一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について

目次

概要

このドキュメントでは、IPSec VPN に関する問題の最も一般的なソリューションについて説明します。 これらのソリューションは、Cisco のテクニカルサポートで解決されたサービス リクエストから直接導出されたものです。 これらのソリューションの多くは、IPSec VPN 接続について徹底的なトラブルシューティングを行う前に適用できます。 その結果、このドキュメントは、接続のトラブルシューティングを開始して Cisco テクニカルサポートに問い合せをする前に試す、共通手順のチェックリストとして提供されています。

サイト間 VPN とリモート アクセス VPN のためのコンフィギュレーション例のドキュメントが必要な場合は、『コンフィギュレーションの例とテクニカルノート』の「*リモート アクセス VPN、PIX によるサイト間 VPN (L2L)、IOS によるサイト間 VPN (L2L)*」セクションと「*VPN3000 によるサイト間 VPN (L2L)*」セクションを参照してください。

注: このドキュメントに記載している設定例はルータやセキュリティ アプライアンスで使用するものですが、ほとんどすべての概念は VPN 3000 コンセントレータにも応用できます。

注: Cisco IOS® ソフトウェアと PIX の両方で IPSec のトラブルシューティングに使用される一般的な debug コマンドの説明は、『IP Security のトラブルシューティング：debug コマンドの説明と使用』を参照してください。

注: ASA/PIX では、IPsec VPN トンネルを介してマルチキャスト トラフィックを渡すことはできません。

注: このドキュメント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。

警告： この文書で説明しているソリューションの多くは、適用時に、そのデバイスでのすべての IPSec VPN 接続が一時的に失われる可能性があります。 これらのソリューションは、十分に注意して、組織の変更管理ポリシーに従って適用することを推奨いたします。

前提条件

要件

次のシスコ デバイスでの IPSec VPN 設定に関する知識を得ておくことを推奨します:

- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco IOS ルータ
- Cisco VPN 3000 シリーズ コンセントレータ（*オプション*）

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くものです。

- Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- Cisco IOS

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『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。

IPsec VPN コンフィギュレーションが機能しない

問題

最近設定または設定を変更した IPSec VPN ソリューションが機能しない。

現在の IPSec VPN の設定が機能しなくなった。

解決策

このセクションでは、IPSec VPN に関する問題の最も一般的なソリューションについて説明します。 特定の順番にはなっていませんが、これらのソリューションは、詳細なトラブルシューティングや TAC への連絡を行う前に試すチェックリスト項目として使用できます。 これらのソリューションはすべて TAC サービス リクエストから直接引用したものであり、多数のお客様の問題を解決した実績があります。

- NAT トラバーサルをイネーブルにする（#1 RA VPN の問題）
- 接続が正しいことをテストする
- ISAKMP をイネーブルにする
- PFS をイネーブル/ディセーブルにする
- 古いまたは既存のセキュリティ アソシエーション（トンネル）をクリアする
- ISAKMP ライフタイムを確認する
- ISAKMP キープアライブをイネーブルまたはディセーブルにする
- 事前共有キーを再入力するか元に戻す
- 事前共有鍵が一致しない
- クリプト マップを削除してから再適用する
- sysopt コマンドがあることを確認する（PIX/ASA のみ）
- ISAKMP 識別情報を確認する
- アイドル/セッション タイムアウトを確認する
- ACL が正しいこと、およびクリプト マップにバインドされていることを確認する
- ISAKMP ポリシーを確認する
- ルーティングが正しいことを確認する
- トランスフォーム セットが正しいことを確認する
- クリプト マップのシーケンス番号と名前を確認する

- ピア IP アドレスが正しいことを確認する
- トンネル グループおよびグループ名を確認する
- L2L ピアについて XAUTH をディセーブルにする
- VPN プールの枯渇
- VPN Client トラフィックの遅延による問題

注: これらのセクションで表記するコマンドの中には、スペースの関係上 2 行にわたって表記されているものがあります。

NAT トラバーサルをイネーブルにする（#1 RA VPN の問題）

NAT トラバーサル（NAT-T）を使用すると、Linksys SOHO ルータなどの NAT デバイスや PAT デバイス上を VPN トラフィックが通過できるようになります。 NAT-T をイネーブルにしていないと、VPN クライアント ユーザから PIX または ASA に問題なくアクセスできているように見えていながら、セキュリティ アプライアンスの背後にある社内ネットワークにはアクセスできないという事態が頻繁に生じます。

NAT/PAT デバイスで NAT-T をイネーブルにしていないと、PIX/ASA で「regular translation creation failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4」というエラー メッセージを受け取る場合があります。

同様に、同じ IP アドレスからの同時ログインができない場合は、「Secure VPN connection terminated locally by client. `Reason 412: The remote peer is no longer responding.` 」というエラー メッセージが表示されます。 このエラーを解決するには、VPN デバイスのヘッドエンドで NAT-T をイネーブルにします。

注: Cisco IOS ソフトウェア リリース 12.2(13)T 以降では、Cisco IOS で NAT-T はデフォルトでイネーブルになっています。

Cisco セキュリティ アプライアンスで NAT-T をイネーブルにするコマンドを次に示します。 この例では、キープアライブ時間を 20 に設定しています（デフォルト）。

PIX/ASA 7.1 以前

```
pix(config)#isakmp nat-traversal 20
```

PIX/ASA 7.2(1) 以降

```
securityappliance(config)#crypto isakmp nat-traversal 20
```

これが機能するには、クライアントでも修正が必要です。

Cisco VPN Client で、**Connection Entries** を選択して、**Modify** をクリックします。 これにより新しいウィンドウが表示されますが、ここで **[Transport]** タブを選択する必要があります。 このタブで、[Enable Transparent Tunneling] と [IPSec over UDP（NAT / PAT）] のオプション ボタンを選択します。 次に、**[Save]** をクリックして、接続をテストします。

注: このコマンドは、PIX 6.x と PIX/ASA 7.x で共通です。

注: PIX/ASA は NAT デバイスとして動作するため、ACL の設定により、NAT-T 用 UDP 4500、UDP 500 および ESP ポートを許可することが重要です。 PIX/ASA での ACL の設定についての詳細は、『NAT を使用したファイアウォール経由の IPSec トンネルの設定』を参照してください。

VPN コンセントレータ

VPN コンセントレータで NAT-T をイネーブルにするには、[Configuration] > [Tunneling and Security] > [IPSEC] > [NAT Transparency] > [Enable: IPsec over NAT-T] の順に選択して、VPN コンセントレータで NAT-T をイネーブルにします。

注: NAT-T では、複数の VPN クライアントを PIX、ルータ、コンセントレータなどのあらゆるヘッドエンドに PAT デバイス経由で同時に接続することもできます。

接続が正しいことをテストする

VPN の接続は、暗号化を実行するエンドポイント デバイスの背後にあるデバイスからテストするのが理想的ですが、多くのユーザは暗号化を行うデバイスから **ping** コマンドを使用して VPN の接続をテストしています。 通常 **ping** はこの目的で機能しますが、ping を正しいインターフェイスから発信することが重要です。 **ping** の発信元が正しくないと、VPN 接続が実際には正しく動作しているときでも失敗したように見える場合があります。 例として次のシナリオを参照してください。

Router A のクリプト ACL

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Router B のクリプト ACL

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

この状況では、いずれかのルータの背後にある「内部」ネットワークから **ping** を発信する必要があります。 これは、クリプト ACL は、これらの送信元アドレスを持つトラフィックを暗号化するためだけに設定されているためです。 ルータのインターネット側インターフェイスから発信された **ping** は暗号化されません。 ルータの「内側の」インターフェイスから ping を発信するには、特権 EXEC モードで **ping** コマンドの拡張オプションを使用します。

```
routerA#ping Protocol [ip]: Target IP address: 192.168.200.10 Repeat count [5]: Datagram size
[100]: Timeout in seconds [2]: Extended commands [n]: y Source address or interface:
192.168.100.1 Type of service [0]: Set DF bit in IP header? [no]: 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, 100-byte ICMP Echos to 192.168.200.1, timeout is
2 seconds: Packet sent with a source address of 192.168.100.1 !!!!! Success rate is 100 percent
(5/5), round-trip min/avg/max = ½/4 ms
```

この図にあるルータを PIX または ASA セキュリティ アプライアンスと交換したと想像してください。 接続テスト用に使用する **ping** は、**inside** キーワードを付けて Inside インターフェイスから発信することもできます。

```
securityappliance#ping inside 192.168.200.10 Type escape sequence to abort. Sending 5, 100-byte
ICMP Echos to 192.168.200.10, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5),
round-trip min/avg/max = 1/1/1 ms
```

注: **ping** でセキュリティ アプライアンスの内側のインターフェイスを対象とすることは推奨いたしません。 **ping** で内側のインターフェイスを対象とする必要がある場合は、そのインターフェイスで **management-access** をイネーブルにする必要があります。これを行っていないと、アプライアンスは応答を返しません。

```
securityappliance(config)#management-access inside
```

注: 接続に問題がある場合、VPN のフェーズ 1 でさえも起動されません。 ASA で接続が失敗した場合、SA の出力は、この例と同じように、不正クリプト ピア設定や不正な ISAKMP プロポーザルの設定を示します。

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG2
```

注: 状態は、メイン モード（MM）での状態遷移のエラーを示す MM_WAIT_MSG2 から MM_WAIT_MSG5 に移行する可能性があります。

注: フェーズ 1 がアップするときのクリプト SA の出力は、次に示す例のようになります。

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_ACTIVE
```

ISAKMP をイネーブルにする

IPSec VPN トンネルが動作しているという兆候がまったくない場合は、ISAKMP がイネーブルになっていないことが考えられます。 デバイスで ISAKMP がイネーブルになっていることを確認してください。 デバイスで ISAKMP をイネーブルにするには、次のコマンドのいずれかを使用します。

- Cisco IOS`router(config)#`**`crypto isakmp enable`**
- Cisco PIX 7.1 以前（**outside** を任意のインターフェイスで置き換えます）`pix(config)#`**`isakmp enable outside`**
- Cisco PIX/ASA 7.2(1) 以降（**outside** を任意のインターフェイスで置き換えます）`securityappliance(config)#`**`crypto isakmp enable outside`**

このエラーは、outside インターフェイス上で ISAKMP をイネーブルにする場合も表示されることがあります。

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

インターフェイス上で ISAKMP がイネーブルになる前に、ASA/PIS の背後にあるクライアントが UDP ポート 500 への PAT 設定を完了してしまうことが、このエラーの原因になる場合もあります。 PAT トランスレーションが削除（clear xlate）されると、ISAKMP をイネーブルにすることができます。

注: ピアとの ISAKMP 接続のネゴシエーション用に UDP 500 および 4500 のポート番号が予約されていることを常に確認してください。

注: ISAKMP がインターフェイスで有効になっていない場合、VPN Client は、次に示すようなエラー メッセージが表示されます。

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

注: このエラーを解決するには、VPN ゲートウェイのクリプト インターフェイス上で ISAKMP をイネーブルにします。

PFS をイネーブル/ディセーブルにする

IPSec のネゴシエーションでは、Perfect Forward Secrecy（PFS; 完全転送秘密）によって、それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。 両方のトンネル ピアで PFS をイネーブルまたはディセーブルにします。 そうでないと、PIX/ASA/IOS ルータで LAN-to-LAN（L2L）の IPSec トンネルが確立されません。

PIX/ASA：

PFS はデフォルトでディセーブルになっています。 PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで、enable キーワードを指定して **pfs** コマンドを使用します。 PFS を無効にするには、disable キーワードを指定します。

```
hostname(config-group-policy)#pfs {enable | disable}
```
実行コンフィギュレーションから PFS アトリビュートを削除するには、このコマンドの no 形式を入力します。 グループ ポリシーでは PFS に関する値を他のグループ ポリシーから継承できます。 値を継承しないようにするには、このコマンドの no 形式を使用します。

```
hostname(config-group-policy)#no pfs
```
IOS ルータ：

このクリプト マップのエントリに対して新しいセキュリティ アソシエーションが要求された場合に、IPSec で PFS を要求するように指定する、あるいは IPSec で新しいセキュリティ アソシエーションに対する要求を受け取ったときに PFS を要求するように指定するには、クリプト マップ設定モードで **set pfs** コマンドを使用します。 IPSec で PFS を要求しないようにするには、このコマンドの no 形式を入力します。 デフォルトでは、PFS は要求されません。 このコマンドでグループを指定しない場合は、デフォルトで group1 が使用されます。

```
set pfs [group1 | group2]
no set pfs
```
set pfs コマンドについて：

- group1：新しいデフィーヘルマン交換が実行される際に、IPSec で 768 ビットのデフィーヘルマン プライム係数グループを使用する必要があることを指定します。
- group2：新しいデフィーヘルマン交換が実行される際に、IPSec で 1024 ビットのデフィーヘルマン プライム係数グループを使用する必要があることを指定します。

例：

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```
注: Perfect Forward Secrecy（PFS; 完全転送秘密）は Cisco 独自のものであり、サード パーティ製デバイスではサポートされていません。

古いまたは既存のセキュリティ アソシエーション（トンネル）をクリアする

IOS ルータに次のエラー メッセージが表示される場合、SA がすでに期限切れになっているか、クリアされていることが問題です。 リモート トンネルのエンド デバイスでは、自身が期限切れの SA を使用して（SA 設定パケット以外の）パケットを送信していることがわかりません。 新しい SA が確立されたら通信が再開されます。これにより、トンネルを対象トラフィックが流れ始め、新しい SA が作成されて、トンネルが再確立されます。

```
%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x has no SA
```
IPSec VPN の問題を解決するのに最もシンプルであり、多くの場合に最適となるソリューションは、ISKAMP（フェーズ I）と IPSec（フェーズ II）のセキュリティ アソシエーション（SA）をクリアすることです。

SA をクリアすれば、さまざまなエラー メッセージや不審な動作をトラブルシューティングすることなく高い頻度で解決できます。 このテクニックはあらゆる状況で容易に使用できます。また、現在の IPSec VPN の設定を変更したり、内容を追加したりした後には、ほとんどの場合 SA をクリアする必要があります。 さらに、特定のセキュリティ アソシエーションだけをクリアすることができますが、デバイス上の SA 全体をクリアする方が大きなメリットがあります。

注: セキュリティ アソシエーションをクリアしたら、トンネルにトラフィックを送信して、セキュリティ アソシエーションを再確立する必要があります。

警告： クリアするセキュリティ アソシエーションを指定しない場合、ここに一覧するコマンドはデバイス上のすべてのセキュリティ アソシエーションをクリアします。 他の IPSec VPN トンネルを使用している場合は、操作に注意してください。

1. クリアする前に、対象とするセキュリティ アソシエーションを確認します。**Cisco IOS**`router#show crypto isakmp sa router#show crypto ipsec sa` **Cisco PIX/ASA セキュリティ アプライアンス**`securityappliance#show crypto isakmp sa securityappliance#show crypto ipsec sa` **注:** これらのコマンドは、PIX 6.x と PIX/ASA 7.x で共通です。
2. セキュリティ アソシエーションをクリアします。 各コマンドは太字で示した部分のみで入力するか、もしくはさらにオプションを付けて入力することができます。**Cisco IOSISAKMP（フェーズ I）** `router#clear crypto isakmp ? <0 - 32766> connection id of SA <cr>` **IPSec（フェーズ II）** `router#clear crypto sa ? counters Reset the SA counters map Clear all SAs for a given crypto map peer Clear all SAs for a given crypto peer spi Clear SA by SPI <cr>` **Cisco PIX/ASA セキュリティ アプライアンスISAKMP（フェーズ I）** `securityappliance#clear crypto isakmp sa` **IPSec（フェーズ II）** `security appliance#clear crypto ipsec sa ? counters Clear IPsec SA counters entry Clear IPsec SAs by entry map Clear IPsec SAs by map peer Clear IPsec SA by peer <cr>`

ISAKMP ライフタイムを確認する

L2L トンネルを使用しているときに通信が頻繁に切断される場合は、ISAKMP SA に設定されているライフタイムが短いことが問題である可能性があります。 ISAKMP ライフタイムに何らかの不一致が発生すると、「**%PIX|ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision**」というエラー メッセージを PIX/ASA で受け取る場合があります。 FWSM の場合は、「%FWSM-5-713092: `Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision` これを修正するには、ピアどうしで同じ値を設定します。

デフォルトは 86,400 秒、つまり 24 時間です。 一般的な規則として、ライフタイムが短いほど、ISAKMP ネゴシエーションが（ある程度までは）安全になるとされていますが、ライフタイムが短いと、セキュリティ アプライアンスが IPSec SA を作成する回数が多くなります。

一致したとの判断は、2 つのピアの両方のポリシーで同じ暗号、ハッシュ、認証、Diffie-Hellman パラメータ値が設定されている場合、および、リモート ピアのポリシーにおいて、比較するポリシーで指定されているライフタイムと同じかそれ以下のライフタイムが指定されている場合になされます。 ライフタイムが同一でない場合、リモート ピアのポリシーにより、短い方のライフタイムが使用されます。 一致の条件が満たされない場合、IKE はネゴシエーションを拒否し、IKE SA は確立されません。

SA のライフタイムを指定します。 この例では、4 時間（14,400 秒）のライフタイムを設定しています。 デフォルトは 86,400 秒、つまり 24 時間です。

PIX/ASA

```
hostname(config)#isakmp policy 2 lifetime 14400
```

IOS ルータ

```
R2(config)#crypto isakmp policy 10 R2(config-isakmp)#lifetime 86400
```

設定されている最大のライフタイムを超えた場合は、VPN 接続の終端時に、次のメッセージを受け取ります。

`Secure VPN Connection terminated locally by the Client. Reason 426:` Maximum Configured

Lifetime Exceeded.

このエラー メッセージを解決するには、**lifetime** 値に *0* を設定し、IKE セキュリティ アソシエーションのライフタイムを無限大に設定します。 VPN は常に接続され、終端しません。

```
hostname(config)#isakmp policy 2 lifetime 0
```

問題を解決するために、**グループ ポリシーで re-xauth をディセーブルにする**こともできます。

ISAKMP キープアライブをイネーブルまたはディセーブルにする

ISAKMP キープアライブを設定すると、LAN-to-LAN またはリモート アクセス VPN が散発的にドロップするのを防ぐのに役立ちます。これには、VPN クライアント、トンネル、非アクティブになった後にドロップされるトンネルが含まれます。 この機能によって、トンネルのエンドポイントではリモート ピアが継続的に存在することが監視され、自身の存在がそのピアに報告されます。 ピアからの応答がなくなると、エンドポイントは接続を解除します。 ISAKMP キープアライブが動作するためには、両側の VPN エンドポイントでこの機能がサポートされている必要があります。

- 次のコマンドで、Cisco IOS に ISAKMP キープアライブを設定します。`router(config)#`**`crypto isakmp keepalive 15`**
- PIX/ASA セキュリティ アプライアンスで ISAKMP キープアライブを設定するには、次のコマンドを使用します。Cisco PIX 6.x`pix(config)#`**`isakmp keepalive 15`** Cisco PIX/ASA 7.x 以降で、トンネル グループの名前が **10.165.205.222 の場合**`securityappliance(config)#`**`tunnel-group 10.165.205.222 ipsec-attributes`** `securityappliance(config-tunnel-ipsec)#`**`isakmp keepalive threshold 15 retry 10`** 状況によっては、問題解決のためにこの機能をディセーブルにする必要がある場合があります。たとえば、VPN クライアントが DPD パケットを阻止しているファイアウォールの背後にある場合などです。Cisco PIX/ASA 7.x 以降で、トンネル グループの名前が **10.165.205.222 の場合**デフォルトではイネーブルになっている IKE キープアライブ処理をディセーブルにします。`securityappliance(config)#`**`tunnel-group 10.165.205.222 ipsec-attributes`** `securityappliance(config-tunnel-ipsec)#`**`isakmp keepalive disable`** **Cisco VPN Client 4.x のキープアライブを無効にする**問題が検出されたクライアント PC 上で [%System Root%] > [Program Files] > [Cisco Systems] > [VPN Client] > [Profiles] を選択して IKE キープアライブをディセーブルにし、**PCF ファイル**の接続を必要に応じて編集します。**'ForceKeepAlives=0'**（デフォルト）を **'ForceKeepAlives=1'** に変更します。

注: キープアライブは Cisco 独自のものであり、サード パーティ製デバイスによってサポートされていません。

事前共有キーを再入力するか元に戻す

IPSec VPN トンネルが起動しないときには、単純な入力ミスが原因になっていることもよくあります。 たとえば、セキュリティ アプライアンスでは、事前共有キーは入力されると非表示になります。 このため、キーが誤っていることがわかりません。**各 VPN エンドポイントについて、事前共有鍵が正しく入力されていることを確認してください。** キーが正しいことを確認するには、キーを再入力します。 これは詳細なトラブルシューティングを避けるのに役立つ簡単な手段です。

リモート アクセス VPN では、CiscoVPN クライアントに有効なグループ名や事前共有キーが入力されていることを確認します。 このエラーは、グループ名や事前共有キーが VPN クライアントとヘッドエンド デバイスとの間で一致しない場合に発生することがあります。

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
```

```
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... may be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

PIX/ASA セキュリティ アプライアンスで設定を変更せずに事前共有キーを元に戻すこともできます。 ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： 事前共有キーの回復』を参照してください。

警告： クリプト関連のコマンドを削除する際には、1 つあるいはすべての VPN トンネルがダウンしてしまう可能性があります。 これらのコマンドは十分に注意して使用し、以降の手順を実行する前にお客様の組織の変更管理ポリシーを確認してください。

- IOS でピア 10.0.0.1 またはグループ vpngroup に対する事前共有キー secretkey を削除および再入力するには、次のコマンドを使用します。Cisco LAN-to-LAN VPN`router(config)#no crypto isakmp key secretkey address 10.0.0.1 router(config)#crypto isakmp key secretkey address 10.0.0.1` Cisco リモート アクセス VPN`router(config)#crypto isakmp client configuration group vpngroup router(config-isakmp-group)#no key secretkey router(config-isakmp-group)#key secretkey`
- PIX/ASA セキュリティ アプライアンスでピア 10.0.0.1 に対する事前共有キー secretkey を削除および再入力するには、次のコマンドを使用します。Cisco PIX 6.x`pix(config)#no isakmp key secretkey address 10.0.0.1 pix(config)#isakmp key secretkey address 10.0.0.1` Cisco PIX/ASA 7.x 以降`securityappliance(config)#tunnel-group 10.0.0.1 ipsec-attributes securityappliance(config-tunnel-ipsec)#no pre-shared-key securityappliance(config-tunnel-ipsec)#pre-shared-key secretkey`

事前共有鍵が一致しない

VPN トンネルの起動が切断されます。 この問題は、フェーズ I のネゴシエーション時に事前共有鍵が一致しないことが原因で発生することがあります。

show crypto isakmp sa コマンドの MM_WAIT_MSG_6 メッセージは、次の例で示すように事前共有鍵の不一致を示しています。

```
ASA#show crypto isakmp sa 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: 10.7.13.20 Type : L2L Role : initiator Rekey : no State : MM_WAIT_MSG_6
```

この問題を解決するには、両方のアプライアンスで事前共有鍵を再入力します。 事前共有鍵は、一意かつ一致している必要があります。 詳細は、『事前共有鍵を再入力するか元に戻す』を参照してください。

クリプト マップを削除してから再適用する

セキュリティ アソシエーションをクリアしても、IPSec VPN の問題が解決されない場合、VPN トンネルの散発的なドロップおよび一部の VPN サイトの起動エラーを含む広範囲な問題を解決するために、関連するクリプト マップを削除してから再適用します。

警告： インターフェイスからクリプト マップを削除すると、そのクリプト マップに対応付けられているすべての IPSec トンネルが**必ず**ダウンします。 これらの手順は十分に注意して実行し、実行する前にお客様の組織の変更管理ポリシーを十分に考慮してください。

- Cisco IOS でクリプト マップの削除と置き換えを行うには、下記のコマンドを使用します。まず、インターフェイスからクリプト マップを削除します。 **crypto map** コマンドの no 形式を使用します。`router(config-if)#`**`no crypto map mymap`** 引き続き **no** 形式を使用して暗号化マップ全体を削除します。`router(config)#`**`no crypto map mymap 10`** ピア **10.0.0.1** の Ethernet0/0 インターフェイスのクリプト マップを置き換えます。 次の例ではクリプト マップの必要最小限の設定を行っています。`router(config)#`**`crypto map mymap 10 ipsec-isakmp`** `router(config-crypto-map)#`**`match address 101`** `router(config-crypto-map)#`**`set transform-set mySET`** `router(config-crypto-map)#`**`set peer 10.0.0.1`** `router(config-crypto-map)#`**`exit`** `router(config)#`**`interface ethernet0/0`** `router(config-if)#`**`crypto map mymap`**
- PIX や ASA では、次のコマンドを使用してクリプト マップの削除と置き換えを行います。まず、インターフェイスからクリプト マップを削除します。 **crypto map** コマンドの no 形式を使用します。`securityappliance(config)#`**`no crypto map mymap interface outside`** 引き続き **no** 形式を使用して他の暗号化マップ コマンドを削除します。`securityappliance(config)#`**`no crypto map mymap 10 match address 101`** `securityappliance(config)#`**`no crypto map mymap set transform-set mySET`** `securityappliance(config)#`**`no crypto map mymap set peer 10.0.0.1`** ピア **10.0.0.1** の暗号化マップを置き換えます。 次の例ではクリプト マップの必要最小限の設定を行っています。`securityappliance(config)#`**`crypto map mymap 10 ipsec-isakmp`**
  `securityappliance(config)#`**`crypto map mymap 10 match address 101`**
  `securityappliance(config)#`**`crypto map mymap 10 set transform-set mySET`**
  `securityappliance(config)#`**`crypto map mymap 10 set peer 10.0.0.1`**
  `securityappliance(config)#`**`crypto map mymap interface outside`**

注: 暗証化マップの削除と再適用を行うと、ヘッドエンドの IP アドレスが変わった場合の接続の問題も解決されます。

sysopt コマンドがあることを確認する（PIX/ASA のみ）

sysopt connection permit-ipsec コマンドと **sysopt connection permit-vpn** コマンドを使用すると、IPSec トンネルからのパケットとそのペイロードに関して、セキュリティ アプライアンスのインターフェイス ACL をバイパスさせることができます。 セキュリティ アプライアンスで終端される IPSec トンネルでは、これらのコマンドのどちらかがイネーブルになっていないと失敗する確立が高くなります。

セキュリティ アプライアンス ソフトウェア バージョン 7.0 以前では、この状況に関連する sysopt コマンドは **sysopt connection permit-ipsec** です。

セキュリティ アプライアンス ソフトウェア バージョン 7.1(1) 以降では、この状況に関連する sysopt コマンドは **sysopt connection permit-vpn** です。

PIX 6.x では、この機能はデフォルトで**ディセーブル**になっています。 PIX/ASA 7.0(1) 以降では、この機能はデフォルトで**イネーブル**になっています。 使用しているデバイスで対応する **sysopt** コマンドが有効であるかどうかを判定するには、次の show コマンドを使用します。

- Cisco PIX 6.x`pix# **show sysopt** no sysopt connection timewait sysopt connection tcpmss 1380 sysopt connection tcpmss minimum 0 no sysopt nodnsalias inbound no sysopt nodnsalias outbound no sysopt radius ignore-secret no sysopt uauth allow-http-cache **no sysopt connection permit-ipsec** *!--- sysopt connection permit-ipsec is disabled* no sysopt connection permit-pptp no sysopt connection permit-l2tp no sysopt ipsec pl-compatible`
- Cisco PIX/ASA 7.x`securityappliance# **show running-config all sysopt** no sysopt connection timewait sysopt connection tcpmss 1380 sysopt connection tcpmss minimum 0 no sysopt nodnsalias inbound no sysopt nodnsalias outbound no sysopt radius ignore-secret **sysopt connection permit-vpn** *!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)*`

使用しているデバイスに適した **sysopt** コマンドをイネーブルにするには、次のコマンドを使用します。

- Cisco PIX 6.x および PIX/ASA 7.0`pix(config)#**sysopt connection permit-ipsec**`
- Cisco PIX/ASA 7.1(1) 以降`securityappliance(config)#**sysopt connection permit-vpn**`

注: sysopt connection コマンドを使用しない場合は、送信元から宛先への対象トラフィックである必要なトラフィックを Outside ACL で明示的に許可する必要があります。例としては、リモート デバイスの LAN からローカル デバイスの LAN へ、および、リモート デバイスの Outside インターフェイスからローカル デバイスの Outside インターフェイスへの「UDP port 500」があります。

ISAKMP 識別情報を確認する

IKE ネゴシエーションの中で IPSec VPN トンネルの確立に失敗した場合、その原因は PIX か、ピアがその相手ピアの識別情報を認識できなかったことが原因である可能性があります。 2 つのピアで IPSec セキュリティ アプライアンスの確立に IKE を使用している場合は、各ピアがリモート ピアに対して自身の ISAKMP 識別情報を送信します。 ピアは保持している ISAKMP 識別情報に応じて、自身の IP アドレスまたはホスト名を送信します。 デフォルトでは、PIX ファイアウォール ユニットの ISAKMP 識別情報は IP アドレスに設定されています。 一般的な規則としては、IKE ネゴシエーションの失敗を回避するために、セキュリティ アプライアンスとその相手ピアの識別情報を同じ方式で設定します。

ピアに送信するフェーズ 2 の ID を設定するには、グローバル コンフィギュレーション モードで **isakmp identity** コマンドを使用します。

```
crypto isakmp identity address
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as
authentication type
```

または

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by
connection type; IP address for !--- preshared key or cert DN for certificate authentication.
```

または

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchanging ISAKMP identity
information (default). !--- This name comprises the hostname and the domain name.
```

PIX/ASA 設定移行ツールを使用して、設定を PIX から ASA に移動すると VPN トンネルが起動に失敗します。 ログに次のメッセージが表示されます。

```
[[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry found, removing! [[IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match! [[IKEv1]: Group =
x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): No SPI to identify Phase 2 SA! [[IKEv1]: Group
= x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

この問題は、PIX がデフォルトで、ASA が IP として識別する接続を hostname として識別するように設定されているためです。 この問題を解決するには、次に示すように、crypto isakmp identity コマンドをグローバル コンフィギュレーション モードで使用します。

```
crypto isakmp identity hostname !--- Use the fully-qualified domain name of !--- the host exchanging ISAKMP identity information (default). !--- This name comprises the hostname and the domain name.
```

「Received an un-encrypted INVALID_COOKIE」というエラー メッセージが表示されたら、address crypto isakmp コマンドを発行して問題を解決します。

注: ソフトウェア バージョン 7.2(1) からは、**isakmp identity** コマンドは使用されなくなっています。 詳細については、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』を参照してください。

アイドル/セッション タイムアウトを確認する

アイドル タイムアウトが 30 分（デフォルト）に設定されている場合、これは 30 分間にわたってトンネルを通過するトラフィックがなかった場合にトンネルがドロップされることを意味します。 VPN クライアントは、アイドル タイムアウトの設定にかかわらず 30 分後に接続解除され、PEER_DELETE-IKE_DELETE_UNSPECIFIED エラーが発生します。

サードパーティ製デバイスを使用する場合であっても、トンネルが常時**アップ状態**でドロップされることのないようにするには、idle timeout と session timeout を none に設定します。

PIX/ASA 7.x 以降

ユーザのタイムアウト期間を設定するには、次のように、グループ ポリシー コンフィギュレーション モードかユーザ名コンフィギュレーション モードで vpn-idle-timeout コマンドを入力します。

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-timeout none
```

次のように、グループ ポリシー コンフィギュレーション モードかユーザ名コンフィギュレーション モードで vpn-session-timeout コマンドにより、VPN 接続に対する最大総時間を設定します。

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-session-timeout none
```

注: tunnel-all が設定されている場合は、VPN アイドル タイムアウトが設定されていても、（tunnel-all が設定されているため）すべてのトラフィックがトンネルを通過してしまって動作しないので、idle-timeout を設定する必要はありません。 つまり、対象トラフィック（さらに PC によって生成されたトラフィックまで）が通過対象となり、アイドル タイムアウトを起動させることはできません。

Cisco IOS ルータ

IPSec SA アイドル タイマーを設定するには、グローバル コンフィギュレーション モードかクリプト マップ設定モードで crypto ipsec security-association idle-time コマンドを使用します。 デフォルトでは、IPSec SA アイドル タイマーはディセーブルになっています。

```
crypto ipsec security-association idle-time seconds
```

時間は*秒単位*で、このアイドル タイマーにより非アクティブなピアで SA が維持できます。 引数

seconds の有効な値の範囲は 60 から 86400 です。

ACL が正しいこと、およびクリプト マップにバインドされていることを確認する

通常の IPSec VPN 設定ではアクセス リストを 2 つ使用します。 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用します。 もう一方のアクセス リストでは、暗号化するトラフィックが定義されます。 これには、LAN-to-LAN 設定のクリプト 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 が誤って設定されていたり、存在しなかったりすると、トラフィックが VPN トンネルを 1 方向にしか流れなかったり、トンネルにトラフィックがまったく送られなかったりします。

注: グローバル コンフィギュレーション モードで、crypto map match address コマンドを使用して、クリプト ACL をクリプト マップに確実にバインドします。

IPSec VPN の設定に必要なすべてのアクセス リストを設定していることと、それらのアクセス リストにトラフィックが正確に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 にあることが疑われる場合に確認する単純な項目が含まれています。

- NAT 除外 ACL とクリプト 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 トンネルと複数のクリプト 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。**注:** VPN コンセントレータでは、次のような ログが表示されます。`Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy`このメッセージが表示されないようにして、トンネルを起動するには、クリプト ACL がオーバーラップしていないこと、および同じ対象トラフィックが他の設定済み VPN トンネルによって使用されていないことを確認します。
- ACL を 2 回使用しないようにします。 NAT 免除 ACL とクリプト ACL で同じトラフィックが指定されている場合でも、2 つの異なるアクセス リストを使用してください。
- リモート アクセス コンフィギュレーションには、対象トラフィック用のダイナミック クリプト マップが備わったアクセス リストは使用しないでください。 このようにしてしまうと、VPN クライアントがヘッドエンド デバイスに接続できなくなります。 リモート アクセス VPN にクリプト ACL を誤って設定してしまうと、「%ASA-3-713042: `IKE Initiator unable to find policy:` Intf 2」というエラー メッセージを受け取る場合があります。**注:** VPN サイト間トンネルの場合は、アクセス リストがピアと一致していることを確認してください。 これらはピアで逆順になっている必要があります。Cisco VPN Client と PIX/ASA 間にリモート アクセス VPN 接続を設定する方法を示した設定例は、『PIX/ASA 7.x および Cisco VPN Client 4.x で Active Directory に対する Windows 2003 IAS RADIUS 認証を使用するための設定例』を参照してください。
- 使用しているデバイスで、NAT 除外 ACL を使用するように設定されていることを確認します。 ルータの場合、これは **route-map** コマンドを使用することを意味します。 PIX や ASA の場合、これは **nat (0)** コマンドを使用することを意味します。 NAT 免除 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。この例では、IOS ルータで **192.168.100.0 /24** と **192.168.200.0 /24** または **192.168.1.0 /24** との間で送信されるトラフィックを NAT 処理から除外するよう設定しています。 他を宛先とするトラフィックは、NAT オーバーロードの対象となります。

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any
```

```
route-map nonat permit 10
  match ip address 110
```

`ip nat inside source route-map nonat interface FastEthernet0/0 overload`この例では、PIX で 192.168.100.0 /24 と 192.168.200.0 /24 または 192.168.1.0 /24 との間で送信されるトラフィックを NAT 処理から除外するよう設定しています。 たとえば、その他のトラフィックはすべて、NAT オーバーロードの対象となります。`access-list` **`noNAT`** `extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0 access-list` **`noNAT`** `extended permit ip 192.168.100.0 255.255.255.0 192.168.1.0 255.255.255.0 nat (inside) 0 access-list` **`noNAT`** `nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface` **注:** 下記の例（access-list noNAT）に示されているように、NAT 免除 ACL が機能するのは IP アドレスや IP ネットワークでだけで、クリプト マップ ACL に一致している必要があります。 NAT 免除 ACL はポート番号（たとえば 23、25 など）では機能しません。**注:** ネットワーク間の音声コールが VPN 経由で通信される VOIP 環境では、NAT 0 ACL が正しく設定されていないと、音声コールは動作しません。 VOIP のトラブルシューティングを詳しく実行する前に、問題が NAT 免除 ACL の設定ミスによる可能性があるため、VPN の接続状態を確認することを推奨します。**注**: NAT 免除（nat 0）ACL に誤設定があると、下記のエラー メッセージを受け取る場合があります。`%PIX-3-305005:` **`No translation group`** `found for icmp src outside:192.168.100.41 dst inside:192.168.200.253 (type 8, code 0) %ASA-3-305005: No translation group found for udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p`**注: 誤った例：**`access-list noNAT extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0` **`eq 25`** NAT 免除（nat 0）が機能しない場合、機能させるためには、それを削除してから、**NAT 0** コマンドを発行してみてください。

- ACL が古いものではなく、正しいタイプであることを確認してください。LAN-to-LAN 設定のためのクリプト ACL と NAT 免除 ACL は、ACL を設定するデバイスの視点から記述する必要があります。 このことは、各 ACL は互いに**ミラー関係**である必要があることを意味します。 この例では、LAN-to-LAN トンネルを 192.168.100.0 /24 と 192.168.200.0 /24 との間に設定しています。Router A のクリプト ACL`access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255`Router B のクリプト ACL`access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255`**注:** ここでは説明していませんが、同じ概念が PIX および ASA セキュリティ アプライアンスにも該当します。リモート アクセス設定のためのスプリット トンネル ACL は、VPN クライアントがアクセスする必要のあるネットワークへのトラフィックを許可する**標準**アクセス リストである必要があります。 IOS ルータは、スプリット トンネル用の拡張 ACL を使用できます。**注:** 拡張アクセス リストにおいて、スプリット トンネル ACL の発信元に「**any**」を指定することは、スプリット トンネルをディセーブルにすることと同じです。 スプリット トンネル用の拡張 ACL では発信元ネットワークだけを使用します。**注: 正しい例：**`access-list 140 permit ip` **`10.1.0.0 0.0.255.255`** `10.18.0.0 0.0.255.255` **注: 誤った例：**`access-list 140 permit ip` **`any`** `10.18.0.0 0.0.255.255` Cisco IOS`router(config)#` **`access-list 10 permit ip 192.168.100.0`** `router(config)#` **`crypto isakmp client configuration group MYGROUP`** `router(config-isakmp-group)#` **`acl 10`** Cisco PIX 6.x`pix(config)#` **`access-list 10 permit`** `192.168.100.0 255.255.255.0 pix(config)#` **`vpngroup MYGROUP split-tunnel 10`** Cisco PIX/ASA 7.x`securityappliance(config)#` **`access-list 10 standard permit 192.168.100.0 255.255.255.0`** `securityappliance(config)#` **`group-policy MYPOLICY internal`** `securityappliance(config)#` **`group-policy MYPOLICY attributes`** `securityappliance(config-group-policy)#` **`split-tunnel-policy tunnelspecified`** `securityappliance(config-group-policy)#` **`split-tunnel-network-list value 10`**

ASA で NO NAT ACLL が誤って設定されているか、または設定されていない場合に、ASA 8.3 で次のエラーが発生します。

```
%%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection for udp
```

```
src outside: x.x.x.x/xxxxx dst inside: x.x.x.x/xx denied due to NAT reverse path failure
```

この問題を解決するには、設定が正しく行われていることを確認し、設定に誤りがある場合は再設定します。

サイト間 VPN トンネル用の ASA バージョン 8.3 の NAT 免除の設定：

サイト間 VPN は、バージョン 8.3 を使用して両方の ASA で HOASA と BOASA との間に確立する必要があります。 HOASA での NAT 免除設定は次のようになります。

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

ISAKMP ポリシーを確認する

IPSec トンネルがアップになっていない場合は、リモート ピアとの間で ISAKMP ポリシーが一致しているかどうか確認してください。 この ISAKMP ポリシーは、サイト間（L2L）とリモート アクセス IPSec VPN の両方に適用されます。

Cisco VPN クライアントまたはサイト間 VPN でリモート デバイスとのトンネルが確立できない場合は、**2 つのピアで同じ暗号、ハッシュ、認証、Diffie-Hellman パラメータ値が設定されていること**、およびリモート ピアのポリシーで、発信側が送信するポリシーで指定されているライフタイムと同じかそれ以下のライフタイムが指定されていることを確認してください。 ライフタイムが同じでない場合、セキュリティ アプライアンスでは短い方のライフタイムが使用されます。 一致の条件が満たされない場合、ISAKMP はネゴシエーションを拒否し、SA は確立されません。

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

次に詳細ログ メッセージを示します。

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, dropping
```

このメッセージは通常、ISAKMP ポリシーが不一致の場合または NAT 0 文が見つからない場合に表示されます。

また、次のメッセージも表示されます。

```
Error Message    %PIX|ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

このメッセージは、フェーズ 1 の完了後にフェーズ 2 のメッセージがキューイングされていることを示しています。 このエラー メッセージの原因としては、次のいずれかが考えられます。

- いずれかのピア上でフェーズが一致していない
- ピアによるフェーズ 1 の完了を ACL がブロックしている

このメッセージは通常、エラー メッセージ「Removing peer from peer table failed, no match!」というエラー メッセージが表示されます。

Cisco VPN Client がヘッドエンド デバイスに接続できない場合、ISAKMP ポリシーのミスマッチ

が問題である可能性があります。 ヘッドエンド デバイスは、Cisco VPN Client の IKE プロポーザルのいずれかに一致している必要があります。

注: ISAKMP ポリシーと PIX/ASA で使用されている IPSec トランスフォーム セットに関して、Cisco VPN クライアントでは DES と SHA を組み合わせたポリシーは使用できません。 DES を使用している場合は、ハッシュ アルゴリズムに MD5 を使用する必要があります。または、3DES と SHA、および 3DES と MD5 といった他の組み合わせも使用できます。

ルーティングが正しいことを確認する

ルーティングは、ほとんどのすべての IPSec VPN の展開において重要な部分です。 ルータや PIX あるいは ASA セキュリティ アプライアンスなどの暗号化デバイスで、VPN トンネルへトラフィックを送信するために正しいルーティング情報が設定されていることを確認してください。 さらに、ゲートウェイ デバイスの背後に他のルータがある場合は、トンネルへの到達方法と、反対側にあるネットワークについて、これらのルータで認識されていることを確認してください。

VPN の展開において、ルーティングのキーとなるコンポーネントの 1 つに Reverse Route Injection (RRI) があります。 RRI により、リモート ネットワークまたは VPN クライアントに対するエントリが VPN ゲートウェイのルーティング テーブルにダイナミックにインポートされます。 RRI によって設定されたルートは EIGRP や OSPF などのルーティング プロトコルによって再配布できるため、このようなルートは、ルートを設定したデバイスやネットワーク上にある他のデバイスにとって便利です。

- LAN-to-LAN の設定では、トラフィックを暗号化する必要のあるネットワークへのルートを各エンドポイントが認識していることが重要です。 たとえば、Router A は、Router B の背後にあるネットワークを **10.89.129.2** 経由するルートとして認識している必要があります。 ルータ B は **192.168.100.0 /24** ルートも同様に認識している必要があります。各ルータで適切なルートが確実に認識されているようにする第一の方法は、各宛先ネットワークへのスタティック ルートを設定することです。 たとえば、Router A では次のような route 文を設定できます。`ip route 0.0.0.0 0.0.0.0 172.22.1.1`
`ip route 192.168.200.0 255.255.255.0 10.89.129.2`
`ip route 192.168.210.0 255.255.255.0 10.89.129.2`
`ip route 192.168.220.0 255.255.255.0 10.89.129.2`
`ip route 192.168.230.0 255.255.255.0 10.89.129.2`Router A を PIX や ASA に置き換えると、設定は次のようになります。`route outside 0.0.0.0 0.0.0.0 172.22.1.1`
`route outside 192.168.200.0 255.255.255.0 10.89.129.2`
`route outside 192.168.200.0 255.255.255.0 10.89.129.2`
`route outside 192.168.200.0 255.255.255.0 10.89.129.2`各エンドポイントの背後に非常に多数のネットワークがある場合には、スタティック ルートの設定は維持するのが困難になります。 そのような場合には、代わりに上記の Reverse Route Injection (RRI) を使用することを推奨します。 RRI は暗号化マップ用 ACL に記載されているすべてのリモート ネットワークのルーティング テーブルのルートをインポートします。 たとえば、暗号化マップ用 ACL とルータ A の暗号化マップは次のようになります。`access-list 110 permit ip 192.168.100.0 0.0.0.255`
`   192.168.200.0 0.0.0.255`
`access-list 110 permit ip 192.168.100.0 0.0.0.255`
`   192.168.210.0 0.0.0.255`
`access-list 110 permit ip 192.168.100.0 0.0.0.255`
`   192.168.220.0 0.0.0.255`
`access-list 110 permit ip 192.168.100.0 0.0.0.255`
`   192.168.230.0 0.0.0.255`

```
crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
 reverse-route set transform-set mySET match address 110
```

Router A を PIX や ASA で置き換えると、設定は次のようになります。

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
crypto map mymap 10 set reverse-route
```

- リモート アクセスの設定では、ルーティングの変更は常に必要とは限りません。 しかし、VPN ゲートウェイ ルータやセキュリティ アプライアンスの背後に他のルータがある場合は、これらのルータで VPN クライアントへのパスを何らかの方法で学習する必要があります。この例では、VPN クライアントが接続する際に 10.0.0.0 /24 の範囲のアドレスを付与されると仮定しています。ゲートウェイと他のルータとの間でルーティング プロトコルが使用されていない場合は、Router 2 などのルータでスタティック ルートを使用できます。

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

ゲートウェイと他のルータとの間で EIGRP や OSPF などのルーティング プロトコルを使用している場合は、先に説明したように Reverse Route Injection (RRI) を使用することを推奨します。 RRI により、VPN クライアントへのルートがゲートウェイのルーティング テーブルに自動的に追加されます。 この後、これらのルートはネットワーク上の他のルータに配信されます。Cisco IOS ルータ：

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
 reverse-route
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco PIX または ASA セキュリティ アプライアンス：

```
crypto dynamic-map dynMAP 10 set transform-set mySET
crypto dynamic-map dynMAP 10 set reverse-route
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

注: VPN クライアントに割り当てられた IP アドレスのプールが、ヘッドエンド デバイスの内部ネットワークと重複していると、ルーティングに問題が生じます。 詳細は、「プライベート ネットワークのオーバーラップ」のセクションを参照してください。

トランスフォーム セットが正しいことを確認する

両端のトランスフォーム セットで使用する IPSec の暗号とハッシュ アルゴリズムが同じであることを確認してください。 詳細は、『Cisco セキュリティ アプライアンス コンフィギュレーション ガイド』の「コマンド リファレンス」セクションを参照してください。

注: ISAKMP ポリシーと PIX/ASA で使用されている IPSec トランスフォーム セットに関して、Cisco VPN クライアントでは DES と SHA を組み合わせたポリシーは使用できません。 DES を使用している場合は、ハッシュ アルゴリズムに MD5 を使用する必要があります。または、3DES と SHA、および 3DES と MD5 といった他の組み合わせも使用できます。

クリプト マップが IPSec トンネルの起点/終点の適切なインターフェイスに適用されていることを確認する

スタティックおよびダイナミックなピアが同じクリプト マップで設定されている場合、クリプト マップのエントリの順序は非常に重要です。 ダイナミック暗証マップのエントリのシーケンス番

号は、他のスタティック暗証マップのすべてのエントリよりも大きい**必要があります**。 スタティック エントリにダイナミック エントリよりも高い番号付けがされている場合、これらのピアでの接続が失敗して、デバッグでは次のように表示されます。

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

注: セキュリティ アプライアンスの各インターフェイスに許可されているのは、ダイナミック クリプトマップが 1 つだけです。

スタティック エントリとダイナミック エントリが含まれるクリプト マップの、正しい番号付けの例を次に示します。 ダイナミック エントリのシーケンス番号が最も大きく、また、ある程度の余裕を持たせてスタティック エントリを追加できるようにしています。

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside
crypto map mymap 60000 ipsec-isakmp dynamic cisco
```

注: クリプト マップ名では大文字と小文字が区別されます。

注: 次のエラー メッセージは、ダイナミック クリプト マップのシーケンスが正しくないためピアが間違ったクリプト マップをヒットしてしまう場合、および対象トラフィックを定義するクリプト アクセス リストが不一致の場合にも発生する可能性があります。 `%%ASA-3-713042: IKE Initiator unable to find policy:`

複数の VPN トンネルを同じインターフェイスで終端するシナリオでは、同じ名前のクリプト マップを作成する必要がありますが（インターフェイスごとに 1 つのクリプト マップしか許可されないため）、シーケンス番号は異なるものにします。 このことは、ルータ、PIX、ASA に該当します。

同じインターフェイスに同じクリプト マップを異なるシーケンス番号で設定するハブ PIX コンフィギュレーションについての詳細は、『VPN Client と拡張認証による、ハブ PIX とリモート PIX 間の IPSec 設定』を参照してください。 同様に、L2L とリモート アクセス VPN シナリオのためのクリプト マップ設定についての詳細は、『PIX/ASA 7.X： 既存の L2L VPN への新しいトンネルやリモートアクセスの追加』を参照してください。

ピア IP アドレスが正しいことを確認する

PIX/ASA セキュリティ アプライアンス 7.x LAN-to-LAN（L2L）の IPsec VPN 設定では、IPSec での接続に特定した記録のデータベースの作成と管理のため、**tunnel-group <name> type ipsec-l2l** コマンドでトンネル グループの **<name>** に**リモート ピアの IP アドレス**（リモートのトンネル エンド）を指定する必要があります。 **tunnel group name** コマンドと **Crypto map set address** コマンドでのピアの IP アドレスは一致している必要があります。 ASDM で VPN を設定する際には、トンネル グループ名は正しいピアの IP アドレスで自動的に生成されます。 ピアの IP アドレスの設定が正しくないと、ログに次のメッセージが含まれる場合があります。その場合は、**ピアの IP アドレス**を正しく設定すると、解決できます。

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

PIX 6.x LAN-to-LAN（L2L）IPSec VPN コンフィギュレーションで、IPSec VPN 接続が成功するには、ピアの IP アドレス（リモートのトンネル エンド）がクリプト マップ内の **isakmp key address** と **set peer** のコマンドと一致している必要があります。

ピアの IP アドレスが ASA 暗号設定で正しく設定されていない場合、ASA は VPN トンネルを確立できず、*MM_WAIT_MSG4* 段階だけでハングします。 この問題を解決するには、設定でピアの IP アドレスを修正します。

VPN トンネルが MM_WAIT_MSG4 状態でハングする場合の **show crypto isakmp sa** コマンドの出力を次に示します。

```
hostname#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG4
```

トンネル グループおよびグループ名を確認する

```
%PIX|ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

このメッセージは、グループ ポリシーで指定されている許可済みトンネルがトンネルグループ設定内の許可済みトンネルと異なっていることが原因でトンネルが廃棄されている場合に表示されます。

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines should read: `vpn-tunnel-protocol ipsec l2tp-ipsec`

デフォルト グループ ポリシー内の既存のプロトコルに対して、デフォルト グループ ポリシー内の IPSec を有効にします。

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

L2L ピアについて XAUTH をディセーブルにする

LAN-to-LAN トンネルとリモート アクセス VPN が同じクリプト マップに設定されていると、LAN-to-LAN ピアに XAUTH 情報の入力を求めるメッセージが表示され、**show crypto isakmp sa** コマンドの出力の「***CONF_XAUTH***」で LAN-to-LAN トンネルに障害が発生します。

SA の出力の例を次に示します。

```
Router#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id slot status X.X.X.X
Y.Y.Y.Y CONF_XAUTH 10223 0 ACTIVE X.X.X.X Z.Z.Z.Z CONF_XAUTH 10197 0 ACTIVE
```

注: この問題は Cisco IOS および PIX 6.x の場合にのみ発生します。PIX/ASA 7.x ではトンネル グループを使用しているため、この問題の影響を受けません。

isakmp キーを入力するときに、**no-xauth** キーワードを使用すると、デバイスからピアに対して XAUTH 情報 (ユーザ名やパスワード) の入力を求められなくなります。 このキーワードによって、スタティックな IPSec ピアに対する XAUTH がディセーブルになります。 同じクリプト マップで、L2L と RA VPN の両方が設定されているデバイスで、これと同様のコマンドを入力します。

```
router(config)#crypto isakmp key cisco123 address 172.22.1.164 no-xauth
```

PIX/ASA 7.x が Easy VPN サーバとして動作しているシナリオでは、Xauth の問題が原因で Easy VPN クライアントがヘッドエンドに接続できなくなります。 この問題を解決するには、次に示すように、PIX/ASA でユーザ認証をディセーブルにします。

```
ASA(config)#tunnel-group example-group type ipsec-ra ASA(config)#tunnel-group example-group
ipsec-attributes ASA(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

isakmp ikev1-user-authentication コマンドについての詳細は、このドキュメントの「その他」のセクションを参照してください。

VPN プールの枯渇

VPN プールに割り当てられている IP アドレスの範囲が不十分の場合、次の 2 つの方法で IP アドレスのアベイラビリティを拡張できます。

1. 既存の範囲を削除し、新しい範囲を定義します。 次に例を示します。`CiscoASA(config)#no ip local pool testvpnpool 10.76.41.1-10.76.41.254 CiscoASA(config)#ip local pool testvpnpool 10.76.41.1-10.76.42.254`
2. 隣接していないサブネットが VPN プールに追加される場合、2 つの別個の VPN プールを定義し、それらを「トンネル グループ属性」の下に順番に指定できます。 次に例を示します。`CiscoASA(config)#ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254 CiscoASA(config)#ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254 CiscoASA(config)#tunnel-group test type remote-access CiscoASA(config)#tunnel-group test general-attributes CiscoASA(config-tunnel-general)#address-pool (inside) testvpnpoolAB testvpnpoolCD CiscoASA(config-tunnel-general)#exit`

ユーザがプールを指定する順序は、ASA がこれらのプールから、このコマンドでプールが表示される順序でアドレスを割り当てるため非常に重要です。

注: グループ ポリシーの address-pools コマンドによるアドレス プール設定は、トンネル グループの address-pool コマンドによるローカル プール設定を上書きします。

VPN Client トラフィックの遅延による問題

VPN 接続で遅延問題がある場合、これを解決するには、次の項目を確認してください。

1. パケットの MSS をさらに削減できるかどうかを確認します。
2. IPSec/udp の代わりに IPSec/tcp が使用されている場合、preserve-vpn-flow を設定します。
3. Cisco ASA をリロードします。

VPN Client が ASA/PIX で接続できない

問題

X-auth が Radius サーバで使用されていると、Cisco VPN Client では認証ができません。

解決策

この問題は xauth のタイムアウトによるものである可能性があります。 この問題を解決するには、AAA サーバのタイムアウト値を大きくします。

次に、例を示します。

```
Hostname(config)#aaa-server test protocol radius hostname(config-aaa-server-group)#aaa-server
test host 10.2.3.4 hostname(config-aaa-server-host)#timeout 10
```

問題

X-auth が Radius サーバで使用されていると、Cisco VPN Client では認証ができません。

解決策

まず、認証が正しく動作していることを確認します。 問題を絞り込むには、最初に ASA のローカル データベースによる認証を確認します。

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

これが正常に動作している場合、問題は Radius サーバ設定に関連しているはずです。

ASA から Radius サーバの接続を確認します。 ping が正常に動作する場合は、ASA の Radius 関連の設定と Radius サーバのデータベース設定を確認します。

Radius に関する問題のトラブルシューティングを行うには、**debug radius** コマンドを使用できます。 **debug radius** 出力の例については、次の出力例を参照してください。

注: ASA で **debug** コマンドを使用する前に、 警告メッセージを参照してください。

「VPN Client Drops Connection Frequently on First Attempt」または「Security VPN Connection terminated by peer Reason 433」または「Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)」

問題

Cisco VPN Client ユーザは、ヘッドエンド VPN デバイスとの接続を試行する際、次のエラーを受け取ることがあります。

「*VPN client drops connection frequently on first attempt*」または「*Security VPN Connection terminated by peer. Reason 433.*」または「*Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)*」または「*Attempted to assign network or broadcast IP address, removing (x.x.x.x) from pool*」

解決策 1

この問題は、ASA/PIX、Radius サーバ、DHCP サーバ、または DHCP サーバとして機能する Radius サーバを介した IP プールの割り当てと関連している場合があります。 **debug crypto** コマンドを使用して、ネットマスクおよび IP アドレスが正しいことを確認します。 また、ネットワーク アドレスおよびブロードキャスト アドレスがプールに含まれていないことも確認します。 また、Radius サーバは、適切な IP アドレスをクライアントに割り当てることができなければなりません。

解決策 2

この問題は、拡張認証の失敗によっても発生します。 このエラーを修復するには、AAA サーバを確認する必要があります。 サーバとクライアントのサーバ認証パスワードを確認し、AAA サーバ

をリロードすることによって、この問題を解決できる場合があります。

解決策 3

この問題のもう一つの回避策は、脅威検出機能をディセーブルにすることです。 別の不完全なセキュリティ アソシエーション（SA）に複数の再送信がある場合、脅威検出機能がイネーブルにされた ASA によってスキャニング攻撃が発生し、VPN ポートが主な攻撃者としてマークされると考えます。 これにより ASA の処理で大量のオーバーヘッドが発生する可能性があるため、脅威検出機能をディセーブルにしてください。 脅威検出をディセーブルにするには、次のコマンドを使用します。

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

この機能の詳細については、「脅威の検出」を参照してください。

注: これは、実際の問題を修正できるかどうかを確認する回避策として使用できます。 Cisco ASA で脅威の検出をディセーブルにすることによって、アプリケーション インスペクションや不完全なセッションに障害が発生するスキャン試行、無効な SPI パケットを含む DoS の軽減など、複数のセキュリティ機能が実際に損なわれるかどうかを確認します。

解決 4

この問題は、トランスフォーム セットが正しく設定されていない場合にも発生します。 この問題を解決するには、トランスフォーム セットを正しく設定します。

リモート アクセス ユーザおよび EZVPN ユーザが、VPN には接続されるものの、外部リソースにアクセスできない

問題

リモート アクセス ユーザが VPN にアクセスすると、インターネットにアクセスできなくなる。

リモート アクセス ユーザが同じデバイス上の他の VPN の背後にあるリソースにアクセスできない。

リモート アクセス ユーザがローカル ネットワークにしかアクセスできない。

解決策

この問題を解決するには、次の解決策を試してください。

- DMZ にあるサーバにアクセスできない
- VPN クライアントが DNS を解決できない
- スプリット トンネル：インターネットや除外されたネットワークにアクセスできない
- ヘアピニング
- ローカル LAN へのアクセス
- プライベート ネットワークのオーバーラップ

DMZ にあるサーバにアクセスできない

VPN クライアントが VPN ヘッドエンド デバイス（PIX/ASA/IOS ルータ）との間に IPSec トンネルを確立すると、その後 VPN クライアント ユーザは内部ネットワーク（10.10.10.0/24）のリソースにはアクセスできますが、DMZ ネットワーク（10.1.1.0/24）にはアクセスできなくなります。

図

DMZ ネットワークのリソースにアクセスするために、スプリット トンネル、NO NAT 設定がヘッドエンド デバイスに追加されていることを確認してください。

例

ASA/PIX

```
ciscoasa#show running-config !--- Split tunnel for the inside network access access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any !--- Split tunnel for the DMZ network access access-list vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0 any !--- Create a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients. ip local pool vpnclient 192.168.1.1-192.168.1.5 !--- This access list is used for a nat zero command that prevents !--- traffic which matches the access list from undergoing NAT. !--- No Nat for the DMZ network. access-list nonat-dmz permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 !--- No Nat for the Inside network. access-list nonat-in permit ip 10.10.10.0 255.255.255.0 192.168.1.0 255.255.255.0 !--- NAT 0 prevents NAT for networks specified in the ACL nonat . nat (DMZ) 0 access-list nonat-dmz nat (inside) 0 access-list nonat-in
```

ASA バージョン 8.3 の設定：

次の設定は、DMZ ネットワークの NAT 免除を設定して、VPN ユーザが DMZ ネットワークにアクセスできるようにする方法を示します。

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

NAT 設定に新しいエントリを追加した後に、NAT 変換をクリアします。

```
Clear xlate
Clear local
```

確認：

トンネルが確立されたら、**Cisco VPN Client** に進み、[Status] > [Route Details] の順に選択して、DMZ ネットワークと内部 ネットワークの両方について安全なルートが表示されることを確認してください。

ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： DMZ でのメール サーバ アクセスの設定例

』を参照してください。

ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： 既存の L2L VPN への新しいトンネルやリモート アクセスの追加』を参照してください。

ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： ASA で VPN クライアントのスプリット トンネリングを許可するための設定例』を参照してください。

Cisco VPN Client (Windows 用は 4.x) と PIX 500 シリーズ セキュリティ アプライアンス 7.x 間にリモート アクセス VPN 接続を設定する方法についての詳細は、『PIX/ASA 7.x および Cisco VPN Client 4.x で Active Directory に対する Windows 2003 IAS RADIUS 認証を使用するための設定例』を参照してください。

VPN クライアントが DNS を解決できない

トンネルを確立した後、VPN クライアントが DNS を解決できない場合は、ヘッドエンド デバイス (ASA/PIX) での DNS サーバの設定に問題がある可能性があります。 さらに、VPN クライアントと DNS サーバ間の接続をチェックしてください。 DNS サーバの設定はグループ ポリシーの設定の下で行い、tunnel-group の一般的な属性の中のグループ ポリシーの下で適用する必要があります。 例：

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP
address(172.16.1.1) !--- and the domain name(cisco.com) in the group policy. group-policy
vpn3000 internal group-policy vpn3000 attributes dns-server value 172.16.1.1 default-domain
value cisco.com !--- Associate the group policy(vpn3000) to the tunnel group !--- using the
default-group-policy. tunnel-group vpn3000 general-attributes default-group-policy vpn3000
```

VPN クライアントが内部サーバに名前で接続できない

VPN クライアントがリモートやヘッドエンド内部ネットワークのホストやサーバに、名前で ping を通すことができません。 この問題を解決するには、ASA でスプリット DNS コンフィギュレーションをイネーブルにする必要があります。

スプリット トンネル：インターネットや除外されたネットワークにアクセスできない

スプリット トンネルを設定すると、リモート アクセス IPSec クライアントが条件に応じてパケットを暗号化された形式で IPSec トンネルに送信したり、あるいはパケットをネットワーク インターフェイスに暗号化されていないクリアテキストの形式で送信したりして、その後に最終的な宛先に送信されるようにすることができます。 スプリット トンネリングは tunnelall トラフィックであるため、デフォルトではディセーブルにされています。

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

注: [excludespecified] オプションは、Cisco VPN Client に対してのみサポートされており、EZVPN クライアントに対してはサポートされていません。

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

スプリット トンネリングの詳細な設定例は、下記のドキュメントを参照してください。

- PIX/ASA 7.x： ASA で VPN クライアントのスプリット トンネリングを許可するための設定

例
- スプリット トンネリングを使用する VPN クライアントが IPSec とインターネットに接続するのをルータで許可する設定例
- VPN 3000 コンセントレータでの VPN クライアントのスプリット トンネリング設定例

ヘアピニング

この機能は、あるインターフェイスに着信した後に同じインターフェイスからルーティングされる VPN トラフィックに対して便利な機能です。 たとえば、ハブ アンド スポークの VPN ネットワークを構築していて、セキュリティ アプライアンスがハブ、リモート VPN ネットワークがスポークである場合、あるスポークが他のスポークと通信するためには、トラフィックがセキュリティ アプライアンスに着信した後、他のスポーク宛てに再び発信される必要があります。

トラフィックが同じインターフェイスから着発信できるようにするには、**same-security-traffic** 設定を使用します。

```
securityappliance(config)#same-security-traffic permit intra-interface
```

ローカル LAN へのアクセス

リモート アクセス ユーザは VPN に接続し、ローカル ネットワークにしかアクセスできません。

さらに詳細な設定例は、『PIX/ASA 7.x： VPN クライアントでローカル LAN アクセスを許可するための設定例』を参照してください。

プライベート ネットワークのオーバーラップ

問題

トンネルを確立した後に内部ネットワークにアクセスできない場合は、VPN クライアントに割り当てている IP アドレスが、ヘッドエンド デバイスの背後にある内部ネットワークと重複していないかどうかを確認してください。

解決策

VPN クライアント、ヘッドエンド デバイスの内部ネットワーク、VPN クライアントの内部ネットワークにそれぞれ割り当てられるプール内の IP アドレスが別のネットワークにあることを、常時、確認してください。 同一のメジャー ネットワークを別のサブネットに割り当てることはできますが、ルーティングに問題が生じる場合があります。

次の例では、「DMZ でサーバにアクセスできない」セクションの*図*と*例*を参照してください。

3 人を超える VPN Client ユーザに接続できない

問題

3 人の VPN クライアントが ASA/PIX に接続していると、 4 人目の接続が失敗します。 失敗した際には、次のエラー メッセージが表示されます。

```
Secure VPN Connection terminated locally by the client.
 Reason 413: User Authentication failed.tunnel rejected; the maximum tunnel count has been
```

reached

解決策

ほとんどの場合、この問題はグループ ポリシー内の同時ログイン設定と最大セッション制限に関係するものです。

この問題を解決するには、次の解決策を試してください。

- 同時ログインを設定する
- CLI による ASA/PIX の設定
- コンセントレータを設定する

詳細は、『Cisco ASA 5500 シリーズ バージョン 5.2 用に選択された ASDM VPN 設定手順』の「グループ ポリシーの設定」セクションを参照してください。

同時ログインを設定する

ASDM で [Inherit] チェックボックスが選択されている場合、ユーザに許可されているのはデフォルトの同時ログイン数になります。 同時ログイン数のデフォルト値は 3 です。

この問題を解決するには、同時ログイン数の値を増やします。

1. ASDM を起動し、[Configuration] > [VPN] > [Group Policy] の順に移動します。
2. 適切な [**Group**] を選択し、[**Edit**] ボタンをクリックします。
3. **[General]** タブを開いたら、**[Connection Settings]** の下にある **[Simultaneous Logins]** に対する **[Inherit]** チェック ボックスの選択を解除します。 フィールドに適切な値を選択します。 **注:** このフィールドの最小値は 0 です。この値にすると、ログインが無効になり、ユーザ アクセスができなくなります。**注:** 別の PC で同じユーザ アカウントを使用してログインすると、現在のセッション (同じユーザ アカウントを使用しますが別の PC で確立された接続) が終了し、新しいセッションが確立されます。 これはデフォルトの動作であり、VPN の同時ログインとは関係ありません。

CLI による ASA/PIX の設定

同時ログイン数を任意の数に設定するには、次の手順を実行します。 この例では、任意の値として 20 を選択しています。

```
ciscoasa(config)#group-policy Bryan attributes ciscoasa(config-group-policy)#vpn-simultaneous-logins 20
```

このコマンドの詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』を参照してください。

VPN セッションをセキュリティ アプライアンスで許可されているよりも低い値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-session-limit** コマンドを使用します。 セッションの制限を解除するには、このコマンドの no 形式を使用します。 現在の設定を上書きするには、このコマンドを再度使用します。

```
vpn-sessiondb max-session-limit {session-limit}
```

次の例には、最大 VPN セッションの制限を 450 に設定する方法が示されています。

```
hostname#vpn-sessiondb max-session-limit 450
```

コンセントレータを設定する

エラー メッセージ

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

解決策

同時ログイン数を任意の数に設定するには、次の手順を実行します。 次のように、SA の同時ログインを 5 に設定してみることもできます。

[Configuration] > [User Management] > [Groups] > [Modify 10.19.187.229] > [General] > [Simultaneouts Logins] の順に選択して、ログイン数を **5** に変更します。

トンネルが確立されるとセッションやアプリケーションを開始できず転送が遅くなる

問題

IPSec トンネルを確立した後に、トンネル経由でアプリケーションやセッションを開始できなくなることがあります。

解決策

ping コマンドを使用してネットワークを確認し、ネットワークからアプリケーション サーバに到達できるかどうかを確認します。 これはルータまたは PIX/ASA デバイスを通過する一時的なパケットのための maximum segment size (MSS; 最大セグメント サイズ) 、特に SYN ビットが設定された TCP セグメントに関する問題である可能性があります。

Cisco IOS ルータ：ルータの Outside インターフェイス (トンネル終端インターフェイス) の MSS 値を変更する

次のコマンドを実行し、ルータの Outside インターフェイス (トンネル終端インターフェイス) の MSS 値を変更します。

```
Router>enable Router#configure terminal Router(config)#interface ethernet0/1 Router(config-
if)#ip tcp adjust-mss 1300 Router(config-if)#end
```

これらのメッセージには、TCP MSS のデバッグ出力が表示されています。

```
Router#debug ip tcp transactions Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 ->
10.0.1.1(38437)] Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS
1300, MSS is 1300 Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751 Sep 5
18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300 Sep 5 18:42:46.251: TCP0:
state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

MSS は設定に従いルータ上で 1300 に調整されています。

詳細は、『PIX/ASA 7.x と IOS： VPN フラグメンテーション』を参照してください。

PIX/ASA 7.X：PIX/ASA のドキュメントを参照

MTU サイズ エラー メッセージと MSS の問題があるため、インターネットに正常にアクセスできなくなったり、トンネル経由での転送が遅くなります。 この問題を解決するには、次のドキュメントを参照してください。

- PIX/ASA 7.x と IOS： VPN フラグメンテーション
- PIX/ASA 7.0 の問題： MSS 超過 - HTTP クライアントが一部の Web サイトをブラウズできない

ASA/PIX から VPN トンネルを開始できない

問題

ASA/PIX インターフェイスから VPN トンネルの始動ができず、トンネルが確立された後でも、リモートのエンド/VPN クライアントでは、VPN トンネルで ASA/PIX の Inside インターフェイスに ping を通すことができません。 たとえば、VPN クライアントでは、VPN トンネル経由で ASA の Inside インターフェイスへの SSH や HTTP での接続が開始できない場合があります。

解決策

グローバル コンフィギュレーション モードで **management-access** コマンドが設定されていないと、PIX の内部インターフェイスではトンネルの反対側からの ping を受信できません。

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access inside
```

注: このコマンドは、VPN トンネル経由で ASA の Inside インターフェイスへの SSH や HTTP での接続を開始するのにも有効です。

注: この情報は、DMZ インターフェイスの場合にも当てはまります。 たとえば、PIX/ASA の DMZ インターフェイスに対して ping を実行する場合や、DMZ インターフェイスからトンネルを起動する場合は、**management-access DMZ** コマンドが必要です。

```
PIX-02(config)#management-access DMZ
```

注: VPN クライアントで接続ができない場合は、ESP と UDP のポートがオープンであることを確認します。ポートがオープンではない場合、VPN クライアントの接続エントリでこのポートを選択することにより、TCP 10000 での接続を試みます。 [modify] > [transport tab] > [IPsec over TCP] の順に右クリックします。 IPSec over TCP の詳細については、『任意のポートで IPsec over TCP をサポートするための PIX/ASA 7.x の設定例』を参照してください。

VPN トンネルを介してトラフィックを渡すことができない

問題

VPN トンネルにトラフィックを渡すことができません。

解決策

この問題は、Cisco Bug ID CSCtb53186（登録ユーザ専用）のために発生します。 この問題を解

決するには、ASA をリロードします。 詳細は、バグを参照してください。

この問題は、ESP パケットがブロックされたときにも発生することがあります。 この問題を解決するには、VPN トンネルを再設定します。

この問題は、データが暗号化されていないが、次の出力に示すように VPN トンネルを介して復号化される場合にのみ発生する場合があります。

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 #pkts decaps: 393, #pkts decrypt: 393,
#pkts verify: 393 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #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 #send
errors: 0, #recv errors: 0
```

この問題を解決するには、次のチェックを行います。

1. クリプト アクセス リストがリモート サイトと一致するかどうか、および NAT 0 アクセス リストが正しかどうか。
2. ルーティングが正しいかどうか、およびトラフィックが inside を通過する outside インターフェイスをヒットするかどうか。 出力例は、復号化が行われているが暗号化は発生しないことを示しています。
3. sysopt permit connection-vpn コマンドが ASA で設定されているかどうか。 設定されていない場合、ASA がインターフェイス チェックから暗号化/VPN トラフィックを除外できるように、このコマンドを設定します。

同じクリプト マップでの VPN トンネルのバックアップ ピアの設定

問題

単一の VPN トンネルで複数のバックアップ ピアを使用する必要があります。

解決策

複数のピアを設定することは、フォールバック リストを指定することと同じです。 トンネルごとに、セキュリティ アプライアンスはリスト内の最初のピアとネゴシエートしようとします。

ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。

ASA は、あらかじめプライマリ ピアとして設定されたクリプト マップを備えている必要があります。 セカンダリ ピアは、プライマリ ピアの後に追加できます。

この設定例では、プライマリ ピアが X.X.X.X、バックアップ ピアが Y.Y.Y.Y と示されています。

ASA(config)#**crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y**
詳細については、『*Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 8.0*』の「クリプト マップ セット ピア」セクションを参照してください。

VPN トンネルのディセーブル/再起動

問題

VPN トンネルを一時的にディセーブルにした後、該当サービスを再起動するには、このセクションで解説する手順を実行します。

解決策

グローバル コンフィギュレーション モードで **crypto map interface** コマンドを使用し、インターフェイスに対する定義済みの クリプト マップ セットを削除します。 このコマンドの **no** 形式を使用して、クリプト マップ セットをインターフェイスから削除します。

hostname(config)#**no crypto map** *map-name* **interface** *interface-name*
このコマンドにより、任意のアクティブなセキュリティ アプライアンス インターフェイスに対するクリプト マップ セットが削除され、該当するインターフェイスで IPSec VPN トンネルが非アクティブになります。

インターフェイス上で IPSec トンネルを再起動するには、該当インターフェイスが IPSec サービスを提供できるように、該当インターフェイスにクリプト マップ セットを割り当てる必要があります。

hostname(config)#**crypto map** *map-name* **interface** *interface-name*

一部のトンネルが暗号化されていない

問題

VPN ゲートウェイで、膨大な数のトンネルが設定されている場合、トンネルがトラフィックを渡さない場合があります。 ASA は、これらのトンネルの暗号化パケットを受信しません。

解決策

この問題は、ASA がトンネルを介して暗号化パケットを渡すことができないためです。 重複する暗号化ルールが ASP テーブル内に作成されます。 これは既知の問題であり、この問題を解決するために、Bug ID CSCtb53186 (登録ユーザ専用) が報告されました。 この問題を解決するには、ASA をリロードするか、このバグが修正されているバージョンにソフトウェアをアップグレードします。

エラー： -%ASA-5-713904: Group = DefaultRAGroup, IP = x.x.x.x, Client is using an unsupported Transaction Mode v2 version.Tunnel terminated.

問題

「%ASA-5-713904: `Group = DefaultRAGroup, IP = 99.246.144.186, Client is using an unsupported Transaction Mode v2 version.`Tunnel terminated」というエラー メッセージが表示されます。

解決策

「Transaction Mode v2」というエラー メッセージが表示される理由は、ASA が IKE Mode Config V6 のみをサポートしており、旧 V2 モード バージョンをサポートしていないためです。このエラーを解決するには、IKE Mode Config V6 バージョンを使用してください。

エラー： -%ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

問題

「%ASA-6-722036: 「Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)」というエラー メッセージが ASA のログに出力されます。 このログの意味と解決方法を教えてください。

解決策

このログ メッセージは、大きなパケットが該当クライアントに送信されたことを示しています。該当パケットの送信元は、クライアントの MTU を意識していません。 また、圧縮不能なデータの圧縮が原因の場合もあります。 その場合の回避策は、revocation-check none svc コマンドを使用して SVC 圧縮を無効にすることです。これによって問題が解決します。

エラー： The authentication-server-group none command has been deprecated

問題

バージョン 7.0.x を実行している PIX/ASA から、7.2.x を実行している他のセキュリティ アプライアンスに VPN の設定を転送すると、次のエラー メッセージが表示されます。

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
instead.
```

解決策

authentication-server-group は、7.2(1) 以降ではサポートされていません。 このコマンドは廃止されており、tunnel-group の general-attributes 設定モードに移行されています。

このコマンドのさらに詳細な情報は、コマンド リファレンスの「isakmp ikev1-user-authentication」セクションを参照してください。

VPN トンネルの一端で QoS をイネーブルにしてあるとエラー メッセージが表示される

問題

VPN トンネルの一端で QoS をイネーブルにしてあると、次のようなエラー メッセージを受け取る場合があります。

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay checking
```

解決策

通常、このメッセージは、トンネルの一端で QoS が実行されている場合に発生します。 これが発生するのは、順序を外れたパケットが検出される場合です。 QoS をディセーブルにすると、これを止められますが、トラフィックがトンネルを通過できる限りは、これを無視することもできます。

WARNING: crypto map entry will be incomplete

問題

crypto map mymap 20 ipsec-isakmp コマンドを実行すると、次のエラーが発生する場合があります。

```
 crypto map entry will be incomplete
```

次に、例を示します。

```
ciscoasa(config)#crypto map mymap 20 ipsec-isakmp WARNING: crypto map entry will be incomplete
```

解決策

これは、新規のクリプト マップを作成するときの一般的な Warning メッセージで、動作前に設定される必要がある、アクセス リスト (マッチ アドレス) 、トランスフォーム セット、ピア アドレスなどを設定するためのリマインダとなります。 クリプト マップを定義するために入力する最初の行がコンフィギュレーションに表示されないのも、正常です。

エラー： -%ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside

問題

VPN トンネルを介して大きな ping パケットを渡すことができません。 大きな ping パケットを渡そうとすると、「%ASA-4-400024: `IDS:2151 Large ICMP packet from to on interface outside`

解決策

この問題を解決するには、シグニチャ 2150 および 2151 をディセーブルにします。これらのシグニチャをディセーブルにすると、ping が正常に動作します。

シグニチャをディセーブルにするには、次のコマンドを使用します。

ASA(config)#ip **audit signature 2151 disable**

ASA(config)#ip **audit signature 2150 disable**

エラー： -%PIX|ASA-4-402119: IPSEC： Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.

問題

ASA のログ メッセージで次のエラーを受け取りました。

```
Error: -%PIX|ASA-4-402119: IPSEC Received a protocol packet (SPI=spi, sequence number= seq_num)
from remote_IP (username) to local_IP that failed anti-replay checking.
```

解決策

このエラーを解決するには、crypto ipsec security-association replay window-size コマンドを使用して、ウィンドウ サイズを変更します。

```
hostname(config)#crypto ipsec security-association replay window-size 1024
```

注: 再生防止の問題を除去するには、フルのウィンドウ サイズ 1024 を使用するよう推奨します。

Error Message - %PIX|ASA-4-407001: Deny traffic for local-host interface_name: inside_address, license limit of number exceeded

問題

インターネットに接続できないホストがほとんどなく、次のエラー メッセージが syslog に出力されます。

```
Error Message - %PIX|ASA-4-407001: Deny traffic for local-host interface_name: inside_address,
license limit of number exceeded
```

解決策

このエラー メッセージは、使用中のライセンスのユーザ限度をユーザの数が超えると出力されます。 このエラーは、ライセンスをアップグレードして、ユーザ数を増やすと解決できます。 ユーザ ライセンスに含まれるユーザ数としては、50 名、100 名、または無制限を必要に応じて選択できます。

Error Message - %VPN_HW-4-PACKET_ERROR:

問題

「Error Message - %VPN_HW-4-PACKET_ERROR:」というエラー メッセージは、ルータが受信する HMAC を含む ESP パケットが一致していないことを示します。 このエラーは、次の問題によって発生する可能性があります。

- 欠陥のある VPN H/W モジュール
- 不正な ESP パケット

解決策

このエラー メッセージを解決するには、

- トラフィックの中断がない場合、エラー メッセージを無視します。
- トラフィックの中断がある場合は、モジュールを交換します。

エラー メッセージ： Command rejected: delete crypto connection between VLAN XXXX and XXXX, first.

問題

このエラー メッセージは、スイッチのトランク ポートに許可された VLAN を追加しようとすると表示されます。 `Command rejected:` delete crypto connection between VLAN XXXX and VLAN XXXX, first...

WAN エッジ トランクは、追加の VLAN を許可するように変更できません。 つまり、**IPSEC VPN SPA** トランクに VLAN を追加することはできません。

このコマンドを許可すると、潜在的な IPSec セキュリティ違反を引き起こす、インターフェイスの許可済み VLAN リストに属している暗号化で接続されたインターフェイス VLAN を発生させるので、このコマンドは拒否されます。 この動作は、すべてのトランク ポートに適用されることに注意してください。

解決策

switchport trunk allowed vlan （ vlanlist ）コマンドの代わりに、switchport trunk allowed vlan none コマンドまたは switchport trunk allowed vlan （ vlanlist ）コマンドを使用します。

Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropping packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

問題

このエラーは、VPN トンネルの終端にあるデバイスから Telnet を試みるか、ルータ自体から Telnet を試みると発生します。

```
Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropping packet - Invalid Window Scale
```

```
option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1,
factor 2)]
```

解決策

ユーザ ライセンスに含まれるユーザ数としては、50 名、100 名、または無制限を必要に応じて選択できます。 高帯域高遅延ネットワーク (LFN) でデータの高速送信を可能にするために、ウィンドウ スキャニングが追加されました。 これらは、通常、非常に大きな帯域幅ではあるが高遅延ではない接続です。 衛星通信を使用するネットワークは、衛星リンクには常に高い伝搬遅延があるが、通常は高帯域幅であるため LFN の 1 例です。 ウィンドウ スケーリングが LFN をサポートできるようにするには、TCP ウィンドウ サイズを 65,535 より大きくする必要があります。 このエラー メッセージは、TCP ウィンドウのサイズを 65,535 より大きいサイズに増やすことによって解決できます。

%%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Please update this issue flows

問題

VPN トンネルが起動すると、次のエラー メッセージが表示されます。

```
%%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Please update this issue
flows
```

解決策

NAT を使用するホストと同じインターフェイス上ではないときに、この問題を解決するには、ホストに接続された実際のアドレスの代わりに、マッピングされたアドレスを使用します。 また、アプリケーションに IP アドレスが埋め込まれている場合は、**inspect** コマンドをイネーブルにします。

%%PIX|ASA-5-713068: Received non-routine Notify message: notify_type

問題

VPN トンネルが起動に失敗すると、次のエラー メッセージが表示されます。

```
%%PIX|ASA-5-713068: Received non-routine Notify message: notify_type
```

解決策

このメッセージは、設定ミスによって (つまり、ピア上のポリシーまたは ACL の設定が同一でない場合に) 発生します。 ポリシーと ACL が一致する場合、トンネルは問題なく起動します。

%%ASA-5-720012: ((VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit (または) %ASA-6-

720012: ((VPN-unit) Failed to update IPsec failover runtime data on the standby unit

問題

Cisco 適応型セキュリティ アプライアンス（ASA）をアップグレードしようとすると、次のいずれかのエラー メッセージが表示されます。

```
%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit.

%%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.
```

解決策

このエラー メッセージは情報伝達のためのエラーです。 このメッセージは、ASA または VPN の機能に影響しません。

このメッセージは、対応する IPSec トンネルがスタンバイ装置で削除されているため、VPN フェールオーバー サブシステムが IPSec 関連のランタイム データをアップデートできないときに表示されます。 これを解決するには、アクティブ装置で **wr standby** コマンドを実行します。

この動作に対処し、これらのバグが修正される ASA のソフトウェア バージョンにアップグレードするために、2 つのバグが報告されました。 詳細は、Cisco Bug ID CSCtj58420（登録ユーザ専用）および CSCtn56517（登録ユーザ専用）を参照してください。

エラー： -%ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0

問題

「%ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0」というエラー メッセージが表示され、トンネルが起動できません。

解決策

このメッセージは、IKE ピア アドレスが L2L トンネルに対して設定されていない場合に表示されます。 このエラーは、クリプト マップのシーケンス番号の変更し、その後クリプト マップを削除し、再適用することによって解決できます。

エラー： %%ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.

問題

「%ASA-3-752006: `Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Probable mis-configuration of the crypto map or tunnel-group.` というエラー メッセージが Cisco ASA に記録されます。

解決策

このエラー メッセージは、クリプト マップまたはトンネル グループの設定ミスによって発生する可能性があります。 両方とも正しく設定されていることを確認します。 このエラー メッセージの詳細については、「エラー 752006」を参照してください。

次に是正措置の一部を示します。

- （たとえば、ダイナミック マップに関連付けられていない）クリプト ACL を削除します。
- 未使用の IKEv2 関連の設定があれば削除します。
- クリプト ACL が正しく一致していることを確認します。
- 重複したアクセス リスト エントリがあれば削除します。

エラー： %%ASA-4-402116: IPSEC： Received an ESP packet (SPI= 0x99554D4E, sequence number= 0x9E) from XX.XX.XX.XX (user= XX.XX.XX.XX) to YY.YY.YY.YY

LAN-to-LAN VPN トンネルのセットアップでは、次のエラーが ASA の一端に表示されます。

```
The decapsulated inner packet doesn't match the negotiated policy in the SA.

The packet specifies its destination as 10.32.77.67, its source as 10.105.30.1, and its protocol
as icmp.

The SA specifies its local proxy as 10.32.77.67/255.255.255.255/ip/0 and its remote_proxy as
10.105.42.192/255.255.255.224/ip/0.
```

解決策

VPN トンネルの両端で定義されている対象トラフィックのアクセス リストを確認する必要があります。 両方が正確なミラー イメージのように一致する必要があります。

0xffffffff エラーにより、仮想アダプタをイネーブルにする 64 ビット VA インストーラを起動できない

問題

AnyConnect が接続に失敗すると、「Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff」というログ メッセージが表示されます。

解決策

この問題を解決するには、次の手順を実行します。

1. [System] > [Internet Communication Management] > [Internet Communication settings] の順に選択し、[Turn Off Automatic Root Certificates Update] がディセーブルになっていることを確認します。
2. ディセーブルになっている場合、影響を受けるマシンとテストに再度割り当てられた GPO

の**管理用テンプレート**部分全体をディセーブルにします。
詳細は、「Turn off Automatic Root Certificates Update 」 を参照してください。

Error 5: No hostname exists for this connection entry. Unable to make VPN connection.

問題

新しい PC のインストール中に、「Error 5: `No hostname exists for this connection entry.` Unable to make VPN connection error message」というエラー メッセージが表示されます。

解決策

これは、Cisco Bug ID CSCso94244 (登録ユーザ専用) によるものです。 詳細は、このバグを参照してください。

Cisco VPN Client は Windows 7 のデータ カードでは機能しない

問題

Cisco VPN Client は Windows 7 のデータ カードでは動作しません。

解決策

Windows 7 にインストールされた Cisco VPN Client は、データ カードが Windows 7 マシンにインストールされた VPN クライアントでサポートされていないため 3G 接続では動作しません。

警告メッセージ：＂「VPN functionality may not work at all」

問題

ASA の outside インターフェイスで isakmp をイネーブルにしようとすると、次の警告メッセージが表示されます。

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

この時点で、ssh を介して ASA にアクセスします。 HTTPS が停止し、他の SSL クライアントにも影響を与えます。

解決策

この問題は、ロガーやクリプトなどの異なるモジュールのメモリ要件が原因です。 **logging queue 0** コマンドを使用していないことを確認します。 このコマンドはキューのサイズを 8192 に設定し、その結果メモリ割り当てが急激に増大します。

ASA5505 および ASA5510 などのプラットフォームでは、このメモリ割り当てによって他のモジ

ュール（IKE など）がメモリ不足になりがちになります。 このような種類に動作に対処するために、Cisco Bug ID CSCtb58989（登録ユーザ専用）が記録されています。 この問題を解決するには、ロギング キューを小さい値（512 など）に設定します。

IPSec Padding エラー

問題

次のエラー メッセージが表示されます。

```
%PIX|ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
 0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
 incorrect IPsec padding
```

解決策

この問題は、IPSec VPN がハッシュ アルゴリズムなしでネゴシエートするために発生します。 パケット ハッシュにより、ESP チャネルの完全性チェックが確実に行われます。 つまりハッシュなしの場合、不正なパケットが Cisco ASA で検出されずに受け入れられ、これらのパケットの復号化が試行されます。 ただし、これらのパケットが不正であるため、ASA はパケットを復号化する間に欠陥を検出します。 この結果、パディング エラー メッセージが表示されます。

VPN のトランスフォーム セットにハッシュ アルゴリズムを組み込み、ピア間のリンクの最小パケットの変形を確保することを推奨します。

リモート サイトの電話の無音遅延時間

問題

リモート サイトの電話で無音の遅延時間が発生します。 どうすれば、この問題を解決できますか。

解決策

この問題を解決するには、Skinny および SIP インスペクションをディセーブルにします。

```
asa(config)# no inspect sip asa(config)# no inspect skinny
```

VPN のトンネルが 18 時間ごとに接続解除される

問題

ライフタイムが 24 時間に設定されているにもかかわらず、VPN トンネルは 18 時間ごとに接続解除されます。

解決策

ライフタイムは SA が鍵の再生成に使用できる最大時間です。 設定でライフタイムとして入力する値は、SA の鍵再生成時間によって異なります。 そのため、現在のライフタイムが期限切れになる前に、新しい SA（IPsec の場合は SA のペア）とネゴシエートする必要があります。 鍵再生

成時間は、最初の鍵再生成が失敗した場合に複数回試行できるように、常にライフタイムよりも小さい値にする必要があります。 RFC では、鍵再生成時間の計算方法は指定されていません。これは、実装者の裁量に委ねられています。 したがって、この時間は、使用するプラットフォーム、ソフトウェア バージョンなどによって異なります。

一部の実装では、鍵再生成タイマーを計算するために任意の係数を使用できます。 たとえば、ASA がトンネルを開始する場合、64800 秒 = 86400 x 75% として鍵を再生成することができます。 ルータが開始する場合、ASA は、鍵再生成を開始する時間よりも長く待機する時間をピアに指定することができます。 これにより、VPN ネゴシエーションに別のキーを使用するために、VPN セッションを 18 時間ごとに接続解除することができます。 これにより、VPN ドロップや VPN の問題を引き起こさないようにする必要があります。

LAN-to-Lan トンネルが再ネゴシエートされた後にトラフィック フローが維持されない

問題

LAN to LAN トンネルが再ネゴシエートされた後に、トラフィック フローが維持されません。

解決策

ASA は ASA を通過するすべての接続を監視し、アプリケーション検査機能に従って状態テーブルでエントリを維持します。 VPN を通過する暗号化済みトラフィックの詳細は、セキュリティ アソシエーション（SA）データベースの形式で維持されます。 LAN to LAN VPN 接続では、2 つの異なるトラフィック フローが維持されます。 1 つは VPN ゲートウェイ間の暗号化されたトラフィックです。 もう 1 つは VPN ゲートウェイの背後にあるネットワーク リソースと反対側の背後にあるエンド ユーザ間のトラフィック フローです。 VPN を終了すると、この特定 SA のフロー詳細は削除されます。 ただし、この TCP 接続用に ASA によって維持されていた状態テーブル エントリは、アクティビティがないために古くなり、これがダウンロードを妨害します。 つまり、ユーザ アプリケーションが終了している間でも、ASA はこの特定フローの TCP 接続を維持します。 しかし TCP アイドル タイマーが切れると、TCP 接続は離れて最終的にタイムアウトになります。

この問題は、Persistent IPSec Tunneled Flows と呼ばれる機能の導入によって解決しました。VPN トンネルの再ネゴシエーション時の状態テーブル情報を保持するために、新しいコマンド、sysopt connection preserve-vpn-flows、が Cisco ASA に統合されました。 デフォルトでは、このコマンドはディセーブルです。 これを有効にすると、L2L VPN が中断から回復してトンネルを再確立したときに、Cisco ASA は TCP 状態テーブル情報を維持します。

エラー メッセージは帯域幅が暗号化機能のために達したことを示す

問題

次のエラー メッセージが 2900 シリーズ ルータで受信されます。

```
Error: Mar 20 10:51:29: %%CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps reached
for Crypto functionality with securityk9 technology package license.
```

解決策

これは、米国政府によって発行された厳格なガイドラインのために発生する既知の問題です。 これによれば、securityk9 ライセンスは 90Mbps に近いレートまでペイロード暗号化をイネーブルにし、デバイスに対する暗号化されたトンネル/TLS セッションの数を制限することだけが可能です。 暗号化の輸出制限に関する詳細は、『Cisco ISR G2 SEC and HSEC Licensing』を参照してください。

シスコ デバイスの場合、双方向合計 170 Mbps の ISR G2 ルータの着信または発信の 85Mbps 単方向トラフィック未満で取得されます。 この要件は Cisco 1900、2900、3900 ISR G2 プラットフォームに適用されます。 次のコマンドは、これらの制限を表示するのに便利です。

```
Router#show platform cerm-information Crypto Export Restrictions Manager(CERM) Information: CERM
functionality: ENABLED ---------------------------------------------------------------- Resource
Maximum Limit Available ---------------------------------------------------------------- Tx
Bandwidth(in kbps) 85000 85000 Rx Bandwidth(in kbps) 85000 85000 Number of tunnels 225 225
Number of TLS sessions 1000 1000 ---Output truncated----
```

この動作を解決するためのバグが報告されています。 詳細は、Cisco Bug ID CSCtu24534（登録ユーザ専用）を参照してください。

この問題を回避するには、HSECK9 ライセンスを購入する必要があります。 hseck9 機能ライセンスでは、ペイロード暗号化機能が拡張され、VPN トンネル数とセキュアな音声セッション数が増加します。 Cisco ISR ルータ ライセンスの詳細は、『ソフトウェア アクティベーション』を参照してください。

問題： 受信側復号化トラフィックが動作している場合でも、IPSec トンネルの発信側暗号化トラフィックで障害が発生する可能性があります。

解決策

この問題は、複数の鍵再生成後の IPSec 接続で見られますが、この問題を引き起こす条件は明確ではありません。 この問題の存在は、**show asp drop** コマンドの出力を調べて、Expired VPN context カウンタが発信パケットごとに増加することを確認することによって確立できます。 詳細は、Cisco Bug ID CSCtd36473（登録ユーザ専用）を参照してください。

その他

show crypto isakmp sa コマンドと debug コマンドの出力に AG_INIT_EXCH メッセージが表示される

トンネルが始動されないと、**show crypto isakmp sa** コマンドの出力と **debug** 出力にも AG_INIT_EXCH メッセージが表示されます。 この理由は ISAKMP ポリシーのミスマッチによる可能性がありますが、あるいは、ポート udp 500 が途中でブロッキングされている場合も考えられます。

「Received an IPC message during invalid state」というデバッグ メッセージが表示される

このメッセージは情報提供のためのものであり、VPN トンネルの接続解除に対応するものではありません。

関連情報

- PIX/ASA 7.0 の問題： MSS 超過 - HTTP クライアントが一部の Web サイトをブラウズできない
- PIX/ASA 7.x と IOS： VPN フラグメンテーション
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- IPSec ネゴシエーション/IKE プロトコル
- Cisco VPN 3000 シリーズ コンセントレータ
- テクニカルサポートとドキュメント - Cisco Systems