Configuring FlexVPN Spoke to Spoke

Last Published Date: March 28, 2014

The FlexVPN Spoke to Spoke feature enables a FlexVPN client to establish a direct crypto tunnel with another FlexVPN client leveraging virtual tunnel interfaces (VTI), Internet Key Exchange Version 2 (IKEv2), and Next Hop Resolution Protocol (NHRP) to build spoke-to-spoke connections.

- Finding Feature Information, on page 1
- Prerequisites for FlexVPN Spoke to Spoke, on page 1
- Information About FlexVPN Spoke to Spoke, on page 2
- How to Configure FlexVPN Spoke to Spoke, on page 4
- Configuration Examples for FlexVPN Spoke to Spoke, on page 11
- Additional References for Configuring FlexVPN Spoke to Spoke, on page 16
- Feature Information for FlexVPN Spoke to Spoke, on page 17

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for FlexVPN Spoke to Spoke

IKEv2, the FlexVPN server, and the FlexVPN spoke must be configured.

Information About FlexVPN Spoke to Spoke

FlexVPN and NHRP

FlexVPN is Cisco's implementation of the IKEv2 standard featuring a unified paradigm and CLI that combines site to site, remote access, hub and spoke topologies and partial meshes (spoke to spoke direct). FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm while remaining compatible with legacy VPN implementations using the crypto maps.

The FlexVPN server provides the server side functionality of FlexVPN. The FlexVPN client establishes a secure IPsec VPN tunnel between a FlexVPN client and another FlexVPN server.

NHRP is an Address Resolution Protocol (ARP)-like protocol that alleviates nonbroadcast multiaccess (NBMA) network problems. With NHRP, NHRP entities attached to an NBMA network dynamically learn the NBMA address of the other entities that are part of that network, allowing these entities to directly communicate without requiring traffic to use an intermediate hop.

The FlexVPN Spoke to Spoke feature integrates NHRP and FlexVPN client (spoke) to establish a direct crypto channel with another client in an existing FlexVPN network. The connections are built using virtual tunnel interfaces (VTI), IKEv2 and NHRP, where NHRP is used for resolving the FlexVPN clients in the network.

The following is recommended in FlexVPN:

- Routing entries are not exchanged between spokes.
- Different profiles are used for the spokes and the **config-exchange** command is not configured for the spokes.

The FlexVPN IPv6 Direct Spoke to Spoke feature supports the use of IPv6 addresses for FlexVPN spokes. The support for IPv6 addresses provides support for IPv6 over IPv4, IPv4 over IPv6, and IPv6 over IPv6 transports.

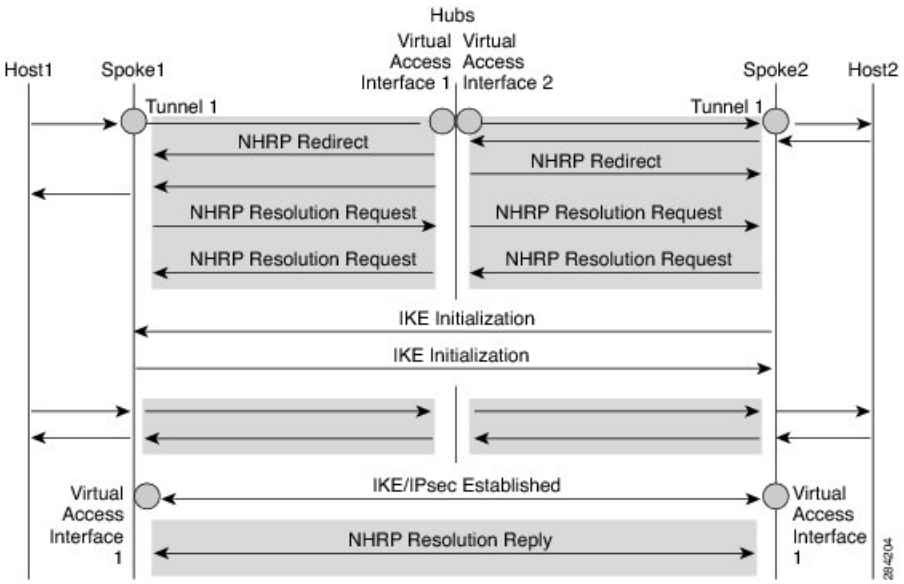
The Multiple FlexVPN Spokes Behind a Single NAT Device feature supports multiple spokes behind a Network Address Translation (NAT) device on FlexVPN.

Note Spoke to Spoke FlexVPN does not support dynamic AAA authorization.

NHRP Resolution Request and Reply in FlexVPN

The following diagram illustrates the NHRP resolution request and reply in FlexVPN.

Figure 1: NHRP Resolution Request and Reply



Due to bidirectional traffic, similar events occur in both directions at Spoke1, Spoke2, and hub. For clarity, events from Host1 to Host2 are discussed. Assume that there is a network N1 (192.168.1.0/24) behind Spoke1 and another network N2 (192.168.2.0/24) behind Spoke2. The network between the two spokes is matched through an access control list (ACL). This is because ACLs are applied on the IKEv2 policies on both spokes.

The network along with its prefix information from both the spokes is conveyed to the hub via IKEv2 information payload exchanges. This causes a route addition in the routing table by IKEv2 at the hub as follows:

- 192.168.1.0/24—Connected via virtual access interface1
- 192.168.2.0/24—Connected via virtual access interface2

The hub will push a summarized route via IKEv2 to both spokes, and the spokes will install the route in their routing table as follows:

- 192.168.0.0/16—next hop <tunnel address of the hub> - interface Tunnel 1

Note The routing protocol can also add the route to the routing table.

Assuming that traffic moves from N1 to N2, the traffic flow is as follows:

1. Host1 sends traffic destined to Host2. The traffic reaches the LAN interface of spoke1, looks up the route, hits the summarized route, and routes the packet to interface tunnel 1.
2. When the traffic reaches the hub's virtual access interface1, the traffic looks up the route table for a route entry for N2, either directly connected over virtual access interface 2 or via a point-to-point tunnel interface.
3. The traffic from Host1 to Host2 traverses the hub through virtual access interface1 and virtual access interface2. The hub determines that ingress and the egress interfaces (virtual access interface1 and virtual access interface2) belong to same NHRP network (network D configured on both the interfaces). The hub sends out an NHRP redirect message to spoke1 on virtual access interface1.

4. On receiving the redirect, Spoke1 initiates a resolution request for Host2 over the point-to-point tunnel interface (the same interface over which it received the redirect). The resolution request traverses the routed path (Spoke1-hub-spoke2). On receiving the resolution request, Spoke2 determines that it is the exit point and needs to respond to the resolution request.
5. Spoke2 receives the resolution request on the tunnel interface and retrieves the virtual template number from the tunnel interface. The virtual template number is used to create the virtual access interface to start a crypto channel and establishes IKEv2 and IPsec security associations (SAs). Once the crypto SAs between the two spokes are up, Spoke2 installs the necessary NHRP cache entries for Spoke1 and its network under the newly created virtual access interface and sends out the resolution reply over the virtual access interface.
6. After receiving the resolution request over the virtual access interface, Spoke1 installs the necessary cache entries for Spoke2 and its network. Spoke1 also deletes the temporary cache entry pointing to the hub to resolve the network under tunnel interface1.
7. NHRP adds shortcut routes as next-hop override (NHO) or H route. For more information on shortcut switching, refer to Shortcut Switching Enhancements for NHRP in DMVPN Networks.

How to Configure FlexVPN Spoke to Spoke

Configuring the Virtual Tunnel Interface on the FlexVPN Server

Before you begin

The FlexVPN server and client must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type tunnel**
4. **ip unnumbered loopback** *number*
5. Do one of the following:
   - **ip nhrp network-id** *number*
   - **ipv6 nhrp network-id** *number*
6. **ip nhrp redirect** [**timeout** *seconds*]
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **type tunnel** **Example:** `Device(config)# interface virtual-template 1 type tunnel`	Creates a virtual template interface that can be configured and applied dynamically to create virtual access interfaces.
Step 4	**ip unnumbered loopback** *number* **Example:** `Device(config-if)# ip unnumbered loopback 0`	Assigns the IP address of an existing interface (usually a loopback interface) to the virtual tunnel interface.

Step 5	Do one of the following:
	• **ip nhrp network-id** *number*
	• **ipv6 nhrp network-id** *number*
	Example:
	`Device(config-if)# ip nhrp network-id 1`
	Example:
	`Device(config-if)# ipv6 nhrp network-id 1`
		Enables NHRP on the interface.

Step 6	**ip nhrp redirect** [**timeout** *seconds*] **Example:** `Device(config-if)# ip nhrp redirect`	Enables redirect traffic indication if traffic is forwarded with the NHRP network. To avoid sending duplicate redirects, use the **timeout** keyword and the *seconds* argument to indicate when to expire a redirect entry created.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Configuring NHRP Shortcuts on the FlexVPN Spoke

Perform this task to configure NHRP shortcuts on the tunnel interface on the FlexVPN spoke.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. Do one of the following:
   - **ip nhrp shortcut** *virtual-template-number*
   - **ipv6 nhrp shortcut** *virtual-template-number*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 1`	Configures the FlexVPN client interface and enters interface configuration mode.

Step 4	Do one of the following:
	• **ip nhrp shortcut** *virtual-template-number*
	• **ipv6 nhrp shortcut** *virtual-template-number*
	Example:
	`Device(config-if)# ip nhrp shortcut 1`
	Example:
	`Device(config-if)# ipv6 nhrp shortcut 1`
		Enables NHRP shortcuts on the FlexVPN client tunnel interface. This is necessary to establish spoke-to-spoke tunnels. The virtual-template number specified in this configuration and the virtual-template number specified in the Configuring the Virtual Tunnel Interface on the FlexVPN Spoke task must be same.

Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Configuring the Virtual Tunnel Interface on the FlexVPN Spoke

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type tunnel**
4. **ip unnumbered tunnel** *number*
5. Do one of the following:
   - **ip nhrp network-id** *number*
   - **ipv6 nhrp network-id** *number*
6. Do one of the following:
   - **ip nhrp shortcut** *virtual-template-number*
   - **ipv6 nhrp shortcut** *virtual-template-number*
7. **ip nhrp redirect** [**timeout** *seconds*]
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **type tunnel** **Example:** `Device(config)# interface virtual-template 1 type tunnel`	Creates a virtual template interface that can be configured and applied dynamically to create virtual access interfaces.
Step 4	**ip unnumbered tunnel** *number* **Example:** `Device(config-if)# ip unnumbered tunnel 1`	Assigns the IPv4 address of the FlexVPN tunnel interface to the virtual tunnel interface.

Step 5	Do one of the following:
	• **ip nhrp network-id** *number*
	• **ipv6 nhrp network-id** *number*
	Example:
	`Device(config-if)# ip nhrp network-id 1`
	Example:
	`Device(config-if)# ipv6 nhrp network-id 1`
		Enables NHRP on the interface.

Step 6	Do one of the following:
	• **ip nhrp shortcut** *virtual-template-number*
	• **ipv6 nhrp shortcut** *virtual-template-number*
	Example:
	`Device(config-if)# ip nhrp shortcut 1`
	Example:
	`Device(config-if)# ipv6 nhrp shortcut 1`
		Enables NHRP shortcut switching on an interface.
		Note The current virtual template number must be specified. The virtual template number must be same as configured on the FlexVPN client tunnel interface.

Step 7	**ip nhrp redirect** [**timeout** *seconds*] **Example:** `Device(config-if)# ip nhrp redirect`	Enables NHRP redirects on the virtual tunnel interface. This is useful when networks move from one spoke to another. • To avoid sending duplicate redirects, use the **timeout** keyword and the *seconds* argument to indicate when to expire a redirect entry created.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Verifying the FlexVPN Spoke Configuration

Use the following commands to verify the FlexVPN spoke configuration.

SUMMARY STEPS

1. **show crypto ikev2 client flexvpn**
2. **show ipv6 route**
3. **show ipv6 nhrp**

DETAILED STEPS

Step 1 show crypto ikev2 client flexvpn

Example:

```
Device# show crypto ikev2 client flexvpn

  Profile : flexblk
  Current state:ACTIVE
  Peer : 4001::2000:1
  Source : Ethernet0/0
  ivrf : IP DEFAULT
  fvrf : IP DEFAULT
  Backup group: None
  Tunnel interface : Tunnel0
```

Displays the FlexVPN connection status between the FlexVPN server and client.

Step 2 show ipv6 route

Example:

```
Device# show ipv6 route

IPv6 Routing Table - default - 15 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   3001::/112 [0/0]
     via Tunnel0, directly connected
S   3001::1/128 [2/0], tag 1
     via 3001::1, Virtual-Access1 [Shortcut]
     via Virtual-Access1, directly connected
L   3001::2/128 [0/0]
     via Tunnel0, receive
S   3001::3/128 [2/0], tag 1
     via Tunnel0, directly connected
C   4001::2000:0/112 [0/0]
     via Ethernet0/0, directly connected
L   4001::2000:3/128 [0/0]
     via Ethernet0/0, receive
S   5001::/64 [2/0], tag 1
     via Tunnel0, directly connected
C   5001::2000:0/112 [0/0]
```

```
     via Loopback0, directly connected
L   5001::2000:1/128 [0/0]
     via Loopback0, receive
D   5001::3000:0/112 [90/28288000]
     via FE80::A8BB:CCFF:FE01:F400, Tunnel0
D   5001::4000:0/112 [90/28288000]
     via FE80::A8BB:CCFF:FE01:F400, Tunnel0
H   5001::4000:1/128 [250/1]
     via 3001::1, Virtual-Access1
C   5001::5000:0/112 [0/0]
     via Loopback1, directly connected
L   5001::5000:1/128 [0/0]
     via Loopback1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Displays the IPv6 routes and Next Hop Resolution Protocol (NHRP) mapping information.

Step 3 **show ipv6 nhrp**

Example:

```
Device# show ipv6 nhrp

3001::1/128 via 3001::1
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router implicit rib nho
   NBMA address: 172.17.1.9
    (Claimed NBMA address: 172.16.2.1)
5001::4000:1/128 via 3001::1
   Virtual-Access1 created 00:00:56, expire 01:59:03
   Type: dynamic, Flags: router rib
   NBMA address: 172.17.1.9
    (Claimed NBMA address: 172.16.2.1)
5001::5000:1/128 via 3001::2
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router unique local
   NBMA address: 172.17.2.10
```

Example:

```
Device# show ipv6 nhrp

3001::1/128 via 3001::1
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router implicit rib nho
   NBMA address: 4001::2000:2
5001::4000:1/128 via 3001::1
   Virtual-Access1 created 00:00:56, expire 01:59:03
   Type: dynamic, Flags: router rib
   NBMA address: 4001::2000:2
5001::5000:1/128 via 3001::2
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router unique local
   NBMA address: 4001::2000:3
```

Displays the NHRP cache entries. In the first example, the output indicates that the transport is IPv4 (NBMA address). The remote spoke is behind Network Address Translation (NAT), as indicated by the Claimed NBMA address field, which is the pre-NAT address of the remote spoke. The cache entries also show the flags associated with each spoke, indicating the kind of route that has been inserted for each entry in the routing table. Next-Hop-Override (NHO) indicates the shortcut route. The *rib* flag indicates addition of an NHRP H route for that cache entry. The second example indicates

that the transport is IPv6 (NBMA address). The remote spoke is not behind NAT, as indicated by the absence of claimed address in the output.

Troubleshooting Tips for FlexVPN Spoke Configuration

Here are few tips for troubleshooting FlexVPN spoke configuration:

1. Verify the connection between the spokes.
2. Check the configuration on the client (spoke) and the server.
3. Check the reachability of the remote hosts behind the spokes.
4. Verify the routing protocol configuration that is used to advertise the routes.
5. Verify that IKEv2 and IPsec are configured properly.
6. Verify the NHRP shortcut configuration on the spoke and the redirect configuration on the server (hub).

Problem	Troubleshooting Tips
Spoke to hub connection is not created.	A connection may not be created due to the absence of virtual access interfaces created at the hub. • Check the connectivity between the hub and spoke. • Use the **show crypto session** command to check the state of security associations (SAs) on the hub and spoke. • If SAs are active (as displayed in the **show crypto session** command), verify the output of the **show crypto ikev2 client flexvpn** command on the state of FlexVPN on the spoke.

Problem	Troubleshooting Tips
Spoke to spoke tunnel is not created.	Traffic must flow from spoke to spoke via the hub to initiate a spoke to spoke tunnel. • Verify the hub configuration to check if NHRP redirect is enabled. • Verify the spoke configuration to check if NHRP shortcut is enabled. • Verify the configuration in the FlexVPN server (hub) by using the **show ip** [**ipv6**] **nhrp traffic** command whether the hub has sent a traffic indirection to the spoke. • Verify the spokes have received the traffic and sent a resolution request by using either the **show ip** [**ipv6**] **nhrp traffic** command. • Verify the presence of NHRP cache entries for remote host and spoke on either spoke by using the **show ip** [**ipv6**] **nhrp** command. • Use the **show ip** [**ipv6**] **nhrp traffic** command on the remote spoke to verify that the resolution request is received. • Use the **show crypto ikev2 sa** command and the **show crypto session** command to verify that the spoke has received the resolution request and initiated a crypto session. • Use the **show ip** [**ipv6**] **interface brief** command to check if the virtual-access interface is present on both spokes. • Use the **show ip** [**ipv6**] **nhrp traffic** command on the spokes to verify that the resolution reply has been sent, and received by the peer on the virtual-access interface. • Use the **show ip** [**ipv6**] **nhrp** command to verify that the complete NHRP cache entries are present for the remote host and on all the spokes. • Use the **show ip** [**ipv6**] **route** command to check for the presence of H routes and/or next-hop-override (NHO) routes.

Configuration Examples for FlexVPN Spoke to Spoke

Example: Configuring FlexVPN Spoke to Spoke with Static Routing

The following example shows how to configure FlexVPN spoke to spoke with IKE-propagated static routing on the FlexVPN server and the FlexVPN client. The following is the configuration on the FlexVPN server:

```
hostname hub
!
crypto ikev2 authorization policy default
 pool flex-pool
 def-domain cisco.com
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip local pool flex-pool 172.16.0.1 172.16.0.254
!
ip access-list standard flex-route
 permit any
```

The following is the configuration on the first FlexVPN client:

```
hostname spoke1
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
```

```
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.110 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.110.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip access-list standard flex-route
 permit 192.168.110.0 0.0.0.255
```

The following is the configuration on the second FlexVPN client:

```
hostname spoke2
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.120 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.120.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip access-list standard flex-route
 permit 192.168.120.0 0.0.0.255
```

Example: Configuring FlexVPN Spoke to Spoke with Dynamic Routing using BGP

The following example shows how to configure FlexVPN spoke to spoke with dynamic routing, using BGP on the FlexVPN server (with dynamic neighbor discovery) and the FlexVPN client. The following is the configuration on the FlexVPN server:

```
hostname hub
!
crypto ikev2 authorization policy default
 pool flex-pool
 def-domain cisco.com
 route set interface
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip local pool flex-pool 172.16.0.1 172.16.0.254
!
router bgp 65100
 bgp router-id 10.0.0.100
 bgp log-neighbor-changes
 bgp listen range 172.16.0.0/24 peer-group spokes
 neighbor spokes peer-group
 neighbor spokes remote-as 65100
 neighbor spokes transport connection-mode passive
 neighbor spokes update-source Loopback0
 !
 address-family ipv4
  neighbor spokes activate
  neighbor spokes default-originate
  neighbor spokes prefix-list no-default in
 exit-address-family
!
ip prefix-list no-default seq 5 deny 0.0.0.0/0
ip prefix-list no-default seq 10 permit 0.0.0.0/0 le 32
```

The following is the configuration on the first FlexVPN client:

```
hostname spoke1
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.110 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.110.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 65100
 bgp router-id 10.0.0.110
 bgp log-neighbor-changes
 neighbor hubs peer-group
 neighbor hubs remote-as 65100
 neighbor hubs update-source Tunnel0
 neighbor 172.16.1.1 peer-group hubs
 !
 address-family ipv4
  network 192.168.110.0
  neighbor 172.16.1.1 activate
 exit-address-family
```

The following is the configuration on the second FlexVPN client:

```
hostname spoke2
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local rsa-sig
```

```
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.120 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.120.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 65100
 bgp router-id 10.0.0.120
 bgp log-neighbor-changes
 neighbor hubs peer-group
 neighbor hubs remote-as 65100
 neighbor hubs update-source Tunnel0
 neighbor 172.16.1.1 peer-group hubs
 !
 address-family ipv4
  network 192.168.120.0
  neighbor 172.16.1.1 activate
 exit-address-family
```

Additional References for Configuring FlexVPN Spoke to Spoke

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
Security commands	• *Cisco IOS Security Command Reference Commands A to C* • *Cisco IOS Security Command Reference Commands D to L* • *Cisco IOS Security Command Reference Commands M to R* • *Cisco IOS Security Command Reference Commands S to Z*

Related Topic	Document Title
Shortcut Switching Enhancements	*Shortcut Switching Enhancements for NHRP in DMVPN Networks*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for FlexVPN Spoke to Spoke

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for FlexVPN Spoke to Spoke

Feature Name	Releases	Feature Information
FlexVPN Spoke to Spoke	Cisco IOS XE Release 3.9S	The FlexVPN Spoke to Spoke feature enables a FlexVPN client to establish a direct crypto channel with another FlexVPN client. The feature leverages VTIs, IKEv2, and NHRP to build spoke to spoke connections. In Cisco IOS Release 15.2(2)T, this feature was introduced. The following sections provide information about this feature: • Information About FlexVPN Spoke to Spoke • How to Configure FlexVPN Spoke to Spoke The following commands were introduced or modified: **ip unnumbered loopback0, tunnel source, tunnel mode gre ip, nhrp network-id, ip nhrp redirect, ip nhrp shortcut.**

Feature Name	Releases	Feature Information
FlexVPN IPv6 Direct Spoke to Spoke	Cisco IOS XE Release 3.11S	The FlexVPN IPv6 Direct Spoke to Spoke feature supports the use of IPv6 addresses for FlexVPN spokes. The support for IPv6 addresses provides support for IPv6 over IPv4, IPv4 over IPv6, and IPv6 over IPv6 transports. The following sections provide information about this feature: • Information About FlexVPN Spoke to Spoke • How to Configure FlexVPN Spoke to Spoke The following commands were introduced or modified: **ipv6 nhrp shortcut.**
Multiple FlexVPN Spokes Behind a Single NAT Device	Cisco IOS XE Release 3.12S	The Multiple FlexVPN Spokes Behind a Single NAT Device feature supports multiple spokes behind a Network Address Translation (NAT) device on FlexVPN. No commands were introduced or modified for this feature.