了解并使用调试命令排除 IPsec 问题

目录

简介

本文档介绍对 Cisco IOS® 软件和 PIX/ASA 上的 IPsec 问题进行故障排除时常用的调试命令。

先决条件

要求

本文档假定您已配置了 IPsec。有关详细信息，请参阅 IPSec 协商/IKE 协议。

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 — 表示单个功Data Encryption Standard (DES)能(在Cisco IOS®软件版本11.2及更高版本上)。
  - k2 - 表示三重 DES 功能（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 及更高版本，需要单一或三重 DES 许可证密钥才能激活。

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。如果您的网络处于活动状态，请确保您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。

背景信息

有关 IPsec VPN 问题的常用解决方案，请参阅常用的 L2L 和远程访问 IPsec VPN 故障排除解决方案了解更多信息。

其中包含一些常用步骤的要点概览，在开始排除连接问题和联系思科技术支持团队之前，您可以先尝试这些操作。

Cisco IOS® 软件调试

本节的主题是介绍 Cisco IOS® 软件的调试命令。有关详细信息，请参阅 IPSec 协商/IKE 协议。

show crypto isakmp sa

此命令显示对等体之Internet Security Association Management Protocol (ISAKMP) Security Associations (SAs)间已构建的。

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   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。10.1.0.1 与 10.1.0.2 之间将构建加密隧道，供网络 10.1.0.0 与 10.1.1.0 之间进出的流量使用。

您可以看到入站和出Encapsulating Security Payload (ESP)站构建的两个SA。由于没有 AH SA，因此未使用身份验证报头 (AH)。

此输出显示命令的示**show crypto ipsec sa**例。

```
<#root>

  interface: FastEthernet0
    Crypto map tag: test, local addr.

10.1.0.1

   local  ident (addr/mask/prot/port): (

10.1.0.0/255.255.255.0/0/0

)
   remote ident (addr/mask/prot/port): (

10.1.1.0/255.255.255.0/0/0

)
   current_peer:

10.1.0.2

     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.: 10.1.0.1, remote crypto endpt.: 10.1.0.2

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。

由于第2阶段Security Associations (SAs)是单向的，因此每个SA仅显示一个方向的流量（加密为出站，解密为入站）。

debug crypto isakmp

此输出显示命令的示**debug crypto isakmp**例。

<#root>

```
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

此命令显示IPsec隧道端点的源和目标Src_proxy。它dest_proxy们是客户端子网。

sa created两个消息在每个方向上显示一个。（如果同时执行 ESP 和 AH，则会显示四个消息。）

此输出显示命令的示**debug crypto ipsec**例。

<#root>

```
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= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      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 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest=

10.1.0.2

, src=

10.1.0.1

,

**dest_proxy= 10.1.1.0/255.255.255.0/0/0,
      src_proxy= 10.1.0.0/255.255.255.0/0/0,**

      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=

10.1.0.2

, dest=

10.1.0.1,

**src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,**

      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= 10.1.0.2, 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= 10.1.0.2, 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

以下输出显示错误示"Replay Check Failed"例：

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

当传输介质重新排序（尤其是在有并行路径的情况下）时，或者，如果在负载情况下 Cisco IOS® 内部处理的大型数据包和小型数据包路径不相等，就可能导致该错误。

请更改转换集以反映这一点。仅reply check在启用时会transform-set esp-md5-hmac显示。要阻止此错误消息，请禁用esp-md5-hmac，仅执行加密。

请参阅思科漏洞 ID CSCdp19680（仅限注册客户）。

QM FSM 错误

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

一个可能的原因是代理身份(如异常流量Access Control List (ACL),或加密ACL)两端不匹配。

请检查两端设备上的配置，并确保加密 ACL 匹配。

另一个可能的原因是转换集参数不匹配。验证两端的 VPN 网关是否使用参数完全相同的同一转换集。

Invalid Local Address

下面是此错误消息的一个输出示例：

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

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**该命令导致路由器使用错误的地址作为标识，因为它强制路由器使用指定的地址。
- Crypto map 应用到错误的接口或根本不应用。请检查配置以确保加密映射应用于正确的接口。

IKE message from X.X.X.X failed its sanity check or is malformed

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。

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

主模式进程因对等体而失败

这是错误消息的Main Mode示例。主模式故障表示两端上的阶段 1 策略不匹配。

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

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

```
dst          src        state             conn-id         slot
10.1.1.2  10.1.1.1   MM_NO_STATE        1           0
```

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。

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

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。

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

每个对等设备上的访问列表需要相互镜像（所有条目都需要可逆）。以下示例说明了这一点。

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

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。

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

请验证两端上的转换集是否匹配：

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
```

```
? esp-3des and esp-sha-hmac
? comp-lzs
```

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。

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

Peer Address X.X.X.X Not Found

此错误消息与错误消息一VPN 3000 Concentrator 起出现"Message: No proposal chosen(14)"。因为这些连接是主机到主机模式。

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。

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

IPsec Packet has Invalid SPI

下面是此错误消息的一个输出示例：

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

收到的IPsec数据包指 Security Parameters Index (SPI)定中不存在的 Security Associations Database (SADB)数据包。这

可能是由以下原因导致的临时情况：

- IPsec对等体之间的老化方Security Sssociations (SAs)面略有差异。
- 本地 SA 已清除.
- IPSec 对等体发送的数据包不正确.

这可能是受到了网络攻击。

建议操作：

对等体可能未确认本地SA已清除。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，如果问题持续超过一段时间，则请尝试建立新连接或联系对等体的管理员。

PSEC(initialize_sas)：代理ID无效

此错误"21:57:57: IPSEC(initialize_sas): invalid proxy IDs"表示收到的代理身份与根据访问列表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，access-list 103 permit ip 10.1.1.0 0.0.0.255 10.1.0.0 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。

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

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。

用户会在路由器"Hash algorithm offered does not match policy!""Encryption algorithm offered does not match policy!"上收到任何一条错误消息。

<#root>

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
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

当IPsec数据包上的线程验证失败时，将报Hash Message Authentication Code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。

<#root>

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39:
%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure

Sep 22 11:02:39 203.0.113.16 2436:
```

```
Sep 22 11:02:39:

%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
                  PktEngReturn_MACMiscompare
```

如果偶尔遇到此错误消息，可以忽略它。但是，如果这种情况变得比较频繁，则需要调查数据包损坏的根源。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。请确保两对等体上配置的转换集相互匹配。

所有 IPSec SA 提议均不可接受

当本地站点和远程站点的第 2 阶段 IPSec 参数不匹配时，会出现此错误消息。

要解决此问题，请在转换集中指定相同的参数，使其匹配并成功建立 VPN。

Packet Encryption/Decryption Error

下面是此错误消息的一个输出示例：

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

出现此错误消息可能有以下原因：

- 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。

解决方法

1. 关闭任何一种针对 3DES 转换集的身份验证，并使用 ESP-DES/3DES。这将有效禁用身份验证/反重播保护，从而防止与未排序（混合）IPsec流量相关的丢包错%HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615误。
2. 适用于此处所述原因的一种解决方法是将入站Maximum Transmission Unit (MTU)流的大小设置为小于1400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：

```
ip tcp adjust-mss 1300
```

3. 禁用 AIM 卡。
4. 关闭路由器接口上的快速/CEF 交换。要删除快速交换，请在接口配置模式下使用此命令：

```
no ip route-cache
```

ESP 序列失败导致数据包接收错误

以下是错误消息的示例：

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

此错误消息通常表示存在以下某种情况：

- 由于 QoS 机制配置错误，加密路由器会无序转发 IPsec 加密数据包。
- 由于中间设备上的数据包重新排序，使得解密路由器接收的 IPsec 数据包顺序混乱。
- 收到的 IPsec 数据包呈分段状态，需要重组后才能进行身份验证和解密。

解决方法

1. 在加密或中间路由器上禁用 IPsec 流量的 QoS。
2. 在加密路由器上启用 IPsec 预分段。

```
<#root>
Router(config-if)#
crypto ipsec fragmentation before-encryption
```

3. 将 MTU 值设置为不必分段的大小。

```
<#root>
Router(config)#
```

```
interface type [slot_#/]port_#
```

```
<#root>

Router(config-if)#

ip mtu MTU_size_in_bytes
```

4. 将 Cisco IOS® 映像升级到该系列中可用的最新稳定映像。

如果更改任何路由器上的MTU大小，则在该接口上终止的所有隧道都会被拆除。

制定计划，在计划停机时间内完成此解决方法。

尝试在 7600 系列路由器上建立 VPN 隧道时出错

当您尝试在 7600 系列路由器上建立 VPN 隧道时，会收到以下错误：

```
crypto_engine_select_crypto_engine: can't handle any more
```

出现此错误的原因是7600系列路由器不支持软件加密。7600 系列路由器在没有 IPsec SPA 硬件的情况下不支持 IPsec 隧道终止。仅在 7600 路由器上使用 IPSEC-SPA 卡时才能支持 VPN。

PIX 调试

show crypto isakmp sa

此命令用于显示对等体之间构建的 ISAKMP SA。

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

在show crypto isakmp sa输出中，状态必须始终为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。

```
<#root>

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。10.1.0.1 与 10.1.0.2 之间将构建一个加密隧道，供网络 10.1.0.0 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。

此输出中**show crypto ipsec sa**显示了命令的示例。

```
<#root>

interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (

10.1.0.0/255.255.255.0/0/0

)
   remote ident (addr/mask/prot/port): (

10.1.0.2/255.255.255.255/0/0

)
   current_peer: 10.2.1.1


dynamic allocated peer ip: 10.1.0.2

     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.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     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。

第二次尝试匹配(尝试使用3DES而非DES并且这Secure Hash Algorithm (SHA)些是可接受的，并且构建了 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。此输出显示命令的示**debug crypto isakmp**例。


```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
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 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   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 10.1.0.1 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。

<#root>

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
```

```
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0):
```

Creating IPSec SAs
inbound SA from 10.1.0.2 to 10.1.0.1
(proxy 10.32.8.1 to 10.1.0.1.)
has spi 3576885181 and conn_id 2 and flags 4
outbound SA from 10.1.0.1 to 10.1.0.2
(proxy 10.1.0.1 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= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (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=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (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 隧道外的子网：分割隧道

此路由器配置输出示例显示如何为 VPN 连接启用分割隧道。

该命**split tunnel**令与命令中配置的组相**crypto isakmp client configuration group hw-client-groupname**关联。

这样Cisco VPN Client，可以使用路由器访问不属于VPN隧道的其他子网。

这样做不会影响 IPsec 连接的安全。该隧道形成于 192.0.2.18 网络上。

流量未加密地流向命令中未定**access list 150**义的设备（例如Internet）。

<#root>

```
!
```

crypto isakmp client configuration group hw-client-groupname

```
 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool

acl 150


!
!
access-list 150 permit ip 192.0.2.18 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。

隧道建立后无流量：无法在 PIX 后面的网络内部 ping 通

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。

```
!--- Address of PIX inside interface.
ip address inside 10.1.1.1 255.255.255.240
!--- Route to the networks that are on the inside segment. !--- The next hop is the router on the inside
route inside 172.16.0.0 255.255.0.0 10.1.1.2 1
 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client for the I
ip local pool mypool 10.1.2.1-10.1.2.254
!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then the route
ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

隧道启动后，用户无法浏览互联网：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，发往Internet的流量不起作用。

要解决此问题，请使用命**split tunnel**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。

<#root>

```
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
```

vpngroup vpn3000 split-tunnel 90命令用于启用分割隧道access-list number 90。

access-list number 90该命令定义哪些流量流经隧道，其余流量在访问列表末尾被拒绝。

访问列表必须与denyon PIX相Network Address Translation (NAT)同。

隧道启动后，某些应用无法运行：客户端上的 MTU 调整

建立隧道后，虽然您可以ping通PIX防火墙后面的网络上的计算机，但您无法使用Microsoft等某些应用程序

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。

该命**show interface**令显示可访问的路由器或您自己的本地路由器上该特定接口的MTU。

为了确定从源到目的地的整个路径的MTU，将发送各种大小的数据报并设置位Do Not Fragment (DF)数，这样，如果发送的数据报大于MTU，则会将以下错误消息发送回源：

```
frag. needed and DF set
```

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。

<#root>

```
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
```

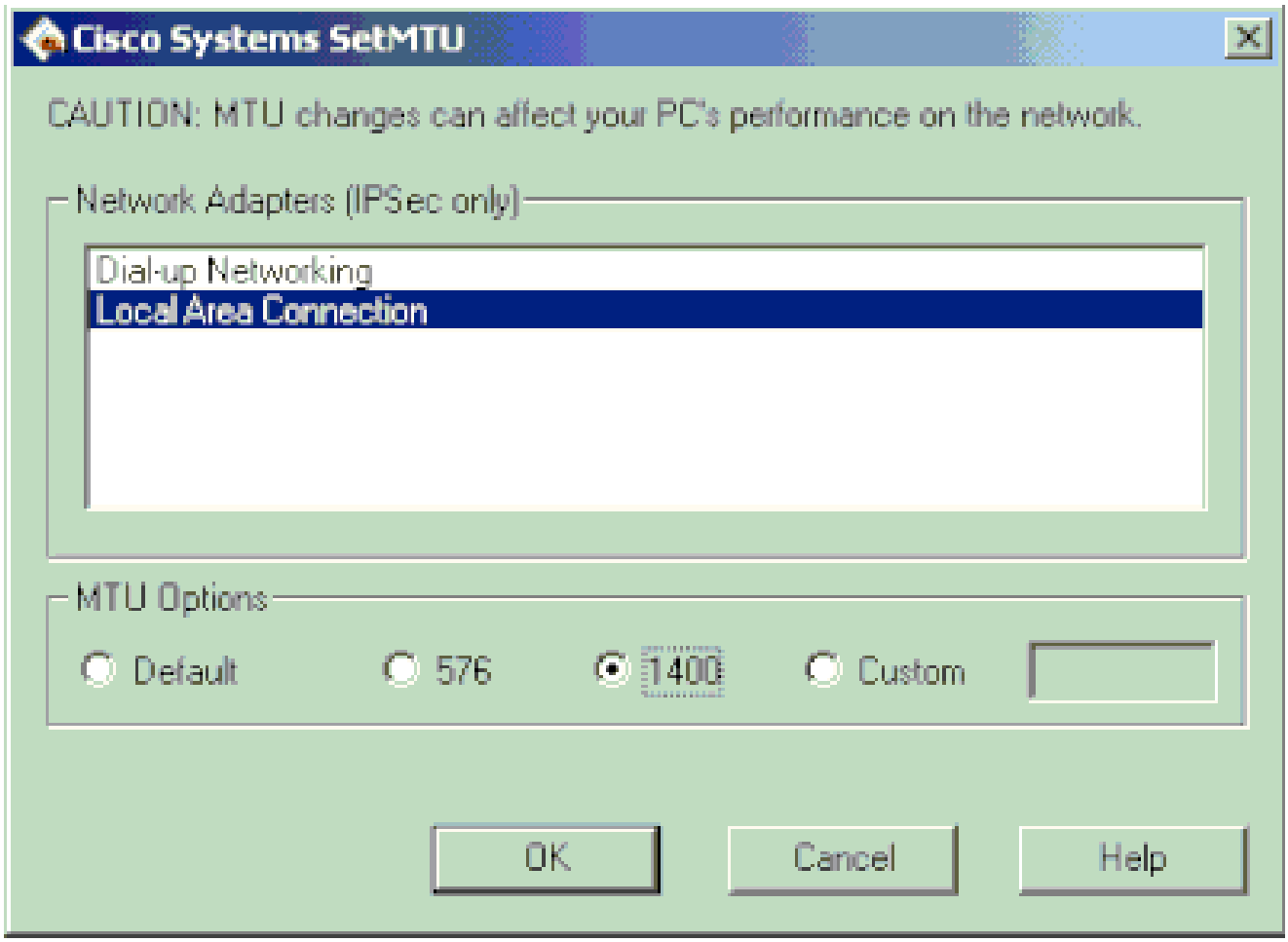
```
Repeat count [5]:
Datagram size [100]:

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
```

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。

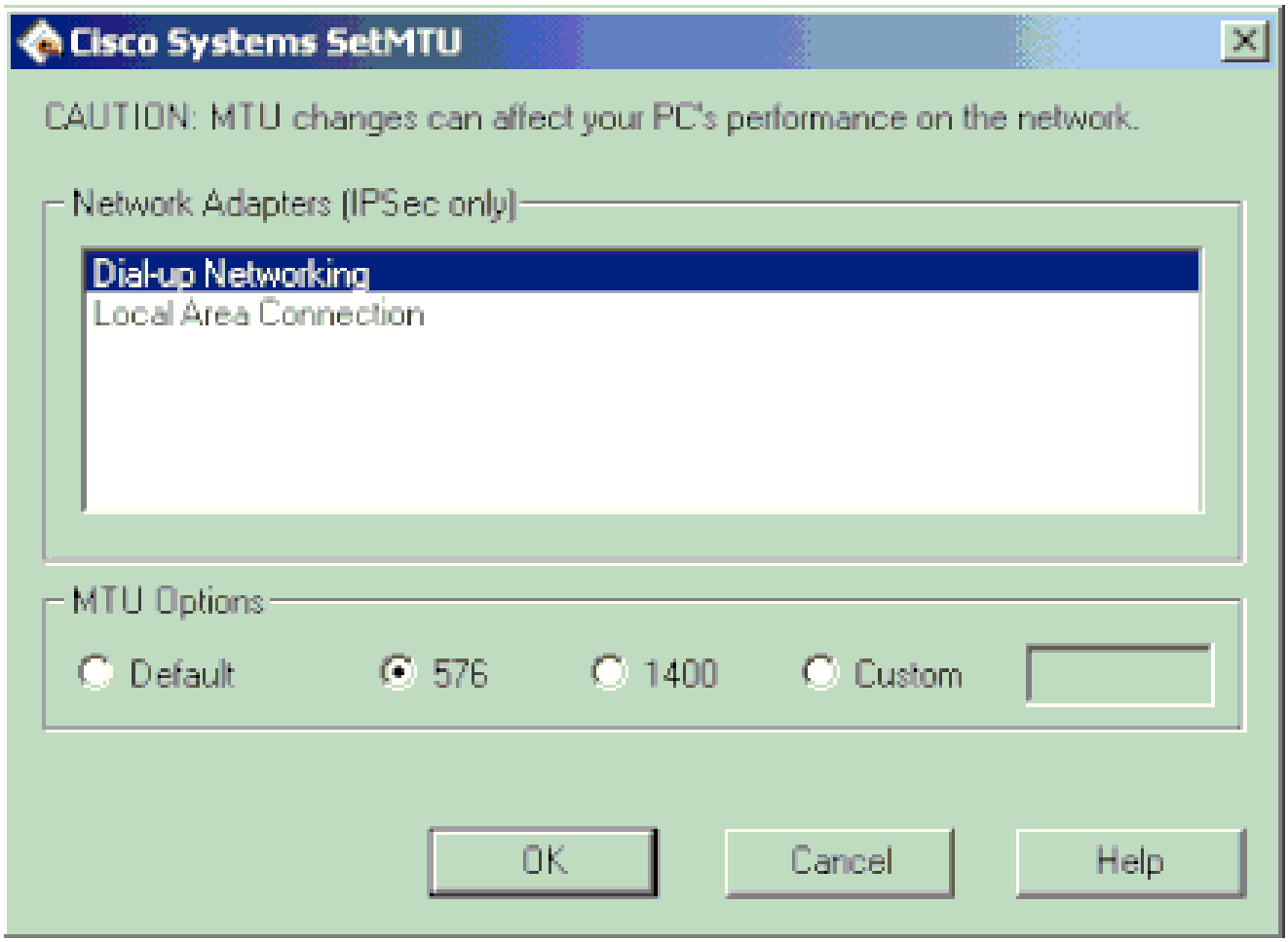
若要为 VPN Client 调整 MTU 实用程序，请完成以下步骤。

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. 点击**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

在PIX上的IPsec配置中使用命**sysopt connection permit-ipsec**令，以允许IPsec流量通过PIX防火墙，而无需检查**conduit access-list**/命令语句。

默认情况下，任何入站会话必须由or命令语句**conduit**明**access-list**确允许。对于 IPSec 保护的流量，备用访问列表检查可能是多余的。

要启用始终允许的IPsec身份验证/加密入站会话，请使用命**sysopt connection permit-ipsec**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。这包括 LAN 到 LAN 设置中的加密 ACL 或远程访问配置中的分割隧道 ACL。

当这些 ACL 配置不当或缺失时，流量可能仅在一个方向上流经 VPN 隧道，或者根本不通过隧道发送。

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。即，在路由**route-map**器上使用命令；在**nat (0)**PIX或ASA上使用命令。LAN 到 LAN 配置和远程访问配置都需要使用 NAT 免除 ACL。

要详细了解如何验证 ACL 语句，请参阅常用的 L2L 和远程访问 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
- PIX 支持页
- 技术说明
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。