Analysis and System Design

HAIDA LU | YANG YANG | ZIJIAN HUANG | ZHICHAO ZHOU
haida | yangy2 | zijianh | zhizho @kth.se

February 12, 2021

1 Analysis

By analyzing the introduction file, we conclude these network security system requirements:
1. Only computers with IP addresses from the headquarters or the branch should be accessed to connect to the internal network.
2. Employees should take the two-factor authentication when not using their cryptographic credentials to access the secure web server.
3. Only trusted users including employees using their personal laptops at home can be accessed to the main web server containing critical data.
4. Information exchange between two networks should be protected, and all communications between server and user should be encrypted and authenticated.
5. Employees can only exchange files with other ACME employees, and confidentiality, integrity and authenticity should be guaranteed in this process.
6. Authorization and authentication should be done via the wireless network. And using this WiFi, visiting employees can connect to the Stockholm headquarters.
7. Network traffic should be logged.

2 Design

2.1 Employee Authentication

To guarantee security, authentication is necessary for employees who want to be trusted. We use authenticated digital identity and device to guarantee authentication. Each employee has a digital identity verified by digital certificates and a device for authentication.

When applying for authentication, the employee needs to show their digital identities, then the authentication server will send his device a verification code. The employee can make the authentication by showing this code to the server.

2.2 Secure Connectivity

To ensure secure connectivity, we set up a secure web server in the headquarter network. This server, which is implemented on a virtual machine, integrates the functions of firewalls, Network Access Control (NAC), and Virtual Private Networks (VPNs) gateways.

VPNs can build a tunnel between the headquarter network in Stockholm and the branch networks in London so that visiting employees in London are allowed to access the secure web servers in the Stockholm headquarters. More precisely, two gateways are creating a link through some specific handshake protocols (e.g. based on X.509 certification). Data exchange will start after the establishment of a handshake and the session also needs encryption before sending data (e.g. AES encryption). Besides the gateways for building VPNs, firewalls are also required due to the need for preventing unauthenticated devices out of the Stockholm headquarters or the London branch from connecting to the internal network. To be exact, a firewall is needed between the corporate network and the external network. By configuring the firewall to filter packets according to source IP addresses, the connecting requests not from the corporate network will be denied. There should also be a firewall close to the secure web server and log all packets to the web server before they reach it.

As for the tools to achieve such functions, we consider OpenVPN for building VPNs and IPtables for firewalls. They are both available on Linux which is the platform we will use to set up the server.

2.3 Confidentiality

To achieve confidentiality, a VPN tunnel will be built between the corporate network of the headquarters in Stockholm and the branch in London, and all communication between our VPN gateways should be encrypted and authenticated. Moreover, another proxy server will be connected to the internal network so that employees from their homes with their personal laptops can send requests to the proxy for access to the internal network. Information exchanged between the proxy and the internal network will also be encrypted and authenticated. In this way, the main web server containing critical corporate data will be accessed only by trusted users. The secret keys are obtained from the PKI.

2.4 Secure Wireless Access

When connecting to the Wifi, there is an authentication. We set up a NAC server in Stockholm, employees need authentication to get access to this router. And this router will be set on the internal network so that messages from this router can pass through the firewall and devices connected to the router can access the internal network.

2.5 Secure File Exchange

To promise confidentiality, employees will apply for a key from PKI and encrypt the file. In this process, employees should prove their identity to get the key. And only the public key of those who have been authenticated can be applied. To promise the integrity and the authenticity of the file, we will use Message Authentication Code (MAC).

2.6 Other Security

Intrusion detection systems (IDS) can be built so that when attackers try to infiltrate our corporate network, they can set off the alarm for intruders. IDS is able to help monitor the whole security system for malicious attacks and report such activity when discovering it. It is possible that IDS gives a false alarm, so fine-tuning is required when first installing IDS. In other words, we should properly configure IDS so that it can learn what normal activity looks like compared to suspicious activity [1].

3 Topology

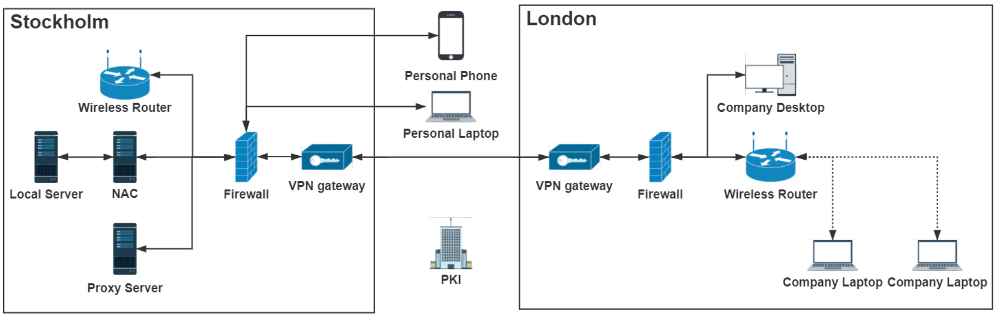

Figure 1: Topology of System

4 Revise Explanation

According to the review for our draft, we have revised our design report. The expression has been improved, especially for some wordy sentences. Also, more precise implementation details are added. For example, VPNs handshake could be achieved based on X.509 certification. Moreover, the review also indicates that the PKI configuration should be clear, such as the trust model. Considering that further guidelines about the NSS-VPKI will be announced later, we will add more details about the implementation after that.

References

[1] https://www.geeksforgeeks.org/intrusion-detection-system-ids/#: :text=An%20Intrusion%20Detection %20System%20(IDS,harmful%20activity%20or%20policy%20breaching.