スプリット トンネリングを使用する VPN クライアントが IPSec とインターネットに接続するのをルータで許可する設定例

目次

概要

このドキュメントでは、VPN Client が Cisco IOS® ルータにトンネリングされている間に、VPN Client にインターネットへのアクセスを許可する方法の段階的な手順について説明します。 この設定は、VPN Client に対して IPsec 経由での社内のリソースへの安全なアクセスを許可し、それと同時にインターネットへの非セキュアなアクセスを許可するために必要になります。 この設定をスプリット トンネリングと呼びます。

注: スプリット トンネリングの設定にはセキュリティ上のリスクが伴います。 VPN Client がセキュリティ保護されない状態でインターネットにアクセスするため、攻撃者による危険にさらされる可能性があります。 このような攻撃者は、その後、IPsec トンネルを経由して企業 LAN にアクセスできるようになります。 フル トンネリングとスプリット トンネリングの折衷案として、VPN Client にローカル LAN アクセスだけを許可することができます。 ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x： VPN クライアントでローカル LAN アクセスを許可するための設定例』を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.4 が稼動する Cisco 3640 ルータ
- Cisco VPN Client 4.8

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

リモート アクセス VPN は、モバイル ユーザからの要求を処理し、組織のネットワークに安全に接続できるようにします。 モバイル ユーザは、自身の PC にインストールした VPN Client ソフトウェアを使用して、安全な接続を確立できます。 VPN Client は、これらの要求を受け入れるよう設定されている中央サイトのデバイスへの接続を開始します。 この例で使用する中央サイトのデバイスは、ダイナミック クリプト マップを使用する Cisco IOS ルータです。

VPN 接続用にスプリット トンネリングをイネーブルにすると、ルータ上で Access Control List（ACL;アクセス コントロール リスト）の設定が必要になります。 この例では、**access-list 101** コマンドがスプリット トンネリング用のグループに関連付けられており、トンネルは 10.10.10.x/24 ネットワークに対して形成されます。 デバイスへの暗号化されていないトラフィック フロー（インターネットなど）は、ACL 101 で設定されるネットワークからは除外されます。

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

グループ プロパティで ACL を適用します。

```
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
```

この設定例では、IPSec トンネルの設定に次の要素が含まれています。

- PIX の Outside インターフェイスに適用されるクリプト マップ
- ローカル認証に対する VPN Client の拡張認証（Xauth）
- プールから VPN Client へのプライベート IP アドレスのダイナミック割り当て
- nat 0 access-list コマンドの機能により、 LAN 上のホストは、リモート ユーザに対してプライベート IP アドレスを使用し、信頼されていないネットワークにアクセスするときに PIX から Network Address Translation（NAT）アドレスを取得できます。

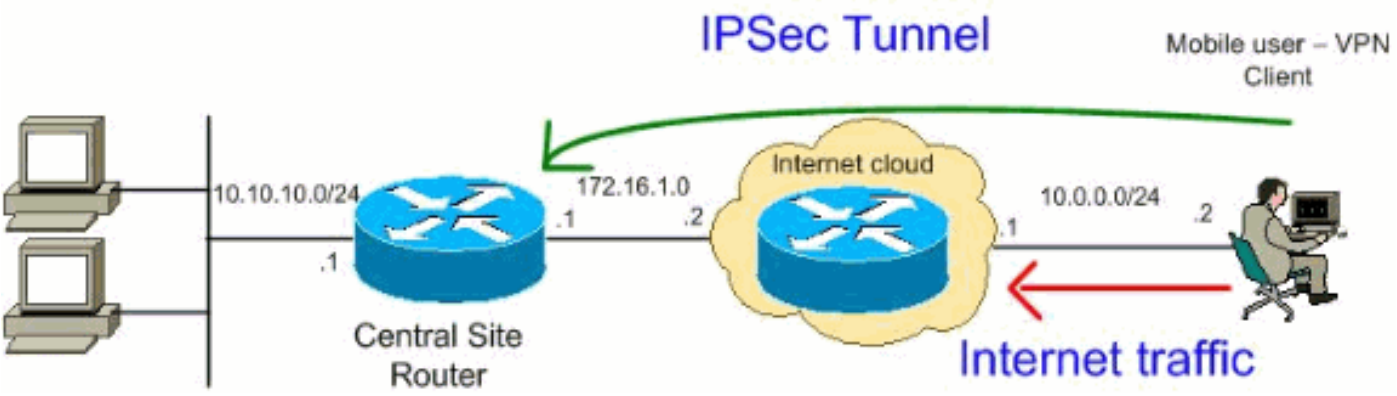
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは、ラボ環境で使用された RFC 1918 のアドレスです。

設定

このドキュメントでは、次の設定を使用します。

- ルータ
- Cisco VPN Client

ルータ

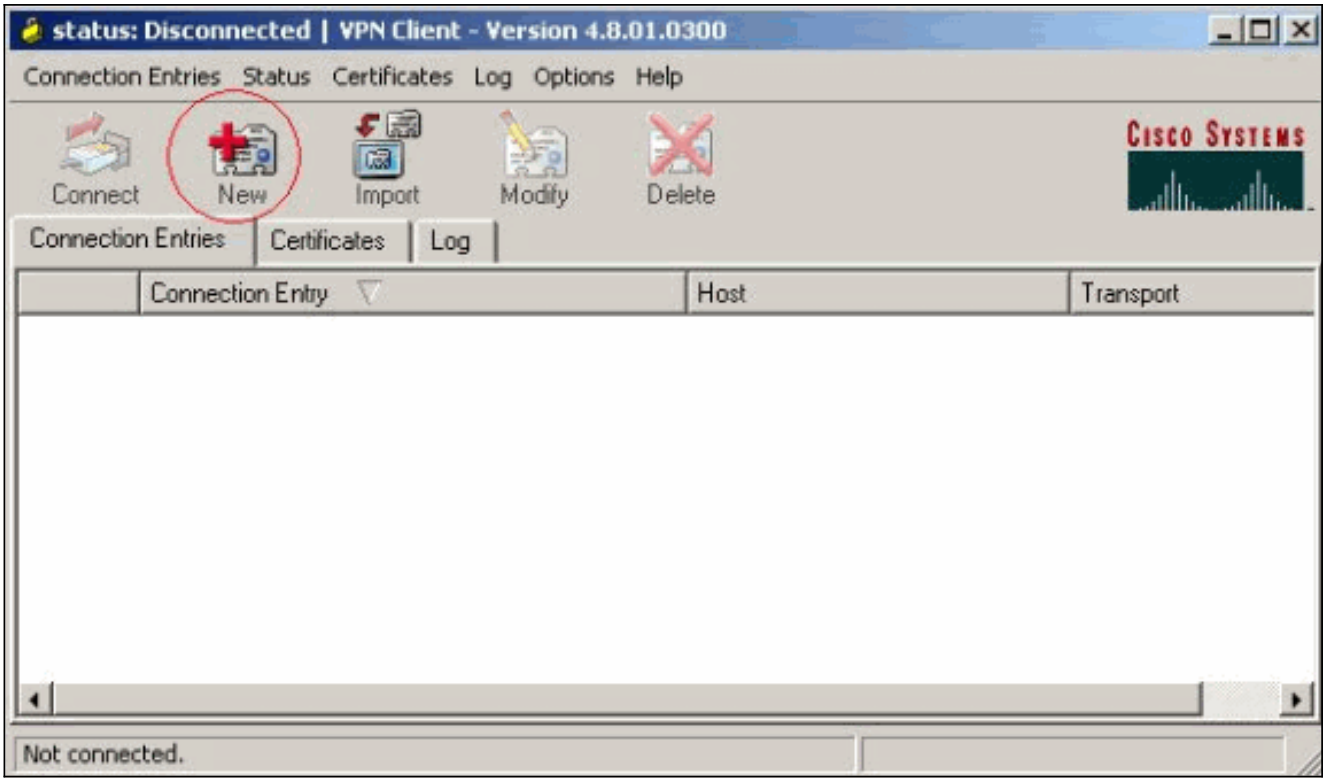
```
VPN#show run Building configuration... Current
configuration : 2170 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
VPN ! boot-start-marker boot-end-marker ! ! !--- Enable
authentication, authorization and 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
```

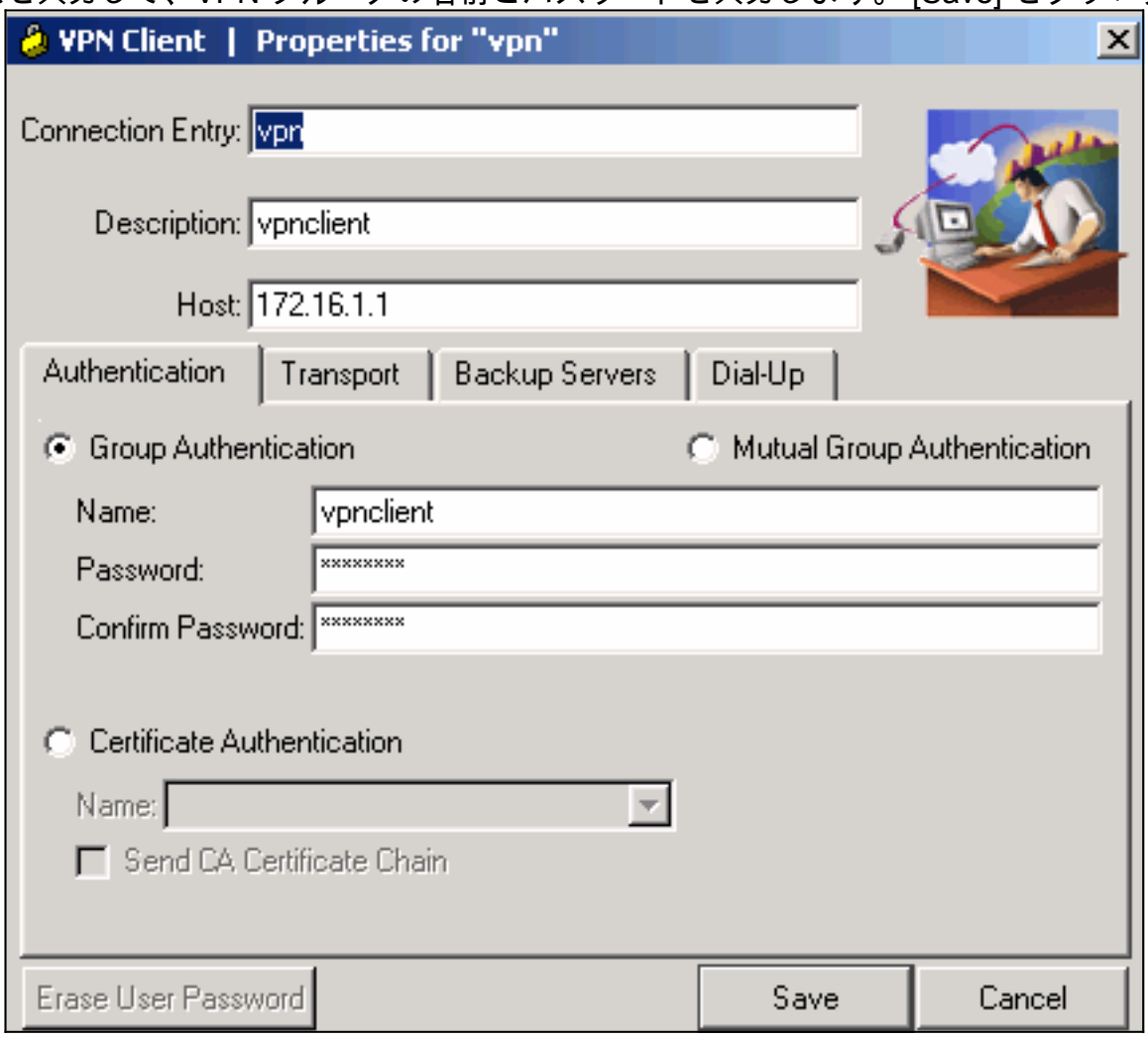
VPN Client 4.8 の設定

VPN Client 4.8 を設定するには、次の手順を実行します。

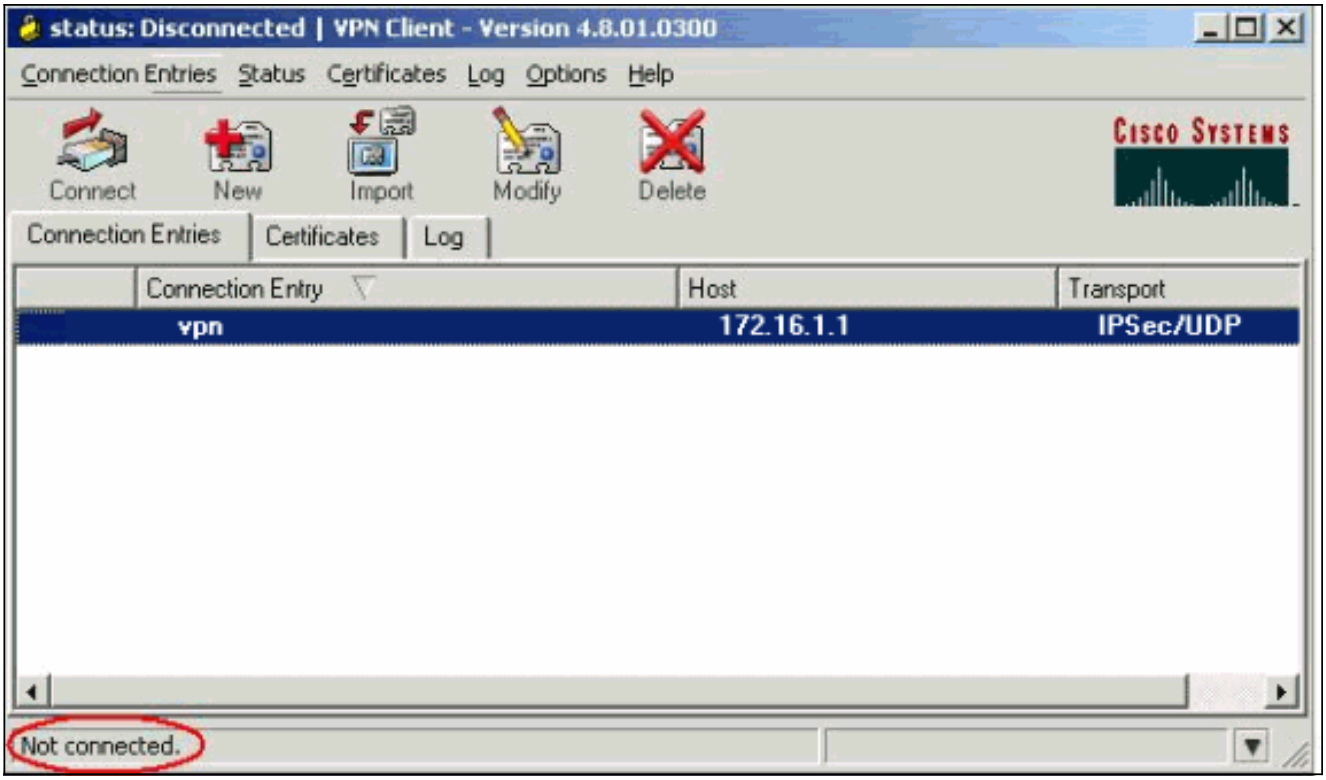
1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択します。
2. [New] をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。



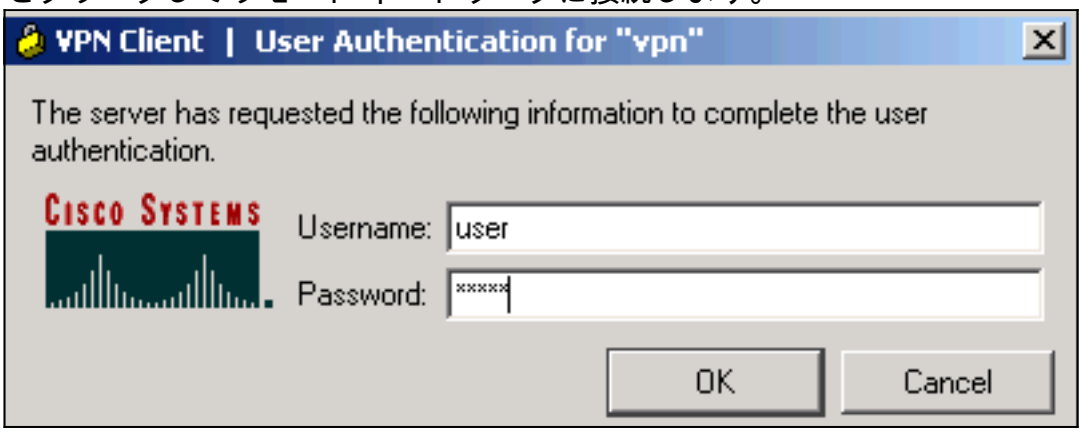
3. 説明と一緒に Connection Entry の名前を入力し、[Host] ボックスにルータの Outside IP アドレスを入力して、VPN グループの名前とパスワードを入力します。 [Save] をクリックします。



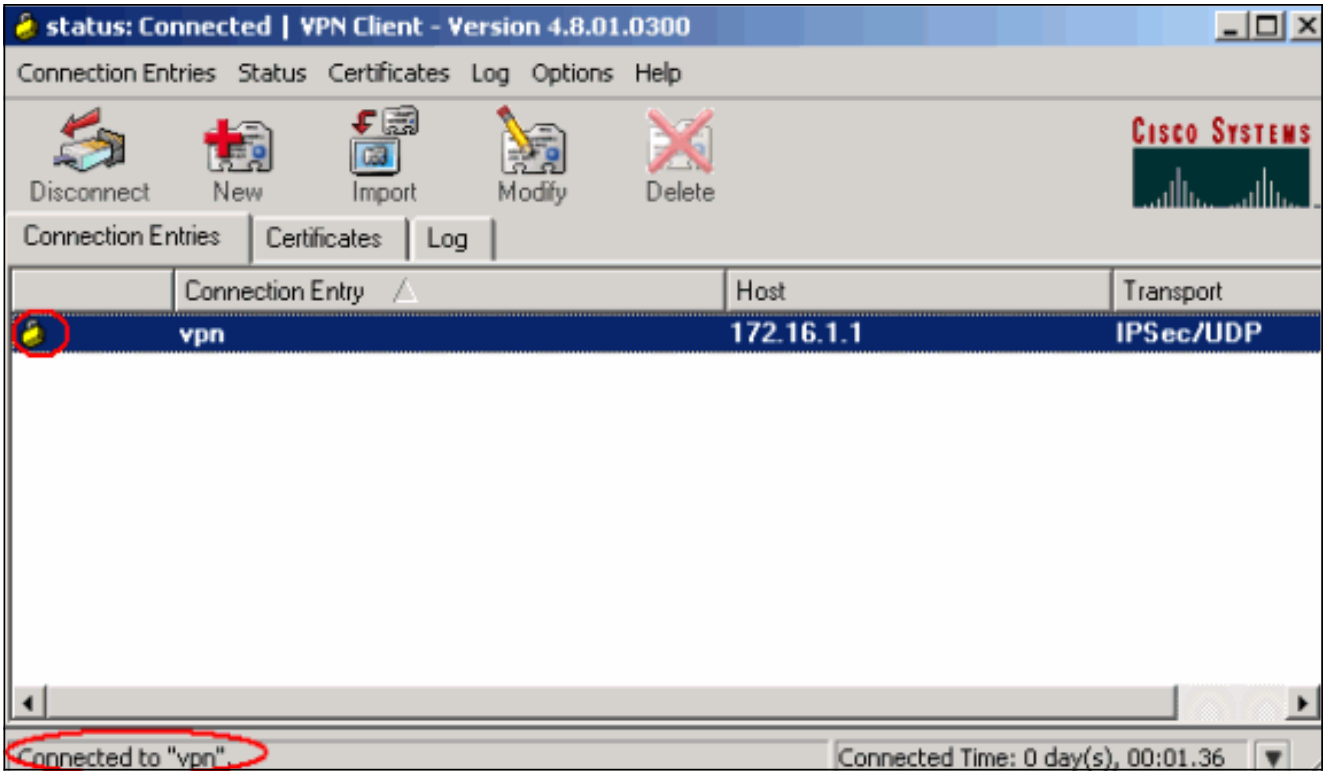
4. 使用する接続をクリックし、VPN Client のメイン ウィンドウから [Connect] をクリックします。



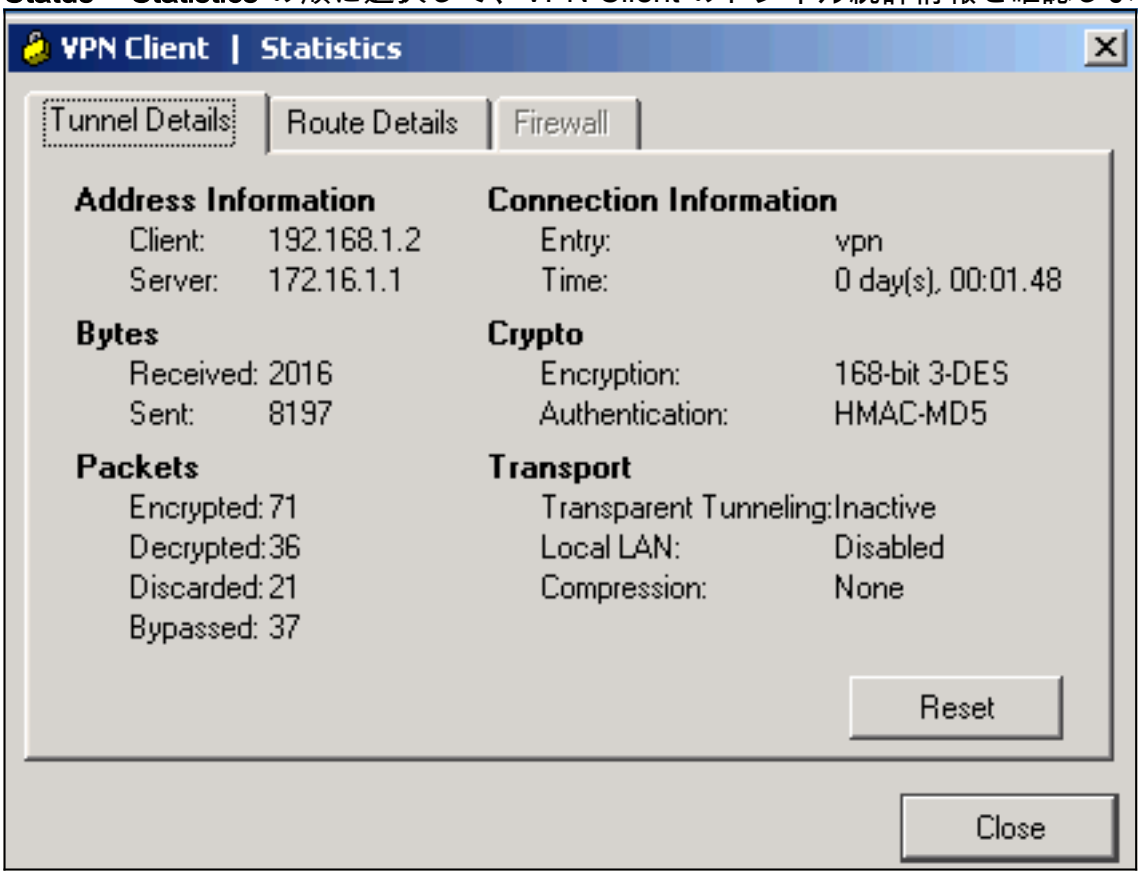
5. ダイアログ ボックスが表示されたら、Xauth のユーザ名とパスワード情報を入力し、[OK] をクリックしてリモート ネットワークに接続します。



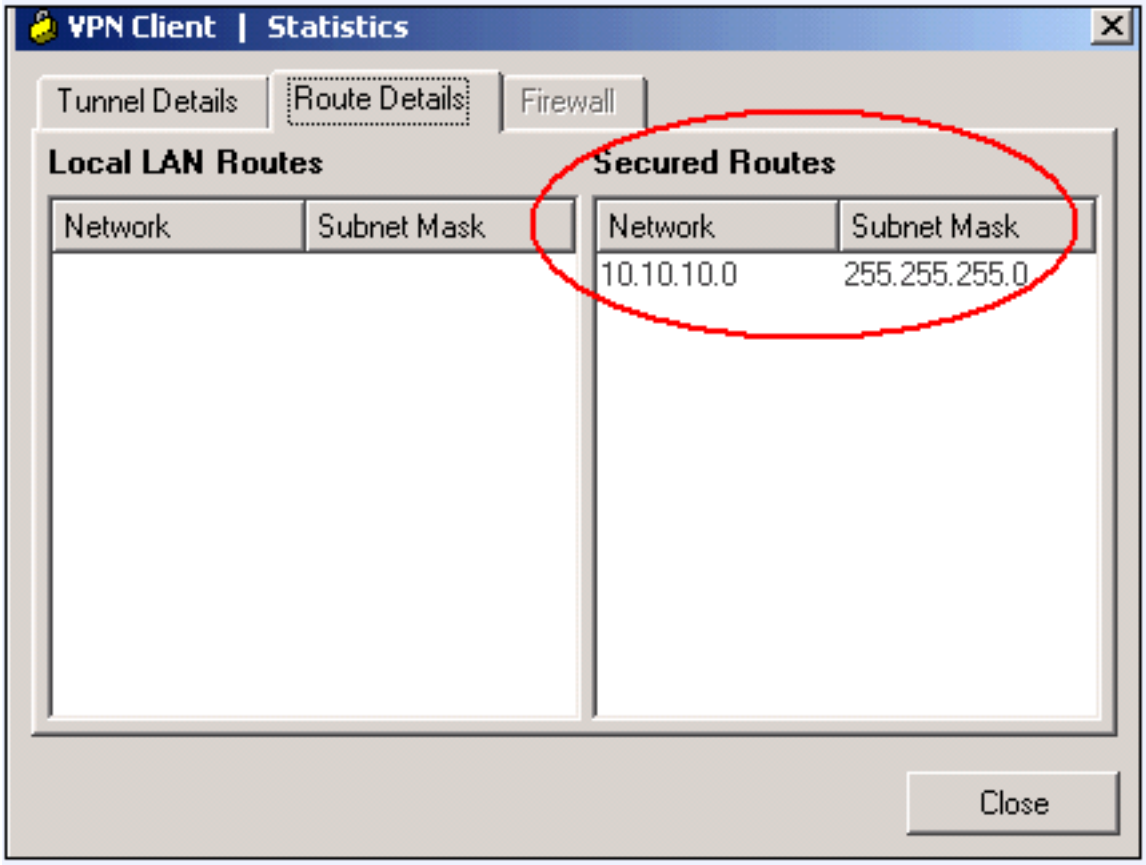
6. VPN Client が中央サイトのルータに接続されます。



7. Status > Statistics の順に選択して、VPN Client のトンネル統計情報を確認します。



8. [Route Details] タブに移動し、VPN Client がルータへの安全を保護するルートを確認します。この例では、VPN Client は 10.10.10.0/24 へのアクセスを保護しますが、一方で、他のすべてのトラフィックは暗号化されず、トンネルを経由しては送信されません。 保護されたネットワークは、中央サイトのルータで設定された ACL 101 からダウンロードされます。



確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto isakmp sa**：ピアの現在の IKE セキュリティ アソシエーション（SA）すべてを表示します。`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**：現在の SA が使用している設定を表示します。`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`

トラブルシューティング

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto ipsec**：フェーズ 2 の IPSec ネゴシエーションを表示します。
- **debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。

関連情報

- IPSec ネゴシエーション/IKE プロトコル
- Cisco VPN Client：製品に関するサポート ページ
- Cisco ルータ：製品に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems