

A thick dark grey vertical bar is positioned on the left side of the page. To its right, there is an orange arrow pointing right, containing the date '08/01/2018'. Further down, several thin, curved lines in black and grey originate from the left and sweep upwards and to the right.

08/01/2018

Mise en place de VPN avec IPSec

Léo Guilpain & Legris Thomas

Table des matières

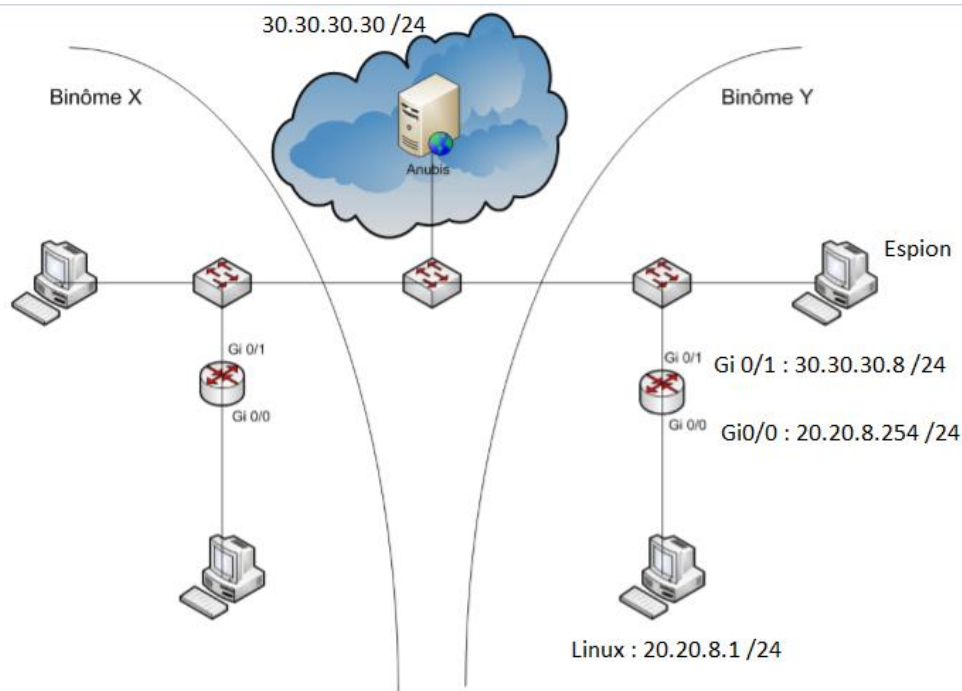
Introduction.....	2
Mise en place de 2 sites	2
Mise en place d'un tunnel IPSec en AH.....	3
Travail à réaliser	3
Mise en place sur GNS3.....	3

Introduction

Le but de ce TP est de relier deux sites d'une même entreprise à l'aide d'un tunnel sécurisé par IPSEC. On utilisera dans un premier temps le protocole AH (pas de chiffrement) puis le protocole ESP (chiffrement des données) à clé manuelle.

Ensuite, il faudra mettre en place le protocole IKE pour échanger les clés. On l'utilisera d'abord avec des clés partagées puis avec des clés publique RSA.

Mise en place de 2 sites



Après avoir réalisé la commande :

```
Router(config)#ip route 20.20.7.0 255.255.255.0 30.30.30.7
```

Ensuite nous avons ajouté la route par défaut suivante :

```
root@localhost:~# route add default gw 20.20.8.254
```

D'après la capture ci-dessus, nous voyons que la connectivité se fait bien. Nous arrivons à pinger la machine voisine.

```
root@localhost:~# ping 20.20.7.1
PING 20.20.7.1 (20.20.7.1) 56(84) bytes of data.
64 bytes from 20.20.7.1: icmp_seq=1 ttl=62 time=0.795 ms
64 bytes from 20.20.7.1: icmp_seq=2 ttl=62 time=0.777 ms
64 bytes from 20.20.7.1: icmp_seq=3 ttl=62 time=0.800 ms
64 bytes from 20.20.7.1: icmp_seq=4 ttl=62 time=0.780 ms
64 bytes from 20.20.7.1: icmp_seq=5 ttl=62 time=0.779 ms
```

Mise en place d'un tunnel IPsec en AH

Travail à réaliser

Après avoir réalisé ces différents ACL, nous arrivons à pinger la machine.

```
Router#show access-list
Standard IP access list 1
 20 permit 30.30.30.7
 10 deny   30.30.30.0
Router#
```

On met en place les différentes combinaisons possibles de protocoles et algorithmes utilisables dans les transform set

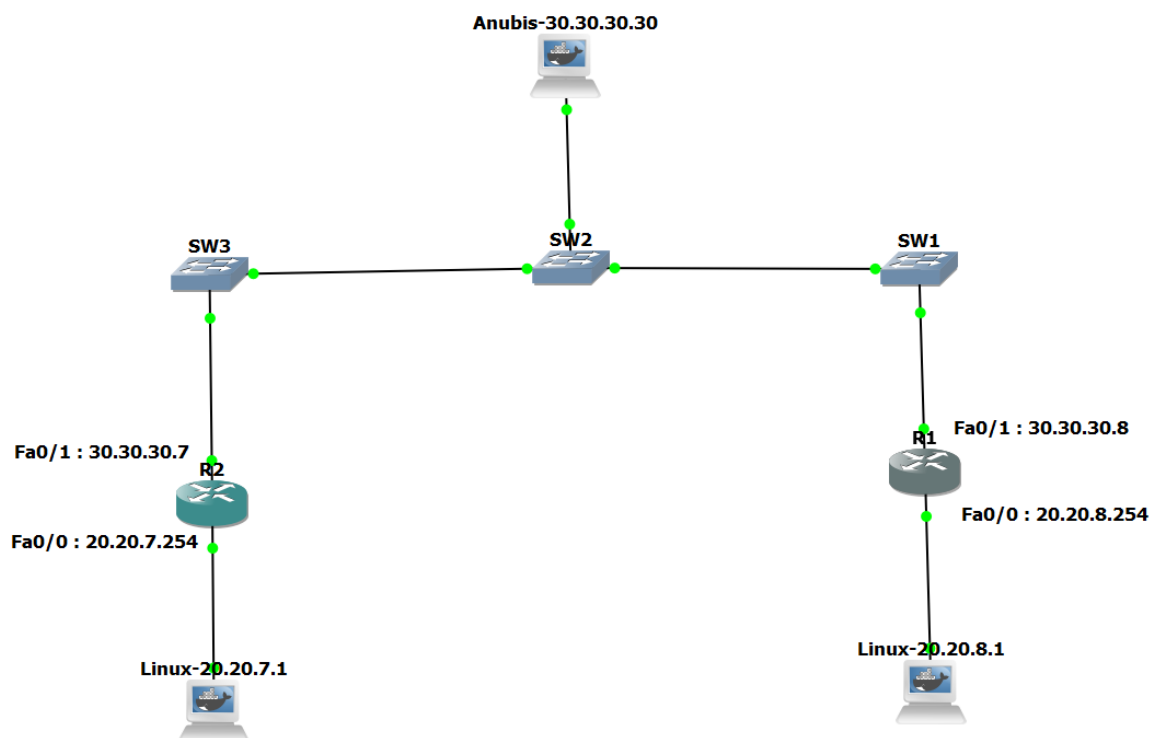
```
Router(config)#crypto ipsec transform-set tunnel ah-md5-hmac
Router(cfg-crypto-trans)#
```

Ensuite nous avons suivi la procédure pour créer un tunnel IPsec avec clefs manuelles :


```
Router(config-crypto-map)#match address access-list-1
Router(config-crypto-map)#set peer 30.30.30.7
Router(config-crypto-map)#set transform-set tunnel

set session-key inbound ah 256 012345678901234567890$
```

Mise en place sur GNS3



Après avoir attribué les différentes adresses aux différents postes, on peut voir que la connectivité se fait correctement :

 Linux-20.20.8.1

```
/ # ping 20.20.7.1
PING 20.20.7.1 (20.20.7.1): 56 data bytes
64 bytes from 20.20.7.1: seq=0 ttl=62 time=25.273 ms
64 bytes from 20.20.7.1: seq=1 ttl=62 time=28.276 ms
64 bytes from 20.20.7.1: seq=2 ttl=62 time=36.279 ms
64 bytes from 20.20.7.1: seq=3 ttl=62 time=30.902 ms
^C
--- 20.20.7.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 25.273/30.182/36.279 ms
```

Ensuite, on a mis en place différents ACL.

```
R1#show access-list
Standard IP access list 1
 10 permit 30.30.30.7
Standard IP access list 2
 10 deny 30.30.30.0
```

```
R2#show access-list
Standard IP access list 1
 10 permit 30.30.30.8
Standard IP access list 2
 10 deny 30.30.30.0
```

Après avoir mis en place les ACL, on obtient :

805	653.753758	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)
806	654.747696	20.20.8.1	20.20.7.1	ICMP	98 Echo (ping) request id=0x4c00, seq=341/21761, ttl=64 (no response found!)
807	654.758948	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)
808	655.747786	20.20.8.1	20.20.7.1	ICMP	98 Echo (ping) request id=0x4c00, seq=342/22017, ttl=64 (no response found!)
809	655.756988	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)
810	656.747895	20.20.8.1	20.20.7.1	ICMP	98 Echo (ping) request id=0x4c00, seq=343/22273, ttl=64 (no response found!)
811	656.760071	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)
812	657.748032	20.20.8.1	20.20.7.1	ICMP	98 Echo (ping) request id=0x4c00, seq=344/22529, ttl=64 (no response found!)
813	657.761795	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)
814	658.748563	20.20.8.1	20.20.7.1	ICMP	98 Echo (ping) request id=0x4c00, seq=345/22785, ttl=64 (no response found!)
815	658.761948	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)
816	659.748502	20.20.8.1	20.20.7.1	ICMP	98 Echo (ping) request id=0x4c00, seq=346/23041, ttl=64 (no response found!)
817	659.754566	20.20.8.254	20.20.8.1	ICMP	70 Destination unreachable (Communication administratively filtered)

On met en place les différentes combinaisons possibles de protocoles et algorithmes utilisables dans les transform set :

```
R1(config)#crypto ipsec transform-set tunnel ah-md5-hmac
R1(cfg-crypto-trans)#crypto map tunnel 1 ipsec-manual
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#match address access-list-1
R1(config-crypto-map)#set peer 30.30.30.7
R1(config-crypto-map)#set transform-set tunnel
R1(config-crypto-map)#$-key inbound ah 256 012345678901234567890123456789
R1(config-crypto-map)#$-key outbound ah 256 012345678901234567890123456789
```

On réalise ceci sur les deux routeurs.

Ensuite, on l'applique à l'interface sur lequel le tunnel est utilisé.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Fa0/1
R1(config-if)#crypto map tunnel
```