FlexVPN迁移：从DMVPN的硬移动到在同样设备的FlexVPN

目录

简介

本文提供关于如何的信息从现有DMVPN网络移植给在同样设备的FlexVPN。

两个框架的配置在设备将共存。

在本文中仅多数常见情况显示：DMVPN使用验证的预先共享密钥和EIGRP作为路由协议。

本文给BGP (推荐的路由协议)和较不理想EIGRP展示迁移。

先决条件

要求

本文假设，读者认识DMVPN和FlexVPN基本概念。

使用的组件

注意不是所有的软件和硬件支持IKEv2。参考Cisco Feature Navigator信息。理论上来讲，将使用的软件版本是：

- ISR -15.2(4)M1或更新
- ASR1k - 3.6.2版本15.2(2)S2或更新

在更新的平台和软件中优点是使用下一代加密算法的可能性，例如， AES GCM加密在IPsec。这在RFC 4106讨论。

AES GCM准许到达在一些硬件的更加快速的加密速度。

为了看到在使用和移植的Cisco推荐到下一代加密算法，参考：

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

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

迁移步骤

目前，推荐的方式从DMVPN移植到FlexVPN是为同时运行两个的框架。

此限制将就该删除的对新的迁移功能介绍在ASR 3.10版本，被跟踪在多个增强请求下在思科侧下，包括CSCuc08066。那些功能应该取得到在2013年6月下旬。

两个框架在同样设备同时共存并且运行的迁移将指软的迁移，指示最低的影响和平稳的故障切换从一个框架到另一个。

两个框架的配置共存的迁移，但是同时不运行指硬迁移。这表明从一个框架的一个切换到另一个含义缺乏在VPN的通信，即使最小。

在同样设备的硬迁移

在本文中从现有DMVPN网络的迁移到在同样设备的新的FlexVPN网络讨论。

此迁移要求两个框架在设备同时不运行，根本要求DMVPN功能在启用FlexVPN前禁用全面的。

直到新的迁移功能是可用的，方式进行迁移使用同样设备对：

1. 验证在DMVPN的连接。
2. 添加到位FlexVPN配置并且关闭属于新的配置的通道和虚拟模板接口。
3. (在维护窗口期间)请在移动关闭在所有spoke的所有DMVPN隧道接口和集线器对步骤4.前。
4. Unshut FlexVPN隧道接口。
5. 验证发言对集线器连接。
6. 验证分支对分支连接。
7. *如果在点5或6的验证没有适当地去请恢复回到DMVPN通过关闭FlexVPN接口和非关闭DMVPN接口。*
8. *验证发言对集线器通信。*
9. *验证分支对分支通信。*

自定义方法

如果，由于您的网络或路由复杂性，方法也许不是您的最好的想法，请在移植前开始与您的思科代表的一讨论。讨论自定义迁移进程的最好的人是您的系统工程师或高级服务服务工程师。

网络拓扑

传输网络网络拓扑结构

此图表显示主机一典型的连接拓扑在互联网的。在本文中， loopback0 (172.25.1.1)的集线器的IP地址用于终止IPSec会话。

重叠网络拓扑

此拓扑图显示用于重叠的两独立的网云：DMVPN (绿色连接)和FlexVPN连接。

局域网前缀为对应侧显示。

10.1.1.0/24子网不代表实际子网根据接口编址，然而相当IP空间大块投入FlexVPN网云。后边基本原理是讨论以后在FlexVPN配置部分。

配置

DMVPN 配置

此部分包含DMVPN星型网基本配置。

预先共享密钥(PSK)使用IKEv1验证。

一旦IPsec设立了， NHRP注册进行从发言到集线器，因此集线器能动态地学习spoke的NBMA地址。

当NHRP进行在分支和集线器时的注册，路由adjacancy能设立和被交换的路由。在本例中，EIGRP使用作为基本路由协议覆盖网络。

分支DMVPN配置

这是DMVPN和EIGRP的基本示例配置与预先共享密钥验证的作为路由协议。

```
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
```

集线器DMVPN配置

在集线器上配置通道从loopback0来源用172.25.1.1的IP地址。

其余是DMVPN集线器的标准的部署有EIGRP的作为路由协议。

```
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配置

FlexVPN根据这些同样基本的技术：

- IPsec ：不同于在DMVPN的默认， IKEv2用于而不是IKEv1协商IPSec SAS。IKEv2从弹性和结束开始提供在IKEv1的改进，与多少个消息是需要的设立保护数据数据通道。
- GRE ：不同于DMVPN，使用静态和动态点对点接口，并且不仅在静态多点GRE建立接口。此配置允许已添加灵活性，特别是每分支/每HUB行为。
- NHRP ：在FlexVPN NHRP主要用于设立分支到分支通信。Spoke不注册到集线器。
- 路由：由于spoke不进行NHRP注册到集线器，您在其他机制需要取决于确保星型网能通信双向。可以使用对DMVPN的Simliar，动态路由协议。然而， FlexVPN允许您使用IPsec引入路由信息。默认是介绍作为IP地址的/32路由在通道的另一侧，将允许spoke-to-hub直接通信。

在从DMVPN的硬迁移到FlexVPN两framemworks在同样设备同时不运作。然而，推荐保持他们分开。

分离他们在几个级别上：

- NHRP -请使用不同的NHRP网络ID (建议使用)。
- 路由-请使用分开的路由进程(建议使用)。
- VRF - VRF分离能允许已添加灵活性，但是不讨论此处(可选)。

分支FlexVPN配置

其中一差异在辐条配置方面在与DMVPN比较的FlexVPN，是您有潜在两个接口。

有一个必要的通道为发言到集线器通信和可选通道分支的到分支通道。如果选择没有动态分支到分支建立隧道并且相当会一切通过集线器设备，您能消除虚拟模板接口和从隧道接口删除NHRP快捷方式交换。

您也注意静态隧道接口有根据协商接收的一个IP地址。这允许集线器提供隧道接口IP动态地发言，不用需要创建在FlexVPN网云的静态地址。

```
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
```

思科推荐使用AES GCM在支持它的硬件方面。

```
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是执行的大规模验证推荐的方式在IKEv2的。

然而，只要您知道它是限制，您能仍然使用预先共享密钥。

这是配置示例使用“cisco”作为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集线器上配置

典型地集线器只将终止动态spoke-to-hub通道。这就是为什么在集线器的配置里您不会查找FlexVPN的一个静态隧道接口，反而使用虚拟模板接口。这将产生每连接的一个虚拟访问接口。

注意在集线器端您需要指出池地址将分配到spoke。

从此池的地址在路由表以后将被添加作为每分支的/32路由。

```
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
```

思科推荐使用AES GCM在支持它的硬件方面。

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

在配置里注意，在AES GCM操作之下注释。

```
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
```

使用在IKEv2的验证，同一个原理在集线器适用和在分支。

对于可扩展性和灵活性，请使用证书。然而，您能重新使用PSK的相同的配置和在分支。

注意： IKEv2提供灵活性根据验证。一端能验证使用PSK，当其他RSA-SIG时。

流量迁移

移植到BGP作为重叠路由协议[Recommended]

BGP是根据单播交换的路由协议。归结于它它是在DMVPN网络的最好的扩展的协议的特性。

在本例中，使用iBGP。

分支BGP配置

分支迁移包括两部分。启用BGP作为动态路由。

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

在BGP邻居出现(看到在迁移的此部分的集线器BGP配置)后，并且了解在BGP的新建的前缀，您能摇摆从现有DMVPN网云新建的FlexVPN网云的流量。

集线器BGP配置

在避免的集线器上保持每结邻配置分开发言，动态监听程序配置。

在此设置BGP中不会首次新连接，然而接受从IP地址的提供的池的连接。在这种情况下前述池是10.1.1.0/24，是在新的FlexVPN网云的所有地址。

```
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
```

移植流量到FlexVPN

如上所述迁移需要由关闭DMVPN功能完成和提出FlexVPN。

此步骤保证最低的影响。

1. 在所有spoke ：`interface tunnel 0`
   `shut`
2. 在集线器上：`interface tunnel 0`
   `shut`这时请确保没有IKEv1会话建立对从spoke的此集线器。这可以通过检查crypto记录日志会话生成的**show crypto isakmp sa命令**和监控的系统消息的输出验证。一旦这被确认了您能继续到启动FlexVPN。
3. 继续在集线器：`interface Virtual-template 1`
   `no shut`
4. 在spoke ：`interface tunnel 1`
   `no shut`

验证步骤

IPsec稳定性

评估IPsec稳定性的最佳方法由监控sylog用启用的此配置命令：

```
crypto logging session
```

如果看到会话上升和下降，这能指示在需要更正的IKEv2/FlexVPN级别上的一问题，在迁移能开始前。

填充的BGP信息

如果IPsec稳定的，请确保BGP表带有从spoke的从集线器的条目(在集线器)和摘要(在spoke)。

在BGP的情况下，这可以由执行查看：

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

正确信息示例从集线器的：

```
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
```
您能看到集线器了解从其中每一个的1个前缀spoke和两个spoke动态(标记用星号(*)符号)。

相似的信息示例从分支的：

```
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
```
分支接收从集线器的一个前缀。在此设置的情况下，此前缀应该是在集线器通告的摘要。

移植到新的通道使用EIGRP

EIGRP是在DMVPN网络的一普遍的选择由于它是相对简单部署和快速收敛。

它，然而，比BGP将扩展坏，并且不提供能由BGP直通使用箱外的许多先进的机制。

使用一个新的EIGRP进程，此下一部分描述其中一个方式移动向FlexVPN。

更新辐条配置

在本例中，新的AS添加与一个分开的EIGRP进程。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
 passive-interface default
 no passive-interface Tunnel1
```
注意： 因而您应该避免设立在分支的路由协议邻接到分支通道，只使接口tunnel1 (发言到集线器)不被动。

更新集线器上配置

同样集线器， DMVPN应该在首选的方法交换流量。然而， FlexVPN应该已经通告和了解同样前缀。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```
有两种方式提供往分支的摘要上一步。

- 再分布指向null0 (首选)的静态路由。`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
  ```
  此选项准许有对摘要的控制和再分配，不用感人的集线器的VT配置。
- 或者，您能设置在虚拟模板的一DMVPN斯太尔summary-address。此配置没有推荐由于前述摘

要的内部处理和复制对每次虚拟访问的。它显示此处供参考：`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
```

移植流量到FlexVPN

迁移需要由关闭DMVPN功能完成和提出FlexVPN。

以下步骤保证最低的影响。

1. 在所有spoke ：`interface tunnel 0`
   `shut`
2. 在集线器上：`interface tunnel 0`
   `shut`这时请确保没有IKEv1会话建立对从spoke的此集线器。这可以通过检查crypto记录日志会话生成的**show crypto isakmp sa命令**和监控的系统消息的输出验证。一旦这被确认了您能继续到启动FlexVPN。
3. 继续在集线器：`interface Virtual-template 1`
   `no shut`
4. 在所有spoke ：`interface tunnel 1`
   `no shut`

验证步骤

IPsec稳定性

如果IPsec稳定的，和在BGP的情况下，您需要评估。如此要执行的最佳方法由监控sylog用启用的此配置命令：

```
crypto logging session
```

如果看到会话上升和下降，这能指示在需要更正的IKEv2/FlexVPN级别上的一问题，在迁移能开始前。

EIGRP数据在拓扑表里

确保您安排您的EIGRP拓扑表带有分支在集线器和摘要的LAN条目在spoke。这可以通过发出此on命令集线器和分支验证。

```
show ip eigrp topology
```

适当的输出示例从分支的：

```
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
```

您注意分支知道关于其LAN子网(以斜体字)和那些的摘要(在**粗体**)。

适当的输出示例从集线器的。

```
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
```

您注意到，集线器知道关于spoke的LAN子网(以通告的斜体字)，概略的前缀(在**粗体**)和每个spoke的指定的IP地址通过协商。

另外的考虑事项

对分支通道的现有分支

由于关闭DMVPN隧道接口造成NHRP条目删除，对分支通道的现有分支将被切断。

清除NHRP条目

如上所述， FlexVPN集线器如何不会依靠从发言的NHRP注册过程知道到路由流量上一步。然而，对分支通道的动态分支依靠NHRP条目。

在集线器的清除的NHRP可能导致短期的连接问题的DMVPN。

在FlexVPN清除在spoke的NHRP将引起FlexVPN IPSec会话，涉及与分支分支通道，被切断。在清除NHRP集线器在FlexVPN会话不会有一效果。

这归结于在FlexVPN，默认情况下的事实：

- Spoke不注册到集线器。
- 集线器仅工作作为NHRP转向器，并且不安装NHRP条目。
- NHRP快捷方式条目在spoke-to-spoke通道的spoke安装并且动态。

已知问题说明

对分支流量的分支也许受CSCub07382的影响。

相关信息

- 技术支持和文档 - Cisco Systems