

Using a Juniper SRX 300 with a KPN fiberglas (glasvezel) internet connection

1. Prelude

A lot of folks in the Netherlands who are technically inclined, want to replace their ISP supplied modem with something more.... well, *more* basically.

As I am a Juniper and Cisco contractor / instructor, I decided a few years ago to get rid of the Experiabox supplied by KPN and replace it with a Juniper SRX. I love the SRX boxes: they are not too expensive, are full of tricks (and sometimes pitfalls..) and give me (almost) every option in the book.

So here goes..

2. The VLANs and TRUNK configuration

Internet comes in on VLAN 6 and voice on VLAN 7, via a trunk, as this website will tell you: <http://netwerkje.com/eigen-router>

Now unfortunately KPN (wisely) will not allow you to see the SIP / Voice credentials. So as far as I am aware, I cannot completely drop the \$%^&*() modem – I will still need it for terminating the VOICE VLAN 7.

Since the SRX is both a switch as well as a Firewall, the first thing I did is to create the necessary VLANs: (I do not use IPTv)

```
SRX300# show vlans
vlan-internet {
    vlan-id 6;
    l3-interface irb.6;
}
vlan-voip {
    vlan-id 7;
    l3-interface irb.7;
```

The interface towards KPN is configured as a Trunk:

```
SRX300# show interfaces
ge-0/0/0 {
    description "Trunk towards KPN Internet";
    mtu 1518;
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members [ vlan-internet vlan-voip ];
```

One interface is used to switch the voice vlan to the Experiabox modem for voice:

```
ge-0/0/1 {
    description "VOIP VLAN access port";
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
```

Using a Juniper SRX 300 with a KPN fiberglass (glasvezel) internet connection

```
members vlan-voip;
```

VLAN 6 (internet) requires a PPPoE interface. SRXs do NOT SUPPORT PPPOE ON A VLAN INTERFACE. (and yes that sucks)

They do on a VLAN-Tagging interface but that is a router-on-a-stick, which is not what I am after.

SO.. how do I get this done if I cannot run PPPoE on a VLAN interface?.. well this part is a bit filthy: I could of course simply take a switch and split off VLAN 6 as an access port and connect it to the SRX. Then that access port could be used by PPPOE. But it requires an extra switch,- which I have but I want to keep my number of cables (and devices) to a bare minimum. (easier for troubleshooting)

So what I did was.. interface 3 become an access port in VLAN 6:

```
ge-0/0/3 {
  description "Access port in vlan-internet to ge-0/0/4 to allow PPPoE
VLAN";
  unit 0 {
    family ethernet-switching {
      interface-mode access;
      vlan {
        members vlan-internet;
      }
    }
  }
}
```

3. The PPPoE configuration

This interface 3 is connected directly to the next interface (loop!...) 4. This interface is now the basis for the PPPoE interface..

```
ge-0/0/4 {
  unit 0 {
    description "IF with Internet IP via PPPoE";
    encapsulation ppp-over-ether;
  }
}
```

And this is what the PPPoE interface definition looks like:

```
pp0 {
  inactive: traceoptions {
    flag all;
  }
  unit 0 {
    ppp-options {
      pap {
        local-name "*****";
        local-password "*****"; ## SECRET-DATA
        passive;
      }
    }
    pppoe-options {
      underlying-interface ge-0/0/4.0;
      auto-reconnect 3;
      client;
    }
    family inet {
```

Using a Juniper SRX 300 with a KPN fiberglas (glasvezel) internet connection

```
mtu 1492;
filter {
    input dropped;
}
sampling {
    input;
    output;
}
negotiate-address;
```

Now.. once you add the PPPoe interface to your “untrust zone” and you get your PPPoe interface up.. say hellalujah!

```
# run show interfaces pp0 terse
```

Interface	Admin	Link	Proto	Local	Remote
pp0	up	up			
pp0.0	up	up	inet	84.87.114.31	--> 195.190.228.34

Add a default route and try a ping:

```
set routing-options static route 0.0.0.0/0 next-hop pp0.0
```

```
SRX300> ping inet google.com
```

```
PING google.com (172.217.19.206): 56 data bytes
64 bytes from 172.217.19.206: icmp_seq=0 ttl=119 time=10.873 ms
```

4. And now the fun begins..

Once you have gotten this far, the rest is a lot of work but pretty standard:

- Configure your security zones and add the internal interfaces.
- Configure the DHCP server(s).
- Configure your Source NAT configuration.
- Configure security policies for destination nat etc. (port – forwarding)
- Configure Internet screens if you dare..

5. Things that are NOT working

The configuration above has been running for ages. Initially on my SRX 210, and for about 3 years on my SRX 300,- which I love. And the performance is good as well. (NAT works without a hitch for the full 200Mbps)

BUT.. there are a few things that I can **NOT** get to work.

-IPv6 over PPPoe should work on the KPN network. No matter what settings I try, the PPPoe client will not receive a SLAAC address for PD from KPN. And I tried this with multiple Junos versions by the way.

My configuration looks something like this:

```
family inet6 {
    dhcpv6-client {
        client-type stateful;
        client-ia-type ia-na;
        client-ia-type ia-pd;
        client-identifier duid-type duid-ll;
        req-option dns-server;
```

Using a Juniper SRX 300 with a KPN fiberglas (glasvezel) internet connection

```
retransmission-attempt 9;
update-server;
}
mtu 1492;
negotiate-address;
```

The problem remains very persistent. Tracefiles of PPPoE.. reboots, restarts.. I have tried them all. And it should be possible.. so if some guru (read: fellow nerd) in the Netherlands has more success with this, I would be most obliged if you drop me a line.

I tried the Juniper suggested settings like this one:

https://kb.juniper.net/InfoCenter/index?page=content&id=KB30956&cat=SRX_650&actp=LIST

The problem remains:

```
SRX300> show dhcpv6 client binding detail
```

```
Client Interface/Id: pp0.0
  Hardware Address:          **:**:**:**:**:**
  State:                     INIT (DHCPV6_CLIENT_STATE_INIT)
  ClientType:                STATEFUL
  Bind Type:                 IA_NA IA_PD
  Preferred prefix length   0
  Sub prefix length         0
  Client DUID:              LL0x**-**:**:**:**:**:**
  Rapid Commit:             Off
  Server Identifier:        ::/0
  Update Server             Yes
  Client IP Address:        ::/0
  Client IP Prefix:         ::/0
```

-Then the other thing that REALLY annoys me on the SRX: getting a remote access IPsec VPN tunnel to work towards my OsX Apple laptop WITHOUT using commercial clients like Pulse¹ Secure (why Juniper sold of that successful product line is beyond me) or NCP.

I tried IPsecuritas, shrew, the build in OsX IPsec clients; no joy. So for the VPN I had to resort to Linux and both OpenVPN (brilliant) and Strongswan. (easy) Both work excellently but require again more boxes and complexity and port-forwarding, while I have an enterprise grade firewall at my disposal. Juniper's lack of remote access VPN support in this is one of a number of reasons why customers (like the Dutch Police department) are turning their backs on Juniper and are moving towards Fortigate. (sigh..)

Again; if anyone has a success story on either the VPN or IPv6 part, please let me know.

I hope this has helped a few diehard Juniper lovers like me.

¹ See other articles on my website on how to setup an IPsec remote access VPN with Pulse secure and the SRX