Contents

[Reference: Zones of Trust 3](#_Toc70011048)

[Claim 3](#_Toc70011049)

[Zone 1 – The “Internet” 3](#_Toc70011050)

[Zone 2 – The Demilitarised Zone (DMZ) – 192.168.2.0/24 3](#_Toc70011051)

[Zone 3 – Employees Subnet – 192.168.3.0/24 4](#_Toc70011052)

[Zone 4 – Servers Subnet – 192.168.4.0/24 4](#_Toc70011053)

[Zone 5 – Managerial Subnet – 192.168.5.0/24 4](#_Toc70011054)

[Zone 6 - Proxy Subnet – 192.168.6.0/24 4](#_Toc70011055)

[Zone 7 - Virtual Private Network (VPN) 5](#_Toc70011056)

[Zone 8 - Intrusion Detection System (IDS) – 192.168.8.0/24 5](#_Toc70011057)

[Evidence 5](#_Toc70011058)

[Reference: Infrastructure assets 5](#_Toc70011059)

[Claim 5](#_Toc70011060)

[Evidence 5](#_Toc70011061)

[Reference: Firewalls 5](#_Toc70011062)

[Claim 5](#_Toc70011063)

[Evidence 6](#_Toc70011064)

[Reference: Secure Shell (SSH) 6](#_Toc70011065)

[Claim 6](#_Toc70011066)

[SSH Authentication 6](#_Toc70011067)

[SSH Security Policies and Procedures 6](#_Toc70011068)

[Secure SSH Implementation 6](#_Toc70011069)

[Evidence 7](#_Toc70011070)

[Reference: System logging 7](#_Toc70011071)

[Claim 7](#_Toc70011072)

[Evidence 7](#_Toc70011073)

[Reference: Internet protocol tables 7](#_Toc70011074)

[Claim 7](#_Toc70011075)

[Reference: Domain Name System (DNS) 8](#_Toc70011076)

[Claim 8](#_Toc70011077)

[DNS security 8](#_Toc70011078)

[Evidence 8](#_Toc70011079)

[Reference: Virtual Private Network (VPN) 8](#_Toc70011080)

[Claim 8](#_Toc70011081)

[OpenVPN Authentication 9](#_Toc70011082)

[Evidence 9](#_Toc70011083)

[Reference: Mail 9](#_Toc70011084)

[Claim 9](#_Toc70011085)

[Evidence 9](#_Toc70011086)

[Reference: Dynamic Host Configuration Protocol (DHCP) 9](#_Toc70011087)

[Claim 9](#_Toc70011088)

[DHCP security 10](#_Toc70011089)

[DHCP network configuration 10](#_Toc70011090)

[Evidence 10](#_Toc70011091)

[References 10](#_Toc70011092)

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. For easier addressing, each zone will be allocated a different subnet. By default, each subnet will a /24 subnet; since the company is small, this leaves 254 usable hosts which should be more than enough. As per RFC 1918 (Rekhter, Moskowitz, Karrenberg, de Groot, & Lear, 1996), all the subnets will conform to the requirements of sitting within 192.168.0.0/16 and to help manage the network, each zone will increment the 3rd octet of the IP address denoting which zone it’s in. Given the initial 8 zones, this leaves possibility many more zones or extending the number of machines on the existing subnets.

### 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 are untrustworthy. The internal subnet border firewalls must drop packets containing IP addresses that are not routable publicly. The traffic explained here is network traffic that starts inside of network and proceeds through its routers to a destination somewhere outside of the network. This egress traffic can cause congestion on the WAN link. Ingress traffic applies to all network traffic and data that comes 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 the Network address translation (NAT) service. While most of the subnets allow for a larger amount of machines than there is currently, the /24 subnet is common for many household networks and allows for an adequate number of hosts while not taking up a large chunk of the allocated address space.

### Zone 2 – The Demilitarised Zone (DMZ) – 192.168.2.0/24

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 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 network would be allowed. For example, the firewall would allow http traffic if the connection was started via a staff machine as seen from a typical web browser since otherwise, they wouldn’t be able to receive http responses from the external websites they’re trying to connect to.

### Zone 3 – Employees Subnet – 192.168.3.0/24

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 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 – 192.168.4.0/24

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 – 192.168.5.0/24

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 – 192.168.6.0/24

Using a reverse proxy requires the origin server to only be accessed by that and not the public. Therefore, connected to the dual-homed surrogate is Int-WWW. Because of the access restrictions, a firewall has been placed between the two machines so that only the proxy on the correct HTTP port can access the webserver. NTP, DNS queries, and SSH sessions from administrators can also pass through to configure the website. The subnet could be expanded to host more webservers behind the proxy which will allow for load balancing if the organisation expects the load of the webserver to increase with the expansion of their staff-base. Int-WWW could also be dual-homed to form a firewalled backend network that hosts API or database servers.

### 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) – 192.168.8.0/24

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.

## Evidence

# Reference: Infrastructure assets

## Claim

MEME’s infrastructure lacked the key machines needed to secure and increase the efficiency of the network; therefore, changes have been made to remove, append and change aspects of the network.

## Evidence

# Reference: Firewalls

## Claim

The firewall systems for MEME includes software and hardware firewalls. Each of the hardware firewalls is placed in zone perimeters. Managing traffic is the main priority for these devices.

Each machine will have specific rules. These will be known as the software firewalls which are previous versions of the network’s ingress traffic filtering which will act as backups. To reduced unneeded traffic on the cables, egress traffic will be filtered on each of the machines.

For the hardware firewalls, they will be using Linux’s bridging making them transparent. This allows the processing power to not be dedicated to the routing. Broadcast domains are preserved which means that subnet address and routing tables do not need to be changed when implementing, removing, or replacing firewalls. The firewalls will not have an IP address which means they are not vulnerable directly on protocols above layer 2. This will also hide them from network mapping tools.

This way of implementing the firewalls is efficient because each zone will have its own dedicated firewall. This will make it easier for administrators to work with each of the firewalls and more easily understand what each one is doing and how it needs to be configured, reducing the chance of human errors. This method will also protect the integrity of the whole network because if one firewall was to be compromised the rest of the zones will still be protected by different firewalls.

## Evidence

# Reference: Secure Shell (SSH)

## Claim

OpenSSH is used to access the Admin and IDS-Manager machines remotely which provides access to the command-line of the machines and file transfer capabilities. The SSH protocol ensures confidentiality and authenticity via public-key cryptography unlikely protocols such as FTP and Telnet which is important given the privileges that these machines are given over the entire network.

### SSH Authentication

The reason why the use for using public key authentication over simple passwords is because of the security. Public key authentication will be provided cryptographic strength that even long and complex passwords are not able to offer. By using SSH, public key authentication considerably improves the security as it allows people to not have to remember all their passwords or from writing them down.

Furthermore, public key authentication also offers usability benefits – it allows users to implement single sign-on throughout the SSH servers they connect to. Public key authentication also allows automated, password-less login that is a key enabler for the countless secure automation processes that execute within enterprise networks globally. (ssh.com, n.d.)

### SSH Security Policies and Procedures

The SSH Policies and procedures play a critical role in SSH security by establishing consistent requirements across the dissimilar systems and environments where SSH is deployed. The definition of policies should clearly explain the roles and responsibilities so that misunderstandings that result in security lapses are prevented and to ensure accountability. All SSH stakeholders (system administrators, security professionals, business application owners, etc.) must be informed on SSH security policies and processes. (Tatu Ylonen, 2015)

### Secure SSH Implementation

To make sure that the implementation of OpenSSH is secure a few baselines need to be followed:

* SSH should only be enabled on systems where it is required. (Tatu Ylonen, 2015)
* Regular updates of OpenSSH must be kept so that server and client implementations fully up to date across all systems and bugs found are irradicated. (Tatu Ylonen, 2015)
* Hardening SSH server and client implementations, including disabling SSH v1 protocol, disabling unapproved authentication methods, preventing implicit access by limiting SSH accessible accounts and groups (including root), disabling port forwarding, limiting access to environment variables, using approved cipher, properly configuring supporting subsystems and enforcing SSH inactivity timeouts on the system. (Tatu Ylonen, 2015)

## Evidence

# Reference: System logging

## Claim

The internal network has remote machine logging over the syslog protocol. Logs captured on every machine through the rsyslog daemon are forwarded over the network on port 514 to the central logging server in the Managerial subnet. The advantage of the security side of things is that it eases the administrator’s workload. To make the maintenance cycles more efficient remote sessions are not required to view logs as they are all collated in one place. The system also allows for the administrators to implement a single IDS on the server (as opposed to one on each machine) that can display anything that is not expected. This ensures the logs do not require monitoring constantly and will reduce any risk of errors going unnoticed. The current rsyslog configuration uses the TCP protocol which, as opposed to the UDP mode, provides reliable transport to ensure log messages are received.

## Evidence

# Reference: Internet protocol tables

## Claim

Iptables are at the centre of all the firewalls on the network. Each set of firewall rules are specifically configured for each machine. INPUT and OUTPUT chains have a default policy set to drop packets. This is more reliable than settings specific rules as due to human error intruders could find a way to dodge all the existing firewall rules.

Most of the machines will accept ICMP because it is used for more than just pings. It is a utility protocol for maintaining networks such as *host unreachable* or *port unreachable*. Apart from webserver pings, ICMP will be blocked from the internet to prevent ping sweeps of the internal network or a private host if it is on the DMZ.

The firewall rules have all been set so that it monitors the full state of active network connections. This means that stateful firewalls are constantly analysing the whole context of traffic and data packets, trying to enter the network rather than discrete traffic and data packets in isolation. (Wilkins, 2013)

# Reference: Domain Name System (DNS)

## Claim

The domain name system (DNS) is a naming database where internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name one would use to locate a website to the IP address that a computer uses to locate a website. For example, if someone types google.com into a web browser, a server backend will match that name to the corresponding IP address, something similar in structure to 8.8.8.8. (Burke, 2019)

### DNS security

DNS does have multiple vulnerability’s that have been discovered over time. Cache poisoning of DNS is one such vulnerability. In DNS cache poisoning, data is distributed to caching resolvers, posing as a privileged origin server. The data will then be able to present false information and can then affect the time to live. (Burke, 2019)

An intruder with malicious intent can create a dangerous website with a misleading header to try and convince users that the website they are on is real, giving the individual access to the user's information. By replacing a character in a domain name with a similar looking character, for example, the number “1” and a lowercase L “l”, which may look similar depending on the font they use. A user could be fooled into clicking a false link. This is usually exploited with phishing attacks. (Burke, 2019)

One similar method is known as homograph spoofing or a punycode attack. This attack is done through the use of non-latin characters which are virtually indistinguishable from their latin counterparts. (Hannay & Baatard, 2012) This would result in possible impersonation of domains which could then be used to trick users into sending confidential information to a malicious actor.

While homograph spoofing is a phishing attack, measures can be taken to ensure that the risk is reduced for staff. One easy way would be to ensure web browsers on staff computers are kept up to date meaning correct measures are implemented to prevent this – such as to prohibit domain names that mix letters from different alphabets. (Gabrilovich & Gontmakher, 2002)

## Evidence

# Reference: Virtual Private Network (VPN)

## Claim

The VPN server being used will be OpenVPN. The server has been configured to allow external employees the ability to access the internal network via an encrypted tunnel. The clients will have access to the internal Web, Mail and LDAP servers.

### OpenVPN Authentication

OpenVPN uses multi-factor authentication which is typically managed with a token. This can be something like an RSA SecureID hardware token, or it can be a device such as your mobile phone.

The initial implementation using cell phones, was a 4-to-6-digit number calculated by the vendor or site, sent as a text message. The end-user would then enter this number after already successfully entering their username and password as a validation code. This code can use either a random number generator that the site tracks temporarily or one of the HOTP/TOTP methods. (Crist, n.d.)

Nowadays with mobile phones can be used to access an app to generate a code. Google Authenticator is common, along with commercial MFA vendor tools like Okta. Both services use a protocol TOTP (Time-based One-Time Passwords) and HOTP (HMAC-based One-Time Passwords). (Crist, n.d.)

The main difference between these two mechanisms is where and how the validation code or one-time password is calculated or communicated. With TOTP, SMS messages can potentially be stolen via SIM hijacking or other malicious methods and rely on a reliable cellular or data connection to the receiving device. The other mechanism requires no network connection on the device, calculating either the challenge or the response. (Crist, n.d.)

## Evidence

# Reference: Mail

## Claim

The Mail server will run all mail clients on MEME’S internal network. The server will use Simple Mail Transfer Protocol (SMTPS) to allow clients to submit mail requests. Internet Message Access Protocol Secure (IMAPS) will be used to retrieve mail. TLS is used for two protocols to stop malicious attempts of reading the content of the emails during transit.

For mail on the internal network to the meme.cyber.test domain, the system stops at this point. Mail is then stored on the server and retrieved when employees refresh their web clients. For any mail going to external domains, the server forwards the mail over SMTPS to the mail relay in the DMZ before that relays the mail to a public mail server looking to towards the internet, where the intended recipient can retrieve it. This also happens in reverse with the relay listening for incoming mail from a designated public server.

## Evidence

# Reference: Dynamic Host Configuration Protocol (DHCP)

## Claim

DHCP helps with the workload of network administrators by using the Int-DNS server in MEME’s network to automatically assign IP addresses to machines. It also provides machines with the correct routing and gateway information.

### DHCP security

DHCP is a protocol that does not need authentication from the client, any user within or outside the network can obtain a lease of IP. This can reveal data such as the DNS server IP or server data to the unauthorised user, compromising the security of the network. Attackers physical access to the DHCP-enabled network can instigate a denial-of-service attack on DHCP servers by flooding the server with lease requests, thereby depleting the number of leases that are available to other DHCP clients. (CIOReview, 2016)

There are many attacks on DHCP such as the DHCP starvation attack, where the hacker can exhaust the address space available to the DHCP servers for a particular period. This type of attack is carried out by broadcasting DHCP requests with spoofed MAC addresses. DHCP snooping, the DHCP security feature that provides network security by filtering DHCP messages that are not trusted and by creating and maintaining a DHCP snooping binding database, is also exploited by hackers to gain access. (CIOReview, 2016)

### DHCP network configuration

To help protect against these attacks measure must be taken. Proper physical security protocols for the hardware components like the server, switches and routers can limit unauthorised access into the server system. Restricting wireless access for non-authorised individuals internal or external of the system by maintaining the user access policies can also improve the security perimeter. (CIOReview, 2016)

DHCP is however located on a different broadcast domain to the Employees and Managerial subnets. The Int-Router must have the ability to reciprocate ingress DHCP broadcasts from the interface towards the Servers zone with unicast (this must be a DHCP relay agent).

The main network machines, such as routers, will have static IP addresses for the routing table. Critical servers have static addresses such that client configuration files do not need to rely on domain names. Safety-critical infrastructure is also static. This means that it will immediately start network logging and intrusion detection.

## Evidence

# References

Burke, J. (2019, 7). *domain name system (DNS)*. Retrieved from searchnetworking: https://searchnetworking.techtarget.com/definition/domain-name-system#:~:text=The%20domain%20name%20system%20(DNS,uses%20to%20locate%20a%20website.

CIOReview. (2016, 8 3). *How to Secure a Network from DHCP Attacks*. Retrieved from cioreview: https://www.cioreview.com/news/how-to-secure-a-network-from-dhcp-attacks-nid-15482-cid-21.html#:~:text=DHCP%20Attacks%20and%20Security&text=Since%20DHCP%20is%20a%20protocol,user%2C%20compromising%20the%20network's%20security.

Crist, E. F. (n.d.). *Multi-Factor Authentication with OpenVPN | Community Edition*. Retrieved from openvpn: https://openvpn.net/multi-factor-authentication-with-openvpn-community-edition/

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.

Gabrilovich, E., & Gontmakher, A. (2002). The Homograph Attack. *Communications of the ACM*, 128-130. doi:10.1145/503124.503156

Hannay, P., & Baatard, G. (2012). The 2011 IDN Homograph Attack Mitigation Survey. *ECU Publications 2012* (pp. 653-657). Edith Cowan University: School of Computer and Security Science. Retrieved from https://ro.ecu.edu.au/ecuworks2012/175/

Rekhter, Y., Moskowitz, R. G., Karrenberg, D., de Groot, G. J., & Lear, E. (1996). *Address Allocation for Private Internets.* IEFT. Retrieved from https://tools.ietf.org/html/rfc1918

ssh.com. (n.d.). *What is SSH Public Key authentication?* Retrieved from ssh: http://www.ssh.com/academy/ssh/public-key-authentication

Tatu Ylonen, P. T. (2015, 10 15). *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*. Retrieved from NIST: https://www.nist.gov/publications/security-interactive-and-automated-access-management-using-secure-shell-ssh

Wilkins, S. (2013, 1 9). *Stateful Firewall Fundamentals: A Better, Easier, More Secure Firewall*. Retrieved from pluralsight: https://www.pluralsight.com/blog/it-ops/stateful-firewall-fundamentals#:~:text=A%20stateful%20firewall%20is%20a,and%20data%20packets%20in%20isolation.