Verificación e identificación de la pérdida de paquetes en la WAN para SD-WAN

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Background Proceso de Troubleshooting Proceso general Marque el tráfico deseado con DSCP Capturar el tráfico con la captura incorporada Análisis mediante Wireshark Filtrar el tráfico deseado por secuencia ESP Información Relacionada

Introducción

Este documento describe cómo identificar y recopilar datos cuando el tráfico ha perdido a través de la WAN pero no se ven caídas en el extremo de la SD-WAN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa definida por software (SD-WAN) de Cisco
- Captura de paquetes integrada o captura de paquetes vManage
- Wireshark
- Microsoft Excel

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- C8000V versión 17.03.04
- vManage versión 20.3.4
- Wireshark versión 2.6.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Para ayudar con este desafío, los pasos descritos en este documento muestran cómo marcar el tráfico específico con el punto de código de servicios diferenciados (DSCP) para ayudar a identificar los paquetes deseados. DSCP se puede utilizar para identificar el tráfico ya que este valor se copia del encabezado de paquete interno al encabezado IPsec. Una vez que se identifican los paquetes deseados, se muestra cómo hacer coincidir el tráfico a través de dos capturas de WAN para garantizar que el tráfico circule desde el origen al destino.

Se utilizan dos sitios de router individuales para demostrar esta técnica de solución de problemas. En este caso, el tráfico ICMP de 10.0.0.10 a 10.0.2.10 en forma de 100 pings, como se muestra en la imagen. No hay pérdidas en este ejemplo, pero esta misma técnica de solución de problemas se utiliza en el caso de que haya una pérdida para identificarla.



Proceso de Troubleshooting

Proceso general

- 1. Para el tráfico rastreado a través de la WAN, se necesita una lista de acceso (ACL) (o política centralizada) para marcar el tráfico con algún valor DSCP no utilizado. En este ejemplo, se utiliza DSCP 27.
- 2. Una vez marcado el tráfico, la captura de paquetes integrada se utiliza para capturar los paquetes en la interfaz de transporte del router de origen y destino.

Nota: La captura de paquetes de vManage también se puede utilizar aunque hay una limitación de 5 MB de datos o 5 minutos de tiempo de ejecución.

- 1. Una vez realizadas las capturas, ábralas en Wireshark para verlas.
- 2. El filtro se aplica en Wireshark para mostrar qué paquetes se desean y, a continuación, se comparan.
- 3. Microsoft Excel se utiliza para capturas de gran tamaño para garantizar la precisión.

Marque el tráfico deseado con DSCP

Una lista de acceso como el ejemplo Se configura en el router de origen (cEdge1 en este ejemplo) y se aplica en la interfaz en la parte SD-WAN de la configuración del router como se muestra.

Se aplica un contador opcional para verificar que el tráfico llega a la política como se esperaba. Esto se puede verificar con el comando **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
```

Capturar el tráfico con la captura incorporada

Nota: Cómo configurar una captura de paquetes integrada en Cisco IOS XE para capturar los paquetes cifrados que atraviesan la WAN, navegue hasta <u>Ejemplo de Configuración de</u> <u>Captura de Paquetes Integrada para Cisco IOS y Cisco IOS XE</u>

Nota: Se debe utilizar una ACL para limitar el EPC en la WAN, ya que podría haber más del límite de velocidad de 1000 PPS para el EPC.

Ejemplo:

Una ACL se configura en cEdge1 y cEdge3 ya que el tráfico sólo se verifica en la dirección de origen a destino en este ejemplo.

Nota: Las direcciones IP de WAN se utilizan para filtrar la captura. Hay varias salidas que se pueden utilizar para identificar la trayectoria que toma el tráfico de modo que se puedan identificar las IP de WAN correctas para el filtro ACL. Los comandos que se pueden utilizar para generar esta salida son **show sdwan app-fwd cflow flows** y **show sdwan policy service path**. Desplácese hasta <u>Seguimiento de paquete condicional</u> para la condición de depuración.

ip access-list extended CAP-Filter

10 permit ip host 192.168.23.149 host 192.168.28.240

En este punto, las capturas se inician en ambos routers y se envían 100 pings a través de la superposición.

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms Una vez que las capturas se detienen y se recopilan de ambos routers, deben abrirse en Wireshark para verlas.

Análisis mediante Wireshark

Una vez que se abre la captura cEdge1 en Wireshark, se ve que todo el tráfico está cifrado y no es fácil descifrar qué paquetes son los pings que se enviaron.

colors filter and the la		<u> </u>	22							
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	UOP	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	UOP	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	UOP	168	Class Selector 6				12386 + 12407 Len=126	
31 13.779958	192.168.23.149	192.168.28.240	UOP	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	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	UOP	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	UDP	176	Default				12386 - 12407 Len=134	
39 14,188998	192,168,23,149	192, 168, 28, 248	LIDP	176	Default				12386 a 12407 Lena134	

Filtre esta captura con un filtro de visualización **ip.dsfield.dscp == 27**, se ve que solo se muestran 100 paquetes en la parte inferior de la pantalla y se ve que el valor de la columna DSCP muestra todos 27.

Destination									CD 1
	n Pro	tocol Length	ESP Sequence	Differentiated Services Codepoint	Source Port	Destination Port	Sequence Number	Info	
68.23.149 192.168	.28.248 UDF	• 1	76	27				12386 + 12407 Len=134	
.68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF	. 1	76	27				12386 → 12407 Len=134	
68.23.149 192.168	.28.240 UDF	. 1	76	27				12386 + 12407 Len=134	
.68.23.149 192.168	.28.240 UDF	. 1	76	27				12386 → 12407 Len=134	
68.23.149 192.168	.28.240 UDF	. 1	76	27				12386 → 12407 Len=134	
68.23.149 192.168	.28.240 UDF	• 1	76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF	• 1	76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF	. 1	76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF	- 1	76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 → 12407 Len=134	
68.23.149 192.168	.28.240 UDP	. 1	76	27				12386 → 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12487 Len=134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68,23,149 192,168	.28.240 UDF		76	27				12386 + 12407 Len+134	
68,23,149 192,168	.28.240 UDF		76	27				12386 + 12407 Len+134	
68.21.149 192.168	.28.240 LIDE		76	27				12386 + 12407 Len=134	
68, 21, 149 192, 168	-28.240 UDF		76	27				12186 + 12407 Lene134	
68.23.149 192.168	.28.240 UDF		76	27				12386 + 12407 Len=134	
68, 23, 149 192, 168	.28.240 UDS		76	27				12386 + 12407 Len=134	
68 23 140 102 168	28.248 100		26	27				12386 a 12407 Lena134	
68 23 140 102 168	28.240 100		26	27				12386 a 12407 Lena134	
69 33 140 103 169	28.240 000		76	37				13386 - 13487 Len-134	
68.23.149 192.168	28.240 000		26	27				12386 a 12407 Lenal34	
100.23.149 192.100	28.240 000		70	27				12300 * 12407 Len-134	
100.23.149 192.100	20.240 000		170	27				12300 * 1240/ Len=134	
66.23.149 192.168	28.240 000		76	27				12380 + 12407 Len=134	
10.23.149 192.100	28.240 007		76	27				12300 * 12407 Len*134	
68.23.149 192.168	.28.240 009		.76	27				12386 + 12487 Len=134	
68.23.149 192.168	.28.240 009		76	27				12386 + 12407 Len=134	
68.23.149 192.168	.28.240 UDP		176	27				12360 + 12407 Len=134	
60.23.149 192.168	.20.240 UDF	1	16	10				12300 + 12407 Len+134	
68.23.149 192.168	.28.240 UDF	1	76	27				12386 + 12487 Len=134	
68.23.149 192.168	.28.240 UDF	1	76	27				12386 = 12407 Len=134	
68.23.149 192.168	.28.240 UDF	. 1	76	27				12386 + 12407 Len=134	
	3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160 3.23.140 197.160	3.3.1.40 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60 132.1.60	4.33.140 152.146.36.2440 100° 1 4.33.140 152.146.36.2440 100° 1 5.33.140 152.146.36.2440 100° 1 5.33.140 152.146.37.2440 100° 1 5.33.140 152.146.37.2440 100° 1 5.33.140 152.146.37.2440 100° 1 5.33.140 152.146.37.2440 100° 1 5.33.140 152.146.37.2440 100° 1 6.23.140 152.146.37.2440 100° 1 6.23.140 152.146.37.2440 100° 1 6.23.140 152.146.37.2440 100° 1 6.23.140 152.146.37.240 100° 1 6.23.140 152.146.37.240 100° 1 6.23.140 152.146.37.240 100° 1 6.23.140 152.146.37.240 100° 1 6.23.140 152.146.37.240 100° 1 6.23.140 152.146.37.240 100° 1 6.23.1	4.23.14 192.148.3.244 USP 176 6.23.14 192.148.3.244 USP 176 6.23.14 192.148.3.244 USP 176 6.23.14 192.148.3.244 USP 176 6.23.144 192.148.3.244 USP 176 6.23.144 192.148.3.244 USP 176 6.23.144 192.148.3.244 USP 176 6.23.149 192.148.3.244 USP 176 6.23.140 192.148.3.244 USP 176 6.23.141 192.148.3.244 USP 176 6.23.140 192.148.3.244 USP 176 6.23.141 192.148.3.244 USP 176 6.23.141 192.148.3.244 USP 176 6.23.141	4.33.44 152.148.8.2.44 UOP 176 27 8.23.149 152.148.8.2.44 UOP 176 27 8.23.140 152.148.8.2.44 UOP 176	4.33.44 132.148 13.24 100 126 4.33.144 132.148.32.44 100 126 27 4.33.144 132.148.32.44 100 126 27 4.33.144 132.148.32.44 100 126 27 4.33.144 132.148.32.44 100 126 27 4.33.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126 27 8.23.140 132.148.32.44 100 126	4.3.3.4 19.2.14.8.3.2.49 0.09 76 77 4.3.3.49 19.2.14.8.3.2.49 0.09 176 27 4.3.3.49 19.2.14.8.3.2.49 0.09 176 27 4.3.3.49 19.2.14.8.3.2.49 0.09 176 27 4.3.3.49 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 19.2.14.8.3.2.49 0.09 176 27 8.3.3.149 1	4.33.4 32.14.8.3.240 USP 176 27 4.33.14 32.14.8.3.240 USP 176 27 4.33.14 32.146.3.240 USP 176 27 4.33.14 32.146.3.240 USP 176 27 4.33.14 152.146.3.240 USP 176 27 4.33.140 152.146.3.540 USP 176 27 4.33.140 152.146.3.340 USP 176	4.23.44 102.148.2.484 109 176 27 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1.207 1206 1

En algunos casos en los que el valor DSCP se mantiene a través de la WAN, se puede utilizar el mismo filtro en la captura de destino.

En otros casos, esto no es posible, como en una situación en la que el valor DSCP se borra a través de una conexión de Internet pública.

Filtrar el tráfico deseado por secuencia ESP

En cualquier caso, el tráfico se puede identificar con los números de secuencia ESP.

Para ver los números de secuencia ESP en el paquete, haga clic con el botón derecho en la captura y elija **Decodificar** como se muestra.

	12386
	12386
Mark/Unmark Packet Ctrl+M	12386
Ignore/Unignore Packet Ctrl+D	12386
Ignole/Onighole Packet Ctil+D	12386
Set/Unset Time Reference Ctrl+T	12386
Time Shift Ctrl+Shift+T	12386
Packet Comments	12386
	12386
Edit Resolved Name	12386
	12386
Apply as Filter	12386
Prepare as Filter	12386
	12386
Conversation Filter	12386
Colorize Conversation	12386
SCTP •	12386
5011	12386
Follow	12386
Comu	12386
Сору	12386
Protocol Preferences	12386
	12386
Decode As	12386
Show Packet in New Window	12386

Seleccione el menú desplegable **Campo actual** y, en ese campo, escriba **UDPENCAP** o selecciónelo en el menú desplegable.



Field	Value	Type	Default	Current
UDP port	12386	Integer, base 10	(none)	(none)
				(none)
				3GPP2 A11
				A21
				AC DR
				ADP
				ADwin
				ALC
				AMP
+ -	Ф (
				OK Save Copy from Cancel Help
				Concernation Copy Iron Cancer Nep

×

Seleccione OK una vez que haya terminado.

Wiresh	ark • De	code As							
ield	Value	Туре	Default	Current					
IDP port	12386	Integer, base 10	(none)	UDPENCAP					
	Ph (
	-	-0				1			_
					OK	Save	Copy from	Cancel	Help

Dentro de la sección Detalles del Paquete Wireshark, expanda la parte **Carga de Seguridad de Encapsulación** del paquete para ver la **Secuencia ESP**.

```
      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)
      Fthernet 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: 0X040001ac (6/109340)
      ESP Sequence: 319
```

Haga clic con el botón derecho del ratón en **ESP Sequence** y seleccione **apply as column** para que la secuencia ESP se pueda ver como una columna en la sección Packet List en la parte superior de la pantalla Wireshark.

	/04 IJZ.100.2J.14J	102.100.20.240	601
456 55.4	Evene of Cultures		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	compservin		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	Commention 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 byt	Wiki Protocol Page		08 hits)
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 De chat in Mar	. Monday.	
ESP Sequence: 31_	Show Link d Packet in New	w window	J

Nota: el SPI ESP para los paquetes en cEdge1 es **0x040001dc**. Se utiliza para un filtro en la captura de destino.

```
> 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
```

Abra la captura de destino, repita los pasos para decodificar como **UDPENCAP** y muestre los números de secuencia ESP en los paquetes.

Una vez que los paquetes muestran el número de secuencia ESP, el SPI ESP de la primera captura se puede utilizar como filtro en la segunda captura para mostrar sólo el tráfico dentro de ese SPI que coincida con el tráfico deseado.

Observe que los números de secuencia de paquetes que coinciden con ambos tienen DSCP 27 marcado.



Esta comparación se puede realizar en Wireshark manualmente o se puede utilizar Microsoft Excel para realizar esta comparación.

Para utilizar Microsoft Excel para realizar la comparación, es necesario dividir ambas capturas para que contengan sólo paquetes que se encuentren en ambas capturas.

En la captura de origen, el primer paquete relevante tiene la secuencia ESP 306 y corresponde al paquete número 451.

CAP.pcap						-		\times
File Edit View Go Capture	Analyze Statistics Tel	ephony Wireless Tools	Help					
📶 🔳 🖉 💿 📙 🛅 🗙 🖸 🗎	९ 🗢 🗢 🗟 🚹 👲	🚽 📃 🔍 🔍 🔍 🖽						
ip.dsfield.dscp == 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	

El último paquete relevante en la captura de origen tiene la secuencia ESP 405 y es el paquete número 550.

	548 55.608962 549 55.609969	192.168.23.149 192.168.23.149	192.168.28.240 192.168.28.240	ESP	176 176	403 27 404 27	
<	550 55.610960	192.168.23.149	192.168.28.240	ESP	176	405 27	~

En la captura de destino, el primer paquete relevante corresponde a la captura de origen con la secuencia ESP 306, pero en esta captura está el paquete 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

El último paquete relevante también está presente con la secuencia ESP 405 y es el paquete 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	
					-	

La primera captura se debe dividir para incluir sólo los paquetes relevantes.

Vaya a Archivo > Exportar disecciones de paquetes > Como CSV...

CAP	.pca	р
-----	------	---

File	Edit View Go	Capture	Analyze S	tatisti	cs Telephony	Wireless	Tools	Help		
	Open	(Ctrl+O	1	5 🕭 📃 🔳	Θ Θ	Q. 🎹			
	Open Recent		•							
	Merge				Destinati	on		Protocol	Length	E
	Import from Hex D	ump		149 192.168.28.240				ESP	-	176
	Close		`trl+W	149	192.16	8.28.24	0	ESP		176
	Close	```	2014 11	149	192.16	8.28.24	0	ESP		176
	Save	(Ctrl+S	149	192.16	8.28.24	0	ESP		176
	Save Ac	0	Ttrl+Shift+S	149	192.16	8.28.24	0	ESP		176
	Save As	```	Surt-Surt-S	149	192.16	8.28.24	0	ESP		176
	File Set		•	149	192.16	8.28.24	0	ESP		176
				149	192.16	8.28.24	0	ESP		176
	Export Specified Pa	ckets		149	192.16	8.28.24	0	ESP		176
	Export Packet Disse	ctions	•		As Plain Text	.24	0	ESP		176
	Export Dacket Buter		Ttrl+Shift+Y		Ar CSV	.24	0	ESP		176
	export Packet bytes		Lui+Shirt+A		AS COV	.24	0	ESP		176
	Export PDUs to File.				As "C" Arrays	.24	0	ESP		176
	Export TLS Session	Keys				.24	0	ESP		176
	Export Objects		•		As PSML XML	.24	0	ESP		176
	export objects				As PDML XML	.24	0	ESP		176
	Print	(Ctrl+P		As ISON	.24	0	ESP		176
	FIIItan						0	ESP		176
	Quit	(Ctrl+Q	149	192.16	8.28.24	0	ESP		176
-	247 23	.000902	192.100.23	.149	192.16	8.28.24	0	ESP		176
	548 55	608962	192.168.23	.149	192.16	8.28.24	0	ESP		176

Seleccione **Captured** y **Range** y en el campo **Range** escriba el rango desde el primer paquete relevante hasta el último paquete relevante.

Introduzca un nombre de archivo en el campo Nombre de archivo y haga clic en Guardar.

	Wireshark · Export Packet Dissections
--	---------------------------------------

Save in:	Desktop		~	G 🦻	P 🖪	•	
Quick access	Name	^ No items r	match your s	Status earch.		Date mo	odified
Desktop							
Libraries							
This PC							
Network	<	CAP1 slice			~	_	> Save
	Save as type:	CSV (Comma Separate	ed Values sum	mary) (*.c	sı ~	(Cancel Help
	Packet Range						Pack
			•	aptured	O Dis	played	Pa
	○ All packets			880		100	
	O Selected pack	ket		1		1	⊡ Pa
	Marked packe	ets		0		0	F
	First to last ma	irked		0		0	
	Range: 451-	550 red packets		100		100	
				0		0	

Repita el mismo proceso en la captura 2 para los paquetes relevantes.

 \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 V 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

Abra ambos archivos CSV en Microsoft Excel.

En la captura de origen CSV, guárdela como un formato XLSX.

Save As		
L Recent	↑ ☐ Desktop CAP1_slice	
Cisco	Excel Workbook (*.xlsx)	🔛 Save

En la parte inferior de la pantalla, seleccione el símbolo + para agregar otra hoja. Asígnele el nombre 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)	
3	487	55.51796 192.168.2	192.168.28 ESP	176	342	27	ESP (SPI=0x040001dc)	
-	•	CAP1_slice	÷					

Abra el archivo CAP2 CSV y presione CTRL + a para seleccionar all y CTRL + c para copiarlo.

J77 \checkmark : $\times \checkmark f_x$

1	А	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

Navegue hasta el archivo **CAP1_slice.xlsx** y en la segunda pestaña para CAP2_slice, pegue (**CTRL + v**) la información copiada en la celda **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>		1			is i	-	
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Different	Source Po	Destinatio	Info		Sequence	e N
2	463	60.99901	192.168.23	192.168.28	ESP	176	306	27			ESP	(SPI=0	x040001d	c)
3	464	61.00301	192.168.23	192.168.28	ESP	176	307	27			ESP	(SPI=0	x040001d	c)
4	465	61.00506	192.168.23	192.168.28	ESP	176	308	27			ESP	(SPI=0	x040001d	c)
5	466	61.00706	192.168.23	192.168.28	ESP	176	309	27			ESP	(SPI=0	x040001d	c)
6	467	61.00905	192.168.23	192.168.28	ESP	176	310	27			ESP	(SPI=0	x040001d	c)
7	468	61.01006	192.168.23	192.168.28	ESP	176	311	27			ESP	(SPI=0	x040001d	c)
8	469	61.01105	192.168.23	192.168.28	ESP	176	312	27			ESP	(SPI=0	x040001d	c)
9	470	61.01305	192.168.23	192.168.28	ESP	176	313	27			ESP	(SPI=0	x040001d	c)
10	471	61.01406	192.168.23	192.168.28	ESP	176	314	27			ESP	(SPI=0	x040001d	c)
11	472	61.01606	192.168.23	192.168.28	ESP	176	315	27			ESP	(SPI=0	x040001d	c)
12	473	61.01806	192.168.23	192.168.28	ESP	176	316	27			ESP	(SPI=0	x040001d	c)
13	474	61.02106	192.168.23	192.168.28	ESP	176	317	27			ESP	(SPI=0	x040001d	c)
14	475	61.02205	192.168.23	192.168.28	ESP	176	318	27			ESP	(SPI=0	x040001d	c)
15	476	61.02306	192.168.23	192.168.28	ESP	176	319	27			ESP	(SPI=0	x040001d	c)
16	477	61.02506	192.168.23	192.168.28	ESP	176	320	27			ESP	(SPI=0	x040001d	c)
17	478	61.02605	192.168.23	192.168.28	ESP	176	321	27			ESP	(SPI=0	x040001d	c)
18	479	61.02805	192.168.23	192.168.28	ESP	176	322	27			ESP	(SPI=0	x040001d	c)
19	480	61.02906	192.168.23	192.168.28	ESP	176	323	27			ESP	(SPI=0	x040001d	c)
20	481	61.02906	192.168.23	192.168.28	ESP	176	324	27			ESP	(SPI=0	x040001d	c)
21	482	61.03005	192.168.23	192.168.28	ESP	176	325	27			ESP	(SPI=0	x040001d	c)
22	483	61.03206	192.168.23	192.168.28	ESP	176	326	27			ESP	(SPI=0	x040001d	c)
23	484	61.03306	192.168.23	192.168.28	ESP	176	327	27			ESP	(SPI=0	x040001d	c)
24	485	61.03505	192.168.23	192.168.28	ESP	176	328	27			ESP	(SPI=0	x040001d	c)
25	486	61.03606	192.168.23	192.168.28	ESP	176	329	27			ESP	(SPI=0	x040001d	c)
26	487	61.03905	192.168.23	192.168.28	ESP	176	330	27			ESP	(SPI=0	x040001d	c)
27	488	61.04105	192.168.23	192.168.28	ESP	176	331	27			ESP	(SPI=0	x040001d	c)
28	489	61.04206	192.168.23	192.168.28	ESP	176	332	27			ESP	(SPI=0	x040001d	c)
29	490	61.04406	192.168.23	192.168.28	ESP	176	333	27			ESP	(SPI=0	x040001d	c)
30	491	61.04606	192.168.23	192.168.28	ESP	176	334	27			ESP	(SPI=0	x040001d	c)
31	492	61.06305	192.168.23	192.168.28	ESP	176	335	27			ESP	(SPI=0	x040001d	c)
32	493	61.06505	192.168.23	192.168.28	ESP	176	336	27			ESP	(SPI=0	x040001d	c)
33	494	61.06705	192.168.23	192.168.28	ESP	176	337	27			ESP	(SPI=0	x040001d	c)
34	495	61.06905	192.168.23	192.168.28	ESP	176	338	27			ESP	(SPI=0	x040001d	c)
35	496	61.07105	192.168.23	192.168.28	ESP	176	339	27			ESP	(SPI=0	x040001d	c)
36	497	61.07105	192.168.23	192.168.28	ESP	176	340	27			ESP	(SPI=0	x040001d	c)
7	400	£1 07005	100 160 00	100 160 00	F60	176	241	27			CCD.	(001-0	w040001d	2

Vaya de nuevo a la hoja **CAP1_slice** y cree una nueva columna llamada **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	100 160 0	103 160 30	ren	176	200	77			ren (eni-	0.000001d	4					

Dado que el número de secuencia ESP se encuentra en la Columna G, cree un comando VLOOKUP como se muestra para comparar las dos hojas y asegurarse de que todo lo que se encuentra en la Columna G en el origen está en la Columna G en el destino.

=SI(ISNA(BUSCARV(G2,CAP2_slice!G:G,1,FALSO)),"FALTANTE","PRESENTE")

•	\times	~	fx	=16	(ISNA(VLO	OKUP(G2,	CAP2_slice	lG:G,1,FAL	SE)), "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	So	ource	De	estinati	Protocol	Length	ESP Seque	Differenti	Source Po	Destinati	Info	Sequence	Number		COMPA -	ESP_SEQ	UENCE							
55.441	96 19	92.168.2	19	2.168.2	ESP	176	306	27			ESP (SPI=	0x040001dc)		=IF(ISNA(VLOOKUP	G2,CAP2_	slice!G:G,1	,FALSE)),"	MISSING","	PRESENT")			
55.445	98 19	92.168.2	: 19	2.168.2	ESP	176	307	27			ESP (SPI=	0x040001dc	:)			Ī								

Después de seleccionar Enter, se muestra la palabra PRESENT. Esto significa que el paquete con la secuencia ESP **306** está presente en la segunda hoja. Esto es significativo porque significa

que el paquete llegó desde el origen al destino.

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		COMPA -	ESP_SEQ	JENCE		
2		451	55.44196	192.168.23	192.168.28	ESP	176	306	27			ESP (SPI=0	0x040001dd	;)		PRESENT				
3		452	55.44598	192.168.23	192.168.28	ESP	176	307	27			ESP (SPI=0	0x040001dd	;)						

Seleccione la columna O fila 2 y sitúe el cursor sobre la esquina inferior derecha del cuadro verde que rodea la celda.

N	0	Р	Q	R	S
	COMPARE	ESP_SEQ	JENCE		
	3 10				

Seleccione y mantenga pulsado, y arrastre el ratón hacia abajo para copiar esta fórmula en la parte inferior de las celdas que tienen valores.

	* 1	× ✓	f _x	=IF(ISNA(VL	OOKUP(G2	,CAP2_slice	G:G,1,FAI	.SE)),"MISS	SING","PRE	SENT")												
	B	С	D	E	F	G	н	1	J	K	L	м	N	0	Р	Q	R	S	т	U	V	W
	Time	Source	Desti	natic Protocol	Length	ESP Sequ	E Different	i Source Po	Destinati	c Info	Sequence	Numbe	r	COMPARE	ESP_SEC	UENCE						
51	55.4419	6 192.168.	23192.1	68.28 ESP	17	6 30	5 27	'		ESP (S	PI=0x040001dc)			PRESENT								
52	55.4459	8 192.168.	2:192.1	68.28 ESP	17	6 30	27	1		ESP (S	PI=0x040001dc)											
53	55.4489	7 192.168.	2:192.1	68.28 ESP	17	6 308	3 27			ESP (S	PI=0x040001dc)			_								
24	55.4509	7 192.168.	2:192.1	68.28 ESP	17	6 305	27			ESP (S	PI=0x040001dc)											
20	55.4529	6 192.108.	2: 192.1	68.20ESP	17	6 310	27			ESP (S	PI=0x040001dc)											
50	55.4559	7 192 168	2: 192.1	68 25 ESD	17	6 313	27	,		ESP (S	PI=0x040001dc)											
58	55,4569	8 192 168	2: 192.1	68.25 FSP	17	6 313	27	,		ESP (S	PI=0x040001dc)											
59	55,4579	7 192.168.	2: 192.1	68.28 ESP	17	6 314	27	,		ESP (S	PI=0x040001dc)											
50	55.4589	8 192.168.	2: 192.1	68.28 ESP	17	6 315	27	,		ESP (S	PI=0x040001dc)											
51	55.4619	7 192.168.	2:192.1	68.28 ESP	17	6 316	5 27	,		ESP (S	PI=0x040001dc)											
52	55.4639	7 192.168.	2:192.1	68.28 ESP	17	6 317	27	,		ESP (S	PI=0x040001dc)											
53	55.4659	6 192.168.	2:192.1	68.28 ESP	17	6 318	3 27	1		ESP (S	PI=0x040001dc)											
54	55.4669	7 192.168.	2:192.1	68.28 ESP	17	6 319	27	,		ESP (S	PI=0x040001dc)											
55	55.4679	6 192.168.	23192.1	68.28 ESP	17	6 320	27	'		ESP (S	PI=0x040001dc)											
56	55.4699	6 192.168.	2:192.1	68.28 ESP	17	6 321	27	·		ESP (S	PI=0x040001dc)											
57	55.4709	7 192.168.	23192.1	68.28 ESP	17	6 322	2 27	1		ESP (S	PI=0x040001dc)											
	J35 J3	.00257	92.10	0.23 132.100	.20 EOP		1/0	374	4	/		C	ər (əri-q	0X0400010	cj.		PRO	SEINT				
	540 55	60496 1	92.16	8.23 192.168	3.28 ESP		176	395	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	541 55	.60596 1	92.16	8.23 192.168	3.28 ESP		176	396	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	542 55	60696 1	92.16	8.23 192.168	.28 ESP		176	397	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				-
	543 55	6.60696 1	92.16	8.2: 192.168	.28 ESP		176	398	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT			_	
	544 55	60696 1	92.16	8.2: 192.168	.28 ESP		176	399	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	545 55	6.60796 1	92.16	8.2: 192.168	.28 ESP		176	400	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	546 55	6.60796 1	92.16	8.2: 192.168	3.28 ESP		176	401	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	547 55	6.60896 1	92.16	8.2: 192.168	3.28 ESP		176	402	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	548 55	6.60896 1	92.16	8.2: 192.168	.28 ESP		176	403	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	549 55	6.60997 1	92.16	8.23 192.168	3.28 ESP		176	404	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				
	550 55	6.61096 1	92.16	8.23 192.168	3.28 ESP		176	405	2	7		E	SP (SPI=0	0x040001d	c)		PRE	SENT				

Vuelva a la parte superior de la hoja y haga clic en **COMPARE_ESP_SEQUENCE**. A continuación, seleccione **Ordenar y filtrar**.

] onal ng ~	Format as Table ~	Normal Neutral	Style	Bad Calculation	Good Check (Cell	lnser	t Delete For	rmat γ	AutoSum Fill ~ Clear ~	° A Z∑ Sort & F Filter ∼ S	nd &
V	O COMPAR	P RE_ESP_SE	QUENC	R	S	Т	U	V	W	х	Y	

Elija Filter en el menú desplegable.



Aparecerá un menú desplegable en la columna COMPARE_ESP_SEQUENCE.

M	N	0	Р	
lumber		COMPA 👻	ESP_SEQU	JEN
		PRESENT		
		PRESENT		
		PRESENT		

Haga clic en el menú desplegable del encabezado **COMPARE_ESP_SEQUENCE**. Observe que en este ejemplo, el único valor que se muestra es **PRESENT**. Esto significa que todos los paquetes están presentes en ambas capturas.

	к	L	м	N	0	
c Inf	0	Sequence	Number		COMPA -	ES
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 ES	\	lear Filter Fro	om "COMPA	RE_ESP_SEC	UENCE"	
ES	Filt	er by Color			>	
ES	Tex	t <u>F</u> ilters			>	
ES	Se	arch			Q	_
ES	1	✓ (Select A	AII)			
ES		PRESEN	T			
ES						
ES						
ES						
ES						
FS						

Para crear un ejemplo problemático, elimine 10 paquetes de CAP2_slice, para demostrar cómo funcionaría esto en una prueba en la que faltan algunos paquetes perdidos.

11	4/2	01.01000 192.108.2: 192.108.28 ESP	1/0	312	27	ESP (SPI=0X0400010C)	
12	473	61.01806 192.168.23 192.168.28 ESP	176	316	27	ESP (SPI=0x040001dc)	
13	474	61.02106 192.168.2: 192.168.2ESP	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 192.168.23 192.168.28 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)	
1	•	CAP1_slice CAP2_slice +					

Vuelva a la hoja **CAP1_slice** y ahora se ve que faltan 10 paquetes.

	33.43737 IJE.100.E. IJE.100.EC.DI	110	314	£1	Loi (011-000100)	1 NEWLINE
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 192.168.2: 192.168.2ESP	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 192.168.2: 192.168.2EESP	176	329	27	ESP (SPI=0x040001dc)	PRESENT

Cuando se selecciona el menú desplegable en la columna **COMPARE_ESP_SEQUENCE**, ahora se ve que también hay paquetes **PERDIDOS**. Esto se puede alternar para ver solamente los paquetes **PERDIDOS**.

	ĸ	L	M	N	0										
nf	0	Sequence	Number		COMPA										
S	<mark>2</mark> ↓ <u>s</u> o	^A _Z ↓ <u>Sort A to Z</u>													
S	Z↓ So	ort Z to A			-										
S	Sor	Sor <u>t</u> by Color													
S	She	et <u>V</u> iew			>										
S	Clear Filter From "COMPARE_ESP_SEQUENCE"														
s	Filte	er by Color			>										
S	Tex	t <u>F</u> ilters			>										
S	Sea	arch			Q										
1 24 24 24 24 24 24 24 24 24 24 2		(Select A I MISSING I PRESENT	III) F												
5 5			0	K	Cancel .:										



Ahora solo se muestran los paquetes que faltan en la hoja de Excel.

4	Α	В	C	D	E	E F	G	н		J	K	L	M	N	0	P
	No.	Time	Source	Destinati	c Protocol	Length	ESP Seque	Different	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 8	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 8	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																

Información Relacionada

- Captura de paquetes integrada de Cisco
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).