排除故障解决方案的最普通的DMVPN

目录

简介
先决条件
要求
使用的组件
规则
DMVPN配置不工作
问题
解决方案
常见问题
如果ISAKMP信息包阻塞在ISP，请验证
请验证，如果GRE通过删除通道保护工作
NHRP注册失败
验证寿命是否适当地配置
是否只验证在一个方向的通信流
验证路由协议邻接建立
关于集成远程访问VPN的问题与DMVPN
问题
解决方案
与DUAL HUB DUAL DMVPN的问题。
问题
解决方案
登录服务器的麻烦通过DMVPN
问题
解决方案
无法通过特定端口访问在DMVPN的服务器
问题
解决方案
相关信息

简介

本文包含多数同一解决方案对动态多点VPN (DMVPN)问题。许多这些解决方案可以在DMVPN连接的详细故障排除之前实现。在您开始排除故障连接和呼叫思科技术支持前，提交本文，当普通的步骤清单尝试。

如果需要DMVPN的配置示例文档，参考DMVPN配置示例和TechNotes。

注意： 参考的IPSec排除故障-了解和使用调试指令提供使用排除故障IPsec问题普通的调试指令的

说明。

先决条件

要求

思科建议您有DMVPN配置知识在Cisco IOS路由器的。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

DMVPN配置不工作

问题

一最近已配置的或已修改DMVPN解决方案不工作。

不再一当前DMVPN配置工作。

解决方案

此部分包含解决方案对最普通的DMVPN问题。

这些解决方案(在没有特定顺序)可以用于作为项目验证或尝试清单，在您参与详细故障排除前：

- 常见问题
- 如果ISAKMP信息包阻塞在ISP，请验证
- 请验证，如果GRE通过删除通道保护优良工作
- NHRP注册失败
- 验证寿命是否适当地配置
- 是否只验证在一个方向的通信流
- 验证路由协议邻接建立

注意： 在您开始前，请检查这些：

1. 同步在星型网之间的时间戳
2. Enable (event)**毫秒调试和日志时间戳**：`Router(config)#serviceRouter(config)#service`
3. 调试会话的Enable (event)**终端的EXEC提示时间戳**：`Router#terminal EXEC`

注意： 这样，您能容易地关联**debug输出**与**show命令输出**。

常见问题

验证基本连通性

1. 从集线器ping到spoke的使用NBMA地址并且倒转。这些ping应该直接地通过物理接口，不DMVPN通道。有希望地，没有阻塞ping信息包的防火墙。如果这不工作，请检查路由和所有防火墙在星型网路由器之间。
2. 并且，检查加密隧道数据包采取的路径的使用traceroute。
3. 请勿请使用**Debug与Show**调试指令验证连接：**debug ip icmpdebug ip packet注意： debug ip packet命令**生成大量的输出并且使用大量的系统资源。此should命令在生产网络小心地使用。请用**访问列表命令**总是请使用。**注意：** 关于如何以**调试ip数据包**使用的更多信息**access-list**，参考排除故障与IP访问列表。

为不兼容ISAKMP策略验证

如果配置的 ISAKMP 策略与远程对等体提议的策略不匹配，则路由器会尝试使用默认策略 65535。如果那不配比，发生故障ISAKMP协商。

show crypto isakmp sa命令显示ISAKMP SA在**MM_NO_STATE**，含义失败的主模式。

为不正确预先共享密钥机密验证

如果预共享秘密不是相同的在两边，协商将发生故障。

路由器返回**“健全性检查失败的”**消息。

为不兼容IPsec转换集验证

如果Ipsec transform-set不是兼容或不匹配的在两个IPSec设备， IPsec协商将发生故障。

路由器返回IPsec建议的**“atts不可接受”**消息。

如果ISAKMP信息包阻塞在ISP，请验证

```
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)
```

以上显示VPN通道飘荡。

进一步，验证检查的**debug crypto isakmp**分支路由器发送udp 500数据包：

```
Router#debug crypto isakmp
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
```

上述**debug输出**在每10秒显示分支路由器发送udp 500数据包。

检查与ISP发现分支路由器是否直接地连接到ISP路由器确保他们允许udp 500流量。

在ISP允许的udp 500以后，请添加在出口接口的入站ACL，是允许udp的隧道源500确保udp 500流量进入路由器。请使用show access-list命令验证命中数计数是否增加：

```
Router#show access-lists 101
Router#show access-lists 101
```

警告： 确保您有**ip所有其中任一**允许在您access-list。否则，其他流量将阻塞作为一**access-list**已应用入站在出口接口。

请验证，如果GRE通过删除通道保护工作

当DMVPN不在排除故障工作时，与IPsec前，请验证GRE隧道优良工作，不用IPSec加密。

欲知更多信息，参考配置GRE隧道。

NHRP注册失败

在星型网之间的VPN通道是UP，但是无法通过数据流：

```
Router#show crypto isakmp sa
        dst             src             state          conn-id  slot   status
        172.17.0.1      172.16.1.1      QM_IDLE           1082    0    ACTIVERouter#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 !---
```

它显示回程数据流不从通道的另一端回来。

检查在分支路由器的NHS条目：

```
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
```

它显示NHS请求失败。要解决此问题，请确保在隧道接口正确的分支路由器的配置。

配置示例：

```
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 !---
```

与正确条目的配置示例NHS服务器的：

```
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 !---
```

现在，请验证NHS条目，并且IPsec加密/解密计数器：

```
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 !---
```

验证寿命是否适当地配置

请使用这些命令验证SA当前寿命和时期的下重新协商：

- **show crypto isakmp sa详细信息**
- **show crypto ipsec sa对等体***<NBMA-address-peer>*

SA公告寿命值。如果他们是接近已配置的寿命(默认是ISAKMP的24小时和IPsec的1个小时)，则该含义这些SAS最近协商。如果过了一会儿查找，并且他们再重新了协商，则ISAKMP和IPsec可能上下反弹。

```
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
```

是否只验证在一个方向的通信流

在spoke-to-spoke路由器之间的VPN通道是UP，但是无法通过数据流：

```
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 !---
```

没有在分支1的decap数据包，含义特别是数据包在路径返回丢弃某处从往分支1的分支2。

分支2路由器显示encap和decap，因此意味着ESP流量在到达的分支2前被过滤。它可能发生在ISP末端在分支2或在所有防火墙在分支2路由器和分支1路由器之间的路径。在允许ESP以后(IP协议50)，分支1和分支2两个显示encaps，并且decap计数器增加。

```
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 !---
```

验证路由协议邻接建立

Spoke无法建立路由协议邻接关系：

```
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
```

如果NHRP组播映射在集线器，适当地配置请验证。

在集线器中，它要求有在集线器隧道接口配置的动态NHRP组播映射。

配置示例：

```
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
```

与正确条目的配置示例动态NHRP组播映射的：

```
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 !---
```

这允许NHRP自动地添加分支路由器到组播NHRP映射。

欲知更多信息，参考NHRP命令的**ip nhrp map multicast动态**部分。

```
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
```

了解对spoke的路由通过eigrp协议。

关于集成远程访问VPN的问题与DMVPN

问题

DMVPN优良工作，但是无法设立RAVPN。

解决方案

请使用ISAKMP配置文件和IPSec简档达到此。

创建DMVPN和RAVPN的独立的配置文件。

欲知更多信息，参考DMVPN和Easy VPN Server与ISAKMP配置文件配置示例。

与DUAL HUB DUAL DMVPN的问题。

问题

与DUAL HUB DUAL DMVPN的问题。特别地，通道断开和无法重新协商。

解决方案

也请使用共享关键字在通道IPSec保护两个隧道接口在集线器和在分支。

配置示例：

```
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
```

欲知更多信息，参考在Cisco IOS安全命令参考的**通道保护**部分。

登录服务器的麻烦通过DMVPN

问题

关于访问一个服务器的问题通过DMVPN网络。

解决方案

问题可能与使用GRE和IPsec数据包的MTU和MSS大小涉及。

现在，数据包大小能是与分段的一个问题。要消除此问题，请使用这些命令：

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

您可能也配置**tunnel path-mtu-discovery命令**动态地发现MTU大小。

对于更多详细说明，参考解决IP分段， MTU、MSS和PMTUD问题与GRE和IPSEC。

无法通过特定端口访问在DMVPN的服务器

问题

无法对在DMVPN的接入服务器通过特定端口。

解决方案

验证由禁用IOS防火墙特性组并且看到是否工作。

如果它良好工作，则问题涉及与IOS防火墙设置，不与DMVPN。

相关信息

- 动态多点 VPN (DMVPN)
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems