Verify and Identify Packet Loss in the WAN for SD-WAN

Contents

Introduction Prerequisites Requirements Components Used Background Troubleshoot Process Overview Process Mark the Desired traffic with DSCP Capture the Traffic with the Embedded Capture Analysis through Wireshark Filter the Desired Traffic by ESP Sequence Related Information

Introduction

This document describes how to identify and collect data when traffic has loss across the WAN but no drops are seen on the SD-WAN Edge.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Embedded Packet Capture or vManage Packet Capture
- Wireshark
- Microsoft Excel

Components Used

The information in this document is based on these software and hardware versions:

- C8000V version 17.03.04
- vManage version 20.3.4
- Wireshark version 2.6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background

In order to assist with this challenge, the steps described in this doc shows how to mark specific traffic with Differentiated Services Code Point (DSCP) to help to identify the desired packets. DSCP can be used to identify the traffic since this value is copied from the inner packet header to the IPsec header. Once the desired packets are identified, it shows how to match the traffic across two WAN captures to ensure traffic made it from source to destination.

Two single router sites are used to demonstrate this troubleshoot technique. In this case, ICMP traffic from 10.0.0.10 to 10.0.2.10 in the form of 100 pings as shown in the image. There is no loss in this example but this same troubleshoot technique is used in the case where there is a loss to identify it.



Troubleshoot Process

Overview Process

- 1. For the traffic traced across the WAN, an Access List (ACL) (or centralized policy) is needed to mark traffic with some unused DSCP value. In this example, DSCP 27 is used.
- 2. Once the traffic is marked, embedded packet capture is used to capture the packets on the transport interface of the source and destination router.

Note: vManage packet capture can also be used although there is a limitation of 5MB of data or 5 minutes of runtime.

- 1. After the captures are taken, open them in Wireshark to view.
- 2. The filter is applied in Wireshark to show which packets are desired and then they are compared.
- 3. Microsoft Excel is used for large captures to ensure accuracy.

Mark the Desired traffic with DSCP

An access-list such as the example Is configured on the source router (cEdge1 in this example) and applied on the interface in the SD-WAN portion of the router config as shown.

An optional counter is applied to verify that traffic hits the policy as expected. This can be checked

with the command show sdwan policy access-list-counters.

```
policy
access-list mark_dscp_27
sequence 10
match
source-ip 10.0.0.10/32
destination-ip 10.0.2.10/32
1
action accept
count MARK_DSCP_27_COUNT (optional counter to verify packets that hit the policy)
set
dscp 27
1
1
1
default-action accept
sdwan
 interface GigabitEthernet3
 access-list mark_dscp_27 in
```

Capture the Traffic with the Embedded Capture

Note: How to configure an embedded packet capture in Cisco IOS XE to capture the encrypted packets which traverse the WAN, navigate to <u>Embedded Packet Capture for</u> <u>Cisco IOS and Cisco IOS XE Configuration Example</u>

Note: An ACL must be used to limit the EPC on the WAN as there could be more than the 1000 PPS rate-limit for the EPC.

Example

An ACL is configured on cEdge1 and cEdge3 since traffic is only checked in the direction of source to destination in this example.

Note: The WAN IP addresses are used to filter the capture. There are multiple outputs which can be used to identify the path the traffic takes so that the correct WAN IPs can be identified for the ACL filter. The commands which can be used to generate this output are the **show sdwan app-fwd cflowd flows** and **show sdwan policy service path**. Please, navigate to <u>Conditional Packet Trace</u> for debug condition.

ip access-list extended CAP-Filter

10 permit ip host 192.168.23.149 host 192.168.28.240

At this point, the captures are started on both routers and 100 pings are sent across the overlay.

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms After the captures are stopped and collected from both routers, they need to be opened in Wireshark to view them.

Analysis through Wireshark

Once the cEdge1 capture is opened in Wireshark it is seen that all the traffic is encrypted and it is not easy to decipher which packets are the pings which were sent.

sola	fiter <ctrl-></ctrl->										
	Time	Source	Destination	Protocol Length	ESP Sequence	Differentiated Services Codepoint	Source Port	Destination Port	Sequence Number	Info	
	1 0.000000	192.168.23.149	192.168.28.240	UOP	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	UDP	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	192,168,28,248	LIDP	175	Class Selector 6				12386 + 12487 Lene133	
	22 9.653957	192, 168, 23, 149	192,168,28,248	LIDP	168	Class Selector 6				12386 + 12407 Len=126	
	23 18.882988	192.168.23.149	192.168.28.248	LIDP	175	Class Selector 6				12386 + 12407 Lene133	
	24 18.564957	192,168,23,149	192,168,28,248	LIDP	168	Class Selector 6				12386 + 12487 Len=126	
	25 18.949999	192, 168, 23, 149	192, 168, 28, 248	LIDP	175	Class Selector 6				12386 + 12407 Lene133	
	26 11.416978	192.168.23.149	192.168.28.240	LIDP	168	Class Selector 6				12386 + 12407 Lene126	
	27 11.937991	192, 168, 23, 149	192 168 28 248	LIDP	175	Class Selector 6				12386 + 12407 Lene133	
	28 12.400964	192.168.23.149	192.168.28.240	LIDP	168	Class Selector 6				12386 + 12407 Lene126	
	20 12 836998	192 168 23 149	192 168 28 248	LIDE	175	Class Selector 6				12386 - 12407 Lene133	
	38 13 266984	192.168.23.149	192.168.28.240	LIDP	168	Class Selector 6				12386 + 12407 Lene126	
	31 13 770058	102 168 23 149	102 168 28 240	100	175	Class Selector 6				13386 - 13407 (
	33 14 171099	103 168 33 140	103 169 39 340	100	175	Cass Selector o				12205 - 12407 Len-124	
	33 14 172086	103 168 33 140	103 168 38 340	100	176	Default				12286 - 12497 Lan-124	
	34 14 174978	102 168 23 149	102.168.28.240	LIDE	176	Default				12386 - 12407 Len-134	
	35 14 176025	103 168 33 140	103 169 39 340	100	176	Default				12286 - 12487 Lan-124	
	35 14.175905	102 168 23 149	192.100.20.240	100	170	Default				12200 - 12407 Len-124	
	37 14 176977	103 168 33 140	103 168 38 340	100	176	Default				12205 - 12407 Lan-124	
	37 14.176977	192.100.23.149	192.100.20.240	UDP	170	Default				12300 + 12407 Len-134	
	30 14.178991	192.100.23.149	192.106.28.240	COP	110	Detant				17300 + 1540\ FGU=134	

Filter this capture with a display filter **ip.dsfield.dscp == 27**, it is seen that only 100 packets are displayed at the bottom of the screen and it is seen that the DSCP column value all shows 27.

TheDardeDescriptionProteoProteoDefendationDescription </th <th></th>	
451 53.4489 19.21.46.3.3.49 19.21.46.3.3.49 192.146.3.2.49 100 176 27 123 453 54.4596 192.146.3.3.49 192.146.3.2.49 100 176 27 123 453 54.4596 192.146.3.3.49 192.146.3.2.49 100 176 27 123 453 54.4596 192.146.3.3.49 192	the
42 25 44976 192,146,3,3,49 192,146,3,2,49 00P 176 27 123 44 53 544966 192,146,3,1,49 192,146,1,2,49 00P 176 27 133 44 53 544966 192,146,3,1,49 192,146,3,1,49 192,146,3,1,49 192,146,3,1,49 193,148,3,1,49 193,146,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,148,3,1,49 193,149 193,149,3,1	2386 + 12407 Len=134
433 53.44996 152.146.3.3.49 102 176 27 133 443 54.49966 152.146.3.3.49 102.146.3.3.49 100 176 27 133 445 55.49966 152.146.3.3.49 102.146.3.3.49 100 176 27 133 445 55.49967 152.146.3.3.49 102.146.3.3.49 100 176 27 133 447 55.49978 152.146.3.3.49 102.146.3.3.49 100 176 27 133 446 55.49978 152.146.3.3.49 102.146.3.3.49 100 176 27 133 446 55.49978 152.146.3.3.49 102.146.3.3.49 100 176 27 133 442 55.49978 152.146.3.3.49 152.146.3.3.49 100 176 27 133 445 54.49978 152.146.3.3.49 102.146.3.2.49 100 176 27 133 445 54.49978 152.146.3.3.49 102.146.2.2.49 100 176 27 133 445 54.49979 152.146.3.3.49 10	2386 + 12407 Len=134
444 55.45996 192.168.3.3.49 192.168.2.3.49 100 176 27 123 455 55.45964 192.168.2.3.49 102.168.2.3.49 100 176 27 133 455 55.45964 192.168.2.3.49 102.168.2.3.49 100 176 27 133 456 55.45976 192.168.2.3.49 100 176 27 133 469 55.45976 192.168.2.3.49 100 176 27 133 469 55.45976 192.168.2.3.49 100 176 27 133 461 55.45976 192.168.2.3.49 100 176 27 133 463 56.49976 192.168.2.3.49 100 176 27 133 464 56.49976 192.168.2.3.49 100 176 27 133 464 56.49976 192.168.2.3.49 100 176 27 133 464 56.49776 192.168.2.3.49 100 176 27 133 475 56.49786 192.168.2.3.49 100	2386 + 12407 Len+134
495 56.5996 192.162.3.3.49 132.146.2.3.49 109 176 27 133 495 56.5997 192.146.3.3.49 132.146.2.3.49 109 176 27 133 497 56.5997 192.146.3.3.49 132.146.2.3.49 109 176 27 133 497 56.5997 192.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.54975 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.54975 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.54976 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.54976 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.54976 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.49971 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.49971 132.146.3.3.49 132.146.2.3.49 109 176 27 133 449 55.49971 132.146.3.3.49 132.146.2.3.49 109 176 27 133 479 55.49971 13	2386 → 12407 Len=134
446 55.45990 192.146.3.3.49	2386 → 12407 Len=134
477 55.5970 192.168.3.3.40 192.168.2.3.40 100 176 27 123 489 55.65077 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 192.168.2.3.40 193.168.2.1.40 192.168.2.3.40 192.16	2386 → 12407 Len=134
448 55.45970 192.168.3.3.49 192.168.2.3.49 197 27 123 449 55.45976 192.168.3.3.49 192.168.2.3.49	2386 → 12407 Len=134
499 95.45796 92.168.3.3.49 132.168.2.3.49 100° 176 27 133 440 95.45807 92.168.3.3.49 132.168.2.3.49 100° 176 27 133 441 55.45807 132.168.2.3.49 100° 176 27 133 443 55.45807 132.168.2.3.49 100° 176 27 133 443 55.45907 132.168.2.3.49 100° 176 27 133 445 55.45907 132.168.2.3.49 100° 176 27 133 446 55.45907 132.168.2.3.49 100° 176 27 133 446 55.47907 132.168.2.3.49 100° 176 27 133 446 55.47907 132.168.2.3.49 100° 176 27 133 447 55.47906 132.168.2.3.49 100° 176 27 133 470 55.47906 132.168.2.3.49 100° 176 27 133 473 54.4906 132.168.2.3.49 100° 176 <t< td=""><td>2386 + 12407 Len=134</td></t<>	2386 + 12407 Len=134
440 55.458075 132.148.23.440 132.448.2.3.400 137.6 27 123 441 55.45806 132.148.2.3.400 102.148.2.400 102.148.2.400 102.148.2.400 102.148.2.400 102.148.2.400 10	2386 + 12407 Len=134
441 54.4566 492.146.33.469 192.146.23.469 192 123 442 55.45676 192.146.23.469 192.146.23.46	2386 + 12407 Len+134
442 35.43965 192.148.3.3.49 192.148.2.3.49 192.148.2.3.49 192.148.2.3.49 192.148.2.3.49 192.148.2.3.49 193.149 193.148.2.3.49 <td< td=""><td>2386 → 12407 Len=134</td></td<>	2386 → 12407 Len=134
443 54.4954 192.146.23.49 192.146.23.49 192 123 443 54.4971 192.146.23.49	2386 → 12407 Len=134
444 35.46971 132.148.23.248 132.148.23.248 136 27 133 445 35.46972 132.148.23.248 109 176 27 133 447 35.46972 132.148.23.149 132.148.22.248 109 176 27 133 447 35.46972 132.148.23.149 132.148.22.248 109 176 27 133 449 55.47976 132.148.23.149 132.148.23.248 109 176 27 133 449 55.47976 132.148.23.149 132.148.23.248 109 176 27 133 447 155.47976 132.148.23.149 132.148.2.248 109 176 27 133 473 55.47967 132.148.2.3.49 109 176 27 133 473 55.47967 132.148.2.3.49 109 176 27 133 473 54.49967 132.148.2.3.49 109 176 27 133 473 54.49978 132.148.2.3.49 109 176 27 133 473 <t< td=""><td>2386 → 12407 Len=134</td></t<>	2386 → 12407 Len=134
448 35.4792 192.146.2.3.49 192.146.	2386 + 12407 Len+134
446 35.40961 192.146.23.40 192.146.23.40 192.146.23.40 192.146.23.40 193.140<	2386 → 12407 Len=134
447 93.47986 192.146.2.3.48 102.446.2.3.48 102 176 27 123 447 93.47986 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 192.146.2.3.48 193.148 192.146.2.3.	2386 + 12407 Len+134
448 35.11707 192.146.2.1.49 101.46.2.1.49 102 123 448 35.11707 192.146.2.1.49 102 126 27 123 448 35.11707 192.146.2.1.49 102 135 123 135 449 35.11707 192.146.2.1.49 102 135 123 133 471 35.11470 192.146.2.1.49 102 176 27 123 471 35.11470 192.146.2.1.49 102 176 27 123 473 35.1162 192.146.2.1.49 102 176 27 123 473 35.1162 192.146.2.1.49 102 176 27 123 475 54.1196 192.146.2.1.49 102 176 27 123 475 54.1196 192.146.2.1.49 102 176 27 123 475 54.1196 192.146.2.1.49 102 176 27 123 475 54.1196 192.146.2.1.49 102 176 27 123 485 192.	2386 + 12407 Len+134
449 35.4789 192.186.23.149 192.186.22.149 109 176 27 133 449 35.4789 192.186.23.149 192.186.22.149 109 176 27 133 419 55.4786 192.186.23.149 192.186.22.149 109 176 27 133 419 55.4786 192.186.23.149 192.1	2386 * 12407 Len*134
449 53 449 53 449 53 449 54 27 123 449 53 449 53 449 54 <t< td=""><td>2386 * 12407 Len*134</td></t<>	2386 * 12407 Len*134
41 35.47997 192,148,23,149 192,148,23,149 192,148,23,149 192,148,23,149 192,148,23,149 192,148,23,149 193,148,23,149	2386 + 12407 Len=154
4/2 35.4005 192,184,23,140 192,184,23,140 192,184,23,140 193,184,23,144 193,184,23,144,194,194,194,194,194,194,194,194,194	2386 + 12407 Len+134
94 39 3.10091 192.100.2.1.09 192.100.2.1.09 192.100.2.1.09 192 103 94 39 3.10091 192.100.2.1.09 192.100.2.1.09 192 102 103 94 39 3.10091 192.100.2.1.09 192.100.2.1.09 192 102 103 94 55 5.448091 192.100.2.1.09 192.100.2.1.09 192.100.2.1.09 192 103 476 55.448091 192.100.2.1.00 192.100.2.1.00 192.100.2.1.00 192.100.2.1.00 192.100 192 478 55.448091 192.100.2.1.00 192.100.2.1.00 192.100 176 27 123 478 55.448091 192.100.2.1.00 192.100 176 27 123 489 55.491951 192.100.2.1.00 192.100 176 27 123 412 55.519561 192.100.2.1.00 192.100 176 27 123 412 55.519561 192.100.2.1.00 192.100 176 27 123 412 55.519561 192.100.2.1.00 192.100 176 27 123 415 5.39951 192.100.2.1.00 192.100 176 27 123	2386 + 12407 Len+134
A # 35 .400% / 12 .18 .23 .10 / 12 .18 .23 .24 / 10 / 16 / 27 / 13 / 13 / 14 / 27 / 13 / 14 / 27 / 13 / 14 / 27 / 13 / 14 / 27 / 13 / 14 / 27 / 12 / 27 / 27	2386 + 12407 Len*134
10 10 <td< td=""><td>2380 + 12407 Len+134</td></td<>	2380 + 12407 Len+134
A # 3 3.44877 192.148.23.149 192.148.23.149 192.148.2.248 009 176 27 133 479 35.448977 192.148.23.149 192.148.2.248 009 176 27 132 479 35.44897 192.148.23.149 192.148.2.249 009 176 27 132 441 55.10881 192.148.23.149 192.148.2.249 009 176 27 122 441 55.10881 192.148.23.149 192.148.2.249 009 176 27 122 445 55.10861 192.148.23.149 192.148.2.249 009 176 27 123 445 55.10861 192.148.23.149 192.148.2.249 009 176 27 123 447 55.10861 192.148.23.149 192.148.2.249 009 176 27 123 449 55.250861 192.148.23.149 192.148.23.249 009 176 27 123 449 55.250861 192.148.23.149 192.148.2.249 009 176 27 123 459 55.250861 192.148.23.149 192.148.2.249 009 176 27 123 450 55.20087 192.148.23.149 192.148.2.249 009 176 27 123 450 55.20087 192.148.23.149 192.148.2.249 009 176 27 123 450 55.20087 192.148.23.149 192.148.2.249 109 176 192.148.2.249 109 176 192.148.2.249 109 176 192.149 192.148.2.249 109 176 192.149 192.149 192.148.2.249 109 176 192.149 192.149 192.148.2.249 109 176 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192.149 192 192.149 192.149 192.149 192	2386 + 12407 Len*134
147 35 4,2007, 123,100 123,1007, 123,100 123,1007, 123,100 123,1007, 123,100 147 35 5,4007, 123,100, 132,100, 12,100, 124,00 100 126 127 123 440 55,50165, 132,100, 132,100, 122,100, 12,00 100 176 27 123 440 55,50165, 132,100, 132,100, 122,100, 12,00 100 176 27 123 440 55,50165, 132,100, 132,100, 122,100, 12,00 100 176 27 123 442 55,51055, 132,100, 132,100, 132,100, 22,200 100 176 27 123 445 55,51056, 132,100, 132,100, 132,100, 22,200 100 176 27 123 445 55,51056, 132,100, 132,100, 132,100, 22,200 100 176 27 123 445 55,51057, 132,100, 132,100, 132,100, 22,200 100 176 27 123 445 55,51057, 132,100, 132,100, 132,100, 22,200 100 176 27 123 445 55,51057, 132,100, 132,100, 132,100, 132,100, 22,200 100 176 27 123 455,51057, 132,100, 1	2380 + 12407 Len+134
44 8 5.49% 192,148,23,149 192,148,23,248 000 176 27 45 5.49% 192,148,23,149 192,148,23,249 000 176 27 41 15,1084 192,148,23,149 192,148,22,249 000 176 27 41 15,1084 192,148,23,149 192,148,22,249 000 176 27 43 55,1196 192,148,23,149 192,148,22,249 000 176 27 44 5 5,1196 192,148,23,149 192,148,22,249 000 176 27 45 55,1597 192,148,23,149 192,148,22,249 000 176 27 47 55,1597 192,148,23,149 192,148,22,249 000 176 27 48 55,1597 192,148,23,149 192,148,23,249 100 176 27 49 55,1597 192,148,23,149 192,148,23,249 100 176 27 49 55,1597 192,148,23,149 192,148,23,249 100 176 27 49 55,1597 192,148,23,149 192,148,23,249 100 176 100 100 100 100 100 100 100 100 100 10	2300 + 1240/ Len+134
140 35.00000 10000 10000	2386 + 12407 Len+134
and 35, Soudhil 192, 162, 21, 149 102, 164, 21, 149 </td <td>2300 * 12407 Len=134</td>	2300 * 12407 Len=134
10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 11 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 14 10 10 10 10 10 10 15 10 10 10 10 10 10 <	2300 * 12407 Len+134
448 55.1356 102.164.21.149 102.464.21.249 UOP 176 17 448 55.1356 102.164.21.149 102.464.21.249 UOP 176 121 448 55.13567 102.164.21.249 UOP 176 27 122 445 55.13567 102.164.21.249 UOP 176 27 122 445 55.13677 102.164.21.249 UOP 176 27 122 447 55.13795 102.164.21.249 UOP 176 27 123 447 55.13795 102.164.21.249 UOP 176 27 123 445 55.23956 102.164.21.249 UOP 176 27 123 445 55.23956 102.164.21.249 UOP 176 27 123 455 55.23956 102.164.21.249 UOP 176 27 123 176	2306 - 12407 Len-134
444 55 51369 192162.31.49 192166.32.49 (UP 176 177 123 446 55 51369 192162.31.49 192166.32.49 (UP 176 177 123 446 55 51369 192162.31.49 192166.32.49 (UP 176 177 123 446 55 51369 192162.31.49 192166.32.49 (UP 176 177 123 448 55 51369 192162.31.49 192166.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192166.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192166.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192166.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192166.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192166.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 177 123 448 55 51369 192162.31.49 192162.32.49 (UP 176 176 176 177 177 177 177 177 177 177	2386 + 12487 Len+134
445 55.14972 192.146.23.149 192.149 </td <td>2386 a 12407 Lena134</td>	2386 a 12407 Lena134
446 55.10071 192.106.21.349 192.108.22.404 (DP 176 27 123 4475 55.10071 192.106.21.349 192.108.22.400 (DP 176 27 123 448 55.23595 192.106.21.349 192.108.22.400 (DP 176 27 123 448 55.23595 192.106.21.349 192.108.22.400 (DP 176 27 123 449 55.2366 192.106.21.349 192.108.22.400 (DP 176 27 123 447 55.2366 192.106.21.349 192.108.22.400 (DP 176 27 123 475 55.2366 192.106.21.349 192.108.22.400 (DP 176 124 475 55.2366 192.106.21.349 192.108.23.400 (DP 176 124 475 55.2366 192.106.21.349 192.106.23.400 (DP 176 124 475 55.2366 192.106.21.349 (DP 176 124 475 55.2366 192.106.21.349 (DP 176 124 475 55.2366 192.106.21.340 (DP 176 124 475 55.2366 192.106.21.340 (DP 176 124 475 55.2366 (DP 176 124)	2386 a 12407 Lena134
487 55.3798 192.162.31.49 102.46.23.494 102.46.23.494 102.46.23.494 102.41.21 487 55.3298 192.166.23.149 192.166.23.494 100 176 27 123 489 55.2398 192.166.23.149 192.166.23.494 100 176 27 123 489 55.2398 192.166.23.149 192.166.23.494 100 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) 176 27 123 </td <td>2386 + 12407 Len=134</td>	2386 + 12407 Len=134
448 55.23955 192.162.31.49 192.164.22.40 (DP 176 27 122 499 55.23965 192.162.31.49 192.168.22.40 (DP 176 27 122 176 bytes on wire (1480 bits), 176 bytes carred (1480 bits) 176 bytes on wire (1480 bits), 176 bytes on wire (1480 bits) 176 bytes on wire (1480 bits), 176 bytes	2386 = 12407 Len=134
489 55.52466 192.162.31.48 192.168.20.248 UDP 176 27 122 176 bytes on wire (1448 bits), 176 bytes captured (1468 bits) 1, Src: 190.168, 156, bits 14, 176 bytes captured (1468 bits) 1, Src: 190.168, 1546, bits 12462 bytes (00:50:56:56:64:e2:b7) rotocol Version 4, Src: 192.168, 1546, bits 12462 ram Protocol, Src Pert: 12366, Dit Pert: 12467 bytes)	2386 + 12407 Len=134
176 bytes on wire (1400 bits), 176 bytes captured (1400 bits) 176 bytes on wire (1400 bits), 176 bytes captured (1400 bits) 176 bytes on wire (1400 bits), 187 bytes (1400 bits) 176 bytes on wire (1400 bits), 187 bytes (1400 bits) 176 bytes on wire (1400 bits), 187 bytes (1400 bits) 176 bytes on wire (1400 bits), 187 bytes (1400 bits) 176 bytes on wire (1400 bits), 187 bytes (1400 b	2386 + 12407 Len=134
:176 bytes on wire (1440 bits), 176 bytes captured (1440 bits) I, Src: UMware_B41sf165 (00;56:56:141:4f36), Dat: UMware_B41s21b7 (00:56:56:84:e2:b7) Yonool Version 4, Src: 132:186, J.148, Dat: 132:06.28.28.280 Yman Frotocol, Src Port: 12566, Dat Port: 12407 Bytes)	
I, Src: Whare_BitafieS (00:50:56:84:af:45), Dat: Whare_Bit2:D7 (00:50:56:84:e2:b7) rotocol Version 4, Src: 192.100.2: 100.2: 102.100.28.240 am Protocol, Src Port: 12386, Dst Port: 12407 lytes)	
votecol Version 4, Src: 192.166.23.140, Dati 192.166.28.240 am Protecol, Src Port: 12366, Dst Port: 12407 ytes)	
ram Protocol, Src Port: 12306, Dst Port: 12407 bytes)	
bytes)	
(2 84 #2 157 88 K8 K6 84 #4 K6 88 88 85 K7 DV D. V E 81	

In some cases where DSCP value is maintained across the WAN, the same filter can be used on the destination capture.

In other cases, this is not possible such as a situation where DSCP value is cleared across a public-internet connection.

Filter the Desired Traffic by ESP Sequence

In either case, the traffic can be identified with the ESP sequence numbers.

To see the ESP sequence numbers in the packet, right click on the capture and choose **Decode as** as shown.

		12386
		12386
Mark/Unmark Packet	Ctrl+M	12386
		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
Edit Resolved Hame		12386
Apply as Filter	•	12386
Prepare as Filter	+	12386
Conversation Filter	•	12386
Conversation Filter		12386
Colorize Conversation	•	12386
SCTP	•	12386
F-ll-		12386
Follow	•	12386
Conv	•	12386
сору		12386
Protocol Preferences	•	12386
Decode Ac		12386
Decode As		12386
Show Packet in New Window	N	12386

Select the **Current** field dropdown menu and in that field type **UDPENCAP** or select it from the dropdown.



Wireshark	۰.)ecode	Δs
THE SHORE		<i>ccouc</i>	

Field	Value	Туре	Default	Current
UDP port	12386	Integer, base 10	(none)	(none) ~
				(none)
				3GPP2 A11
				A21
				ACtrace
				ADP
				ADwin
				ALC AMP
+ -	ъ (R		
				OK Sava Conv from Cancel Hale
				OK Save Copy from Cancel Help

Select the **OK** once this is completed.

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

Within the Wireshark Packet Details section, expand the Encapsulating Security Payload portion of the packet to see **ESP Sequence**.

×

```
      479 55 488973 192 168 23 149
      192 168 28 240
      FSP
      176

      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 (00:50:56:84: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
      Encapsulating Security Payload

      ESP SPI: 0X0400010C (6/109340)
      ESP Sequence: 319
```

Right click on **ESP Sequence** and choose **apply as column** so the ESP Sequence can be seen as a column in the Packet List section at the top portion of the Wireshark screen.

	04 102.100.20.140	102.100.20.240	6.51
456 55.4	Evenend Subtrace		ESP
457 55.4	Expand Subtrees		ESP
458 55.4	Collapse Subtrees		ESP
459 55.4	Expand All		ESP
460 55.4	Collapse 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	Conversation Filter	,	ESP
467 55.4	Conversation miter		ESP
468 55.4	Colorize with Filter	,	ESP
469 55.4	Follow	•	ESP
470 55.4			ESP
471 55.2	Сору	,	ESP
472 55.2	Show Packet Butes	Ctrl+Shift+O	ESP
473 55.2	Show Packet bytes	Cur+Suint+O	ESP
474 55.2	Export Packet Bytes	Ctrl+Shift+X	COP
	Wiki Protocol Page		
Frame 464: 176 byt	Sile Sile C		08 bits)
Ethernet II, Src:	Filter Field Reference		re_84:e2:b7 (0
Internet Protocol	Protocol Preferences	•	8.240
User Datagram Prot		C 1 C 1 C 1	
UDP Encapsulation	Decode As	Ctrl+Shift+U	
Encapsulating Secu	Go to Linked Packet		
ESP SPT: 0x0400	Show Link d Packet in New	v Window	
ESP Sequence: 31]

Note: The ESP SPI for the packets on cEdge1is **0x040001dc**. This is used for a filter on the destination capture.

```
> 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
```

Open the destination capture, repeat the steps to decode as **UDPENCAP**, and display the ESP Sequence numbers in the packets.

Once the packets display the ESP Sequence number, the ESP SPI from the first capture can be used as a filter on the second capture to display only the traffic within that SPI that matches the desired traffic.

Notice that the packet sequence numbers that match both have DSCP 27 marked.



This comparison can be done in Wireshark manually or Microsoft Excel can be used to do this comparison.

In order to use Microsoft Excel to compare, it is necessary to slice both captures to contain only packets which are in both captures.

In the source capture, the first relevant packet has ESP sequence 306 and that corresponds to packet number 451.

CAP.pcap							-		\times
File Edit View	w Go Capture	Analyze Statistics Tel	ephony Wireless Tools	Help					
	📙 🛅 🔀 🖸	९ 🗢 🗢 鼞 🚹 👲	💶 🔍 🔍 🔍 🎹						
ip.dsfield.dscp	== 27							$\times \rightarrow$	• +
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	

The last relevant packet in the source capture has ESP sequence 405 and is packet number 550.

	J., JJ.000000L		20212001201210	14.47		104 E.
	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
						¥
<						>

In the destination capture, the first relevant packet corresponds to the source capture with ESP Sequence 306 but in this capture is packet 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

The last relevant packet is also present with ESP Sequence 405 and it is packet 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	
					-	

The first capture must now be sliced to include only relevant packets.

Navigate to File > Export Packet Dissections > As CSV...

🚄 CAP.pcap	
------------	--

File	Edit View	Go	Capture	Analyze	Statisti	cs Telephony	Wire	ess	Tools	Help		
	Open			Ctrl+0	1	§ 🕹 📃 🔳	Ð,	ວຸ ∈				
	Open Recent			•								
	Merge					Destinati				Destand	Length	
	land for the					Destinati	on	240		Protocol	Length	476
	Import from H	iex Du	mp		149	192.16	8.28	240		ESP		176
	Close			Ctrl+W	149	192.16	8.28	240		ESP		176
					_149	192.16	8.28	.240		ESP		176
	Save			Ctrl+S	149	192.16	8.28	.240		ESP		176
	Save As			Ctrl+Shift+S	149	192.16	8.28	.240		ESP		176
					149	192.16	8.28	240		ESP		176
	File Set			•	149	192.16	8.28	240		ESP		176
					- 149	192.16	8.28	240		ESP		176
	Export Specifie	ed Pac	kets		149	192.16	8.28	240		ESP		176
	Export Packet	Dissec	tions	•		As Plain Text	- I	240		ESP		176
	Export Dacket	Buter		Ctrl+Shift+X		Ac CSV	- I	240		ESP		176
	export Packet	bytes.		CurtShirt+X		AS C5V		.240		ESP		176
	Export PDUs to	o File				As "C" Arrays	- I-	240		ESP		176
	Export TLS Ses	sion K	eys					240		ESP		176
	Evport Objects					As PSML XML	- I-	240		ESP		176
	export objects	•				As PDML XML	. I.	240		ESP		176
	Print			Ctrl+P			- I.	240		ESP		176
				carri		A375014	J	240		ESP		176
	Quit			Ctrl+Q	149	192.16	8.28	240		ESP		176
-	24	+/ >>	.000902	192.100.2	. 149	192.16	8.28	240		ESP		176
	54	18 55	.608962	192.168.2	3.149	192.16	8.28	240		ESP		176

Select **Captured** and **Range** and in the **Range** field type the range from the first relevant packet to the last relevant packet.

Enter a file name in the **File Name** field and click **Save**.

📕 Wireshark • E	xport Packet Disse	ctions					×
Save in:	Desktop		\sim	G 🤌	ڬ 📂	•	
Quick access Desktop Libraries	Name	^ No items	s match your s	Status search.		Date mo	dified
Network	< File name: Save as type:	CAP1_slice CSV (Comma Separa	ated Values sum	nmary) (*.c	∽ s1 ∽	Ci	> Save ancel Help
	Packet Range						Pack
	 All packets Selected pack Marked packets First to last material Range: 451- Remove Ignore 	k et ets rked 550 ed packets		Captured 880 1 0 100	ODisp	layed 100 1 0 100 0	 ✓ Pa ✓ Pa ✓ Pa ✓ Pa ✓ Pa ✓ Pa

Repeat the same process on capture 2 for the relevant packets.

 \times Wireshark - Export Packet Dissections Save in: E Desktop 🗿 🤌 📂 🛄 🕶 \checkmark × Date modified Name Status No items match your search. Quick access Desktop Libraries This PC < > Network CAP2_slice ~ Save File name: Cancel CSV (Comma Separated Values summary) (".csi ~ Save as type: Help Packet Range Packe O Displayed Captured Pa Pa All packets 904 904 \mathbb{P} Selected packet 1 1 Pa Pa Marked packets A First to last marked Pa Range: 463-564 102 Ea Ea Remove Ignored packets

Open both CSV files in Microsoft Excel.

On the source capture CSV, save as an XLSX format.

Save As		
L Recent	↑	
Cisco	Excel Workbook (*.xlsx)	🔛 Save

At the bottom of the screen, select the + symbol to add another sheet. Name it CAP2_slice.

j.	485	55.51497 192.168.2	192.168.28 ESP	176	340	27	ESP (SPI=0x040001dc)	
•	486	55.51697 192.168.2	192.168.28 ESP	176	341	27	ESP (SPI=0x040001dc)	
1	487	55.51796 192.168.2	192.168.28 ESP	176	342	27	ESP (SPI=0x040001dc)	
-	Þ	CAP1_slice	÷					

Open the CAP2 CSV file and press CTRL + a to select all and CTRL + c to copy it.

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	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=	0x040001dd	
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=	0x040001dc	
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=	0x040001dd	
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	
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	

Navigate to the **CAP1_slice.xlsx** file and on the second tab for CAP2_slice, paste (**CTRL + v**) the copied information into the cell **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.	A .	= = =		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	(+)								

1					-		~						-	
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info		Seque	ence N
2	463	60.99901	192.168.23	192.168.28	ESP	176	306	27			ESP	(SPI=0	x0400	01dc)
3	464	61.00301	192.168.23	192.168.28	ESP	176	307	27			ESP	(SPI=0	x0400	01dc)
4	465	61.00506	192.168.23	192.168.28	ESP	176	308	27			ESP	(SPI=0	x0400	01dc)
5	466	61.00706	192.168.23	192.168.28	ESP	176	309	27			ESP	(SPI=0	x0400	01dc)
6	467	61.00905	192.168.23	192.168.28	ESP	176	310	27			ESP	(SPI=0	x0400	01dc)
7	468	61.01006	192.168.23	192.168.28	ESP	176	311	27			ESP	(SPI=0	x0400	01dc)
8	469	61.01105	192.168.23	192.168.28	ESP	176	312	27			ESP	(SPI=0	x0400	01dc)
9	470	61.01305	192.168.23	192.168.28	ESP	176	313	27			ESP	(SPI=0	x0400	01dc)
10	471	61.01406	192.168.23	192.168.28	ESP	176	314	27			ESP	(SPI=0	x0400	01dc)
11	472	61.01606	192.168.23	192.168.28	ESP	176	315	27			ESP	(SPI=0	x0400	01dc)
12	473	61.01806	192.168.23	192.168.28	ESP	176	316	27			ESP	(SPI=0	x0400	01dc)
13	474	61.02106	192.168.23	192.168.28	ESP	176	317	27			ESP	(SPI=0	x0400	01dc)
14	475	61.02205	192.168.23	192.168.28	ESP	176	318	27			ESP	(SPI=0	x0400	01dc)
15	476	61.02306	192.168.23	192.168.28	ESP	176	319	27			ESP	(SPI=0	x0400	01dc)
16	477	61.02506	192.168.23	192.168.28	ESP	176	320	27			ESP	(SPI=0	x0400	01dc)
17	478	61.02605	192.168.23	192.168.28	ESP	176	321	27			ESP	(SPI=0	x0400	01dc)
18	479	61.02805	192.168.23	192.168.28	ESP	176	322	27			ESP	(SPI=0	x0400	01dc)
19	480	61.02906	192.168.23	192.168.28	ESP	176	323	27			ESP	(SPI=0	x0400	01dc)
20	481	61.02906	192.168.23	192.168.28	ESP	176	324	27			ESP	(SPI=0	x0400	01dc)
21	482	61.03005	192.168.23	192.168.28	ESP	176	325	27			ESP	(SPI=0	x0400	01dc)
22	483	61.03206	192.168.23	192.168.28	ESP	176	326	27			ESP	(SPI=0	x0400	01dc)
23	484	61.03306	192.168.23	192.168.28	ESP	176	327	27			ESP	(SPI=0	x0400	01dc)
24	485	61.03505	192.168.23	192.168.28	ESP	176	328	27			ESP	(SPI=0	x0400	01dc)
25	486	61.03606	192.168.23	192.168.28	ESP	176	329	27			ESP	(SPI=0	x0400	01dc)
26	487	61.03905	192.168.23	192.168.28	ESP	176	330	27			ESP	(SPI=0	x0400	01dc)
27	488	61.04105	192.168.23	192.168.28	ESP	176	331	27			ESP	(SPI=0	x0400	01dc)
28	489	61.04206	192.168.23	192.168.28	ESP	176	332	27			ESP	(SPI=0	x0400	01dc)
29	490	61.04406	192.168.23	192.168.28	ESP	176	333	27			ESP	(SPI=0	x0400	01dc)
30	491	61.04606	192.168.23	192.168.28	ESP	176	334	27			ESP	(SPI=0	x0400	01dc)
31	492	61.06305	192.168.23	192.168.28	ESP	176	335	27			ESP	(SPI=0	x0400	01dc)
32	493	61.06505	192.168.23	192.168.28	ESP	176	336	27			ESP	(SPI=0	x0400	01dc)
33	494	61.06705	192.168.23	192.168.28	ESP	176	337	27			ESP	(SPI=0	x0400	01dc)
34	495	61.06905	192.168.23	192.168.28	ESP	176	338	27			ESP	(SPI=0	x0400	01dc)
35	496	61.07105	192.168.23	192.168.28	ESP	176	339	27			ESP	(SPI=0	x0400	01dc)
36	497	61.07105	192.168.23	192.168.28	ESP	176	340	27			ESP	(SPI=0	x0400	01dc)
7	400	61 07205	100 160 00	103 160 30	FCD	176	241	77			CCD.	(001-0		01 do

Navigate back to **CAP1_slice** sheet and make a new column called **COMPARE_ESP_SEQUENCE**.

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	102 160 2	103 160 30	ren	176	200	27			ren (eni-	0.000001d	4					

As the ESP Sequence number is in Column G, compose a VLOOKUP command as shown to compare the two sheets to ensure that everything in Column G on the source is in Column G on the destination.

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

•	×	~	f _x	=1	F(ISNA <mark>(</mark> VLO	OKUP(G2,	CAP2_slice	G:G,1,FA	LSE)),"MISS	ING","PRE	SENT")														
в		с	1	D	E	F	G	н	1	J.	к	L	м	N	0	Р		Q	R	s	т	U	v	w	x
ime	S	ource	De	stinat	ic Protocol	Length	ESP Seque	Different	i Source Po	Destinati	c Info	Sequence	Number		COMPA -	ESP_SI	QUEN	ICE							
55.441	96 1	92.168.2	19	2.168.2	28 ESP	176	306	27	1		ESP (SPI:	=0x040001dd	;)		=IF(ISNA(VLOOKU	P(G2,	CAP2_s	lice!G:G,	I,FALSE)),"	MISSING","	PRESENT")			
55.445	98 1	92.168.2	19	2.168.2	2EESP	176	307	27	1		ESP (SPI=	=0x040001dd	:)			T									

After Enter is selected the word PRESENT is displayed. This means that the packet with ESP Sequence **306** is present in the second sheet. This is significant because it means that the packet

made it from the source to the destination.

1 No. Time Source Destinatic Protocol Length ESP Seque Differenti Source Po Destinatic Info Sequence Number COMPA ⊆ ESP_SEQUEN				
2 451 55 44105 102 159 25102 159 25 55D 175 205 27 55D (5DI-0v040001de) DESENT	I N	P_SEQUEN	ENCE	
2 431 53.44150 152.108.22 152.108.22 ESP 170 500 27 ESP (SPI=0X0400010C) PRESENT	2			
3 452 55.44598 192.168.22 192.168.22 ESP 176 307 27 ESP (SPI=0x040001dc)	3			

Select Column **O** Row 2 and hover over the bottom right corner of the green box around that cell.



Select and hold, and drag the mouse down to copy this formula to the bottom of the cells which have values.

B	C	D	E	F	G	н	1.1	J	K	L	M	N	0	Ρ	Q	R	S	т	U	V	W
Time	Source	Destinat	ic Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPARE	ESP_SEC	UENCE						
51 55.44	196 192.168.	2:192.168.2	28 ESP	176	306	27			ESP (SPI	=0x040001d	c)		PRESENT								
52 55.44	598 192.168.	2:192.168.2	28 ESP	176	307	27			ESP (SPI	=0x040001dd	c)										
53 55.44	897 192.168.	2:192.168.2	2EESP	176	308	27			ESP (SPI	=0x040001d	c)										
54 55.45	097 192.168.	2:192.168.2	28 ESP	176	309	27			ESP (SPI	=0x040001d	c)		_								
55 55.45	296 192.168.	2:192.168.2	28 ESP	176	310	27			ESP (SPI	=0x040001dd	c)										
56 55.45	496 192.168.	2:192.168.2	28 ESP	176	311	27			ESP (SPI	=0x040001d	c)										
57 55.45	597 192.168.	2:192.168.2	28 ESP	176	312	27			ESP (SPI	=0x040001dd	c)										
55.45	698 192.168.	2: 192.168.2	28 ESP	176	313	27			ESP (SPI	=0x040001dd	c)										
59 55.45	/97 192.168.	2: 192.168.2	RESP	176	314	27			ESP (SPI	=0x040001dd	c) -)										
50 55.45	598 192.108. 107 103 169	2: 192.108.2	CESP CESP	170	315	27			ESP (SPI	=0x040001dd											
52 55 46	197 192.108. 207 102 169	2: 192.100.2	CESP CESD	170	217	27			ESP (SPI	-0x040001dd	-)										
53 55.46	596 192.168	2:192.168.2	25 ESP	176	318	27			ESP (SPI	=0x040001dd	-) c)										
54 55.46	697 192.168.	2: 192.168.2	ESP	176	319	27			ESP (SPI	=0x040001d	c)										
55 55.46	796 192.168.	2: 192.168.2	2EESP	176	320	27			ESP (SPI	=0x040001d	c)										
56 55.46	996 192.168.	2: 192.168.2	2EESP	176	321	27			ESP (SPI	=0x040001dd	c)										
57 55.47	097 192.168.	2: 192.168.2	2EESP	176	322	27			ESP (SPI	=0x040001dd	c)										
333	55.00257	172.100.2	172.100.	20EOP		110	374	4	/		E.3	r (sri-u	X0400010	-)		PN	SEIVI				
540	55.60496	192.168.2	192.168.	.28 ESP		176	395	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
541	55.60596	192.168.2	192.168.	28 ESP		176	396	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
542	55.60696	192.168.2	192.168.	28 ESP		176	397	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
543	55.60696	192.168.2	192.168.	28 ESP		176	398	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
544	55.60696	192.168.2	192.168.	28 ESP		176	399	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
545	55,60796	192.168.2	192.168.	28 ESP		176	400	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
546	55,60796	192,168,2	192,168	28 ESP		176	401	2	7		ES	P (SPI=0	x040001d	c)		PR	SENT				
547	55 60896 1	192 168 2	192 168	25 ESD		176	402	2	7		ES	D (SDI-0	v040001d	c)		DR	SENT			-	-
549	55 60896 1	192.100.2	192.100.	20 550		176	402	2	7	_	5	D (SDI-0	v040001d	c)		DPI	SENT				
540	55 60007	102 160 2	192.100.	2000		176	403	2	7		50		v040001d			DB	SENT			-	-
549	55.00997	192.108.2	192.108.	20 500		170	404	2			ES	P (SPI=0				PRI	SENT				\rightarrow
550	55.61096	192.168.2	192.168.	28 ESP		176	405	2	/		ES	P (SPI=0	x040001d	c)	_	PRI	SENT	-		-	\rightarrow

Scroll back to the top of the sheet and click the **COMPARE_ESP_SEQUENCE**. Then select **Sort & Filter**.

] onal ng ~	Format as Table ~	Normal Neutral	Bad Calculation	Good Check Cell	~	Insert v	Delete	Format	∑ Auto ↓ Fill ~ ♦ Clear	Sum '	× AZ Z Sort & Filter ∼	Find & Select 1
_		Styl	es				Cells				in ing	-
V	O	P (RE_ESP_SEQUENC	R	S	T	U	V	V	V	x	Y	

Choose Filter from the dropdown menu.



A dropdown menu appears on the **COMPARE_ESP_SEQUENCE** column.

М	Ν	0	Р	
lumber		COMPA 🗵	ESP_SEQ	UEN
		PRESENT		
		PRESENT		
		PRESENT		

Click the dropdown menu on the **COMPARE_ESP_SEQUENCE** heading. Notice that in this example, the only value shown is **PRESENT**. This means all the packets are present in both captures.

к	L	м	N	0	
c Info	Sequence	Number		COMPA -	ESI
ES ^A _Z ↓	Sort A to Z				
ES ZI	C + 7 + A				
ES A↓	3 <u>o</u> rt 2 to A				
ES S	or <u>t</u> by Color			>	
ES S	heet <u>V</u> iew			>	
ES		1001/01			
ES 1×	Clear Filter Fro	om "COMPA	RE_ESP_SEQ	UENCE.	
ES F	ilter by Color			>	
ES T	ext <u>F</u> ilters			>	
ES	lanch			0	
ES	bearch			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
ES	✓ (Select A	AII) T			
ES	PRESEN	1			
ES					
EC.					

To create a problematic example, delete 10 packets from the CAP2_slice, to demonstrate how this would work in a test where some missed packets are missing.

11	4/2	01.01000 192.108.2:	192.108.2	ESP	1/0	312	21	ESP (SPI=0X0400010C)	
12	473	61.01806 192.168.23	192.168.2	ESP	176	316	27	ESP (SPI=0x040001dc)	
13	474	61.02106 192.168.23	192.168.2	ESP	176	317	27	ESP (SPI=0x040001dc)	
14	475	61.02205 192.168.23	192.168.2	ESP	176	318	27	ESP (SPI=0x040001dc)	
15	476	61.02306 192.168.23	192.168.2	ESP	176	319	27	ESP (SPI=0x040001dc)	
16	477	61.02506 192.168.23	192.168.2	ESP	176	320	27	ESP (SPI=0x040001dc)	
17	478	61.02605 192.168.23	192.168.2	ESP	176	321	27	ESP (SPI=0x040001dc)	
18	479	61.02805 192.168.23	192.168.2	ESP	176	322	27	ESP (SPI=0x040001dc)	
19	480	61.02906 192.168.23	192.168.2	ESP	176	323	27	ESP (SPI=0x040001dc)	
20	481	61.02906 192.168.23	192.168.2	ESP	176	324	27	ESP (SPI=0x040001dc)	
21	482	61.03005 192.168.23	192.168.2	ESP	176	325	27	ESP (SPI=0x040001dc)	
22	483	61.03206 192.168.23	192.168.2	ESP	176	326	27	ESP (SPI=0x040001dc)	
23	484	61.03306 192.168.23	192.168.2	ESP	176	327	27	ESP (SPI=0x040001dc)	
24	485	61.03505 192.168.23	192.168.2	ESP	176	328	27	ESP (SPI=0x040001dc)	
25	486	61.03606 192.168.23	192.168.2	ESP	176	329	27	ESP (SPI=0x040001dc)	
26	487	61.03905 192.168.23	192.168.2	ESP	176	330	27	ESP (SPI=0x040001dc)	
27	488	61.04105 192.168.23	192.168.2	ESP	176	331	27	ESP (SPI=0x040001dc)	
28	489	61.04206 192.168.23	192.168.2	ESP	176	332	27	ESP (SPI=0x040001dc)	
29	490	61.04406 192.168.23	192.168.2	ESP	176	333	27	ESP (SPI=0x040001dc)	
30	491	61.04606 192.168.23	192.168.2	ESP	176	334	27	ESP (SPI=0x040001dc)	
31	492	61.06305 192.168.23	192.168.2	ESP	176	335	27	ESP (SPI=0x040001dc)	
32	493	61.06505 192.168.23	192.168.2	ESP	176	336	27	ESP (SPI=0x040001dc)	
33	494	61.06705 192.168.23	192.168.2	ESP	176	337	27	ESP (SPI=0x040001dc)	
34	495	61.06905 192.168.23	192.168.2	ESP	176	338	27	ESP (SPI=0x040001dc)	
35	496	61.07105 192.168.23	192.168.2	ESP	176	339	27	ESP (SPI=0x040001dc)	
36	497	61.07105 192.168.23	192.168.2	ESP	176	340	27	ESP (SPI=0x040001dc)	
37	498	61.07205 192.168.23	192.168.2	ESP	176	341	27	ESP (SPI=0x040001dc)	
38	499	61.07605 192.168.23	192.168.2	ESP	176	342	27	ESP (SPI=0x040001dc)	
-	•	CAP1_slice CA	P2_slice	+					

Navigate back to **CAP1_slice** sheet and now it is seen that there are 10 packets missing.

	55.45757 152.100.2, 152.100.2, CS	110	J 14	21	231 (311-000100200)	THESE IT	
460	55.45898 192.168.23 192.168.28 ESP	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 192.168.2: 192.168.2ESP	176	318	27	ESP (SPI=0x040001dc)	MISSING	
464	55.46697 192.168.2: 192.168.2ESP	176	319	27	ESP (SPI=0x040001dc)	MISSING	
465	55.46796 192.168.2: 192.168.2ESP	176	320	27	ESP (SPI=0x040001dc)	MISSING	
466	55.46996 192.168.2: 192.168.2ESP	176	321	27	ESP (SPI=0x040001dc)	MISSING	
467	55.47097 192.168.2: 192.168.2ESP	176	322	27	ESP (SPI=0x040001dc)	MISSING	
468	55.47198 192.168.2: 192.168.2ESP	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 192.168.2: 192.168.2ESP	176	325	27	ESP (SPI=0x040001dc)	MISSING	
471	55.47597 192.168.2: 192.168.2ESP	176	326	27	ESP (SPI=0x040001dc)	MISSING	
472	55.47697 192.168.2: 192.168.2ESP	176	327	27	ESP (SPI=0x040001dc)	MISSING	
473	55.47896 192.168.2: 192.168.2ESP	176	328	27	ESP (SPI=0x040001dc)	PRESENT	
474	55.48096 192.168.23 192.168.28 ESP	176	329	27	ESP (SPI=0x040001dc)	PRESENT	

When the dropdown menu is selected on the **COMPARE_ESP_SEQUENCE** column, now it is seen that there are **MISSING** packets also. This can be toggled to view only the **MISSING** packets.

	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	Clear Filter From "COMPARE_ESP_SEQUENCE"										
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 .:						



Now only the missing packets are shown in the Excel sheet.

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

Related Information

- <u>Cisco Embedded Packet Capture</u>
- <u>Technical Support & Documentation Cisco Systems</u>