Exemple Dynamique-à-statique de configuration ASA-à-ASA IKEv1/IPsec

Contenu

Introduction

Ce document décrit comment permettre à l'appliance de sécurité adaptable (ASA) de recevoir les connexions VPN dynamiques de site à site d'IPsec de n'importe quel pair dynamique (ASA dans ce cas). Pendant que le schéma de réseau dans ce document affiche, le tunnel d'IPsec est établi quand le tunnel est initié de l'extrémité Distant-ASA seulement. La Central-ASA ne peut pas initier un tunnel VPN en raison de la configuration dynamique d'IPsec. L'adresse IP de la Distant-ASA est inconnue.

Configurez la Central-ASA afin de recevoir dynamiquement des connexions d'une adresse IP de caractère d'ambiguité (0.0.0.0/0) et d'une clé pré-partagée de caractère d'ambiguité. La Distant-ASA est alors configurée pour chiffrer le trafic des gens du pays aux sous-réseaux Central-ASA comme spécifiés par la crypto liste d'accès. Les deux côtés effectuent l'exemption de Traduction d'adresses de réseau (NAT) afin de sauter NAT pour le trafic d'IPsec.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur le pare-feu, version 9.x de Cisco ASA (5510 et 5520) et plus tard.

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

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Configuration ASDM

Central-ASA (pair statique)

Sur une ASA avec une adresse IP statique, installez le VPN de telle manière qu'il reçoive les connexions dynamiques d'un pair inconnu tandis qu'il authentifie toujours le pair utilisant une clé IKEv1 pré-partagée :

1. Choisissez la **configuration > le site à site VPN > a avancé > des crypto map.** La fenêtre affiche la liste d'entrées de crypto map qui sont déjà en place (s'il y en a). Puisque l'ASA ne sait pas ce qu'est l'adresse IP de pair, pour que l'ASA reçoive la connexion configurez la Dynamique-**MAP** avec le transform-set assorti (proposition d'IPsec). Cliquez sur **Add**.
2. Dans la fenêtre de règle d'IPsec de création, de la stratégie de tunnel (crypto map) - l'onglet de base, choisissent **dehors de la** liste déroulante d'interface et **dynamique de la** liste déroulante de type de stratégie. Dans le champ de priorité, assignez la priorité pour cette entrée au cas où il y aurait des plusieurs entrées sous la Dynamique-MAP. Ensuite, clic **choisi** à côté du champ de proposition de l'IKE v1 IPsec afin de sélectionner la proposition d'IPsec.
3. Quand la boîte de dialogue choisie de propositions d'IPsec (jeux de transformations) s'ouvre, choisissez parmi les propositions actuelles d'IPsec ou cliquez sur Add afin de créer un neuf et utiliser la même chose. Cliquez sur **OK** quand vous avez terminé.

4. De la stratégie de tunnel (crypto map) - l'onglet Avancé, cochent la case de l'**enable NAT-T** (requise si l'un ou l'autre de pair est derrière un périphérique NAT) et la case de **Reverse Route Injection d'enable**. Quand le tunnel VPN est soulevé pour le pair dynamique, l'ASA installe une artère dynamique pour le réseau VPN distant négocié ces points sur l'interface VPN.Sur option, de l'onglet de sélection du trafic vous pouvez également définir le trafic VPN intéressant pour le pair dynamique et cliquer sur OK. Comme cité précédemment, puisque l'ASA n'a aucune information sur l'adresse IP dynamique distante de pair, la demande de connexion d'inconnu débarque sous DefaultL2LGroup qui existe sur l'ASA par défaut. Pour que l'authentification réussisse la clé pré-partagée (cisco123 dans cet exemple) configurée sur le pair distant doit s'assortir avec un DefaultL2LGroup de dessous.
5. Choisissez la **configuration > le site à site VPN > a avancé > des groupes de tunnel**, sélectionne **DefaultL2LGroup**, clique sur Edit et configure la clé pré-partagée désirée. Cliquez sur **OK** quand vous avez terminé.**Note**: Ceci crée une clé pré-partagée de masque sur le pair statique (Central-ASA). N'importe quels périphérique/pair qui connaît cette clé pré-partagée et ses propositions assorties peut avec succès établir un tunnel VPN et accéder à des ressources au-dessus de VPN. Assurez que cette clé pre-skared n'est pas partagée avec les entités inconnues et n'est pas facile à deviner.
6. Choisissez la **configuration >** le **site à site VPN > stratégies de groupe** et sélectionnez la stratégie de groupe de votre choix (stratégie de groupe par défaut dans ce cas). Cliquez sur Edit et éditez la stratégie de groupe dans la boîte de dialogue interne de stratégie de groupe d'éditer. Cliquez sur **OK** quand vous avez terminé.
7. Choisissez la **configuration >** le **Pare-feu >** les **règles NAT** et de la fenêtre nat de règle d'ajouter, ne configurent une règle (NAT-EXEMPT) pas nat pour le trafic VPN. Cliquez sur **OK** quand vous avez terminé.

Distant-ASA (pair dynamique)

1. Choisissez les **assistants > les assistants VPN > l'assistant du site à site VPN** une fois que l'application ASDM se connecte à l'ASA.
2. Cliquez sur **Next** (Suivant).
3. Choisissez **dehors de la** liste déroulante d'interface d'accès VPN afin de spécifier l'adresse IP extérieure du pair distant. Sélectionnez l'interface (**WAN)** où le crypto map est appliqué. Cliquez sur **Next** (Suivant).
4. Spécifiez les hôtes/réseaux qui devraient être permis pour traverser le tunnel VPN. Dans cette étape, vous devez fournir les réseaux locaux et les réseaux distants pour le tunnel VPN. Cliquez sur les boutons à côté des champs de réseau local et de réseau distant et choisissez l'adresse selon la condition requise. Cliquez sur Next quand vous êtes fait.
5. Écrivez les informations d'authentification pour l'utiliser, qui sont clé pré-partagée dans cet exemple. La clé pré-partagée utilisée dans cet exemple est **cisco123**. Le Tunnel Group Name est l'adresse IP distante de pair par défaut si vous configurez l'entre réseaux locaux (L2L) VPN.**OU**Vous pouvez personnaliser la configuration pour inclure l'IKE et la stratégie d'IPsec de votre choix. Il faut au moins une stratégie assortie entre les pairs :Des méthodes d'authentification tabulez, écrivez la version 1 d'IKE pré-partagée clé dans la zone de tri Pré-partagée. Dans cet exemple, c'est **cisco123**.Cliquez sur l'onglet d'**algorithmes de chiffrement**.
6. Cliquez sur **gèrent** à côté du champ de stratégie IKE, cliquent sur Add et configurent une stratégie IKE faite sur commande **(**phase-1**)**. Cliquez sur **OK** quand vous avez terminé.
7. Cliquez sur **choisi** à côté le du champ de proposition d'IPsec et sélectionnez la proposition

désirée d'IPsec. Cliquez sur Next quand vous êtes fait.Sur option, vous pouvez aller à l'onglet de perfect forward secrecy et cocher la case de **perfect forward secrecy d'enable (PFS)**. Cliquez sur Next quand vous êtes fait.

8. Cochez l'**hôte/réseau exempts de côté ASA de la** case de **traduction d'adresses** afin d'empêcher le trafic du tunnel dès le début de la traduction d'adresses réseau. Choisissez les **gens du pays ou l'intérieur de la** liste déroulante afin de placer l'interface où le réseau local est accessible. Cliquez sur **Next** (Suivant).
9. L'ASDM affiche un résumé du VPN juste configuré. Vérifiez et cliquez sur Finish.

Configuration CLI

Configuration centrale ASA (pair statique)

1. Configurez une règle NO-NAT/NAT-EXEMPT pour le comme indiqué dans cet exemple du trafic VPN :
```
object network 10.1.1.0-remote_network
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network
 subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup
```
2. Configurez la clé pré-partagée sous DefaultL2LGroup afin d'authentifier n'importe quel distant Dynamic-L2L-peer :
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. Définissez la stratégie phase-2/ISAKMP :
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. Définissez le jeu de transformations phase-2/stratégie d'IPsec :
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. Configurez la carte dynamique avec ces paramètres : Transform-set requisActivez l'Injection inversée de routes (RRI), qui permet aux dispositifs de sécurité pour apprendre les informations de routage pour les clients connectés (facultatifs)
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```
6. Liez la carte dynamique au crypto map, appliquez le crypto map et activez ISAKMP/IKEv1 sur l'interface extérieure :
```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside
crypto ikev1 enable outside
```

Distant-ASA (pair dynamique)

1. Configurez une règle de nat exemption pour le trafic VPN :
```
object network 10.1.1.0-inside_network
```

```
subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network
subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup
```

2. Configurez un groupe de tunnels pour un homologue VPN et une clé pré-partagée statiques.
```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```
3. Définissez la stratégie PHASE-1/ISAKMP :
```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```
4. Définissez un jeu de transformations phase-2/stratégie d'IPsec :
`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`
5. Configurez une liste d'accès qui définit le trafic VPN/réseau intéressants :
`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`
6. Configurez le crypto map statique avec ces paramètres : Liste d'accès Crypto/VPNAdresse IP distante de pair d'IPsecTransform-set requis
`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`
7. Appliquez le crypto map et activez ISAKMP/IKEv1 sur l'interface extérieure :
`crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac`

Vérifiez

Employez cette section pour confirmer que la configuration fonctionne correctement.

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.

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair.
- **show crypto ipsec sa** - Affiche tout l'IPsec en cours SAS.

Cette section affiche l'outout de vérification d'exemple pour les deux ASA.

ASA centrale

```
Central-ASA#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: 172.16.1.1
    Type    : L2L             Role    : responder
```

```
    Rekey   : no              State   : MM_ACTIVE

    Central-ASA# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1

        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1

        #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.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      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: 30D071C0
      current inbound spi : 38DA6E51

      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, IKEv1, }
         slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
         sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

DISTANT-ASA

```
Remote-ASA#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: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

```
  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

        #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
      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: 38DA6E51
      current inbound spi : 30D071C0

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 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): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 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): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

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**.

Servez-vous de ces commandes comme montré :

```
Remote-ASA#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: 172.16.2.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

  Remote-ASA#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1

        access-list outside_cryptomap extended permit ip 10.1.1.0
255.255.255.0 10.1.2.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      current_peer: 172.16.2.1

        #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.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0
      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: 38DA6E51
      current inbound spi : 30D071C0

      inbound esp sas:
      spi: 0x30D071C0 (818966976)
         transform: esp-aes-256 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): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x0000001F
    outbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 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): (4373999/28676)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Attention : La commande de **clear crypto isakmp SA** est intrusive car elle efface tous les tunnels VPN actifs.

Dans la version de logiciel 8.0(3) et ultérieures PIX/ASA, IKE individuel SA peut être effacé utilisant le *>command d'IP address de <peer de* **clear crypto isakmp SA**. Dans des versions logicielles plus tôt que 8.0(3), emploient la commande de *<tunnel-group-name> de* **groupe de tunnels de déconnexion de VPN-sessiondb** afin d'effacer l'IKE et l'IPsec SAS pour un tunnel simple.

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

Debugs utilisés :

```
Remote-ASA#vpn-sessiondb logoff tunnel-group 172.16.2.1
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1
```

Distant-ASA (demandeur)

Sélectionnez cette commande de **traceur de paquets** afin d'initier le tunnel :

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed

IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
```

```
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin quick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED


Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
 Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
 Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
:
.
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
:
.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
:
.
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Central-ASA (responder)

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
```

with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
:
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
.
Jan 20 12:42:35 **[IKEv1]IP = 172.16.1.1, Connection landed on tunnel_group
DefaultL2LGroup**
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]**Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED**
:
.
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, **IKE Responder starting QM**:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, **Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0**:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, **Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0**Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 **[IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match**
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
.
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
**Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0**:
.
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE

```
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
.
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0
```

Informations connexes

- Références de commandes de gamme de Cisco ASA
- Page de support de la négociation IPSec/des protocoles IKE
- Demandes de commentaires (RFC)
- Soutien technique et documentation - Système de Cisco