Configuration et vérification de la redondance/haute disponibilité PPPoE dans ASA/FTD

Introduction

Ce document décrit la configuration et la vérification de la redondance PPPoE (haute disponibilité ou HA) dans Secure Firewall ASA ou Secure Firewall Threat Defense (FTD).

Conditions préalables

Exigences

Connaissances de base sur les produits.

Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Secure Firewall Threat Defense (FTD) version 10.0.0 géré par Secure Firewall Management Center (FMC) version 10.0.1.
- ASA version 9.24.1.

Informations générales

Le logiciel pare-feu prend en charge la configuration de plusieurs sessions PPPoE. Dans ce document, 2 sessions PPPoE sont prises en compte et la « haute disponibilité » ou la « redondance » sont utilisées de manière interchangeable.

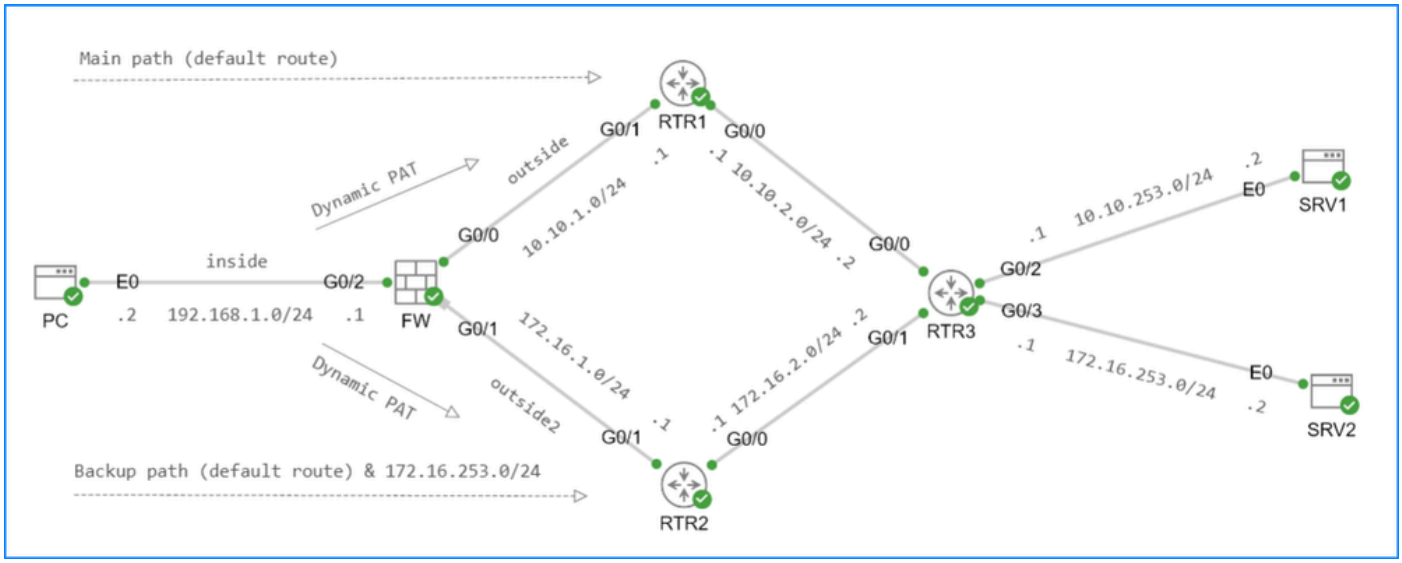
En association avec le contrat de niveau de service (SLA), le suivi et le routage avec le suivi, les utilisateurs peuvent configurer différents modes de redondance :

- Redondance active-active avec partage de charge
- Redondance active-active avec partage de charge et suivi de route client PPPoE
- Redondance active-veille sans partage de charge

Notez que la configuration du routage sur les périphériques homologues ne fait pas partie du champ d'application de cet article.

Redondance active-active avec partage de charge

Reportez-vous à cet exemple de topologie :



Redondance active-active avec partage de charge

Principaux points :

- PPPoE est configuré dans les interfaces externes et externes2 du pare-feu.
- RTR1 et RTR2 sont des serveurs PPPoE.

- Le pare-feu installe la route par défaut via l'interface externe. La route par défaut via l'interface outside2 a une distance de routage plus élevée, c'est-à-dire moins préférable.
- Les routes statiques de partage de charge vers des sous-réseaux spécifiques sont installées via l’interface outside2. Les routes sont suivies. Le suivi est facultatif ; cependant, il assure un basculement plus rapide vers le chemin via l'interface externe en cas de défaillance du chemin via l'interface outside2.
- Par souci de simplicité, la traduction d'adresses de port dynamique (PAT) est configurée via les interfaces outside et outside2.

Configuration ASA

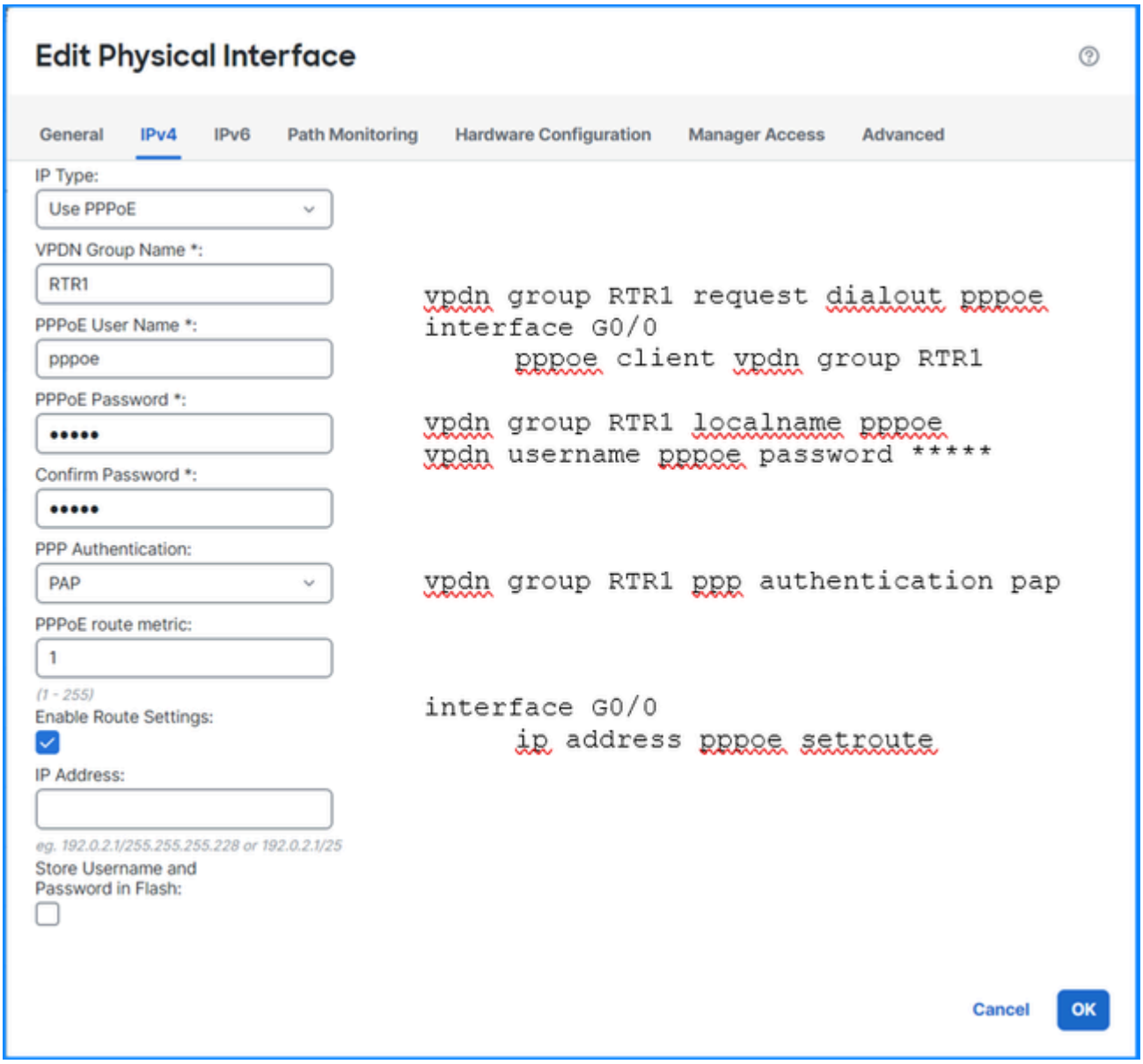
<#root>

```
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
```

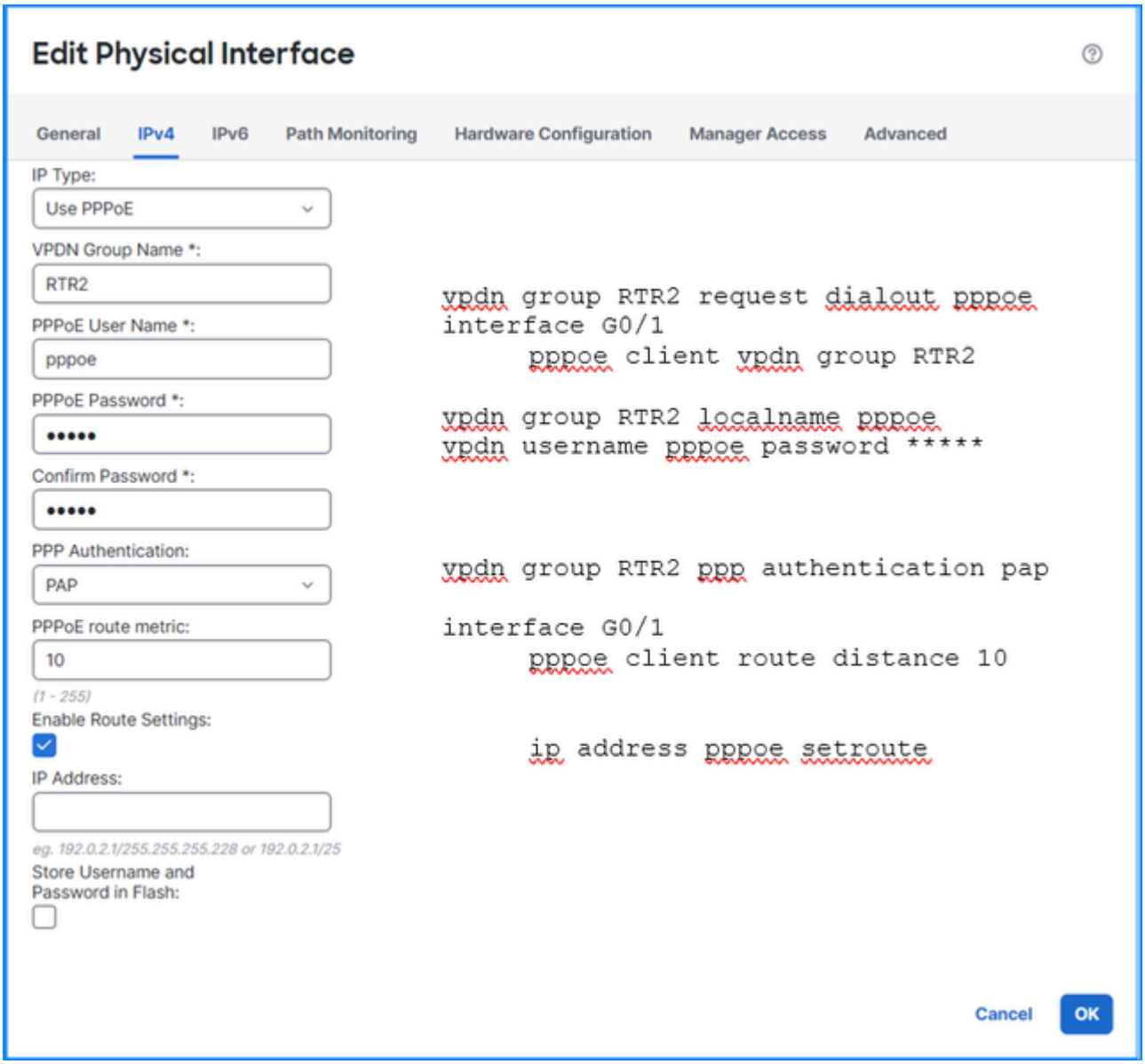
```
nat (inside,outside) source dynamic net-192.168.1.0 interface
nat (inside,outside2) source dynamic net-192.168.1.0 interface


route outside2 172.16.253.0 255.255.255.0 172.16.1.1 1 track 1
```

Configuration FTD

Cette section couvre uniquement la configuration PPPoE spécifique à FTD. Voici la comparaison de la configuration PPPoE des interfaces outside et outside2 sur FTD et des commandes déployées sur le plan de données :

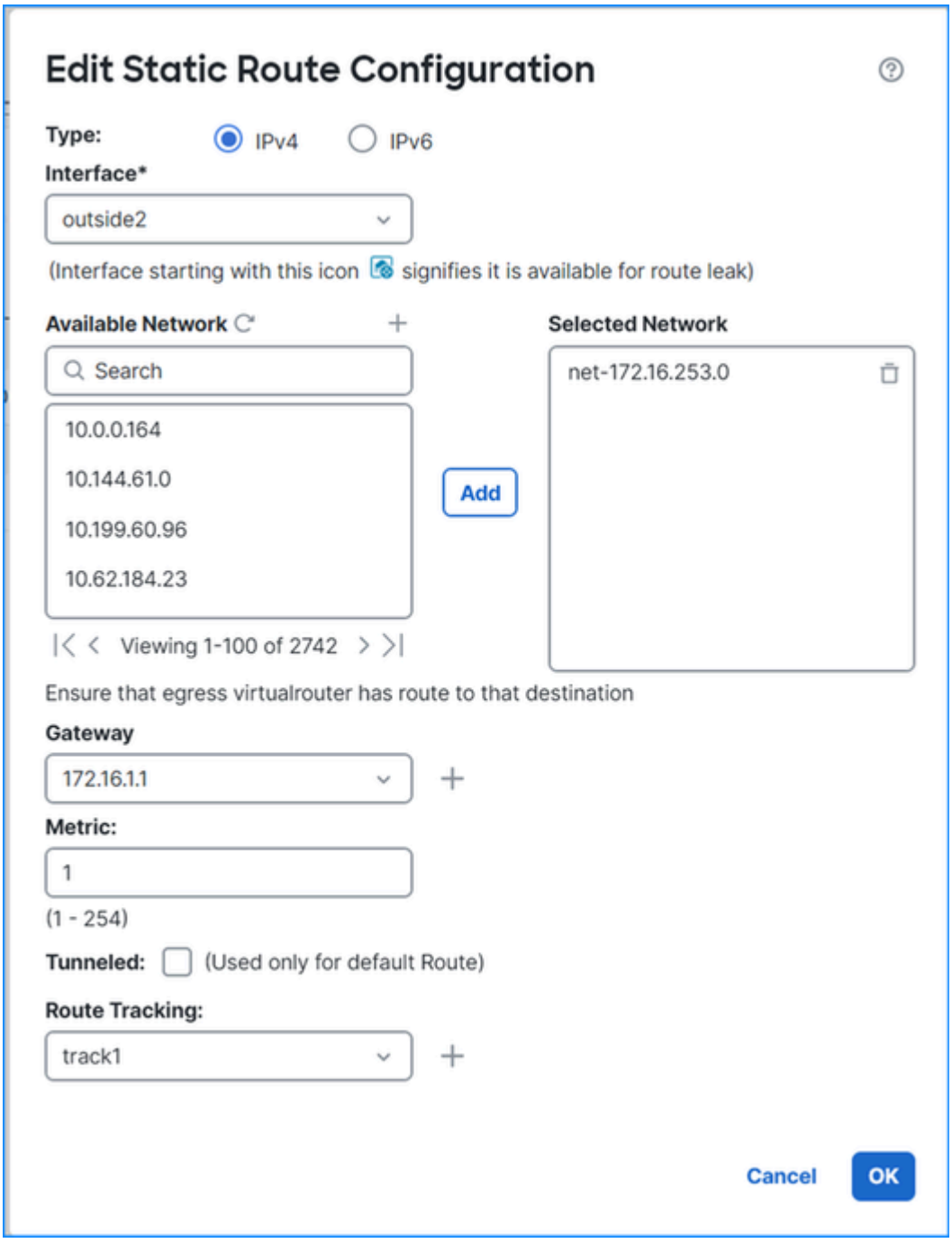


configuration d'interface PPPoE externe sur l'interface FMC



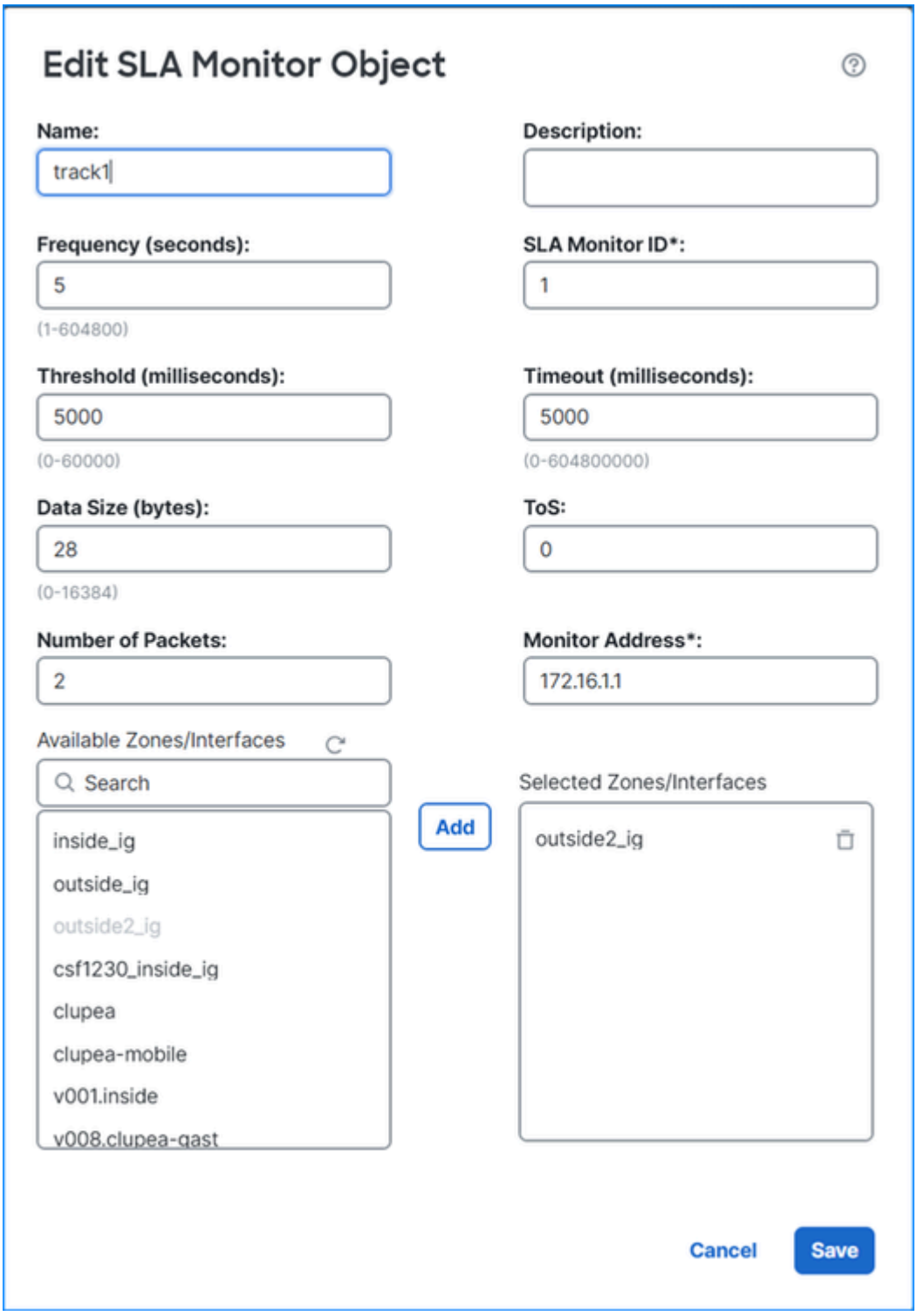
configuration de l'interface PPPoE outside2 sur l'interface FMC

Route statique avec suivi :



Route statique avec suivi

Configuration de l'objet SLA monitor :



Configuration SLA

Principaux points :

- RTR1 et RTR2 sont respectivement 2 groupes VPDN sur les interfaces G0/0 et G0/1.
- Track 1/SLA1 assure le suivi de l'accessibilité à RTR2. L'objet de suivi est utilisé dans la configuration de la route statique via l'interface outside2.
- La commande pppoe client route distance 10 demande au pare-feu d'appliquer la distance administrative de 10 à la route par défaut reçue de RTR2 et donc de la rendre moins

préférable.
- Les routes vers des sous-réseaux spécifiques via l'interface outside2 sont configurées avec le suivi.
- Par conséquent, les deux sessions PPPoE deviennent actives et le trafic provenant du PC est partagé en charge en fonction de la configuration du routage.

Vérification

1. La session PPPoE avec RTR1 via l'interface externe est établie :

<#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

SYSLOG:

<#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. La session PPPoE avec RTR2 via l'interface outside2 est établie :

<#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
```

SYSLOG:

<#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. Les paquets des adresses IP du PC 192.168.1.2 à 10.10.253.2 et 172.16.253.2 sont envoyés. En raison de la PAT, les captures capo et capo2 affichent l'adresse IP de l'interface de sortie (adresses mappées) :

<#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. Simulez une défaillance de liaison distante sur RTR1. Le basculement vers le chemin de secours via l'interface outside2 prend environ 1 minute :

RTR1 :

<#root>

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

Pare-feu

<#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

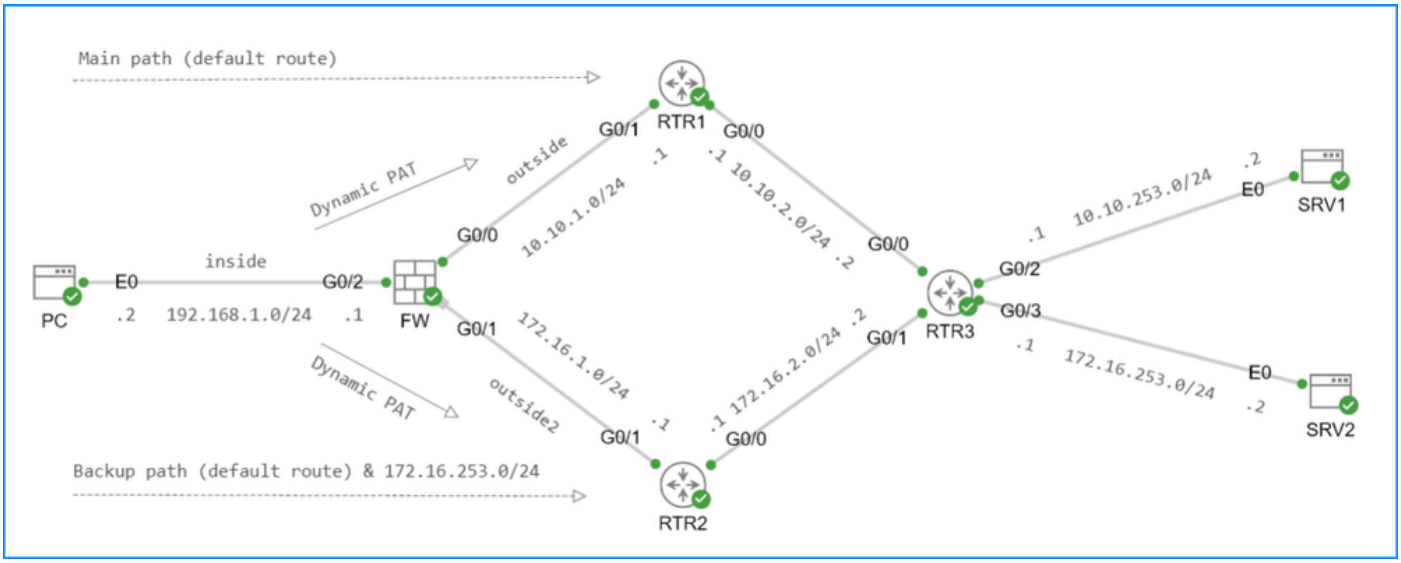
Mar 15 2026 20:44:17: %ASA-7-110006: Add Entry:0.0.0.0/0.0.0.0 nh:172.16.1.1 nh_cnt:1 flags:0 timestamp
Mar 15 2026 20:44:17: %ASA-6-305010: Teardown static translation from outside:0.0.0.0 to inside:0.0.0.0

```
firewall#

show route

…

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

Redondance active-active avec partage de charge et suivi de route client PPPoE

Ce cas est basé sur la redondance active-active avec partage de charge et nécessite en outre le déploiement de la commande supplémentaire track and pppoe client route track x sous l'interface externe à l'aide de FlexConfig.

Reportez-vous à cet exemple de topologie :



Redondance active-active avec partage de charge et suivi de route client PPPoE

Principaux points :

- PPPoE est configuré dans les interfaces externes et externes2 du pare-feu.
- RTR1 et RTR2 sont des serveurs PPPoE.
- En utilisant route-distance, le pare-feu installe la route par défaut via l'interface externe. La

route par défaut via l'interface outside2 a une distance de routage plus élevée et est moins préférable.

- La route par défaut vers RTR1 via l’interface externe est suivie. Elle est facultative. Cependant, en fonction de la fréquence SLA et des valeurs de délai d’attente, elle permet un basculement plus rapide vers le chemin via RTR2.
- Les routes statiques de partage de charge vers des sous-réseaux spécifiques sont installées via l’interface outside2. Les routes sont suivies. Le suivi est facultatif ; cependant, il assure un basculement plus rapide vers le chemin via RTR1.
- Par souci de simplicité, la traduction d'adresses de port dynamique (PAT) est configurée via les interfaces outside et outside2.

Configuration ASA

<#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
```

Configuration FTD

Cette section couvre uniquement la configuration PPPoE spécifique à FTD. Les étapes de configuration sont les mêmes que la configuration FTD dans la section « Redondance active-active avec partage de charge » avec l'ajout du déploiement de la commande pppoe client route track x sous l'interface externe. Étant donné que l'interface utilisateur FMC ne prend pas en charge nativement les pistes pour les options du client, FlexConfig doit être utilisé.

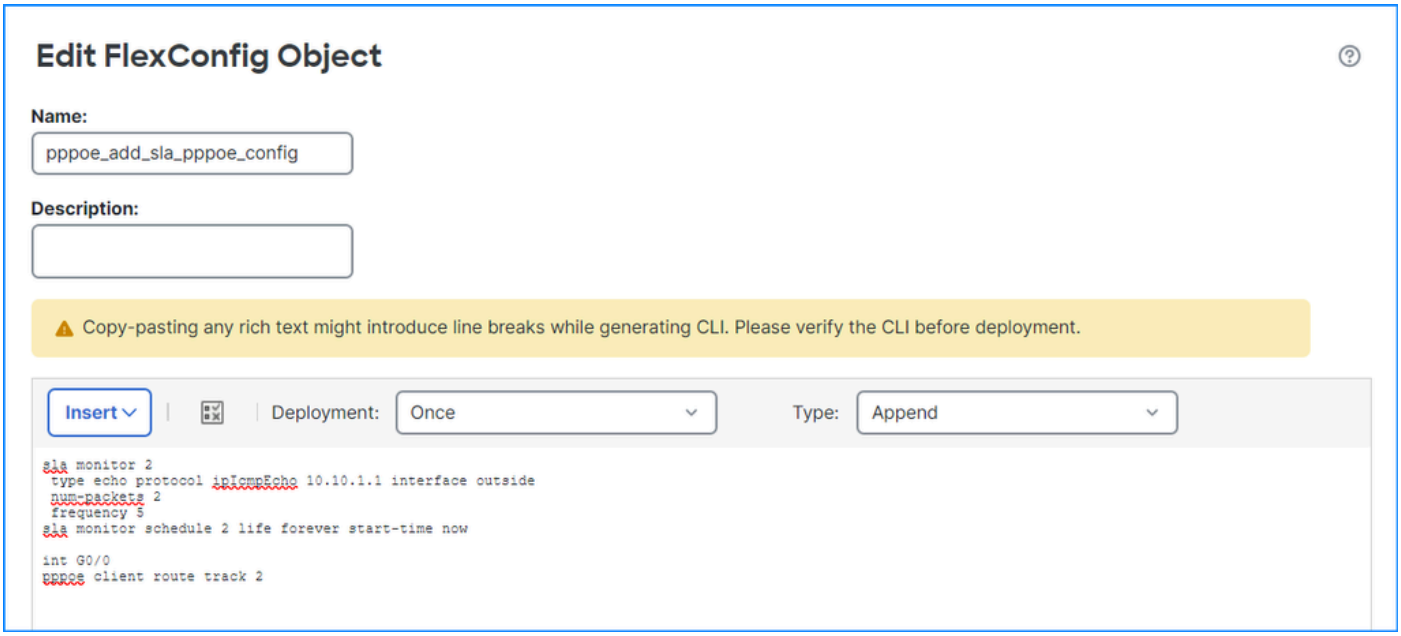
Veillez à tenir compte des points suivants :

1. Les stratégies FlexConfig ne contiennent intentionnellement pas de validation d'entrée étendue. Vous devez vous assurer que les configurations de cette stratégie FlexConfig sont correctes. Des configurations incorrectes entraînent un échec du déploiement qui peut entraîner une interruption du réseau. En outre, pensez à isoler le déploiement de sorte qu'il n'inclue que les modifications FlexConfig et aucune autre mise à jour de stratégie.

2. Pendant le déploiement, FMC supprime toute piste x. déployée par FlexConfig. Pour la persistance, vous devez définir le déploiement de l'objet FlexConfig sur Everytime et le déployer dans un objet FlexConfig distinct.

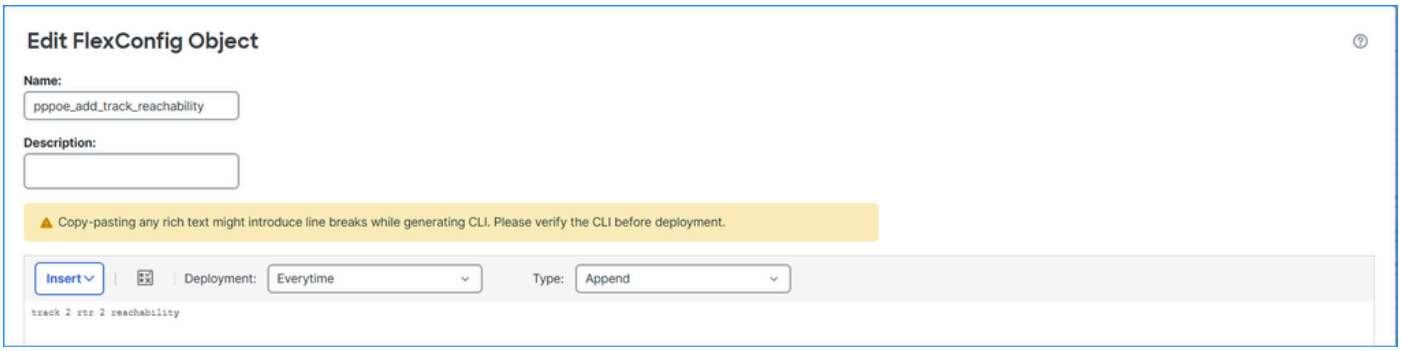
Étapes de configuration FlexConfig

1. Créez un objet FlexConfig pour la configuration des configurations de client SLA et PPPoE pour l'interface externe. Assurez-vous de définir le déploiement sur Une fois et tapez sur Ajouter. Dans cet exemple, la piste 2, SLA 2 sont utilisées. Notez que la commande d'accessibilité track 2 rtr 2 est manquante :



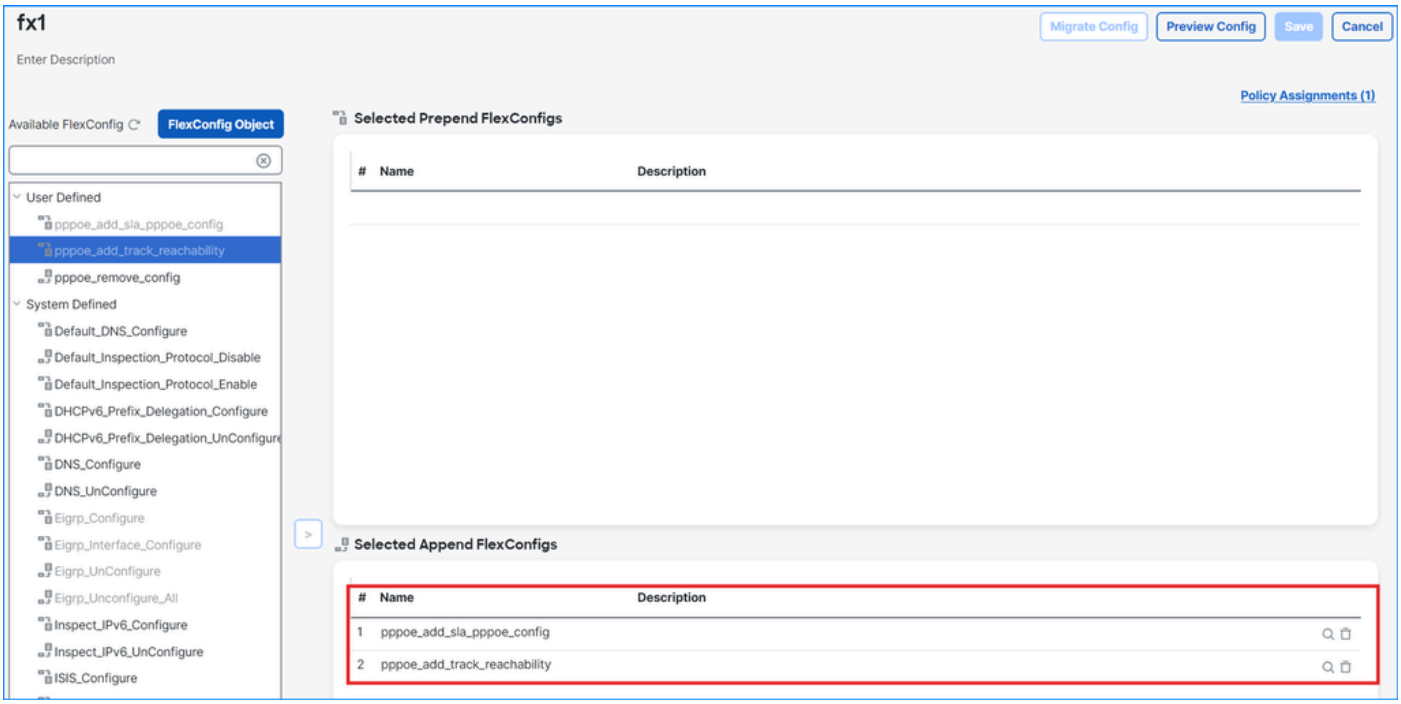
FlexConfig pour SLA

2. Créez un autre objet FlexConfig pour la configuration de la commande track 2 rtr 2 reachability. Assurez-vous de définir Deployment sur Everytime et Type sur Append:



FlexConfig pour piste

3. Ajoutez des objets à la stratégie FlexConfig. Assurez-vous que l'objet avec la commande track 2 rtr 2 reachability en bas (dernière), et déployez les stratégies :



Stratégie FlexConfig

Principaux points :

- RTR1 et RTR2 sont respectivement 2 groupes VPDN sur les interfaces G0/0 et G0/1.
- La commande Track 2/SLA2 suit l'accessibilité à RTR1. La commande pppoe client route track 2 demande au pare-feu d'installer la route par défaut via l'interface externe si la piste 2 est active.
- Track 1/SLA1 assure le suivi de l'accessibilité à RTR2. L'objet de suivi est utilisé dans la configuration de la route statique via l'interface outside2.
- La commande pppoe client route distance 10 demande au pare-feu d'appliquer la distance administrative de 10 à la route par défaut reçue de RTR2 et donc de la rendre moins préférable.
- Les routes vers des sous-réseaux spécifiques via l'interface outside2 sont configurées avec le suivi.
- Par conséquent, les deux sessions PPPoE deviennent actives et le trafic provenant du PC est partagé en charge en fonction de la configuration du routage.

Vérification

1. La session PPPoE avec RTR1 via l'interface externe est établie :

<#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
```

SYSLOG:

<#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. La session PPPoE avec RTR2 via l'interface outside2 est établie :

<#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

SYSLOG:

<#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. Les paquets des adresses IP du PC 192.168.1.2 à 10.10.253.2 et 172.16.253.2 sont envoyés. En raison de la PAT, les captures capo et capo2 affichent l'adresse IP de l'interface de sortie (adresses mappées) :

<#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. Simulez une défaillance de liaison distante sur RTR1. Le basculement vers le chemin de secours via l'interface outside2 dépend des minuteurs de track1 :

RTR1 :

<#root>

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

Pare-feu

<#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

Remarque :

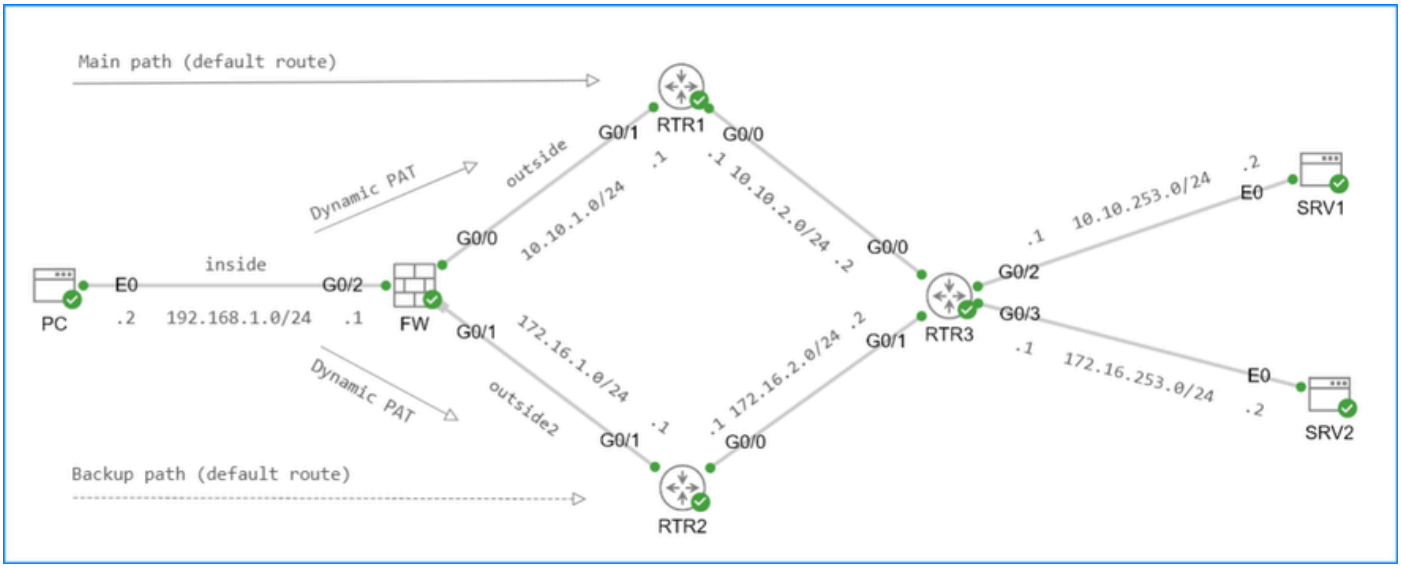
Les modifications apportées au routage ne sont pas appliquées aux connexions existantes. Par conséquent, la connexion existante continue à utiliser l'« ancien » chemin même si un meilleur chemin devient disponible. En effet, cela peut avoir un impact après les modifications de routage. Pour demander au pare-feu d'utiliser le nouveau chemin, pensez à activer le minuteur de conn flottant. Si le délai d'attente de connexion flottante est activé et est défini sur une valeur non nulle, alors si une meilleure route devient disponible, alors ce délai d'attente permet de fermer les connexions afin qu'une connexion puisse être rétablie pour utiliser la meilleure route. Reportez-vous à la description de flottante-conn dans 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.

Redondance active-veille sans partage de charge

Dans ce cas, une seule session PPPoE est active, l'autre est inactive jusqu'à ce que la piste de la session active soit désactivée.

La commande pppoe client secondary track x est utilisée pour l'interface outside2 (backup).

Reportez-vous à cet exemple de topologie :



Topologie de secours active

Principaux points :

- PPPoE est configuré dans les interfaces G0/0 et G0/1 du pare-feu.
- RTR1 et RTR2 sont des serveurs PPPoE.
- À l'aide de route-distance, le pare-feu installe la route par défaut vers RTR1 via l'interface externe. La route par défaut vers RTR2 présente une distance de routage plus élevée et est

moins préférable.

- La route par défaut vers RTR1 via l’interface externe est suivie. Elle est facultative, mais elle permet un basculement plus rapide vers le chemin via RTR2.
- La session PPPoE vers RTR2 via l'interface outside2 est établie uniquement si la piste utilisée pour la route par défaut vers RTR1 via l'interface externe est inactive.
- À un moment donné, seule une session PPPoE est active.
- Par souci de simplicité, la traduction d'adresses de port dynamique (PAT) est configurée via les interfaces outside et outside2.

Configuration ASA

<#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
```

Configuration FTD

Cette section couvre la configuration de la commande pppoe client secondary track x pour l'interface outside2 (backup). Étant donné que l'interface utilisateur FMC ne prend pas en charge nativement les pistes pour les options du client, FlexConfig doit être utilisé.

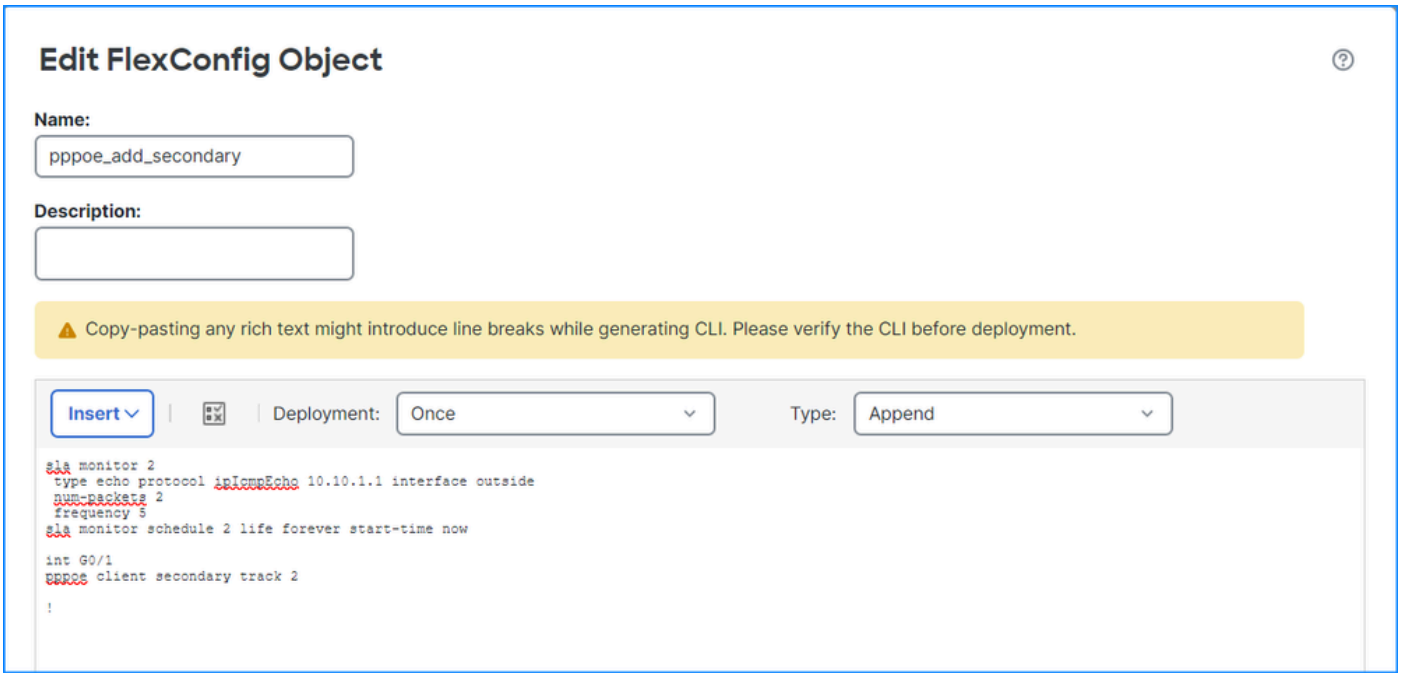
Vous devez vous assurer de configurer le reste de la configuration, y compris la configuration PPPoE, le routage et autres.

Veillez à tenir compte des points suivants :

1. Les stratégies FlexConfig ne contiennent pas intentionnellement de validation d'entrée étendue. Vous devez vous assurer que les configurations de cette stratégie FlexConfig sont correctes. Des configurations incorrectes entraînent un échec du déploiement qui peut entraîner une interruption du réseau. En outre, pensez à isoler le déploiement de sorte qu'il n'inclue que les modifications FlexConfig et aucune autre mise à jour de stratégie.
2. Pendant le déploiement, FMC supprime toute piste x. déployée par FlexConfig. Pour la persistance, vous devez définir le déploiement de l'objet FlexConfig sur Everytime et le déployer dans un objet FlexConfig distinct.

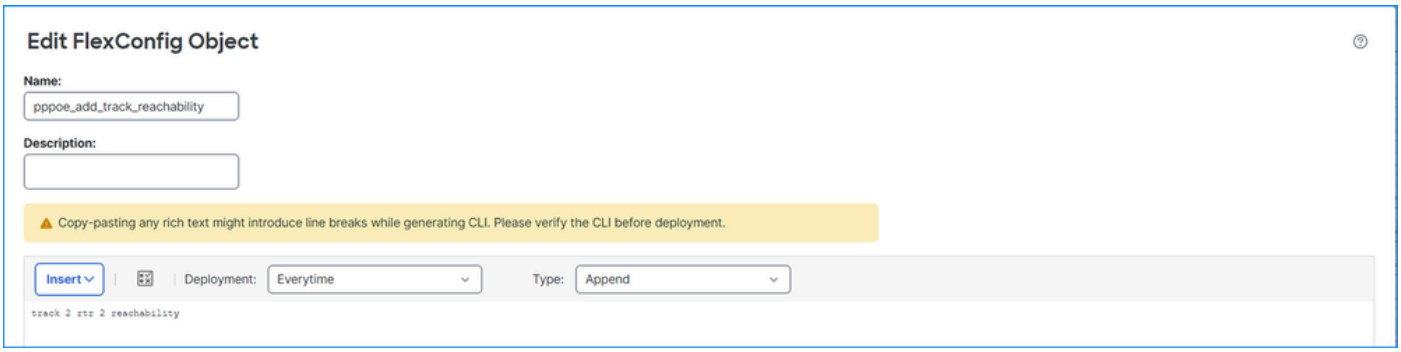
Étapes de configuration FlexConfig

1. Créez un objet FlexConfig pour la configuration des configurations de client SLA et PPPoE pour l'interface outside2 (backup). Assurez-vous de définir Deployment sur Once et Type sur Append. Dans cet exemple, le suivi 2, SLA 2 sont utilisés. Notez que la commande track 2 rtr 2 reachability est manquante :



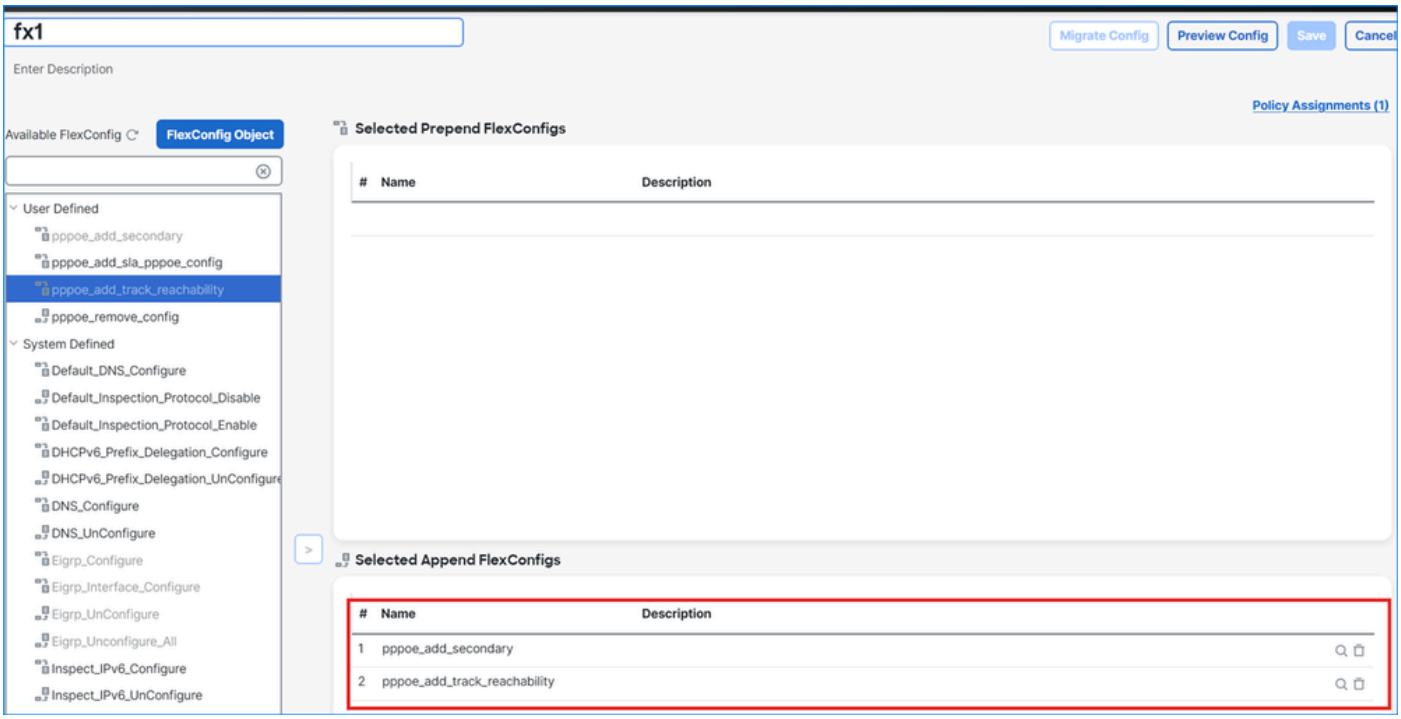
FlexConfig pour SLA

2. Créez un autre objet FlexConfig pour la configuration de la commande track 2 rtr 2 reachability. Assurez-vous de définir Deployment sur Everytime et Type sur Append:



FlexConfig pour piste

3. Ajoutez des objets à la stratégie FlexConfig. Assurez-vous que l'objet avec la commande track 2 rtr 2 reachability en bas (dernière), et déployez les stratégies :



Stratégie FlexConfig

Principaux points :

- La commande pppoe client secondary track 2 sous l'interface G0/1 demande au pare-feu d'activer la session PPPoE via l'interface G0/1 uniquement si la piste 2 échoue. En effet, la défaillance de la piste 2 qui suit l'accessibilité via le chemin principal active le chemin de secours.
- Par conséquent, seule une session PPPoE est active à un moment donné.

Vérification

1. La session PPPoE avec RTR1 via l'interface externe est déjà établie. La session de sauvegarde est inactive :

<#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. La session PPPoE vers RTR1 via l'interface externe échoue (par exemple, en raison d'une défaillance de l'interface physique ou de la liaison). La session PPPoE vers RTR2 via l'interface outside2 est établie.

SYSLOG:

<#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. Les paquets des adresses IP du PC 192.168.1.2 à 10.10.253.2 et 172.16.253.2 sont envoyés. En raison d’une défaillance du chemin principal, tous les paquets sont envoyés via l’interface outside2. En outre, en raison de la PAT, capture capo2 affiche l'adresse IP de l'interface de sortie (adresses mappées) :

<#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. Le chemin via l'interface externe est restauré, la session PPPoE vers RTR1 est rétablie. La session via l'interface outside2 passe à l'état de réutilisation en attente :

<#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
```

SYSLOG:

<#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. Les paquets provenant des adresses IP de PC 192.168.1.2 à 10.10.253.2 et 172.16.253.2 sont envoyés via l'interface externe (chemin principal). En outre, en raison de la PAT, capture capo affiche l'adresse IP de l'interface de sortie (adresses mappées) :

<#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
```

Remarque :

Les modifications apportées au routage ne sont pas appliquées aux connexions existantes. Par conséquent, la connexion existante continue à utiliser l'« ancien » chemin même si un meilleur chemin devient disponible. En effet, cela peut avoir un impact après les modifications de routage. Pour demander au pare-feu d'utiliser le nouveau chemin, pensez à activer le minuteur de conn flottant. Si le délai d'attente de connexion flottante est activé, c'est-à-dire défini sur une valeur non nulle, alors si une meilleure route devient disponible, alors ce délai d'attente permet aux connexions d'être fermées afin qu'une connexion puisse être rétablie pour utiliser la meilleure route. Reportez-vous à la description de flottante-conn dans 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.

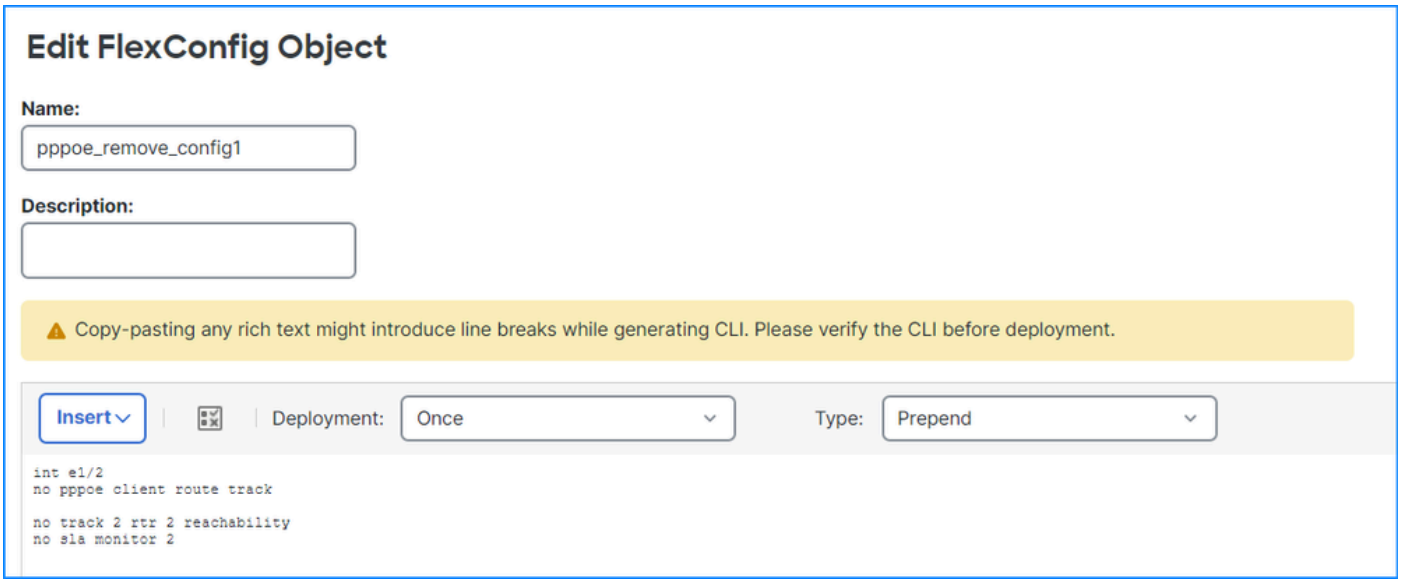
Comment supprimer ou annuler des commandes déployées à l'aide de FlexConfig ?

Si vous souhaitez supprimer ou annuler la configuration déployée par FlexConfig, vous devez effectuer les étapes suivantes :

1. Créez un FlexConfig avec des commandes de négation dans cet ordre et assurez-vous de définir le Type sur Prepend :

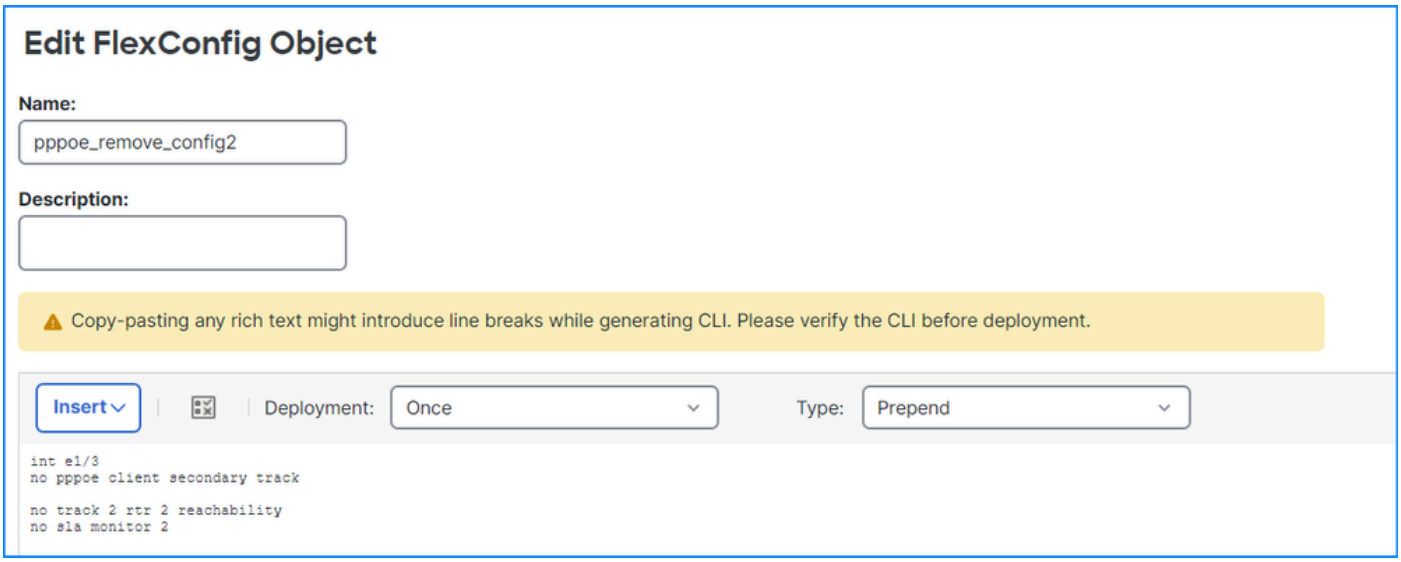
- Suppression de la référence aux objets de piste
- Suppression d'objets de piste
- Suppression d’objets SLA

Exemple de suppression de la configuration déployée pour la redondance active-active avec partage de charge et suivi de route du client PPPoE :



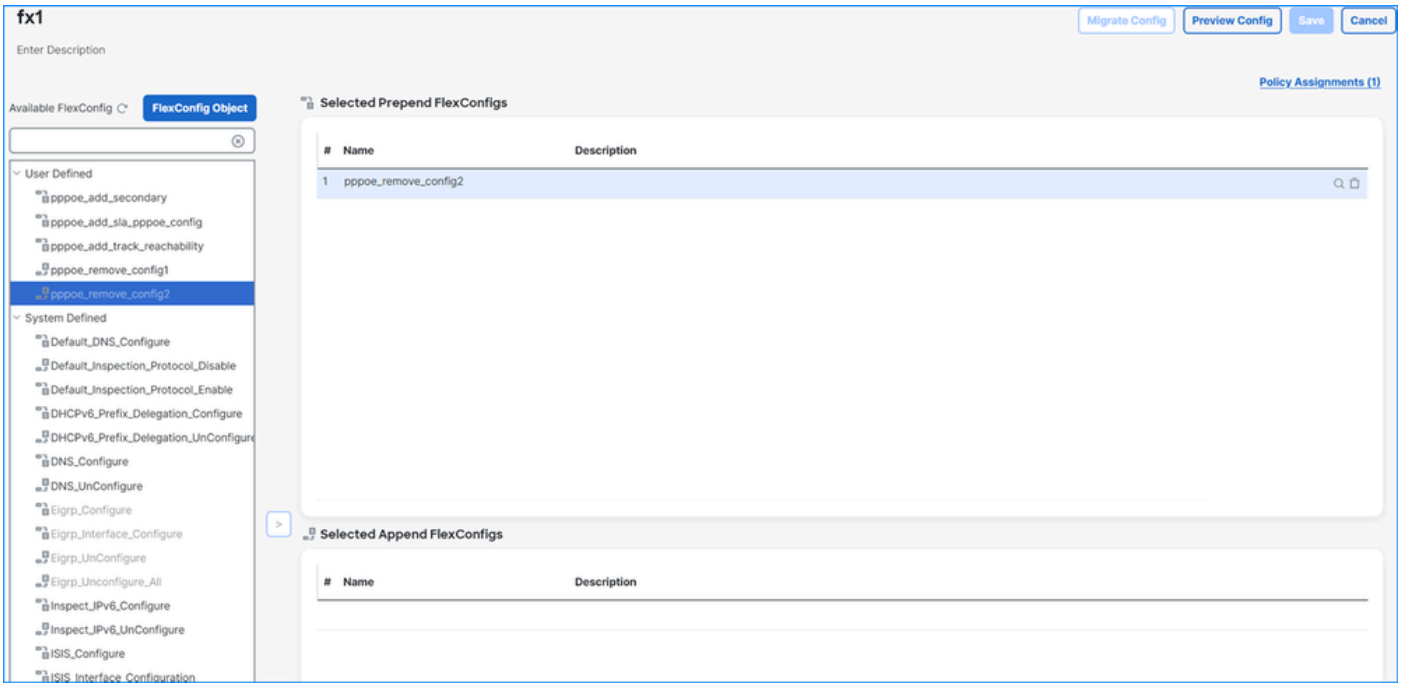
Enlèvement de flexonfig 1

Exemple de suppression de la configuration déployée pour la redondance active-veille sans partage de charge :



Retrait de Flexonfig 2

2. Ajoutez l'objet de négation créé à l'étape 1 à la stratégie FlexConfig. Assurez-vous que les objets pour l'ajout de commandes PPPoE sont supprimés et n'existent pas dans la stratégie :



Politique de suppression FlexConfig

3. Déployez des stratégies et vérifiez la suppression des commandes dans l'interface de ligne de commande.

4. Supprimez l'objet de négation créé à l'étape 1 de la stratégie FlexConfig et redéployez-le.

Références

- ID de bogue Cisco CSCwt39430 "ENH : Prise en charge des commandes et sous-commandes de configuration client DHCP/PPPoE de l'interface FTD sur l'interface FMC

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.