DISCLAIMER:

ALL INFORMATION IS STRICTLY FICTIONAL THIS DOCUMENT IS A NETWORK DESIGN MODULE FROM MY FIRST YEAR AT UNIVERSITY

ROYAL MINT NETWORK DESIGN

Creating a High-Level Network Security Design

Sergiusz Pieszak

Contents

1. Introduction

The Royal Mint seeks a High-Level Network Security Design (HLD) (Figure 1) for its corporate network, covering departmental structure, communication flow, device selection, security measures, vulnerability identification, departmental isolation, OT integration, scalability, and construction challenges. Key aspects include IP addressing, VLANs, Access Control, and Firewalls, guided by CIA Triad principles and the newest frameworks and standards. The design should include diagrams and a Departments, IP Addresses & VLAN IDs table, considering the user/device count, connection types, access permissions, and OT involvement.

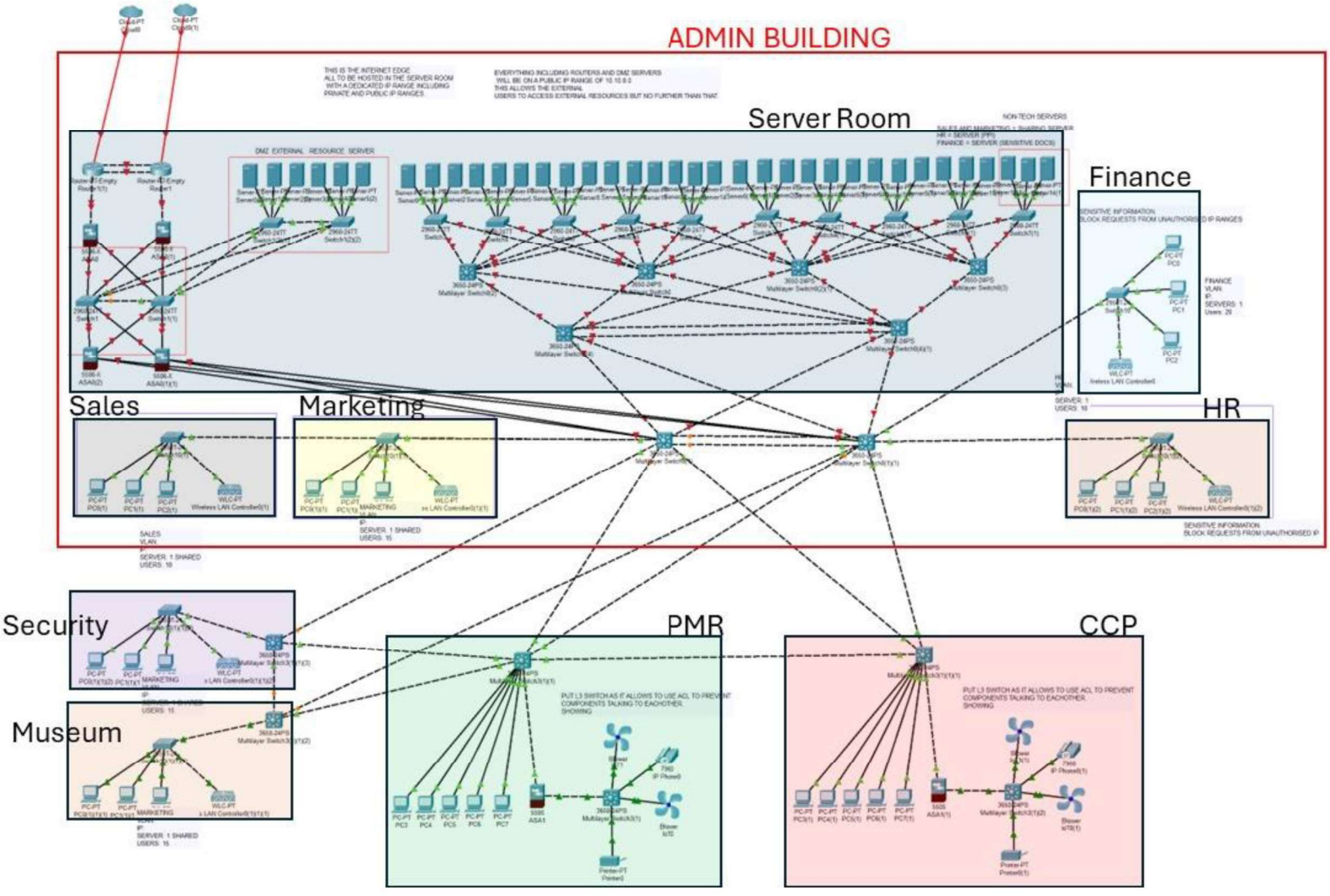


Figure 1 – Topology of the completed Network Design

2. Industry standards

In network design, adherence to necessary standards and frameworks is essential. The cyber landscape encompasses diverse standards and certifications to enhance businesses' cybersecurity and information security. These standards provide businesses with a variety of techniques, controls, and processes to establish and uphold a specific security threshold. Aligning with a chosen security standard allows businesses to showcase enhanced credibility to stakeholders, insurance providers, prospective clients, and partners. This is just one of the several advantages associated with meeting these standards as stated by Tripwire (2021)

In the UK there are several guidelines a company must abide by depending on what data and function they provide:

GDPR	GDPR stands for General Data Protection Legislation. It is a European Union (EU) law that came into effect on 25th May 2018. GDPR governs the way in which we can use, process, and store personal data (information about an identifiable, living person) - VinciWorks(2022)
Cyber Essentials	Cyber Essentials is a simple but effective, government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks. National Cyber Security Centre (no date a) It also has a self-assessment or more in depth certification called Cyber Essentials Plus
ISO 27000 Series	The ISO 27000 family of information security management standards is a series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best-practice information security management. - IT Governance (2016 a)
NIST	NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their

	networks and data. The Framework is voluntary. It gives your business an outline of best practices to help you decide where to focus your time and money for cybersecurity protection. You can put the NIST Cybersecurity Framework to work in your business in these five areas: Identify, Protect, Detect, Respond, and Recover. Federal Trade Commission (2018)
PCI DSS	The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard designed to reduce payment card fraud by increasing security controls around cardholder data. The Standard is a result of a collaboration between the major payment brands and is administered by the PCI SSC (Payment Card Industry Security Standards Council). - IT Governance (2016 b)

CIA Triad

The CIA triad —Confidentiality, Integrity, and Availability — is a fundamental component of security system development. It helps in identifying vulnerabilities and devising solutions. These three principles are essential for business operations and segmenting them helps security teams address each issue effectively. Achieving all three standards strengthens the organization's security profile, enhancing its ability to handle threats. “Ideally, when all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents.” as quoted by Fortinet (no date a)

ISO 27000 Series

ISO/IEC 27001 stands as the most comprehensive global standard for information security management systems (ISMS) and their requirements. Complemented by over a dozen standards within the ISO/IEC 27000 family, it encompasses the most effective practices in data protection and cyber resilience. As mentioned by ISO (no date) these standards enable organizations of different sectors and sizes to oversee

the security of assets such as financial data, intellectual property, employee information, and entrusted third-party data. ISO/IEC 27001 is widely regarded as the pinnacle standard coveted by all, hence our focus on it.

3. Architecture of the network

1. Zero Trust

Zero Trust Architecture (ZTA) is a cybersecurity strategy founded on the principle of "trust no one, verify everything". Unlike traditional security models, which often permit unrestricted access to users and devices once inside the perimeter, ZTA recognizes threats can occur from both inside and outside the network.

Access controls are strictly enforced regardless of user location, inside or outside the network perimeter. Each access request requires rigorous authentication and authorization. Ongoing monitoring continuously evaluates access based on factors such as device health, user behaviour, and resource sensitivity. This approach reduces the attack surface and mitigates the risk of data breaches by granting minimal access required for user or device functions.

The National Cyber Security Centre (no date b) discusses the principles of ZTA by delving into the following principles:

1. Understand your architecture, encompassing users, devices, and services.
2. Establish a robust single user identity.
3. Establish a robust device identity.
4. Implement authentication everywhere.
5. Monitor device and service health.
6. Prioritize monitoring of devices and services.
7. Apply policies based on service or data value.
8. Control access to services and data.
9. Do not trust the network, including the local network.

10. Select services designed for zero trust.

2. IEEE 802.1X

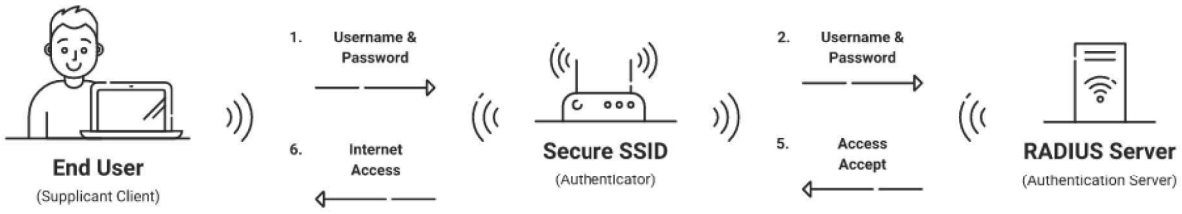


Figure 2 – Diagram from SecureW2 (no date), showing the connection of 802.1X protocol

Early IEEE 802 LAN protocols allowed users to access LAN resources through a control device, like an access switch, raising security concerns. To address this, the committee introduced the 802.1X protocol for wireless and wired LANs. Unlike other methods, 802.1X controls user-level access through access ports, defining controlled and uncontrolled ports. Successful authentication allows service packet transmission, while unsuccessful attempts restrict access to only authentication packets.

For instance, Yue, Z. (2021) mentions, on high security enterprise networks, 802.1X authentication is recommended. However, it requires the installation of 802.1X client software on terminals, making it unsuitable for public places such as airports and business centres with high user mobility and low security requirements. In such cases, Portal authentication is preferred. Additionally, for printers and fax machines that do not support 802.1X client software, MAC address authentication is employed instead of 802.1X.

3. Physical Access Control and Security

Ensuring physical access control and security is essential for network security. Incorporating measures such as RFID-controlled server rooms and CCTV surveillance is crucial to prevent unauthorized access. It's worth noting that this type of work is typically conducted by a separate third party.

4. Connecting to the internet

I have decided to have 2 ISP connections on the network edge to increase redundancy and resiliency to the network in case of attacks such as DDoS.

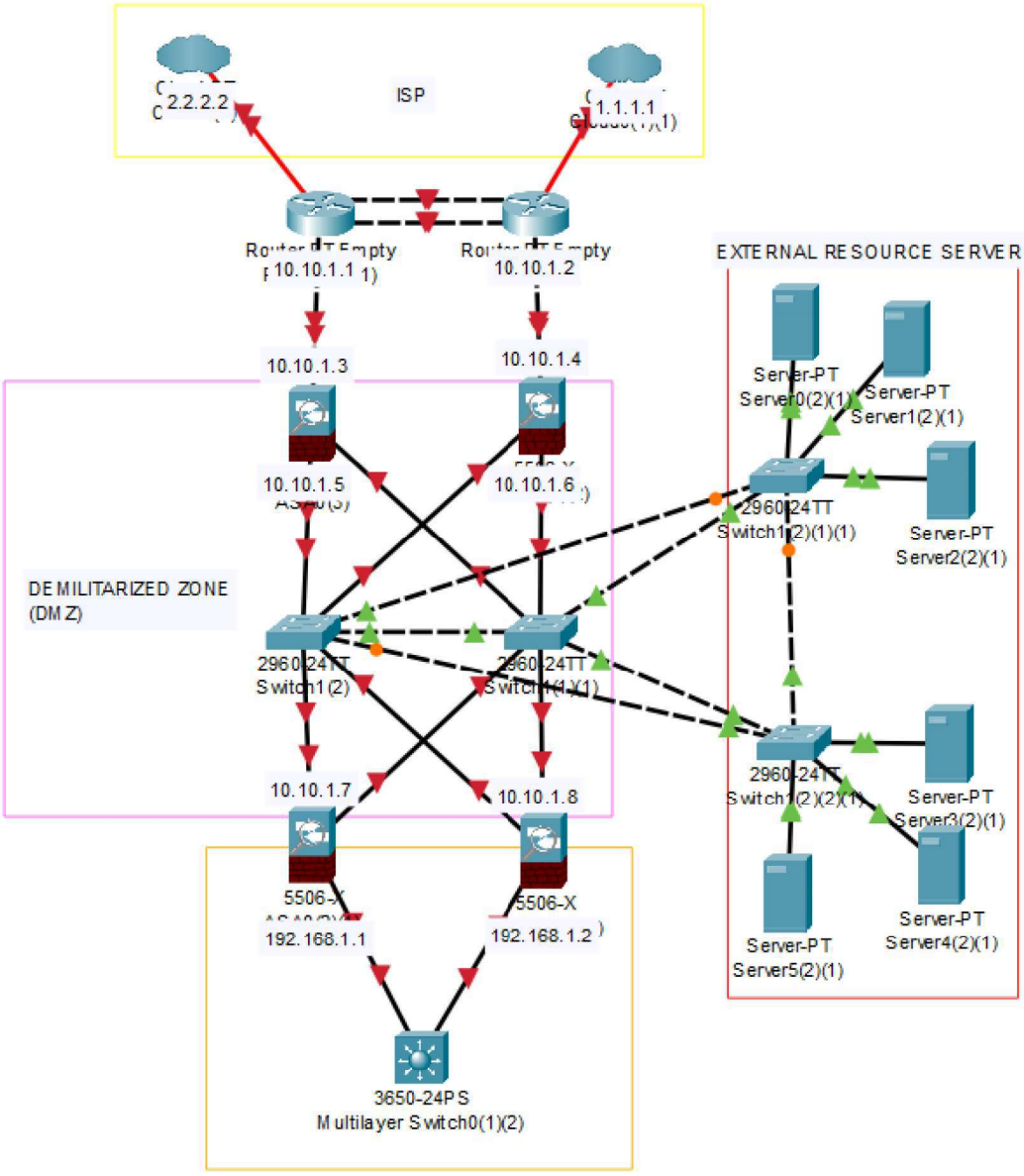


Figure 3 – Edge of network, including router and DMZ.

1. DMZ

As described by Fortinet (no date b) a DMZ, or demilitarized zone, acts as a perimeter network enhancing an organization's internal LAN security against untrusted traffic. By hosting external-facing services like DNS, FTP, mail, proxy, and web servers in the DMZ, organizations enable internet access while safeguarding their LAN from direct intrusion. This setup minimizes vulnerabilities, ensuring secure communication and data sharing among employees.

Implemented a DMZ to separate external and internal networks, isolating externally facing data such as website hosting and VoIP to prevent interference with the internal network. In case of attack, only DMZ-connected resources are affected, ensuring uninterrupted internal network operation. The DMZ is fortified with two external and two internal firewalls. The first pair filters all traffic, while the second pair monitors and blocks further traffic.

2. Router and firewall setup

Opted for dual ISP connections to enhance reliability and connectivity robustness. Each ISP connection is supported by a dedicated router interconnected for load balancing; however, this configuration can lead to 'double NAT' issues, causing data delays. This challenge is solved using HSRP, a redundancy protocol ensuring fault-tolerant default gateway operation. Hitzel, B. (2022)

The external firewalls offer simplified deployment and management by monitoring the network perimeter and blocking unauthorized external access. They are a frontline defence against external threats such as hackers, malware, and denial-of-service attacks, and can facilitate network address translation (NAT) to hide internal network addresses.

However, external firewalls are not sufficient to protect against internal threats such as insider attacks or compromised devices. They rely on traditional port-based threat identification, which can be evaded by sophisticated attackers. Which is why 802.1X has been implemented, to counteract such a threat.

3. Server room

Chose to establish a dedicated server room with its own IP range to enhance security and operational convenience. This centralized space provides the internet connection, DMZ, all servers, and L3 switches for distributing data to various departments, providing a more secure alternative to having servers scattered across departments. Choosing a mesh topology provides numerous advantages such as load balancing, reducing single points of failure, scalability and redundancy. Despite

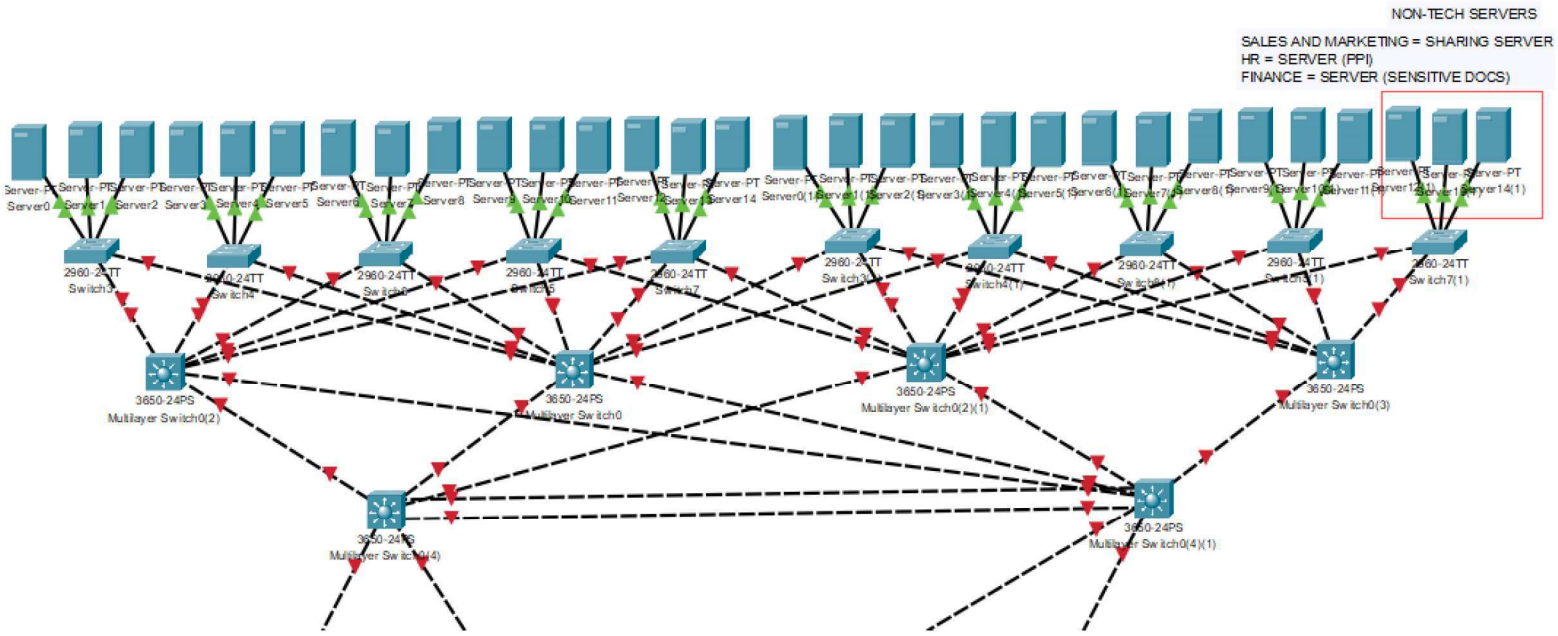


Figure 4 – Mesh network showing server interconnectivity

the higher cost, prioritizing reliable access to data over cost savings is paramount in today's paramount landscape.

5. IP and subnetting Scheme

Department	IP Address	Hosts	Subnet Mask	VLAN ID	Number of Switches	End Devices
Server Room (Internet	10.10.1.0	30	255.255.255.224	NULL	x2 L2 for DMZ	External servers (number unknown)

connectivity and DMZ)					For external resource servers (Unknown)	2 External Routers 2 External Firewalls
Server Room (Technology Dep)	172.16.1.0	126	255.255.255.128	1	20 x 2960-24TT 12 x 3650-24PS 2 x for internal distribution	60 Internal Servers 2 Internal Firewalls
Finance	192.168.11.0	30	255.255.255.224	11	L2 – No fibre required	20 PC
Technology	192.168.12.0	62	255.255.255.192	12	L2 - No fibre required	30 PC
HR	192.168.13.0	30	255.255.255.224	13	L2 - No fibre required	10 PC
Marketing	192.168.14.0	30	255.255.255.224	14	L2 - No fibre required	15 PC
Sales	192.168.15.0	30	255.255.255.224	15	L2 - No fibre required	10 PC
CCP (IT)	192.168.21.0	30	255.255.255.224	21	3650-24PS	10 Shared PC
CCP (OT)	192.168.22.0	30	255.255.255.224	22	3650-24PS Need's L3	10 OT
PMR (IT)	192.168.31.0	30	255.255.255.224	31	3650-24PS	20 Shared PC

PMR (OT)	192.168.32.0	30	255.255.255.224	32	3650-24PS Need's L3	20 OT
Museum	192.168.41.0	14	255.255.255.240	41	3650-24PS	4 Tills 1 WAP
Security Lodge	192.168.51.0	14	255.255.255.240	51	3650-24PS	5 PC

1. Subnetting

Subnetting is a crucial component of network management and security by restricting IP ranges. It minimizes surplus broadcast traffic and fortifies security by limiting accessible ports, hindering potential attackers. Furthermore, it complicates network scanning tools such as Nmap, hindering attackers' comprehension of the network structure. To balance security and future scalability, I have chosen to allocate each department to a distinct IP range while constraining the subnet. This approach facilitates effortless expansion through straightforward resubnetting when departments require additional hosts on the network.

2. VLANs

VLANs provide streamlined administration by grouping dispersed end-stations logically, eliminating the need for frequent reconfiguration when users relocate or alter job functions. They also confine broadcast domains, reducing the need for routers and minimizing network traffic. Additionally, VLANs enforce security policies by preventing end-stations from receiving unintended broadcasts and blocking communication between VLANs without a router, thus enhancing network security. University of Wollongong (no date)

6. Departments

All other departments are very similar to each other, requiring PC connectivity and having wireless access points. Additional changes to individual departments are listed below:

1. Additional Servers:

HR, Finance, Sales, and Marketing departments require servers. HR and Finance, providing SPII and High-Risk Data, necessitate dedicated servers. To restrict access to specific departments, a server-side firewall was implemented to prevent all other traffic from being blocked.

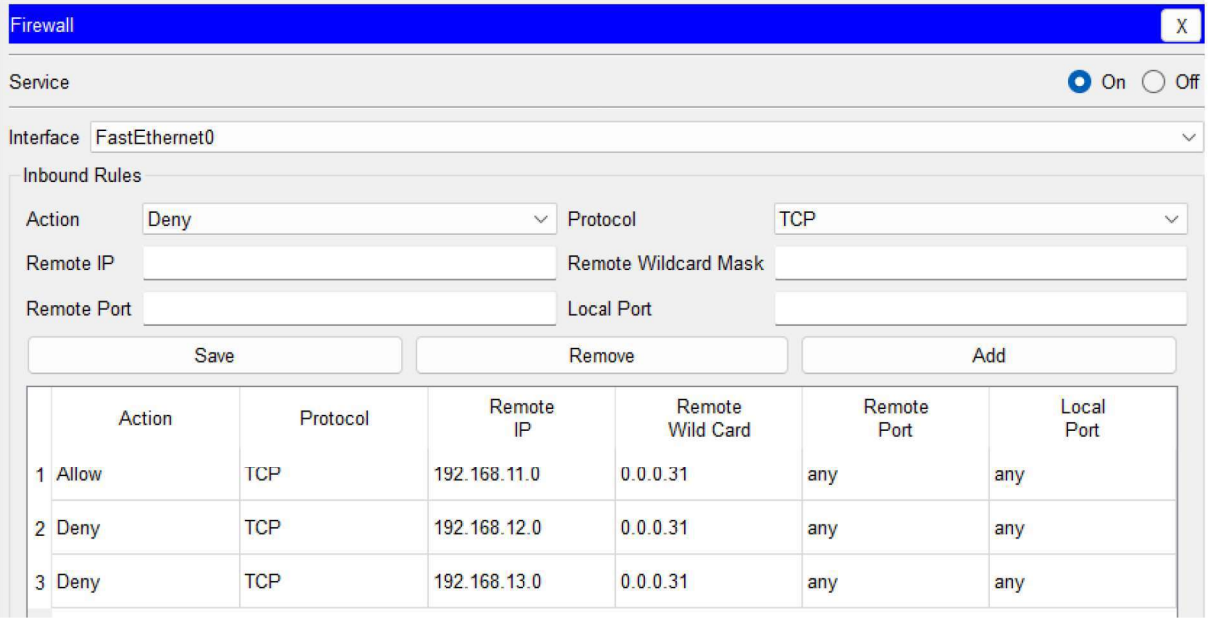
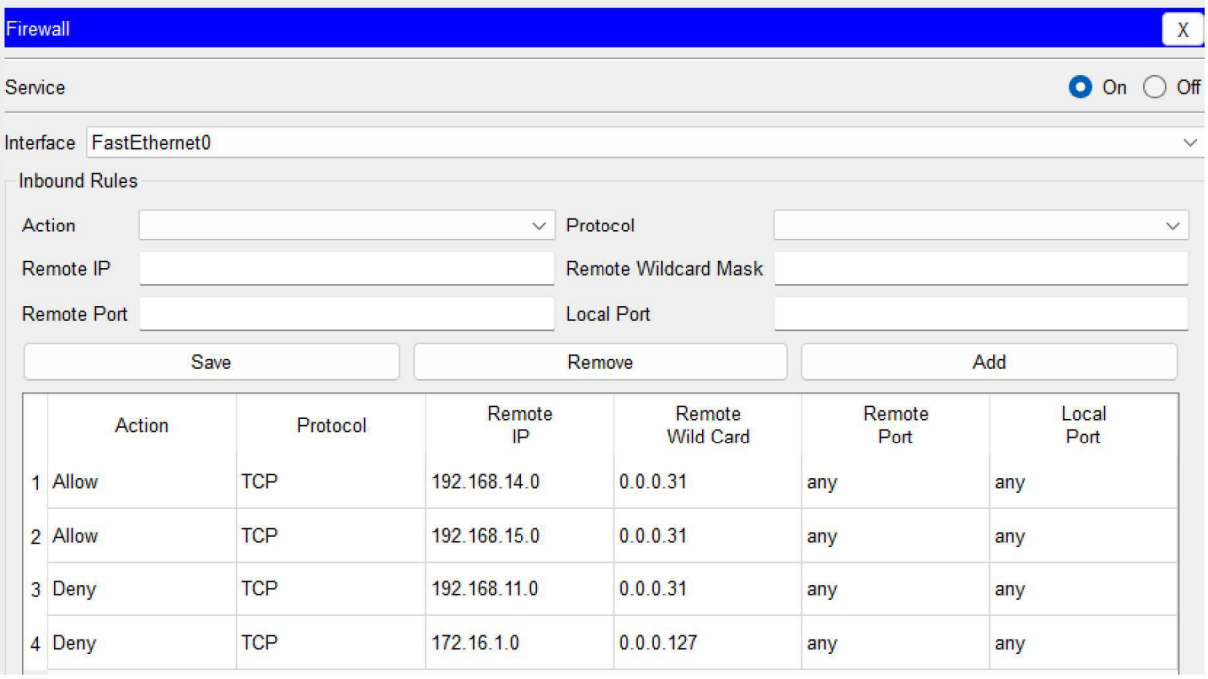


Figure 5 – Firewall rules example, this would be used for HR and Finance

Sales and marketing share a server; therefore, firewall rules have been implemented to allow both departments to access the information.



	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	TCP	192.168.14.0	0.0.0.31	any	any
2	Allow	TCP	192.168.15.0	0.0.0.31	any	any
3	Deny	TCP	192.168.11.0	0.0.0.31	any	any
4	Deny	TCP	172.16.1.0	0.0.0.127	any	any

Figure 6 – Firewall rules for Sales and Marketing, note 2 ip ranges being allowed access

2. Museum

In managing financial transactions through tills, the museum maintains strict compliance with the Payment Card Industry Data Security Standard (PCI DSS 4.0) to ensure network safety. This updated version entails a comprehensive checklist Harrington, D. (2023):

1. Install and maintain a firewall.
2. Eliminate vendor default settings.
3. Protect stored cardholder data.
4. Encrypt payment data transmission.
5. Regularly update antivirus software.
6. Deploy secure systems and applications.
7. Restrict cardholder data as necessary.
8. Assign user access identification.
9. Restrict physical access to data

10. Track and monitor network access.
11. Conduct ongoing systems and process testing.
12. Create and maintain an information security policy.

7. CCP and PMR

1. IT

All IT end devices are detailed in the table provided. The choice has been made to divide the IP range between IT and OT for streamlined expansion and network management by administrators.

2. OT

Operational Technology (OT) demands heightened security measures when integrating with a network. To enhance security, a firewall isolates the OT from other network components. Internally, OT connectivity is facilitated through an L3 switch, which enables access control and restricts OT communication, mitigating risks such as USB drop attacks. This precaution is vital given the susceptibility of SCADA and OT systems to such attacks, owing to historically limited security focus from developers.

8. References

Federal Trade Commission (2018) *Understanding the NIST cybersecurity framework*. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (Accessed on: 11 March 2024)

Fortinet (no date a) *What is the CIA Triad and Why is it important?* Available at: https://www.fortinet.com/uk/resources/cyberglossary/cia-triad (Accessed on: 8 March 2024)

Fortinet (no date b) *What Is a DMZ Network and Why Would You Use It?* Available at: https://www.fortinet.com/uk/resources/cyberglossary/what-is-dmz (Accessed on: 14 March 2024)

Harrington, D. (2023) *The 12 PCI DSS Requirements: 4.0 Compliance Checklist.* Available at: https://www.varonis.com/blog/pci-dss-requirements (Accessed on: 2 March 2024)

Hitzel, B. (2022) *Network Design: Dual ISP, DMZ, and the Network Edge*. Available at: https://www.networkdefenseblog.com/post/network-design-network-edge (Accessed on: 9 March 2024)

IT Governance (2016 a) *ISO 27000 Series of Standards*. Available at: https://www.itgovernance.co.uk/iso27000-family (Accessed on: 7 March 2024)

IT Governance (2016 b) *PCI DSS | What It Is and How to Comply*. Available at: https://www.itgovernance.co.uk/pci_dss (Accessed on: 8 March 2024)

ISO (no date) *ISO/IEC 27000 family.* Available at: https://www.iso.org/standard/iso-iec-27000-family (Accessed on: 12 March 2024)

National Cyber Security Centre (no date a) *Cyber Essentials*. Available at: https://www.ncsc.gov.uk/section/products-services/cyber-essentials (Accessed on: 9 March 2024)

National Cyber Security Centre (no date b) *Zero trust architecture design principles*. Available at: https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles (Accessed on: 8 March 2024)

SecureW2 (no date) *What is 802.1X? How Does it Work?* Available at: https://www.securew2.com/solutions/802-1x (Accessed on: 14 March 2024)

Tripwire (2021) *The Importance of Cybersecurity Standards and Certifications for SMBs.* Available at: https://www.tripwire.com/state-of-security/the-importance-of-cybersecurity-standards-and-certifications-for-smbs (Accessed: 12 March 2024)

University of Wollongong (no date) *Advantages of VLANs*. Available at: https://documents.uow.edu.au/~blane/netapp/ontap/nag/networking/concept/c_oc_netw_vlan-advantages.html (Accessed on: 11 March 2024)

VinciWorks (2022) *What is GDPR in simple terms?*, Available at: https://vinciworks.com/blog/what-is-gdpr-in-simple-terms (Accessed: 11 March 2024).

Yue, Z. (2021) *What Is 802.1X?* Available at: https://info.support.huawei.com/info-finder/encyclopedia/en/802.1X.html (Accessed on: 14 March 2024)