一般的なDMVPN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、ダイナミックマルチポイントVPN(DMVPN)の問題に対する最も一般的なソリューションについて説明します。

前提条件

要件

Cisco IOS® ルータの DMVPN 設定に関する知識があることが推奨されます。

使用するコンポーネント

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

- Cisco IOS

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

表記法

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

背景説明

このドキュメントでは、ダイナミックマルチポイントVPN(DMVPN)の問題に対する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の多くは、DMVPN接続の詳細なトラブルシューティングの前に実装できます。このドキュメントは、接続のトラブルシューティングやシスコ テクニカル サポートへの電話を始める前に試すべき一般的な手順のチェックリストとして提供されています。

詳細については、『ダイナミックマルチポイントVPNコンフィギュレーションガイド、Cisco IOSリリース15M&T』を参照してください。

IPSecの問題のトラブルシューティングに使用される一般的なdebugコマンドの詳細は、『debugコマンドを使用したIPSecのトラブルシューティング』を参照してください。

DMVPN 設定が機能しない

問題

最近設定した、または設定を変更した DMVPN ソリューションが機能しません。

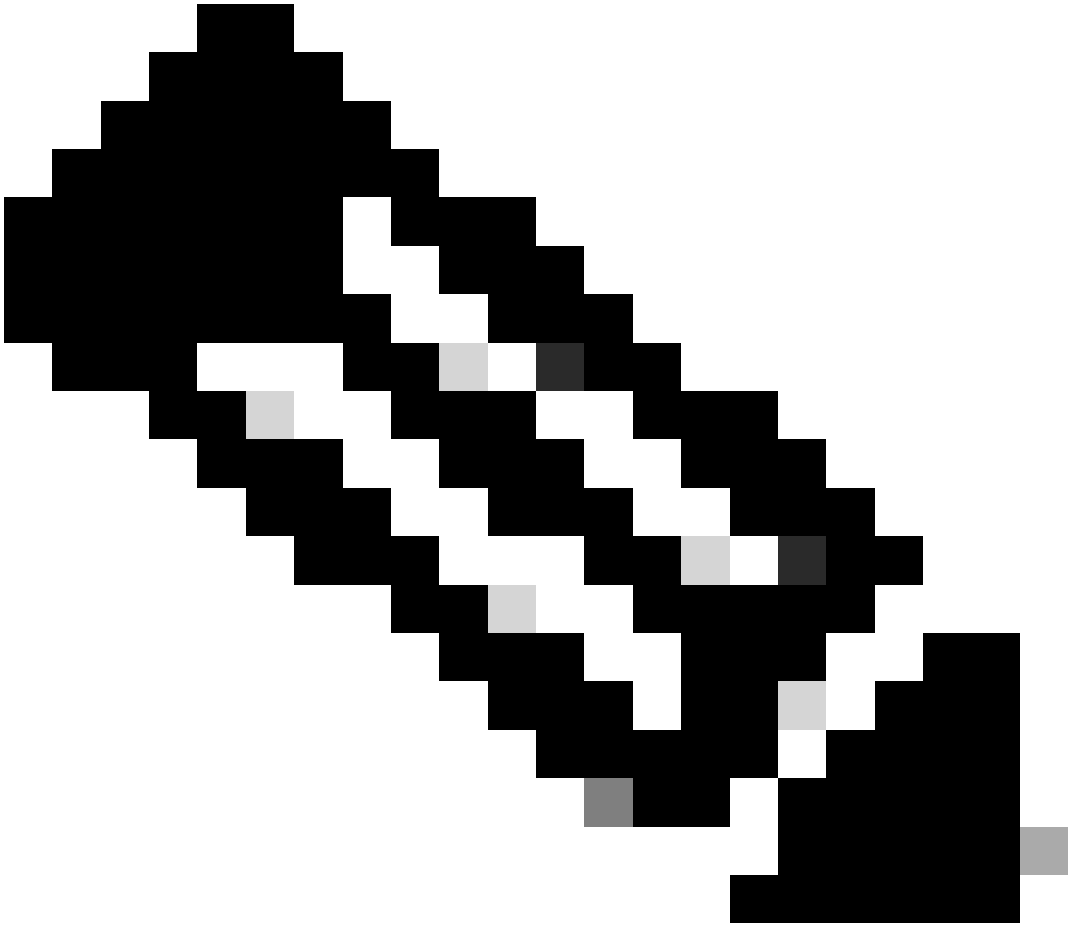
現在の DMVPN の設定が機能しなくなりました。

解決方法

この項では、DMVPN に関する最も一般的な問題のソリューションについて説明します。

次のソリューションは、詳細なトラブルシューティング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（順序は特にありません）。

- 一般的な問題
- インターネットサービスプロバイダー(ISP)でInternet Security Association and Key Management Protocol(ISAKMP)パケットがブロックされているかどうかを確認します。
- トンネル保護が解除されたときに総称ルーティングカプセル化(GRE)が機能するかどうかを確認します。
- Next-Hop Resolution Protocol(NHRP)の登録が失敗する。
- ライフタイムが正しく設定されているかどうかを確認します。
- トラフィックが一方向だけに流れているかどうか確認する.
- ルーティングプロトコルネイバーが確立されていることを確認します。



注：作業を開始する前に、次の手順を確認してください。

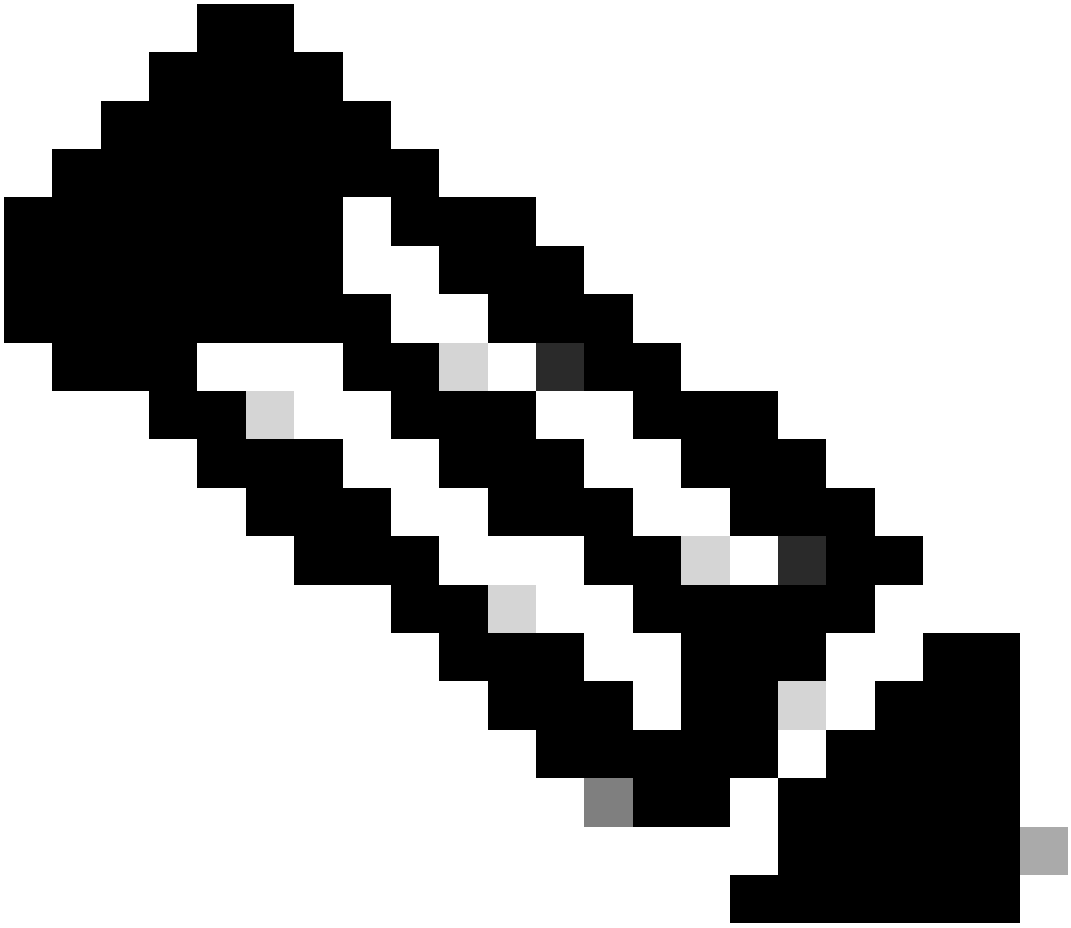
1. ハブとスポークの間でタイムスタンプが同期していること
2. 次のデバッグとログのミリ秒単位のタイムスタンプが有効になっていること

```
Router(config)#service timestamps debug datetime msec

Router(config)#service timestamps log datetime msec
```

3. デバッグ セッションのため、次の terminal exec prompt timestamp が有効になっていること

```
Router#terminal exec prompt timestamp
```



注：この方法により、debugの出力をshowコマンドの出力と関連付けることが簡単にできるようになります。

一般的な問題

基本的な接続の確認

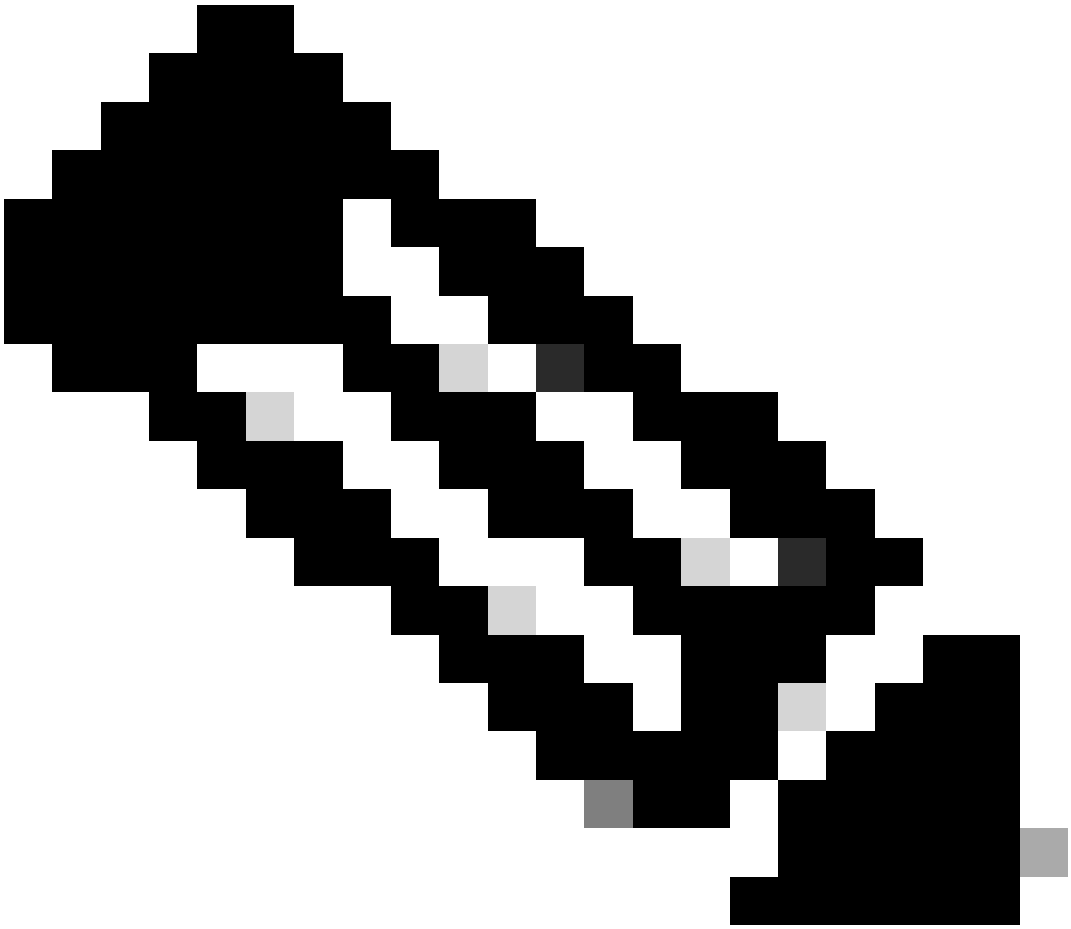
1. ハブからスポークに、NBMAアドレスを使用してpingを実行し、その逆を実行します。

   これらのpingは、DMVPNトンネル経由ではなく、物理インターフェイスから直接送信される必要があります。ping パケットをブロックするファイアウォールがないのが望ましい状態です。ping が機能しない場合は、ルーティングを確認し、ハブ ルータとスポーク ルータの間にファイアウォールがないか確認します。

2. また、tracerouteを使用して、暗号化されたトンネルパケットがとおるパスも確認します。

3. 次の debug コマンドと show コマンドを使用して、接続がないことを確認します。

- debug ip icmp
- debug ip packet



注：debug ip packetコマンドを使用すると、かなりの量の出力が生成され、相当量のシステムリソースが使用されます。このコマンドは、実稼働ネットワークでは注意して使用する必要があります。必ず access-list コマンドとともに使用してください。 access-listとdebug ip packetの使用方法については、『IPアクセスリストの設定』の「トラブルシューティング」を参照してください。

一致しない ISAKMP ポリシーがないか確認する

設定された ISAKMP ポリシーが、リモート ピアによって提示されたポリシーと一致しない場合、ルータは 65535 デフォルト ポリシーを試行します。それも一致しない場合は、ISAKMP ネゴシエーションが失敗します。

show crypto isakmp saコマンドは、ISAKMP SAがMM_NO_STATEにあることを示します。これ

は、メインモードの失敗を意味します。

事前共有キーが不適切でないか確認する

事前共有秘密が両側で同じでない場合、ネゴシエーションは失敗します。

ルータによって「sanity check failed」というメッセージが返されます。

IPSec トランスフォーム セットの不一致がないか確認する

2つのIPsecデバイスでIPsecトランスフォームセットに互換性がないか、または一致しない場合、IPsecネゴシエーションは失敗します。

ルータによって、IPSecプロポーザルに対する「atts not acceptable」のメッセージが返されます。

ISAKMP パケットが ISP でブロックされていないか確認する

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
Dst                 src                   state       conn-id      slot       status
172.17.0.1      172.16.1.1        MM_NO_STATE         0               0       ACTIVE
172.17.0.1      172.16.1.1        MM_NO_STATE         0               0       ACTIVE (deleted)
172.17.0.5        172.16.1.1        MM_NO_STATE      0              0       ACTIVE
172.17.0.5        172.16.1.1        MM_NO_STATE      0              0       ACTIVE (deleted)
```

前の例は、VPNトンネルフラッピングを示しています。

さらに、debug crypto isakmp をチェックして、スポークルータがudp 500パケットを送信することを確認します。

<#root>

```
Router#
```

debug crypto isakmp

<#root>

```
04:14:44.450: ISAKMP:(0):Old State = IKE_READY
                        New State = IKE_I_MM1
```

04:14:44.450: ISAKMP:(0): beginning Main Mode exchange

```
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
```

04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE..

```
.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

上記のdebug の出力は、スポークルータがUDP 500パケットを10秒ごとに送信することを示しています。

スポークルータがISPルータに直接接続されているかどうかをISPに確認し、UDP 500トラフィックを許可していることを確認します。

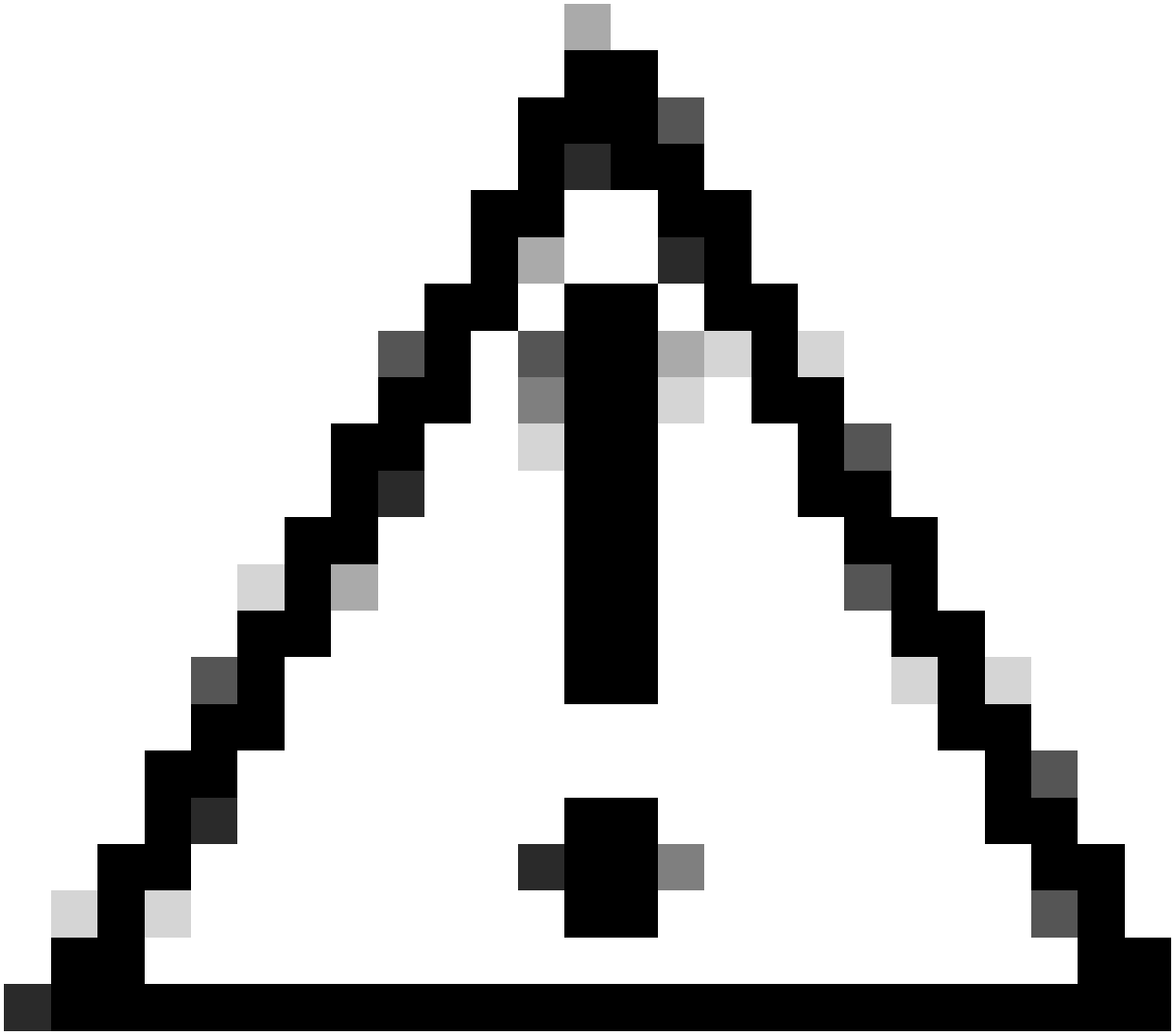
ISPがUDP 500を許可した後、出力インターフェイスに着信ACLを追加します。これは、UDP 500トラフィックがルータに着信することを確認するためにUDP 500を許可するトンネル送信元です。show access-listコマンドを使用して、ヒットカウントが加算されているかどうかを確認します。

```
    <#root>

Router#


show access-lists 101


Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
    30 permit ip any any (295 matches)
```



注意：使用しているアクセスリストでip any anyが許可されていることを確認してください。許可されていないと、出力インターフェイスの着信にaccess-listが適用されるため、その他のすべてのトラフィックがブロックされる可能性があります。

トンネル保護を解除した場合にGREが機能するかどうかの確認

DMVPNが機能しない場合は、IPSecに関するトラブルシューティングを行う前に、GREトンネルがIPSec暗号化を使用せずに正常に機能することを確認します。

詳細は、『GREトンネルの設定方法』を参照してください。

NHRP登録が失敗する

ハブとスポークの間の VPN トンネルはアップ状態にありますが、データ トラフィックを渡すことができません。

<#root>

Router#

show crypto isakmp sa

dst	src	state	conn-id	slot	status
172.17.0.1	172.16.1.1	QM_IDLE	1082	0	ACTIVE

<#root>

Router#

show crypto IPSEC sa

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)

#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0

```
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)

!--- !--- Output is truncated !---
```

これは、リターントラフィックがトンネルの反対側から戻ってこないことを示しています。

スポーク ルータの NHS エントリを確認します。

<#root>

```
Router#
```

show ip nhrp nhs detail

```
Legend: E=Expecting replies, R=Responding
Tunnel0: 172.17.0.1  E  req-sent 0
```

req-failed 30

```
 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

これは、NHS要求が失敗したことを示しています。この問題を解決するには、スポーク ルータのトンネル インターフェイスを正しく設定します。

設定例：

```
    <#root>


interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1




ip nhrp nhs 172.17.0.1




!--- !--- Output is truncated !---
```

NHS サーバに関するエントリが正しい設定例：

```
    <#root>


interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1




ip nhrp nhs 10.0.0.1




!--- !--- Output is truncated !---
```

ここで、NHS エントリと、IPSec 暗号化および復号化のカウンタを確認します。

<#root>

Router#

show ip nhrp nhs detail

Legend: E=Expecting replies, R=Responding
Tunnel0:   10.0.0.1 RE req-sent 4

req-failed 0

repl-recv 3 (00:01:04 ago)

Router#

show crypto IPSec sa

local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)

#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

inbound esp sas:
spi: 0x1B7670FC(460747004)
outbound esp sas:
spi: 0x3B31AA86(993110662)

!--- !--- Output is truncated !---

ライフタイムが適切に設定されているか確認する

次のコマンドを使用して、現在の SA ライフタイムと、次回の再ネゴシエーションまでの時間を確認します。

- **show crypto isakmp sa detail**
- **show crypto ipsec sa peer <NBMA-address-peer>**

SA ライフタイムの値に注目します。この値が、設定されているライフタイム (デフォルトは、ISAKMP は 24 時間、IPSec は 1 時間) に近い場合、その SA は最近ネゴシエートされたということです。しばらくしてから見て、再びネゴシエートされた場合は、ISAKMPやIPSecがアップとダウンに頻繁に切り替わる可能性があります。

<#root>

```
Router#
```

show crypto ipsec security-assoc lifetime

Security association lifetime: 4608000 kilobytes/3600 seconds

```
Router#
```

show crypto isakmp policy

```
Global IKE policy
Protection suite of priority 1
Encryption algorithm: DES-Data Encryption Standard (65 bit keys)
Hash algorithm: Message Digest 5
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
```

Lifetime: 86400 seconds, no volume limit

```
Default protection suite
 Encryption algorithm: DES- Data Encryption Standard (56 bit keys)
 Hash algorithm: Secure Hash Standard
 Authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 Lifetime: 86400 seconds, no volume limit

Router#
```

show crypto ipsec sa

```
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer: 172.17.0.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
     path mtu 1500, media mtu 1500
     current outbound spi: 8E1CB77A

 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
```

sa timing: remaining key lifetime (k/sec): (4456885/3531)

```
        IV size: 8 bytes
        replay detection support: Y
```

トラフィックが一方向だけに流れていないか確認する

スポークルータ間のVPNトンネルはアップ状態にありますが、データトラフィックを渡すことができません。

```
    <#root>

Spoke1#
```

show crypto ipsec sa peer 172.16.2.11

```
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
```

```
#pkts encaps: 110, #pkts encrypt: 110
    #pkts decaps: 0, #pkts decrypt: 0,



local crypto endpt.: 172.16.1.1,
remote crypto endpt.: 172.16.2.11
      inbound esp sas:
      spi: 0x4C36F4AF(1278669999)
      outbound esp sas:
      spi: 0x6AC801F4(1791492596)

!--- !--- Output is truncated !---


Spoke2#



sh crypto ipsec sa peer 172.16.1.1



   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)



 #pkts encaps: 116, #pkts encrypt: 116,
   #pkts decaps: 110, #pkts decrypt: 110,



local crypto endpt.: 172.16.2.11,
remote crypto endpt.: 172.16.1.1
     inbound esp sas:
     spi: 0x6AC801F4(1791492596)
     outbound esp sas:
     spi: 0x4C36F4AF(1278669999

!--- !--- Output is truncated !---
```

スポーク１には、カプセル化が解除されたパケットがありません。これは、ESP パケットが スポーク２からスポーク１に向かって戻るパスのどこかでドロップされたことを意味します。

spoke2ルータはカプセル化とカプセル化解除の両方を示します。つまり、ESPトラフィックはspoke2に到達する前にフィルタリングされます。この問題は、spoke2のISP側、またはspoke2ルータとspoke1ルータ間のパスにあるファイアウォールで発生する可能性

があります。ESP（IPプロトコル50）を許可すると、spoke1とspoke2の両方でencapとdecapsのカウンタが増加します。

```
   <#root>

spoke1#


show crypto ipsec sa peer 172.16.2.11


   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)


 #pkts encaps: 300, #pkts encrypt: 300
    #pkts decaps: 200, #pkts decrypt: 200


!--- !--- Output is truncated !---

spoke2#


sh crypto ipsec sa peer 172.16.1.1


   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)


#pkts encaps: 316, #pkts encrypt: 316,
   #pkts decaps: 300, #pkts decrypt: 310


!--- !--- Output is truncated !---
```

ルーティングプロトコルネイバーが確立されていることの確認

スポークがルーティング プロトコルのネイバー関係を確立できません。

<#root>

Hub#

show ip eigrp neighbors

```
H   Address     Interface   Hold Uptime     SRTT    RTO       Q      Seq
                              (sec)             (ms)  Cnt     Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000       1      0
0   10.0.0.5     Tu0         11     00:00:47   1587   5000       0     1483
1   10.0.0.11    Tu0         13     00:00:56     1    5000       1      0
```

Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub#

show ip route eigrp

```
    172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

ハブで NHRP マルチキャスト マッピングが正しく設定されているか確認します。

ハブでは、ダイナミック NHRP マルチキャスト マッピングがハブ トンネル インターフェイスで設定されている必要があります。

設定例：

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

ダイナミック NHRP マルチキャスト マッピングのエントリが正しい設定例：

<#root>

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
```

ip nhrp map multicast dynamic

```
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

これにより、NHRP において、スポーク ルータが自動的にマルチキャスト NHRP マッピングに追加されるようになります。

詳細については、『Cisco IOS IPアドレッシングサービスコマンドリファレンス』のip nhrp map multicast dynamic コマンドを参照してください。

<#root>

```
Hub#
```

show ip eigrp neighbors

```
IP-EIGRP neighbors for process 10
H   Address     Interface   Hold   Uptime   SRTT    RTO     Q     Seq
                                           (sec)    (ms)   Cnt    Num
2   10.0.0.9     Tu0         12   00:16:48   13     200     0     334
1   10.0.0.11    Tu0         13   00:17:10   11     200     0     258
0   10.0.0.5     Tu0         12   00:48:44  1017    5000    0     1495

Hub#
```

show ip route

```
     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
```

D   192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0

```
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, Tunnel0
C    192.168.0.0/24 is directly connected, FastEthernet0/1
```

```
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
```

```
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

スポークへのルートは、EIGRP プロトコルを介して学習されます。

DMVPN統合によるリモートアクセスVPNに関する問題

問題

DMVPNは正常に動作していますが、RAVPNを確立できません。

解決方法

確立するためには、ISAKMP プロファイルおよび IPSec プロファイルを使用します。 DMVPN と RAVPN に別々のプロファイルを作成します。

詳細については、『ISAKMP プロファイルを使用した DMVPN および Easy VPN サーバの設定例』を参照してください

デュアルハブデュアルDMVPNに関する問題

問題

デュアル ハブ デュアル DMVPN に関する問題具体的には、トンネルはダウンし、再ネゴシエートできません。

解決方法

トンネルIPsec保護で、ハブ上とスポーク上の両方のトンネルインターフェイスにsharedキーワードを使用します。

設定例：

```
interface Tunnel43
 description <<tunnel to primary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---

interface Tunnel44
 description <<tunnel to secondary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---
```

詳細については、『Cisco IOSセキュリティコマンドリファレンス(A-C)』の**tunnel protection** コマンドを参照してください。

DMVPNを介したサーバへのログインに関する問題

問題

DMVPNネットワークサーバ経由の問題トラフィックにアクセスできない。

解決方法

この問題は、GREとIPsecを使用するパケットのMTUとMSSサイズに関連している可能性があります。

ここでは、フラグメンテーションに伴うパケット サイズの問題であるとします。この問題を解消するには、次のコマンドを使用します。

<#root>

```
ip mtu 1400
ip tcp adjust-mss 1360
crypto IPSec fragmentation after-encryption (global)
```

また、MTUサイズを動的に検出するように**tunnel path-mtu-discovery**コマンドを設定することもできます。

詳細については、『GREおよびIPSECによるIPフラグメンテーション、MTU、MSS、およびPMTUDの問題の解決』を参照してください。

特定のポートが DMVPN 上のサーバへのアクセスに使用できない

問題

特定のポートが DMVPN 上のサーバへのアクセスに使用できません。

解決方法

Cisco IOSファイアウォール機能セットを無効にして、機能するかどうかを確認します。

正常に機能する場合、問題はDMVPNではなく、Cisco IOSファイアウォールの設定に関連しています。

関連情報

- **Dynamic Multipoint VPN（DMVPN）**
- **IPSec ネゴシエーション/IKE プロトコル**
- シスコのテクニカルサポートとダウンロード

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。