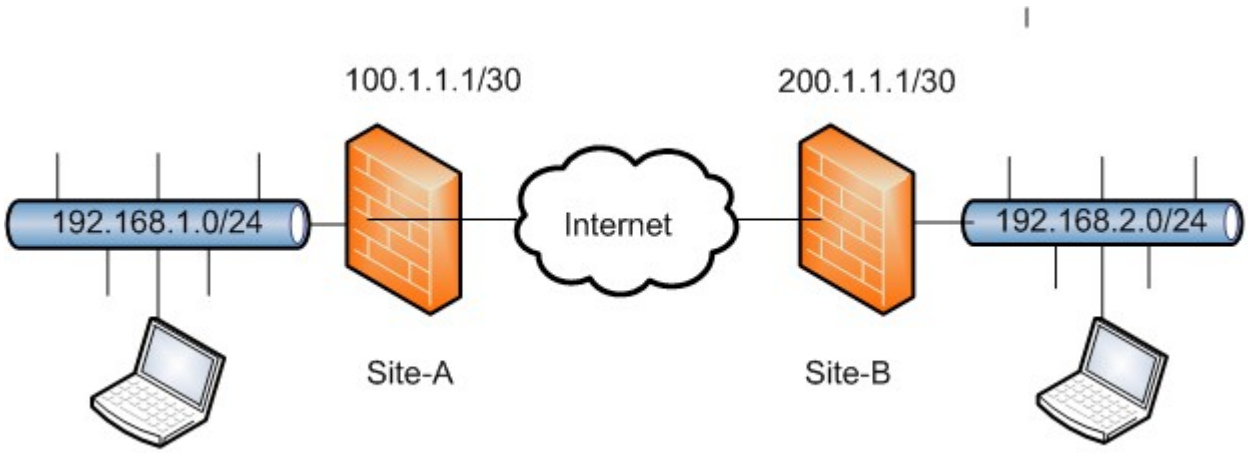
Robert Kristian Alm
LABORATORY VPN 1
Movant Lund

Resume/Goal:
This laboratory asks us to use a VPN tunneling to access our private server from a the main local network that we use in class.

THE THEORY BEFORE THE LABORATORY

VPN sounds and looks like something over-complicated and intimidating because it includes network architecture details and security/encryption details, but after someone got the hang of it shows its simplicity that makes VPN one of the most effective ways to do secure remote access to a network.



VPN:
VPN is the acronym for Virtual Private Network and it is a method of accessing a remote device through public network by using tunneling.Tunneling is the process that we add one more layer of encryption between two routers. In that way we reduce the possiblity of letting someone to spy on the informations that are passing through inside this virual tunnel, (between the two routers – two devices).
To use dedicated line instead of VPN is far more safer than VPN, but the problem is the cost that force as to use VPN. VPN is a very safe and recommended choice but still there is some possiblity to get compromised by hackers.
VPN uses the port 1723 and I works usually in two modes, on tunnel encryption mode, (the two devices are just doing encryption and decryption), and the authentication mode, (on this mode the two devices need to be sure that are connected with each other and not with someone else).
For this lab we will use Tunnel encryption mode with PPTP protocol and the port 1723. We will not use further encryption, (for example SSL), or other security measure for reasons of simplicity.

Why do we need VPN?
There are many uses for VPN, (every time that two nodes wish to communicate safely with each other), but for a non IT technician are usually two reasons:

a)To browse to the internet through a public Wifi.
b)To connect to a remote network through internet, safely.
When VPN is used, possible intruders are losing a very part of information, that usually have, the knowledge which packet is going where, so without this foundational knowledge, it becomes even more difficult for an intruder to intercept the communication.
VPN is an additional measure of safety, other measures, (encryption, firewall, etc) should be included for sufficient protection.

How A VPN works:
It is in the nature of VPN to seem mystical and magical to the eyes of the common user, but as I said the implementation of a VPN connection is fairly simple, (at least in theory). A VPN has by its nature two or more networks that are involved, and of course it includes and two nodes that are doing the encryption decryption of the packets.
As I said earlier VPN is actually one more layer of encryption that encrypts the actually packets and pass a new pair of IP addresses for the new encrypted packets between the two nodes. With the word nodes, we usually mean VPN friendly routers. But sometimes a piece of software can be used as VPN as well for example when we use VPN browsing through our laptop on public places, (no possible to configure the public wifi as our node).
The sender sends the packets towards the receiver. The node of the sender encrypts the packets and send the encrypted packet with the destination the node of the receiver. The node of the receiver decrypts the packets and sends the decrypted packets to the receivers. It is actually just on more layer of encapsulation in our network, and some kind of encryption. Nothing more.

THE IMPLEMENTATION OF THE LABORATORY

What we will use
I have already installed a physical server windows server 2012 r2 that supports a network of virtual servers and I have a laptop that is configured and connected to the same network with the 2 virtual domain controllers. There are already shared folders that I can use.
I added as well a VPN capable router, (ASUS
rt-ac51u dual-band router), and the only necessary addition to the existant
architecture is the necessary role feature to make My Domain controller to work as VPN server.

The existant Architecture:
Before I add the router that I am using now, I had an architecture with 4 registered IP addresses to the main network of the Movan Lund 10.20.0.x. The IP adress 10.20.0.158 was dedicated to my physical server, and two IP addresses (10.20.0.159 and 10.20.0.160) were dedicated to my two virtual servers that are managing the Active domain on my virtual network.
The last IP address 10.20.0.161 was used as wildcard either for my physical laptop or either for the virtual workspaces
that I used to install every now on the then.

The old architecture had as Standard gateway the IP address 10.20.0.1 and as DNS the very same IP or in the case of my Domain controller the loop back address 127.0.0.1.

After installing my Router, i had to configure a new architecture. My new architecture was based to the ip address that my router gave me through DHCP. The router, (my standard gateway) took the IP address 192.168.1.1 for itself by default and it gave me through DHCP the following IP addresses.
The IP adress 192.168.1.223 was dedicated to my physical server, and two IP addresses

(192.168.1.224 and 192.168.1.225) were dedicated to my two virtual servers that are managing the Active domain on my virtual network. The last IP address 192.168.1.226 was used as wildcard either for my physical laptop or either for the virtual workspaces that I used to install every now on the then.

The new architecture has as Standard gateway the IP address 192.168.1.1 and as DNS the very same IP for the physical server and in the case of my Domain controllers the address of my main domain controller 192.168.1.224.

What we will do

After configuring correctly both sides of the pipe, (the VPN server and the VPN client), we will have to access with the client's laptop from a public network, (actually is the local network of my school but that is not an important factor), to a shared folder of the server just to see and copy from that folder. If the transfer of the file completes without issues that means that the VPN works flawlessly.

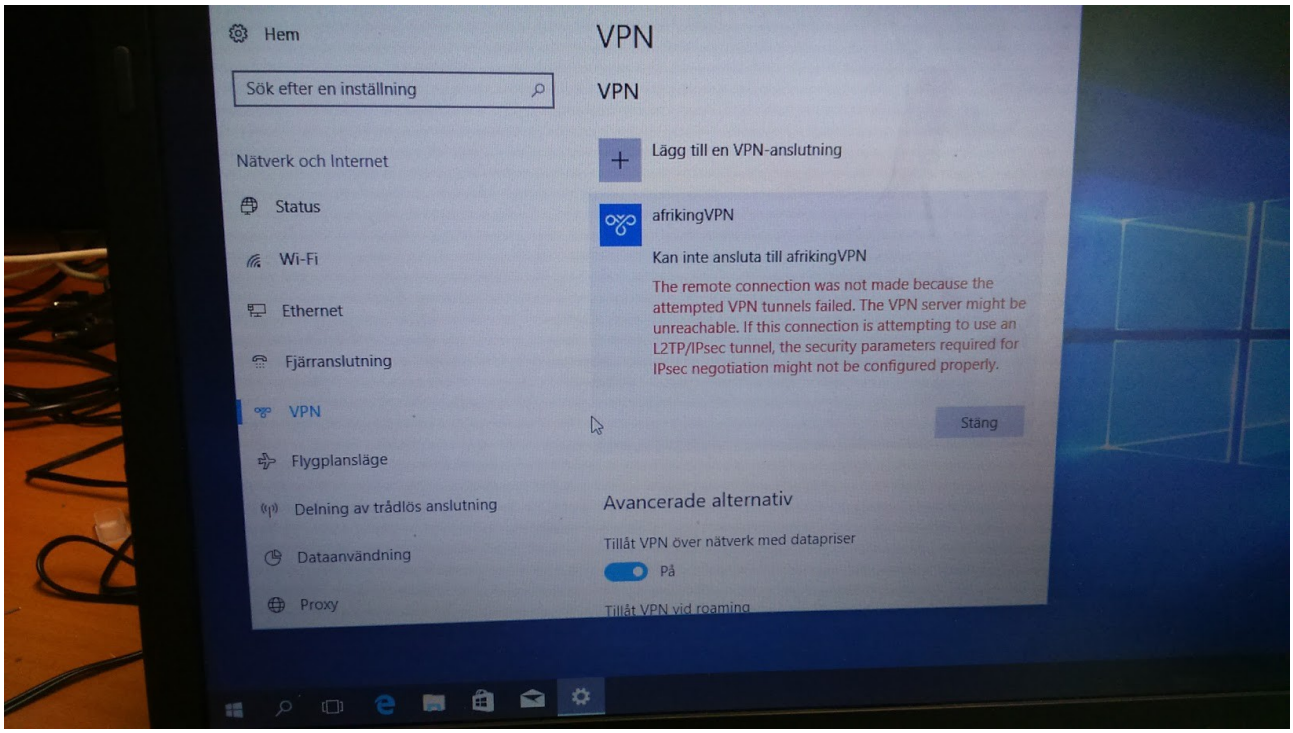
What we will face

The big thing with the are the configurations. Many details, may numbers and many ways to go wrong. And even with problem-free implementation there is always the feeling that after so many details in relatively short time for preparation, (I strongly believe that a good VPN configuration is an long term work), that the configuration of the whole structure is not as optimal as it can be.

OTHER PROBLEMS

They enough problems that they were arised by the implementation of the laboratory and the first one was that my client laptop had a strange issue. Some critical mistake, (I suspect old hard disc), revoke my ability to login to any account possible. I tried to install windows 10 but there was a still a problem that didn't let me connect anywhere despite the fact that my wifi driver was installed. Finally I used other persons computer to do my work bit quicker.

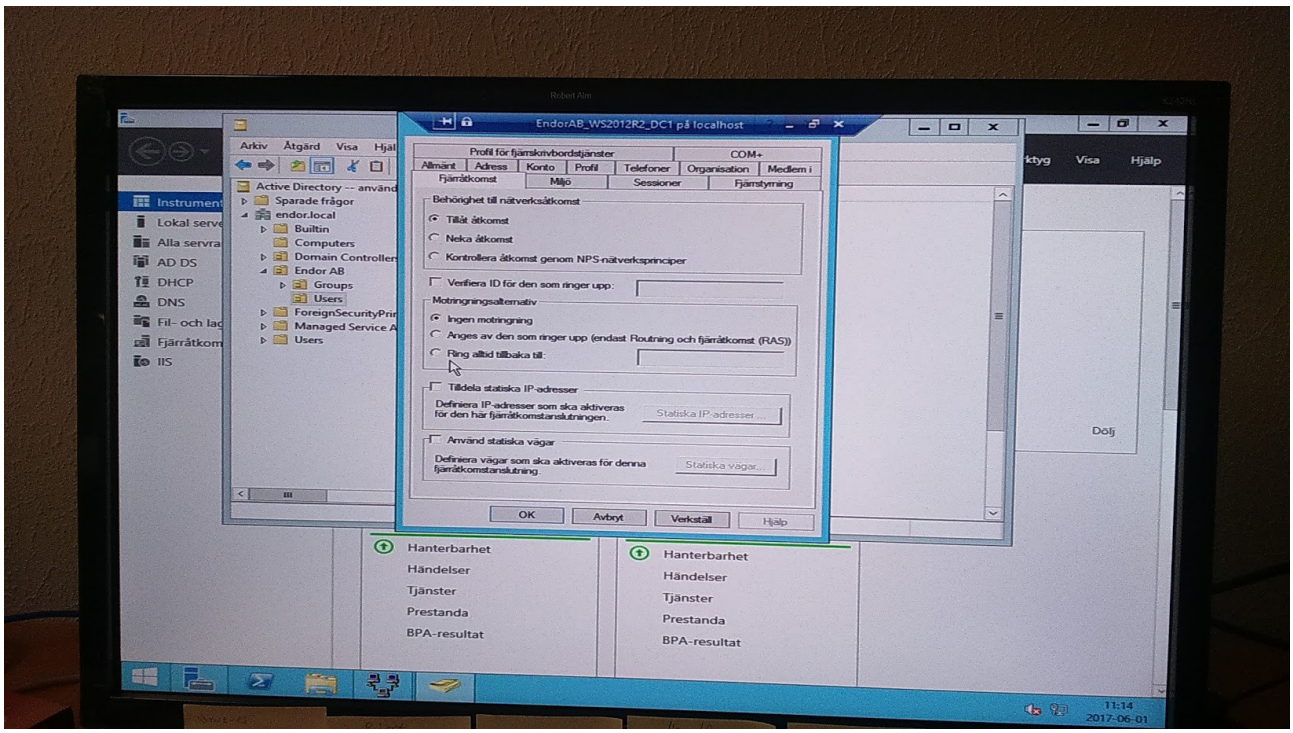
Te architecture of the VPN network (issues)
Despite the efforts that I made to have a solid understanding on how a vpn networks work. On the implementation I had issues because I thought that I had to target necessary the VPN server and not the VPN end device before the server, (the router). I took me a bit to understand that but finally when it was clear to me what is going on I just changed the destination address to point out the outer address of the router and everything was ok.



THE ACTUAL IMPLEMENTATION

On the server side.
On the server side and because we use windows server architecture my decision was to install the VPN server on the main domain controller of my active domain in order to make the VPN server to be a part of my active domain. The installation was a role based feature that was installed as expected through the server manager. The configuration was bit tricky. I had as expected to add the IP address of my VPN server, which is the same with the actual domain controller in which is the VPN server installed, (192.168.1.224), and I had to choose a protocol. I choose PPTP because it was suggested to me and not because I had some kind of solid knowledge about the issue.

On the users
I had to go to my users management on my server manager in order to allow remote access. That was necessary to be done even for the administrator that usually doesn't need much configuration.



On the router

We had as well to change the configuration as well to the router. So I gone through the Web browser interface through the address http://192.168.1.1 which is the default address to access the router, and I activated vpn, and I choose my VPN to work with PPTP and on port 1723. I also had to note the wan address of the router and to allow ping, (yeap, I had to do that manually, I believe it is for security reasons, as everything actually).

On the client side – the laptop

The activation of VPN is activated as expected through the network and sharing center of a windows client OS, (windows 10 in our case). WE had to choose a protocol pptp port 1723 and to give, NOT the address of the VPN server but the WAN address of the router, (it took me bit time to figure this out).

The VPN connection was established and I was able to access my share folder through my client, (my laptop).

CONCLUSIONS

My main thought after implementing this laboratory is that I feel that I have to dig bit deeper on the theory and the praxis of Windows server. I feel my self as really competent with managing an active domain and doing stuff on windows server, (at least on the windows server 2012 r2 version), but I am getting the feeling that it could be extremely beneficial for me if I turn my self to some kind of windows server expert. Ir is just a thought, and I will have my hands full for at least a year of studying more stuff about my work, (security, linux etc etc), but I can see and I can't ignore the benefits that a windows server expertise has to offer to my career.

Another thing that I noticed is that it is a very good practice to take as much notes as possible and to have as much organized as possible. In a long term, especially for those who work with different projects all the time it can be extremely beneficial and in anyway I totally understand the usefulness of a good documentation.