ASA 8.X: Distribuindo o tráfego SSL VPN com o exemplo em túnel da configuração de gateway de voz padrão

Índice

Introdução

Este documento descreve como configurar o Adaptive Security Appliance (ASA) para rotear o tráfego de SSL VPN através de um gateway padrão em túnel (TDG). Quando você cria uma rota padrão com a opção em túnel, todo o tráfego de um túnel que termina no ASA que não pode ser utilização distribuída aprendida ou em rotas estáticas está enviado a esta rota. Para o tráfego que emerge de um túnel, esta rota cancela todas as rotas padrão configuradas ou aprendidas outro.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- ASA que é executado na versão 8.x
- Cisco SSL VPN Client (SVC) 1.x**Nota:** Transfira o pacote do cliente VPN SSL (sslclient-win*.package) da transferência de software Cisco (clientes registrados somente). Copie o SVC à memória Flash no ASA. O SVC precisa de ser transferido aos computadores do usuário remoto a fim estabelecer a conexão de VPN SSL com o ASA.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5500 Series ASA que executa a versão de software 8.x
- Versão do Cisco SSL VPN Client para Windows 1.1.4.179
- PC que executa Windows 2000 Professional ou Windows XP
- Versão 6.1(5) do Cisco Adaptive Security Device Manager (ASDM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O cliente VPN SSL (SVC) é uma tecnologia de tunelamento VPN que dê a usuários remotos os benefícios de um cliente do IPSec VPN sem a necessidade para que os administradores de rede instalem e configurem clientes do IPSec VPN em computadores remotos. O SVC usa a criptografia SSL que está já atual no computador remoto assim como o início de uma sessão WebVPN e a autenticação da ferramenta de segurança.

Na encenação atual, há um cliente VPN SSL que conecta aos recursos internos atrás do ASA através do túnel SSL VPN. O túnel em divisão não é permitido. Quando o cliente VPN SSL é conectado ao ASA, todos os dados estarão escavados um túnel. Além de alcançar os recursos internos, o critério principal é distribuir este tráfego em túnel através do gateway escavado um túnel padrão (DTG).

Você pode definir uma rota padrão separada para o tráfego em túnel junto com a rota padrão padrão. O tráfego não criptografado recebido pelo ASA, para que há não estático ou uma rota aprendida, é distribuído através da rota padrão padrão. O tráfego criptografado recebido pelo ASA, para que há não estático ou uma rota aprendida, será passado ao DTG definido através da rota padrão em túnel.

A fim definir uma rota padrão em túnel, use este comando:

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

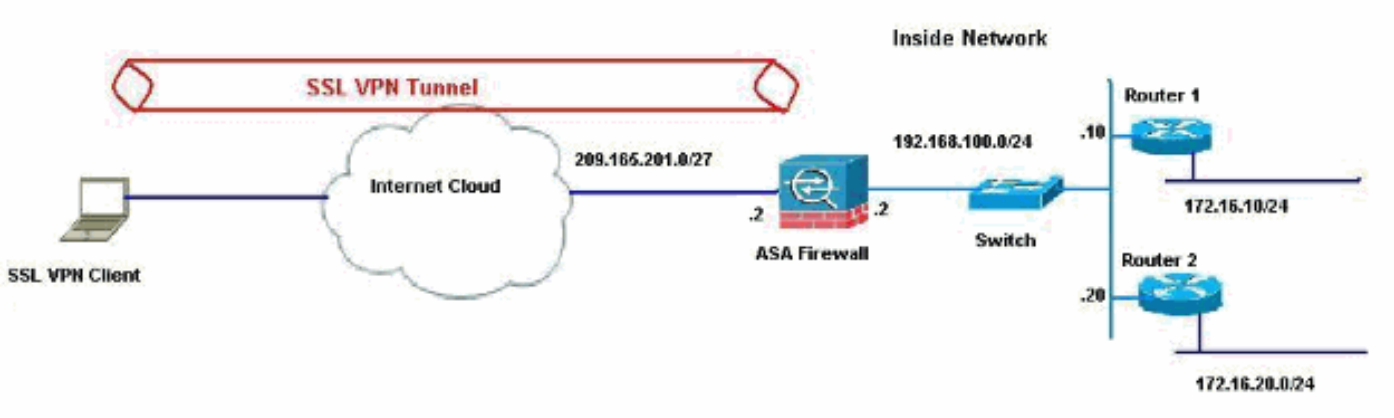
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Neste exemplo, os acessos de cliente VPN SSL a rede interna do ASA através do túnel. O tráfego significado para destinos diferentes da rede interna é escavado um túnel igualmente, porque não há nenhum túnel em divisão configurado, e distribuído com o TDG (192.168.100.20).

Depois que os pacotes são distribuídos ao TDG, que é roteador2 neste caso, executa a tradução de endereços para distribuir aqueles pacotes adiante ao Internet. Para obter mais informações sobre de configurar um roteador como um Gateway de Internet, refira como configurar um roteador Cisco atrás de um Cable Modem de terceiros.

Configuração ASA usando o ASDM 6.1(5)

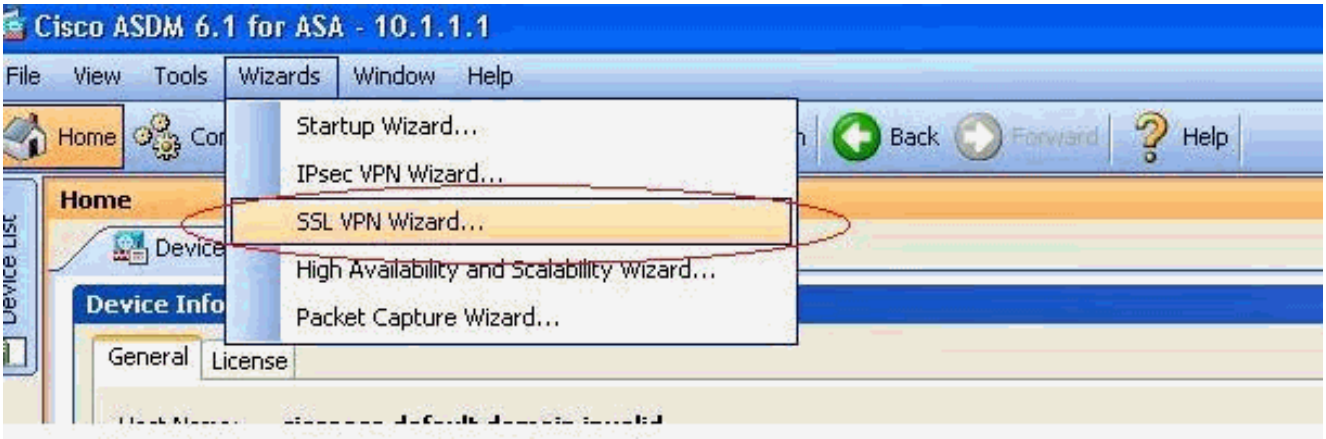
Este documento supõe as configurações básicas, tais como a configuração da interface, é completo e trabalho corretamente.

Nota: Refira permitir o acesso HTTPS para o ASDM para obter informações sobre de como permitir que o ASA seja configurado pelo ASDM.

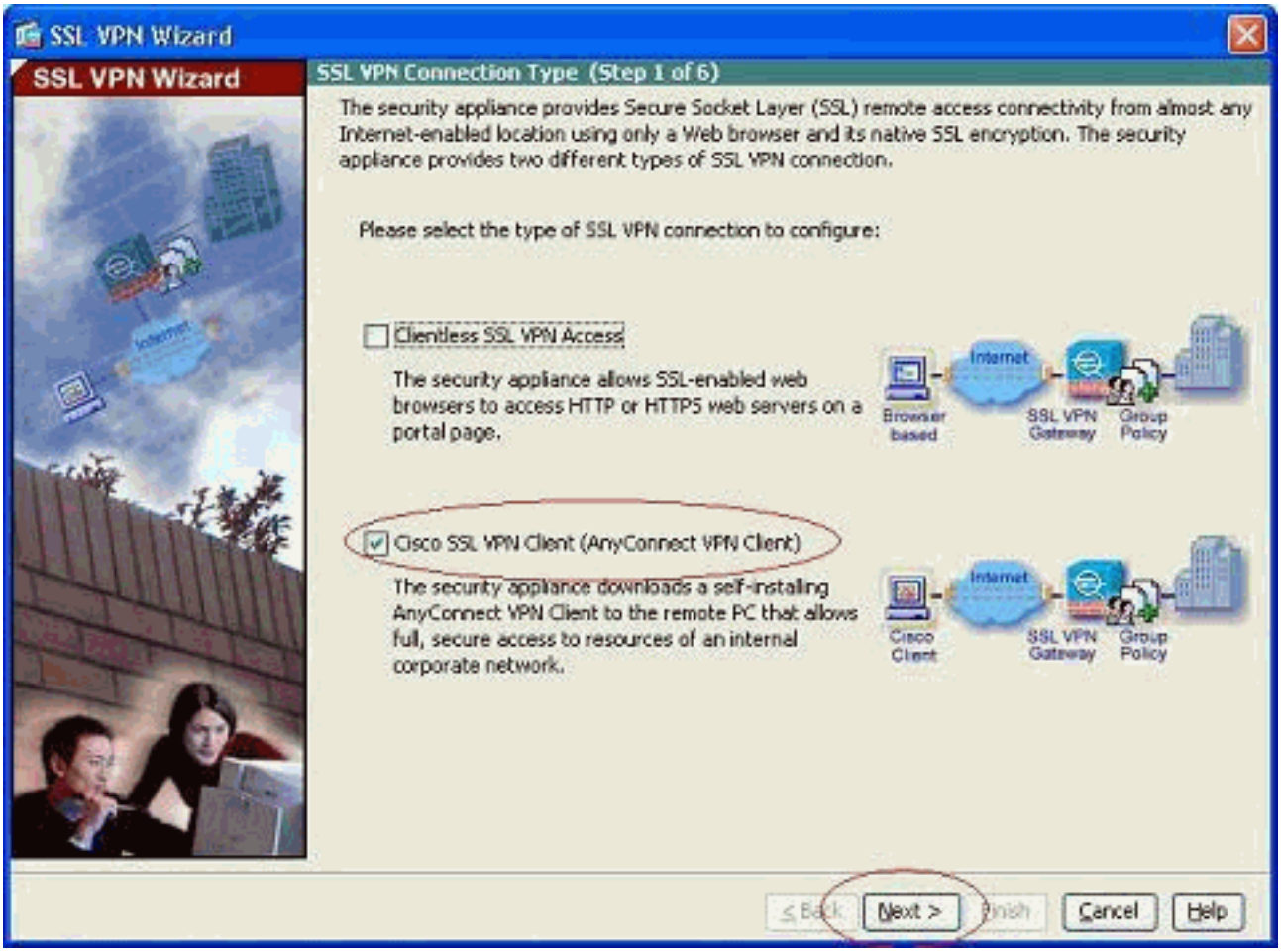
Nota: O WebVPN e o ASDM não podem ser ativados na mesma interface do ASA, a menos que você altere os números de porta. Consulte ASDM e WebVPN Habilitados na Mesma Interface do ASA para obter mais informações.

Termine estas etapas a fim configurar o SSL VPN usando o wizard VPN SSL.

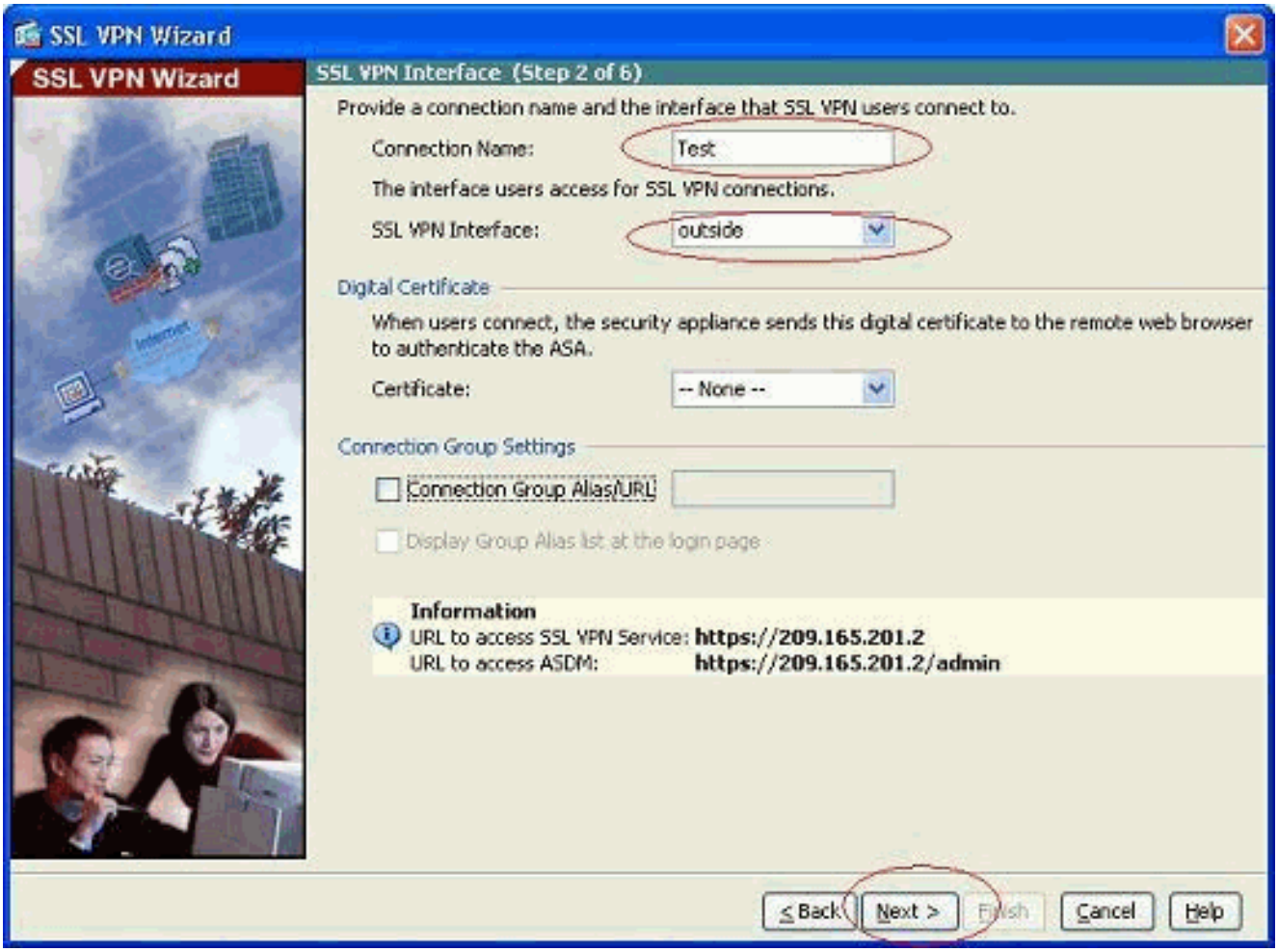
1. Do menu dos assistentes, escolha o **wizard VPN SSL**.



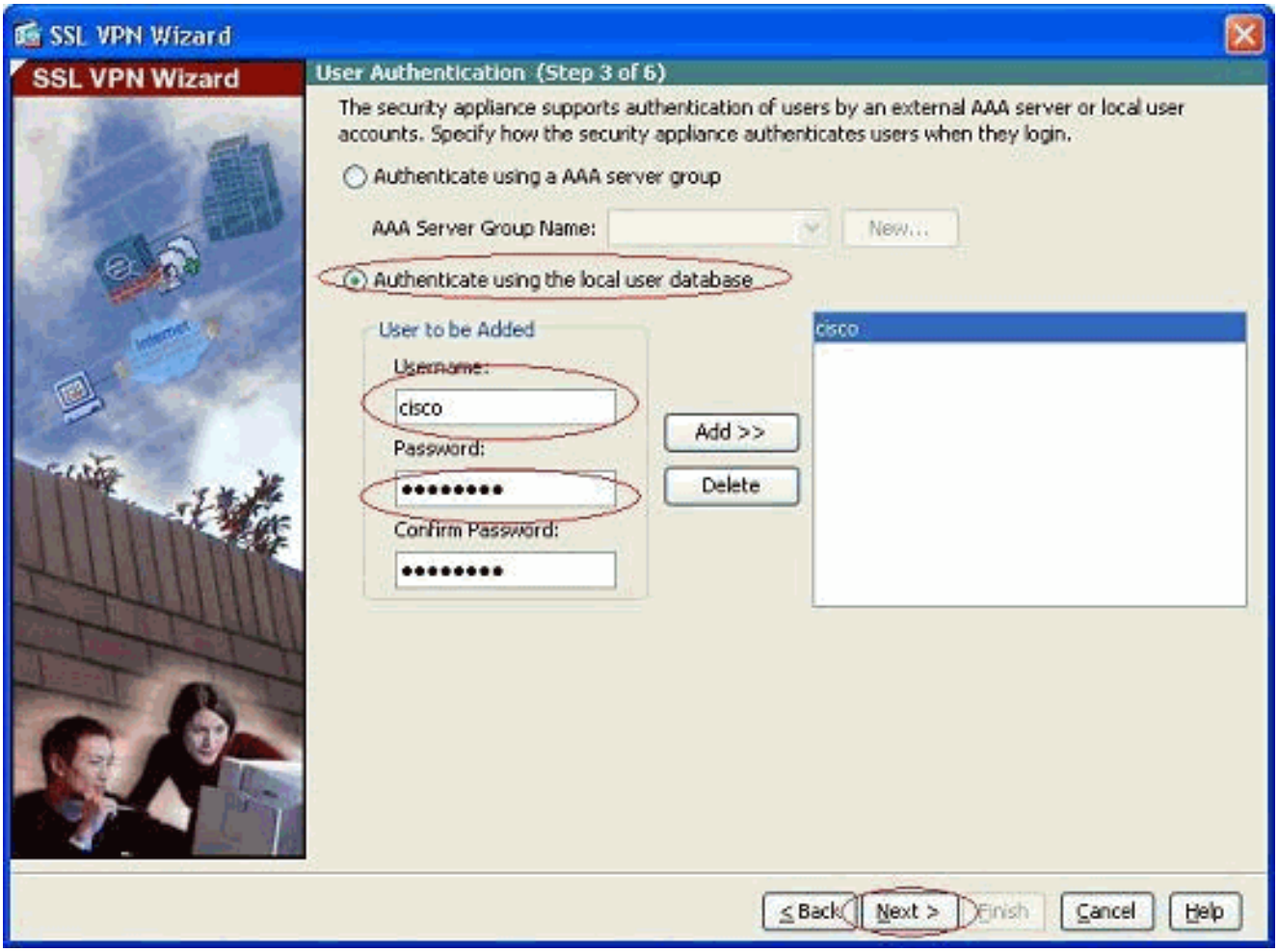
2. Clique a caixa de verificação do **Cisco SSL VPN Client**, e clique-a **em seguida**.



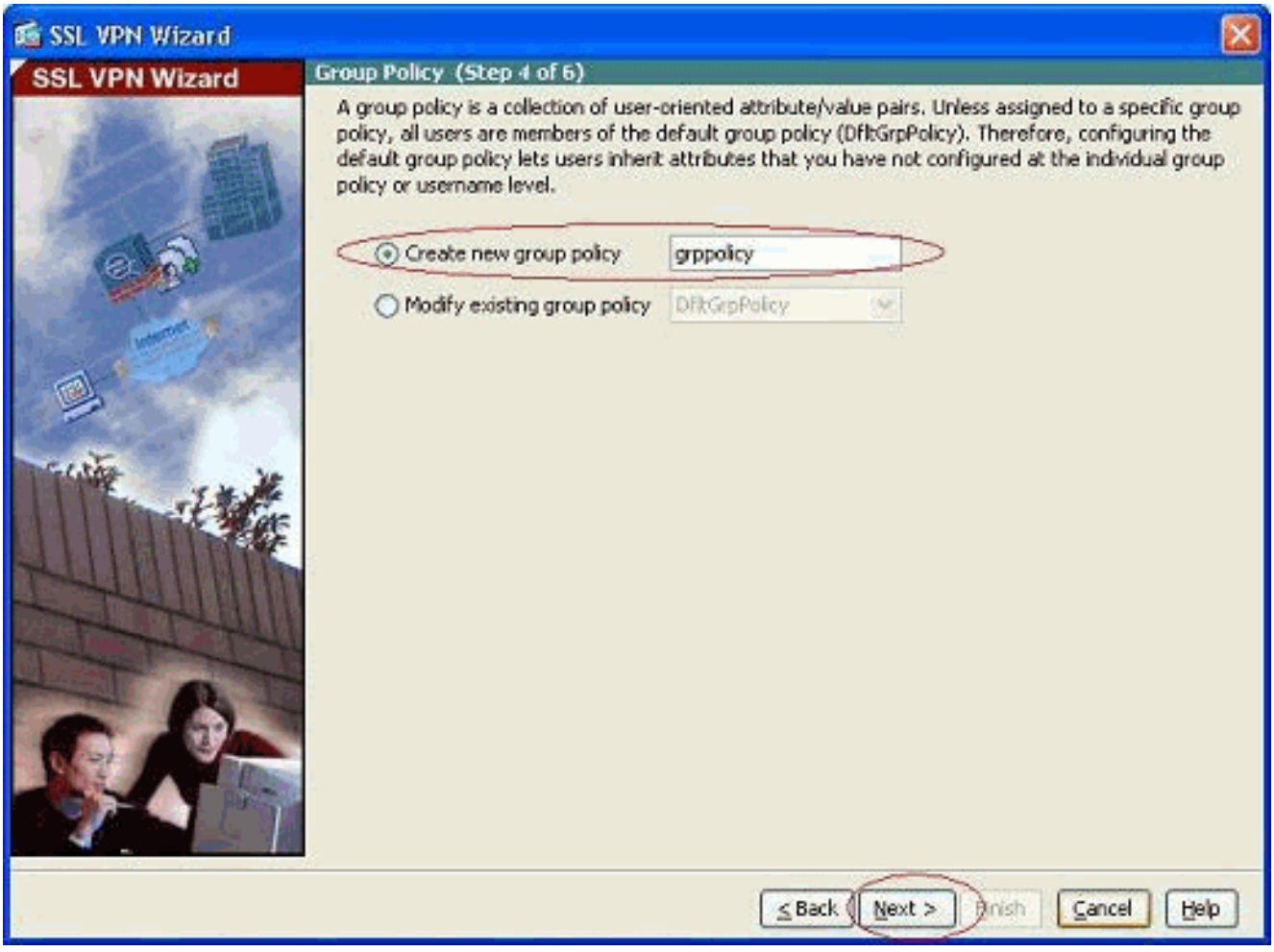
3. Dê entrada com um nome para a conexão no campo de nome de conexão, e escolha então a relação que está sendo usada pelo usuário para alcançar o SSL VPN da lista de drop-down da relação SSL
   VPN.



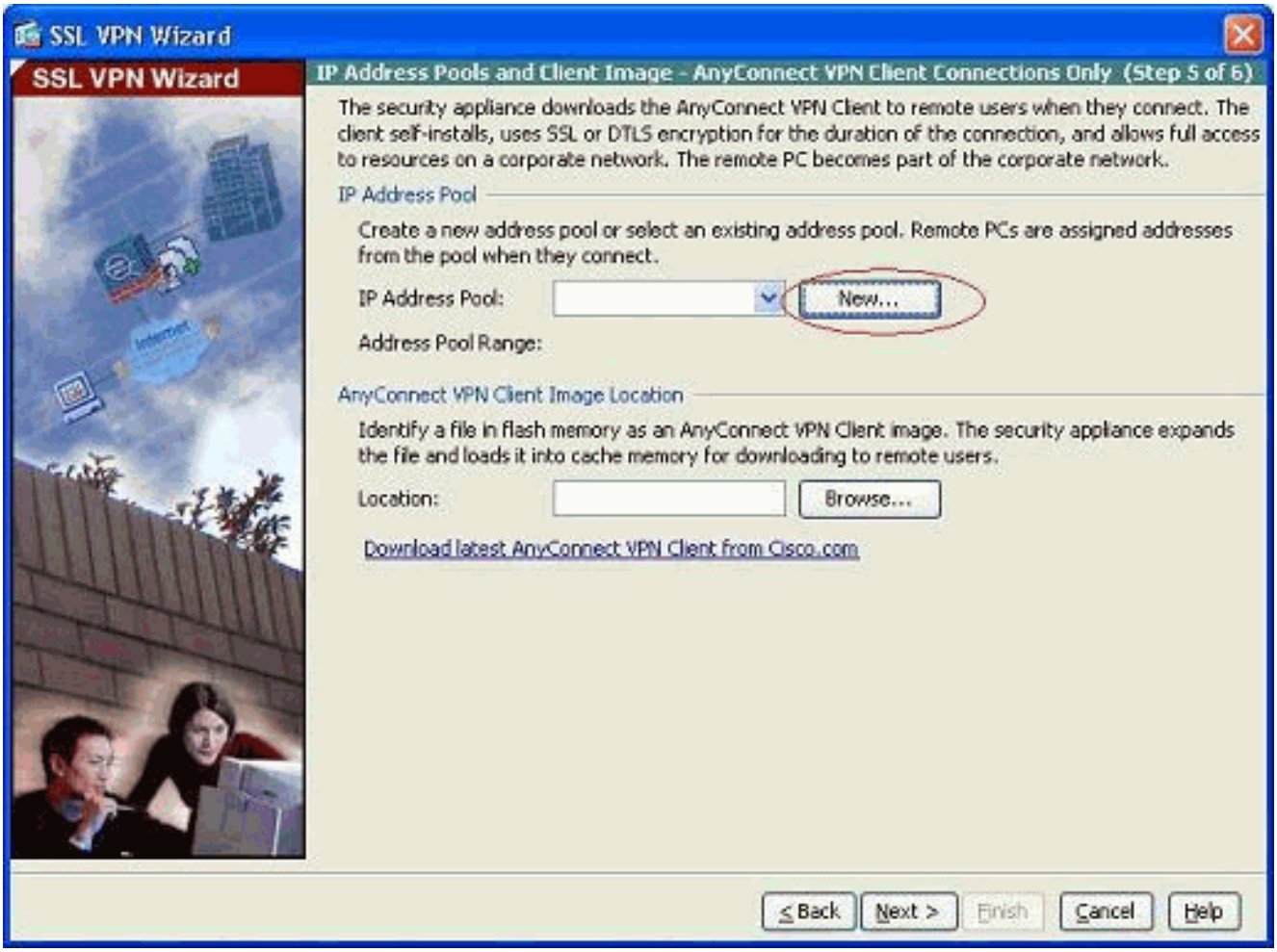
4. Clique em Next.
5. Escolha um modo de autenticação, e clique-o **em seguida**. (Este exemplo usa a autenticação
   local.)



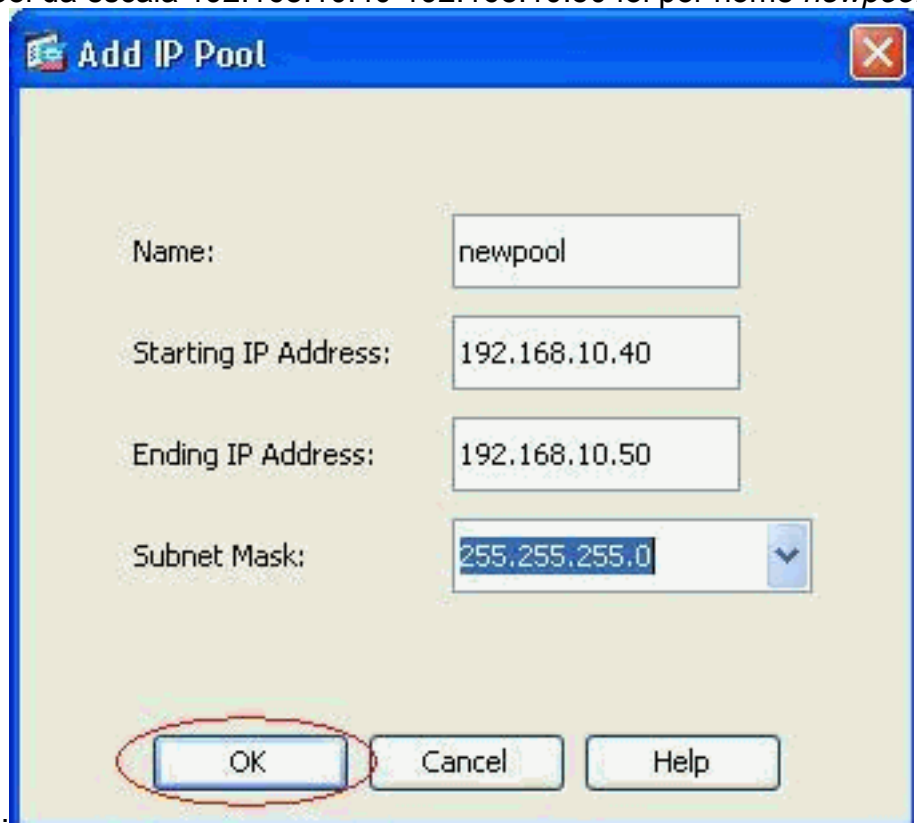
6. Criam uma política nova do grupo a não ser a política do grupo padrão existente.



7. Cria um conjunto de endereço novo que seja atribuído ao cliente VPN PC SSL uma vez que obtém
conectado.

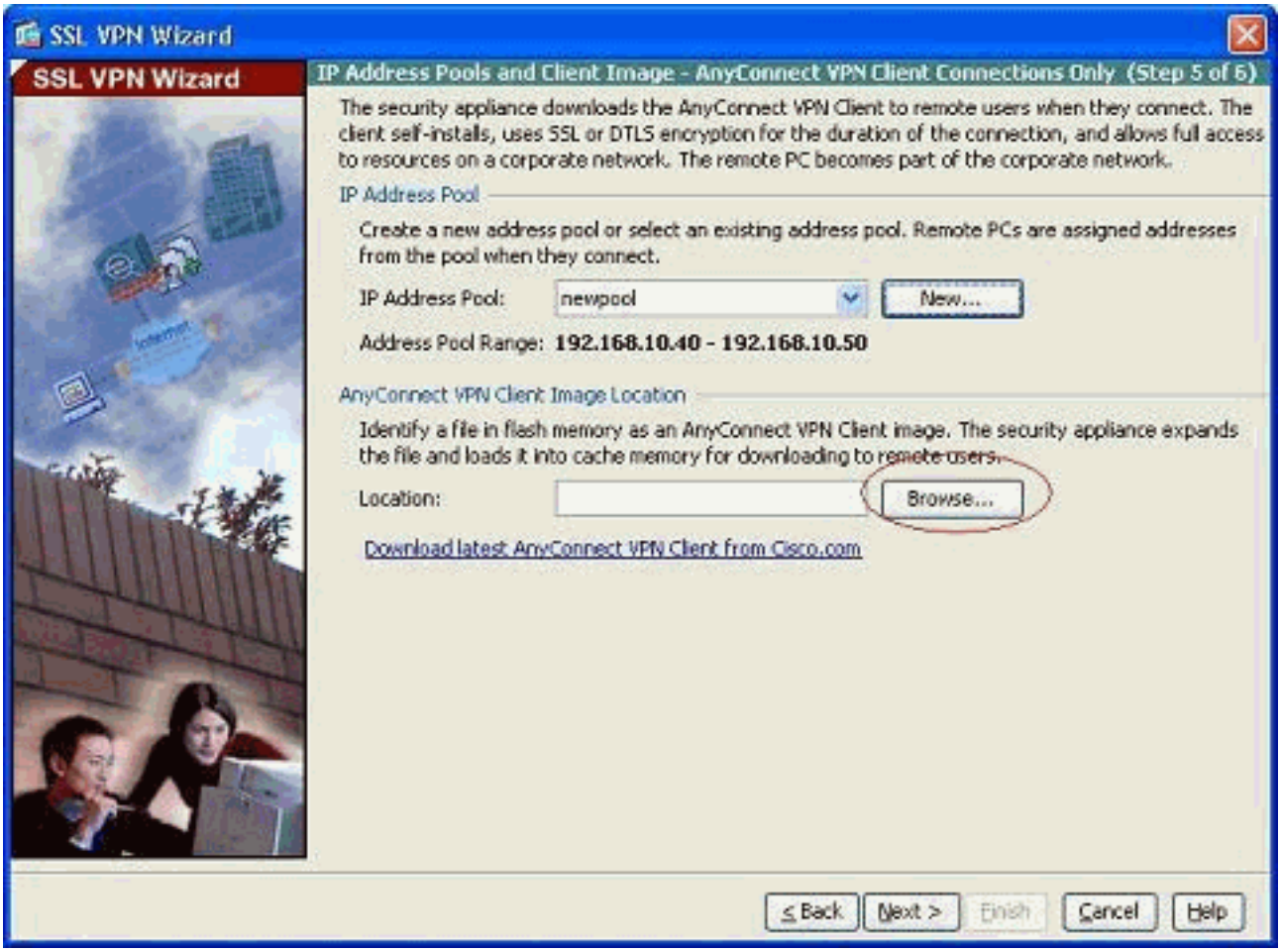


Um pool da escala 192.168.10.40-192.168.10.50 foi por nome *newpool*
criado.

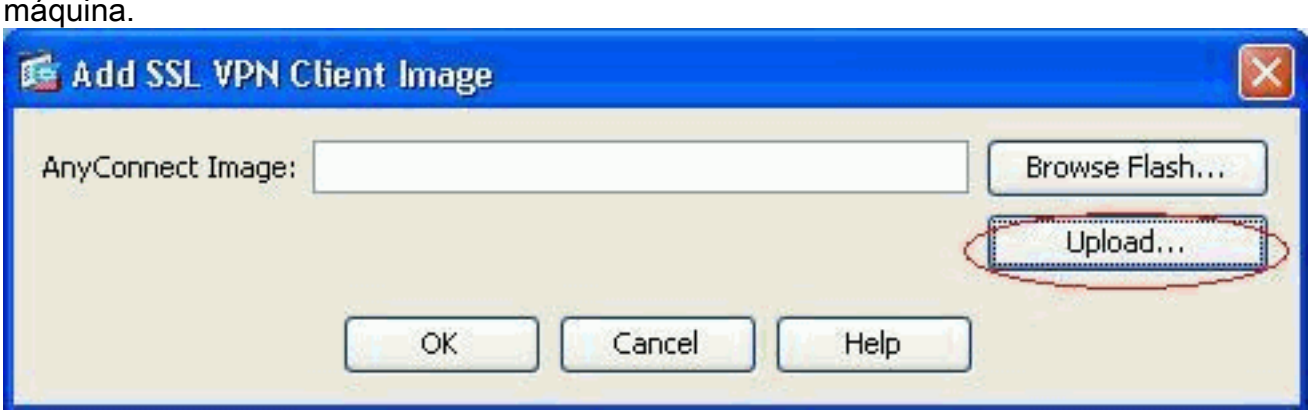


8. O clique **consulta** a fim escolher e transferir arquivos pela rede a imagem do cliente VPN

SSL à memória Flash do
ASA.

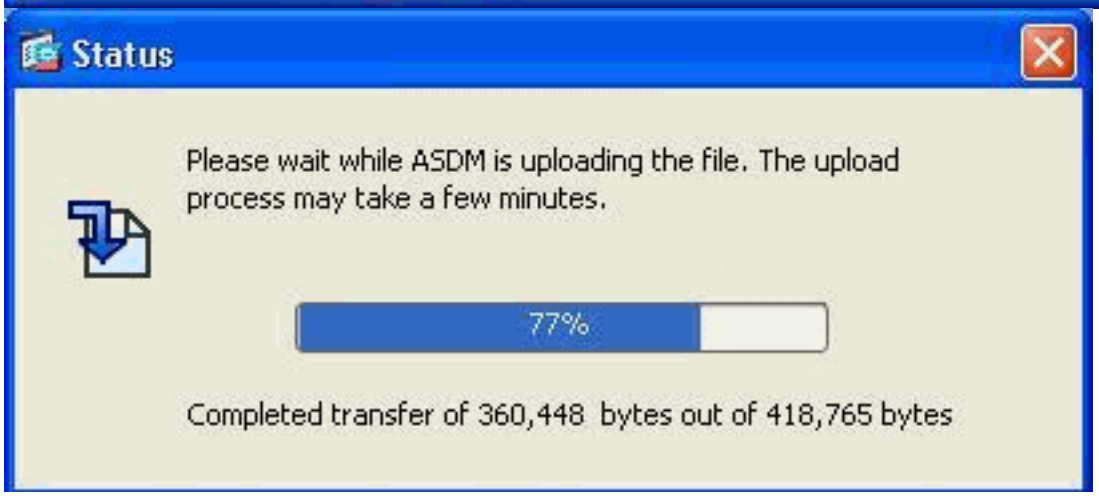


9. Clique a **transferência de arquivo pela rede** a fim ajustar o caminho de arquivo do diretório local da
máquina.



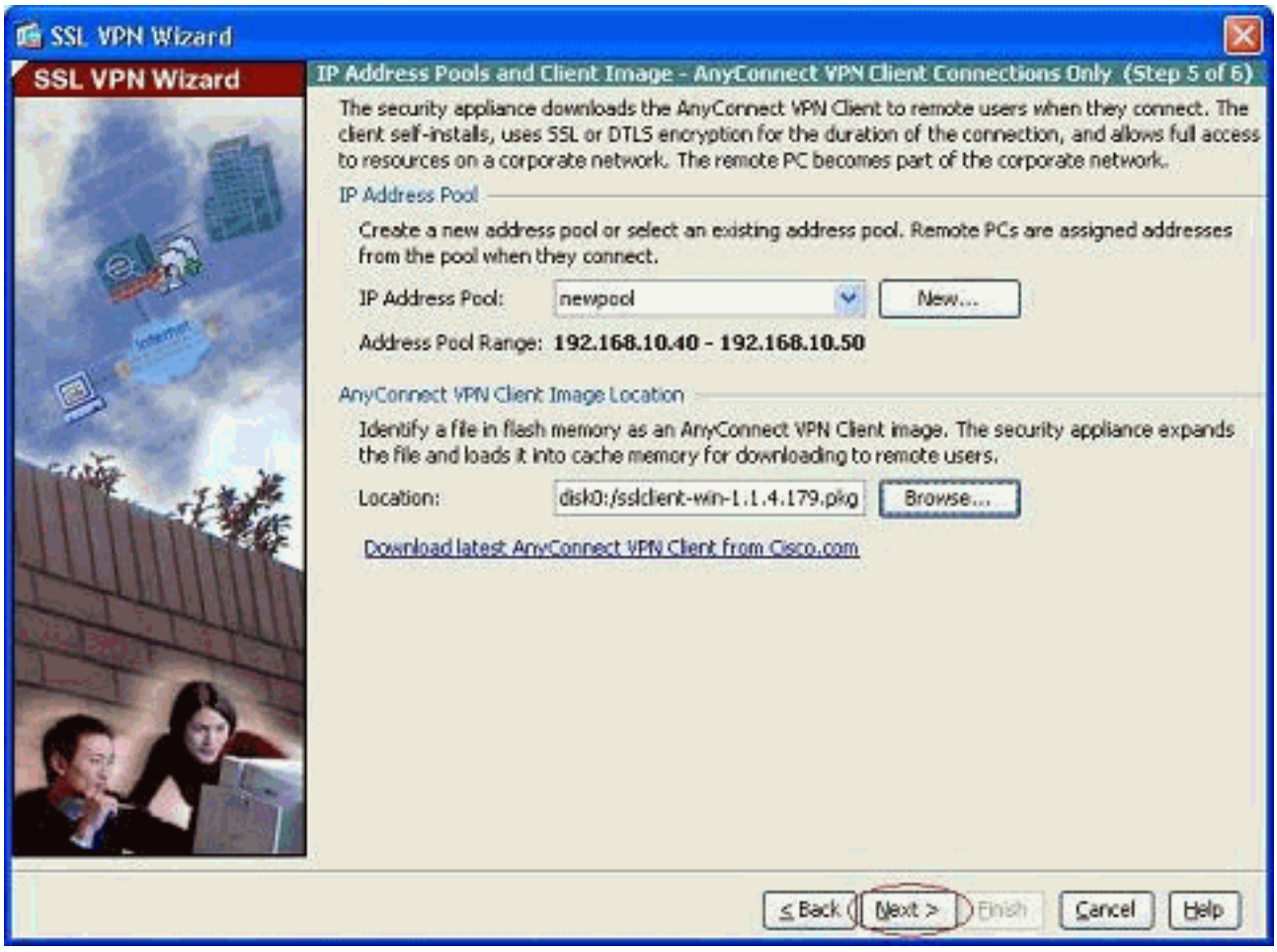
10. O clique **consulta arquivos locais** a fim selecionar o diretório onde o arquivo sslclient.pkg existe.

11. **Arquivo da transferência de arquivo pela rede do** clique a fim transferir arquivos pela rede o arquivo selecionado ao flash do
ASA.

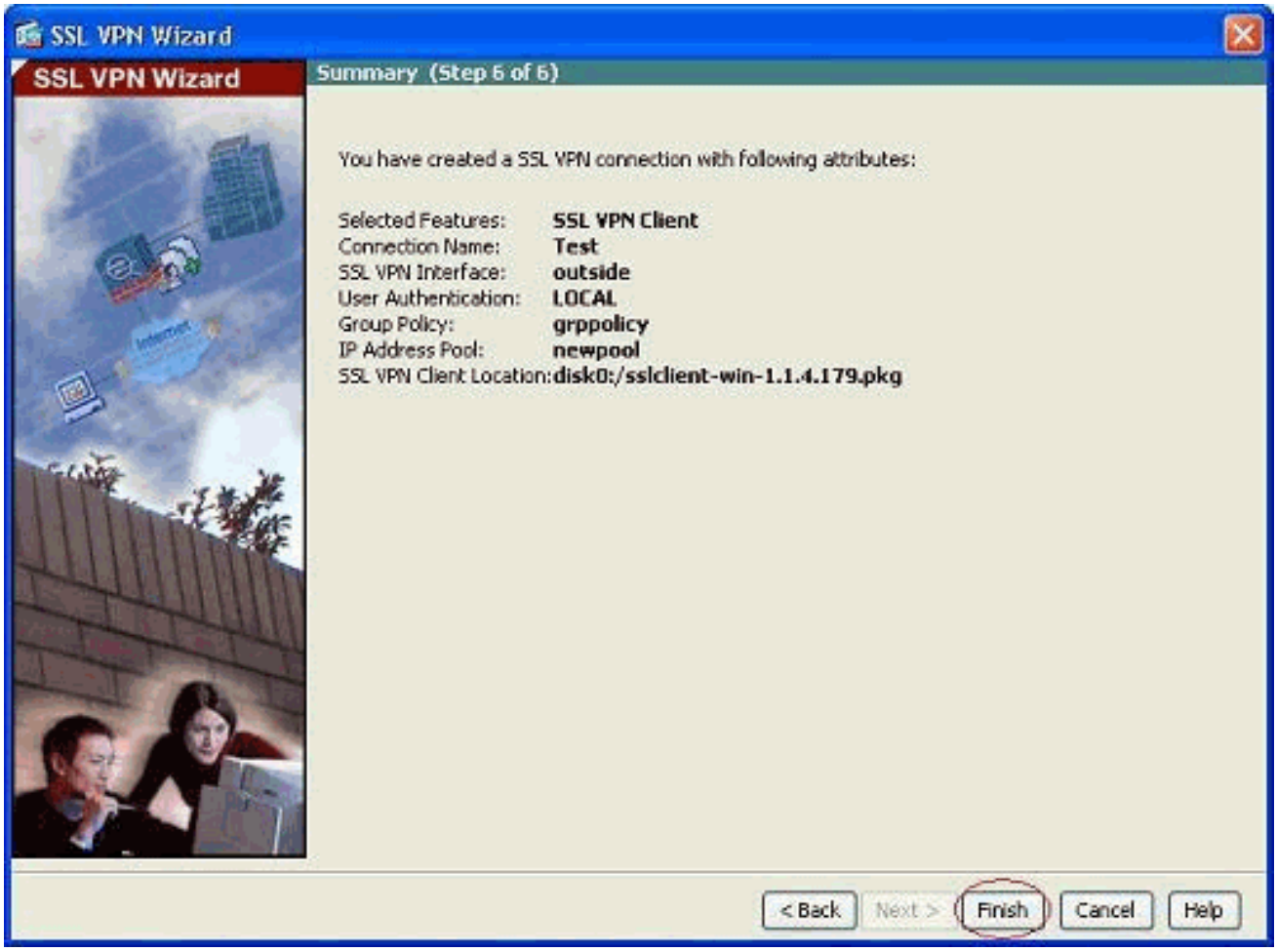


12. O arquivo é transferido arquivos pela rede uma vez sobre ao flash do ASA, **APROVAÇÃO do** clique para terminar essa
tarefa.

13. Agora mostra o arquivo de pacote o mais atrasado do anyconnect transferido arquivos pela rede sobre ao flash do ASA. Clique em
Next.



14. O sumário da configuração de cliente VPN SSL é mostrado. **Revestimento do** clique para terminar o assistente.



A configuração mostrada no ASDM refere-se principalmente a configuração do wizard de cliente VPN SSL.

No CLI, você pode observar alguma configuração adicional. A configuração de CLI completa é mostrada abaixo e os comandos importantes foram destacados.

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#
```

Verificar

Os comandos dados nesta seção podem ser usados para verificar esta configuração.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre que o webvpn svc** — — indica as imagens SVC armazenadas na memória Flash ASA.
- **show vpn-sessiondb svc** — Mostra informações sobre as conexões SSL atuais.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Apoio adaptável da ferramenta de segurança do Cisco 5500 Series
- PIX/ASA e cliente VPN para os Internet públicas VPN em um exemplo de configuração da vara
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Suporte Técnico e Documentação - Cisco Systems