

Tunnel VPN dynamique du site à site IKEv2 entre une ASA et un exemple de configuration de routeur IOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Scénario 1](#)

[Diagramme du réseau](#)

[Configuration](#)

[Scénario 2](#)

[Diagramme du réseau](#)

[Configuration](#)

[Vérifiez](#)

[ASA statique](#)

[Routeur dynamique](#)

[Routeur dynamique \(avec l'ASA dynamique distante\)](#)

[Dépannez](#)

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 une appliance 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.

[Composants utilisés](#)

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

- Version de Cisco IOS® 15.1(1)T ou plus tard
- 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. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Ce document discute ces scénarios :

- [Scénario 1](#) : Une ASA est configurée avec une adresse IP statique qui utilise un groupe Désigné de tunnel et le routeur est configuré avec une adresse IP dynamique.
- [Scénario 2](#) : Une ASA est configurée avec une adresse IP dynamique et le routeur est configuré avec une adresse IP dynamique.
- [Scénario 3](#) : Ce scénario n'est pas discuté ici. Dans ce scénario, l'ASA est configurée avec une adresse IP statique mais utilise le groupe de tunnel DefaultL2LGroup. La configuration pour ceci est semblable à ce qui est décrit dans le [tunnel VPN dynamique du site à site IKEv2 entre l'article d'exemple de configuration 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 que le nom de groupe de tunnel configuré sur l'ASA. Ceci est accompli avec cette commande sur le routeur :

```
identity local key-id <name of the tunnel-group on the static ASA>
```

L'avantage d'utiliser les groupes Désignés de tunnel sur l'ASA statique est que quand le DefaultL2LGroup est utilisé, la configuration sur les ASA/Routeurs dynamiques distants, qui inclut les clés pré-partagées, doit être identique et il ne tient pas compte de beaucoup de finesse avec l'installation des stratégies.

Configurez

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 la même manière que vous configurez normalement dans les cas où le routeur est un site dynamique pour le tunnel IKEv2 L2L en plus d'une commande comme affiché 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, le clé-id est différent et un groupe de tunnels correspondant doit être créé sur l'ASA statique avec le bon nom, qui augmente également la finesse des politiques qui sont mis en application sur une ASA.

Scénario 2

Note: Cette configuration est seulement possible quand au moins un côté est un routeur. Si les deux côtés sont des ASA, cette installation ne fonctionne pas à ce moment. Dans la version 8.4, l'ASA ne peut pas utiliser le Fully Qualified Domain Name (FQDN) avec l'ordre de **pair de positionnement**, mais l'amélioration [CSCus37350](#) a été demandée pour des versions futures.

Si l'adresse IP du distant l'ASA est dynamique aussi bien cependant a un nom de domaine complet assigné pour son interface VPN, alors plutôt que définissent l'adresse IP du distant ASA, vous définissent maintenant le FQDN du distant ASA avec cette commande sur le routeur :

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

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

Conseil : Le mot clé **dynamique** est facultatif. Quand vous spécifiez l'adresse Internet d'un pair distant d'IPsec par l'intermédiaire de l'ordre de **pair de positionnement**, vous pouvez également émettre le mot clé dynamique, qui reporte la résolution de Domain Name Server (DN) de l'adresse Internet jusqu'à ce que juste avant IPsec le tunnel ait été établi.

La résolution de report permet au logiciel de Cisco IOS de la détecter si l'adresse IP du pair d'IPsec de 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 de Cisco IOS ne peut pas détecter une modification et, en conséquence, des tentatives d'adresse IP 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 que la [configuration statique ASA](#) à seulement une exception, qui est que l'adresse IP sur l'interface physique n'est 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
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

ASA statique

- Voici le résultat de la **crypto** commande de **det d'IKEv2 SA d'exposition** :

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 de **show crypto ipsec sa** :

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
```

Routeur dynamique

- Voici le résultat de la **crypto** commande de **détail d'IKEv2 SA d'exposition** :

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/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 de **show crypto ipsec sa** :

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/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

Routeur dynamique (avec l'ASA dynamique distante)

- Voici le résultat de la **crypto** commande de **détail d'IKEv2 SA d'exposition** :

```
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
```

Note: L'ID distant et local dans cette sortie est le **groupe de tunnels Désigné** que vous avez défini sur l'ASA pour vérifier si vous tombez sur le bon groupe de tunnels. Ceci peut également être vérifié si vous mettez au point IKEv2 sur l'un ou l'autre d'extrémité.

Dépannez

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

[L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Note: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Sur le routeur Cisco IOS, utilisation :

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

Sur l'ASA, utilisation :

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