

Ejemplo de Troubleshooting de Problemas SD-WAN de IOS-XE con Ayuda de EPC y Packet-Trace

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

[Solución de problemas con EPC](#)

[Solución de problemas con la ayuda de Cisco IOS-XE Packet Tracer Utility](#)

Introducción

Este documento describe el ejemplo de enfoque de solución de problemas de fallas de conectividad intermitente en un router que ejecuta Cisco IOS-XE SD-WAN mediante las utilidades de captura de paquetes incorporada (EPC) y seguimiento de paquetes.

Problema

Los usuarios de un sitio de sucursal informan de que algunas aplicaciones de Internet que utilizan acceso directo a Internet (DIA) como SAP®, SSH, algunos clientes FTP y un conjunto de otras aplicaciones están agotando el tiempo de espera si un usuario está inactivo durante más de 2-3 minutos. Si realizan alguna acción activa dentro de las aplicaciones que requieren comunicación de red, las aplicaciones funcionan bien y no se observan problemas.

Por ejemplo, si ejecuta **show version** y deja la sesión durante más de 2 minutos inactiva sin ninguna actividad y después de eso presione cualquier tecla en el teclado como en la salida aquí:

```
router#Connection reset by 100.64.2.9 port 22
```

El tiempo de espera de IDLE en la línea de terminal del router se verificó y se encontró que **exec-timeout** se establece en 10 minutos y no es responsable del comportamiento descrito (tenga en cuenta que otras aplicaciones también se ven afectadas):

```
router#show user
```

Line	User	Host(s)	Idle	Location
* 1 vty 0	ekhabaro	idle	00:00:00	10.149.4.41

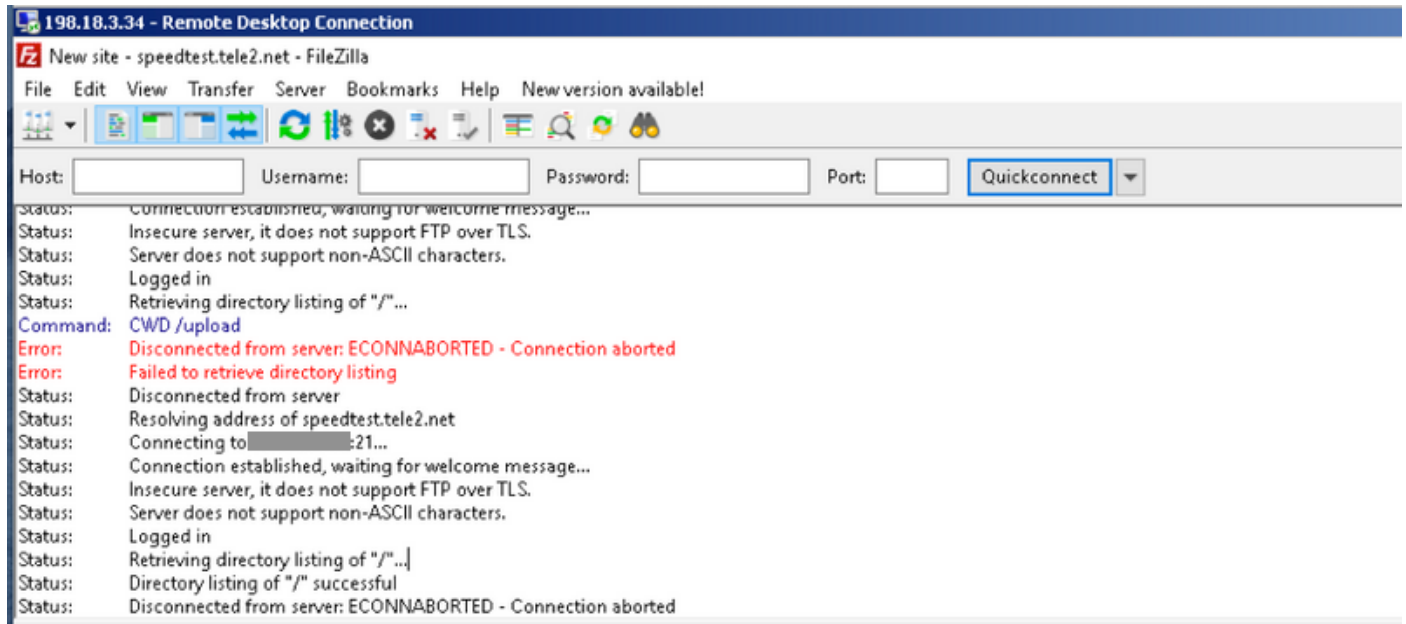
Interface	User	Mode	Idle	Peer Address
unknown	(ONEP)	csrmgmt_infr	00:00:14	

```
router#show line vty 0 | s Timeout
```

Timeouts:	Idle EXEC	Idle Session	Modem Answer	Session	Dispatch
	00:10:00	never		none	not set
		Idle Session Disconnect Warning			
		never			
		Login-sequence User Response			

```
00:00:30
Autoselect Initial Wait
not set
```

Otra forma de experimentar el problema en vivo es conectarse a algún FTP público. A continuación, si intenta actualizar la lista de directorios, cambiar de carpeta o descargar algo después de 2-3 minutos de inactividad, el mensaje se verá (en rojo):



Solución

Estos problemas son complejos para resolver problemas a veces, pero la gran ayuda puede proporcionar las utilidades [IOS-XE Datapath Packet Trace](#) y Embedded Packet Capture (EPC) IOS-XE. Aquí hay un ejemplo de uso y enfoque para resolver problemas.

Solución de problemas con EPC

Configure e inicie la captura de paquetes integrada (EPC) en el router. Dado que este sitio utiliza DIA, debe capturar el tráfico en las interfaces externas e internas por separado. Aquí 198.51.100.7 es la dirección IP del servidor FTP y 10.5.40.14 es la dirección IP del cliente:

```
Branch#config-transaction

admin connected from 127.0.0.1 using console on Branch
Branch(config)# ip access-list extended CAP_ACL
Branch(config-ext-nacl)# 10 permit ip any host 10.5.40.14
Branch(config-ext-nacl)# 20 permit ip host 10.5.40.14 any
Branch(config-ext-nacl)# 30 permit ip any host 198.51.100.7
Branch(config-ext-nacl)# 40 permit ip host 198.51.100.7 any
Branch(config-ext-nacl)# commit
Commit complete.
Branch(config-ext-nacl)# end
Branch#

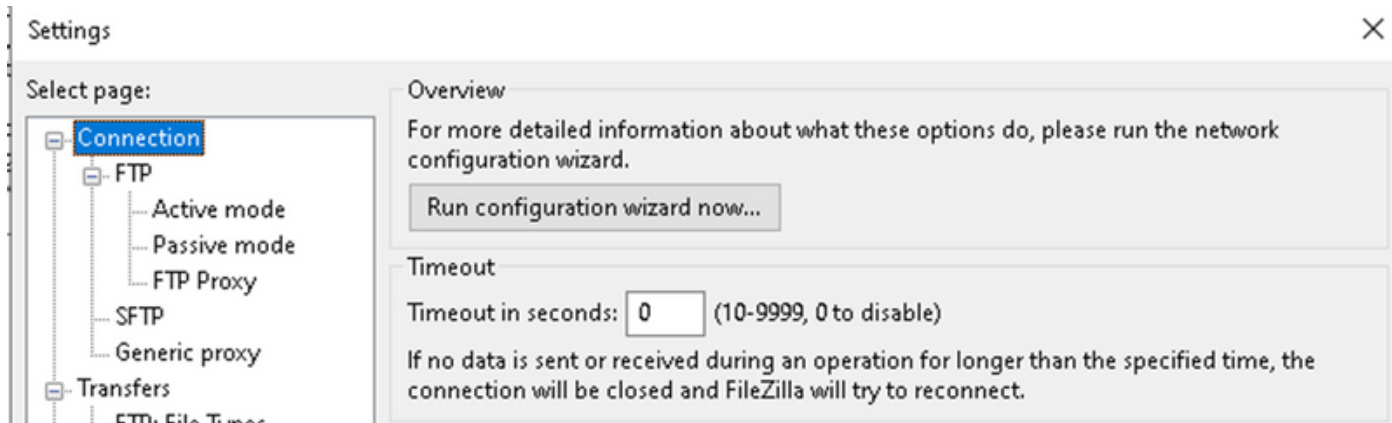
Branch#monitor capture CAP_EXT interface GigabitEthernet 2 both
Branch#monitor capture CAP_EXT interface GigabitEthernet 3 both
Branch#monitor capture CAP_INT interface GigabitEthernet 7 both
Branch#monitor capture CAP_EXT access-list CAP_ACL
Branch#monitor capture CAP_INT access-list CAP_ACL
Branch#monitor capture CAP_EXT start
```

```
Started capture point : CAP_EXT
```

```
Branch#monitor capture CAP_INT start
```

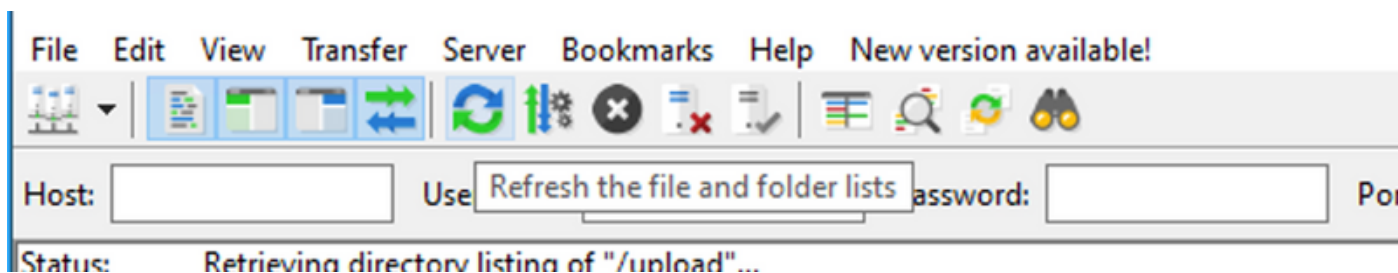
```
Started capture point : CAP_INT
```

A continuación, desde el host del usuario con conexión al servidor FTP mediante el cliente FTP FileZilla. Asegúrese de inhabilitar el tiempo de espera del cliente FTP para la conexión en **Edit > Settings** of FTP client options:



De forma predeterminada, el cliente FTP FileZilla cierra la sesión en sí después de 20 segundos y no puede reproducir el problema visto por el usuario con otras aplicaciones.

Después de aproximadamente 2-3 minutos de inactividad, intente actualizar el listado del directorio:



A continuación, en el cliente FTP verá el mensaje de error como en la captura de pantalla:

```
18:49:06      Status:    Retrieving directory listing of "/"...
18:49:25      Command:  PASV
18:49:25      Error:    Disconnected from server: ECONNABORTED - Connection aborted
18:49:25      Error:    Failed to retrieve directory listing
18:49:25      Status:    Disconnected from server
```

Luego, verifique que algunos paquetes fueron capturados tanto en interfaces internas como externas, detenga EPC y exporte búfers:

```
Branch#show monitor capture CAP_EXT buffer
buffer size (KB) : 10240
buffer used (KB) : 128
packets in buf   : 37
packets dropped  : 0
packets per sec  : 24
```

```
Branch#show monitor capture CAP_INT buffer
buffer size (KB) : 10240
```

```
buffer used (KB) : 128
packets in buf   : 39
packets dropped  : 0
packets per sec  : 1
```

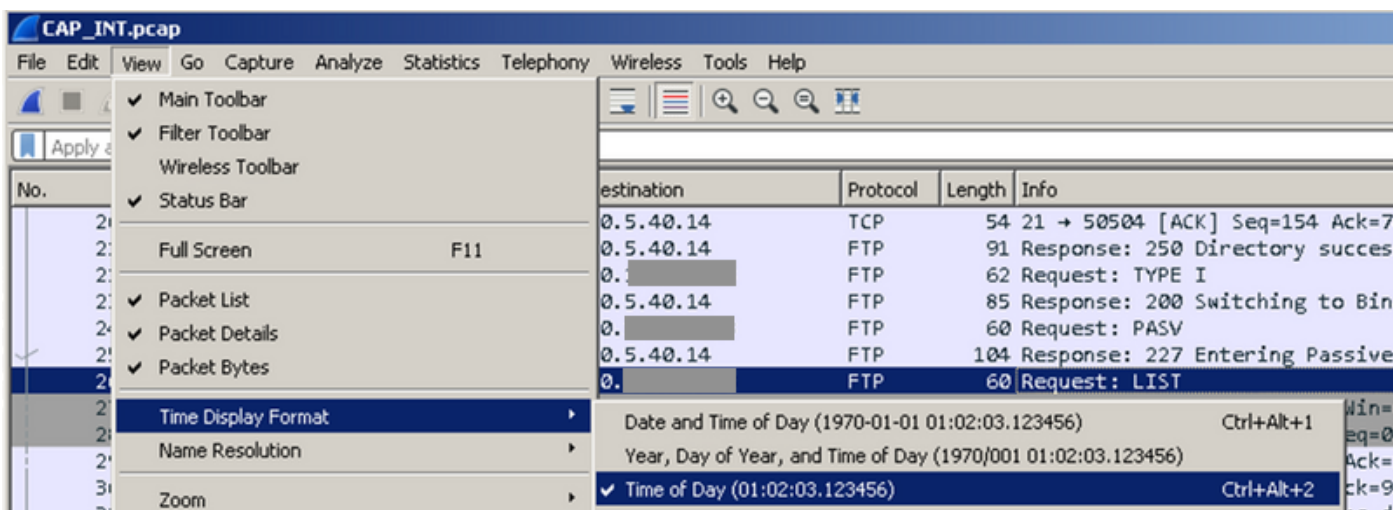
```
Branch#monitor capture CAP_INT stop_export
Exported Successfully
```

```
Branch#monitor capture CAP_EXT stop_export
Exported Successfully
```

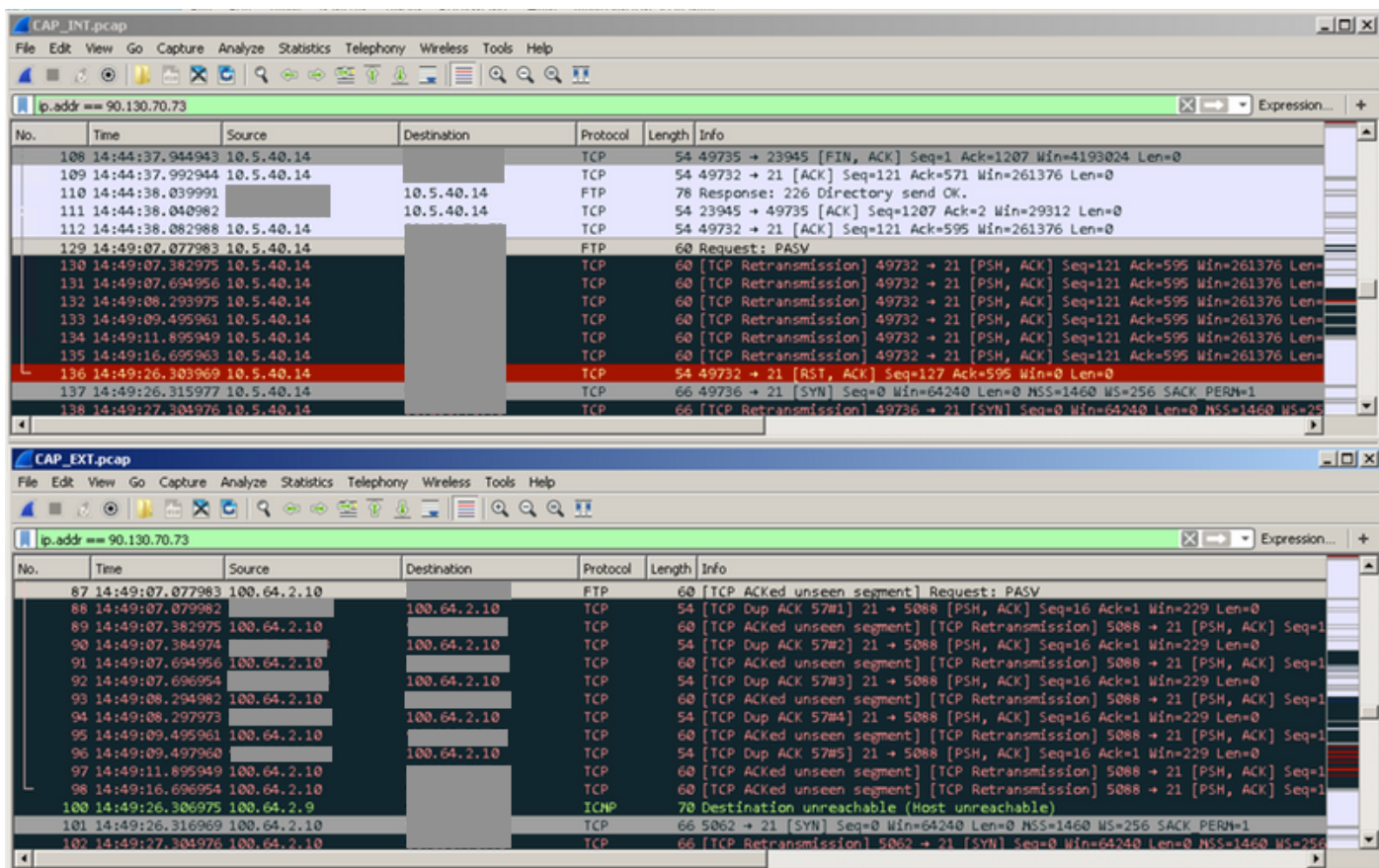
Y cargue capturas en su PC para que pueda analizarlas con Wireshark:

```
Branch#copy flash:CAP_INT.pcap sftp://admin:admin@203.0.113.36: vrf Mgmt-intf
Address or name of remote host [203.0.113.36]?
Destination username [admin]?
Destination filename [CAP_INT.pcap]?
SFTP send: Writing to /CAP_INT.pcap size 4362
!
4362 bytes copied in 0.296 secs (14736 bytes/sec)
Branch#copy flash:CAP_EXT.pcap sftp://admin:admin@203.0.113.36: vrf Mgmt-intf
Address or name of remote host [203.0.113.36]?
Destination username [admin]?
Destination filename [CAP_EXT.pcap]?
SFTP send: Writing to /CAP_EXT.pcap size 3839
!
3839 bytes copied in 0.299 secs (12839 bytes/sec)
```

Abra ambos archivos en las ventanas separadas de Wireshark y establezca **Time Display Format** para facilitar la correlación de paquetes en la interfaz exterior con paquetes en la interfaz interna mediante marcas de tiempo:



A continuación, alinee las ventanas y observe la diferencia entre las capturas de paquetes realizadas en las interfaces externas e internas (busque la solicitud **FTP PASV** en sus capturas):



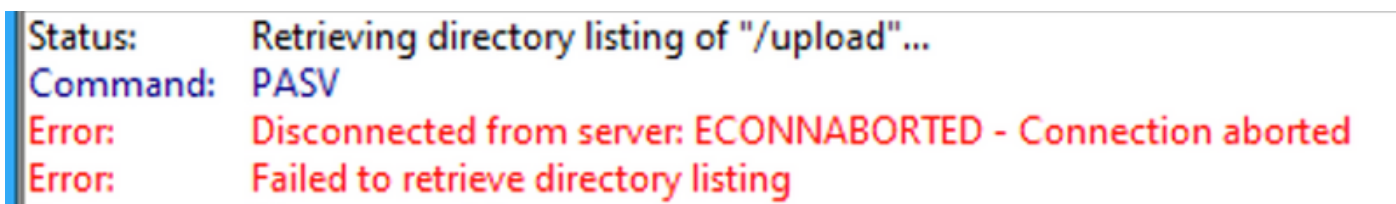
Pueden ver que la solicitud se envía al exterior y se han producido muchas retransmisiones. En este punto, no está claro por qué los paquetes de los hosts externos (por ejemplo, los paquetes número 88, 90, 92, etc.) no llegan al host interno, pero EPC nos proporcionó información valiosa y confirmó que algunos paquetes están siendo descartados por el router de borde c.

Solución de problemas con la ayuda de Cisco IOS-XE Packet Tracer Utility

Para investigar más a fondo, debe utilizar la captura de paquetes y filtrar los datos en función de la dirección pública del servidor FTP:

```
debug platform condition ipv4 198.51.100.7/32 both
debug platform packet-trace packet 1024 fia-trace data-size 4096
debug platform condition start
!if you want to capture HEX data of the packet, use as well:
debug platform packet-trace copy packet both size 2048 L2
```

A continuación, conéctese al FTP por segunda vez y espere más de 2-3 minutos antes de hacer clic en el botón de actualización o volver a descargar algo. En el registro, puede observar el mismo mensaje de error, como se muestra en la imagen:



Ahora, desde packet-trace puede ver que uno de los paquetes fue descartado:

Una vez realizada la configuración, repitamos la prueba, pero asegúrense de detener packet-trace y volver a empezar antes:

```
debug platform condition stop
debug platform packet-trace packet 1024 fia-trace data-size 4096
debug platform condition start
```

Cuando el problema se reproduce una vez más (por ejemplo, cuando intenta cambiar el directorio) y la conexión se pierde según los registros del cliente FTP (el cliente FTP intentó reconectarse), veamos las estadísticas de seguimiento de paquetes una vez más:

```
Branch# show platform packet-trace statistics
Packets Summary
  Matched  292
  Traced   292
Packets Received
  Ingress  282
  Inject   10
    Count   Code  Cause
    10      6    QFP Fwall generated packet
Packets Processed
  Forward  134
  Punt     134
    Count   Code  Cause
    5       22   QFP Fwall generated packet
    129     64   Service Engine packet
  Drop     24
    Count   Code  Cause
    21      55   ForUs
  Consume  0
```

Ahora puede notar otro código de descarte, "DROP 55 (ForUs)", a pesar de que desactivó la ACL implícita con la configuración **allow-service all**, los paquetes todavía se están descartando. Eche un vistazo más de cerca e intente comprender la diferencia entre los paquetes descartados y los paquetes reenviados:

```
Branch#show platform packet-trace summary
<skipped>
269  Gi3          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
270  Gi3          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
271  Tu6000001    Gi7                      FWD
272  Tu6000001    Gi7                      FWD
273  Gi7          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
274  Gi7          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
275  Tu6000001    Gi3                      FWD
276  Tu6000001    Gi3                      FWD
277  Gi7          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
278  Tu6000001    Gi3                      FWD
279  Gi3          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
280  Tu6000001    Gi7                      FWD
281  Gi7          internal0/0/svc_eng:0    PUNT  64  (Service Engine packet)
282  Tu6000001    Gi3                      FWD
283  Gi3          Gi3                      DROP  55  (ForUs)
284  Gi3          Gi3                      DROP  55  (ForUs)
285  Gi3          Gi3                      DROP  55  (ForUs)
286  Gi3          Gi3                      DROP  55  (ForUs)
287  Gi3          Gi3                      DROP  55  (ForUs)
```


tuple.l4_protocol : TCP
tuple.l3_protocol : IPV4
pkt_sb_state : 0
pkt_sb.num_flows : 1
pkt_sb.tuple_epoch : 32
returned cft_error : 0
returned fid : 0xec4eeb70

Feature: NBAR

Packet number in flow: N/A
Classification state: Final
Classification name: ftp-data
Classification ID: [IANA-L4:20]
Classification source: Unknown
Number of matched sub-classifications: 0
Number of extracted fields: 0
Is PA (split) packet: False
TPH-MQC bitmask value: 0x0
Is optimized packet: False

Feature: IPV4_INPUT_STILE_LEGACY_EXT

Entry : Input - 0x81835ba8
Input : GigabitEthernet3
Output : <unknown>
Lapsed time : 315800 ns

Feature: IPV4_INPUT_FNF_FIRST_EXT

Entry : Input - 0x81818128
Input : GigabitEthernet3
Output : <unknown>
Lapsed time : 62200 ns

Feature: SDWAN_APP_ROUTE_POLICY_EXT

Entry : Input - 0x8183c758
Input : GigabitEthernet3
Output : <unknown>
Lapsed time : 12440 ns

Feature: SDWAN_DATA_POLICY_OUT_EXT

Entry : Input - 0x8183c754
Input : GigabitEthernet3
Output : <unknown>
Lapsed time : 12520 ns

Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT

Entry : Input - 0x817e8864
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 8900 ns

Feature: IPV4_INPUT_IPOPTIONS_GOTO_OUTPUT_FEATURE_EXT

Entry : Output - 0x817e895c
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 9840 ns

Feature: CBUG_OUTPUT_FIA

Entry : Output - 0x817e8840
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 6520 ns

Feature: IPV4_OUTPUT_VFR

Entry : Output - 0x817e89b4
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 3660 ns

Feature: ZBFW

Action : Fwd
Zone-pair name : ZP_GUEST-INSIDE_OUTSID_642078363
Class-map name : BRANCH-DIA-GUEST-seq-11-cm_
Input interface : GigabitEthernet3
Egress interface : GigabitEthernet7

AVC Classification ID : 0
AVC Classification name: N/A
Feature: IPV4_OUTPUT_INSPECT
Entry : Output - 0x8181c97c
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 296980 ns
Feature: CFT
API : cft_handle_pkt
packet capabilities : 0x00000014
input vrf_idx : 0
calling feature : UTD
direction : Input
triplet.vrf_idx : 3
triplet.network_start : 0x01003f8e
triplet.triplet_flags : 0x00000004
triplet.counter : 32
cft_bucket_number : 942419
cft_l3_payload_size : 20
cft_pkt_ind_flags : 0x00000100
cft_pkt_ind_valid : 0x0000bbff
tuple.src_ip : 198.51.100.7
tuple.dst_ip : 10.5.40.14
tuple.src_port : 28143
tuple.dst_port : 49588
tuple.vrfid : 3
tuple.l4_protocol : TCP
tuple.l3_protocol : IPV4
pkt_sb_state : 0
pkt_sb.num_flows : 1
pkt_sb.tuple_epoch : 32
returned cft_error : 0
returned fid : 0xec4eeb70
Feature: UTD Policy (First FIA)
Action : Divert
Input interface : GigabitEthernet3
Egress interface: GigabitEthernet7
Feature: OUTPUT_UTD_FIRST_INSPECT
Entry : Output - 0x8183a0d8
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 117420 ns
Feature: UTD Inspection
Action : Divert
Input interface : GigabitEthernet3
Egress interface: GigabitEthernet7
Feature: OUTPUT_UTD_FINAL_INSPECT
Entry : Output - 0x8183a108
Input : GigabitEthernet3
Output : GigabitEthernet7
Lapsed time : 122900 ns
Feature: IPV4_OUTPUT_LOOKUP_PROCESS_EXT
Entry : Output - 0x817ee0e8
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 10980 ns
Feature: IPV4_OUTPUT_GOTO_OUTPUT_FEATURE_EXT
Entry : Output - 0x817edfd0
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 16200 ns
Feature: CBUG_OUTPUT_FIA
Entry : Output - 0x817e8840
Input : GigabitEthernet3

Output : Tunnel6000001
Lapsed time : 4960 ns
Feature: IPV4_OUTPUT_VFR
Entry : Output - 0x817e89b4
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 520 ns
Feature: IPV4_OUTPUT_INSPECT
Entry : Output - 0x8181c97c
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 4420 ns
Feature: IPV4_OUTPUT_THREAT_DEFENSE
Entry : Output - 0x81838278
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 3300 ns
Feature: IPV4_VFR_REFRAG
Entry : Output - 0x817e89c0
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 320 ns
Feature: DEBUG_COND_APPLICATION_OUT_CLR_TXT
Entry : Output - 0x817e8854
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 4740 ns
Feature: UTD Encaps
Action : Encaps
Input interface : GigabitEthernet3
Egress interface: Tunnel6000001
Feature: IPV4_OUTPUT_L2_REWRITE
Entry : Output - 0x817e83b0
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 296420 ns
Feature: DEBUG_COND_MAC_EGRESS
Entry : Output - 0x817e8844
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 860 ns
Feature: DEBUG_COND_APPLICATION_OUT
Entry : Output - 0x817e8850
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 300 ns
Feature: IPV4_OUTPUT_FRAG
Entry : Output - 0x817e89a8
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 2560 ns
Feature: IPV4_OUTPUT_SDWAN_FNF_FINAL
Entry : Output - 0x818181b8
Input : GigabitEthernet3
Output : Tunnel6000001
Lapsed time : 100980 ns
Feature: IPV4_TUNNEL_OUTPUT_FINAL
Entry : Output - 0x81838bac
Input : Tunnel6000001
Output : Tunnel6000001
Lapsed time : 55460 ns
Feature: IPV4_TUNNEL_GOTO_OUTPUT
Entry : Output - 0x81838bb0
Input : Tunnel6000001

Output : Tunnel6000001
Lapsed time : 3920 ns
Feature: IPV4_TUNNEL_FW_CHECK_EXT
Entry : Output - 0x81838de8
Input : Tunnel6000001
Output : Tunnel6000001
Lapsed time : 9520 ns
Feature: IPV4_INPUT_DST_LOOKUP_ISSUE_EXT
Entry : Output - 0x817e8858
Input : Tunnel6000001
Output : Tunnel6000001
Lapsed time : 14960 ns
Feature: IPV4_INPUT_ARL_EXT
Entry : Output - 0x817e89d0
Input : Tunnel6000001
Output : Tunnel6000001
Lapsed time : 5680 ns
Feature: IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT
Entry : Output - 0x817e8870
Input : Tunnel6000001
Output : Tunnel6000001
Lapsed time : 1260 ns
Feature: IPV4_TUNNEL_ENCAP_FOR_US_EXT
Entry : Output - 0x81838db8
Input : Tunnel6000001
Output : Tunnel6000001
Lapsed time : 5460 ns
Feature: IPV4_INPUT_LOOKUP_PROCESS_EXT
Entry : Output - 0x817e8864
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 960 ns
Feature: IPV4_TUNNEL_ENCAP_GOTO_OUTPUT_FEATURE_EXT
Entry : Output - 0x817ee30c
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 13020 ns
Feature: CBUG_OUTPUT_FIA
Entry : Output - 0x817e8840
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 1980 ns
Feature: IPV4_OUTPUT_VFR
Entry : Output - 0x817e89b4
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 660 ns
Feature: IPV4_OUTPUT_INSPECT
Entry : Output - 0x8181c97c
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 15960 ns
Feature: IPV4_OUTPUT_THREAT_DEFENSE
Entry : Output - 0x81838278
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 1720 ns
Feature: IPV4_VFR_REFRAG
Entry : Output - 0x817e89c0
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 660 ns
Feature: DEBUG_COND_APPLICATION_OUT_CLR_TXT
Entry : Output - 0x817e8854

Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 1560 ns
Feature: IPV4_OUTPUT_L2_REWRITE
Entry : Output - 0x817e83b0
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 10420 ns
Feature: DEBUG_COND_MAC_EGRESS
Entry : Output - 0x817e8844
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 520 ns
Feature: DEBUG_COND_APPLICATION_OUT
Entry : Output - 0x817e8850
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 180 ns
Feature: IPV4_OUTPUT_FRAG
Entry : Output - 0x817e89a8
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 940 ns
Feature: IPV4_OUTPUT_SDWAN_FNF_FINAL
Entry : Output - 0x818181b8
Input : Tunnel6000001
Output : VirtualPortGroup1
Lapsed time : 2560 ns
Feature: OUTPUT_SERVICE_ENGINE
Entry : Output - 0x81834550
Input : Tunnel6000001
Output : internal0/0/svc_eng:0
Lapsed time : 65820 ns
Feature: IPV4_INTERNAL_ARL_SANITY_EXT
Entry : Output - 0x817e89f4
Input : Tunnel6000001
Output : internal0/0/svc_eng:0
Lapsed time : 12280 ns
Feature: ZBFW
Action : Fwd
Zone-pair name : N/A
Class-map name : N/A
Input interface : Tunnel6000001
Egress interface : internal0/0/svc_eng:0
AVC Classification ID : 0
AVC Classification name: N/A
Feature: IPV4_OUTPUT_INSPECT_EXT
Entry : Output - 0x8181c97c
Input : Tunnel6000001
Output : internal0/0/svc_eng:0
Lapsed time : 38200 ns
Feature: IPV4_OUTPUT_THREAT_DEFENSE_EXT
Entry : Output - 0x81838278
Input : Tunnel6000001
Output : internal0/0/svc_eng:0
Lapsed time : 1980 ns
Feature: IPV4_VFR_REFRAG_EXT
Entry : Output - 0x817e89c0
Input : Tunnel6000001
Output : internal0/0/svc_eng:0
Lapsed time : 400 ns
Feature: IPV4_OUTPUT_DROP_POLICY_EXT
Entry : Output - 0x817e893c
Input : Tunnel6000001

Flags: unknown
Appl type: none
WLAN-Flags: unknown
Mac-Address: 0000.0000.0000 Input-IDB:
VRF: 40, entry-id: 0xee541ec0, use_count:1
In_pkts: 24 In_bytes: 698, Out_pkts: 13 Out_bytes: 605
Output-IDB: GigabitEthernet3

tcp 100.64.2.10:5795 10.5.40.14:49644 52.179.129.229:443 52.179.129.229:443
create: 11/07/19 13:01:18, use: 11/07/19 13:01:18, timeout: 00:00:09
Map-Id(In): 1
Flags: timing-out
Appl type: none
WLAN-Flags: unknown
Mac-Address: 0000.0000.0000 Input-IDB:
VRF: 40, entry-id: 0xee542640, use_count:1
In_pkts: 29 In_bytes: 5114, Out_pkts: 12 Out_bytes: 7113
Output-IDB: GigabitEthernet3

tcp 100.64.2.10:5802 10.5.40.14:49649 198.51.100.7:21319 198.51.100.7:21319
create: 11/07/19 13:02:06, use: 11/07/19 13:02:06, timeout: 00:00:57
Map-Id(In): 1
Flags: timing-out
Appl type: none
WLAN-Flags: unknown
Mac-Address: 0000.0000.0000 Input-IDB:
VRF: 40, entry-id: 0xee541380, use_count:1
In_pkts: 8 In_bytes: 184, Out_pkts: 4 Out_bytes: 837
Output-IDB: GigabitEthernet3

tcp 100.64.2.10:5800 10.5.40.14:49636 198.51.100.7:21 198.51.100.7:21
create: 11/07/19 13:02:05, use: 11/07/19 13:02:05, timeout: 00:00:56
Map-Id(In): 1
Flags: timing-out
Appl type: none
WLAN-Flags: unknown
Mac-Address: 0000.0000.0000 Input-IDB:
VRF: 40, entry-id: 0xee5423c0, use_count:1
In_pkts: 2 In_bytes: 66, Out_pkts: 1 Out_bytes: 20
Output-IDB: GigabitEthernet3

tcp 100.64.2.10:5633 10.5.40.14:49432 52.242.211.89:443 52.242.211.89:443
create: 11/07/19 12:44:18, use: 11/07/19 13:01:17, timeout: 00:00:08
Map-Id(In): 1
Flags: unknown
Appl type: none
WLAN-Flags: unknown
Mac-Address: 0000.0000.0000 Input-IDB:
VRF: 40, entry-id: 0xee527840, use_count:1
In_pkts: 53 In_bytes: 6257, Out_pkts: 29 Out_bytes: 7030
Output-IDB: GigabitEthernet3

tcp 100.64.2.10:5792 10.5.40.14:49647 51.143.111.7:443 51.143.111.7:443
create: 11/07/19 13:02:00, use: 11/07/19 13:02:09, timeout: 00:01:00
Map-Id(In): 1
Flags: syn_in
Appl type: none
WLAN-Flags: unknown
Mac-Address: 0000.0000.0000 Input-IDB:
VRF: 40, entry-id: 0xee542500, use_count:1
In_pkts: 6 In_bytes: 224, Out_pkts: 3 Out_bytes: 96
Output-IDB: GigabitEthernet3

Total number of translations: 12

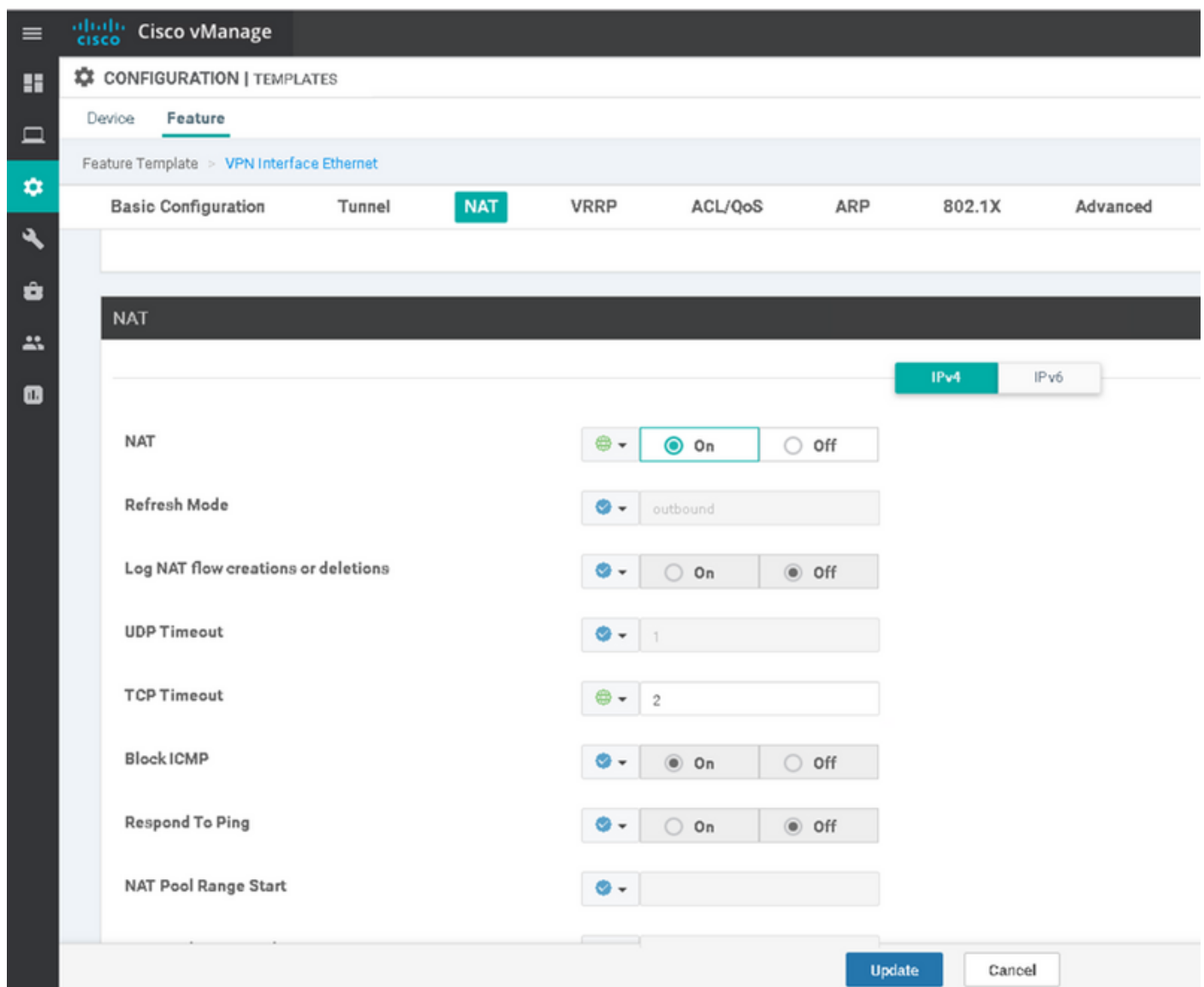
Y preste atención al tiempo de espera. ¿No parece sospechosamente bajo? Después de aproximadamente 2-3 minutos de inactividad del cliente FTP, vuelva a comprobarlo y podrá ver que no hay traducciones en la tabla NAT:

```
Branch# show ip nat translations | i 198.51.100.7
Branch#
```

¡Voila! Para que la causa raíz del problema: las sesiones caducan demasiado rápido y, a pesar de que desde la perspectiva de la sesión del cliente FTP aún existe, el router cEdge ya no sabe nada acerca de esa sesión TCP y descarta el tráfico de retorno. Si marca la configuración, encontrará que el tiempo de espera de la sesión NAT se configura como 120 segundos, probablemente por error:

```
Branch#show run | i tcp-timeout
ip nat translation tcp-timeout 120
Branch#
```

Y este temporizador se debe corregir en la plantilla de dispositivo correspondiente en vManage:



Por ejemplo, cámbielo a 60 min y luego se resuelve el problema.