ASA 8.X：トンネリングされたデフォルト ゲートウェイを使用した SSL VPN トラフィック ルーティングの設定例

内容

概要

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）を設定して、トンネリングされたデフォルト ゲートウェイ（TDG）を経由するように SSL VPN トラフィックをルーティングする方法について説明します。 tunneled オプションを使用してデフォルト ルートを作成すると、ASA で終端しているトンネルからのトラフィックで、学習されたルートまたはスタティック ルートのいずれを使用してもルーティングできないトラフィックは、すべてこのルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- バージョン 8.x が稼働する ASA
- Cisco SSL VPN Client（SVC）1.x**注：SSL VPN Clientパッケージ**(sslclient-win*.pkg)をCisco Software Download（登録ユーザ専用）からダウンロードしてください。 SVC を ASA のフラッシュ メモリにコピーします。ASA との SSL VPN 接続を確立するには、リモート ユーザのコンピュータに SVC をダウンロードする必要があります。

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。

- ソフトウェア バージョン 8.x が稼働している Cisco 5500 シリーズ ASA
- Windows 1.1.4.179 用のバージョンの Cisco SSL VPN Client
- Windows 2000 Professional または Windows XP が稼働している PC
- Cisco Adaptive Security Device Manager（ASDM）バージョン 6.1(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。

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

SSL VPN Client（SVC）は、ネットワーク管理者によるリモート コンピュータへの IPSec VPN クライアントのインストールおよび設定を必要とせずに、リモート ユーザに IPSec VPN クライアントのメリットを提供する VPN トンネリング技術です。SVC は、リモート コンピュータに既存の SSL 暗号化およびセキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

現在のシナリオでは、SSL VPN トンネルを経由して ASA の背後にある内部リソースに接続する SSL VPN クライアントが存在します。スプリットトンネルはイネーブルではありません。SSL VPN クライアントが ASA に接続しているときは、すべてのデータがトンネリングされます。主な基準は、内部リソースへのアクセスに加えて、このトンネリングされたトラフィックを Default Tunneled Gateway（DTG）を経由してルーティングすることです。

標準のデフォルト ルートに加えて、トンネル トラフィック用に別のデフォルト ルートを定義できます。ASA が受信した暗号化されていないトラフィック（スタティック ルートも学習されたルートも存在しないもの）は、標準のデフォルト ルートを経由してルーティングされます。ASA が受信した暗号化されているトラフィック（スタティック ルートも学習されたルートも存在しないもの）は、トンネリングされたデフォルト ルートを使用して定義された DTG に渡されます。

トンネリングされたデフォルト ルートを定義するには、次のコマンドを使用します。

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

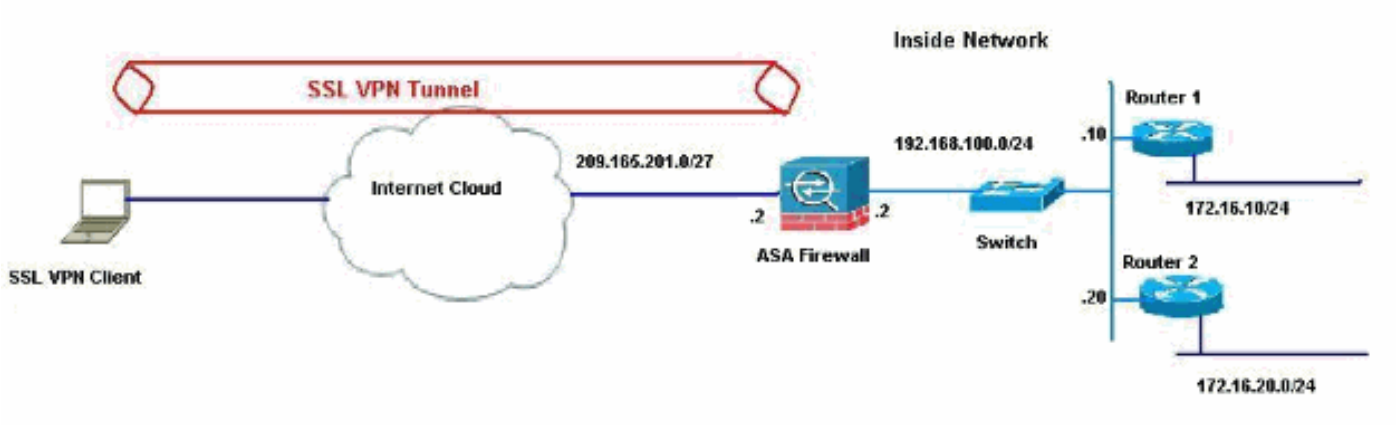
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

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 セットアップを使用します。



この例では、SSL VPN クライアントはトンネル経由で ASA の内部ネットワークにアクセスします。スプリットトンネルは設定されていないため、内部ネットワーク以外に送信されるトラフィックもトンネリングされ、TDG (192.168.100.20) 経由でルーティングされます。

パケットが TDG (この例ではルータ 2) にルーティングされた後は、これらのパケットをインターネットにルーティングするためのアドレス変換が実行されます。インターネット ゲートウェイとしてのルータ設定の詳細については、「Cisco 製ではないケーブル モデムに接続された Cisco ルータの設定方法」を参照してください。

ASDM 6.1(5) を使用した ASA 設定

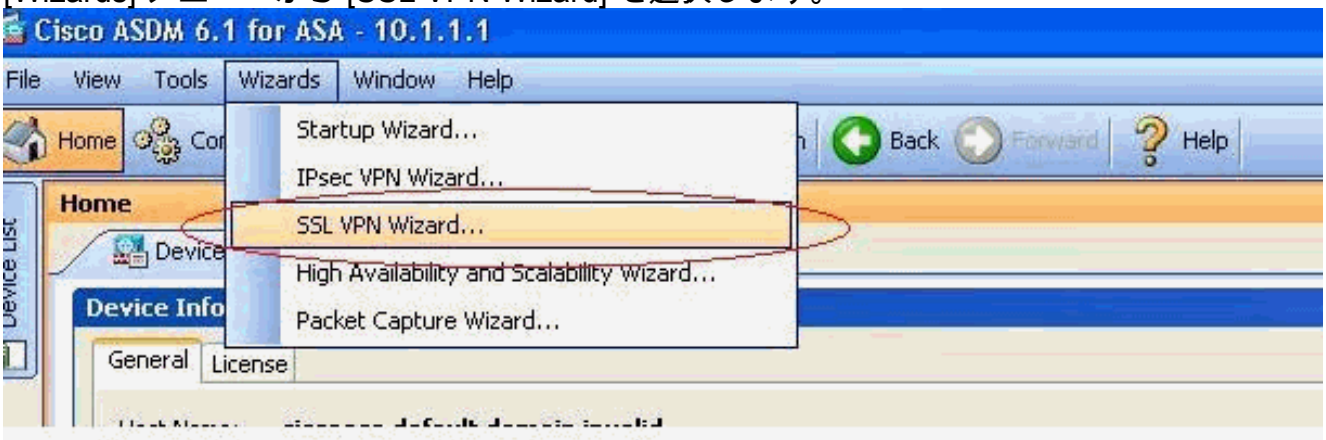
このドキュメントは、インターフェイス設定などの基本設定がすでに行われていて適切に動作していることを前提としています。

注：ASDMでASAを設定する方法については、『ASDMでのHTTPSアクセスの許可』を参照してください。

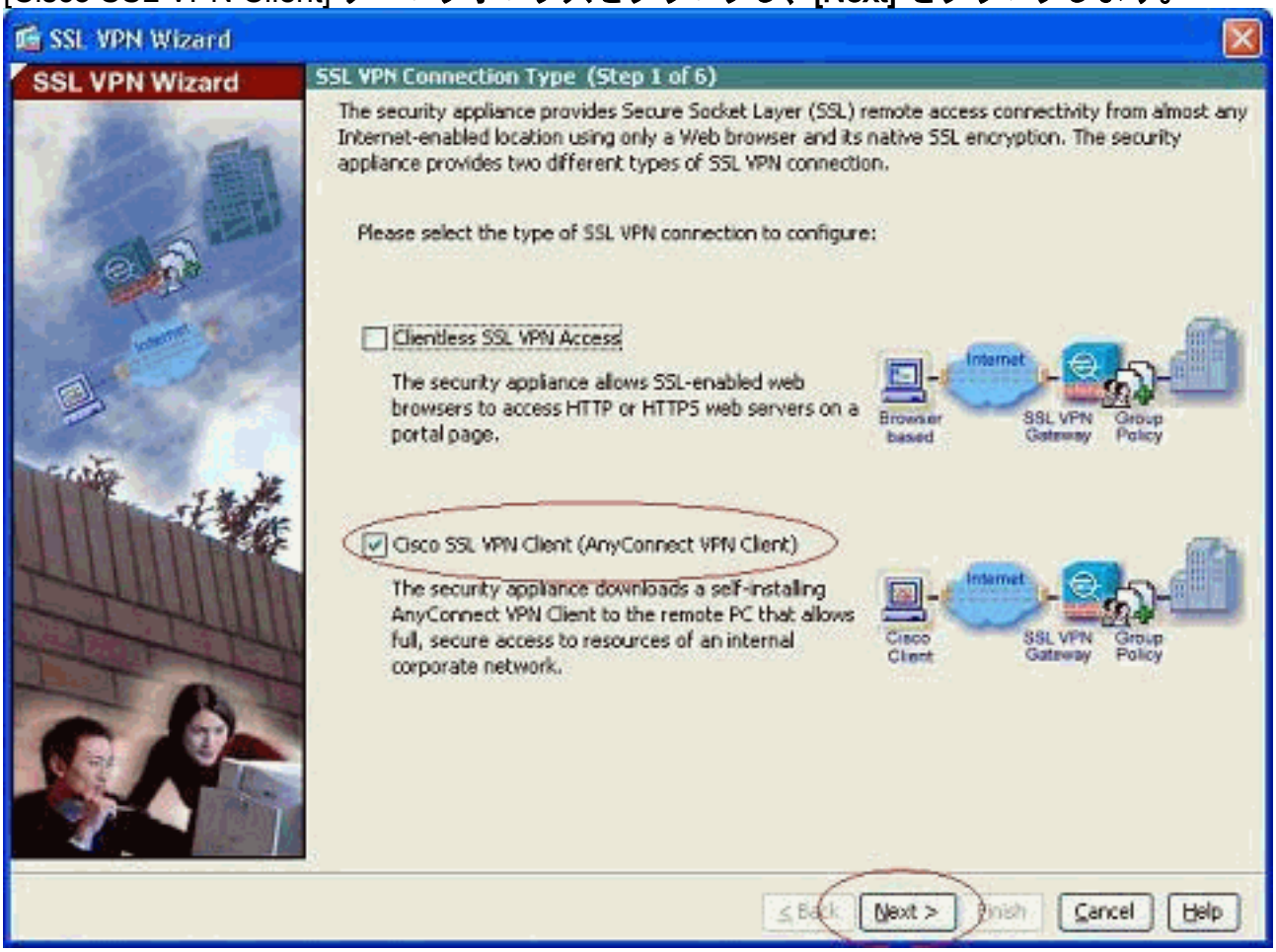
注：ポート番号を変更しない限り、WebVPNとASDMを同じASAインターフェイスで有効にすることはできません。詳細は、「ASA の同じインターフェイスでイネーブルになる ASDM および WebVPN」を参照してください。

SSL VPN ウィザードを使用して SSL VPN を設定するには、次の手順を実行します。

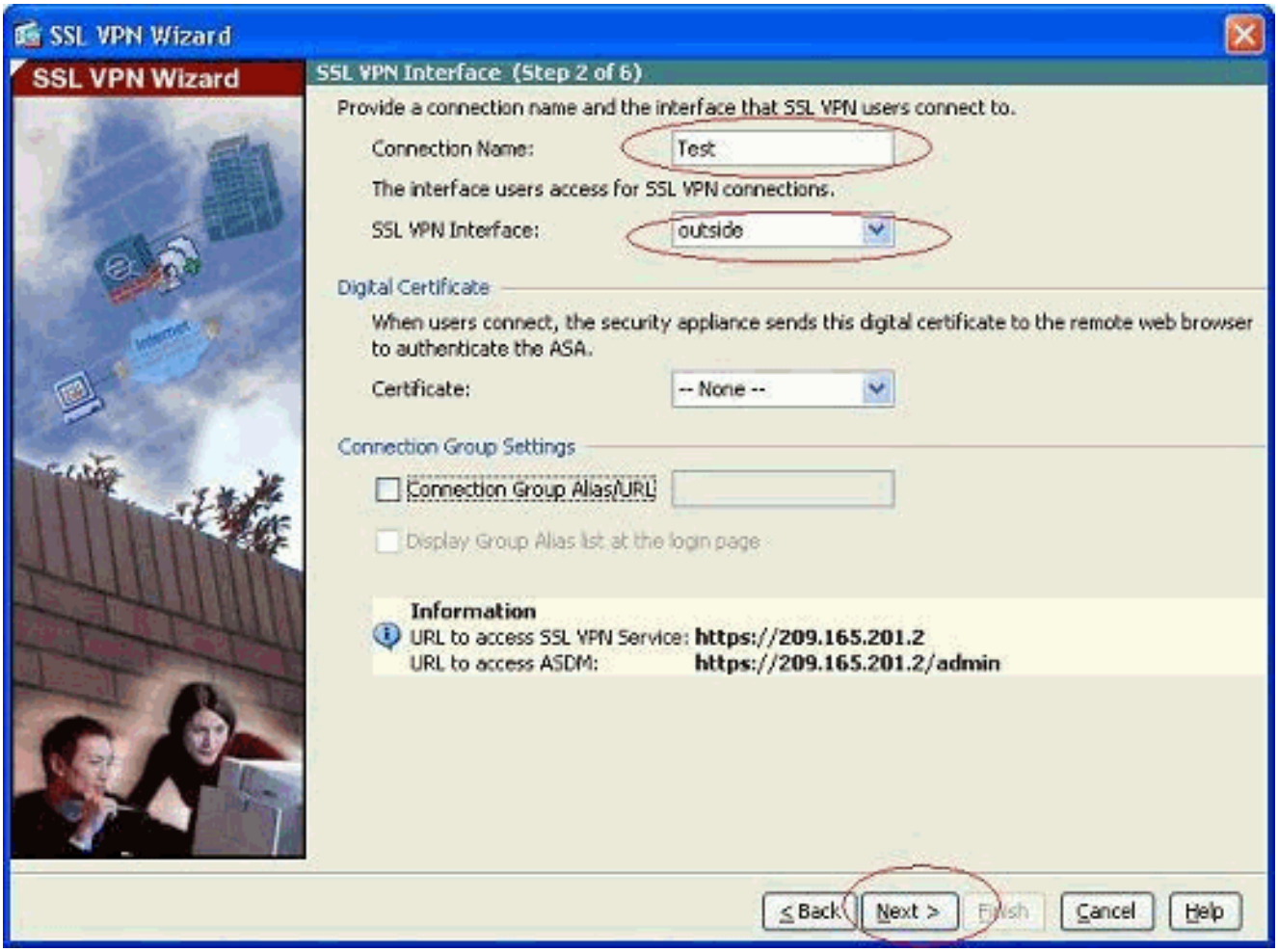
1. [Wizards] メニューから [SSL VPN Wizard] を選択します。



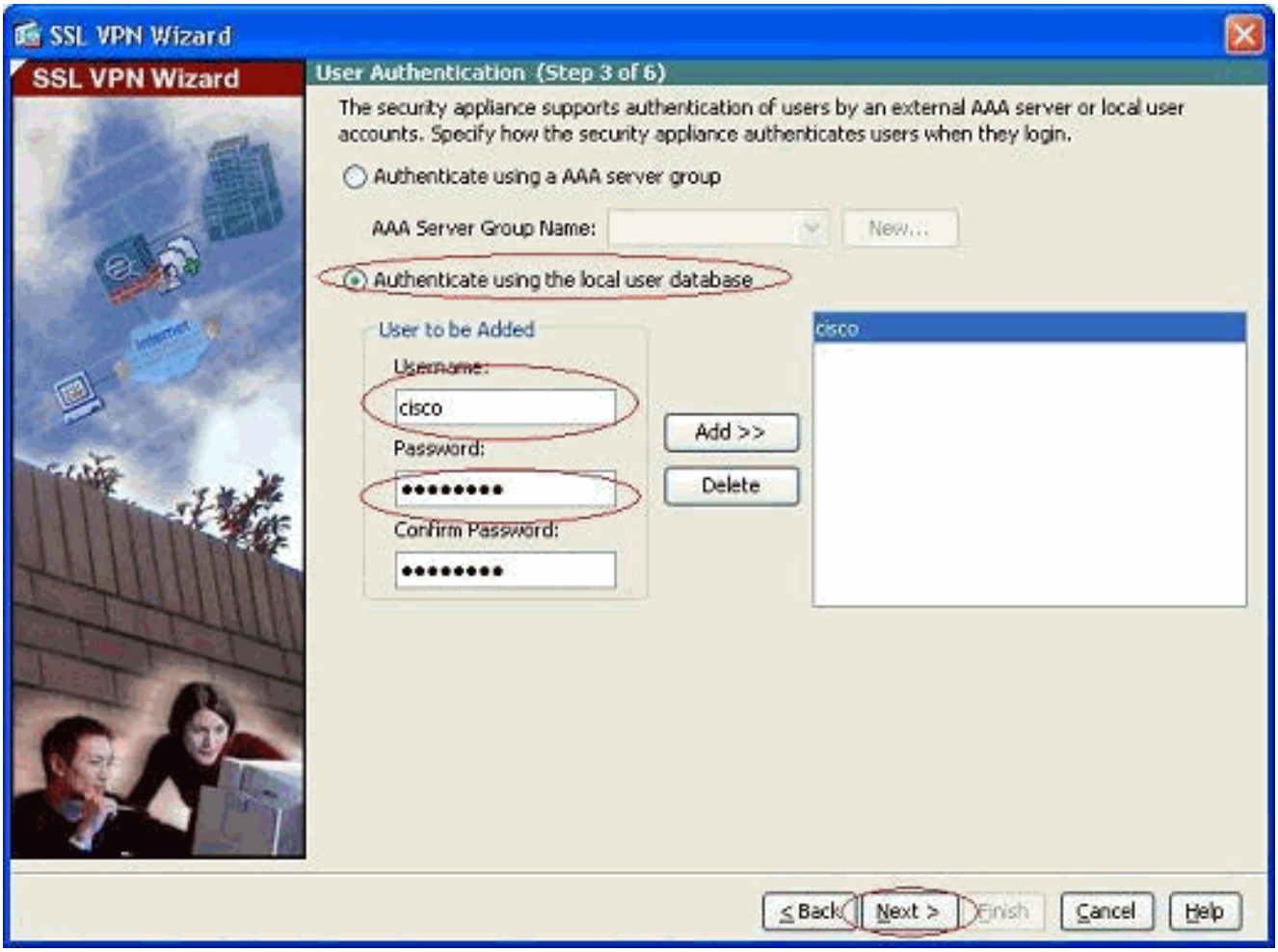
2. [Cisco SSL VPN Client] チェックボックスをクリックし、[Next] をクリックします。



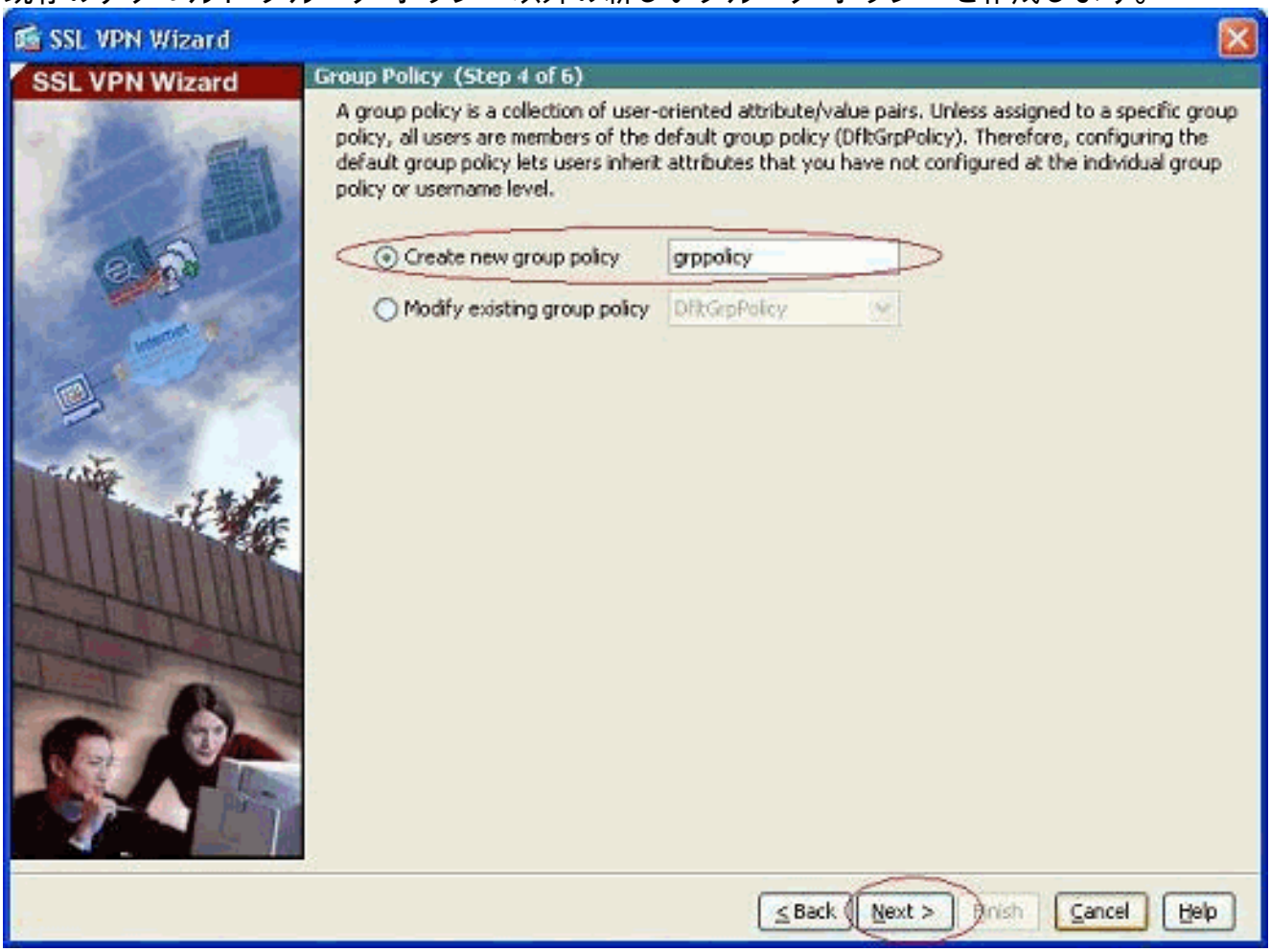
3. [Connection Name] フィールドに接続の名前を入力して、ユーザが SSL VPN へのアクセスに使用しているインターフェイスを [SSL VPN Interface] ドロップダウン リストから選択します。



4. [next] をクリックします。
5. 認証モードを選択し、[Next] をクリックします。（この例では、ローカル認証を使用しています。
   ）

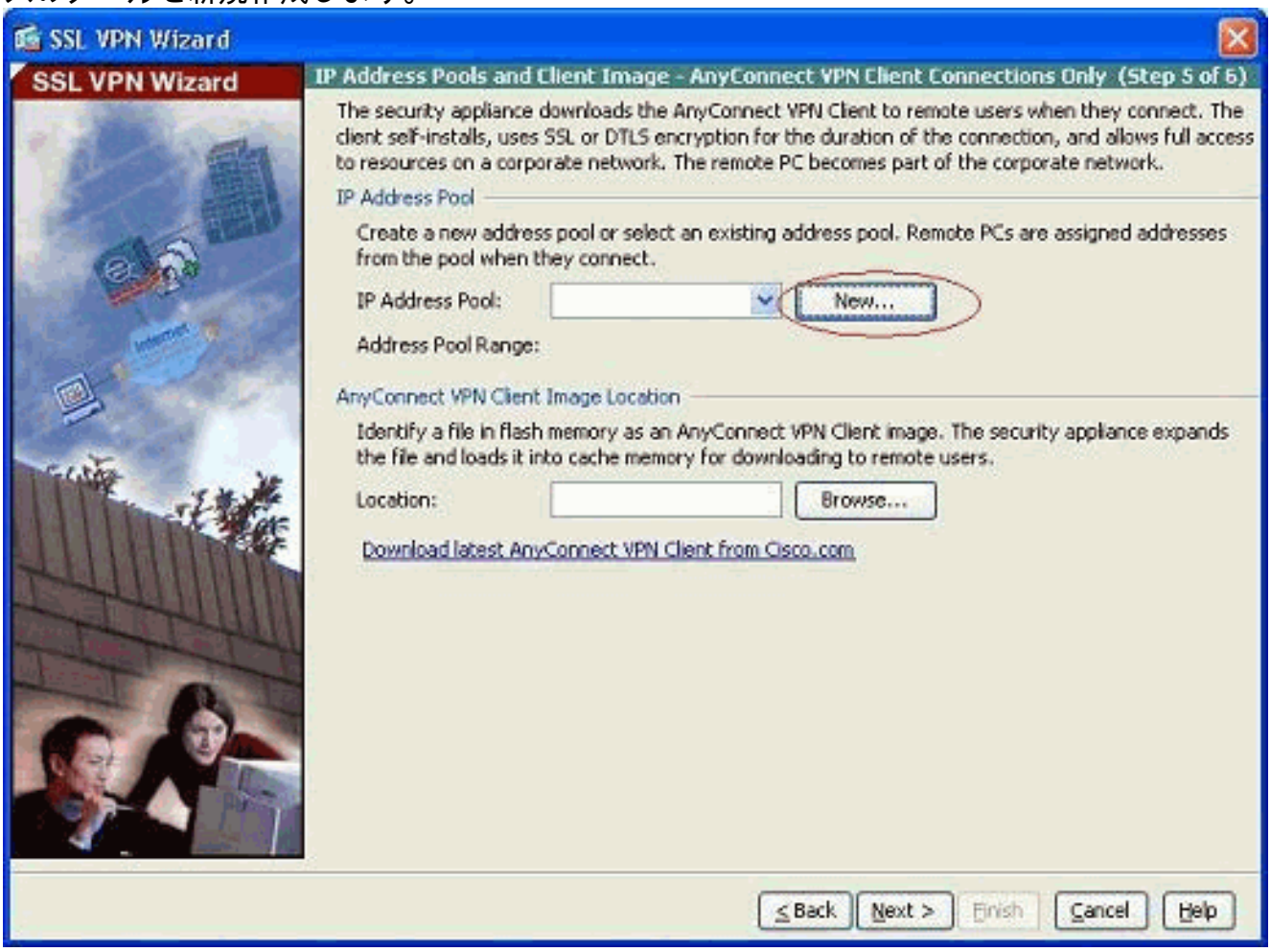


6. 既存のデフォルト グループ ポリシー以外の新しいグループ ポリシーを作成します。

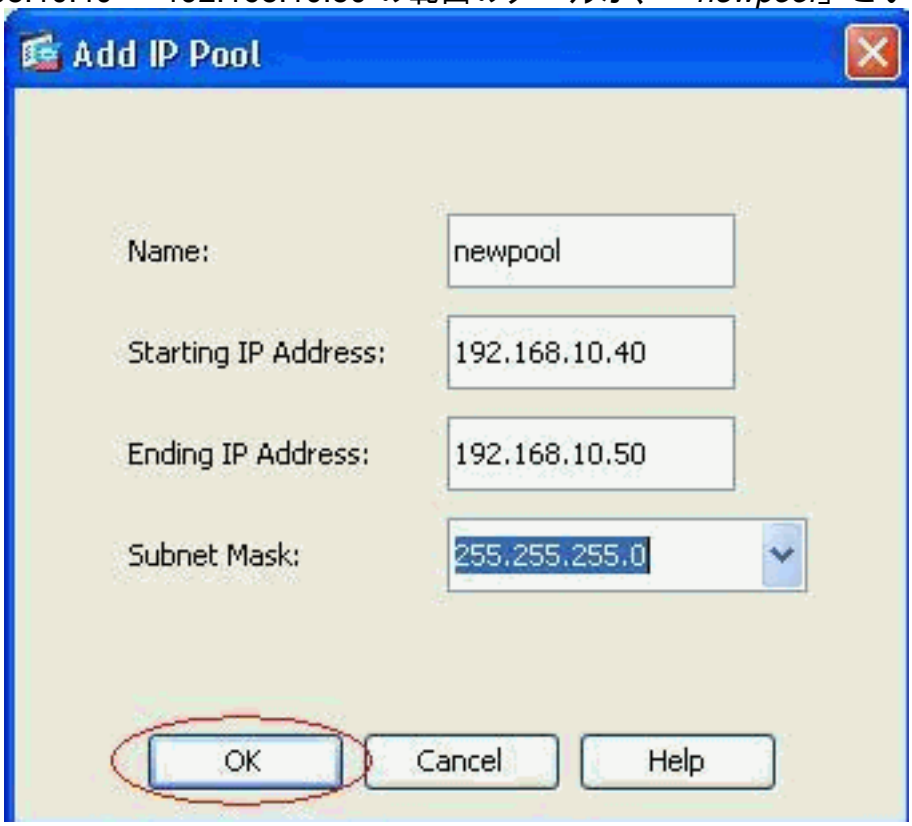


7. SSL VPN クライアント PC の接続が確立したときにこれらの PC に割り当てられるアドレ

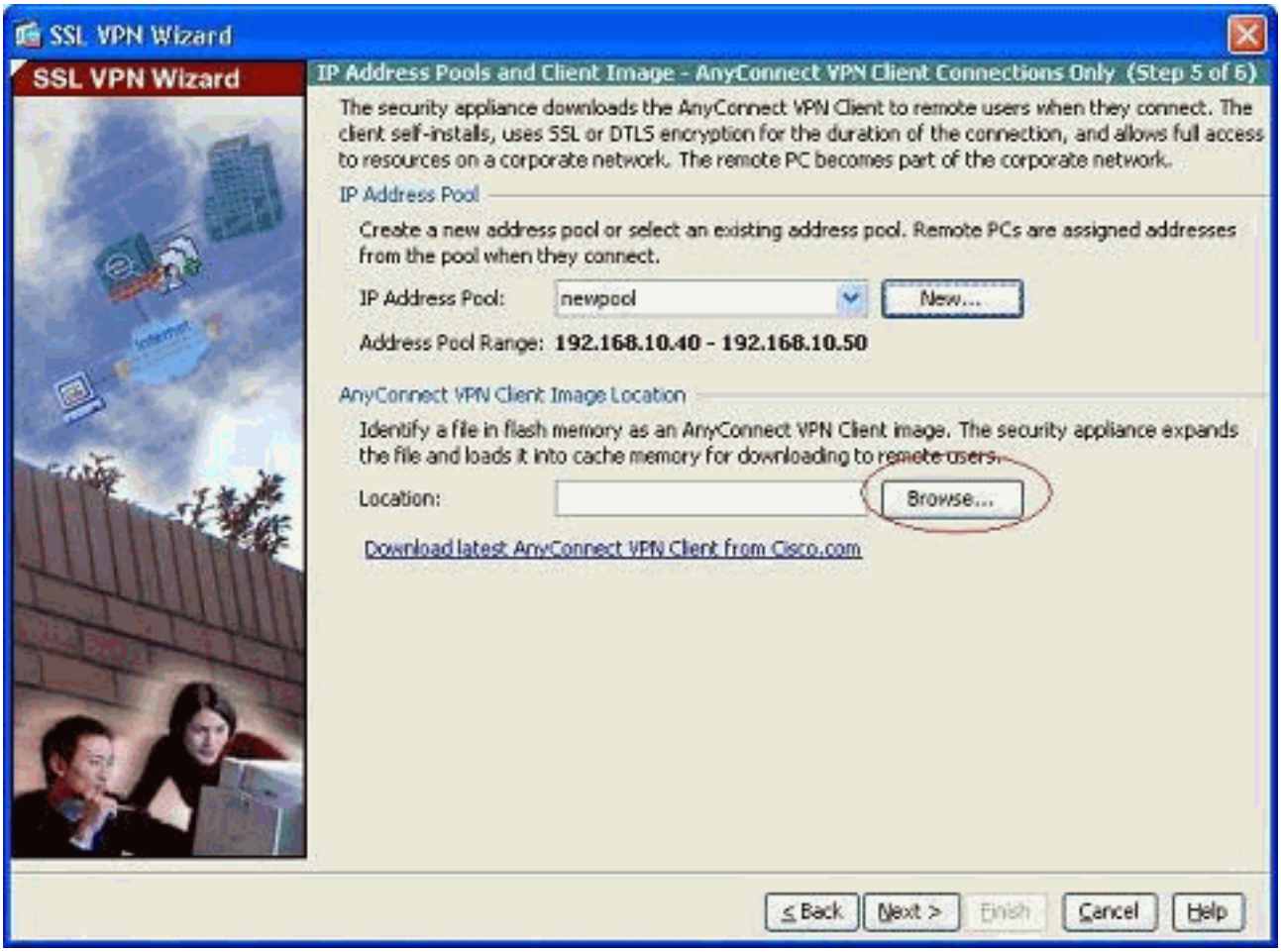
スのプールを新規作成します。



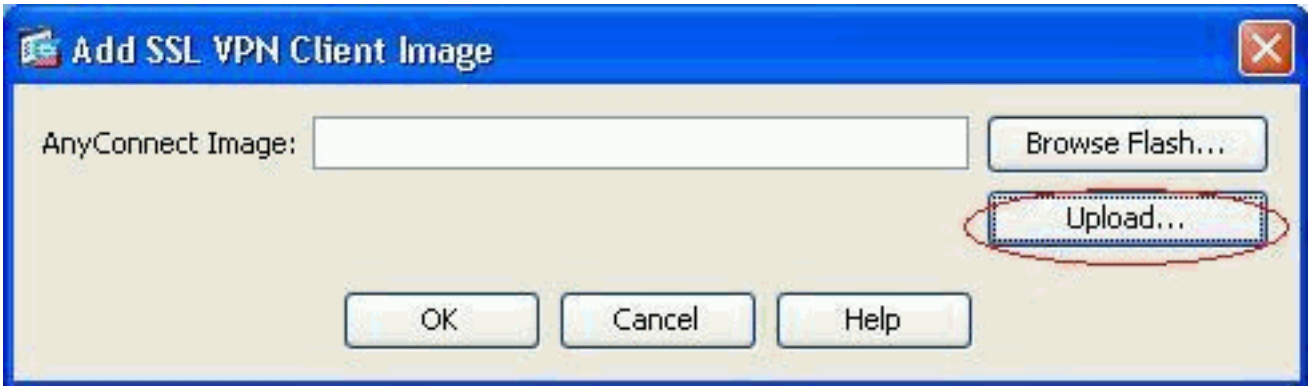
192.168.10.40 ~ 192.168.10.50 の範囲のプールが、「*newpool*」という名前で作成されました。



8. [Browse] をクリックし、SSL VPN クライアント イメージを選択して ASA のフラッシュ メモリにアップロードします。

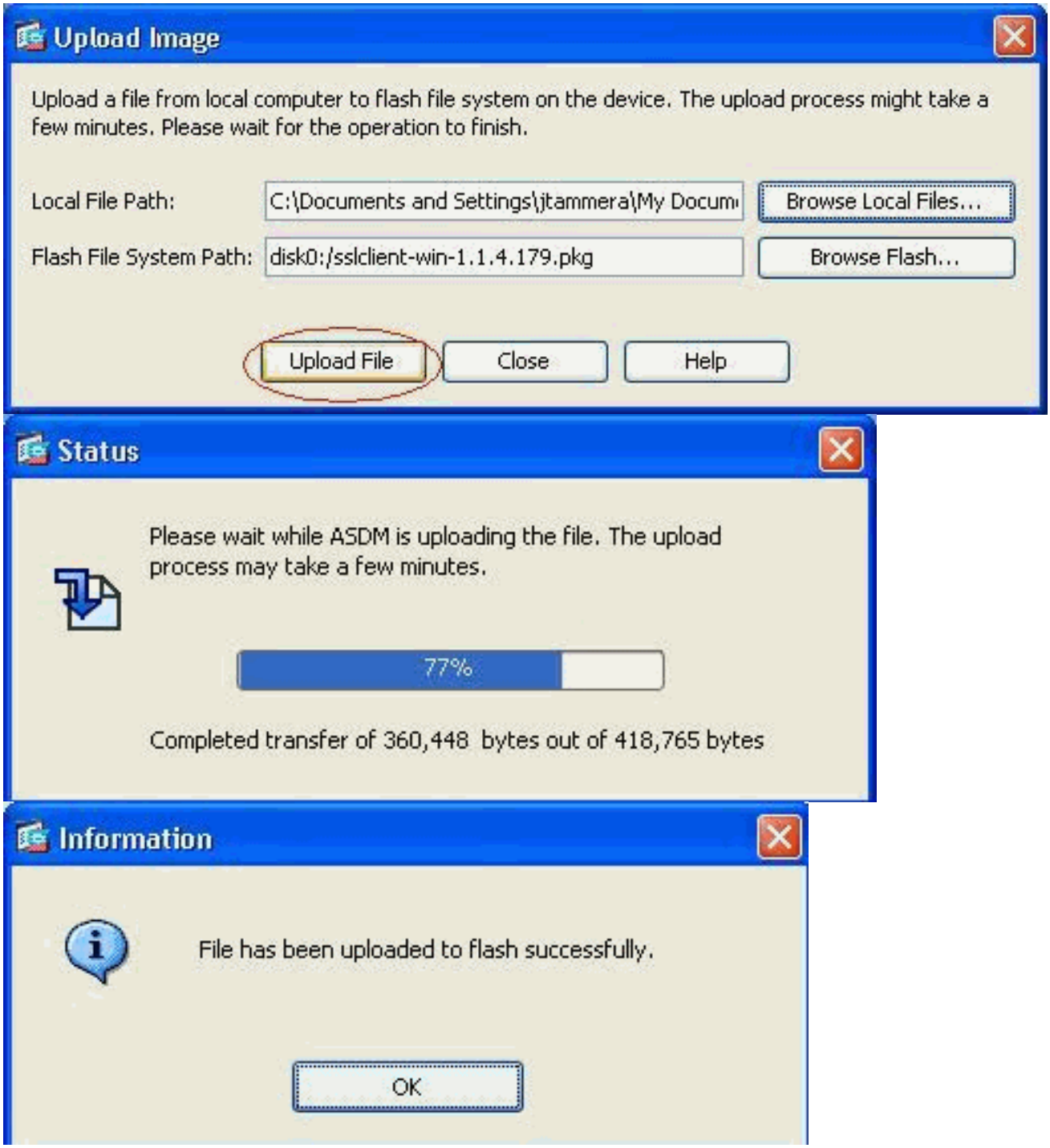


9. [Upload] をクリックして、マシンのローカル ディレクトリのファイルのパスを設定します。



10. [Browse Local Files] をクリックして、sslclient.pkg ファイルが存在するディレクトリを選択します。

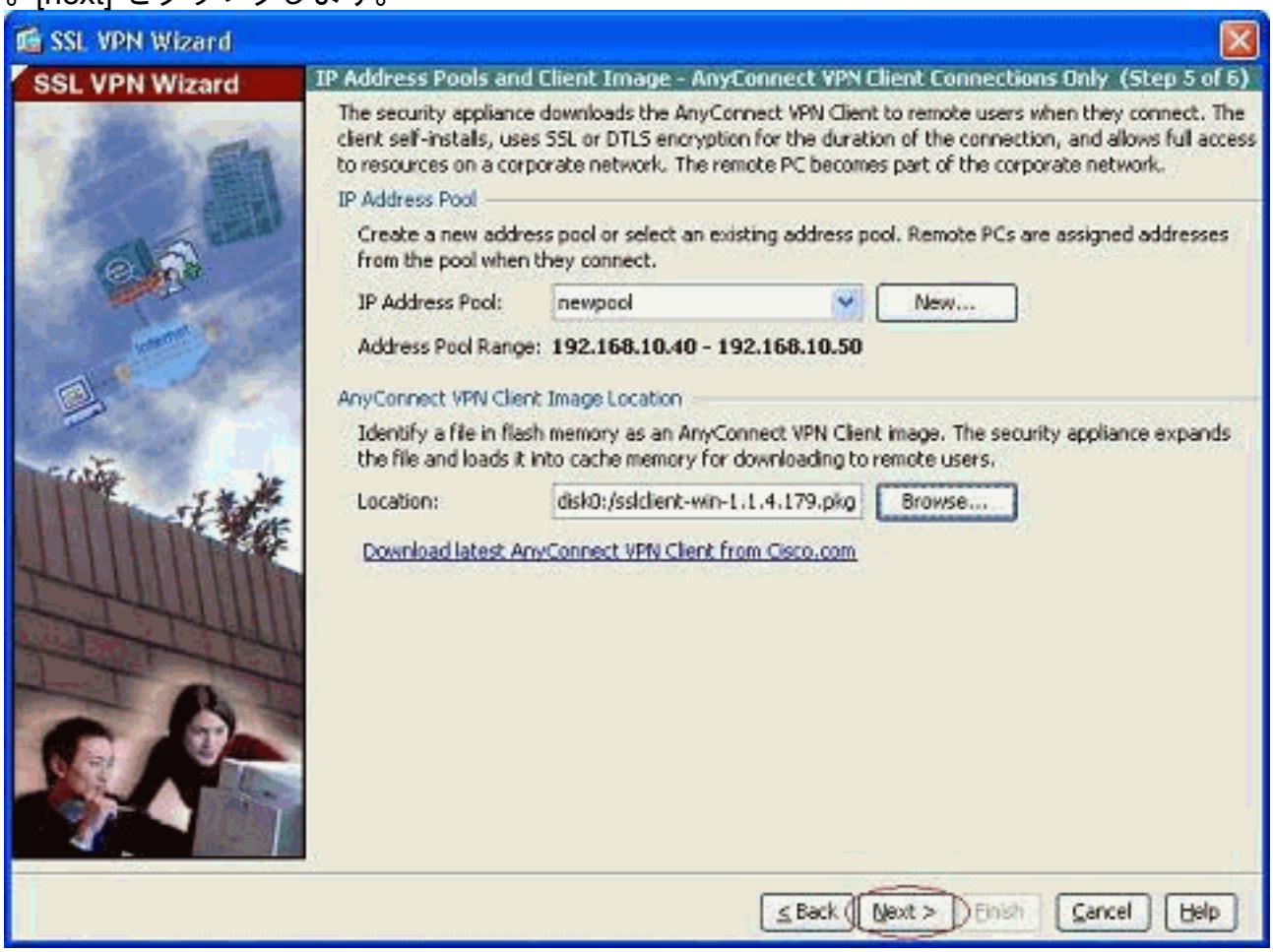
11. [Upload File] をクリックして、選択したファイルを ASA のフラッシュにアップロードします。



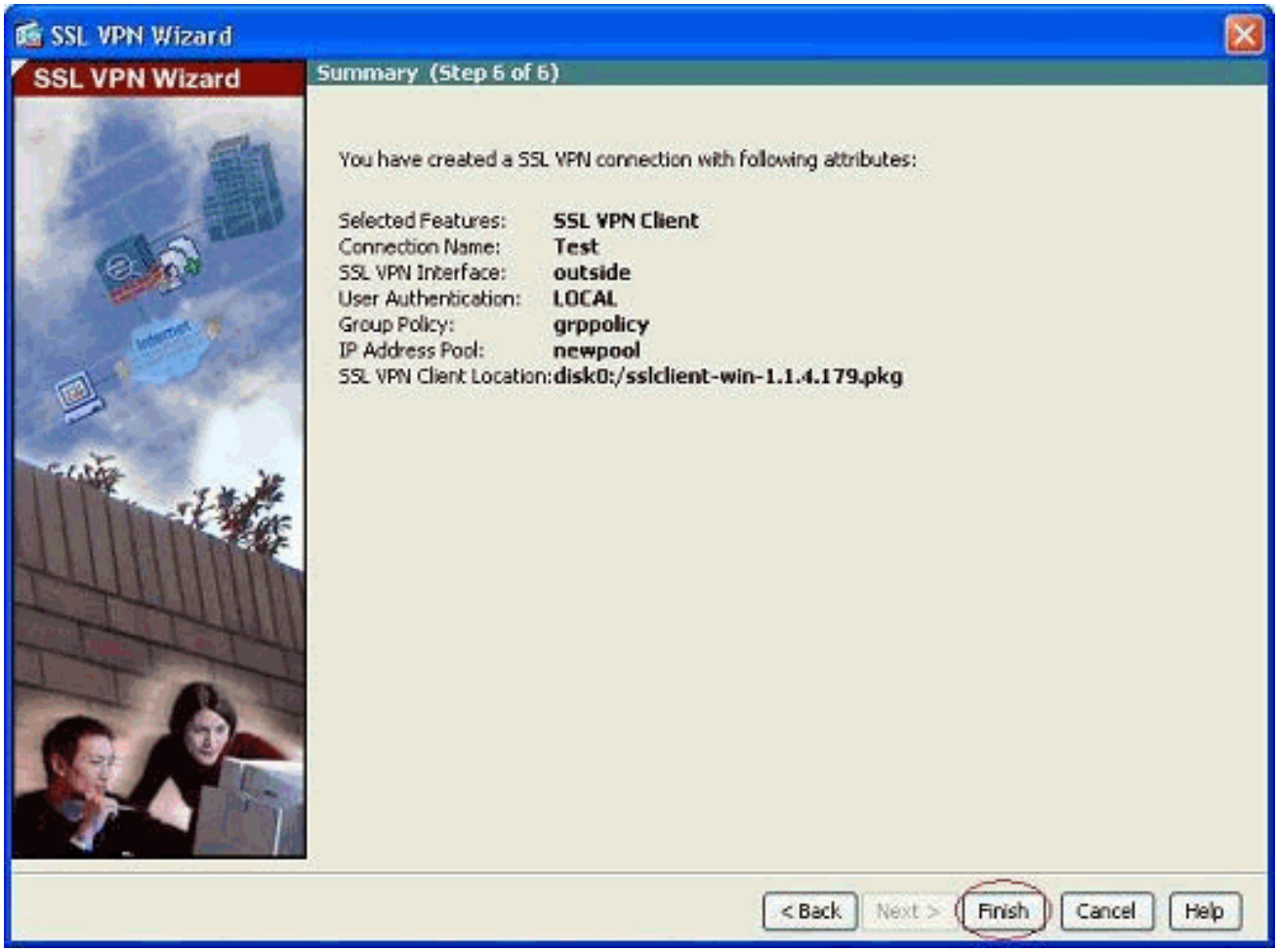
12. ファイルが ASA のフラッシュにアップロードされたら、[OK] をクリックしてタスクを完了します。

13. ASA のフラッシュにアップロードされた最新の anyconnect pkg ファイルが表示されます

。[next] をクリックします。



14. SSL VPN クライアントの設定の要約が表示されます。[Finish] をクリックしてウィザードを完了します。



ASDM に表示された設定は、主に SSL VPN クライアントのウィザード設定に関係があります。

CLI では、追加の設定の一部を確認できます。次に CLI の設定のすべてを示します。重要なコマンドは強調表示されています。

CiscoASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.2 255.255.255.0
!
interface Ethernet0/2
 nameif manage
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/3
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list nonat extended permit ip 192.168.100.0
255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0
!--- ACL to define the traffic to be exempted from NAT.
no pager logging enable logging asdm informational mtu
outside 1500 mtu inside 1500 mtu manage 1500 !---
Creating IP address block to be assigned for the VPN
clients ip local pool newpool 192.168.10.40-
192.168.10.50 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!--- Default route is configured through "inside"
interface for normal traffic. route inside 0.0.0.0
0.0.0.0 192.168.100.20 tunneled
!--- Tunneled Default route is configured through
"inside" interface for encrypted traffic ! 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
!--- Configuring the ASA as HTTP server. http 10.1.1.0
255.255.255.0 manage
!--- Configuring the network to be allowed for ASDM
access. ! !--- Output is suppressed ! telnet timeout 5
ssh timeout 5 console timeout 0 threat-detection basic-
threat threat-detection statistics access-list ! class-
map inspection_default match default-inspection-traffic
! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map 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 ! !--- Output suppressed !
webvpn
 enable outside
!--- Enable WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1
!--- Assign the AnyConnect SSL VPN Client image to be
used svc enable
!--- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal
!--- Create an internal group policy "grppolicy" group-
policy grppolicy attributes
 VPN-tunnel-protocol svc
!--- Specify SSL as a permitted VPN tunneling protocol !
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 15
!--- Create a user account "cisco" tunnel-group Test
type remote-access
!--- Create a tunnel group "Test" with type as remote
access tunnel-group Test general-attributes
 address-pool newpool
!--- Associate the address pool vpnpool created default-
group-policy grppolicy
!--- Associate the group policy "clientgroup" created
prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

確認

このセクションで説明するコマンドは、設定の確認に使用できます。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show webvpn svc**：ASA フラッシュ メモリに格納された SVC イメージを表示します。
- **show VPN-sessiondb svc ：現在の SSL 接続についての情報を表示します。**

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート
- 公衆インターネット VPN on a Stick のための PIX/ASA および VPN Client の設定例
- ASDM を使用した ASA での SSL VPN Client（SVC）の設定例
- テクニカル サポートとドキュメント – Cisco Systems