

Konfiguration und Überprüfung der PPPoE-Redundanz/Hochverfügbarkeit in ASA/FTD

Einleitung

Dieses Dokument beschreibt die Konfiguration und Verifizierung der PPPoE-Redundanz (hohe Verfügbarkeit oder HA) in Secure Firewall ASA oder Secure Firewall Threat Defense (FTD).

Voraussetzungen

Anforderungen

Grundlegendes Produktwissen.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Secure Firewall Threat Defense (FTD) Version 10.0.0, verwaltet vom Secure Firewall Management Center (FMC) Version 10.0.1.
- ASA Version 9.24.1.

Hintergrundinformationen

Die Firewall-Software unterstützt die Konfiguration mehrerer PPPoE-Sitzungen. In diesem Dokument werden 2 PPPoE-Sitzungen berücksichtigt, und "HA" oder "Redundanz" werden synonym verwendet.

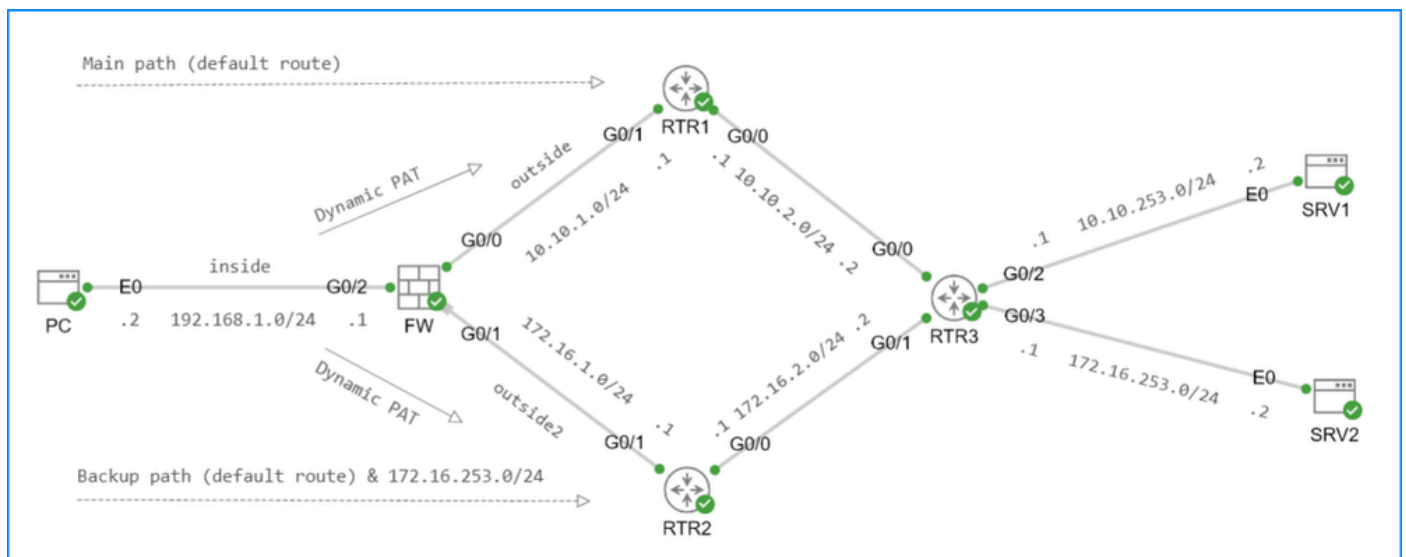
In Kombination mit dem Service Layer Agreement (SLA) können Benutzer durch Nachverfolgung, Nachverfolgung und Routing unterschiedliche Redundanzmodi konfigurieren:

- Aktiv-Aktiv-Redundanz mit Lastverteilung
- Aktiv-Aktiv-Redundanz mit Lastverteilung und PPPoE-Client-Routenverfolgung
- Aktiv/Standby-Redundanz ohne Lastverteilung

Beachten Sie, dass die Konfiguration des Routings auf Peer-Geräten nicht in diesem Artikel behandelt wird.

Aktiv-Aktiv-Redundanz mit Lastverteilung

Weitere Informationen finden Sie in der folgenden Beispieltopologie:



Aktiv-Aktiv-Redundanz mit Lastverteilung

Wichtigste Punkte:

- PPPoE wird in der Firewall außerhalb und innerhalb von 2 Schnittstellen konfiguriert.
- RTR1 und RTR2 sind PPPoE-Server.
- Die Firewall installiert die Standardroute über die externe Schnittstelle. Die Standardroute über die outside2-Schnittstelle hat eine höhere Routing-Distanz, was weniger bevorzugt ist.
- Die zur Lastverteilung verwendeten statischen Routen zu bestimmten Subnetzen werden über die outside2-Schnittstelle installiert. Die Routen werden nachverfolgt. Die

Nachverfolgung ist optional. Falls jedoch der Pfad über die outside2-Schnittstelle ausfällt, wird ein schnelleres Failover auf den Pfad über die externe Schnittstelle ermöglicht.

- Der Einfachheit halber wird die dynamische Port-Adressumwandlung (PAT) über die Außen- und Außen-2-Schnittstellen konfiguriert.

ASA-Konfiguration

```
<#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-Konfiguration

In diesem Abschnitt wird nur die FTD-spezifische PPPoE-Konfiguration behandelt. Dies ist der Vergleich der PPPoE-Konfiguration der Außen- und der Außen-2-Schnittstellen auf FTD mit den auf der Datenebene bereitgestellten Befehlen:

Edit Physical Interface

General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:
Use PPPoE

VPDN Group Name *:
RTR1

PPPoE User Name *:
pppoe

PPPoE Password *:

Confirm Password *:

PPP Authentication:
PAP

PPPoE route metric:
1

(1 - 255)

Enable Route Settings:

IP Address:

eg. 192.0.2.1/255.255.255.228 or 192.0.2.1/25

Store Username and Password in Flash:

```
vpdn group RTR1 request dialout pppoe
interface G0/0
    pppoe client vpdn group RTR1

vpdn group RTR1 localname pppoe
vpdn username pppoe password *****

vpdn group RTR1 ppp authentication pap

interface G0/0
    ip address pppoe setroute
```

Cancel **OK**

Konfiguration der externen PPPoE-Schnittstelle auf der FMC-Benutzeroberfläche

Edit Physical Interface ?

General **IPv4** IPv6 Path Monitoring Hardware Configuration Manager Access Advanced

IP Type:

VPDN Group Name *:

PPPoE User Name *:

PPPoE Password *:

Confirm Password *:

PPP Authentication:

PPPoE route metric:

(1 - 255)

Enable Route Settings:

IP Address:

eg. 192.0.2.1/255.255.255.228 or 192.0.2.1/25

Store Username and Password in Flash:

```

vpdn group RTR2 request dialout pppoe
interface G0/1
    pppoe client vpdn group RTR2

vpdn group RTR2 localname pppoe
vpdn username pppoe password *****

vpdn group RTR2 ppp authentication pap

interface G0/1
    pppoe client route distance 10

ip address pppoe setroute
  
```

Cancel **OK**

outside2 PPPoE-Schnittstellenkonfiguration auf der FMC-Benutzeroberfläche

Statische Route mit Nachverfolgung:

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*

outside2

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

10.0.0.164
10.144.61.0
10.199.60.96
10.62.184.23

Add

Selected Network

net-172.16.253.0 

|< < Viewing 1-100 of 2742 > >|

Ensure that egress virtualrouter has route to that destination

Gateway

172.16.1.1 +

Metric:

1

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

track1 +

Cancel

OK

Statische Route mit Nachverfolgung

Konfiguration des SLA-Überwachungsobjekts:

Edit SLA Monitor Object ?

Name: <input type="text" value="track1"/>	Description: <input type="text"/>
Frequency (seconds): <input type="text" value="5"/> <small>(1-604800)</small>	SLA Monitor ID*: <input type="text" value="1"/>
Threshold (milliseconds): <input type="text" value="5000"/> <small>(0-60000)</small>	Timeout (milliseconds): <input type="text" value="5000"/> <small>(0-604800000)</small>
Data Size (bytes): <input type="text" value="28"/> <small>(0-16384)</small>	ToS: <input type="text" value="0"/>
Number of Packets: <input type="text" value="2"/>	Monitor Address*: <input type="text" value="172.16.1.1"/>

Available Zones/Interfaces ↻

- inside_ig
- outside_ig
- outside2_ig
- csf1230_inside_ig
- clupea
- clupea-mobile
- v001.inside
- v008.clupea-gast

Add

Selected Zones/Interfaces

- outside2_ig ✕

Cancel
Save

SLA-Konfiguration

Wichtigste Punkte:

- RTR1 und RTR2 sind zwei VPDN-Gruppen an G0/0- bzw. G0/1-Schnittstellen.
- Track 1/SLA1 verfolgt die Erreichbarkeit zu RTR2. Das Track-Objekt wird in der statischen Routenkonfiguration über die outside2-Schnittstelle verwendet.
- Der Befehl `ppoe client route distanz 10` weist die Firewall an, die administrative Distanz von 10 auf die von RTR2 empfangene Standardroute anzuwenden und diese somit weniger

vorzuziehen.

- Routen zu bestimmten Subnetzen über die outside2-Schnittstelle werden mit Tracking konfiguriert.
- Dies führt dazu, dass beide PPPoE-Sitzungen aktiv werden und der Datenverkehr vom PC abhängig von der Routing-Konfiguration zur Lastverteilung beiträgt.

Verifizierung

1. PPPoE-Sitzung mit RTR1 über die externe Schnittstelle wird aufgebaut:

```
<#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_dyn

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-Sitzung mit RTR2 über die outside2-Schnittstelle wird aufgebaut:

<#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:0.0.0.0.  
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. Pakete von der PC-IP-Adresse 192.168.1.2 bis 10.10.253.2 und 172.16.253.2 werden gesendet. Aufgrund von PAT zeigen die Aufnahmen capo und capo2 die IP-Adresse der Ausgangsschnittstelle (zugeordnete Adressen) an:

```
<#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. Simulieren Sie den Ausfall einer Remote-Verbindung auf RTR1. Das Failover auf den Backup-Pfad über die outside2-Schnittstelle dauert ca. 1 Minute:

RTR1:

<#root>

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

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
```

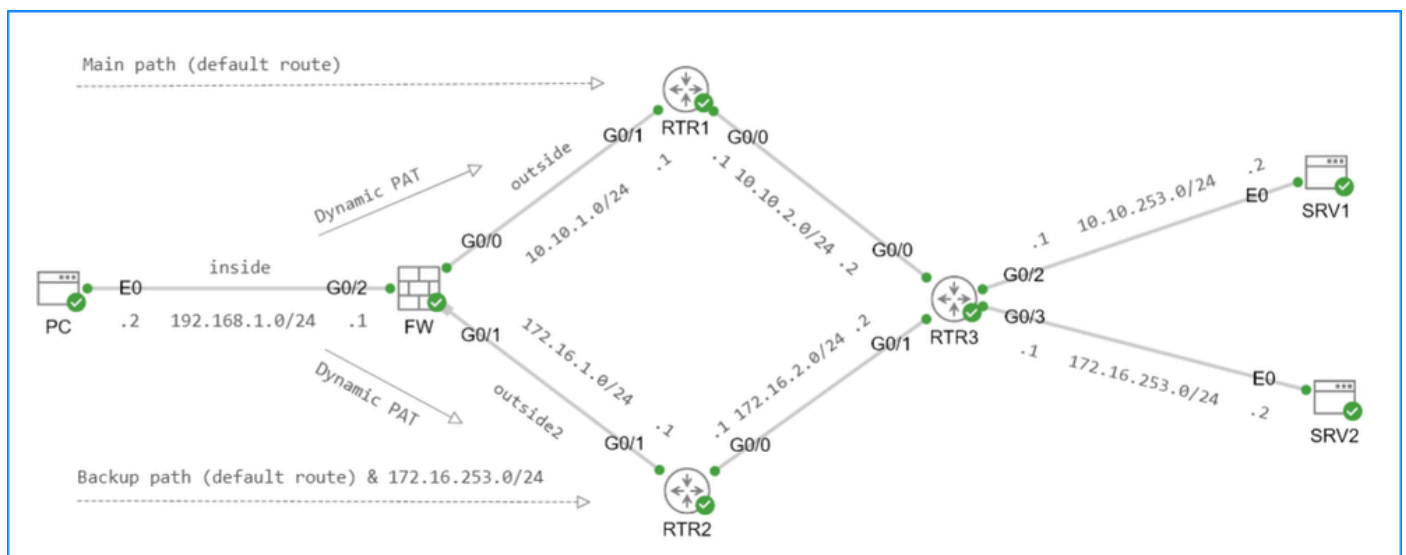
```
...
```

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

Aktiv-Aktiv-Redundanz mit Lastverteilung und PPPoE-Client-Routenverfolgung

Dieser Fall basiert auf der Aktiv-Aktiv-Redundanz mit Lastverteilung und erfordert zusätzlich die Bereitstellung des zusätzlichen Befehls `track` und `pppoe client route track x` unter der externen Schnittstelle mithilfe von FlexConfig.

Weitere Informationen finden Sie in der folgenden Beispieltopologie:



Aktiv-Aktiv-Redundanz mit Lastverteilung und PPPoE-Client-Routenverfolgung

Wichtigste Punkte:

- PPPoE wird in der Firewall außerhalb und außerhalb von 2 Schnittstellen konfiguriert.
- RTR1 und RTR2 sind PPPoE-Server.
- Die Firewall installiert die Standardroute über die externe Schnittstelle unter Verwendung

von route-distanz. Die Standardroute über die outside2-Schnittstelle hat eine höhere Routing-Distanz und ist weniger bevorzugt.

- Die Standardroute zu RTR1 über die externe Schnittstelle wird nachverfolgt. Er ist optional. Je nach SLA-Frequenz und Timeout-Werten kann er jedoch ein schnelleres Failover auf den Pfad über RTR2 bereitstellen.
- Die zur Lastverteilung verwendeten statischen Routen zu bestimmten Subnetzen werden über die outside2-Schnittstelle installiert. Die Routen werden nachverfolgt. Die Nachverfolgung ist optional. Es ermöglicht jedoch ein schnelleres Failover auf den Pfad über RTR1.
- Der Einfachheit halber wird die dynamische Port-Adressumwandlung (PAT) über die Außen- und Außen-2-Schnittstellen konfiguriert.

ASA-Konfiguration

```
<#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-Konfiguration

In diesem Abschnitt wird nur die FTD-spezifische PPPoE-Konfiguration behandelt. Die Konfigurationsschritte entsprechen der FTD-Konfiguration im Abschnitt "Aktiv-Aktiv-Redundanz mit Lastverteilung". Außerdem wird der Befehl `pppoe client route track x` unter der externen Schnittstelle bereitgestellt. Da die FMC-Benutzeroberfläche keine Tracks für die Client-Optionen unterstützt, muss FlexConfig verwendet werden.

Achten Sie auf folgende Punkte:

1. FlexConfig-Richtlinien enthalten absichtlich keine umfassende Eingabevalidierung. Sie müssen sicherstellen, dass die Konfigurationen in dieser FlexConfig-Richtlinie korrekt sind. Falsche Konfigurationen führen zu einer fehlerhaften Bereitstellung, die zu einer Netzwerkunterbrechung führen kann. Sie sollten die Bereitstellung auch isolieren, damit sie nur FlexConfig-Änderungen und keine anderen Richtlinienaktualisierungen umfasst.
2. Während der Bereitstellung entfernt FMC alle Spuren von FlexConfig. Um die Persistenz sicherzustellen, müssen Sie die Bereitstellung des FlexConfig-Objekts auf Everytime festlegen und in einem separaten FlexConfig-Objekt bereitstellen.

Konfigurationsschritte bei FlexConfig

1. Erstellen Sie ein FlexConfig-Objekt für die Konfiguration von SLA- und PPPoE-Client-Konfigurationen für die externe Schnittstelle. Stellen Sie sicher, dass die Bereitstellung auf Einmal und Typ auf Anfügen festgelegt wird. In diesem Beispiel werden Track 2, SLA 2 verwendet. Beachten Sie, dass der Befehl zur Erreichbarkeit von Track 2 rtr 2 fehlt:

Edit FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Deployment: | Type:

```
sla monitor 2
type echo protocol icmpEcho 10.10.1.1 interface outside
num-packets 2
frequency 5
sla monitor schedule 2 life forever start-time now
int G0/0
pppoe client route track 2
```

FlexConfig für SLA

2. Erstellen Sie ein weiteres FlexConfig-Objekt für die Konfiguration des Befehls track 2 rtr 2 reachability. Stellen Sie sicher, dass die Bereitstellung auf Jederzeit und Typ festgelegt ist, an den angehängt werden soll:

Edit FlexConfig Object

Name:

Description:

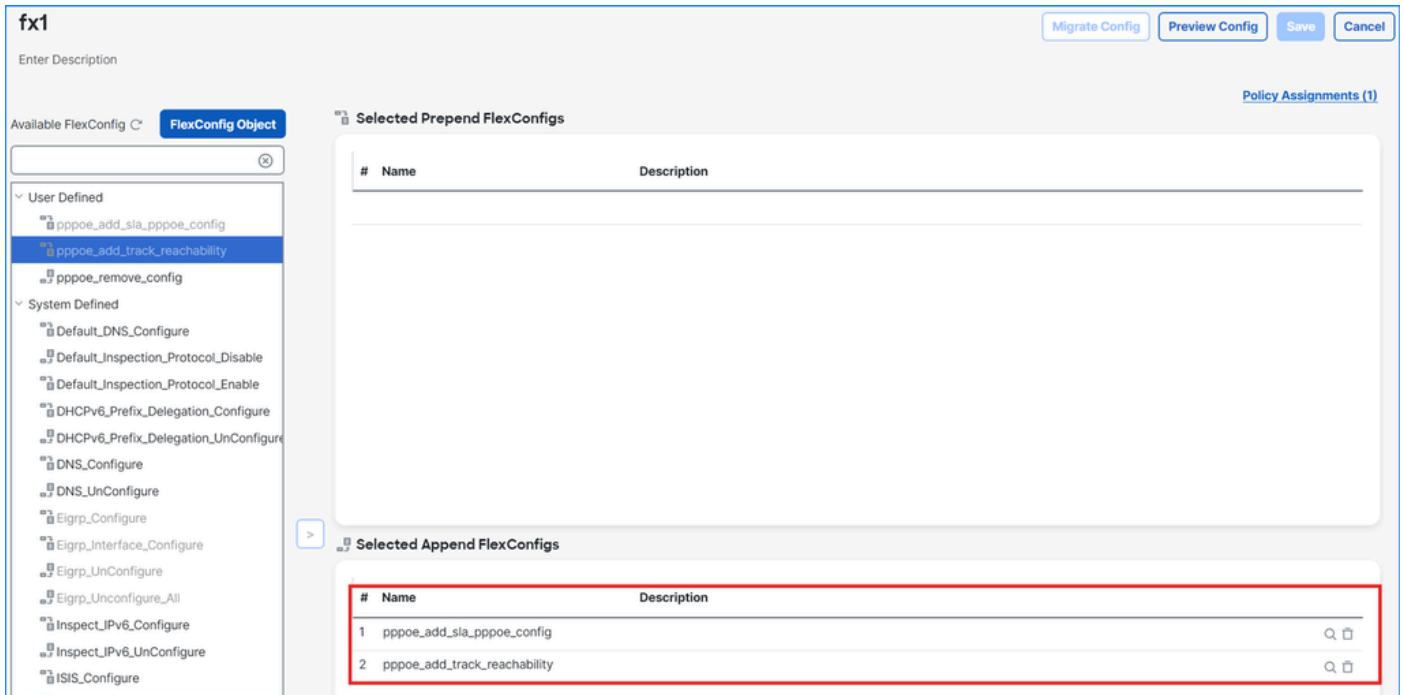
⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Deployment: | Type:

```
track 2 rtr 2 reachability
```

FlexConfig für Track

3. Fügen Sie der FlexConfig-Richtlinie Objekte hinzu. Stellen Sie sicher, dass das Objekt mit dem Befehl track 2 rtr 2 reachability am Ende (last) steht, und stellen Sie Richtlinien bereit:



FlexConfig-Richtlinie

Wichtigste Punkte:

- RTR1 und RTR2 sind zwei VPDN-Gruppen an G0/0- bzw. G0/1-Schnittstellen.
- Track 2/SLA2 verfolgen die Erreichbarkeit zu RTR1. Der Befehl pppoe client route track 2 weist die Firewall an, die Standardroute über die externe Schnittstelle zu installieren, wenn Track 2 aktiv ist.
- Track 1/SLA1 verfolgt die Erreichbarkeit zu RTR2. Das Track-Objekt wird in der statischen Routenkonfiguration über die outside2-Schnittstelle verwendet.
- Mit dem Befehl pppoe client route distanz 10 wird die Firewall angewiesen, die administrative Distanz 10 auf die von RTR2 empfangene Standardroute anzuwenden und diese somit weniger vorzuziehen.
- Routen zu bestimmten Subnetzen über die outside2-Schnittstelle werden mit Tracking konfiguriert.
- Dies führt dazu, dass beide PPPoE-Sitzungen aktiv werden und der Datenverkehr vom PC abhängig von der Routing-Konfiguration zur Lastverteilung beiträgt.

Verifizierung

1. PPPoE-Sitzung mit RTR1 über die externe Schnittstelle wird aufgebaut:

```
<#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_d

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-Sitzung mit RTR2 über die outside2-Schnittstelle wird aufgebaut:

<#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:0.0.0.0.
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. Pakete von der PC-IP-Adresse 192.168.1.2 bis 10.10.253.2 und 172.16.253.2 werden gesendet. Aufgrund von PAT zeigen die Aufnahmen capo und capo2 die IP-Adresse der Ausgangsschnittstelle (zugeordnete Adressen) an:

<#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. Simulieren Sie den Ausfall einer Remote-Verbindung auf RTR1. Das Failover auf den Backup-Pfad über die Schnittstelle outside2 hängt von den Timern von track1 ab:

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
```

Anmerkung:

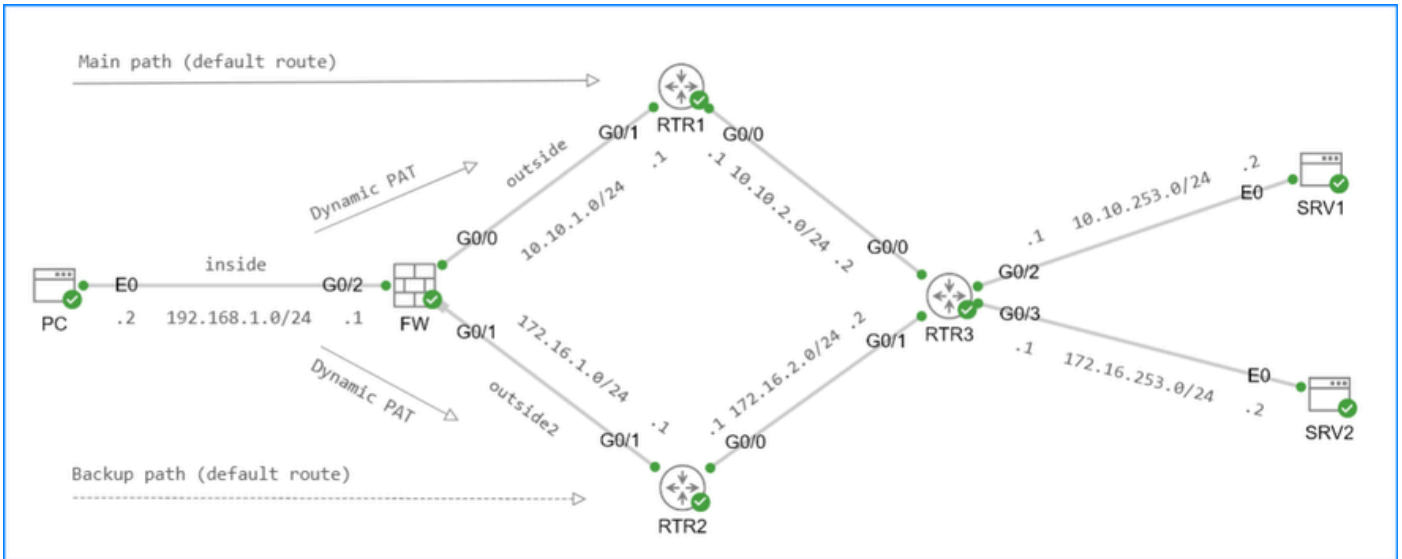
Die Routing-Änderungen werden nicht auf bestehende Verbindungen angewendet. Daher verwendet die bestehende Verbindung weiterhin den "alten" Pfad, auch wenn ein besserer Pfad verfügbar wird. Dies kann sich nach Routing-Änderungen negativ auswirken. Um die Firewall anzuweisen, den neuen Pfad zu verwenden, sollten Sie den Timer für Floating Conn aktivieren. Wenn der Timeout für Floating-Verbindungen aktiviert ist und auf einen Wert ungleich null gesetzt ist, können Verbindungen geschlossen werden, wenn eine bessere Route verfügbar wird. Auf diese Weise kann eine Verbindung wiederhergestellt werden, um die bessere Route zu verwenden. Weitere Informationen finden Sie in der Beschreibung von floating-conn unter <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>.

Aktiv/Standby-Redundanz ohne Lastverteilung

In diesem Fall ist nur eine PPPoE-Sitzung aktiv, die andere ist inaktiv, bis der Titel für die aktive Sitzung ausfällt.

Der Befehl `pppoe client second track x` wird für die outside2 (backup) Schnittstelle verwendet.

Weitere Informationen finden Sie in der folgenden Beispieltopologie:



Aktive Standby-Topologie

Wichtigste Punkte:

- PPPoE wird an den Schnittstellen G0/0 und G0/1 der Firewall konfiguriert.
- RTR1 und RTR2 sind PPPoE-Server.
- Die Firewall installiert über die externe Schnittstelle die Standardroute zu RTR1. Die Standardroute zu RTR2 weist eine höhere Routing-Distanz auf und ist weniger bevorzugt.

- Die Standardroute zu RTR1 über die externe Schnittstelle wird nachverfolgt. Sie ist optional, bietet jedoch ein schnelleres Failover auf den Pfad über RTR2.
- Die PPPoE-Sitzung zu RTR2 über die outside2-Schnittstelle wird nur eingerichtet, wenn die für die Standardroute zu RTR1 über die externe Schnittstelle verwendete Spur ausgefallen ist.
- Zu einem bestimmten Zeitpunkt ist nur eine PPPoE-Sitzung aktiv.
- Der Einfachheit halber wird die dynamische Port-Adressumwandlung (PAT) über die Außen- und Außen-2-Schnittstellen konfiguriert.

ASA-Konfiguration

```
<#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-Konfiguration

In diesem Abschnitt wird die Konfiguration des sekundären x-Befehls pppoe client für die outside2-Schnittstelle (Backup) behandelt. Da die FMC-Benutzeroberfläche keine Tracks für die Client-Optionen unterstützt, muss FlexConfig verwendet werden.

Sie müssen sicherstellen, dass die restliche Konfiguration konfiguriert wird, einschließlich PPPoE-Konfiguration, Routing und andere.

Achten Sie auf folgende Punkte:

1. FlexConfig-Richtlinien enthalten absichtlich keine umfassende Eingabevalidierung. Sie müssen sicherstellen, dass die Konfigurationen in dieser FlexConfig-Richtlinie korrekt sind. Falsche Konfigurationen führen zu einer fehlerhaften Bereitstellung, die zu einer Netzwerkunterbrechung führen kann. Sie sollten die Bereitstellung auch isolieren, damit sie nur FlexConfig-Änderungen und keine anderen Richtlinienaktualisierungen umfasst.
2. Während der Bereitstellung entfernt FMC alle Spuren von FlexConfig. Um die Persistenz sicherzustellen, müssen Sie die Bereitstellung des FlexConfig-Objekts auf Everytime festlegen und in einem separaten FlexConfig-Objekt bereitstellen.

Konfigurationsschritte bei FlexConfig

1. Erstellen Sie ein FlexConfig-Objekt für die Konfiguration von SLA- und PPPoE-Client-Konfigurationen für die externe 2 (Backup)-Schnittstelle. Stellen Sie sicher, dass Deployment auf Once und Type auf Append festgelegt ist. In diesem Beispiel werden Track 2, SLA 2 verwendet. Beachten Sie, dass der Befehl track 2 rtr 2 reachability fehlt:

Edit FlexConfig Object ?

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Deployment: | Type:

```

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

int G0/1
 pppoe client secondary track 2
!

```

FlexConfig für SLA

2. Erstellen Sie ein weiteres FlexConfig-Objekt für die Konfiguration des Befehls track 2 rtr 2 reachability. Stellen Sie sicher, dass die Bereitstellung auf Jederzeit und Typ festgelegt ist, an den angehängt werden soll:

Edit FlexConfig Object ?

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert | | Deployment: | Type:

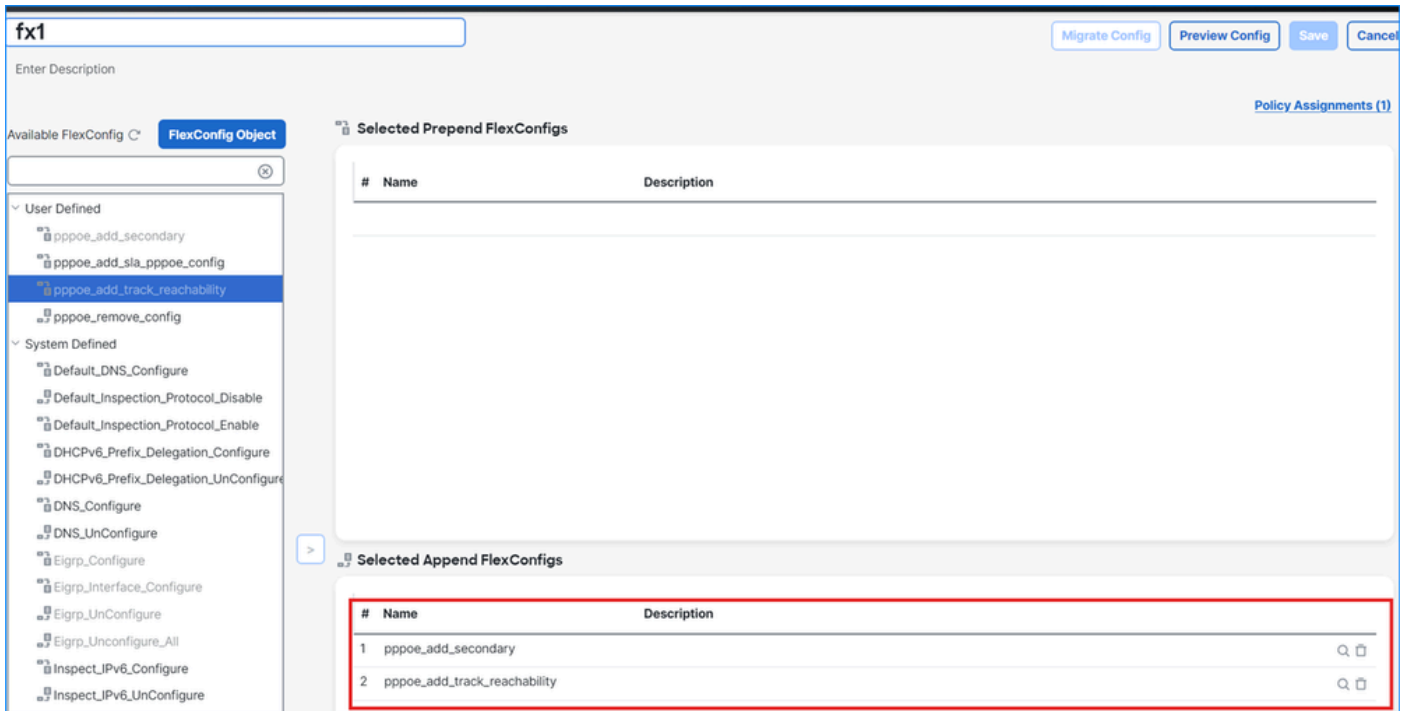
```

track 2 rtr 2 reachability

```

FlexConfig für Track

3. Fügen Sie der FlexConfig-Richtlinie Objekte hinzu. Stellen Sie sicher, dass das Objekt mit dem Befehl track 2 rtr 2 reachability am Ende (last) steht, und stellen Sie Richtlinien bereit:



FlexConfig-Richtlinie

Wichtigste Punkte:

- Der Befehl `pppoe client second track 2` unter der G0/1-Schnittstelle weist die Firewall an, die PPPoE-Sitzung über die G0/1-Schnittstelle nur zu aktivieren, wenn Track 2 fehlschlägt. Effektiv aktiviert der Ausfall von Track 2, der die Erreichbarkeit über den Hauptpfad verfolgt, den Backup-Pfad.
- Daher ist jeweils nur eine PPPoE-Sitzung aktiv.

Verifizierung

1. PPPoE-Session mit RTR1 über die externe Schnittstelle ist bereits aufgebaut. Die Sicherungssitzung ist inaktiv:

```
<#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. Die PPPoE-Sitzung zu RTR1 über die externe Schnittstelle schlägt fehl (z. B. aufgrund eines physischen Schnittstellen- oder Verbindungsfehlers). Die PPPoE-Sitzung zu RTR2 über die outside2-Schnittstelle wird aufgebaut.

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. Pakete von der PC-IP-Adresse 192.168.1.2 bis 10.10.253.2 und 172.16.253.2 werden gesendet. Aufgrund eines Ausfalls des Hauptpfads werden alle Pakete über die outside2-Schnittstelle gesendet. Aufgrund von PAT zeigt capture capo2 außerdem die IP-Adresse der Ausgangsschnittstelle an (zugeordnete Adressen):

<#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. Pfad über die externe Schnittstelle wird wiederhergestellt, PPPoE-Sitzung zu RTR1 wird wiederhergestellt. Die Sitzung über die outside2-Schnittstelle wechselt in den Zustand "Ausstehende Wiederverwendung":

```
<#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_dyn
```

```
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. Pakete von PC-IP-Adresse 192.168.1.2 bis 10.10.253.2 und 172.16.253.2 werden über die externe Schnittstelle (Hauptpfad) gesendet. Aufgrund von PAT zeigt Capo außerdem die IP-Adresse der Ausgangsschnittstelle (mapped) Adressen):

```
<#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

Anmerkung:

Die Routing-Änderungen werden nicht auf bestehende Verbindungen angewendet. Daher verwendet die bestehende Verbindung weiterhin den "alten" Pfad, auch wenn ein besserer Pfad verfügbar wird. Dies kann sich nach Routing-Änderungen negativ auswirken. Um die Firewall anzuweisen, den neuen Pfad zu verwenden, sollten Sie den Timer für Floating Conn aktivieren. Wenn der Timeout für Floating-Verbindungen aktiviert ist, d. h. auf einen Wert ungleich null gesetzt ist, können Verbindungen geschlossen werden, wenn eine bessere Route verfügbar wird. Auf diese Weise kann eine Verbindung wiederhergestellt werden, um die bessere Route zu verwenden. Weitere Informationen finden Sie in der Beschreibung von floating-conn unter 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.

Wie werden mit FlexConfig bereitgestellte Befehle entfernt oder deaktiviert?

Wenn Sie eine von FlexConfig bereitgestellte Konfiguration entfernen oder deaktivieren möchten, müssen Sie folgende Schritte ausführen:

1. Erstellen Sie eine FlexConfig mit Negationsbefehlen in dieser Reihenfolge, und stellen Sie sicher, dass Type auf Prepend festgelegt ist:
 - Entfernen von Verweisen auf Trackobjekte
 - Löschen von Track-Objekten
 - Löschen von SLA-Objekten

Beispiel für das Entfernen der Konfiguration für die Aktiv-Aktiv-Redundanz mit Lastverteilung und PPPoE-Client-Routenverfolgung:

Edit FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

Type:

Prepend ▾

```
int e1/2
no pppoe client route track
no track 2 rtr 2 reachability
no sla monitor 2
```

Flexconfig-Entfernung 1

Beispiel für das Entfernen der Konfiguration, die für eine Aktiv/Standby-Redundanz ohne Lastverteilung bereitgestellt wurde:

Edit FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾



Deployment:

Once ▾

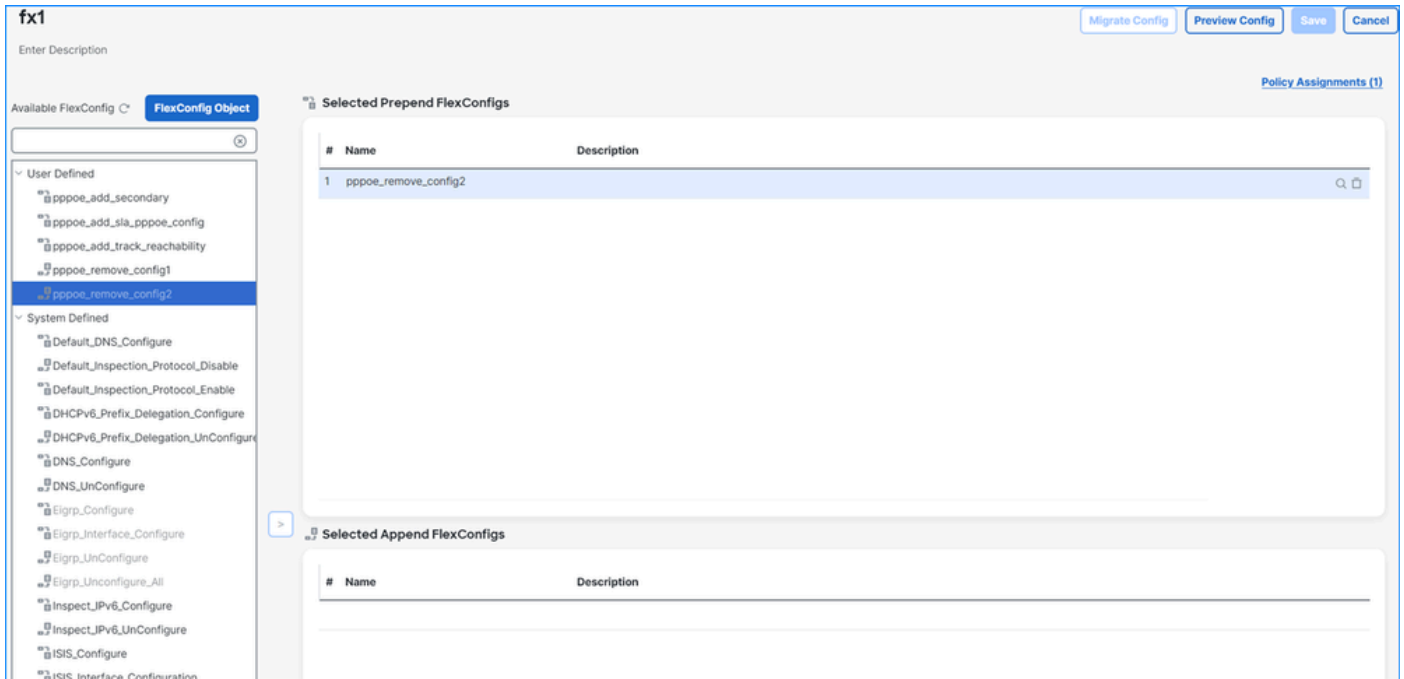
Type:

Prepend ▾

```
int e1/3
no pppoe client secondary track
no track 2 rtr 2 reachability
no sla monitor 2
```

Flexconfig-Entfernung 2

2. Fügen Sie das in Schritt 1 erstellte Negationsobjekt der FlexConfig-Richtlinie hinzu. Stellen Sie sicher, dass die Objekte zum Hinzufügen von PPPoE-Befehlen entfernt wurden und nicht in der Richtlinie vorhanden sind:



Richtlinie zum Entfernen von FlexConfig

3. Bereitstellen von Richtlinien und Überprüfen der Entfernung von Befehlen in der CLI

4. Entfernen Sie das in Schritt 1 erstellte Negationsobjekt aus der FlexConfig-Richtlinie, und stellen Sie es erneut bereit.

Referenzen

- Cisco Bug-ID [CSCwt39430](#) "ENH: Unterstützung der FTD-Schnittstelle für DHCP/PPPoE-Client-Konfigurationsbefehle und -Unterbefehle auf der FMC-Benutzeroberfläche"

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.