NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-005 and Zero Trust

Project 2016-02 Project Update

Project 2016-02 CIP SDT Members
February 2020

RELIABILITY | ACCOUNTABILITY

Disclaimer

Virtualization changes to CIP standards are to ***ENABLE*** new methods/models

NOT

REQUIRE Them

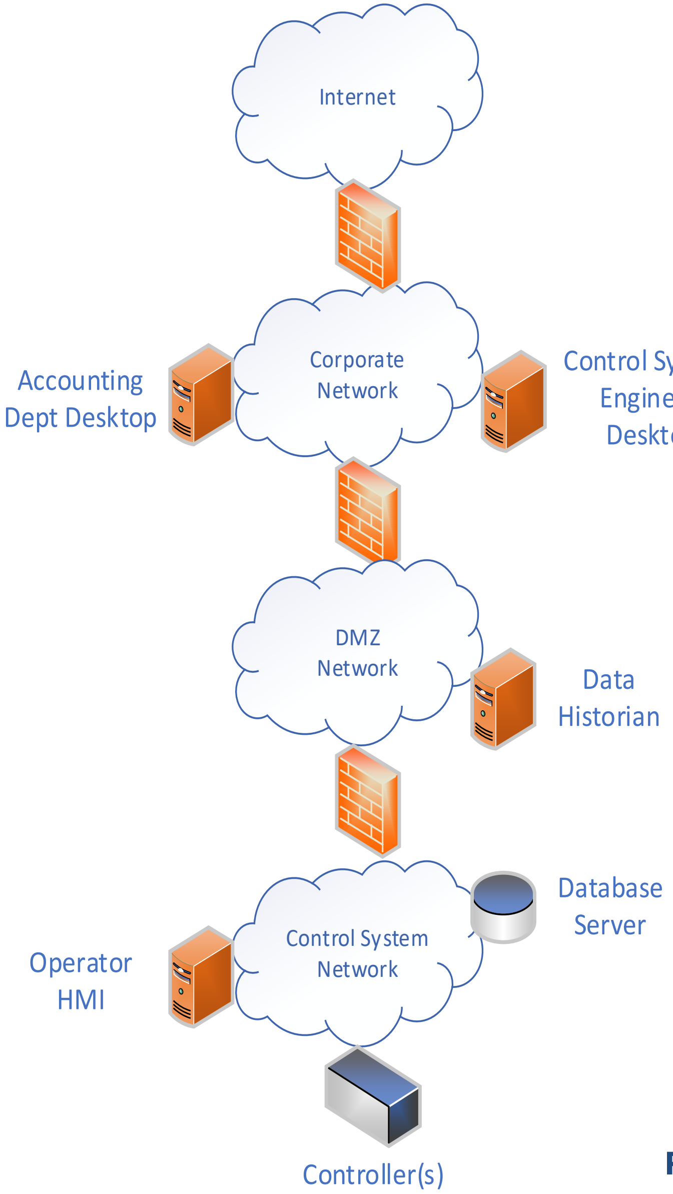
Agenda

- Discuss current security state and issues
- Discuss emerging security models (Zero Trust)
- CIP-005 changes to allow ESP plus other models

Current State

- Network Perimeter (ESP) based
- Castle & Moat
  - Everything inside the castle = good
  - All the bad is outside the castle
  - The moat (FW) provides separation and controlled access
- ***Trust is based on your network location***
  - Internet, Corporate network, DMZ, ICS network, Controller network
  - Your trust level = Which perimeter are you within
  - Security controls are mostly for North/South traffic (crossing perimeters)
  - All your network peers are same trust level (PCAs in CIP)
  - East/West traffic within the perimeter has no security controls

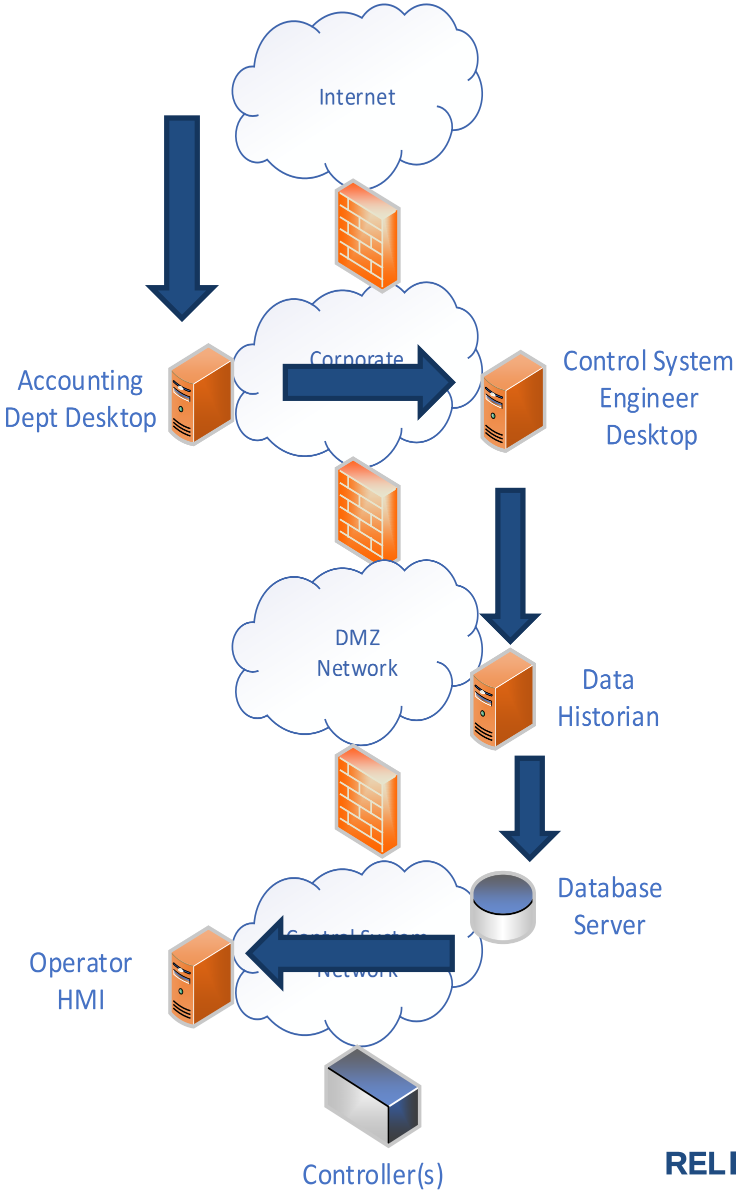
Typical Network Model



Issues

- Adversaries are intelligent and adaptable
- As perimeter model improved -> Attackers adapt and hack the humans instead (phishing, watering hole attacks, etc.)
- Result – **the "inside" is also hostile** and the model provides for easy lateral movement (network access controlled at perimeter, not inside)
    - Ransomware – get on one system inside and then destroy 30,000 PCs from within your perimeter

Typical Security Breach



Other Perimeter Issues

- Remote access, VPN, Cloud services, Vendor access, etc.
  - The true perimeter is very dynamic now
  - The data historian – may be a cloud service in the future
  - VPN – the purpose is to essentially “put a remote machine on the local network”
- “Inside” and “outside” a perimeter – is there a another better way to think about network security models?

Virtualization Enables Other Models

- Virtualized environments are enabling new and different ways to think about network security to address these issues
- Security controls – network or host
  - Network – isolation, but lose context
  - Host – context but not isolation
- Enter the Hypervisor with ubiquitous context

Zero Trust Architecture

- *New and evolving security strategy* that **fundamentally** changes networking from implicit trust to zero trust
- ***The basic premise is there is no implicit trust granted to systems based on their physical or network location***
  - Treats EVERY network as hostile (thus the zero trust name)
  - DOESN'T CARE what network address you have or where you are
  - DOES CARE who you are as a person or process, the state of your machine, whether you are authorized RIGHT NOW for what type of access to the particular data or resource
  - ALL traffic is encrypted/protected because no network is trusted
- ONLY authorized communications are allowed

Security Breaches in Zero Trust

Zero Trust Model

- Assumes ANY network is hostile - NO implicit trust
- Access granted only when access needed and only for duration of access
- Authorize the user and device at the time access is needed
- Protects resources and data, *not network segments*
- Network location is no longer a prime component of security posture
- Attacker reconnaissance and lateral movement mitigated
- This is a **fundamentally** different model than ESP

Policies and Zones

- Network segments and perimeters replaced with policies and zones
- Based on “need to know” preconfigured access policies
- Protects access to data, assets, applications, and services, not network segments
- Policies can include machines, users, processes, services *regardless of where they are on a network*.
- “Policy not Topology”

Policy Example

- Individuals in AD group “Historian_Access” on a device with OS=“Windows” can only use TLS-Version =“1.2” encrypted communication to access workloads with Tag= “Control_Historian_APP”
- This policy defines allowed communications
  - With no reference to where anything is on a network
  - An encrypted temporary “network” is established between the user wherever they are to the historian app wherever it is
  - No other communication allowed
  - Policy is enforced end to end and everywhere in-between

CIP-005

- Current
  - 1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
  - 1.2 All External Routable Connectivity must be through an identified Electronic Access Point.

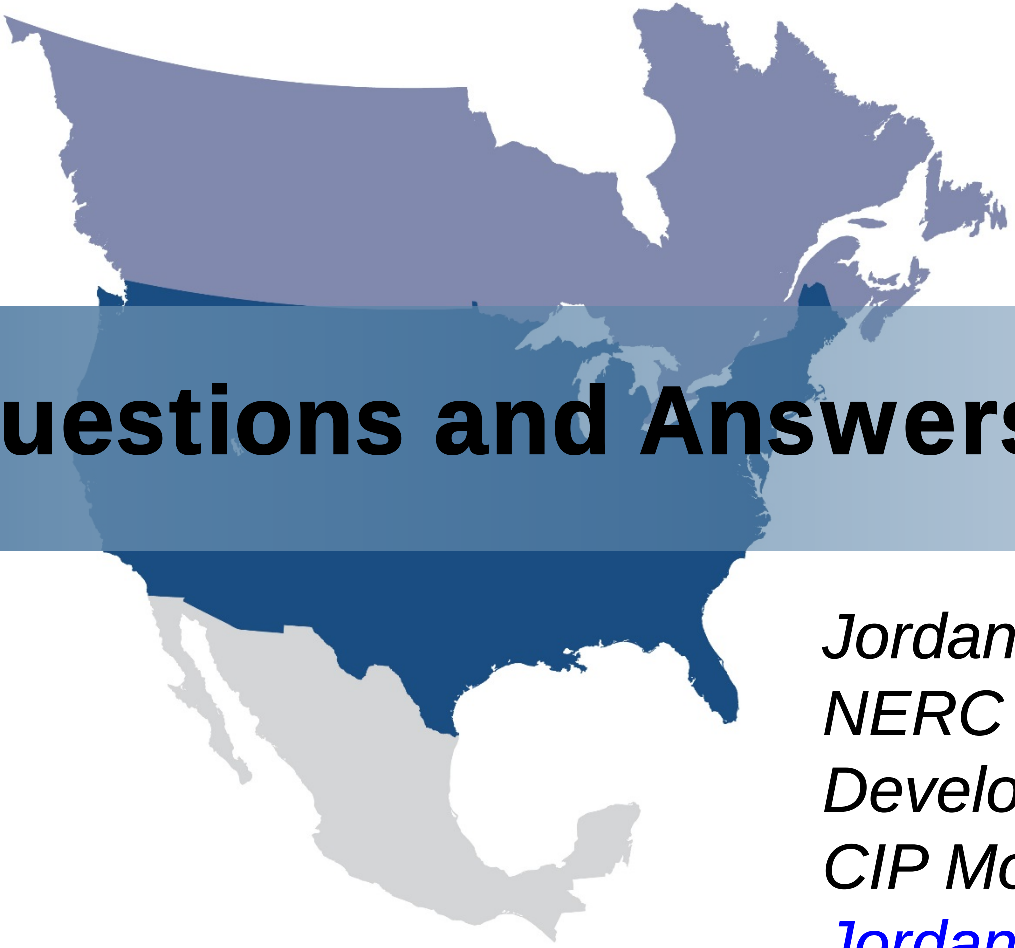
- Proposed
  - 1.1 Have one or more methods for allowing only needed and controlled communications to and from applicable systems either individually or as a group and logically isolating all other communications.

Hybrid Models

- Typically not “either/or” network models
- Hybrid environments will be the norm
- Security objectives allow for current/future/hybrid models

ESP Conforming Changes

- PCA
    - Current – One or more Cyber Assets connected using a routable protocol within or on an ESP…
    - Proposed – Cyber Assets that are not logically isolated from a BES Cyber System…
- 4.2.3.2 Exemption
    - Current – Cyber Assets associated with communication networks and data communication links between discrete ESPs.
    - Proposed – Cyber Assets associated with communication links logically isolated from BES Cyber Systems or SCI.



Questions and Answers

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