EP2520/FEP3250 Building Networked Systems Security (BNSS)

Initial requirement analysis 1-3

Group 6: Ziyang Song, Enze Wang, Keyao Huang, Zhiyuan Lin

February 25, 2023

1 Project requirements

1.1 Basics

Employees should be able to connect to the cooperate network (two servers). Employees can exchange files (SFTP, confidentiality, integrity and authenticity). For Mobile devices/untrusted devices two-factor authentication are needed. For employees with laptops should be able to work remotely via VPN (except sensitive operations). Routers in both Stockholm and London should provide wired/wireless connections (laptops and mobile devices). There will be working hours restrictions on-site for critical server (We assume the web server in Stockholm is critical) and no working hour restriction for file exchange server(less critical server).

1.2 Securities

Authentication for users that request for services. Secure Connection between employees and servers, employees and employees, logging network traffic and requests should be satisfied. Information exchange should be encrypted, authenticated and integrity ensured. For Wireless Access, Authorization and Authentication should also be guaranteed other aspects includes alerting for attacks, preventing clogging DoS, guaranteeing domains cannot be exploited or employees misleading, handling equipment stolen and credentials compromised.

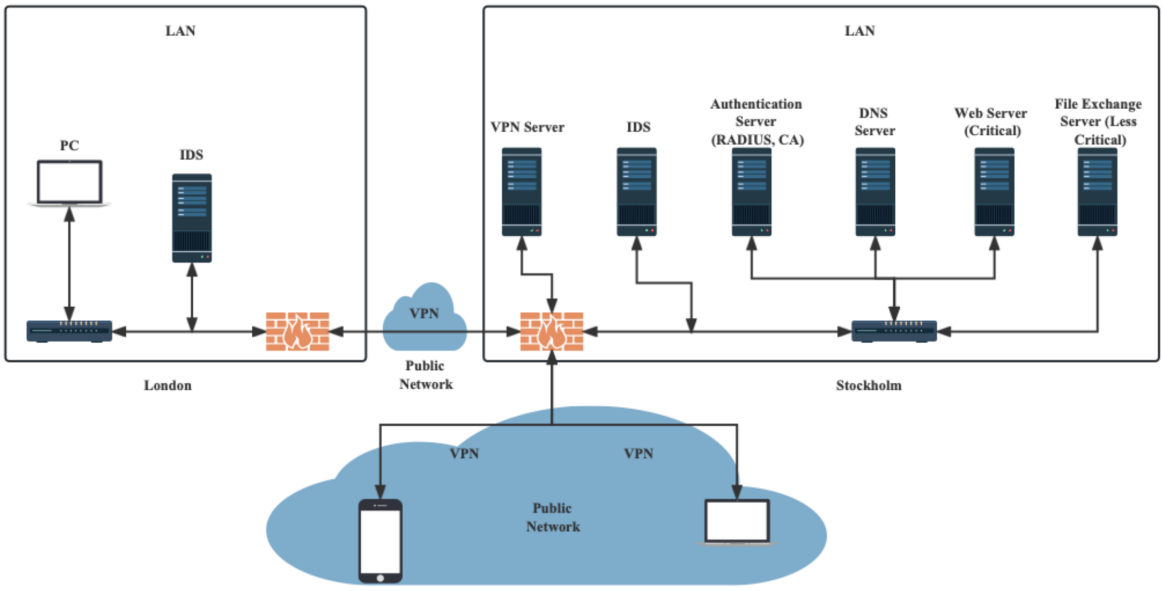

Figure 1: Topology of Network

2 Implementation Details

2.1 Explanation of Network Topology Diagram

As shown in the figure, the whole network architecture is divided into the London part and the Stockholm part, both of which have their own LANs. It is worth mentioning that our firewall and VPN server are

deployed on the router, but we have drawn the firewall and router separately for the sake of brevity of the drawing. The two LANs communicate via VPN, and employees who are not in the company also need to connect to Stockholm's company via VPN. In both LANs we have deployed IDSs to monitor incoming and outgoing traffic. In the Stockholm company we set up four servers: authentication server, DNS server, web server and file transfer server. Besides, we defined the web server as critical and the file transfer server as less critical.

2.2 Employees Connect to the Corporate Network

Install two servers (e.g., Linux servers) with appropriate operating systems. Configure the servers for secure remote access for employees, for example, by using SSH or Telnet. Implement firewalls on the routers to restrict inbound and outbound traffic, and allow only the necessary protocols.

2.3 Exchange Files between Employees

Install and configure an SFTP server on one of the servers to allow employees to securely transfer files for only employees that transfer files to each other can access the files. Implement SSL/TLS encryption for confidentiality, integrity, and authenticity. Enable user authentication to access the SFTP server by using public key infrastructure (PKI) or password-based authentication.

2.4 Authentication

Implement two-factor authentication (2FA) to secure remote access from mobile devices and untrusted devices. Use a device management solution, such as Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solution, to manage and secure the mobile devices. We use FreeRADIUS[1]which is a open source authentication tool based on RADIUS protocol which will handle requests from the router for clients who attempt to access other servers. We use OpenSSL[3] as library to implement PKI and encrypted communication on RADIUS server with CA.

2.5 Securely Work Remotely

Establish a Virtual Private Network (VPN) solution to allow employees to securely work remotely from their laptops and allow communicate between two routers (London and Stockholm). Implement encryption and user authentication for the VPN connection. Disable sensitive operations when working remotely by implementing network access control (NAC) policies. We intend to firstly flash OpenWRT[4] on both routers in order to establish VPN between them. We will use openVPN[2] and the server and client are included in OpenWRT firmware. For employees who are not in the office, they need to install the OpenVPN client on their cell phones or computers to connect to the OpenVPN server located in Stockholm.

2.6 Wireless Connections

The wireless would be implemented in IEEE 802.11. Configure the Access point to support secure connections, by enabling WPA3 encryption for wireless connections.

2.7 Firewall and IDS: Internal Security

In order to be sure that only internal network users can access the servers in Stockholm, we need to place a firewall and set the firewall rules on routers to block all packets from outside public network except VPN tunnels. We plan to use Iptables to achieve the firewall or utilize the built-in firewall function of OpenWRT. we also need Intrusion detection system for detection of potential network attacks, located at Stockholm site and London site, independent of but connected to router. After discussion, we plan to use SNORT[6] to achieve IDS, which is one such open-source IDS. SNORT can also deal with Dos attacks as we can detect unwanted behaviours to our internet.

2.8 Other Security

SNORT can also deal with Dos attacks as we can detect unwanted behaviours to our internet. We can prevent employees from being misled on the internet and other DNS attacks(DNS hijack) by using

DNSSEC. Any equipment stolen and credentials compromised should be reported and get the certificates revoked as soon as possible.

Appendix

Improvements based on reviews

Based on the feedback, we have refined some details. We rearranged the DNS server in Stockholm to prevent DNS attacks. We also set up IDS at our London office as well. Since we need to allow the London employees to access the network through the London router, IDS is needed. Finally, we redrew the topology of the network structure to show the network architecture more clearly.

References

[1] FreeRADIUS, https://freeradius.org/documentation

[2] OpenVPN, https://openvpn.net

[3] OpenSSL, https://www.openssl.org/ -crypto library and toolkit, implementing a broad gamut of popular crypto primitives. It allows you to create keys, certificates, a CA. Generic public key cryptography and TLS/SSL. A free reference: https://www.feistyduck.com/library/openssl-cookbook/online/

[4] OpenWRT, https://openwrt.org/docs/guide-user/services/vpn/start

[5] Iptables, https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-iptables

[6] SNORT, https://www.snort.org/?/