# Konfigurieren eines standortübergreifenden FlexVPN-Tunnels mit einem Peer mit dynamischer IP-Adresse

## Inhalt


[Einleitung](#)

[Voraussetzungen](#)

- [Anforderungen](#)
- [Verwendete Komponenten](#)

[Hintergrundinformationen](#)

- [Netzwerkdiagramm](#)

[Konfigurationen](#)

- [Konfiguration auf dem Router der Zentrale](#)
- [Konfiguration des Außenstellen-Routers](#)
- [Routing-Konfiguration](#)
- [Vollständige Konfiguration des Router-Hauptsitzes](#)
- [Konfiguration des Außenstellen-Routers abgeschlossen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)


## Einleitung

In diesem Dokument wird die Konfiguration eines FlexVPN-Site-to-Site-VPN-Tunnels zwischen zwei Cisco Routern beschrieben, wenn der Remote-Peer über eine dynamische IP-Adresse verfügt.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FlexVPN
- IKEv2-Protokoll

### Verwendete Komponenten

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

- CSR1000V-Gerät
- Cisco IOS® XE Software, Version 17.3.4

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.

# Hintergrundinformationen

## Netzwerkdiagramm


Topologie für dynamische Peers

Die Topologie in diesem Beispiel zeigt einen Cisco Router und einen anderen Cisco Router, der über eine dynamische IP-Adresse auf der öffentlich zugänglichen Schnittstelle verfügt.

# Konfigurationen

In diesem Abschnitt wird beschrieben, wie der standortübergreifende FlexVPN-Tunnel auf einem Cisco Router konfiguriert wird, wenn der Remote-Peer eine dynamische IP-Adresse verwendet.

In diesem Konfigurationsbeispiel wird die Pre-Shared-Key (PSK)-Authentifizierungsmethode verwendet. Es kann jedoch auch die Public Key Infrastructure (PKI) verwendet werden.

## Konfiguration auf dem Router der Zentrale

In diesem Beispiel wurden die IKEv2 Smart Defaults des Routers verwendet. Die Funktion IKEv2 Smart Defaults minimiert die FlexVPN-Konfiguration, da sie die meisten Anwendungsfälle abdeckt. IKEv2 Smart Defaults können für bestimmte Anwendungsfälle angepasst werden, dies wird jedoch nicht empfohlen. Die intelligenten Standardeinstellungen umfassen die IKEv2-Autorisierungsrichtlinie, das IKEv2-Angebot, die IKEv2-Richtlinie, das Internet Protocol Security (IPsec) Profile und den IPsec-Transformationssatz.

Um die Standardwerte in Ihrem Gerät zu überprüfen, können Sie die unten aufgeführten Befehle ausführen.

- show crypto ikev2, Autorisierungsrichtlinie Standard

- show crypto ikev2, Standardvorschlag
- show crypto ikev2, Richtlinie Standard
- show crypto ipsec profile default
- show crypto ipsec transformation-set default

Schritt 1 Konfigurieren des IKEv2-Keyrings

- In diesem Fall kennt der Router im Hauptsitz die Peer-IP nicht, da sie dynamisch ist, und stimmt daher mit einer IP-Adresse überein.
- Remote- und lokale Schlüssel werden ebenfalls konfiguriert.
- Es wird empfohlen, starke Schlüssel zu haben, um Schwachstellen zu vermeiden.

```
crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123
```

Schritt 2: Konfigurieren des AAA-Modells (Authentication, Authorization and Accounting)

- Dadurch wird das Management-Framework für die Benutzer erstellt, die für diese Instanz eine Verbindung herstellen können.
- Da die Verbindungsaushandlung von diesem Gerät aus initiiert wird, verweist das Modell auf seine lokale Datenbank, um die autorisierten Benutzer zu bestimmen.

```
aaa new-model
aaa authorization network FLEXVPN local
```

Schritt 3 Konfigurieren des IKEv2-Profils

- Da die Remote-Peer-IP-Adresse dynamisch ist, können Sie keine bestimmte IP-Adresse verwenden, um den Peer zu identifizieren.
- Sie können den Remote-Peer jedoch anhand der auf dem Peer-Gerät definierten Domäne, des FQDN oder der Schlüssel-ID identifizieren.

- Die AAA-Gruppe (Authentication, Authorization and Accounting) muss für die Autorisierungsmethode des Profils hinzugefügt werden, wobei als Methode PSK verwendet wird.
- Wenn die Authentifizierungsmethode PKI ist, wird sie hier als cert anstatt PKI angegeben.
- Da das Ziel darin besteht, eine dynamische virtuelle Tunnelschnittstelle (dVTI) zu erstellen, ist dieses Profil mit einer virtuellen Vorlage verknüpft.

```
crypto ikev2 profile FLEXVPN_PROFILE
```

```
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1
```

Schritt 4 Konfigurieren des IPsec-Profils

- Ein benutzerdefiniertes IPsec-Profil kann konfiguriert werden, wenn Sie das Standardprofil nicht verwenden.
- Das in Schritt 3 erstellte IKEv2-Profil wird diesem IPsec-Profil zugeordnet.

```
crypto ipsec profile defualt
 set ikev2-profile FLEXVPN_PROFILE
```

Schritt 5 Konfigurieren der Loopback-Schnittstelle und Virtual Template Interface

- Da das Remote-Gerät über eine dynamische IP-Adresse verfügt, muss aus einer Vorlage ein dVTI erstellt werden.
- Bei dieser virtuellen Vorlage handelt es sich um eine Konfigurationsvorlage, aus der dynamische Virtual-Access-Schnittstellen erstellt werden.

```
interface Loopback1
 ip address 192.168.1.1 255.255.255.0
```

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default
```

## Konfiguration des Außenstellen-Routers

Konfigurieren Sie für den Router der Außenstelle den IKEv2-Keyring, das AAA-Modell, das IPsec-Profil und das IKEv2-Profil wie in den vorherigen Schritten beschrieben, einschließlich der erforderlichen Konfigurationsänderungen und der nachfolgend beschriebenen:

1. Konfigurieren Sie die lokale Identität, die als Kennung an den Router im Hauptsitz gesendet wird.

```
crypto ikev2 profile FLEXVPN_PROFILE
```

```
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
```

Schritt 5: Konfigurieren der statischen virtuellen Tunnelschnittstelle

- Da die IP-Adresse für den Router im Hauptsitz bekannt ist und nicht geändert wird, wird eine statische VTI-Schnittstelle konfiguriert.

```
interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default
```

## Routing-Konfiguration

In diesem Beispiel wird das Routing bei der Einrichtung der IKEv2-Sicherheitszuordnung (Security Association, SA) mit der Konfiguration einer Zugriffskontrollliste definiert. Dies definiert den Datenverkehr, der über das VPN gesendet wird. Sie können auch dynamische Routing-Protokolle konfigurieren. Dies ist jedoch nicht im Umfang dieses Dokuments enthalten.

Schritt 5: Definieren der ACL

Router im Hauptsitz:

```
ip access-list standard Flex-ACL
 permit 10.10.10.0 255.255.255.0
```

Zweigstellen-Router:

```
ip access-list standard Flex-ACL
 permit 10.20.20.0 255.255.255.0
```

Schritt 6: Ändern Sie die IKEv2-Autorisierungsprofile auf jedem Router, um die ACL festzulegen.

```
crypto ikev2 authorization policy default
 route set interface
```

```
 route set access-list Flex-ACL
```

## Vollständige Konfiguration des Router-Hauptsitzes

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer spoke
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote key-id Peer123
 identity local address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default
 virtual-template 1

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback1
 ip address 192.168.1.1 255.255.255.0

interface Loopback10
 ip address 10.10.10.10 255.255.255.255

interface GigabitEthernet0
 ip address 172.16.1.1 255.255.255.0

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 tunnel protection ipsec profile default

ip access-list standard Flex-ACL
 5 permit 10.10.10.0 255.255.255.0
```

## Konfiguration des Außenstellen-Routers abgeschlossen

```
aaa new-model
aaa authorization network FLEXVPN local

crypto ikev2 authorization policy default
 route set interface
```

```
 route set access-list Flex-ACL

crypto ikev2 keyring FLEXVPN_KEYRING
 peer HUB
  address 0.0.0.0 0.0.0.0
  pre-shared-key local Cisco123
  pre-shared-key remote Cisco123

crypto ikev2 profile FLEXVPN_PROFILE
 identity local key-id Peer123
 match identity remote address 172.16.1.1
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FLEXVPN default

crypto ipsec profile default
 set ikev2-profile FLEXVPN_PROFILE

interface Loopback20
 ip address 10.20.20.20 255.255.255.255

interface Tunnel0
 ip address 192.168.1.10 255.255.255.0
 tunnel source GigabitEthernet0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface GigabitEthernet0
 ip address dhcp
 negotiation auto

ip access-list standard Flex-ACL
 10 permit 10.20.20.0 255.255.255.0
```

# Überprüfung

Um den Tunnel zu verifizieren, müssen Sie sicherstellen, dass Phase 1 und Phase 2 in Betrieb sind und ordnungsgemäß funktionieren.

```
Headquarter#show crypto ikev2 sa detail
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         172.16.1.1/500        172.16.2.1/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK, Auth verify: P
      Life/Active Time: 86400/74645 sec
      CE id: 61256, Session-id: 1
      Status Description: Negotiation done
      Local spi: D5129F36B1180175       Remote spi: F9298874F90BFEC7
      Local id: 172.16.1.1
      Remote id: 172.16.2.1
      Local req msg id:  16             Remote req msg id:  31
      Local next msg id: 16             Remote next msg id: 31
      Local req queued:  16             Remote req queued:  31
      Local window:      5              Remote window:      5
```

```
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
      Remote subnets:                  -------------> This section shows the traffic to be routed acros
      192.168.1.10 255.255.255.255
      10.20.20.20 255.255.255.255

 IPv6 Crypto IKEv2  SA
```

## Phase 2, IPSec

```
Headquarter#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.1/255.255.255.255/47/0)
   current_peer 172.16.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 225, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 225, #pkts decrypt: 225, #pkts verify: 225
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.16.2.1
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0
     current outbound spi: 0xC124D7C1(3240417217)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xC2AADCAB(3265977515)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2912, flow_id: CSR:912, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
        sa timing: remaining key lifetime (k/sec): (4607993/628)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC124D7C1(3240417217)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Transport, }
        conn id: 2911, flow_id: CSR:911, sibling_flags FFFFFFFF80000008, crypto map: Virtual-Access1-he
        sa timing: remaining key lifetime (k/sec): (4608000/628)
        IV size: 16 bytes
```

```
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Sie müssen auch überprüfen, ob sich die Virtual Access-Schnittstelle im UP-Status befindet.

```
show interface Virtual-Access1
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Interface is unnumbered. Using address of Loopback1 (192.168.1.1)
  MTU 9934 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL
  Tunnel vaccess, cloned from Virtual-Template1
  Vaccess status 0x4, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 172.16.1.1, destination 172.16.2.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1434 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "default")
  Last input 20:53:34, output 20:53:34, output hang never
  Last clearing of "show interface" counters 20:55:43
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     586 packets input, 149182 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     15 packets output, 1860 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

# Fehlerbehebung

In diesem Abschnitt wird die Fehlerbehebung bei der Tunneleinrichtung beschrieben.

Führen Sie die folgenden Schritte aus, wenn die IKE-Verhandlung fehlschlägt:

1. Überprüfen Sie mit den folgenden Befehlen den aktuellen Status:

- show crypto ikev2 sa
- show crypto ipsec sa
- Kryptografiesitzung anzeigen

2. Verwenden Sie diese Befehle, um den Tunnelaushandlungsprozess zu debuggen:

- debuggen crypto ikev2
- debuggen crypto ipsec

## Zugehörige Informationen

- Technischer Support und Downloads von Cisco

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.