ASA 7.1/7.2: Permitir tunelamento dividido para SVC no exemplo de configuração do ASA

Contents

Introduction

Este documento fornece instruções passo a passo sobre como permitir o acesso de Clientes VPN SSL (Secure Socket Layer) à Internet enquanto estão encapsulados em um Cisco Adaptive Security Appliance (ASA). Essa configuração permite que o SVC tenha acesso seguro aos recursos corporativos por meio de SSL e fornece acesso não seguro à Internet com o uso de tunelamento dividido.

A capacidade de transmitir tráfego protegido e não protegido na mesma interface é conhecida como tunelamento dividido. O tunelamento dividido exige que você especifique exatamente qual tráfego está protegido e qual é o destino desse tráfego, de modo que somente o tráfego especificado entre no túnel, enquanto o restante é transmitido não criptografado pela rede pública (Internet).

Prerequisites

Requirements

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

- Privilégios administrativos locais em todas as estações de trabalho remotas
- Controles Java e AtiveX na estação de trabalho remota

- A porta 443(SSL) não está bloqueada em nenhum lugar ao longo do caminho da conexão

Componentes Utilizados

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

- Cisco 5500 Series Adaptive Security Appliance (ASA) que executa a versão de software 7.2(2)
- Versão do Cisco SSL VPN Client para Windows 1.1.4.179**Observação:** faça o download do pacote SSL VPN Client (sslclient-win*.pkg) do download do software Cisco (somente clientes registrados) . Copie o SVC para a memória flash do ASA, que deve ser baixado para os computadores do usuário remoto para estabelecer a conexão VPN SSL com o ASA. Consulte a seção Instalação do Software SVC do guia de configuração do ASA para obter mais informações.
- PC com Windows 2000 Professional SP4 ou Windows XP SP2
- Cisco Adaptive Security Device Manager (ASDM) versão 5.2(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

O SSL VPN Client (SVC) é uma tecnologia de tunelamento VPN que oferece aos usuários remotos os benefícios de um cliente IPsec VPN sem a necessidade de administradores de rede instalarem e configurarem clientes IPsec VPN em computadores remotos. O SVC usa a criptografia SSL que já está presente no computador remoto, bem como o login e a autenticação da WebVPN do Security Appliance.

Para estabelecer uma sessão SVC, o usuário remoto insere o endereço IP de uma interface WebVPN do Security Appliance no navegador, e o navegador se conecta a essa interface e exibe a tela de login do WebVPN. Se você atender ao login e à autenticação, e o Security Appliance identificar você como exigindo o SVC, o Security Appliance fará o download do SVC para o computador remoto. Se o Security Appliance identificar você com a opção de usar o SVC, ele baixará o SVC para o computador remoto enquanto apresenta um link na janela para ignorar a instalação do SVC.

Após o download, o SVC é instalado e configurado a si mesmo, e o SVC permanece ou se desinstala, o que depende da configuração, do computador remoto quando a conexão é encerrada.

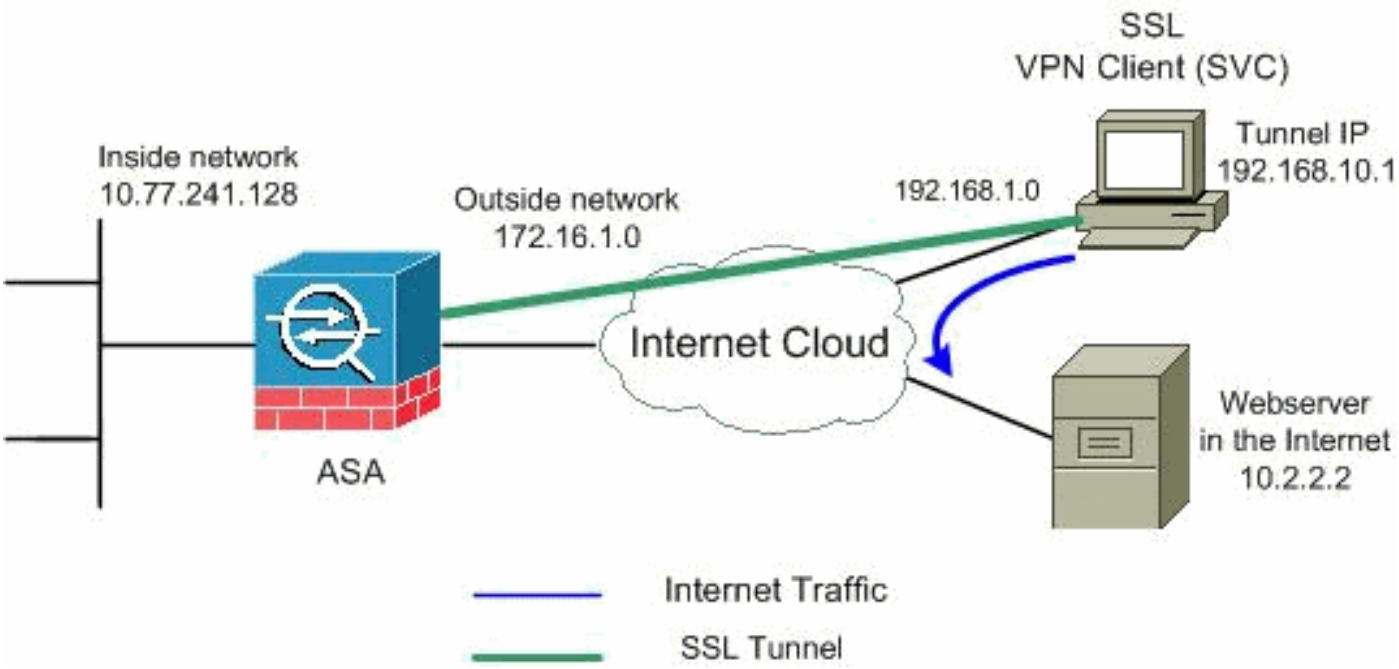
Configurar

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:

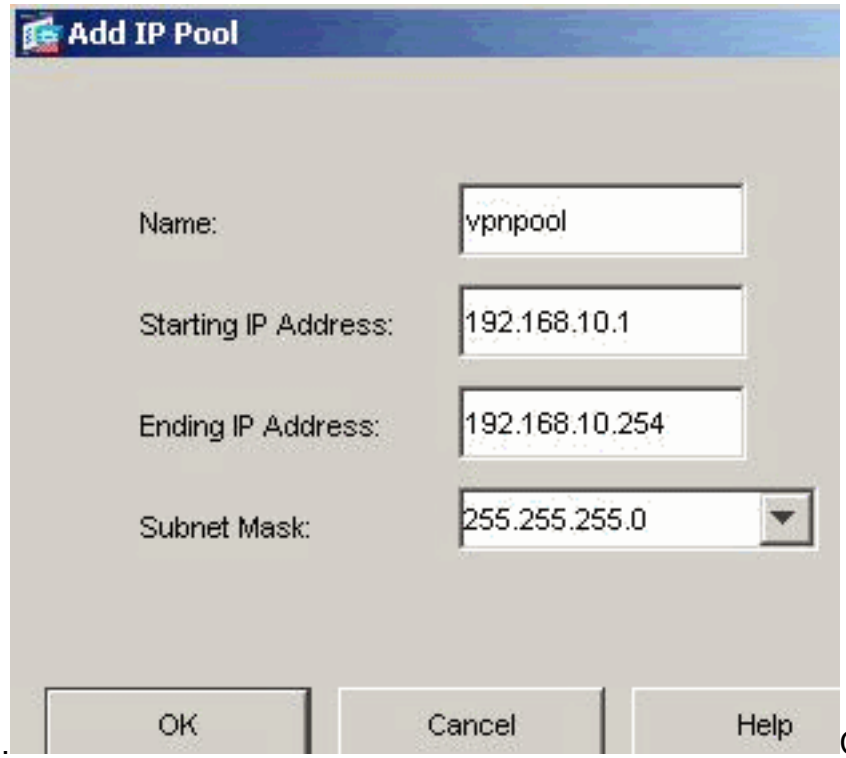


Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços RFC 1918 que foram usados em um ambiente de laboratório.

Configurações do ASA usando o ASDM 5.2(2)

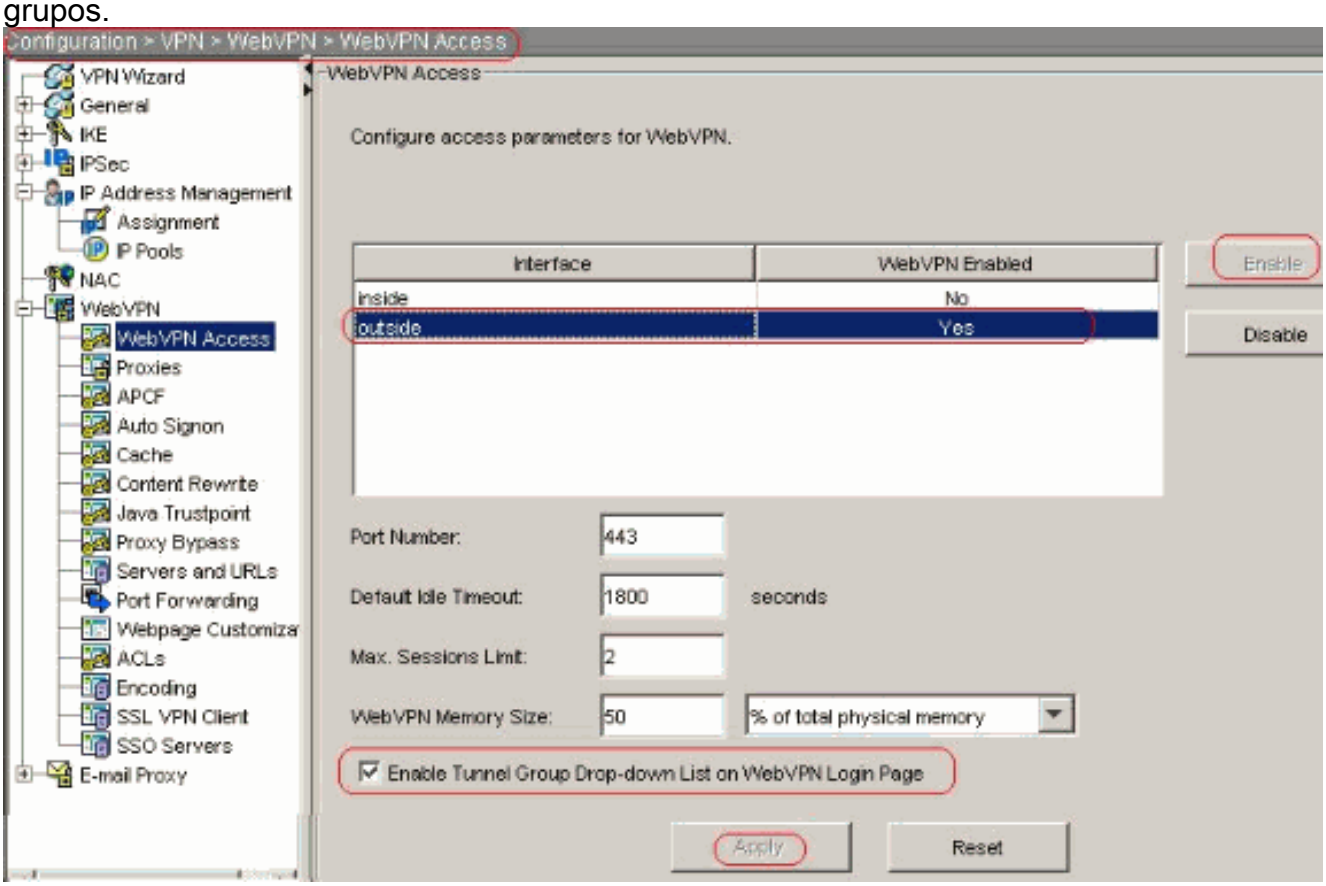
Conclua estes passos para configurar a VPN SSL no ASA com tunelamento dividido como mostrado:

1. O documento pressupõe que a configuração básica, como a configuração de interface e assim por diante, já foi feita e funciona corretamente.**Observação:** consulte Permitindo Acesso HTTPS para ASDM para permitir que o ASA seja configurado pelo ASDM.**Observação:** WebVPN e ASDM não podem ser habilitados 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.
2. Escolha **Configuration > VPN > IP Address Management > IP Pools** para criar um pool de endereços IP: **vpnpool** para clientes

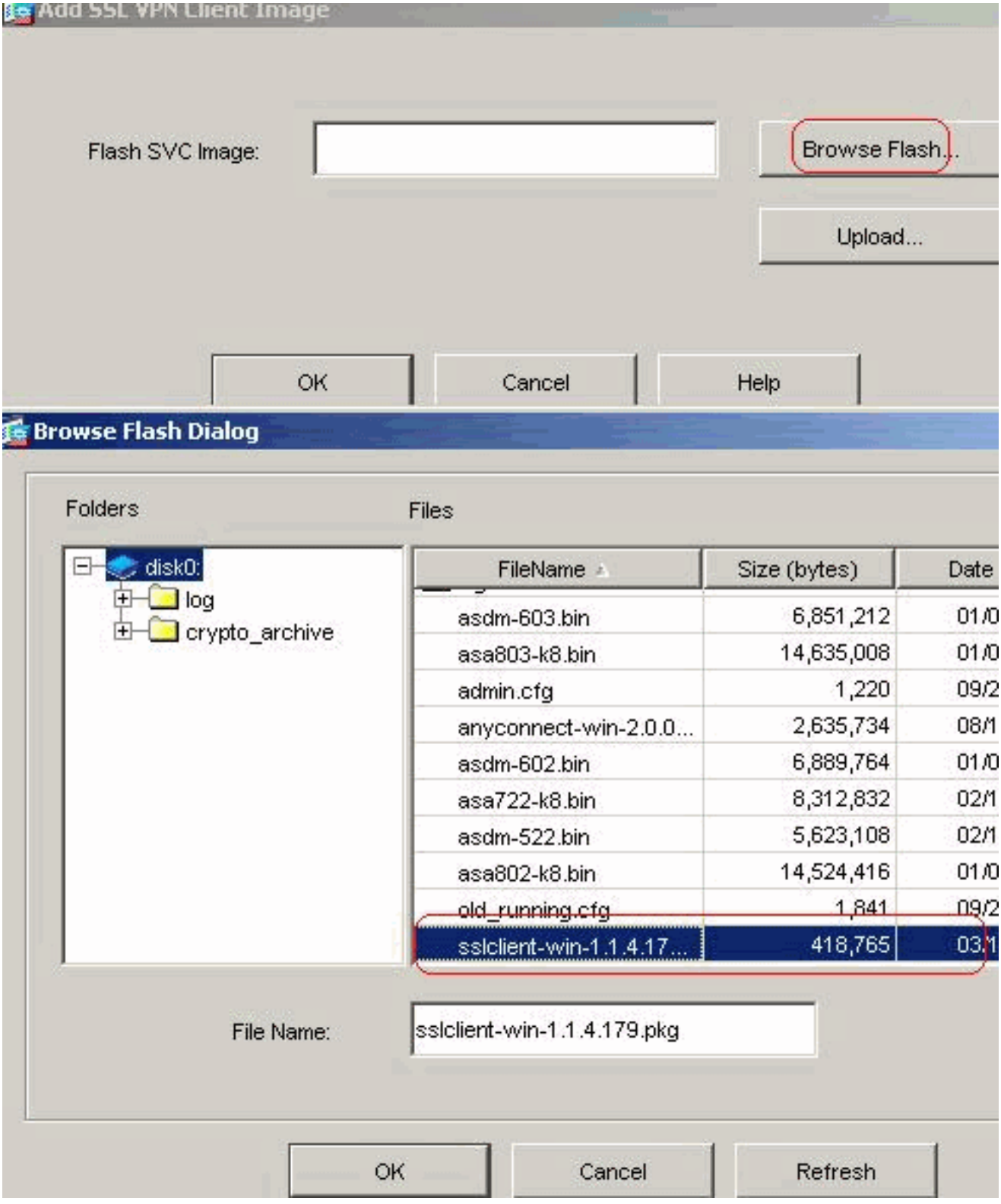


VPN. Clique em Apply.

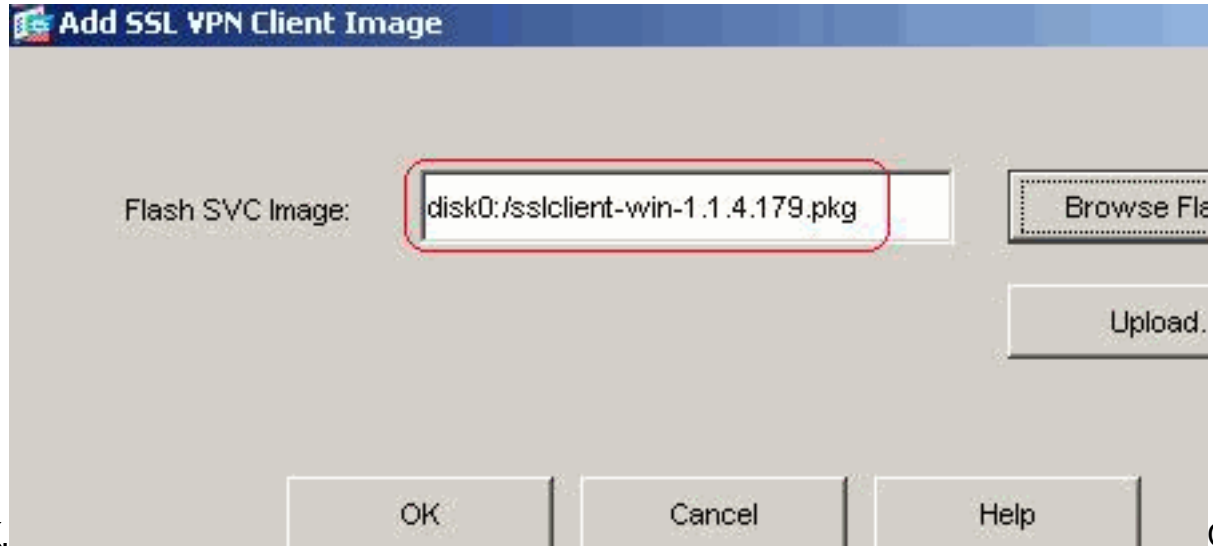
3. **Ative o WebVPN**Escolha **Configuration > VPN > WebVPN > WebVPN Access** e realce a interface externa com o mouse e clique em **Enable**. Marque a caixa de seleção **Enable Tunnel Group Drop-down List on WebVPN Login Page** para habilitar a lista suspensa aparecer na página de login para os usuários, para escolher seus respectivos grupos.



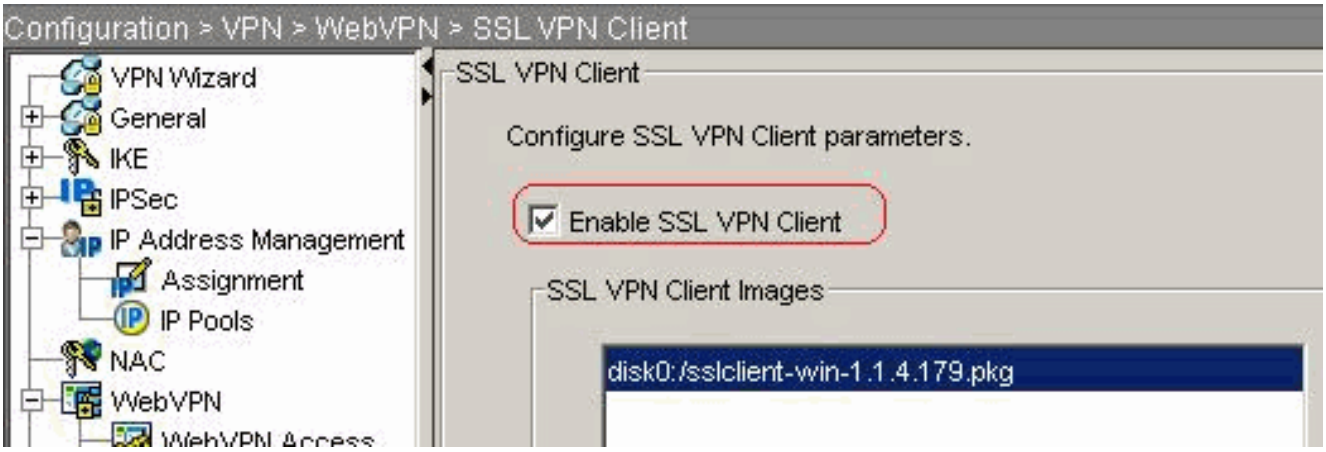
Clique em Apply.Escolha **Configuration > VPN > WebVPN > SSL VPN Client > Add** para adicionar a imagem do cliente SSL VPN da memória flash do ASA conforme mostrado.


Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin
6,851,212
01/0
asa803-k8.bin
14,635,008
01/0
admin.cfg
1,220
09/2
anyconnect-win-2.0.0...
2,635,734
08/1
asdm-602.bin
6,889,764
01/0
asa722-k8.bin
8,312,832
02/1
asdm-522.bin
5,623,108
02/1
asa802-k8.bin
14,524,416
01/0
old_running.cfg
1,841
09/2
sslclient-win-1.1.4.17...
418,765
03/1
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

Click

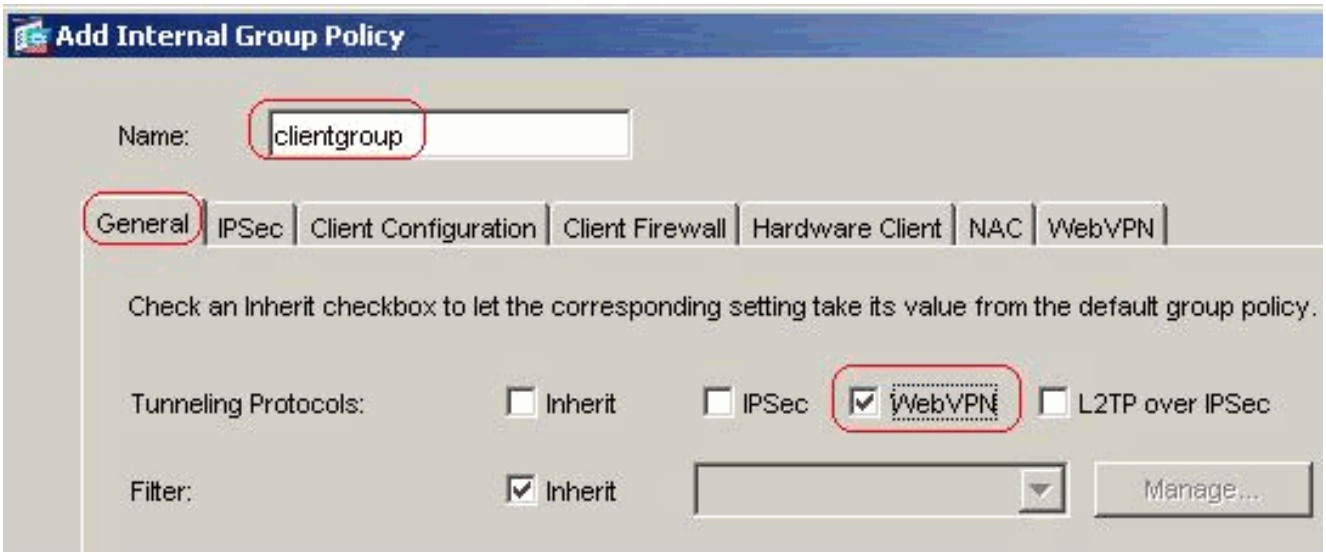


OK.Click **OK**.Clique na caixa de seleção **SSL VPN Client**.



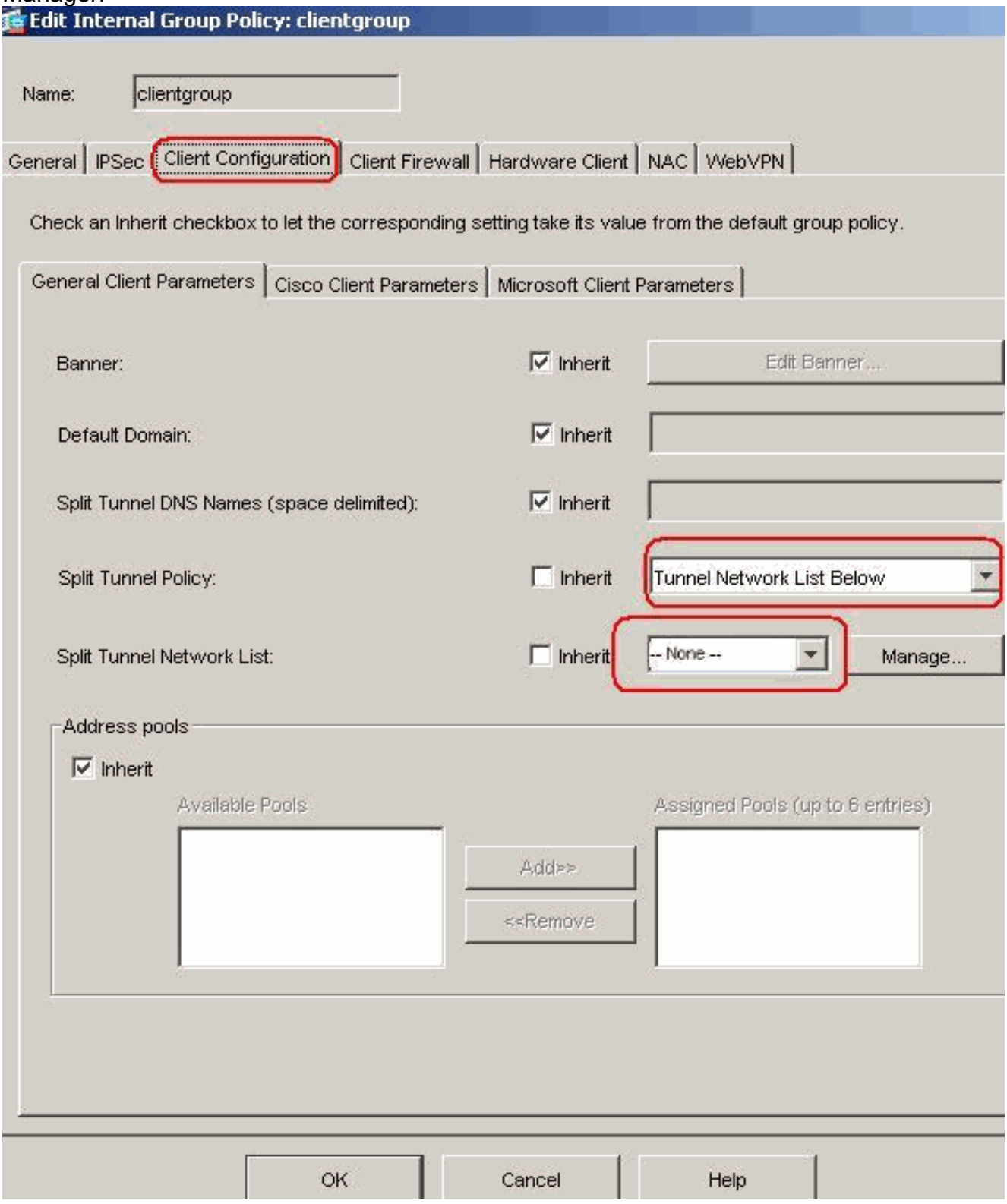
Clique em Apply.**Configuração via CLI Equivalente:**

4. **Configure a Política de Grupo**Escolha **Configuration > VPN > General > Group Policy > Add (Internal Group Policy) (Configuração > VPN > Geral > Política de Grupo > Adicionar)** para criar uma política de grupo interna **clientgroup**. Em **Geral**, escolha a caixa de seleção **WebVPN** para ativar o WebVPN como protocolo de tunelamento.

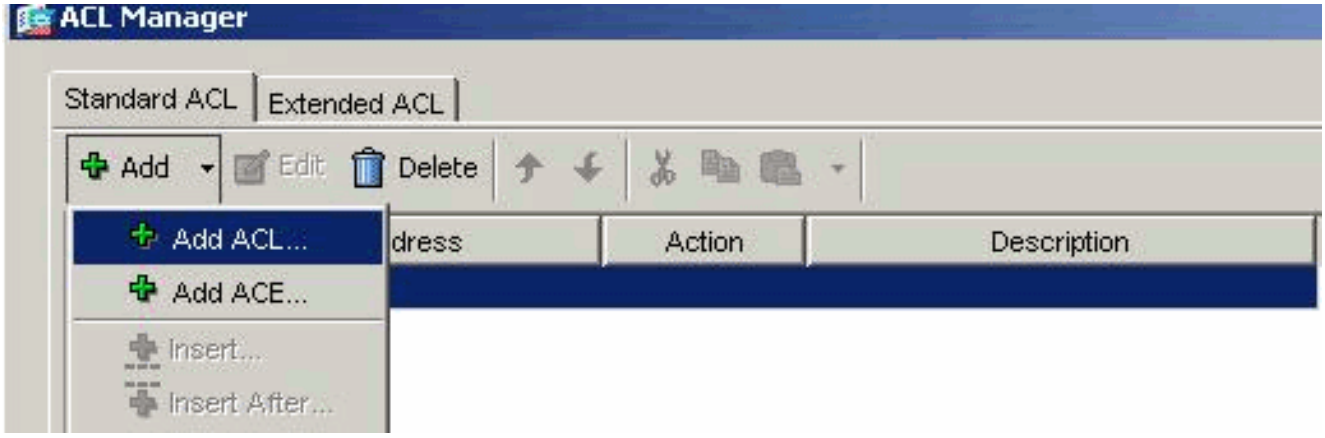


Na guia **Client Configuration > General Client Parameters**, desmarque a caixa **Inherit** para Split Tunnel Policy e escolha **Tunnel Network List Below** na lista suspensa.Desmarque a caixa **Inherit** para **Split Tunnel Network List** e clique em **Manage** para iniciar o ACL

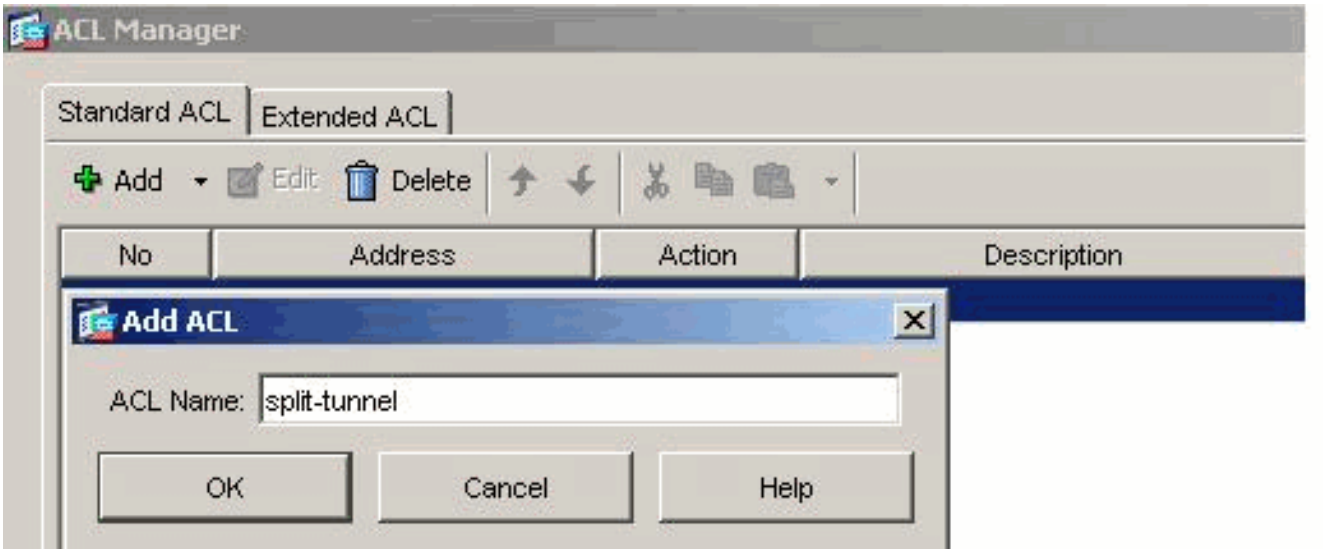
Manager.



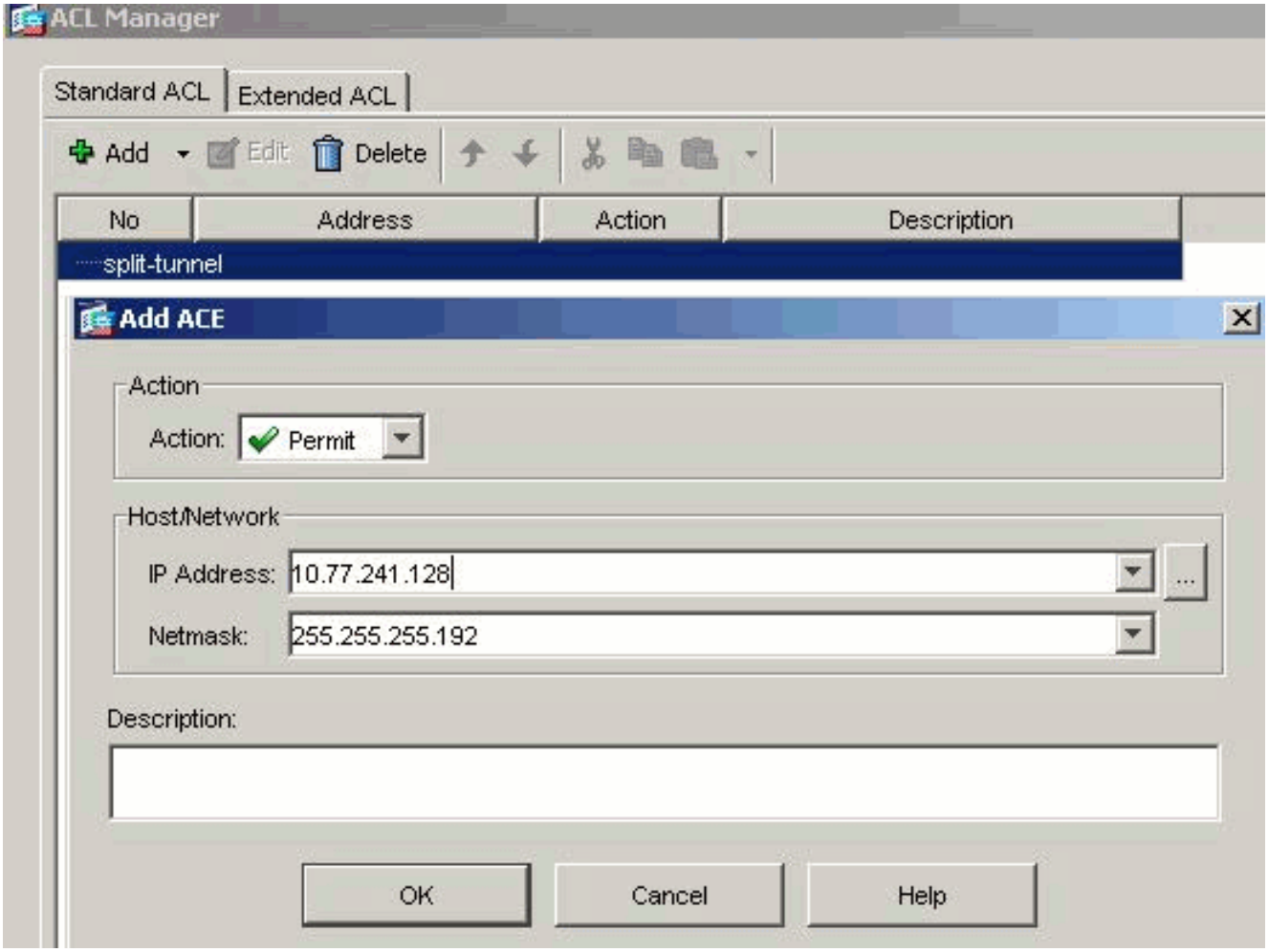
No ACL Manager, escolha **Add > Add ACL...** para criar uma nova lista de acesso.



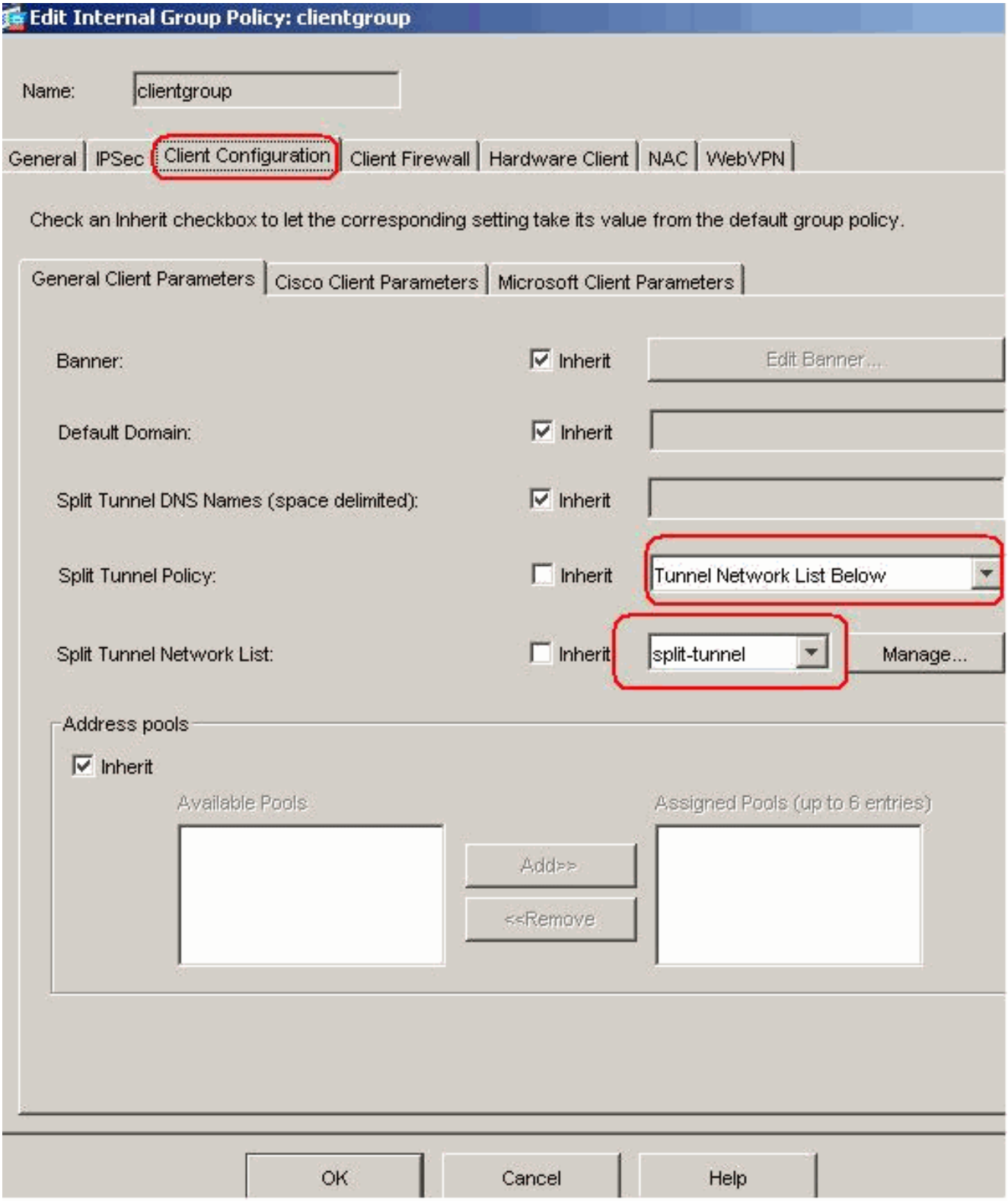
Forneça um nome para a ACL e clique em **OK**.



Uma vez que o nome da ACL é criado, escolha **Add > Add ACE para adicionar uma entrada de controle de acesso (ACE).**Defina a ACE que corresponde à LAN por trás do ASA. Nesse caso, a rede é 10.77.241.128/26 e escolha **Permit**.Clique em **OK para sair do ACL Manager.**

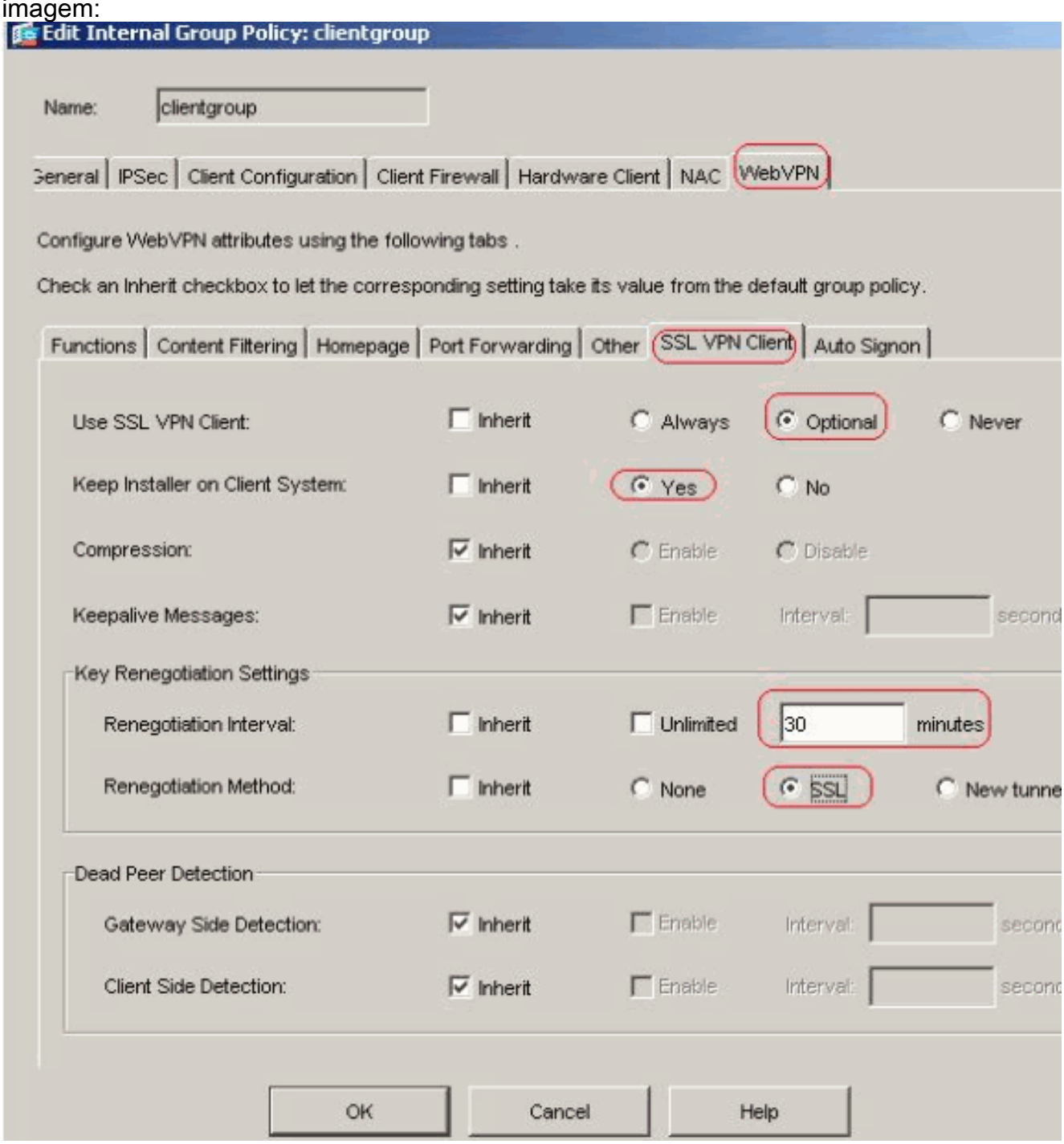


Certifique-se de que a ACL que você acabou de criar esteja selecionada para a Split Tunnel Network List.Clique em **OK para retornar à configuração da Política de Grupo.**

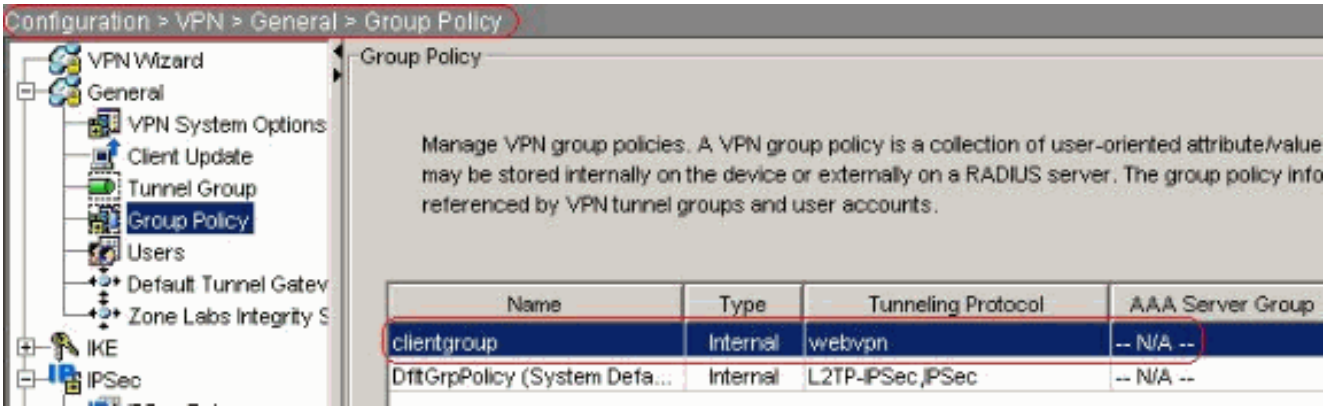


Na página principal, clique em **Apply** e em **Send** (se necessário) para enviar os comandos ao ASA.Para a opção Usar cliente VPN SSL, desmarque a caixa de seleção **Herdar** e clique no botão de opção **Opcional**.Essa opção permite que o cliente remoto escolha se deseja clicar na guia **WebVPN > SSLVPN Client** e escolha estas opções:Não faça o download do SVC. A opção Always garante que o SVC seja transferido para a estação de trabalho remota durante cada conexão VPN SSL.Para a opção Keep Installer on Client System, desmarque a caixa de seleção **Inherit e clique no botão de opção Yes.**Esta ação permite que o software SVC permaneça na máquina cliente; Consequentemente, o ASA não precisa fazer o download do software SVC para o cliente toda vez que uma conexão é feita. Esta opção é uma boa escolha para os usuários remotos que acessam frequentemente a rede corporativa.Para a opção Renegotiation Interval, desmarque a caixa **Inherit, desmarque a**

caixa de seleção Unlimited e insira o número de minutos até a geração de uma nova chave.A segurança é aprimorada quando você define os limites no período de tempo em que uma chave é válida.Para a opção Renegotiation Method, desmarque a caixa de seleção **Inherit e clique no botão de opção SSL.** A renegociação pode utilizar o túnel SSL existente ou um túnel novo criado especificamente para a renegociação.Os atributos do cliente VPN SSL devem ser configurados conforme mostrado nesta
imagem:

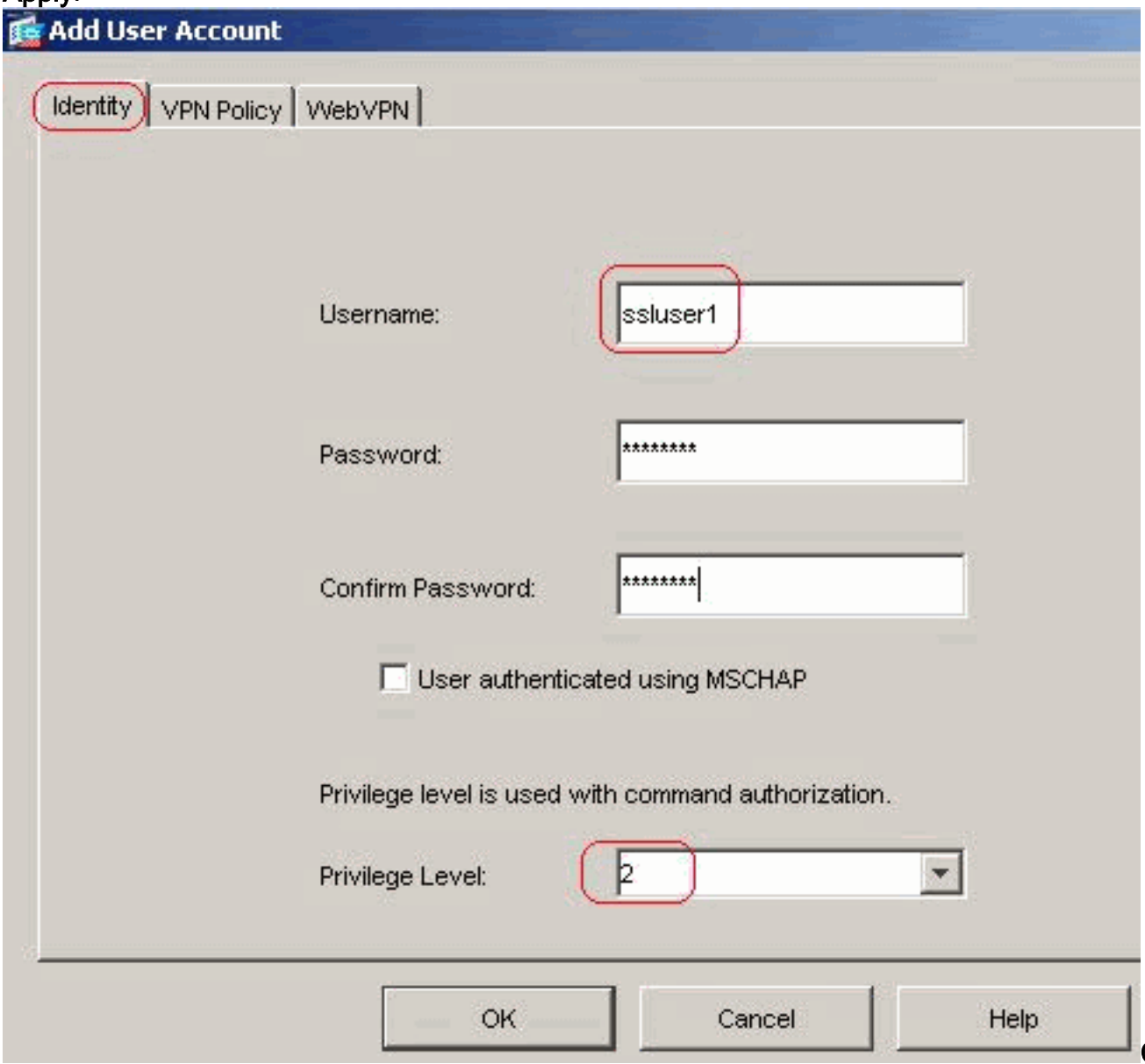


Clique em **OK e, em seguida, em Apply**.



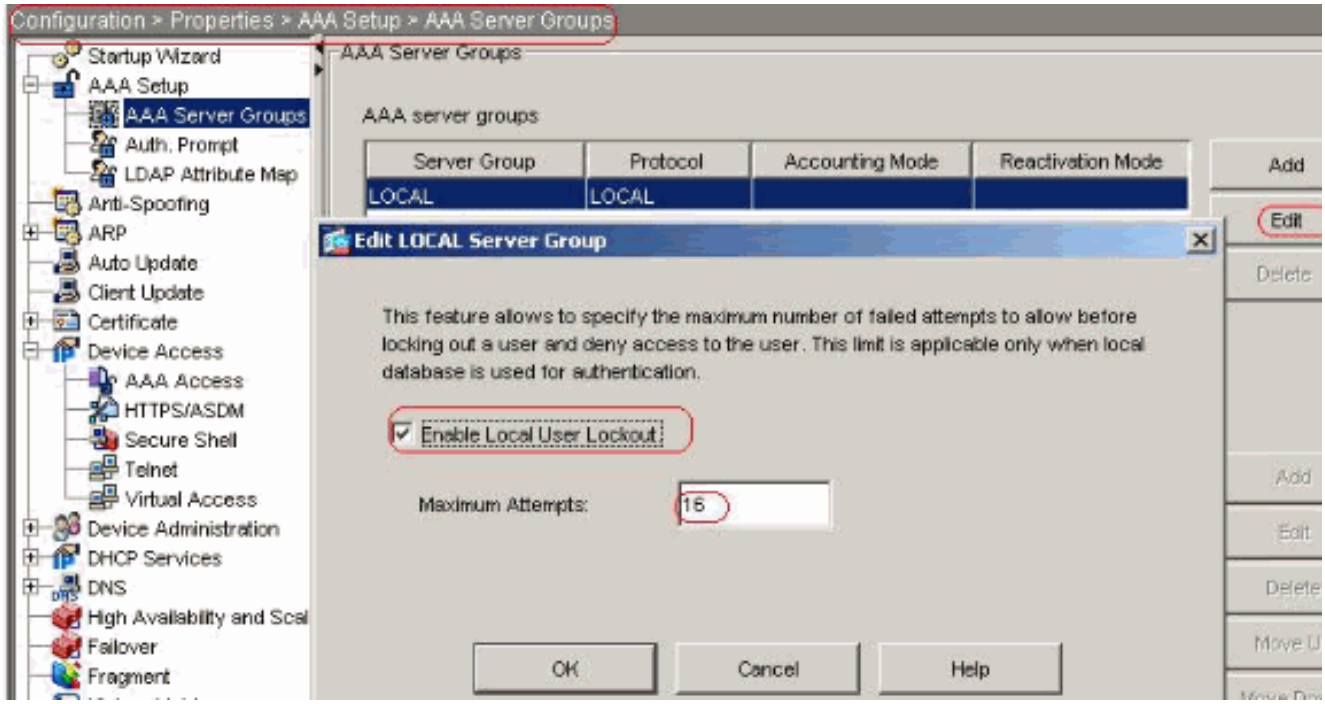
Configuração via CLI Equivalente:

5. Escolha **Configuration > VPN > General > Users > Add** para criar uma nova conta de usuário **ssluser1**. Clique em **OK e, em seguida, em Apply**.



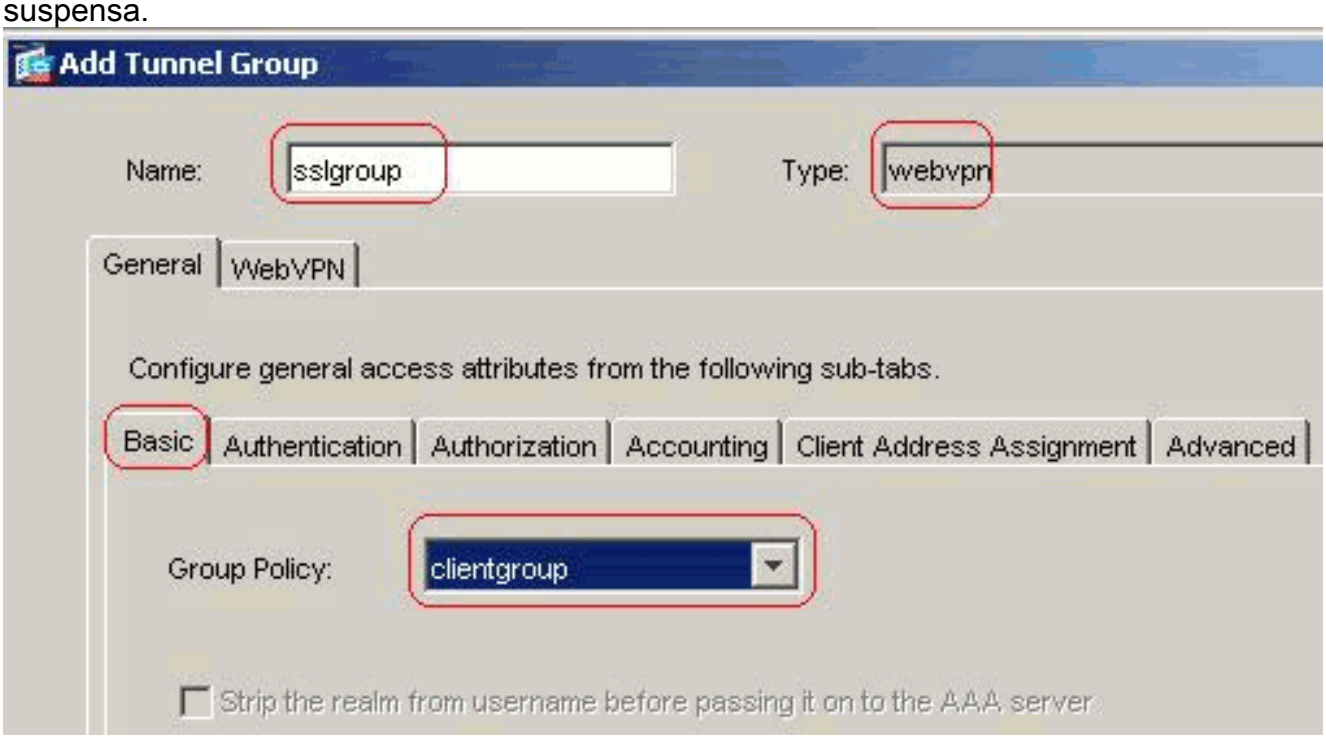
Configuração via CLI Equivalente:

6. Escolha **Configuration > Properties > AAA Setup > AAA Servers Groups > Edit** para modificar o grupo de servidores padrão **LOCAL** e escolha a caixa de seleção **Enable Local User Lockout** com valor máximo de tentativas como **16**.

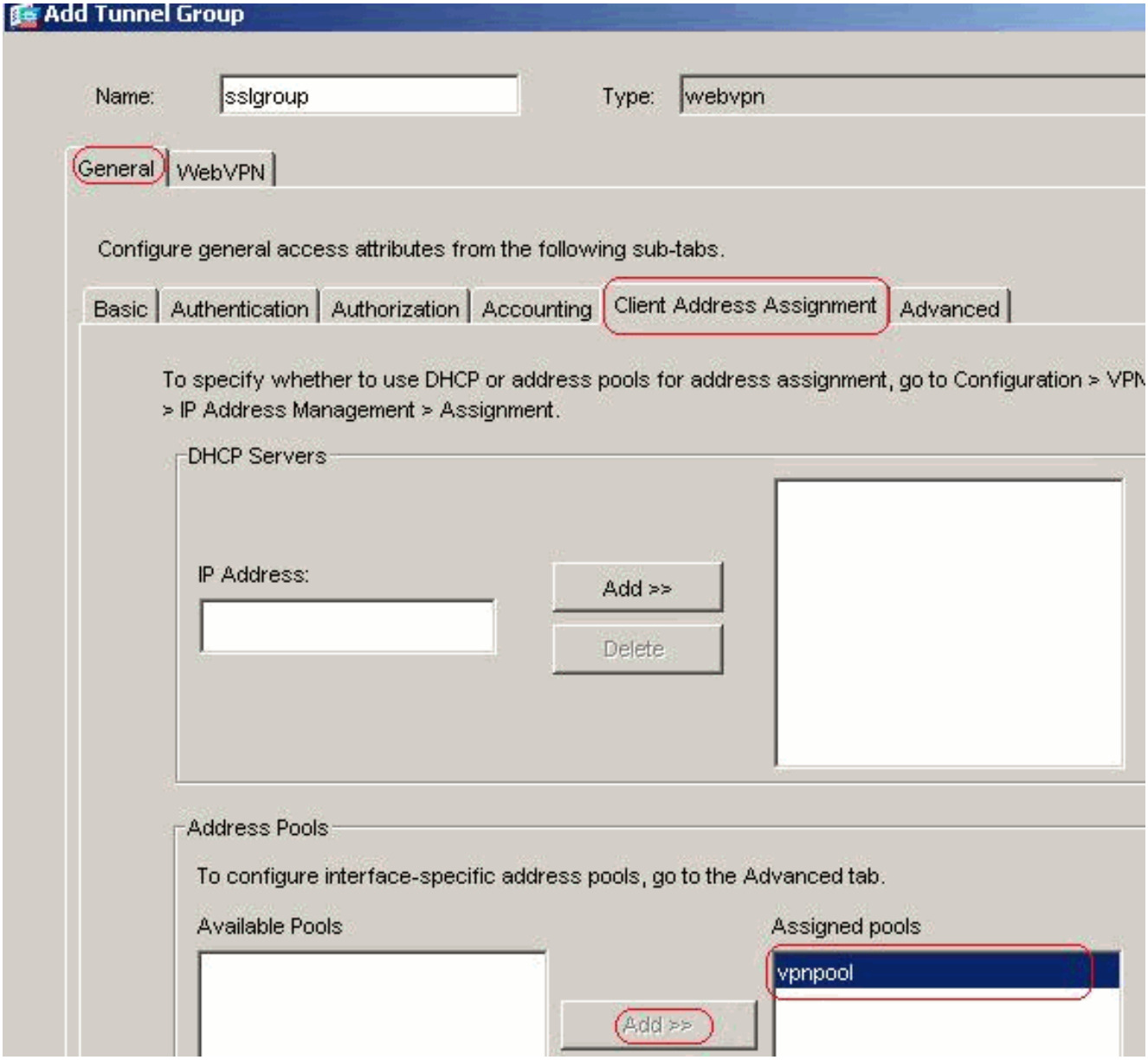


Configuração via CLI Equivalente:

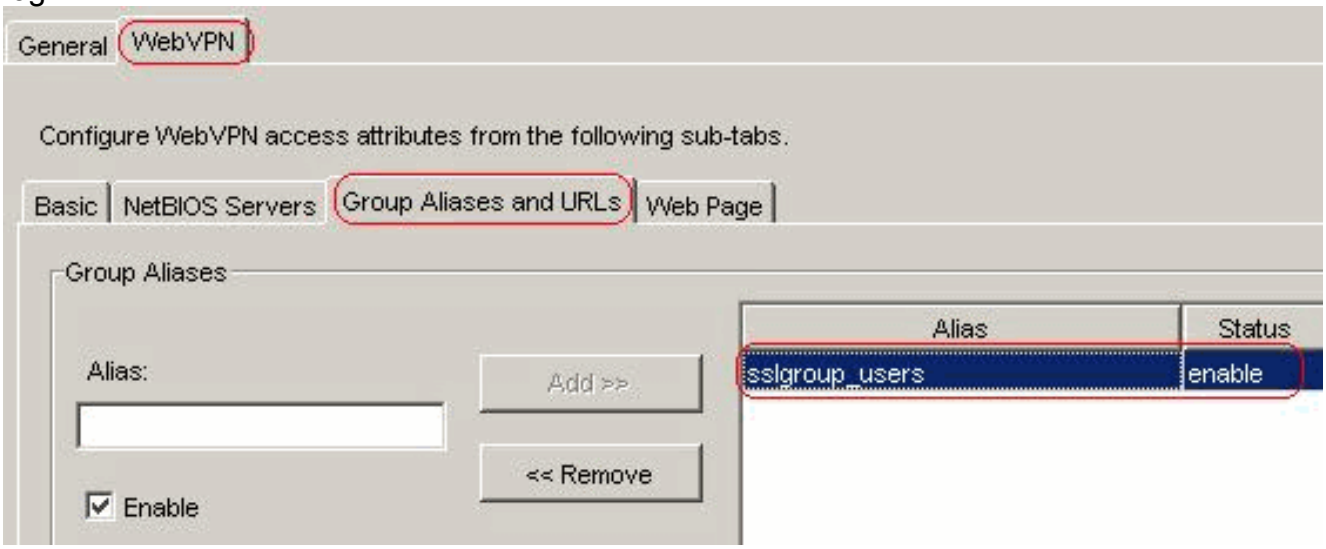
7. **Configure o Grupo de Túneis**Escolha **Configuration > VPN > General > Tunnel Group > Add (WebVPN access)** para criar um novo **sslgroup** de grupo de túneis.Na guia **Geral > Básico**, escolha a Política de Grupo como **clientgroup** na lista suspensa.



Em **Geral > Atribuição de Endereço do Cliente**, na guia Grupos de Endereços, clique em **Adicionar >>** para atribuir o pool de endereços disponível **vpnpool**.



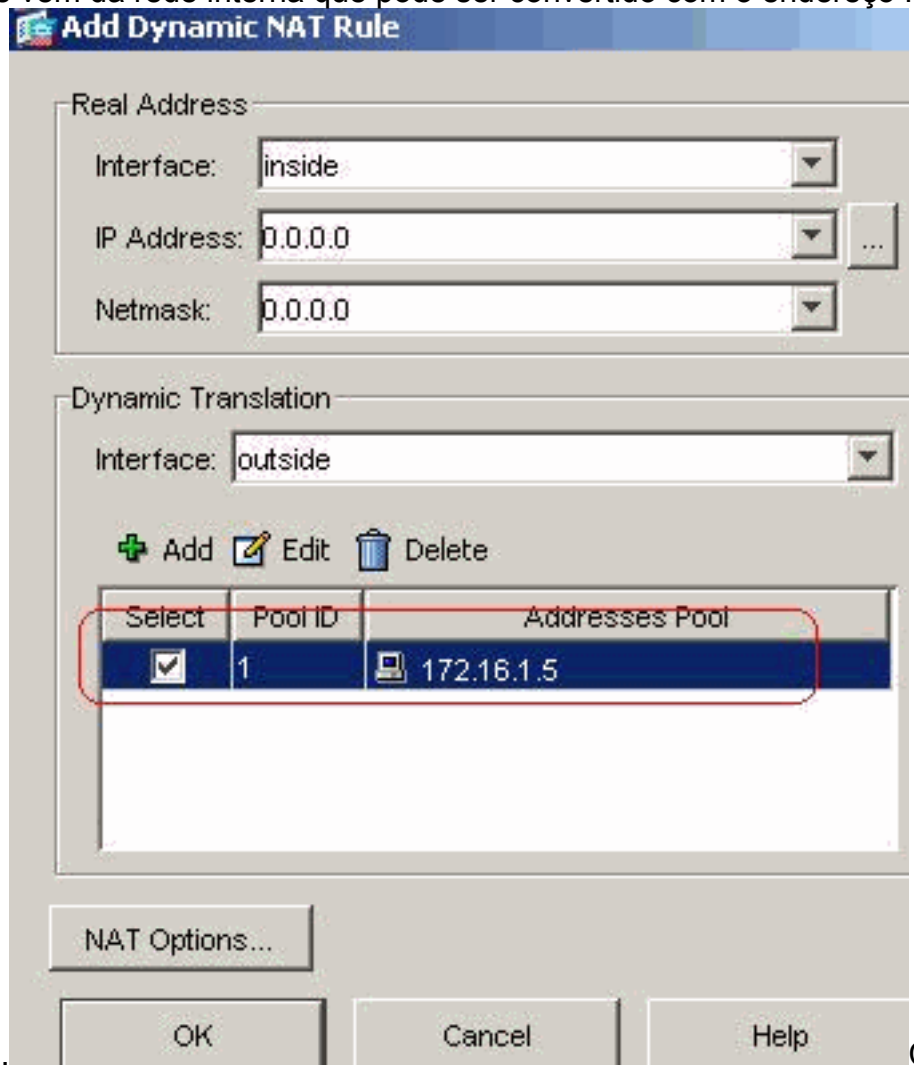
Na guia **WebVPN > Apelidos de grupo e URLs**, digite o nome do alias na caixa de parâmetros e clique em **Adicionar >>** para fazê-lo aparecer na lista de nomes de grupo na página de
login.



Clique em **OK e, em seguida, em Apply**.**Configuração via CLI Equivalente:**

8. **Configure o NAT**Escolha **Configuration > NAT > Add > Add Dynamic NAT Rule** para o

tráfego que vem da rede interna que pode ser convertido com o endereço IP externo



172.16.1.5. Clique em **OK** e clique em **Aplicar** na página principal.**Configuração via CLI Equivalente:**

9. Configure a isenção de nat para o tráfego de retorno da rede interna para o cliente VPN.

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
ciscoasa(config)#nat (inside) 0 access-list nonat
```

Configuração do ASA 7.2(2) usando CLI

Cisco ASA 7.2(2)
ciscoasa#**show running-config** : Saved : ASA Version 7.2(2) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside security-level 100 ip address 10.77.241.142 255.255.255.192 ! interface Ethernet0/1

```
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list split-tunnel standard permit 10.77.241.128
255.255.255.192
!--- ACL for Split Tunnel network list for encryption.
access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !--
- ACL to define the traffic to be exempted from NAT.
pager lines 24 mtu inside 1500 mtu outside 1500 ip local
pool vpnpool 192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 0.0.0.0 0.0.0.0


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup".
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-
```

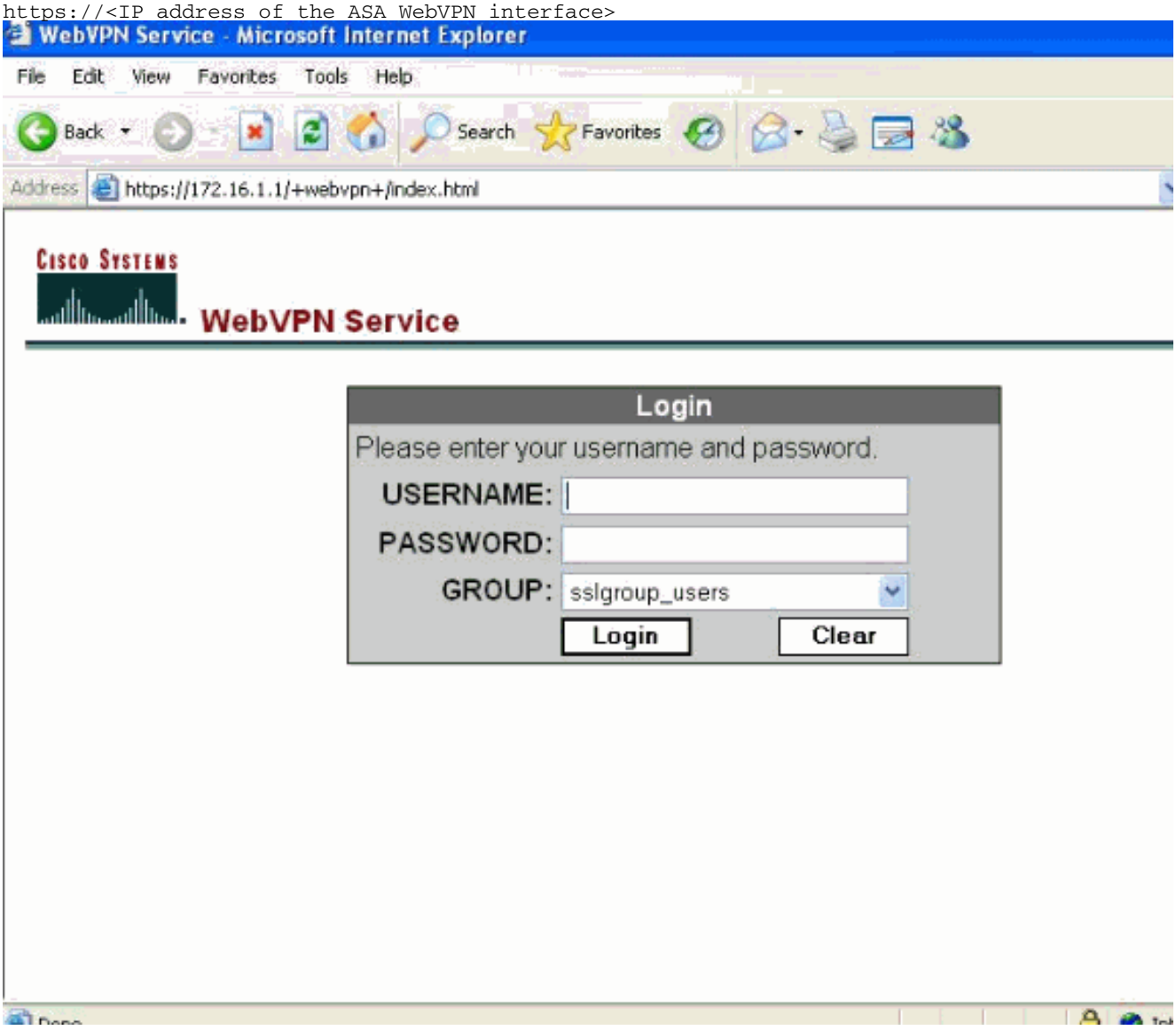
```
policy tunnelspecified
 split-tunnel-network-list value split-tunnel

!--- Encrypt the traffic specified in the split tunnel
ACL only. webvpn
  svc required

!--- Activate the SVC under webvpn mode. svc keep-
installer installed

!--- When the security appliance and the SVC perform a
rekey, !--- they renegotiate the crypto keys and
initialization vectors, !--- and increase the security
of the connection. svc rekey time 30

!--- Command that specifies the number of minutes !---
from the start of the session until the rekey takes
place, !--- from 1 to 10080 (1 week).  svc rekey method
ssl

!--- Command that specifies that SSL renegotiation !---
takes place during SVC rekey. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1". aaa local
authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server
enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as
WebVPN. tunnel-group sslgroup general-attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created.
default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created.
tunnel-group sslgroup webvpn-attributes

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet
timeout 5 ssh timeout 5 console timeout 0 ! 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
webvpn
 enable outside

!--- Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. svc enable

!--- Enable the security appliance to download !--- SVC
```

```
images to remote computers. tunnel-group-list enable

!--- Enable the display of the tunnel-group list !--- on
the WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

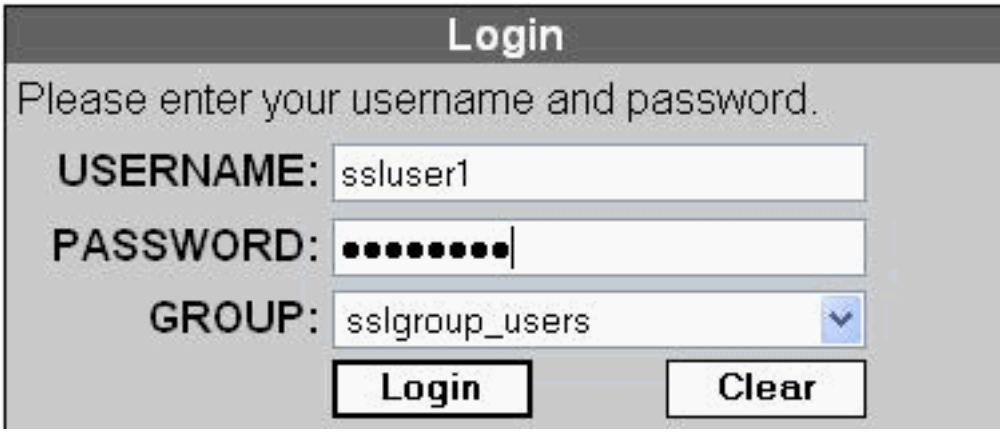
Estabeleça a conexão VPN SSL com o SVC

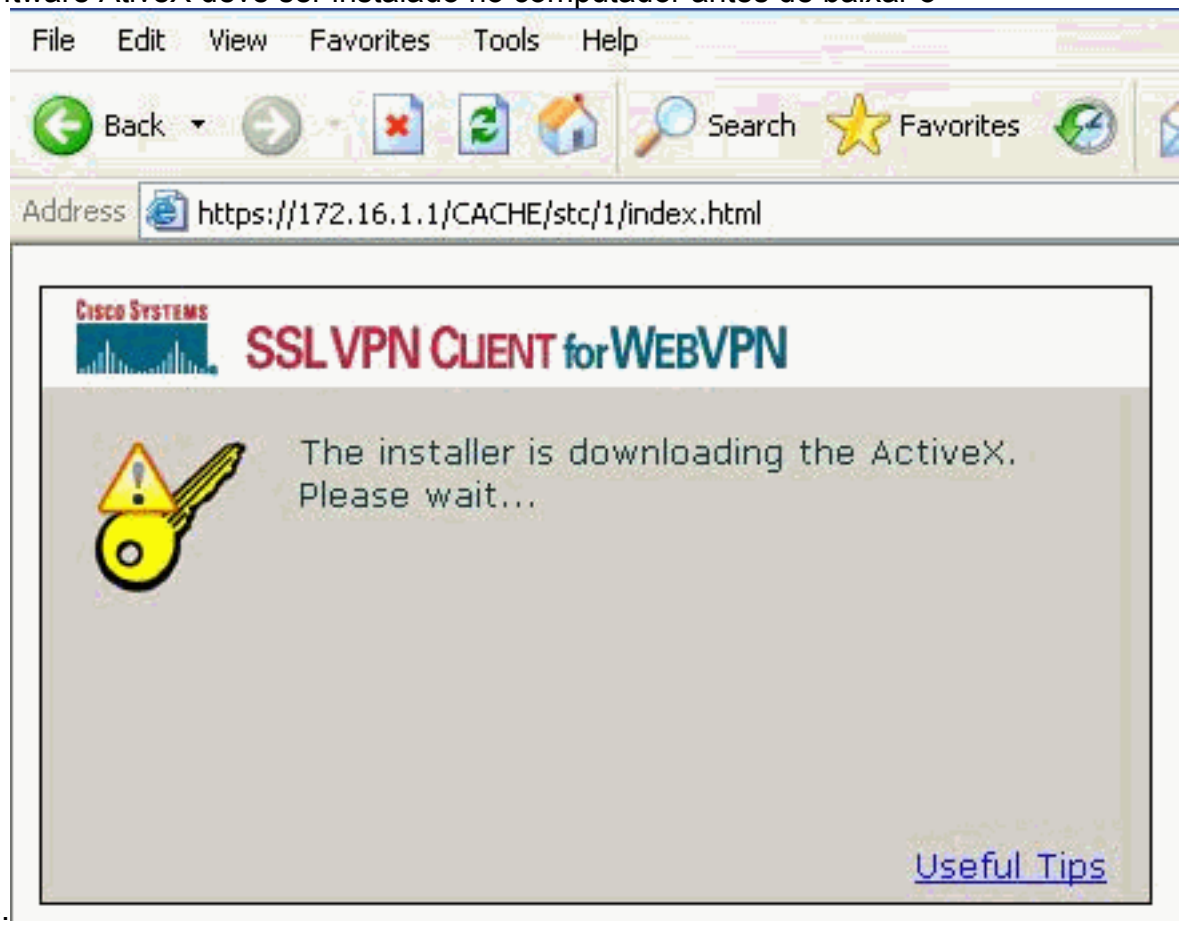
Conclua estes passos para estabelecer uma conexão VPN SSL com o ASA.

1. Digite o URL ou o endereço IP da interface WebVPN do ASA em seu navegador da Web no formato mostrado.
   `https://url`
   OU
   `https://<IP address of the ASA WebVPN interface>`



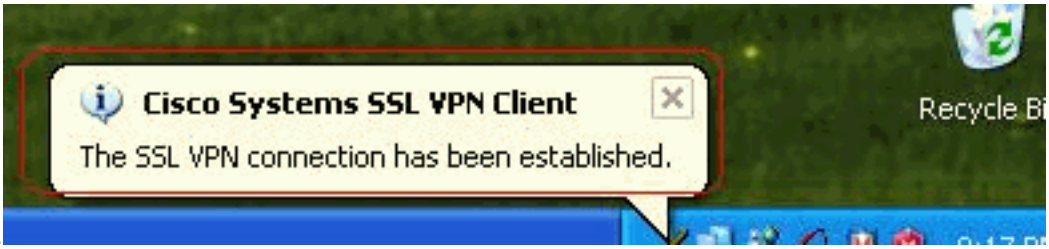
2. Digite seu nome de usuário e senha e escolha seu respectivo grupo na lista suspensa como

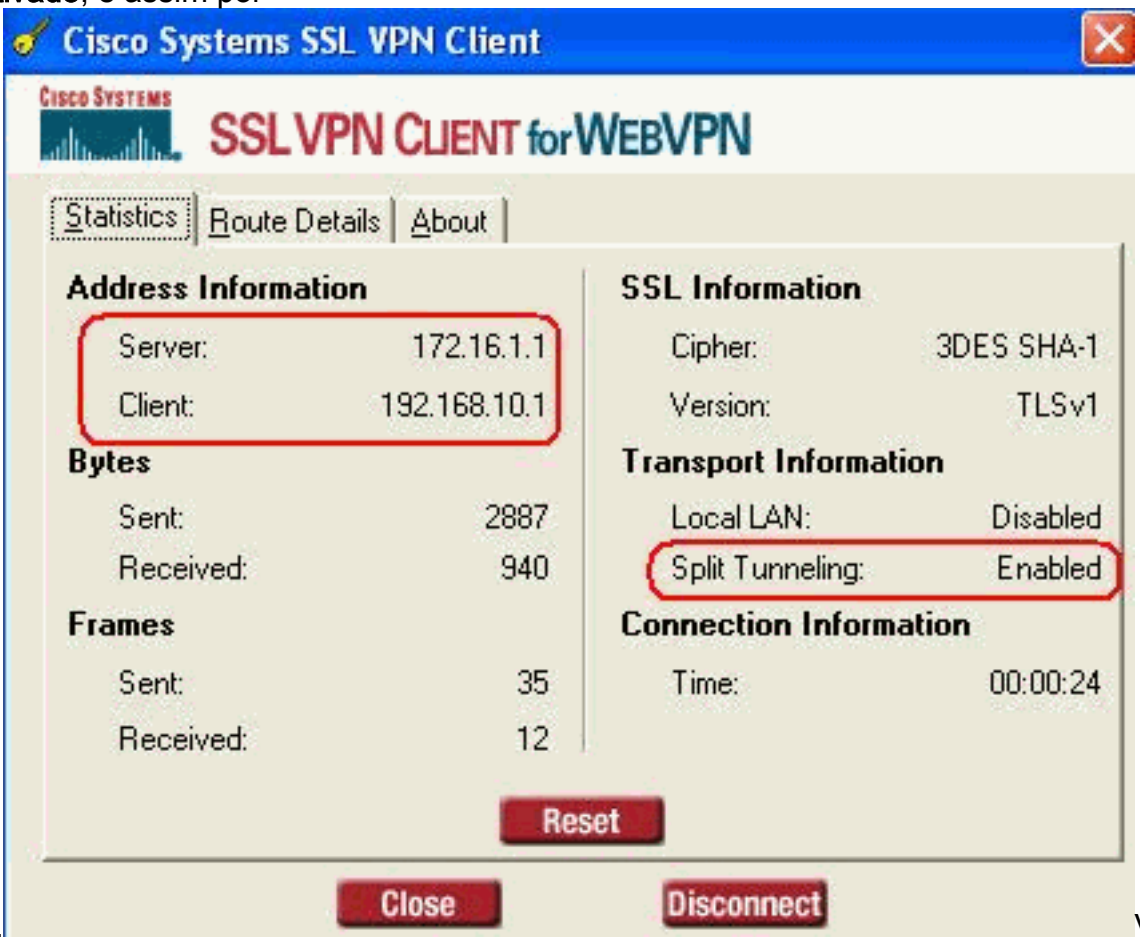
mostrado. 

3. O software AtiveX deve ser instalado no computador antes de baixar o SVC. 

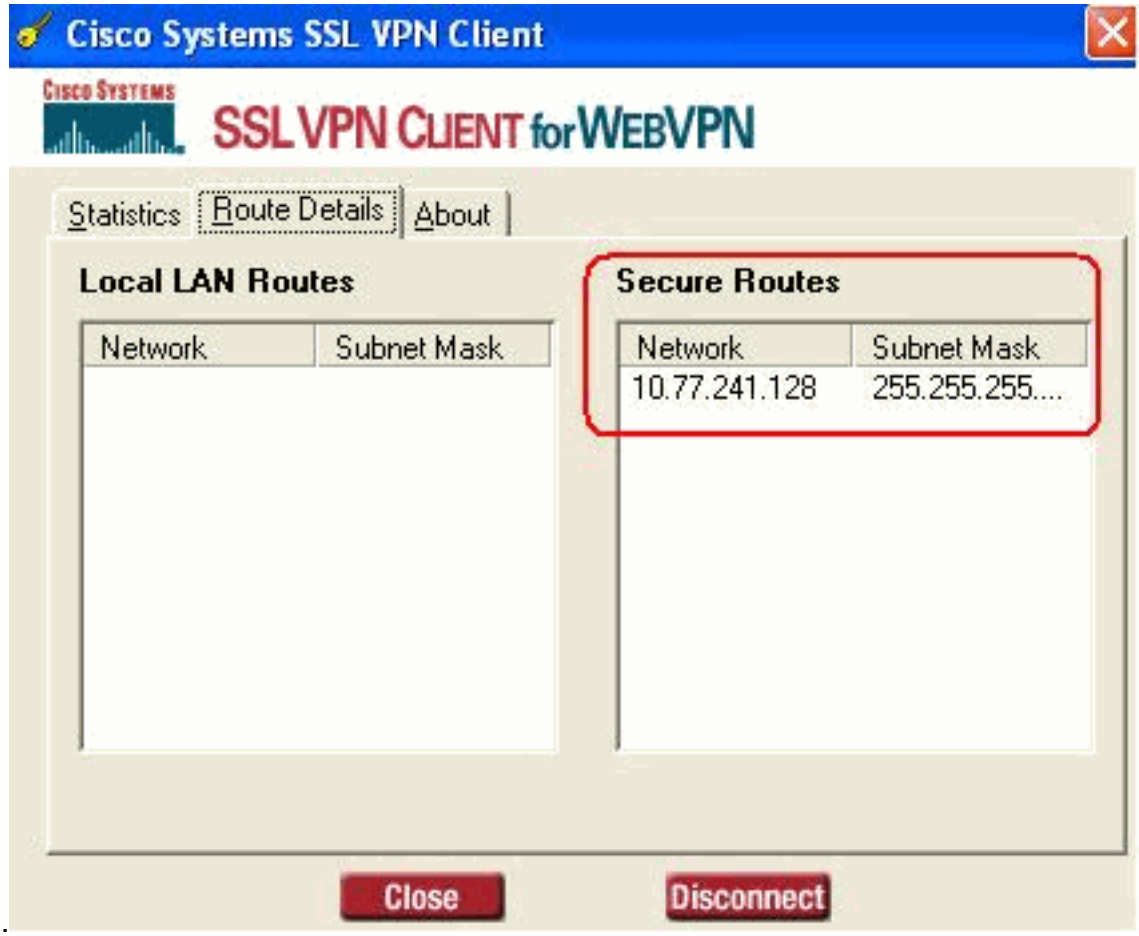
4. Essas janelas aparecem antes que a conexão VPN SSL seja estabelecida. 

5. Essas janelas podem ser obtidas assim que a conexão for

estabelecida. 

6. Clique na tecla amarela exibida na barra de tarefas do computador. Essas janelas são exibidas e fornecem informações sobre a conexão SSL. Por exemplo, **192.168.10.1** é o IP atribuído para o endereço IP do cliente e do servidor é 172.16.1.1, **o tunelamento dividido está ativado**, e assim por diante. 

Você também pode verificar a rede segura a ser criptografada por SSL, a lista de rede é baixada da lista de acesso de túnel dividido configurada no ASA.Neste exemplo, o SSL VPN Client protege o acesso a 10.77.241.128/24 enquanto todo o tráfego restante não é criptografado e não é enviado através do



túnel.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

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

- **show webvpn svc — Mostra as imagens do SVC armazenadas na memória flash do ASA.**

```
ciscoasa#show webvpn svc
1. disk0:/sslclient-win-1.1.4.179.pkg 1
  CISCO STC win2k+ 1.0.0
  1,1,4,179
  Fri 01/18/2008 15:19:49.43

1 SSL VPN Client(s) installed
```

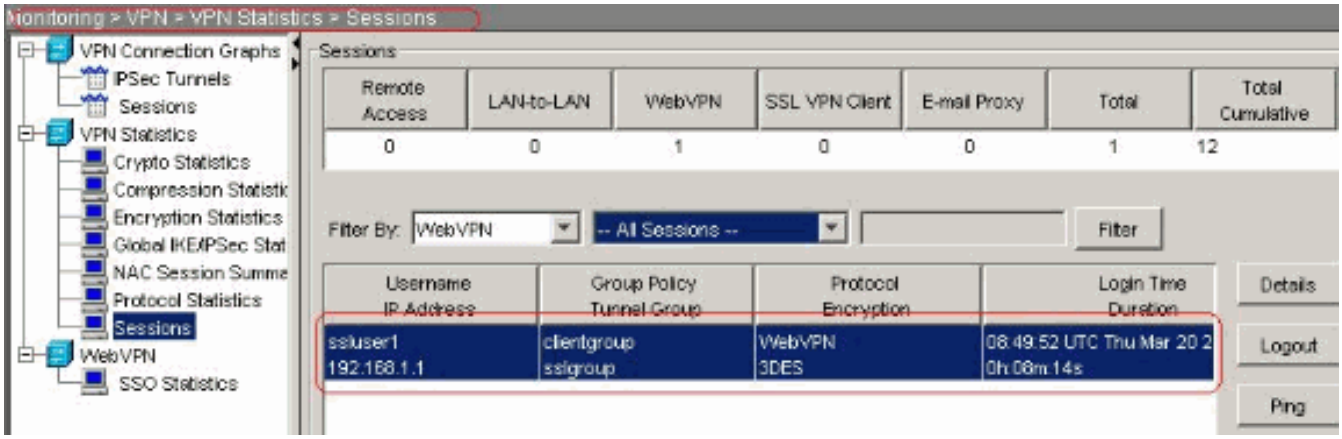
- **show vpn-sessiondb svc — Mostra informações sobre as conexões SSL atuais.**

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1
Index        : 1
Assigned IP  : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : SVC                    Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 131813                 Bytes Rx     : 5082
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration     : 0h:00m:53s
Filter Name  :
```

- **show webvpn group-alias — Exibe o alias configurado para vários grupos.**

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- No ASDM, escolha **Monitoring > VPN > VPN Statistics > Sessions** para saber sobre as sessões atuais do WebVPN no ASA.



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

1. **vpn-sessiondb logoff name <username> — Comando para desconectar a sessão VPN SSL**

para o nome de usuário específico.

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Called vpn_remove_uauIth: success!
webvpn_svc_np_tear_down: no ACL
NFO: Number of sessions with name "ssluser1" logged off : 1
```

De forma semelhante, você pode utilizar o comando vpn-sessiondb logoff svc para encerrar todas as seções do SVC.

2. Observação: se o PC for para o modo de espera ou hibernação, a conexão VPN SSL poderá ser encerrada.

```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL
```

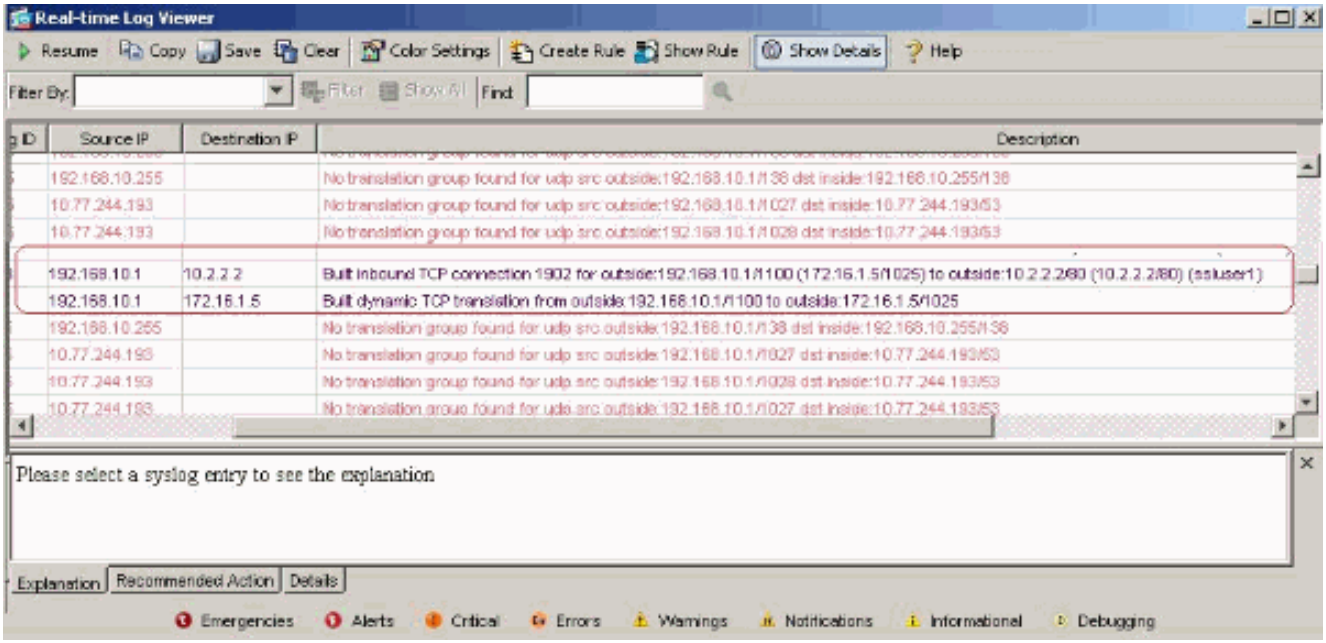
```
ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

3. depurar o webvpn svc <1-255> — Fornece os eventos tempos real do WebVPN a fim de estabelecer a sessão.

```
Ciscoasa#debug webvpn svc 7

ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
```

```
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
SVC: Sending response
CSTP state = CONNECTED
```

4. No ASDM, selecione **Monitoring > Logging > Real-time Log Viewer > View para ver os eventos em tempo real.** Este exemplo mostra as informações da sessão entre o SVC 192.168.10.1 e o Servidor Web 10.2.2.2 na Internet através do ASA 172.16.1.5.



Informações Relacionadas

- Suporte ao produto Cisco 5500 Series Adaptive Security Appliance
- ASA/PIX: Exemplo de Configuração de Habilitação do Tunelamento Dividido for VPN Clients no ASA
- Exemplo de Configuração de Roteador que Permite Clientes VPN se Conectarem via IPsec e à Internet Usando a Separação de Túneis
- Exemplo de Configuração de PIX/ASA 7.x e VPN Client para VPN de Internet Pública "on a Stick"
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Suporte Técnico e Documentação - Cisco Systems