EP2520/FEP3250 Building Networked Systems Security (BNSS)

Initial requirement analysis 1-2

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

February 10, 2023

1 Project requirements

1.1 Basics

1. Employees connect to the cooperate network (two servers)
2. Exchange files between employees (SFTP, confidentiality, integrity and authenticity)
3. Mobile devices / untrusted devices: two-factor authentication
4. Laptops: securely work remotely (VPN)(except sensitive operations)
5. Routers: provide wired/wireless connections (laptops and mobile devices)
6. Working hours restrictions

1.2 Securities

1. Authentication: digital identity
2. Secure Connectivity: employees → servers, logging network traffic and requests. Employee ↔ Employee
3. Confidentiality and Anonymity: Information exchange encrypted, authenticated, integrity.
4. Secure Wireless Access: Authorization and Authentication
5. Other: alerting for attacks, preventing clogging DoS, guaranteeing domains cannot be exploited or employees misleading, handling equipment stolen and credentials compromised

2 Implementation Details

To design a simple secure network that fulfills the requirements, we can implement the following steps:

- Employees Connect to the Corporate Network:
  - Install two servers (e.g., Linux servers) with appropriate operating systems and security patches.
  - 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.
  - Establish a domain name system (DNS) server to assign static IP addresses to the servers.
- Exchange Files Between Employees:
  - Install and configure an SFTP server on one of the servers to allow employees to securely transfer 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.
- 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.

- VPN: 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 build the openVPN server on Stockholm's router to accept remote connections from employees who need to install openVPN[2] on their phones or computers.
  - On both routers, we also need OpenWRT[4] in order to run VPN on the router.

- Routers: Wireless Connections:
  - Install routers that support both wired and wireless connections.
  - Configure the routers to support secure connections, by enabling WPA3 encryption for wireless connections.

- 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 for the server and set the firewall rules to block all packets from outside public network except VPN tunnels.
  - The firewall is expected to be installed in the web server to prevent unauthorized users which are from external networks to get access to the internal network. We plan to use Iptables to achieve the firewall.
  - we also need Intrusion detection system for detection of potential network attacks. After discussion, we plan to use SNORT[6] to achieve IDS, which is one such open source IDS.

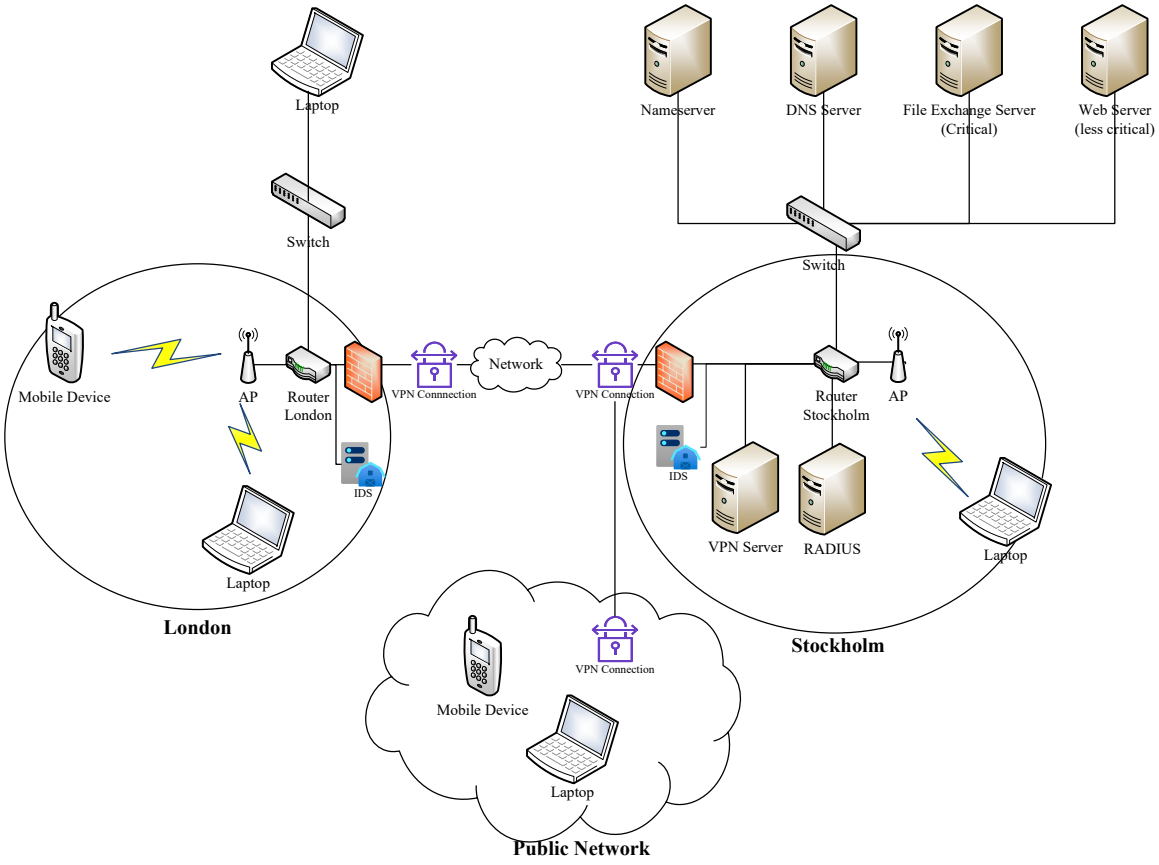

Figure 1: Topology of Network

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/?/