Nittany Network Solutions

Sheetz Network in Centre County Area

DJ Wheeler, Nick Hadden, Dominic Eicholtz, Jake Allen, Danny Mitchell, Aiman Sohail

Group 12

IST 220, Section 003: Networking and Telecommunications

Dr. Nick Giacobe

April 26th, 2024

Table of Contents

Overview/Executive Summary

Our group, Nittany Network Solutions, has been tasked with designing an enterprise network that will connect nineteen Sheetz locations together. We will implement local area networks at each Sheetz location and tie them all together under one wide area network. A central location in the WAN will be designated as an IT headquarters to provide important services to the company network. This includes infrastructure services like DNS and DHCP, communication services like email, and a domain controller for Active Directory for authorization and authentication. This location will also host application services like the database server, which will be important for tracking customer, employee and supplier information, as well as transactions, inventory, and other important business information. These application services will also include a web server for hosting the company website and a file server to store and manage access to important documentation.

We will contract an Internet Service Provider to connect this central location to other branch locations. We believe that this is a cost-effective way to provide high-speed reliable connectivity throughout the different company branches. We will use a business VPN to secure traffic traveling across the Internet between branch locations and the main headquarters.

To protect the sensitive information on the network, such as that found on the database and file servers, we will need to implement various forms of cybersecurity. The headquarters containing all the company servers will need to have a firewall installed to provide perimeter security to the company network. This firewall will block all incoming traffic to end devices on the company network unless the traffic is a response to an outgoing message.

Description of Needs/Requirements

List of Computer Systems –

Type of Location	Uses of Systems	Users	Software Requirements
Main Site	- 24 Desktop Computers - 10 Routers - 40 IoT devices - 5 Switches - 2 Access Points - 8 Printers	Marketing Department - 8 Employees IT Department - 4 Employees HR Department - 8 Employees Maintenance Department - 4 Employees	- Software for main site employee information - Servers and databases for each area of information mentioned below - Security software for the physical building (cams, etc.) and the network - Communication software including audio and video for conference calls or just general transmission between sites
Typical Local	- 2 Desktop Computers - 2 Checkout Tablets - 2 Card readers - 8 Gas Pump card readers - 10 IoT devices - 1 Printer - 2 Routers - 1 Switch - 2 Access Points	- 2 Cashiers - 1 IT technician - 1 Maintenance Worker - Source outside help for network construction, updates	- Transaction software for basic customer interactions (cash and credit card payments at the register) and history of the transactions - Stock management software, for gas as well - Security software for physical building - Scheduling software for employees
Total	1 Main + 18 Local - 60 Desktop Computers - 36 Checkout Tablets - 36 Card Readers	Marketing Department - 8 Employees IT Department - 22 Employees HR Department - 8 Employees Maintenance Department	- 2 Security software, vary in complexity based on site - Both contain software with information regarding employees and stock

	- 144 Gas Pumps and readers - 220 IoT devices - 26 printers - 46 Routers - 23 Switches - 41 Access Points	- 22 Employees Cashiers/Food - 36 Employees	- Main site software for various servers

The typical local site contains card readers at the registers and at the pumps. These are a necessary aspect of the company due to the rising popularity of using credit or debit cards instead of cash. Card-reading software would be necessary to make the necessary transactions with customers. Each location would also need a couple of desktop computers for the employees to see the stock information in the database mentioned in more detail later. It would also be needed to access transaction data, security footage, employee data, etc. The necessary software would be incorporated to make this usable and trackable for local site employees. Other entities that would be on a typical local network would include private and public Wi-Fi and food ordering tablets to allow people to order their food. Food ordering tablets are necessary to make customer transactions more efficient, and the different Wi-Fi channels provide extra protection for company information.

All this information would strongly benefit from having connections to a main location. The main benefits that connecting to a main site location would be the security of stored information and keeping the network alive. A final aspect of a local site is security, needing cameras and other equipment to monitor the premises. This would apply to the local site network as well, requiring a firewall and the software necessary to manage and implement it.

The users for this system would be the cashiers working the registers, the IT worker managing the system, and a maintenance employee cleaning the location. The maintenance employee would not have as much access as the rest of the employees, as it does not pertain as much to his job and offers a potential leak to the company's information. All employees would operate under the private Wi-Fi network.

List of Network Segments -

Type of Location	Areas of Segmentation	Uses
Main Site	- Public Wi-Fi VLAN - Private Wi-Fi VLAN - IoT VLAN - Internal Main Site Employee Database separated by department - External Local Site Employee Database separated by branch - Customer Database/Transaction History - Database of suppliers, delivery methods - Server room with Web, Employee, File, DHCP, Database, VoIP, Printer servers	- Separates network usage for visitors versus employees - Includes network for the various devices in the building - Designates servers and networks for important general information
Typical Local	- Public Wi-Fi VLAN - Private Wi-Fi VLAN - IoT VLAN - Credit Card data VLAN - Employee information, scheduling VLAN	- Provides separate networks for guests and employees - Divides information of different subjects/importance into manageable areas

List of Locations

Num	Address	Town/City	Zip Code
1	1781 N Atherton St	State College	16803
2	223 Colonnade Blvd	State College	16803
3	101 Valley Vista Dr	State College	16803
4	3261 W College Ave	State College	16801
5	120 Southridge Plz	State College	16801
6	765 Benner Pike	State College	16801
7	106 Savannah Ln	Centre Hall	16828
8	2850 Benner Pike	Bellefonte	16823
9	820 S Eagle Valley Rd	Bellefonte	16823
10	718 Bellwood Ave	Altoona	16601
11	808 N Front St	Philipsburg	16866
12	1400 Logan Ave	Tyrone	16686
13	9894 Shaner Blvd	Huntingdon	16652
14	1330 Moore St	Huntingdon	16652
15	9681 William Penn Hwy	Huntingdon	16652
16	10 Sheetz Dr	Reedsville	17084
17	101 N Logan Blvd	Burnham	17009
18	113 N Juniata St, Lewistown	Lewistown	17044
19	24578 Rte 35 N	Mifflintown	17059

These are the 19 Sheetz locations we will be using when creating our network, and we will connect all of them together to give our network a seamless connection to each of the fellow storefronts as well as the headquarters location. This connection will allow our stores to be able to communicate financial information, other customer information, and stocking information.

Because the company would be acquiring sensitive credit card information, this information needs to be stored and dealt with correctly. Connecting our sites to a main location gives each location the ability to store customer information at a more secure site. Any stocking information would also be able to be communicated with the headquarters, so the company would have better knowledge of what needs ordered to each location. This also gives the headquarters location a better idea of each store's profitability. Our connection to sites also provides a form of prevention against the network going down. If one store's network happens to fail, there would be a loss of money made because none of the card readers would work. Having a connection between sites allows for the network to remain functional even if there are problems within the network.

The main site will contain servers for all different aspects of the company. Having these all in one place allows for tighter security as well as cheaper security. It is cheaper because there are not as many things that need to be purchased for each individual site. Within the main site, there are also many administrative bodies that need to be there in order to run the company. There are other security devices implemented which will be explained in later parts as well as web servers for the company's website.

Security Requirements

Sheetz is a business that deals with many transactions, many of which will be done with credit/debit cards. Because of this, it is imperative that we consider the Payment Card Industry Data Security Standard when designing the network. The safety of customers' financial information must be a priority, as customer trust is a crucial part of any business. We consulted PCI SSC (2018) for the compliance requirements.

The first goal of the PCI DSS is to construct a secure company network. To accomplish this the first steps that we will take are to install and configure an enterprise-tier firewall around the whole network, the details of which will be described in the ‘Security Apparatus’ section below. We will also configure the domain controller for Active Directory to make sure that no accounts on the network can be created using the default credentials, such as ‘admin:admin’ or ‘guest:guest’. Multi-factor authentication will also be used as an additional layer of security to prevent account breaches. Because we are employing the use of an Internet Service Provider to connect far away sites together, we will need to use virtual private networks to add security at the network level. This will protect sensitive information from the ISP and anyone who can breach their network.

Another important part of creating a secure company network is network segmentation. We will use VLANs to divide the networks logically into segments based on purpose. The most important and therefore secure segment will be the one containing the servers that store sensitive information and provide critical network functions. This VLAN will have the most limited access, and the credentials for privileged users should be stored offline in a physically secure place. There will also be network segments to represent each department of employees. These VLANs should also be secure but not as isolated as the server segment. Splitting departments into separate segments like this will keep network resources more split up, making it more difficult for intruders to attack laterally. The main site will also have a network segment for the demilitarized zone. The DMZ VLAN will contain servers that provide services accessible externally to the public Internet, such as web and public file servers. At each location there should be a separate VLAN for IoT devices, as they are very insecure and need to be isolated from the network segments that need to be more secure. Finally, there will be segments for public 802.11 networks with limited security. It should be noted that no sensitive data should travel through this last group of VLANs, as they are very vulnerable to attack.

The next goal of PCI DSS is to protect stored cardholder data. This will be accomplished by encrypting all card data traveling across the network using AES, and by carefully managing the authorization to the database where card information is stored through Active Directory. We will adhere to the Principle of Least Privilege (PoLP) when considering Active Directory authorization, which dictates that user accounts should only have access to the resources on the network that they absolutely need to do their job. The servers that contain cardholder information and the domain controllers will be installed in a room that is physically secure, under surveillance and with very limited personnel access. Sensitive information stored within these servers will not sit in plaintext and will be encrypted to add extra security in case of a network breach.

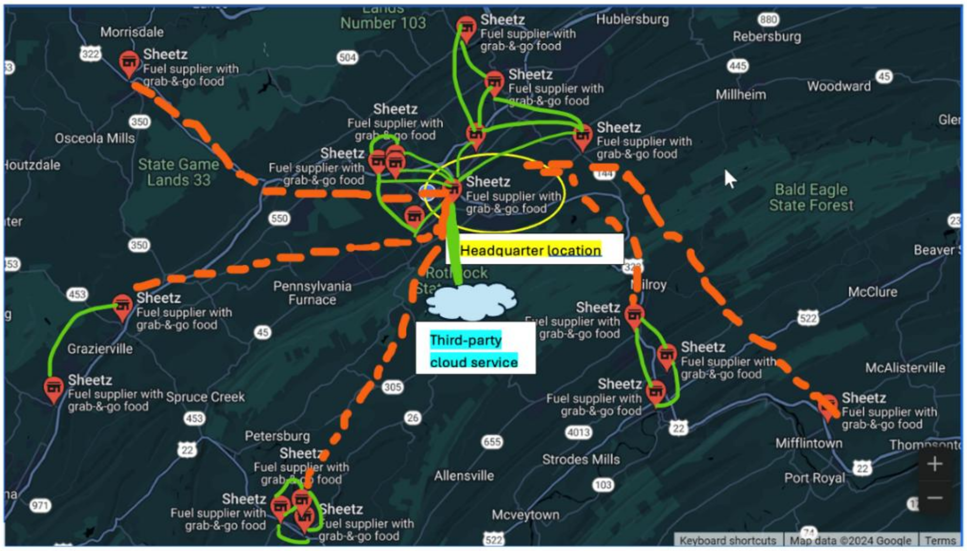
PCI DSS also dictates that the endpoints on the network have software that can manage vulnerabilities. We have decided that since the network will be composed of Microsoft Windows devices, Microsoft Defender with Defender for Endpoint is a good choice to fulfill this role. Additionally, the company IT policy will dictate that all applications stay up to date. If there is a critical application that must be kept online, it should be hosted on a server cluster or run on multiple virtual machines so that the application can be updated with minimal downtime. If there is hardware that no longer supports the newest versions of any applications it needs, then it needs to be replaced.

The network will be monitored 24/7 with all events logged with records kept for a year after recording. These logs will be audited frequently, using software to help filter events to look for suspicious activity. To ensure that the network is up to date in cybersecurity practices, full-scale penetration tests will be done on the network quarterly. The penetration tests will be conducted by outside companies, ideally rotating the companies performing the testing to get different perspectives of attack.

The final mandate of the PCI DSS is to develop and maintain an information security policy that all employees and third parties must abide by. This policy will detail the many security measures listed above, and the protocols for maintaining these systems. The policy will additionally outline the proper procedures for interacting with the network. Examples of network or data misuse should be provided and emphasized. A plan for regularly training employees in security practices will be outlined. This training should bring awareness about social engineering attacks such as phishing and insist upon crucial practices such as never leaving an unlocked device on the company network unattended.

Network Design

Site-to-Site connectivity



━━ Dedicated Fiber optic line.

☁ Third party cloud service

▬ ▬ ▬ ▬ ▬ Comcast ISP connection (wireless and cabled connection)

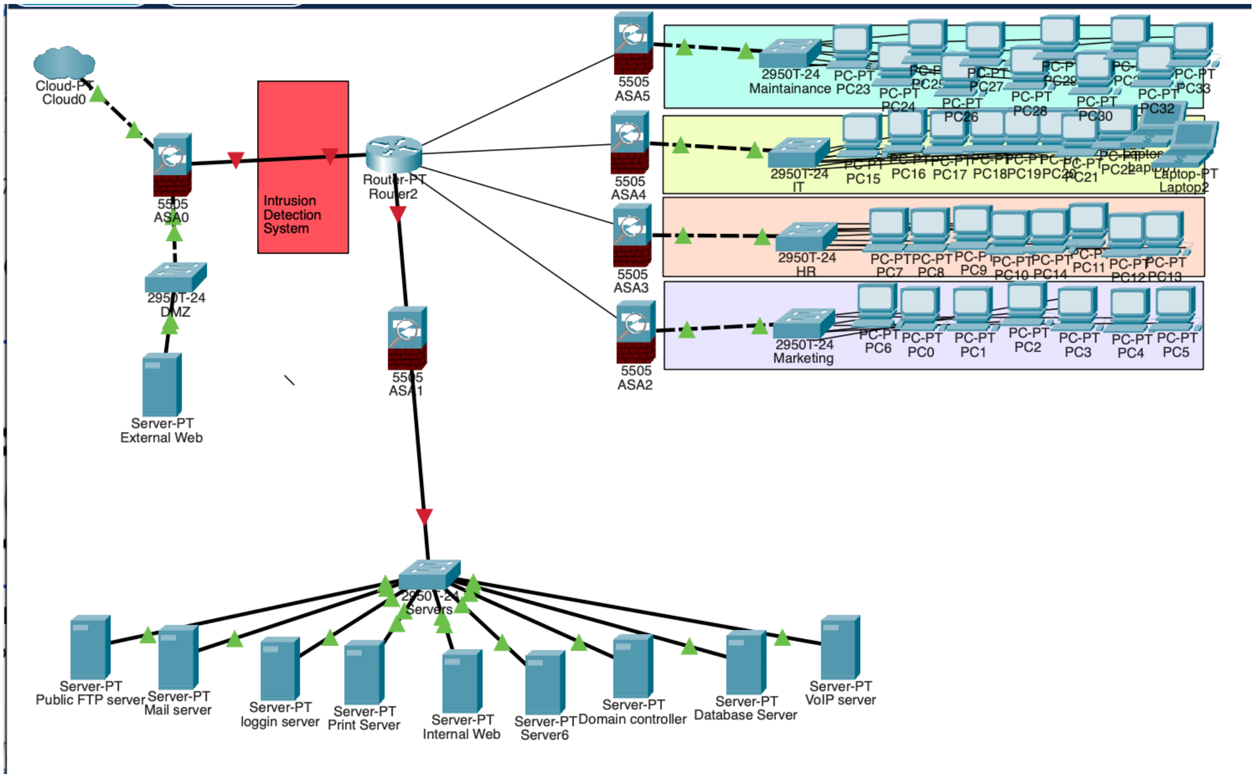
○ Headquarter location (@State College)

The locations near the State College area are connected to the headquarters (in State College) via dedicated Fiber optic cables offering them the privilege of fast reliable & dedicated connections. We have also added redundancy to the network. The locations that are further away from the State College area and are faced with difficult geographical terrain like high mountain ranges or dense forests are then connected via using the already built Comcast ISP infrastructure.

Site-To-Site Connectivity Description

We will segment network in parts based on distance of sites from each other, for example all the State College locations will be connected to each other via fiber, while the locations further away from the State College area will be using ISPs. The locations closer to State College will use fiber because there are no obstacles in the way in between the locations. Fiber is also better to use for these locations because fiber is very reliable compared to other options and it is unlikely to have interference with any environmental factors like a mountain or a deep valley. Fiber is also a very secure type of wiring, and it is very hard for signals to get interrupted using the fiber optic wiring. The locations further away from State College will use ISPs as some locations have big mountain ranges in between locations. The mountains make using fiber wiring very difficult to use. Using an unguided media source like an ISP would make more sense. Having a tower between locations with mountain ranges would make sure the distant locations would still be able to connect between each other and connect to the headquarters. Another reason why using an ISP would be useful is the fact that ISPs are cheap. Using an ISP would save the company money and if the tower connecting the locations needs to be fixed it would cost less than digging up the fiber wires in the ground. The tower would be much easier to fix and would also cost less to fix than the fiber wiring under the ground. We would also use a VPN with the ISP to provide extra security. The VPN would help the ISP retain its reliability and stability when providing a connection between locations or between a location and the headquarters. The VPN would also introduce latency which would slow down the time it takes for the packets to be sent and received but the packets would be more reliable to get there and to get to the destination without any interference.

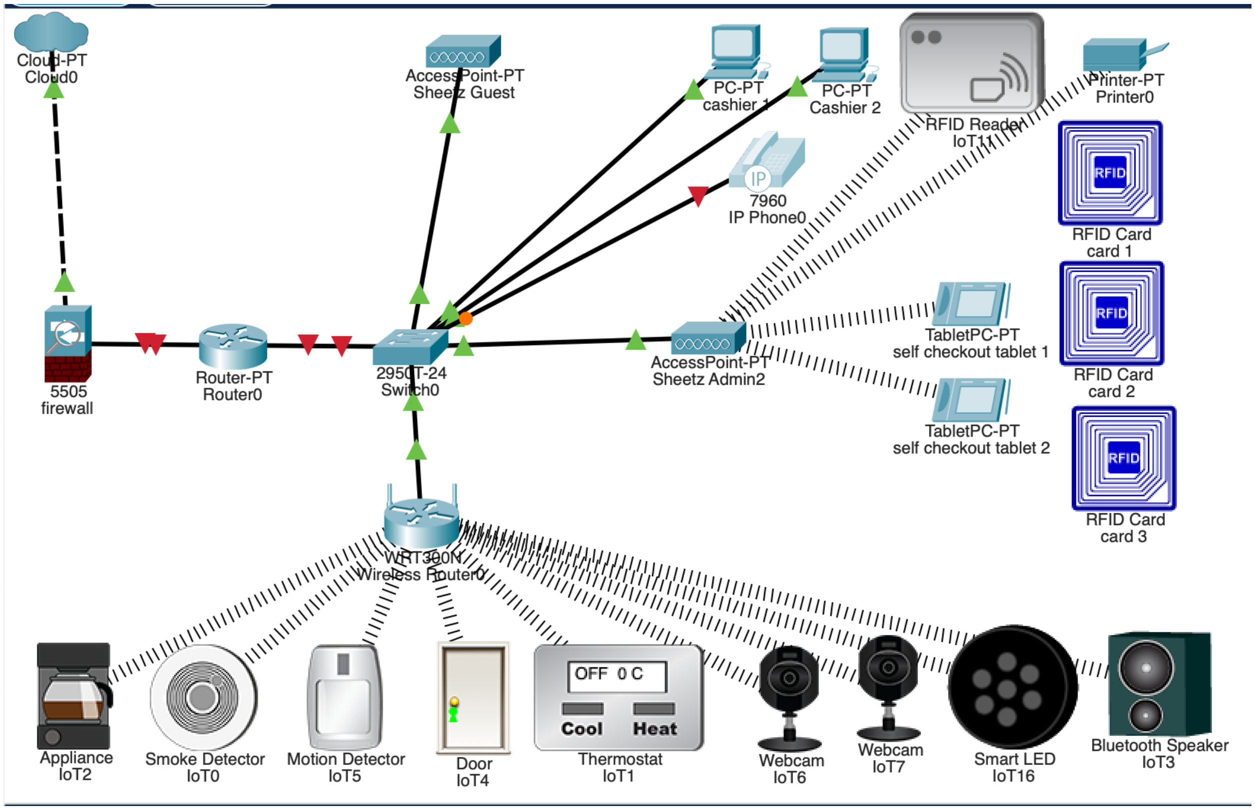
Main Site


Cloud-PT
Cloud0
5505
ASA0
Intrusion Detection System
Router-PT
Router2
2950T-24
DMZ
Server-PT
External Web
5505
ASA1
5505
ASA5
2950T-24
Maintainance
PC-PT PC23
PC-PT PC24
PC-PT PC25
PC-PT PC26
PC-PT PC27
PC-PT PC28
PC-PT PC29
PC-PT PC30
PC-PT PC31
PC-PT PC32
PC-PT PC33
5505
ASA4
2950T-24
IT
PC-PT PC15
PC-PT PC16
PC-PT PC17
PC-PT PC18
PC-PT PC19
PC-PT PC20
PC-PT PC21
PC-PT PC22
Laptop-PT Laptop1
Laptop-PT Laptop2
5505
ASA3
2950T-24
HR
PC-PT PC7
PC-PT PC8
PC-PT PC9
PC-PT PC10
PC-PT PC14
PC-PT PC11
PC-PT PC12
PC-PT PC13
5505
ASA2
2950T-24
Marketing
PC-PT PC6
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
2950T-24
Servers
Server-PT
Public FTP server
Server-PT
Mail server
Server-PT
loggin server
Server-PT
Print Server
Server-PT
Internal Web
Server-PT
Server6
Server-PT
Domain controller
Server-PT
Database Server
Server-PT
VoIP server

Main Site Description

For the main site or the headquarters of our project, we decided to have a Demilitarization Zone. The Demilitarization Zone will allow web-based services such as a web server, a public FTP server, and an email server. The DMZ is configured as its own network segment or VLAN. The VLAN would be positioned outside the perimeter firewall, and it would directly face the external users. This would also provide an extra layer of protection for the internal network. There are many different departments throughout the headquarters. These departments include Marketing, HR, IT, and Maintenance. All the different departments will have their own network segment and firewall. The firewall will enhance network security by isolating departmental resources and it will control access to certain information. Each of these firewalls will be configured to restrict certain traffic between these departments. We have established a physically secured server room to house certain critical infrastructure components. These components include the database, the server, the server domain controller, the DHCP server, and the secure file server. This server room would be on its own separate network segment away from everything else. These network segments will have very limited access ensuring that only authorized individuals can access it and manage the resources in it. By isolating all these components, we can ensure that the information that is stored in the headquarters database is secure and safe.

Typical Local Site



- separate network for guests vs. Admin
- Separate VLAN for sensitive payment processing devices (‘Sheetz Admin2’ with WPA2-PSK security password ‘highsecurity’) --> RFID reader, self-checkout, printer for receipt, etc.
- Other IOT devices connected on different VLAN (‘Sheetz Administration’ with WPA2-PSK security)
- Firewall for security

Typical Local Site Description

For each typical Sheetz location, we need to ensure smooth and secure network operations across all of them. Each location will need IP address ranges and segmented across the network accordingly. At the main site IP address ranges allow for various things that happen. Some of these include internal data transmission, Wi-Fi available for the public to use, Wi-Fi that is only available for members of the company to use, VoIP phones, cash registers, and administration devices. Each of these will have its own unique and distinct IP address range to prevent conflicts from happening. Similar producers from the main site will also take place across that main typical local site as well. VLANs will be used to achieve segmentation and each VLAN will be assigned to a specific function like the cash registers or the public Wi-Fi. Using this approach will minimize unauthorized access and breaches. The network infrastructure will allow multiple processes to happen. This could include people inside the gas station with a connection to the Wi-Fi or the cash register being able to make a transaction process between a customer and the store. The segmentation across all the locations will not only help security but it will also help communication between the locations and help the store maintain customers' satisfaction.

Security Apparatus

The most sensitive resources in the company network will be at the headquarters, so it will have the most security measures. Logically there will be a perimeter firewall around the headquarters network, with additional firewalls for the different VLAN segments within the network. There will also be a firewall at each branch location, as they will be physically separated from the headquarters network by the ISP. We will be using a Next Generation Firewall, or NGFW, as this type of firewall provides additional security services. Like a normal firewall, this will provide filtering, inspection, and VPN identification services. Additionally, an NGFW can also perform deep packet inspection and can adapt to better fit the applications we will be running on the network, providing intrusion prevention. (CloudFlare, 2024) The Fortinet NGFW is a good choice for this, as it used a hybrid-mesh firewall that allows us to unify every firewall on the network under one management tool. As network end points will be addressed using IPv4 we will set up NAT and use IP addresses from private ranges.

An Access Control List (ACL) will need to be configured for each firewall throughout the network. These are rules for inbound and outbound connections traveling through the firewall. When initializing the firewall, by default all connections should be denied, and then we will add rules above this to allow for specific connections. Outbound connections to the web, that is from end devices on the network, should be allowed, but the firewall should only allow connections to trusted websites and domains. This will help prevent employees from accidentally downloading malicious software, as well as an attacker that has breached an end device downloading malware intentionally. Inbound connections should be very limited. Stateful packet filtering should be used to keep track of current TCP connections which must be established by end devices on the network and allow this traffic through. Inbound TCP packets with an ACK bit equal to ‘0’ should be rejected, as they are an outside attempt to establish a TCP connection. All UDP flows should be rejected with a few exceptions, such as port 53 for DNS, or for internal network services that may use UDP like VoIP. The firewall for the DMZ will need to be more lenient to allow users to access public resources across the internet. On the web server, inbound connections should be allowed on ports 80 and 433 for the HTTP and HTTPS protocols.

As mentioned before, the NGFW we will be using has software in it that will allow us to configure VPN connections that will be allowed into the internal network. However, the firewalls for the different segments inside the network will have rules to limit these incoming VPN connections to accessing only the department(s) they are supposed to. The firewalls for each network segment should also limit incoming traffic from other segments by default, only allowing traffic from specific IP addresses and applications from network end-devices that need to communicate according to the Principle of Least Privilege. Certain applications that allow employees to communicate like internal mail will likely span most of the internal network. The firewall for the network segment containing data protected by PCI DSS should be particularly limited when it comes to inbound connections. The firewall system should be configured to send all network events to a logging server, in compliance with PCI DSS. Logging servers will be in the server room on a separate VLAN with similar restrictions to the segment with sensitive database and file servers, but with more lenient access rules for the IT department who will need to audit the logs.

Just inside the perimeter firewall an Intrusion Detection System will be installed to provide another checkpoint for network traffic. Because new malware is being developed all the time, we have decided to use an anomaly-based IDS. This will perform further deep packet inspection and alert the IT administrators in case of suspicious packets that have made it past the perimeter firewall and its integrated IPS. Information will be collected and sent to a security information and event management system (SIEM) where it can be analyzed and responded to by the IT staff. (Barracuda Networks, 2024)

Finally, for additional security in the application layer, we will be using Microsoft's Active Directory service. Active Directory will ensure that authentication remains consistent across all end points on the network and will make managing the many types of Windows accounts across the network easier. A hierarchy of domains will be created that contain different departments or other groups of devices. These domains can be further grouped into trees and all trees will be grouped under one forest, which the root domain controller will govern. User accounts will be created and classified into domains based on the function of the account, and the access control to network resources of different user accounts or account types can be defined through domain controllers. Access to resources across domains and trees will be dictated by the root domain controller. This separation will provide similar security benefits to the network segmentation through VLANs, but functions at the application layer rather than the data-link layer. (Microsoft Learn, 2014)

Breakdown of Team Member responsibilities and contributions

Who wrote what?

Danny Mitchell & Aiman Sohail – Table of Contents/Cover Page

DJ Wheeler & Dominic Eicholtz– Overview/Summary

Description of Needs Requirements:

Jacob Allen/Danny Mitchell –List/Description of Computer Systems

Jacob Allen/Danny Mitchell – List/Description of Network Segmentation

Danny Mitchell – Locations Table

Dominic Eicholtz – Justification of Each Location

DJ Wheeler – Security Requirements

Network Design

Aiman Sohail – Network Design Diagrams

Nick Hadden – Site-to-Site Connectivity (Writing)

Nick Hadden – Main Site (Writing)

Nick Hadden – Typical Local Site (Writing)

DJ Wheeler – Security Apparatus

Citations, References, Resources Used

- (2024). *How to Setup a Firewall in 6 Steps for Your Small Business*. Cisco. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/how-to-setup-a-firewall.html
- PCI SSC. (2018, August 20). *PCI DSS v3.2.1 Quick Reference Guide*. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
- (2024). *What is a next-generation firewall (NGFW)?*. CloudFlare. https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/
- Stone, M. (2021, March 15). *What is network segmentation? NS best practices, requirements explained*. Cybersecurity.att.com https://cybersecurity.att.com/blogs/security-essentials/network-segmentation-explained
- (2024). *Intrusion Detection System (IDS)*. Barracuda Networks. https://www.barracuda.com/support/glossary/intrusion-detection-system
- (2014, November 19). *Active Directory Structure and Storage Technologies: Active Directory*. Microsoft Learn. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759186(v=ws.10)