**Individual Project**

By

Buwaneka Hettiarachchi

SRT551-Section A

Professor Mohammed Al-Ani

Date: December 13, 2021

Network Designing

Contents

[Defense-in-depth design and explanation 2](#_Toc90246783)

[Zero-Trust Architecture design and explanation 4](#_Toc90246784)

[Design Comparison 6](#_Toc90246785)

[References 8](#_Toc90246786)

[Figure 1: Network Diagram Based on the Defense-in-depth method 2](file:///C:\Users\buwan\Documents\SRT551_IndividualProject.docx#_Toc90246799)

[Figure 2: Network Diagram Based on the Zero-Trust Architecture 4](file:///C:\Users\buwan\Documents\SRT551_IndividualProject.docx#_Toc90246800)

# Diagram Description automatically generatedDefense-in-depth design and explanation

Figure 1: Network Diagram Based on the Defense-in-depth method

The above diagram represents a description of a Defense-in-depth diagram of a company network that is trying to shift their focus on to putting, about 50 percent of the company staff on work at home, mostly due to Covid-19 pandemic. The Company CIO proposed us to create two methods, one being the traditional Defense-in-depth method and the other being the Zero trust method.

In the above method, the company architecture work as following, the company would have about 50 percent of the employees work remotely . The company connects their outside router into the modem, which connects to the Internet. The Connection between the Router and the Firewall, acts as the DMZ zone of the network, in this zone, lies the DNS server of the company and the Email Server. Then after coming through the firewall, we will be coming into the internal Network of the company, where the File Server and the Active Directory Domain Service takes place on.

The Internal Users and guests are connected to Wi-Fi services via the use of a wireless adapter that is connected to the users who are using machines physically inside the company. The company also has its branches that are acting as a subdomain and is also the branch acts as a portal to 3 party suppliers which use the company Webserver. The branch also has its servers for departments such as the HR department, Accounting Department, and CRM solutions. The Cloud Mail service is connected to the Internet, for remote users to connect to the cloud network, they have to connect to the company machine through the internet and then connect to the cloud network to access mails and other deliverables

# Zero-Trust Architecture design and explanation

Diagram

Description automatically generated

Figure 2: Network Diagram Based on the Zero-Trust Architecture

The above diagram shows the second representation of the Company Architecture that could be implemented due to most of the company going to work remotely. The Zero-Trust Network is different from the Defense-in-depth because rather than the traditional methods, it uses many policies using the Policy Administrator and the Policy Engine, this machine is also known as the Policy Decision Point (PDP).

In this scenario, the Remote users need to access the Internet and the get into the company network to the portal of the company through a PEP Gateway also known as the Policy Enforcement Point. After coming into the Portal of the company, It can redirect the remote users to the Cloud Mail environment so that the remote user has full access to their Email and other services by reaching through the company network. The File service is located in the internal Network with the Domain controller, which is connected to the Policy decision point. The policy decision point is where the machine looks into the requests that are performed by the outside source and then compares that request to their policy to imply and see that if it fits into the description or not.

Similar to the traditional Defense-in-depth network diagram, we also have all internal switches that carry actions into the users and an intranet communication that comes into the Branch with Its own DNS server and the Server Environment to its HR department, Accounting Department, and CRM solutions department. The internal users are connected to a Wi-Fi network from the wireless adapter connecting to the client environment which gives them access to their company work environment.

# Design Comparison

In comparison with both the models, we can realize that both these Network architectures have different ways of providing a secure and safer work environment in a company and their different methods on how to secure information that is related to the company.

In terms for the Defense-in-depth Network diagram, we can see that the whole network itself is placed together in technology such as Firewalls, Endpoints, proxies etc. These are some of the defining features within the network diagram as the firewalls are responsible on what types of traffic comes into the network and what type of traffic goes out the network. Mostly in these Network architecture, we can see that there are three different levels of security, these levels are the Public level, the DMZ level, and the Internal Level of security. The Firewall put in the rules depending on the level of the Network Architecture. For Example, the firewall would give out 0 level of security in the public zone while it will give 100 level of security within the Internal network of the company, and a level of 50 in the DMZ zone. One of the cons in this type of architecture is that it is prone to many social engineering attacks because if an attacker can gain credential information, they can elevate their privileges to take control of the company system.

For the Zero-Trust Network diagram, this models is a highly secure based model because in this model, it is made to think that every connection that in on the premises of the organization is hostile. In this network, all the users and machines are authenticated. The traffic in the company flow by a set of policies that are requested to them through machines such as the Policy Decisions Point (PDP), which allocates to make sure that traffic requests are valid or not.

In conclusion, I would pick the Zero-Trust Network over the Defense-in-depth network because the Zero trust method tends to be more secure and we can ensure that user information can be securely stored without the thought of having them stolen at some point. Another implication is that the Zero-Trust-architecture is being implemented by many companies because of its efficiency.

# References

Wang, Shuangbao (Paul). “Dual-Data Defense in Depth Improves SCADA Security.” SIGNAL Magazine, 3 Oct. 2016, www.afcea.org/content/Article-dual-data-defense-depth-improves-scada-security.

Dostaler, Tristan. “Zero Trust Architecture – What It Is and What I Think of It.” Okiok, Okiok, 4 Feb. 2021, www.okiok.com/zero-trust-architecture-what-it-is-and-what-i-think-of-it/.

Sharma, Vikas, and Frank Alfieri. “Zero Trust Architecture - Modern Work Anywhere Architecture Without VPN.” Security Magazine RSS, Security Magazine, 7 Sept. 2021, www.securitymagazine.com/articles/96025-zero-trust-architecture-zta-modern-work-anywhere-architecture-without-vpn.

Editor, CSRC Content. “Policy Decision Point (PDP) - Glossary.” CSRC, csrc.nist.gov/glossary/term/policy\_decision\_point.

“Policy Enforcement Point.” Ldapwiki, ldapwiki.com/wiki/Policy%20Enforcement%20Point.

“10 Reasons Why Enterprises Need Zero Trust Security.” ColorTokens, 8 Dec. 2021, colortokens.com/blog/why-enterprises-need-zero-trust-security/.

“Network Topology Software.” Network Topology Software- Try It Free and Make Network Topology Diagrams, https://www.smartdraw.com/network-diagram/network-topology-software.htm.