ASA 間、動的静的間 IKEv1/IPsec の設定例

目次

概要

この資料に適応型セキュリティ アプライアンス（ASA）ソフトウェア 有効に なる方法を（ASA）あらゆるダイナミック ピア（ASA この場合）からのダイナミック IPsec Site to Site VPN 接続を許可するために記述されています。 この資料のネットワークダイアグラムが示すと同時に、IPSecトンネルはトンネルがリモート ASA 端だけから開始するとき確立されます。 中央 ASA はダイナミック IPSec構成が理由で VPN トンネルを開始できません。 リモート ASA の IP アドレスは不明です。

動的にワイルド カード IP アドレス（0.0.0.0/0）およびワイルドカード事前共有キーからの接続を許可するために中央 ASA を設定して下さい。 リモート ASA はそれから暗号 access-list によって規定 されるようにローカルから中央 ASA サブネットにトラフィックを暗号化するために設定されます。 両側は IPSecトラフィックのための NAT をバイパスするためにネットワーク アドレス変換（NAT）免除を行います。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

この 文書に記載されている 情報は基づいた on Cisco ASA です（5510 および 5520）ファイアウォールソフトウェアリリース 9.x およびそれ以降。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

> **注:** このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

ASDM の設定

中央 ASA（静的なピア）

静的IP アドレスの ASA で、まだ IKEv1 事前共有キーを使用してピアを認証する間、未知のピアからのダイナミック 接続を許可するように VPN を設定して下さい:

1. **> Site to Site VPN > 進みました > クリプト マップ** 『Configuration』 を選択 して下さい。 ウィンドウは（あれば）既に設定されていている暗号マップエントリのリストを表示します。 ピアIP アドレスがであるもの ASA が認知していないので接続を許可する ASA のために一致する transform-set（IPsec 提案）で**ダイナミック マップを**設定して下さい。 [Add] をクリックします。
2. トンネル ポリシー（クリプト マップ）からの作成 IPsec ルール ウィンドウで、-基本的なタブはインターフェイス ドロップダウン リストから、ポリシーの種類ドロップダウン リストから**ダイナミック**『outside』 を選択 し。 優先順位フィールドでは、複数のエントリがダイナミック マップの下にあったらこのエントリに優先順位を割り当てて下さい。 次に、IPsec 提案を選択するために IKE v1 IPsec 提案フィールドの隣で『SELECT』 をクリック して下さい。
3. 『IPSec』 を選択提案（トランスフォーム セット）ダイアログボックスが開くとき、IPsec 現在の提案間で選択するか、または新しいものを作成し、同じを使用するために『Add』 をクリック して下さい。 完了したら、[OK] をクリックします。
4. トンネル ポリシー（クリプト マップ（必要などちらかのピアが NAT デバイスの後ろにある

場合）)から- Advanced タブは、**イネーブル NAT-T チェックボックス**および**イネーブル Reverse Route Injection** チェックボックスをチェックします。 VPN トンネルがダイナミック ピアのために起動するとき、ASA は VPN インターフェイスにネゴシエートされたリモート VPN ネットワークのためのダイナミックルートをそのポイント インストールします。任意で、トラフィック選択タブからまたダイナミック ピアのための関連した VPN トラフィックを定義し、『OK』 をクリック することができます。 ASA にリモート ダイナミック ピア IP アドレスについての情報がないので上記されるように、未知数接続要求は DefaultL2LGroup の下で上陸しま ASA でデフォルトで存在 します。 認証のためにリモートピアで設定される事前共有キー（この例の cisco123）を成功することは 1 下 DefaultL2LGroup と一致する必要があります。
5. **> Site to Site VPN > 進み、> トンネル グループ**、選択し、**DefaultL2LGroup を**、『Edit』 をクリック し、設定します望ましい事前共有キーを『Configuration』 を選択 して下さい。 完了したら、[OK] をクリックします。**注:** これは静的なピア（中央 ASA）のワイルドカード事前共有キーを作成します。 この事前共有キーおよび一致する提案を知っているデバイス/ピアは VPN トンネルをうまく確立し、VPN 上のリソースにアクセスできます。 この前 skared キーを共有されないし、未知エンティティと推測し易くないです確認して下さい。
6. **>Site to Site VPN > グループ ポリシー**『Configuration』 を選択 し、選択（デフォルト グループ ポリシーこの場合）のグループ ポリシーを選択して下さい。 編集 Internal Group Policy ダイアログボックスのグループ ポリシーを『Edit』 をクリック し、編集して下さい。 完了したら、[OK] をクリックします。
7. **>ファイアウォール >** 追加 NAT ルール ウィンドウからの **NAT ルール**および、設定しません VPN トラフィックのための NAT（NAT-EXEMPT）ルールを『Configuration』 を選択 して下さい。 完了したら、[OK] をクリックします。

リモート ASA（ダイナミック ピア）

1. ASDM アプリケーションが ASA に接続したら **> VPN ウィザード > Site to Site VPN ウィザード**『Wizards』 を選択 して下さい。
2. [Next] をクリックします。
3. リモートピアの外部 IP アドレスを規定 するために VPN アクセスインターフェイス ドロップダウン リストから『outside』 を選択 して下さい。 クリプト マップが適用するところインターフェイス（**WAN）を**選択して下さい。 [Next] をクリックします。
4. パススルーに VPN トンネル許可する必要があるネットワーク/ホストを規定 して下さい。 このステップでは、ローカルネットワークを提供する必要があり、VPN のためのリモートネットワークはトンネル伝送します。 ボタンをローカルネットワークおよびリモートネットワーク フィールドの隣でクリックし、要件によってアドレスを選択して下さい。 読み終わったら [Next] をクリックします。
5. 使用するためにこの例の事前共有キーである認証情報を入力して下さい。 次の例では、**cisco123** という事前共有鍵を使用しています。 トンネル グループ名前は LAN-to-LAN（L2L）VPN を設定する場合デフォルトでリモートピア IP アドレスです。**または**選択の IKE および IPsec ポリシーを含むために設定をカスタマイズできます。 ピア間に少なくとも 1 一致するポリシーがある必要があります:認証方式から Pre-Shared Key フィールドで IKE バージョン 1 事前共有キーを記録して下さい、入力して下さい。 この例では、それは **cisco123** です。**暗号化アルゴリズム** タブをクリックして下さい。
6. IKE ポリシー フィールドの隣で『Manage』 をクリック し、カスタム IKE ポリシー（phase-1）**を**『Add』 をクリック し、設定して下さい。 完了したら、[OK] をクリックします。

7. IPsec 提案フィールドの隣で『SELECT』 をクリック し、IPsec 望ましい提案を選択して下さい。 読み終わったら [Next] をクリックします。任意で、完全転送秘密タブに行き、**イネーブル 完全転送秘密（PFS）**チェックボックスをチェックできます。 読み終わったら [Next] をクリックします。
8. ネットワーク アドレス変換（NAT）のトンネルトラフィックを初めから防ぐために**アドレス 変換** チェックボックス**からの免除されている ASA 側ホスト/ネットワークを**チェックして下さい。 ローカルネットワークが到達可能であるところでインターフェイスを設定するためにドロップダウン リストから**ローカルか内部を**選択して下さい。 [Next] をクリックします。
9. ASDM はちょうど設定される VPN の要約を表示します。 確認し、『Finish』 をクリック して下さい。

CLI 設定

中央 ASA（静的なピア）設定

1. この例が示すように VPN トラフィックのための NO-NAT/NAT-EXEMPT ルールを設定して下さい:
```
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. リモート Dynamic-L2L-peer を認証するために DefaultL2LGroup の下で事前共有キーを設定して下さい:
```
tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123
```
3. phase-2/ISAKMP ポリシーを定義して下さい:
```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
```
4. 設定される/IPsec ポリシー phase-2 トランスフォームを定義して下さい:
```
crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac
```
5. これらのパラメータでダイナミック マップを設定して下さい: 必須 transform-setイネーブル Reverse Route Injection（RRI）、セキュリティ アプライアンス モデルが学ぶように接続されたクライアントのためのルーティング情報をする（オプションの）
```
crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset
crypto dynamic-map outside_dyn_map 1 set reverse-route
```
6. ダイナミック マップをクリプト マップに結合 し、クリプト マップを加え、outside インターフェイスの ISAKMP/IKEv1 を有効に して下さい:
```
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

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

リモート ASA（ダイナミック ピア）

1. VPN トラフィックのための NAT 免除ルールを設定して下さい:
```
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. 静的な VPN ピアおよび事前共有キーのためのトンネル グループを設定して下さい。
```
tunnel-group 172.16.2.1 type ipsec-l2l
tunnel-group 172.16.2.1 ipsec-attributes
ikev1 pre-shared-key cisco123
```
3. PHASE-1/ISAKMP ポリシーを定義して下さい:
```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```
4. 設定される/IPsec ポリシー phase-2 トランスフォームを定義して下さい:
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
5. access-list を設定して下さい関連した VPN トラフィック/ネットワークを定義する:
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
6. これらのパラメータでスタティック暗号マップを設定して下さい: Crypto/VPN access-listリモート IPSec ピア IP アドレス必須 transform-set
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```
7. クリプト マップを加え、outside インターフェイスの ISAKMP/IKEv1 を有効に して下さい:
```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```

確認

設定がきちんと機能することを確認するのにこのセクションを使用して下さい。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

- show crypto isakmp sa - ピアにおける現在の IKE Security Association（SA; セキュリティ アソシエーション）すべてを表示します。
- **show crypto ipsec sa** -すべての現在の IPSec SA を表示します。

このセクションは 2 ASA のための例確認 outout を示します。

中央 ASA

```
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
```

リモート 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
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

注: debug コマンドを使用する前に、**『debug コマンドの重要な情報』**を参照してください。

表示されているとおりに、次のコマンドを使用します。

```
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
```

注意： **clear crypto isakmp sa** コマンドはそれとして嵌入的クリアしますすべてのアクティブな VPN トンネルをです。

PIX/ASA ソフトウェアリリース 8.0(3) およびそれ以降では、個々の IKE SA **clear crypto isakmp sa** *<peer IP アドレス >command* を使用してクリアすることができます。 先のソフトウェア リリースではより 8.0(3) は、単一トンネルのための IKE および IPSec SA をクリアするために VPNsessiondb ログオフ トンネル グループ *<tunnel-group-name>* コマンドを使用します。

```
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
```

使用されるデバッグ:

```
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
```

リモート ASA（開始プログラム）

トンネルを開始するためにこのパケット **トレーサー** コマンドを入力して下さい:

```
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)
```

中央 ASA（応答側）

```
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 0Jan 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
```

関連情報

- Cisco ASA シリーズ コマンドレファレンス
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- Requests for Comments (RFC)
- テクニカル サポート及びドキュメント- Cisco システム