IT Technology 2. sem

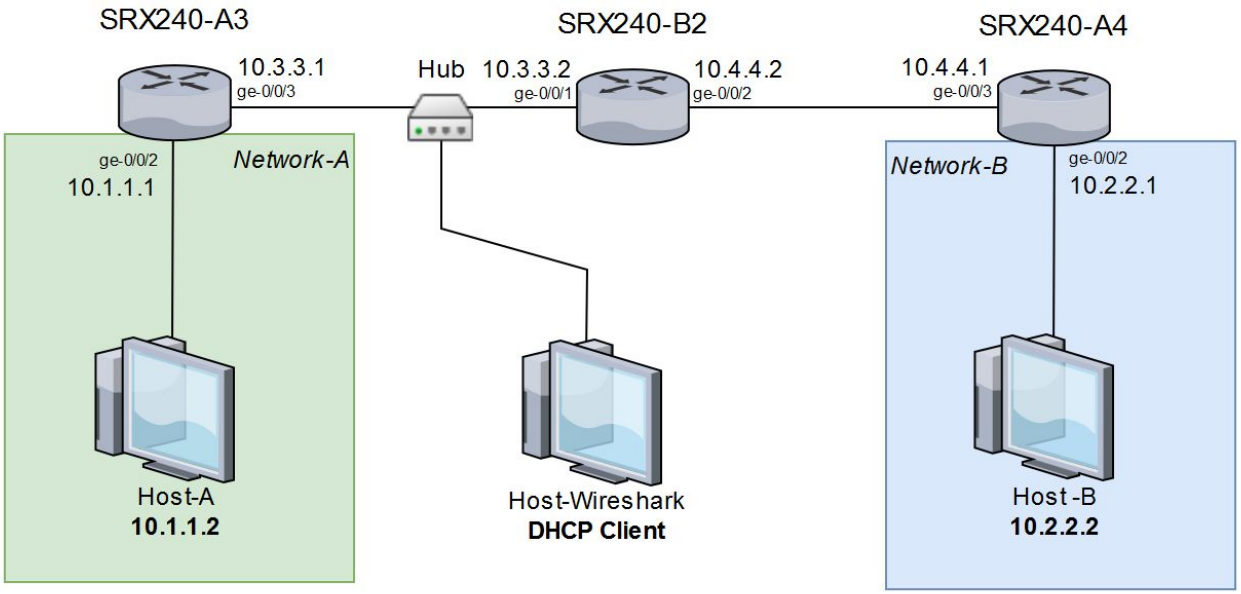
Virtual Private Network

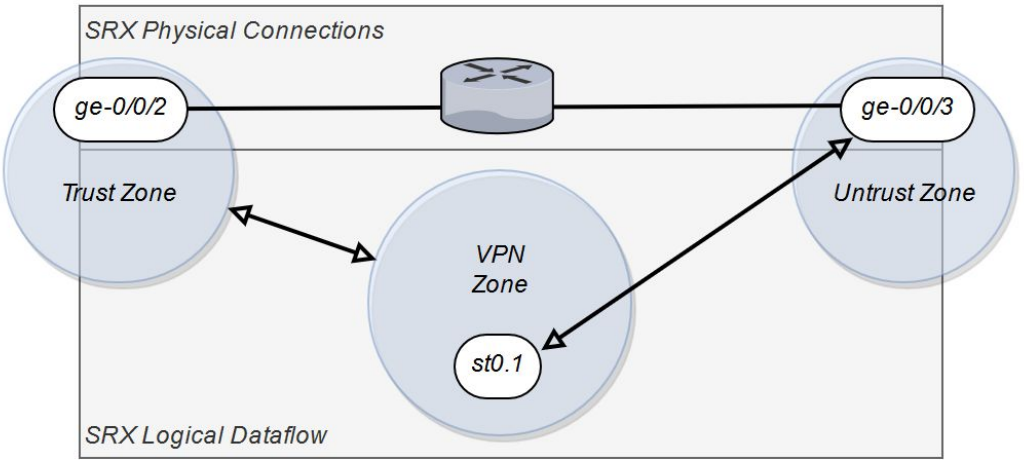
University College
Authors
Sebastian Thomle Mason
seba7286@edu.eal.dk
Anthony James Peak
anth0662@edu.eal.dk
Thomas Bargisen
thom8723@edu.eal.dk

Sunday 5 May 2019

Table of Contents

A HLD with explanation





st0.1 is the virtual interface for the VPN.
IKE defines the configuration for the VPN.
IKE is configured on A3 and A4.
IKE configuration on A3 specifies ge-0/0/3 as interface and 10.4.4.1 as gateway.
IKE configuration on A4 specifies ge-0/0/3 as interface and 10.3.3.1 as gateway.
Static routes are configured both ways between A3 and B2, and between B2 and A4.

An inventory of used devices.

Everything used is already in stock, as such nothing is needed to be purchased.
Do make note that while the PC's are listed together they may vary in model and producer, ultimately it doesn't make a difference.

A link has been added for the SRX240 from Junipers Website.

- x13 Patch cables
- x3 USB to RJ45 Converter Cable
- x3 SRX240[1]
- x3 PC's with ethernet ports
- x1 Ethernet hub

[1] http://www.buyjuniper.net/Available-Products/By-Category/Security/SRX-Series/Juniper-SRX240.aspx

A Low Level Design

LOW LEVEL DESIGN ass16					
INSTANCE TYPE	INTERFACE	IP ADDRESS	MASK	CONNECTS TO	Comments
SRX240-A3	ge-0/0/2	10.1.1.1	/24	Host A	
	ge-0/0/3	10.3.3.1	/24	Hub	
SRX240-B2	ge-0/0/1	10.3.3.2	/24	Hub	
	ge-0/0/2	10.4.4.2	/24	SRX240-A4	
SRX240-A4	ge-0/0/2	10.2.2.1	/24	Host B	
	ge-0/0/3	10.4.4.1	/24	SRX240-B2	
Host-A	eth0	10.1.1.2	/24	SRX240-A3	
Host-B	eth0	10.2.2.2	/24	SRX240-A4	
Hub	eth0	-	-	SRX240-A4	
	eth1	-	-	SRX240-B2	
	eth2	-	-	Host-Wireshark	
Host-Wireshark	eth0	DHCP	/24	Hub	Used for monitoring traffic

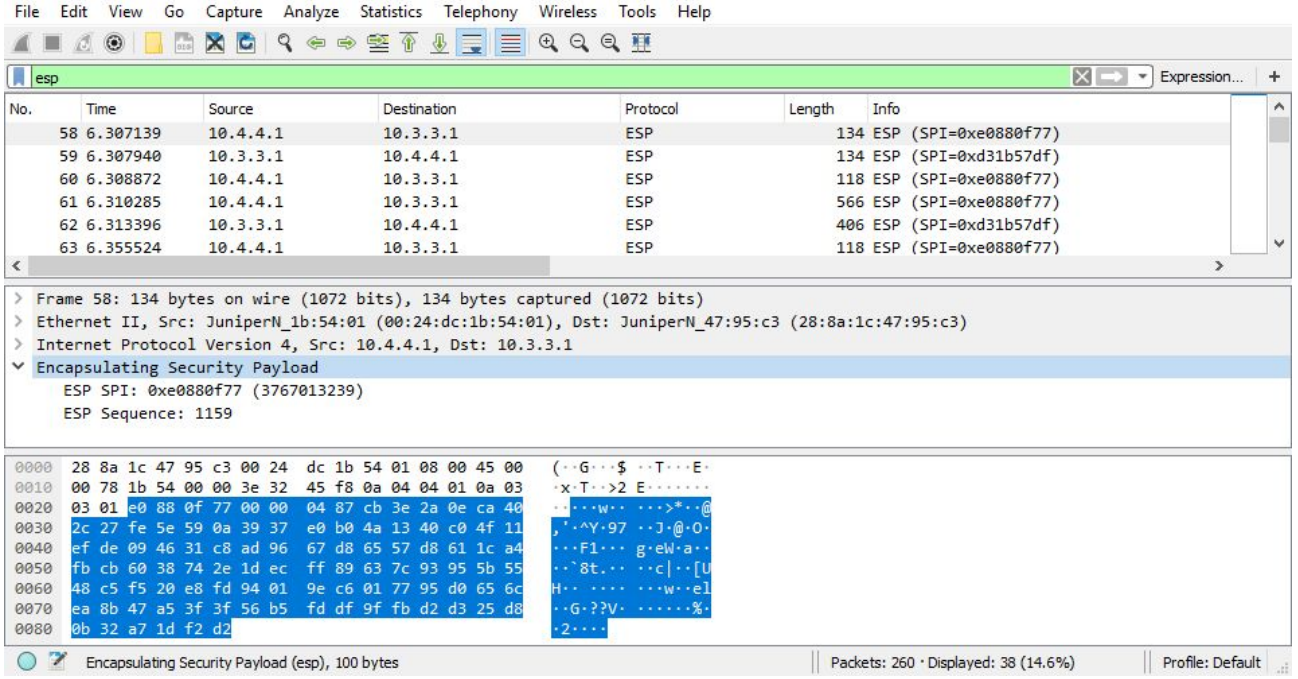
Brief step by step guide

1. Connect everything physically as shown in HLD.
2. Connect USB to RJ45 cables to allow access to routers.
3. Connect to routers using PuTTY.
4. Configure routers.
    a. Paste relevant configuration to router using “load override terminal”
    b. Set password using “set system root-authentication plain-text-password”
    c. Commit
5. Set IPs for hosts as shown.
6. Set Wireshark to listen on the network interface connected to the hub and decrypt traffic.
    a. Type “esp” as the filter.
    b. Ctrl+Shift+P to enter properties
    c. Select Protocols > ESP
    d. Check the “Attempt to detect/decode encrypted ESP payloads” box
    e. Click “Edit...” next to “ESP SAs”
    f. See ESP Wireshark decryption guide on filling out this section.
    g. Click OK.
7. Ping between hosts A and B.
8. The encrypted traffic being sent by VPN should be decrypted and visible.

A filled out test plan

TEST PLAN			
ASSERTION	METHOD	EXPECTED RESULT	SUCCESS
Able to ping	Ping from Host A to Host B	Successful ping	✓
Able to ping local router from host (same subnet)	Ping A3 from host A and ping SRX-A4 from B	Successful ping	✓
Able to sniff traffic with hub	Use wireshark to sniff from hub while pinging between hosts	Encrypted traffic seen between host IPs	✓
Traffic is expected ping traffic	Configure wireshark with the ESP keys to decrypt traffic	Decrypted ping traffic observed between host IPs	✓

Check encryption using wireshark



As seen in the picture above, all traffic going through the VPN is encrypted. The only available information is the router's ip's, and the SPI (Security Parameter Index) tag.

It is possible to decrypt the traffic using wireshark with access to the Authentication and Encryption keys.

To obtain these keys, there is a couple of steps to follow.

1. Add these commands to the router config and commit
    a. `set security ike traceoptions file iktrace size 10m files 10 world-readable`
    b. `set security ike traceoptions flag all`
    c. `set security ike traceoptions level 15`

2. Get the keys from the router
    a. `run show log iketrace | match key.out`
    b. Should look like this

```
[May  3 09:01:50]<none>:500 (Initiator) <-> 10.4.4.1:500 { 11c75fa5 07f06d04 - fe1086f0 4f0d54f1 [0] / 0x1563lcfd } QM;
key.out[36] = 0x8eeec774 d6cac40a 39ac2a91 4293a494 2cbc006c c80f777c 990e3a82 1a36a65a 5558993d
[May  3 09:01:50]<none>:500 (Initiator) <-> 10.4.4.1:500 { 11c75fa5 07f06d04 - fe1086f0 4f0d54f1 [0] / 0x1563lcfd } QM;
key.out[36] = 0x950ceb3b f6bdd838 5f957a29 0c5478bf 1cfdfc99 a78e7d35 ad9e5634 596b5f6f c1272455
```

    c. The keys can be seen after the "="-sign, in this case they are (remember to remove the "0x" prefix):
        i. 8eeec774 d6cac40a 39ac2a91 4293a494 2cbc006c c80f777c 990e3a82 1a36a65a 5558993d
        ii. 950ceb3b f6bdd838 5f957a29 0c5478bf 1cfdfc99 a78e7d35 ad9e5634 596b5f6f c1272455
    d. There is two sets of keys here, one for incoming traffic and one for outgoing traffic

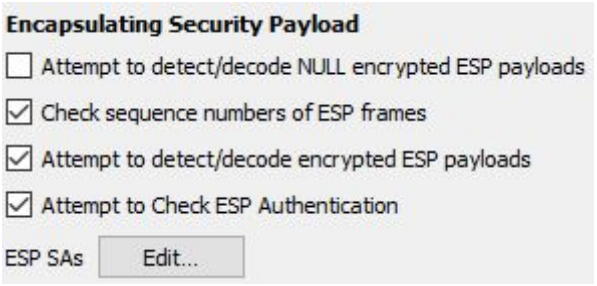
e. To isolate the individual key the string needs to be split up with the first 16 bytes being the encryption-key, and the remaining 20 bytes being the Auth-key
    i. First one
        1. Encryption key: 8eeec774d6cac40a39ac2a914293a494
        2. Authentication key: 2cbc006cc80f777c990e3a821a36a65a5558993d
    ii. Second one
        1. Encryption key: 950ceb3bf6bdd8385f957a290c5478bf
        2. Authentication key: 1cfdfc99a78e7d35ad9e5634596b5f6fc1272455

3. Get IP's and SPI (Security Parameter Index) from Wireshark
    a. Identify ESP (Encapsulating Security Payload) packets containing encrypted data in Wireshark (get one in both directions)

```
 58 6.307139   10.4.4.1  10.3.3.1  ESP   134 ESP (SPI=0xe0880f77)
257 52.311483  10.3.3.1  10.4.4.1  ESP   134 ESP (SPI=0xd31b57df)
```

        i. Note values from Wireshark, in this case
            1. From A to B
                a. Src = 10.4.4.1 Dst = 10.3.3.1 SPI = e0880f77
            2. From B to A
                a. Src = 10.3.3.1 Dst = 10.4.4.1 SPI = d31b57df

4. Set up Wireshark to decrypt ESP traffic
    a. Open Edit>Preferences
    b. Navigate to Protocols>ESP
    c. Check all but "Attempt to detect/decode NULL encrypted ESP payloads"



    d. Click "Edit…" to open the ESP SA table
    e. Add two new lines by clicking the "+"-symbol
    f. Enter the data from the previous steps (remember to add the "0x" prefix to the SPI, Encryption-key and the Auth-key)
    g. For the "Encryption" tab choose "AES-CBC [RFC3602]"
    h. For the "Authentication" tab choose "HMAC-SHA-1-96 [RFC2404]"
    i. Click "OK" twice to apply the settings

Put the router configuration and the topology diagram in GitHub

Diagram[2]

Config_A3[3] Config_A4[4] Config_B2[5]

[2] https://github.com/Sebski123/Network/blob/master/ITT2/ass16VirtualPrivateNetwork/Diagrams/VPN_Topology.pdf
[3] https://github.com/Sebski123/Network/blob/master/ITT2/ass16VirtualPrivateNetwork/Router_configs/ass16SRX-A3.json
[4] https://github.com/Sebski123/Network/blob/master/ITT2/ass16VirtualPrivateNetwork/Router_configs/ass16SRX-A4.json
[5] https://github.com/Sebski123/Network/blob/master/ITT2/ass16VirtualPrivateNetwork/Router_configs/ass16SRX-B2.json

Sources:

https://www.youtube.com/watch?v=4fhLZIbJ-ls
- Information on how to configure VPN on SRX240-routers

http://www.configrouter.com/decrypt-vpn-encrypted-traffic-esp-traffic-auto-ike-vpn-tunnel-4936/
- Information on how to obtain private keys from SRX240-routers

https://cookbook.fortinet.com/decrypting-esp-payloads-using-wireshark-56/
- Information on how to decrypt ESP traffic in Wireshark