FlexVPN-Migration: Ältere Versionen von EzVPN-NEM+ und FlexVPN auf demselben Server

Inhalt

Einleitung

Dieses Dokument beschreibt den Migrationsprozess von EzVPN zu FlexVPN. FlexVPN ist die neue Unified VPN-Lösung von Cisco. FlexVPN nutzt das IKEv2-Protokoll und kombiniert Remote-Zugriff, Site-to-Site-, Hub-and-Spoke- und partielle Mesh-VPN-Bereitstellungen. Bei älteren Technologien wie z. B. EzVPN empfiehlt Cisco dringend, zu FlexVPN zu migrieren, um die zahlreichen Funktionen nutzen zu können.

In diesem Dokument wird eine bestehende EzVPN-Bereitstellung untersucht, die aus Legacy-EzVPN-Hardware-Clients besteht, die Tunnel auf einem EzVPN-Headend-Gerät terminieren, das auf einer veralteten Crypto Map basiert. Ziel ist die Migration von dieser Konfiguration zur Unterstützung von FlexVPN mit folgenden Anforderungen:

- Vorhandene Clients arbeiten weiterhin reibungslos, ohne dass Konfigurationsänderungen erforderlich sind. Dies ermöglicht eine schrittweise Migration dieser Clients auf FlexVPN im Laufe der Zeit.
- Das Headend-Gerät sollte gleichzeitig die Terminierung neuer FlexVPN-Clients unterstützen.

Zur Umsetzung dieser Migrationsziele werden zwei wichtige IPsec-Konfigurationskomponenten verwendet: IKEv2 und Virtual Tunnel Interfaces (VTI). Diese Ziele werden in diesem Dokument kurz beschrieben.

Weitere Dokumente dieser Serie

- FlexVPN-Bereitstellungsleitfaden: AnyConnect zu IOS-Headend über IPsec mit IKEv2 und Zertifikaten

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

IKEv1 und IKEv2

FlexVPN basiert auf dem IKEv2-Protokoll, dem auf RFC 4306 basierenden Schlüsselverwaltungsprotokoll der nächsten Generation, und einer Erweiterung des IKEv1-Protokolls. FlexVPN ist nicht abwärtskompatibel mit Technologien, die nur IKEv1 unterstützen (z. B. EzVPN). Dies ist eine der wichtigsten Überlegungen bei der Migration von EzVPN zu FlexVPN. Eine Protokoll-Einführung zu IKEv2 und ein Vergleich mit IKEv1 finden Sie in IKE-Version 2 auf einen Blick.

Crypto Map und Virtual Tunnel Interfaces

Virtual Tunnel Interface (VTI) ist eine neue Konfigurationsmethode für VPN-Server- und Client-Konfigurationen. VTI:

- Ersetzung dynamischer Kryptokarten, die jetzt als veraltete Konfiguration angesehen werden.
- Unterstützt natives IPsec-Tunneling.
- Keine statische Zuordnung einer IPsec-Sitzung zu einer physischen Schnittstelle erforderlich; bietet daher Flexibilität für das Senden und Empfangen von verschlüsseltem Datenverkehr über eine beliebige physische Schnittstelle (z. B. mehrere Pfade).

- Minimale Konfiguration, da der virtuelle On-Demand-Zugriff über die Virtual-Template-Schnittstelle geklont wird.
- Der Datenverkehr wird bei der Weiterleitung an die Tunnelschnittstelle verschlüsselt/entschlüsselt und über die IP-Routing-Tabelle verwaltet (dies spielt bei der Verschlüsselung eine wichtige Rolle).
- Funktionen können entweder auf Klartext-Pakete an der VTI-Schnittstelle oder auf verschlüsselte Pakete an der physischen Schnittstelle angewendet werden.

Die beiden verfügbaren VTIs sind:

- Statisch (sVTI) - Eine statische virtuelle Tunnel-Schnittstelle verfügt über eine feste Tunnelquelle und ein festes Tunnelziel und wird in der Regel in einem Szenario verwendet, in dem die Bereitstellung vom Standort zum Standort erfolgt. Im Folgenden finden Sie ein Beispiel für eine sVTI-Konfiguration:

```
interface Tunnel2
 ip address negotiated
 tunnel source Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile testflex
```

- Dynamisch (dVTI) - Mit einer dynamischen virtuellen Tunnelschnittstelle können dynamische IPsec-Tunnel terminiert werden, die kein festes Tunnelziel haben. Nach erfolgreicher Tunnelverhandlung werden Virtual-Access-Schnittstellen aus einer virtuellen Vorlage geklont und übernehmen alle L3-Funktionen dieser virtuellen Vorlage. Das Beispiel zeigt eine dVTI-Konfiguration:

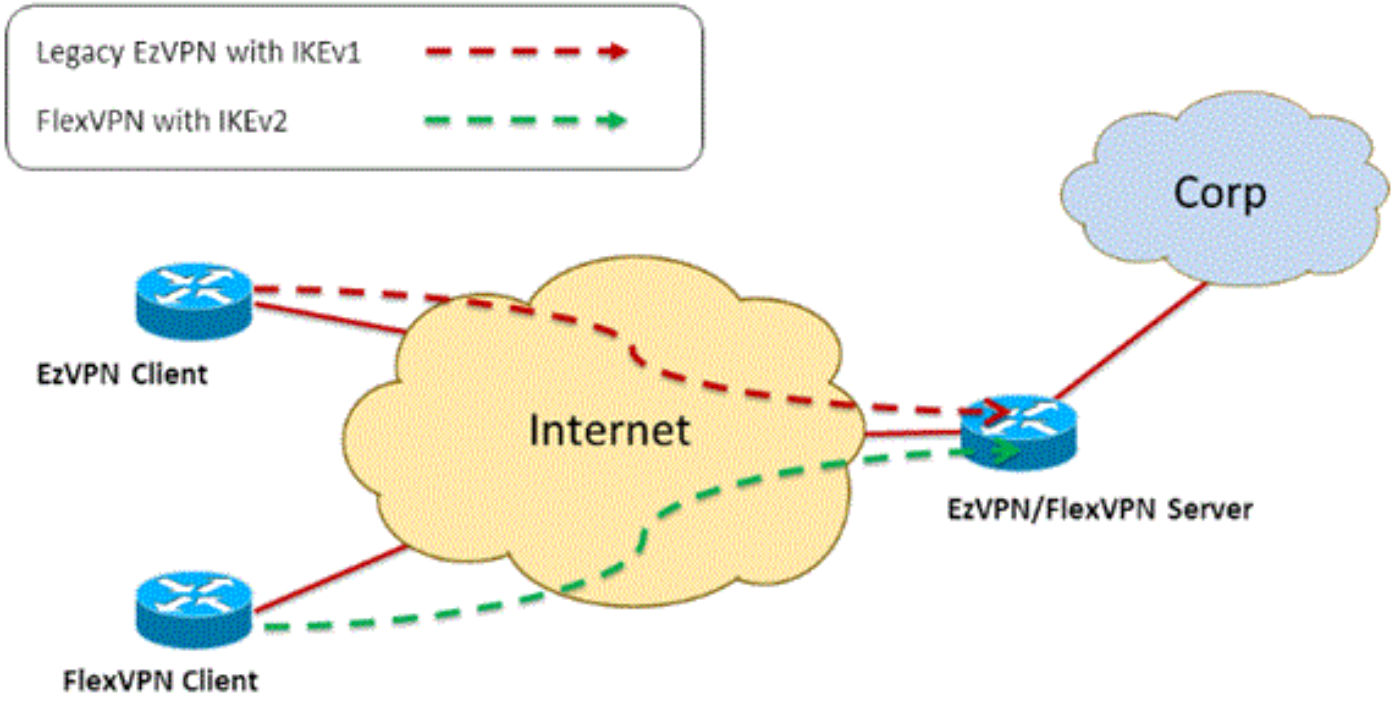
```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile testflex
```

Weitere Informationen zu dVTI finden Sie in diesen Dokumenten:

- Konfigurieren von Cisco Easy VPN mit IPSec Dynamic Virtual Tunnel Interface (DVTI)
- Einschränkungen für die IPsec Virtual Tunnel Interface
- Konfigurieren der Multi-SA-Unterstützung für dynamische virtuelle Tunnelschnittstellen mithilfe von IKEv1

Damit EzVPN- und FlexVPN-Clients gleichzeitig verwendet werden können, müssen Sie zunächst den EzVPN-Server von der Konfiguration der Legacy-Crypto Map zu einer dVTI-Konfiguration migrieren. In den folgenden Abschnitten werden die erforderlichen Schritte ausführlich erläutert.

Netzwerktopologie



Aktuelle Konfiguration mit EzVPN-Client mit Legacy-NEM+-Modus

Client-Konfiguration

Nachfolgend finden Sie eine typische EzVPN-Client-Router-Konfiguration. In dieser Konfiguration wird der Network Extension Plus (NEM+)-Modus verwendet, der mehrere SA-Paare sowohl für das LAN innerhalb der Schnittstellen als auch für die dem Client zugewiesene Moduskonfiguration erstellt.

```
crypto ipsec client ezvpn legacy-client
 connect manual
 group Group-One key cisco123
 mode network-plus
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description EzVPN WAN interface
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description EzVPN LAN inside interface
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
```

Serverkonfiguration

Auf dem EzVPN-Server wird vor der Migration eine veraltete Konfiguration der Crypto Map als Basiskonfiguration verwendet.

```
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network ezvpn-author local
!
username client1 password 0 client1
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address respond
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description EzVPN server WAN interface
 ip address 192.168.1.10 255.255.255.0
 crypto map client-map
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
!
ip access-list extended split-tunnel-acl
  remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
```

Migration von Server zu FlexVPN

Wie in den vorherigen Abschnitten beschrieben, verwendet FlexVPN IKEv2 als Kontrollebenenprotokoll und ist nicht abwärtskompatibel mit einer IKEv1-basierten EzVPN-Lösung. Daher besteht die allgemeine Idee dieser Migration darin, den vorhandenen EzVPN-Server so zu konfigurieren, dass sowohl Legacy-EzVPN (IKEv1) als auch FlexVPN (IKEv2) koexistieren. Um dieses Ziel zu erreichen, können Sie diesen zweistufigen Migrationsansatz verwenden:

1. Verlagern Sie die Legacy-EzVPN-Konfiguration am Headend von einer auf der Crypto Map basierenden Konfiguration auf dVTI.
2. Fügen Sie die FlexVPN-Konfiguration hinzu, die ebenfalls auf dVTI basiert.

Verlagerung der Legacy-Crypto-Map zu dVTI

Serverkonfigurationsänderungen

Ein EzVPN-Server, der auf der physischen Schnittstelle mit einer Crypto Map konfiguriert ist, weist hinsichtlich der Unterstützung und Flexibilität von Funktionen mehrere Einschränkungen auf. Wenn Sie über EzVPN verfügen, empfiehlt Cisco nachdrücklich die Verwendung von dVTI. Als ersten Schritt für die Migration zu einer vorhandenen EzVPN- und FlexVPN-Konfiguration müssen Sie diese in eine dVTI-Konfiguration ändern. Dadurch wird die IKEv1- und IKEv2-Trennung zwischen den verschiedenen Schnittstellen virtueller Vorlagen ermöglicht, um beide Arten von Clients zu unterstützen.

Hinweis: Zur Unterstützung des Network Extension Plus Mode des EzVPN-Betriebs auf den EzVPN-Clients muss der Headend-Router die Multi-SA-on-dVTI-Funktion unterstützen. Auf diese Weise können mehrere IP-Datenflüsse durch den Tunnel geschützt werden, der für das Headend erforderlich ist, um den Datenverkehr in das interne Netzwerk des EzVPN-Clients zu verschlüsseln, sowie die IP-Adresse, die dem Client durch die Konfiguration des IKEv1-Modus zugewiesen wurde. Weitere Informationen zur Unterstützung mehrerer SAs auf dVTI mit IKEv1 finden Sie unter Multi-SA Support for Dynamic Virtual Tunnel Interfaces for IKEv1.

Gehen Sie wie folgt vor, um die Konfigurationsänderung auf dem Server zu implementieren:

Schritt 1 - Entfernen Sie die Crypto Map von der physischen Ausgangsschnittstelle, die die EzVPN-Client-Tunnel terminiert:

```
interface Ethernet0/0
 ip address 192.168.1.10 255.255.255.0
 no crypto map client-map
```

Schritt 2 - Erstellen einer virtuellen Vorlagenschnittstelle, über die virtuelle Zugriffsschnittstellen nach der Einrichtung der Tunnel geklont werden:

```
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
```

Schritt 3 - Ordnen Sie diese neu erstellte virtuelle Vorlagenschnittstelle dem isakmp-Profil für die konfigurierte EzVPN-Gruppe zu:

```
crypto isakmp profile Group-One-Profile
   match identity group Group-One
   client authentication list client-xauth
   isakmp authorization list ezvpn-author
   client configuration address initiate
   client configuration address respond
   virtual-template 1
```

Überprüfen Sie, ob die bestehenden EzVPN-Clients auch weiterhin funktionieren. Jetzt werden ihre Tunnel jedoch auf einer dynamisch erstellten virtuellen Zugriffsschnittstelle terminiert. Dies kann mithilfe des Befehls **show crypto session** verifiziert werden (siehe folgendes Beispiel):

```
PE-EzVPN-Server#show crypto session
Crypto session current status
Interface: Virtual-Access1
Username: client1
Profile: Group-One-Profile
Group: Group-One
```

```
Assigned address: 10.1.1.101
Session status: UP-ACTIVE
Peer: 192.168.2.101 port 500
  IKEv1 SA: local 192.168.1.10/500 remote 192.168.2.101/500 Active
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 host 10.1.1.101
        Active SAs: 2, origin: crypto map
  IPSEC FLOW: permit ip 172.16.0.0/255.255.255.0 172.16.1.0/255.255.255.0
        Active SAs: 2, origin: crypto map
```

Hinzufügen der FlexVPN-Konfiguration zum Server

In diesem Beispiel wird RSA-SIG (d. h. Certificate Authority) sowohl auf dem FlexVPN-Client als auch auf dem Server verwendet. Bei der Konfiguration in diesem Abschnitt wird davon ausgegangen, dass der Server bereits erfolgreich authentifiziert und beim CA-Server registriert wurde.

Schritt 1 - Überprüfen der IKEv2 Smart Default-Konfiguration

Mit IKEv2 können Sie jetzt die Smart Default-Funktion nutzen, die in 15.2(1)T eingeführt wurde. Sie vereinfacht eine FlexVPN-Konfiguration. Hier einige Standardkonfigurationen:

Standard-IKEv2-Autorisierungsrichtlinie:

```
VPN-Server#show crypto ikev2 authorization policy default
 IKEv2 Authorization Policy : default
 route set interface
 route accept any tag : 1 distance : 1
```

Standard-IKEv2-Angebot:

```
VPN-Server#show crypto ikev2 proposal default
 IKEv2 proposal: default
 Encryption : AES-CBC-256 AES-CBC-192 AES-CBC-128
 Integrity : SHA512 SHA384 SHA256 SHA96 MD596
 PRF : SHA512 SHA384 SHA256 SHA1 MD5
 DH Group : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

IKEv2-Standardrichtlinie:

```
VPN-Server#show crypto ikev2 policy default
 IKEv2 policy : default
 Match fvrf : any
 Match address local : any
 Proposal : default
```

Standard-IPsec-Profil:

```
VPN-Server#show crypto ipsec profile default
IPSEC profile default
 Security association lifetime: 4608000 kilobytes/3600 seconds
 Responder-Only (Y/N): N
 PFS (Y/N): N
 Transform sets={
 default: { esp-aes esp-sha-hmac } ,
 }
```

Standard-IPsec-Umwandlungssatz:

```
VPN-Server#show crypto ipsec transform default
{ esp-aes esp-sha-hmac }
 will negotiate = { Transport, },
```

Weitere Informationen zur IKEv2 Smart Default-Funktion finden Sie unter IKEv2 Smart Defaults (nur registrierte Kunden).

Schritt 2 - Ändern Sie die Standard-IKEv2-Autorisierungsrichtlinie und fügen Sie ein Standard-IKEv2-Profil für die FlexVPN-Clients hinzu.

Das hier erstellte IKEv2-Profil wird mit einer Peer-ID auf der Grundlage des Domänennamens cisco.com abgeglichen, und die für die Clients erstellten virtuellen Zugriffsschnittstellen werden aus der virtuellen Vorlage 2 erstellt. Beachten Sie außerdem, dass die Autorisierungsrichtlinie den IP-Adresspool definiert, der für die Zuweisung von Peer-IP-Adressen und Routen verwendet wird, die über den IKEv2-Konfigurationsmodus ausgetauscht werden sollen:

```
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
```

Schritt 3 - Erstellen Sie die virtuelle Vorlagenschnittstelle für die FlexVPN-Clients:

```
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
```

Konfiguration des FlexVPN-Clients

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
```

```
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
```

Vollständige Konfiguration

Vollständige Hybrid-Server-Konfiguration

```
hostname VPN-Server
!
!
aaa new-model
!
aaa authentication login client-xauth local
aaa authorization network default local
aaa authorization network ezvpn-author local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=vpn-server.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 07
 certificate ca 01
username client1 password 0 client1
username cisco password 0 cisco
!
crypto ikev2 authorization policy default
 pool flexvpn-pool
 def-domain cisco.com
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn VPN-Server.cisco.com
 authentication remote pre-share
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
 virtual-template 2
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
!
```

```
crypto isakmp client configuration group Group-One
 key cisco123
 pool Group-One-Pool
 acl split-tunnel-acl
 save-password
crypto isakmp profile Group-One-Profile
 match identity group Group-One
 client authentication list client-xauth
 isakmp authorization list ezvpn-author
 client configuration address initiate
 client configuration address respond
 virtual-template 1
!
crypto ipsec transform-set aes-sha esp-aes esp-sha-hmac
!
crypto ipsec profile default
 set ikev2-profile default
!
crypto ipsec profile legacy-profile
 set transform-set aes-sha
!
crypto dynamic-map client-dynamic-map 1
 set transform-set aes-sha
 reverse-route
!
crypto map client-map 1 ipsec-isakmp dynamic client-dynamic-map
!
interface Ethernet0/0
 description WAN
 ip address 192.168.1.10 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.0.1 255.255.255.0
!
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet1/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile legacy-profile
!
interface Virtual-Template2 type tunnel
 ip unnumbered Ethernet1/0
 tunnel protection ipsec profile default
!
ip local pool Group-One-Pool 10.1.1.100 10.1.1.200
ip local pool flexvpn-pool 10.1.1.201 10.1.1.250
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
!
ip access-list extended split-tunnel-acl
 remark EzVPN split tunnel ACL
 permit ip 172.16.0.0 0.0.0.255 any
!
access-list 1 permit 172.16.0.0 0.0.0.255
```

Vollständige Konfiguration des IKEv1-EzVPN-Clients

```
hostname Client1
!
crypto ipsec client ezvpn legacy-client
```

```
 connect manual
 group Group-One key cisco123
 mode network-extension
 peer 192.168.1.10
 username client1 password client1
 xauth userid mode local
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.101 255.255.255.0
 crypto ipsec client ezvpn legacy-client
!
interface Ethernet1/0
 description LAN
 ip address 172.16.1.1 255.255.255.0
 crypto ipsec client ezvpn legacy-client inside
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

Vollständige Konfiguration des IKEv2 FlexVPN-Clients

```
hostname Client2
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
!
no ip domain lookup
ip domain name cisco.com
ip host ca-server 192.168.2.1
!
crypto pki trustpoint flex-trustpoint
 redundancy
 enrollment url http://ca-server:80
 serial-number
 ip-address none
 fingerprint 08CBB1E948A6D9571965B5EE58FBB726
 subject-name cn=Client2.cisco.com, OU=Flex, O=cisco
 revocation-check crl
 rsakeypair flex-key-pair 1024
!
!
crypto pki certificate chain flex-trustpoint
 certificate 06
 certificate ca 01
!
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list 1
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Client2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint flex-trustpoint
 aaa authorization group cert list default default
```

```
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination 192.168.1.10
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 description WAN
 ip address 192.168.2.102 255.255.255.0
!
interface Ethernet1/0
 description LAN
 ip address 172.16.2.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.2.1
!
access-list 1 permit 172.16.2.0 0.0.0.255
```

Konfigurationsprüfung

Nachfolgend sind einige der Befehle aufgeführt, mit denen die EzVPN-/FlexVPN-Vorgänge auf einem Router überprüft werden:

```
show crypto session

show crypto session detail

show crypto isakmp sa

show crypto ikev2 sa

show crypto ipsec sa detail

show crypto ipsec client ez (for legacy clients)

show crypto socket

show crypto map
```

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme