ACME Scandinavia

Requirement Analysis and System Design

Group 76

Michal Winiarski michalwi@kth.se
Shubhanker Singh shusin@kth.se
Waseem Ashraf Bhat wabhat@kth.se

Requirements

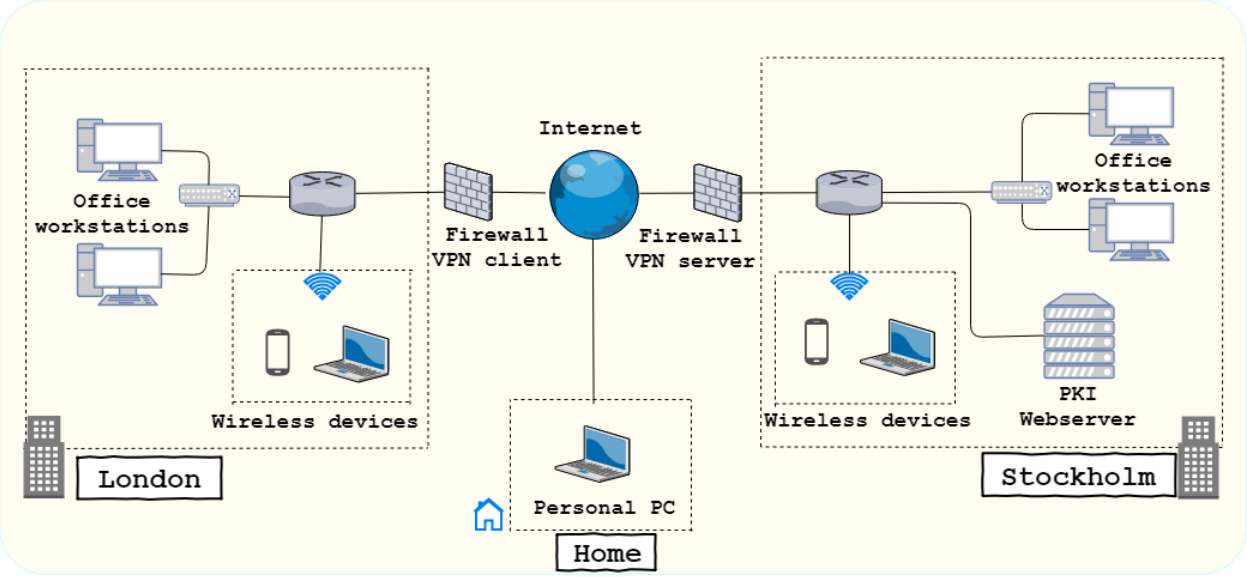
Each office, in Stockholm and in London has its own internal network, protected by firewall from outside world. Networks are able to connect to each other using secure connection. Nobody from outside is allowed to read, change or insert any information. Inside of each network there are computer stations connected by wire to the router, only allowed to use by trusted personnel.

There are also devices like laptops and phones issued by ACME, which can connect to the network using wireless access point. All laptops should be able to connect to both networks. Mobile devices should be able to transfer files securely between each other.

Web server

There is a web server deployed in Stockholm office. Any device connected to either of the networks can access it. ACME devices should be able to access the server from outside the network using cryptographic credentials. Private devices should be able to access the server using two-factor authentication using corporate mobile phone. The web server will be implemented using nginx, it will only allow HTTPS requests and all of them will be logged.

System design



Private Network

The private connection between offices will be implemented using Virtual Private Network (VPN). OpenVPN software used in tunnel mode will be placed on the Virtual Machines guarding both networks, hence all the traffic between offices will be encrypted. On the same VMs, the firewalls (IPtables) will be placed, preventing traffic from outside world to enter private networks. Incoming packets will be logged.

Devices connected to the internal network must be either connected by wire or to the WiFi. This means they are already authenticated and are considered safe.

Authentication

Every laptop and mobile device issued by ACME must be identifiable using certificate issued by ACME's own infrastructure. The certificates will be issued by Internal Public Key Infrastructure (PKI) software placed on the VM inside the Stockholm network. PKI will be implemented using OpenCA. Every certificate shall be assigned to a corporate device by IT department.

As the web server must be accessible for employees from home while using their personal computers, the two-factor authentication system Google Authenticator will be deployed on the web server.

WiFi access

Only corporate laptops and mobiles are allowed to access WiFi networks. WiFi is protected by WPA2. EAP-TLS with a RADIUS server will be used for wireless network to authenticate users.

Intrusion detection system

There shall be an IDS monitoring network traffic and raising the alarm in case of network penetration. For that case the Snort software will be used.