ITN 263 – Project Part 2: Firewall Selection and Placement

A diagram of a flowchart

AI-generated content may be incorrect.

To provide maximum security in the network, assigning firewalls for internet traffic, on the web server, and the workstations and servers will be vital in ensuring proper access and reduced attack surfaces. Firstly, traffic from the internet is met by a next-generation firewall which not only filters unwanted traffic, but also provides intrusion detection and prevention, deep packet inspection, advanced malware detection, and threat intelligence to identify known threats. These additional security measures provide comprehensive protection in just one security device. Through integrated intrusion detection and prevention, threats are detected and prevented in real time. Deep packet inspection inspects the full packet of traffic rather than just the header which will identify threats hidden in the body of the packet. Advanced malware detection and threat intelligence feeds combine to block domain and IP addresses that are associated with known signatures of malware and threats.

The public web server is protected with a web application firewall to prevent attacks such as SQL injections, cross-site scripting attacks, and cross-site forgery attempts. This is done by examining and inspecting malicious HTTP and HTTPS requests made to the web server and blocking them to stop these attacks. This firewall will not only protect the web server but will also protect the network by not allowing an attacker to take a path onto the internal network. After the web application firewall, there will be an internal firewall to block any traffic that makes it past the next-generation firewall or any malicious traffic from the web server. Placing an internal firewall after the web server also makes a demilitarized zone which will isolate the web server because it can be accessed by the public to prevent anyone from finding a way onto the internal network. This will effectively make the network more secure by first examining and filtering traffic from the internet onto the web server and then examining and filtering the traffic from the public web server to prevent it from coming onto the network while still allowing legitimate network traffic to continue.

Finally, to protect each individual workstation and server, they will be equipped with Windows Defender Firewall to allow only necessary inbound and outbound traffic. For example, workstations should allow TCP ports 80 and 443 for HTTP and HTTPS traffic while servers should allow TCP port 3389 for Remote Desktop Protocol (RDP) connection through VPN for remote workers.

To create secure authentication to internal network resources, I recommend using IEEE 802.1x as it provides the most comprehensive authentication services. As a user sends their authentication credentials to the authenticator, it is forwarded to the RADIUS authenticator that checks the credentials against the database which stores accepted authentication credentials. The authenticator then decides to allow or deny the request based on it finding a match with the credentials in the database. If the request is accepted, the user is allowed access to the internal network which prevents others who are not authenticated from easily accessing internal network resources. Using 802.1x as our authentication method provides a simple, yet effective authentication method against unauthorized devices.

Citations:

Stewart, James Michael, and Denise Kinsey. *Network Security, Firewalls, and VPNS*. Jones and Bartlett Learning, 2021.

“What Is 802.1x? How Does It Work?” SecureW2, 13 Jan. 2025, www.securew2.com/solutions/802-1x.

“What is a Next-Generation Firewall (NGFW)? | Cloudflare.” Cloudflare.com, www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/. Accessed 30 Mar. 2025.

“What is a WAF? | Web Application Firewall Explained | Cloudflare.” Cloudflare.com, www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/. Accessed 30 Mar. 2025.