Project network

Final report

Winter 2016

Lillebaelt Academy of
University of applied sciences

IT Technology

Author
Martin B. K. Grønholdt mart80c7@edu.eal.dk
Cristian Iacobanu Balan cris0691@edu.eal.dk
Kasper Soelberg kasp062e@edu.eal.dk

2017-01-23

Table of Contents

1 Introduction....1
2 Technical achievement....1
2.1 The routers....2
2.1.1 ROUTER-EXT....3
2.2 The servers....3
2.2.1 SERVER-DMZ-WEB....3
2.2.2 SERVER-SRVLAN-DNS....3
2.3 Client....3
2.4 VPN IPSEC tunnel (untested)....4
2.5 Testing the system....4
2.6 Building the system....6
3 What we learned during the project....7
4 Project management....7
5 Conclusion....8

1 Introduction

In this document we describe in detail what this project is all about how to recreate it and the process and the difficulties we met upon the way. We don't really go into much detail regarding how to recreate the system but we link to our GitHub[1] page where you can find a step by step guide. We go over the topology and how our whole system is setup including screen shots proving that it works. We go into detail regarding how we managed this whole project and whether we succeeded or failed. We describe what we learned amongst the way and how it will be able to help us in the future and in other projects.

2 Technical achievement

The group has setup a small virtualised network in VMWare, using Linux and Juniper SRX machines.

The network consists of:

- 2 routers.
- 3 subnets DMZ, SRVLAN and URSLAN.
- 2 servers, a web server, and a DNS server.
- 1 client.
- 1 VPN tunnel connected to another groups network.

The internal network uses a DNS server in the SRVLAN network. Clients on the USRLAN network have internal DHCP and DNS services, access to the web server in the DMZ network as well as internet access through the routers. The web server is accessible from the outside on IP address 10.7.0.4.

1 GitHub Repository: https://github.com/deadbok/project_network
GitHup Page: https://deadbok.github.io/project_network

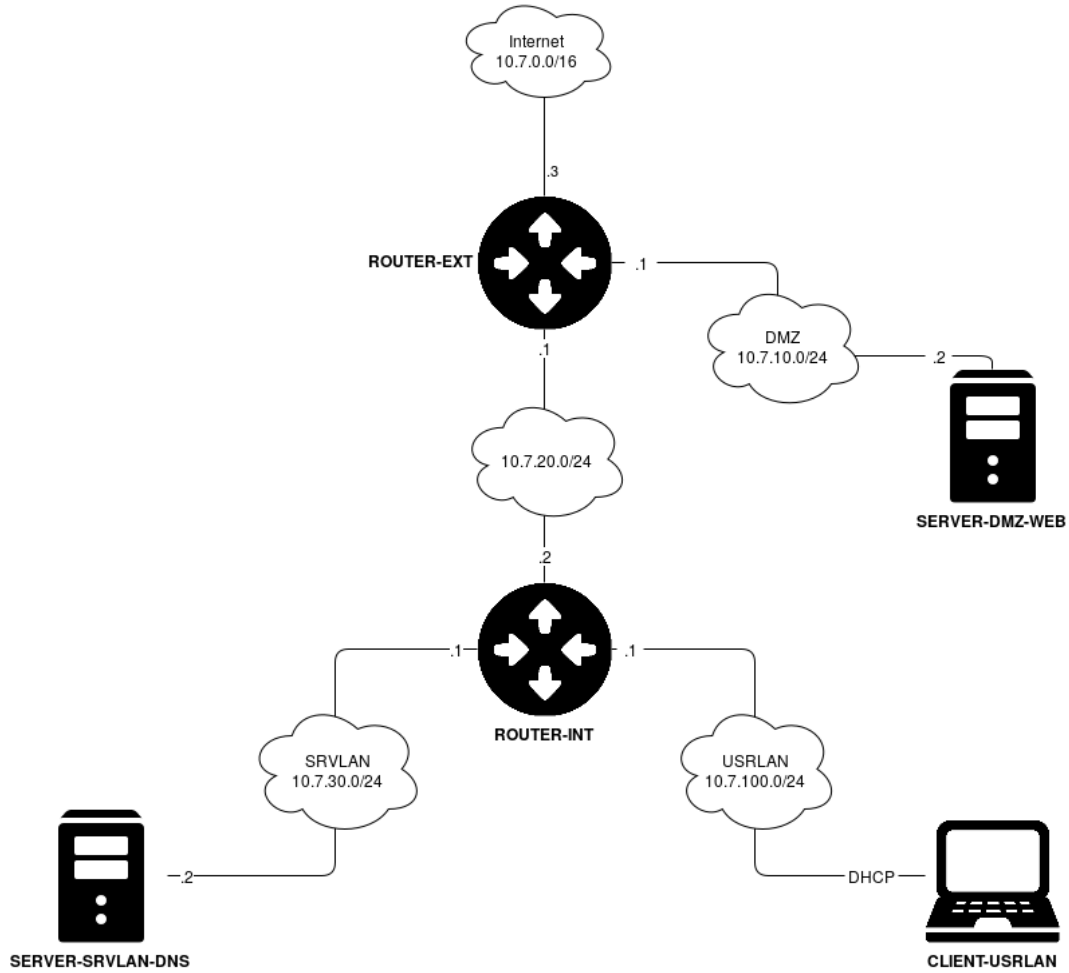

Illustration 1: The layer 3 topology of the networks.

As seen in illustration 1, there are subnets for each network use case:

- USRLAN: The network users connect to.
- SRVLAN: The network that houses the servers only needed in the internal network
- DMZ: The demilitarized network, that is accessible from both the Internet and the internal network.

2.1 The routers

The routers are Virtual Machines running JUNOS vSRX[2]. In doing this project configuration of these routers have been a core task, of getting the network up and running.

The routers have been configured for these tasks

- Static routing between the subnets.
- OSPF area including both routers.
- Some firewalling by configuring the routers with zones for the subnet, and controlling inter-zone access.

2 JUNOS vSRX: http://www.juniper.net/us/en/products-services/security/srx-series/vsrx/

- Internal router redirects initial DHCP request from USRLAN to the DNS/DHCP server in SRVLAN.

2.1.1 ROUTER-EXT

- Connects to the Internet.
- Connects to the VPN.
- Routes external HTTP requests to the web server.

2.2 The servers

The servers are running Ubuntu Server Linux, chosen for the easier installation in VMWare than Debian Linux. The servers are on two subnets doing different tasks.

2.2.1 SERVER-DMZ-WEB

- NGINX as a web server.
- The server runs a homepage that is the documentation for the whole project.

2.2.2 SERVER-SRVLAN-DNS

- DHCP server for USRLAN using dnsmasq
- DNS server for USRLAN using dnsmasq

dnsmaq does local name resolution using the entries in the /etc/hosts file as well as host names gotten from DHCP requests, and passes unknown request onto Googles DNS server at 8.8.8.8

2.3 Client

The client is running Ubuntu Desktop Linux and is used to test the network from a user perspective. The client also bootstraps the build process by being the system that the rest of the Virtual Machines are configured from. This was done to have a known base system to run the build process from.

2.4 VPN IPSEC tunnel (untested)

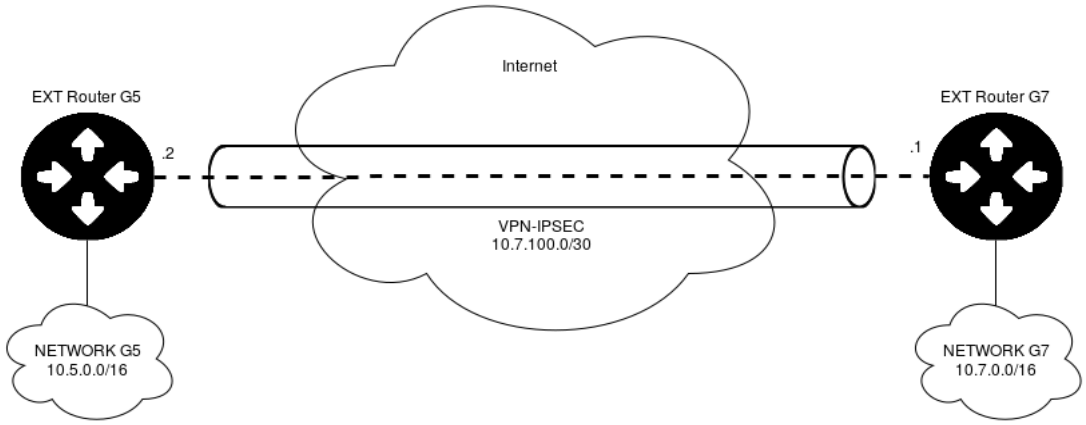

Illustration 2: The router ROUTER-EXT is configured to connect to another network through the Internet using an encrypted tunnel.

The router ROUTER-EXT is configured for using IPSEC to create a VPN tunnel to another vSRX router on interface st0, over the internet. In other words it can connect to another network over the internet, hiding the traffic inside an encrypted tunnel as shown in *Illustration 2*. This has not been tested in the real world and routing needs to be configured but the basic IPSEC connection is made as shown in *Illustration 3*.

```
root@router-ext.localnet> show security ipsec security-associations
 Total active tunnels: 1
 ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
 <131073 ESP:3des/md5  d6e91bb5 2133/ unlim   -   root 500   10.7.0.3
 >131073 ESP:3des/md5  2a73b943 2133/ unlim   -   root 500   10.7.0.3

root@router-ext.localnet> show security ipsec statistics
ESP Statistics:
 Encrypted bytes:           241056
 Decrypted bytes:           142016
 Encrypted packets:           1883
 Decrypted packets:           1870
AH Statistics:
 Input bytes:                    0
 Output bytes:                   0
 Input packets:                  0
 Output packets:                 0
Errors:
 AH authentication failures: 0, Replay errors: 0
 ESP authentication failures: 0, ESP decryption failures: 0
 Bad headers: 0, Bad trailers: 0
```

Illustration 3: IPSEC information on ROUTER-EXT showing that a connection has been made.

2.5 Testing the system

The configuration files for the routers were mostly edited in the Ubuntu client, uploaded and then committed to test the result. Most tests were done pinging IP addresses on the network to see what was accessible. Another useful tool was wireshark, that showed the actual traffic on the “wires”, as well as being able to inspect the packages, to see if they were handled correctly, an example of this is shown in *Illustration 4*. In that example CLIENT-USRLAN (10.7.100.52) is asking for the web

server by the name network.tools and SERVER-SRVLAN-DNS (10.7.30.2) is answering that it is at IP address 10.7.10.2.

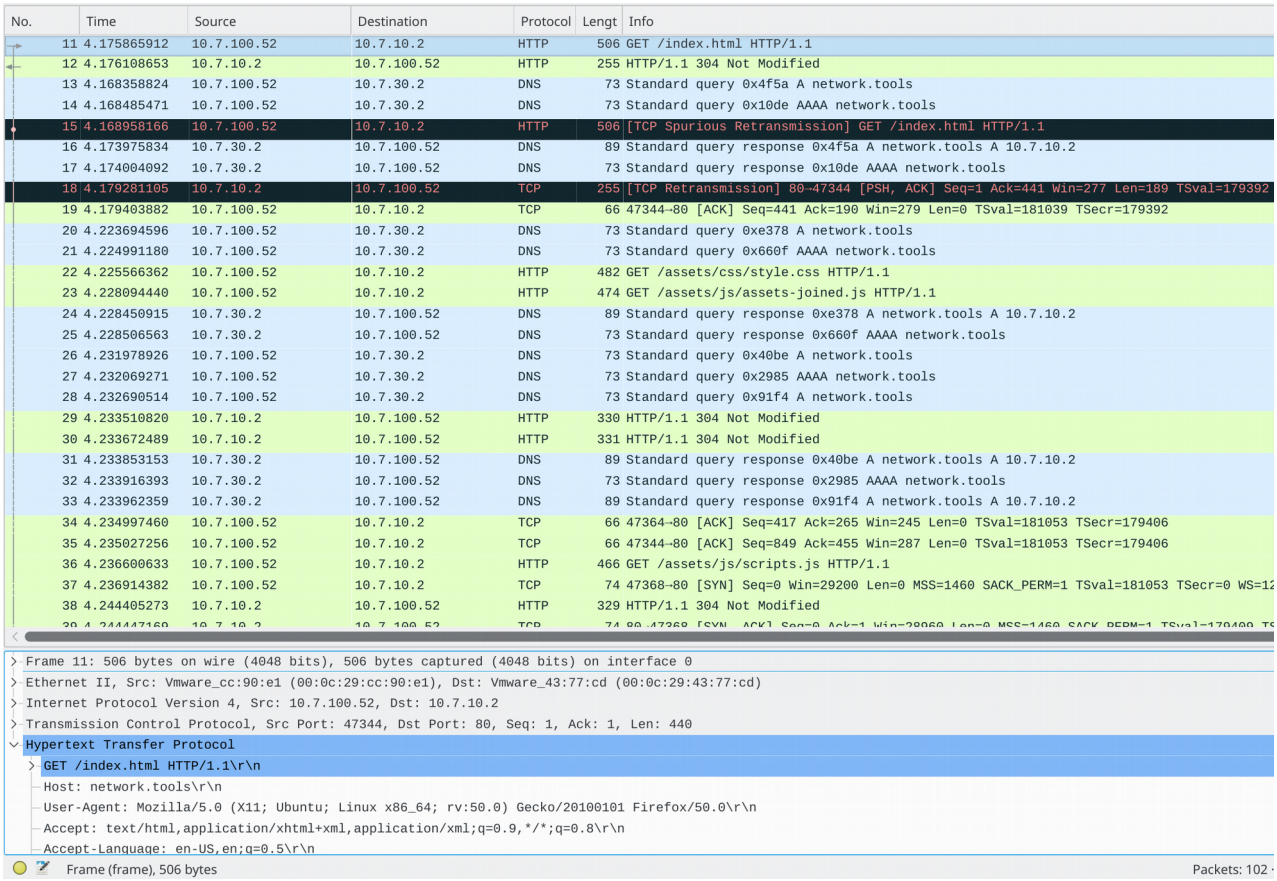

Illustration 4: Wireshark traffic capture on the DMZ network, while the index page of the web server is requested from the internal client.

In the client and on the host a web browser was used to test the connectivity of the web server as shown in *Illustration 5*.

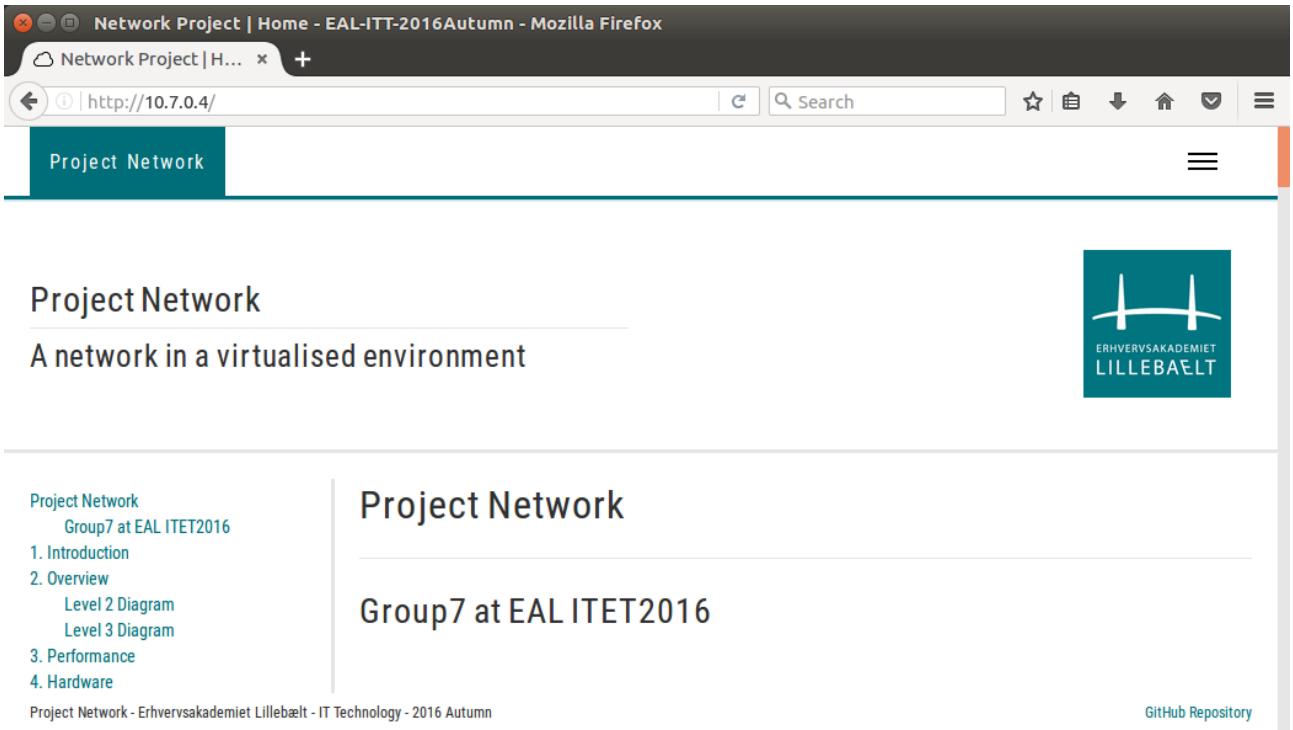

Illustration 5: Testing external access to the web server.

In the case of external access, another physical computer was hooked up either directly or through a switch, and connection was tested using this computer.

2.6 Building the system

To build the system recovery documentation has been written[3]. Testing this recovery documentation proved harder, as writing it would mean getting involved to the point where one was no longer able to see the errors, therefore it had to be tested by a less involved individual.

Some effort has gone in to making the recovery process simple. Using Vagrant for creating the Virtual Machines and Fabric to deploy the configuration, the process could be automated even more.

3 Recovery Documentation: https://deadbok.github.io/project_network/recovery

3 What we learned during the project

We learned a lot during this project, we learned how to work as a unit, we quickly figured out that being able to have each group member working on different task made it possible to spend more time on each task and get into even more detail with everything going on whether it was making a HLD or setting up a web server. We have learned a lot about debugging and the importance of having a diagram of the network when you need to troubleshoot. We have of course encountered a lot of technical problems which in the end have given us a better understanding of not just this network but also how we should handle our self in any other situation with a network. The things we take away from this project is the ability to make something from scratch and get it to work, it is the ability to understand that even though you think you do everything correct there can still be a problem hindering you from getting the end result. What we also take away from this project is that patience gets you a long way when dealing with technical difficulties and getting it to work in the end is a far superior feeling to the horrible times when you can't get anything to work and have to debug and debug and debug.
We have really learned the importance of being able to depend on your teammates and that having some sort of contact with them both in and outside of the school is very important. As mentioned earlier we divided our tasks out amongst us and therefore it is even more important to be in constant dialog to know whether your teammates are behind or on track, you also have the responsibility to tell your teammates if you are falling behind so you can get the proper help. The way we know that we have learned all these things is that we have failed at almost all of them, there has been times where communication has failed or a group member hasn't informed the others that they have fallen behind or we have been debugging without any kind of diagram. We have all experienced these failures and are therefore better prepared for working on projects in the future.

4 Project management

The way we managed our project was every time we got the plan for the particular week we would divide the weeks work into different little task and hand them out so that each person in the group would be able to dive deeper into their particular task. Besides dividing up the work we tried to always have an ongoing dialog not just about the workload but also to have very specific agreements on for example which type of servers we wanted or when we meet up or if one person had to stay home how could they still contribute to the group. The bad thing about this is that it is necessary to have a lot of dialog and that is harder than it sounds especially if there is diseases or something amongst the lines hindering people from showing up, it is possible to still communicate but it is a lot harder when you are not there in person and specially when there is need for debugging or when you can't just transfer something from Linux to Windows or the other way around. Other negative things about this way of working is that when you are done with a task you can't just take the next task you have to include the rest of the group and very particularly explain what have been done so that they also understand it and would be able to recreate it. This sounds extremely easy in theory but when you actually have to do it you realize that it is way more difficult to explain something especially if you barely understood it yourself of course this also leaves you the possibility to go back and check your work which is always nice. The negative thing is that not only do you have to explain something that you have spent 4 hours on in 10-15 minutes, but everyone in the group has to do this making it a big task on the schedule to both set of the time and

for the individual not to run in to significant problems straining the already hard pressed time budget. Overall this is a good method if executed the right way you will learn way more in the end but if executed the wrong way you will be left with a small understanding of somethings and zero understanding of the rest. We executed it somewhere in the middle some weeks went beyond expectation and others went quite poorly in total we had a fine dialog thru out this course, but we also had to work at home sometimes to keep up with the pace of this project but all in all we executed it nicely.

5 Conclusion

In conclusion this project has been both good and bad. We have succeeded in almost everything we set out for in the technical aspect of the project, we didn't test out our VPN tunnels but other than that we finished all the task that where handed to us. We didn't succeed in the managing the project at all, in hindsight it's clear that we should have done somethings differently for example keeping a clear schedule and having an ongoing conversation on whether we are hitting the marks at the right time or we are falling behind. But all in all we have learned a lot throughout this project both technical and how a network can be setup. But also a lot about what it actually takes to get a group to work, and how much work it actually is to keep a project on track especially when there is sickness or absence of any kind. So to sum it up we have learned a lot during this project and we are excited carry on working with IT-Networks.