Un tunnel IKE v2 dynamique site à site entre une ASA et un exemple de configuration de routeur IOS

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations générales
Configuration
Scénario 1
Diagramme du réseau
Configuration
Scénario 2
Diagramme du réseau
Configuration
Vérification
ASA statique
Routeur dynamique
Routeur dynamique (avec l'ASA dynamique distante)
Dépannage

Introduction

Ce document décrit comment configurer un tunnel VPN de la version 2 d'échange de clés Internet (IKE) de site à site (IKEv2) entre un dispositif de sécurité adaptable (ASA) et un routeur de Cisco où le routeur a une adresse IP dynamique et l'ASA a une adresse IP statique sur les interfaces de public-revêtement.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS® Version 15.1(1)T ou ultérieure
- Version 8.4(1) ou ultérieures de Cisco ASA

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le présent document aborde ces scénarios :

- Scénario 1 :Un ASA est configuré avec une adresse IP statique qui utilise un groupe désigné de tunnels. Le routeur est configuré avec une adresse IP dynamique.
- Scénario 2 :Un ASA et le routeur sont configurés avec une adresse IP dynamique.
- Scénario 3 :Le présent scénario n'est pas abordé ici.Dans ce scénario, l'ASA est configuré avec une adresse IP statique mais utilise le groupe de tunnel DefaultL2LGroup. La configuration pour cela est similaire à celle décrite dans l'article Exemple de configuration de tunnel VPN IKEv2 site à site dynamique entre deux ASA.

La plus grande différence de configuration entre les scénarios 1 et 3 est l'ID de Protocole ISAKMP (Internet Security Association and Key Management Protocol) utilisé par le routeur distant.Quand le DefaultL2LGroup est utilisé sur l'ASA statique, l'ID de l'ISAKMP du pair sur le routeur doit être l'adresse de l'ASA.Cependant, si un groupe désigné de tunnel est utilisé, l'ID de l'ISAKMP du pair sur le routeur doit être identique au nom de groupe de tunnel configuré sur l'ASA.Ceci est accompli avec cette commande sur le routeur :

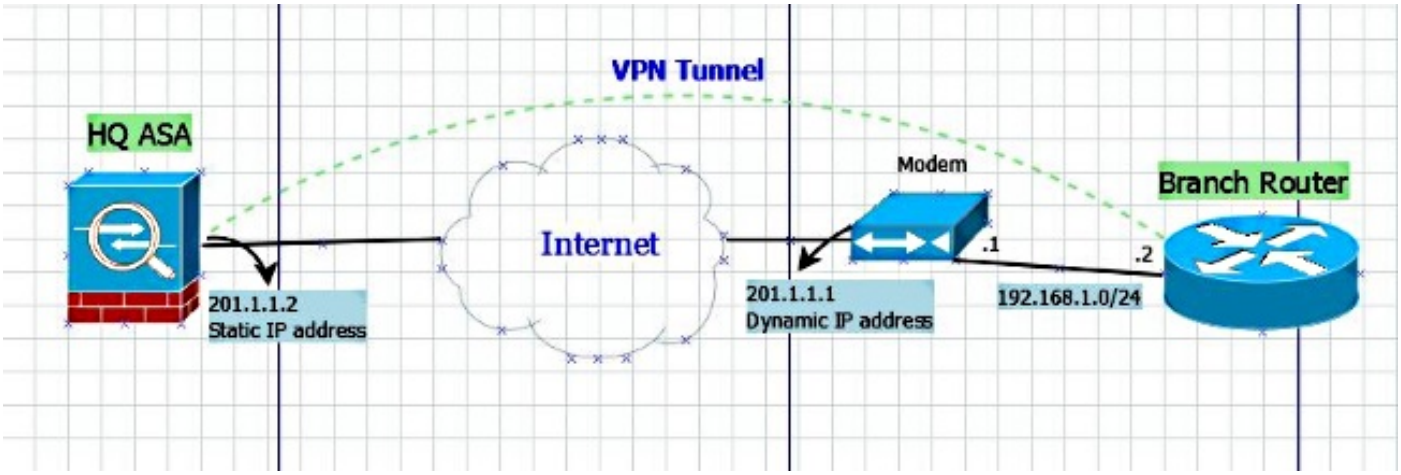
```
identity local key-id
```

L'avantage d'utiliser les groupes désignés de tunnel sur l'ASA statique est que quand DefaultL2LGroup est utilisé, la configuration sur les ASA/routeurs dynamiques distants, qui comprend les clés pré-partagées, doit être identique et autorise peu de paramétrage de politiques à un niveau plus fin (granularité).

Configuration

Scénario 1

Diagramme du réseau



Configuration

Cette section décrit la configuration sur l'ASA et le routeur basés sur la configuration désignée de groupe de tunnels.

Configuration statique ASA

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

Configuration de routeur dynamique

Le routeur dynamique est configuré presque de la même manière qu'une configuration normale dans les cas où le routeur est un site dynamique pour le tunnel IKEv2 L2L avec en plus la commande affichée ici :

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

Ainsi sur chaque pair dynamique, l'identifiant de la clé est différent et un groupe de tunnels correspondant doit être créé sur l'ASA statique avec le bon nom, ce qui augmente également la granularité des politiques qui sont mises en application sur un ASA.

Scénario 2

> **Remarque** : cette configuration n'est possible que si au moins un côté est un routeur.Si les deux extrémités sont des ASA, ce paramétrage ne fonctionnera pas.Dans la version 8.4, l'ASA ne peut pas utiliser le nom de domaine complètement qualifié (Fully Qualified Domain Name,FQDN) avec la commande set peer (paramétrage du pair),
> mais l'amélioration CSCus37350 a été demandée pour des versions futures.

Si l'adresse IP de l'ASA distant est également dynamique et a cependant un nom de domaine complètement qualifié attribué à son interface VPN, alors plutôt que définir l'adresse IP de l'ASA

distant, vous définissez maintenant le FQDN de l'ASA distant avec cette commande sur le routeur :

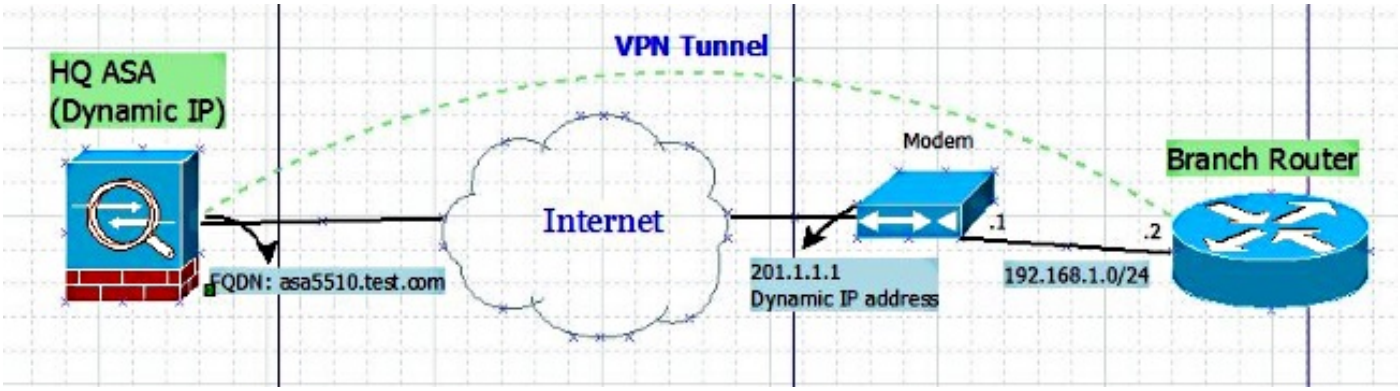
```
C1941(config)#do show run | sec crypto map

crypto map vpn 10 ipsec-isakmp
 set peer <FQDN> dynamic
```

Astuce :Le mot-clé dynamique est facultatif.Quand vous spécifiez l'adresse Internet d'un pair distant d'IPsec par l'intermédiaire de la commande set peer (paramétrage du pair), vous pouvez également émettre le mot clé dynamique, qui reporte la résolution du nom de domaine du serveur DNS de l'adresse Internet juste avant que le tunnel IPsec ait été établi.

Le report de la résolution permet au logiciel de Cisco IOS de détecter si l'adresse IP du pair d'IPsec distant a changé.Ainsi, le logiciel peut contacter le pair à la nouvelle adresse IP.Si le mot clé dynamique n'est pas émis, l'adresse Internet est résolue juste après qu'elle est spécifiée.Ainsi, le logiciel d'exploitation Cisco IOS ne peut pas détecter une modification d'adresse IP et, en conséquence, tente de se connecter à l'adresse IP qu'elle a précédemment résolue.

Diagramme du réseau



Configuration

Configuration dynamique ASA

La configuration sur l'ASA est identique à la [configuration statique ASA à la seule exception, que l'adresse IP sur l'interface physique ne soit pas statiquement définie.]

Configuration du routeur

```
crypto ikev2 keyring L2L-Keyring
 peer vpn
 hostname asa5510.test.com
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
```

```
 !
crypto ikev2 profile L2L-Prof
 match identity remote fqdn domain test.com
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel

crypto map vpn 10 ipsec-isakmp
 set peer asa5510.test.com dynamic
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

ASA statique

- Voici le résultat de la commande**show cryptoIKEv2 SA det :**

```
IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                Remote     Status         Role
120434199        201.1.1.2/4500        201.1.1.1/4500      READY    RESPONDER
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/915 sec
     Session-id: 23
     Status Description: Negotiation done
     Local spi: 97272A4B4DED4A5C       Remote spi: 67E01CB8E8619AF1
     Local id: 201.1.1.2
      Remote id: S2S-IKEv2
     Local req mess id: 43             Remote req mess id: 2
     Local next mess id: 43            Remote next mess id: 2
     Local req queued: 43              Remote req queued: 2
     Local window: 1                   Remote window: 5
     DPD configured for 10 seconds, retry 2
     NAT-T is detected  outside
Child sa: local selector  201.1.1.2/0 - 201.1.1.2/65535
          remote selector 10.10.10.1/0 - 10.10.10.1/65535
          ESP spi in/out: 0x853c02/0x41aa84f4
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

- Voici le résultat de la commande **show crypto ipsec sa :**

```
interface: outside
   Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2

     local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
     remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
     current_peer: 201.1.1.1


     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #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.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
     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: 41AA84F4
     current inbound spi : 00853C02

   inbound esp sas:
     spi: 0x00853C02 (8731650)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 94208, crypto-map: dmap
        sa timing: remaining key lifetime (kB/sec): (4101119/27843)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x0000001F
   outbound esp sas:
     spi: 0x41AA84F4 (1101694196)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel,  NAT-T-Encaps, IKEv2, }
        slot: 0, conn_id: 94208, crypto-map: dmap
        sa timing: remaining key lifetime (kB/sec): (4055039/27843)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Routeur dynamique

- Voici le résultat de la commande **show crypto IKE v2 SA detail :**

```
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1013 sec
     CE id: 1023, Session-id: 23
     Status Description: Negotiation done
     Local spi: 67E01CB8E8619AF1       Remote spi: 97272A4B4DED4A5C
      Local id: S2S-IKEv2
     Remote id: 201.1.1.2
```

```
     Local req msg id:  2              Remote req msg id:  48
     Local next msg id: 2              Remote next msg id: 48
     Local req queued:  2              Remote req queued:  48
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

  IPv6 Crypto IKEv2  SA
```

- Voici le résultat de la commande **show crypto ipsec sa :**

```
interface: GigabitEthernet0/0
   Crypto map tag: vpn, local addr 192.168.1.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
  current_peer 201.1.1.2 port 4500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
   #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
   #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.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
    plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0x853C02(8731650)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0x41AA84F4(1101694196)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0x853C02(8731650)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
       sa timing: remaining key lifetime (k/sec): (4263591/2510)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

    outbound ah sas:
```

```
        outbound pcp sas:
```

Routeur dynamique (avec l'ASA dynamique distante)

- Voici le résultat de la commande **show crypto IKE v2 SA detail :**

```
C1941#show cry ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         192.168.1.2/4500      201.1.1.2/4500        none/none            READY
     Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
     Life/Active Time: 86400/1516 sec
     CE id: 1034, Session-id: 24
     Status Description: Negotiation done
     Local spi: 98322AED6163EE83       Remote spi: 092A1E5620F6AA9C
      Local id: S2S-IKEv2
      Remote id: asa5510.test.com
     Local req msg id:  2              Remote req msg id:  73
     Local next msg id: 2              Remote next msg id: 73
     Local req queued:  2              Remote req queued:  73
     Local window:      5              Remote window:      1
     DPD configured for 0 seconds, retry 0
     Fragmentation not configured.
     Extended Authentication not configured.
     NAT-T is detected inside
     Cisco Trust Security SGT is disabled
     Initiator of SA : Yes

 IPv6 Crypto IKEv2  SA
```

> Remarque:L'ID distant et local dans ce résultat est le groupe de tunnels désigné quevous avez défini sur l'ASA pour vérifier si vous tombez sur le bon groupe de tunnels.Ceci peut également être vérifié si vous déboguerIKEv2 sur une ou l'autre des extrémités.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines **commandes d'affichage.**Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

> Remarque:Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Sur le routeur Cisco IOS, utilisez :

```
deb crypto ikev2 error
deb crypto ikev2 packet
```

```
deb crypto ikev2 internal
```

Sur l'ASA, utilisez :

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```