

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du concentrateur VPN](#)

[Vérification](#)

[Sur le routeur](#)

[Sur le concentrateur VPN](#)

[Dépannage](#)

[Sur le routeur](#)

[Problème - Impossible d'initier le tunnel](#)

[PFS](#)

[Informations connexes](#)

[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)**aRemarque** : 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](#).

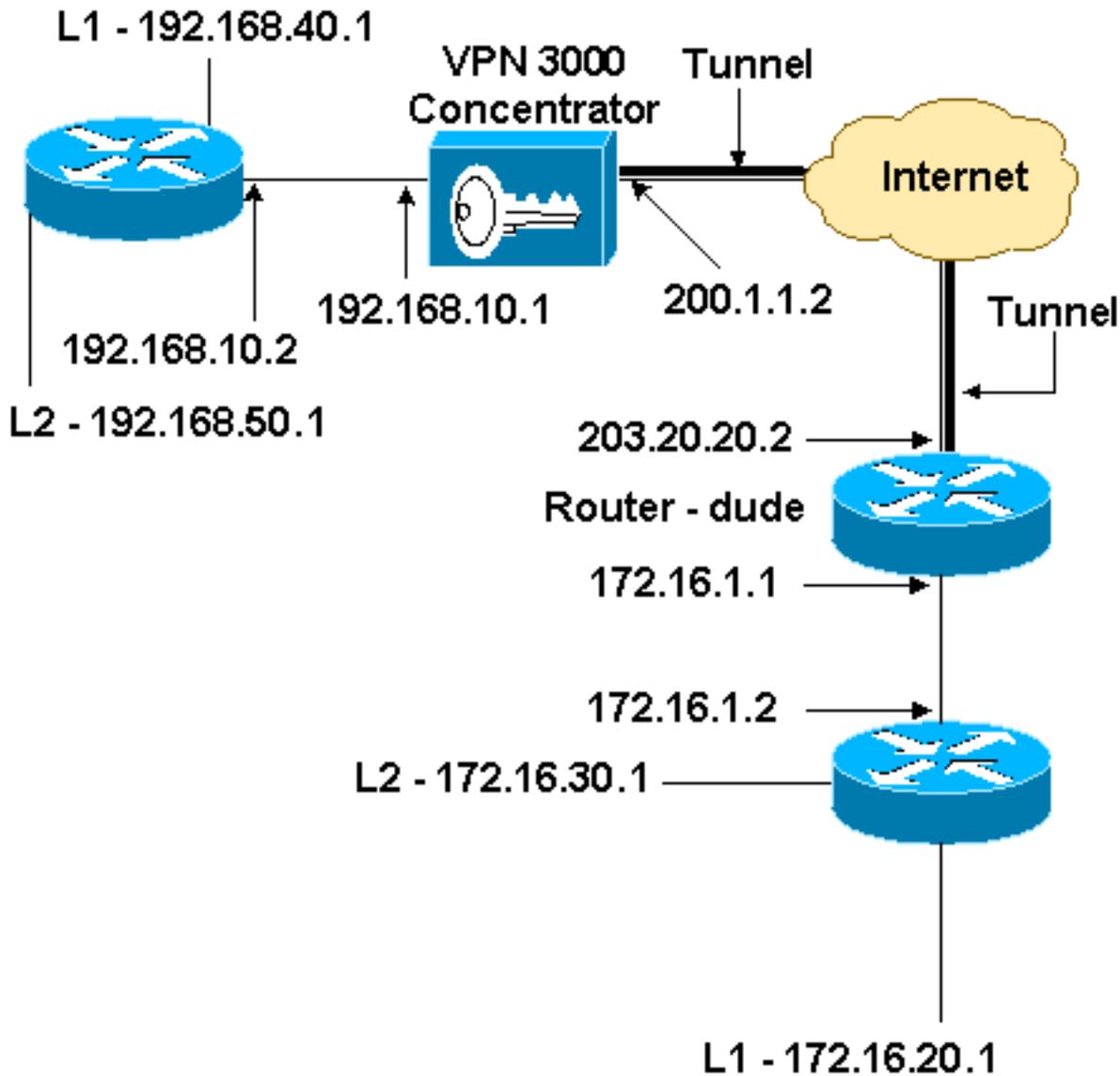
[Configuration](#)

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)

À ce 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.

Configuration | Interfaces Thursday, 03 July 2003 14:04:38
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.10.1	255.255.255.0	00.03.A0.88.00.7D	
Ethernet 2 (Public)	UP	200.1.1.2	255.255.255.0	00.03.A0.88.00.7E	200.1.1.1
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- [Power Supplies](#)

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.

Configuration | System | IP Routing | Default Gateways

Configure the default gateways for your system.

Default Gateway Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.

Metric Enter the metric, from 1 to 16.

Tunnel Default Gateway Enter the IP address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.

Override Default Gateway Check to allow learned default gateways to override the configured default gateway.

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

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name Name of the Network List you are adding. The name must be unique.

Network List

192.168.10.0/0.0.0.255
 192.168.40.0/0.0.0.255
 192.168.50.0/0.0.0.255

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note:** Enter a **wildcard mask**, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Voici les réseaux distants

:

The screenshot shows the 'Modify' page for a Network List. The breadcrumb navigation is 'Configuration | Policy Management | Traffic Management | Network Lists | Modify'. The main heading is 'Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.'

The 'List Name' field contains 'router_subnet'. To the right, a note states: 'Name of the Network List you are adding. The name must be unique.'

The 'Network List' text area contains three entries:
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255

Below the text area are three buttons: 'Apply', 'Cancel', and 'Generate Local List'.

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

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.

The screenshot shows the 'Network Lists' page. The breadcrumb navigation is 'Configuration | Policy Management | Traffic Management | Network Lists'. The main heading is 'This section lets you add, modify, copy, and delete Network Lists.'

Below the heading is the instruction: 'Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.'

The page features a table with two columns: 'Network List' and 'Actions'.

Network List	Actions
VPN Client Local LAN (Default) vpn_local_subnet router_subnet	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

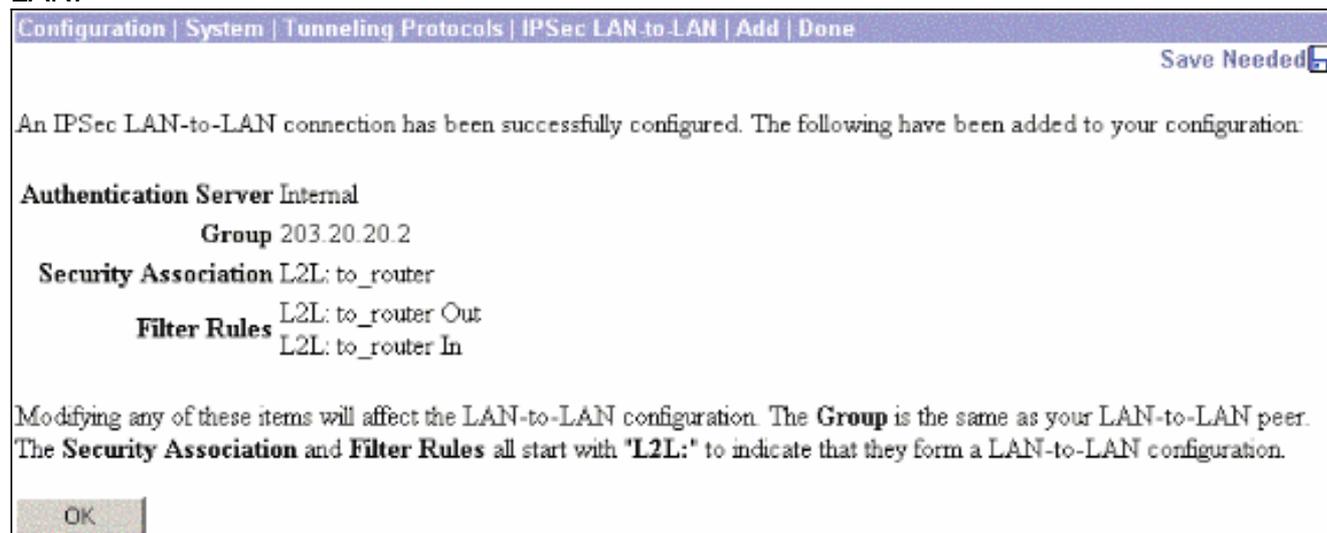
5. Choisissez **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** et définissez le tunnel LAN-to-LAN.

Add a new IPSec LAN-to-LAN connection.

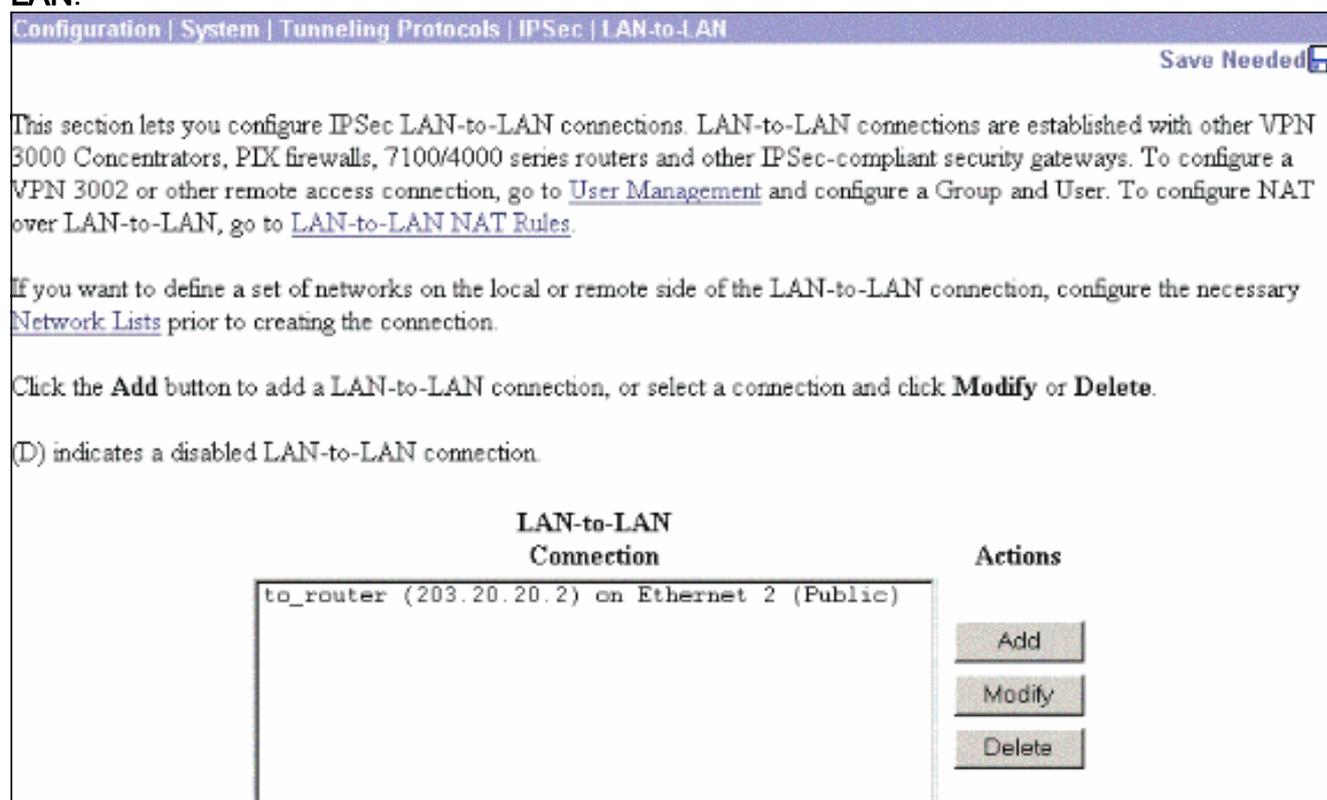
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet 2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 2px; min-height: 100px;"> <p>203.20.20.2</p> </div> <p>Digital Certificate <input type="text" value="None (Use Preshared Keys)"/></p> <p>Certificate <input type="radio"/> Entire certificate chain</p> <p>Transmission <input checked="" type="radio"/> Identity certificate only</p> <p>Preshared Key <input type="text" value="cisco123"/></p> <p>Authentication <input type="text" value="ESP/MD5/HMAC-128"/></p> <p>Encryption <input type="text" value="3DES-168"/></p> <p>IKE Proposal <input type="text" value="IKE-3DES-MD5"/></p>	<p>Check to enable this LAN-to-LAN connection.</p> <p>Enter the name for this LAN-to-LAN connection.</p> <p>Select the interface for this LAN-to-LAN connection.</p> <p>Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.</p> <p>Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.</p> <p>Select the digital certificate to use.</p> <p>Choose how to send the digital certificate to the IKE peer.</p> <p>Enter the preshared key for this LAN-to-LAN connection.</p> <p>Specify the packet authentication mechanism to use.</p> <p>Specify the encryption mechanism to use.</p> <p>Select the IKE Proposal to use for this LAN-to-LAN connection.</p>
<p>Filter <input type="text" value="-None-"/></p> <p>IPSec NAT-T <input type="checkbox"/></p> <p>Bandwidth Policy <input type="text" value="-None-"/></p> <p>Routing <input type="text" value="None"/></p>	<p>Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.</p> <p>Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.</p> <p>Choose the bandwidth policy to apply to this LAN-to-LAN connection.</p> <p>Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.</p>
<p>Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.</p> <p>Network List <input type="text" value="vpn_local_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p>Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.</p> <p>Network List <input type="text" value="router_subnet"/></p> <p>IP Address <input type="text"/></p> <p>Wildcard Mask <input type="text"/></p>	
<p><input type="button" value="Add"/> <input type="button" value="Cancel"/></p>	

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.

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.

Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
CiscoVPNClient-3DES-MD5 IKE-3DES-MD5 IKE-3DES-MD5-DH1 IKE-DES-MD5 IKE-3DES-MD5-DH7 IKE-3DES-MD5-RSA CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-AES128-SHA IKE-AES128-SHA	<input type="button" value="« Activate"/> <input type="button" value="Deactivate »"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES256-SHA IKE-AES256-SHA

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

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs	Actions
ESP-3DES-MD5 ESP-3DES-MD5-DH5 ESP-3DES-MD5-DH7 ESP-3DES-NONE ESP-AES128-SHA ESP-DES-MD5 ESP-L2TP-TRANSPORT ESP/IKE-3DES-MD5 L2L: to_router	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

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

SA Name	<input type="text" value="L2L: to_router"/>	Specify the name of this Security Association (SA).
Inheritance	<input type="text" value="From Rule"/>	Select the granularity of this SA.
IPSec Parameters		
Authentication Algorithm	<input type="text" value="ESP/MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the ESP encryption algorithm to use.
Encapsulation Mode	<input type="text" value="Tunnel"/>	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	<input type="text" value="Disabled"/>	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IPSec keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="28800"/>	Specify the time lifetime in seconds.
IKE Parameters		
Connection Type	<input type="text" value="Bidirectional"/>	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	<input type="text" value="203.20.20.2"/>	
Negotiation Mode	<input type="text" value="Main"/>	Select the IKE Negotiation mode to use.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use as IKE initiator.

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](#)