Pragmatic Security

Security Reference Architecture

AKA Protection Level Topology

Ernie Edmonds CISSP SSCP CAP MCSE MCSA FSCA CEH CSEPS
Senior Managing Consultant | CMTC
May 2023

CMTC®
California's Manufacturing Network

Pragmatic Security

Agenda:

This session will not follow the normal structure.

- Concepts ~15 Minutes
- Exercise ~15 Minutes
- Q/A ~Remaining Time
- Caution- Heavy Technical Ahead!

CMTC
California's Manufacturing Network

Why This Session?

The CMTC Security Reference Architecture(s) provide an extensible and scalable framework to support the following requirements:

- CMMC CM.3.068 / NIST SP800-171r2 Requirement 3.4.7
  - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
- CMMC SC.3.180 / NIST SP800-171r2 Requirement 3.13.2
  - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
- CMMC SC.3.183 / NIST SP800-171r2 Requirement 3.13.6
  - Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

There are nine (9) CMTC Security Reference Architectures. We will be covering **Model 6**

CMTC California's Manufacturing Network

Security Reference Architecture

- Process
  1. Choose a competent Firewall and Network Components
  2. Determine Existing Puzzle Pieces
  3. Determine Where they Currently Exist
  4. Determine Where They Live in a Perfect State
     - Particular Attention to CUI, IP, and Company Sensitive
     - Particular Attention to General Support Systems such as DNS, NTP, and other External Support Systems. (MOST RESTRICTIVE)
     - Use Aliases if you can- MODULAR CONSTRUCT
  5. Delete All Existing Rules!
  6. Determine Which Roles *NEED* to talk to which roles and provide one-way rules for each *NEEDED* instance.
  7. Build it to Perfection- nothing is too granular.

Security Reference Architecture

- Rules:
  1. Level Hopping Is Prohibited
  2. Refer to Rule #1

- Firewall Constructs that are Important to Understand
  – Aliasing (Many (but not all) firewalls support this- *GREAT if so!*)
  1. External GSS Alias
     A. DNS = Risk Remediated DNS 1 and 2 per CMMC SC.3.192 (Implement Domain Name System (DNS) filtering services.)
     B. NTP = Trusted NTP Server per CMMC AU.2.043 / 800-171r1 3.3.7 (Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit logs.)
  2. Allowed External (Allowed_External)
     A. Create GEO_IP/GEO_BLOCK Alias
     B. Add all countries
     C. Deselect the countries you don't ever want to connect with (This will also block them from connecting to you)
        A. Russia and other former Soviet blocks
        B. Western Samoa and other known sources for malware
        C. Iran, Iraq, Yemen, Somalia, Syria, and other terrorism hotspots
        D. North Korea, Vietnam, Cuba, Venezuela, others with non-US stances
        E. Others as you see that there will never be a need

CMTC California's Manufacturing Network

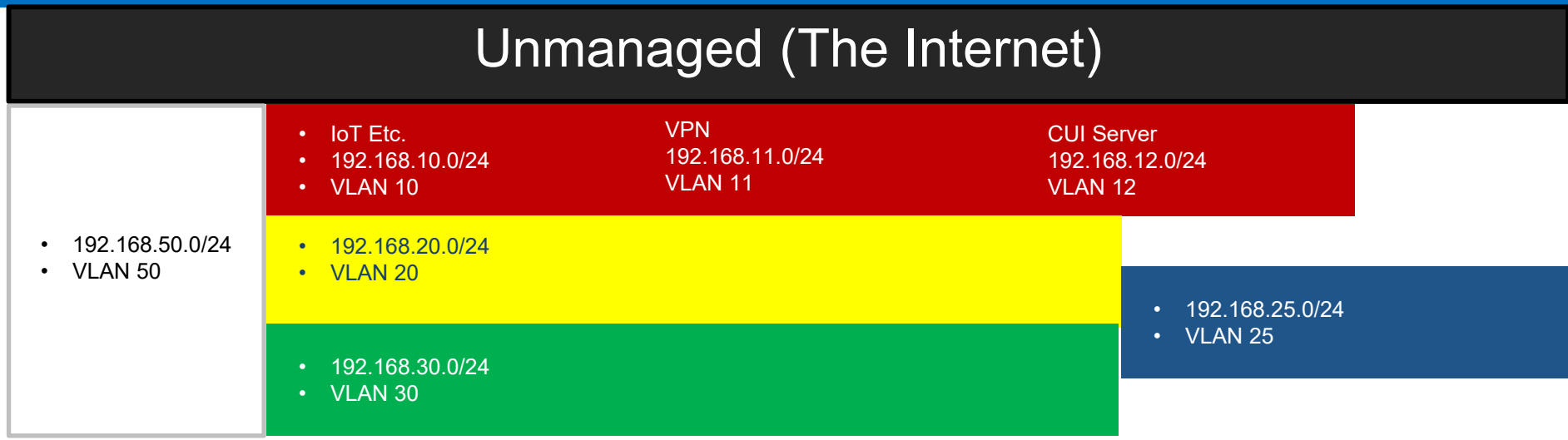
Security Reference Architecture

- Firewall Constructs that are Important to Understand
  - Aliasing (Continued)

1. Host Alias
   A. Can be IP address based.
   B. Can be Fully Qualified Domain Name based (FQDN) or Relative Domain Name based (RDN)
   C. Can Contain more than one- This is called a Range

2. Protocol Alias
   A. Always includes the port number.
   B. Can contain the Transmission Type (TCP,UDP, ICMP, All)
   C. Will Allow multiple protocols to be grouped into one named group which is MUCH easier for humans.

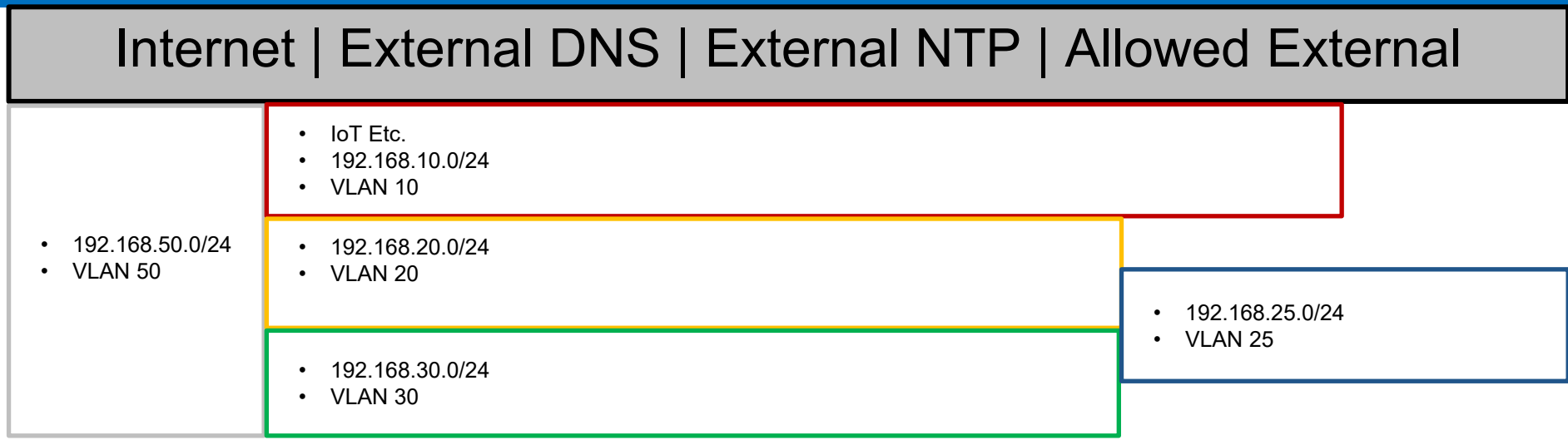
Security Reference Architecture



Standard IP Schema for SRA Model 4 (Can be adjusted for larger networks)
x.x.x.1 Router/Firewall/Gateway
x.x.x.2-10 Switching and AP
x.x.x.11-20 Windows AD and other Windows Server Addresses
x.x.x.21-30 Linux and other servers
x.x.x.31-40 Print Devices
x.x.x.41-50 Security Cameras and other devices
x.x.x.51-100 AND 251-254 Unassigned but can be used for testing, troubleshooting and other temporary assignments as needed
x.x.x.101.250 DHCP Scope range (In Red and Yellow | White, Blue, Green should NOT use DHCP
x.x.x.255 Broadcast Address

CMTC
California's Manufacturing Network

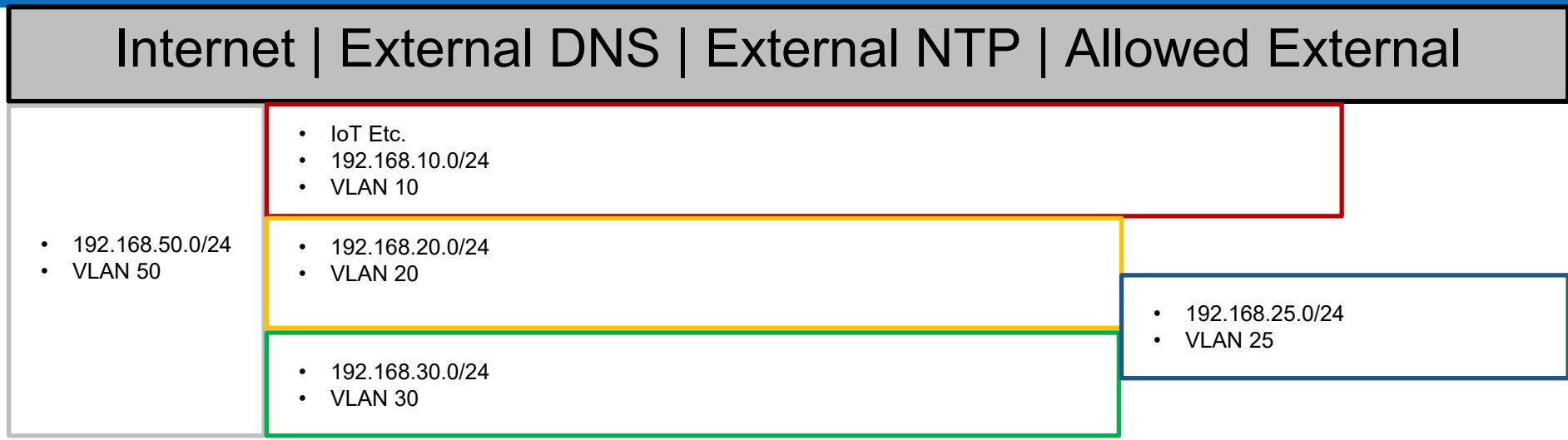
Security Reference Architecture



Aliases:

- Host – An identifier that can consolidate a single IP Address or FQDN, or group multiples into a common, reusable name (Object).
- Protocol – An identifier that can consolidate a single transmission type and port number, or group multiples into a common, reusable name (Object).
- Geo-Block – An identifier that can allow for granular provisioning of traffic allow/deny based on geographic location, or political affiliation.

Security Reference Architecture



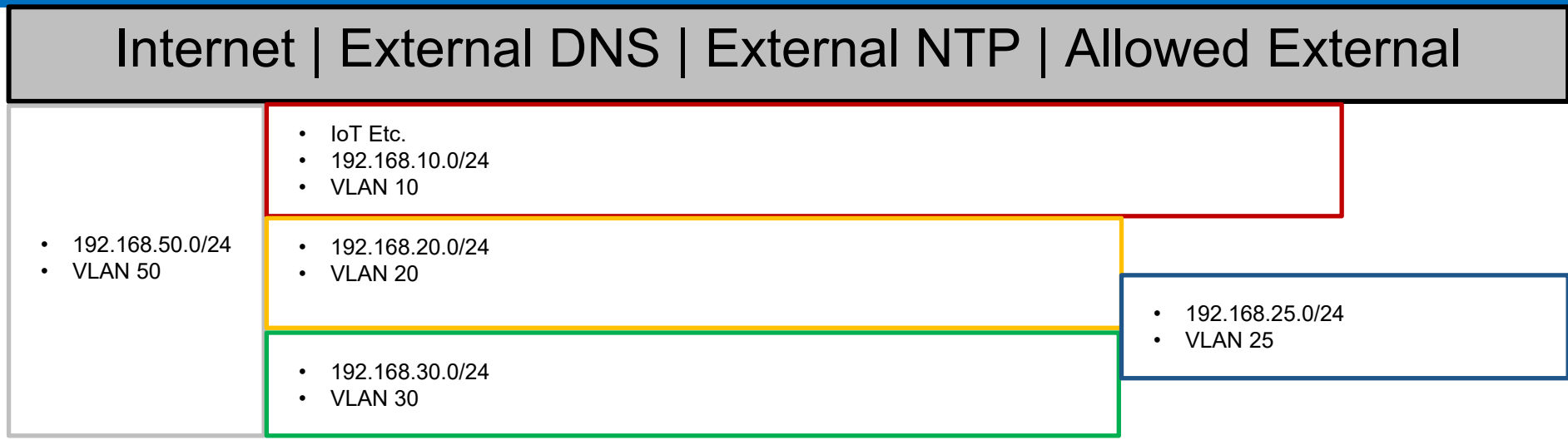
Firewall Services:

- NTP
- DNS
- Web Proxy (Optional)

Architectural Rules:

- No Zone Hopping
- Refer to Rule #1!
- Exception for web traffic if proxy not used. Not ideal, but sometimes proxy overhead is prohibitive.

Security Reference Architecture



Firewall Services:

- NTP
- DNS
- Web Proxy (Optional)

Architectural Rules:

- No Zone Hopping
- All traffic must be explicitly defined. Nothing can be gratuitous and still comply with 800-171 and/or CMMC
- Exception for web traffic if proxy not used. Not ideal, but sometimes proxy overhead is prohibitive (Organizational Decision).

Security Reference Architecture

Internet | External DNS | External NTP | Allowed External

- Management Interfaces
- Admin WS
- IDS/IPS
- SIEM
- Other Devices of a Management Nature

Firewall

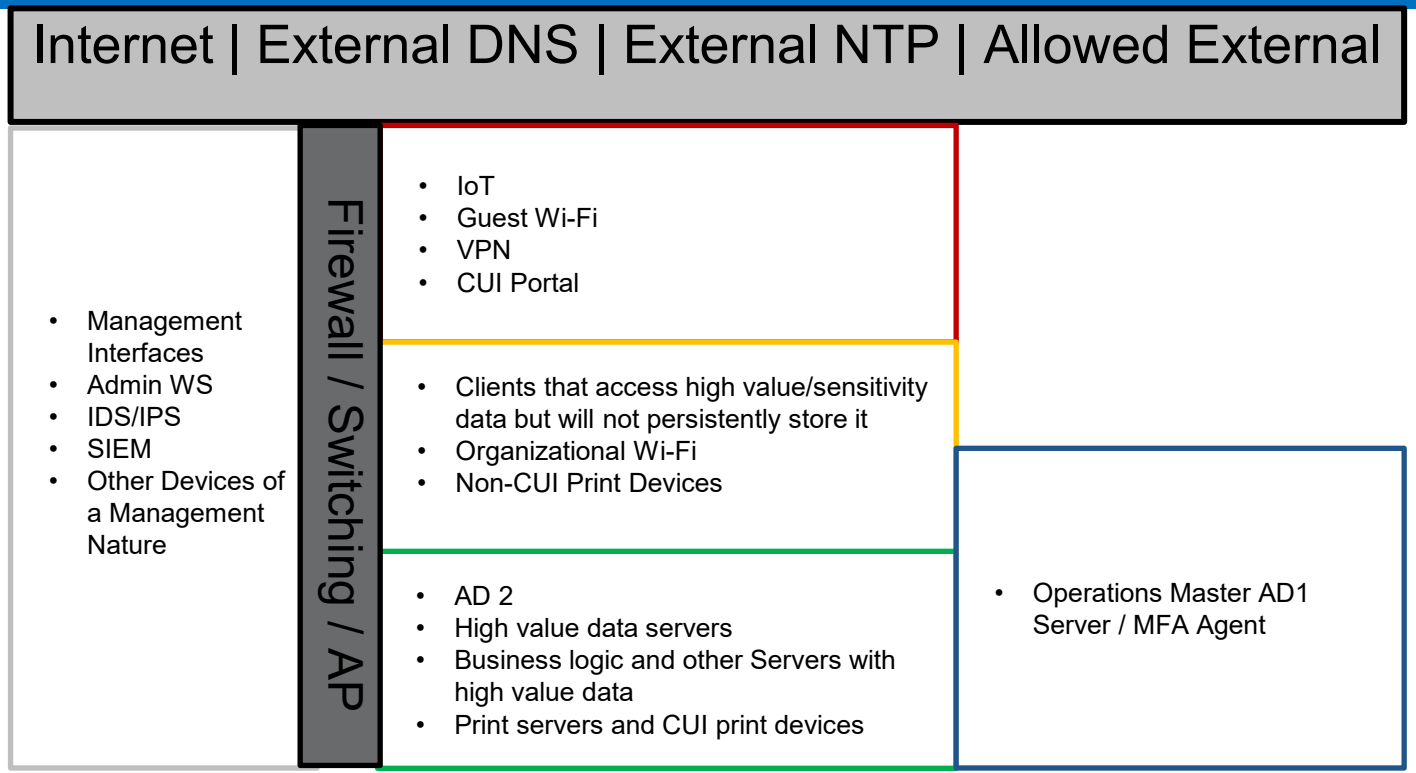
- IoT
- Guest Wi-Fi
- VPN
- CUI Portal

- Clients that access high value/sensitivity data but will not persistently store it
- Organizational Wi-Fi
- Non-CUI Print Devices

- AD 2
- High value data servers
- Business logic and other Servers with high value data
- Print servers and CUI print devices

- Operations Master AD1 Server / MFA Agent

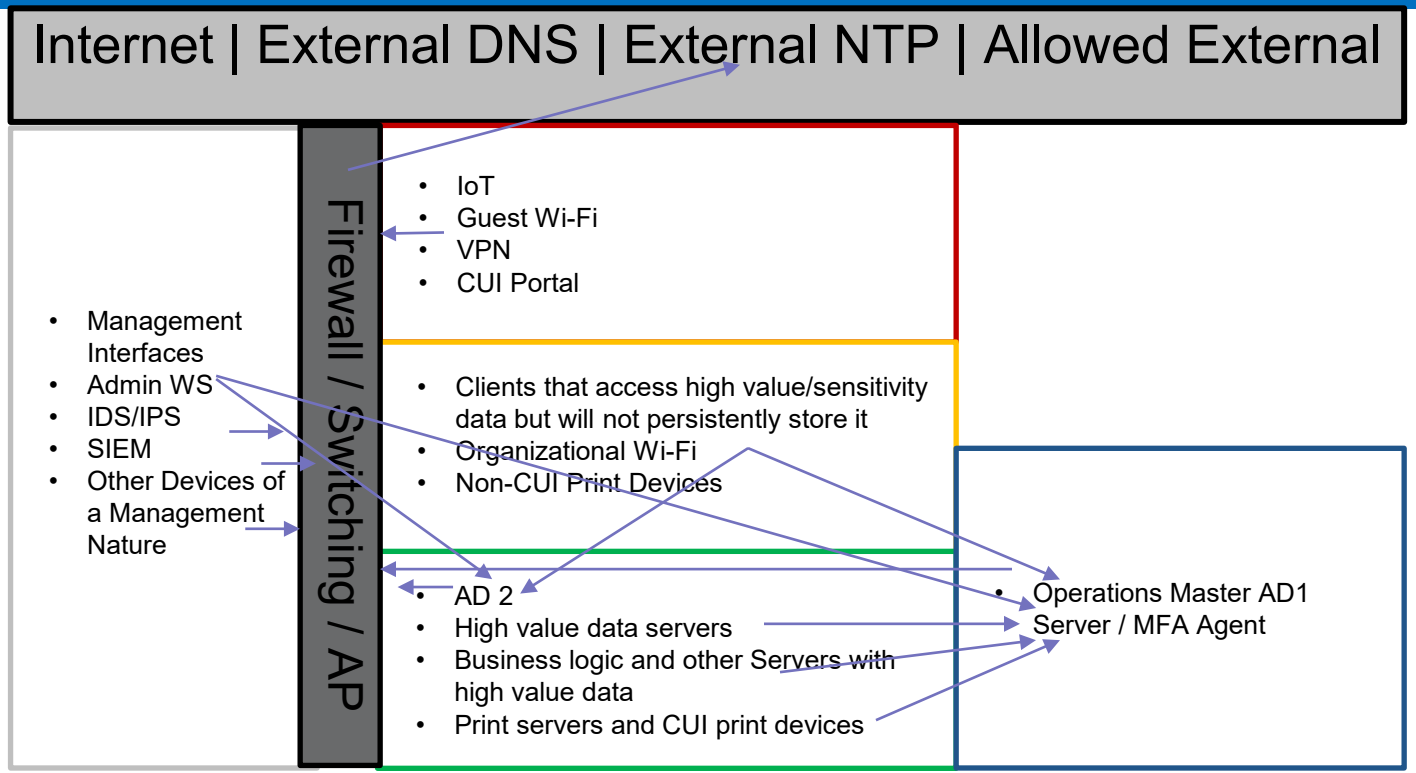
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

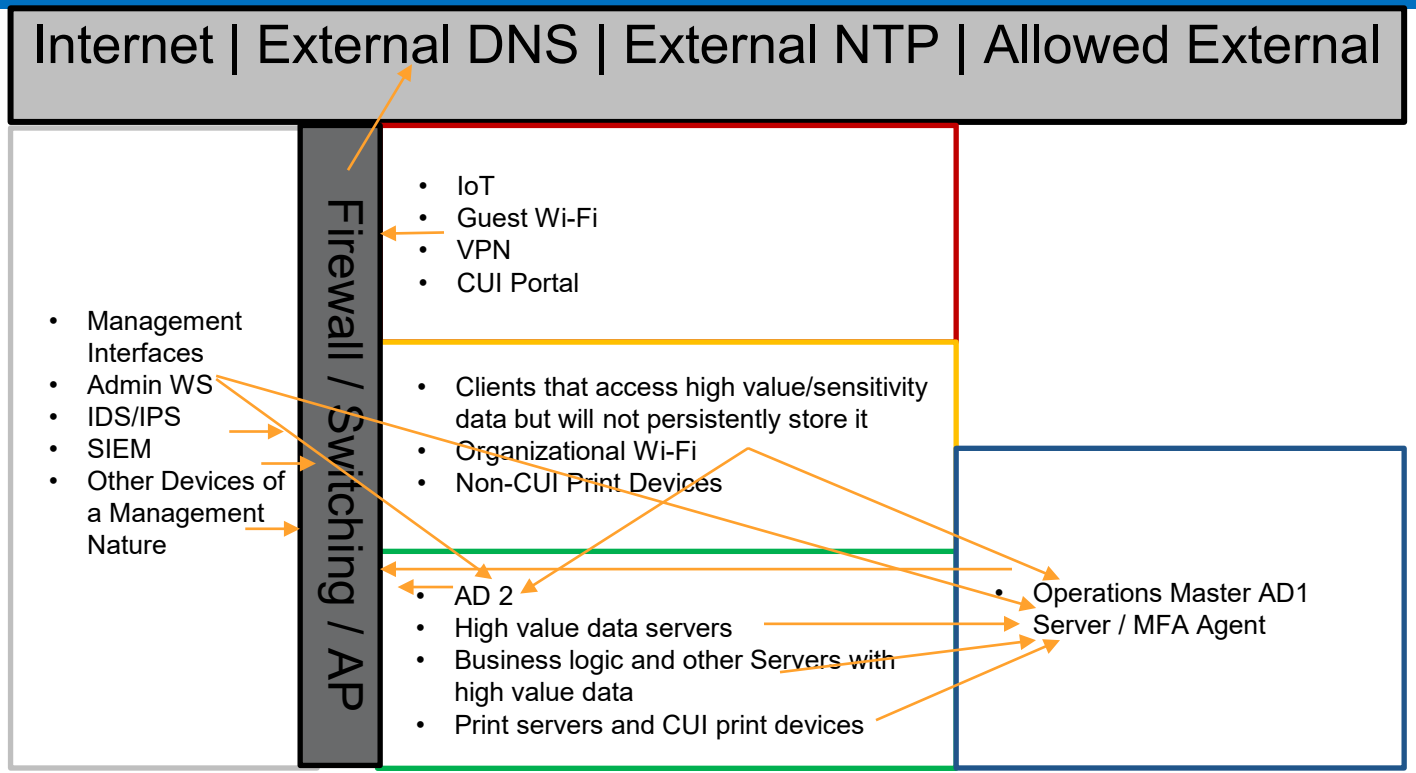
Security Reference Architecture



Legend:

- **NTP - Purple**
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

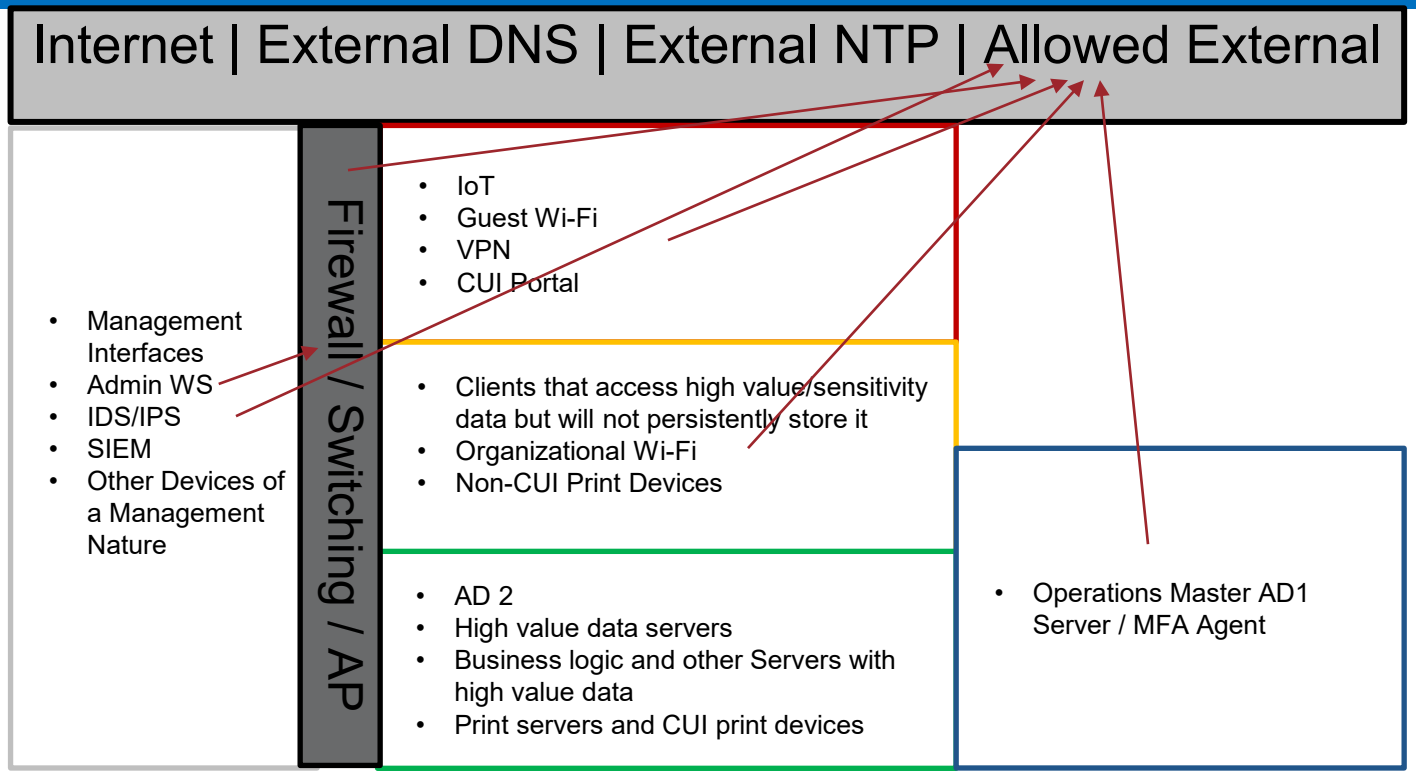
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

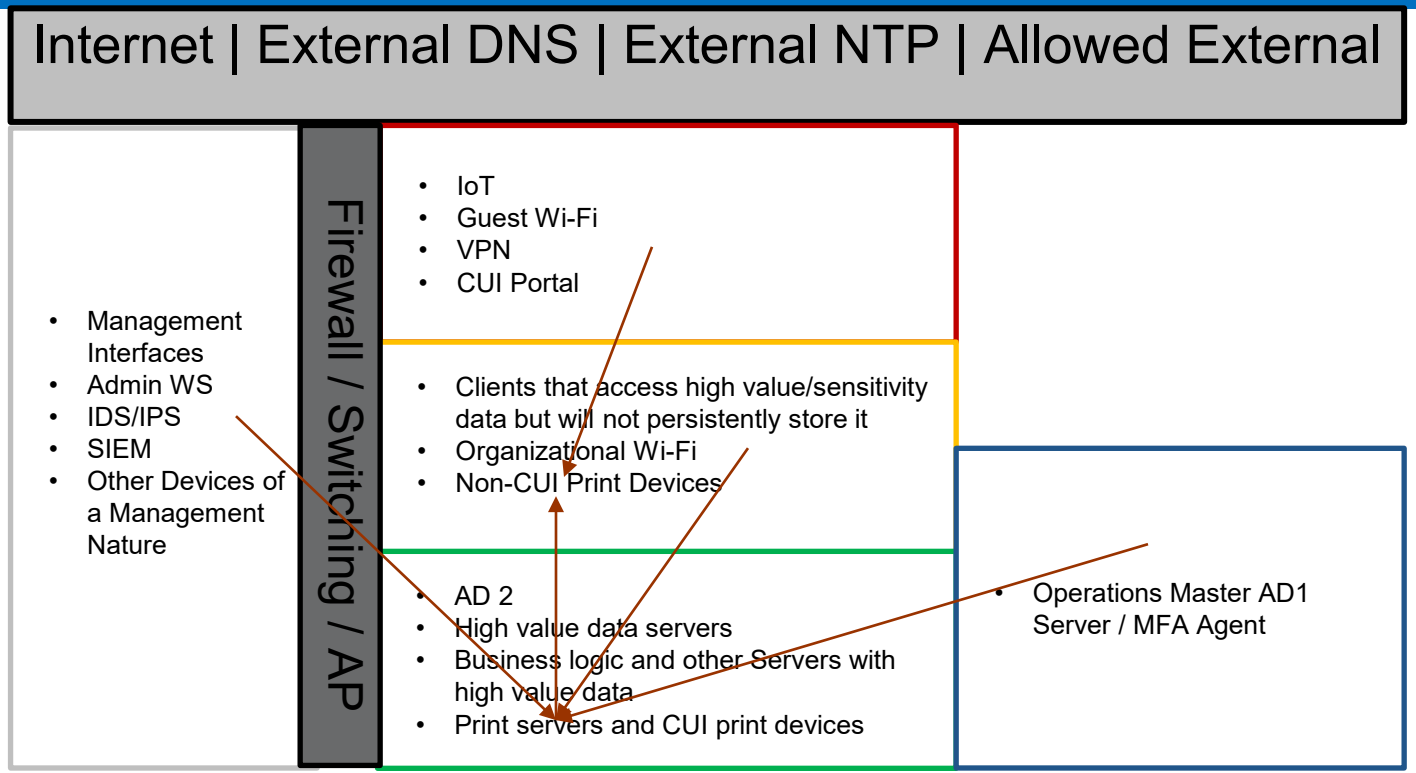
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- **W3 - Red**
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

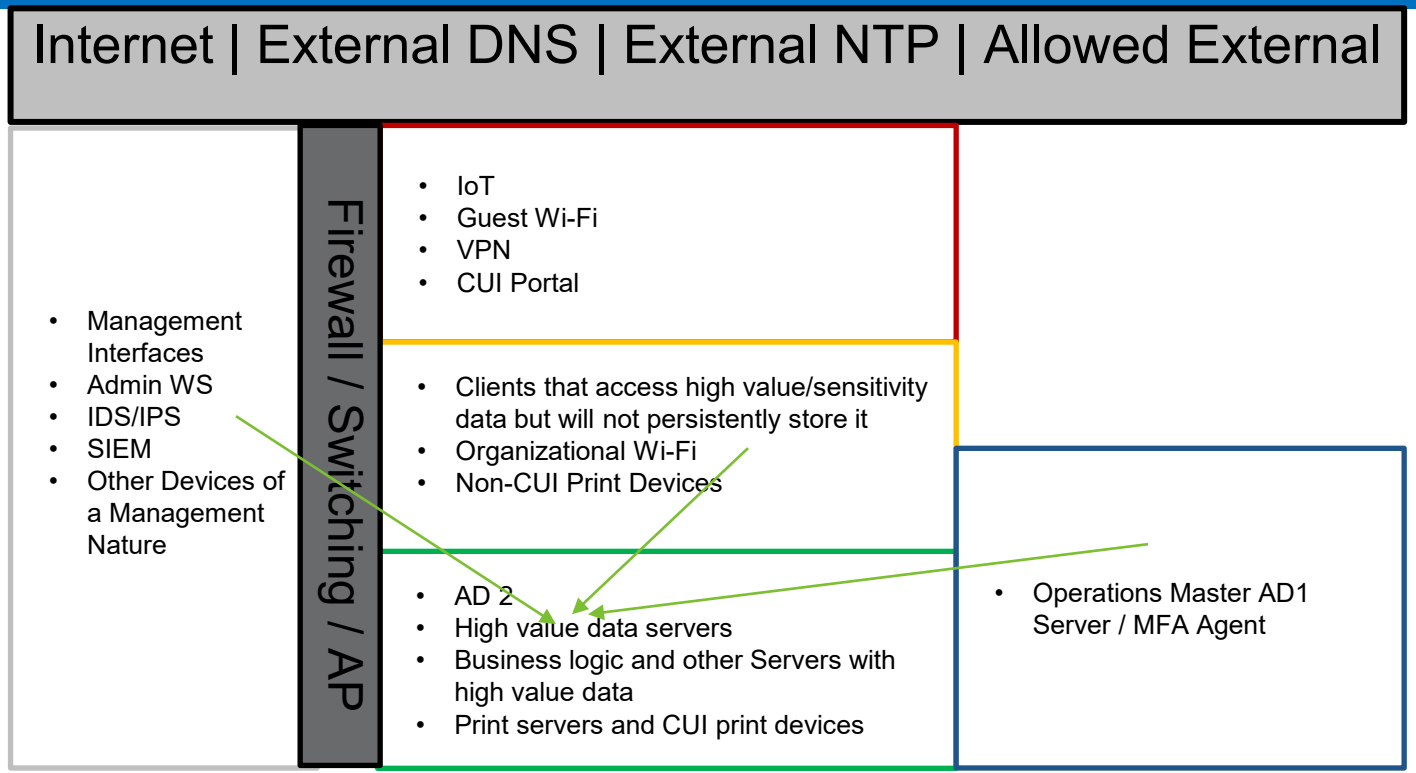
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- **Print - Burgundy**
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

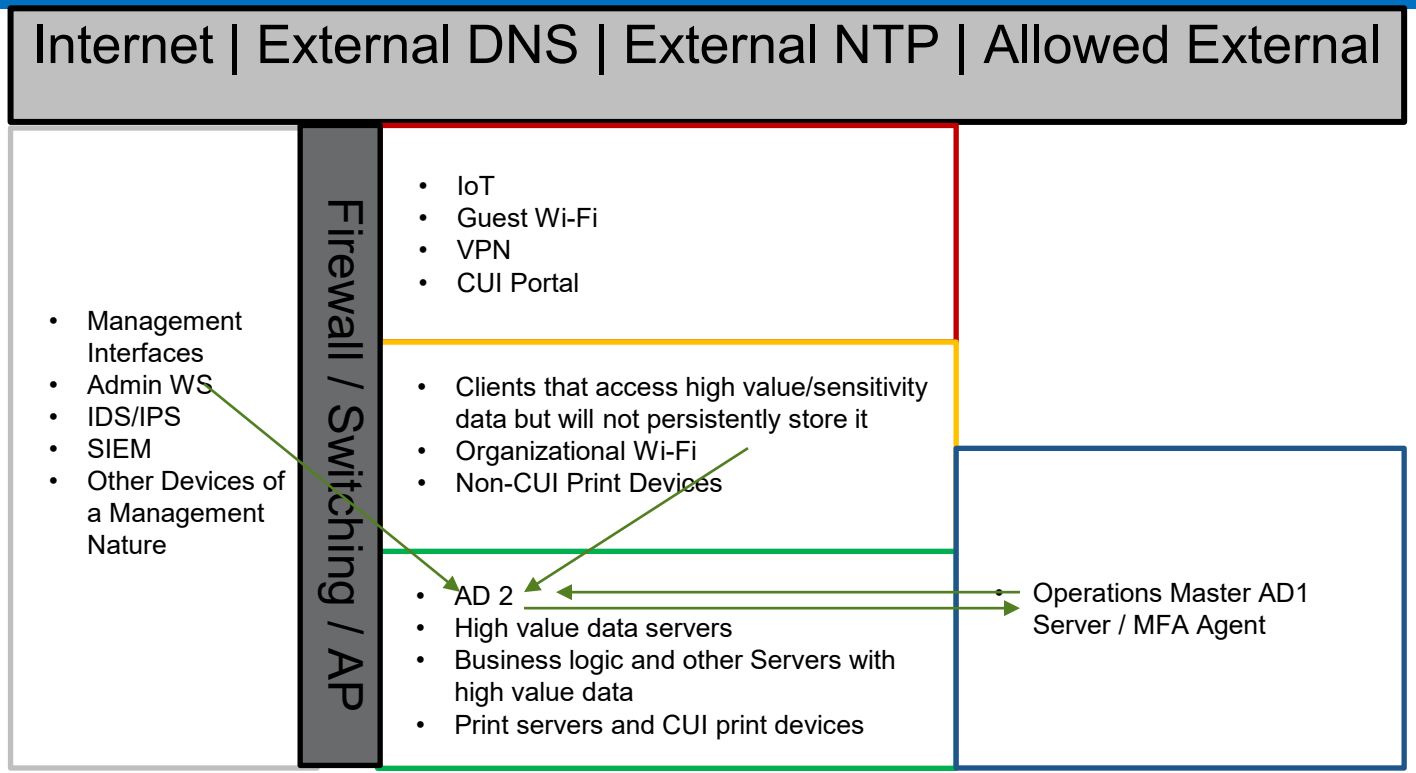
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- **File Transfer – L Green**
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

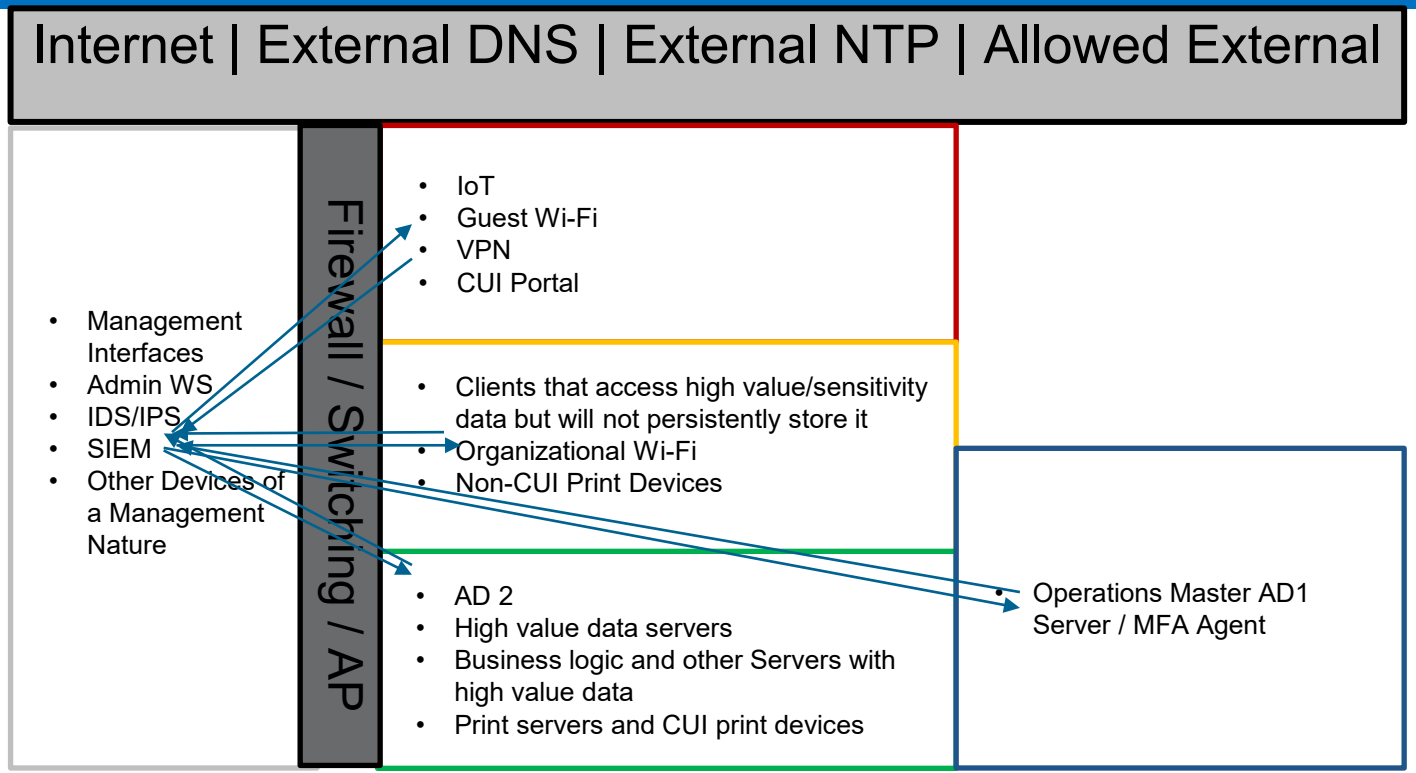
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- **Windows AD - Green**
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

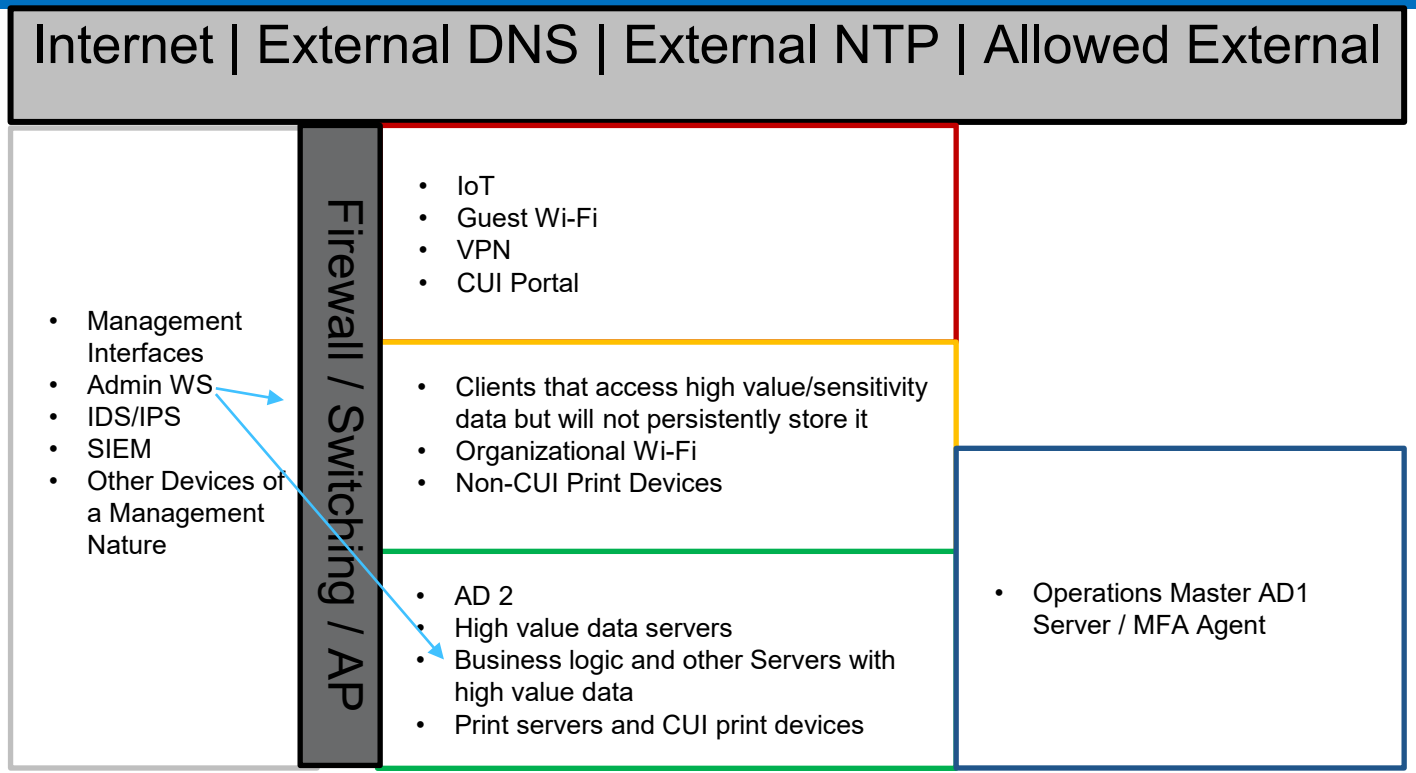
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- **IDS/SIEM - Blue**
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

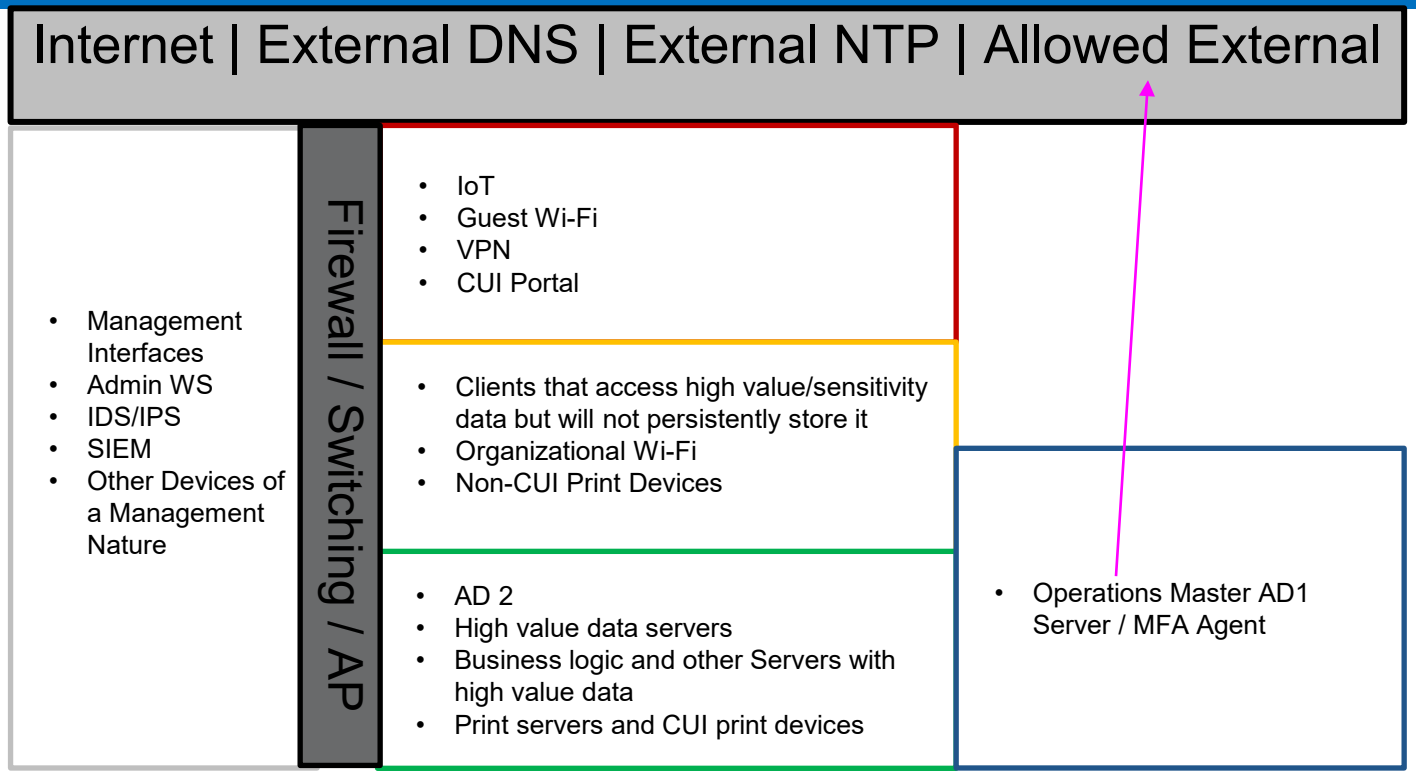
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- **SSH – L Blue**
- MFA Auth - Pink
- VPN - Black

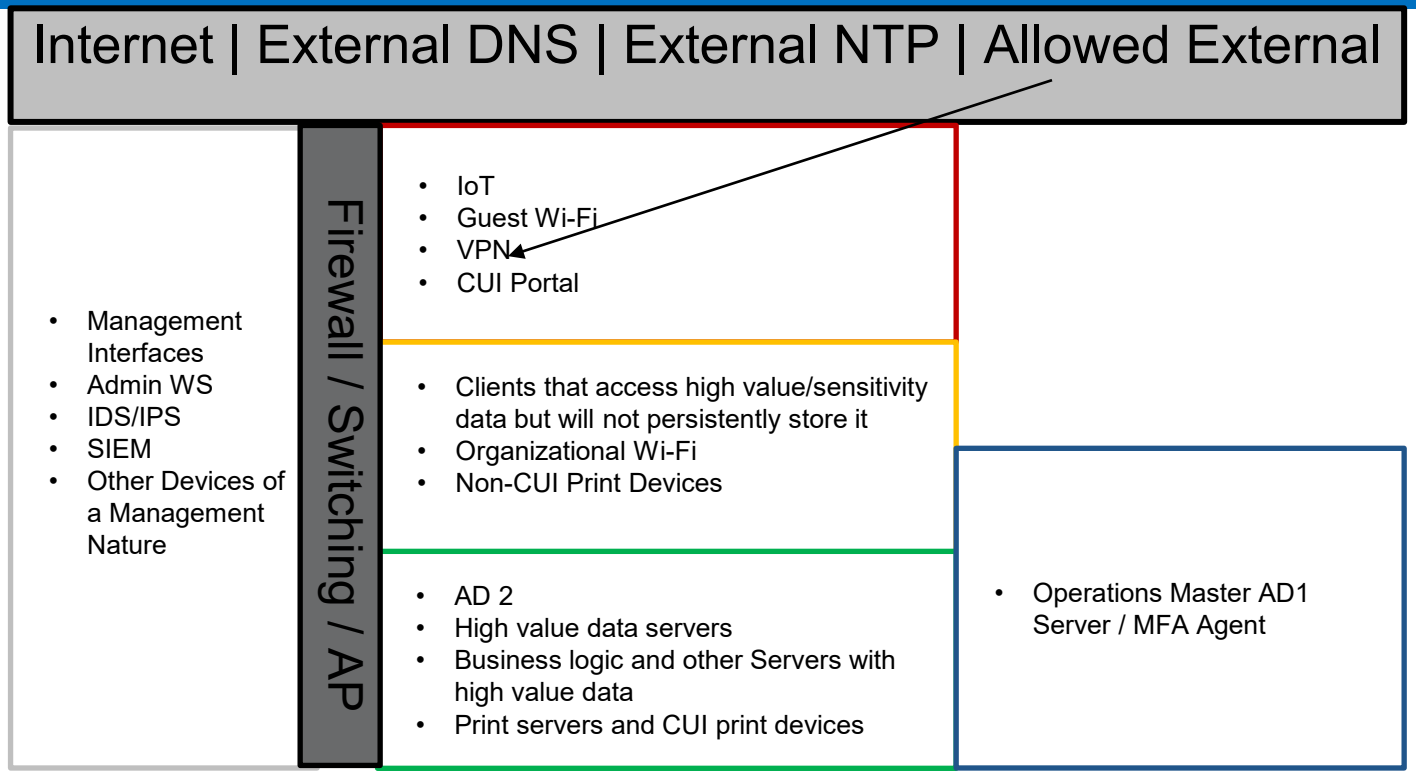
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- **MFA Auth - Pink**
- VPN - Black

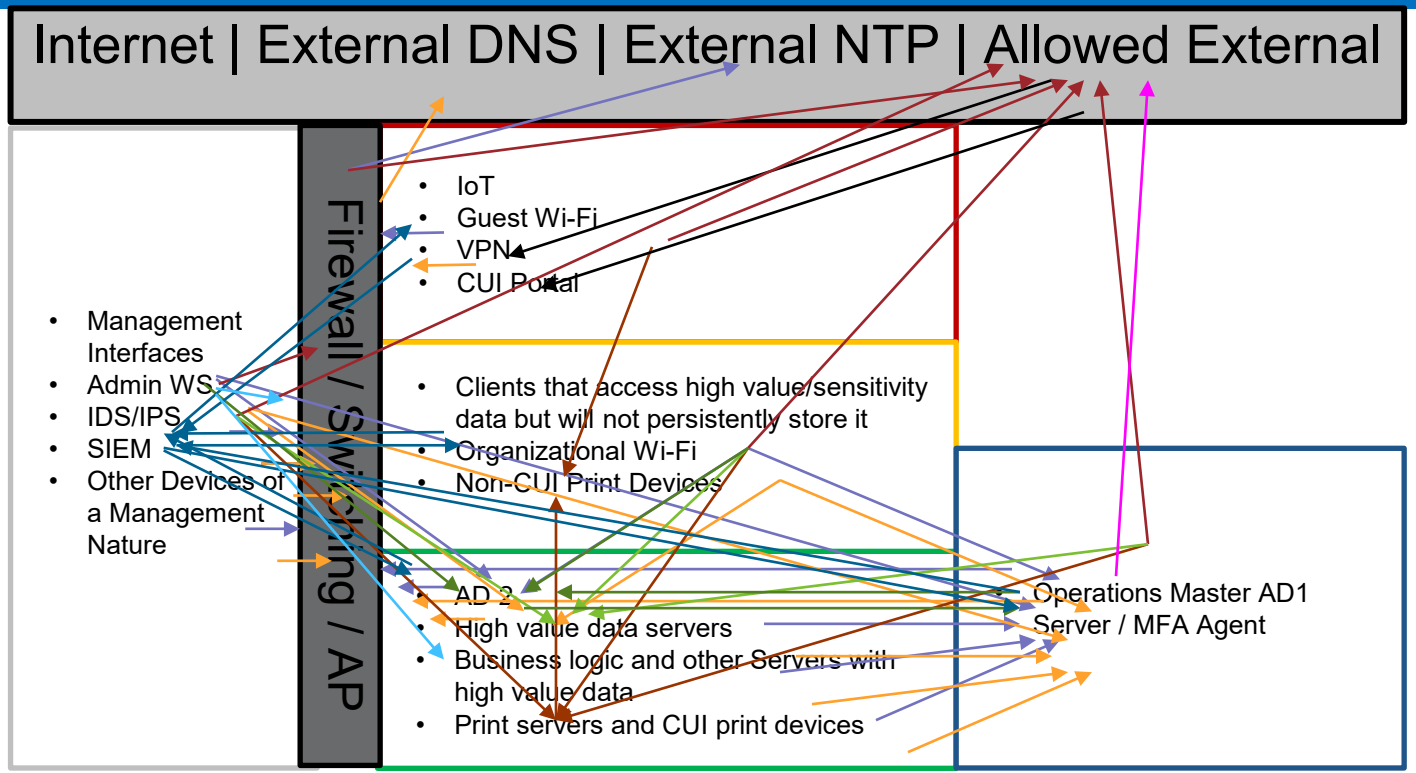
Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- **VPN - Black**

Security Reference Architecture



Legend:

- NTP - Purple
- DNS - Orange
- W3 - Red
- Print - Burgundy
- File Transfer – L Green
- Windows AD - Green
- IDS/SIEM - Blue
- SSH – L Blue
- MFA Auth - Pink
- VPN - Black

Questions and Answers

Q/A

Contact Information

Ernie Edmonds
info@cmtc.com
310.263.3060

CMTC
California's Manufacturing Network