Basic CNSSO Batch 41 - Day 4
Demilitirized Zone

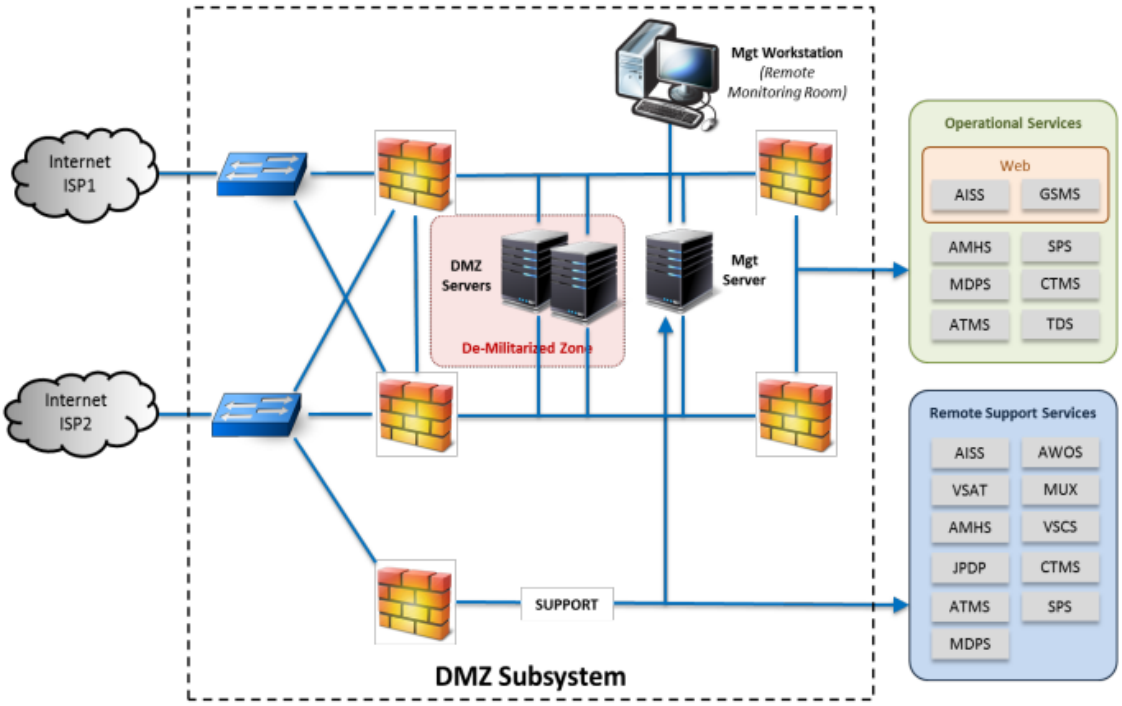
Demilitirized Zone (DMZ)

DMZ is a subnetwork that seperate an internal local area network (LAN) from other untrusted network.

DMZ purpose is to:

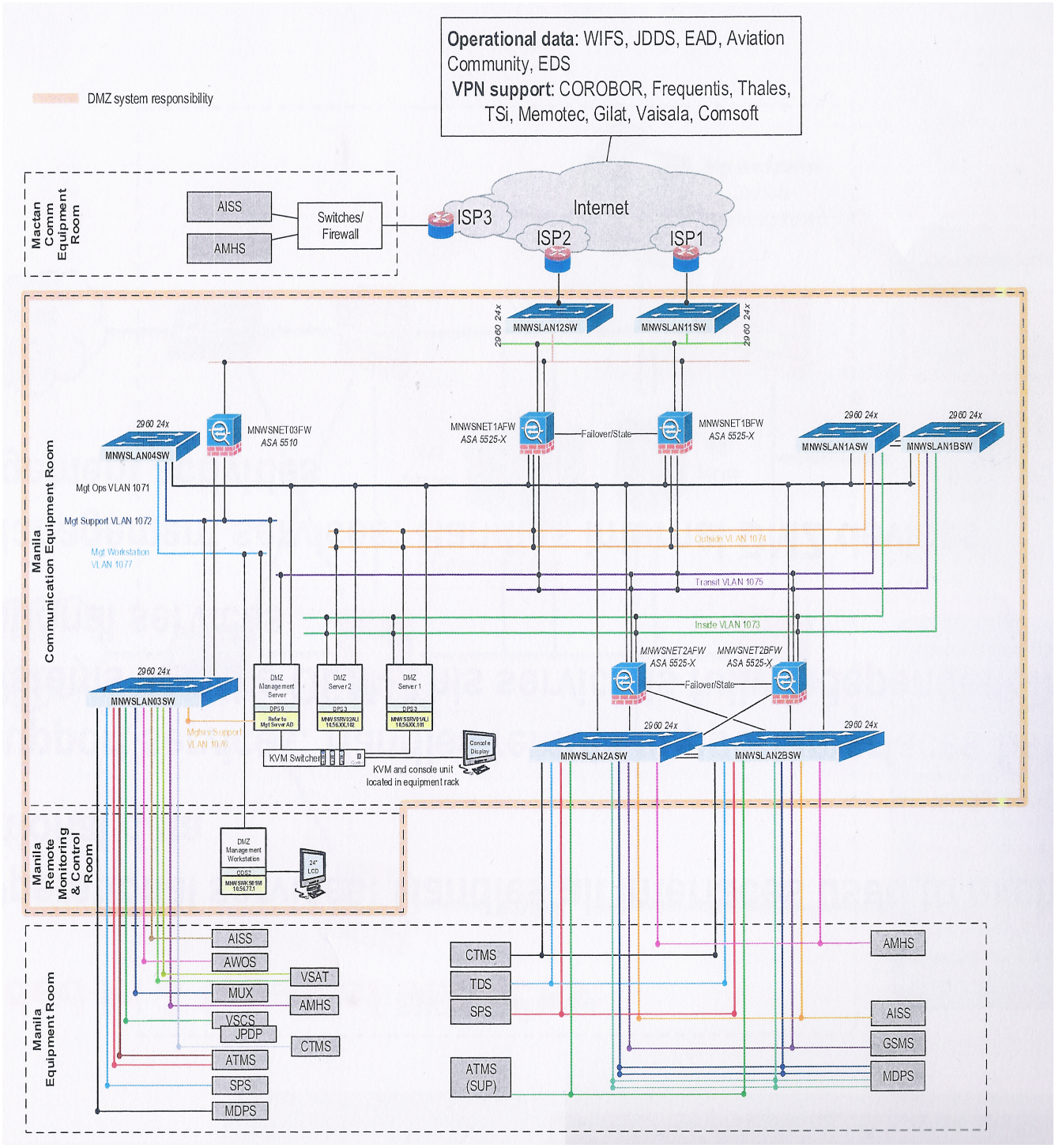
- protect other subsystems from intrusion and malicious intentions from external parties via the public internet;
- implement web server proxies in a demilitarized zone for AISS and GSMS web services;
- protect web servers from direct access by internet users;
- provide other types of secured connections to/from the internet via its firewall devices (FTP, IPsec tunnels, etc).

DMZ architecture



DMZ Global Architecture

DMZ Physical Architecture



Demilitarized Zone (DMZ)

Security Consideration

- CISCO ASA X Series Firewall hardware and software for operational data flow.
- Enabling only required services on DMZ servers.
- SELinux to control separation of processes on DMZ servers.
- Separate overlay networks for the DMZ and remote support equipment with seperate management switch and server.
- Central logging of firewall, ethernet switch, server events to the management server
- DMZ internal technical monitoring with a remote CTMS.
- DMZ summary state information availble on the central CTMS.

Operational Consideration

- Web proxy services: Where a subsytem external interface requires an HTTP connection to the internet.
- Tunnelling proxy services: Where a subsystem external interface requires an IPSEC tunnel to be established over internet.
- Firewall services: Where subsystem external interface is implemented via the internet but cannot be proxy'ed (such as FTP)
- NAT and PAT services: Network address and port translation.

Redundant Consideration

- Redundant Operational Firewalls: Inside/ Outside networks by active/ standby configuration
- Redundant Operational LANs: Inside/ Transit/ Outside networks.
- Clustered operational servers: AISS proxy, GSMS proxy and user account management server
- Failure detection: active/ standby switch over for failure.

Demilitarized Zone (DMZ)