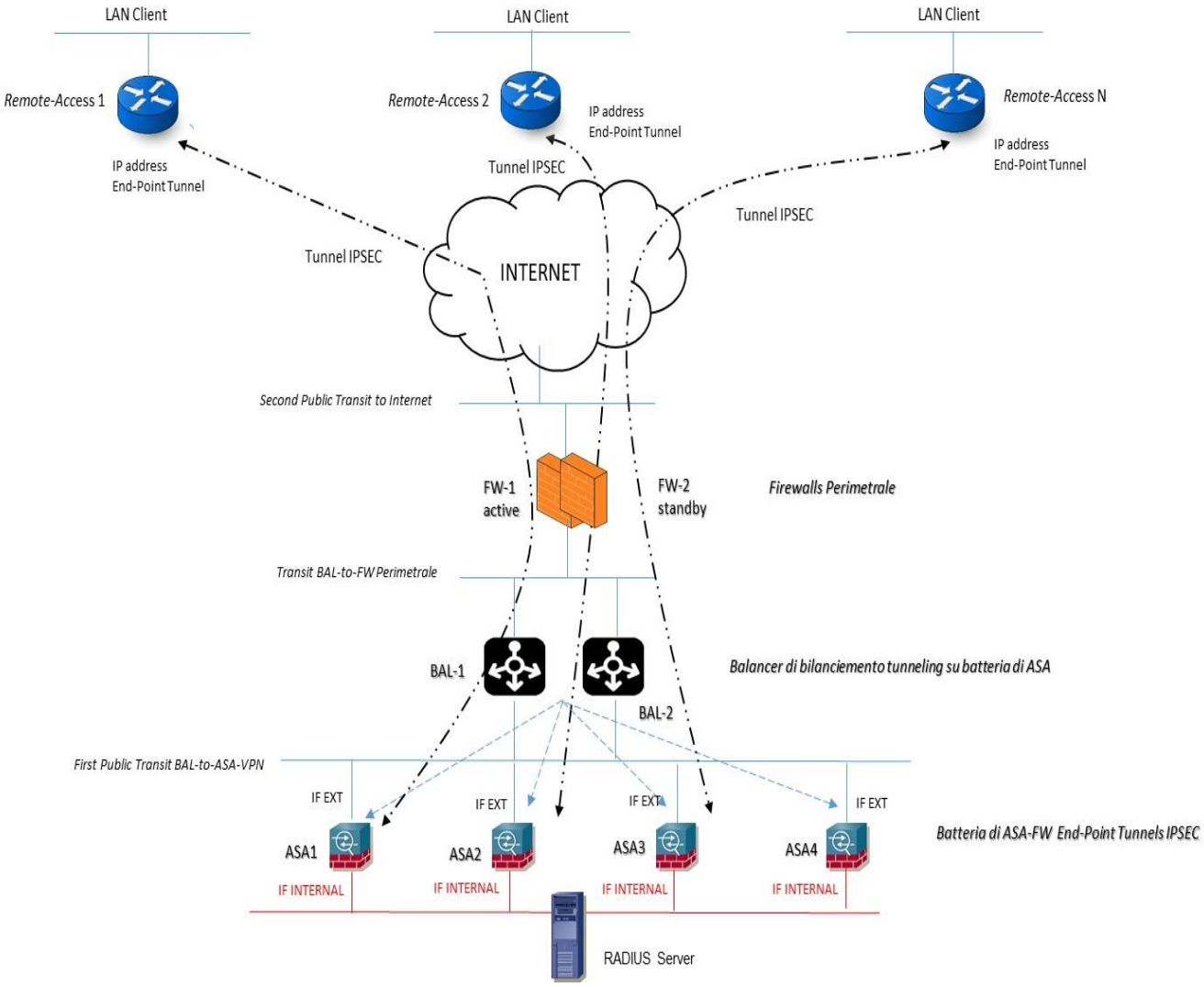
Massimiliano Sbaraglia **Network Engineer**

Esempio di configurazione ASA per Dynamic Tunnels IPSEC in Remote Access

Architettura di esempio:



Steps di configurazione Tunnels IPSEC RA presso un ASA-FW di esempio:

Massimiliano Sbaraglia **Network Engineer**

1) Configurazione interface

interface po1
vlan x
nameif EXTERNAL
ip address < *public ip address* >
!
interface po2
vlan y
nameif INTERNAL
ip address < *private ip address* >

2) Configurazione Access-List VPN

access-list ACL-VPN extended permit ip < LAN-Client > any
access-list ALC-VPN extended permit tcp < LAN-Client > any
access-list ACL-VPN extended permit udp < LAN-Client > any
access-list ACL-VPN extended permit icmp < LAN-Client > any
access-list ACLVPN remark Subnets permitted in tunnel
!
access-list ACL-Local-Access standard permit host < *ip address host 1* >
access-list ACL-Local-Access standard permit host < ip address host 2 >
access-list ACL-Local-Access remark Subnets not routed in vpn tunnel
!

3) Configurazione routing

route EXTERNAL 0.0.0.0 0.0.0.0 < *ip address next-hop public* >
route INTERNAL < *ip address LAN-INTERNAL-A* > < *mask* > < *ip address next-hop internal* >
route INTERNAL < *ip address LAN-INTERNAL-B*> < *mask* > < *ip address next-hop internal* >

!
route INTERNAL-2 0.0.0.0 0.0.0.0 < *ip address next-hop internal* > tunneled *(nella architettura non compare questa vlan internal-2 interface)*

in caso si abbia bisogni di una seconda default-route che consente al traffico VPN tunneled di essere trasmesso ad una diversa destinazione/diverso devices

4) Configurazione AAA authentication Radius Server

```
aaa-server RADIUS protocol radius
 reactivation-mode timed
aaa-server RADIUS (IF-MGMT-Radius) host < ip address server-radius >
 key < key >
 authentication-port 1812
 accounting-port 1813
!
aaa authentication  serial console LOCAL
aaa authentication ssh console LOCAL
aaa authorization command LOCAL
aaa authorization exec authentication-server
```

5) Configurazione IPSEC IKEv1 and IKEv2 Proposal and Policy (esempi)

```
crypto ipsec ikev1 transform-set  ESP-AES-256-SHA  esp-aes-256  esp-sha-hmac
crypto ipsec ikev1 transform-set  ESP-AES-256-MD5  esp-aes-256  esp-md5-hmac
crypto ipsec ikev1 transform-set  3DES-SHA  esp-3des  esp-sha-hmac
!
crypto ipsec ikev2 ipsec-proposal AES256
  protocol esp encryption aes-256
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
  protocol esp encryption aes-192
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
  protocol esp encryption aes
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal3DES
  protocol esp encryption 3des
  protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposalDES
  protocol esp encryption des
  protocol esp integrity sha-1 md5
!
crypto ipsec security-association pmtu-aging infinite
!
crypto ikev1 enable EXTERNAL
crypto ikev1 ipsec-over-tcp port 10000
!
crypto ikev1 policy 10
 authentication pre-share
  encryption aes-256
  hash sha
  group 2
 lifetime 86400
```

```
crypto ikev1 policy 20
 authentication pre-share
 encryption aes-256
 hash md5
 group 2
 lifetime 86400

!


crypto ikev2 enable EXTERNAL

crypto ikev2 policy 10
 encryption aes-256
 integrity sha
 group < numbers groups >
 pfr sha
 lifetime seconds 86400

crypto ikev2 policy 20
 encryption aes
 integrity sha
 group < numbers groups >
 pfr sha
 lifetime seconds 86400


crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group < numbers groups >
 pfr sha
 lifetime seconds 86400


crypto ikev2 policy 40
 encryption des
 integrity sha
 group < numbers groups >
 pfr sha
 lifetime seconds 86400
```

6) Configurazione IPSEC DYNAMIC MAP

```
crypto dynamic-map DYN-MAP 65535 set ikev1 transform-set ESP-AES-256-SHA  ESP-AES-256-MD5
crypto dynamic-map DYN-MAP 65535 set ikev2 ipsec-proposal AES256  AES192  AES  3DES  DES
crypto dynamic-map DYN-MAP 65535 set security-association lifetime seconds < seconds >
crypto dynamic-map DYN-MAP 65535 set security-association lifetime kilobytes  < kilobytes >
!
crypto map VPN-MAP 65535 ipsec-isakmp dynamic DYN-MAP
crypto map VPM-MAP interface EXTERNAL
```

7) Configurazione GROUP-POLICY

```
group-policy GROUP-POLICY internal
group-policy GROUP-POLICY attributes
  vpn-simultaneous-logins < number >
  vpn-filter value ACL-VPN
  vpn-tunnel-protocol ikev1 (or ikev2) (or ikev1 ikev2)
  group-lock value TUNNEL-GROUP
  ipsec-udp enable
  split-tunnel-policy excludespecified
  split-tunnel-network-list value ACL-Local-Access
```

8) Configurazione TUNNEL-GROUP

```
tunnel-group TUNNEL-GROUP type remote-access
tunnel-group TUNNEL-GROUP general-attributes
  authentication-server-group RADIUS
  default-group-policy GROUP-POLICY
!
tunnel-group TUNNEL-GROUP ipsec-attributes
 ikev1 pre-shared key < key >
 isakmp keepalive threshold 30 retry 10
```