October 30, 2018

Boundary Protection for Transmission Facilities

CIGRE 2018 GOTF

Presented by: Jeff Pack

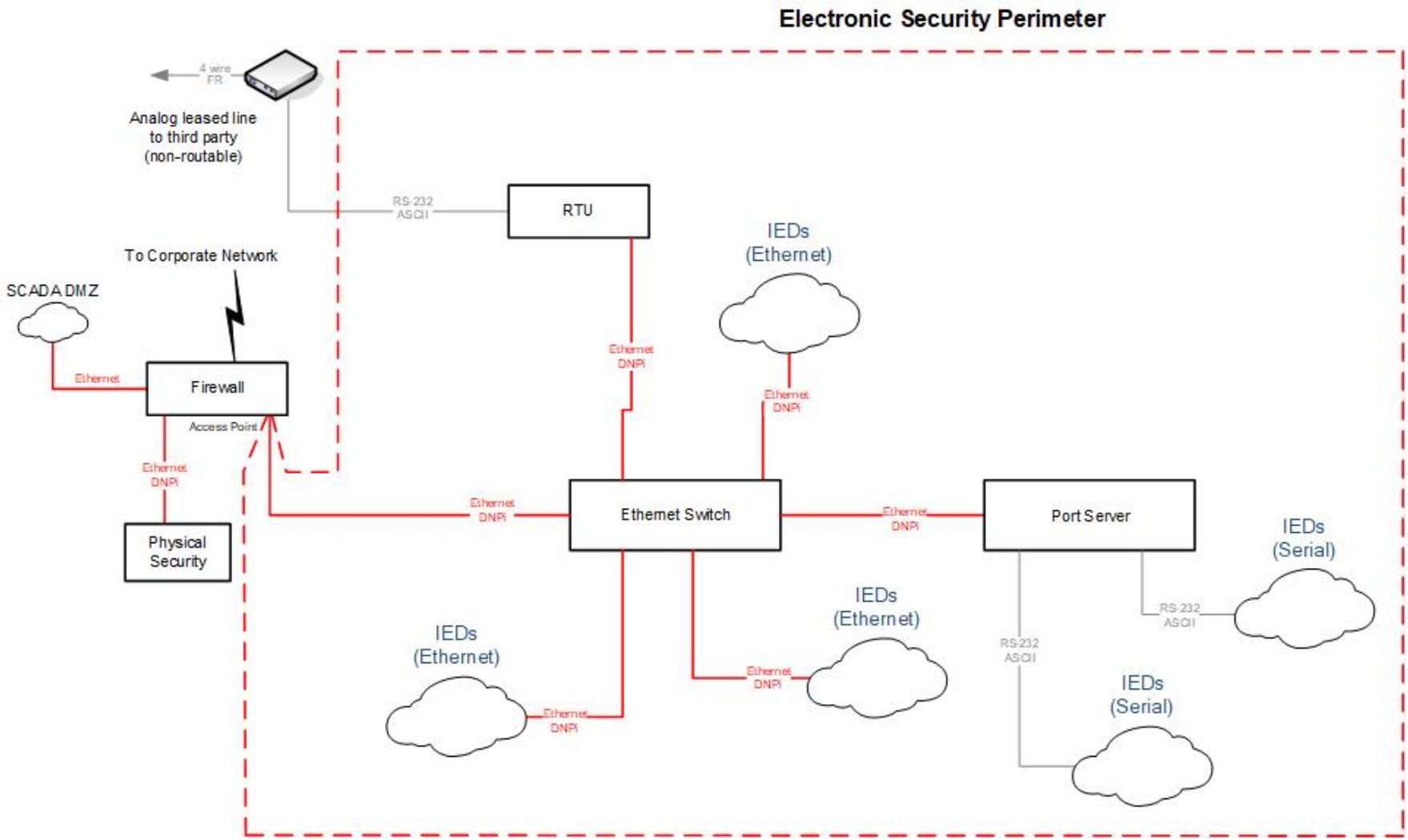
Agenda

Introduction	» What is the issue?
Boundary Protection	» Incorrect configuration and excess access
Logical Separation	» Inadequate separation from other networks
Jump Server	» Eliminate direct connection to ICS devices
Authentication	» Use of common authentication credentials
Network Services	» Excessive network services
System Maintenance	» Access to vendor networks for maintenance

Introduction

» Boundary Protection
  – NERC CIP-005
» Historical References
  – Firewalls and Internet Security, 1994
    • Cheswick and Bellovin
» Why is this still an issue?
  – Hard to maintain secure configuration
  – Increased dependence on network services
  – Increased exposure of ICS vulnerabilities

Boundary Protection



Boundary Protection

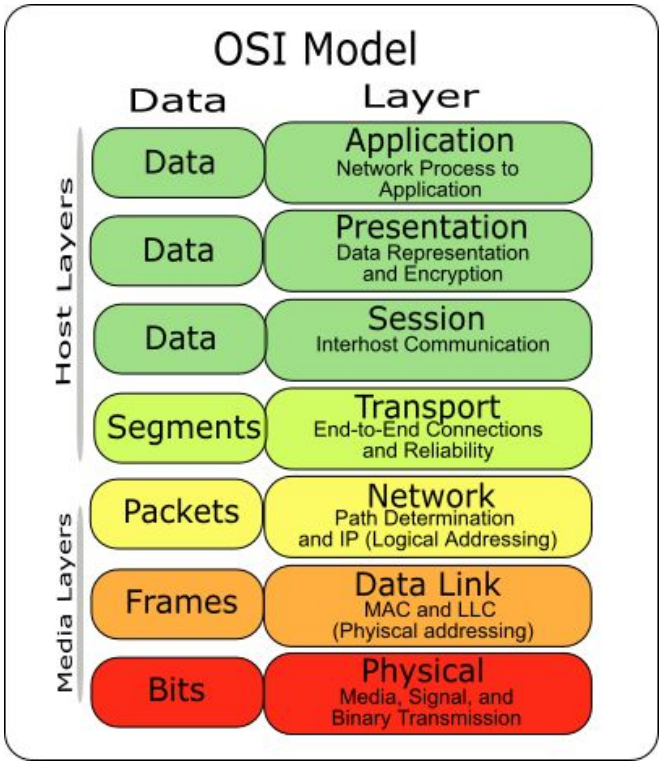
» Firewall
- Limited to pre-defined devices and services
- Review and approve all firewall changes
- Only enable operational requirements
- Beware of global parameters

» Dial-up Connection
- Use authentication
- No remote access – data only

Logical Separation

» Look at each layer in the network

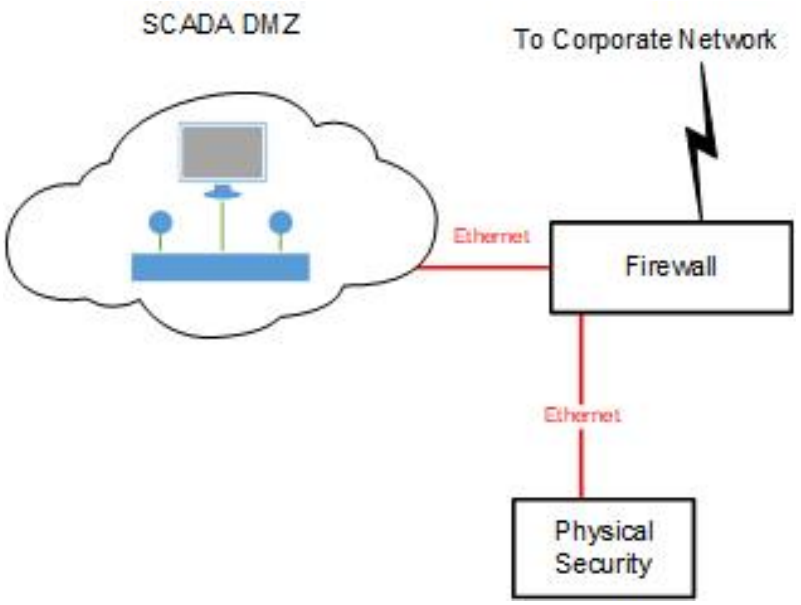
- Layer 2
  - VLAN
  - GOOSE
  - ACL
- Layer 3
  - Deny by default
  - Fail to known state
- Layers 4-7
  - Least privilege
  - Configuration management



Jump Server for ICS Access

» Why a Jump Server
  - Eliminate direct connection to IEDs
  - More restrictive firewall rules
  - Enables authentication and encryption

» Required for High and Medium BES Cyber Systems



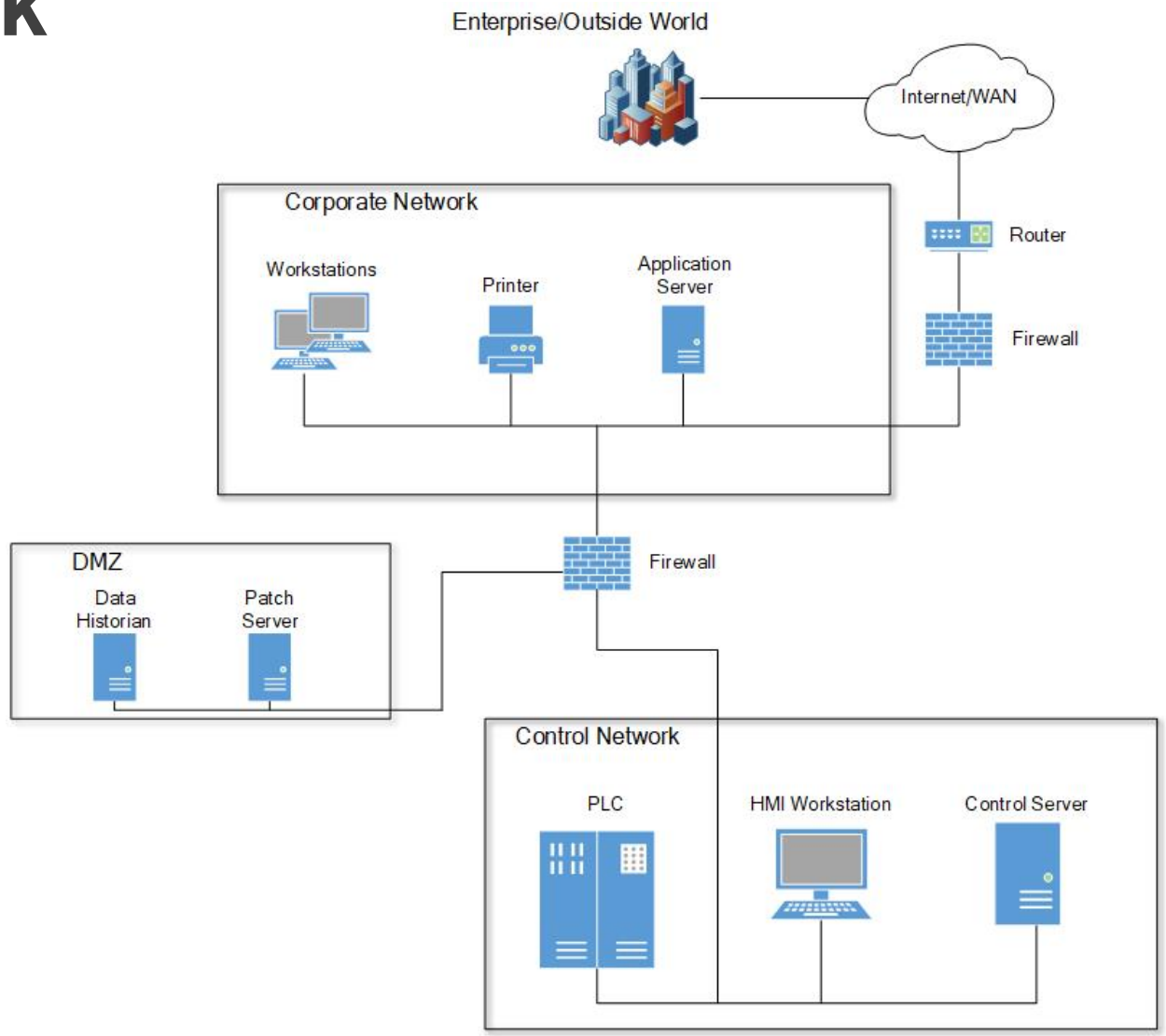
Authentication

» Separate credentials and domains for business and control system networks
  - Reduce probability of credential harvesting
  - Reinforce differentiation of control network

» Centralized and local accounts
  - Rapid credential management response
  - Review local account automation systems

DMZ Network

» Limit access to ICS support servers
  - Don't manage like other servers
  - Treat as protected devices
  - Default deny



ICS System Maintenance

» No outbound access for IEDs
  - Software/Firmware updates
  - Anti-Malware signatures

» Provide Services in DMZ
  - Patching
  - Data Historian
  - Jump Server
  - Reduce transient cyber asset risk

Summary

- Introduction
- Boundary Protection
- Logical Separation
- Jump Server
- Authentication
- Network Services
- System Maintenance

» Review Boundary Controls

» Review architecture

» Test for effectiveness and response

Thank you