BI-SSB - Lab Manual 6
IPSec VPN in GNS3 use router firmware 3725

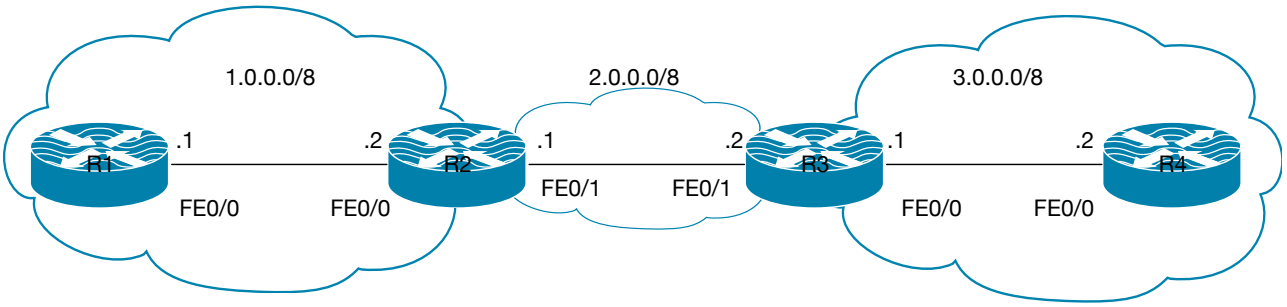
1. Introduction

In the beginning I have to explain you the following keywords: topology formation, IKE phase 1, IKE phase 2, ISAKMP (Internet Security Association and Key Management Protocol), Diffie - Hellman, IPSec, transformset, cryptomap.

IPSec has two phases: IKE phase 1 (ISAKMP) and IKE phase 2 (IPSec). Thus we need to specify the security methods twice (once for each phase). The security elements you can remember using the term HAGLE (to “haggle” in English means trying to obtain a better price): H = hash, A = authentication, G = group number, L = lifetime, E = encryption. To simplify the setup for this topology we choose:

- (E) Encryption: AES 128 bit;
- (H) Hash: SHA;
- (L) Lifetime: 24 h;
- (G) Diffie Hellman Group Level 2;
- Tunnel mode (not transport mode, the whole packet is encrypted, together with the IP headers);
- Tunnel encryption: ESP-AES
- Tunnel hash: ESP-SHA-NMAC.

The topology is very simple:



The networks 1.0.0.0 and 3.0.0.0 represent 2 companies (they are private networks, not primate IPs) while the network 2.0.0.0 represents a public network. We are going to use Telnet (insecure by nature) from router R1 to login remotely to router R4. On the network 2.0.0.0 we shall start Wireshark and capture the data traffic. Before VPN we will be able to see all the data in plain text. Once the VPN is activated then the traffic from network 1.0.0.0 to network 3.0.0.0 (and backwards) will be encrypted. The VPN settings are applied on the routers R2 and R3 (the enterprise border routers).

2. Configuring the basic setup

2.1. Setting up the interfaces:

Be careful of which router you setup what addresses. My explanation is based on the exact given diagram. In reality the names of the interfaces may differ.

```
R1#             configure terminal
R1-conf#            interface fastEthernet 0/0
R1-conf-if#                 ip address 1.0.0.1 255.0.0.0
                            no shutdown
                            exit

R2#             configure terminal
R2-conf#            interface fastEthernet 0/0
R2-conf-if#                 ip address 1.0.0.2 255.0.0.0
                            no shutdown
                            exit
R2-conf#            interface fastEthernet 0/1
R2-conf-if#                 ip address 2.0.0.1 255.0.0.0
                            no shutdown
                            exit

R3#             configure terminal
R3-conf#            interface fastEthernet 0/1
R3-conf-if#                 ip address 2.0.0.2 255.0.0.0
                            no shutdown
                            exit
R3-conf#            interface fastEthernet 0/0
R3-conf-if#                 ip address 3.0.0.1 255.0.0.0
                            no shutdown
                            exit

R4-conf#            interface fastEthernet 0/0
                            ip address 3.0.0.2 255.0.0.0
                            no shutdown
                            end
```

2.2 Setting up EIGRP dynamic routing

We need to activate EIGRP on all participating networks. Let us suppose the autonomous system number is 10.

```
R1-conf#            router eigrp 10
R1-conf-router#             network 1.0.0.0

R2-conf#            router eigrp 10
R2-conf-router#             network 1.0.0.0
R2-conf-router#             network 2.0.0.0

R3-conf#            router eigrp 10
R3-conf-router#             network 2.0.0.0
R3-conf-router#             network 3.0.0.0

R4-conf#            router eigrp 10
R4-conf-router#             network 3.0.0.0
```

2.3 Testing connectivity

From any router you should be able to ping all the addresses: 1.0.0.1, 1.0.0.2, 2.0.0.1, 2.0.0.2, 3.0.0.1 and 3.0.0.2.

2.4 Setting up Telnet on router R4

We need to define a username and a password (username mama, administrator level - 15, password tata):

R4-conf# username mama privilege 15 secret tata

And activate the Telnet on the remote connection terminal lines (line vty, all 16 of them):

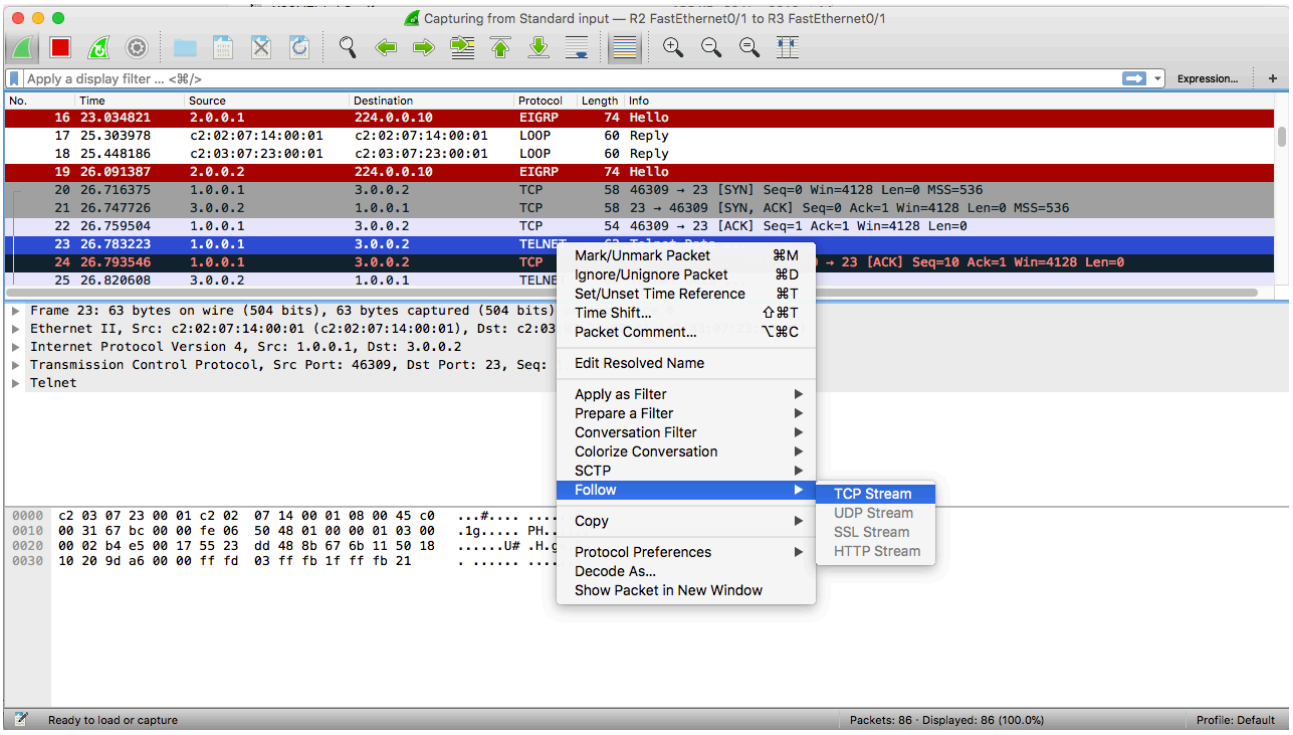
```
R4-conf#        line vty 0 15
R4-conf-line#           transport input telnet
                        login local                     //use the local database of users
```

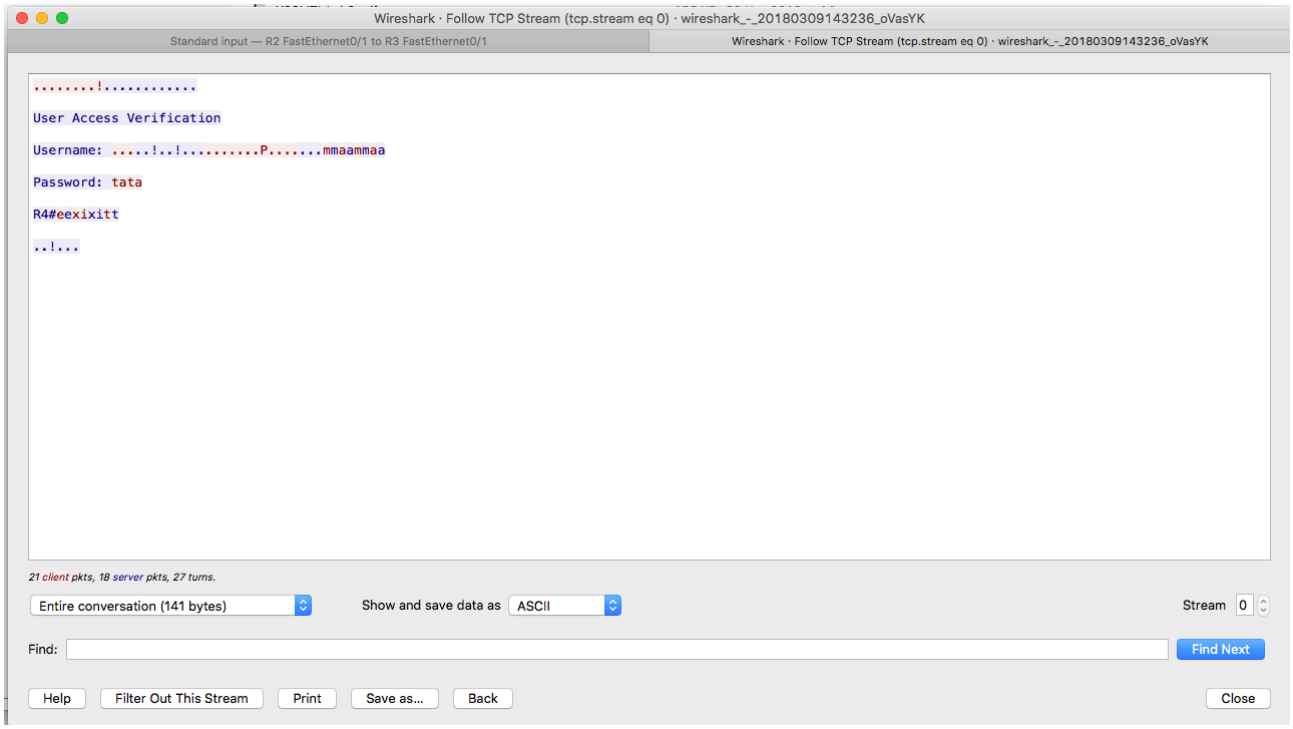
2.5 Testing and conclusions

You need to have Wireshark installed. Right-click on the cable between R2 and R3. Start capturing.

Go on router R1 and do telnet 3.0.0.2. Put your username and password. You should now be remotely connected.

Go on Wireshark and see the content of the packets. Can you spot the username and the password? The username is doubled because when you type the letter m on R1 it goes from R1 to R4 and back from R4 to R1 to be displayed. The password is not displayed thus it is only once, each letter. Each letter is in one packet but try to aggregate (Follow TCP Stream) the communication. Can you spot the username and password in plain text? Use the command exit to exit the remote connection.





3. Setting up the IPSec VPN

The VPN setup will be done on routers R2 and R3 (the enterprise border routers). Be careful because the configurations must be perfectly mirrored (the same but with corresponding parameters) otherwise it does not work.

3.1 Setup of R2

3.1.1. ISAKMP activation

R2-conf# crypto isakmp enable

3.1.2. IKE Phase 1 (ISAKMP)

R2(config)# crypto isakmp policy ?
// why more policies ? Ahaaa - priorities
R2(config)# crypto isakmp policy 100
R2(config-isakmp)# encryption aes ? // look !
R2(config-isakmp)# encryption aes 128
R2(config-isakmp)# hash sha
R2(config-isakmp)# authentication pre-share ?
//Question: why are you not allowed to enter the key here ???
R2(config-isakmp)# authentication pre-share

R2(config-isakmp)# group ?
R2(config-isakmp)# group 2
R2(config-isakmp)# lifetime 86400
R2(config-isakmp)# exit
R2# show crypto isakmp policy
//Question: why more than one ? Who programmed the other one ?

R2(config)# crypto isakmp identity ?
R2(config)# crypto isakmp identity address
R2(config)# crypto isakmp key ?
R2(config)# crypto isakmp key 0 SUPERSECRET ? //this is the password for auth
R2(config)# crypto isakmp key 0 SUPERSECRET address 2.0.0.2
//Router R2 authenticates router R3 based on a password (SUPERSECRET) and its IP address (2.0.0.2)

3.1.3. IKE Phase 2 (IPSec)

R2(config)# crypto ipsec transform-set MYSET ?
R2(config)# crypto ipsec transform-set MYSET esp-aes 128 esp-sha-hmac
R2(cfg-crypto-trans)# mode tunnel
R2(cfg-crypto-trans)# exit
R2(config)# crypto ipsec security-association ?
R2(config)# crypto ipsec security-association lifetime seconds 3600

3.1.4. Define the traffic which will trigger the VPN tunnel

R2(config)# ip access-list extended VPNTRAFFIC
R2(config-ext-nacl)# permit ip 1.0.0.0 0.0.0.255 3.0.0.0 0.0.0.255

//The accesslist permits traffic from network 1.0.0.0 to network 3.0.0.0
//Be careful when configuring this on the other side (R2) – again: traffic from ... to ... - they must be configured properly relatively to your router
//If you have multiple subnets – not your case – you must define one line for EACH subnet

---

3.1.5. Define a crypto map

//A cryptomap thighs everything together.

R2(config)# crypto map MYMAP 1 ipsec-isakmp
R2(config-crypto-map)# set peer 2.0.0.2 //Yes, you have to define the peer twice...
R2(config-crypto-map)# set transform-set MYSET
R2(config-crypto-map)# match address VPNTRAFFIC
R2(config-crypto-map)# set pfs group2
//PFS = Perfect Forward Security

3.1.6. Apply the crypto map to the interface

R2(config)# interface fastEthernet 0/1
R2(config-if)# crypto map MYMAP

3.2 Setup of R3

3.2.1. ISAKMP activation

R3-conf# crypto isakmp enable

3.2.2. IKE Phase 1 (ISAKMP)

R3(config)# crypto isakmp policy ?
// why more policies ? Ahaaa - priorities
R3(config)# crypto isakmp policy 100
R3(config-isakmp)# encryption aes ? // look !
R3(config-isakmp)# encryption aes 128
R3(config-isakmp)# hash sha
R3(config-isakmp)# authentication pre-share ?
//Question: why are you not allowed to enter the key here ???
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group ?
R3(config-isakmp)# group 2
R3(config-isakmp)# lifetime 86400
R3(config-isakmp)# exit
R3# show crypto isakmp policy
//Question: why more than one ? Who programmed the other one ?

R3(config)# crypto isakmp identity ?
R3(config)# crypto isakmp identity address
R3(config)# crypto isakmp key ?
R3(config)# crypto isakmp key 0 SUPERSECRET ? //this is the password for auth
R3(config)# crypto isakmp key 0 SUPERSECRET address 2.0.0.1
//Router R2 authenticates router R3 based on a password (SUPERSECRET) and its IP address (2.0.0.1)

3.2.3. IKE Phase 2 (IPSec)

R3(config)# crypto ipsec transform-set MYSET ?
R3(config)# crypto ipsec transform-set MYSET esp-aes 128 esp-sha-hmac
R3(cfg-crypto-trans)# mode tunnel
R3(cfg-crypto-trans)# exit
R3(config)# crypto ipsec security-association ?
R3(config)# crypto ipsec security-association lifetime seconds 3600

3.2.4. Define the traffic which will trigger the VPN tunnel

R3(config)# ip access-list extended VPNTRAFFIC
R3(config-ext-nacl)# permit ip 3.0.0.0 0.0.0.255 1.0.0.0 0.0.0.255

3.2.5. Define a crypto map

//A cryptomap thighs everything together.

R3(config)# crypto map MYMAP 1 ipsec-isakmp
R3(config-crypto-map)# set peer 2.0.0.1 //Yes, you have to define the peer twice...
R3(config-crypto-map)# set transform-set MYSET
R3(config-crypto-map)# match address VPNTRAFFIC
R3(config-crypto-map)# set pfs group2
//PFS = Perfect Forward Security

3.2.6. Apply the crypto map to the interface

R3(config)# interface fastEthernet 0/1
R3(config-if)# crypto map MYMAP

4. Testing

The VPN is triggered ONLY by traffic from network 1.0.0.0 to 3.0.0.0 or the opposite direction, thus from R1 to R4 ONLY. Any other traffic will NOT trigger the VPN.

Telnet from R1 to R4 and capture the traffic in Wireshark:

R1# telnet 3.0.0.2

You will see ESP (Encapsulated Security Payload) in Wireshark. You cannot intercept the passwords. The rest works EXACTLY as before.

5. Debugging (if needed)

Debugging:

R2 or 3# debug crypto isakmp //for phase 1
R2 or 3# debug crypto ipsec //for phase 2

See the configuration:

R1# show run
R1# show run | transform
R1# show run | crypto