Configurez un tunnel d'IPSec IKEv1 de site à site entre une ASA et un routeur Cisco IOS

Contenu

Introduction

Ce document décrit comment configurer un tunnel de la version 1 d'échange de clés Internet (IKE) d'IPSec de site à site (entre réseaux locaux) (IKEv1) par l'intermédiaire du CLI entre une appliance de sécurité adaptable Cisco (ASA) et un routeur qui exécute le logiciel de Cisco IOS®.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- **Cisco IOS**
- Cisco ASA
- Concepts du Général IPSec

Composants utilisés

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

- Gamme Cisco 5512-X ASA qui exécute la version de logiciel 9.4(1)
- L'Integrated Services Router de gamme Cisco 1941 (ISR) ce exécute la version de logiciel 15.4(3)M2 de Cisco IOS

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.

Configurez

Cette section décrit comment des configurations CLI se terminer ASA et IOS routeur.

Diagramme du réseau

Les informations dans ce document utilisent cette configuration réseau :

Configuration ASA

Configurez les interfaces ASA

Si les interfaces ASA ne sont pas configurées, assurez-vous que vous configurez au moins les adresses IP, reliez les noms, et les Sécurité-niveaux :

```
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 y a de Connectivité à l'interne et aux réseaux externes, et particulièrement au pair distant qui sera utilisé afin d'établir un tunnel VPN de site à site. Vous pouvez employer un ping afin de vérifier la Connectivité de base.

Configurez la stratégie IKEv1 et activez IKEv1 sur l'interface extérieure

Afin de configurer les stratégies de Protocole ISAKMP (Internet Security Association and Key Management Protocol) pour les connexions IKEv1, sélectionnez la **crypto** commande de **<priority> de la stratégie ikev1** :

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

> **Remarque:** Une correspondance de la stratégie IKEv1 existe quand chacun des deux stratégies des deux pairs des valeurs contiennent la mêmes authentification, cryptage, informations parasites, et de Diffie-Hellman paramètre. Pour IKEv1, la stratégie distante de pair doit également spécifier une vie inférieur ou égal à la vie dans la stratégie que le demandeur envoie. Si les vies ne sont pas identiques, alors l'ASA utilise la vie plus courte.

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

Vous devez activer IKEv1 sur l'interface qui termine le tunnel VPN. Typiquement, c'est l'interface extérieure (ou *public*). Afin d'activer IKEv1, sélectionnez la **crypto** commande de **<interface-name> de l'enable ikev1** en mode de configuration globale :

```
crypto ikev1 enable outside
```

Configurez le groupe de tunnel (le profil de connexion entre réseaux locaux)

Pour un tunnel entre réseaux locaux, le type de profil de connexion est **ipsec-l2l**. Afin de configurer la clé pré-partagée IKEv1, écrivez le mode de configuration d'ipsec-*attributs de groupe de tunnels* :

```
crypto ikev1 enable outside
```

Configurez l'ACL pour le trafic VPN d'intérêt

L'ASA emploie le Listes de contrôle d'accès (ACL) afin de différencier le trafic qui devrait être protégé avec le chiffrement IPSec contre le trafic qui n'exige pas la protection. Il protège les paquets sortants qui apparient une engine de contrôle d'application d'autorisation (ACE) et s'assure que les paquets entrant qui apparient une autorisation ACE ayez la protection.

```
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:** Un ACL pour le trafic VPN utilise la source et les adresses IP de destination après Traduction d'adresses de réseau (NAT).

> **Remarque:** Un ACL pour le trafic VPN doit être reflété sur chacun des deux homologues VPN.

> **Remarque:** S'il y a un besoin d'ajouter un nouveau sous-réseau au trafic protégé, d'ajouter simplement un sous-réseau/hôte au groupe d'objets respectif et de se terminer une modification de miroir sur l'homologue VPN distant.

Configurez un nat exemption

> Remarque: La configuration qui est décrite dans cette section est facultative.

Typiquement, il devrait n'y avoir pas de NAT exécuté sur le trafic VPN. Afin d'exempter ce trafic, vous devez créer une règle NAT d'identité. La règle NAT d'identité traduit simplement une adresse à la même adresse.

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

Configurez le jeu de transformations IKEv1

Un jeu de transformations IKEv1 est une combinaison des protocoles de Sécurité et des algorithmes qui définissent la manière dont l'ASA protège des données. Pendant les négociations de l'association de sécurité IPSec (SA), les pairs doivent identifier un jeu de transformations ou une proposition qui est identiques pour chacun des deux pairs. L'ASA applique alors le jeu de transformations ou la proposition apparié afin de créer SA qui protège des flux de données dans la liste d'accès pour ce crypto map.

Afin de configurer le jeu de transformations IKEv1, sélectionnez la **crypto** commande de **transform-set de l'ipsec ikev1** :

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

Configurez un crypto map et appliquez-le à une interface

Un crypto map définit une stratégie IPSec à négocier à IPSec SA et l'inclut :

- Une liste d'accès afin d'identifier les paquets que la connexion d'IPSec permet et protège
- Identification de pair
- Une adresse locale pour le trafic d'IPSec
- Les jeux de transformations IKEv1

Voici un exemple :

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

Vous pouvez alors appliquer le crypto map à l'interface :

```
crypto map outside_map interface outside
```

Configuration finale ASA

Voici la configuration finale sur l'ASA :

```
crypto map outside_map interface outside
```

Configuration CLI de routeur IOS

Configurez les interfaces

Si les interfaces de routeur IOS ne sont pas encore configurées, alors au moins les interfaces de LAN et WAN devraient être configurées. Voici un exemple :

```
crypto map outside_map interface outside
```

Assurez-vous qu'il y a de Connectivité à l'interne et aux réseaux externes, et particulièrement au pair distant qui sera utilisé afin d'établir un tunnel VPN de site à site. Vous pouvez employer un ping afin de vérifier la Connectivité de base.

Configurez la stratégie de l'ISAKMP (IKEv1)

Afin de configurer les stratégies ISAKMP pour les connexions IKEv1, sélectionnez la commande de **<priority> de crypto isakmp policy** en mode de configuration globale. Voici un exemple :

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

Remarque: Vous pouvez configurer de plusieurs stratégies IKE sur chaque pair qui participe

à IPSec. Quand la négociation d'IKE commence, elle tente de trouver une stratégie commune qui est configurée sur chacun des deux pairs, et elle commence par les stratégies les plus prioritaires qui sont spécifiées sur le pair distant.

Configurez un crypto isakmp key

Afin de configurer une clé *preshared d'*authentification, sélectionnez la commande de **crypto isakmp key** en mode de configuration globale :

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configurez un ACL pour le trafic VPN d'intérêt

Employez la liste d'accès étendue ou Désignée afin de spécifier le trafic qui devrait être protégé par cryptage. Voici un exemple :

```
crypto isakmp key cisco123 address 172.16.1.1
```

Remarque: Un ACL pour le trafic VPN utilise la source et les adresses IP de destination après NAT.

Remarque: Un ACL pour le trafic VPN doit être reflété sur chacun des deux homologues VPN.

Configurez un nat exemption

Remarque: La configuration qui est décrite dans cette section est facultative.

Typiquement, il devrait n'y avoir pas de NAT exécuté sur le trafic VPN. Si la surcharge NAT est utilisée, alors un route-map devrait être utilisé afin d'exempter le trafic VPN d'intérêt de la traduction. Notez que dans la liste d'accès qui est utilisée dans le route-map, le trafic VPN d'intérêt devrait être refusé.

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configurez un jeu de transformations

Afin de définir un jeu de transformations d'IPSec (une combinaison acceptable des protocoles et des algorithmes de Sécurité), sélectionnez la commande de **crypto ipsec transform-set** en mode de configuration globale. Voici un exemple :

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

Configurez un crypto map et appliquez-le à une interface

Afin de créer ou modifier une entrée de crypto map et écrire le mode de configuration de crypto

map, sélectionnez la commande de configuration globale de **crypto map**. Afin de l'entrée de crypto map soyez complète, là sont quelques aspects qui doivent être définis à un minimum :

- L'IPsec scrute à ce que le trafic protégé peut être expédié doit être défini. Ce sont les pairs avec lesquels SA peut être établie. Afin de spécifier un pair d'IPSec dans une entrée de crypto map, sélectionnez la commande de **pair de positionnement**.
- Les jeux de transformations qui sont acceptables pour l'usage avec le trafic protégé doivent être définis. Afin de spécifier les jeux de transformations qui peuvent être utilisés avec l'entrée de crypto map, sélectionnez la commande de **set transform-set**.
- Le trafic qui devrait être protégé doit être défini. Afin de spécifier une liste d'accès étendue pour une entrée de crypto map, sélectionnez la commande d'**adresse de correspondance**.

Voici un exemple :

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

La dernière étape est d'appliquer le crypto map précédemment défini réglé à une interface. Afin d'appliquer ceci, sélectionnez la commande de configuration d'interface de **crypto map** :

```
interface GigabitEthernet0/0
crypto map outside_map
```

Configuration finale IOS

Voici la configuration CLI de routeur IOS de finale :

```
interface GigabitEthernet0/0
crypto map outside_map
```

Vérifiez

Avant que vous le vérifiiez si le tunnel est haut et celui passe le trafic, vous devez s'assurer que le trafic d'intérêt est envoyé vers l'ASA ou le routeur IOS.

> **Remarque:** Sur l'ASA, l'outil de traceur de paquets qui s'assortit le trafic d'intérêt peut être utilisé afin d'initier le tunnel d'IPSec (tel que le **traceur de paquets entré à l'intérieur de TCP 10.10.10.10 12345 10.20.10.10 80 détaillé** par exemple).

Vérification de Phase 1

Afin de vérifier si le Phase 1 IKEv1 est en hausse sur l'ASA, sélectionnez la commande de **show crypto isakmp sa**. La sortie prévue est de voir l'état **MM_ACTIVE** :

```
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 le Phase 1 IKEv1 est en hausse sur l'IOS, sélectionnez la commande de **show crypto isakmp sa**. La sortie prévue est de voir l'**état active** :

```
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           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Vérification de Phase 2

Afin de vérifier si le Phase 2 IKEv1 est en hausse sur l'ASA, sélectionnez la commande de **show crypto ipsec sa**. La sortie prévue est de voir l'index d'arrivée et sortant de paramètre de Sécurité (SPI). Si le trafic traverse le tunnel, vous devriez voir les encaps/compteurs de decaps incrémenter.

> **Remarque:** Pour chaque rubrique de liste ACL il y a SA d'arrivée/sortante distincte créée, qui pourrait avoir comme conséquence une longue sortie de commande de **show crypto ipsec sa** (dépendante sur le nombre d'entrées d'ACE dans le crypto ACL).

Voici un exemple :

```
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: 1005, #pkts encrypt: 1005, #pkts digest: 1005
      #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #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: 8A9FE619
     current inbound spi : D8639BD0

    inbound esp sas:
      spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

Afin de vérifier si le Phase 2 IKEv1 est en hausse sur l'IOS, sélectionnez la commande de **show crypto ipsec sa**. La sortie prévue est de voir le SPI d'arrivée et sortant. Si le trafic traverse le tunnel, vous devriez voir les encaps/compteurs de decaps incrémenter.

Voici un exemple :

```
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: 2024, #pkts encrypt: 2024, #pkts digest: 2024
    #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
```

```
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

     outbound esp sas:
      spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

Phase 1 et vérification 2

Cette section décrit les commandes que vous pouvez utiliser sur l'ASA ou l'IOS afin de vérifier les détails pour les deux Phase 1 et 2.

Sélectionnez la commande de **VPN-sessiondb d'exposition** sur l'ASA pour la vérification :

```
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)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m: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   : AES128                Hashing      : SHA1
 Rekey Int (T): 86400 Seconds         Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 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   : AES128                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     : 100500                 Bytes Rx     : 101400
 Pkts Tx      : 1005                   Pkts Rx      : 1014

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#
```

Sélectionnez la commande de **show crypto session** sur l'IOS pour la vérification :

```
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 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

Dépannez

Cette section fournit les informations que vous pouvez employer afin de dépanner votre configuration.

> **Remarque:** Référez-vous aux informations importantes sur des commandes de debug et le dépannage de sécurité IP - en comprenant et en utilisant des documents Cisco de commandes de débogage avant que vous utilisiez des commandes de **débogage**.

Outil de contrôleur d'entre réseaux locaux d'IPSec

Afin de vérifier automatiquement si la configuration entre réseaux locaux d'IPSec entre l'ASA et l'IOS est valide, vous pouvez utiliser l'outil de contrôleur d'entre réseaux locaux d'IPSec. L'outil est conçu de sorte qu'il reçoive un **tech** ou une **commande show running-config d'exposition d'un** routeur ASA ou IOS. Il examine la configuration et les tentatives de détecter si un crypto tunnel à base de cartes d'IPSec d'entre réseaux locaux est configuré. Si configuré, il exécute un contrôle multipoint de la configuration et met en valeur n'importe quelles erreurs et configurations de configuration pour le tunnel qui serait négocié.

Debugs ASA

Afin de dépanner la négociation de tunnel d'IPSec IKEv1 sur un Pare-feu ASA, vous pouvez utiliser ces commandes de **débogage** :

```
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 **commande du pair A.B.C.D de debug crypto condition** devrait être utilisée avant que vous activiez mette au point afin de limiter les sorties de débogage pour inclure seulement le pair spécifié.

Debugs de routeur IOS

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

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

> **Remarque:** Si le nombre de tunnels VPN sur l'IOS est significatif, l'**ipv4 A.B.C.D de pair de debug crypto condition devrait** être utilisé avant que vous activiez mette au point afin de limiter les sorties de débogage pour inclure seulement le pair spécifié.

> **Conseil** : Référez-vous au L2L et au document Cisco de solutions de dépannage VPN d'IPSec d'Accès à distance les plus communs pour plus d'informations sur la façon dépanner un site à site VPN.

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
- Contrôleur d'entre réseaux locaux d'IPSec
- Support et documentation techniques - Cisco Systems