

Solution: How to Make Dynamic L2L Tunnels Fall into Different Tunnel Groups

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Symptom](#)

[Cause / Problem Description](#)

[Conditions / Environment](#)

[Resolution](#)

[Related Information](#)

[Introduction](#)

This document provides information on how to make dynamic L2L tunnels fall into different tunnel groups.

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

This document is not restricted to specific software and hardware versions.

[Conventions](#)

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

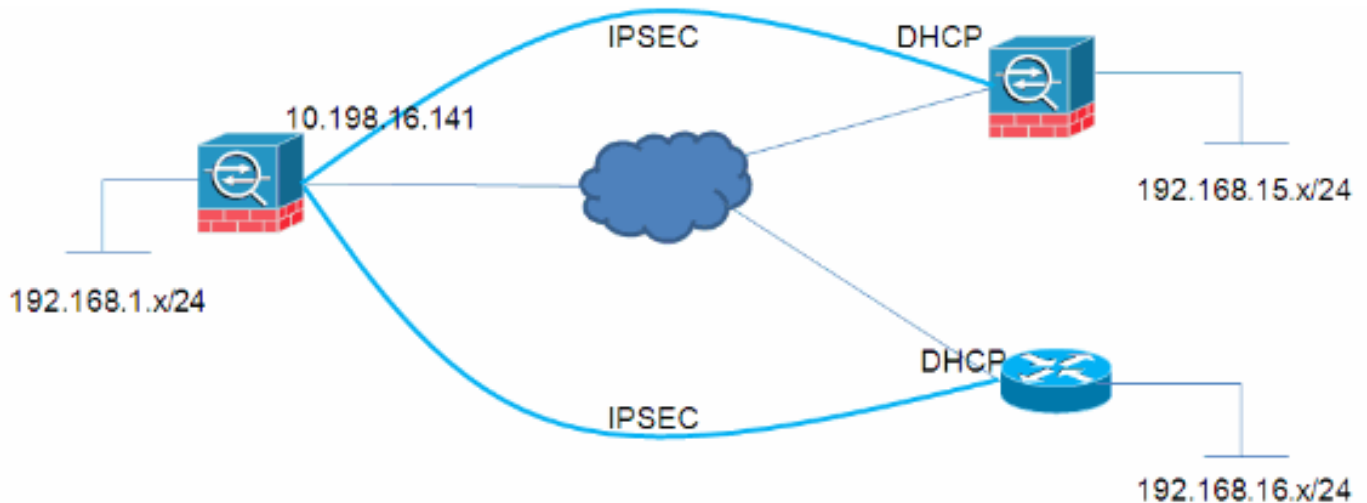
[Symptom](#)

In this document's example, the network administrator needs to create VPN policies where different remote VPN spokes connecting to a hub should connect to separate Tunnel-Groups so that different VPN policies can be applied to each remote connection.

Cause / Problem Description

In dynamic L2L tunnels, one side of the tunnel (the initiator) has a dynamic IP address. Because the receiver does not know which IP addresses they are coming from, unlike static L2L tunnels, different peers automatically fall into the Default L2L Group. However, in some situations this is not acceptable and the user might need to assign a different group-policy or pre-shared key to each peer.

Conditions / Environment



Resolution

This can be accomplished in these two ways:

- **Certificates** The tunnel-group lookup process on the ASA will land the connections based on a certificate field presented by the spokes.

```
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 and Aggressive Mode** Not all users will have a PKI infrastructure. However, the same can still be accomplished using an aggressive mode parameter as described here:**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 cisco456SPOKE1access-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 cisco123SPOKE2ip 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 VERIFICATIONSession 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 :

[Related Information](#)

- [Technical Support & Documentation - Cisco Systems](#)