SD-WANのWANでのパケット損失の確認と特定

内容

概要
前提条件
要件
使用するコンポーネント
背景
トラブルシューティングプロセス
プロセスの概要
目的のトラフィックをDSCPでマーキングする
組み込み型キャプチャによるトラフィックのキャプチャ
Wiresharkによる分析
ESPシーケンスによる目的のトラフィックのフィルタリング
関連情報

概要

このドキュメントでは、WAN全体でトラフィックが失われたが、SD-WANエッジでドロップが見 られない場合に、データを識別して収集する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Software-Defined Wide Area Network(SD-WAN)
- 組み込みパケットキャプチャまたはvManageパケットキャプチャ
- Wireshark
- Microsoft Excel

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C8000Vバージョン17.03.04
- vManageバージョン20.3.4
- Wiresharkバージョン2.6.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景

この課題を解決するために、このドキュメントで説明する手順では、特定のトラフィックを DiffServコードポイント(DSCP)でマークして目的のパケットを識別する方法を示します。この値 は内部パケットヘッダーからIPsecヘッダーにコピーされるため、DSCPを使用してトラフィック を識別できます。目的のパケットが特定されたら、2つのWANキャプチャ間でトラフィックを照 合し、送信元から宛先までのトラフィックを確認する方法を示します。

このトラブルシューティングテクニックを示すために、2つの単一のルータサイトを使用します。 この例では、図に示すように、10.0.0.10から10.0.2.10へのICMPトラフィックが100回のpingの形 式で送信されます。この例では損失はありませんが、損失を特定するために損失がある場合は、 この同じトラブルシューティングテクニックを使用します。



トラブルシューティングプロセス

プロセスの概要

- WAN上でトレースされるトラフィックの場合、未使用のDSCP値を使用してトラフィックを マーキングするには、アクセスリスト(ACL)(または集中型ポリシー)が必要です。この例 では、DSCP 27が使用されます。
- トラフィックがマーキングされると、組み込みパケットキャプチャが使用され、送信元ルー タと宛先ルータのトランスポートインターフェイス上のパケットがキャプチャされます。

注:vManageパケットキャプチャも使用できますが、データの上限は5 MBまたはランタイムの場合は5分です。

- 1. キャプチャが取得されたら、Wiresharkで開いて表示します。
- 2. Wiresharkでフィルタを適用して、必要なパケットを表示し、比較します。
- 3. Microsoft Excelは、精度を確保するために大きなキャプチャに使用されます。

目的のトラフィックをDSCPでマーキングする

例Isのようなアクセスリストは、送信元ルータ(この例ではcEdge1)で設定され、次に示すよう にルータ設定のSD-WAN部分のインターフェイスに適用されます。

オプションのカウンタを適用して、トラフィックが期待どおりにポリシーにヒットすることを確

認します。これは、show sdwan policy access-list-countersコマンドで確認できます。

```
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
!
default-action accept
sdwan
interface GigabitEthernet3
access-list mark_dscp_27 in
組み込み型キャプチャによるトラフィックのキャプチャ
```

注:WANを通過する暗号化パケットをキャプチャするようにCisco IOS XEで埋め込みパケットキャプチャを設定する方法については、「<u>Cisco IOSおよびCisco IOS XEの埋め込みパケ</u> ットキャプチャの設定例」に移動してください。

注:EPCのレート制限が1000 PPSを超える可能性があるため、WAN上のEPCを制限するに はACLを使用する必要があります。

例

この例では、トラフィックは送信元から宛先への方向でのみチェックされるため、ACLは cEdge1とcEdge3で設定されます。

注:WAN IPアドレスは、キャプチャをフィルタリングするために使用されます。トラフィッ クが通るパスを特定するために使用できる複数の出力があり、ACLフィルタに対して正しい WAN IPを特定できます。この出力の生成に使用できるコマンドは、show sdwan app-fwd cflowd flowsおよびshow sdwan policy service pathです。デバッグ条件については、「<u>条件</u> 付きパケットトレース」に移動してください。

ip access-list extended CAP-Filter

10 permit ip host 192.168.23.149 host 192.168.28.240

この時点で、両方のルータでキャプチャが開始され、100回のpingがオーバーレイ経由で送信され ます。

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms 両方のルータからキャプチャが停止および収集された後、キャプチャを表示するにはWiresharkで 開く必要があります。

Wiresharkによる分析

0 00 50 56 84 e2 b7 00 50 56 84 af 45 08 00 45 6c ··PV····P V··E··E1

WiresharkでcEdge1キャプチャを開くと、すべてのトラフィックが暗号化されていることが確認 でき、どのパケットが送信されたpingであるかを容易に判断できません。

📕 САР.рсар										- o
File Edit View Go Capture	Analyze Statistics	Telephony Wireless Tool	ls Help							
	0.00000									
	1.4 4 4 18 18 1	· 🗶 🔲 a a a a :	2							
Apply a display filter <ctrl-></ctrl->										
No. 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	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	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	192.168.28.240	UDP	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 + 12407 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 + 12407 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	UOP	176	Default				12386 + 12407 Len=134	
35 14.175985	192.168.23.149	192.168.28.240	UOP	176	Detault				12586 + 12407 Len=134	
36 14.176977	192.168.23.149	192.168.28.240	UOP	176	Default				12300 + 12407 Len=134	
37 14.176977	192.168.23.149	192.168.28.240	UOP	176	Default				12386 + 12407 Len=134	
38 14.178991	192.168.23.149	192.168.28.240	UOP	176	Derault				12300 + 12407 Len=134	
39 14.188998	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	

表示フィルタip.dsfield.dscp == 27を使用してこのキャプチャをフィルタリングすると、画面の下 部に100個のパケットだけが表示され、DSCP列の値がすべて27であることが分かります。

	*****	Profession .	Protocol 1		All weeks to be from the first		and the first	for a second second	14
Time	Source	Destnation	Protocol Leng	h ESP Sequence	Differentiated Services Codepoint	Spurce Port De	estination Port	Sequence Number	into
451 55.441963	192.168.25.149	192.168.28.240	009	176	27	-			12360 + 12407 Len+134
432 33,443976	192.100.23.149	192.100.20.240	000	176	27				12300 * 12407 Len=134
453 55.448966	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
454 55.450965	192.168.23.149	192.168.28.240	009	176	27				12386 + 12487 Len+134
455 55.452964	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
450 55.454903	192.168.23.149	192.168.28.240	UDP	176	27				12380 - 12407 Len=134
457 55.455970	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
458 55.450977	192.168.23.149	192.108.28.240	000	176	27				12360 + 12407 Len+134
459 55.457968	192.168.25.149	192.168.28.240	000	176	27				12586 * 12487 Len*154
468 55.458975	192.168.23.149	192.168.28.240	000	176	27				12386 + 12487 Len+134
461 55.461966	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
462 55.463965	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
463 55.465964	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
464 55.466971	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
465 55.467962	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
466 55.469961	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
467 55.470968	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
468 55.471975	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
469 55.472967	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
470 55.474966	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
471 55.475973	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
472 55.476965	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
473 55.478963	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
474 55.480962	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
475 55.481969	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
476 55.484975	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
477 55.485967	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
478 55.487966	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
479 55.488973	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
480 55.491963	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
481 55.508961	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
482 55.510959	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
483 55.511966	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
484 55.513965	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
485 55.514972	192.168.23.149	192.168.28.240	UDP	176	27				12386 → 12407 Len=134
486 55.516971	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
487 55.517963	192.168.23.149	192.168.28.240	UDP	176	27				12386 + 12407 Len=134
	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
488 55.523959	192.168.23.149	192.168.28.240	UDP	176	27				12386 - 12407 Len=134
488 55.523959 489 55.524966									

DSCP値がWAN全体で維持される場合は、宛先キャプチャで同じフィルタを使用できます。

また、パブリックインターネット接続でDSCP値がクリアされる状況など、このような状況は発 生しません。

Packets: 880 Displayed: 200 11.4%)

ESPシーケンスによる目的のトラフィックのフィルタリング

いずれの場合も、トラフィックはESPシーケンス番号で識別できます。

パケット内のESPシーケンス番号を表示するには、キャプチャを右クリックし、次に示すように [Decode] を選択します。

		12386
		12386
Mark/Unmark Packet	Ctrl+M	12386
	C. I. D.	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 miter		12386
Colorize Conversation	•	12386
SCTP	•	12386
Follow	•	12386
Follow		12386
Copy	•	12386
		12386
Protocol Preferences	•	12386
Decode Ac		12386
Decode As		12386
Show Packet in New Window	N	12386

[Current field]ドロップダウンメニューを選択し、そのフィールドに**UDPENCAP**と入力するか、ド ロップダウンから選択します。



V	Vi	in	esl	har	k	D	ec	0	d	e	As.
٠	•		-	101	~	-	~	v	u	-	~

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

×

これが完了したら、[OK] を選択します。

	-									
4	Wiresh	ark • De	code As							×
	Field	Value	Туре	Default	Current					
	UDP port	12386	Integer, base 10	(none)	UDPENCAP					
	+ -	ъ (R							
			-							
						OK	Save	Copy from	Cancel	Help
_										

Wiresharkの[Packet Details]セクションで、パケットの[Encapsulating Security Payload] 部分を展開し、**ESPシーケンス**を表示します。

,	479 55 488973 192 168 23 1	149 192 1	68 78 740	FSP	176
<u>،</u>					
>	Frame 464: 176 bytes on wire (1408 bi	ts), 176 bytes	captured (1408	bits)	
>	Ethernet II, Src: VMware_84:af:45 (00	:50:56:84:af:45	5), Dst: VMware_	84:e2:b7 (00:50	:56:84:e2:b7)
>	Internet Protocol Version 4, Src: 192	.168.23.149, Ds	st: 192.168.28.2	240	
>	User Datagram Protocol, Src Port: 123	86, Dst Port: 1	12407		
	UDP Encapsulation of IPsec Packets				
Ν	Encapsulating Security Payload				
	ESP SPI: 0X0400010C (67109340)				
	ESP Sequence: 319				

[ESP Sequence] を右クリックし、[apply as column] を選択します。これにより、Wireshark画面 の上部にある[Packet List]セクションに、ESPシーケンスが列として表示されます。

		00.20.240	6.51
456 55	.4		ESP
457 55	Expand Subtrees		ESP
458 55	Collapse Subtrees		ESP
459 55	- 4 Expand All		ESP
460 55	Collapse All		ESP
461 55			ESP
462 55	• Apply as Column	Ctrl+Shift+I	ESP
463 55			ESP
464 55	Apply as Filter	•	ESP
465 55	Prepare as Filter	· · · · ·	ESP
466 55	Conversation Filter		ESP
467 55			ESP
468 55	Colorize with Filter	•	ESP
469 55	-4 Follow	→	ESP
470 55			ESP
471 55	-4 Copy	•	ESP
472 55	.4 Shaw Dasket Brites	Chill Chiffy O	ESP
473 55	2 Show Packet Bytes	Ctri+Shift+O	ESP
474 55	Export Packet Bytes	Ctrl+Shift+X	ESP
	MGH: Deate cal Daga		
Frame 464: 176 by	yt	08	bits)
Ethernet II, Src:	Filter Field Reference	re	_84:e2:b7 (0
Internet Protocol	1 Protocol Preferences	▶ 8.	240
User Datagram Pro	pt		
UDP Encapsulation	n Decode As	Ctrl+Shift+U	
Encapsulating Sec	Cu Go to Linked Packet		
ESP SPT+ 0x040	ARE SHOW LINK d Packet in New Window		
ESP Sequence:	31		

注:cEdge1上のパケットのESP SPIは**0x040001dc**です。これは、宛先キャプチャのフィルタ に使用されます。 > 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

宛先キャプチャを開き、UDPENCAPとしてデコードする手順を繰り返し、パケット内のESPシー ケンス番号を表示します。

パケットにESPシーケンス番号が表示されると、最初のキャプチャのESP SPIを2番目のキャプチャのフィルタとして使用して、そのSPI内で目的のトラフィックに一致するトラフィックのみを 表示できます。

両方とも一致するパケットシーケンス番号にDSCP 27がマークされていることに注意してください。



この比較は、Wiresharkで手動で行うことも、Microsoft Excelを使用して行うこともできます。

Microsoft Excelを使用して比較するには、両方のキャプチャに含まれるパケットだけを含むよう に両方のキャプチャをスライスする必要があります。

ソースキャプチャでは、最初に関連するパケットにESPシーケンス306が含まれており、これが パケット番号451に対応しています。

CAP.pcap						\times
File Edit View Go Capture Analyze Stati	stics Telephony Wireless Tools	; Help				
🛋 🔳 🖉 💿 📙 🛅 🗙 🖆 I 🍳 👄 🕾	🝸 🕹 📃 🔳 🍳 🍳 🖳					
ip.dsfield.dscp == 27					\times	• +
No. Time Source	Destination	Protocol	Length	ESP Sequence	Different	· ^
451 55.441963 192.168.23.1	19 192.168.28.240	ESP	176	300	5 27	
452 55.445976 192.168.23.1	192.168.28.240	ESP	176	30	7 27	
453 55.448966 192.168.23.1	192.168.28.240	ESP	176	308	3 27	
454 55.450965 192.168.23.1	192.168.28.240	ESP	176	309	9 27	
455 55.452964 192.168.23.1	192.168.28.240	ESP	176	310	3 27	
456 55.454963 192.168.23.1	192.168.28.240	ESP	176	31:	L 27	
457 55.455970 192.168.23.1	192.168.28.240	ESP	176	312	2 27	
458 55.456977 192.168.23.1	19 192.168.28.240	ESP	176	313	3 27	

ソースキャプチャの最後の関連パケットはESPシーケンス405で、パケット番号550です。

517 551000502		10211001201210		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	
						~
					<pre>></pre>	

宛先キャプチャでは、最初の関連パケットはESPシーケンス306による送信元キャプチャに対応しますが、このキャプチャではパケット463です。

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

最後の関連パケットもESPシーケンス405に含まれており、これはパケット564です。

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

最初のキャプチャは、関連するパケットのみを含むようにスライスする必要があります。

[File] > [Export Packet Dissections] > [As CSV...]に移動します。

CAP.pcap

Edit View Go Capture	e Analyze St	atisti	s Telephony \	Wireless Tools	Help		
Open	Ctrl+O	E 7	5 🕭 🥃 🔳 (Ð. Q. Q. 🎹			
Open Recent	•	F					
Merge		F	Destination		Destand	1 and the	-
incigen.			Destination	ו	Protocol	Length	E
Import from Hex Dump		149	192.168	.28.240	ESP	176	5
Close	Ctrl+W	149	192.168	.28.240	ESP	176	5
		149	192.168	.28.240	ESP	176	5
Save	Ctrl+S	149	192.168	.28.240	ESP	176	5
Save Ar	Ctrl. Shift, S	149	192.168	.28.240	ESP	176	5
Save As	Cur+Shirt+S	149	192.168	.28.240	ESP	176	5
File Set	•	149	192.168	.28.240	ESP	176	5
- ne oet		149	192.168	.28.240	ESP	176	5
Export Specified Packets		149	192.168	.28.240	ESP	176	5
Export Packet Dissections	•		As Plain Text	.240	ESP	176	5
5			A	1.240	ESP	176	5
Export Packet Bytes	Ctrl+Shift+X		As CSV	.240	ESP	176	5
Export PDUs to File			As "C" Arrays	.240	ESP	176	5
Export TLS Session Keys				. 240	ESP	176	5
5			As PSML XML	.240	ESP	176	5
Export Objects	•		As PDML XML	. 240	ESP	176	5
Drint	Chally D			.240	ESP	176	5
Print	Cui+P		AS JOUN		ESP	176	5
Ouit	Ctrl+O	149	192.168	.28.240	ESP	176	5
04/ 00.00090Z	192.100.20	149	192.168	.28.240	ESP	176	5
548 55.608962	192.168.23.	149	192.168	.28.240	ESP	176	5
	EditViewGoCaptureOpenOpen RecentImport from Hex DumpImport from Hex DumpCloseSaveSaveSave AsFile SetSave AsExport Specified PacketsExport Packet DissectionsExport Packet BytesExport PDUs to FileExport TLS Session KeysExport ObjectsPrintQuitS47 55.000502548 55.608962	EditViewGoCaptureAnalyzeStOpenCtrl+ OOpen RecentMergeImport from Hex DumpCloseCtrl+ WCloseCtrl+ SSaveCtrl+ SSave AsCtrl+ SFile Set </td <td>EditViewGoCaptureAnalyzeStatisticOpenCtrl+OImport from RecentImport from Hex DumpImport from Hex DumpImport from Hex DumpCloseCtrl+WImport from Hex DumpImport from Hex DumpImport from Hex DumpCloseCtrl+SImport from Hex DumpImport from Hex DumpSaveCtrl+SImport from Hex DumpImport from Hex DumpFile SetImport from Hex DumpCtrl+Shift+XImport from Hex DumpExport Packet DissectionsImport from Hex DumpImport from Hex DumpImport from Hex DumpExport PDUs to FileExport Packet BytesCtrl+PImport from Hex DumpQuitCtrl+QImport from Hex DumpImport from Hex DumpDetermineCtrl+QImport from Hex DumpImport from Hex DumpSave S5.608962192.168.23.149Import from Hex DumpImport from Hex Dump</td> <td>EditViewGoCaptureAnalyzeStatisticsTelephonyVOpenCtrl+OImport from RecentImport from Hex DumpImport from Hex Dump<td>Edit View Go Capture Analyze Statistics Telephony Wireless Tools Open Ctrl+ O</td><td>Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+ 0 Import Import Import Import Import Import Import Import Protocol Import from Hex Dump Ctrl+ W 149 192.168.28.240 ESP Close Ctrl+ W 149 192.168.28.240 ESP Save As Ctrl+ S 149 192.168.28.240 ESP Save As Ctrl+ Shift+S 149 192.168.28.240 ESP File Set Ctrl+Shift+S 149 192.168.28.240 ESP Export Specified Packets Ctrl+Shift+S 149 192.168.28.240 ESP Export Packet Dissections As Plain Text .240 ESP Export Packet Bytes Ctrl+Shift+X As CSV .240 ESP Export Packet Bytes Ctrl+Shift+X As PDML XML .240 ESP Export Plus to File As PDML XML .240 ESP .240 ESP As PDML XML .240 ESP<</td><td>Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+O Ctrl+O Image: Imag</td></td>	EditViewGoCaptureAnalyzeStatisticOpenCtrl+OImport from RecentImport from Hex DumpImport from Hex DumpImport from Hex DumpCloseCtrl+WImport from Hex DumpImport from Hex DumpImport from Hex DumpCloseCtrl+SImport from Hex DumpImport from Hex DumpSaveCtrl+SImport from Hex DumpImport from Hex DumpFile SetImport from Hex DumpCtrl+Shift+XImport from Hex DumpExport Packet DissectionsImport from Hex DumpImport from Hex DumpImport from Hex DumpExport PDUs to FileExport Packet BytesCtrl+PImport from Hex DumpQuitCtrl+QImport from Hex DumpImport from Hex DumpDetermineCtrl+QImport from Hex DumpImport from Hex DumpSave S5.608962192.168.23.149Import from Hex DumpImport from Hex Dump	EditViewGoCaptureAnalyzeStatisticsTelephonyVOpenCtrl+OImport from RecentImport from Hex DumpImport from Hex Dump <td>Edit View Go Capture Analyze Statistics Telephony Wireless Tools Open Ctrl+ O</td> <td>Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+ 0 Import Import Import Import Import Import Import Import Protocol Import from Hex Dump Ctrl+ W 149 192.168.28.240 ESP Close Ctrl+ W 149 192.168.28.240 ESP Save As Ctrl+ S 149 192.168.28.240 ESP Save As Ctrl+ Shift+S 149 192.168.28.240 ESP File Set Ctrl+Shift+S 149 192.168.28.240 ESP Export Specified Packets Ctrl+Shift+S 149 192.168.28.240 ESP Export Packet Dissections As Plain Text .240 ESP Export Packet Bytes Ctrl+Shift+X As CSV .240 ESP Export Packet Bytes Ctrl+Shift+X As PDML XML .240 ESP Export Plus to File As PDML XML .240 ESP .240 ESP As PDML XML .240 ESP<</td> <td>Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+O Ctrl+O Image: Imag</td>	Edit View Go Capture Analyze Statistics Telephony Wireless Tools Open Ctrl+ O	Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+ 0 Import Import Import Import Import Import Import Import Protocol Import from Hex Dump Ctrl+ W 149 192.168.28.240 ESP Close Ctrl+ W 149 192.168.28.240 ESP Save As Ctrl+ S 149 192.168.28.240 ESP Save As Ctrl+ Shift+S 149 192.168.28.240 ESP File Set Ctrl+Shift+S 149 192.168.28.240 ESP Export Specified Packets Ctrl+Shift+S 149 192.168.28.240 ESP Export Packet Dissections As Plain Text .240 ESP Export Packet Bytes Ctrl+Shift+X As CSV .240 ESP Export Packet Bytes Ctrl+Shift+X As PDML XML .240 ESP Export Plus to File As PDML XML .240 ESP .240 ESP As PDML XML .240 ESP<	Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help Open Ctrl+O Ctrl+O Image: Imag

CapturedおよびRangeを選択し、Rangeフィールドに、最初に関連するパケットから最後に関連 するパケットまでの範囲を入力します。 [File Name] フィールドにファイル名を入力し、[Save] をクリックします。

📕 Wireshark • E	xport Packet Disse	ections				×
Save in:	Desktop		~	G 🦻	► 🔝 🏷	
Quick access Desktop Libraries	Name	^ No iter	ns match your s	Status search.	Date	nodified
Network	< File name: Save as type:	CAP1_slice CSV (Comma Sepa	arated Values sum	nmary) (*.ce	∽ 51 ∽	> Save Cancel Help
	Packet Range All packets Selected pack Marked packet First to last material Range: 451- Remove Ignored	ket ets arked -550 red packets		Captured 880 1 0 0 100	O Displayed 100 1 0 100 100 0	Pack Pack Pack Pack Pack Pack Pack Pack

該当するパケットについて、キャプチャ2で同じプロセスを繰り返します。

Wireshark - E	port Packet	Dissections
---------------	-------------	-------------

-			
- 1	ω	۴.	
	۰		
		ъ.	
-			

Save in:	E Desktop		~	G 🕫	• 🖽 🔁	
A Quick access	Name	Noit	ems match your s	Status earch.	Date n	nodified
Desktop						
Libraries						
Lange Contract This PC						
Network	۲					>
	File name:	CAP2_slice			~	Save
	Save as type:	CSV (Comma Se	parated Values sum	mary) (".c	sı ~	Cancel
						Help
	Packet Range					Packe
			۲	aptured	O Displayed	⊠ Pa
	 All packets 			904	904	2
	 Selected participation 	cket		1	1	
	 Marked pack 	kets		0	0	
	 First to last m 	arked		0	0	
	Range: 46	3-564		102	102	
	Remove Ign	ored packets		0	0	LE

両方のCSVファイルをMicrosoft Excelで開きます。

ソースキャプチャCSVで、XLSX形式で保存します。

Save As		
(L) Recent	1 🗁 Desktop	
	CAP1_slice	
Cisco	Excel Workbook (*.xlsx)	🖓 Save

画面の下部で、+記号を選択して別のシートを追加します。これにCAP2_sliceという名前を付けます。

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)	
-	- F	CAP1_slice	÷					

CAP2 CSVファイルを開き、Ctrl + aを押してすべてを選択し、Ctrl + cを押してコピーします。

J77 \checkmark : $\times \checkmark f_x$

	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	=0x040001dc	
3	464	61.00301	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI	=0x040001dc	
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	=0x040001do	
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	=0x040001dc	
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	=0x040001dc	
10	471	61.01406	192.168.2	192.168.28	ESP	176	314	27			ESP (SPI	=0x040001dc	
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	=0x040001dc	
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	=0x040001do	
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	=0x040001dc	
17	478	61.02605	192.168.2	192.168.28	ESP	176	321	27			ESP (SPI	=0x040001dc	

CAP1_slice.xlsxファイルに移動し、CAP2_sliceの2番目のタブで、コピーした情報をセルA1に貼 り付けます(**Ctrl + v**)。

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	(+)								

- All 1	~				-	· · · · ·	•		· · · ·			N	-	
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info		Seque	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	100 160 00	FCD	176	241	77			CCD.	(001-0		1de)

CAP1_sliceシートに戻り、COMPARE_ESP_SEQUENCEという名前の新しい列を作成します。

	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_SEQU	JENCE	
2		451	55.44196	192.168.2	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001d	:)					
3		452	55.44598	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001d	;)					
	1	450	EE 44007	102 160 2	103 169 30	ren	176	200	27			ren (eni-	0-040001d	4					

ESPシーケンス番号が列Gにあるため、図に示すようにVLOOKUPコマンドを作成して2つのシートを比較し、送信元の列G内のすべてのデータが宛先の列G内にあることを確認します。

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

· +	X																					
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	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPA -	ESP_SEO	UENCE							
55.4419	6 192.168.2	192.168.2	ESP	176	306	27			ESP (SPI=	0x040001dd	c)		=IF(ISNA(VLOOKUP	G2,CAP2_	slice!G:G,1	,FALSE)),"N	AISSING","	PRESENT")			
55.4459	8 192.168.2	192.168.2	ESP	176	307	27			ESP (SPI=	0x040001dd	c)			T								

[Enter]を選択すると、PRESENTという単語が表示されます。これは、ESPシーケンス**306**のパケットが2番目のシートに存在することを意味します。これは、パケットが送信元から宛先に到達したことを意味するため、重要です。

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		COMPA -	ESP_SEQU	JENCE		
2		451	55.44196	192.168.23	192.168.28	ESP	176	306	27			ESP (SPI=0	0x040001dc	;)		PRESENT				
3		452	55.44598	192.168.23	192.168.28	ESP	176	307	27			ESP (SPI=0	0x040001dc	:)						

[Column O Row 2] を選択し、そのセルを囲む緑色のボックスの右下隅にカーソルを合わせます。

N	0	Р	Q	R	S
	COMPARE	ESP_SEQ			
	3 10				

値を持つセルの下部にこの数式をコピーするには、マウスを下にドラッグします。

Ŧ		\times	\checkmark	f_{x}	=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"MISSING","PRESENT"	')
---	--	----------	--------------	---------	--	----

	в	с	D	E	F	G	н	1	J.	к		L	м	N	0	Р	Q	R	S	т	U	v	w
	Time	Source	Destinat	ic Protocol	Length	ESP Seque	Differenti	Source Po	Destinati	c Info	S	equence	Number		COMPARE	ESP_SEQ	UENCE						
51	55.44196	192.168.2	2:192.168.	28 ESP	176	306	27			ESP (S	PI=0x	040001dc)			PRESENT								
52	55.44598	192.168.2	2:192.168.	28 ESP	176	307	27			ESP (S	PI=0x	040001dc)											
53	55.44897	192.168.2	2:192.168.	28 ESP	176	308	27			ESP (S	PI=0x	040001dc)											
54	55.45097	192.168.2	23192.168.	28 ESP	176	309	27			ESP (S	PI=0x	040001dc)											
55	55.45296	192.168.2	2:192.168.	28 ESP	176	310	27			ESP (S	PI=0x	040001dc)											
56	55.45496	192.168.2	2:192.168.	28 ESP	176	311	27			ESP (S	PI=0x	040001dc)											
57	55.45597	192.168.2	2:192.168.	28 ESP	176	312	27			ESP (S	PI=0x	040001dc)											
58	\$ 55.45698	192.168.	23 192.168.	28 ESP	176	313	27			ESP (S	PI=0x	040001dc)											
59	55.45797	192.168.	2: 192.168.	ZEESP	176	314	27			ESP (S	PI=0x	040001dc)											
20	55.45898	192.168.	2: 192.168.	ZEESP	1/6	315	27			ESP (S	PI=0xi	040001dc)											
21	55 46297	192.108.	2: 192.108.	20 550	170	310	27			ESP (S	PI=0xi	040001dc)											
53	55 46596	192.100.	2: 192.100.	25 ESD	176	318	27			ESP (S	DI=0vi	040001dc)											
1	55.46697	192.168	2: 192.168	25 ESP	176	319	27			ESP (S	PI=0xi	040001dc)											
55	55.46796	192.168.3	2: 192.168.	28 ESP	176	320	27			ESP (S	PI=0xi	040001dc)											
56	55.46996	192.168.2	2: 192.168.	28 ESP	176	321	27			ESP (S	PI=0x	040001dc)											
57	55.47097	192.168.2	2: 192.168.	2EESP	176	322	27			ESP (S	PI=0x	040001dc)											
	JS9 JJ.	.00257 1	92.100.2	: 172.100.	ZCEOP		170	374	4	/			E3	e (SPI-0	04000100	1		Pho	SCINI				
	540 55.	.60496 1	92.168.2	192.168.	28 ESP		176	395	2	7			ES	P (SPI=0)	x040001dd	:)		PRE	SENT				
	541 55.	.60596 1	92.168.2	192.168.	28 ESP		176	396	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	542 55.	.60696 1	92.168.2	192.168.	28 ESP		176	397	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	543 55.	.60696 1	92.168.2	192.168.	28 ESP		176	398	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	544 55.	.60696 1	92.168.2	192.168.	28 ESP		176	399	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	545 55.	.60796 1	92.168.2	192.168.	28 ESP		176	400	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	546 55.	.60796 1	92.168.2	192.168.	28 ESP		176	401	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	547 55.	60896 1	92.168.2	192.168.	28 ESP		176	402	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	548 55.	.60896 1	92.168.2	192.168.	28 ESP		176	403	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	549 55.	60997 1	92.168.2	192.168.	28 ESP		176	404	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				
	550 55.	61096 1	92.168.2	192.168.	28 ESP		176	405	2	7			ES	P (SPI=0	x040001dd	:)		PRE	SENT				

シートの先頭に戻ってスクロールし、COMPARE_ESP_SEQUENCEをクリックします。次に、 [Sort & Filter] を選択します。

] onal ng ~	Format as Table ~	Normal Neutral Styl	Bad Calculation es	Good Check Cel		Insert v	Delete Čells	Format	∑ AutoSum	Y AZY Sort & Filter Y S	Find &
V	О		R	S	T	U	V	V	v x	Y	

ドロップダウンメニューから[Filter] を選択します。



COMPARE_ESP_SEQUENCE列にドロップダウンメニューが表示されます。

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

COMPARE_ESP_SEQUENCE見出しのドロップダウンメニューをクリックします。この例では 、表示されている値はPRESENTだけであることに注意してください。これは、すべてのパケッ トが両方のキャプチャに存在することを意味します。

	к	L	м	N	0	
c Inf	o	Sequence	Number		COMPA -	ESI
ES	2,↓ s	ort A to Z				
ES ES	Z↓ Sg	ort Z to A				
ES	Sor	<u>t</u> by Color			>	
ES	She	eet <u>V</u> iew			>	
ES	\	lear Filter Fro	om "COMPA	RE_ESP_SEQ	UENCE"	-
ES	Filt	er by Color			>	
ES	Tex	t <u>F</u> ilters			>	
ES ES	Se	arch			Q	_
ES		Select A	AII)			
ES		PRESEN	T			
ES						
ES						
ES						
ES						
ES						

問題のある例を作成するには、CAP2_sliceから10個のパケットを削除します。これは、一部のパ ケットが欠落しているテストでこれが動作する方法を示します。

11	4/2	01.01000 192.108.2: 192.10	8.28 ESP	1/0	312	27	ESP (SPI=0X0400010C)	
12	473	61.01806 192.168.23 192.16	8.28 ESP	176	316	27	ESP (SPI=0x040001dc)	
13	474	61.02106 192.168.23 192.16	8.28 ESP	176	317	27	ESP (SPI=0x040001dc)	
14	475	61.02205 192.168.23 192.16	8.28 ESP	176	318	27	ESP (SPI=0x040001dc)	
15	476	61.02306 192.168.23 192.16	8.28 ESP	176	319	27	ESP (SPI=0x040001dc)	
16	477	61.02506 192.168.23 192.16	8.28 ESP	176	320	27	ESP (SPI=0x040001dc)	
17	478	61.02605 192.168.23 192.16	8.28 ESP	176	321	27	ESP (SPI=0x040001dc)	
18	479	61.02805 192.168.23 192.16	8.28 ESP	176	322	27	ESP (SPI=0x040001dc)	
19	480	61.02906 192.168.23 192.16	8.28 ESP	176	323	27	ESP (SPI=0x040001dc)	
20	481	61.02906 192.168.23 192.16	8.28 ESP	176	324	27	ESP (SPI=0x040001dc)	
21	482	61.03005 192.168.23 192.16	8.28 ESP	176	325	27	ESP (SPI=0x040001dc)	
22	483	61.03206 192.168.23 192.16	8.28 ESP	176	326	27	ESP (SPI=0x040001dc)	
23	484	61.03306 192.168.23 192.16	8.28 ESP	176	327	27	ESP (SPI=0x040001dc)	
24	485	61.03505 192.168.23 192.16	8.28 ESP	176	328	27	ESP (SPI=0x040001dc)	
25	486	61.03606 192.168.23 192.16	8.28 ESP	176	329	27	ESP (SPI=0x040001dc)	
26	487	61.03905 192.168.23 192.16	8.28 ESP	176	330	27	ESP (SPI=0x040001dc)	
27	488	61.04105 192.168.23 192.16	8.28 ESP	176	331	27	ESP (SPI=0x040001dc)	
28	489	61.04206 192.168.23 192.16	8.28 ESP	176	332	27	ESP (SPI=0x040001dc)	
29	490	61.04406 192.168.23 192.16	8.28 ESP	176	333	27	ESP (SPI=0x040001dc)	
30	491	61.04606 192.168.23 192.16	8.28 ESP	176	334	27	ESP (SPI=0x040001dc)	
31	492	61.06305 192.168.23 192.16	8.28 ESP	176	335	27	ESP (SPI=0x040001dc)	
32	493	61.06505 192.168.23 192.16	8.28 ESP	176	336	27	ESP (SPI=0x040001dc)	
33	494	61.06705 192.168.23 192.16	8.28 ESP	176	337	27	ESP (SPI=0x040001dc)	
34	495	61.06905 192.168.23 192.16	8.28 ESP	176	338	27	ESP (SPI=0x040001dc)	
35	496	61.07105 192.168.23 192.16	8.28 ESP	176	339	27	ESP (SPI=0x040001dc)	
36	497	61.07105 192.168.23 192.16	8.28 ESP	176	340	27	ESP (SPI=0x040001dc)	
37	498	61.07205 192.168.23 192.16	8.28 ESP	176	341	27	ESP (SPI=0x040001dc)	
38	499	61.07605 192.168.23 192.16	8.28 ESP	176	342	27	ESP (SPI=0x040001dc)	
4	•	CAP1_slice CAP2_slice	•					

CAP1_sliceシートに戻ると、10個のパケットが欠落していることが確認できます。

	33.43737 13		110	J14	£1	L31 (311-0x04000100)	Theorem 1
460	55.45898 19	2.168.2: 192.168.2ESP	176	315	27	ESP (SPI=0x040001dc)	PRESENT
461	55.46197 19	2.168.23 192.168.28 ESP	176	316	27	ESP (SPI=0x040001dc)	PRESENT
462	55.46397 19	2.168.2: 192.168.2ESP	176	317	27	ESP (SPI=0x040001dc)	PRESENT
463	55.46596 19	2.168.23 192.168.28 ESP	176	318	27	ESP (SPI=0x040001dc)	MISSING
464	55.46697 19	2.168.23 192.168.28 ESP	176	319	27	ESP (SPI=0x040001dc)	MISSING
465	55.46796 19	2.168.23 192.168.28 ESP	176	320	27	ESP (SPI=0x040001dc)	MISSING
466	55.46996 19	2.168.23192.168.28ESP	176	321	27	ESP (SPI=0x040001dc)	MISSING
467	55.47097 19	2.168.23192.168.28ESP	176	322	27	ESP (SPI=0x040001dc)	MISSING
468	55.47198 19	2.168.23192.168.28ESP	176	323	27	ESP (SPI=0x040001dc)	MISSING
469	55.47297 19	2.168.23192.168.28ESP	176	324	27	ESP (SPI=0x040001dc)	MISSING
470	55.47497 19	2.168.23192.168.28ESP	176	325	27	ESP (SPI=0x040001dc)	MISSING
471	55.47597 19	2.168.23192.168.28ESP	176	326	27	ESP (SPI=0x040001dc)	MISSING
472	55.47697 19	2.168.23 192.168.28 ESP	176	327	27	ESP (SPI=0x040001dc)	MISSING
473	55.47896 19	2.168.23192.168.28ESP	176	328	27	ESP (SPI=0x040001dc)	PRESENT
474	55.48096 19	2.168.23192.168.28ESP	176	329	27	ESP (SPI=0x040001dc)	PRESENT

COMPARE_ESP_SEQUENCE列でドロップダウンメニューが選択されると、MISSINGパケット も存在することが確認されます。これは、MISSINGパケットだけを表示するように切り替えるこ とができます。

	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 .:



Excelシートに見つからないパケットだけが表示されるようになりました。

1	Α	В	С	D	E	F	G	н		J	K	L	М	N	0	P
	No.	Time	Source	Destinati	Protocol	Length	ESP Seque	Differenti	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																

関連情報

- <u>Cisco Embedded Packet Capture</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。