Securing Hometown Pizza’s Network: Gaining Cybersecurity Insurance

Aaron Caton, Alex Cook, Serena Mitchell

Western Kentucky University

CIT 490: Senior Research

Dr. Mowafi

December 2, 2024

Table of Contents

Deliverable 5: “System Design”

Aaron Caton, Alex Cook, Serena Mitchell

System Design:

Narrative

Hometown Pizza needs an upgrade to their network environment within their fourteen branch locations and their corporate office. The company will need to adapt a policy for terminated employees to ensure terminated employees do not create a vulnerability. Our team will implement several key components that will ensure confidentiality, integrity, and availability of their intellectual data while maintaining customers’ confidentiality and integrity of their data.

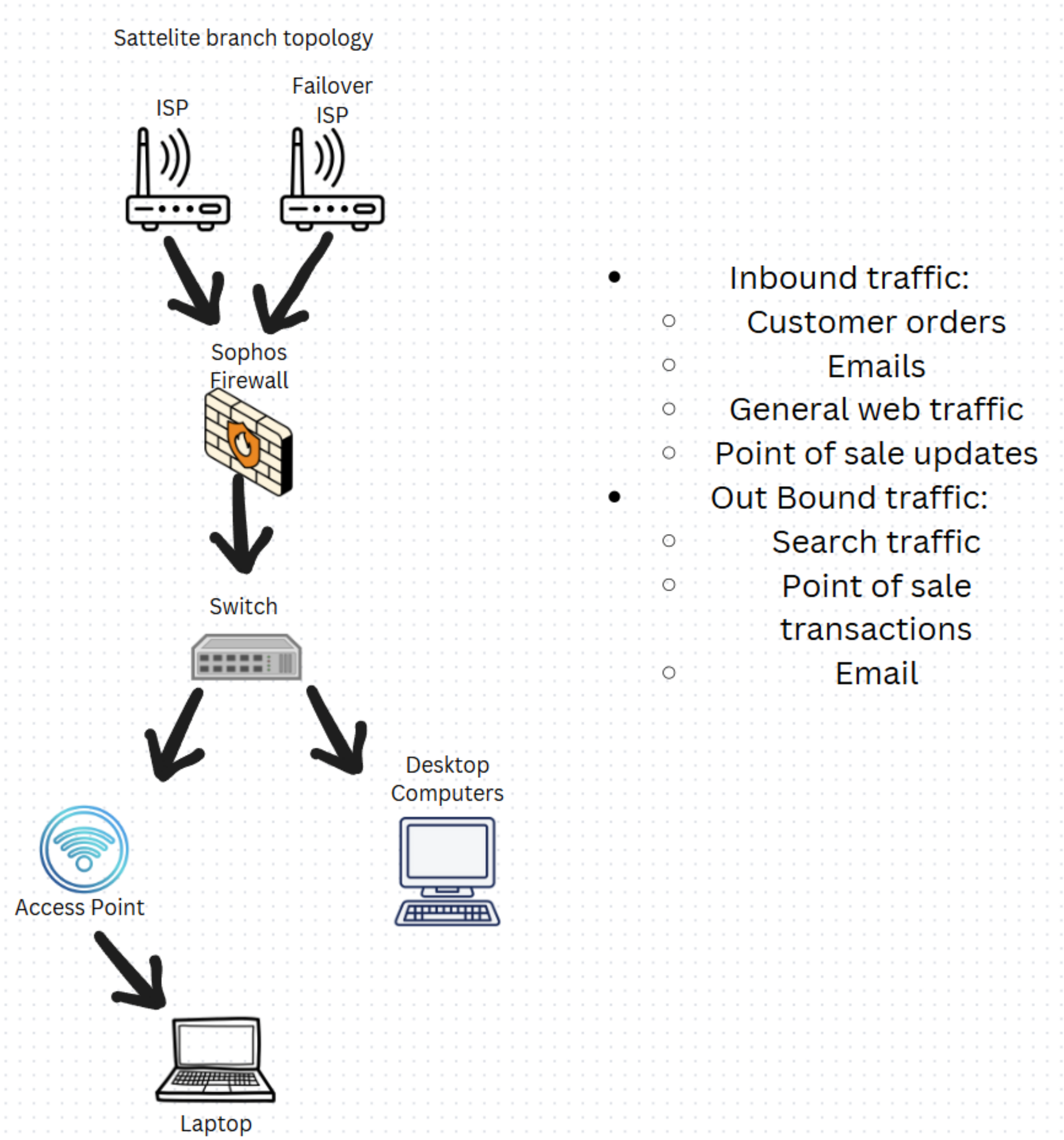
First, we will be removing the out-of-date SonicWalls that exist within the fourteen branch locations. We evaluated several solutions to securing their network environment; we examined network segmentation and cloud-based firewalls. While those are a great solution to an outdated firewall, we believe it is in the best interest of our client to install physical firewall devices. We will be installing SOPHOS XGS 116 behind their internet service provider modem and their failover device. This device will enable Hometown Pizza administration to view general management dashboards via a web browser from anywhere. It will monitor traffic including the ability to have stateful packet inspections, it will be able to route traffic to appropriate destinations, implement Quality of Service rules for VOIP traffic, administration will receive live alerts from Intrusion Detection, and even stop attacks before they happen with Intrusion Prevention system. Hometown Pizza’s administration can create access control lists to prevent unwanted network traffic or any future vulnerabilities. The great news about this device is that end users within the branch location will not be hindered by this change. The end users will not even notice a difference between the SonicWall and the SOPHOS device. SOPHOS XGS 116 will provide optimal security for branch locations whereas the SonicWall was no more than a glorified router.

Second, we will be implementing SOPHOS's Intercept X for their file server at the corporate location. Hometown Pizza currently does not have any additional protection for their file server, and it sits behind the outdated SonicWall. Additionally, the file server is not being backed up properly or routinely. Our team will be moving the physical server to a different closet that has sustainable airflow and a ventilation system. It is important for the physical health of the device to be in a well-ventilated area to mitigate the risk of excessive heat exposure. Next, we will be applying the SOPHOS Intercept X to the file server that will carry out many vital functions. Those vital functions would include web protection, application control, data loss prevention, server lockdown option, ransomware file protection, anti-malware scanning, file integrity monitoring, and routine backups that can be stored on the cloud. The end users at the corporate location should see no impact by implementing this if they are in line with the company technology policies. End users will still connect to the file server the same as before and authentication of users will remain the same. Intercept X will only impact the bad actors trying to gain access to the file server.

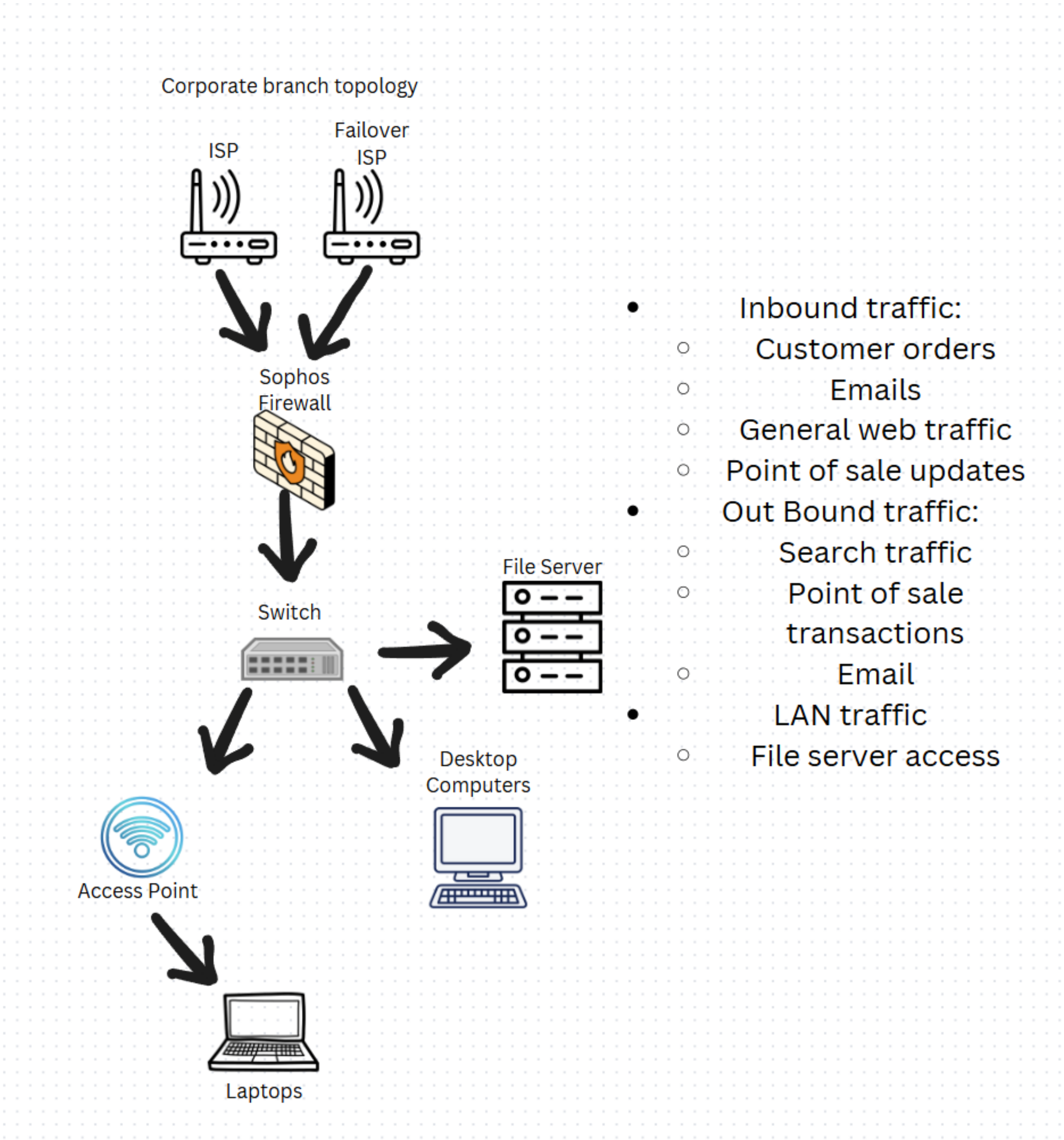
Lastly, we will produce an exit policy for the company handbook that will include a process on safely dismissing an employee from the company. The policy would include all services and accounts that the user would have access to. It would include important documentation for the Human Resource Department to carry out the necessary steps to remove all access per individual. Our team is aware of the potential damage that could occur from a terminated employee still having access to the company’s assets. We want to help Hometown Pizza enforce a proper exit policy for their handbook.

We understand that there are requirements and constraints within this project. Our recommendation will fulfill those requirements for Hometown Pizza and will allow them to secure cybersecurity insurance. We have a plan to combat the constraints of installation times and the physical distance between the branch locations. We will schedule accordingly to make best use of our time and Hometown Pizza’s time. We will implement strict budget controls to minimize the risk of exceeding the projected budget provided by Hometown Pizza. We strongly believe that we are recommending the best tools and resources to secure the network environment for the corporate office and branch locations with minimal impact to Hometown Pizza employees and customers.

Process Model:



- Inbound traffic:
  - Customer orders
  - Emails
  - General web traffic
  - Point of sale updates
- Out Bound traffic:
  - Search traffic
  - Point of sale transactions
  - Email



- Inbound traffic:
  - Customer orders
  - Emails
  - General web traffic
  - Point of sale updates
- Out Bound traffic:
  - Search traffic
  - Point of sale transactions
  - Email
- LAN traffic
  - File server access

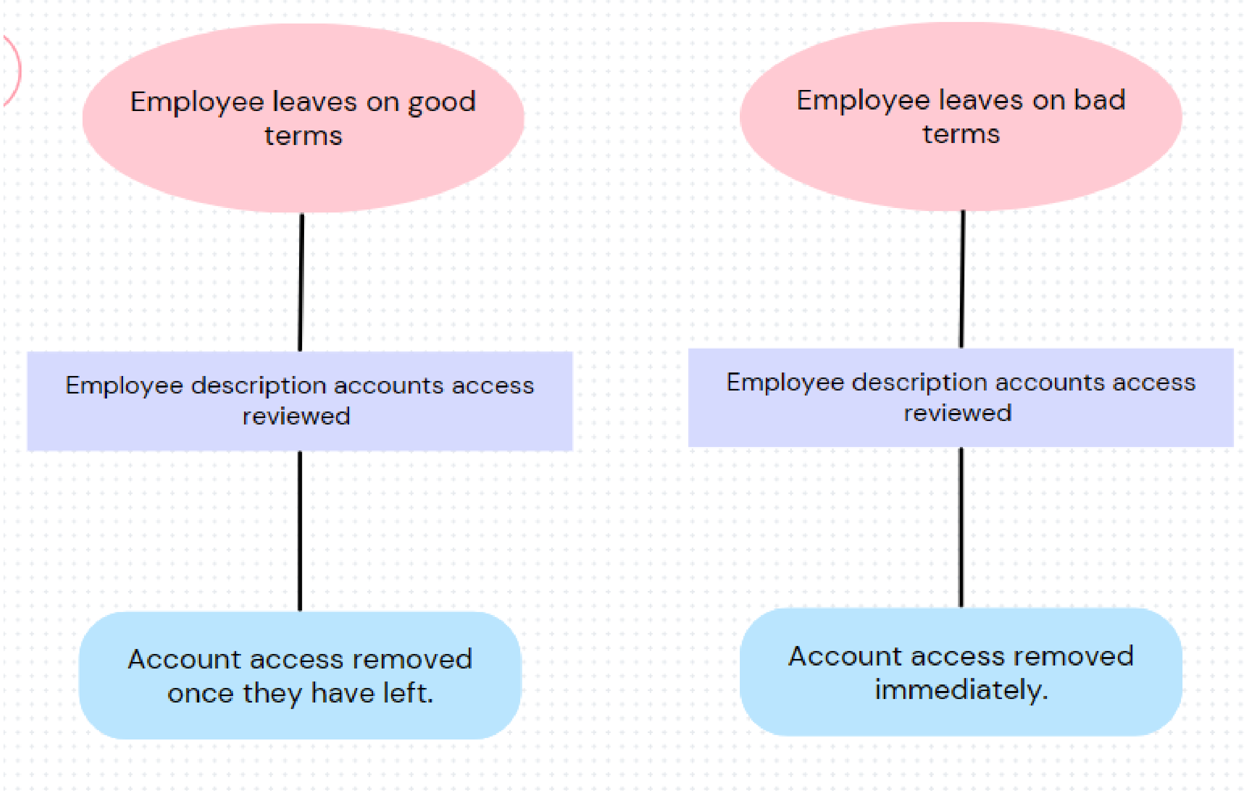
Each device on the corporate network currently sends traffic from the device through the switches, through the firewall, then out to the internet. All inbound and outbound traffic is monitored, but the monitoring leaves a lot to be desired since the current firewall is out of date.

All inbound and outbound traffic that is perceived as a threat will be blocked by the new firewall to prevent possible intrusions or use of our client's network as some form of bot net.

The file server can be accessed by any device on the corporate network, and it does not have any special security to prevent any user from being able to access files on the server. It is not an online server, so that makes it somewhat more secure, but with there being little to no security on the server itself, an attacker could still hijack a local machine and access whatever files they wanted.

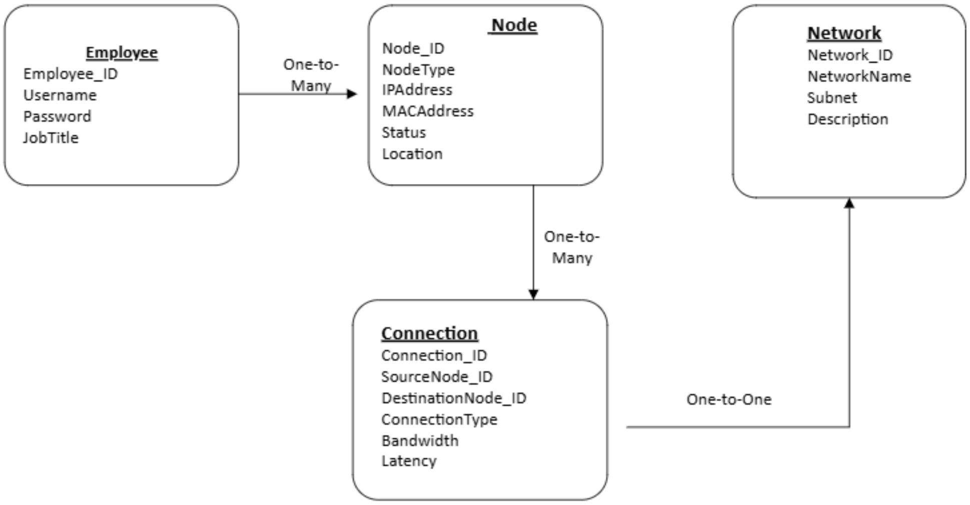
The new Sophos firewall will provide state of the art protection while allowing for the IT manager to monitor existing threats, potential breaches, and confirmed breaches, if there were one, from a cloud-based monitoring platform. This would allow the IT manager to monitor traffic like they never could before, and it would protect the company better than the old sonic wall ever could.

Employee Exit Policy Process Model:


Employee leaves on good terms
Employee leaves on bad terms
Employee description accounts access reviewed
Employee description accounts access reviewed
Account access removed once they have left.
Account access removed immediately.

The employee exit policy is very simple to avoid missing employee account access. HR will evaluate the employee's role to see what accounts that employee role has access to as the first step. The accounts are then terminated according to how the employee leaves. There are usually two scenarios in which an employee leaves, on bad terms or good terms. If the employee leaves on bad terms, they usually don't give two weeks' notice, or just don't show back up. Those who leave on good terms usually give some form of notice as well. The process overview is basic, but the decision tree provides more details on what will happen in the account termination process.

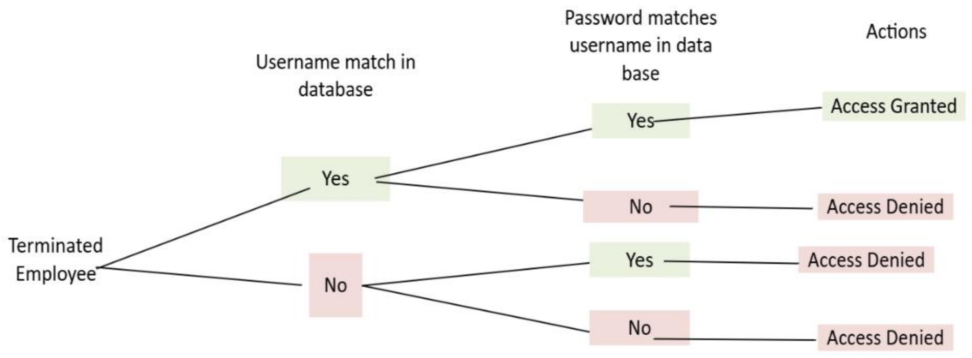
Data Model:



Our data model depicts each entity and the relationship among the entities. The entities are the key players within this data model with their corresponding attributes to describe the entity. Each employee has access to a node, but the employee is not limited to which node is being used. The nodes use connections, and one node can have various connections at any single moment of time. Each connection can only be on one network at a time; the connection would break if it was jumping networks. The data model will remain the same for the new system, but each entity will be more secure and managed than in the prior system.

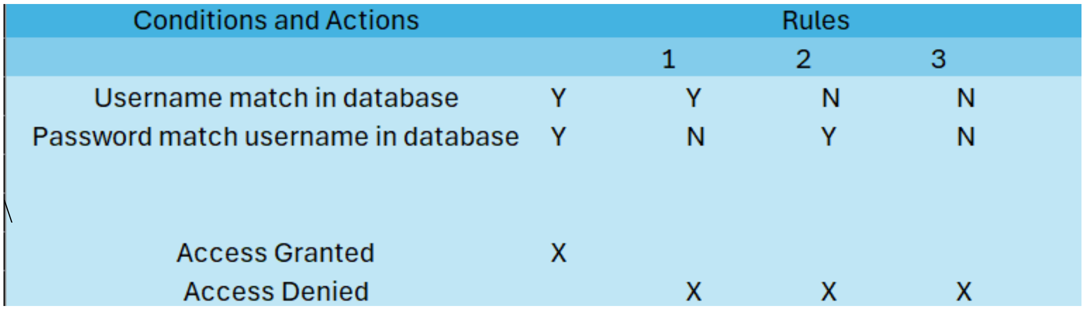
Logic Model:

Decision Tree for Terminated Employee Access:



This decision tree showcases the decisions the system will need to make in authenticating a user to allow them into the system. The system needs both the username and password to be correct to have access granted. The system will test if the username matches in the database and then proceed to the password matching within the database. This decision tree correlates with the proposed exit policy that our team will be implementing, so a terminated employee will have access denied.

Decision Table for Terminated Employee Access:



Conditions and Actions		Rules		
		1	2	3
Username match in database	Y	Y	N	N
Password match username in database	Y	N	Y	N
Access Granted	X			
Access Denied		X	X	X

Our decision table shows our decision tree, but in table format. We have the conditions and actions listed within the table. The conditions would be what is being tested. First condition is, “username match in database” and second condition is, “password match username in database”. Depending on the decision for those conditions the user would receive an action. That action would be access granted, or access denied.

Sequential Structured English for Terminated Employee Access:

1. Launch Program.
2. Prompt for username.
3. Database checks for True or False on username.
4. Prompt for Password
5. Database checks for True or False on password.
6. If both True, Then Access Granted
7. If either are False, Then Access Denied

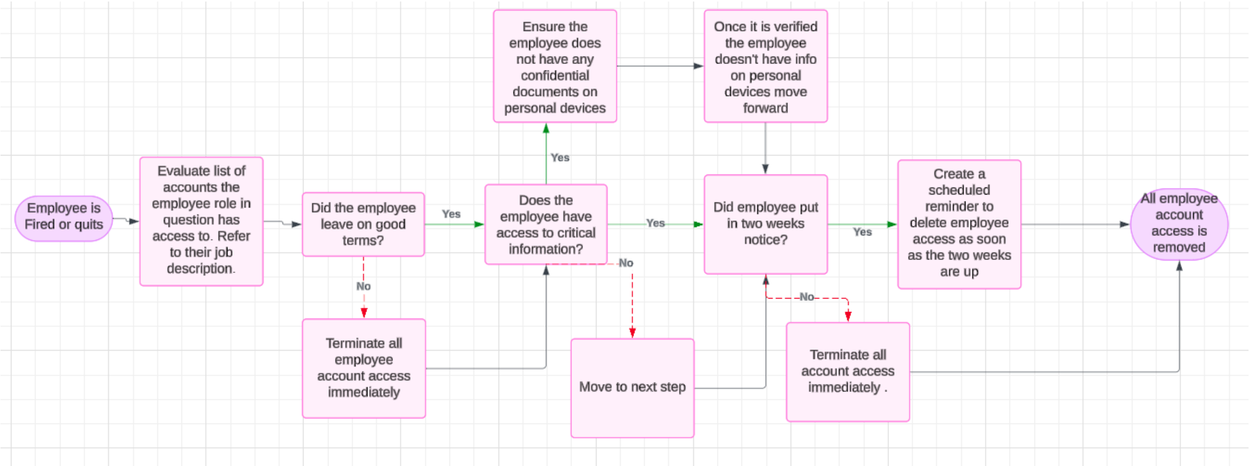
This structured English is described as a sequential, because it shows the order of steps the system will take in granting access or denying access for the user.

Decision Structured English for Terminated Employee Access:

- IF username matches in database and password matches username in database THEN Access Granted.
- IF username matches in database and password does not match username in database THEN Access Denied.
- If username does not match in database and password matches username in database, THEN Access Denied.
- If username does not match in database and password does not match in database, THEN Access Denied.

This structured English is described as decision making, because it uses IF/THEN statements to depict if condition is True then the action occurs. It is the same information depicted in the above logic models but makes the TRUE/FALSE more concise.

Employee Exit Policy Activity Diagram:


Employee is Fired or quits
Evaluate list of accounts the employee role in question has access to. Refer to their job description.
Did the employee leave on good terms?
Yes
No
Terminate all employee account access immediately
Does the employee have access to critical information?
Yes
Ensure the employee does not have any confidential documents on personal devices
Once it is verified the employee doesn't have info on personal devices move forward
Yes
No
Move to next step
Did employee put in two weeks notice?
Yes
No
Terminate all account access immediately .
Create a scheduled reminder to delete employee access as soon as the two weeks are up
All employee account access is removed

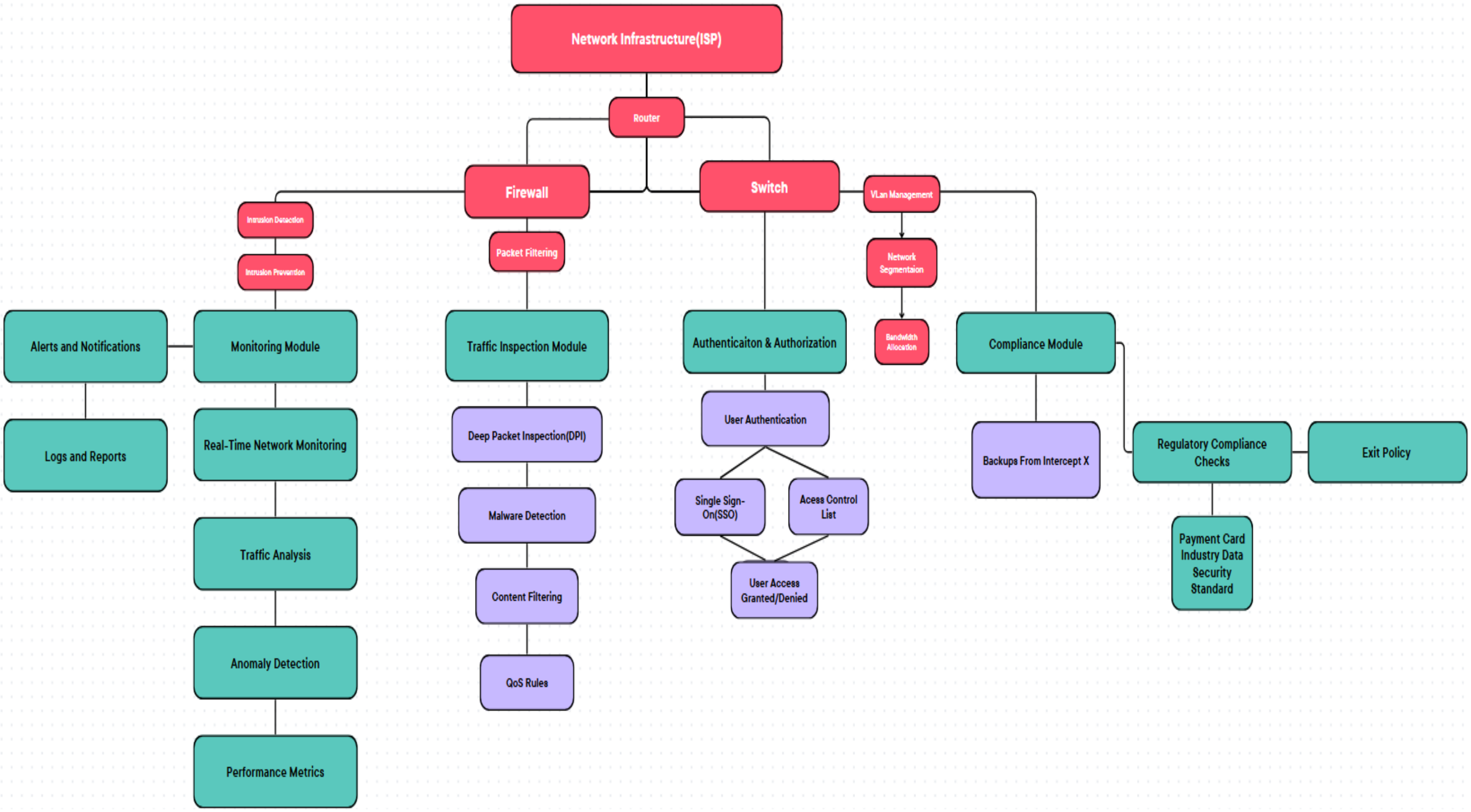
The employee exit policy consists of a few critical questions that include the following: Did the employee leave on good terms? Does the employee have access to critical information? Did the employee put in a two weeks' notice?

These questions are critical in determining how and when to remove employee account access. If the employee left on bad terms or holds some kind of grudge against the company, the employee should have all accounts terminated immediately and physical access removed.

If the employee left on good terms and some form of notice was given, all accounts would need to be noted, and a form of reminder would need to be created to ensure that all the accounts are terminated appropriately in a timely manner. It would also be important to ensure that employees who did not give a form of notice did not have company information on personal devices, however this could be more difficult but not impossible if the employee left on good terms.

If all the steps are followed correctly, an employee should have all account access and physical access removed. This would remove the possibility of an employee using their account access to perform attacks on the company with account access that could be forgotten or just never removed.

Software Design Structure Chart:



This structure chart was created to represent the relationships of the different components and modules from the hardware to the software design. The main network infrastructure hardware is positioned at the top levels of the structure chart, which is the foundation in our system design and the chart shows how it relates to each of the software modules. The main software functions are represented in four main modules, Monitoring, Traffic Inspection, Authentication/Authorization, and Compliance modules the structure chart shows how they interact with the foundation hardware at each hometown pizza location and corporate. There are also sub-modules represented to show extra detail of the processes of each module. Overall, there is a unique dynamic with the SOPHOS firewall and its software design modules, specifically when it comes to the SOPHO's Intercept X backups that are preformed and stored at the corporate location.

Conclusion

We began this project by creating a Project Proposal (See Appendix A) for Hometown Pizza. This included learning about our client and their current problems securing cybersecurity insurance. The next phase of our project was to create a Baseline Project Plan (See Appendix B) which included system description and feasibility analysis. Next, we evaluated the structured requirements (See Appendix C) including alternative solutions to determine which would be the best fit for Hometown Pizza's needs. Finally, we evaluated an alternative solution (See Appendix D) to the current problem Hometown Pizza is facing. The conclusion of this project was determining the solutions our team would facilitate to ensure Hometown Pizza was eligible to get cybersecurity insurance.

Appendix A

Deliverable 1: "Project Proposal"

Aaron Caton, Alex Cook, Serena Mitchell

Introduction

In today's technology-driven world, where businesses and consumers depend heavily on technology for daily tasks, the risk of cybercrimes has significantly increased. Companies today can have in-house information technology departments that can create a safe technology environment to mitigate attacks. Unfortunately, some companies are so involved in day-to-day tasks, that they may lose sight of vulnerabilities within their technology environment. Maybe they just need a hand in tidying up the technology environment for securing cyber insurance and receiving the cyber insurance at a fair rate. That is where our team comes into play. Let's dive into the details of this proposal.

Organization Information

We want to help Hometown Pizza Corporate Office, located in La Grange, Ky, tidy up loose ends to successfully gain cyber insurance and for them to receive that cyber insurance at a fair rate. Hometown Pizza is a medium-sized business with approximately 500 employees spread amongst the corporate office, and fourteen locations. This company is in the restaurant industry, making it a commercial business; this can cause this business to be a target as they process many employees through onboarding as well as perform credit card transactions daily.

Who will be Assisting us?

Our main contact at Hometown Pizza to help us complete our task of securing the technology environment will be Beth Toombs. She is an administrative professional with daily tasks like a compliance officer. She will be communicating with us and the insurance company to process the cyber insurance application after our project is completed. We will be able to reach her at beth@hometownpizza.com or via phone (502-222-5541). Also, we are utilizing an insurance checklist from Chubb Group of Insurance Companies that Hometown pizza must pass to acquire cybersecurity insurance. We are looking forward to working with Mrs. Toombs to help Hometown Pizza secure their technological environment.

What Will We Be Resolving?

In today's world cyber-crimes such as ransomware, identity theft, and credit card fraud are unfortunately commonplace. Some of these crimes result in people’s lives being completely ruined by being bankrupted by credit card fraud, people impersonating others by stealing social security numbers and other personal information, or corporations losing money by having confidential information stolen from them. Often this information is stolen through social engineering and is on a person-by-person basis. However, there are many instances of companies being hacked and millions of pieces of personal information being stolen and sold on the black market. A good example of this is the data breach with the credit card company Capital One in July of 2019, which affected 100 million Americans and 6 million Canadians. Information leaked included things such as names, social security numbers, addresses, and other personal information (The 12 Worst Data Breaches in the Last Decade: Sunmark Credit Union | the Bright Way to Bank - New York Capital Region, n.d.)

Hometown Pizza was looking at getting cyber insurance, but did not meet the requirements to acquire it. According to Nationwide Insurance, “Cyber insurance generally covers your business' liability for a data breach involving sensitive customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers and health records” (What Is Cyber Insurance? – Nationwide, n.d.). This can be an extremely important piece of insurance to have, especially in the food service industry where people’s payment methods are being used or stored constantly. In order to help Hometown secure cyber insurance, we will be implementing a new firewall, an employee exit check list, and new web server security.

With our goal of helping provide cybersecurity insurance for Hometown Pizza we reviewed the insurance checklist that must be passed. And we noticed there was a lack of detail when it came to any sort of employee exit policy. We brought up details of how previous employees have hurt this company in the past with access to personal information. So, we wanted to go the extra mile and provide a step-by-step check list for an employee exit policy. Which is crucial within cybersecurity because often employees leave the company with a bitter taste in their mouth and can cause a lot of harm. “12% of employees took sensitive IP with them when they left an organization, including customer data, employee data, health records, and sales contracts.” (Bonnie, Secureframe) Employees often can still access personal information after termination, and it is important to have a plan in place to ensure the sensitive information is secure and access to resources is properly managed.

Why Us?

In today's competitive market, having a skilled, caring, and focused team can make all the difference. We are a team who are compassionate about helping your business and we are passionate about the work we do. Our team is network and security focused, which is exactly what team you will need to accomplish the given project. We have provided a light overview of each member below:

My name is Aaron Caton. I am currently a senior with WKU pursuing my final class for my bachelors in CIT. I currently am in my fourth year working as a computer maintenance technician for the Henderson County school system here in Kentucky. Before that I worked as a systems administrator for RC Cola where my boss and I oversaw all the IT related stuff for 7 different locations across Kentucky, Indiana, Missouri, and Illinois. I will be the technician during this project and the boots on the ground for the organization. I will be specializing in malware protection/prevention amongst the hosts and networks within the organization.

My name is Serena Mitchell. I am currently a senior at Western Kentucky University and will be completing my degree this Fall. I have secured several certifications throughout my college career which are CIT Fundamentals, A+ Prep, Security+ Prep, Computer Tech Basic, and Information Security Specialist. I have completed network reviews, created functional network topologies, and replaced network environments to ensure functional and secure networks. I have experience in reviewing penetration tests and troubleshooting any holes within networks. My major role in this project will be Project Manager and specializing in Web Server Security.

My name is Alex Cook, and I am a 22-year-old student at Western Kentucky University finishing my degree in Computer Information Technology this fall. At Western Kentucky University I serve as the Student President of WKU Cru. Where I've learned many leadership skills and helped many younger students grow in their walks of life. I am also an active member of the National Scholars Leadership Society. Where I have developed my leadership skills even further. I am very passionate about cybersecurity, and I am currently pursuing various certifications to further enhance my skills. I also have a fascination for Artificial Intelligence development, and I have done previous research reports on how AI development has impacted cybersecurity / the IT industry in recent years. Lastly, I have a background in computer science and a certificate in game design where I can be creative. My major role will be handling the compliance tasks and being project liaison between our team and the organization. I will be specializing in the policies needed for the organization.

References

Bonnie, Emily . “101 of the Latest Data Breach Statistics for 2024.” *Secureframe*, 19 Mar. 2024, secureframe.com/blog/data-breach-statistics.

The 12 Worst Data Breaches in the Last Decade :: Sunmark Credit Union | The Bright Way To Bank - New York Capital Region. (n.d.). Www.sunmark.org. https://www.sunmark.org/connect/sunmark-360/12-worst-data-breaches-last-decade

What Is Cyber Insurance? – Nationwide. (n.d.). Www.nationwide.com. https://www.nationwide.com/business/solutions-center/cybersecurity/what-is-cyber-insurance

Appendix B

Deliverable 2: Baseline Project Plan (BPP)

Aaron Caton, Alex Cook, Serena Mitchell

1.) **Introduction**

A.) Hometown Pizza consists of fourteen units that are defined as full-service restaurants. They have one main office in La Grange, Ky, that houses corporate staff offices. The fourteen units each have their own independent networking environment. The networking environment consists currently of a low-grade firewall, switches, and one router. Each of the fourteen units has a management laptop not secured to an appropriate standard. At the main office, they have ten laptops that are not secured to an appropriate standard, and they have a Microsoft 2016 server used for data storage and shared files. The Microsoft Server is not appropriately configured with security in mind.

B.) Hometown Pizza is seeking cyber insurance, but currently they deem themselves not up to par on security compliance. Hometown Pizza has been made aware that their networking environment at the fourteen units is not safe and secure. They believe they are at risk of data breach or a malicious attack. The firewall is outdated and does not include enhanced capabilities of the current state of technology provided in the firewalls today. The laptops at each location do not have malware protection installed which poses a risk to the laptop, data, and the network environment. The Microsoft Server 2016 does not have malware protection in place and does not have regularly scheduled backups. The Microsoft Server 2016 is not in the most practical physical environment either. It is in a closed closet that does not have any air flow, and the closet does not have a physical lock. Hometown Pizza needs a security upgrade regarding virus prevention, intrusion detection & penetration testing on hosts and network. Hometown Pizza also needs an exit policy created to ensure the confidentiality, integrity, and availability of their data.

C.) Hometown Pizza is currently impacted by this problem due to the unsafe networking environment at the fourteen sites and the main office. Hometown Pizza as a business is vulnerable to loss of confidentiality, integrity, and availability of its data. One of the biggest threats to the business is loss of revenue. If a bad actor invades the networking environment and causes stop in service, then Hometown Pizza will be unable to conduct sales and tend to their customers. They would be unable to utilize their point-of-sale system including acceptance of payments from guests. They would be unable to use phones that are VOIP. The employees at each location would not be able to conduct their daily activities if the network was impacted due to negligence of information technology functions. If the computer server at the main office is negatively impacted due to negligence, then employees' personal identifiable information could be at risk of exposure and the corporate staff could not handle their day-to-day tasks if shared files were unreachable. Hometown Pizza's intellectual property could be held at ransom or even stolen if the server was comprised due to lack of security measures. The impacts of resolving these current problems would be minimum compared to the impacts of not resolving. Our team would plan to conduct the solutions before business hours to reduce the amount of downtime that would impact the business, employees, and their customers.

D.) The recommendation is to proceed with this project as the feasibility analysis concludes that the benefits would outweigh the costs of this project. Our team may encounter technical issues such as faulty equipment on site or lack of organizational(customer) skillset. We believe that we will be prepared for any technical issues that may arise for us and will be able to provide on-site training for managers in case a troubleshooting call may occur. We have the necessary skillset to complete the tasks included in this project. Economically, our team will have profitability, and we should be in the positive after completing this project. We will be charging the vendor price of the hardware to breakeven, but we will have increase and profitability by charging extra on license fees and monthly maintenance fees. We should not encounter any high-level risks associated with stakeholders, legal, or schedule issues. This project should be a win/win for our team and Hometown pizza. We have the necessary tools needed to complete this project without hindering our team's success.

2.) **System Description**

A.) The solution for improving the firewall situation would be installing a Sophos Firewall device at each of the 14 branch locations. That firewall would be the Sophos next gen firewall. With this setup, all traffic from each branch, wireless or hardwired, would be filtered regardless of the type of system. This option would drastically reduce the possibility of a device becoming infected with malware, becoming a victim of ransomware. With the Sophos systems, each branch location can be managed from a single cloud management portal. We will be preconfiguring all the firewalls in advance to minimize downtime at each location.

Once the firewalls have been installed, we will have penetration testing performed on the branch locations to ensure that everything that was installed was configured correctly and with no compromises to network security. This testing would ensure that our configurations were correct and provide a tangible report to Hometown Pizza that allows them to see that their network is safe rather than just taking our word for it. This should be done by an outside credited vendor as to not provide

The best solution for creating a formal exit policy would be to have a comprehensive list of job descriptions along with each of their levels of access as well as the systems they have access to. It is very easy to miss accounts and levels of access if there is not a list of different job-related accounts. For immediate termination cases, the associated accounts would need to be deleted immediately. For those who are putting their two weeks' notice in, some form of reminder needs to be created to delete the employees' accounts. To acquire the information, we need we would require a detailed organizational structure complete with access levels, physical and software.

Original Alternative(s):

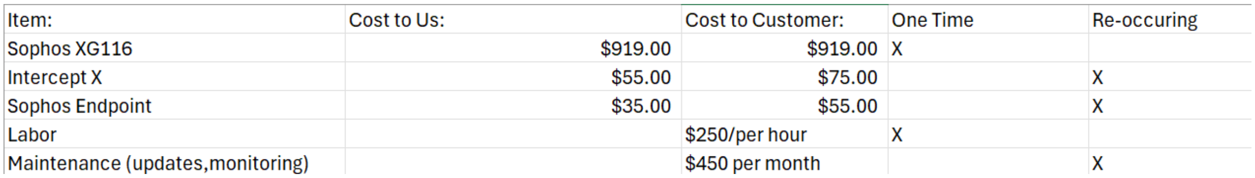
B.) Another option would include enabling the firewall on some Meraki mx68 devices, so each branch has its own application-based firewall on each of the devices. This would not be ideal considering not all the devices at a branch would be application compatible, which would not filter all the traffic. We would also implement Cisco's advanced malware protection to help add to the malware protection. This would work with the Meraki devices so we would not have to have multiple systems to implement

3.) Feasibility Analysis

A.) Technical: At all 14 destinations the process will consist of installing various equipment and tools like routers, firewall hardware, antivirus software, and other security devices. Which will take skilled technicians that understand both how to build network and establish the proper security protocols. A required skill set would be how to properly troubleshoot any issues that occur, which will undoubtedly happen at some point, even in the installation. Troubleshooting becomes essential, especially when facing issues such as device configuration errors, connectivity failures, or potential cyber threats that could turn into loss of revenue or company trust. With the current equipment that already exists at each location it is not plausible to replace all the hardware. Lack of compatibility between new equipment and existing infrastructure can lead to delays, additional costs, and overall poor time management. Broken system interfaces, external installation of antivirus software, and faulty firewalls may also lead to cyber-threats leading to sensitive information leaking and being stolen. This ultimately requires the deployment of proper management to maintain network integrity and meet cybersecurity insurance standards via our checklist. Our project’s success will depend on continuous monitoring, updating, and adherence to industry best practices to ensure long-term security and reliability.

B.) Economic: There are many costs to evaluate when it comes to installing a network and providing the proper upkeep of the security system. There are tangible and intangible costs in addition to one time and recurring fees. A one-time tangible cost will be hardware, for example our product of choice for a hardware firewall appliance the Sophos XG 116. Physical maintenance and estimated labor costs are also tangible expenses we must consider. There are also many intangible costs that we must consider for our project to properly budget. A software license would be an example of an intangible cost when accounting for expenses.

Featured below is an informal estimation of the costs that we know of at this current time. Our team would be projected to be profitable after completing this project. We would break even with the hardware costs, but we would increase profits by including an additional $20.00 fee with the subscription license to justify our time of managing those subscription licenses. We would charge a $450 flat rate fee monthly for maintenance on hardware and software that was deployed.



Item:	Cost to Us:	Cost to Customer:	One Time	Re-occuring
Sophos XG116	$919.00	$919.00	X	
Intercept X	$55.00	$75.00		X
Sophos Endpoint	$35.00	$55.00		X
Labor		$250/per hour	X	
Maintenance (updates,monitoring)		$450 per month		X

C.) The stakeholders involved in this existing system would be Tyler Carter who is the owner of the organization. He will be the one responsible for approving this project from

Hometown Pizza perspective. Beth Toombs will be ensuring our team completes the outlined services and ensuring compliance needs for Hometown Pizza are met. Tyler and Beth are both individuals from Hometown Pizza that would be able to request a change in the project or to stop the project from occurring.

Legal: NONE

Schedule: Based on the geographic locations of each branch being reasonably close to one another and since we would be preconfiguring the new firewalls before installation, we believe that a timeline of 7 - 10 business days for installation, and 2 days for configuring of the units would be feasible for comp this project. We would allow 2-4 hours for installation of the new firewalls and for any troubleshooting that may be needed. This should give us plenty of time to get 2 branch locations a day. Based on recommendations from Hometown Pizza, we would not be working on the busiest days of Thursday - Sunday. We would only be working Mondays - Wednesdays so as not to cause too much disruption to the flow of business.

4.) **<u>Management Issues</u>**

A) We have three team members each with different responsibilities all with a common goal. While working hand in hand with each other to obtain cybersecurity insurance. Alex Cook serves as the project liaison; he manages policies and compliance tasks specifically risk approach to certain procedures. We also have Aaron Caton, he is the project technician, who focuses on host and network malware protection and prevention. Organizing what products to implement. Serena Mitchell is the project manager creating deliverable layouts, meetings and sharing documents. She also specializes in server security to ensure preventive measures are in place. Our team will be working together to ensure both policy adherence and comprehensive cybersecurity measures are in place for the organization.

B.) Risks and Constraints: There are many different risks and constraints that can arise when it comes to implementing new security measures and installing new networks. There are a lot of things we must take into consideration that must align with company policies. Revenue is important for any business and our goal would be to prevent any sort of revenue loss. There is always the risk of installation errors that may cause setbacks, which would result in revenue loss. Lack of network security and errors upon installation result in cyber-attacks leading to personal information being stolen. We are also constrained to the limited configuration management team. Network security requires upkeep and managers to ensure proper system performance. Unfortunately, there is a lack of management in the department spread thin between many locations that need to be maintained. There are also scheduling conflicts and restrictions, installation must be done on either Monday - Wednesday. Hometown pizza cannot afford network down time Thursday-Sunday, because they are the busiest times. Lastly when creating a plan to adhere to the insurance policies we noticed there was a lack of an exit policy, so we are adding one to ensure there is no risk of former employees releasing personal information.

Data Collection:

We have been doing research on which products would be best suited for our client. We have been comparing Sophos against the Meraki products. We have been doing research on protection models of Sophos malware protection against less expensive products. After completing our walkthrough of Hometown Pizza, we have been developing reasons on why the current SonicWall is not feasible for Hometown Pizza. We have been using vendor websites and technology experts that have been in the field for thirty plus years. We have had a preliminary interview with Hometown Pizza to gather facts on the current network environment and the hosts' environment to identify all possible risks associated with the vulnerabilities that exist today. We will further our data collection before implementing the projected solutions.

Statement of Work Agreement

Securing Hometown Pizza

The purpose of this agreement is to ensure Hometown Pizza (client) and AAS (service provider) agree on the general outline of this project of securing Hometown Pizza. Hometown Pizza's network environment at their restaurant sites and their main office is not deemed secure. Hometown Pizza is not meeting industry standards to obtain the cybersecurity insurance they need. AAS has completed a preliminary walkthrough in which we have identified several items that need to be addressed. We have identified firewalls on site currently are not up to standard which pose a risk to the business of Hometown Pizza and the customers of Hometown Pizza. We have identified the laptops within the company do not have the necessary malware protection included on them. Lastly, we have identified the Microsoft Sever 2016 is vulnerable to threats as well. AAS aims to remedy the above items that were identified to ensure the confidentiality, integrity, and availability of Hometown Pizza's data.

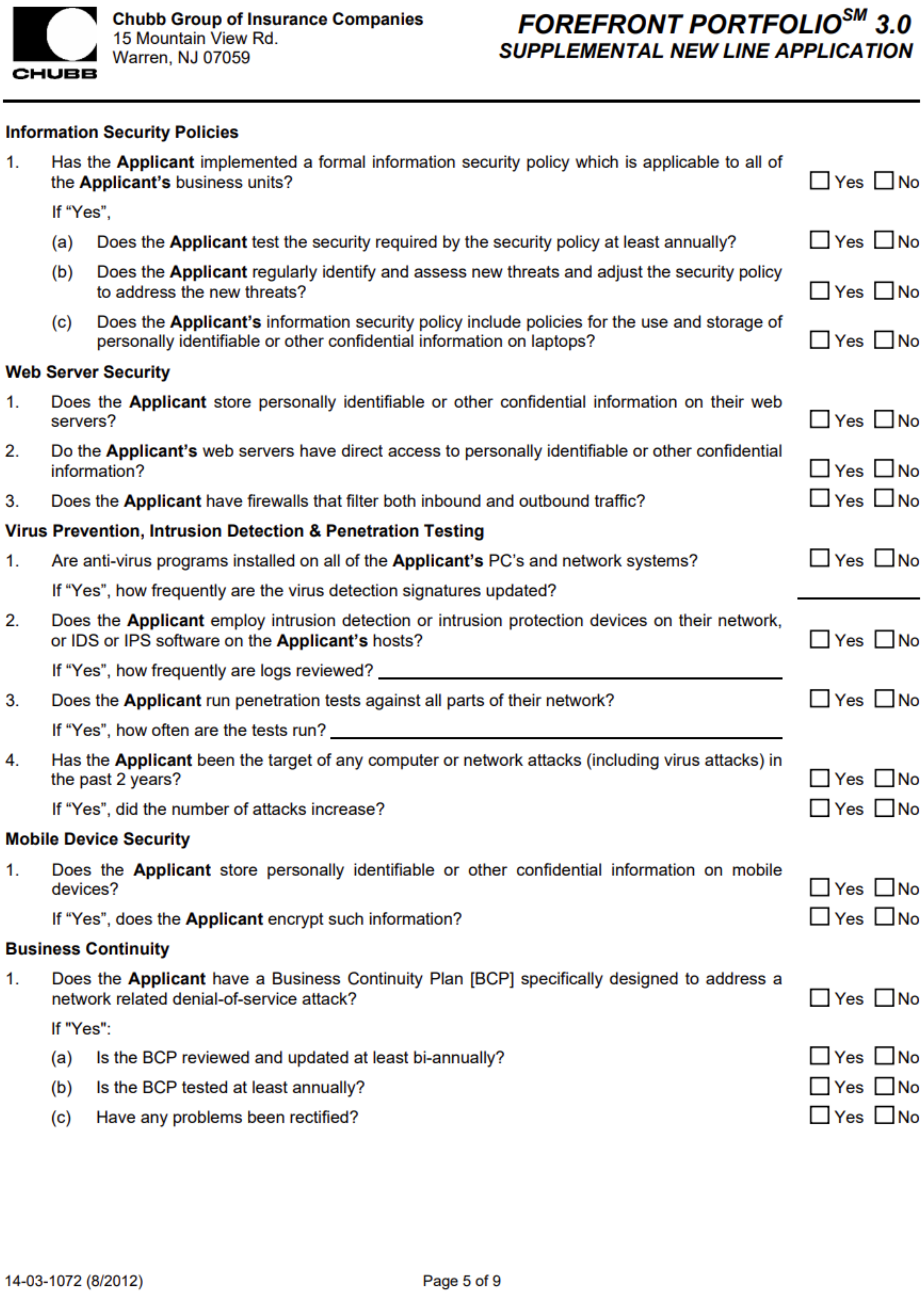
AAS will start by removing the outdated SonicWalls from the restaurant sites and replacing those with Sophos XG 116 firewall appliances. These Sophos XG 116 appliances will enhance security for each restaurant location that will mitigate cyber-attacks to the business or to the customers using the guest networks. AAS will implement malware protection on the laptop devices used by Hometown Pizza's general managers and corporate staff. AAS will also implement a product onto the Microsoft Server 2016 that will mitigate attacks on the server that would prevent loss of data, ransomware, or corruption of data that is stored on the server. AAS will also create an exit policy for the human resource department to include within Hometown Pizza's handbook that will mitigate any cyber issues related to terminated employees. After completing each of these tasks, AAS will ensure that the hardware and software necessary to perform business operations are not hindered by our solutions. AAS will conduct tests to make sure the network is performing as it should.

AAS will explore another option to solve Hometown Pizza's current problem which would be implementing a lower cost firewall and lower cost malware protection. Although, we (AAS) may deem this alternative solution not feasible to fully solving the given problem. AAS is committed to solving the problem that is best suited for Hometown Pizza.

AAS will require at least thirty minutes from the on-site general managers of each location to investigate network and laptop conditions. AAS will require thirty minutes from the corporate staff to discuss the malware protection that will be installed and how it will work. AAS will require one hour to interview Mr. Carter and Mrs. Toombs to make sure we have fully established the problem, and all have acknowledged the solutions that we aim to implement. AAS will require access to the site locations before business hours so that AAS may complete the required tasks without hindering the business from operating as normal.

After the project is completed, Hometown Pizza should be able to obtain cybersecurity insurance and Hometown Pizza should have the satisfaction of knowing their network environment is secured.

Supplemental Materials: Insurance Policy Checklist



CHUBB

Chubb Group of Insurance Companies
15 Mountain View Rd.
Warren, NJ 07059

FOREFRONT PORTFOLIO^{SM} 3.0
SUPPLEMENTAL NEW LINE APPLICATION

Information Security Policies

1. Has the **Applicant** implemented a formal information security policy which is applicable to all of the **Applicant's** business units? □ Yes □ No

   If "Yes",

   (a) Does the **Applicant** test the security required by the security policy at least annually? □ Yes □ No

   (b) Does the **Applicant** regularly identify and assess new threats and adjust the security policy to address the new threats? □ Yes □ No

   (c) Does the **Applicant's** information security policy include policies for the use and storage of personally identifiable or other confidential information on laptops? □ Yes □ No

Web Server Security

1. Does the **Applicant** store personally identifiable or other confidential information on their web servers? □ Yes □ No

2. Do the **Applicant's** web servers have direct access to personally identifiable or other confidential information? □ Yes □ No

3. Does the **Applicant** have firewalls that filter both inbound and outbound traffic? □ Yes □ No

Virus Prevention, Intrusion Detection & Penetration Testing

1. Are anti-virus programs installed on all of the **Applicant's** PC's and network systems? □ Yes □ No

   If "Yes", how frequently are the virus detection signatures updated? ____________

2. Does the **Applicant** employ intrusion detection or intrusion protection devices on their network, or IDS or IPS software on the **Applicant's** hosts? □ Yes □ No

   If "Yes", how frequently are logs reviewed? ____________

3. Does the **Applicant** run penetration tests against all parts of their network? □ Yes □ No

   If "Yes", how often are the tests run? ____________

4. Has the **Applicant** been the target of any computer or network attacks (including virus attacks) in the past 2 years? □ Yes □ No

   If "Yes", did the number of attacks increase? □ Yes □ No

Mobile Device Security

1. Does the **Applicant** store personally identifiable or other confidential information on mobile devices? □ Yes □ No

   If "Yes", does the **Applicant** encrypt such information? □ Yes □ No

Business Continuity

1. Does the **Applicant** have a Business Continuity Plan [BCP] specifically designed to address a network related denial-of-service attack? □ Yes □ No

   If "Yes":

   (a) Is the BCP reviewed and updated at least bi-annually? □ Yes □ No

   (b) Is the BCP tested at least annually? □ Yes □ No

   (c) Have any problems been rectified? □ Yes □ No

14-03-1072 (8/2012) Page 5 of 9

Security Assessments

1. Has an external system security assessment, other than vulnerability scans or penetration tests, been conducted within the past 12 months? □ Yes □ No

   If "Yes", please indicate who conducted the assessment, attach copies of the result, and indicate whether all critical recommendations been corrected or complied with.

   If "No", please attach explanation.

Backup & Archiving

1. How frequently does the **Applicant** back up electronic data? ____________________

2. Does the **Applicant** store back up electronic data with a third party service provider? □ Yes □ No

   (a) If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? □ Yes □ No

   (b) If "Yes" to 2(a), does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? □ Yes □ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? □ Yes □ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? □ Yes □ No

Service Providers

1. Does the **Applicant** use third-party technology service providers? □ Yes □ No

   (a) If "Yes", does the **Applicant** have a written contract with the respective service provider(s)? □ Yes □ No

   (b) If "Yes" to 1(a), does the **Applicant's** contract with the service provider(s) state that the service provider:

   i) Has primary responsibility for the security of the **Applicant's** information? □ Yes □ No

   ii) Have a contractual responsibility for any losses or expenses associated with any failure to safeguard the **Applicant's** electronic data? □ Yes □ No

   iii) Does the **Applicant** review their most recent information security audit (i.e. SAS 70)? □ Yes □ No

Incident Response Plans

1. Does the **Applicant** have a formal incident response plan that addresses network security incidents or threats? □ Yes □ No

Security Incident And Loss History:

1. Has the **Applicant** had any computer or network security incidents during the past two years? Incident includes any unauthorized access or exceeding authorized access to any computer, system, data base or data; intrusion or attack; the denial of use of any computer or system; intentional disruption, corruption or destruction of electronic data, programs or applications; or any other incidents similar to the foregoing? □ Yes □ No

   Note: if the answer to this Question 1 is "Yes", please attach a complete description of the incident(s), including whether the ***Applicant*** *reported the incident(s) to law enforcement and/or the* ***Applicant's*** *insurance carrier.*

References

Ogden, Jacqueline von. “Top 5 Network Security Risks and Threats.” *Www.cimcor.com*, 19 Jan. 2023, www.cimcor.com/blog/top-5-network-security-risks-and-threats.

“RHINO.” *Rhinonetworks*, www.rhinonetworks.com/product/device/meraki-mx68.

Sophos. “Sophos Intercept X Endpoint Protection.” *SOPHOS*, www.sophos.com/en-us/products/endpoint-antivirus.

“Workload Protection Specifications - Sophos Server Security.” *SOPHOS*, 2024, www.sophos.com/en-us/products/server-security/tech-specs. Accessed 29 Sept. 2024.

Appendix C

Deliverable 3: “Structured Requirements”

Aaron Caton, Alex Cook, Serena Mitchell

Narrative

The current system needs upgrading because the sonic walls that are in place are no longer supported, they do not receive regular updates, and they do not meet the needs of the insurance check list. The firewall also does not adequately monitor traffic as well as the company wants. Since the firewalls are no longer supported, they no longer receive regular signature updates to protect from the latest malware and other forms of attack.

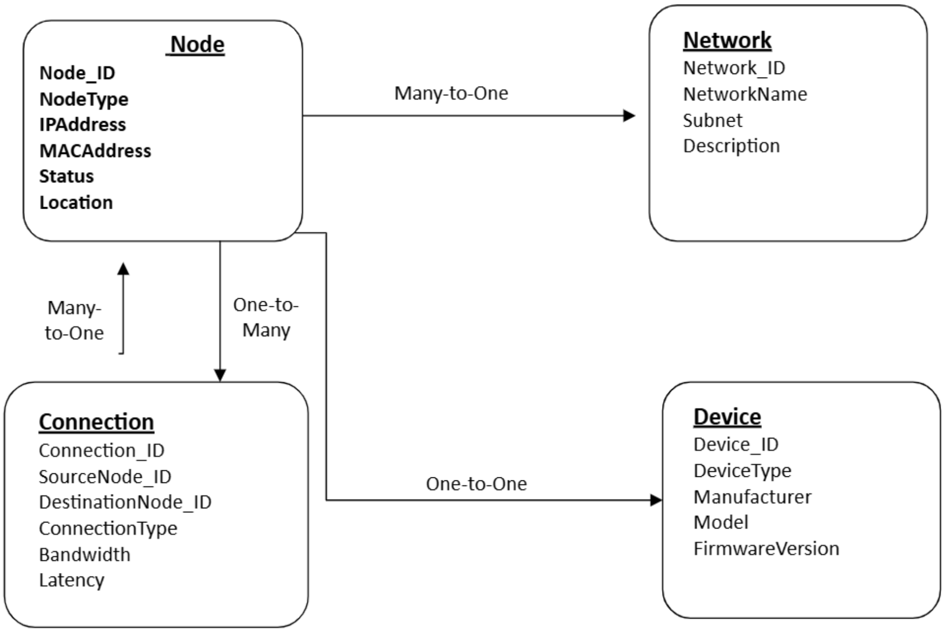
Each location has its own sonic wall that all the local traffic passes through. Such traffic includes customer's personal information such as names, addresses, phone numbers, and even credit card transactions. Users such as cashiers will regularly run transactions through the credit card machine and that traffic travels over a peer-to-peer encrypted tunnel to the transaction company.

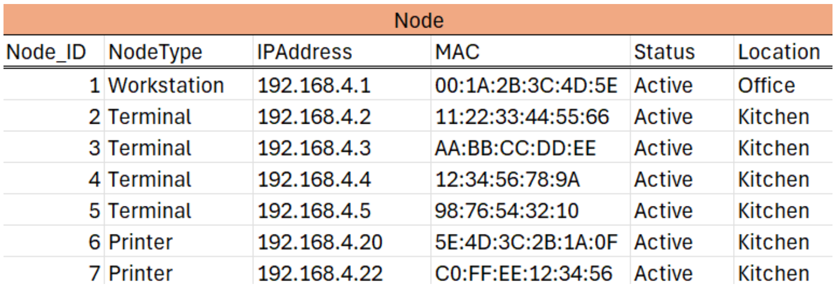
As for the removal of employee access to systems and physical access, there is no formal check list for what systems employees have access to. With no formal checklist, it could be easy to overlook or forget miss removing access to critical systems for departing employees.

The current corporate file server is locally hosted with bare minimum-security provisions. It is sitting behind the firewall and only has LAN access, but an attacker could still get to it. It was said to be pretty much wide open according to the IT admin. The Microsoft Server 2016 does not have malware protection in place and does not have regularly scheduled backups. Users of the file server store various files and business-related data on the server, but there is no customer data stored there.

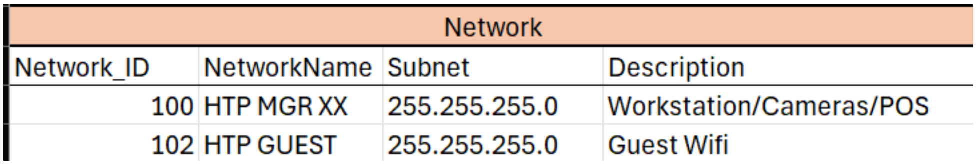
The Microsoft Server 2016 is not in the most practical physical environment either. It is in a closed closet that does not have any air flow, and the closet does not have a physical lock. Hometown Pizza needs a security upgrade regarding virus prevention, intrusion detection & penetration testing on hosts and network. Hometown Pizza also needs an exit policy created to ensure the confidentiality, integrity, and availability of their data.

Original Data Modeling

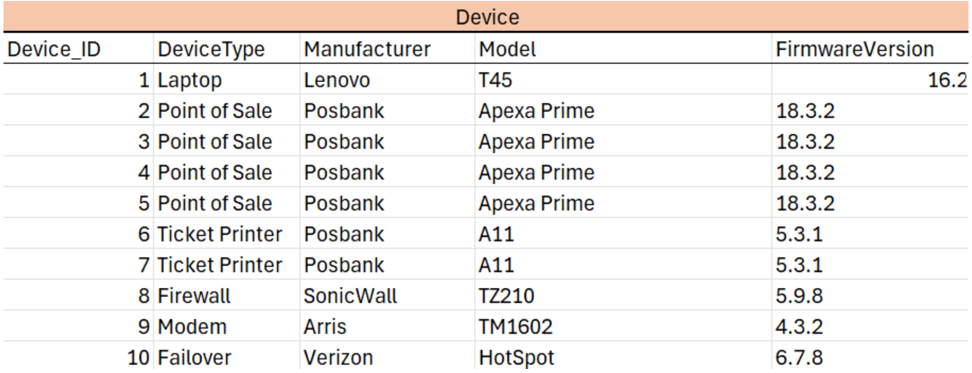




Node					
Node_ID	NodeType	IPAddress	MAC	Status	Location
1	Workstation	192.168.4.1	00:1A:2B:3C:4D:5E	Active	Office
2	Terminal	192.168.4.2	11:22:33:44:55:66	Active	Kitchen
3	Terminal	192.168.4.3	AA:BB:CC:DD:EE	Active	Kitchen
4	Terminal	192.168.4.4	12:34:56:78:9A	Active	Kitchen
5	Terminal	192.168.4.5	98:76:54:32:10	Active	Kitchen
6	Printer	192.168.4.20	5E:4D:3C:2B:1A:0F	Active	Kitchen
7	Printer	192.168.4.22	C0:FF:EE:12:34:56	Active	Kitchen



Network			
Network_ID	NetworkName	Subnet	Description
100	HTP MGR XX	255.255.255.0	Workstation/Cameras/POS
102	HTP GUEST	255.255.255.0	Guest Wifi

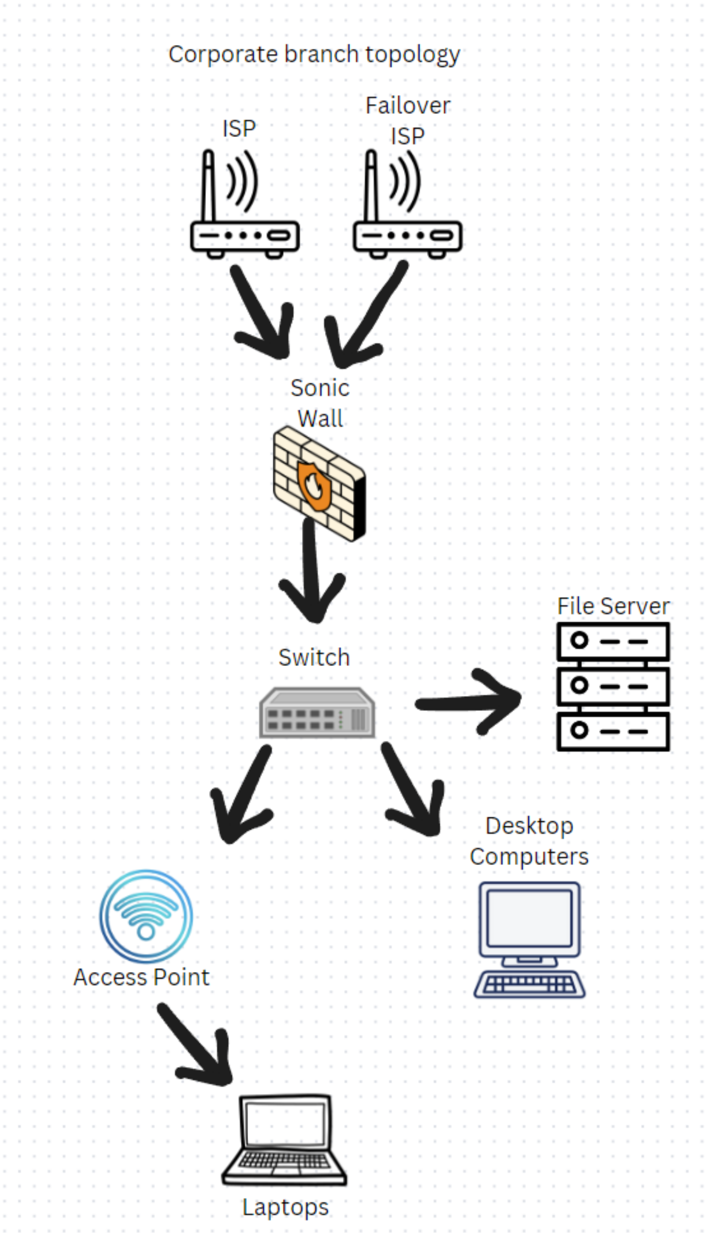


Device				
Device_ID	DeviceType	Manufacturer	Model	FirmwareVersion
1	Laptop	Lenovo	T45	16.2
2	Point of Sale	Posbank	Apexa Prime	18.3.2
3	Point of Sale	Posbank	Apexa Prime	18.3.2
4	Point of Sale	Posbank	Apexa Prime	18.3.2
5	Point of Sale	Posbank	Apexa Prime	18.3.2
6	Ticket Printer	Posbank	A11	5.3.1
7	Ticket Printer	Posbank	A11	5.3.1
8	Firewall	SonicWall	TZ210	5.9.8
9	Modem	Arris	TM1602	4.3.2
10	Failover	Verizon	HotSpot	6.7.8

Connection: The connections change and would have to be documented for a specific instance in time.

Within the Data Models we identified all the entity types labeling and establishing relationships. Each entity has unique attributes separating them from the rest and creating different types of relationships between different entities. Then we studied and labeled the nature of each relationship within the data model. All creating different cardinality for example, Many-To-One in our model from Nodes to Network. Another example being Node to Device being a one-to-one relationship. Above you see our Data Model with additional context provided.

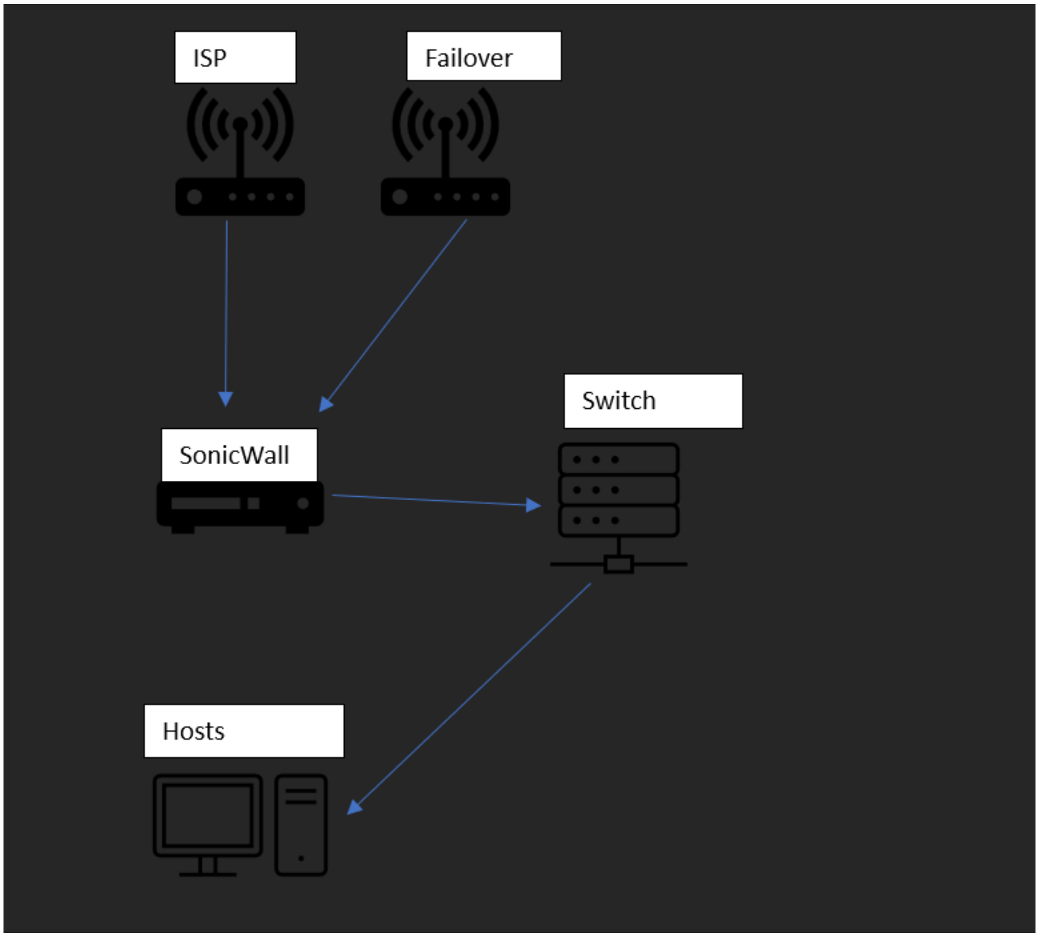
Process Modeling



Each device on the corporate network currently sends traffic from their device through the switches, through the firewall, then out to the internet. Any inbound and outbound traffic is monitored, but the monitoring leaves a lot to be desired since the current firewall is out of date.

The file server can be accessed by any device on the corporate network, and it does not have any special security to prevent any user from being able to access files on the server. It is not an online server, so that makes it somewhat more secure, but with there being little to no security on the server itself, an attacker could still hijack a local machine and access whatever files they wanted.

Branch Network Topology



Currently the point-of-sale equipment piggy backs off the desktop computer's internet connection and sends all transaction data over a peer-to-peer encrypted tunnel to the transaction company. All other devices send their data through the network, out the firewall, and out to the internet. The issue with the current firewall is that it is out of date and needs to be upgraded to a new, updated firewall that is up to date with current viruses and attack signatures.

Logic Modeling

Original Structured English

IF incoming traffic detected

THEN go to step 2

ELSE no action needed

IF source IP or device identified

THEN go to step 3

ELSE unknown traffic poses high risk

IF source IP from known, trusted entity

THEN go to step 4

ELSE untrusted source may indicate malicious intent

IF traffic type is legitimate

THEN go to step 5

ELSE unrecognized traffic type may indicate a security threat

IF traffic intended for specific service/application

THEN go to step 6

ELSE unexpected traffic may indicate unauthorized access attempts

IF traffic behavior normal (consistent patterns)

THEN allow and monitor

ELSE anomalous behavior could signal a breach or attack

IF existing security controls in place

THEN all set

ELSE lack of security measures exposes network to attacks

IF record of incoming traffic and actions taken

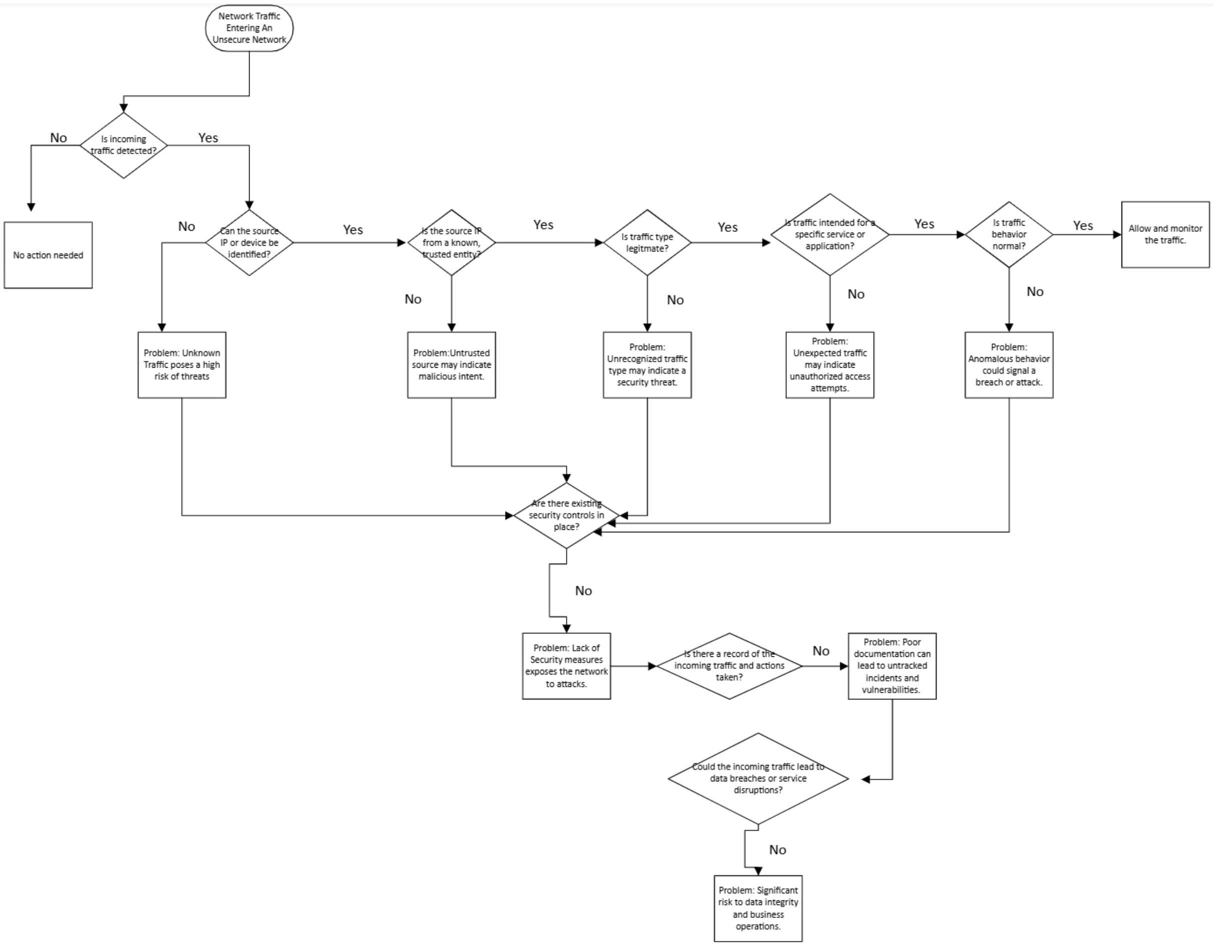
THEN you will have documentation

ELSE poor documentation can lead to untracked incidents and vulnerabilities

IF incoming traffic could lead to data breaches

THEN significant risk to data integrity and business operations

Original Activity Diagram


Network Traffic Entering An Unsecure Network
No
Is incoming traffic detected?
Yes
No action needed
No
Can the source IP or device be identified?
Yes
Is the source IP from a known, trusted entity?
Yes
Is traffic type legitmate?
Yes
Is traffic intended for a specific service or application?
Yes
Is traffic behavior normal?
Yes
Allow and monitor the traffic.
No
No
No
No
Problem: Unknown Traffic poses a high risk of threats
Problem:Untrusted source may indicate malicious intent.
Problem: Unrecognized traffic type may indicate a security threat.
Problem: Unexpected traffic may indicate unauthorized access attempts.
Problem: Anomalous behavior could signal a breach or attack.
Are there existing security controls in place?
No
Problem: Lack of Security measures exposes the network to attacks.
Is there a record of the incoming traffic and actions taken?
No
Problem: Poor documentation can lead to untracked incidents and vulnerabilities.
Could the incoming traffic lead to data breaches or service disruptions?
No
Problem: Significant risk to data integrity and business operations.

Case Scenario Table

Condition / Scenario	Action / Outcome	Problem Identified
1. Incoming traffic detected?	Yes → Go to step 2	
	No → No action needed	
2. Source IP or device identified?	Yes → Go to step 3	
	No	**Problem:** Unknown traffic poses high risk
3. Source IP from known, trusted entity?	Yes → Go to step 4	
	No	**Problem:** Untrusted source may indicate malicious intent
4. Traffic type legitimate?	Yes → Go to step 5	
	No	**Problem:** Unrecognized traffic type may indicate a security threat
5. Traffic intended for specific service/application?	Yes → Go to step 6	
	No	**Problem:** Unexpected traffic may indicate unauthorized access attempts
6. Traffic behavior normal (consistent patterns)?	Yes → Allow and monitor	
	No	**Problem:** Anomalous behavior could signal a breach or attack
7. Existing security controls in place?	Yes	
	No	**Problem:** Lack of security measures exposes network to attacks
8. Record of incoming traffic and actions taken?	Yes	
	No	**Problem:** Poor documentation can lead to untracked incidents and vulnerabilities
9. Incoming traffic could lead to data breaches?	Yes	**Problem:** Significant risk to data integrity and business operations

In our logic model, we wanted to show the problems that could occur when network traffic enters an unsecure network environment. We also wanted to depict the steps to take to examine the network traffic entering the network environment.

Revisiting alternatives

An alternative solution to improve the network security of Hometown pizza is to omit the use of a physical hardware firewall. We propose utilizing cloud-native solutions and effective network segmentation strategies. They both have their cons, but they provide a very different route that has advantages over traditional hardware firewalls like our original Sophos. Our Sophos requires physical installation and management, cloud firewalls provide flexibility with different points of failure, as they can be managed together and identify threats.

There are benefits to using a cloud-based network firewall, they offer unique forms of management that cannot be offered by a physical firewall. Cloud-based firewalls have more utilization tools like inspecting traffic in real time. They allow for centralized control with full visibility and automatic updates, reducing maintenance. "Administrators can define and enforce consistent security rules across multiple cloud instances, regions, or even different cloud providers" (Convergence) There being many locations a cloud-based solution will ensure reliable security while making it easier to manage with different cloud instances. With room to grow because cloud-based firewalls provide scalability to meet any sort of business needs in the future.

In addition to a cloud-based firewall we have the option to segment each network which enhances security by dividing it into smaller, manageable sections, which limit potential threats that could cause greater harm to a central network. This approach reduces the scale of the attack point and makes it easier to monitor and respond to security threats, ultimately strengthening the overall network by importantly isolating the point of attack.

We turned to look at the healthcare industry and how their network systems practice network segmentation to protect all sorts of sensitive data. We learned that "... medical devices, which are often targets for cyber-attacks due to their outdated software, can be isolated on a specific segment" (Hewitt) It is incredibly important to isolate any point of a potential threat. The separation or isolation of the device protects the rest of the network if there is a compromise.

There are many benefits to network segmentation, and it is useful to truly optimize network security. What makes Network Segmentation effective is dividing the network into smaller parts, isolating the point of attacks and improving performance. Limiting breaches reaching other devices, reduces network traffic, and allows for easy management of security measures. In conclusion Segmentation creates a secure network that is effective and well optimized enhancing security a step further.

References

Convergence, I. T. "Cloud Firewall Advantages & Disadvantages | Importance of Firewalling." *IT Convergence*, 12 July 2023, www.itconvergence.com/blog/building-a-secure-perimeter-the-importance-of-firewalling-in-cloud-managed-services/.

Hewitt, Nik. "The Benefits of Network Segmentation • TrueFort." *TrueFort*, 22 May 2023, truefort.com/network-segmentation-benefits/.

Appendix D

Deliverable 4: “Systems Proposal”

Aaron Caton, Alex Cook, Serena Mitchell

Section I: Introduction

Project Overview:

Target Organization

Our target organization is the company Hometown Pizza with its fourteen different locations including the corporate headquarters. Currently each branch has its own network that is independent from corporate and each other branch. Each site has its own network infrastructure that consists of switches, access points, and its own firewall. The network also contains devices such as laptops and point of sale systems that need to be brought to an appropriate standard to fulfill insurance requirements. Data storage is handled by an outdated, unsecured 2016 Microsoft server for shared files that is not properly managed or configured with any security in mind.

Problem statement

Currently Hometown Pizza is seeking to acquire cyber insurance through Chubb but does not meet all the necessary requirements to be approved. The three issues we are trying to address is the need for a new firewall for each of the fourteen branch locations, securing the company’s file server, and implementing an official employee exit policy to ensure employees network and service account access is taken away immediately to ensure disgruntled employees can’t affect the company’s network or services after being let go.

The current Microsoft Server 2016 file server has no existing malware security, which leaves it wide open for attack if someone were to breach the network. This is coupled with the fact that the existing SonicWall firewall is completely outdated and no longer getting new signature updates, is out of warranty, and has very little support if any since it is so old.

Finally, there currently is no existing formal employee exit policy for employees who leave or are terminated. With no exit policy or guideline in place, it can be easy to miss what services or account each employee would have access to. This is important because if an employee's account access is not terminated when the employee leaves, they could use that access to negatively affect business functions if they wanted to.

Scope statement

Hometown Pizza is vulnerable to losing confidentiality, integrity, revenue, and more due to unsafe network environments. There are fourteen locations that need improved network security because any sort of attack can stop Hometown Pizza from conducting sales. One of the biggest threats network attacks poses is significant loss of revenue. These network attacks could take out their point-of-sale system that accepts payments from customers, cut off the VOIP phones that are used to receive customer orders, or interrupt critical daily tasks at the corporate office. Employees and customers' personal information is at risk and can even be held ransom due to the companies lack security measures. Taking the proper security measures is crucial to prevent the devastating attacks that could develop. Our team has conducted a plan to implement solutions before business hours to reduce downtown for the business, employees, and customers.

Recommendation:

The final recommended solution would be to install SOPHOS NextGen 116 at all the branch locations. This would provide a physical firewall that is up to date with the necessary functions to keep Hometown Pizza's network environment secure. We decided against the network segmentation because Hometown Pizza would still be using the outdated SonicWall that had an end-of-life support date of July 2017. We decided against the cloud-based firewall because the client preferred a physical device to keep their network secure.

For file security, we will be using SOPHOS's Intercept X for Servers to keep their file server secure. This software will provide network protection including ransomware file protection. This software will also provide live protected backups as Hometown Pizza is currently not conducting backups. We did not have an alternative solution to this issue because the Sophos Intercept X would work in conjunction with our selection of the Sophos firewall system, whereas other solutions may not.

We will be creating an exit policy for the company's HR team to prevent any malicious attacks by terminated employees. Since this has been an issue in the past, we figured there needed to be a formal policy that included a list of services and accounts any given role would have access to. Hometown Pizza does not currently have an exit policy which opens the door to many issues that could impact Hometown Pizza technologically and legally. There is not an alternative solution for this issue, either.

We believe our solution is technologically sound, economically rewarding for us and the client, and we believe that the stakeholders will agree with our recommended solution. Our final recommendation will provide the technical upgrade that Hometown Pizza needs to secure cybersecurity insurance.

Section II: System Description

Requirements and Constraints:

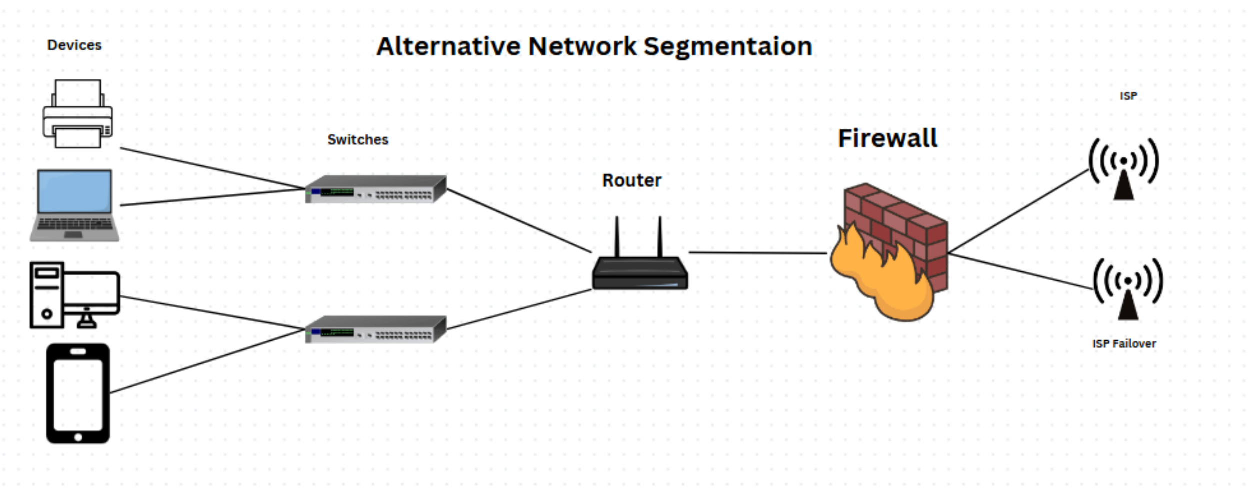
- **Requirements:**
    - New firewall - The new Sophos firewall will need to replace the old SonicWall firewall that is not secure. The old firewall is outdated, no longer supported, no longer receives regular signature updates, and it does not monitor traffic as well as the customer would like. The Sophos firewall system meets all of these requirements and is within the customer's budget.
    - File server security – The current file server has little to no security, which leaves it vulnerable to attack from multiple vectors. SOPHOS's Intercept X Advanced for Server will add a sufficient security level between the file server and the internet to prevent bad actors from being able to access it. Should we mention something about limiting the file server to only having specific users allowed to access the file server?
    - HR exit policy – Currently there is no formal exit policy for employees who leave the company or are terminated. There has been an issue in the past where a disgruntled employee was able to mess with the network due to still having access. We plan to implement an exit policy that will include job descriptions along with a list of IT-related services those positions have access to as well as

access control related resources. This will streamline the process of removing unwanted access to employees who are no longer employed and ensure that no accounts or permissions are missed when removing access to said employee.

- **Constraints:**
    - Budget – The customer does have the money necessary to procure the necessary equipment and necessary licenses required to operate the new Sophos system and facilitate installation requirements. The budget is limited so any major issues that would require extra time for configurations, troubleshooting, or installation may result in going over budget.
    - Installation times – It was made known to us that the window of time we have to do installations is limited to Mondays – Wednesday. Thursdays – Sundays are off limits due to possible major loss of income since those days are the busiest time of the week. This is not ideal since it prolongs the installation time significantly because we lose 2 or 3 days a week since working Saturdays would be considered for installation.
    - Physical distance between locations – Each location is anywhere from 30 – 40 minutes apart from one another. While it is not a major constraint, travel can be considered since we would have to drive to the first location from where we would be based out of and then to the next location afterward if you could do 2 locations per day. This could add up to close to 2 hours of travel per day.

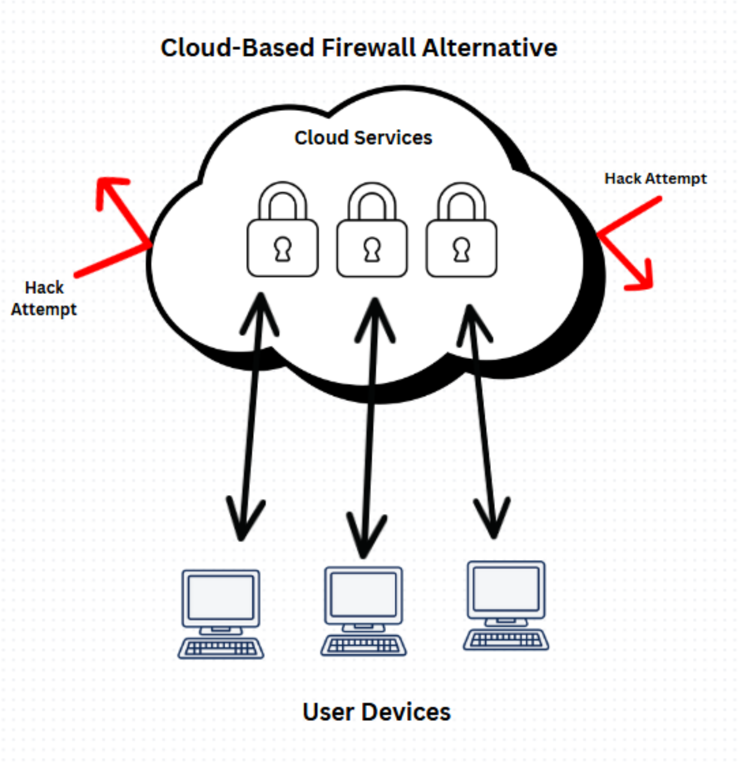
Model Descriptions of the Alternative(s):

Proposed Alternatives



Network Segmentation Alternative

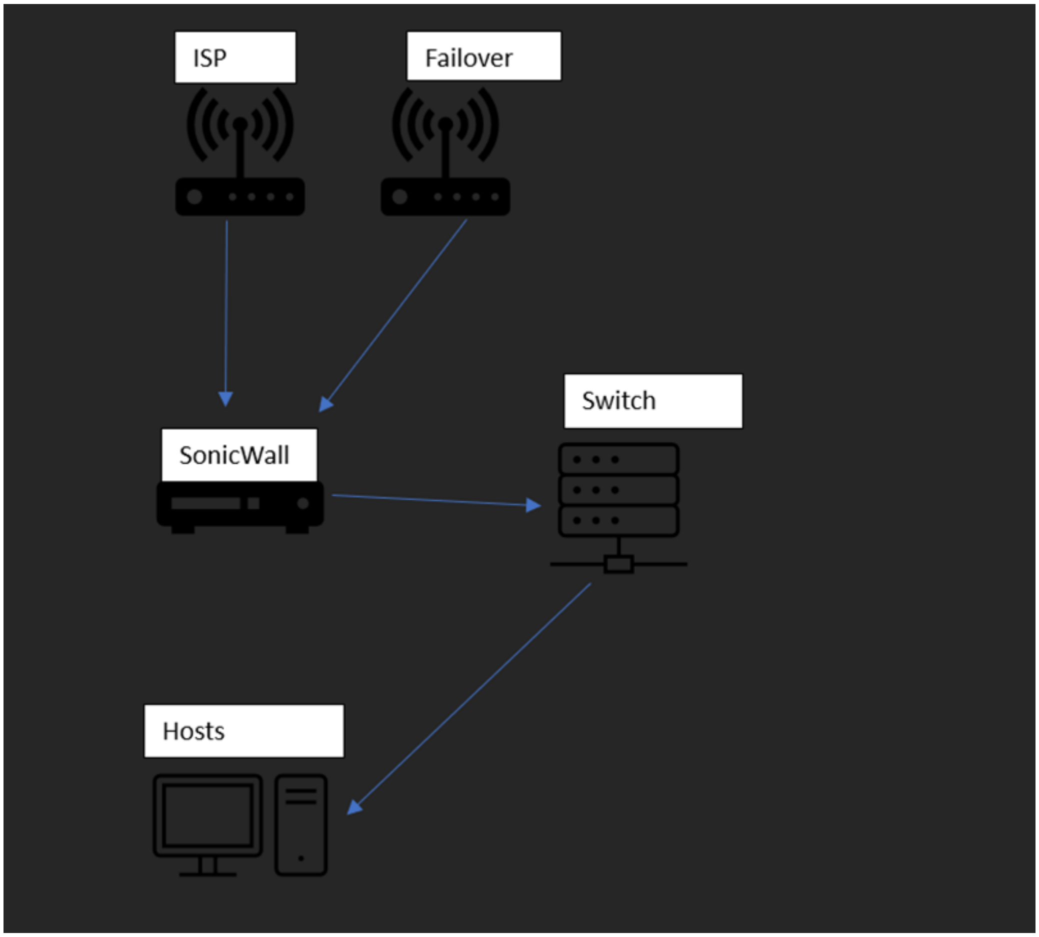
The original Hometown pizza network is under a single network where all devices such as computers, laptops, smartphones, and printers are all within the same Network. This leaves the original network vulnerable to congestion due to network traffic and vulnerable to many security threats. The segmented network divides the larger network into many different points, cutting the network in half and improving overall performance. Manageable access between segments also makes it easier to troubleshoot by eliminating variables for network issues. This means segmented networks are also easier to manage allowing for more specific actions or details for control over the network at each level. While a normal network is simpler and cheaper to set up, a segmented network offers greater scalability and protection. Making it more ideal for larger organizations or networks with higher security and performance needs to be implemented. Which would be essential for hometown pizza if they wanted to scale their business further, allowing us to plan for their future which would an alternative installation process.



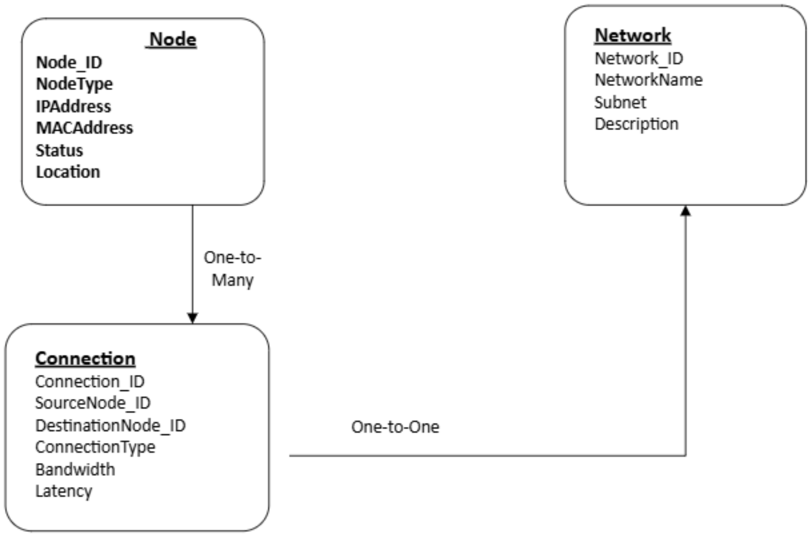
Cloud-Based Firewall Alternative

Another alternative solution would be to use a cloud-based firewall instead of using a physical firewall. This could reduce the physical space needed within the server rack, and it could reduce the amount of heat being conducted by the appliances. In addition, the cloud-based firewall would allow access to administration without having to remote into the location’s network or being on-site. The downside is that it would be 100% online, so if the provider went offline, you would not be able to access your firewall whereas a physical firewall you would not have that issue. The technicality of the cloud-based firewall would be the same as a physical firewall, so we will be considering it as an alternative.

Current Topology:

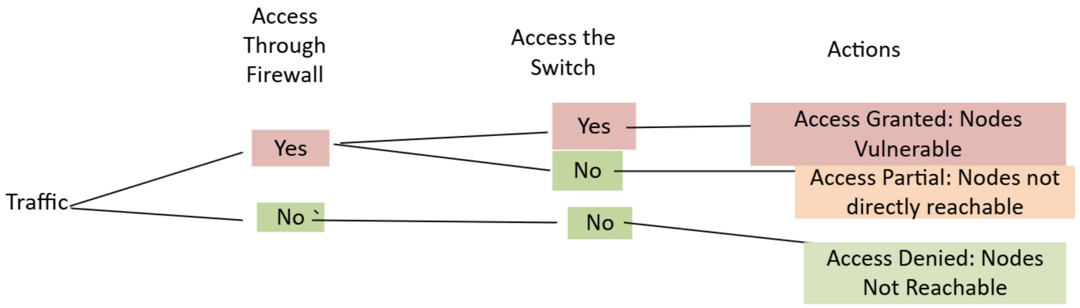


Data Modeling



The node would be the main entity in this diagram. The node creates connections to communicate. Those connections are communicated through a particular network. The node can have various connections at one time, but the connections can only be on one network at a time.

Decision Tree 1:



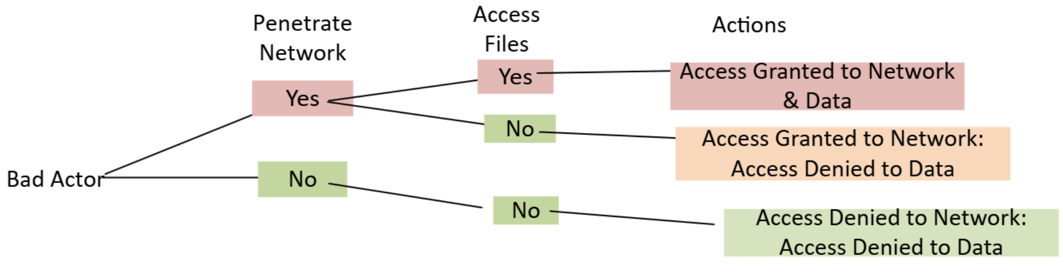
This decision table shows the traffic's ability to gain access to nodes within the network. If the traffic can make access through the firewall, then the traffic meets another decision. It will need to access the switch to directly access the nodes. If the traffic cannot make access through the firewall, then it will be unable to access the switch. Today, the traffic can access through the firewall and the switch.

Decision Table 1:

	Rules		
Conditions and Actions	1	2	3
Access Through Firewall	Y	Y	N
Access Through Switch	Y	N	N
Access Granted: Nodes Vulnerable	X		
Access Partial: Nodes not directly reachable		X	
Access Denied: Nodes Not Reachable			X

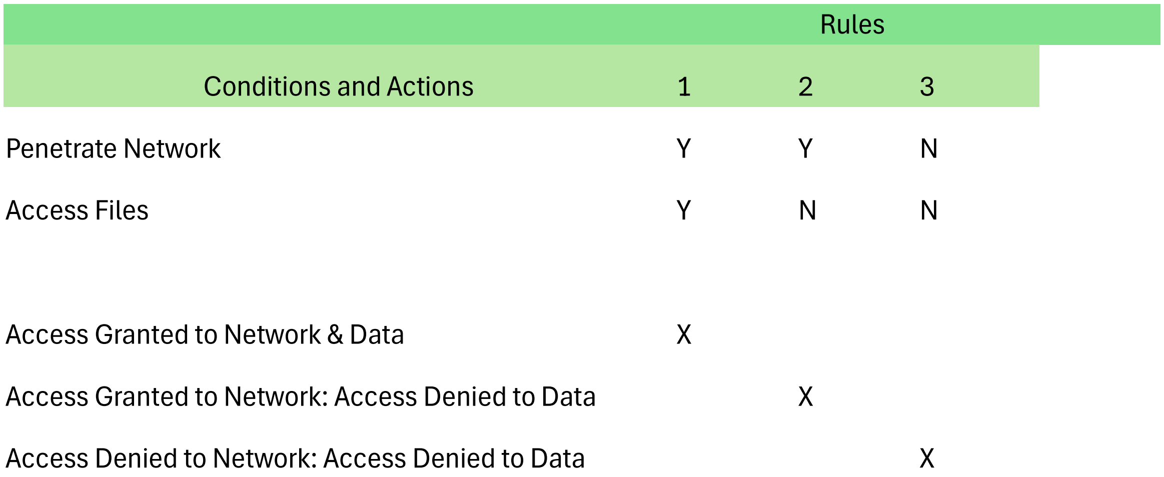
The decision table shows the decision tree, but within table form.

Decision Tree 2:


Penetrate Network
Access Files
Actions
Bad Actor
Yes
No
Yes
No
No
Access Granted to Network & Data
Access Granted to Network: Access Denied to Data
Access Denied to Network: Access Denied to Data

This decision tree shows the process of a bad actor penetrating the network and accessing files. If the bad actor can penetrate the network, then the bad actor may or may not have access to the files. If the bad actor cannot penetrate the network, then it cannot access the files, and the network is still secure. Today, the bad actor can penetrate the network and access files.

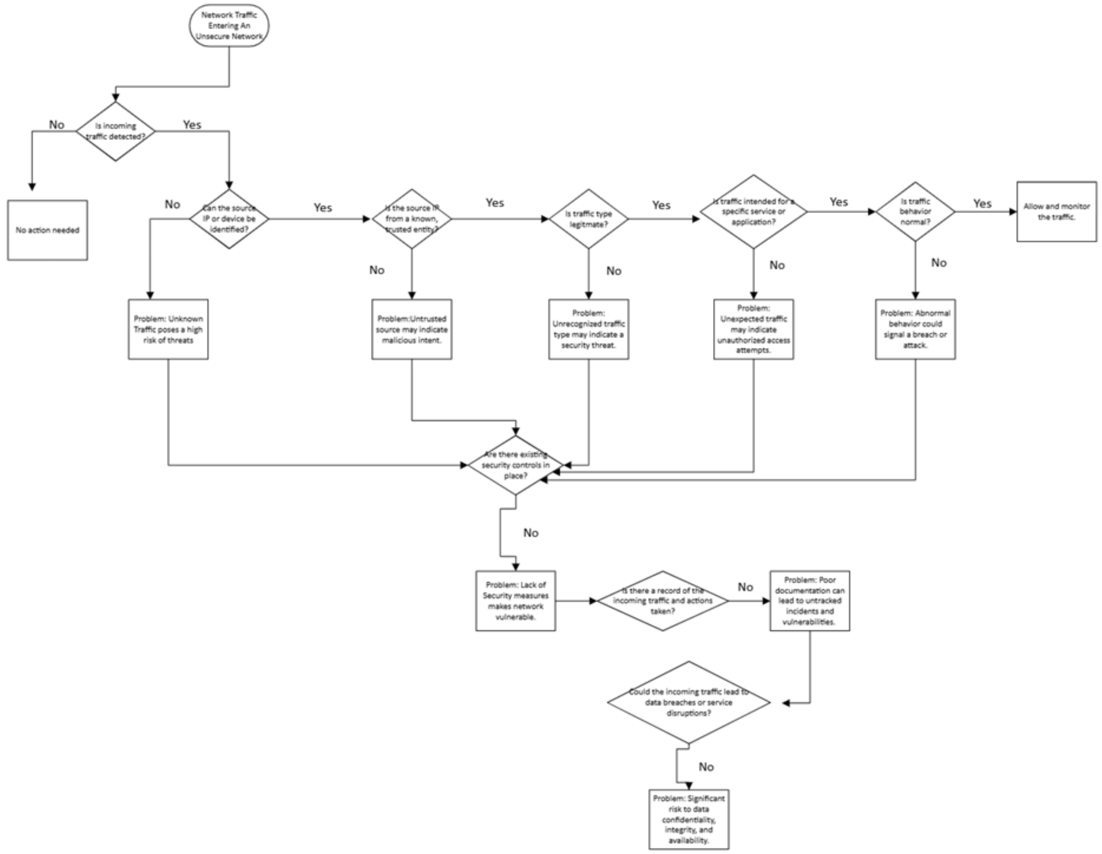
Decision Table 2:



	Rules		
Conditions and Actions	1	2	3
Penetrate Network	Y	Y	N
Access Files	Y	N	N
Access Granted to Network & Data	X		
Access Granted to Network: Access Denied to Data		X	
Access Denied to Network: Access Denied to Data			X

The decision table shows the decision tree, but within table form.

Original Activity Diagram:


Network Traffic Entering An Unsecure Network
No
Is incoming traffic detected?
Yes
No action needed
No
Can the source IP or device be identified?
Yes
Is the source IP from a known, trusted entity?
Yes
Is traffic type legitmate?
Yes
Is traffic intended for a specific service or application?
Yes
Is traffic behavior normal?
Yes
Allow and monitor the traffic.
No
No
No
No
Problem: Unknown Traffic poses a high risk of threats
Problem:Untrusted source may indicate malicious intent.
Problem: Unrecognized traffic type may indicate a security threat.
Problem: Unexpected traffic may indicate unauthorized access attempts.
Problem: Abnormal behavior could signal a breach or attack.
Are there existing security controls in place?
No
Problem: Lack of Security measures makes network vulnerable.
Is there a record of the incoming traffic and actions taken?
No
Problem: Poor documentation can lead to untracked incidents and vulnerabilities.
Could the incoming traffic lead to data breaches or service disruptions?
No
Problem: Significant risk to data confidentiality, integrity, and availability.

The activity diagram shows how network traffic would process through the network environment. Right now, the client answers “no” to most of these questions. This creates a concern for us. The source IP is identified, but it does not know if it can be trusted. The current firewall is allowing all traffic through regardless of the source IP. The same is true for outbound traffic; the firewall is pushing through any data regardless of the source IP. It may not be a trusted source IP that is allowed to be sending communications through Hometown Pizza’s firewall. The firewall is unable to determine if the traffic is legitimate, or and it is unable to determine if it is normal behavior. The current firewall is essentially acting just as a router.

Case Scenario:

Condition / Scenario	Action / Outcome	Problem Identified
1. Incoming traffic detected?	Yes → Go to step 2	
	No → No action needed	
2. Source IP or device identified?	Yes → Go to step 3	
	No	**Problem:** Unknown traffic poses high risk
3. Source IP from known, trusted entity?	Yes → Go to step 4	
	No	**Problem:** Untrusted source may indicate malicious intent
4. Traffic type legitimate?	Yes → Go to step 5	
	No	**Problem:** Unrecognized traffic type may indicate a security threat
5. Traffic intended for specific service/application?	Yes → Go to step 6	
	No	**Problem:** Unexpected traffic may indicate unauthorized access attempts
6. Traffic behavior normal (consistent patterns)?	Yes → Allow and monitor	
	No	**Problem:** Abnormal behavior could signal a breach or attack
7. Existing security controls in place?	Yes	
	No	**Problem:** Lack of security measures makes network vulnerable
8. Record of incoming traffic and actions taken?	Yes	
	No	**Problem:** Poor documentation can lead to untracked incidents and vulnerabilities
9. Incoming traffic could lead to data breaches?	Yes	**Problem:** Significant risk to data confidentiality, integrity, and availability

This is a case scenario table that describes our activity diagram.