EP2520 - Building Networked Systems Security

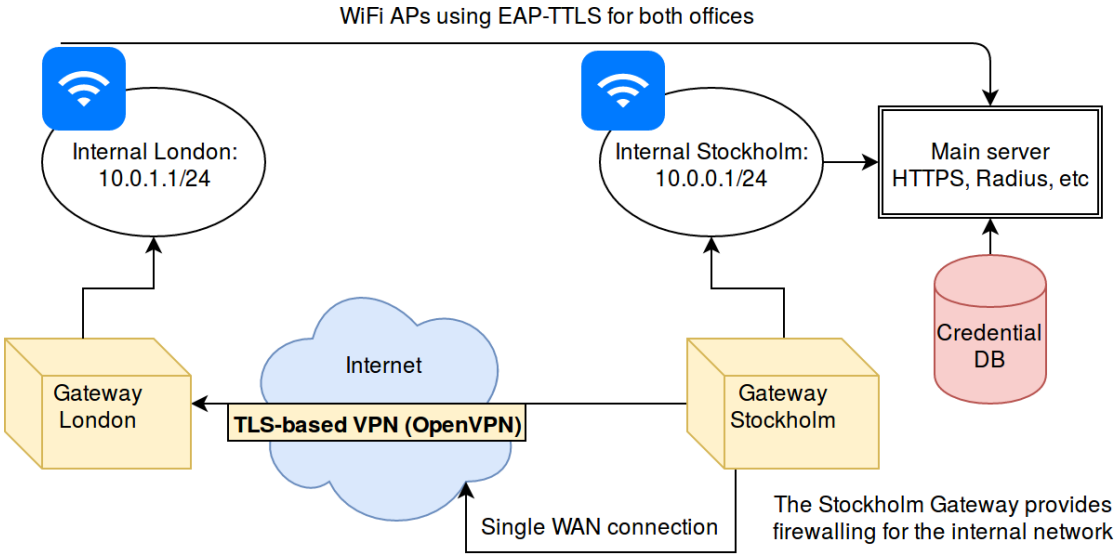
Moric Jacquier, Alexandre Guinaudeau, Peter Caprioli, Daniel Malmhake

February 7, 2017

Introduction

In this report, we present a first outline of our design to fulfill the ACME requirements. ACME's Network is organized around two offices. The headquarters, in Stockholm, host the main Web server. The London Office should be connected to the Stockholm network to allow the employees to access ACME's IT resources. Moreover, external connections (from anywhere else in the world) are required, but for accessing the Web server only.

1 Overview of the solution



1.1 Network overview

The network design will be fairly simple. It will consist in two different subnets, one for each office. The offices are connected via OpenVPN over the internet and all traffic between the two offices are routed inside the VPN tunnel in order to provide security. Each office has one (or possibly more) access point, providing access using the same SSID in both offices in order to support seamless routing. The access points will be configured to authenticate clients using EAP-TTLS with the RADIUS server located in Stockholm.

The Stockholm gateway will provide internet access to both offices. It will also be responsible for firewalling the internal network. This makes it easier to provide security and IDS since all traffic will pass via a single point in the network.

Inside of the Stockholm network there are both an FTP server and the main webserver. Both servers can access a password database storing the user credentials, which are used to add another layer of security to the system.

1.2 External connections

Devices outside the two office networks will not be able to send any traffic into either of the networks; however, the employees are still able to reach the Web server from outside. To ensure that functionality, a two-factor authentication is used, thanks to the company's mobile phones. When connecting to the server, the employee is authenticated with its certificate (using TLS protocol) first, and then a code generated by its phone (using an app such as Google Authenticator) is presented to the web server via a form on the web site. Finally, they use their credentials to access data.

2 Practical solutions

2.1 Fulfilling requirements

Employee Authentication & Confidentiality

Employees are authenticated with a certificate, credentials and their mobile phone.

There are always two layers of security when they access the web server: their certificate and their credentials are used, and they also need 2-factor authentication from their mobile phones when they access from outside the network. Administration of gateways can only be done by someone who has access to the physical device. All connections to the webserver are encrypted using TLS, which ensures the confidentiality. Finally, the two gateways are connected via a VPN configured in tunnel mode, so a third party doesn't have any information on hosts within the networks.

The web server will implement HSTS and pinned certificates together with HTTP $\rightarrow$ HTTPS redirects. This will guarantee that no other CA than our own can sign a certificate and possibly perform a MITM attack on our website over the internet. Most modern browsers (including on smart phones) support HSTS and cert pinning.

Secure connectivity & Secure Wireless Access

As explained above, the authentication is ensured using certificates and the TLS protocol. Both Wi-Fi connection (EAP-TTLS) and communication between gateways (OpenVPN) are secure. Then, firewalling makes it possible to ensure that there is no intrusion from the outside. We need thus a really basic firewall in London (only allowing connections from Stockholm's gateway) and a more sophisticated one in Stockholm, for the internal network of the company. Except the web server, it is accessible only from London's office in this way.

Secure File Exchange

The ACME requirements aren't really precise for this part, so we decided the employees should be able to exchange large files from both their computers or their phones. As specified in the requirements, users can only exchange files from within the internal network (London or Stockholm). We assume all employees have an email address, which isn't necessarily secure.

We will set up an FTP server where each employee has access some shared folders. Whenever a file is uploaded to the server, an email is sent to notify all the users who have access to this folder. This email doesn't contain any sensitive information, it only notifies the users that a new file has been uploaded. To access the file, the user has to connect to the FTP server, which ensures the security of the file exchange. They use the same credentials to access the files and the webserver.

Scalability

This network structure can easily be scaled up by adding more subnets to each gateway, effectively expanding the number of possible hosts in either office. Adding new office sites are also easy.

2.2 Used technologies

Implementation with Virtual Machines

We will use VirtualBox with an Ubuntu 16.04 appliance. We will use one server only; the two gateways will be implemented in the two routers

Softwares and tools

- **OpenVPN** : OpenVPN is an open-source application which allows the creation of Virtual Private Networks using the standard TLS protocol. It supports strong encryption and can also be used over UDP together with its own reliability layer in order to not use TCP, which in turn will give better performance since TCP-over-TCP is bad for congestion control.
- **Snort** : Snort is an open source Network Intrusion Detection System(NIDS) which can be used to log traffic and detect anomalous traffic. We plan to use it to see that we can detect and maybe prevent erroneous or malicious traffic.
- **FileZilla** : FileZilla is an ftp-client which we will use on the host machines to connect to the file server.
- **Mobile Phone FTP Client** : There are an extensive selection of possible FTP[S] clients on both Android and iOS.
- **RADIUS** : We will configure FreeRADIUS to authenticate Wi-Fi clients using PKI. Phones and laptops connecting via Wi-Fi will have our CA preinstalled, hence authentication is done both ways. On Android, this particularly important since the default behavior is to not verify the CA of the network. iOS does not have this issue; but rather pins the first certificate it sees.
- **Google Authenticator** : Google Authenticator is an application implementing 2-factor authentication service. We plan to deploy this on our authentication to give us the ability to demand two-factor authentication for users outside the internal network.
- **Hostapd** : Hostapd is a user-space implementation of a WiFi AP. Most open source router firmwares use it and it is also possible to use it on a laptop or desktop computer, provided the hardware is capable of master (i.e. AP) mode.
- **TLS** : We will use TLS 1.2 together with strong cipher suits that provide forward secrecy. All services using TLS will also have a common revocation list to revoke certificates which are compromised or otherwise should no longer have access.
- **Netfilter** : We will use Netfilter in order to provide firewalling between networks.

2.3 Other reflections

Port security and layer 2 attacks Handling security for users which are already inside the network is a bit more tricky. If we had more expensive switches available, we could set up port security for the ethernet network. The same problem appears for the Wi-Fi side; we currently cannot prevent someone from, for example, setting up a DHCP server and redirecting client traffic over his/her own gateway. This might be somewhat prevented by activating client isolation in Hostapd, but it will not prevent IP spoofing on the network segment and other similar attacks. We will therefore simply assume that clients which are already inside the network are not compromised.

One possible solution would be to dynamically assign virtual LANs and have the Radius server assign each client its own VLAN; effectively putting each Wi-Fi device on its own logical network. This does however require support for VLAN and would take a long time to implement, hence we will simply assume that devices within the network will not perform any of these attacks.