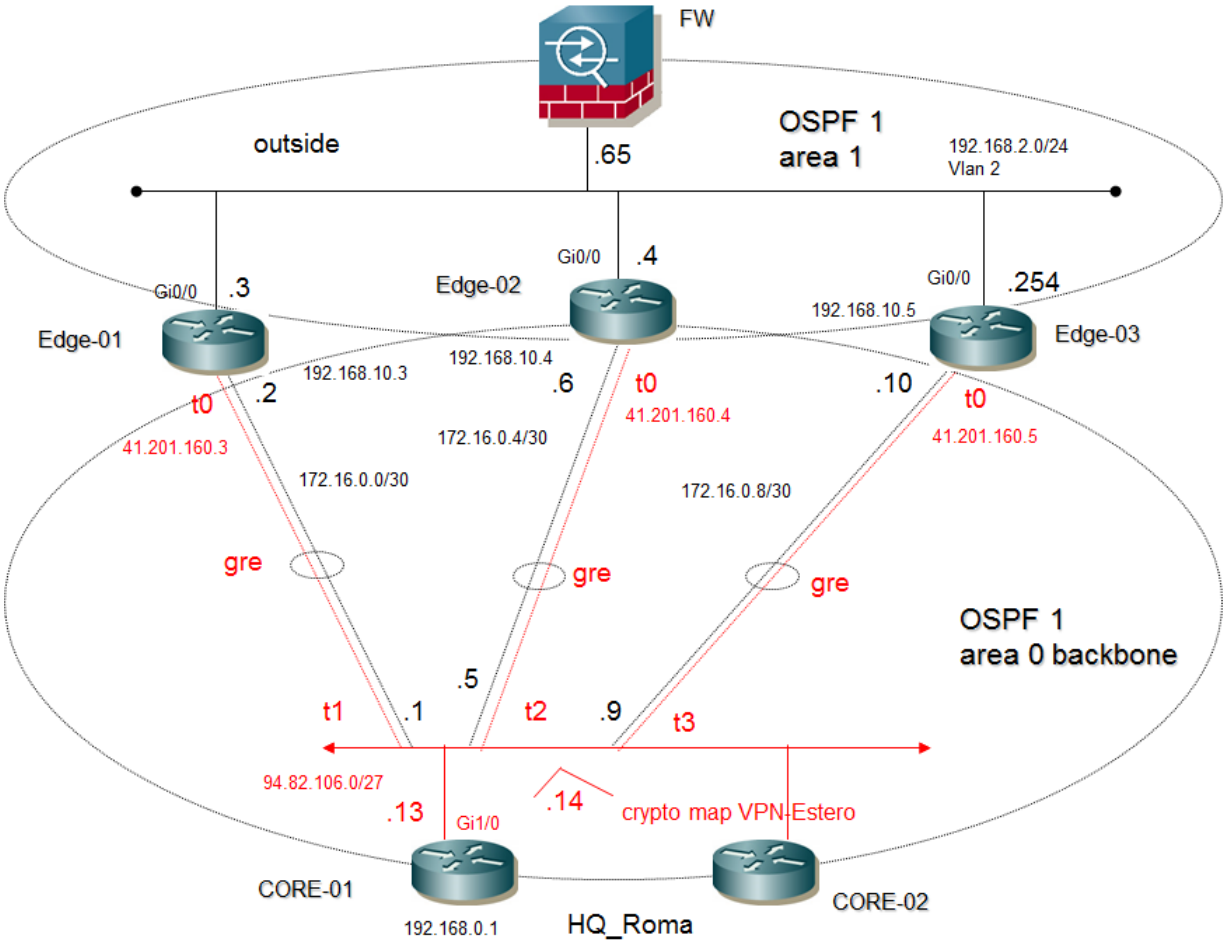
Il presente documento ha come obiettivo quello di fornire le linee guida di configurazione per un nuovo collegamento IPSEC via Satellite tra la sede HQ ed il branch-office Estero.

L'architettura backbone IPSEC internet è distribuita come in figura:



Le principali caratteristiche sono:

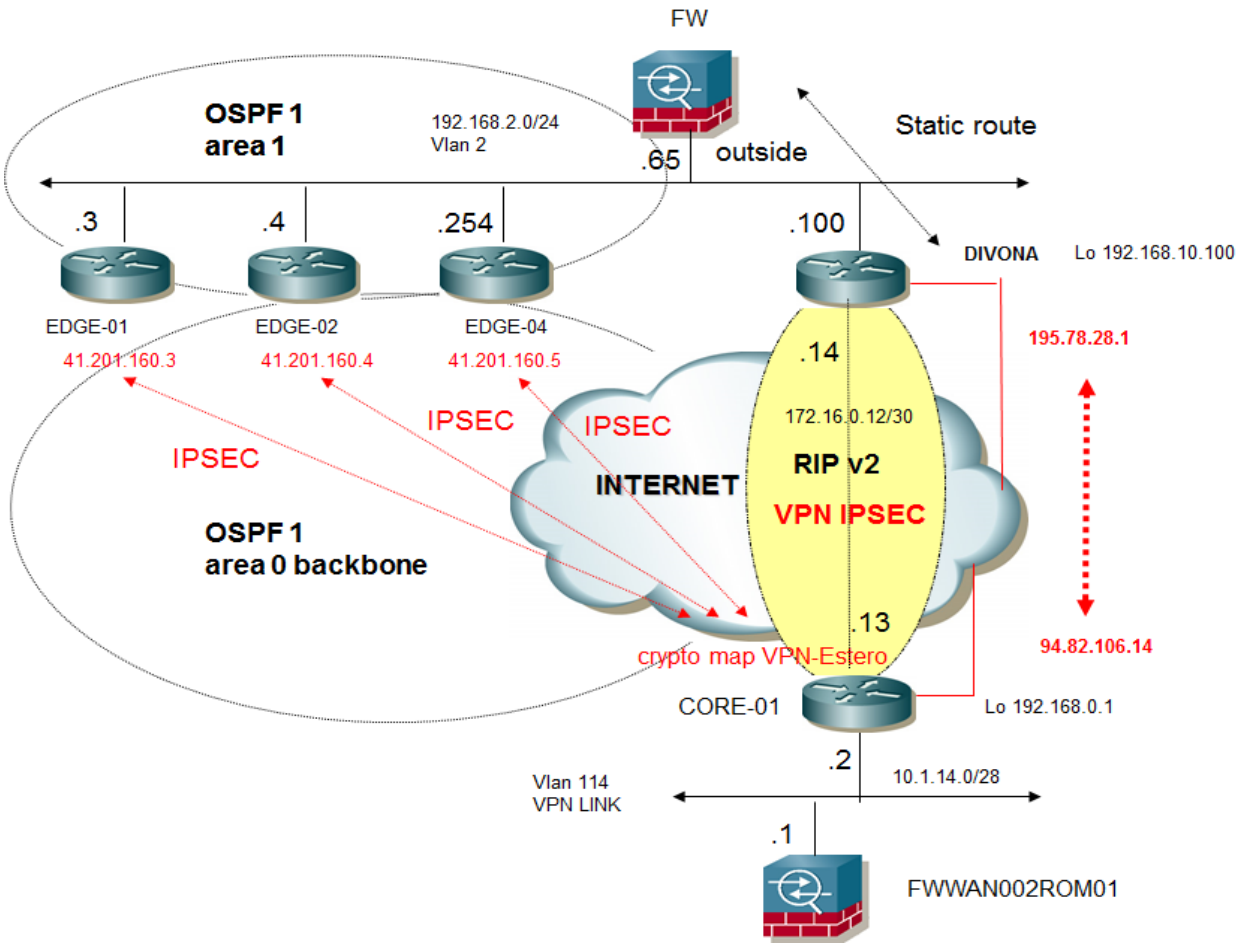
- **IGP**: OSPF area backbone 0.0.0.0 + area firewall 0.0.0.1

- **FW:**
  - n° 3 default route in equal-cost-path verso i n° 3 router HDSL via outside vlan x
  - isakmp-ipsec verso sito Estero via interface outside

- **EDGE-01 – EDGE-02 – EDGE-03:**
  - tunnel mode GRE
  - isakmp-ipsec con peering il router HQ 94.82.106.14 applicata sulla interfaccia Dialer0 (crypto map VPN-HQ)
  - default route statica via dialer0
  - redistribute static subnets route-map Rotte_Estero via OSPF
  - default-information originate via OSPF
  - per interfaccia
    - load-sharing per packet via CEF in modo da gestire il traffico in uscita equal-cost-path
    - abilitazione autenticazione MD5 via key-id e password via OSPF

- **CORE-01 :**
  - router active
  - n° 3 tunnel GRE, uno per ciascun routers
  - isakmp-ipsec (VPN_Estero) con tre policy, una per ciascun peer
  - redistribute static subnets route-map Rotte_HQ via OSPF

Attraverso un nuovo canale via Satellite tra la sede Estero e l'HQ, si vuole creare una VPN IPSEC per traffico IT criptato, rispettando l'attuale architettura di trasporto.



CORE-01	Descrizione
crypto map VPN-Algeria 40 ipsec-isakmp set peer 195.78.28.1 set transform-set VPN-Estero match address Tunnel4 ! interface Tunnel4 description gre-sat **ip address 172.x.x.x 255.255.255.252** tunnel source 94.82.106.14 tunnel destination 195.78.28.1 ip rip send version 2 ip rip receive version 2 no ip split-horizon ! router rip version 2 redistribute static subnets route-map LAN_HQ_SAT **network 10.0.0.0** no auto-summary ! ip access-list extended Tunnel4 permit gre host 94.82.106.14 host 195.78.28.1 ! ip access-list standard LAN_RM_SAT permit a.b.c.0 0.0.0.255 permit a.b.z.0 0.0.0.255 ! route-map LAN_HQ_SAT permit 10 match ip address LAN_HQ_SAT	Definizione di una nuova crypto map con peering l'indirizzo IP pubblico del router DIVONA Specifica quale VPN settare specifica via acl extended una entry per la crypto ! Creazione un un tunnel mode GRE p2p tra il rouer di Roma e quello DIVONA con sorgente e destinazione del tunnel gli IP pubblici internet

Il router DIVONA ha il compito di:

- stabilire adiacenze RIP con il relativo neighbor HQ
- VPN IPSEC Lan to Lan con il router HQ
- Tunnel GRE
- Default Gateway per la rete LAN-ESTERO x.y.z.0/24

DIVONA ROUTER	Descrizione
interface vlan 50 description LAN Estero ip address x.y.z.1 255.255.255.0 ! interface fa0/3 switchport access vlan 50 !	
crypto isakmp policy 1 authentication pre-share group 2	definizione di una policy ISAKMP metodo di autenticazione in iSAKMP policy assegnazione gruppo di security
crypto isakmp key xxxxxxx address 0.0.0.0 0.0.0.0	ISAKMP Key
crypto isakmp invalid-spi-recovery crypto isakmp keepalive 10	dead peer detection (DPD)
i crypto ipsec transform-set VPN-HQ esp-aes esp-sha-hmac	algoritmi di criptazione per la VPN HQ

! crypto map VPN-HQ 10 ipsec-isakmp set peer 94.82.106.14 set transform-set VPN-HQ match address VPN-HQ !	Static crypto map for L2L tunnel
interface Tunnel0 description gre-sat **ip address 172.x.x.x 255.255.255.252** tunnel source 195.78.28.1 tunnel destination 94.82.106.14 !	Tunnel GRE
interface < interface-IN > description INTERNAL ip address r.s.t.0 255.255.255.0	
interface < interface-OUT > description INTERNET ip address w.q.z.a 255.255.255.252 crypto map VPN-HQ !	
router rip version 2 redistribuite static route-map LAN_Estero **network 10.0.0.0** no auto-summary !	
ip access-list extended VPN-HQ permit gre host 195.78.28.1 host 94.82.106.14 !	
ip access-list standard LAN_Estero permit x.y.z.0 0.0.0.255 !	
route-map LAN_Estero permit 10 match ip address LAN_Eastero	