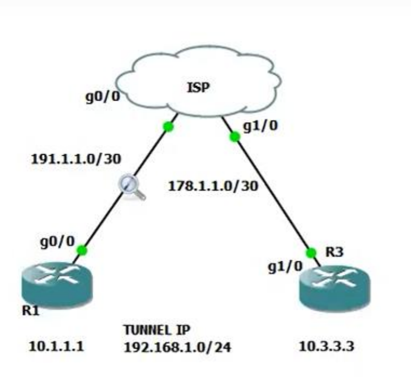
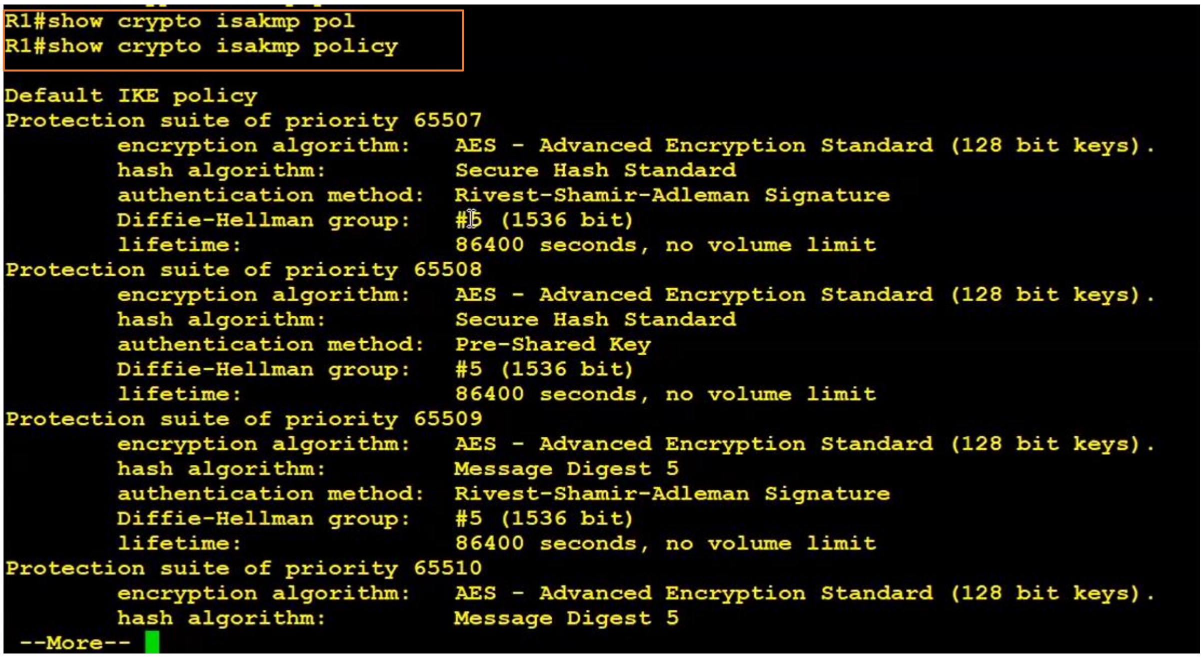
Advance Class-4



**config the basic-ip on the R1, R2 and isp and Loopback address on the R1 and R3 && ## config the default route for the ISP.
**config the tunnel with the tunnel-ip and along with ## Routing for the R1 and R3 to access each other.

#R1

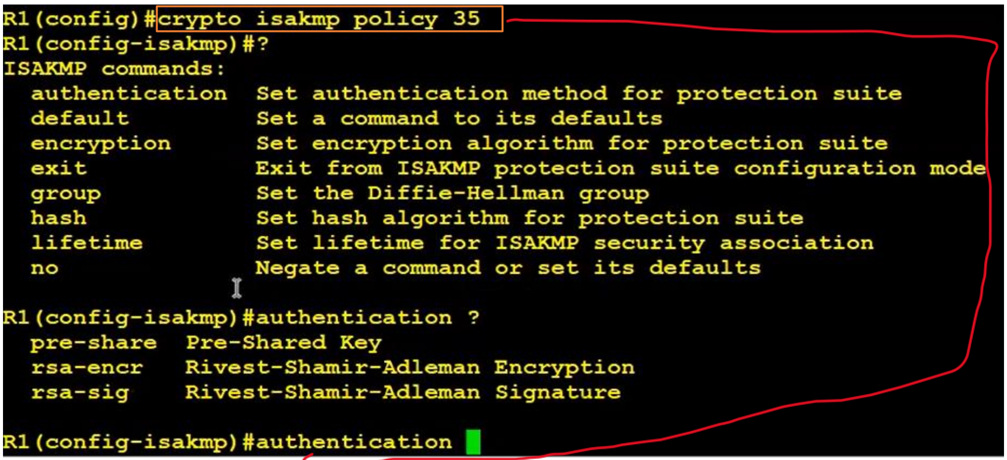


```
R1#show crypto isakmp pol
R1#show crypto isakmp policy

Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
 --More--
```

** to verify wt all default functions supported by Phase-1 mechanism of router.

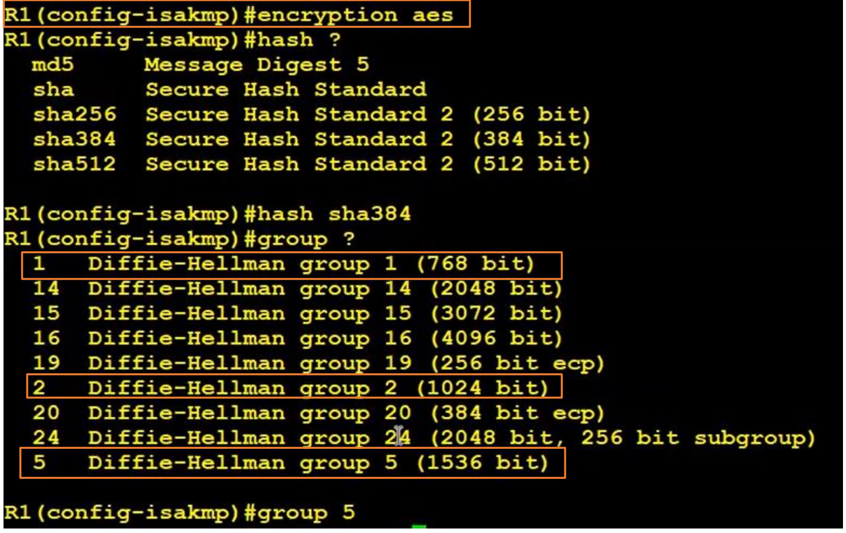
###Config IPSEC over GRE Tunnel

#R1



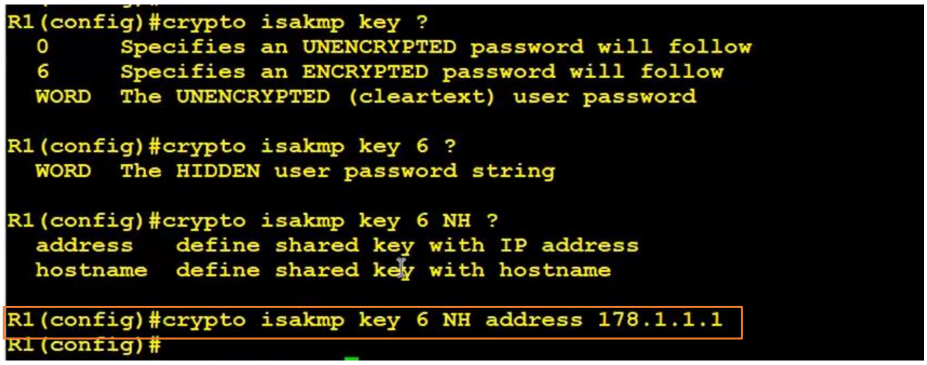
```
R1(config)#crypto isakmp policy 35
R1(config-isakmp)#?
ISAKMP commands:
  authentication   Set authentication method for protection suite
  default          Set a command to its defaults
  encryption       Set encryption algorithm for protection suite
  exit             Exit from ISAKMP protection suite configuration mode
  group            Set the Diffie-Hellman group
  hash             Set hash algorithm for protection suite
  lifetime         Set lifetime for ISAKMP security association
  no               Negate a command or set its defaults

R1(config-isakmp)#authentication ?
  pre-share   Pre-Shared Key
  rsa-encr    Rivest-Shamir-Adleman Encryption
  rsa-sig     Rivest-Shamir-Adleman Signature

R1(config-isakmp)#authentication
```

** higher the value of priority we get more preference



```
R1(config-isakmp)#encryption aes
R1(config-isakmp)#hash ?
  md5      Message Digest 5
  sha      Secure Hash Standard
  sha256   Secure Hash Standard 2 (256 bit)
  sha384   Secure Hash Standard 2 (384 bit)
  sha512   Secure Hash Standard 2 (512 bit)

R1(config-isakmp)#hash sha384
R1(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)
  24  Diffie-Hellman group 24 (2048 bit, 256 bit subgroup)
  5   Diffie-Hellman group 5 (1536 bit)

R1(config-isakmp)#group 5
```

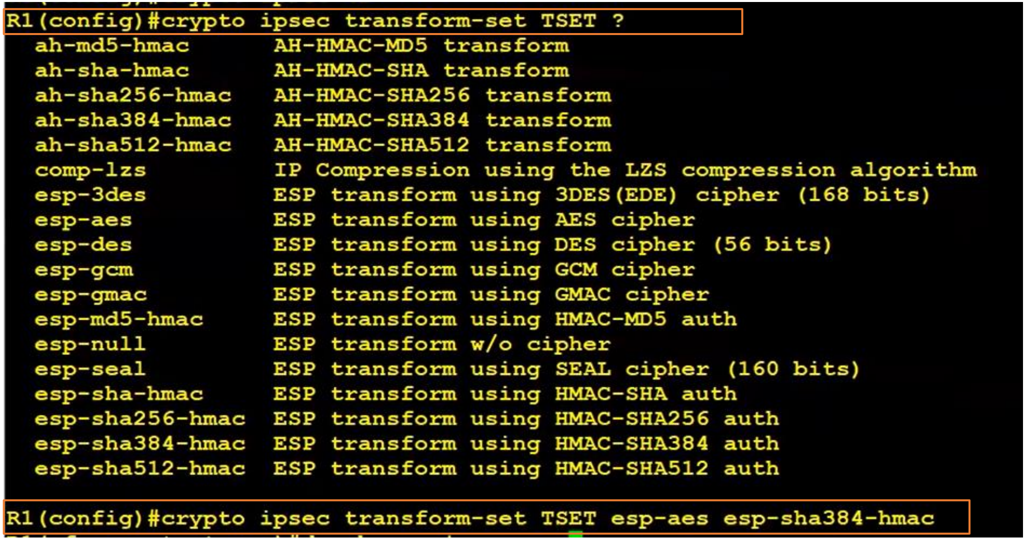
** group 1,2,5 are using for the Router and Others for Firewall



```
R1(config)#crypto isakmp key ?
  0      Specifies an UNENCRYPTED password will follow
  6      Specifies an ENCRYPTED password will follow
  WORD   The UNENCRYPTED (cleartext) user password

R1(config)#crypto isakmp key 6 ?
  WORD   The HIDDEN user password string

R1(config)#crypto isakmp key 6 NH ?
  address    define shared key with IP address
  hostname   define shared key with hostname

R1(config)#crypto isakmp key 6 NH address 178.1.1.1
R1(config)#
```

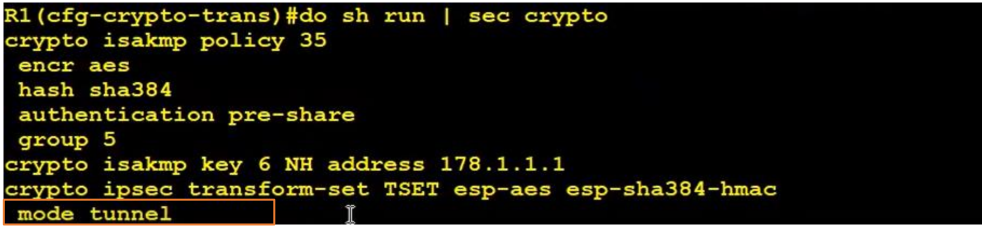
**address= Config the public-ip address of the next-hop router

** config the Crypto isakmp key



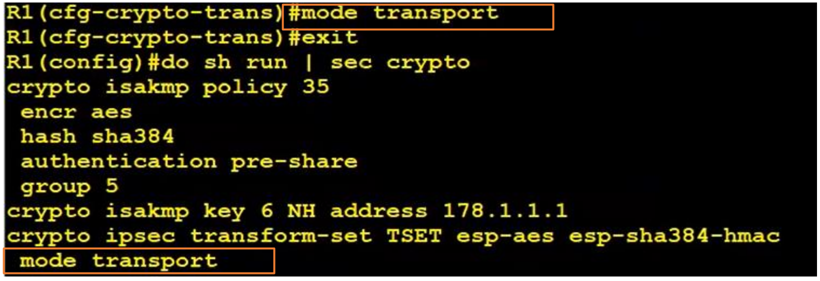
```
R1(config)#crypto ipsec transform-set TSET ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth

R1(config)#crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
```

** we have specify based on aes,hash and Group.



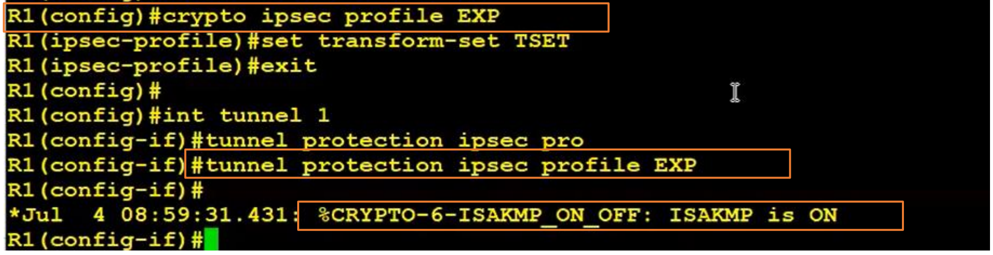
```
R1(cfg-crypto-trans)#do sh run | sec crypto
crypto isakmp policy 35
 encr aes
 hash sha384
 authentication pre-share
 group 5
crypto isakmp key 6 NH address 178.1.1.1
crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
 mode tunnel
```

** we r having a tunnel-mode



```
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
R1(config)#do sh run | sec crypto
crypto isakmp policy 35
 encr aes
 hash sha384
 authentication pre-share
 group 5
crypto isakmp key 6 NH address 178.1.1.1
crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
 mode transport
```

** change mode to Transport



```
R1(config)#crypto ipsec profile EXP
R1(ipsec-profile)#set transform-set TSET
R1(ipsec-profile)#exit
R1(config)#
R1(config)#int tunnel 1
R1(config-if)#tunnel protection ipsec pro
R1(config-if)#tunnel protection ipsec profile EXP
R1(config-if)#
*Jul  4 08:59:31.431: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

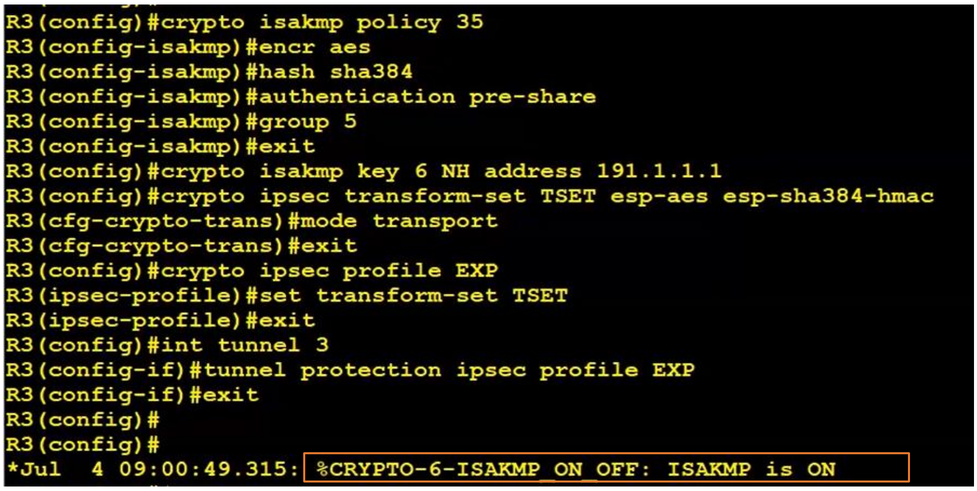
** create a ipsec-profile

** apply on the tunnel.

#R3

```
crypto isakmp policy 35
encr aes
hash sha384
authentication pre-share
group 5
exit
crypto isakmp key 6 NH address 191.1.1.1
crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
mode transport
exit
crypto ipsec profile EXP
set transform-set TSET
exit
int tunnel 3
tunnel protection ipsec profile EXP
exit
```

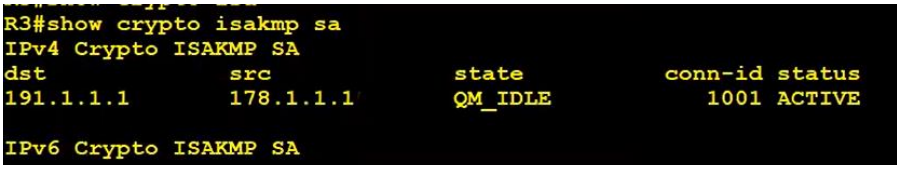
** same on the Router 3.



```
R3(config)#crypto isakmp policy 35
R3(config-isakmp)#encr aes
R3(config-isakmp)#hash sha384
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypto isakmp key 6 NH address 191.1.1.1
R3(config)#crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit
R3(config)#crypto ipsec profile EXP
R3(ipsec-profile)#set transform-set TSET
R3(ipsec-profile)#exit
R3(config)#int tunnel 3
R3(config-if)#tunnel protection ipsec profile EXP
R3(config-if)#exit
R3(config)#
R3(config)#
*Jul  4 09:00:49.315: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

To-verify

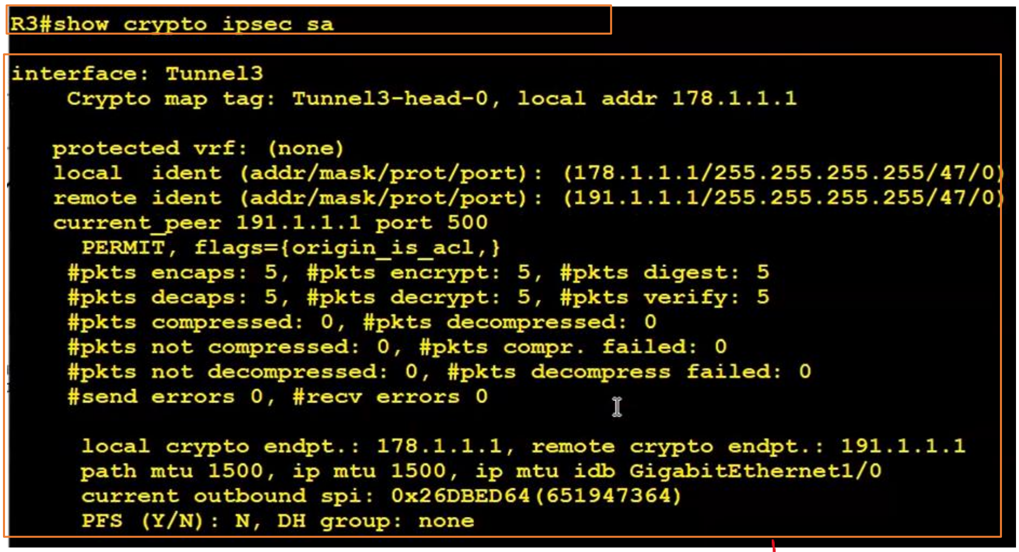
##1



```
R3#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
191.1.1.1       178.1.1.1       QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

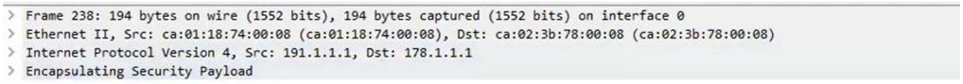
**se=security-association

##2



```
R3#show crypto ipsec sa

interface: Tunnel3
    Crypto map tag: Tunnel3-head-0, local addr 178.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (178.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (191.1.1.1/255.255.255.255/47/0)
   current_peer 191.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
    #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.: 178.1.1.1, remote crypto endpt.: 191.1.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1/0
     current outbound spi: 0x26DBED64(651947364)
     PFS (Y/N): N, DH group: none
```

**if any hacker is tried to hack will we get from this

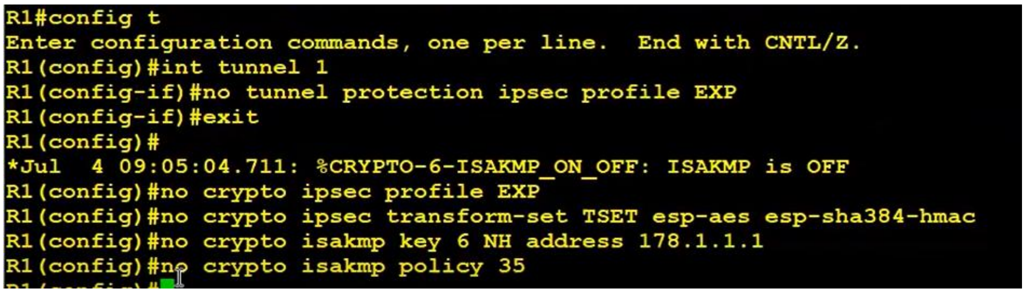


```
> Frame 238: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface 0
> Ethernet II, Src: ca:01:18:74:00:08 (ca:01:18:74:00:08), Dst: ca:02:3b:78:00:08 (ca:02:3b:78:00:08)
> Internet Protocol Version 4, Src: 191.1.1.1, Dst: 178.1.1.1
> Encapsulating Security Payload
```

** In IP-SEC we have 2 Header ➔ 1= ip header for public ip
2= ESP header for Public ip

This is Router-Based-VPN

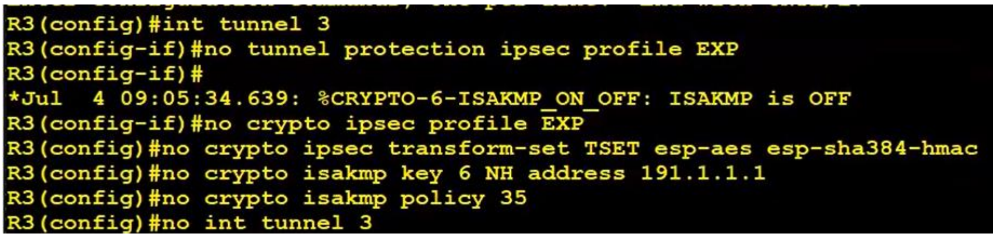
#R1



```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int tunnel 1
R1(config-if)#no tunnel protection ipsec profile EXP
R1(config-if)#exit
R1(config)#
*Jul  4 09:05:04.711: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R1(config)#no crypto ipsec profile EXP
R1(config)#no crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
R1(config)#no crypto isakmp key 6 NH address 178.1.1.1
R1(config)#no crypto isakmp policy 35
```

** remove all the commands from #R1

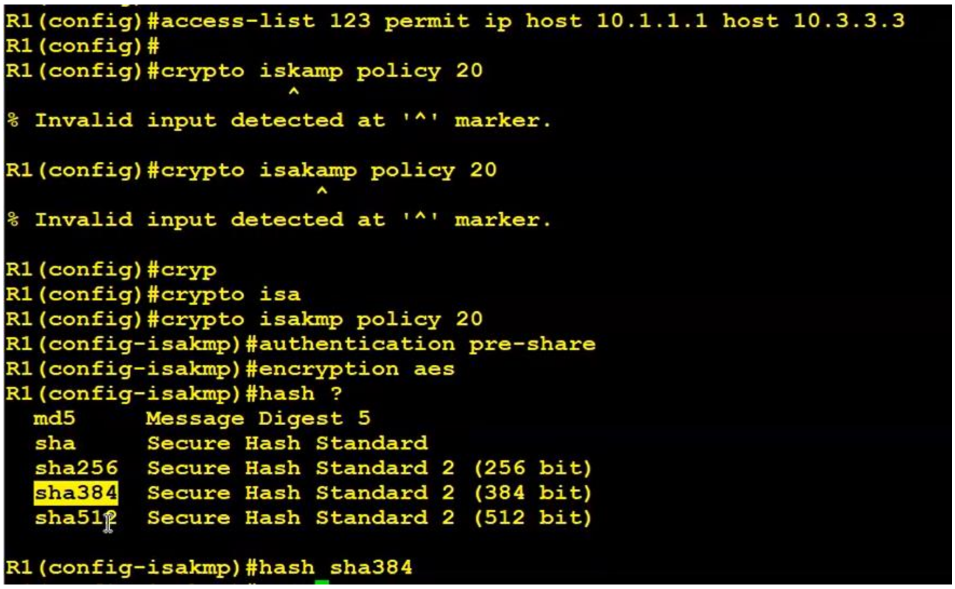
#R3



```
R3(config)#int tunnel 3
R3(config-if)#no tunnel protection ipsec profile EXP
R3(config-if)#
*Jul  4 09:05:34.639: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R3(config-if)#no crypto ipsec profile EXP
R3(config)#no crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
R3(config)#no crypto isakmp key 6 NH address 191.1.1.1
R3(config)#no crypto isakmp policy 35
R3(config)#no int tunnel 3
```

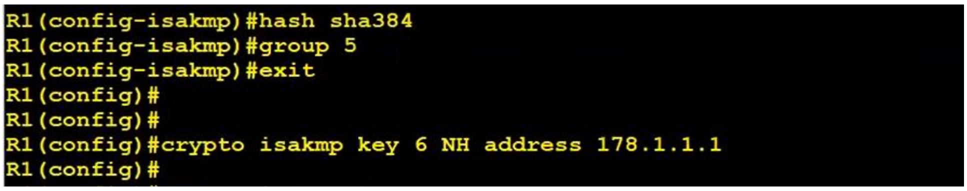
IP-SEC Tunnel
Policy-based-vpn

#R1

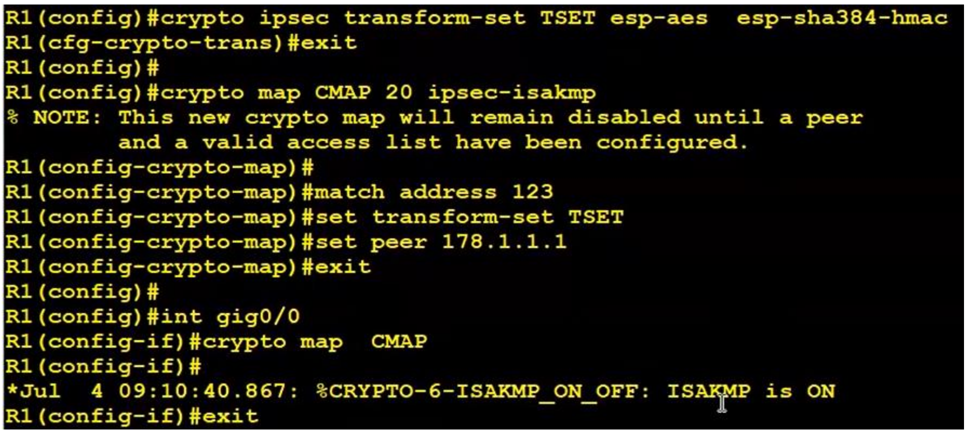


```
R1(config)#access-list 123 permit ip host 10.1.1.1 host 10.3.3.3
R1(config)#
R1(config)#crypto iskamp policy 20
                        ^
% Invalid input detected at '^' marker.

R1(config)#crypto isakamp policy 20
                          ^
% Invalid input detected at '^' marker.

R1(config)#cryp
R1(config)#crypto isa
R1(config)#crypto isakmp policy 20
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes
R1(config-isakmp)#hash ?
  md5     Message Digest 5
  sha     Secure Hash Standard
  sha256  Secure Hash Standard 2 (256 bit)
  sha384  Secure Hash Standard 2 (384 bit)
  sha512  Secure Hash Standard 2 (512 bit)

R1(config-isakmp)#hash sha384
```

** create a ACL

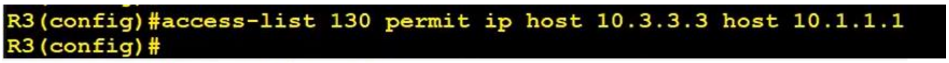


```
R1(config-isakmp)#hash sha384
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#
R1(config)#
R1(config)#crypto isakmp key 6 NH address 178.1.1.1
R1(config)#
```

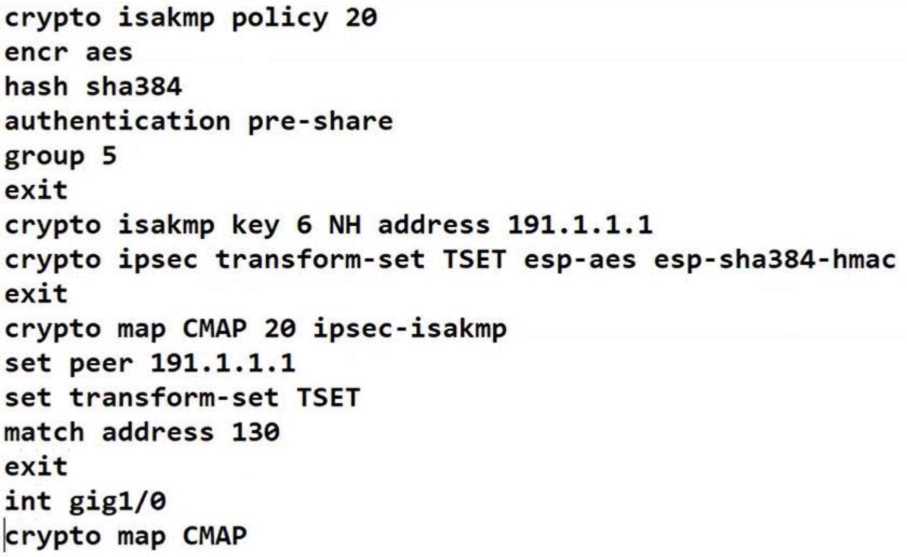


```
R1(config)#crypto ipsec transform-set TSET esp-aes  esp-sha384-hmac
R1(cfg-crypto-trans)#exit
R1(config)#
R1(config)#crypto map CMAP 20 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#
R1(config-crypto-map)#match address 123
R1(config-crypto-map)#set transform-set TSET
R1(config-crypto-map)#set peer 178.1.1.1
R1(config-crypto-map)#exit
R1(config)#
R1(config)#int gig0/0
R1(config-if)#crypto map  CMAP
R1(config-if)#
*Jul  4 09:10:40.867: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
```

#R3



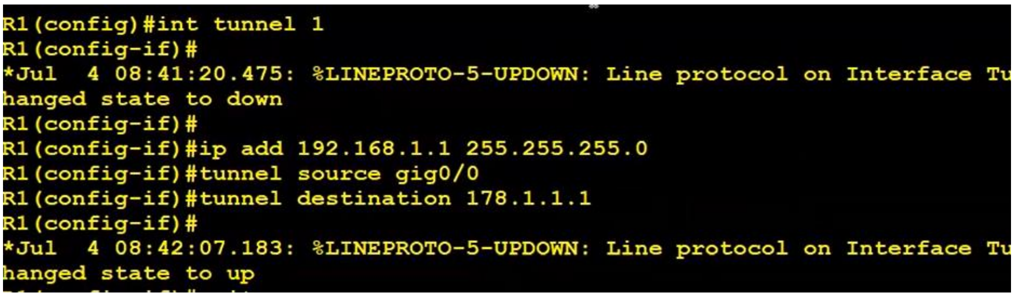
```
R3(config)#access-list 130 permit ip host 10.3.3.3 host 10.1.1.1
R3(config)#
```



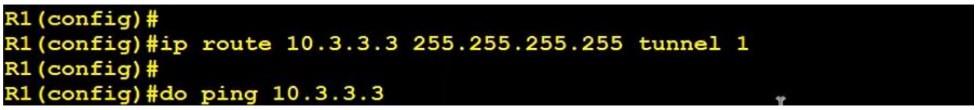
```
crypto isakmp policy 20
encr aes
hash sha384
authentication pre-share
group 5
exit
crypto isakmp key 6 NH address 191.1.1.1
crypto ipsec transform-set TSET esp-aes esp-sha384-hmac
exit
crypto map CMAP 20 ipsec-isakmp
set peer 191.1.1.1
set transform-set TSET
match address 130
exit
int gig1/0
crypto map CMAP
```

##Tunnel

#R1

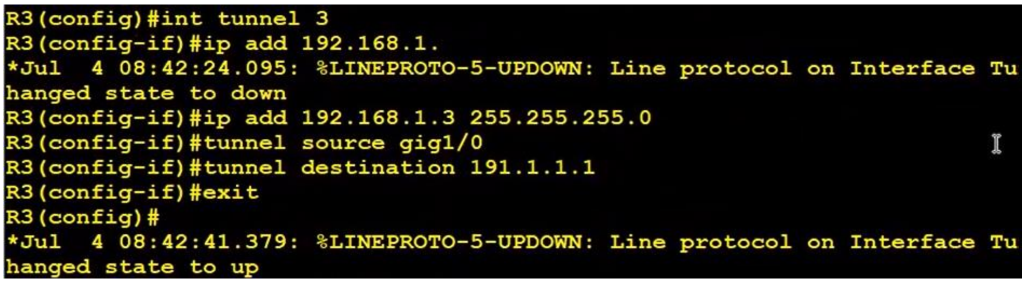


```
R1(config)#int tunnel 1
R1(config-if)#
*Jul  4 08:41:20.475: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tu
hanged state to down
R1(config-if)#
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#tunnel source gig0/0
R1(config-if)#tunnel destination 178.1.1.1
R1(config-if)#
*Jul  4 08:42:07.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tu
hanged state to up
```

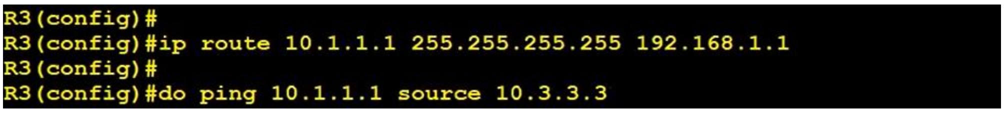


```
R1(config)#
R1(config)#ip route 10.3.3.3 255.255.255.255 tunnel 1
R1(config)#
R1(config)#do ping 10.3.3.3
```

#R3



```
R3(config)#int tunnel 3
R3(config-if)#ip add 192.168.1.
*Jul  4 08:42:24.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tu
hanged state to down
R3(config-if)#ip add 192.168.1.3 255.255.255.0
R3(config-if)#tunnel source gig1/0
R3(config-if)#tunnel destination 191.1.1.1
R3(config-if)#exit
R3(config)#
*Jul  4 08:42:41.379: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tu
hanged state to up
```



```
R3(config)#
R3(config)#ip route 10.1.1.1 255.255.255.255 192.168.1.1
R3(config)#
R3(config)#do ping 10.1.1.1 source 10.3.3.3
```