Ollscoil Teicneolaíochta an Atlantaigh

Atlantic Technological University

Assignment 1

Lecturer:	John O'Raw
Report Title:	Technical assessment of a student's computer: Enterprise and Data Center Networking
File Name:	L00169649.pdf
Submit to:	Blackboard in PDF format only
Date Submitted:	19th May 2023

Student Name:	Konrad Jeziorski
Student Number:	L00169649
Programme of Study:	PGDip in Cloud Computing
Module:	Networking

Contents

Summary

This document describes the WAN design for the customer. The goal is to convince the client that the project is professional, reliable, and cost-effective. The project includes designing and testing a WAN network solution for one of the client's branches, which is the network infrastructure of one of the electric petrol stations, two data centers, and the company's headquarters. The client requested a local network of the charging station in the Maynooth branch as part of the WAN. The contractor has already designed LAN for this company branch.

The project does not include the purchase of network equipment or the provision of Internet access services. Instead, the potential deployment of a remote site and the availability of network infrastructures in each area are proposed. A cost estimate for the network equipment solution and services related to their installation will also be presented.

The customer is responsible for ensuring access to the necessary resources and the appropriate access rights and providing the required data regarding the existing network infrastructure.

The assumptions made cover the customer's network needs. Requirements include throughput, reliability, security, and WAN scalability.

In addition, the WAN design must adhere to security standards, particularly PCI DSS (Payment Card Industry Data Security Standard) requirements, as Visa card payments will be processed on the network. Appropriate safeguards such as data encryption, access control, and network traffic monitoring will be required. This applies to all network infrastructure elements, including servers, routers, cables, firewalls, etc. It is also recommended to take care of regular security audits to ensure compliance with PCI DSS requirements and minimize the risk of data security breaches. Adhering to security standards is crucial to ensure that payment processing complies with legal requirements and to protect customer privacy.

Another important criterion is to minimize the risks associated with the network infrastructure and integration with the existing network by conducting performance and integration tests. In addition, there are some risks associated with the implementing a WAN. One of them is the possibility of hardware failure, which can lead to downtime and data loss. Another risk is the potential for cyber-attacks, which can result in data breaches, malware infections, and other security-related issues. It is also important to consider the impact of natural disasters or other unforeseen events that may affect the WAN's infrastructure. To mitigate these risks, it is essential to implement best practices and standards for network security, backup and recovery, and disaster recovery. Regular testing and maintenance of the WAN can also help prevent downtime and ensure that it is operating efficiently. Additionally, it is important to establish clear communication channels and processes for incident management and troubleshooting and to provide ongoing training and support for network administrators and end-users. The final risk acceptance of the project will take place after these tests have been carried out and the client has approved the results.

It is planned to complete the project within three months from the start date. It is assumed that the client will be available for meetings and WAN testing at every project stage.

The project will use industry standards and certifications such as CISCO, CCNA, and Fortinet to ensure the highest quality of design. In the interests of security, the project considers the requirements related to data protection under the regulations of the GDPR.

The project aims to develop a WAN connectivity solution for three site types - Data Centers in Cork and Malin, Skierries Head Office, and the Maynooth remote site. The solution will include a physical

diagram, bill of materials (BOM), and technical summary. Additionally, it will provide listings from the GNS3 emulator that feature firewalls and routers.

WAN design and Costings

As the first step in WAN connectivity solutions, it was necessary to determine the exact location for the EV charging station in Maynooth. The client considered placing such a station near major junctions or motorways in Maynooth to ensure easy access and convenient charging for users. Locations near shopping malls or public places such as parking lots were also thought of to allow charging while shopping or staying in these places. However, for WAN designers, access to existing network infrastructures is essential. The limitations of such an eventuality come down to increasing the cost of connecting to the WAN. In such cases, the solutions usually boil down to using more network equipment or less effective technologies, which results in network bandwidth. A too-large area of the station was a limitation for location decisions. Finally, it was decided that the complex of facilities for this station would be built in the southwestern part of Maynooth, on its outskirts. This area is between the M4 road to the south and the N4 motorway to the north. The site is close to network hubs providing access to various operators such as Eir, Vodafone, Three Ireland, Virgin Media, and others. Renewable energy sources such as wind farms and solar farms are also nearby. Although the station has its energy generators, the possibility of using additional resources in the event of a failure of one of them should be considered.

Each site will have two IPSs to ensure redundancy and reduce the risk of disconnections between these areas. The client requested a minimum of 100 Mb/s data transfer rate, which was an ambitious benchmark for searches. ISPs may have different ways of connecting to local networks, but one common method is to use FortiGate's firewall and connect directly to it. This solution has been implemented for each of the sites.

The solution for the Maynooth site was to connect to the existing fiber broadband network infrastructure on the M4 motorway and another within the city. Potential ISPs would be Magnet and Eir. Additional fiber optic cables to fiber broadband access points would need to be routed. An IPsec VPN would be configured on both WAN interfaces that are connected to the ISPs to connect the remote site to both Data Centers. OSPF has been chosen as the routing protocol for the outside network, while the reliability of the network inside is ensured by HSRP (designed in the LAN project).

The proposed solution for providing internet connectivity to the Data Center in Cork, which is located at the Airport Business Park, would be similar to that of the Maynooth site, which is a connection to fiber optics. However, due to the close proximity of the airport, there may be restrictions on the use of radio antennas for providing internet connectivity. This is because the use of radio antennas in the vicinity of airports can cause interference with air traffic control systems, leading to potential safety hazards. Therefore, the use of fiber optics would be the recommended option to ensure reliable and safe internet connectivity for the Data Center in Cork. Cork Airport Business Park has a ready-made fiber broadband network infrastructure. The park is served by a network of underground wires that allow quick and easy connection to any of the buildings from the many telecommunications providers. Additionally, the Park is connected to Cork's Metropolitan Fiber Network, giving users and businesses access to the fastest broadband speeds. Potential ISPs include eir and Pure Telecom. OSPF was chosen as the routing protocol.

The WAN solution for Malin data cenre located in Co Donegal, a greenfield site on the R242, 1km south from Malin village, was a bit more complicated. The location of the connection to FTTP (Fiber to the Premises) has been established, 1 km from Malin, along the road R242. It will be necessary to perform a partial technical infrastructure and obtain appropriate consents to use the existing poles to lead the optical fiber to its destination. The second solution had to be chosen and for reliable redundancy, it was decided to use a robust radio antenna. The choice fell on the AF-24 network antenna. The AF-24

antenna is a radio antenna that uses airFiber technology, which provides a very high data transmission speed. According to the manufacturer (Ubiquiti Networks), the AF-24 can reach speeds of up to 1.4 Gbps with a range of up to 13 km. ISPs are available in Carndonagh, a few miles from the Data Centre. At least six providers offer fiber broadband there, including Digiweb, eir, Pure Telecom, Sky Ireland, Virgin Media, and Vodafone, which suggests that there are indeed wireless internet service providers (WISPs) in the area. The routing protocol that will be used in this IP network is OSPF.

Two notable ISPs that provide broadband services in Skerries are SIRO and National Broadband Ireland (NBI). SIRO offers high-speed broadband services for businesses in Skerries to help them process payments, avoid downtime, collaborate, and grow their business. NBI, on the other hand, is currently constructing fiber broadband to thousands of premises in Skerries Intervention Area. For the Head Office, these two ISPs were selected to connect to the WAN using fiber broadband. The OSPF routing protocol will be used here as in the above-mentioned local networks.

In most cases, different Internet Service Providers (ISPs) use their own optical fibers. Although, in some cases, ISPs may run on the same physical fiber cables, depending on the agreements made with infrastructure owners. Although many Internet service companies have their own fiber network, there are also large companies that build and maintain fiber infrastructure rented by various ISPs. In any case, even if different ISPs use the same fibers, they usually have separate network nodes and end devices, which means that Internet traffic is separated and assigned to specific users and subscribers. However, to ensure network reliability and reduce the chances of network services failing, it is advisable to review the contract terms for businesses in the same area and ensure each provider uses different physical network infrastructures. This approach can help reduce the risk of both network services failing simultaneously.

Some activities are beyond the scope of the WAN designer, but their conditions must be met. The client will need to purchase approximately 5 km of fiber optic cables and poles to build an extension of their network infrastructure. Additionally, the client must obtain the appropriate certificates and permits to complete the project. These permits may include a building permit, which grants permission to construct the necessary infrastructure, and other certificates and licenses as required by local regulations. It is essential for the client to ensure that they obtain all the necessary permits and certificates before commencing the project to avoid any legal or financial consequences. Once the appropriate documentation has been obtained, the client can proceed with the purchase of the fiber optic cables and poles and begin construction of the network infrastructure.

Figure 1 Potential location for an electric service station in Maynooth

Below is a diagram of the proposed WAN solution, along with port designations, routing, VPN tunnels, etc.

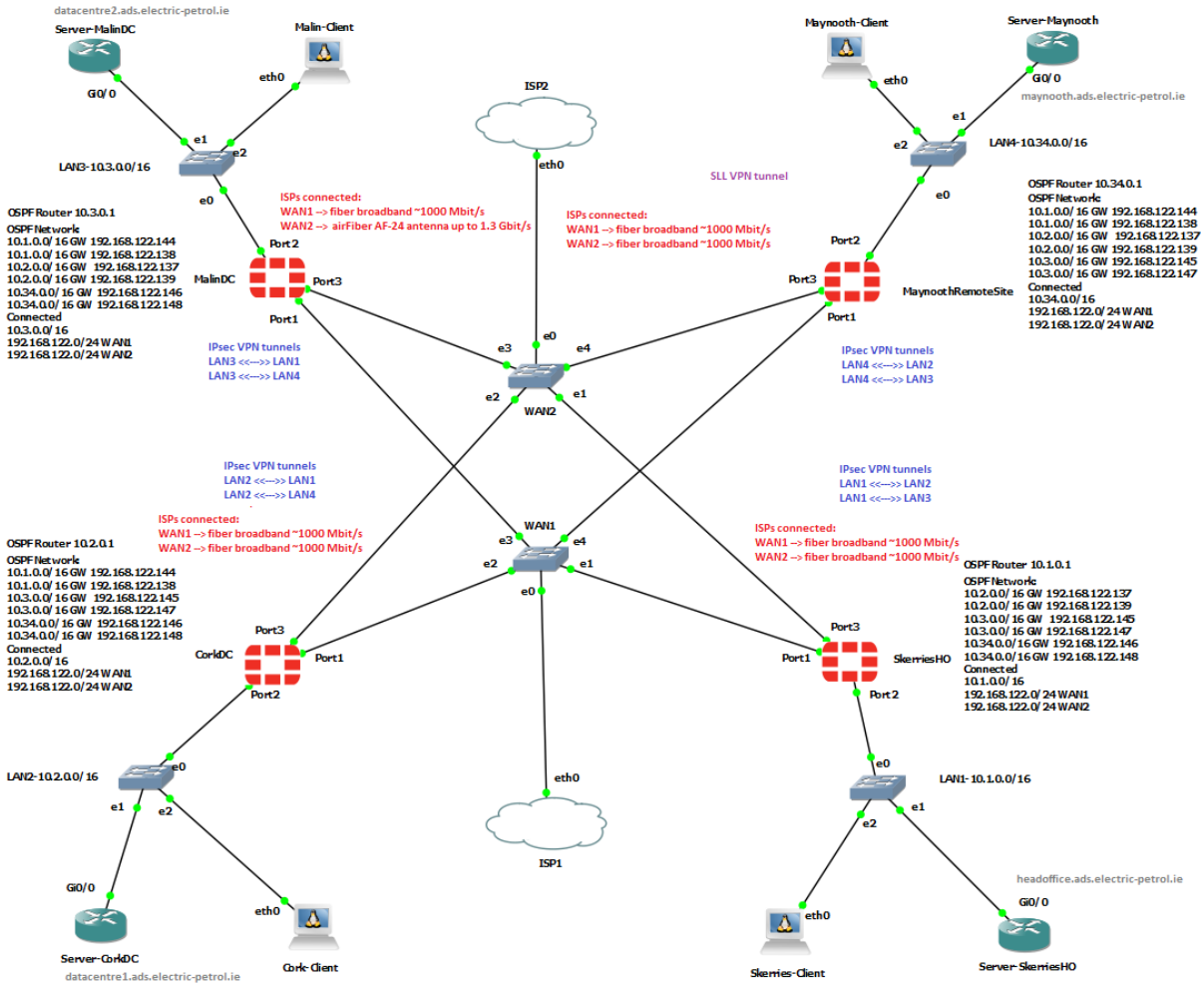

Figure 2 - WAN summary diagram

Technical Summary

The client has servers in their data centers that need to be accessible on the internet to enable remote client applications to function. Each branch's FortiGate network security devices can be configured to allow external server access. FortiGate is a network security device that can be used to provide secure remote access to HTTP, HTTPS, and anonymous FTP servers in corporate data centers. To enable access to HTTP, HTTPS, and FTP servers from the internet, an IPsec VPN was configured between FortiGate firewalls in the data centers and branches. This configuration allowed for secure data flow between the branches. IPSec VPN rules were created on the FortiGates in each branch, and servers were configured to allow external access, meaning they were visible from the internet, and remote clients could use the applications. At the same time, the IPsec protocol provided secure encryption and authentication of data sent between remote devices. NAT was an important component of this setup because it enables devices in a local network that use private IP addresses to send data over a public WAN IP address and access internet resources. NAT can also be used to protect the network from outside attacks by hiding the private IP addresses of devices in the local network.

OSPF (Open Shortest Path First) is an internal gateway protocol that controls the flow of packets inside an autonomous system (AS). Its features are multipath routing, least-cost routing, and load balancing. Furthermore, if are create several areas (multi-area OSPF), each must be connected to area 0, allowing for easier network administration and scaling. In the context of redundancy and information processing in two data centers in Cork and Malin, using two ISPs, OSPF can help ensure network connection redundancy. Each area of the OSPF network was connected to two different ISPs through WAN1 and WAN2 ports in FortiGate. In the event of a failure of one Internet provider, network traffic will be automatically directed to the other provider, ensuring the continuity of the network connection. This way, the OSPF protocol provides a reliable network connection and minimizes the risk of failures that can lead to data loss or system damage. Firewalls and routers will be responsible for forwarding network traffic. When a payment visa card is used to pay at Maynooth station, devices on each network will need to transmit the information to the appropriate data centre. Card payment processing applications must be located in both data centers to enable load balancing and minimize the risk of failure. Dividing the network into areas allows you to separate payment traffic and process it in one place, optimizing the flow of information. OSPF also allows the implementation of policy-based routing, which can route traffic based on specific criteria where different types of traffic require different service levels. OSPF has been configured on every WAN port and internal port in Firewalls. Server ports on LANs are also set to this type of routing. It is suggested to install at least two routers in each LAN and connect them to Fortigate devices in all areas to provide more redundancy ((included in BOM). The remote side has a configured HSRP protocol in which the VLAN responsible for card payments is prioritized.

If the client will host their email from Microsoft Office 365, it is crucial to create a firewall rule that allows secure access to Office 365. This rule should allow traffic for HTTPS (port 443) and from the email category, like SMTPS (port 465)), to Office 365 servers. In addition, rules are proposed that limit access to Office 365 user accounts to only necessary IP addresses to ensure connection to the Office 365 service or set rules that block network traffic from suspicious or untrusted sources to minimize the risk of network attacks and user accounts. This firewall policy was implemented on the Maynooth site. Security features such as multi-factor authentication for Office 365 user accounts can also be applied to increase security and prevent unauthorized access to user accounts. Office 365 tools like Data Loss Prevention protect private information from accidental or malicious loss and can add extra protection.

Several potential solutions could be implemented to ensure external contractors can access equipment on-site without breaching PCI DSS. One approach would be establishing a secure remote access protocol for the contractors. This would involve providing the contractors with remote access software to securely connect to the equipment on-site from their own devices. It would also ensure that access is limited to authorized individuals and that all access is monitored and logged for compliance. Another solution might involve setting up a virtual private network (VPN) to connect the contractors' devices with the on-site equipment. This would allow the contractors to access the equipment as if they were on the same network without being on-site physically. However, ensuring that the VPN is adequately secured, and access is limited to authorized individuals would be essential. As a network security appliance, FortiGate could potentially play a role in securing remote access for external contractors by providing a firewall and other security features to protect against unauthorized access and potential security breaches. Efforts have gone into the project to ensure the client's network infrastructure is carefully configured and secured to ensure PCI DSS compliance. It is important to note that engaging with external contractors requires careful consideration and management to ensure compliance with relevant policies and regulations and minimize potential risks and liabilities. The external supplier must be employed under a written contract using standard terms and conditions, and legal counsel should review and approve any deviation from these terms. Contractors also have significant duties and responsibilities relating to safety and other issues. They must cooperate with the principal contractor or project supervisor for the construction stage (PSCS) to ensure compliance with relevant regulations and standards.

SSL VPN refers to a virtual private network that provides secure remote network access via SSL (Secure Sockets Layer), which is now being replaced by the newer Transport Layer Security (TLS) protocol. With an SSL VPN, users can securely access a private network over the public internet by encrypting all client-server traffic with SSL or TLS encryption. SSL VPNs are commonly used by businesses to enable remote access to internal systems, applications, and data and to enable secure communication between geographically dispersed offices and employees on the move. Based on customer information, traveling senior staff members need access to business applications. To achieve this, SSL VPN technology will provide secure remote access to the branch office network protected by FortiGate appliances. With SSL VPN, employees can securely access their resources from any device with an internet connection.

Software-defined WAN (SD-WAN) is a virtualized WAN architecture that centralizes the management of smaller and otherwise disconnected WAN networks, providing more flexibility and lower costs while maintaining application performance and security. SD-WAN is particularly useful in scenarios where a more traditional WAN approach might not be the best solution, such as in the case of remote login access by a customer's own technical staff. SD-WAN can provide the necessary flexibility and bandwidth efficiency for remote access while maintaining security and data privacy. Therefore, SD-WAN could be a good solution for the customer requirement, where the customer's technical staff needs to log in remotely with no limitations on their access.