Exemple de configuration d'un routeur et d'un client VPN pour l'Internet public sur un stick

Contenu

Introduction

Ce document décrit comment installer un routeur de lieu d'exploitation principal pour exécuter le trafic d'IPsec sur un bâton. Cette installation applique à un cas spécifique où le routeur, sans activer la Segmentation de tunnel, et les utilisateurs nomades (Client VPN Cisco) peuvent accéder à l'Internet par l'intermédiaire du routeur de lieu d'exploitation principal. Afin de réaliser ceci, configurez la carte de stratégie dans le routeur pour indiquer tout le trafic VPN (Client VPN Cisco) une interface de bouclage. Ceci permet au trafic Internet pour être adresse du port traduite (PATed) au monde extérieur.

Référez-vous à PIX/ASA 7.x et client vpn pour l'Internet public VPN sur un exemple de configuration de bâton afin de se terminer une configuration semblable sur un Pare-feu du lieu d'exploitation principal PIX.

Remarque: Afin d'éviter superposer des adresses IP dans le réseau, affectez le groupe entièrement différent d'adresses IP au client vpn (par exemple, 10.x.x.x, 172.16.x.x, 192.168.x.x). Ce schéma d'adressage IP vous aide à dépanner votre réseau.

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 de logiciel 12.4 de Cisco IOS®
- 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.

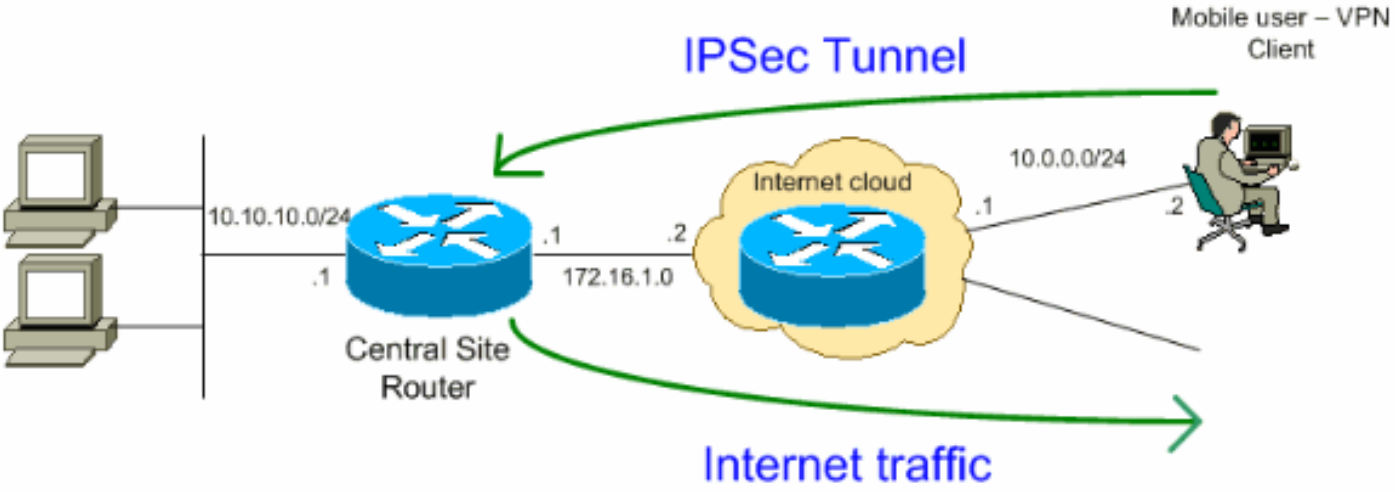
Configurez

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

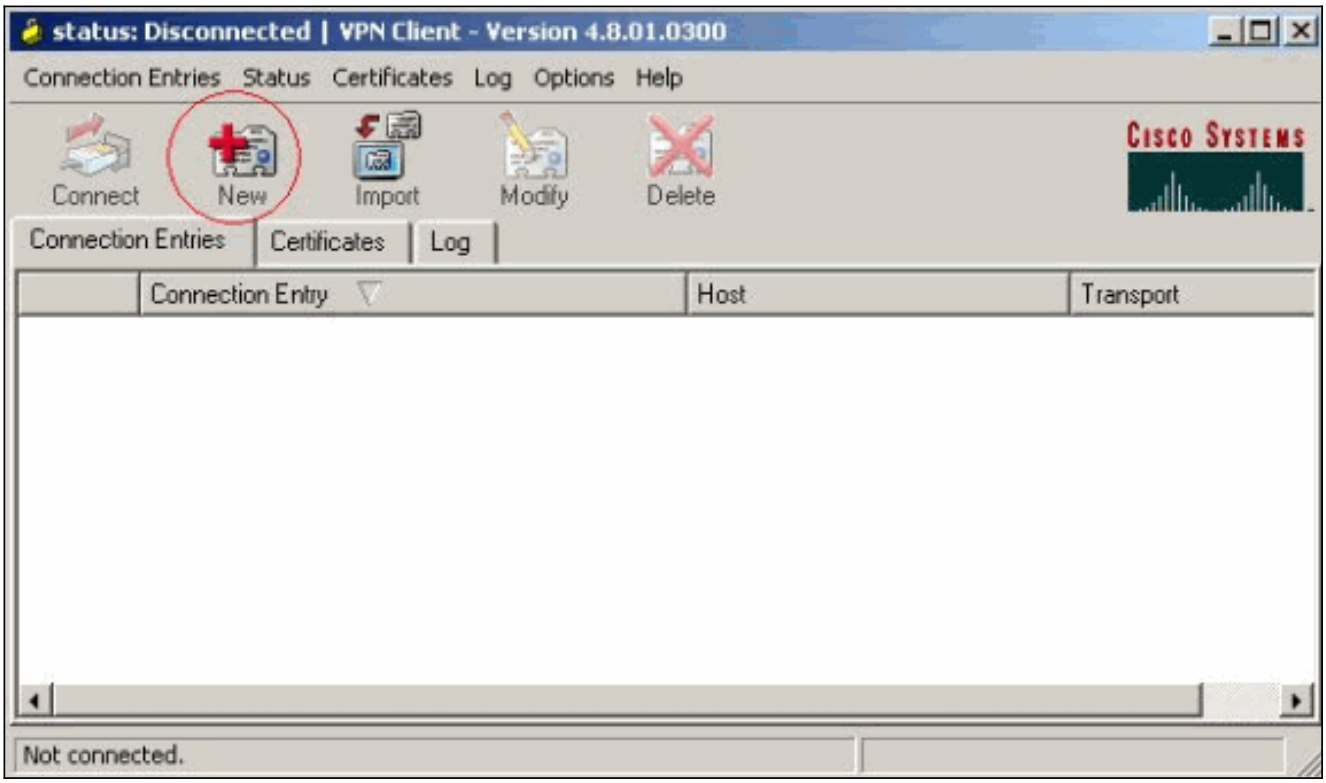
```
 VPN#show run Building configuration... Current
configuration : 2170 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
VPN ! boot-start-marker boot-end-marker ! ! !--- Enable
authentication, authorization and 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. crypto isakmp
client configuration group vpnclient key cisco123 dns
10.10.10.10 wins 10.10.10.20 domain cisco.com pool
ippool ! !--- 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 ! ! ! ! !--- Create the loopback
interface for the VPN user traffic . interface Loopback0
ip address 10.11.0.1 255.255.255.0 ip nat inside ip
virtual-reassembly ! interface Ethernet0/0 ip address
10.10.10.1 255.255.255.0 half-duplex ip nat inside !---
Apply the crypto map on the interface. interface
FastEthernet1/0 ip address 172.16.1.1 255.255.255.0 ip
nat outside ip virtual-reassembly ip policy route-map
VPN-Client 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 10.0.0.0 255.255.255.0
172.16.1.2 !--- Enables Network Address Translation
(NAT) !--- of the inside source address that matches
access list 101 !--- and gets PATed with the
FastEthernet IP address. ip nat inside source list 101
interface FastEthernet1/0 overload ! !--- The access
list is used to specify which traffic is to be
```

```
translated for the !--- outside Internet. access-list
101 permit ip any any !--- Interesting traffic used for
policy route. access-list 144 permit ip 192.168.1.0
0.0.0.255 any !--- Configures the route map to match the
interesting traffic (access list 144) !--- and routes
the traffic to next hop address 10.11.0.2. ! route-map
VPN-Client permit 10 match ip address 144 set ip next-
hop 10.11.0.2 ! ! control-plane ! line con 0 line aux 0
line vty 0 4 ! end
```

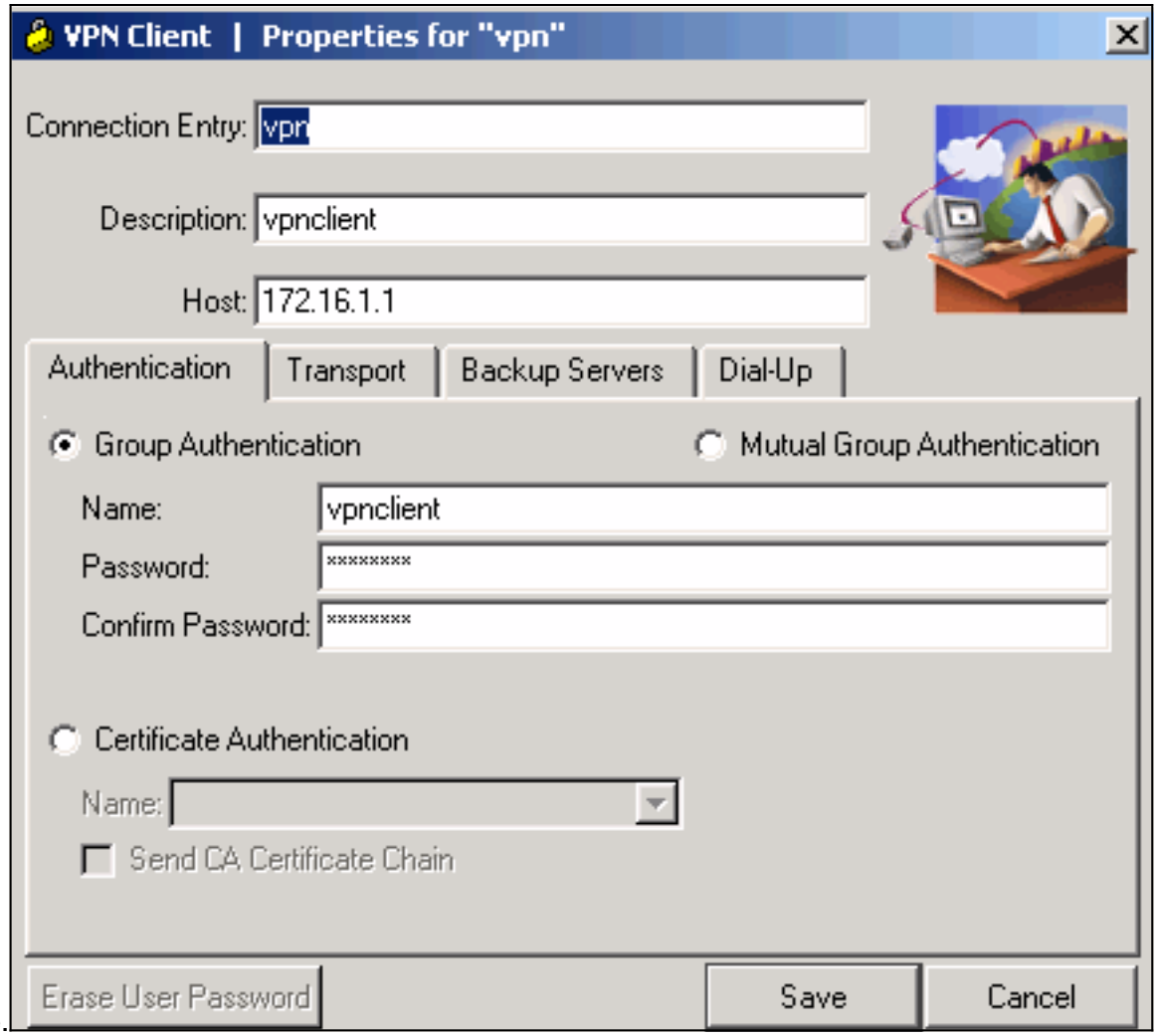
Configuration VPN Client 4.8

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.

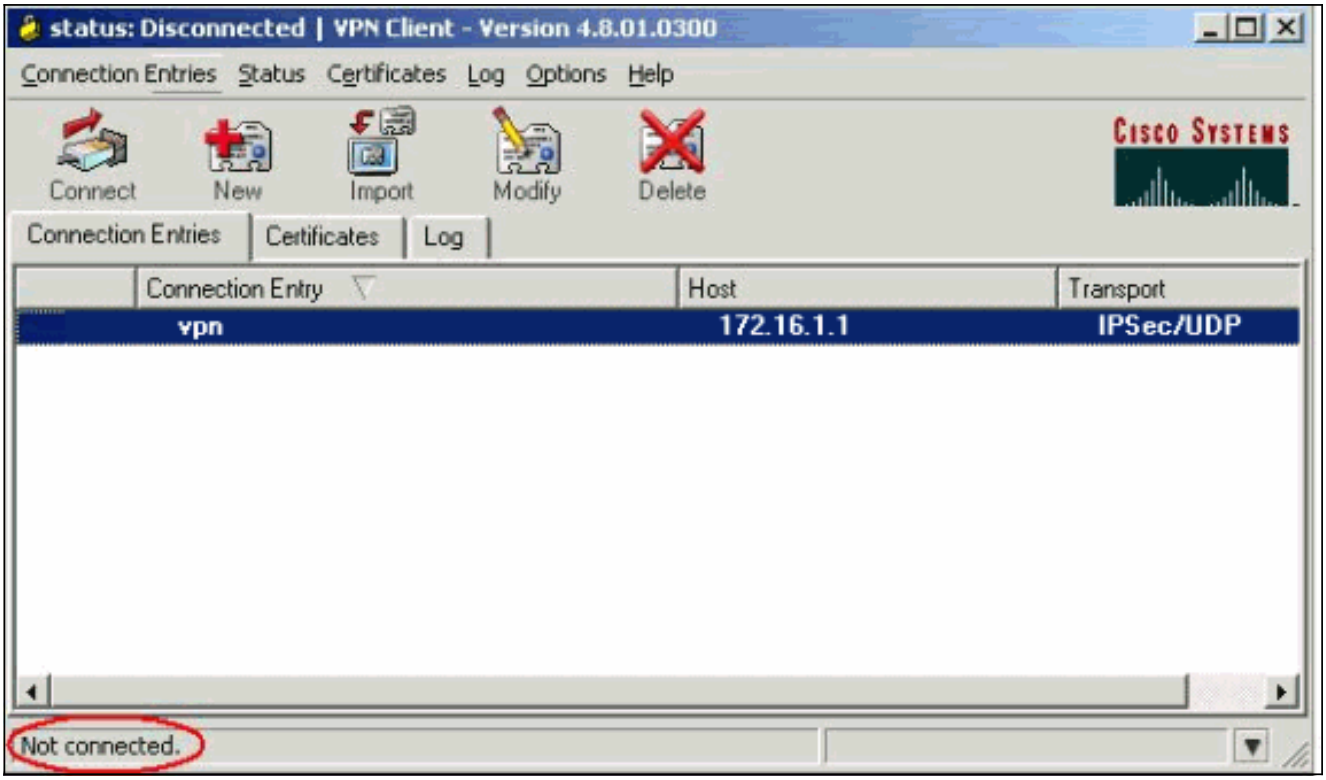


3. Écrivez le nom de l'entrée de connexion avec une description, écrivez l'adresse IP extérieure du routeur dans la case d'hôte, et entrez le nom et le mot de passe de groupe VPN. Cliquez



sur **Save**.

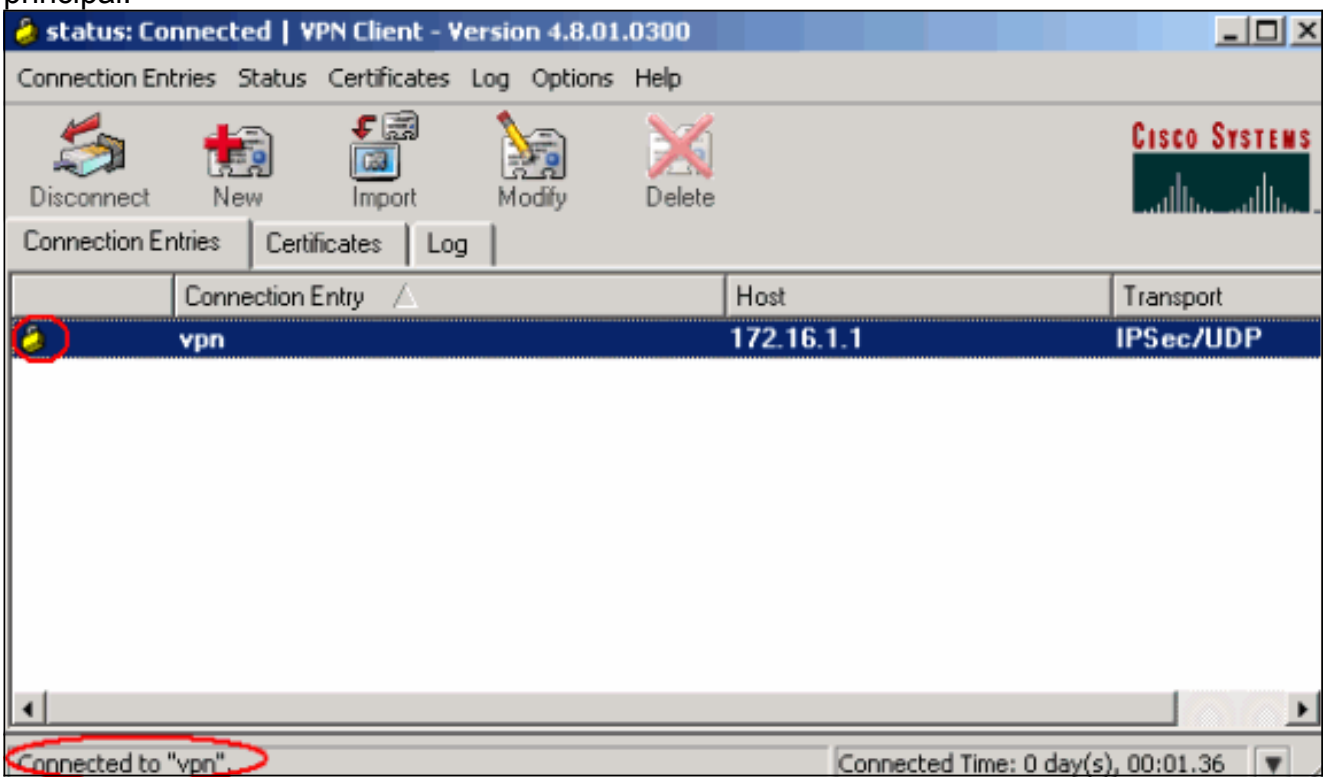
4. Cliquez sur la connexion que vous souhaitez utiliser et cliquez sur **Connect** dans la fenêtre principale du Client
VPN.



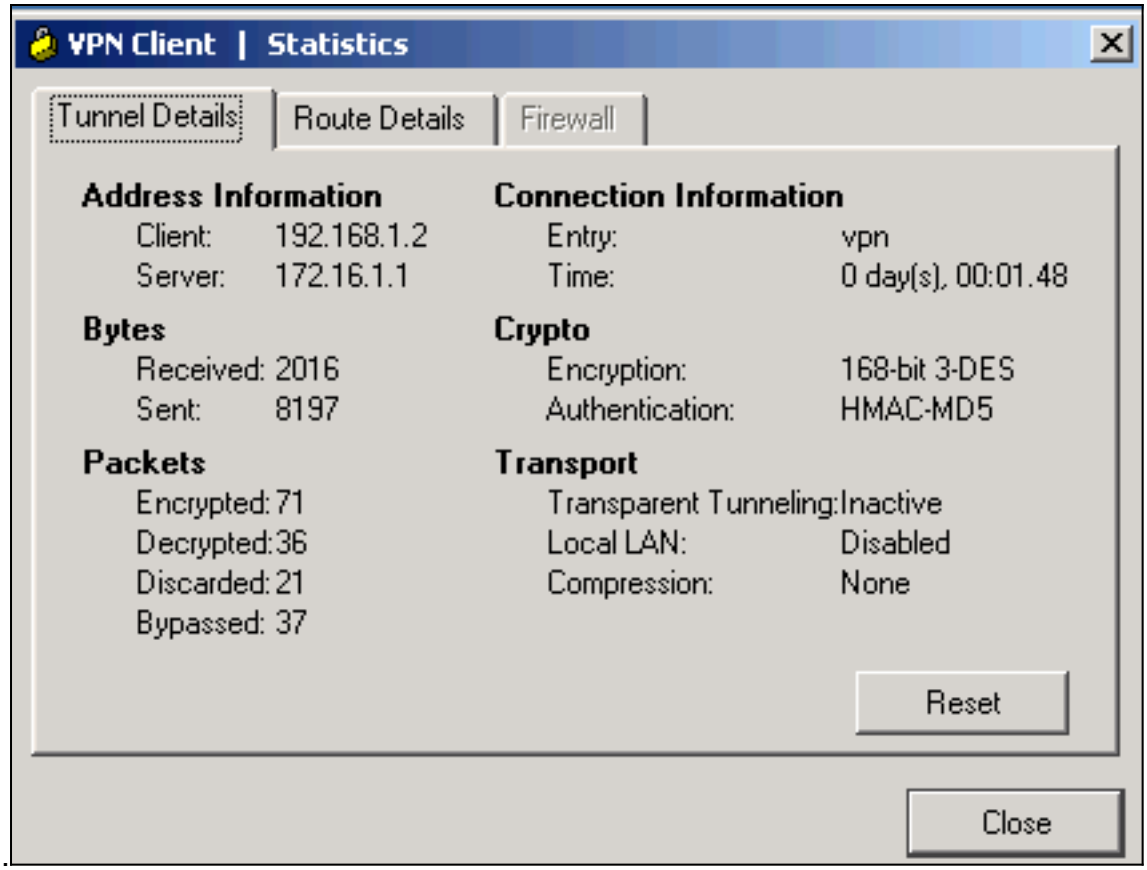
5. Une fois incité, écrivez les informations de nom d'utilisateur et mot de passe pour le Xauth et cliquez sur OK afin de se connecter au réseau

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.

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