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**
April 18, 2017

RELIABILITY | ACCOUNTABILITY

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.

Agenda

- Opening Remarks and Introduction of Presenters
- Administrative Items
  - Antitrust and Disclaimers
  - Webinar Format
- Standard Drafting Team
- Hypervisors
- What is multi-tenancy?
- Questions and Answers

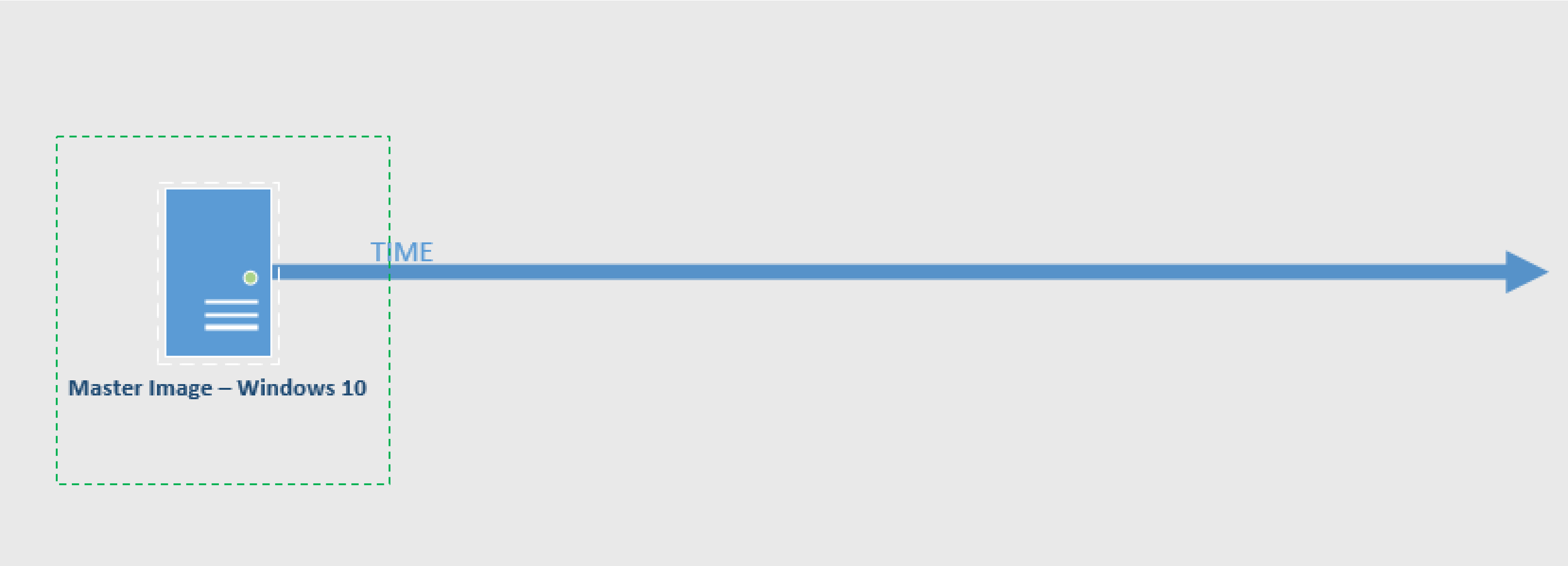
CIP Standard Drafting Team

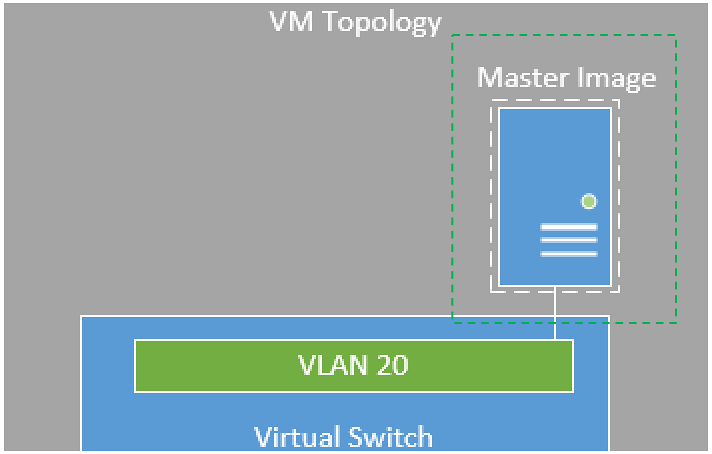
	Name	Entity
Co-Chair	Christine Hasha	Electric Reliability Council of Texas
Co-Chair	David Revill	Georgia System Operations Corporation
Members	Steven Brain	Dominion
	Jay Cribb	Southern Company
	Jennifer Flandermeyer	Kansas City Power and Light
	Tom Foster	PJM Interconnection
	Richard Kinas	Orlando Utilities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

Virtualization Webinar Summary

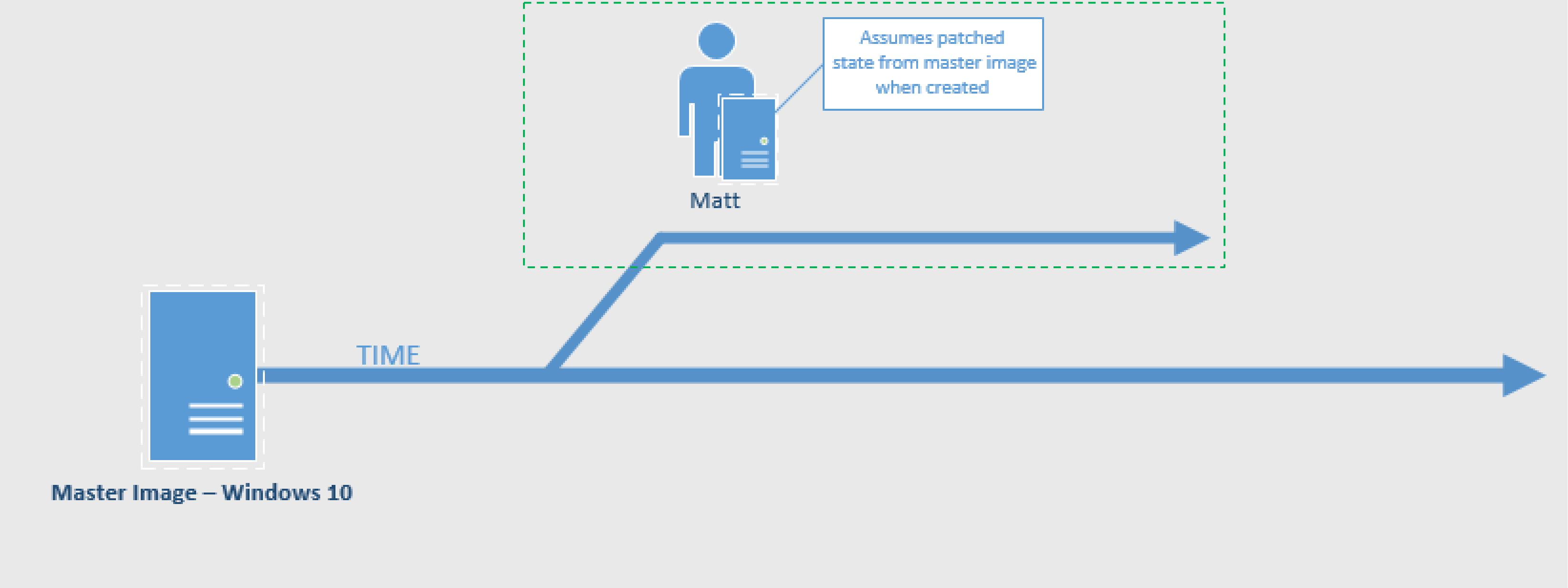
1. **Hypervisors**
   - Template Considerations
   - Why VM guest need to be treated as CyberAsset
   - Security Patches address ongoing Hypervisor Vulnerabilities
2. **What is multi-tenancy?**
   - Define Multi-tenancy, Tenants, Overlay, and Underlay
   - Building a multi-tenant environment
   - Introduce ESZ Concept

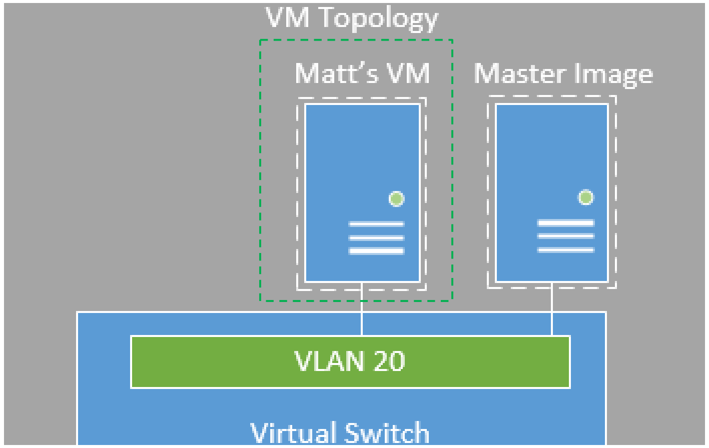
Hypervisor Templates – VDI Use Cases



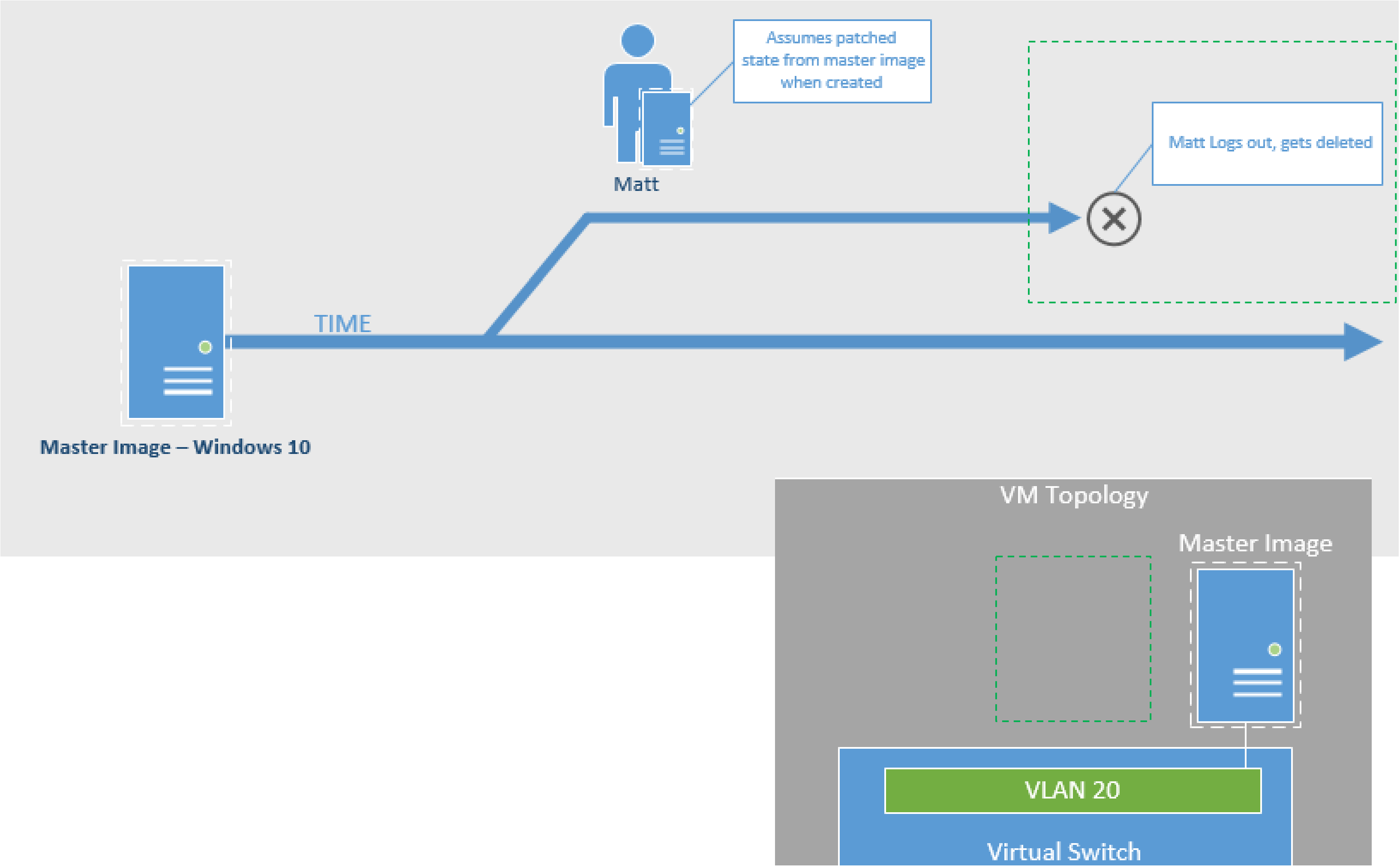


Hypervisor Templates – VDI Use Cases


Assumes patched state from master image when created
Matt
TIME
Master Image – Windows 10



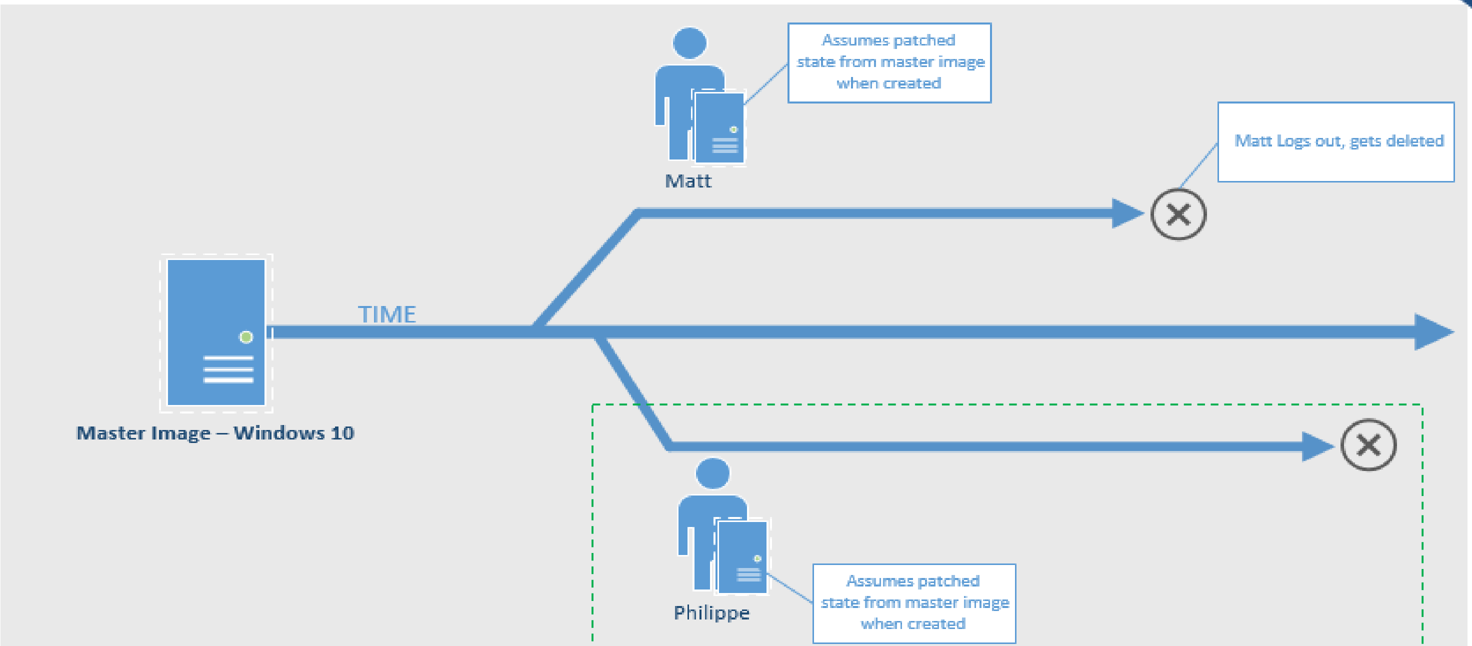
Hypervisor Templates – VDI Use Cases

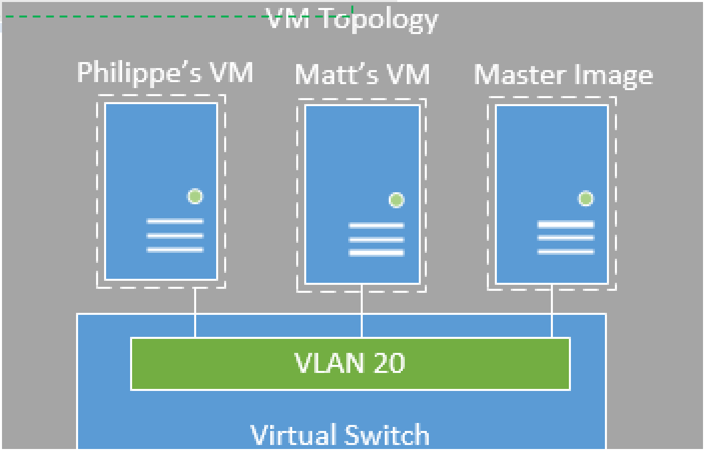


Assumes patched state from master image when created

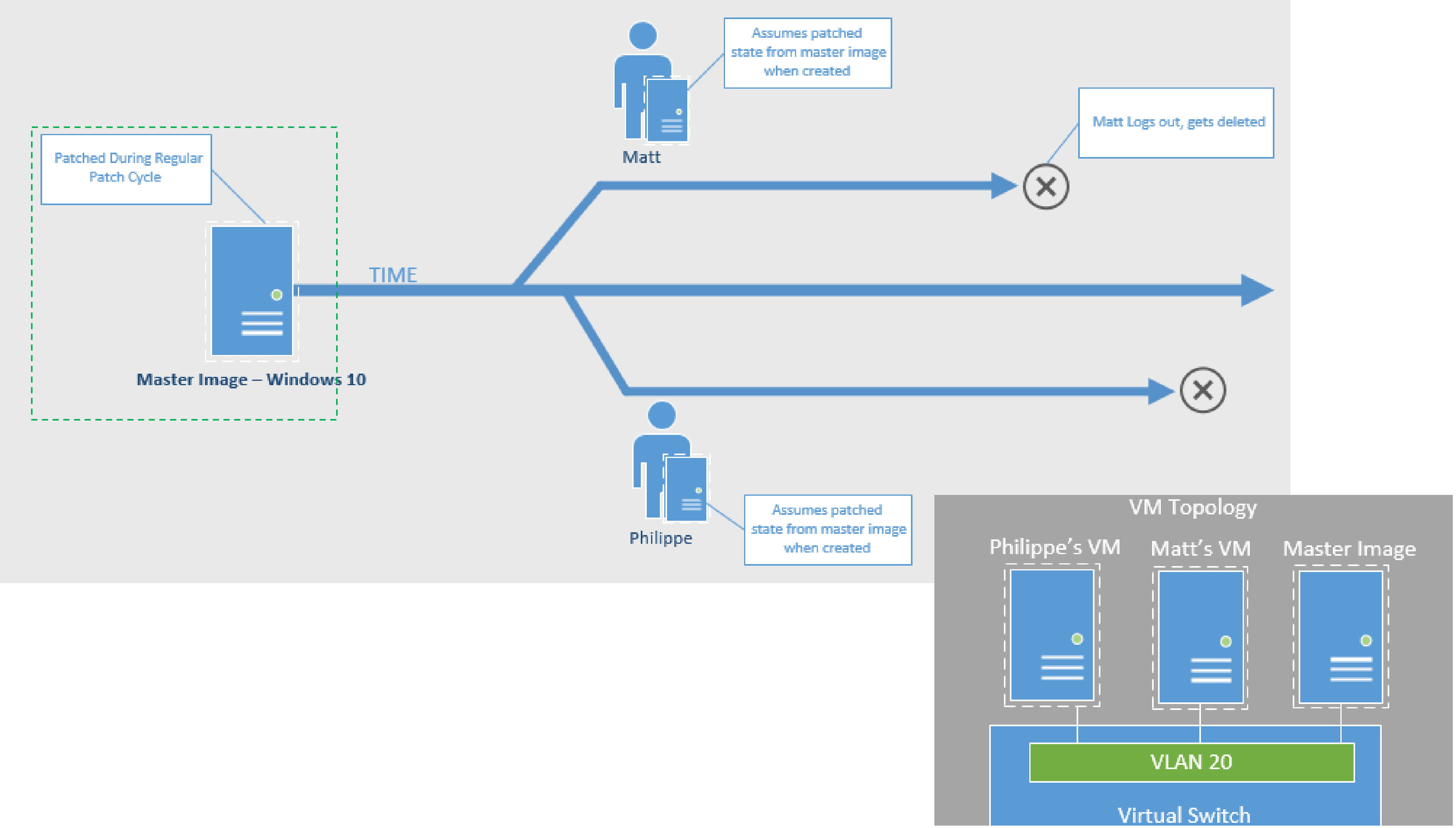
Matt Logs out, gets deleted

Hypervisor Templates – VDI Use Cases

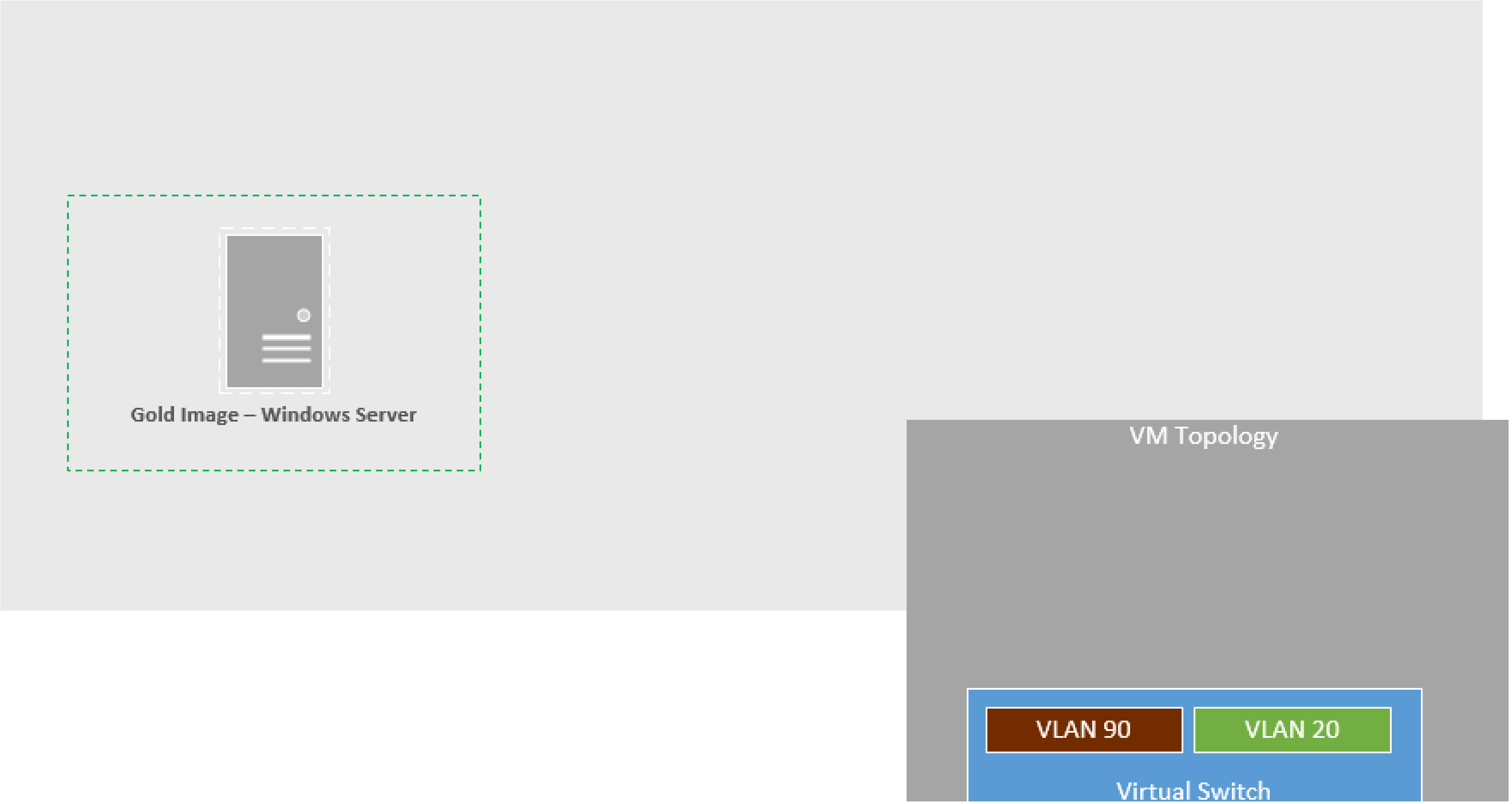

Assumes patched state from master image when created
Matt
Matt Logs out, gets deleted
TIME
Master Image – Windows 10
Philippe
Assumes patched state from master image when created



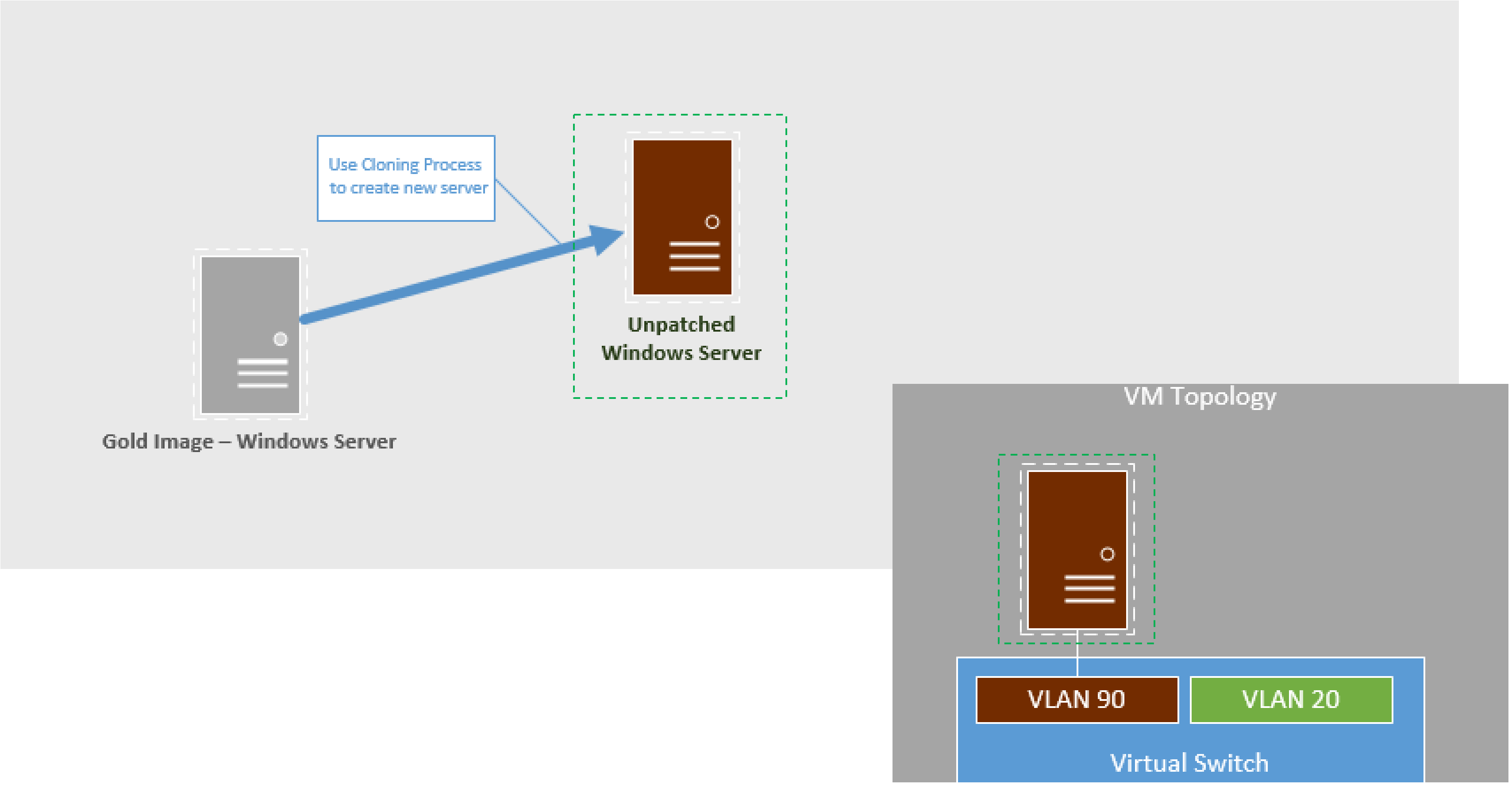
Hypervisor Templates – VDI Use Cases


Patched During Regular Patch Cycle
Master Image – Windows 10
TIME
Matt
Assumes patched state from master image when created
Matt Logs out, gets deleted
Philippe
Assumes patched state from master image when created
VM Topology
Philippe's VM
Matt's VM
Master Image
VLAN 20
Virtual Switch

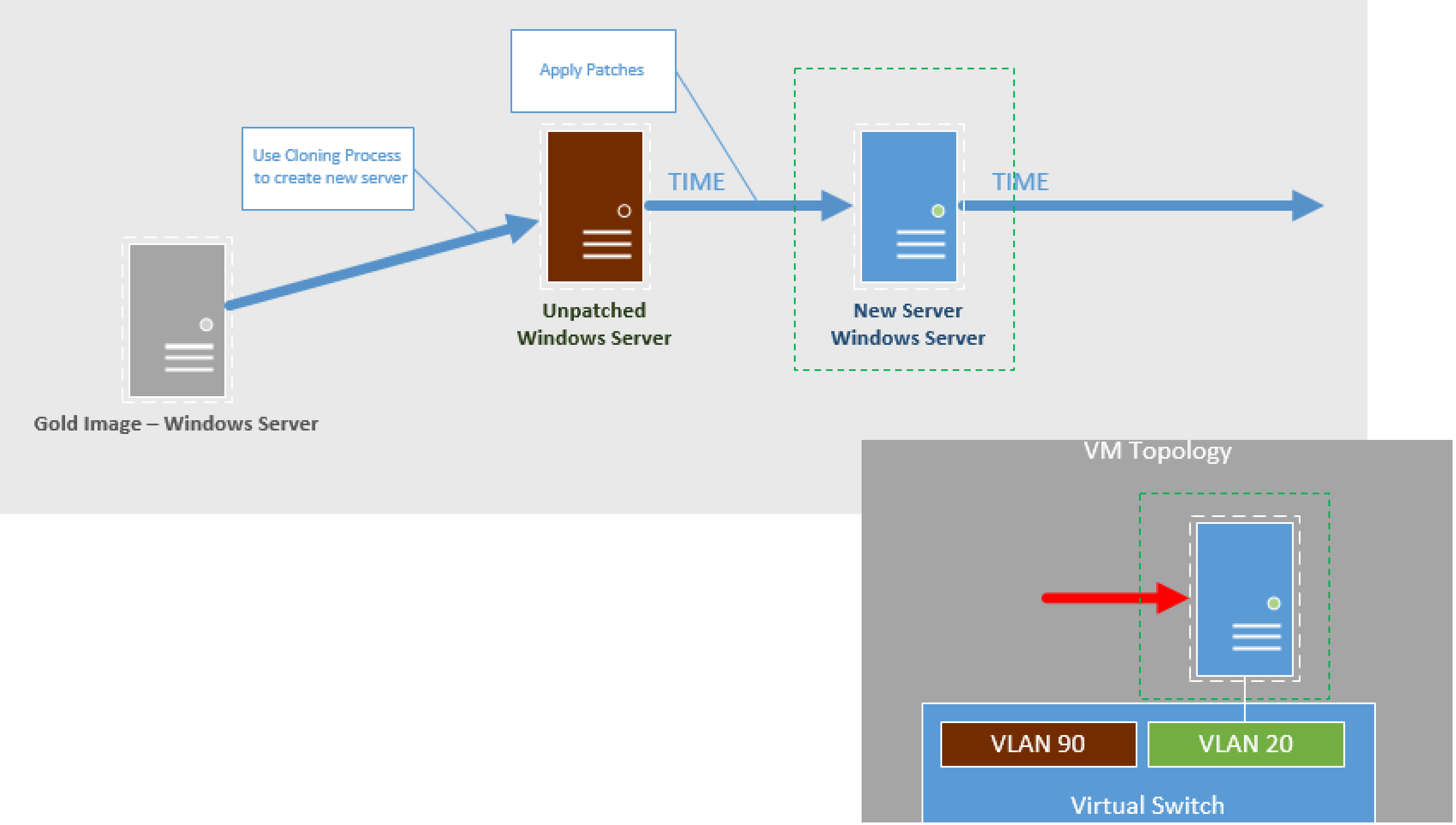
HV Templates – Dormant Images



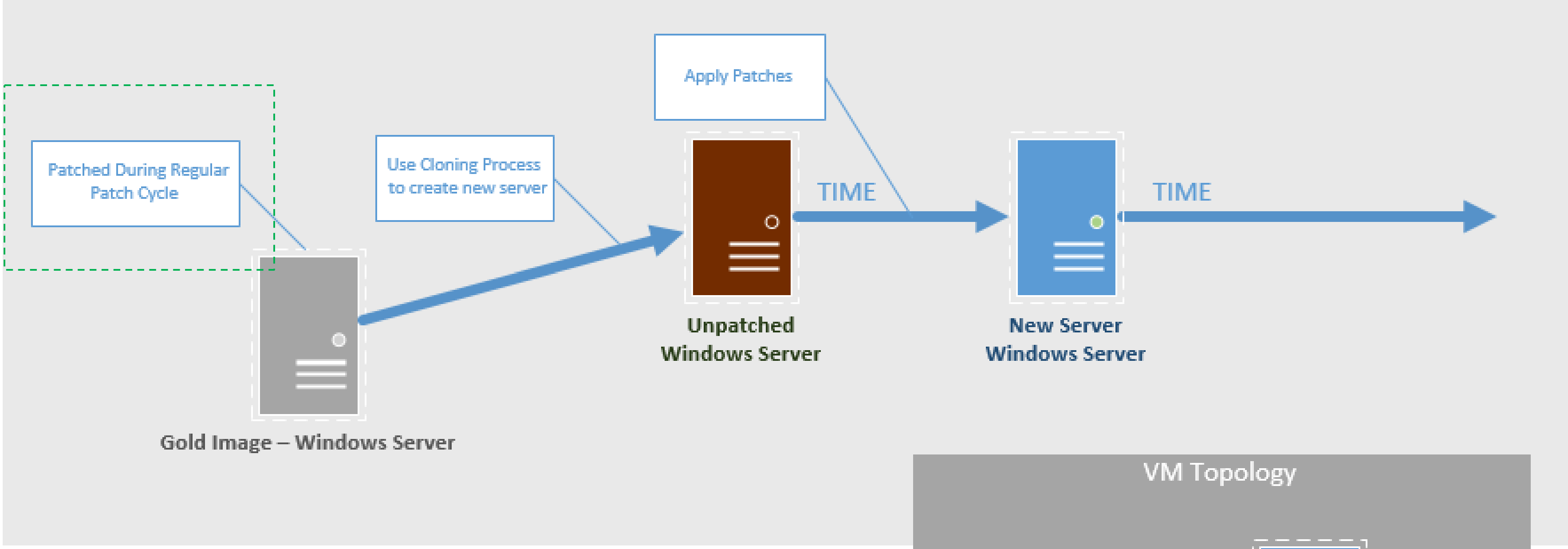
HV Templates – Dormant Images

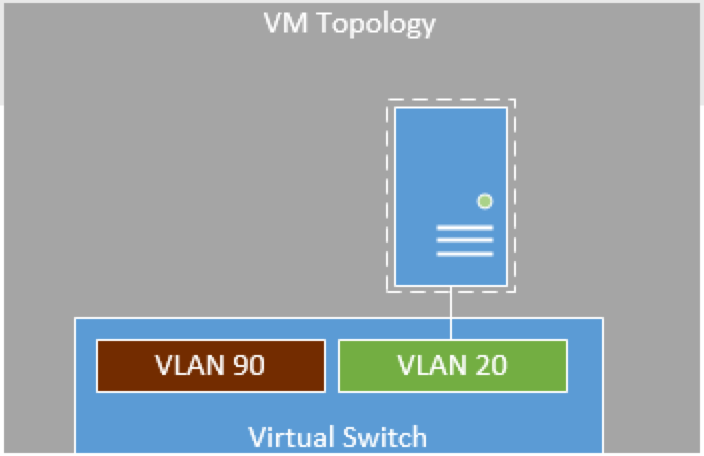

Use Cloning Process to create new server
Unpatched Windows Server
Gold Image – Windows Server
VM Topology
VLAN 90
VLAN 20
Virtual Switch

HV Templates – Dormant Images

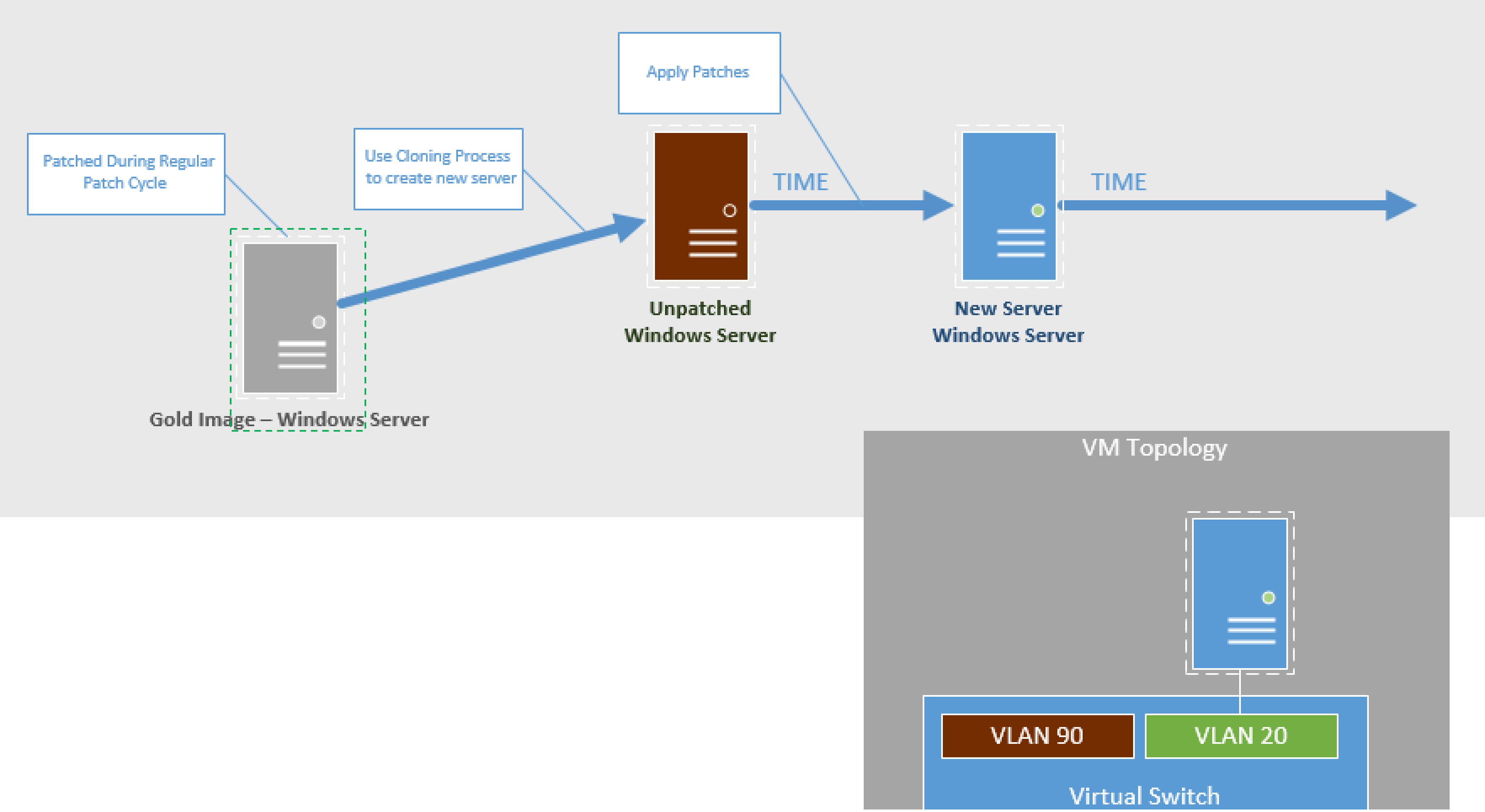

Apply Patches
Use Cloning Process to create new server
TIME
TIME
Unpatched Windows Server
New Server Windows Server
Gold Image – Windows Server
VM Topology
VLAN 90
VLAN 20
Virtual Switch

HV Templates – Dormant Images


Apply Patches
Patched During Regular Patch Cycle
Use Cloning Process to create new server
TIME
TIME
Unpatched Windows Server
New Server Windows Server
Gold Image – Windows Server



CIP Considerations for the Gold Images

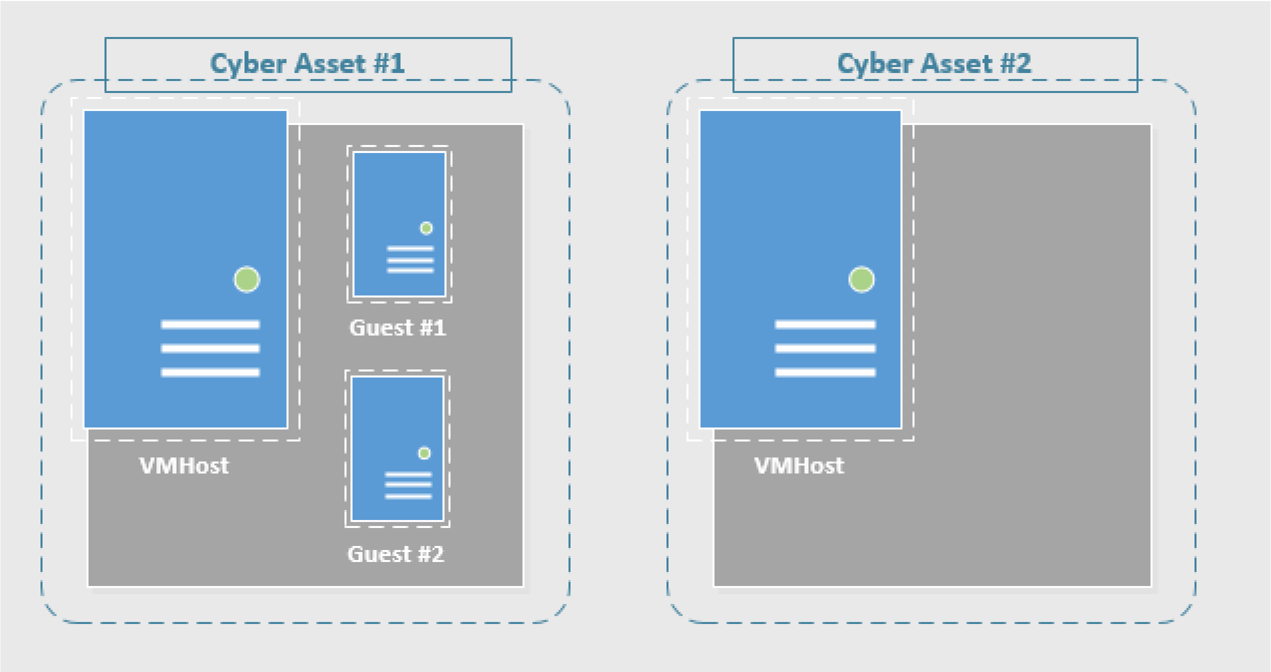

Patched During Regular Patch Cycle
Use Cloning Process to create new server
Apply Patches
TIME
TIME
Unpatched Windows Server
New Server Windows Server
Gold Image – Windows Server
VM Topology
VLAN 90
VLAN 20
Virtual Switch

Considerations for Templates in CIP-010

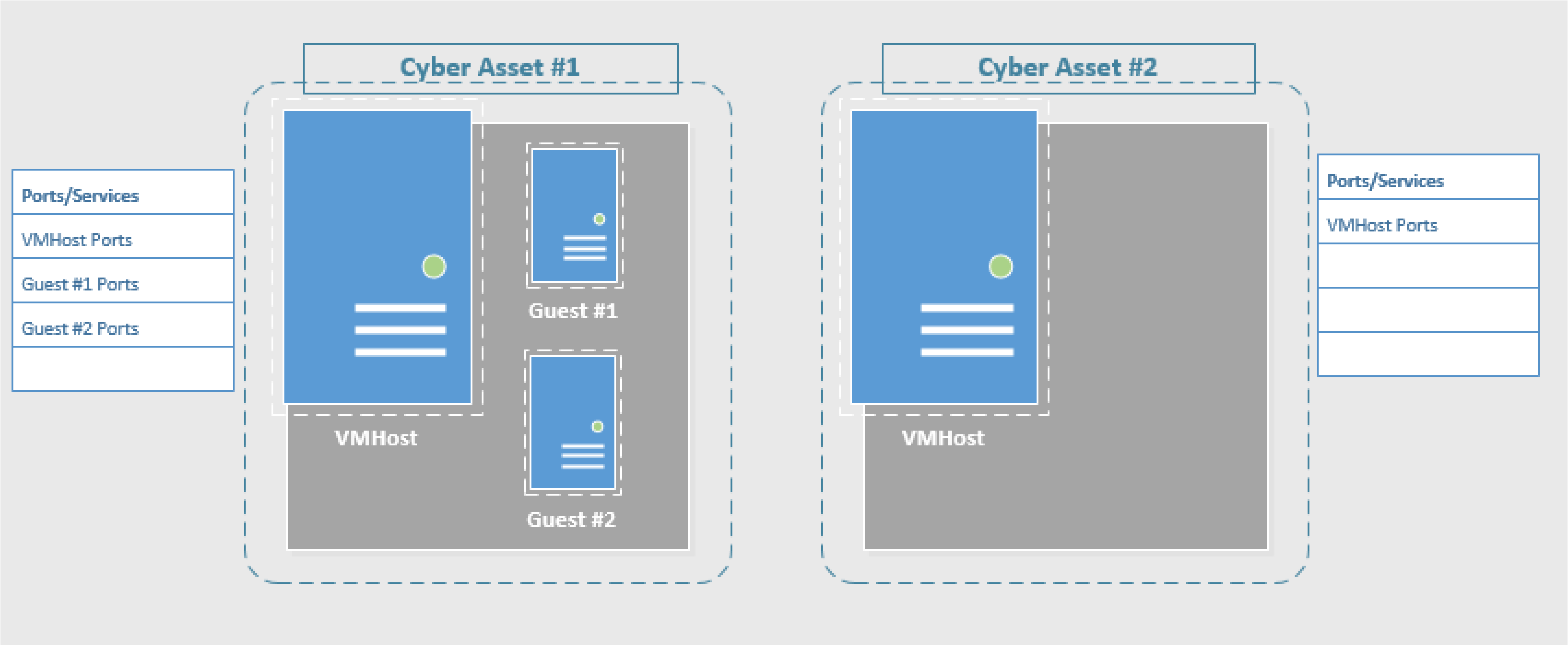
- *Baseline Templates*
  - *Could be created for Database Servers, Webservers, etc*
  - *Contains no specific application settings but is up to date with security patches and baselined software packages for rapid deployment*

- *CIP-010 Part 1.1 requires the development of a baseline configuration individually or by group, demonstration of compliance for the VMs could be achieved by using the baseline configuration of the Master Image, all baseline configuration elements being identical to the master image for all instances created.*

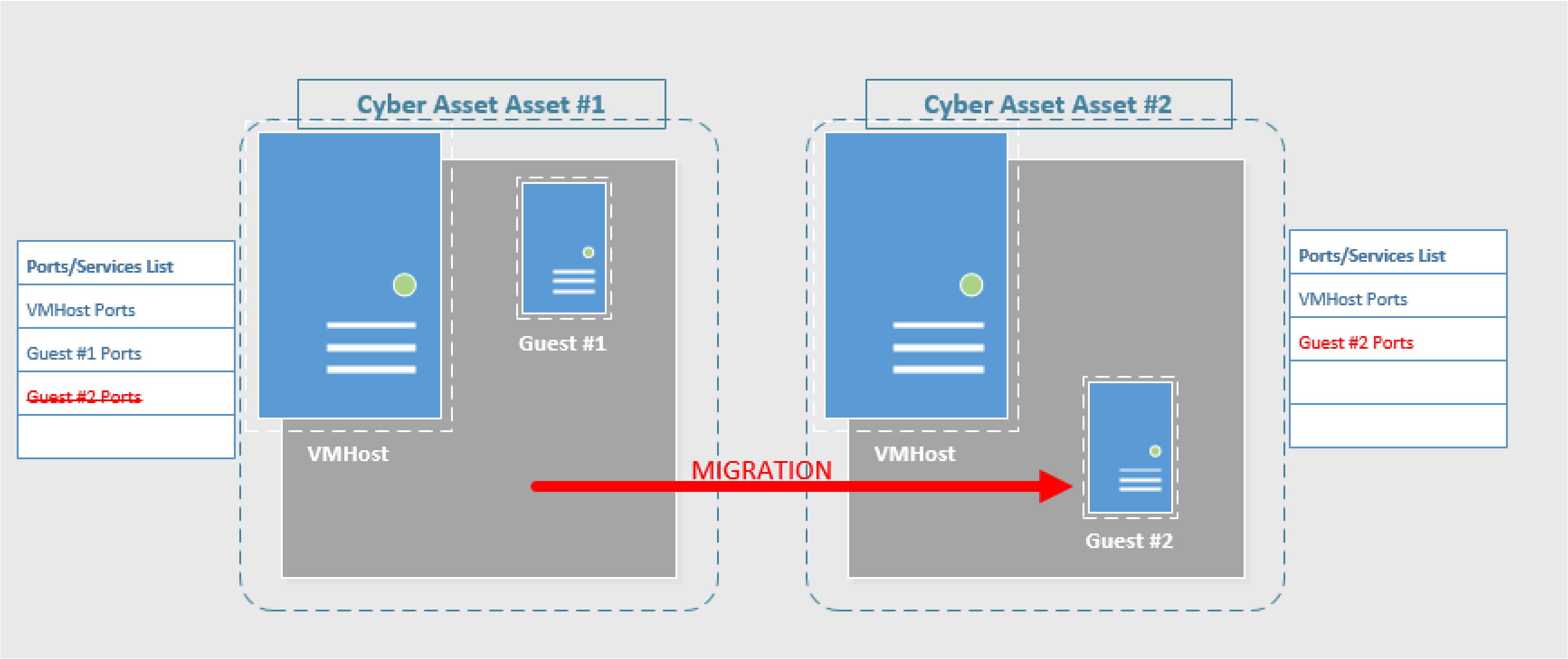
VM's as Software on Cyber Assets



VM’s as Software on Assets: Ports/Services



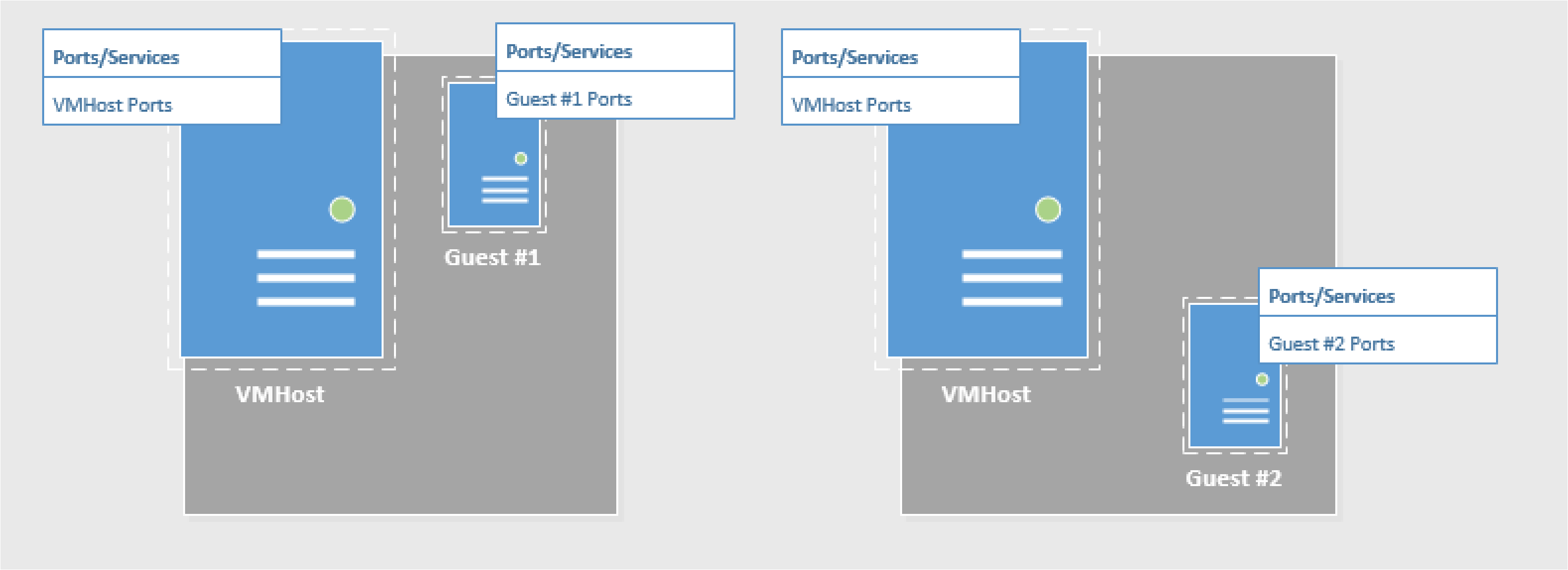
VM’s as Software on Assets: Ports/Services



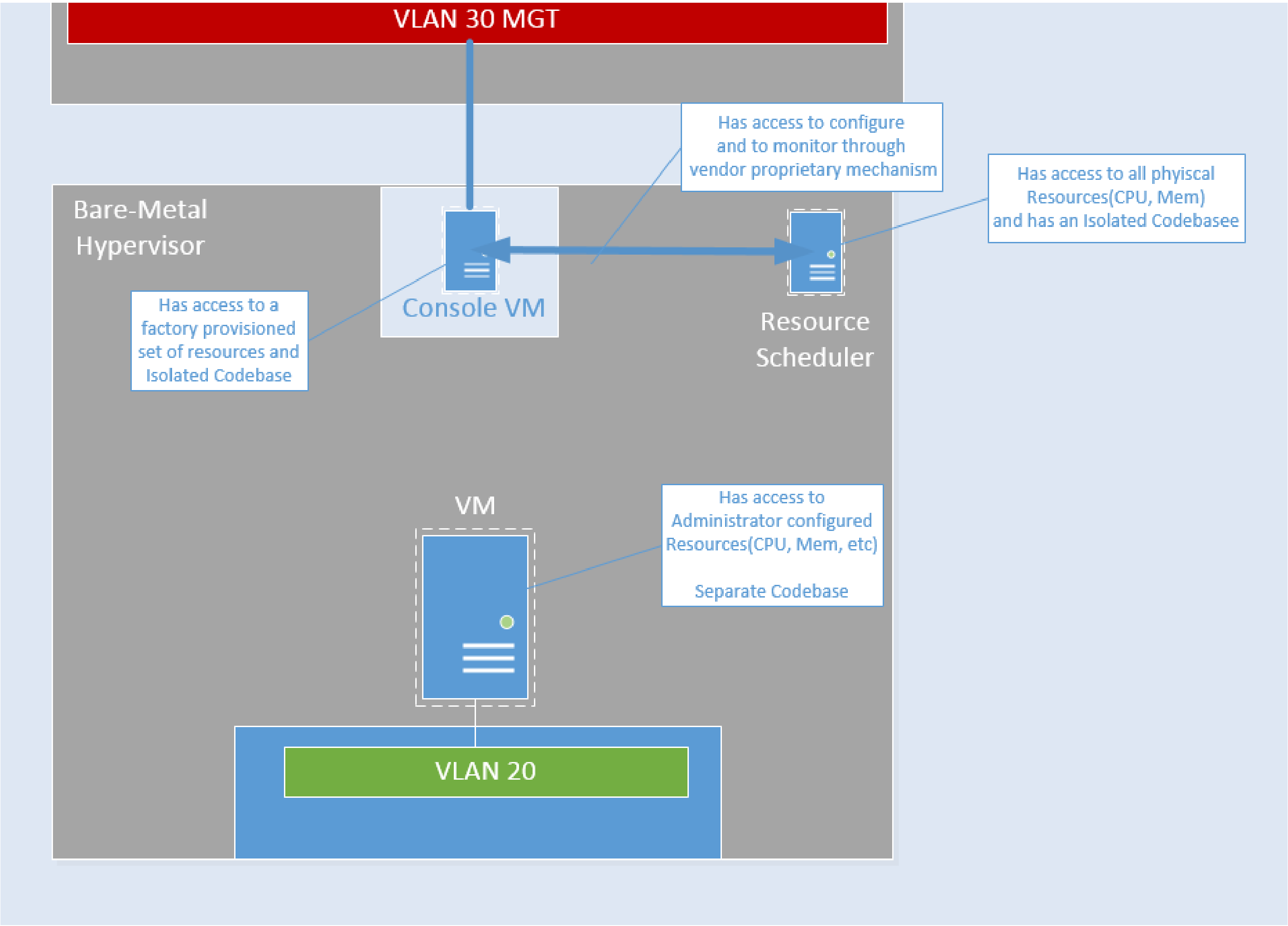
Ports/Services List
VMHost Ports
Guest #1 Ports
~~Guest #2 Ports~~

Ports/Services List
VMHost Ports
Guest #2 Ports

VM's treated as CA's: Ports/Services



VM’s treated as Software on bare-metal HV: Malware Prevention



Has access to configure and to monitor through vendor proprietary mechanism

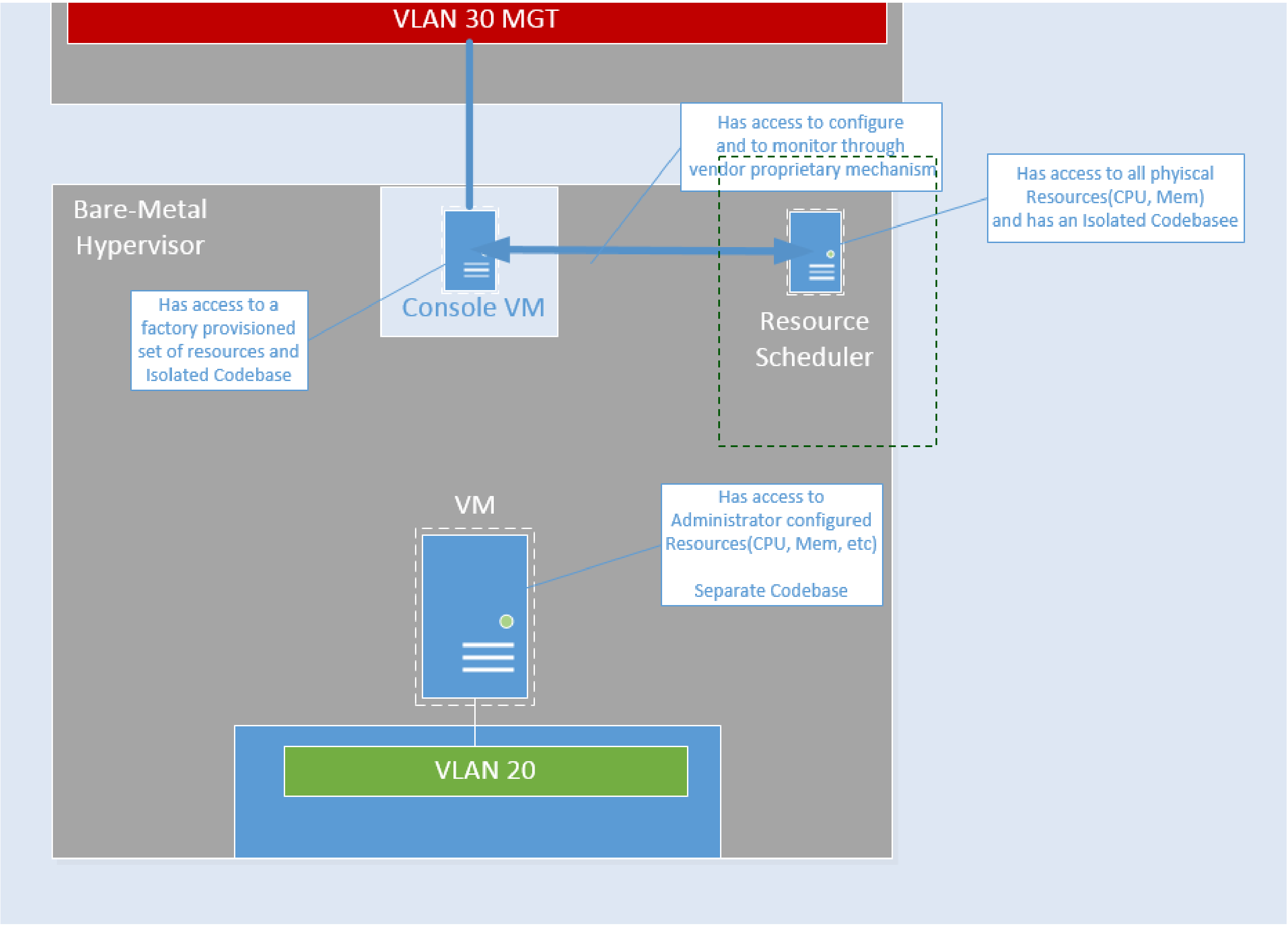
Has access to all phyiscal Resources(CPU, Mem) and has an Isolated Codebasee

Has access to a factory provisioned set of resources and Isolated Codebase

Has access to Administrator configured Resources(CPU, Mem, etc)

Separate Codebase

VM’s treated as Software on bare-metal HV: Malware Prevention



Has access to configure and to monitor through vendor proprietary mechanism

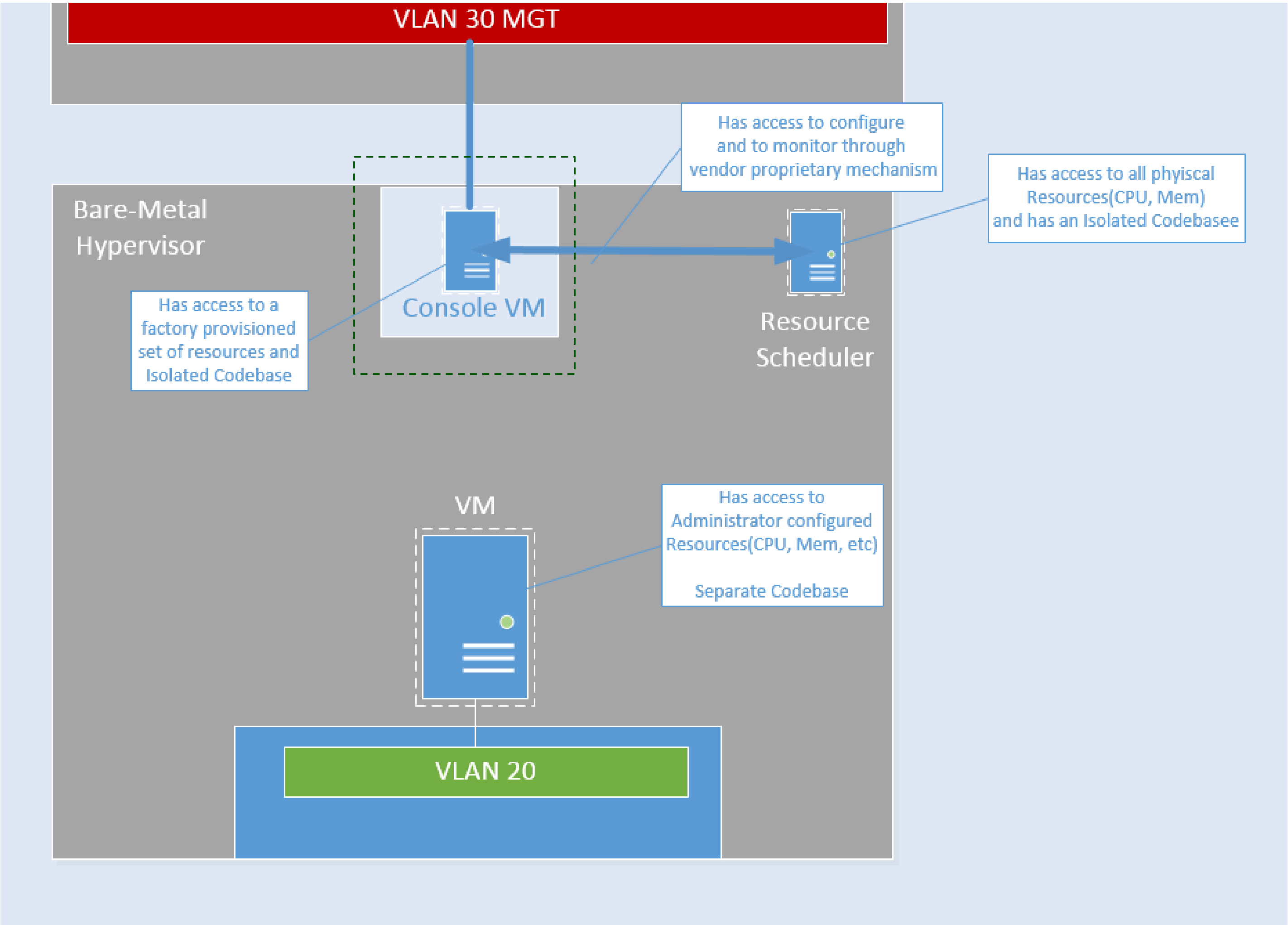
Has access to all phyiscal Resources(CPU, Mem) and has an Isolated Codebasee

Has access to a factory provisioned set of resources and Isolated Codebase

Has access to Administrator configured Resources(CPU, Mem, etc)

Separate Codebase

VM’s treated as Software on bare-metal HV: Malware Prevention



Has access to configure and to monitor through vendor proprietary mechanism

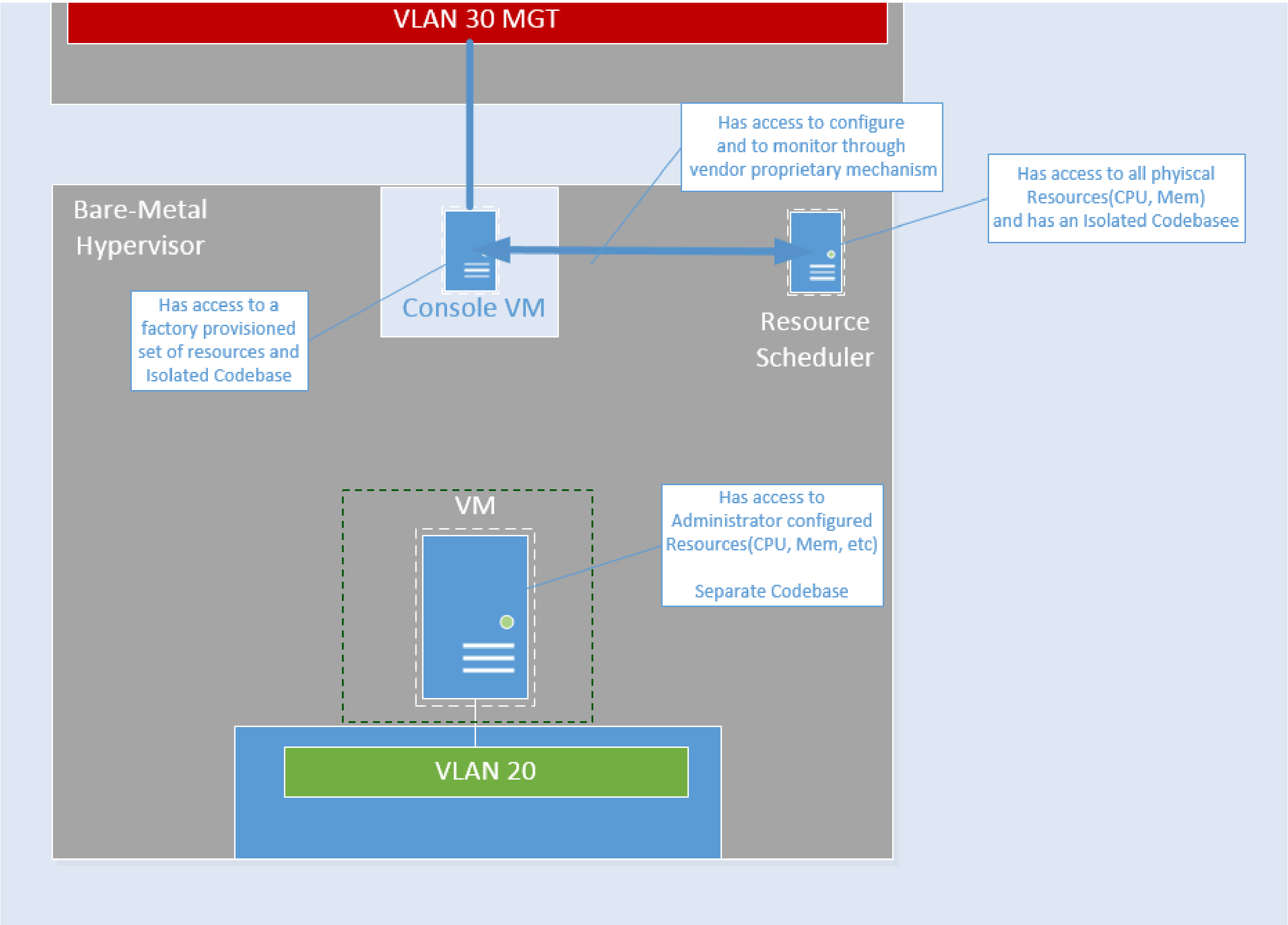
Has access to all phyiscal Resources(CPU, Mem) and has an Isolated Codebasee

Has access to a factory provisioned set of resources and Isolated Codebase

Has access to Administrator configured Resources(CPU, Mem, etc)

Separate Codebase

VM’s treated as Software on bare-metal HV: Malware Prevention



Has access to configure and to monitor through vendor proprietary mechanism

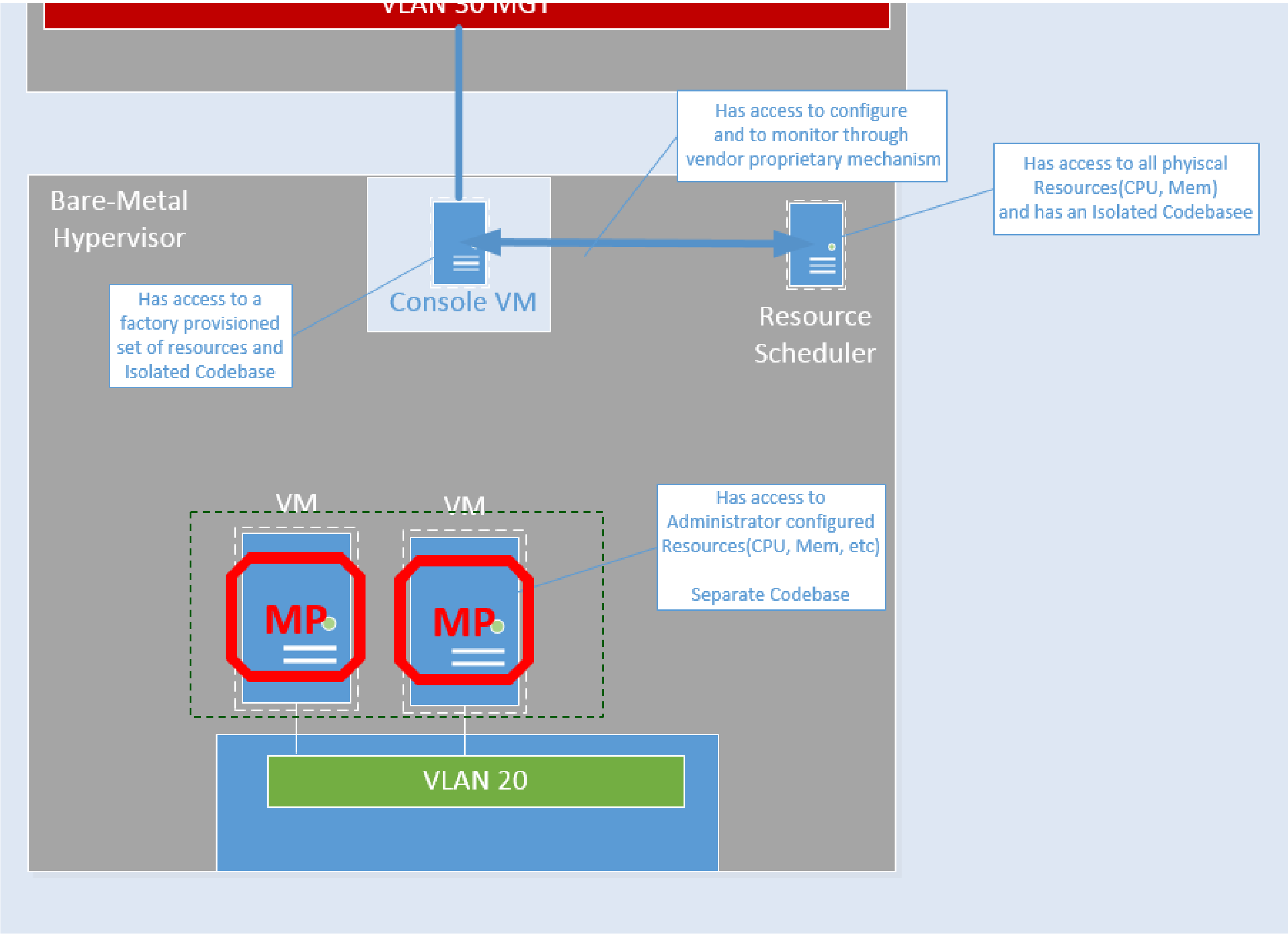
Has access to all phyiscal Resources(CPU, Mem) and has an Isolated Codebasee

Has access to a factory provisioned set of resources and Isolated Codebase

Has access to Administrator configured Resources(CPU, Mem, etc)

Separate Codebase

VM's treated as Software on bare-metal HV: Malware Prevention



Has access to configure and to monitor through vendor proprietary mechanism

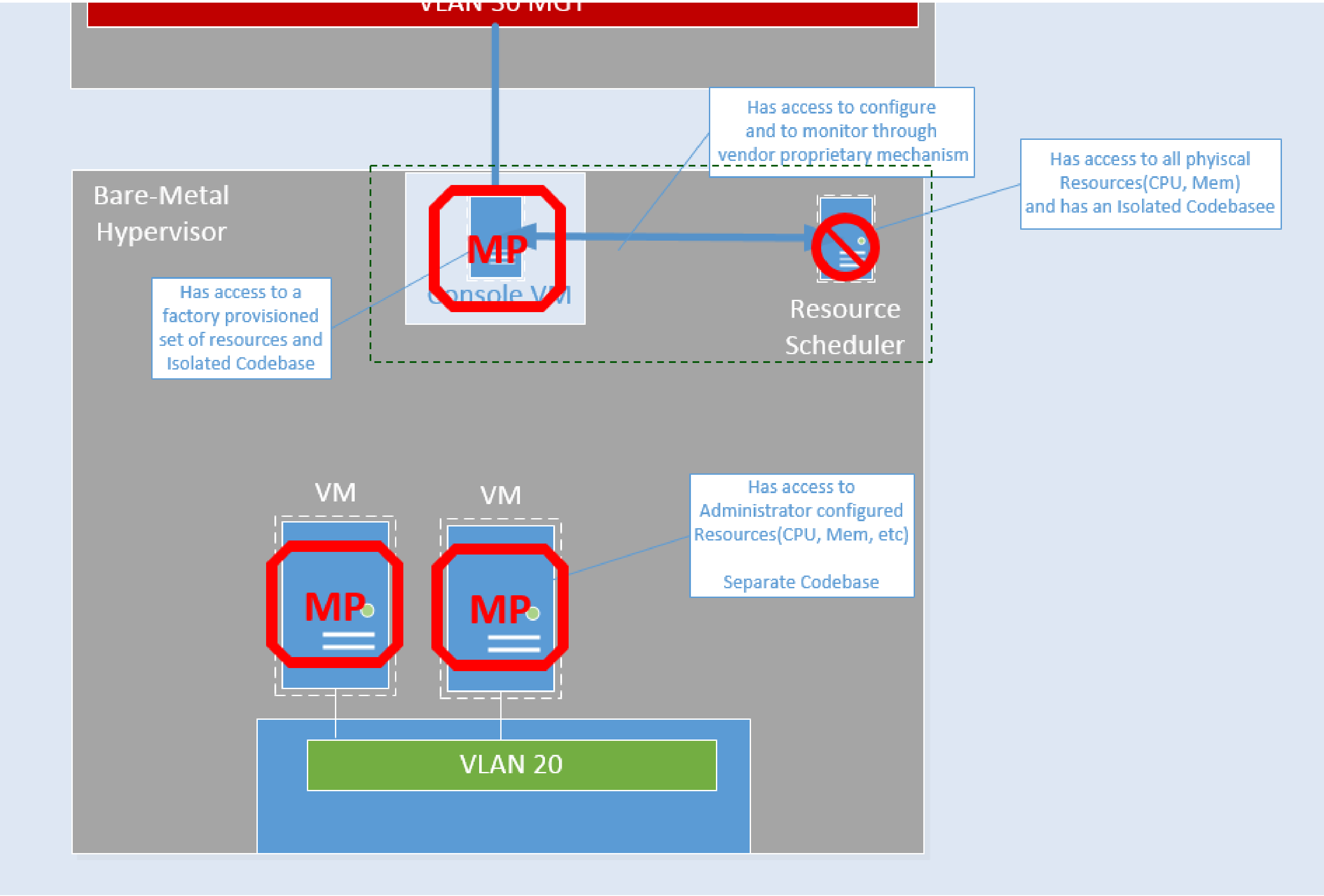
Has access to all phyiscal Resources(CPU, Mem) and has an Isolated Codebasee

Has access to a factory provisioned set of resources and Isolated Codebase

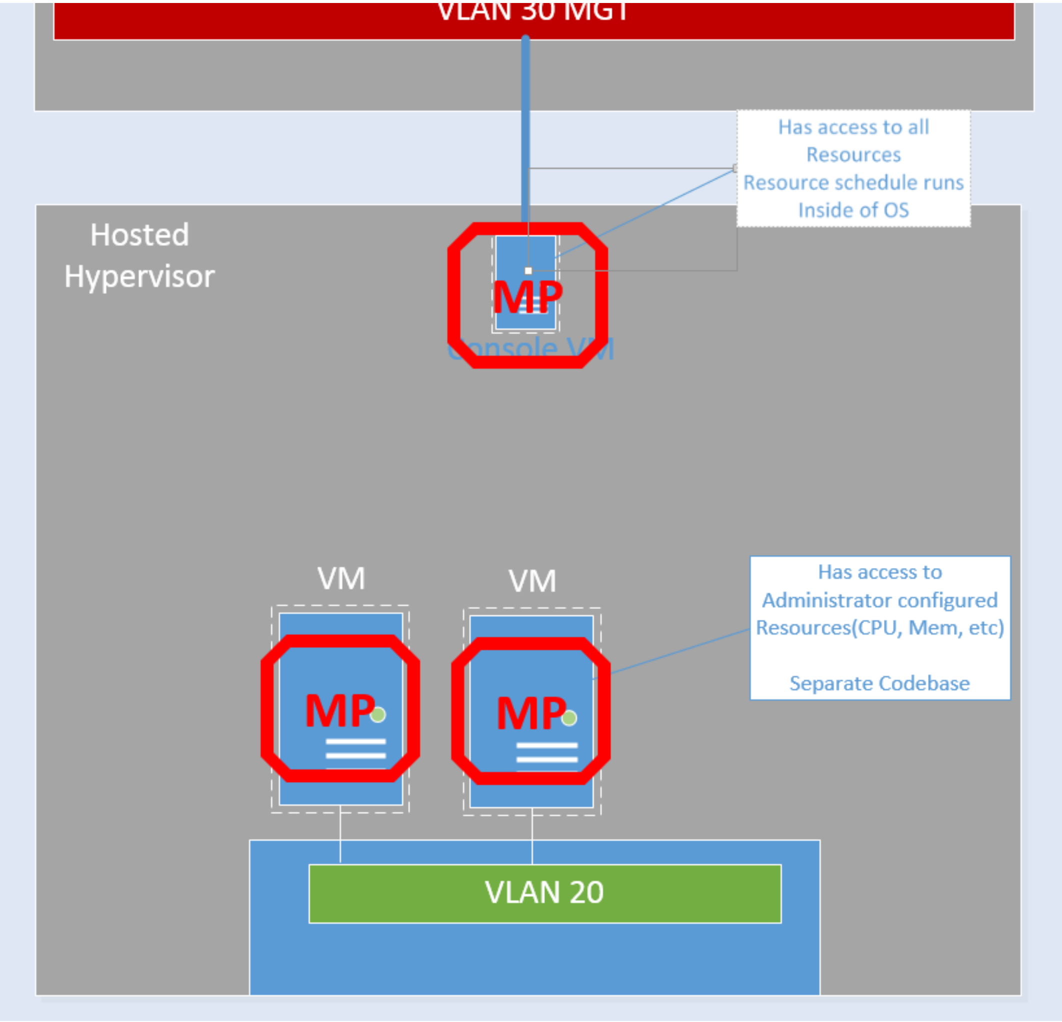
Has access to Administrator configured Resources(CPU, Mem, etc)

Separate Codebase

VM's treated as Software on bare-metal HV: Malware Prevention


VLAN 30 MGT
Has access to configure and to monitor through vendor proprietary mechanism
Has access to all phyiscal Resources(CPU, Mem) and has an Isolated Codebasee
Bare-Metal Hypervisor
MP
Console VM
Resource Scheduler
Has access to a factory provisioned set of resources and Isolated Codebase
VM
VM
MP
MP
Has access to Administrator configured Resources(CPU, Mem, etc)
Separate Codebase
VLAN 20

VM’s treated as Software on Hosted HV: Malware Prevention



Has access to all Resources
Resource schedule runs Inside of OS

Has access to Administrator configured Resources(CPU, Mem, etc)

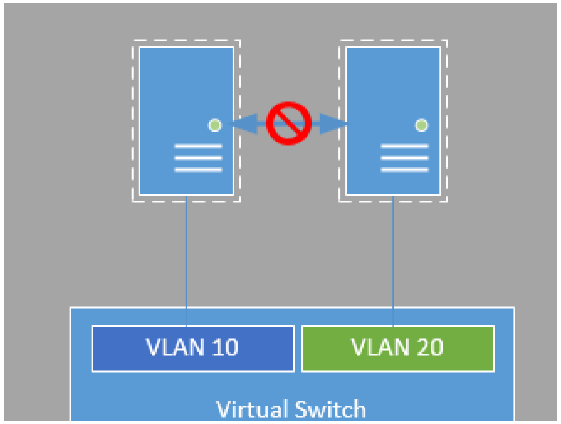
Separate Codebase

Hypervisor : Bare-Metal and Hosted Considerations

- Hypervisors and VM’s should be treated as discrete cyber assets
  - It is difficult to keep proper redundancy strategies in place with hypervisors when treating VM’s as software on the CA
  - Bare-metal hypervisors have strong separation using an independent resource scheduler that prevents malware from accessing the backplane. Hosted platforms do not have this separation and require additional steps to maintain security such as management plane isolation
  - Malware detection considerations need to be applied direction to all operating systems involved. Applying them at the hypervisor is not sufficient to ensure security

Hypervisor Threats

- Because the hypervisor ensures the separation of guests, it needs to be patched regularly:
  - Security patches address ongoing Hypervisor vulnerabilities such as VM escape attacks
  - Hypervisor is a Cyber Asset; afforded same controls including physical security
  - NIST bare-metal hypervisors have a smaller attack surface (SP800-125 chapter 2)
    - Reduced devices drivers
    - Management Plane Separation



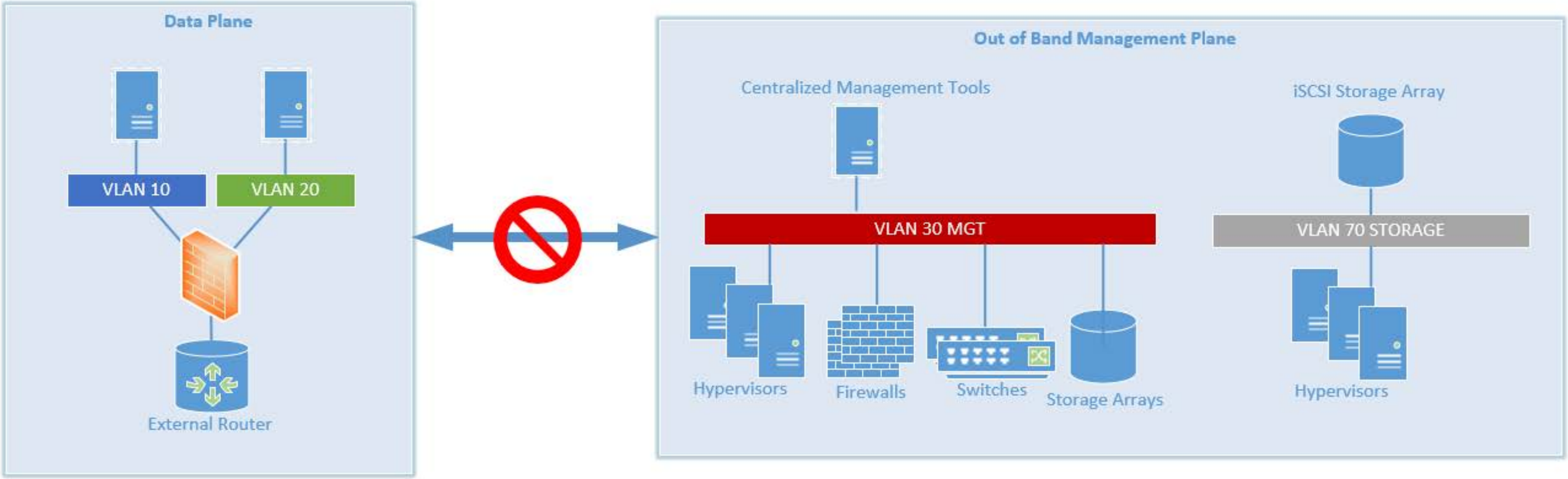
Virtualization Webinar Summary

1. **Hypervisors**
   - Template Considerations
   - Why VM guest need to be treated as PCA's
   - Security Patches address ongoing Hypervisor Vulnerabilities
2. **What is multi-tenancy?**
   - Define Multi-tenancy, Tenants, Overlay, and Underlay
   - Building a multi-tenant environment
   - Introduce ESZ Concept

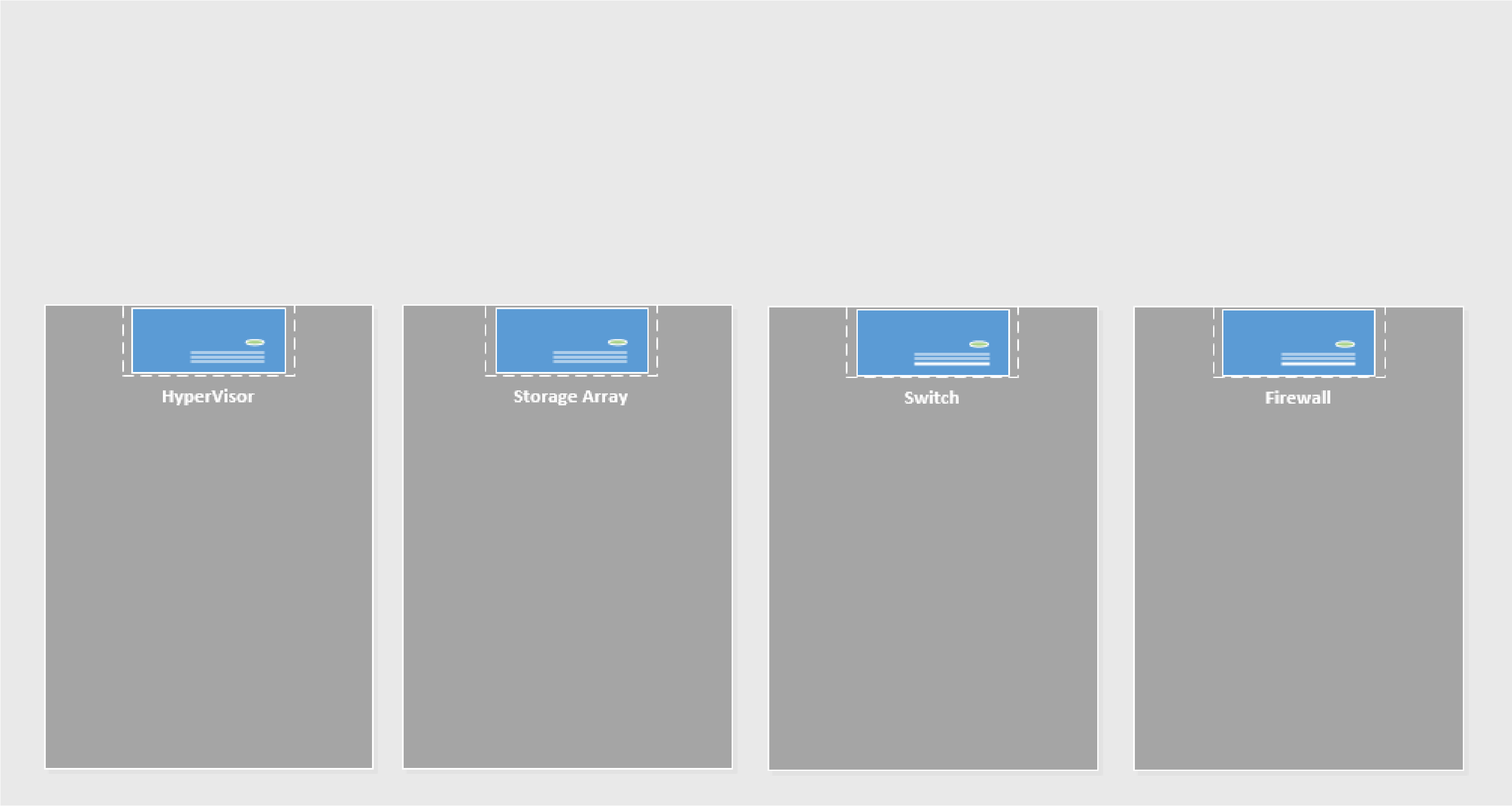
Multi-Tenancy Definitions

- **Multi-Tenancy -** an environment where a shared infrastructure serves multiple tenants.
- **Tenants –**discrete groups of applications, functions, or environments that share a common resource with specific privileges or security levels that consume resources from the shared infrastructure. The instances (Tenants) are logically isolated but physically interconnected.
- **Underlay Network –** A network that supports Overlay Networks. It does not trust the overlay network.
- **Overlay Network –** A network utilized by Tenant. It is unaware that the underlay network exists.
- **Centralized Management System -** A centralized system for administration or configuration of BES Cyber Systems, including but not limited to systems management, network management, storage management or patch management

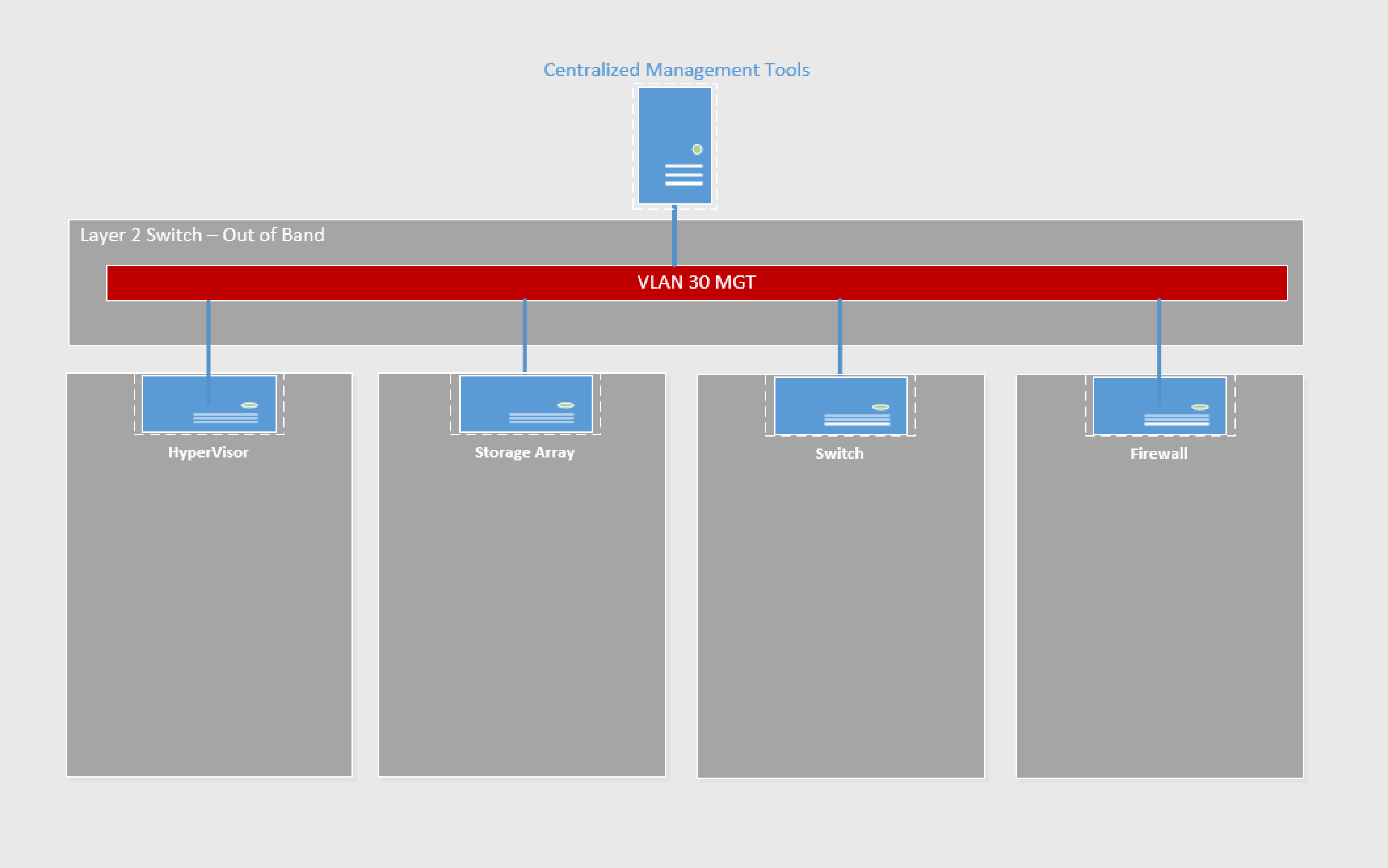
Multi-Tenancy: Management and Data Plane Isolation



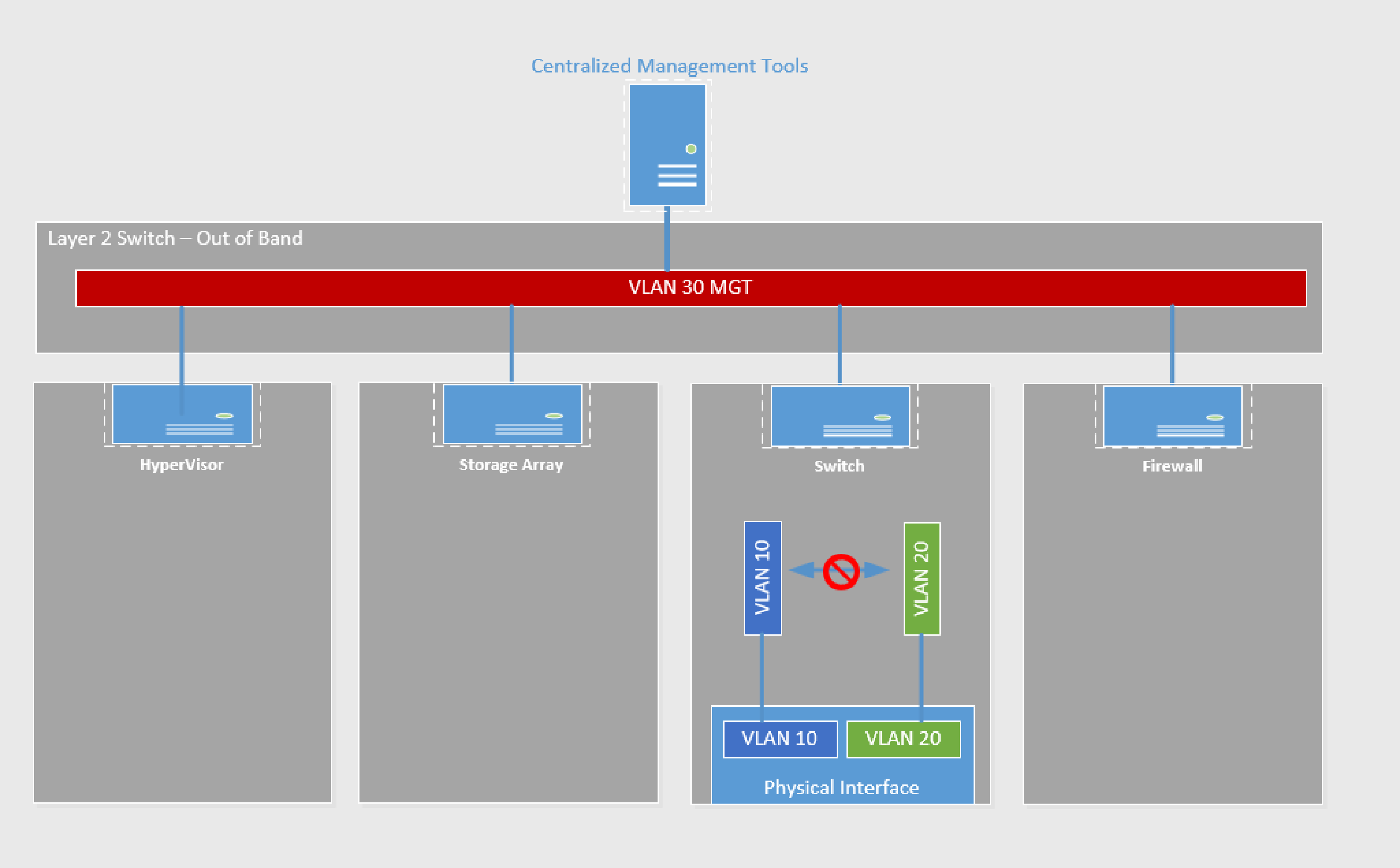
Multi-Tenancy: Basic Physical Devices



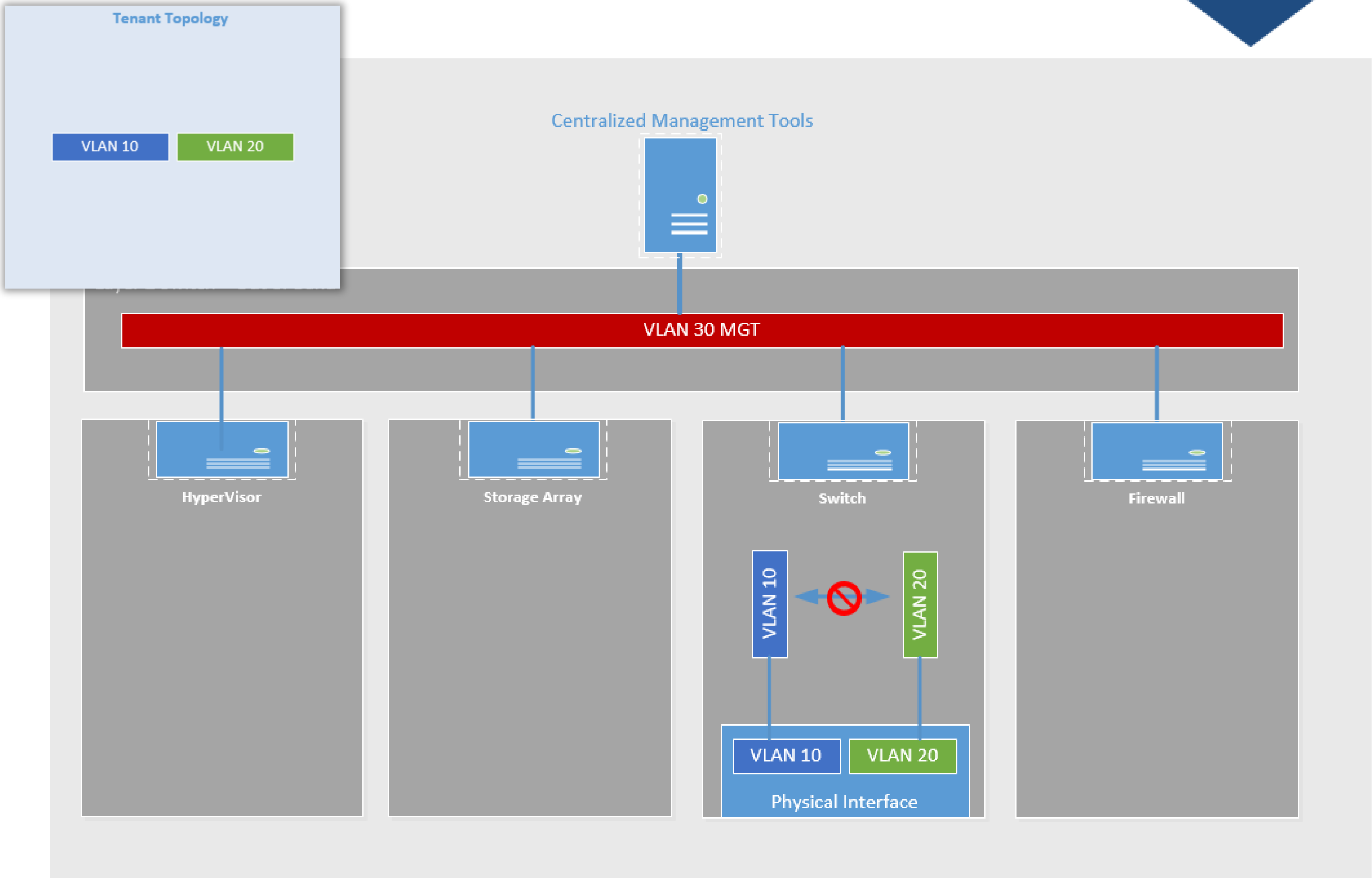
Multi-Tenancy: Centralized Management Systems



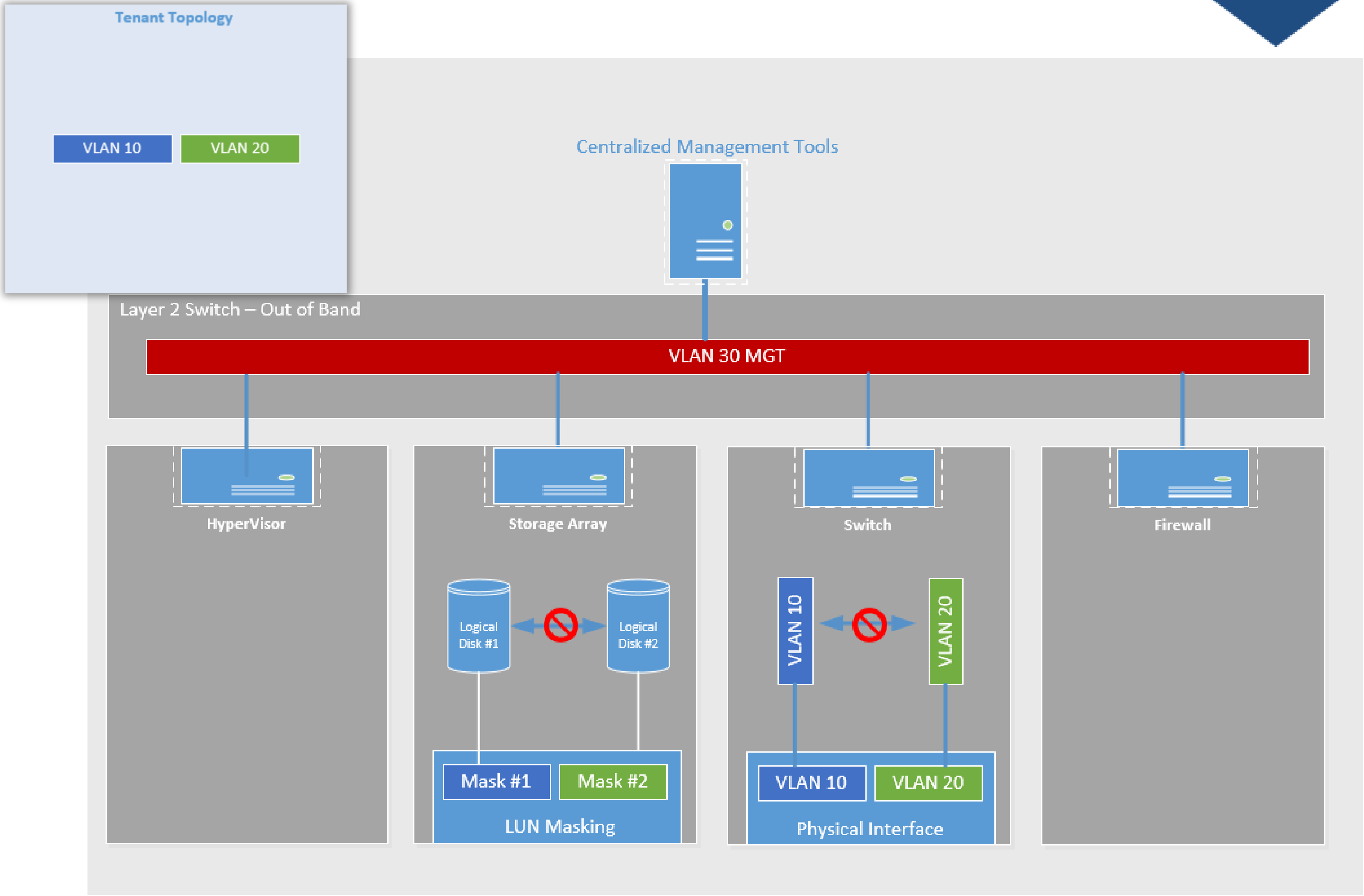
Multi-Tenancy : Adding Tenant Networks



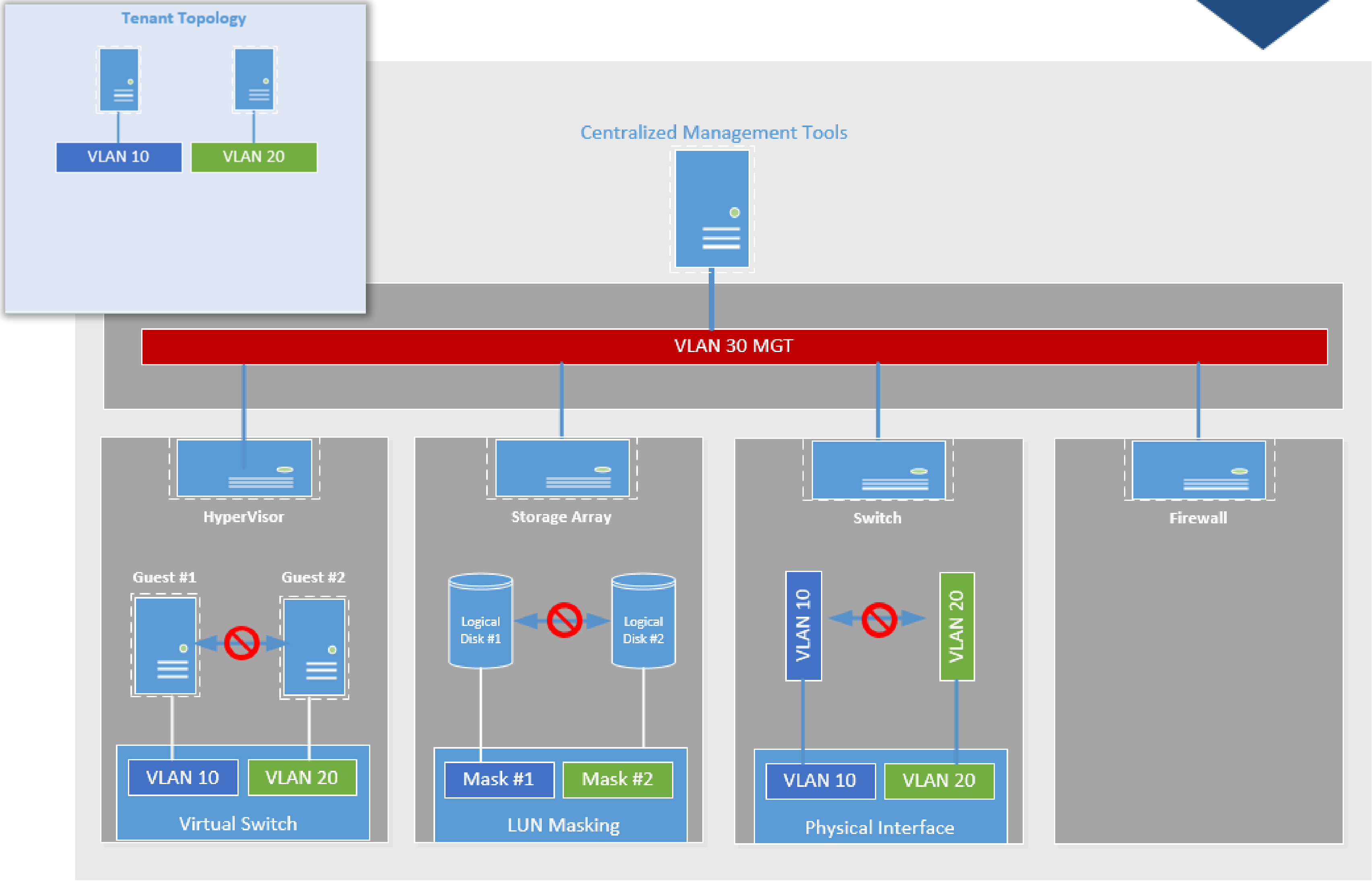
Multi-Tenancy : Adding Tenant Networks



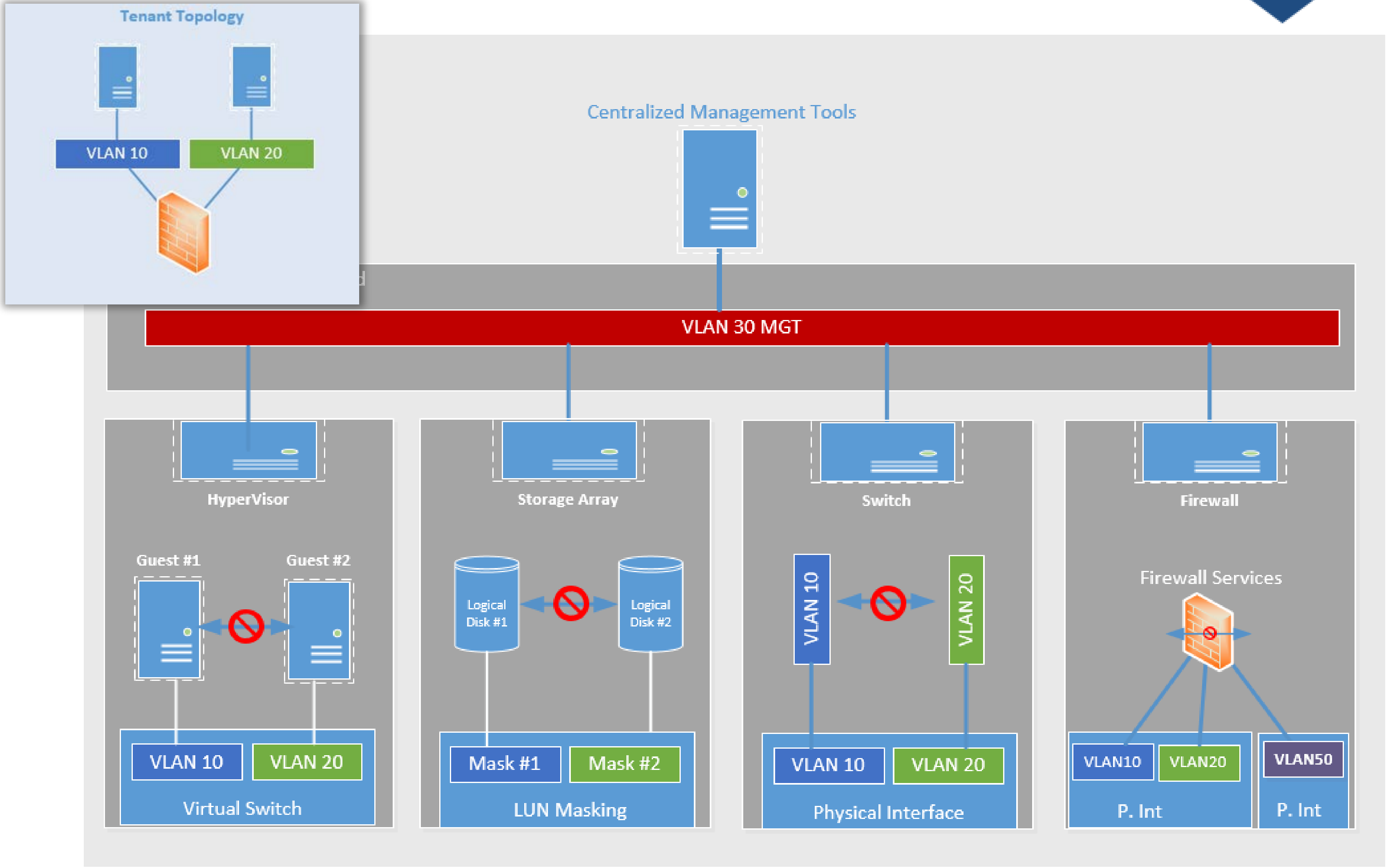
Multi-Tenancy : Add Some Storage



Multi-Tenancy : Add some VM's



Multi-Tenancy : Add a Firewall



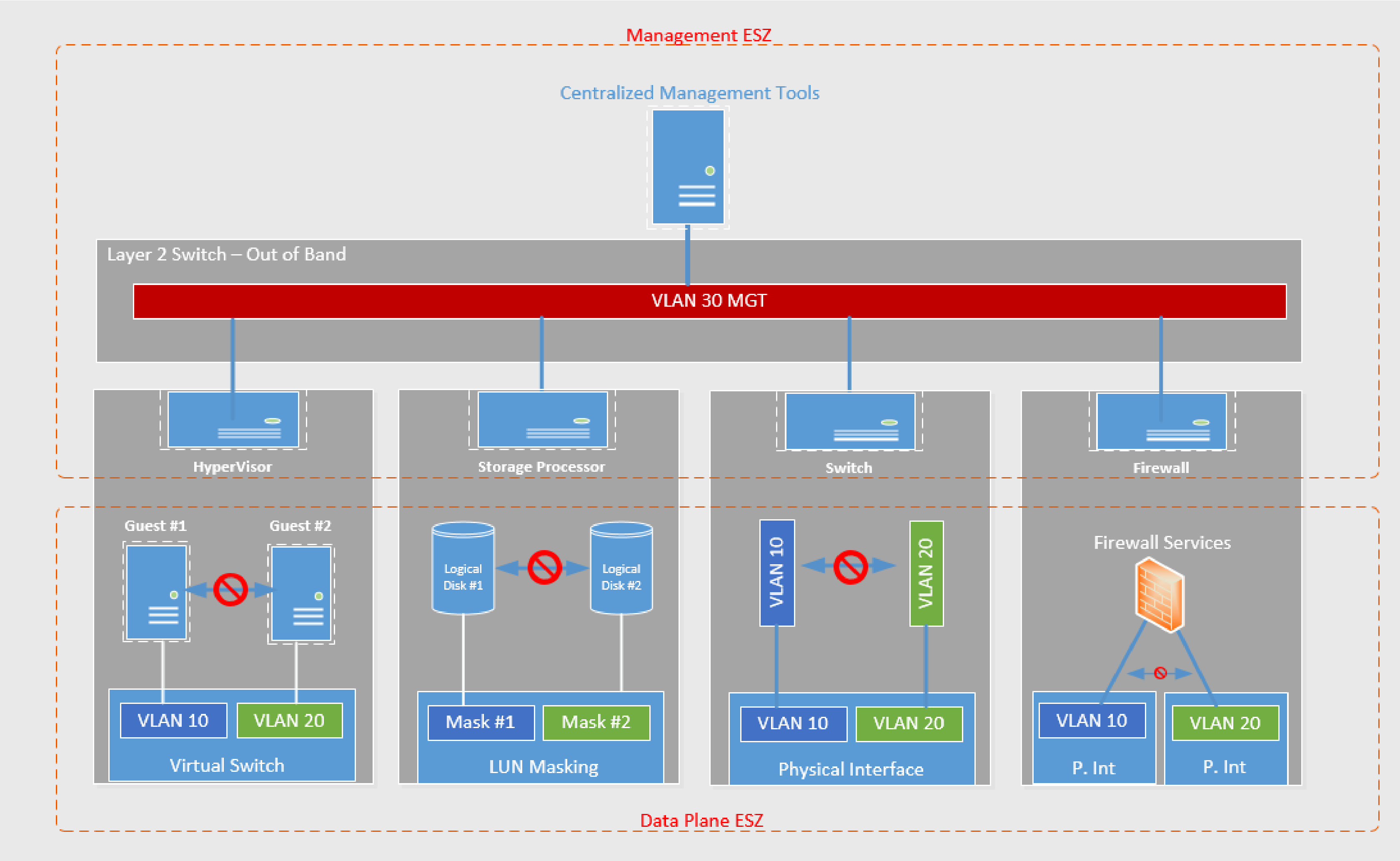
Multi-Tenancy: Considerations

- Multi-Tenancy Considerations
  - VM Infrastructures are designed to support Multi-Tenancy from the ground up and should be considered to be Multi-Tenant environments even if there is only one Tenant
  - Tenant Systems should not have access to the management plane (Logical Isolation at a minimum, Physical is best)
  - Underlay hardware assumes the highest level of security because it required for all Tenants to perform their functions
  - Tenants “Transit” the Underlay, but have no means of accessing it

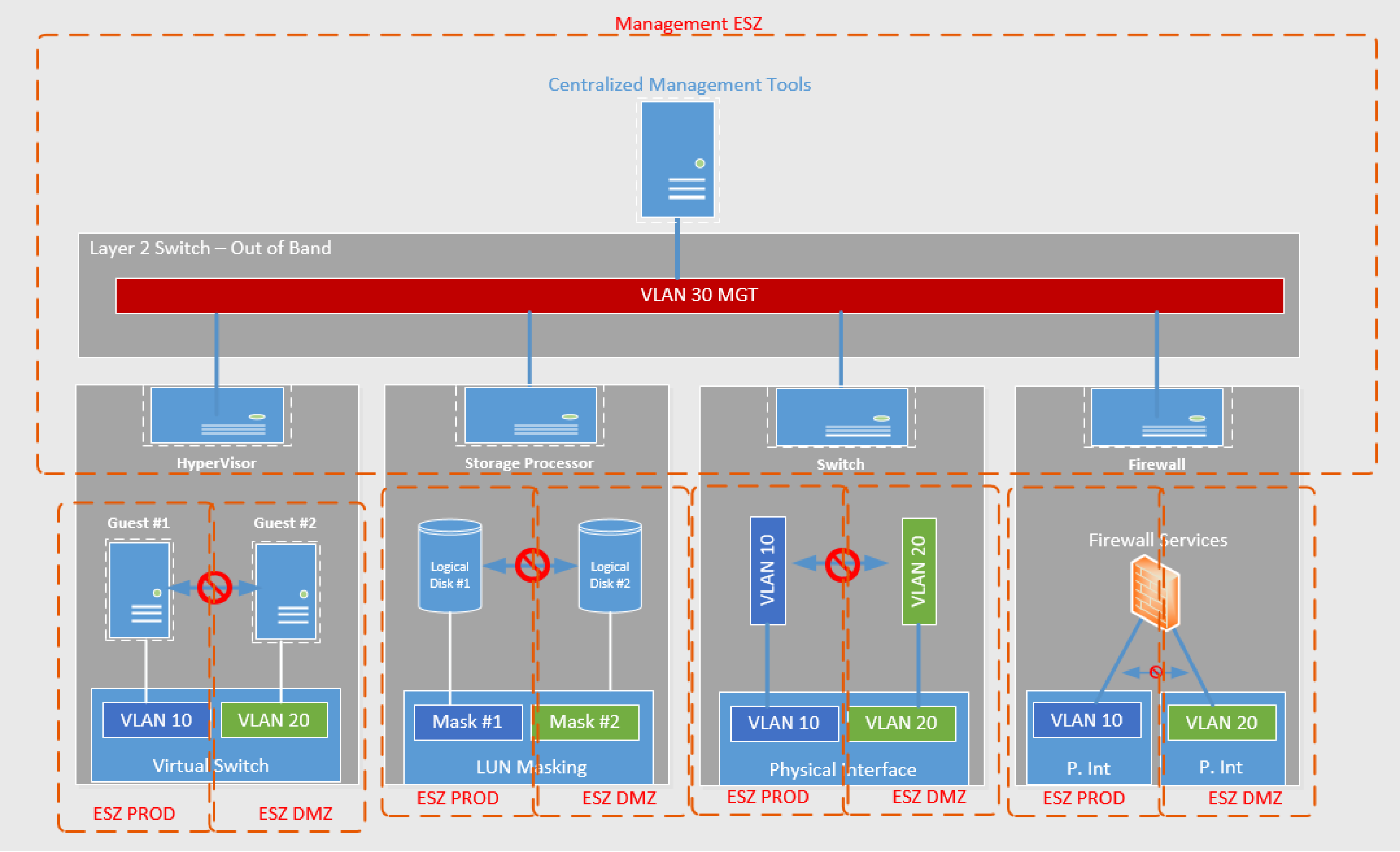
ESZ Concept

- 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

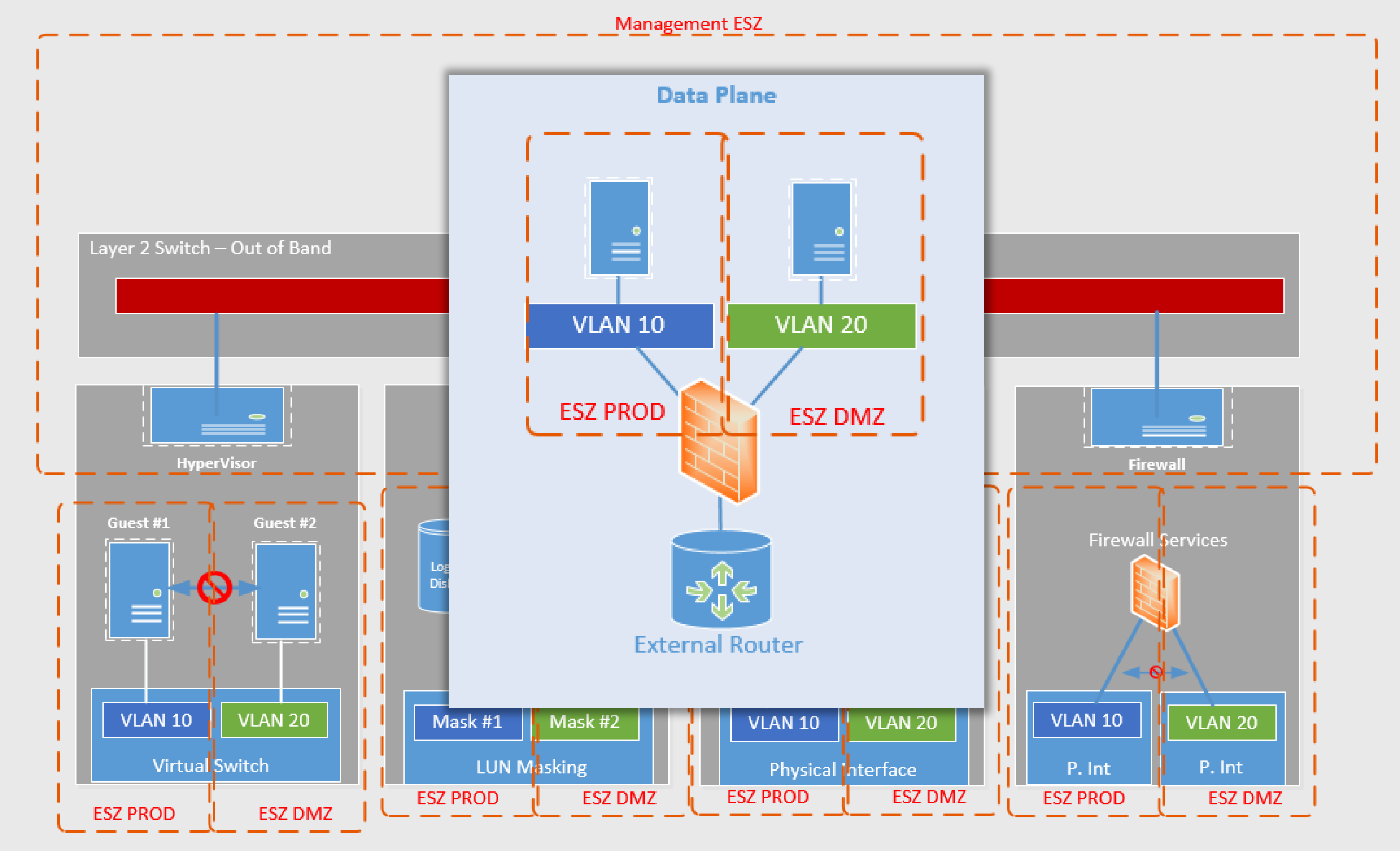
ESZ Example: Management Plane Isolation



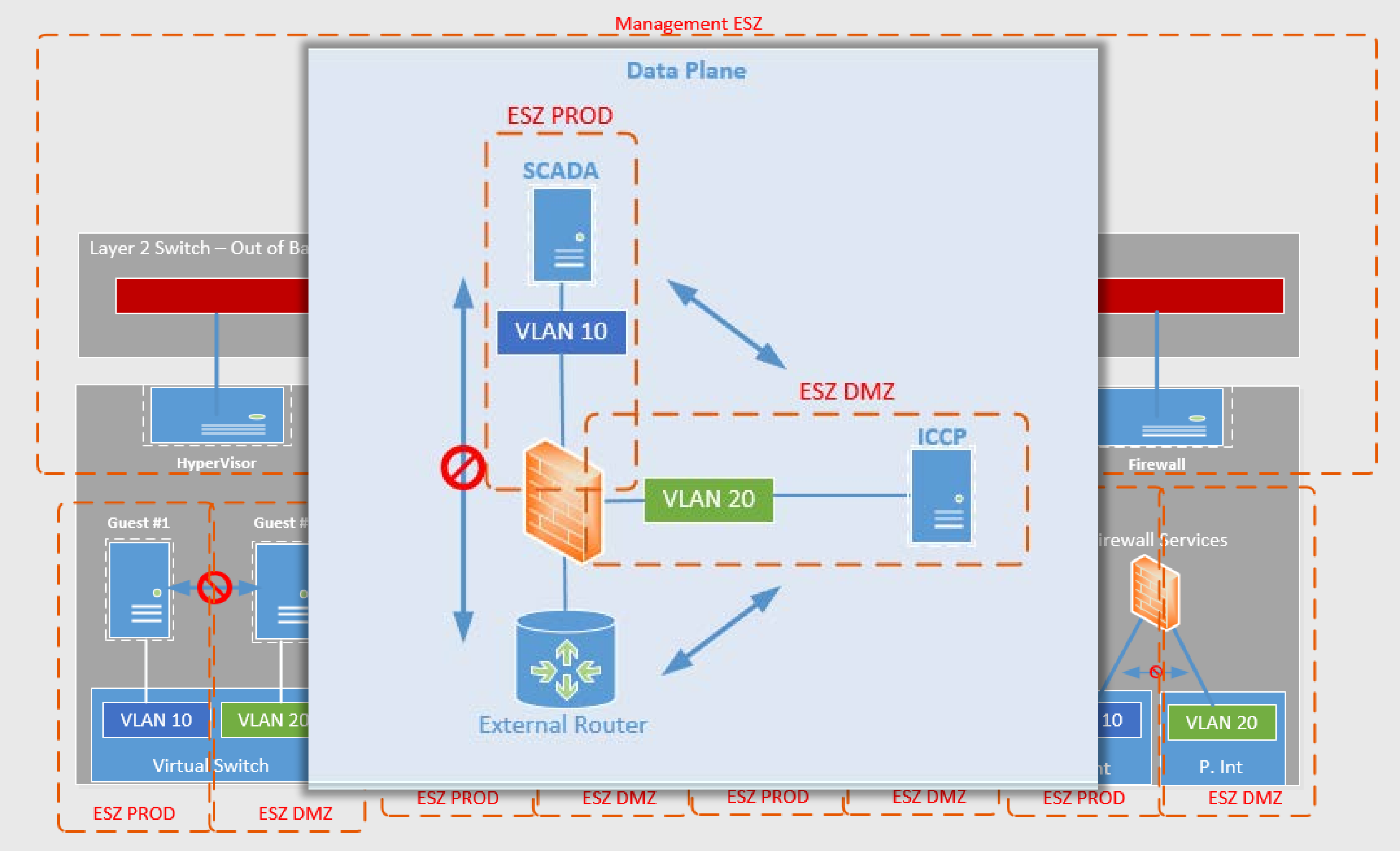
ESZ Example: DMZ Seperation



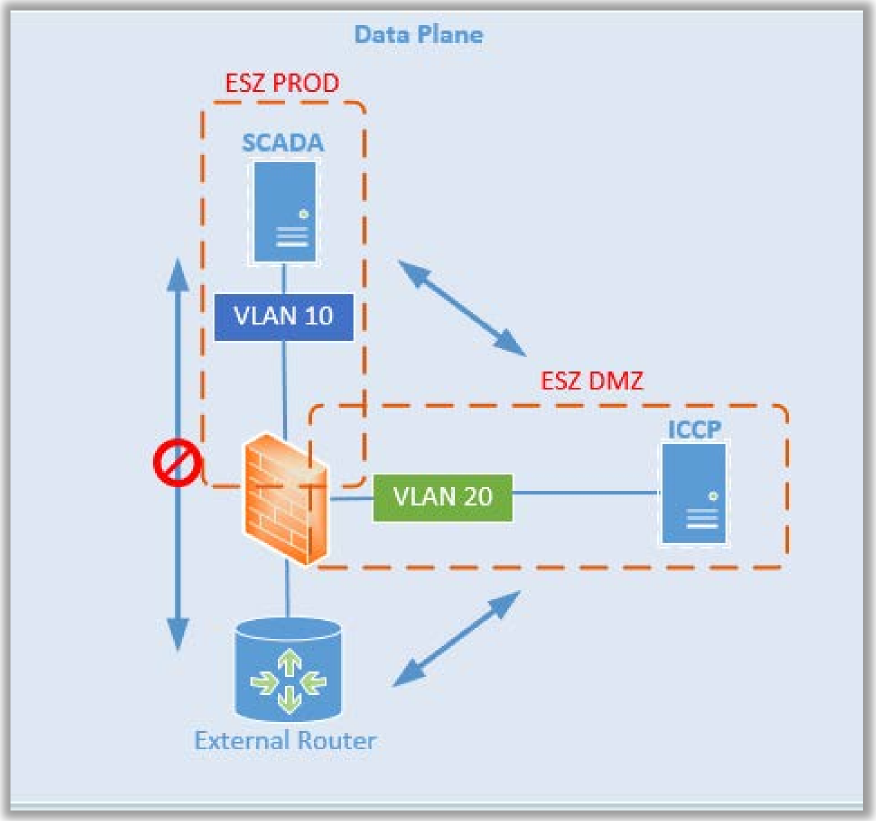
ESZ Example: DMZ Seperation

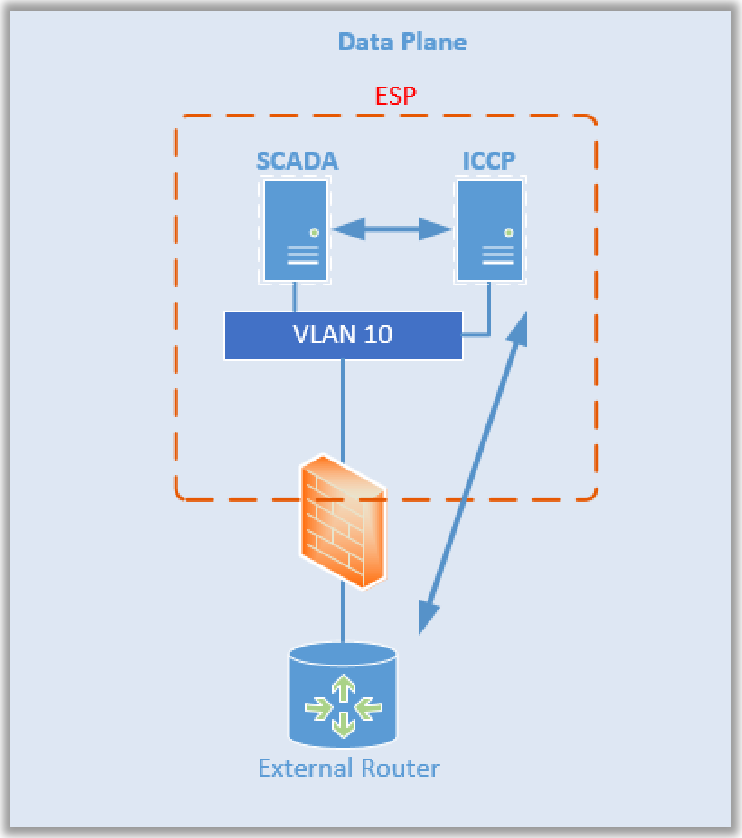


ESZ Example: DMZ Seperation

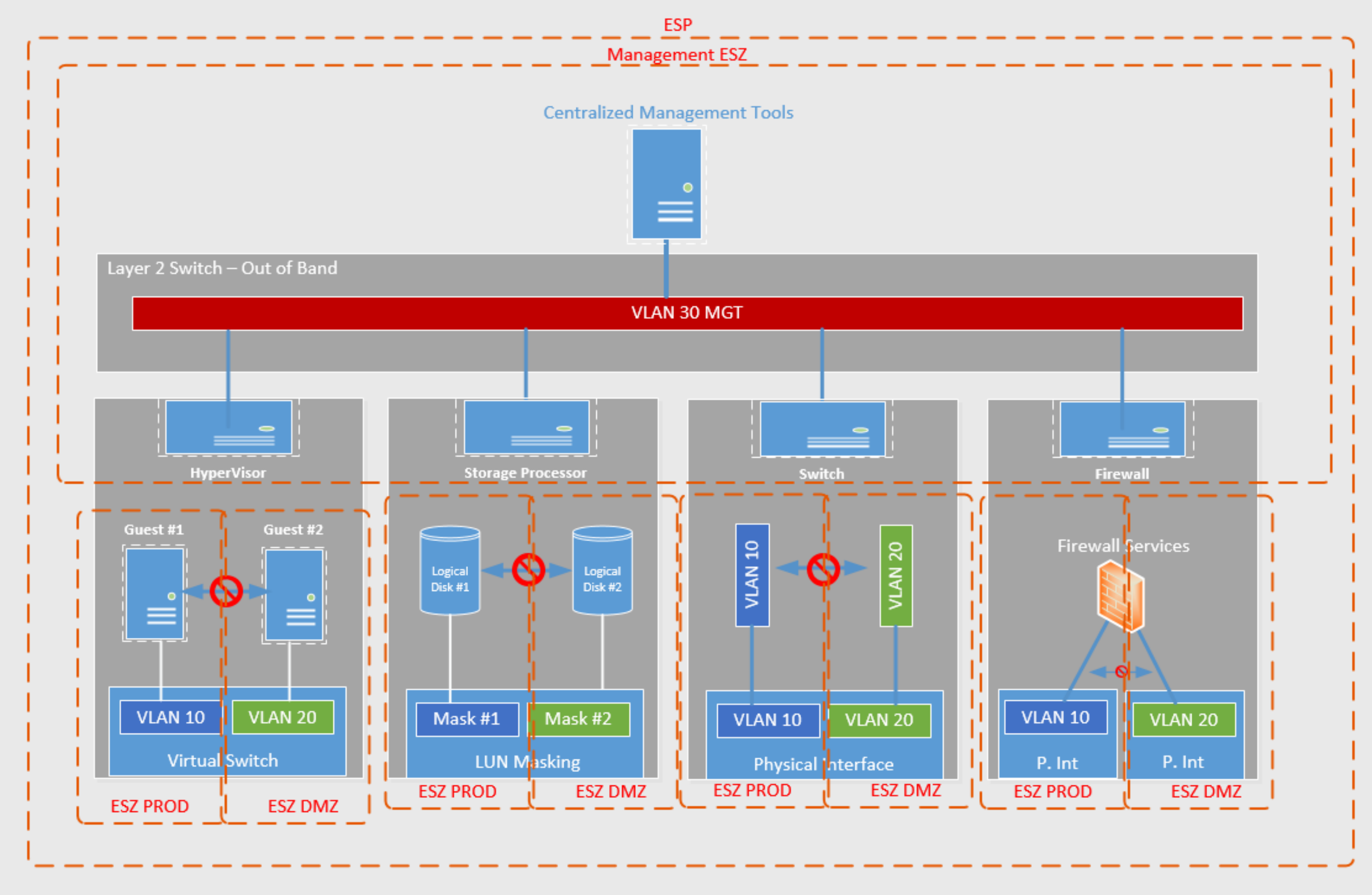


ESZ Example: ESZ vs ESP





ESP and ESZ Interaction?



ESZ Considerations

- 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

Questions and Answers