验证并识别SD-WAN中WAN的数据包丢失

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 背景 <u>故障排除过程</u> <u>做述流程</u> 使用DSCP标记所需的流量 使用嵌入式捕获捕获捕获流量</u> 通过Wireshark进行分析 <u>按ESP序列过滤所需流量</u> 相关信息

简介

本文档介绍当流量在WAN上丢失但在SD-WAN Edge上未发现丢包时,如何识别和收集数据。

先决条件

要求

Cisco 建议您了解以下主题:

- •思科软件定义的广域网(SD-WAN)
- •嵌入式数据包捕获或vManage数据包捕获
- Wireshark
- Microsoft Excel

使用的组件

本文档中的信息基于以下软件和硬件版本:

- C8000V版本17.03.04
- vManage版本20.3.4
- Wireshark版本2.6.3

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

为了帮助解决此难题,本文档中介绍的步骤说明如何使用差分服务代码点(DSCP)标记特定流量,以 帮助识别所需的数据包。DSCP可用于标识流量,因为此值从内部数据包报头复制到IPsec报头。确 定所需的数据包后,它将显示如何匹配两个WAN捕获中的流量以确保流量从源流向目标。

两个单路由器站点用于演示此故障排除技术。在本例中,从10.0.0.10到10.0.2.10的ICMP流量形式 为100次ping,如图所示。本示例没有丢失,但在发生丢失以识别丢失的情况下也使用相同的故障排 除技术。



故障排除过程

概述流程

- 1. 对于通过WAN跟踪的流量,需要使用访问列表(ACL)(或集中策略)将流量标记为某些未使用 的DSCP值。在本示例中,使用DSCP 27。
- 2. 标记流量后,使用嵌入式数据包捕获功能捕获源路由器和目标路由器的传输接口上的数据包。

注意:虽然有5MB的数据或5分钟的运行时限制,但也可使用vManage数据包捕获。

- 1. 捕获捕获后,在Wireshark中打开这些捕获以进行查看。
- 2. 该过滤器在Wireshark中应用,以显示需要的数据包,然后对其进行比较。
- 3. Microsoft Excel用于大型捕获,以确保准确性。

使用DSCP标记所需的流量

在源路由器上配置访问列表(如本示例中的cEdge1),并将其应用于路由器配置的SD-WAN部分的 接口,如下所示。

应用可选计数器以验证流量是否按预期到达策略。这可以通过命令show sdwan policy access-list-counters来检查。

policy access-list mark_dscp_27 sequence 10 match source-ip 10.0.0.10/32 destination-ip 10.0.2.10/32

```
!
action accept
count MARK_DSCP_27_COUNT (optional counter to verify packets that hit the policy)
set
dscp 27
!
!
default-action accept
sdwan
interface GigabitEthernet3
```

access-list mark_dscp_27 in

使用嵌入式捕获捕获捕获流量

注:如何在Cisco IOS XE中配置嵌入式数据包捕获,以捕获穿越广域网的加密数据包,请导航至<u>Cisco IOS和Cisco IOS XE的嵌入式数据包捕获(Embedded Packet Capture for Cisco</u> IOS and Cisco IOS XE)配置示例

注:必须使用ACL来限制WAN上的EPC,因为EPC的PPS速率限制可能超过1000。

示例

在cEdge1和cEdge3上配置了ACL,因为在本例中只检查从源到目的地的方向的流量。

注:WAN IP地址用于过滤捕获。有多个输出可用于标识流量所采用的路径,以便为ACL过滤器 标识正确的WAN IP。可用于生成此输出的命令是**show sdwan app-fwd cflowd flows**和**show** sdwan policy service path。请导航到<u>条件数据包跟踪</u>以了解调试条件。

ip access-list extended CAP-Filter 10 permit ip host 192.168.23.149 host 192.168.28.240 此时,两个路由器上都会启动捕获,并在重叠网络上发送100次ping。

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms 在从两台路由器停止捕获并收集捕获信息后,需要在Wireshark中打开捕获信息才能查看捕获信息。

通过Wireshark进行分析

在Wireshark中打开cEdge1捕获后,您会发现所有流量都经过加密,因此很难分辨出哪些数据包是 发送的ping。

Ő	Apply a display filter <ctrl-></ctrl->	1 III - I	1 1 1 1 1 1 1 1 1	***							
	lo. Time	Source	Destination	Protocol Length	ESP Sequence	Differentiated Services Codepo	nt Source Port	t Destination Port	Sequence Number	Info	
	1 0.000000	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	2 0.563966	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 - 12407 Len=126	
	3 0.903996	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 - 12407 Len=133	
	4 1.428978	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	5 1.896993	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	6 2.417977	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 - 12407 Len=126	
	7 2.792958	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	8 3.323973	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	9 3.781957	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 - 12407 Len=133	
	10 4.145988	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	11 4.769949	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	12 4.981995	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	13 5.722954	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	14 5.970994	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	15 6.532961	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 - 12407 Len=133	
	16 6.949999	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	17 7.348980	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	18 7.923999	192.168.23.149	192.168.28.240	UOP	168	Class Selector 6				12386 + 12407 Len=126	
	19 8,193990	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	20 8,774953	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	21 9.111993	192.168.23.149	192.168.28.240	UOP	175	Class Selector 6				12386 + 12407 Len=133	
	22 9.653957	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	23 10.082988	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	24 10.564957	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	25 10.949999	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	26 11.416970	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	27 11.937991	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	28 12.400964	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	29 12.836998	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	30 13.266984	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12487 Len=126	
	31 13.779958	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	32 14.171988	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12487 Len=134	
	33 14.173986	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	34 14.174978	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	35 14.175985	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	36 14.176977	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	37 14.176977	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	38 14.178991	192.168.23.149	192.168.28.240	UOP	176	Default				12386 + 12407 Len=134	

使用显示过滤器ip.dsfield.dscp == 27过滤此捕获,在屏幕底部只显示100个数据包,并且显示 DSCP列值全部显示27。

The Source Detenden Protect Leg Sequence Offerentiated Services Codegoot pare for 1 Destination Port 45 55 443 55 443 55 443 55 443 55 443 55 443 55 443 55 443 55 445 55 445 55 445 55 445 55 445 55 445 55 445 55 445 55 445 55 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445 52 445	eganor Number Prif 2286 + 12287 / Lenn 134 1286 + 12497 / Lenn 134
451 55.44983 192.146.23.240 192.146.23.240 100 176 27 451 55.44986 192.146.23.240 100 176 27 453 55.44986 192.146.23.240 100 176 27 453 55.44986 192.146.23.240 100 176 27 453 55.44986 192.146.23.240 100 176 27 453 55.44986 192.146.23.240 100 176 27 455 55.45986 192.146.23.240 100 176 27 455 55.45986 192.146.23.240 100 176 27 455 55.45986 192.146.23.240 100 176 27 455 55.45986 192.146.23.240 100 176 27 455 54.69976 192.146.23.240 100 176 27 464 55.46976 192.146.23.240 100 176 27 464 55.46976 192.146.23.240 100 176 27 464 55.46971 192.146.23.240 <th>12366 - 12407 Lem-134 12366 - 12407 Lem-134</th>	12366 - 12407 Lem-134 12366 - 12407 Lem-134
422 55.44976 192.148.23.149 192.148	12366 - 12407 (cm=134 12366 - 12407 (cm=134
433 55.44896 192.146.23.149 192.146.33.248 UP 176 27 445 55.44895 192.146.23.149 192.146.33.248 UP 176 27 457 55.45997 192.146.23.149 192.146.33.248 UP 176 27 458 55.45997 192.146.23.149 192.146.33.248 UP 176 27 468 55.45997 192.146.23.149 192.146.33.248 UP 176 27 469 55.46991 192.146.23.149 192.146.33.248 UP 176 27 479 55.47981 192.146.23.149 192.146.33.248 UP 176 27 479 55.44991 192.146.33.149 192.146.33.248 UP 176 27 489 55.54997 192.146.33.149 192.146.33.248 UP 176 27 489 55.54997 192.146.33.149 192.146.33.248 UP 176 27 489 55.54997 192.146.33.149 192.146.33.248 UP 176 27 499 55.44911 192.146.33.149 192.146.33.248 UP 17	12366 + 12407 (cm=134 12366 + 12407 (cm=134
445 45.459905 192.146.2.3.149 192.166.3.2.340 UOP 176 27 455 55.45905 49 192.146.2.3.149 192.166.3.2.40 UOP 176 27 455 55.45905 49 192.146.2.3.149 192.166.3.2.40 UOP 176 27 458 55.45905 49 192.146.2.3.149 192.166.3.2.40 UOP 176 27 458 55.45905 49 192.146.2.3.149 192.168.3.2.40 UOP 176 27 458 55.45905 49 192.146.2.3.149 192.168.3.2.40 UOP 176 27 458 55.45905 49 192.146.2.3.149 192.168.3.2.40 UOP 176 27 463 55.46907 192.146.3.149 192.168.3.2.40 UOP 176 27 464 55.46907 192.146.3.149 192.168.3.2.40 UOP 176 27 464 55.46907 192.146.3.149 192.168.3.2.40 UOP 176 27 465 55.46907 192.146.3.149 192.168.3.2.40 UOP 176 27 465 55.46907 192.146.3.149 192.168.3.2.40 UOP 176 27 475 55.47907 192.146.3.149 192.168.3.2.40 UOP 176 27 479 55.47907 192.146.3.149 192.168.3.2.40 <t< td=""><td>12366 - 12407 (cm=134 12366 - 12407 (cm=134</td></t<>	12366 - 12407 (cm=134 12366 - 12407 (cm=134
455 55.45804 192.146.32.149 192.146.32.149 192.146.32.149 465 55.45804 192.146.32.149 192.146.32.149 192.146.32.149 467 55.45807 192.146.32.149 192.146.32.149 192.146.32.149 467 55.45807 192.146.32.149 192.146.32.149 192.146.32.149 467 55.45807 192.146.32.149 192.146.32.149 192.146.32.149 468 55.458075 192.146.32.149 192.146.32.149 192.146.32.149 468 55.458075 192.146.32.149 192.146.32.149 192.146.32.149 469 55.468075 192.146.32.149 192.146.32.149 192.146.32.149 469 192.146.32.149 192.146.32.149 192.146.32.149 192.146.32.149 469 192.146.32.149 192.146.32.149 192.146.32.149 192.146.32.149 479 55.46971 192.146.32.149 192.146.32.149 192.146.32.149 479 55.46971 192.146.32.149 192.146.32.149 192.146.32.149 479 55.46971 192.146.32.149 192.146.32.149 192.146.32.149 479 55.46	12366 - 12407 (em=134 12386 - 12407 (em=134
446 55.49403 192.146.33.240 100 176 27 448 55.49403 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 448 55.4907 192.146.33.240 100 176 27 445 55.4907 192.146.33.240 100 176 27 445 55.4907 192.146.33.240 100 176 27 447 55.4908 192.146.33.240 100 176 27 447 55.49091 192.146.33.240 100 176 27 449 55.49071 192.146.33.240 100 176 27 449 55.49071 192	12366 + 12407 (cm=134 12366 + 12407 (cm=134
477 55.4997 192.146.32.3.49 192.146.33.48 UOP 176 27 489 55.45977 192.146.33.48 192.146.33.48 UOP 176 27 489 55.45977 192.146.33.48 192.146.33.48 UOP 176 27 489 55.45977 192.146.33.48 192.146.33.48 UOP 176 27 440 55.45978 192.146.33.48 UOP 176 27 442 55.44995 192.146.33.48 UOP 176 27 444 55.44997 192.146.33.48 UOP 176 27 444 55.44997 192.146.33.48 UOP 176 27 444 55.44997 192.146.33.48 UOP 176 27 445 55.44997.1 192.146.33.48 UOP 176 27 446 55.44997.1 192.146.33.48 UOP 176 27 447 55.47997.1 192.146.33.48 UOP 176 27 477 55.47997.1 192.146.33.48 UOP 176 27 477 55.47997.1 192.146.33.48 UOP 176 27 475 55.44997.1 192.146.3.	12366 - 12407 (em=134 12386 - 12407 (em=134 12286 - 12407 (em=134 12286 - 12407 (em=134 12386 - 12407 (em=134 12386 - 12407 (em=134 12386 - 12407 (em=134
448 55.45097 192.146.3.3.46 102.146.3.3.46 UCP 176 27 449 55.45097 192.146.3.3.46 102.146.3.3.46 UCP 176 27 449 55.45097 192.146.3.3.46 102.146.3.3.46 UCP 176 27 440 55.45097 192.146.3.3.46 102.146.3.3.46 UCP 176 27 440 55.45097 192.146.3.3.48 102.146.3.3.48 UCP 176 27 442 55.45097 192.146.3.3.49 102.146.3.3.48 UCP 176 27 445 55.45097 192.146.3.3.49 102.146.3.3.48 UCP 176 27 445 55.45097 192.146.3.3.49 102.146.3.3.48 UCP 176 27 445 55.47097 192.146.3.3.49 102.146.3.3.48 UCP 176 27 447 55.47096 192.146.3.3.49 192.146.3.3.48 UCP 176 27 449 55.472097 192.146.3.3.49 192.146.3.3.48 UCP 176 27 449 55.472097 192.146.3.3.49 192.146.3.3.48 UCP 176 27 471 55.472097 192.146.3.3.49 192.146.3.3.48 UCP 176 27 473 55.47090 192.146.3.3.49 192.146.3.3.48 UCP	12366 - 12407 (cm=134 12366 - 12407 (cm=134
499 55.4597 192.148.33.149 192.148.33.248 UOP 176 27 440 55.4597 192.148.33.248 UOP 176 27 441 55.4597 192.148.33.248 UOP 176 27 441 55.4597 192.148.33.248 UOP 176 27 441 55.4597 192.148.33.248 UOP 176 27 444 55.44971 192.148.33.248 UOP 176 27 444 55.44971 192.148.33.248 UOP 176 27 445 55.44971 192.148.33.248 UOP 176 27 446 55.44971 192.148.33.248 UOP 176 27 446 55.449714 192.148.33.248 UOP 176 27 447 55.449714 192.148.33.248 UOP 176 27 449 55.479754 192.148.33.248 UOP 176 27 473 54.47964 192.148.33.248 UOP 176 27 473 54.47964 192.148.33.248	12366 - 12407 (cm=134 12386 - 12407 (cm=134 12386 - 12407 (cm=134 12386 - 12407 (cm=134 12386 - 12407 (cm=134 12286 - 12407 (cm=134 12286 - 12407 (cm=134 12386 - 12407 (cm=134 12386 - 12407 (cm=134 12386 - 12407 (cm=134
440 55.45897 192.148.33.149 192.148.33.248 UOP 176 27 442 55.45895 192.148.33.148 192.148.33.248 UOP 176 27 442 55.45895 192.148.33.148 192.148.33.248 UOP 176 27 442 55.45895 192.148.33.148 192.148.33.248 UOP 176 27 445 55.45995 192.148.33.148 192.148.33.248 UOP 176 27 445 55.45995 192.148.33.148 192.148.33.248 UOP 176 27 446 55.47995 192.148.33.248 UOP 176 27 447 55.47995 192.148.33.248 UOP 176 27 449 55.47995 192.148.33.248 UOP 176 27 471 55.47995 192.148.33.248 UOP 176 27 473 55.47995 192.148.33.248 UOP 176 27 473 55.47995 192.148.33.248 UOP 176 27 473 55.48199 192.148.33.248 </td <td>12366 - 12407 (cm=134 12366 - 12407 (cm=134</td>	12366 - 12407 (cm=134 12366 - 12407 (cm=134
441 55.43966 192.148.33.249 192.148.33.248 UOP 176 27 443 55.44975 192.148.33.248 UOP 176 27 443 55.44975 192.148.33.248 UOP 176 27 443 55.44975 192.148.33.248 UOP 176 27 445 55.44975 192.148.33.248 UOP 176 27 445 55.44975 192.148.33.248 UOP 176 27 445 55.44976 192.148.33.248 UOP 176 27 447 55.449765 192.148.33.248 UOP 176 27 447 55.449766 192.148.33.248 UOP 176 27 447 55.449766 192.148.33.248 UOP 176 27 447 55.449766 192.148.33.248 UOP 176 27 447 55.44986 192.148.33.248 UOP 176 27 447 55.44997 192.148.33.248 UOP 176 27 447 55.44997 192.148.33.248 UOP 176 27 447 55.44997 192.148.33.248 UOP 176 27 <	12366 + 12407 (cm=134 12366 + 12407 (cm=134
442 55.46995 192.146.3.3.49 192.146.3.3.49 UOP 176 27 443 55.46995 492.192.146.3.3.49 192.146.3.3.49 UOP 176 27 444 55.46997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 444 55.46997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 445 55.46997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 447 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 447 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 449 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 479 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 473 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 473 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 473 55.47997 192.146.3.3.49 192.146.3.3.49 UOP 176 27 474 55.44996 192.146.3.3.49 192.146.3.3.49 UOP 176 27 475 55.44997 192.146.3.3.49 192.146.3.3.49 UOP	12366 - 12407 (em=134 12366 - 12407 (em=134
443 55.4697 192.146.33.149 192.146.33.249 UDP 176 27 445 55.4697 192.146.33.149 192.146.33.249 UDP 176 27 445 55.4697 192.146.33.149 192.146.33.249 UDP 176 27 447 55.47968 192.146.33.149 192.146.33.249 UDP 178 27 447 55.47968 192.146.33.149 192.146.33.249 UDP 178 27 449 55.47978 192.146.33.149 192.146.33.249 UDP 176 27 477 55.47978 192.146.33.149 192.146.33.249 UDP 176 27 478 55.44978 192.146.33.149 192.146.33.249 UDP 176 27 478 55.54978 1	12366 + 12407 (Lem-134 12366 + 12407 (Lem-134 12366 + 12407 (Lem-134 12366 + 12407 (Lem-134 12366 + 12407 Lem-134 12366 + 12407 Lem-134 12366 + 12407 Lem-134
444 55.46071 192.146.33.240 192.146.33.240 192.146.33.240 192.146.33.240 192.146.33.240 446 55.46071 192.146.33.240 192.146.33.240 192.146.33.240 192 193 446 55.46071 192.146.33.240 192.146.33.240 192 193 27 446 55.46071 192.146.33.240 192.146.33.240 192 193 27 446 55.40716 192.146.33.240 192.146.33.240 192 193 27 449 55.47907 192.146.33.240 192.146.33.240 192 193 27 479 55.47907 192.146.33.240 192.146.33.240 192 192.146.33.240 192 192.146.33.240 192 192.146.33.240 192 192.146.33.240 192 192.146.33.240 192.146.33.240 192 192.146.33.240 192.146.3	12366 - 12407 (em=134 12366 - 12407 (em=134
445 55.467961 192.146.33.249 192.146.33.249 100 176 27 445 55.467961 192.146.33.249 100 176 27 447 55.47966 192.146.33.249 100 176 27 447 55.47966 192.146.33.249 100 176 27 447 55.47966 192.146.33.249 100 176 27 447 55.47966 192.146.33.249 100 176 27 449 55.479767 192.146.33.249 100 176 27 449 55.479767 192.146.33.249 100 176 27 474 55.448976 192.146.33.249 100 176 27 474 55.448976 192.146.33.249 100 176 27 474 55.448976 192.146.33.249 100 176 27 474 55.448976 192.146.33.249 100 176 27 474 55.448976 192.146.33.249 100 176 27 475 55.448976 192.146.33.249 100 176 27 478 55.44976 192.146.3.3.49 192.146.3.3.49 100 176 <td>12366 + 12407 (em-134 12366 + 12407 (em-134 12366 + 12407 (em-134 12366 + 12407 (em-134 12368 + 12407 (em-134</td>	12366 + 12407 (em-134 12366 + 12407 (em-134 12366 + 12407 (em-134 12366 + 12407 (em-134 12368 + 12407 (em-134
446 55.46906; 192.146.33.240	12366 + 12407 Len-134 12386 + 12407 Len-134 12386 + 12407 Len-134 12386 + 12407 Len-134
447 35.47996 192.146.33.249 132.146.33.249 100 176 27 448 55.47297 192.146.33.249 132.146.33.249 100 176 27 449 55.47297 192.146.33.249 132.146.33.249 100 176 27 449 55.47297 192.146.33.249 132.146.33.249 100 176 27 449 55.47297 192.146.33.249 132.146.33.249 100 176 27 471 55.47397 192.146.33.149 132.146.33.249 100 176 27 471 55.44897 192.146.33.149 132.146.33.249 100 176 27 474 55.44897 192.146.33.149 132.146.33.249 100 176 27 474 55.44897 192.146.33.149 132.146.33.249 100 176 27 474 55.44897 192.146.33.149 132.146.33.249 100 176 27 475 55.44897 192.146.33.149 132.146.33.249 100 176 27 478 55.44897 192.146.33.149 132.146.33.249 100 176 27 478 55.44897 192.146.33.149 132.146.33.249 100 176 27 481 55.51999 192.146.3.3.149 132.146.33.249 100 <t< td=""><td>12386 = 12407 Len=134 12386 = 12407 Len=134 12386 = 12407 Len=134</td></t<>	12386 = 12407 Len=134 12386 = 12407 Len=134 12386 = 12407 Len=134
448 55.47297 192.146.33.249 192.146.33.249 192.146.33.249 192.146.33.249 449 55.47296 192.146.33.249 192.146.33.249 192 193.149 449 55.47296 192.146.33.249 192.146.33.249 192 193.149 479 55.47296 192.146.33.249 192.146.33.249 192 193.149 479 55.47296 192.146.33.249 192.146.33.249 192 193.149 473 55.47296 192.146.33.249 192.146.33.249 192 193.149 473 55.47296 192.146.33.249 193.146.33.249 193.146.32.244 193.146.32	12386 + 12407 Len=134 12386 + 12407 Len=134
449 55.7296 192.148.3.3.49 192.148.3.8.248 UDP 176 27 471 55.7296 192.148.3.3.49 192.148.3.8.248 UDP 176 27 471 55.7496 192.148.3.3.49 192.148.3.8.248 UDP 176 27 472 55.7496 192.148.3.3.49 192.148.3.8.248 UDP 176 27 475 55.4497 192.148.3.3.49 192.148.3.8.248 UDP 176 27 476 55.4497 192.148.3.3.49 192.148.3.8.248 UDP 176 27 476 55.4497 192.148.3.3.49 192.148.3.8.248 UDP 176 27 476 55.4497 192.148.3.3.49 192.148.3.8.248 UDP 176 27 478 55.4997 192.148.3.3.49 192.148.3.8.248 UDP 176 27 481 55.5989 192.148.3.3.49 192.148.3.8.49 UDP 176 27 481 55.5989 192.148.3.3.49 192.148.3.498 UDP 176 27 481 55.5989 192.148.3.3.49 192.148.3.498 UDP 176 27 481 55.5989 192.148.3.3.49 192.148.3.498 UDP 176 27 481 55.5989 192.148.3.3.	12386 + 12407 Len=134
40° 55.474966 192.148.33.149 192.148.33.249 100° 176 27 472 55.47906 192.148.33.149 192.148.38.248 100° 176 27 472 55.47066 192.148.33.149 192.148.38.248 100° 176 27 474 55.44096 192.148.33.149 192.148.38.248 100° 176 27 474 55.44096 192.148.33.149 192.148.38.248 100° 176 27 475 55.44096 192.148.33.149 192.148.38.248 100° 176 27 476 55.44097 192.148.33.149 192.148.38.248 100° 176 27 478 55.44096 192.148.33.149 192.148.38.248 100° 176 27 481 55.51096 193.148.31.149 192.148.38.248 100° 176 27 481 55.51096 193.148.33.149 192.148.38.248 100° 176 27 481 55.51096 192.148.33.149 192.148.38.248 100° 176 27 485 55.53097 192.148.33.149 1	
471 55.47997 192.146.33.249	12386 * 12407 Len=134
4/2 35.47005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 4/2 35.47005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 4/3 55.44005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 4/3 55.44005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 4/3 55.44005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 4/3 55.44005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 4/3 55.44005 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 193.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 193.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 193.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 193.148.33.149 192.148.33.149 192.1	12386 + 12407 Len=134
473 55.74995 192.148.33.149 192.148.33.249 UDP 176 27 475 55.44956 192.148.33.149 192.148.33.249 UDP 176 27 475 55.44956 192.148.33.149 192.148.33.249 UDP 176 27 478 55.44957 192.148.33.149 192.148.33.248 UDP 176 27 478 55.44957 192.148.33.149 192.148.33.248 UDP 176 27 478 55.44956 192.148.33.149 192.148.33.248 UDP 176 27 478 55.44956 192.148.33.149 192.148.33.248 UDP 176 27 448 55.51959 192.148.33.149 192.148.33.248 UDP 176 27 442 55.51959 192.148.33.149 192.148.33.248 UDP 176 27 445 55.51959 193.148.33.149 192.148.33.248 UDP 176 27 445 55.51959 193.148.33.149 192.148.33.448 UDP 176 27 455 55.51959 193.148.33.149 193.148.39.1488 UDP 176 27 455 55.51959 193.148.33.149 193.148.39.1488 UDP 176 27 455 55.51959 193.148.33.149 193.148.39.1488 UDP 176 7 455 75.57	12386 + 12407 Len=134
474 55.448995 192.146.33.149 122.146.38.248 UDP 176 27 476 55.448975 192.146.33.149 122.146.38.248 UDP 176 27 476 55.448975 192.146.33.149 122.146.38.248 UDP 176 27 478 55.448975 192.146.33.149 122.146.38.248 UDP 176 27 478 55.48975 192.148.33.149 122.146.38.248 UDP 176 27 478 55.48975 192.148.33.149 122.146.38.248 UDP 176 27 448 55.49165 122.148.33.149 122.146.38.248 UDP 176 27 448 55.49165 120.148.33.149 122.146.38.248 UDP 176 27 448 55.51905 120.148.33.149 122.146.38.248 UDP 176 27 448 55.51905 120.148.33.149 122.146.38.248 UDP 176 27 448 55.51905 120.148.33.149 122.146.38.248 UDP 176 27 447 55.51905 120.148.33.149 122.146.38.248 UDP 176 27 445 55.51907 120.148.33.149 122.146.38.248 UDP 176 27 445 55.51907 120.148.33.149 122.146.38.248 UDP 176 27 445 55.51907 120.148.33.149 122.148.38.248 UDP 176 27 445 55.51907 120.148.33.149 122.148.38.248 UDP 176 27 445 55.51907 120.148.33.149 122.148.38.248 UDP 176 27 447 55.51906 120.148.33.149 122.148.38.248 UDP 176 27 448 55.51906 120.148.33.149 120.148.38.248 UDP 176 27 449 55.	12386 → 12407 Len=134
475 55.44309 192.146.33.490	12386 + 12407 Len=134
476 55.448975 192.146.33.249 192.146.33.248 UDP 176 27 478 55.448975 192.146.33.248 UDP 176 27 478 55.448975 192.146.33.248 UDP 176 27 448 55.41966 192.146.33.248 UDP 176 27 448 55.41966 192.146.33.248 UDP 176 27 448 55.51966 192.146.33.248 UDP 176 27 449 55.51966 192.146.33.149 192.146.33.248 UDP 176 27 449 55.51966 192.146.33.149 192.146.33.248 UDP 176 27 449 55.51966 192.146.33.149 192.146.33.148 UDP 176 27 449 55.51966 192.146.33.149 192.148.33.148 UDP 176 27 449 55.51966 192.146.33.149 192.148.31.488 UDP 176 27 449 55.51966 192.146.31.149 192.148.31.488 UDP 176 27 449 55.51966 192.146.31.149 192.148.31.488 UDP 176 27 449 55.51966 192.146.31.149 192.148.31.488 UDP 176 192.	12386 → 12407 Len=134
477 55.45996 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 479 55 45976 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 479 55 45976 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 479 55 53976 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 415 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 415 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 415 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 416 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 416 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 416 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 416 55.51997 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 192.148.33.149 416 55.51997	12386 + 12407 Len=134
478 55.44996 192.164.33.249 192.164.33.249 100 176 27 449 55.44996 192.164.33.248 100 176 27 449 55.49965 192.164.33.248 100 176 27 449 55.49965 192.164.33.248 100 176 27 449 55.49965 192.164.33.484 100 176 27 442 55.19965 192.164.33.484 100 176 27 442 55.19965 192.164.33.484 100 176 27 445 55.19965 192.164.33.484 100 176 27 445 55.19965 192.164.33.484 100 176 27 445 55.19965 192.164.33.149 192.164.33.494 100 176 27 445 55.19965 193.164.33.149 192.164.33.494 100 176 27 447 55.19965 193.164.33.149 192.164.33.494 100 176 27 449 55.29966 193.164.33.149 192.164.33.494 100 <	12386 + 12407 Len=134
479 55.488973 192.168.23.249 192.168.23.249 100 176 27 441 55.488973 192.168.23.249 192.168.23.249 100 176 27 441 55.58965 192.168.23.249 100 176 27 442 55.51965 192.168.23.249 100 176 27 443 55.51965 192.168.23.249 100 176 27 443 55.51965 192.168.23.249 100 176 27 445 55.51967 192.168.23.249 100 176 27 445 55.51967 192.168.23.249 100 176 27 445 55.51967 192.168.23.249 100 176 27 445 55.51967 192.168.23.249 100 176 27 447 55.51967 192.168.23.249 100 176 27 447 55.51967 192.168.23.249 100 176 27 448 55.51967 192.168.23.249 100 176 27 448 55.51967 192.168.23.249 100 176 27 449 55.52967 192.168.23.249 100 176 27	12386 + 12407 Len=134
440 55.04950 192.164.23.249 440 55.04950 192.164.23.249 442 55.04950 192.164.23.249 442 55.04950 192.164.23.240 442 55.04950 192.164.23.240 445 55.01950 192.164.23.240 445 55.01950 192.164.23.240 445 55.01950 192.164.23.240 445 55.01950 192.164.23.240 447 55.01950 192	12386 + 12407 Len=134
411 55.00005 1 92.164.23.149 122.164.28.240 UDP 176 27 423 55.10005 192.164.23.149 132.164.28.240 UDP 176 27 443 55.1006 192.164.23.149 132.164.28.240 UDP 176 27 445 55.1007 132.164.23.149 132.164.28.240 UDP 176 27 445 55.1007 132.164.23.149 132.164.28.240 UDP 176 27 445 55.1007 132.164.23.149 132.164.28.240 UDP 176 27 447 55.17163 132.164.23.249 132.164.28.240 UDP 176 27 447 55.17163 132.164.23.249 132.164.28.240 UDP 176 27 447 55.17163 132.164.23.249 132.164.28.240 UDP 176 27 448 55.52097 132.164.23.149 132.164.28.240 UDP 176 27 449 55.52097 132.164.23.149 132.164.28.240 UDP 176 27 449 55.52095 132.164.31.149 132.164.38.240 UDP 176 27 449 55.52095 132.164.38.240 UDP 176 27 449 55.52005 132.164.38.240 UDP 176 27 449	12386 + 12407 Len=134
422 35.51895 9 192.146.23.249 122.146.28.248 UDP 176 27 442 35.51895 9 192.146.23.249 UDP 176 27 445 35.51896 192.146.23.249 UDP 176 27 445 35.51897 192.146.23.249 UDP 176 27 446 35.51897 192.146.23.249 UDP 176 27 446 35.51897 192.146.23.249 UDP 176 27 446 35.51897 192.146.23.249 UDP 176 27 447 35.52896 192.146.23.249 UDP 176 27 448 35.52896 192.146.23.249 UDP 176 27 449 35.52896 192.146.23.149 122.146.35.249 UDP 176 27 449 35.52896 192.146.33.149 122.147.349 122.14	12386 + 12407 Len=134
443 35.51366 192.164.23.249 192.164.23.49 102.164.23.249 UDP 176 27 445 35.51367 192.164.23.249 UDP 176 27 445 35.51697 192.164.23.249 UDP 176 27 445 35.51697 192.164.23.249 UDP 176 27 447 35.517163 192.164.23.149 192.164.23.249 UDP 176 27 447 35.517163 192.164.23.149 192.164.23.249 UDP 176 27 447 35.52916 192.164.23.149 192.164.23.249 UDP 176 27 449 35.52916 192.164.23.149 192.164.23.249 UDP 176 27 449 35.52916 192.164.23.149 192.164.23.249 UDP 176 27 449 35.52916 192.164.23.149 192.164.23.249 UDP 176 27 176 bytes on wire (1448 bits), 176 bytes captured (1448 bits)	12386 + 12407 Len=134
444 55.51996 5 192.164.23.249 122.164.28.249 UD9 176 27 445 55.51997 192.164.23.249 UD9 176 27 446 55.51997 192.164.23.249 UD9 176 27 446 55.51997 192.164.23.249 UD9 176 27 447 95.51769 192.164.23.249 UD9 176 27 449 55.52806 192.164.23.249 UD9 176 27 449 55.5880 UD9 176 176 176 176 176 176 176 176 176 176	12386 → 12407 Len=134
455 55.51497 192.164.23.249 122.164.28.248 UDP 176 27 465 55.51497 192.164.23.249 UDP 122.164.28.248 UDP 176 27 447 55.51716 192.164.23.149 192.164.28.248 UDP 176 27 447 55.52956 192.164.23.149 192.164.28.249 UDP 176 27 498 55.52956 192.164.23.149 192.164.28.249 UDP 176 27 195 55466 192.164.23.149 192.164.28.249 UDP 176 27 196 bytes on wire (1448 bits), 176 bytes captured (1448 bits)	12386 + 12407 Len=134
446 55.51697 192.184.33.469 22.184.38.249 UDP 176 27 447 55.51769 192.184.33.491 92.184.38.249 UDP 176 27 448 55.52959 192.184.33.491 92.186.38.249 UDP 176 27 448 55.52959 192.184.33.491 92.186.38.249 UDP 176 27 448 55.52959 192.184.31.491 92.186.38.249 UDP 176 27 448 55.52959 192.184.31.491 92.186.38.249 UDP 176 27 176 bytes on wire (1488 bits), 176 bytes captured (1488 bits)	12386 + 12407 Len=134
427 35.31786 3192.184.23.499 122.184.28.2489 UDP 176 27 4485 55.23956 3192.184.23.149 122.184.28.2489 UDP 176 27 449 55.52466 192.184.23.149 122.184.28.2489 UDP 176 27 155.52466 192.184.23.149 122.184.28.2489 UDP 176 27	12386 + 12407 Len=134
448 55.22975 192.184.31.349 192.186.31.494 USP 175 27 448 55.2296 192.184.31.49 192.186.31.494 USP 175 27 194 55.2296 192.184.31.494 192.186.31.494 USP 175 27 176 bytes on wire (1488 bits), 176 bytes captured (1488 bits)	12386 + 12407 Len=134
489 35.524966 192.184.23.149 192.186.28.440 UGV 176 27	12386 * 12407 Len=134
176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)	12386 * 12487 Len*134
176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)	
I, Src: Whare_64:st:45 (00:50:50:64:st:45), DSt: Whare_64:e2:b7 (00:50:56:64:e2:b7)	
TODODI VETSION 4, STC: SMI.HOB.25.149, USI: SMI.HO.28.249	
ram Protocol, Src Port: 12380, USt Port: 1240/	
altes)	

在广域网中保持DSCP值的一些情况下,可以在目标捕获上使用相同的过滤器。

在其他情况下,这不可能,例如通过公共Internet连接清除DSCP值的情况。

按ESP序列过滤所需流量

无论哪种情况,都可以使用ESP序列号来标识流量。

要查看数据包中的ESP序列号,请右键单击捕获并选择解码,如下所示。

C Profie: Default

Packets: 880 Displayed: 100 11.4%)

			12386
			12386
	Mark/Unmark Packet	Ctrl+M	12386
		current of	12386
	Ignore/Unignore Packet	Ctrl+D	12386
	Set/Unset Time Reference	Ctrl+T	12386
	Time Shift	Ctrl+Shift+T	12386
	Packet Comments	•	12386
	Packet comments		12386
	Edit Resolved Name		12386
			12386
	Apply as Filter	+	12386
	Prepare as Filter	•	12386
	Commention Filter		12386
	Conversation Filter	,	12386
	Colorize Conversation	•	12386
	SCTP	+	12386
	Follow	•	12386
	Follow		12386
	Copy	•	12386
			12386
	Protocol Preferences	•	12386
	Decode As		12386
L			12386
	Show Packet in New Window		12386

选择**Current** field**下**拉菜单,并在该字段中键入**UDPENCAP,**或从下拉列表中选择它。



V	V	ir	es	hai	rk	D	ec	0	d	e	As
٠		••	-			$\boldsymbol{\nu}$	~~	-	-	-	

Field	Value	Туре	Default	Current					
UDP port	12386	Integer, base 10	(none)	(none)					~
				(none) 3GPP2 A11 A21 AC DR ACtrace ADP ADwin ALC AMP					•
+ -	գ. (
					OK	Save	Copy from	Cancel	Help

 \times

完成后选择OK。

📕 Wiresh	ark • De	code As							×
Field	Value	Туре	Default	Current					
UDP port	12386	Integer, base 10	(none)	UDPENCAP					
+ -	ъſ								
		-0							
					ОК	Save	Copy from	Cancel	Help

在Wireshark Packet Details(Wireshark数据包详细信息)部分,展开数据包的**Encapsulating** Security Payload部分,查看ESP Sequence。

11					
	479 55 488973 192 168 23 1	149 192 168 28 240	A FSP	176	
<					
>	Frame 464: 176 bytes on wire (1408 bi	its), 176 bytes captured	(1408 bits)		
>	Ethernet II, Src: VMware_84:af:45 (00	0:50:56:84:af:45), Dst:	VMware_84:e2:b7	(00:50:56:84:e2:b7)	
>	Internet Protocol Version 4, Src: 192	2.168.23.149, Dst: 192.1	68.28.240		
>	User Datagram Protocol, Src Port: 123	386, Dst Port: 12407			
	UDP Encapsulation of IPsec Packets				
Ν	Encapsulating Security Payload				
ľ	ESP SPI: 0X0400010C (67109340)				
	ESP Sequence: 319				

右键点击**ESP Sequence**,然后选择**apply as**列,这样,ESP Sequence就可以视为Wireshark屏幕 顶部的Packet List部分中的一列。

TJJ JJ.TJLJ	H 172.100.23.143	102.100.20.240	6.01
456 55.4			ESP
457 55.4	Expand Subtrees		ESP
458 55.4	Collapse Subtrees		ESP
459 55.4	Expand All		ESP
460 55.4	Collanse All		ESP
461 55.4	compse An		ESP
462 55.	Apply as Column	Ctrl+Shift+I	ESP
463 55.			ESP
464 55.4	Apply as Filter	•	ESP
465 55.4	Prepare as Filter	•	ESP
466 55.4	Conversion Filter		ESP
467 55.4	Conversation Filter	,	ESP
468 55.4	Colorize with Filter	•	ESP
469 55.4	Follow	•	ESP
470 55.4			ESP
471 55.4	Сору	•	ESP
472 55.4			ESP
473 55.4	Show Packet Bytes	Ctrl+Shift+O	ESP
474 55.4	Export Packet Bytes	Ctrl+Shift+X	ESP
Frame 464: 176 bvt	Wiki Protocol Page		08 bits)
Ethernet II, Src:	Filter Field Reference		re 84:e2:b7 (0
Internet Protocol	Protocol Preferences	•	8.240
User Datagram Prot			
UDP Encapsulation	Decode As	Ctrl+Shift+U	
Encapsulating Secu	Go to Linked Packet		
ESP SPT · 0x0400	d Dacket in New	w Window	
ESP Sequence: 31	Show Elliki u Packet in Nel	WWINDOW]

注:cEdge1上数据包的ESP SPI是0x040001dc。这用于目标捕获上的过滤器。

```
> Frame 464: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: VMware_84:af:45 (00:50:56:84:af:45), Dst: VMware_84:e2:b7
> Internet Protocol Version 4, Src: 192.168.23.149, Dst: 192.168.28.240
> User Datagram Protocol, Src Port: 12386, Dst Port: 12407
UDP Encapsulation of IPsec Packets
> Encansulating Security Payload
ESP SPI: 0x040001dc (67109340)
ESP Sequence: 319
```

打开目标捕获,重复上述步骤解码为UDPENCAP,并显示数据包中的ESP序列号。

一旦数据包显示ESP序列号,来自第一个捕获的ESP SPI可用作第二个捕获的过滤器,以仅显示该 SPI中匹配所需流量的流量。

请注意,匹配两个数据包序列号的数据包都标记了DSCP 27。



这种比较可以在Wireshark中手动完成,也可以使用Microsoft Excel进行这种比较。

为了使用Microsoft Excel进行比较,需要对两个捕获进行切片,以便仅包含两个捕获中的数据包。

在源捕获中,第一个相关数据包的ESP序列为306,对应于数据包编号451。

CAP.pcap							_		\times
File Edit Vi	ew Go Capture	Analyze Statistics 1	Telephony Wireless Tools	Help					
	- 📑 🔀 🛅	९ 🗢 🗢 🗟 👔 🎍	📃 📃 🔍 🔍 🔍 🎹						
ip.dsfield.dsc	p == 27								- +
No.	Time	Source	Destination	Protocol	Length	ESP Sequence		Different	^
	451 55.441963	192.168.23.149	192.168.28.240	ESP	176		306	27	
	452 55.445976	192.168.23.149	192.168.28.240	ESP	176		307	27	
	453 55.448966	192.168.23.149	192.168.28.240	ESP	176		308	27	
	454 55.450965	192.168.23.149	192.168.28.240	ESP	176		309	27	
	455 55.452964	192.168.23.149	192.168.28.240	ESP	176		310	27	
	456 55.454963	192.168.23.149	192.168.28.240	ESP	176		311	27	
	457 55.455970	192.168.23.149	192.168.28.240	ESP	176		312	27	
	458 55.456977	192.168.23.149	192.168.28.240	ESP	176		313	27	

源捕获中的最后一个相关数据包的ESP序列为405,数据包编号为550。

					210		
	548 55.608962	192.168.23.149	192.168.28.240	ESP	176	403 27	
	549 55.609969	192.168.23.149	192.168.28.240	ESP	176	404 27	
	550 55.610960	192.168.23.149	192.168.28.240	ESP	176	405 27	
							~
4						>	

在目标捕获中,第一个相关数据包对应于ESP序列306的源捕获,但此捕获中是数据包463。

461 60.522028	192.168.23.149	192.168.28.240	ESP	168	407 Class Se
462 60.715026	192.168.23.149	192.168.28.240	ESP	175	408 Class Se
463 60.999008	192.168.23.149	192.168.28.240	ESP	176	306 27
464 61.003006	192.168.23.149	192.168.28.240	ESP	176	307 27

最后一个相关数据包也包含ESP序列405,它是数据包564。

560 61.165052	192.168.23.149	192.168.28.240	ESP	1/6	403 27
561 61.166043	192.168.23.149	192.168.28.240	ESP	176	404 27
562 61.166043	192.168.23.149	192.168.28.240	ESP	176	405 27
563 61.431029	192.168.23.149	192.168.28.240	ESP	168	409 Class Se
564 61.584021	192.168.23.149	192.168.28.240	ESP	175	410 Class Se

现在,必须对第一个捕获进行切片,使其仅包含相关数据包。

导航到文件>导出数据包分段>作为CSV...

CAP.pcap

File	Edit	View	Go	Capture	Analyze	Sta	tistic	s Telepho	ony V	Vireless	Tools	Help			
	Open Ctrl+O							🕹 📃		00	Q 🎹				
	Open F	ecent				•									
	Merge.							De	stination			Protocol	Length		F
	Import from Hex Dump						149	19	2.168.	28.240)	ESP	cengui	176	
	Close				Ctrl+W		149	19	2.168.	28.240)	ESP		176	
	ciose				current		149	19	2.168.	28.240)	ESP		176	
	Save				Ctrl+S		149	19	2.168.	28.240)	ESP		176	
	Save As	s			Ctrl+Shift+S	5	149	19	2.168.	28.240)	ESP		176	
							149	19	2.168.	28.240)	ESP		176	
	File Set					•	149	19	2.168.	28.240)	ESP		176	
							149	19	2.168.	28.240)	ESP		176	
	Export	Specifie	d Pac	kets			149	19	2.168.	28.240)	ESP		176	
	Export	Packet	Dissec	tions		•		As Plain Te	xt	. 240)	ESP		176	
	Export	Packet	Bvtes.		Ctrl+Shift+)	<		As CSV		. 240		ESP		176	
				-				A		. 240		ESP		176	
	Export	PDUs to	File					As "C" Arra	ays	. 240)	ESP		176	
	Export	TLS Ses	sion K	eys					N.AI	. 240)	ESP		176	
	Export	Objects				•		AS POIVIL A	IVIL	.240)	ESP		176	
	Print Ctrl+P			_		As PDML X	(ML	.240)	ESP		176			
			Ctrl+P			As JSON		.240)	ESP		176			
)	ESP		176				
	Quit Ctrl+Q				149 192.168.28.24)	ESP		176			
-		24		.000902	192.100.	22.	149	19	2.168.	28.240)	ESP		176	
	548 55.608962 192.168.2							192.168.28.240				ESP		176	

选择Captured和Range,在Range字段中键入从第一个相关数据包到最后一个相关数据包的范围。 在File Name(文件名)字段中**输入文**件名,然后单击Save(保存)。

Name Status Date modified No items match your search. Date modified Desktop Image: Status Image: Status Packet Image: Status Image: Status Image: Status Image: Status Image: Status	Save in:	E Desktop		~	G 🦻	📁 对	•		
Desktop Libraries Image: Libraries	Quick access	Name	^ No items r	match your se	Status earch.	()ate m	odified	ł
Libraries This PC Network File name: CAP1_slice	Desktop								
This PC Image: This PC Image: CAP1_slice File name: CAP1_slice Save as type: CSV (Comma Separated Values summary) (*.cs) Cancel Help Packet Range Image: Packet Range Image: All packets Image: Image: All packets Image: Image: All packets Image: Image: All packets Image: Image: Image: Image: All packets Image:	Libraries								
Network File name: CAP1_slice Save as type: CSV (Comma Separated Values summary) (*.csi v Save as type: CSV (Comma Separated Values summary) (*.csi v Packet Range Help Packet Range O Captured Displayed All packets 880 100 Selected packet 1 1 Marked packets 0 0 First to last marked 0 0 Range: 451-550 100 100 Remove Ignored packets 0 0	This PC								
File name: CAP1_slice Save Save as type: CSV (Comma Separated Values summary) (*.csr v Cancel Help Help Packet Range © Captured Displayed All packets 880 100 Selected packet 1 1 Marked packets 0 0 First to last marked 0 0 Remove Ignored packets 0 0	Matura k	<							>
Save as type: CSV (Comma Separated Values summary) (*.csv ∨ Cancel Help Help Packet Range	Network	File name:	CAP1_slice			\sim		Save	
Help Packet Range Pack		Save as type:	CSV (Comma Separate	ed Values sum	mary) (*.c	s1 ~		Cancel	
Packet Range Pack ● Captured ● Displayed ● Pack ● All packets 880 100 ● ● Selected packet 1 1 ● ● Marked packets 0 0 ● ● First to last marked 0 0 ● ● Range: 451-550 100 100 ● ● Remove Ignored packets 0 0 ● ●								Help	
● Captured● Displayed○ All packets880100○ Selected packet11○ Marked packets00○ First to last marked00● Range:451-550100100○ Remove Ignored packets00		Packet Range						F	ack
○ All packets 880 100 ○ Selected packet 1 1 P ○ Marked packets 0 0 P ○ First to last marked 0 0 P ● Range: 451-550 100 100 P ■ Remove Ignored packets 0 0 E				00	aptured	○ Displ	ayed	6	<mark>⊿ P</mark> a
○ Selected packet 1 1 I		○ All packets			880		100		
Marked packets 0 0 0 First to last marked 0 0 0 • Range: 451-550 100 100 Packets • Remove Ignored packets 0 0 Ea		O Selected pack	ket		1		1	6	<mark>⊿ P</mark> a
Image: Image: <th></th> <th>Marked packet Direct to last market</th> <th>ets etc.e.d</th> <th></th> <th>U</th> <th></th> <th>U</th> <th></th> <th>ŀ</th>		Marked packet Direct to last market	ets etc.e.d		U		U		ŀ
Remove Ignored packets 0 0		Range: 451-	550		100		100		Pa
		Remove Ignor	red packets		0		0		Ea

对相关数据包在capture 2上重复相同的过程。

		a		
- 7	u	r		
	n	٤.		
		-		

Save in:	E Desktop		~	G 🕫	•13 ٵ	
Auick access	Name	Noit	ems match your s	Status earch.	Date	modified
Desktop						
Libraries						
Unis PC						
۲	<					>
Network	File name:	CAP2_slice			· [Save
	Save as type:	CSV (Comma Se	parated Values sum	mary) (".c	sı ~	Cancel
						Help
	Packet Range		0.0			Packe
			۲	aptured	O Displayed	d ⊠Pa
	O All packets			904	90	4 🗹
	 Selected part 	ket		1		
	 Marked pack 	cets		0		0
	 First to last m 	arked		0	1	
	Range: 463	3-564	102	10		
	Remove Ign	red packets		0		

在Microsoft Excel中打开两个CSV文件。

在源捕获CSV上,另存为**XLSX格式**。

Save As		
L Recent	↑ ☐ Desktop	
Cisco	Excel Workbook (*.xlsx)	🖓 Save

在屏幕底部,选择+符号以添加其他工作表。将其命**名为CAP2_slice。**

485 55.51497 192.168.2: 192.168.2ESP	176	340	27	ESP (SPI=0x040001dc)
486 55.51697 192.168.23 192.168.28 ESP	176	341	27	ESP (SPI=0x040001dc)
487 55.51796 192.168.2 192.168.2 ESP	176	342	27	ESP (SPI=0x040001dc)
CAP1_slice				

打开CAP2 CSV文件并按CTRL +a选择全部,按CTRL + c复制该文件。

J77 \checkmark : $\times \checkmark f_x$

1	Α	В	С	D	E	F	G	Н	1	J	K	L	М
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number
2	463	60.99901	192.168.2	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001dd	
3	464	61.00301	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001dd	
4	465	61.00506	192.168.2	192.168.28	ESP	176	308	27			ESP (SPI=	0x040001dc	5
5	466	61.00706	192.168.2	192.168.28	ESP	176	309	27			ESP (SPI=	0x040001dd	
6	467	61.00905	192.168.2	192.168.28	ESP	176	310	27			ESP (SPI=	0x040001dc)
7	468	61.01006	192.168.2	192.168.28	ESP	176	311	27			ESP (SPI=	0x040001dd	
8	469	61.01105	192.168.2	192.168.28	ESP	176	312	27			ESP (SPI=	0x040001dd	5
9	470	61.01305	192.168.2	192.168.28	ESP	176	313	27			ESP (SPI=	0x040001do	
10	471	61.01406	192.168.2	192.168.28	ESP	176	314	27			ESP (SPI=	0x040001dd	
11	472	61.01606	192.168.2	192.168.28	ESP	176	315	27			ESP (SPI=	0x040001dc	
12	473	61.01806	192.168.2	192.168.28	ESP	176	316	27			ESP (SPI=	0x040001dd	
13	474	61.02106	192.168.2	192.168.28	ESP	176	317	27			ESP (SPI=	0x040001dc	5
14	475	61.02205	192.168.2	192.168.28	ESP	176	318	27			ESP (SPI=	0x040001dd	
15	476	61.02306	192.168.2	192.168.28	ESP	176	319	27			ESP (SPI=	0x040001dc)
16	477	61.02506	192.168.2	192.168.28	ESP	176	320	27			ESP (SPI=	0x040001dd	
17	478	61.02605	192.168.2	192.168.28	ESP	176	321	27			ESP (SPI=	0x040001dd	5

导航到CAP1_slice.xlsx文件,在CAP2_slice的第二个选项卡上,将复制的信息粘贴(CTRL + v)到单 元格A1。

Auto	Save On O	R	9- 9				CAP	1_slice.xlsx	• Saved •				2
File	Home	Inse	rt Pag	e Layout	Formulas	Dat	a Review	View	Help				
ĥ	👗 Cut		Calibri		v 11 v /	A° Aĭ	= = =	89	🐉 Wrap Te	ect	Genera	I	~
Paste	Copy ~		BI		1. 0.	Α.	= = =		Merge /	R Center v	¢.,	%	€ <u>0</u> .00
*	ダ Format P	ainter	0.1		 -	- ·			Merge	a center -		/0 /	.00 -20
	Clipboard	13	ù l	Font	t	F2		Aligne	nent	5		Number	5
A1	Ŧ	: >	\sim	f _x									
	A	B	С	D	E	F	G	н	1	J	К	L	N
1													
3		_											_
4													
5													
6													
7													_
8													
10		_											
11													
12													
13													
14													_
15													_
17		_											
18													_
19													
20													
21													_
22													
23													_
25		_											_
26													
27													
28							_						
29							_						_
30													
32													
33													-
34													
35													
36													_
37							_						
38													
-	> (CAP1_sl	ice CA	P2_slice	(+)								

-	<u> </u>				-	1	<u> </u>		· · · · ·			N	-	
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Different	i Source Po	Destinatio	Info		Sequer	nce N
2	463	60.99901	192.168.23	192.168.28	ESP	176	306	27	,		ESP	(SPI=0)x04000	1dc)
3	464	61.00301	192.168.23	192.168.28	ESP	176	307	27	,		ESP	(SPI=0)x04000	1dc)
4	465	61.00506	192.168.23	192.168.28	ESP	176	308	27	,		ESP	(SPI=0)x04000	1dc)
5	466	61.00706	192.168.23	192.168.28	ESP	176	309	27	,		ESP	(SPI=0)x04000	1dc)
6	467	61.00905	192.168.23	192.168.28	ESP	176	310	27	,		ESP	(SPI=0)x04000	1dc)
7	468	61.01006	192.168.23	192.168.28	ESP	176	311	27	,		ESP	(SPI=0)x04000	1dc)
8	469	61.01105	192.168.23	192.168.28	ESP	176	312	27	,		ESP	(SPI=0)x04000	1dc)
9	470	61.01305	192.168.23	192.168.28	ESP	176	313	27	,		ESP	(SPI=0)x04000	1dc)
10	471	61.01406	192.168.23	192.168.28	ESP	176	314	27	,		ESP	(SPI=0)x04000	1dc)
11	472	61.01606	192.168.23	192.168.28	ESP	176	315	27	,		ESP	(SPI=0)x04000	1dc)
12	473	61.01806	192.168.23	192.168.28	ESP	176	316	27	,		ESP	(SPI=0)x04000	1dc)
13	474	61.02106	192.168.23	192.168.28	ESP	176	317	27	,		ESP	(SPI=0)x04000	1dc)
14	475	61.02205	192.168.23	192.168.28	ESP	176	318	27	,		ESP	(SPI=0)x04000	1dc)
15	476	61.02306	192.168.23	192.168.28	ESP	176	319	27	,		ESP	(SPI=0)x04000	1dc)
16	477	61.02506	192.168.23	192.168.28	ESP	176	320	27	,		ESP	(SPI=0)x04000	1dc)
17	478	61.02605	192.168.23	192.168.28	ESP	176	321	27	,		ESP	(SPI=0)x04000	1dc)
18	479	61.02805	192.168.23	192.168.28	ESP	176	322	27	,		ESP	(SPI=0)x04000	1dc)
19	480	61.02906	192.168.23	192.168.28	ESP	176	323	27	,		ESP	(SPI=0)x04000	1dc)
20	481	61.02906	192.168.23	192.168.28	ESP	176	324	27	,		ESP	(SPI=0)x04000	1dc)
21	482	61.03005	192.168.23	192.168.28	ESP	176	325	27	,		ESP	(SPI=0)x04000	1dc)
22	483	61.03206	192.168.23	192.168.28	ESP	176	326	27	,		ESP	(SPI=0)x04000	1dc)
23	484	61.03306	192.168.23	192.168.28	ESP	176	327	27	,		ESP	(SPI=0)x04000	1dc)
24	485	61.03505	192.168.23	192.168.28	ESP	176	328	27	,		ESP	(SPI=0)x04000	1dc)
25	486	61.03606	192.168.23	192.168.28	ESP	176	329	27	,		ESP	(SPI=0)x04000	1dc)
26	487	61.03905	192.168.23	192.168.28	ESP	176	330	27	,		ESP	(SPI=0)x04000	1dc)
27	488	61.04105	192.168.23	192.168.28	ESP	176	331	27	,		ESP	(SPI=0)x04000	1dc)
28	489	61.04206	192.168.23	192.168.28	ESP	176	332	27	,		ESP	(SPI=0)x04000	1dc)
29	490	61.04406	192.168.23	192.168.28	ESP	176	333	27	,		ESP	(SPI=0)x04000	1dc)
30	491	61.04606	192.168.23	192.168.28	ESP	176	334	27	,		ESP	(SPI=0)x04000	1dc)
31	492	61.06305	192.168.23	192.168.28	ESP	176	335	27	,		ESP	(SPI=0)x04000	1dc)
32	493	61.06505	192.168.23	192.168.28	ESP	176	336	27	,		ESP	(SPI=0)x04000	1dc)
33	494	61.06705	192.168.23	192.168.28	ESP	176	337	27	,		ESP	(SPI=0)x04000	1dc)
34	495	61.06905	192.168.23	192.168.28	ESP	176	338	27	,		ESP	(SPI=0)x04000	1dc)
35	496	61.07105	192.168.23	192.168.28	ESP	176	339	27	,		ESP	(SPI=0)x04000	1dc)
36	497	61.07105	192.168.23	192.168.28	ESP	176	340	27	,		ESP	(SPI=0)x04000	1dc)
7	400	61 07005	100 160 00	103 160 30	FCD	176	241	27	,		FCD	(001-0	w04000	1do)

返回CAP1_slice工作表并创建一个名为COMPARE_ESP_SEQUENCE的新列。

1	1	A	в	С	D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R
1	No.		Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPARE	ESP_SEQ	JENCE	
2		451	55.44196	192.168.2	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001dd)					
3		452	55.44598	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001dd)					
		450	EE 44007	100 160 0	103 160 30	ren	176	200	77			ren (eni-	0.000001d	4					

由于ESP序列号位于列G中,请按照所示合成一个VLOOKUP命令来比较两个工作表,以确保源上 G列中的所有内容都位于目标上G列中。

=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G, 1,FALSE)),"MISSING","PRESENT")

· •	× ✓	f _x =IF	(ISNA(VLC	OKUP(G2,	AP2_slice	IG:G,1,FAL	SE)) ,"MISS	ING","PRE	SENT")													
в	с	D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R	S	т	U	v	w	x
ime	Source	Destinati	c Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	e Number		COMPA -	ESP_SEC	UENCE							
55.4419	6 192.168.2	192.168.2	ESP .	176	306	27			ESP (SPI=	0x040001d	ic)		=IF(ISNA(VLOOKUP	(G2,CAP2_	slice!G:G,1	FALSE)),"	MISSING","	PRESENT")			
55.445	8 192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=	0x040001d	ic)			ī.								

选择Enter后,将显示PRESENT一词。这意味着具有ESP序列306的**数据**包存在于第二张表中。这 一点很重要,因为它意味着数据包是从源发送到目的地。

	А	В	с	D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R	
1 N	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPA -	ESP_SEQ	JENCE		
2	451	55.44196	192.168.23	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001dc)		PRESENT				
3	452	55.44598	192.168.23	192.168.28	ESP	176	307	27			ESP (SPI=0	0x040001dc)						

选择**列O**行2,并将鼠标悬停在该单元格周围的绿色框的右下角。

N	0	Р	Q	R	S
	COMPARE	ESP_SEQ	JENCE		
	3 10				

选择并按住,然后向下拖动鼠标,将此公式复制到有值的单元格的底部。

B	C	D	E	F	G	н	1.1	J	K	L	м	N	0	Р	Q	R	S	т	U	v	W
Time	Source	e Destin	atic Protocol	Length	ESP Seque	Different	ti Source Po	Destination	c Info	Sequence	Number		COMPARE	ESP_SEC	UENCE						
1 55.44	196 192.16	8.23192.16	8.28 ESP	176	306	2	7		ESP (SPI	=0x040001dc			PRESENT								
2 55.44	598 192.16	8.2: 192.16	8.28 ESP	176	307	2	7		ESP (SPI	=0x040001dc											
3 55.44	897 192.16	8.2: 192.16	8.28 ESP	176	308	2	7		ESP (SPI	=0x040001dc											
4 55.43	097 192.16	8.2: 192.16	8.22 ESP	1/6	309	2	/		ESP (SPI	=0x040001dc											
6 55 4	496 192.10	8.2: 192.10	8.22ESP	170	310	2	7		ESP (SPI	=0x040001dc											
7 55 49	597 192 16	8 2: 192.10	8 25 ESD	176	312	2	7		ESP (SPI	-0x040001dc											
8 55.4	698 192.16	8.2: 192.16	8.28 ESP	176	313	2	7		ESP (SPI	=0x040001dc											
9 55.4	797 192.16	8.2: 192.16	B.2EESP	176	314	2	7		ESP (SPI	=0x040001dc											
0 55.45	898 192.16	8.2: 192.16	8.28 ESP	176	315	2	7		ESP (SPI	=0x040001dc											
1 55.46	197 192.16	8.2: 192.16	8.28 ESP	176	316	2	7		ESP (SPI	=0x040001dc											
2 55.40	397 192.16	8.2: 192.16	8.28 ESP	176	317	2	7		ESP (SPI	=0x040001dc											
3 55.40	596 192.16	8.2: 192.16	8.28 ESP	176	318	2	7		ESP (SPI	=0x040001dc)										
4 55.46	697 192.16	8.2:192.16	8.28 ESP	176	319	2	7		ESP (SPI	=0x040001dc)										
5 55.40	796 192.16	8.23192.16	8.28 ESP	176	320	2	7		ESP (SPI	=0x040001dc)										
6 55.40	996 192.16	8.25192.16	8.28 ESP	176	321	2	7		ESP (SPI	=0x040001dc											
7 55.47	097 192.16	8.23192.16	8.28 ESP	176	322	2	7		ESP (SPI	=0x040001dc)										
	11.00/7/	174.000	<174 HIG	(CEAR			2.74	,			15.01					IFAC					
540	55 60496	192 169	2: 102 169	25 550		176	205	2	7		ESI		v040001d	c)		DPE	ENT			-	-
540	55.00450	192.100.	2: 192.100.	20 500	-	170	335	2	-		50	- (5-1-0	000100		-	PRES				-	-
541	55.60596	192.168.	.2: 192.168.	ZEESP	_	1/6	396	2	/		ESI	P (SPI=0	x040001d	c)	_	PRES	SENT				
542	55.60696	192.168.	.23192.168.	28 ESP		176	397	2	7		ESI	P (SPI=0	x040001d	c)		PRES	SENT			_	
543	55.60696	192.168.	.2:192.168.	28 ESP		176	398	2	7		ES	P (SPI=0	x040001d	c)		PRES	SENT				
544	55.60696	192.168.	2:192.168.	28 ESP		176	399	2	7		ESI	P (SPI=0	x040001d	c)		PRES	SENT				
545	55.60796	192.168.	2: 192.168.	28 ESP		176	400	2	7		ESI	P (SPI=0	x040001d	c)		PRES	SENT				
546	55.60796	192.168.	.2: 192.168.	28 ESP		176	401	2	7		ES	P (SPI=0	x040001d	c)		PRES	SENT				
547	55,60896	192,168	2: 192.168.	28 ESP		176	402	2	7		ESI	P (SPI=0	x040001d	c)		PRES	SENT				
548	55,60896	192,168	2:192.168	28 ESP	_	176	403	2	7		ES	P (SPI=0	x040001d	c)		PRE	SENT				
549	55,60997	192,168	2:192.168	28 ESP		176	404	2	7		ESI	P (SPI=0	x040001d	c)		PRE	SENT				-
550	55 61096	192 169	2:192.169	25 ESD		176	405	2	7		FCI	0(501-0	v040001d	c)		DPE	SENT			-	-
350	33.01090	192.100.	2. 192.100.	ZC EOP	-	1/0	403	2			231	(3P1=0	A04000100			PAE	JUNI I	1		-	-

滚动回工作表顶部,然后单击COMPARE_ESP_SEQUENCE。然后选择**排序和过滤**。

) onal ng ~	Format as Table ~	Normal Neutral Sty	Bad Calculation	Good Check C	ell	Insert	Delete Fo Cells	rmat ✓	AutoSum Fill ~ Clear ~	Sort & F Filter ~ S	nd &
N	O COMPAR		C R	S	T	U	V	w	X	Y	

从下拉菜单中选择Filter。



COMPARE_ESP_SEQUENCE列中会出现一个下拉菜单。

м	N	0	Р	
lumber		COMPA -	ESP_SEQ	JEN
		PRESENT		
		PRESENT		
		PRESENT		

单击COMPARE_ESP_SEQUENCE标题上的下拉菜单。请注意,在本例中,显示的唯一值为 PRESENT。这意味着两个捕获中都存在所有数据包。

к	L	м	N	0	
c Info	Sequence	Number		COMPA -	ESI
ES AJ	Sort A to Z				
ES ZI	C				
ES A↓	Sort 2 to A				
ES S	ort by Color			>	
ES S	heet <u>V</u> iew			>	
ES	01 E11 E	100100			
ES 1×	Clear Filter Fro	om "COMPA	RE_ESP_SEQ	UENCE"	
ES F	ilter by Color			>	
ES 1	ext <u>F</u> ilters			>	
ES	Canach			0	
ES	Search			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
ES	✓ (Select A	4II) ~			
ES	PRESEN	I			
ES					

要创建有问题的示例,请从CAP2_slice删除10个数据包,以演示在缺少某些丢失数据包的测试中如 何执行此操作。

11	4/2	01.01000 192.108.2: 192.108.28 ESP	1/0	315	27	ESP (SPI=0X040001ac)	
12	473	61.01806 192.168.23 192.168.28 ESP	176	316	27	ESP (SPI=0x040001dc)	
13	474	61.02106 192.168.23 192.168.28 ESP	176	317	27	ESP (SPI=0x040001dc)	
14	475	61.02205 192.168.23 192.168.28 ESP	176	318	27	ESP (SPI=0x040001dc)	
15	476	61.02306 192.168.23192.168.28 ESP	176	319	27	ESP (SPI=0x040001dc)	
16	477	61.02506 192.168.23 192.168.28 ESP	176	320	27	ESP (SPI=0x040001dc)	
17	478	61.02605 192.168.23 192.168.28 ESP	176	321	27	ESP (SPI=0x040001dc)	
18	479	61.02805 192.168.23 192.168.28 ESP	176	322	27	ESP (SPI=0x040001dc)	
19	480	61.02906 192.168.23 192.168.28 ESP	176	323	27	ESP (SPI=0x040001dc)	
20	481	61.02906 192.168.23 192.168.28 ESP	176	324	27	ESP (SPI=0x040001dc)	
21	482	61.03005 192.168.23 192.168.28 ESP	176	325	27	ESP (SPI=0x040001dc)	
22	483	61.03206 192.168.23 192.168.28 ESP	176	326	27	ESP (SPI=0x040001dc)	
23	484	61.03306 192.168.23 192.168.28 ESP	176	327	27	ESP (SPI=0x040001dc)	
24	485	61.03505 192.168.23 192.168.28 ESP	176	328	27	ESP (SPI=0x040001dc)	
25	486	61.03606 192.168.23 192.168.28 ESP	176	329	27	ESP (SPI=0x040001dc)	
26	487	61.03905 192.168.23 192.168.28 ESP	176	330	27	ESP (SPI=0x040001dc)	
27	488	61.04105 192.168.23 192.168.28 ESP	176	331	27	ESP (SPI=0x040001dc)	
28	489	61.04206 192.168.23 192.168.28 ESP	176	332	27	ESP (SPI=0x040001dc)	
29	490	61.04406 192.168.23 192.168.28 ESP	176	333	27	ESP (SPI=0x040001dc)	
30	491	61.04606 192.168.23 192.168.28 ESP	176	334	27	ESP (SPI=0x040001dc)	
31	492	61.06305 192.168.23 192.168.28 ESP	176	335	27	ESP (SPI=0x040001dc)	
32	493	61.06505 192.168.23 192.168.28 ESP	176	336	27	ESP (SPI=0x040001dc)	
33	494	61.06705 192.168.23 192.168.28 ESP	176	337	27	ESP (SPI=0x040001dc)	
34	495	61.06905 192.168.23 192.168.28 ESP	176	338	27	ESP (SPI=0x040001dc)	
35	496	61.07105 192.168.23 192.168.28 ESP	176	339	27	ESP (SPI=0x040001dc)	
36	497	61.07105 192.168.23 192.168.28 ESP	176	340	27	ESP (SPI=0x040001dc)	
37	498	61.07205 192.168.23 192.168.28 ESP	176	341	27	ESP (SPI=0x040001dc)	
38	499	61.07605 192.168.23 192.168.28 ESP	176	342	27	ESP (SPI=0x040001dc)	
-	•	CAP1_slice CAP2_slice					

返回CAP1_slice表,现在发现有10个数据包丢失。

	33.43737 132.100.2.132.100.2CC3	110	314	£1	L31 (311-0X04000100)	T NEVENT
460	55.45898 192.168.2: 192.168.2ESP	176	315	27	ESP (SPI=0x040001dc)	PRESENT
461	55.46197 192.168.23 192.168.28 ESP	176	316	27	ESP (SPI=0x040001dc)	PRESENT
462	55.46397 192.168.23 192.168.28 ESP	176	317	27	ESP (SPI=0x040001dc)	PRESENT
463	55.46596 192.168.23 192.168.28 ESP	176	318	27	ESP (SPI=0x040001dc)	MISSING
464	55.46697 192.168.23 192.168.28 ESP	176	319	27	ESP (SPI=0x040001dc)	MISSING
465	55.46796 192.168.23 192.168.28 ESP	176	320	27	ESP (SPI=0x040001dc)	MISSING
466	55.46996 192.168.23 192.168.28 ESP	176	321	27	ESP (SPI=0x040001dc)	MISSING
467	55.47097 192.168.23 192.168.28 ESP	176	322	27	ESP (SPI=0x040001dc)	MISSING
468	55.47198 192.168.23 192.168.28 ESP	176	323	27	ESP (SPI=0x040001dc)	MISSING
469	55.47297 192.168.23 192.168.28 ESP	176	324	27	ESP (SPI=0x040001dc)	MISSING
470	55.47497 192.168.23 192.168.28 ESP	176	325	27	ESP (SPI=0x040001dc)	MISSING
471	55.47597 192.168.23 192.168.28 ESP	176	326	27	ESP (SPI=0x040001dc)	MISSING
472	55.47697 192.168.23 192.168.28 ESP	176	327	27	ESP (SPI=0x040001dc)	MISSING
473	55.47896 192.168.23 192.168.28 ESP	176	328	27	ESP (SPI=0x040001dc)	PRESENT
474	55.48096 192.168.23 192.168.28 ESP	176	329	27	ESP (SPI=0x040001dc)	PRESENT

在COMPARE_ESP_SEQUENCE列上选择下拉菜单后,现在还会看到缺少数据包。可以将其切换 为仅查看MISSING数据包。

	K	L	M	N	0
nf	0	Sequence	Number		COMPA -
S	<mark>2</mark> ↓ <u>s</u> o	ort A to Z			_
S	Z↓ S <u>o</u>	ort Z to A			-
S	Sor	<u>t</u> by Color			>
S	She	et <u>V</u> iew			>
5	∑× ⊆	lear Filter Fro	m "COMPA	RE_ESP_SEQ	UENCE"
S	Filt	er by Color			>
S	Tex	t <u>F</u> ilters			>
5	Sea	arch			Q
1 14 14 14 14 14 14 14 14 14 14		I (Select A I MISSING I PRESENT	III) F		
5 5			0	K	Cancel .:



现在,Excel表格中只显示缺失的数据包。

A		В	С	D	E	F	G	н		J	K	L	M	N	0	P
No.	Т	ime	Source	Destinati	Protocol	Length	ESP Seque	Different	Source Po	Destinatio	Info	Sequence	Number		COMPA J	_ESP_SEQ
4	463	55.46596	192.168.23	192.168.2	ESP .	176	318	27			ESP (SPI	=0x040001dc)		MISSING	
5	464	55.46697	192.168.23	192.168.2	ESP .	176	319	27			ESP (SPI	=0x040001dc)		MISSING	
6	465	55.46796	192.168.23	192.168.2	ESP .	176	320	27			ESP (SPI	=0x040001dc)		MISSING	
7	466	55.46996	192.168.23	192.168.2	ESP .	176	321	27			ESP (SPI	=0x040001dc)		MISSING	
8	467	55.47097	192.168.23	192.168.2	ESP .	176	322	27			ESP (SPI	=0x040001dc)		MISSING	
9	468	55.47198	192.168.23	192.168.2	ESP	176	323	27			ESP (SPI	=0x040001dc)		MISSING	
0	469	55.47297	192.168.23	192.168.2	ESP	176	324	27			ESP (SPI	=0x040001dc)		MISSING	
1	470	55.47497	192.168.23	192.168.2	ESP .	176	325	27			ESP (SPI	=0x040001dc)		MISSING	
2	471	55.47597	192.168.23	192.168.2	ESP .	176	326	27			ESP (SPI	=0x040001dc)		MISSING	
3	472	55.47697	192.168.23	192.168.2	ESP .	176	327	27			ESP (SPI	=0x040001dc)		MISSING	
2																
)3																

相关信息

- <u>思科嵌入式数据包捕获</u>
 <u>技术支持和文档 Cisco Systems</u>

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)。