EPCおよびパケットトレースを使用したIOS-XE SD-WAN問題のトラブルシューティングの例

内容

概要

このドキュメントでは、組み込みパケットキャプチャ(EPC)およびパケットトレースユーティリティを使用してCisco IOS-XE SD-WANを実行するルータでの断続的な接続障害のトラブルシューティングアプローチの例について説明します。

問題

ブランチサイトのユーザは、SAP®、SSH、一部のFTPクライアント、その他のアプリケーションのセットなど、ダイレクトインターネットアクセス(DIA)を使用する一部のインターネットアプリケーションが、ユーザのアイドル時間が約2 ~ 3分を超えるとタイムアウトすると報告しています。ネットワーク通信を必要とするアプリケーション内でアクティブなアクションを実行すると、アプリケーションは正常に動作し、問題は発生しません。

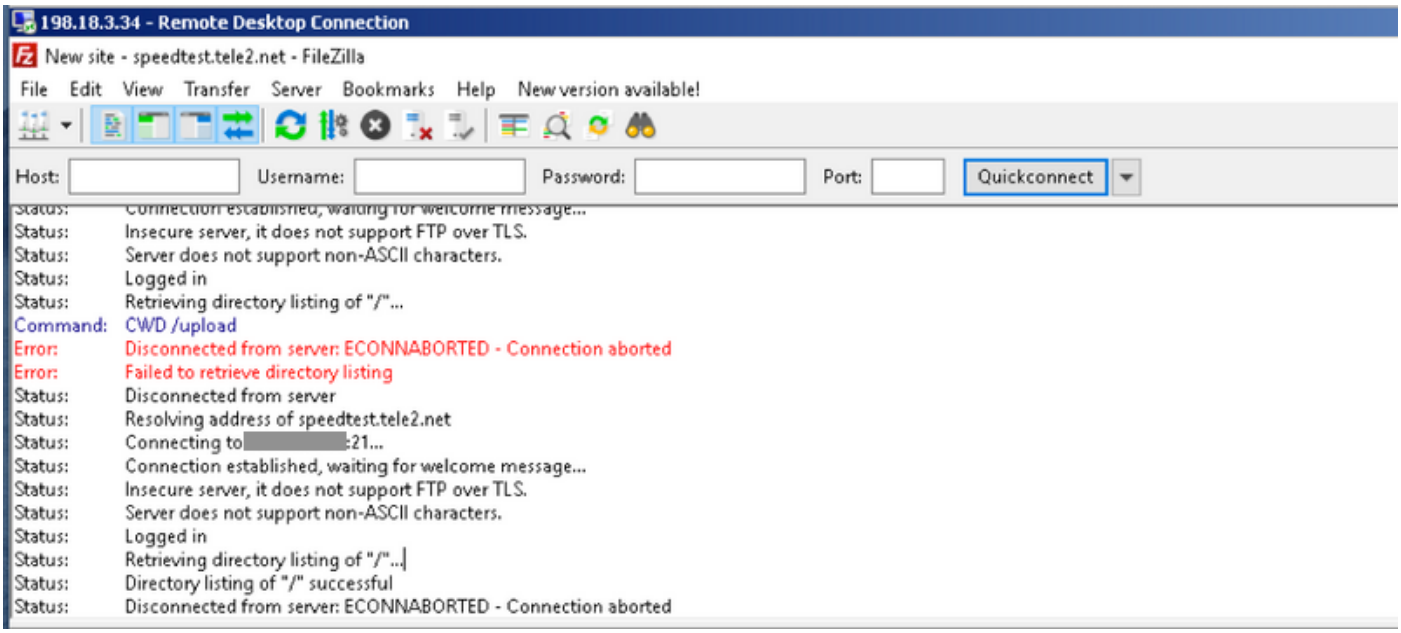
たとえば、**show version**を実行し、セッションをアクティビティなしで2分以上アイドル状態のままにし、その後、次の出力のようにキーボードの任意のキーを押します。

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

ルータの端末回線のIDLEタイムアウトがチェックされ、**exec-timeoutが10分に設定さ**れ、説明されている動作は行われていません（他のアプリケーションも影響を受けます）。

```
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
```

問題をライブで体験するもう1つの方法は、パブリックFTPに接続することです。次に、ディレクトリのリストを更新したり、フォルダを変更したり、何かをダウンロードしたりしようとすると、メッセージが表示されます（赤色）。



解決方法

このような問題はトラブルシューティングに複雑な場合もありますが、IOS-XE Datapath Packet Trace機能と組み込みパケットキャプチャ(EPC) IOS-XEユーティリティを利用する上で役立ちます。ここでは、トラブルシューティングの使用例とアプローチを示します。

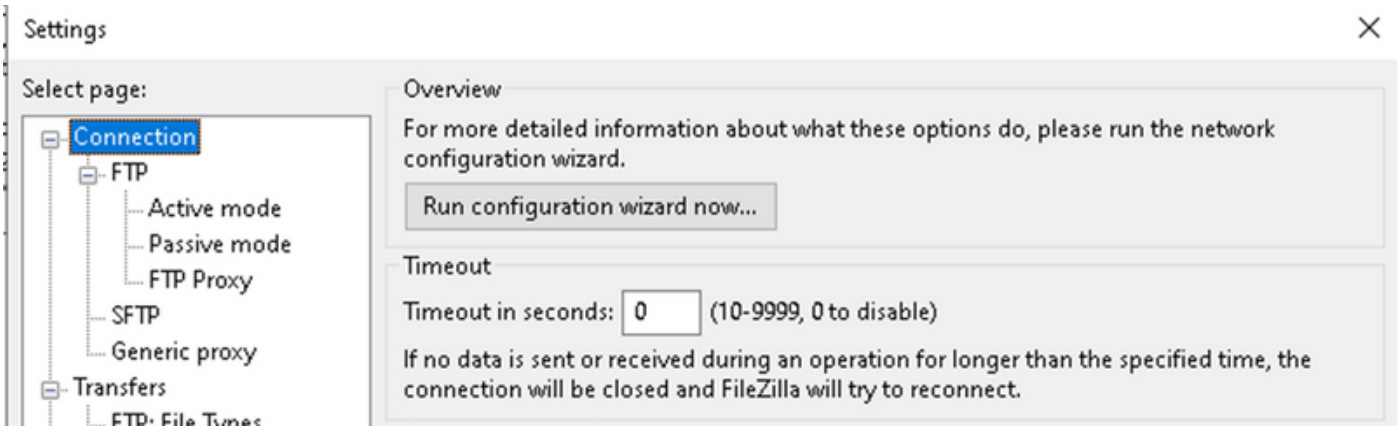
EPCでのトラブルシューティング

ルータでEmbedded Packet Capture(EPC)を設定して開始します。このサイトはDIAを使用しているため、外部インターフェイスと内部インターフェイスのトラフィックを別々にキャプチャする必要があります。ここで、198.51.100.7はFTPサーバのIPアドレス、10.5.40.14はクライアントのIPアドレスです。

```
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
```

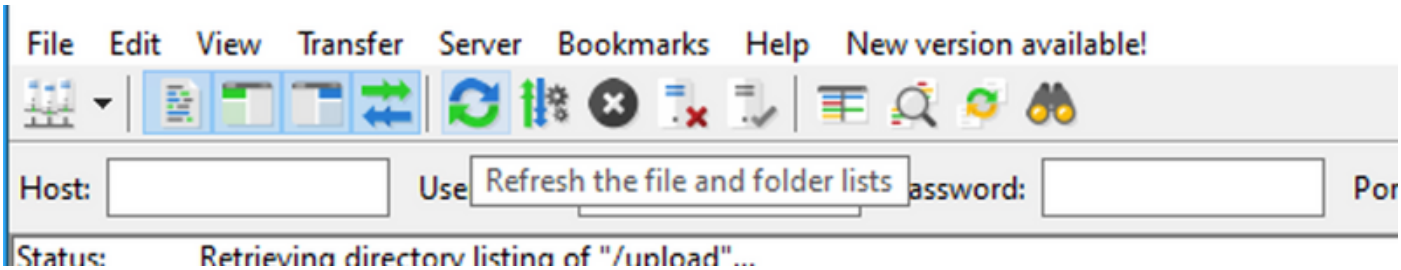
```
Branch#monitor capture CAP_INT start
Started capture point : CAP_INT
```

次に、ユーザのホストからFileZilla FTPクライアントを使用してFTPサーバに接続します。FTPクライアントオプションの[**Edit**] > [Settings]で、接続に対するFTPクライアントの**タイムアウトを無効にする**ことを確認します。

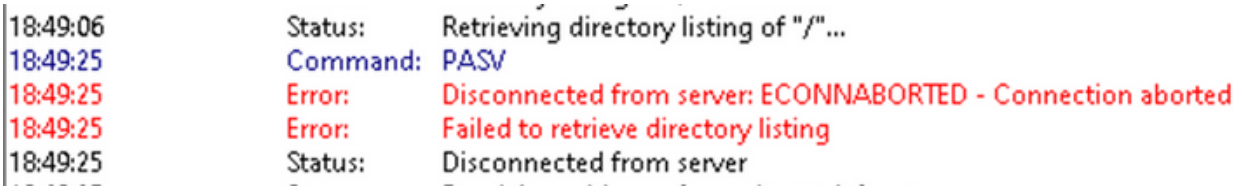


デフォルトでは、FileZilla FTPクライアントは20秒後にセッション自体を閉じ、ユーザが他のアプリケーションで見た問題を再現することはできません。

非アクティブ状態が2 ~ 3分程度したら、ディレクトリのリストを更新してみてください。



次に、FTPクライアントで次のようなエラーメッセージがスクリーンショットに表示されます。



次に、一部のパケットが内部インターフェイスと外部インターフェイスの両方でキャプチャされたことを確認し、EPCを停止してバッファをエクスポートします。

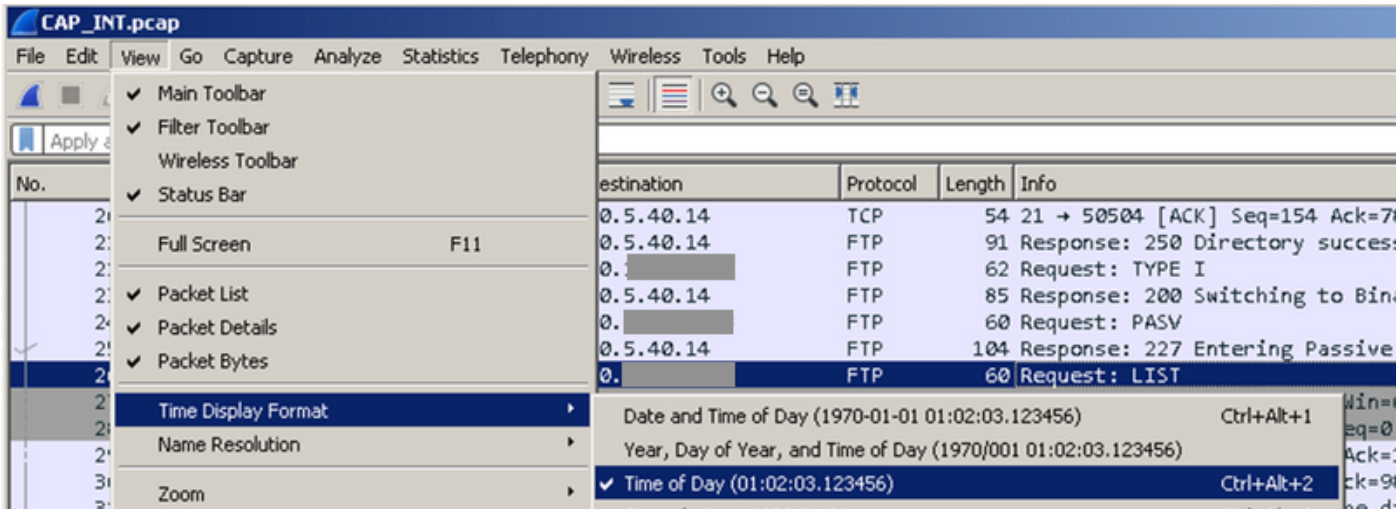
```
Branch#show monitor capture CAP_EXT buffer
 buffer size (KB) : 10240
 buffer used (KB) : 128
 packets in buf   : 37
 packets dropped  : 0
 packets per sec  : 24

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
```

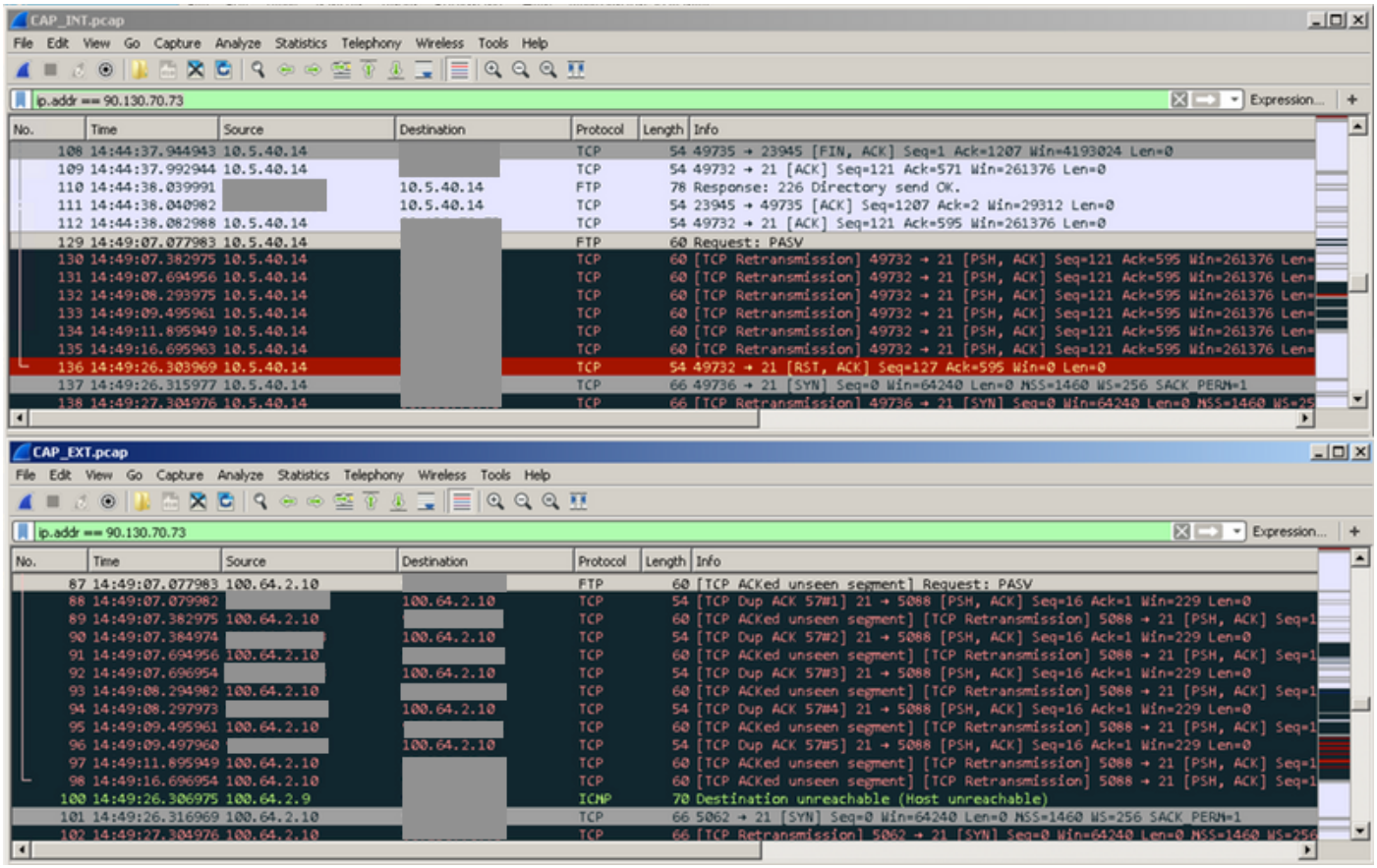
キャプチャをPCにアップロードして、Wiresharkで分析できるようにします。

```
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)
```

両方のファイルを別々のWiresharkウィンドウで開き、[Time Display Format]を設定して、外部インターフェイスのパケットと内部インターフェイスのパケットをタイムスタンプによって簡単に関連付けます。



次に、ウィンドウを整列し、外部インターフェイスと内部インターフェイスで行われたパケットキャプチャの違いに注目します(キャプチャでFTP PASV要求を探します)。



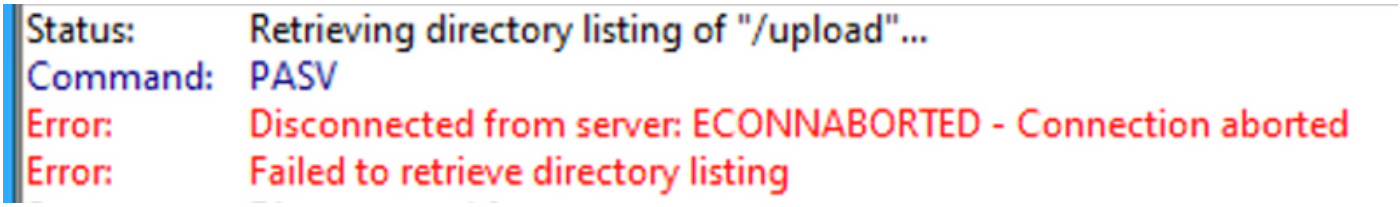
要求が外部に送信され、再送信が多数発生していることがわかります。この時点では、外部ホストからのパケット（パケット番号88,90,92など）が内部ホストに到達しない理由は不明ですが、EPCから貴重な情報が得られ、一部のパケットがcEdgeルータによって廃棄されていることが確認されました。

Cisco IOS-XE Packet Tracerユーティリティを使用したトラブルシューティング

詳細を調査するには、FTPサーバのパブリックアドレスに基づいて、パケットキャプチャとフィルタデータを使用する必要があります。

```
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
```

次に、2回目にFTPに接続し、2 ~ 3分以上待ってから、更新ボタンをクリックするか、何かを再度ダウンロードします。ログには、図に示すように、同じエラーメッセージが表示されます。



次に、パケットトレースから、パケットの1つがドロップされたことを確認できます。

```
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)
```

特定のパケットの詳細を確認することもできます。

```
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
```

これらのパケットは、対象のFTPサーバから再送信されます。同様の一連の再送信がパケットキャプチャですでに見られています。

パケットトレースの出力から判断すると、何らかの理由でSD-WAN暗黙的ACL(実際には**tunnel-interface設定で許可されるサービスのリスト)がパケットをドロップしているようです**。これは、<<<<<マークで強調表示された行から結論付けることができます。テストするには、SD-WAN暗黙的ACLを除外し、対応する外部インターフェイスの設定ですべてのサービスを許可します。

```
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.
```

> **ヒント**：別のオプションとして、明示的なIPv4アクセスリストを設定し、**access-groupコマンドを使用して**GigabitEthernet3インターフェイス上のリモートホストからのパケットを許可し、SDWAN暗黙的ACLを上書きします。

設定がコミットされたら、テストを繰り返しますが、パケットトレースを停止して前に最初からやり直します。

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

問題がもう一度再現され（ディレクトリを変更しようとした場合など）、FTPクライアント（FTPクライアントが再接続を試行したログ）のログによって接続が失われた場合は、パケットトレースの統計情報をもう一度確認します。

```
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
```

次に、別のドロップコード「DROP 55 (ForUs)」が表示されます。**allow-service all設定で暗黙的なACLを無効にしているが、パケットは引き続き廃棄されています。**詳細を確認し、ドロップされたパケットと転送されたパケットの違いを理解してみます。

```
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)
```

上記の出力では、Gi7はサービス側インターフェイス、Gi3はトランスポート側インターフェイスです。たとえば、パケット279とパケット283の違いを比較します (重要な違いは<<<<<) でマークされます。

```
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
```

ご覧のように、主な違いは、通常は外部からのパケットがコードSDWAN_NAT_DIAで許可される点と、ドロップされたパケットSDWAN_SERV_ALLで許可される点です。これに加え、IPV4_INPUT_VFRとIPV4_NAT_INPUT_FIAの間で許可されたパケットに対しては、異なるIOS-XE機能がNATとOCE TRACE すべての違いによって、問題がNATに関連していると考えられる場合があります。したがって、FTPセッションが確立された後でNAT変換を確認してみましょう。

```
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
```

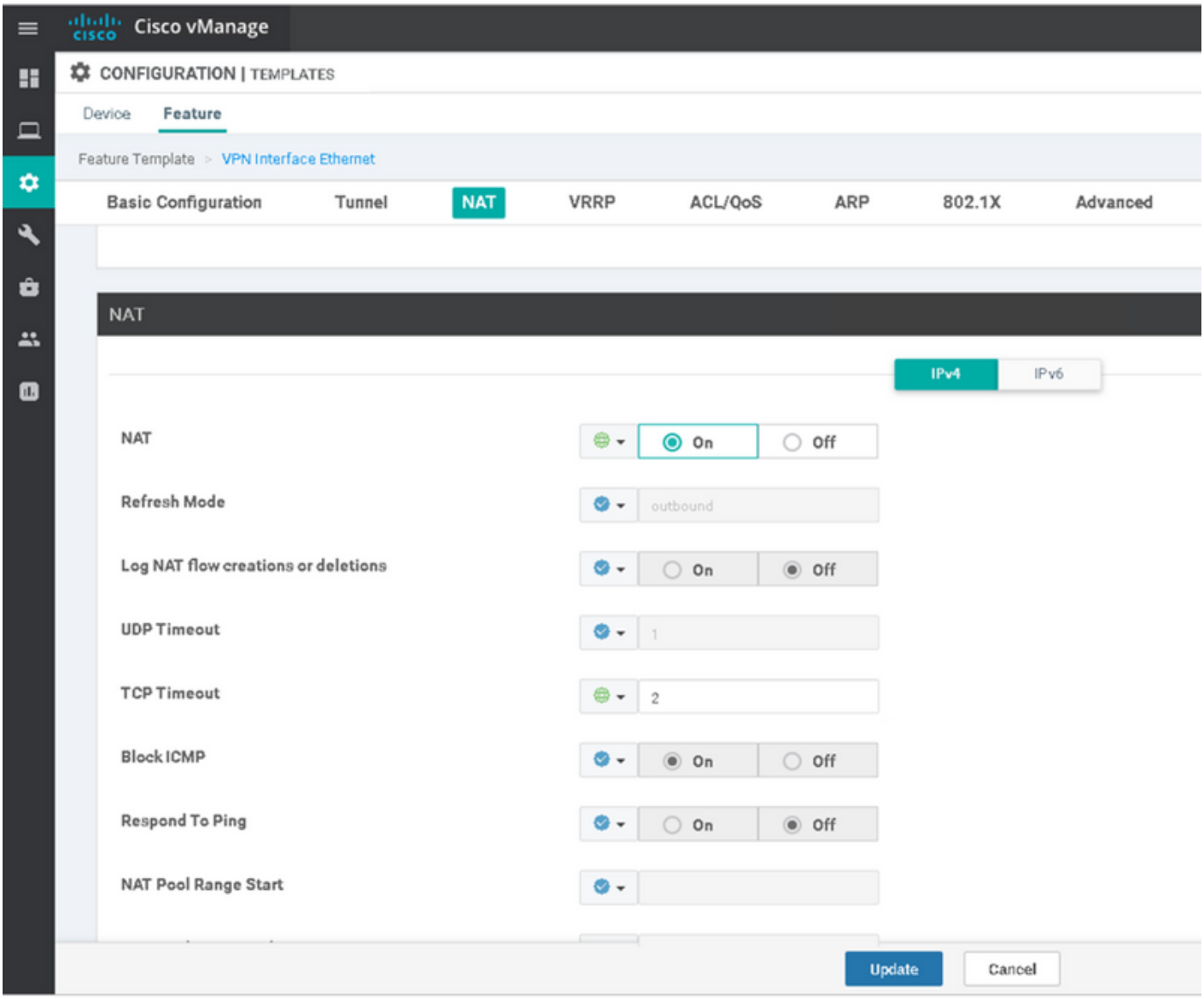
タイムアウトに注意してください。怪しげな低く見えませんか？約2 ~ 3分のFTPクライアントが非アクティブになった後、もう一度チェックすると、NATテーブルに変換がないことがわかります。

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

ほら！したがって、問題の根本原因は次のとおりです。セッションの有効期限が短くなりすぎているため、FTPクライアントセッションの観点からは存在しますが、cEdgeルータはTCPセッションについてすでに何も認識せず、リターントラフィックをドロップします。設定を確認すると、NATセッションタイムアウトが120秒に設定されていることがわかります。おそらく誤っています。

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

このタイマーは、vManageの対応するデバイステンプレートで修正する必要があります。



たとえば60分に変更すると、問題が解決します。