

# Beispiel für IOS-XE SD-WAN-Probleme

## Fehlerbehebung mithilfe von EPC und Packet-Trace

### Inhalt

[Einführung](#)

[Problem](#)

[Lösung](#)

[Fehlerbehebung mit EPC](#)

[Fehlerbehebung mithilfe des Cisco IOS-XE Packet Tracer-Dienstprogramms](#)

### Einführung

In diesem Dokument wird das Beispiel für zeitweilige Verbindungsfehler beschrieben. Bei der Fehlerbehebung auf einem Router, auf dem Cisco IOS-XE SD-WAN mit den Dienstprogrammen Embedded Packet Capture (EPC) und Packet Trace ausgeführt wird, wird ein Ansatz zur Fehlerbehebung unterstützt.

### Problem

Ihre Benutzer einer Zweigstelle berichten, dass einige Internetanwendungen, die Direct Internet Access (DIA) verwenden, z. B. SAP®, SSH, einige FTP-Clients und eine Reihe anderer Anwendungen, zeitgesteuert sind, wenn ein Benutzer länger als etwa 2-3 Minuten im Leerlauf ist. Wenn sie in den Anwendungen, die eine Netzwerkkommunikation erfordern, aktive Aktionen ausführen, funktionieren die Anwendungen gut, und es werden keine Probleme beobachtet.

Wenn Sie beispielsweise **show version** ausführen und die Sitzung mehr als 2 Minuten ohne Aktivität belassen, drücken Sie anschließend eine beliebige Taste auf der Tastatur, wie in der Ausgabe hier gezeigt:

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

IDLE Timeout auf der Endleitung des Routers wurde überprüft und festgestellt, dass **exec-Timeout** auf 10 Minuten festgelegt ist und nicht für das beschriebene Verhalten verantwortlich ist (beachten Sie, dass auch andere Anwendungen betroffen sind):

```
router#show user
```

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

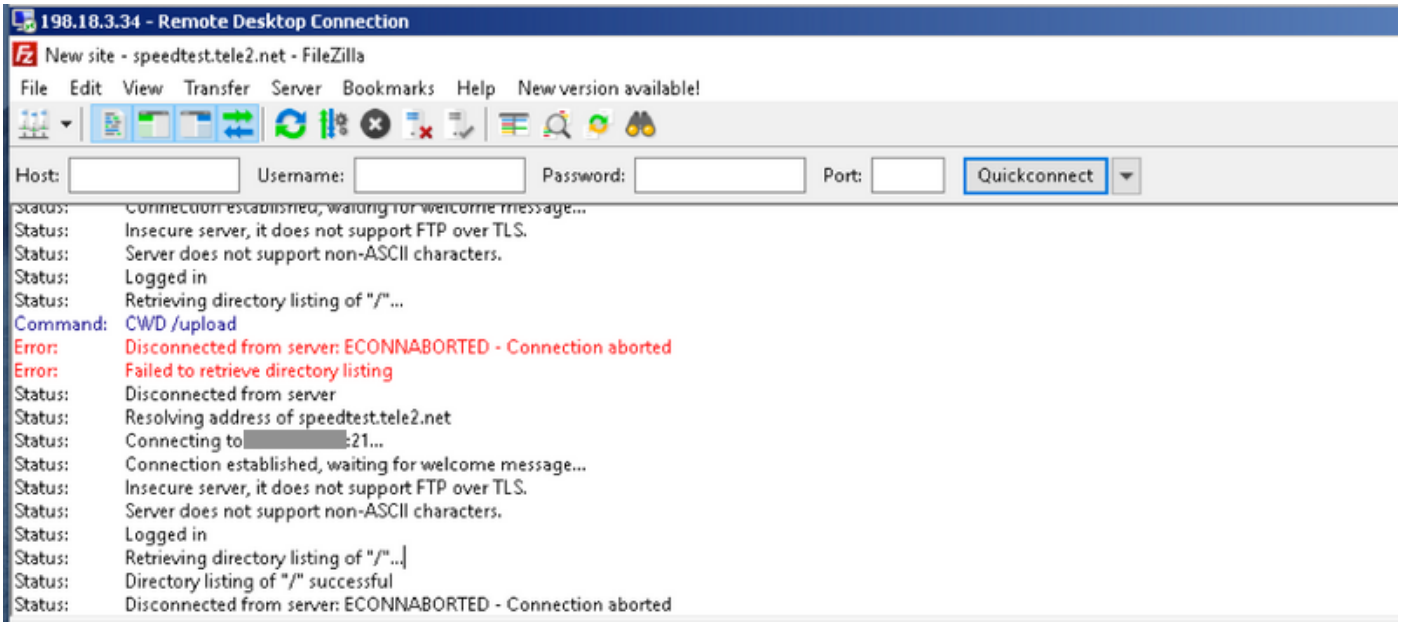
Interface	User	Mode	Idle	Peer Address
unknown	(ONEP)	csrmgmt_infr	00:00:14	

```
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
```

Eine andere Möglichkeit, das Problem live zu erleben, besteht darin, eine Verbindung zu einem öffentlichen FTP herzustellen. Wenn Sie dann versuchen, die Verzeichnisliste zu aktualisieren, den Ordner zu ändern oder etwas nach 2-3 Minuten Inaktivität herunterzuladen, wird die Meldung angezeigt (rot):



## Lösung

Solche Probleme sind manchmal komplex zu beheben, aber eine große Hilfe kann [IOS-XE Datapath Packet Trace-Funktion](#) und Embedded Packet Capture (EPC) IOS-XE-Dienstprogramme bereitstellen. Hier ein Beispiel für die Verwendung und den Ansatz zur Fehlerbehebung.

## Fehlerbehebung mit EPC

Konfigurieren und starten Sie Embedded Packet Capture (EPC) auf dem Router. Da dieser Standort DIA verwendet, müssen Sie den Datenverkehr an externen und internen Schnittstellen separat erfassen. Hier ist 198.51.100.7 die IP-Adresse des FTP-Servers und 10.5.40.14 die IP-Adresse des Clients:

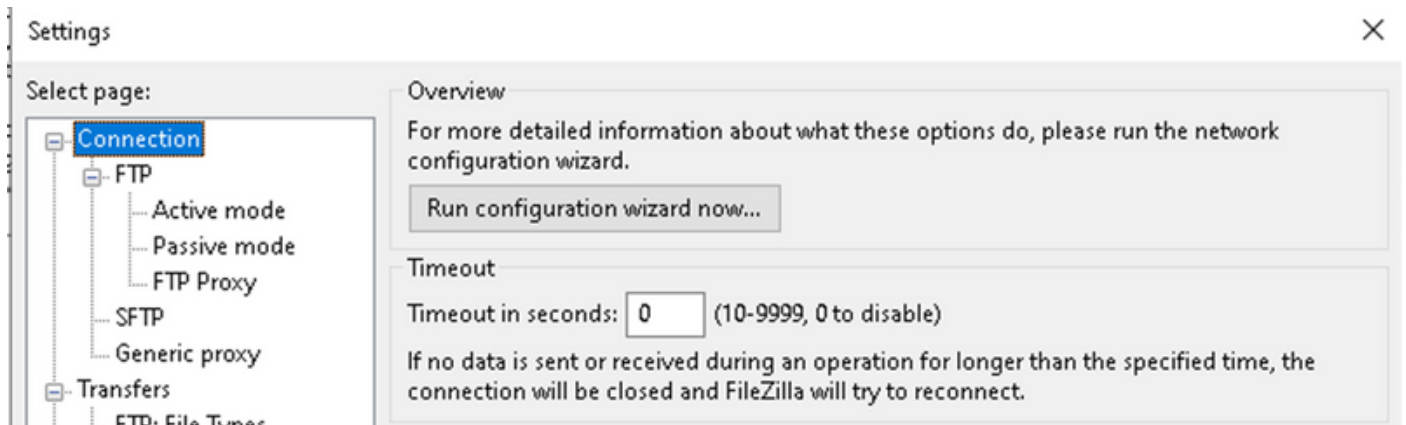
```
Branch#config-transaction
```

```
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
```

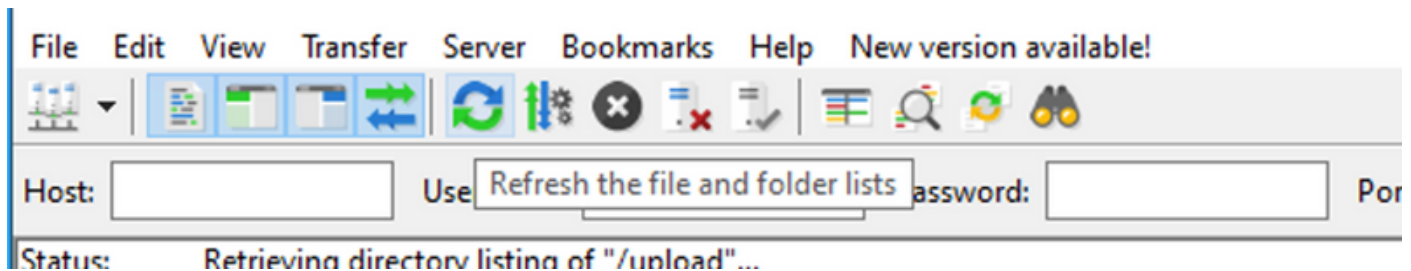
```
Branch#monitor capture CAP_INT start
Started capture point : CAP_INT
```

Anschließend vom Host des Benutzers mit Verbindung zum FTP-Server über den FTP-Client FileZilla. Stellen Sie sicher, dass das FTP-Client-Timeout für die Verbindung unter **Bearbeiten > Einstellungen** der FTP-Clientoptionen deaktiviert wird:



Standardmäßig schließt der FileZilla FTP-Client die Sitzung selbst nach 20 Sekunden und Sie können das vom Benutzer erkannte Problem nicht mit anderen Anwendungen reproduzieren.

Nach etwa 2-3 Minuten Inaktivität versuchen Sie, das Verzeichnis zu aktualisieren:



Anschließend wird im FTP-Client die Fehlermeldung wie im Screenshot angezeigt:

```
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
```

Überprüfen Sie anschließend, ob einige Pakete sowohl auf internen als auch auf externen Schnittstellen erfasst wurden, beenden Sie EPC und führen Sie Exportpuffer durch:

```
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
```

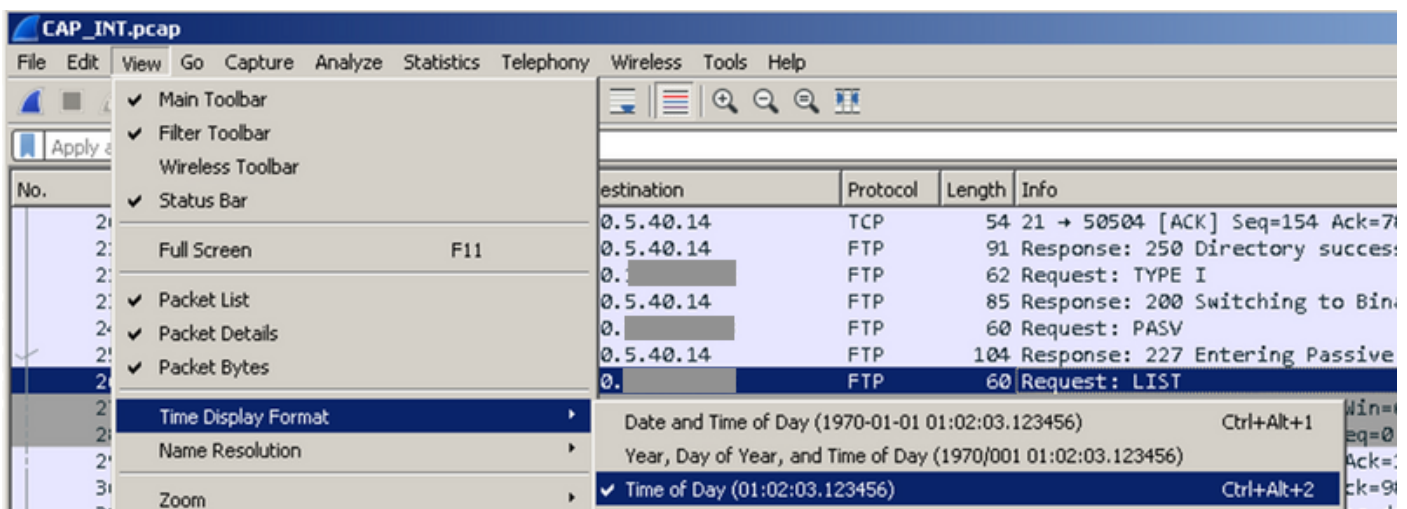
```
Branch#monitor capture CAP_INT stop_export
Exported Successfully
```

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

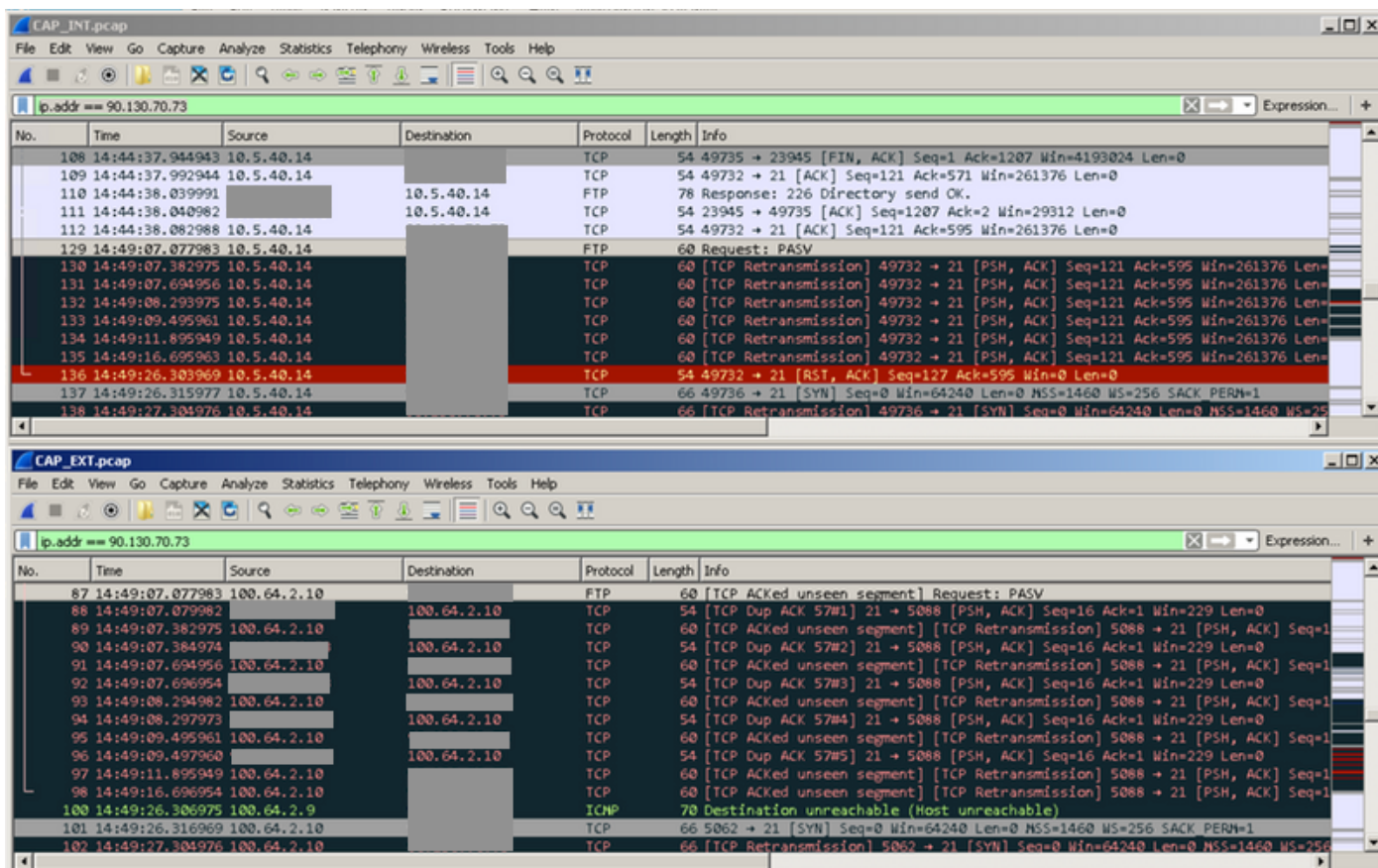
Laden Sie außerdem Aufzeichnungen auf Ihren PC hoch, damit Sie diese mit Wireshark analysieren können:

```
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)
```

Öffnen Sie beide Dateien in den separaten Wireshark-Fenstern, und legen Sie das **Time Display Format** fest, um die Korrelation von Paketen auf der externen Schnittstelle mit Paketen auf der internen Schnittstelle mithilfe von Zeitstempeln zu vereinfachen:



Ordnen Sie dann die Fenster an, und achten Sie auf die Unterschiede zwischen der Paketerfassung an der externen und der internen Schnittstelle (suchen Sie in Ihren Erfassungen nach **FTP PASV-Anfrage**):



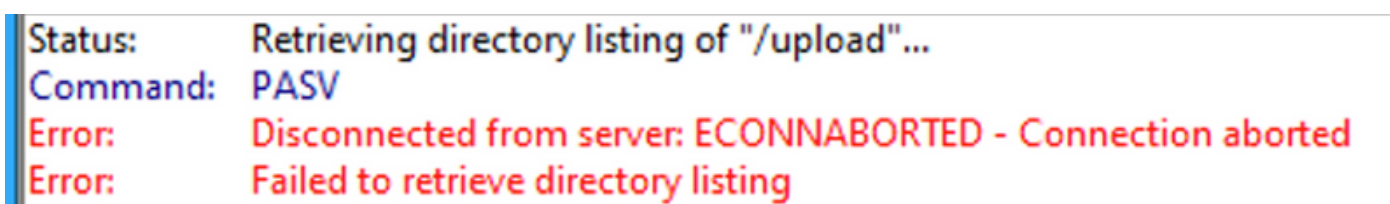
Wie Sie sehen, wird die Anfrage an die Außenstellen gesendet, und es sind mehrere Neuübertragungen aufgetreten. Zu diesem Zeitpunkt ist nicht klar, warum Pakete von den externen Hosts (z. B. Pakete mit den Nummern 88, 90, 92 usw.) nicht auf den internen Host gelangen. EPC gab uns jedoch wertvolle Informationen und bestätigte, dass einige Pakete vom cEdge-Router verworfen werden.

## Fehlerbehebung mithilfe des Cisco IOS-XE Packet Tracer-Dienstprogramms

Um weiter zu untersuchen, müssen Sie die Paketerfassung verwenden und Daten auf Grundlage der öffentlichen Adresse des FTP-Servers filtern:

```
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
```

Stellen Sie anschließend eine zweite Verbindung mit dem FTP her, und warten Sie länger als 2-3 Minuten, bevor Sie auf die Aktualisierungsschaltfläche klicken oder erneut etwas herunterladen. Im Protokoll wird die gleiche Fehlermeldung angezeigt, wie im Bild gezeigt:



Nun, von der Paketverfolgung aus sehen Sie, dass eines der Pakete verworfen wurde:





Wiederholen wir den Test nach dem Festlegen der Konfiguration, aber stellen Sie sicher, dass die Paketverfolgung gestoppt und vor dem Abschluss der Konfiguration wieder gestartet wird:

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

Wenn das Problem erneut auftritt (z. B. wenn Sie versuchen, das Verzeichnis zu ändern) und die Verbindung je Protokoll des FTP-Clients (FTP-Client versucht, erneut eine Verbindung herzustellen) verloren geht, sehen wir uns die Paketverfolgungsstatistiken noch einmal an:

```
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
```

Jetzt können Sie einen weiteren Drop-Code bemerken: "DROP 55 (ForUs)", obwohl Sie die implizite ACL mit **allow-service all**-Konfiguration deaktiviert haben, werden Pakete immer noch verworfen. Werfen Sie einen genaueren Blick auf den Unterschied zwischen verworfenen Paketen und weitergeleiteten Paketen:

```
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







```
create: 11/07/19 13:02:05, use: 11/07/19 13:02:06, timeout: 00:00:57
Map-Id(In): 1
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

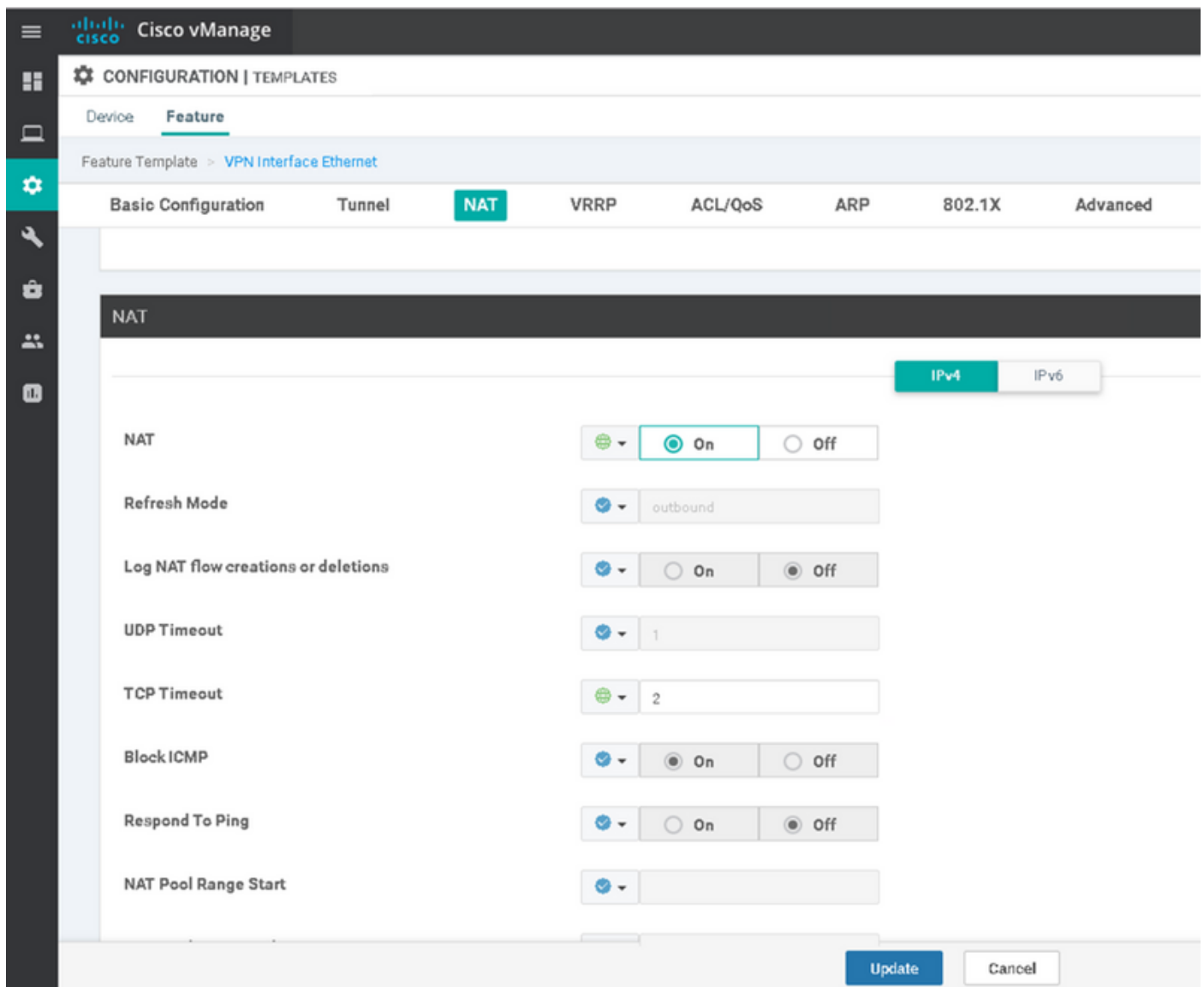
Und achten Sie auf die Zeitüberschreitung. Sieht es nicht verdächtig niedrig aus? Wenn der FTP-Client etwa 2-3 Minuten inaktiv ist, überprüfen Sie es noch einmal, und Sie sehen, dass die NAT-Tabelle keine Übersetzungen enthält:

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

Voila! Damit die Ursache des Problems: Sitzungen laufen zu schnell ab, und obwohl aus Sicht der FTP-Client-Sitzung noch nichts über diese TCP-Sitzung bekannt ist und Rückverkehr verworfen wird. Wenn Sie die Konfiguration überprüfen, wird das Timeout für die NAT-Sitzung möglicherweise versehentlich auf 120 Sekunden festgelegt:

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

Dieser Timer muss in der entsprechenden Gerätevorlage in vManage festgelegt werden:



Ändern Sie sie beispielsweise auf 60 Minuten, und das Problem wird behoben.