FlexVPN Migration: Hard Move from DMVPN to FlexVPN on Same Devices

Document ID: 115726

Contributed by Marcin Latosiewicz, Cisco TAC Engineer.
Jan 09, 2013

Contents

Introduction

This document provides information about how to migrate from existing DMVPN network to FlexVPN on the same devices.

Both frameworks' configurations will co−exist on the devices.

In this document only the most common scenario is shown: DMVPN using pre−shared key for authentication and EIGRP as routing protocol.

This document demonstrates migration to BGP (recommended routing protocol) and less desirable EIGRP.

Prerequisites

Requirements

This document assumes that the reader knows basic concepts of DMVPN and FlexVPN.

Components Used

Note that not all software and hardware supports IKEv2. Refer to the Cisco Feature Navigator for information. Ideally, software versions to be used are:

- ISR − 15.2(4)M1 or newer
- ASR1k − 3.6.2 release 15.2(2)S2 or newer

Among the advantages of newer platform and software is the possibility of using Next Generation Cryptography, for example, AES GCM for encryption in IPsec. This is discussed in RFC 4106.

AES GCM allows to reach much faster encryption speed on some hardware.

In order to see Cisco recommendations on using and migrating to Next Generation Cryptography, refer to:

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Migration procedure

Currently, the recommended way to migrate from DMVPN to FlexVPN is for the two frameworks not to operate at the same time.

This limitation will be removed due to new migration features to be introduced in the ASR 3.10 release, tracked under multiple enhancement requests under the Cisco side, including CSCuc08066. Those features should be available in late June, 2013.

A migration where both frameworks co−exist and operate at the same time on same devices will be referred to as soft migration, which indicates minimum impact and smooth failover from one framework to another.

A migration where both frameworks' configuration co−exist, but do not operate at the same time is referred to as hard migration. This indicates that a switchover from one framework to another means a lack of communication over VPN, even if minimal.

Hard migration on same devices

In this document the migration from an existing DMVPN network to a new FlexVPN network on same devices is discussed.

This migration requires that both frameworks do not operate at the same time on the devices, essentially requiring that DMVPN functionality is disabled across the board before enabling FlexVPN.

Until the new migration feature is available, the way to perform migrations using same devices is to:

1. Verify connectivity over DMVPN.
2. Add FlexVPN configuration in place and shut down Tunnel and Virtual template interfaces belonging to new configuration.
3. (During a maintenance window) Shut down all DMVPN tunnel interfaces on all spokes and hubs before moving to step 4.
4. Unshut FlexVPN tunnel interfaces.
5. Verify spoke to hub connectivity.
6. Verify spoke to spoke connectivity.
7. *If verification in point 5 or 6 did not go properly revert back to DMVPN by shutting down FlexVPN interface and un−shutting DMVPN interfaces.*
8. *Verify spoke to hub communication.*
9. *Verify spoke to spoke communication.*

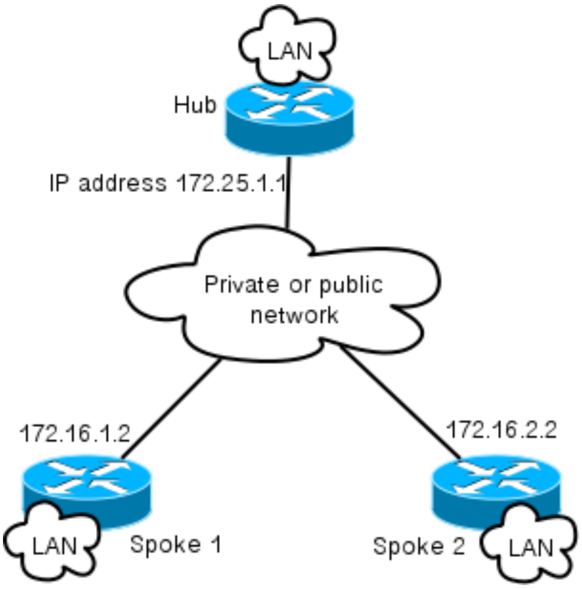
Custom approach

If, due to your network or routing complexities, the approach might not be the best idea for you, start a discussion with your Cisco representative before migrating. The best person to discuss a custom migration process is your System Engineer or Advanced Services Engineer.

Network topology

Transport network topology

This diagram shows a typical connections topology of hosts on the Internet. In this document, the hub's IP address of loopback0 (172.25.1.1) is used to terminate the IPsec session.

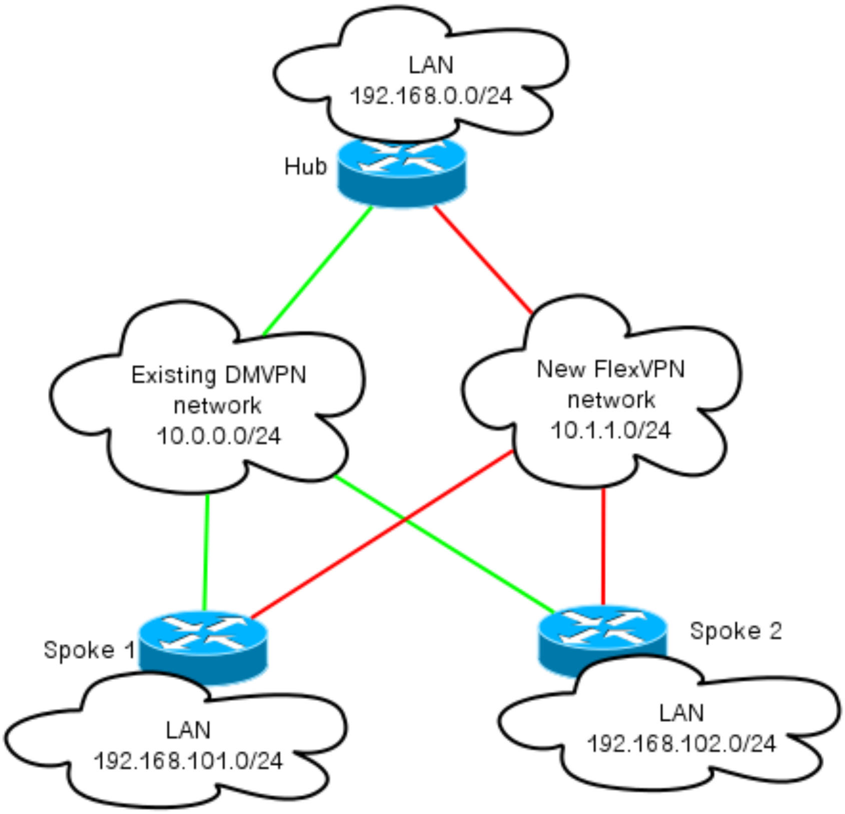


Overlay network topology

This topology diagram shows two separate clouds used for overlay: DMVPN (green connections) and FlexVPN connections.

Local Area Network prefixes are shown for corresponding sides.

The 10.1.1.0/24 subnet does not represent an actual subnet in terms of interface addressing, but rather a chunk of IP space dedicated to FlexVPN cloud. Rationale behind is discussed later in FlexVPN Configuration section.



Configuration

DMVPN Configuration

This section contains basic configuration of DMVPN hub and spoke.

Pre−shared key (PSK) is used for IKEv1 authentication.

Once IPsec has been established, NHRP registration is performed from spoke to hub, so that hub can learn the dynamically spokes' NBMA addressing.

When NHRP performs registration on spoke and hub, routing adjacency can establish and routes exchanged. In this example, EIGRP is used as basic routing protocol for the overlay network.

Spoke DMVPN configuration

This is a basic example configuration of DMVPN with pre−shared key authentication and EIGRP as routing protocol.

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto isakmp keepalive 30 5
crypto isakmp profile DMVPN_IKEv1
  keyring DMVPN_IKEv1
  match identity address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
  mode transport
crypto ipsec profile DMVPN_IKEv1
  set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1
interface Tunnel0
ip address 10.0.0.101 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 10.0.0.1 172.25.1.1
 ip nhrp map multicast 172.25.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp nhs 10.0.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.102.0
 passive-interface default
 no passive-interface Tunnel0
```

Hub DMVPN configuration

In hub configuration the tunnel is sourced from loopback0 with an IP address of 172.25.1.1.

The rest is standard deployment of DMVPN hub with EIGRP as routing protocol.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1
 interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp server-only
 ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
 ip tcp adjust-mss 1360
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel0
```

FlexVPN configuration

FlexVPN is based on these same fundamental technologies:

- IPsec: Unlike default in DMVPN, IKEv2 is used instead of IKEv1 to negotiate IPsec SAs. IKEv2 offers improvements over IKEv1, starting with resiliency and ending with how many messages are needed to establish a protected data channel.
- GRE: Unlike DMVPN, static and dynamic point to point interfaces are used, and not only on static multipoint GRE interfaces. This configuration allows added flexibility, especially for per−spoke/per−hub behavior.
- NHRP: In FlexVPN NHRP is primarily used to establish spoke to spoke communication. Spokes do not register to hub.
- Routing: Because spokes do not perform NHRP registration to hub, you need to rely on other mechanisms to make sure hub and spokes can communicate bi−directionally. Simliar to DMVPN, dynamic routing protocols can be used. However, FlexVPN allows you to use IPsec to introduce routing information. The default is to introduce as /32 route for the IP address on the other side of the tunnel, which will allow spoke−to−hub direct communication.

In hard migration from DMVPN to FlexVPN the two framemworks do not work at the same time on same devices. However, it is recommended to keep them separate.

Separate them on several levels:

- NHRP − Use different NHRP network ID (recommended).
- Routing − Use separate routing processes (recommended).
- VRF − VRF separation can allow added flexibility but will not be discussed here (optional).

Spoke FlexVPN configuration

One of the differences in spoke configuration in FlexVPN as compared to DMVPN, is that you have potentially two interfaces.

There is a necessary tunnel for spoke to hub communication and optional tunnel for spoke to spoke tunnels. If you choose not to have dynamic spoke to spoke tunneling and would rather that everything goes through hub device, you can remove the virtual−template interface and remove NHRP shortcut switching from the tunnel interface.

You will also notice that the static tunnel interface has an IP address received based on negotiation. This allows the hub to provide tunnel interface IP to spoke dynamically without the need to create static addressing in the FlexVPN cloud.

```
aaa new−model
aaa authorization network default local
aaa session−id common

crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa−sig
 authentication local rsa−sig
 aaa authorization group cert list default default
 virtual−template 1
crypto ikev2 dpd 30 5 on−demand
```

Cisco recommends using AES GCM in hardware that supports it.

```
crypto ipsec transform−set IKEv2 esp−gcm
```

```
    mode transport
crypto ipsec profile default
 set ikev2−profile Flex_IKEv2
! set transform−set IKEv2
interface Tunnel1
 ip address negotiated
 ip mtu 1400
 ip nhrp network−id 2
 ip nhrp shortcut virtual−template 1
 ip nhrp redirect
 ip tcp adjust−mss 1360
 shutdown
 tunnel source Ethernet0/0
 tunnel destination 172.25.1.1
 tunnel path−mtu−discovery
 tunnel protection ipsec profile default
interface Virtual−Template1 type tunnel
 ip unnumbered Tunnel1
 ip mtu 1400
 ip nhrp network−id 2
 ip nhrp shortcut virtual−template 1
 ip nhrp redirect
 ip tcp adjust−mss 1360
 tunnel path−mtu−discovery
 tunnel protection ipsec profile default
```

PKI is the recommended way of performing large scale authentication in IKEv2.

However, you can still use pre−shared key as long as you are aware of it's limitations.

Here is an example configuration using "cisco" as PSK:

```
crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre−shared−key local cisco
 pre−shared−key remote cisco
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre−share
 authentication local pre−share
 keyring local Flex_key
 aaa authorization group psk list default default
```

FlexVPN Hub configuration

Typically a hub will only terminate dynamic spoke−to−hub tunnels. This is why in the hub's configuration you will not find a static tunnel interface for FlexVPN, instead a virtual−template interface is used. This will spawn a virtual−access interface for each connection.

Note that on hub side you need to point out pool addresses to be assigned to spokes.

Addresses from this pool will be added later on in the routing table as /32 routes for each spoke.

```
aaa new−model
aaa authorization network default local
aaa session−id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa−sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco recommends using AES GCM in hardware which supports it.

```
crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

Note that in the configuration below the AES GCM operation has been commented out.

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

With authentication in IKEv2, the same principle applies on hub as on spoke.

For scalability and flexibility, use certificates. However, you can re−use the same configuration for PSK as on spoke.

Note: IKEv2 offers flexibility in terms of authentication. One side can authenticate using PSK while the other RSA−SIG.

Traffic Migration

Migrating to BGP as overlay routing protocol [Recommended]

BGP is a routing protocol based on unicast exchange. Due to it's characteristics it has been the best scaling protocol in DMVPN networks.

In this example, iBGP is used.

Spoke BGP configuration

Spoke migration consists of two parts. Enabling BGP as dynamic routing.

```
router bgp 65001
 bgp log-neighbor-changes
 network 192.168.101.0
 neighbor 10.1.1.1 remote-as 65001
```

After the BGP neighbor comes up (see the Hub BGP configuration in this section of migration) and new prefixes over BGP are learned, you can swing traffic from the existing DMVPN cloud to new FlexVPN cloud.

Hub BGP configuration

On hub to avoid keeping neighborship configuration for each spoke separately, dynamic listeners are configured.

In this setup BGP will not initiate new connections, but will accept connection from the provided pool of IP addresses. In this case the said pool is 10.1.1.0/24, which is all the addresses in the new FlexVPN cloud.

```
router bgp 65001
 network 192.168.0.0
 bgp log-neighbor-changes
 bgp listen range 10.1.1.0/24 peer-group Spokes
 aggregate-address 192.168.0.0 255.255.0.0 summary-only
 neighbor Spokes peer-group
 neighbor Spokes remote-as 65001
```

Migrating traffic to FlexVPN

As mentioned before migration needs to be done by shutting down DMVPN functionality and bringing FlexVPN up.

This procedure guarantees minimum impact.

1. On all spokes:

   ```
   interface tunnel 0
      shut
   ```
2. On Hub:

   ```
   interface tunnel 0
     shut
   ```

   At this point make sure that there are no IKEv1 sessions established to this hub from spokes.

   This can be verified by checking the output of the **show crypto isakmp sa** command and monitoring syslog messages generated by the crypto logging session.

   Once this has been confirmed you can proceed to bringing up FlexVPN.
3. Continuing on hub:

   ```
   interface Virtual-template 1
    no shut
   ```
4. On spokes:

   ```
   interface tunnel 1
      no shut
   ```

Verification Steps

IPsec stability

The best way to evaluate IPsec stability is by monitoring sylogs with this configuration command enabled:

```
crypto logging session
```

If you see sessions going up and down, this can indicate a problem on IKEv2/FlexVPN level that needs to be corrected before migration can begin.

BGP information populated

If IPsec is stable, make sure that the BGP table is populated with entries from spokes (on hub) and summary from hub (on spokes).

In case of BGP, this can be viewed by performing:

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Example of correct information from hub:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1
*10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

You can see that hub has learned that 1 prefix from each of the spokes and both spokes are dynamic (marked with asterisk (*) sign).

Example of similar information from spoke:

```
Spoke1#show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 11 11 6 0 0 00:03:43 1
```

Spoke has received one prefix from hub. In case of this setup, this prefix should be the summary advertised on hub.

Migrating to new tunnels using EIGRP

EIGRP is a popular choice in DMVPN networks due to it's relatively simple deployment and fast convergence.

It will, however, scale worse than BGP and does not offer many of advanced mechanisms that can be used by BGP straight out of the box.

This next section describes one of the ways to move to FlexVPN using a new EIGRP process.

Updated spoke configuration

In this example, a new AS is added with a separate EIGRP process.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
 passive-interface default
 no passive-interface Tunnel1
```

Note: You should avoid establishing routing protocol adjacency over spoke to spoke tunnels, thus only make interface of tunnel1 (spoke to hub) not passive.

Updated hub configuration

Similarly on hub, DMVPN should remain the preferred way to exchange traffic over. However, FlexVPN should advertise and learn same prefixes already.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```

There are two ways to provide summary back towards the spoke.

- Redistributing a static route pointing to null0 (Preferred option).

  ```
  ip route 192.168.0.0 255.255.0.0 null 0
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
   redistribute static metric 1500 10 10 1 1500
  ```

  This option allows to have control over summary and redistribution without touching hub's VT configuration.
- Or, you can set up a DMVPN−style summary address on Virtual−template. This configuration is not recommended because of internal processing and replication of said summary to each virtual access. It is shown here for reference:

  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 172.16.1.0 255.255.255.0
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   delay 2000
  ```

Migrating traffic to FlexVPN

Migration needs to be done by shutting down DMVPN functionality and bringing FlexVPN up.

The following procedure guarantees minimum impact.

1. On all spokes:

   ```
   interface tunnel 0
      shut
   ```
2. On Hub:

   ```
   interface tunnel 0
     shut
   ```

   At this point make sure that there are no IKEv1 sessions established to this hub from spokes.

   This can be verified by checking the output of the **show crypto isakmp sa** command and monitoring syslog messages generated by crypto logging session.

   Once this has been confirmed you can proceed to bringing up FlexVPN.
3. Continuing on hub:

```
interface Virtual-template 1
 no shut
```

4. On all spokes:

```
interface tunnel 1
   no shut
```

Verification steps

IPsec stability

As in case of BGP, you need to evaluate if IPsec is stable. The best way to do so is by monitoring sylogs with this configuration command enabled:

```
crypto logging session
```

If you see sessions going up and down, this can indicate a problem on IKEv2/FlexVPN level that needs to be corrected before migration can begin.

EIGRP information in topology table

Make sure that you do have your EIGRP topology table populated with spoke LAN entries on hub and summary on spokes. This can be verified by issuing this command on hub(s) and spoke(s).

```
show ip eigrp topology
```

Example of proper output from spoke:

```
Spoke1#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted as output related to DMVPN cloud ...)
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
 via Rstatic (26112000/0)


P 192.168.101.0/24, 1 successors, FD is 281600
 via Connected, Ethernet1/0


P 192.168.0.0/16, 1 successors, FD is 26114560
 via 10.1.1.1 (26114560/1709056), Tunnel1


P 10.1.1.107/32, 1 successors, FD is 26112000
 via Connected, Tunnel1
```

You will notice that spoke knows about its LAN subnet (in italic) and the summaries for those (in **bold**).

Example of proper output from hub.

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
```

```
(...omitted, related to DMVPN...)
EIGRP−IPv4 Topology Table for AS(200)/ID(172.25.1.1)
Codes: P − Passive, A − Active, U − Update, Q − Query, R − Reply,
 r − reply Status, s − sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
 via Connected, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600
 via 10.1.1.107 (1561600/281600), Virtual−Access1


P 192.168.0.0/16, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 10.1.1.107/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 10.1.1.106/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 0.0.0.0/0, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 192.168.102.0/24, 1 successors, FD is 1561600
 via 10.1.1.106 (1561600/281600), Virtual−Access2
```

You will note that hub knows about spokes' LAN subnets (in italic), the summary prefix it is advertising (in **bold**) and each spoke's assigned IP address via negotiation.

Additional considerations

Existing spoke to spoke tunnels

Because shutting down the DMVPN tunnel interface causes NHRP entries to be removed, existing spoke to spoke tunnels will be torn down.

Clearing NHRP entries

As mentioned before, a FlexVPN hub will not rely on the NHRP registration process from spoke to know how to route traffic back. However, dynamic spoke to spoke tunnels rely on NHRP entries.

In DMVPN where clearing NHRP on hub could have resulted in short−lived connectivity problems.

In FlexVPN clearing NHRP on spokes will cause FlexVPN IPsec session, related to spoke to spoke tunnels, to be torn down. In clearing NHRP no hub will have an effect on FlexVPN session.

This is due to the fact that in FlexVPN, by default:

- Spokes do not register to hubs.
- Hubs work only as NHRP redirector and do not install NHRP entries.
- NHRP shortcut entries are installed on spokes for spoke−to−spoke tunnels and are dynamic.

Known Caveats

Spoke to spoke traffic might be affected by CSCub07382.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.