Routeur VPN IOS : Exemple de configuration d'ajout ou de suppression d'un tunnel VPN LAN à LAN

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour que la façon ajoute ou retire un réseau sur un tunnel VPN existant de l'entre réseaux locaux (L2L).

Conditions préalables

Conditions requises

Assurez-vous que vous configurez correctement votre tunnel VPN du courant L2L IPsec avant que vous tentiez cette configuration.

Composants utilisés

Les informations dans ce document sont basées sur deux Routeurs de Cisco IOS® qui exécutent la version de logiciel 12.4(15)T1.

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.

Conventions

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

Informations générales

Il y a actuellement un tunnel VPN L2L entre les sièges sociaux (QG) bureau et la succursale (BO). Le bureau QG a juste ajouté un nouveau réseau à utiliser par l'équipe de vente. Cette équipe a besoin de l'accès aux ressources qui résident dans le bureau de la BO. La tâche actuelle est d'ajouter un nouveau réseau au tunnel VPN déjà existant L2L.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations décrites dans cette section. Ces configurations incluent un L2L VPN qui fonctionne entre le réseau de 172.16.10.0 du bureau QG et le réseau de 10.10.10.0 du bureau de la BO. La sortie affichée en texte en gras affiche que la configuration exigée intégrait le nouveau réseau 192.168.10.0 du bureau QG dans le même tunnel VPN avec 10.10.10.0 que le réseau de destination.

QG-routeur

```
HQ-Router#show running-config Building configuration...
Current configuration : 1439 bytes ! version 12.4
service timestamps debug uptime service timestamps log
uptime no service password-encryption ! hostname HQ-
Router ! !--- Output suppressed. ! crypto isakmp policy
1 hash md5 authentication pre-share crypto isakmp key
cisco123 address 209.165.200.225 ! ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac ! crypto map
rtp 1 ipsec-isakmp set peer 209.165.200.225 set
transform-set rtpset match address 115 ! interface
Ethernet0 ip address 172.16.10.1 255.255.255.0 ip nat
inside ! interface Ethernet1 ip address 209.165.201.2
255.255.255.224 ip nat outside crypto map rtp !
interface Ethernet2 ip address 192.168.10.1
255.255.255.0 ip nat inside ! interface Serial0 no ip
address shutdown no fair-queue ! interface Serial1 no ip
address shutdown ! ip nat inside source route-map nonat
interface Ethernet1 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.201.1 ! !--- Output suppressed.
access-list 110 deny ip 172.16.10.0 0.0.0.255 10.10.10.0
```

```
0.0.0.255 access-list 110 permit ip 172.16.10.0
0.0.0.255 any ! !--- Add this ACL entry to include
192.168.10.0 !--- network with the nat-exemption rule.
access-list 110 deny ip 192.168.10.0 0.0.0.255
10.10.10.0 0.0.0.255 access-list 110 permit ip
192.168.10.0 0.0.0.255 any access-list 115 permit ip
172.16.10.0 0.0.0.255 10.10.10.0 0.0.0.255 ! !--- Add
this ACL entry to include 192.168.10.0 !--- network into
the crypto map. access-list 115 permit ip 192.168.10.0
0.0.0.255 10.10.10.0 0.0.0.255 route-map nonat permit 10
match ip address 110 ! !--- Output suppressed. end
```

BO-routeur

```
BO-Router#show running-config Building configuration...
Current configuration : 2836 bytes ! version 12.4
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname BO-Router ! !--- Output
suppressed. ! crypto isakmp policy 1 hash md5
authentication pre-share crypto isakmp key cisco123
address 209.165.201.2 ! ! crypto ipsec transform-set
rtpset esp-des esp-md5-hmac ! crypto map rtp 1 ipsec-
isakmp set peer 209.165.201.2 set transform-set rtpset
match address 115 ! !--- Output suppressed. interface
FastEthernet0/0 ip address 209.165.200.225
255.255.255.224 ip nat outside ip virtual-reassembly
duplex auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.10.10.1 255.255.255.0 ip
nat inside ip virtual-reassembly duplex auto speed auto
! ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 ! !--- Output
suppressed. ! ip http server no ip http secure-server ip
nat inside source route-map nonat interface
FastEthernet0/0 overload ! !--- Add this ACL entry to
include 192.168.10.0 !--- network with the nat-exemption
rule. access-list 110 deny ip 10.10.10.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 access-list
110 permit ip 10.10.10.0 0.0.0.255 any access-list 115
permit ip 10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 !
!--- Add this ACL entry to include 192.168.10.0 !---
network into the crypto map. access-list 115 permit ip
10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255 ! route-map
nonat permit 10 match ip address 110 ! !--- Output
suppressed. ! end
```

Retirez un réseau d'un tunnel d'IPsec

Terminez-vous les étapes décrites dans cette section afin de retirer le réseau de la configuration de tunnel d'IPsec. Notez que le réseau 192.168.10.0/24 a été retiré de la configuration de routeur QG.

1. Employez cette commande afin de démolir la connexion d'IPsec :`HQ-Router#`**`clear crypto sa`**
2. Employez cette commande afin d'effacer les associations d'ISAKMPSecurity (SAS) :`HQ-Router#`**`clear crypto isakmp`**
3. Employez cette commande afin de retirer l'ACL du trafic intéressant pour le tunnel d'IPsec :`HQ-Router(config)#`**`no access-list 115 permit ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255`**
4. Employez cette commande afin de retirer la déclaration nat-exempte d'ACL pour le réseau de 192.168.10.0 :`HQ-Router(config)#`**`no access-list 110 deny ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255`**

5. Employez cette commande afin d'effacer la traduction NAT :`HQ-Router#clear ip nat translation *`
6. Employez ces commandes afin de retirer et réappliquer le crypto map sur l'interface pour s'assurer que la crypto configuration en cours la prend effet :`HQ-Router(config)#int ethernet 1 HQ-Router(config-if)#no crypto map rtp *May 25 10:35:12.153: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF HQ-Router(config-if)#crypto map rtp *May 25 10:36:09.305: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON` **Remarque:** Retirer le crypto map de l'interface déchire toutes les connexions VPN existantes associées avec ce crypto map. Avant de faire ceci, assurez-vous s'il vous plaît que vous avez pris le temps d'arrêt prié et avez suivi la politique de contrôle de modification de votre organisation en conséquence.
7. Employez la commande de **write memory** afin de sauvegarder la configuration active à l'éclair.
8. Terminez-vous ces étapes sur l'autre extrémité du tunnel VPN (BO-routeur) afin de retirer les configurations.
9. Initiez le tunnel d'IPsec et vérifiez la connexion.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Employez cet ordre de ping afin de s'assurer que le nouveau réseau peut passer des données par le tunnel VPN :

```
HQ-Router#clear crypto sa HQ-Router# HQ-Router#ping 10.10.10.1 source 172.16.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 172.16.10.1 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms HQ-Router#ping 10.10.10.1 source 192.168.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.10.1 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms HQ-Router#ping 10.10.10.1 source 192.168.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.10.1 !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

show crypto ipsec sa

```
HQ-Router#show crypto ipsec sa interface: Ethernet1
Crypto map tag: rtp, local addr. 209.165.201.2 local
ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 9, #pkts encrypt:
9, #pkts digest 9 #pkts decaps: 9, #pkts decrypt: 9,
#pkts verify 9 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: FB52B5AB
inbound esp sas: spi: 0x612332E(101856046) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2002, flow_id: 3, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607998/3209) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xFB52B5AB(4216501675) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2003,
flow_id: 4, crypto map: rtp sa timing: remaining key
```

```
lifetime (k/sec): (4607998/3200) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
local ident (addr/mask/prot/port):
(172.16.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt:
4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4,
#pkts verify 4 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: C9E9F490
inbound esp sas: spi: 0x1291F1D3(311554515) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2000, flow_id: 1, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607999/3182) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xC9E9F490(3387552912) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2001,
flow_id: 2, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607999/3182) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
```

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Utilisez cette section afin de dépanner votre configuration.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** — affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** — Affiche les sessions chiffrées.

Informations connexes

- Présentation du chiffrement IPSec (IP Security)
- Page de support de la négociation IPSec/des protocoles IKE
- Configuration d'un poste LAN à LAN dynamique de routeur IPSec et de clients VPN
- Support et documentation techniques - Cisco Systems