EP2520
BNSS
Group 9 - ☃ HerculeS ♔
Jens Ekenblad, ekenblad@kth.se
Lukas Mattsson, lukasmat@kth.se
Ley-Olivia Avila Rojas, loar2,@kth.se
Stefan Garrido, sagv@kth.se

Requirement analysis & design

Overview

In accordance with the requirements provided by ACME, our group has created a suggested solution that will fulfill these conditions and provide the sought-after security properties for communication with the branches in Stockholm and London. Our understanding of the requirements is summarized in the appendix, which we will refer to when we present our design.

Specifics

Authentication

To authenticate users in both branches, a RADIUS authentication server (freeRADIUS) will be implemented based on the xPKI provided by ACME. Each corporate computer will be provided a private certification that is used to authenticate users in the network. The server will be located in the headquarters in Stockholm. In case of compromised/stolen equipment, certificates/credentials will be revoked. This is assumed to be included on the provided xPKI. If ACMEs xPKI is not provided, the use of an open source PKI (ie.EJBCA) will be implemented.

For non corporate computers to authenticate with the network, a 2FA system will be implemented with Google Authenticator installed on the user's mobile device.

- ***Fulfills requirement***: 1.1, 1.2, 2.2, 6.4

Secure communication

All communication between the two branches as well as for users connecting externally will be using a VPN service using tunnel mode along with ESP protocol. This will be implemented using OPENVPN. For secure communication between the servers and the users TLS will be implemented using OPENSSL. An assumption is made that for remote access, users have prior established access to the network from within the office at Stockholm or London.

- ***Fulfills requirement***: 2.1, 2.6, 3.1, 3.4, 3.5

Secure wireless access

WPA2-Enterprise will be implemented (due to router limitations) for all wireless connections using EAP-TLS and authenticating to the RADIUS server as mentioned above. Adequate authorizations to internal services will be provided from the authentication server.

- ***Fulfills requirement***: 4.1, 4.2

EP2520
BNSS
Group 9 - ☃ HerculeS ♔
Jens Ekenblad, ekenblad@kth.se
Lukas Mattsson, lukasmat@kth.se
Ley-Olivia Avila Rojas, loar2,@kth.se
Stefan Garrido, sagv@kth.se

Web and file servers

An FTP server will be set up to allow file sharing between employees. It will be set up at the Stockholm branch in connection to the less secure web server (Apache server). The servers will be available to all employees inside the network provided that they are authenticated. Employees who want to access the services from outside the network can do so, provided that they have connected to the network through VPN and have been authenticated. The FTP and less web server uses TLS to ensure confidentiality of data. The servers are only to be accessed by employees.

For the main web server (Apache server), only a selected few are allowed to access it using adequate credentials. A firewall will further enhance the security by only allowing certain internal network addresses as well as restricting outgoing traffic.

- ***Fulfills requirement***: 3.2, 5.1, 5.2

Internal and perimeter security

Each branch will have a stateful firewall as a first line of defense to monitor in and outgoing traffic to the network using IPtables on dedicated Linux virtual machines. Furthermore, another firewall will be placed in front of the main web server to provide another layer of security with stricter rules. IPtables will be configured to secure the network against potential DDoS attacks.

Given that there is time over, the goal is to implement an IDS behind the main firewalls that monitors/logs the traffic that goes through the Stockholm and London network. This will be achieved with the use of SNORT.

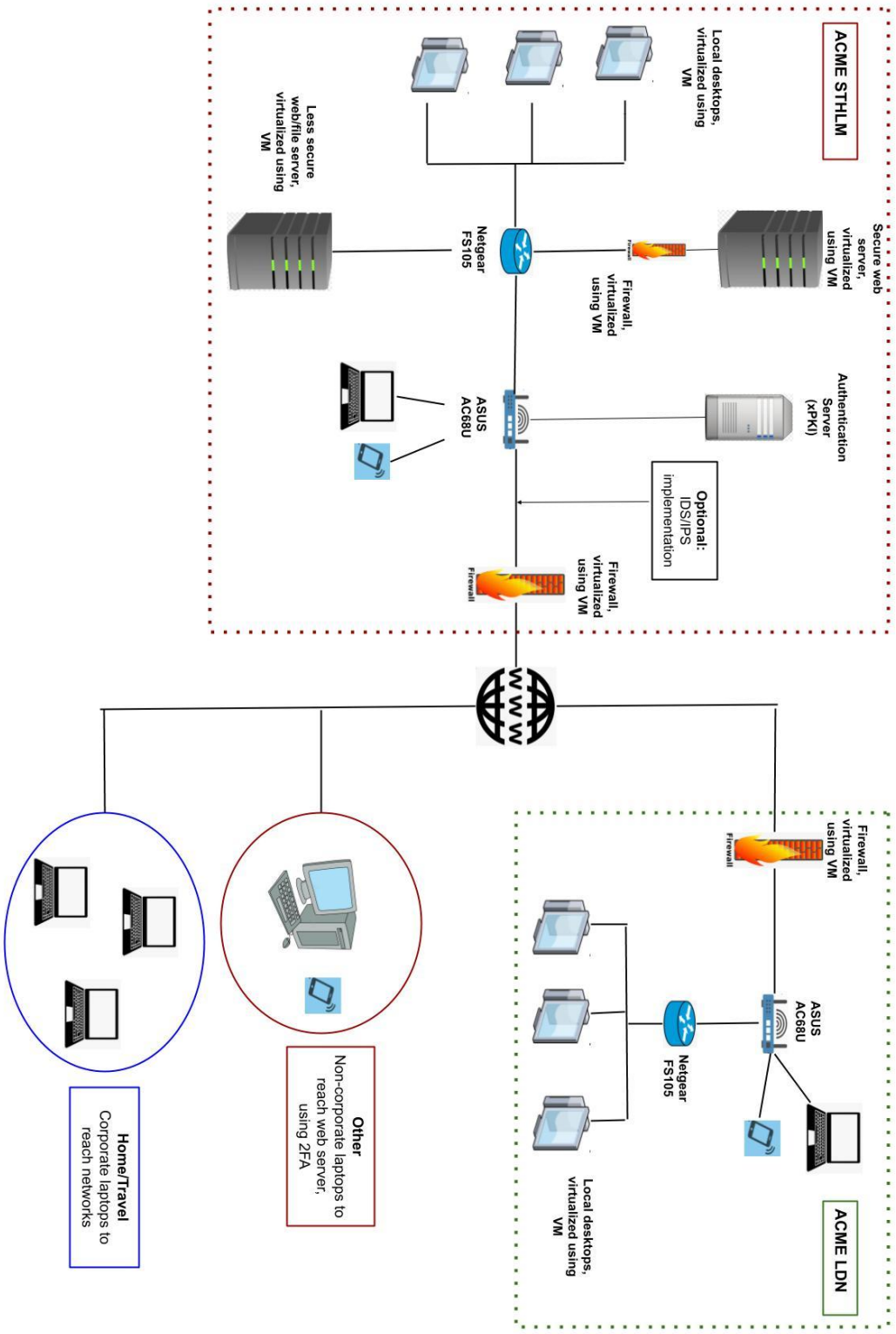
On the other hand, logging of traffic to all servers (main, less critical and FTP) will be implemented using internal logging systems in the servers.

A corporate DNS server will be set up at the Stockholm branch with DNSSEC enabled to protect the ACME domains from being exploited as well as raising the security for the employees.

- ***Fulfills requirement***: 2.3, 2.4, 2.5, 3.2, 3.3, 6.1, 6.2, 6.3

EP2520
BNSS
Group 9 - ☃ HerculeS ♔
Jens Ekenblad, ekenblad@kth.se
Lukas Mattsson, lukasmat@kth.se
Ley-Olivia Avila Rojas, loar2,@kth.se
Stefan Garrido, sagv@kth.se

Topology of the proposed network



EP2520
BNSS
Group 9 - ♚ HerculeS ♔
Jens Ekenblad, ekenblad@kth.se
Lukas Mattsson, lukasmat@kth.se
Ley-Olivia Avila Rojas, loar2,@kth.se
Stefan Garrido, sagv@kth.se

Appendix

Security requirements for the network

1. **Employee Authentication:**
   - 1.1. Each employee has a digital identity verified by digital certificates issued by our own infrastructure.
   - 1.2. Use phones for 2FA.
2. **Secure connectivity:**
   - 2.1. The London network should connect to the web server in Stockholm.
   - 2.2. Only ACME employees should access the infrastructure.
   - 2.3. Only computers with addresses from the Stockholm headquarters or the London branch should be able to connect to our internal network.
   - 2.4. Remote access should be handled very carefully.
   - 2.5. Logging of network traffic and requests to our web server is vital.
   - 2.6. Employee-to-employee communication should also be secured.
3. **Confidentiality and anonymity:**
   - 3.1. Exchanges between London and Stockholm should be hidden from third parties.
   - 3.2. The main web server should be accessed only by trusted users, i.e., employees at London's branch and Stockholm's headquarters.
   - 3.3. Less critical web servers should be accessible within and outside the network, e.g., from homes with personal laptops.
   - 3.4. All communications between any server and a user should be *Encrypted* and *Authenticated*.
   - 3.5. Employees need to hide from curious observers when they connect to our network or when they securely exchange files with each other.
4. **Secure Wireless Access:**
   - 4.1. Visiting employees in London should be able to connect to Stockholm using their laptop computers and a Wi-Fi connection.
   - 4.2. *Authorization* and *authentication* should be done via the wireless network.
5. **Secure File Exchange:**
   - 5.1. *Confidentiality*, *Integrity* and *Authenticity* of file exchange process between employees' mobile phones (and laptops?) should be guaranteed.
   - 5.2. Only ACME employees should be able to exchange files.
6. **Other Security:**
   - 6.1. It is critical for ACME to be alerted whenever an attack is launched against the infrastructure.
   - 6.2. ACME is concerned with *clogging* Denial of Service (DoS) attacks against the infrastructure.
   - 6.3. ACME wants to be sure their domains cannot be exploited or that employees are misled when browsing the Internet, relating to DNS.
   - 6.4. ACME wants to swiftly handle cases with stolen (employee) equipment or compromised (employee) credentials.