Exemple de configuration de tunnel IPsec dynamique à dynamique

Contenu

Introduction

Ce document décrit comment construire un tunnel IPsec LAN à LAN entre les routeurs Cisco lorsque les deux extrémités ont des adresses IP dynamiques mais que le système de noms de domaine dynamique (DDNS) est configuré.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN site à site avec tunnel IPSec et encapsulation de routage générique (GRE)
- Interface de tunnel virtuel (VTI) IPsec
- Prise en charge DNS dynamique du logiciel Cisco IOS

Astuce : Référez-vous à la section Configuration du VPN du Cisco 3900, 2900 et 1900 Series Software Configuration Guide et à l'article Configuration d'une interface de tunnel virtuelle avec la sécurité IP pour plus d'informations.

Components Used

Les informations de ce document sont basées sur un routeur à services intégrés Cisco 2911 qui exécute la version 15.2(4)M6a.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

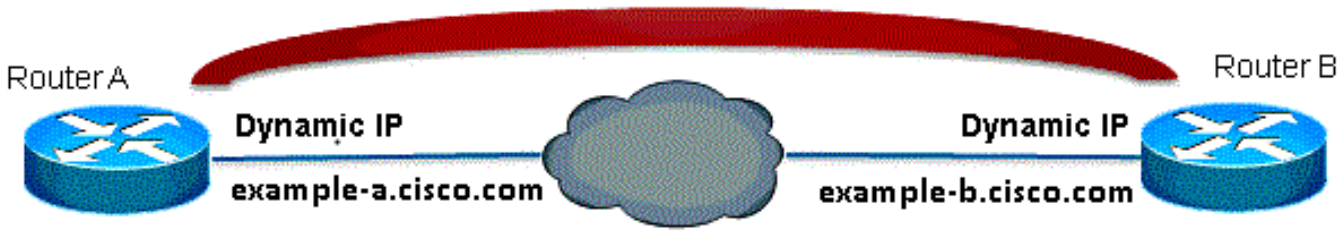
Lorsqu'un tunnel LAN à LAN doit être établi, l'adresse IP des deux homologues IPSec doit être connue. Si l'une des adresses IP n'est pas connue parce qu'elle est dynamique, telle qu'une adresse obtenue via DHCP, alors une alternative est d'utiliser une carte de chiffrement dynamique. Cela fonctionne, mais le tunnel ne peut être élevé que par l'homologue qui a l'adresse IP dynamique, car l'autre homologue ne sait pas où trouver son homologue.

Pour plus d'informations sur les protocoles dynamique à statique, référez-vous à Configuration d'IPSec dynamique à statique de routeur à routeur avec NAT.

Configuration

Résolution en temps réel pour homologue de tunnel IPsec

Cisco IOS® a introduit une nouvelle fonctionnalité dans la version 12.3(4)T qui permet de spécifier le nom de domaine complet (FQDN) de l'homologue IPSec. Lorsqu'il y a du trafic qui correspond à une liste d'accès de chiffrement, Cisco IOS résout le nom de domaine complet (FQDN) et obtient l'adresse IP de l'homologue. Il essaie ensuite d'ouvrir le tunnel.



Note: Cette fonctionnalité est limitée : la résolution des noms DNS pour les homologues IPsec distants ne fonctionnera que s'ils sont utilisés comme initiateur. Le premier paquet à chiffrer déclenchera une recherche DNS ; une fois la recherche DNS terminée, les paquets suivants déclencheront l'échange de clés Internet (IKE). La résolution en temps réel ne fonctionne pas sur le répondeur.

Afin de répondre à la limitation et de pouvoir initialiser le tunnel à partir de chaque site, vous disposerez d'une entrée de crypto-carte dynamique sur les deux routeurs afin que vous puissiez mapper les connexions IKE entrantes au crypto dynamique. Cela est nécessaire car l'entrée statique avec la fonctionnalité de résolution en temps réel ne fonctionne pas lorsqu'elle agit en tant que répondeur.

Router A

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-b.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

Router B

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
```

```
permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-a.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

Remarque : comme vous ne savez pas quelle adresse IP le FQDN utilisera, vous devez utiliser une clé pré-partagée générique : 0.0.0.0 0.0.0.0

Mise à jour de la destination du tunnel avec Embedded Event Manager (EEM)

Vous pouvez également VTI afin d'accomplir ceci. La configuration de base est présentée ici :

Router A

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-b.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

Router B

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2
```

```
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-a.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

Une fois la configuration précédente en place avec un nom de domaine complet (FQDN) comme destination du tunnel, la commande **show run** affiche l'adresse IP au lieu du nom. C'est parce que la résolution n'a lieu qu'une fois :

```
RouterA(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.201.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end

RouterB(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.200.225
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

Une solution de contournement est de configurer une applet afin de résoudre la destination du tunnel toutes les minutes :

Router A

```
event manager applet change-tunnel-dest
event timer cron name TAC cron-entry "* * * * *"
action 1.0 cli command "enable"
action 1.1 cli command "configure terminal"
action 1.2 cli command "interface tunnel1"
action 1.3 cli command "tunnel destination example-b.cisco.com"
```

Router B

```
event manager applet change-tunnel-dest
event timer cron name TAC cron-entry "* * * * *"
```

```
action 1.0 cli command "enable"
action 1.1 cli command "configure terminal"
action 1.2 cli command "interface tunnel1"
action 1.3 cli command "tunnel destination example-a.cisco.com"
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

```
RouterA(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.200.225 YES NVRAM up up
FastEthernet0/1 192.168.10.1 YES NVRAM up up
Tunnel1 172.16.12.1 YES manual up up


RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.201.1 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up

RouterA(config)#do show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.201.1 QM_IDLE 2 0 ACTIVE

RouterB(config)#do show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.201.1 QM_IDLE 1002 0 ACTIVE

RouterA(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.200.225

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 209.165.201.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 209.165.200.225, remote crypto endpt.: 209.165.201.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x8F1592D2(2400555730)

inbound esp sas:
spi: 0xF7B373C0(4155732928)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: AIM-VPN/BPII-PLUS:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4501866/3033)
```

```
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8F1592D2(2400555730)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: AIM-VPN/BPII-PLUS:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4501866/3032)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

```
RouterB(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.201.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 209.165.200.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 209.165.201.1, remote crypto endpt.: 209.165.200.225
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF7B373C0(4155732928)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8F1592D2(2400555730)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4424128/3016)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF7B373C0(4155732928)
transform: esp-3des esp-sha-hmac ,
```

```
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4424128/3016)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Après avoir modifié l'enregistrement DNS pour b.cisco.com sur le serveur DNS de 209.165.201.1 à 209.165.202.129, le module EEM fera réaliser le routeur A et le tunnel reprendra avec la nouvelle adresse IP correcte.

```
RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.202.129 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up
```

```
RouterA(config-if)#do show run int tunn1
Building configuration...

Current configuration : 192 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.252
tunnel source fastethernet0/0
tunnel destination 209.165.202.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end

Router1841A#show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.202.129 QM_IDLE 3 0 ACTIVE
```

Dépannage

Vous pouvez vous référer aux débogages IOS IPSec et IKE - Dépannage du mode principal IKEv1 pour le dépannage IKE/IPsec courant.

Informations connexes

- Résolution en temps réel pour homologue de tunnel IPsec
- Support et documentation techniques - Cisco Systems