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

March 21, 2017

RELIABILITY | ACCOUNTABILITY




Agenda

- Administrative Items
  - Antitrust and Disclaimers
  - Webinar Format
- Standard Drafting Team
- Opening Remarks and Introduction of Presenters
- Logical Isolation
- Centralized Management System (CMS)
- Resiliency and Virtual Machines
- 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.

Drafting Team Scope

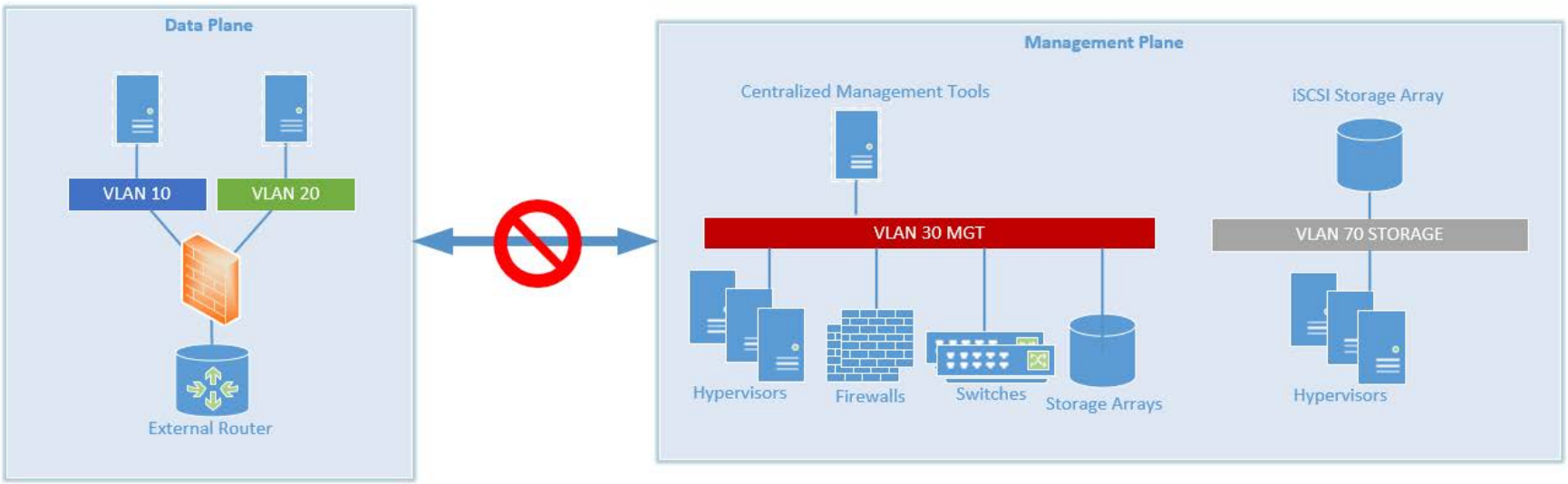
Issue Area	Source	Status
LERC definition	Order 822	Completed
Transient devices for low impact	Order 822	Completed
Communication between BES Control Centers	Order 822	Development in progress
Cyber Asset and BES Cyber Asset Definitions	V5TAG	Development in progress
Network and Externally Accessible Devices	V5TAG	Development in progress
Transmission Owner (TO) Control Centers	V5TAG	Posted for informal comment
Virtualization	V5TAG	Posted for informal comment
CIP Exceptional Circumstances	SAR	Development in progress
“Shared BES Cyber Systems” in CIP-002-5.1a	EnergySec RFI	Completed

Presenters

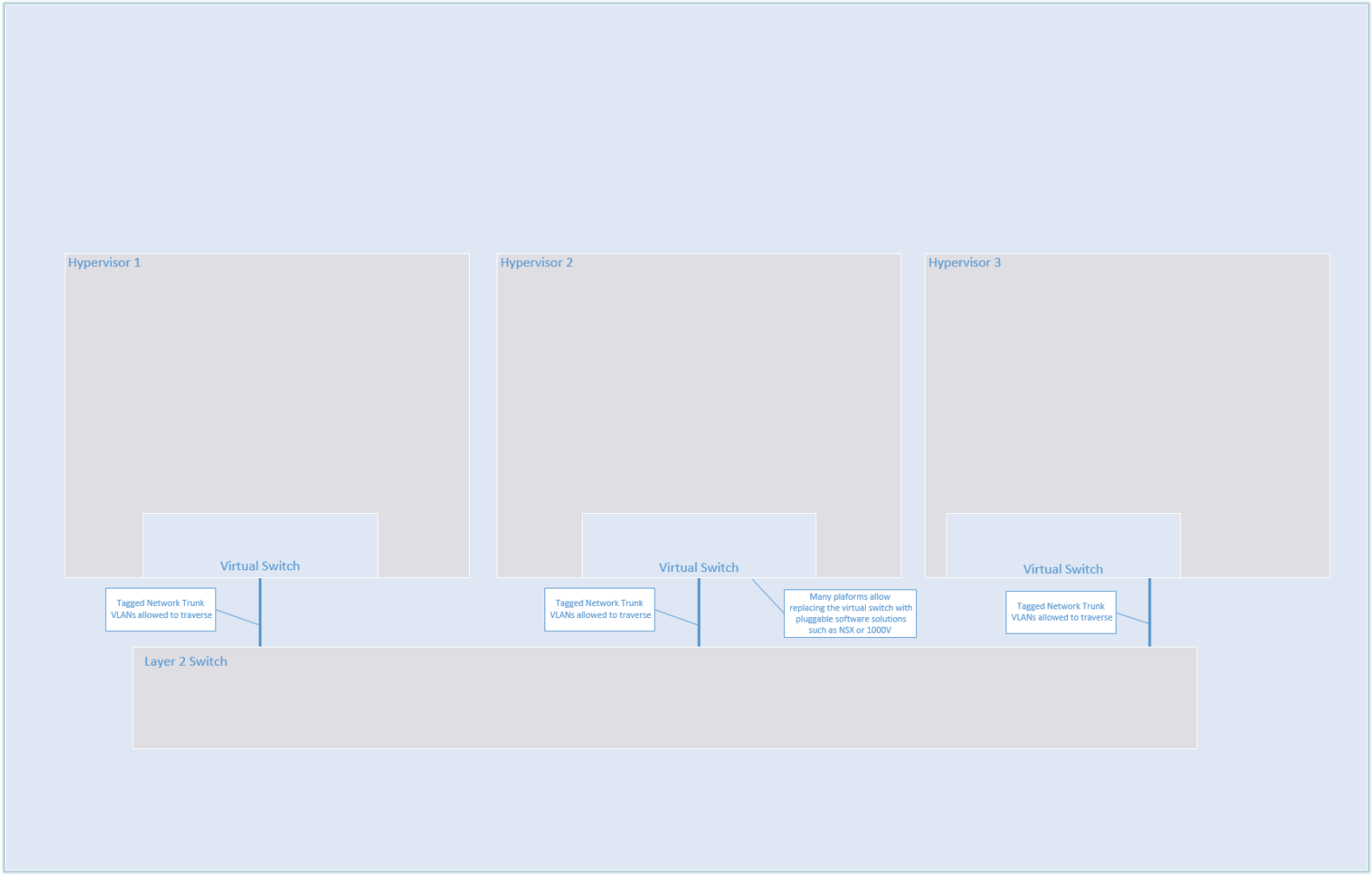
- Christine Hasha – Electric Reliability Council of Texas (ERCOT)
- Philippe Labrosse – Hydro-Québec TransÉnergie
- Forrest Krigbaum – Bonneville Power Administration
- Matthew Hyatt – Tennessee Valley Authority (TVA)
- Larry Good – ACT-1 Group

Logical Isolation

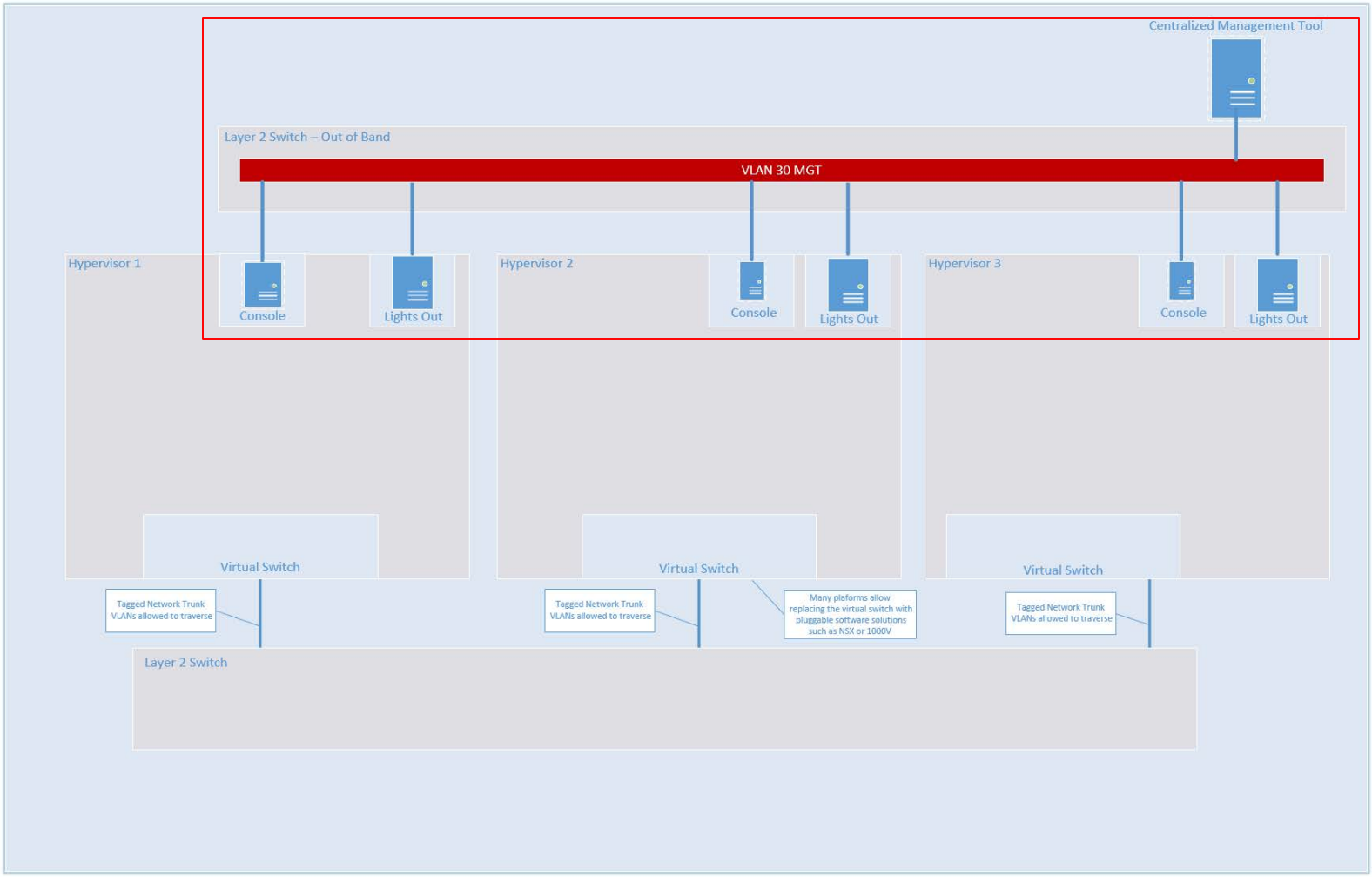
Data / Management Plane Isolation



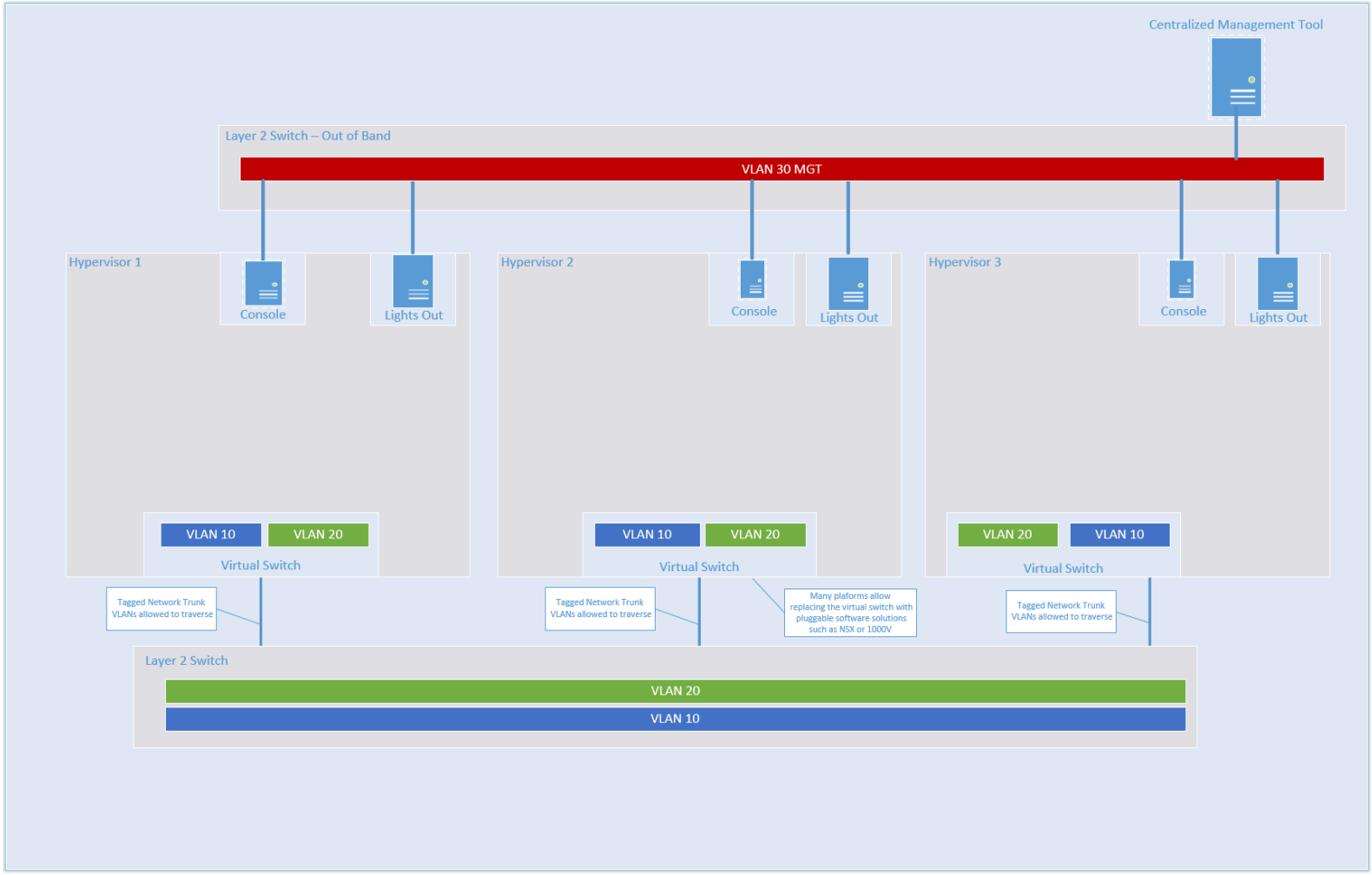
Basic Virtualization Platform



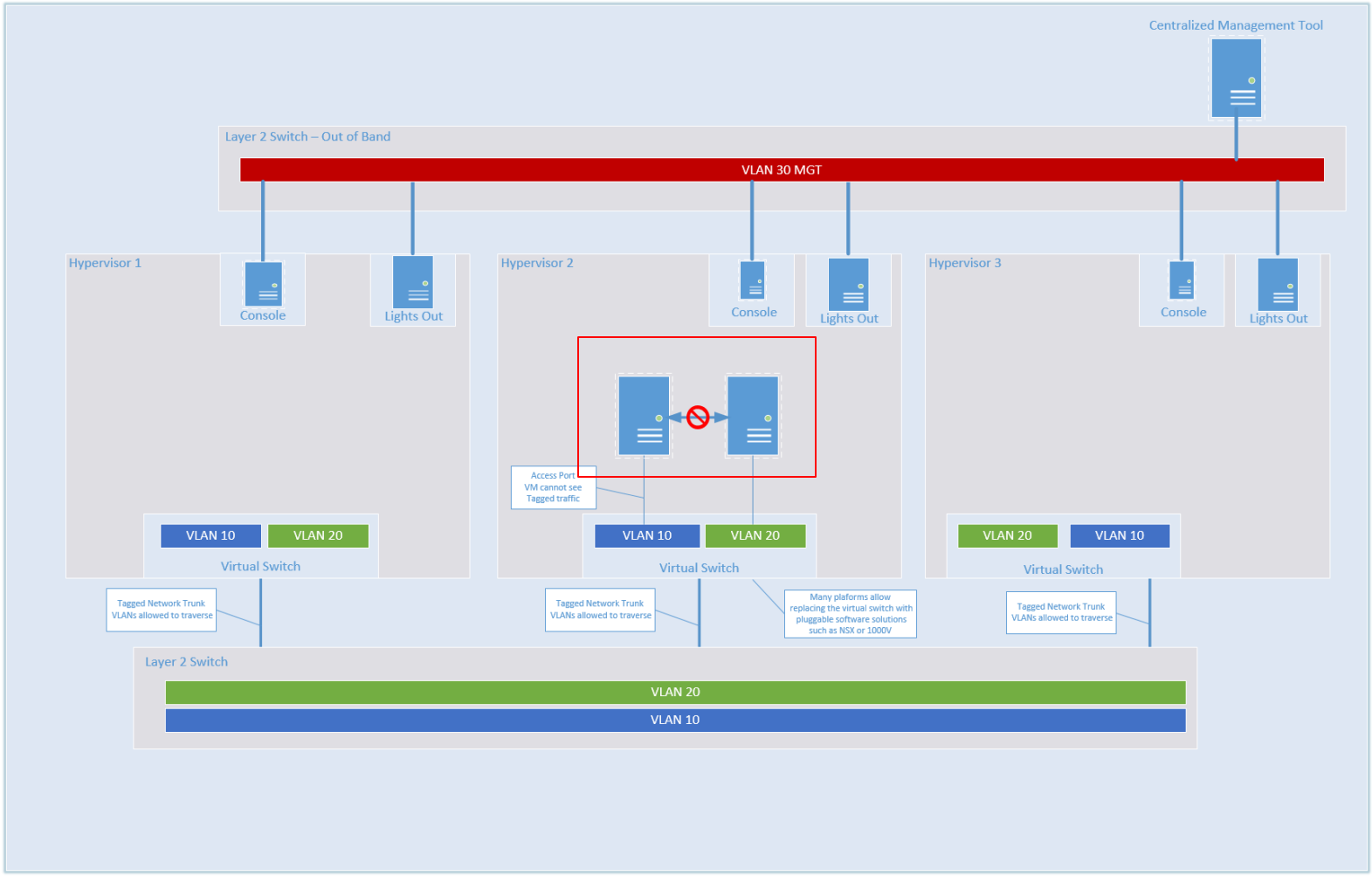
Add Centralized Management



Add Virtual Local Area Networks (VLANs)



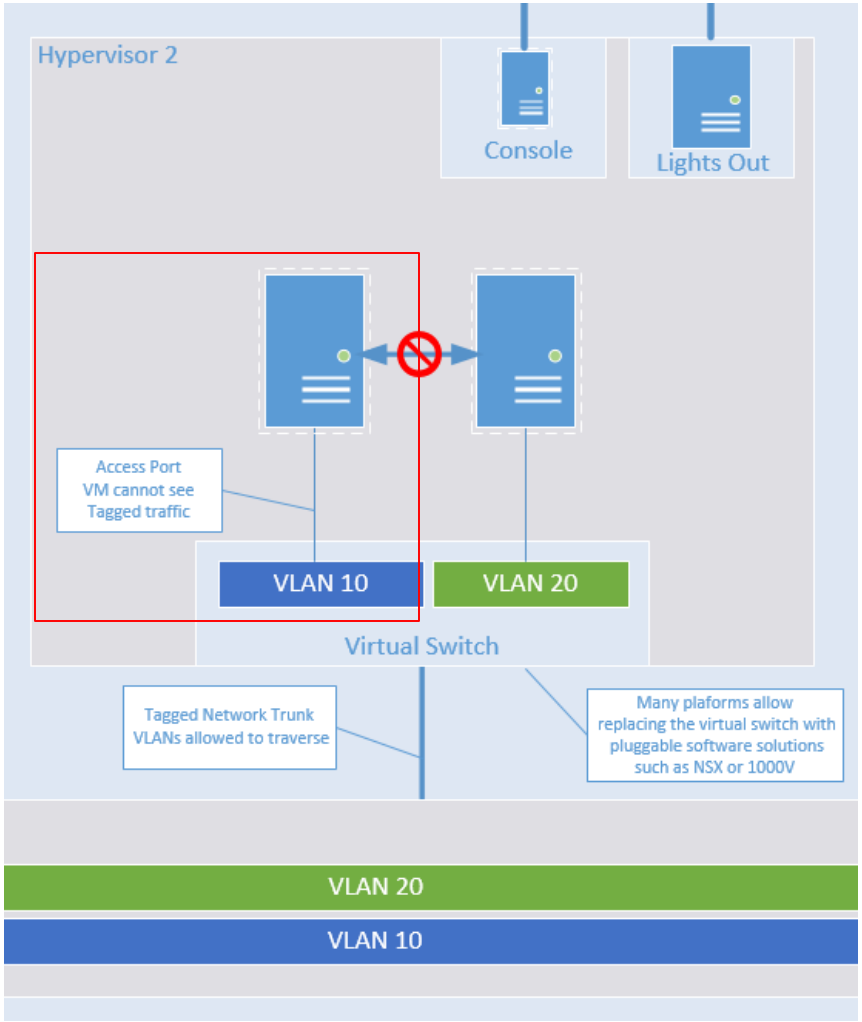
Add Virtual Machines (VMs)



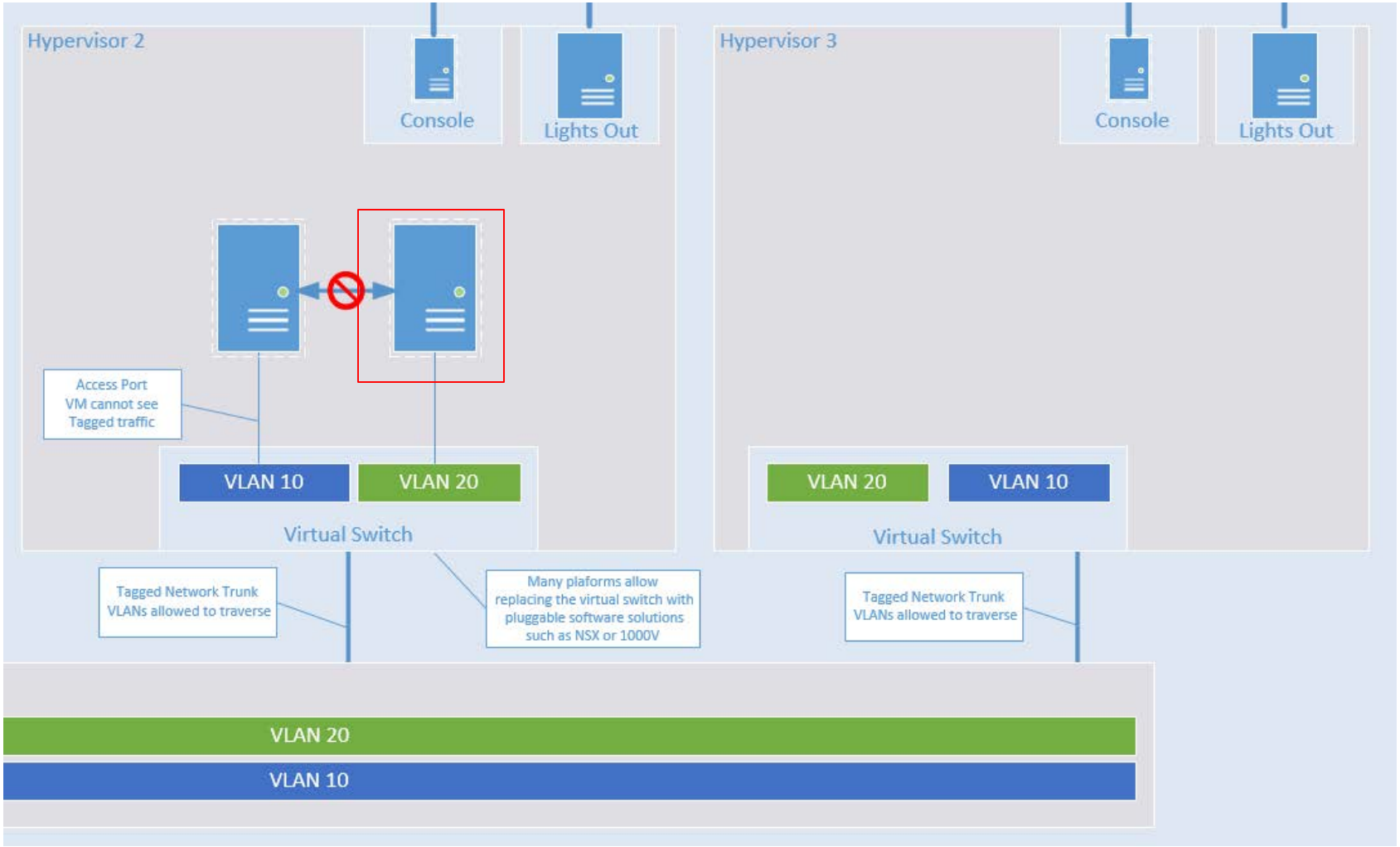
Centralized Management System (CMS)

- The proposed Centralized Management System (CMS) definition is:
  - 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.

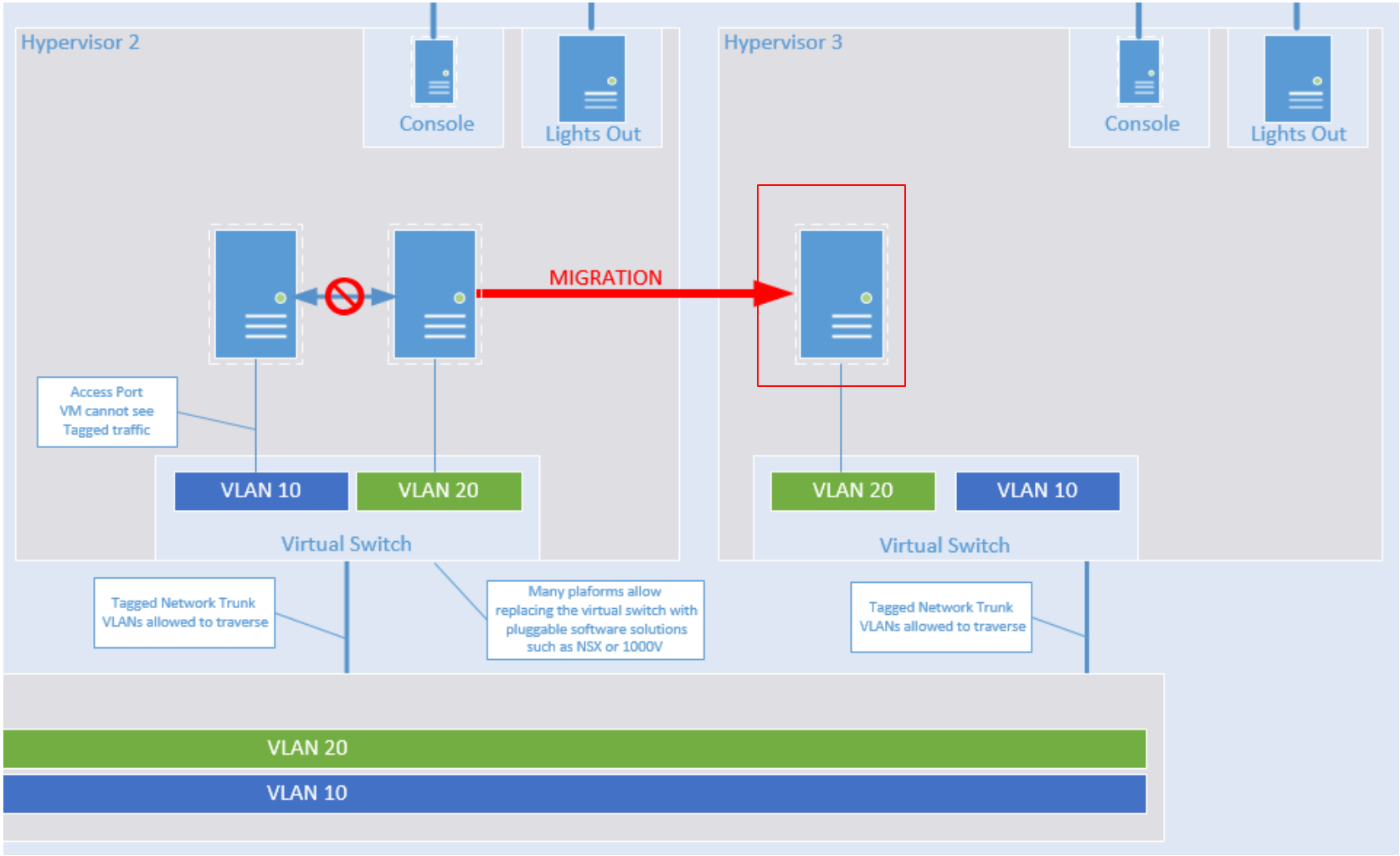
VMs cannot see Tagged Traffic (Q5)



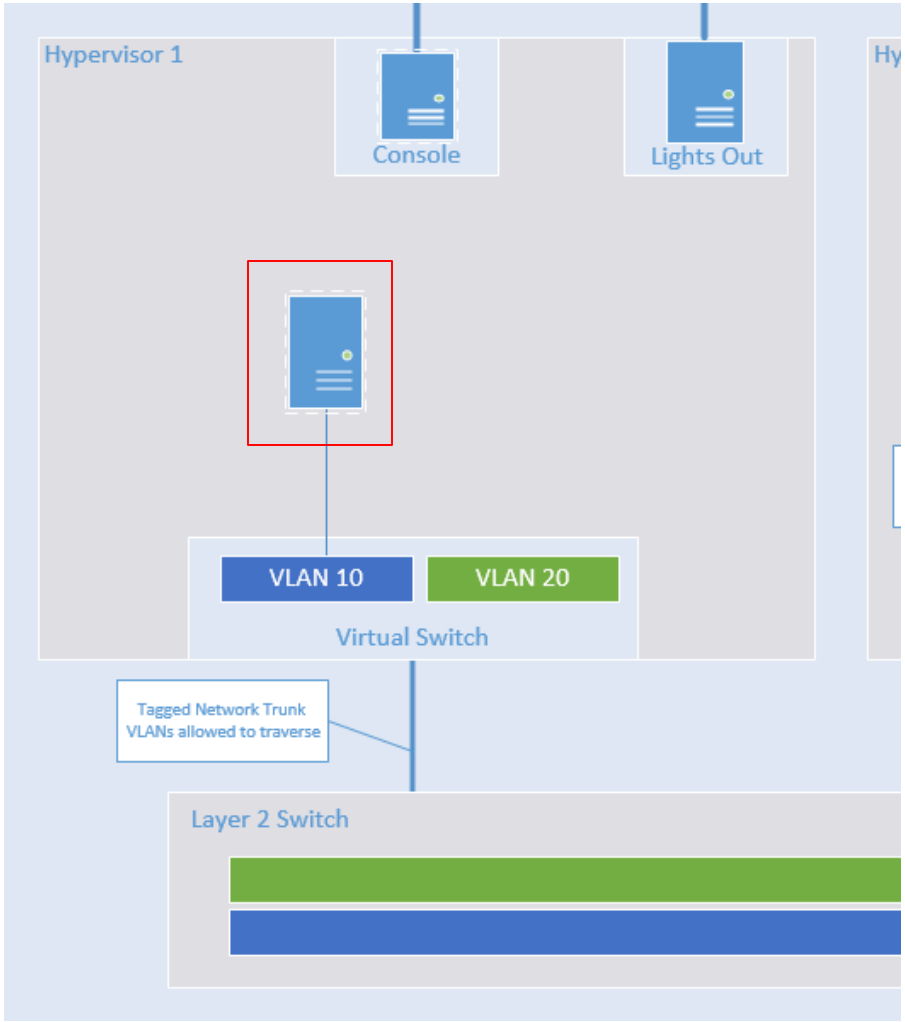
VMs are Mobile



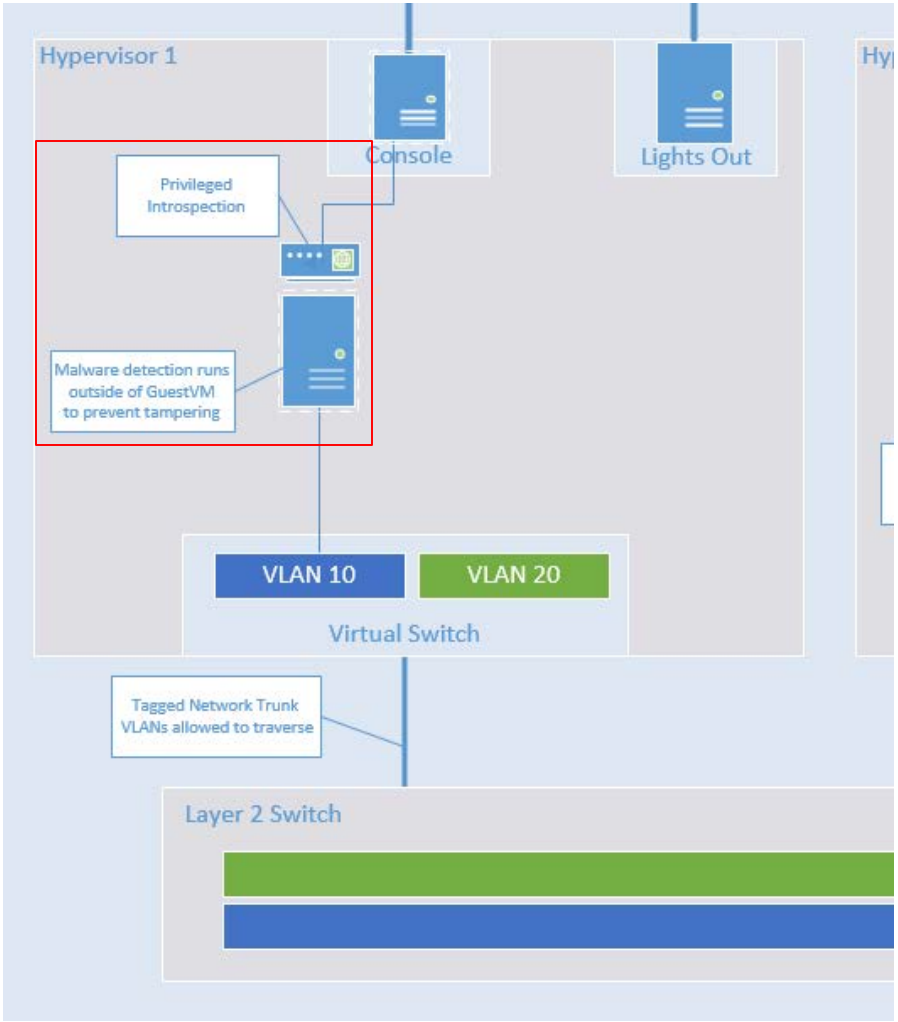
VMs are Mobile



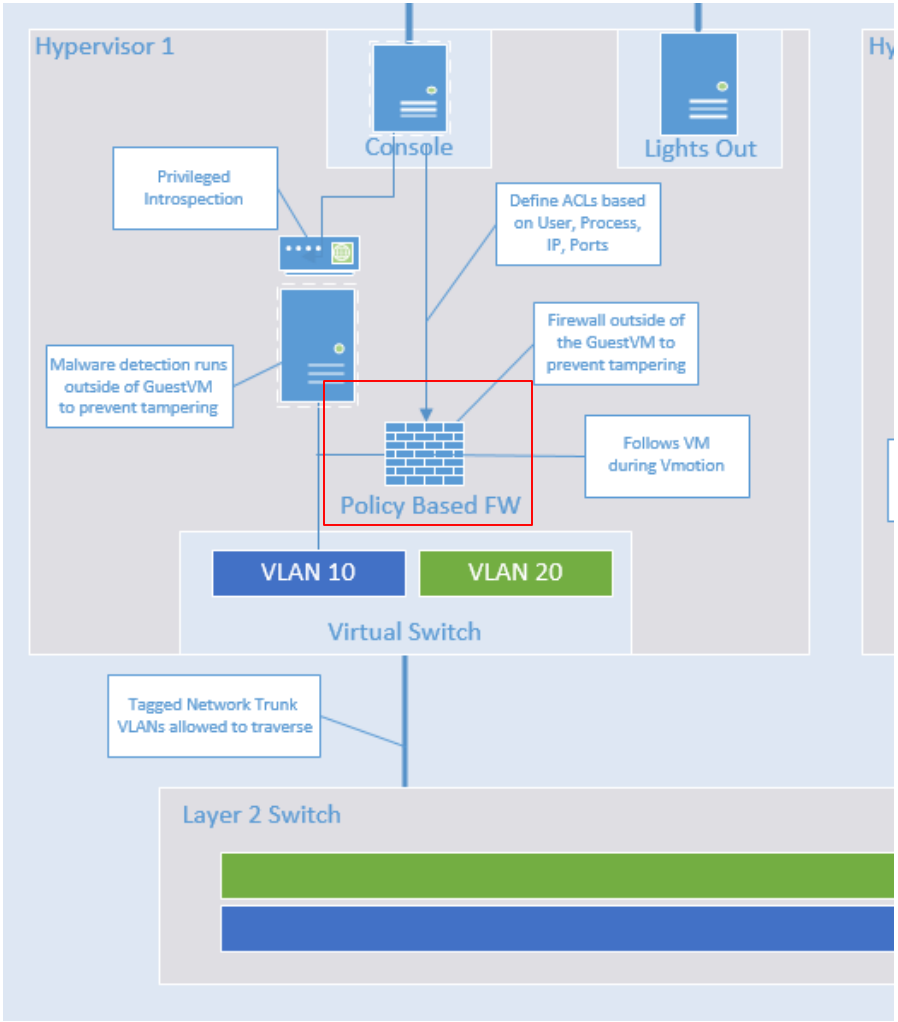
Introspection: Malware Detection



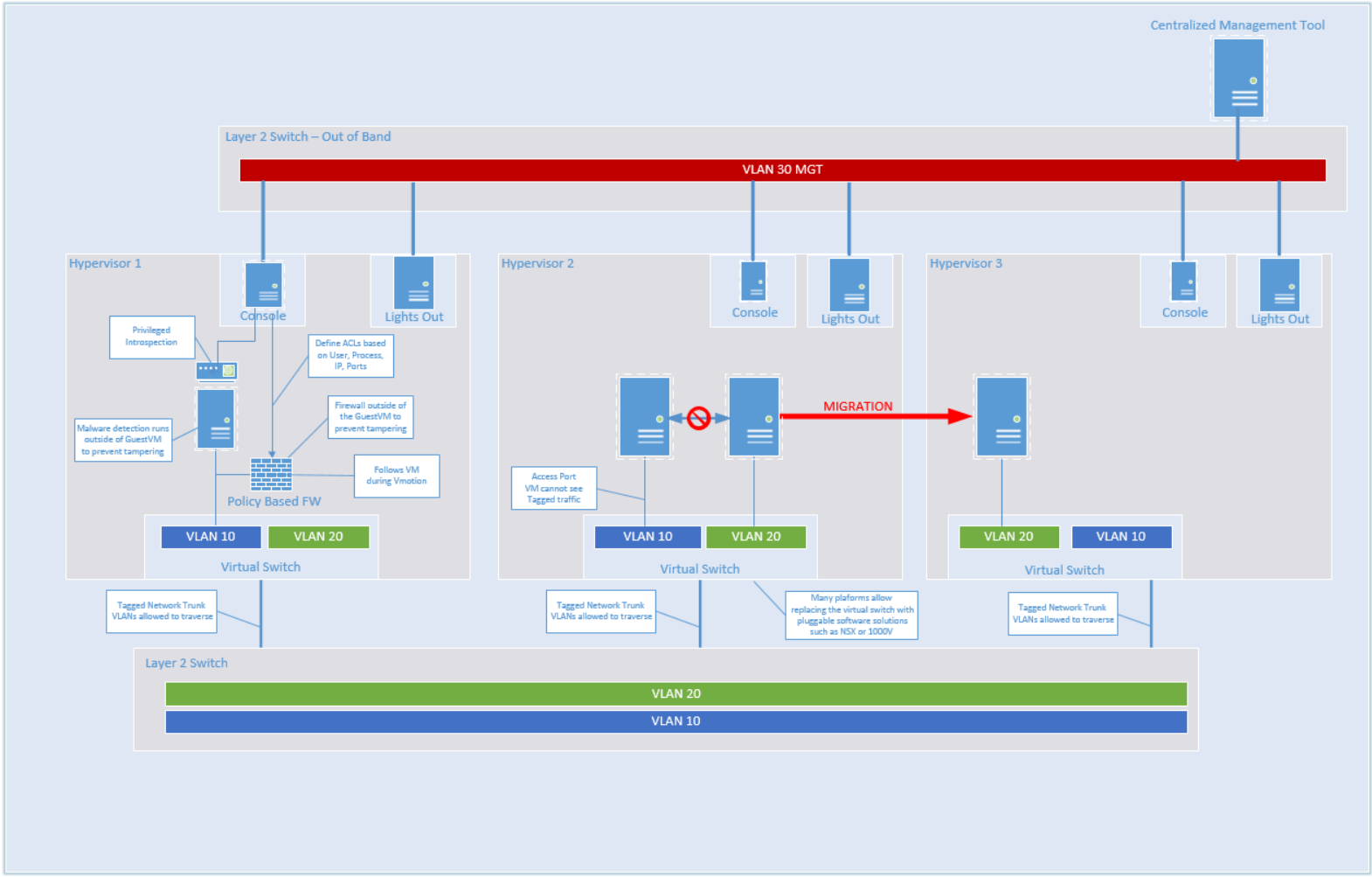
Introspection: Malware Detection



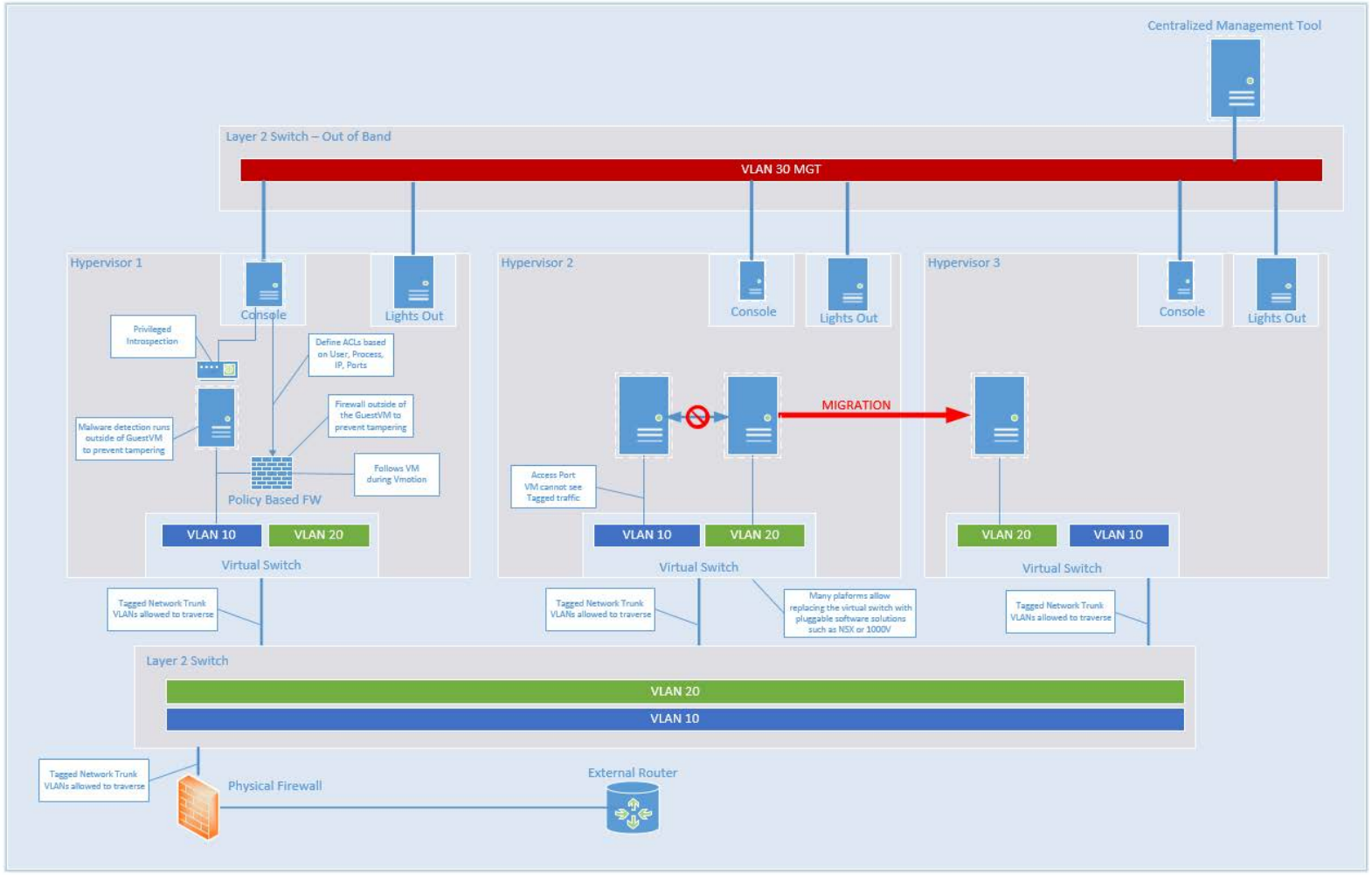
Policy Based Firewalling



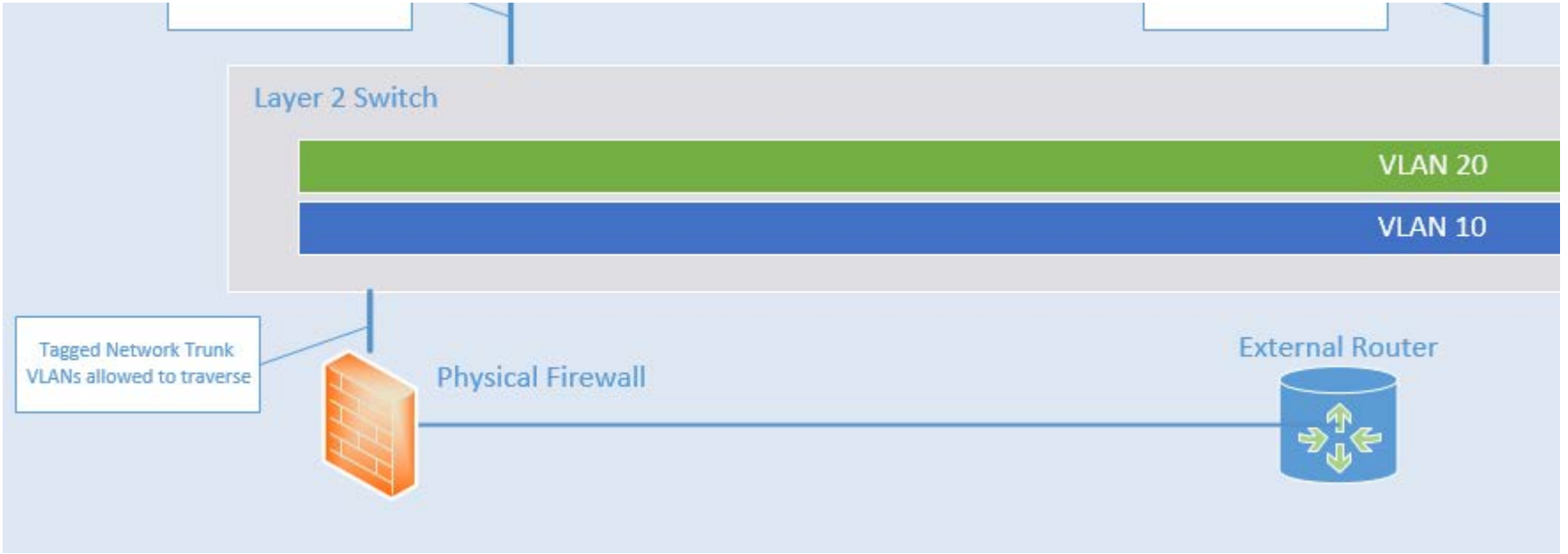
Topology Overview



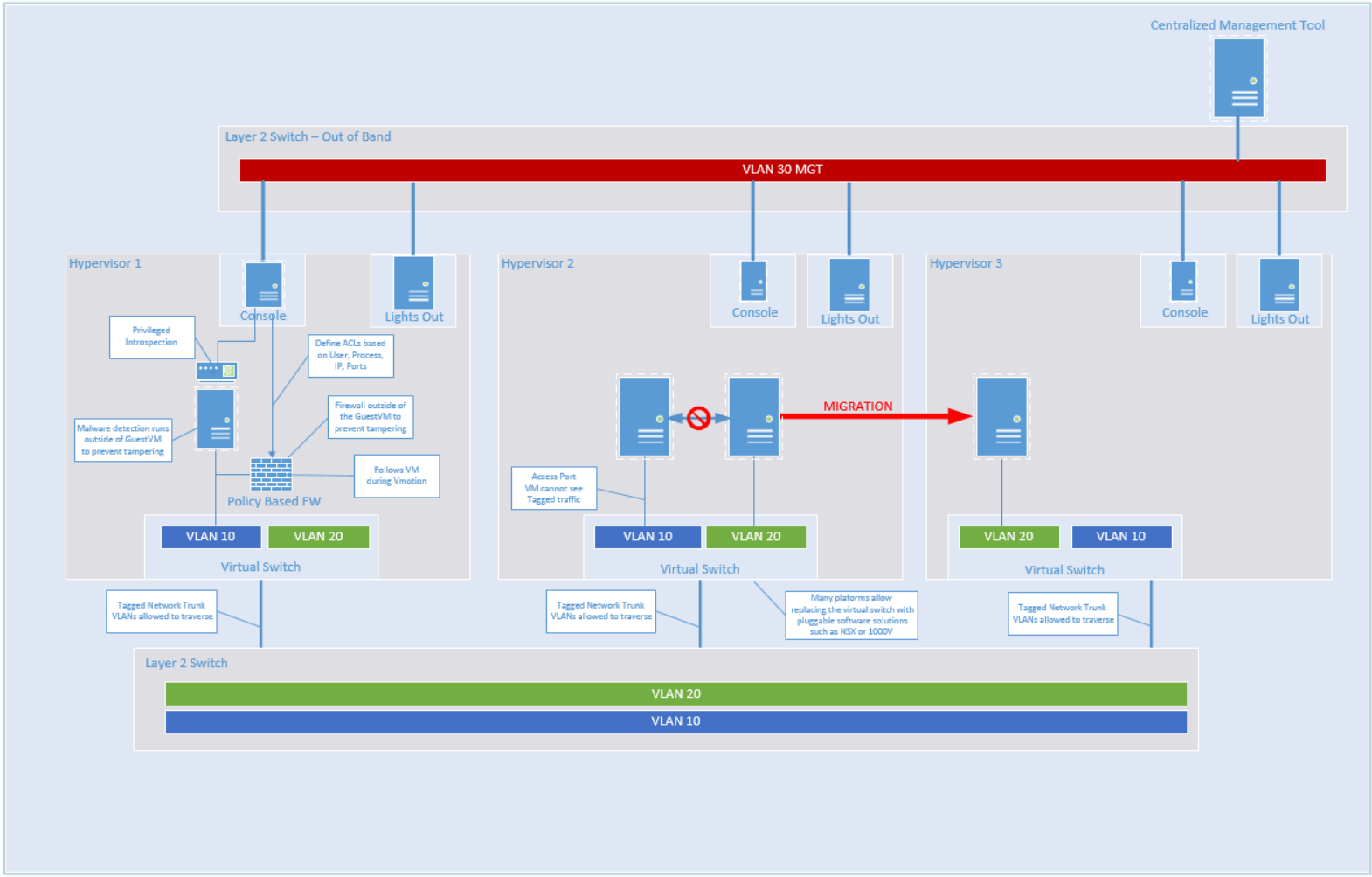
Add a Physical Firewall



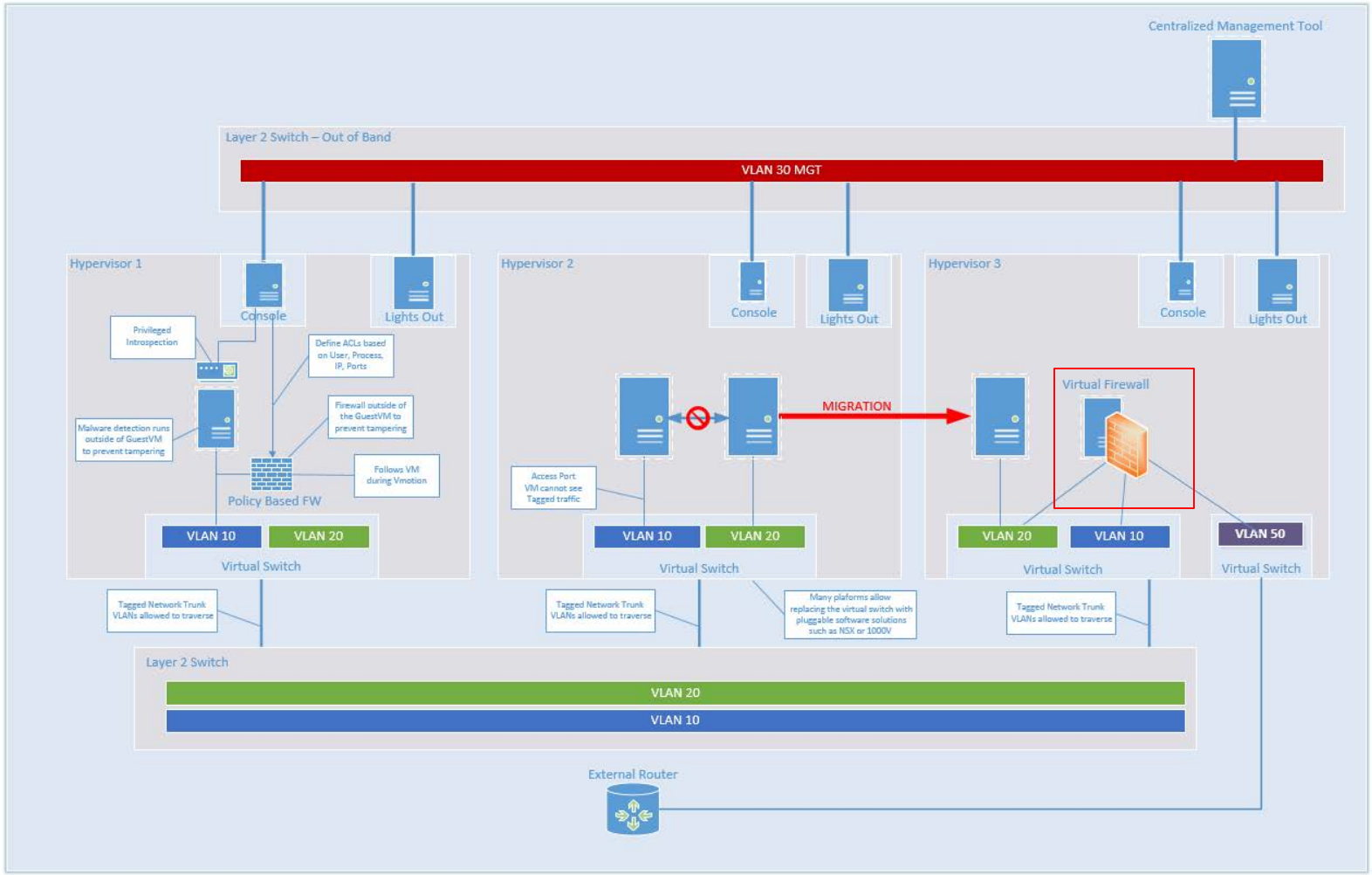
Add a Physical Firewall



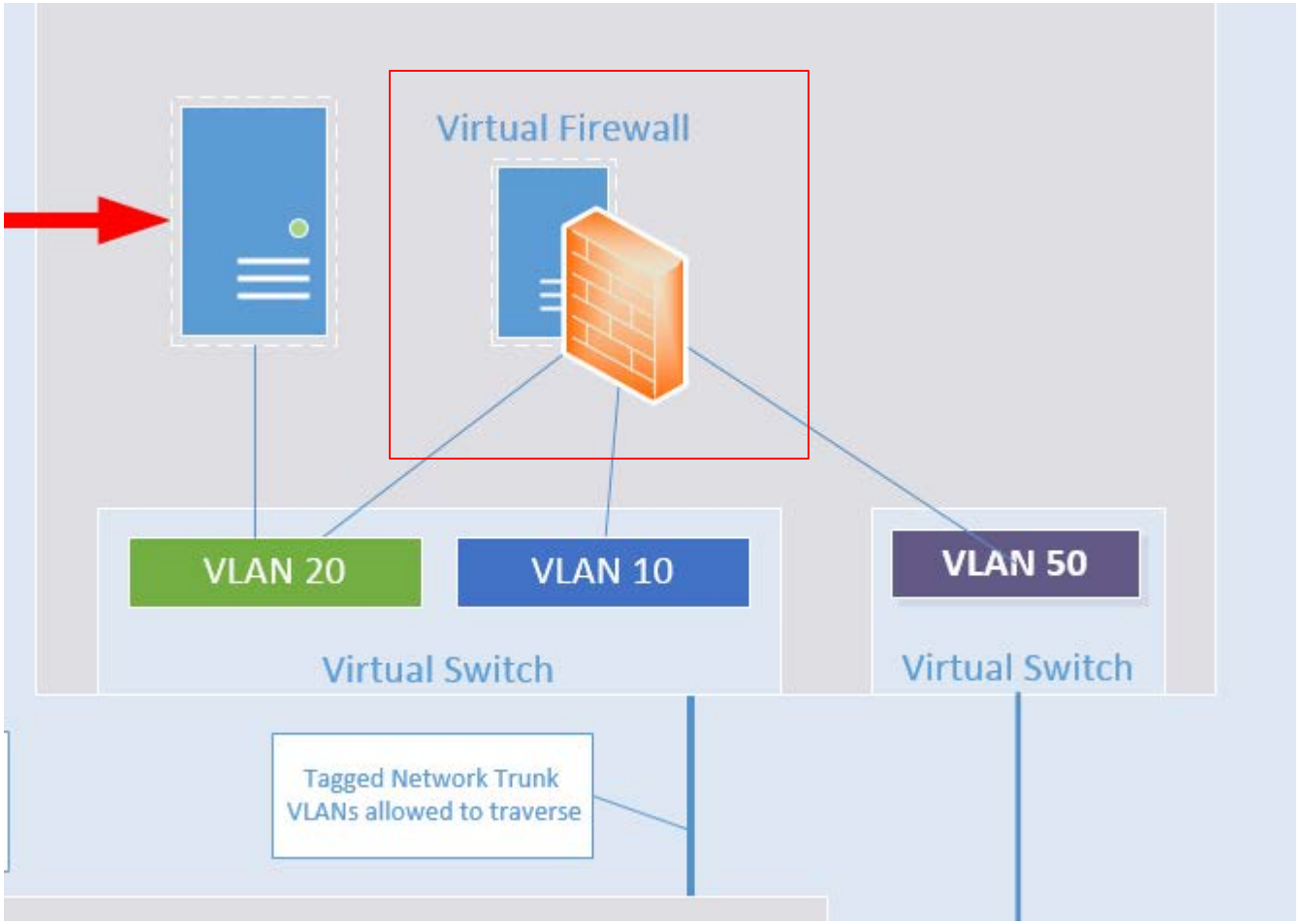
Topology Overview



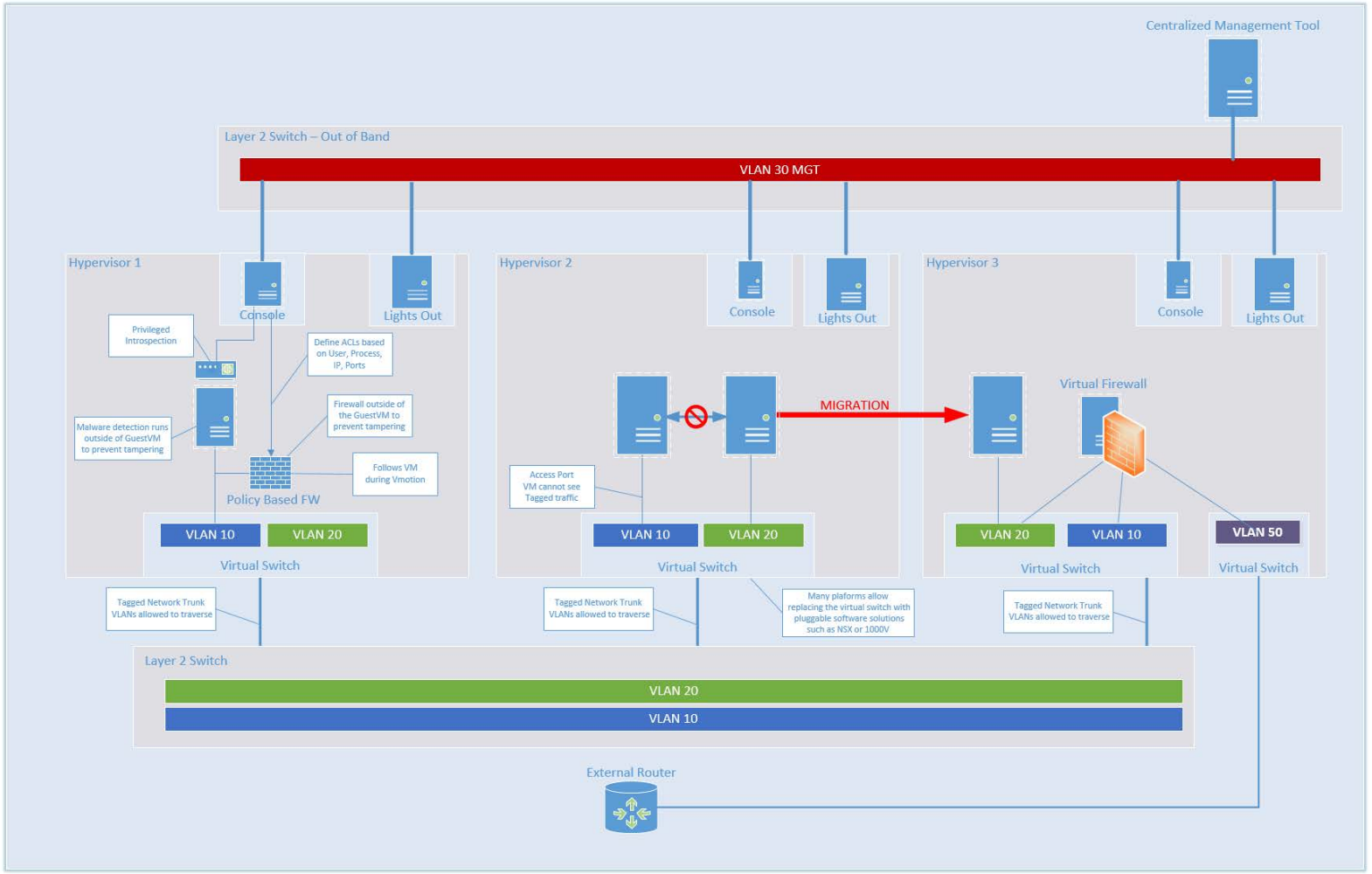
Adding a Virtual Firewall



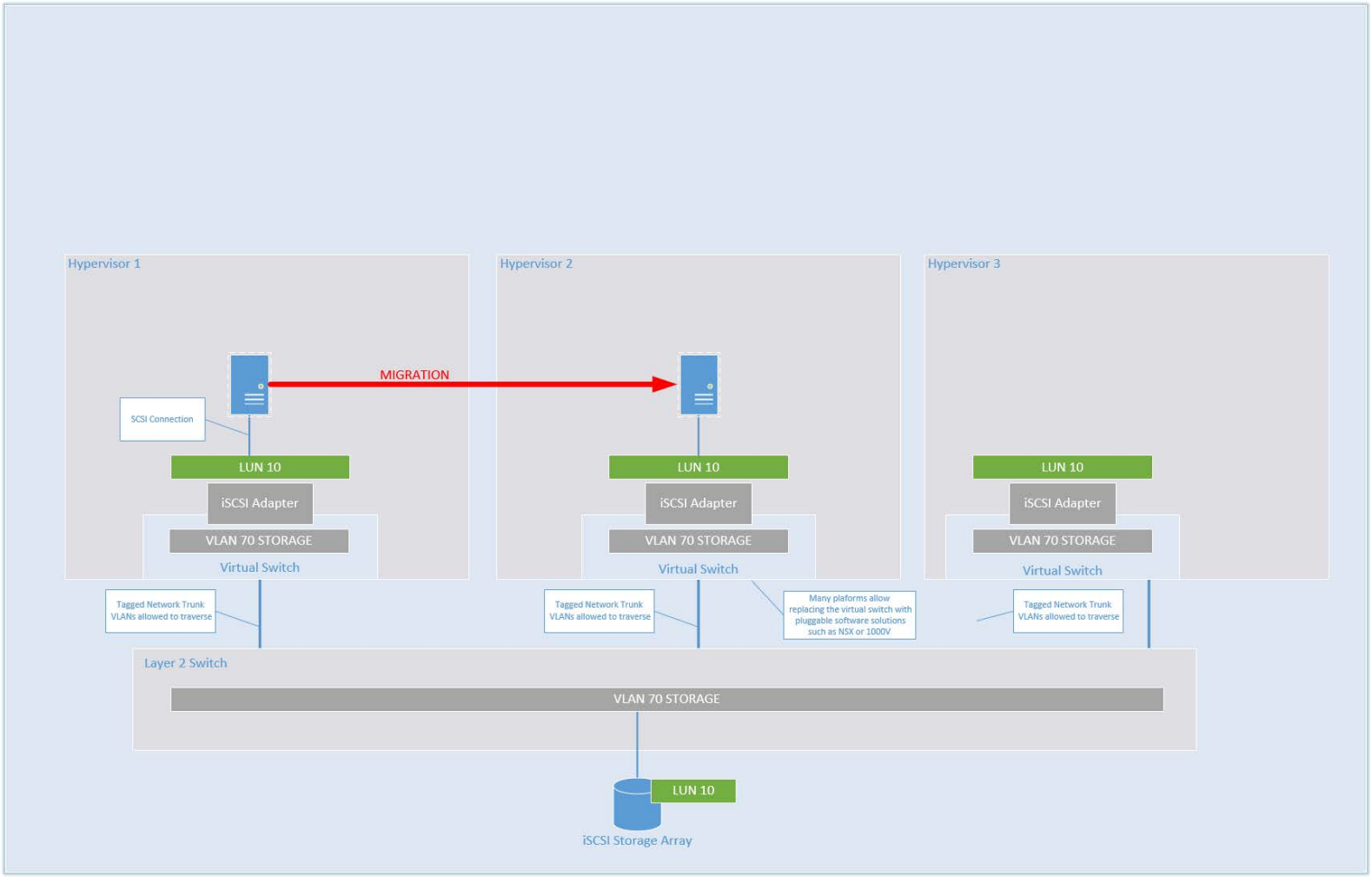
Adding a Virtual Firewall



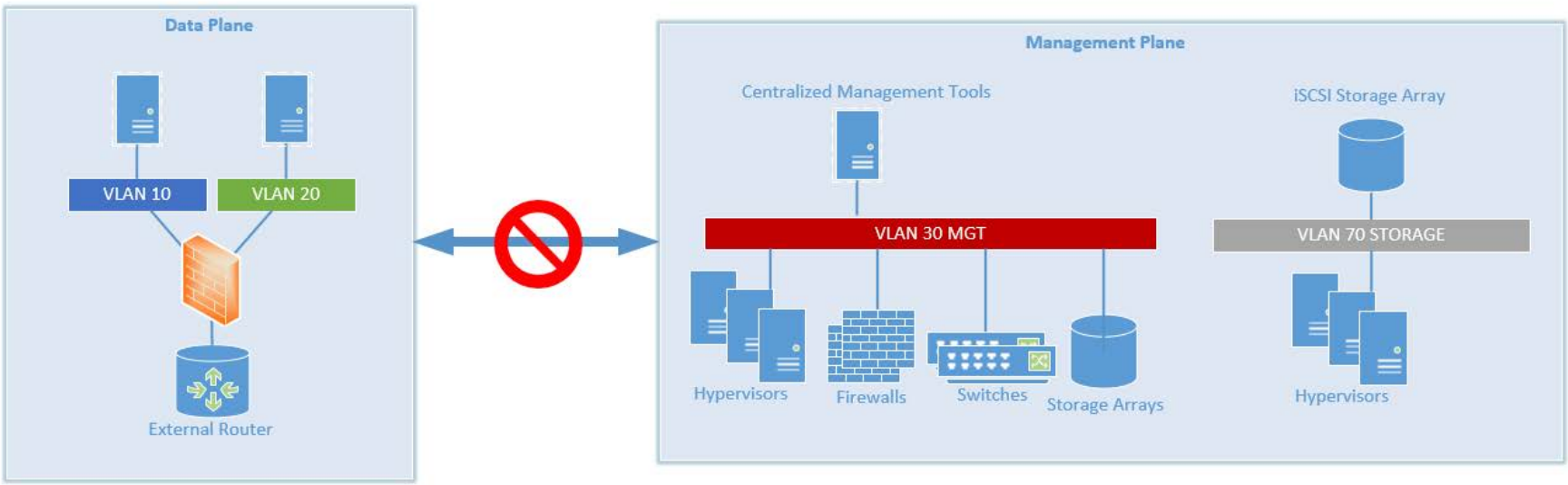
Topology Overview



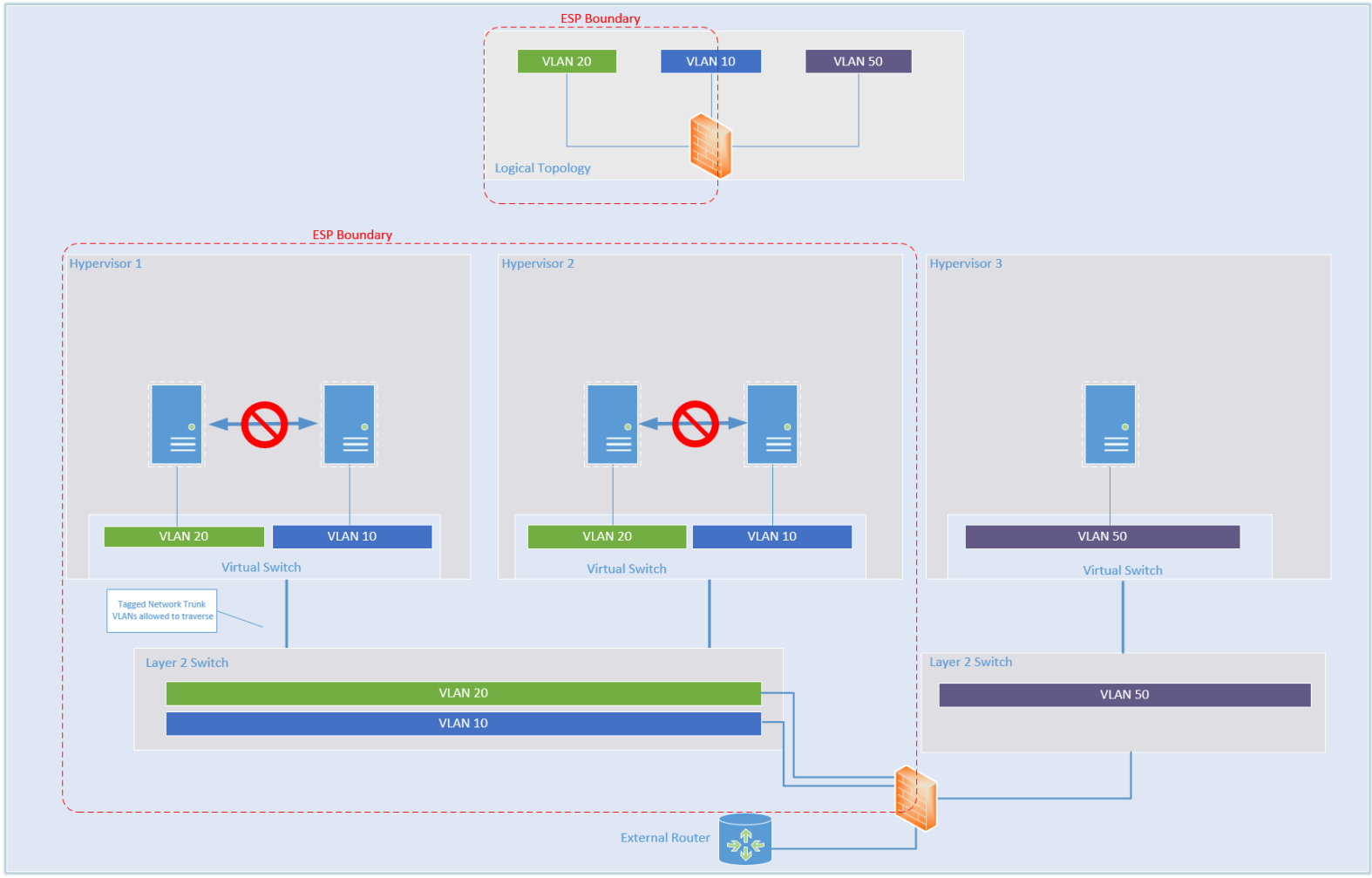
Storage Topology Overview



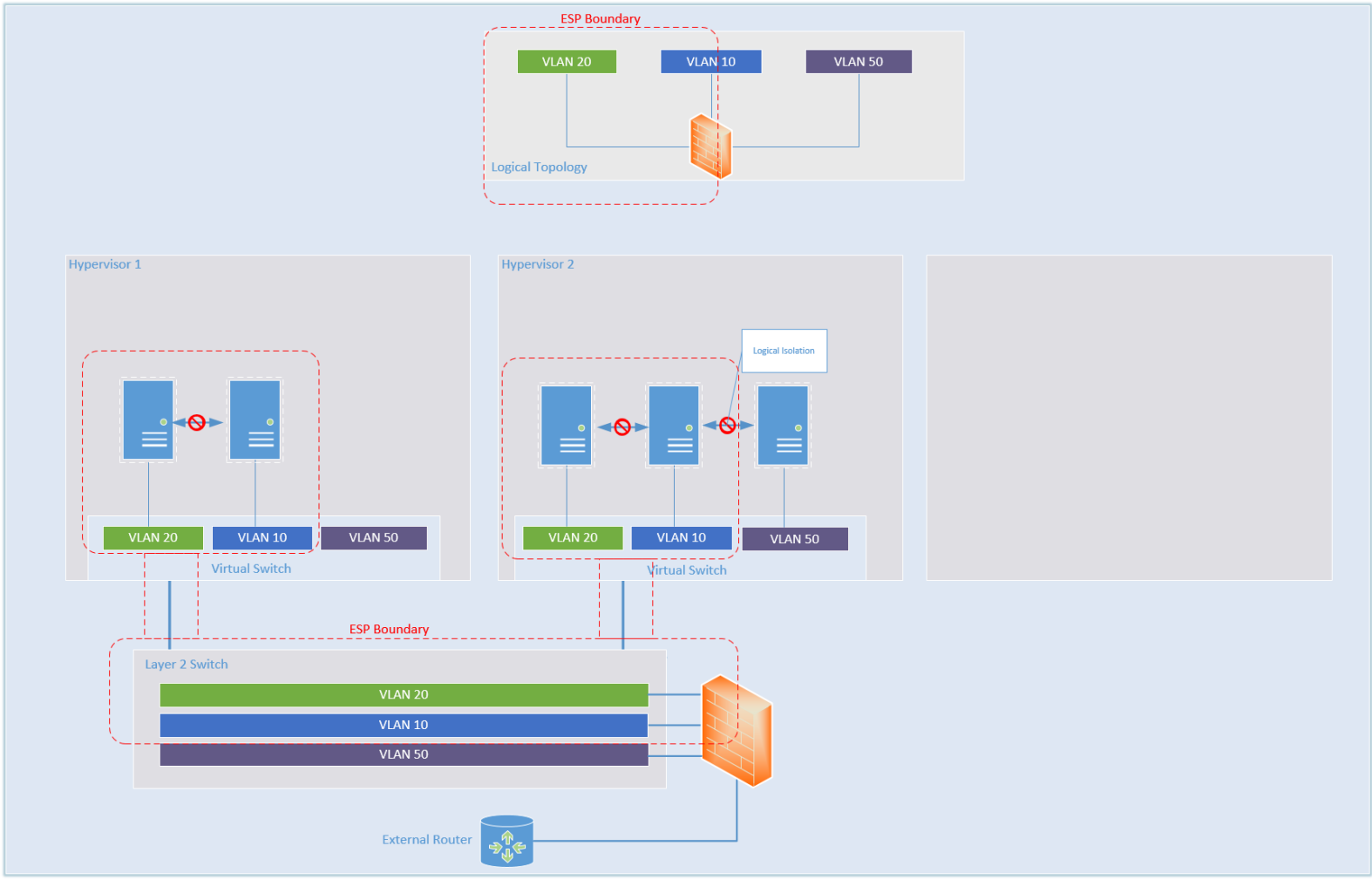
Data / Management Plane Isolation



Physical Isolation and Electronic Security Perimeter (ESP)



Q4: Logical Isolation and ESP

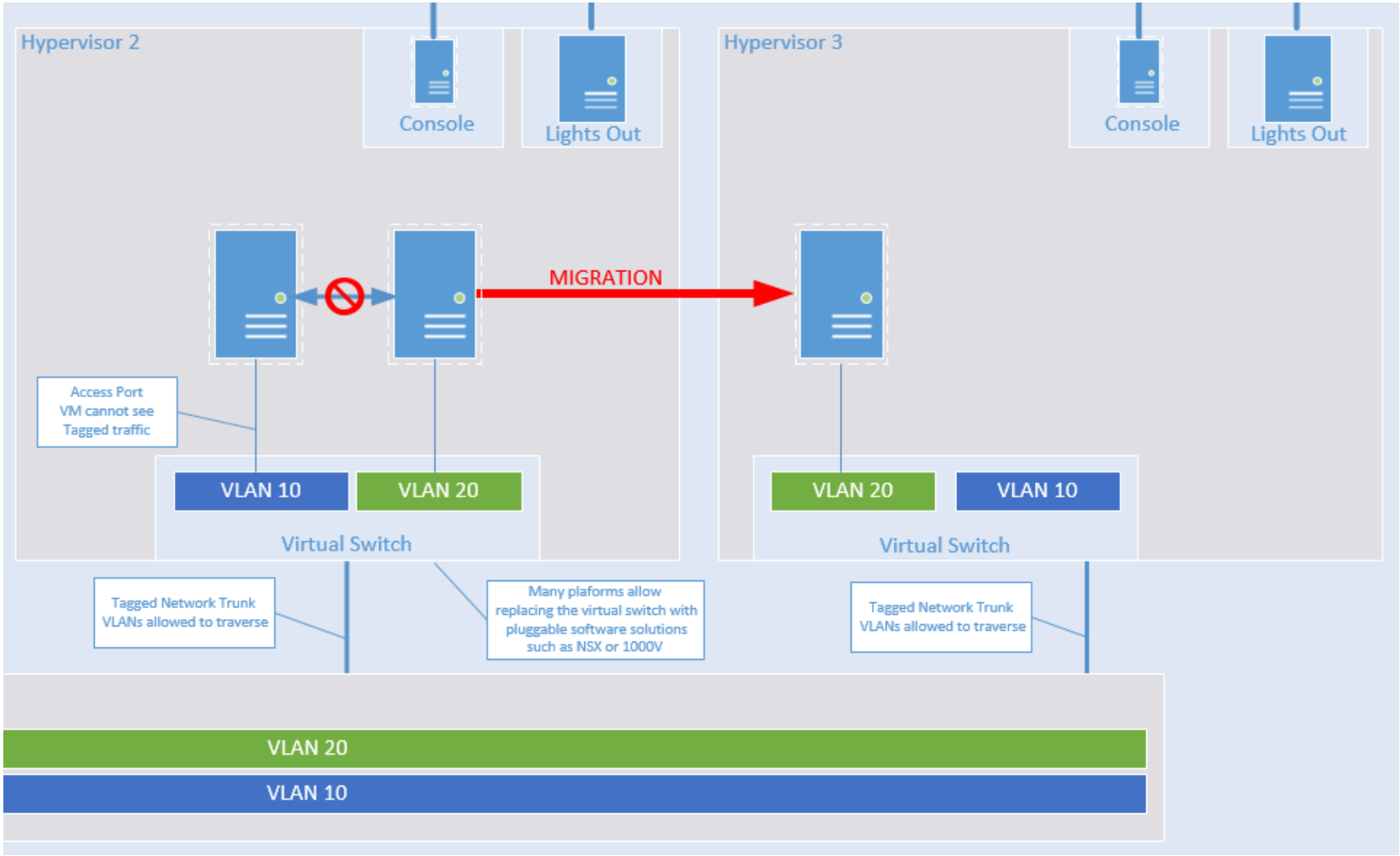


Virtualization and Resilience

Virtualization and Resilience

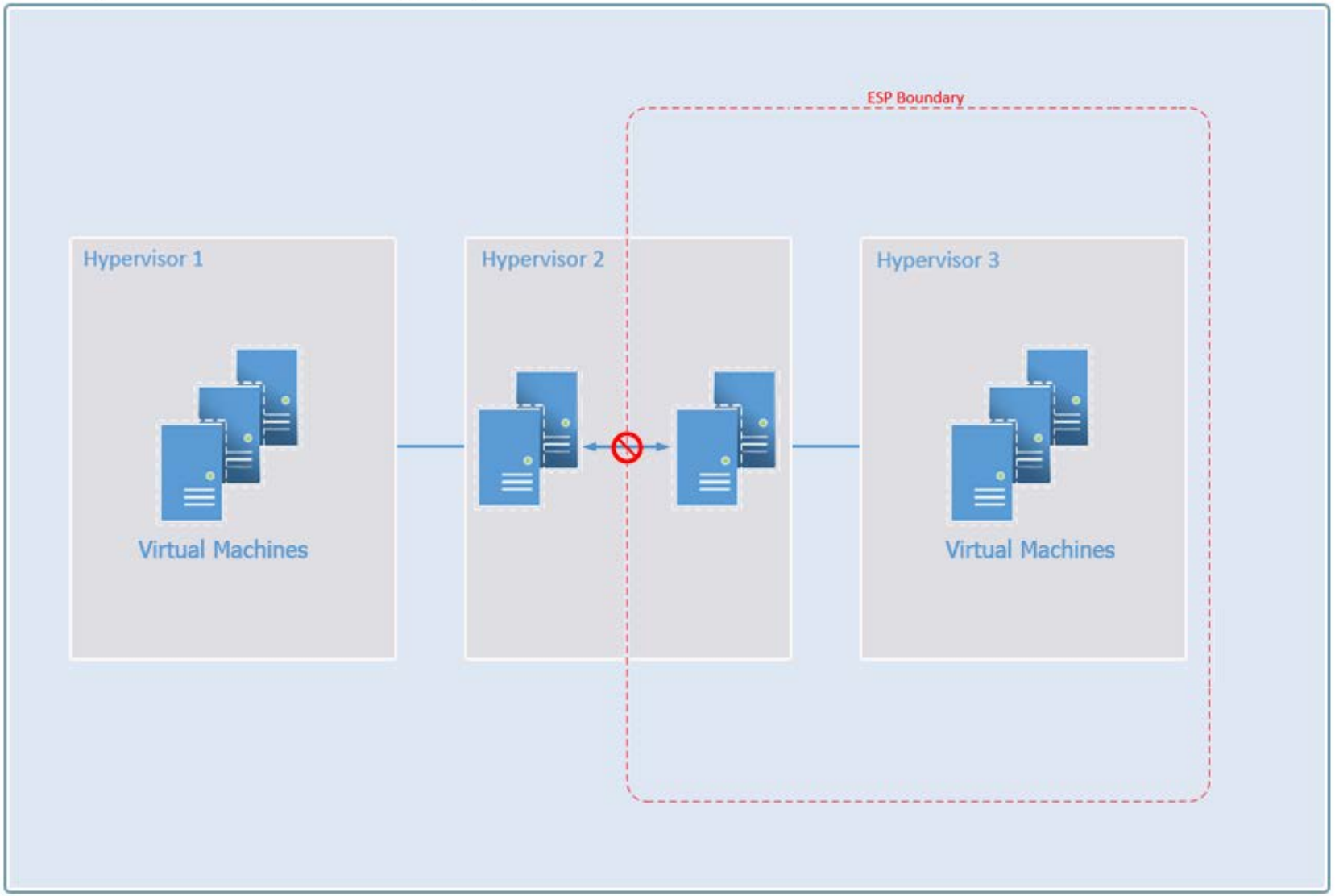
- Introduction to Virtualization Resilience
  - VM mobility impact on location
  - CIP-010: Change management and Template-based vulnerability assessment
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)
- Introduction to agile response
  - Templates, baselines, configuration management
  - Security benefits and technology
  - Cost effectiveness
- Virtualization impact to the CIP Definition of Cyber Asset

VM Resilience: Dynamic Resources and Mobility



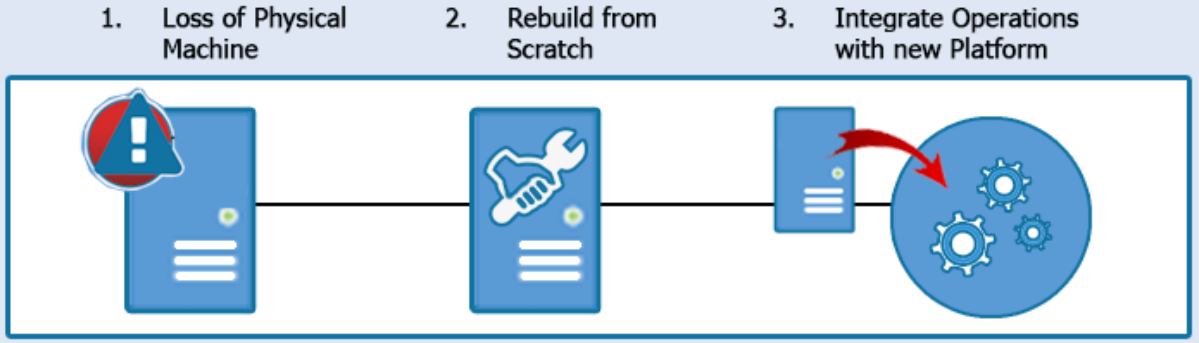
VM Mobility and Asset Location (CIP 5)

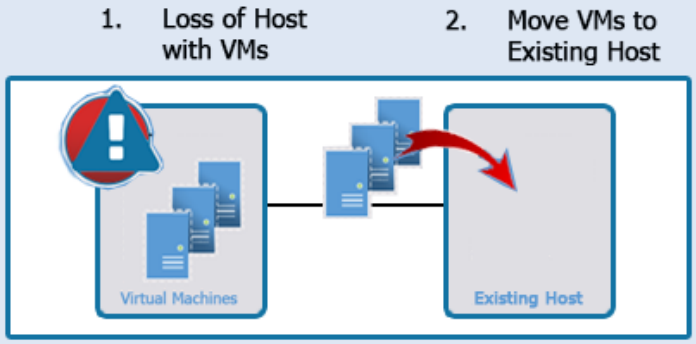
Example of VM mobility within configured parameters



VM Resilience: Recovery Time Objective (RTO)

Outage Stages - Physical Machine vs. Host with Internal VMs





VM Resilience: Recovery Point Objective (RPO)

Traditional Environment:

- Backup files and directories (lengthy process)
- Test restoration periodically
  - Lengthy process, often skipped, media failures
  - Requires a fresh build
- Outage scenario
  - Requires a fresh build from scratch, including exact settings and software
  - Restore files and directories from backup media
  - Validate backup integrity and completeness (often inadequate)
  - Delete / recreate computer objects in directory services

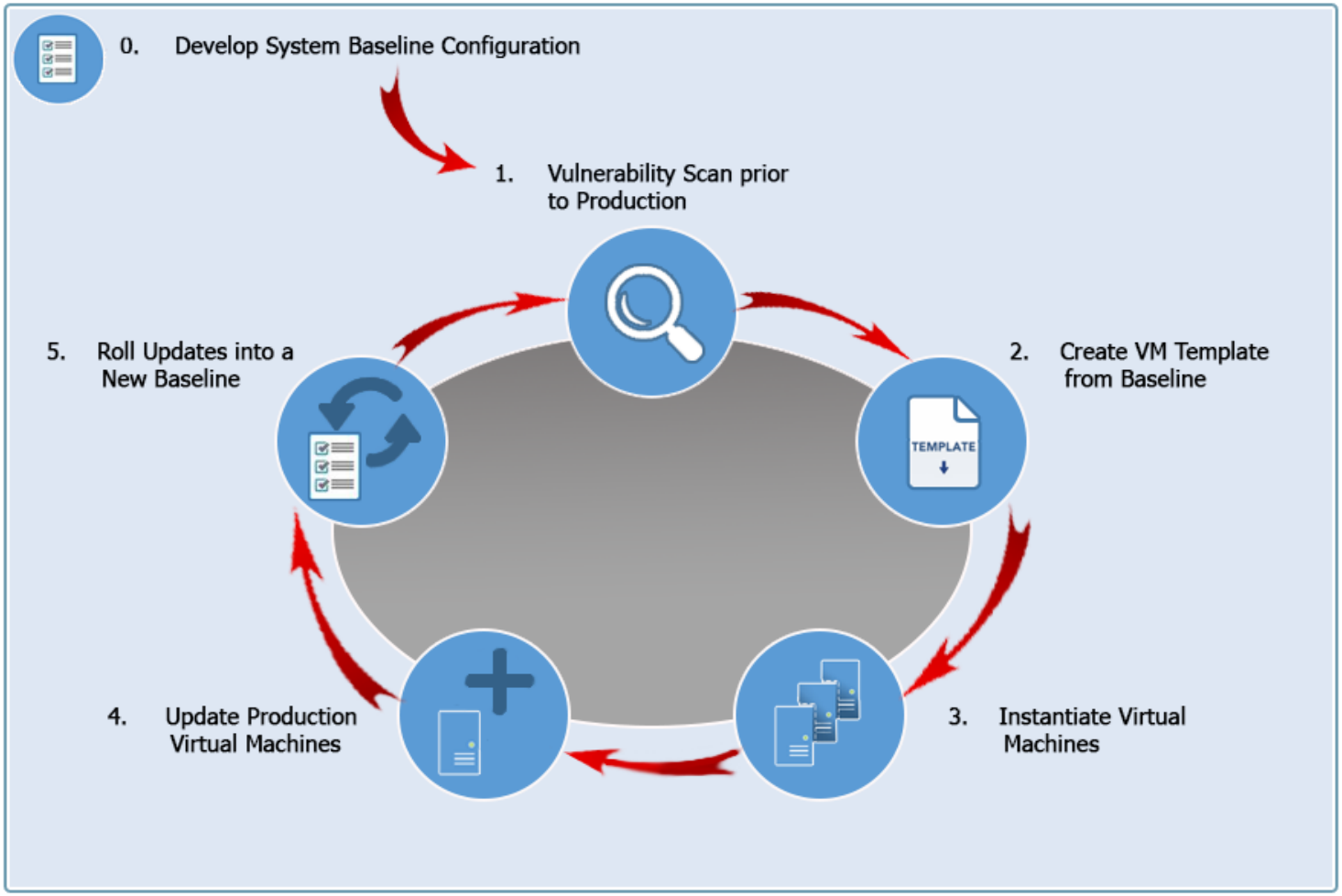
VM Resilience: RPO

Virtual Environment:

- Configure Snapshot interval
- Test restoration
  - Periodically boot Snapshot image to isolated test network, takes minutes to verify state and operation
- Outage scenario
  - Locate desired Snapshot and boot to target host
    - Snapshot is literally just an earlier state of the actual Cyber Asset to be restored
    - No deletion / recreation of computer objects in directory service,
    - no change to IP address, hostname, GUID etc.

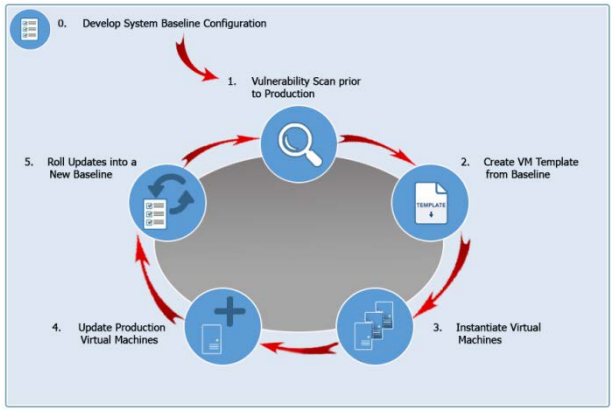
CIP-010: Lifecycle of a VM Baseline

Life Cycle of Virtual Machine Templates using a Developed System Configuration



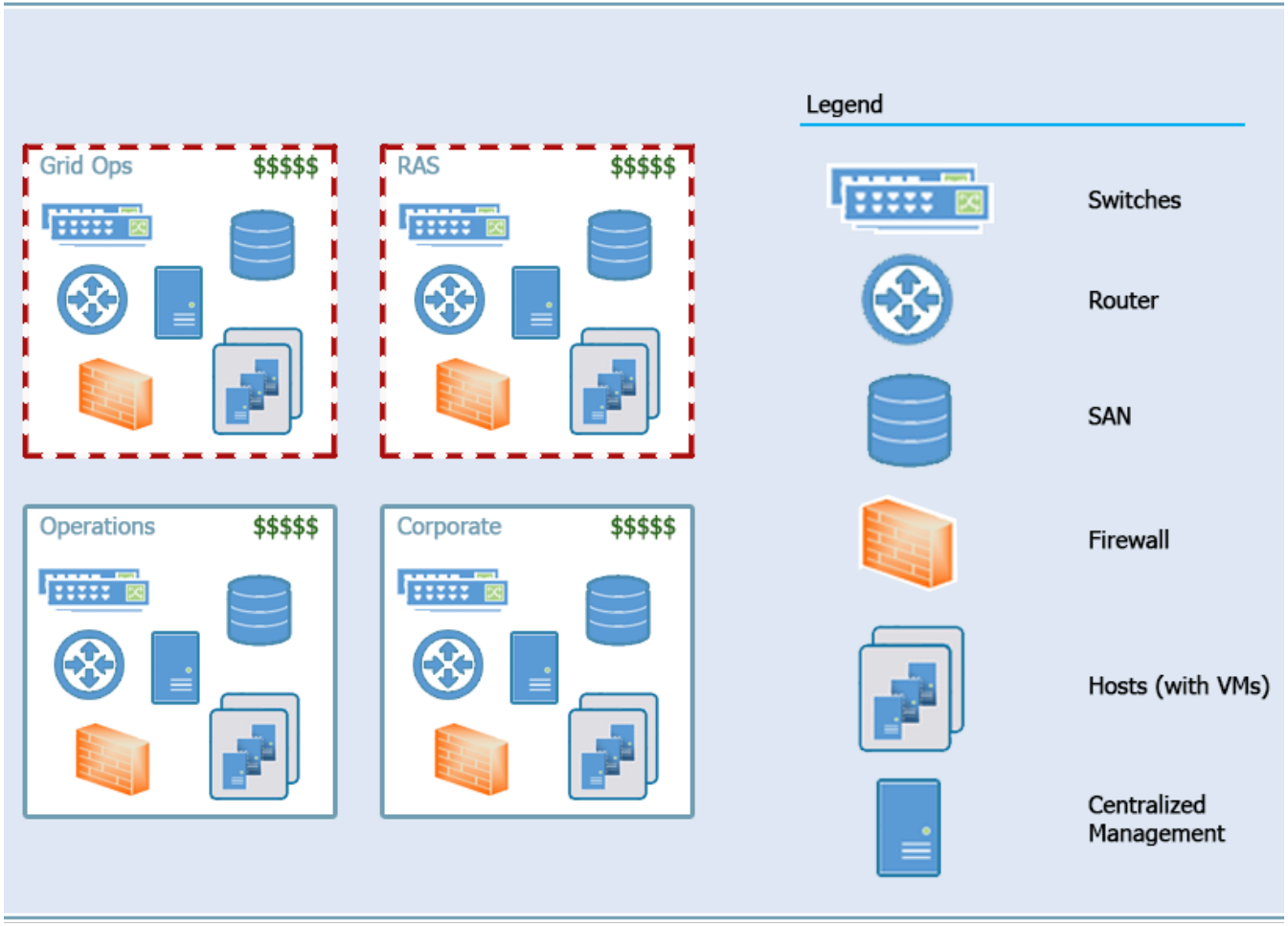
Agile Response

- Develop a CIP-010 system configuration baseline and scan it
- Create a VM template from the system configuration baseline
- Subsequent instances created from the template inherit the scan of the baseline (CIP-010-2, R3.3)
- Per CIP-010-2, R1.3, changes to the baseline start the process over again
- The process is consistent and efficient



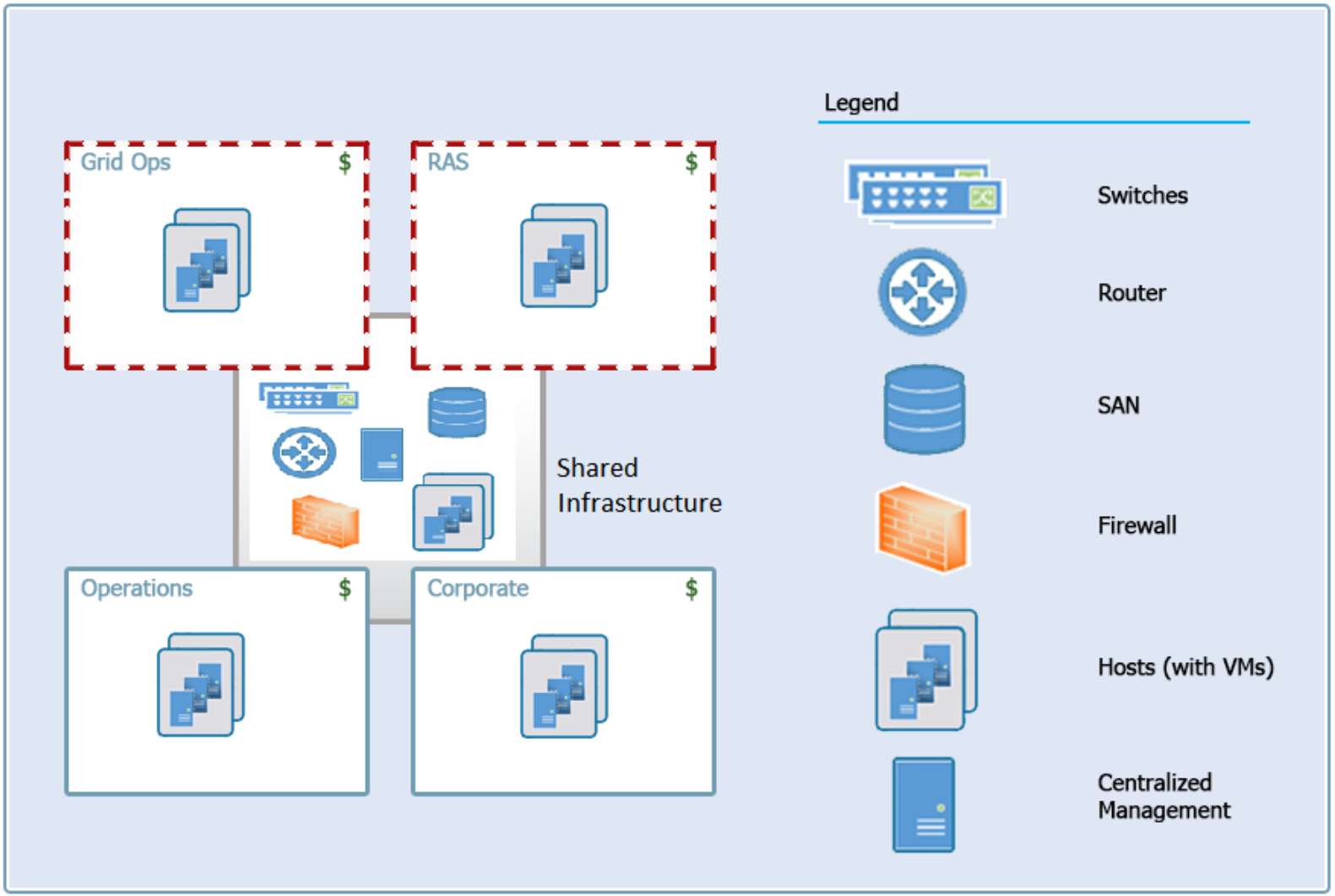
Cost Effectiveness

ost Prohibitive Networks



Cost Effectiveness

Cost Effective Networks



Security Benefits and Cost Effectiveness

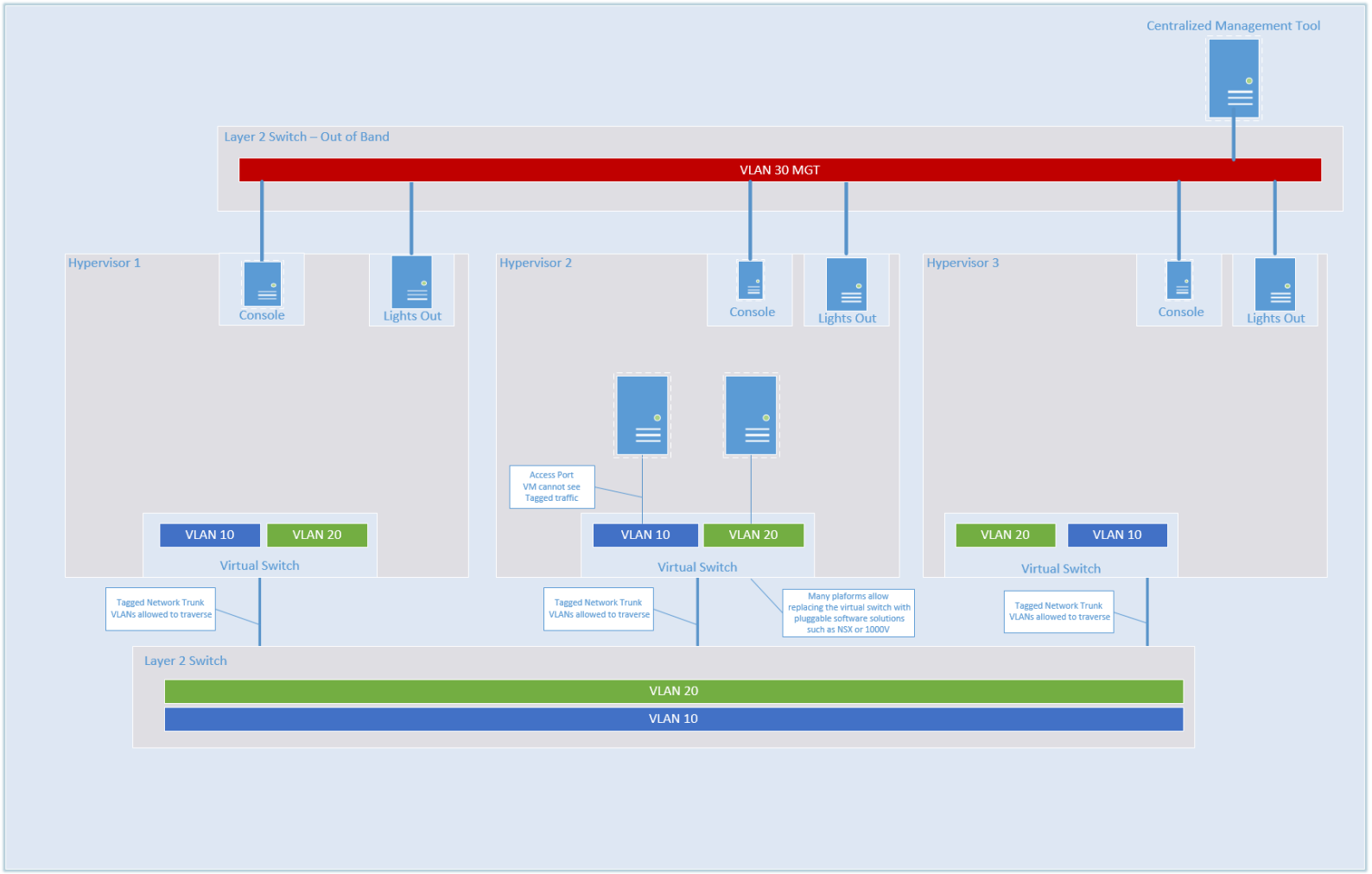
- NERC has transitioned to include risk analysis in all aspects of its regulatory model, focusing the Electric Reliability Organization's and stakeholder resources on the highest risks to the reliability of the Bulk Electric System.
- Registered entities vary in their operations and vulnerabilities; therefore, the costs for Reliability Standard implementation may vary by orders of magnitude by entity.
- Costs from the implementation of NERC Reliability Standards are implicitly considered throughout the standards development process where detailed comments are sought from the standards ballot pool, which represents a cross-section of interested participants. The Standard Drafting Team may then modify the proposed standards to provide appropriate latitude for implementation of the standards.

Cyber Asset Definition (Q2)

- The proposed *Cyber Asset* definition is:
  - ~~*Programmable*~~*An electronic device*~~*s*~~ *(physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in* ~~*those devices*~~ *the device. A virtual machine is itself a distinct asset from its host(s).*

  - *An electronic device (physical or virtual) whose operation is controlled by a stored program that can be changed or replaced by the end user, including the hardware, software, and data in the device. A virtual machine is itself a distinct asset from its host(s).*

Systems Approach (Q1)



Resources

- This slide deck and other information relative to the CIP Modifications Standard Drafting Team may be found on the Project 2016-02 Project and Related Files pages:

  Project 2016-02 Modifications to CIP Standards

- Cost Effectiveness in NERC Standards:

  Cost Effectiveness Pilot

  - Contact Info for further questions:
    - Katherine.Street@NERC.net
    - Mat.Bunch@NERC.net

References

A Virtual Machine Introspection Based Architecture for Intrusion Detection, Garfinkel, T. and Rosenblum, M. Computer Science Department, Stanford University. Retrieved from Internet website: https://suif.stanford.edu/papers/vmi-ndss03.pdf

Special Publication 800-125: Guide to Security for Full Virtualization Technologies, Scarfone et. al. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, January 2011. Retrieved from Internet website: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

Special Publication 800-125A {Draft}: Security Recommendations for Hypervisor Deployment, Chandramouli, R. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, October 2014. Retrieved from Internet website: http://csrc.nist.gov/publications/drafts/800-125a/sp800-125a_draft.pdf

Special Publication 800-125B: Secure Virtual Network Configuration for Virtual Machine (VM) Protection, Chandramouli, R. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, March 2016. Retrieved from Internet website: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf

Special Publication 800-180 (DRAFT): NIST Definition of Microservices, Application Containers and System Virtual Machines, Karmel A., et.al. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology (NIST), February 2016, Retrieved from Internet website:

http://csrc.nist.gov/publications/drafts/800-180/sp800-180_draft.pdf

Questions and Answers