Configuring Dynamic VPN

Version 1.2
November 2009

Table of Contents

Introduction

Dynamic VPN is Juniper's clientless solution for remote access IPSEC VPN. This client is dynamically delivered from the SRX to end users, and simplifies remote access by enabling users to establish secure IPSec VPN tunnels without having to configure VPN settings on their computers. This process is initiated by the client browsing to https://<serverhost>/dynamic-vpn and authenticates using a username and password.

Feature License

Dynamic-VPN is a licensed feature. Licenses are available for 5, 10, 25 and 50 concurrent users. A two user evaluation license is provided free of cost. These evaluation licenses do not expire. More information on licensing on specific products can be found at the product datasheet at http://www.juniper.net/us/en/local/pdf/datasheets/1000281-en.pdf .

Platform support

Table below lists the minimum software release required to support DVPN on SRX platforms:

Platform	JUNOS release
SRX 100	10.0
SRX 210	9.6
SRX 240	9.6
SRX 650	Not supported yet
SRX 3000 series	Not supported
SRX 5000 series	Not supported

The Dynamic-VPN client is supported on Windows XP and Windows Vista both32 bit and 64 bit versions and all service packs.

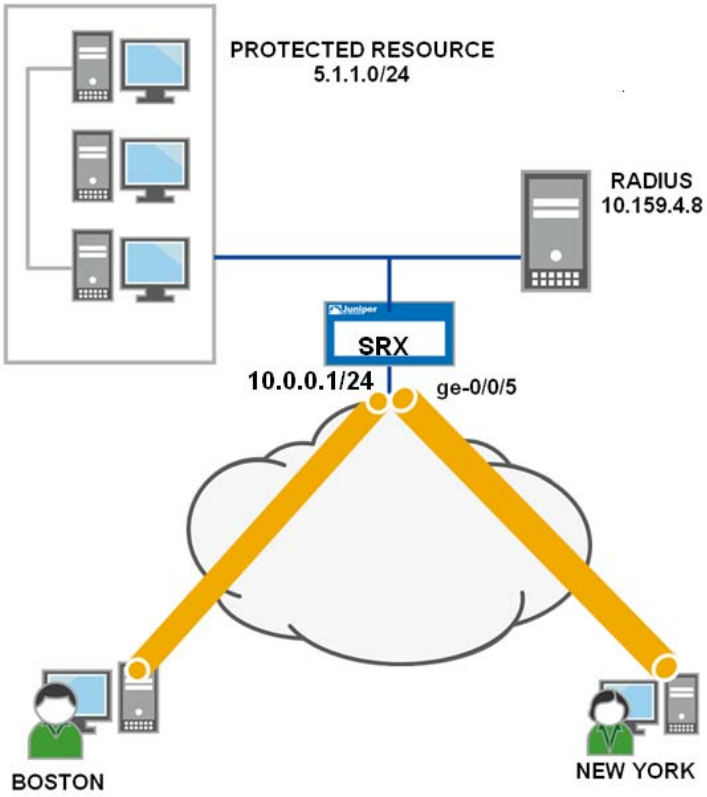
Limitations

- External RADIUS server is required for XAUTH and to provide an IP address
- Shared IKE id is not supported
- Perfect Forward Secrecy-PFS is mandatory
- Custom IKE/IPSEC security proposals are required
- FQDN is the only IKE-id supported

Dynamic VPN Example

Dynamic VPN requires configuration only on the SRX services gateway. The example below illustrates how two remote users, Boston and Newyork will establish a secure tunnel and communicate with a protected resource behind the SRX gateway. The user first navigates to the URL https://10.0.0.1/dynamic-vpn. The address 10.0.0.1 is the IP address of the public interface of the SRX gateway. The user then authenticates to the SRX gateway. The Dynamic-VPN client along with the necessary configuration is automatically downloaded. The user will be prompted to enter the Xauth username and password. The tunnel is then established and a virtual interface will be created on the Windows PC along with routes for the protected resources.

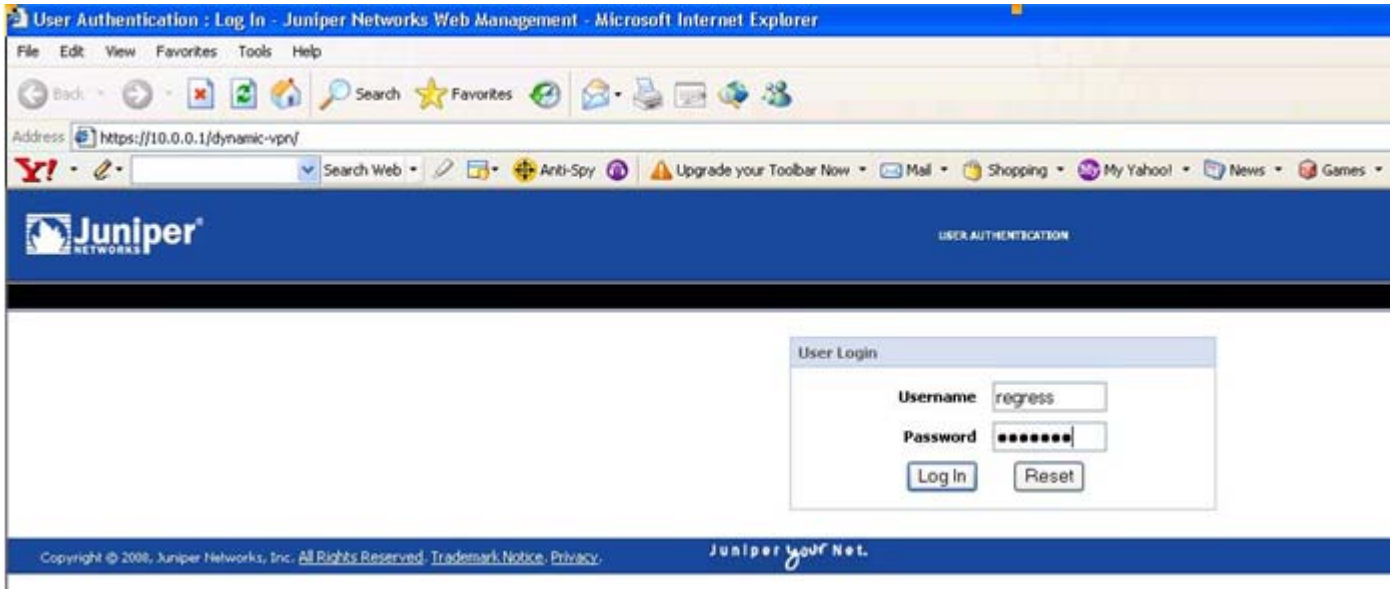
Topology



Sequence of Events

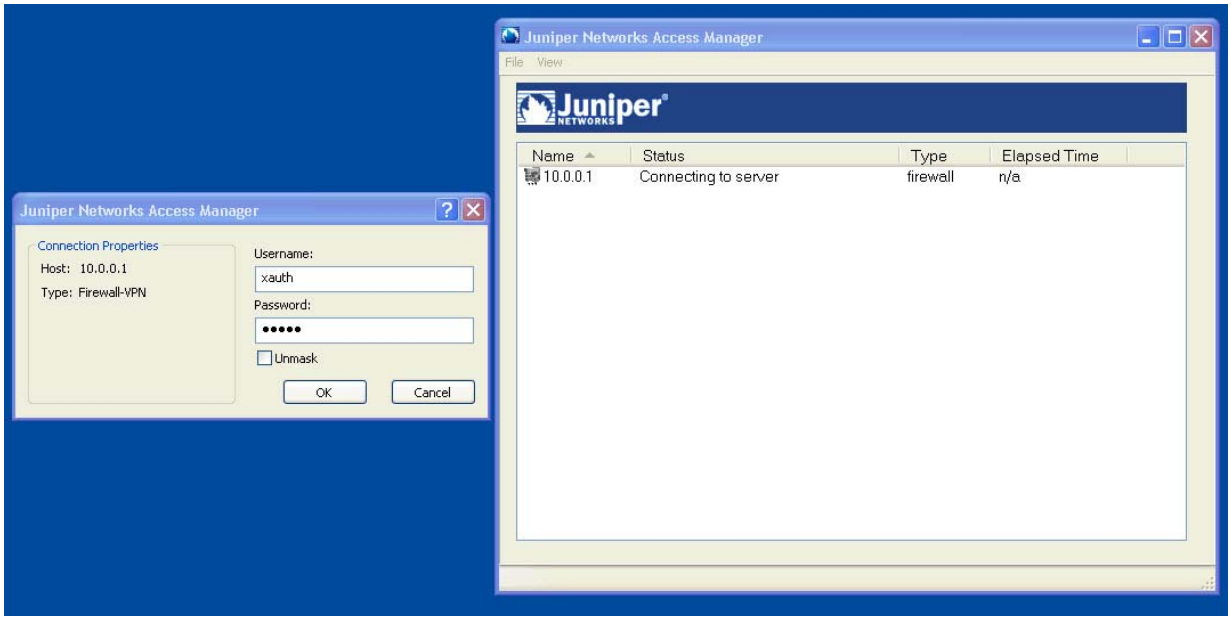
This section describes the sequence of events in establishing an IPSec tunnel to access the protected resource behind the SRX gateway.

1. User points the browser to https://10.0.0.1/dynamic-vpn
2. The WEBAUTH process on the SRX gateway prompts the user for login credentials. The user can be authenticated by local database on the SRX device or via a RADIUS server.

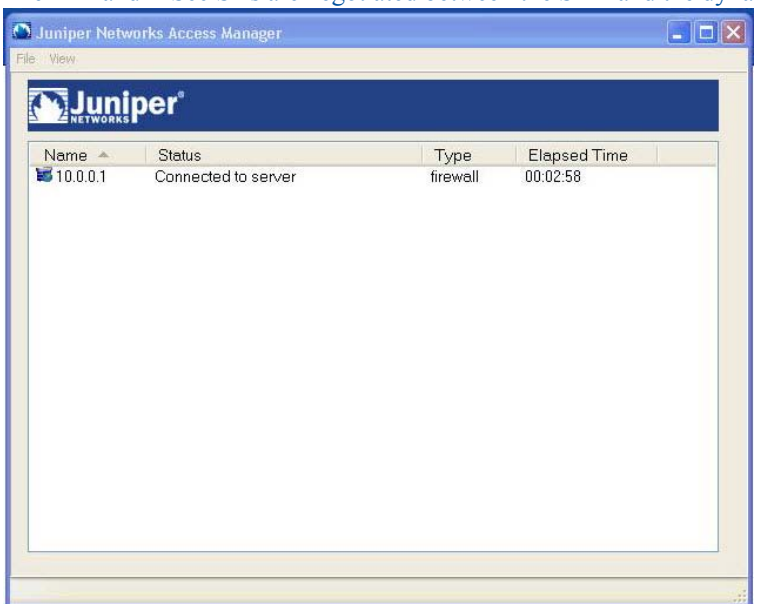


3. Upon successful authentication IPSec client is downloaded to the user's computer.
4. The user is then prompted to accept the certificate from the SRX gateway. Once the certificate is accepted, the relevant IPSec configuration to establish the tunnel is pushed from the SRX gateway to the IPSec client.

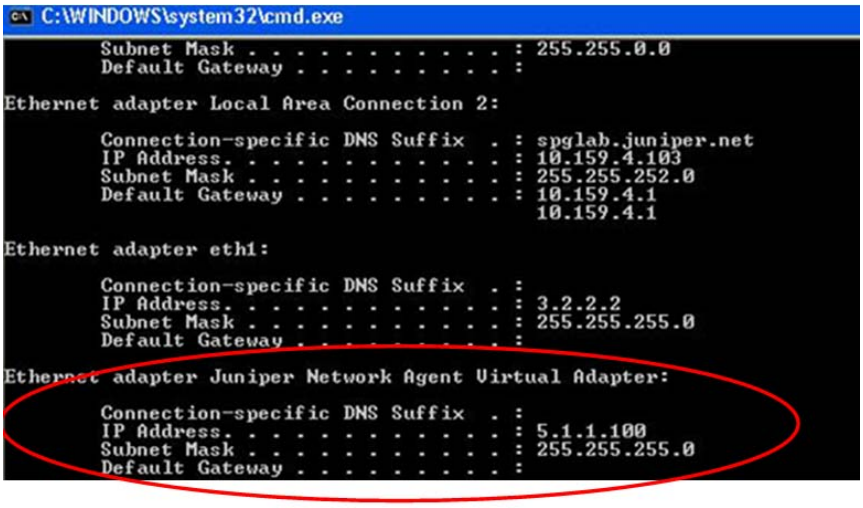
5. The dynamic client attempts to establish the IPSec tunnel.
6. The configuration on the SRX gateway initiates the XAUTH process, prompting the user for XAUTH credentials. XAUTH process on the SRX gateway requires a RADIUS server.



7. The user credentials are passed on to RADIUS server. The RADIUS server authenticates the user and also pushes an IP address and a subnet mask. In this example the client is assigned an IP address 5.1.1.100 and with subnet mask 255.255.255.0
8. The IKE and IPSec SAs are negotiated between the SRX and the dynamic-VPN client.



9. A virtual adapter is created on the client PC and routes to the protected resource are installed.
10. The user can now access the protected resources.




```
C:\Documents and Settings\Administrator>route print 5.1.1.0 mask 255.255.255.0
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 04 23 d0 93 27 ...... Intel(R) PRO/1000 MT Dual Port Server Adapter #2
 - Packet Scheduler Miniport
0x3 ...00 04 23 d0 93 26 ...... Intel(R) PRO/1000 MT Dual Port Server Adapter -
Packet Scheduler Miniport
0x10005 ...00 30 48 88 e2 78 ...... Broadcom NetXtreme Gigabit Ethernet #2 - Pac
ket Scheduler Miniport
0x10006 ...00 30 48 88 e2 79 ...... Broadcom NetXtreme Gigabit Ethernet - Packet
 Scheduler Miniport
0x30007 ...02 05 85 7f eb 80 ...... Juniper Networks Virtual Adapter - Packet Sc
heduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          5.1.1.0    255.255.255.0        5.1.1.100       5.1.1.100       10
Default Gateway:        10.159.4.1
```

Configuration

The configuration on the SRX Chassis can be divided into five steps

1. Access configuration
2. HTTPS configuration
3. IKE/IPSEC configuration
4. Dynamic VPN configuration
5. Policy Configuration

Step 1 : Access Configuration

The access configuration defines user profiles that are used for authentication. The profile *user-auth-profile* is used for authenticating via webauth to the SRX device when the user points the browser to https://srx-ip-address/dynamic-vpn. In this example the authentication is done using the local database with the users boston-user and newyork-user; these profiles are used in Step 4. (The steps for creating Dynamic VPN users in Steel Belted Radius are documented in the Appendix.)

It is possible to use RADIUS for web-authentication. The profile *radius-server* is used to specify the RADIUS server used for Xauth during IKE negotiation.

```
  root@coloclaw# show access
  profile user-auth-profile {
      client boston-user {
          firewall-user {
              password "$9$bns4JGUH.fQDiQ3/tIRvM8"; ## SECRET-DATA
          }
      }
      client newyork-user {
          firewall-user {
              password "$9$km5FCtOcyKn/yKM8dVqmf"; ## SECRET-DATA
          }
      }
  }
  profile radius-server {
      authentication-order radius;
      radius-server {
          10.159.4.8 secret "$9$HkfzCtOEcl69A01Irl"; ## SECRET-DATA
      }
  }
  firewall-authentication {
      web-authentication {
          default-profile radius-server;
      }
      }
  [edit]
root@coloclaw#
```

Step 2: HTTPS Configuration

This configuration is used to enable https service on the SRX chassis. It also used to generate a local certificate for https and define which interfaces the https daemon binds to.

```
root@coloclaw# show system services web-management https

system-generated-certificate;

interface ge-0/0/5.0;

[edit]

root@coloclaw#
```

Step 3: IKE/IPSec Configuration

This section defines the phase1 and phase2 parameters for IPSec tunnel setup. In the below configuration we use the profile *radius-server* for XAUTH which is defined under the access configuration.

IMPORTANT NOTE: AN IKE gateway and VPN must be defined for every single remote user that will require remote access via the dynamic VPN tunnel. (In other words, for every user, there must be a corresponding IKE gateway and VPN). If you have 20 users at a site and a Dynamic VN license on your SRX for only 10 users, a separate user, IKE Gateway, and VPN must be defined for every user.

The RADIUS server defined in the access profile will be used in the XAUTH process to IP address to the IPSec client.

IKE (Phase1) Configuration

```
root@coloclaw# show security ike
proposal phase1-prop {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
policy ike-pol {
    mode aggressive;
    proposals phase1-prop;
    pre-shared-key ascii-text "$9$km5FCtOcyKn/yKM8dVqmf"; ## SECRET-DATA
}

gateway dyn-gw-boston {
    ike-policy ike-pol;
    dynamic hostname boston;
    external-interface ge-0/0/5.0;
    xauth access-profile radius-server;
}

gateway dyn-gw-newyork {
    ike-policy ike-pol;
```

```
      dynamic hostname newyork;
      external-interface ge-0/0/5.0;
      xauth access-profile radius-server;
  }
root@coloclaw#
```

IPSec (Phase 2) Configuration

```
  root@coloclaw# show security ipsec
  proposal phase2-prop {
      protocol esp;
      authentication-algorithm hmac-sha1-96;
      encryption-algorithm 3des-cbc;
  }
  policy ipsec-pol {
      perfect-forward-secrecy {
          keys group2;
      }
      proposals phase2-prop;
  }
  vpn dynamic-vpn-boston {
      ike {
          gateway dyn-gw-boston;
          ipsec-policy ipsec-pol;
      }
  }
  vpn dynamic-vpn-newyork {
      ike {
          gateway dyn-gw-newyork;
          ipsec-policy ipsec-pol;
      }
  }
root@coloclaw#
```

Step 4: Dynamic VPN Configuration

The dynamic VPN configuration defines the protected resources that can be accessed only through the VPN tunnel and associates the remote user to an IPSec tunnel.

In the CLI remote-protected-resources identify the networks or hosts that will access via the tunnel encrypted and remote-exceptions identify that networks to which traffic is sent in clear text.

In this example the user *boston-user* is associated with the IPSec VPN *dynamic-vpn-boston* and only the traffic destined to the subnet 5.1.1.0/24 will be encrypted. The rest of the traffic will be clear text. It is possible to have multiple subnets/hosts as protected resources and remote exceptions.

```
  root@coloclaw# show security dynamic-vpn

  access-profile user-auth-profile;
  clients {
      client1 {
          remote-protected-resources {
              5.1.1.0/24;
```

```
        }

        remote-exceptions {
            0.0.0.0/0;
        }
        ipsec-vpn dynamic-vpn-boston;
        user {
            boston-user;
        }
    }
    client2 {
        remote-protected-resources {
            5.1.1.0/24;
        }
        remote-exceptions {
            0.0.0.0/0;
        }
        ipsec-vpn dynamic-vpn-newyork;
        user {
            newyork-user;
        }
  }
}
[edit]
root@coloclaw#
```

Step 5: Policy Configuration

The policy configuration defines security policy for allowing traffic to traverse the SRX chassis. It also defines the IPSec tunnel binding. One important thing to note is that the first policy to meet the match criteria need not necessarily be the policy that is used for the tunnel (see explanation below).

```
root@coloclaw# show security policies from-zone untrust to-zone trust
policy vpn-boston {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit {
            tunnel {
                ipsec-vpn dynamic-vpn-boston;
            }
        }
    }
}
policy vpn-newyork {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit {
            tunnel {
                ipsec-vpn dynamic-vpn-newyork;
            }
```

```
            }
        }
    }
    root@coloclaw#
```

From the above snippet, it may appear that the policy with "vpn-newyork" will never match. However this is an exception only for remote access VPN. For remote access, the VPN policy match is based on the IPSec tunnel that is bound to the dynamic VPN. Hence if the IKE and IPSec SA's are up for VPN "dynamic-vpn-newyork" the policy with vpn-newyork is matched and not policy vpn-boston. This may seem counter intuitive, but this exception is needed when there are similar match criteria for different VPN tunnels in the same zone context.

Technical Documentation Reference

For additional information, refer to the following technical documentation:

JUNOS Software, Security Configuration Guide, Chapter 17 - Dynamic VPNs

PDF:

http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/junos-security-swconfig-security.pdf

HTML:

http://www.juniper.net/techpubs/software/junos-security/junos-security96/junos-security-swconfig-security/frameset.html.

Troubleshooting Dynamic VPN

Unable to connect to the https://router-ip/dynamic-vpn?

- Verify the SRX gateway's IP address is reachable. The system service ping must be enabled on the interface for it respond to ICMP echo requests
- Verify that a certificate is configured and HTTPS service is enabled on the interface. Use the command: ***show system services web-management https***
- If the problem still persists enable traceoptions using the command ***set system services web-management traceoptions flag all***. The logs can be viewed using the operational mode command ***show log httpd-gk***

Login at https://router-ip/dynamic-vpn always fails with the message user not found?

Configure authd debug with the following config command ***"set system processes general-authentication-service traceoptions flag all"*** and check the logs at /var/log/authd .The logs can be viewed using the operational mode command ***"show log authd"***

Login at https://router-ip/dynamic-vpn always fails with the message no configuration for user

Verify the configuration for any errors. There must be a dynamic VPN access profile as described in step 4 configured for every remote user. If the error persists with the dynamic VPN access profile configured, from the Unix shell delete token-info file ***"rm -rf /var/db/dynamic-vpn-ipsec/tokens-info"***
Then restart web-management from the operational CLI using the command ***"restart web-management"***

The client fails to download after successful login at https://router-ip/dynamic-vpn

Look for logs in the httpd-gk file. Enable traceoptions using the command ***set system services web-management traceoptions flag all***. The logs can be viewed using the operational mode command ***show log httpd-gk***

The client downloads, but I am never prompted for Xauth?

Configure traceoptions for IKE logging with the following command ***set security ike traceoptions flag all***
Check the logs at "/var/log/kmd" for any phase-1 errors like "no proposal choosen" or "no vpn found ".
If you the above errors are present, view the logs in "/var/log/httpd-gk" to see what IKE/IPSec parameters were pushed to the remote client.
If there are no messages in "/var/log/kmd" the dynamic-VPN client did not trigger the tunnel. Client side debug needs to performed.

Xauth succeeds but the connection is never established?

Verify the IKE and IPSec SA and tunnel sessions are established.

```
root@coloclaw# run show security ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
2629    10.0.0.101      UP     c2f78e874174f510  26fdd605fb9b912e  Aggressive
2630    10.0.0.102      UP     30dcd92afb08d32d  76dfcfbe2b5ae837  Aggressive

root@coloclaw# run show security ipsec security-associations
  Total active tunnels: 2
```

```
    ID    Gateway         Port  Algorithm          SPI         Life:sec/kb  Mon vsys
    <2    10.0.0.101      500   ESP:3des/sha1    59efbecf  28772/ 450000 -   0
    >2    10.0.0.101      500   ESP:3des/sha1    b7cf005   28772/ 450000 -   0
    <3    10.0.0.102      500   ESP:3des/sha1    bc7948b0 12397/ 449988 -   0
    >3    10.0.0.102      500   ESP:3des/sha1    d636d7ae  12397/ 449988 -   0
    <3    10.0.0.102      500   ESP:3des/sha1    8582728d  25395/ 449988 -   0
    >3    10.0.0.102      500   ESP:3des/sha1    7b8ef29a  25395/ 449988 -   0

root@coloclaw#
   root@coloclaw# run show security flow session tunnel
   Session ID: 3, Policy name: N/A, Timeout: N/A
     In: 10.0.0.102/34178 --> 10.0.0.1/29325;esp, If: ge-0/0/5.0
   Session ID: 4, Policy name: N/A, Timeout: N/A
     In: 0.0.0.0/0 --> 10.0.0.1/0;esp, If: ge-0/0/5.0
   Session ID: 61646, Policy name: N/A, Timeout: N/A
     In: 10.0.0.101/48249 --> 10.0.0.1/18608;esp, If: ge-0/0/5.0
   Session ID: 61647, Policy name: N/A, Timeout: N/
     In: 10.0.0.101/0 --> 10.0.0.1/0;esp, If: ge-0/0/5.0
   4 sessions displayed
   root@coloclaw#
```

If there are no SAs or the tunnel session check the logs at "/var/log/kmd".

Configuring Radius

The snippet shows the RADIUS configuration from the file /etc/raddb/users of the free RADIUS server which was used for this example.

```
   xauth   Auth-Type := Local, User-Password == "xauth"
                Service-Type = Login-User,
                Login-Service = Telnet,
                Framed-IP-Address = 5.1.1.100,
                Framed-IP-Netmask = 255.255.255.0

   xauth1   Auth-Type := Local, User-Password == "xauth1"
                Service-Type = Login-User,
                Login-Service = Telnet,
                Framed-IP-Address = 5.1.1.200,
                Framed-IP-Netmask = 255.255.255.0
```

Full Configuration

The complete configuration from the router is pasted below.

```
system {
    ports {
        console log-out-on-disconnect;
    }
    root-authentication {
        encrypted-password "$1$c4d/BCbo$HG5uIZqnnuJoMpAjIBLDT/"; ## SECRET-DATA
    }

    services {
        web-management {
            traceoptions {
                level all;
                flag dynamic-vpn;
            }
            http {
                interface ge-0/0/5.0;
            }
            https {
                system-generated-certificate;
                interface ge-0/0/5.0;
            }
        }
    }
    processes {
        general-authentication-service {
            traceoptions {
```

```
                flag all;
            }
        }
    }
}
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 10.159.5.173/22;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 5.1.1.1/24;
            }
        }
    }
    ge-0/0/5 {
        unit 0 {
            family inet {
                address 10.0.0.1/24;
            }
        }
    }
}
routing-options {
    static {
```

```
        route 0.0.0.0/0 next-hop 10.159.4.1;
    }
}
security {
    ike {
        traceoptions {
            flag all;
            level 15;
        }
        proposal phase1-prop {

            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm 3des-cbc;
        }
        policy ike-pol {
            mode aggressive;
            proposals prop;
            pre-shared-key ascii-text "$9$km5FCtOcyKn/yKM8dVqmf"; ## SECRET-DATA
        }
        gateway dyn-gw-boston {
            ike-policy ike-pol;
            dynamic hostname boston;
            external-interface ge-0/0/5.0;
            xauth access-profile radius-server;
        }

        gateway dyn-gw-newyork {
            ike-policy ike-pol;
```

```
        dynamic hostname newyork;
        external-interface ge-0/0/5.0;
        xauth access-profile radius-server;
    }
}
ipsec {
    proposal phase2-prop {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
    }
    policy ipsec-pol {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals phase2-prop;
    }
    vpn dynamic-vpn-boston {
        ike {
            gateway dyn-gw-boston;
            ipsec-policy ipsec-pol;
        }
    }
    vpn dynamic-vpn-newyork {
        ike {
            gateway dyn-gw-newyork;
            ipsec-policy ipsec-pol;
        }
    }
}
```

```
zones {
    security-zone untrust {
        host-inbound-traffic {
            system-services {
                any-service;
            }
        }
        interfaces {
            ge-0/0/5.0;


        }
    }
    security-zone trust {
        host-inbound-traffic {
            system-services {
                any-service;
            }
        }
        interfaces {
            ge-0/0/1.0;
        }
    }
    security-zone management {
        host-inbound-traffic {
            system-services {
                any-service;
            }
        }
        interfaces {
            ge-0/0/0.0;
```

```
        }
    }
}
policies {
    from-zone untrust to-zone trust {
        policy vpn-boston {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn dynamic-vpn-boston;
                    }
                }
            }
        }
        policy vpn-newyork {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    tunnel {
                        ipsec-vpn dynamic-vpn-newyork;
                    }
```

```
                }
            }
        }
    }
}
dynamic-vpn {
    access-profile user-auth-profile;
    clients {

        client1 {
            remote-protected-resources {
                5.1.1.0/24;
            }
            remote-exceptions {
                0.0.0.0/0;
            }
            ipsec-vpn dynamic-vpn-boston;
            user {
                boston-user;
            }
        }
        client2 {
            remote-protected-resources {
                5.1.1.0/24;
            }
            remote-exceptions {
                0.0.0.0/0;
            }
            ipsec-vpn dynamic-vpn-newyork;
            user {
```

```
                    newyork-user;
                }
            }
        }
    }
}

access {
    profile user-auth-profile {
        client boston-user {
            firewall-user {
                password "$9$bns4JGUH.fQDiQ3/tIRvM8"; ## SECRET-DATA
            }
        }
        client newyork-user {
            firewall-user {
                password "$9$km5FCtOcyKn/yKM8dVqmf"; ## SECRET-DATA
            }
        }

    }
    profile radius-server {
        authentication-order radius;
        radius-server {
            10.159.4.8 secret "$9$HkfzCtOEcl69A01Irl"; ## SECRET-DATA
        }
    }
    firewall-authentication {
        web-authentication {
            default-profile radius-server;
```

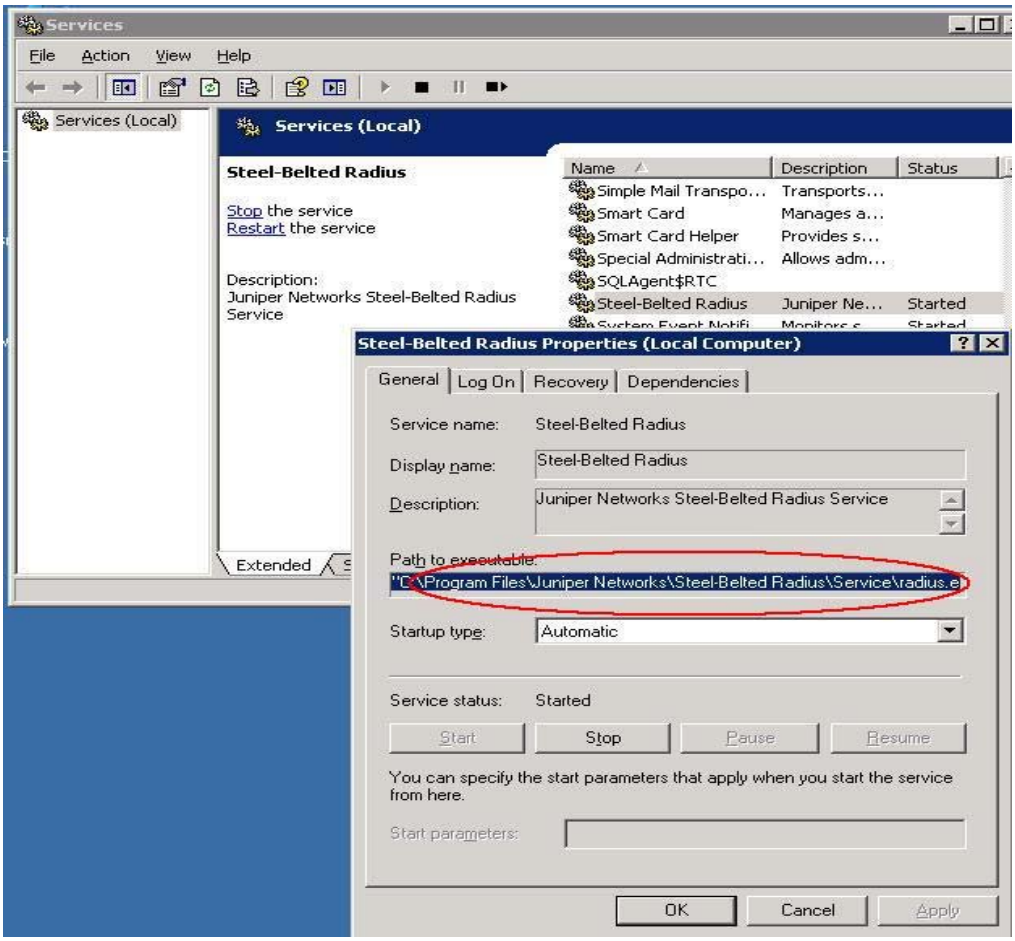
```
        }
        traceoptions {
            flag all;
        }
    }
}
```

Appendix - Configuring Steel Belted Radius

In this Application Note, users were authenticated to the local database. The steps for setting up Steel Belted Radius for Dynamic VPN users (based on SBR v5.3.0) are as follows:

1. Locate the Juniper Networks dictionary files on the Steel Belted Radius.

In order to modify the dictionary file, first find out the location from which the SBR instance is running. This can be located by going to the Start -> Administative Tools -> Services. Then right click and select properties as per the illustration below:



Go to the folder as highlighted above and locate the juniper.dct file. If the juniper.dct file is available, continue on to Step 2.

If the juniper.dct file is not available, create it. A sample dictionary file is attached to this technote in the KB.

After creating the juniper.dct file, you will also need to edit the vendor.ini file and add the following additional components.

vendor-product = Juniper M/T Series

dictionary = Juniper

ignore-ports = no

port-number-usage = per-port-type

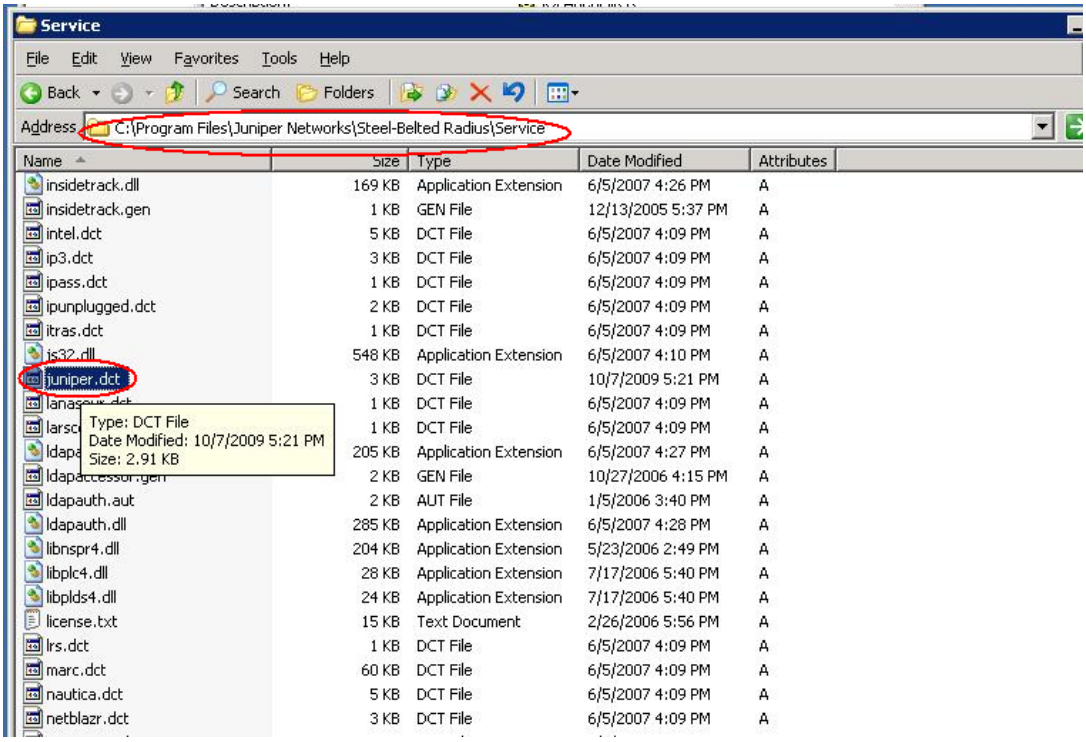
help-id = 2000

Important: Restart the SBR service from the Start -> Administative Tools -> Services tab (after creating the juniper.dct file and modifying the vendor.ini file).

.

2. Edit the juniper dictionary file

Edit the juniper.dct file.



The attributes that are required for Dynamic VPN are the following:

Framed-IP-Address

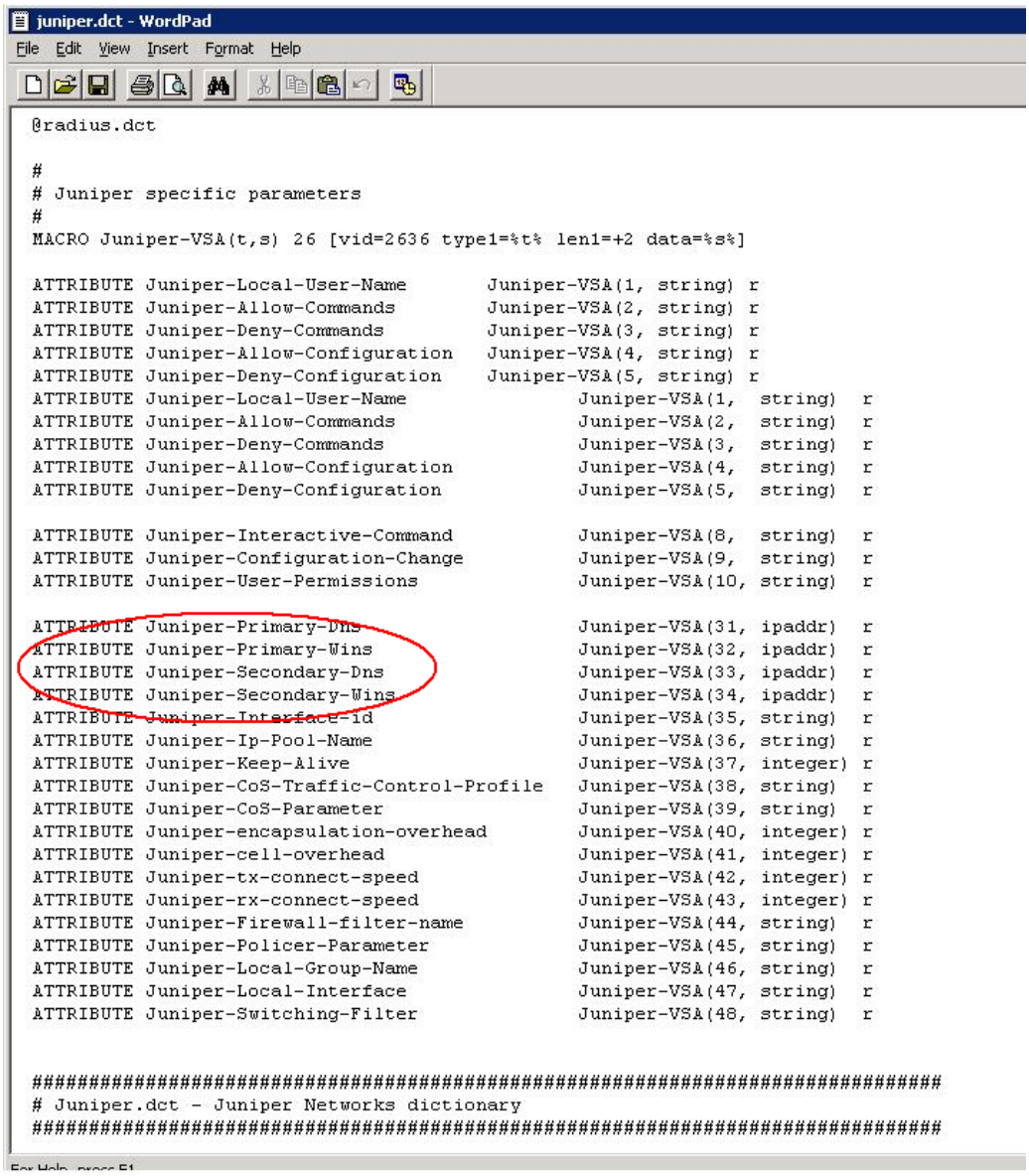
Framed-IP-Netmask

Juniper-Primary-Dns (Vendor Specific Attribute)

Juniper-Primary-Wins (Vendor Specific Attribute)

If these attributes are not in the juniper.dct file, add them.

After editing, the juniper.dct file should look something like the following:



juniper.dct - WordPad

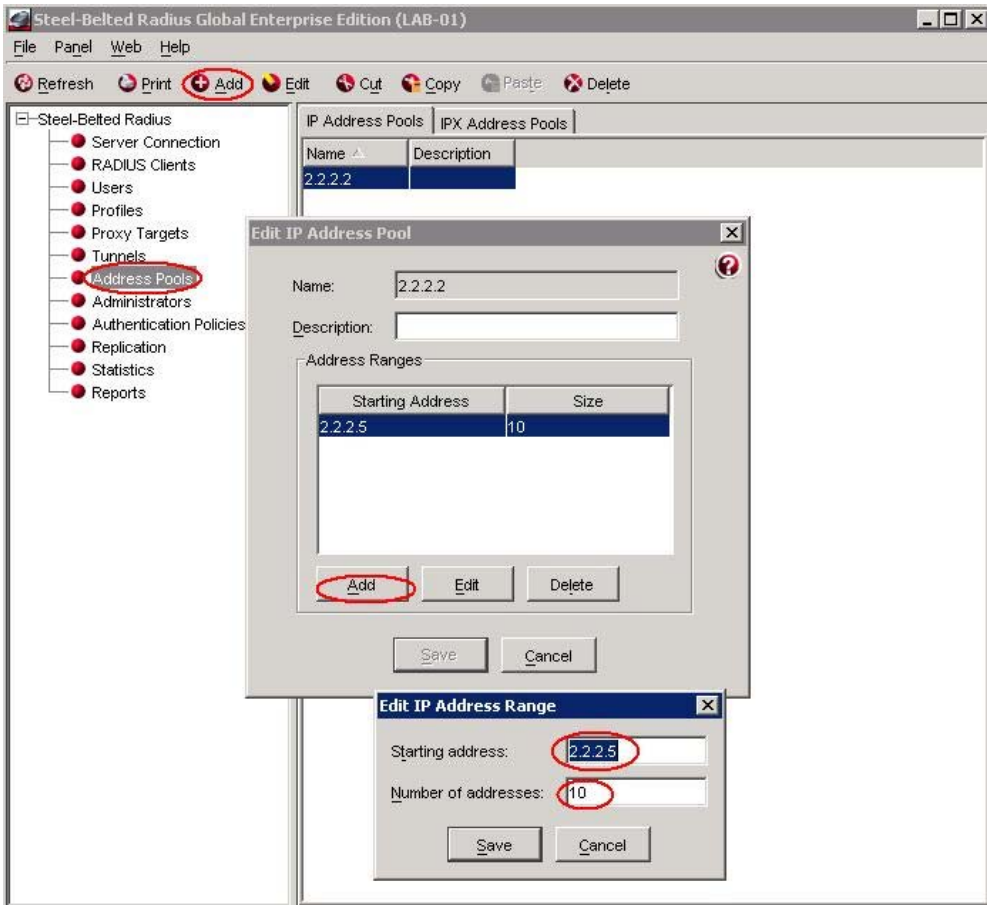
File Edit View Insert Format Help

```
@radius.dct

#
# Juniper specific parameters
#
MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%]

ATTRIBUTE Juniper-Local-User-Name       Juniper-VSA(1, string) r
ATTRIBUTE Juniper-Allow-Commands        Juniper-VSA(2, string) r
ATTRIBUTE Juniper-Deny-Commands         Juniper-VSA(3, string) r
ATTRIBUTE Juniper-Allow-Configuration   Juniper-VSA(4, string) r
ATTRIBUTE Juniper-Deny-Configuration    Juniper-VSA(5, string) r
ATTRIBUTE Juniper-Local-User-Name               Juniper-VSA(1,  string)  r
ATTRIBUTE Juniper-Allow-Commands                Juniper-VSA(2,  string)  r
ATTRIBUTE Juniper-Deny-Commands                 Juniper-VSA(3,  string)  r
ATTRIBUTE Juniper-Allow-Configuration           Juniper-VSA(4,  string)  r
ATTRIBUTE Juniper-Deny-Configuration            Juniper-VSA(5,  string)  r

ATTRIBUTE Juniper-Interactive-Command           Juniper-VSA(8,  string)  r
ATTRIBUTE Juniper-Configuration-Change          Juniper-VSA(9,  string)  r
ATTRIBUTE Juniper-User-Permissions              Juniper-VSA(10, string)  r

ATTRIBUTE Juniper-Primary-Dns                   Juniper-VSA(31, ipaddr)  r
ATTRIBUTE Juniper-Primary-Wins                  Juniper-VSA(32, ipaddr)  r
ATTRIBUTE Juniper-Secondary-Dns                 Juniper-VSA(33, ipaddr)  r
ATTRIBUTE Juniper-Secondary-Wins                Juniper-VSA(34, ipaddr)  r
ATTRIBUTE Juniper-Interface-id                  Juniper-VSA(35, string)  r
ATTRIBUTE Juniper-Ip-Pool-Name                  Juniper-VSA(36, string)  r
ATTRIBUTE Juniper-Keep-Alive                    Juniper-VSA(37, integer) r
ATTRIBUTE Juniper-CoS-Traffic-Control-Profile   Juniper-VSA(38, string)  r
ATTRIBUTE Juniper-CoS-Parameter                 Juniper-VSA(39, string)  r
ATTRIBUTE Juniper-encapsulation-overhead        Juniper-VSA(40, integer) r
ATTRIBUTE Juniper-cell-overhead                 Juniper-VSA(41, integer) r
ATTRIBUTE Juniper-tx-connect-speed              Juniper-VSA(42, integer) r
ATTRIBUTE Juniper-rx-connect-speed              Juniper-VSA(43, integer) r
ATTRIBUTE Juniper-Firewall-filter-name          Juniper-VSA(44, string)  r
ATTRIBUTE Juniper-Policer-Parameter             Juniper-VSA(45, string)  r
ATTRIBUTE Juniper-Local-Group-Name              Juniper-VSA(46, string)  r
ATTRIBUTE Juniper-Local-Interface               Juniper-VSA(47, string)  r
ATTRIBUTE Juniper-Switching-Filter              Juniper-VSA(48, string)  r


##############################################################################
# Juniper.dct - Juniper Networks dictionary
##############################################################################
```

For Help, press F1

3. Create an IP Pool for Dynamic VPN users

Start or go to the Steel-Belted Radius Application. Click the Address Pool option on the left panel, and then click the Add option as highlighted in red below.



Then setup the first IP address for the Dynamic VPN client and the number of addresses required.

Click save to save the configuration.

4. Configure the Radius Client (SRX)

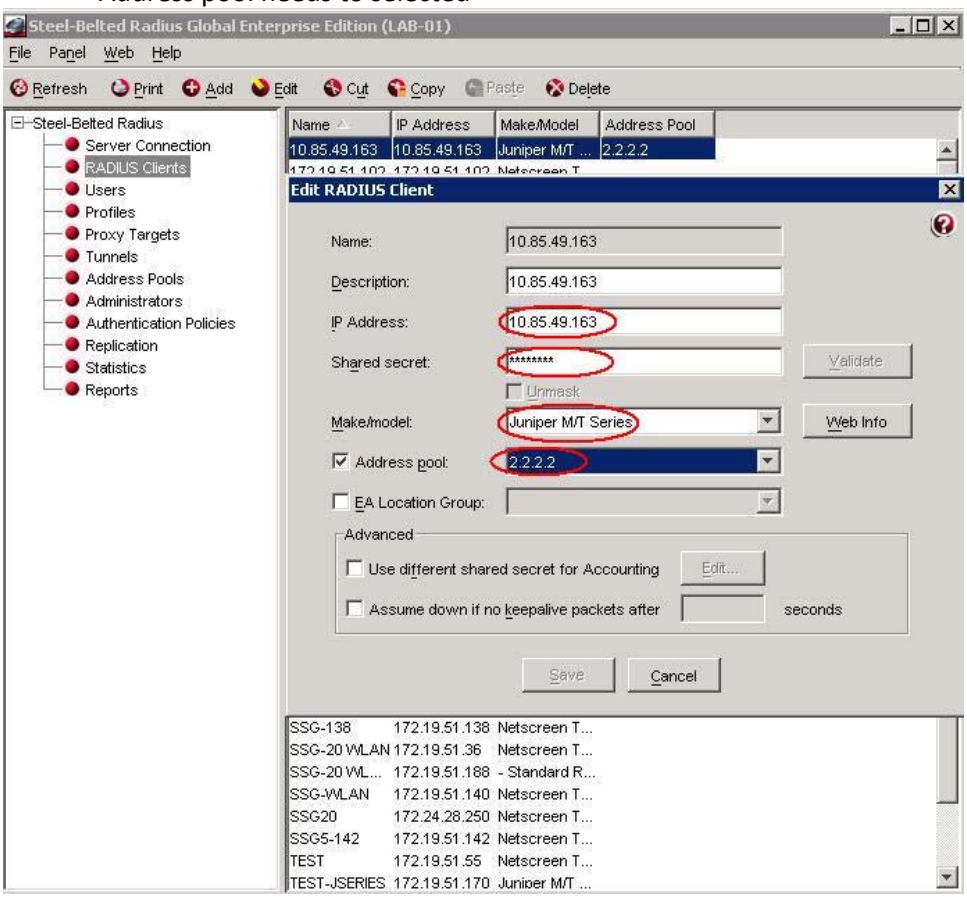
Click the RADIUS Clients option on the left panel, and make sure that the following fields are correctly configured:

- IP address (the IP address of the SRX)
- shared secret (it needs to be same value assigned on the SRX)
  EG:

  root@SRX210> show configuration access

```
profile radius-profile {
    authentication-order radius;
    radius-server {
        10.85.49.24 secret "$9$/JJeAu1Srv7-wRh-wYgUD9Ap";  **note hashed shared secret
    }
}
```

- Make/Model should be selected as the Juniper M/T Series
- Address pool needs to selected



5. Setup the Radius Access Profile

First, click the Profiles option and then the Add option.

On the Return list tab, select the Add option to add the following:

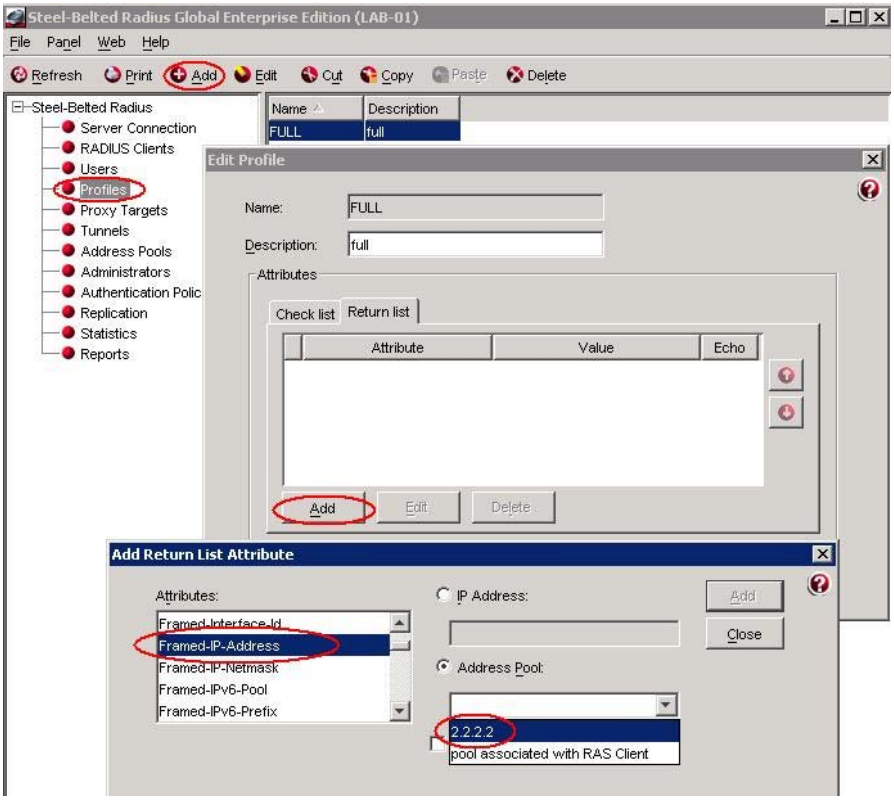
Framed-IP-Address

Framed-IP-Netmask

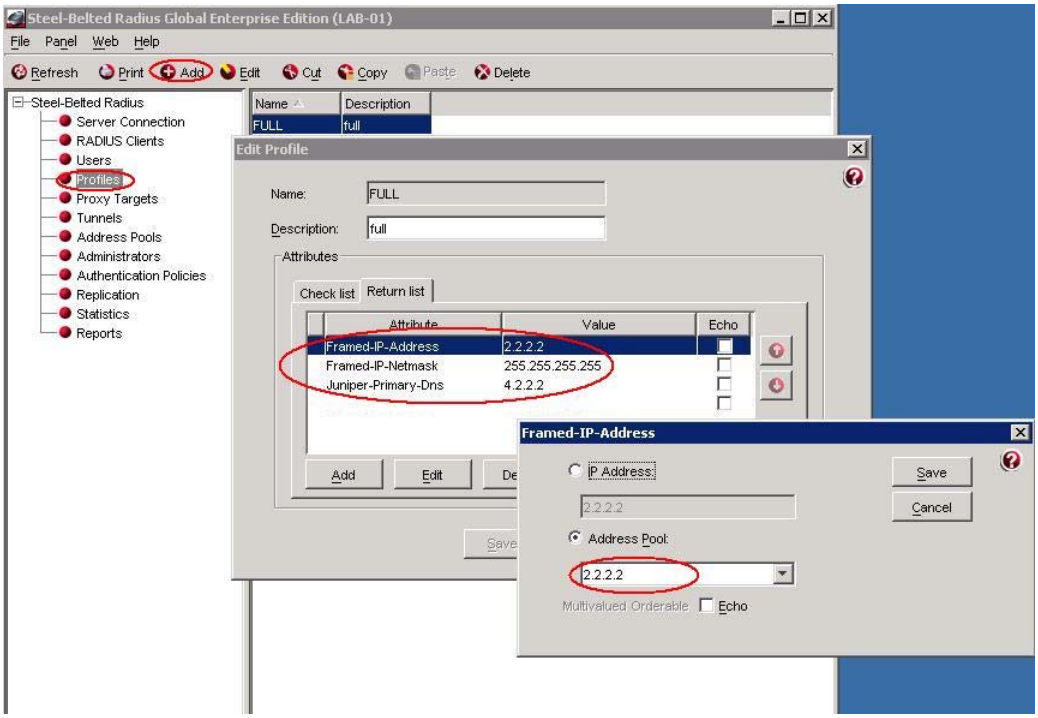
Juniper-Primary-Dns (Vendor Specific Attribute) *optional

Juniper-Primary-Wins (Vendor Specific Attribute) *optional

The following illustrates the setup:



The final setup should look like the following:

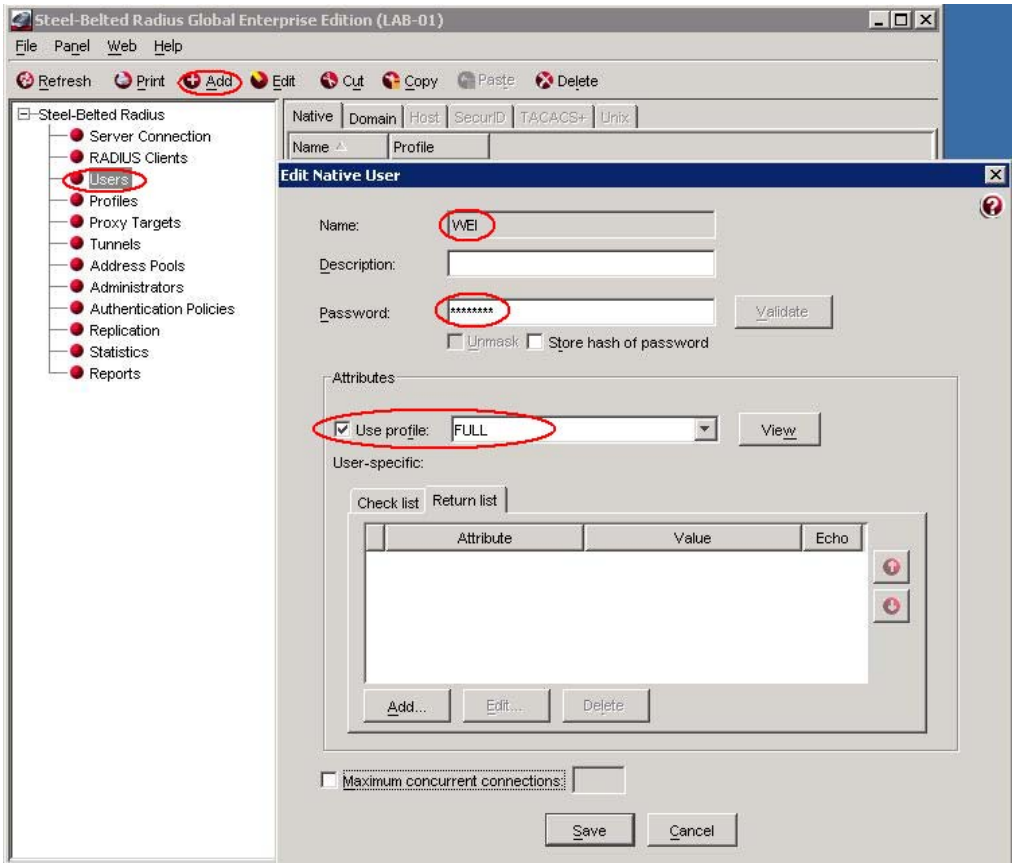


* Note that the Return list may be applied either to a specific user or to the Profile.

6. Create the users on the Steel Belted Radius

The last step is to setup the individual users (Dynamic VPN users) and apply the correct access profile to the users.

Click the Users option then select Add to add a new user. The highlighted fields, Name, Password, and Attributes profile, need to be filled in. Also ensure that the correct profile (created in the previous step). The following illustration is a sample configuration:



About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.