Building Networked Systems Security (BNSS)

Project Implementation

Group 6

Fuhao Huang(fuhao@kth.se)

Quanyu Tao(quanyu@kth.se)

1. Analysis needs and precision of security requirements

1.1 Overview

In this project, three main functions need to be achieved. First, computers and mobile phones in Stockholm headquarters need to be able to connect to the main server in Stockholm. Second, employees' devices in London's branch can also connect to the main server in Stockholm through VPN. And they should be verified in two ways: Certificate or two-factor authentication. Besides, all connections should be built securely. Finally, employees' mobile phones can exchange files and the confidentiality, integrity, and authenticity of the file exchange process should be guaranteed.

To achieve these several goals, two company networks are needed separately in Stockholm and London. Besides, several different kinds of software and tools are also needed to be deployed to implement these functions. Here is a detailed analysis of the requirements and software.

1.2 Needs analysis

From the material, a few needs and precision are concluded as below.

1.2.1 Two ways to make employee authentication before VPN connection and internal service :

(a) Use an authenticated laptop and mobile devices (with certificate) access to the system directly.

Implement software: easy-rsa.

To make authentication, we use RSA asymmetric encryption algorithm. In the initialization phase, the CA server should assign a certificate to every employee's device, which is converted into the employee's certificate and stored in the certificate library. In the process of connecting the employee to the server each time, the employee's device sends the certificate to the server. The server uses the CA's public key to decrypt the digital signature to generate an information digest and redirect the content of the information to generate a hash digest. The employee's identity can be determined after the comparison between two hash digests. From then on, the employee's identity can be authenticated, and a symmetric key will be sent. In a subsequent communication, the sender and receivers use the symmetric key for encryption to achieve the purpose of secure communication.

Easy-rsa is used to build a CA server on VM1 and then create a Public Key Infrastructure (PKI). First the root public and private key pair for Certificate Authority should be created by an easy-rsa script, then we can get public certificate file (ca.crt) and private key(ca.key) of our CA. The public certificate of the CA should be kept by every server and client to verify that they are trusted by the same CA, and the private key of CA is used to sign certificates for servers and clients. The private key should be kept secretly, and a CA password should be used when sign other certificates to guarantee the security.

Employees who use the company's devices with certificates can just authenticate themselves with certificates signed by CA. So, when they are in internal networks, they can just use any services and do not need to input passwords. Because they can be authenticated with assigned certificates. Besides, if they are in external networks, they can also use certificates to log in VPN server.

(b) Use other unauthenticated devices (without certificate) with two-factor authentication way.

Implement software: Google Authenticator& Kerberos

For other unauthenticated devices, users need to input their username and password on the web page and Using Google Authenticator to have two-factor authentication.

Google Authenticator is a two-factor authentication application for mobile and server devices. It first uses pseudo-random numbers to generate a large number of original keys, commonly known as seeds.

Then the key is selected through the calculation of time and other encryption algorithms. The principle of all this should be based on the synchronization of the client and server time, to achieve the purpose of secondary verification.

If they use their own devices, they will not have any certificate signed by the CA. When they connect to the VPN server, they should use the account name and password plus Google authenticator(two-factor authentication). The password is the combination of the original password and numbers on Google authenticator. When they are in the internal network, they need to use Kerberos to get a ticket to access any web service. They also need an account name and password for getting the ticket.

(c) Password management.

We use Kerberos to store the password information. Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. We use Kerberos to make mutual authentication.

1.2.2 File exchange

(a) Authentication before File exchange.

Implement software: OpenSSL / Google Authenticator

Encrypt files to protect the security of the files and Use verification to ensure the file integrity.

(b) Implement software: Seafile

We use Seafile to exchange files. Seafile is an open-source file sync and share platform with high reliability and performance. It allows users to host the server on their hardware. The core feature of Seafile is file sync and share. It provides client apps for most operating systems like Windows, Mac OS, Linux, iOS, and Android. It also provides a user-friendly web interface for accessing files in a web browser.

1.2.3 Connectivity Security

(a) Establish a firewall and discard all the requests from third parties.

Implement software: firewalld

In this part, we will place a firewall at each server of each network in Stockholm (both Stockholm and London), which will check all the traffic going to and coming from our servers. For security requirements, firewalls work in public zone on all servers, which means they are configured with default drop policy so they only approve traffic from some specific services and ports. Assume that we do not trust any other computers and servers on the network, so we only allow the required ports and services. For external traffic, we only allow connection requests to the VPN server (on port 1194) from any source. For internal traffic, we only open some specific ports on different servers which provide different service. For example, we only allow traffic through port 443 on our seafile server because users need to access the seafile server with HTTPS. Traffic to other ports will be dropped with the default drop policy. Besides, we also open port 22 for SSH connection to config our servers.

(b) Authentication before Communication.

In this part, each user should be authenticated through a certificate or two-factor authentication. Only authorized users can start communicating with others.

1.2.4 Secure connect Network

(a) Use VPN to establish a new connection between headquarter and outside Stockholm.

Implement software: OpenVPN

Using VPN can guarantee secure connections between Stockholm and London. We use OpenVPN to implement VPN between headquarters and branches (based on SSL), and all messages will be encrypted in VPN. Besides, if employees work at home, they should also use VPN to connect to the company's local network.

In this part, the VPN server is implemented on VM5. It can generate certificate and private key for each client and request CA to sign the certificate. Then the server can generate a config file for each client using client's certificate and private key. The VPN server can authenticate client in two ways: using certificate or using two-factor authentication (password + Google authenticator). Certificate is used for client who has company's devices, and two-factor authentication is used for client who uses their private devices.

For keys generation and asymmetric encryption, the server and client will use modern Elliptic Curve Cryptography (ECC). ECC is a substitute for RSA, and it is much faster than RSA. When a client and server attempt to establish a shared symmetric key, they can use ECC because the numbers are much smaller and the computations are faster[7].

In order to increase security, we also use a pre-shared static key (tls-key) to encrypt control channel packets in control channel. Encrypting control channel packets has three main advantages[8]:

It provides more privacy by hiding the certificate used for the TLS connection.

It is harder to identify OpenVPN traffic.

It provides post-quantum security, against attackers who will never know the pre-shared key.

With the help of control channel encryption, the VPN server can quickly check incoming packets. If it is signed with a pre-shared static key, it will be processed. Or it will be dropped because it may from an untrusted source. Then the server can cope with unauthenticated traffic and DoS attack.

When connecting to a server, the client sends the encrypted key to the server in the first packet. The server then decrypts that key, and both parties can use the same client-specific key for tls-crypt packets[8] .

(b) Authentication before connecting to WLAN.

Implement software: freeradius & OpenWrt

We use WPA2 EAP-TLS authentication in routers before connecting to routers every time. We establish a radius server in a virtual machine. Every time client request to connect to the routes, it needs to input his private username and password to radius server, and the server will verify them in the MySQL database.

The routers in London will be equipped with firmware OpenWrt, which will be configured as an OpenVPN client. Therefore users in Stockholm can access to the internal network as soon as they make the connection with routers.

Besides, port 1812 is used in radius authentication. All the traffics connected to this port are configured to be forwarded to radius server by gateway server.

(c) Authentication before connecting to VPN server (VM5).

There are two ways of authentication, which are used by different kinds of clients.

For clients who use company's devices:

The company's devices have certificates so they can just use them to authenticate instead of using account name and passwords. This case will use udp on port 1194.

For clients who use their own devices:

Their own devices do not have certificates so they have to use their own account and passwords to log in and use VPN to connect to the company's local network. Besides, for security goals, they should also use Google authenticator as two-factor authentication.

1.2.5 Intrusion alert

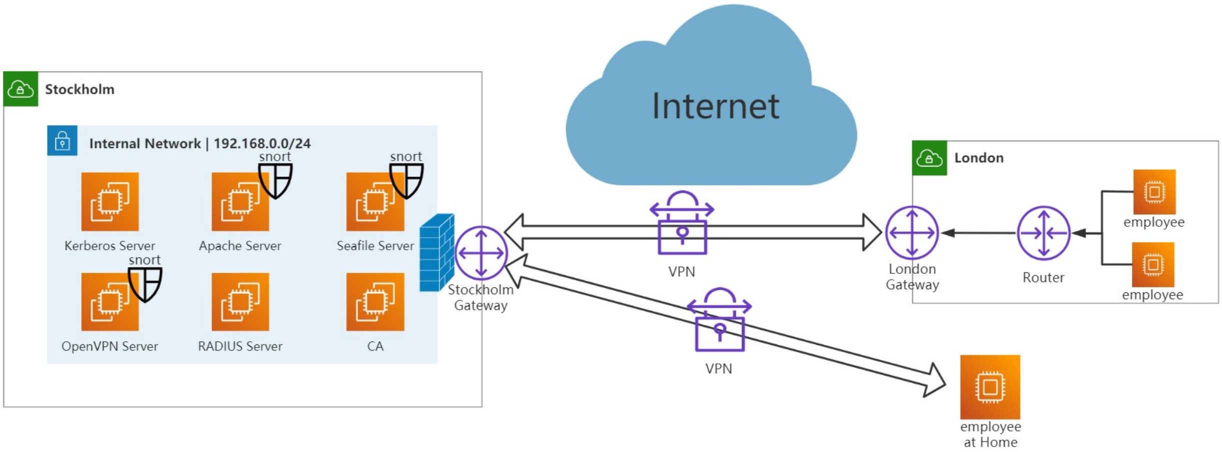
(d) Identify the attack when attackers try infiltrating networks. (snort)

Implement software: Snort

Configure snort in network intrusion detection mode. Snort will match each packet with a configured rule set and take corresponding actions.

We implement Snort in the VPN server and the Apache server. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users. If anyone in the external network ping the public IP address of the VPN server, or if anyone in the internal network ping the private IP address of the VPN server, Snort will also generate an ICMP alert in the command line, which shows the source of the ping.

2. Network Topology



3. Software and tools

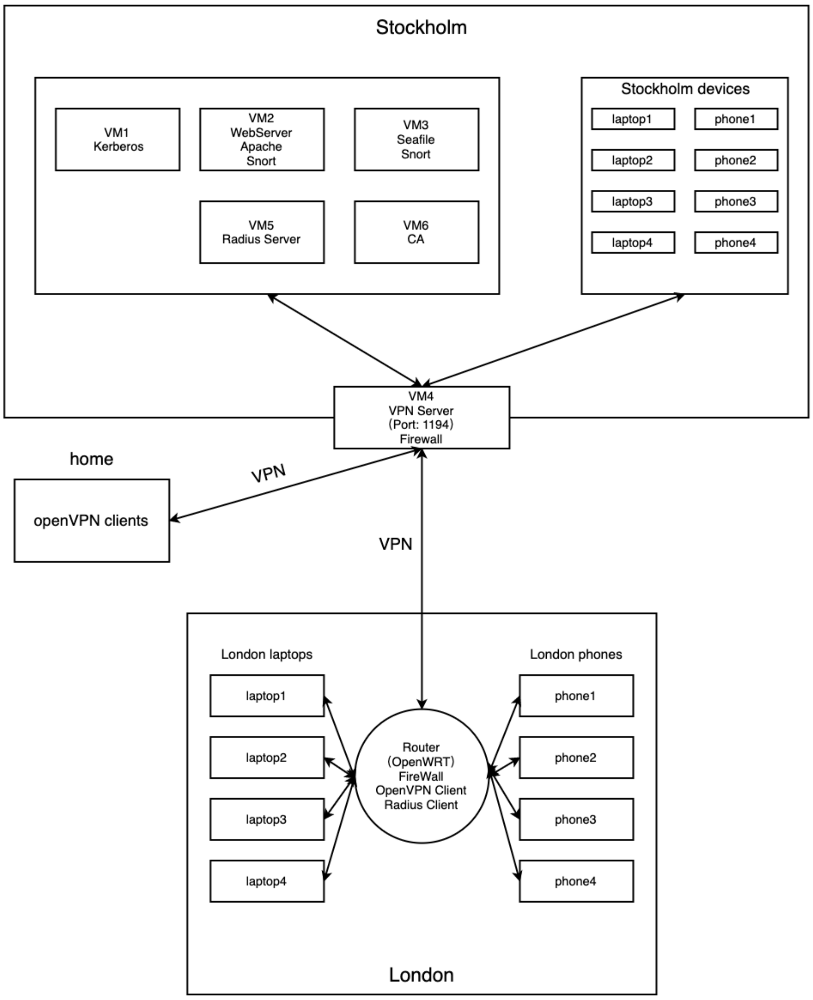
3.1 Analysis

For the main server in Stockholm, Six virtual machines are needed to achieve these functions. The Kerberos server will be set up on VM1. The web server will be set up on VM2, which uses Apache server and MySQL software. On VM3, we deploy the SeaFile server on it. VM4 is the VPN server, it controls all the VPN connection and process authentication before connection. Radius server will be deployed on VM5. In VM6, PKI and CA will be set up by OpenSSL. Besides, IDS will be set on VM2, VM3 and VM4 by snort.

Firewall, WPA2 enterprise, and radius client will be set on the gateway Server in Stockholm. For the router in London, WPA2 enterprise and radius client will also be deployed.

SeaFile client will be deployed on all laptops and mobile phones, regardless of their location. As for devices in London, OpenVPN clients will be needed.

3.2 Network infrastructure and software



Reference

[1]Seafile, *About Seafile*, viewed 2 Feb 2021, <https://www.seafile.com/en/about/#about-contact>.

[2]OpenSSL, *Homepage*, viewed 2 Feb 2021, <https:// https://www.openssl.org/>.

[3]Google 2-Step Verification, *How it protects you*, viewed 2 Feb 2021, <https://www.google.com/landing/2step/#tab=how-it-protects >.

[4] ACME-project-2021.pdf

[5] Snort, document, viewed 2 Feb 2021, https://www.snort.org/#documents

[6] OpenVPN, getting started, viewed 2 Feb 2021, https://openvpn.net/vpn-server-resources/getting-started/

[7] OpenVPN, How To Set Up and Configure an OpenVPN Server on CentOS 8, viewed 8 Mar 2021, https://www.digitalocean.com/community/tutorials/how-to-set-up-and-configure-an-openvpn-server-on-centos-8

[8] OpenVPN, Control channel encryption, viewed 8 Mar 2021, https://build.openvpn.net/doxygen/group__tls__crypt.html