Configuration de la connexion du concentrateur Cisco VPN 300 à un routeur Cisco

Contenu

Introduction

Cet exemple de configuration montre comment connecter un réseau privé derrière un routeur qui exécute le logiciel Cisco IOS® à un réseau privé derrière le concentrateur Cisco VPN 3000. Les périphériques des réseaux se connaissent par leurs adresses privées.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Routeur Cisco 2611 avec logiciel Cisco IOS Version 12.3.1(1)a**Remarque :** assurez-vous que

les routeurs de la gamme Cisco 2600 sont installés avec une image IOS VPN IPsec cryptée qui prend en charge la fonctionnalité VPN.
- Concentrateur Cisco VPN 3000 avec 4.0.1 B

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.

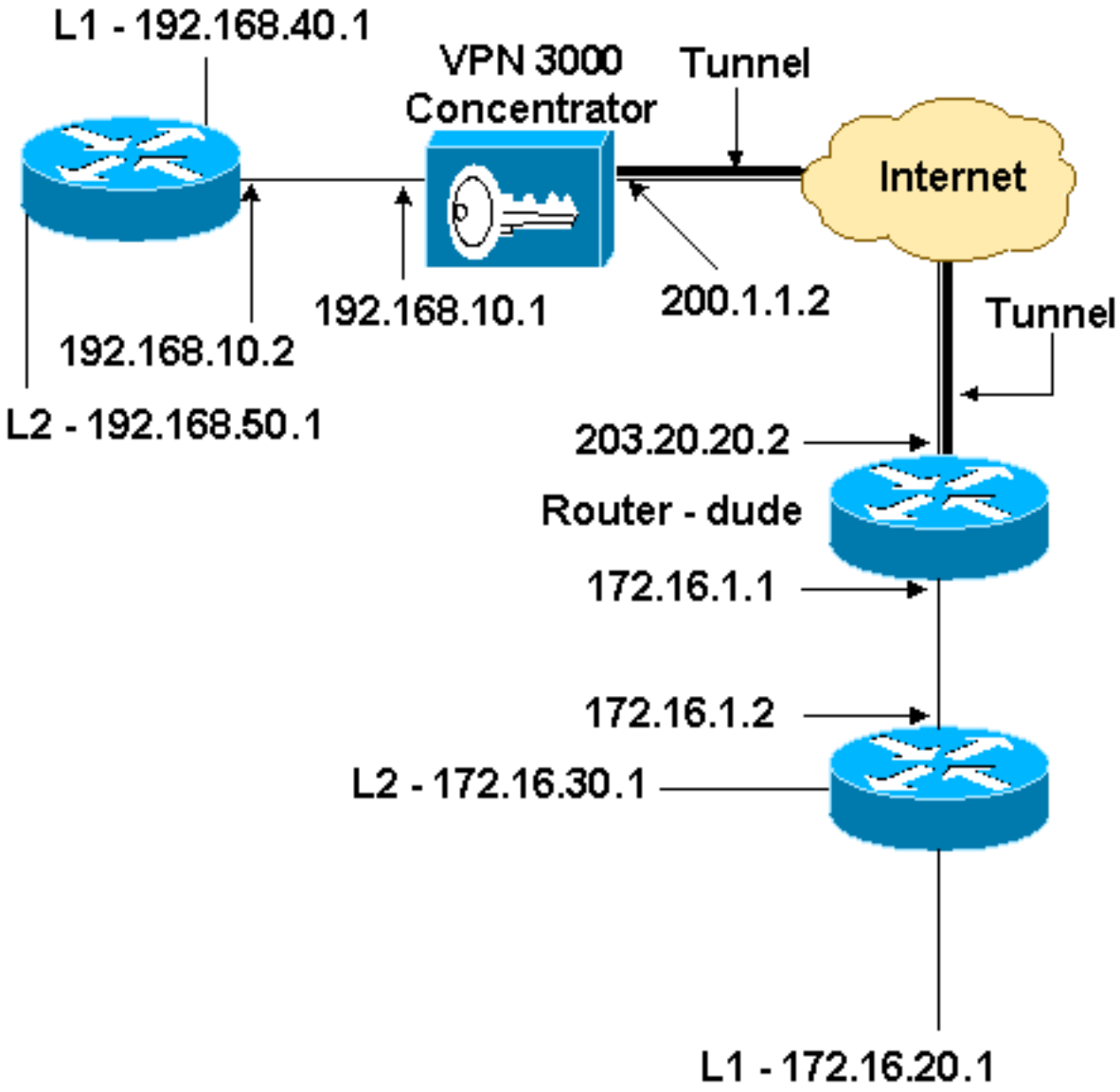
Configuration

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

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise la configuration suivante .

Configuration du routeur

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
```

```
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
```

```
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configuration du concentrateur VPN

Dans ce paramètre de travaux pratiques, le concentrateur VPN est d'abord accessible via le port de console et une configuration minimale est ajoutée afin que la configuration supplémentaire puisse être effectuée via l'interface utilisateur graphique (GUI).

Choisissez **Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration** pour vous assurer qu'il n'y a aucune configuration existante dans le concentrateur VPN.

Le concentrateur VPN apparaît dans Configuration rapide et ces éléments sont configurés après le redémarrage :

- Heure/Date
- Interfaces/masques dans **Configuration > Interfaces** (public=200.1.1.2/24, private=192.168.10.1/24)
- Passerelle par défaut dans **Configuration > Système > Routage IP >Passerelle par défaut** (200.1.1.1)

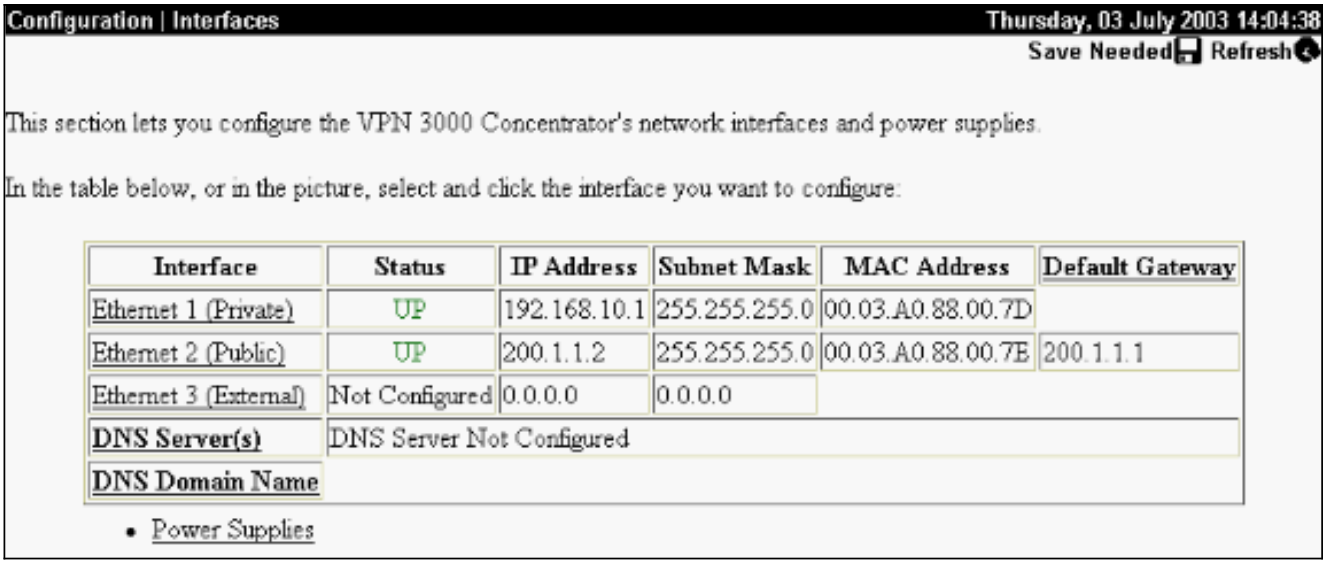
Àce stade, le concentrateur VPN est accessible via HTML depuis le réseau interne.

Remarque : Comme le concentrateur VPN est géré de l'extérieur, vous devez également sélectionner :

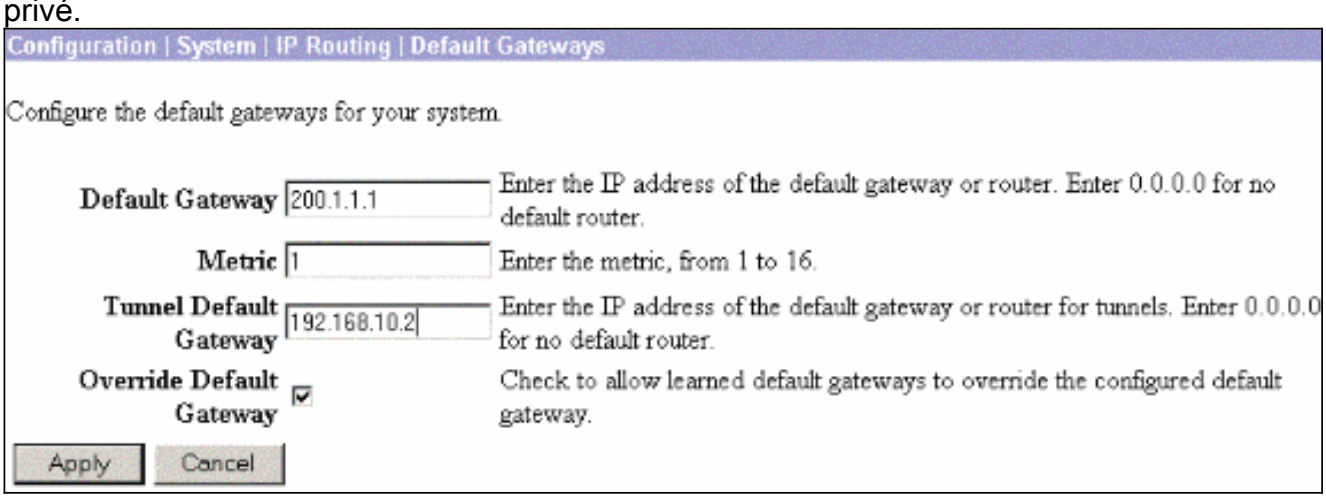
- **Configuration > Interfaces > 2-public > Sélectionnez IP Filter > 1. Privé (par défaut)**.
- **Administration > Access Rights > Access Control List > Add Manager Workstation** pour ajouter l'adresse IP du *gestionnaire externe*.

Ceci n'est pas nécessaire à moins que vous ne gérez le concentrateur VPN de l'*extérieur*.

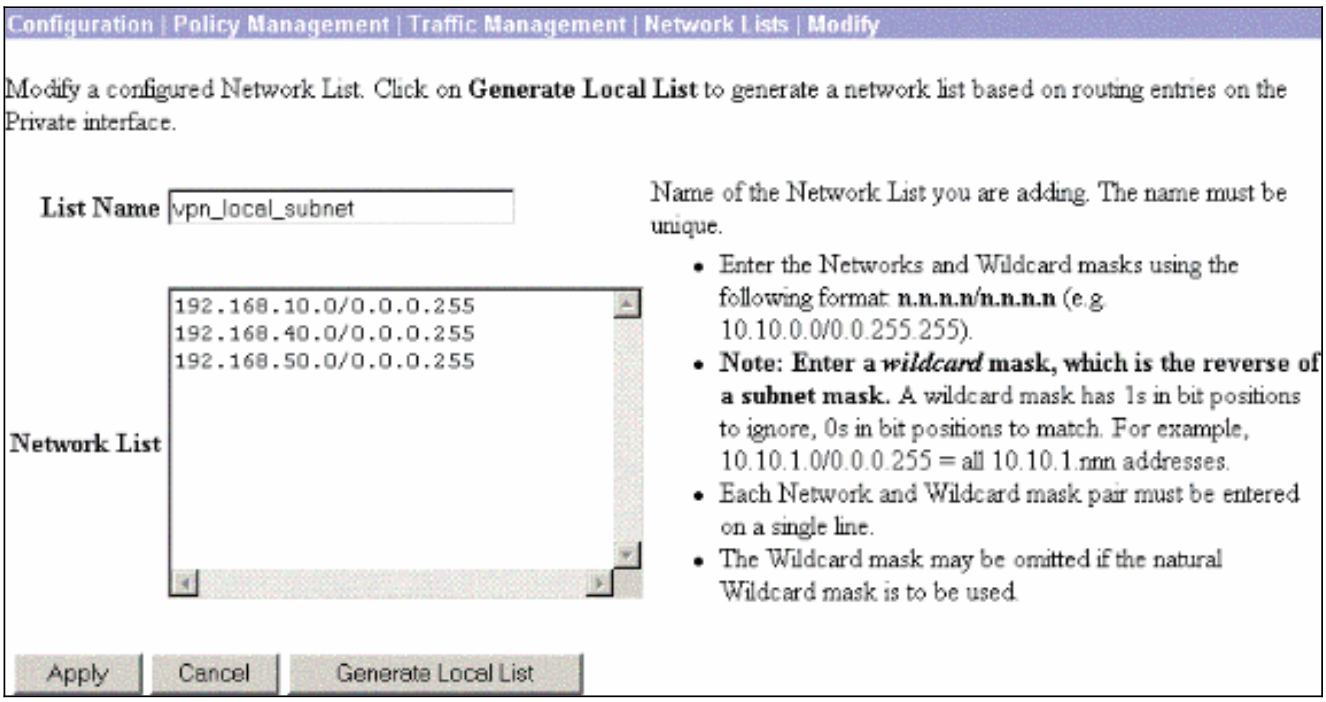
1. Choisissez **Configuration > Interfaces** pour vérifier les interfaces après avoir activé l'interface utilisateur
   graphique.



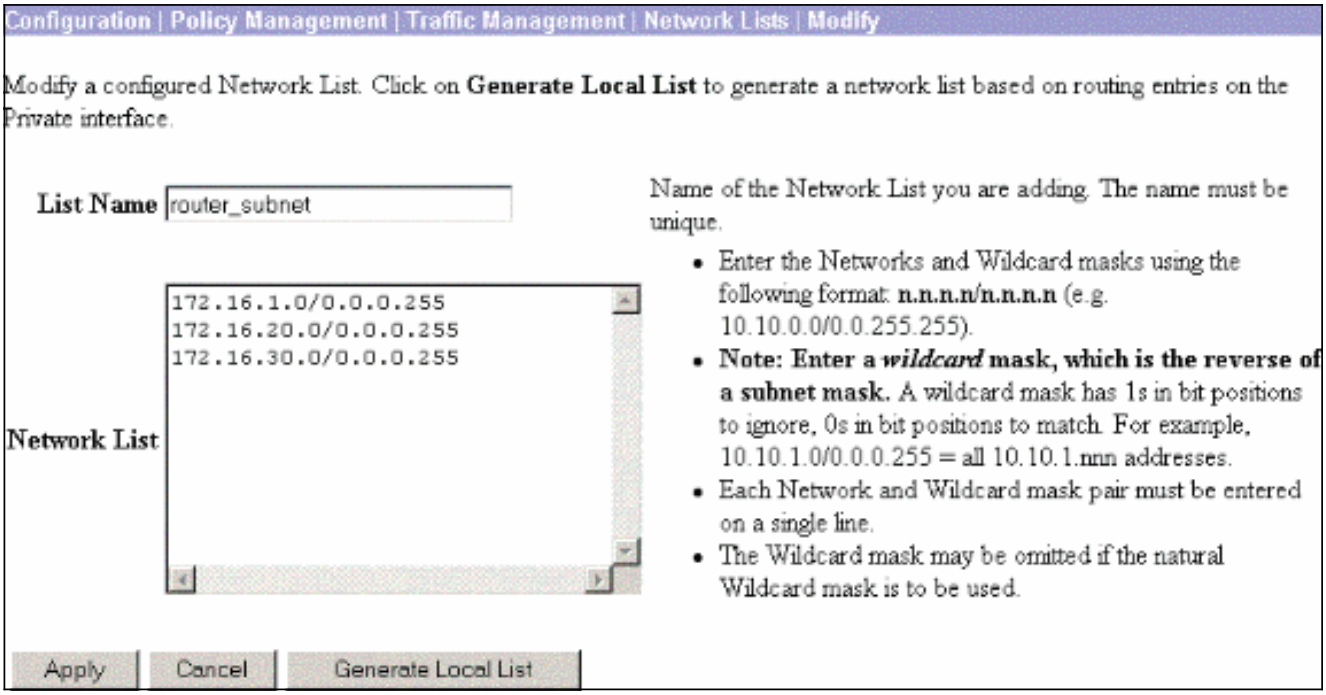
2. Choisissez Configuration > System > IP Routing > Default Gateways pour configurer la passerelle par défaut (Internet) et la passerelle par défaut du tunnel (interne) **Gateway** pour IPsec pour atteindre les autres sous-réseaux du réseau privé.



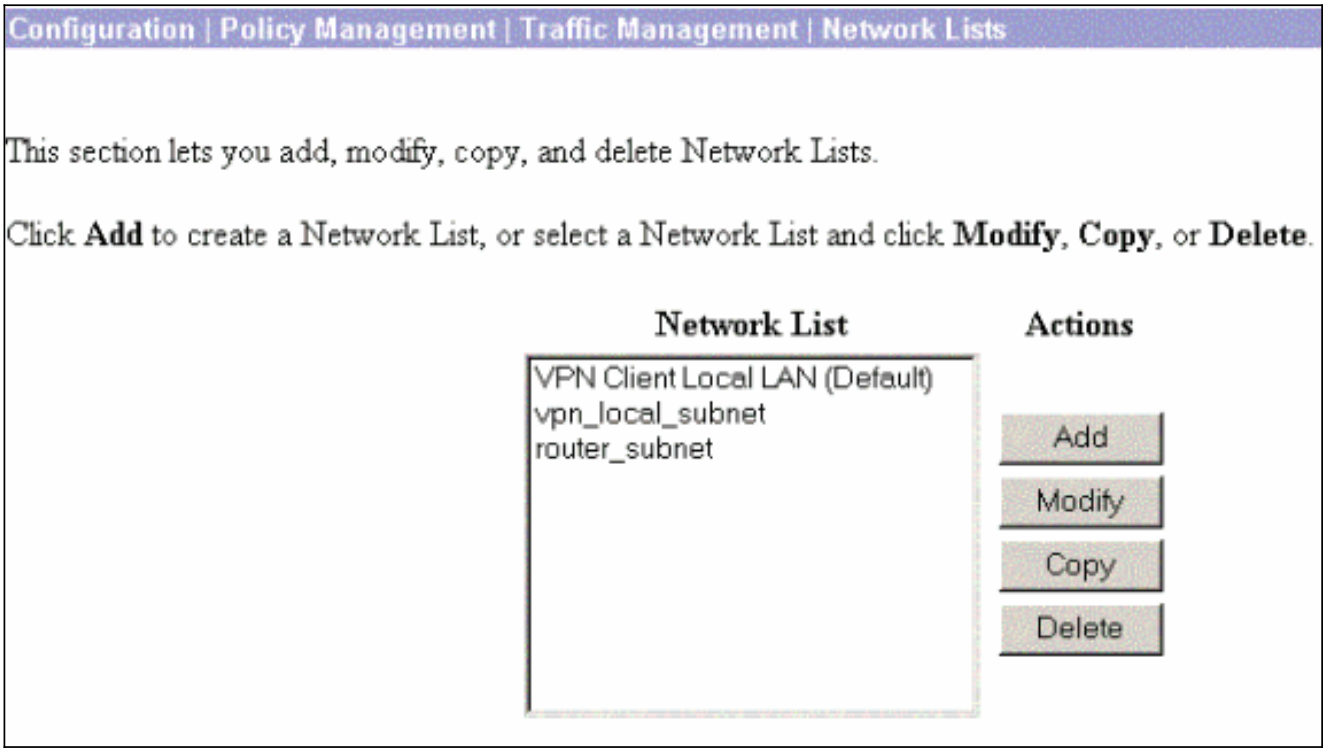
3. Choisissez **Configuration > Policy Management > Network Lists** pour créer les listes réseau qui définissent le trafic à chiffrer.Voici les réseaux locaux :



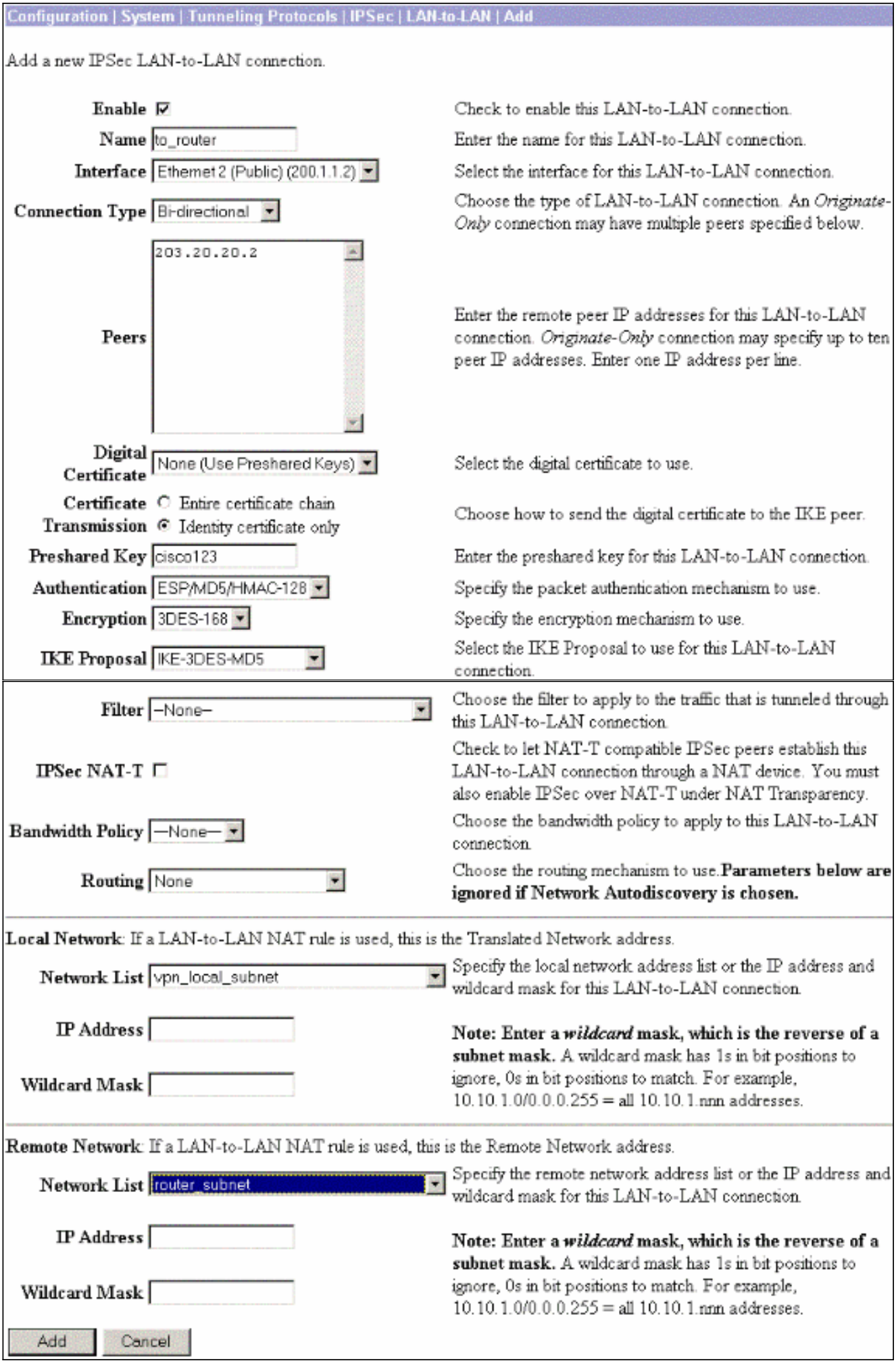
Voici les réseaux distants
:



4. Ensuite, notez les deux listes de réseaux :**Remarque :** si le tunnel IPsec ne s'active pas, vérifiez si le trafic intéressant correspond des deux côtés. Le trafic intéressant est défini par la liste d'accès sur le routeur et les zones PIX. Ils sont définis par des listes de réseau dans les concentrateurs
VPN.

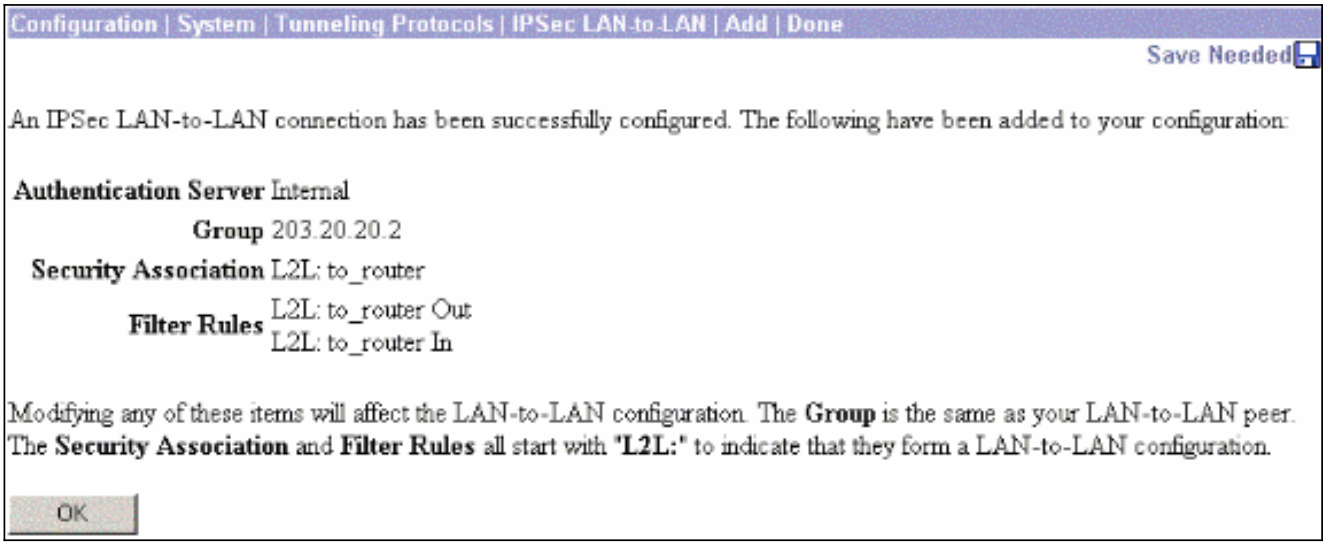


5. Choisissez **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** et définissez le tunnel LAN-to-
LAN.

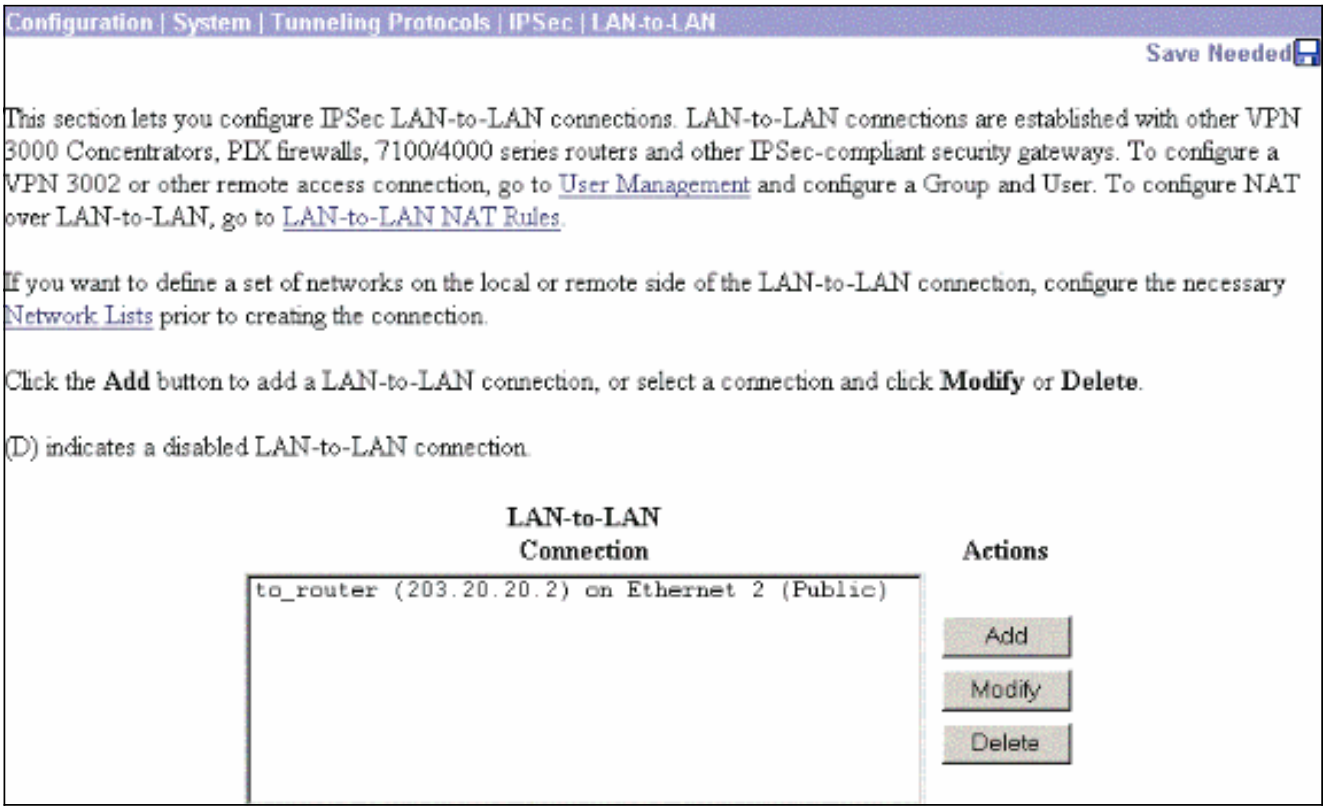


6. Après avoir cliqué sur **Apply**, cette fenêtre s'affiche avec l'autre configuration créée

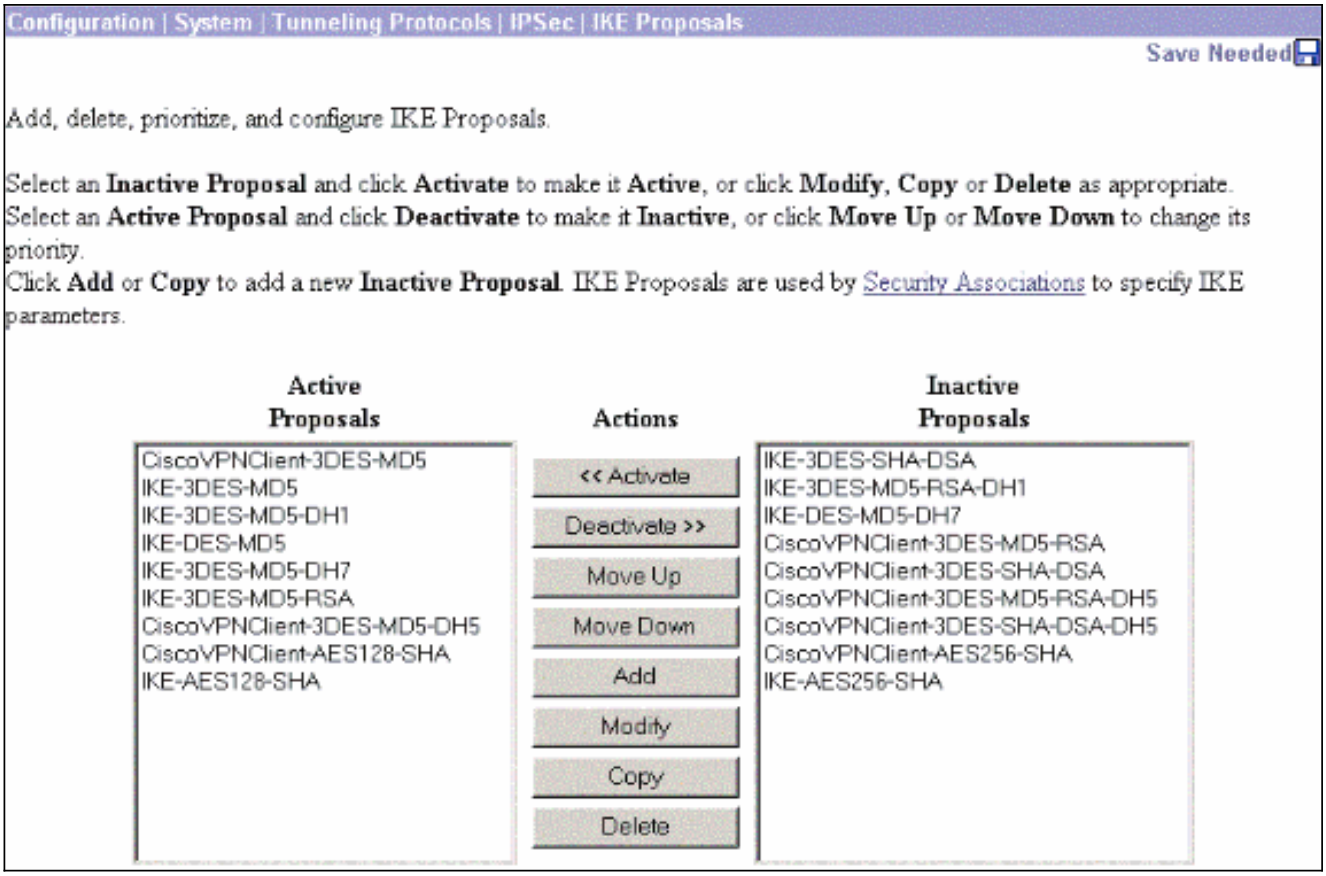
automatiquement à la suite de la configuration du tunnel LAN à LAN.



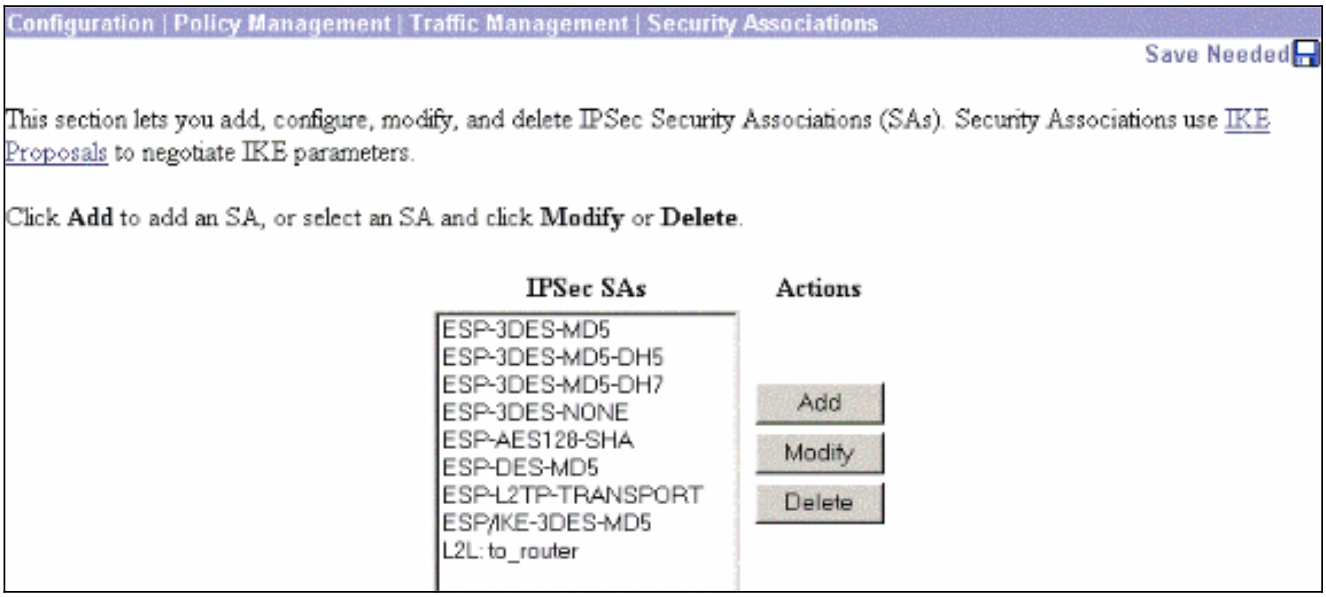
Les paramètres IPsec LAN à LAN précédemment créés peuvent être affichés ou modifiés dans **Configuration > System > Tunneling Protocols > IPSec LAN à LAN**.



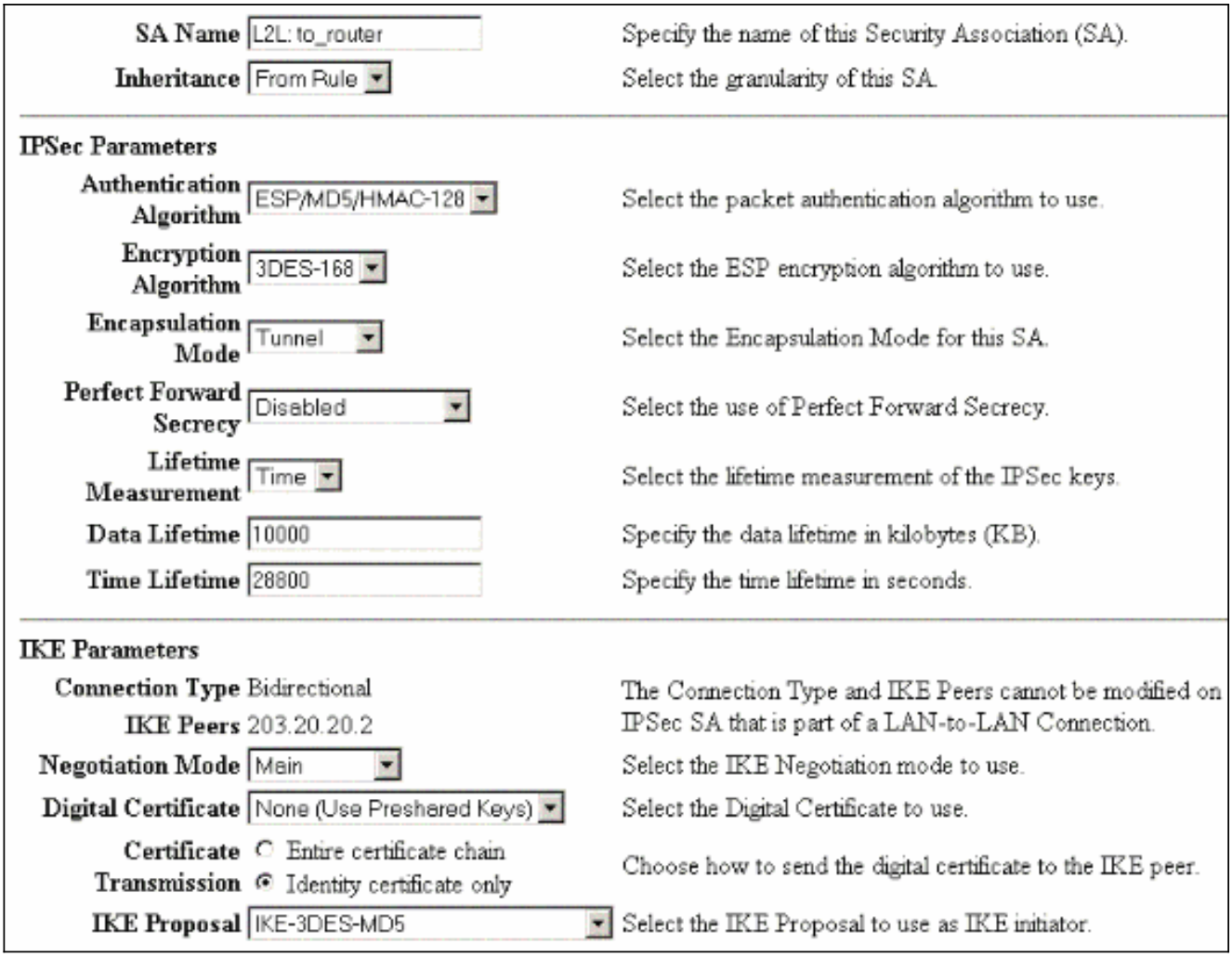
7. Choisissez Configuration > **System > Tunneling Protocols > IPSec > IKE Propositions** pour confirmer la proposition IKE active.



8. Choisissez **Configuration > Policy Management > Traffic Management > Security Associations** pour afficher la liste des associations de sécurité.



9. Cliquez sur le nom de l'association de sécurité, puis cliquez sur **Modifier** pour vérifier les associations de sécurité.



Vérification

Cette section répertorie les commandes **show** utilisées dans cette configuration.

Sur le routeur

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

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 .**

- **show crypto ipsec sa** - Affiche les paramètres utilisés par les associations de sécurité actuelles.
- **show crypto isakmp sa** - Affiche toutes les associations de sécurité Internet Key Exchange actuelles sur un homologue.
- **show crypto engine connection active** - Affiche les connexions de session chiffrées actives actuelles pour tous les moteurs de chiffrement.

Vous pouvez utiliser l'outil de recherche de commandes IOS (clients enregistrés uniquement) pour afficher plus d'informations sur des commandes particulières.

Sur le concentrateur VPN

Choisissez Configuration > **System > Events > Classes > Modify** pour activer la journalisation. Ces options sont disponibles :

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Gravité du journal = 1-13

Gravité vers la console = 1-3

Sélectionnez **Monitoring > Event Log** pour récupérer le journal des événements.

Dépannage

Sur le routeur

Référez-vous à Informations importantes sur les commandes de débogage avant d'essayer une commande de débogage.

- **debug crypto engine : Cette commande affiche le trafic chiffré.**
- **debug crypto ipsec — affiche les négociations IPsec de la Phase 2.**
- **debug crypto isakmp — affiche les négociations ISAKMP de la Phase 1.**

Problème - Impossible d'initier le tunnel

Message d'erreur

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solution

Complétez cette action afin de configurer le nombre souhaité de connexions simultanées ou définissez les connexions simultanées sur 5 pour cette SA :

Accédez à **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins** et définissez le nombre de connexions sur 5.

PFS

Dans des négociations IPsec, le Perfect Forward Secrecy (PFS) assure que chacune nouvelle clé cryptographique est indépendante de toute clé précédente. Activez ou désactivez PFS sur les deux homologues du tunnel . Sinon, le tunnel IPsec LAN à LAN (L2L) n'est pas établi dans les routeurs.

Afin de spécifier qu'IPsec doit demander PFS quand de nouvelles associations de sécurité sont demandées pour cette entrée de crypto-carte, ou qu'IPsec requiert PFS lorsqu'il reçoit des demandes de nouvelles associations de sécurité, utilisez la commande **set pfs** en mode de configuration de crypto-carte. Afin de spécifier qu'IPsec ne doit pas demander PFS, utilisez la forme **no** de cette commande.

```
set pfs [group1 | group2]
no set pfs
```

Pour la commande set pfs :

- *group1* : spécifie qu'IPsec doit utiliser le groupe de modules principaux Diffie-Hellman 768 bits lorsque le nouvel échange Diffie-Hellman est effectué.
- *group2* : spécifie qu'IPsec doit utiliser le groupe de modules principaux Diffie-Hellman 1 024 bits lorsque le nouvel échange Diffie-Hellman est effectué.

Par défaut, PFS n'est pas demandé. Si aucun groupe n'est spécifié avec cette commande, group1 est utilisé par défaut.

Exemple :

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Référez-vous à Référence des commandes de sécurité Cisco IOS pour plus d'informations sur la commande **set pfs**.

Informations connexes

- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Concentrateurs VPN de la gamme Cisco 3000
- Cisco VPN 3002 Hardware Clients
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems