해결책: 동적 L2L 터널이 다른 터널 그룹에 속하도록 만드는 방법

목차

소개

이 문서에서는 동적 L2L 터널이 서로 다른 터널 그룹에 속하도록 만드는 방법에 대한 정보를 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

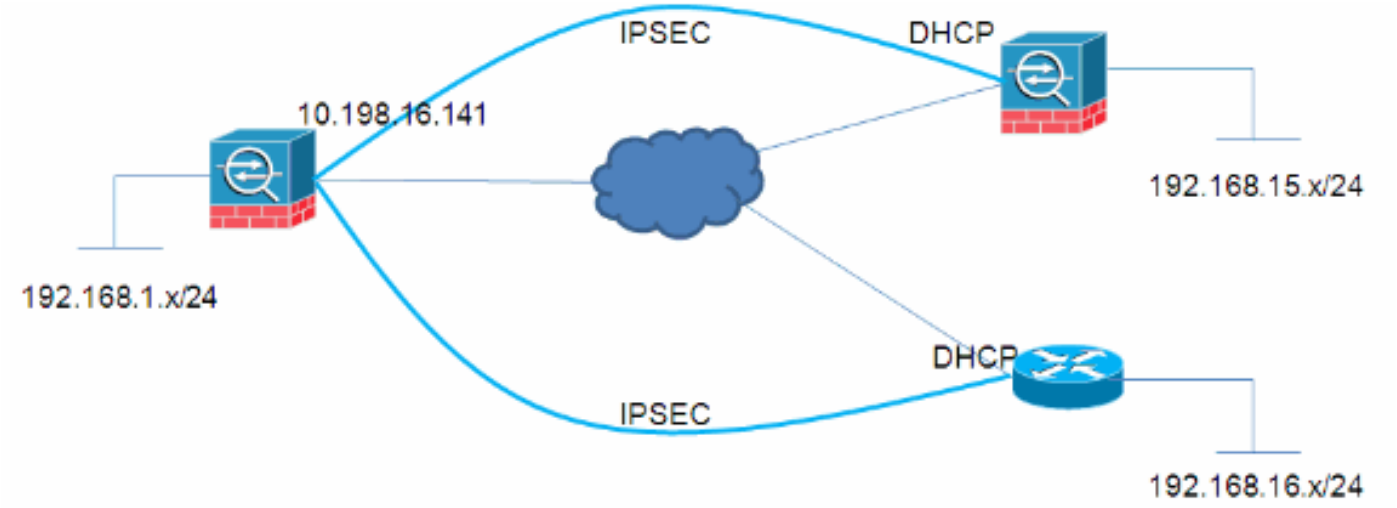
증상

이 문서의 예에서 네트워크 관리자는 허브에 연결하는 서로 다른 원격 VPN 스포크가 개별 터널 그룹에 연결되어야 각 원격 연결에 서로 다른 VPN 정책을 적용할 수 있는 VPN 정책을 생성해야 합니다.

원인/문제 설명

동적 L2L 터널에서 터널의 한 면(개시자)에는 동적 IP 주소가 있습니다. 수신은 고정 L2L 터널과 달리 어떤 IP 주소에서 오는지 모르기 때문에 다른 피어가 자동으로 기본 L2L 그룹에 속합니다. 그러나 경우에 따라 이는 허용되지 않으며 사용자가 각 피어에 다른 그룹 정책 또는 사전 공유 키를 할당해야 할 수도 있습니다.

조건/환경



해결

이 작업은 다음 두 가지 방법으로 수행할 수 있습니다.

- **인증서**ASA의 터널 그룹 조회 프로세스는 스포크가 제공한 인증서 필드를 기반으로 연결을 시작합니다.

```
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 및 적극적인 모드**모든 사용자에게 PKI 인프라가 있는 것은 아닙니다. 그러나 여기에 설명된 대로 aggressive mode 매개변수를 사용하여 동일한 작업을 수행할 수 있습니다.**허브**

```
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
```

스포크1

```
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
```

스포크2

```
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
```

허브 확인

```
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 :
```

관련 정보

- 기술 지원 및 문서 – Cisco Systems