Network Infrastructure

Student’s Name

Institution

Date

**Introduction**

Installation of network infrastructure requires analysis of the firm’s needs and the purpose of the network. The network design and installation includes the devices required and configuration of the network to meet the demand. The network of the company will have several computers connected to the server and therefore, the network intends to have external firewall, internal firewall, remote access server IDS and web server. Since the company is Small and medium enterprise in ICT offering online services. It would be essential to include a security setup structure as indicated in the topography below. Therefore, the below shall be the network topography of the company. This topography is chosen based on the fact that it provides a clear network security system and therefore, it provides effective way of establishing secure operations.

A screenshot of a computer

Description automatically generated

**Printers**

The network shall have a printing pool for all printers in the organization. The printing pool would be located at the back office next to the administrator manager. The printers will be connected through internet and shared so that all employees could send all the printing work at one stations. The CEO and the accountants department will have a separate printing pool because of the nature of their work.

**Server**

The servers will be located in the server room located at the back office. All the servers will be connected directly to the computers through the switches and routers. It means that all the operations of the company shall be saved in the server. The server to connect to the network through the firewalls and DMZ (Chapple, 2015), which will be installed to ensure that there, is maximum protection of the network infrastructure. The communication between the server and the workstation shall be protected as well and therefore the server will have static Internet Protocol (IP) address. The static IP shall also be implemented in all workstations and the entire network system.

**Rationale**

This topography will be implemented because of its scalability and reliability of the structure. First, addition workstations can easily be added to the network because of its scalability. This will make it easier for the administration to add more workstations as the company expands. As stated by Ahmad (2018) scalability of network infrastructure is an important aspect to consider when installation network for any organization. It is because most campaniles experience growth and therefore, as companies growth positions is created and therefore, more workstations would be required (Bader, Zhou, & Rababah, 2018). With this kind of topography illustrated above, it would be easier for the management to provide additional workstations to accommodate the growth aspect of the company. Secondly, security is a major factor in businesses today, and every company deserves to have a secure network infrastructure. And therefore, with the illustrated network topography, the implementation of network security would be easier and faster. The network topography includes the installation of firewall, IDS and remote server access and therefore, penetrating the DMZ wall would be difficult for any external intruder and therefore, this topography is chosen because of various security options it provides for installations.

**Implementation of network security**

Under this network infrastructure, the network security can be implemented in there levels on the network infrastructure. It can be implemented at the backbone, servers, and at the computer (King, 2014). At the backbone level, the network security is installed at router, gateway, and switches to prevent any unauthorized access to the system. When using CISCO router, the network security is configured in two levels to prevent any access to the system. This is to ensure that the entry point to the system is protected and it becomes difficult to gain entry into the system or the network (Rababah, Zhou, & Bader, 2018). The switches also should be configured with strong passwords or key to prevent any entry and therefore, installation of network security is necessary to be done at the entry point to ensure that the system is protected. Besides installation of security at the gateway and switches, it is important to install strong firewall hardware and set software as well. This will limit access to the system to ensure that unauthorized person does not get access to the network. In some cases, the security is also deployed at the gateway to ensure that the system is fully protected. However, it would be important to ensure that there is a clear security policy, to prevent the data from being accessed.

**Comprehensive security policy**

Security policy is an important measure which is taken to prevent the access to the system. The best way to protect a system is derived a policy which can protect the system from unauthorized access. An organization can derive policies regarding login and accessibility of the system (Michael, 2014). The security policy can be including login password strength, active status and how clients can be able to log to the system and stay active after certain duration. The network administrator must come up with security policy to prevent people from login to the system. The policy would be able to prevent the system from external attack such as hackers and therefore, it is important to ensure that there is a proper security system based on the policy. For instance, the system can be set to require string password such word and letters, and at least eight. This is to make sure that nobody can easily guess the password and use to access a system.

**Biometric and password**

Mostly entries are protected using biometric and password. It is important to ensure that the password is strong. The personal computer, server, and other electronic devices should be protected using passwords; it is upon the network administrator to design the kind of passwords allowed and the biometric devices which is applicable. The biometrical could be figure print, eye and other allowed system. It is therefore, important to ensure that every employee has a unique passwords and clear policy for login. The passwords are set at the server and configured for every end user could be best way to ensure that the system is protected. It is also required that users should change their passwords often at specific time and any user who failed to change the password would be lockout. It is some of the policies which should be included as part of the network policy to protect the system.

**Ethical issues**

The employees are expected to utilize concerns and a lot of ethical when dealing with computers, network system of the company. The employees will be required to avoid the use of flash dish and other portable devices to avoid the spread of virus among the computers of the company. It will also be required that employees should never share passwords among themselves and even with any none staff members. All employees will also be expected to report any suspected activities, which can compromise the network system of the company.

# Bibliography

Ahmad, N. (2018). Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of. 2-31.

Ahmed, A., Bwisa, H. M., & Karanja, K. (2018). Strategic Decision Making: Process, Models, and Theories. *Business Management and Strategy* , 2-35.

Bader, M., Zhou, S., & Rababah, B. (2018). Evaluation the Performance of DMZ. *https://www.researchgate.net/publication/322165207\_Evaluation\_the\_Performance\_of\_DMZ* , 2-35.

Chapple, M. (2015). Evaluation the Performance of DMZ. *https://www.researchgate.net/publication/322165207\_Evaluation\_the\_Performance\_of\_DMZ* , 2-35.

King, T. (2014). CompTIA Security+ Exam: Devices, Media, and Topology Security. 2-3.

Kumar, A., & Malhotra, S. (2015). Network Security Threats and Protection Models. *Technical Report – CSE-101507* , 2-34.

kumarasamy, S., & Asokan, D. (2011). DISTRIBUTED DENIAL OF SERVICE (DDOS)ATTACKS DETECTION MECHANISM. *International Journal of Computer Science, Engineering and Information Technology* , 2-38.

Michael, P. (2014). Effective decision making . *http://www.cimaglobal.com/documents/importeddocuments/40\_effective\_decision\_making.pdf* , 2-35.

Ossi, V. (2018). 2 EVALUATION OF FIREWALLS AND RESEARCH. *Degree Programme in Information Technology* , 5-38.

Rababah, B., Zhou, S., & Bader, M. (2018). Evaluation the Performance of DMZ. *I.J. Wireless and Microwave Technologies,* , 2-35.

Salah, A. (2018). Design and Implementation of a Network Security Model for Cooperative Network. *https://www.researchgate.net/publication/50367393\_Design\_and\_Implementation\_of\_a\_Network\_Security\_Model\_for\_Cooperative\_Network* , 2-35.

Sousa, W. H., Galante Porto, M. C., Takenouchi, P., & Marcatonio, P. M. ( 2015 ). Planning the Decision Making Process: A Multiple Case Study. *Engineering Management Research; Vol. 4, No. 1* , 2-35.