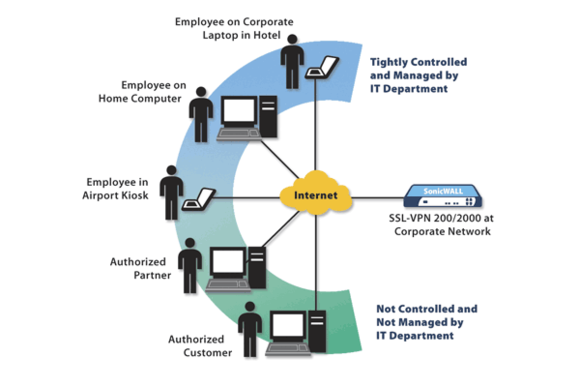
**D2 – Design a network security policy for a small organisation**

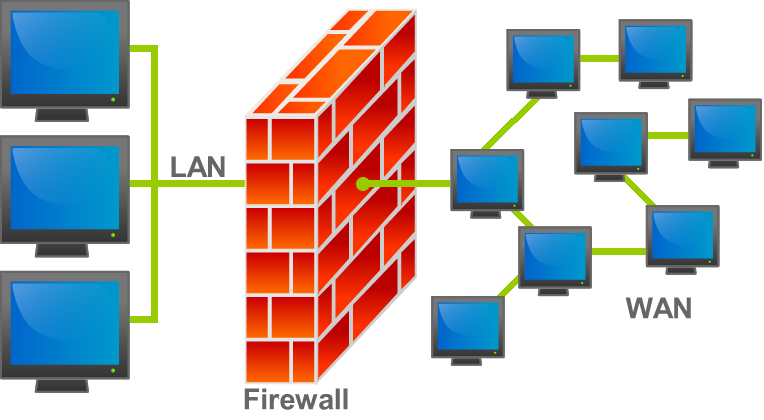
**Introduction**

In this report, I will be explaining the security policy for a small organisation. The benefit of having a security policy can remove any potential issues that could be created. For example, if a person has all of the websites unlocked, he can potentially be distracted and not do any assigned work. It minimises data loss, e.g. if the network manager daily runs a security scan can potentially not harm the network and not lose any data. The main aspect of having a security policy is to remove any that can harm the computer, which could be physical or internally.

**-VPN access**

VPN stands for virtual private network. This network connects to a private network. This needs to be set-up by usually using wires to enable connection to the private network. Large companies use VPN technology. It is confusing the way it works, but they use the private network to transport any data through the network. IPsec is used to secure the network. The disadvantage of using VPN is that data can be loss through the quality of its services. As it is a private network that it has been connected to, you never know the extent of the quality. Sometimes it can disconnect by the bandwidth not being long enough to cover it. However, large companies use it because it is inexpensive. The image shows how the VPN works. It acts as if so other computers connect to the internet. It is the “centre of attention”.

**Firewalls**

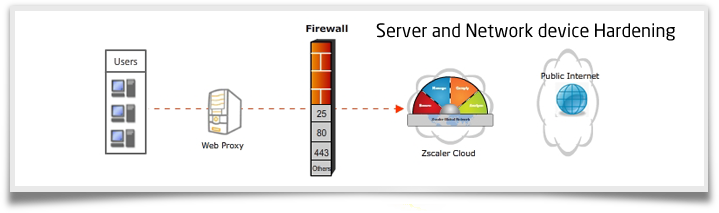
The benefits of using firewall are that it secures the computer network. It disallows other networks from entering your secured network. As it blocks other networks, it blocks viruses and hackers from entering the network. It acts like a secure “wall”. It does not let anything past it. For organisations who have secure data on their computers, it is vital that they tell/ask all employees to keep their firewalls ON. It is important and if anything is let past, it can access the files and the virus can spread/multiple quickly. The disadvantages of using firewall is that it acts like a central point of attack for intruders. If they are passed firewall, they have access to the whole network. In addition, it only protects one point of it, it does not protect the other parts of it e.g. modem.

**Access Control Lists**

Access Control Lists (ACL) is a network tool, which applies to routers, ACL denies access to any intruders that are entering the network. Like Firewall, ACLs are rooted to security regulations. This is available on Layer 3 on the OSI Layer. The advantages of using ACLs are its simple to set-up. It is flexible. Therefore, it allows users to deny and gain access to the network. However, the biggest disadvantage is that once the user has gained access to the network, it can allow intruders to access the whole network. It can gain access to the whole network and it is potentially bad for the network. Denying any access to specific sites could be an advantage for a business. This is because if you block all the gaming websites, the users would not be allowed to use any gaming websites.

**Device hardening**

Device hardening is the process of making the system secure by removing, or reducing any ‘attack surface’. Attack surface is the total numbers of unauthorised users who try to attack the extract data from the computer. They are many procedures to hardening the system by enabling firewall; close any open network ports and many more. Any device can be secured e.g. laptop, mobile device. This can secure the system by the unauthorised user getting access to the users’ data. The image below shows how a network should be secured.



**Continuous policy review**

This means when the manager continuously keeps an eye if you are following the policy that he has set out. When a manager has set out a task, he comes in every 10 minutes to check if the employee is doing his/her work. It could even turn out that the employee is not doing his/her work. Keeping an eye on each employee is important, so he/she do not get distracted.

**Forensic analysis**

Forensic analysis is when data is examined. This completely links to crimes. Most forensics use computer forensic. For example, if a person has been murdered, forensics analyse any DNA or any other data and they get those data and put it into a system where it needs to be analysed. Once the DNA is matched, the suspect can be identified. This is the most current system they have been using. However, latest technologies show that a shine of a specific torch can show data that cannot be seen by the naked eye e.g. foot print that has been rubbed off. This can come in handy for the police to deal with as well.

**User rights**

User rights works in every company. They have a legal right to do something. For example, if they work from 9AM to 5PM, legally they should have at least an hour break. This is because every employee needs time to eat for a long amount of time. In addition, if the user is employing any disabled people, they should require a lift or any sort of equipment that should help the user go around the building. Most buildings have it nowadays, but before they never used to follow this rule. This is the exactly how a network should be followed. No network can run for hours. It should take time for it to almost ‘digest’ each instruction; otherwise, it would just crash.

**How often they should be reviewed**

Within a network, everything should be reviewed twice a day. This is because any new information can be leaked out within two seconds. If anything goes wrong and it is not detected, it can create more problems e.g. costs rising even more than the current cost of the initial problem.

**Reference**

* <http://en.wikipedia.org/wiki/Forensic_data_analysis>
* <http://en.wikipedia.org/wiki/Hardening_(computing)>
* <http://m.c.lnkd.licdn.com/mpr/mpr/p/3/005/079/27e/07588d9.jpg>
* <http://www.isecurenet.in/images/inn-banner/Server%20and%20Network%20device%20Hardening.PNG>
* <http://en.wikipedia.org/wiki/Attack_surface>
* <http://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png>
* P6 Unit 9