Configure and Verify PPPoE Redundancy/High Availability in ASA/FTD

Introduction

This document describes the configuration and verification of PPPoE redundancy (high availability or HA) in Secure Firewall ASA or Secure Firewall Threat Defense (FTD).

Prerequisites

Requirements

Basic product knowledge.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

- Secure Firewall Threat Defense (FTD) version 10.0.0 managed by the Secure Firewall Management Center (FMC) version 10.0.1.
- ASA version 9.24.1.

Background Information

The firewall software supports the configuration of multiple PPPoE sessions. In this document, 2 PPPoE sessions are considered, and “HA” or “redundancy” are used interchangeably.

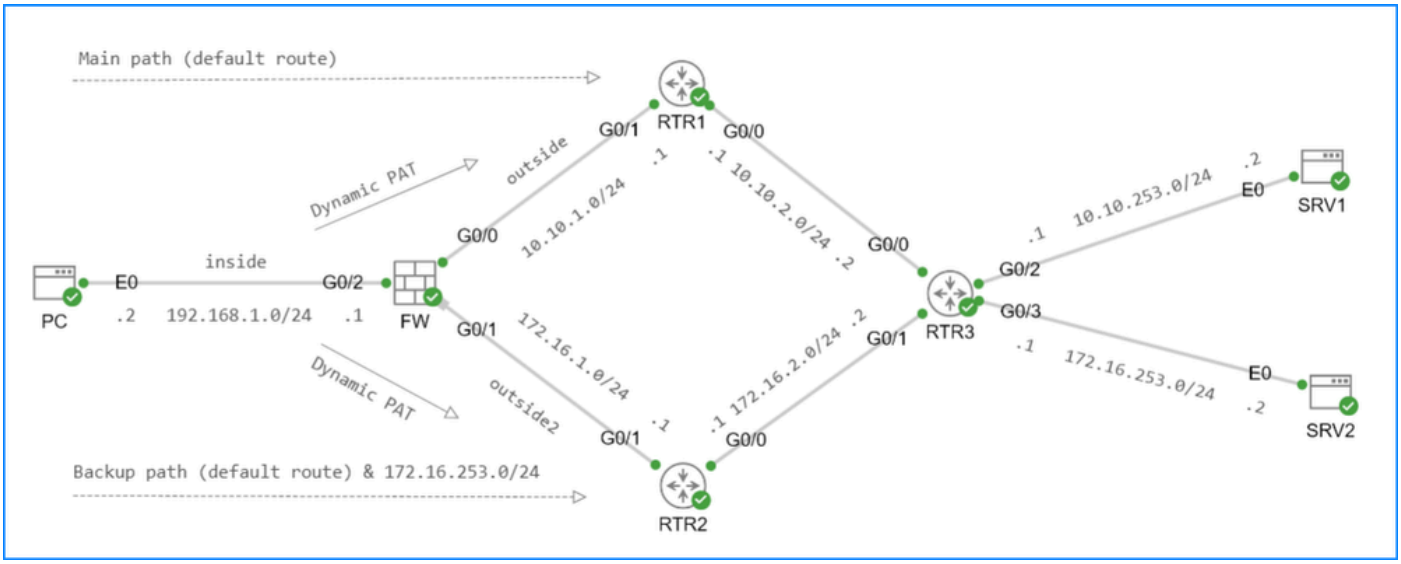
In combination with the Service Layer Agreement (SLA), tracking, and routing with tracking users can configure different redundancy modes:

- Active-active redundancy with load-sharing
- Active-active redundancy with load-sharing and PPPoE client route tracking
- Active-standby redundancy without load-sharing

Note that the configuration of routing on peer devices is outside of the scope of this article.

Active-Active Redundancy with Load-Sharing

Refer to this example topology:



Active-Active Redundancy with Load-Sharing

Key points:

- PPPoE is configured in firewall **outside** and **outside2** interfaces.
- RTR1 and RTR2 are PPPoE servers.
- The firewall installs the default route via the **outside** interface. The default route via the **outside2** interface has higher routing distance, that is, less preferrable.
- The achieve load-sharing, static routes to specific subnets are installed via the **outside2** interface. The routes are tracked. Tracking is optional; however, it provides faster failover to the path via the **outside** interface in case the path via the **outside2** interface fails.
- For the sake of simplicity, dynamic port address translation (PAT) is configured via the **outside** and **outside2** interfaces.

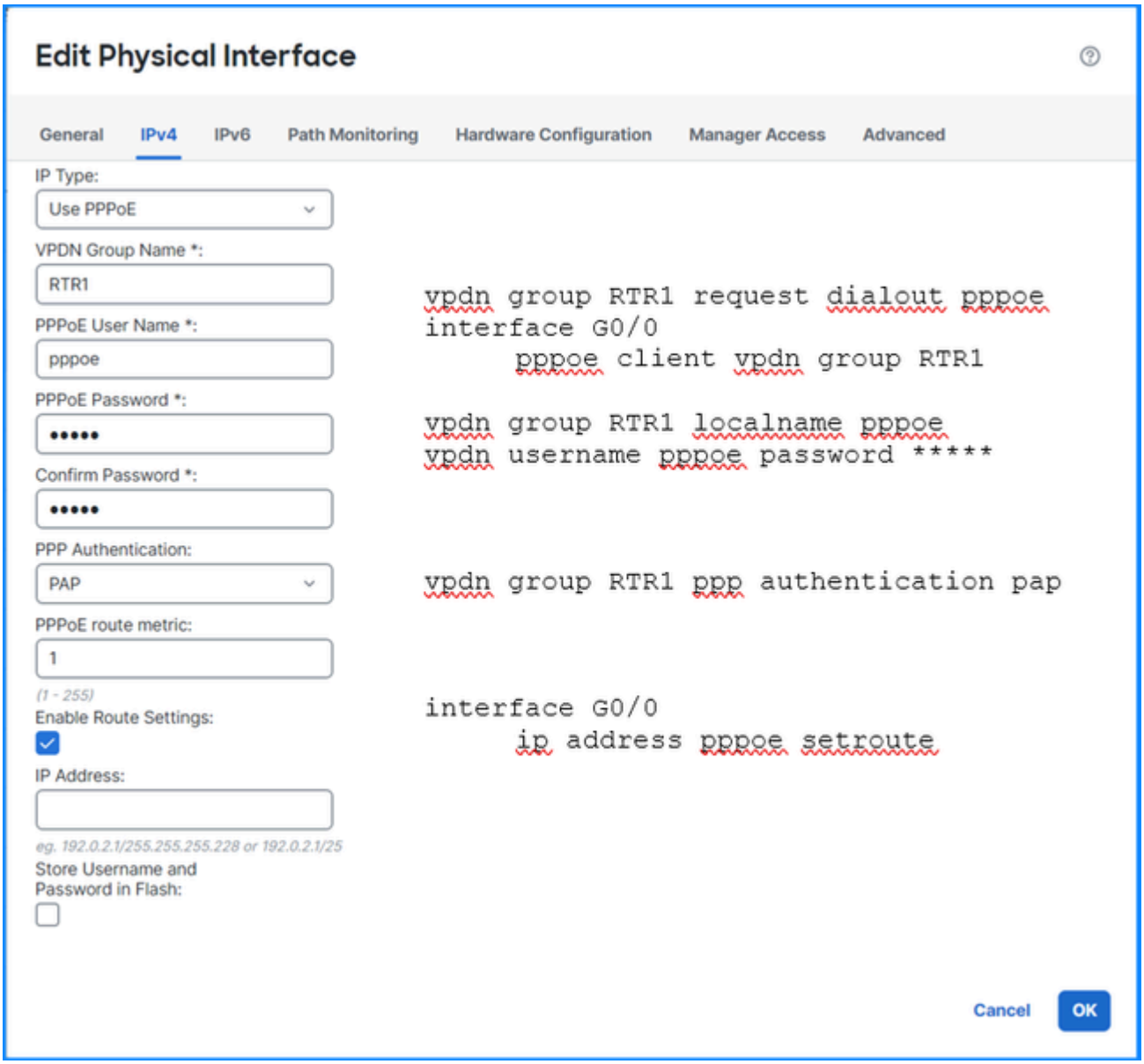
ASA Configuration

<#root>

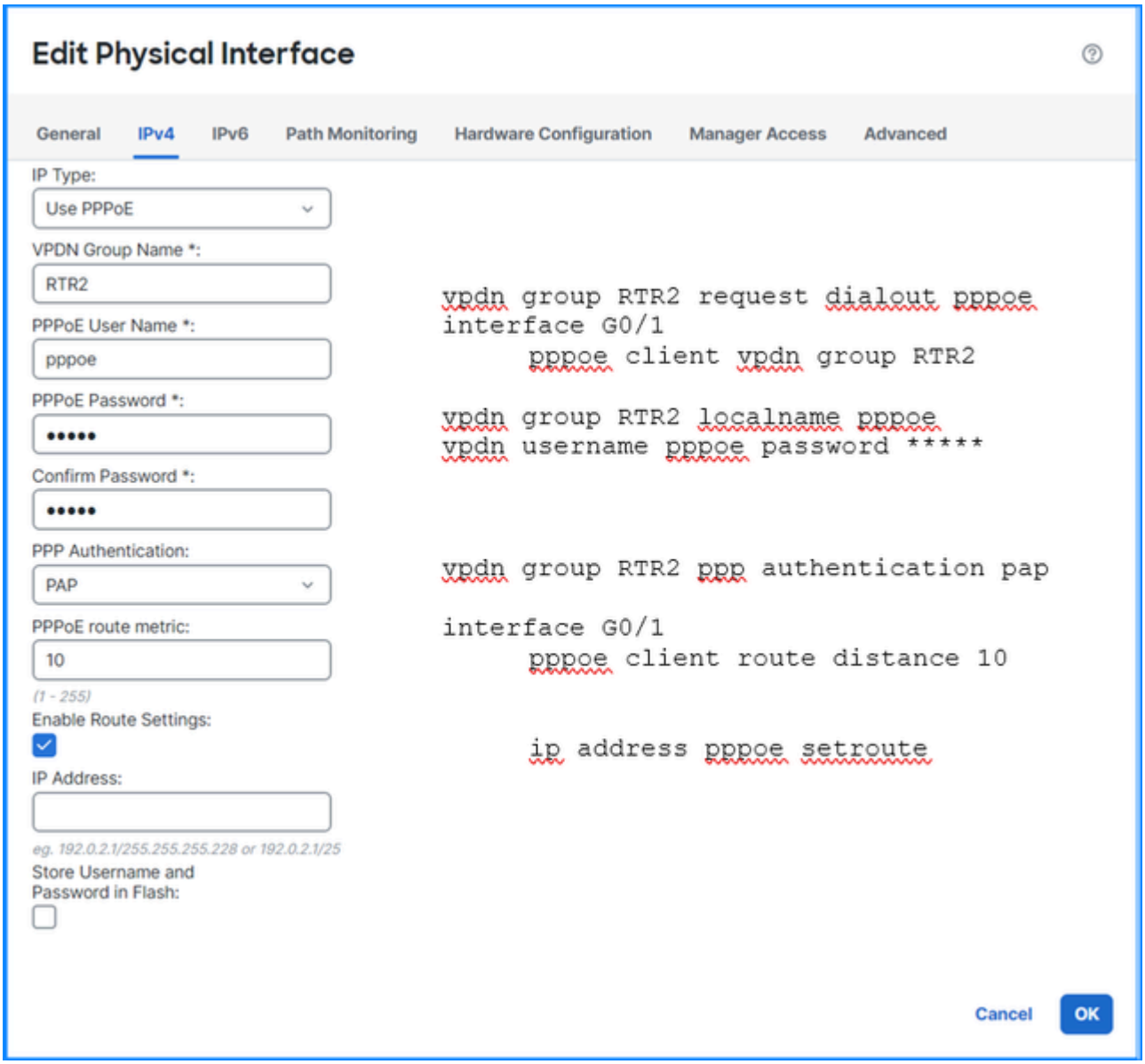
```
interface GigabitEthernet0/0
 nameif outside
 security-level 0

 pppoe client vpdn group RTR1


ip address pppoe setroute

interface GigabitEthernet0/1
 nameif outside2
 security-level 0

 pppoe client vpdn group RTR2




 pppoe client route distance 10


 ip address pppoe setroute

vpdn group RTR1 request dialout pppoe
vpdn group RTR1 localname pppoe
vpdn group RTR1 ppp authentication pap
vpdn group RTR2 request dialout pppoe
vpdn group RTR2 localname pppoe
vpdn username pppoe password *****
sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.1 interface outside2
 num-packets 2
 timeout 5
 frequency 5

sla monitor schedule 1 life forever start-time now
track 1 rtr 1 reachability

object network net-192.168.1.0
 subnet 192.168.1.0 255.255.255.0

nat (inside,outside) source dynamic net-192.168.1.0 interface
nat (inside,outside2) source dynamic net-192.168.1.0 interface


route outside2 172.16.253.0 255.255.255.0 172.16.1.1 1 track 1
```

FTD Configuration

This section covers only FTD-specific PPPoE configuration. This is the comparison of the **outside** and the **outside2** interfaces PPPoE configuration on FTD and the commands deployed to the data plane:

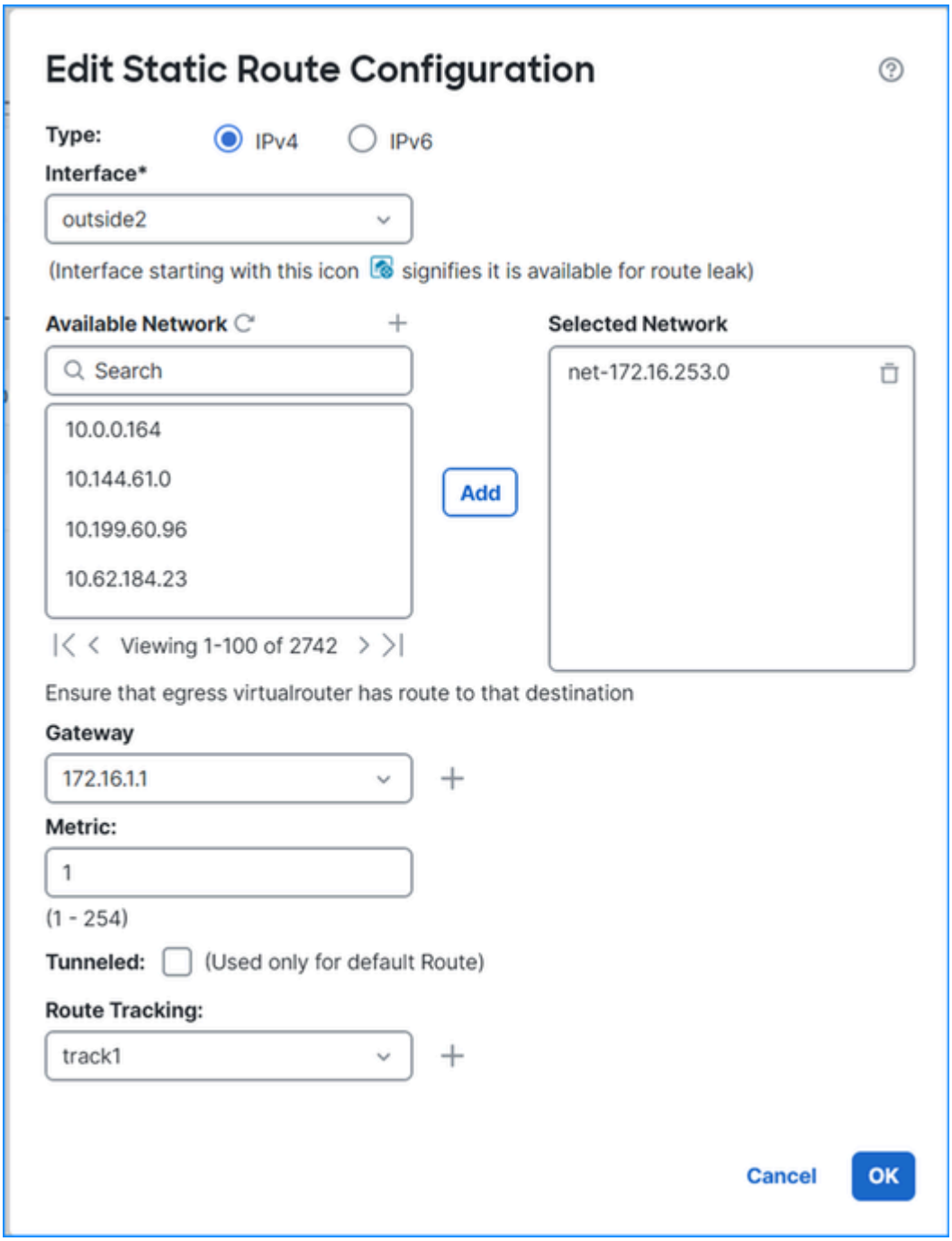


outside PPPoE interface configuration on FMC UI



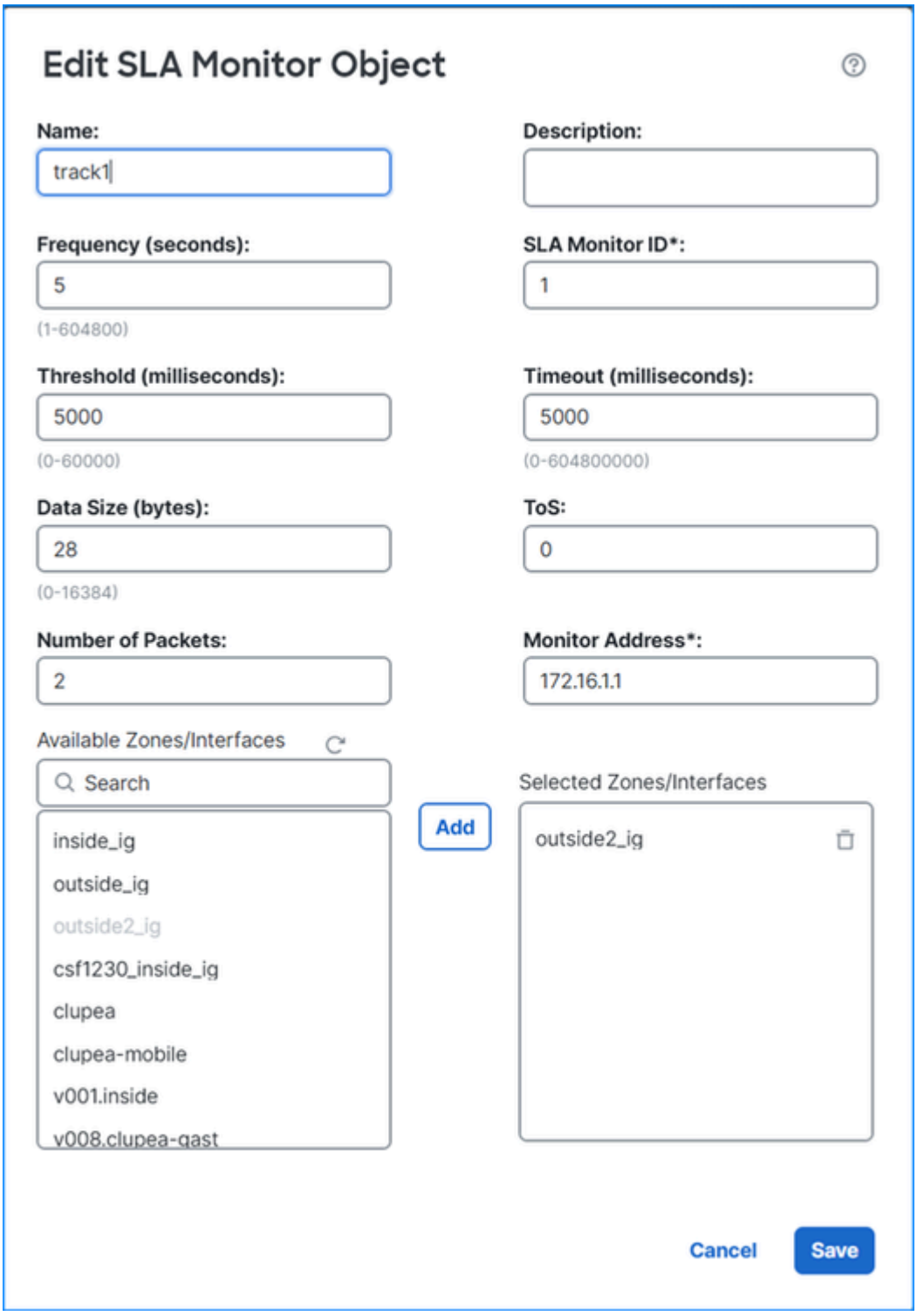
outside2 PPPoE interface configuration on FMC UI

Static route with tracking:



Static route with tracking

SLA monitor object configuration:



SLA configuration

Key points:

- **RTR1** and **RTR2** are 2 VPDN groups on G0/0 and G0/1 interfaces respectively.
- Track 1/SLA1 track the reachability to RTR2. The track object is used in the static route configuration via the **outside2** interface.
- The **pppoe client route distance 10** command instructs the firewall to apply administrative distance of **10** to the default route received from RTR2 and hence make it less preferable.
- Routes to specific subnets via the **outside2** interface are configured with tracking.
- As a result, both PPPoE sessions become active, and traffic from PC is load-shared depending on the

routing configuration.

Verification

1. PPPoE session with **RTR1** via the **outside** interface is established:

<#root>

```
firewall#

show vpdn session pppoe state


PPPoE Session Information (Total tunnels=2 sessions=1)

SessID TunID Intf     State       Last Chg
   23      5 outside2   PADI_SENT  225 secs

   14      4 outside  SESSION_UP  150 secs



firewall#

show vpdn pppinterface



PPP virtual interface id = 1
PPP authentication protocol is PAP
Server ip address is 10.10.1.1

Our ip address is 10.10.1.10



Transmitted Pkts: 33, Received Pkts: 33, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0

PPP virtual interface id = 2 was deleted and pending reuse

firewall#

show route



…

S*       0.0.0.0 0.0.0.0 [1/0] via 10.10.1.1, outside
```

```
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
```

Syslogs:

<#root>

```
Mar 15 2026 20:23:26: %ASA-6-305009: Built static translation from outside:0.0.0.0 to inside:0.0.0.0
Mar 15 2026 20:23:26: %ASA-6-603108:
```

Built PPPOE Tunnel, tunnel_id = 4, remote_peer_ip = 10.10.1.1, ppp_virtual_interface_id = 1, client_dyna

```
Mar 15 2026 20:23:26: %ASA-6-317077:
```

Added STATIC route 0.0.0.0 0.0.0.0 via 10.10.1.1 [1/0] on [outside] [G0/0] tableid [0

2. PPPoE session with **RTR2** via the **outside2** interface is established:

<#root>

```
firewall#
```

show vpdn session pppoe state

```
PPPoE Session Information (Total tunnels=2 sessions=2)
SessID TunID Intf     State       Last Chg
```

24 5 outside2 SESSION_UP 76 secs

14 4 outside SESSION_UP 349 secs

```
firewall#
```

show vpdn pppinterface

```
PPP virtual interface id = 1
PPP authentication protocol is PAP
Server ip address is 10.10.1.1
```

Our ip address is 10.10.1.10

Transmitted Pkts: 67, Received Pkts: 67, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0, MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0, MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0

PPP virtual interface id = 2
PPP authentication protocol is PAP
Server ip address is 172.16.1.1

Our ip address is 172.16.1.10

Transmitted Pkts: 54, Received Pkts: 54, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0, MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0, MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0

firewall#

show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
…

S*   0.0.0.0 0.0.0.0 [1/0] via 10.10.1.1, outside

S   172.16.253.0 255.255.255.0 [1/0] via 172.16.1.1, outside2

C   192.168.1.0 255.255.255.0 is directly connected, inside
L   192.168.1.1 255.255.255.255 is directly connected, inside

Syslogs:

<#root>

Mar 15 2026 20:27:59: %ASA-6-317077:

Added STATIC route 0.0.0.0 0.0.0.0 via 0.0.0.0 [10/0] on [outside2] [G0/1] tableid [0]

Mar 15 2026 20:27:59: %ASA-6-305009: Built static translation from outside2:0.0.0.0 to inside:0.0.0.0
Mar 15 2026 20:27:59: %ASA-6-603108:

Built PPPOE Tunnel, tunnel_id = 5, remote_peer_ip = 172.16.1.1, ppp_virtual_interface_id = 2, client_dyn

```
Mar 15 2026 20:27:59: %ASA-6-305010: Teardown static translation from outside2:0.0.0.0 to inside:0.0.0.
Mar 15 2026 20:28:04: %ASA-6-622001:

Adding tracked route 172.16.253.0 255.255.255.0 172.16.1.1, distance 1, table default, on interface outs


Mar 15 2026 20:28:04: %ASA-6-317077:

Added STATIC route 172.16.253.0 255.255.255.0 via 172.16.1.1 [1/0] on [outside2] [G0/1] tableid [0]
```

3. Packets from PC IP address 192.168.1.2 to 10.10.253.2 and 172.16.253.2 are sent. Due to PAT, the captures **capo** and **capo2** show the egress interface IP address (mapped addresses):

```
<#root>
Mar 14 2026 23:13:13: %ASA-6-305011: Built dynamic ICMP translation from

inside:192.168.1.2/2668 to outside:10.10.1.10/2668


Mar 14 2026 23:13:19: %ASA-6-305011: Built dynamic ICMP translation from

inside:192.168.1.2/2669 to outside2:172.16.1.10/2669



firewall#

show cap


capture capo type raw-data interface outside [

Capturing - 456 bytes

]
  match icmp any host 10.10.253.2
capture capo2 type raw-data interface outside2 [

Capturing - 456 bytes

]
  match icmp any host 172.16.253.2

firewall#

show cap capo
```

```
4 packets captured

   1: 23:13:13.409387

10.10.1.10 > 10.10.253.2 icmp: echo request


   2: 23:13:13.417764

10.10.253.2 > 10.10.1.10 icmp: echo reply


   3: 23:13:14.409799       10.10.1.10 > 10.10.253.2 icmp: echo request
   4: 23:13:14.415978       10.10.253.2 > 10.10.1.10 icmp: echo reply

4 packets shown

firewall#

show cap capo2


4 packets captured
   1: 23:13:19.500584

172.16.1.10 > 172.16.253.2 icmp: echo request


   2: 23:13:19.506321

172.16.253.2 > 172.16.1.10 icmp: echo reply


   3: 23:13:20.502201       172.16.1.10 > 172.16.253.2 icmp: echo request
   4: 23:13:20.508076       172.16.253.2 > 172.16.1.10 icmp: echo reply
```

4. Simulate remote link failure on RTR1. Failover to the backup path via the **outside2** interface takes around 1 minute:

RTR1:

```
<#root>

Mar 15 20:43:19.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state t
```

Firewall:

```
<#root>
```

Mar 15 2026 20:44:17: %ASA-3-403503:

PPPoE:PPP link down:

Mar 15 2026 20:44:17: %ASA-3-403503:

PPPoE:PPP link down:Peer not responding

Mar 15 2026 20:44:17: %ASA-3-403503:

PPPoE:PPP link down:

Mar 15 2026 20:44:17: %ASA-3-403503:

PPPoE:PPP link down:LCP down

Mar 15 2026 20:44:17: %ASA-6-603109:

Teardown PPPOE Tunnel, tunnel_id = 4, remote_peer_ip = 10.10.1.1

Mar 15 2026 20:44:17: %ASA-6-305009: Built static translation from outside:0.0.0.0 to inside:0.0.0.0
Mar 15 2026 20:44:17: %ASA-6-317078:

Deleted STATIC route 0.0.0.0 0.0.0.0 via 10.10.1.1 [1/0] on [outside] [G0/0] tableid [0]

Mar 15 2026 20:44:17: %ASA-7-110007:

Del Entry:0.0.0.0/0.0.0.0 nh:10.10.1.1 nh_cnt:1 flags:0 timestamp:147 resolver_cnt:0 ifcout:outside resu

Mar 15 2026 20:44:17: %ASA-6-317077: Added STATIC route 0.0.0.0 0.0.0.0 via 172.16.1.1 [10/0] on [outsid

Mar 15 2026 20:44:17: %ASA-7-110006: Add Entry:0.0.0.0/0.0.0.0 nh:172.16.1.1 nh_cnt:1 flags:0 timestamp
Mar 15 2026 20:44:17: %ASA-6-305010: Teardown static translation from outside:0.0.0.0 to inside:0.0.0.0

firewall#

show route

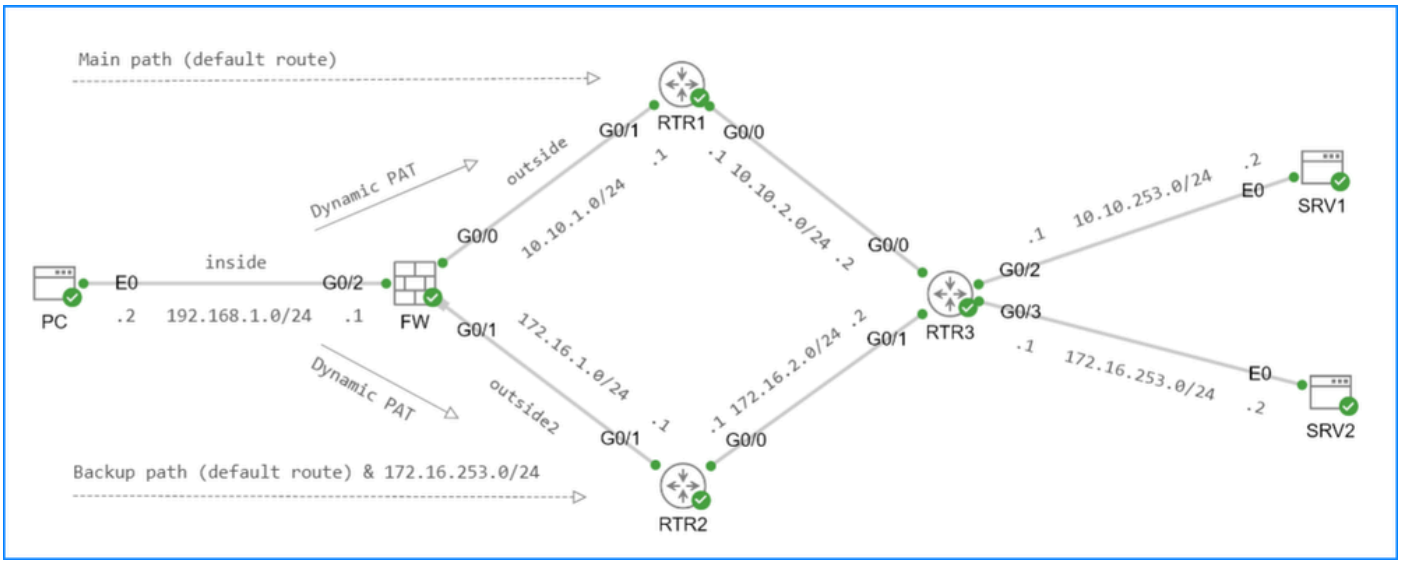
…

S* 0.0.0.0 0.0.0.0 [10/0] via 172.16.1.1, outside2

Active-Active Redundancy with Load-Sharing and PPPoE Client Route Tracking

This case is based on the active-active redundancy with load-sharing and additionally requires the deployment of the additional track and **pppoe client route track x** command under the **outside** interface using FlexConfig.

Refer to this example topology:



Active-Active Redundancy with Load-Sharing and PPPoE Client Route Tracking

Key points:

- PPPoE is configured in firewall **outside** and **outside2** interfaces.
- RTR1 and RTR2 are PPPoE servers.
- Using route-distance, the firewall installs the default route via the **outside** interface. The default route via the **outside2** interface has higher routing distance and is less preferrable.
- The default route to RTR1 via the outside interface is tracked. It's optional, however depending on the SLA frequency and timeout values, it can provides faster failover to the path via RTR2.
- The achieve load-sharing, static routes to specific subnets are installed via the **outside2** interface. The routes are tracked. Tracking is optional; however, it provides faster failover to the path via RTR1.
- For the sake of simplicity, dynamic port address translation (PAT) is configured via the **outside** and **outside2** interfaces.

ASA Configuration

<#root>

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
```

```
 pppoe client vpdn group RTR1



 pppoe client route track 2



 ip address pppoe setroute

interface GigabitEthernet0/1
 nameif outside2
 security-level 0

 pppoe client vpdn group RTR2



 pppoe client route distance 10



 ip address pppoe setroute

vpdn group RTR1 request dialout pppoe
vpdn group RTR1 localname pppoe
vpdn group RTR1 ppp authentication pap
vpdn group RTR2 request dialout pppoe
vpdn group RTR2 localname pppoe
vpdn username pppoe password *****

sla monitor 2
 type echo protocol ipIcmpEcho 10.10.1.1 interface outside
 num-packets 2
 timeout 5
 frequency 5

sla monitor schedule 2 life forever start-time now

sla monitor 1
 type echo protocol ipIcmpEcho 172.16.1.1 interface outside2
 num-packets 2
 timeout 5
 frequency 5
sla monitor schedule 1 life forever start-time now

track 1 rtr 1 reachability
track 2 rtr 2 reachability

object network net-192.168.1.0
 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) source dynamic net-192.168.1.0 interface
nat (inside,outside2) source dynamic net-192.168.1.0 interface



route outside2 172.16.253.0 255.255.255.0 172.16.1.1 1 track 1
```

FTD Configuration

This section covers only FTD-specific PPPoE configuration. The configuration steps are the same as the FTD configuration in the "Active-Active Redundancy with Load-Sharing" section with the addition of the deployment of the **pppoe client route track x** command under the **outside** interface. Since FMC UI does not natively support tracks for the client options, FlexConfig must be used.

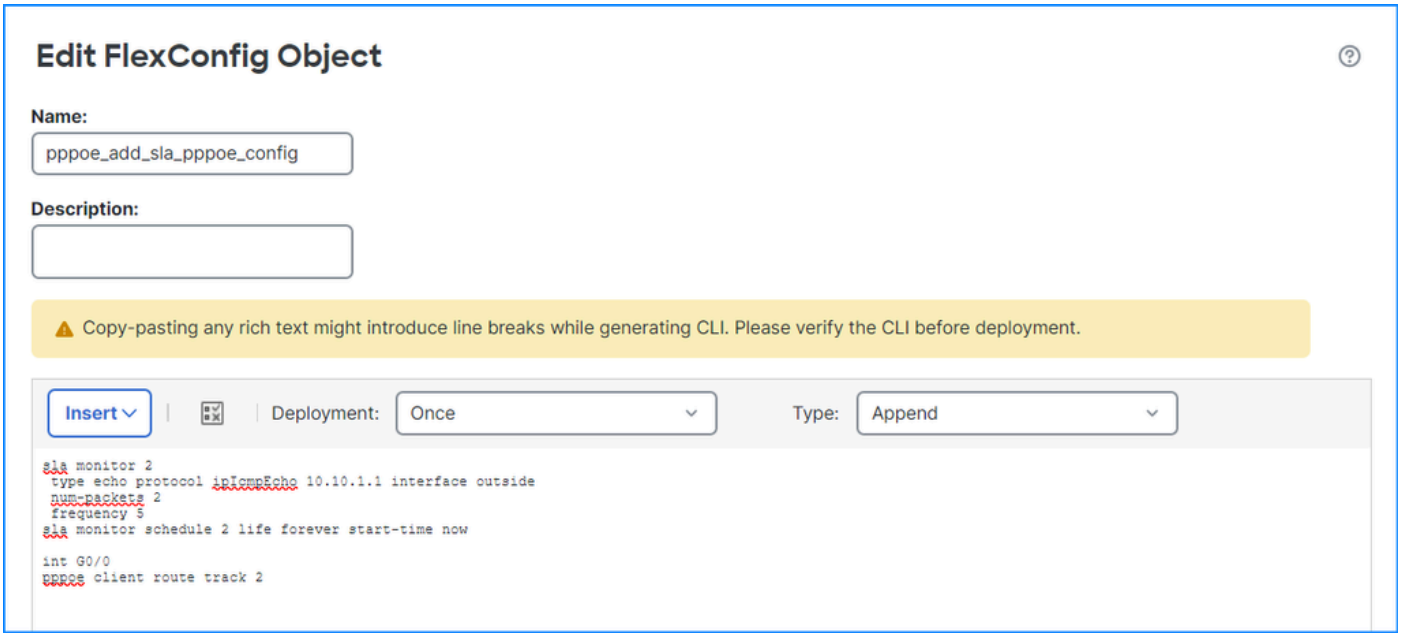
Ensure that you consider these points:

1. FlexConfig policies intentionally do not contain extensive input validation. You must ensure that the configurations in this FlexConfig policy are correct. Incorrect configurations results in a failed deployment that can cause a network interruption. Also, consider isolating the deployment so it includes just FlexConfig changes, and no other policy updates.

2. During the deployment FMC removes any **track x..** command deployed by FlexConfig. For persistence you must set the deployment of the FlexConfig object to **Everytime** and deploy in a separate FlexConfig object**.**

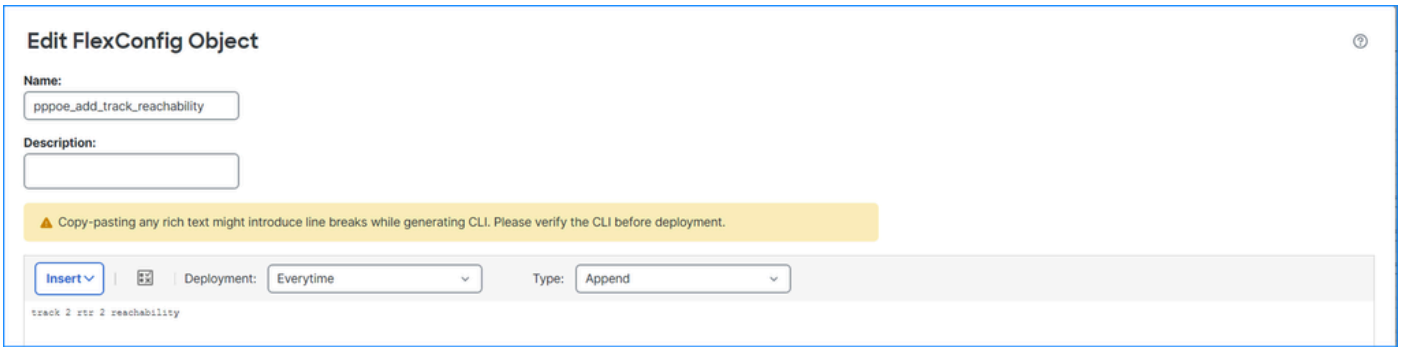
FlexConfig Configuration Steps

1. Create a FlexConfig object for the configuration of SLA and PPPoE client configurations for the **outside** interface. Ensure to set **Deployment** to **Once** and **Type** to **Append**. In this example, track 2, SLA 2 are used. Notice that the **track 2 rtr 2 reachability** command is missing:



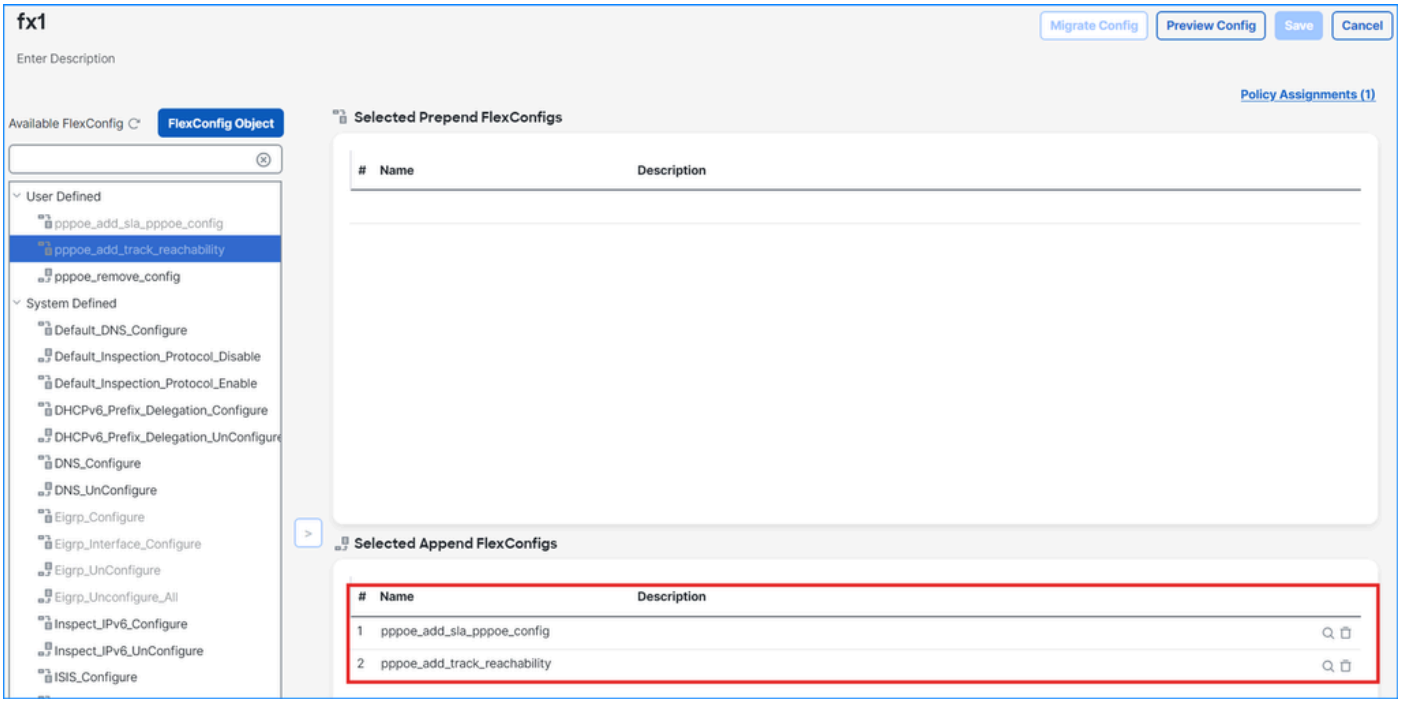
FlexConfig for SLA

2. Create another FlexConfig object for the configuration of **track 2 rtr 2 reachability** command. Ensure to set **Deployment** to **Everytime** and **Type** to **Append:**



FlexConfig for track

3. Add objects to the FlexConfig policy. Ensure that the object with the **track 2 rtr 2 reachability** command at the bottom (last), and deploy policies:



FlexConfig policy

Key points:

- **RTR1** and **RTR2** are 2 VPDN groups on G0/0 and G0/1 interfaces respectively.
- Track 2/SLA2 track the reachability to RTR1. The **pppoe client route track 2** command instructs the firewall to install the default route via the **outside** interface if track 2 is up.
- Track 1/SLA1 track the reachability to RTR2. The track object is used in the static route configuration via the **outside2** interface.
- The **pppoe client route distance 10** command instructs the firewall to apply administrative distance of 10 to the default route received from RTR2 and hence make it less preferable.
- Routes to specific subnets via the **outside2** interface are configured with tracking.
- As a result, both PPPoE sessions become active, and traffic from PC is load-shared depending on the routing configuration.

Verification

1. PPPoE session with **RTR1** via the **outside** interface is established:

```
<#root>
firewall#

show vpdn session pppoe state


PPPoE Session Information (Total tunnels=2 sessions=1)

SessID TunID Intf     State       Last Chg


12      3 outside  SESSION_UP  80 secs


   12      4 outside2   PADI_SENT  74 secs

firewall#

show vpdn pppinterface




PPP virtual interface id = 1


PPP authentication protocol is PAP
Server ip address is 10.10.1.1

Our ip address is 10.10.1.10


Transmitted Pkts: 71, Received Pkts: 71, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0


PPP virtual interface id = 2 was deleted and pending reuse



firewall#

show route
```

…

S* 0.0.0.0 0.0.0.0 [1/0] via 10.10.1.1, outside

C 192.168.1.0 255.255.255.0 is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside

Syslogs:

<#root>

Mar 14 2026 22:54:46: %ASA-4-411001: Line protocol on Interface GigabitEthernet0/0, changed state to up
Mar 14 2026 22:54:50: %ASA-6-305009:

Built static translation from outside:0.0.0.0 to inside:0.0.0.0

Mar 14 2026 22:54:50: %ASA-6-603108

: Built PPPOE Tunnel, tunnel_id = 3, remote_peer_ip = 10.10.1.1, ppp_virtual_interface_id = 1, client_dy

Mar 14 2026 22:54:51: %ASA-6-305010: Teardown static translation from outside:0.0.0.0 to inside:0.0.0.0
Mar 14 2026 22:54:52: %ASA-6-622001:

Adding tracked route 0.0.0.0 0.0.0.0 10.10.1.1, distance 1, table default, on interface outside

Mar 14 2026 22:54:52: %ASA-6-317077:

Added STATIC route 0.0.0.0 0.0.0.0 via 10.10.1.1 [1/0] on [outside] [Gi0/0] tableid [0]

Mar 14 2026 22:54:52: %ASA-7-110006: Add Entry:0.0.0.0/0.0.0.0 nh:10.10.1.1 nh_cnt:1 flags:0 timestamp:

2. PPPoE session with **RTR2** via the **outside2** interface is established:

<#root>

firewall#

show vpdn session pppoe state

PPPoE Session Information (Total tunnels=2 sessions=2)
SessID TunID Intf State Last Chg

12 3 outside SESSION_UP 412 secs

```
   13      4 outside2  SESSION_UP  89 secs


firewall#

show vpdn pppinterface



PPP virtual interface id = 1


PPP authentication protocol is PAP
Server ip address is 10.10.1.1

Our ip address is 10.10.1.10


Transmitted Pkts: 238, Received Pkts: 238, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0

PPP virtual interface id = 2
PPP authentication protocol is PAP
Server ip address is 172.16.1.1

Our ip address is 172.16.1.10


Transmitted Pkts: 56, Received Pkts: 56, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0

firewall#

show route



Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.10.1.1 to network 0.0.0.0
```

```
S*       0.0.0.0 0.0.0.0 [1/0] via 10.10.1.1, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside

S        172.16.253.0 255.255.255.0 [1/0] via 172.16.1.1, outside2
```

Syslogs:

<#root>

```
Mar 14 2026 22:59:45: %ASA-4-411001: Line protocol on Interface GigabitEthernet0/1, changed state to up
Mar 14 2026 23:00:13: %ASA-6-603108:

 Built PPPOE Tunnel, tunnel_id = 4, remote_peer_ip = 172.16.1.1, ppp_virtual_interface_id = 2, client_dy


Mar 14 2026 23:00:14: %ASA-6-305010: Teardown static translation from outside2:0.0.0.0 to inside:0.0.0.
Mar 14 2026 23:00:18: %ASA-6-622001:

 Adding tracked route 172.16.253.0 255.255.255.0 172.16.1.1, distance 1, table default, on interface out


Mar 14 2026 23:00:18: %ASA-6-317077:

 Added STATIC route 172.16.253.0 255.255.255.0 via 172.16.1.1 [1/0] on [outside2] [Gi0/1] tableid [0]


Mar 14 2026 23:00:18: %ASA-7-110006:

 Add Entry:172.16.253.0/255.255.255.0 nh:172.16.1.1 nh_cnt:1 flags:0 timestamp:339 resolver_cnt:0 ifcout
```

3. Packets from PC IP address 192.168.1.2 to 10.10.253.2 and 172.16.253.2 are sent. Due to PAT, the captures capo and capo2 show the egress interface IP address (mapped addresses):

<#root>

```
Mar 14 2026 23:13:13: %ASA-6-305011: Built dynamic ICMP translation from

inside:192.168.1.2/2668 to outside:10.10.1.10/2668


Mar 14 2026 23:13:19: %ASA-6-305011: Built dynamic ICMP translation from

inside:192.168.1.2/2669 to outside2:172.16.1.10/2669


firewall#
```

show cap

capture capo type raw-data interface outside [

Capturing - 456 bytes

]
  match icmp any host 10.10.253.2
capture capo2 type raw-data interface outside2 [

Capturing - 456 bytes

]
  match icmp any host 172.16.253.2

firewall#

show cap capo

4 packets captured

   1: 23:13:13.409387

10.10.1.10 > 10.10.253.2 icmp: echo request

   2: 23:13:13.417764

10.10.253.2 > 10.10.1.10 icmp: echo reply

   3: 23:13:14.409799   10.10.1.10 > 10.10.253.2 icmp: echo request
   4: 23:13:14.415978   10.10.253.2 > 10.10.1.10 icmp: echo reply

4 packets shown

firewall#

show cap capo2

4 packets captured

   1: 23:13:19.500584

172.16.1.10 > 172.16.253.2 icmp: echo request

   2: 23:13:19.506321

172.16.253.2 > 172.16.1.10 icmp: echo reply

```
   3: 23:13:20.502201       172.16.1.10 > 172.16.253.2 icmp: echo request
   4: 23:13:20.508076       172.16.253.2 > 172.16.1.10 icmp: echo reply
```

4. Simulate remote link failure on RTR1. Failover to the backup path via the outside2 interface depends on the timers of track1:

RTR1:

<#root>

Mar 15 21:06:11.608: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/0/0, changed st

Firewall:

<#root>

Mar 15 2026 21:06:14: %ASA-3-317012: Interface IP route counter negative - Ethernet1/2

Mar 15 2026 21:06:14: %ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.10.1.1, distance 1, table

Mar 15 2026 21:06:14: %ASA-6-317078: Deleted STATIC route 0.0.0.0 0.0.0.0 via 10.10.1.1 [1/0] on [outsid

Mar 15 2026 21:06:14: %ASA-7-110007: Del Entry:0.0.0.0/0.0.0.0 nh:10.10.1.1 nh_cnt:1 flags:0 timestamp:1

Mar 15 2026 21:06:14: %ASA-6-317077: Added STATIC route 0.0.0.0 0.0.0.0 via 172.16.1.1 [10/0] on [outsid

Mar 15 2026 21:06:14: %ASA-7-110006: Add Entry:0.0.0.0/0.0.0.0 nh:172.16.1.1 nh_cnt:1 flags:0 timestamp

KSEC-CSF1210-1#

show route

…

S*   0.0.0.0 0.0.0.0 [10/0] via 172.16.1.1, outside2

Note:

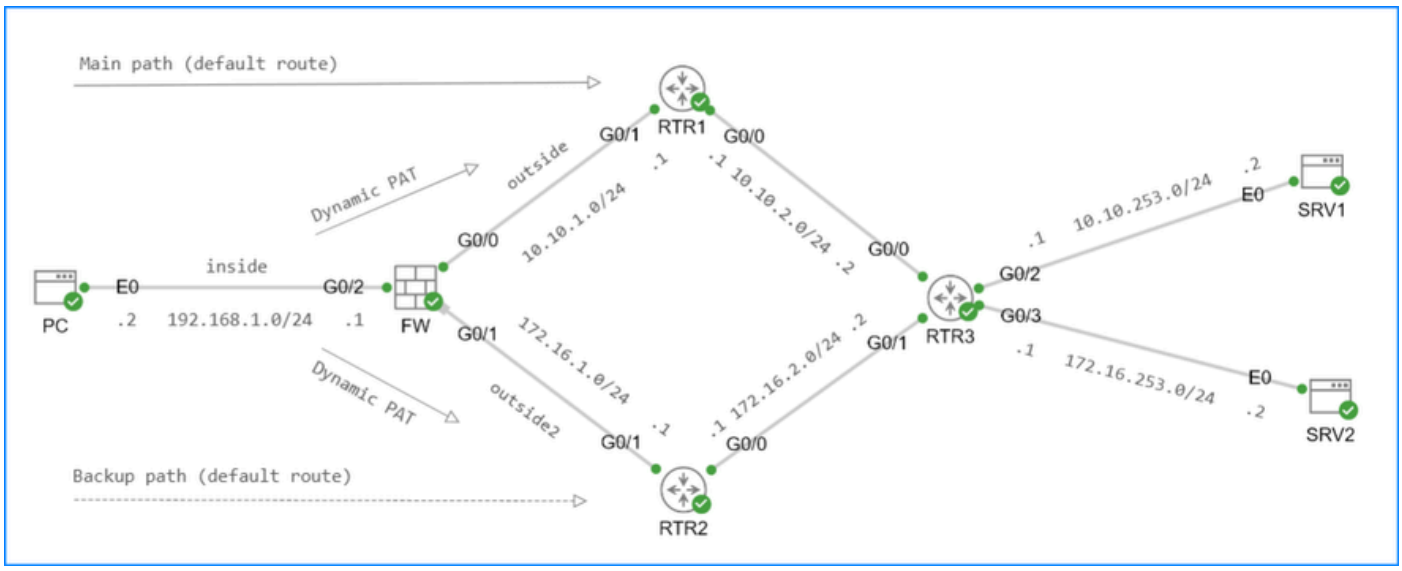
The changes in routing are not applied to existing connections. Therefore, existing connection continue using the “old” path even if a better path becomes available. Effectively, this can cause impact after routing changes. To instruct the firewall to use the new path, consider enabling the floating conn timer. If the floating-conn timeout is enabled, and is set to non-zero value, then if a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. Refer to the description of **floating-conn** in https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/T-Z/asa-command-ref-T-Z/m_ta-tk.html.

Active-Standby Redundancy Without Load-Sharing

In this case, only 1 PPPoE session is active, the other is inactive until the track for the active session becomes down.

The command **pppoe client secondary track x** is used for the **outside2** (backup) interface.

Refer to this example topology:



Active standby topology

Key points:

- PPPoE is configured in firewall G0/0 and G0/1 interfaces.
- RTR1 and RTR2 are PPPoE servers.
- Using route-distance, the firewall installs the default route to RTR1 via the **outside** interface. The default route to RTR2 has higher routing distance and is less preferrable.
- The default route to RTR1 via the **outside** interface is tracked. It’s optional, however, it provides faster failover to the path via RTR2.
- The PPPoE session to RTR2 via the **outside2** interface is established only if the track used for the

default route to RTR1 via the **outside** interface is down.
- At a given time only 1 PPPoE session is active.
- For the sake of simplicity, dynamic port address translation (PAT) is configured via the **outside** and **outside2** interfaces.

ASA Configuration

<#root>

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0

 pppoe client vpdn group RTR1



 pppoe client route track 2


 ip address pppoe setroute

interface GigabitEthernet0/1
 nameif outside2
 security-level 0

 pppoe client vpdn group RTR2



 pppoe client route distance 10



 pppoe client secondary track 2


 ip address pppoe setroute

vpdn group RTR1 request dialout pppoe
vpdn group RTR1 localname pppoe
vpdn group RTR1 ppp authentication pap
vpdn group RTR2 request dialout pppoe
vpdn group RTR2 localname pppoe
vpdn username pppoe password *****

sla monitor 2
 type echo protocol ipIcmpEcho 10.10.1.1 interface outside
 num-packets 2
 timeout 5
 frequency 5
sla monitor schedule 2 life forever start-time now

track 2 rtr 2 reachability
```

```
object network net-192.168.1.0
 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) source dynamic net-192.168.1.0 interface
nat (inside,outside2) source dynamic net-192.168.1.0 interface
```

FTD Configuration

This section covers configuration of the **pppoe client secondary track x** command for the **outside2** (backup) interface. Since FMC UI does not natively support tracks for the client options, FlexConfig must be used.

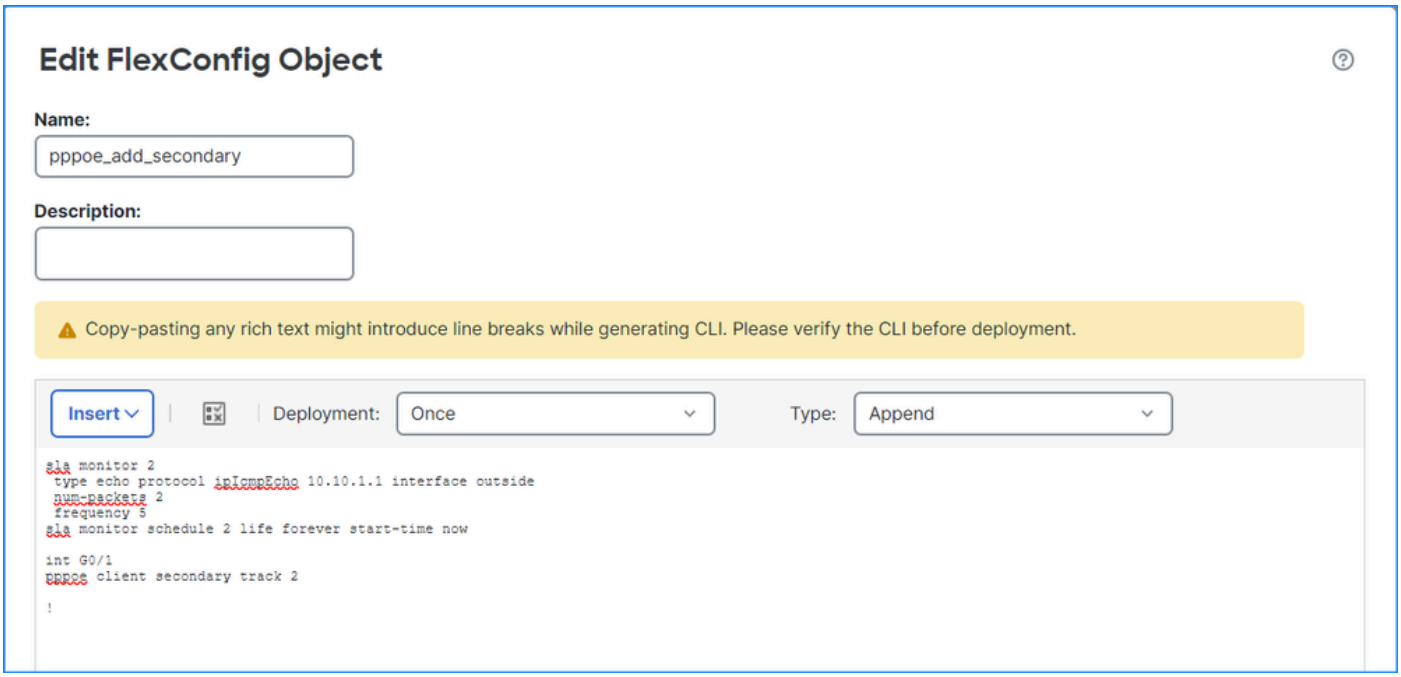
You must ensure configuring rest of the configuration including PPPoE configuration, routing and others.

Ensure that you consider these points:

1. FlexConfig policies intentionally do not contain extensive input validation. You must ensure that the configurations in this FlexConfig policy are correct. Incorrect configurations results in a failed deployment that can cause a network interruption. Also, consider isolating the deployment so it includes just FlexConfig changes, and no other policy updates.
2. During the deployment FMC removes any **track x..** command deployed by FlexConfig. For persistence you must set the deployment of the FlexConfig object to **Everytime** and deploy in a separate FlexConfig object**.**

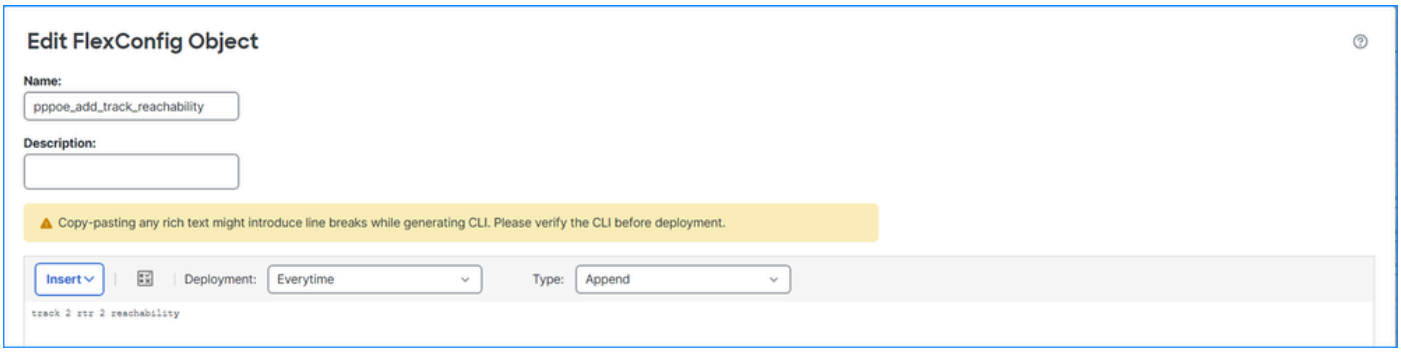
FlexConfig Configuration Steps

1. Create a FlexConfig object for the configuration of SLA and PPPoE client configurations for the **outside2** (backup) interface. Ensure to set **Deployment** to **Once** and **Type** to **Append**. In this example, track 2, SLA 2 are used. Notice that the **track 2 rtr 2 reachability** command is missing:



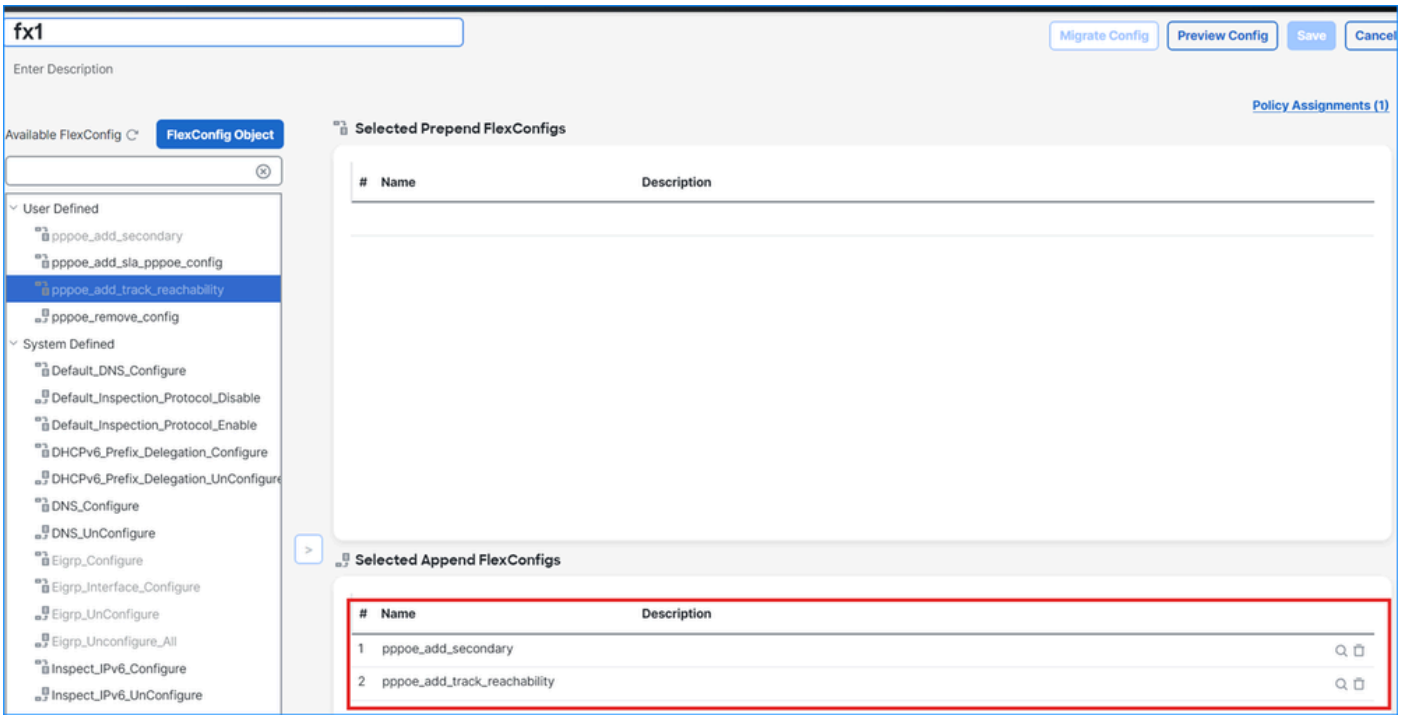
FlexConfig for SLA

2. Create another FlexConfig object for the configuration of **track 2 rtr 2 reachability** command. Ensure to set **Deployment** to **Everytime** and **Type** to **Append:**



FlexConfig for track

3. Add objects to the FlexConfig policy. Ensure that the object with the **track 2 rtr 2 reachability** command at the bottom (last), and deploy policies:



FlexConfig policy

Key points:

- The **pppoe client secondary track 2** command under the **G0/1** interface instructs the firewall to activate the PPPoE session via the G0/1 interface **only** if track 2 **fails**. Effectively the failure of track 2 that tracks reachability via the main path activates the backup path.
- As a result, only 1 PPPoE session is active at a given time.

Verification

1. PPPoE session with **RTR1** via the **outside** interface is already established. The backup session is idle:

```
<#root>
firewall#

show vpdn session pppoe state



PPPoE Session Information (Total tunnels=1 sessions=1)

SessID TunID Intf     State       Last Chg

   13      3 outside  SESSION_UP  72 secs



firewall#
```

show vpdn pppinterface

```
PPP virtual interface id = 1
PPP authentication protocol is PAP
Server ip address is 10.10.1.1
```

Our ip address is 10.10.1.10

```
Transmitted Pkts: 60, Received Pkts: 60, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0
```

PPP virtual interface id = 2 was deleted and pending reuse

2. The PPPoE session to RTR1 via the **outside** interface fails (for example, due to physical interface or link failure). The PPPoE session to RTR2 via the **outside2** interface is established.

Syslogs:

<#root>

```
Mar 14 2026 23:40:50: %ASA-3-403503: PPPoE:PPP link down:Peer not responding
Mar 14 2026 23:40:50: %ASA-3-403503: PPPoE:PPP link down:
Mar 14 2026 23:40:50: %ASA-3-403503:
```

PPPoE:PPP link down:LCP down

```
Mar 14 2026 23:40:50: %ASA-6-603109:
```

Teardown PPPOE Tunnel, tunnel_id = 3, remote_peer_ip = 10.10.1.1

```
Mar 14 2026 23:40:50: %ASA-6-305009: Built static translation from outside:0.0.0.0 to inside:0.0.0.0
Mar 14 2026 23:39:44: %ASA-4-411002:
```

Line protocol on Interface GigabitEthernet0/0, changed state to down

```
Mar 14 2026 23:39:44: %ASA-7-713906: IKE Receiver: Interface 3(outside) going down
Mar 14 2026 23:39:44: %ASA-3-317012: Interface IP route counter negative - GigabitEthernet0/0
Mar 14 2026 23:39:44: %ASA-6-317078:
```

Deleted STATIC route 0.0.0.0 0.0.0.0 via 10.10.1.1 [1/0] on [outside] [Gi0/0] tableid [0]

```
Mar 14 2026 23:39:44: %ASA-7-110007: Del Entry:0.0.0.0/0.0.0.0 nh:10.10.1.1 nh_cnt:1 flags:0 timestamp:
Mar 14 2026 23:39:48: %ASA-6-622001:

Removing tracked route 0.0.0.0 0.0.0.0 10.10.1.1, distance 1, table default, on interface outside


Mar 14 2026 23:39:48: %ASA-6-305009: Built static translation from outside2:0.0.0.0 to inside:0.0.0.0
Mar 14 2026 23:39:48: %ASA-6-603108:

Built PPPOE Tunnel, tunnel_id = 4, remote_peer_ip = 172.16.1.1, ppp_virtual_interface_id = 2, client_dyn


Mar 14 2026 23:39:48: %ASA-6-317078: Deleted CONNECTED route 172.16.1.10 255.255.255.255 via 0.0.0.0 [0
Mar 14 2026 23:39:48: %ASA-6-317077:

Added STATIC route 0.0.0.0 0.0.0.0 via 172.16.1.1 [10/0] on [outside2] [Gi0/1] tableid [0]


Mar 14 2026 23:39:48: %ASA-7-110006: Add Entry:0.0.0.0/0.0.0.0 nh:172.16.1.1 nh_cnt:1 flags:0 timestamp

firewall#

show vpdn session pppoe state



PPPoE Session Information (Total tunnels=2 sessions=1)

SessID TunID Intf     State       Last Chg
   13      3 outside   PADI_SENT  0 secs

   14      4 outside2  SESSION_UP  82 secs



firewall#

show vpdn pppinterface



PPP virtual interface id = 1 was deleted and pending reuse


PPP virtual interface id = 2
PPP authentication protocol is PAP
Server ip address is 172.16.1.1

Our ip address is 172.16.1.10


Transmitted Pkts: 56, Received Pkts: 56, Error Pkts: 0
```

```
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0

firewall#
```

show route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is 172.16.1.1 to network 0.0.0.0
```

S* 0.0.0.0 0.0.0.0 [10/0] via 172.16.1.1, outside2

S 172.16.253.0 255.255.255.0 [1/0] via 172.16.1.1, outside2

```
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
```

3. Packets from PC IP address 192.168.1.2 to 10.10.253.2 and 172.16.253.2 are sent. Due to failure of the main path, all packets are sent via the **outside2** interface. Additionally, due to PAT, capture **capo2** shows the egress interface IP address (mapped addresses):

<#root>

```
Mar 14 2026 23:46:07: %ASA-6-305011:
```

Built dynamic ICMP translation from inside:192.168.1.2/2677 to outside2:172.16.1.10/2677

```
Mar 14 2026 23:46:09: %ASA-6-305011:
```

Built dynamic ICMP translation from inside:192.168.1.2/2678 to outside2:172.16.1.10/2678

```
firewall#
```

show cap

```
capture capo type raw-data interface outside [Capturing - 0 bytes]
  match icmp any host 10.10.253.2
capture capo2 type raw-data interface outside2 [

Capturing - 912 bytes

]
  match icmp any host 172.16.253.2
  match icmp any host 10.10.253.2

firewall#

show cap capo2



8 packets captured

   1: 23:46:07.533694

172.16.1.10 > 172.16.253.2 icmp: echo request



   2: 23:46:07.541842

172.16.253.2 > 172.16.1.10 icmp: echo reply



   3: 23:46:08.534075       172.16.1.10 > 172.16.253.2 icmp: echo request
   4: 23:46:08.540621       172.16.253.2 > 172.16.1.10 icmp: echo reply
   5: 23:46:09.773031

172.16.1.10 > 10.10.253.2 icmp: echo request



   6: 23:46:09.780034

10.10.253.2 > 172.16.1.10 icmp: echo reply



   7: 23:46:10.773946       172.16.1.10 > 10.10.253.2 icmp: echo request
   8: 23:46:10.778569       10.10.253.2 > 172.16.1.10 icmp: echo reply
```

4. Path via the outside interface is recovered, PPPoE session to RTR1 is re-established. The session via the **outside2** interface transitions to the **pending reuse state**:

```
<#root>

firewall#

show vpdn session pppoe state
```

```
PPPoE Session Information (Total tunnels=1 sessions=1)

SessID TunID Intf     State       Last Chg

   17      3 outside  SESSION_UP  89 secs



firewall#

show vpdn pppinterface



PPP virtual interface id = 1
PPP authentication protocol is PAP
Server ip address is 10.10.1.1

Our ip address is 10.10.1.10



Transmitted Pkts: 58, Received Pkts: 58, Error Pkts: 0
MPPE key strength is None
  MPPE_Encrypt_Pkts: 0,  MPPE_Encrypt_Bytes: 0
  MPPE_Decrypt_Pkts: 0,  MPPE_Decrypt_Bytes: 0
  Rcvd_Out_Of_Seq_MPPE_Pkts: 0


PPP virtual interface id = 2 was deleted and pending reuse




firewall#

show route



...


S*       0.0.0.0 0.0.0.0 [1/0] via 10.10.1.1, outside


C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
```

Syslogs:

<#root>

```
Mar 15 2026 00:04:36: %ASA-4-411001:
```

Line protocol on Interface GigabitEthernet0/0, changed state to up

Mar 15 2026 00:05:27: %ASA-6-603108:

Built PPPOE Tunnel, tunnel_id = 3, remote_peer_ip = 10.10.1.1, ppp_virtual_interface_id = 1, client_dyna

Mar 15 2026 00:05:35: %ASA-6-622001:

Adding tracked route 0.0.0.0 0.0.0.0 10.10.1.1, distance 1, table default, on interface outside

Mar 15 2026 00:05:35: %ASA-6-603109:

Teardown PPPOE Tunnel, tunnel_id = 4, remote_peer_ip = 172.16.1.1

Mar 15 2026 00:05:40: %ASA-6-622001:

Removing tracked route 172.16.253.0 255.255.255.0 172.16.1.1, distance 1, table default, on interface ou

Mar 15 2026 00:05:40: %ASA-6-317078:

Deleted STATIC route 172.16.253.0 255.255.255.0 via 172.16.1.1 [1/0] on [outside2] [Gi0/1] tableid [0]

5. Packets from PC IP address 192.168.1.2 to 10.10.253.2 and 172.16.253.2 are sent via the **outside** interface (main path), Additionally, due to PAT, capture **capo** shows the egress interface IP address (mapped addresses):

<#root>

Mar 15 2026 00:17:27: %ASA-6-305011:

Built dynamic ICMP translation from inside:192.168.1.2/2685 to outside:10.10.1.10/2685

Mar 15 2026 00:17:29: %ASA-6-305011:

Built dynamic ICMP translation from inside:192.168.1.2/2686 to outside:10.10.1.10/2686

firewall#

show capture

```
capture capo type raw-data interface outside [

Capturing - 912 bytes


]
  match icmp any host 10.10.253.2
  match icmp any host 172.16.253.2
capture capo2 type raw-data interface outside2 [Capturing - 0 bytes]
  match icmp any host 172.16.253.2
  match icmp any host 10.10.253.2

firewall#

show capture  capo



8 packets captured

   1: 00:17:27.680247

10.10.1.10 > 10.10.253.2 icmp: echo request



   2: 00:17:27.688761

10.10.253.2 > 10.10.1.10 icmp: echo reply



   3: 00:17:28.680415       10.10.1.10 > 10.10.253.2 icmp: echo request
   4: 00:17:28.683405       10.10.253.2 > 10.10.1.10 icmp: echo reply
   5: 00:17:29.732673

10.10.1.10 > 172.16.253.2 icmp: echo request



   6: 00:17:29.739799

172.16.253.2 > 10.10.1.10 icmp: echo reply



   7: 00:17:30.732979       10.10.1.10 > 172.16.253.2 icmp: echo request
   8: 00:17:30.736656       172.16.253.2 > 10.10.1.10 icmp: echo reply

8 packets shown
```

Note:

The changes in routing are not applied to existing connections. Therefore, existing connection continue using the “old” path even if a better path becomes available. Effectively, this can cause impact after routing changes. To instruct the firewall to use the new path, consider enabling the floating conn timer. If the floating-conn timeout is enabled, that is set to non-zero value, then if a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. Refer to

the description of **floating-conn** in https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/T-Z/asa-command-ref-T-Z/m_ta-tk.html.

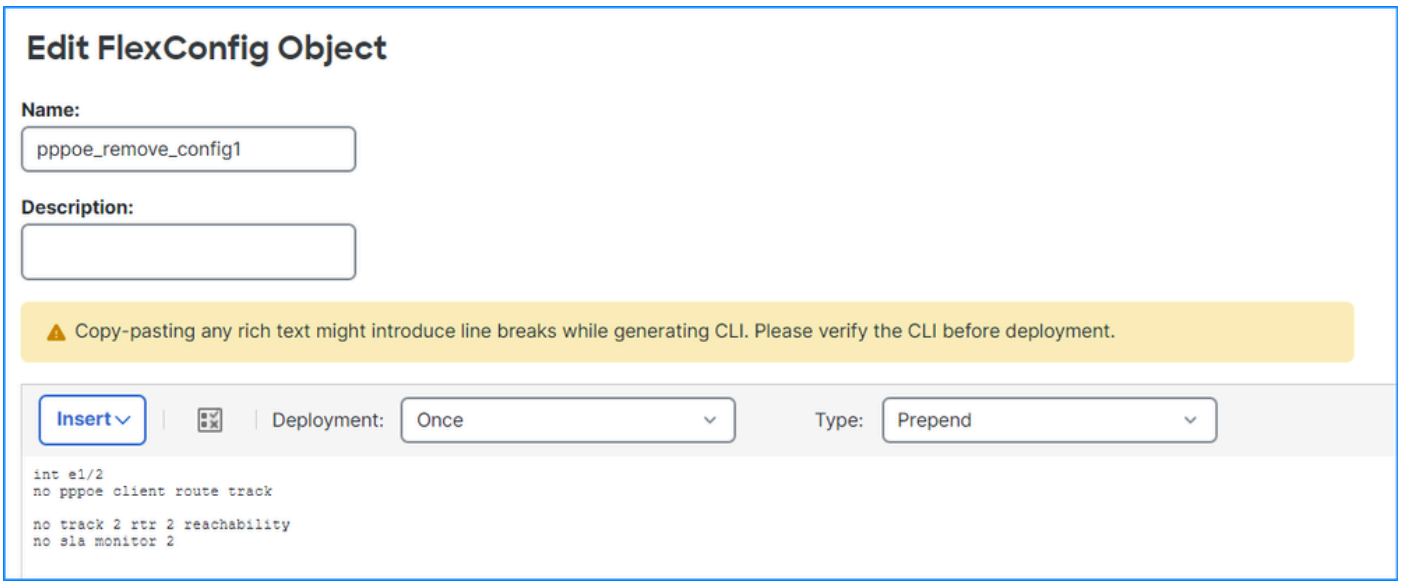
How to Remove or Negate Commands Deployed by Using FlexConfig?

If you want to remove or negate configuration deployed by FlexConfig, then you must perform these steps:

1. Create a FlexConfig with negation commands in this order and ensure setting the **Type** to **Prepend**:

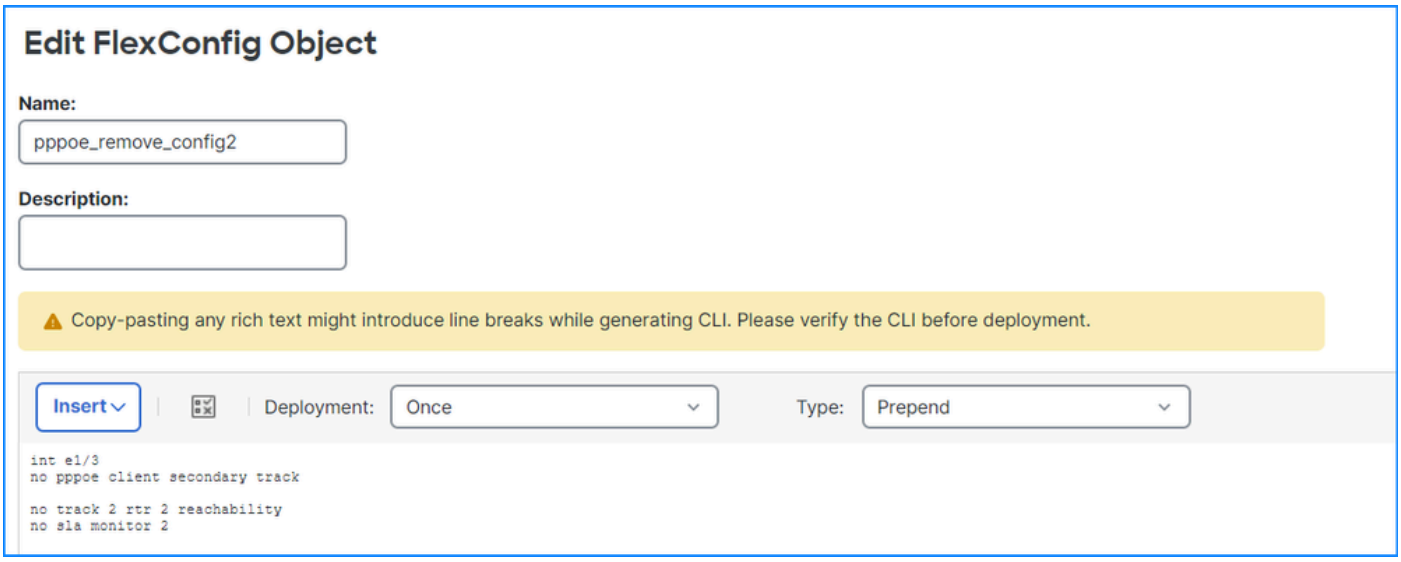
- Removal of reference to track objects
- Deletion of track objects
- Deletion of SLA objects

Example of removal of configuration deployed for the active-active redundancy with load-sharing and PPPoE client route tracking:



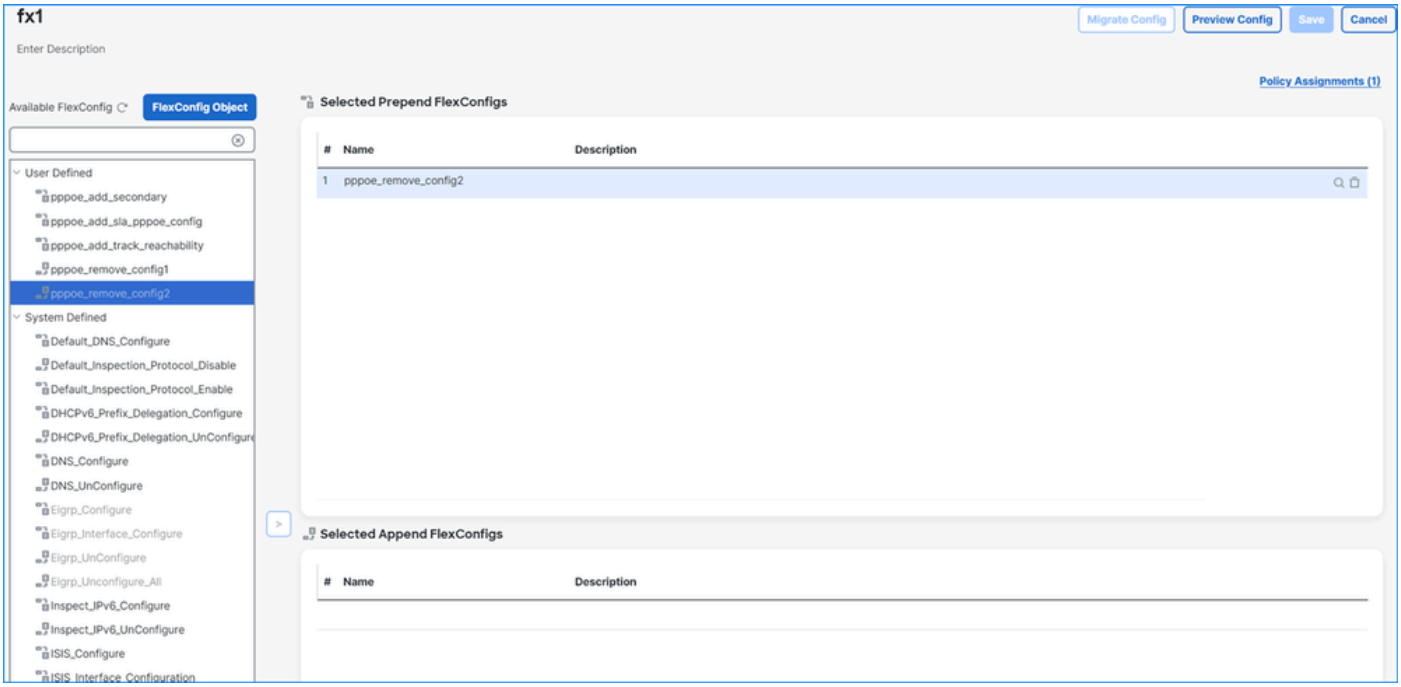
Flexonfig removal 1

Example of removal of configuration deployed for active-standby redundancy without load-sharing:



Flexonfig removal 2

2. Add the negation object created at step 1 to the FlexConfig policy. Ensure the objects for the addition of PPPoE commands are removed and do not exist in the policy:



FlexConfig Removal Policy

3. Deploy policies and verify the removal of commands in the CLI.

4. Remove the negation object created at step 1 from the FlexConfig policy and re-deploy.

References

- Cisco bug ID CSCwt39430 "ENH: Support FTD interface DHCP/PPPoE client configuration commands and subcommands on FMC UI"