NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP SDT Outreach Slides

Project 2016-02 Project Update

CIP SDT Members
April 2019

RELIABILITY | ACCOUNTABILITY

Presenters

- Jay Cribb, Southern Company
- Matt Hyatt, TVA
- Jerry Freese, NIPSCO
- Scott Klauminzer, Tacoma Power
- Jake Brown, ERCOT
- Heather Morgan, EDP Renewables North America LLC

NERC Antitrust Compliance 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.

Public Announcement

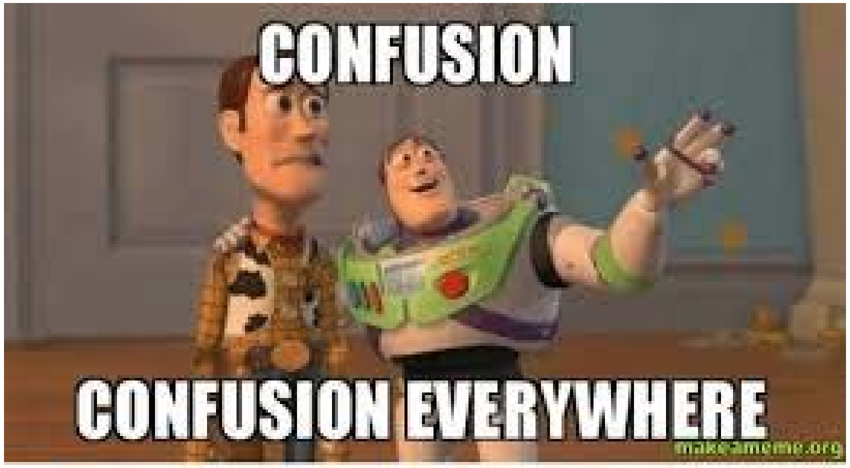
Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities.

Agenda

- Why
- Many Challenges
- What we Heard
- How we can move forward

Why

- Why are we here and why are these changes needed?



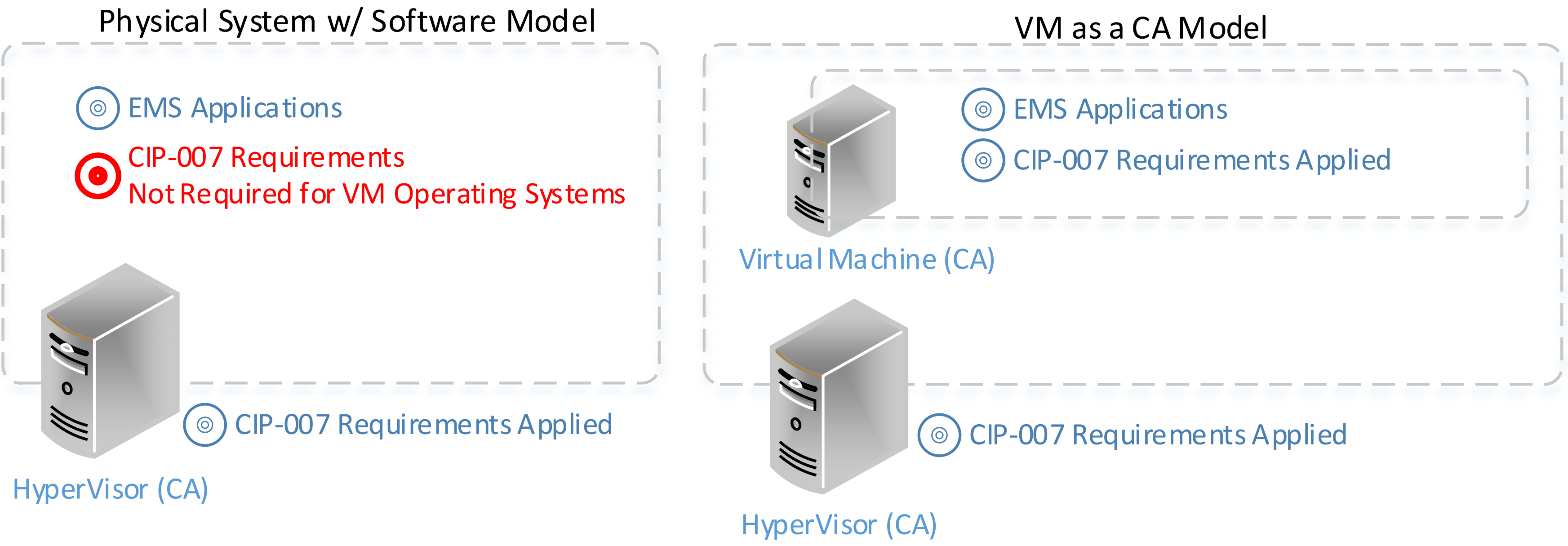
Many Challenges

- CIP v5 Technology Specific
  - Cyber Assets (inclusive of hardware 1:1)
  - Prescribed network architecture restricts best practices
- Virtualization Challenges
  - Virtualized Firewall Interfaces
  - Storage
  - Shared Infrastructure
  - Management Plane Considerations
  - Privileged Introspection & Distributed firewalls
  - Remediation VLANs
  - Super ESP

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

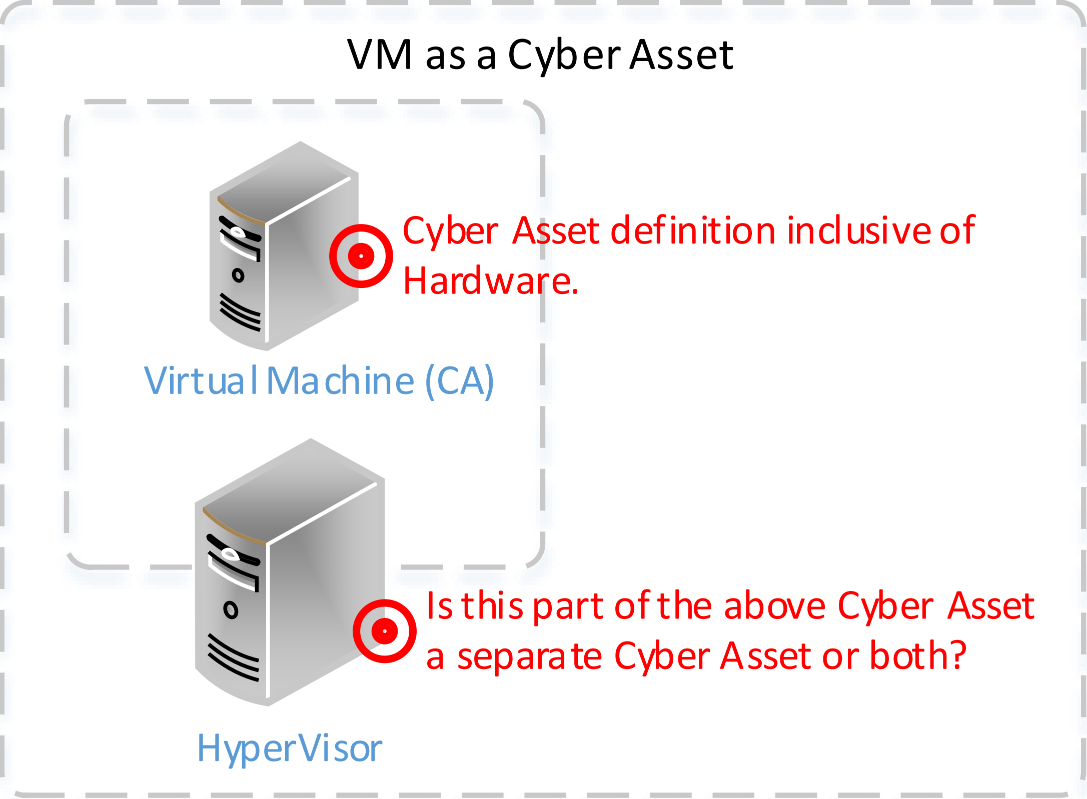
Many Challenges – Identifying Cyber Assets

- Treating virtual machines as software can leave security gaps


Physical System w/ Software Model
◎ EMS Applications
◎ CIP-007 Requirements Not Required for VM Operating Systems
◎ CIP-007 Requirements Applied
HyperVisor (CA)
VM as a CA Model
◎ EMS Applications
◎ CIP-007 Requirements Applied
Virtual Machine (CA)
◎ CIP-007 Requirements Applied
HyperVisor (CA)

Many Challenges – Asset Identification

- Virtual Cyber Assets (inclusive of hardware 1:1)
- Treating VMs as a Cyber Asset creates the "hall of mirrors" because Cyber Asset is inclusive of its hardware

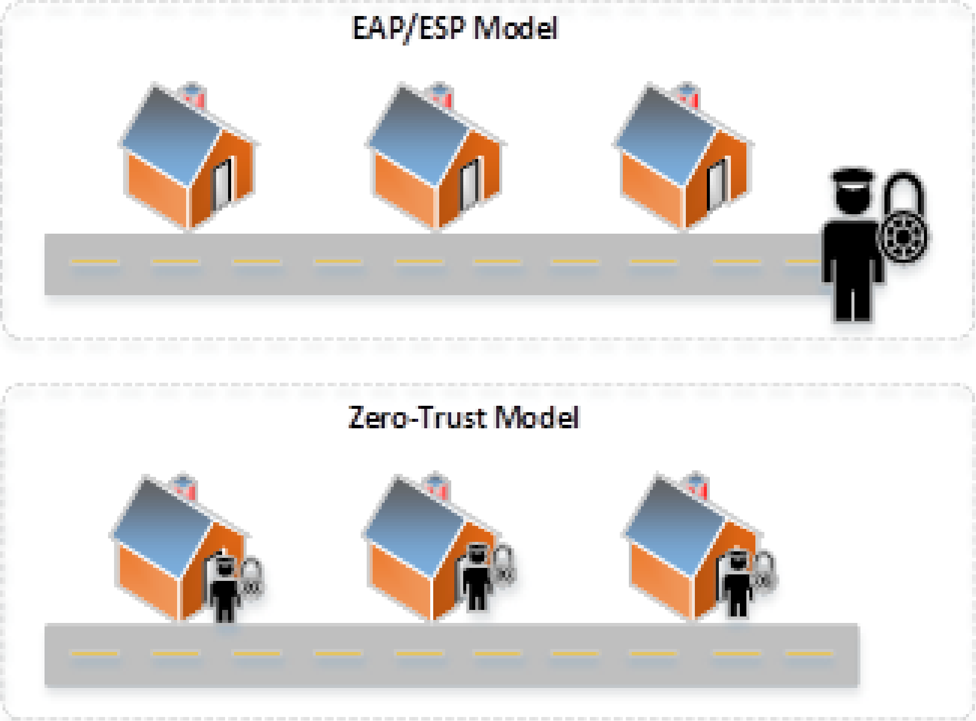


Cyber Asset definition inclusive of Hardware.

Is this part of the above Cyber Asset a separate Cyber Asset or both?

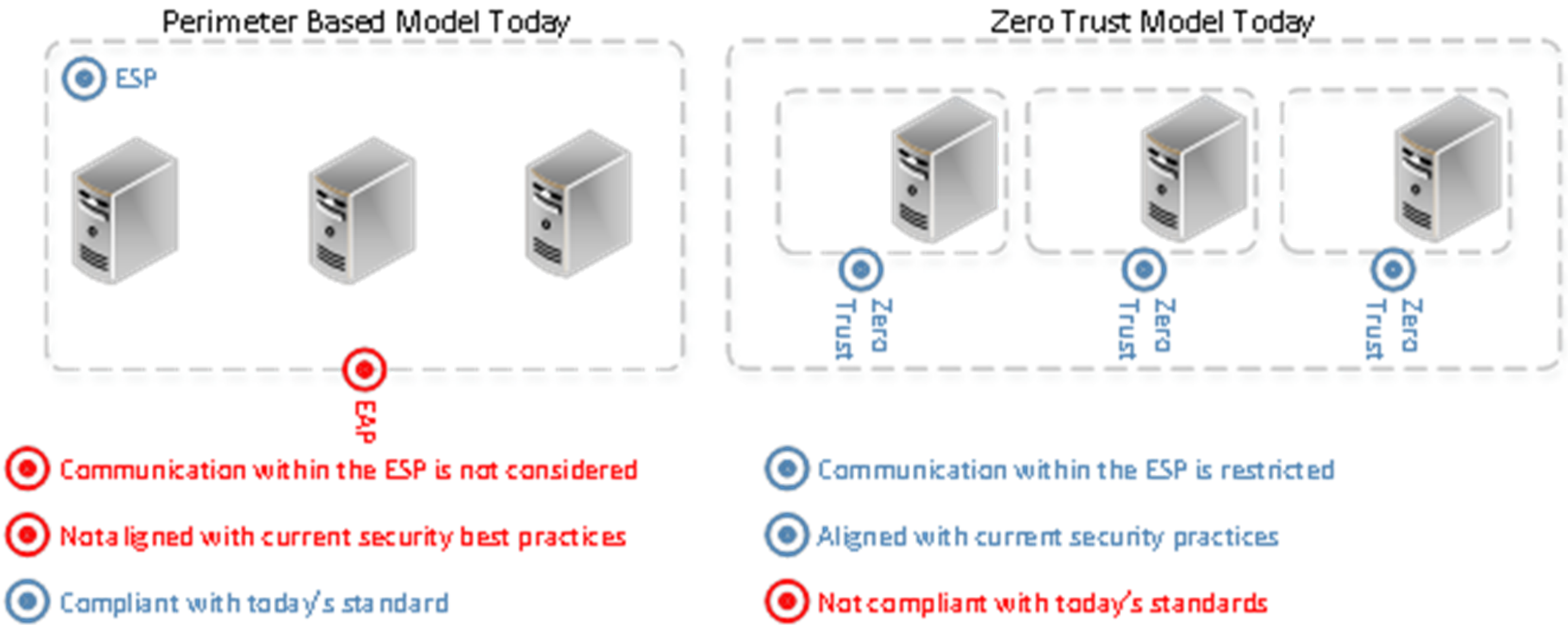
Many Challenges – Network Architecture

- Gated community diagram.



Many Challenges – Network Architecture

- Prescribed network architecture restricts best practices



◉ Communication within the ESP is not considered

◉ Not aligned with current security best practices

◉ Compliant with today's standard

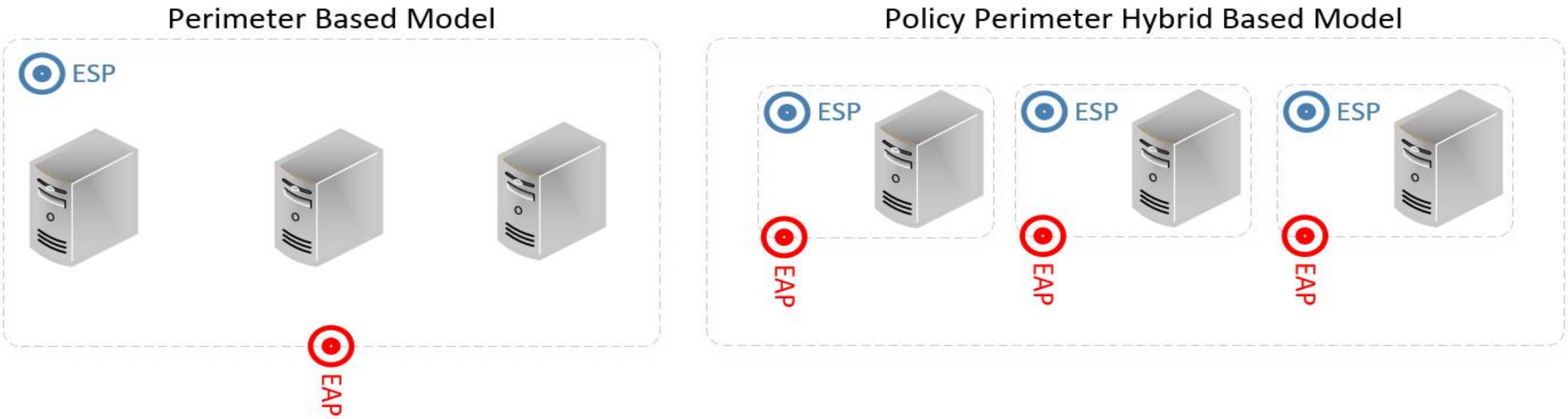
◉ Communication within the ESP is restricted

◉ Aligned with current security practices

◉ Not compliant with today's standards

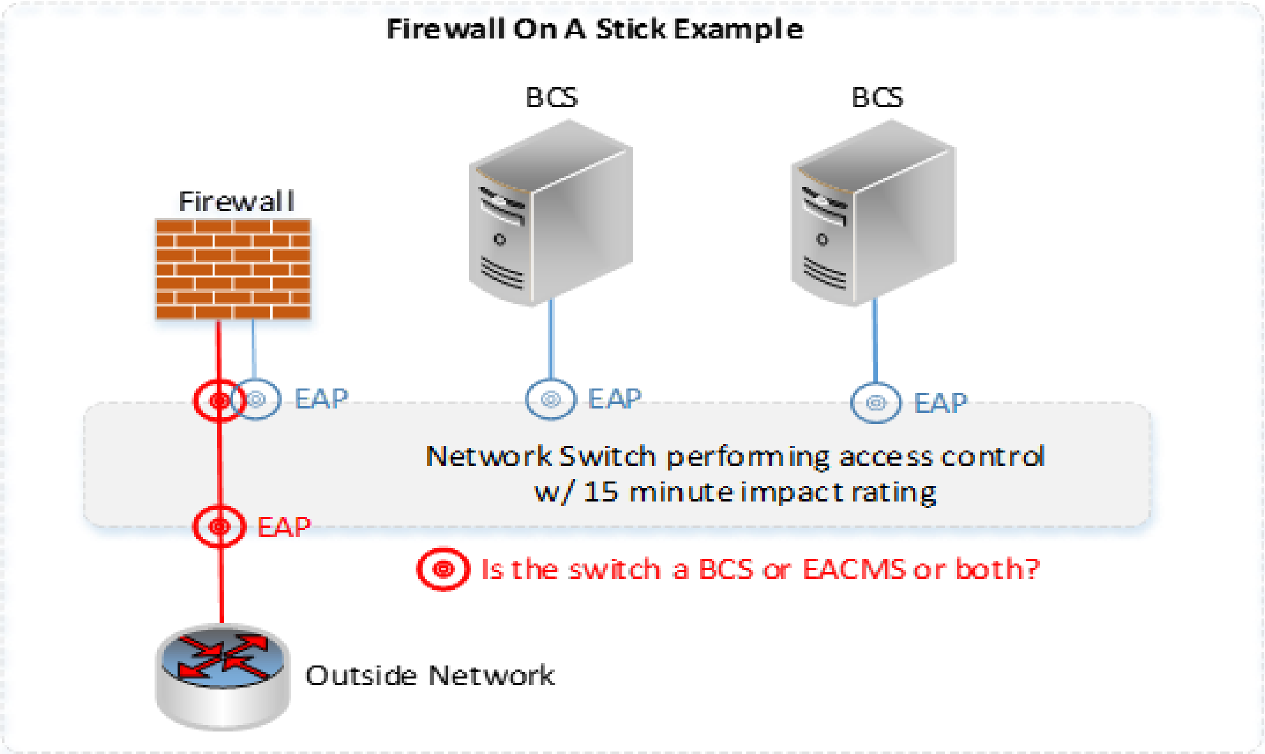
Many Challenges – Network Architecture

- Current standard applied to Zero Trust



Many Challenges – Virtualized Firewall Interfaces

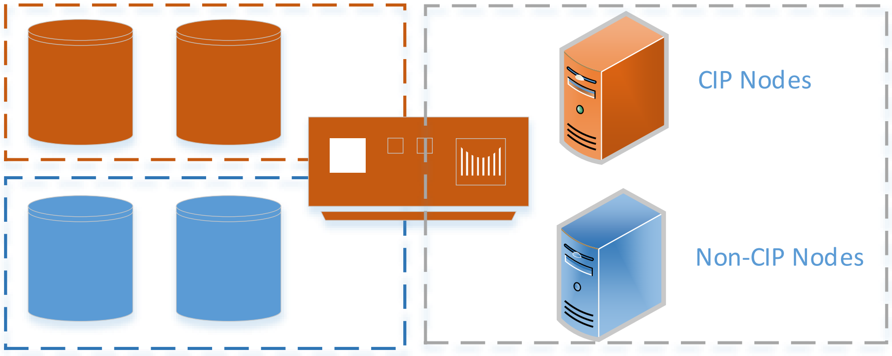
- Virtualized Firewall Interfaces (‘Firewall on a Stick’)

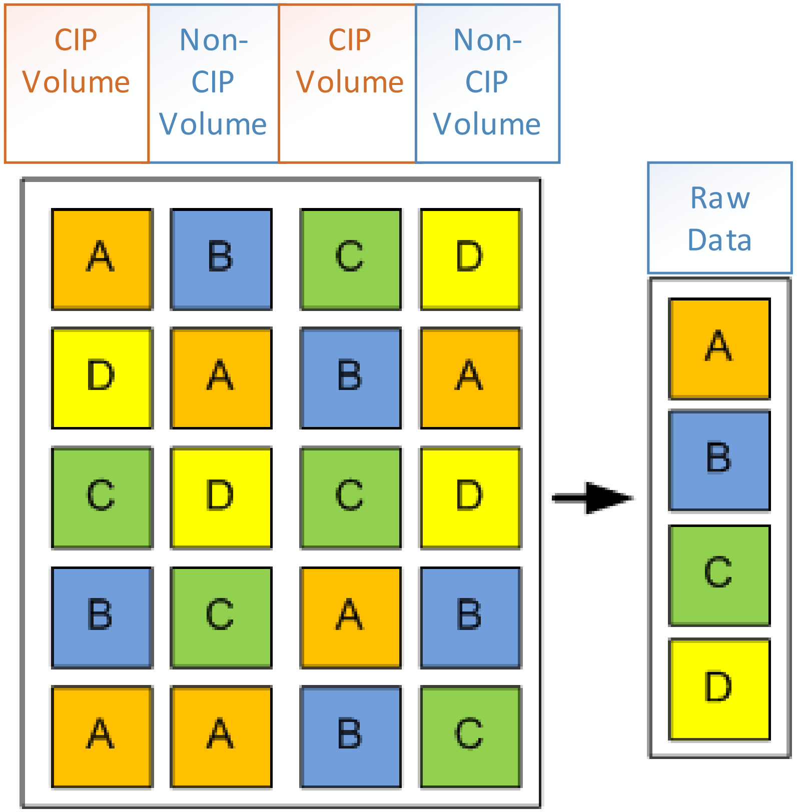


Firewall On A Stick Example
BCS
BCS
Firewall
EAP
EAP
EAP
Network Switch performing access control w/ 15 minute impact rating
EAP
Is the switch a BCS or EACMS or both?
Outside Network

Many Challenges - Storage

- SAN/NAS deduplication & sanitization





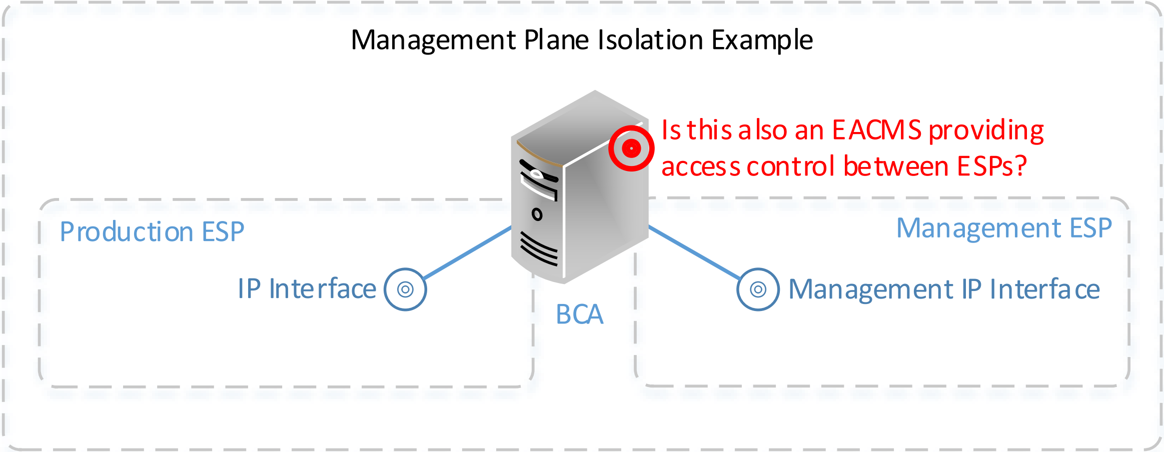
CIP Volume	Non-CIP Volume	CIP Volume	Non-CIP Volume
A	B	C	D
D	A	B	A
C	D	C	D
B	C	A	B
A	A	B	C

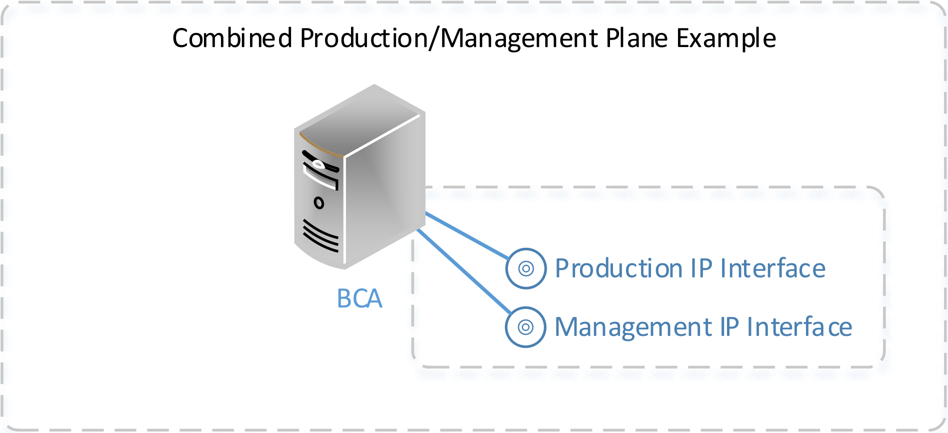
Raw Data
A
B
C
D

Deduplication Example

Many Challenges - Management

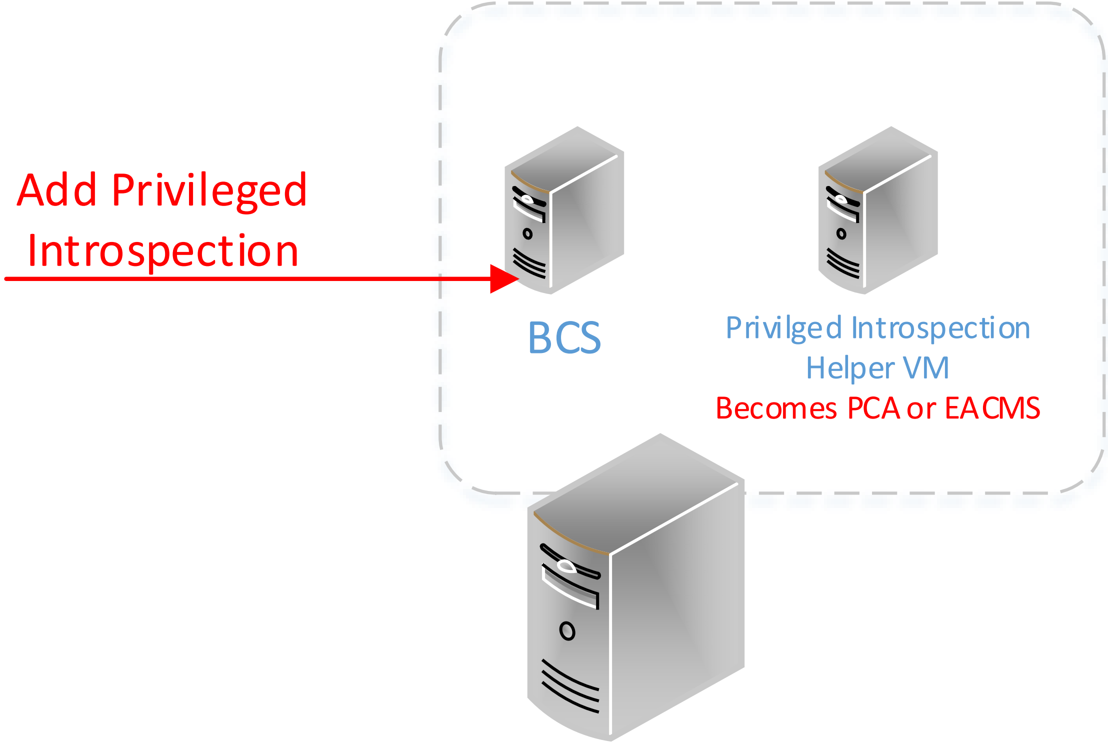
- Management Plane Considerations


Management Plane Isolation Example
Is this also an EACMS providing access control between ESPs?
Production ESP
IP Interface
BCA
Management ESP
Management IP Interface



Many Challenges – Introspection

- Privileged Introspection



Add Privileged Introspection

BCS

Privilged Introspection Helper VM

Becomes PCA or EACMS

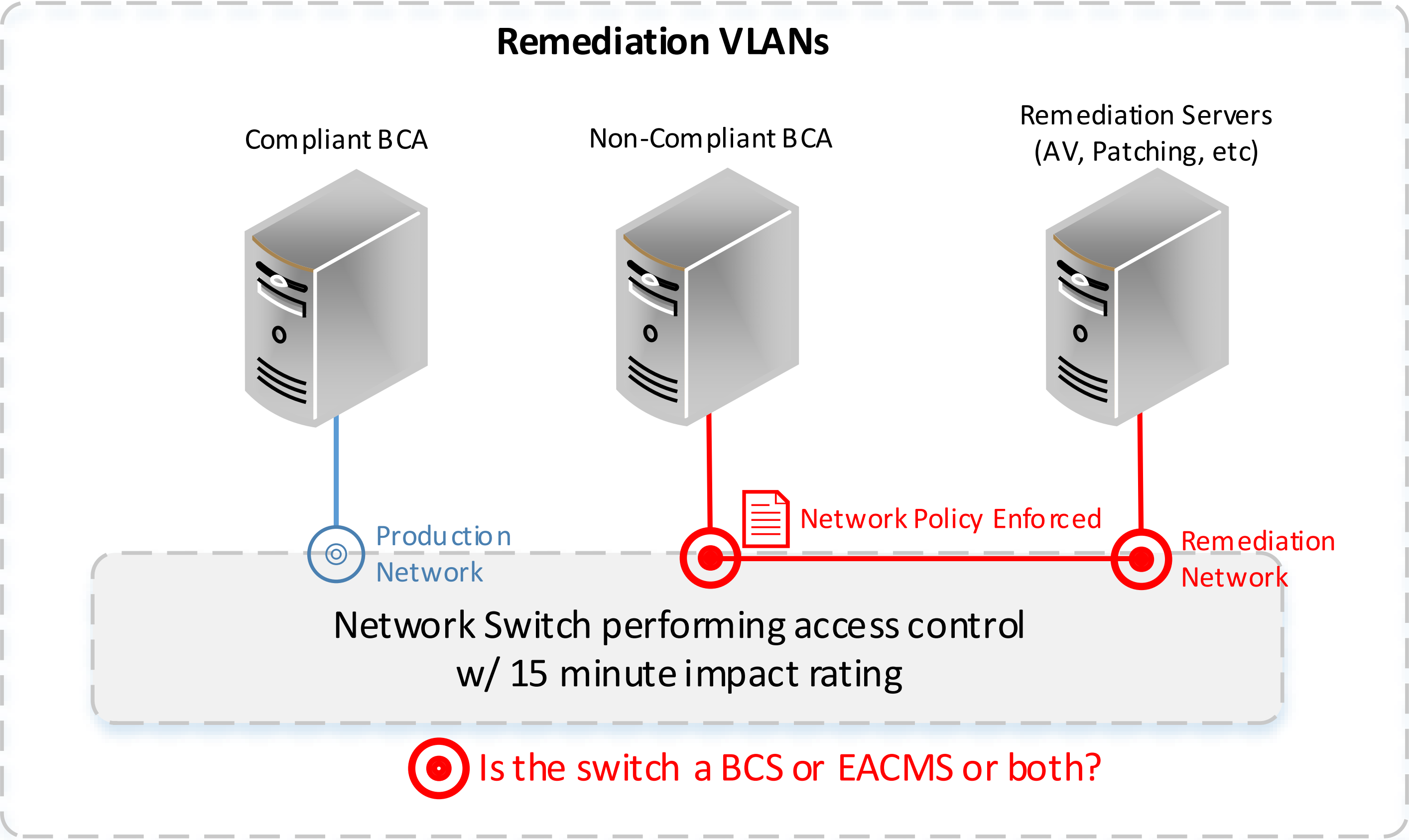
HyperVisor

BCS or EACMS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Many Challenges - Remediation

- Remediation VLANs



Remediation VLANs

Compliant BCA

Non-Compliant BCA

Remediation Servers (AV, Patching, etc)

Production Network

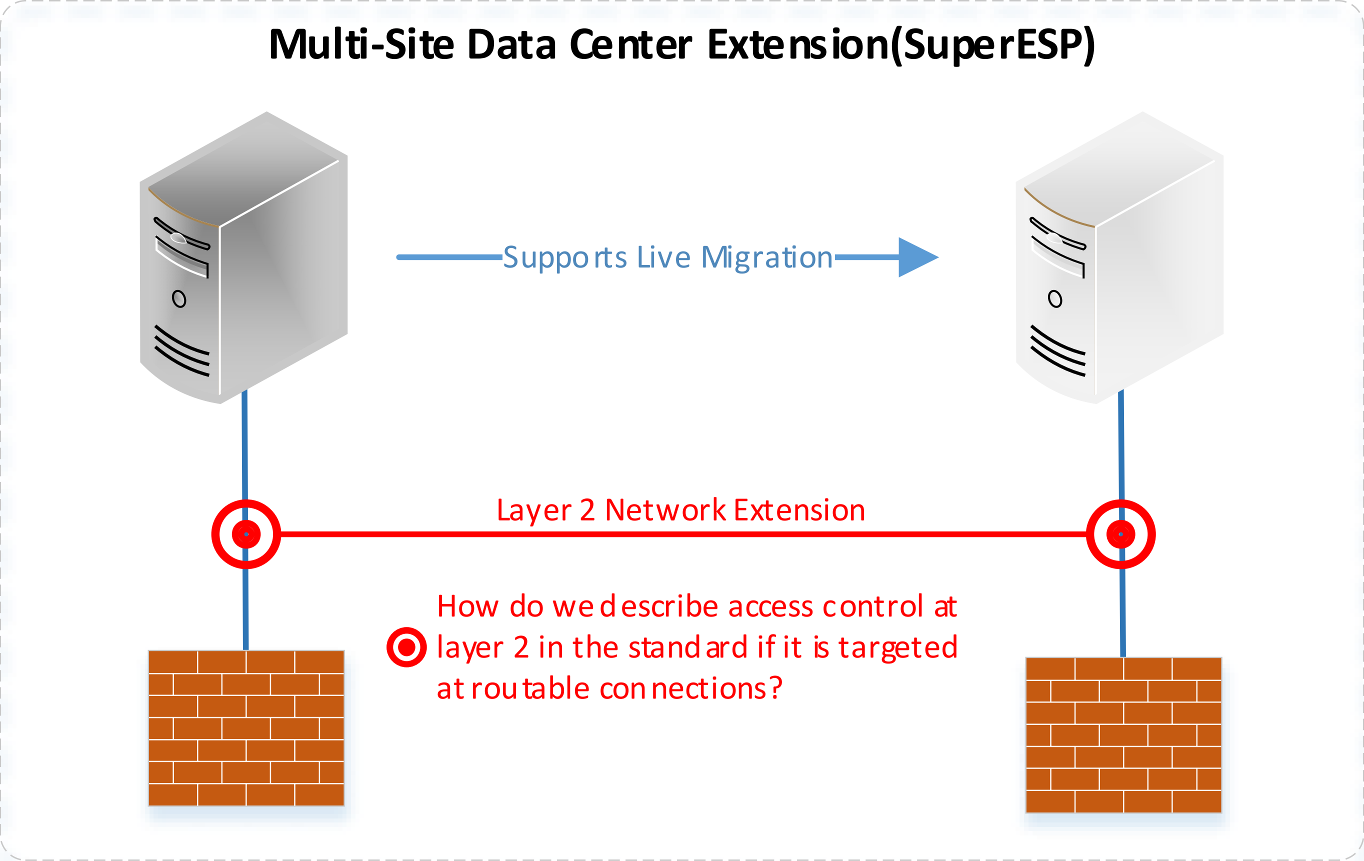
Network Policy Enforced

Remediation Network

Network Switch performing access control w/ 15 minute impact rating

Is the switch a BCS or EACMS or both?

Many Challenges – Super ESP



Multi-Site Data Center Extension(SuperESP)
Supports Live Migration
Layer 2 Network Extension

How do we describe access control at layer 2 in the standard if it is targeted at routable connections?

Q&A – Current State

What We Heard

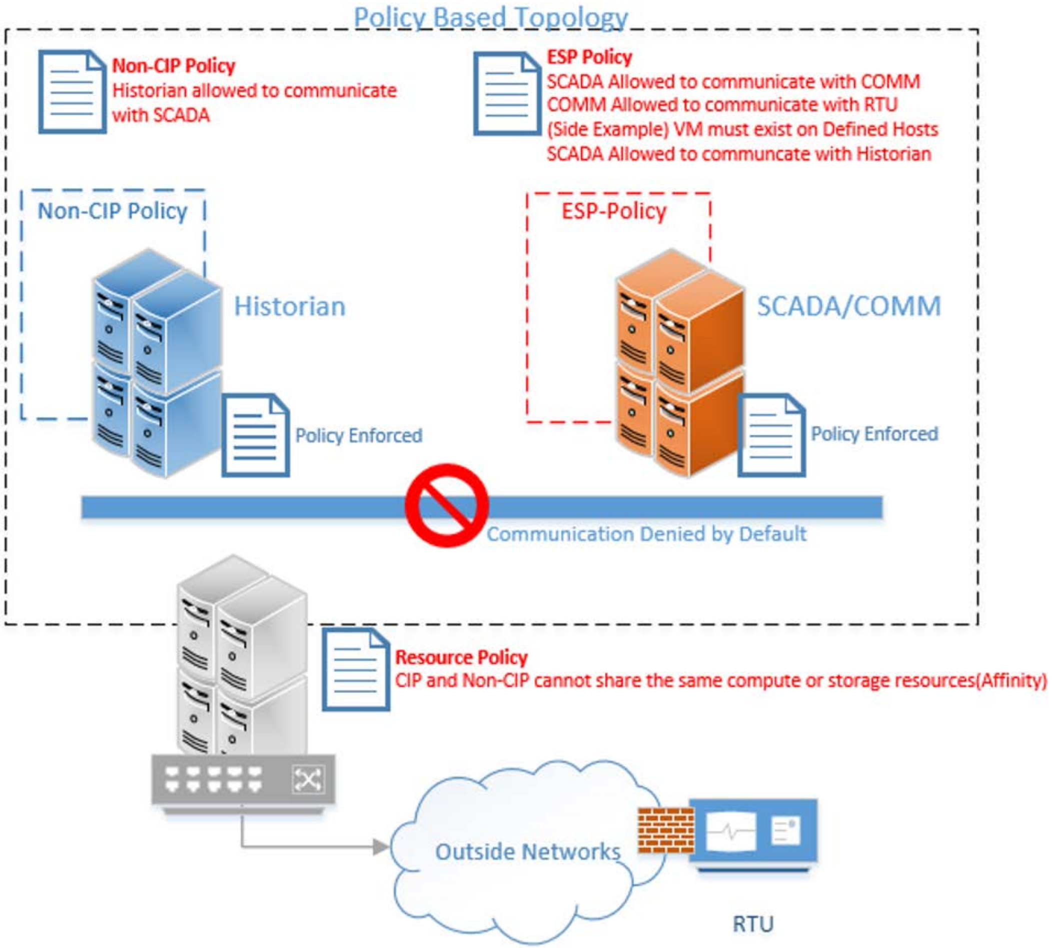
- Why change?
- Removed the “programmable” floor
- Other options to deal with virtualization
- LIZ vs. ESP
- Objective language level and clarity
- Secure Configuration scope expansion and use
- ERC as a scoping mechanism

What is the Goal?

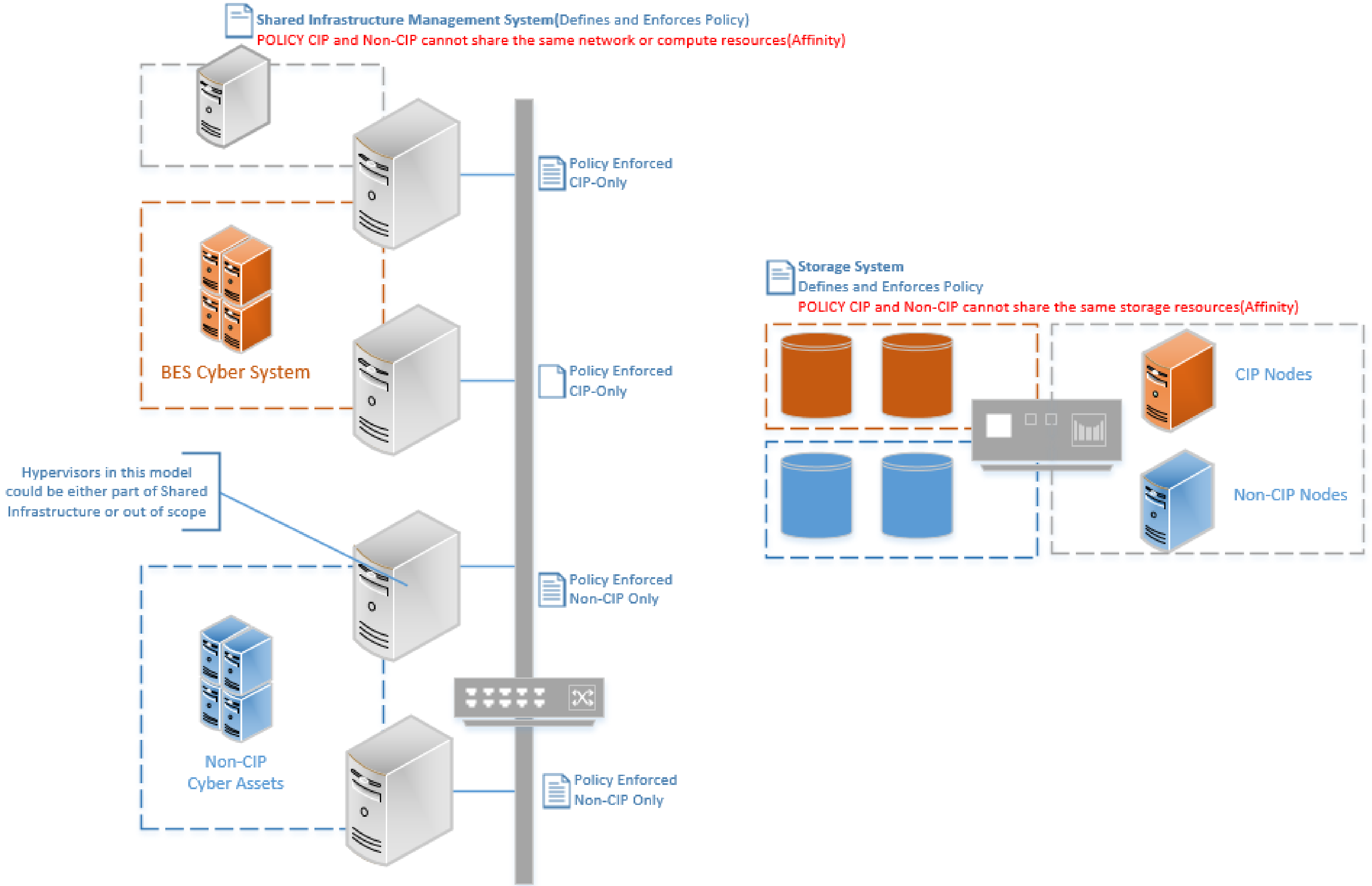
- Stabilize the standards
- To provide clarity for virtualization within the standards
- Encourage security best practices

What is the Goal?

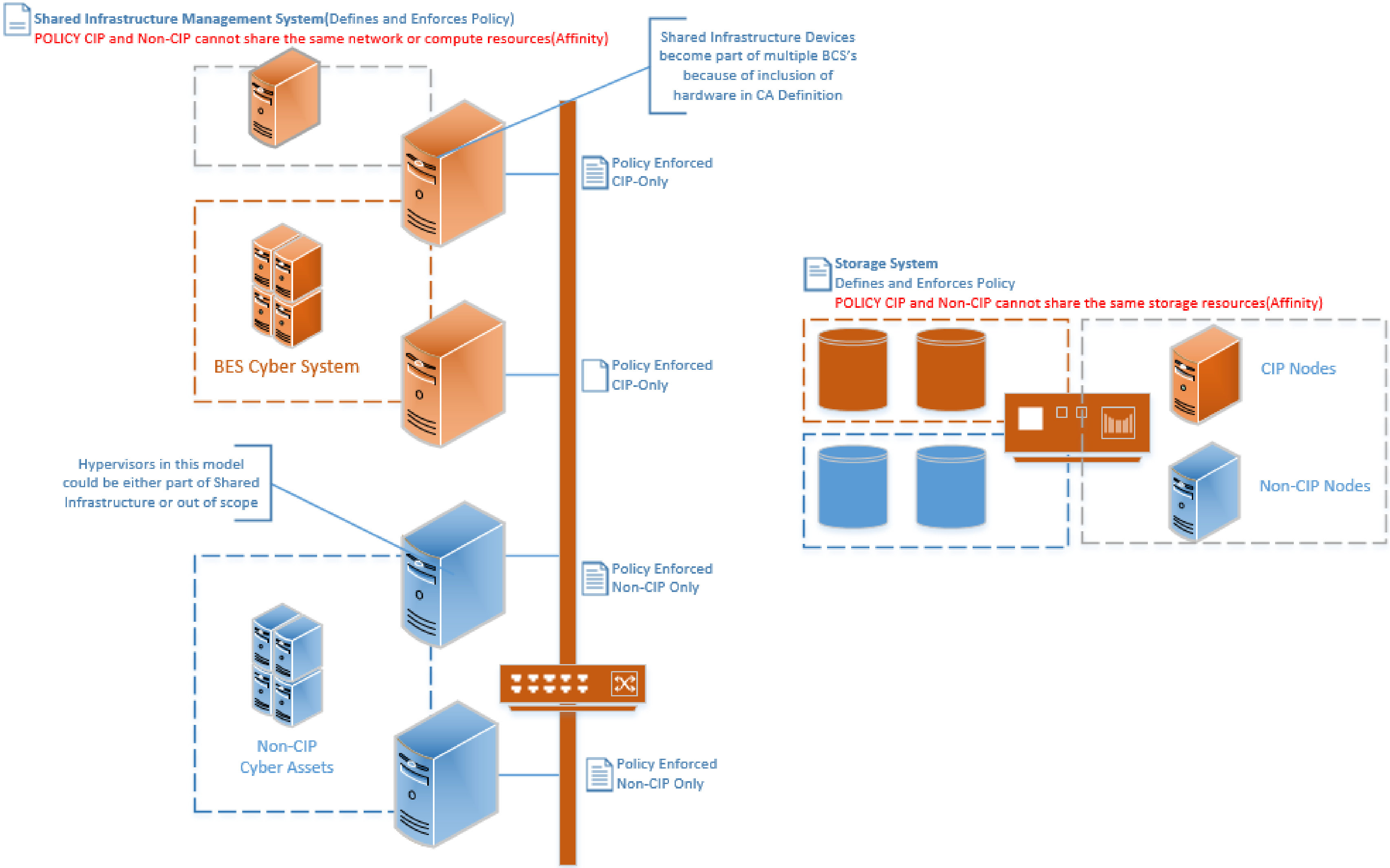
- Environments like this and many others are allowed and compliant


Policy Based Topology
Non-CIP Policy
Historian allowed to communicate with SCADA
ESP Policy
SCADA Allowed to communicate with COMM
COMM Allowed to communicate with RTU
(Side Example) VM must exist on Defined Hosts
SCADA Allowed to communcate with Historian
Non-CIP Policy
ESP-Policy
Historian
SCADA/COMM
Policy Enforced
Policy Enforced
Communication Denied by Default
Resource Policy
CIP and Non-CIP cannot share the same compute or storage resources(Affinity)
Outside Networks
RTU

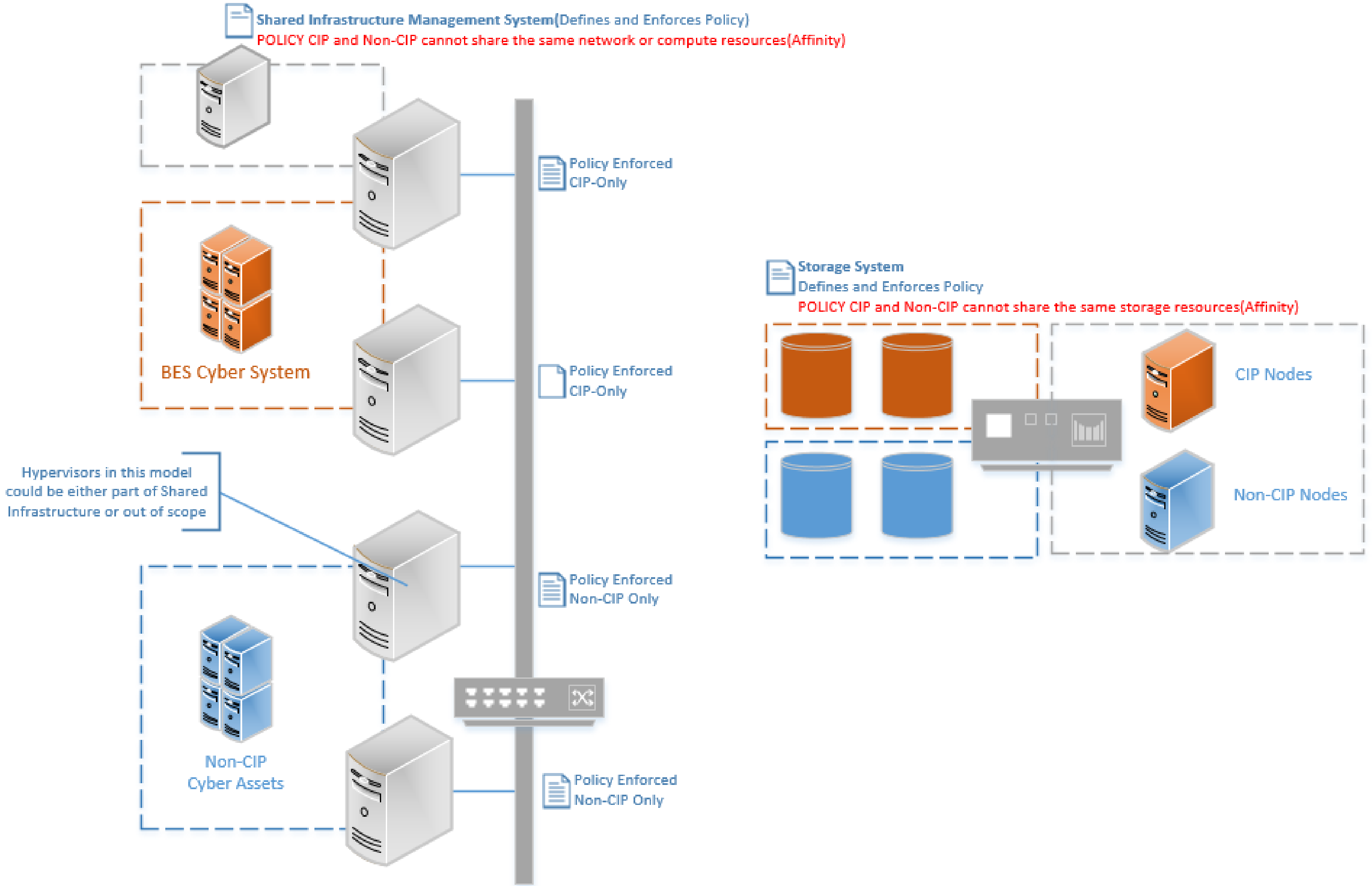
What is the Goal?


Shared Infrastructure Management System(Defines and Enforces Policy)
POLICY CIP and Non-CIP cannot share the same network or compute resources(Affinity)
Policy Enforced CIP-Only
BES Cyber System
Policy Enforced CIP-Only
Hypervisors in this model could be either part of Shared Infrastructure or out of scope
Policy Enforced Non-CIP Only
Non-CIP Cyber Assets
Policy Enforced Non-CIP Only
Storage System
Defines and Enforces Policy
POLICY CIP and Non-CIP cannot share the same storage resources(Affinity)
CIP Nodes
Non-CIP Nodes

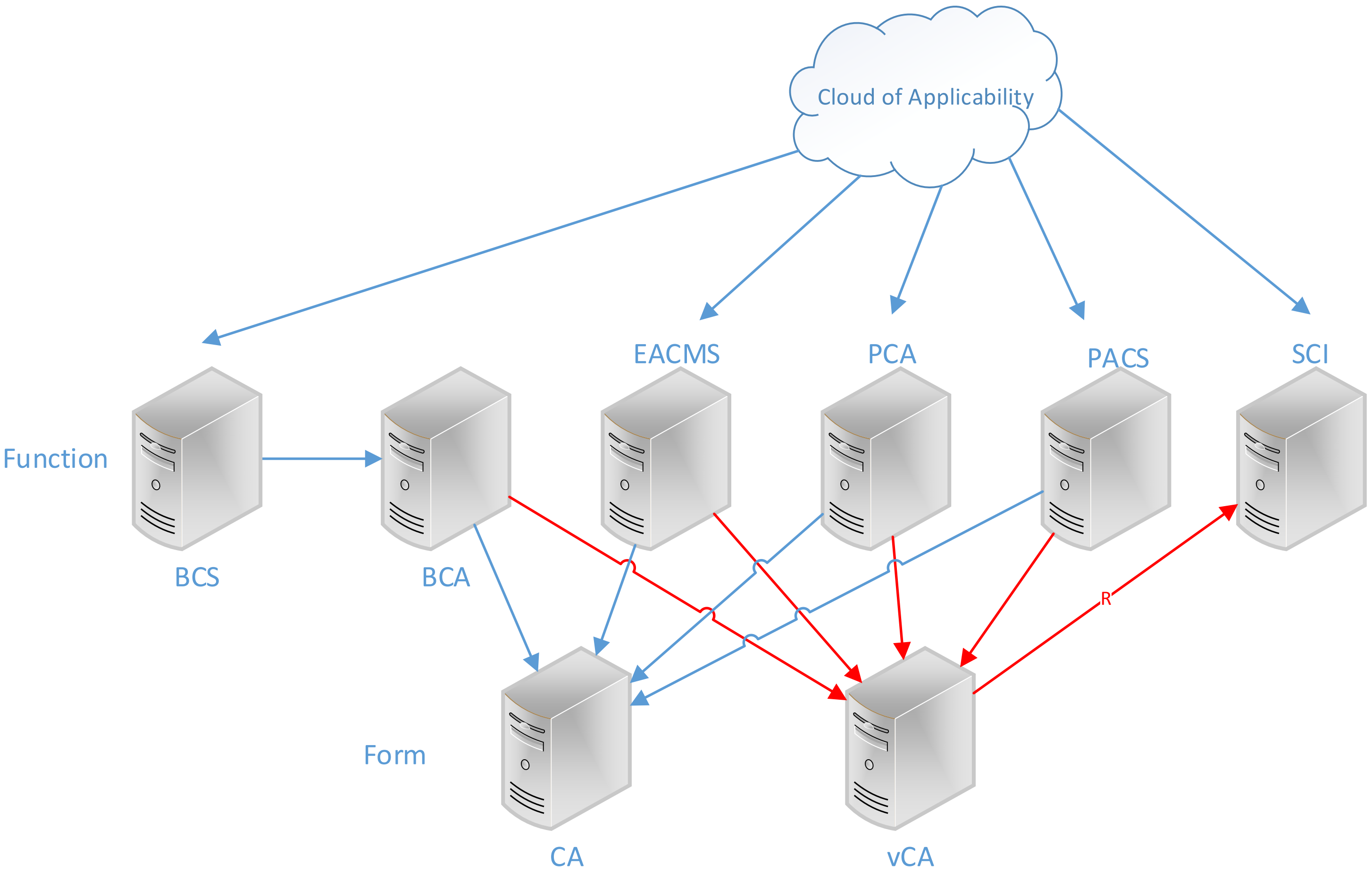
What is the Goal?


Shared Infrastructure Management System(Defines and Enforces Policy)
POLICY CIP and Non-CIP cannot share the same network or compute resources(Affinity)
Shared Infrastructure Devices become part of multiple BCS's because of inclusion of hardware in CA Definition
Policy Enforced CIP-Only
BES Cyber System
Policy Enforced CIP-Only
Hypervisors in this model could be either part of Shared Infrastructure or out of scope
Policy Enforced Non-CIP Only
Non-CIP Cyber Assets
Policy Enforced Non-CIP Only
Storage System
Defines and Enforces Policy
POLICY CIP and Non-CIP cannot share the same storage resources(Affinity)
CIP Nodes
Non-CIP Nodes

What is the Goal?


Shared Infrastructure Management System(Defines and Enforces Policy)
POLICY CIP and Non-CIP cannot share the same network or compute resources(Affinity)
Policy Enforced CIP-Only
BES Cyber System
Policy Enforced CIP-Only
Hypervisors in this model could be either part of Shared Infrastructure or out of scope
Policy Enforced Non-CIP Only
Non-CIP Cyber Assets
Policy Enforced Non-CIP Only
Storage System
Defines and Enforces Policy
POLICY CIP and Non-CIP cannot share the same storage resources(Affinity)
CIP Nodes
Non-CIP Nodes

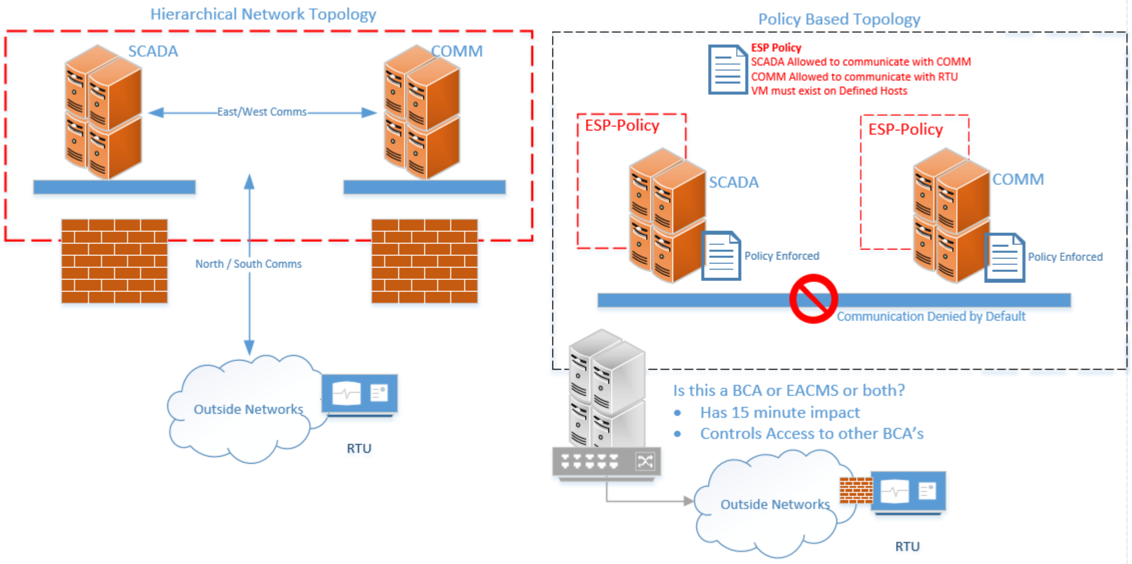
How We Can Move Forward



How We Can Move Forward

- An example of an objective requirement that clearly describes a measurable “what” but avoids prescriptive “how’s” for CIP-005 R1 could conceptually be:

  “Deny all access to and from the networks on which high and medium impact BES Cyber Systems and their associated PCAs are connected and only allow network communication that has documented access permissions including the reason for granting access.”

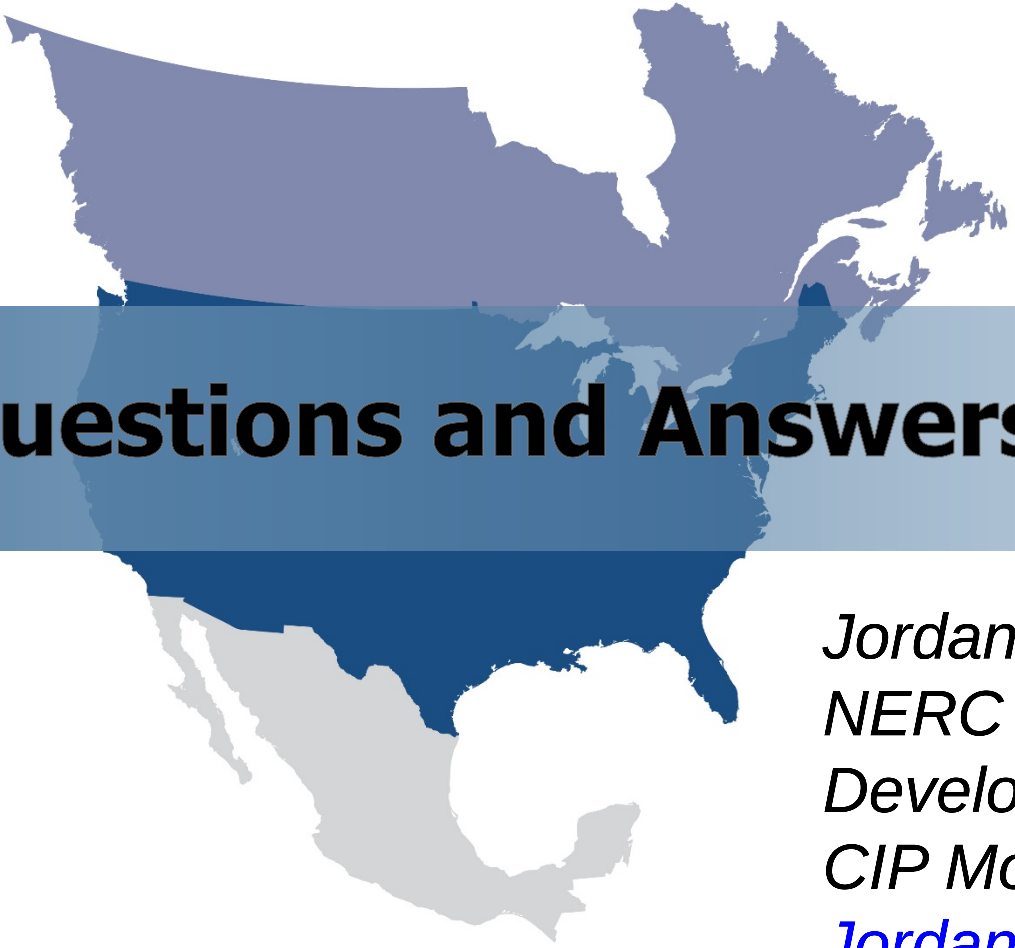

Hierarchical Network Topology
SCADA
COMM
East/West Comms
North / South Comms
Outside Networks
RTU
Policy Based Topology
ESP Policy
SCADA Allowed to communicate with COMM
COMM Allowed to communicate with RTU
VM must exist on Defined Hosts
ESP-Policy
ESP-Policy
SCADA
COMM
Policy Enforced
Policy Enforced
Communication Denied by Default
Is this a BCA or EACMS or both?
Has 15 minute impact
Controls Access to other BCA’s
Outside Networks
RTU

How We Can Move Forward

- Move toward technology agnostic requirements.
- New terms to help describe the virtual environment.
  - Clarify new requirements for the virtual environment.
- Preserve Cyber Asset term for backwards compatibility.

Next Steps

- Continue Virtualization Standard Drafting Efforts:
  - Thursday Conference Calls (noon – 2:00 p.m. Eastern)
  - May 21-23, 2019 in-person CIP SDT meeting – ERCOT
  - June 25-27, 2019 in-person CIP SDT Meeting – Tacoma Power



Questions and Answers

Jordan Mallory
NERC Senior Standards Developer for Project 2016-02 CIP Modifications
Jordan.Mallory@nerc.net