Configuration d'un tunnel IPSec IKEv1 site à site entre ASA et le routeur Cisco IOS XE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - Diagramme du réseau
  - Configuration ASA
    - Configurer les interfaces ASA
    - Configurer la politique IKEv1 et activer IKEv1 sur l'interface externe
    - Configurer le groupe de tunnels (profil de connexion LAN à LAN)
    - Configurer l'ACL pour le trafic VPN d'intérêt
    - Configurer une exemption de NAT
    - Configurer l'ensemble de transformation IKEv1
    - Configurer une carte cryptographique et l'appliquer à une interface
    - Configuration finale de l'ASA
  - Configuration CLI du routeur Cisco IOS XE
    - Configurer les interfaces
    - Configurer la politique ISAKMP (IKEv1)
    - Configurer une clé de chiffrement ISAKMP
    - Configurer une ACL pour le trafic VPN d'intérêt
    - Configurer une exemption de NAT
    - Configurer un ensemble de transformation
    - Configurer une carte cryptographique et l'appliquer à une interface
    - Configuration finale de Cisco IOS XE
- Vérifier
  - Vérification de la phase 1
  - Vérification de la phase 2
  - Vérification des phases 1 et 2
- Dépannage
  - Outil de contrôle IPSec LAN à LAN
  - Débogage de l'ASA
  - Débogages du routeur Cisco IOS XE
- Références

Introduction

Ce document décrit comment configurer un tunnel de site à site IKEv1 via l'interface de ligne de commande entre un Cisco ASA et un routeur qui exécute le logiciel Cisco IOS® XE.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco IOS® XE
- Appareil de sécurité adaptatif Cisco (ASA)
- Concepts généraux d'IPSec

Composants utilisés

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

- Cisco ASAv exécutant la version 9.20(2)2 du logiciel Cisco
- Cisco CSRv exécutant le logiciel Cisco IOS® XE Version 17.03.03

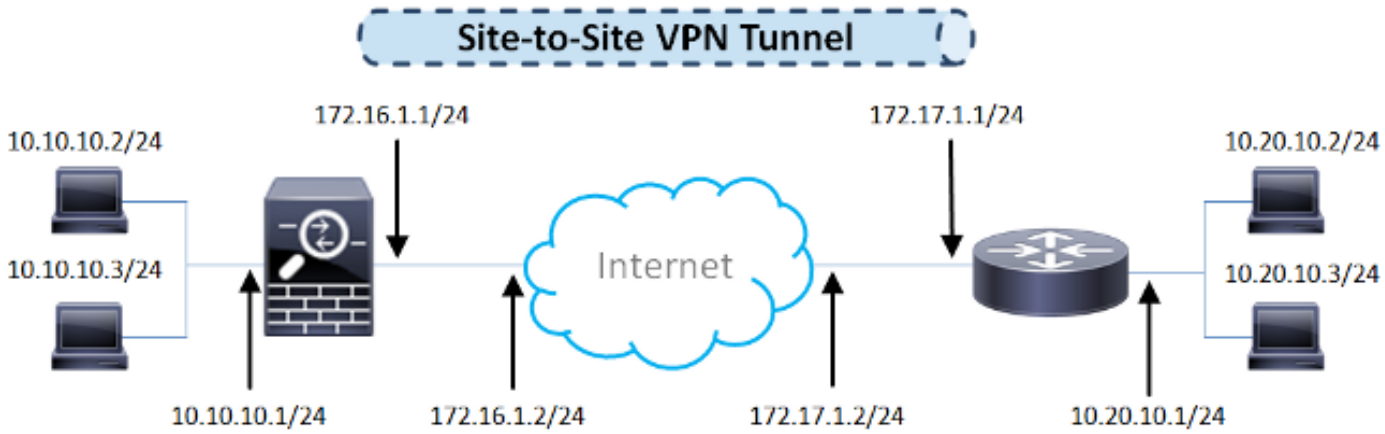
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Cette section décrit comment effectuer les configurations CLI des routeurs ASA et Cisco IOS® XE.

Diagramme du réseau

Le présent document utilise cette configuration de réseau :



Configuration ASA

Configurer les interfaces ASA

Si les interfaces ASA ne sont pas configurées, assurez-vous de configurer au moins les adresses IP, les noms d'interface et les niveaux de sécurité :

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

Remarque : Assurez-vous qu'il existe une connectivité aux réseaux internes et externes, en particulier à l'homologue distant utilisé afin d'établir un tunnel VPN site à site. Vous pouvez utiliser un message ping pour vérifier la connectivité de base.

Configurer la politique IKEv1 et activer IKEv1 sur l’interface externe

Afin de configurer les stratégies ISAKMP (Internet Security Association and Key Management Protocol) pour les connexions IPSec IKEv1 (Internet Key Exchange Version 1), entrez la`crypto ikev1 policy` commande suivante :

```
<#root>
crypto ikev1 policy 10


 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
```

Remarque : une correspondance de stratégie IKEv1 existe lorsque les deux stratégies des deux homologues contiennent les mêmes valeurs de paramètre d'authentification, de chiffrement, de hachage et Diffie-Hellman. Pour le protocole IKEv1, la politique de l’homologue distant doit également indiquer une durée de vie inférieure ou égale à celle figurant dans la politique envoyée par l’initiateur. Si les durées de vie ne sont pas identiques, l’ASA utilise alors la plus courte.

Remarque : si vous ne spécifiez pas de valeur pour un paramètre de stratégie donné, la valeur par défaut est appliquée.

Vous devez activer le protocole IKEv1 sur l'interface qui met fin au tunnel VPN. En général, il s'agit de l'interface externe (ou publique). Afin d'activer IKEv1, entrez la`crypto ikev1 enable` commande en mode de configuration globale :

```
<#root>

crypto ikev1 enable outside
```

Configurer le groupe de tunnels (profil de connexion LAN à LAN)

Pour un tunnel LAN à LAN, le type de profil de connexion est`ipsec-l2l`. `tunnel-group ipsec-attributes`Afin de configurer la clé prépartagée IKEv1, passez en mode de configuration :

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

Configurer l'ACL pour le trafic VPN d'intérêt

L'ASA utilise des listes de contrôle d'accès (ACL) afin de différencier le trafic qui doit être protégé par cryptage IPSec du trafic qui ne nécessite pas de protection. Il protège les paquets sortants qui correspondent à un moteur de contrôle des applications (ACE) et veille à ce que les paquets entrants qui correspondent à un permis ACE soient protégés.

```
<#root>

object-group network

local-network


 network-object 10.10.10.0 255.255.255.0
object-group network

remote-network
```

```
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group

local-network


 object-group

remote-network
```

Remarque : une liste de contrôle d'accès pour le trafic VPN utilise les adresses IP source et de destination après la traduction d'adresses réseau (NAT).

Remarque : Une ACL pour le trafic VPN doit être mise en miroir sur les deux homologues VPN.

Remarque : s'il est nécessaire d'ajouter un nouveau sous-réseau au trafic protégé, il vous suffit d'ajouter un sous-réseau/hôte au groupe d'objets correspondant et de modifier le miroir sur l'homologue VPN distant.

Configurer une exemption de NAT

Remarque : La configuration décrite dans cette section est facultative.

En général, aucune fonction NAT ne doit être exécutée sur le trafic VPN. Pour exempter ce trafic, vous devez créer une règle de NAT d’identité. La règle de NAT d’identité traduit simplement une adresse à la même adresse.

```
<#root>

nat (inside,outside) source static

local-network local-network

 destination static


remote-network remote-network

 no-proxy-arp route-lookup
```

Configurer l’ensemble de transformation IKEv1

Un ensemble de transformation IKEv1 est une combinaison de protocoles de sécurité et d'algorithmes qui définissent la façon dont l'ASA protège les données. Lors des négociations de l'association de sécurité IPSec (SA), les homologues doivent cibler un ensemble de transformation ou une proposition, identique pour les deux homologues. L'ASA applique ensuite l'ensemble de transformation ou la proposition correspondante afin de créer un SA qui protège les flux de données dans la liste d'accès pour cette carte cryptographique.

Afin de configurer le jeu de transformation IKEv1, entrez la`crypto ipsec ikev1 transform-set`commande suivante :

<#root>

```
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
```

Configurer une carte cryptographique et l'appliquer à une interface

Une carte cryptographique détermine une politique IPSec à négocier dans le SA d'IPSec et comprend ce qui suit :

- Une liste d'accès servant à déterminer les paquets que permet et protège la connexion IPSec;
- L'identification des homologues;
- Une adresse locale pour le trafic IPSec;
- Les ensembles de transformation IKEv1.
- Secret de transmission parfait (facultatif)

Voici un exemple :

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
```

Vous pouvez ensuite appliquer la carte cryptographique à l'interface :

<#root>

```
crypto map outside_map interface outside
```

Configuration finale de l’ASA

Voici la configuration finale de l'ASA :

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
 object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
 static remote-network remote-network no-proxy-arp route-lookup
!
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
!
crypto ikev1 enable outside
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
crypto map outside_map interface outside
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
!
```

Configuration CLI du routeur Cisco IOS XE

Configurer les interfaces

Si les interfaces du routeur Cisco IOS XE ne sont pas encore configurées, vous devez au moins configurer les interfaces LAN et WAN. Voici un exemple :

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 no shutdown
```

Assurez-vous qu'il existe une connectivité aux réseaux internes et externes, en particulier à l'homologue distant utilisé afin d'établir un tunnel VPN site à site. Vous pouvez utiliser un message ping pour vérifier la connectivité de base.

Configurer la politique ISAKMP (IKEv1)

Afin de configurer les stratégies ISAKMP pour les connexions IKEv1, entrez la`crypto isakmp policy` commande en mode de configuration globale. Voici un exemple :

```
<#root>
crypto isakmp policy 10

 encryption aes 256
 hash sha
 authentication pre-share
 group 14
```

Remarque : vous pouvez configurer plusieurs stratégies IKE sur chaque homologue participant à IPSec. Lorsque la négociation IKE commence, elle tente de trouver une politique commune qui est configurée sur les deux homologues, et elle commence par les politiques ayant la plus haute priorité, lesquelles sont précisées sur l’homologue distant.

Configurer une clé de chiffrement ISAKMP

Afin de configurer une clé d'authentification pré-partagée, entrez la commande`crypto isakmp key`en mode de configuration globale :

<#root>

crypto isakmp key cisco123 address 172.16.1.1

Configurer une ACL pour le trafic VPN d’intérêt

Utilisez la liste d'accès étendue ou nommée afin de spécifier le trafic qui doit être protégé par le chiffrement. Voici un exemple :

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Remarque : une liste de contrôle d'accès pour le trafic VPN utilise les adresses IP source et de destination après NAT.

Remarque : Une ACL pour le trafic VPN doit être mise en miroir sur les deux homologues VPN.

Configurer une exemption de NAT

Remarque : La configuration décrite dans cette section est facultative.

En général, aucune fonction NAT ne doit être exécutée sur le trafic VPN. Si la surcharge NAT est utilisée, alors une route-map doit être utilisée afin d'exempter le trafic VPN d'intérêt de la traduction. Notez que dans la liste d'accès utilisée dans la route-map, le trafic VPN d'intérêt doit être refusé.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

Configurer un ensemble de transformation

Afin de définir un jeu de transformation IPSec (une combinaison acceptable de protocoles et d'algorithmes de sécurité), entrez la commande du mode de configuration globale (crypto ipsec transform-set, en anglais). Voici un exemple :

<#root>

```
crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac

 mode tunnel
```

Configurer une carte cryptographique et l’appliquer à une interface

Pour créer ou modifier une entrée de carte cryptographique et saisir le mode de configuration de la carte cryptographique, entrez la commande de configuration globale crypto map. Pour que l’entrée de la carte cryptographique soit complète, certains aspects doivent être réglés au minimum :

- Les homologues IPSec auxquels le trafic protégé peut être transféré doivent être définis. Il s’agit des homologues avec lesquels une SA peut être établie. Afin de spécifier un homologue IPSec dans une entrée de crypto-carte, entrez la commandeset peer.
- Les ensembles de transformation pouvant être utilisés avec le trafic protégé doivent être définis. Afin de spécifier les jeux de transformation qui peuvent être utilisés avec l'entrée de crypto-carte, entrez la commandeset transform-set.
- Le trafic qui doit être protégé doit être défini. Afin de spécifier une liste d'accès étendue pour une entrée de crypto-carte, entrez la commandematch address.

Voici un exemple :

<#root>

```
crypto map outside_map 10 ipsec-isakmp

 set peer 172.16.1.1
 set transform-set ESP-AES256-SHA
 match address 110
```

La dernière étape consiste à appliquer l’ensemble de cartes cryptographiques précédemment défini à une interface. Afin d'appliquer ceci, entrez la commande de configuration d'crypto map'interface :

<#root>

```
interface GigabitEthernet0/0

crypto map outside_map
```

Configuration finale de Cisco IOS XE

Voici la configuration finale de l'interface de ligne de commande du routeur Cisco IOS XE :

```
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES256-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
```

```
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

Vérifier

Avant de vérifier si le tunnel est actif et s'il transmet le trafic, vous devez vous assurer que le trafic d'intérêt est envoyé vers le routeur ASA ou le routeur Cisco IOS XE.

Remarque : sur l'ASA, l'outil Packet Tracer qui correspond au trafic d'intérêt peut être utilisé afin d'initier le tunnel IPSec (comme`packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed`par exemple).

Vérification de la phase 1

Pour vérifier si la phase 1 d'IKEv1 est en fonction sur l'ASA, saisissez la commande show crypto isakmp sa. Le résultat attendu est de voir l'`MM_ACTIVE`état :

<#root>

```
ciscoasa#
```

show crypto isakmp 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: 172.17.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Afin de vérifier si l'IKEv1 Phase 1 est actif sur Cisco IOS XE, entrez la commande`show crypto isakmp sa`. Le résultat attendu est de voir l'`ACTIVE`état :

<#root>

```
Router#

show crypto isakmp sa


IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           2003 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Vérification de la phase 2

show crypto ipsec saAfin de vérifier si IKEv1 Phase 2 est actif sur l'ASA, entrez la commande . On s'attend ici à voir à la fois l'index de paramètre de sécurité (SPI) entrant et sortant. Si le trafic passe par le tunnel, vous devez voir les compteurs encaps/decaps augmenter.

Remarque : Pour chaque entrée de liste de contrôle d'accès, une SA entrante/sortante distincte est créée, ce qui peut entraîner une longue sortie de commande (en fonction du nombre d'entrées ACE dans la liste de contrôle d'accès de chiffrement).show crypto ipsec sa

---

Voici un exemple :

<#root>

```
ciscoasa#

show crypto ipsec sa peer 172.17.1.1


peer address: 172.17.1.1
    Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
   10.20.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 989, #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.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 5397114D
current inbound spi : 9B592959

inbound esp sas:
spi: 0x9B592959 (2606311769)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFD7FF

outbound esp sas:
spi: 0x5397114D (1402409293)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa#
```

Afin de vérifier si IKEv1 Phase 2 est actif sur Cisco IOS XE, entrez la commande IKEv1 Phase`show crypto ipsec sa`2. On s'attend ici à voir à la fois le SPI entrant et sortant. Si le trafic passe par le tunnel, vous devez voir les compteurs encaps/decaps augmenter.

Voici un exemple :

<#root>

```
Router#
```

`show crypto ipsec sa peer 172.16.1.1`

```
interface: GigabitEthernet0/0
    Crypto map tag: outside_map, local addr 172.17.1.1

   protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
```

```
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#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.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet3
current outbound spi: 0x9B592959(2606311769)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x5397114D(1402409293)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607857/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x9B592959(2606311769)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607901/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Router#
```

Vérification des phases 1 et 2

Cette section décrit les commandes que vous pouvez utiliser sur ASA ou Cisco IOS XE afin de vérifier les détails des phases 1 et 2.

Entrez la commande`show vpn-sessiondb`sur l'ASA pour la vérification :

<#root>

```
ciscoasa#
```

show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

```
Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                     IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 98900               Bytes Rx     : 134504
Login Time   : 06:15:52 UTC Fri Sep 6 2024
Duration     : 0h:15m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 2.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 84093 Seconds
  D/H Group    : 14
  Filter Name  :

IPsec:
  Tunnel ID    : 2.2
  Local Addr   : 10.10.10.0/255.255.255.0/0/0
  Remote Addr  : 10.20.10.0/255.255.255.0/0/0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3293 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607901 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 26 Minutes
  Bytes Tx     : 98900                 Bytes Rx     : 134504
  Pkts Tx      : 989                   Pkts Rx      : 989

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 309 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :

ciscoasa#
```

Entrez la commande`show crypto session`sur Cisco IOS XE pour la vérification :

```
<#root>

Router#

show crypto session remote 172.16.1.1 detail
```

```
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 172.16.1.1
      Desc: (none)
  IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
          Capabilities:(none) connid:1005 lifetime:23:56:23
  IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 989 drop 0 life (KB/Sec) 4449870/3383
        Outbound: #pkts enc'ed 989 drop 0 life (KB/Sec) 4449868/3383

Router#
```

Dépannage

Cette section fournit des renseignements qui vous permettront de régler les problèmes de configuration.

Remarque : consultez les documents Cisco Informations importantes sur les commandes de débogage et le dépannage de la sécurité IP - Présentation et utilisation des commandes de débogage avant d'utiliser desdebugcommandes.

Outil de contrôle IPSec LAN à LAN

Afin de vérifier automatiquement si la configuration IPSec LAN-to-LAN entre l'ASA et Cisco IOS XE est valide, vous pouvez utiliser l'outil IPSec LAN-to-LANChecker. L'outil est conçu de telle sorte qu'il accepte une commandeshow techoushow running-configd'un routeur ASA ou Cisco IOS XE. Il examine la configuration et tente de détecter si un tunnel IPSec LAN à LAN basé sur une carte de chiffrement est configuré. Dans ce cas, il effectue une vérification multipoint de la configuration et met en évidence les paramètres et les erreurs de configuration qui concernent le tunnel faisant l'objet de la négociation.

Débogage de l'ASA

Afin de dépanner la négociation de tunnel IPSec IKEv1 sur un pare-feu ASA, vous pouvez utiliser cesdebugcommandes :

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

Remarque : Si le nombre de tunnels VPN sur l'ASA est significatif, la`debug crypto condition peer A.B.C.D`commande doit être utilisée avant d'activer les débogages afin de limiter les sorties de débogage pour inclure uniquement l'homologue spécifié.

Débogages du routeur Cisco IOS XE

Afin de dépanner la négociation de tunnel IPSec IKEv1 sur un routeur Cisco IOS XE, vous pouvez utiliser ces commandes de débogage :

<#root>

```
debug crypto ipsec
debug crypto isakmp
```

Remarque : Si le nombre de tunnels VPN sur le Cisco IOS XE est significatif, le`debug crypto condition peer ipv4 A.B.C.D`doit être utilisé avant d'activer les débogages afin de limiter les sorties de débogage pour inclure uniquement l'homologue spécifié.

Conseil : Consultez le document Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions [Les solutions de dépannages les plus courantes pour l'accès à distance et la connexion L2L au VPN d'IPSec] de Cisco pour avoir plus d'informations sur le dépannage d'un VPN de site à site.

Références

- Informations importantes sur les commandes debug
- Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage
- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Outil de contrôle IPSec LAN à LAN
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.