Coursework 2 – Design security controls of your network

The reason for why we use perimeter security for our network is that the Perimeter security of the network is a technology that can help us to provide a range of security services from a basic firewall protection and it can also be through end-to-end security for your network or business. If we go back to our design of the network. We have ensured that our employees are safe when they are browsing around the internet. Perimeter security can also be a defence system around your network designed to help stop unwelcome user to enter our internet.

Draw of the network Design:

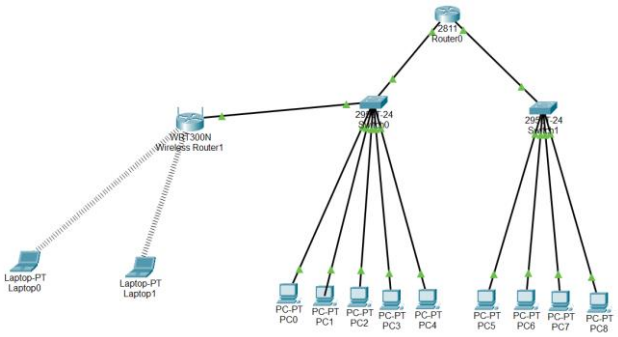


Figure 1: Network Topology

This the network design I choose to make from coursework 1, if we look further, we can see that our design not got any security protocols or information that help to hold the network safe. The draw design of the network is developed to a network for a greenfield company that have ten employee and need a LAN network.

Why is perimeter network security important?

It is important question to ask yourself why network security is important, one of the main point is that in the technology world today one main thing its hackers. According to study from Clark School study, **hackers attack every 39 second** [1].

Different ways we can protect our network:

- **Firewalls**
- **IDS/IPS**
- **Two-factor authentication:**
- **VPN**

Firewalls:

Firewall always plays a vital role in network security that help us to supporting the internal networks. We start with the first thing that is to secure the firewall, the securing a firewall is most vital step to first ensure only the authorized administrators to have access to it, in our case it is the ten employees for the greenfield site. The next part is to then establish firewall Zones.

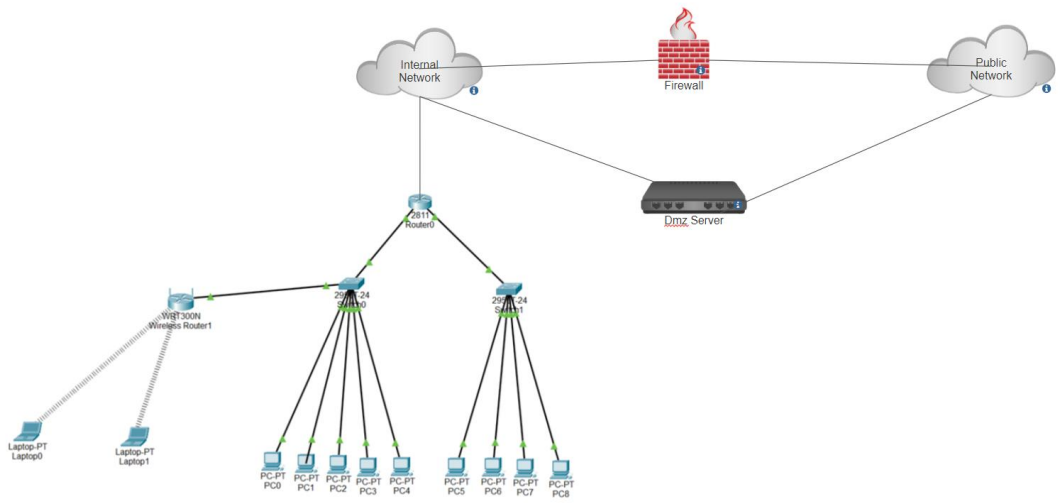


Figure 2: Firewall in our network

If we go back to our network design with firewalls. We see that a firewall can operate in the manner I have illustrated above, and we can see the purpose is to then hinder or isolate the company's internal network as wee see how the traffic is going between the internal and public network. The firewall can then permit the transmission from our internal network to either the public network or the DMZ. The firewall then has rules to deny or either accept the IP-Address if the administration of the company has set the rules, but they can also base it on protocols or domain names.

Our firewall can come in different types, we can have **hosed-based firewall**, that means that the firewall is based on a type of software that is based on installation on a computer which then protect that exact computer only and then we can also have the **antivirus**.

The hosted-based firewall is firewall software that installed directly on the computers to the company (rather than a network). If we go back to use hosted-based network it can helps us to detect and stop different viruses, other malware. Using hosted-based firewall is regularly updated and is running on the computer, we are sure that the company computer is protected against viruses.

We know that many popular **Anti-virus** programs include a host-based firewall feature. We you got a Host-based firewall installed on our computer, then you first can confirm that you have an Anti-virus program installed on your computer.

Another type of firewall that we can use is the network-based firewall. The network-based firewall can we say are a good combination of hardware and software, it operates at the network layer and then its placed between our external and internal network. Back to the draw of the designed of the firewall in my network we can see that I have chosen to use **network-based firewall**, the reason that I choose to use network-based firewall is that the host-based firewall or most of the only time sufficient for small networks, but when we are using network-based firewall can they be used for much larger networks. The main reason for network-based firewall is that they are deployed in line with the traffic flow, and it's protecting the entire network, but in the other side the host-based network is just only operated on the single computer.

Example how our firewall works. Our Firewall can regulate the network traffic, by using Packet filtering. The packet filtering when we are using a firewall, are that the packet that contain small amounts of data, these types of packets are then attempting to enter our network and run against a group of filters. When we are using these filters, they can remove the packets that match then certain identified treats and then allow the other one through the network and go to their indented destination. We can also use network control list.

IPS/IPS:

We first start to IPS, Intrusion prevention systems that help us to comprise one of the elements in comprehensive cybersecurity portfolio, this helps us to proactively neutralize the cyberthreats before they enter the infrastructure and our network. We also have IDS, intrusion detection system that is a passive system that scans internal network traffic and then report back about potential threats. We also know that it also operates outside of the traffic flow, it also not affects the network performance. We also know that the IDS can detect to different types of threats like malware or attacks like trojan.

Before we start, you need to understand a few things about our network and the traffic. What kind of traffic do we see? How complex is our network, how many different connections are between our networks? After you have asked yourself this question, by this information that will help you to decide how many IDS or IPS devices you then will need and what kind of hardware you will need. IDS/IPS is strategically placed in an entrance of an organisation.

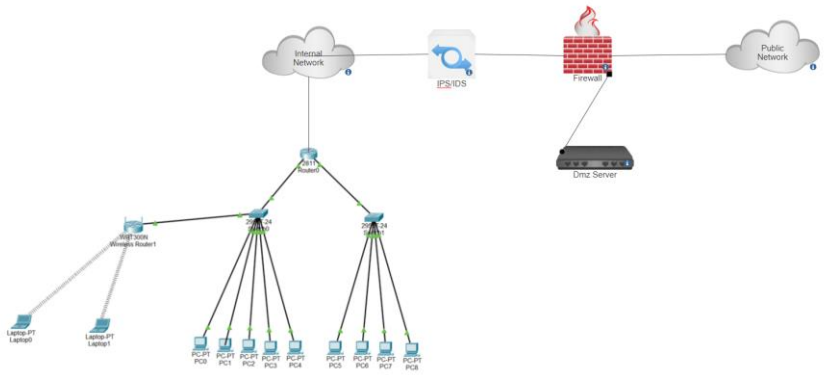


Figure 3: IPS/IDS integrated to our company network:

If we look above, we see that the IPS is installed between the firewall and our internal network for our company, the reason that I have placed the IPS there is because I want to provide to us a type of an extra layer of security before the internet traffic passed into our internal network. To give an example on how it works, if our network gets an unwanted person/user to get through our network it can be the public network and get further in our network and passed the firewall. The last solution can be that the IPS/IDS will see the danger and then can decide to stop the unwanted and then report a potential threat to our company. We can setup the IPS/IDS by set the IPS behind the firewall, that is adding another layer of analysis that then remove dangerous content from the data that flows in. Our IPS then sits then in the communication path between our destination and the source, its analysing traffic and then act, they can send alerts and also dropping malicious packets and in the end block traffic.

Other Protection to the network:

You can also use a VPN. To explain VPN further a VPN can create a secure connection between you and your internet. Also, when our employees work from home could they connect to internet through a VPN, that then means all your data traffic is then sent through an encrypted virtual tunnel.

Two-factor authentication:

Two-factor authentication or referred to (2FA), can also be sometimes referred to as two-step verification, the 2FA is a security process in which the users provide two different authentication factors to verify themselves.

The two-factor is implemented in a way to protect both of us a user's credentials and the resources the user can access.

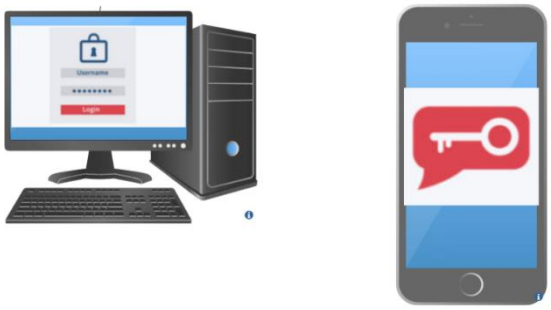


Figure 4: 2FA:

We have two additional steps, the two-factor authentication methods rely on a employee inside our network to type in a username and a password as the first additional step, the second step is to get send a message to your own personal phone. Another security factor can be to us BankID in your phone to secure that its your personal login.

The reason is chosen to use 2FA is that is add an additional layer of security to the authentication process by making it a lot harder for attackers or unwanted persons to gain access to our employee's devises, using 2FA is somebody can hack or gain access to our employees' user, have we made it possible that the password alone isn't enough to pass the authentication check. Before the use of SMS message was popular, but because of MIM attack its not good to use. The MIM attack is a type of attack where the attacker hid relays and also potentially change the communication between the two parts that use the internet that think they are communicate directly.

Web treats or danger that the network can face:

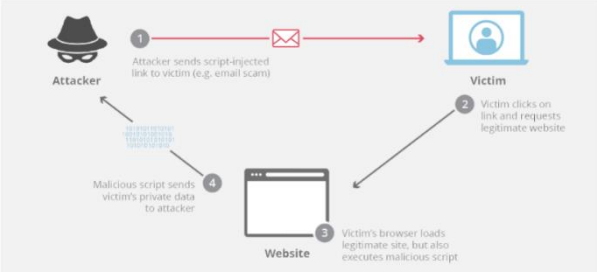
Example to different treats to a network, often depend on the design of the actual network we got. If we talk about today one of the main treats to a network can be hacking, when you hack a network, you can use various type to treat the network. But treats to our network can be:

- **XSS**
- **SQl injection**
- **doS attack**
- **Trojan attacks**

XSS:

XSS can be a type of a treat to our network. The XSS or Cross-site scripting is a web security that allows an unwanted attacker to compromise the interactions that's the users have example with a vulnerable application. That's helping to allow an unwanted attacker to circumvent the same origin policy, then it's designed to then segregate the different websites form each other. We often see that the XSS attacks most of the time occur when an attacker uses a type of a web application to then send malicious code, its most of the times in a form of a browser side script.

Example of how XSS works:



We start with the attacker start to attach code into a new legitimate website that will after that execute when use user/employee loads the website the attacker has sent.

Figure from Google [3].**How to prevent XSS?**

There is no efficient answer to prevent XSS, but there are some tips that you can use like, if their possible, avoid downloading HTML links that are sent to you from people you don't know. You can also be taking cookies security measures. We also got user **Input validation** that is a technique to prevent XSS, this technique helps us to provide a form for security to certain forms of data, that are specified to go against certain attacks and can therefore not be reliably applied as a general security rule.

Example on XSS: **Phishing attack:**

We also got Phising attack that is a type of an attack that is used to steal user data, that often include that they can get login credentials and private things like your card numbers. The phishing often occurs when the unwanted attacker, can then masquerading as an entity that is trusted, then it dupes a victim into then opening an email, or an instant message. Phising attack can be a massive treat to our network and we as a company, it can unauthorized people can get access to our network, and they can maybe do identity theft to our employees and maybe also steal funds from the company. Example on a common phishing attack: This photo illustrates one of the most common

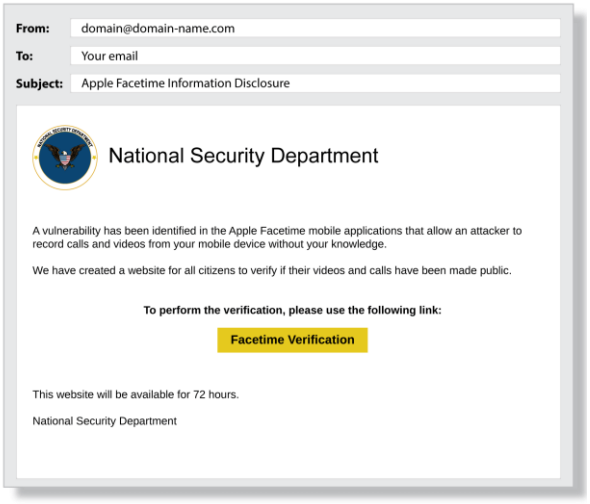


Figure Google [4] This photo illustrates one of the most common phishing attacks. We got a spoofed email ostensibly from National Security Department and tells us to access a link that is facetime. There are several things that can occur by clicking the link, like a false page that can look like a real page, and they can ask you a user a username and password that is private for you. If you as a user type in your private information, that can risk that the attacker can monitoring your page and then hijack your original password to then gain access to our network or private information.

How to prevent phishing attack?

To the employees for our network is **vigilance** is very important key. Most of the spoofed message very often contains subtle mistakes that often exposes its identity. We can also prevent phishing attacks from email phishing by see after **spelling mistakes** or **changes to the domain name**. But one of the most important things to prevent phishing attack is that you as an employee should maybe stop and ask yourself why you are receiving this email.

SQL injection:

SQL injection or Structed query Language, is an injection that is a code injection used to modify or retrieve data from SQL (database). If you start to insert different SQL statements into an entry field, then the attacker is then able to then execute different commands that help us allow for the retrieval of data from a database. If the SQL commands execution, then the unwanted user is then able to spoof the identity of a more privileged user. The SQL injection attacks then can be used to then bypass the different authentication that help us to see that the unwanted user to then disclose different type of confidential information.

Solution to prevent SQL injection: One of the best things to prevent SQL injection attacks is to have a web application firewall. The reason to use a web application firewall is that it can be operating in front of our web server, and it can monitor the traffic that goes in and out of the webserver. We can also use IDS that help us to analyse the unwanted person and then we can communicate with our company to hinder the attacker get access to our network.

doS attack:

doS or Denial-Of-Service attack is an attack that is meant to shut down a network or a machine, that makes it inaccessible to its users. Most of the times the doS attacks are accomplish by flooding the different targets with traffic or sending information that often triggers a crash. We often see that the doS attacks are characterized by using of a single computer to launch the attack.

The reason the doS Attack can be a massive threat to our network, it that it can shut down and cause our company a lot of time and money to handle.

Prevent doS Attack:

- We can use Monitor and then analyse network traffic. The network traffic can by surprised via IDS. Then our administrator to the network can setup rules that then can create different alerts for unusual traffic, and then identify traffic sources. We also can strengthen our security posture.

Trojan attack:

In the end we got the trojan horse, or trojan. Trojan is a type of a malicious code or a type of software it can look legitimate, but it can also take your control of our company computer. To describe a Trojan, it is designed to make a damage, steal and disrupt or make harmful action to our network. Example on how Trojan attack happened it you can receive an email from someone you may know and after that you click on what maybe looks like a legitimate attachment. But in after you have clicked in, that the trojan attack happened, many of the times the email or the message/attachment is from a cybercriminal, after you have downloaded and opened it, have you installed malware on your device.

Setup Web Server: The task is to setup a webserver the most important thing to remember when we are setting up a webserver is to have computers available, but since we are working in a firm that have the chance to allow their employees to have a laptop or a computer in the job. After that we can choose to be running the webserver by the help by running Windows, or Linux or a Mac computer running macOS

Sources:

https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html

https://www.google.com/search?q=sql+injection+attack&rlz=1C1VDKB_noNO976NO976&sxsrf=APq-WBtldfj0gB3N3NL-gRSCSJQexrZE9w:1649780286426&source=lnms&tbm=isch&sa=X&ved=2ahUKEwib5be_9o73AhUWCRAIHTyMA1YQ_AUoAXoECAIQAw&biw=1494&bih=823&dpr=1.5#imgrc=tZoIZdfxPmhVZM

https://www.cloudflare.com/learning/security/threats/sql-injection/

[3]: Hentet figur https://www.cloudflare.com/learning/security/threats/cross-site-scripting/

Email https://terranovasecurity.com/top-examples-of-phishing-emails/

[4] Hentet figur 4 https://terranovasecurity.com/top-examples-of-phishing-emails/