Dynamique à l'exemple dynamique de configuration de tunnel d'IPsec

Contenu

Introduction

Ce document décrit comment construire un tunnel d'IPsec d'entre réseaux locaux entre les Routeurs de Cisco quand les deux extrémités ont des adresses IP dynamiques mais le Dynamic Domain Name System (DDNS) est configuré.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Site à site VPN avec un tunnel et l'Encapsulation de routage générique (GRE) d'IPSec
- Interface de tunnel virtuelle d'IPsec (VTI)
- [Soutien dynamique de DN de logiciel de Cisco IOS](#)

Conseil : Référez-vous à la section de configuration VPN de la gamme Cisco 3900, gamme 2900, et guide de configuration du logiciel de gamme 1900 et la configuration d'une interface de tunnel virtuelle avec le pour en savoir plus d'article de sécurité IP.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Quand un tunnel entre réseaux locaux doit être établi, l'adresse IP des deux pairs d'IPSec doit être connue. Si une des adresses IP n'est pas connue parce qu'elle est dynamique, comme une obtenue par l'intermédiaire du DHCP, alors d'une alternative est utiliser une crypto-carte dynamique. Ceci fonctionne, mais le tunnel peut seulement être apporté par le pair qui a l'IP address dynamique puisque l'autre pair ne sait pas où trouver son pair.

Pour plus d'informations sur dynamique à la charge statique, référez-vous à configurer le routeur à routeur IPSec Dynamique-à-statique avec NAT.

Configurez

Résolution en temps réel pour le pair de tunnel d'IPsec

Le Cisco IOS® a introduit une nouvelle caractéristique dans la version 12.3(4)T qui permet le Fully Qualified Domain Name (FQDN) du pair d'IPSec à spécifier. Quand il y a du trafic qui apparie une crypto liste d'accès, l'IOS de Cicso alors résout le FQDN et obtient l'adresse IP du pair. Il puis essais pour apporter le tunnel.

Remarque: Il y a une limite sur cette caractéristique : La résolution de noms DNS pour les pairs distants d'IPsec fonctionnera seulement s'ils sont utilisés comme demandeur. Le

premier paquet qui doit être chiffré déclenchera une consultation de DN ; après que la consultation de DN soit complète, les paquets suivants déclencheront l'Échange de clés Internet (IKE). La résolution en temps réel ne travaillera pas au responder.

Afin d'adresser la limite et pouvoir initier le tunnel de chaque site, vous aurez une entrée dynamique de la carte de chiffrement sur les deux Routeurs ainsi vous pouvez tracer les connexions entrantes d'IKE au crypto dynamique. C'est nécessaire puisque l'entrée statique avec la configuration en temps réel de résolution ne fonctionne pas quand elle agit en tant que responder.

routeur 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
```

routeur 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: Puisque vous ne connaissez pas quelle adresse IP le FQDN utilisera, vous devez utiliser un pre-shared-key de masque : 0.0.0.0 0.0.0.0

Mise à jour de destination de tunnel avec le gestionnaire encastré d'événement (EEM)

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

routeur 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
```

routeur 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 que la configuration précédente est en place avec un FQDN comme destination de tunnel, l'**exposition exécutent la** commande affiche l'adresse IP au lieu du nom. C'est parce que la résolution se produit juste 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
```

Un contournement pour ceci est de configurer un applet afin de résoudre la destination de tunnel chaque minute :

routeur 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"
```

routeur 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"
```

Vérifiez

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 que vous changiez l'enregistrement DNS pour b.cisco.com sur le serveur DNS de 209.165.201.1 à 209.165.202.129, l'EEM incitera le routeur A de cause pour réaliser et le tunnel rétablira 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
```

Dépannez

Vous pouvez se référer à IOS IPSec et l'IKE met au point - le dépannage principal du mode IKEv1 pour le dépannage commun IKE/IPsec.

Informations connexes

- Résolution en temps réel pour le pair de tunnel d'IPsec
- Support et documentation techniques - Cisco Systems