

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du concentrateur VPN](#)

[Vérifiez](#)

[Sur le routeur](#)

[Sur le concentrateur VPN](#)

[Dépannez](#)

[Sur le routeur](#)

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

[PFS](#)

[Informations connexes](#)

[Introduction](#)

Cette configuration d'échantillon affiche comment connecter un réseau privé derrière un routeur qui exécute le logiciel de Cisco IOS® à un réseau privé derrière le concentrateur de Cisco VPN 3000. Les périphériques sur les réseaux se connaissent par leurs adresses privées.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Routeur de Cisco 2611 avec la version du logiciel Cisco IOS 12.3.(1)**Note:** Assurez-vous que

des Routeurs de gamme Cisco 2600 sont installés avec une image crypto IOS d'IPsec VPN qui prend en charge la caractéristique VPN.

- Concentrateur de Cisco VPN 3000 avec 4.0.1 B

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](#).

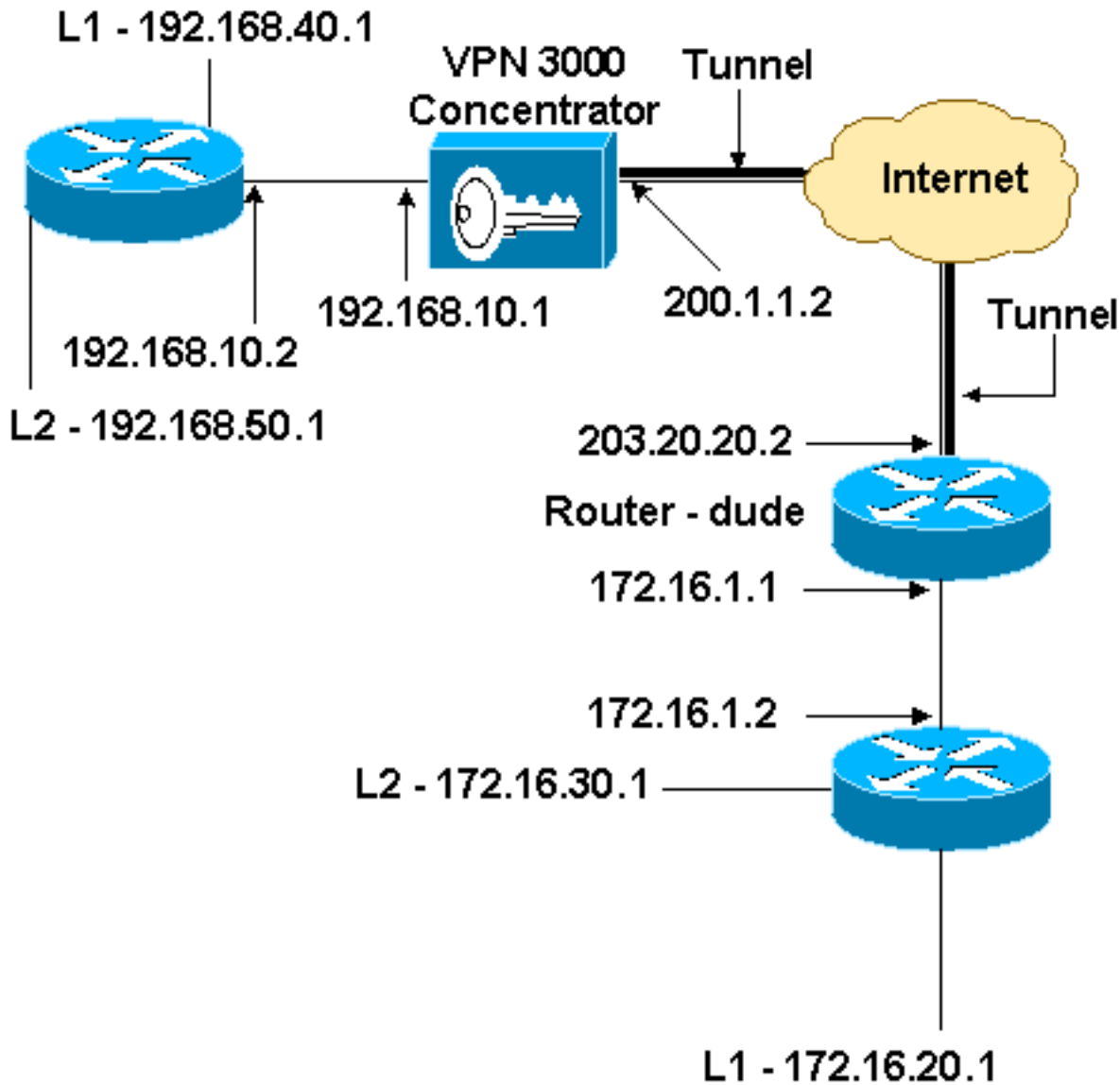
[Configurez](#)

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

Note: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

[Diagramme du réseau](#)

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise cette configuration.

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

En cette configuration de laboratoire, le concentrateur VPN est d'abord accédé à par le port de console et une configuration minimale est ajoutée de sorte que la configuration supplémentaire puisse être faite par l'interface utilisateur graphique (GUI).

Choisissez la **gestion** > la **réinitialisation** > la **réinitialisation planification** > la **réinitialisation de système avec l'usine/configuration par défaut** pour s'assurer qu'il n'y a aucune configuration existante dans le concentrateur VPN.

Le concentrateur VPN apparaît dans la configuration rapide, et ces éléments sont configurés après la réinitialisation :

- Heure/date
- Interfaces/masques dans le **Configuration** > **Interfaces** (public=200.1.1.2/24, private=192.168.10.1/24)
- Passerelle par défaut dans la **configuration** > le **système** > le **Routage IP** > le **Default_Gateway** (200.1.1.1)

En ce moment, le concentrateur VPN est accessible par le HTML du réseau intérieur.

Note: Puisque le concentrateur VPN est géré de l'extérieur, vous devez également sélectionner :

- **Configuration** > **Interfaces** > **2-public** > **filtre IP choisi** > **1. privé (par défaut)**.
- **L'Administration** > **Access Rights** > **Access Control List** > ajoutent le poste de travail de **gestionnaire** pour ajouter l'adresse IP du *gestionnaire externe*.

Ce n'est pas nécessaire à moins que vous gériez le concentrateur VPN de l'*extérieur*.

1. Choisissez le **Configuration** > **Interfaces** pour revérifier les interfaces après que vous apportiez le GUI.

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 la **configuration > le système > le Routage IP > les passerelles par défaut** pour configurer la **passerelle par défaut** (d'Internet) et la **passerelle de par défaut de tunnel** (à l'intérieur) pour qu'IPsec atteigne les autres sous-réseaux dans le 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 la **configuration > la Gestion des stratégies > les listes des réseaux** pour créer les listes des réseaux qui définissent le trafic à chiffrer. Ce sont 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.

Ce sont les réseaux distants

:

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.

- 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.

Network List

```
172.16.1.0/0.0.0.255
172.16.20.0/0.0.0.255
172.16.30.0/0.0.0.255
```

Apply Cancel Generate Local List

4. Une fois terminés, ce sont les deux listes des réseaux :**Note:** Si le tunnel d'IPsec ne monte pas, vérifier pour voir si le trafic intéressant s'assortit des deux côtés. Le trafic intéressant est défini par la liste d'accès sur le routeur et des cases PIX. Ils sont définis par des listes des réseaux dans les concentrateurs VPN.

Configuration | Policy Management | Traffic Management | Network Lists

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default)	Add Modify Copy Delete
vpn_local_subnet	
router_subnet	

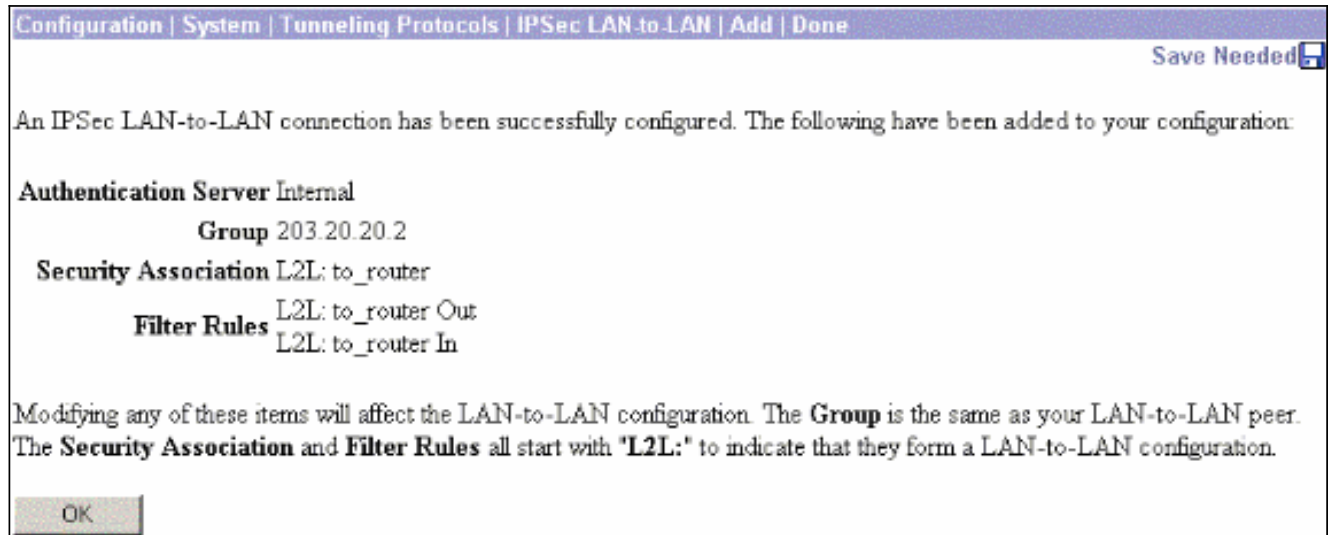
5. Choisissez la **configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux d'IPSec** et définissez le tunnel entre réseaux locaux.

Add a new IPSec LAN-to-LAN connection.

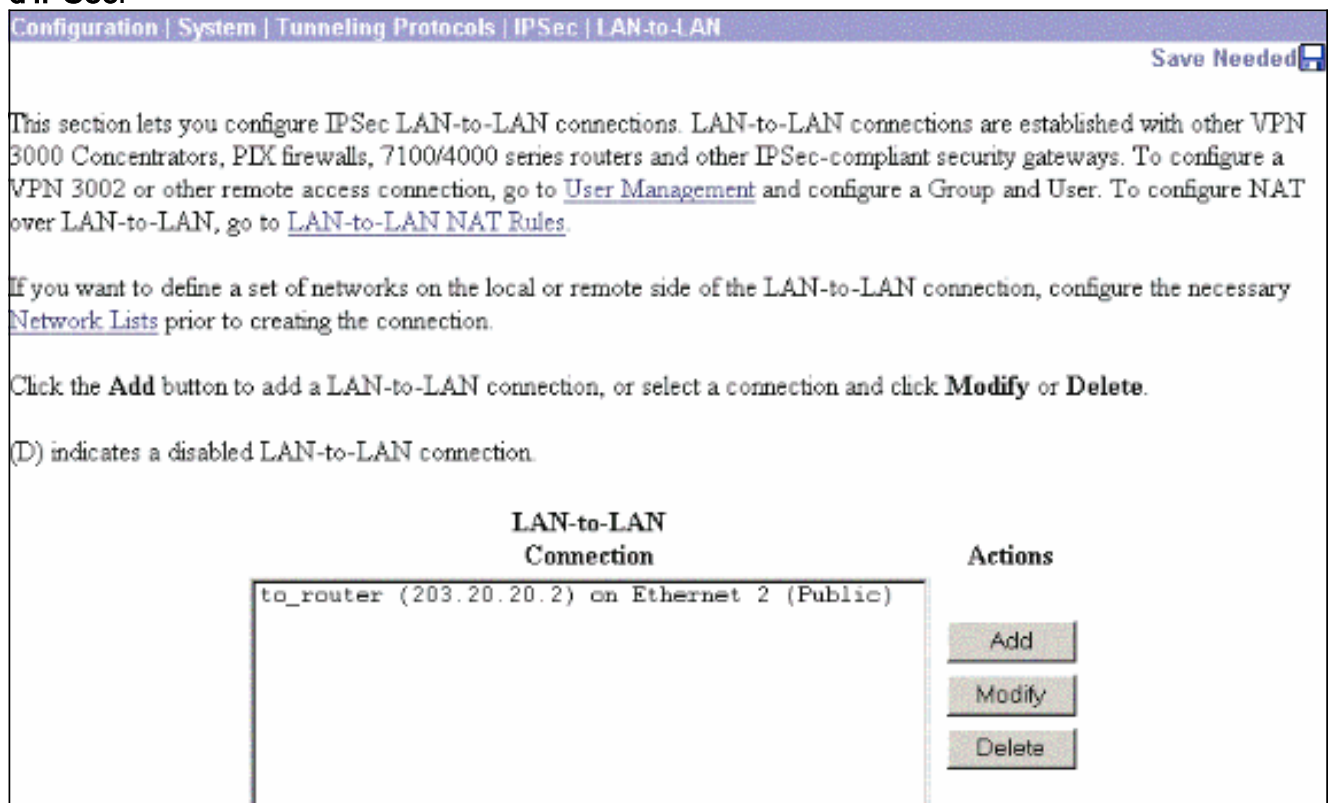
<p>Enable <input checked="" type="checkbox"/></p> <p>Name <input type="text" value="to_router"/></p> <p>Interface <input type="text" value="Ethernet2 (Public) (200.1.1.2)"/></p> <p>Connection Type <input type="text" value="Bi-directional"/></p> <p>Peers</p> <div style="border: 1px solid gray; padding: 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 que vous cliquez sur Apply, cette fenêtre est affichée avec l'autre configuration qui est

automatiquement créée en raison de la configuration de tunnel entre réseaux locaux.



Les paramètres précédemment créés d'IPsec d'entre réseaux locaux peuvent être visualisés ou modifiés dans la configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux d'IPsec.



7. Choisissez la configuration > les protocoles de système > de Tunnellisation > l'IPsec > les propositions d'IKE pour confirmer la proposition active d'IKE.

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 la configuration > la **Gestion des stratégies** > la **gestion de trafic** > les **associations de sécurité** pour visualiser la liste d'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 d'association de sécurité, et 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	Bidirectional	The Connection Type and IKE Peers cannot be modified on IPSec SA that is part of a LAN-to-LAN Connection.
IKE Peers	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.

Vérifiez

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 configurations utilisées par les associations de sécurité en cours.
- **show crypto isakmp sa** — Affiche toutes les associations en cours de sécurité IKE à un pair.
- **show crypto engine connection active** — Affiche les connexions de session chiffrées par active en cours pour tous les moteurs de chiffrement.

Vous pouvez utiliser l'[utilitaire de recherche de commande IOS](#) (clients [enregistrés](#) seulement) pour voir plus d'informations sur des commandes particulières.

[Sur le concentrateur VPN](#)

Choisissez la **configuration** > le **système** > les **événements** > les **classes** > **modifiez** pour activer

se connecter. Ces options sont disponibles :

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

Sévérité pour se connecter = 1-13

Sévérité pour consoler = 1-3

Sélectionnez la **surveillance** > le **journal d'événements** pour récupérer le journal d'événements.

Dépannez

Sur le routeur

Référez-vous aux [informations importantes sur des commandes de debug](#) avant que vous tentiez toutes les commandes de débogage.

- **debug crypto engine** — Affiche le trafic qui est chiffré.
- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** — affiche les négociations ISAKMP de la phase 1.

Problème - Incapable d'initier le tunnel

```
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

```

Solution

Terminez-vous cette action afin de configurer le nombre désiré de procédures de connexion simultanées ou placer les procédures de connexion simultanées à 5 pour cette SA :

Allez au **Configuration > User Management > Groups > modifiant 10.19.187.229 > le général > les procédures de connexion de Simultaneouts** et changent le nombre de procédures de connexion à 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 le PFS sur les

les deux les pairs de tunnel. Autrement, le tunnel d'IPsec de l'entre réseaux locaux (L2L) n'est pas établi dans des Routeurs.

Afin de spécifier qu'IPsec devrait demander le PFS quand de nouvelles associations de sécurité sont priées pour cette entrée de crypto map, ou qu'IPsec a besoin du PFS quand elle reçoit des demandes de nouvelles associations de sécurité, utilisez le **set pfs** commandent dans le mode de configuration de crypto map. Afin de spécifier qu'IPsec ne devrait pas demander le PFS, utilisez le **forme no de** cette commande.

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

Pour la commande set pfs :

- *group1* — Spécifie qu'IPsec devrait utiliser le groupe de module de perfection 768-bit Diffie-Hellman quand le nouvel échange de Diffie-Hellman est exécuté.
- *group2* — Spécifie qu'IPsec devrait utiliser le groupe de module de perfection 1024-bit Diffie-Hellman quand le nouvel échange de Diffie-Hellman est exécuté.

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 la [référence de commandes de Cisco IOS Security](#) pour plus d'informations sur la commande de **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](#)