Mise en place de VPN IPSec Avec des ASA 5506-X et dernier le NAT

Ershad RAMEZANI

Introduction

Le présent document explique la procédure de configuration d'un tunnel VPN IPSec de site à site en utilisant la version 1 d'échange de clés Internet (IKEv1) entre deux ASA 5506-X.

Les tunnels VPN IPSec de site à site sont largement utilisés pour assurer une transmission sécurisée de données, de voix et de vidéo entre deux sites distants, tels que des bureaux ou des succursales. Ce type de tunnel VPN est établi sur le réseau public d'Internet et est chiffré à l'aide d'algorithmes de cryptage avancés pour garantir la confidentialité des données échangées entre les deux sites.

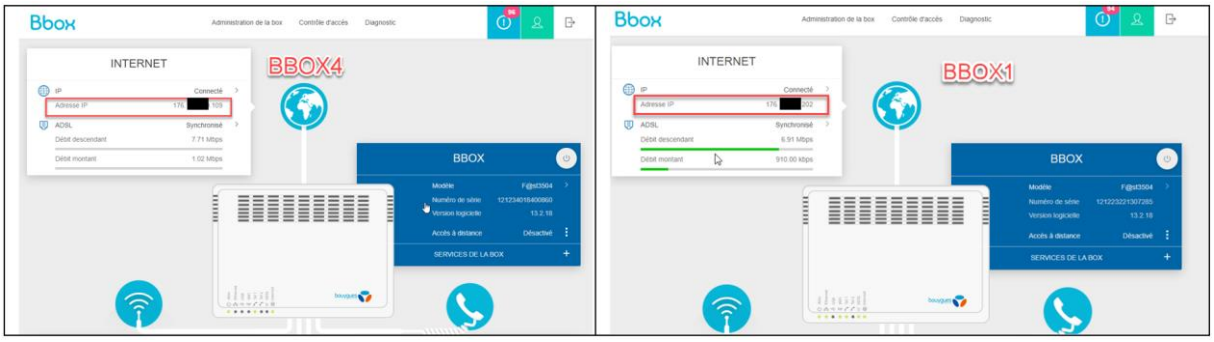
La configuration de ce tunnel VPN IPSec site à site nécessite deux étapes :

1. Configuration d'ISAKMP (Phase 1 d'ISAKMP)
2. Configuration d'IPSec (Phase 2 d'ISAKMP, ACLs, Crypto MAP)

Les équipements utilisés

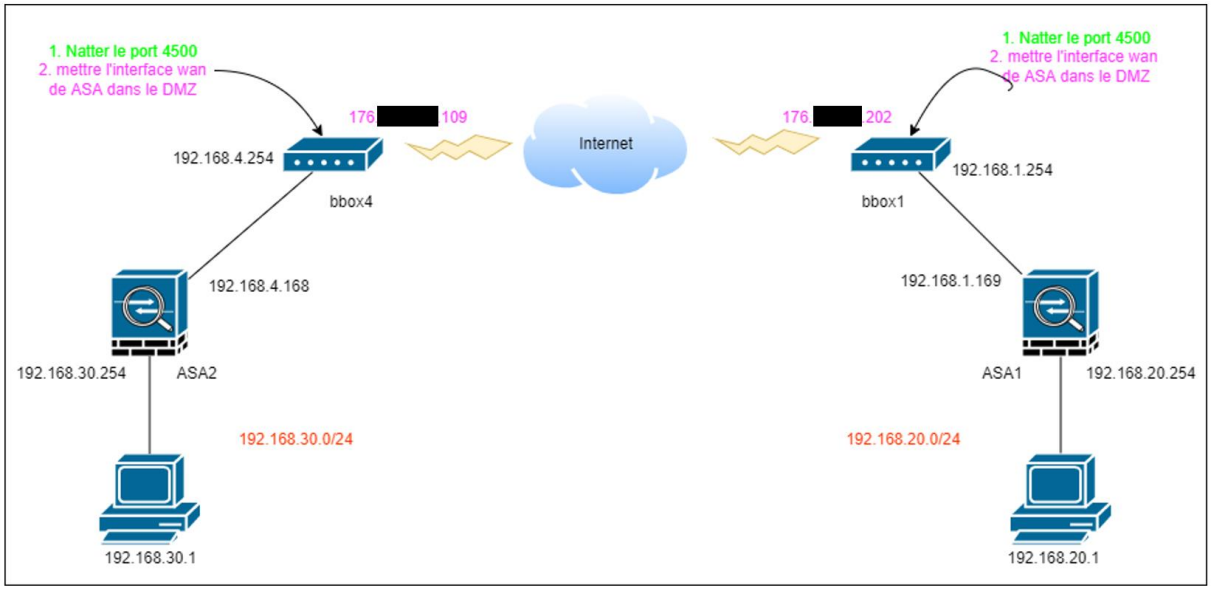
- Deux ASAs model 5506-X :

- Deux box internet Bbox :



- Deux PC clients Windows :

Le schéma



Les règles pour ASAs

Il existe trois règles à respecter en ce qui concerne les ASAs :

Règle 1 : Les routes doivent être définies pour que les routeurs (et les ASAs) sachent où envoyer les paquets.

Règle 2 : Par défaut, les requêtes émanant d'un niveau de sécurité élevé vers un niveau de sécurité inférieur sont autorisées, mais pas dans le sens inverse. Ainsi, le LAN (niveau de sécurité 100) peut envoyer des requêtes (telles que des ping echo) vers les réseaux externes. Cependant, les requêtes (de quelque type que ce soit) émanant de l'extérieur (niveau de sécurité 0) vers le LAN (niveau de sécurité 100) sont bloquées par défaut. C'est pourquoi nous ajouterons plus tard l'ACL 200 sur les interfaces externes, ce qui permettra au réseau externe de faire des pings vers le réseau interne.

Règle 3 : L'inspection des protocoles sur l'ASA permet de savoir quelles sont les requêtes qui arrivent de l'extérieur (niveau de sécurité plus bas) et qui sont des réponses aux requêtes envoyées de l'intérieur (niveau de sécurité plus élevé). Ainsi, dans notre cas, l'inspection de ICMP permet à l'ASA de laisser passer les réponses echo-reply de l'extérieur vers le LAN de Toulouse (en dépit de la règle 2 !).

Configuration des ASAs

Configuration des interfaces sur les deux ASAs :

La configuration des ASAs inclut la configuration des interfaces sur les deux appareils. Tout d'abord, il est nécessaire de configurer les interfaces sur chaque ASA. Une interface avec un niveau de sécurité de 0 est définie comme étant "outside" et une autre interface avec un niveau de sécurité de 100 est définie comme étant "inside".

- ASA1 :

```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 192.168.1.169 255.255.255.0
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 192.168.20.254 255.255.255.0
!
```

- ASA2 :

```
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 192.168.4.168 255.255.255.0
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 192.168.30.254 255.255.255.0
!
```

Configuration des routes par défaut sur les deux ASAs (la règles 1) :

ASA1 :

```
route outside 0.0.0.0 0.0.0.0 192.168.1.254 1
```

ASA2 :

```
route outside 0.0.0.0 0.0.0.0 192.168.4.254 1
```

Création des objets network :

La création d'objets Network nous permettra de définir différents *subnet* ou différents *host* dans un objet et de les utiliser pour créer des ACLs ou des NAT, ce qui facilitera grandement la vie ! Nous allons donc créer un objet pour le réseau distant, car nous en aurons besoin lors de la configuration du VPN IPSec site-à-site.

ASA1 :

```
object network local-net
 subnet 192.168.20.0 255.255.255.0
object network remote-net
 subnet 192.168.30.0 255.255.255.0
```

ASA2 :

```
object network local-net
 subnet 192.168.30.0 255.255.255.0
object network remote-net
 subnet 192.168.20.0 255.255.255.0
```

Mise en place de l'inspection des paquets (la règle 3) :

Par défaut, l'inspection des paquets est configurée sur l'ASA. Si l'on souhaite, il est possible de créer sa propre politique au lieu d'utiliser la politique globale (la politique par défaut).

- ASA1 :

```
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
```

- ASA2 :

```
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
```

Mise en place du NAT dynamique :

Le NAT dynamique, également connu sous le nom de NAT overload, permet à notre réseau interne d'accéder à l'internet. Pour cela, le NAT est ajouté à l'objet réseau local et notre interface est configurée comme étant "outside".

- ASA1 :

```
object network local-net
 nat (inside,outside) dynamic interface
```

- ASA2 :

```
object network local-net
 nat (inside,outside) dynamic interface
```

Création des ACL 200 sur les deux ASAs pour autoriser le ping :

Comme déjà dit dans la règle 2, pour autoriser le ping depuis outside vers inside il nous faut une ACL sur l'interface outside pour le protocole demandé.

ASA1 :

```
access-list 200 extended permit icmp any any
```

```
access-group 200 in interface outside
```

ASA2 :

```
access-list 200 extended permit icmp any any
```

```
access-group 200 in interface outside
```

Mise en place de VPN IPSec

Configuration de la phase 1 sur ASA1 :

- Création de crypto ikev1 :
  - Activer IKEv1 sur l'interface outside :
  - Créer un policy IKEv1 qui définit les algorithmes/méthodes à utiliser pour le hachage, l'authentification, le groupe Diffie-Hellman, la durée de vie et le chiffrement :

```
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

- Création du tunnel-group :
  - Créer un groupe de tunnels sous les attributs IPsec et configurez l'adresse IP du peer et la clé pré-partagée du tunnel :

```
tunnel-group 176.[redacted].202 type ipsec-l2l
tunnel-group 176.[redacted].202 ipsec-attributes
 ikev1 pre-shared-key *****
```

Configuration de la phase 1 sur ASA2 :

- Création de crypto ikev1 :

```
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

- Création du tunnel-group :

```
tunnel-group 176.       .109 type ipsec-l2l
tunnel-group 176.       .109 ipsec-attributes
 ikev1 pre-shared-key *****
```

Configuration de la phase 2 sur ASA1 :

- Création d'un ACL pour le trafic à envoyer sur le tunnel :

Créez une liste d'accès qui définit le trafic à chiffrer et passer par le tunnel

```
access-list 100 extended permit ip object local-net object remote-net
```

- Création du transform-set myset :

Configurez le Transform Set (TS), qui doit impliquer le mot-clé IKEv1. Un TS identique doit également être créé sur l'extrémité distante :

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

- Configuration de crypto map :

Configurez le crypto map, qui contient ces composants :

  - L'adresse IP du peer
  - La liste d'accès définie qui contient le trafic d'intérêt
  - Le Transform set

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 176.       .202
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set security-association lifetime seconds 86400
crypto map outside_map interface outside
```

Configuration de la phase 2 sur ASA2 :

- Création d'un ACL pour le trafic à envoyer sur le tunnel :

```
access-list 100 extended permit ip object local-net object remote-net
```

- Création du transform-set myset :

```
crypto ipsec ikev1 transform-set myset esp-aes esp-sha-hmac
```

- Configuration de crypto map :

```
crypto map outside_map 20 match address 100
crypto map outside_map 20 set peer 176.[redacted].109
crypto map outside_map 20 set ikev1 transform-set myset
crypto map outside_map 20 set security-association lifetime seconds 86400
crypto map outside_map interface outside
```

NAT exemption :

L'exemption NAT vous permet d'empêcher le trafic d'être traduit avec NAT. Un scénario dans lequel vous en avez généralement besoin est lorsque vous disposez d'un tunnel VPN de site à site.

- ASA1 :

```
nat (inside,outside) source static local-net local-net destination static remote-net
 remote-net no-proxy-arp route-lookup
```

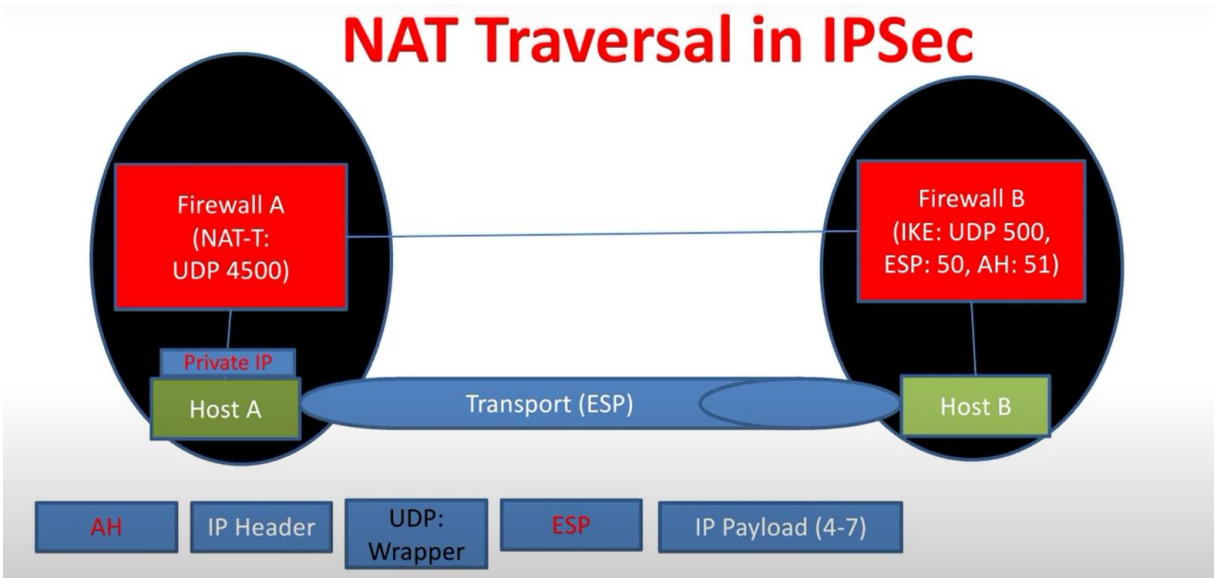
- ASA2 :

```
nat (inside,outside) source static local-net local-net destination static remote-net remote-net no-proxy-arp route-lookup
```

Définir le keeplive pour NAT-Traversal :

La définition du keeplive pour NAT-Traversal est la suivante : si un client distant se connecte à partir d'une adresse IP publique directe, il se connecte via le tunnel de la même manière qu'un tunnel régulier établi sur le port UDP 500. Toutefois, si le client se connecte à partir d'une adresse IP NATée (où l'adresse IP est privée mais que le FAI utilise le PAT/NAT), il se connecte également via UDP 500, mais est encapsulé dans un autre en-tête, l'en-tête NAT-Traversal, et communique via UDP 4500. Dans ce cas, il est nécessaire d'activer le NAT-T sur le pare-feu, tel qu'un ASA, afin de maintenir une communication continue.

Si NAT-T est activé, les clients avec une adresse IP publique et les clients NATés pourront se connecter via le tunnel VPN. En revanche, si NAT-T n'est pas activé, seuls les clients ayant une adresse IP publique pourront établir une connexion via le tunnel VPN. Il est donc important d'activer NAT-T si vous prévoyez de permettre à des clients derrière un NAT de se connecter via le tunnel VPN.



Le NAT-Traversal est par défaut activé sur ASA. Mais on peut changer son keepalive.

- ASA1 :

```
crypto isakmp nat-traversal 3600
```

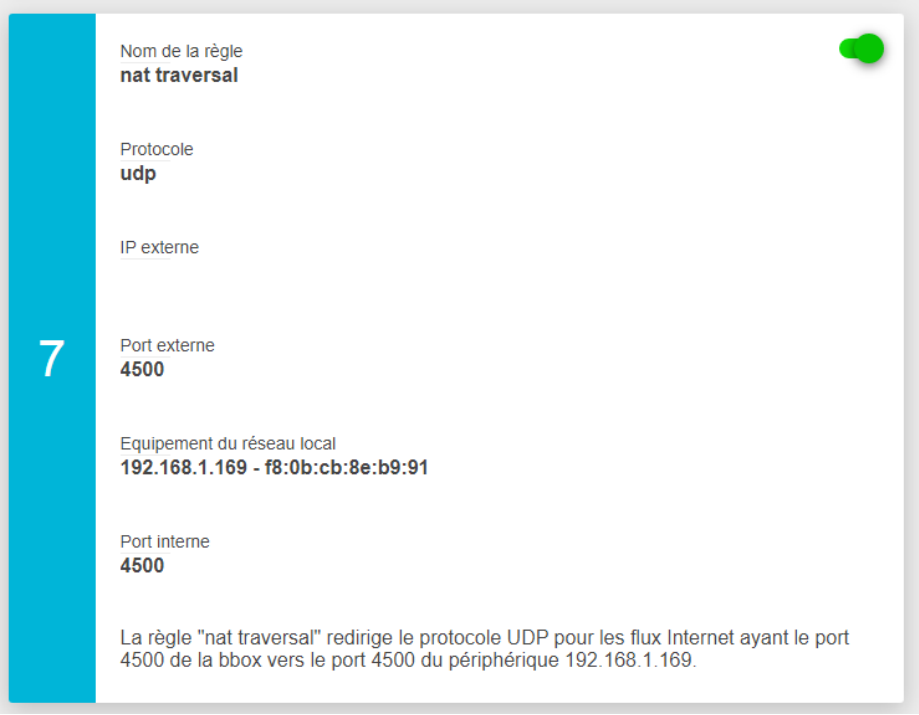
- ASA2 :

```
crypto isakmp nat-traversal 3600
```

Port forwarding sur le BBOX :

Il est obligatoire de configurer le port forwarding pour le port 4500 (NAT-Traversal) sur les deux boxes internet afin que le Bbox puisse permettre le passage des paquets pour le trafic VPN IPSec. Il est clair que le port forwarding pour le port 500 de la phase 1 n'est pas requis.

- BBOX1 :



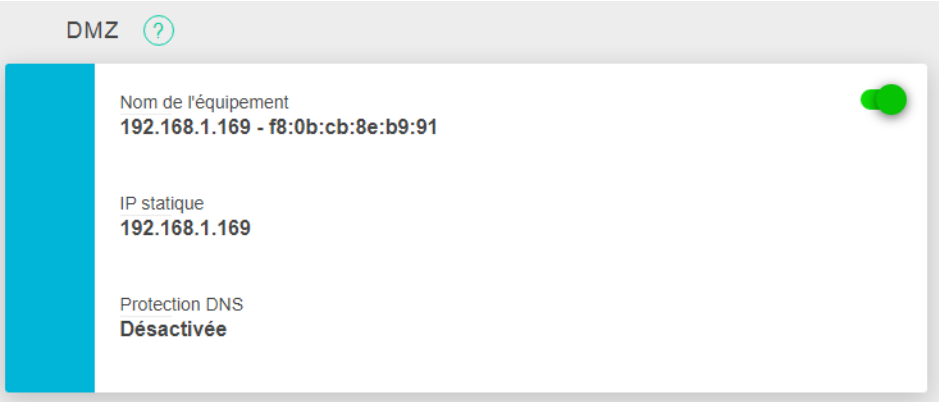
- BBOX4 :

Mettre l'interface WAN des ASAs dans le DMZ :

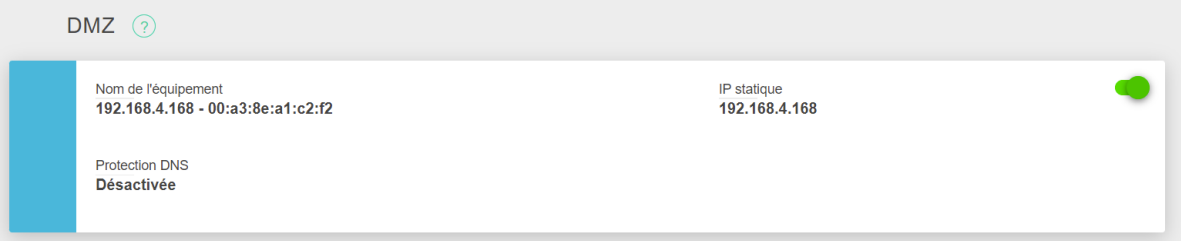
Il existe d'autres protocoles nécessaires pour assurer le bon fonctionnement du tunnel VPN IPSec. Sur les BBOXs, étant donné qu'il n'est pas possible d'accéder à la configuration avancée pour définir ces protocoles et les faire passer à travers le pare-feu, deux options s'offrent à nous : soit désactiver le

pare-feu sur le BBOX, soit placer l'interface "outside" de l'ASA dans le DMZ où tous les protocoles par défaut sont autorisés et où il n'y a pas de pare-feu.

- ASA1 et sur BBOX1 :



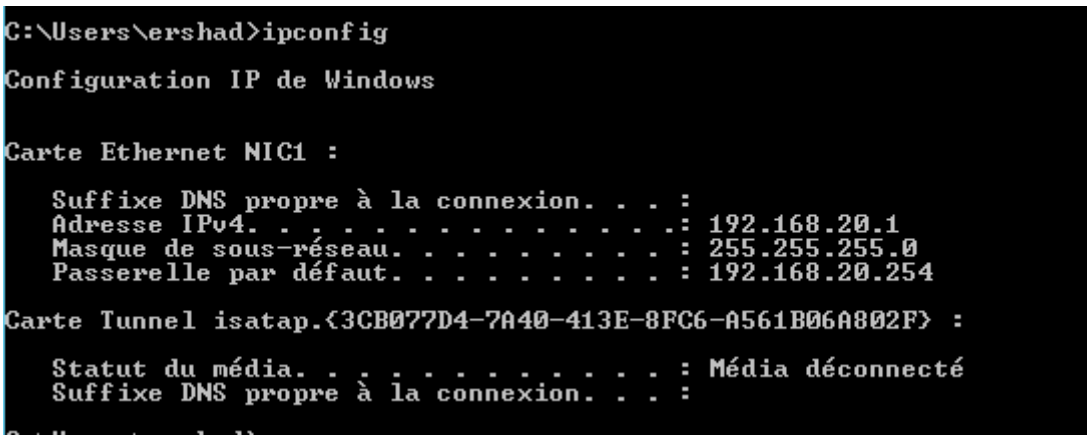
- ASA2 et sur BBOX4 :



Déclencher le VPN IPSec :

Configuration réseau sur les PC locaux pour ASA1 et ASA2 :

- Derrière ASA1 :



- Derrière ASA2 :

```
C:\Users\ersha>ipconfig

Configuration IP de Windows


Carte inconnue Connexion au réseau local :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet vEthernet (externe) :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.30.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.30.254
```

Faire un ping pour déclencher la création du tunnel :

faire au moins un ping est obligatoire pour que le vpn commence à fonctionner et le tunnel soit établi.

- Depuis le pc derrière ASA1 :

```
C:\Users\ershad>ping 192.168.30.1

Envoi d'une requête 'Ping'  192.168.30.1 avec 32 octets de données :
Réponse de 192.168.30.1 : octets=32 temps=64 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=73 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128

Statistiques Ping pour 192.168.30.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 62ms, Maximum = 73ms, Moyenne = 65ms

C:\Users\ershad>
```

- Depuis le pc derrière ASA2 :

```
C:\Users\ersha>ping 192.168.20.1

Envoi d'une requête 'Ping'  192.168.20.1 avec 32 octets de données :
Réponse de 192.168.20.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.20.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.20.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.20.1 : octets=32 temps=62 ms TTL=128

Statistiques Ping pour 192.168.20.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 62ms, Maximum = 63ms, Moyenne = 62ms
```

Vérifier la création de la phase 1 (ikev1) :

On peut vérifier la situation de ikev1 (la phase 1) avec la commande *show crypto ikev1 sa.*

- ASA1 :

```
ASA1(config)# show crypto ikev1 sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 176.[redacted].109
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
ASA1(config)#
```

- ASA2 :

```
ASA2(config)# show crypto ikev1 sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 176.[redacted].202
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE
ASA2(config)#
```

Vérifier la création de la phase 2 (IPSec) :

Et pour la phase 2, la commande est *show crypto ipsec sa.*

- ASA1 :

```
ASA1(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.1.169

      access-list 100 extended permit ip 192.168.20.0 255.255.255.0 192.168.30.0 255.255.255.0
      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)
      current_peer: 176.[redacted]109


      #pkts encaps: 3243, #pkts encrypt: 3243, #pkts digest: 3243
      #pkts decaps: 3249, #pkts decrypt: 3249, #pkts verify: 3249
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 3243, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.1.169/4500, remote crypto endpt.: 176.[redacted].109/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 46252644
      current inbound spi : D60F5E19

    inbound esp sas:
      spi: 0xD60F5E19 (3591331353)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv1, }
         slot: 0, conn_id: 16384, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3914809/84733)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x46252644 (1176839748)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv1, }
         slot: 0, conn_id: 16384, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (3914809/84733)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

- ASA2 :

```
ASA2(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.4.168

      access-list 100 extended permit ip 192.168.30.0 255.255.255.0 192.168.20.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.30.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
      current_peer: 176[redacted].202


      #pkts encaps: 3423, #pkts encrypt: 3423, #pkts digest: 3423
      #pkts decaps: 3417, #pkts decrypt: 3417, #pkts verify: 3417
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 3423, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.4.168/4500, remote crypto endpt.: 176.[redacted]202/4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D60F5E19
      current inbound spi : 46252644

    inbound esp sas:
      spi: 0x46252644 (1176839748)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv1, }
         slot: 0, conn_id: 16384, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373799/84645)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD60F5E19 (3591331353)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv1, }
         slot: 0, conn_id: 16384, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec): (4373799/84645)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Les commandes pour diagnostiquer le tunnel :

les tests sont fait seulement sur ASA2.

Show vpn-sessiondb l2l :

```
ASA2(config)# show vpn-sessiondb l2l

Session Type: LAN-to-LAN

Connection    : 176.[redacted].202
Index         : 16                    IP Addr      : 176.[redacted].202
Protocol      : IKEv1 IPsecOverNatT
Encryption    : IKEv1: (1)AES128  IPsecOverNatT: (1)AES128
Hashing       : IKEv1: (1)SHA1  IPsecOverNatT: (1)SHA1
Bytes Tx      : 40800                 Bytes Rx     : 44940
Login Time    : 00:21:36 UTC Thu Jan 2 2014
Duration      : 0h:11m:50s

ASA2(config)#
```

Show vpn-sessiondb summary :

```
ASA2(config)# show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
Site-to-Site VPN           :      1 :         16 :           1
  IKEv1 IPsec              :      1 :         16 :           1
-------------------------------------------------------------------------
Total Active and Inactive  :      1            Total Cumulative :     16
Device Total VPN Capacity  :     50
Device Load                :     2%
-------------------------------------------------------------------------
```

Show vpn-sessiondb detail :

```
ASA2(config)# show vpn-sessiondb detail
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
Site-to-Site VPN           :      1 :         16 :           1
  IKEv1 IPsec              :      1 :         16 :           1
-------------------------------------------------------------------------
Total Active and Inactive  :      1            Total Cumulative :     16
Device Total VPN Capacity  :     50
Device Load                :     2%
-------------------------------------------------------------------------

-------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------------
IKEv1                      :      1 :         16 :               1
IPsecOverNatT              :      1 :         16 :               1
-------------------------------------------------------------------------
Totals                     :      2 :         32
-------------------------------------------------------------------------

ASA2(config)#
```

Faire une capture de isakmp :

Faire une capture de isakmp sur l'interface outside et visualiser cette capture :

```
ASA2(config)# capture ipseccapture type isakmp interface outside
ASA2(config)# show capture ipseccapture decode
```

Le résultat pour ce capture :

```
1: 20:03:45.72166580       192.168.4.168.500 > 176.[redacted]202.500:  udp 172
   ISAKMP Header
     Initiator COOKIE: 5f 75 b4 2d eb 70 68 a1
     Responder COOKIE: 00 00 00 00 00 00 00 00
     Next Payload: Security Association
     Version: 1.0
     Exchange Type: Identity Protection (Main Mode)
     Flags: (none)
     MessageID: 00000000
     Length: 172
     Payload Security Association
       Next Payload: Vendor ID
       Reserved: 00
       Payload Length: 60
       DOI: IPsec
       Situation:(SIT_IDENTITY_ONLY)
       Payload Proposal
         Next Payload: None
         Reserved: 00
         Payload Length: 48
         Proposal #: 1
         Protocol-Id: PROTO_ISAKMP
         SPI Size: 0
         # of transforms: 1
         Payload Transform
           Next Payload: None
           Reserved: 00
           Payload Length: 40
           Transform #: 1
           Transform-Id: KEY_IKE
           Reserved2: 0000
           Group Description: Group 2
           Encryption Algorithm: AES-CBC
           Key Length: 128
           Hash Algorithm: SHA1
           Authentication Method: Preshared key
           Life Type: seconds
           Life Duration (Hex): 00 01 51 80
     Payload Vendor ID
       Next Payload: Vendor ID
       Reserved: 00
       Payload Length: 20
       Data (In Hex):
         90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
     Payload Vendor ID
       Next Payload: Vendor ID
       Reserved: 00
       Payload Length: 20
```

```
        Transform #: 1
        Transform-Id: KEY_IKE
        Reserved2: 0000
        Group Description: Group 2
        Encryption Algorithm: AES-CBC
        Key Length: 128
        Hash Algorithm: SHA1
        Authentication Method: Preshared key
        Life Type: seconds
        Life Duration (Hex): 00 01 51 80
   Payload Vendor ID
     Next Payload: Vendor ID
     Reserved: 00
     Payload Length: 20
     Data (In Hex):
       90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
   Payload Vendor ID
     Next Payload: Vendor ID
     Reserved: 00
     Payload Length: 20
     Data (In Hex):
       7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
   Payload Vendor ID
     Next Payload: Vendor ID
     Reserved: 00
     Payload Length: 20
     Data (In Hex):
       4a 13 1c 81 07 03 58 45 5c 57 28 f2 0e 95 45 2f
   Payload Vendor ID
     Next Payload: None
     Reserved: 00
     Payload Length: 24
     Data (In Hex):
       40 48 b7 d5 6e bc e8 85 25 e7 de 7f 00 d6 c2 d3
       c0 00 00 00
```

Supprimer le phase 1 et 2 de tunnel :

Supprimer le phase 1 de tunnel par une commande sur ASA et vérifier son effet. On voit bien que après le commande ***clear***, pendant deux ping, il y a pas de ***IKEv1 SAs*** présent sur le ASA et on voit deux paquet perdu sur le ping .

```
ASA2(config)# clear crypto ikev1 sa 176       .202
ASA2(config)# show crypto ikev1 sa

There are no IKEv1 SAs
ASA2(config)# show crypto ikev1 sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 176.       202
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM ACTIVE
```

```
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=65 ms TTL=128
```

- Supprimer le phase 2 de tunnel par une commande sur ASA et vérifier son effet :

Pareil pour la phase 2 comme la phase 1.

```
ASA2(config)# clear crypto ipsec sa peer 176.      202
ASA2(config)# show crypto ipsec sa

There are no ipsec sas
ASA2(config)# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local addr: 192.168.4.168

      access-list 100 extended permit ip 192.168.30.0 255.255.255.0 192.168.20.0 255
.255.255.0
      local ident (addr/mask/prot/port): (192.168.30.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
      current_peer: 176.      .202


      #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 comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.4.168/4500, remote crypto endpt.: 176.      202/
4500
      path mtu 1500, ipsec overhead 82(52), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 7146934F
```

```
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=64 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 192.168.30.1 : octets=32 temps=63 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=61 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
Réponse de 192.168.30.1 : octets=32 temps=62 ms TTL=128
```

FIN