

# Exemple de configuration de tunnel IPsec dynamique entre un ASA à adressage statique et un routeur Cisco IOS à adressage dynamique qui utilise CCP

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Vérifier les paramètres de tunnel via CCP](#)

[Vérifier l'état du tunnel via l'interface de ligne de commande ASA](#)

[Vérifier les paramètres du tunnel via l'interface de ligne de commande du routeur](#)

[Dépannage](#)

[Informations connexes](#)

## Introduction

Ce document fournit un exemple de configuration pour permettre au dispositif de sécurité PIX/ASA d'accepter des connexions IPsec dynamiques à partir du routeur Cisco IOS<sup>®</sup>. Dans ce scénario, le tunnel IPsec est établi quand le tunnel est initié de l'extrémité du routeur seulement. L'ASA n'a pas pu initier un tunnel VPN en raison de la configuration IPsec dynamique.

Cette configuration permet au dispositif de sécurité PIX de créer un tunnel LAN à LAN (L2L) IPsec dynamique avec un routeur VPN distant. Ce routeur reçoit dynamiquement son adresse IP publique externe de son fournisseur d'accès Internet. Le protocole DHCP (Dynamic Host Configuration Protocol) fournit ce mécanisme afin d'allouer des adresses IP dynamiquement à partir du fournisseur. Cela permet de réutiliser les adresses IP lorsque les hôtes n'en ont plus besoin.

La configuration sur le routeur s'effectue à l'aide de [Cisco Configuration Professional](#) (CCP). CCP est un outil de gestion de périphériques basé sur une interface utilisateur graphique qui vous permet de configurer des routeurs basés sur Cisco IOS. Référez-vous à [Configuration de base d'un routeur à l'aide de Cisco Configuration Professional](#) pour plus d'informations sur la façon de

configurer un routeur avec CCP.

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

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

## Conditions préalables

### Conditions requises

Avant d'essayer cette configuration, assurez-vous que l'ASA et le routeur ont tous deux une connectivité Internet afin d'établir le tunnel IPSEC.

### Components Used

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

- Routeur Cisco IOS1812 qui exécute le logiciel Cisco IOS Version 12.4
- Logiciel Cisco ASA 5510 version 8.0.3

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.

### 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 192.168.100.0 est derrière l'ASA et le réseau 192.168.200.0 est derrière le routeur Cisco IOS. Il est supposé que le routeur obtient son adresse publique via DHCP de son FAI. Comme cela pose un problème dans la configuration d'un homologue statique sur l'extrémité ASA, vous devez approcher le mode de configuration de chiffrement dynamique pour établir un tunnel site à site entre ASA et le routeur Cisco IOS.

Les utilisateurs Internet de l'extrémité ASA sont traduits en adresse IP de son interface externe. Il est supposé que NAT n'est pas configuré sur l'extrémité du routeur Cisco IOS.

Voici maintenant les principales étapes à configurer sur l'extrémité ASA afin d'établir un tunnel dynamique :

1. Configuration ISAKMP de phase 1
2. Configuration de l'exemption Nat
3. Configuration de la carte de chiffrement dynamique

Le routeur Cisco IOS a une carte de chiffrement statique configurée car l'ASA est supposé avoir une adresse IP publique statique. Voici maintenant la liste des étapes principales à configurer sur l'extrémité du routeur Cisco IOS pour établir un tunnel IPSEC dynamique.

1. Configuration ISAKMP de phase 1
2. Configuration liée à la crypto-carte statique

Ces étapes sont décrites en détail dans ces configurations.

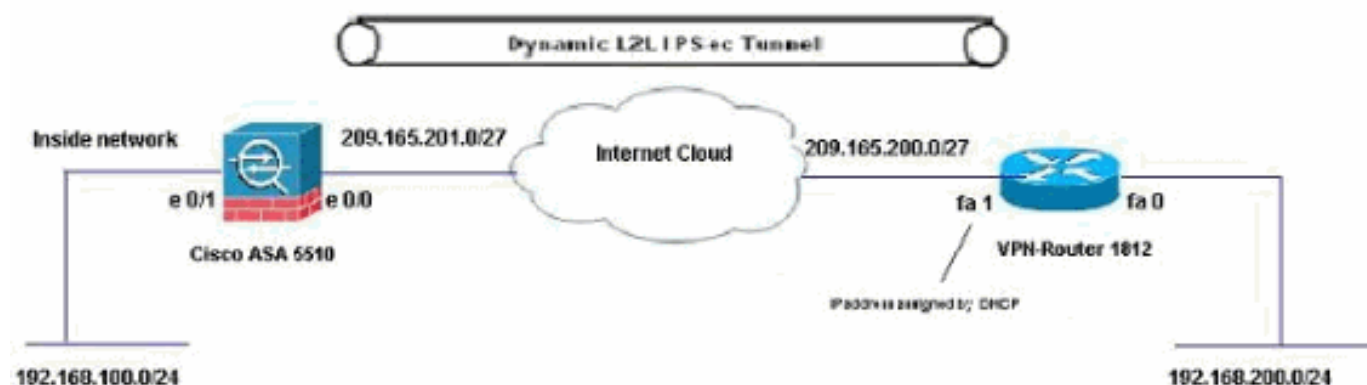
## Configuration

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

**Remarque :** utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## Diagramme du réseau

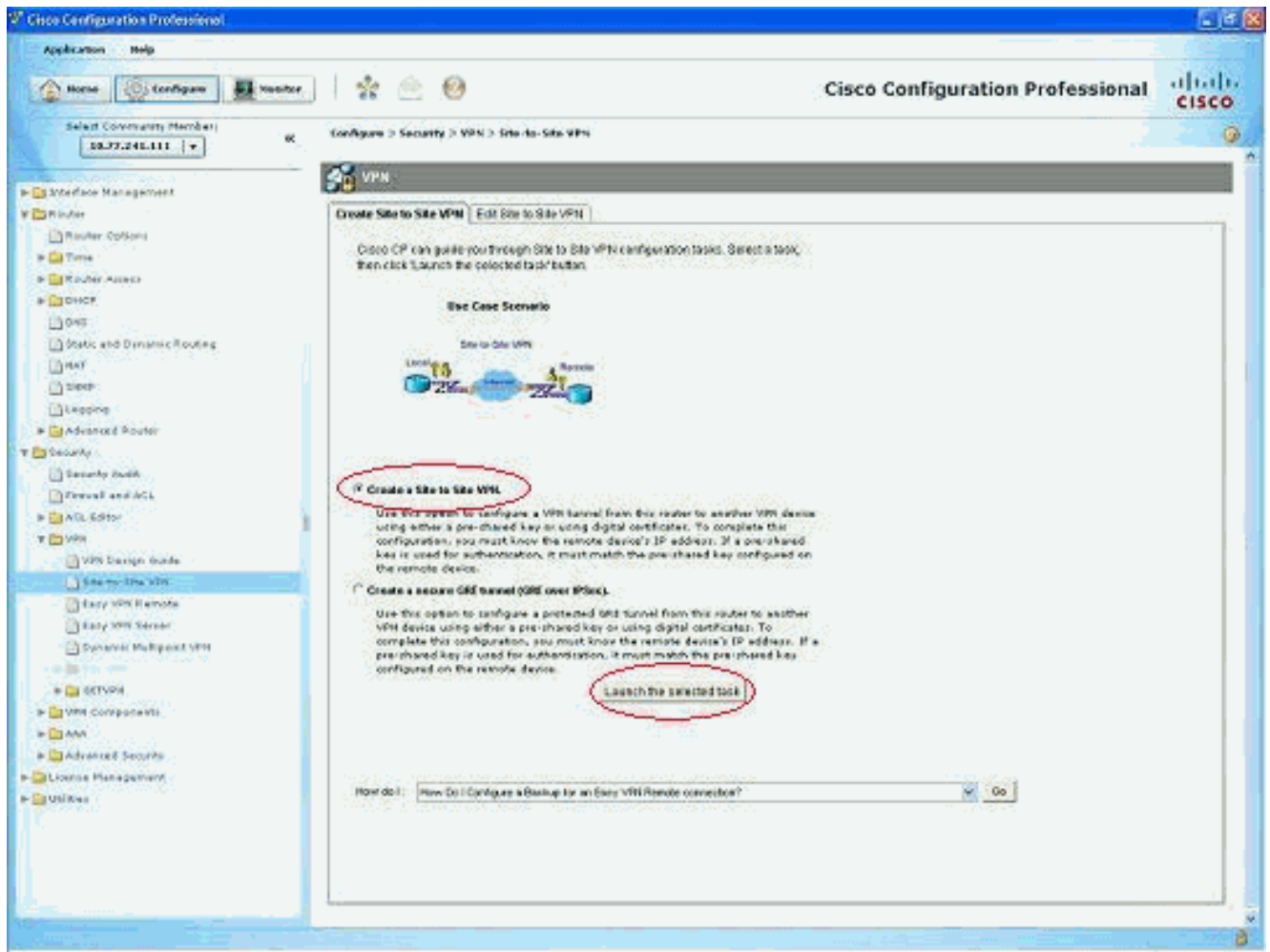
Ce document utilise la configuration réseau suivante :



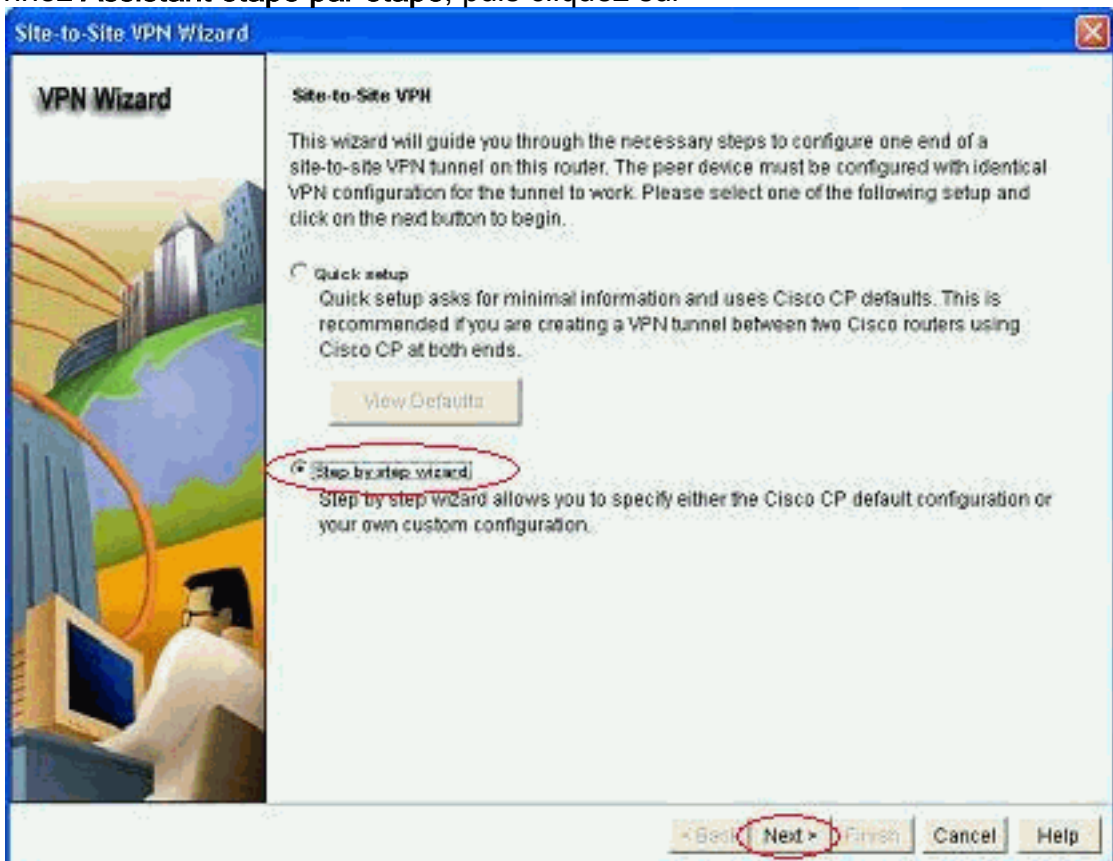
## Configurations

Il s'agit de la configuration VPN IPsec sur le routeur VPN avec CCP. Procédez comme suit :

1. Ouvrez l'application CCP et choisissez **Configure > Security > VPN > Site to Site VPN**. Cliquez sur l'onglet **Lancer la sélection**.

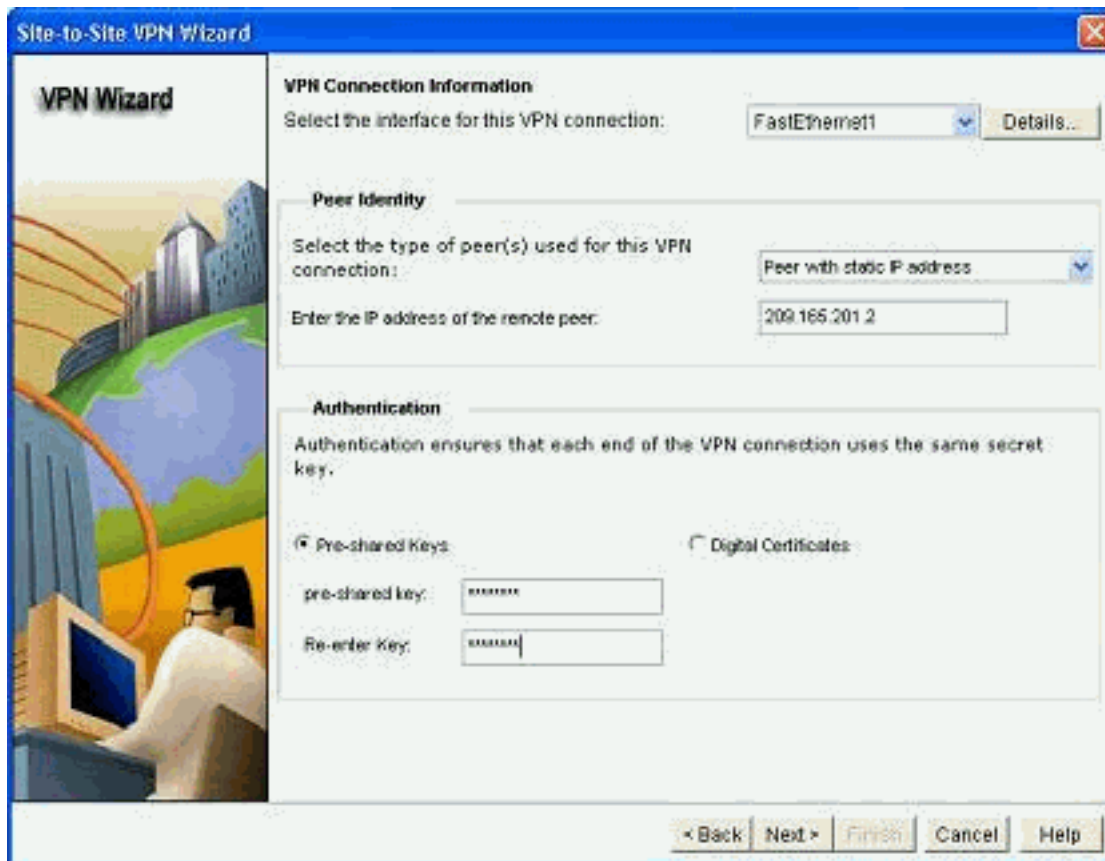


2. Sélectionnez Assistant étape par étape, puis cliquez sur

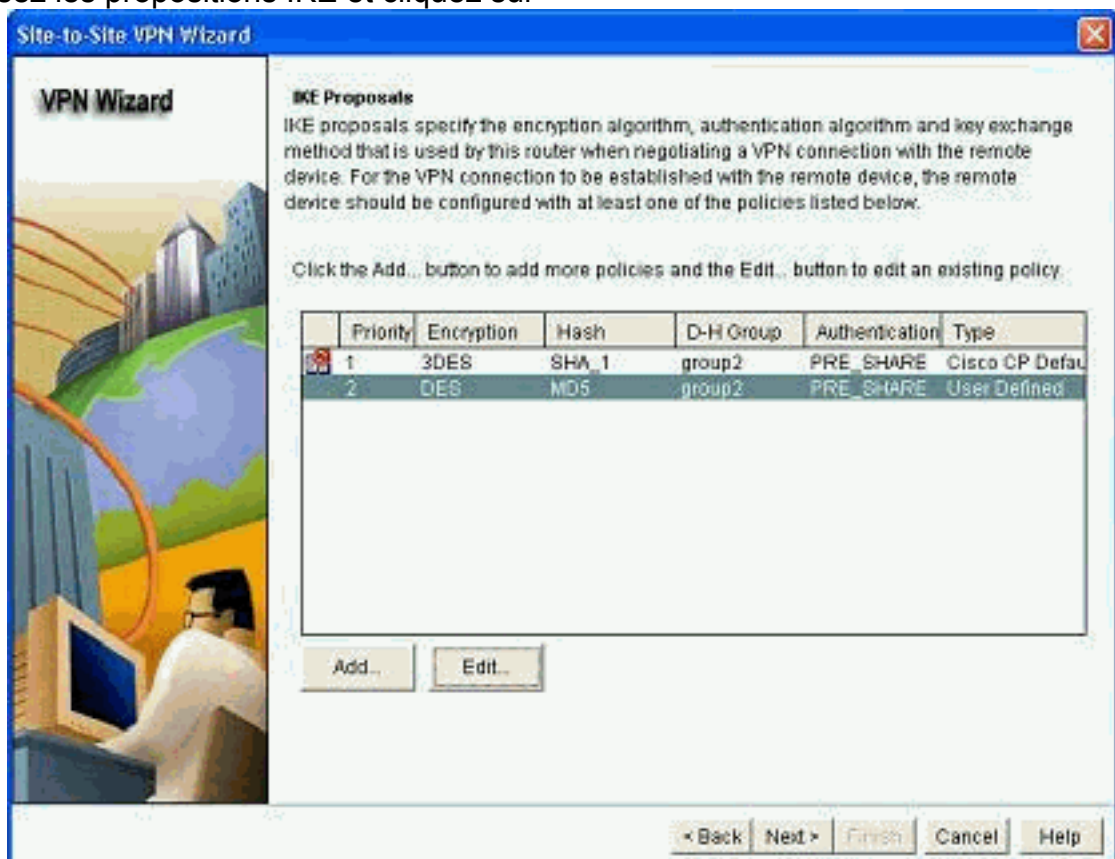


Suivant.

3. Complétez l'adresse IP de l'homologue distant avec les détails de l'authentification.



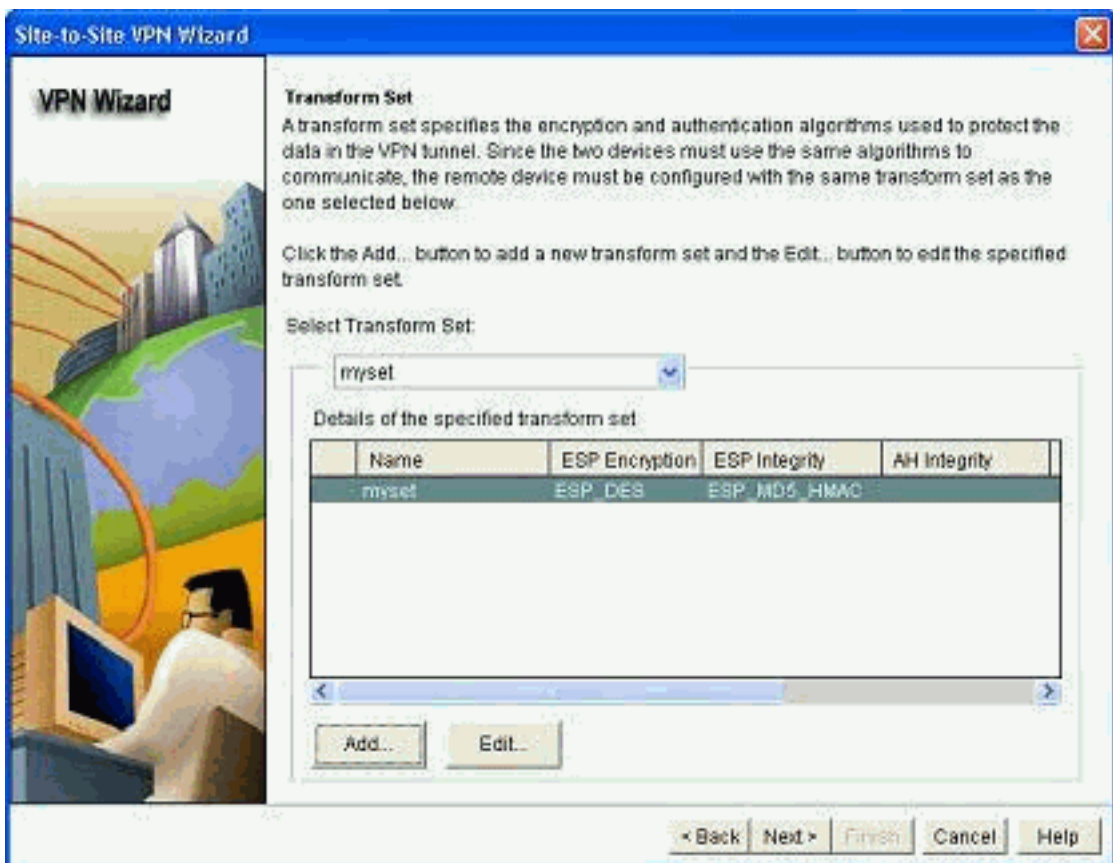
4. Choisissez les propositions IKE et cliquez sur



Suivant.

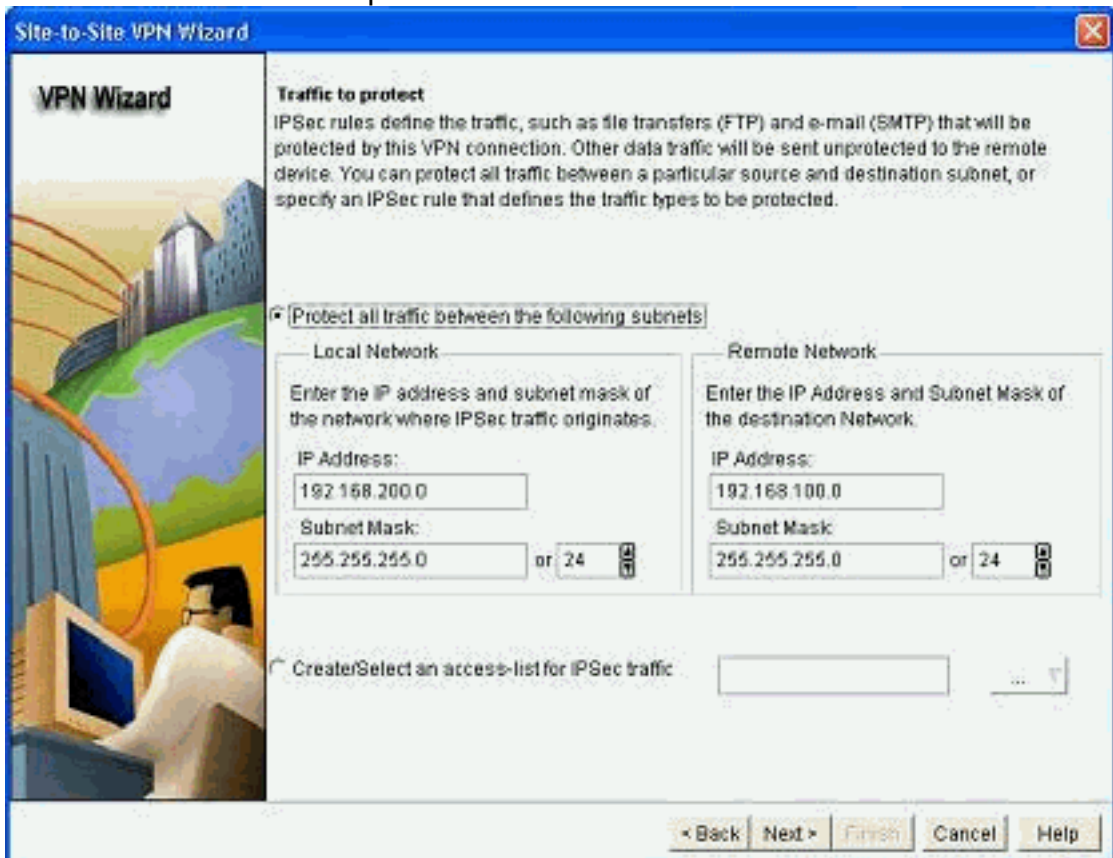
5. Définissez les détails du jeu de transformation et cliquez sur





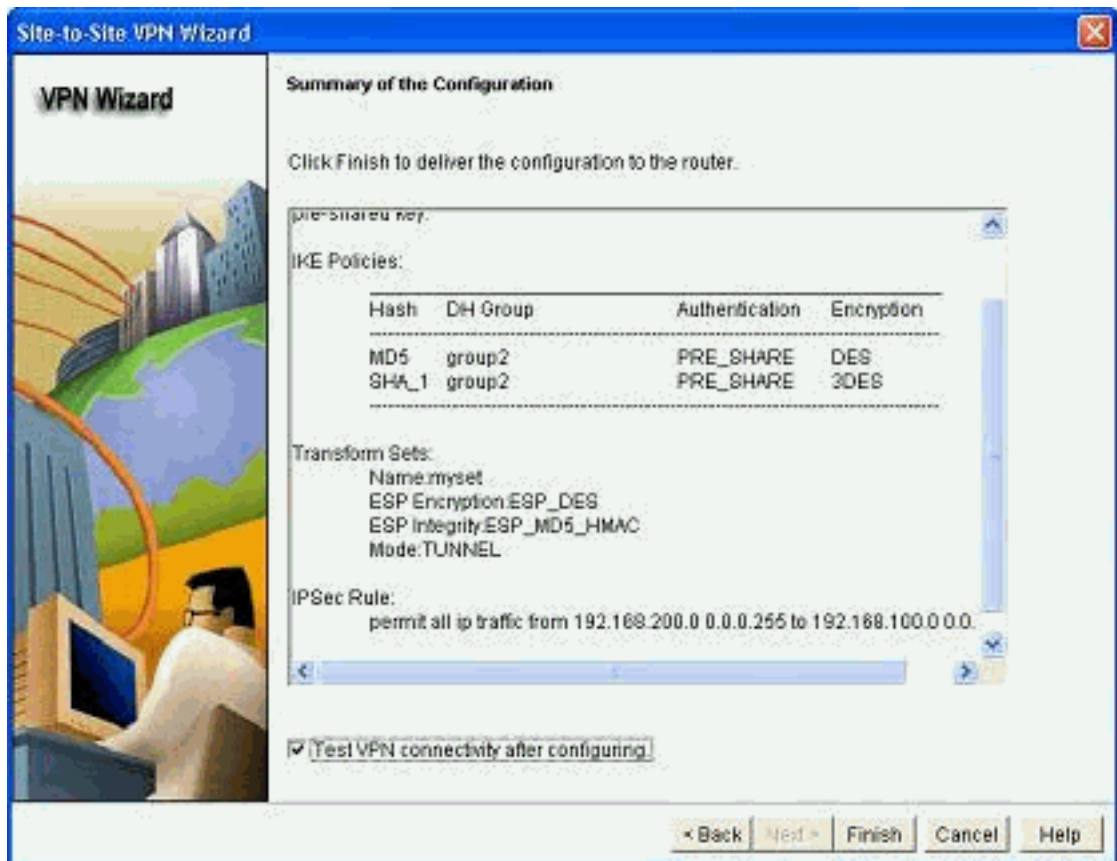
Suivant.

6. Définissez le trafic à chiffrer et cliquez sur



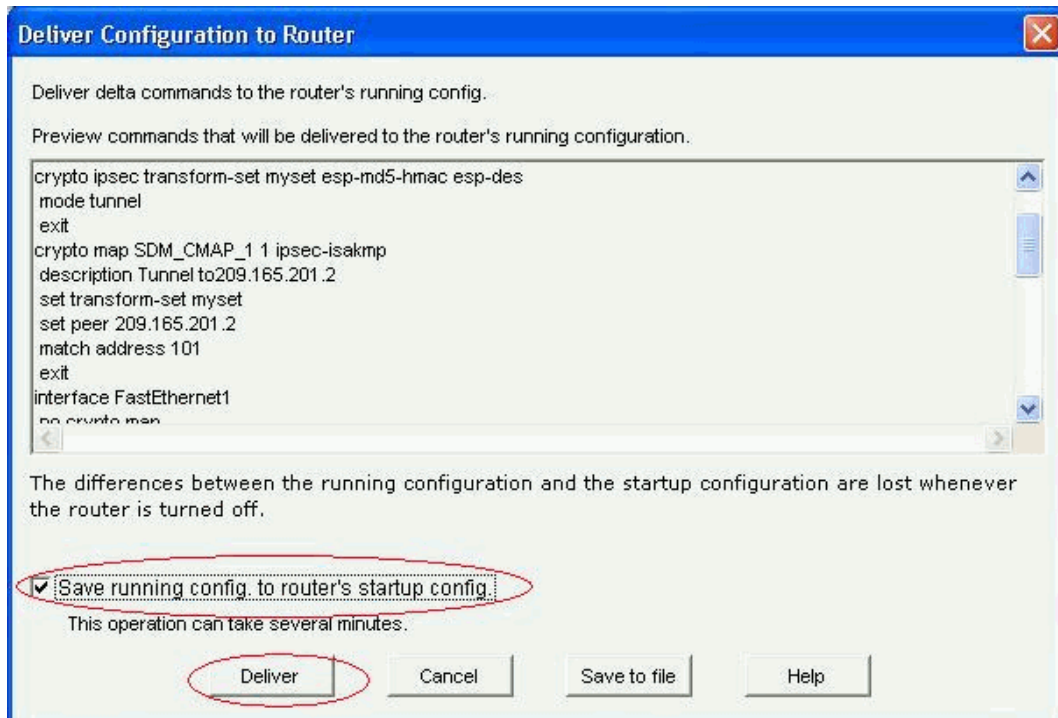
Suivant.

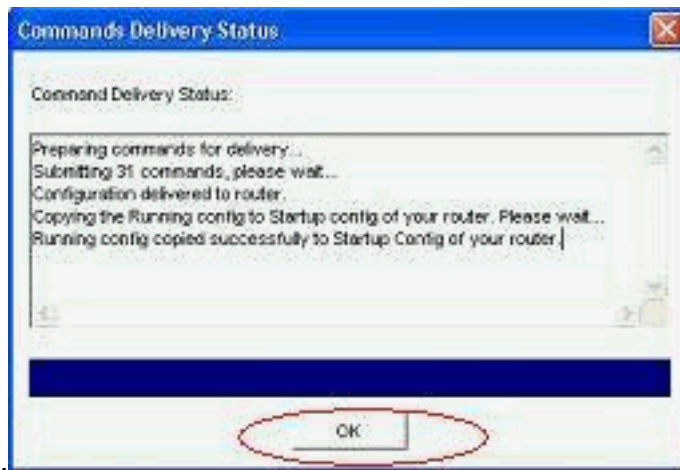
7. Vérifiez le résumé de la configuration IPsec de chiffrement et cliquez sur



Terminer.

8. Cliquez sur **Deliver** afin d'envoyer la configuration au routeur VPN.





9. Click 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)#

```

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
```

## Vérification

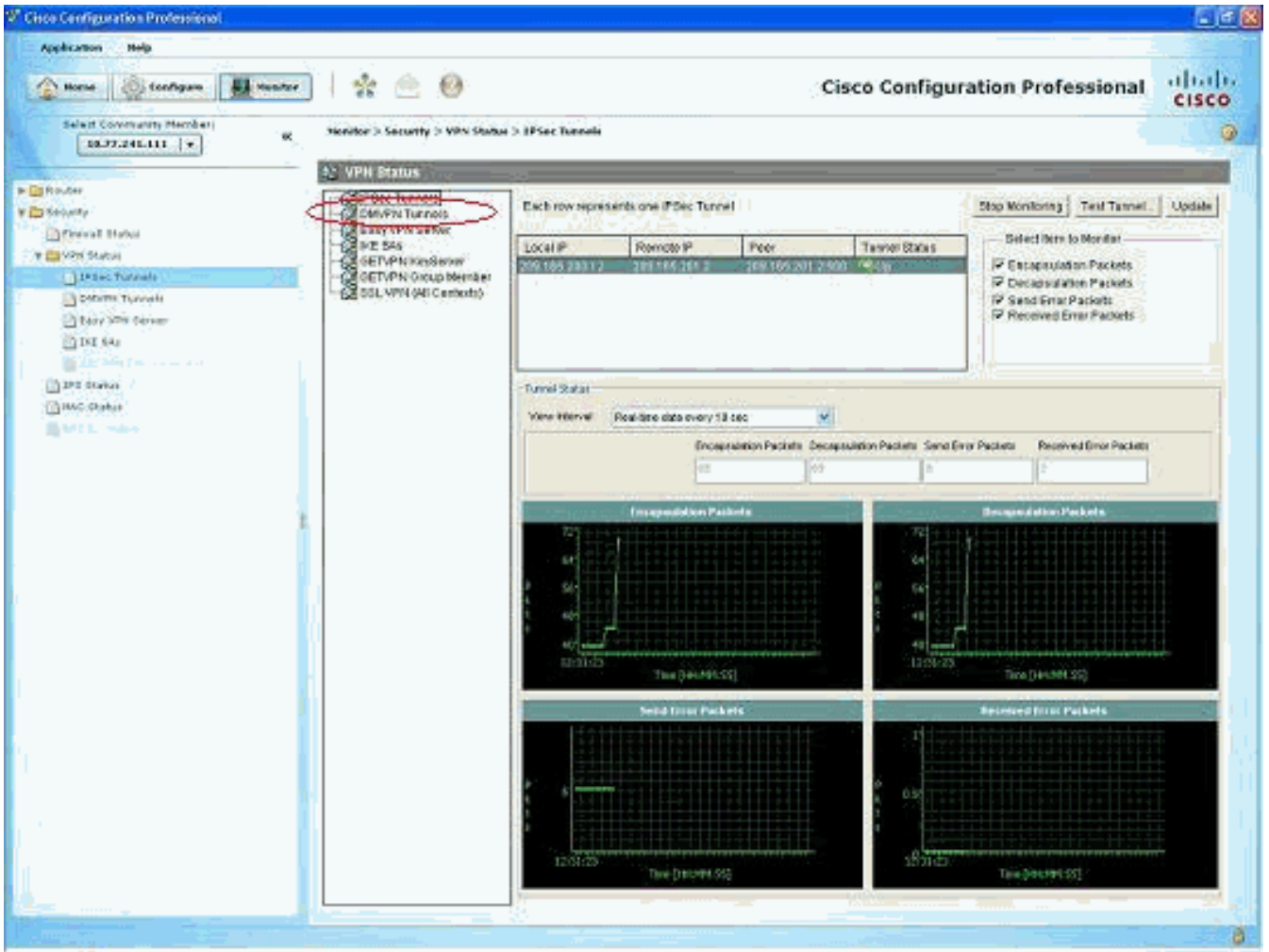
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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`.

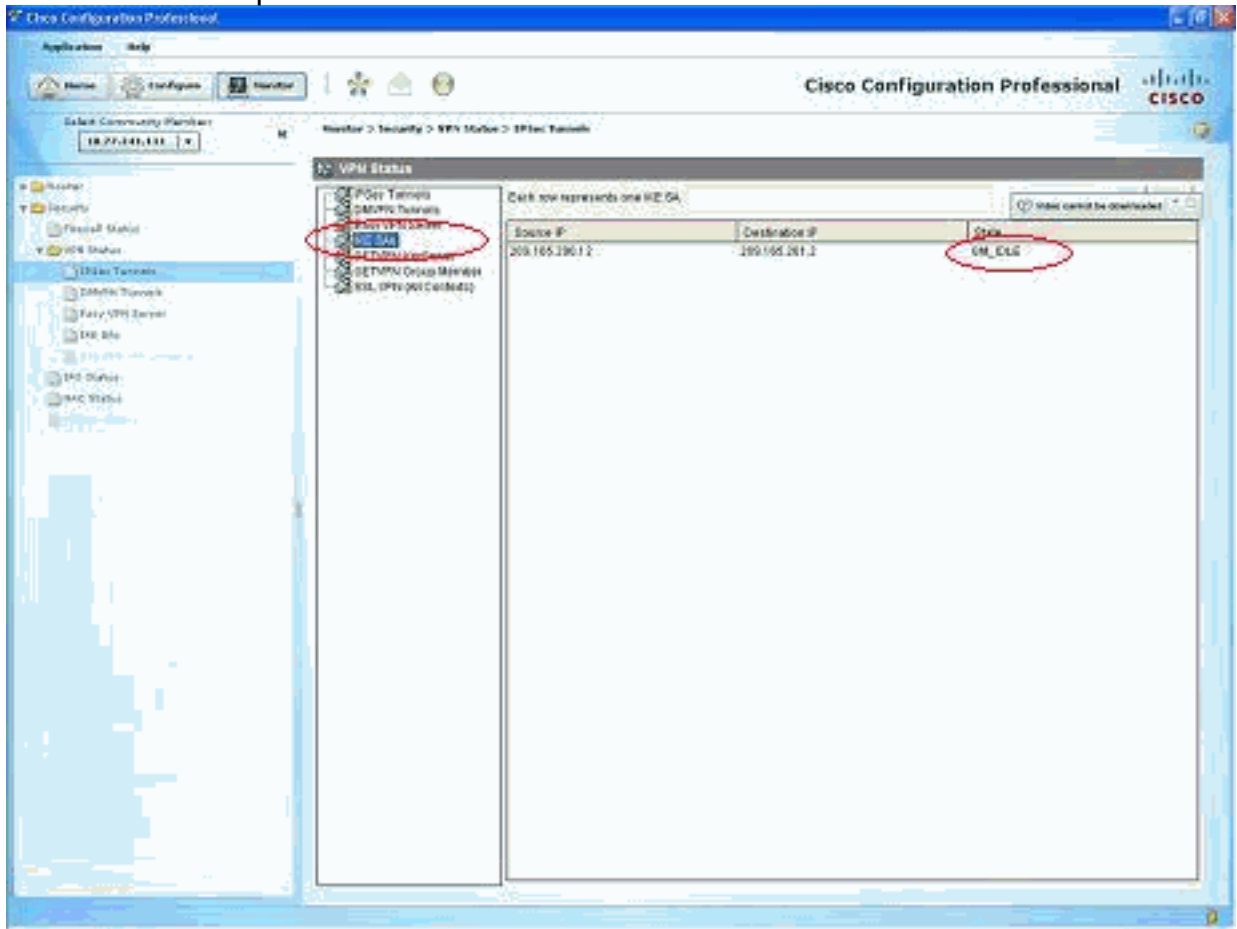
- [Vérification des paramètres de tunnel via CCP](#)
- [Vérification de l'état du tunnel via l'interface de ligne de commande ASA](#)
- [Vérification des paramètres de tunnel via l'interface de ligne de commande du routeur](#)

## Vérifier les paramètres de tunnel via CCP

- Surveillez le trafic traversant le tunnel IPsec.



- Surveillez l'état de la phase I ISAKMP



SA.



## Vérifier l'état du tunnel via l'interface de ligne de commande ASA

- Vérifiez l'état de la phase I ISAKMP SA.

```
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 comme répondeur, qui indique que l'initiateur de ce tunnel se trouve à l'autre extrémité, par exemple, le routeur VPN.

- Vérifiez les paramètres de la phase II IPSEC SA.

```
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, #rcv 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
```

## Vérifier les paramètres du tunnel via l'interface de ligne de commande du routeur

- Vérifiez l'état de la phase I ISAKMP SA.

```
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 de la phase II IPSEC SA.

```
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:
```

## Dépannage

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

- Désactiver les connexions cryptographiques existantes.

```
ciscoasa#clear crypto ipsec sa
ciscoasa#clear crypto isakmp sa
```

```
VPN-Router#clear crypto isakmp
```

- Utilisez les commandes **debug** afin de résoudre les problèmes avec le tunnel VPN. **Remarque** : Si vous activez le débogage, cela peut perturber le fonctionnement du routeur lorsque les réseaux connaissent des conditions de charge élevée. **Utilisez avec prudence les commandes debug**. 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 à [debug crypto isakmp](#) dans [Understanding and Using debug Commands](#) pour plus d'informations sur les commandes de débogage.

## [Informations connexes](#)

- [Page de support de la négociation IPsec/des protocoles IKE](#)
- [Documentation relative au logiciel de système d'exploitation Cisco ASA Security Appliance](#)
- [Solutions de dépannage VPN IPSEC les plus courantes](#)
- [Demandes de commentaires \(RFC\)](#)