

# Oplossing: Hoe u dynamische L2L-tunnels in verschillende tunnelgroepen kunt laten vallen

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Symptoom](#)

[Oorzaak / Beschrijving van probleem](#)

[Voorwaarden / milieu](#)

[Resolutie](#)

[Gerelateerde informatie](#)

## [Inleiding](#)

Dit document geeft informatie over hoe dynamische L2L-tunnels in verschillende tunnelgroepen kunnen worden ondergebracht.

## [Voorwaarden](#)

### [Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

### [Gebruikte componenten](#)

Dit document is niet beperkt tot specifieke software- en hardware-versies.

### [Conventies](#)

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\)](#) voor meer informatie over documentconventies.

## [Symptoom](#)

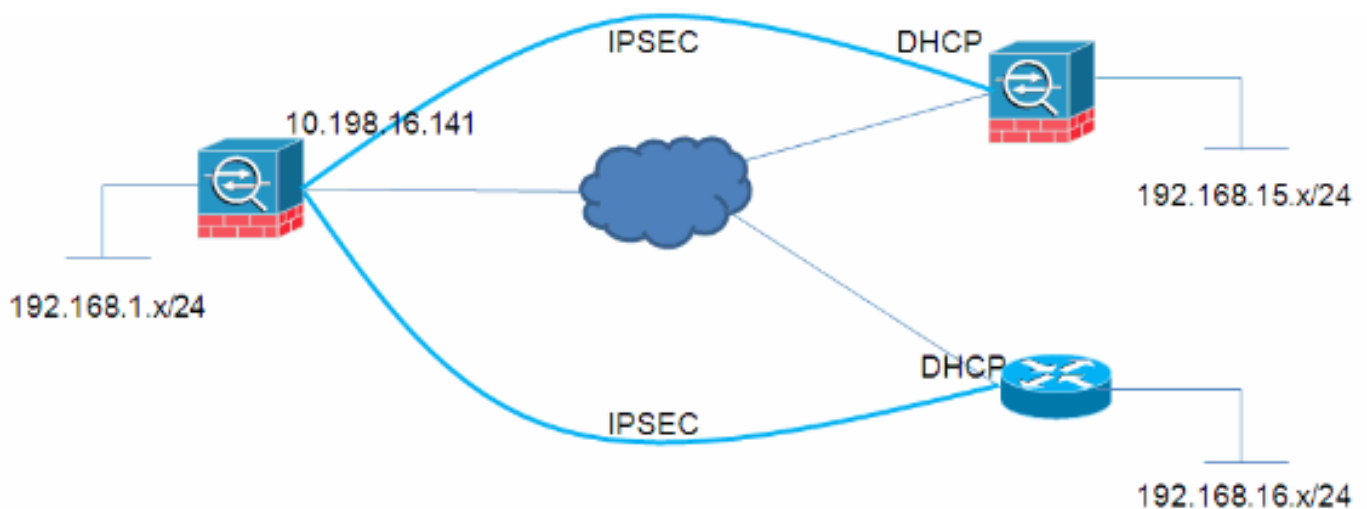
In het voorbeeld van dit document moet de netwerkbeheerder een beleid van VPN creëren waar de verschillende afstandsbediening van VPN die met een hub verbinden met afzonderlijke Tunnelgroepen moet verbinden zodat het verschillende beleid van VPN op elke externe verbinding kan

worden toegepast.

## Oorzaak / Beschrijving van probleem

In dynamische L2L-tunnels heeft één kant van de tunnel (de initiator) een dynamisch IP-adres. Omdat ontvanger niet weet van welke IP-adressen ze komen, in tegenstelling tot statische L2L-tunnels, vallen verschillende peers automatisch in de Default L2L Group. In sommige situaties is dit echter niet aanvaardbaar en de gebruiker kan een andere groep-beleid of een vooraf gedeelde sleutel aan elke peer toewijzen.

## Voorwaarden / milieu



## Resolutie

Dit kan op deze twee manieren worden bereikt:

- **Certificaten** De tunnelgroepsraadpleging op de ASA zal de verbindingen leggen op basis van een door de woordvoerders aangeboden certificatieveld.

```
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's en agressieve modus** Niet alle gebruikers zullen een PKI infrastructuur hebben. Hetzelfde kan echter nog worden bereikt met behulp van een agressieve mode-parameter zoals hier beschreven: **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
```

## SPOELEN1

```
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
```

## SPOELEN2

```
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
```

## HUB-VERIFICATIE

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  
SQ Int (T) : 0 Seconds  
Hold Left (T): 0 Seconds  
Redirect URL :

Reval Left(T): 0 Seconds  
EoU Age(T) : 9 Seconds  
Posture Token:

## [Gerelateerde informatie](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)