解决方案：如何使动态L2L隧道落入不同的隧道组

目录

简介

本文档提供有关如何使动态L2L隧道落入不同隧道组的信息。

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

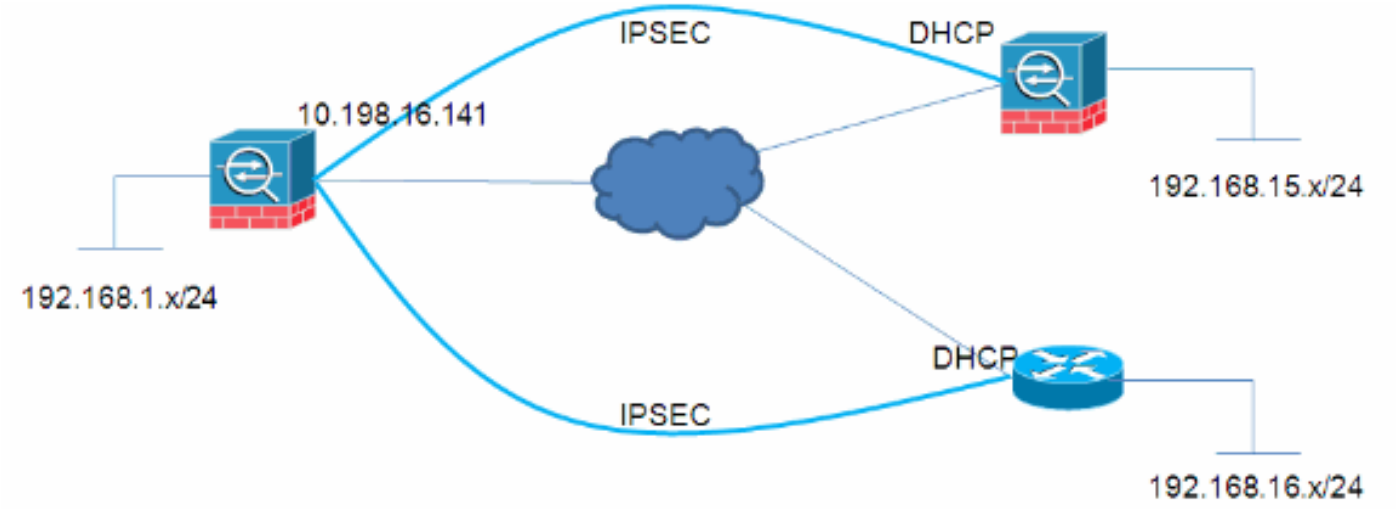
在本文档示例中，网络管理员需要创建VPN策略，其中连接到集线器的不同远程VPN分支应连接到单独的隧道组，以便可以对每个远程连接应用不同的VPN策略。

原因/问题描述

在动态L2L隧道中，隧道的一端（发起方）具有动态IP地址。由于接收方不知道来自哪些IP地址，因

此不同的对等体会自动落入默认L2L组中。但是，在某些情况下，这是不可接受的，用户可能需要为每个对等体分配不同的组策略或预共享密钥。

条件/环境



分辨率

这可以通过以下两种方式实现：

- **证书**ASA上的隧道组查找过程将根据分支提供的证书字段确定连接。

```
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
```

- **PSK和主动模式**并非所有用户都有PKI基础设施。但是，使用主动模式参数仍然可以实现此目的，如下所述：**集线器**

```
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
```

SPOKE1

```
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
```

SPOKE2

```
ip 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 mymap
```

集线器验证

```
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