对数据包捕获的IPsec隧道和常见控制平面问题进行故障排除

目录

简介

本文档介绍在协商Cisco IOS® XE路由器上的站点到站点VPN时，数据包捕获、其他工具如何帮助解决控制平面问题。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS® CLI配置的基本知识。
- IKEv2和IPsec的基础知识。

使用的组件

本文档中的信息基于以下软件版本：

- CSR1000V — 运行版本16.12.0的Cisco IOS XE软件。

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。

背景信息

数据包捕获是一个强大的工具，可帮助您验证数据包是否在VPN对等设备之间发送/接收。它们还确认IPsec调试中看到的行为是否与捕获上收集的输出一致，因为调试是一种逻辑解释，而捕获表示对等体之间的物理交互。因此，您可以确认或丢弃连接问题。

有用的工具

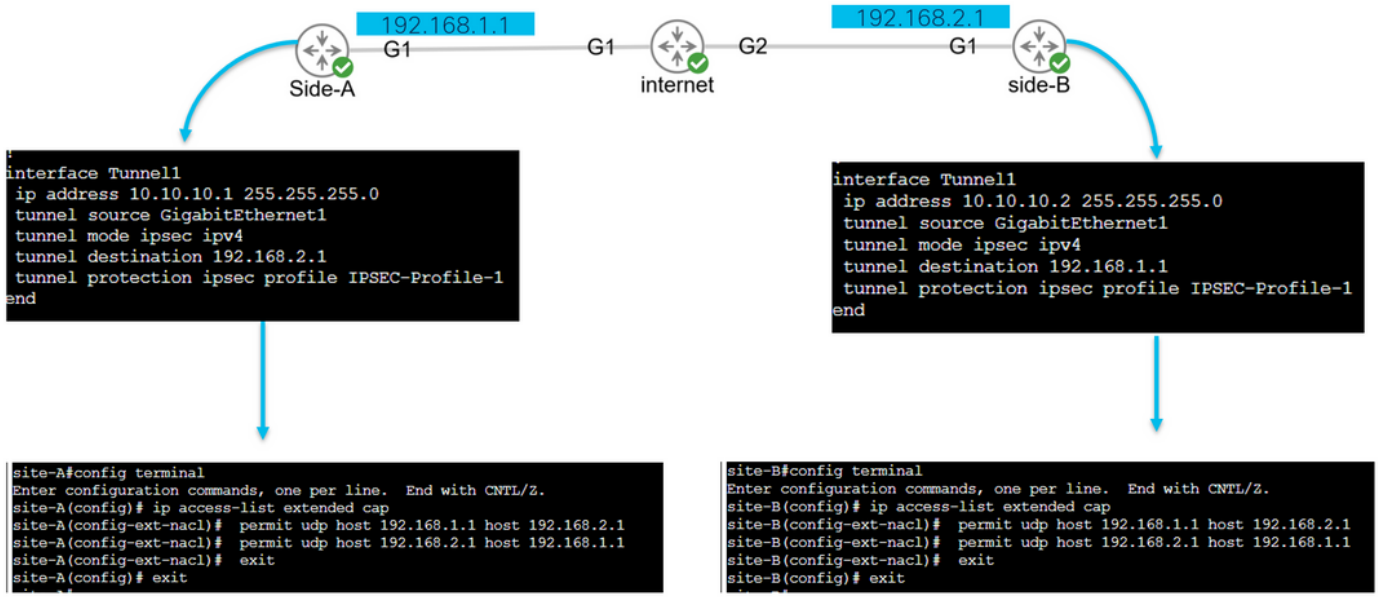
有一些有用的工具可帮助您配置捕获、提取输出并进一步分析输出。其中包括：

- Wireshark：这是一款广为人知且使用的开源数据包分析器。
- 监控器捕获：路由器上的Cisco IOS XE功能，可帮助您收集捕获，并提供流量外观、收集的协议及其时间戳的简单输出。

如何在IOS XE路由器上配置捕获

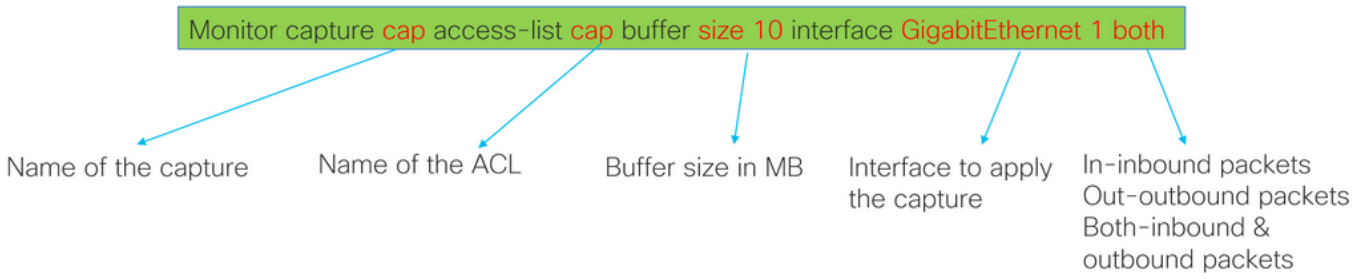
捕获使用扩展访问列表(ACL)，定义要收集的流量类型以及VPN对等体或相关流量段的源地址和目标地址。如果沿路径启用NAT-T，则隧道协商使用UDP端口500和端口4500。一旦协商完成并建立了隧道，如果启用NAT-T，相关流量将使用IP协议50(ESP)或UDP 4500。

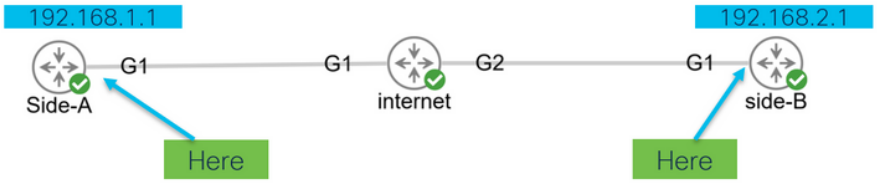
为了排除与控制平面相关的问题，必须使用VPN对等体IP地址捕获如何协商隧道。



```
config terminal
ip access-list extended <ACL name>
permit udp host <local address> host <peer address>
permit udp host <peer address> host <source address>
exit
exit
```

配置的ACL用于缩小捕获的流量，并放置在用于协商隧道的接口上。






```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-A#
```

```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-B#
```

```
monitor capture <capture name> access-list <ACL name> buffer size <custom buffer size in MB> interface
```

配置捕获后，可以通过操作将其停止、清除或提取使用以下命令收集的流量：

- 检查常规捕获信息：show monitor capture
- 开始/停止捕获：监控捕获上限开始/停止
- 验证捕获正在收集数据包：show monitor capture cap buffer

- 请参阅流量的简要输出:show monitor capture cap buffer brief
- 清除捕获：monitor capture cap clear
- 提取捕获输出：
  - monitor cap cap buff dump
  - monitor capture cap export bootflash:capture.pcap

使用数据包捕获分析隧道建立

如前所述，要协商IPSec隧道，如果启用了NAT-T，数据包将通过UDP与端口500和端口4500发送。通过捕获，可以看到来自这些数据包的更多信息，例如正在协商的阶段（阶段1或阶段2）、每个设备的角色（发起方或响应方），或者刚刚创建的SPI值。

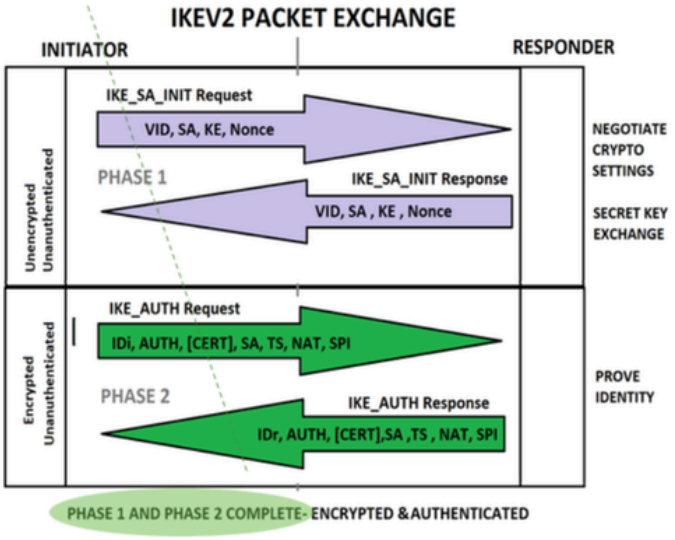
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

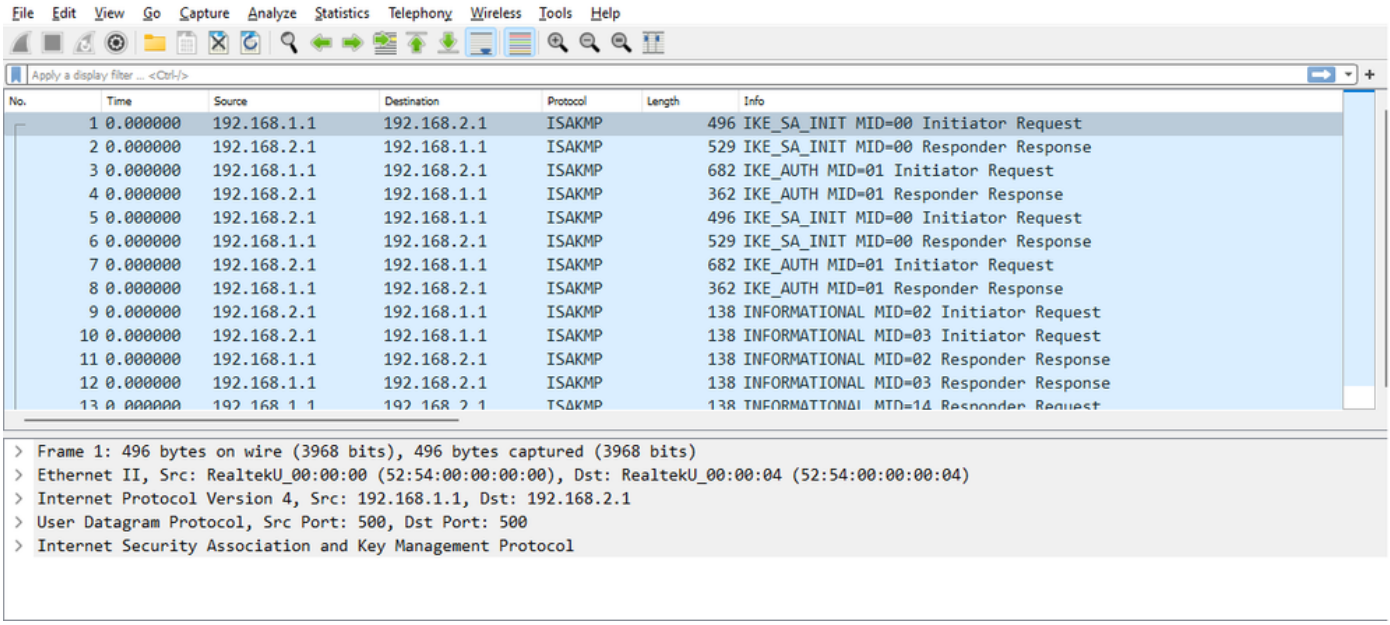
Phase 2 encrypted



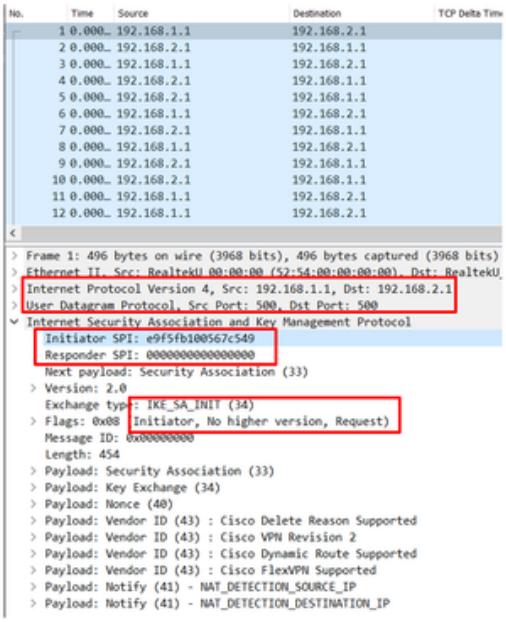
显示路由器捕获的简要输出，可以看到对等体之间的交互，发送UDP数据包。

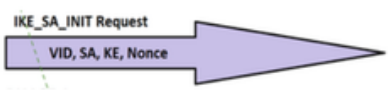
```
site-A#show monitor cap cap buffer brief
 ----------------------------------------------------------------------------
 #   size   timestamp     source               destination      dscp    protocol
 ----------------------------------------------------------------------------
   0  496    0.000000   192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   1  529    0.011992   192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   2  682    0.026991   192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   3  362    0.035993   192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   4  496    0.579016   192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   5  529    0.593023   192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   6  682    0.610020   192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   7  362    0.616017   192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   8  138    0.638019   192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   9  138    0.638019   192.168.2.1      ->  192.168.1.1      48 CS6  UDP
  10  138    0.641009   192.168.1.1      ->  192.168.2.1      48 CS6  UDP
  11  138    0.655016   192.168.1.1      ->  192.168.2.1      48 CS6  UDP
```

提取转储并从路由器导出pcap文件后，可以使用wireshark查看数据包的更多信息。



在发送的第一个IKE_SA_INIT Exchange数据包的Internet Protocol部分上，找到UDP数据包的源地址和目的地址。在用户数据报协议(User Datagram Protocol)部分中，显示使用的端口、互联网安全关联和密钥管理协议(Internet Security Association and Key Management Protocol)部分显示协议的版本、所交换的消息类型、设备的角色以及创建的SPI。收集IKEv2调试时，调试日志中会显示相同的信息。





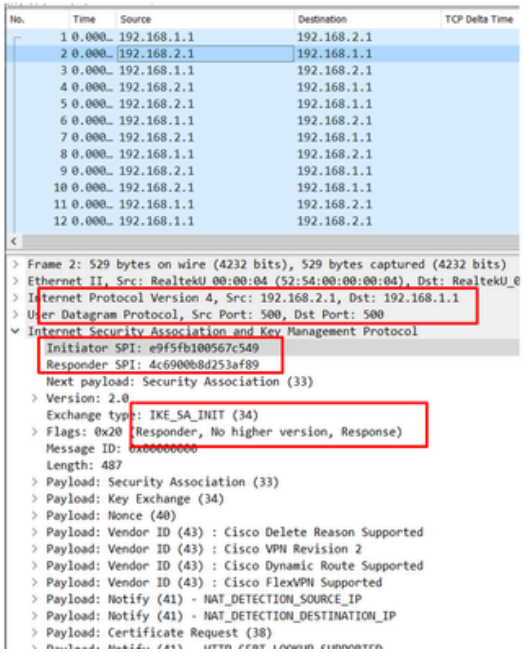
Unencrypted!

IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 0000000000000000
Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)

Debug crypto ikev2
Debug crypto ipsec

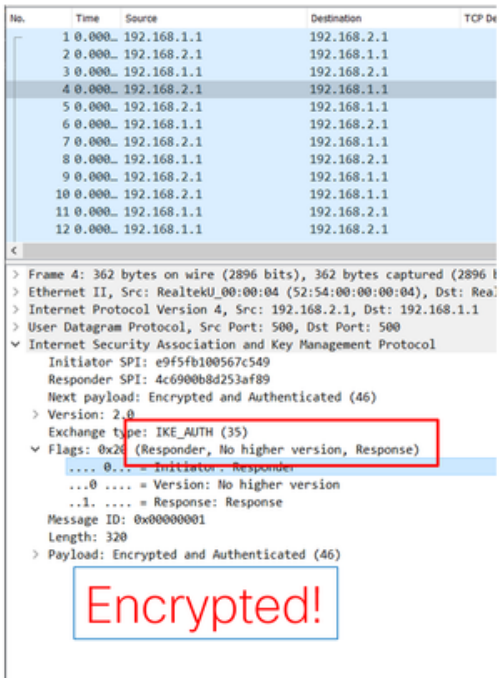
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

Unencrypted!



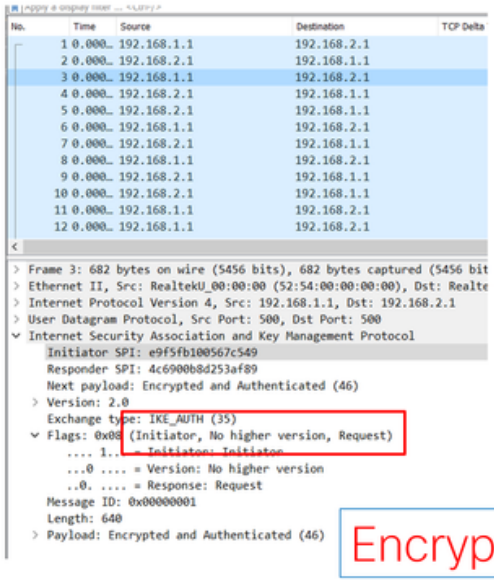
发生IKE_AUTH交换协商时，会加密负载，但可以看到一些有关协商的信息，例如以前创建的SPI和正在进行的事务类型。

IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE



Encrypted!

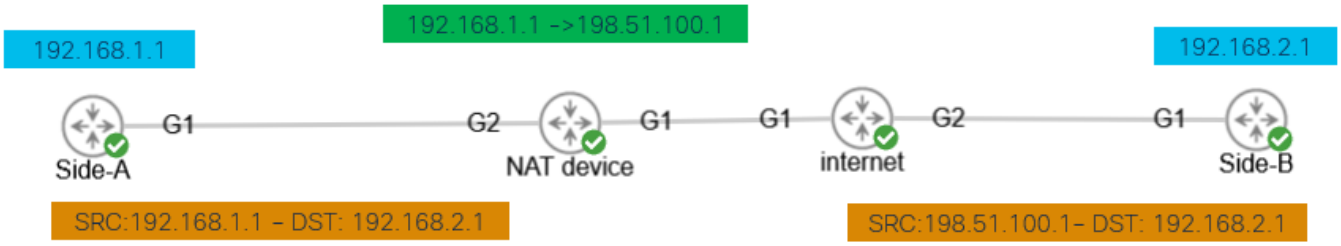
收到最后一个IKE_AUTH Exchange数据包后，隧道协商完成。



Encrypted!

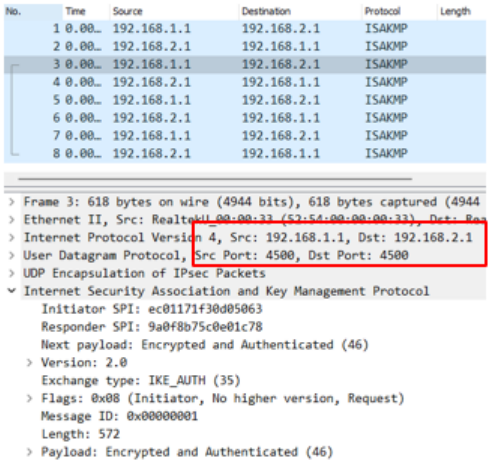
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

NAT处于中间状态时的事务处理



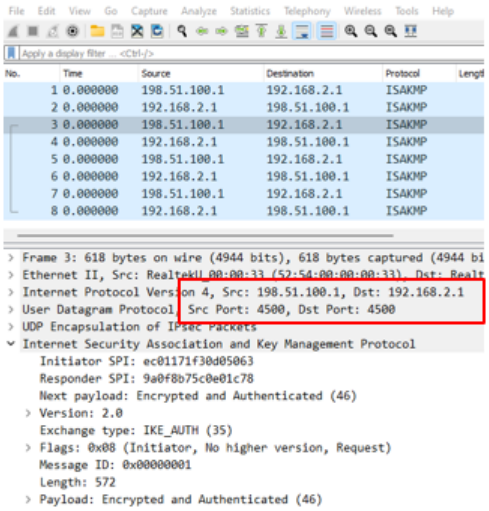
Nat-transversal是进行隧道协商时可以看到的另一项功能。如果中间设备选择用于隧道的一个或两个地址，则在协商第2阶段（IKE_AUTH交换）时，设备会将UDP端口从500更改为4500。

捕获在A侧：



IKEv2:(SESSION ID = 10,SA ID = 1):Received Packet [From 192.168.1.1:4500/To 192.168.2.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
.....
IKEv2:(SESSION ID = 10,SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SESSION ID = 10,SA ID = 1):Checking NAT discovery
IKEv2:(SESSION ID = 10,SA ID = 1):NAT INSIDE found
IKEv2:(SESSION ID = 10,SA ID = 1):NAT detected float to init port 4500, resp port 4500

捕获在B侧：




```
IKEv2:(SESSION ID = 11,SA ID = 1):Sending Packet [To
192.168.2.1:4500/From 198.51.100.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
```

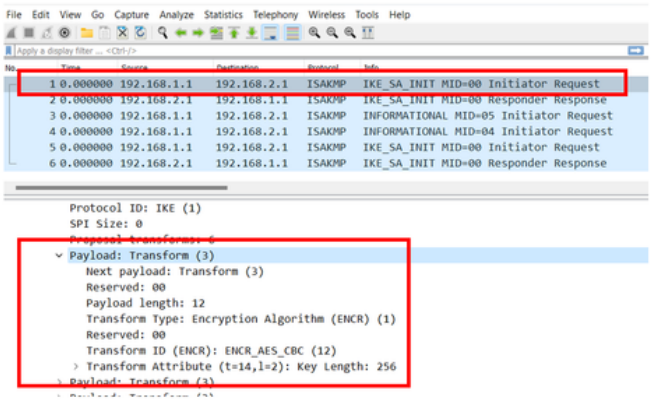
常见控制平面问题

可能会有影响隧道协商的本地或外部因素，也可以通过捕获进行识别。以下场景最为常见。

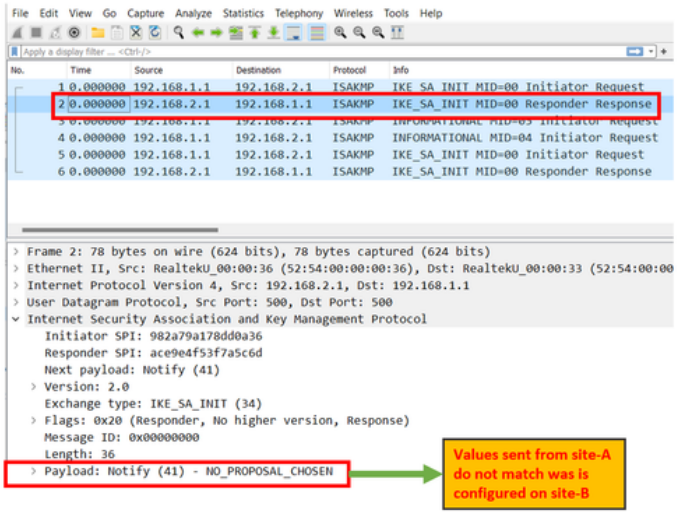
配置不匹配

此场景可以通过查看每个设备阶段1和阶段2配置来解决。但是，可能会出现无法访问远程端的情况。通过确定第1阶段或第2阶段数据包中发送了NO_PROPOSAL_CHOSEN的设备，捕获帮助。该响应表示配置可能存在问题，需要调整哪个阶段。

Side-A



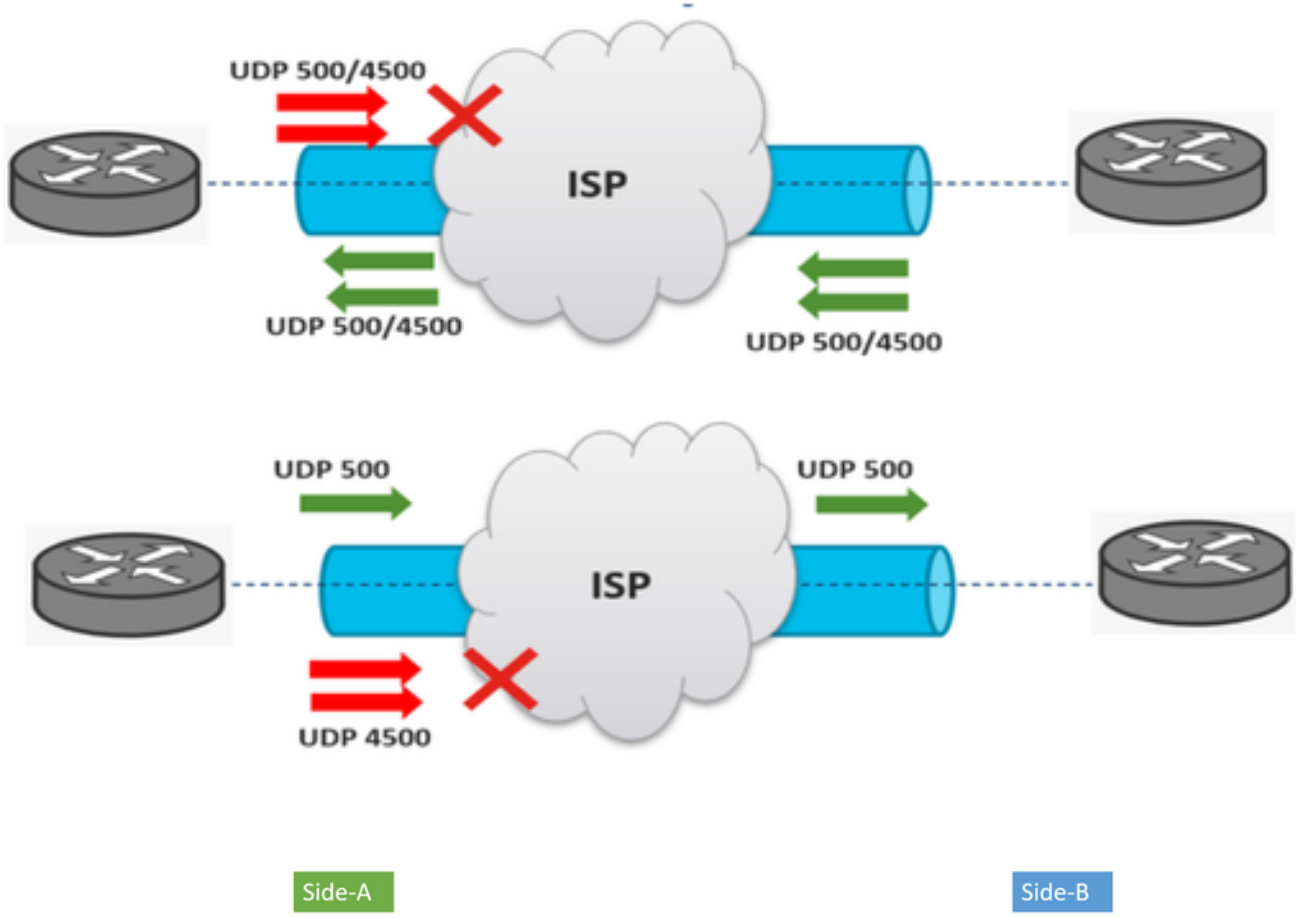
Side-B



重新传输

IPSec隧道协商可能会失败，因为协商数据包在终端设备之间的路径上被丢弃。丢弃的数据包可以是第1阶段或第2阶段数据包。在这种情况下，预期收到响应数据包的设备将重新传输最后一个数据包，如果尝试了5次后没有响应，则隧道会结束并从开始处重新启动。

通过识别可能阻止流量的内容以及流量受影响的方向，在隧道每一端进行捕获会有所帮助。



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
3	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response
4	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
5	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
6	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
7	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
8	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
9	0.000000	192.168.1.1	192.168.2.1	ISAKMP	IKE_SA_INIT MID=00 Responder Response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
2	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
3	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request
4	0.000000	192.168.2.1	192.168.1.1	ISAKMP	IKE_SA_INIT MID=00 Initiator Request

A device or service in between is blocking UDP packets that come from side-A

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）。