VPN 3000 コンセントレータでの VPN クライアントのスプリット トンネリング設定例

内容

概要

このドキュメントでは、VPN Client が VPN 3000 シリーズ コンセントレータにトンネリングされている間に、それ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。この設定により、VPN Client は IPSec を使用した企業リソースへのセキュアなアクセスと、セキュリティ保護されていないインターネット アクセスの両方を実現できます。

注：スプリットトンネリングを設定すると、セキュリティ上のリスクが生じる可能性があります。VPN クライアントに許可されるため、攻撃者がクライアントに侵入する可能性があります。IPsec トンネル経由で企業 LAN にアクセスできるようになる可能性があります。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。詳細については、『VPN 3000 コンセントレータで VPN Client のローカル LAN アクセスを許可する設定例』を参照してください。

前提条件

要件

このドキュメントでは、VPN コンセントレータでリモート アクセス VPN 設定がすでに存在していることを前提としています。まだ設定していない場合は、『VPN 3000 コンセントレータに接続する VPN Client での IPsec 設定例』を参照してください。

使用するコンポーネント

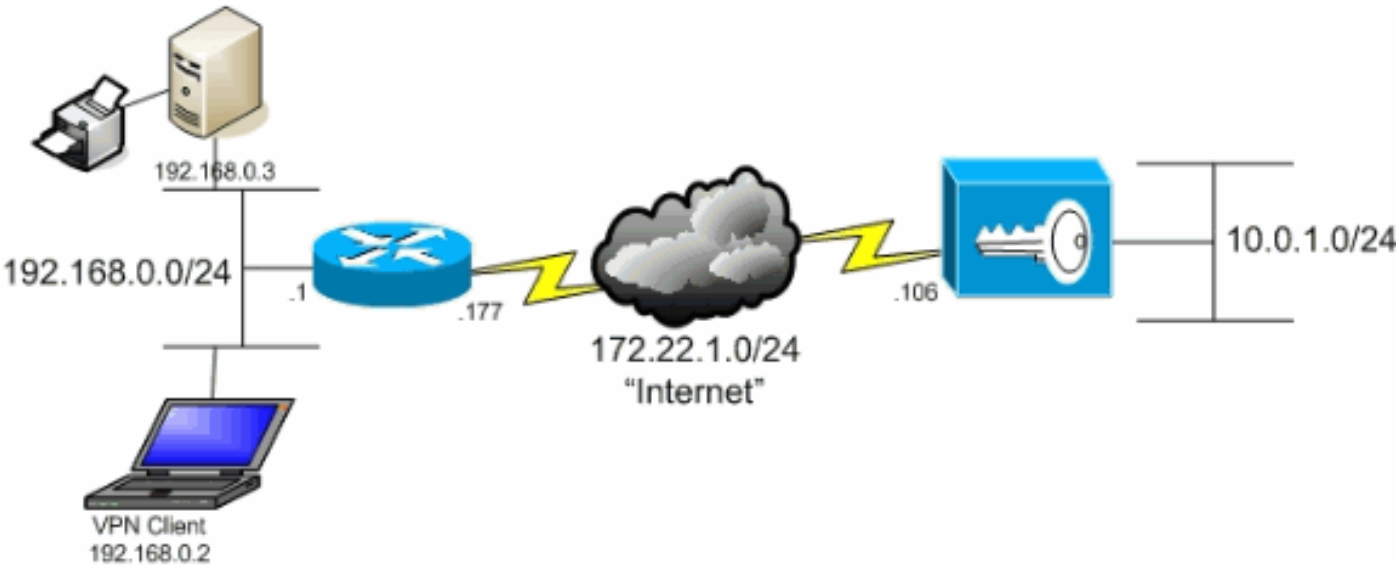
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco VPN 3000 コンセントレータ シリーズ ソフトウェア バージョン 4.7.2.H
- Cisco VPN Client バージョン 4.0.5

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

VPN Client は一般的な SOHO ネットワーク上にあり、インターネット経由で本社に接続しています。



表記法

ドキュメント表記の詳細については、『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

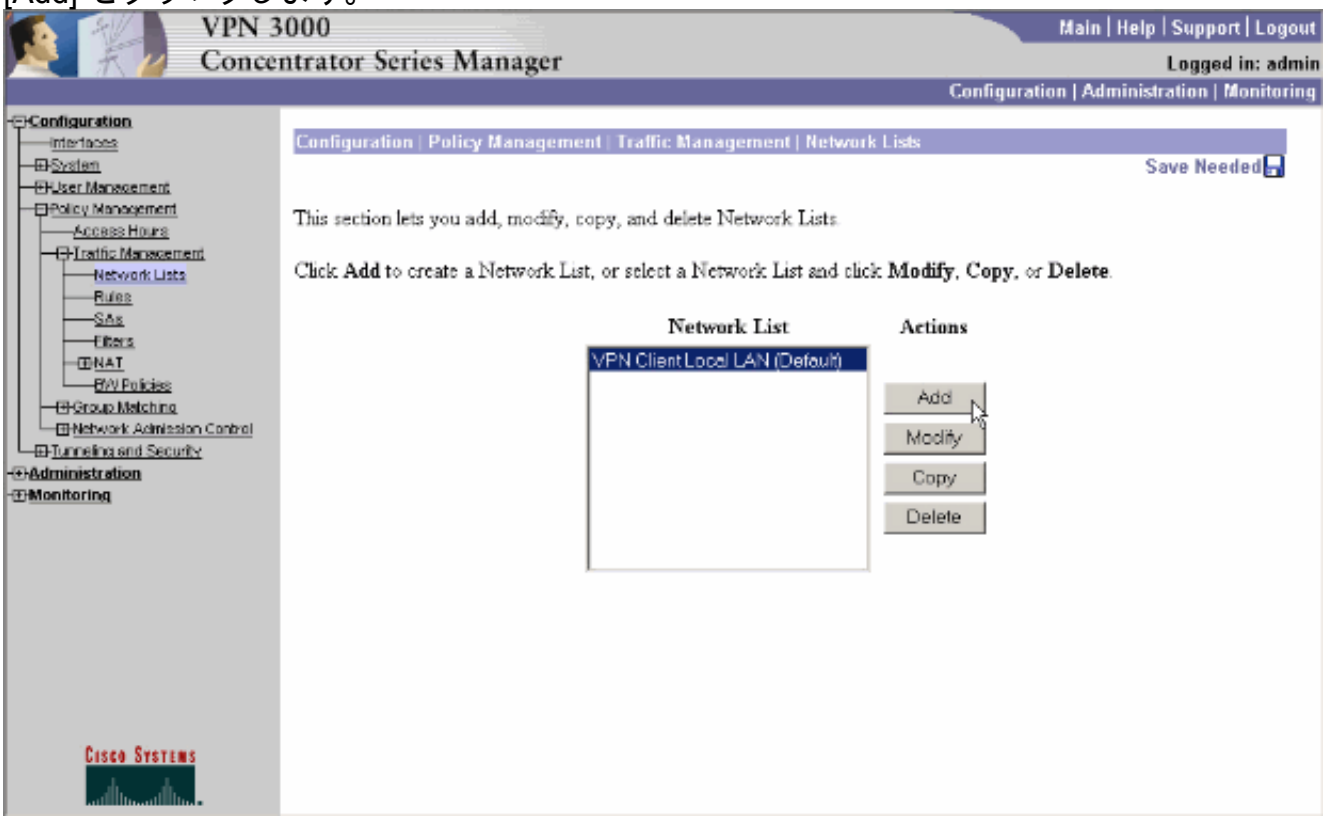
VPN Client と VPN コンセントレータの基本的な接続シナリオでは、宛先に関係なく、VPN Client からのすべてのトラフィックは暗号化されて VPN コンセントレータに送信されます。企業の構成とサポートしているユーザ数によっては、このような設定は帯域幅を多く消費します。スプリット トンネリングでは、トンネル接続で、企業ネットワーク向けトラフィックの送信だけがユーザに許可されるため、この問題の軽減に役立ちます。IM、電子メール、または通常の Web 閲覧など、その他すべてのトラフィックは、VPN Client のローカル LAN 経由でインターネットに送出されます。

VPN コンセントレータでのスプリット トンネリングの設定

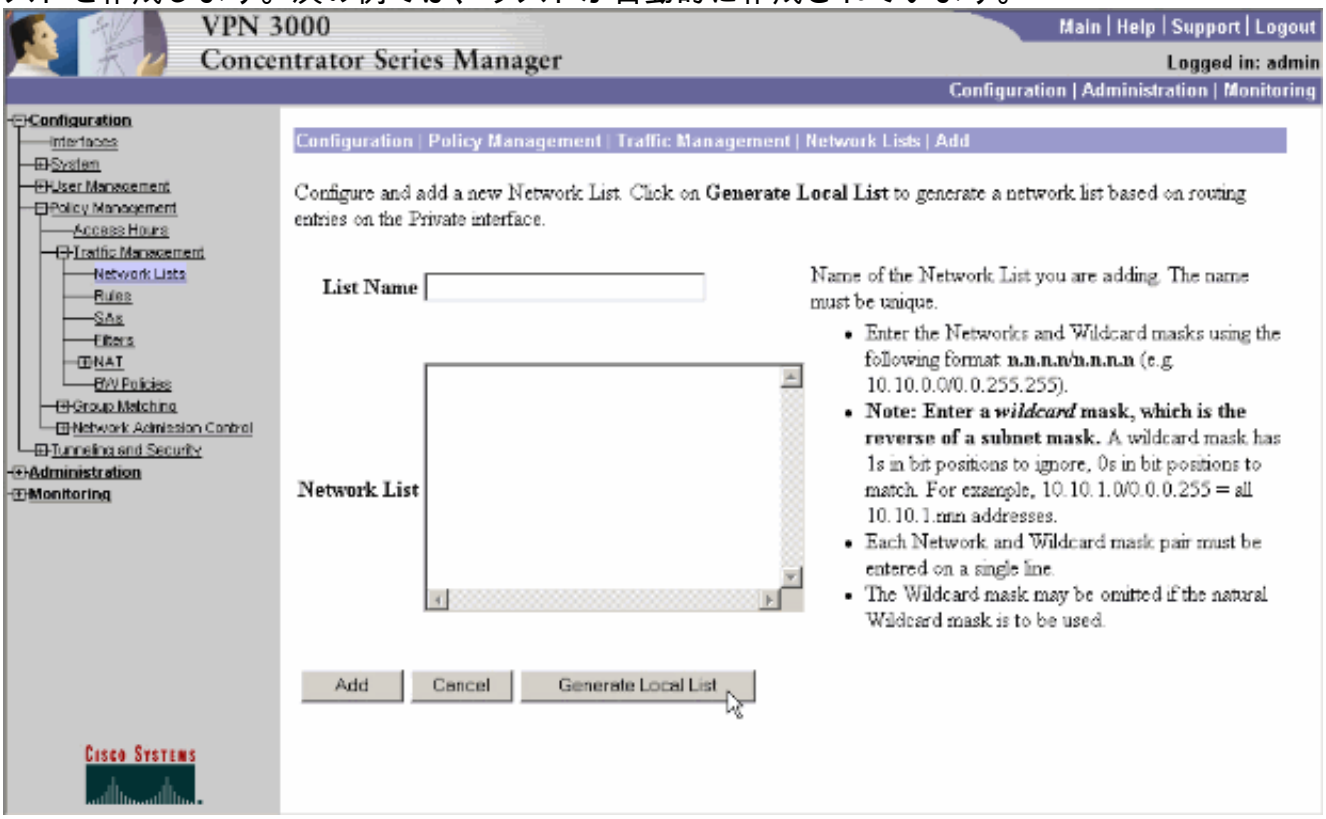
次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループを設定します。最初にネットワーク リストを作成します。このリストは、VPN Client が暗号化トラフィックを送信する宛先ネットワークを定義します。リストが作成されたら、このリストをク

ライアント トンネル グループのスプリット トンネリング ポリシーに追加します。

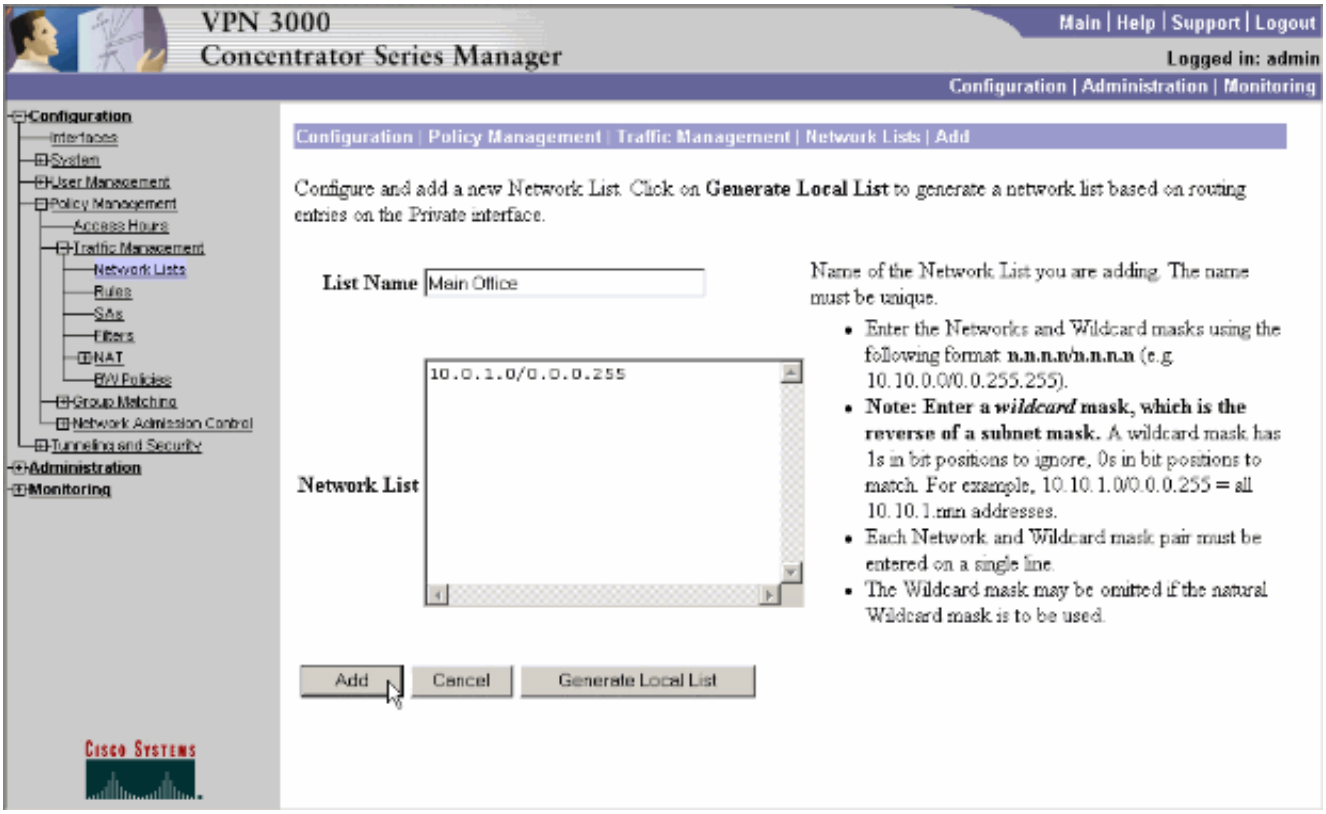
1. [Configuration] > [Policy Management] > [Traffic Management] > [Network Lists] を選択し、[Add] をクリックします。



2. このリストは、VPN Client が暗号化トラフィックを送信する宛先ネットワークを定義します。これらのネットワークを手動で入力するか、[Generate Local List] をクリックして、VPN コンセントレータのプライベート インターフェイスのルーティング エントリに基づいてリストを作成します。次の例では、リストが自動的に作成されています。

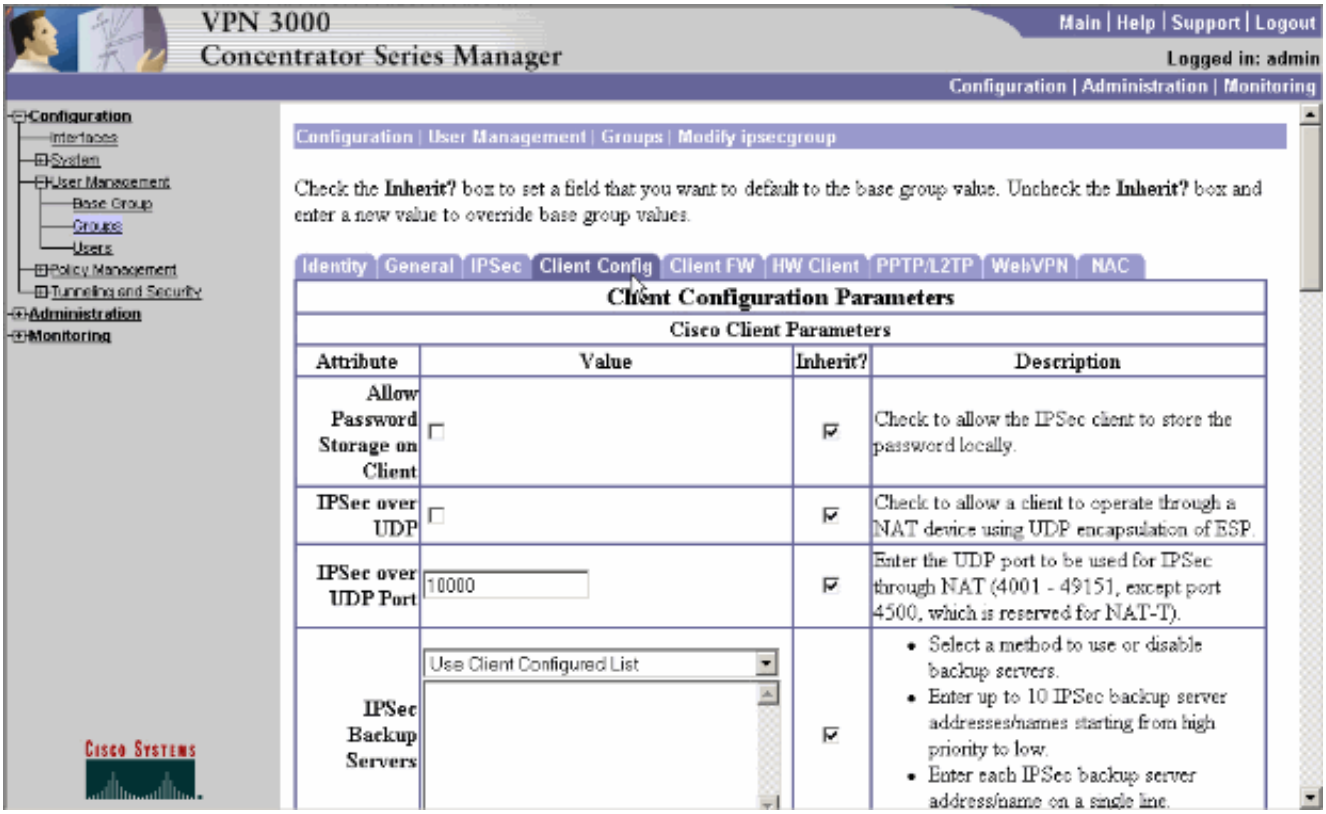


3. 作成され、データが取り込まれたリストに名前を指定し、[Add] をクリックします。

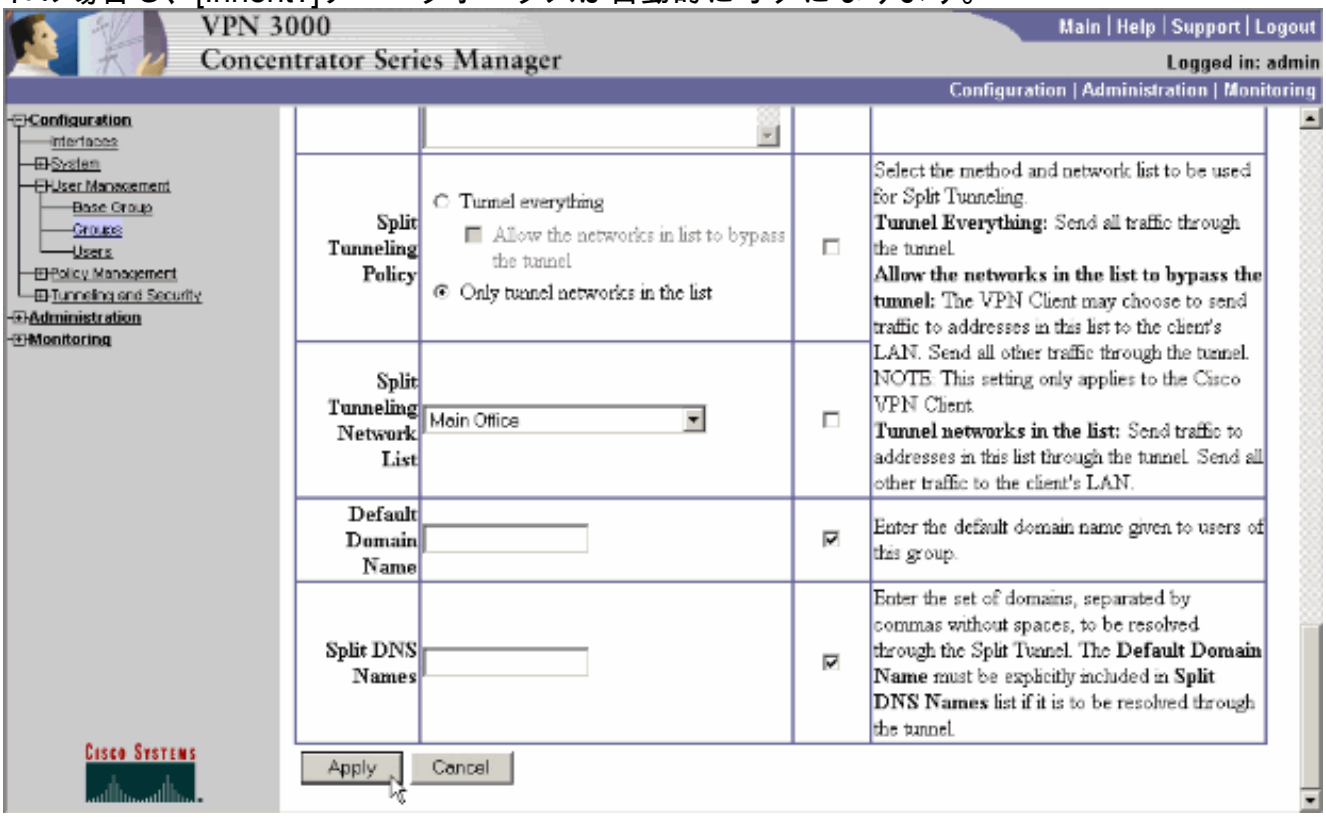


4. 作成したネットワーク リストをトンネル グループに割り当てます。[Configuration] > [User Management] > [Groups] を選択し、変更するグループを選択して、[Modify Group] をクリックします。

5. 変更するように選択したグループの [Client Config] タブに移動します。



6. [Split Tunneling Policy] および [Split Tunneling Network List] セクションにスクロールし、[Only tunnel networks in the list] をクリックします。
7. 前に作成したリストをドロップダウンから選択します。この場合は [Main Office] です。いずれの場合も、[Inherit?]チェックボックスは自動的にオフになります。



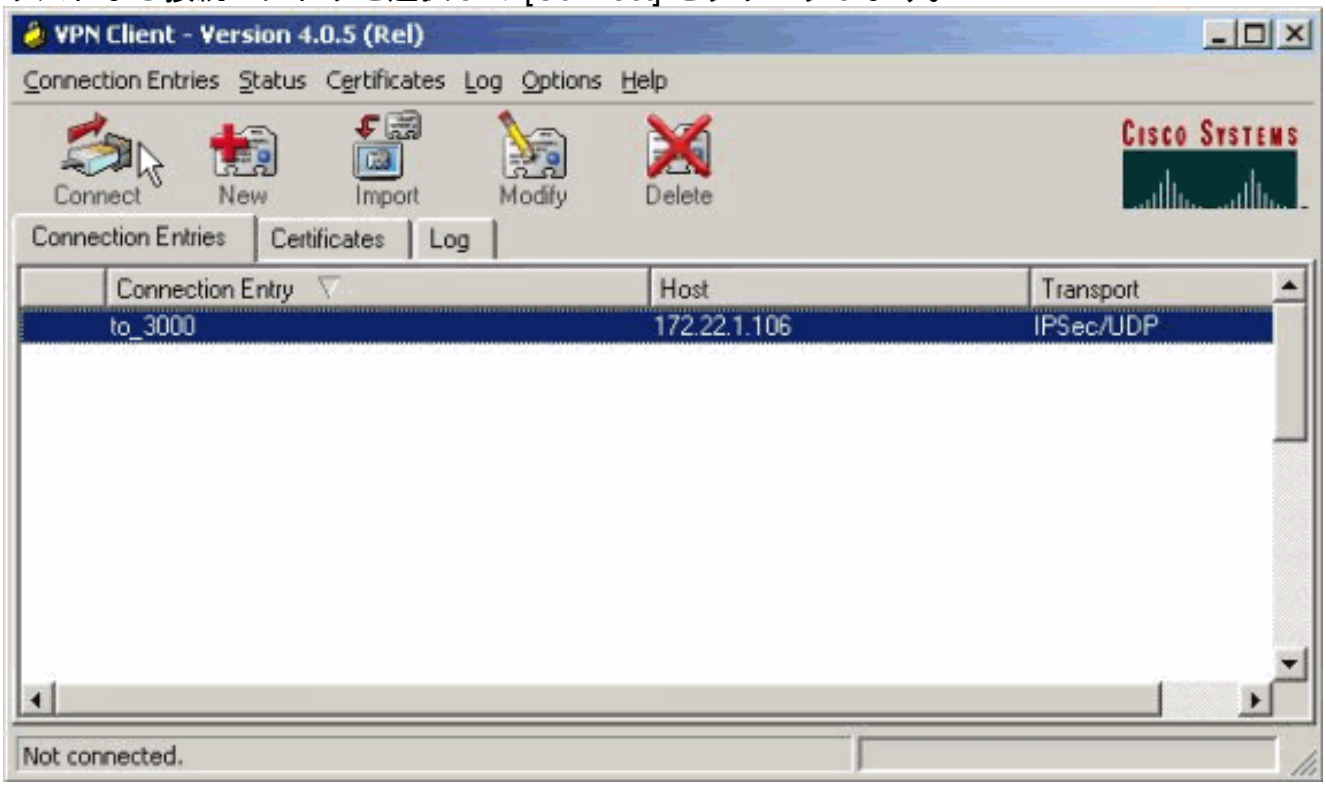
8. 設定が終了したら、[Apply] をクリックします。

確認

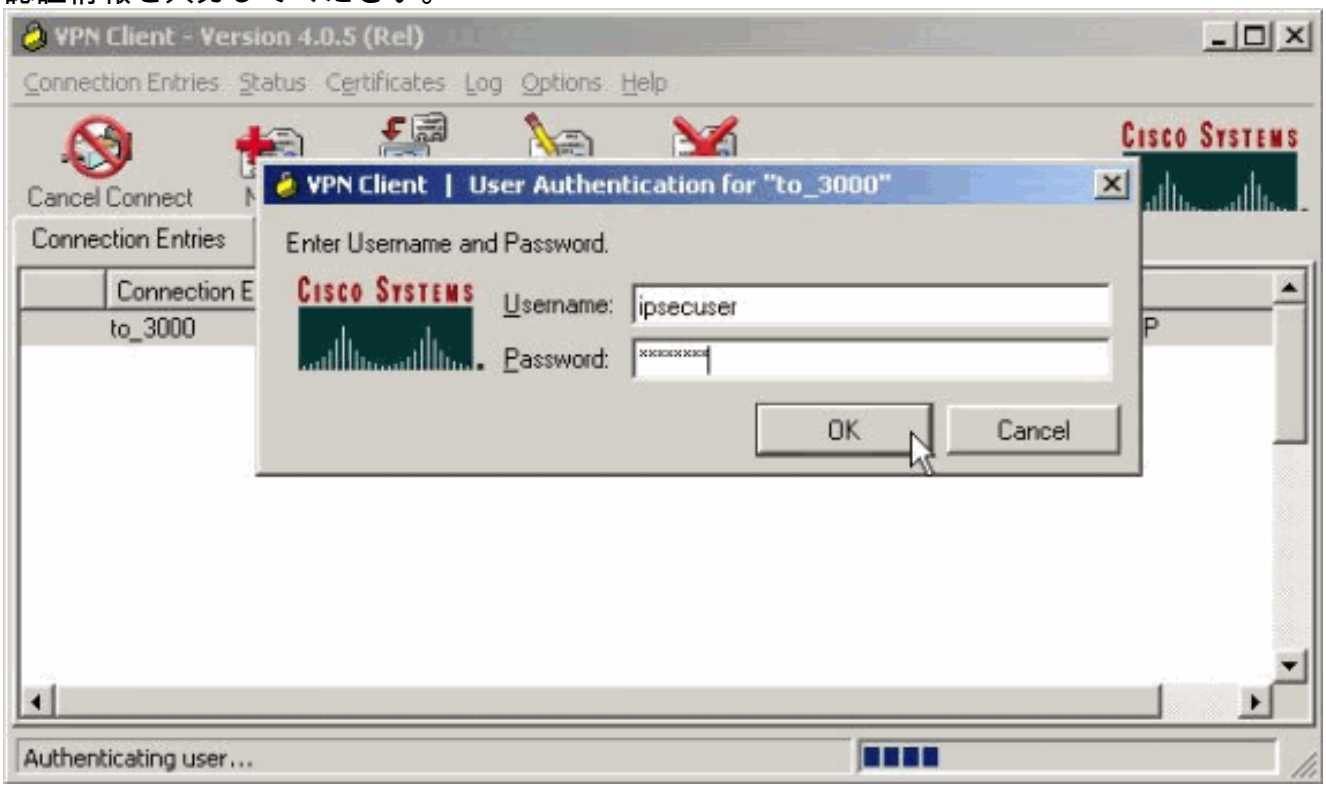
VPN Client で接続する

VPN Client を VPN コンセントレータに接続して、設定を確認します。

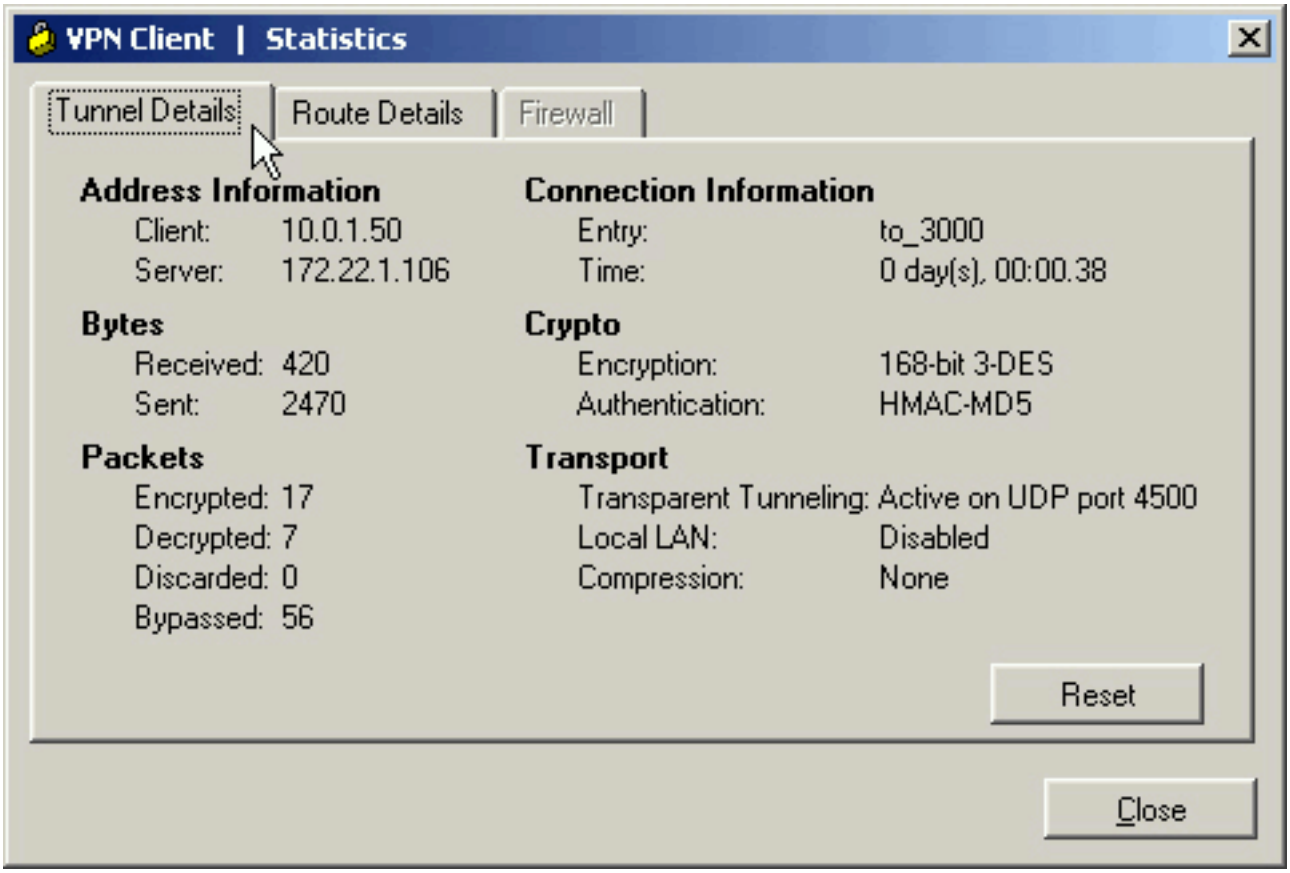
1. リストから接続エントリを選択して [Connect] をクリックします。



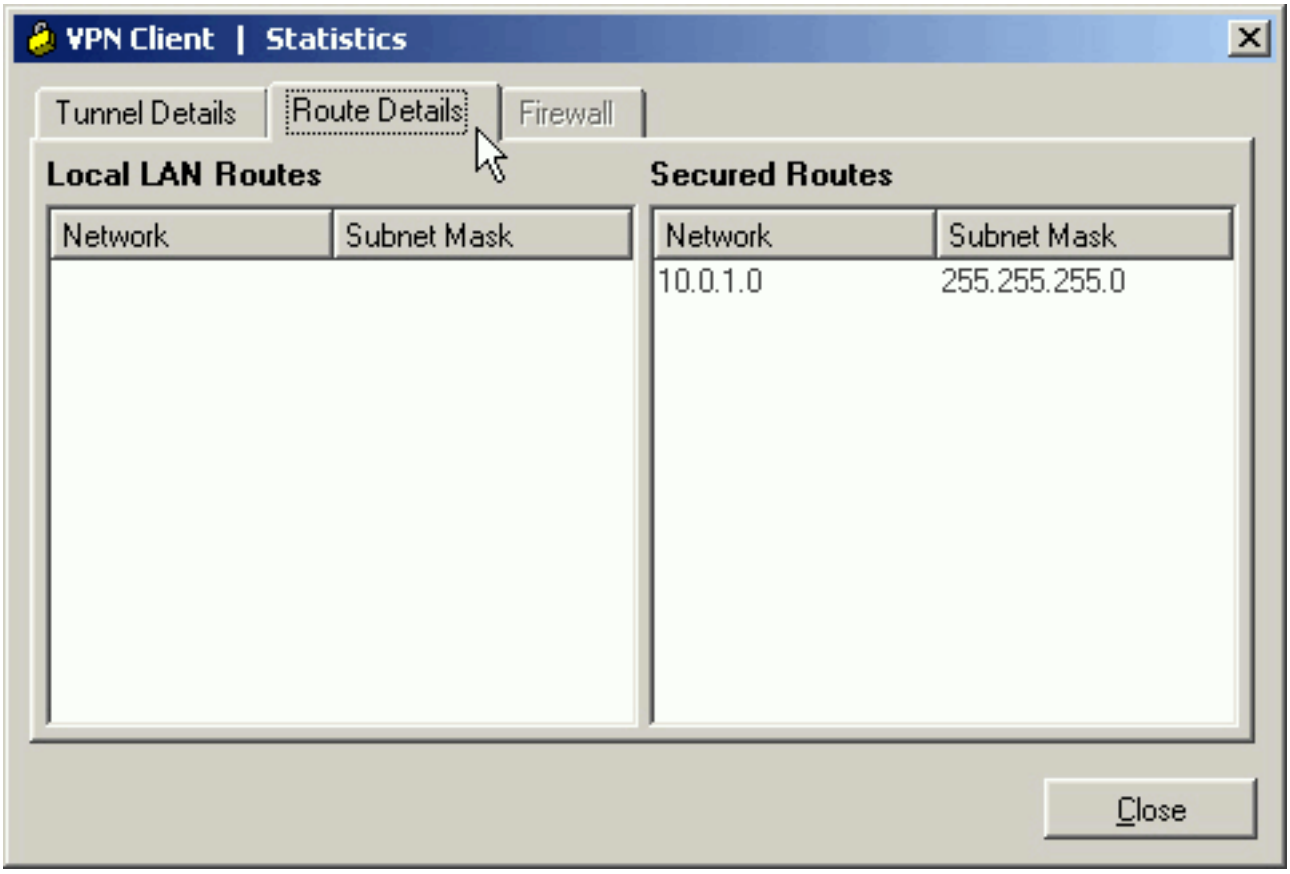
2. 認証情報を入力してください。



3. [Status] > [Statistics...] の順に選択して、[Tunnel Details] ウィンドウを表示します。ここでトンネルの詳細を調べ、トラフィックの流れを確認できます。



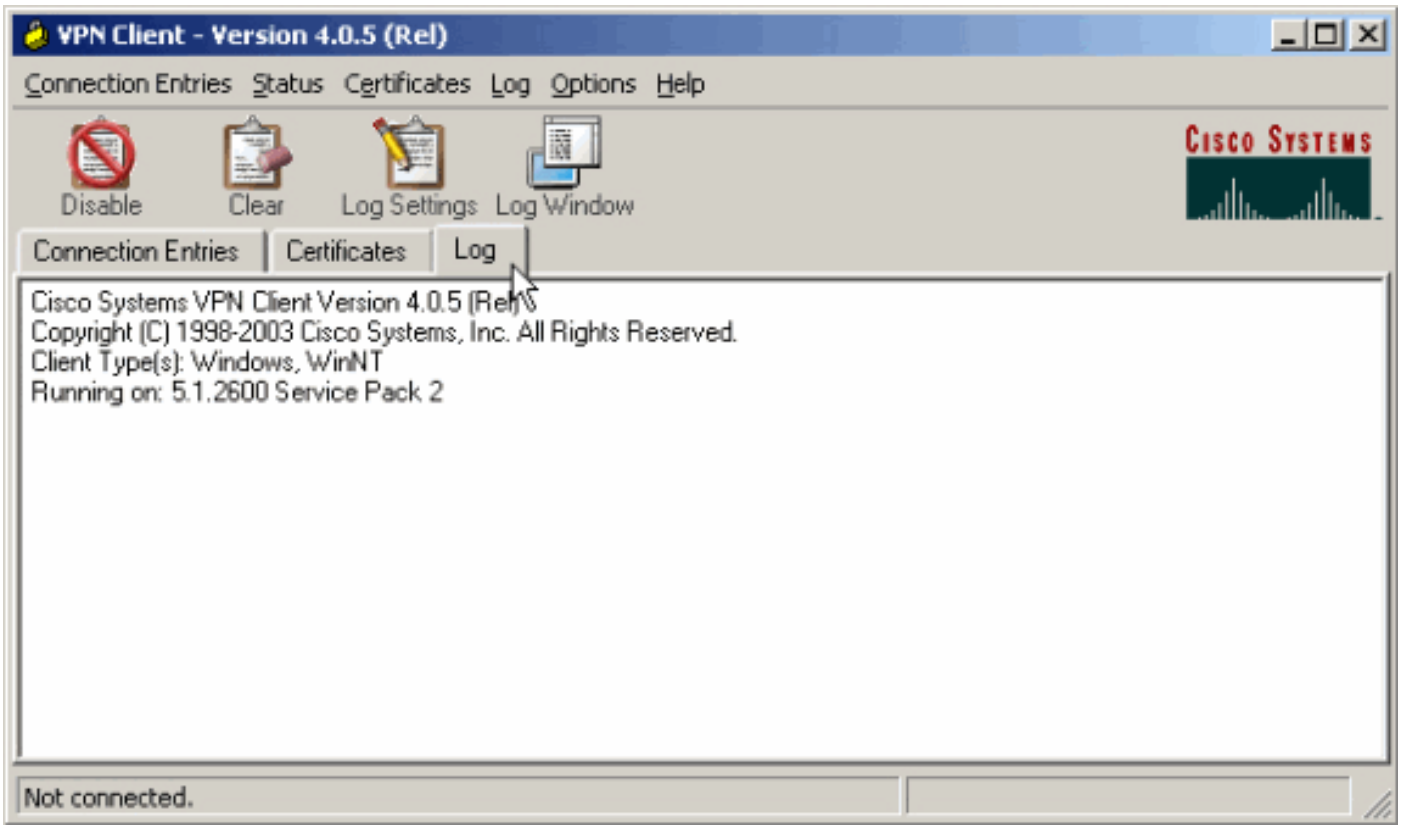
4. [Route Details] タブに移動して、VPN Client が暗号化トラフィックを送信するネットワークを確認します。この例では、VPN Client は 10.0.1.0/24 と安全に通信しますが、その他のすべてのトラフィックは暗号化されていない状態でインターネットに送信されます。



VPN Client ログの表示

VPN Client ログを調査すると、スプリット トンネリングを許可するパラメータが設定されている

かどうかを確認できます。ログを表示するには、VPN Client の [Log] タブに移動します。[Log Settings] をクリックして、記録される内容を調整します。この例では、IKE および IPsec は **3-High** に設定されており、他のすべてのログ要素は **1 - Low** に設定されています。




```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:21:43.106  07/21/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.

!--- Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30
14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
= 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0
mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed.
```

トラブルシュート

この設定のトラブルシューティングに関する一般的な情報については、『VPN 3000 コンセントレータに接続する VPN Client での IPsec 設定例』の「トラブルシューティング」を参照してください。

関連情報

- VPN 3000 コンセントレータに接続する VPN Client での IPsec 設定例
- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco VPN Client
- テクニカル サポートとドキュメント – Cisco Systems