Anexo B
GUÍA LABORATORIO GET VPN NOC CORPORATIVO

El anexo adjunto, presenta el desarrollo de configuraciones para llevar a cabo el laboratorio GET VPN, procedimiento, comandos, y pruebas de verificación. Contiene toda la información que sustenta toda la simulación del proyecto.

GUÍA LABORATORIO GET VPN
NOC CORPORATIVO

GERENCIA DE GESTION DE RED

DICIEMBRE DE 2014

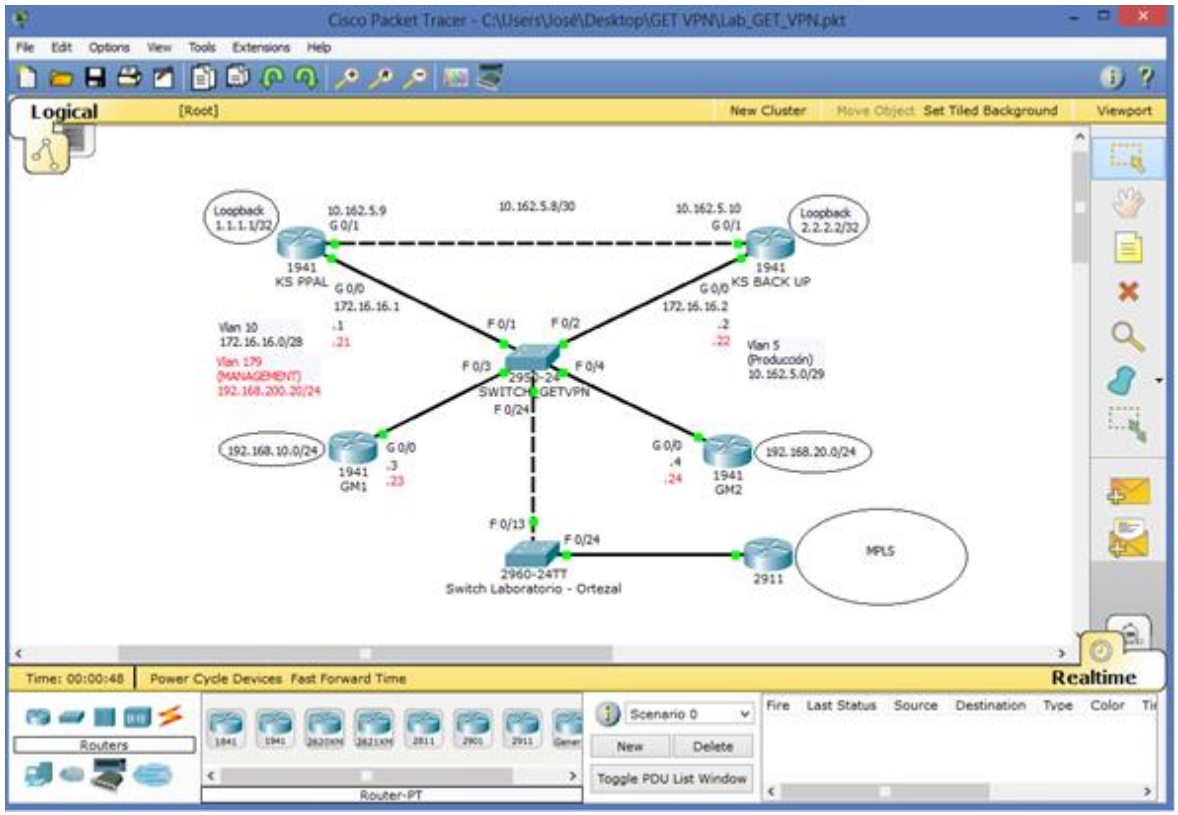
BOGOTÁ

CONTROL DE MODIFICACIONES

Fecha de Cambio	Versión	Cambiado Por:	Secciones Cambiadas	Motivo del Cambio
2014-12-29	1	José Sánchez	Todas	Primera versión del Documento.

Contenido

1. Topología y Direccionamiento del Laboratorio



2. Acceso y Gestión Remota de los Equipos

Al realizar la conexión y configuración de la topología final GET VPN, los equipos fueron debidamente instalados en el rack del laboratorio NOC Corporativo – Ortezal. *Figura 1.* La idea de su instalación allí, es que todos los ingenieros del NOC, puedan acceder a ellos desde sus puestos de trabajo mediante la herramienta putty, la cual emplean a diario para realizar configuraciónes.

Figura 1. Rack Laboratorio Ortezal

Al tener acceso a los equipos desde su puesto de trabajo, podrán practicar las configuraciones de los elementos principales que componen el tema GET VPN *Figura 2*, reforzar sus conocimientos, e incluso podrán simular un caso que se les esté presentando con algún cliente.

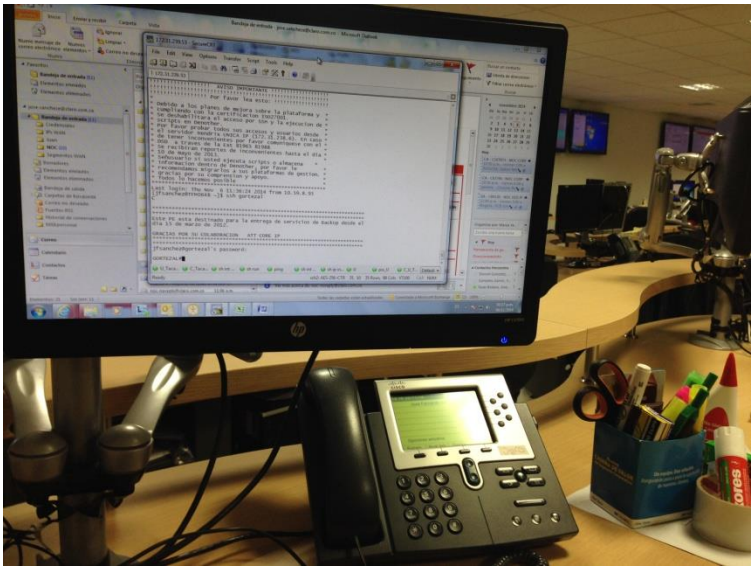


Figura 2. Puesto de Trabajo Ingeniero NOC Corporativo

Las pruebas que se muestran a continuación, son tomadas desde el putty de uno de los puestos de trabajo, donde se ingresa al SW de Ortezal (SW2960), y se prueba conectividad desde allí a los router que componen la topología final GET VPN.

2.1 Gestión de los equipos (proyecto GET VPN) desde el puesto de trabajo.

Para ingresar a los equipos (Proyecto GET VPN) desde el puesto de trabajo de cada uno de los ingenieros, una de las formas es la que se describe a continuación.

RESERVADO: Esta parte del documento contiene secretos del negocio e información de propiedad de **Claro Colombia Soluciones Fijas**

3. Configuración GET VPN – Pre shared Keys

3.1 Configuración del Key Server Principal

3.1.1 Configurar una política IKE sobre el router Key Server Principal:

```
KSPPAL#conf
KSPPAL#configure t
KSPPAL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
KSPPAL(config)#cry
KSPPAL(config)#crypto isa
KSPPAL(config)#crypto isakmp policy 20
KSPPAL(config-isakmp)#authe
KSPPAL(config-isakmp)#authentication ?
  pre-share  Pre-Shared Key
  rsa-encr   Rivest-Shamir-Adleman Encryption
  rsa-sig    Rivest-Shamir-Adleman Signature

KSPPAL(config-isakmp)#authentication pre-sh
KSPPAL(config-isakmp)#authentication pre-share
KSPPAL(config-isakmp)#group?
group

KSPPAL(config-isakmp)#group ?
  1   Diffie-Hellman group 1 (768 bit)
  14  Diffie-Hellman group 14 (2048 bit)
  15  Diffie-Hellman group 15 (3072 bit)
  16  Diffie-Hellman group 16 (4096 bit)
  19  Diffie-Hellman group 19 (256 bit ecp)
  2   Diffie-Hellman group 2 (1024 bit)
  20  Diffie-Hellman group 20 (384 bit ecp)
  21  Diffie-Hellman group 21 (521 bit ecp)
  24  Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)
  5   Diffie-Hellman group 5 (1536 bit)

KSPPAL(config-isakmp)#group 5
KSPPAL(config-isakmp)#exit

KSPPAL#show crypto isakmp policy

Global IKE policy
Protection suite of priority 20
        encryption algorithm:   DES - Data Encryption Standard (56 bit
keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
                lifetime:               86400 seconds, no volume limit
```

3.1.2 Generar y configurar credenciales de autenticación. Se usara autenticación PSK para que pormedio de las credenciales generadas se autentiquen los miembros.

```
KSPPAL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSPPAL(config)#cry
KSPPAL(config)#crypto isa
KSPPAL(config)#crypto isakmp KSPPAL(config)#crypto isakmp key cisco123
address 10.162.5.3
KSPPAL(config)#
```

3.1.3 Generar llaves RSA para autenticación rekey:

```
KSPPAL(config)#crypto key generate rsa modulus 2048 label key_rekey
exportable
The name for the keys will be: key_rekey

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 11 seconds)
```

3.1.4 Política de protección de tráfico sobre el Key Server Principal.

```
KSPPAL(config)#crypto ipsec tra
KSPPAL(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
KSPPAL(cfg-crypto-trans)#exit

KSPPAL(config)#cry
KSPPAL(config)#crypto ip
KSPPAL(config)#crypto ipsec profi
KSPPAL(config)#crypto ipsec profile MYIPSECPROFILE
KSPPAL(ipsec-profile)#set tran
KSPPAL(ipsec-profile)#set transform-set MYSET
KSPPAL(ipsec-profile)#exit
KSPPAL(config)#
```

Se crea una lista de acceso para los miembros GET VPN.

```
KSPPAL(config)#
KSPPAL(config)#ip acc
KSPPAL(config)#ip acces
KSPPAL(config)#ip access-list exte
KSPPAL(config)#ip access-list extended REDES-A-CIFRAR
KSPPAL(config-ext-nacl)#
KSPPAL(config-ext-nacl)#deny   esp any any
KSPPAL(config-ext-nacl)#deny   tcp any any eq tacacs
KSPPAL(config-ext-nacl)#deny   tcp any eq tacacs any
KSPPAL(config-ext-nacl)#deny   tcp any any eq 22
KSPPAL(config-ext-nacl)#deny   tcp any eq 22 any
KSPPAL(config-ext-nacl)#deny   tcp any any eq bgp
KSPPAL(config-ext-nacl)#deny   tcp any eq bgp any
KSPPAL(config-ext-nacl)#deny   ospf any any
KSPPAL(config-ext-nacl)#deny   eigrp any any
KSPPAL(config-ext-nacl)#deny   pim any 224.0.0.0 0.0.0.255
KSPPAL(config-ext-nacl)#deny   udp any any eq ntp
KSPPAL(config-ext-nacl)#deny   udp any any eq 1645
KSPPAL(config-ext-nacl)#deny   udp any any eq 1646
KSPPAL(config-ext-nacl)#deny   udp any any eq 1812
KSPPAL(config-ext-nacl)#deny   udp any any eq 1813
KSPPAL(config-ext-nacl)#deny   tcp any eq 443 any
KSPPAL(config-ext-nacl)#deny   tcp any any eq 443
KSPPAL(config-ext-nacl)#deny   udp any eq isakmp any eq isakmp
KSPPAL(config-ext-nacl)#deny   udp any any eq 848
KSPPAL(config-ext-nacl)#deny   ip host 10.162.5.1 any
KSPPAL(config-ext-nacl)#deny   ip any host 10.162.5.1
KSPPAL(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0
0.0.0.255
KSPPAL(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 192.168.10.0
0.0.0.255
KSPPAL(config-ext-nacl)#exit
KSPPAL(config)#
```

3.1.5 Habilitar la función GET VPN en Key Server principal

```
KSPPAL(config)#cry
KSPPAL(config)#crypto gd
KSPPAL(config)#crypto gdoi gro
KSPPAL(config)#crypto gdoi group MYGETVPNGROUP
KSPPAL(config-gdoi-group)#ident
KSPPAL(config-gdoi-group)#identity num
KSPPAL(config-gdoi-group)#identity number 7
KSPPAL(config-gdoi-group)#server local
KSPPAL(gdoi-local-server)#add
KSPPAL(gdoi-local-server)#address ipv4 1.1.1.1
```

Politica de protección de tráfico IPsec (SA)

```
KSPPAL(gdoi-local-server)#sa ipsec 10
KSPPAL(gdoi-sa-ipsec)#prof
KSPPAL(gdoi-sa-ipsec)#profile MYIPSECPROFILE
KSPPAL(gdoi-sa-ipsec)#mat
KSPPAL(gdoi-sa-ipsec)#match add
KSPPAL(gdoi-sa-ipsec)#match address ip
KSPPAL(gdoi-sa-ipsec)#match address ipv4 REDES-A-CIFRAR
          KSPPAL(gdoi-sa-ipsec)#
```

3.1.6 Ajustar política de Rekey

```
KSPPAL(gdoi-local-server)#
KSPPAL(gdoi-local-server)#rek
KSPPAL(gdoi-local-server)#rekey trans
KSPPAL(gdoi-local-server)#rekey transport uni
          KSPPAL(gdoi-local-server)#rekey transport unicast
```

3.1.7 Referenciar llaves RSA

```
KSPPAL(gdoi-local-server)#rek
KSPPAL(gdoi-local-server)#rekey aut
KSPPAL(gdoi-local-server)#rekey authentication mypubk
KSPPAL(gdoi-local-server)#rekey authentication mypubkey rsa key_rekey
KSPPAL(gdoi-local-server)#
KSPPAL(gdoi-local-server)#exit
KSPPAL(config-gdoi-group)#exit
KSPPAL(config)#exit
KSPPAL#
```

3.2 Verificación de la configuración del Key Server Principal

3.2.1 Verificar los ajustes básicos del Key Server Principal

```
KSPPAL#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPNGROUP (Unicast)
    Group Identity           : 7
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Group Members            : 0
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 86400 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2

      IPSec SA Number        : 10
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : MYIPSECPROFILE
      Replay method          : Count Based
      Replay Window Size     : 64
      ACL Configured         : access-list REDES-A-CIFRAR
      Group Server list       : Local
```

3.2.2 Verificar política del rekey

```
KSPPAL#show crypto gdoi ks rekey
Group MYGETVPNGROUP (Unicast)
    Number of Rekeys sent                : 0
    Number of Rekeys retransmitted       : 0
    KEK rekey lifetime (sec)             : 86400
    Retransmit period                    : 10
    Number of retransmissions            : 2
    IPSec SA 10 lifetime (sec)           : 3600
```

3.2.3 Miembros registrados

```
KSPPAL#show crypto gdoi ks members

Group Member Information :

No Group Members found for this group : MYGETVPNGROUP

KSPPAL#
```

3.3 Configuración del Group Member UNO GET VPN

3.3.1 Configurar política IKE

```
GM1#
GM1#sh ip int br
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively
down down
GigabitEthernet0/0         unassigned      YES NVRAM  up
up
GigabitEthernet0/0.5       10.162.5.3      YES NVRAM  up
up
GigabitEthernet0/0.179     192.168.200.23  YES NVRAM  up
up
GigabitEthernet0/1         unassigned      YES NVRAM  administratively
down down
Serial0/0/0                unassigned      YES NVRAM  administratively
down down
Loopback30                 192.168.10.1    YES NVRAM  up
up
GM1#
GM1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GM1(config)#cry
GM1(config)#crypto isa
GM1(config)#crypto isakmp policy 20
GM1(config-isakmp)#au
GM1(config-isakmp)#authentication pre-sh
GM1(config-isakmp)#authentication pre-share
GM1(config-isakmp)#grop
```

```
GM1(config-isakmp)#grou
GM1(config-isakmp)#group 5
GM1(config-isakmp)#lif
GM1(config-isakmp)#lifetime 300
GM1(config-isakmp)#exit
```

3.3.2 Configurar credenciales de autenticación

```
GM1(config)#crypto isakmp key cisco123 address 1.1.1.1
GM1(config)#
```

3.3.3 Habilitar función de GET VPN en Group Member Uno

```
GM1(config)#crypto gdoi group MYGETVPNGROUP
GM1(config-gdoi-group)#ide
GM1(config-gdoi-group)#identity num
GM1(config-gdoi-group)#identity number 7
GM1(config-gdoi-group)#server address ipv4 1.1.1.1
GM1(config-gdoi-group)#exit
GM1(config)#
```

3.3.4 Crear y aplicar crypto map GET VPN

```
GM1(config)#crypto map MYCRYPTOMAP 10 gd
GM1(config)#crypto map MYCRYPTOMAP 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
        group has been configured.
GM1(config-crypto-map)#set group MYGETVPNGROUP
GM1(config-crypto-map)#exit

GM1(config)#int gi
GM1(config)#int GigabitEthernet0/0.5
GM1(config-if)#cry
GM1(config-if)#crypto map MYCRYPTOMAP
GM1(config-if)#exit
GM1#
```

3.3.5 Verificar el registro del Group Member Uno

Se Muestra el estado del registro del miembro con el Key Server Principal

```
GM1#
GM1#
GM1#sh cry
GM1#sh crypto gd
GM1#sh crypto gdoi

    Group Name               : MYGETVPNGROUP
    Group Identity           : 7
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both
    Active Group Server      : 1.1.1.1
    Group Server list        : 1.1.1.1

    GM Reregisters in        : 3205 secs
    Rekey Received           : never

    Rekeys received
         Cumulative          : 0
         After registration  : 0


 ACL Downloaded From KS 1.1.1.1:
   access-list   deny esp any any
   access-list   deny tcp any any port = 49
   access-list   deny tcp any port = 49 any
   access-list   deny tcp any any port = 22
   access-list   deny tcp any port = 22 any
   access-list   deny tcp any any port = 179
   access-list   deny tcp any port = 179 any
   access-list   deny ospf any any
   access-list   deny eigrp any any
   access-list   deny pim any 224.0.0.0 0.0.0.255
   access-list   deny udp any any port = 123
   access-list   deny udp any any port = 1645
   access-list   deny udp any any port = 1646
   access-list   deny udp any any port = 1812
   access-list   deny udp any any port = 1813
   access-list   deny tcp any port = 443 any
   access-list   deny tcp any any port = 443
   access-list   deny udp any port = 500 any port = 500
   access-list   deny udp any any port = 848
   access-list   deny ip host 10.162.5.1 any
   access-list   deny ip any host 10.162.5.1
   access-list   permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
   access-list   permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
       ....
```

```
GM1#sh cry
GM1#sh crypto isa
GM1#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.162.5.3      1.1.1.1      GDOI_IDLE         1004   0   ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
GM1#
GM1#sh crypto isakmp sa de
GM1#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH
Lifetime Cap.

1004  10.162.5.3      1.1.1.1             ACTIVE des sha    psk  5
00:03:04
       Engine-id:Conn-id =  SW:4

    IPv6 Crypto ISAKMP SA
```

Se debe validar en el Key Server Principal que ya aparezca registrado el Group Member Uno

```
KSPPAL#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group MYGETVPNGROUP : 0

Group Member ID     : 10.162.5.3
 Group ID           : 7
 Group Name         : MYGETVPNGROUP
 Key Server ID      : 1.1.1.1
Rekeys sent       : 0
Rekeys retries    : 0
Rekey Acks Rcvd   : 0
Rekey Acks missed : 0

Sent seq num :    0    0    0    0
Rcvd seq num :    0    0    0    0
```

3.4 Configuración del Group Member DOS GET VPN

3.4.1 Configuración Group Member Dos

En el router Key Server Principal debe configurarse primero lo siguiente.

```
KSPPAL(config)#crypto isakmp key cisco123 address 10.162.5.4
```

Seguidamnete:

```
GM2#
GM2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM2(config)#
GM2(config)#
GM2(config)#
GM2(config)#crypto isakmp policy 20
GM2(config-isakmp)#authentication pre-share
GM2(config-isakmp)#gro
GM2(config-isakmp)#group 5
GM2(config-isakmp)#life
GM2(config-isakmp)#lifetime 300
GM2(config-isakmp)#exit
GM2(config)#crypto isakmp key cisco123 address 1.1.1.1
GM2(config)#
GM2(config)#
GM2(config)#crypto gdoi group MYGETVPNGROUP
GM2(config-gdoi-group)#iden
GM2(config-gdoi-group)#identity num
GM2(config-gdoi-group)#identity number 7
GM2(config-gdoi-group)#server address ipv4 1.1.1.1
GM2(config-gdoi-group)#exit
GM2(config)#
GM2(config)#
GM2(config)#
GM2(config)#crypto map MYCRYPTOMAP 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
        group has been configured.
GM2(config-crypto-map)#set group MYGETVPNGROUP
GM2(config-crypto-map)#exit
GM2(config)#int
GM2(config)#interface
GM2#
GM2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
GM2(config)#
GM2(config)#int
GM2(config)#interface g
GM2(config)#interface gigabitEthernet 0/0.5
GM2(config-subif)#crypto map MYCRYPTOMAP
GM2(config-subif)#exit
GM2(config)#
GM2(config)#
GM2(config)#exit
GM2#
GM2#
GM2#wr
Building configuration...
[OK]
GM2#
```

3.4.2 Verificar registro de Group Member Dos

```
GM2#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPNGROUP
    Group Identity           : 7
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 1.1.1.1

    Group member             : 10.162.5.4       vrf: None
       Version               : 1.0.4
       Registration status   : Registered
       Registered with       : 1.1.1.1
       Re-registers in       : 2070 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 25
       Unicast rekey received: 0
       Rekey ACKs sent       : 0
       Rekey Received        : never
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Acks sents      : 0

ACL Downloaded From KS 1.1.1.1:
  access-list   deny esp any any
```

```
   access-list   deny tcp any any port = 49
   access-list   deny tcp any port = 49 any
   access-list   deny tcp any any port = 22
   access-list   deny tcp any port = 22 any
   access-list   deny tcp any any port = 179
   access-list   deny tcp any port = 179 any
   access-list   deny ospf any any
   access-list   deny eigrp any any
   access-list   deny pim any 224.0.0.0 0.0.0.255
   access-list   deny udp any any port = 123
   access-list   deny udp any any port = 1645
   access-list   deny udp any any port = 1646
   access-list   deny udp any any port = 1812
   access-list   deny udp any any port = 1813
   access-list   deny tcp any port = 443 any
   access-list   deny tcp any any port = 443
   access-list   deny udp any port = 500 any port = 500
   access-list   deny udp any any port = 848
   access-list   deny ip host 10.162.5.1 any
   access-list   deny ip any host 10.162.5.1
   access-list   permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
   access-list   permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 23888
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 2048

TEK POLICY for the current KS-Policy ACEs Downloaded:
  GigabitEthernet0/0.5:
    IPsec SA:
        spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (2174)
Anti-Replay : Disabled
```

Se verifica sesión SA se encuentre activa:

```
GM2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.162.5.4      1.1.1.1         GDOI_REKEY        1002 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
GM2#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash    Auth DH
Lifetime Cap.

1002  10.162.5.4      1.1.1.1                ACTIVE 3des sha     rsig 0  0
       Engine-id:Conn-id =  SW:2

IPv6 Crypto ISAKMP SA
```

Se valida en el Key Server Principal queya aparezca registrado el Group Member Dos:

```
KSPPAL#sh crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPNGROUP (Unicast)
    Group Identity           : 7
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Group Members            : 2
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 23645 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 10
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : MYIPSECPROFILE
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 1931 secs
      ACL Configured         : access-list REDES-A-CIFRAR

     Group Server list       : Local
```

3.4.3 Verificar conectividad LAN-to-LAN y funcionamiento del cifrado

Se debe tener ping desde la red LAN del router Group Member Uno que es la Loopback (192.168.10.1/24) hacia la red LAN del router Group Member Dos que es la Loopback (192.168.20.1/24):

```
GM1#ping ip 192.168.20.1 source 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
GM1#show crypto ipsec sa

interface: GigabitEthernet0/0.5
    Crypto map tag: MYCRYPTOMAP, local addr 10.162.5.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.162.5.3, remote crypto endpt.: 0.0.0.0
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.5
     current outbound spi: 0xF12842B9(4045947577)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2083, flow_id: Onboard VPN:83, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3035)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
```

```
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2084, flow_id: Onboard VPN:84, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3035)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.162.5.3, remote crypto endpt.: 0.0.0.0
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.5
     current outbound spi: 0xF12842B9(4045947577)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2081, flow_id: Onboard VPN:81, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3035)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2082, flow_id: Onboard VPN:82, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3035)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Si se realiza el mismo ping con 90 repeticiones se debe confirmar que esos 90 paquetes pasen encriptados:

```
GM1#ping ip 192.168.20.1 source 192.168.10.1 repeat 90
Type escape sequence to abort.
Sending 90, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (90/90), round-trip min/avg/max = 1/1/4 ms
GM1#show crypto ipsec sa

interface: GigabitEthernet0/0.5
    Crypto map tag: MYCRYPTOMAP, local addr 10.162.5.3

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.162.5.3, remote crypto endpt.: 0.0.0.0
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.5
     current outbound spi: 0xF12842B9(4045947577)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2083, flow_id: Onboard VPN:83, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3019)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
```

```
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2084, flow_id: Onboard VPN:84, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3019)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.162.5.3, remote crypto endpt.: 0.0.0.0
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0.5
     current outbound spi: 0xF12842B9(4045947577)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2081, flow_id: Onboard VPN:81, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3019)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
      spi: 0xF12842B9(4045947577)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2082, flow_id: Onboard VPN:82, sibling_flags 80000040,
crypto map: MYCRYPTOMAP
        sa timing: remaining key lifetime (sec): (3019)
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

4. Configuracion Alta disponibilidad GET VPN

4.1 Configuración de redundancia GET VPN

4.1.1 Importar el mismo par de llaves RSA para la autenticación del rekey a los Key Servers del cluster

Es necesario distribuir este par de llaves RSA

```
KSPPAL(config)#crypto key export rsa key_rekey pem terminal des 12345678
% Key name: key_rekey
   Usage: General Purpose Key
   Key data:
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6GONtCc7HnsxSirnaVKi
QiBwBv+zx4bFYEOzgSJbfD210hPHVOgrru4Rnj5NGmqCnLBCLUNZ1r1vc3X0RRqB
KsWizgnCFsk/ymnUWEsyPQQHnNpK/OoqOcrMlfcUauBqvdT2JTnkLZbpB/OsozKR
h5Tgf4u7IesH7SpD9QekFX1dsiA2TDl0HVWyiXNe/4cEIk4dhVVywhBWim+attPK
agRw0zcuHEYPHK2OBJ+wuJ8qOmU3XL4v166Miiq/Sw4kKfcgk0X74JxHIL6GjAN+
VhC3nKjHaleEY6S4sAkB9N/RgSlicunKn8HPRK9g2hEFhHaWHrzfoLAjcrswDq/Z
9QIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,29EB35473E02316C
```

```
TmW0a/czzgcuC11VRlTxO7X5ZwHBVayY2njzrdF5QwWRKrmLcGRNrC3ug4yjH8tw
vup1GdZZfWF42Kpze2XZjoU39Bnw/XmbMbsIRN5he+/FcVmP2JWmzhItVzJI1Dfe
Iem6wrEhOQfiooABlteDSaxfdWmdPbVHAPZVkf55K2bS3+GfqRGu17k6DxL0CDfH
lCAQ4ptqDO6tFs9ka4XBz6Bk6LqUBhdXdvOFjA7S4w0WmTeDXGGRem/XWUgBo4qN
JZKh0GOgAK+hHKsJ1Joch9ZT9zCCM26Vxa2/DZFoPLSNQAvHdWGDFXOFiC6UJsth
JSIFum4l5oat4+VzFf+m5tv0d6EDjN1o8jYXNl3fG4ZmBEHXc6oGTPd95BSqkcSp
RdkqiulY8ewxu/uYg7GcAAUtkjesViv+m1DdnX7WzyIHlAIWCT0xF0JiEgEri8Mw
5BybuWPmbw5tH1/B1/vo1XaX1LW6L8AP9HapM6paHKuHmuUnCQZK2bFQYBOk1uN8
4oIsBKDZdJ6NqgszBdSkkEhOnVhFj84xy7UvAxqcE0ViihEWAY3RI418OW3vxU25
1CC93jHSVBr1JZg6KfxqE3i+msXQp30nF7dqVHJfMlbuY0/ROks4Frab+eWJM7fK
5nFh+PcrlCeiwUxQhsWC46ChRIBrGXD6xR4obIp3kQD8hm4nUk1GPim65xDscAr9
tpowB/rsy6Uk9SQtDtV52smfzEdL3zggEQX7OmByrYMUMZwaZRrFiNKIxeaNGjMI
7aZYaZjJ4Au1/zAiTvid6n8q5AdI0wi8O5aL2VcBfm/IQrBCllrnmbNQOd52Hbeq
PJdAOwfpZbttU7N5cANUxedDaAdlPoEJIT77QJRZfVVmeQM9Z7qKcg2Neb1kcelv
Pp79Sql5DQNMQO9n5WrSKC1jVjAqBx1LDl+DSnYQv7gMM8XXl95s/oKX+MwQjdlB
yv83u3pTHrCUTf3xkAsuXNYuFB0Qi9hed9GLHMcelReY2YLN1kD7G6CiV+wzrEZX
N+CNNw7nLmmGvepfdVuSUjplY+W0y22O0uezqwQoCKBOIHKgKslw2S27tVvXEXgO
kCNepSyRG+z+tAsDrepuV7vWn0ZzPGfdlMwkUL5n7tsiZSih9SjSZLfIMsyuljVC
SY6i5GhgylmBOvEyAYF8BEcIl1muQb9vJmhbWdg6WUeMM6xgJ1rvuTmwcnXbGu1O
+J38XCYEhavuR2K15AMVZkTmMHNwHdHaR/0r8ujqFFsyQfZ0l3JicYAtamNsxeRA
/WvtDZ3nz7FAmQRgnZFb9KCrHeHy7Vg8w+12Ds/djdPIFP8TSMAZEoDZiJFgggEl
NDw+gCzwdN8UhLrao+GyVTJRQmsb1mdE0NK6p1rzfsOmjeyhfyddl463OR7Rcjtj
Bs+4KyvLtixFWrvcZy52kGJDMCdQOcevmaRuwcsjf1EhIDlrXHRZ7BjgHex5X1mI
pvgSPqE+RWdUvLR15e/Zfx3F9tKZeWfbUN2/2GSO9WRVjuV0W4tyMCA+2lateaPV
xze6wHdFOcN7XfO6NYcnN1OuMvIAJjWS1jj1DhjCT87+cdFCyV8YlyloHi6YYA6c
-----END RSA PRIVATE KEY-----
```

Se debe importar el par de llaves RSA del rekeying en el Key Server Backup:

```
KSBACKUP(config)#crypto key import  rsa key_rekey exportable terminal
12345678
% Enter PEM-formatted public General Purpose key or certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA6GONtCc7HnsxSirnaVKi
QiBwBv+zx4bFYEOzgSJbfD210hPHVOgrru4Rnj5NGmqCnLBCLUNZ1r1vc3X0RRqB
KsWizgnCFsk/ymnUWEsyPQQHnNpK/OoqOcrMlfcUauBqvdT2JTnkLZbpB/OsozKR
h5Tgf4u7IesH7SpD9QekFX1dsiA2TDl0HVWyiXNe/4cEIk4dhVVywhBWim+attPK
agRw0zcuHEYPHK2OBJ+wuJ8qOmU3XL4V166Miiq/Sw4kKfcgk0X74JxHIL6GjAN+
VhC3nKjHaleEY6S4sAkB9N/RgSlicunKn8HPRK9g2hEFhHaWHrzfoLAjcrswDq/Z
9QIDAQAB
-----END PUBLIC KEY-----
quit
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,29EB35473E02316C


TmW0a/czzgcuC11VRlTxO7X5ZwHBVayY2njzrdF5QwWRKrmLcGRNrC3ug4yjH8tw
vup1GdZZfWF42Kpze2XZjoU39Bnw/XmbMbsIRN5he+/FcVmP2JWmzhItVzJI1Dfe
Iem6wrEhOQfiooABlteDSaxfdWmdPbVHAPZVkf55K2bS3+GfqRGu17k6DxL0CDfH
lCAQ4ptqDO6tFs9ka4XBz6Bk6LqUBhdXdvOFjA7S4w0WmTeDXGGRem/XWUgBo4qN
JZKh0GOgAK+hHKsJ1Joch9ZT9zCCM26Vxa2/DZFoPLSNQAvHdWGDFXOFiC6UJsth
JSIFum4l5oat4+VzFf+m5tv0d6EDjN1o8jYXNl3fG4ZmBEHXc6oGTPd95BSqkcSp
RdkqiulY8ewxu/uYg7GcAAUtkjesViv+m1DdnX7WzyIHlAIWCT0xF0JiEgEri8Mw
5BybuWPmbw5tH1/B1/vo1XaX1LW6L8AP9HapM6paHKuHmuUnCQZK2bFQYBOk1uN8
4oIsBKDZdJ6NqgszBdSkkEhOnVhFj84xy7UvAxqcE0ViihEWAY3RI418OW3vxU25
1CC93jHSVBr1JZg6KfxqE3i+msXQp30nF7dqVHJfMlbuY0/ROks4Frab+eWJM7fK
5nFh+PcrlCeiwUxQhsWC46ChRIBrGXD6xR4obIp3kQD8hm4nUk1GPim65xDscAr9
tpowB/rsy6Uk9SQtDtV52smfzEdL3zggEQX7OmByrYMUMZwaZRrFiNKIxeaNGjMI
7aZYaZjJ4Au1/zAiTvid6n8q5AdI0wi8O5aL2VcBfm/IQrBCllrnmbNQOd52Hbeq
PJdAOwfpZbttU7N5cANUxedDaAdlPoEJIT77QJRZfVVmeQM9Z7qKcg2Neb1kcelv
Pp79Sql5DQNMQO9n5WrSKC1jVjAqBx1LDl+DSnYQv7gMM8XXl95s/oKX+MwQjdlB
yv83u3pTHrCUTf3xkAsuXNYuFB0Qi9hed9GLHMcelReY2YLN1kD7G6CiV+wzrEZX
N+CNNw7nLmmGvepfdVuSUjplY+W0y22O0uezqwQoCKBOIHKgKslw2S27tVvXEXgO
kCNepSyRG+z+tAsDrepuV7vWn0ZzPGfdlMwkUL5n7tsiZSih9SjSZLfIMsyuljVC
SY6i5GhgylmBOvEyAYF8BEcIl1muQb9vJmhbWdg6WUeMM6xgJ1rvuTmwcnXbGu1O
+J38XCYEhavuR2K15AMVZkTmMHNwHdHaR/0r8ujqFFsyQfZ0l3JicYAtamNsxeRA
/WvtDZ3nz7FAmQRgnZFb9KCrHeHy7Vg8w+12Ds/djdPIFP8TSMAZEoDZiJFgggEl
NDw+gCzwdN8UhLrao+GyVTJRQmsb1mdE0NK6p1rzfsOmjeyhfyddl463OR7Rcjtj
Bs+4KyvLtixFWrvcZy52kGJDMCdQOcevmaRuwcsjf1EhIDlrXHRZ7BjgHex5X1mI
pvgSPqE+RWdUvLR15e/Zfx3F9tKZeWfbUN2/2GSO9WRVjuV0W4tyMCA+2lateaPV
xze6wHdFOcN7XfO6NYcnN10uMvIAJjWS1jj1DhjCT87+cdFCyV8YlyloHi6YYA6c
-----END RSA PRIVATE KEY-----
quit


% Key pair import succeeded.
```

4.1.2 Configurar una malla de conectividad fullmesh de intercambio IKE entre los Key Servers

```
KSPPAL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSPPAL(config)#crypto isakmp policy 20
KSPPAL(config-isakmp)#lifetime 86400
KSPPAL(config-isakmp)#exit
KSPPAL(config)#
KSPPAL(config)#crypto isakmp key cisco123 address 2.2.2.2
KSPPAL(config)#
KSPPAL(config)#
KSPPAL(config)#crypto isakmp keepalive 10 periodic
KSPPAL(config)#
KSPPAL(config)#exit
KSPPAL#
```

4.1.3 Configurar el protocolo COOP

```
KSPPAL#
KSPPAL#
KSPPAL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSPPAL(config)#crypto gdoi group MYGETVPNGROUP
KSPPAL(config-gdoi-group)#server local
KSPPAL(gdoi-local-server)#redun
KSPPAL(gdoi-local-server)#redundancy
KSPPAL(gdoi-coop-ks-config)#local prio
KSPPAL(gdoi-coop-ks-config)#local priority 100
KSPPAL(gdoi-coop-ks-config)#peer add
KSPPAL(gdoi-coop-ks-config)#peer address ip
KSPPAL(gdoi-coop-ks-config)#peer address ipv4 2.2.2.2
KSPPAL(gdoi-coop-ks-config)#exit
KSPPAL(gdoi-local-server)#exit
KSPPAL(config-gdoi-group)#exit
KSPPAL(config)#exit
KSPPAL#
KSPPAL#
```

4.1.4 Configuración del Key Server Backup

```
KSBACKUP#
KSBACKUP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSBACKUP(config)#
KSBACKUP(config)#
KSBACKUP(config)#crypto isakmp key cisco123 address 1.1.1.1
KSBACKUP(config)#crypto isakmp key cisco123 address 10.162.5.3
KSBACKUP(config)#crypto isakmp key cisco123 address 10.162.5.4
KSBACKUP(config)#
KSBACKUP(config)#
KSBACKUP(config)#cry
KSBACKUP(config)#crypto isa
KSBACKUP(config)#crypto isakmp poli
KSBACKUP(config)#crypto isakmp policy 20
KSBACKUP(config-isakmp)#au
KSBACKUP(config-isakmp)#authentication pre
KSBACKUP(config-isakmp)#authentication pre-share
KSBACKUP(config-isakmp)#gro
KSBACKUP(config-isakmp)#group 5
KSBACKUP(config-isakmp)#exit
KSBACKUP(config)#
KSBACKUP(config)#
KSBACKUP(config)#cry
KSBACKUP(config)#crypto ip
KSBACKUP(config)#crypto ipsec trsn
KSBACKUP(config)#crypto ipsec trans
```

```
KSBACKUP(config)#crypto ipsec transform-set MYSET esp-aes
KSBACKUP(config)#crypto ipsec transform-set MYSET esp-aes esp-sha
KSBACKUP(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
KSBACKUP(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
KSBACKUP(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
KSBACKUP(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac
KSBACKUP(cfg-crypto-trans)#exit
KSBACKUP(config)#
KSBACKUP(config)#
KSBACKUP(config)#
KSBACKUP(config)#cry
KSBACKUP(config)#crypto ipse
KSBACKUP(config)#crypto ipsec profil
KSBACKUP(config)#crypto ipsec profile MYPROFILE
KSBACKUP(ipsec-profile)#set tran
KSBACKUP(ipsec-profile)#set transform-set MYSET
KSBACKUP(ipsec-profile)#ip acc
KSBACKUP(ipsec-profile)#exit
KSBACKUP(config)#ip acc
KSBACKUP(config)#ip access-list extended REDES-A-CIFRAR
KSBACKUP(config-ext-nacl)#
KSBACKUP(config-ext-nacl)#deny   esp any any
KSBACKUP(config-ext-nacl)#deny   tcp any any eq tacacs
KSBACKUP(config-ext-nacl)#deny   tcp any eq tacacs any
KSBACKUP(config-ext-nacl)#deny   tcp any any eq 22
KSBACKUP(config-ext-nacl)#deny   tcp any eq 22 any
KSBACKUP(config-ext-nacl)#deny   tcp any any eq bgp
KSBACKUP(config-ext-nacl)#deny   tcp any eq bgp any
KSBACKUP(config-ext-nacl)#deny   ospf any any
KSBACKUP(config-ext-nacl)#deny   eigrp any any
KSBACKUP(config-ext-nacl)#deny   pim any 224.0.0.0 0.0.0.255
KSBACKUP(config-ext-nacl)#deny   udp any any eq ntp
KSBACKUP(config-ext-nacl)#deny   udp any any eq 1645
KSBACKUP(config-ext-nacl)#deny   udp any any eq 1646
KSBACKUP(config-ext-nacl)#deny   udp any any eq 1812
KSBACKUP(config-ext-nacl)#deny   udp any any eq 1813
KSBACKUP(config-ext-nacl)#deny   tcp any eq 443 any
KSBACKUP(config-ext-nacl)#deny   tcp any any eq 443
KSBACKUP(config-ext-nacl)#deny   udp any eq isakmp any eq isakmp
KSBACKUP(config-ext-nacl)#deny   udp any any eq 848
KSBACKUP(config-ext-nacl)#deny   ip host 10.162.5.1 any
KSBACKUP(config-ext-nacl)#deny   ip any host 10.162.5.1
KSBACKUP(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0
0.0.0.255
KSBACKUP(config-ext-nacl)#
KSBACKUP(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 192.168.10.0
0.0.0.255
KSBACKUP(config-ext-nacl)#
KSBACKUP(config-ext-nacl)#exit
KSBACKUP(config)#
KSBACKUP(config)#cry
KSBACKUP(config)#crypto gdo
KSBACKUP(config)#crypto gdoi gro
KSBACKUP(config)#crypto gdoi group MYGETVPNGROUP
KSBACKUP(config-gdoi-group)#iden
KSBACKUP(config-gdoi-group)#identity number 7
KSBACKUP(config-gdoi-group)#server local
```

```
KSBACKUP(gdoi-local-server)#add
KSBACKUP(gdoi-local-server)#address ip
KSBACKUP(gdoi-local-server)#address ipv4 2.2.2.2
KSBACKUP(gdoi-local-server)#rek
KSBACKUP(gdoi-local-server)#rekey trans
KSBACKUP(gdoi-local-server)#rekey transport uni
KSBACKUP(gdoi-local-server)#rekey transport unicast
KSBACKUP(gdoi-local-server)#
KSBACKUP(gdoi-local-server)#rekey au
KSBACKUP(gdoi-local-server)#rekey authentication my
KSBACKUP(gdoi-local-server)#rekey authentication mypubkey rsa key_rekey
KSBACKUP(gdoi-local-server)#sa ip
KSBACKUP(gdoi-local-server)#sa ipsec 10
KSBACKUP(gdoi-sa-ipsec)#cry
KSBACKUP(gdoi-sa-ipsec)#exit
KSBACKUP(gdoi-local-server)#exit
KSBACKUP(config-gdoi-group)#exit
KSBACKUP(config)#cry
KSBACKUP(config)#crypto ips
KSBACKUP(config)#crypto ipsec pro
KSBACKUP(config)#crypto ipsec profile MYIPSECPROFILE
KSBACKUP(ipsec-profile)#se
KSBACKUP(ipsec-profile)#set trans
KSBACKUP(ipsec-profile)#set transform-set MYSET
KSBACKUP(ipsec-profile)#
KSBACKUP(ipsec-profile)#exit
KSBACKUP(config)#exit
KSBACKUP#
KSBACKUP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSBACKUP(config)#cry
KSBACKUP(config)#crypto gdo
KSBACKUP(config)#crypto gdoi grou
KSBACKUP(config)#crypto gdoi group MYGETVPNGROUP
KSBACKUP(config-gdoi-group)#ser
KSBACKUP(config-gdoi-group)#server local
KSBACKUP(gdoi-local-server)#sa ips
KSBACKUP(gdoi-local-server)#sa ipsec 10
KSBACKUP(gdoi-sa-ipsec)#profi
KSBACKUP(gdoi-sa-ipsec)#profile MYIPSECPROFILE
KSBACKUP(gdoi-sa-ipsec)#matc
KSBACKUP(gdoi-sa-ipsec)#match add
KSBACKUP(gdoi-sa-ipsec)#match address ip
KSBACKUP(gdoi-sa-ipsec)#match address ipv4 REDES-A-CIFRAR
KSBACKUP(gdoi-sa-ipsec)#exit
KSBACKUP(gdoi-local-server)#exit
KSBACKUP(config-gdoi-group)#exit
KSBACKUP(config)#cry
KSBACKUP(config)#crypto map MYCRYPTOMAP 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
        group has been configured.
KSBACKUP(config-crypto-map)#set gr
KSBACKUP(config-crypto-map)#set group MYGETVPNGROUP
      KSBACKUP(config-crypto-map)#exit
```

4.1.5 Configurar el protocolo COOP en el Key Server Backup

```
KSBACKUP(config)#crypto gdoi gr
KSBACKUP(config)#crypto gdoi group MYGETVPNGROUP
KSBACKUP(config-gdoi-group)#server lo
KSBACKUP(config-gdoi-group)#server local
KSBACKUP(gdoi-local-server)#redun
KSBACKUP(gdoi-local-server)#redundancy
KSBACKUP(gdoi-coop-ks-config)#local pri
KSBACKUP(gdoi-coop-ks-config)#local priority 75
KSBACKUP(gdoi-coop-ks-config)#peer add
KSBACKUP(gdoi-coop-ks-config)#peer address ipv
KSBACKUP(gdoi-coop-ks-config)#peer address ipv4 1.1.1.1
KSBACKUP(gdoi-coop-ks-config)#exit
KSBACKUP(gdoi-local-server)#exit
KSBACKUP(config-gdoi-group)#exit
KSBACKUP(config)#
KSBACKUP(config)#exit
```

4.1.6 Configurar múltiples Key Servers en los Group members

Se debe ingresar a los Group Members UNO y Dos, configurar las credenciales de autenticación para los key server configurados

```
GM1#
GM1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM1(config)#
GM1(config)#crypto isakmp key cisco123 address 2.2.2.2
GM1(config)#cry
GM1(config)#crypto gdo
GM1(config)#crypto gdoi gro
GM1(config)#crypto gdoi group MYGETVPNGROUP
GM1(config-gdoi-group)#ser
GM1(config-gdoi-group)#server add
GM1(config-gdoi-group)#server address ip
GM1(config-gdoi-group)#server address ipv4 2.2.2.2
GM1(config-gdoi-group)#exit
GM1(config)#exit
```

```
GM2#
GM2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM2(config)#crypto isakmp key cisco123 address 2.2.2.2
GM2(config)#crypto gdoi group MYGETVPNGROUP
GM2(config-gdoi-group)#server address ipv4 2.2.2.2
GM2(config-gdoi-group)#exit
```

```
!
!
!
!
crypto isakmp policy 20
 authentication pre-share
 group 5
 lifetime 300
crypto isakmp key cisco123 address 1.1.1.1
crypto isakmp key cisco123 address 2.2.2.2
!
!
!
!
crypto gdoi group MYGETVPNGROUP
 identity number 7
 server address ipv4 1.1.1.1
 server address ipv4 2.2.2.2
!
!
crypto map MYCRYPTOMAP 10 gdoi
 set group MYGETVPNGROUP
!
!
```

Se ingresa al Key Server Backup para verificar los 2 Group Members registrados:

```
KSBACKUP#
KSBACKUP#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID     : 10.162.5.3  GM Version: 1.0.4
Group Member ID     : 10.162.5.4  GM Version: 1.0.4
KSBACKUP#
KSBACKUP#
```

4.1.7 Verificacion redundancia GET VPN

Se debe verificar que las asociaciones de seguridad (SAs) IKE entre los key Servers se encuentran arriba

```
KSPPAL#
KSPPAL#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.162.5.4      1.1.1.1         GDOI_REKEY           0 ACTIVE
2.2.2.2         1.1.1.1         GDOI_IDLE         1015 ACTIVE

IPv6 Crypto ISAKMP SA

KSPPAL#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH
Lifetime Cap.

0     1.1.1.1         10.162.5.4             ACTIVE 3des sha         0  0
       Engine-id:Conn-id =  SW:16

1015  1.1.1.1         2.2.2.2                ACTIVE des  sha    psk  5
23:25:22 D
       Engine-id:Conn-id =  SW:15

IPv6 Crypto ISAKMP SA



KSBACKUP#
KSBACKUP#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
2.2.2.2         1.1.1.1         GDOI_IDLE         1001 ACTIVE

IPv6 Crypto ISAKMP SA

KSBACKUP#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH
Lifetime Cap.
```

```
1001  2.2.2.2         1.1.1.1                ACTIVE des   sha    psk   5
23:24:19
       Engine-id:Conn-id =  SW:1

IPv6 Crypto ISAKMP SA

KSBACKUP#
```

Se verifica que se haya establecido la sesión COOP entre los 2 Key Servers:

```
KSPPAL#
KSPPAL#show crypto gdoi ks coop
Crypto Gdoi Group Name :MYGETVPNGROUP
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 1.1.1.1
        Local Priority: 100
        Local KS Role: Primary    , Local KS Status: Alive
        Local KS version: 1.0.4
        Primary Timers:
                Primary Refresh Policy Time: 20
                Remaining Time: 7
                Antireplay Sequence Number: 228

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 2.2.2.2
                Peer Version: 1.0.4
                Peer Priority: 75
                Peer KS Role: Secondary , Peer KS Status: Alive
                Antireplay Sequence Number: 0

                IKE status: Established
                Counters:
                    Ann msgs sent: 83
                    Ann msgs sent with reply request: 36
                    Ann msgs recv: 0
                    Ann msgs recv with reply request: 1
                    Packet sent drops: 73
                    Packet Recv drops: 0
                    Total bytes sent: 92911
                    Total bytes recv: 152
```

Con el siguiente comando se puede verificar si el peer local fue elegido como Key Server Primario ó Secundario.

```
KSBACKUP#show crypto gdoi ks coop
Crypto Gdoi Group Name :MYGETVPNGROUP
        Group handle: 2147483650, Local Key Server handle: 2147483650

        Local Address: 2.2.2.2
        Local Priority: 75
        Local KS Role: Secondary , Local KS Status: Alive
        Local KS version: 1.0.4
        Secondary Timers:
                Sec Primary Periodic Time: 30
                Remaining Time: 15, Retries: 0
                Invalid ANN PST recvd: 0
                New GM Temporary Blocking Enforced?: No
                Antireplay Sequence Number: 1

        Peer Sessions:
        Session 1:
                Server handle: 2147483651
                Peer Address: 1.1.1.1
                Peer Version: 1.0.4
                Peer Priority: 100
                Peer KS Role: Primary   , Peer KS Status: Alive
                Antireplay Sequence Number: 229

                IKE status: Established
                Counters:
                    Ann msgs sent: 0
                    Ann msgs sent with reply request: 1
                    Ann msgs recv: 85
                    Ann msgs recv with reply request: 0
                    Packet sent drops: 0
                    Packet Recv drops: 0
                    Total bytes sent: 152
                       Total bytes recv: 66833
```

5. Configuración GET VPN autenticación basada en PKI

Antes de pasar la solución GET VPN a PKI, se debe actualizar el reloj de los routers y procurar que todos queden sincronizados:

```
KSPPAL#show clock
*20:26:10.338 UTC Wed Dec 17 2014
KSPPAL#clock set 15:35:00 17 Dec 2014
KSPPAL#show clock
15:36:20.619 UTC Wed Dec 17 2014
```

GM1#show clock
*20:26:59.214 UTC Wed Dec 17 2014
GM1#clock set 15:35:00 17 Dec 2014
GM1#show clock
15:36:19.859 UTC Wed Dec 17 2014

GM2#show clock
15:31:28.862 UTC Wed Dec 17 2014
GM2#clock set 15:35:00 17 Dec 2014
GM2#show clock
15:36:19.555 UTC Wed Dec 17 2014

KSBACKUP#show clock
*20:25:04.138 UTC Wed Dec 17 2014
KSBACKUP#clock set 15:35:00 17 Dec 2014
KSBACKUP#show clock
15:36:19.147 UTC Wed Dec 17 2014

5.1 Configurar el servidor de Certificados basado en IOS Cisco

5.1.1 Crear un par de llaves RSA. Se debe generar un par de llaves RSA con un nombre y longitud:

KSPPAL#config t
Enter configuration commands, one per line. End with CNTL/Z.
KSPPAL(config)#crypto key generate rsa label PKI_SRV modulus 2048
The name for the keys will be: PKI_SRV

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 26 seconds)

5.1.2 Crear un trustpoint PKI y referenciar el par de llaves creadas.

```
KSPPAL(config)#crypto pki trustpoint PKI_SRV
KSPPAL(ca-trustpoint)#rsakeypair PKI_SRV
KSPPAL(ca-trustpoint)#exit
KSPPAL(config)#
```

5.1.3 Crear un servidor de certificados y configurar la ubicación de la base de datos.

```
KSPPAL(config)#
KSPPAL(config)#crypto pki server PKI_SRV
KSPPAL(cs-server)#issuer-name CN = CLARO, OU = PROGETVPNUSTA, C = CO
KSPPAL(cs-server)#database url flash:/PKI_SRV
% Server database url was changed. You need to move the
% existing database to the new location.
KSPPAL(cs-server)#database level ?
  complete  Each issued certificate is saved to the database
  minimum   Minimum certificate info is saved to the database
  names     Certificate serial-number & subject name is saved to the database

KSPPAL(cs-server)#database level names
```

5.1.4 Configurar política de emisión de certificados.

```
KSPPAL(cs-server)#
KSPPAL(cs-server)#
KSPPAL(cs-server)#hash sha1
KSPPAL(cs-server)#lifetime certificate 730
KSPPAL(cs-server)#lifetime ca-certificate 1825
KSPPAL(cs-server)#grant auto
KSPPAL(cs-server)#
KSPPAL(cs-server)#
```

5.1.5 Configurar una política de revocación.

```
KSPPAL(cs-server)#
KSPPAL(cs-server)#lifetime crl ?
  <0-336>  Lifetime in hours

KSPPAL(cs-server)#lifetime crl 4
KSPPAL(cs-server)#
KSPPAL(cs-server)#
```

5.1.6 Configurar la intefaz SCEP(Simple Certificate Enrollment Protocol)

```
KSPPAL(config)#
KSPPAL(config)#ip http server
KSPPAL(config)#
```

5.1.7 Habilitar servidor de certificados en el Key Server Principal

```
KSPPAL(config)#
KSPPAL(config)#crypto pki server PKI_SRV
KSPPAL(cs-server)#no shut
KSPPAL(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:

% Certificate Server enabled.
KSPPAL(cs-server)#
```

5.1.8 Verificar servidor de certificados basado en IOS Cisco.

```
KSPPAL#show crypto pki server
Certificate Server PKI_SRV:
   Status: enabled
   State: enabled
   Server's configuration is locked  (enter "shut" to unlock it)
   Issuer name: CN = CLARO, OU = PROGETVPNUSTA, C = CO
   CA cert fingerprint: 1344DE56 492A40BF FCCAD436 BB9F99BB
   Granting mode is: auto
   Last certificate issued serial number (hex): 1
   CA certificate expiration timer: 16:13:37 UTC Dec 16 2019
   CRL NextUpdate timer: 20:13:38 UTC Dec 17 2014
   Current primary storage dir: flash:/PKI_SRV
   Database Level: Names - subject name data written as <serialnum>.cnm
KSPPAL#
KSPPAL#
```

5.2 Configurar enrolamiento PKI.

5.2.1 Crear un par de llaves RSA.

```
KSPPAL#
KSPPAL#
KSPPAL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSPPAL(config)#crypto key generate rsa label PKI_KS modulus 2048 exportable
The name for the keys will be: PKI_KS

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 18 seconds)

KSPPAL(config)#exit
KSPPAL#

KSPPAL#
KSPPAL#show crypto key mypubkey rsa
% Key pair was generated at: 19:25:05 UTC Dec 15 2014
Key name: key_rekey
Key type: RSA KEYS
 Storage Device: private-config
```

Usage: General Purpose Key
Key is exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C916E6 62AD72D1 0150B591 EC7E52F6 4B1232C0 E3EBD6BC 46910051 14C4F82D
4F467C24 D3A4325D 1190D912 41B37F36 919CCF43 0B61F524 4589DFAF B0BE669A
B34847A7 5AA2F80A 7D359026 EA4BEB65 866FAAAD FD61CF3F EB652586 2F17526C
0BDB013D ACB94AC6 3A130E2F 8A934E51 ED1CDC46 D163A576 FE1A9BCA 95104D6F
69777804 18E2827B 15EC771B 07211DA5 302423A6 B3F32E24 18D79216 FBA52F3E
DBAACDC5 FD9FFBCD 7FA48B84 D64F52BE 3DA91419 E2B3C43D B9ED8646 653923E8
552A32EC 2ACCC9DA 70655353 E0026428 D4894B35 B1E4909D EDC7A576 E2A32935
1C3E1FB7 2D06DBBB 64A72E91 D6CF37DC B94747EE 4D528176 F1B4CDE3 94C678F9
CF020301 0001
% Key pair was generated at: 20:25:55 UTC Dec 17 2014
Key name: key_rekey.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D9C6A0 43BA226B
7006002C 0A7D73C2 925E5F2A D5E99427 8C6432C4 4C636599 B626E049 F421A2C2
E0C7762B DAA8DA07 968447E3 C41F8E68 E38C8CD3 BACE5B05 E93ABA50 0D0652F9
CF6ECC5E 2591A77B BD4DB593 9FCB26ED 1B35AB79 6C3C5968 05020301 0001
% Key pair was generated at: 15:47:08 UTC Dec 17 2014
Key name: PKI_SRV
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00A5BFD5 93A84092 7C402347 9265354B 452AD9BD 911F1CC4 0932680A 7657B888
25EC8B2F 68A0E787 FC3072C5 3685453E 1749055F 08A4F2F2 4689BCA4 E9D9CFAE
ACC47F25 91D31467 0EB023CE B9D600D6 3219B1E4 3ED7AA22 E742119E 5AA800DD
2802EC24 EB86B1D9 8ECF44E6 CEF10675 9FC80D3C 95513A32 1D897AF3 3F585314
42C0CF48 324F4B0B 779F50A8 43F027AC 8BDA9698 323C9A90 348F4CFB E38EB67D
3D77E33F A37FD443 2D3BE7F1 27F06D87 C679670F 88C1F26F 3B04DEFB C02755B7
496A5ED9 69BE20FA D02033B3 48DF3354 4A2BB075 CBFAFFFE B93C2EDE 6C2EDB87
3B5189E4 B76BC27D 9CF35F9D BC2C12B7 FE787290 0017D86F 736C3716 249B241F
F1020301 0001
% Key pair was generated at: 16:20:05 UTC Dec 17 2014

Key name: PKI_KS
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00BD9C01 2E257ECA E63A1C6D 1A5A38C2 60A967F0 25C130B0 1CACA8FE C472CB3E
185A091C 20775AA6 48199957 0E63DC35 0AD24971 1C18C431 81C9C750 2CB09BBD
D4D019F5 F864C477 617242E9 E7F2DF3C 5B870BAC 20D358EC E763BC57 803BC153
7ED2B4A4 436CAB45 F9D769FB 0E52585F 7537058E 50E7FBCF 22D1153E 795F78A7
3A478698 96121036 3A3355D3 2580C178 48D58BD8 E9407A24 FC7583B0 49A41665
3854AE46 E7F21251 5DF40754 A3BF9B02 7B21AEE2 DB95566E 08A6DBD6 C17D7FE7
ED17A82A C4B876D3 3CD7E916 0CF3C06D F92104A5 2436F3E1 052BCF01 8E5EC559
A0525D91 0E481477 F8C0172A 13699ACE 2E57360C D5059541 AB0C2D38 6491C2C2
C3020301 0001
KSPPAL#
KSPPAL#

5.2.2 Crear un trustpoint PKI

KSPPAL#config t
Enter configuration commands, one per line. End with CNTL/Z.
KSPPAL(config)#crypto pki trustpoint PKI_KS
pkiKSPPAL(ca-trustpoint)#enrollment url http://1.1.1.1
KSPPAL(ca-trustpoint)#subject-name OU=GETVPN
KSPPAL(ca-trustpoint)#revocation-check crl
KSPPAL(ca-trustpoint)#rsakeypair PKI_KS
KSPPAL(ca-trustpoint)#

5.2.3 Autenticar Autoridad Certificadora (CA) PKI

KSPPAL(config)#
KSPPAL(config)#crypto pki authenticate PKI_KS
Certificate has the following attributes:
Fingerprint MD5: 1344DE56 492A40BF FCCAD436 BB9F99BB
Fingerprint SHA1: 317EB2A4 6F7FABC1 B59A785E 856E0344 7CBF49C9

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
KSPPAL(config)#

5.2.4 Crear solicitud de enrolamiento en el router

KSPPAL(config)#
KSPPAL(config)#crypto pki enroll PKI_KS
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: OU=GETVPN
% The subject name in the certificate will include: KSPPAL
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose PKI_KS' commandwill show the fingerprint.

KSPPAL#
KSPPAL#
KSPPAL#show crypto pki certificates
Certificate
Status: Available
Certificate Serial Number (hex): 02
Certificate Usage: General Purpose
Issuer:
cn=CLARO
ou=PROGETVPNUSTA

```
    c=CO
  Subject:
    Name: KSPPAL
    hostname=KSPPAL
    ou=GETVPN
  Validity Date:
    start date: 16:37:06 UTC Dec 17 2014
    end   date: 16:37:06 UTC Dec 16 2016
  Associated Trustpoints: PKI_KS

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: PKI_KS PKI_SRV


KSPPAL#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    Name: KSPPAL
    hostname=KSPPAL
    ou=GETVPN
  Validity Date:
```

```
   start date: 16:37:06 UTC Dec 17 2014
   end   date: 16:37:06 UTC Dec 16 2016
  Associated Trustpoints: PKI_KS

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: PKI_KS PKI_SRV
```

5.3 Configurar el enrolamiento PKI en el router Group Member Uno

5.3.1 Crear un par de llaves RSA

```
GM1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM1(config)#crypto key generate rsa label PKI_KS modulus 2048 exportable
The name for the keys will be: PKI_KS

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 10 seconds)

GM1(config)#exit
GM1#show crypto key mypubkey rsa
% Key pair was generated at: 17:13:28 UTC Dec 17 2014
Key name: PKI_KS
Key type: RSA KEYS
 Storage Device: not specified
```

```
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00C193DA 9492AE1B 62B9CF80 A48854E1 AFA518B7 5DF74DE8 5E0BBD06 BA462CEE
  6BD16939 05396225 16830F57 D61668B0 8DF27305 25AC3799 5191C110 CF4611F4
  8AAA25F4 5A5119EC 117C6341 197518C1 FD3E825E 1839E529 8856984F 6DACE3D7
  5C83C363 C6EC70C4 A0F9CEF0 ECE0105A 3E56ABED 2A7451FE F198D8B8 8044F535
  53266E51 D3FDE446 B8D3CA5D 756CE031 84A857DE 4AD3EE4B 968675A3 9390C785
  43673323 2CDF981C 8F176843 D6C6EB93 FB5C32CC 2FDBE243 CD76BDC6 E24F6021
  0109CC33 2D8715B7 8646270D D35F1ADA 4BF9CAD2 ADCD4A6A 81F0D5ED F6696822
  8B8BF794 14F381E3 9DDA784D CE8F3959 9BB8A7A8 BC9A14F3 9A7E6990 C5499EBB
  C3020301 0001
% Key pair was generated at: 17:13:29 UTC Dec 17 2014
Key name: PKI_KS.server
Key type: RSA KEYS
Temporary key
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D13ED6 E710F6CE
  83E9C999 B3EAF80A 9A25BA8A 5D9C2D63 4BBB6E36 58147BEB DC05848F ED1B0384
  60C03AA9 5C9FD364 370FF6D7 14324328 2CFC292A B4401861 4FED689D 6CD175E1
  0FD3F57C 20E16205 F17C41FA 3BE3DE81 2E3D3AF9 43D9047C D3020301 0001
```

5.3.2 Crear un trustpoint PKI.

```
GM1(config)#
GM1(config)#
GM1(config)#crypto pki trustpoint GETVPN
GM1(ca-trustpoint)#enrollment url http://1.1.1.1
GM1(ca-trustpoint)#subject-name OU=GETVPN
GM1(ca-trustpoint)#revocation-check crl
GM1(ca-trustpoint)#rsakeypair PKI_KS
GM1(ca-trustpoint)#auto-enroll 90 regenerate
GM1(ca-trustpoint)#exit
GM1(config)#exit
GM1#
```

5.3.3 Autenticar el Group Member PKI

```
GM1(config)#crypto pki authenticate GETVPN
Certificate has the following attributes:
      Fingerprint MD5: 1344DE56 492A40BF FCCAD436 BB9F99BB
     Fingerprint SHA1: 317EB2A4 6F7FABC1 B59A785E 856E0344 7CBF49C9

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
GM1(config)#
```

5.3.4 Crear una solicitud de enrolamiento en el router

```
GM1(config)#crypto pki enroll GETVPN
Trustpoint GETVPN has already enrolled and has a router cert issued to it.
If you successfully re-enroll this trustpoint,the existing certificate will be replaced.

Do you want to continue with re-enrollment? [yes/no]: yes
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: OU=GETVPN
% The subject name in the certificate will include: GM1
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
```

% The 'show crypto pki certificate verbose GETVPN' commandwill show the fingerprint.

GM1(config)#

GM1#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    Name: GM1
    hostname=GM1
    ou=GETVPN
  Validity Date:
    start date: 17:23:38 UTC Dec 17 2014
    end   date: 17:23:38 UTC Dec 16 2016
    renew date: 17:23:37 UTC Oct 4 2016
  Associated Trustpoints: GETVPN

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: GETVPN

GM1#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    Name: GM1
    hostname=GM1
    ou=GETVPN
  Validity Date:
    start date: 17:23:38 UTC Dec 17 2014
    end   date: 17:23:38 UTC Dec 16 2016
    renew date: 17:23:38 UTC Oct 4 2016
  Associated Trustpoints: GETVPN

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: GETVPN

-----> Antes de clarear el cifrado en el Group Member Uno debe hacerse lo siguiente:

KSPPAL#

```
KSPPAL#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSPPAL(config)#crypto isakmp policy 10
KSPPAL(config-isakmp)#auth
KSPPAL(config-isakmp)#authentication ?
  pre-share  Pre-Shared Key
  rsa-encr   Rivest-Shamir-Adleman Encryption
  rsa-sig    Rivest-Shamir-Adleman Signature

KSPPAL(config-isakmp)#authentication rsa-si
KSPPAL(config-isakmp)#authentication rsa-sig
KSPPAL(config-isakmp)#exit
KSPPAL(config)#
KSPPAL(config)#exit
KSPPAL#sh cry
KSPPAL#sh crypto isa
KSPPAL#sh crypto isakmp pol
KSPPAL#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 20
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit


GM1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM1(config)#crypto isakmp policy 10
GM1(config-isakmp)#authentication rsa-sig
GM1(config-isakmp)#exit
GM1(config)#exit
GM1#
```

-----> se clarea el cifrado

```
GM1#
GM1#clear crypto gdoi
% The Key Server and Group Member will destroy created and downloaded policies.
% All Group Members are required to re-register.

Are you sure you want to proceed ? [yes/no]: yes
```

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.162.5.3      1.1.1.1         GDOI_REKEY     1030 ACTIVE
1.1.1.1         10.162.5.3      GDOI_IDLE      1029 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
GM1#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local         Remote        I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1030  10.162.5.3    1.1.1.1              ACTIVE 3des sha    rsig 0  0
      Engine-id:Conn-id =  SW:30

1029  10.162.5.3    1.1.1.1              ACTIVE des  sha    rsig 1  23:58:40
      Engine-id:Conn-id =  SW:29

IPv6 Crypto ISAKMP SA
```

-----> Se verifica el registro del miembro y se valida que se haya descargado la lista de acceso del Key Server Principal

```
GM1#show crypto gdoi
```

GROUP INFORMATION

Group Name : MYGETVPNGROUP
Group Identity : 7
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 1.1.1.1
2.2.2.2

Group member : 10.162.5.3 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 1.1.1.1
Re-registers in : 3330 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 4
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 0
After latest register : 0
Rekey Acks sents : 0

ACL Downloaded From KS 1.1.1.1:
access-list deny esp any any
access-list deny tcp any any port = 49
access-list deny tcp any port = 49 any
access-list deny tcp any any port = 22
access-list deny tcp any port = 22 any
access-list deny tcp any any port = 179
access-list deny tcp any port = 179 any
access-list deny ospf any any

```
  access-list   deny eigrp any any
  access-list   deny pim any 224.0.0.0 0.0.0.255
  access-list   deny udp any any port = 123
  access-list   deny udp any any port = 1645
  access-list   deny udp any any port = 1646
  access-list   deny udp any any port = 1812
  access-list   deny udp any any port = 1813
  access-list   deny tcp any port = 443 any
  access-list   deny tcp any any port = 443
  access-list   deny udp any port = 500 any port = 500
  access-list   deny udp any any port = 848
  access-list   deny ip host 10.162.5.1 any
  access-list   deny ip any host 10.162.5.1
  access-list   permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
  access-list   permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

KEK POLICY:
   Rekey Transport Type     : Unicast
   Lifetime (secs)          : 75332
   Encrypt Algorithm        : 3DES
   Key Size                 : 192
   Sig Hash Algorithm       : HMAC_AUTH_SHA
   Sig Key Length (bits)    : 2048

TEK POLICY for the current KS-Policy ACEs Downloaded:
 GigabitEthernet0/0.5:
   IPsec SA:
      spi: 0xD2ED283(221172355)
      transform: esp-aes esp-sha-hmac
      sa timing:remaining key lifetime (sec): (223)
      Anti-Replay : Disabled

   IPsec SA:
      spi: 0x434194EE(1128371438)
      transform: esp-aes esp-sha-hmac
      sa timing:remaining key lifetime (sec): (3438)
      Anti-Replay : Disabled


------> confirma conectividad hacia la red LAN
```

GM1#sh ip int br
Interface IP-Address OK? Method Status Protocol
Embedded-Service-Engine0/0 unassigned YES NVRAM administratively down down
GigabitEthernet0/0 unassigned YES NVRAM up up
GigabitEthernet0/0.5 10.162.5.3 YES NVRAM up up
GigabitEthernet0/0.179 192.168.200.23 YES NVRAM up up
GigabitEthernet0/1 unassigned YES NVRAM administratively down down
Serial0/0/0 unassigned YES NVRAM administratively down down
Loopback30 192.168.10.1 YES manual up up

GM1#ping ip 192.168.20.1 so 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

-----> Se confirma que se observa el Group Member en ambos Key Servers

KSPPAL#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4

KSBACKUP#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4

KSPPAL#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

```
C-id  Local         Remote        I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1055  1.1.1.1       10.162.5.3          ACTIVE des  sha    rsig 1  07:49:12 D
      Engine-id:Conn-id =  SW:55

1054  1.1.1.1       2.2.2.2             ACTIVE des  sha    psk  5  05:54:26 D
      Engine-id:Conn-id =  SW:54

0     1.1.1.1       10.162.5.4          ACTIVE 3des sha       0  0
      Engine-id:Conn-id =  SW:53

IPv6 Crypto ISAKMP SA
```

5.4 Crear una solicitud de enrolamiento en el router Group Member Dos

5.4.1 Crear un par de llaves RSA

```
GM2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
GM2(config)#crypto key generate rsa label PKI_KS modulus 2048 exportable
The name for the keys will be: PKI_KS

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 8 seconds)

GM2(config)#exit
GM2#show crypto key mypubkey rsa
% Key pair was generated at: 09:07:34 UTC Dec 18 2014
Key name: PKI_KS
Key type: RSA KEYS
```

Storage Device: not specified
Usage: General Purpose Key
Key is exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
009FE81F 87BDC0B7 F38BD876 C28402C9 203CF39B 098422D6 334C6BDB D94A85CA
75493CAB 39D995BF B6C1F8BB 405CF8DC 1A4DC157 17803F24 29E80AD8 3B54C075
001D6F16 8D68B6E5 D72236FF 379A785A DEB8DC86 26B97B7E 79B5FCB1 4EAD618D
C9A9D1F1 336C3895 9839607F B217803D 78675494 1C1B8CAA 4B827AE7 E1FC3004
47902C53 FA47AA8B 8A69E524 8D03ACE0 E75D31C4 6A1A49C2 D22C2352 A6EE74E6
59A1DCD5 2E47C331 3C3C0A19 F8387251 2CA99989 0722DF20 97755ECA 9DFA9E70
C9DA751C 091A925C E61B151C B780496B D9525037 1986807E 883948E9 5A96BF2D
3D281FCC 7B88E569 F901F891 5B81B660 74292AE5 CB4104E5 70BC178E E011E65D
9F020301 0001
% Key pair was generated at: 09:07:35 UTC Dec 18 2014
Key name: PKI_KS.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00E68C13 808D41D5
A13F0B84 30E38BE9 0BF1008D FFA2E95E 1DD964D7 5E02B72B 376DA5D0 9C79C0F4
6D842E5D C1DBAD6E 71626EBF 1C4F2C28 6CBA0ABF 3283152A 2CE96230 09929939
B15BB075 B1892D15 4CF06793 6BD4084F 52DB8184 9C797B53 E7020301 0001

5.4.2 Crear un trustpoint PKI

```
GM2#
GM2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM2(config)#crypto pki trustpoint GETVPN
GM2(ca-trustpoint)#enrollment url http://1.1.1.1
GM2(ca-trustpoint)#subject-name OU=GETVPN
GM2(ca-trustpoint)#revocation-check crl
GM2(ca-trustpoint)#rsakeypair PKI_KS
GM2(ca-trustpoint)#auto-enroll 90 regenerate
GM2(ca-trustpoint)#exit
GM2(config)#exit
```

5.4.3 Autenticar el Group Member Dos PKI

GM2(config)#crypto pki authenticate GETVPN
Certificate has the following attributes:
Fingerprint MD5: 1344DE56 492A40BF FCCAD436 BB9F99BB
Fingerprint SHA1: 317EB2A4 6F7FABC1 B59A785E 856E0344 7CBF49C9

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

5.4.4 Crear una solicitud de enrolamiento en el router

GM2(config)#
GM2(config)#crypto pki enroll GETVPN
Trustpoint GETVPN has already enrolled and has a router cert issued to it.
If you successfully re-enroll this trustpoint,the existing certificate will be replaced.

Do you want to continue with re-enrollment? [yes/no]: yes
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: OU=GETVPN
% The subject name in the certificate will include: GM2
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority

% The 'show crypto pki certificate verbose GETVPN' commandwill show the fingerprint.

GM2(config)#exit

-----> verificar validez del certificado recibido

M2#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    Name: GM2
    hostname=GM2
    ou=GETVPN
  Validity Date:
    start date: 09:14:56 UTC Dec 18 2014
    end   date: 09:14:56 UTC Dec 17 2016
    renew date: 09:14:56 UTC Oct 5 2016
  Associated Trustpoints: GETVPN

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: GETVPN

GM2#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    Name: GM2
    hostname=GM2
    ou=GETVPN
  Validity Date:
    start date: 09:14:56 UTC Dec 18 2014
    end   date: 09:14:56 UTC Dec 17 2016
    renew date: 09:14:55 UTC Oct 5 2016
  Associated Trustpoints: GETVPN

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: GETVPN

----> Se configura una política IKE con autenticación rsa-sig

GM2#config
GM2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
GM2(config)#cry
GM2(config)#crypto isakmp policy 10
GM2(config-isakmp)#aut
GM2(config-isakmp)#authentication rsa-sig
GM2(config-isakmp)#
GM2(config-isakmp)#exit
GM2(config)#exit
GM2#
GM2#

-----> Se clarea el cifrado y se verifica que la sesión SA se encuentre activa

GM2#clear crypto gdoi
% The Key Server and Group Member will destroy created and downloaded policies.
% All Group Members are required to re-register.

Are you sure you want to proceed ? [yes/no]: yes
GM2#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
1.1.1.1 10.162.5.4 GDOI_IDLE 1033 ACTIVE
10.162.5.4 1.1.1.1 GDOI_REKEY 1034 ACTIVE

IPv6 Crypto ISAKMP SA

GM2#sh crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
    K - Keepalives, N - NAT-traversal
    T - cTCP encapsulation, X - IKE Extended Authentication
    psk - Preshared key, rsig - RSA signature
    renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1031 10.162.5.4 1.1.1.1 ACTIVE des sha rsig 1 00:03:02 D
Engine-id:Conn-id = SW:31

1032 10.162.5.4 1.1.1.1 ACTIVE 3des sha rsig 0 0
Engine-id:Conn-id = SW:32

IPv6 Crypto ISAKMP SA

---> Se verifica el registro del Group Member Dos y se valida que se haya descargado la lista de acceso del Key Server Principal.

GM2#sh crypto gdoi
GROUP INFORMATION

Group Name : MYGETVPNGROUP
Group Identity : 7
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 0
IPSec SA Direction : Both

Group Server list : 1.1.1.1
2.2.2.2

Group member : 10.162.5.4 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 1.1.1.1
Re-registers in : 2166 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 0.0.0.0
Last rekey seq num : 22
Unicast rekey received: 0
Rekey ACKs sent : 0
Rekey Received : never
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP


```
  Rekeys cumulative
    Total received      : 0
    After latest register : 0
    Rekey Acks sents    : 0

 ACL Downloaded From KS 1.1.1.1:
   access-list  deny esp any any
   access-list  deny tcp any any port = 49
   access-list  deny tcp any port = 49 any
   access-list  deny tcp any any port = 22
   access-list  deny tcp any port = 22 any
   access-list  deny tcp any any port = 179
   access-list  deny tcp any port = 179 any
   access-list  deny ospf any any
   access-list  deny eigrp any any
   access-list  deny pim any 224.0.0.0 0.0.0.255
   access-list  deny udp any any port = 123
   access-list  deny udp any any port = 1645
   access-list  deny udp any any port = 1646
   access-list  deny udp any any port = 1812
   access-list  deny udp any any port = 1813
   access-list  deny tcp any port = 443 any
   access-list  deny tcp any any port = 443
   access-list  deny udp any port = 500 any port = 500
   access-list  deny udp any any port = 848
   access-list  deny ip host 10.162.5.1 any
   access-list  deny ip any host 10.162.5.1
   access-list  permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
   access-list  permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

 KEK POLICY:
    Rekey Transport Type    : Unicast
    Lifetime (secs)         : 16275
    Encrypt Algorithm       : 3DES
    Key Size                : 192
    Sig Hash Algorithm      : HMAC_AUTH_SHA
    Sig Key Length (bits)   : 2048

 TEK POLICY for the current KS-Policy ACEs Downloaded:
   GigabitEthernet0/0.5:
```

IPsec SA:
spi: 0x32533ED2(844316370)
transform: esp-aes esp-sha-hmac
sa timing:remaining key lifetime (sec): (2251)
Anti-Replay : Disabled

---> Se verifica conectividad hacia la red LAN

GM2#ping ip 192.168.10.1 so 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

---> Finalmente se confirma que se observa el Group Member Dos en ambos Key Servers

KSPPAL#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4

KSBACKUP#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4

-------->

KSPPAL#sh crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1055 1.1.1.1 10.162.5.3 ACTIVE des sha rsig 1 07:30:57 D
Engine-id:Conn-id = SW:55

1057 1.1.1.1 10.162.5.4 ACTIVE des sha rsig 1 23:55:24 D
Engine-id:Conn-id = SW:57

1054 1.1.1.1 2.2.2.2 ACTIVE des sha psk 5 05:36:11 D
Engine-id:Conn-id = SW:54

0 1.1.1.1 10.162.5.4 ACTIVE 3des sha 0 0
Engine-id:Conn-id = SW:53

IPv6 Crypto ISAKMP SA

5.5 Configurar el enrolamiento PKI en el Key Server Backup

Para que la solución GET VPN en autenticación PKI quede completa se debe realizar el enrolamiento en el Key Server Backup.

5.5.1 Crear un par de llaves RSA

KSBACKUP#show crypto key mypubkey rsa
% Key pair was generated at: 20:24:01 UTC Dec 15 2014
Key name: key_rekey
Key type: RSA KEYS

Storage Device: private-config
Usage: General Purpose Key
Key is exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C916E6 62AD72D1 0150B591 EC7E52F6 4B1232C0 E3EBD6BC 46910051 14C4F82D
4F467C24 D3A4325D 1190D912 41B37F36 919CCF43 0B61F524 4589DFAF B0BE669A
B34847A7 5AA2F80A 7D359026 EA4BEB65 866FAAAD FD61CF3F EB652586 2F17526C
0BDB013D ACB94AC6 3A130E2F 8A934E51 ED1CDC46 D163A576 FE1A9BCA 95104D6F
69777804 18E2827B 15EC771B 07211DA5 302423A6 B3F32E24 18D79216 FBA52F3E
DBAACDC5 FD9FFBCD 7FA48B84 D64F52BE 3DA91419 E2B3C43D B9ED8646 653923E8
552A32EC 2ACCC9DA 70655353 E0026428 D4894B35 B1E4909D EDC7A576 E2A32935
1C3E1FB7 2D06DBBB 64A72E91 D6CF37DC B94747EE 4D528176 F1B4CDE3 94C678F9
CF020301 0001
% Key pair was generated at: 10:32:23 UTC Dec 18 2014
Key name: key_rekey.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C6DADD F22300B1
DFE95520 964E5924 3531A214 23BA5E02 C11F4F39 25489ED4 93880DC7 62985448
7D13A612 551206E7 373F8C83 10898095 3C9898EA C8DF2B32 76B0A73F 6BC06EB2
FEC8F298 874989C3 B0122E3C EA5CE964 2063D94E 2498F0BE 03020301 0001
% Key pair was generated at: 10:34:24 UTC Dec 18 2014
Key name: PKI_KS
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is exportable.
Key Data:
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00A3FCF8 21BD31F1 9BF8BE94 5213AAFA 4F8EC526 70BF7B30 A7294E34 6207A20A
34CDD3D4 E8F3F978 A4AF60AA B96C86F0 E13E6E88 5D692F81 4046955F F1495243
BA9F90A5 6F58ACE6 9D828ED6 AAF93F11 06FF6337 7FF4DDB6 2DA71D45 3C585FE5
F72F724D F68ABC82 E176B716 FB829E2E E7F65284 4E3CA1E7 828961BA 1CB66C4D
1E37139C 3EBC71B6 2912FD13 776E4E7C E26B29C0 B3CB5EE6 D7D3D6A9 AFA0C3C9
F56FD6CF 9C6F371D F1ED8C2B 3C36DA22 6C955E37 C5AD043A 936F1957 2137137D
78743544 2FA2630B 8CF1C8B1 30143B2E F3D5449A D6D78D40 F875F52A 542E8F17
C6B4E25C 0E49C6DB 8B2BEDD4 BA637811 06FFEB19 1A1777B1 DDBF6131 965A5C0D

A1020301 0001

------> Se puede observar que la sesión SA contra el Key Server Principal se encuentra por Preshared keys

```
KSBACKUP#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
2.2.2.2         1.1.1.1         GDOI_IDLE      1026 ACTIVE

IPv6 Crypto ISAKMP SA

KSBACKUP#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1026  2.2.2.2         1.1.1.1               ACTIVE des  sha    psk  5  05:06:46 D
      Engine-id:Conn-id =  SW:26

IPv6 Crypto ISAKMP SA
```

5.5.2 Crear un trustpoint PKI

```
KSBACKUP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSBACKUP(config)#crypto pki trustpoint PKI_KS
KSBACKUP(ca-trustpoint)#enrollment url http://1.1.1.1
KSBACKUP(ca-trustpoint)#subject-name OU=GETVPN
KSBACKUP(ca-trustpoint)#revocation-check crl
```

```
KSBACKUP(ca-trustpoint)#rsakeypair PKI_KS
KSBACKUP(ca-trustpoint)#exit
KSBACKUP(config)#
```

5.5.3 Autenticar el Key Server Backup PKI

```
KSBACKUP(config)#crypto pki authenticate PKI_KS
Certificate has the following attributes:
      Fingerprint MD5: 1344DE56 492A40BF FCCAD436 BB9F99BB
     Fingerprint SHA1: 317EB2A4 6F7FABC1 B59A785E 856E0344 7CBF49C9

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted
```

5.5.4 Crear una solicitud de enrolamiento en el router

```
KSBACKUP(config)#crypto pki enroll PKI_KS
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: OU=GETVPN
% The subject name in the certificate will include: KSBACKUP
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
```

% The 'show crypto pki certificate verbose PKI_KS' commandwill show the fingerprint.

KSBACKUP(config)#

----> Se verifica la validez del certificado

KSBACKUP#show crypto pki certificates
Certificate
 Status: Available
 Certificate Serial Number (hex): 07
 Certificate Usage: General Purpose
 Issuer:
  cn=CLARO
  ou=PROGETVPNUSTA
  c=CO
 Subject:
  Name: KSBACKUP
  hostname=KSBACKUP
  ou=GETVPN
 Validity Date:
  start date: 10:43:53 UTC Dec 18 2014
  end date: 10:43:53 UTC Dec 17 2016
 Associated Trustpoints: PKI_KS

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
  cn=CLARO
  ou=PROGETVPNUSTA
  c=CO
 Subject:
  cn=CLARO
  ou=PROGETVPNUSTA
  c=CO
 Validity Date:
  start date: 16:13:37 UTC Dec 17 2014
  end date: 16:13:37 UTC Dec 16 2019
 Associated Trustpoints: PKI_KS

```
KSBACKUP#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 07
  Certificate Usage: General Purpose
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    Name: KSBACKUP
    hostname=KSBACKUP
    ou=GETVPN
  Validity Date:
    start date: 10:43:53 UTC Dec 18 2014
    end   date: 10:43:53 UTC Dec 17 2016
  Associated Trustpoints: PKI_KS

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Subject:
    cn=CLARO
    ou=PROGETVPNUSTA
    c=CO
  Validity Date:
    start date: 16:13:37 UTC Dec 17 2014
    end   date: 16:13:37 UTC Dec 16 2019
  Associated Trustpoints: PKI_KS
```

----> Al igual que en el Key Server Principal, también debe configurarse una política IKE con autenticación rsa-sig, con una secuencia menor que la configurada para Preshared keys

```
KSBACKUP#config t
Enter configuration commands, one per line.  End with CNTL/Z.
KSBACKUP(config)#crypto isakmp policy 10
KSBACKUP(config-isakmp)#authentication rsa-sig
KSBACKUP(config-isakmp)#exit
KSBACKUP(config)#exit
KSBACKUP#
```

---> Se clarea el cifrado, y se verifica que la sesión SA quede activa

```
KSBACKUP#
KSBACKUP#clear crypto gdoi
% The Key Server and Group Member will destroy created and downloaded policies.
% All Group Members are required to re-register.

Are you sure you want to proceed ? [yes/no]: yes

KSBACKUP#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
2.2.2.2         1.1.1.1         MM_NO_STATE    1026 ACTIVE (deleted)
1.1.1.1         2.2.2.2         GDOI_IDLE      1027 ACTIVE

IPv6 Crypto ISAKMP SA


KSBACKUP#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local       Remote      I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1027  2.2.2.2     1.1.1.1            ACTIVE des  sha    rsig 1  23:55:31 D
      Engine-id:Conn-id =  SW:27

IPv6 Crypto ISAKMP SA
```

----> Se verifica que la sesión COOP se encuentre establecida nuevamente entre los Key Server

```
KSBACKUP#
KSBACKUP#show crypto gdoi ks coop
Crypto Gdoi Group Name :MYGETVPNGROUP
    Group handle: 2147483651, Local Key Server handle: 2147483653

    Local Address: 2.2.2.2
    Local Priority: 75
    Local KS Role: Secondary , Local KS Status: Alive
    Local KS version: 1.0.4
    Secondary Timers:
        Sec Primary Periodic Time: 30
        Remaining Time: 13, Retries: 0
        Invalid ANN PST recvd: 0
        New GM Temporary Blocking Enforced?: No
        Antireplay Sequence Number: 2

    Peer Sessions:
    Session 1:
        Server handle: 2147483652
        Peer Address: 1.1.1.1
        Peer Version: 1.0.4
        Peer Priority: 100
        Peer KS Role: Primary   , Peer KS Status: Alive
        Antireplay Sequence Number: 12185

        IKE status: Established
        Counters:
          Ann msgs sent: 0
          Ann msgs sent with reply request: 1
          Ann msgs recv: 21
          Ann msgs recv with reply request: 0
          Packet sent drops: 1
          Packet Recv drops: 0
          Total bytes sent: 152
          Total bytes recv: 16023
```


```
KSPPAL#show crypto gdoi ks coop
Crypto Gdoi Group Name :MYGETVPNGROUP
    Group handle: 2147483651, Local Key Server handle: 2147483653

    Local Address: 1.1.1.1
    Local Priority: 100
    Local KS Role: Primary   , Local KS Status: Alive
    Local KS version: 1.0.4
    Primary Timers:
        Primary Refresh Policy Time: 20
        Remaining Time: 9
        Antireplay Sequence Number: 12190

    Peer Sessions:
    Session 1:
        Server handle: 2147483652
        Peer Address: 2.2.2.2
        Peer Version: 1.0.4
        Peer Priority: 75
        Peer KS Role: Secondary , Peer KS Status: Alive
        Antireplay Sequence Number: 1

        IKE status: Established
        Counters:
          Ann msgs sent: 12127
          Ann msgs sent with reply request: 20
          Ann msgs recv: 2
          Ann msgs recv with reply request: 2
          Packet sent drops: 23
          Packet Recv drops: 0
          Total bytes sent: 9402703
          Total bytes recv: 1410
```

-------> Se valida que los key Servers se encuentran sincronizados

KSBACKUP#show crypto gdoi ks policy
Key Server Policy:
For group MYGETVPNGROUP (handle: 2147483651) server 2.2.2.2 (handle: 2147483653):

For group MYGETVPNGROUP (handle: 2147483651) server 1.1.1.1 (handle: 2147483652):

```
 # of teks : 1  Seq num : 23
 KEK POLICY (transport type : Unicast)
   spi : 0x010CA8416C964A995210F45E235B1533
   management alg     : disabled    encrypt alg      : 3DES
   crypto iv length   : 8           key size         : 24
   orig life(sec): 86400       remaining life(sec): 12498
   sig hash algorithm : enabled     sig key length    : 294
   sig size           : 256
   sig key name       : key_rekey

 TEK POLICY (encaps : ENCAPS_TUNNEL)
   spi              : 0xD1BF73D9
   access-list       : REDES-A-CIFRAR
   transform         : esp-aes esp-sha-hmac
   alg key size      : 16           sig key size         : 20
   orig life(sec)    : 3600         remaining life(sec)   : 1690
   tek life(sec)     : 2284         elapsed time(sec)     : 594
   override life (sec): 0           antireplay window size: 64
```

KSPPAL#show crypto gdoi ks policy
Key Server Policy:
For group MYGETVPNGROUP (handle: 2147483651) server 1.1.1.1 (handle: 2147483653):

```
 # of teks : 1  Seq num : 23
 KEK POLICY (transport type : Unicast)
   spi : 0x010CA8416C964A995210F45E235B1533
   management alg     : disabled    encrypt alg      : 3DES
   crypto iv length   : 8           key size         : 24
   orig life(sec): 86400       remaining life(sec): 12484
   sig hash algorithm : enabled     sig key length    : 294
   sig size           : 256
   sig key name       : key_rekey
```

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0xD1BF73D9
access-list : REDES-A-CIFRAR
transform : esp-aes esp-sha-hmac
alg key size : 16 sig key size : 20
orig life(sec) : 3600 remaining life(sec) : 1675
tek life(sec) : 3600 elapsed time(sec) : 1925
override life (sec): 0 antireplay window size: 64

For group MYGETVPNGROUP (handle: 2147483651) server 2.2.2.2 (handle: 2147483652):

----------> Se confirma conectividad LAN-to-LAN entre los Group Members Uno y Dos

GM1#ping ip 192.168.20.1 so 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

GM2#ping ip 192.168.10.1 so 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

---------> Se verifica que después del cambio se observen los Group Members en ambos Key Servers

KSPPAL#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4

KSBACKUP#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4

-------> Se verifica la entrega de Certificados Digitales del key Server Principal a key Server Backup, Group Member Uno y Group Member Dos

KSPPAL#sh crypto isakmp sa de
Codes: C - IKE configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal
T - cTCP encapsulation, X - IKE Extended Authentication
psk - Preshared key, rsig - RSA signature
renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id Local Remote I-VRF Status Encr Hash Auth DH Lifetime Cap.

1055 1.1.1.1 10.162.5.3 ACTIVE des sha rsig 1 06:19:04 D
Engine-id:Conn-id = SW:55

1058 1.1.1.1 2.2.2.2 ACTIVE des sha rsig 1 23:38:08 D
Engine-id:Conn-id = SW:58

1057 1.1.1.1 10.162.5.4 ACTIVE des sha rsig 1 22:43:30 D
Engine-id:Conn-id = SW:57

0 1.1.1.1 10.162.5.4 ACTIVE 3des sha 0 0
Engine-id:Conn-id = SW:53

IPv6 Crypto ISAKMP SA

→Prueba Final

Se forza el Group Member Dos para que se asocie al Key Server Backup, para confirmar que se sigue teniendo conectividad LAN to LAN entre los Group Member Uno y Dos

```
GM2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM2(config)#
GM2(config)#
GM2(config)#
GM2(config)#crypto gdoi group MYGETVPNGROUP
GM2(config-gdoi-group)#no server address ipv4 1.1.1.1
GM2(config-gdoi-group)#exit
GM2(config)#exit
GM2#
GM2#

GM2#
GM2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
GM2(config)#crypto gdoi group MYGETVPNGROUP
GM2(config-gdoi-group)#server address ipv4 1.1.1.1
GM2(config-gdoi-group)#exit
GM2(config)#exit
GM2#
GM2#
```

---→ Despues de Realizar las configuraciones para forzar el Group Member Dos a trabajar con el Key Server Backup, se verifica que el GM 2 descargue las llaves del Key Server Backup.

```
GM2#clear crypto gdoi
% The Key Server and Group Member will destroy created and downloaded policies.
% All Group Members are required to re-register.

Are you sure you want to proceed ? [yes/no]: yes
GM2#
GM2#
```


```
GM2#
GM2#sh cry
GM2#sh crypto gdoi
GROUP INFORMATION

    Group Name              : MYGETVPNGROUP
    Group Identity          : 7
    Crypto Path             : ipv4
    Key Management Path     : ipv4
    Rekeys received         : 0
    IPSec SA Direction      : Both

     Group Server list      : 2.2.2.2
                              1.1.1.1

    Group member            : 10.162.5.4      vrf: None
      Version               : 1.0.4
      Registration status   : Registered
      Registered with       : 2.2.2.2
      Re-registers in       : 656 sec
      Succeeded registration: 1
      Attempted registration: 1
      Last rekey from       : 0.0.0.0
      Last rekey seq num    : 0
      Unicast rekey received: 0
      Rekey ACKs sent       : 0
      Rekey Received        : never
      allowable rekey cipher: any
      allowable rekey hash  : any
      allowable transformtag: any ESP

    Rekeys cumulative
      Total received        : 0
      After latest register : 0
      Rekey Acks sents      : 0

  ACL Downloaded From KS 2.2.2.2:
    access-list   deny esp any any
    access-list   deny tcp any any port = 49
    access-list   deny tcp any port = 49 any
```

```
   access-list   deny tcp any any port = 22
   access-list   deny tcp any port = 22 any
   access-list   deny tcp any any port = 179
   access-list   deny tcp any port = 179 any
   access-list   deny ospf any any
   access-list   deny eigrp any any
   access-list   deny pim any 224.0.0.0 0.0.0.255
   access-list   deny udp any any port = 123
   access-list   deny udp any any port = 1645
   access-list   deny udp any any port = 1646
   access-list   deny udp any any port = 1812
   access-list   deny udp any any port = 1813
   access-list   deny tcp any port = 443 any
   access-list   deny tcp any any port = 443
   access-list   deny udp any port = 500 any port = 500
   access-list   deny udp any any port = 848
   access-list   deny ip host 10.162.5.1 any
   access-list   deny ip any host 10.162.5.1
   access-list   permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
   access-list   permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 84835
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 2048

TEK POLICY for the current KS-Policy ACEs Downloaded:
  GigabitEthernet0/0.5:
    IPsec SA:
       spi: 0xF877C53D(4168598845)
       transform: esp-aes esp-sha-hmac
       sa timing:remaining key lifetime (sec): (712)
       Anti-Replay : Disabled
```


```
GM2#ping ip 192.168.10.1 so 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
GM2#
```

---→ Se confirma que la sesión de Certificados digitales siga arriba despues de forzar el Group Member Dos contra el Key Server Backup

```
GM2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
2.2.2.2         10.162.5.4      GDOI_IDLE      1038 ACTIVE
10.162.5.4      2.2.2.2         GDOI_REKEY     1039 ACTIVE

IPv6 Crypto ISAKMP SA

GM2#show crypto isakmp sa de
GM2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF  Status Encr Hash   Auth DH Lifetime Cap.

1038  10.162.5.4      2.2.2.2               ACTIVE des  sha    rsig 1  23:55:13 D
      Engine-id:Conn-id =  SW:38

1039  10.162.5.4      2.2.2.2               ACTIVE 3des sha    rsig 0  0
      Engine-id:Conn-id =  SW:39

IPv6 Crypto ISAKMP SA
```

--→ Se validan las mismas llaves, estando los Group Members Uno y Dos trabajando con key Servers diferentes.

KSBACKUP#show crypto gdoi ks policy
Key Server Policy:
For group MYGETVPNGROUP (handle: 2147483651) server 2.2.2.2 (handle: 2147483653):

For group MYGETVPNGROUP (handle: 2147483651) server 1.1.1.1 (handle: 2147483652):

```
 # of teks : 2  Seq num : 1
 KEK POLICY (transport type : Unicast)
   spi : 0x693F88780B27A6B995982168D8F6C1AB
   management alg     : disabled    encrypt alg      : 3DES
   crypto iv length   : 8           key size         : 24
   orig life(sec): 86400       remaining life(sec): 84498
   sig hash algorithm : enabled     sig key length    : 294
   sig size           : 256
   sig key name       : key_rekey

 TEK POLICY (encaps : ENCAPS_TUNNEL)
   spi              : 0xF877C53D
   access-list      : REDES-A-CIFRAR
   transform        : esp-aes esp-sha-hmac
   alg key size     : 16          sig key size        : 20
   orig life(sec)   : 3600        remaining life(sec)  : 374
   tek life(sec)    : 3595        elapsed time(sec)    : 3221
   override life (sec): 0         antireplay window size: 64


 TEK POLICY (encaps : ENCAPS_TUNNEL)
   spi              : 0x67968D5
   access-list      : REDES-A-CIFRAR
   transform        : esp-aes esp-sha-hmac
   alg key size     : 16          sig key size        : 20
   orig life(sec)   : 3600        remaining life(sec)  : 3589
   tek life(sec)    : 3595        elapsed time(sec)    : 6
   override life (sec): 0         antireplay window size: 64
```


```
KSPPAL#show crypto gdoi ks policy
Key Server Policy:
For group MYGETVPNGROUP (handle: 2147483651) server 1.1.1.1 (handle: 2147483653):

 # of teks : 2  Seq num : 1
 KEK POLICY (transport type : Unicast)
   spi : 0x693F88780B27A6B995982168D8F6C1AB
   management alg    : disabled    encrypt alg      : 3DES
   crypto iv length  : 8           key size         : 24
   orig life(sec): 86400       remaining life(sec): 84506
   sig hash algorithm : enabled     sig key length    : 294
   sig size          : 256
   sig key name      : key_rekey

 TEK POLICY (encaps : ENCAPS_TUNNEL)
   spi             : 0xF877C53D
   access-list       : REDES-A-CIFRAR
   transform         : esp-aes esp-sha-hmac
   alg key size      : 16          sig key size         : 20
   orig life(sec)    : 3600        remaining life(sec)   : 382
   tek life(sec)     : 3600        elapsed time(sec)     : 3218
   override life (sec): 0          antireplay window size: 64


 TEK POLICY (encaps : ENCAPS_TUNNEL)
   spi             : 0x67968D5
   access-list       : REDES-A-CIFRAR
   transform         : esp-aes esp-sha-hmac
   alg key size      : 16          sig key size         : 20
   orig life(sec)    : 3600        remaining life(sec)   : 3597
   tek life(sec)     : 3600        elapsed time(sec)     : 3
   override life (sec): 0          antireplay window size: 64

For group MYGETVPNGROUP (handle: 2147483651) server 2.2.2.2 (handle: 2147483652):
```

-→ Se verifican Group Members Uno y Dos en los Keys Servers

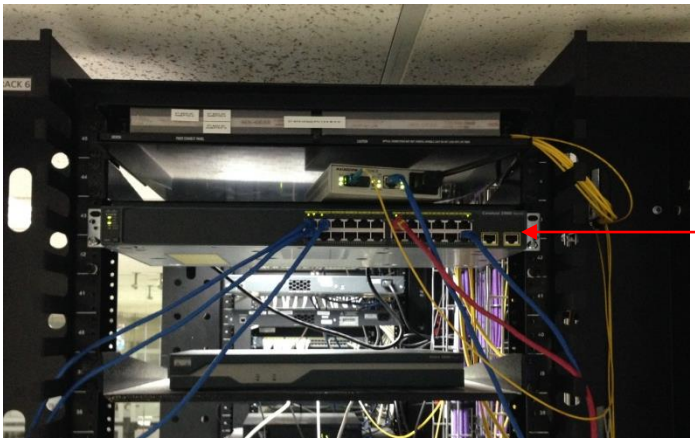
KSPPAL#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.4 GM Version: 1.0.4
Group Member ID : 10.162.5.3 GM Version: 1.0.4
KSPPAL#

KSBACKUP#
KSBACKUP#show crypto gdoi ks members | inc Mem
Group Member Information :
Group Member ID : 10.162.5.3 GM Version: 1.0.4
Group Member ID : 10.162.5.4 GM Version: 1.0.4
KSBACKUP#

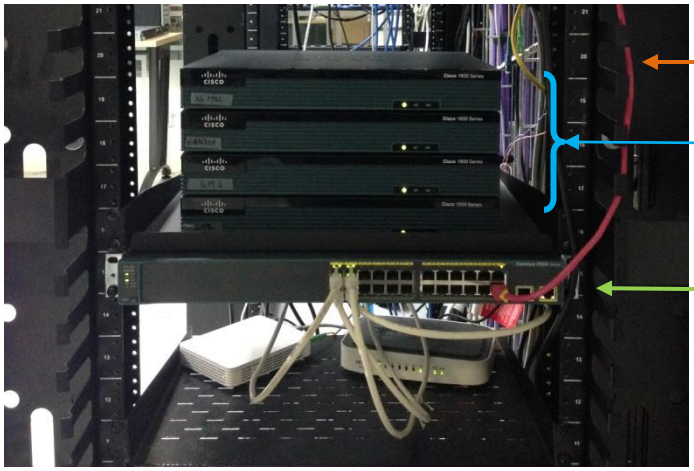
Referencias

- RANGEL Fabián y HERNANDEZ Pablo, Manual de Laboratorio GET VPN NOC Corporativo, Tipo de Documento: pdf de uso exclusivo de Claro Soluciones Fijas, Bogotá, Mayo de 2014.
- RANGEL Fabián, GET VPN Conceptos, Redes y Troubleshooting, Tipo de Documento: presentación Power Point uso exclusivo de Claro Soluciones Fijas, Marzo 2014.
- IPSEC VPNS, Tipo de Documento: presentación PowerPoint perteneciente a Cisco.

Anexos



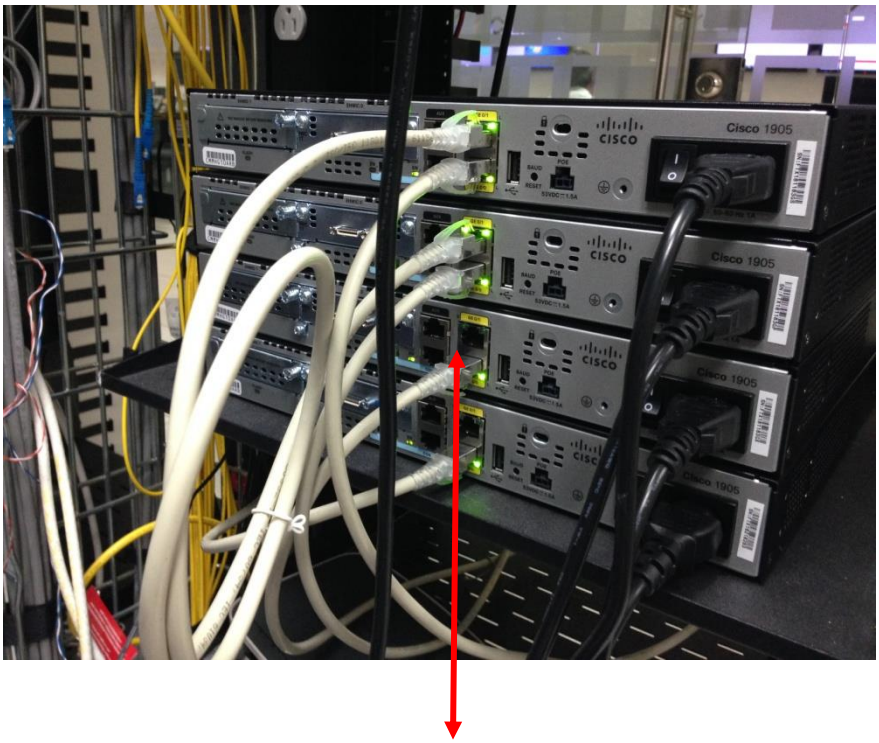
SW2960
SW Laboratorio Ortezal



Patch Cord entre (SW Laboratorio Ortezal y SWITCH_GETVPN)

4 Routers Cisco 1905

SWITCH_GETVPN
SW 2960 (Proyecto)



Conexiones Routers 1905 Topología Final Get VPN