[Date]

Tunnel VPN IPsec site-à-site

Cisco

Mamadou Camara
BTS SIO

Table des matières

Présentation *1*

Objectif **2**

Activation du module securityk9 ..... **3**

Adressage IP *4*

Routage OSPF *5*

Mise en place du VPN **6**

Configuration 1ère Routeur R-Limoges **6.1**

Phase 1 ..... **a**

Phase 2 ..... **b**

Configuration 2ème Routeur R-Bordeaux **6.2**

Phase 1 ..... **a**

Phase 2 ..... **b**

Configuration 3ère Routeur R-Toulouse **6.3**

Phase 1 ..... **a**

Phase 2 ..... **b**

Test **7**

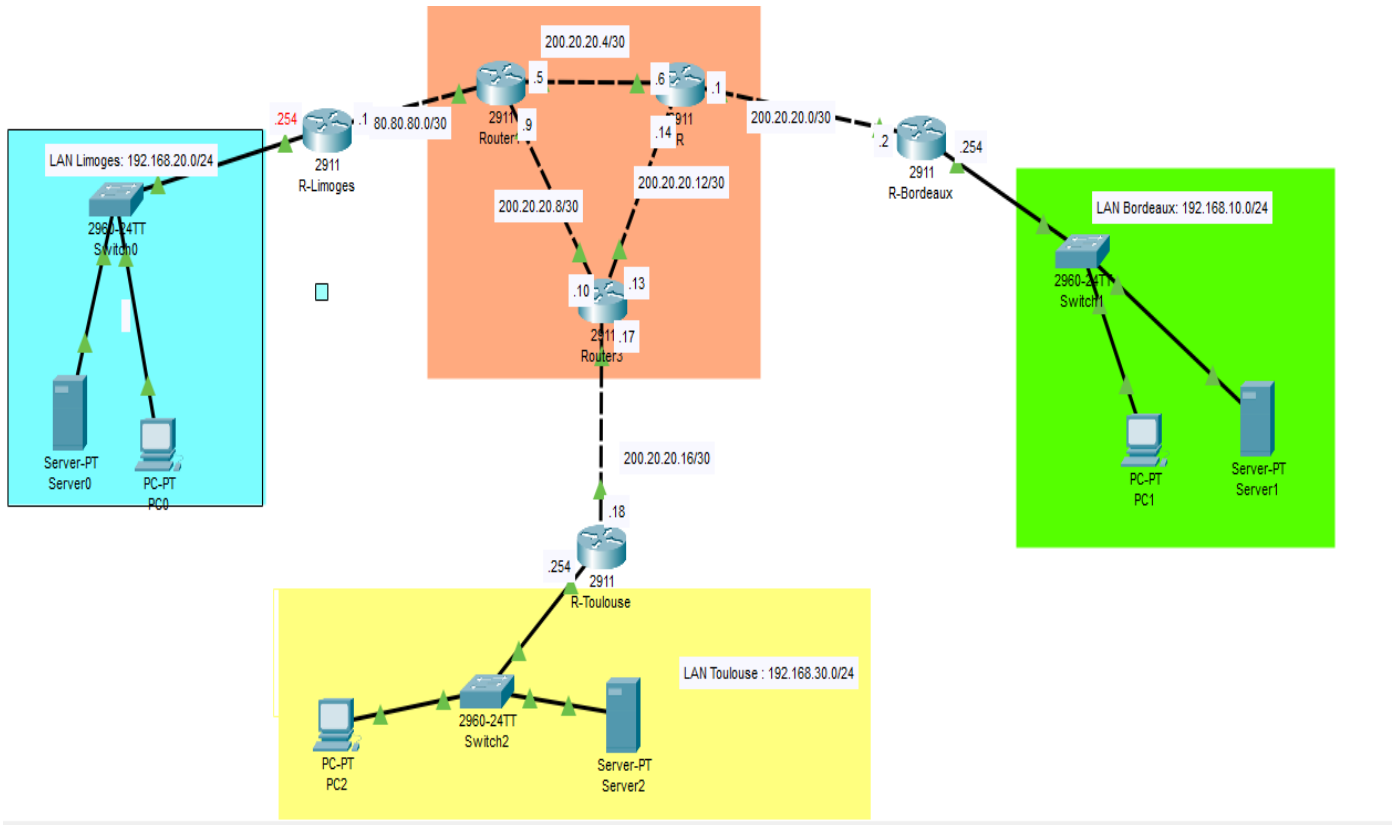
Diagnostique VPN **8**

1. Présentation :

La mise en place d'un tunnel **IPSec** est une solution sécurisée pour interconnecter les différents sites d'une entreprise au travers d'un réseau non sécurisé comme **Internet**. Elle permet en effet d'échanger des données entre sites de manière sécurisée en mettant en œuvre les mécanismes **d'authentification**, de **chiffrement**, et **d'intégrité**.

IPSec utilise le chiffrement **asymétrique** et **symétrique** pour assurer la rapidité et la sécurité du transfert des données. Dans le cas du chiffrement asymétrique, la clé de chiffrement est rendue publique tandis que la clé de déchiffrement reste privée. IPSec établit une connexion sécurisée avec un chiffrement asymétrique et passe au chiffrement symétrique pour accélérer le transfert des données.

Maquette de l'atelier :



LAN Limoges : 192.168.20.0/24

LAN Bordeaux : 192.168.10.0/24

LAN Toulouse : 192.168.30.0/24

2. Objectif :

L'objectif est de mettre en place un **tunnel VPN IPsec** reliant les routeurs R-Limoges, R-Toulouse et R-Bordeaux afin de **sécuriser** le trafic transitant entre les réseaux 192.168.20.0/24, 192.168.10.0/24 et 192.168.30.0/24.

3. Activation du module « securityk9 »

Sous Packet tracer, il faut dans un premier temps activer le module de sécurité **securityk9** sur les routeurs 2911 de Limoges, Bordeaux et de Toulouse:

- Exécutez la commande ***show version*** pour vérifier que la licence du pack sécurité n'est pas activée.
- Activez le module **securityk9** avec la commande suivante :

```
R(config)#license boot module c2900 technology-package securityk9
```

- Sauvegarder la configuration puis, redémarrer le routeur :

```
R# copy run start
R# reload
```

- Vérifier l'activation du pack **securityk9** :

```
# show version
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#    PID                 SN
-------------------------------------------------
*0         CISCO2911/K9        FTX1524240A-


Technology Package License Information for Module:'c2900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            disable       None          None
data          disable       None          None

Configuration register is 0x2102


Router#
```

4. Adressage IP

Réaliser l'adressage des PC et des interfaces des routeurs.

Exemple : sur les interfaces du routeur R-Limoges

```
Conf t
R-Limoges(config)#Interface gi0/0
R-Limoges(config-interface)#Ip address 192.168.20.254  255.255.255.0
R-Limoges(config-interface)#no shudown
Exi
Interface gi0/1
R-Limoges(config)#Ip address 80.80.80.1  255.255.255.252
R-Limoges(config-interface)#no shudown
exite
```

5. Routage dynamique OSPF

- Configurer le routage dynamique sur les routeurs.
  Par exemple, sur le routeur R-Limoges :

  ```
  conf t
  Router ospf 1
  network 192.168.20.0  0.0.0.255 area 0
  network 80.80.80.0  0.0.0.3 area 0
  ```

  En effet, ces deux réseaux sont reliés aux routeur R-Limoges. On fait pareil pour les autres
- Vérifier la connectivité entre les différents réseaux.

6. Mise en place du VPN

L'objectif est de mettre en place un **tunnel VPN IPsec** reliant les routeurs R-Limoges, R-Bordeaux et R-Toulouse afin de **sécuriser** le trafic transitant entre les réseaux 192.168.20.0/24, 192.168.30.0/24 et 192.168.10.0/24.

La configuration du **tunnel VPN IPsec** sur les routeurs Limoges, Toulouse et Bordeaux, consiste à définir les paramètres des 2 phases suivantes :

6.1 Configuration du 1ère routeur : R-Limoges

a. Phase 1 :

Pendant cette phase, les deux routeurs négocient les conditions requises pour établir une connexion sécurisée. Elle inclut un accord mutuel sur les paramètres de chiffrement, d'authentification et d'autres associations de sécurité (AS).

A faire sur le routeur R-Limoges:

- Stratégie ISAKMP numérotée 10 :

```
R-Limoges(config)#crypto isakmp policy 10
```

- Chiffrement : AES

```
R-Limoges(config-isakmp)#encryption aes
```

- Authentification par clé pré-partagée ;
- Groupe Diffie-Hellman : 5 ;
- Renégociation : toutes les 15 minutes ;

```
R-Limoges(config-isakmp)#authentication pre-share
R-Limoges(config-isakmp)#group 5
R-Limoges(config-isakmp)#lifetime 900
R-Limoges(config-isakmp)#exit
```

- Définition de la clé pré-partagée « cisco1234 » et l'adresse du routeur homologue :

```
R-Limoges(config)#crypto isakmp key cisco1234 address @ip-R-Bordeaux
```

R-Limoges(config)#crypto isakmp **key cisco1234** address **@ip-R-Toulouse**

Explications :

@ip-R-Bordeaux : 200.20.20.2 (l''interface externe du routeur R-Bordeaux)

@ip-R-Toulouse : 200.20.20.18 (l'interface externe du routeur R-Toulouse)

Ces premières commandes permettent la définition d'une **stratégie IKE** (Internet Key Exchange) portant le n° 10. Cette stratégie utilise le protocole de chiffrement AES (Advanced Encryption standard), une méthode d'authentification basée sur une clé pré-partagée

spécifiée, un échange de clé Diffie-Hellman de groupe 5 et une renégociation toutes les 15 minutes (soit 900 secondes). Il s'agit de la phase 1.

Les deux routeurs VPN devront avoir une **stratégie IKE commune** et avoir **validé** entièrement **la phase 1** avant de pouvoir passer à l'étape suivante, c'est-à-dire la phase 2.

b. Phase 2 :

- IPsec SA (Security Association) numérotée **50** avec authentification AH/SHA et chiffrement ESP/3DES :

```
R-Limoges(config)#crypto ipsec transform-set 50 ah-sha-hmac esp-3des
```

- Crypto map : **MYMAP** associée à la stratégie IKE n° 10 et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes :

```
R-Limoges(config)# crypto map MYMAP 10 ipsec-isakmp
R-Limoges(config-crypto-map)#set peer @ip-R-Bordeaux
R-Limoges(config-crypto-map)#set security-association lifetime seconds
                              1800
R-Limoges(config-crypto-map)#set transform-set 50
R-Limoges(config-crypto-map)#match address 101
R-Limoges(config-crypto-map)#exit
```

- Crypto map : **MYMAP** associée à la stratégie IKE n° **20** et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes :

  R-Limoges(config)# crypto map **MYMAP 20** ipsec-isakmap
  R-Limoges(config-crypto-map)#set peer @**ip-R-Toulouse**
  R-Limoges(config-crypto-map)#set security-association lifetime seconds 1800
  R-Limoges(config-crypto-map)#set transform-set **50**
  R-Limoges(config-crypto-map)#set Match adress **102**
  R-Limoges(config-crypto-map)#exit

- Application de la crypto map à l'interface gig0/1 :

```
R-Limoges(config)#interface gig0/1
R-Limoges(config-if)#crypto map MYMAP
```

- Création de l'ACL n° **101** (192.168.20.0 /24 > 192.168.10.0 /24).

```
R-Limoges(config)#access-list 101 permit ip 192.168.20.0 0.0.0.255
192.168.10.0 0.0.0.255
```

- Création de l'ACL n° **102** (192.168.20.0 /24 > 192.168.30.0 /24).

R-Limoges(config)#access-list **102** permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255

Explications :

Les commandes ci-dessus indiquent les modifications (transformations) à appliquer aux paquets IP en termes de chiffrement et hachage (ESP-AES, AH-SHA-HMAC).

Elles permettent également de définir le routeur homologue, la durée de vie de l'association de sécurité, la stratégie de transformation à utiliser (ici 50), ainsi qu'une ACL (ici 101 et 102) pour définir quel trafic sera soumis au tunnel. Il s'agit de la phase 2.

Pour terminer, les paramètres du tunnel IPsec sont associés à **l'interface gig0/1.**

6.2 Configuration du 2ème routeur : R-Bordeaux

La configuration du routeur de Bordeaux est quasi identique à celle du routeur de Limoges (hormis bien sûr, **l'homologue** et **l'ACL** qui diffèrent).

Reprenez les mêmes :

A faire sur le routeur R-Bordeaux:

a. **Phase 1 :**

- Stratégie ISAKMP numérotée 10 :
  R-Bordeaux(config)#crypto isakmp policy 10
- Chiffrement : AES
  R-Bordeaux(config-isakmp)#encryption aes
- Authentification par clé pré-partagée ;
- Groupe Diffie-Hellman : 5 ;
- Renégociation : toutes les 15 minutes ;
  R-Bordeaux(config-isakmp)#authentification pre-share
  R-Bordeaux(config-isakmp)#group 5
  R-Bordeaux(config-isakmp)#lifetime 900
  R-Bordeaux(config-isakmp)#exit
- Définition de la clé pré-partagée « cisco1234 » et l'adresse du routeur homologue :
  R-Bordeaux(config)#crypto isakmp **key cisco1234** address **@ip-R-Limoges**
  R-Bordeaux(config)#crypto isakmp **key cisco1234** address **@ip-R-Toulouse**

Explications :

@ip-R-Limoges : 80.80.80.1 (l''interface externe du routeur R-Limoges)

@ip-R-Toulouse : 200.20.20.18 (l'interface externe du routeur R-Toulouse)

c. Phase 2 :

- IPsec SA (Security Association) numérotée **50** avec authentification AH/SHA et chiffrement ESP/3DES :
  R-Bordeaux(config)#crypto ipsec transform-set **50** ah-sha-hmac esp-3des
- Crypto map : **MYMAP** associée à la stratégie IKE n° 10 et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes entre le routeur R-Bordeaux et R-Limoges :
  R-Bordeaux(config)# crypto map **MYMAP 10** ipsec-isakmap
  R-Bordeaux(config-crypto-map)#set peer @**ip-R-Limoges**
  R-Bordeaux(config-crypto-map)#set security-association lifetime seconds 1800
  R-Bordeaux(config-crypto-map)#set transform-set **50**
  R-Bordeaux(config-crypto-map)#set Match adress **101**
  R-Bordeaux(config-crypto-map)#exit

- Crypto map : **MYMAP** associée à la stratégie IKE n° **20** et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes entre le routeur R-Bordeaux et R-Toulouse :
  R-Bordeaux(config)# crypto map **MYMAP 20** ipsec-isakmap
  R-Bordeaux(config-crypto-map)#set peer @**ip-R-Toulouse**
  R-Bordeaux(config-crypto-map)#set security-association lifetime seconds 1800
  R-Bordeaux(config-crypto-map)#set transform-set **50**
  R-Bordeaux(config-crypto-map)#set Match adress **102**
  R-Bordeaux(config-crypto-map)#exit

- Création de l'ACL n° **101** (192.168.10.0 /24 > 192.168.20.0 /24).
  R-Bordeaux(config)#access-list **101** permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
- Création de l'ACL n° **102** (192.168.10.0 /24 > 192.168.30.0 /24).
  R-Bordeaux(config)#access-list **101** permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
- Application de la crypto map à l'interface gig0/1 :
  R-Bordeaux(config)#interface gi0/0
  R-Bordeaux(config)#crypto map MYMAP

6.3 Configuration du 3ème routeur : R-Toulouse

La configuration du routeur **R-Toulouse** est quasi identique à celle de des autres routeurs Limoges (Limoges et Bordeaux) hormis , **l'homologue** et **l'ACL** qui diffèrent).

Reprenez les mêmes :

A faire sur le routeur R-Toulouse:

b. Phase 1 :

- Stratégie ISAKMP numérotée 10 :
  R-Toulouse(config)#crypto isakmp policy 10
- Chiffrement : AES
  R-Toulouse(config-isakmp)#encryption aes
- Authentification par clé pré-partagée ;
- Groupe Diffie-Hellman : 5 ;
- Renégociation : toutes les 15 minutes ;
  R-Toulouse(config-isakmp)#authentification pre-share
  R-Toulouse(config-isakmp)#group 5
  R-Toulouse(config-isakmp)#lifetime 900
  R-Toulouse(config-isakmp)#exit
- Définition de la clé pré-partagée « cisco1234 » et l'adresse du routeur homologue :
  R-Toulouse(config)#crypto isakmp **key cisco1234** address @**ip-R-Limoges**
  R-Toulouse(config)#crypto isakmp **key cisco1234** address @**ip-R-Bordeaux**

Explications :

@ip-R-Limoges : 80.80.80.1 (l''interface externe du routeur R-Limoges)

@ip-R-Bordeaux : 200.20.20.2 (l'interface externe du routeur R-Bordeaux)

d. Phase 2 :

- IPsec SA (Security Association) numérotée **50** avec authentification AH/SHA et chiffrement ESP/3DES :
  R-Toulouse(config)#crypto ipsec transform-set **50** ah-sha-hmac esp-3des
- Crypto map : **MYMAP** associée à la stratégie IKE n° 10 et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes entre le routeur R-Bordeaux et R-Limoges :
  R-Toulouse(config)# crypto map **MYMAP 10** ipsec-isakmap
  R-Toulouse(config-crypto-map)#set peer @**ip-R-Limoges**

R-Toulouse(config-crypto-map)#set security-association lifetime seconds 1800
R-Toulouse(config-crypto-map)#set transform-set **50**
R-Toulouse(config-crypto-map)#set Match adress **101**
R-Toulouse(config-crypto-map)#exit

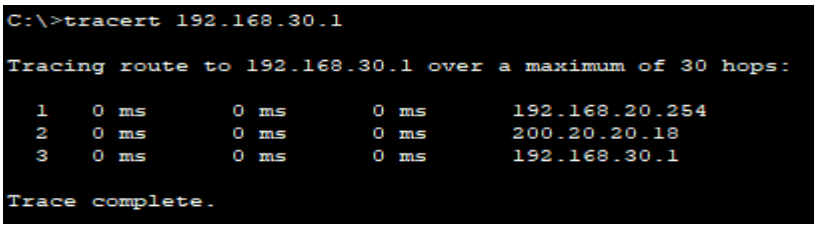
- Crypto map : **MYMAP** associée à la stratégie IKE n° **20** et à la stratégie de transformation n° 50, renouvellement de l'association de sécurité toutes les 30 minutes entre le routeur R-Bordeaux et R-Toulouse :
  R-Toulouse(config)# crypto map **MYMAP 20** ipsec-isakmap
  R-Toulouseconfig-crypto-map)#set peer @**ip-R-Bordeaux**
  R-Toulouse(config-crypto-map)#set security-association lifetime seconds 1800
  R-Toulouse(config-crypto-map)#set transform-set **50**
  R-Toulouse(config-crypto-map)#set Match adress **102**
  R-Toulouse(config-crypto-map)#exit

- Création de l'ACL n° **101** (192.168.30.0 /24 > 192.168.20.0 /24).
  R-Toulouse(config)#access-list **101** permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
- Création de l'ACL n° **102** (192.168.30.0 /24 > 192.168.10.0 /24).
  R-Toulouse(config)#access-list **101** permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
- Application de la crypto map à l'interface gig0/1 :
  R-Toulouse(config)#interface gi0/0
  R-Toulouse(config)#crypto map MYMAP

7. Tests

- **Tracert**
  Vérifiez le routage des paquets IP au travers du tunnel IPsec en testant avec la commande **`tracert`** entre les hôtes distants

Entre Limoges et Toulouse :



Entre Limoges et Bordeaux :

```
C:\>tracert 192.168.10.1

Tracing route to 192.168.10.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.20.254
  2    *         0 ms      0 ms      200.20.20.2
  3    0 ms      0 ms      0 ms      192.168.10.1

Trace complete.
```

- **Ping**

  Entre Limoges et Toulouse :

```
C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=126
Reply from 192.168.30.1: bytes=32 time<1ms TTL=126
Reply from 192.168.30.1: bytes=32 time<1ms TTL=126
Reply from 192.168.30.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Entre Limoges et Bordeaux :

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=126
Reply from 192.168.10.1: bytes=32 time<1ms TTL=126
Reply from 192.168.10.1: bytes=32 time<1ms TTL=126
Reply from 192.168.10.1: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

8. Diagnostic des routeurs VPN

- **IKE sur R-Limoges**

  #show crypto isakmp policy

```
Router#sh crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        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:               900 seconds, no volume limit
Router#
```

#show crypto isakmp sa

```
Router#sh crypto isakmp s
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
200.20.20.18    80.80.80.1      QM_IDLE           1070    0 ACTIVE

200.20.20.2     80.80.80.1      QM_IDLE           1065    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

- **IPSEC**

#show crypto ipsec ?

#show crypto ipsec sa

```
    inbound esp sas:
     spi: 0x4A1C5333(1243370291)
       transform: esp-3des ,
       in use settings ={Tunnel, }
       conn id: 2005, flow_id: FPGA:1, crypto map: MYMAP
       sa timing: remaining key lifetime (k/sec): (4525504/1602)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:
     spi: 0xF3E45E56(4091829846)
       transform: ah-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2005, flow_id: FPGA:1, crypto map: MYMAP
       sa timing: remaining key lifetime (k/sec): (4525504/1602)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound pcp sas:

    outbound esp sas:
     spi: 0xB9F83E55(3120053845)
       transform: esp-3des ,
       in use settings ={Tunnel, }
       conn id: 2006, flow_id: FPGA:1, crypto map: MYMAP
       sa timing: remaining key lifetime (k/sec): (4525504/1602)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:
     spi: 0x164D759E(374175134)
       transform: ah-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2006, flow_id: FPGA:1, crypto map: MYMAP
       sa timing: remaining key lifetime (k/sec): (4525504/1602)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound pcp sas:

  local  ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
  remote  ident (addr/mask/prot/port): (192.168.30.0/255.255.255.0/0/0)
--More--
```

```
Router#sh crypto ipsec sa

interface: GigabitEthernet0/1
    Crypto map tag: MYMAP, local addr 80.80.80.1

   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 200.20.20.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
   #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.: 80.80.80.1, remote crypto endpt.:200.20.20.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
     current outbound spi: 0xC8FF5C78(3372178552)

     inbound esp sas:
      spi: 0x04819E9F(75603615)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:1, crypto map: MYMAP
        sa timing: remaining key lifetime (k/sec): (4525504/1596)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
      spi: 0xC8728566(3362948454)
        transform: ah-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2005, flow_id: FPGA:1, crypto map: MYMAP
```

#show crypto ipsec transform-set

```
Router#sh crypto ipsec tr
Router#sh crypto ipsec transform-set
Transform set 50: { ah-sha-hmac  }
    will negotiate = { Tunnel,  },
   { esp-3des  }
   will negotiate = { Tunnel,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },
Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },

Router#
```

p