KTH Computer Science
and Communication

ACME Scandinavia

Secure IT environment

Preliminary Analysis and System Design

Group 1

ADAM JOHANSSON	adajoh@kth.se
ERIK NORELL	eriknore@kth.se
IGNACIO QUEZADA CRUZ	piqc@kth.se
MICKE SÖDERQVIST	mickeso@kth.se

Royal Institute of Technology
EP2520 - Building Networked Systems Security (BNSS)
Instructor: Panos Papadimitratos (papadim@kth.se)
Main Teaching Assistant: Stylianos Gisdakis (gisdakis@kth.se)

February 24, 2015

Requirements

Two separate networks are required, one in Stockholm and one in London. These are to be connected over the insecure internet in a secure manner, meaning no information is exposed to any outsiders, no information is lost and it is not possible for any outsider to insert false information.

Wired connection to the network at each office is required and only accessible using company desktop workstations. These can not be used by unauthorized personnel.

Wireless connections to the networks at each office is required as well. Wireless connection will only be possible using company supplied laptops and company supplied mobile phones with authentication of users using digital identities and certificates. Employees from Stockholm visiting in London shall be able to access the Stockholm network using their company supplied laptops on the London wireless network.

It shall be possible to transfer files between two company supplied mobile phones in a secure manner. It shall not be possible to transfer a file from an employee to a non-employee.

Specifics to Stockholm office

There shall be an intrusion detection system (IDS) deployed in the Stockholm network, monitoring traffic in the network and raising an alarm if an intrusion is detected as well as logging information about the intrusion.

A web server with access to company data shall be accessible to company employees from outside the network (e.g. from home with private computer), only by using two factor authentication. This authentication must be performed using an application on the company supplied mobile phone. All traffic to and from this server shall be logged.

Finally, the complete security solution presented shall be scalable to accommodate for further expansions of the company's IT infrastructure.

Design

Here we present our design categorized under the different types of security addressing all parts of the requirements.

Confidentiality

All traffic between the London and Stockholm network is encrypted using a Virtual Private Network (VPN) in tunnel mode (using SSL), the software used is OpenVPN. All traffic between employees outside of any of the networks using the web server is encrypted using OpenSSL after proper authentication has been performed (two-factor auth, more details below).

Perimeter Security

A Firewall is placed at the entry point of each network using stateful packet filters. This will prevent unauthorized outsiders on the internet to get access to the internal network. The firewall is implemented using iptables and will also be used for routing.

All traffic going to and coming from the webserver will be logged. The webserver will be an HTTPS Apache server.

Internal Security

It is assumed that the internal network is physically secure from outsiders, i.e. that an outsider does not have physical access to the offices of ACME. In other words there is no need to encrypt the internal traffic.

An open source IDS called Snort is installed at the Stockholm office monitoring traffic and raising an alarm if intrusion is detected. It will use both anomaly and signature detection.

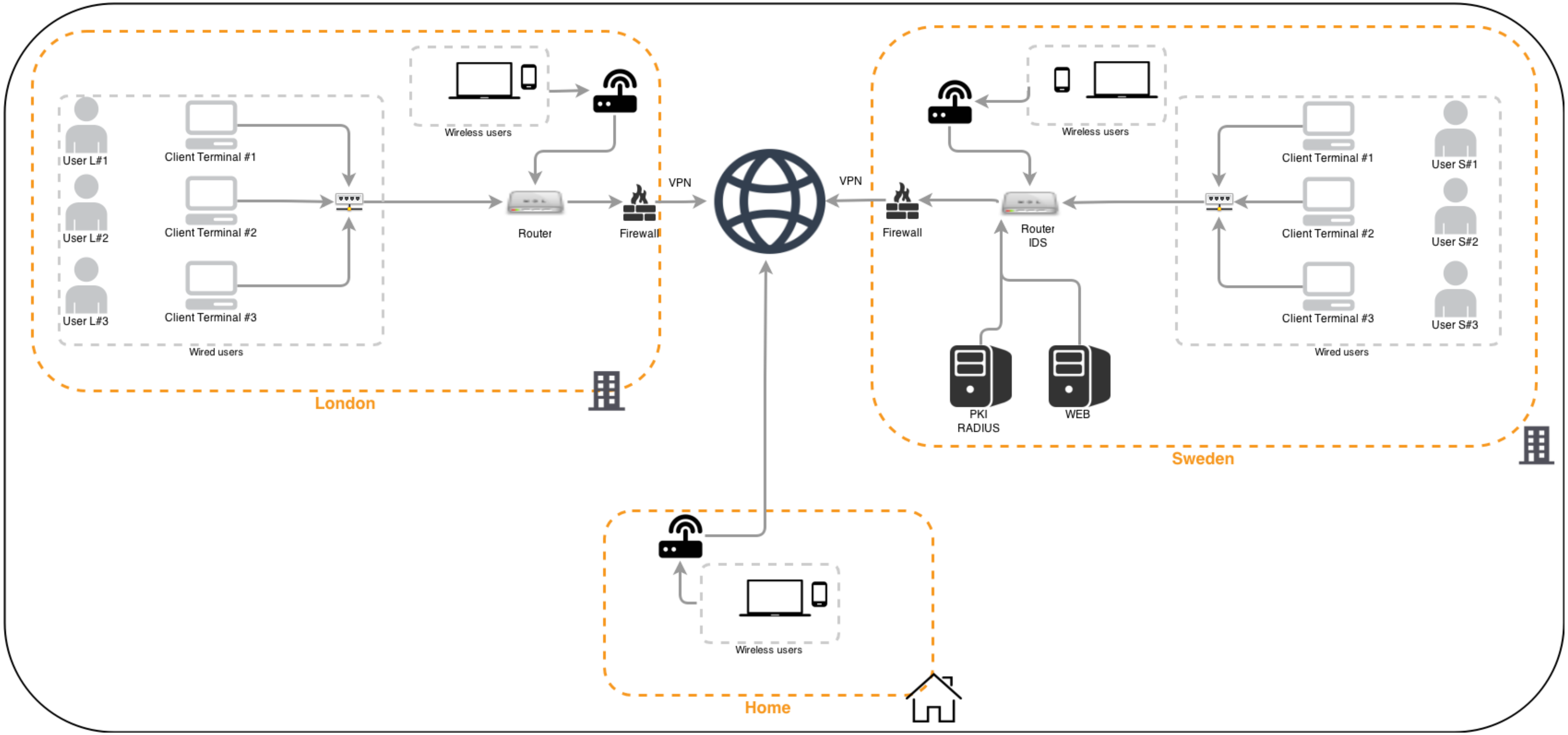
Authentication

All authentication will be performed using private and public keys issued from an internal Public key infrastructure (PKI), implemented using OpenSSL. The wireless network will use WPA2 Enterprise (IEEE 802.11i) and EAP-TLS with a RADIUS server to authenticate users using digital certificates.

To access resources on the web server a 2FA or 3FA can be used depending on if employees are required to have their certificates or not. If that is the case a two-way authentication can be made, meaning both client and server are authenticated using certificates issued by ACMEs CA. This is what we would recommend. If it is not possible a one-way authentication of the server will be made and all traffic will be encrypted using SSL. Either way a user account is generated for each emplyee. These can be protected by both a static password/PIN-code as well as a 6-digit one time password generated by the mobile application Google Authenticator, or only an OTP if that would be preffered. The OTP is regenerated every 30 seconds and after 5 bad login attempts the account is locked.

Additional services

There was also a requirement that it would be possible to transfer files between company phones. This will be solved by encrypting the file using the recpient's public key achieving confidentiality and integrity. The file is transfered over HTTPS after verification of certificates to the server. Lastly the receiver is notified and can retrieve the file for decryption. We will host a small API on the web server which will be used by the android application.


User L#1
User L#2
User L#3
Client Terminal #1
Client Terminal #2
Client Terminal #3
Wired users
Wireless users
Router
Firewall
VPN
London
VPN
Firewall
Router
IDS
Wireless users
Client Terminal #1
Client Terminal #2
Client Terminal #3
User S#1
User S#2
User S#3
Wired users
PKI
RADIUS
WEB
Sweden
Wireless users
Home

Appendix

These are the suggestions of improvements we got from group 2. After each suggestion we give an account for what we have changed, if anything.

1. In the design proposal it is not clearly pointed out as to where the different services are going to be run. Where is the RADIUS server? Where will the IDS system run? Furthermore it was unclear what was to run on the entrypoint machines. As it seems, looking at the network map and reading your descriptions, the only service running on them would be the firewall.

We have improved our figure to make this more clear.

2. The 2 factor authentication on HTTPS? We do not think that it is really possible doing this, as this would be more of a web authentication.

Well, this is what we believe ACME wants. We interpreted the requirement as secure access to a web server was needed. Using HTTPS in combination with other authentication forms will achieve this. A VPN would for example give access to the whole internal network, which is not the same as the requirement (as we interpret it).

3. We have found it unclear as to how your P2P file exchange works. You mention it but have not described as to how you will accomplish this.

We have made this more clear in the description. However, exactly how we will achieve this is not entirely finalized.

4. As it looks like in your design routing will be done on the small WiFi routers? This seems like those small routers could be a potential bottle neck in the network and we think that they should only be utilised as WiFi Access Points.

This is not the case, we have made it more clear in the figure.

5. You describe that you will be using OpenCA however our understanding is that you are supposed to use the x-PKI infrastructure provided by ACME, hence it seems a bit too complicated to use your own implementation.

Group 2 must have misunderstood this. We are to implement our own PKI before implementing the x-PKI.

6. We believe that all traffic should be logged, not only the traffic to and from the web server as stated in the design proposal. What if someone is doing prohibited things inside the internal network?

It was stated explicitly that all traffic to and from the web server was to be logged, no other critical points was mentioned. There is an IDS within the network which ideally will log any attack. We assume that the internal network is safe (meaning we can trust the employees and risk of unauthorized outsiders compromising the network by physical access is negligable), so logging all traffic within the network will not be necessary.

7. When you are using 2 factor authentication, what is the other factor? Usually this should be user credentials. If so, where are these user credential stored and how are they protected? What technology is used for this?

This has been made more clear in the documents.