KTH Computer Science
and Communication

ACME Scandinavia

Analysis and System Design Draft

Group 18

Junjie Shan	jshan@kth.se
Yuchi Zhang	yuchi@kth.se
Gaoya Wang	gywang@kth.se

EP2520 - Building Networked Systems Security (BNSS)
Examiner: Panos Papadimitratos (papadim@kth.se)
Main Teaching Assistant: Cihan Eryonucu (eryonucu@kth.se)

March 8, 2021

1 Requirements

According to the project description, the following requirements should be satisfied:

- There are two independent networks that locate in London and Stockholm(headquarter). Each network can communicate with each other via a secure connection and the traffic should be hidden from a third party.
- The web server is set in Stockholm and requests to the web server and network traffic should be logged.
- These two networks should be protected from outsiders, so no one from outside can access the information or change the information inside.
- There is a certain number of desktops in both networks which can connect to the internal network. Also, visiting employees in London can connect their cooperate laptops using the wireless connection provided in London to access the Stockholm network.
- A two-factor authentication is used when an employee tries to connect to the web server using devices other than ACME specified devices.
- The employees should be able to transfer files to each other using their mobile devices and no one else should be able to transfer files with ACME employees.
- Each network should be equipped with an intrusion detection system that can identify possible attacks against infrastructure.

2 System Design

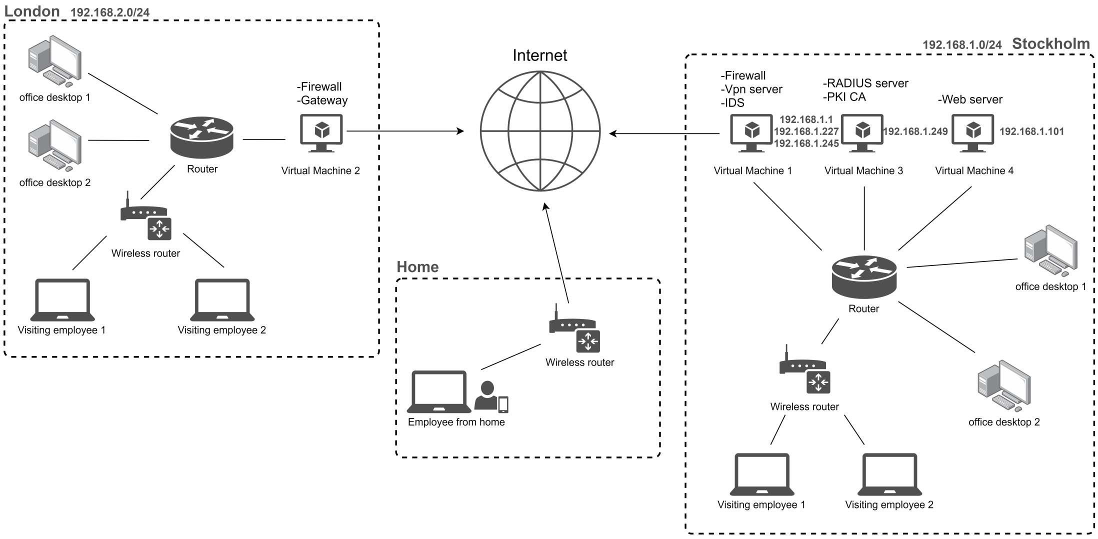

Figure 1: Network topology

2.1 Confidentiality

Confidentiality needs to be provided for all traffic between the London and Stockholm network, as well as all traffic inside the Stockholm office.

Internal Security

At each network access point in London and Stockholm network, a firewall with stateful packet filter will be placed. The firewall will use iptables to prevent any access to the network from unauthorized users. With proper authentication, it is assumed that no outsider has physical access to the internal network in the Stockholm office.

External Security

All the traffic between London and Stockholm offices should be sent using Virtual Private Network (VPN) in SSL tunnel mode. This will be implemented using OpenVPN and OpenSSL software.

All the traffic between authorized users in the outside network and the web server inside the Stockholm network should be encrypted using SSL as well. Besides, all the traffic from and to the web server should be logged, this will be implemented using an HTTPS Apache server.

2.2 Intrusion Detection System

However, we still need an Intrusion Detection System (IDS) to monitor the network traffic and notify us if there were any penetration detected. We will install an open source IDS called Snort at the Stockholm office, including both anomaly and signature detection.

2.3 Authentication

Every device provided by ACME should be assigned with a certificate that can be authenticated by ACME. For that, we will use Public key infrastructure (PKI) to manage certificates. This will be implemented on a server inside the Stockholm office using OpenCA software.

Employees using their own devices should authenticate themselves every time when they try to connect to the internal network. For that, we will set up a two-factor authentication system on the web server inside the Stockholm office, employees can authenticate themselves through the web server using both their digital certificate and the phone provided by ACME. This will be implemented using Google Authenticator.

2.4 Secure Wireless Access

To prevent outsiders from connecting to the inside network through a wireless access point, the WiFi will use WPA2 Enterprise (IEEE 802.11i) and EAP-TLS with a RADIUS server to authenticate users using digital certificates.

2.5 Secure File Exchange

For the employee using mobile devices to share files with each other, certificates are needed to authenticate users to make sure only employees of ACME can exchange files. Also, a file exchange server will be set so that users can transfer their files without knowing another user's IP address. The security of the transfer is ensured by using TLS for all communication. This is done with client authentication enabled which makes it so that only clients with valid certificates will be able to access the server and thus perform the file transfer.

3 Configurations

3.1 VPN

VPN in our solution is provided by the OpenVPN that uses the SSL/TLS. The authentication is provided by the radius server that is used also for authenticating users when connecting to the Wi-Fi router. To establish a connection from home, two factor authentication needs to be used. We enabled the Google authenticator for users logging in at home. Employees at home can use their usernames, passwords, and their Google Authenticator's tokens to log into the webpage of VPN server and download client configuration files and certificates automatically distributed by the OpenVPN access server, which can be easily revoked by the VPN server operator later.

3.2 PKI

We use a standalone computer to work as CA and use CFSSL, CloudFlare's open source PKI toolkit to generate and sign certificates for servers and users. The CA has a self-signed certificate with expiry set to 365 days, it can be use to sign, to generate cipher keys and authentication. Also, the revoking can easily be done by the CA manager using CFSSL. When employees apply for a certificate, they need to provide a json file including their personal information, then use genkey command to generate their keys and Certificate Signing Request (CSR), which then be signed by the CA. An entry will be added to Certificates table once CA signs a certificate. When revoking a certificate, using revoke command, then the revoked certificate will be removed from the Certificate table.

Employee and server: We use CFSSL to generate certificates and import them into servers and employees' devices. Each server and employee has a certificate with expiry set to 365 days, the key size is 2048 using RSA.

3.3 Wi-Fi Security

We choose to use two routers as two gateways for the Stockholm sub-network and London sub-network, so the iptables rules will be directly applied to the routers. Also, the router has been set up in WPA2 Enterprise mode in order to interact with the radius server to support wireless authentication with independent user accounts. And we installed OpenVPN on the London router to connect the London subnet to the main network in Stockholm.

3.4 Radius Server

A radius server is set up on a virtual machine inside the Stockholm internal network for authentication purposes. We choose freeradius and daloradius to manage clients and users. And we added some access points like VPN server and Wi-Fi router as clients and employees as users with password protected, so users may use their usernames and passwords to authenticate themselves and log into the internal network.

3.5 File transfer

The file sharing application is working with ownCloud server. This server is set to run at VM3 (IP 192.168.1.101). The purpose of this server is to allow the different users to share files to each other without knowing each other's IP-addresses. This allows users to transfer files between each other without having another channel of communication with each other.

The data transfer is protected by ownCloud's comprehensive encryption, which uses up to three layers of safeguards: encryption in transit, encryption at rest and end-to-end encryption (E2EE). If a user wants to share files or download files. He must use Openvpn to connect to the inner network of Stockholm, then he have to login the ownCloud server within username, password, and one time 6-digit pincodes (OTP). All the three elements (vpn, password and OTP) are necessary to access to the ownCloud server.

3.6 Snort

The snort and snowl are set up in Stockholm internal network, and we import some rule sets from snort.org and detailed rules can be customized according to the specific security requirements of the internal network. And a swatchdog is deployed to monitor the alert logs of snort, and automatically send emails about the chosen kinds of alert to the designed email address. Also, we add a rule to alert any ICMP packet inside the internal network only for demonstration.

3.7 Firewall

The firewall was configured with the default DROP policy which means that all traffic that is not specifically listed to pass through will be dropped. The allowed traffics are:

- All traffic from any source to ports forwarded to VPN server
- All traffic from any source to VPN Access Server
- All traffic with RELATED or ESTABLISHED state
- SSH traffic to all virtual machines, for remote configurations of machines
- Internal traffic to the router for configuration of router and web management

4 Appendix

4.1 Changes after peer-review

We made some changes after peer-review:

1. We correct some grammar errors.
2. We changed the part about internal network communication, and we decided to encrypt the communication between any two users, since an internal host may be compromised, so encrypt internal communication is still important.
3. We decided to use an off-the-shelf solution to the file transfer, since developing an app ourselves is time-consuming and may introduce some vulnerabilities.
4. We made the London part of the network topology more detailed.

Considering that there may be some differences between our design and final implementation, we will explain our software choices and detailed configuration later in the final report.

4.2 Configurations

4.2.1 Tools used in our project

- VPN: OpenVPN & OpenVPN Access Server
- Firewall: IPTables
- Radius: FreeRadius
- IDS: Snort
- Router: OpemWrt
- PKI: CFSSL
- Fire sharing: ownCloud & FreeOTP

4.2.2 IP addresses allocation

- Stockholm office: 192.168.1.0/24
- London office: 192.168.2.0/24
- Web server in Stockholm: 192.168.1.101
- Firewall, IDS, Vpn server in Stockholm: 192.168.1.1, 192.168.1.245, 192.168.1.227
- RADIUS server, PKI CA in Stockholm: 192.168.1.249
- Firewall, Gateway in London: The IP of London Router
- Employee from home: Any IP

4.3 Possible improvement in the future

1. Define security groups for different users for different access rights.
2. Combine the IDS with firewall settings to stop possible internal attacks and block suspicious users.
3. Set up customized snort rules and iptables rules in every server for potential users.