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 17, 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.

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

Internal Security

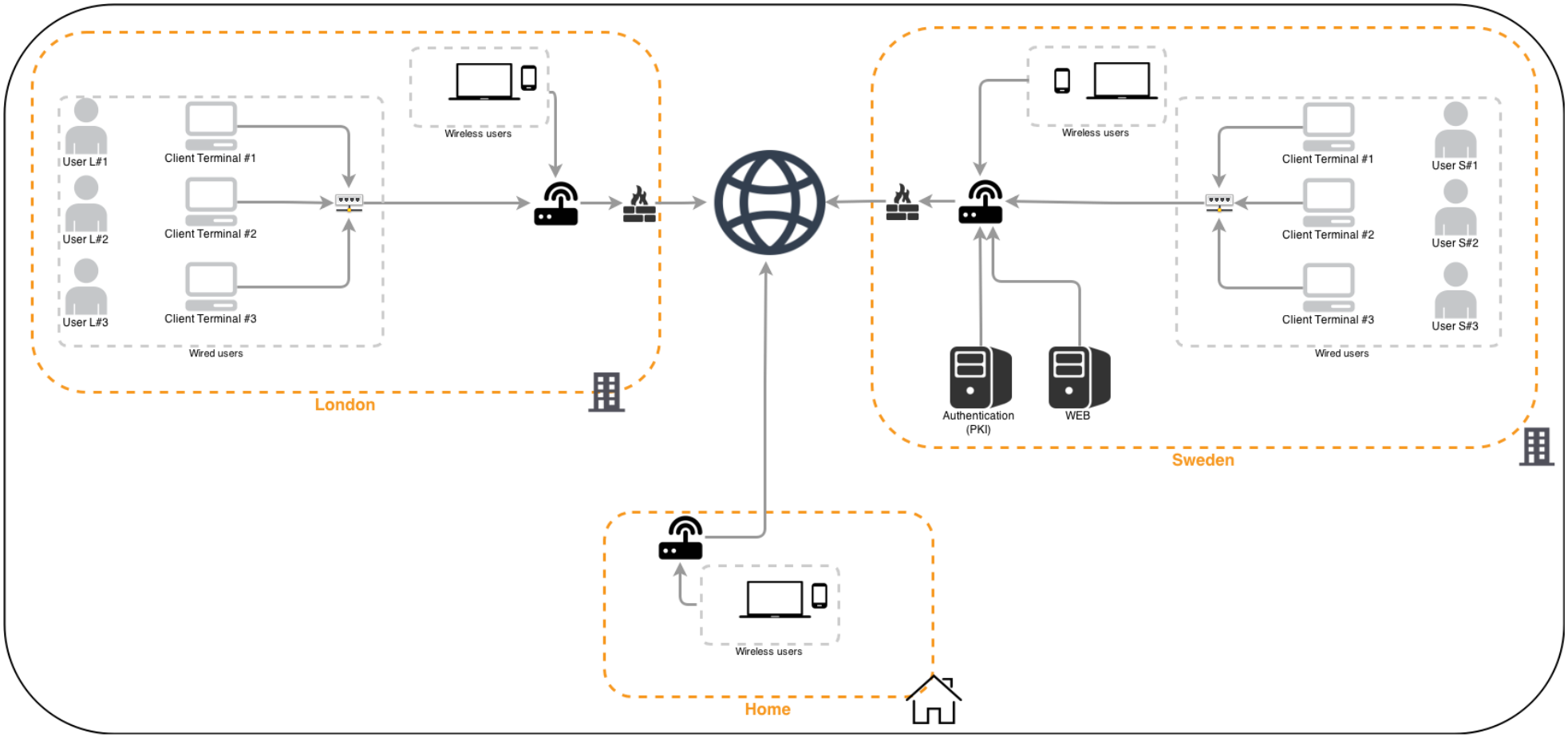
It is assumed that the internal network is physically secure from outsiders, i.e. that an outsider does not have physical access to the offices of ACME. In other words there is no need to encrypt the internal traffic.

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 OpenCA. 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 an employee must identify her-/himself using the digital certificate, however also use an application on the company mobile phone to further identify her- or himself. The mobile application for this will be Google Authenticator.


User L#1
User L#2
User L#3
Client Terminal #1
Client Terminal #2
Client Terminal #3
Wired users
Wireless users
London
Wireless users
Client Terminal #1
Client Terminal #2
Client Terminal #3
Wired users
User S#1
User S#2
User S#3
Authentication (PKI)
WEB
Sweden
Wireless users
Home