Tunnel VPN IPsec site-à-site

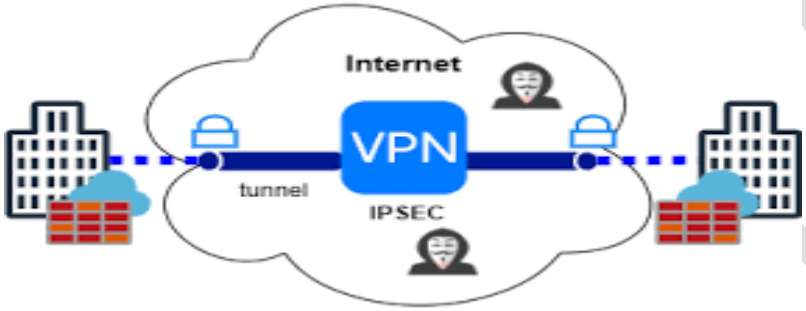
ES-SAIDI Naoufal

Sommaire

Tunnel VPN IPsec site-à-site

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.



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#
```

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, RBordeaux 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 1ERE 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 :

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.

a. 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
```

- 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).

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) 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.**

1. 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 commandes en faisant attention aux points suivants :

```
R-Bordeaux(config)#crypto isakmp key cisco1234 address ????
```

```
R-Bordeaux(config-crypto-map)#set peer ????
```

```
R-Bordeaux(config)#interface ???
```

```
R-Bordeaux(config)#access-list 101 permit ip ????
```

2. Tests

- **Tracert**

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

- En mode simulation, analyser le contenu des paquets IP échangés via le VPN. **Réaliser des copies d'écran.**

3. Diagnostic des routeurs VPN

- **IKE**

  #show crypto isakmp policy

  #show crypto isakmp sa

  #show crypto isakmp peers

- **IPSEC**

  #show crypto ipsec ?

  #show crypto ipsec sa

  #show crypto ipsec transform-set

- **DEBUG**

#debug crypto isakmp

#debug crypto ipsec