IPsec のトラブルシューティング目的とした debug コマンドの理解と使用

内容

はじめに

このドキュメントでは、Cisco IOS® ソフトウェアと PIX/ASA の両方で IPsec の問題をトラブルシューティングするために使用される一般的なデバッグコマンドについて説明します。

前提条件

要件

このマニュアルでは、IPsec をすでに設定していることを前提としています。詳細については、「IPSec ネゴシエーション/IKE プロトコル」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS(R) ソフトウェア
  - IPsec 機能セット。
  - 56i：単一の機Data Encryption Standard (DES)能を示します(Cisco IOS®ソフトウェアリリース11.2以降)。
  - k2：Triple DES 機能を示します（Cisco IOS® ソフトウェア リリース 12.0 以降）。トリプル DES は、Cisco 2600 シリーズ以降で使用できます。
- PIX ： V5.0以降。アクティブにするためには、シングルまたはトリプル DES のライセンスキーが必要です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

IPsec VPN の問題に対する最も一般的な解決策については、「一般的な L2L およびリモートアクセス IPSec VPN の問題のトラブルシューティング」を参照してください。

ここでは、接続のトラブルシューティングを開始して、シスコ テクニカル サポートに問い合わせる前に試行できる一般的な手順のチェックリストが提供されています。

Cisco IOS® ソフトウェアのデバッグ

このセクションのトピックでは、Cisco IOS® ソフトウェアのデバッグコマンドについて説明します。詳細については、「 IPSec ネゴシエーション/IKE プロトコル」を参照してください。

show crypto isakmp sa

このコマンドは、ピア間の構築Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)状況を表示します。

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto ipsec sa

このコマンドは、ピア間で構築された IPsec SA を示します。ネットワーク 10.1.0.0 と 10.1.1.0 の間を流れるトラフィックのために 10.1.0.1 と 10.1.0.2 の間に暗号化トンネルが構築されます。

インバウンドとアウトバウンドで構築された2つのEncapsulating Security Payload (ESP)SAを確認できます。AH SA がないため、認証ヘッダー (AH) は使用されません。

このコマンドの出力例を次に示**show crypto ipsec sa**します。

```
<#root>

  interface: FastEthernet0
    Crypto map tag: test, local addr.

10.1.0.1

   local  ident (addr/mask/prot/port): (

10.1.0.0/255.255.255.0/0/0

)
   remote ident (addr/mask/prot/port): (

10.1.1.0/255.255.255.0/0/0
```

)
   current_peer:

10.1.0.2

     PERMIT, flags={origin_is_acl,}

#pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
**   #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382**

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2

     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound

esp

 sas:
      spi: 0x136A010F(325714191)
        transform:

esp-3des esp-md5-hmac

 ,
        in use settings ={

Tunnel

, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing:

remaining key lifetime (k/sec): (4608000/52)

        IV size: 8 bytes
        replay detection support: Y
     inbound

ah

 sas:
     inbound pcp sas:
inbound pcp sas:
outbound

esp

 sas:
   spi: 0x3D3(979)
    transform:

esp-3des esp-md5-hmac

 ,
    in use settings ={

Tunnel

, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing:

```
 remaining key lifetime (k/sec): (4608000/52)

    IV size: 8 bytes
    replay detection support: Y
outbound

ah

 sas:
outbound pcp sas:
```

show crypto engine connection active

このコマンドは、構築された個々のフェーズ 2 SA と、送信されたトラフィックの量を示します。

フェーズ2Security Associations (SAs)は単方向であるため、各SAは一方向のトラフィックのみを示します（暗号化は発信、復号化は着信）。

debug crypto isakmp

このコマ**debug crypto isakmp**ンドの出力例を次に示します。

<#root>

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
    encryption DES-CBC
          hash SHA
    default group 2
    auth pre-share
    life type in seconds
    life duration (basic) of 240

atts are acceptable

. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipsec

このコマンドは、IPSecトンネルエンドポイントの送信元と宛先を表示しますSrc_proxy。これらはクライアントサブネットdest_proxyです。

sa created2つのメッセージが各方向に1つずつ表示されます。（ESP と AH を実行する場合、4 つのメッセージが表示されます。）

このコマンドの出力例を次に示**debug crypto ipsec**します。

<#root>

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
    encaps is 1
    SA life type in seconds
    SA life duration (basic) of 3600
    SA life type in kilobytes
    SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
```

atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
not acceptable".

```
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest=
```

10.1.0.2

```
, src=
```

10.1.0.1

```
,
```

dest_proxy= 10.1.1.0/255.255.255.0/0/0,
src_proxy= 10.1.0.0/255.255.255.0/0/0,

```
      protocol=
```

ESP

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
               keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=
```

10.1.0.2

```
, dest=
```

10.1.0.1,

```
 src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,

      protocol=
```

ESP

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa):
```

sa created

```
,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa):
```

sa created

```
,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

エラー メッセージの例

次の debug コマンドによって、下記に例示するエラー メッセージが生成されます。

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

Replay Check Failed

このエラーの出力例を次に示し"Replay Check Failed"ます。

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

このエラーは、（特に並列パスが存在する場合に）伝送メディアの順序が変更されたため、または負荷がかかった際の大きなパケットと小さなパケットに対する Cisco IOS® 内部のパケット処理パスが同等でないために発生します。

これを反映するように transform-set を変更します。こreply checkれは、が有効な場合にのみ表示さtransform-set esp-md5-hmacれます。このエラーメッセージを抑制するには、esp-md5-hmac無効にして暗号化のみを行います。

Cisco bug ID CSCdp19680（登録ユーザー専用）を参照してください。

QM FSM エラー

IPsec L2L VPN トンネルが PIX ファイアウォールまたは ASA で起動せず、QM FSM エラーメッセージが表示されます。

考えられる理由の1つは、通常とは異なるトラフィックAccess Control List (ACL),やクリプトACLなどのプロキシIDが両端で一致しないことです。

両方のデバイスの設定を確認し、暗号化 ACL が一致していることを確認してください。

もう 1 つの考えられる理由は、トランスフォーム セット パラメータの不一致です。両端でまったく同じパラメータが設定され、VPN ゲートウェイが同じトランスフォームセットを使用していることを確認してください。

Invalid Local Address

次に、このエラー メッセージの出力例を示します。

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

このエラー メッセージは、次の 2 つの一般的な問題のいずれかに起因します。

- **crypto map map-name local-address interface-id**このコマンドを使用すると、ルータは指定されたアドレスを使用するように強制されるため、誤ったアドレスが識別情報として使用されます。
- Crypto map が誤ったインターフェイスに適用されているか、またはまったく適用されていない。設定を確認し、暗号マップが正しいインターフェイスに適用されていることを確かめます。

IKE Message from X.X.X.X Failed its Sanity Check or is Malformed

この debug エラーは、ピアの事前共有キーが一致しない場合に表示されます。この問題を修正するには、両端で事前共有キーを確認します。

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

ピアでメインモードの処理に失敗した

エラーメッセージの例を次に示Main Modeします。メイン モードの障害は、フェーズ 1 ポリシーが両端で一致しないことを示しています。

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

show crypto isakmp saコマンドは、ISAKMP SAの場所を表示しますMM_NO_STATE。これは、メイン モードが失敗したことも意味しています。

```
dst          src        state              conn-id         slot
10.1.1.2  10.1.1.1   MM_NO_STATE        1           0
```

フェーズ 1 ポリシーが両方のピアで設定されていること、またすべての属性が一致していることを確認してください。

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

Proxy Identities Not Supported

このメッセージは、IPsec トラフィック用のアクセス リストが一致しない場合にデバッグで表示されます。

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

各ピア上のアクセスリストは互いにミラーリングする必要があります (すべてのエントリが復元可能である必要があります) 。次の例は、この点について説明しています。

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
```

```
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

Transform Proposal Not Supported

このメッセージは、フェーズ 2（IPsec）が両端で一致していない場合に表示されます。これが最もよく発生するのは、トランスフォーム セット内に不一致や非互換性が存在する場合です。

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

トランスフォーム セットが両端で一致することを確認してください。

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

No Cert and No Keys with Remote Peer

このメッセージは、ルータに設定されたピア アドレスが間違っているか、変更されたことを示しています。ピア アドレスが正しいこと、およびアドレスが到達可能であることを確認します。

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

Peer Address X.X.X.X Not Found

通常、このエラーメッセージはエラーメッセージと共に表示VPN 3000 Concentrator されます"Message: No proposal chosen(14)"。これは、接続がホスト間で行われているためです。

ルータ設定では、ルータ用に選択されたプロポーザルがピアではなくアクセス リストに一致するような順序で IPSec プロポーザルが設定されています。

トラフィックと交差するホストを含む、よりも大きなネットワークがアクセス リストで指定されています。これを修正するには、コンセントレータからルータまでのこの接続に対応するルータ プロポーザルが先に行に現れるようにします。

これにより、特定のホストに最初に一致します。

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

IPsec Packet has Invalid SPI

このエラー メッセージの出力例は次のとおりです。

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

受信したIPsecパケットは、に存在し Security Parameters Index (SPI)ないを指定してい Security Associations Database (SADB)ます。これは次の原因による一時的な状態である可能性があります。

- IPSecピア間のエージングにわずかな違Security Sssociations (SAs)いがあります。
- ローカル SA がクリアされている.
- 誤ったパケットが IPsec ピアによって送信された.

これは攻撃の可能性があります。

推奨処置：

ピアは、ローカルSAがクリアされたことを認識しない可能性があります。ローカル ルータから新しい接続が確立されると、2 つのピアが正常に再確立される場合があります。 あるいは、問題の発生が短期間にとどまらない場合は、接続を新規に確立してみるか、またはピアの管理者に問い合わせます。

PSEC(initialize_sas)：無効なプロキシID

このエラーは、受信したプロキシIDが、アクセスリストで設定されているプロキシIDと一致しないことを"21:57:57: IPSEC(initialize_sas): invalid proxy IDs"示しています。

両方が一致していることを確かめるには、debug コマンド出力を確認します。

プロポーザル要求の debug コマンド出力では、access-list 103 permit ip 10.1.1.0 0.0.0.255 10.1.0.0 0.0.0.255 が一致していません。

アクセス リストは、一方の端ではネットワーク固有であり、他方の端ではホスト固有です。

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

Reserved Not Zero on Payload 5

これは ISAKMP キーが一致していないことを意味します。正確に一致させるには、キーの再生成またはリセットを行います。

Hash Algorithm Offered does not Match Policy

設定された ISAKMP ポリシーが、リモート ピアによって提示されたポリシーと一致しない場合、ルータは 65535 デフォルト ポリシーを試行します。

それでも一致しない場合は、ISAKMP ネゴシエーションが失敗します。

ユーザは、ルータ上でどちらかの"Hash algorithm offered does not match policy!""Encryption algorithm offered does not match policy!"理論的なメッセージを受け取ります。

<#root>

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1):

Checking ISAKMP transform 1 against priority 1 policy

ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):

Hash algorithm offered does not match policy!

ISAKMP (0:1):

atts are not acceptable. Next payload is 0

=RouterB=
ISAKMP (0:1):
```

```
Checking ISAKMP transform 1 against priority 65535 policy

ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):

Encryption algorithm offered does not match policy!

ISAKMP (0:1):

atts are not acceptable. Next payload is 0

ISAKMP (0:1):

 no offers accepted!

ISAKMP (0:1):

phase 1 SA not acceptable!
```

HMAC Verification Failed

このエラーメッセージは、IPSecパケットでの検証に失敗した場合Hash Message Authentication Codeに報告されます。これは通常、パケットが何らかの形で破損している場合に起こります。

<#root>

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39:

%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure

Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39:

%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                  PktEngReturn_MACMiscompare
```

このエラーメッセージがときどき表示される場合は、無視できます。しかし、たびたび繰り返される場合は、パケットの破損の原因を調査する必要があります。暗号アクセラレータの欠陥が原因である場合があります。

Remote Peer Not Responding

このエラー メッセージは、トランスフォーム セットの不一致がある場合に表示されます。両方のピアで一致するトランスフォームセットが設定されていることを確認します。

All IPSec SA Proposals Found Unacceptable

このエラー メッセージは、フェーズ 2 IPsec パラメータがローカルおよびリモート サイトの間で

一致しない場合に発生します。

この問題を解決するには、それらが一致し、正常な VPN が確立されるように、トランスフォーム セットで同じパラメータを指定します。

Packet Encryption/Decryption Error

このエラー メッセージの出力例は次のとおりです。

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

このエラーメッセージの原因は、次のいずれかの可能性があります。

- フラグメンテーション：フラグメント化された暗号化パケットがプロセス スイッチングされます。これにより、ファストスイッチングされたパケットが、プロセス スイッチングされたパケットよりも前に VPN カードに強制的に送信されます。

プロセススイッチング パケットよりも前に処理されるファストスイッチング パケットが多くなると、プロセススイッチング パケットの ESP または AH シーケンス番号が古くなり、それらのパケットが VPN カードに到着するときには、シーケンス番号がリプレイ枠外になります。

これは、使用するカプセル化に応じて AH または ESP シーケンス番号エラー（それぞれ 4615 と 4612）の原因となります。

- 古くなったキャッシュ エントリ：このエラーが発生する別の例は、ファストスイッチ キャッシュ エントリが古くなり、キャッシュ欠落を伴う最初のパケットがプロセススイッチングされる場合です。

回避策

1. 3DES トランスフォーム セットですべての種類の認証をオフにして、ESP-DES/3DES を使用します。これにより、認証/アンチリプレイ保護が効果的に無効になり、順序の不正な（混在した）IPSecトラフィックに関連するパケット廃棄エラーが防止さ%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615れます。
2. ここで説明する理由に適用される回避策の1つは、着信ストリームのサイMaximum Transmission Unit (MTU)ズを1400バイト未満に設定することです。受信側ストリームの最大伝送ユニット（MTU）サイズを 1400 バイトより小さく設定するには、次のコマンドを入力します。

   ```
   ip tcp adjust-mss 1300
   ```

3. AIM カードを無効にします。

4. ルータ インターフェイスでファスト/CEF スイッチングをオフにします。ファーストスイッチングを削除するには、インターフェイスコンフィギュレーションモードで次のコマンドを使用します。

```
no ip route-cache
```

Packets Receive Error Due to ESP Sequence Fail

このエラー メッセージの例を次に示します。

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

このエラー メッセージは通常、以下のいずれかの状態を示しています。

- QoS メカニズムが誤って設定されているために、IPsec 暗号化パケットが暗号化ルータによって不適切な順序で転送される。
- 中間デバイスでパケットの順序が変更されたために、複合ルータで受信した IPsec パケットの順序が誤っている。
- 受信した IPsec パケットがフラグメント化され、認証確認と復号の前にこれをリアセンブルする必要がある。

回避策

1. 暗号化ルータまたは中間ルータで IPsec トラフィックの QoS を無効にします。
2. 暗号化ルータの IPsec 事前フラグメンテーションを有効にします。

```
<#root>
Router(config-if)#
crypto ipsec fragmentation before-encryption
```

3. フラグメント化する必要がないサイズに MTU 値を設定します。

```
<#root>
Router(config)#
interface type [slot_#/]port_#
```

```
<#root>

Router(config-if)#

ip mtu MTU_size_in_bytes
```

4. そのトレインで使用可能な最新の安定版イメージに Cisco IOS® イメージをアップグレードします。

いずれかのルータでMTUサイズを変更すると、そのインターフェイスで終端しているすべてのトンネルが切断されます。

この回避策は、スケジュールされたダウンタイムの間にのみ実行するよう計画してください。

7600 シリーズ ルータで VPN トンネルを確立する際のエラー

7600 シリーズ ルータで VPN トンネルを確立しようとしたときに、このエラーを受け取ります。

```
crypto_engine_select_crypto_engine: can't handle any more
```

このエラーは、7600シリーズルータでソフトウェア暗号化がサポートされていないために発生します。7600 シリーズ ルータでは、IPsec SPA ハードウェアなしで IPsec トンネル終端をサポートできません。7600 ルータで IPSEC-SPA カードを使用する場合にのみ VPN がサポートされます。

PIX のデバッグ

show crypto isakmp sa

このコマンドは、ピア間に構築された ISAKMP SA を示します。

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto isakmp saの出力では、状態は常にQM_IDLEである必要があります。状態が MM_KEY_EXCH である場合は、設定された事前共有キーが正しくないか、ピアの IP アドレスが異なっています。

<#root>

```
PIX(config)#
```

show crypto isakmp sa

```
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

この問題は、正しい IP アドレスまたは事前共有キーを設定することで修正できます。

show crypto ipsec sa

このコマンドは、ピア間で構築された IPsec SA を示します。ネットワーク 10.1.0.0 と 10.1.1.0 の間を流れるトラフィック用に 10.1.0.1 と 10.1.0.2 の間に暗号化トンネルが構築されます。

着信側および発信側で構築された 2 つの ESP SA を確認できます。AH SA がないため、AH は使用されません。

このコマンドの例**show crypto ipsec sa**を次の出力に示します。

<#root>

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (
```

10.1.0.0/255.255.255.0/0/0

```
)
   remote ident (addr/mask/prot/port): (
```

10.1.0.2/255.255.255.255/0/0

```
)
   current_peer: 10.2.1.1
```

dynamic allocated peer ip: 10.1.0.2

```
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound
```

esp

```
 sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={
```

Tunnel

```
, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound
```

esp

```
 sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={
```

Tunnel

```
, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

このコマンドでは IPSec 接続に関するデバッグ情報が表示され、両端で互換性がないために拒否された最初の属性セットが示されます。

2回目の照合(DESの代わりに3DESを試行しSecure Hash Algorithm (SHA)て受け入れられ、ISAKMP SAが構築されます。

また、このデバッグはローカル プールからの IP アドレス (10.32.8.1) を受け入れるダイヤルアップ クライアントからも出力されます。ISAKMP SA が構築されると、IPSec 属性がネゴシエートされ、受け入れ可能と見なされます。

その後、PIX は次のように IPSec SA を設定します。このコマンドの出力例を次に示**debug crypto isakmp**します。

<#root>

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are not acceptable

```
. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are acceptable

```
. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0):
```

peer accepted the address!

```
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0):
```

atts not acceptable.

```
 Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0):
```

atts are acceptable.

```
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

このコマンドは、IPSec 接続に関する debug 情報を示します。

<#root>

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0):
```

Creating IPSec SAs
inbound SA from 10.1.0.2 to 10.1.0.1
(proxy 10.32.8.1 to 10.1.0.1.)
has spi 3576885181 and conn_id 2 and flags 4
outbound SA from 10.1.0.1 to 10.1.0.2
(proxy 10.1.0.1 to 10.32.8.1)
has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
got a queue event...
IPSEC(initialize_sas

```
): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(
```

initialize_sas

```
): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

ルータと VPN クライアントの間の一般的な問題

VPN トンネル外のサブネットにアクセスできない：スプリットトンネル

次のルータ設定出力の例は、VPN 接続のスプリットトンネルを有効にする方法を示しています。

コマ**split tunnel**ンドは、コマンドで設定されたグループに関連付け**crypto isakmp client configuration group hw-client-groupname**れます。

これにより Cisco VPN Client、はルータを使用して、VPNトンネルの一部ではない追加のサブネットにアクセスできます。

IPSec 接続のセキュリティを損なうことなく、これが行われます。192.0.2.18 ネットワーク上に

トンネルが形成されます。

コマンドで定義されていないデバイス (インターネットなど) へ**access list 150**のトラフィックフローは暗号化されません。

<#root>

```
!

crypto isakmp client configuration group hw-client-groupname

 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool


acl 150


!
!

access-list 150 permit ip 192.0.2.18 0.0.0.127 any

!
```

PIX と VPN クライアントの間の一般的な問題

このセクションのトピックでは、VPN Client 3.x を使用して IPSec に PIX を設定する際に生じる一般的な問題について説明しています。PIX の設定例は、バージョン 6.x に基づいています。

トンネルの確立後にトラフィックが流れない：PIX 背後のネットワーク内で ping できない

これはルーティングに関連する一般的な問題です。内部に位置し、なおかつ同じサブネットに直接接続されていないネットワークのルートが PIX に設定されていることを確認してください。

また、内部ネットワークには、クライアント アドレス プール内のアドレス用に、PIX に戻るルートも必要です。

次に出力例を示します。

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on the inside

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1
```

```
 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client for the I

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then the route

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

トンネルのアップ後、ユーザーがインターネットを参照できない：スプリットトンネル

この問題の最も一般的な原因は、VPN クライアントから PIX への IPSec トンネルで、すべてのトラフィックがトンネルを通じて PIX ファイアウォールに送られることです。

PIX の機能では、トラフィックを受信したインターフェイスにそのトラフィックを送り戻すことは許可されていません。したがって、インターネット宛てのトラフィックは動作しません。

この問題を解決するには、コマンドを使用**split tunnel**します。この修正は、1 つだけ特定のトラフィックをトンネル経由で送信し、残りのトラフィックはトンネル経由ではなくインターネットに直接送られる、という考え方に基づいています。

<#root>

```
vpngroup vpn3000 split-tunnel 90

access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

vpngroup vpn3000 split-tunnel 90このコマンドは、を使用してスプリットトンネルを有効にしますaccess-list number 90。

access-list number 90このコマンドは、どのトラフィックがトンネルを通過するかを定義し、残りはアクセスリストの最後で拒否されます。

アクセスリストは、denyon PIXと同じである必要がありNetwork Address Translation (NAT)ます。

トンネルのアップ後、特定のアプリケーションが動作しない：クライアントでの MTU 調整

トンネルが確立されると、PIXファイアウォールの背後にあるネットワーク上のマシンにpingを実行できますが、Microsoftなどの特定のアプリケーションを使用できません

見通し

よく見られる問題は、パケットの最大伝送ユニット（MTU）サイズです。IPSec ヘッダーは最大で 50 ~ 60 バイトになることがあり、これが元のパケットに追加されます。

パケットのサイズが 1500（インターネットのデフォルト）を超えた場合、デバイスでパケットをフラグメント化する必要があります。これにより、IPSec ヘッダーを追加した後も、サイズは 1496（ IPSec での最大値）未満になります。

このコ**show interface**マンドは、アクセス可能なルータまたは構内のルータ上の特定のインターフェイスのMTUを表示します。

発信元から宛先までのすべてのパスのMTUを判別するために、送信されたデータグラムがMTUより大きい場合にこのエラーメッセージが発信元に送り返されるように、さまざまなサイズのデータグラムがビッDo Not Fragment (DF)トを設定して送信されます。

```
frag. needed and DF set
```

次の出力例は、IP アドレス 10.1.1.2 および 172.16.1.56 のホスト間のパスの MTU を見つける方法を示しています。

<#root>

```
Router#
debug ip icmp
ICMP packet debugging is on

!--- Perform an extended ping.

Router#
ping
Protocol [ip]:
Target IP address:
172.16.1.56
Repeat count [5]:
Datagram size [100]:
1550
Timeout in seconds [2]:

!--- Make sure you enter y for extended commands.

Extended commands [n]:
y
Source address or interface:
10.1.1.2
Type of service [0]:
```

```
!--- Set the DF bit as shown.


Set DF bit in IP header? [no]:

y

Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#

ping

Protocol [ip]:
Target IP address:

172.16.1.56

Repeat count [5]:
Datagram size [100]:

1500

Timeout in seconds [2]:
Extended commands [n]:

y

Source address or interface:

10.1.1.2

Type of service [0]:
Set DF bit in IP header? [no]:

y

Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
```

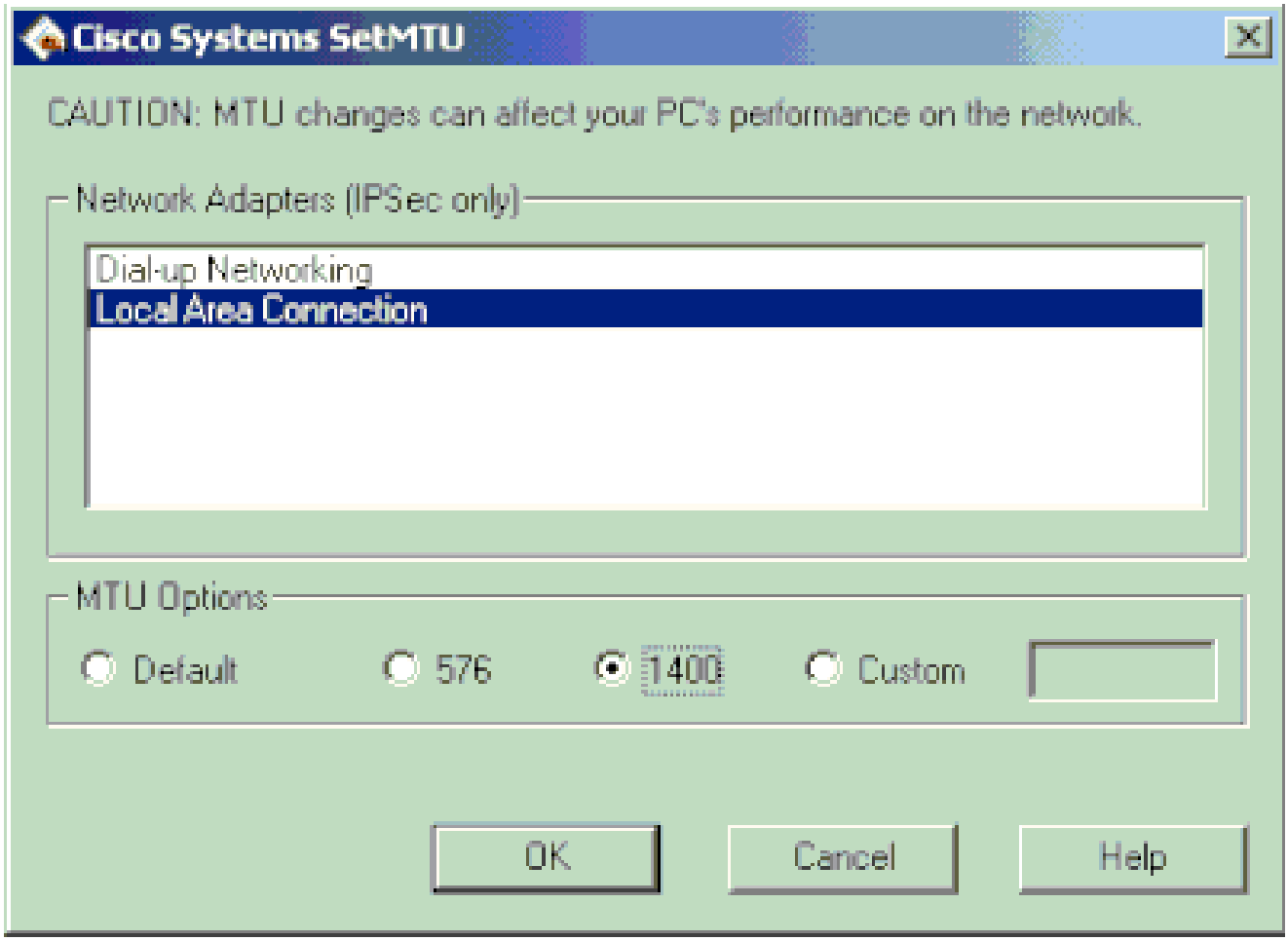
```
Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

VPN クライアントには MTU 調整ユーティリティが付属しており、ユーザはこれを使用して Cisco VPN Client の MTU を調整できます。

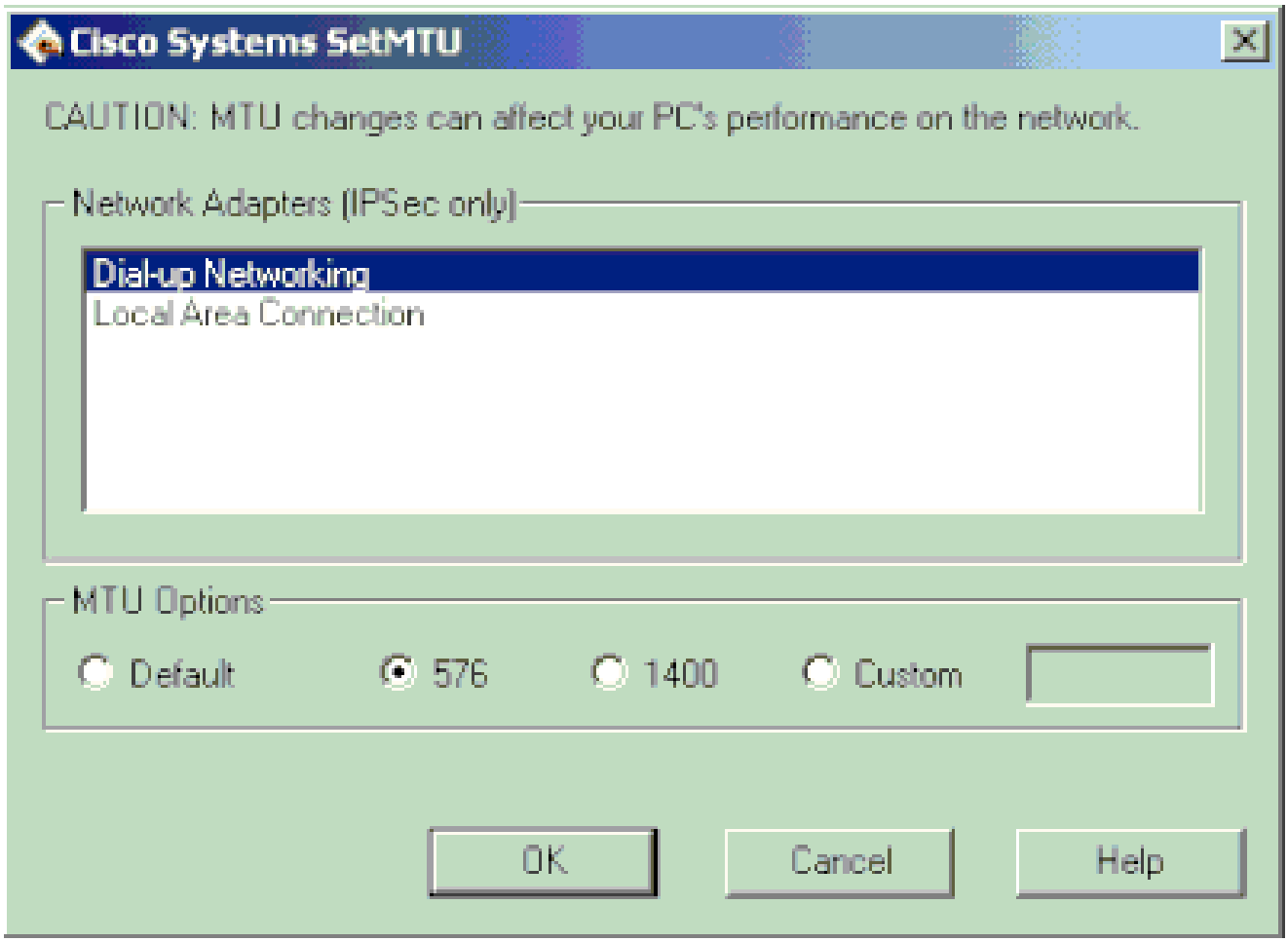
PPP over Ethernet（PPPoE）クライアント ユーザの場合は、PPPoE アダプタの MTU を調整します。

VPN クライアントの MTU ユーティリティを調整するには、次の手順を実行します。

1. 選択 **Start** > **Programs** > **Cisco System VPN Client** > **Set MTU**.
2. を選択し**Local Area Connection**、1400オプションボタンをクリックします。
3. クリック**OK**.



4. 手順1を繰り返し、**Dial-up Networking**.
5. 576をクリックしますオプションボタンをクリックし、**OK**.



sysopt コマンドの欠落

PIXのIPSec設定でコ**sysopt connection permit-ipsec**マンドを使用し、check of**conduit access-list**/command文を使用せずにIPSecトラフィックがPIXファイアウォールをパススルーすることを許可します。

デフォルトでは、すべての着信セッションは、**conduit**または**access-list**command文によって明示的に許可される必要があります。IPSec 保護トラフィックでは、二次的なアクセス リスト チェックが冗長になる可能性があります。

IPSecの認証/暗号化着信セッションが常に許可されるようにするには、このコマンドを使用**sysopt connection permit-ipsec**します。

アクセス制御リスト（ACL）の検証

通常の IPSec VPN 設定では 2 つのアクセス リストを使用します。 一方のアクセス リストは、VPN トンネルに宛てられたトラフィックを NAT プロセスから除外するために使われます。

もう一方のアクセス リストは、暗号化するトラフィックを定義します。このアクセスリストには、LAN 間設定の暗号 ACL またはリモートアクセス設定のスプリットトンネリング ACL が含まれます。

これらの ACL が誤って設定されたり、なかったりすると、トラフィックは VPN トンネルを一方向のみに通過するか、まったくトンネルを通過しない場合があります。

IPSec VPN 設定に必要なすべてのアクセス リストが設定済みであること、およびそれらのアクセス リストでトラフィックが正しく定義されていることを確認してください。

このリストには、IPSec VPN の問題の原因が ACL であると疑われる場合に確認すべき項目が含まれています。

- NAT 除外 ACL と暗号化 ACL でトラフィックが正しく指定されていることを確認します。
- 複数の VPN トンネルと複数の暗号化 ACL がある場合は、それらの ACL が重複していないことを確認します。
- ACL を 2 回使用しないでください。NAT 除外 ACL と暗号化 ACL で同じトラフィックが指定される場合でも、2 つの異なるアクセス リストを使用してください。
- NAT 除外 ACL を使用するようにデバイスが設定されていることを確認します。つまり、コマンドはルータ**route-map**で使用し、コマンド**nat (0)**はPIXまたはASAで使用します。NAT 除外 ACL は、LAN-to-LAN 設定とリモート アクセス設定の両方に必要です。

ACL ステートメントを確認する方法の詳細については、「一般的な L2L および リモートアクセス IPSec VPN の問題のトラブルシューティング」の「 ACL が正しいことを確認する」セクションを参照してください。

関連情報

- 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
- PIX に関するサポート ページ
- テクニカルノート
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。