IPSEC HIGH-AVAILABILITY

Failover strategies

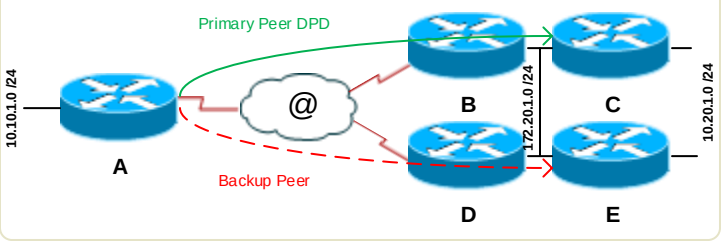
Les meilleurs plans de redondance ne peuvent être mis en place seulement si l'on sait reconnaitre l'état de Failure.

2 modes → **Stateless**- L'état du tunnel IPSec n'est pas connu
Statefull - Utilisation de deux équipements redondants qui communiquent afin de connaitre à chaque instant qui est Actif.

IPSEC Stateless Failover

DPD (Dead Peer Detection)
IGP Within GRE over IPSEC
HSRP (Hot Standby Routing Protocol)

Dead Peer Detection



Router A

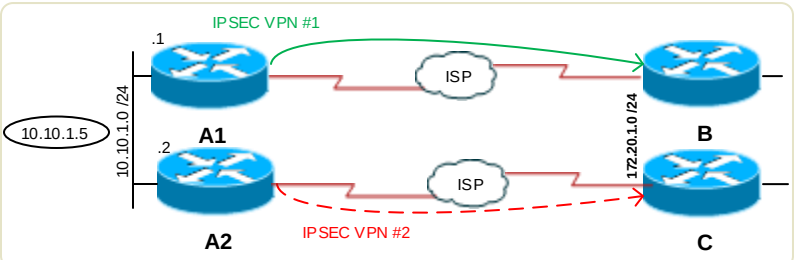
```
crypto isakmp keepalives 10 3
crypto isakmp seconds [retries] [periodic |on-demand]
!
crypto ipsec transform-set to-central esp-3des esp-sha-hmac
access-list 120 permit ip 10.10.1.0 0.0.0.255 10.20.1.0 0.0.0.255
!
crypto map central-office 10 ipsec-isakmp
        set-peer 172.20.1.1 default
        set-peer 172.20.1.2
        set transform-set to-central
        match-address 120
```

IGP Within a GRE over IPSec tunnel

Un VPN IPSEC ne peut pas transporter de protocol de routage. On crée donc un tunnel GRE pour le traffic de routage, et on le fait passer par un tunnel IPSEC pour la confidentialité.

OSPF et EIGRP ont une convergence très rapide, l'usage d'un backup GRE over IPSEC fournis de la redondance, au coût d'un flux important de l'IGP à l'intérieur du tunnel.

HSRP (Hot Standby Routing Protocol)



Router A1

```
int fast 0/1
 ip add 10.10.1.1 255.255.255.0
 standby 1 ip 10.10.1.5
 standby 1 priority 150
 standby 1 preempt
```

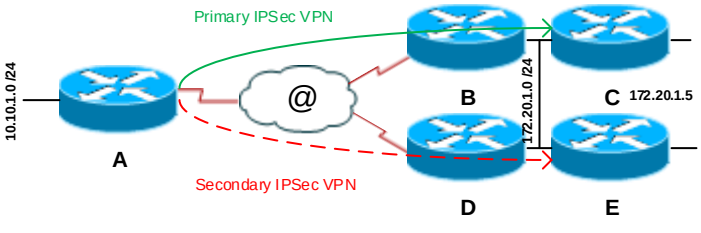
Router A2

```
int fast 0/1
 ip add 10.10.1.2 255.255.255.0
 standby 1 ip 10.10.1.5
```

IPSEC StateFull Failover

HSRP – Monitor les interfaces INSIDE & OUTSIDE
SSO (Statefull SwitchOver) – Partage les infos IKE et SA IPSec entre le routeur actif et passif

Limitations / restrictions: IOS identique, ACTIF & Standby connectés via le LAN.
Load-balancing, Keepalives, L2TP, idle-timers non supportés.



Router C

```
crypto dynamic-map from-remote
        set transform-set trans1
        reverse-route
crypto map central-office 10 ipsec-isakmp dynamic from-remote
Interface f0/1
        ip address 172.20.1.1 255.255.255.0
        standby 1 ip 172.20.1.5
        standby 1 priority 150
        standby 1 preempt
        standby 1 name vpn-remote
        crypto map central-office redundancy vpn-remote stateful
redundancy inter-device scheme standby vpn-remote
ipc zone default
        association 1                          ! Initie la connection
        protocol sctp                          ! Crée une association
        local-port 12321                   =   ! Stream Control Transimtion protocol
        local-ip 10.20.1.1                     Adresses physiques
        retransit-timeout 300 10000
        path-retransmit 10                     ! Nb d'essai avant Fail
        assoc-retransmit 20
            remote-port 12321
        remote-ip 10.20.1.2
```

HSRP

SSO