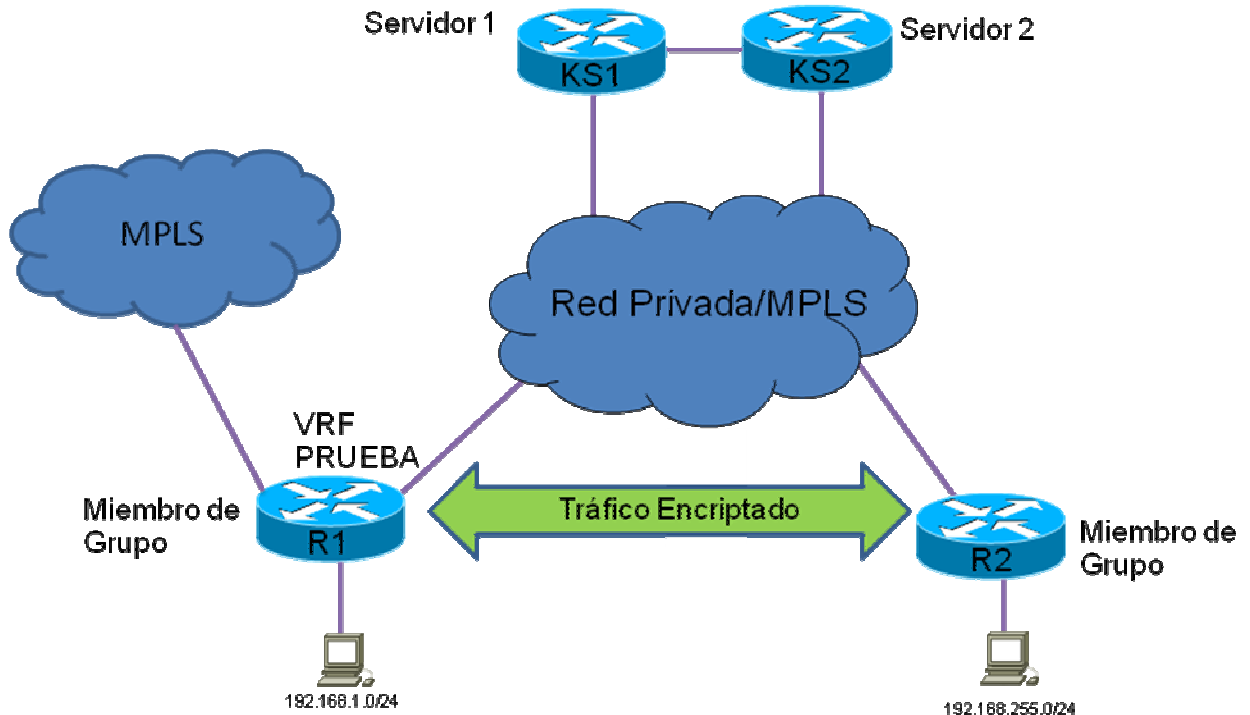


GETVPN SOBRE VRF

Introducción. GETVPN es una tecnología que no requiere la negociación de túneles punto a punto y es implementado principalmente en redes privadas o MPLS. Dadas las características en las que esta tecnología funciona, no es posible habilitar MPLS en la misma interfaz donde el mapa de encriptación está aplicado. Es posible, sin embargo, aplicar el mapa en una interfaz habilitada con una VRF.

Topología.



Modo de Operación.

El siguiente enlace muestra a detalle el modelo de configuración de GETVPN en un equipo que tiene aplicada una VRF en la interfaz de salida del router:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/deployment_guide_c07-624088.html

En el documento anterior, se utiliza una configuración de GETVPN que autentica a los miembros del grupo GDOI a través de certificados digitales. Bajo este esquema, no se requiere de ningún tipo de configuración especial, GETVPN funciona de manera transparente sobre la tabla de ruteo virtual generada por la VRF. Sin embargo, este esquema cambia cuando el método de autenticación para el túnel de VPN se modifica para utilizar llaves compartidas (pre-shared keys).

Como se puede observar en la figura anterior, le interfaz que conecta al equipo R1 a la red MPLS sobre la que se tiene una red GETVPN tiene aplicada la VRF PRUEBA. La conexión hacia los dos servidores KS1 y KS2 se autentica a través de una llave compartida:

```
crypto isakmp policy 10
authentication pre-share
encr aes 256
group 2
lifetime 86400

crypto isakmp key 57T3lm3xM9Y9eyTq7Yo8Z83K90F4 address 10.161.77.178
crypto isakmp key 57T3lm3xM9Y9eyTq7Yo8Z83K90F4 address 10.161.77.58

crypto ipsec transform-set MYSET esp-aes 256 esp-sha-hmac

crypto ipsec profile GETVPN
set security-association lifetime seconds 28800
set transform-set MYSET

crypto gdoi group GETVPN
identity number 72
server address ipv4 10.161.77.58
server address ipv4 10.161.77.178

crypto map MYMAP 1 gdoi
set group GETVPN

interface GigabitEthernet0/0
ip vrf forwarding PRUEBA
ip address 10.255.255.100 255.255.255.0
duplex auto
speed auto
crypto map MYMAP
```

Si se corre un “debug crypto isakmp” para observar la negociación de fase 1 del equipo con la configuración de arriba observaríamos que el túnel no puede establecer una conexión de fase 1 exitosa debido a los siguientes errores:

```
debug crypto isakmp
*Mar 10 23:33:10.587: ISAKMP:(0): SA request profile is (NULL)
*Mar 10 23:33:10.587: ISAKMP: Created a peer struct for 10.161.77.58, peer
port 848
*Mar 10 23:33:10.587: ISAKMP: New peer created peer = 0x5371AD0 peer_handle =
0x80000007
*Mar 10 23:33:10.587: ISAKMP: Locking peer struct 0x5371AD0, refcount 1 for
isakmp_initiator
*Mar 10 23:33:10.587: ISAKMP: local port 848, remote port 848
*Mar 10 23:33:10.587: ISAKMP: set new node 0 to QM_IDLE
*Mar 10 23:33:10.587: ISAKMP:(0):insert sa successfully sa = 4BB2330
*Mar 10 23:33:10.587: ISAKMP:(0):Can not start Aggressive mode, trying Main
mode.
*Mar 10 23:33:10.587: ISAKMP:(0):No pre-shared key with 10.161.77.58!
*Mar 10 23:33:10.587: ISAKMP:(0): No Cert or pre-shared address key.
```

La causa de la falla es que a pesar de que las llaves compartidas están configuradas en el equipo, R1 está asumiendo que las direcciones IP de los servidores KS1 y KS2 se alcanzan a través de la tabla de ruteo global, en lugar de la tabla que pertenece a la VRF PRUEBA. Es por esto que al intentar negociar la fase 1 de GETVPN no tenemos llave de autenticación para la interfaz donde está aplicado el mapa. Hay que realizar los siguientes cambios para que la conexión sea exitosa:

```
R1#config t
R1(config)#no crypto isakmp key 57T3lm3xM9Y9eyTq7Yo8Z83K90F4 address 10.161.77.178
R1(config)#no crypto isakmp key 57T3lm3xM9Y9eyTq7Yo8Z83K90F4 address 10.161.77.58
R1(config)#crypto keyring GETVPN vrf PRUEBA
R1(conf-keyring)#pre-shared-key address 10.161.77.58 key
57T3lm3xM9Y9eyTq7Yo8Z83K90F4
R1(conf-keyring)#pre-shared-key address 10.161.77.178 key
57T3lm3xM9Y9eyTq7Yo8Z83K90F4
```

R1 ahora sabe que los servidores deben ser alcanzados sobre la VRF PRUEBA con las llaves compartidas configuradas. Sólo hay que re-iniciar la negociación con el comando “clear crypto gdoi group GETVPN”, o bien remover y reconfigurar el mapa MYMAP de la interfaz. Una vez realizado esto la negociación es exitosa:

```
*Mar 10 23:39:47.483: ISAKMP:(0): SA request profile is (NULL)
*Mar 10 23:39:47.483: ISAKMP: Created a peer struct for 10.161.77.58, peer
port 848
*Mar 10 23:39:47.483: ISAKMP: New peer created peer = 0x476AF40 peer_handle =
0x8000000C
*Mar 10 23:39:47.483: ISAKMP: Locking peer struct 0x476AF40, refcount 1 for
isakmp_initiator
*Mar 10 23:39:47.483: ISAKMP: local port 848, remote port 848
*Mar 10 23:39:47.483: ISAKMP: set new node 0 to QM_IDLE
*Mar 10 23:39:47.483: ISAKMP:(0):insert sa successfully sa = 4FCDE00
*Mar 10 23:39:47.483: ISAKMP:(0):Can not start Aggressive mode, trying Main
mode.
*Mar 10 23:39:47.483: ISAKMP:(0):found peer pre-shared key matching
10.161.77.58
*Mar 10 23:39:47.483: ISAKMP:(0): constructed NAT-T vendor-rfc3947 ID
*Mar 10 23:39:47.483: ISAKMP:(0): constructed NAT-T vendor-07 ID
*Mar 10 23:39:47.483: ISAKMP:(0): constructed NAT-T vendor-03 ID
*Mar 10 23:39:47.483: ISAKMP:(0): constructed NAT-T vendor-02 ID
*Mar 10 23:39:47.483: ISAKMP:(0):Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_MM
*Mar 10 23:39:47.483: ISAKMP:(0):Old State = IKE_READY New State = IKE_I_MM1

*Mar 10 23:39:47.483: ISAKMP:(0): beginning Main Mode exchange
*Mar 10 23:39:47.483: ISAKMP:(0): sending packet to 10.161.77.58 my_port 848
peer_port 848
(I) MM_NO_STATE
*Mar 10 23:39:47.483: ISAKMP:(0):Sending an IKE IPv4 Packet.
*Mar 10 23:39:47.487: ISAKMP (0): received packet from 10.161.77.58 dport 848
sport 848
falabella-intra (I) MM_NO_STATE
*Mar 10 23:39:47.487: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
*Mar 10 23:39:47.487: ISAKMP:(0):Old State = IKE_I_MM1 New State = IKE_I_MM2

*Mar 10 23:39:47.487: ISAKMP:(0): processing SA payload. message ID = 0
*Mar 10 23:39:47.487: ISAKMP:(0): processing vendor id payload
*Mar 10 23:39:47.487: ISAKMP:(0): vendor ID seems Unity/DPD but major 69
mismatch
*Mar 10 23:39:47.487: ISAKMP (0): vendor ID is NAT-T RFC 3947
*Mar 10 23:39:47.487: ISAKMP:(0):found peer pre-shared key matching
10.161.77.58
*Mar 10 23:39:47.487: ISAKMP:(0): local preshared key found
```