Configuring a Remote Access / Dynamic IPsec VPN on the Juniper SRX and the Pulse Secure client on OSX

1. Configuring the SRX

As anyone knows, Juniper does not have great remote access VPN support. They got rid of the brilliant SSL VPN line when they got rid of what is now known as Pulse Sure, and for clients to setup a remote access VPN, Juniper simply tells you “to go somewhere else” for the client software.
And to use public domain software like shrew / ipsecuritas etc. on eg OsX is a nightmare to say the least. If someone has a working setup that I can use on OsX I’d be happy to hear about it.

For me that means that they basically don’t take their own SRX Firewall product line very serious anymore, just like they got rid of the Wireless portfolio as well.
Bummer, because I like the SRX’s.

So anyway, by looking at the many documents (that never completely coincide) on the net on how to configure a remote access VPN with Pulse Secure, I will now configure this on an obsolete, dirt cheap SRX100. (You can buy these for about €25,- second hand in The Netherlands..)
I stole most of the configuration below shamelessly from the Juniper documentation website by the way, and Pulse Secure is running on OsX Mojave.

The Pulse secure client can still be downloaded for free here-and-there, and as long as you do not need more than 2 simultaneous Remote Access VPN’s to the box, you won’t have to bother with a license.

For the configuration below, the zone “Internet” has been setup with 100.100.100.1/24. The “INTERNAL” zone has been setup with 200.200.200.1/24.

Let’s allow IKE in on the Internet zone, as well as HTTPS which is needed for Pulse Secure to authenticate :

```
set security zones security-zone Internet host-inbound-traffic system-services ike
set security zones security-zone Internet host-inbound-traffic system-services https
```

And allow the HTTPS web-management traffic on the Internet facing interface as Pulse first authenticates with HTTPS.. I know, seems silly :

```
set system services web-management https interface fe-0/0/0.0
```

I am going to make it easy for myself, and will use an ike policy that refers to proposal-set “standard” and password “juniper” :

```
set security ike policy ike-dyn-vpn-policy mode aggressive
set security ike policy ike-dyn-vpn-policy proposal-set standard
set security ike policy ike-dyn-vpn-policy pre-shared-key ascii-text "$9$iqPQ/CuEclFnclKMN-Hqm"
```

For the ike-id (something that is always explained or interpreted differently by different vendors), I will use the group-ike-id, the external interface is supplied and for xauth I will use an access-profile:

```
set security ike gateway dyn-vpn-local-gw ike-policy ike-dyn-vpn-policy
set security ike gateway dyn-vpn-local-gw dynamic hostname dynvpn
set security ike gateway dyn-vpn-local-gw dynamic connections-limit 5
set security ike gateway dyn-vpn-local-gw dynamic ike-user-type group-ike-id
set security ike gateway dyn-vpn-local-gw external-interface fe-0/0/0.0
set security ike gateway dyn-vpn-local-gw xauth access-profile dyn-vpn-access-profile
```

So, that should be it for IKE. (Cisco "ISAKMP")

Now let's configure IPSEC:
Again as IPSEC policy I will refer to the proposal-set "standard".

```
set security ipsec policy ipsec-dyn-vpn-policy proposal-set standard
```

Next for the VPN we will refer to the previously configured statements:

```
set security ipsec vpn dyn-vpn ike gateway dyn-vpn-local-gw
set security ipsec vpn dyn-vpn ike ipsec-policy ipsec-dyn-vpn-policy
```

The **internal subnet** (200.200.200.0/24) that is to be accessed via the VPN tunnel is associated with a VPN. An xauth user will be created called "client1".

```
set security dynamic-vpn access-profile dyn-vpn-access-profile
set security dynamic-vpn clients all remote-protected-resources 200.200.200.0/24
set security dynamic-vpn clients all remote-exceptions 0.0.0.0/0
set security dynamic-vpn clients all ipsec-vpn dyn-vpn
set security dynamic-vpn clients all user client1
```

Next we will create the security policy to allow the traffic to enter the VPN from the Internet towards 200.200.200/0/24, and create an addressbook entry for that as well :

```
set security address-book global address INTERN-NET 200.200.200.0/24

set security policies from-zone Internet to-zone INTERNAL policy dyn-vpn-policy match source-
address any
set security policies from-zone Internet to-zone INTERNAL policy dyn-vpn-policy match
destination-address INTERN-NET
set security policies from-zone Internet to-zone INTERNAL policy dyn-vpn-policy match
application any
set security policies from-zone Internet to-zone INTERNAL policy dyn-vpn-policy then permit
tunnel ipsec-vpn dyn-vpn
```

Let's create the access-profile for user1, the password used here will be "juniper" once more.

```
set access profile dyn-vpn-access-profile client client1 firewall-user password juniper
```

And assign the IP addresses for the client(s):

```
set access profile dyn-vpn-access-profile address-assignment pool dyn-vpn-address-pool
set access address-assignment pool dyn-vpn-address-pool family inet network 192.168.100.0/24
set access address-assignment pool dyn-vpn-address-pool family inet xauth-attributes primary-
dns 8.8.8.8/32 // optional
```

Lastly, tell the firewall to use web-authentication :

```
set access firewall-authentication web-authentication default-profile dyn-vpn-access-profile
```

Prior to starting the VPN from Pulse, first browse to the Internet IP address 100.100.100.1 and make sure the HTTPS page comes up.

2. The proof is in the pudding

Once that works, supply Pulse with the name and IP address and you're good to go.

Once the tunnel has come up :

```
# run show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
5346920 UP     b4ea31c77fd01cf5  87b8a47093caddfe  Aggressive     100.100.100.2
```

And:

```
# run show security ipsec security-associations
  Total active tunnels: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon lsys Port  Gateway
  <268173322 ESP:aes-cbc-128/sha1 44f710d2 3470/  499970 - root 59240 100.100.100.2
  >268173322 ESP:aes-cbc-128/sha1 20fc0134 3470/  499970 - root 59240 100.100.100.2
```