EPC 및 패킷 추적을 통해 트러블슈팅하는 IOS-XE SD-WAN 문제의 예

목차

소개

이 문서에서는 EPC(Embedded Packet Capture) 및 Packet Trace 유틸리티를 사용하여 Cisco IOS-XE SD-WAN을 실행하는 라우터에서 간헐적인 연결 실패 문제 해결 접근 방식의 예를 설명합니다.

문제

지사 사이트의 사용자는 SAP®, SSH, 일부 FTP 클라이언트 및 기타 애플리케이션 세트와 같은 DIA(Direct Internet Access)를 사용하는 일부 인터넷 애플리케이션이 유휴 시간이 약 2-3분 이상 경과하면 시간 초과된다고 보고합니다.네트워크 통신이 필요한 애플리케이션 내에서 활성 작업을 수행하면 애플리케이션이 제대로 작동하며 문제가 관찰되지 않습니다.

예를 들어, **show version을** 실행하고 아무 작업 없이 2분 이상 세션을 유휴 상태로 둔 경우 다음 출력에서와 같이 키보드의 아무 키나 누릅니다.

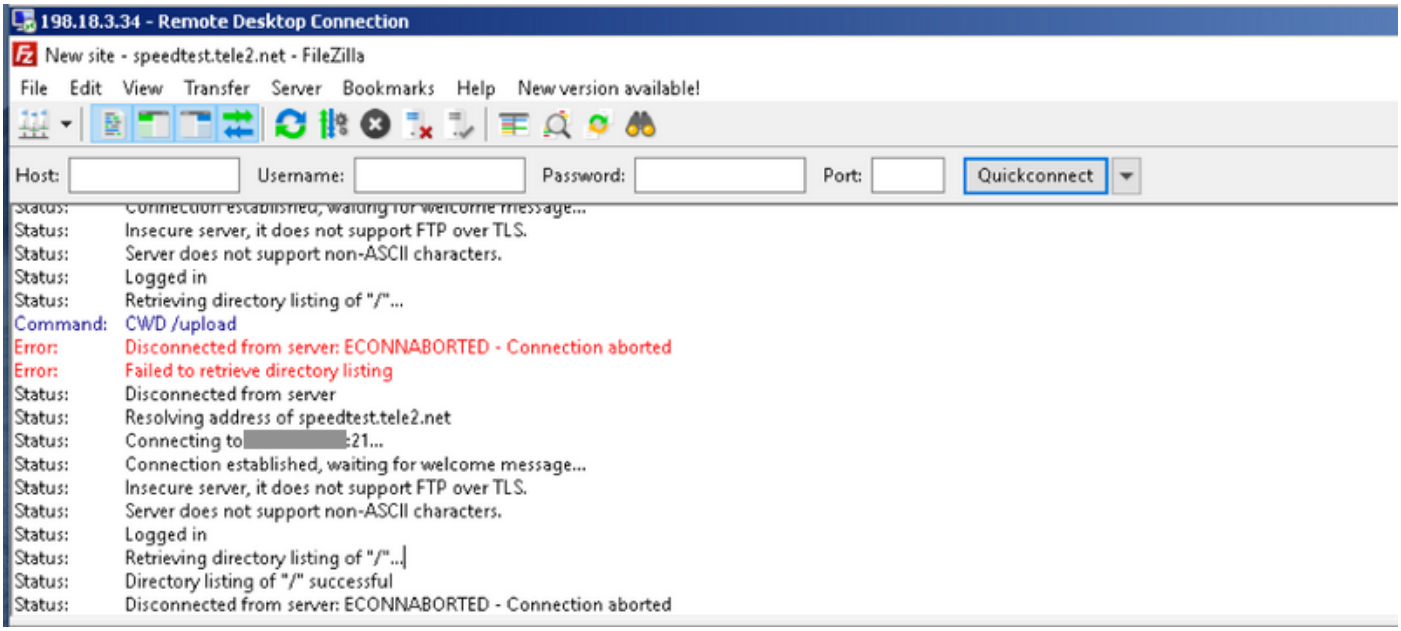
```
router#Connection reset by 100.64.2.9 port 22
```

라우터의 터미널 회선에서 IDLE 시간 초과가 확인되었으며 exec-**timeout**이 10분으로 설정되었으며 설명된 동작에 대해 책임지지 않음을 발견했습니다(다른 애플리케이션에도 영향을 미침).

```
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
```

이 문제를 실시간으로 경험하는 또 다른 방법은 일부 공용 FTP에 연결하는 것입니다.그런 다음 2-3분 동안 활동이 없으면 디렉터리 목록을 새로 고치거나 폴더를 변경하거나 다운로드하려고 하면

메시지가 빨간색으로 표시됩니다.



솔루션

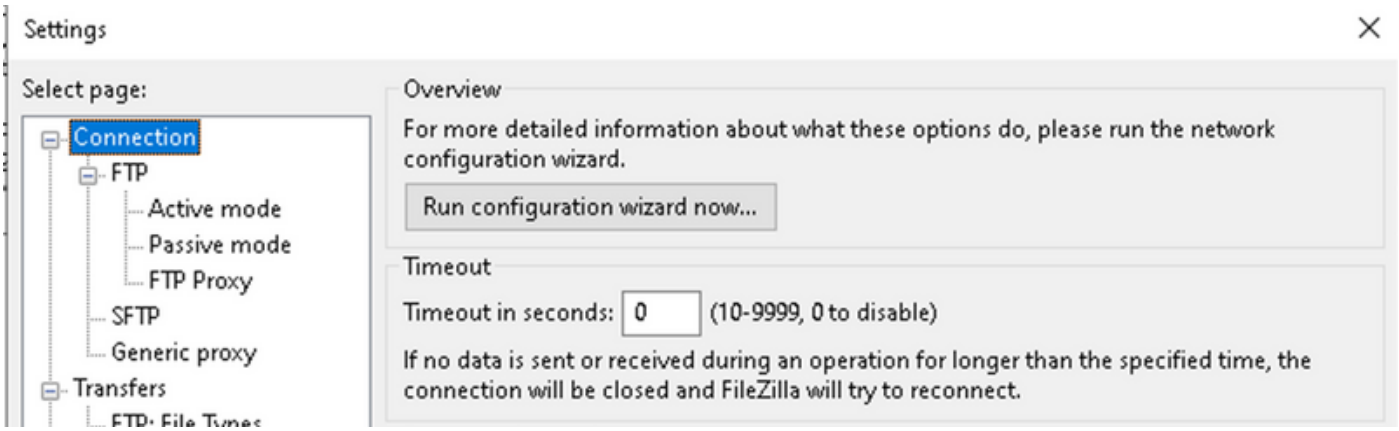
이러한 문제는 가끔 문제를 해결하는 데 복잡하지만, IOS-XE Datapath Packet Trace 기능 및 EPC(Embedded Packet Capture) IOS-XE 유틸리티를 제공하는 데 큰 도움이 될 수 있습니다.다음은 트러블슈팅을 위한 사용 및 접근 방식의 예입니다.

EPC로 문제 해결

라우터에서 EPC(Embedded Packet Capture)를 구성하고 시작합니다.이 사이트는 DIA를 사용하므로 외부 및 내부 인터페이스에서 트래픽을 별도로 캡처해야 합니다.198.51.100.7은 FTP 서버의 IP 주소이며 10.5.40.14은 클라이언트의 IP 주소입니다.

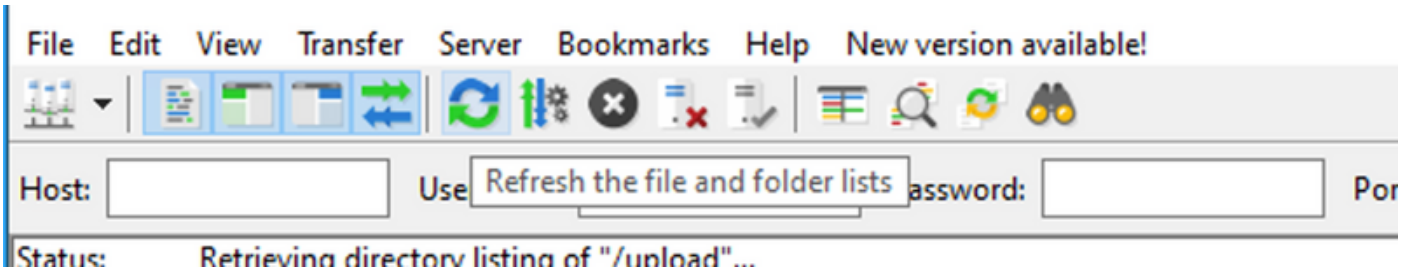
```
Branch#config-transaction

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
```

다음으로, FileZilla FTP 클라이언트를 사용하여 FTP 서버에 연결하는 사용자의 호스트에서Edit(편집) > Settings of FTP client options(FTP 클라이언트 옵션의 설정)에서 연결에 대한 FTP 클라이언트 시간 제한을 비활성화해야 합니다.

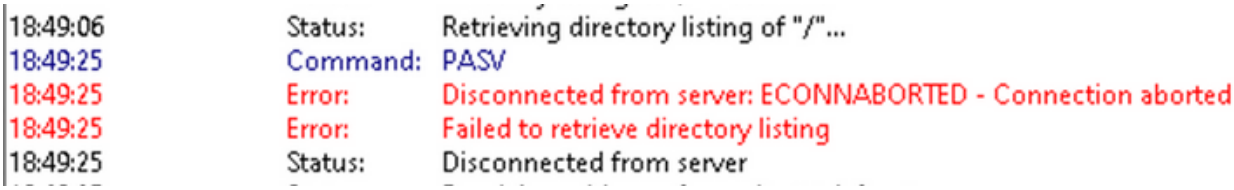


기본적으로 FileZilla FTP 클라이언트는 20초 후 세션 자체를 닫으며 사용자가 다른 응용 프로그램을 사용하여 확인한 문제를 재현할 수 없습니다.

비활성 상태가 약 2-3분 후에 디렉터리 목록을 새로 고쳐 보십시오.



그런 다음 FTP 클라이언트에서 스크린샷과 같은 오류 메시지가 표시됩니다.



다음으로, 내부 및 외부 인터페이스 모두에서 일부 패킷이 캡처되었는지 확인하고 EPC를 중지하고 버퍼를 내보냅니다.

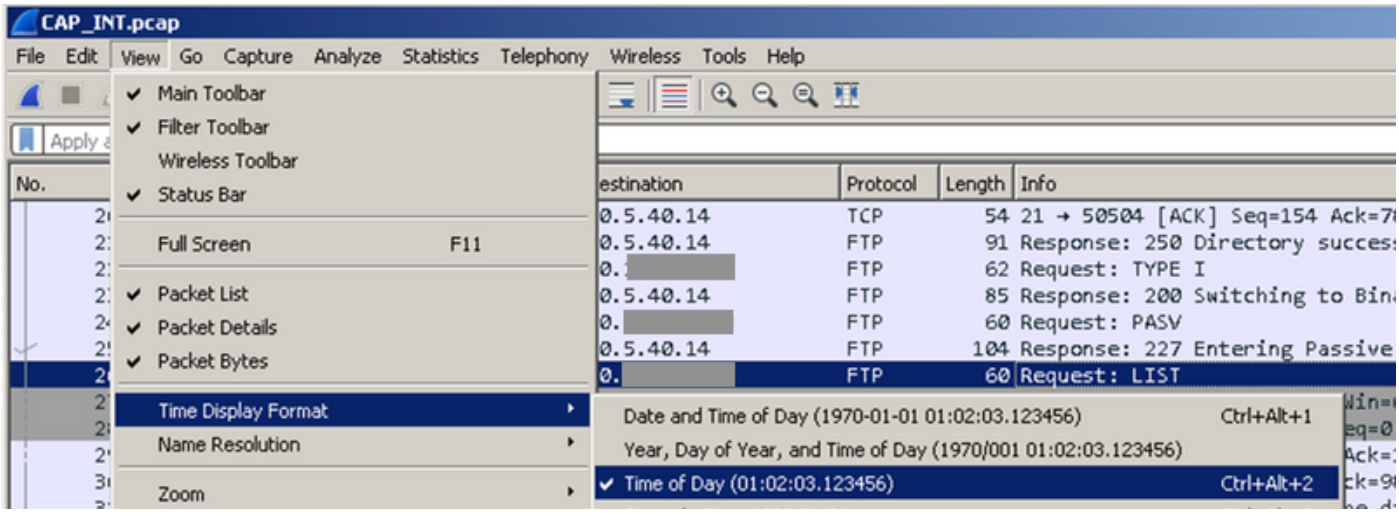
```
Branch#show monitor capture CAP_EXT buffer
 buffer size (KB) : 10240
 buffer used (KB) : 128
 packets in buf   : 37
 packets dropped  : 0
 packets per sec  : 24

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
```

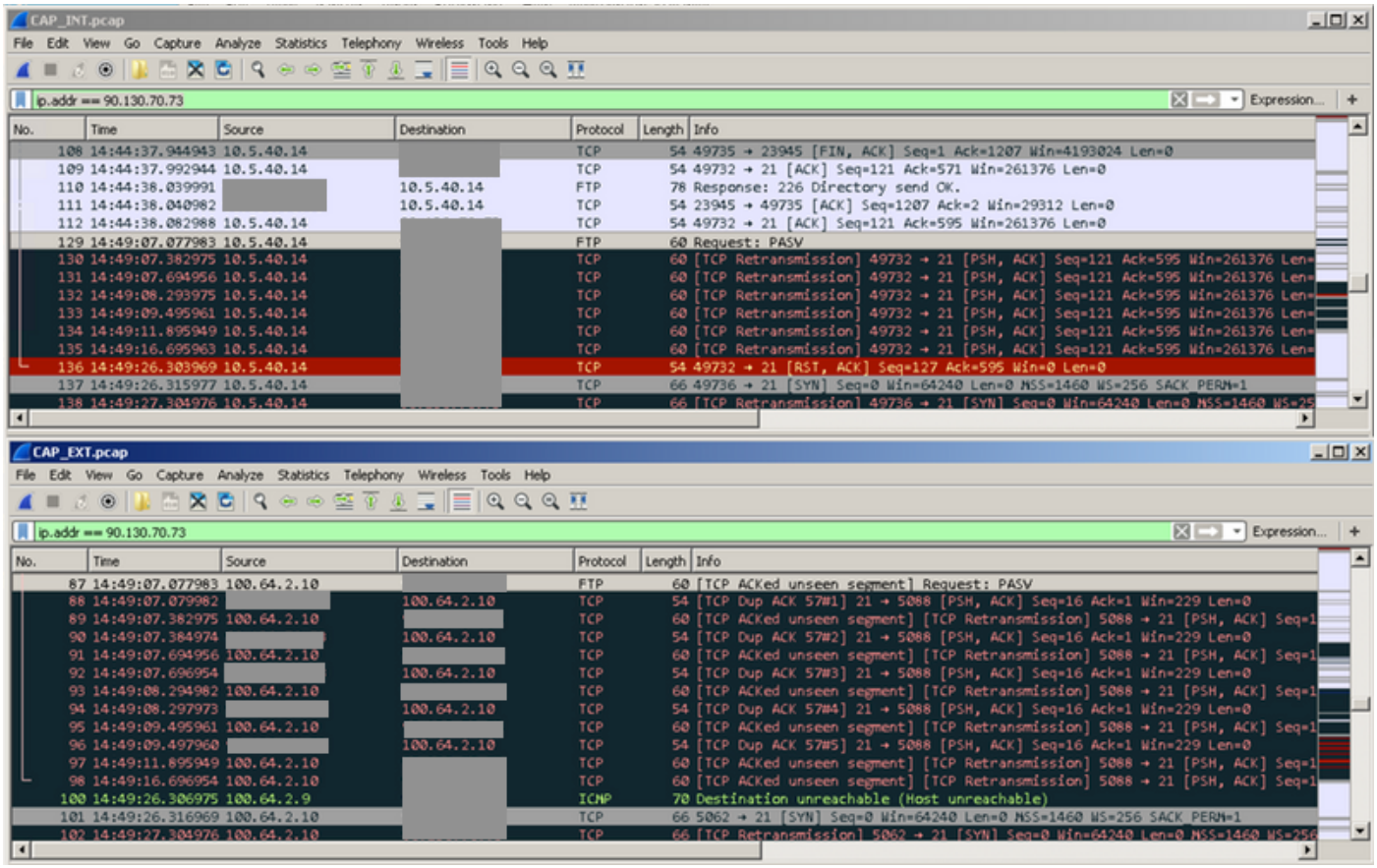
Wireshark를 사용하여 분석할 수 있도록 캡처를 PC에 업로드합니다.

```
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)
```

두 파일을 별도의 Wireshark 창에서 열고 **Time Display Format을** 설정하여 외부 인터페이스의 패킷과 타임스탬프를 기준으로 내부 인터페이스의 패킷의 상관관계를 보다 쉽게 파악할 수 있습니다.



그런 다음 윈도우를 정렬하고 외부 및 내부 인터페이스에서 수행된 패킷 캡처 간의 차이를 확인합니다(캡처에서 **FTP PASV 요청을** 찾음).



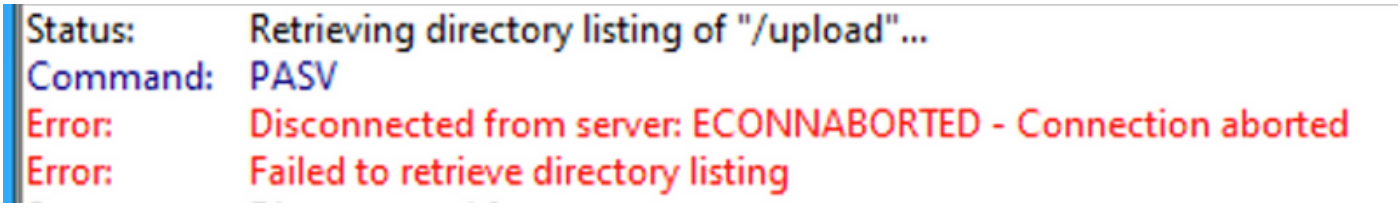
요청이 외부로 전송되고 다수의 재전송이 발생했음을 알 수 있습니다.이때 외부 호스트의 패킷(예: 패킷 번호 88,90,92 등)이 내부 호스트에 도달하지 않는 이유는 명확하지 않지만 EPC는 유용한 정보를 제공하고 일부 패킷이 cEdge 라우터에 의해 삭제되고 있음을 확인했습니다.

Cisco IOS-XE Packet Tracer Utility의 도움으로 문제 해결

더 자세히 조사하려면 FTP 서버 공용 주소를 기반으로 패킷 캡처를 사용하고 데이터를 필터링해야 합니다.

```
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
```

그런 다음 FTP에 다시 연결한 다음 2-3분 이상 기다렸다가 새로 고침 버튼을 클릭하거나 다른 항목을 다시 다운로드하십시오.로그에서 이미지에 표시된 것과 동일한 오류 메시지를 확인할 수 있습니다.



이제 packet-trace에서 패킷 중 하나가 삭제된 것을 확인할 수 있습니다.

```
134   Gi3                    internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
```

```
135   Tu6000001               Gi7                       FWD
136   Gi7                     internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
137   Tu6000001               Gi3                       FWD
138   Gi3                     internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
139   Tu6000001               Gi7                       FWD
140   Gi7                     internal0/0/svc_eng:0     PUNT   64  (Service Engine packet)
141   Tu6000001               Gi3                       FWD
142   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
143   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
144   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
145   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
146   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
147   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
148   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
149   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
150   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
151   Gi3                     Gi3                       DROP   479 (SdwanImplicitAclDrop)
```

또한 특정 패킷의 세부사항을 확인할 수 있습니다.

```
Branch#show platform packet-trace packet 151
Packet: 151         CBUG ID: 151
Summary
  Input     : GigabitEthernet3
  Output    : GigabitEthernet3
  State     : DROP 479 (SdwanImplicitAclDrop)
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Timestamp
    Start   : 179731083510 ns (11/07/2019 13:08:27.567722 UTC)
    Stop    : 179731145820 ns (11/07/2019 13:08:27.567785 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 198.51.100.7
    Destination : 100.64.2.10
    Protocol    : 6 (TCP)
      SrcPort   : 21
      DstPort   : 5801
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x817e8838
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 8280 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x817e885c
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 4160 ns
  Feature: SDWAN Implicit ACL
<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Action : DISALLOW
    Reason : SDWAN_SERV_TCP
    Defer Action to Ingress ACL : No
  Feature: STILE_LEGACY_DROP_EXT
    Entry       : Input - 0x81835c68
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 12900 ns
  Feature: INGRESS_MMA_LOOKUP_DROP_EXT
    Entry       : Input - 0x8182be6c
    Input       : GigabitEthernet3
```

```
    Output      : <unknown>
    Lapsed time : 14940 ns
  Feature: INPUT_DROP_FNF_AOR_EXT
    Entry       : Input - 0x81819480
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 22040 ns
  Feature: INPUT_FNF_DROP_EXT
    Entry       : Input - 0x818185bc
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 17580 ns
  Feature: INPUT_DROP_FNF_AOR_RELEASE_EXT
    Entry       : Input - 0x81818e08
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 4680 ns
  Feature: INPUT_DROP_EXT
    Entry       : Input - 0x817ed780
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 5540 ns
  Feature: IPV4_SDWAN_IMPLICIT_ACL     <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Entry       : Input - 0x8183c774
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 449760 ns
Packet Copy In
  00505608 6e500050 56add375 08004500 00363481 40002d06 122c5a82 46496440
  020a0015 16a9f873 89d3efaa e3785019 00e523cb 00003432 31205469 6d656f75
Packet Copy Out
  00505608 6e500050 56add375 08004500 00363481 40002c06 132c5a82 46496440
  020a0015 16a9f873 89d3efaa e3785019 00e523cb 00003432 31205469 6d656f75
```

이러한 패킷은 대상 FTP 서버에서 재전송됩니다.이미 패킷 캡처에서 유사한 재전송 세트가 발견되었습니다.

packet-trace 출력에 따라 어떤 이유로 SD-WAN 암시적 ACL(**터널 인터페이스** 컨피그레이션에서 허용되는 서비스 목록)이 패킷을 삭제하는 것 같습니다.이 과정을 **<<<<<<<<** 표시 로 강조 표시된 행에서 완료할 수 있습니다.테스트하려면 SD-WAN 암시적 ACL을 제외하고 해당 외부 인터페이스의 컨피그레이션에서 모든 서비스를 허용합니다.

```
Branch#config-transaction

admin connected from 127.0.0.1 using console on Branch
Branch(config)# sdwan
Branch(config-sdwan)# interface GigabitEthernet3
Branch(config-interface-GigabitEthernet3)# tunnel-interface
Branch(config-tunnel-interface)# allow-service all
Branch(config-tunnel-interface)# commit
Commit complete.
```

> **팁**:또 다른 옵션은 명시적 IPv4 access-list를 구성하고 GigabitEthernet3 인터페이스의 원격 호스트에서 **access-group** 명령을 사용하여 패킷을 허용하는 것이며, 이는 SDWAN 암시적 ACL을 재정의합니다.

컨피그레이션이 커밋되면 테스트를 반복하되 패킷 추적을 중지하고 다음 이전에 다시 시작해야 합니다.

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

문제가 한 번 더 재현된 경우(예: 디렉터리를 변경하려고 할 때) FTP 클라이언트(FTP 클라이언트가 다시 연결하려고 시도함)의 로그에 따라 연결이 손실된 경우 패킷 추적 통계를 다시 한 번 확인합니다.

```
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
```

이제 또 다른 삭제 코드인 "DROP 55 (ForUs)"를 발견할 수 있습니다. 암시적 ACL을 **allow-service all 컨피그레이션으로 비활성화했지만** 패킷은 여전히 삭제됩니다.자세히 살펴보고 삭제된 패킷과 전달된 패킷의 차이를 파악하십시오.

```
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)
290   Gi3                    Gi3                       DROP   55  (ForUs)
291   Gi3                    Gi3                       DROP   55  (ForUs)
292   Gi3                    Gi3                       DROP   55  (ForUs)
```

```
293   Gi3                     Gi3                     DROP   55  (ForUs)
```

이전 출력에서 Gi7은 서비스 측 인터페이스이고 Gi3은 전송 측 인터페이스입니다.예를 들어, 패킷 279와 패킷 283의 차이를 비교합니다(중요한 차이점은 **<<<<<<**)로 표시됨).

```
Branch#show platform packet-trace packet 279
Packet: 279         CBUG ID: 794
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/svc_eng:0
  State     : PUNT 64  (Service Engine packet)
  Timestamp
    Start   : 142279273535701 ns (11/07/2019 12:46:47.57026 UTC)
    Stop    : 142279273732912 ns (11/07/2019 12:46:47.57223 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 198.51.100.7
    Destination : 100.64.2.10
    Protocol    : 6 (TCP)
      SrcPort   : 28143
      DstPort   : 5668
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x817e8838
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 5880 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x817e885c
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 7320 ns
  Feature: SDWAN Implicit ACL   <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Action : ALLOW
    Reason : SDWAN_NAT_DIA    <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Defer Action to Ingress ACL : No
  Feature: IPV4_SDWAN_IMPLICIT_ACL
    Entry       : Input - 0x8183c774
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 112800 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x817e8860
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 78480 ns
  Feature: DEBUG_COND_APPLICATION_IN
    Entry       : Input - 0x817e8848
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 1460 ns
  Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
    Entry       : Input - 0x817e884c
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 120 ns
  Feature: IPV4_INPUT_VFR     <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Entry       : Input - 0x817e89b0
    Input       : GigabitEthernet3
```

```
  Output      : <unknown>
  Lapsed time : 3880 ns
Feature: NAT                <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Direction   : OUT to IN
  Action      : Translate Destination
  Steps       :
  Match id    : 1
  Old Address : 100.64.2.10 05668
  New Address : 10.5.40.14  49588
Feature: IPV4_NAT_INPUT_FIA <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
  Entry       : Input - 0x8182c8a8
  Input       : GigabitEthernet3
  Output      : <unknown>
  Lapsed time : 117600 ns
Feature: IPV4_INPUT_DST_LOOKUP_ISSUE_EXT
  Entry       : Input - 0x817e8858
  Input       : GigabitEthernet3
  Output      : <unknown>
  Lapsed time : 19620 ns
Feature: RELOOKUP_NOTIFY_EXT
  Entry       : Input - 0x817eed90
  Input       : GigabitEthernet3
  Output      : <unknown>
  Lapsed time : 14040 ns
Feature: IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT
  Entry       : Input - 0x817e8870
  Input       : GigabitEthernet3
  Output      : <unknown>
  Lapsed time : 4620 ns
Feature: IPV4_INPUT_FOR_US_EXT
  Entry       : Input - 0x817e89a4
  Input       : GigabitEthernet3
  Output      : <unknown>
  Lapsed time : 280 ns
Feature: IPV4_VFR_REFRAG_EXT
  Entry       : Input - 0x817e89c0
  Input       : GigabitEthernet3
  Output      : <unknown>
  Lapsed time : 2720 ns
Feature: CFT
  API                   : cft_handle_pkt
  packet capabilities   : 0x0000018c
  input vrf_idx         : 0
  calling feature       : STILE
  direction             : Input
  triplet.vrf_idx       : 3
  triplet.network_start : 0x01003f8e
  triplet.triplet_flags : 0x00000000
  triplet.counter       : 32
  cft_bucket_number     : 942419
  cft_l3_payload_size   : 20
  cft_pkt_ind_flags     : 0x00000100
  cft_pkt_ind_valid     : 0x00009bff
  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: 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
Feature: INTERNAL_TRANSMIT_PKT_EXT
  Entry       : Output - 0x817e88e4
  Input       : Tunnel6000001
  Output      : internal0/0/svc_eng:0
```

```
    Lapsed time : 156540 ns



Branch#show platform packet-trace packet 283
Packet: 283         CBUG ID: 798
Summary
  Input     : GigabitEthernet3
  Output    : GigabitEthernet3
  State     : DROP 55  (ForUs)
  Timestamp
    Start   : 142367023778233 ns (11/07/2019 12:48:14.807268 UTC)
    Stop    : 142367023853492 ns (11/07/2019 12:48:14.807343 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 198.51.100.7
    Destination : 100.64.2.10
    Protocol    : 6 (TCP)
      SrcPort   : 21
      DstPort   : 5635
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x817e8838
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 12340 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x817e885c
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 7140 ns
  Feature: SDWAN Implicit ACL    <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Action : ALLOW
    Reason : SDWAN_SERV_ALL      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Defer Action to Ingress ACL : No
  Feature: IPV4_SDWAN_IMPLICIT_ACL
    Entry       : Input - 0x8183c774
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 139700 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x817e8860
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 97840 ns
  Feature: DEBUG_COND_APPLICATION_IN
    Entry       : Input - 0x817e8848
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 2260 ns
  Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
    Entry       : Input - 0x817e884c
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 140 ns
  Feature: IPV4_INPUT_VFR      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Entry       : Input - 0x817e89b0
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 5860 ns
  Feature: OCE_TRACE(Input)    <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Input       : GigabitEthernet3
```

```
    Output      : <unknown>
    Type        : OCE_ADJ_RECEIVE
  Feature: IPV4_NAT_INPUT_FIA  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
    Entry       : Input - 0x8182c8a8
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 166780 ns
  Feature: STILE_LEGACY_DROP_EXT
    Entry       : Input - 0x81835c68
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 1920 ns
  Feature: INGRESS_MMA_LOOKUP_DROP_EXT
    Entry       : Input - 0x8182be6c
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 8340 ns
  Feature: INPUT_DROP_FNF_AOR_EXT
    Entry       : Input - 0x81819480
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 10920 ns
  Feature: INPUT_FNF_DROP_EXT
    Entry       : Input - 0x818185bc
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 6460 ns
  Feature: INPUT_DROP_FNF_AOR_RELEASE_EXT
    Entry       : Input - 0x81818e08
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 2240 ns
  Feature: INPUT_DROP_EXT
    Entry       : Input - 0x817ed780
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 1200 ns
  Feature: IPV4_INPUT_LOOKUP_PROCESS
    Entry       : Input - 0x817e8864
    Input       : GigabitEthernet3
    Output      : <unknown>
    Lapsed time : 176340 ns
```

보시다시피 주요 차이점은 일반적으로 코드 SDWAN_NAT_DIA와 삭제된 패킷 SDWAN_SERV_ALL을 사용하여 외부 패킷이 허용된다는 것입니다.뿐만 아니라 IPV4_INPUT_VFR과 IPV4_NAT_INPUT_FIA 함수 간에 허용되는 패킷에 대해 다른 IOS-XE 기능이 NAT 대 OCE_TRACE와 관련됩니다.이 모든 차이는 이미 문제가 NAT와 관련이 있다는 것을 알 수 있으므로 FTP 세션이 설정된 후 NAT 변환을 확인하겠습니다.

```
Branch#show ip nat translations tcp verbose | b 198.51.100.7
tcp  100.64.2.10:5801      10.5.40.14:49648      198.51.100.7:21       198.51.100.7:21
  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
```

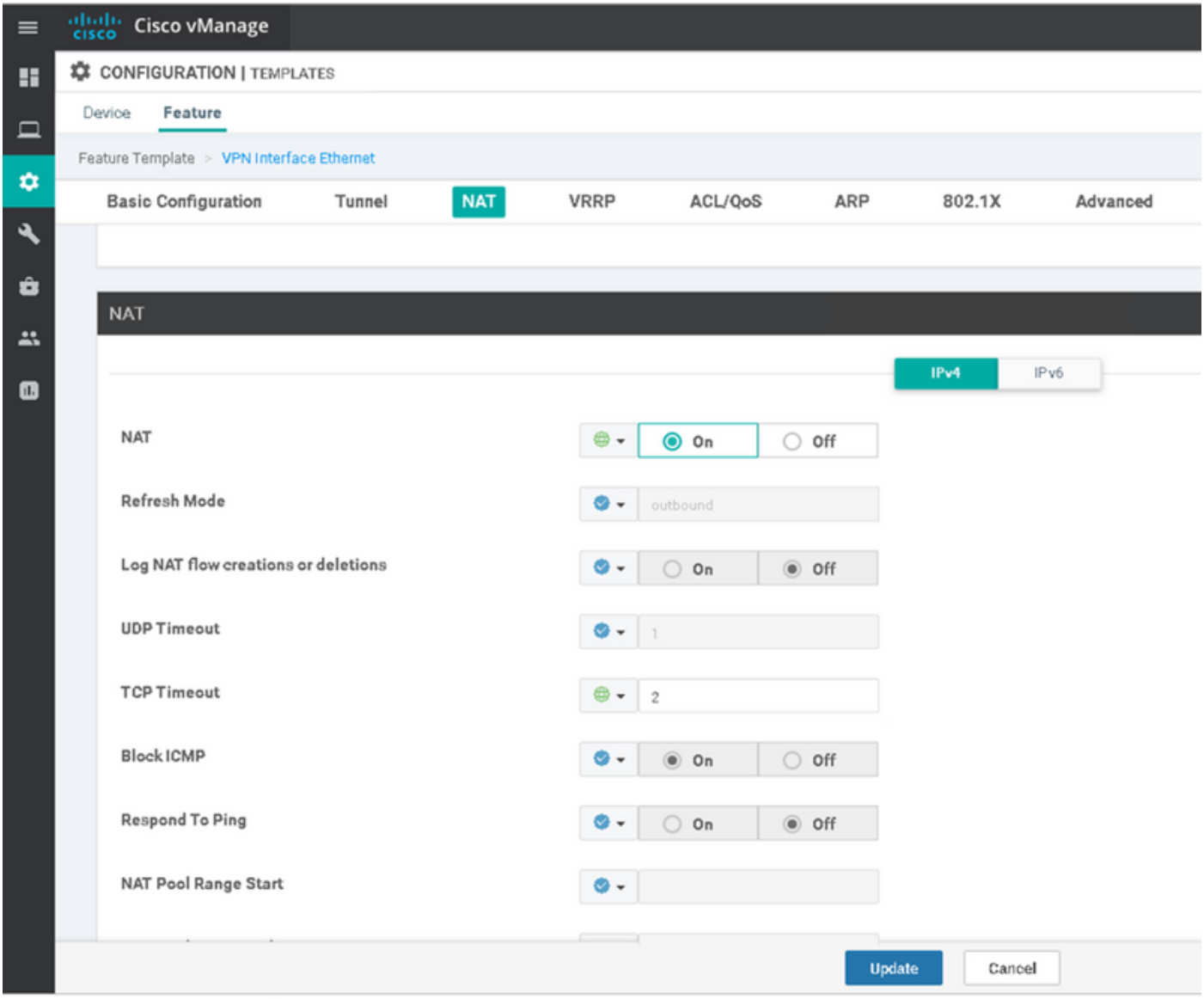
시간 초과에 주목하십시오.수상해 보이지 않나요?FTP 클라이언트 비활성 상태가 약 2-3분 후에 다시 확인하면 NAT 테이블에 변환이 없음을 알 수 있습니다.

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

보이라!따라서 문제의 근본 원인은 다음과 같습니다.세션이 너무 빠르게 만료되고 FTP 클라이언트 세션의 관점에서 세션이 여전히 존재하지만 cEdge 라우터는 이미 해당 TCP 세션에 대해 아무것도 알지 못하고 반환 트래픽을 삭제합니다.컨피그레이션을 확인하면 NAT 세션 시간 초과가 120초로 구성되며, 이는 실수로 인한 것일 수 있습니다.

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

그리고 이 타이머는 vManage의 해당 디바이스 템플릿에서 수정되어야 합니다.



예를 들어 60분으로 변경하면 문제가 해결됩니다.