IOS VPN (routeur) : Ajouter un nouveau tunnel LAN à LAN ou un accès à distance à un VPN LAN à LAN existant

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Diagramme du réseau
Informations générales
Ajoutez un tunnel supplémentaire L2L à la configuration
Instructions pas à pas
Exemple de configuration
Ajoutez un Accès à distance VPN à la configuration
Instructions pas à pas
Exemple de configuration
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document présente les étapes nécessaires pour ajouter un nouveau tunnel VPN site à site (L2L) ou un VPN d'accès à distance à une configuration site à site qui existe déjà dans un routeur IOS.

Conditions préalables

Conditions requises

Assurez-vous que vous configurez correctement le tunnel VPN L2L IPSec qui est actuellement opérationnel avant que vous tentiez cette configuration.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Deux Routeurs IOS qui exécutent les versions de logiciel 12.4 et 12.2
- Une appliance de sécurité adaptable Cisco (ASA) cette exécute la version de logiciel 8.0

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Ces sorties sont les configurations en cours d'exécution du routeur QG (HUB) et de la succursale 1 (BO1) ASA. Dans cette configuration, il y a un tunnel d'IPSec L2L configuré entre le QG et le BO1 ASA.

Configuration de routeur QG de courant (HUB)

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
!
```

```
!
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Configuration BO1 ASA

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
```

```
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list 100 extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list nonat extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
```

```
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

Informations générales

Actuellement, il y a un tunnel existant L2L installé entre le bureau QG et le bureau BO1. Votre société a récemment ouvert une nouvelle succursale (BO2). Ce nouveau bureau exige la Connectivité aux ressources locales qui se trouvent dans le bureau QG. En outre, il y a une condition requise supplémentaire de permettre à des employés l'occasion de fonctionner de la maison et d'accéder à sécurisé les ressources qui se trouvent sur le réseau interne à distance. Dans cet exemple, un nouveau tunnel VPN est configuré aussi bien qu'un serveur VPN d'Accès à distance qui se trouve dans le le bureau QG.

Ajoutez un tunnel supplémentaire L2L à la configuration

C'est le schéma de réseau pour cette configuration :

Instructions pas à pas

Cette section fournit les procédures exigées qui doivent être exécutées sur le routeur QG de HUB.

Procédez comme suit :

1. Créez cette nouvelle liste d'accès à utiliser par le crypto map afin de définir le trafic intéressant :
   ```
   HQ_HUB(config)#ip access-list extended VPN_BO2
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#exit
   ```

   Avertissement : Pour que la transmission ait lieu, l'autre côté du tunnel doit avoir l'opposé de cette entrée de liste de contrôle d'accès (ACL) pour ce réseau particulier.
2. Ajoutez ces entrées à l'aucune déclaration nat afin d'exempter nating entre ces réseaux :
   ```
   HQ_HUB(config)#ip access-list extended NAT_Exempt
   HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
   HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
   ```

   Ajoutez ces ACLs au **nonat de** carte de route existante :

```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```

Avertissement : Pour que la transmission ait lieu, l'autre côté du tunnel doit avoir l'opposé de ce rubrique de liste ACL pour ce réseau particulier.

3. Spécifiez l'adresse de pair dans la configuration de la phase 1 comme affichée :
```
HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2
```

Note: Le pre-shared-key doit s'assortir exactement des deux côtés du tunnel.

4. Créez la configuration de crypto map pour le nouveau tunnel VPN. Utilisez le même jeu de transformations qui a été utilisé en la première configuration du VPN, comme toutes les configurations de la phase 2 sont les mêmes.
```
HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
 HQ_HUB(config-crypto-map)#set peer 192.168.12.2
 HQ_HUB(config-crypto-map)#set transform-set newset
 HQ_HUB(config-crypto-map)#match address VPN_BO2
```

5. Maintenant que vous avez configuré le nouveau tunnel, vous devez envoyer le trafic intéressant à travers le tunnel afin de l'apporter. Afin d'exécuter ceci, émettez la commande ping étendue de cingler un hôte sur le réseau intérieur du tunnel distant.Dans cet exemple, un poste de travail de l'autre côté du tunnel avec l'adresse 10.20.20.16 est cinglé. Ceci apporte le tunnel entre le QG et le BO2. Maintenant, il y a deux tunnels connectés au bureau QG. Si vous n'avez pas accès à un système derrière le tunnel, référez-vous à la plupart des solutions communes de dépannage VPN d'IPSec L2L et d'Accès à distance pour trouver une solution alternative utilisant Gestion-Access.

Exemple de configuration

HUB_HQ - A ajouté une nouvelle configuration de tunnel VPN L2L

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
```

```
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
```

```
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Configuration de tunnel VPN BO2 L2L

```
BO2#show running-config
Building configuration...

3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match address 100
!
!
!
!
interface Ethernet0
 ip address 10.20.20.10 255.255.255.0
 ip nat inside
!

!
interface Ethernet1
 ip address 192.168.12.2 255.255.255.0
 ip nat outside
 crypto map map1
!
interface Serial0
 no ip address
```

```
 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 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0
0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

Ajoutez un Accès à distance VPN à la configuration

C'est le schéma de réseau pour cette configuration :

Dans cet exemple, la caractéristique appelée la **Segmentation de tunnel** est utilisée. Cette caractéristique permet à un client d'IPSec de remote-access pour diriger conditionnellement des paquets au-dessus d'un tunnel d'IPSec sous la forme chiffrée, ou à une interface réseau sous la forme des textes clairs. La Segmentation de tunnel étant activé, des paquets non attachés pour des destinations de l'autre côté du tunnel d'IPSec ne doivent pas être chiffrés, envoyé à travers le tunnel, ont déchiffré, et alors conduit à une destination définitive. Ce concept s'applique la stratégie de Segmentation de tunnel à un réseau spécifié. Le par défaut est de percer un tunnel tout le trafic. Afin de placer une stratégie de Segmentation de tunnel, spécifiez un ACL où le trafic signifié pour l'Internet peut être mentionné.

Instructions pas à pas

Cette section fournit les procédures exigées pour ajouter la capacité d'Accès à distance et pour permettre à des utilisateurs distants pour accéder à tous les sites.

Procédez comme suit :

1. Créez un groupe d'adresse IP à utiliser pour les clients qui se connectent par l'intermédiaire du tunnel VPN. En outre, créez un utilisateur de base afin d'accéder au VPN une fois que la configuration est terminée.
   ```
   HQ_HUB(config)#ip local pool ippool 10.10.120.10 10.10.120.50
   ```

```
HQ_HUB(config)#username vpnuser password 0 vpnuser123
```

2. Le trafic spécifique exempt de nated.

```
HQ_HUB(config)#ip access-list extended NAT_Exempt
HQ_HUB(config-ext-nacl)#deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip host 10.10.10.0 any
HQ_HUB(config-ext-nacl)#exit
```

   Ajoutez ces ACLs au **nonat de** carte de route existante :

```
HQ_HUB(config)#route-map nonat permit 10
HQ_HUB(config-route-map)#match ip address NAT_Exempt
HQ_HUB(config)#ip nat inside source route-map nonat interface Serial2/0 overload
```

   Notez que la transmission nat entre les tunnels VPN est exemptée dans cet exemple.

3. Permettez la transmission entre les tunnels L2L et les utilisateurs existants de l'Accès à distance VPN.

```
HQ_HUB(config)#ip access-list extended VPN_BO1
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

   Ceci permet à des utilisateurs d'Accès à distance la capacité de communiquer avec des réseaux derrière les tunnels spécifiés.**Avertissement :** Pour que la transmission ait lieu, l'autre côté du tunnel doit avoir l'opposé de ce rubrique de liste ACL pour ce réseau particulier.

4. **Configurez la Segmentation de tunnel**Afin d'activer la Segmentation de tunnel pour les connexions VPN, veillez-vous pour configurer un ACL sur le routeur. Dans cet exemple, la commande de **split_tunnel de liste d'accès** est associée avec le groupe pour des buts de partitionner la mise en tunnel, et le tunnel est formé à 10.10.10.0 /24 et 10.20.20.0/24 et 172.16.1.0/24 réseaux. La circulation décryptée aux périphériques pas dans le tunnel partagé d'ACL (par exemple, l'Internet).

```
HQ_HUB(config)#ip access-list extended split_tunnel
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

5. Configurez l'authentification locale, l'autorisation et les informations de configuration de client, telles que des wins, des dn. acl du trafic intéressant et groupe d'IP, pour les clients vpn.

```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthor local
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
HQ_HUB(config-isakmp-group)#key cisco123
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
HQ_HUB(config-isakmp-group)#domain cisco.com
HQ_HUB(config-isakmp-group)#pool ippool
```

```
HQ_HUB(config-isakmp-group)#acl split_tunnel
HQ_HUB(config-isakmp-group)#exit
```

6. Configurez les informations requises dynamiques de carte et de carte de cryto à la création de tunnel VPN.

```
HQ_HUB(config)#crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#match identity group vpngroup
HQ_HUB(config-isakmp-group)#client authentication list userauthen
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthor
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

Exemple de configuration

Exemple de configuration 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
```

```
 domain cisco.com
 pool ippool
 acl split_tunnel
crypto isakmp profile vpnclient
   match identity group vpngroup
   client authentication list userauthen
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
hmac
!
crypto dynamic-map dynmap 10
 set transform-set remote-set
 set isakmp-profile vpnclient
 reverse-route
!
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255



!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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** .

- **ping** — Cette commande te permet pour initier le tunnel VPN L2L comme affiché.

Dépannez

Référez-vous à ces documents pour information que vous pouvez employer afin de dépanner votre configuration :

- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage

Conseil : Quand vous autorisez des associations de sécurité, et il ne résout pas un problème d'IPsec VPN, alors retirez et réappliquez le crypto map approprié afin de résoudre une grande variété de problèmes.

Avertissement : Si vous retirez un crypto map d'une interface, elle réduit tous les tunnels d'IPSec associés avec ce crypto map. Suivez ces étapes avec prudence et tenez compte de la politique de contrôle de modification de votre organisation avant de commencer.

Exemple

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
```

```
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

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