Contents

[Reference: Zones of Trust 2](#_Toc69481694)

[Claim 2](#_Toc69481695)

[Zone 1 – The “Internet” 2](#_Toc69481696)

[Zone 2 – The Demilitarised Zone (DMZ) – (ip address here) 2](#_Toc69481697)

[Zone 3 – Employees Subnet – (IP address here) 3](#_Toc69481698)

[Zone 4 – Servers Subnet – (IP address here) 3](#_Toc69481699)

[Zone 5 – Managerial Subnet – (IP address here) 3](#_Toc69481700)

[Zone 6 - Proxy Subnet – (IP address here) 3](#_Toc69481701)

[Zone 7 - Virtual Private Network (VPN) 3](#_Toc69481702)

[Zone 8 - Intrusion Detection System (IDS) – (IP address) 3](#_Toc69481703)

[References 4](#_Toc69481704)

WM143 NCCD Network Architecture

This document details the network architecture proposal for Midland Endpoint Mobile Enterprise (MEME) and the prepared expansion to their workforce.

# Reference: Zones of Trust

## Claim

The network has been split into 8 trust zones to help ease the management of the firewall rules and administration access permissions.

### Zone 1 – The “Internet”

The Internet zone will include machines not owned by MEME. This means that the machines as far as the organisation knows is untrustworthy. The internal subnet border firewalls must drop packets containing IP addresses which are not routable publicly. This type of traffic is network traffic that begins inside of network and proceeds through its routers to a destination somewhere outside of the network. This is egress traffic can cause congestion on the WAN link. Ingress traffic applies to all network traffic and data that come from outside the local network and normally lands on a specific location within it. This type of traffic could indicate a man-in-the-middle on the WAN link or cause problems with the (Internet service provider) ISP. These filters should be looked at if the ISP provides its own Network address translation (NAT) service.

### Zone 2 – The Demilitarised Zone (DMZ) – (IP address here)

DMZ is a network that is either physical or logical and used to connect hosts which provide an interface to an external untrusted network while keeping the internal, private network – usually the corporate network – separated from the external network. (doubleoctopus, n.d.)

The assets within the DMZ zone are the webserver’s reverse proxy and MEME’s mail relay server, Squid and SMTP-Relay. The proxy is used by the public whenever a client accesses the website. The mail relay will frequently exchange emails with the public relays. Firewall rules make sure that SMTP-Relay will only communicate with MEME’s public mail relay: Ext-DNS (8.8.8.8).

The internal DMZ firewall will limit the office ingress traffic to established connections to add more protection to private machines. Traffic moving from public recorded already on the firewall’s connection tracking module – except for handshake initiations with the OpenVPN server on the private net.

### Zone 3 – Employees Subnet – (IP address here) /19?

The employee subnet has been limited to just usual work traffic. The employee and managerial subnet are the only two with access to surf the web. Therefore, the firewall rules have been configured to restrict browsing to HTTP/HTTPS and to use stateful tracking to allow just established connections through.

Protocols such as FTP have been blocked by default because they are not necessary in today’s use case. This can be undone by administrators if they wish to do so.

The network mask will allow for the use of 8,190 machines in the zone – which is a sample space for the any major expansion in which MEME would want to make in the foreseeable future. This zone would benefit from being split into specific department networks which should then be separated with firewalled routers.

### Zone 4 – Servers Subnet – (IP address here)

This zone is where servers for private use by the office are located. The public should never be able to access these servers. Therefore, they are located behind the DMZ. The internal traffic is managed by a firewall behind the central router. Packets are restricted by their source subnet and destination server. Port-checking is enforced so that only valid traffic moves into the subnet. The only traffic allowed between the subnet and Internet is DNS queries from the DNS server to the specific external DNS server. The mail is the only traffic that is allowed into the DMZ to allow mail exchange with the relay server. This ensures that internal emails are not leaked onto the internet.

### Zone 5 – Managerial Subnet – (IP address here)

The managerial zone will manage the network’s administrators, so that administrative traffic such as system logs and SSH sessions are sourced/destined from valid locations to prevent unauthorised network monitoring or remote sessions. The confinement allows other areas of the office network to be opened to traffic without compromising the integrity of the services for the administration.

### Zone 6 - Proxy Subnet – (IP address here)

### 

### Zone 7 - Virtual Private Network (VPN)

The VPN (OpenVPN) will allow employees outside of the network with authorised certificates to be able to connect to the internal network through a TLS-encrypted VPN tunnel. This allows the Mail and LDAP servers to have suitable access and any other resources MEME may choose to provide internal employees with. Therefore, it is the only internal host accessible on the internet without first requiring an established connection record on the firewalls.

The server is in the employee’s subnet which means the VPN clients get identical privileges as normal employees, which creates a well-established external link of the network. Protocols such as NTP, SSH, remote logging have been disabled for OpenVPN clients as they are not physical hosts. HTTP connections can only be made to the internal webserver which means every other web connection is to be made via the client’s physical network. Every host within the internal network has a route back to VPN clients.

### Zone 8 - Intrusion Detection System (IDS) – (IP address)

The intrusion detection system on the network has two points of monitoring: the internal network and the DMZ. The taps for this network are fully passive and do not have an IP address on their monitoring ethernet interfaces. The networks OSI layer is secure as it only allows connections on the internal network with DNS and NTP through an IDSManager, the zone for the IDS will, therefore, have the highest levels of trust on the network.

### 

# References

doubleoctopus. (n.d.). *DEMILITARIZED ZONE (DMZ)*. Retrieved from doubleoctopus: https://doubleoctopus.com/security-wiki/network-architecture/demilitarized-zone/#:~:text=A%20DMZ%2C%20short%20for%20demilitarized,isolated%20form%20the%20external%20network.