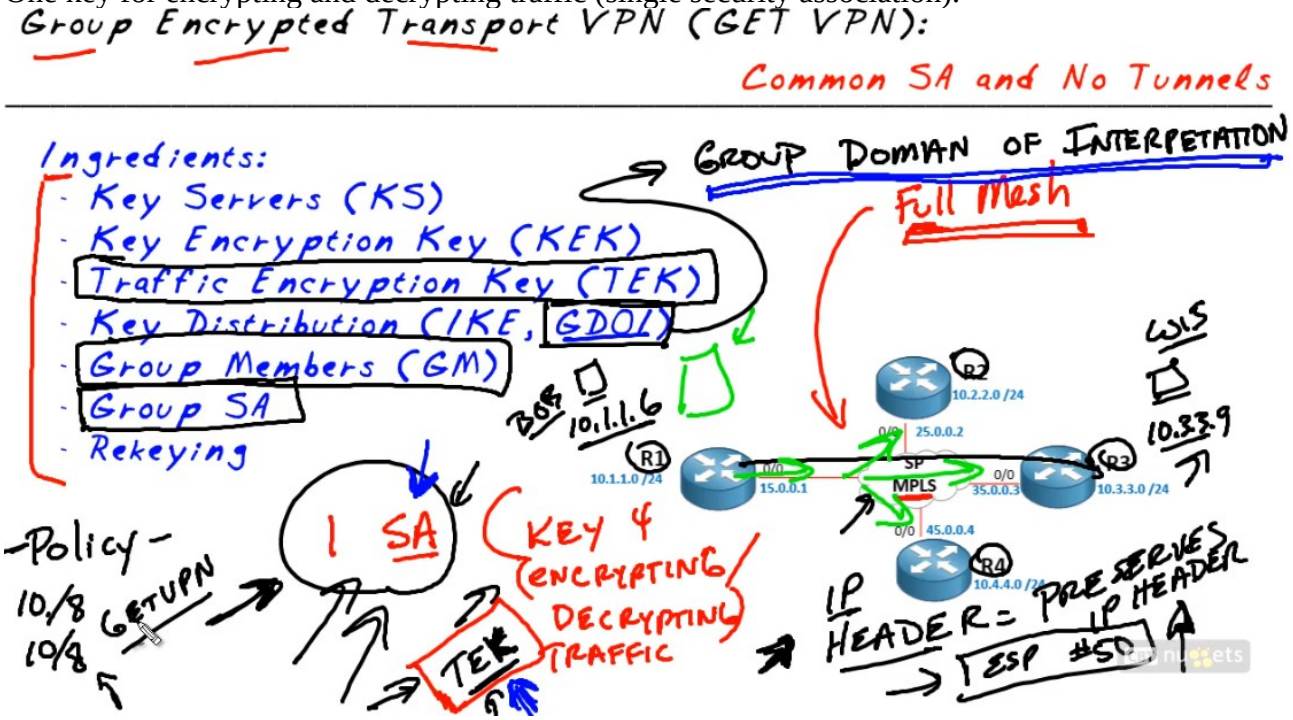
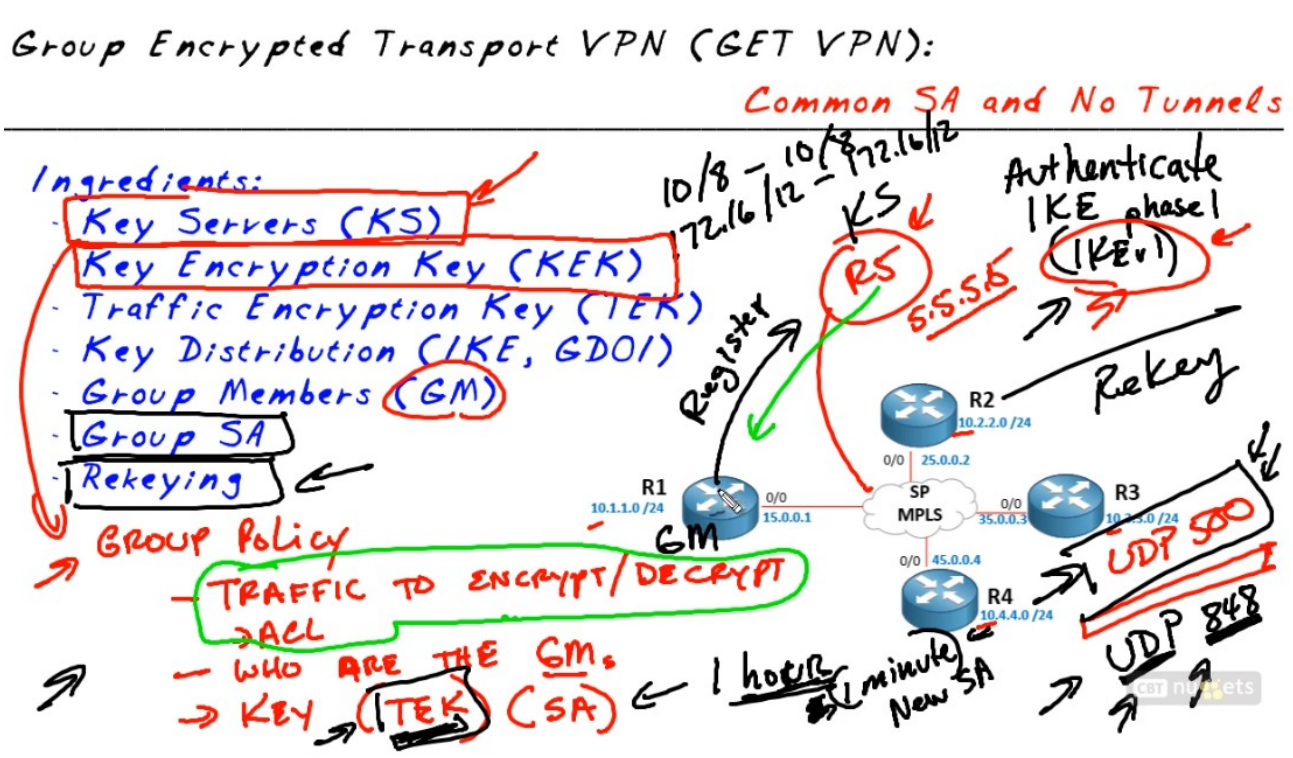
GET VPN (Group Encrypted VPN):

Used usually for full mesh MPLS networks to avoid delays noticed in DMVPN and also to avoid Multicast related problems.

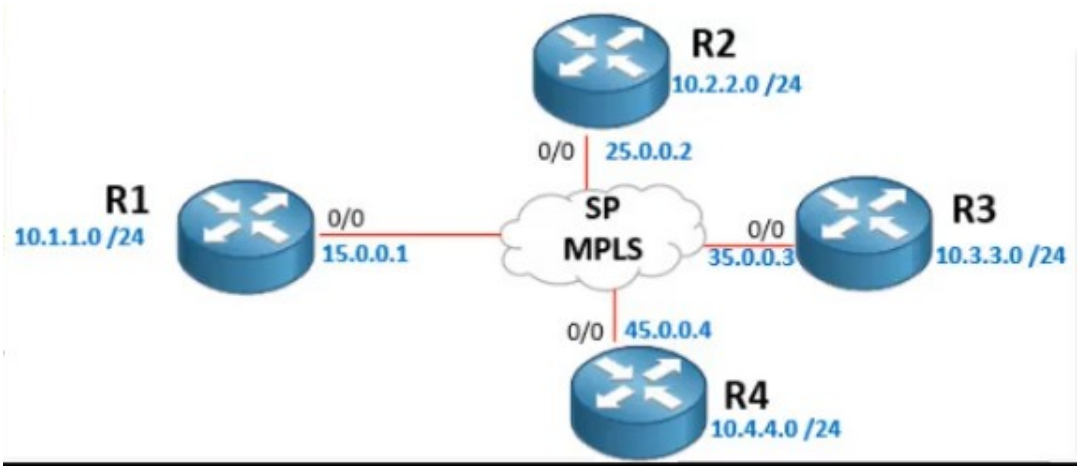
One key for encrypting and decrypting traffic (single security association).





KEK (between group server and the member)

TEK (to encrypt the traffic)



GETVPN:
No IPsec tunnels between group memebers, simply uses GDOI and common SA following the policy they received from the key server.

R5 (Key Server):
crypto isakmp policy 10
hash sha256
authentication pre-share
group 14
lifetime 180
encryption aes 256
exit

show crypto isakmp policy
crypto isakmp key cisco123 address 0.0.0.0
crypto key generate rsa general label GETVPN mod 1024 exportable

crypto ipsec trnasform-set Our-TSET esp-aes esp-sha-hmac
exit

crypto ipsec profile GDOI-Profile
set transform-set Our-TSE
set security-association lifetime seconds 300 (TEK)
exit

crypto gdoi group Our-GETVPN
identity number 6783
server local
address ipv4 5.5.5.5
rekey lifetime seconds 600 (KEK)
rekey retransmit 10 number 2
rekey authentication mypubkey rsa GETVPN
sa ipsec 1
profile GDOI-Profile
match address ipv4 101
replay time window-size 5 (time based anti-replay/TBAR)
exit
exit
exit

ip access-list exteded 101
permit ip 10.0.0.0 0.255.255.255. 10.0.0.0 0.255.255.255
exit

router ospf 1
network 0.0.0.0 255.255.255.255 area 0 (put all interface in area 0)
end

R1:
crypto isakmp policy 10
hash sha256
authentication pre-share
group 14
lifetime 180
encryption aes 256
exit

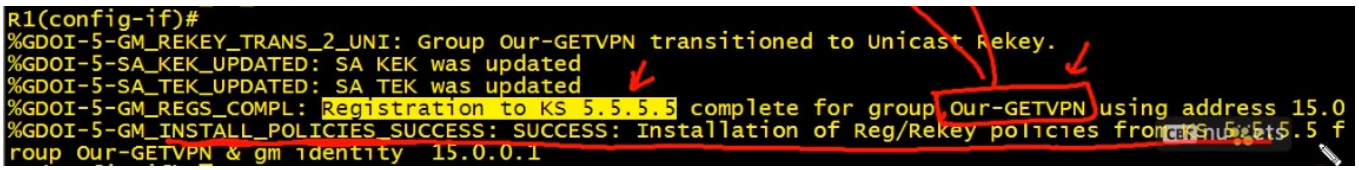
crypto isakmp key cisco123 address 0.0.0.0

crypto gdoi group Our-GETVPN
identity number 6783
server address ipv4 5.5.5.5
exit

crypto map GETVPN-MAP 10 gdoi
set group Our-GETVPN
exit
interface e0/0
crypto map GETVPN-MAP

ip tcp adjust-mss 1360
exit

router ospf 1
network 0.0.0.0 255.255.255.255 area 0
end



R2, R3 and R4 Group Memebers config is identical to R1.

Force a re-key:

```
R5-KS#crypto gdoi ks rekey replace-now

% There has not been a GDOI policy change for group Our-GETVPN, a rekey is not needed

Are you sure you want to proceed? [yes/no]:
% Please answer 'yes' or 'no'.
Are you sure you want to proceed? [yes/no]: yes
R5-KS#
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey with policy-replace now for group Our-GETVPN
 address 5.5.5.5 with seq # 1
R5-KS#
R5-KS#
```

```
R1#
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_RECV_REKEY: Received Rekey for group Our-GETVPN from 5.5.5.5 to 15.0.0.1 with seq # 1
%GDOI-4-GM_RECV_POLICY_REPLACE_NOW: GM received policy replace now rekey from KS in group Our-GETV
R1#
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies from 5.5.5.5 f
roup Our-GETVPN & gm identity  15.0.0.1
R1#
```

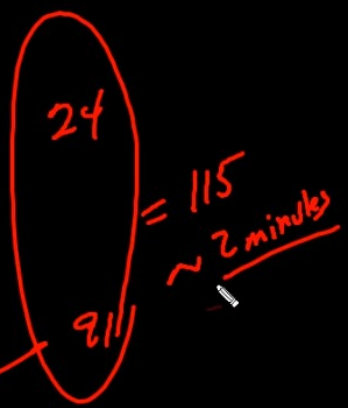
```
R5-KS#show crypto gdoi
GROUP INFORMATION

    Group Name                  : Our-GETVPN (Unicast)
    Group Identity              : 6783
    Crypto Path                 : ipv4
    Key Management Path         : ipv4
    Group Members               : 4
    IPSec SA Direction          : Both
    Group Rekey Lifetime        : 600 secs
    Group Rekey
        Remaining Lifetime      : 514 secs
        Time to Rekey           : 289 secs
    Rekey Retransmit Period     : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime      : 0 secs

      IPSec SA Number           : 1
      IPSec SA Rekey Lifetime: 300 secs
      Profile Name              : GDOI-Profile
      Replay method             : Time Based
      Replay Window Size        : 5
      Tagging method            : Disabled
      SA Rekey
         Remaining Lifetime     : 215 secs
        Time to Rekey           : 99 secs
      ACL Configured            : access-list 101

     Group Server list          : Local
```

KEK

TEK

```
R5-KS#show crypto gdoi ks policy
Key Server Policy:
For group Our-GETVPN (handle: 2147483650) server 5.5.5.5 (handle: 2147483650):

  # of teks : 2  Seq num : 0
  KEK POLICY (transport type : Unicast)
    spi : 0x36F4C764D96D1FCD4F36BFE92BE5D652
    management alg      : disabled    encrypt alg       : 3DES
    crypto iv length    : 8           key size          : 24
    orig life(sec): 600           remaining life(sec): 588
    time to rekey (sec): 363
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : GETVPN

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x6C19096A
    access-list        : 101
    transform          : esp-192-aes esp-sha-hmac
    alg key size       : 24            sig key size          : 20
    orig life(sec)     : 300           remaining life(sec)   : 104
    tek life(sec)      : 300           elapsed time(sec)     : 196
    override life (sec): 0             antireplay window size: 5
    time to rekey (sec): n/a


  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xC8216A8E
    access-list        : 101
    transform          : esp-192-aes esp-sha-hmac
```

```
    spi : 0x36F4C764D96D1FCD4F36BFE92BE5D652
    management alg      : disabled    encrypt alg       : 3DES
    crypto iv length    : 8           key size          : 24
    orig life(sec): 600           remaining life(sec): 323
    time to rekey (sec): 98
    sig hash algorithm : enabled     sig key length    : 162
    sig size           : 128
    sig key name       : GETVPN

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xC8216A8E
    access-list        : 101
    transform          : esp-192-aes esp-sha-hmac
    alg key size       : 24            sig key size          : 20
    orig life(sec)     : 300           remaining life(sec)   : 24
    tek life(sec)      : 300           elapsed time(sec)     : 276
    override life (sec): 0             antireplay window size: 5
    time to rekey (sec): n/a

  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x640E5471
    access-list        : 101
    transform          : esp-192-aes esp-sha-hmac
    alg key size       : 24            sig key size          : 20
    orig life(sec)     : 300           remaining life(sec)   : 209
    tek life(sec)      : 300           elapsed time(sec)     : 91
    override life (sec): 0             antireplay window size: 5
    time to rekey (sec): 93

Replay Value 4325.75 secs
```




```
R5-KS#show crypto gdoi ks acl
Group Name: Our-GETVPN
 Configured ACL:
   access-list 101  permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
```

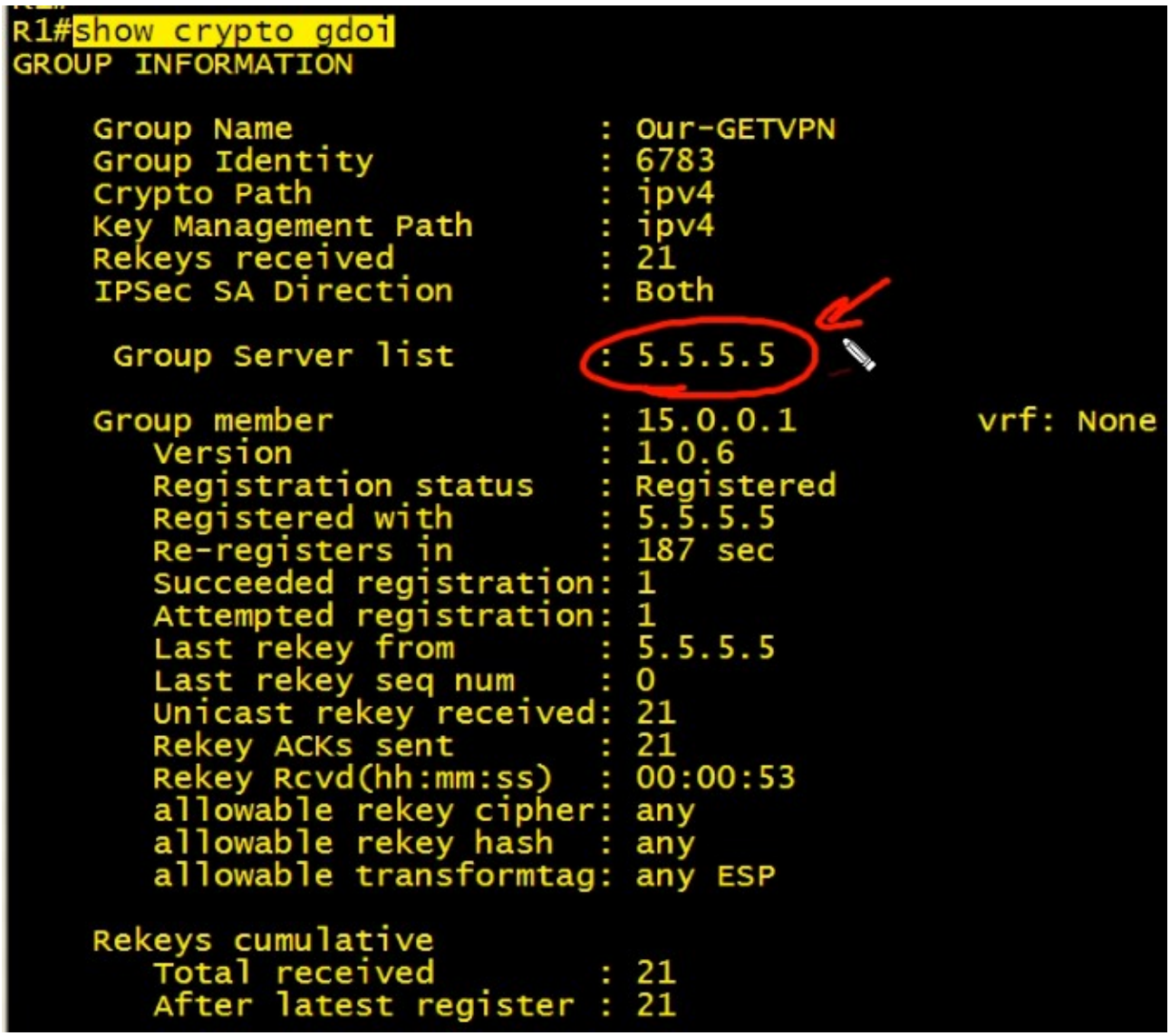
```
R5-KS#show crypto gdoi ks rekey
Group Our-GETVPN (Unicast)
    Number of Rekeys sent                  : 17
    Number of Rekeys retransmitted         : 0
    KEK rekey lifetime (sec)               : 600
        Remaining lifetime (sec)           : 419
        Remaining time until rekey (sec): 194
    Retransmit period                      : 10
        Number of retransmissions          : 2
        Time until next retransmit (sec): n/a
    IPSec SA 1 lifetime (sec)              : 300
        Remaining lifetime (sec)           : 120
        Remaining time until rekey (sec): 4
```

```
R5-KS#show crypto gdoi ks member

Group Member Information :

Number of rekeys sent for group Our-GETVPN : 18

Group Member ID     : 15.0.0.1     GM Version: 1.0.6
 Group ID           : 6783
 Group Name         : Our-GETVPN
 Key Server ID      : 5.5.5.5
 Rekeys sent        : 18
 Rekeys retries     : 0
 Rekey Acks Rcvd    : 18
 Rekey Acks missed  : 0

 Sent seq num : 2       1       2       1
Rcvd seq num :  2       1       2       1

Group Member ID     : 25.0.0.2     GM Version: 1.0.6
 Group ID           : 6783
 Group Name         : Our-GETVPN
 Key Server ID      : 5.5.5.5
 Rekeys sent        : 17
 Rekeys retries     : 0
 --More--
```

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
15.0.0.1        5.5.5.5         GDOI_REKEY        1012 ACTIVE
15.0.0.1        5.5.5.5         GDOI_REKEY        1013 ACTIVE

IPv6 Crypto ISAKMP SA
```

```
R1#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.

1012  15.0.0.1        5.5.5.5                ACTIVE 3des sha     rsig 0  0
      Engine-id:Conn-id =  SW:12

1013  15.0.0.1        5.5.5.5                ACTIVE 3des sha     rsig 0  0
      Engine-id:Conn-id =  SW:13

IPv6 Crypto ISAKMP SA
```

```
R1#show crypto session
Crypto session current status

Interface: Ethernet0/0
Session status: UP-ACTIVE
Peer: 0.0.0.0 port 848
  IKEv1 SA: local 15.0.0.1/848 remote 5.5.5.5/848 Active
  IKEv1 SA: local 15.0.0.1/848 remote 5.5.5.5/848 Active
  IPSEC FLOW: permit ip 10.0.0.0/255.0.0.0 10.0.0.0/255.0.0.0
        Active SAs: 4, origin: crypto map
```


R1#show crypto gdoi
GROUP INFORMATION
Group Name : Our-GETVPN
Group Identity : 6783
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 21
IPSec SA Direction : Both
Group Server list : 5.5.5.5
Group member : 15.0.0.1 vrf: None
Version : 1.0.6
Registration status : Registered
Registered with : 5.5.5.5
Re-registers in : 187 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 5.5.5.5
Last rekey seq num : 0
Unicast rekey received: 21
Rekey ACKs sent : 21
Rekey Rcvd(hh:mm:ss) : 00:00:53
allowable rekey cipher: any
allowable rekey hash : any
allowable transformtag: any ESP
Rekeys cumulative
Total received : 21
After latest register : 21

```
 ACL Downloaded From KS 5.5.5.5:
   access-list   permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255

KEK POLICY:
    Rekey Transport Type      : Unicast
    Lifetime (secs)           : 545
    Encrypt Algorithm         : 3DES
    Key Size                  : 192
    Sig Hash Algorithm        : HMAC_AUTH_SHA
    Sig Key Length (bits)     : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet0/0:
    IPsec SA:
        spi: 0x62E1A0DA(1658953946)
        transform: esp-192-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (62)
        Anti-Replay(Time Based) : 5 sec interval
        tag method : disabled
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL

        spi: 0xA905CF2D(2835730221)
        transform: esp-192-aes esp-sha-hmac
        sa timing:remaining key lifetime (sec): (247)
        Anti-Replay(Time Based) : 5 sec interval
        tag method : disabled
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL
```

```
R1#show crypto gdoi gm rekey
Group Our-GETVPN (Unicast)
    Number of Rekeys received (cumulative)       : 23
    Number of Rekeys received after registration : 23
    Number of Rekey Acks sent                    : 23


R1#
R1#
R1#show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
   53  IPsec   AES192+SHA               0        0        0 15.0.0.1
   54  IPsec   AES192+SHA               0        0        0 15.0.0.1
   55  IPsec   AES192+SHA               0        0        0 15.0.0.1
   56  IPsec   AES192+SHA               0        0        0 15.0.0.1
 1014  IKE     SHA+3DES                 0        0        0
 1015  IKE     SHA+3DES                 0        0        0
```

```
R1#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: GETVPN-MAP, local addr 15.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.0/255.0.0.0/0/0)
   Group: Our-GETVPN
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #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.: 15.0.0.1, remote crypto endpt.: 0.0.0.0
     plaintext mtu 1426, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x20AA01B1(548012465)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x20AA01B1(548012465)
        transform: esp-192-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 55, flow_id: SW:55, sibling_flags 80000040, crypto map: GETVPN-MAP
        sa timing: remaining key lifetime (sec): 153
        Kilobyte Volume Rekey has been disabled
        IV size: 16 bytes
```

```
    current outbound spi: 0x20AA01B1(548012465)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x20AA01B1(548012465)
       transform: esp-192-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 55, flow_id: SW:55, sibling_flags 80000040, crypto map: GETVPN-MAP
       sa timing: remaining key lifetime (sec): 153
       Kilobyte Volume Rekey has been disabled
       IV size: 16 bytes
       replay detection support: Y  replay window size: 5
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x20AA01B1(548012465)
       transform: esp-192-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 56, flow_id: SW:56, sibling_flags 80000040, crypto map: GETVPN-MAP
       sa timing: remaining key lifetime (sec): 153
       Kilobyte Volume Rekey has been disabled
       IV size: 16 bytes
       replay detection support: Y  replay window size: 5
       Status: ACTIVE(ACTIVE)

    outbound ah sas:

    outbound pcp sas:
```

A → TEK ⇄

B → TEK ⇄

```
R1#ping 10.2.2.2 source 10.1.1.1 repeat 123
Type escape sequence to abort.
Sending 123, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (123/123), round-trip min/avg/max = 12/16/34 ms
R1#
R1#show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
   57  IPsec   AES192+SHA                0      123        0 15.0.0.1
   58  IPsec   AES192+SHA              123        0        0 15.0.0.1
   59  IPsec   AES192+SHA                0        0        0 15.0.0.1
   60  IPsec   AES192+SHA                0        0        0 15.0.0.1
 1015  IKE     SHA+3DES                  0        0        0
 1016  IKE     SHA+3DES                  0        0        0
```

```
R1#
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_RECV_REKEY: Received Rekey for group Our-GETVPN from 5.5.5.5 to 15.0.0.1 with seq # 1
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies from KS 5.5.5.5 f
roup Our-GETVPN & gm identity  15.0.0.1
R1#show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt LastSeqN IP-Address
   59  IPsec   AES192+SHA                0        0        0 15.0.0.1
   60  IPsec   AES192+SHA                0        0        0 15.0.0.1
   61  IPsec   AES192+SHA                0        0        0 15.0.0.1
   62  IPsec   AES192+SHA                0        0        0 15.0.0.1
 1015  IKE     SHA+3DES                  0        0        0
 1016  IKE     SHA+3DES                  0        0        0
```