July 2007

Common Application Guide

VPN Based WAN Failover

Brief Overview of Application

A common scenario for many users involves two sites linked with a T1, each site with its own independent internet access. The point to point T1 provides site-to-site connectivity for many applications, but if the T1 fails, then the sites lose the ability to communicate with what could potentially be critical traffic. A method used to add redundancy to this scenario is VPN based failover. A VPN tunnel is configured for both sites to connect. Traffic is then directed through the T1 as a primary and over the VPN as a backup. This provides a safe and secure way to ensure communications between sites.

The basic theory behind this scenario involves both the use of static routes across the T1 as well as the binding of rules to specific security policies. When the T1 between the two sites fails, the router automatically removes the route to the other side, since an interface no longer exists in the same subnet as the T1. That, in turn, causes the "allow" rule permitting traffic between the two sites to fail since there is no longer a valid route within the security policy. Since the only route in place that matches the site to site traffic is the default route to the internet, the traffic is re-routed out the public interface. The crypto map applied to the public interface sees traffic that matches the VPN selectors, and the tunnel is initiated. At this point, site to site traffic has been restored and will continue to function until the T1 comes back up, at which point the static route will be automatically re-inserted and traffic will flow across the point to point link.

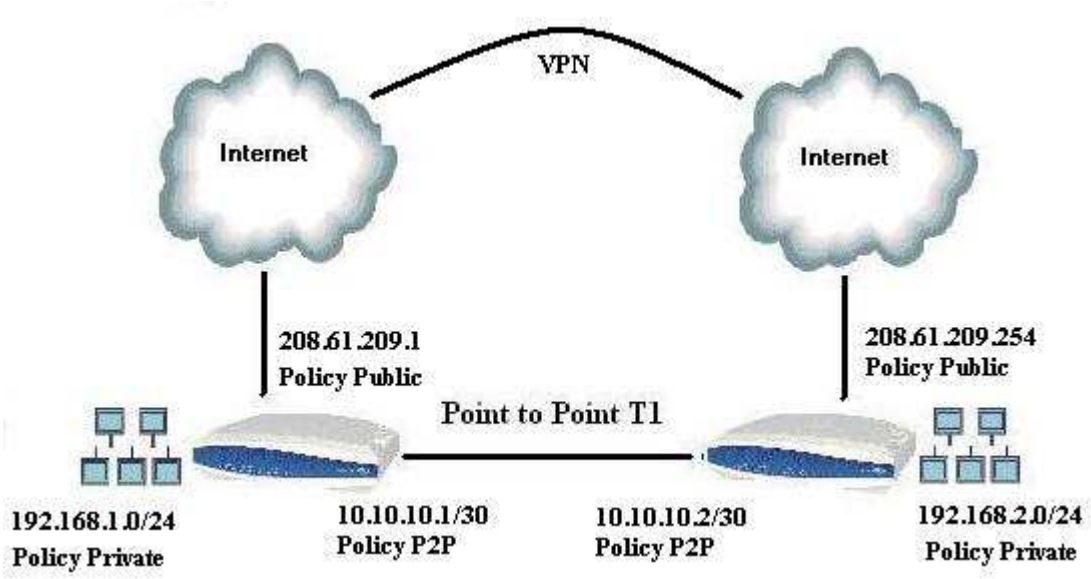
Hardware/Software Requirements/Limitations

The router must be capable of terminating an internet connection, a point to point connection, and a LAN. Examples of these routers include the 3305, 3430, 3448, 4305, 1224R, and 1335.

The router must have the Enhanced Feature Pack installed to enable VPN functionality.

Configuration in CLI and web GUI

Configuration for this application requires that a VPN tunnel be configured between the two sites. One of the most basic elements of VPN configuration is the VPN selector. This is an access list defined to determine which traffic goes through the tunnel. The VPN tunnel must be configured as it would be without taking the point to point network into account. This can be done either with the VPN Wizard or manually in the GUI, or through the CLI.



Configuring in the GUI

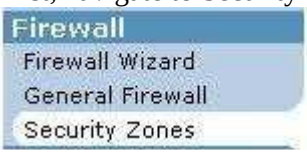
First, configure the VPN between the sites. For this example configuration, the two sites will be using the following settings:

Site A	Site B
Typical Setup	Typical Setup
Public Interface: Eth 0/1	Public Interface: Eth 0/1
Static Peer: 208.61.209.254	Static Peer: 208.61.209.1
Remote Network: 192.168.2.0 /24	Remote Network: 192.168.1.0 /24
Local Network: 192.168.1.0 /24	Local Network: 192.168.2.0 /24
PSK: 1234567890	PSK: 1234567890
Remote ID: IP Address 208.61.209.254	Remote ID: IP Address 208.61.209.1
Local ID: IP Address 208.61.209.1	Local ID: IP Address 208.61.209.254

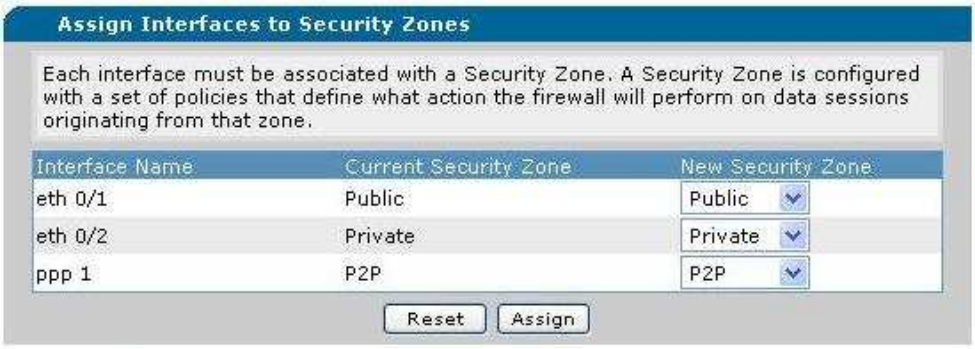
For additional information on how to configure a VPN in the GUI, please consult http://kb.adtran.com.

Once the VPN is configured, the firewall policies need to be modified. Firewall rules must exist to allow point to point traffic across the network. Additionally, the firewall rule must have a destination security policy set as the policy assigned to the point to point interface. Doing this links the allow to the state of the point to point interface. If the point to point network goes down, the router will skip the allow and move on to the next.

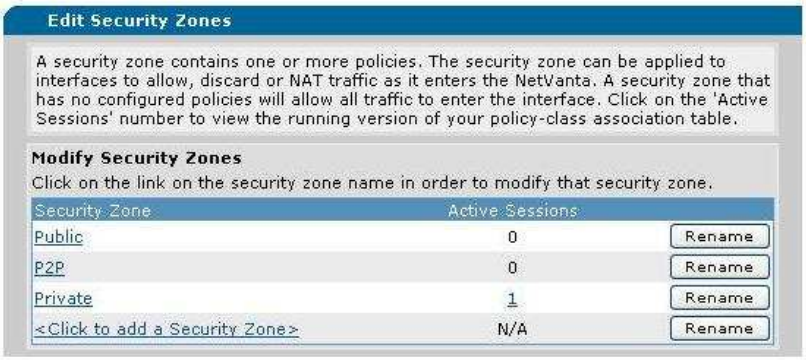
First, navigate to Security Zones.



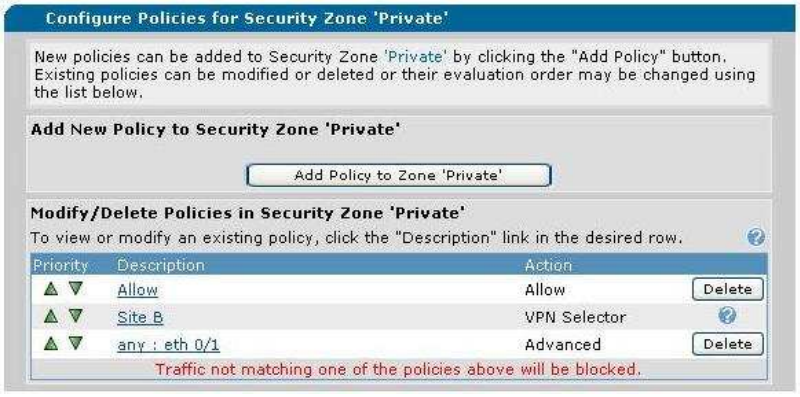
Next, ensure that you have three security zones created for your internet, LAN, and point to point connections.



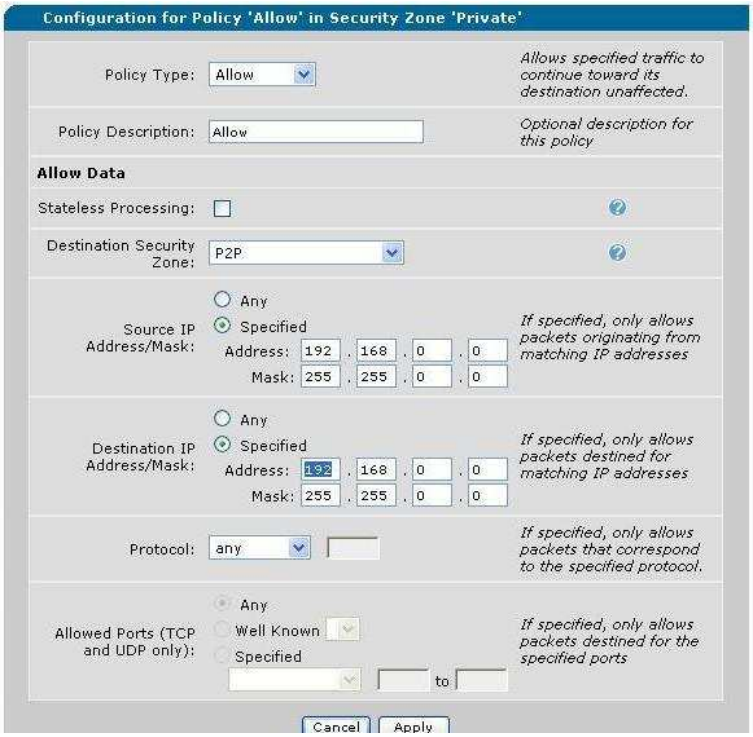
Next, navigate to the editing area and select your private security policy by clicking on the hyperlinked name.



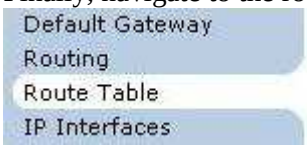
Next, ensure that 3 policies have been created. They should be ordered as below. An “allow” list will allow traffic between networks, followed by the VPN selectors, and finally the internet NAT.



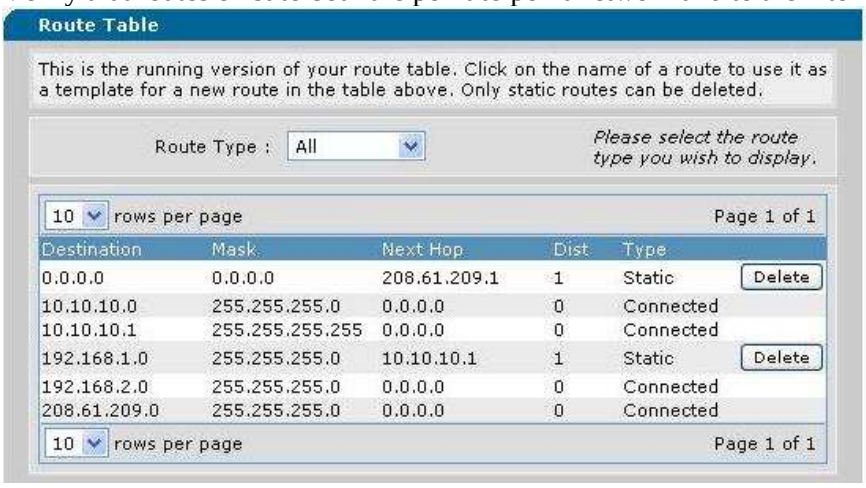
The “allow” policy should be configured with a destination security zone of the zone assigned to the point to point network. This will link the policy to the health of the routes in that security zone. Therefore, when the T1 goes down, traffic will no longer be allowed over it and the VPN will be triggered.



Finally, navigate to the route table.



Verify that routes exist to both the point to point network and to the internet.



Configuring in the CLI

1. Ensure that a separate security policy has been created and assigned to each interface

   Syntax: **ip policy-class** *<policy name>*
   EX: (config)# **ip policy-class Private**
   Syntax: **access-policy** *<policy name>*
   EX: (config-eth 0/2)# **access-policy Private**

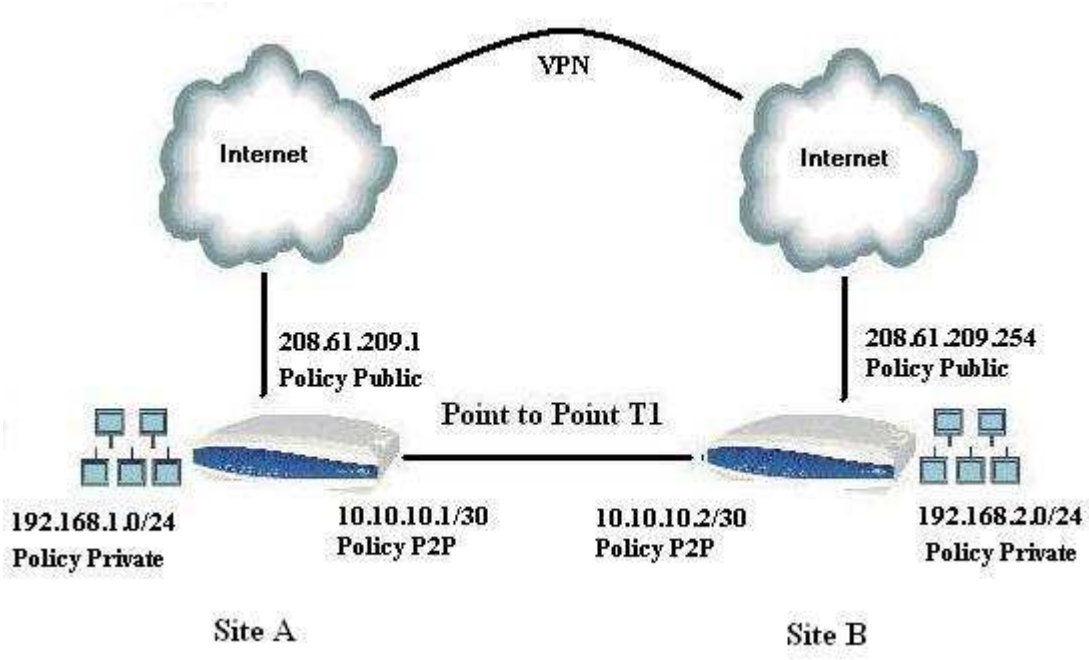
2. Create an access list which covers traffic from LAN to LAN.

   Syntax: **ip access-list extended** <*ACL name*>
   Syntax: **permit ip** <*source network*> <*wildcard mask*> <*destination network*> <*wildcard mask*>
   EX: **ip access-list extended LAN2LAN**
   EX: **permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255**

3. Apply the access list that has been created to the private security policy. Ensure that it is above all other policies and that it references the policy class assigned to the point to point.

   Syntax: **allow list** <*list name*> **policy** <*policy name*>
   Ex: **allow list LAN2LAN policy P2P**

Example configurations



Configuration for Site A	Configuration for Site B
hostname "Site_A" ! ip routing ! ip firewall ! ip crypto ! crypto ike policy 100 initiate main respond anymode local-id address 208.61.209.1 peer 208.61.209.254 attribute 1 encryption 3des hash md5 authentication pre-share ! crypto ike remote-id address 208.61.209.254 preshared-key 1234567890 ike-policy 100 crypto map VPN 10 no-mode-config no-xauth ! crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac mode tunnel ! crypto map VPN 10 ipsec-ike description Site B match address VPN-10-vpn-selectors set peer 208.61.209.254 set transform-set esp-3des-esp-md5-hmac ike-policy 100 ! ! !	hostname "Site_B" ! ip routing ! ip firewall ! ip crypto ! crypto ike policy 100 initiate main respond anymode local-id address 208.61.209.254 peer 208.61.209.1 attribute 1 encryption 3des hash md5 authentication pre-share ! crypto ike remote-id address 208.61.209.1 preshared-key 1234567890 ike-policy 100 crypto map VPN 10 no-mode-config no-xauth ! crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac mode tunnel ! crypto map VPN 10 ipsec-ike description Site B match address VPN-10-vpn-selectors set peer 208.61.209.1 set transform-set esp-3des-esp-md5-hmac ike-policy 100 ! ! !

```
!
interface eth 0/1
  ip address  208.61.209.1  255.255.255.0
  access-policy Public
  crypto map VPN
  no shutdown
!
interface eth 0/2
  ip address  192.168.1.1  255.255.255.0
  access-policy Private
  no shutdown
!
interface t1 2/1
  clock source internal
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address  10.10.10.1  255.255.255.0
  access-policy P2P
  no shutdown
  cross-connect 1 t1 2/1 1 ppp 1
!
ip access-list extended matchall
  permit ip any  any
!
ip access-list extended P2P
  permit ip 192.168.0.0 0.0.255.255  192.168.0.0 0.0.255.255
!
ip access-list extended VPN-10-vpn-selectors
  permit ip 192.168.1.0 0.0.0.255  192.168.2.0 0.0.0.255
!
ip policy-class P2P
  allow list VPN-10-vpn-selectors stateless
  allow list matchall
!
ip policy-class Private
  allow list P2P policy P2P
  allow list VPN-10-vpn-selectors stateless
  nat source list matchall interface eth 0/1 overload
!
ip policy-class Public
  allow reverse list VPN-10-vpn-selectors stateless
!
ip route 0.0.0.0 0.0.0.0 208.61.209.254
ip route 192.168.2.0 255.255.255.0 10.10.10.2
```

```
!
interface eth 0/1
  ip address  208.61.209.254  255.255.255.0
  access-policy Public
  crypto map VPN
  no shutdown
!
interface eth 0/2
  ip address  192.168.2.1  255.255.255.0
  access-policy Private
  no shutdown
!
interface t1 2/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
!
interface ppp 1
  ip address  10.10.10.2  255.255.255.0
  access-policy P2P
  no shutdown
  cross-connect 1 t1 2/1 1 ppp 1
!
ip access-list extended matchall
  permit ip any  any
!
ip access-list extended P2P
  permit ip 192.168.0.0 0.0.255.255  192.168.0.0 0.0.255.255
!
ip access-list extended VPN-10-vpn-selectors
  permit ip 192.168.2.0 0.0.0.255  192.168.1.0 0.0.0.255
!
ip policy-class P2P
  allow list VPN-10-vpn-selectors stateless
  allow list matchall
!
ip policy-class Private
  allow list P2P policy P2P
  allow list VPN-10-vpn-selectors stateless
  nat source list matchall interface eth 0/1 overload
!
ip policy-class Public
  allow reverse list VPN-10-vpn-selectors stateless
!
ip route 0.0.0.0 0.0.0.0 208.61.209.1
ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

Troubleshooting

For assistance in troubleshooting the VPN connection, please refer to the appropriate VPN configuration guide on the knowledgebase.

Issuing the command **show ip policy-sessions** from the command prompt allows the user to view the holes that are currently being opened in the firewall for traffic to pass. The following image shows a ping from a PC on site B to the Ethernet port on site A. Traffic is being allowed on the Private policy class.

```
Site_B#show ip policy-sessions

Protocol (TTL) [in crypto map] -> [out crypto map] Destination policy-class
  Src IP Address  Src Port Dest IP Address Dst Port NAT IP Address    NAT Port
  --------------- -------- --------------- -------- ----------------- --------

Policy class "P2P":

Policy class "Private":
icmp (60) -> P2P
  192.168.2.2     512      192.168.1.1     512

Policy class "Public":
```

When the T1 between the two routers is severed, another view of the policy sessions shows that there is now traffic between the public interfaces of the routers on port 500 (IPSec). The ping traffic also shows that it is traveling using the VPN selectors.

```
Site_B#show ip policy-sessions

Protocol (TTL) [in crypto map] -> [out crypto map] Destination policy-class
  Src IP Address  Src Port Dest IP Address Dst Port NAT IP Address    NAT Port
  --------------- -------- --------------- -------- ----------------- --------

Policy class "P2P":

Policy class "Private":
icmp (60) -> [VPN 10] Public
  192.168.2.2     512      192.168.1.1     512

Policy class "Public":

Policy class "self":
udp (32) -> Public
  208.61.209.254  500      208.61.209.1    500
```