解决方案：如何做动态L2L通道落入其它通道组

目录

简介

本文提供信息关于怎样做动态L2L通道落入其它通道组。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

症状

在本文的示例中，网络管理员需要创建连接对集线器的不同的远程VPN spoke应该连接分离隧道群的VPN策略，以便不同的VPN策略可以应用到每远程连接。

原因/问题说明

在动态L2L通道中，通道(发起者)的一端有一个动态IP地址。由于接收不知道哪些IP地址他们来自

，不同于静态L2L建立隧道，不同的对等体自动地落入默认L2L组。然而，在一些情况中这不是可接受，并且用户也许需要分配一不同的组政策或预先共享密钥对每对等体。

情况/环境

解决方法

这可以完成用这两个方式：

- **证书**在ASA的隧道群查找进程将登陆根据证书字段的连接提交由spoke。`no tunnel-group-map enable rules`
```
tunnel-group-map enable ou
tunnel-group-map enable ike-id
tunnel-group-map enable peer-ip
tunnel-group-map default-group DefaultRAGroup
```
- **PSKs和积极模式**不是所有的用户将有PKI基础设施。然而，同样可以仍然是实现的使用积极模式参数如描述此处：**HUB**`crypto ipsec transform-set myset esp-3des esp-sha-hmac`
```
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto dynamic-map mydyn 10 set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic mydyn
crypto map mymap interface outside

crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400

tunnel-group SPOKE1 type ipsec-l2l
tunnel-group SPOKE1 ipsec-attributes
 pre-shared-key cisco123
tunnel-group SPOKE2 type ipsec-l2l
tunnel-group SPOKE2 ipsec-attributes
```
 `pre-shared-key cisco456`**分支1**`access-list interesting extended permit ip 192.168.15.0 255.255.255.0 192.168.1.0 255.255.255.0`
```

crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map mymap 10 match address interesting
crypto map mymap 10 set peer 10.198.16.141
crypto map mymap 10 set transform-set myset
crypto map mymap 10 set phase1-mode aggressive
crypto map mymap interface outside
crypto isakmp identity key-id SPOKE1
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400

tunnel-group 10.198.16.141 type ipsec-l2l
tunnel-group 10.198.16.141 ipsec-attributes
```

```
 pre-shared-key cisco123分支2ip access-list extended interesting
 permit ip 192.168.16.0 0.0.0.255 192.168.1.0 0.0.0.255

crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2

crypto isakmp peer address 10.198.16.141
 set aggressive-mode password cisco456
 set aggressive-mode client-endpoint fqdn SPOKE2

crypto ipsec transform-set myset esp-3des esp-sha-hmac

crypto map mymap 10 ipsec-isakmp
 set peer 10.198.16.141
 set transform-set myset
 match address interesting

interface FastEthernet0/0
 crypto map mymapHUB验证Session Type: LAN-to-LAN Detailed

Connection   : SPOKE2
Index        : 59                    IP Addr      : 10.198.16.132
Protocol     : IKE IPsec
Encryption   : 3DES                  Hashing      : SHA1
Bytes Tx     : 400                   Bytes Rx     : 400
Login Time   : 23:45:00 UTC Thu Oct 27 2011
Duration     : 0h:00m:18s
IKE Tunnels: 1
IPsec Tunnels: 1

IKE:
  Tunnel ID    : 59.1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeys
  Encryption   : 3DES                  Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 86381 Seconds
  D/H Group    : 2
  Filter Name  :

IPsec:
  Tunnel ID    : 59.2
  Local Addr   : 192.168.1.0/255.255.255.0/0/0
  Remote Addr  : 192.168.16.0/255.255.255.0/0/0
  Encryption   : 3DES                  Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds          Rekey Left(T): 3581 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 400                   Bytes Rx     : 400
  Pkts Tx      : 4                     Pkts Rx      : 4

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 21 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :

Connection   : SPOKE1
Index        : 60                    IP Addr      : 10.198.16.142
Protocol     : IKE IPsec
Encryption   : 3DES                  Hashing      : SHA1
```

```
Bytes Tx     : 400                    Bytes Rx     : 400
Login Time   : 23:45:12 UTC Thu Oct 27 2011
Duration     : 0h:00m:08s
IKE Tunnels: 1
IPsec Tunnels: 1

IKE:
  Tunnel ID    : 60.1
  UDP Src Port : 500                  UDP Dst Port : 500
  IKE Neg Mode : Aggressive           Auth Mode    : preSharedKeys
  Encryption   : 3DES                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds        Rekey Left(T): 86391 Seconds
  D/H Group    : 2
  Filter Name  :

IPsec:
  Tunnel ID    : 60.2
  Local Addr   : 192.168.1.0/255.255.255.0/0/0
  Remote Addr  : 192.168.15.0/255.255.255.0/0/0
  Encryption   : 3DES                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds        Rekey Left(T): 28791 Seconds
  Rekey Int (D): 4608000 K-Bytes      Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes           Idle TO Left : 29 Minutes
  Bytes Tx     : 400                  Bytes Rx     : 400
  Pkts Tx      : 4                    Pkts Rx      : 4

NAC:
  Reval Int (T): 0 Seconds            Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds            EoU Age(T)   : 9 Seconds
  Hold Left (T): 0 Seconds            Posture Token:
  Redirect URL :
```

相关信息

- 技术支持和文档 - Cisco Systems