Konfiguration und Überprüfung der FlexVPN-Lösung

Inhalt

Einleitung

In diesem Dokument wird die Flex Virtual Private Network-Umgebung beschrieben, ihre Funktionen vorgestellt und die Konfiguration der einzelnen FlexVPN-Topologien erläutert.

Voraussetzungen

Anforderungen

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

- Cisco IOS und Cisco IOS XE
- Internet Key Exchange (IKE) Version 2
- Internetprotokollsicherheit (IPsec)
- FlexVPN

Verwendete Komponenten

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

- Cisco IOS XE Amsterdam 17.3.6

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

FlexVPN ist eine vielseitige und umfassende VPN-Lösung von Cisco, die entwickelt wurde, um ein einheitliches Framework für verschiedene Arten von VPN-Verbindungen bereitzustellen. FlexVPN basiert auf dem IKEv2-Protokoll (Internet Key Exchange Version 2) und wurde entwickelt, um die Konfiguration, Verwaltung und Bereitstellung von VPN zu vereinfachen. Dabei kommt eine Reihe konsistenter Tools zum Einsatz. Dieselben Befehle und Konfigurationsschritte gelten für verschiedene VPN-Typen (Site-to-Site, Remote-Zugriff usw.). Diese Konsistenz trägt zur Reduzierung von Fehlern bei und ermöglicht eine intuitivere Bereitstellung.

IKEV2 im Vergleich zu IKEV1

FlexVPN nutzt IKEv2, das moderne kryptografische Algorithmen wie AES (Advanced Encryption Standard) und SHA-256 (Secure Hash Algorithm) unterstützt. Diese Algorithmen bieten eine starke Verschlüsselung und Datenintegrität, sodass die über das VPN übertragenen Daten nicht abgefangen oder manipuliert werden.

IKEv2 bietet im Vergleich zu IKEv1 mehr Authentifizierungsmethoden. Neben PSK (Pre-Shared Key) und zertifikatbasierten und hybriden Authentifizierungstypen ermöglicht IKEv2 dem Responder, das Extensible Authentication Protocol (EAP) für die Client-Authentifizierung zu verwenden.

In FlexVPN wird EAP für die Client-Authentifizierung verwendet. Der Router fungiert als Relay und leitet EAP-Nachrichten zwischen dem Client und dem Back-End-EAP-Server (in der Regel ein RADIUS-Server) weiter. FlexVPN unterstützt verschiedene EAP-Methoden, darunter EAP-TLS, EAP-PEAP, EAP-PSK und andere, zur Sicherung des Authentifizierungsprozesses.

Die Tabelle zeigt die Unterschiede zwischen den Funktionen IKEv1 und IKEv2:

	IKEv2	IKEv1
Nachrichten zur Protokollerstellung	4 Nachricht	6 Nachricht
EAP-Unterstützung	Ja (2 zusätzliche Nachrichten)	Nein
Verhandlung für Sicherheitszuordnungen	2 zusätzliche Nachrichten	3 zusätzliche Nachrichten
Ausführung über UDP 500/4500	Ja	Ja
NAT-Traversal (NAT-T)	Ja	Ja
Rückübertragungs- und Bestätigungsfunktionen	Ja	Ja
Identitätsschutz, DoS-Schutz und Perfect Forward Secrecy (PFS)	Ja	Ja
Unterstützung von Verschlüsselungstechnologien der nächsten Generation	Ja	Nein

Skalierbarkeit

FlexVPN kann problemlos von kleinen Büros auf große Unternehmensnetzwerke erweitert werden. Dies macht es zur idealen Wahl für Unternehmen mit einer großen Anzahl von Remote-Benutzern, die einen sicheren und zuverlässigen Netzwerkzugriff benötigen.

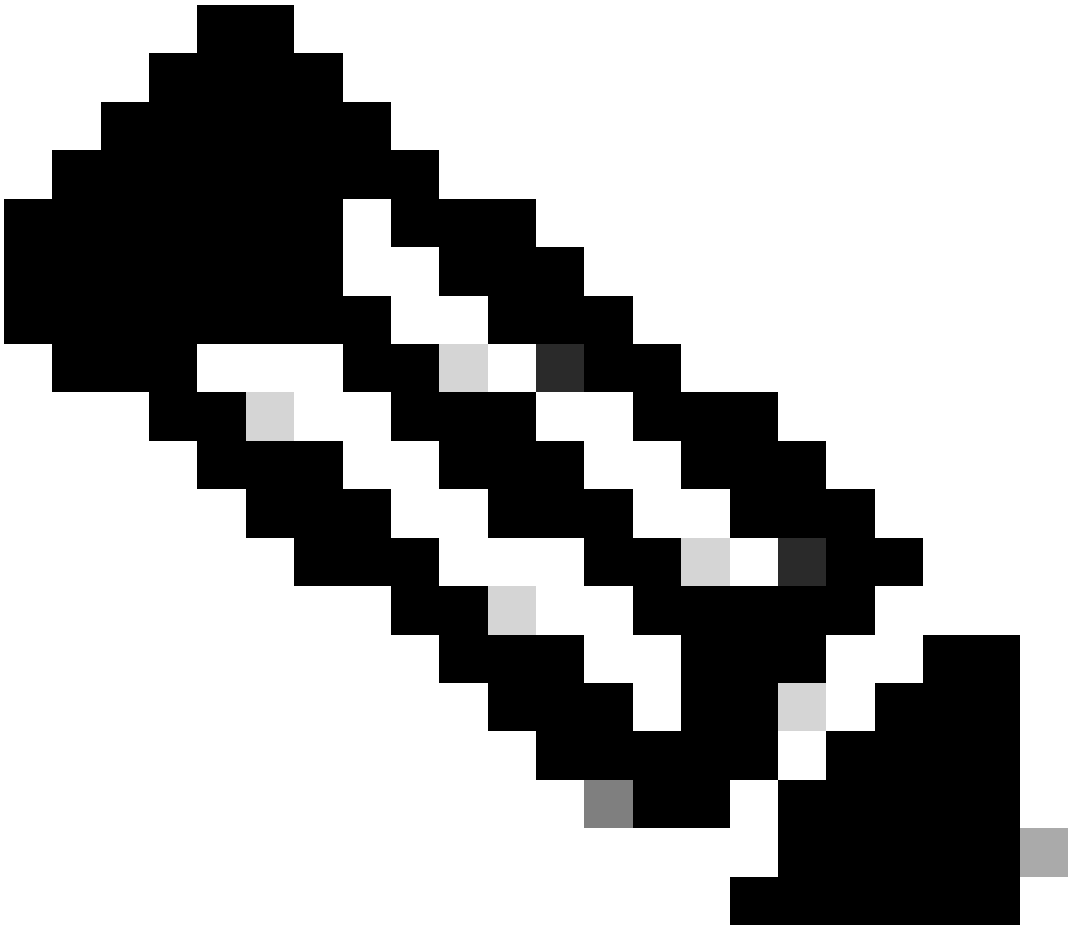
Wichtigste Funktionen

- Dynamische Konfiguration und On-Demand-Tunnel:
  - Eine FlexVPN-Verbindung wird initiiert, das System generiert eine virtuelle Zugriffsschnittstelle auf Basis einer vorkonfigurierten Vorlage. Diese Schnittstelle fungiert während der Dauer der Verbindung als Tunnelendpunkt. Sobald der Tunnel nicht mehr benötigt wird, wird die virtuelle Zugriffsschnittstelle außer Betrieb genommen, wodurch Systemressourcen freigesetzt werden.

- Flexible Bereitstellung:
  - Hub-and-Spoke-Modell: Ein zentraler Hub ist mit mehreren Zweigstellen verbunden. FlexVPN vereinfacht die Einrichtung dieser Verbindungen in einem einzigen Framework und eignet sich somit ideal für große Netzwerke.
  - Vollständige und teilweise vermaschte Topologien: Alle Standorte können direkt miteinander kommunizieren, ohne einen zentralen Hub zu durchlaufen. Dies reduziert Verzögerungen und verbessert die Leistung.

- Hohe Verfügbarkeit und Redundanz:
  - Redundante Hubs: Unterstützt mehrere Hubs für Backups. Wenn ein Hub ausfällt, können Zweigstellen eine Verbindung zu einem anderen Hub herstellen, um eine kontinuierliche Verbindung sicherzustellen.

- Lastenausgleich: Dadurch werden VPN-Verbindungen auf mehrere Geräte verteilt, um eine Überlastung einzelner Geräte zu vermeiden. Dies ist für die Aufrechterhaltung der Leistung in großen Bereitstellungen von entscheidender Bedeutung.



Anmerkung: Der nächste Leitfaden enthält weitere Informationen zur Konfiguration für den Lastenausgleich für die Hubs-Verbindung.

Konfigurieren des IKEv2 Load Balancer

- Skalierbare Authentifizierung und Authentifizierung:
  - AAA-Integration: Kann mit AAA-Servern wie Cisco ISE oder RADIUS für die zentralisierte Verwaltung von Benutzeranmeldeinformationen und -richtlinien verwendet werden, die für eine umfangreiche Nutzung unerlässlich sind.
  - PKI und Zertifikate: Unterstützt die Public Key Infrastructure (PKI) und digitale Zertifikate für eine sichere Authentifizierung, die skalierbarer ist als die Verwendung von Pre-Shared Key, insbesondere in großen Umgebungen.

Routing

Die Routing-Funktionen in FlexVPN sind auf eine verbesserte Skalierbarkeit und ein effizientes Management mehrerer VPN-Verbindungen ausgelegt und ermöglichen eine dynamische Weiterleitung des Datenverkehrs zu jedem einzelnen VPN. Die nächsten wichtigen Komponenten und Mechanismen, die ein effizientes FlexVPN-Routing ermöglichen:

- Schnittstelle für virtuelle Vorlagen: Hierbei handelt es sich um eine Konfigurationsvorlage, die alle erforderlichen Einstellungen für eine VPN-Verbindung enthält, z. B. IP-Adresszuweisung, Tunnelquelle und IPsec-Einstellungen. In dieser Schnittstelle wird der`ip unnumbered`Befehl zum Ausleihen einer IP-Adresse konfiguriert, in der Regel von einem Loopback, anstatt eine bestimmte IP-Adresse als Tunnelquelle zu konfigurieren. Auf diese Weise kann dieselbe Vorlage von jedem Spoke verwendet werden, sodass jeder Spoke seine eigene Quell-IP-Adresse verwenden kann.

- Virtuelle Zugriffsschnittstelle: Dabei handelt es sich um dynamisch erstellte Schnittstellen, die ihre Einstellungen von der Schnittstelle für virtuelle Vorlagen übernehmen. Bei jedem Aufbau einer neuen VPN-Verbindung wird auf Basis der virtuellen Vorlage eine neue virtuelle Zugriffsschnittstelle erstellt. Das bedeutet, dass jede VPN-Sitzung über eine eigene Schnittstelle verfügt, die das Management und die Skalierung vereinfacht.

- Dynamic Routing-Protokolle: Er arbeitet mit Routing-Protokollen wie OSPF, EIGRP und BGP über VPN-Tunnel zusammen. Dadurch werden Routing-Informationen automatisch aktualisiert, was für große und dynamische Netzwerke wichtig ist.

- IKEv2 kündigt Routen an, indem der FlexVPN-Server dem Client Netzwerkattribute per Push zuweist. Diese werden dann auf der Tunnelschnittstelle installiert. Während des Austauschs im Konfigurationsmodus kommuniziert der Client außerdem seine eigenen Netzwerke mit dem Server, wodurch Routenaktualisierungen auf beiden Seiten möglich sind.

- NHRP (Next Hop Resolution Protocol) ist ein Protokoll zur dynamischen Adressauflösung, das in Hub-and-Spoke-Topologien verwendet wird, um privaten VPN-Endpunkten öffentliche IP-Adressen zuzuordnen. Es ermöglicht Stationen, andere Stationen IPs für die direkte Kommunikation zu entdecken.

Autorisierungsrichtlinie

Eine IKEv2-Autorisierungsrichtlinie für FlexVPN kann so konfiguriert werden, dass verschiedene Aspekte der VPN-Verbindung gesteuert werden. Eine IKEv2-Autorisierungsrichtlinie definiert die lokale Autorisierungsrichtlinie und enthält lokale und/oder Remote-Attribute:

- Lokale Attribute wie VPN-Routing und -Weiterleitung (VRF) und die QoS-Richtlinie werden lokal angewendet.
- Remote-Attribute, z. B. Routen, werden über den Konfigurationsmodus an den Peer weitergeleitet.
- Verwenden Sie den Befehl crypto ikev2 authentication policy, um die lokale Richtlinie zu definieren.

- Die IKEv2-Autorisierungsrichtlinie wird vom IKEv2-Profil mithilfe des Befehls AAA-Autorisierung referenziert.

Diese Tabelle bietet einen Überblick über die wichtigsten Parameter, die in der IKEv2-Autorisierungsrichtlinie konfiguriert werden können.

Parameter	Beschreibung
AAA	Integration mit AAA-Servern zur Validierung von Benutzeranmeldeinformationen, zur Autorisierung des Zugriffs und zur Benutzerkontennutzung Die Richtlinie kann angeben, ob die Validierung lokal auf dem Router oder remote erfolgt, z. B. über einen RADIUS-Server.
Client-Konfiguration	Übermittelt Konfigurationseinstellungen an den Client, z. B. Leerlaufzeitüberschreitungswerte, Keepalives, DNS- und WINS-Serverzuweisungen usw.
Client-spezifische Konfiguration	Ermöglicht unterschiedliche Konfigurationen für verschiedene Clients basierend auf ihrer Identität oder Gruppenmitgliedschaft.
Routensatz	Bei dieser Konfiguration kann bestimmter Datenverkehr durch den VPN-Tunnel geleitet werden. Dadurch wird die Route Injection durchgeführt, die bei erfolgreicher Verbindung an den VPN-Client gesendet wird.

FlexVPN im Vergleich zu anderen Technologien

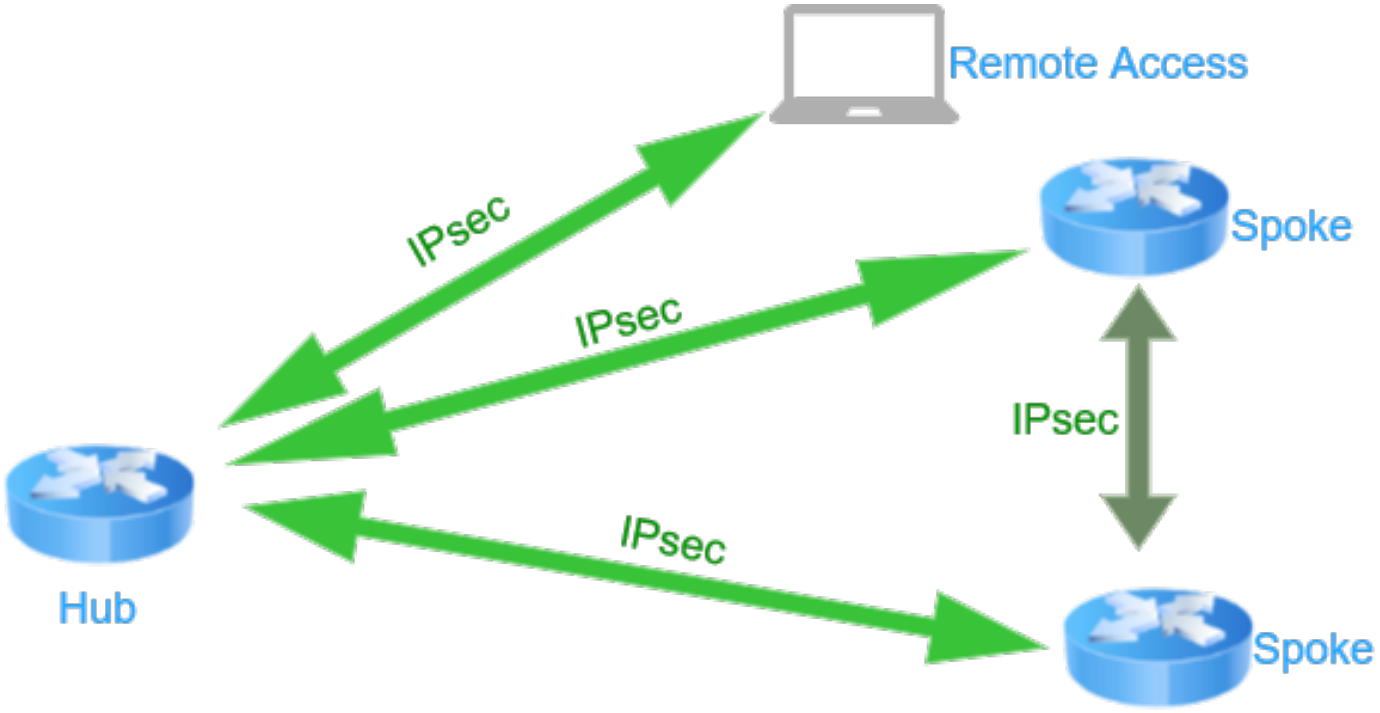
FlexVPN bietet eine Reihe von Vorteilen, die es zu einer attraktiven Wahl für moderne Netzwerkumgebungen machen. Durch die Bereitstellung eines einheitlichen Frameworks vereinfacht FlexVPN die Konfiguration und das Management, erhöht die Sicherheit, unterstützt die Skalierbarkeit, gewährleistet Interoperabilität und reduziert die Komplexität.

	Kryptografieübersicht	DMVPN	FlexVPN
Dynamisches Routing	Nein	Ja	Ja
Dynamisch Spoke-to-Spoke-Direkt	Nein	Ja	Ja
Remote Access-VPN	Ja	Nein	Ja
Push-Konfiguration	Nein	Nein	Ja
Peer-Peer-Konfiguration	Nein	Nein	Ja
Peer-Peer-QoS	Nein	Ja	Ja

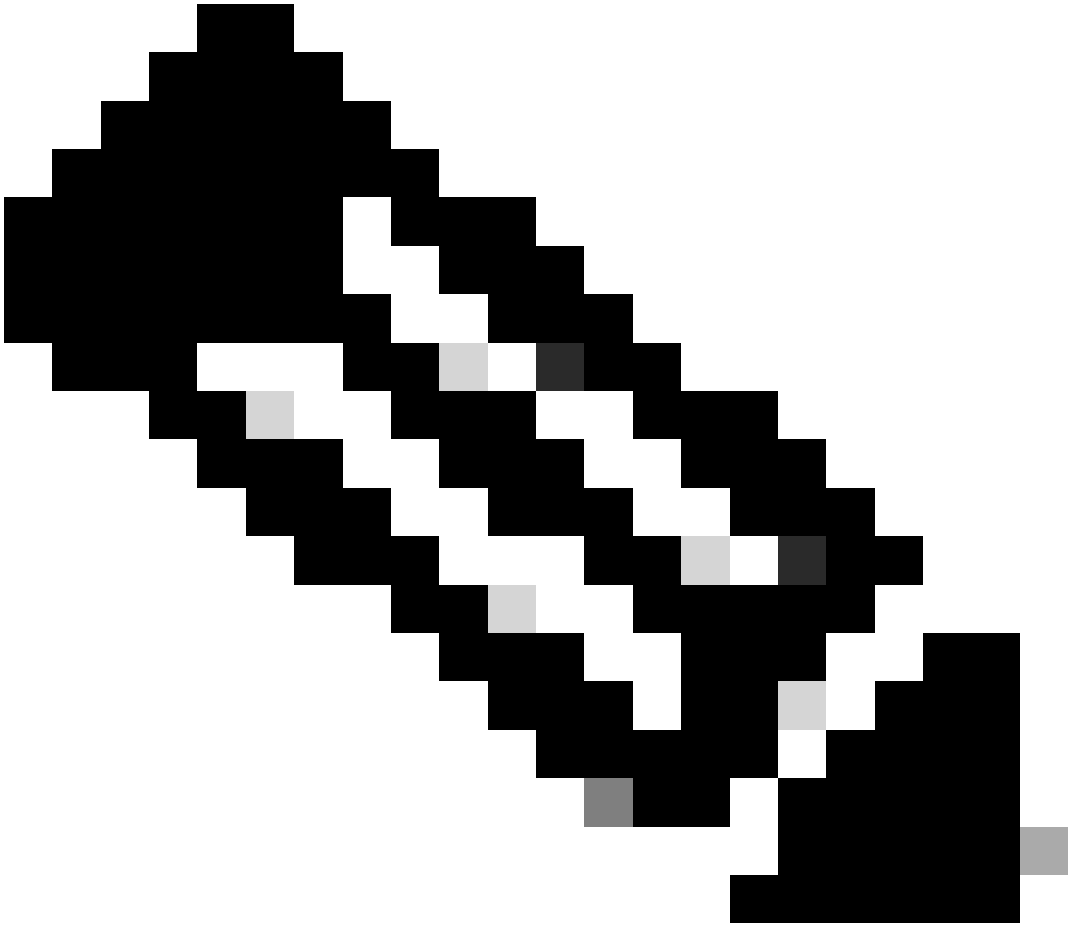
AAA-Serverintegration	Nein	Nein	Ja

Netzwerkdiagramm

FlexVPN ermöglicht die Erstellung von Tunneln zwischen Geräten, um die Kommunikation zwischen Hub und Spokes zu ermöglichen. Es ermöglicht auch die Erstellung von Tunneln für die direkte Kommunikation zwischen Stationen und die Verbindung für Remote Access VPN-Benutzer, wie in der Abbildung dargestellt.



FlexVPN-Diagramm



Anmerkung: Die Konfiguration für Remote Access VPN wird in diesem Leitfaden nicht behandelt. Weitere Informationen zur Konfiguration finden Sie im Leitfaden:

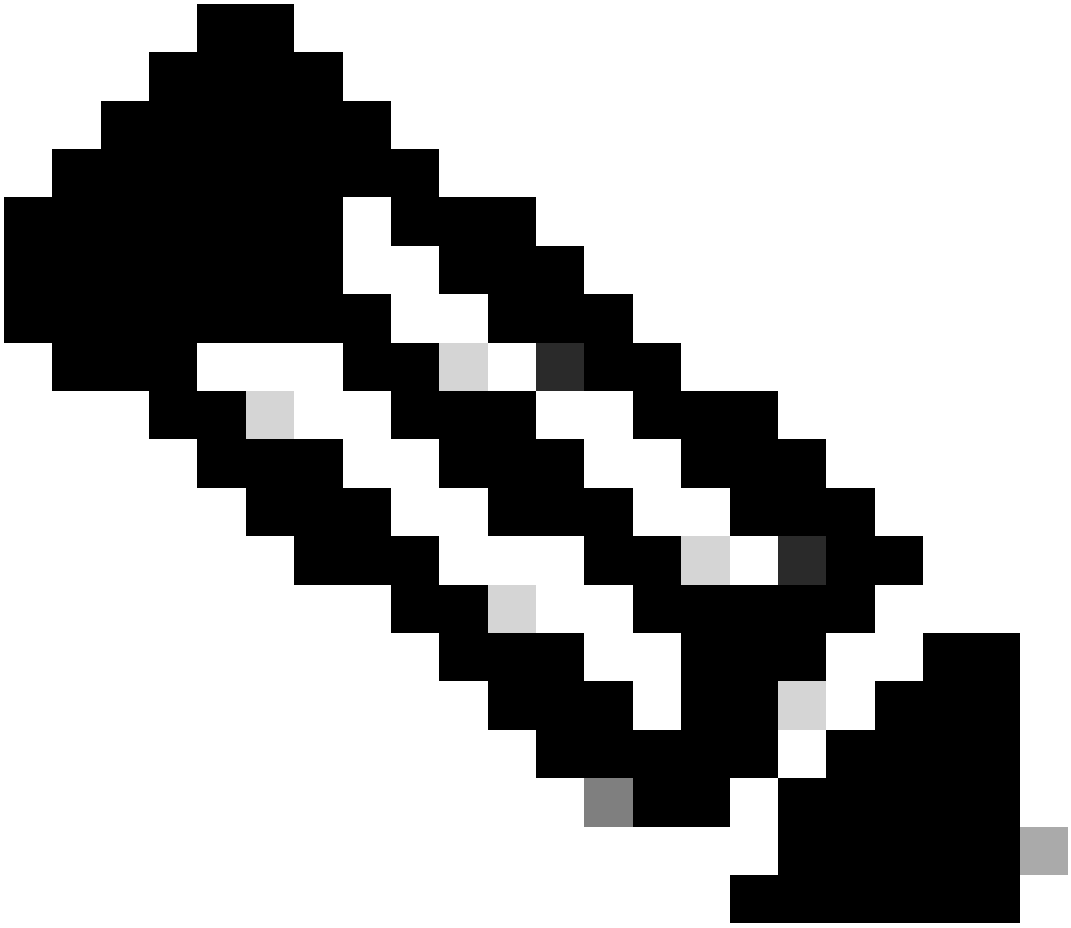
Konfigurieren des FlexVPN-Headends für den sicheren Client (AnyConnect) IKEv2-Remote-Zugriff mithilfe der lokalen Benutzerdatenbank

Konfigurieren

FlexVPN zeichnet sich durch eine einfache Konfiguration aus. Diese Einfachheit wird durch die konsistenten Konfigurationsblöcke deutlich, die für verschiedene Arten von VPNs verwendet werden. FlexVPN bietet einfache Konfigurationsbausteine, die allgemein anwendbar sind, mit optionalen Konfigurationen oder zusätzlichen Schritten, die je nach den spezifischen Merkmalen oder Anforderungen der Topologie verfügbar sind:

- IKEv2-Angebot: Definiert die Algorithmen, die bei der Aushandlung der IKEv2 Security Association (SA) verwendet werden. Hängen Sie dieses Angebot nach der Erstellung an eine IKEv2-Richtlinie an, damit es während der Verhandlung ausgewählt wird.

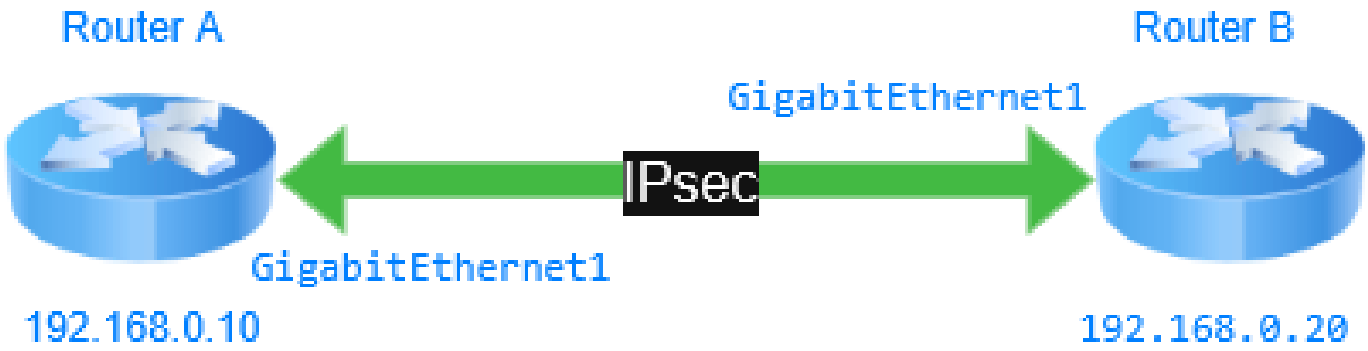
- IKEv2-Richtlinie: Verknüpfen Sie das Angebot mit einer VRF-Instanz (Virtual Routing and Forwarding) oder einer lokalen IP-Adresse. Der Richtlinienlink zum IKEv2-Angebot.
- IKEv2-Keyring: Gibt PSKs (Pre-Shared Keys) an, die asymmetrisch sein können, wenn sie für die Peer-Authentifizierung verwendet werden.
- Vertrauenspunkt (optional): Konfiguriert Identitäts- und Zertifizierungsstellenattribute für die Peer-Authentifizierung, wenn Public Key Infrastructure (PKI) als Authentifizierungsmethode verwendet wird.
- AAA-Integration (optional): FlexVPN integriert AAA-Server wie die Cisco ISE (Identity Services Engine) oder RADIUS-Server als Authentifizierungsmethode.
- IKEv2-Profil: Speichert nicht übertragbare Parameter der IKE SA, z. B. die VPN-Peer-Adresse und die Authentifizierungsmethoden. Es gibt kein IKEv2-Standardprofil. Daher müssen Sie es konfigurieren und an ein IPsec-Profil auf dem Initiator anhängen. Wenn die PSK-Authentifizierung verwendet wird, verweist das IKEv2-Profil auf den IKEv2-Keyring. Wenn eine PKI- oder AAA-Authentifizierungsmethode verwendet wird, wird hier verwiesen.
- IPsec-Transformationssatz: Gibt eine Kombination von Algorithmen an, die für die IPsec-Sicherheitszuordnung zulässig sind.
- IPsec-Profil: Konsolidiert FlexVPN-Einstellungen in einem Profil, das auf eine Schnittstelle angewendet werden kann. Dieses Profil verweist auf den IPsec-Transformationssatz und das IKEv2-Profil.



Anmerkung: In den Konfigurationsbeispielen werden vorinstallierte Schlüssel verwendet, um die einfache FlexVPN-Konfiguration darzustellen. Pre-Shared Keys können für eine einfache Bereitstellung und kleinere Topologien verwendet werden, AAA- oder PKI-Methoden eignen sich jedoch besser für größere Topologien.

Standortübergreifende FlexVPN-Konfiguration

Die FlexVPN-Site-to-Site-Topologie ist für direkte VPN-Verbindungen zwischen zwei Standorten ausgelegt. Jeder Standort ist mit einer Tunnelschnittstelle ausgestattet, die einen sicheren Kanal für den Datenverkehr bereitstellt. In der Konfiguration wird erläutert, wie eine direkte VPN-Verbindung zwischen zwei Standorten hergestellt wird, wie im Diagramm gezeigt.



Site-to-Site-Diagramm

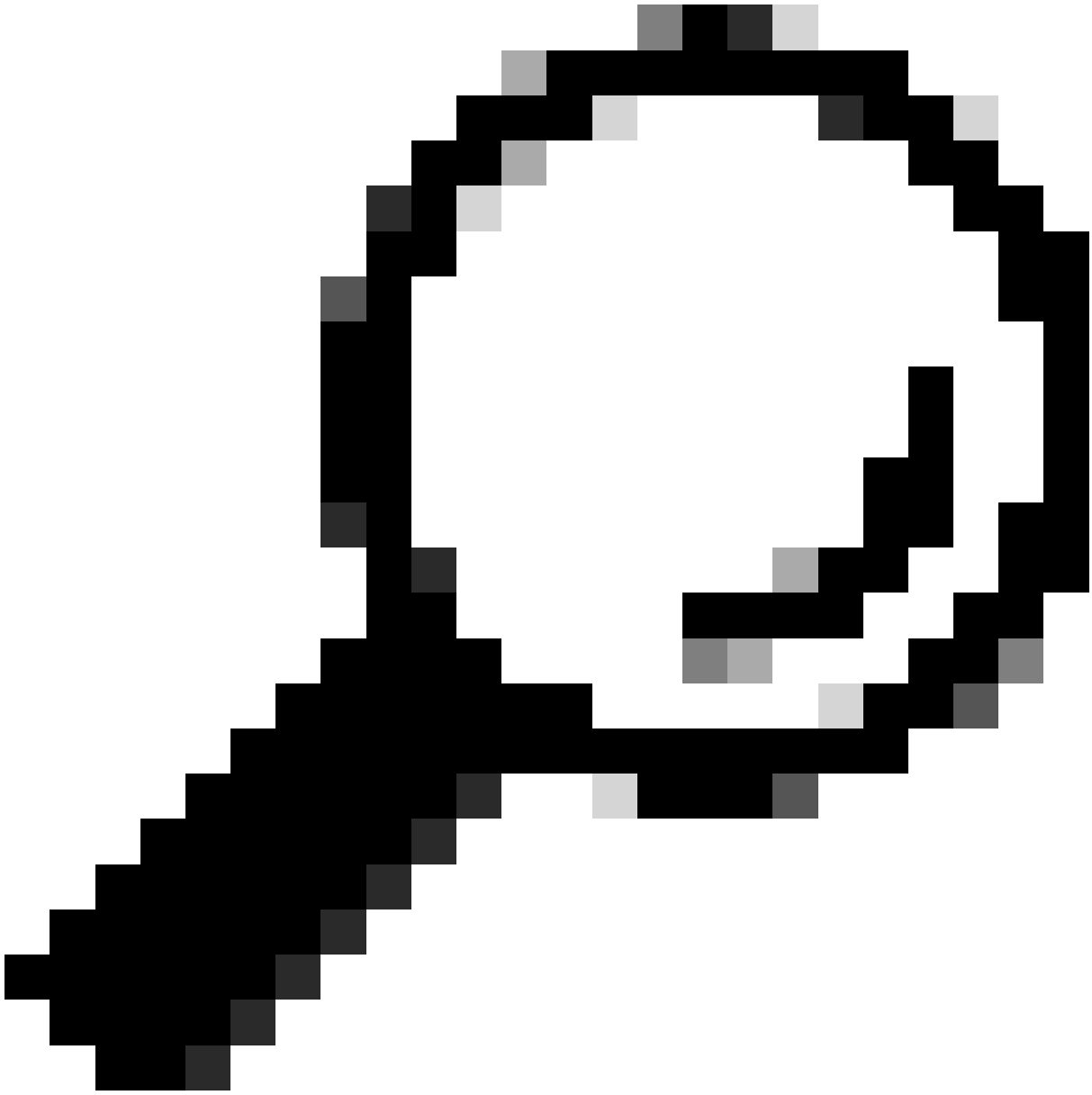
Schritt 1: Konfiguration von Router A

antwort: Definition von IKEv2-Angebot und -Richtlinie.

b. Konfigurieren Sie einen Keyring, und geben Sie einen Pre-Shared Key ein, der zur Authentifizierung des Peers verwendet wird.

c. Erstellen Sie eine IKEv2 profile , und weisen Sie die zu keyring.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



Tipp: Die **IKEv2 Smart Defaults** Funktion minimiert dieFlexVPNKonfiguration, da sie die meisten Anwendungsfälle abdeckt. Sie können diese Vorgehensweise **IKEv2 Smart Defaults** für bestimmte Anwendungsfälle anpassen, Cisco empfiehlt sie jedoch nicht.

d. Erstellen Sie einen Transport Set und definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

e. Erstellen Sie eine **IPsec profile.**

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
```

```
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Konfigurieren Sie die Tunnelschnittstelle.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g. Konfigurieren Sie dynamisches Routing, um die Tunnelschnittstelle anzukündigen. Danach kann es andere Netzwerke ankündigen, die den Tunnel passieren müssen.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Phase 2: Router B-Konfiguration

antwort: Definition von IKEv2-Angebot und -Richtlinie.

b. Konfigurieren Sie eine keyring , und geben Sie eine einPre-Shared Key, die zur Authentifizierung des Peers verwendet wird.

c. Erstellen Sie eine IKEv2 profile , und weisen Sie die zu keyring.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
```

```
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

d. Erstellen Sie einen Transport Set und definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

e. Erstellen Sie ein IKEv2-Profil, IPsec profile und weisen Sie es sowie den zuvor erstellten Transformationssatz zu.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Konfigurieren Sie die Tunnel interface.

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g. Konfigurieren Sie dynamisches Routing, um die Tunnelschnittstelle anzukündigen. Danach kann es andere Netzwerke ankündigen, die den Tunnel passieren müssen.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Überprüfung

- Verwenden Sie den Befehl show ip interface brief, um den Tunnelschnittstellenstatus zu überprüfen und zu überprüfen, ob der Tunnel betriebsbereit ist.

<#root>

```
RouterB#
```

```
show ip interface brief
```

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

```
up
```

```
 up
```

1. Verwenden Sie den Befehl show crypto ikev2 sa, um sicherzustellen, dass die sichere Verbindung zwischen den Routern hergestellt ist.

<#root>

```
RouterB#
```

```
show crypto ikev2 sa
```

```
IPv4 Crypto IKEv2 SA

Tunnel-id  Local                Remote               fvrf/ivrf   Status
2          192.168.0.20/500     192.168.0.10/500     none/none
```

```
READY
```

```
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

```
Life/Active Time: 86400/3139 sec
```

```
IPv6 Crypto IKEv2 SA
```

- Verwenden Sie den Befehl show crypto ipsec sa, um zu bestätigen, dass der Datenverkehr verschlüsselt ist und durch den Tunnel fließt, indem Sie überprüfen, ob die Zähler für Encaps und Decaps inkrementiert werden.

<#root>

```
RouterB#
show crypto ipsec sa


interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #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.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
```

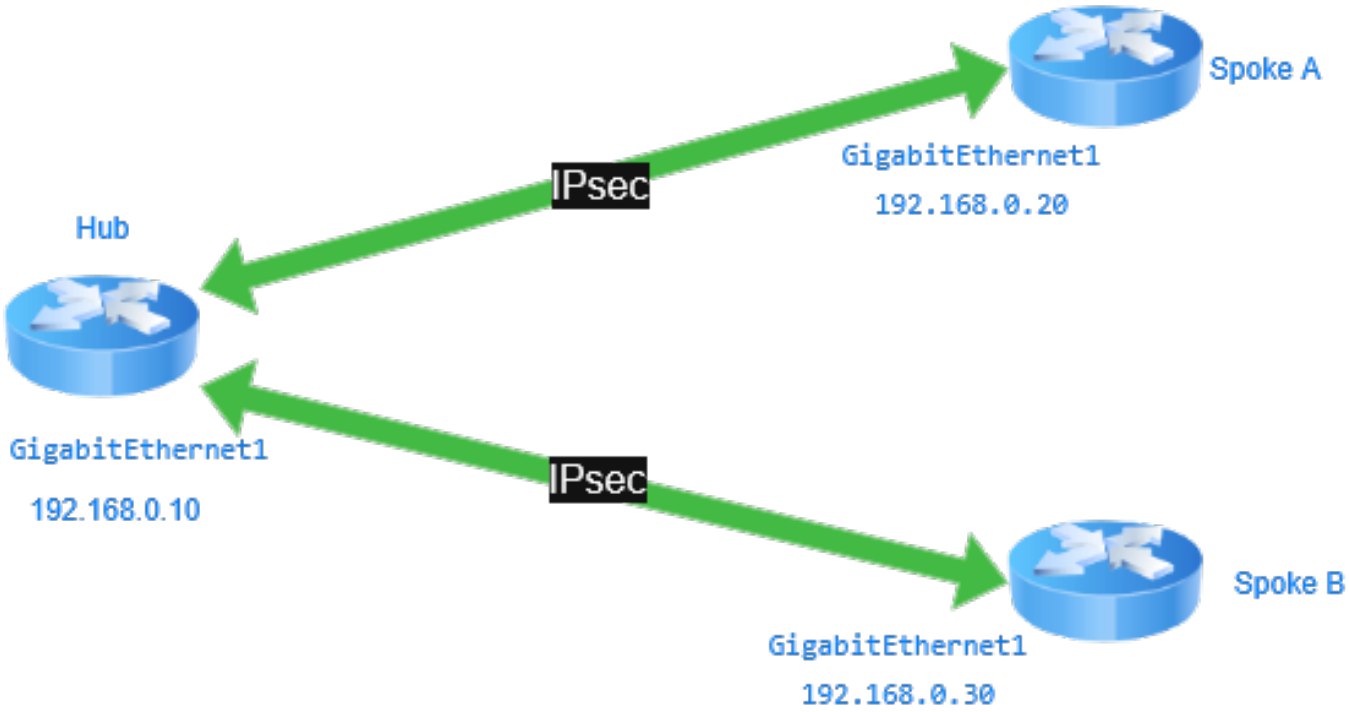
```
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4607991/3137)

         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)

      outbound ah sas:

      outbound pcp sas:
```

- Verwenden Sie den Befehl show ip eigrp neighbors, um sicherzustellen, dass die EIGRP-Adjacency für den anderen Standort eingerichtet ist.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

Hub-and-Spoke-FlexVPN

In der Hub-and-Spoke-Topologie sind mehrere Spoke-Router mit einem zentralen Hub-Router verbunden. Diese Konfiguration ist optimal für Szenarien, in denen Stationen primär mit dem Hub kommunizieren. In FlexVPN können dynamische Tunnel konfiguriert werden, um die Kommunikationseffizienz zu verbessern. Der Hub verwendet IKEv2-Routing, um Routen zu Spoke-Routern zu verteilen und so eine nahtlose Konnektivität sicherzustellen. Wie im Diagramm dargestellt, wird in der Konfiguration die VPN-Verbindung zwischen einem Hub und Spoke erläutert und erläutert, wie der Hub so konfiguriert ist, dass er eine dynamische Verbindung mit mehreren Spokes herstellt und weitere Spokes hinzufügen kann.



Hub_and_Spoke_Diagramm

Schritt 1: Hub-Konfiguration

antwort: Definition von IKEv2-Angebot und -Richtlinie.

b. Konfigurieren Sie eine keyring , und geben Sie eine einPre-Shared Key, die zum Authentifizieren der Stationen verwendet wird.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Aktivieren Sie AAA-Dienste auf dem Hub-Router, und definieren Sie dann eine Netzwerkautorisierungsliste mit dem NamenFlexAuthHub, die Richtlinien aus der Konfiguration des lokalen Geräts angibt.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieren Sie eine IP address poolbenannte Adresse, FlexPooldie die Adressen 10.1.1.2 bis 10.1.1.254 enthält. Dieser Pool wird verwendet, um der Tunnelschnittstelle der Stationen automatisch eine IP-Adresse zuzuweisen.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Definieren Sie eine Standard-IP-Zugriffsliste, die den Namen trägt FlexTrafficund das Netzwerk 10.10.1.0/24 zulässt. Diese ACL definiert die Netzwerke, die an die FlexVPN-Stationen weitergeleitet werden, um sie durch den Tunnel zu erreichen.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

Auf die Zugriffsliste und den IP-Adresspool wird im verwiesen **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Erstellen Sie eine IKEv2 profile, und weisen Sie die Autorisierungsgruppe keyring und die AAA-Autorisierungsgruppe zu.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
```

```
!
```

g. Erstellen Sie einen Transport Set, definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

h. Erstellen Sie eine IPsec profile, weisen Sie die IKEv2 profile und die Transport Set zuvor erstellten zu.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Konfigurieren Sie die **virtual-template 1** as **type tunnel**. Verweisen Sie auf die Schnittstelle als ‚IP unnumbered addressund wenden Sie die **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Phase 2: Spoke-Konfiguration

antwort: Definition von IKEv2-Angebot und -Richtlinie.

b. Konfigurieren Sie einen Keyring, und geben Sie einen Pre-Shared Key ein, der für die Authentifizierung am Hub verwendet wird.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
```

```
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Aktivieren Sie AAA-Dienste auf dem Hub-Router, und definieren Sie dann eine Netzwerkautorisierungsliste mit dem Namen , **FlexAuth** die Richtlinien aus der Konfiguration des lokalen Geräts angibt. Konfigurieren Sie als Nächstes die Richtlinie für die Moduskonfiguration, um die IP-Adresse und die Routen zu den FlexVPN-Stationen zu übertragen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieren Sie eine Standard-IP-Zugriffsliste mit dem Namen **FlexTraffic** und der Berechtigung für das Netzwerk 10.20.2.0/24. Diese ACL definiert die Netzwerke, die von dieser Station gemeinsam genutzt werden, um den Tunnel zu passieren.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

Die Zugriffsliste wird in der zugewiesen **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Erstellen Sie eine IKEv2 profile, weisen Sie die Autorisierungsgruppe keyring und die AAA-Autorisierungsgruppe zu.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f. Erstellen Sie ein Transport Set, und definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

g. Erstellen Sie ein IPsec-Profil, weisen Sie das IKEv2-Profil und den zuvor erstellten Transportsatz zu.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Konfigurieren Sie die Tunnelschnittstelle mit der Eigenschaft der ausgehandelten IP-Adresse, die aus dem Pool abgerufen wird, den sie auf dem Hub konfiguriert hat.

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Überprüfung

Verwenden Sie den Befehl show ip interface brief, um den Status "Tunnel", "Virtual-Template" und "Virtual-Access" zu überprüfen:

- Auf dem Hub hat die virtuelle Vorlage den Status "up/down", was normal ist. Für jeden Spoke, der eine Verbindung mit dem Hub herstellt, wird ein Virtual-Access erstellt, der einen "up/up"-Status anzeigt.
- Auf dem Spoke hat die Tunnelschnittstelle eine IP-Adresse empfangen und zeigt den Status "up/up" an.

<#root>

```
FlexVPN_HUB#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up

Virtual-Access1        10.1.1.1        YES unset  up               up

 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up


FlexVPN_Spoke#

show ip interface brief

Interface              IP-Address      OK? Method  Status            Protocol
GigabitEthernet1       192.168.0.20    YES NVRAM   up                up
GigabitEthernet2       10.20.2.20      YES manual  up                up

Tunnel0                10.1.1.8        YES manual  up                up <<<<<<

The tunnel interface received an IP address from pool defined
```

- Verwenden Sie den Befehl show crypto ikev2 sa, um sicherzustellen, dass die sichere Verbindung zwischen Hub und Spoke hergestellt ist.

<#root>

```
FlexVPN_HUB#

show crypto ikev2 sa

 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none

READY

 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec


 IPv6 Crypto IKEv2 SA
```

- Verwenden Sie den Befehl show crypto ipsec sa, um zu bestätigen, dass der Datenverkehr verschlüsselt ist und durch den Tunnel fließt, indem Sie überprüfen, ob die Zähler für Encaps und Decaps inkrementiert werden.

<#root>

```
FlexVPN_HUB#
show crypto ipsec sa

interface: Virtual-Access1

    Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   current_peer 192.168.0.20 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

    #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.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xAFC2F841(2948790337)
     PFS (Y/N): N, DH group: none

     inbound esp sas:

spi: 0x7E780336(2121794358)

        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h

sa timing: remaining key lifetime (k/sec): (4607998/3010)

        IV size: 16 bytes
        replay detection support: Y

Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
```

```
spi: 0xAFC2F841(2948790337)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-

sa timing: remaining key lifetime (k/sec): (4607998/3010)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      outbound ah sas:

      outbound pcp sas:
```

- Verwenden Sie den Befehl show ip route, um zu überprüfen, ob die Routen zu den Stationen weitergeleitet wurden:
  - Die Route für 10.1.1.1/32 wurde aufgrund der Routensatz-Schnittstellenanweisung in der HUB-Konfiguration über IKEv2-Konfigurations-Payloads per Push übertragen.
  - Die Route für 10.10.1.0/24 wurde aufgrund der FlexTraffic-Anweisung in der HUB-Konfiguration der Route Set-Zugriffsliste über die IKEv2-Konfigurations-Payloads per Push übertragen.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- Verwenden Sie den Befehl ping, um die Verbindung zu den angekündigten Netzwerken zu überprüfen.

<#root>

```
FlexVPN_HUB#
```

ping 10.20.2.20

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
FlexVPN_Spoke#
```

ping 10.10.1.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Spoke zu Spoke FlexVPN

FlexVPN in Hub-and-Spoke-Topologie mit Spoke-to-Spoke-Verbindungen ermöglicht eine dynamische, skalierbare und sichere VPN-Kommunikation. Der Hub fungiert als zentraler Kontrollpunkt, an dem NHRP Spokes den Hub nach anderen Spoke-IP-Adressen abfragen lässt. Dadurch werden direkte Spoke-to-Spoke-IPsec-Tunnel für eine effiziente Kommunikation und eine reduzierte Latenz ermöglicht.

Auf dem Hub wird der **ip nhrp redirect** Befehl verwendet, um Spokes darüber zu informieren, dass eine direkte Spoke-to-Spoke-Kommunikation möglich ist. Dadurch wird der Datenverkehrsfluss optimiert, da der Hub für Datenverkehr auf Datenebene umgangen wird. Bei Stationen ermöglicht der **ip nhrp shortcut** Befehl ihnen, nach dem Empfang der Umleitung vom Hub dynamisch direkte Tunnel zu anderen Stationen aufzubauen. Das Diagramm zeigt den Datenverkehr zwischen Hub und Spoke sowie die Kommunikation zwischen Spoke und Spoke.

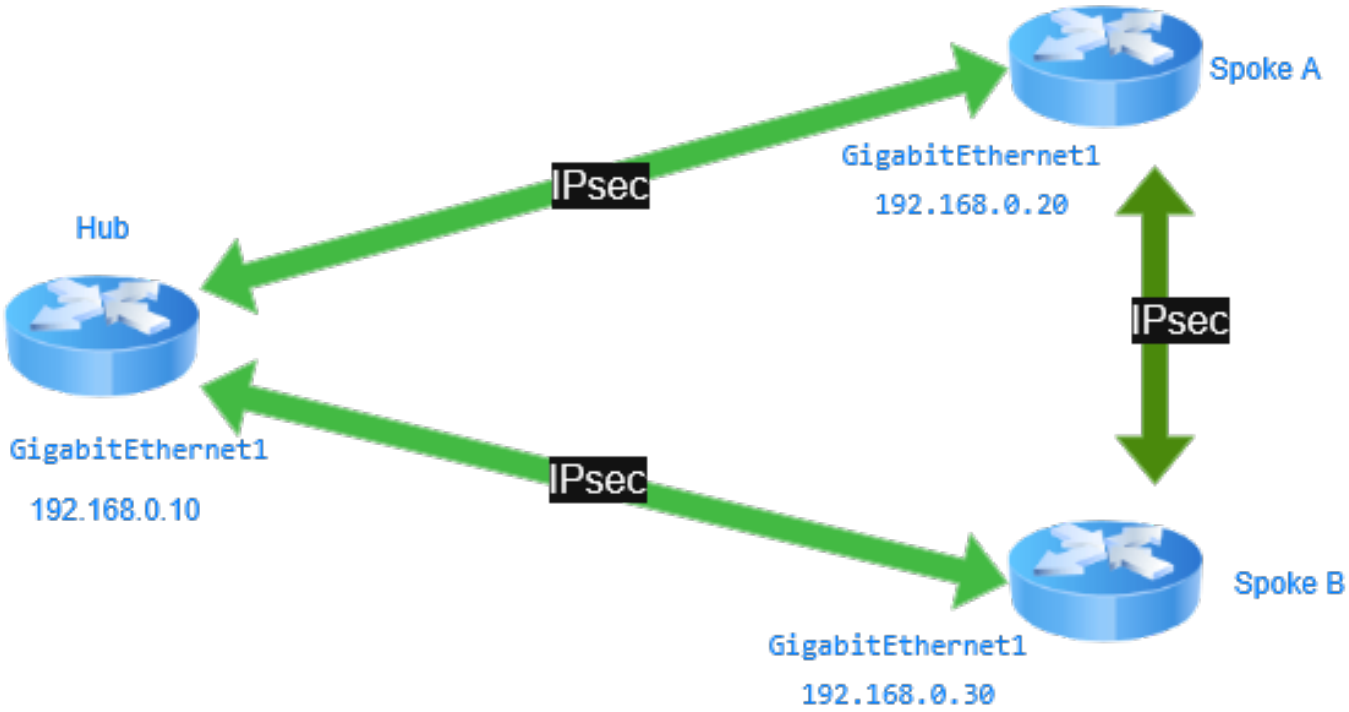


Diagramm der Speichen-zu-Speichen

Schritt 1: Hub-Konfiguration

antwort: IKEv2-Richtlinien und -Profile definieren.

b. Konfigurieren Sie eine keyring , und geben Sie eine einPre-Shared Key, die zum Authentifizieren der Stationen verwendet wird.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

FlexAuth c. Aktivieren Sie die AAA-Dienste auf dem Hub-Router, definieren Sie dann eine Netzwerkautorisierungsliste mit dem Namen , in der Richtlinien aus der Konfiguration des lokalen Geräts angegeben sind, und konfigurieren Sie dann die Richtlinie für die Moduskonfiguration, um die IP-Adresse und die Routen an die FlexVPN-Stationen weiterzuleiten.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieren Sie eine IP address pool benannte Adresse, **FlexPool**, die die Adressen 10.1.1.2 bis 10.1.1.254 enthält. Dieser Pool wird verwendet, um der Tunnelschnittstelle der Stationen automatisch eine IP-Adresse zuzuweisen.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Definieren Sie eine Standard-IP-Zugriffsliste, die den Namen trägt FlexTraffic und das Netzwerk 10.0.0.0/8 zulässt. Diese ACL definiert die Netzwerke, die an die FlexVPN-Stationen weitergeleitet werden, einschließlich der Netzwerke für andere Stationen, die mit dem Hub verbunden sind, sodass die Stationen wissen, dass diese Netzwerke zuerst über den Hub erreicht werden.

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

Die Zugriffslisten und IP address pool werden in der zugewiesen **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Erstellen Sie eine IKEv2 profile, weisen Sie die Autorisierungsgruppe keyring und die AAA-Autorisierungsgruppe zu.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
```

```
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. Erstellen Sie einen Transport Set und definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

h. Erstellen Sie eine IPsec profile, weisen Sie die zu IKEv2 profile und Transport Set zuvor erstellt.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Konfigurieren Sie die **virtual-template 1** as **type tunnel**. Verweisen Sie auf die Schnittstelle als **IP unnumbered address** , und wenden Sie die **IPsec profile**an.

Der **ip nhrp redirect** Befehl wird auf der virtuellen Vorlage konfiguriert, um die Stationen zu informieren, dass eine direkte Verbindung mit anderen Stationen hergestellt werden muss, um ihre Netzwerke zu erreichen.

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Phase 2: Konfiguration von Spoke A

antwort: IKEv2-Richtlinien und -Profile definieren.

b. Konfigurieren Sie eine keyring , und geben Sie eine einPre-Shared Key, die zum Authentifizieren der Stationen verwendet wird.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
```

```
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Aktivieren Sie AAA-Dienste auf dem Hub-Router, und definieren Sie dann eine Netzwerkautorisierungsliste mit dem Namen , **FlexAuth** die Richtlinien aus der Konfiguration des lokalen Geräts angibt. Konfigurieren Sie als Nächstes die Richtlinie für die Moduskonfiguration, um die IP-Adresse und die Routen zu den FlexVPN-Stationen zu übertragen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieren Sie eine Standard-IP-Zugriffsliste mit dem Namen **FlexTraffic** und der Berechtigung für das Netzwerk 10.20.2.0/24. Diese ACL definiert die Netzwerke, die von dieser Station gemeinsam genutzt werden, um den Tunnel zu passieren.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

Die Zugriffsliste wird im **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Erstellen Sie eine IKEv2 profile, weisen Sie die Autorisierungsgruppe keyring und die AAA-Autorisierungsgruppe zu.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Erstellen Sie einen Transport Set und definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

g. Erstellen Sie ein IPsec-Profil, weisen Sie das IKEv2-Profil und den zuvor erstellten Transportsatz zu.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Konfigurieren Sie die Tunnelschnittstelle und die virtuelle Vorlage. Geben Sie **Virtual-Template1** an, welche dVTIs unterstützt werden sollen **NHRP shortcuts**. Legen Sie außerdemtunnel0als nicht nummerierte Adresse auf demvirtual-templatefest.

Der **ip nhrp shortcut** Befehl wird auf den Spokes konfiguriert, damit diese basierend auf NHRP-Umleitungsnachrichten vom Hub dynamisch direkte Tunnel zu anderen Spokes einrichten können.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Schritt 3: Konfiguration von Spoke B

antwort: IKEv2-Richtlinien und -Profile definieren.

b. Konfigurieren Sie eine keyring , und geben Sie eine einPre-Shared Key, die zum Authentifizieren der Stationen verwendet wird.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Aktivieren Sie AAA-Dienste auf dem Hub-Router, definieren Sie dann eine Netzwerkautorisierungsliste mit dem Namen , die Richtlinien aus der Konfiguration des lokalen Geräts **FlexAuth** angibt, und konfigurieren Sie dann die Richtlinie für die Moduskonfiguration, um die IP-Adresse und die Routen an die FlexVPN-Spokes zu übertragen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieren Sie eine benannte Standard-IP-Zugriffsliste, die das Netzwerk **FlexTraffic** zulässt.10.30.3.0/24. Diese ACL definiert die Netzwerke, die von dieser Station gemeinsam genutzt werden, um durch den Tunnel zu gelangen.

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

Auf die Zugriffsliste wird im IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Erstellen Sie eine IKEv2 profile, weisen Sie die Autorisierungsgruppe keyring und die AAA-Autorisierungsgruppe zu.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Erstellen Sie einen Transport Set und definieren Sie die Verschlüsselungs- und Hash-Algorithmen, die zum Schutz von Daten verwendet werden.

g. Erstellen Sie eine IPsec profile, weisen Sie die IKEv2 profile und Transport Set zuvor erstellt.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Konfigurieren Sie das tunnel interface und virtual template. Geben Sie **Virtual-Template1** die zu unterstützenden dVTIs an NHRP shortcuts. Legen Sie außerdemtunnel0als nicht nummerierte Adresse auf demvirtual-templatefest.

Der **ip nhrp shortcut** Befehl wird auf den Spokes konfiguriert, damit diese basierend auf NHRP-Umleitungsnachrichten vom Hub dynamisch direkte Tunnel zu anderen Spokes einrichten können.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
```

```
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

Überprüfung

Verwenden Sie den Befehl show ip interface brief, um den Status "Tunnel", "Virtual-Template" und "Virtual-Access" zu überprüfen. Jetzt besteht eine direkte Spoke-to-Spoke-Verbindung:

- Auf den Spokes hat die virtuelle Vorlage den normalen Up/Down-Status. Ein Virtual-Access wird für eine Verbindung im Up/Up-Status erstellt.

<#root>

```
FlexVPN_Spoke#

show ip interface brief


Interface                  IP-Address      OK?  Method  Status                Protocol
GigabitEthernet1           192.168.0.30    YES  NVRAM   up                    up
GigabitEthernet2           10.20.2.20      YES  manual  up                    up

Tunnel0                    10.1.1.12       YES  manual  up                    up


Virtual-Access1            10.1.1.12       YES  unset   up                    up

Virtual-Template1          10.1.1.12       YES  unset   up                    down
```

- Verwenden Sie den Befehl show crypto ikev2 sa, um sicherzustellen, dass die sichere Verbindung zwischen den einzelnen Geräten hergestellt ist.
- Verwenden Sie den Befehl show crypto ipsec sa, um zu bestätigen, dass der Datenverkehr verschlüsselt ist und durch den Tunnel fließt, indem Sie überprüfen, ob die Zähler für Encaps und Entcaps inkrementiert werden.
- Verwenden Sie den Befehl show ip nhrp, um die Umleitung des Datenverkehrs zwischen den Stationen zu überprüfen.
  <#root>

  ```
  FlexVPN_Spoke#

  show ip nhrp
  ```

```
      10.1.1.10/32 via 10.1.1.10
         Virtual-Access1 created 00:00:13, expire 00:09:46
         Type:

      dynamic

      , Flags: router nhop rib nho
         NBMA address: 192.168.0.30

      10.30.3.0/24 via 10.1.1.10


         Virtual-Access1 created 00:00:13, expire 00:09:46
         Type:

      dynamic

      , Flags: router rib nho
         NBMA address: 192.168.0.30
```

Verwenden Sie den Befehl show ip route, um zu überprüfen, ob die Routen zum Spoke weitergeleitet wurden:

- Die beiden Routen, die der Virtual-Access1-Schnittstelle zugeordnet sind, sind neu und den NHRP-Verknüpfungen zugeordnet.
- Das Zeichen % gibt eine Next-Hop-Außerkraftsetzung an.

<#root>

```
FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0

S  %     10.1.1.10/32 is directly connected, Virtual-Access1


C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2

S  %     10.30.3.0/24 is directly connected, Virtual-Access1


      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- Verwenden Sie den Befehl ping, um die Verbindung zu den angekündigten Netzwerken zu überprüfen.

<#root>

```
FlexVPN_Spoke#

ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!


Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration. Verwenden Sie die folgenden Befehle, um den Tunnelaushandlungsprozess zu debuggen:

debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states

NHRP-Fehlerbehebungen können bei der Fehlerbehebung von Spoke-to-Spoke-Verbindungen helfen.

debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing

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.