ASA/PIX： CLI および ASDM による VPN Client トラフィック用の着信 NAT を使用したリモート VPN サーバの設定例

目次

概要

このドキュメントでは、Adaptive Security Device Manager（ASDM）か CLI を使用して、リモート VPN サーバとして機能し、着信 VPN Client トラフィックに NAT を実行するように Cisco 5500 シリーズ適応型セキュリティ アプライアンス（ASA）を設定する方法について説明します。 ASDM では、直感的で使用が容易な Web ベースの管理インターフェイスにより、ワールドクラスのセキュリティ管理と監視機能が提供されています。 Cisco ASA の設定が完了したら、Cisco VPN Client を使用して設定を検証できます。

前提条件

要件

このドキュメントでは、ASA が完全に動作していて、Cisco ASDM か CLI で設定を変更できるように設定されていることを想定しています。 また、ASA をアウトバウンド NAT に関して設定することも想定しています。 アウトバウンド NAT の設定方法の詳細については、「PAT を使用して内部ホストから外部ネットワークへアクセスを許可」を参照してください。

注: 「ASDM 用の HTTPS アクセスの許可」または「PIX/ASA 7.x： 内部および外部インターフェ

イスの SSH の設定例」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くものです。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Adaptive Security Device Manager バージョン 5.x 以降
- Cisco VPN Client バージョン 4.x 以降

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。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

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 アクセス設定により、モバイル ユーザなどの Cisco VPN Client にセキュアなリモート アクセスが提供されます。 リモート アクセス VPN により、リモート ユーザが中央のネットワーク リソースに安全にアクセスできるようになります。 Cisco VPN Client は IPSec プロトコルに準拠しており、特にセキュリティ アプライアンスと連動する設計になっています。 一方、セキュリティ アプライアンスは、多様なプロトコルに準拠するクライアントと IPSec 接続を確立できます。 IPSec の詳細については、『ASA 構成ガイド』を参照してください。

グループとユーザは、VPN のセキュリティの管理とセキュリティ アプライアンスの設定では中心となる概念です。 これらにより、ユーザによる VPN へのアクセスと使用を決定する属性が指定されます。 グループはユーザの集合で、単一のエンティティとして扱われます。 ユーザは自身の属性をグループのポリシーから取得します。 トンネル グループでは、特定の接続のグループ ポリシーが識別されます。 特定のグループ ポリシーをユーザに割り当てない場合は、その接続のデフォルトのグループ ポリシーが適用されます。

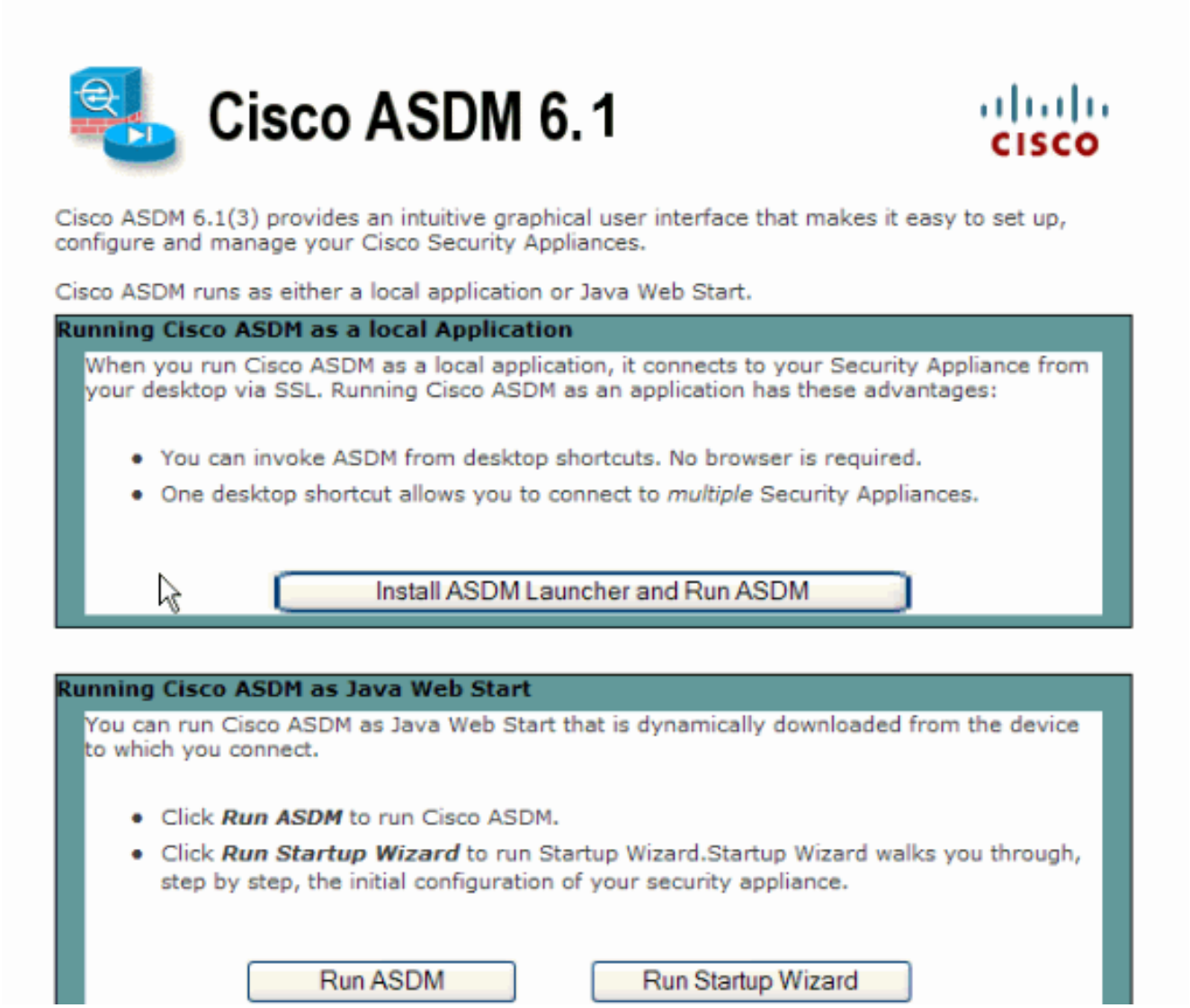
トンネル グループは、トンネル接続のポリシーを決定するレコードのセットで構成されています。 これらのレコードにより、トンネル ユーザが認証されているサーバ、および接続情報の送信先となるアカウンティング サーバ（存在する場合）が識別され、 接続のデフォルトのグループ ポリシーも識別されます。レコードには、プロトコル固有の接続パラメータも含まれています。 トンネル グループには、トンネル自体の作成に関連した少数の属性が含まれています。 トンネル グループには、ユーザ指向の属性を定義するグループ ポリシーに対するポインタが含まれています。

設定

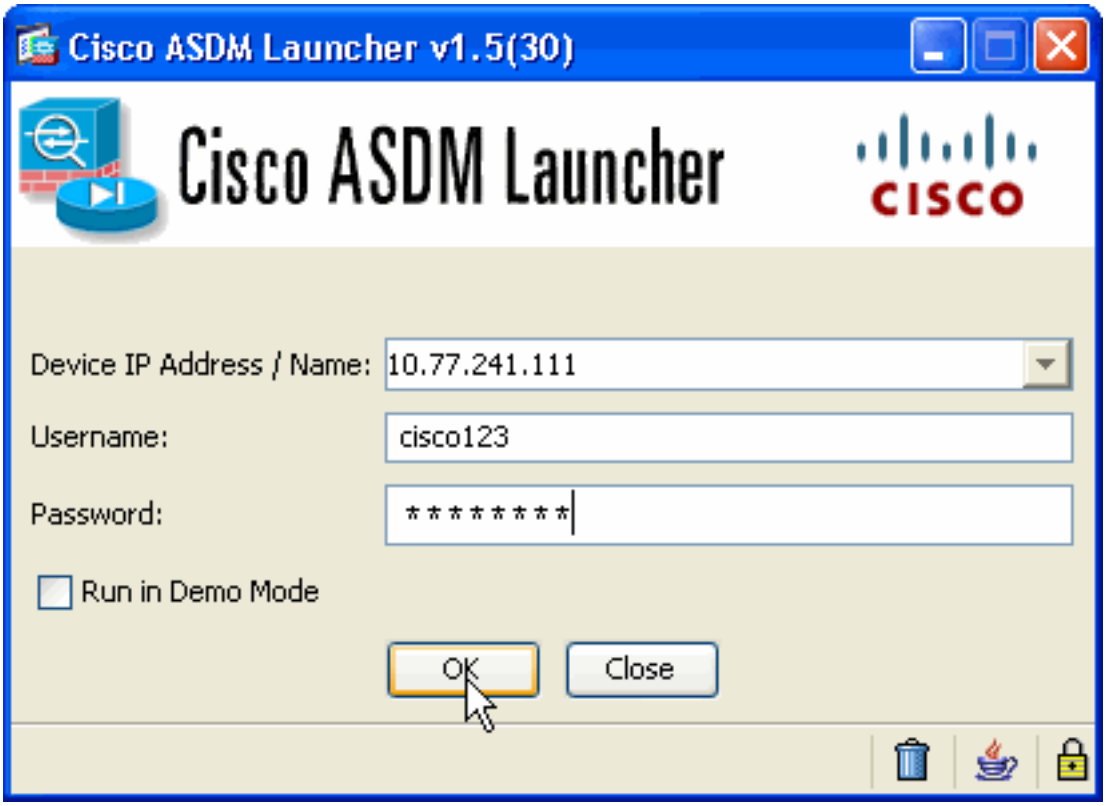
ASDM を使用した、リモート VPN サーバとしての ASA/PIX の設定

ASDM を使用して Cisco ASA をリモート VPN サーバとして設定するには、次の手順を実行します。

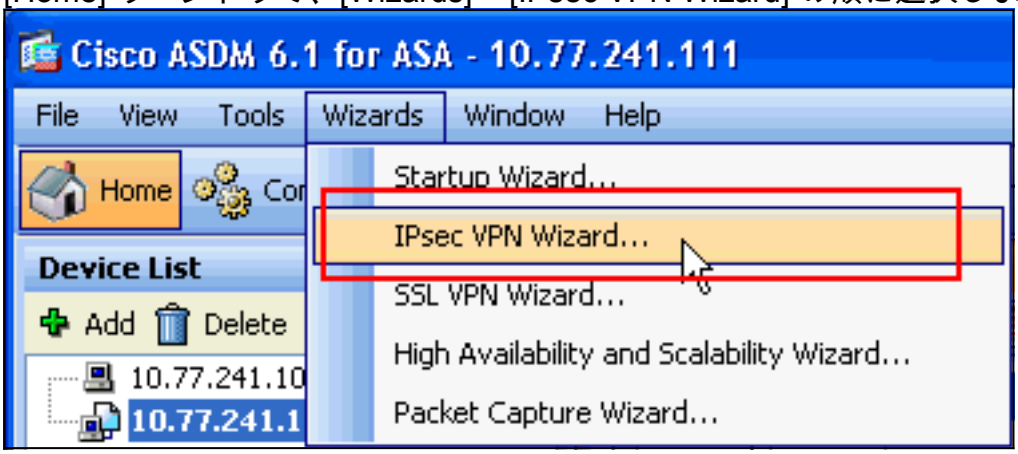
1. ブラウザを開き、**https://<ASDM アクセス用に設定された ASA のインターフェイスの IP アドレス>** を入力して、ASA 上の ASDM にアクセスします。SSL 証明書の信頼性に関連してブラウザから出力されるすべての警告を承認します。 デフォルトのユーザ名とパスワードは、両方とも空白です。ASA がこのウィンドウを表示するのは、ASDM アプリケーションのダウンロードを許可するためです。 次の例の場合、アプリケーションはローカル コンピュータにロードされ、Java アプレットでは動作しません。



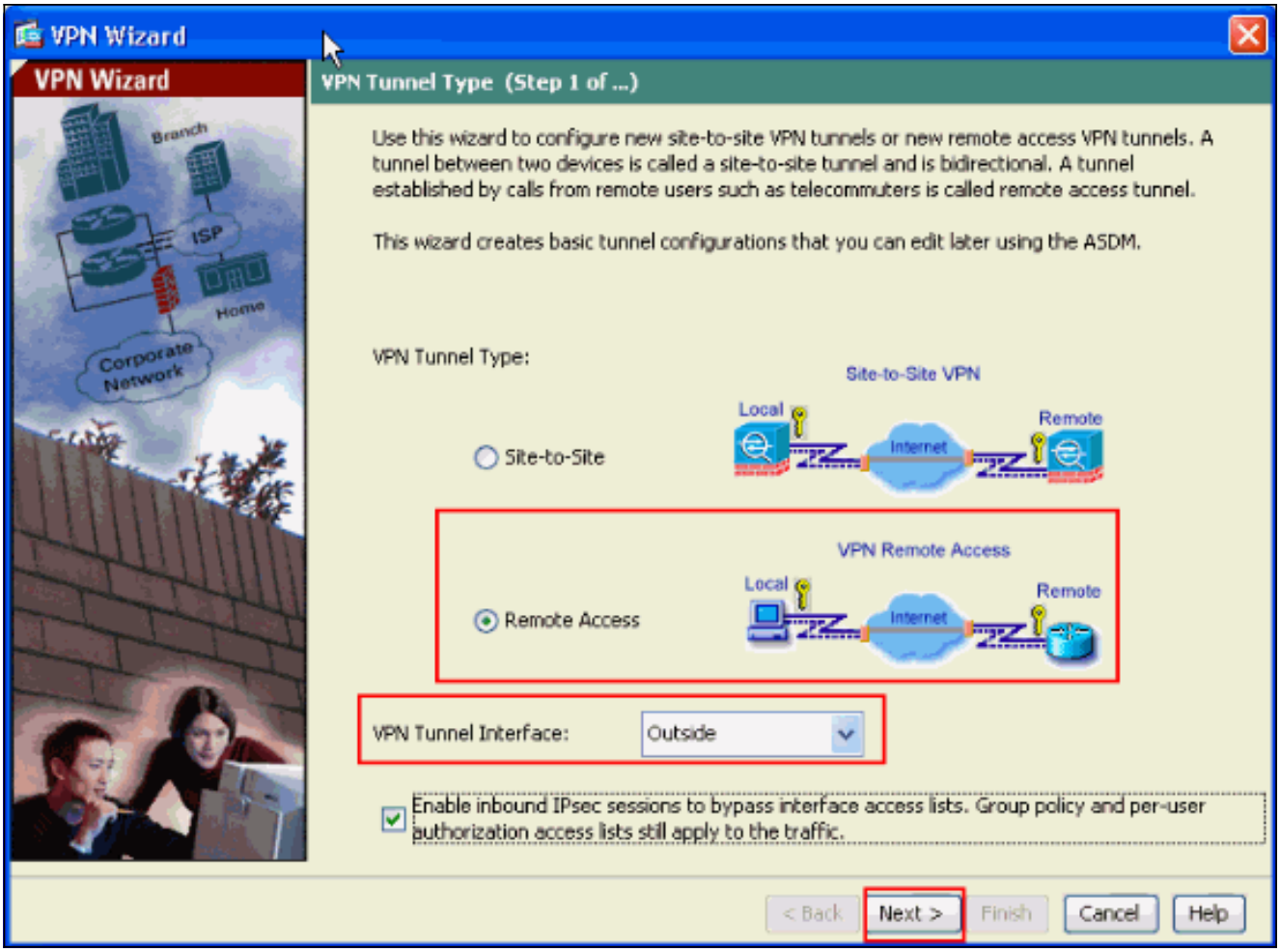
2. [Download ASDM Launcher and Start ASDM] をクリックして、ASDM アプリケーションのインストーラをダウンロードします。
3. ASDM Launcher がダウンロードされたら、プロンプトに従って一連のステップを実行し、該当ソフトウェアをインストールした後、Cisco ASDM Launcher を起動します。
4. **http -** コマンドで設定したインターフェイスの IP アドレスとユーザ名とパスワード（指定した場合）を入力します。次の例では、ユーザ名として **cisco123** 、パスワードとして **cisco123** を使用しています。



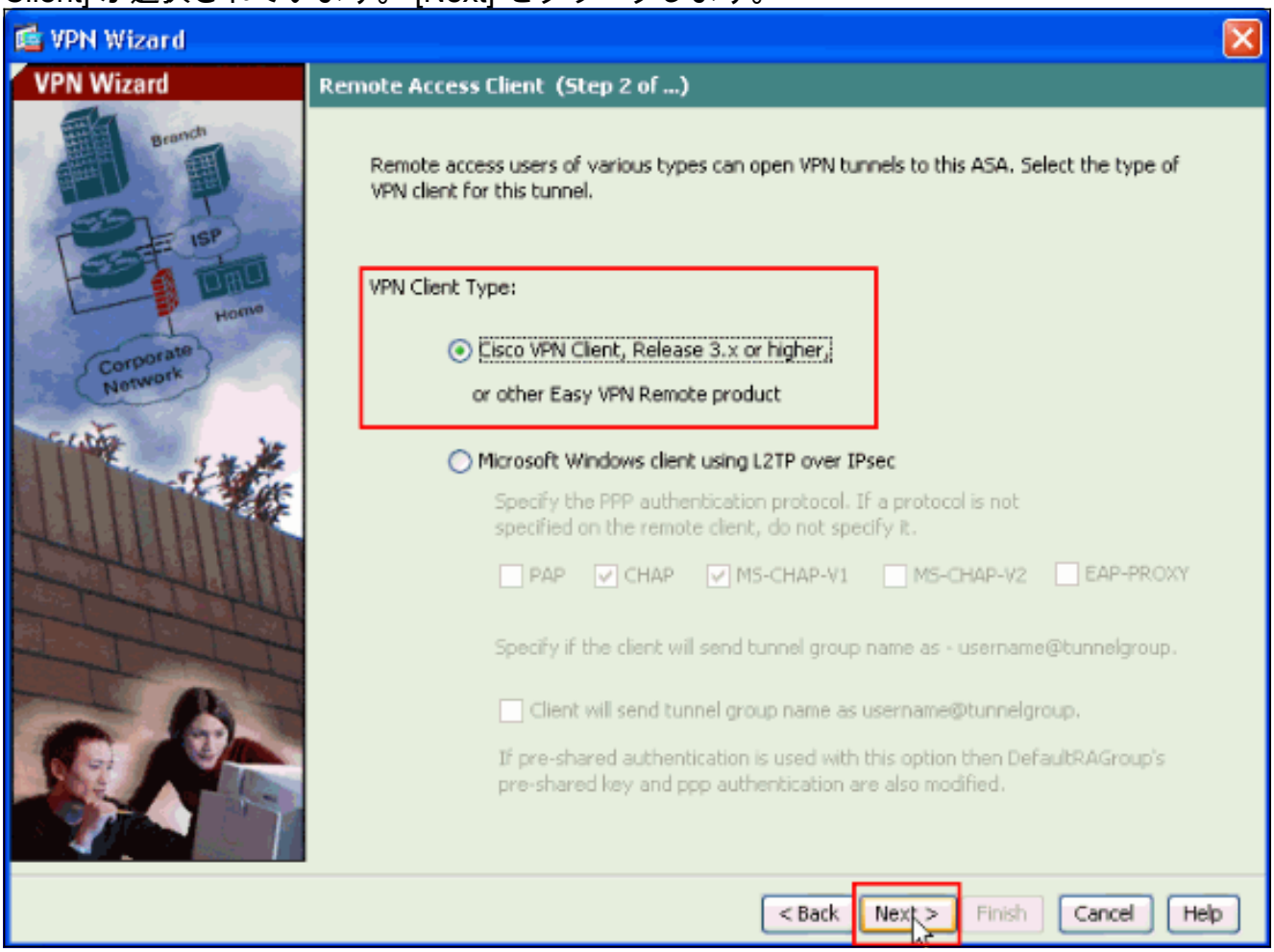
5. [Home] ウィンドウで、[Wizards] > [IPsec VPN Wizard] の順に選択します。



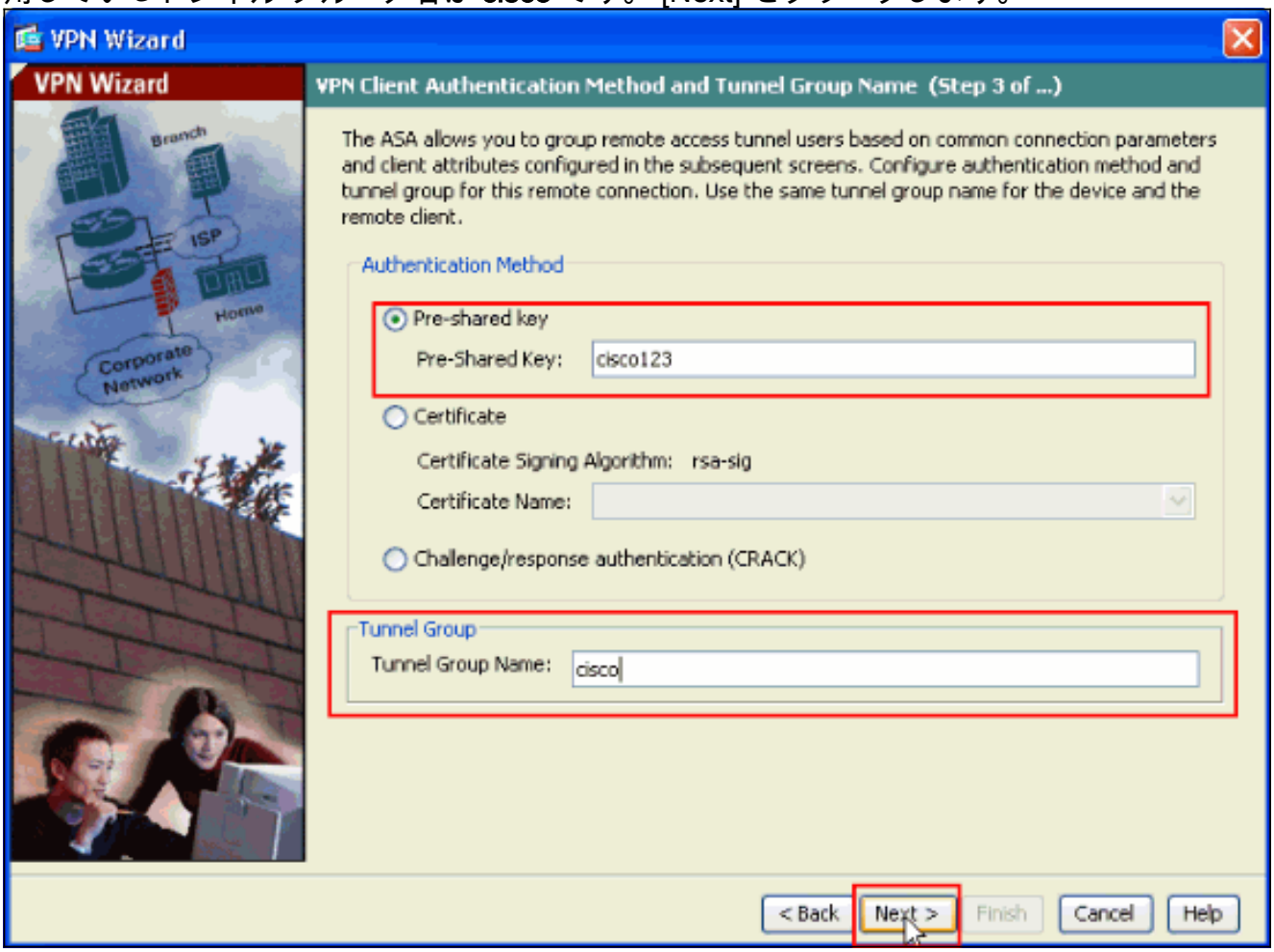
6. 次に示すように、[Remote Access] VPN トンネル タイプを選択し、VPN トンネル インターフェイスが意図どおりに設定されていることを確認し、[Next] をクリックします。



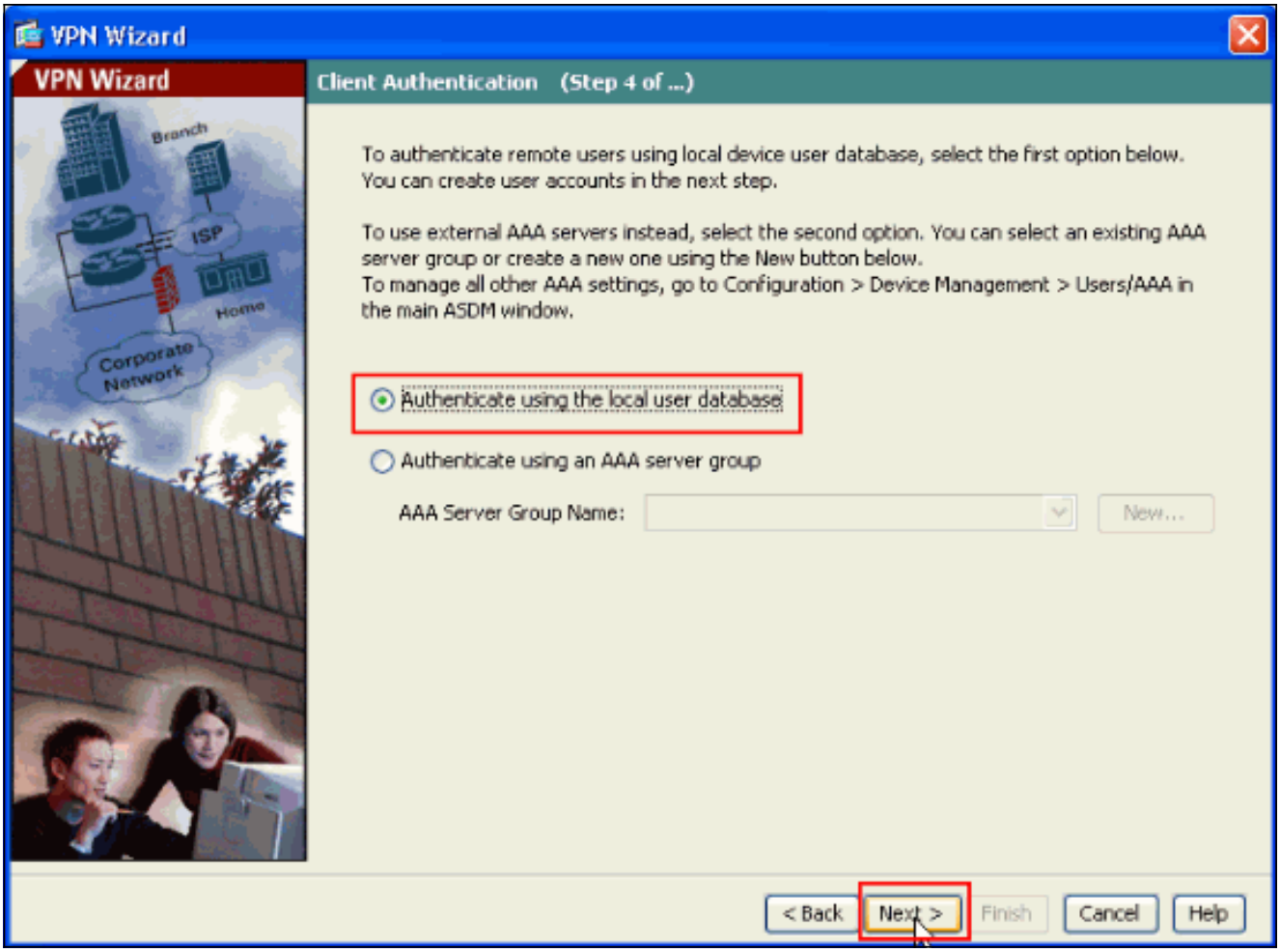
7. 次に示すとおり、VPN クライアント タイプが選択されています。 ここでは、[Cisco VPN Client] が選択されています。 [Next] をクリックします。



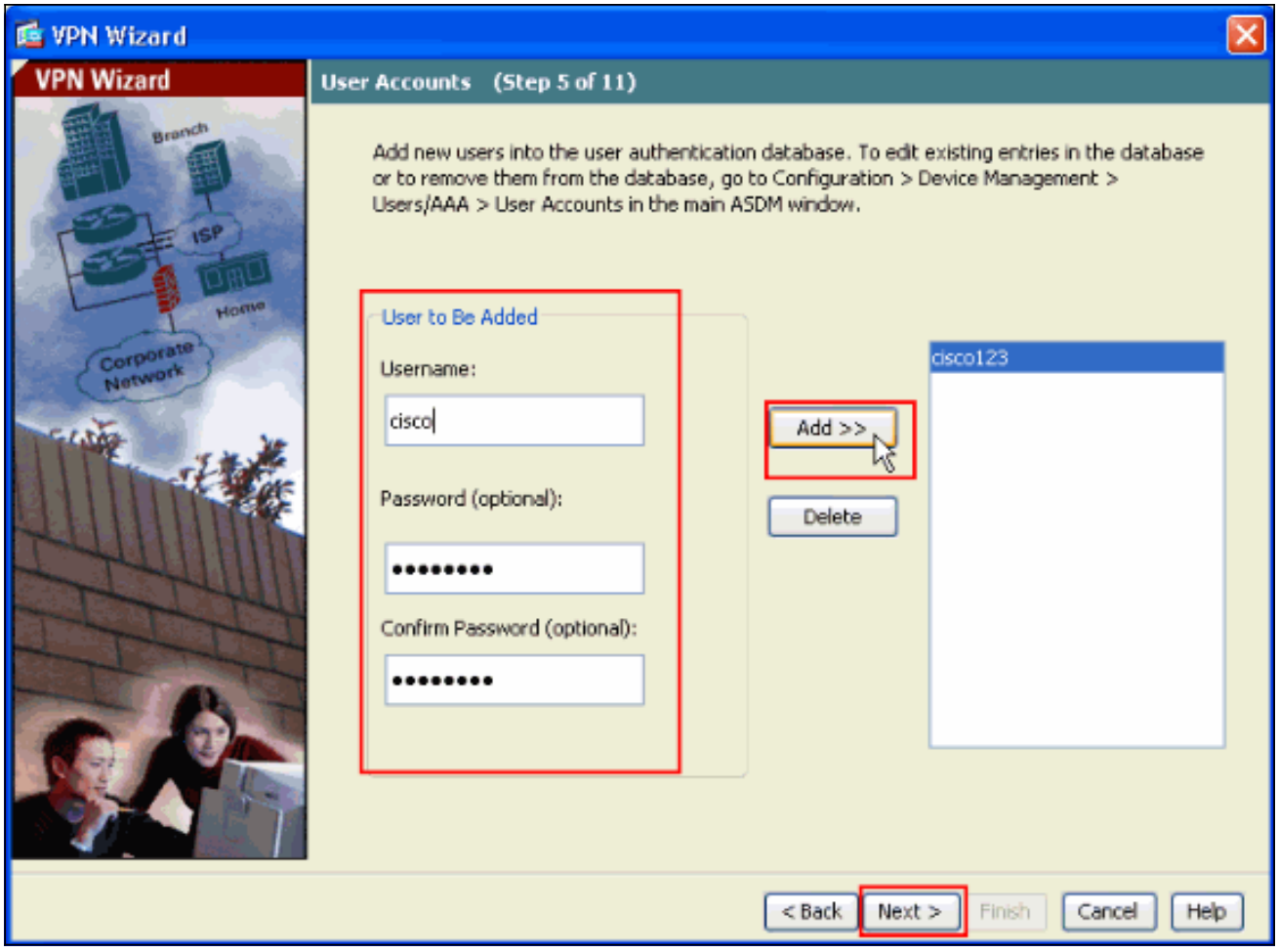
8. [Tunnel Group Name] の名前を入力します。 使用する認証情報（この例では**事前共有キー**）を入力します。 次の例では、**cisco123** という事前共有鍵を使用しています。 この例で使用しているトンネル グループ名は **cisco** です。 [Next] をクリックします。



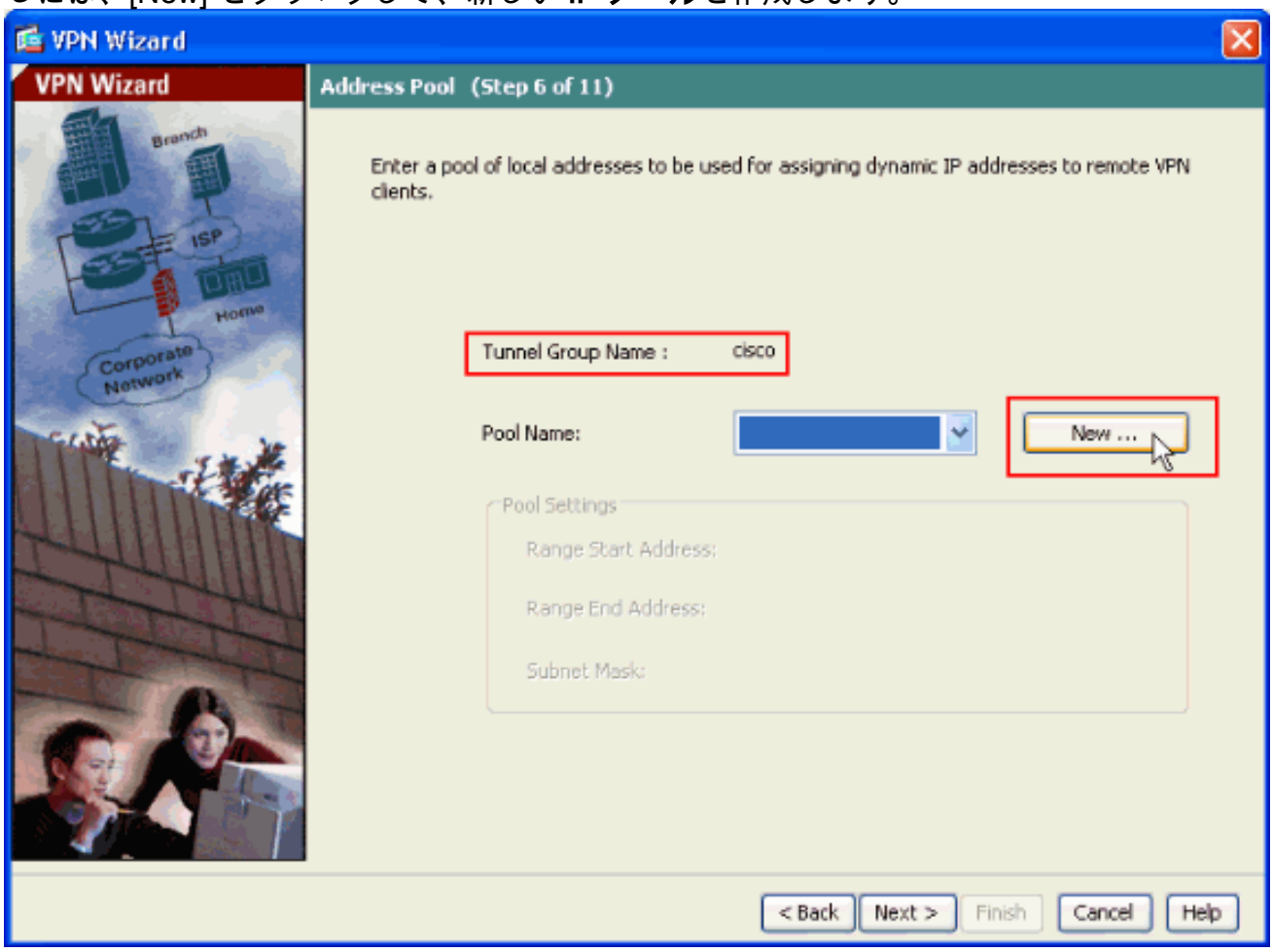
9. リモート ユーザの認証用にローカル ユーザのデータベースか外部 AAA サーバ グループを選択します。**注:** ステップ 10 で、ローカル ユーザのデータベースにユーザを追加します。**注:** ASDM で外部 AAA サーバ グループを設定する方法の詳細については、「PIX/ASA 7.x：ASDM での VPN ユーザの認証と認可サーバ グループの設定例」を参照してください。



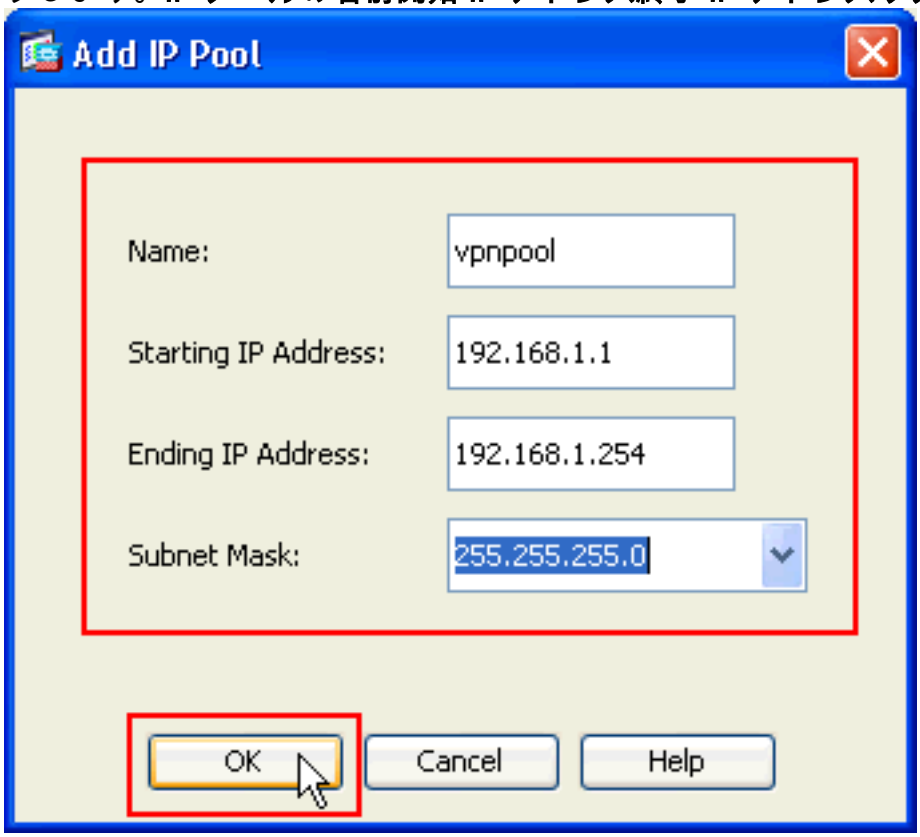
10. [Username] とオプションの [Password] を入力し、[Add] をクリックして、ユーザ認証データベースに新しいユーザを追加します。 [Next] をクリックします。**注:** このウィンドウで既存のユーザを削除しないようにしてください。 データベースの既存エントリを編集する、またはデータベースから既存エントリを削除するには、メインの [ASDM] ウィンドウで、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] の順に選択します。



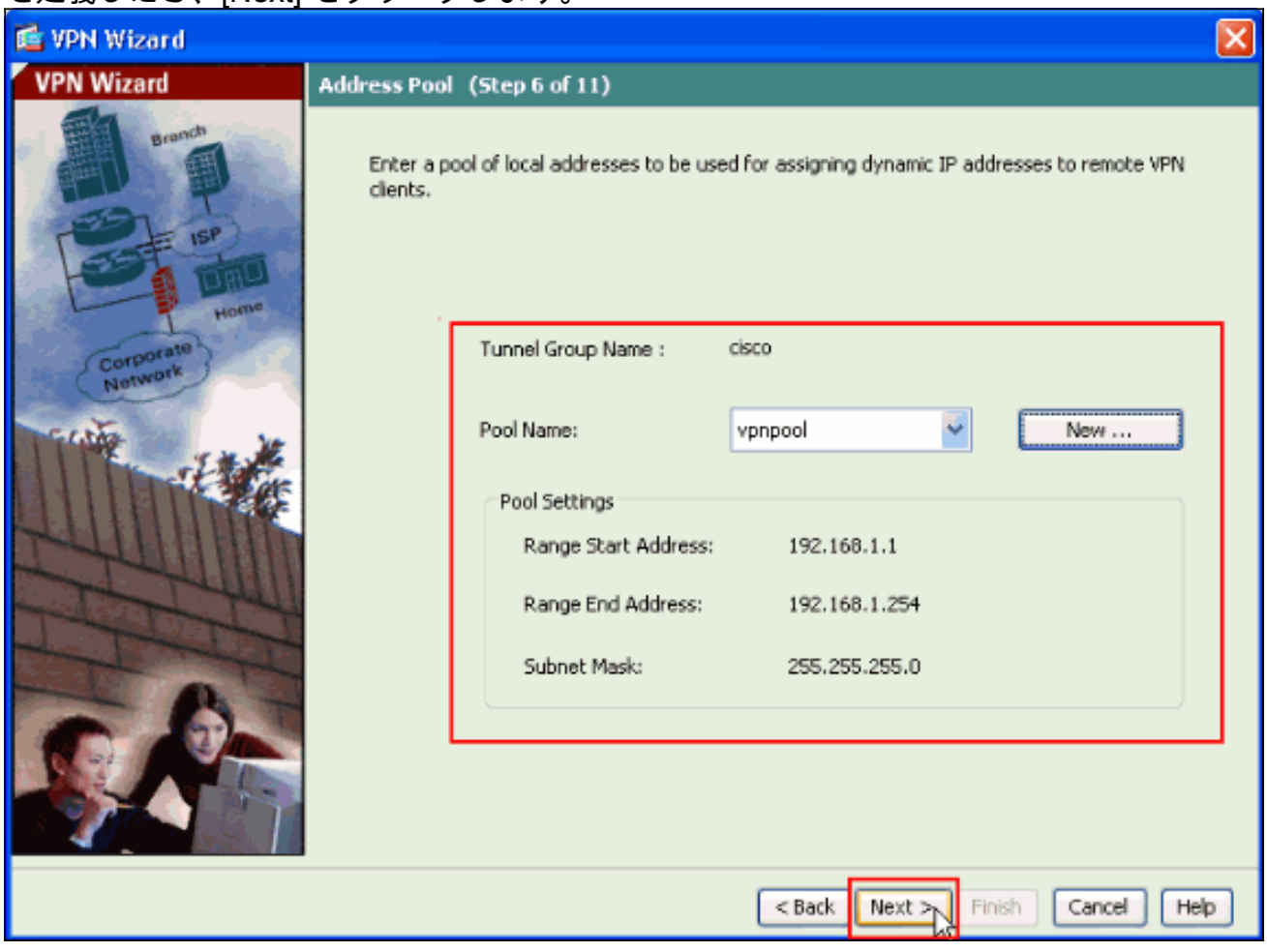
11. リモート VPN クライアントに動的に割り当てられるローカル アドレスのプールを定義するには、[New] をクリックして、新しい **IP プール**を作成します。



12. [Add IP Pool] という名前の新しいウィンドウに以下の情報が表示されたら、[OK] をクリックします。**IP プールの名前開始 IP アドレス終了 IP アドレスサブネット マスク**

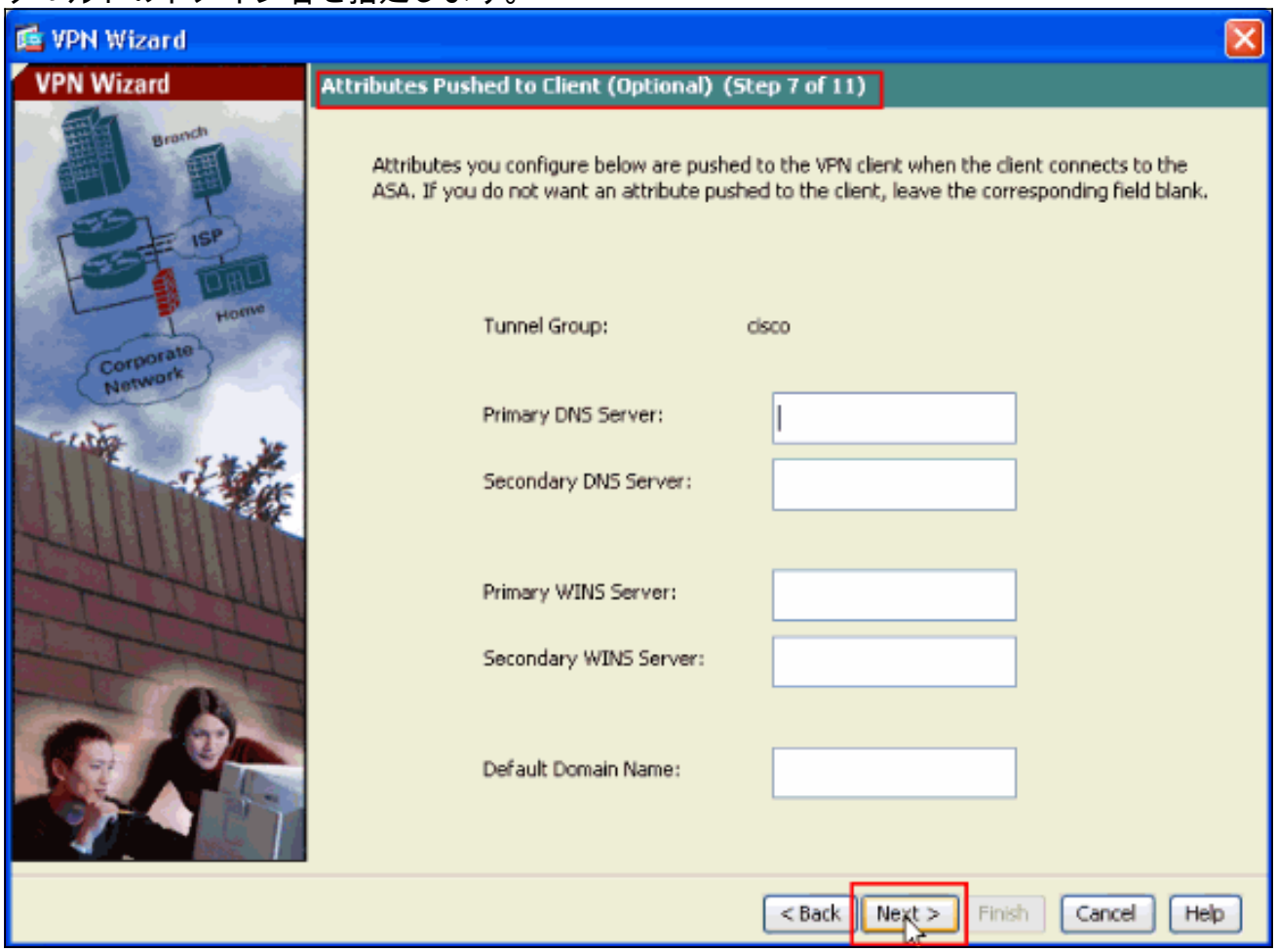


13. リモート VPN クライアントの接続時に動的に割り当てられるローカル アドレスのプールを定義したら、[Next] をクリックします。

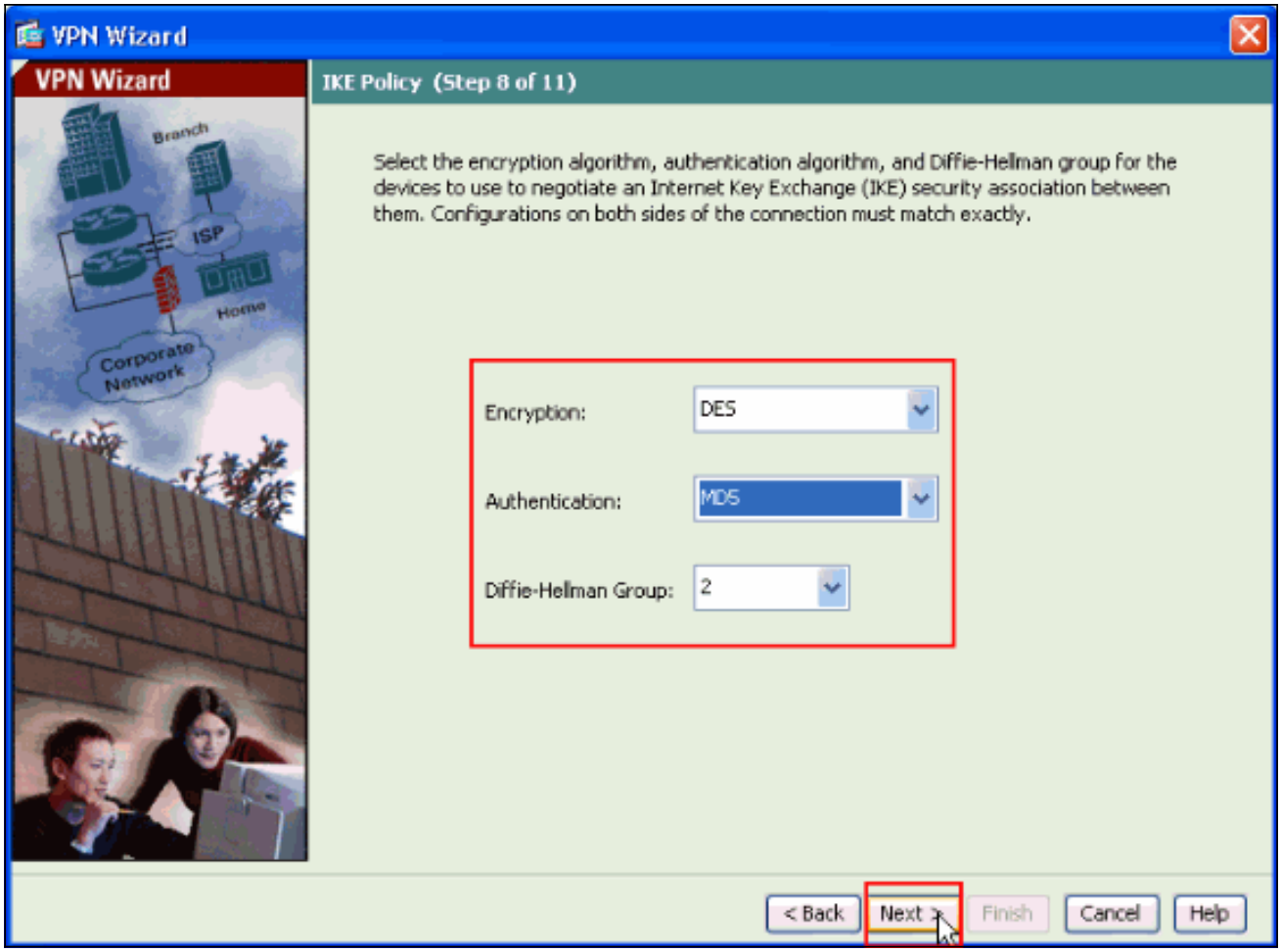


14. *オプション：* DNS と WINS のサーバ情報、およびリモート VPN Client にプッシュするデ

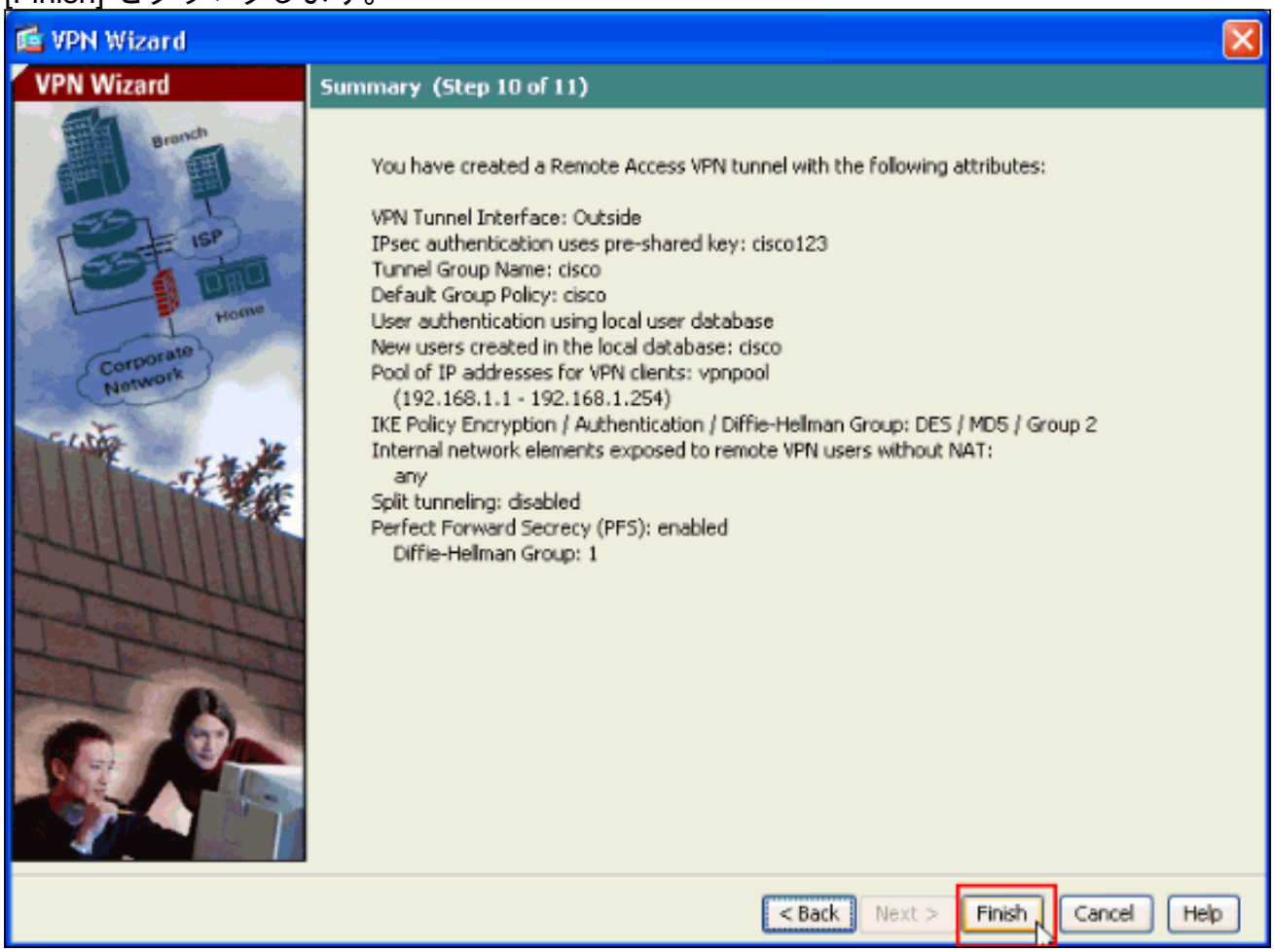
フォルトのドメイン名を指定します。



15. IKE のパラメータを指定します。これは IKE フェーズ 1 とも呼ばれます。トンネルの両側の設定は完全に一致している必要があります。 ただし、Cisco VPN Client では適切な設定が自動的に選択されます。 そのため、クライアント PC で IKE を設定する必要はありません。



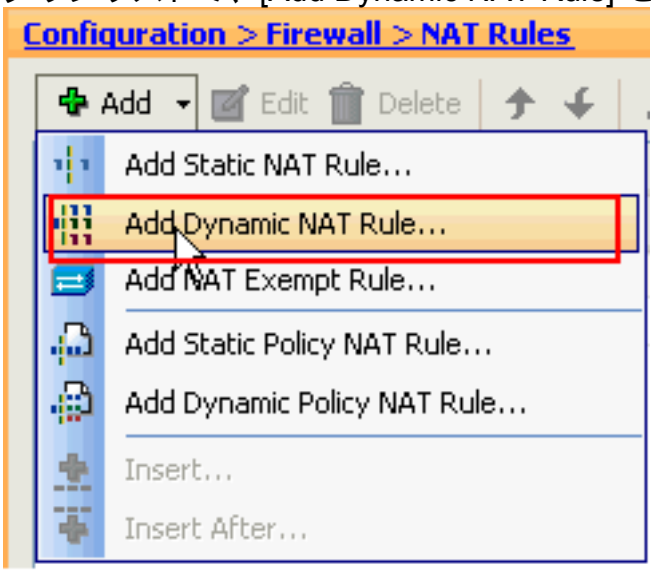
16. このウィンドウにはユーザが行った操作の概要が表示されます。 設定に問題がなければ、[Finish] をクリックします。



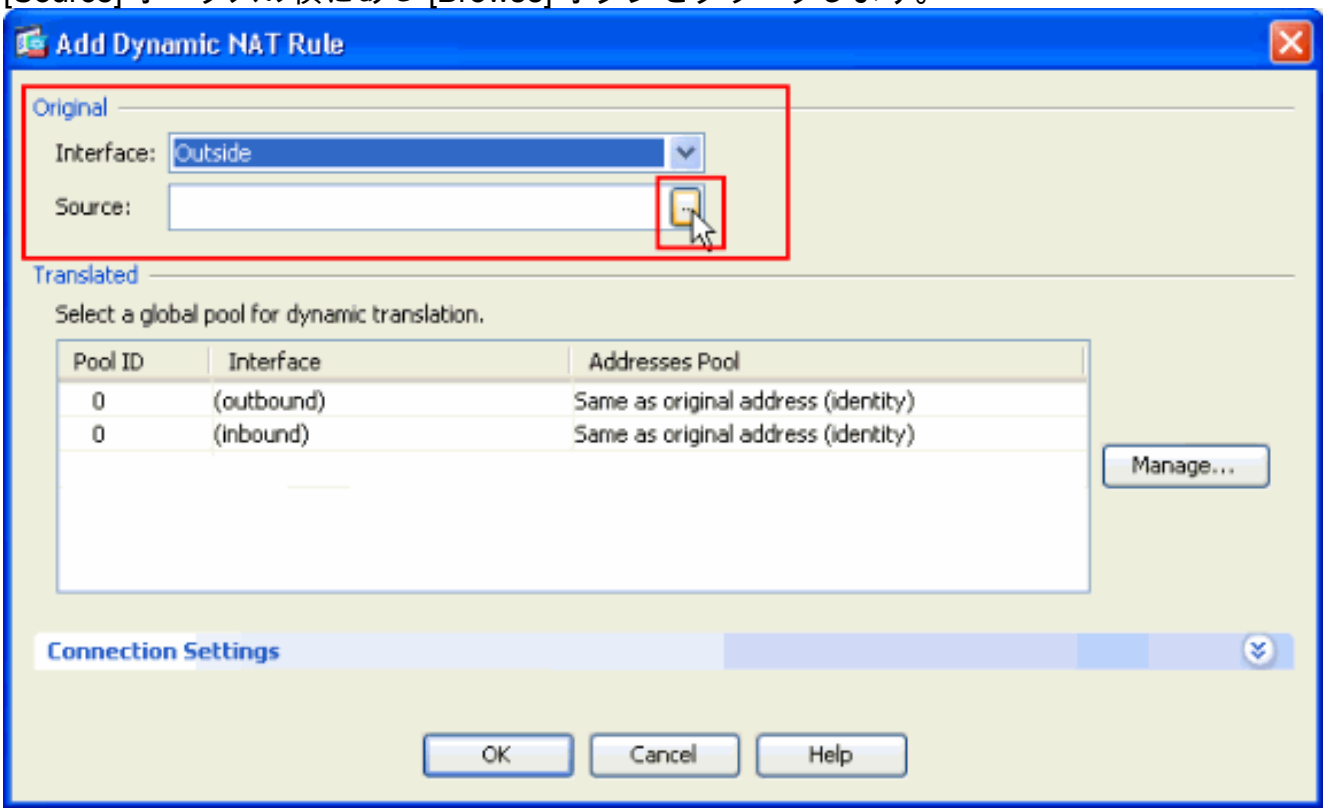
ASDM を使用した、着信 VPN クライアント トラフィックを NAT するための ASA/PIX の設定

ASDM を使用して、着信 VPN クライアント トラフィックを NAT するために Cisco ASA を設定するには、次の手順を実行します。

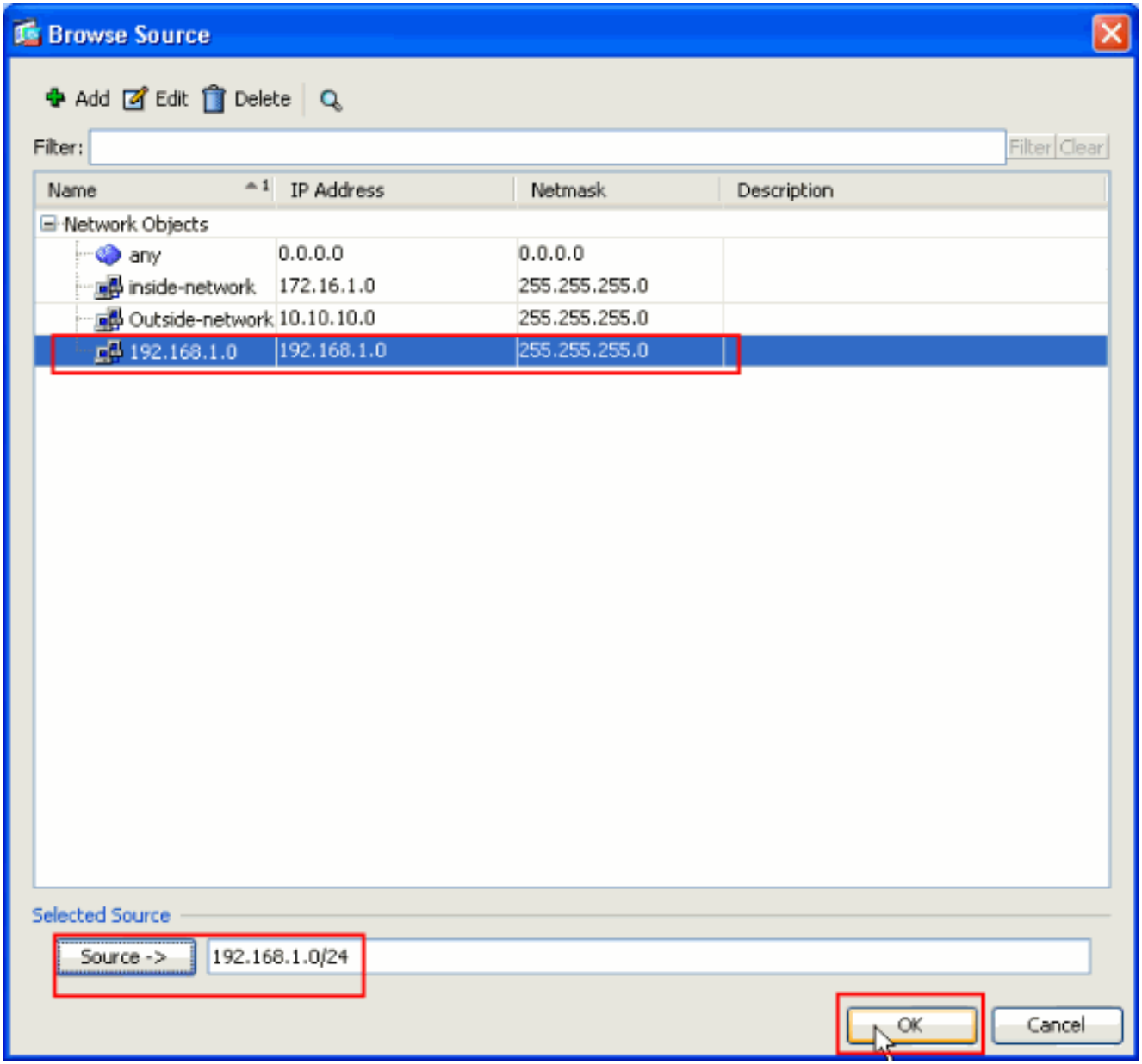
1. [Configuration] > [Firewall] > [Nat Rules] の順に選択し、[Add] をクリックします。 ドロップダウンリストで、[Add Dynamic NAT Rule] を選択します。



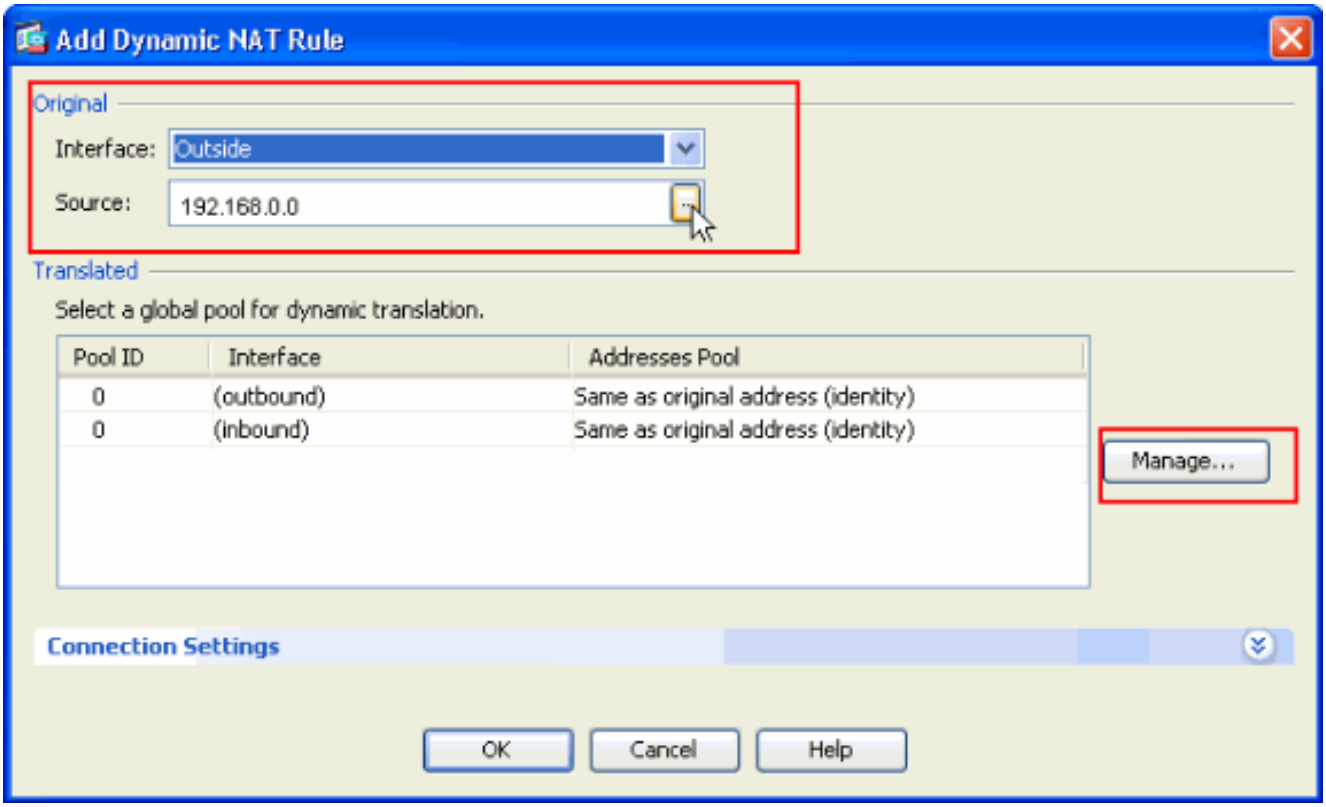
2. [Add Dynamic NAT Rule] ウィンドウで、インターフェイスとして [Outside] を選択し、[Source] ボックスの横にある [Browse] ボタンをクリックします。



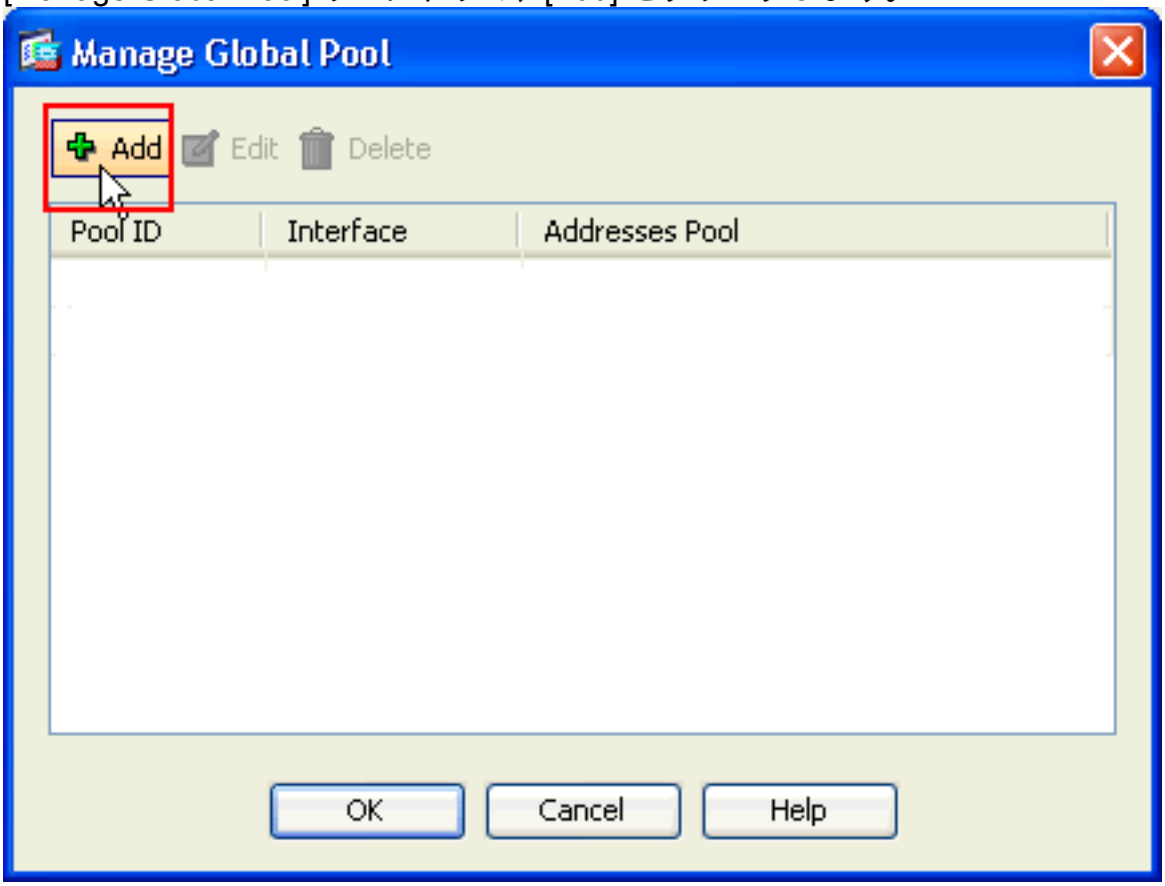
3. [Browse Source] ウィンドウで適切なネットワーク オブジェクトを選択し、[Selected Source] セクションの下で [Source] を選択し、[OK] をクリックします。 ここでは、192.168.1.0 ネットワーク オブジェクトが選択されています。



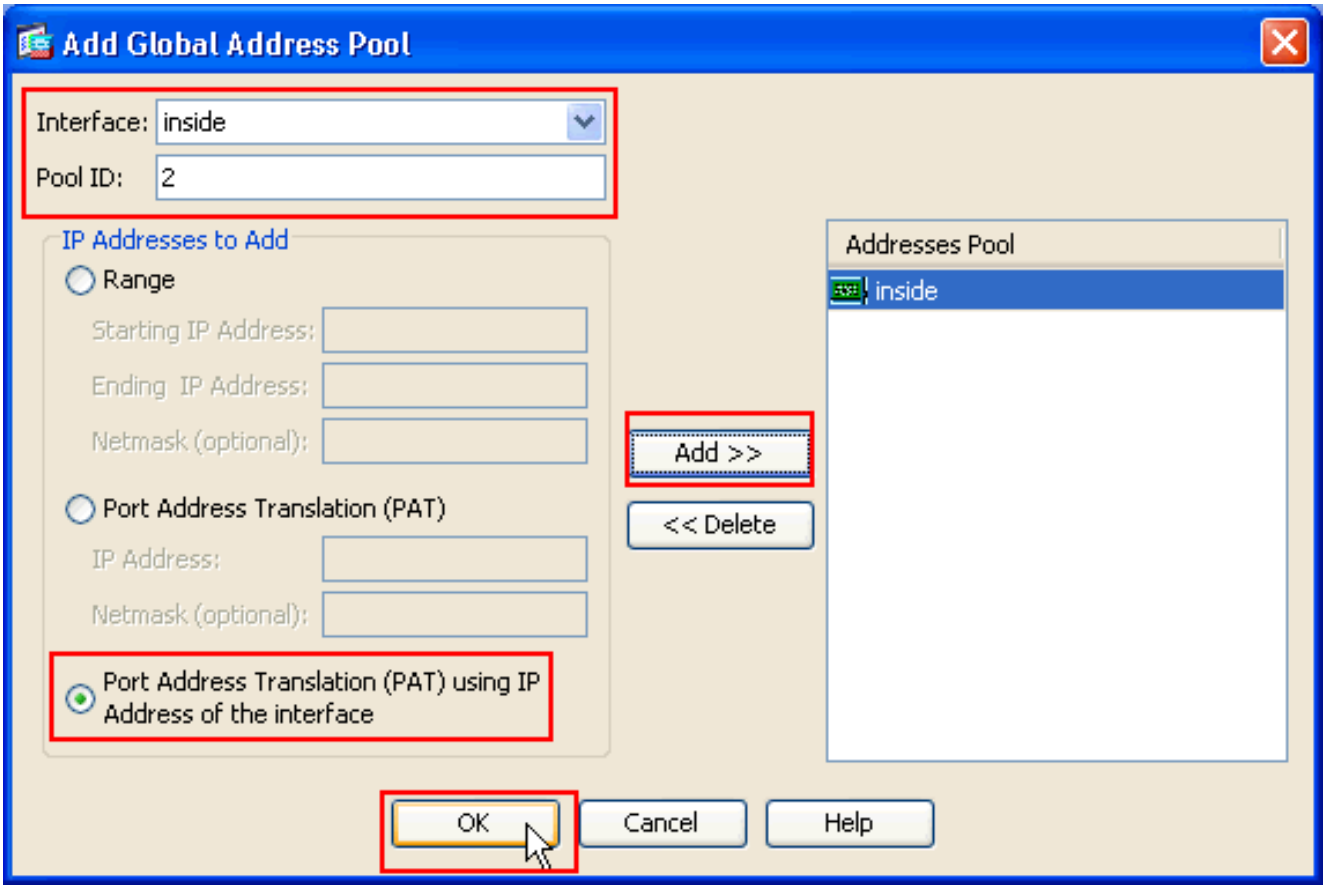
4. [Manage] をクリックします。



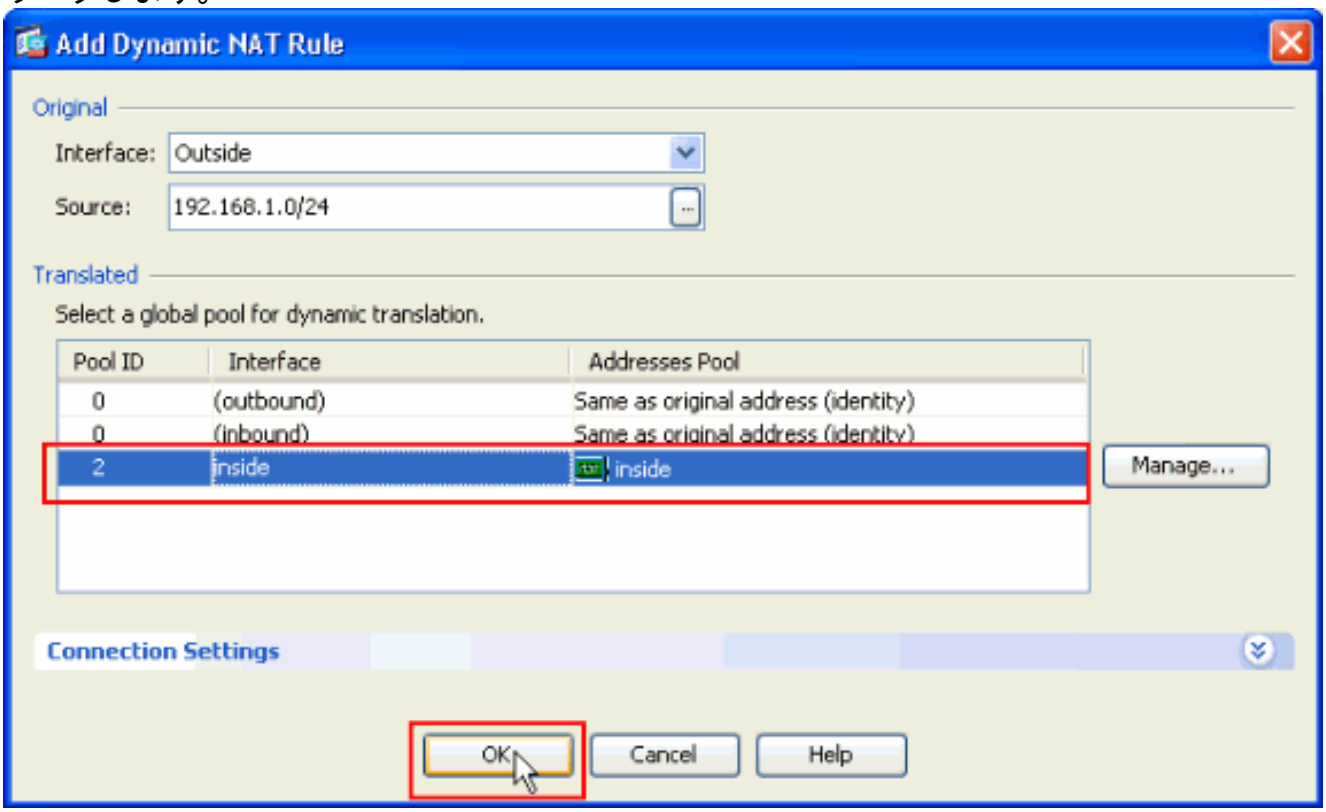
5. [Manage Global Pool] ウィンドウで、[Add] をクリックします。



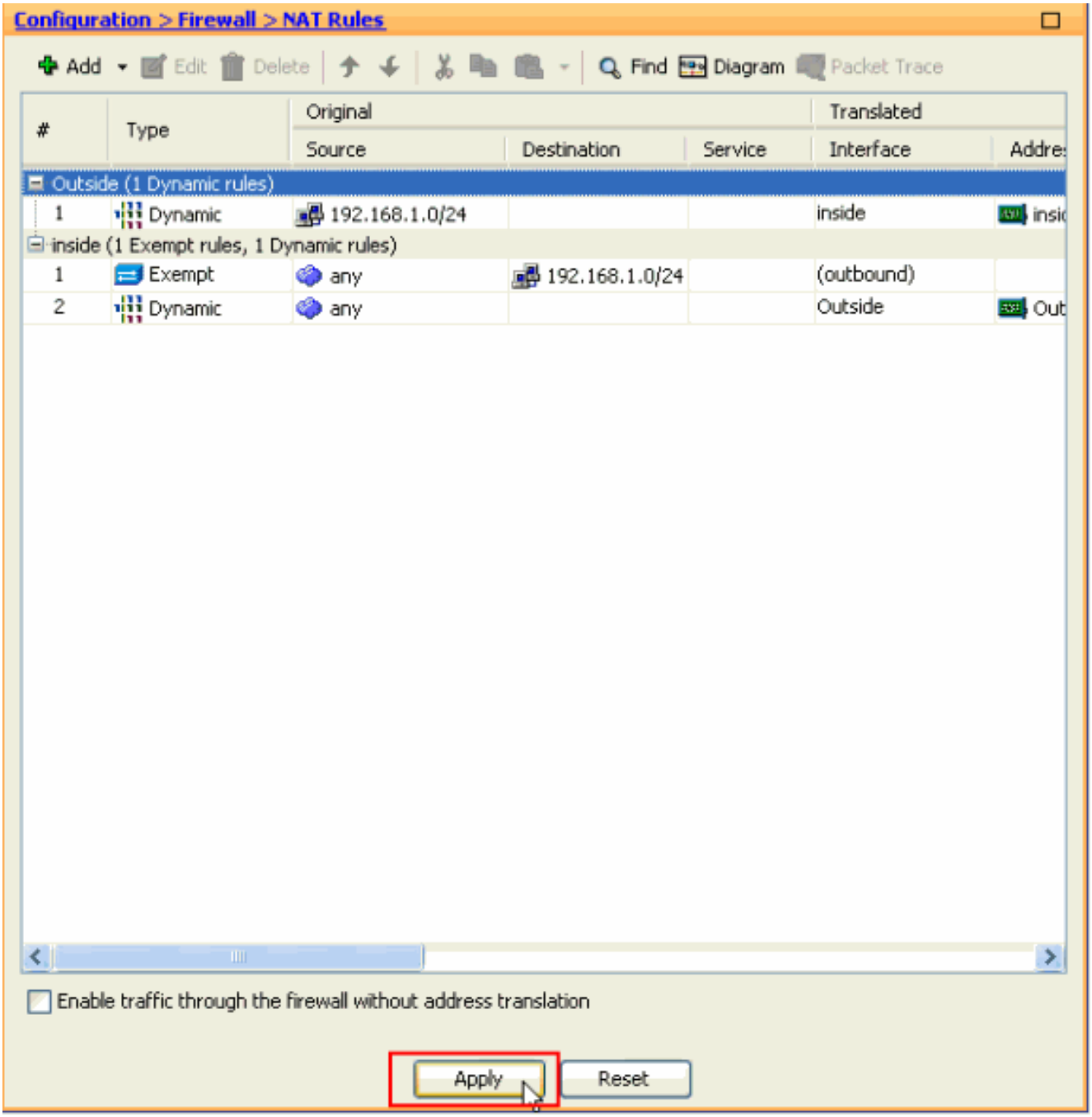
6. [Add Global Address Pool] ウィンドウで、インターフェイスとして [Inside] を選択し、[Pool ID] として 2を選択します。 [Port Address Translation (PAT) using IP Address of the interface] の横のオプション ボタンが選択されていることも確認してください。 [Add>>] をクリックして、[OK] をクリックします。



7. 前のステップで設定したPool ID 2 が設定されたグローバル プールを選択したら、[OK] をクリックします。



8. ここで、[Apply] をクリックすると、設定が ASA に適用されます。これで設定は終了です。



CLI を使用した、リモート VPN サーバとして、および着信を NAT するための ASA/PIX の設定

ASA デバイスでの設定の実行
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 ! ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 **ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control **global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2**

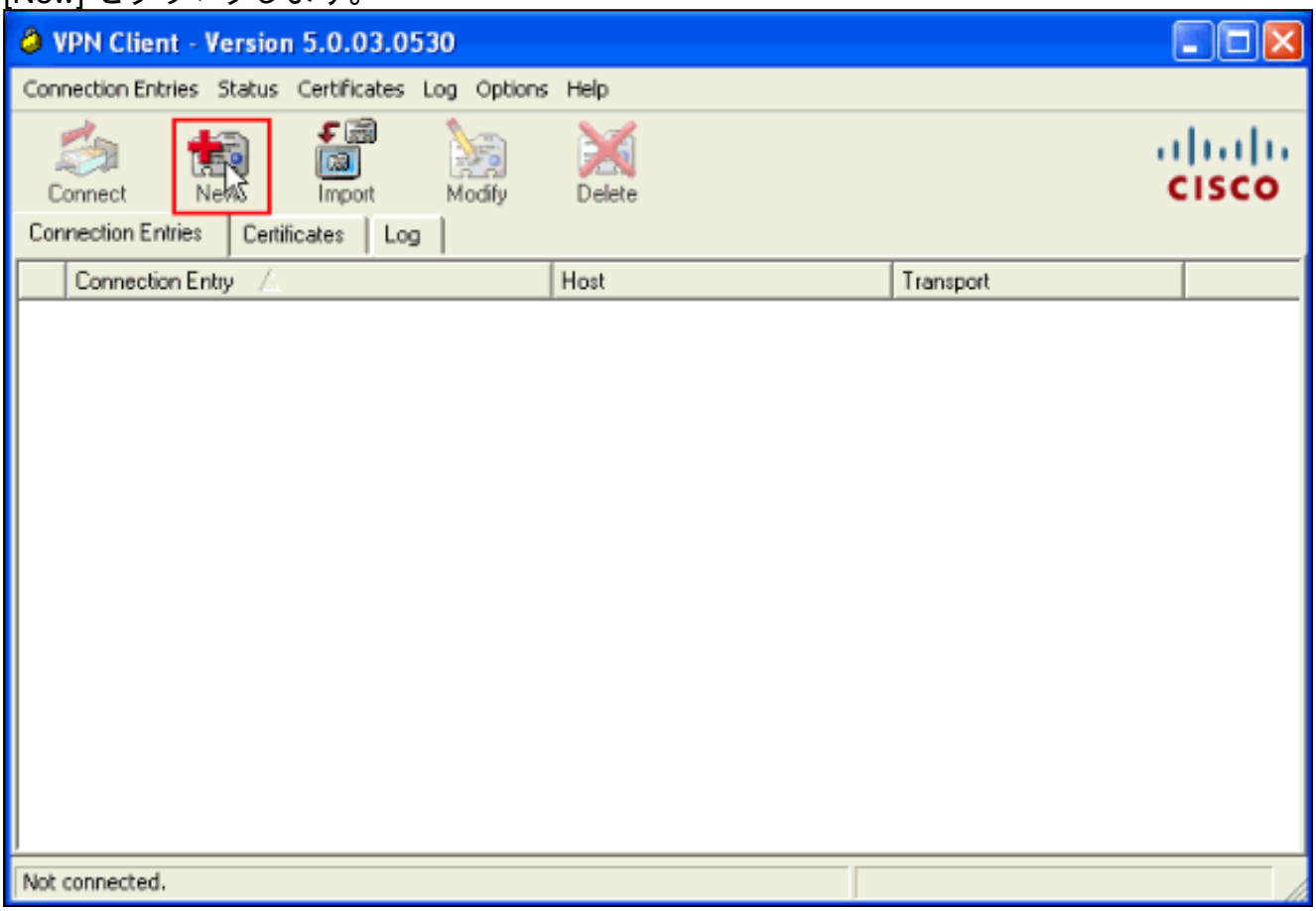
```
192.168.1.0 255.255.255.0 outside nat (inside) 0 access-
list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable no snmp-server location no snmp-server
contact !--- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto
ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP
65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto
map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map
interface Outside crypto isakmp enable Outside !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and !--- Policy
details are hidden as the default values are chosen.
crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 2 lifetime 86400 crypto
isakmp policy 30 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 telnet timeout 5 ssh
timeout 60 console timeout 0 management-access inside
threat-detection basic-threat threat-detection
statistics access-list group-policy cisco internal
group-policy cisco attributes vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 0 username
cisco attributes vpn-group-policy cisco tunnel-group
cisco type remote-access tunnel-group cisco general-
attributes address-pool vpnpool default-group-policy
cisco !--- Specifies the pre-shared key "cisco123" which
must !--- be identical at both peers. This is a global
!--- configuration mode command. tunnel-group cisco
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns migrated_dns_map_1
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
migrated_dns_map_1 inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end
ciscoasa#
```

確認

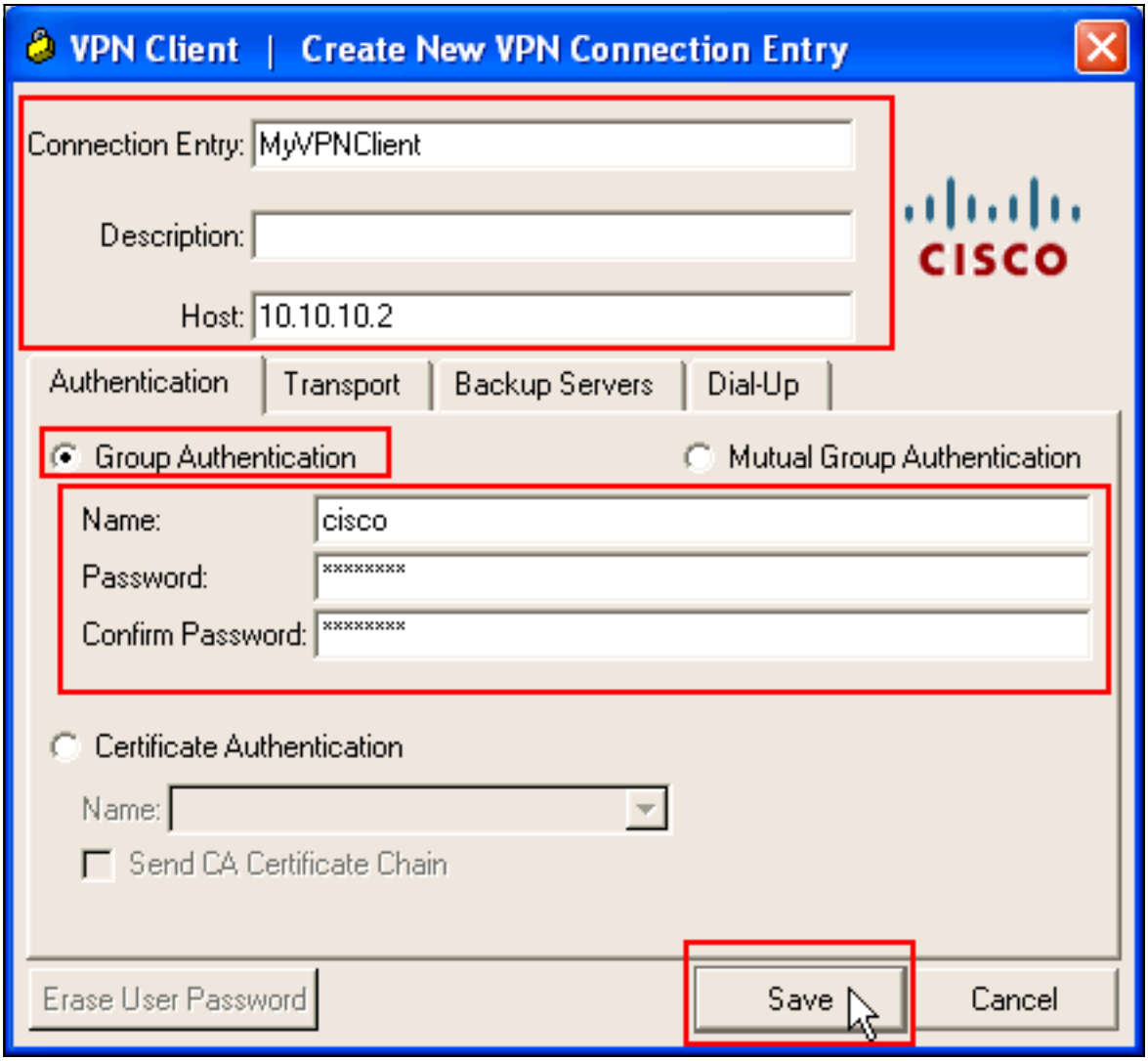
ASA の設定に成功したことを検証するには、Cisco VPN Client を使用して Cisco ASA に接続して

みます。

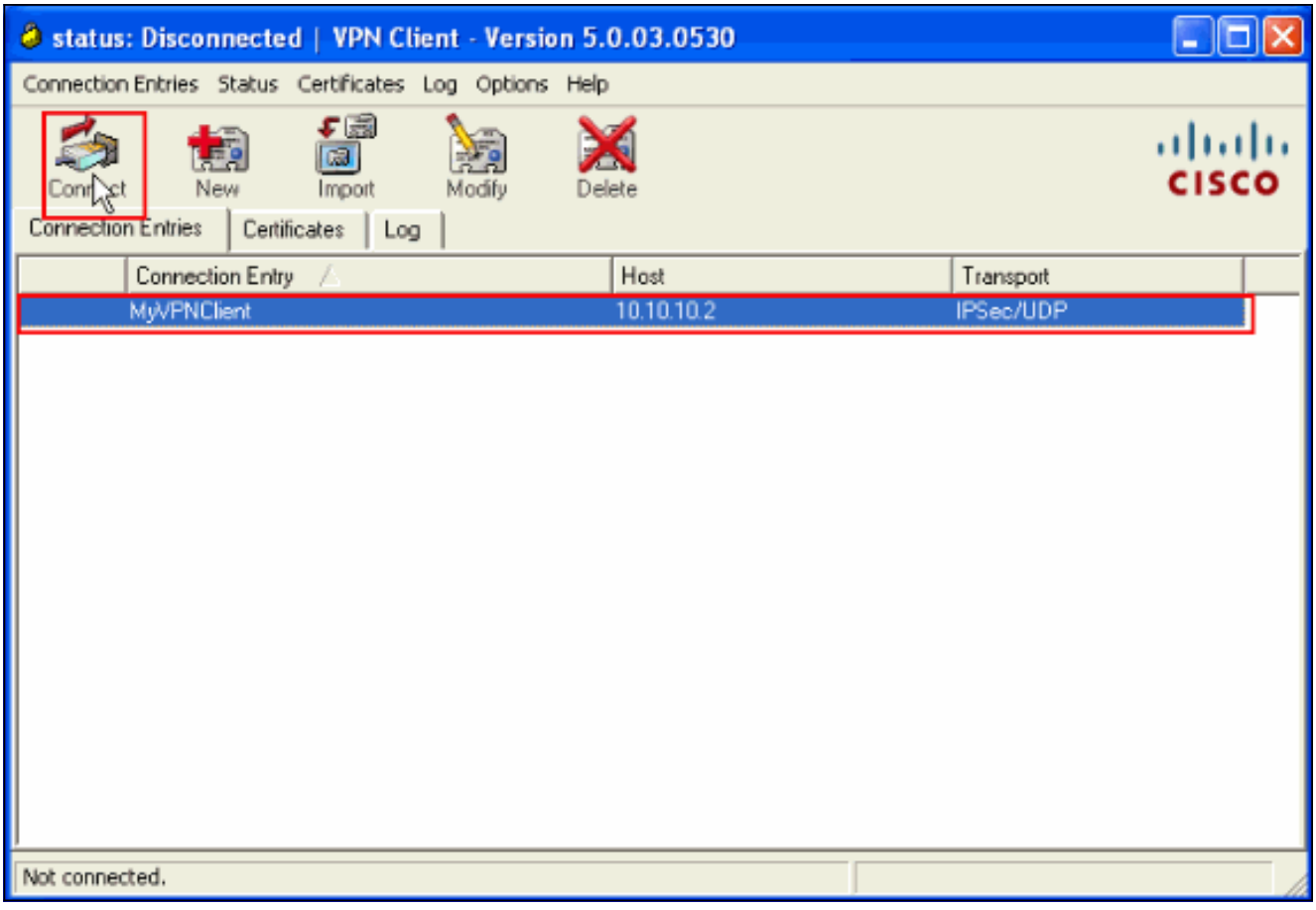
1. [New] をクリックします。



2. 新しい接続の詳細情報を入力します。[Host] フィールドには、設定済みの Cisco ASA の IP アドレスまたはホスト名が含まれている必要があります。 グループ認証情報は、ステップ 4 で使用した情報と一致している必要があります。 終了したら、[Save] をクリックします。

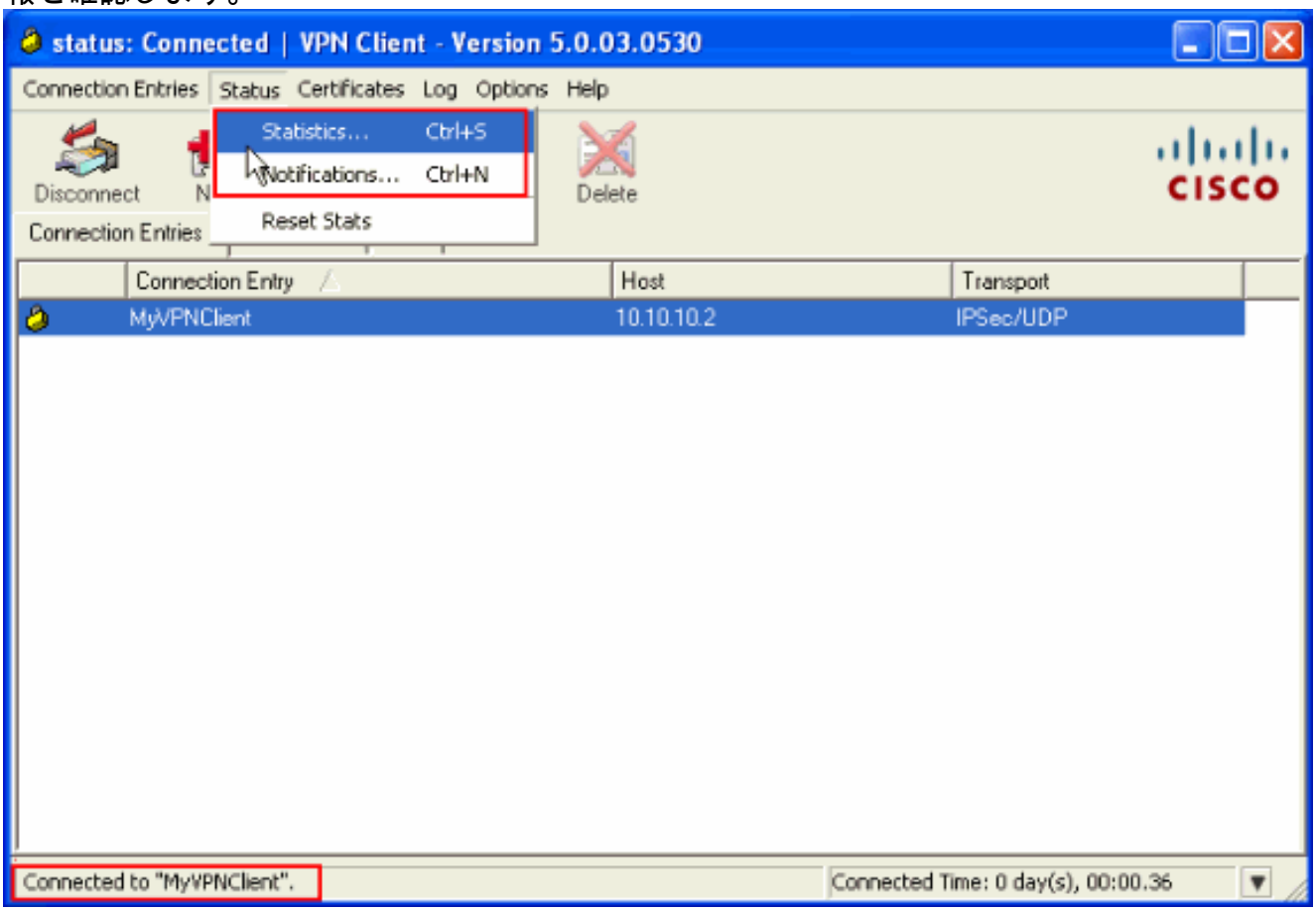


3. 新しく作成した接続を選択し、**Connect** をクリックします。

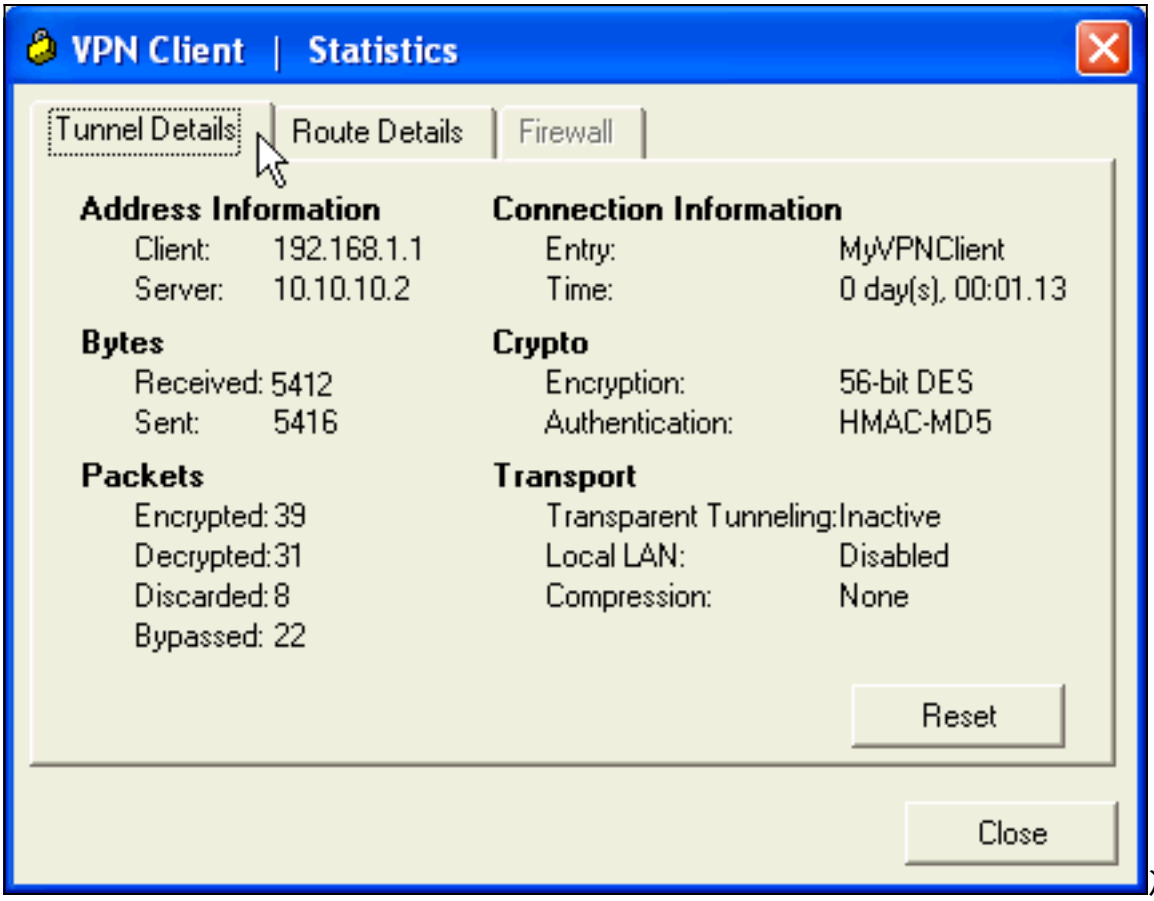


4. 拡張認証用のユーザ名とパスワードを入力します。 この情報は、**ステップ 5 と 6** で指定した情報と一致している必要があります。

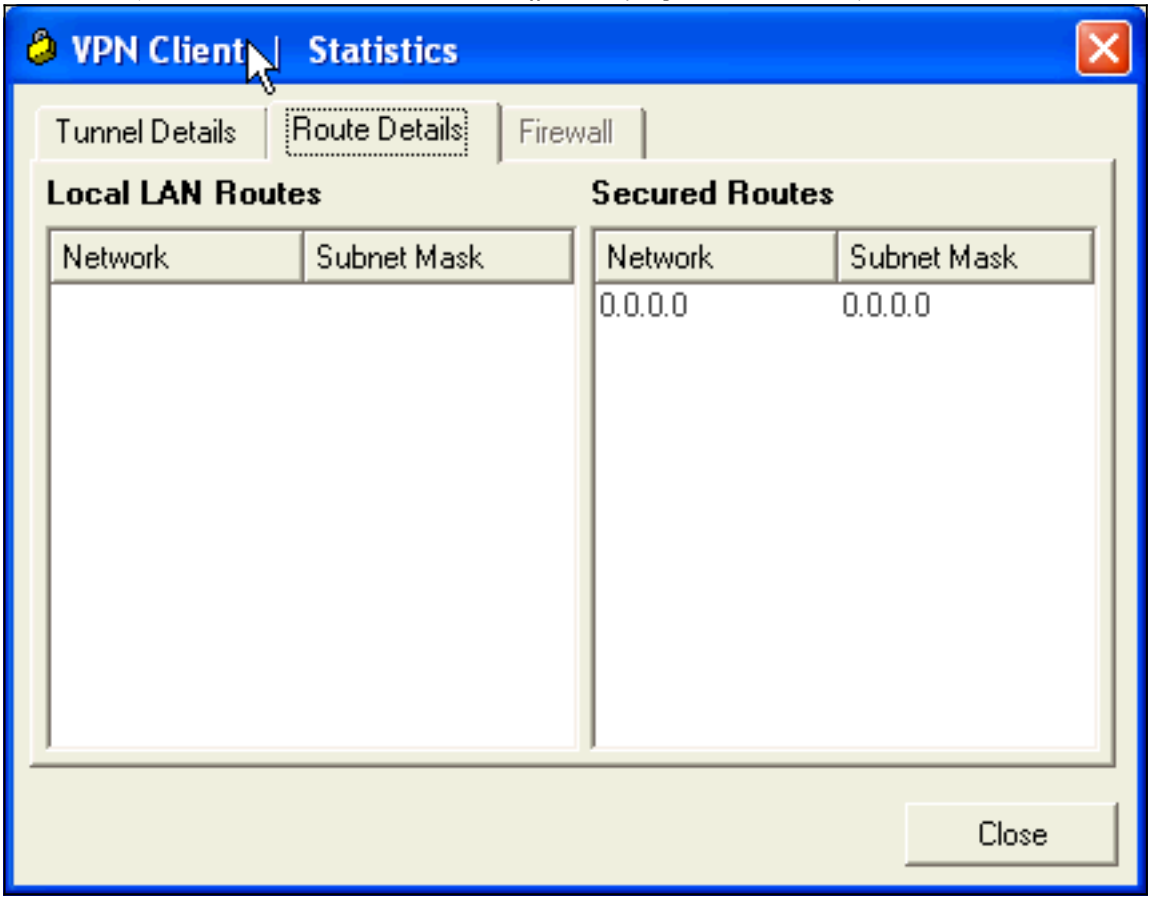
5. 接続が正常に確立されたら、[Status] メニューから [Statistics] を選択し、トンネルの詳細情報を確認します。



次のウィンドウには、トラフィックと暗号の情報が表示されています。



次のウィンドウには、スプリット トンネリング情報が表示されています。



ASA/PIX セキュリティ アプライアンス - show コマンド

- **show crypto isakmp sa**：現在ピアにあるすべての IKE SA を表示します。`ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during`

rekey) Total IKE SA: 1 1 IKE Peer: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE

- **show crypto ipsec sa**：現在ピアにあるすべての IPSec SA を表示します。ASA#**show crypto ipsec sa** interface: Outside **Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 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: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0** #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 **local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1** path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#**debug icmp trace** *!--- Inbound Nat Translation is shown below for Outside to Inside* **ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1** ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 *!--- Inbound Nat Translation is shown below for Inside to Outside* **ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768** ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

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。

サイト間 VPN のトラブルシューティングの詳細については、「一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング ソリューション」を参照してください。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）のトラブルシューティングとアラート
- テクニカルサポートとドキュメント - Cisco Systems