IPSec故障排除：了解和使用调试指令

目录

简介

本文描述用于的普通的调试指令排除故障在两Cisco IOS的IPsec问题？软件和PIX/ASA。本文档假定您已配置了 IPsec。有关详细信息，请参阅常见 IPsec 错误消息和常见 IPsec 问题。

有关 IPsec VPN 问题最常用解决方案的信息，请参阅最常见的 L2L 和远程接入 IPsec VPN 故障排除解决方案。其中包含在您开始排除连接故障之前以及致电 Cisco 技术支持之前可以尝试的常见过程清单。

先决条件

要求

本文档没有任何特定的要求。

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 软件IPsec 功能集。56i - 表示一重数据加密标准 (DES) 功能（适用于 Cisco IOS 软件版本 11.2 及更高版本）。k2 - 表示三重 DES 功能（适用于 Cisco IOS 软件版本 12.0 及更高版本）。Cisco 2600 系列及后来的产品均提供了三重 DES 功能。
- **PIX** —V5.0和以后，要求单个或三重DES许可证密钥为了激活。

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。

Cisco IOS 软件 debug

本部分中的主题介绍 Cisco IOS 软件的 debug 命令。有关详细信息，请参阅常见 IPsec 错误消息和常见 IPsec 问题。

show crypto isakmp sa

此命令用于显示对等体之间构建的 Internet 安全连接和密钥管理协议 (ISAKMP) 安全关联 (SA)。

```
dst      src        state     conn-id     slot
12.1.1.2  12.1.1.1   QM_IDLE    1           0
```

show crypto ipsec sa

此命令用于显示对等体之间构建的 IPSec SA。12.1.1.1 与 12.1.1.2 之间将构建加密隧道，供网络 20.1.1.0 与 10.1.1.0 之间进出的流量使用。您可看到入站和出站时构建的两个封装安全有效负载 (ESP) SA。由于没有 AH SA，因此未使用身份验证报头 (AH)。

下面是 **show crypto ipsec sa** 命令的输出示例。

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 12.1.1.1
   local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 12.1.1.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
    #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0
     local crypto endpt.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound esp sas:
      spi: 0x136A010F(325714191)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4608000/52)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
inbound pcp sas:
outbound esp sas:
   spi: 0x3D3(979)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4608000/52)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

show crypto engine connection active

此命令用于显示构建的每个阶段 2 SA 和已发送的流量数。由于阶段 2（安全关联）SA 是单向的，因此每个 SA 只会显示一个方向的流量（加密为出站流量，解密为入站流量）。

debug crypto isakmp

下面是 **debug crypto isakmp** 命令的一个输出示例。

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
encryption DES-CBC
      hash SHA
default group 2
auth pre-share
life type in seconds
life duration (basic) of 240
atts are acceptable. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipsec

此命令用于显示 IPSec 隧道终结点的源和目标。Src_proxy 和 dest_proxy 是客户端子网。将显示两个“sa created”消息，一个方向上一个。（如果同时执行 ESP 和 AH，则会显示四个消息。）

下面是 **debug crypto ipsec** 命令的一个输出示例。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
```

```
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

错误消息示例

本部分提到的错误消息示例是从下面列出的 debug 命令生成的：

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

Replay Check Failed

下面是“Replay Check Failed”错误的一个输出示例：

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
```

```
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

此错误是由传输介质重新排序（特别是存在并行路径时）造成的，或者是由 Cisco IOS 内部对于大小数据包的数据包处理路径不均衡，再加上负载原因造成的。请更改转换集以反映这一点。仅在启用 transform-set esp-md5-hmac 后才会看到*答复检查*。若要不显示此错误信息，请禁用 esp-md5-hmac，只执行加密。请参阅 Cisco bug ID CSCdp19680（仅限注册用户）。

关于如何配置IPsec反重放窗口的信息，参考如何配置IPsec反重放窗口：展开和禁用。

QM FSM 错误

IPsec L2L VPN 隧道未出现在 PIX 防火墙或 ASA 上，并显示 *QM FSM* 错误消息。

一个可能的原因是两端上的代理身份（如相关的流量、访问控制列表 (ACL) 或加密 ACL）不匹配。请检查两端设备上的配置，并确保加密 ACL 匹配。

另一个可能的来源是不匹配转换集合参数。确保在两端， VPN网关以确切使用同一转换集同样参数。

Invalid Local Address

下面是此错误消息的一个输出示例：

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
```

```
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

此错误消息由以下两个常见问题之一所致：

- crypto map map-name local-address interface-id 命令会使路由器将不正确的地址用作标识，因为它强制路由器使用指定的地址。
- 这样加密映射会应用于错误的接口或根本无法应用。请检查配置以确保加密映射应用于正确的接口。

IKE信息从X.X.X.X失败其健全性检查或是畸形的

如果对等体上的预共享密钥不匹配，则会显示此 debug 错误。若要修复此问题，请检查两端的预共享密钥。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
```

```
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Processing of Main Mode Failed with Peer

下面是*主模式* 错误消息的一个示例。主模式故障表示两端上的阶段 1 策略不匹配。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
```

```
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

show crypto isakmp sa 命令显示 ISAKMP SA 处于 MM_NO_STATE。这也表示主模式已失败。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
```

```
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

请确认两个对等体上均存在阶段 1 策略，并确保所有属性均匹配。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Proxy Identities Not Supported

如果 IPSec 流量的访问列表不匹配，调试中就会显示此消息。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

每个对等体上的访问列表都需要互相反映（所有条目均需可逆）。以下示例说明了这一点。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
```

```
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Transform Proposal Not Supported

如果两端上的阶段 2 (IPsec) 不匹配，则会显示此消息。出现此错误消息的最常见情况是转换集不匹配或不兼容。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
```

```
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

请验证两端上的转换集是否匹配：

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
```

```
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

No Cert and No Keys with Remote Peer

此消息表明路由器上配置的对等体地址是错误的或已发生变化。请验证对等体地址是否正确以及是否可到达。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
```

```
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Peer Address X.X.X.X Not Found

此错误消息通常与相应的 VPN 3000 集中器错误消息 Message:No proposal chosen(14) 一同出现。这是由主机与主机之间的连接所致。路由器配置将 IPSec 提议以为路由器选择的提议顺序与访问控制列表（而不是对等体）匹配。该访问列表有一个更大的网络，其中包含与流量相交的主机。若要更正此错误，请将此集中器到路由器连接的路由器提议设置为最优先采用。这样可使它首先匹配特定的主机。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
```

```
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

IPsec Packet has Invalid SPI

下面是此错误消息的一个输出示例：

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

收到的 IPSec 数据包指定了一个安全关联数据库 (SADB) 中不存在的安全参数索引 (SPI)。这可能是由以下原因导致的临时情况：

- IPSec 对等体之间的安全关联 (SA) 的时效存在细微差异
- 本地 SA 已被清除
- IPSec 对等体发送的数据包不正确

这也可能是一种攻击。

建议操作：对等体可能未确认本地 SA 已被清除。如果新连接是从本地路由器建立的，则二个对等体随后可以成功重新建立连接。否则，如果此问题持续的时间较长，请尝试建立一个新连接或与对等体的管理员联系。

IPSEC(initialize_sas):Invalid Proxy IDs

错误 21:57:57:`IPSEC(initialize_sas):`Invalid proxy IDs 表示按照访问列表，接收到的代理身份与配置的代理身份不匹配。若要确保这两个身份匹配，请检查 **debug** 命令的输出。

在提议请求的 **debug 命令输出**中，对应的访问列表 103 允许 ip 10.1.1.0 0.0.0.255 与 20.1.1.0 0.0.0.255 不匹配。一端上的访问列表特定于网络，而另一端上的网络特定于主机。

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
encaps is 1
SA life type in seconds
SA life duration (basic) of 3600
SA life type in kilobytes
SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
  not acceptable".
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 20.1.1.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 12.1.1.2 to 12.1.1.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1,
      dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 12.1.1.2, dest= 12.1.1.1,
      src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 20.1.1.0/255.255.255.0/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa): sa created,
```

```
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa): sa created,
      (sa) sa_dest= 12.1.1.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Reserved Not Zero on Payload 5

这表示 ISAKMP 密钥不匹配。请重新生成或重置密钥以确保准确性。

Hash Algorithm Offered does not Match Policy

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。如果该策略仍不匹配，则路由器的 ISAKMP 协商失败。此时，用户会在路由器上收到 Hash algorithm offered does not match policy!或 Encryption algorithm offered does not match policy!错误消息。

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matching 209.165.200.227
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Hash algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
=RouterB=
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 65535 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1): Encryption algorithm offered does not match policy!
ISAKMP (0:1): atts are not acceptable. Next payload is 0
ISAKMP (0:1): no offers accepted!
ISAKMP (0:1): phase 1 SA not acceptable!
```

HMAC Verification Failed

如果对 IPSec 数据包验证哈希消息验证代码 (HMAC) 时出错，则会报告此错误消息。当数据包受到任何形式的损坏时通常会发生这种情况。

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

如果偶尔收到此错误信息，则可以忽略它。不过，如果此错误消息出现得越来越频繁，则需要调查

数据包损坏的真正原因。这可能是由加密加速器出错造成的。

Remote Peer Not Responding

如果转换集不匹配，则会收到此错误信息。请确保两个对等体上配置的转换集匹配。

所有SA IPSec建议认为不可接受

当第2阶段IPSec参数不匹配在本地和远端站点之间时，此错误消息出现。为了解决此问题，请指定在设置的转换的同样参数，以便他们配比，并且成功的VPN设立。

Packet Encryption/Decryption Error

下面是此错误消息的一个输出示例：

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

此错误消息可能是由以下原因之一造成的：

- *分段* - 经过分段的加密数据包是以进程方式交换的，这会强制快速交换的数据包在进程交换数据包之前发送至 VPN 卡。如果在进程交换数据包之前处理了足够多的快速交换数据包，进程交换数据包的 ESP 或 AH 序列号就会过期，这样当数据包到达 VPN 卡时，其序列号就会超出重播窗口的范围。这会导致 AH 或 ESP 序列号错误（分别为 4615 和 4612），具体取决于使用的封装。
- *过期的缓存项* - 如果在快速交换项过期且第一个未使用缓存的数据包以进程方式交换时，也可能发生这种情况。

应急方案

1. 关闭任何一种针对 3DES 转换集的身份验证，并使用 ESP-DES/3DES。这可以有效地禁用身份验证/防重播保护，进而防止出现与无序（混合）IPsec 流量相关的数据包删除错误 *%HW_VPN-1-HPRXERR:Hardware VPN0/2:Packet Encryption/Decryption error, status=4615*。
2. 对于上面第一项中提到的原因，一种行之有效的解决方法是将入站流的最大传输单元 (MTU) 大小设置为小于 1400 个字节。输入以下命令可将入站流的最大传输单元 (MTU) 大小设置为小于 1400 个字节：
   ```
   Sep 22 11:02:39 131.203.252.166 2435:
   Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
   Sep 22 11:02:39 131.203.252.166 2436:
   Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                    PktEngReturn_MACMiscompare
   ```
3. 禁用 AIM 卡。
4. 关闭路由器接口上的快速/CEF 交换。若要取消快速交换，可在接口配置模式下使用以下命令：
   ```
   Sep 22 11:02:39 131.203.252.166 2435:
   Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
   ```

```
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

数据包接收错误由于ESP顺序失败

这是错误消息的示例：

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure
Sep 22 11:02:39 131.203.252.166 2436:
Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                 PktEngReturn_MACMiscompare
```

此错误消息通常指示这些可能的情况之一：

- IPsec加密的信息包转发的有故障由加密路由器由于一不正确的配置的QoS机制。
- 解密的路由器接收的IPSec信息包故障中归结于重拨在中间设备的数据包。
- 已接收IPSec信息包被分段并且在验证认证和解密前要求重组。

解决方法

1. 禁用IPSec数据流的QoS在加密或中间路由器。
2. 启用在加密路由器的IPsec PRE分段。
   ```
   Router(config-if)#crypto ipsec fragmentation before-encryption
   ```
3. 设置MTU值为不必须被分段的大小。
   ```
   Router(config)#interface type [slot_#/]port_#


   Router(config-if)#ip mtu MTU_size_in_bytes
   ```
4. 升级IOS镜像对在该系列的最新的可用的稳定的镜像。

注意： 更改在所有路由器接口的MTU大小将导致在该接口终止的所有通道将被切断。在被安排的停工期期间，您必须计划完成此应急方案。

尝试的错误设立在7600系列路由器的VPN通道

当您设法设立在7600系列路由器时的一个VPN通道此错误接收：

```
Router(config-if)#ip mtu MTU_size_in_bytes
```

因为7600系列路由器，不支持软件加密此错误出现。7600系列路由器不支持IPSec隧道终端没有IPsec SPA硬件。VPN仅支持与一个IPSEC-SPA卡7600年路由器。

PIX 调试

show crypto isakmp sa

此命令用于显示对等体之间构建的 ISAKMP SA。

```
Router(config-if)#ip mtu MTU_size_in_bytes
```

在 **show crypto isakmp sa** 输出中，状态应始终为 QM_IDLE。如果状态为 MM_KEY_EXCH，则表示配置的预共享密钥不正确，或对等体的 IP 地址不相同。

```
PIX(config)#show crypto isakmp sa
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

配置正确的 IP 地址或预共享密钥后即可纠正此错误。

show crypto ipsec sa

此命令用于显示对等体之间构建的 IPSec SA。12.1.1.1 与 12.1.1.2 之间将构建一个加密隧道，供网络 20.1.1.0 与 10.1.1.0 之间进出的流量使用。您可看到入站和出站时构建的两个 ESP SA。没有使用 AH，因为没有 AH SA。

下面是 **show crypto ipsec sa** 命令的一个输出示例。

```
interface: outside
    Crypto map tag: vpn, local addr. 12.1.1.1
   local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (12.1.1.2/255.255.255.255/0/0)
   current_peer: 10.2.1.1
   dynamic allocated peer ip: 12.1.1.2
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
     local crypto endpt.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound esp sas:
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
```

```
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

此命令用于显示 IPSec 连接的相关调试信息，同时显示由于两端上的不兼容而被拒绝的第一组属性。第二次匹配尝试（尝试 3DES，而不是 DES 和安全哈希算法 [SHA]）是可接受的并构建了 ISAKMP SA。接收本地池之外 IP 地址 (10.32.8.1) 的拨号客户端也会发出此 debug 命令。构建 ISAKMP SA 之后，就会对 IPSec 属性进行协商，并最终发现它们是可接受的。PIX 随后会设置 IPSec SA，如下所示。

下面是 **debug crypto isakmp** 命令的一个输出示例。

```
crypto_isakmp_process_block: src 12.1.1.1, dest 12.1.1.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 12.1.1.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 12.1.1.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 12.1.1.2, dest 12.1.1.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 12.1.1.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0): peer accepted the address!
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0): atts are acceptable.
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
```

```
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 12.1.1.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

此命令用于显示 IPSec 连接的相关 **debug** 信息。

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  12.1.1.2  to  12.1.1.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 12.1.1.2, dest 12.1.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from  12.1.1.2  to  12.1.1.1
           (proxy 10.32.8.1 to  12.1.1.1.)
        has spi 3576885181 and conn_id 2 and flags 4
        outbound SA from  12.1.1.1  to  12.1.1.2
           (proxy 12.1.1.1 to 10.32.8.1)
        has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
           got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 12.1.1.1, src= 12.1.1.2,
    dest_proxy= 12.1.1.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 12.1.1.1, dest= 12.1.1.2,
    src_proxy= 12.1.1.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

路由器到 VPN Client 的常见问题

无法访问 VPN 隧道外部的子网：分割隧道

下面的路由器配置输出示例说明了如何为 VPN 连接启用分割隧道。**access list 150** 命令与 crypto isakmp client configuration group hw-client-groupname 命令中配置的组关联。这样 Cisco VPN Client 即可使用路由器来访问不属于 VPN 隧道的其他子网。这样做不会损害 IPSec 连接的安全性。该隧道形成于 172.168.0.128 网络上。**access list 150** 命令中未定义对设备来说未加密的流量流，例如 Internet。

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
```

```
 acl 150
!
!
access-list 150 permit ip 172.168.0.128 0.0.0.127 any
!
```

PIX 到 VPN Client 的常见问题

本部分中的主题可解决您在 VPN Client 3.x 的帮助下配置 PIX 到 IPsec 时遇到的常见问题。PIX 的配置示例基于版本 6.x。

建立隧道之后流量不流通：无法 ping 通位于 PIX 后的网络内部

这是与路由选择有关的一个常见问题。请确保 PIX 有一个通往内部网络的路由，而不是直接连接到同一子网。另外，对于客户端地址池中的地址，内部网络需要有一个返回 PIX 的路由。

下面是一个输出示例。

```
!
crypto isakmp client configuration group hw-client-groupname
 key hw-client-password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
 acl 150
!
!
access-list 150 permit ip 172.168.0.128 0.0.0.127 any
!
```

建立隧道之后，用户无法浏览 Internet：分割隧道

产生此问题的最常见原因是，对于从 VPN Client 到 PIX 的 IPSec 隧道，所有流量均通过该隧道发送到 PIX 防火墙。而 PIX 功能不允许流量发送回接收该流量的接口。因此，发送至 Internet 的流量不起作用。若要修复此问题，请使用 **split tunneling** 命令。这种解决方法的背后思想是仅通过该隧道发送一次特定的流量，其余流量直接进入 Internet，不经过该隧道。

```
vpngroup vpn3000 split-tunnel 90
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

注意： **vpngroup vpn3000 split-tunnel 90** 命令用于对访问列表编号 90 启用分割隧道。access-list 90命令用于定义哪些流量流经该隧道，控制列表末尾处的其余流量将被拒绝。访问列表需要相同以拒绝 PIX 上的网络地址转换 (NAT)。

建立隧道之后，某些应用程序无法正常工作：对客户端进行 MTU 调节

有时，建立隧道之后，您也许可以 ping 通位于 PIX 防火墙后网络中的计算机，但却无法使用某些应用程序，如 Microsoft Outlook。常见的一个问题是数据包的最大传送单位 (MTU) 大小。IPSec 报头最长可达 50 到 60 个字节，将添加到原始数据包中。如果数据包的大小超过 1500（Internet 的默认值），则设备就需要对其进行分段处理。数据包添加 IPSec 报头后，大小仍在 1496 以下，这是 IPSec 允许的最大大小。

show interface 命令用于显示可访问的路由器或您自己一端的路由器上该特定接口的 MTU。为了确定从源到目标整个路径的 MTU，将在设置“不分段 (DF)”位的情况下发送各种大小的数据报，这样，如果发送的数据报大于 MTU，将向源发回以下错误消息：

```
vpngroup vpn3000 split-tunnel 90
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

下面的输出示例说明如何查找 IP 地址分别为 10.1.1.2 和 172.16.1.56 的主机之间的路径的 MTU。

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

!--- Perform an extended ping. Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1550
Timeout in seconds [2]:

!--- Make sure you enter y for extended commands. Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:

!--- Set the DF bit as shown. Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

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

!--- Reduce the datagram size further and perform extended ping again. Router#ping
Protocol [ip]:
Target IP address: 172.16.1.56
Repeat count [5]:
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
```

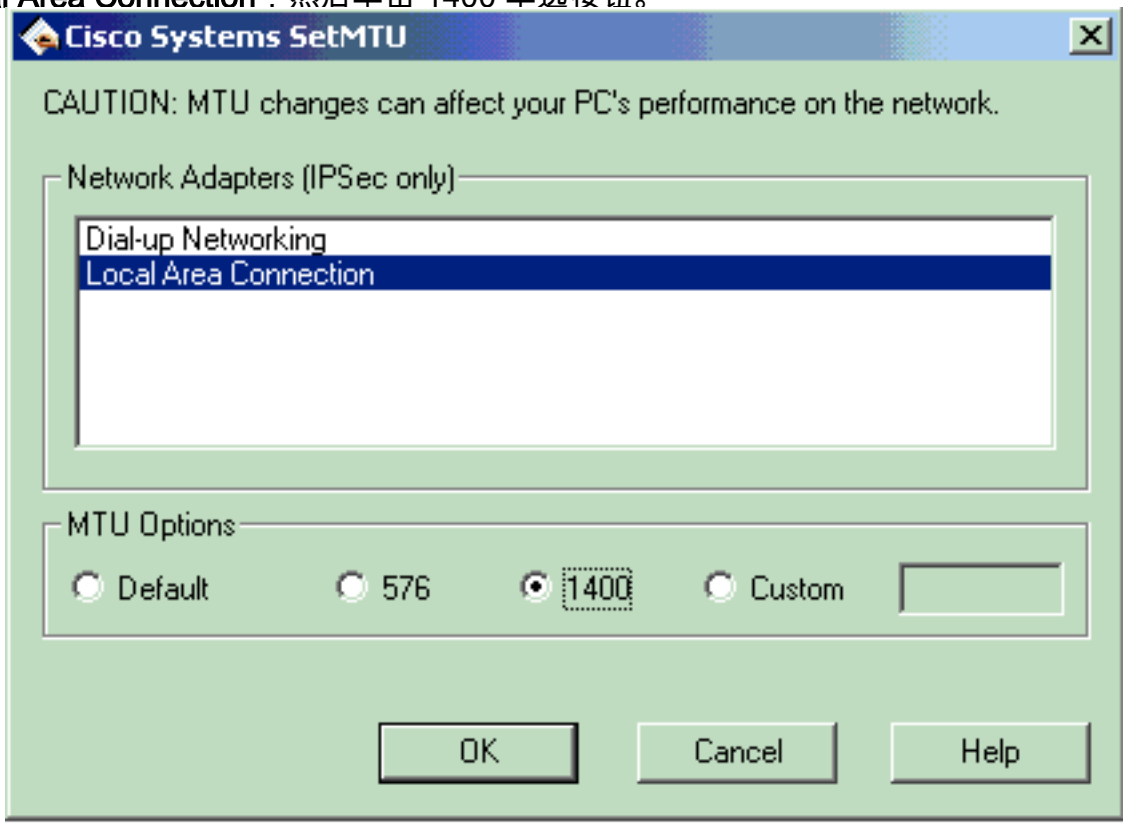
```
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

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

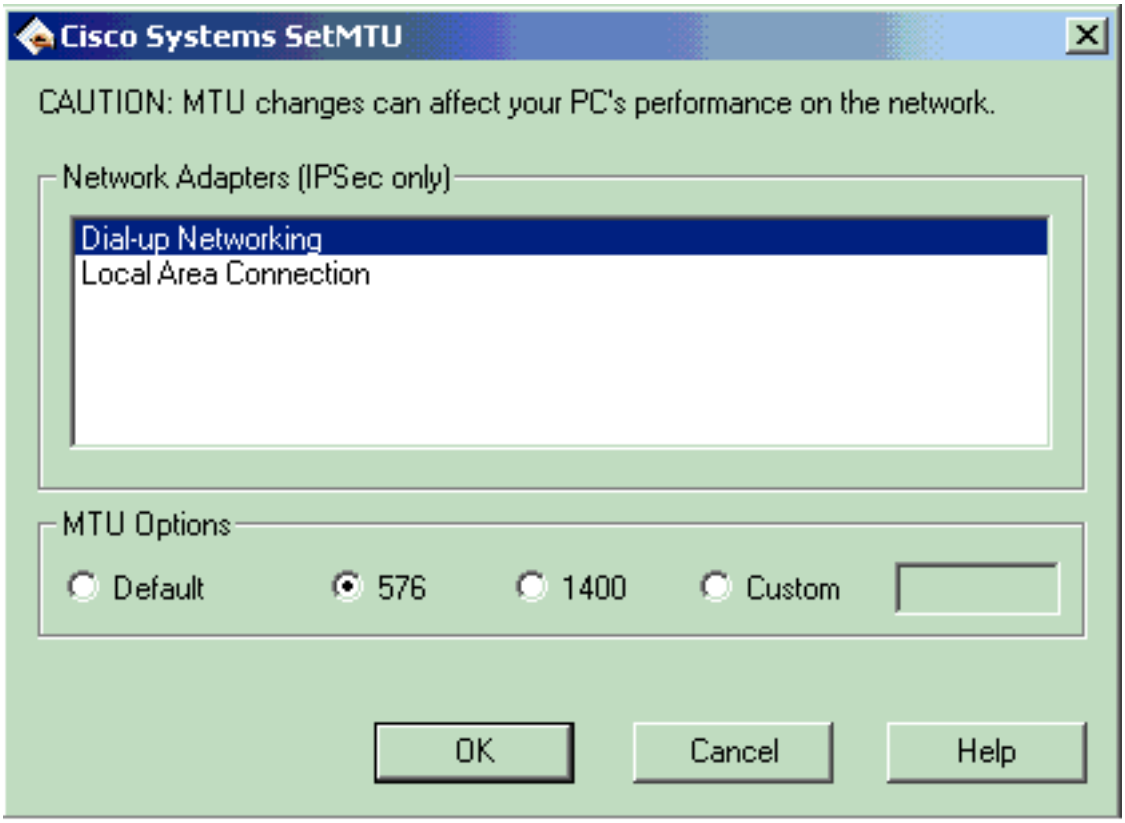
注意： VPN 客户端提供了一个 MTU 调整实用程序，用户可用它调整 Cisco VPN Client 的 MTU。如果是以太网上的 PPP (PPPoE) 客户端用户，请调整 PPPoE 适配器的 MTU。

注意： 若要为 VPN Client 调整 MTU 实用程序，请完成以下步骤。

1. 选择 **Start > Programs > Cisco System VPN Client > Set MTU**。
2. 选择 **Local Area Connection**，然后单击 1400 单选按钮。



3. 单击 **Ok**。
4. 重复步骤 1，然后选择 **Dial-up Networking**。
5. 单击 **576** 单选按钮，然后单击 OK。



无法使用 sysopt 命令

若要允许 IPsec 流量通过 PIX 防火墙而不检查 conduit 或 access-list 命令语句，请在 PIX 上的 IPsec 配置中使用 **sysopt connection permit-ipsec** 命令。默认情况下，所有入站会话均必须由 **conduit** 或 access-list 命令语句显式许可。对于 IPSec 保护的流量，备用访问列表检查可能是多余的。若要使 IPsec 验证的/密码入站会话总是被允许，请使用 **sysopt connection permit-ipsec** 命令。

验证访问控制列表 (ACL)

典型的 IPSec VPN 配置中会使用两个访问列表。一个访问列表用于免除从 NAT 进程发送至 VPN 隧道的流量。另一个访问列表用于定义要加密的流量。其中包括 LAN 到 LAN 设置中的加密 ACL 或远程访问配置中的分割隧道 ACL。如果这些 ACL 的配置不正确或未配置，则流量只会通过 VPN 隧道向一个方向流动，或者根本不通过该隧道发送。

请确保已配置了完成 IPSec VPN 配置所需的所有访问列表，且这些访问列表定义了正确的流量。此列表包含的项目是在您怀疑 ACL 是 IPSec VPN 所出现问题的原因时需要检查的项目。

- 请确保 NAT 免除和加密 ACL 指定了正确的流量。
- 如果有多个 VPN 隧道和多个加密 ACL，请确保这些 ACL 不会重叠。
- 请勿重复使用 ACL。即使 NAT 免除 ACL 和加密 ACL 指定的是相同流量，也请使用两个不同的访问列表。
- 请确保您的设备已配置为使用 NAT 免除 ACL。也就是说，对路由器使用 **route-map** 命令；对 PIX 或 ASA 使用 **nat (0)** 命令。LAN 到 LAN 配置和远程访问配置都需要使用 NAT 免除 ACL。

若要了解有关如何验证 ACL 语句的详细信息，请参阅最常见的 L2L 和远程接入 IPsec VPN 故障排除解决方案中的验证 ACL 是否正确部分。

相关信息

- IPsec 协商/IKE 协议支持页
- IP 安全 (IPsec) 加密简介
- PIX 支持页
- PIX 命令参考
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems