70% DirectSale's Expansion Report - Alfie Nurse

Introduction:

This report will address the challenges faced by **DirectSales UK** in their efforts to expand into Plymouth. To deal with these challenges, it is necessary to set-out a comprehensive networking and cybersecurity infrastructure. The design and implementation of such infrastructure needs to be considered carefully, to both maximise operational speed and efficiency whilst also prioritising data security and accommodating for future growth.

Given the requirements outlined in the project brief, this report will propose a comprehensive network architecture that will provide the necessary infrastructure for staff PCs, staff and guest WiFi, and the company's web/e-commerce systems. My proposal will also contain a robust framework that will support expansion by making use of the latest technological advancements and cybersecurity measures. These technologies include advanced firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to ensure robust security. We will also implement virtual private networks (VPNs) to secure remote access as well as making use of next-generation antivirus solutions. Additionally, the architecture will leverage cloud technologies for enhanced scalability and disaster recovery capabilities. By incorporating these elements, the proposed network will not only meet the current demands but will also be well-equipped to accommodate future growth and technological evolutions, thereby ensuring long-term sustainability and efficiency.

This report is structured as follows: firstly I will provide an overview of the system architecture by explaining the foundational components of the network; secondly I will give a detailed explanation of the design, IP addressing scheme, and security considerations; finally I will explain the *security architecture,* by presenting a comprehensive strategy for safeguarding DirectSales UK's infrastructure against potential and evolving threats. This report concludes with a summation of the key elements of the proposed solution.

Through the use of industry best practices and by leveraging cutting-edge security solutions, this proposal aims to position DirectSales UK at the forefront of technological efficiency, while prioritising security and network performance. Through careful analysis, this report will demonstrate a holistic approach to designing an infrastructure capable of dealing with both new and existing threats, in the rapidly evolving digital landscape.

System Architecture

The proposed solution creates a progressive infrastructure blueprint, underpinned by high-performing technologies without sacrificing scalability to propel DirectSale's expansion. It carefully integrates current operational needs and anticipates future growth, intermixing flexibility and resilience at its core. The architecture comprises of:

- **Staff PCs and Employee WiFi:**
  DirectSales UK's administrative team of 15 hosts and sales team of 35 hosts benefit from high-speed, secure connectivity, which enables smooth operations and boosts productivity. To achieve this, we will deploy a Single-mode fibre optic backbone for our gigabit Ethernet network, ensuring ultra-high-speed and reliable data transfer. Single-mode fibre is selected for its ability to transmit data over long distances without loss, making it ideal for our extensive office layout. This setup offers significant advantages over traditional copper cabling, including greater bandwidth and resistance to electromagnetic interference. For wireless access, Wi-Fi 6 technology will be used, providing higher speeds, increased capacity, and better performance in dense environments. To maintain security, VLANs will be integrated to segregate network traffic between the administrative and sales teams, thereby reducing the risk of data breaches and ensuring that sensitive information is compartmentalised. Additionally, Quality of Service (QoS) protocols will be implemented to prioritise critical business applications and communications, thus enhancing overall network efficiency and supporting seamless operations. *[4]*

  Guest WiFi Network: It will offer a robust, isolated internet access system for up to 55 visitors, ensuring a secure and user-friendly experience without compromising the internal network's integrity. [9]

  Web and E-commerce Servers: The company's online presence and sales platform are hosted on dedicated, high-performance servers (20 hosts) in a secure Demilitarised Zone (DMZ). A DMZ is used to protect the internal network from external access while allowing the web and e-commerce servers to communicate with the internet; this setup uses a buffer zone to protect the network *[3].*

  Network Infrastructure: The network backbone is built on Cisco Catalyst 9300 series layer 3 switches, providing high-speed, resilient connectivity. Cisco Catalyst 2960-X series layer 2 switches are deployed for access layer connectivity, offering a mix of 1 Gbps and 100 Mbps ports to support various devices and future growth. This could be beneficial in many ways, for instance, it ensures that the network can handle increased data traffic without performance degradation. The use of layer 3 switches at the backbone enhances the network’s ability to manage large volumes of traffic efficiently through advanced routing capabilities, thereby reducing latency and improving the overall user experience. Additionally, Layer 2 switches at the access layer facilitate the expansion of network connections to more devices and support varying speed requirements, which is critical for accommodating future technological advancements and increasing network demands[5]. Therefore, this infrastructure setup is both scalable and robust, supporting both current needs and future expansion.

  The network is segmented into VLANs to logically separate staff, guest, and server traffic, enhancing security and performance *[6]*. Access Control Lists (ACLs) are applied

on the layer 3 switches to regulate inter-VLAN communication, ensuring that only authorised traffic is permitted [7]

- **Wireless Infrastructure:** Seamless wireless connectivity is delivered through Cisco Aironet Access Points (APs), managed by a centralised Cisco Catalyst 9800 Wireless Controller. The employee WiFi network is secured with WPA2-Enterprise authentication. While the guest WiFi utilises WPA2-PSK with regular key rotation. This setup ensures a balance between strong security and ease of use in several ways. Firstly, WPA2-Enterprise offers robust security by requiring individual user credentials for access, providing a personalised security environment for each employee. This method is effective in protecting sensitive company data and network resources. Secondly, the guest WiFi network's use of WPA2-PSK, combined with regular key rotation, simplifies connectivity for visitors while still maintaining a secure access point. Regular key changes help mitigate risks associated with password leaks, thereby ensuring that temporary access does not compromise network security. This dual approach not only enhances security but also optimises usability for different user groups, effectively meeting diverse needs within the organisation [10]

- **Firewalls and Security:**
  A Cisco ASA firewall is deployed at the network perimeter to protect against external threats. It is configured with security zones, access rules, and VPN connectivity to enable secure remote access for employees [8] Intrusion Prevention System (IPS) and malware protection are enabled to detect and block potential attacks [11]

  In the DMZ, web and e-commerce servers are protected by dedicated firewalls and regularly patched to mitigate vulnerabilities. Secure Sockets Layer (SSL) certificates are installed on the servers to encrypt sensitive data transmitted over the internet [13]

  This system architecture provides a solid foundation for DirectSales UK's new regional branch, ensuring high performance, security, and scalability to accommodate future growth. The combination of Cisco's robust networking products and a carefully designed topology enables the company to operate efficiently and securely.

Wi-Fi 6, the latest standard in wireless technology (IEEE 802.11ax), is crucial for supporting environments with a high-density of devices due to its efficiency in handling multiple simultaneous connections. It ensures greater data transfer rates and network reliability, which is vital in a bustling office setting. Although the initial setup cost for Wi-Fi 6 is higher than previous standards, the improved capacity and performance significantly enhances productivity and the user experience, making it a valuable investment for future-proofing the network. Devices connect through various access points with assigned IP ranges that facilitate optimal distribution and management of network traffic. [14]

Virtual Local Area Networks (VLANs) provide essential network segmentation, enhancing the security and network management by isolating broadcast domains. This configuration limits network issues to single segments, which simplifies troubleshooting and enhances security by reducing the scope of broadcast storms and potential breaches. The implementation of VLANs is cost-effective, leveraging existing infrastructure to provide these benefits without substantial additional expenditure. Addressing for VLANs involves assigning subnets that suit the scale and scope of each segment, aiding in efficient traffic management and policy enforcement. [15]

The **DMZ (Demilitarized Zone)** serves as a crucial layer in the network's security architecture by creating a physical or logical subnetwork that contains and exposes external-facing services to the internet, such as web servers and email systems, while keeping the rest of the network secure. This separation is vital because it prevents outsiders from gaining direct access to critical internal resources and data. By placing public-facing services in the DMZ, traffic to and from these services can be controlled and monitored more stringently. This allows finer control over access permissions and more detailed scrutiny of inbound and outbound data, which effectively reduces the risk of attacks penetrating deeper into the enterprise network. Additionally, if a security breach occurs, the impact is confined to the isolated area of the DMZ, therefore protecting the internal networks from direct exposure. Hence, the DMZ not only enhances security by isolation but also helps in maintaining network integrity and continuity of operations in the face of external attacks.[16]

Layer 3 switches are integral in facilitating routing between different VLANs within the network, combining the capabilities of both routers and switches. This allows for sophisticated handling of traffic flows and enhances the overall network efficiency, which is especially beneficial in a multi-VLAN environment. Although they are more costly than Layer 2 switches, their ability to reduce the need for additional routers supports a streamlined network infrastructure that is both cost-effective and high performing. The network addresses for Layer 3 managed segments are designed to ensure optimal routing and efficient network topology.
Layer 2 switches are used at the access layer to connect end devices within the same network segment, handling data transfer and connectivity based on MAC addresses. They are less expensive and simpler to manage than Layer 3 switches, making them suitable for straightforward networking needs where routing between different subnets is not required. The cost benefits, coupled with the operational simplicity of Layer 2 switches, make them an appropriate choice for many sections of the network. Addressing in these segments focuses on physical connectivity and MAC-based switching. [17]

Cisco Aironet Access Points provide robust wireless connectivity, supporting high-density environments with advanced security features like WPA2-Enterprise authentication. These access points are chosen for their reliability and support for the latest Wi-Fi standards, ensuring high throughput and secure wireless access. Investing in Cisco’s technology is justified by their extended support and comprehensive feature set, which supports a diverse range of user needs while maintaining strong security protocols. Each access point is assigned a static IP within designated subnets to ensure consistent management and connectivity [18]

WPA2-Enterprise offers a robust security framework by requiring individual authentication, therefore providing personalised security environments for each user. This is vital in protecting sensitive company data and network resources. WPA2-PSK, used for less critical access like guest Wi-Fi, ensures simplicity in connectivity while maintaining security through regular key rotation, which helps mitigate risks associated with password leaks. While the setup and management of WPA2-Enterprise are more complex and costly, it offers superior security, making it a worthwhile investment for protecting business-critical networks.[19]

Firewalls serve as a critical barrier between a company's internal network and the external internet, regulating traffic based on predetermined security rules [8]. This not only prevents unauthorised access but also blocks malicious traffic and attacks. The implementation cost and management overhead of maintaining stateful inspection, application-layer filtering, and other advanced firewall features are justified by the significant enhancement in network security and data integrity firewalls offer. [12]

Security zones are designated areas within a network that have specific security requirements and controls, enhancing the defence against potential breaches by segmenting network resources based on sensitivity and exposure risk. Although creating and managing multiple security zones can increase complexity and administrative overhead, the ability to apply tailored security policies where needed most significantly enhances overall network security. [20]

VPNs (Virtual Private Networks) extend a private network across a public network, enabling users to send and receive data as if their devices were directly connected to the private network. This is crucial for maintaining the confidentiality and integrity of sensitive data transmitted over insecure networks like the internet. The costs associated with VPN technologies are counterbalanced by the critical need for secure remote access capabilities, particularly with increasing mobility and remote work trends.[21]

An **Intrusion Protection System (IPS)** monitors network traffic to detect and prevent attacks in real time. By actively analysing and responding to threats, an IPS enhances the security posture of a network. While IPS systems can be resource-intensive, both in terms of management and performance impact, their role in preventing data breaches and system intrusions justifies the investment, especially in environments susceptible to sophisticated attacks. [22]

Antivirus software is essential for detecting, quarantining, and removing malicious software and viruses from computers and networks. Regular updates and scans are necessary to cope with the constantly evolving landscape of malware. The performance impact and ongoing maintenance costs of antivirus software are outweighed by the benefits of protecting assets from malware-related disruptions and security breaches.[23]

ACLs (Access control lists) provide a list of permissions attached to an object, specifying which users or system processes are granted access to objects, as well as what operations are

allowed on given objects. They are pivotal in enforcing a minimum level of security for sensitive network segments. Implementing ACLs can be complex, requiring careful configuration to avoid inadvertently creating broad permissions or overly restrictive policies, but they are a crucial part of securing network traffic flow and resource access.[24]

QoS (Quality of Service) is a mechanism to manage packet loss, delay and jitter on a network by prioritising certain types of traffic, which is crucial for ensuring that critical business applications, such as VoIP and streaming media, perform well even in congested network environments[25] Implementing QoS involves complexity in configuration and monitoring, but the ability to guarantee the performance of essential services makes it an indispensable tool in a network administrator’s toolkit/[26]

In summary, this report has meticulously addressed the requisites delineated in the project brief for DirectSales UK's expansion into Plymouth. It has proposed a robust and scalable network architecture, designed to optimise operational efficacy whilst safeguarding against both current and emerging security threats. This conclusion underscores the comprehensive measures taken to meet these specified requirements, thereby ensuring the infrastructure's preparedness for future growth and technological integration.

Specifically, the implementation of a Single-mode fibre optic backbone and the use of Cisco Catalyst 9300 series switches are pivotal in providing high-speed, resilient connectivity that is essential for efficient operations. These solutions not only enhance the network's performance but also support substantial data traffic and future expansions, effectively addressing the need for scalability and robust performance. Furthermore, the integration of Wi-Fi 6 technology ensures optimal wireless communication, crucial for maintaining high productivity in a dense device environment.

Concerning security, the deployment of the Cisco ASA firewall, coupled with the sophisticated intrusion prevention system, forms a formidable barrier against external threats. This security architecture is fortified by the strategic use of VLANs and robust wireless security protocols (WPA2-Enterprise and WPA2-PSK), which segregate and protect data across different network segments. These measures meticulously fulfil the brief's demands for a secure, high-performance networking environment that anticipates future security challenges.

Therefore, the network and security solutions articulated herein not only meet but exceed the foundational needs of DirectSales UK's operational and security strategies. By implementing these advanced technologies and strategic frameworks, DirectSales UK is positioned to thrive in its expansion, benefiting from an infrastructure that supports immediate needs and scales effectively for future growth, all while remaining cost-effective. This strategic foresight thereby ensures the company’s long-term sustainability and technological relevance in an ever-evolving digital landscape.

Addressing table

Network: 84.8.4.0/24
No. nutworks = 5

if n = 3:

A.B.C.D/m network, borrow n bits

2^n subnets = 8 subnets

2^(32-m-n) addresses/subnet = 32 addresses per subnet

(2^(32-m-n) – 2) usable hosts = 30 hosts per subnet

Admin

Specification	Value
Number of bits in the subnet	0
New IP mask (decimal)	255.255.224.0
Number of usable subnets	8
No. of usable hosts per subnet	30
Network address	84.8.0.0/24
First IP Host address	84.8.0.1/24
Last IP Host address	84.8.0.254/24

Sales

Specification	Value
Number of bits in the subnet	3
New IP mask (decimal)	255.255.255.224
Number of usable subnets	2^3=8
No. of usable hosts per subnet	30
Network address	84.8.4.0/27
First IP Host address	84.8.4.1
Last IP Host address	84.8.4.30

Guest wifi

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	84.8.4.0/27
First IP Host address	84.8.4.33
Last IP Host address	84.8.4.62

Employee wifi

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	84.8.4.64/27
First IP Host address	84.8.4.65
Last IP Host address	84.8.4.94

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	84.8.4.96/27
First IP Host address	84.8.4.97
Last IP Host address	84.8.4.126

References

[3] Fortinet. (n.d.). What Is a DMZ Network and Why Would You Use It? [online] Available at: https://www.fortinet.com/uk/resources/cyberglossary/what-is-dmz.

[4] SearchUnifiedCommunications. (n.d.). *What is quality of service? Definition from SearchUnifiedCommunications*. [online] Available at: https://www.techtarget.com/searchunifiedcommunications/definition/QoS-Quality-of-Service#:~:text=Quality%20of%20service%20(QoS)%20refers.

[5] Cisco Meraki. (2020). *Comparing Layer 3 and Layer 2 Switches*. [online] Available at: https://documentation.meraki.com/MS/Layer_3_Switching/Comparing_Layer_3_and_Layer_2_Switches.

[6] SOLARWINDS (2024). *What Is VLAN (Virtual LAN)? - IT Glossary | SolarWinds*. [online] www.solarwinds.com. Available at: https://www.solarwinds.com/resources/it-glossary/vlan.

[7] Fortinet. (n.d.). *What Is a Network Access Control List (ACL)?* [online] Available at: https://www.fortinet.com/uk/resources/cyberglossary/network-access-control-list#:~:text=Network%20Access%20Control%20List%20Meaning.

[8] sec.cloudapps.cisco.com. (n.d.). *Cisco Firewall Best Practices*. [online] Available at: https://sec.cloudapps.cisco.com/security/center/resources/firewall_best_practices.

[9] Security, P. (2020). *Guest WiFi Explained + Simple Set-up for Visitor Connectivity*. [online] Panda Security Mediacenter. Available at: https://www.pandasecurity.com/en/mediacenter/guest-wifi/.
[10] Cisco. (n.d.). *Cisco Catalyst 9800 Series Configuration Best Practices*. [online] Available at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/c9800-best-practices.html [Accessed 4 May 2024].
[11] www.sophos.com. (n.d.). *IPS and IDS | Intrusion Protection and Detection Explained*. [online] Available at: https://www.sophos.com/en-us/cybersecurity-explained/ips-and-ids#:~:text=An%20intrusion%20prevention%20system%20(IPS)%20is%20an%20active%20security%20system.
[12] Fortinet. (n.d.). *What are the Benefits of a Firewall?* [online] Available at: https://www.fortinet.com/uk/resources/cyberglossary/benefits-of-firewall.
[13] Kaspersky (2021). *What Is an SSL Certificate – Definition and Explanation*. [online] Kaspersky. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate.
[14] Understanding Wi-Fi 6: What Is It and Do You Need to Upgrade? (n.d.). *Understanding Wi-Fi 6: What Is It and Do You Need to Upgrade?* [online] Available at: https://www.avast.com/c-what-is-wifi-6.
[15] documents.uow.edu.au. (n.d.). *Advantages of VLANs*. [online] Available at: https://documents.uow.edu.au/~blane/netapp/ontap/nag/networking/concept/c_oc_netw_vlan-advantages.html#:~:text=VLANs%20provide%20a%20number%20of.
[16] Fortinet. (n.d.). *What Is a DMZ Network and Why Would You Use It?* [online] Available at: https://www.fortinet.com/uk/resources/cyberglossary/what-is-dmz.
[17]communications @manageengine.com, M. (n.d.). *Switch Port & IP Address Management Software by ManageEngine OpUtils*. [online] ManageEngine OpUtils. Available at: https://www.manageengine.com/products/oputils/tech-topics/layer2-vs-layer3-switch.html.
[18]Cisco. (n.d.). *Wireless Access Points*. [online] Available at: https://www.cisco.com/site/uk/en/products/networking/wireless/access-points/index.html [Accessed 4 May 2024].
[19]SecureW2. (n.d.). *SecureW2 | Next-Gen Wired and Wireless Security*. [online] Available at: https://www.securew2.com/.
[20]www.juniper.net. (n.d.). *Security Zones | Junos OS | Juniper Networks*. [online] Available at: https://www.juniper.net/documentation/us/en/software/junos/security-policies/topics/topic-map/security-zone-configuration.html.
[21]NordVPN (2015). *What Is A VPN? Virtual Private Network Explained | NordVPN*. [online] nordvpn.com. Available at: https://nordvpn.com/what-is-a-vpn/.
[22]VMWare (2021). *What is Intrusion Prevention System? | VMware Glossary*. [online] VMware. Available at: https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html.
[23]Johansen, A.G. (2019). *Norton*. [online] Norton.com. Available at: https://us.norton.com/internetsecurity-malware-what-is-antivirus.html.
[24]Cisco. (2018). *Cisco Guide to Harden Cisco IOS Devices*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html.
[25]Fortinet. (n.d.). *What is Quality of Service (QoS) in Networking?* [online] Available at: https://www.fortinet.com/uk/resources/cyberglossary/qos-quality-of-service#:~:text=Quality%20of%20service%20(QoS)%20is.

[26]Cisco. (2018). *Cisco Guide to Harden Cisco IOS Devices*. [online] Available at: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html.