# **Project 1 – Step 8 - Network Security Checklist**

Group 1

Ryan Briggs

John Cox

Kimberly Edmonds

Victoria Yuen

University of Maryland Global Campus

CYB 670: Capstone in Cybersecurity

Professor Yurek Hinz

October 13, 2021

## Network Security Checklist

In this section of the report, the team will discuss the different components of a network that facilitate secure data communications and network protection. Each of these components protect only a specific aspect of the overall computer network. They only provide adequate protection if they are correctly implemented and monitored. These components are:

1. Firewall
2. Secure Email Gateway (SEG)
3. Web Proxy
4. Access Control
5. Virtual Private Networks (VPN)
6. Intrusion Detection and Protection Systems (IDS & IPS)

**Firewall**

A network firewall is a network security device that monitors traffic coming into or leaving the local network. The firewall device is usually the first line of defense for a computer network and the networking device that secures the internal network from the untrusted outside networks. (Cisco.com, 2021) This is done using a set of rules preconfigured by network engineers and will apply those rules to all traffic that passes that firewall. To determine the rule sets the National Institute of Standards and Technology (NIST) publication 800-41 (Scarfone & Hoffman, 2009) should be used as a guideline for creating, implementing, and testing all firewall rules.

**Secure Email Gateway**

The SEG is an email gateway that protects the organization’s users from malicious email attachments, link, spam, phishing attacks, and malicious code. Like the firewall monitoring network traffic, the SEG monitors the email traffic. Also like the firewall, the SEG is configured to use rules to monitor email traffic. The SEG will watch the incoming email traffic for phishing attempts, spam, and malicious code, then block the emails to protect the users. The SEG will also watch outgoing email traffic from the users for sent unencrypted emails and prevent sensitive organizational data from leaving the network, then work to either encrypt the outgoing emails or prevent them from leaving the local network. (proofpoint.com, 2021)

**Web Proxy**

A web proxy server is a device that sits between the organization’s user’s computer browser and the open internet. There are two types of web proxies and they are forward and reverse. A forward proxy server will retrieve website for the organization’s users. This is done when the user’s browser requests a webpage from the internet, the request will be sent to the web proxy server. The web proxy server will then either go retrieve that webpage and return it to the user or block the request if it is a bad website from a preconfigured list. A reverse web proxy sits in the same location and handles requests but it handles requests coming from the internet to the organization’s servers. (Petters, 2021)

**Access Control**

Access control is the process and methods used to keep unauthorized users and devices off the organization’s network (VMware.com, n.d.). The access control system will conduct the identification, authentication, and authorization of users and devices to allow them access to network resources. This is commonly done through login usernames, passwords, pins, or cards (Patel, 2019). One example could be the physical devices and their connections to the network. If a new device is connected to the network, that device would not be allowed to access anything until it was given permissions to do so. Another example of access control, would be when a user logs into the network, the domain controller would give that user permissions and rights. Those permissions and rights would let that specific user access specific resources and not others. This would separate user’s permission and allow for network administrators to better control access to specific resources. This is an example of a Role-Based Access Control (RBAC), but other access control models exist and can be used to tailor access control for an organization (Patel, 2019).

**Virtual Private Networks**

A VPN can be divided into two types but serve the same purpose of providing a secure encrypted connection between two locations. The first is a personal VPN and that is to provide anonymity and privacy for someone when online. The second is a business or corporate VPN. A corporate VPN is to allow remote users a secure connection to an internal computer network (DeMuro, 2020). This allows a user to access local network resources safely and securely when away from the actual network. This VPN can also tie in the access control, discussed earlier, to require the user to provide a username and password to gain access to the network and by requiring logins, the organization can better monitor the network. Another type of corporate VPN, also called a site-to-site VPN, can also be used to link remote offices together and allow the sharing of network resources between two remote networks. This comes with a trust relationship between the two networks however, because if one location is compromised then it is possible to gain access to the other (DeMuro, 2020). These remote user VPNs and site-to-site VPNs will be used to facilitate data-sharing policies for the summit. If another summit member wishes to have access to a specific resource within the local network, they will have to use a login username, that will be provided, and a VPN connection. This will allow for a secure communication protocol and also the ability to monitor what those users are accessing and attempting to access, while still allowing secure communication and data-sharing.

**Intrusion Detection and Protection Systems**

An Intrusion Detection System (IDS) is a system or software that monitors network traffic for possible malicious activity and then throws an alert to Informational Technology (IT) security personnel for further action (Barracuda.com, n.d.). This type of device or software is passive and does not block or stop the activity. A firewall will block traffic based on a set rule, but an IDS will watch the traffic for either a signature or anomaly, detect it, and then notify security. In order to automatically block or stop any malicious network activity, an Intrusion Prevention System (IPS) is used. However due to the distinction between the two devices, they are deployed in different areas of the network. For example, the IDS should be deployed to watch all internal network traffic, where as the IPS should be deployed behind the firewall but before the internal network. This allows all traffic to flow through it and be able to block any malicious traffic (Barracuda.com, n.d.).

## References

Barracuda.com. (n.d.). *What is an Intrusion Detection System (IDS)?* <https://www.barracuda.com/glossary/intrusion-detection-system>

Cisco.com. (2021). *What is a firewall?* Cisco. <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

DeMuro, J. P. (2020). *What is corporate VPN?* TechRadar. <https://www.techradar.com/vpn/what-is-corporate-vpn>

Patel, P. (2019). *Access control in computer network*. GeeksforGeeks. <https://www.geeksforgeeks.org/access-control-in-computer-network/>

Petters, J. (2021). *What is a proxy server and how does it work?* Inside Out Security. <https://www.varonis.com/blog/what-is-a-proxy-server/>

proofpoint.com. (2021). *Secure email gateways definition & comparison.* Proofpoint. <https://www.proofpoint.com/us/threat-reference/email-gateway>

Scarfone, K., & Hoffman, P., Guidelines on firewalls and firewall policy (2009). <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

VMware.com. (n.d.). *Network access control*. VMware. <https://www.vmware.com/topics/glossary/content/network-access-control>