Final Network Design Report

Caleb Brown

Spokane Falls Community College

IS 244: Network Security

Dr. David Vosen

16th June 2023

Overview

In this report, I will outline the basic requirements for the layout and design of the network, including security features, for the Spokane Public Library Central location. The purpose of this report is to not only explain, in detail, the nuances and functionality of the network but also visually show how and why this design will be the best option going forward.

**Problem Summary**

The public library is a community wide resource, used by all and meant for the purposes of research, enjoyment, and further learning. In today’s world, technology is at the forefront of this experience and because of this, ensuring your patrons can safely and freely use these tools is of upmost importance. From providing your patrons with access to the internet, to ensuring the staff and its ability to properly run this library are executed neatly, network security and proper configuration are integral to the entire experience. Gone are the days of ignorant, albeit blissfully, dialing up on your machine to surf the web and its many treasures. In today’s world, threats in the virtual realm can come from anywhere, from people simply walking into our library and uploading malicious software, to threats perpetrated on the web itself, the risk is very real and carries serious implications.

**Proposed Solution**

In my proposition, I outline every necessary tool and piece of equipment needed to ensure, to the upmost certainty, a safe and secure environment for your patrons of all ages to enjoy. This begins by outlining the basic requirements needed to support what the library needs in terms of computer areas, for both a children’s/early learning section to an area open to the public. On top of this, by building the staff network as the focal point for the whole library, I further ensure smooth operation and ease of control. Once the infrastructure is laid out, it is then time to secure and protect these new resources via several ways and build in a manner that gives the library layers of defense. In essence, by making sure this network is designed in a way that prevents the public from accessing or uploading inappropriate or malicious threats, and by making sure that children utilizing computers aren’t exposed to anything deemed dangerous, we create an environment that stands to make our community proud of what they publicly fund.

**Value Proposition**

The outcome of my proposed design is one that ensures the satisfaction of both the public who funds this service, as well as those that wish to utilize this amazing resource. It simply comes down to making sure our library serves its purpose in a way that is timely and safe. We do this as I described, from the ground up and in a way that puts security at the forefront so that anyone who accesses the library computer can do whatever it is they seek in a safe manner, children included. By building a foundation for a smooth and timely network, we also strive to give these patrons an experience that isn’t riddled by latency or waiting.

**Conclusion and Next Steps**

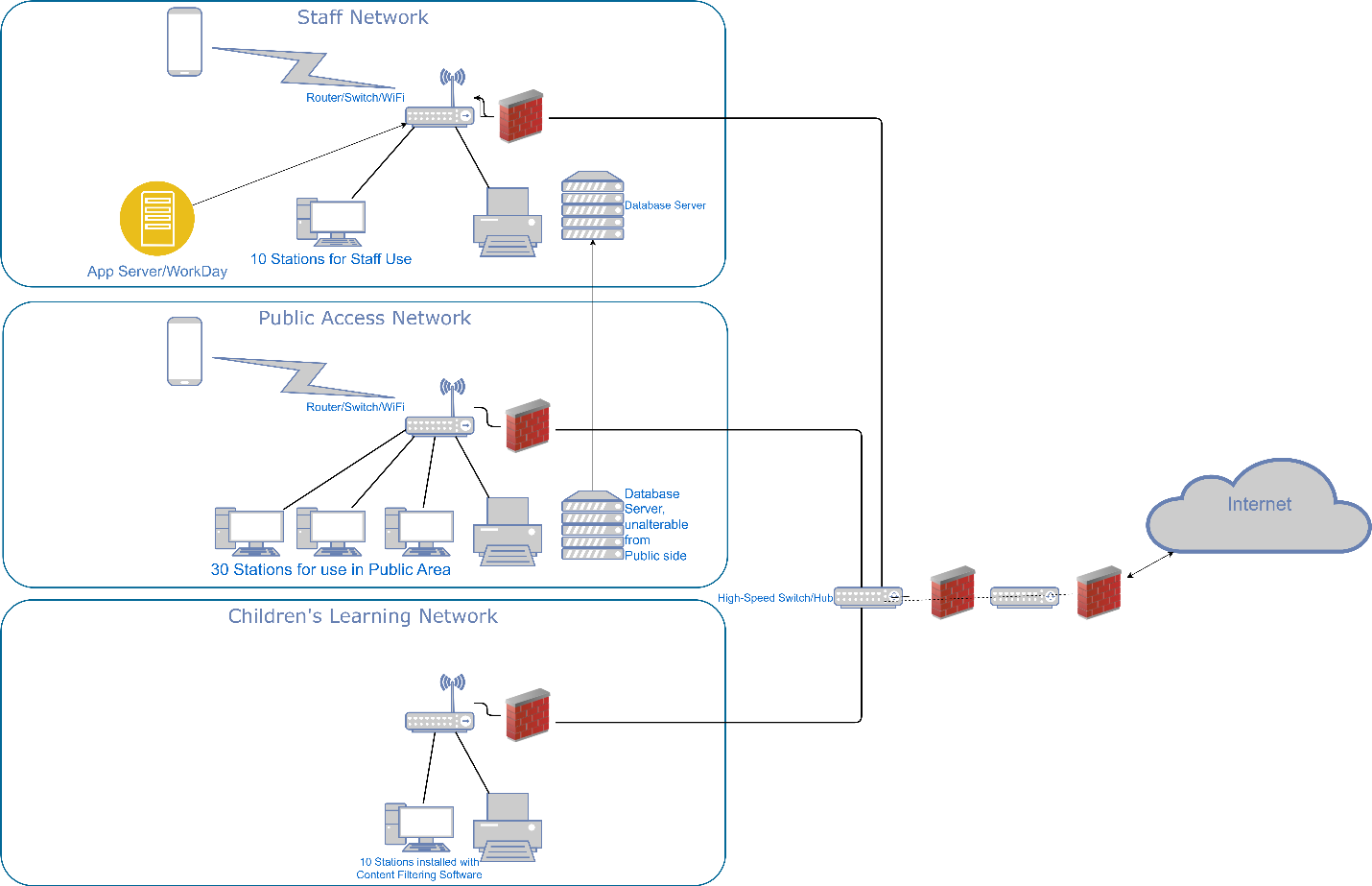
Following this report, I will outline in further detail exactly how we can achieve this goal and make the library a valued tool and destination for our local patrons. From then on, it is important to think about each stage as integral as the other, for a network that doesn’t work properly can’t be secured properly. I hope, at the very least, you can see the importance of safely securing and designing a network so that entities such as our library can perform and be that valuable resource to its public the way it is meant to be.

**Core Network Layout**

My design for the library focuses around three segmented networks, the staff, public and children’s networks. Planning of time is at the core of designing not only a working infrastructure, but one that is also secure. In his article, Steve Petryschuk describes a popular network lifecycle model designed by Cisco called PPDIOO or Prepare, Plan, Design, Implement, Operate, and Optimize. The reason this model is so popular is because each step builds further on the one before and as such, creates and tests whether a network design will run optimally. (Petryschuk, 2021) For the purposes of this library, establishing a hierarchical network and segmenting the networks as described by Hari Subedi in his work will also help in creating a suitable and secure network. (Subedi, 2021) (Breeding, 1998)

My design will incorporate primarily a mesh of network topology designs, from wireless access points to high-speed switches connecting the public access area and separate staff network. The most important aspect to me would be segmenting the different networks so that there is a clear line between them as well as different policies for each. To be more specific, I would want the public access area based on a star topology and the staff network based around a mesh topology. The children section will also be mesh, but with some wireless mesh incorporated as well. It will consist of 2 web servers, one for public use and one for staff, 1 application server for staff, 2 database servers both for staff, 3 print servers for each network (public, children, staff), 1 database server, and lastly 50 workstations overall (30 for public, 10 for children, 10 for staff). Everything will run on Windows when applicable, and webs servers can be based on Linux.

Alternatives in the case of failure or downtime wouldn’t be as dire given the service a library provides. I could see a cause for backing up the local research database server but in terms of back-up power or alternative ISP subscriptions I don’t think there would be a need necessarily.



**Firewall Selection and Placement**

Foundationally speaking, there are two “types” of firewalls, software and hardware. Beyond this characteristic, firewalls come in many default configurations and designs, some excel in simple packet filtering while others can protect an entire network. This paper will briefly explore these differences in effectiveness, scalability, and cost while also highlighting some of the more specific types found in different firewall functionalities.

# Software-based Firewalls

Software firewalls are just that, software installed locally onto a client and implemented to block or filter inbound traffic based on user configuration. There are several paid and open-source versions you can find on the web, and even some anti-virus software will feature an element of packet filtering. This ease of access and installation provides a user with an “endpoint” aspect for security and can help build further layers of security in a network design. While most software firewalls are designed with ease of access and configuration in mind, they do so at a small cost such as consuming a portion of the processing power of the hosting client as well as the day-to-day maintenance to keep them up to date. Overall, software firewalls provide a helpful and useful tool for defending against unwanted traffic, especially at a workstation level, albeit at the cost of needing to properly understand the proper configurations. (Velimirovic,2022)

**Hardware-based Firewalls**

Hardware firewalls, or sometimes referred to as appliance firewalls, are best described as stand-alone physical firewalls that are designed to protect entire networks. As mentioned, they are the first line of defense for an entire network and can protect multiple devices while providing an outer layer of defense for a said network. Unlike software firewalls, or host-based applications, because they are a separate entity means they don’t draw on the processing power of your workstations and be configured by one system admin to be useful. They can sometime be built together with a router in some models, but also come in solitary models meant for just that one purpose. Of course, this higher level of protection does so at a bigger cost and requires a higher level of knowledge to configure properly. The benefits of on-site physical firewalls are numerous but don’t eliminate the need for software firewalls installed on workstations since there can still be a conceivable threat or vulnerability for said stations as well as an increased insider threat vulnerability. (Stephens, 2022)

**Other types of Firewalls**

While firewalls can be considered software or hardware based, there are also several more specific types, or techniques, that perform certain tasks at varying levels. The first of which, and considered the most basic, is a packet-filtering firewall. This type of firewall simply looks at the header of a packet, or datagram, and inspects the addresses for both the inbound and outbound destinations and based on its configuration, will filter or block accordingly. Next are circuit-level gateways, unlike packet-filtering, this technique doesn’t look at the incoming packets but instead focuses more on requested transactions. This of course streamlines your inbound traffic, but because it isn’t analyzing the packets means malicious or hidden data can make its way into your network or station. Stateful inspection firewalls are next, and best thought of as a combination of the previous two firewalls. This firewall looks both at the inbound packets as well as the TCP handshakes, then, based on a database it keeps, will recognize safe traffic it recognizes and block unknown sources. Lastly, we have proxy firewalls. This firewall operates like the previous firewalls but what makes this firewall unique is its location. Proxy firewalls operate between internal and external systems, in some ways as a DMZ, so as it processes inbound traffic it will mask the client’s address to make it unknown to malicious threats. Out of all these firewalls, each one serves a specific purpose in the overall network design with security and more importantly, layers of defense at the core. (Schultz, 2014)

**My plans for Firewalls in this Network**

In my network design for the library, which I am currently interning at, I believe I will employ both hardware and software firewalls. I envision my library as three separate sub-networks, the staff, public-access, and children’s networks. I may alter this design, based on feedback, but as it stands, I believe employing a hardware firewall that separates the staff network from both the public and children’s network will work best. Past that, I would employ software firewalls in all workstations, configured around keeping inbound traffic for the public network and children’s network safe but also making sure that it isn’t bleeding into my staff’s network. I also believe that a single DMZ could be employed for both the public and children’s networks that keeps them safe from malicious threats coming from the WAN. Overall, safety and proper filtering come to mind in keeping my networks safe from certain content as well as the many users that come in to use public-access stations while also making sure the staff network can operate safely in the event of one or both of the public networks is under threat.

**VPN Technology and its place in the Network.**

VPN technologies have grown and advanced immensely over the last decade. In today’s professional environments, the need for secure VPNs has grown exponentially as the number of workers shift to working remotely and the need for secure access has become ever more important. This documentation will solve CorporationTech’s scenario by explaining the differences and advantages to the multiple types of VPN technology available and based on that information, I will provide what I think is the best option going forward.

**Understanding IPsec**

IPsec, or Internet Protocol Security, is a suite of protocols and algorithms used to securely connect across networks. The goal of IPsec is to ensure the integrity, confidentiality, and authentication of data via encapsulation and establishing a Security Association, or SA, by the way of a key exchange, or Internet Key Exchange version 2 (IKEv2). Initially, when wanting to configure a secure connection between two networks on a VPN, whether through a router or firewall, a SA must be established. Sometimes referred to as “tunneling”, this will set up the means for encryption and decryption via IKEv2. Once that has been configured, the next step for secure and encrypted communication involves encapsulating and encrypting data packets. Authentication Header, or AH, and Encapsulating Security Payload, or ESP, are the two protocols responsible for preparing data to be sent and received. These work in conjunction by taking the original data, encrypting it with either a symmetric or asymmetric key, then encapsulating it with the VPN header and trailer along with an IP header. Once it has been sent, the receiving side will then work in reverse using the same process to decrypt and read the data. IPsec is most seen when transferring very sensitive data such as financial or medical records and even internal communication within a corporation. IPsec can be implemented at any IP-based application, and while sometimes difficult to properly configure, comes with a very high level of security. (Loshin, 2023)

**SSL/TLS VPN Connections**

Apart from IPsec, is SSL/TLS, or Secure Sockets Layer and Transport Layer Security. SSL was eventually updated into TLS, but both are commonly mentioned together or interchangeably. This kind of secure connection is primarily seen on a browser or between a host/client and a server. Unlike IPsec, which operates at the network layer, SSL is supported at the browser level and doesn’t require the type of strenuous installation or configuration seen with the latter. This form of security works around the language used in internet traffic, or Hyper Text Markup Language (HTML), and the protocol used for sending and receiving said traffic via HTTP, or Hyper Text Transfer Protocol, to create a secure “tunnel’ like what IPsec provides. By building this SSL VPN tunnel, whether to a corporate network or to the many different VPN providers, it makes the traffic sent and received encrypted much like the way IPsec does. This all starts by establishing the typical TCP handshake seen when wanting to send and receive data between a host and a server, except once that is completed, the server will then send a digital certificate which includes its public key and what CA, or certificate authority, has signed to verify said certificate. This will lead to a similar key exchange seen in IPsec, either symmetric or asymmetric, which guarantees data sent between both sides can only be decrypted and encrypted via both sides’ public and private keys. Overall, SSL/TLS VPNs are primarily seen in a remote-access type of connection for people that maybe work from home or are accessing a corporates network from a separate unrecognized network that wouldn’t be included like what is seen in an IPsec site-to-site setup. This VPN technology provides a less expensive option for individuals all while still insuring secure and encrypted communication, but also includes several vulnerabilities not typically seen in an IPsec configuration. (Fruhlinger, 2022)

# Site-to-Site VPN

Site-to-Site VPNs are a common type of VPN setup that utilize IPsec protocols. As the name would suggest, this type of VPN connects two separated sites virtually and securely using a “tunnel”, or encrypted connection via key exchange. This connection requires both ends to be configured accordingly, via router, firewall, or a standalone VPN client, and unlike other remote VPNs, it is continuously connected. This type of VPN has many benefits, more so for companies with multiple sites that have a need to securely access resources located locally from one another. It is best to think of this VPN as expanding a Local Area Network and with that comes some of the benefits and security from keeping your network internal. Apart from the encrypted traffic, this simplified layout means there is no need for converting internal IP address to external when communicating across networks and it also makes managing access control easier due to known “internal” entities. With that, there are a few slight downsides, including limited scalability and possible network complexity that leads to latency as more sites are added. Overall, site-to-site VPNs provide a vastly secure connection, with the help of IPsec, and can give companies the means to communicate between sites without having to worry about interceptions of data or man-in-the-middle type attacks. (Vasic, 2023)

**Remote-Access VPN**

Unlike site-to-site VPNs, remote-access VPNs are probably the most seen form when using a VPN. When the need for a user to access a company’s network from outside its LAN arises, the most likely tool will be a VPN. In a lot of ways, it isn’t much different from how a site-to-site connections works, the main differences come in the layer at which the “tunnel” is established, and the protocols used for encryption. By using a VPN client software, a user can then establish a secure SSL/TLS connection to said company server via validated user credentials. This comes a at much lower cost for company and user, much like how we explained earlier, and yet it still provides a secure encrypted connection. Remote-access VPN technology is seen in both the public and private sector and while comparable to site-to-site in lot of ways, it doesn’t quite mean it is completely free from the vulnerabilities seen in a typical SSL/TLS connection. (Spadafora, 2020)

Bibliography

Breeding, M. (1998, January 1). *Designing and building the Best Small Office Network from the ground up*. Library Technology Guides. https://librarytechnology.org/document/1236

Contributor, T., & Loshin, P. (2021, April 21). *What is IPsec (internet protocol security)?*. Security. https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security

Schultz, E. E. (2014). 83-10-41 *Types of Firewalls.* Internet:

*http://www. ittoday. info/AIMS/DSM/83-10-41. pdf,[Nov. 5, 2014]*.

Fruhlinger, J. (2022, March 28). *What is SSL? how SSL certificates enable encrypted communication*. CSO Online. https://www.csoonline.com/article/3246212/what-is-ssl-how-ssl-certificates-enable-encrypted-communication.html

LiquidWeb. (n.d.). *What is a hardware firewall? how it keeps you secure*. Liquid Web. https://www.liquidweb.com/blog/hardware-firewall/

Networks, A., & Petryschuk, S. (2023, February 2). *Network design and best practices*. Auvik Networks Inc. https://www.auvik.com/franklyit/blog/network-design-best-practices/

Spadafora, A. (2020, March 9). *Remote Access VPN: What are they, how do they work and which are the best*. TechRadar. https://www.techradar.com/vpn/remote-access-vpn

Subedi, H. (2023, March 16). *Designing a computer network for your business: A step-by-step guide: Jones it*. Jones IT | Managed IT Services, IT Support, IT Consulting. https://www.itjones.com/blogs/2022/1/15/designing-a-computer-network-for-your-business-a-step-by-step-guide#create-network-design

Vasic, D. (2023, May 6). *What is a site-to-site VPN and do you need one?*. DataProt. https://dataprot.net/articles/what-is-a-site-to-site-vpn/

Velimirovic, A. (2022, December 2). *The 8 types of firewalls explained*. phoenixNAP Blog. https://phoenixnap.com/blog/types-of-firewalls