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

## Contenu



# 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)a**Remarque:** 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.

**Remarque:** 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.

**Remarque:** 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.
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.
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 :Ce sont les réseaux distants :
4. Une fois terminés, ce sont les deux listes des réseaux :**Remarque:** 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.
5. Choisissez la **configuration** > les **protocoles de système** > de **Tunnellisation** > l'**entre réseaux locaux d'IPSec** et définissez le tunnel entre réseaux locaux.
6. Après que vous cliquiez 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.
8. Choisissez la **configuration** > la **Gestion des stratégies** > la **gestion de trafic** > les **associations de sécurité** pour visualiser la liste d'associations de sécurité.
9. Cliquez sur le nom d'association de sécurité, et puis cliquez sur **modifient** pour vérifier les associations de sécurité.

# 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** > **modifient** 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

```
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**

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 > modifient 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