# COMP1002 Assignment 2: Report

## Introduction

This report is written with the intention of proposing a robust and scalable solution for a network and cyber security infrastructure for a direct-to-consumer sales company called DirectSales UK. Due to the current dynamic of today’s business environment, scalability is important to ensure growth and adapt to changing demands. With this in mind, my solutions will not only aim to meet the requirements of the company but will also allow for expansion and evolution over time. The report will be structured by beginning with an overview of the system architecture, which is followed by the network architecture and the security architecture, and finally finishing with a conclusion. The system architecture will cover the requirements and set the core infrastructure of the proposal. The network architecture will describe the network solutions, explaining the pros and cons of each and why it is the best fit. The security architecture will be explained in the same way as the network architecture; however, it will cover the security side of the network. Finally, I will conclude everything that I have proposed, discussing any potential issues and providing an insight into any implications.

## System Architecture

The system architecture will provide a high-level view of the solution, describing the components that make up the network and how they interact [1]. Creating the architecture of a system requires the aims and requirements to be defined. DirectSales UK has given me a set of initial requirements that need to be followed in order to create a successful solution. In response to the requirements provided, my proposed solution must encompass key aims such as scalability, reliability, performance, security, and manageability, which will create a successful infrastructure.

**Requirements/aims**

* Scalability: The proposed solution will aim to be scalable in order to accommodate the needs of the company while allowing for future growth. Making the network scalable will allow the company to grow their operations and user base, which needs to be prepared for as they plan to increase the sales team in two years’ time.[2]
* Reliability: Ensuring that the network is always available and providing authentic service is a key aim. The solution will need to consider minimizing downtime and making sure that the main services are always accessible to employees and customers, ensuring availability. [2]
* Performance: The infrastructure will be designed to maximize user performance, ensuring that communication across the network is fast and reliable. There will be considerations of bandwidth requirements, latency, and throughput. [2]
* Security: Providing a secure network is one of the most important requirements. The solution will need to include robust and secure security measures that will protect against data leaks, unauthorized access, and any other risks or threats to the network and company data. This ensure the confidentiality and integrity of the data. [2]
* Manageability: The management of the network is essential for the company to use it efficiently. The management will ensure that everything is monitored and that everything is running smoothly. This will allow for improved productivity and security, as well as minimized costs. [2]

**Core infrastructure**

The initial requirements of hosts that the network needs to have are 140, which are for the staff PC’s, staff Wi-Fi, and guest network. The company’s web and e-commerce systems need to have a minimum of 20 hosts. As the company is going to increase in size, the network needs to be built for scalability while also focusing on reliability, performance, and security.

* Network Components: The network will consist of routers, switches, and access points for the devices to be able to connect to. It will use Cat5e cabling to provide high-speed connectivity but will also have Wi-Fi for the staff and guests. [11]
* Server Components: The server infrastructure will contain critical business applications, databases, and file storage services for day-to-day operations. This includes web servers, application servers, database servers, and file servers. [11]
* Security Components: The security of the network is one of the main concerns in keeping the data secure. There will be robust measures implemented to protect against any cyber threats, unauthorized access, and data breaches. This includes firewalls, intrusion detection and prevention systems, VPNs, encryption protocols, and access control mechanisms to safeguard sensitive information. [11]
* Storage Components: The storage infrastructure comprises network-attached storage (NAS) devices and storage area networks (SANs) to provide centralized data storage, backup, and disaster recovery capabilities. Redundant storage arrays, RAID configurations, and data replication techniques are employed to ensure data integrity, availability, and resilience. [11]

## Network Architecture

The network architecture will serve as the backbone of the company’s operations, facilitating efficient communication, data management, and customer engagement. By providing a robust and reliable infrastructure for data transmission, the network architecture ensures that critical information flows swiftly and securely between employees.

A diagram of a computer network

Description automatically generated

**Architecture type**

The architecture used will be the client-server architecture. It will be implemented to manage the flow of data within the network. In this architecture, client devices communicate with centralized servers to access resources and services. This approach offers several advantages, including centralized data storage, easier management of resources, and enhanced security through access controls enforced at the server level. The servers, including the file, web, application, and data servers, will be used for specific functions and will give client devices the services they need as needed. Using this architecture can ensure that data is managed efficiently and critical business resources are easily accessed. [26]

**Logical Components**

* Network Topology: The star topology stands out as the most suitable choice for DirectSales UK’s network infrastructure, offering simplicity in setup and management. With centralized control and monitoring, it ensures fault tolerance and scalability, allowing seamless expansion as the company grows. However, the centralized switch introduces a single point of failure. If it fails, all connected devices may lose connectivity, potentially causing downtime and latency issues. [8]
* Virtual LANs (VLANs): VLANs are used to separate the network infrastructure to improve its security and efficiency. Despite their benefits in traffic segregation and improved network management, implementing VLANs can be complex and costly [6]. Misconfiguration may introduce a single point of failure, affecting connectivity for devices with the VLAN. This means that careful consideration is essential when implementing VLANs. I have proposed five VLANs for segregating the network.

**Physical Components**

* Cabling: Cate5e Ethernet cables are recommended for the network infrastructure, providing support for up to 1Gbit bandwidth. While Cat6 cables offer higher speeds, the current network requirements do not necessitate the additional expense. Cat5e cables offer a cost-effective solution while still providing sufficient performance for the company’s needs.
* Router: A business-grade router that can support VPN connectivity for secure remote access is essential. The router should be able to accommodate over 200 employees for future scalability. One router will allow the entire company to connect to the internet. The router might have a higher upfront cost; however, the additional features justify the investment. [3]
* Switches: Switches are required to connect users to the local network. Each switch supports VLAN configuration to segregate traffic and ensure efficient network management. The downside to switches is that each switch in the network provides a single point of failure. Therefore, if a switch fails, the devices connected to it may lose connectivity [3]. Though redundancy measures can be implemented to mitigate the single points of failure. Each switch I have provided connects the different parts of the network, making each section more secure with the VLAN.
* Wireless Access Points: Business-grade access points are required to provide adequate coverage for the entire office space. This configuration ensures optimal performance and minimal interference [3]. However, the more access points that are being used, the more gateways there will be for a hacker to access the network. This means that they need to be secured with encryption and SSID masking, and they need to be placed carefully in order to avoid connectivity outside of the building. There are fewer employee hosts using the WAP compared to guests; however, I have included the same amount due to scaling.
* Network Attached Storage (NAS): A 4TB to 8TB NAS with RAID capabilities will be used for storing and backing up data. This scalable storage solution ensures data availability and integrity, with room for expansion as the company grows [4]. The only con to it is that it requires an initial investment, which could be expensive up front. However, this is a better option than choosing cloud storage for backing up data because it is cheaper in the long run and the company will have full control over the storage of the data. A NAS is attached to the admins and sales switches.[5]
* Uninterruptible power supply (UPS): A UPS will provide backup power to the critical components of the network, such as the router, switches, servers, and firewalls, during power outages. It is used to prevent data loss or corruption of any unsaved data [12]. It will have an initial upfront cost and require maintenance, but it is very useful to minimize network.
* Network Printers: Business printers with Ethernet connectivity will be deployed to facilitate printing, scanning, and resource sharing over the network. Features such as duplex printing, secure printing, and mobile printing enhance productivity and efficiency [13]. It requires a lot of maintenance, and it needs to be well configured in order to be efficient. Like the access points, it is also used as another entry way into the network by hackers, meaning that it needs to be secured within the network. I have included a printer for admin and sales to keep the data being sent to the printer specific to that section.
* Servers: File, web, application, and database servers will be deployed to support various business functions. These servers provide essential services and data storage, enabling efficient business operations. The servers may be a costly up-front purchase and will require ongoing maintenance, which could be another big cost [3]. To lower costs, a Virtual Machine (VM) server could be used to implement the web and e-commerce systems. However, I have chosen that server to be physical because it would be easier to secure them physically on site and virtually with firewalls and IDPS. Moreover, the hardware will be reliable to ensure the high availability of the website.

**Addressing Scheme**

A subnet of the network will be created to segregate the network. \*[See end of report]

## Security Architecture

The security architecture for the network needs to be strong to protect against any malicious attacks or threats by stopping them from being able to access or spread across the network [14]. All of the security measures that are listed will cover the security requirement. These are the different security measures that need to be put in place for maximum protection:

* Firewall: A Unified Threat Management (UTM) firewall will provide firewalling, antivirus, and web filtering. This solution is used to control user traffic and protect against various cyber threats. It will create a barrier between the network and internet, which allows the user to control what goes in and out of the network, stopping unauthorized users from being able to gain access [15]. The disadvantages of firewalls are that they will not prevent malware from entering the system; however, other systems will be implemented to protect against this. If a software firewall is implemented, then it will use the processing power of the device to run the firewall, making the performance of the device slow. This means that a physical firewall should be implemented, as it will not affect the performance of any devices in the network [15]. A firewall between the Wi-Fi switch and router should also be implemented in case unauthorized users gain access to the network through the WAPs.
* Intrusion detection and prevention system (IDPS): The IDPS will detect and mitigate any malicious attacks on the network, enhancing integrity and confidentiality. Through network-based IDPS (NIPS), threats are swiftly detected and addressed, preempting potential network damage. Wireless intrusion prevention systems (WIPS) further secure wireless access points, while the network behavior analysis system (NBA) monitors overall network activity [17]. These measures ensure efficient network surveillance, mitigating any risks that human error might overlook.
* VPN: A VPN will be deployed in the router to enable secure remote access to the network for any employees that may be remote. By encrypting data transmissions over public networks, VPNs ensure secure connectivity and protect sensitive information from interception [14]. However, if an attacker gained access to an employee’s VPN credentials, they could exploit network vulnerabilities [18].
* SSID Masking: The Service Set ID (SSID) “acts as the name of your network” [19] and is used so that devices can find and connect to the network wirelessly. SSID masking hides the network name, making it more challenging for attackers to connect. It doesn’t directly protect the network; however, it does make unauthorized access more difficult. This means that users may also find it challenging to connect to the network, particularly those less familiar with technology [20]. Therefore, it’s advisable to only implement it on the employee network rather than the guest network, ensuring that efficiency and productivity for guests are maintained.
* Encryption: While data is at rest and being transported over the network, it should be encrypted to secure it in the event that it is intercepted. This means that the hacker would not be able to access the data unless they had the decryption key, which only the user would have. This provides a high level of security for the data and ensures that integrity is maintained. However, this means that accessing the data can take more effort and time, decreasing productivity [25].
* Access Control Lists (ACLs): An access control list (ACL) is used as a gate to restrict access to specific data or resources [21]. Similar to social media settings, ACLs determine who can access certain information [22]. Implemented in firewalls, ACLs manage data entering and leaving the network and within the network itself. This ensures only authorized users access confidential information, enhancing manageability. However, misconfiguration may lead to unauthorized access or data restriction issues. These risks can be mitigated effectively with proper setup and configuration.
* Network Segmentation: Network segmentation is used as a security measure to split the network into different sections. This allows the business to control what traffic goes in and out of each section controlling what each user can access [25]. It can be done in many different ways, such as through subnetting, VLANs, and access control lists. Without this, there is very limited control over what users can access and what hackers could access if they managed to access the network.
* Data loss prevention: If the data stored on the network gets corrupted or lost, it may not be recovered if there is not a solution in place. Using network-attached storage or cloud storage can be a good way to backup data in the event that it is destroyed. This will allow for easy recovery of the data, and it will not leave the business with a negative impact.
* Antivirus and antimalware software: Antivirus and antimalware software are essential for network security, as they protect against viruses, malware, spam emails, untrustworthy websites, and spyware [23]. Installing this across firewalls, routers, servers, and devices is relatively simple and cost-effective, making it a worthwhile investment. While it may slow down systems due to continuous background operation, it significantly reduces the risk of data loss and network downtime. Although it doesn’t offer absolute protection, it effectively mitigates the majority of threats. Integrating it with IDPS enhances network defense, ensuring that threats are identified and addressed promptly, even if they evade antivirus detection.

## Conclusion

To conclude, the proposed network and cyber security infrastructure for DirectSales UK has provided a robust and scalable solution to meet the company’s current and future needs. The architecture that I have designed encompasses various components and measures to ensure scalability, reliability, performance, security, and manageability.

The foundation set by the system architecture defines clear aims and requirements, as well as highlighting the essential components for creating a robust network and security infrastructure. Delving into the network architecture, the utilization of star topology and client-server architecture facilitates centralized management and control. The incorporation of VLANs and network segregation enhances monitoring and security, safeguarding the confidentiality and availability of company data. The physical components that have been selected will optimize performance, security, and scalability while further allowing the integrity of data to remain with backup solutions like the NAS.

Additionally, the security architecture is thoroughly explored, highlighting various measures implemented to safeguard against malicious threats and unauthorized access, thereby ensuring the confidentiality, integrity, and availability of company data. The security solutions not only protect the network from being attacked, but they also protect the data, through encryption and using the NAS, in the event that the network is attacked and the data is damaged or destroyed. There is also complete control over what users can access with the ACLs and firewalls, which provides a high level of confidentiality.

Throughout the report, careful consideration has been given to designing and implementing the network and security architecture. Factors such as scalability, reliability, performance, security, and manageability have been meticulously addressed to provide a robust solution. However, despite the planning, there are still some open issues and challenges that need to be addressed:

The security measures are used to protect the network, but this can also lead to a decrease in workflow and productivity. There needs to be a perfect balance between security measures and the user experience in order for there to be high performance. This leads to the cost considerations, which, due to their not being a specified budget, may be a challenge. The upfront costs associated with hardware, software, and ongoing maintenance must be evaluated to ensure cost-effectiveness without compromising the security of the network. Implementing a cost-effective network could also create more issues with the complexity of implementation. My proposed solution has been designed with this consideration in mind by designing a relatively simple but secure and efficient network. However with the unknown layout of the building, more components may need to be added where there might be devices that are out of range of the Wi-Fi. Scalability in the future could also pose an issue where more switches or devices may need to be added if the network becomes more congested.

While challenges may arise, the proposed infrastructure lays a strong foundation for DirectSales UK’s operations, enabling them to navigate the complexities of today’s business landscape with confidence and resilience.

## References

[1] InterviewBit Blog (2024) "System Architecture." InterviewBit. Accessed on April 22, 2024. Available at: [https://www.interviewbit.com/blog/system-architecture/]

[2] InformIT. (2002) "The Importance of a Layered Approach to Network Security." Accessed on April 22, 2024. Available at: [https://www.informit.com/articles/article.aspx?p=29030&seqNum=5]

[3] Maundu, Boney (2023) "Computer Networks for Small and Medium-Sized Businesses." LinkedIn. Accessed on April 22, 2024. Available at: [https://www.linkedin.com/pulse/computer-networks-small-medium-sized-businesses-boney-maundu/]

[4] Seagate (No date) "What Is NAS (Network Attached Storage)?" Accessed on April 22, 2024. Available at: [https://www.seagate.com/gb/en/blog/what-is-nas-master-ti/]

[5] StoneFly. (No date) "NAS vs. Cloud Storage: Which Is Best for Your Hybrid Workforce?" Accessed on April 22, 2024. Available at: [https://stonefly.com/blog/nas-vs-cloud-storage-which-is-best-for-your-hybrid-workforce/]

[6] Ergun, Orhan. (2023) "Subnetting vs VLAN." Accessed on April 22, 2024. Available at: [https://orhanergun.net/subnet-vs-vlan#:~:text=Subnetting%20and%20VLANs%20are%20two,within%20the%20same%20physical%20infrastructure.]

[7] LinkedIn.(No date) "What are the Advantages and Disadvantages of Using VLANs?" Accessed on April 22, 2024. Available at: [https://www.linkedin.com/advice/3/what-advantages-disadvantages-using-vlans]

[8] JavaTpoint.(No date) "Star Topology: Advantages and Disadvantages." Accessed on April 22, 2024. Available at: [https://www.javatpoint.com/star-topology-advantages-and-disadvantages]

[9] NordVPN.(2024) "What Is Network Architecture?" Accessed on April 22, 2024. Available at: [https://nordvpn.com/blog/network-architecture/#:~:text=Hide-,What%20is%20network%20architecture%3F,many%20ways%20to%20build%20it.]

[10] Sheldon, Robert (No date) "EIGRP (Enhanced Interior Gateway Routing Protocol)." Accessed on April 22, 2024. Available at: [https://www.techtarget.com/searchnetworking/definition/EIGRP]

[11] PyNet Labs.(2024) "Computer Network Components." Accessed on April 22, 2024. Available at: [https://www.pynetlabs.com/computer-network-components/]

[12] RS Components.(2023) "UPS Power Supplies Guide." Accessed on April 22, 2024. Available at: [https://uk.rs-online.com/web/content/discovery/ideas-and-advice/ups-power-supplies-guide]

[13] Lenovo. (No date) "Network Printer Glossary." Accessed on April 22, 2024. Available at: [https://www.lenovo.com/us/en/glossary/network-printer/?orgRef=https%253A%252F%252Fwww.google.com%252F]

[14] Cisco. (No date) "Small Business Network Security Checklist." Accessed on April 22, 2024. Available at: [https://www.cisco.com/c/en\_uk/solutions/small-business/resource-center/security/network-security-checklist.html#~types-of-security]

[15] Cisco. (No date) "What Is a Firewall?" Accessed on April 22, 2024. Available at: [https://www.cisco.com/c/en\_uk/products/security/firewalls/what-is-a-firewall.html#:~:text=A%20firewall%20is%20a%20network,security%20for%20over%2025%20years.]

[16] Great Learning. (2024) "Disadvantages of Using Firewalls." Accessed on April 22, 2024. Available at: [https://www.mygreatlearning.com/blog/what-is-network-security-firewall/#disadvantages-of-using-firewalls]

[17] Red Hat. (2023) "What Is an Intrusion Detection and Prevention System (IDPS)?" Accessed on April 22, 2024. Available at: [https://www.redhat.com/en/topics/security/what-is-an-IDPS#:~:text=Red%20Hat%20help%3F-,Overview,intrusion%20detection%20system%20(ids).]

[18] Cloudflare. (No date) "What Is a Business VPN?" Accessed on April 22, 2024. Available at: [https://www.cloudflare.com/learning/access-management/what-is-a-business-vpn/]

[19] Charles, Trey. (2023) "What Is an SSID?" Accessed on April 22, 2024. Available at: [https://www.privateinternetaccess.com/blog/what-is-ssid/#:~:text=Yes%2C%20changing%20your%20SSID%20can,take%20some%20additional%20precautionary%20measures.]

[20] Rutledge, Samantha. (2020) "Should You Hide Your Wi-Fi SSID?" Accessed on April 22, 2024. Available at: [https://fractionalciso.com/should-you-hide-your-wi-fi-ssid/]

[21] Anyanwu, Chidiadi. (2023) "A Deep Dive into Access Control Lists." Accessed on April 22, 2024. Available at: [https://www.freecodecamp.org/news/a-deep-dive-into-access-control-lists/]

[22] Syracuse University. "Access Control." Accessed on April 22, 2024. Available at: [https://web.ecs.syr.edu/~wedu/Teaching/CompSec/LectureNotes\_New/Access\_Control.pdf]

[23] GeeksforGeeks. (2022) "Anti-Virus: Its Benefits and Drawbacks." Accessed on April 22, 2024. Available at: [https://www.geeksforgeeks.org/anti-virus-its-benefits-and-drawbacks/]

[24] Cisco. (No date) "What Is Network Segmentation?" Accessed on April 22, 2024. Available at: [https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html]

[25] Catalyst2. (No date) "Encryption at Rest: Its Purpose and Benefits, Setbacks." Accessed on April 22, 2024. Available at: [https://www.catalyst2.com/blog/encryption-at-rest-its-purpose-and-benefits-setbacks/]

[26] Heavy.ai. (No date) 'Client-Server.' Accessed on April 22, 2024. Available at: [https://www.heavy.ai/technical-glossary/client-server](https://www.heavy.ai/technical-glossary/client-server)

**\*Addressing Scheme**

**Network: 26. 2 . 6.0 / 24**

Sales

|  |  |
| --- | --- |
| **Specification** | **Value** |
| Number of bits in the subnet | 2 |
| New IP mask (decimal) | 255.255.255.192 |
| Number of usable subnets | 4 |
| No. of usable hosts per subnet | 62 |
| Network address | 26.2.6.0/26 |
| First IP Host address | 26.2.6.1 |
| Last IP Host address | 26.2.6.62 |
| Broadcast ID | 26.2.6.63 |

Guest wifi

|  |  |
| --- | --- |
| **Specification** | **Value** |
| Number of bits in the subnet | 2 |
| New IP mask (decimal) | 255.255.255.192 |
| Number of usable subnets | 4 |
| No. of usable hosts per subnet | 62 |
| Network address | 26.2.6.64/26 |
| First IP Host address | 26.2.6.65 |
| Last IP Host address | 26.2.6.126 |
| Broadcast ID | 26.2.6.127 |

Employee wifi

|  |  |
| --- | --- |
| **Specification** | **Value** |
| Number of bits in the subnet | 2 |
| New IP mask (decimal) | 255.255.255.192 |
| Number of usable subnets | 4 |
| No. of usable hosts per subnet | 62 |
| Network address | 26.2.6.128/26 |
| First IP Host address | 26.2.6.129 |
| Last IP Host address | 26.2.6.190 |
| Broadcast ID | 26.2.6.191 |

Admin

|  |  |
| --- | --- |
| **Specification** | **Value** |
| Number of bits in the subnet | 3 |
| New IP mask (decimal) | 255.255.255.224 |
| Number of usable subnets | 8 |
| No. of usable hosts per subnet | 30 |
| Network address | 26.2.6.192 /27 |
| First IP Host address | 26.2.6.193 |
| Last IP Host address | 26.2.6.222 |
| Broadcast ID | 26.2.6.223 |

Servers

|  |  |
| --- | --- |
| **Specification** | **Value** |
| Number of bits in the subnet | 3 |
| New IP mask (decimal) | 255.255.255.224 |
| Number of usable subnets | 8 |
| No. of usable hosts per subnet | 30 |
| Network address | 26.2.6.224/27 |
| First IP Host address | 26.2.6.225 |
| Last IP Host address | 26.2.6.254 |
| Broadcast ID | 26.2.6.255 |