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

内容

はじめに

このドキュメントでは、IPsec VPN の問題の最も一般的な解決策について説明します。

背景説明

ここで説明するソリューションは、シスコテクニカルサポートが解決したサービスリクエストから直接得られたものです。

これらのソリューションの多くは、IPSec VPN接続の詳細なトラブルシューティングの前に実装されています。

このドキュメントでは、接続のトラブルシューティングを開始する前に試す一般的な手順の概要について説明します。

このドキュメントの設定例はルータおよびセキュリティアプライアンスで使用するためのものですが、ほとんどすべての概念はVPN 3000(VPN 3000)にも適用されます。

Cisco IOS®ソフトウェアとの両方でIPSecのトラブルシューティングに使用される一般的なdebugコマンドの説明については、『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しません。

警告：このドキュメントで説明されているソリューションの多くは、デバイス上のすべてのIPSec VPN接続が一時的に失われる原因とな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設定に関する知識があることが推奨されます。

- Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco IOS(R) ルータ

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 ASA 5500 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

ドキュメント表記の詳細については、『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。

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。

解決方法

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。

これらのソリューションは特定の順序で記載されているわけではありませんが、詳細な修復を行う前に確認または試行する項目のチェックリスト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提供され、数多くの問題を解決しています。

- 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コマンドが存在することの確認（/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説明するコマンドの一部は、スペースの関係上2行にわたって表記されています。

NAT トラバーサルをイネーブルにする（#1 RA VPN の問題）

NAT-Traversal（またはNAT-T）を使用すると、VPNトラフィックがLinksys SOHOルータなどのNATまたはPATデバイスを通過できるようになります。

NAT-Tがイネーブルになっていない場合、VPN Clientユーザは問題なくASAに接続しているように見えますが、セキュリティアプライアンスの背後にある内部ネットワークにアクセスできません。

NAT/PATデバイスでNAT-Tをイネーブルにしていないと、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アドレスから同時にログインできない場合は、**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®ではNAT-Tがデフォルトで有効になっています。

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。この例の20はキープアライブ時間（デフォルト）です。

ASA

```
<#root>

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に移動し、Modifyをクリックします。新しいウィンドウが開き、ここでTransporttabを選択します。

このタブで、Enable Transparent Tunnelingand theIPSec over UDP（NAT / PAT）オプションボタンをクリックします。次に、Saveをクリックして接続をテストします。

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用のUDP 4500、UDP 500、およびESPポートを許可することが重要です。

ASAでのACL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。

接続が正しいことをテストする

VPN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実行するデバイスでpingcommandコマンドを使用してVPN接続をテストしています。

通常この目的にはpingは機能しますが、正しいインターフェイスからpingを発信することが重要です。

pingの送信元が正しくない場合は、実際には正しく動作しているにもかかわらず、VPN接続が失敗したように見える可能性があります。次に例を示します。

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
```

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APINGSを送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。

いずれかのルータの外部インターフェイスから送信されたAPは暗号化されません。特権EXECモードでpingcommandの拡張オプションを使用して、ルータの内部インターフェイスからpingを発信します。

<#root>

```
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
```

この図のルータがASAセキュリティアプライアンスに置き換えられたとします。接続テストに使用するpingは、insidekeyword:

<#root>

```
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
```

yourpingを使用して、セキュリティアプライアンスのInsideインターフェイスを対象とすることは推奨されません。

yourpingでInside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enablemanagement-accessを実行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。

<#root>

```
securityappliance(config)#
```

management-access inside

接続に問題がある場合は、VPNのフェーズ1(1)でも機能しません。

ASAで接続が失敗した場合、SAの出力は次の例のようになります。これは、暗号ピアの設定が正しくない可能性や、ISAKMPプロポーザルの設定が正しくない可能性を示しています。

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
```

```
    Rekey   : no               State   : MM_WAIT_MSG2
```

状態はMM_WAIT_MSG2からMM_WAIT_MSG5までであり、これはメインモード(MM)での状態交換の失敗を示します。

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。

<#root>

```
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トンネルが機能している兆候がない場合は、ISAKMPがイネーブルになっていない可能性があります。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®

<#root>

```
router(config)#
```

crypto isakmp enable

Cisco ASA(外部を任意のインターフェイスに置き換える)

<#root>

```
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
```

このエラーの原因としては、ASAの背後にあるクライアントが、インターフェイスでisakmpを有効にする前にUDPポート500へのPATを取得することが考えられます。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。

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確認します。

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
```

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。そうでない場合、LAN-to-LAN(L2L)IPSecトンネルはASA/Cisco IOS®ルータで確立されません。

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。

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pfscommand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。

<#root>

```
hostname(config-group-policy)#
```

pfs {enable | disable}

設定から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。値が転送され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。

<#root>

```
hostname(config-group-policy)#
```

no pfs

Cisco IOS®ルータ：

このクリプトマップ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がPFSを要求する必要があることを指定するには、クリプトマップ設定モードでsset pfscommandを使用します。

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信する際にIPSecでPFSが必要であることを指定するには、クリプトマップ設定モードでsset pfscommand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 Diffie-Hellman 交換が実行される際に IPSec で 768 ビットの Diffie-Hellman プライム モジュラス 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 Diffie-Hellman 交換が実行される際に IPSec で 1024 ビットの Diffie-Hellman プライム モジュラス グループを使用する必要があることを指定します。

以下に例を挙げます。

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

set pfs group2

古いまたは現在のセキュリティアソシエーション（トンネル）のクリア

このエラーメッセージがCisco IOS®®ルータで発生した場合、問題はSAが期限切れであるか、クリアされていることです。

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。

<#root>

%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。

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限り、ここで一覧されているコマンドによってデバイス上のすべてのセキュリティアソシエーションがクリアされる可能性があります。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。

    a. Cisco Cisco IOS®

    <#root>

    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa

    b. Cisco ASAセキュリティアプライアンス

```
<#root>

securityappliance#

show crypto isakmp sa

securityappliance#

show crypto ipsec sa
```

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。

   a. Cisco IOS®

      a. ISAKMP (フェーズ I)

```
<#root>

router#

clear crypto isakmp

 ?
  <0 - 32766>  connection id of SA
  <cr>
```

      b. IPSec (フェーズ II)

```
<#root>

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>
```

   b. Cisco ASAセキュリティアプライアンス

      a. ISAKMP (フェーズ I)

```
<#root>

securityappliance#
```

```
clear crypto isakmp sa
```

b. IPSec (フェーズ II)

```
<#root>

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、「%ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekey attempt due to collisionerror」というメッセージが/ASAで表示されます。

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。

ASA

```
<#root>

hostname(config)#
```

```
isakmp policy 2 lifetime  14400
```

Cisco IOS®ルータ

<#root>

```
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.理由426：最大設定ライフタイムを超過しました。

このエラーメッセージを解決するには、IKEセキュリティアソシエーション(SA)のライフタイムを無限大に設定するために、elifetimevalueをゼロ(0)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
```

また、group-policyでre-xauthを無効にして問題を解決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。

次のコマンドを使用して、Cisco IOS®でISAKMPキープアライブを設定します。

<#root>

```
router(config)#

crypto isakmp keepalive 15
```

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。

トンネルグループ名10.165.205.222のCisco ASA

```
<#root>

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 ASA(トンネルグループ名10.165.205.222)

IKEキープアライブ処理を無効にします（デフォルトでは有効）。

```
<#root>

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

問題が発生したクライアントPCで%System Root% > Program Files > Cisco Systems >VPN Client > Profileson the Client PCの順に移動し、IKEキープアライブをディセーブルにして、

PCFファイルを必要に応じて接続に合わせて編集します。

ForceKeepAlives=0（デフォルト）をForceKeepAlives=1に変更します。

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

多くの場合、IPSec VPNトンネルが機能しない場合は、単純な入力エラーが原因である可能性があります。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、VPN Clientとヘッドエンドデバイスの間でグループ名または事前共有キーが一致しない場合に発生する可能性があります。

```
 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... possibly 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)
```

警告：暗号関連のコマンドを削除すると、1つまたはすべてのVPNトンネルがダウンする可能性があります。これらのコマンドは慎重に使用し、crypto関連のコマンドを削除する前に組織の変更管理ポリシーを参照してください。

次のコマンドを使用して、Cisco IOS®でピア10.0.0.1またはgroupvpngroupinに対する事前共有キーのsecretkeyを削除し再入力します。

Cisco LAN-to-LAN VPN

```
<#root>

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

```
<#root>

router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

次のコマンドを使用して、/ASAセキュリティアプライアンスでピア10.0.0.1の事前共有キーのsecretkeyを削除および再入力します。

シスコ6.x

```
<#root>

(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x以降

```
<#root>

securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#

ikev1


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ネゴシエーション中の事前共有鍵の不一致が原因で発生します。

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

```
<#root>

ASA#

show crypto isakmp sa


Active SA: 1
Rekey SA: 0 (A tunnel reports 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キーを再入力します。事前共有キーは一意で一致している必要があります。詳細については、「事前共有キー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や一部のVPNサイトの起動の失敗など、さまざま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関連付けられたすべてのIPSecトンネルが必ずダウンします。次の手順を実行する前に、慎重に進み、組織の変更管理ポリシーを考慮してください。

Cisco IOS®でクリプトマップを削除および置き換えるには、次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 mapcommandのno形式を使用します。

```
<#root>

router(config-if)#

no crypto map mymap
```

引き続きenoformを使用してクリプトマップ全体を削除します。

```
<#root>

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。

```
<#root>

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
```

ASAでクリプトマップを削除および置き換えるには、次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 mapcommandのno形式を使用します。

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

引き続きthenoformを使用して、他のクリプトマップコマンドを削除します。

<#root>

```
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。

<#root>

```
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
```

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コマンドの存在の確認（ASAのみ）

コマンドdssysopt connection permit-ipsecandsysopt connection permit-vpnallowは、IPSecトンネルからのパケットとそのペイロードをセキュリティアプライアンスのインターフェイスACLをバイパスします。

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issysopt 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issysopt connection permit-vpnです。

6.xでは、この機能はデフォルトで無効になっています。/ASA 7.0(1)以降では、この機能はデフォルトで有効になっています。次のshowコマンドを使用して、デバイスで関連するsysoptcommandが有効になっているかどうかを確認します。

Cisco ASA

```
<#root>

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)
```

デバイスに対してcorrectsysoptcommandを有効にするには、次のコマンドを使用します。

Cisco ASA

```
<#root>

securityappliance(config)#

sysopt connection permit-vpn
```

sysopt接続コマンドを使用しない場合は、送信元から宛先への必要な対象トラフィックを明示的に許可します。

たとえば、リモートデバイスのリモートからローカルLAN、およびリモートデバイスの外部インターフェイスからローカルデバイスの外部インターフェイスへの「UDPポート500」は、外部ACLに含まれます。

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、失敗の原因は、ピアがそのピアの識別情報を認識できなかったか、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、ファイアウォールユニットのISAKMP IDはIPアドレスに設定されます。

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。

ピアに送信されるようにフェーズ2 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theisakmp identitycommand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 typ
```

または

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

または

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

ASA設定移行ツールを使用してからASAに設定を移行した後、VPNトンネルが起動できず、次のメッセージがログに表示されます。

[IKEv1]：グループ= x.x.x.x、IP = x.x.x.x、古いPeerTblEntryが見つかりました、削除します！

[IKEv1]：グループ= x.x.x.x、IP = x.x.x.x、相関テーブルからのピアの削除に失敗しました。一致しませんでした。

[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete()：フェーズ2 SAを識別するSPIがありません！

[IKEv1]：グループ= x.x.x.x、IP = x.x.x.x、相関テーブルからのピアの削除に失敗しました。一致しませんでした。

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パラメータにかかわらず30分後に接続解除され、**PEER_DELETE-IKE_DELETE**_UNSPECIFIEDerrorが発生します。

idle timeoutandsession timeoutasnoneeを設定して、サードパーティのデバイスが使用されている場合でもトンネルがドロップされないように、トンネルをalwaysupにします。

ASA

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

<#root>

```
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-timeoutcommandコマンドを使用して、VPN接続の最大時間を設定します。

<#root>

hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-session-timeout none

tunnel-allconfiguredを設定した場合、VPN-idle timeoutを設定しても、すべてのトラフィックがトンネルを通過するため（tunnel-allが設定されているため）機能しないため、idle-timeoutを設定する必要はありません。

したがって、対象トラフィック（またはPCによって生成されたトラフィック）は対象トラフィックであり、アイドルタイムアウトは動作しません。

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ipsec security-association idle-timemcommand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。

<#root>

crypto ipsec security-association idle-time

seconds

時間は秒単位で測定され、このアイドルタイマーにより、非アクティブなピアがSAを維持できるようになります。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 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1つ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。これには、LAN-to-LANセットアップのクリプトACLまたはリモートアクセス設定のスプリットトンネル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トンネルを一方向に流れたり、トンネルにまったく送信されなかったりする可能性があります。

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必ずバインドします。

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 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。

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。ルータでは、これはroute-mapcommandを使用することを意味します。

ASAでは、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、Cisco 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に設定しています。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
```

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除外ACLは、ポート番号（23、25など）では機能しません。

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、音声コールが機能しません。

NAT免除ACLの設定ミスに問題がある可能性があるため、トラブルシューティングを行う前にVPN接続のステータスを確認することを推奨します。

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。

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

誤った例：

```
<#root>

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。

つまり、ACLは他のACLをmirroreachする必要があります。この例では、LAN-to-LANトンネルは192.168.100.0 /24と192.168.200.0 /24の間に設定されます。

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
```

ここでは説明していませんが、同じ概念がASAセキュリティアプライアンスにも適用されます。

ASAでは、リモートアクセス設定用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アクセスリストである必要があります。

Cisco IOS®ルータは、スプリットトンネルに拡張ACLを使用できます。拡張アクセスリストでスプリットトンネルACLの送信元に「any」を使用する方法は、スプリットトンネルをディセーブルにする方法と似ています。

スプリットトンネルには、拡張ACL内の送信元ネットワークのみを使用します。

正しい例：

<#root>

```
access-list 140 permit ip
10.1.0.0 0.0.255.255
 10.18.0.0 0.0.255.255
```

誤った例：

<#root>

```
access-list 140 permit ip
any
 10.18.0.0 0.0.255.255
```

Cisco IOS®

<#root>

```
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 ASA

<#root>

```
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
```

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：

バージョン8.3の両方のASAを使用して、HOASAとBOASAの間にサイト間VPNを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 ClientまたはサイトVPNがリモートエンドデバイスとのトンネルを確立できない場合は、2つのピアに同じ暗号化、ハッシュ、認証、およびDiffie-Hellman(DH)パラメータ値が含まれていることを確認します。

リモートピアポリシーで、イニシエータが送信したポリシーのライフタイム以下のライフタイムが指定されていることを確認します。

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, drop
```

このメッセージは通常、ISAKMPポリシーの不一致またはNAT 0文の欠落が原因で表示されます。

また、次のメッセージも表示されます。

```
Error Message    %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に入っていることを示しています。このエラーメッセージは、次のいずれかの理由が原因で発生します。

- いずれかのピア上でフェーズが一致していない
- ACLはピアのフェーズ1の完了をブロックする

このメッセージは通常、**Removing peer from peer table failed, no match!**エラーメッセージの後に表示されます。

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。

ASAで使用されているISAKMPポリシーとIPsecトランスフォームセットに関して、Cisco VPN ClientはDESとSHAの組み合わせを使用できません。

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

ルータやASAセキュリティアプライアンスなどの暗号化デバイスに、VPNトンネル経由でトラフィックを送信するための適切なルーティング情報があることを確認してください。

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、それらのルータがトンネルへの到達方法と、反対側にあるネットワークを認識していることを確認します。

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
```

ルータAを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
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。

<#root>

```
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
```

ルータAをah ASAに置き換えると、設定は次のようになります。

<#root>

```
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：

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Cisco ASAセキュリティアプライアンス：

<#root>

```
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
```

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重複」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。

詳細については、『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」の項を参照してください。

ASAで使用されているISAKMPポリシーとIPsecトランスフォームセットに関して、Cisco VPN ClientはDESとSHAの組み合わせを使用できません。

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。

ダイナミック暗号マップエントリのシーケンス番号は、他のすべてのスタティック暗号マップエントリよりも大きくなければなりません 。

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!
```

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。

<#root>

```
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 ciscothe

クリプト マップ名では大文字と小文字が区別されます。

こ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、ピアが誤ったクリプトマップにヒットしたときにも表示されます。

これは、対象トラフィックを定義するクリプトアクセスリストの不一致によっても発生します。

%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、シーケンス番号が異なる同じ名前のクリプトマップを作成します（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ません）。

これは、ルータとASAに当てはまります。

同様に、L2Lとリモートアクセスvpnシナリオの両方のクリプトマップ設定についての詳細は、『ASA：既存のL2L VPNへの新しいトンネルまたはリモートアクセスの追加：Cisco』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

IPsecの接続固有レコードのデータベースを作成および管理します。

ASAセキュリティアプライアンスLAN-to-LAN(L2L)IPSec VPN設定の場合、tunnel-group <name> type ipsec-l2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（リモートトンネルエンド）を指定します。

ピアのIPアドレスはintunnel group およびCrypto map set addresscommandsに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アドレスが正しく設定されていない場合、ログに次のメッセージが含まれている可能性があります。このメッセージは、ピアのIPアドレスを正しく設定することで解決できます。

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

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コマンドの出力を次に示します。

<#root>

```
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

```
%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。

<#root>

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

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

Both lines 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トンネルが同じクリプトマップ上に設定されている場合、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 コマンドの出力に「CONF_XAUTH」と表示されて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。

<#root>

```
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
```

この問題はCisco IOS®にのみ該当しますが、ASAはトンネルグループを使用するため、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-xauthkeywordを使用すると、デバイスからピアに対してXAUTH情報（ユーザ名とパスワード）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。

```
<#root>

router(config)#

crypto isakmp key cisco123 address
   172.22.1.164 no-xauth
```

ASAがEasy VPNサーバとして動作するシナリオでは、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ません。

この問題を解決するには、次に示すようにASAでユーザ認証を無効にします。

```
<#root>

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-authenticationcommandコマンドの詳細については、このドキュメントの「Miscellaneous」の項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。ランダム データの例は次のとおりです。

```
<#root>

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. 不連続サブネットをVPNプールに追加する場合は、2つの個別のVPNプールを定義し、「tunnel-group attributes」の下に順番に指定できます。ランダム データの例は次のとおりです。

```
<#root>
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。

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接続で遅延の問題が発生した場合は、次の条件を確認して問題を解決します。

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を使用する場合は、configurepreserve-vpn-flowを設定します。
3. Cisco ASA をリロードします。

VPN ClientがASAに接続できない

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。

解決方法

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。

例：

<#root>

```
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。

解決方法

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
```

これが正常に動作する場合、問題はRadiusサーバの設定に関連しています。

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。sampledebug radiusoutputについては、次の出力例を参照してください。

ASAでdebugコマンドを使用する前に、警告メッセージのドキュメント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 peerReason 433」または「Secure VPN Connection terminated by Peer Reason 433:(Reason Not Specified by Peer)」

問題

Cisco VPN Clientユーザがヘッドエンドvpnデバイスとの接続を試みると、このエラーが発生します。

VPNクライアントが最初の試行時に頻繁に接続をドロップする

セキュリティVPN接続がピアによって終了されました。Reason 433.

Secure VPN Connection terminated by peer Reason 433:(Reason Not Specified by Peer)(セキュアVPN接続がピア理由433:（理由がピアによって指定されていません））

ネットワークまたはブロードキャストIPアドレスの割り当てを試みましたが、プールから(x.x.x.x)を削除しました。

解決策 1

問題は、ASA、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プールの割り当てである可能性があります。

debug cryptocommandコマンドを使用して、ネットマスクと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ます。AAAサーバをリロードすると、この問題を解決できます。

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。

異なる不完全なSecurity Association（SA；セキュリティアソシエーション）に対して複数の再送信が行われる場合、脅威検出機能が有効になっているASAではスキャン攻撃が発生したと見なされ、VPNポートが主な攻撃者としてマークされます。

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で脅威検出を無効にすると、スキャン試行、無効なSPIを持つDoS、アプリケーションインスペクション(AIP)に失敗したパケット、不完全なセッションなど、いくつかのセキュリティ機能が実際に損なわれるようにしてください。

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。

解決方法

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

- 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 ClientがVPNヘッドエンドデバイス(ASA/Cisco IOS®ルータ)とのIPSecトンネルを確立すると、VPN Clientの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)にはアクセスできません。

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。

以下に例を挙げます。

ASA 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
```

次を確認します：

トンネルが確立されている場合は、Cisco VPNクライアントに移動し、Status > Route Detailsの順に選択して、DMZネットワークとINSIDEネットワークの両方に対してセキュアなルートが表示されていることを確認します。

既存のL2L VPN設定に新しいVPNトンネルまたはリモートアクセスVPNを追加するために必要な手順については、『ASA：既存のL2L VPNへの新しいトンネルまたはリモートアクセスの追加：シスコ』を参照してください。

Cisco 5500シリーズ適応型セキュリティアプライアンス(ASA)にトンネル接続しているVPN Clientにインターネットへのアクセスを許可する方法の手順については、『ASA:ASAでVPN

Client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。

VPN クライアントが DNS を解決できない

トンネルが確立された後、VPN ClientがDNSを解決できない場合は、ヘッドエンドデバイス(ASA)のDNSサーバ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、グループポリシーで設定し、tunnel-groupの一般属性のグループポリシーで適用する必要があります。次に例を示します。

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !---
```

```
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 !--- with 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使用すると、リモートアクセスIPSecクライアントは、条件に応じて、パケットをIPSecトンネル経由で暗号化された形式で、またはネットワークインターフェイスに暗号化されていない平文の形式で送信し、最終的な宛先にルーティングすることができます。

スプリットトンネルはデフォルトで無効になっており、これによりtunnelalltrafficが保護されます。

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

オプション excludespecified 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
```

スプリットトンネルの詳細な設定例については、次のドキュメントを参照してください。

- ASA: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

ヘアピンソリューション

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VPNネットワークでは、セキュリティアプライアンスがハブで、リモートVPNネットワークはスポークです。スポーク間の通信トラフィックは、セキュリティアプライアンスに着信した後、もう一方のスポーク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発着信できるようにするには、同じ – security-traffic設定を使用します。

```
<#root>

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、『ASA: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。

解決方法

VPN Clientに割り当てるプール内のIPアドレス、ヘッドエンドデバイスの内部ネットワーク、およびVPN Clientの内部ネットワークが異なるネットワークにあることを確認します。

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。

さらに詳しい例については、「DMZ内のサーバにアクセスできない」セクションのDiagramandExampleof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

ASA/に接続できるVPNクライアントは3つだけで、4つ目のクライアントへの接続は失敗します。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
```

解決方法

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 の設定
- 構成の構成

同時ログインを設定する

ASDMのInheritcheckボックスがチェックされている場合、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だけです。同時ログインのデフォルト値は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Groupgroupを選択し、Editbuttonをクリックします。

3. Generaltabで、Simultaneous LoginsunderConnection SettingsのInheritcheckボックスを元に戻します。フィールドに適切な値を選択します。

   このフィールドの最小値はゼロ(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。

   別のPCから同じユーザアカウントでログインすると、現在のセッション（同じユーザアカウントを持つ別のPCから確立された接続）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 の設定

同時ログインの希望数を設定するには、次の手順を実行します。この例では、希望値として20が選択されています。

```
<#root>

ciscoasa(config)#

group-policy Bryan attributes

ciscoasa(config-group-policy)#

vpn-simultaneous-logins 20
```

このコマンドの詳細については、『Ciscoセキュリティアプライアンスコマンドリファレンス』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enoversion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。

```
<#root>

hostname#

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

設定

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>
```

解決方法

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 > Simultaneous Loginsの順に選択し、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。

解決方法

ネットワークを確認したり、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たりするには、pingコマンドを使用します。

これは、ルータまたは/ASAデバイスを通過する一時的なパケットの最大セグメントサイズ(MSS)、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：ルータの外部インターフェイス（トンネル終端インターフェイス）のMSS値の変更

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。

<#root>

```
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。

<#root>

```
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、『ASAおよびCisco IOS®:VPNフラグメンテーション』を参照してください。

ASA:/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。

- ASAおよびCisco IOS®:VPNフラグメンテーション

ASAからVPNトンネルを開始できない

問題

ASAインターフェイスからVPNトンネルを開始できず、トンネルが確立された後で、リモートエンド/VPNクライアントがVPNトンネル上のASAの内部インターフェイスにpingを実行できません。

たとえば、VPNクライアントは、VPNトンネル経由でASA内部インターフェイスへのSSHまたはHTTP接続を開始できない場合があります。

解決方法

management-accesscommandがグローバルコンフィギュレーションモードで設定されていない限り、の内部インターフェイスにトンネルの反対側からpingを送ることはできません。

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

このコマンドは、VPNトンネルを介したASAのInsideインターフェイスへのSSHの開始またはHTTP接続にも役立ちます。

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、/ASAのDMZインターフェイスにpingを実行する場合、またはDMZインターフェイスからトンネルを開始する場合は、management-access DMZコマンドが必要です。

```
<#root>

ASA-02(config)#

management-access DMZ
```

VPNクライアントが接続できない場合は、ESPおよびUDPポートが開いていることを確認します。

ただし、これらのポートが開いていない場合は、VPNクライアント接続エントリでこのポートを選択して、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。

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。

解決方法

この問題は、ESPパケットがブロックされている場合にも発生する可能性があります。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、次の出力に示すように、データが暗号化されていないが、VPNトンネル経由でのみ復号化されている場合に発生する可能性があります。

<#root>

```
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、次の条件を確認します。

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く、トラフィックが内部を通過する外部インターフェイスに到達した場合。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. ASAでsimple permit connection-vpnコマンドが設定されているかどうか。設定されていない場合は、このコマンドを設定します。これは、ASAがインターフェイスACLチェックから暗号化/VPNトラフィックを除外することを許可するためです。

同じクリプトマップでvpnトンネルのバックアップピアを設定する

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。

解決方法

複数のピアの設定は、フォールバックリストのプロビジョニングと同じです。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には、プライマリピアとして設定されているクリプトマップがあります。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。

<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y

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。

解決方法

グローバルコンフィギュレーションモードでcrypto map interfaceコマンドを使用して、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。

インターフェイスからクリプトマップセットを削除するには、このコマンドのenoformを使用します。

<#root>

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。

<#root>

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。

解決方法

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。

エラー：「%ASA-5-713904: Group = DefaultRAGroup, IP = x.x.x.x, ... unsupported Transaction Mode v2 version.Tunnel terminated.」

問題

%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... unsupported Transaction Mode v2 version.Tunnel terminatederrorメッセージが表示されます。

解決方法

Transaction Mode v2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、古い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)エラーメッセージがASAのログに表示されます。

この口グの意味と解決方法を教えてください。

解決方法

この口グ 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。回避策は、svc compressionコマンドを使用してSVC圧縮をオフにすることです。これにより、問題が解決します。

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をイネーブルにすると、次のエラーメッセージが表示される場合があります。

```
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 check
```

解決方法

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。これは、パケットが故障していると検出された場合に発生します。

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。

警告：クリプトマップエントリが不完全です

問題

クリプトマップmymap 20 ipsec-isakmpcommandを実行すると、次のエラーを受け取る場合があ

ります。

警告：クリプトマップエントリが不完全です

例：

<#root>

ciscoasa(config)#

crypto map mymap 20 ipsec-isakmp

WARNING: crypto map entry incomplete

解決方法

これは、新しいクリプトマップを定義する際の通常のアラートです。アクセスリスト(match address)、トランスフォームセット、ピアアドレスなどのパラメータは、機能する前に設定する必要があることを思い出してください。

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、エラー**%ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside**が表示されます。

解決方法

この問題を解決するには、シグニチャ2150および2151を無効にします。シグニチャを無効にすると、pingは正常に動作します。

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：「%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 check.」

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。

エラー：- %|ASA-4-402119:IPSEC：リモートアドレスの**remote_IP**（ユーザ名）からローカルアドレスの**local_IP**へのプロトコル パケット**(SPI=spi, sequence number= seq_num)**を受信しましたが、アンチリプレイチェックに失敗しました。

解決方法

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

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

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。

エラーメッセージ – %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。

エラーメッセージ – %**ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded**

解決方法

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、ライセンスをより多くのユーザ数にアップグレードすることで解決できます。

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

エラーメッセージ – %VPN_HW-4-PACKET_ERROR:エラーメッセージは、ルータが受信したHMACを持つESPパケットが一致していないことを示しています。このエラーは、次の問題が原因で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

解決方法

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 SPAtrunkにVLANを追加できません。

このコマンドは、許可されたVLANリストに属するインターフェイスVLANに暗号化が接続され、IPSecセキュリティ違反が発生する可能性があるため、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。

解決方法

switchport trunk allowed vlan (vlanlist)コマンドの代わりに、switchport trunk allowed vlan nonecommandまたは"switchport trunk allowed vlan remove (vlanlist)"コマンドを使用します。

エラーメッセージ – % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to 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。

エラーメッセージ – % **FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]**

解決方法

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。ウィンドウスケール機能が追加され、ロングファットネットワーク(LFN)でのデータの高速伝送が可能になりました。

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。

ウィンドウスケール機能でLFNをサポートするには、TCPウィンドウサイズが65,535を超える必要があります。このエラーメッセージは、TCPウィンドウサイズを65,535より大きくすると解決できます。

%ASA-5-305013：非対称NATルールが順方向と逆方向で一致しました（ASAのデフォルトはASAのデフォルトです）。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：非対称NATルールが順方向と逆方向で一致しました（ASAのデフォルトはASAのデフォルトです）。Please update this issue flows

解決方法

NATを使用するホストと同じインターフェイス上にない場合にこの問題を解決するには、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てホストに接続します。

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コマンドを有効にします。

%ASA-5-713068：非ルーチンNotifyメッセージを受信しました：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。

%ASA-5-713068：非ルーチンNotifyメッセージを受信しました： notify_type

解決方法

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)スタンバイユニットでIPSecフェールオーバーランタイムデータを更新できませんでした（または）%ASA-6-720012:(VPN-unit)スタンバイユニットでIPSecフェールオーバーランタイムデータを更新できませんでした

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)スタンバイユニットでIPSecフェールオーバーランタイムデータを更新できませんでした。

%ASA-6-720012:(VPN-unit)スタンバイユニットでIPsecフェールオーバーランタイムデータを更新できませんでした。

解決方法

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。

これらのメッセージは、関連するIPsecトンネルがスタンバイユニットで削除されているために、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更新できない場合に表示されます。

これを解決するには、アクティブユニットでwr standbycommandコマンドを発行します。

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

問題

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

解決方法

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を変更してから、クリプトマップを削除して再適用すると解決できます。

エラー： %ASA-3-752006：トンネルマネージャがKEY_ACQUIREメッセージのディスパッチに失敗しました。

問題

%ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Probably-configuration of the crypto map or tunnel-group."エラーメッセージがCisco ASAでログに記録されます。

解決方法

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」（登録ユーザ専用）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: XX.XX.XX.XX (user= XX.XX.XX.XX)からYY.YY.YY.YYにESPパケット(SPI= 0x99554D4E、シーケンス番号= 0x9E)を受信しました

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。

カプセル化解除された内部パケットが、SAのネゴシエートされたポリシーと一致しません。

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.

解決方法

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。両方とも正確なミラーイメージとして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 0xffffffflog」というメッセージが表示されます。

解決方法

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の順に進み、Turn Off Automatic Root Certificates Updatesがディセーブルになっていることを確認します。
2. 無効になっている場合は、影響を受けるマシンに割り当てられているGPOのentireAdministrativeテンプレート部分を無効にして、もう一度テストします。

詳細については、「自動ルート証明書の更新をオフにする」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。

解決方法

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。

アラート：「VPN機能がまったく動作しない可能性がある」

問題

ASAの外部インターフェイスでisakmpを有効にしようとすると、次のアラートメッセージが表示

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。

解決方法

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コマンドがないことを確認します。これにより、キューサイズが8192に設定され、メモリ割り当てが増加します。

ASA5505や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のメモリが不足する傾向があります。

IPSec Padding エラー

問題

次のエラー メッセージが表示されます。

```
%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
```

解決方法

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チャネルの整合性チェックが保証されます。

そのため、ハッシュがないと、不正なパケットはCisco ASAによって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みられます。

ただし、これらのパケットは不正な形式であるため、ASAはパケットの復号化中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。

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。

解決方法

ライフタイムは、SAがキー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、時間はプラットフォーム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の75 %でキー再生成することは正常です。

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。

解決方法

ASAは、ASAを通過するすべての接続を監視し、アプリケーションインスペクション機能に従って状態テーブルの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、ASAはその特定のフローのTCP接続を保持します。

ただし、TCPアイドルタイマーが時間切れになると、TCP接続が不安定になり、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されています。

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。これを可能にするために、L2L VPNが中断から回復し、トンネルが再確立されるときに、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。

エラー： 3月20日10:51:29: %**CERM-4-TX_BW_LIMIT: securityk9**テクノロジーパッケージライセンスの暗号化機能の**Tx**帯域幅の上限である**85000 Kbps**に達しました。

解決方法

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。

これに従って、securityk9ライセンスでは、90 Mbpsに近いレートまでのペイロード暗号化を許可し、デバイスへの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しかできません。

暗号化のエクスポート制限の詳細については、『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。このコマンドは、次の制限を表示するのに役立ちます。

<#root>

```
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----
```

この問題を回避するには、HSECK9ライセンスを購入します。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については、『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：着信の復号化トラフィックが機能していても、IPSecトンネルの発信暗号化トラフィックは失敗する。

解決方法

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 dropcommandの出力をチェックして、送信される発信パケットごとにExpired VPN contextカウンタが増加することを確認することで確認できます。

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

トンネルが開始されない場合は、**show crypto isakmp** コマンドおよびindebugoutputの出力にもAG_INIT_EXCHmessageが表示されます。

原因としては、isakmpポリシーの不一致や、ポートudp 500が途中でブロックされたことが考えられます。

「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

- ASAおよびCisco 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
- IPSec ネゴシエーション/IKE プロトコル
- 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。