

# Example of IOS-XE SD-WAN Issues Troubleshoot With Help of EPC and Packet-Trace

## Contents

[Introduction](#)

[Problem](#)

[Solution](#)

[Troubleshoot with EPC](#)

[Troubleshoot with Help of Cisco IOS-XE Packet Tracer Utility](#)

## Introduction

This document describes the example of intermittent connectivity failures troubleshoot approach on a router running Cisco IOS-XE SD-WAN using Embedded Packet Capture (EPC) and Packet Trace utilities.

## Problem

Your users of a Branch site report that some Internet applications that use Direct Internet Access (DIA) like SAP®, SSH, some FTP clients and set of others applications are timing out if a user is idle longer than about 2-3 minutes. If they perform any active actions within the applications requiring network communication, applications work well and no problems are observed.

For instance, if you execute **show version** and leave the session for more than 2 minutes idle without any activity and after that press any key on the keyboard as in the output here:

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

IDLE timeout on the terminal line of the router was checked and found that **exec-timeout** is set to 10 minutes and is not responsible for the described behavior (keep in mind that other applications are also affected):

```
router#show user
```

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

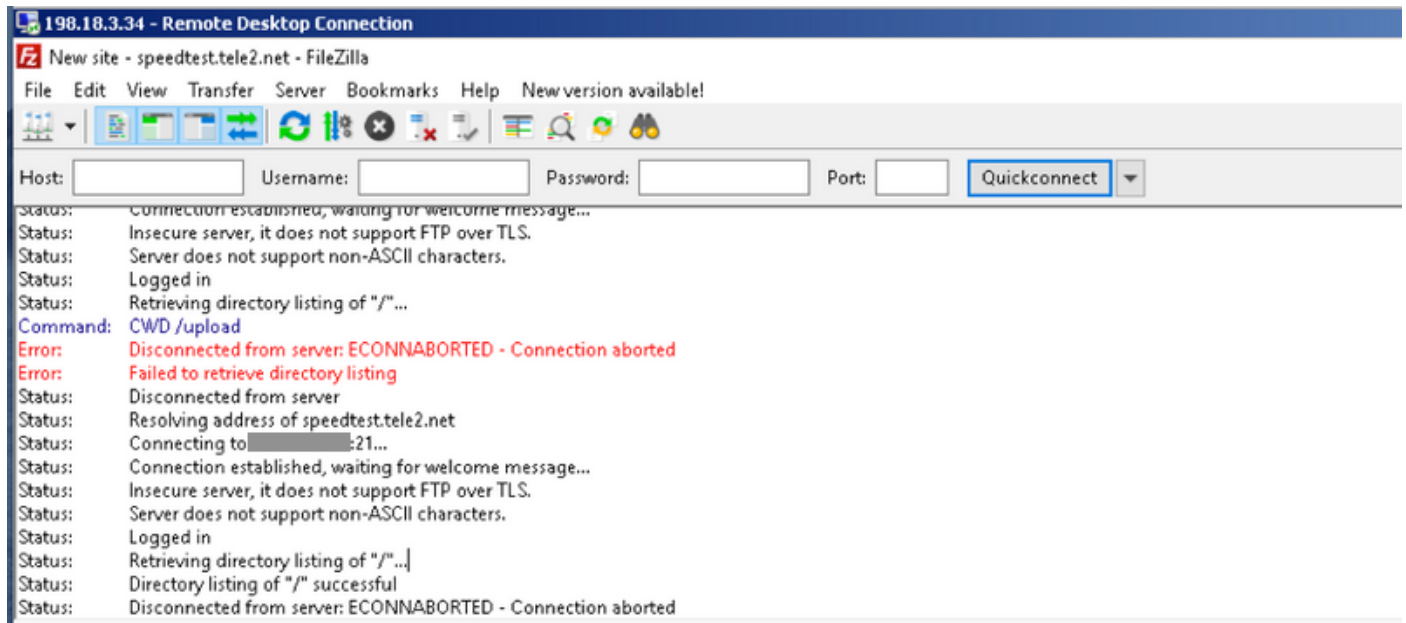
Interface	User	Mode	Idle	Peer Address
unknown	(ONEP)	csrmgmt_infr	00:00:14	

```
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

Another way to experience the problem live is to connect to some public FTP. Then, If you try to refresh directory listing, change folder or download something after 2-3 minutes of inactivity, the message is seen (in red):



## Solution

Such issues are complex to troubleshoot sometimes, but great help can provide [IOS-XE Datapath Packet Trace feature](#) and Embedded Packet Capture (EPC) IOS-XE utilities. Here an example of usage and approach to troubleshoot.

## Troubleshoot with EPC

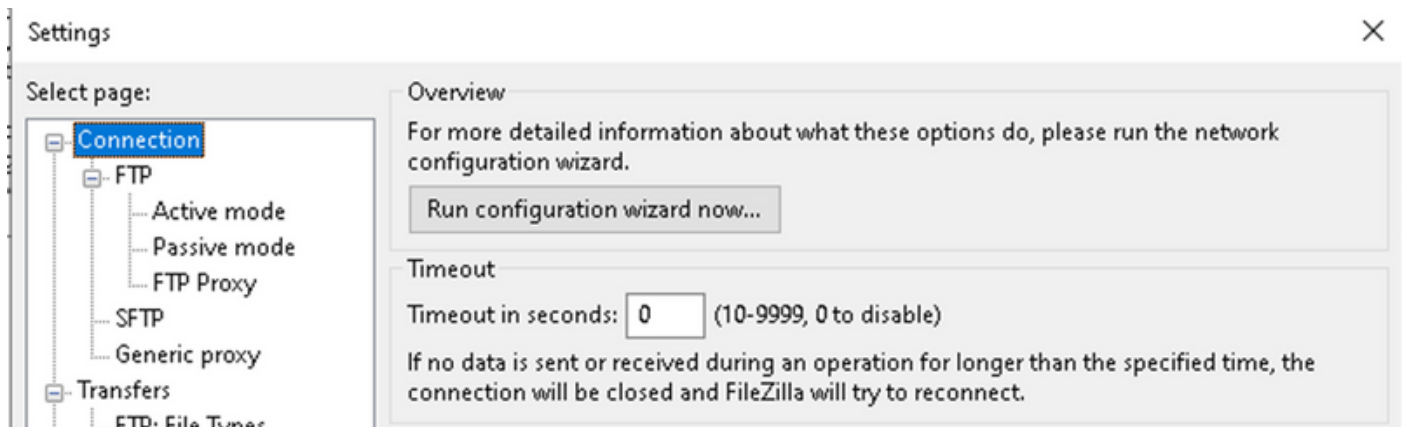
Configure and start Embedded Packet Capture (EPC) on the router. Since this site is using DIA, you need to capture traffic on external and internal interfaces separately. Here 198.51.100.7 is the IP-address of FTP server and 10.5.40.14 is the IP-address of the client:

```
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
```

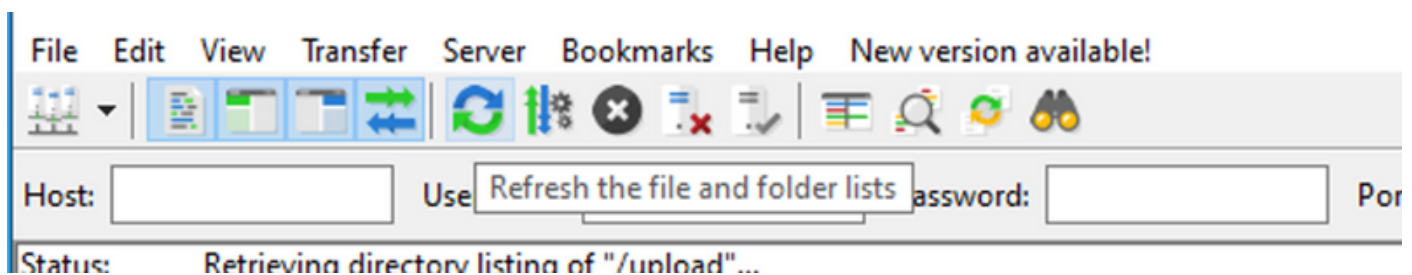
```
Branch#monitor capture CAP_INT start
Started capture point : CAP_INT
```

Next, from the user's host with connect to the FTP server using FileZilla FTP client. Ensure to disable FTP client timeout for connection in the **Edit > Settings** of FTP client options:



By default, FileZilla FTP client closes the session itself after 20 seconds and you are not able to reproduce the problem seen by the user with other applications.

After about 2-3 minutes of inactivity, try refresh directory listing:



Then, in the FTP client you see the error message like on the 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
```

Next, check that some packets were captured on both inside and outside interfaces, stop EPC and 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
```

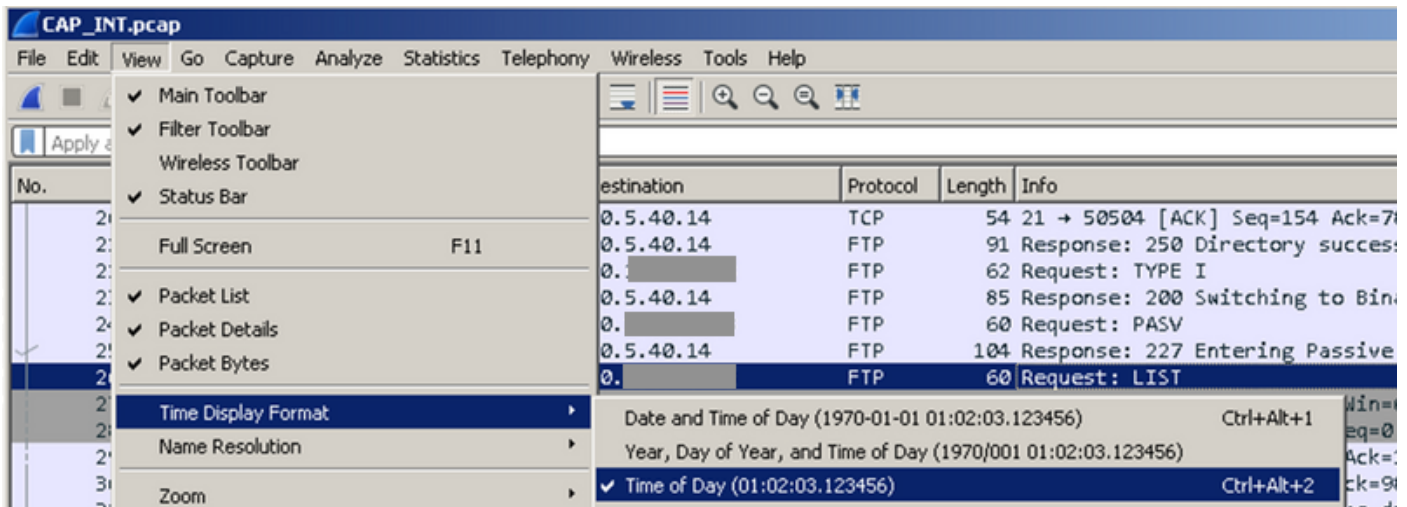
```
Branch#monitor capture CAP_INT stop_export
Exported Successfully
```

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

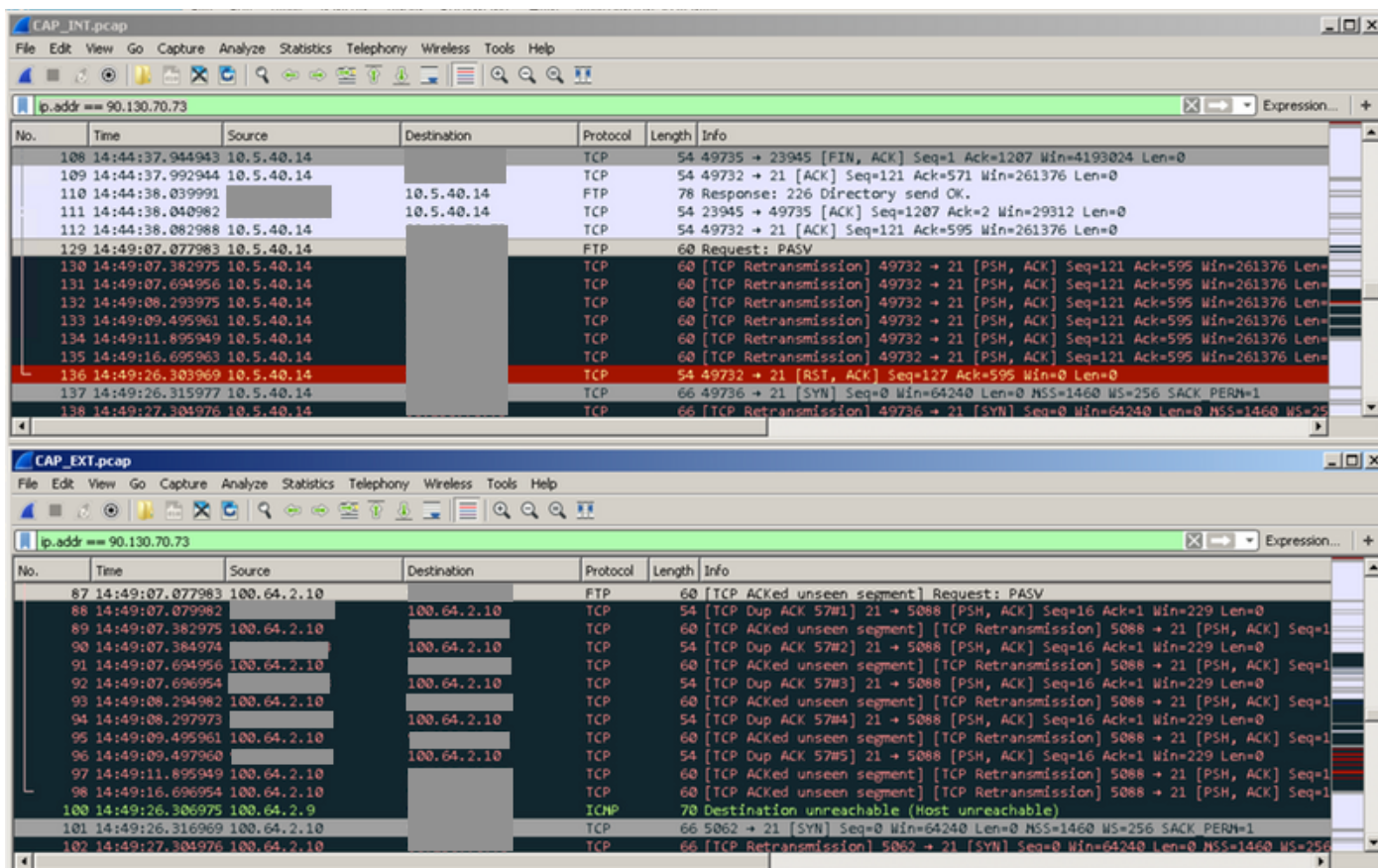
And upload captures to your PC so you can analyze it with Wireshark:

```
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 both files in the separate Wireshark windows and set **Time Display Format** to make it easier to correlate packets on the outside interface with packets on the inside interface by timestamps:



Then align windows and notice the difference between packet captures made on the external and on the internal interfaces (look for **FTP PASV** request in your captures):



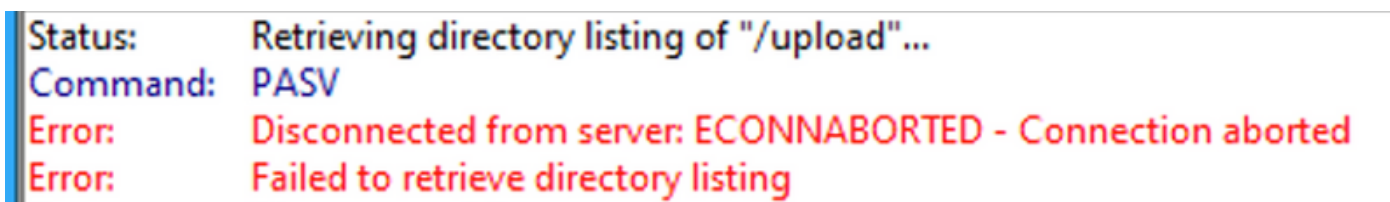
You can see that request is sent to the outside and a bunch of retransmissions happened. At this point, it's not clear why packets from the external hosts (e.g. packets number 88,90,92 and so on) are not reaching to the internal host, but EPC gave us valuable information and confirmed that some packets are being dropped by cEdge router.

## Troubleshoot with Help of Cisco IOS-XE Packet Tracer Utility

To investigate further, you must use packet-capture and filter data based on FTP server public address:

```
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
```

Then, connect to the FTP in a second time and wait for longer than 2-3 minutes before you click the refresh button or downloading something again. In the log, you can notice the same error message, as shown in the image:



Now, from packet-trace you can see one of the packets was dropped:





before:

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

When the problem is reproduced one more time (e.g. when you try to change directory) and the connection is lost as per logs of FTP client (FTP client attempted to reconnect), let's see packet-trace statistics once again:

```
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
```

Now you can notice another drop code, "DROP 55 (ForUs)", despite that you disabled implicit ACL with **allow-service all** configuration, packets are still being dropped. Take a closer look and try to understand the difference between dropped packets and forwarded packets:

```
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)
288  Gi3          Gi3                      DROP  55  (ForUs)
289  Gi3          Gi3                      DROP  55  (ForUs)
```







```
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  
Output : internal0/0/svc\_eng:0  
Lapsed time : 26240 ns







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

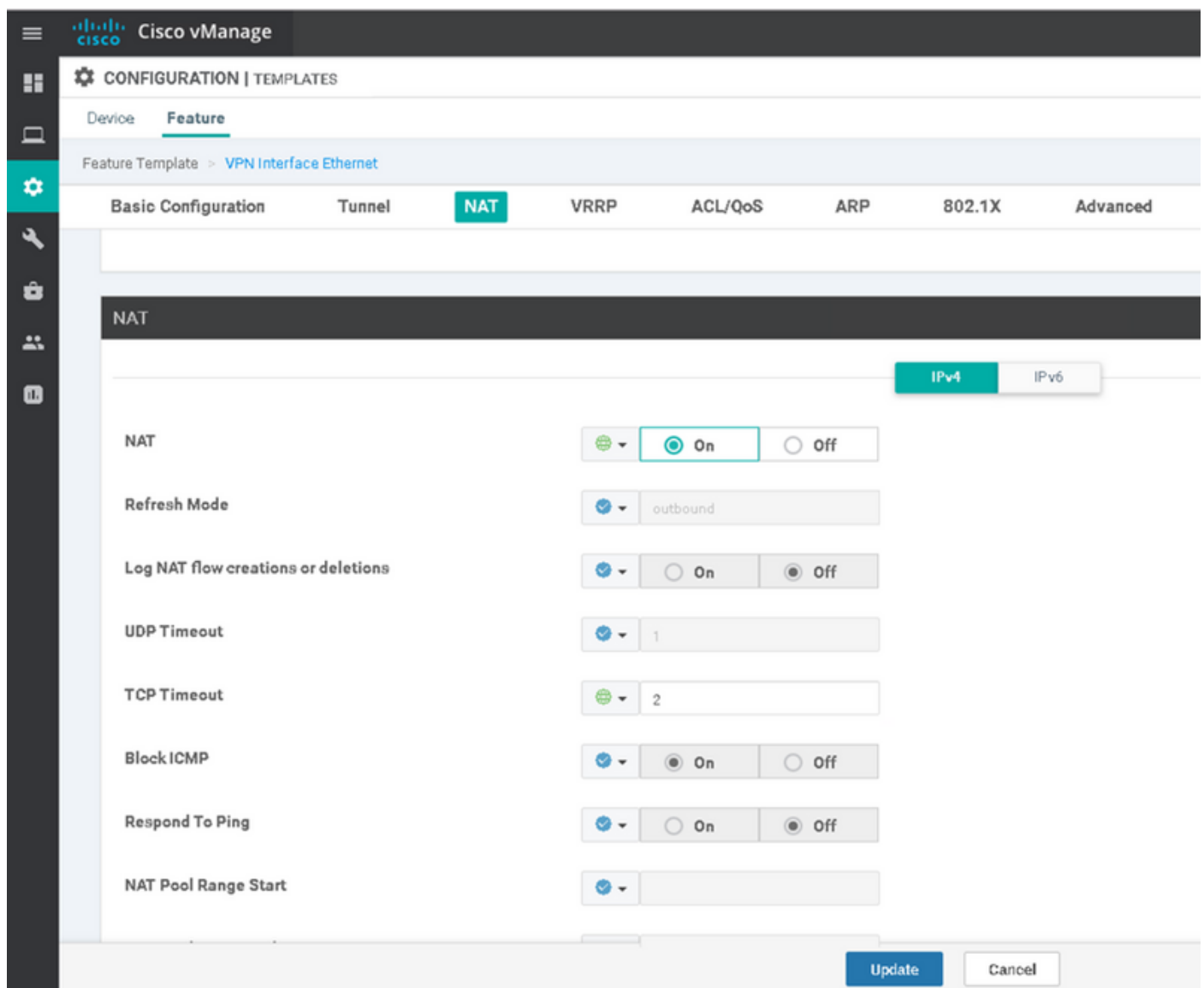
And pay attention to the timeout. Does not it look suspiciously low? After about 2-3 minutes of FTP client inactivity, check again and you can notice there are no translations in the NAT table:

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

Voila! So that the root cause for the problem: sessions are expiring too fast and despite that from the perspective of FTP client session still exists, cEdge router does not know anything about that TCP session already and drops return traffic. If you check configuration, you find that NAT session timeout is configured as 120 seconds, probably by mistake:

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

And this timer must be fixed in the corresponding device template on vManage:



Change it to 60 min for example and then the problem is resolved.