Exemple de configuration d'un routeur autorisant les clients VPN à se connecter à IPsec et à Internet via la transmission tunnel partagée

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Informations générales
Configurez
Diagramme du réseau
Configurations
Configuration VPN Client 4.8
Vérifiez
Dépannez
Dépannage des commandes
Informations connexes

Introduction

Ce document fournit des instructions pas à pas sur la façon dont permettre à des clients vpn l'accès à Internet tandis qu'ils sont percés un tunnel dans un routeur de Cisco IOS®. Cette configuration est requise pour permettre aux clients VPN l'accès sécurisé aux ressources de l'entreprise par l'intermédiaire d'IPsec et en même temps pour permettre un accès non sécurisé à Internet. Cette configuration s'appelle la transmission tunnel partagée.

Remarque: La transmission tunnel partagée peut poser un risque de sécurité une fois configurée. Puisque les clients vpn ont l'accès à Internet sans garantie, ils peuvent être compromis par un attaquant. Cet attaquant peut alors accéder au RÉSEAU LOCAL entreprise par l'intermédiaire du tunnel d'IPsec. Une compromission entre une transmission tunnel totale et une transmission tunnel partagée peut être de ne permettre aux clients VPN que l'accès au LAN. Référez-vous à PIX/ASA 7.x : Exemple de configuration pour permettre aux clients VPN d'accéder au réseau local pour plus d'informations.

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 3640 de Cisco avec la version du logiciel Cisco IOS 12.4
- Client VPN Cisco 4.8

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.

Informations générales

Les VPN d'accès à distance adressent la condition requise du collaborateur mobile pour se connecter en toute sécurité au réseau de l'entreprise. Les utilisateurs mobiles peuvent configurer une connexion sécurisée à l'aide du logiciel client VPN installé sur leurs PC. Le client VPN initie une connexion au périphérique d'un site central configuré pour accepter ces requêtes. Dans cet exemple, le périphérique de lieu d'exploitation principal est un routeur Cisco IOS qui utilise des crypto-cartes dynamiques.

Quand vous activez la Segmentation de tunnel pour des connexions VPN, elle exige la configuration d'une liste de contrôle d'accès (ACL) sur le routeur. Dans cet exemple, la commande de la **liste d'accès 101** est associée avec le groupe pour la Segmentation de tunnel, et le tunnel est formé au réseau 10.10.10.x/24. La circulation décryptée (par exemple, l'Internet) aux périphériques est exclue des réseaux configurés dans l'ACL 101.

```
access-list 101 permit ip 10.10.10.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Appliquez l'ACL sur les propriétés de groupe.

```
crypto isakmp client configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl 101
```

Dans cet exemple de configuration, un tunnel IPsec est configuré avec les éléments suivants :

- Les crypto map se sont appliqués aux interfaces extérieures sur le PIX
- Authentification étendue (Xauth) des clients vpn contre une authentification locale
- Affectation dynamique d'une adresse IP privée d'un groupe aux clients vpn
- La fonctionnalité **nat 0 access-list command**, qui permet à des hôtes sur un LAN d'utiliser des

adresses IP privées avec un utilisateur distant et de toujours obtenir une adresse de Traduction d'adresses de réseau (NAT) du PIX pour visiter un réseau non sécurisé.

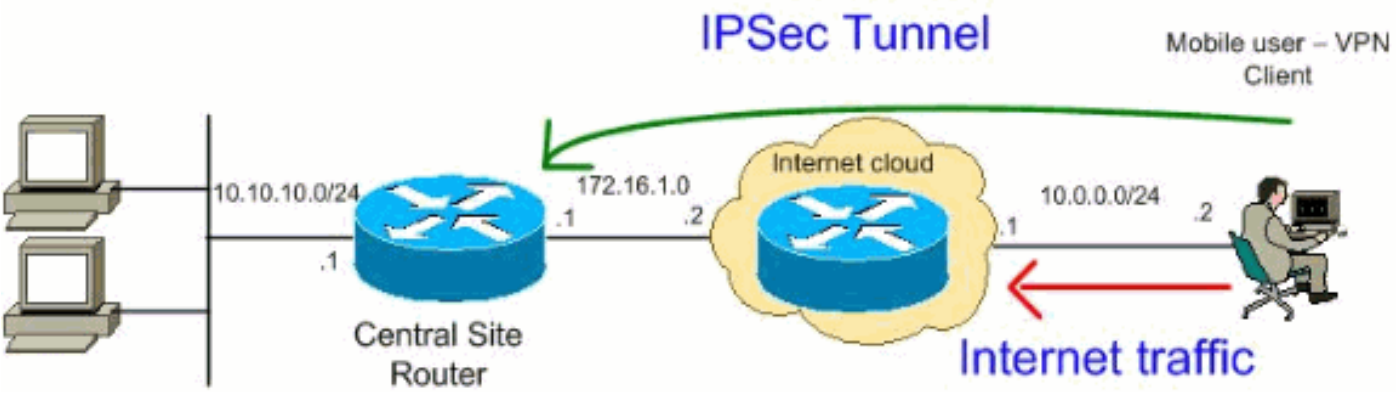
Configurez

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 obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

- Routeur
- Client VPN Cisco

Routeur

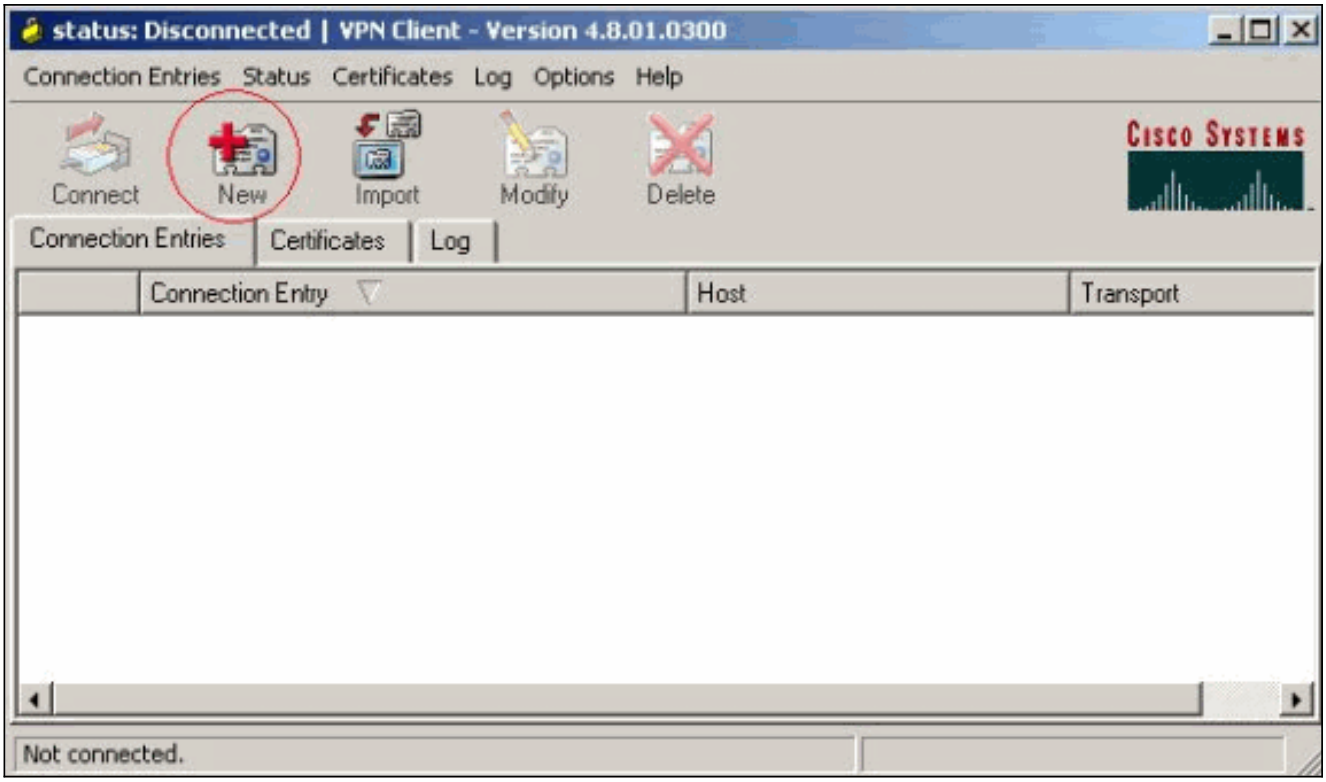
```
VPN#show run Building configuration... Current configuration : 2170 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname VPN ! boot-start-marker boot-end-marker ! ! !--- Enable authentication, authorization and accounting (AAA) !--- for user authentication and group authorization. aaa new-model ! !--- In order to enable Xauth for user authentication, !--- enable the aaa authentication commands. aaa authentication login userauthen local !--- In order to enable group authorization, enable !--- the aaa authorization commands. aaa authorization network groupauthor local ! aaa session-id common ! resource policy ! ! !--- For local authentication of the IPsec user, !--- create the user with a password. username
```

```
user password 0 cisco ! ! !--- Create an Internet
Security Association and !--- Key Management Protocol
(ISAKMP) policy for Phase 1 negotiations. crypto isakmp
policy 3 encr 3des authentication pre-share group 2 !---
Create a group that is used to specify the !--- WINS and
DNS server addresses to the VPN Client, !--- along with
the pre-shared key for authentication. Use ACL 101 used
for !--- the Split tunneling in the VPN Clinet end.
crypto isakmp client configuration group vpnclient key
cisco123 dns 10.10.10.10 wins 10.10.10.20 domain
cisco.com pool ippool acl 101 ! !--- Create the Phase 2
Policy for actual data encryption. crypto ipsec
transform-set myset esp-3des esp-md5-hmac ! !--- Create
a dynamic map and apply !--- the transform set that was
created earlier. crypto dynamic-map dynmap 10 set
transform-set myset reverse-route ! !--- Create the
actual crypto map, !--- and apply the AAA lists that
were created earlier. crypto map clientmap client
authentication list userauthen crypto map clientmap
isakmp authorization list groupauthor crypto map
clientmap client configuration address respond crypto
map clientmap 10 ipsec-isakmp dynamic dynmap ! ! ! !
interface Ethernet0/0 ip address 10.10.10.1
255.255.255.0 half-duplex ip nat inside !--- Apply the
crypto map on the outbound interface. interface
FastEthernet1/0 ip address 172.16.1.1 255.255.255.0 ip
nat outside ip virtual-reassembly duplex auto speed auto
crypto map clientmap ! interface Serial2/0 no ip address
! interface Serial2/1 no ip address shutdown ! interface
Serial2/2 no ip address shutdown ! interface Serial2/3
no ip address shutdown !--- Create a pool of addresses
to be !--- assigned to the VPN Clients. ! ip local pool
ippool 192.168.1.1 192.168.1.2 ip http server no ip http
secure-server ! ip route 0.0.0.0 0.0.0.0 172.16.1.2 !---
Enables Network Address Translation (NAT) !--- of the
inside source address that matches access list 111 !---
and gets PATed with the FastEthernet IP address. ip nat
inside source list 111 interface FastEthernet1/0
overload ! !--- The access list is used to specify which
traffic !--- is to be translated for the outside
Internet. access-list 111 deny ip 10.10.10.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 111 permit ip any any
!--- Configure the interesting traffic to be encrypted
from the VPN Client !--- to the central site router
(access list 101). !--- Apply this ACL in the ISAKMP
configuration. access-list 101 permit ip 10.10.10.0
0.0.0.255 192.168.1.0 0.0.0.255 control-plane ! line con
0 line aux 0 line vty 0 4 ! end
```

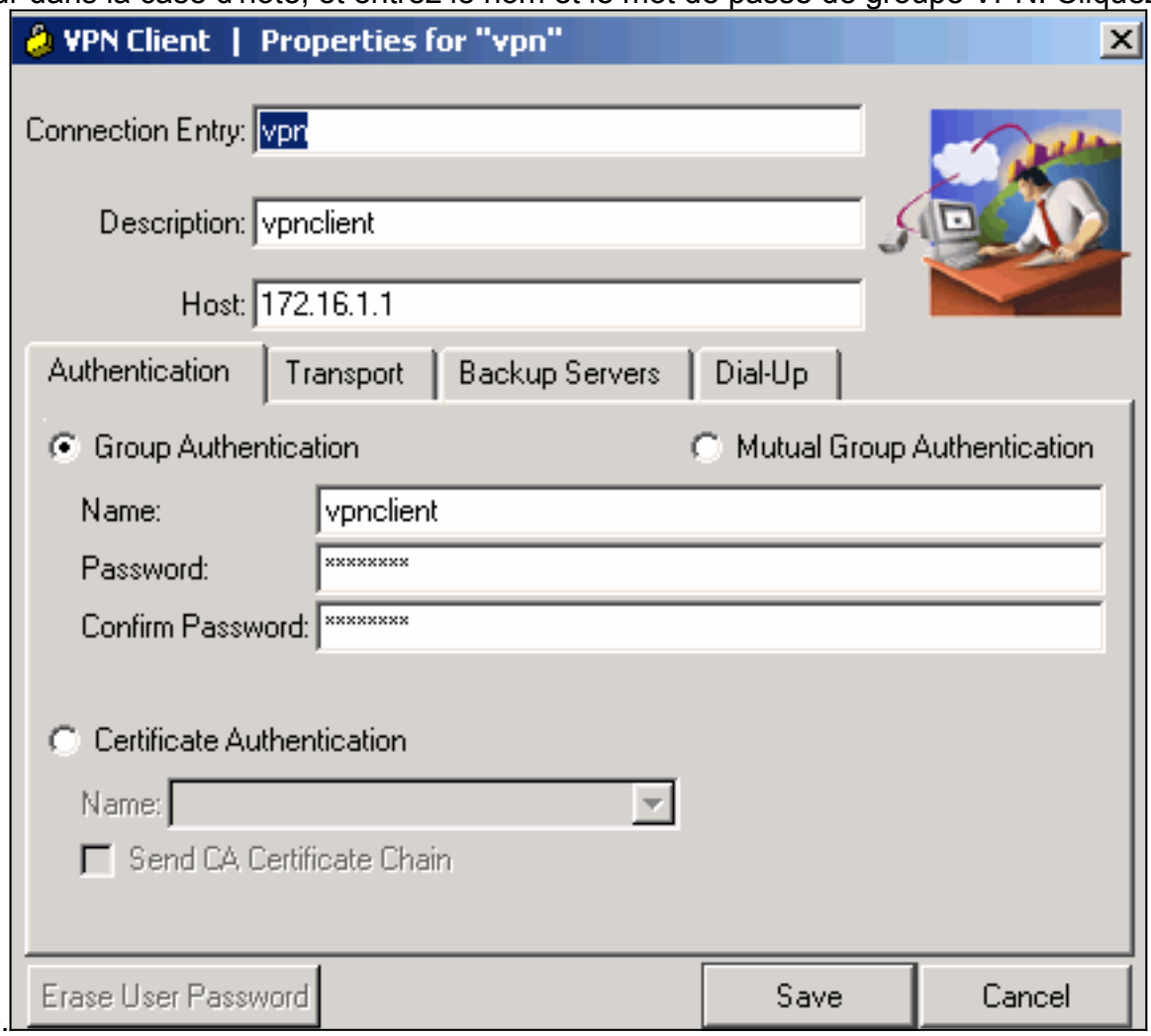
Configuration VPN Client 4.8

Terminez-vous ces étapes afin de configurer le client vpn 4.8.

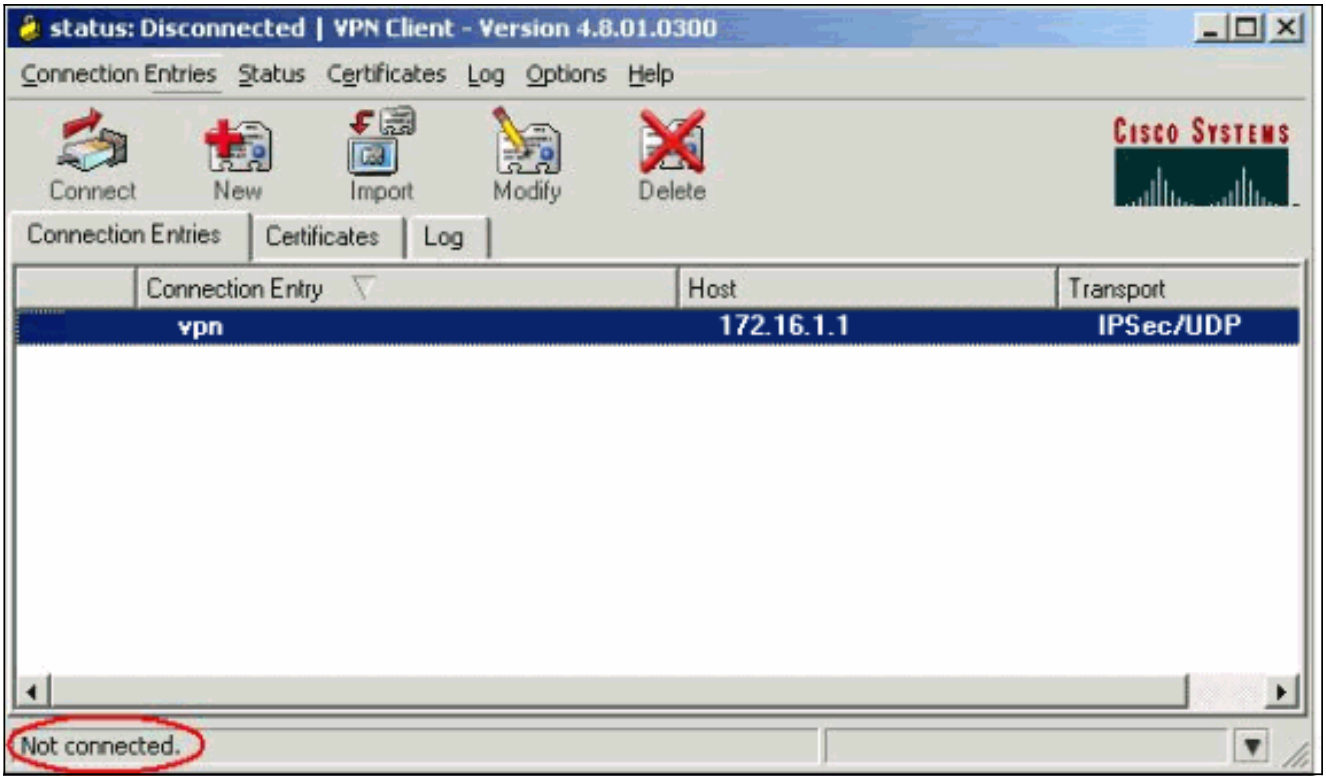
1. Choisissez le **début > les programmes > le client vpn de Cisco Systems > le client vpn**.
2. Cliquez sur New afin de lancer la nouvelle fenêtre d'entrée de connexion VPN de création.



3. Écrivez le nom de l'entrée de connexion avec une description, écrivez l'adresse IP extérieure du routeur dans la case d'hôte, et entrez le nom et le mot de passe de groupe VPN. Cliquez sur **Save**.



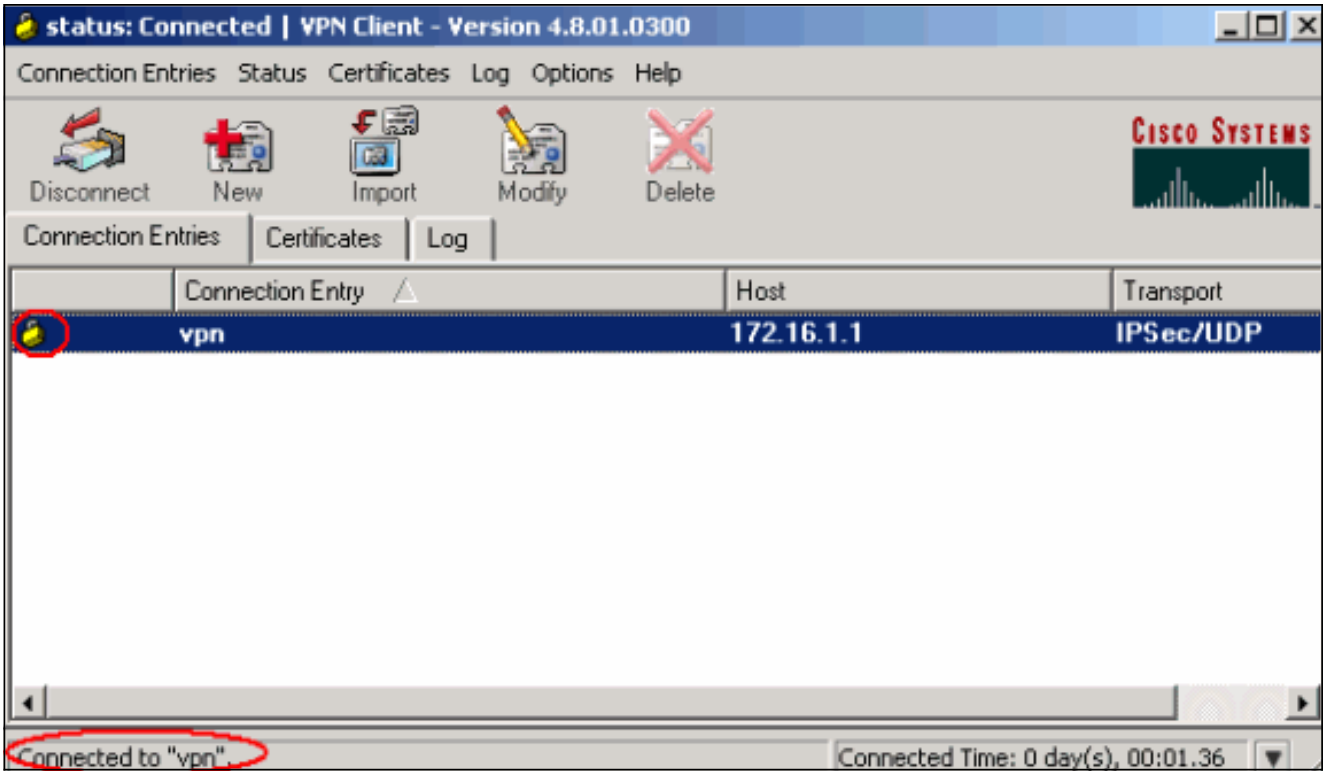
4. Cliquez sur la connexion que vous souhaitez utiliser et cliquez sur **Connect** dans la fenêtre principale du Client
VPN.



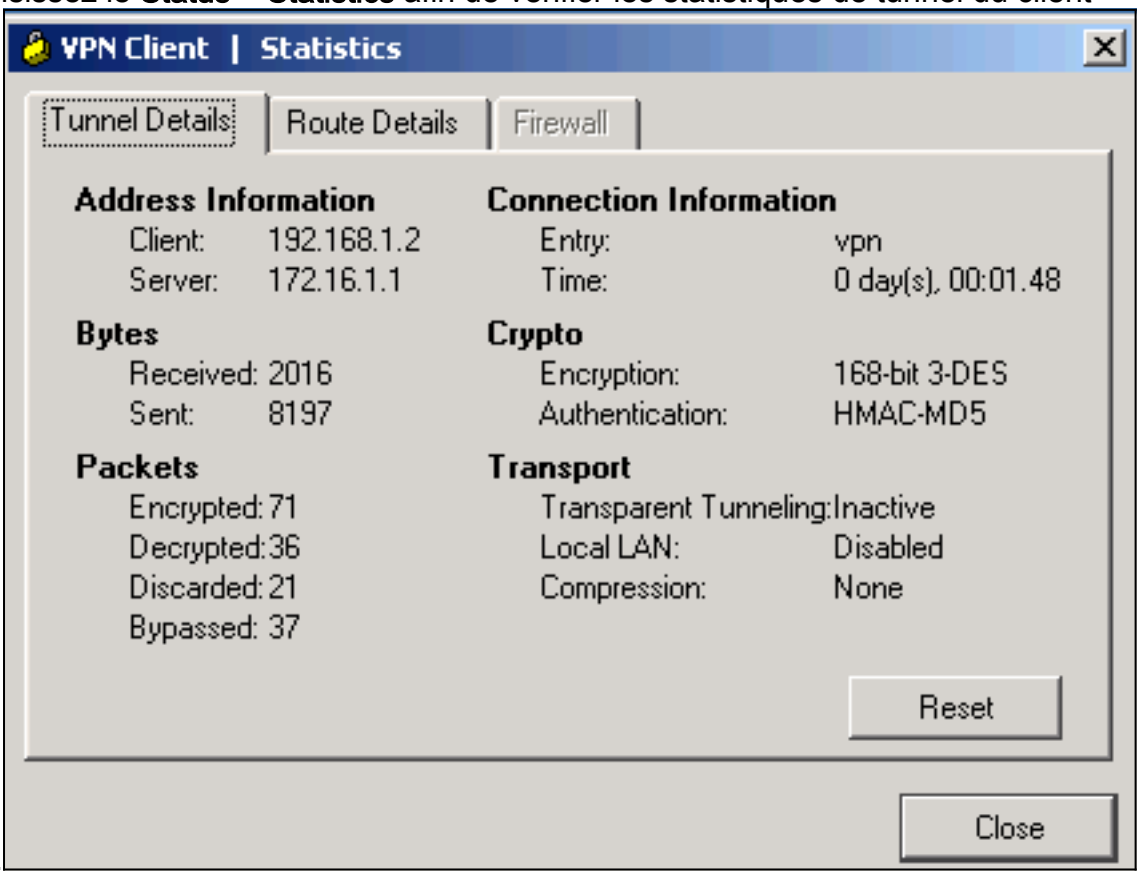
5. Une fois incité, écrivez les informations de nom d'utilisateur et mot de passe pour le Xauth et cliquez sur OK afin de se connecter au réseau distant.



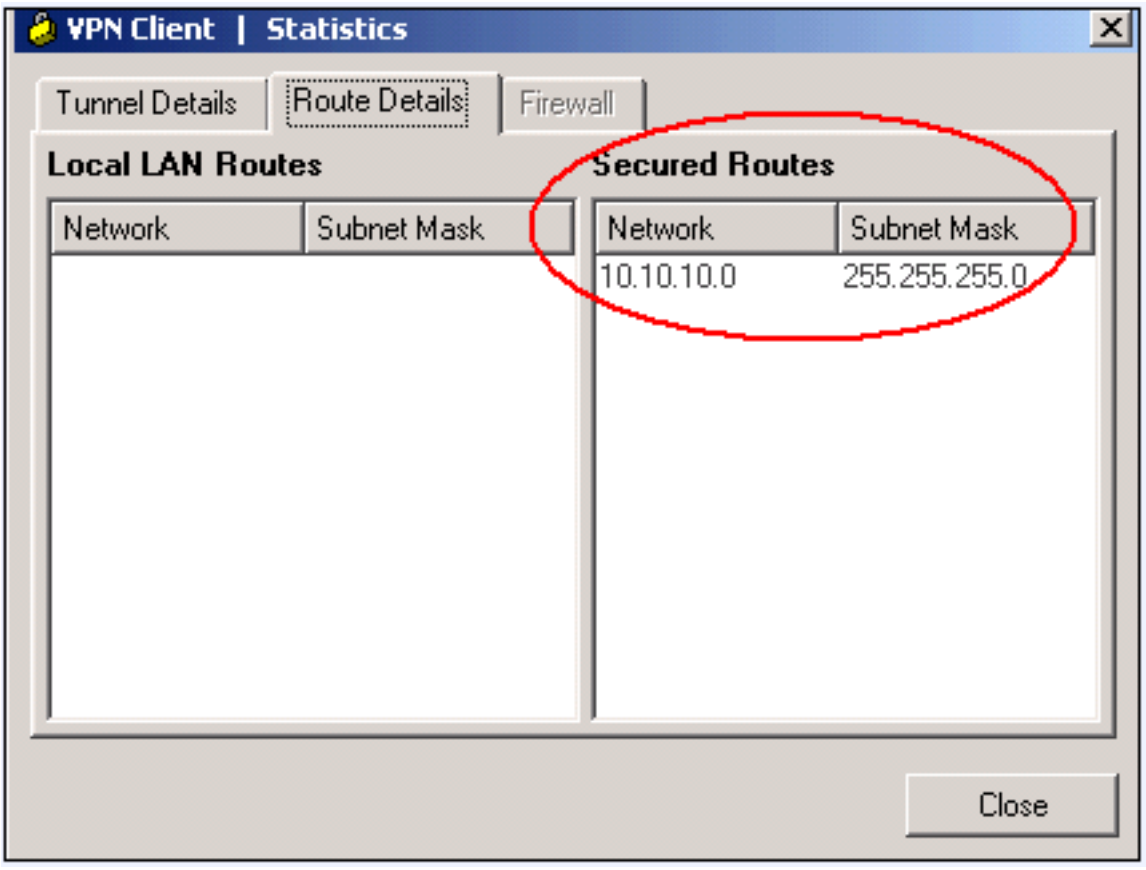
6. Le client vpn obtient lié au routeur au lieu d'exploitation principal.



7. Choisissez le **Status > Statistics** afin de vérifier les statistiques de tunnel du client vpn.



8. Allez aux détails d'artère l'onglet afin de voir les artères que le client vpn sécurise au routeur.Dans cet exemple, le client vpn sécurise l'accès à 10.10.10.0/24 alors que tout autre trafic n'est pas chiffré et n'est pas envoyé à travers le tunnel. Le réseau sécurisé est téléchargé de l'ACL 101 qui est configuré dans le routeur de lieu d'exploitation



principal.

Vérifiez

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 isakmp sa** — Affiche toutes les associations de sécurité actuelles IKE (SA) sur un homologue.`VPN#show crypto ipsec sa interface: FastEthernet1/0 Crypto map tag: clientmap, local addr 172.16.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer 10.0.0.2 port 500 PERMIT, flags={} #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270 #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0 current outbound spi: 0xEF7C20EA(4017889514) inbound esp sas: spi: 0x17E0CBEC(400608236) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: SW:1, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530341/3288) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xEF7C20EA(4017889514) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: SW:2, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530354/3287) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`
- **show crypto ipsec sa** — Affiche les paramètres utilisés par les SA en cours.`VPN#show crypto isakmp sa dst src state conn-id slot status 172.16.1.1 10.0.0.2 QM_IDLE 15 0 ACTIVE`

Dépannez

Dépannage des commandes

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** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec** — affiche les négociations IPsec de la Phase 2.
- **debug crypto isakmp** — affiche les négociations ISAKMP de la Phase 1.

Informations connexes

- Négociation IPSec/Protocoles IKE
- Client VPN Cisco - Support produit
- Support de produit pour routeur de Cisco
- Support et documentation techniques - Cisco Systems