

The implementation of a physical firewall within a network, and a network proposal from a given scenario.

Matthew Cragg
Cyber Security and Networking (of MSc Year 1)
Network Security
University of Wales Trinity St.Davids
Swansea, Wales
Student ID 2207432

	CONTENTS		7	Gantt chart tasks and timeline for the A2Z Technologies Ltd project.	7
I	Part One	2			
	I-A Introduction	2			
	I-B Frameworks	2			
	I-B1 Management Plane	3			
	I-B2 Control Plane	3			
	I-B3 Data Plane	3			
	I-C Tools, Firewalls and other devices.	3			
	I-D Network Security	3			
	I-D1 Network Security Testing	3			
	I-D2 Security	4			
	I-E VPN	4			
	I-F Encryption	5			
II	Part Two.	5			
	II-A Proposed Topology	5			
	II-A1 Security Measures	6			
	II-B Cost	6			
	II-C Time of Implementation	6			
	II-D Potential Attacks	6			
	II-E Testing of systems	7			
	II-F Invoice	8			
III	Terminology	8			
IV	Reference List	8			
	LIST OF FIGURES				
1	A diagram listing the five core elements of the NIST framework [1].	2			
2	An example of a firewall being used within a network, created with Packet Tracer.	3			
3	A packet analyser capturing packets being sent to and from a machine. Captured within Wireshark.	4			
4	Proposed topology for A2Z Technologies Ltd.	5			
5	Gantt chart tasks and timeline for the A2Z Technologies Ltd project.	7	8	Example of ASA Firewall commands to prevent DDoS attacks [2].	7
6	Gantt chart tasks and timeline for the A2Z Technologies Ltd project.	7			

Abstract—Security breaches have been detrimental to modern companies, both in the software business and elsewhere. Therefore, it has become vital for companies to focus on building their whole company with security in focus. Some even go as far as having an on-site security team that can monitor and react to any potential risks. The backbone of any modern company is the network that it operates upon, incorporating many technologies, protocols and concepts to ensure their company remains as secure as possible. In a real environment, a network would consist of routers, switches, firewalls, servers of different kinds and many other technologies. This paper will focus on the concept of a physical firewall, and it's effects on a network and how it can assist in securing the network.

I. PART ONE

A. Introduction

The largest risk a company can face in the modern day is a security breach within their network infrastructure. Attacks of this kind come in many various forms, ranging from malware to internal breaches, but all have the same intention monetary gain. These attacks can be so common, that several frameworks and models have been developed to ensure that engineers and employees are aware of the risks.

B. Frameworks

An example would be the OWASP model. According to Kiruba et al in the paper 'OWASP Attack Prevention', 'OWASP has listed the top 10 vulnerabilities for website users since 2003, and the list changes year to year' [3]. This ensures that the list is always relevant and out-of-date attacks are no longer listed (Though they are still equally as dangerous).

The 2022 OWASP list currently consists of the following risks.

- XSS Injection.
- Broken Authentication.
- XSE.
- Broken Access Control.
- Insecure Deserialization.
- Insufficient logging and monitoring.
- Security misconfiguration.

While these risks may focus upon the software development side of potential risks, they still are relevant to a network security team as any of these risks may impact and eventually allow an attacker to penetrate and gain access to the network.

The cybersecurity side of network safety has its own framework, named the 'NIST Framework'. This framework is split into five parts, each one focusing on appropriate safeguards that must be in place, and how to react if an attack was launched. The NIST framework can be viewed in figure 1, page 2.

Regardless of how well the NIST framework or any other framework has been implemented into a company policies, a dedicated attacker will find a way of penetrating the defences to launch an attack. The most common forms of network security risks are as follows.

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Fig. 1. A diagram listing the five core elements of the NIST framework [1].

- Internal Security Threats - This threat comes from the form of the employees. Current, past or external contractors all fall under this term, as they all pose a threat when exposed to sensitive information or access to data.
- DDoS Attacks - This type of attacks comes in the form of network traffic being sent to a router, firewall or computer. This traffic data, or a packet, may arrive incomplete and in large quantities, resulting in the effected device unable to process the data. This will create a queue of traffic as it attempts to process the attack.
- Malware - Malware is the common type of virus, though there are many subcategories. Malware may appear in the form of a RAT, where someone is able to access the injected computer remotely, copy all of the data from a machine, erase all data from a machine, or gain access to the network system.
- Ransomware - This form of malware locks or encrypts a machine with valuable information, and typically the attackers will ask for a certain amount of currency in exchange for the unlocking or decrypting of data. This type of attack proves the value in backing-up information.
- Phishing attacks - Phishing attacks are a type of social engineering, where an attacker may pretend to be a boss, or a colleague and ask another employee to open a link or run a program that is actually a virus.
- Viruses - Similar to Malware, but this type of attack focuses upon the destruction of information and data instead of theft.

Attackers may use one, or even multiple forms of these attacks at once to find their way into a network. Once they have found a way to gain access to the inside of the companies network, the attacker has access to the core systems that holds the company afloat, with full access to every server, computer, router or switch. From here, they may turn off sections of the network, or the entire network itself.

Cisco, one of the most popular network device distributors, has developed their own framework to assist companies with building defences. This framework consists of three groups, called 'Planes'. Each plane puts together a number of various security concepts and techniques to secure switches and

routers, primarily. These planes are called the 'Management Plane', 'Control Plane' and the 'Data Plane'.

1) *Management Plane*: The management plane focuses on the protocols that a network engineer may put into place when setting up the network, and then hardening it's security. This may include protocols such as password and key encryption, and SSH. If SSH has been misconfigured, then it becomes a severe risk as it leaves a vulnerable switch or router open for attacks to access remotely.

2) *Control Plane*: Similar to the management plane, this plane focuses on the protocols that would be used to share information such as IPs, routing sharing and other protocols that would allow routers to communicate and share information together. An example would be OSPF. If this plane has been misconfigured, then there is the risk of a router not working properly within a network as it may hold packets indefinitely, or lack the ability to share or learn routing information.

3) *Data Plane*: The data plane focuses upon the end user, such as a live website or an employee's computer. If this plane is not followed as per the framework, then employees may not be able to complete their work.

AAA, or Authentication, Authorization and Accounting, is a framework often used within router devices to assist in managing user access, enforce policies set by the network engineers, and measure the network resources used by the router. The entirety of the AAA model can be implemented from the router's CLI, and requires the use of a TACACS+ server. This server will handle the authentication, authorisation and the commands issued and executed on the router.

C. Tools, Firewalls and other devices.

To combat these risks, many companies deploy tools to try and track or mitigate any potential danger that may come their way. While attackers are usually ahead in the race of developing tools, the defensive side of software is not far behind.

Tools such as Packet Analysers are used by security teams to monitor what packets are being sent out from the network, and where incoming packets are coming from. This is valuable as it can help pinpoint any unknown packets as dangerous, and allow the firewall to block them if required. Firewalls are network security devices that are placed within networks to monitor, filter and potentially any incoming and outgoing packets of data. The specific policies that the firewall follows are configured by the network engineer that set-up the firewall, and have a variety of options to allow for custom and specific policies to be implemented. Within a medium-sized network, a firewall is usually placed as the barrier between public and private internet access, to reduce the risk of any unwanted traffic from entering the private network entirely.

While a firewall can be implemented on any computer running Windows or a Linux distro, companies usually purchase dedicated firewalls developed by Cisco called an ASA Firewall. This type of firewall is used in figure 2, page 3. In this packet tracer example, the firewall is placed on the barrier of inside and outside traffic, where it would filter any

unwanted traffic sent through by the R1 router before it can be received by the S1 and S2 switches, and finally the PC-A and PC-B respectively.

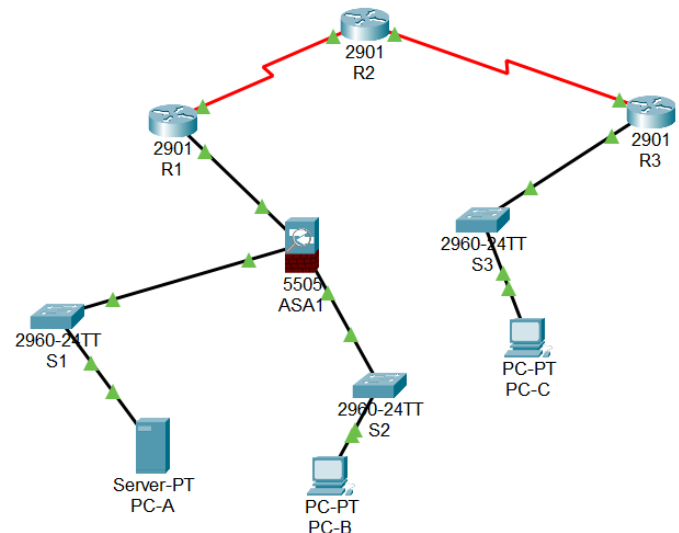


Fig. 2. An example of a firewall being used within a network, created with Packet Tracer.

D. Network Security

1) *Network Security Testing*: Network security consists of policies, practices and processes, all culminating in the best possible defense against unauthorised attacks that may be launched upon a network to gain access, information or data. These policies are usually developed and adopted at the beginning of a company's lifetime and updated as technology advances, to ensure that the company is built with security in mind.

Despite this however, no company is invulnerable from an attack, and the best practice is to test the defenses to expose any weaknesses so that the security team can focus on fixing what went wrong during testing. There are a number of ways that a company can test their defences. A company may use tools themselves to see what is happening on their networks, attempt to break their own defences, or even hire a professional to do this for them. This is known as a 'Penetration Test'.

Network engineers and penetration testers use a variety of tools to test their network, and ensure it is secure. These tools can range from custom made software by in-house software developers, to software easily accessible online. An example of this would be the aforementioned packet analysers, as shown in figure 3, page 4. This application, named Wireshark, captures all of the network data packets being sent to and from the computer. This can be used in a network to analyse if packets have reached their destination, or where they are lost along the way, and why. Packet analysers can also be used to determine where unauthorised packets are being received from, or being to (In the case of a virus like a RAT, where network packets are being sent out from the infected machine unknowingly).

```

root@eve:~# tcpdump -i eth1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
14:35:08.851329 IP bob > eve: ICMP echo request, id 7390, seq 66, length 674
14:35:08.851359 IP eve > bob: ICMP echo reply, id 7390, seq 66, length 674
14:35:11.020692 ARP, Request who-has bob tell eve, length 28
14:35:11.021167 ARP, Reply bob is-at 00:50:79:66:68:01 (out Unknown), length 28
14:35:11.860541 IP bob > eve: ICMP echo request, id 8158, seq 67, length 674
14:35:11.860600 IP eve > bob: ICMP echo reply, id 8158, seq 67, length 674
14:35:14.861684 IP bob > eve: ICMP echo request, id 8926, seq 68, length 674
14:35:14.861718 IP eve > bob: ICMP echo reply, id 8926, seq 68, length 674
14:35:17.863018 IP bob > eve: ICMP echo request, id 9694, seq 69, length 674
14:35:17.863051 IP eve > bob: ICMP echo reply, id 9694, seq 69, length 674
14:35:20.864196 IP bob > eve: ICMP echo request, id 10462, seq 70, length 674
14:35:20.864231 IP eve > bob: ICMP echo reply, id 10462, seq 70, length 674
14:35:23.865378 IP bob > eve: ICMP echo request, id 11230, seq 71, length 674
14:35:23.865429 IP eve > bob: ICMP echo reply, id 11230, seq 71, length 674
14:35:26.866608 IP bob > eve: ICMP echo request, id 11998, seq 72, length 674
14:35:26.866640 IP eve > bob: ICMP echo reply, id 11998, seq 72, length 674
14:35:29.879185 IP bob > eve: ICMP echo request, id 12766, seq 73, length 674
14:35:29.879236 IP eve > bob: ICMP echo reply, id 12766, seq 73, length 674

```

Fig. 3. A packet analyser capturing packets being sent to and from a machine. Captured within Wireshark.

2) *Security*: Anti-virus software is among the most common forms of software found on any computer, either a personal desktop or a workstation. The design that most anti-viruses are developed with is named ‘Signature-based anti-virus’ [4]. This type of anti-virus uses already known strings of data or code that exists in viruses that have been detected before. If a scanned file contains code or data that matches a virus previously found, it will flag and quarantine the application.

An Intrusion Prevention System, or IPS, is a tool used with network security to assist in continuously searching for any unauthorised activity. The IPS can come in the form of hardware or software, and companies may choose to even have both in a network for best results. The IPS has three different types, with the first similar to the aforementioned anti-virus, working by looking for signature-based matches. The second type of IPS is the Anomaly-based Intruder Detection. This type of IPS scans the network constantly for any unnatural traffic or strange fluctuations. If a strange occurrence happens within the traffic, it will flag it as suspicious for manual inspection. The third and final IPS type is the Hybrid Detection, which uses both of the previously mentioned systems in one to look for commonly known malicious signatures, and unnatural behaviours in the network.

The Layer 2 section of the network infrastructure is the most vulnerable layer of the network for attack. The OSI model was built with ease of communication between various devices, and this is ease of access is what creates the most issues. It allows anyone with a laptop and an Ethernet cable to approach a router or switch and connect into the console and change things, and this is why proper network security is crucial. One of the most common attacks in the modern day is known as the ‘Man In The Middle’ attack, and this is performed at the layer 2 of the network. This form of attack is conducted when a network request is made between a computer and a server, and the request packet is intercepted on the way. With this interception, the attacker is able to view what has been requested, what is being viewed, and what has been sent. More importantly, the attacker is able to modify the request packet. If the user has just signed into a website, the

attacker is able to see the username and password once the packet has been sent from the computer to the server. This attack is the reason that proper encryption between servers and customers is vital, and that packets should be verified using ARP (Address Resolution Protocol). These could all be considered endpoint vulnerabilities, as they all are executed on users computers. However, endpoint attacks can be as simple as someone spying on another to steal their password, or a complex attack to gain access to a computers network system. Endpoint attacks are among the most common form of attacks, as they are often the most vulnerable parts of a network. Phishing attacks are another form of endpoint attacks, and can be prevented by only allowing links or files to be sent from company addresses, and disallow files to be downloaded from unknown email addresses. Enforcing a strong password policy within the office will assist with prevent passwords from being brute forced and cracked, and the use of a strong anti-virus on all company computers will assist with preventing any malicious activity. Regular training with employees over the risks of attacks and how to prevent them will help keep employees mindful of what they are doing in the office, and at home. If employees are allowed to work from home or bring their personal devices to work, then having an isolated network for them to connect to would allow isolation from the main network. If their device was to be attacked, then there is no risk of them viewing or accessing the main server, and the risk is reduced.

E. VPN

A VPN, or Virtual Private Network, are often used by people wishing to hide their IP online, making it difficult for unauthorised third parties to track their actual location. A VPN works by masking the users IP with another random IP, usually an IP based in another country picked by the user. This is often used for services such as Netflix, where a user can mask their IP with another countries, to view Netflix’s contents that is exclusive to that country. While this seems powerful, it is important to remember that using a VPN does not make a person invisible, and there are many ways to discover the users original address.

VPNs are used within network systems on the barrier between the ‘Inside’ network and the ‘Outside’ network, where traffic is broadcast into the public network. Here, the VPN can be used similar to a NAT, or Network Address Translation, to obfuscate the original IP that is used inside of the company network. This can assist with encrypting data being sent to and from the network, and conceal the IP address used.

A group of dedicated protocols working together with the intention of encrypting connections between devices create a concept called IPsec. This idea is used within networks to encrypt IP packets as they are sent between network devices, to further assist with enhancing security with in the network.

This concept is most commonly used with key encryption. These keys are a random set of numbers that are used to encrypt and decrypt files, like a real key in a door. IPsec’s purpose is to set-up these keys with the connected devices

only, so only they may access the files. Let's create a scenario to explore how this concept works.

Computer A has a sensitive document that they wish to send to Computer B. On Computer A, their private key is used to encrypt the document. IPsec will set up an identical key on the receiving computer, and the file will begin transmission separately from the key exchange. This is to ensure that if the key is intercepted somehow, the attacker does not also receive the document and can decrypt it themselves. When the encrypted document is delivered to Computer B, the key is used by IPsec to decrypt and decipher the document, making it readable for Computer B's user. The keys are then removed on both computers once confirmation that the transmission has been completed.

The document would be split up into various packets on Computer A's side, so that if the packets are intercepted and stolen, the attacker would not receive the whole document, therefore making it harder to steal information. Each packet is signed, giving authentication that they were sent from the original Computer A, and not intercepted and modified in transit (Such as a Man in the Middle attack, for example).

F. Encryption

Encryption is one of the main fundamentals in the space of security, regardless of if it is in the digital world or in the real world. It's the art of scrambling data or words into a code that can only be understood or read by those who hold the knowledge to unscramble it's true meaning. The first form of 'modern' encryption stems from the year 1553, where a keyword had been agreed upon that was required to decrypt the coded message. This form of encryption would eventually find it's way into the digital world, first appearing in the early 1970s, developed by IBM. This encryption method would eventually be named DES (Data Encryption Standard), and would be used to keep their customers information safe. Even if the DES encryption method has been cracked and deciphered many years ago, any form of encryption is better than none, and a basic layer of encryption could be applied to the delivery of the virus to ensure safer delivery, and delay the time it may take for an anti-virus to identify the virus. The longer it takes for the anti-virus to act, the more information the RAT is able to gather and root itself within the computers lower layers (Depending on it's functions, of course.)

This means that a file may be encrypted, sent to a trusted colleague, and they would be able to open it assuming that the key was shared. This would mean that the file had arrived uninterrupted, so that it has not been changed or edited in any way by a third party, and that it has not been viewed by anyone else. The key would need to be shared between the two employees. If the key had been sent at the same time, then it would defeat the purpose, as an attacker would be able to take both the encrypted file and key, and decrypt it for themselves.

This can be prevented by having all employees share one key that is changed weekly, or to share the key locally by USB. The former solution would mean that the key is constantly

changing, and that a former employee would not be able to use it.

Like the aforementioned IPsec, there are a lot of concepts and protocols that come together to try and achieve anonymity and security between network and end devices. There are different methods of encryption, but they usually revolve around the same principal, which was discussed earlier in the example. However, where they differ is the type of hash and encryption used. A common algorithm for encryption is the MD5 hash,

Yousif Ali and Abdul Hameed in their paper 'Cloud Crypter for bypassing Antivirus' claim 'Results show that our cloud based crypter can be accessed remotely and avoids antivirus detections up to 100% [5]'. They propose a solution to bypassing anti-viruses by delivering their payload through Microsoft Azure, a cloud computing service, which runs the virus through an application called 'Crypter'. This application is designed to encrypt, manipulate and ultimately hide the virus from the victim and any installed anti-viruses. This type of development is dangerous for companies as there is currently not a cheap or easy solution to cracking encrypted attack such as this, without trying to decrypt every application on a computer (A process which can take possibly hours for one large application, and would be costly on computer resources rendering that machine possibly unusable). Advancements such as this in cyber security prove the necessity for firewalls and other defences to put be in place, and set-up properly.

II. PART TWO.

A. Proposed Topology

Figure 4, page 5 displays the proposed topology for use in A2Z Technologies Ltd.

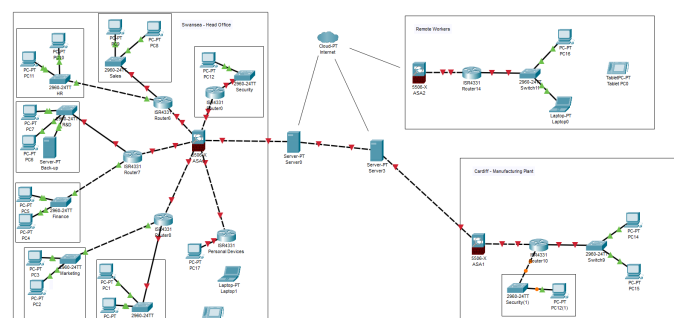


Fig. 4. Proposed topology for A2Z Technologies Ltd.

The topology has been split into four main sections. In the centre, two servers act as connections and back-ups for both departments on either side.

Each section has been labelled accordingly. Starting with the Remote Workers, this router will be the access point for those who work from home, and are isolated on their own router and firewall that is connected directly to the internet. This isolation severs the risk of a remote connection being able to access the other departments and gaining unauthorised access. This reason is also why each department within the Swansea main

office has been split into their own sections, each containing their own switch. This will allow each department to run on their own VLAN, or Virtual Local Area Network, and therefore be isolated from accessing other departments. As an example, an employee in Sales would not be able to see the traffic and computers in Finances.

The Research and Development department has a local server within their department, allowing them to make local and constant back-ups that cannot be interrupted, even if the internet or connection has been broken to the main servers. This server will be making hourly copies of all research and progress, with those back-ups being sent to the main server for further assurance.

Within the Swansea main office, a dedicated router will be set-up for those who wish to bring and use their own personal devices. This router will be connected directly to the firewall, reducing the risk of being able to access the department specific routers and servers.

Both the Swansea and Cardiff offices have their own dedicated cyber security team, who are able to access and view all of the traffic being sent in and out, and are able to access all of the devices set-up in their respective site. The security office will be secured by advanced security measures such as bio-metric security (Finger prints, hand scanner and/or key-cards). This will ensure that the security remains untouched and no change can be made outside of the allowed personnel.

1) Security Measures: The list below consists of the security measures that should be put in place across the network devices.

- The routers, firewalls and switches will need to be configured by the security team to only allow the ports currently in use to be open.
- Any exposed ports that are not in use should be shut down, to prevent any unauthorised access to the devices.
- The Firewall should be configured with privilege levels, only allowing network administrators to configure and change settings on any network device.
- AAA authentication should be enabled across all devices, with a TACACS+ server to allow for a local database of all users.
- Access Control Lists should be implemented to prevent unwanted network traffic from entering, and a VPN should be enabled on the Firewall.
- Each department should be configured to their own Zone on the Firewall, allowing for each zone to be modified as required. (For example, the sales and marketing teams should be allowed more freedom with their network usage, but the Research and Development department should be strict to reduce risk of attacks.)
- IPS software should be installed on the security teams devices to monitor the network for any unnatural network changes, alongside a strong anti-virus such as Kaspersky.

B. Cost

In the topology, ten switches, three firewalls, three servers and seven routers are suggested. This assumes that the com-

pany already has all of the required computers for employees.

Of course, it is possible to spend more per switch to gain extra features, but for now the cheapest of the flagship lines of each manufacturer shall be used. The best price found for a Cisco Catalyst 9200 is £1809.32 on comms-express.com, which is one of Cisco's newer switch models. If A2Z Technologies Ltd wished to go with another vendor to Cisco, the cost would change to £1188.30 with the Netgear GSM4328S. For a Cisco switch, this will cost £18,093.20 for all ten switches, and £11,883 for Netgear switches.

For ASA firewalls, Cisco's main device on offer is the ASA5508, currently on sale for £1,360.57. An alternative to Cisco firewalls could be the SonicWall TZ370W, currently on offer for £1,569.99. For all three firewalls, the Cisco option would cost £4,081.71, and the SonicWall would cost £4,709.97 in total, making the Cisco ASA5508 the cheapest choice.

For routers, there is almost an endless option of devices that could be chosen. In the end, the two on offer for a reasonable price is the Ubiquiti UniFi Dream Machine and Cisco's Cisco 4351. The Dream Machine costs £336.30 each and £2,354.10 for the whole project, and Cisco 4351 is £582.23, and £4,075.61 in total.

For the servers, the PowerEdge R450 Rack Server costs £2,577.73 and is powerful enough to handle all of the issues that may arise in a cyber attack. For all three, the total would cost £7,733.19.

For the recommended software, BitDefender premium is £149.99 for three years, per ten devices. Assuming the company has two hundred employees, this would cost £2,999.80 every three years. Wireshark, Putty and NMap are free softwares, and will not add to the total.

In total, this will cost £36,984.71 if the company wished to implement all Cisco devices, and £29,051.80 for the cheaper alternatives.

C. Time of Implementation

Figure 5, page 7, figure 6, page 7, and figure 7, page 7, all display the estimated tasks and timeline required for the implementation of the aforementioned topology and security measures. This includes testing, hardware installation and configuration of all devices, including the VLANs, remote worker network, Cardiff and Swansea main offices. The Swansea main office will be focused upon first, as it is the most complex scenario of the entire network.

The timeline offers three weeks at the end for final configurations, testing and attacks that the security team may wish to employ other than the ones listed.

D. Potential Attacks

There are almost countless attacks that can be made on a network at any given time. It is almost impossible to be impregnable against cyber attacks, with the best that a company can do is to prepare for the worst and counter attacks that are most common.

One of the more common attacks that are conducted on network infrastructures almost daily are DDoS attacks. Mentioned earlier in the paper, this type of attack relies on sending

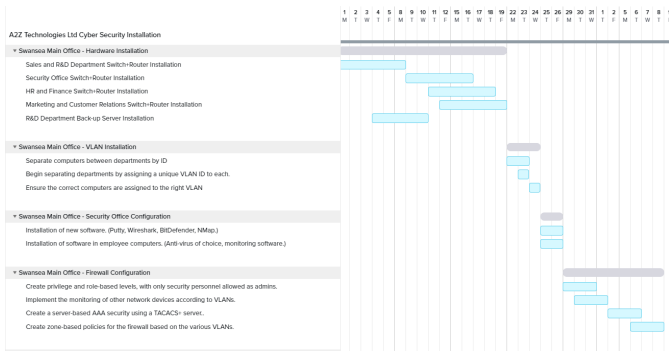


Fig. 5. Gantt chart tasks and timeline for the A2Z Technologies Ltd project.

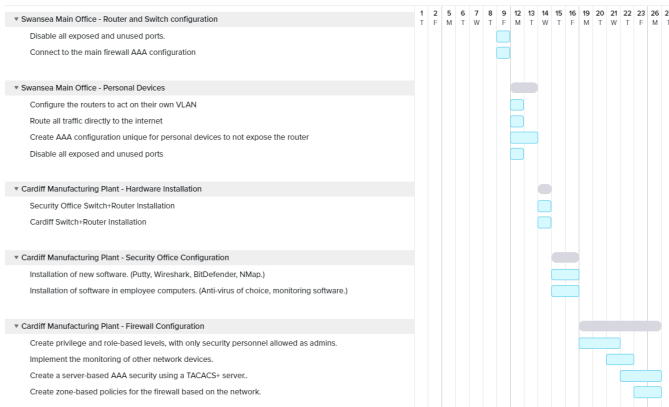


Fig. 6. Gantt chart tasks and timeline for the A2Z Technologies Ltd project.

a large amount of network traffic, or packets, to a router or switch until the affected device is unable to process the large amount of data, and becomes overwhelmed. This type of attack can slow or even halt traffic flow for hours at a time. While the original address IP is usually ‘spoofed’ or faked, there is usually no way of tracing it’s origin. But, it is still possible to prevent such an attack from happening at the ASA Firewall device. The Firewall is able to specify how many connections it can make at a time per client. This can help prevent packets from queuing and preventing the Firewall from preventing. Figure 8, page 7 shows an example of maximum connection and packet requests.

The Man in the Middle attack is another common form of attack that plagues companies on a regular basis. This attack consists of an attacker intercepting a packet in transit, often with the intention of modifying or examining information currently within the packet. This form of attack can be prevented by using secure servers, such as websites with the ‘HTTPS’ prefix, which use Secure Socket Layer to ensure a secure connection.

A third attack that could be launched against a company of A2Z Technologies Ltd size is a phishing attack. This type of attack employs social engineering, and will often manipulate and trick employees into installing or opening fake software, emails or applications with the intention of installing a virus or malware. This infection can spread to

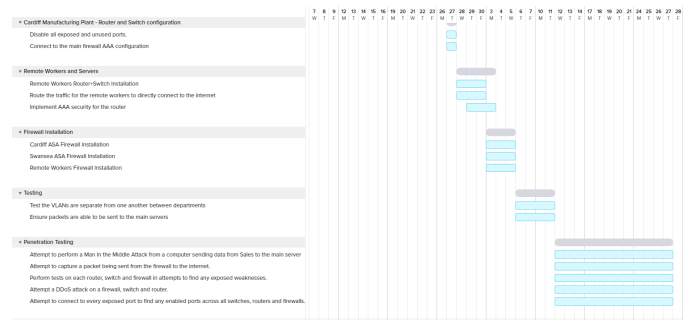


Fig. 7. Gantt chart tasks and timeline for the A2Z Technologies Ltd project.

```
ciscoasa(config)#class-map tcp_syn
ciscoasa(config-cmap)#match port tcp eq 80
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map tcpmap
ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100
ciscoasa(config-pmap-c)#set connection embryonic-conn-max 200
ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5
ciscoasa(config-pmap-c)#set connection random-sequence-number enable
ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0
ciscoasa(config-pmap-c)#set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

Fig. 8. Example of ASA Firewall commands to prevent DDoS attacks [2].

connected computers, network devices and other machines to keep the virus alive if it has been removed on the original host. The virus may duplicate, disguising itself multiple times to avoid detection. Eventually, the virus can copy, delete or manipulate information, data, passwords and even take control of the infected machine. This type of attack can be prevented by ensuring an up-to-date anti-virus has been installed on every computer, and every employee is trained in spotting fake emails and applications. Regular training should be conducted on safety and the risks of viruses, and computers should be updated whenever possible.

E. Testing of systems

A DDoS attack should be used to test the capabilities of the firewall, and see if the current configurations is able to sustain the large number of network packets. These types of attacks are very popular, and therefore should be tested every few months.

The second test should be a Man In the Middle Attack. By sending packets from one department to another, see if a program such as Wireshark is able to snatch and modify the packet as it is in transit between the departments and firewall. This should also be performed every few months.

The final test would be a test of malware. In a controlled environment (Such as a computer that is isolated on it’s own network and not connected in any way to the main servers), use a Raspberry Pi or a USB stick to transfer a virus onto

a computer configured with the same anti-virus used on all company machines to see how long it would take for the anti-virus to flag and remove the virus. If the time is too long, roughly ten minutes, then a new anti-virus should be considered, as this is enough time for a virus to steal all of the required information.

F. Invoice

An invoice has been attached with this paper, named invoice.pdf.

III. TERMINOLOGY

List of terminologies used in this document:-

- OWASP - Open Web Application Security Project.
- NIST - National Institute of Standards and Technology.
- DDoS - Distributed Denial-of-Service.
- AAA - Authentication, Authorization and Accounting.
- TACACS+ - Terminal Access Controller Access Control System.
- RAT - Remote Access Trojan.
- VPN - Virtual Private Network.
- NAT - Network Address Translation.
- IPsec - Internet Protocol Secure.
- VLAN - Virtual Local Area Network.
- IPS - Intrusion Prevention System.

IV. REFERENCE LIST

- [1] Balbix, "What is the nist cybersecurity framework?" 2022.
- [2] Cisco, "Asa/pix 7.x and later: Mitigating the network attacks," 2008.
- [3] B. Kiruba, V. Saravanan, T. Vasanth, and B. Yogeshwar, "Owasp attack prevention," in *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2022, pp. 1671–1675.
- [4] V. G. Tasiopoulos and S. K. Katsikas, "Bypassing antivirus detection with encryption," New York, NY, USA, p. 1–2, 2014. [Online]. Available: <https://doi.org/10.1145/2645791.2645857>
- [5] Y. Ali and A. Hameed, "Cloud crypter for bypassing antivirus," in *2019 15th International Conference on Emerging Technologies (ICET)*, 2019, pp. 1–6.