

Tunnel dynamique d'IPsec entre une ASA statiquement adressée et un routeur Cisco IOS dynamiquement adressé qui utilise l'exemple de configuration CCP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Vérifiez les paramètres de tunnel par le CCP](#)

[Vérifiez l'état de tunnel par ASA CLI](#)

[Vérifiez les paramètres de tunnel par le routeur CLI](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document fournit une configuration d'échantillon pour que la façon permette aux dispositifs de sécurité PIX/ASA de recevoir les connexions dynamiques d'IPsec du routeur de Cisco IOS®. Dans ce scénario, le tunnel d'IPsec établit quand le tunnel est initié de l'extrémité de routeur seulement. L'ASA n'a pas pu initier un tunnel VPN en raison de la configuration dynamique d'IPsec.

Cette configuration permet aux dispositifs de sécurité PIX de créer un tunnel dynamique de l'entre réseaux locaux d'IPsec (L2L) avec un routeur VPN distant. Ce routeur reçoivent dynamiquement son adresse IP publique extérieure de son fournisseur d'accès Internet. Le protocole DHCP (DHCP) fournit ce mécanisme afin d'allouer des adresses IP dynamiquement du fournisseur. Ceci permet des adresses IP à réutiliser quand les hôtes n'ont besoin plus de elles.

La configuration sur le routeur est faite avec l'utilisation du [Cisco Configuration Professional](#) (CCP). Le CCP est un outil de Gestion de périphériques basé sur GUI qui te permet pour configurer les Routeurs basés sur IOS de Cisco. Référez-vous à la [configuration de base du routeur utilisant le Cisco Configuration Professional](#) pour plus d'informations sur la façon configurer un routeur avec le CCP.

Référez-vous au [site à site VPN \(L2L\) avec l'ASA](#) pour plus d'exemples d'information et de configuration sur l'établissement de tunnel d'IPsec qui utilisent l'ASA et les routeurs Cisco IOS.

Référez-vous au [site à site VPN \(L2L\) avec le](#) pour en savoir plus [IOS](#) et un exemple de configuration sur l'établissement dynamique de tunnel d'IPSec avec l'utilisation de PIX et de routeur Cisco IOS.

Conditions préalables

Conditions requises

Avant que vous tentiez cette configuration, assurez-vous que l'ASA et le routeur ont la connexion Internet afin d'établir le tunnel IPSEC.

Composants utilisés

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

- Cisco IOS Router 1812 qui exécute la version du logiciel Cisco IOS 12.4
- Version de logiciel 8.0.3 de Cisco ASA 5510

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

Dans ce scénario, le réseau de 192.168.100.0 est derrière le réseau ASA et de 192.168.200.0 est derrière le routeur Cisco IOS. On le suppose que le routeur obtient son annonce publique par le DHCP de son ISP. Car ceci pose un problème dans la configuration d'un pair statique sur l'extrémité ASA, vous devez approcher la manière de la crypto configuration dynamique d'établir un tunnel de site à site entre l'ASA et le routeur Cisco IOS.

Les internautes à l'extrémité ASA obtiennent traduit à l'adresse IP de son interface extérieure. On le suppose que NAT n'est pas configuré sur l'extrémité de routeur Cisco IOS.

Maintenant ce sont les étapes principales à configurer sur l'extrémité ASA afin d'établir le tunnel dynamique :

1. Configuration relative d'ISAKMP de Phase 1
2. Configuration de nat exemption
3. Configuration de crypto-carte dynamique

Le routeur Cisco IOS fait configurer un crypto map statique parce qu'on assume que l'ASA a une

adresse IP publique statique. Maintenant c'est la liste d'étapes principales à configurer sur l'extrémité de routeur Cisco IOS pour établir le tunnel dynamique IPSEC.

1. Configuration relative d'ISAKMP de Phase 1
2. Configuration relative de crypto map statique

Ces étapes sont décrites en détail dans ces configurations.

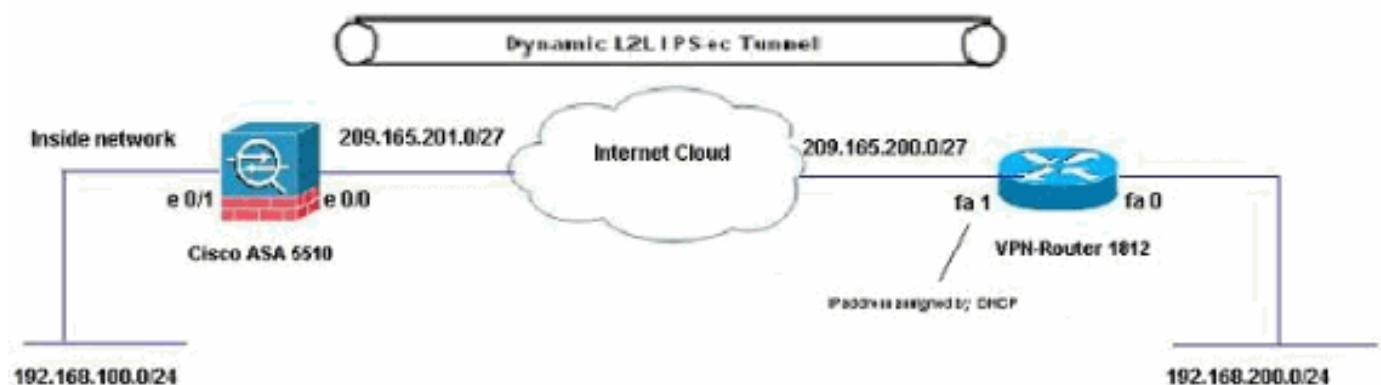
Configurez

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

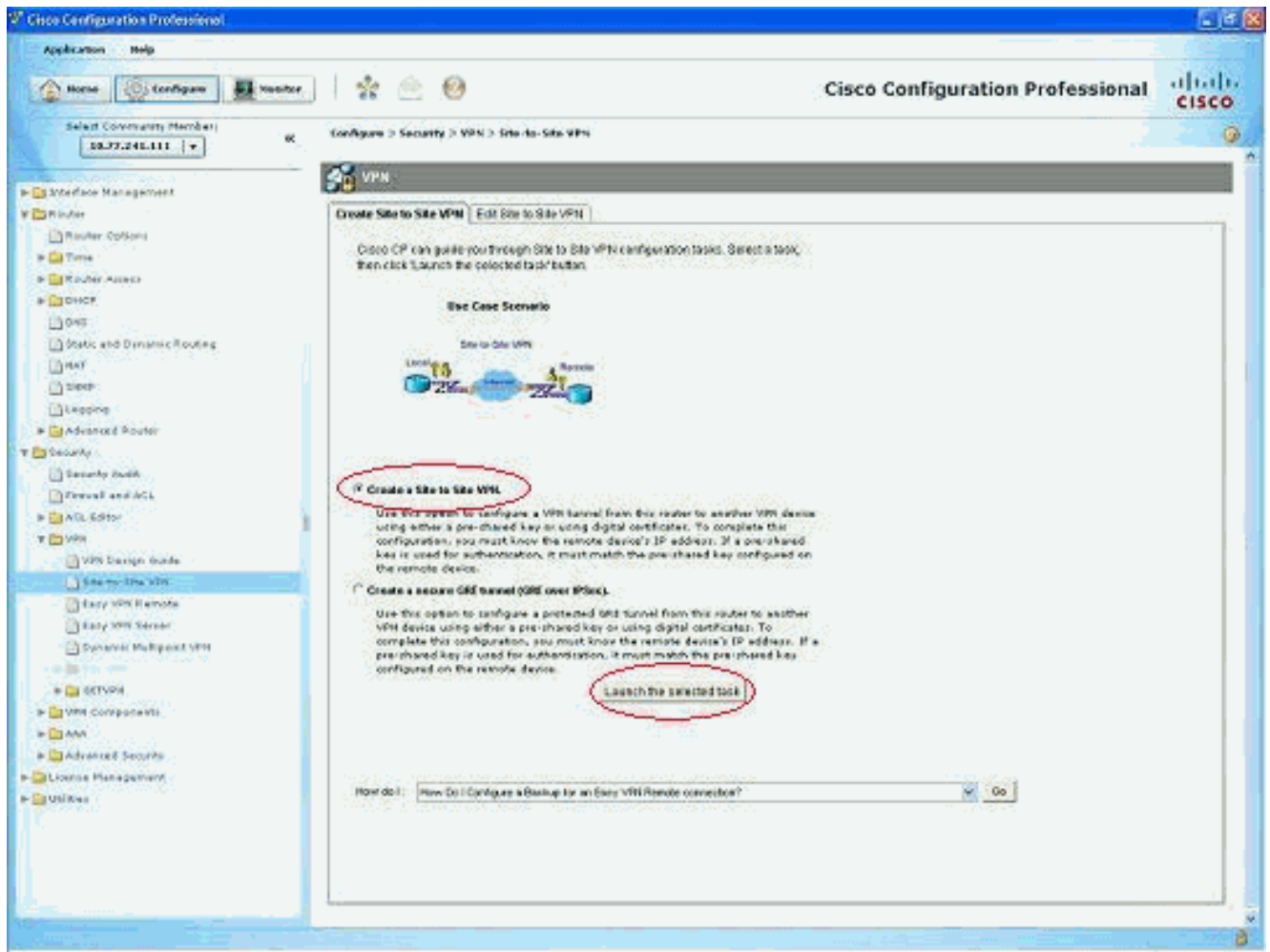
Ce document utilise la configuration réseau suivante :



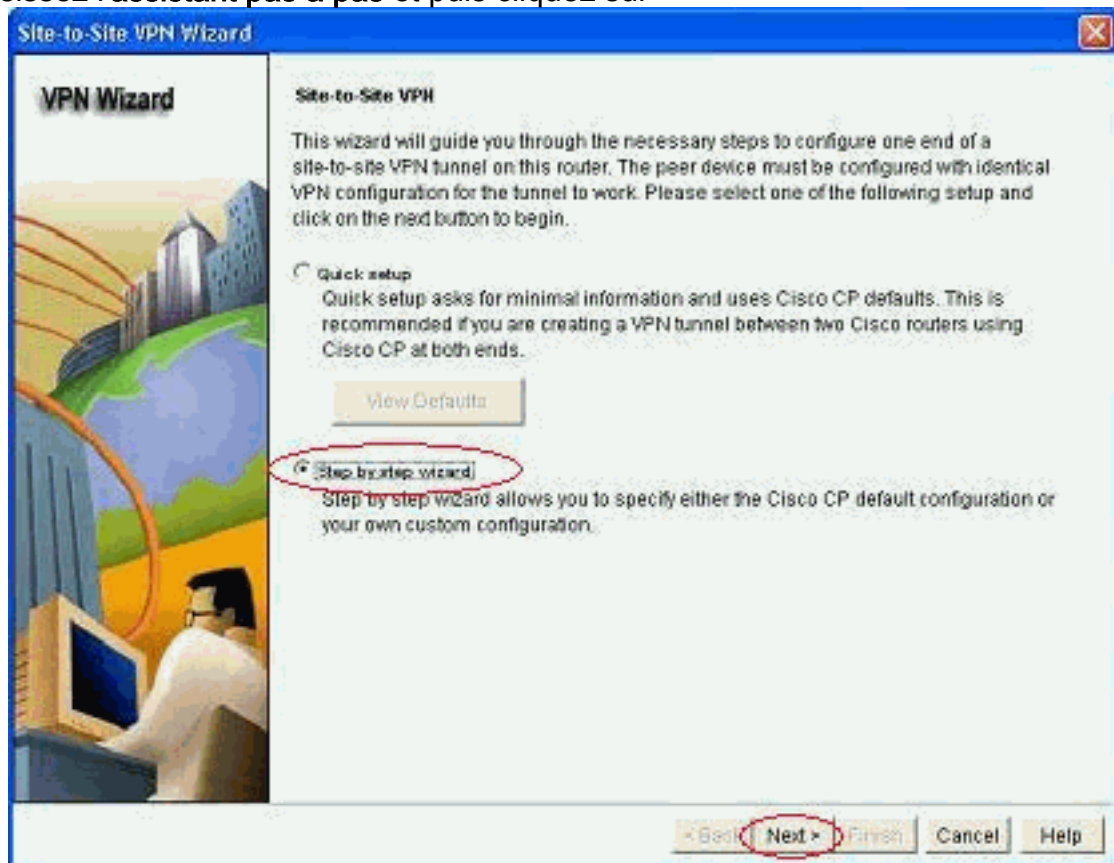
Configurations

C'est la configuration du VPN d'IPsec sur le routeur VPN avec le CCP. Procédez comme suit :

1. Ouvrez l'application CCP et choisissez **configurer > Sécurité > VPN > site à site VPN**. Cliquez sur le **lancement l'onglet sélectionné**.

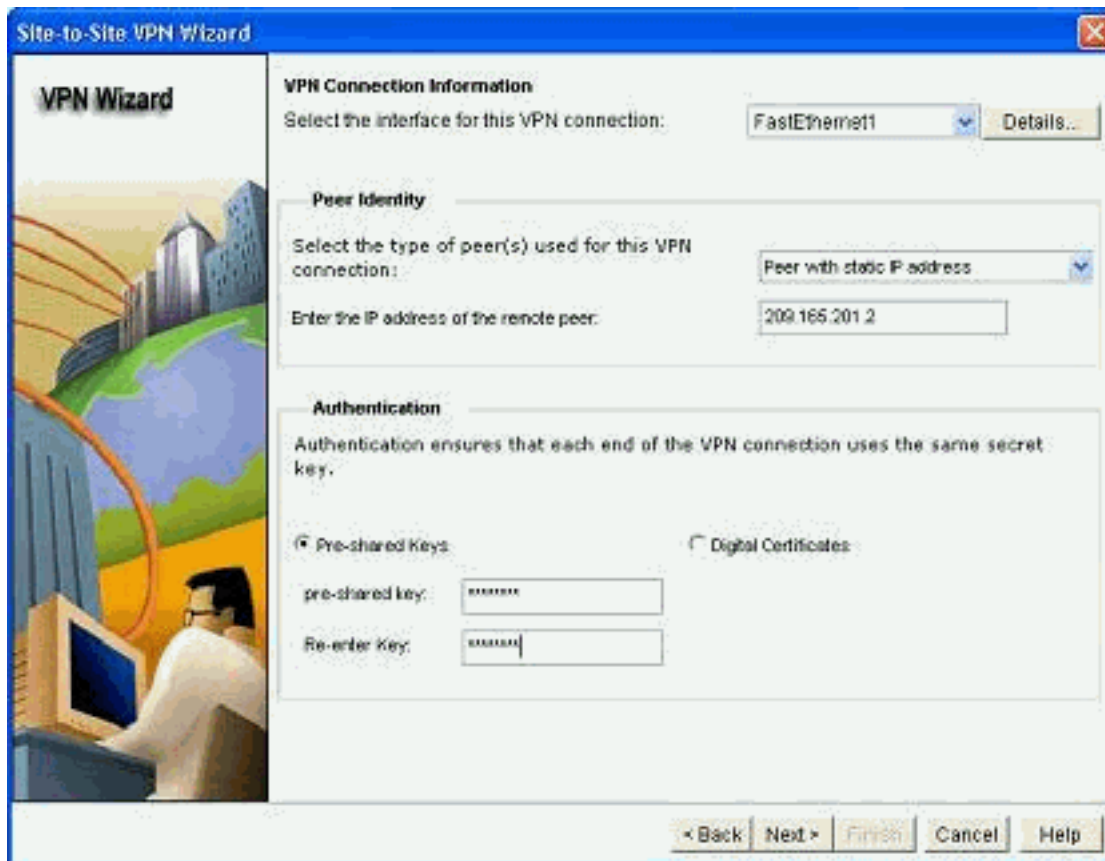


2. Choisissez l'assistant pas à pas et puis cliquez sur

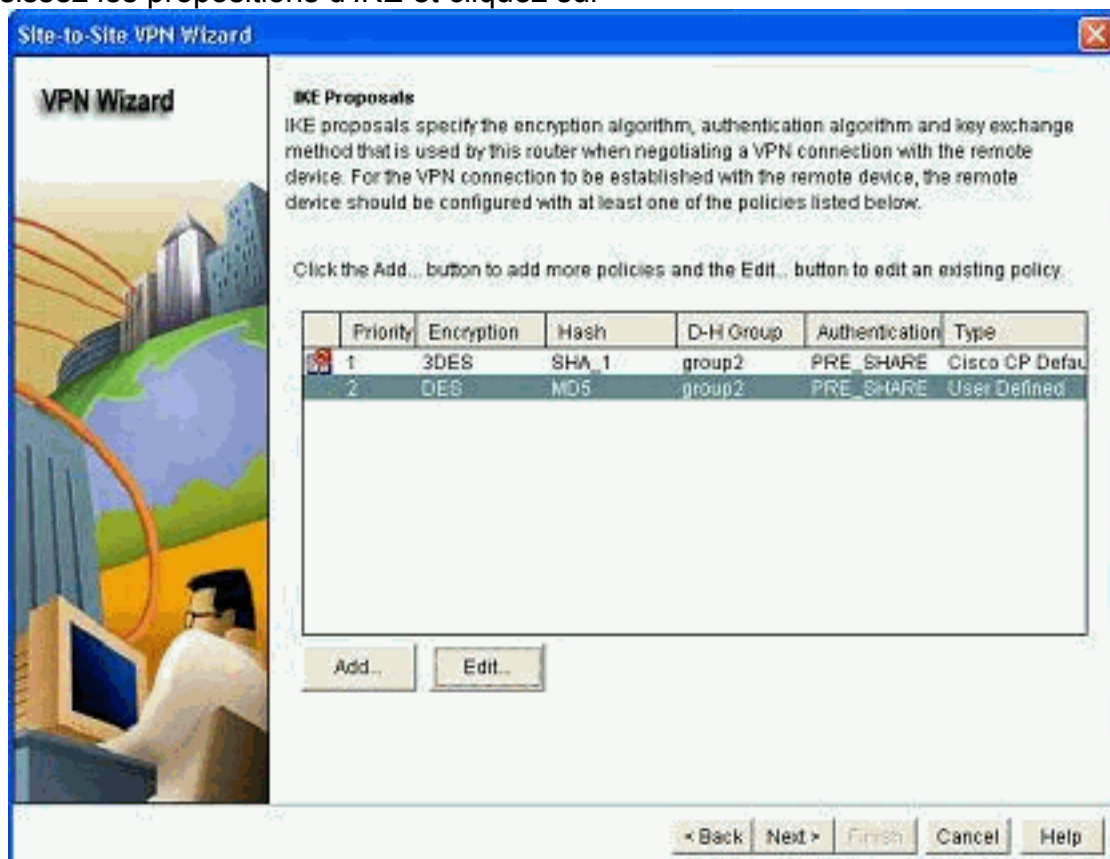


Next.

3. Complétez l'adresse IP distante de pair avec les détails d'authentification.

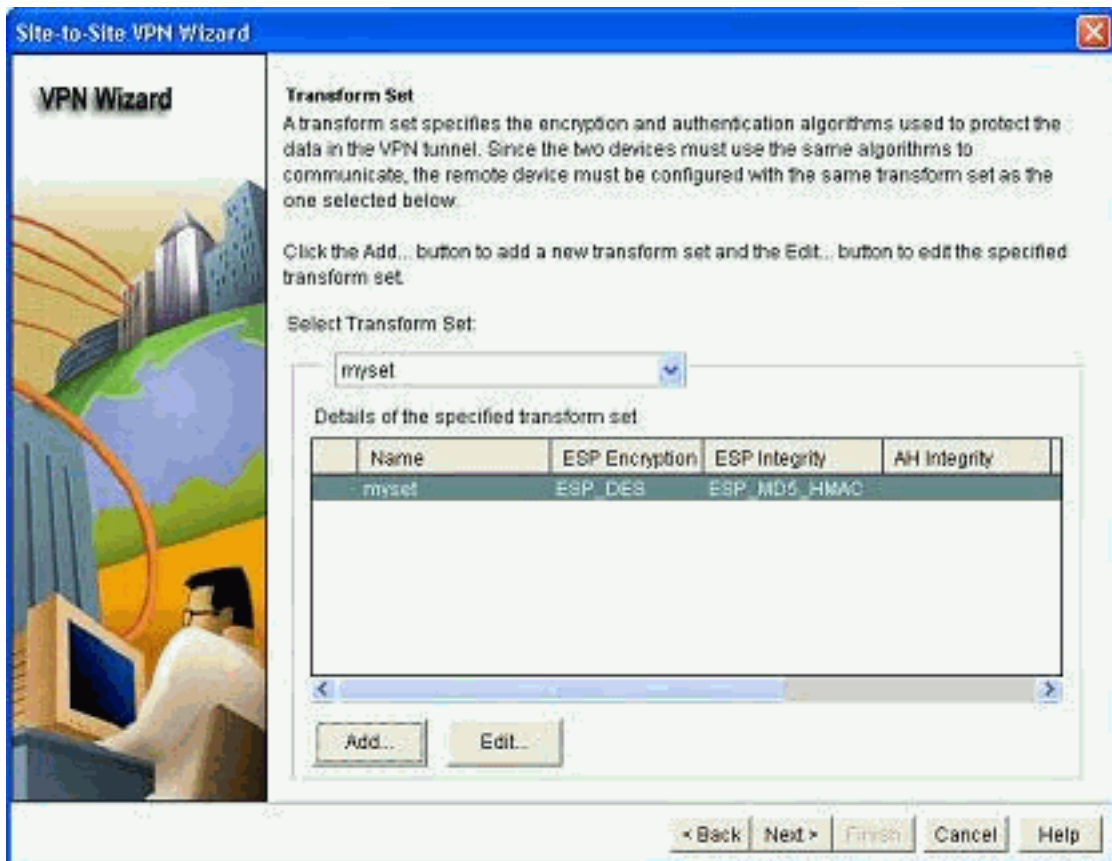


4. Choisissez les propositions d'IKE et cliquez sur



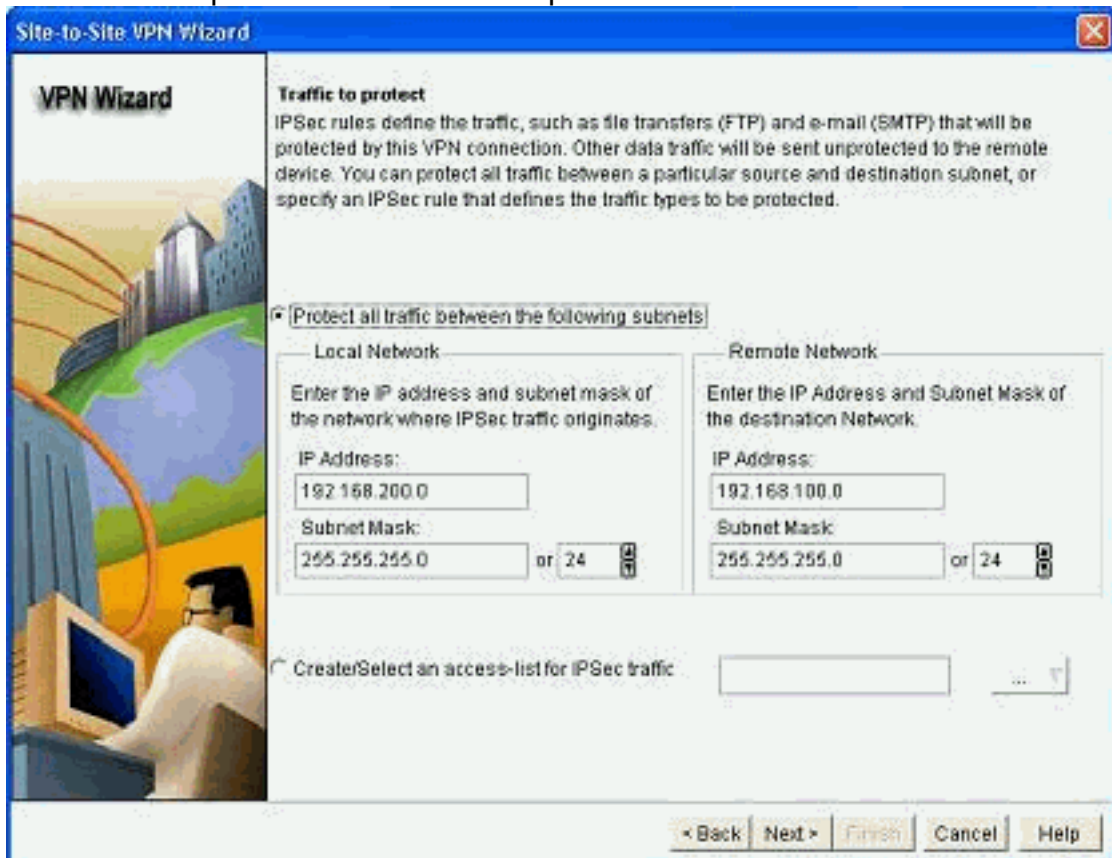
Next.

5. Définissez les détails de transform-set et cliquez sur



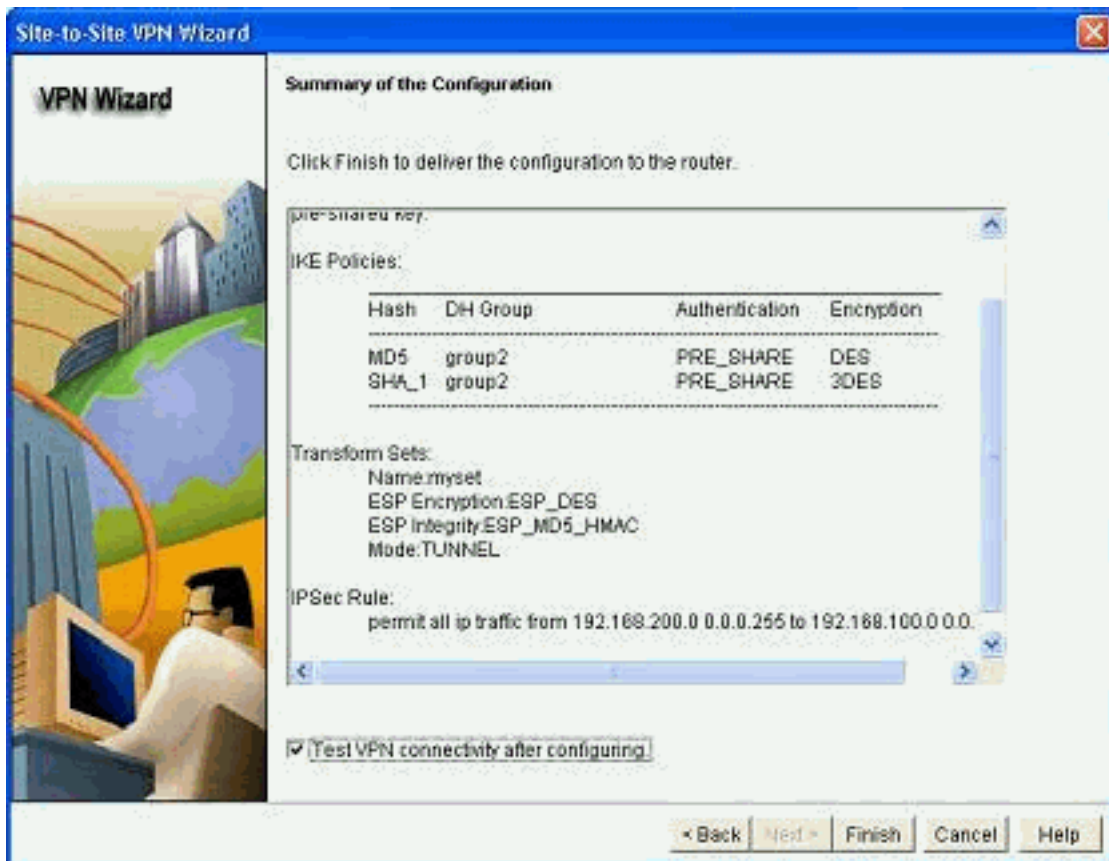
Next.

6. Définissez le trafic qui doit être chiffré et cliquez sur



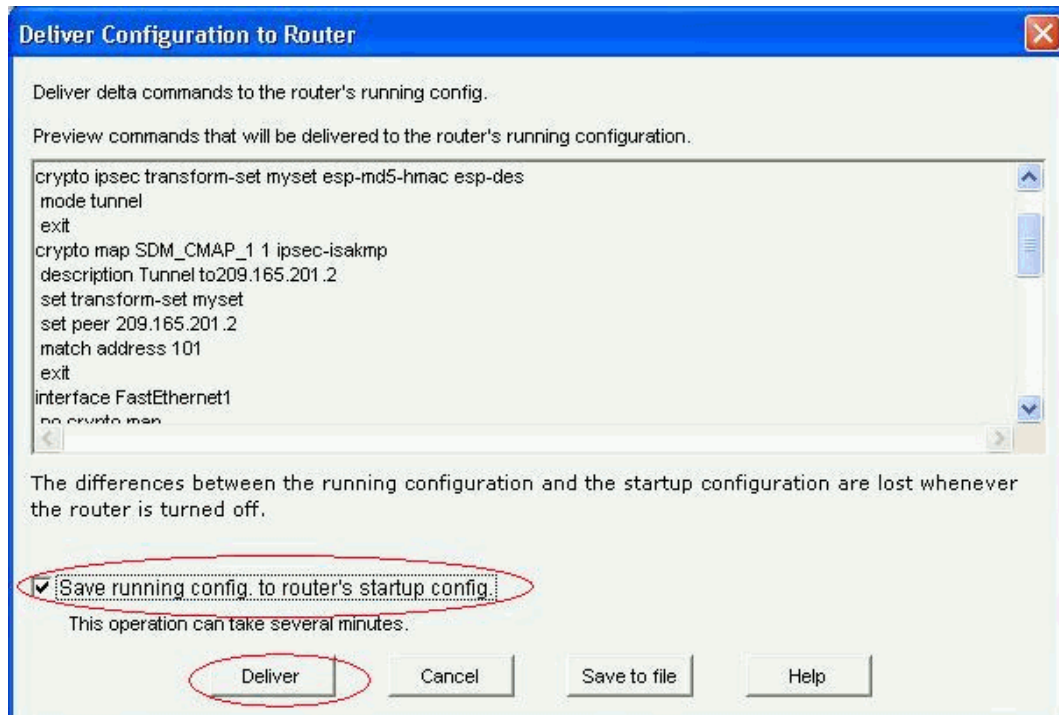
Next.

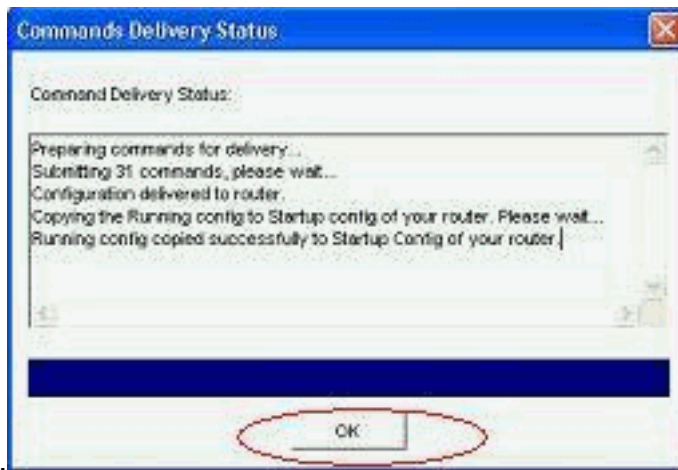
7. Vérifiez le résumé de la crypto configuration d'IPsec et cliquez sur



Finish.

- Le clic **livrent** afin d'envoyer la configuration au routeur VPN.





9. Cliquez sur OK.

Configuration CLI

- [Ciscoasa](#)
- [Routeur VPN](#)

Ciscoasa

```
ciscoasa(config)#show run : Saved : ASA Version 8.0(3) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif outside
security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.1
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive !--- Output suppressed access-list
nonat extended permit ip 192.168.100.0 255.255.255.0
192.168.200.0 255.255.255.0 no pager mtu outside 1500
mtu inside 1500 icmp unreachable rate-limit 1 burst-size
1 asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 ! !--- Define the nat-translation for
Internet users global (outside) 1 interface nat (inside)
1 192.168.100.0 255.255.255.0 ! ! !--- Define the nat-
exemption policy for VPN traffic nat (inside) 0 access-
list nonat ! route outside 0.0.0.0 0.0.0.0 209.165.201.1
1 ! timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite
0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00
absolute dynamic-access-policy-record DfltAccessPolicy
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart ! !--- Configure the IPsec transform-set
crypto ipsec transform-set myset esp-des esp-md5-hmac !
! !--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset crypto dynamic-map
mymap 1 set reverse-route crypto map dyn-map 10 IPSec-
isakmp dynamic mymap crypto map dyn-map interface
outside ! !--- Configure the phase I ISAKMP policy
crypto isakmp policy 10 authentication pre-share
encryption des hash md5 group 2 lifetime 86400 ! ! !---
Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes pre-
shared-key * ! 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 prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa(config)#

```

Le CCP crée cette configuration sur le routeur VPN.

Routeur VPN

```

VPN-Router#show run Building configuration... ! version
12.4 service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname VPN-Router !! username cisco
privilege 15 secret 5 $1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRdfQ01 !! !--- Output
suppressed no aaa new-model ip subnet-zero ! ip cef !
crypto isakmp enable outside ! crypto isakmp policy 1
encrypt 3des authentication pre-share group 2 ! crypto
isakmp policy 2 hash md5 authentication pre-share group
2 !! crypto isakmp key cisco123 address 209.165.201.2 !
! crypto ipsec transform-set myset esp-des esp-md5-hmac
! ! crypto map SDM_CMAP_1 1 IPsec-isakmp description
Tunnel to209.165.201.2 set peer 209.165.201.2 set
transform-set myset match address 101 !!! interface
BRI0 no ip address shutdown ! interface Dot11Radio0 no
ip address shutdown speed basic-1.0 basic-2.0 basic-5.5
6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root ! interface Dot11Radio1 no ip address
shutdown speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0
36.0 48.0 54.0 station-role root ! interface
FastEthernet0 ip address 192.168.200.1 255.255.255.0
duplex auto speed auto ! interface FastEthernet1 ip
address dhcp duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet2 no ip address
shutdown ! interface FastEthernet3 no ip address
shutdown ! interface FastEthernet4 no ip address
shutdown ! interface FastEthernet5 no ip address
shutdown ! interface FastEthernet6 no ip address
shutdown ! interface FastEthernet7 no ip address
shutdown ! interface FastEthernet8 no ip address
shutdown ! interface FastEthernet9 no ip address
shutdown ! interface Vlan1 no ip address ! ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1 !! !--- Output
suppressed ! ip http server ip http authentication local
ip http secure-server ! access-list 100 permit ip
0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0 access-list
101 remark CCP_ACL Category=4 access-list 101 remark
IPSEC Rule access-list 101 permit ip 192.168.200.0
0.0.0.255 192.168.100.0 0.0.0.255 !!! ! control-plane
! ! line con 0 line aux 0 line vty 0 4 privilege level
15 login local transport input telnet ssh line vty 5 15
privilege level 15 login local transport input telnet
ssh ! no scheduler allocate end

```

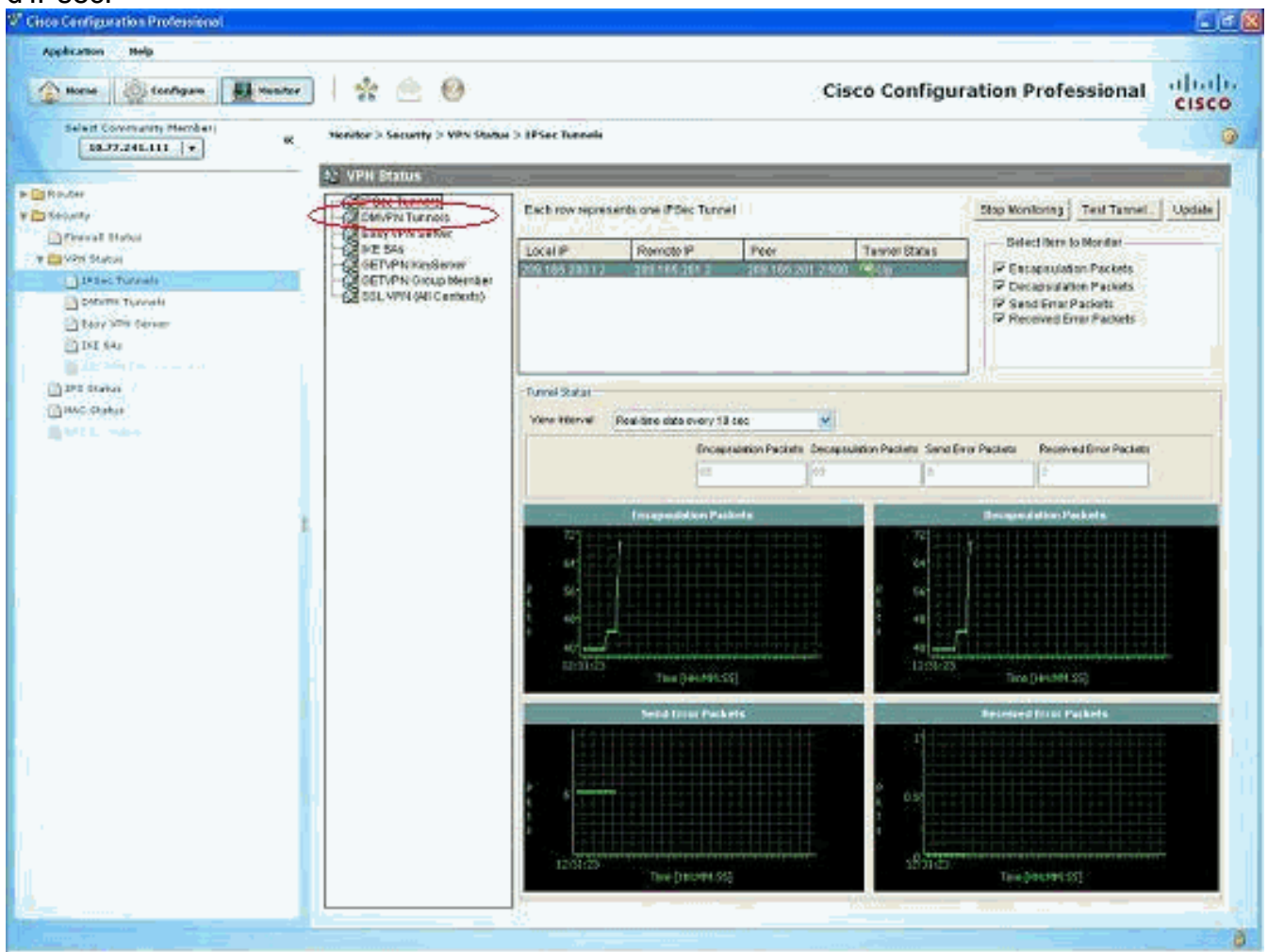
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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**.

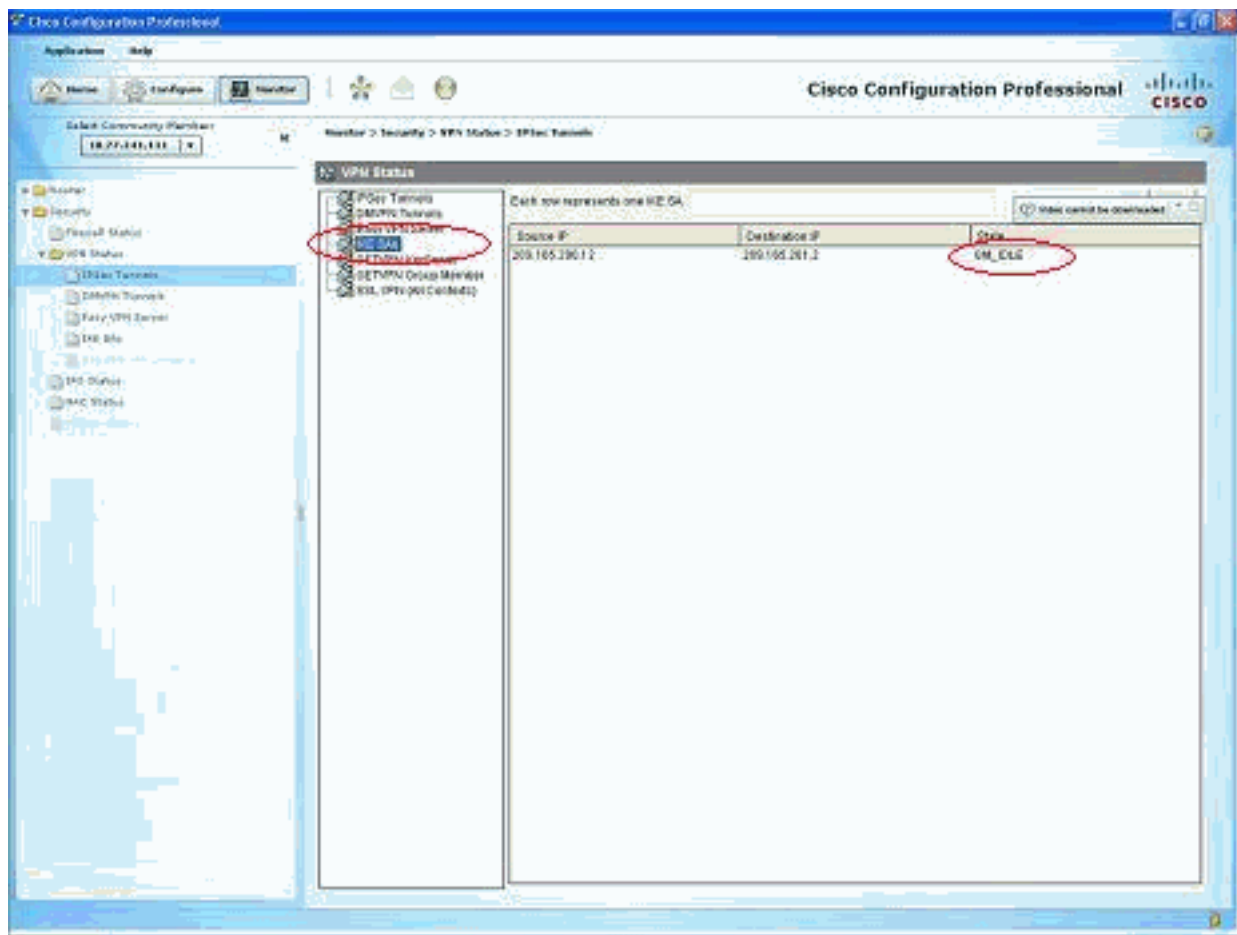
- [Vérifier les paramètres de tunnel par le CCP](#)
- [Vérifier l'état de tunnel par ASA CLI](#)
- [Vérifier les paramètres de tunnel par le routeur CLI](#)

[Vérifiez les paramètres de tunnel par le CCP](#)

- Surveillez le trafic traverse le tunnel d'IPsec.



- Surveillez l'état du SA ISAKMP de la phase



Vérifiez l'état de tunnel par ASA CLI

- Vérifiez l'état du SA ISAKMP de la phase I. `ciscoasa#show crypto isakmp sa` Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 209.165.200.12 Type : L2L Role : **responder** Rekey : no State : **MM_ACTIVE** ciscoasa#
- **Remarque:** Observez le rôle pour être le responder, qui déclare que le demandeur de ce tunnel est à l'autre extrémité, par exemple, le routeur VPN.
- Vérifiez les paramètres d'IPSEC SA de la phase II. `ciscoasa#show crypto ipsec sa interface:`

```
outside Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2 local ident
(addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(192.168.200.0/255.255.255.0/0/0) current_peer: 209.165.200.12 #pkts encaps: 29, #pkts
encrypt: 29, #pkts digest: 29 #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not compressed: 29, #pkts comp failed: 0, #pkts
decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs
sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv
errors: 0 local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12 path mtu
1500, IPsec overhead 58, media mtu 1500 current outbound spi: E7B37960 inbound esp sas: spi:
0xABB49C64 (2880740452) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel,
} slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec):
(4274997/3498) IV size: 8 bytes replay detection support: Y outbound esp sas: spi:
0xE7B37960 (3887298912) transform: esp-des esp-md5-hmac none in use settings ={L2L, Tunnel,
} slot: 0, conn_id: 4096, crypto-map: mymap sa timing: remaining key lifetime (kB/sec):
(4274997/3498) IV size: 8 bytes replay detection support: Y
```

Vérifiez les paramètres de tunnel par le routeur CLI

- Vérifiez l'état du SA ISAKMP de la phase I. `VPN-Router#show crypto isakmp sa dst src state`

```
conn-id slot status 209.165.201.2 209.165.200.12 QM_IDLE 1 0 ACTIVE
```
- Vérifiez les paramètres d'IPSEC SA de la phase II. `VPN-Router#show crypto ipsec sa interface:`

```
FastEthernet1 Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12 protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0) current_peer 209.165.201.2 port 500
PERMIT, flags={origin_is_acl,} #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39 #pkts
decaps: 39, #pkts decrypt: 39, #pkts verify: 39 #pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress
failed: 0 #send errors 6, #recv errors 0 local crypto endpt.: 209.165.200.12, remote crypto
endpt.: 209.165.201.2 path mtu 1500, ip mtu 1500 current outbound spi:
0xABB49C64(2880740452) inbound esp sas: spi: 0xE7B37960(3887298912) transform: esp-des esp-
md5-hmac , in use settings = {Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map:
SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4481818/3375) IV size: 8 bytes replay
detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xABB49C64(2880740452) transform: esp-des esp-md5-hmac , in use settings = {Tunnel, } conn
id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime
(k/sec): (4481818/3371) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound
ah sas: outbound pcp sas:
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Démolir les cryptos connexions existantes.`ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa VPN-Router#clear crypto isakmp`
- Employez les commandes de **débogage** afin de dépanner les problèmes avec le tunnel VPN.**Remarque:** Si vous activez l'élimination des imperfections, ceci peut perturber le fonctionnement du routeur quand les interréseaux éprouvent des conditions de charge élevée. Utilisez les commandes **debug** avec prudence. D'une manière générale, il est recommandé que ces commandes soient seulement utilisées sous les orientations de l'agent d'assistance technique de votre routeur pour le dépannage de problèmes spécifiques.`ciscoasa#debug crypto engine ciscoasa#debug crypto isakmp ciscoasa#debug crypto IPsec ciscoasa# VPN-Router#debug crypto engine Crypto Engine debugging is on VPN-Router#debug crypto isakmp Crypto ISAKMP debugging is on VPN-Router#debug crypto ipsec Crypto IPSEC debugging is on VPN-Router#`

Référez-vous au [debug crypto isakmp](#) dans la [compréhension et les commandes de débogage de utilisation](#) pour plus d'informations sur mettent au point des commangs.

Informations connexes

- [Page de support de la négociation IPsec/des protocoles IKE](#)
- [Documentation pour le logiciel de SYSTÈME D'EXPLOITATION de dispositifs de sécurité de Cisco ASA](#)
- [La plupart des solutions communes de dépannage VPN IPSEC](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)