*** Adtran to Cisco Tunnel Configuration ***

DSL circuit
(tunnel backup)

DSL circuit
(tunnel backup)

Public Internet

3.3.3.1/24
fe 0/1

2.2.2.6/24
eth 0/1

tunnel 869
172.29.29.1/30

BGP

BGP

tunnel 1
172.29.29.2/30

Cisco Router

Adtran NetVanta Router

AOS version R10.4.0.E

Private MPLS Cloud

MPLS circuit
(primary T1)

MPLS circuit
(primary T1)
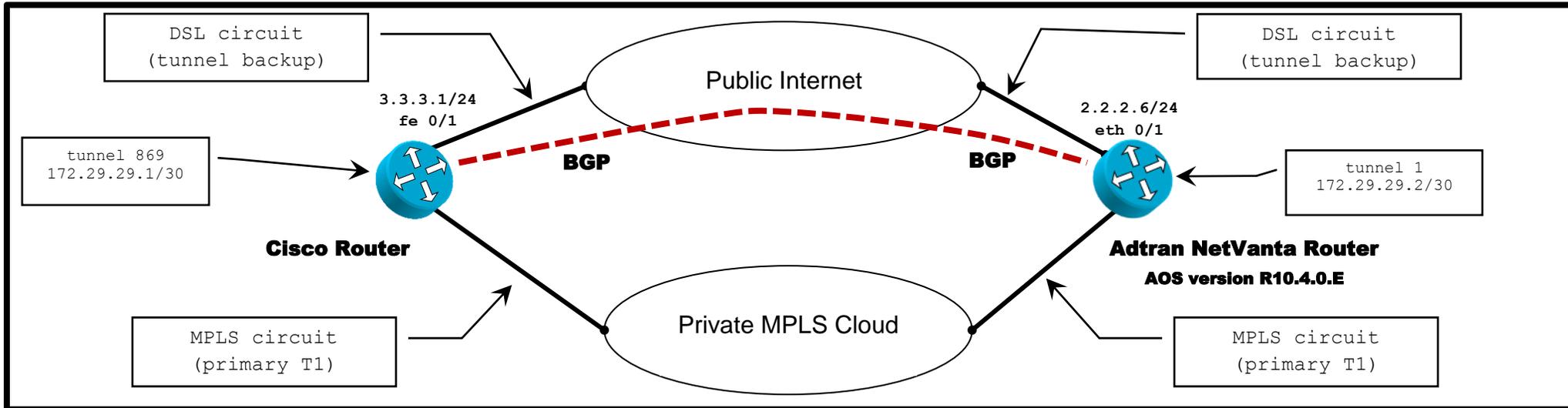
Adtran Crypto Commands

```
sh crypto ike remote-id
sh crypto ike sa {brief}
sh crypto ike policy
sh crypto ipsec sa {brief}
sh crypto ipsec transform-set
```

Adtran BGP Commands

```
sh bgp ipv4 neighbors x.x.x.x {routes} | {advertised-routes} | {received-routes}
sh bgp ipv4 summary
```

Configuration Footnotes

1. These "nat-traversal" lines are *sometimes* required for compatibility with Cisco defaults
2. This line *may* or *may not* need the following sections, experiment to find which works for you:
    a. "ike-policy 100"
    b. "crypto map VPN 10"
    c. "no-mode-config"
    d. "no-xauth"
3. As of October 2012, Adtran AOS only supports "mode tunnel". If the other side is configured for "mode transport", then it will negotiate (fall back to) "mode tunnel"
4. For troubleshooting, bouncing the public interface on the Adtran may work better than clearing crypto on the other side

filename: adtran_to_cisco_tunnel_gre_with_ipsec_configuration
creation date: 08 oct 2012

Adtran Configuration

```
!
ip firewall
!
ip crypto
!
crypto ike policy 100
  initiate main
  respond main
  local-id address 2.2.2.6
  nat-traversal v1 disable          <-------- 1
  nat-traversal v2 force            <-------- 1
  peer 3.3.3.1
  attribute 1
    encryption 3des
    hash md5
    authentication pre-share
    group 2
    lifetime 3600
!
crypto ike remote-id address 3.3.3.1 preshared-key Monchichi ike-policy 100 crypto map VPN 10 no-mode-config no-xauth   <-------- 2
!
crypto ipsec transform-set my-t-set esp-3des esp-md5-hmac
  mode tunnel        <--------------------------------------------- 3
!
crypto map VPN 10 ipsec-ike
  description GRE Tunnel Peer
  match address VPN-Selectors
  set peer 3.3.3.1
  set transform-set my-t-set
  set security-association lifetime kilobytes 216000
  set security-association lifetime seconds 3600
  set pfs group2
  ike-policy 100
!
interface eth 0/1
  description CONN TO PUBLIC INTERNET
  ip address  2.2.2.6  255.255.255.0
  ip access-policy Public
  crypto map VPN
  no shutdown
!
interface tunnel 1 gre ip
  ip address  172.29.29.2  255.255.255.252
  ip mtu 1400
  tunnel source 2.2.2.6
  tunnel destination 3.3.3.1
  no shutdown
!
router bgp 65001
  neighbor 172.29.29.1
    description BGP NEIGHBORSHIP ACROSS TUNNEL
    remote-as 65020
    no shutdown
    exit
  address-family ipv4
    network 192.168.1.0 mask 255.255.255.0
    neighbor 172.29.29.1
      soft-reconfiguration inbound
      no shutdown
      exit
    exit
!
ip access-list extended AdminAccess
  remark Public Admin Access
  permit tcp any  any eq ssh
  permit tcp any  any eq https
!
ip access-list extended allow-icmp
  permit icmp any  any
!
ip access-list extended VPN-Selectors
  remark GRE Tunnel Selectors
  permit gre host 2.2.2.6  host 3.3.3.1
!
ip policy-class Public
  allow reverse list VPN-Selectors stateless
  allow list AdminAccess self
  allow list allow-icmp self stateless
!
ip route 3.3.3.1 255.255.255.255 << x.x.x.x >>   <-------- where x.x.x.x is the next hop to the internet
!
end
```

Cisco Configuration

```
!
crypto keyring my-keyring
  pre-shared-key address 2.2.2.6 key Monchichi
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp profile my-isakmp-profile
   keyring my-keyring
   match identity address 2.2.2.6 255.255.255.255
!
crypto ipsec transform-set my-t-set esp-3des esp-md5-hmac
 mode transport
!
crypto ipsec profile my-ipsec-profile
 set security-association lifetime kilobytes 216000
 set security-association lifetime seconds 3600
 set transform-set my-t-set
 set pfs group2
 set isakmp-profile my-isakmp-profile
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface FastEthernet0/1
 description CONN TO INTERNET
 ip address 3.3.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface Tunnel869
 ip address 172.29.29.1 255.255.255.252
 ip tcp adjust-mss 1400
 ip ospf mtu-ignore
 tunnel source 3.3.3.1
 tunnel destination 2.2.2.6
 tunnel protection ipsec profile my-ipsec-profile
!
router bgp 65020
 bgp log-neighbor-changes
 neighbor 172.29.29.2 remote-as 65001
 !
 address-family ipv4
  neighbor 172.29.29.2 activate
  neighbor 172.29.29.2 route-map AS-PREPEND out
  no auto-summary
  no synchronization
  network 4.4.4.4 mask 255.255.255.255
 exit-address-family
!
route-map AS-PREPEND permit 10
 set as-path prepend 65020 65020
!
ip route 2.2.2.6  255.255.255.255  << x.x.x.x >>    <-------- where x.x.x.x is the next hop to the Internet
!
end
```