

Voorbeeld van IOS-XE SD-WAN probleemoplossing met behulp van EPC en Packet-Trace

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Probleemoplossing met EPC](#)

[Probleemoplossing met Help voor Cisco IOS-XE Packet Tracer-hulpprogramma](#)

Inleiding

Dit document beschrijft het voorbeeld van intermitterende problemen met de probleemoplossing van connectiviteit op een router die Cisco IOS-XE SD-WAN met Embedded Packet Capture (EPC) en Packet Trace Hulpprogramma's uitvoert.

Probleem

Uw gebruikers van een Vestigingssite melden dat sommige internettoepassingen die Direct Internet Access (DIA) gebruiken zoals SAP®, SSH, sommige FTP-clients en een reeks andere toepassingen, de timing van een gebruikershandleiding langer dan ongeveer 2-3 minuten gebruiken. Als zij actieve acties binnen de toepassingen uitvoeren die netwerkcommunicatie vereisen, werken de toepassingen goed en er worden geen problemen waargenomen.

Als u bijvoorbeeld **een show-versie** uitvoert en de sessie meer dan 2 minuten stilaat zonder activiteit en daarna op een toets op het toetsenbord drukt zoals in de output hier:

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

De tijd van het IDLE op de eindlijn van de router werd gecontroleerd en ontdekte dat de **exec-timeout** is ingesteld op 10 minuten en niet verantwoordelijk is voor het beschreven gedrag (houd in gedachten dat andere toepassingen ook worden beïnvloed):

```
router#show user
```

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

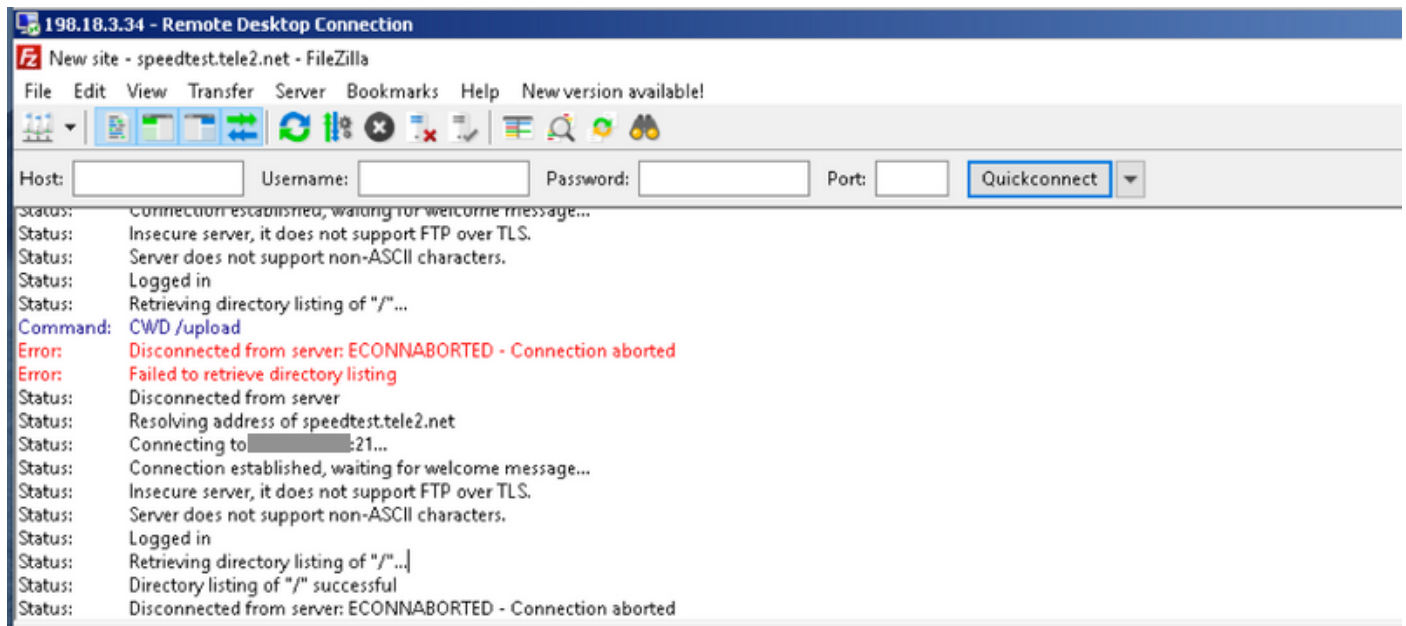
Interface	User	Mode	Idle	Peer Address
unknown	(ONEP)	csrmgmt_infr	00:00:14	

```
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

Een andere manier om het probleem live te ervaren is door verbinding te maken met een of ander openbaar FTP. Als u vervolgens een directory-lijst probeert op te frissen, map te wijzigen of iets te downloaden na 2-3 minuten inactiviteit, wordt het bericht weergegeven (in rood):



Oplossing

Zulke kwesties zijn complex om soms problemen op te lossen, maar grote hulp kan [IOS-XE Datapath Packet Trace-functie](#) en ingesloten Packet Capture (EPC) IOS-XE hulpprogramma's leveren. Hier een voorbeeld van gebruik en benadering van probleemoplossing.

Probleemoplossing met EPC

Configureer en start Embedded Packet Capture (EPC) op de router. Aangezien deze site DIA gebruikt, moet u afzonderlijk verkeer op externe en interne interfaces opnemen. Hier is 198.51.100.7 het IP-adres van FTP server en 10.5.40.14 is het IP-adres van de client:

```
Branch#config-transaction

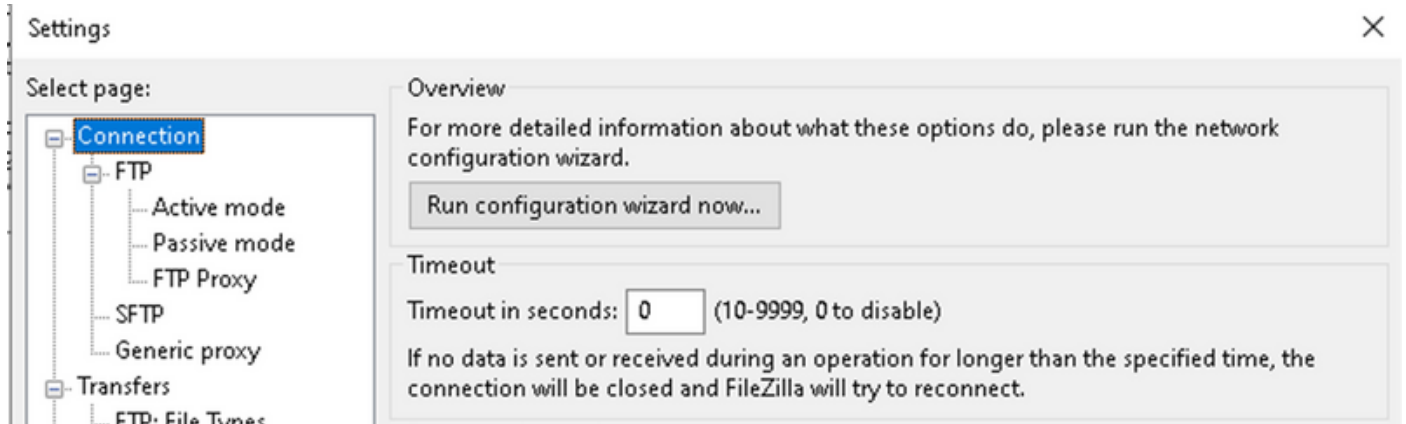
admin connected from 127.0.0.1 using console on Branch
Branch(config)# ip access-list extended CAP_ACL
Branch(config-ext-nacl)# 10 permit ip any host 10.5.40.14
Branch(config-ext-nacl)# 20 permit ip host 10.5.40.14 any
Branch(config-ext-nacl)# 30 permit ip any host 198.51.100.7
Branch(config-ext-nacl)#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

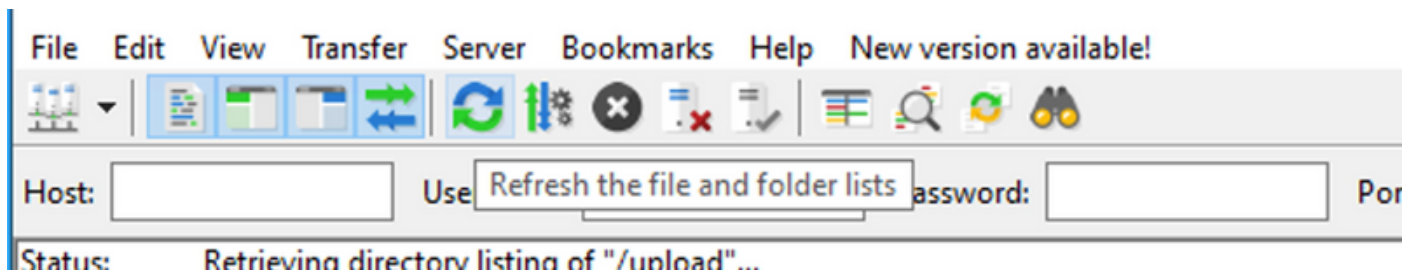
```
Branch#monitor capture CAP_INT start  
Started capture point : CAP_INT
```

Daarna, van de host van de gebruiker met verbinding met de FTP server met FileZilla FTP-client. Zorg ervoor dat de tijdelijke versie van FTP-client voor een verbinding wordt uitgeschakeld in het programma **Bewerken > Instellingen** van FTP-clientopties:



Standaard sluit FileZilla FTP-client de sessie zelf na 20 seconden en kunt u het probleem dat door de gebruiker wordt gezien, niet met andere toepassingen reproduceren.

Probeer na ongeveer 2-3 minuten inactiviteit een directory-lijst op te frissen:



Vervolgens ziet u in de FTP-client de foutmelding zoals in de screenshot:

```
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
```

Controleer vervolgens dat sommige pakketten binnen en buiten interfaces werden opgenomen, stop EPC en export buffers:

```
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
```

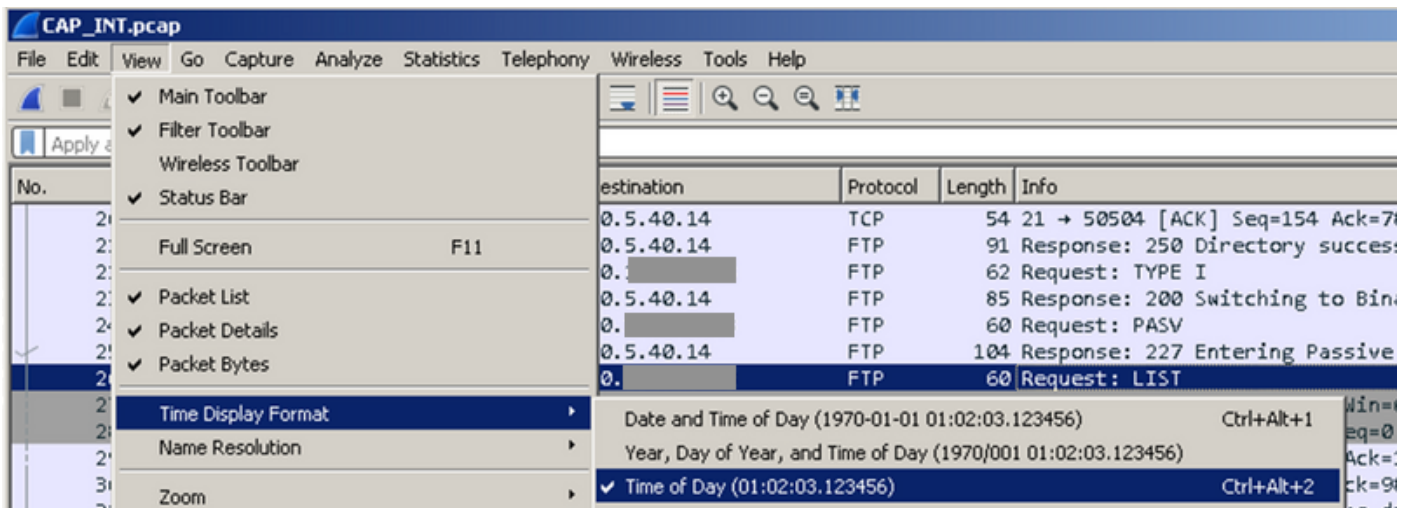
```
Branch#monitor capture CAP_INT stop_export
Exported Successfully
```

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

En uploadtoken op uw pc zodat u deze kunt analyseren met 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)
```

Open beide bestanden in de afzonderlijke Windows-vensters en stel het formaat **Time Display** in zodat het gemakkelijker wordt om pakketten op de externe interface te correleren met pakketten op de interne interface door tijdzegels:



Lijnt vervolgens vensters uit en merk het verschil op tussen pakketvastlegging die op de externe en de interne interfaces is gemaakt (zoek in uw opnamen naar **FTP PASV**-verzoek):

The top screenshot shows a packet capture with a filter 'ip.addr == 90.130.70.73'. The table below represents the visible data:

No.	Time	Source	Destination	Protocol	Length	Info
108	14:44:37.944943	10.5.40.14		TCP	54	49735 → 23945 [FIN, ACK] Seq=1 Ack=1207 Win=4193024 Len=0
109	14:44:37.992944	10.5.40.14		TCP	54	49732 → 21 [ACK] Seq=121 Ack=571 Win=261376 Len=0
110	14:44:38.039991		10.5.40.14	FTP	78	Response: 226 Directory send OK.
111	14:44:38.040982		10.5.40.14	TCP	54	23945 → 49735 [ACK] Seq=1207 Ack=2 Win=29312 Len=0
112	14:44:38.082988	10.5.40.14		TCP	54	49732 → 21 [ACK] Seq=121 Ack=595 Win=261376 Len=0
129	14:49:07.077983	10.5.40.14		FTP	60	Request: PASV
130	14:49:07.382975	10.5.40.14		TCP	60	[TCP Retransmission] 49732 → 21 [PSH, ACK] Seq=121 Ack=595 Win=261376 Len=0
131	14:49:07.694956	10.5.40.14		TCP	60	[TCP Retransmission] 49732 → 21 [PSH, ACK] Seq=121 Ack=595 Win=261376 Len=0
132	14:49:08.293975	10.5.40.14		TCP	60	[TCP Retransmission] 49732 → 21 [PSH, ACK] Seq=121 Ack=595 Win=261376 Len=0
133	14:49:09.495961	10.5.40.14		TCP	60	[TCP Retransmission] 49732 → 21 [PSH, ACK] Seq=121 Ack=595 Win=261376 Len=0
134	14:49:11.895949	10.5.40.14		TCP	60	[TCP Retransmission] 49732 → 21 [PSH, ACK] Seq=121 Ack=595 Win=261376 Len=0
135	14:49:16.695963	10.5.40.14		TCP	60	[TCP Retransmission] 49732 → 21 [PSH, ACK] Seq=121 Ack=595 Win=261376 Len=0
136	14:49:26.303969	10.5.40.14		TCP	54	49732 → 21 [RST, ACK] Seq=127 Ack=595 Win=0 Len=0
137	14:49:26.315977	10.5.40.14		TCP	66	49736 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
138	14:49:27.304976	10.5.40.14		TCP	66	[TCP Retransmission] 49736 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256

The bottom screenshot shows a packet capture with the same filter. The table below represents the visible data:

No.	Time	Source	Destination	Protocol	Length	Info
87	14:49:07.077983	100.64.2.10		FTP	60	[TCP ACKed unseen segment] Request: PASV
88	14:49:07.079982		100.64.2.10	TCP	54	[TCP Dup ACK 57W1] 21 → 5088 [PSH, ACK] Seq=16 Ack=1 Win=229 Len=0
89	14:49:07.382975	100.64.2.10		TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 5088 → 21 [PSH, ACK] Seq=1
90	14:49:07.384974		100.64.2.10	TCP	54	[TCP Dup ACK 57W2] 21 → 5088 [PSH, ACK] Seq=16 Ack=1 Win=229 Len=0
91	14:49:07.694956	100.64.2.10		TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 5088 → 21 [PSH, ACK] Seq=1
92	14:49:07.696954		100.64.2.10	TCP	54	[TCP Dup ACK 57W3] 21 → 5088 [PSH, ACK] Seq=16 Ack=1 Win=229 Len=0
93	14:49:08.294982	100.64.2.10		TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 5088 → 21 [PSH, ACK] Seq=1
94	14:49:08.297973		100.64.2.10	TCP	54	[TCP Dup ACK 57W4] 21 → 5088 [PSH, ACK] Seq=16 Ack=1 Win=229 Len=0
95	14:49:09.495961	100.64.2.10		TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 5088 → 21 [PSH, ACK] Seq=1
96	14:49:09.497960		100.64.2.10	TCP	54	[TCP Dup ACK 57W5] 21 → 5088 [PSH, ACK] Seq=16 Ack=1 Win=229 Len=0
97	14:49:11.895949	100.64.2.10		TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 5088 → 21 [PSH, ACK] Seq=1
98	14:49:16.696954	100.64.2.10		TCP	60	[TCP ACKed unseen segment] [TCP Retransmission] 5088 → 21 [PSH, ACK] Seq=1
100	14:49:26.306975	100.64.2.9		ICMP	70	Destination unreachable (Host unreachable)
101	14:49:26.316969	100.64.2.10		TCP	66	5062 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
102	14:49:27.304976	100.64.2.10		TCP	66	[TCP Retransmission] 5062 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256

Je ziet dat verzoek naar buiten wordt gestuurd en er is een hoop terugzending gebeurd. Op dit punt is het niet duidelijk waarom pakketten van de externe hosts (bijv. pakketten nummer 88,90,92 enzovoort) niet op de interne host terecht komen, maar EPC heeft ons waardevolle informatie verstrekt en bevestigd dat sommige pakketten door cEdge-router worden gedropt.

Probleemoplossing met Help voor Cisco IOS-XE Packet Tracer-hulpprogramma

Om verder te onderzoeken moet u pakketvastlegging en filtergegevens gebruiken die op het openbare adres van de FTP-server zijn gebaseerd:

```
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
```

Sluit vervolgens een tweede keer op de FTP-site en wacht langer dan 2 tot 3 minuten voordat u op de verfrissingsknop klikt of iets opnieuw downloaden. In het logbestand kunt u dezelfde foutmelding waarnemen als in de afbeelding:

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

Vanaf een pakketspoor kunt u zien dat een van de pakketten is gevallen:

Als de configuratie is voltooid, herhaal dan de test, maar zorg ervoor dat u het pakkettraceren stopt en opnieuw start voor:

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

Wanneer het probleem opnieuw wordt gereproduceerd (bijvoorbeeld wanneer u probeert om folder te wijzigen) en de verbinding verloren is als per logs van FTP client (FTP client probeert om verbinding te maken), laten we pakkettraceren statistieken opnieuw zien:

```
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
```

Nu kunt u een andere dalcode, "DROP 55 (Voorons)" merken, ondanks dat u impliciete ACL met **de-dienst alle** configuratie hebt uitgeschakeld, worden de pakketten nog steeds ingetrokken. Neem een kijkje bij de hand en probeer het verschil tussen de gedemonteerde pakketten en de verzonden pakketten te begrijpen:

```
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

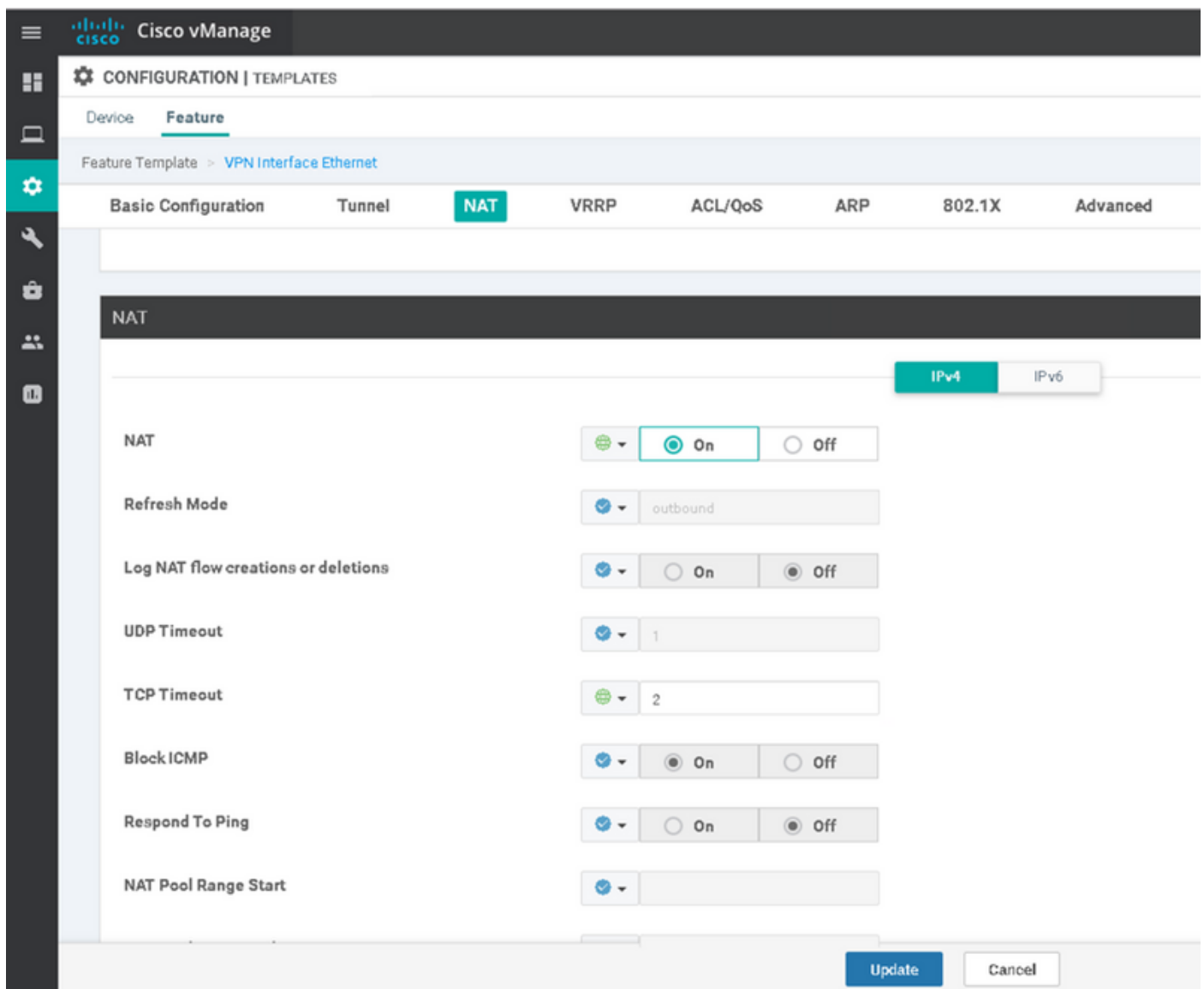
En let op de pauze. Ziet het er niet achterlijk laag uit? Na ongeveer 2-3 minuten inactiviteit van FTP-client, controleer dit nogmaals en u kunt zien dat er geen vertalingen in de NAT-tabel zijn:

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

Voilà! Zodat de oorzaak van het probleem: De sessies verlopen te snel en ondanks dat vanuit het perspectief van de FTP clientsessie nog bestaat, weet de cEdge-router niets over die TCP-sessie al en daalt hij het retourverkeer. Als u de configuratie controleert, ziet u dat de NAT sessietijd ingesteld is op 120 seconden, waarschijnlijk per ongeluk:

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

En deze timer moet in de corresponderende apparaatsjabloon op vManager worden vastgelegd:



Verander bijvoorbeeld naar 60 min. en dan wordt het probleem opgelost.