Solution : Comment transformer les tunnels dynamiques L2L tomber en différents groupes de tunnel

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Symptôme](#)
[Cause/description du problème](#)
[Conditions/environnement](#)
[Résolution](#)
[Informations connexes](#)

Introduction

Ce document fournit des informations sur la façon dont transformer les tunnels dynamiques L2L tomber en différents groupes de tunnel.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Symptôme

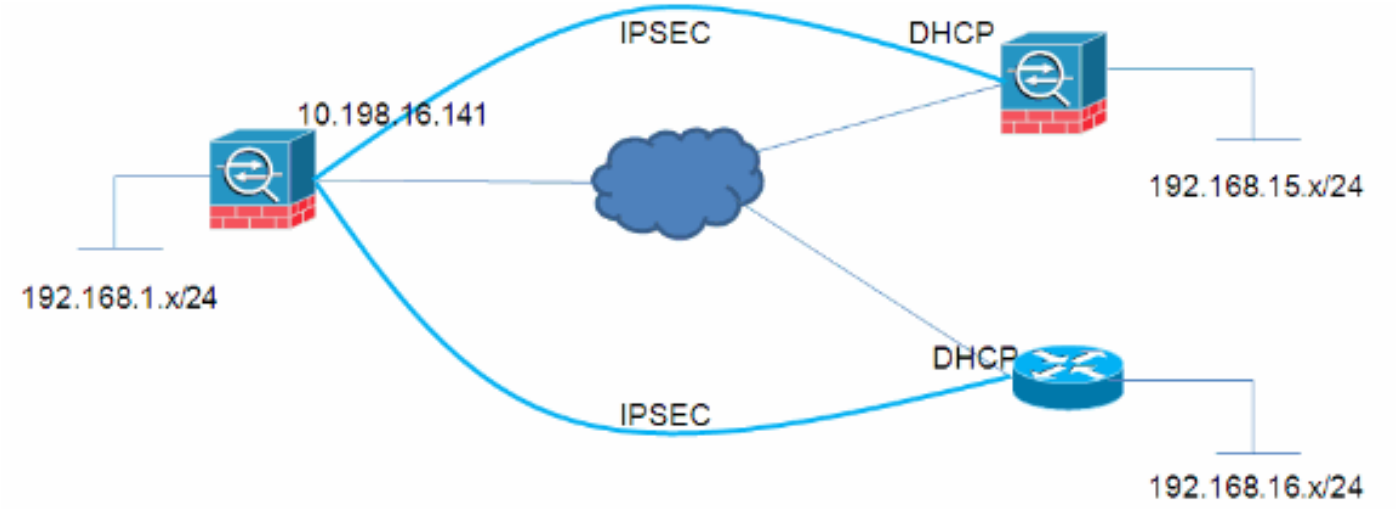
Dans l'exemple de ce document, l'administrateur réseau doit créer des règles VPN où les

différents rais du distant VPN se connectant à un hub devraient se connecter pour séparer des groupes de tunnels de sorte que différentes règles VPN puissent être appliquées à chaque connexion distante.

Cause/description du problème

Dans des tunnels dynamiques L2L, un côté du tunnel (le demandeur) a une adresse IP dynamique. Puisque la réception ne connaît pas quelles adresses IP elles proviennent, à la différence de L2L statique perce un tunnel, différents pairs tombent automatiquement dans le groupe du par défaut L2L. Cependant, dans certaines situations ce n'est pas acceptable et l'utilisateur pourrait devoir assigner une stratégie de groupe différente ou une clé pré-partagée à chaque pair.

Conditions/environnement



Résolution

Ceci peut être accompli de ces deux manières :

- **Certificats**Le processus de recherche de groupe de tunnels sur l'ASA débarquera les connexions basées sur un champ de certificat présenté par les rais.`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 et mode agressif**Non tous les utilisateurs auront une infrastructure de PKI. Cependant, les mêmes peuvent encore faire utilisant un paramètre agressif de mode comme décrit ici :**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
```

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
```

VÉRIFICATION DE HUB

```
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 :
```

Informations connexes

- Support et documentation techniques - Cisco Systems