KTH Royal Institute of Technology
Stockholm

School of Electrical Engineering and
Computer Science

Building Networked Systems Security EP2520

Requirement Analysis and System Design for ACME Network Project

Authors
Thomas Poncet *(trfpo@kth.se)*
Alexios Stournaras *(alexioss@kth.se)*
Emil Ståhl *(emilstah@kth.se)*
Andreas Åström *(aastro@kth.se)*

February 2022

1 ACME needs and requirements

ACME needs a new network infrastructure. It needs a new secure web-server in the headquarters in Stockholm. Moreover employees need to be able to connect to the corporate Wi-Fi with there laptops and smartphones. Employees need also to be able to share files securely between them. If employees are not using their cryptographic credentials they need to use their phone for 2FA.

The security requirements are:

- Each employees must have a digital identity verified by digital certificates.
- Employees must use their corporate mobile phone for two-factor authentication if needed.
- Employees visiting London should be able to connect securely to the access point
- The only traffic allowed to the web-server comes from London or Stockholm branch.
- Exchanges between branch and headquarters must be encrypted.
- The main web server must only be access by trusted users from the branch or at home. When connecting from home it will go through the branch through a VPN.
- All communications with the server must be encrypted and authenticated.
- File exchange process must be confidential, authenticate and guaranty the integrity and only between ACME's employees.
- The infrastructure must alert admins in case of attacks.

2 System Design

This section describes the proposed implementation and chosen technologies to achieve the needs specified by ACME.

2.1 Topology

The proposed network topology and design for achieving ACME's needs is illustrated in Figure 1. The figure shows the ACME headquarter to the top and the ACME London branch to the bottom right. The two sites are connected through an OpenVPN tunnel. At the bottom left the figure illustrates a client connecting from an offsite location using 2FA and OpenVPN.

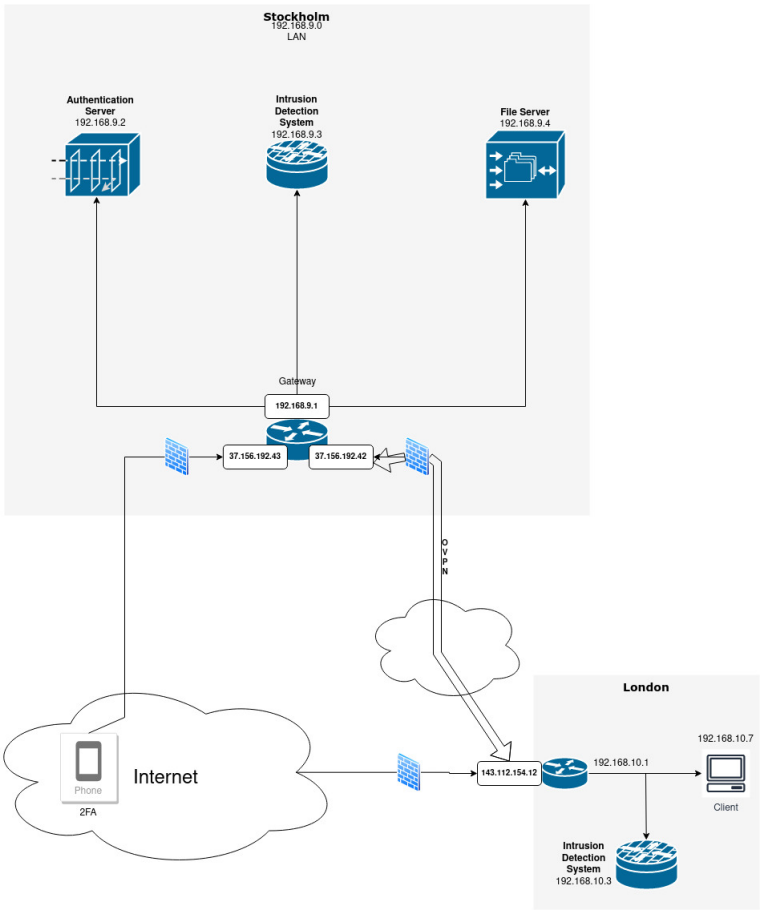

Figure 1: Proposed topology of the new network for ACME

2.2 Implementation details

Our implementation consists of two routers and one Raspberry-Pi. The two routers, one for each branch, hosts two interfaces, as shown in Figure 1. One of the interfaces for each branch is responsible for communication between the branch and the outside world, while the other is dedicated to handle communication with the respective interface located at the other branch. Moreover, we should specify that there are going to be 2 different networks in the branches, one for the company desktops and laptops and one for guests to connect, be it via ethernet or wifi. The tools that are required for the routers is OpenVPN and openWRT. OpenVPN is used to ensure encrypted file exchanges and communication between the branch and headquarters gateways. We will create one VPN connection for London and Stockholm, where the Stockholm router will act as a OpenVPN server, and 2 VPN connections from off-site locations to the respective branches, with each router-gateway of the branch acting a the server. Thus, we will need 3 public IPs.

OpenWRT allows for greater router configurability, however this might not necessarily be needed. openWRT can also act as a firewall. To be more precise, as the reviews suggested, we will have firewalls in each of the branches that prevent access to them, unless the traffic comes from the VPNs that we will create.

The Raspberry-Pi is responsible for running an Authentication Server (AS) and File Server (FS). To act as an AS, the Raspberry-Pi runs FreeIPA, an open source identity management system, that uses VPKI as an external PKI. This allows each employee to have their identity verified by digital certificates, published by a trusted CA through VPKI, and also allows for Two-factor authentication (2FA) for employees. The 2FA is set up for employees that needs to access the branch networks from home or other off-site locations and is going to be achieved with the use of FreeRadius inside FreeIPA, since FreeIPA supports OTPs. FreeRadius is going to be used to just authenticate the users and verify that they have their credentials, and then, they can connect from an off-site location using the OpenVPN that was described above. According to the reviews, we need to specify better how to create the web-server and the file-server. As such,the Raspberry-Pi is going to run an apache server to work as a basic FS, with OwnCloud acting as the interface and the file-control system. OwnCloud has compatible android apps too so we'll be able to connect with phones. We assume that everyone uploads his files at this File Server and whenever anyone wants a specific file, he can download it from the server, acting basically as a modern cloud server.

We also need an Intrusion detection system (IDS) to run on the Raspberry-Pi for detection of potential network attacks. Since we have two networks we will need two instances of an IDS. SNORT is one such open source IDS that can be utilised.

3 Improvements based on reviews

Apart from the two improvements that we mentioned in the previous section, we also need to be more precise about the design choices of the London branch. As for now, we consider that there are only a few employees, and everyone who need to authenticate himself, either from an offsite location or from one of the branches, he does so by authenticating himself with FreeIPA in Stockholm (and OTPs if he is in an offsite location). For scalability later on, we can create another Authentication server in the london branch, to reduce traffic from the VPN that connects the branches together. Furthermore, scalability-wise, every single software and program that we use is also supported in containers. As such, if the company expands and there are a lot more employees, we can containerise our system and run it on a container platform, e.g Kubernetes.