L2 VPN Spoke Configuration

Description

The following configuration is an example of setting up a L2 VPN spoke. In order to get this working on a SRX fireweall it requires quite a few protocols stacked together. I will also assume you understand how to apply a basic configuration to a SRX firewall. Interface ge-0/0/7 has a circuit id of 1 that matches the config on the hub for interface ge-0/0/1. So get ge-0/0/1 on the hub and ge-0/0/7 on this firewall are a pseudowire. The IPSec configuration will allow you to user a dynamic public ip or also work behind a NAT.

Configuration

IPSec is setup to use IKEv2 agressive to allow dynamic IP connections. The df-bit clear is used to allow for fragmentation since we will be sending large packets. I will post the set commands at the botoom of the page. This configuration is not perfect and you should really know what you're getting yourself into! :-)

```
security {
    ike {
        traceoptions {
            file ike-trace-log;
            flag ike;
        }
        proposal ike-v2-prop {
            authentication-method pre-shared-keys;
            dh-group group14;
            authentication-algorithm sha-256;
            encryption-algorithm aes-256-cbc;
        }
        policy ike-policy-1 {
            mode aggressive;
            proposals ike-v2-prop;
            pre-shared-key ascii-text "$9$45aJUikPF6A24aUji.mO1IcevW8X"; ## SECRET-DATA
        }
        gateway ike-gate-1 {
```

```
            ike-policy ike-policy-1;
            address 184.99.162.119;
            dead-peer-detection {
                optimized;
                interval 10;
                threshold 5;
            }
            local-identity user-at-hostname "l2-remote@designlogic.net";
            remote-identity key-id L2-Hub;
            external-interface ge-0/0/0;
            version v2-only;
        }
    }
    ipsec {
        vpn-monitor-options {
            interval 10;
            threshold 10;
        }
        proposal ipsec-prop {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy ipsec-policy-1 {
            perfect-forward-secrecy {
                keys group1;
            }
            proposals ipsec-prop;
        }
        vpn ipsec-vpn-1 {
            bind-interface st0.0;
            df-bit clear;
            vpn-monitor {
                optimized;
            }
            ike {
                gateway ike-gate-1;
                ipsec-policy ipsec-policy-1;
            }
            establish-tunnels immediately;
        }
    }
```

When you apply this next configuration it should also be one under the security stanza. This configuration defines the firewall zones and interfaces that belong to the various zones. You will see configuration below for a pppoe connection but this firewall is not using it anymore.

```
policies {
    from-zone VPN-L2 to-zone VPN-L2 {
        policy allow-all {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone untrust {
        screen untrust-screen;
        interfaces {
            ge-0/0/0.0 {
                host-inbound-traffic {
                    system-services {
                        ike;
                        ssh;
                        dhcp;
                        ping;
                    }
                }
            }
            pp0.0 {
                host-inbound-traffic {
                    system-services {
                        ike;
                        ssh;
                        dhcp;
                        ping;
                    }
                }
            }
        }
    }
```

```
        security-zone VPN-L2 {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                lo0.0;
                st0.0;
                gr-0/0/0.0;
            }
        }
    }
}
```

The following is the inerface section. Please notice the MTU settings for each interface as it is important to have them set correctly otherwise you will not have enough headroom to send full size packets. The GRE interfaces have fragmentation enabled as well. In the configuration below you will see that ge-0/0/0 is being used for internet connectivity. You can ignore interface ge-0/0/1.

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                dhcp;
            }
        }
    }
    gr-0/0/0 {
        description "GRE tunnel to Hub";
        unit 0 {
            clear-dont-fragment-bit;
            tunnel {
                source 10.255.10.10;
                destination 10.255.10.1;
                allow-fragmentation;
            }
            family inet {
                mtu 2000;
```

```
            filter {
                input inet-packet-mode;
            }
            address 10.255.20.2/30;
        }
        family mpls {
            mtu 1900;
            filter {
                input mpls-packet-mode;
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
ge-0/0/6 {
    encapsulation ethernet-ccc;
    unit 0 {
        family ccc {
            filter {
                input l2circuit-packet-mode;
            }
        }
    }
}
ge-0/0/7 {
    mtu 1560;
    encapsulation ethernet-ccc;
    unit 0 {
        family ccc {
            filter {
                input l2circuit-packet-mode;
            }
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 127.0.0.1/32;
            address 10.255.255.10/32 {
```

```
                primary;
            }
        }
        family mpls;
    }
  }
  pp0 {
    unit 0 {
      apply-macro CenturyLink;
      ppp-options {
        chap {
          default-chap-secret "$9$hPyreWLxdsY4IEv8XN2gmP5z9t"; ##
SECRET-DATA
          local-name "<some_user>@centurylink.net";
          no-rfc2486;
          passive;
        }
        pap {
          local-name "<some_user>@centurylink.net";
          no-rfc2486;
          local-password "$9$1XShSevWxdVs0BrKMLbwHk.f3/"; ## SECRET-
DATA
          passive;
        }
      }
      pppoe-options {
        underlying-interface ge-0/0/1.0;
      }
      family inet {
        negotiate-address;
      }
    }
  }
  st0 {
    unit 0 {
      family inet {
        address 10.255.10.10/24;
      }
    }
  }
}
```

This is the routing options configuration. The default gateway and router-id are set here as well at the AS.

```
```

```
routing-options {
    static {
        inactive: route 0.0.0.0/0 {
            qualified-next-hop pp0.0 {
                metric 1;
            }
        }
    }
    router-id 10.255.255.10;
    autonomous-system 65535;
}
```

The following configuration is the procol section.

```
protocols {
    mpls {
        interface gr-0/0/0.0;
        interface lo0.0;
    }
    bgp {
        group VPLS {
            type internal;
            multihop;
            local-address 10.255.255.10;
            mtu-discovery;
            family l2vpn {
                signaling;
            }
            neighbor 10.255.255.1;
        }
    }
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface gr-0/0/0.0;
        }
    }
    ldp {
        interface gr-0/0/0.0;
        interface all {
```

```
            disable;
        }
        interface lo0.0;
        session 10.255.255.1 {
            authentication-key "$9$k.m5z3901hik.5Qz6/lKvL-Vws2"; ## SECRET-
    DATA
        }
        session 10.255.255.11 {
            authentication-key "$9$KbBMWXNdsaGilKMX7Nbwmf5F9ApuO"; ##
    SECRET-DATA
        }
    }
    l2circuit {
        neighbor 10.255.255.1 {
            interface ge-0/0/7.0 {
                virtual-circuit-id 1;
                ignore-mtu-mismatch;
            }
        }
        neighbor 10.255.255.11 {
            interface ge-0/0/6.0 {
                virtual-circuit-id 3;
            }
        }
    }
    l2-learning {
        global-mode switching;
    }
    rstp {
        interface all;
    }
}
```

The firewall configuration below is the last section of the code and it's how we change certain types of traffic from session based to packet based forwarding.

```
firewall {
    family inet {
        filter inet-packet-mode {
            term control-traffic {
                from {
                    protocol tcp;
```

```
                port [ 22 80 8080 646 179 ];
            }
            then accept;
        }
        term packet-mode {
            then {
                packet-mode;
                accept;
            }
        }
    }
    family mpls {
        filter mpls-packet-mode {
            term ALL-TRAFFIC {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
    family ccc {
        filter l2circuit-packet-mode {
            term ALL-TRAFFIC {
                then {
                    packet-mode;
                    accept;
                }
            }
        }
    }
}
```

Full configuration as set commands

I'll even leave the system level stuff in the config below.

> set system login user tyler uid 2000
> set system login user tyler class super-user

```
set system login user tyler authentication encrypted-password
"$6$X7sUSWpb$QlFelybaR.yFXxqxR5yhvzbB3rc8EFCUmvZ/P26NmekvHtqxvV5g
AVVzGYKIsix.kMyBaNzWThEKjF6ovalB90"
set system root-authentication encrypted-password
"$6$v6Frer3T$ORom37iV25p.UEAopdExWdhTZ2MdbNkRTaQA42BAR7pc1f94bhk
.tyy9e.HMqUF6ZLEk2yzhGbpFPVwGSkK08."
set system host-name SRX-L2VPN-Remote
set system name-server 8.8.8.8
set system name-server 8.8.4.4
set system services ssh
set system services web-management https system-generated-certificate
set system syslog archive size 100k
set system syslog archive files 3
set system syslog user * any emergency
set system syslog file messages any notice
set system syslog file messages authorization info
set system syslog file interactive-commands interactive-commands any
set system max-configurations-on-flash 5
set system max-configuration-rollbacks 5
set system license autoupdate url https://ae1.juniper.net/junos/key_retrieval
set system phone-home server https://redirect.juniper.net
set system phone-home rfc-compliant
set security ike traceoptions file ike-trace-log
set security ike traceoptions flag ike
set security ike proposal ike-v2-prop authentication-method pre-shared-keys
set security ike proposal ike-v2-prop dh-group group14
set security ike proposal ike-v2-prop authentication-algorithm sha-256
set security ike proposal ike-v2-prop encryption-algorithm aes-256-cbc
set security ike policy ike-policy-1 mode aggressive
set security ike policy ike-policy-1 proposals ike-v2-prop
set security ike policy ike-policy-1 pre-shared-key ascii-text
"$9$45aJUikPF6A24aUji.mO1IcevW8X"
set security ike gateway ike-gate-1 ike-policy ike-policy-1
set security ike gateway ike-gate-1 address 184.99.162.119
set security ike gateway ike-gate-1 dead-peer-detection optimized
set security ike gateway ike-gate-1 dead-peer-detection interval 10
set security ike gateway ike-gate-1 dead-peer-detection threshold 5
set security ike gateway ike-gate-1 local-identity user-at-hostname "l2-
remote@designlogic.net"
set security ike gateway ike-gate-1 remote-identity key-id L2-Hub
set security ike gateway ike-gate-1 external-interface ge-0/0/0
set security ike gateway ike-gate-1 version v2-only
set security ipsec vpn-monitor-options interval 10
set security ipsec vpn-monitor-options threshold 10
set security ipsec proposal ipsec-prop protocol esp
```

```
set security ipsec proposal ipsec-prop authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-prop encryption-algorithm aes-128-cbc
set security ipsec policy ipsec-policy-1 perfect-forward-secrecy keys group1
set security ipsec policy ipsec-policy-1 proposals ipsec-prop
set security ipsec vpn ipsec-vpn-1 bind-interface st0.0
set security ipsec vpn ipsec-vpn-1 df-bit clear
set security ipsec vpn ipsec-vpn-1 vpn-monitor optimized
set security ipsec vpn ipsec-vpn-1 ike gateway ike-gate-1
set security ipsec vpn ipsec-vpn-1 ike ipsec-policy ipsec-policy-1
set security ipsec vpn ipsec-vpn-1 establish-tunnels immediately
set security screen ids-option untrust-screen icmp ping-death
set security screen ids-option untrust-screen ip source-route-option
set security screen ids-option untrust-screen ip tear-drop
set security screen ids-option untrust-screen tcp syn-flood alarm-threshold 1024
set security screen ids-option untrust-screen tcp syn-flood attack-threshold 200
set security screen ids-option untrust-screen tcp syn-flood source-threshold
1024
set security screen ids-option untrust-screen tcp syn-flood destination-threshold
2048
set security screen ids-option untrust-screen tcp syn-flood timeout 20
set security screen ids-option untrust-screen tcp land
set security policies from-zone VPN-L2 to-zone VPN-L2 policy allow-all match
source-address any
set security policies from-zone VPN-L2 to-zone VPN-L2 policy allow-all match
destination-address any
set security policies from-zone VPN-L2 to-zone VPN-L2 policy allow-all match
application any
set security policies from-zone VPN-L2 to-zone VPN-L2 policy allow-all then
permit
set security zones security-zone untrust screen untrust-screen
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-
traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-
traffic system-services ssh
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-
traffic system-services dhcp
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-
traffic system-services ping
set security zones security-zone untrust interfaces pp0.0 host-inbound-traffic
system-services ike
set security zones security-zone untrust interfaces pp0.0 host-inbound-traffic
system-services ssh
set security zones security-zone untrust interfaces pp0.0 host-inbound-traffic
system-services dhcp
set security zones security-zone untrust interfaces pp0.0 host-inbound-traffic
```

```
system-services ping
set security zones security-zone VPN-L2 host-inbound-traffic system-services all
set security zones security-zone VPN-L2 host-inbound-traffic protocols all
set security zones security-zone VPN-L2 interfaces lo0.0
set security zones security-zone VPN-L2 interfaces st0.0
set security zones security-zone VPN-L2 interfaces gr-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet dhcp
set interfaces gr-0/0/0 description "GRE tunnel to Hub"
set interfaces gr-0/0/0 unit 0 clear-dont-fragment-bit
set interfaces gr-0/0/0 unit 0 tunnel source 10.255.10.10
set interfaces gr-0/0/0 unit 0 tunnel destination 10.255.10.1
set interfaces gr-0/0/0 unit 0 tunnel allow-fragmentation
set interfaces gr-0/0/0 unit 0 family inet mtu 2000
set interfaces gr-0/0/0 unit 0 family inet filter input inet-packet-mode
set interfaces gr-0/0/0 unit 0 family inet address 10.255.20.2/30
set interfaces gr-0/0/0 unit 0 family mpls mtu 1900
set interfaces gr-0/0/0 unit 0 family mpls filter input mpls-packet-mode
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces ge-0/0/6 encapsulation ethernet-ccc
set interfaces ge-0/0/6 unit 0 family ccc filter input l2circuit-packet-mode
set interfaces ge-0/0/7 mtu 1560
set interfaces ge-0/0/7 encapsulation ethernet-ccc
set interfaces ge-0/0/7 unit 0 family ccc filter input l2circuit-packet-mode
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
set interfaces lo0 unit 0 family inet address 10.255.255.10/32 primary
set interfaces lo0 unit 0 family mpls
set interfaces pp0 unit 0 apply-macro CenturyLink
set interfaces pp0 unit 0 ppp-options chap default-chap-secret
"$9$hPyreWLxdsY4IEv8XN2gmP5z9t"
set interfaces pp0 unit 0 ppp-options chap local-name
"<some_user>@centurylink.net"
set interfaces pp0 unit 0 ppp-options chap no-rfc2486
set interfaces pp0 unit 0 ppp-options chap passive
set interfaces pp0 unit 0 ppp-options pap local-name
"<some_user>@centurylink.net"
set interfaces pp0 unit 0 ppp-options pap no-rfc2486
set interfaces pp0 unit 0 ppp-options pap local-password
"$9$1XShSevWxdVs0BrKMLbwHk.f3/"
set interfaces pp0 unit 0 ppp-options pap passive
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 family inet negotiate-address
set interfaces st0 unit 0 family inet address 10.255.10.10/24
set routing-options static route 0.0.0.0/0 qualified-next-hop pp0.0 metric 1
deactivate routing-options static route 0.0.0.0/0
set routing-options router-id 10.255.255.10
```

```
set routing-options autonomous-system 65535
set protocols mpls interface gr-0/0/0.0
set protocols mpls interface lo0.0
set protocols bgp group VPLS type internal
set protocols bgp group VPLS multihop
set protocols bgp group VPLS local-address 10.255.255.10
set protocols bgp group VPLS mtu-discovery
set protocols bgp group VPLS family l2vpn signaling
set protocols bgp group VPLS neighbor 10.255.255.1
set protocols ospf area 0.0.0.0 interface lo0.0 passive
set protocols ospf area 0.0.0.0 interface gr-0/0/0.0
set protocols ldp interface gr-0/0/0.0
set protocols ldp interface all disable
set protocols ldp interface lo0.0
set protocols ldp session 10.255.255.1 authentication-key
"$9$k.m5z3901hik.5Qz6/lKvL-Vws2"
set protocols ldp session 10.255.255.11 authentication-key
"$9$KbBMWXNdsaGilKMX7Nbwmf5F9ApuO"
set protocols l2circuit neighbor 10.255.255.1 interface ge-0/0/7.0 virtual-circuit-
id 1
set protocols l2circuit neighbor 10.255.255.1 interface ge-0/0/7.0 ignore-mtu-
mismatch
set protocols l2circuit neighbor 10.255.255.11 interface ge-0/0/6.0 virtual-circuit-
id 3
set protocols l2-learning global-mode switching
set protocols rstp interface all
set firewall family inet filter inet-packet-mode term control-traffic from protocol
tcp
set firewall family inet filter inet-packet-mode term control-traffic from port 22
set firewall family inet filter inet-packet-mode term control-traffic from port 80
set firewall family inet filter inet-packet-mode term control-traffic from port 8080
set firewall family inet filter inet-packet-mode term control-traffic from port 646
set firewall family inet filter inet-packet-mode term control-traffic from port 179
set firewall family inet filter inet-packet-mode term control-traffic then accept
set firewall family inet filter inet-packet-mode term packet-mode then packet-
mode
set firewall family inet filter inet-packet-mode term packet-mode then accept
set firewall family mpls filter mpls-packet-mode term ALL-TRAFFIC then packet-
mode
set firewall family mpls filter mpls-packet-mode term ALL-TRAFFIC then accept
set firewall family ccc filter l2circuit-packet-mode term ALL-TRAFFIC then packet-
mode
set firewall family ccc filter l2circuit-packet-mode term ALL-TRAFFIC then accept
```

Revision #3
Created 27 June 2022 00:46:18 by Tyler

Updated 27 June 2022 01:23:53 by Tyler