



Western  
Area Power  
Administration

# WAPA Cyber

James Ball-CISO

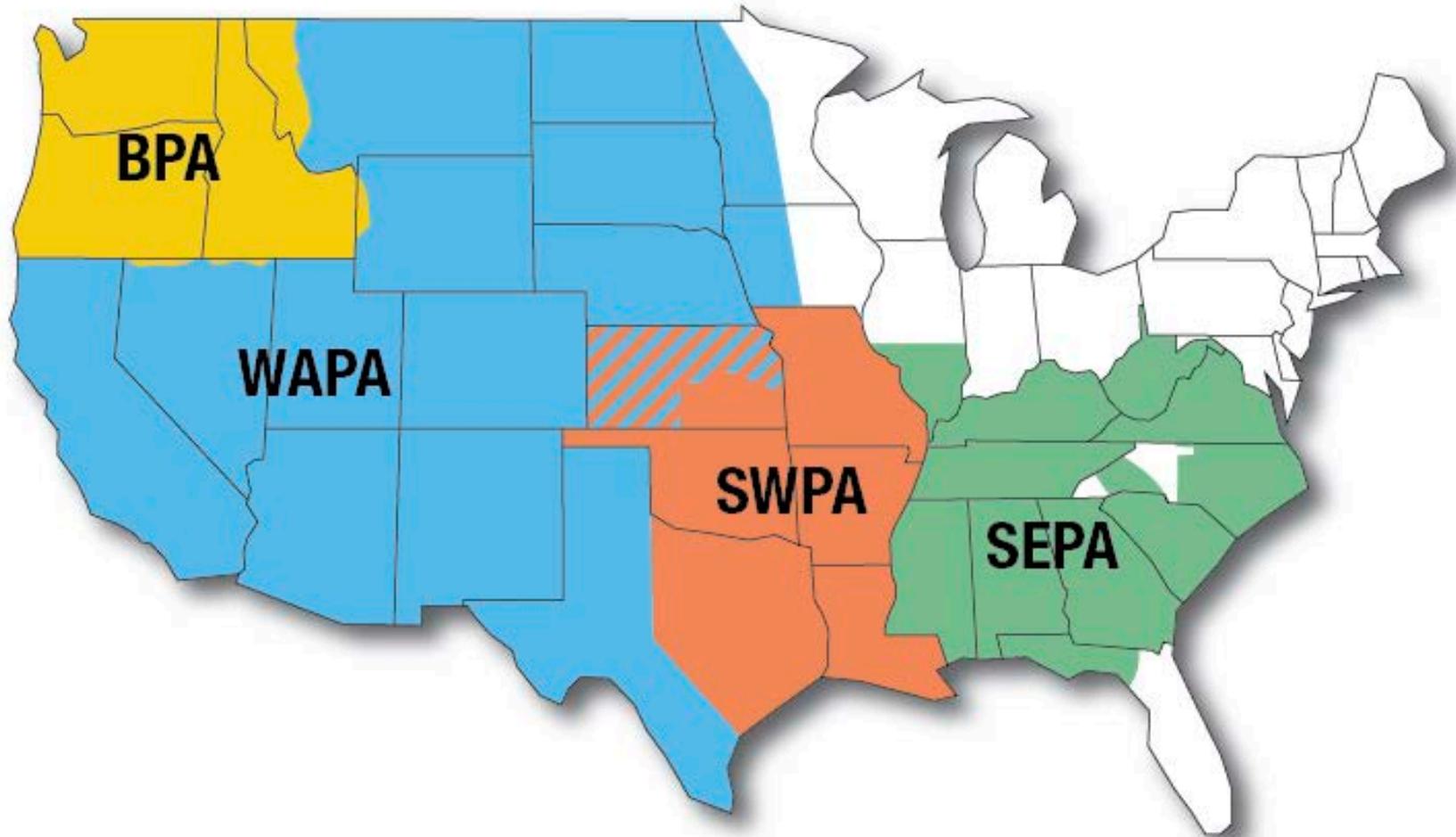


Date

Technology and Security Symposium

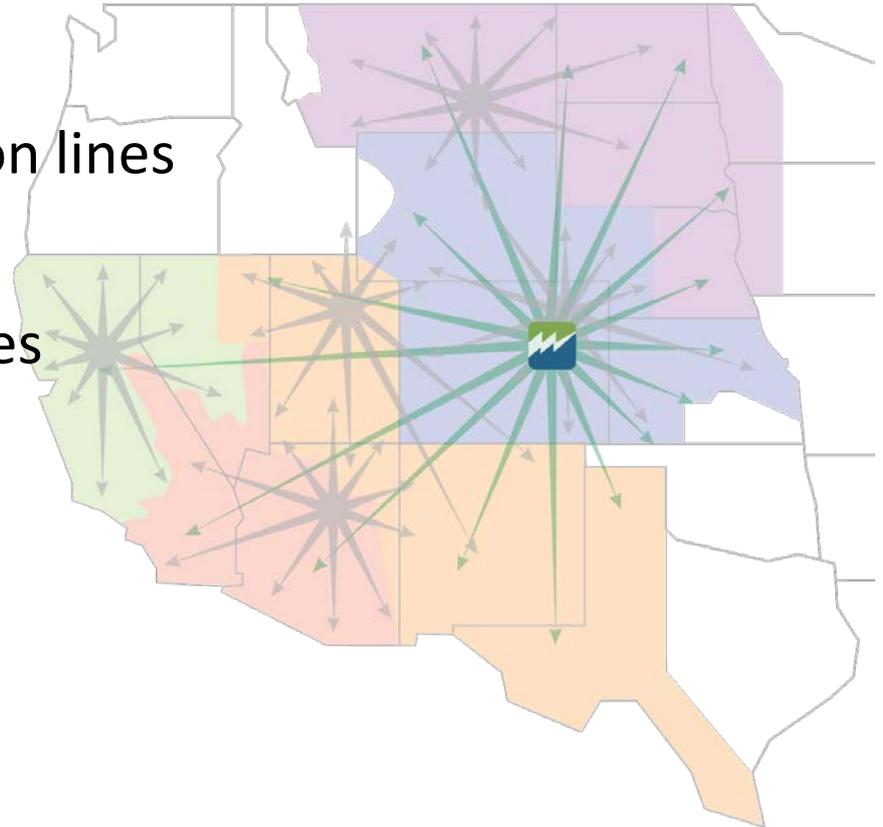
Denver, Colorado

# Power Marketing Administration



# WAPA Footprint

- Power distribution from 56 federal hydropower plants
- 15 western states
- 17,000 miles of transmission lines
- 320 substations
- 500 communication facilities
- 4 SCADA operation centers



# Part of DOE



- Both USG and NERC Cyber Governance
- Broad Audit Landscape
- Standards and Controls Conflicts
- But-Immune from enforcement



# What Do We Do and How Do We Do It ?

- The Business Network is the Gateway
  - Scrutiny of Traffic- Left, Right, and Sideways
    - Visibility
  - Configuration and Change Control
  - Training and Hygeine- User Behaviors
- Support from our Partners
- After Seven Years.....



# The Greater Challenge

- The World of Substations and SCADA
  - Scrutiny of Traffic- Left, Right, and Sideways- Hard
    - Visibility
  - Configuration and Change Control
  - Protocols, Bandwidth, Architectures
- Built to Run- Yes
- To Be Observed- Not So Much
- Another Seven Years ?
- Partners



# OT Remote Connectivity Requirements

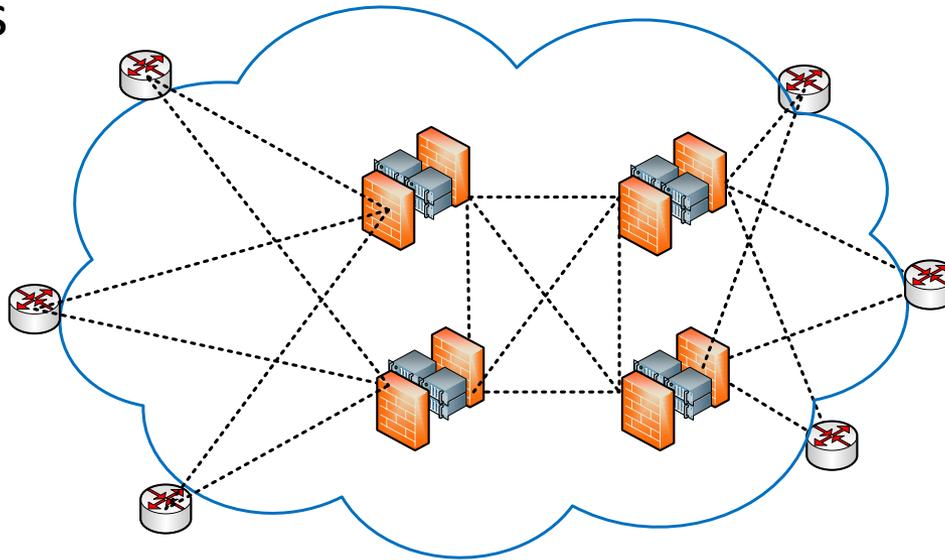
- Substations and communication facilities in remote sites
  - Several sites require a full-day trip to work on-site
  - Some sites are only accessible via helicopter or snowcat
- Windshield time is very costly
- Need instant access to outage details
- Asset management
- Reliability Centered Maintenance (RCM)





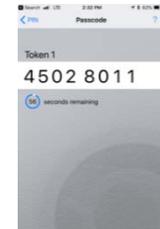
# SESC Topology

- Four geographically disperse mesh-interconnected SESC cores
- Each substation/comm site is connected to 2 SESC core sites
- Logical network overlaid on top of GSS physical network
- Encrypted communication channels
- Virtual Machine infrastructure for quick deployment of systems



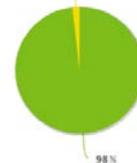
# SESC Services

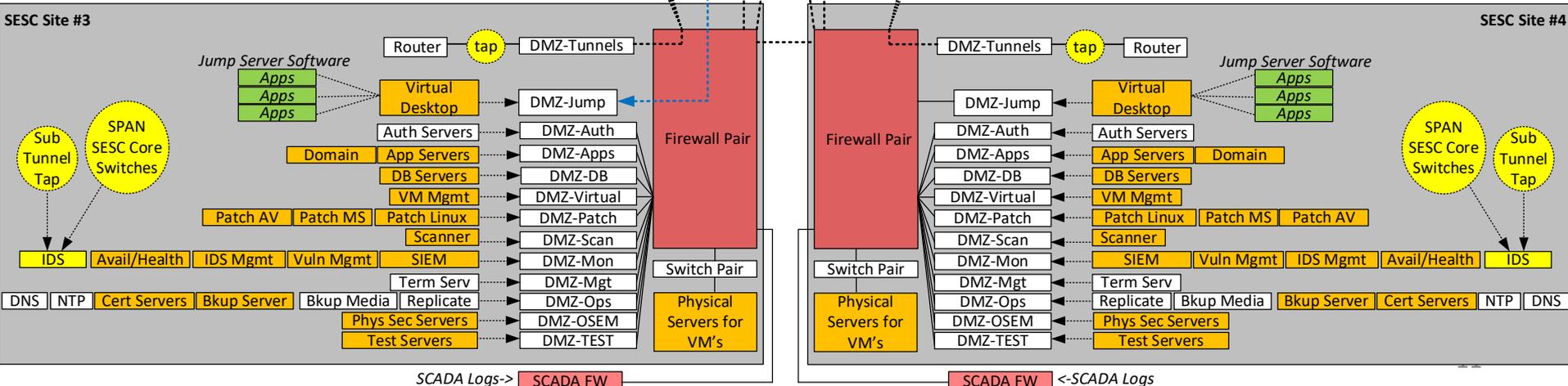
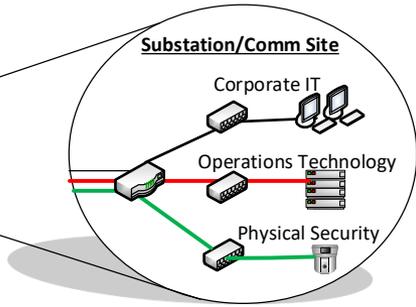
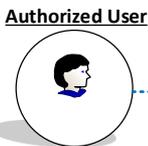
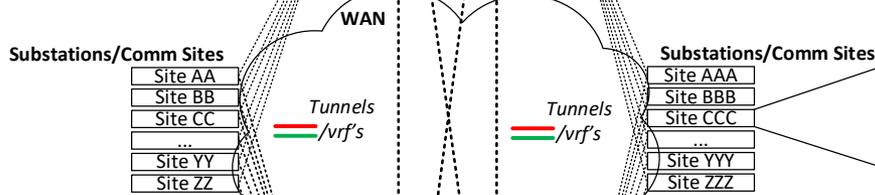
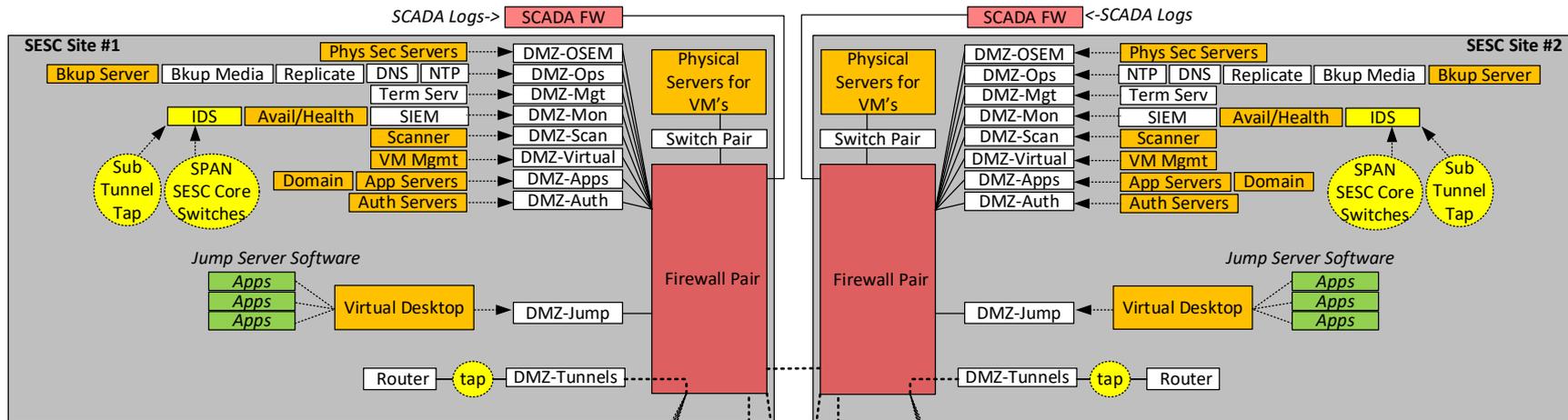
- Secure remote access to OT infrastructure via intermediate systems
- Multi-factor authentication tokens
- Dedicated authentication and account management services
- Security Information and Event Management (SIEM)
- Vulnerability management system
- IDS/IPS
- Patching
- Availability / health monitoring
- System backup and recovery
- System baselining
- Dedicated NTP/DNS/IPAM/CA



Overall Devices Backed Up vs. Not Backed Up  
AS OF LAST UPDATE

■ Backed Up  
■ Not Backed Up





SCADA Logs-> SCADA FW <-SCADA Logs

# A Final Note- What Can You Do

- CRISP
- CMA
- EISAC
- Participate and Share
- Partner !



# Questions?

**James Ball**

Chief Information Security Officer  
Western Area Power Administration  
720-962-7572  
ball@wapa.gov

