# PSCR2021 THE DIGITAL EXPERIENCE #PSCR2021 • PSCR.GOV







How to Manage a World Class Public Safety Communications Research Network

Wyatt Suess - Network Engineer



#### DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

\* Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change









#### INTRODUCTION







4

# ACRONYMS

- 4<sup>th</sup> Generation (4G)
- 5<sup>th</sup> Generation (5G)
- Augmented Reality (AR)
- Demilitarized Zone (DMZ)
- E-UTRAN Node B (ENB)
- Evolved Packet Core (EPC)
- Inter-Radio Frequency Subsystem Interface (ISSI)
- Intrusion Detection System (IDS)

- Intrusion Prevention System (IPS)
- Land Mobile Radio (LMR)
- Long Term Evolution (LTE)
- Mission Critical Push to Talk (MCPTT)
- Power over Ethernet (PoE)
- User Equipment (UE)
- Virtual Machine (VM)
- Virtual Private Network (VPN)
- Virtual Reality (VR)

#### **PSCR NETWORK OVERVIEW**



#### **PSCR PHYSICAL ARCHITECTURE**



#### **PSCR LOGICAL ARCHITECTURE**



# LTE TESTING ZONE

- Aligns with our original network configuration
- Minimize traffic through the firewall
  - Increase speed
  - Traffic stays within core/distribution layer
  - Traffic does not need to be inspected
- Multi-vendor equipment/systems:
  - eNB's
  - 4G/5G core
  - MCPTT
  - Load testers

#### **PSCR LOGICAL ARCHITECTURE**



#### LAND MOBILE RADIO (LMR) ZONE

- Securely connect an isolated system to our network
- Connection to AT&T for the Enhanced Push-To-Talk service
- Three vendor Interworking Function systems that need to communicate with the LMR system
- Presents challenges with scheduling time blocks to test
- Challenge of licensing, 2 ISSI connections
- Automated firewall configuration on LMR side to comply with licensing and allow for testing time blocks

#### **PSCR LOGICAL ARCHITECTURE**



#### **DEPLOYABLE NETWORK**

- Sits outside the main PSCR network
- Each deployable system consists of a firewall, switch, virtualization server
- Often taken off network for exercises
- Isolated from the rest of the lab



#### **PSCR LOGICAL ARCHITECTURE**



### WORKSTATION/LAPTOP ZONE

- Primary zone for our research engineers
- Provides enough access to perform research:
  - Allows access to testing zones and equipment
    - LTE cores
    - eNB's
    - Internal web services
  - Restrict access to network management systems
- Isolated from testing equipment for security purposes

#### **PSCR LOGICAL ARCHITECTURE**



# **VR/AR DEVELOPMENT ZONE**

- Similar to the workstation/laptop zone
- Use of gaming applications normally prohibited
- Consist of:
  - Laptops
  - Workstations
  - Virtual machines
  - Specialized VR equipment

#### **PSCR LOGICAL ARCHITECTURE**



#### **QUARANTINE ZONE**

- Provides limited network and Internet access
  - Bandwidth restrictions
  - Allows for scanning the device
  - Apply secure configurations
- Primarily used for deploying UE devices and placing devices back on the network
  - Activate new UE device
  - Check for updates

#### FLEXIBLE USER ENVIRONMENT





More diverse projects



Change architecture to more specific security zones



Allows for better security and flexibility in our deployments

#### HIGHLY VIRTUALIZED

- Following industry trends
- Physical servers have become virtualized
- Evolved Packet Core
- Network Function Virtualization
- Easy to backup and provides flexibility
- Lower operating costs and efficient management

VM1	VM2	VM3	VM4
VM5	VM6	VM7	VM8
Hypervisor			
Physical Server			

#### **ADJUSTMENTS IN RESEARCH**



#### **Pre-Pandemic**

- Testing took place in the lab
- Remote vendor access

#### Pandemic

- Employee & vendor remote access
- Relies on VPN groups
- Screen sharing tools



#### **DEPLOYMENT PROCESS**



#### **STEP #1 TICKET SUBMISSION**

- Alerts network operations staff of new deployment
- Provides historical documentation of project
- Tracks project throughout life cycle



#### **STEP #2 DEPLOYMENT MEETING**

- Meeting with lab operations and security team
- Discuss deployment in detail
  - Power requirements
  - Network requirements
  - Interconnections with other systems
  - Patching requirements
  - Other special requirements



#### **STEP #3 CREATE OR ADD TO SECURITY ZONE**

- Segment network traffic to/from system
- Avoid unnecessary traffic
- Help secure specialized or legacy systems



#### **STEP #4 INSTALLATION**

- Add equipment to inventory
- Racking of equipment
  - Power
  - Ethernet/Fiber
  - Rails
- Installation of operating system and applications
- System hardening



#### **STEP #5 VULNERABILITY ASSESSMENT**

- First vulnerability scan on the operating system
- Scans Windows or Linux machines
  - Overview of current state of system
  - Open ports
  - Active vulnerabilities
  - Mitigations



#### **STEP #6 FINAL VULNERABILITY/COMPLIANCE SCAN**

- Final vulnerability scan
- Compliance scan
  - Scan security settings and compare to a baseline configuration



#### CONCLUSION









**Deployment Process** 

# THANK YOU

A 003 A 004

#PSCR2021 • PSCR.GOV