ソリューション：異なるトンネル グループにダイナミックな L2L のトンネルを分類する方法

内容

概要

このドキュメントでは、ダイナミック L2L トンネルを異なるトンネル グループに分類する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

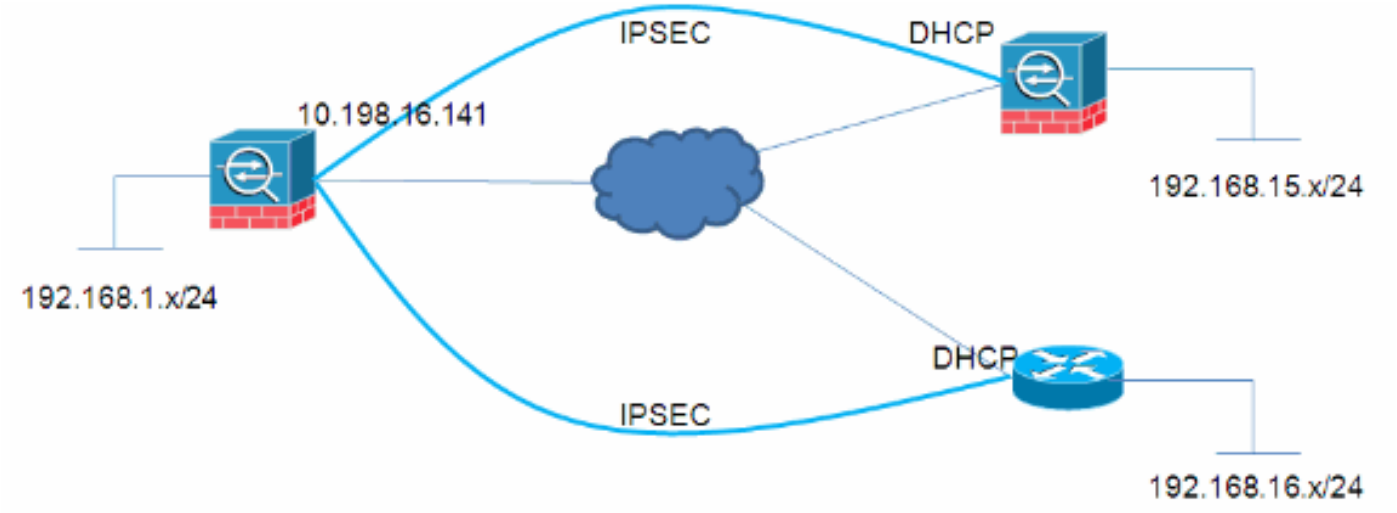
症状

このドキュメントの例では、ネットワーク管理者がVPNポリシーを作成する必要があります。このポリシーでは、ハブに接続する異なるリモートVPNスポークを別々のトンネルグループに接続し、各リモート接続に異なるVPNポリシーを適用できます。

原因/問題の説明

ダイナミックL2Lトンネルでは、トンネル（イニシエータ）の一方の側にダイナミックIPアドレスがあります。スタティックL2Lトンネルとは異なり、受信は送信元のIPアドレスを認識しないため、異なるピアが自動的にデフォルトL2Lグループに分類されます。ただし、状況によっては、これは許容できない場合があり、ユーザは異なるグループポリシーまたは事前共有キーを各ピアに割り当てる必要がある場合があります。

条件/環境



解決方法

これは、次の2つの方法で実現できます。

- **証明書**ASA上のトンネルグループルックアッププロセスは、スポークによって提示される証明書フィールドに基づいて接続を固定します。

```
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およびアグレッシブモード**すべてのユーザがPKIインフラストラクチャを持つわけではありません。ただし、次に示すように、アグレッシブモードパラメータを使用しても同じことが可能です。**ハブ**

```
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
```

スポーク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
```

スポーク2

```
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
```

ハブの検証

```
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 :
```

関連情報

- テクニカル サポートとドキュメント – Cisco Systems