical isolation
  - This concept would be used to separate the management plane from the data plane
  - The concept can be used to create other ESZ's within an ESP (Such as to isolate outbound communication, or to split a storage array)
  - Devices that support multi-tenancy need to use the management ESZ to communicate with their Centralized Management System(CMS)
  - Not limited to networking concepts, can be used to model any type of logical control

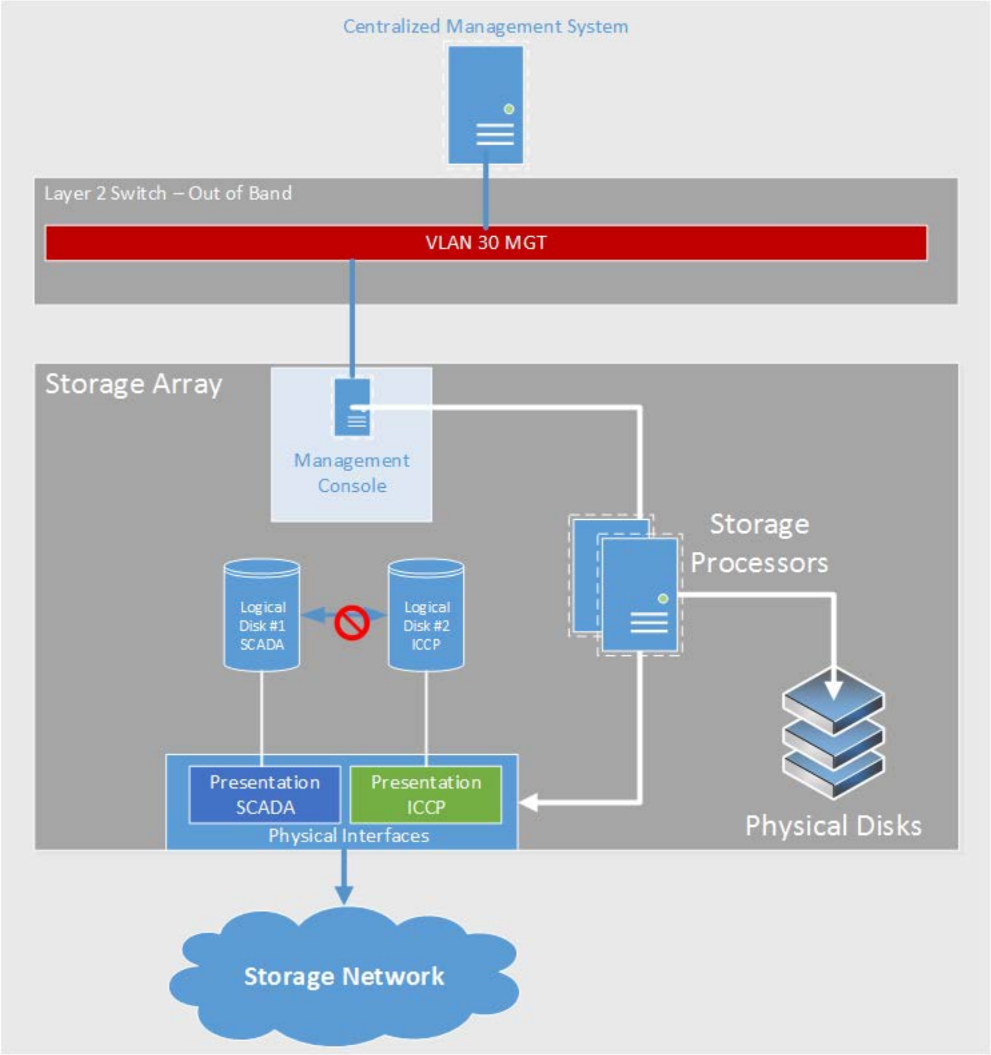
ESZ Storage Network Examples

- Electronic Security Zones applied to Storage Arrays
  - Storage Processors
  - Logically Isolated Management Plane

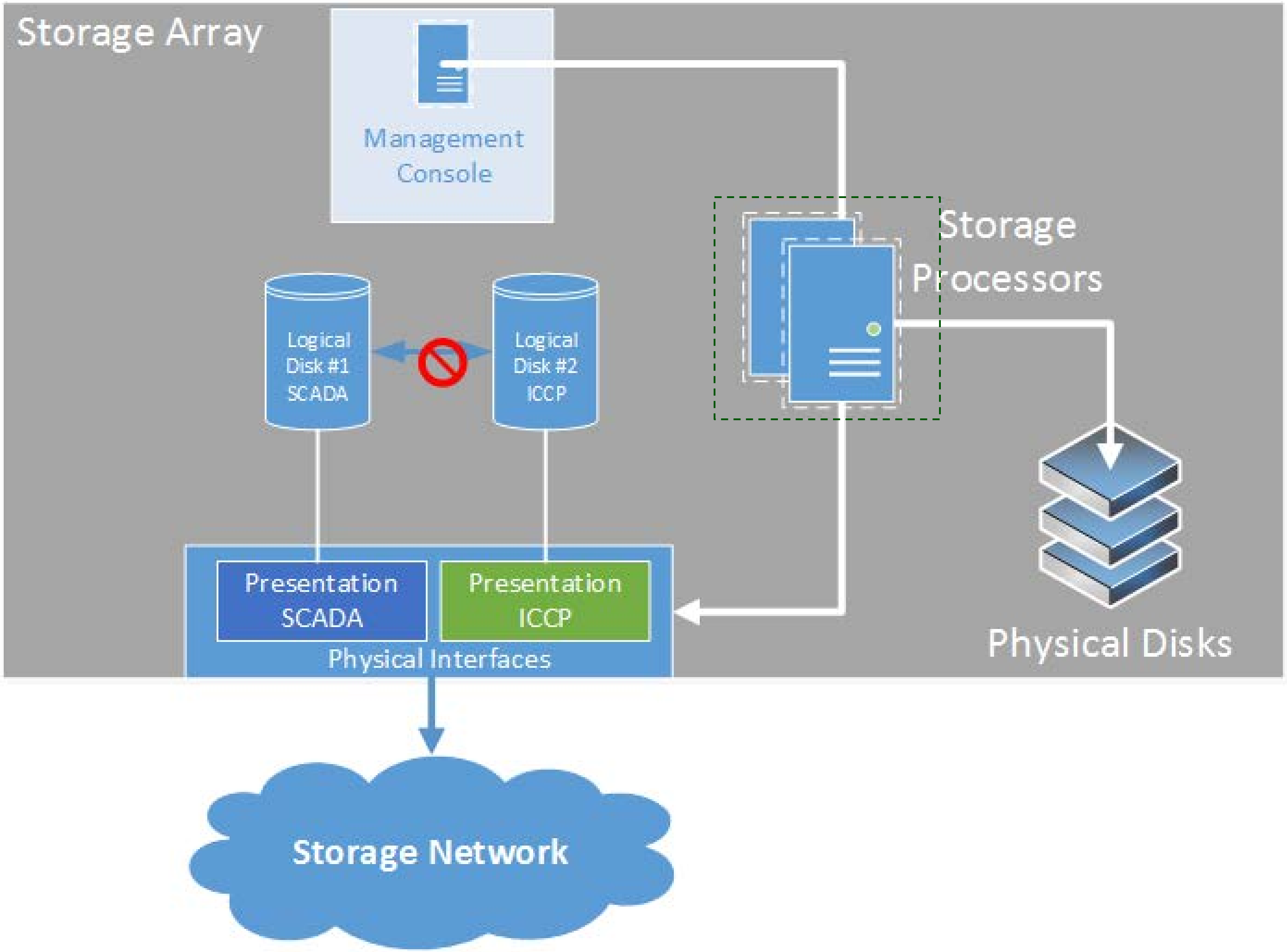
- Electronic Security Zones applied to current/future shared storage networking technologies
  - Fiber Channel
  - iSCSI
  - VSAN**(Future)**

ESZ : Storage Arrays

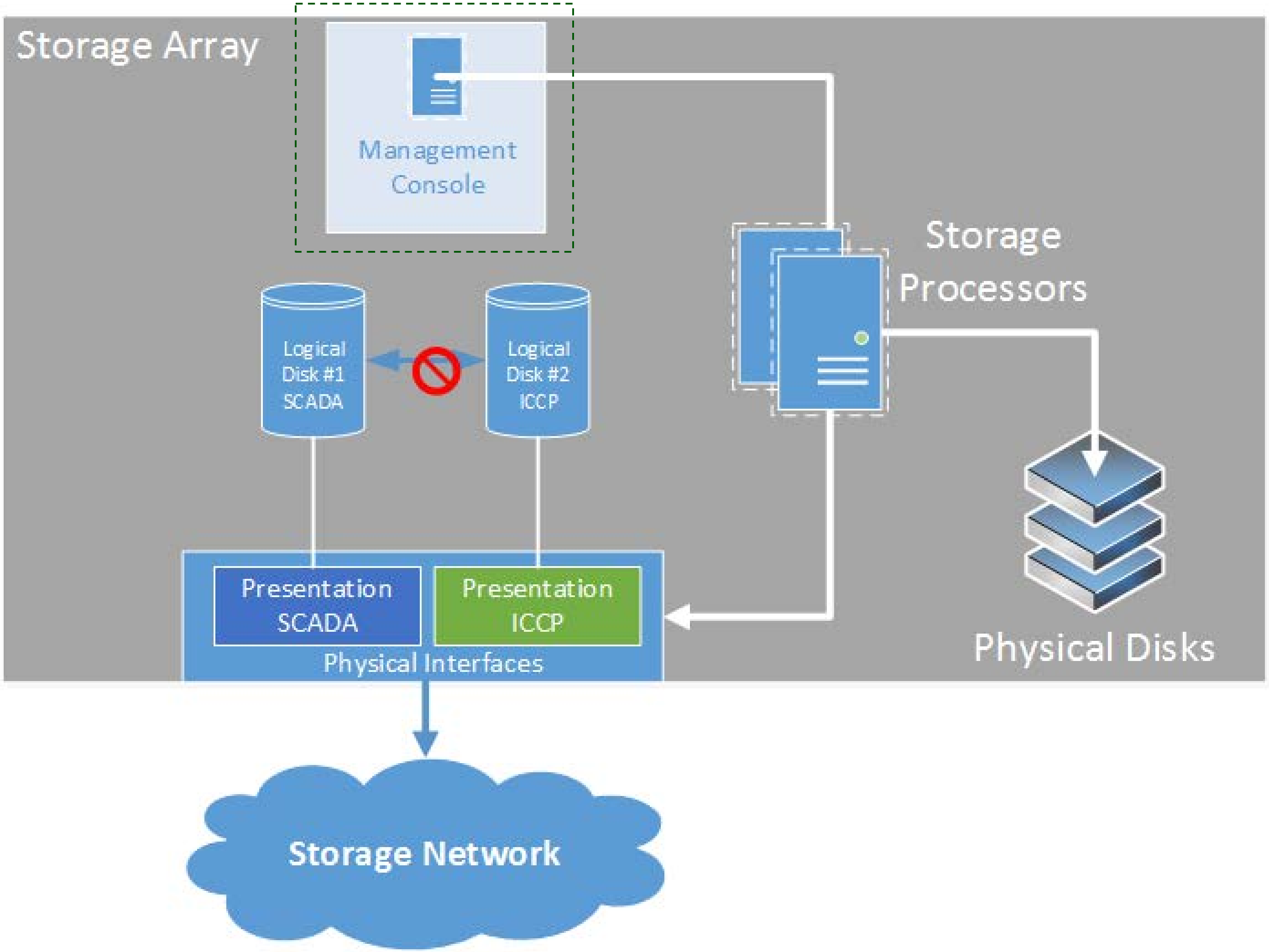
- Components
  - Management Console
  - Storage Processor
  - Physical Disks
  - Logical Disks
  - Logical Presentations
  - Physical Interfaces



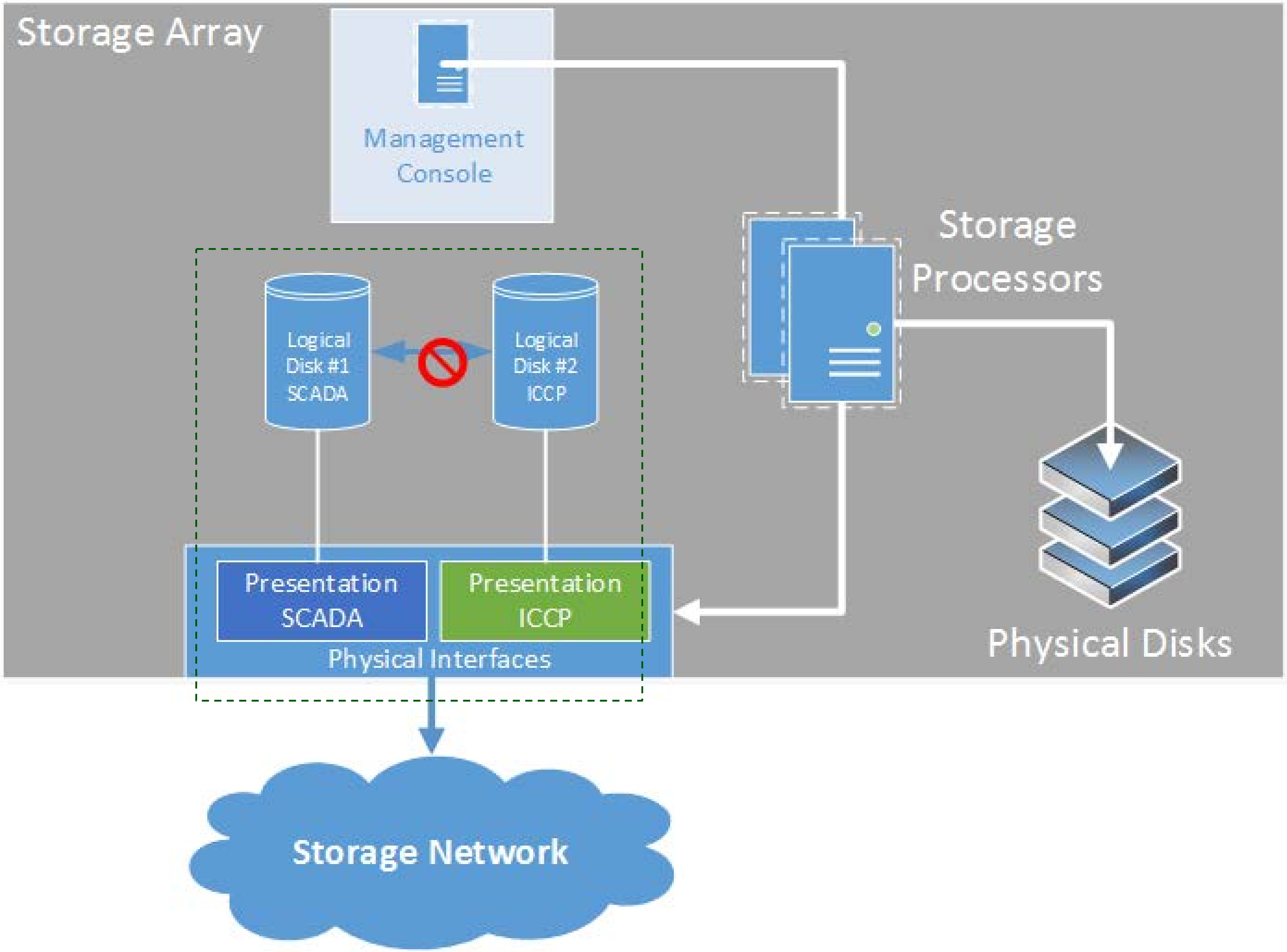
ESZ : Storage Arrays



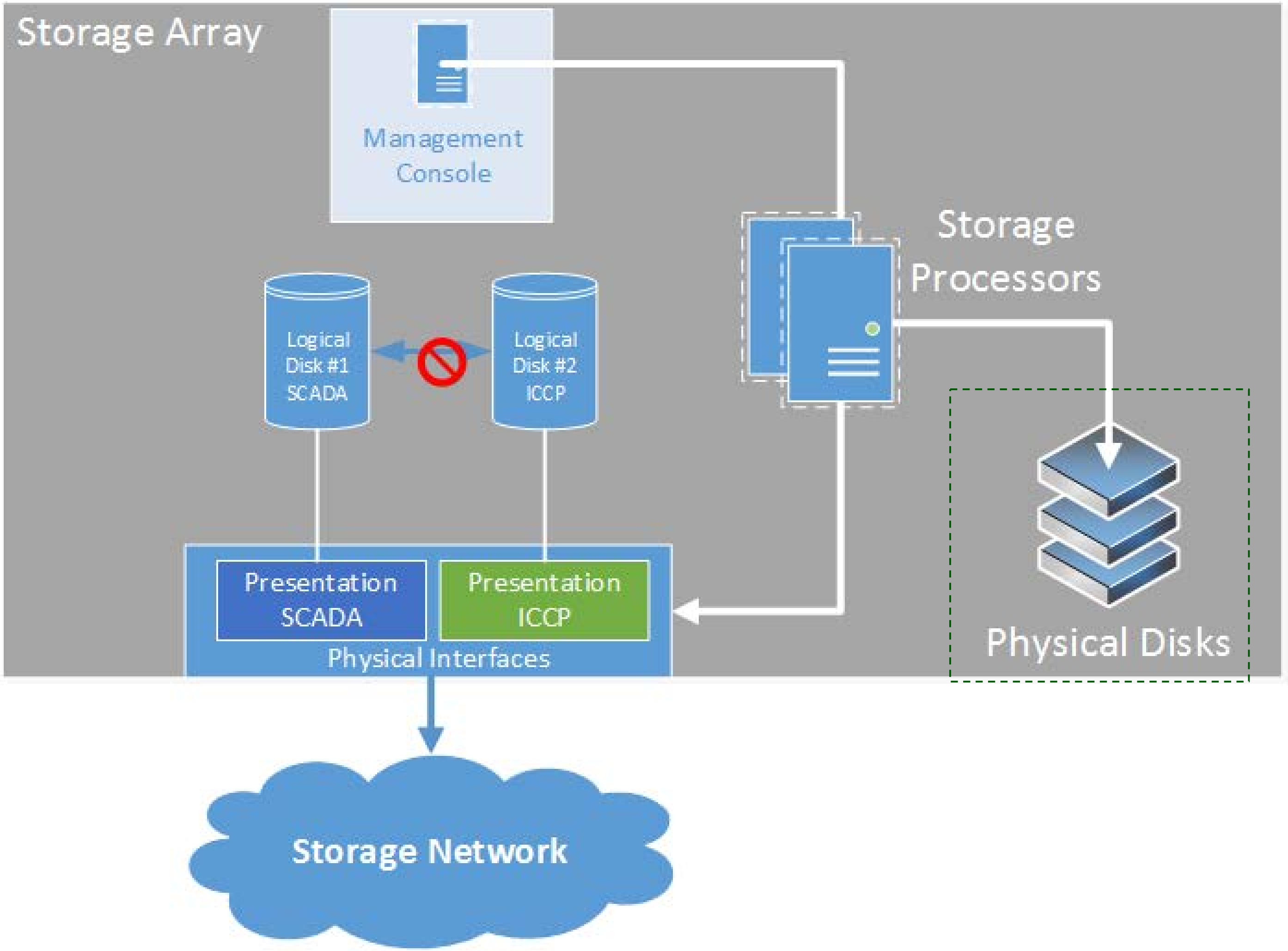
ESZ : Storage Arrays



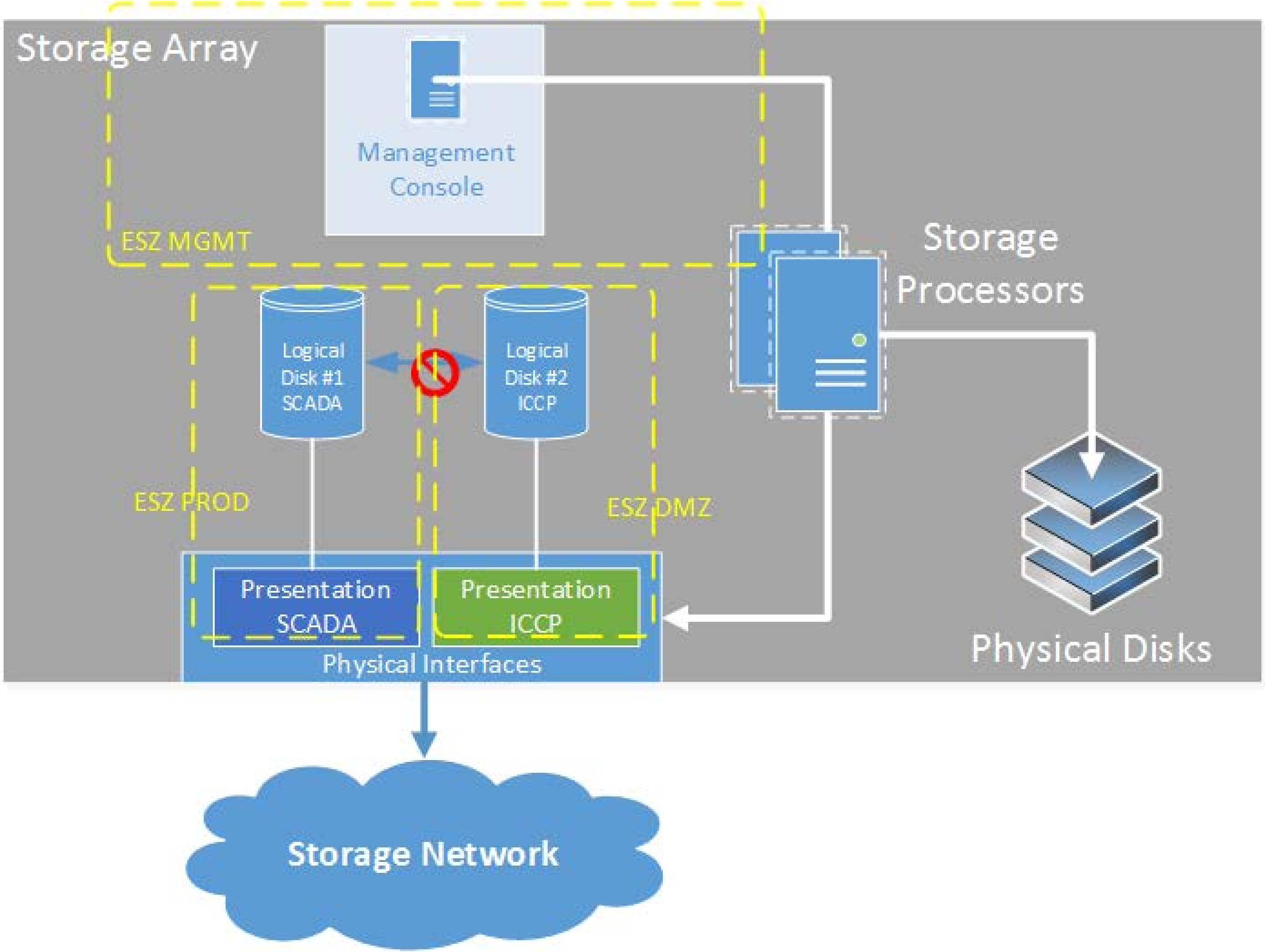
ESZ : Storage Arrays



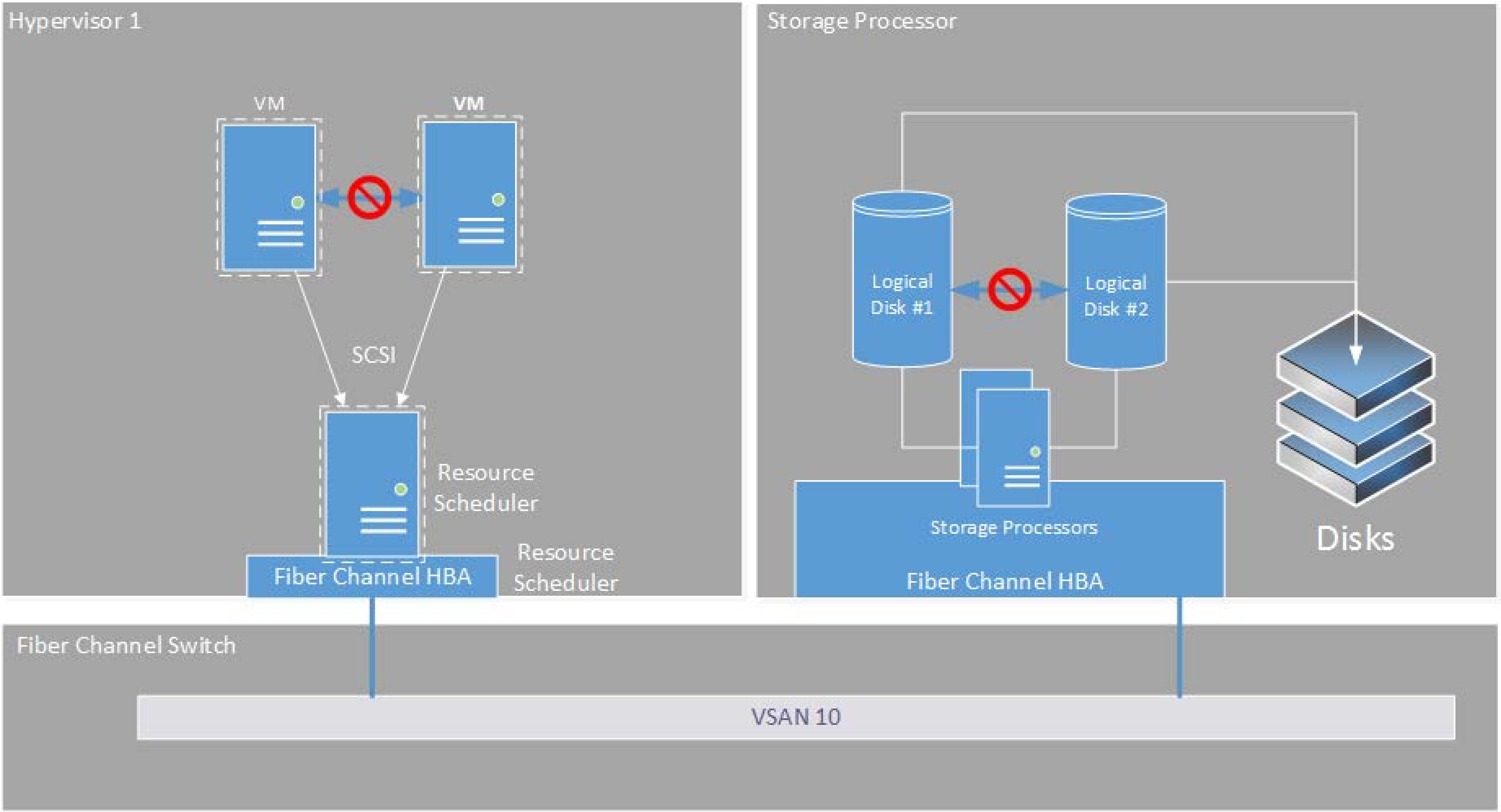
ESZ : Storage Arrays



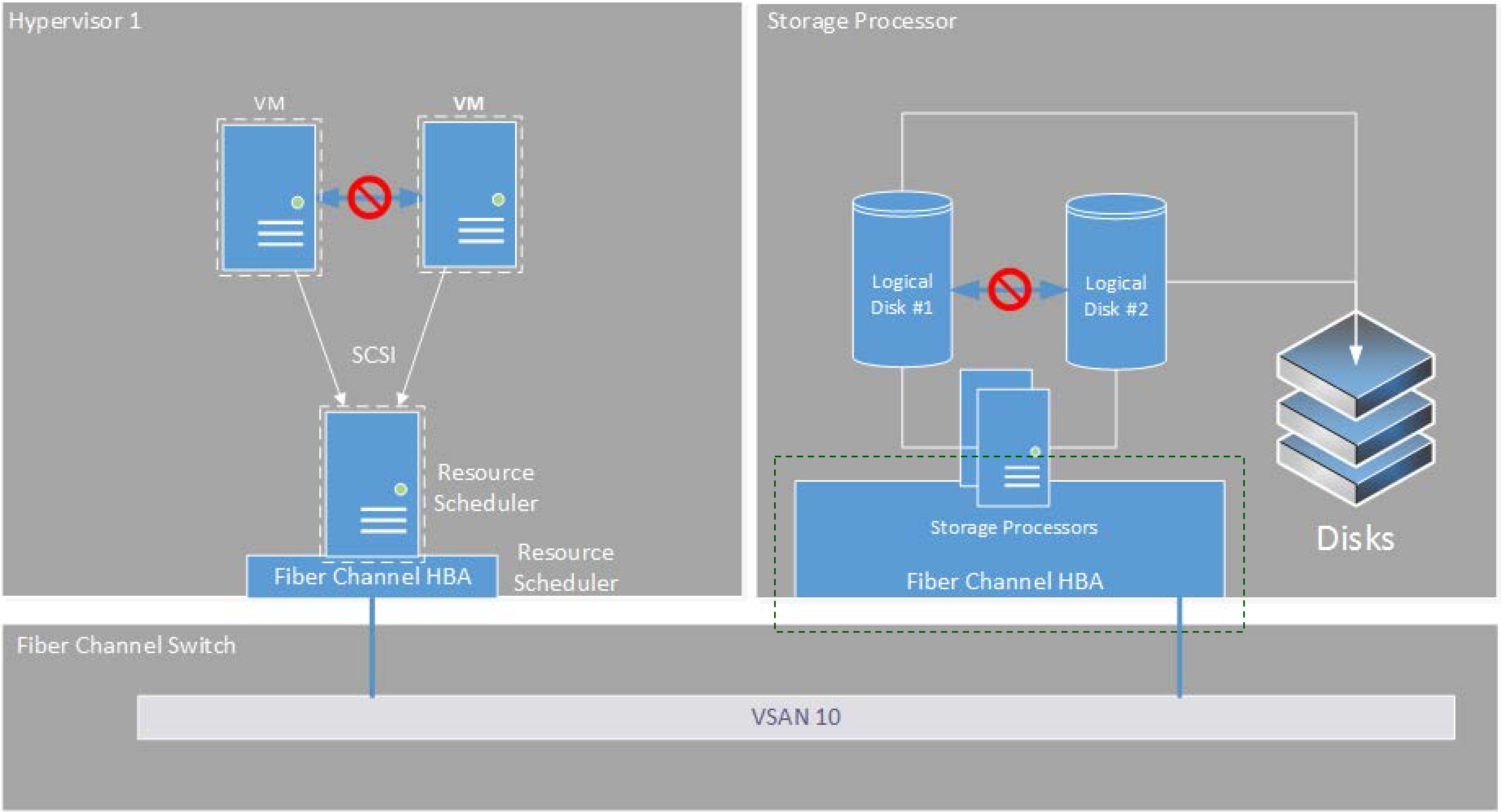
ESZ : Storage Arrays



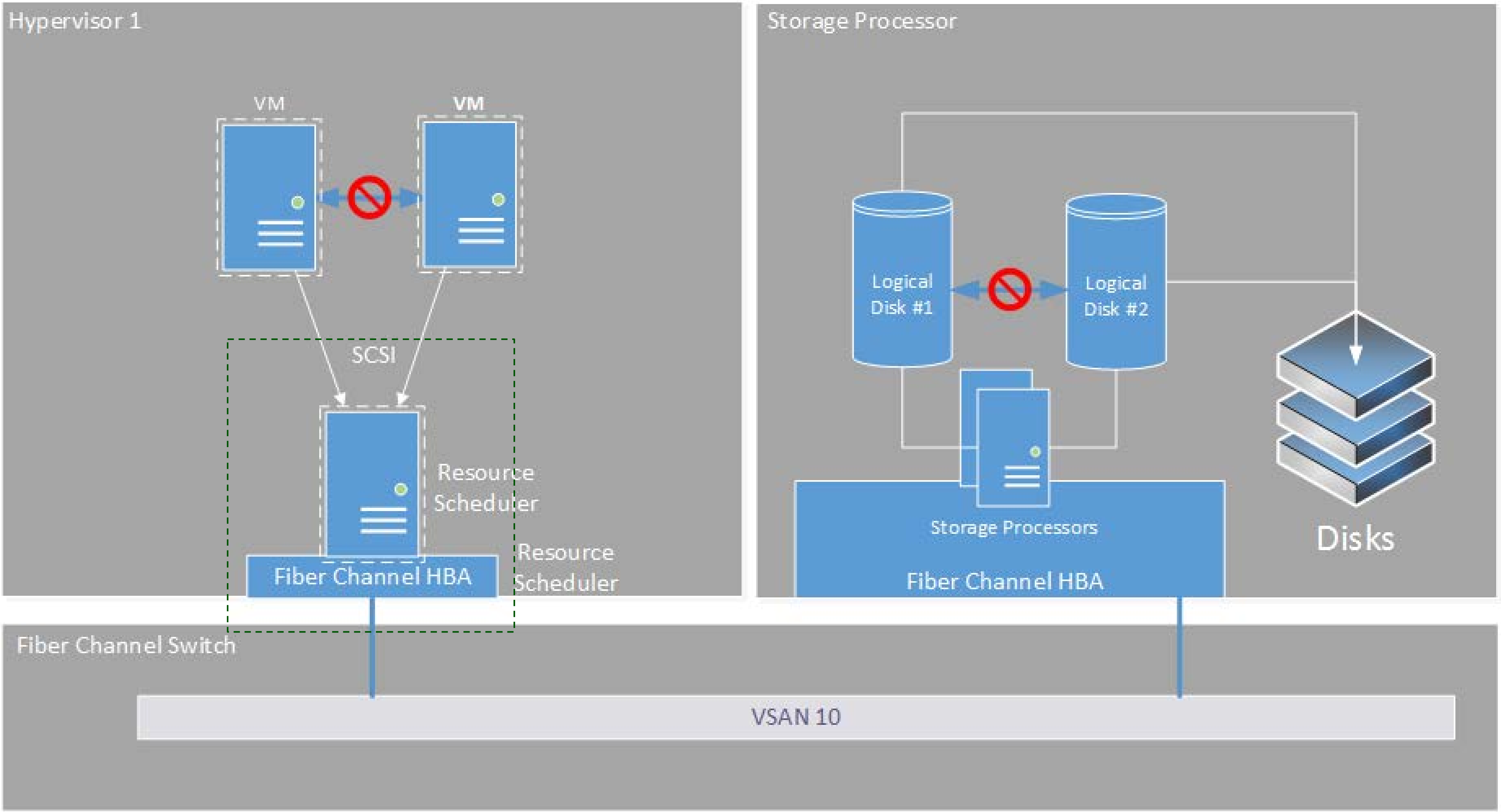
ESZ : Storage Arrays



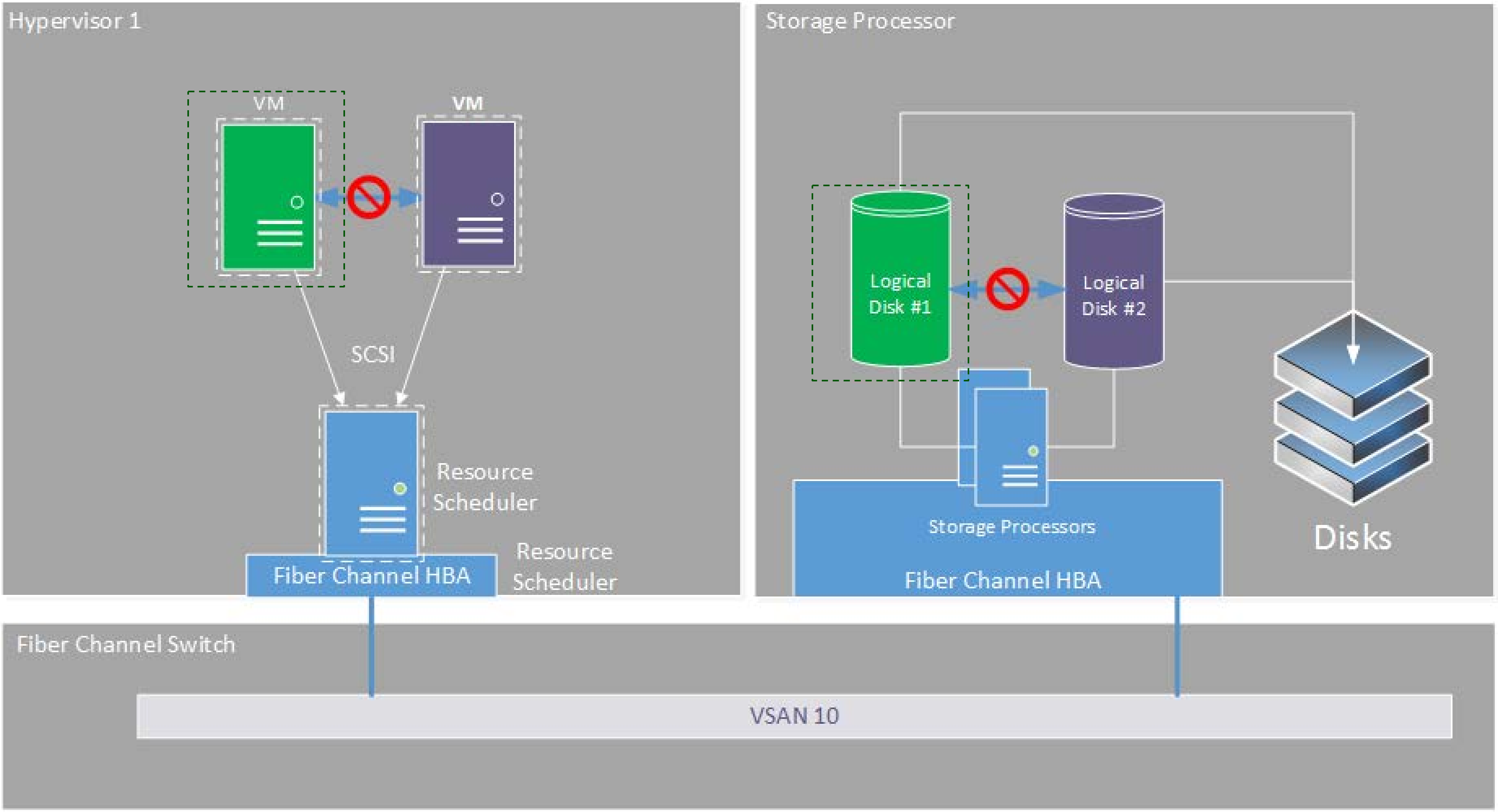
ESZ : Storage Arrays



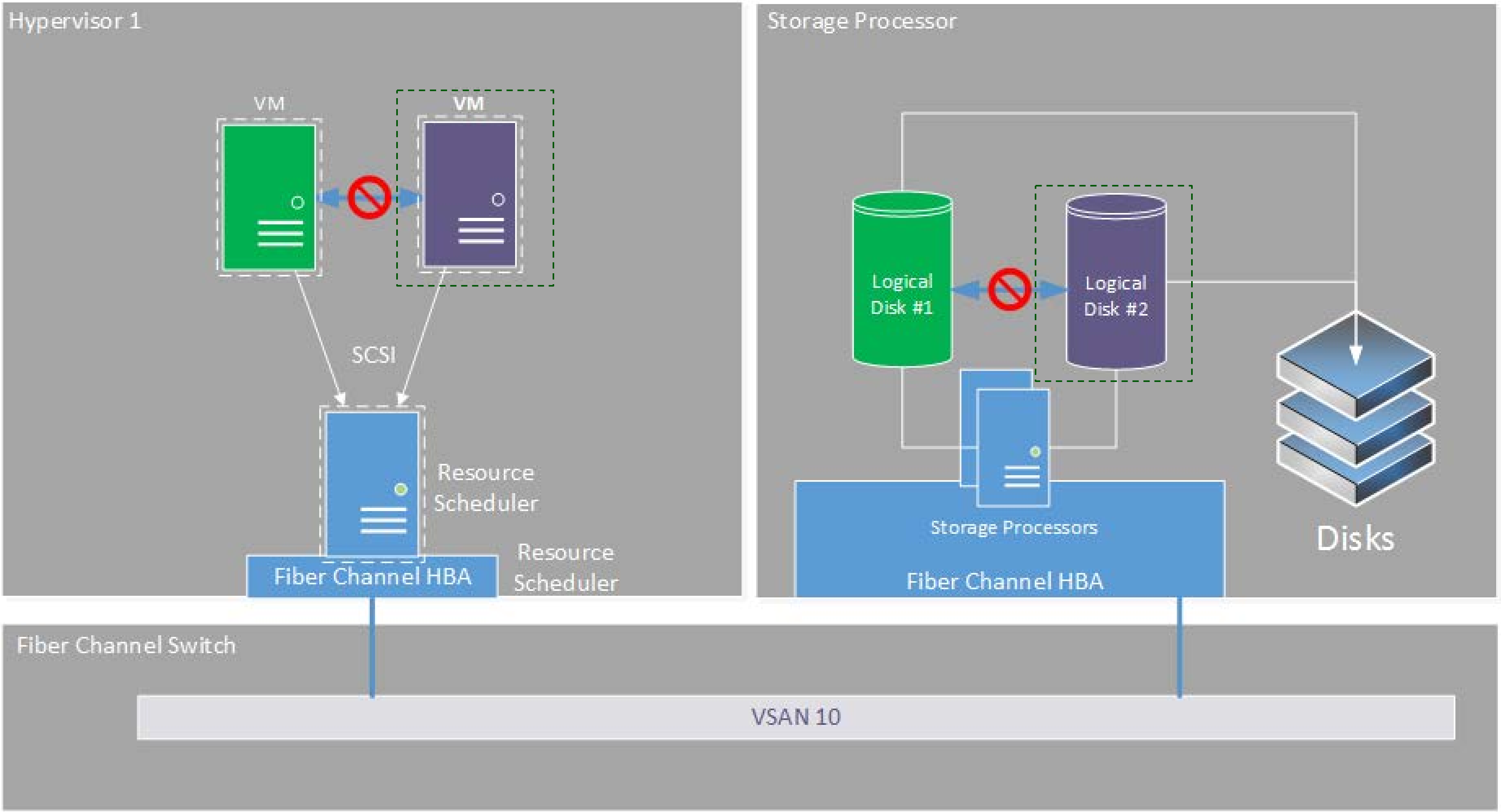
ESZ : Storage Arrays



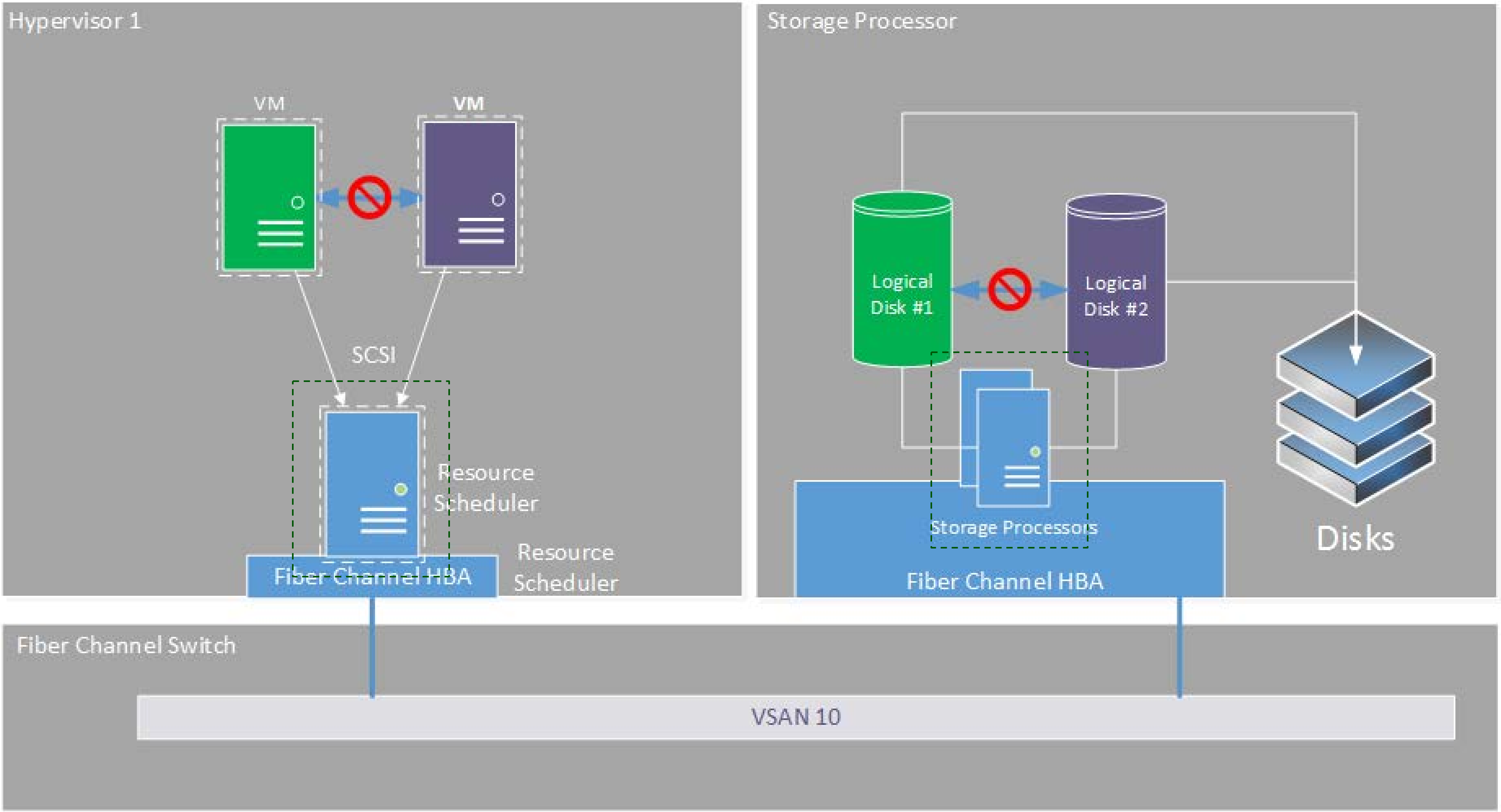
ESZ : Storage Arrays



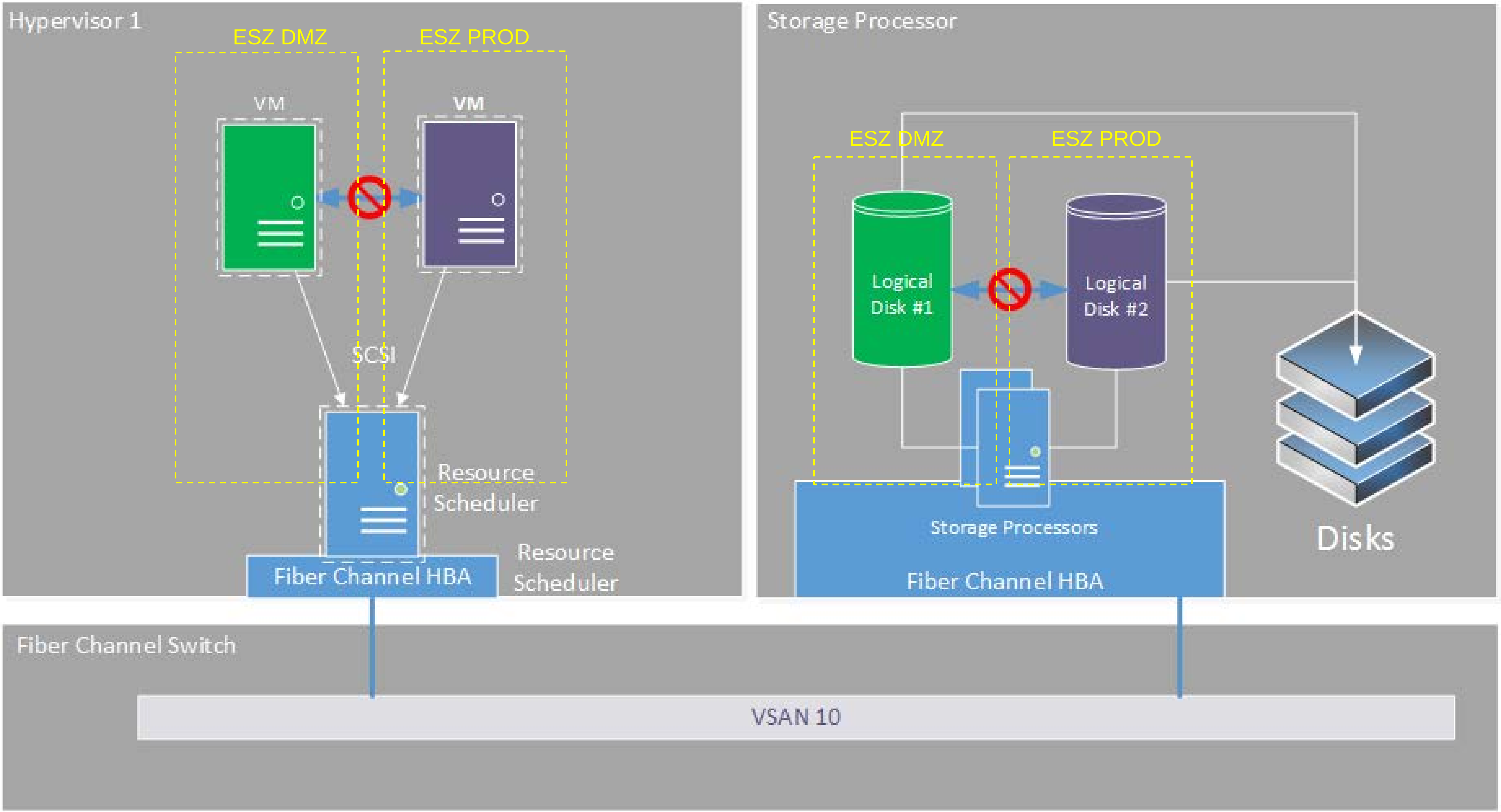
ESZ : Storage Arrays



ESZ : Storage Arrays

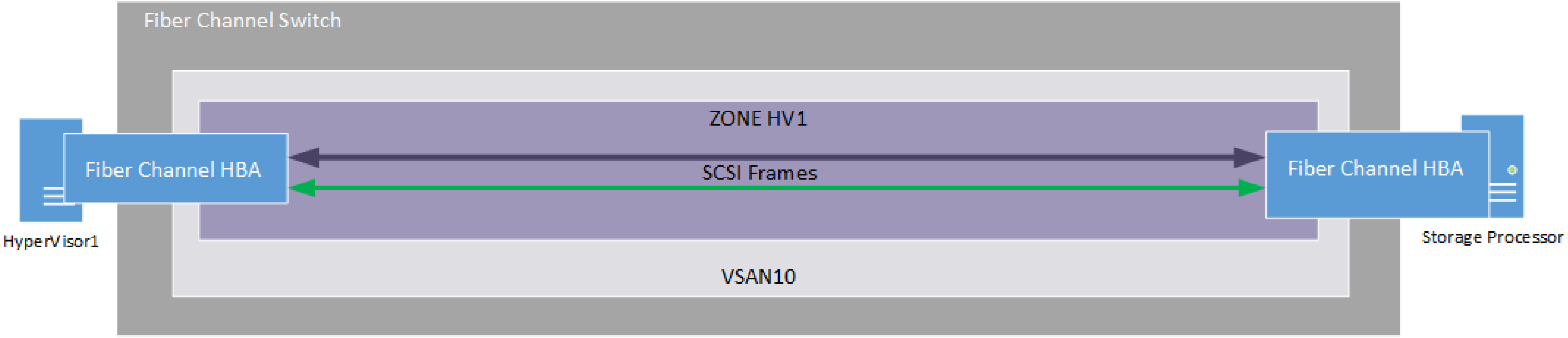


ESZ : Storage Arrays

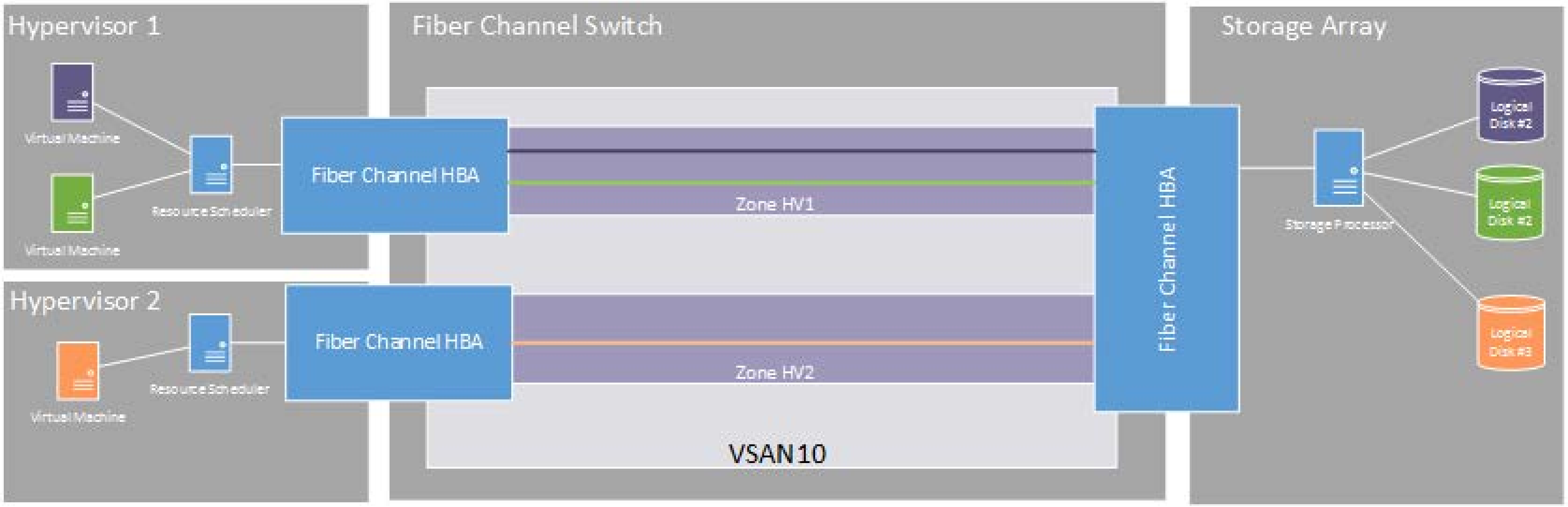


ESZ : Fiber Channel

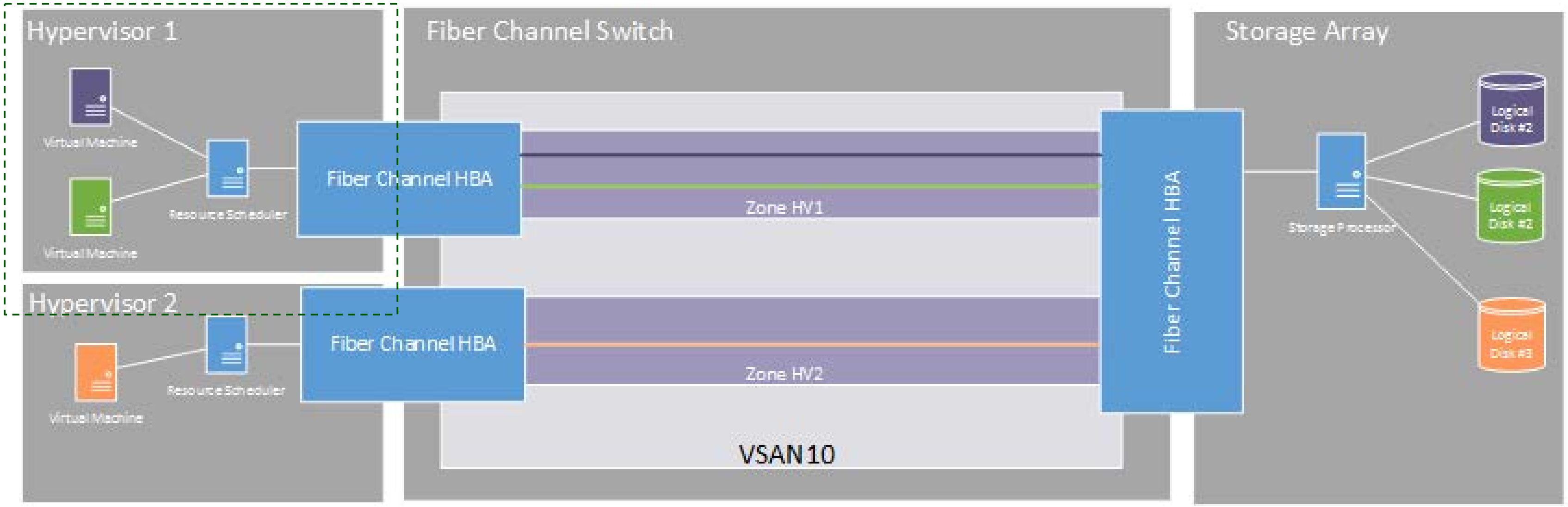
- Fiber Channel Frames are not Ethernet
- They are raw SCSI frames encapsulated in a fiber channel header
- VSAN's divide switches
- Zones control which HBA's can talk to each other



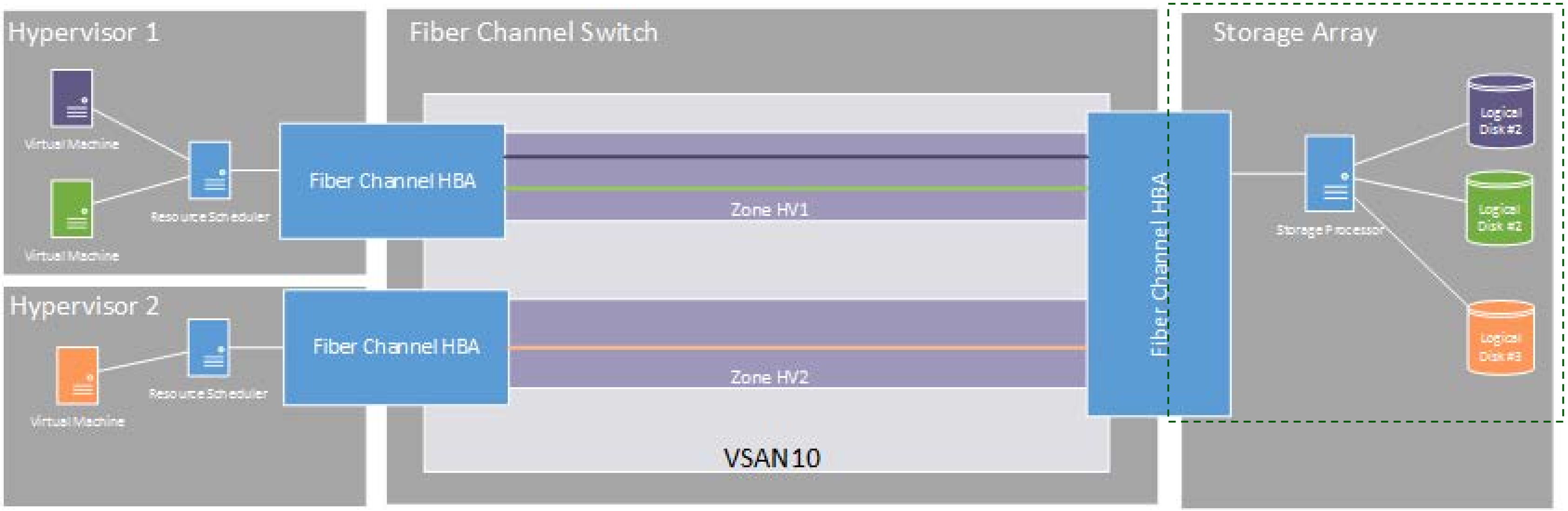
ESZ : Fiber Channel



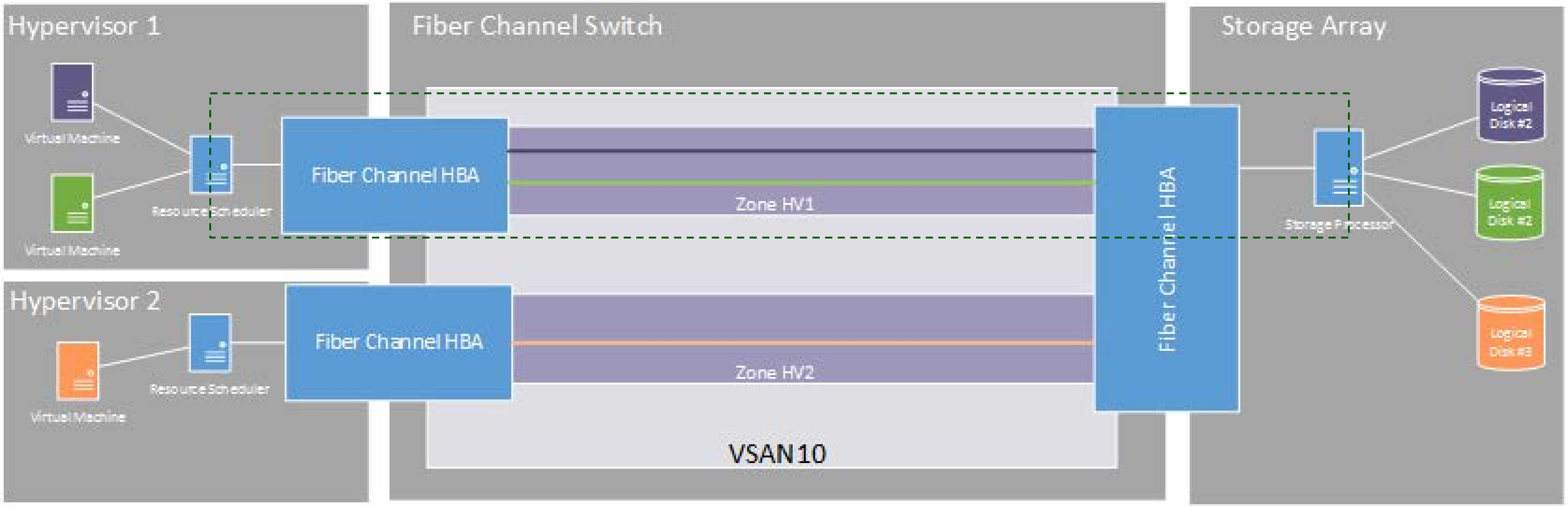
ESZ : Fiber Channel



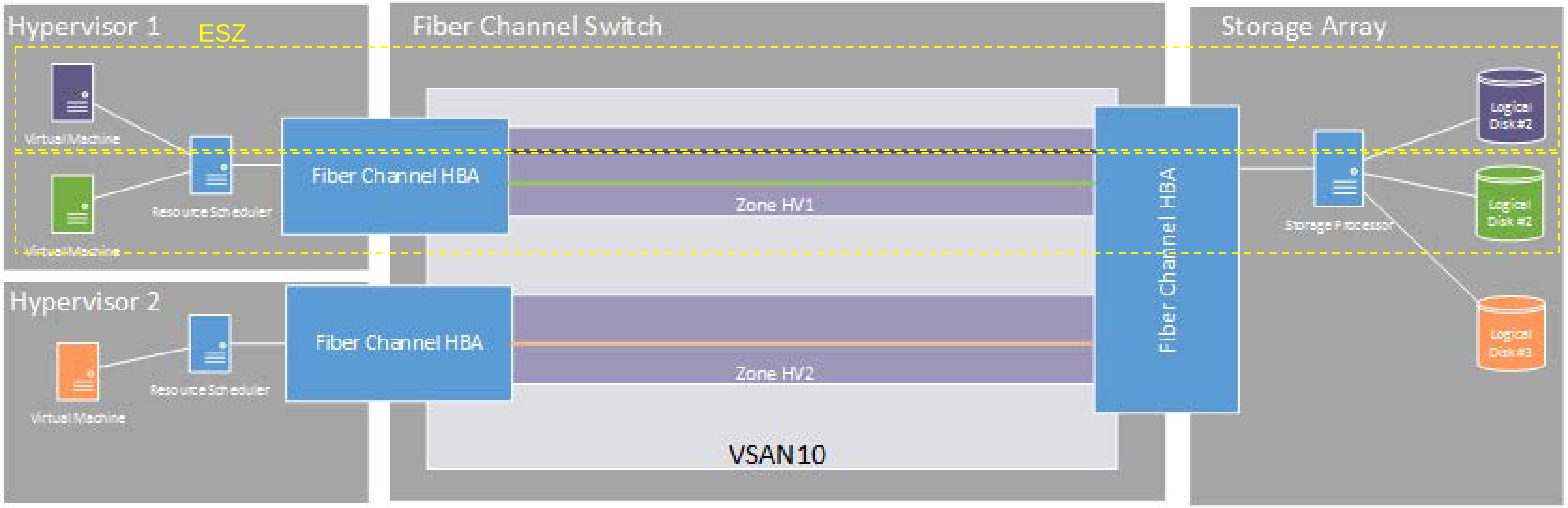
ESZ : Fiber Channel



ESZ : Fiber Channel

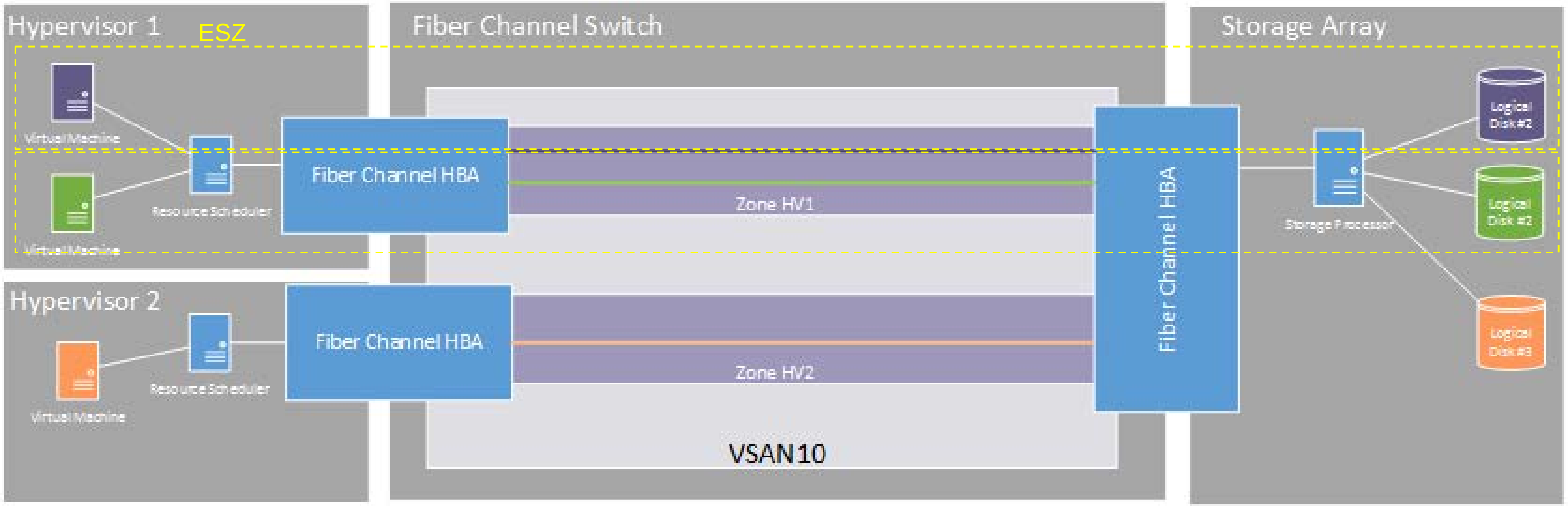


ESZ : Fiber Channel

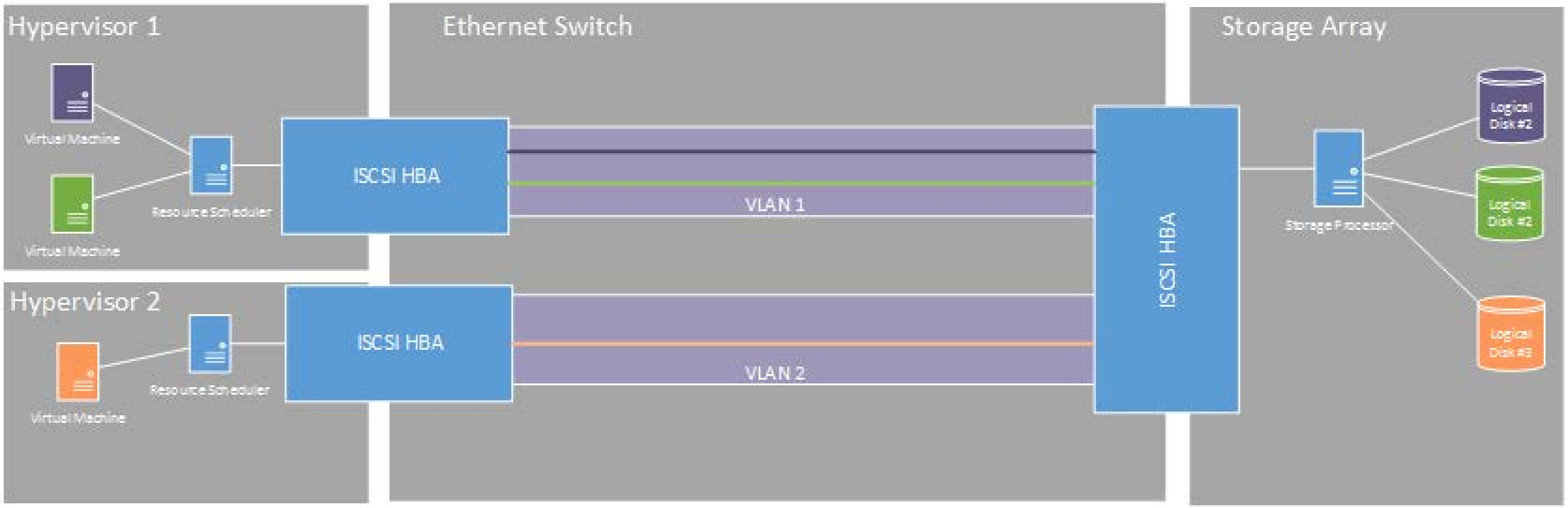


ESZ : Fiber Channel

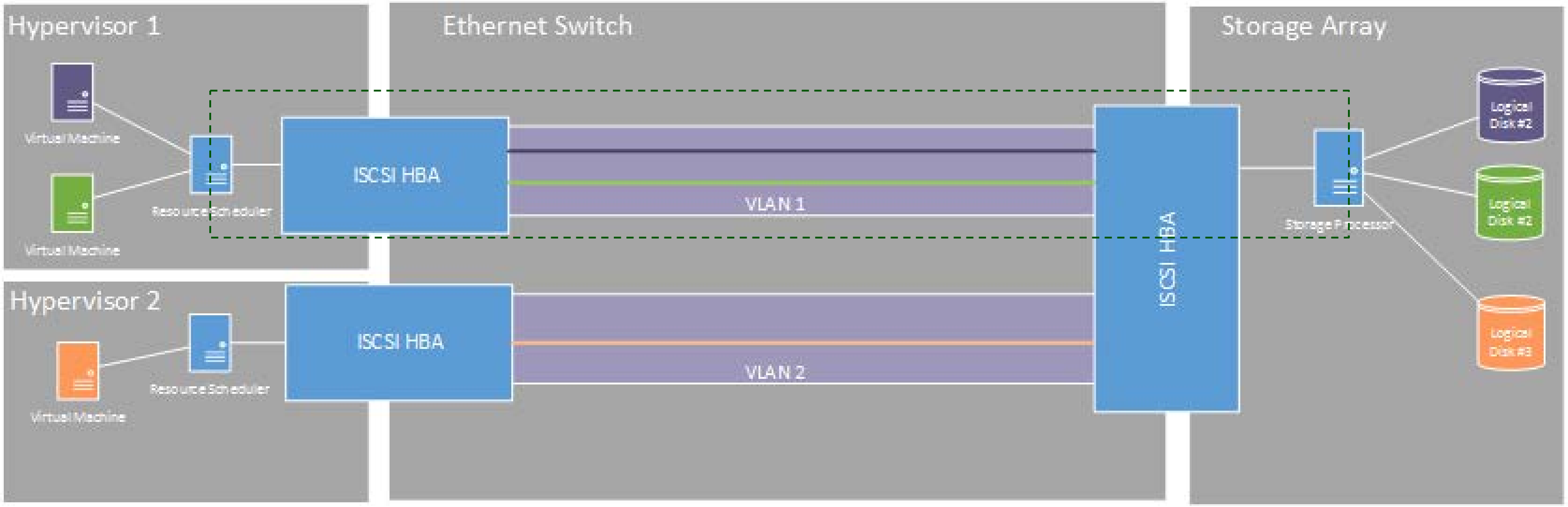
- ESZ Defined by Device Configurations
  - The configuration of the Storage Processor is providing isolation between devices in different ESZ's
  - The configuration of the hypervisor is providing isolation between devices in different ESZ's
  - The configuration of the Fiber Channel switch is ensuring that the correct devices are providing access control to logically isolate the ESZ's



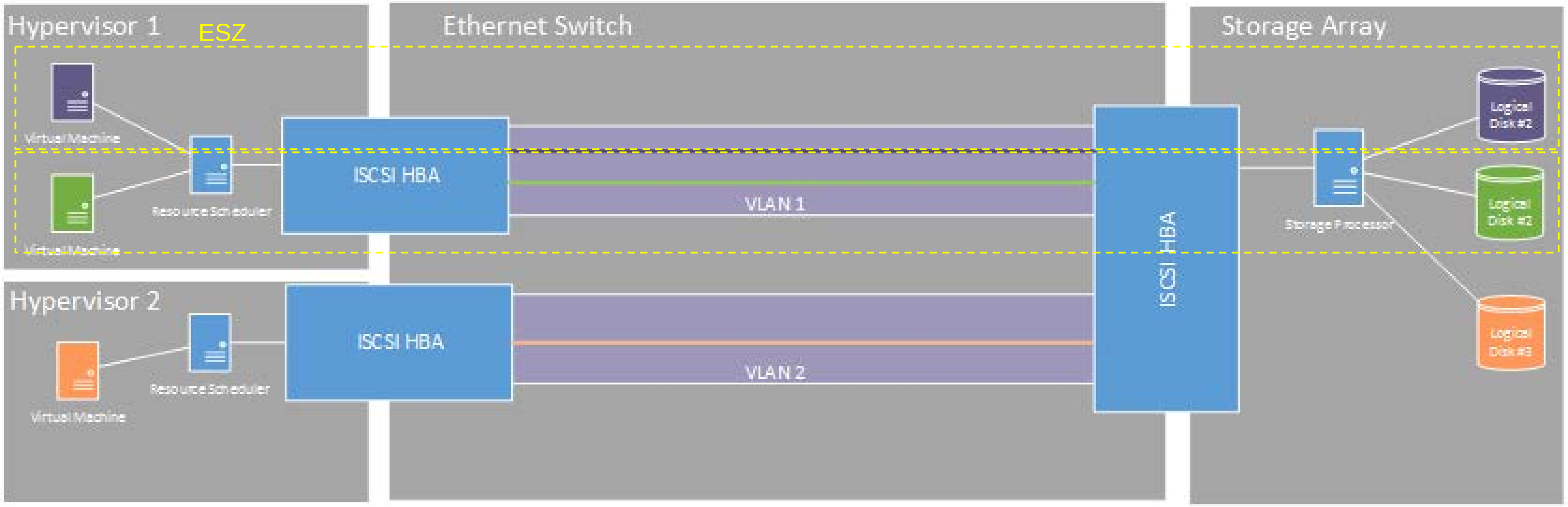
ESZ : iSCSI


Hypervisor 1
Virtual Machine
Virtual Machine
Resource Scheduler
ISCSI HBA
Hypervisor 2
Resource Scheduler
Virtual Machine
ISCSI HBA
Ethernet Switch
VLAN 1
VLAN 2
ISCSI HBA
Storage Array
Storage Processor
Logical Disk #2
Logical Disk #2
Logical Disk #3

ESZ : iSCSI

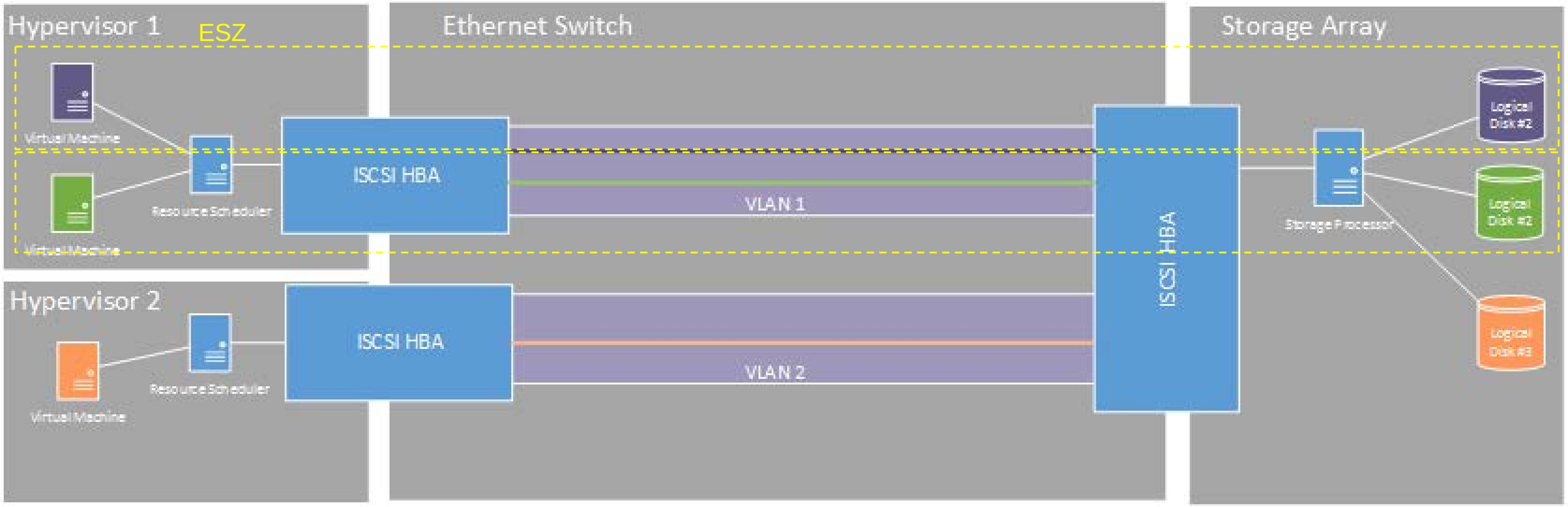

Hypervisor 1
Virtual Machine
Virtual Machine
Resource Scheduler
ISCSI HBA
Ethernet Switch
VLAN 1
Hypervisor 2
Virtual Machine
Resource Scheduler
ISCSI HBA
VLAN 2
ISCSI HBA
Storage Array
Storage Processor
Logical Disk #2
Logical Disk #2
Logical Disk #3

ESZ : iSCSI

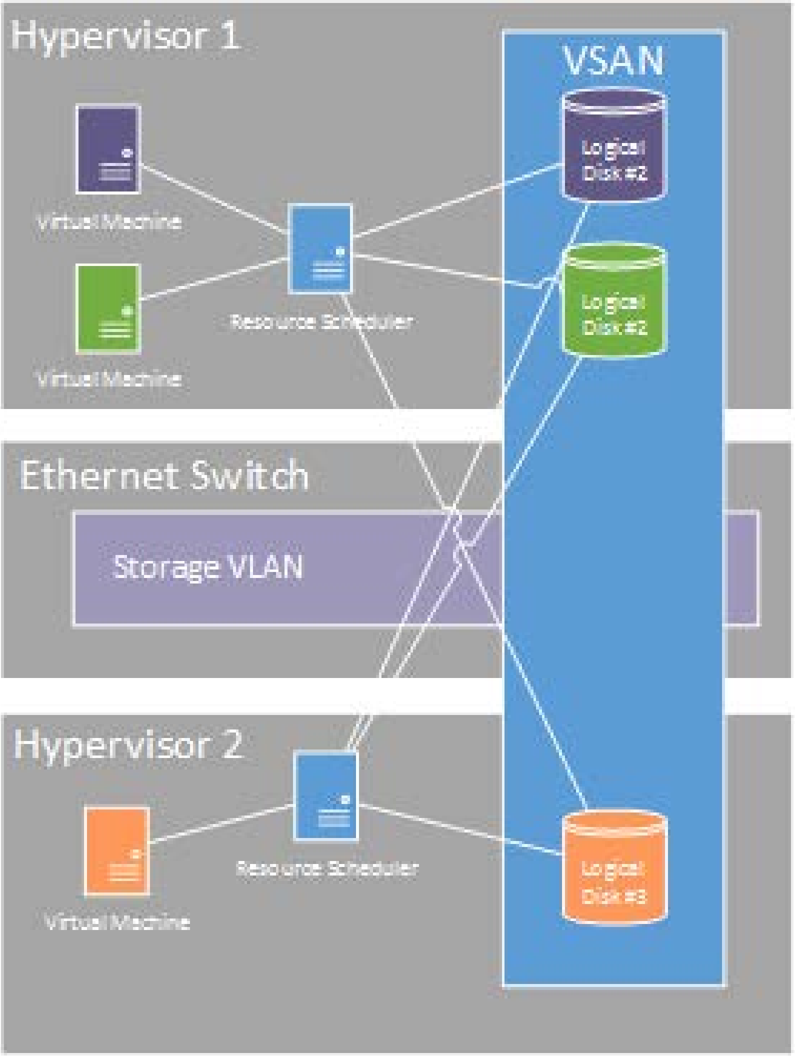

Hypervisor 1
ESZ
Ethernet Switch
Storage Array
Virtual Machine
Resource Scheduler
Virtual Machine
ISCSI HBA
VLAN 1
ISCSI HBA
Storage Processor
Logical Disk #2
Logical Disk #2
Logical Disk #3
Hypervisor 2
Resource Scheduler
Virtual Machine
ISCSI HBA
VLAN 2

ESZ : iSCSI

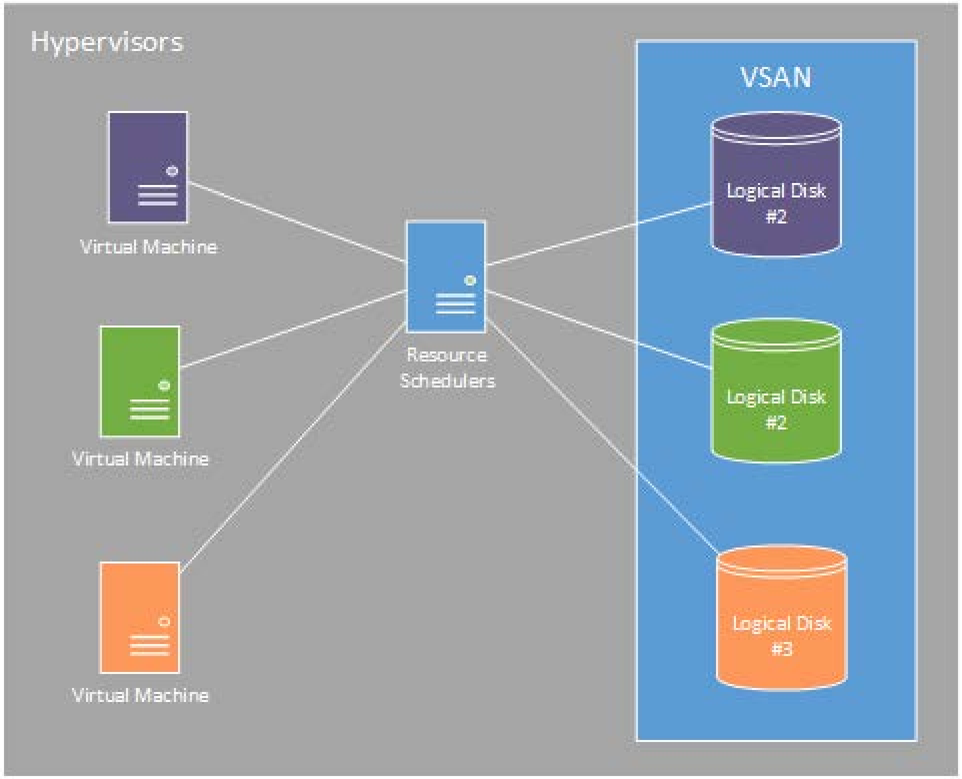
- ESZ Defined by Device Configurations
  - The configuration of the Storage Processor is providing isolation between devices in different ESZ’s
  - The configuration of the hypervisor is providing isolation between devices in different ESZ’s
  - The configuration of the Ethernet switch is ensuring that the correct devices are providing access control to logically isolate the ESZ’s



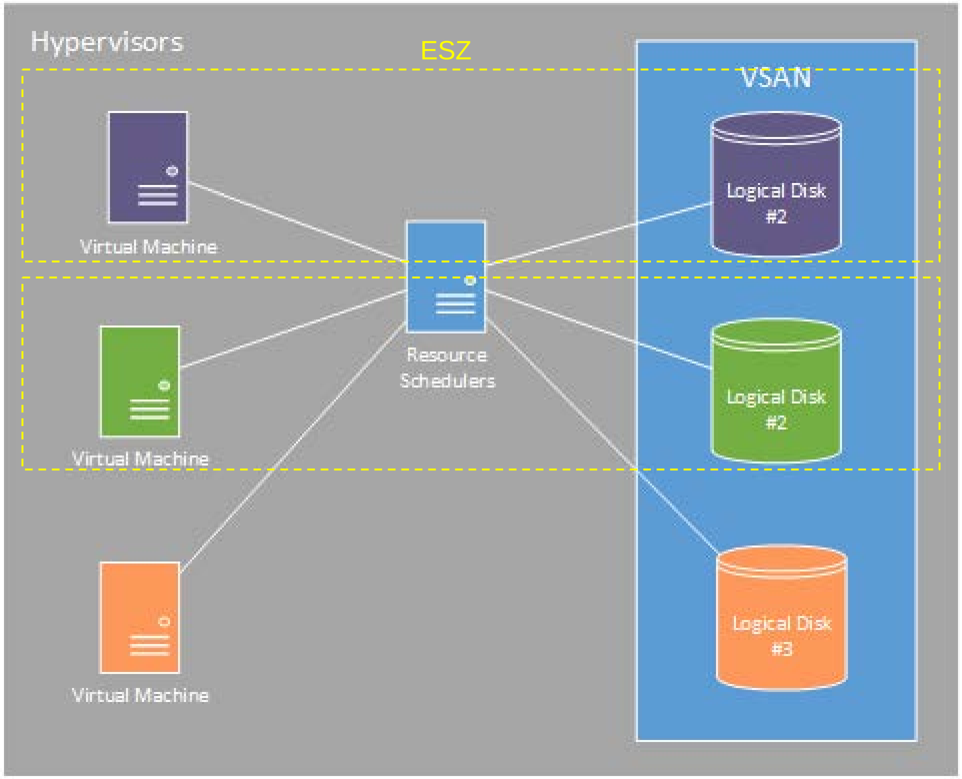
ESZ: Fully Virtualized Storage Array



ESZ: Fully Virtualized Storage Array



ESZ: Fully Virtualized Storage Array



Applying ESZs to Different Storage Systems

- Applying ESZ’s Wrap-up
  - Electronic Security Zones applied to current/future shared storage networking technologies
    - Storage Processors
    - Fiber Channel
    - iSCSI
    - NFS
    - VSAN**(Future)**
  - The configuration of the devices in the multi-instance environment are responsible for ensuring that ESZ’s remain logically isolated.

Webinar 3 - Storage Summary

Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection

Scaling Storage Networks

- Scaling Storage Networks
  - The SDT has asserted in the past few webinars that vendors provide security and resiliency features based on the scale of the environment.
  - Smaller scale environments do not offer as many enterprise grade solutions for security and resiliency
  - Examples from 4 Common Storage Vendors*
    - Sizing based on ~40Tb for CIP Environments and >500TB for non-CIP environments
    - Disclaimer: Information was mined from the vendors publicly available information and was not provided by vendors
    - References will be posted at the end of this section

Scaling Storage Networks

- Comparison #1 : Vendor HP

  - HP StoreEasy 1550
    - Entry-Level
    - Capacity: 80Tb
    - Encryption: N/A
    - DR: N/A

  - HP 3PAR StoreServ 8000
    - Mid-Enterprise Level
    - Capacity: 4000Tb
    - Encryption: Hardware
    - DR: Site-to-Site
    - FIPS/FDE Certified Disks

Scaling Storage Networks

- Comparison #2 : Vendor Dell/EMC

  - Dell Storage PS4210E
    - Entry-Level
    - Capacity: 72Tb
    - Encryption: N/A
    - DR: N/A

  - EMC Unity 500F
    - Mid-Enterprise Level
    - Capacity: 7800Tb
    - Encryption: Hardware
    - DR: Site-to-Site
    - FIPS/FDE Certified Disks

Scaling Storage Networks

- Comparison #3 : Vendor NetApp

  - NetApp SolidFire SF38410
    - Entry-Level
    - Capacity: 84Tb
    - Encryption: Software
    - DR: Site-to-Site

  - NetApp AFF A700
    - Mid-Enterprise Level
    - Capacity: 1800Tb
    - Encryption: Hardware
    - DR: Site-to-Site
    - FIPS/FDE Certified Disks

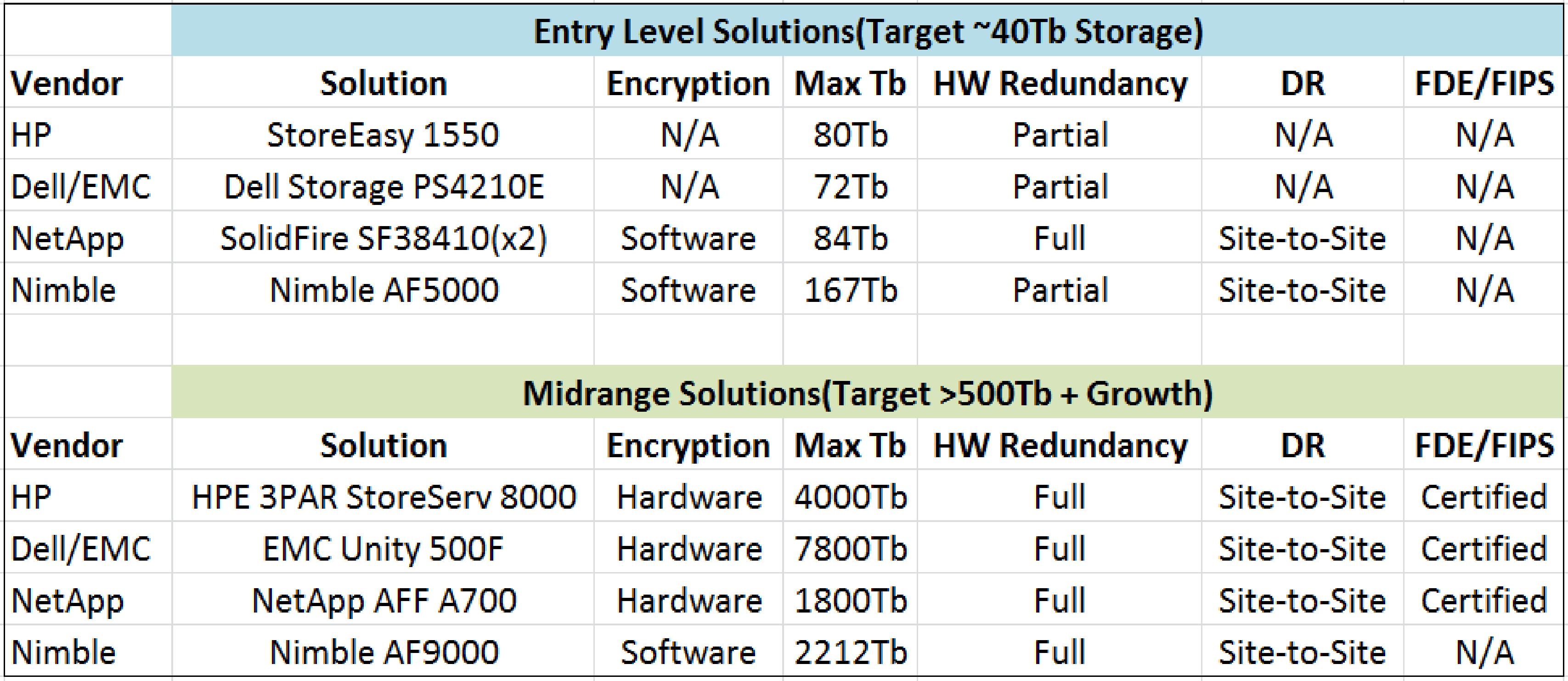
Scaling Storage Networks

- Comparison #4: Vendor Nimble Storage

  - Nimble AF5000
    - Entry-Level
    - Capacity: 167Tb
    - Encryption: Software
    - DR: Site-to-Site

  - Nimble AF9000
    - Mid-Enterprise Level
    - Capacity: 2212Tb
    - Encryption: Software
    - DR: Site-to-Site

Scaling Storage Networks



	Entry Level Solutions(Target ~40Tb Storage)					
Vendor	**Solution**	**Encryption**	**Max Tb**	**HW Redundancy**	**DR**	**FDE/FIPS**
HP	StoreEasy 1550	N/A	80Tb	Partial	N/A	N/A
Dell/EMC	Dell Storage PS4210E	N/A	72Tb	Partial	N/A	N/A
NetApp	SolidFire SF38410(x2)	Software	84Tb	Full	Site-to-Site	N/A
Nimble	Nimble AF5000	Software	167Tb	Partial	Site-to-Site	N/A
	Midrange Solutions(Target >500Tb + Growth)					
Vendor	**Solution**	**Encryption**	**Max Tb**	**HW Redundancy**	**DR**	**FDE/FIPS**
HP	HPE 3PAR StoreServ 8000	Hardware	4000Tb	Full	Site-to-Site	Certified
Dell/EMC	EMC Unity 500F	Hardware	7800Tb	Full	Site-to-Site	Certified
NetApp	NetApp AFF A700	Hardware	1800Tb	Full	Site-to-Site	Certified
Nimble	Nimble AF9000	Software	2212Tb	Full	Site-to-Site	N/A

Scaling Storage Networks

- Scaling Storage Networks Wrap-Up
  - The SDT has asserted in the past few webinars that vendors provide security and resiliency based on the scale of the environment
  - Smaller scale environments do not offer as many enterprise grade solutions for security and resiliency
  - Entry Level Solutions
    - Tend to lack hardware redundancy, have reduce encryption capability, and rely on other software to perform disaster recovery
  - Midrange-Enterprise Solutions
    - Tend to be fully hardware redundant
    - Tend to have built in Site-to-Site disaster recovery capabilities
    - Tend to have better encryption features such as Hardware encryption and support for FIPS certified full disk encryption
  - Since larger storage systems tend to have better security features, sharing infrastructure between CIP and non-CIP assets could in some cases increase the security and reliability of the systems.

Scaling Storage Networks

- **References for Vendor Comparisons**
  - https://www.hpe.com/h20195/v2/GetDocument.aspx?docname=c04111444&doctype=quickspecs&doclang=EN_US&searchquery=&cc=us&lc=en
  - https://www.hpe.com/h20195/v2/GetDocument.aspx?docname=c04607918&doctype=quickspecs&doclang=EN_US&searchquery=&cc=us&lc=en
  - http://learn.nimblestorage.com/c/lb-ds-afa-datasheet-en?x=JKG3xE
  - http://www.netapp.com/us/media/ds-3582.pdf
  - http://www.netapp.com/us/media/ds-3773-solidfire.pdf
  - http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/FY15Q3_87_SS_DellStorage_PS4210_102114.pdf
  - https://www.emc.com/collateral/data-sheet/h14957-unity-all-flash-family-ss.pdf
  - https://www.nimblestorage.com/blog/nimble-storage-adds-encryption-of-data-at-rest/

Webinar 3 - Storage Summary

Storage

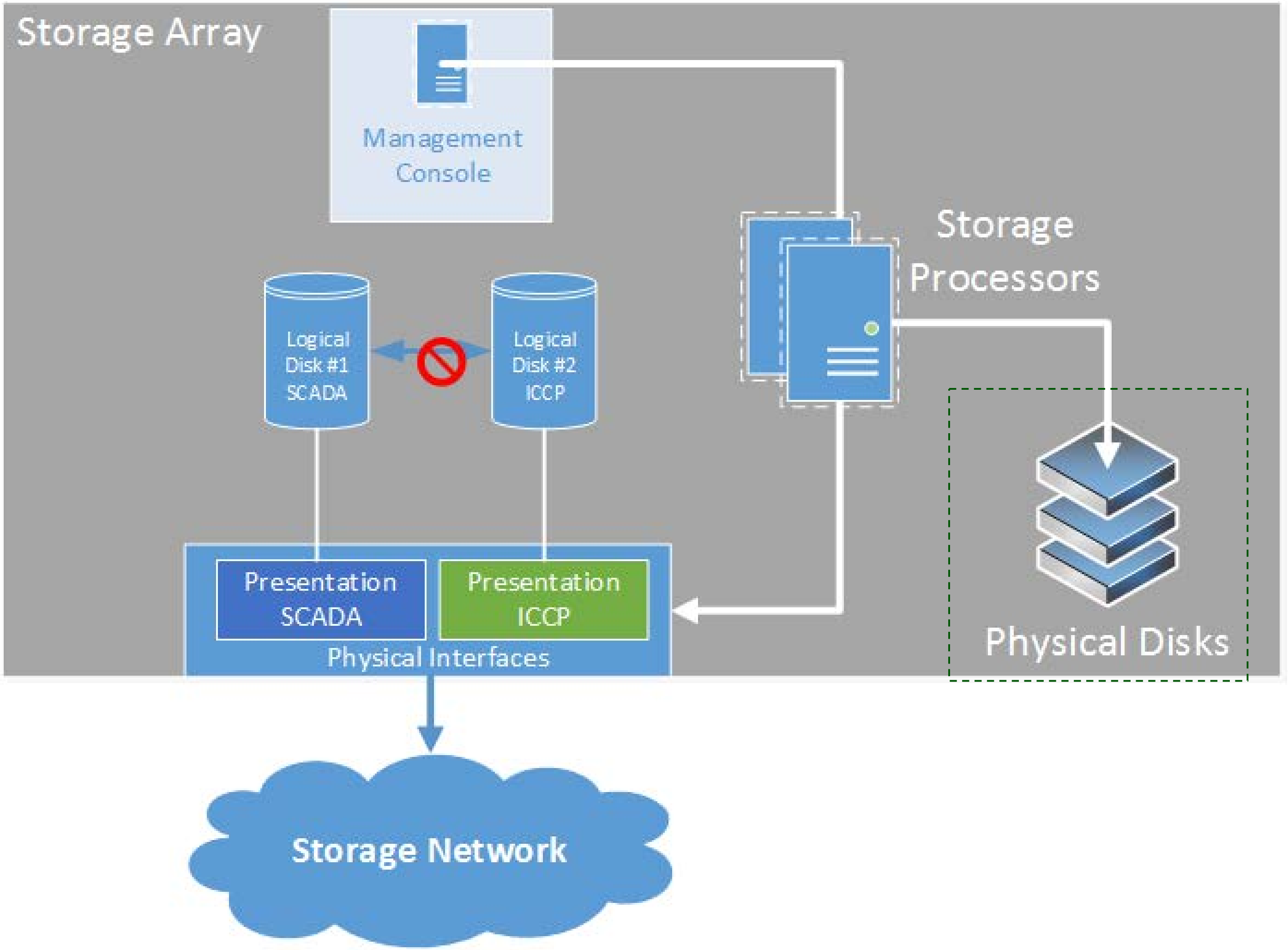
- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection

Data Protection

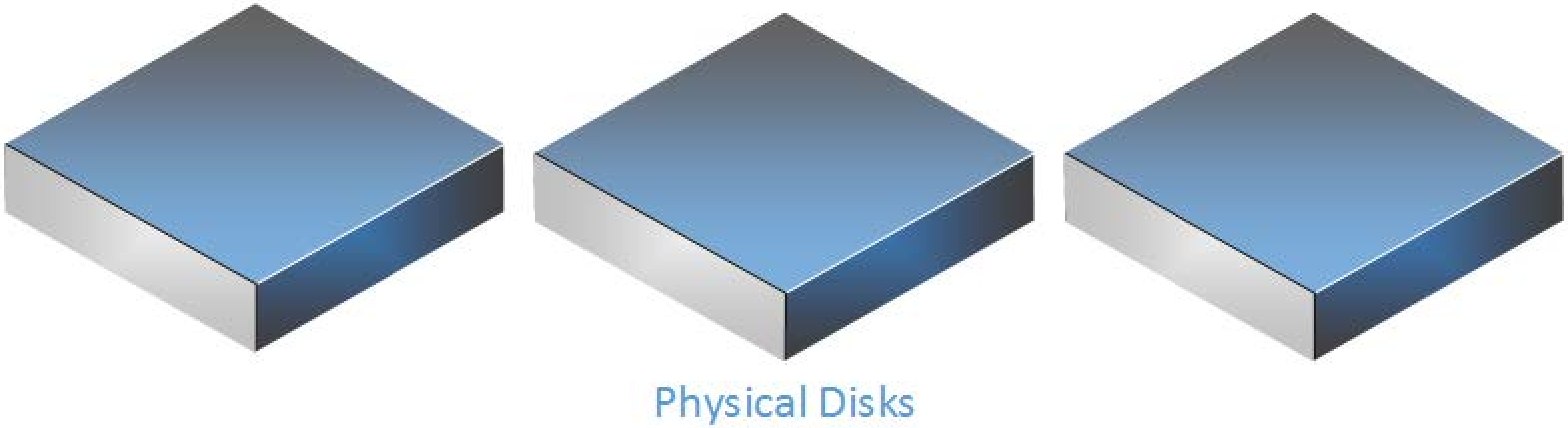
- *Cyber Asset Definition:*
  - *A programmable electronic device (physical or virtual), including the hardware, software, and data in the device. Each virtual machine and host is itself a distinct Cyber Asset.*

- The Storage hardware houses the data and is considered Underlay. Assumes the highest level of security (The CIP definition of Cyber Asset is inclusive of the data)

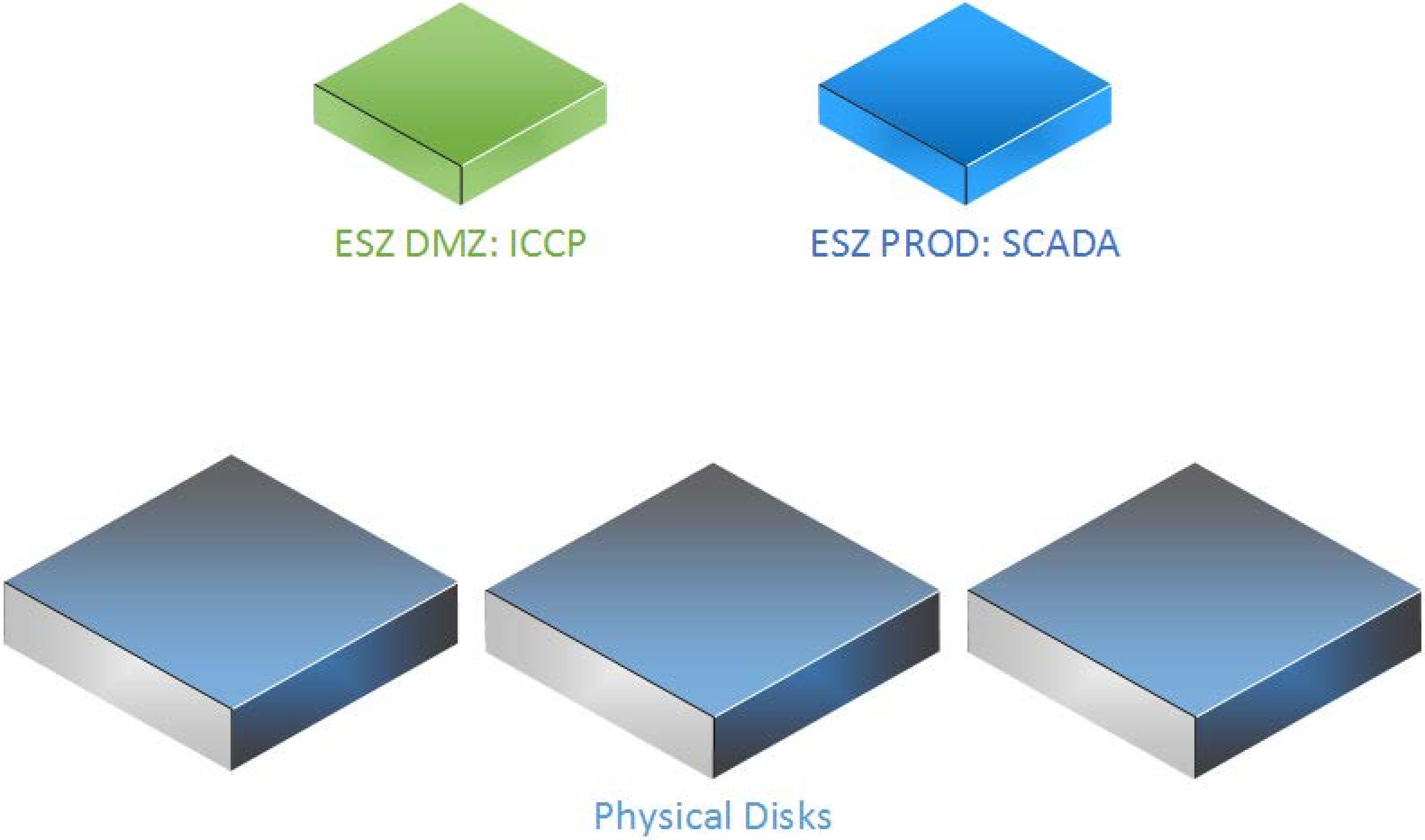
Data Protection



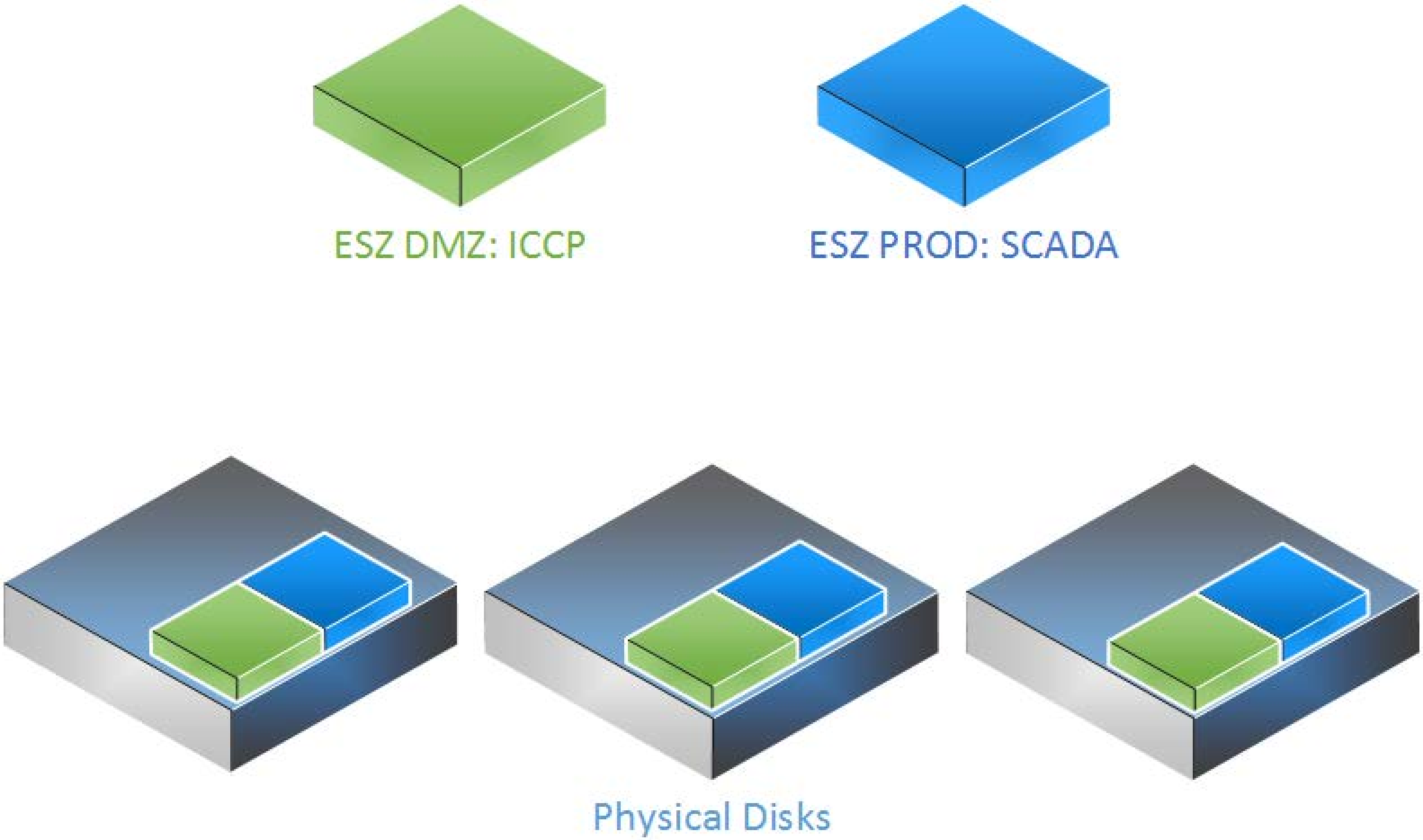
Data Protection



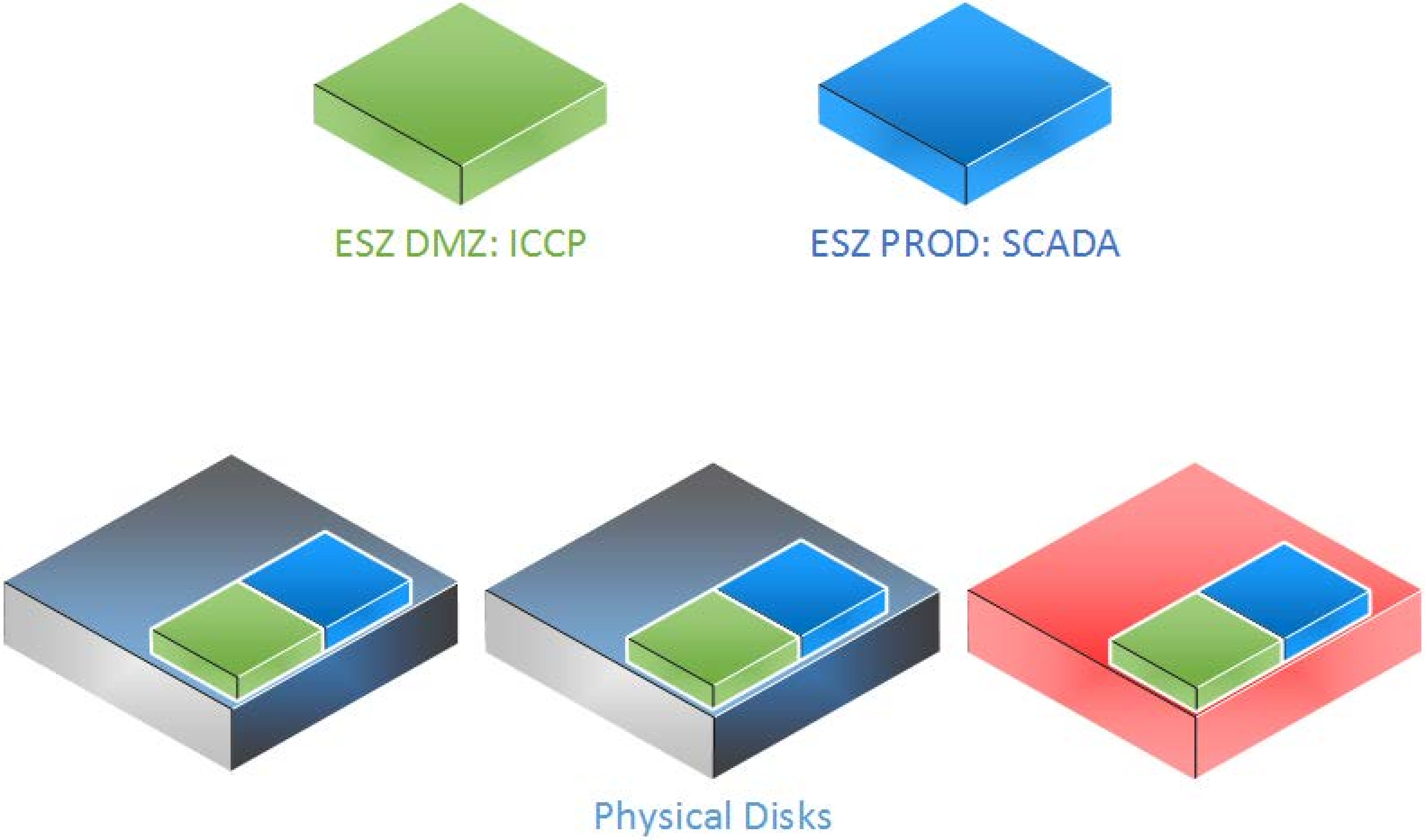
Data Protection



Data Protection



Data Protection

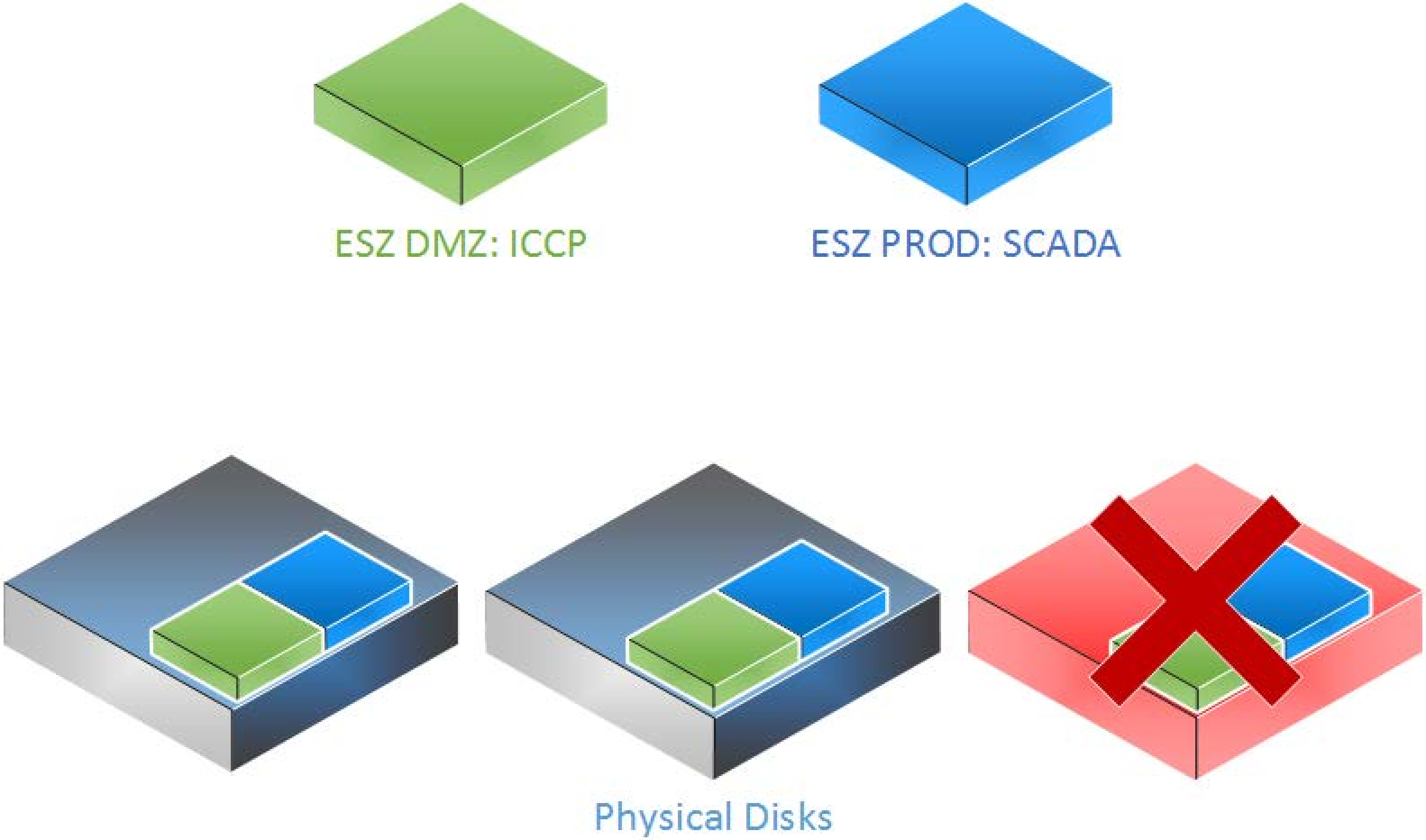


ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks

Data Protection

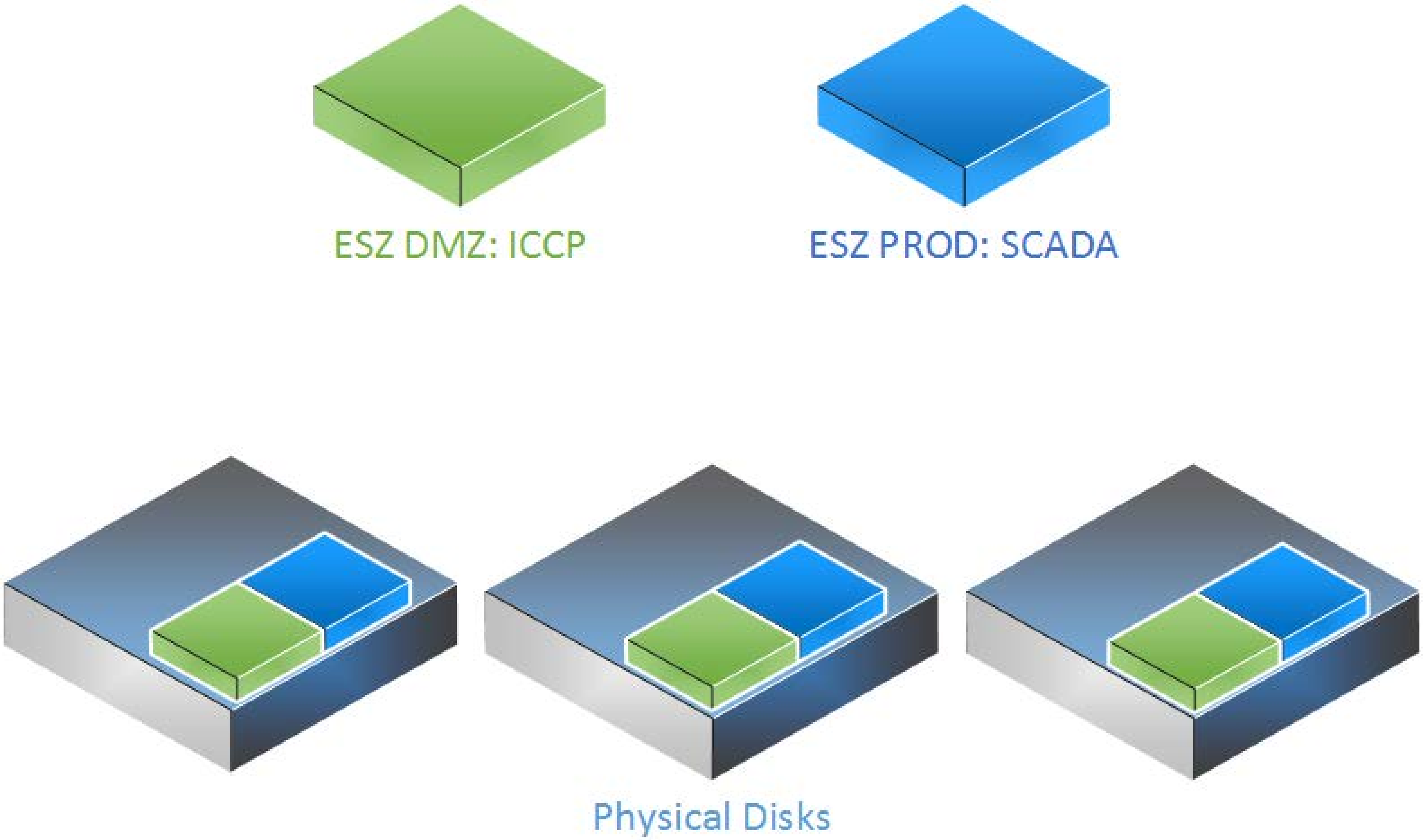


ESZ DMZ: ICCP

ESZ PROD: SCADA

Physical Disks

Data Protection

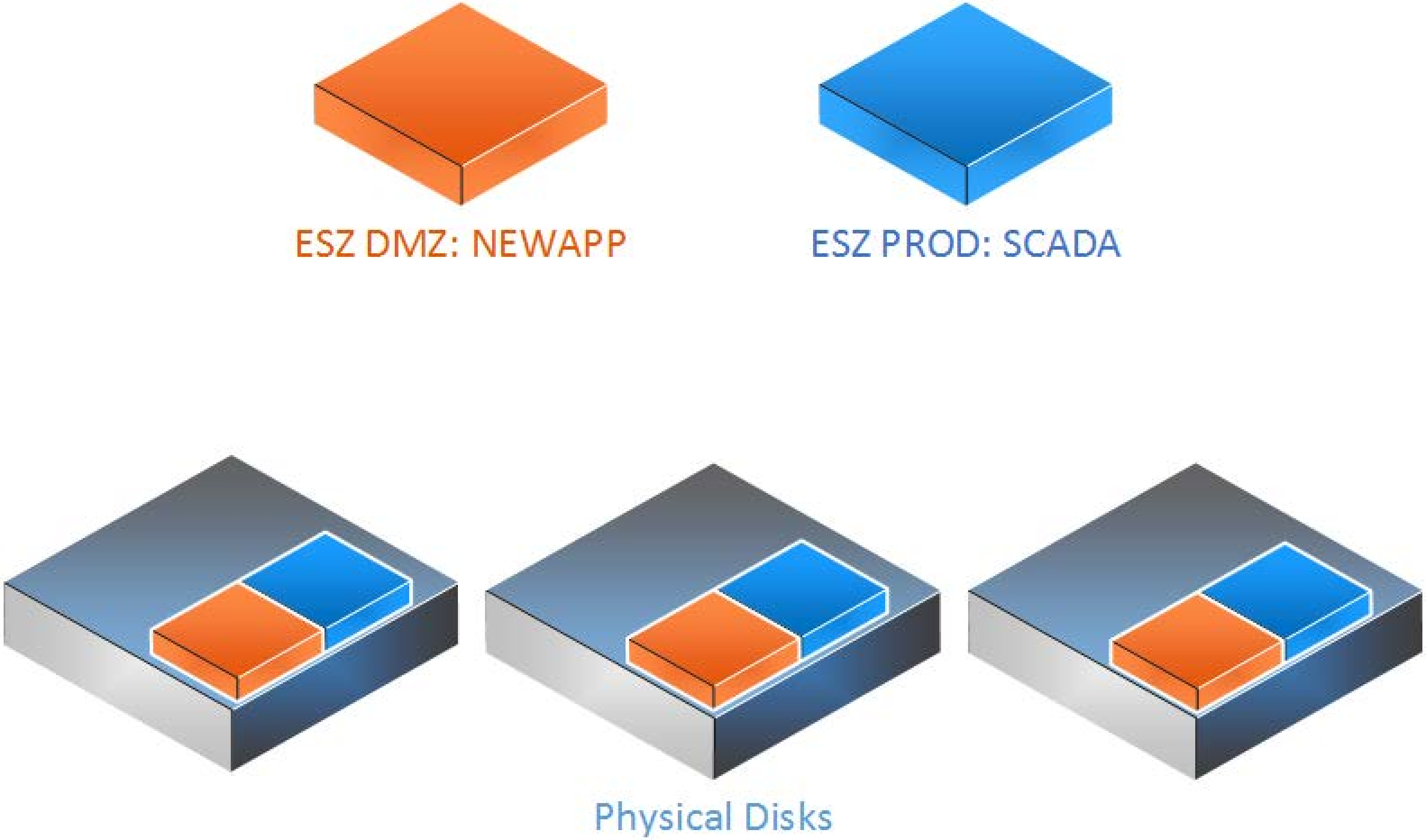


ESZ DMZ: ICCP

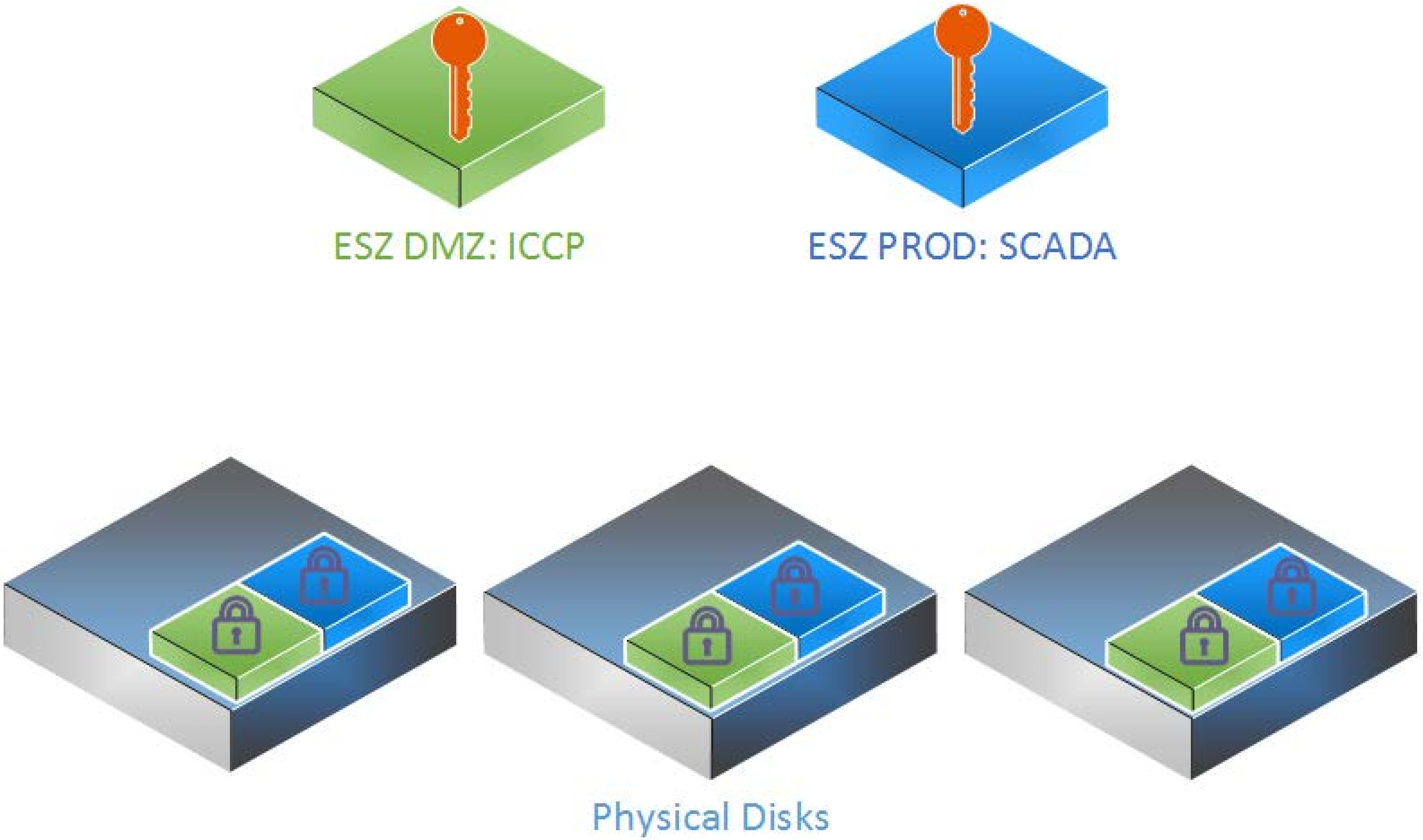
ESZ PROD: SCADA

Physical Disks

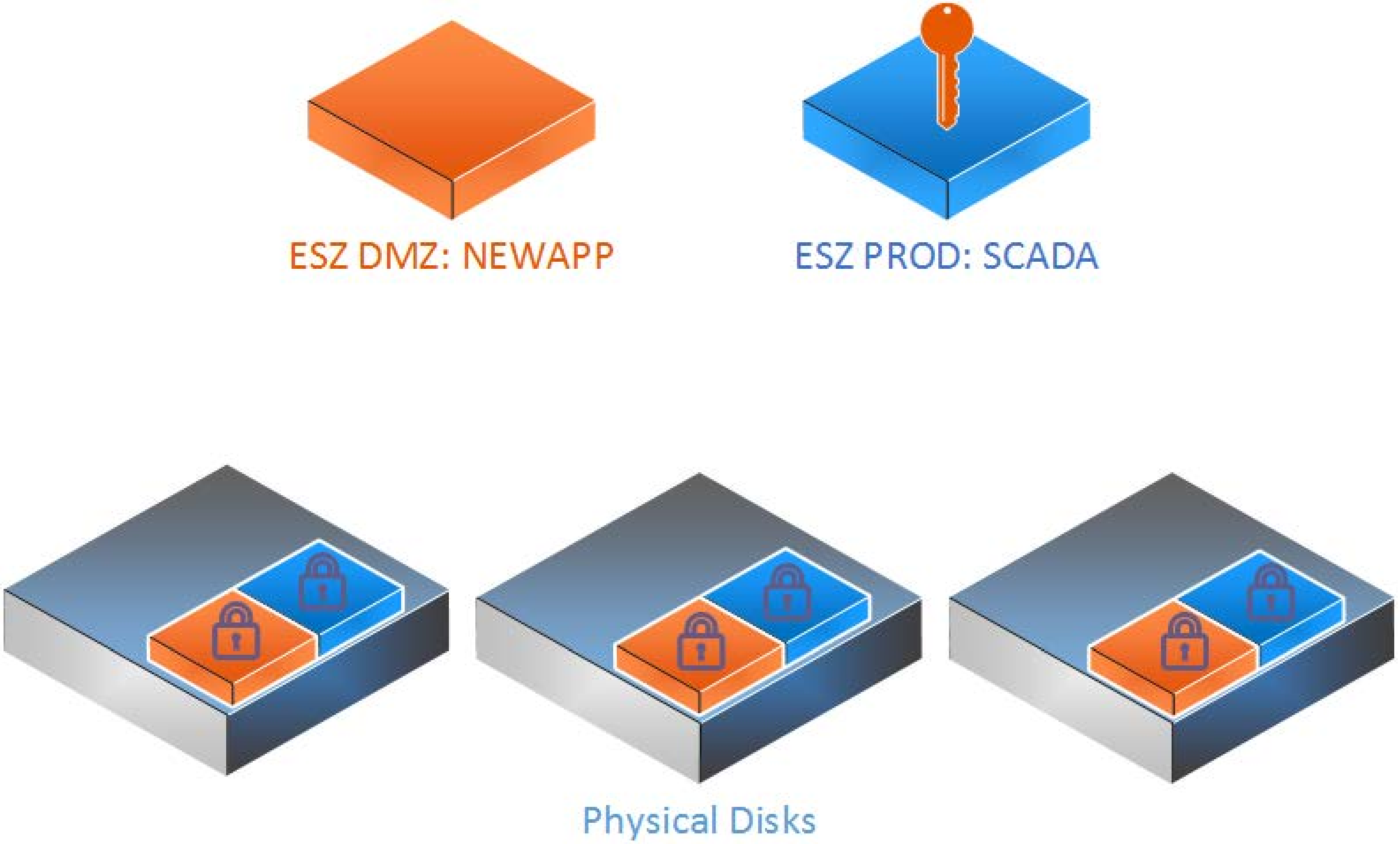
Data Protection



Data Protection



Data Protection



Data Protection

- Controls Exist in CIP11
  - Part 1.1 of CIP-011 is related to BCS Information identification and part 1.2 to BCS Information protection and handling procedures
  - As currently drafted– both apply to physical and virtual environments

- CIP-011 Part 2.1 Requirement:
  - Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset Storage Media

Data Protection

- CIP-011 Part 2.1 Measure:
  - Examples of acceptable evidence include, but are not limited to: Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying;
  - Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

Data Protection

- CIP-011 Part 2.2 Requirement
- Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.

- CIP-011 Part 2.2 Measure
  - Examples of acceptable evidence include, but are not limited to:

    Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

Data Protection

- Data Protection Wrap-up
  - The Cyber Asset Definition is inclusive of data
  - There are two main ways to ensure data is destroyed
    - Destroy ALL physical media
    - Encrypt the data with security zone specific keys
  - CIP11 has Controls that address the risks associated with information protection
    - The SDT believes the applicability of CIP11 as drafted is inclusive of multi-instance environments

Webinar 3 - Storage Summary

Storage

- Storage Systems Evolution and Overview
- Applying ESZ’s to different storage systems
- Scaling Storage Networks
- Data Protection

Questions and Answers