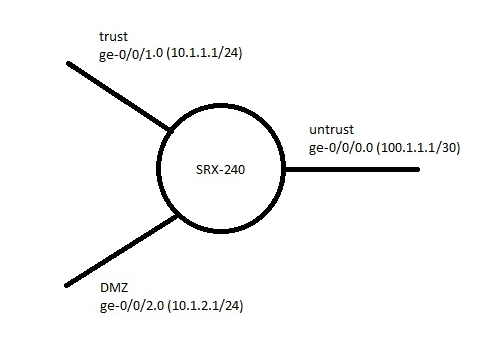
**Topology:**  
  
Consider the following scenario where ge-0/0/0, ge-0/0/1, and ge-0/0/2 are situated in untrust, trust, and DMZ zones respectively.  


ge-0/0/0 is the interface with which a user establishes a Dynamic VPN connection.   
  
  
**Goal:**  
The user needs to reach **10.1.1.0/24** and **10.1.2.0/24** networks once a Dynamic VPN connection is established.  
  
  
**Configuration:**

Assume that the SRX is configured to lease the dynamic-vpn user an IP address in the scope **10.10.10.0/24**.

1. Add the subnets from the trust and DMZ zones to the remote protected resources under the dynamic VPN configuration:

dynamic-vpn {

access-profile dyn-vpn-access-profile;

clients {

all {

remote-protected-resources {

**10.1.1.0/24;**

**10.1.2.0/24;**

}

remote-exceptions {

0.0.0.0/0;

}  
ipsec-vpn dyn-vpn;

user {

test;

}

}

}

}

1. Configure a new address book entry in the untrust zone for **10.10.10.0/24**, which is the subnet that is allocated for the VPN users:

zones {

security-zone untrust {

address-book {

**address 10.10.10.0/24 10.10.10.0/24;**

}

host-inbound-traffic {

system-services {

all;

}

protocols {

all;

}

}

interfaces {

ge-0/0/0.0;

}

}

1. Configure security policies for the user to access both the trust and DMZ networks:

policies {

from-zone untrust to-zone **trust**{

policy dyn-policy-trust {

match {

source-address any;  
destination-address any;  
application any;

}

then {

permit {

tunnel {

**ipsec-vpn dyn-vpn**;

}

}

}

}

}  
from-zone untrust to-zone **DMZ** {

policy dyn-policy-dmz {

match {

source-address **10.10.10.0/24**;  
destination-address any;  
application any;

}  
then {

permit;

}

}

}

}

Notice that only one policy refers to the VPN tunnel (**dyn-policy-trust**). This policy serves the following functions:

* It derives the proxy-id, from which the IPsec SA negotiations with the Junos Pulse VPN client will be accepted.
* It determines if the traffic which is coming out of the tunnel and going into the **trust zone**is allowed.

The Junos Pulse VPN client will attempt to negotiate and bring up two IPsec SAs (one for each subnet that is defined in the remote-protected-resources) and they will be accepted based on the **dyn-policy-trust**policy. After the VPN tunnel has been established, the ESP packets that arrive at the SRX device will first be decrypted, before a policy lookup is performed:

* When a VPN user tries to go to the **10.1.1.0/24** subnet, which is in the trust zone, it will match the **dyn-policy-trust**policy.

* When a VPN user tries to go to the **10.1.2.0/24** subnet, which is in the DMZ zone, it will match the **dyn-policy-dmz**policy.

For the policy that is inside the untrust to DMZ zone, notice that it specifies the source address as the dynamic-VPN user's assigned IP pool. This is to ensure that no other traffic from the untrust zone is able to access the DMZ zone and only the decrypted traffic from the VPN tunnel is allowed.