ASA 8.x: Permita o Split Tunneling para o cliente VPN de AnyConnect no exemplo de configuração ASA

Índice

Introdução

Este documento fornece instruções passo a passo sobre como permitir o acesso do Cisco AnyConnect VPN Client à Internet quando eles estão tunelados em um Cisco Adaptive Security Appliance (ASA) 8.0.2. Esta configuração permite ao cliente acesso seguro aos recursos corporativos via SSL enquanto concede acesso não protegido à Internet através do tunelamento dividido.

Pré-requisitos

Requisitos

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

- O ASA Security Appliance deve executar a versão 8.x
- Cisco AnyConnect VPN Client 2.x**Nota:** Faça download do pacote do AnyConnect VPN Client (anyconnect-win*.pkg) do Download de Software Cisco (somente clientes registrados). Copie o AnyConnect VPN client para a memória flash do ASA, a qual será transferida para os computadores do usuário remoto a fim de estabelecer a conexão VPN SSL com o ASA. Consulte a seção Instalação do AnyConnect Client do guia de configuração do ASA para

obter mais informações.

Componentes Utilizados

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

- Cisco 5500 Series ASA com software versão 8.0(2)
- Cisco AnyConnect SSL VPN Client para Windows versão 2.0.0343
- PC com Microsoft Windows Vista, Windows XP SP2 ou Windows 2000 Professional SP4 com Microsoft Installer versão 3.1
- Cisco Adaptive Security Device Manager (ASDM) versão 6.0(2)

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 Cisco AnyConnect VPN Client fornece conexões SSL seguras ao Security Appliance para usuários remotos. Sem um cliente previamente instalado, os usuários remotos inserem o endereço IP em seu navegador de uma interface configurada para aceitar conexões VPN SSL. A menos que o Security Appliance seja configurado para redirecionar pedidos de http:// para https://, os usuários deverão inserir o URL na forma https://<endereço>.

Após a inserção do URL, o navegador se conecta a essa interface e exibe a tela de login. Se o usuário satisfizer o login e a autenticação, e o Security Appliance identificar que o usuário necessita do cliente, ele faz o download do cliente correspondente ao sistema operacional do computador remoto. Após o download, o cliente é instalado e configurado automaticamente, estabelece uma conexão SSL segura e permanece ou se desinstala (dependendo da configuração do Security Appliance) quando a conexão é encerrada.

No caso de um cliente previamente instalado, quando o usuário autentica, o Security Appliance examina a revisão do cliente e faz seu upgrade conforme o necessário.

Quando o cliente negocia uma conexão VPN SSL com o Security Appliance, ele se conecta usando o Transport Layer Security (TLS), e opcionalmente, o Datagram Transport Layer Security (DTLS). O DTLS, evita os problemas de largura de banda e latência associados a algumas conexões SSL e melhora o desempenho dos aplicativos em tempo real que são sensíveis aos atrasos de pacote.

O AnyConnect Client pode ser obtido do Security Appliance ou pode ser instalado manualmente no PC remoto pelo administrador do sistema. Refira o guia do administrador do Cisco AnyConnect VPN Client para obter mais informações sobre de como instalar manualmente o cliente.

O Security Appliance faz o download do cliente com base na política do grupo ou nos atributos de nome de usuário do usuário que estabelece a conexão. Você pode configurar o Security Appliance para fazer o download automático do cliente ou para perguntar ao usuário remoto se ele deseja fazer o download. No último caso, se o usuário não responder, você poderá configurar o Security Appliance para fazer o download do cliente após um período de timeout ou apresentar a página de login.

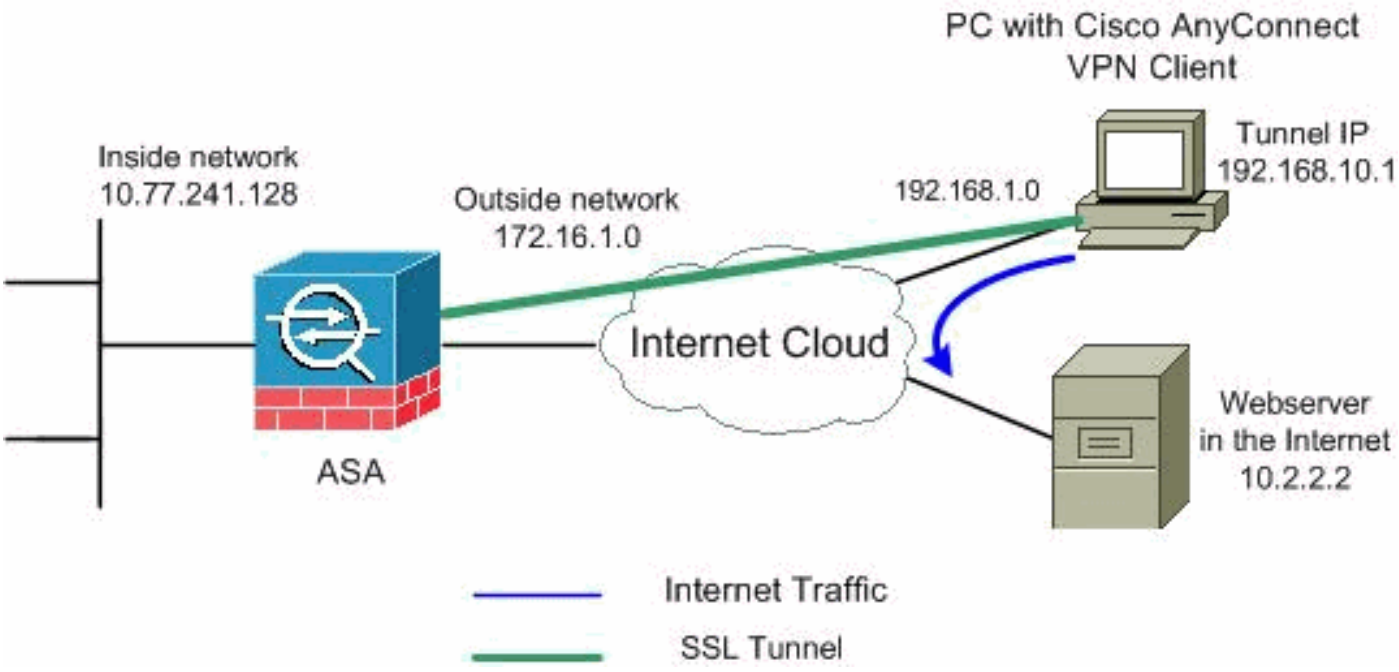
Configurar

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:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Configuração do ASA com o ASDM 6.0(2)

Este documento supõe que a configuração básica, como a configuração da interface esteja pronta e funcionando corretamente.

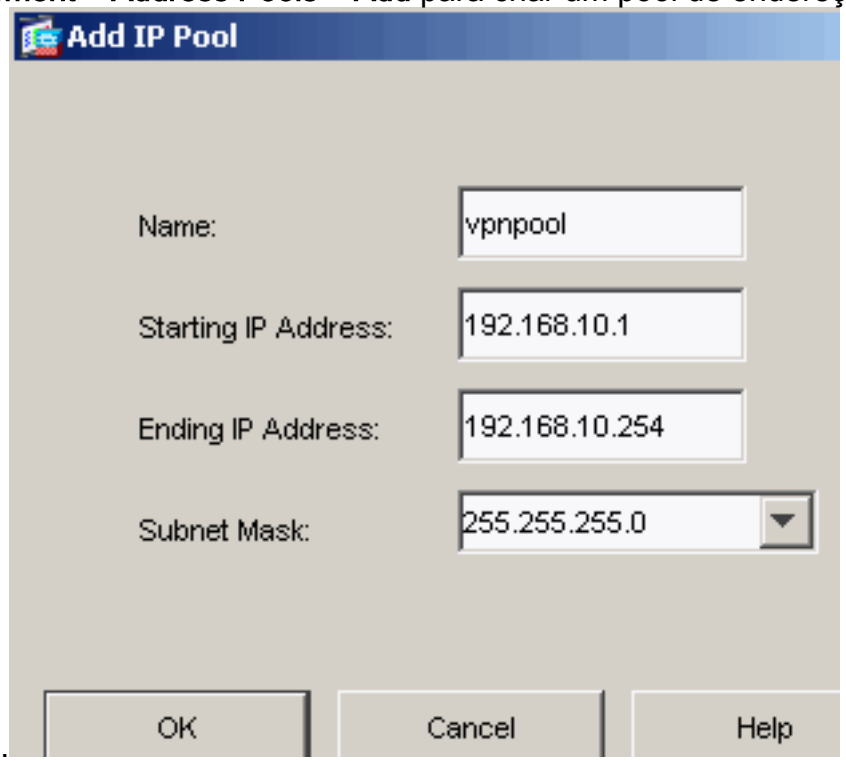
Nota: Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.

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

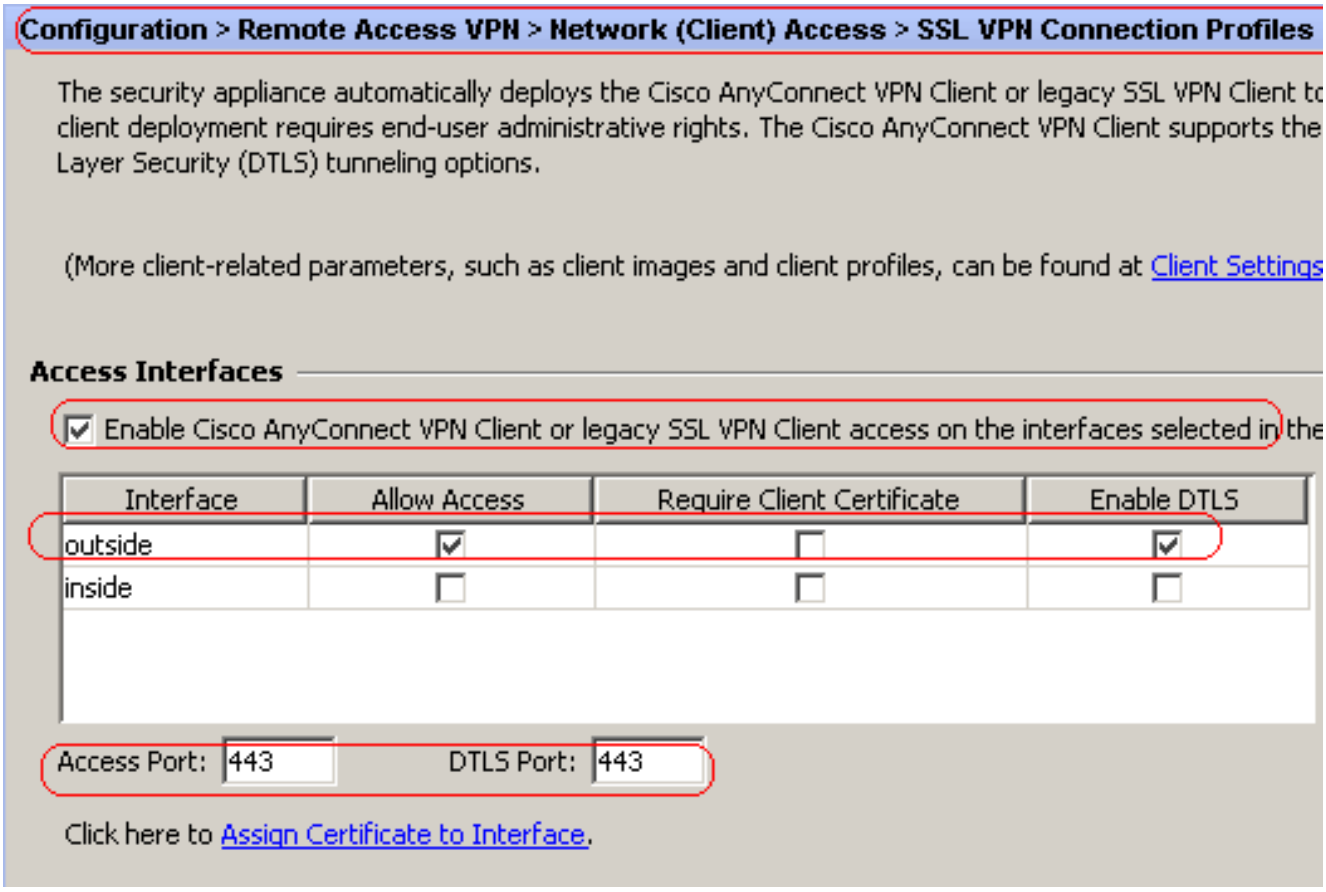
ASA para obter mais informações.

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

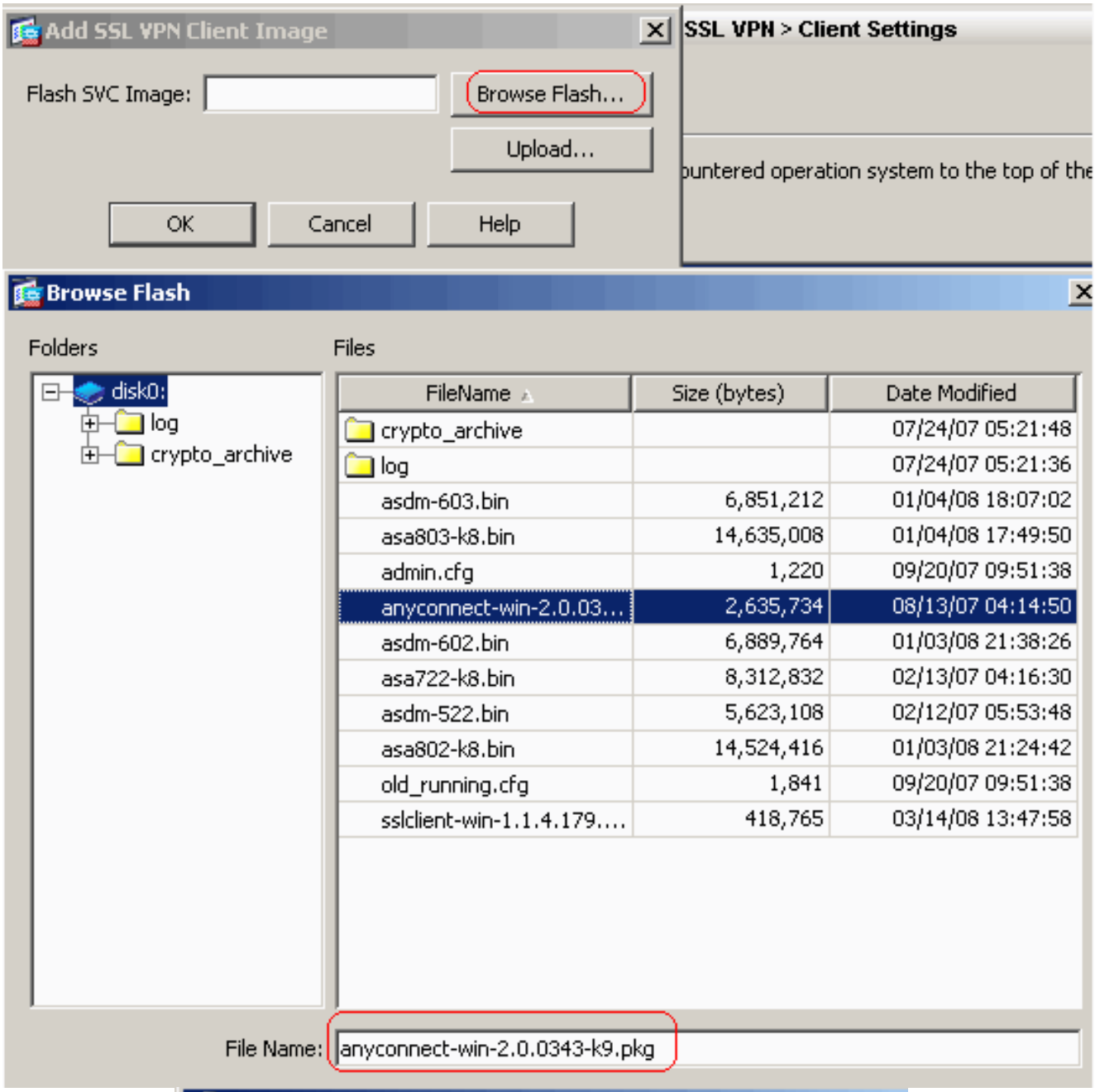
1. Selecione **Configuration > Remote Access VPN > Network (Client) Access > Address Management > Address Pools > Add** para criar um pool de endereços IP vpnpool.

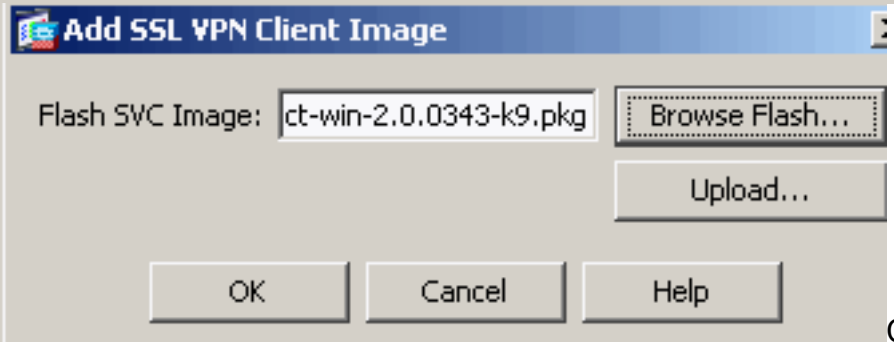


2. Clique em Apply.**Configuração via CLI Equivalente:**
3. Ative o WebVPN.Selecione **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** e, sob **Access Interfaces**, clique nas caixas de seleção **Allow Access** e **Enable DTLS** para a interface externa. Além disso, marque a caixa de seleção **Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below** para ativar a VPN SSL na interface externa.



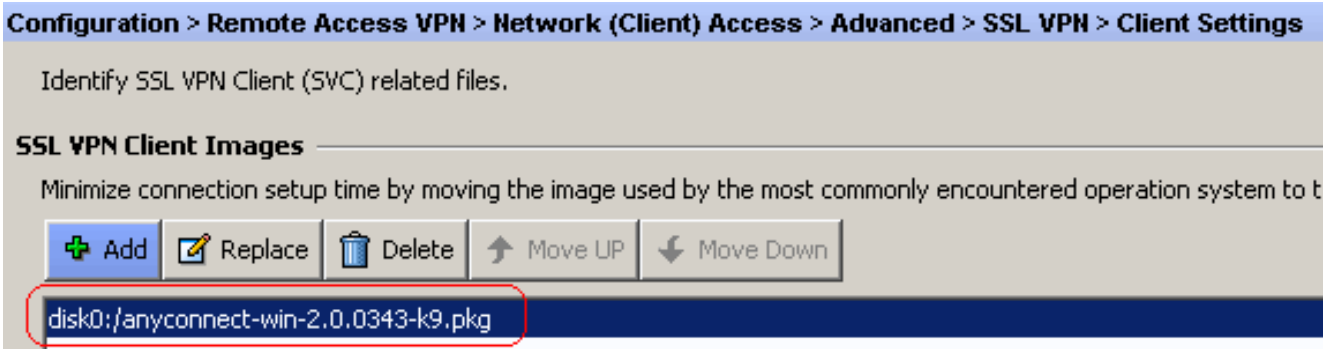
Clique em Apply.Selecione **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings > Add** para adicionar a imagem do Cisco AnyConnect VPN Client da memória flash do ASA conforme mostrado.





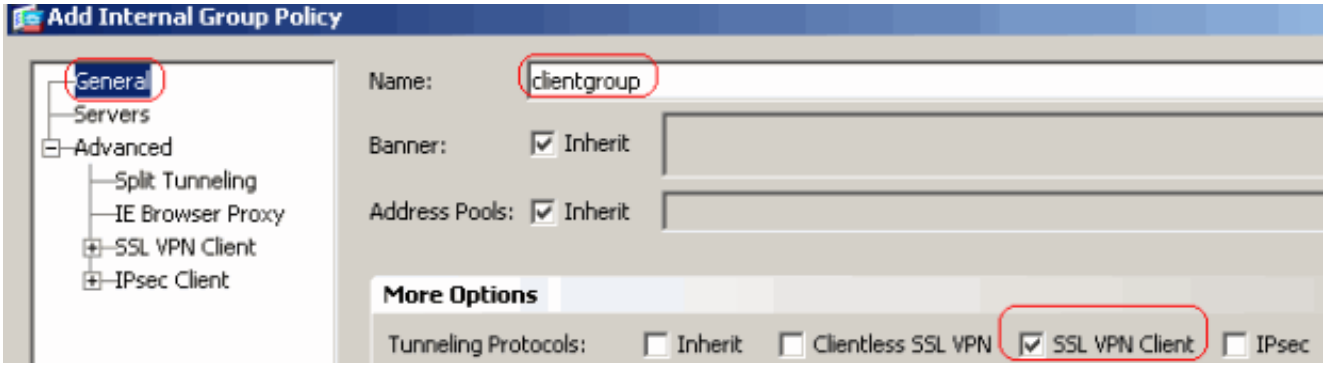
Clique em **OK**.

Clique em Add.

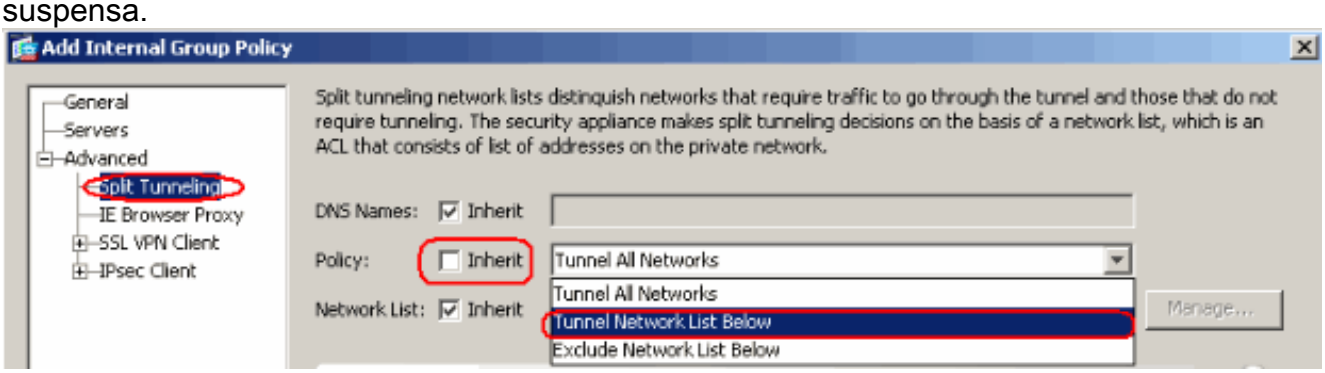


Configuração via CLI Equivalente:

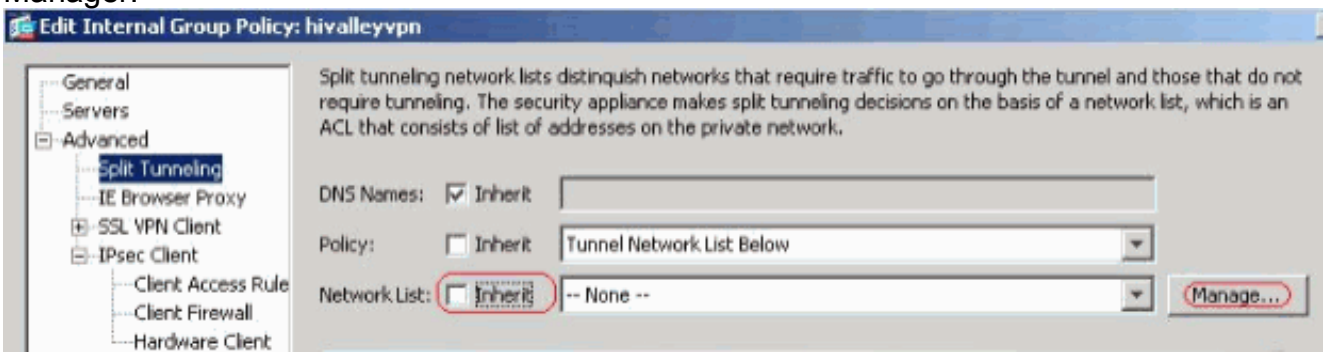
4. Configure a Política de Grupo.Selecione **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** para criar uma política de grupo interna **clientgroup**. Na guia **General**, marque a caixa de seleção **SSL VPN Client** para ativar a WebVPN como protocolo de tunelamento.



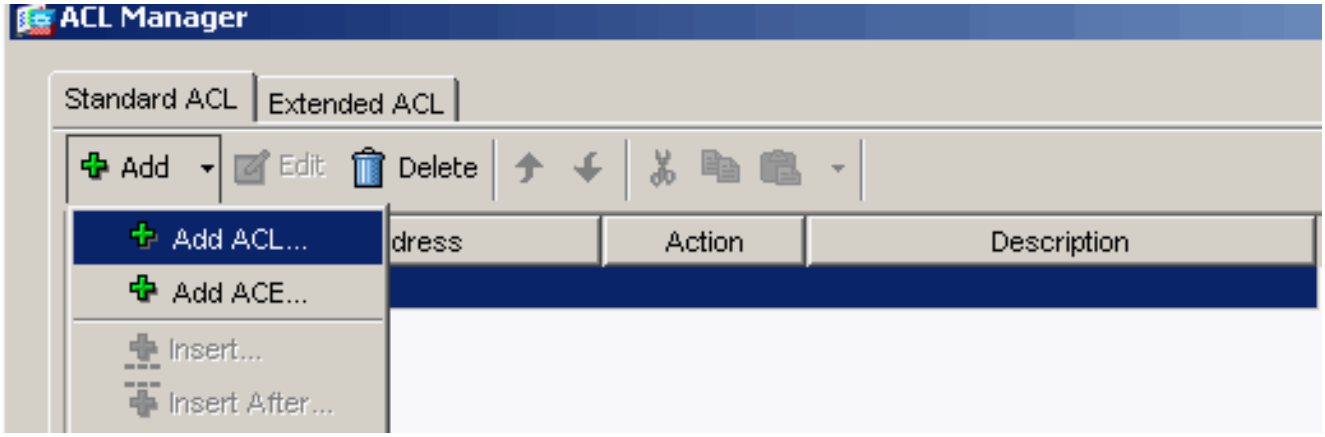
Na guia **Advanced > Split Tunneling**, desmarque a caixa de seleção **Inherit** para a política de tunelamento dividido e escolha **Tunnel Network List Below** na lista suspensa.



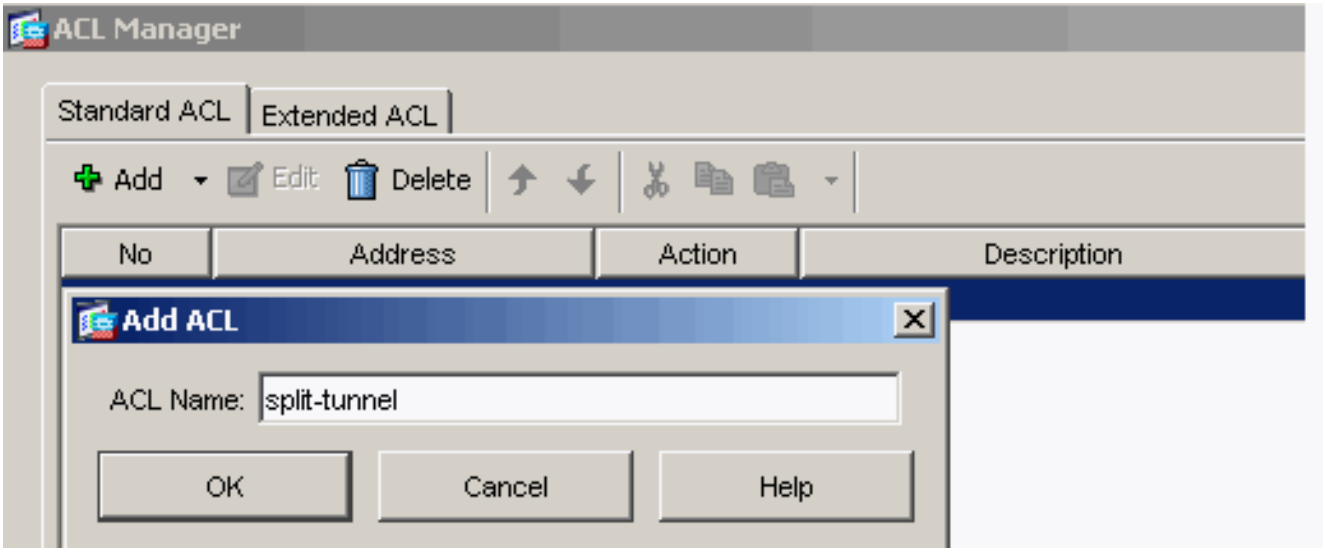
Desmarque a caixa de seleção **Inherit** para **Split Tunnel Network List** e, em seguida, clique em **Manage** para iniciar o ACL Manager.



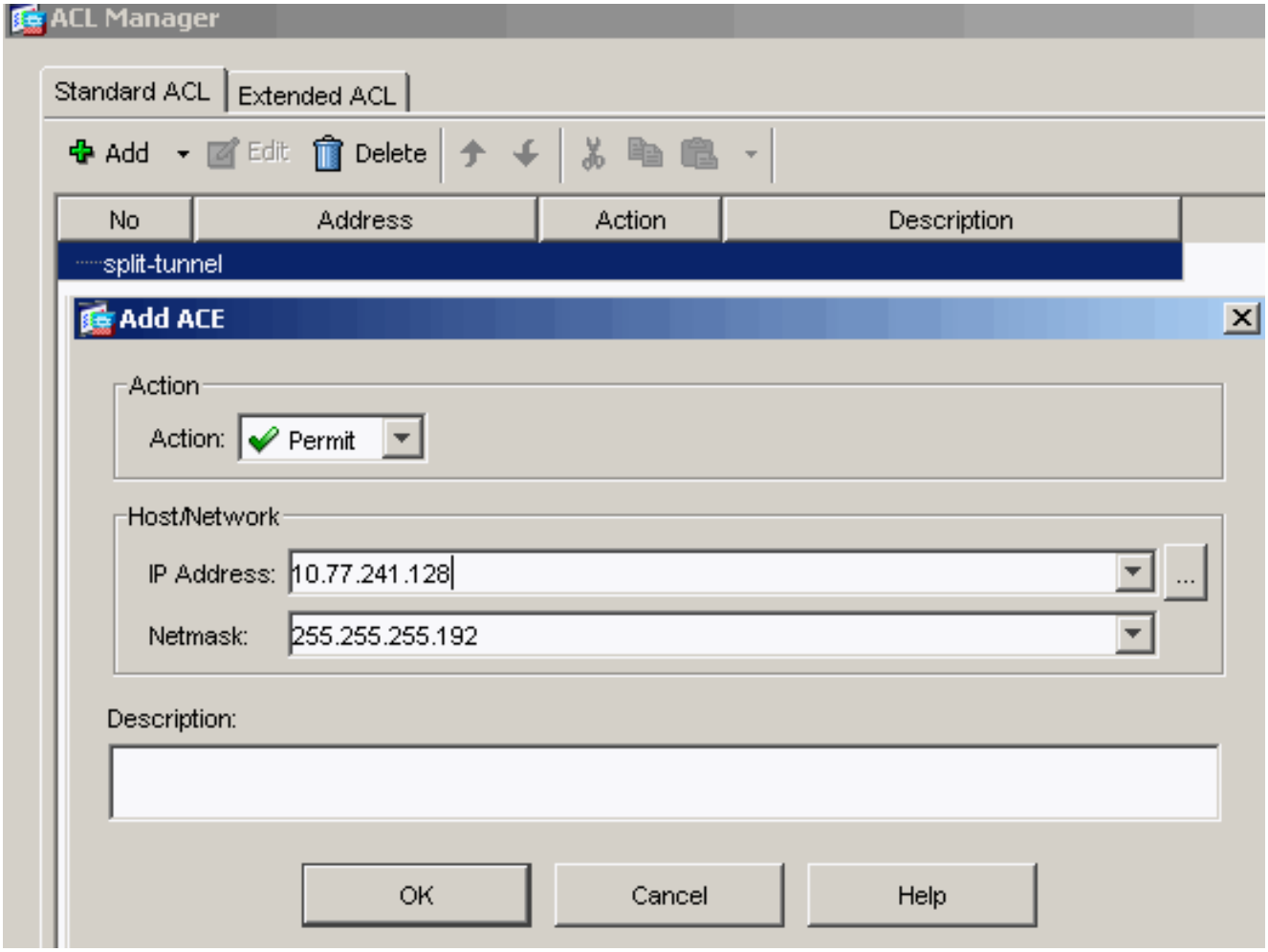
No ACL Manager, selecione **Add > Add ACL...** para criar uma nova lista de acesso.



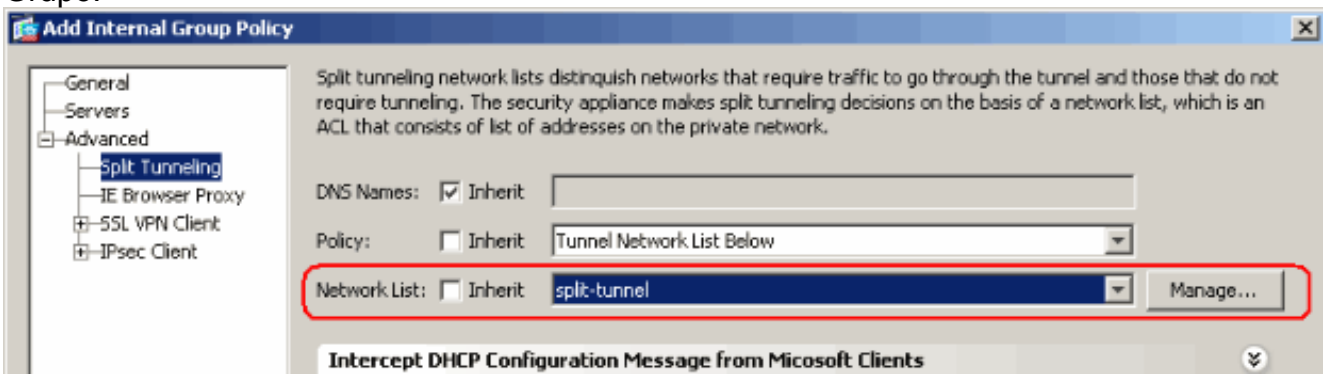
Forneça um nome para a ACL e clique em
OK.



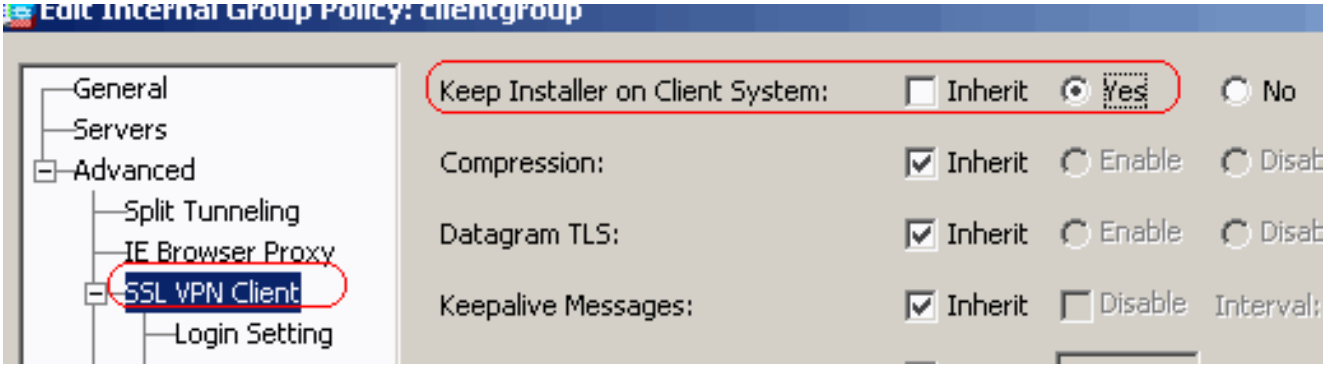
Uma vez que o nome da ACL é criado, escolha **Add > Add ACE** para adicionar uma entrada de controle de acesso (ACE).Defina a ACE que corresponde à LAN por trás do ASA. Neste caso, a rede é 10.77.241.128/26 e selecione a **Permit** como a ação.Clique em **OK** para sair do ACL
Manager.



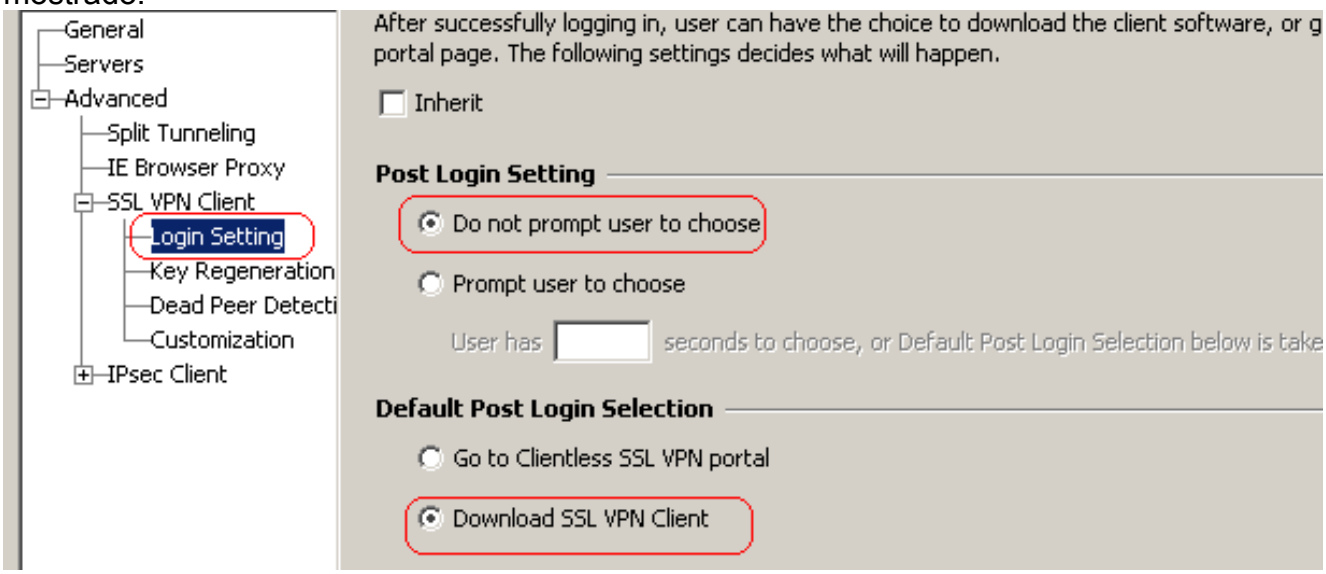
Certifique-se de que o ACL que você acabou de criar esteja selecionado para a lista de redes do túnel dividido. Clique em **OK** para retornar à configuração da Política de Grupo.



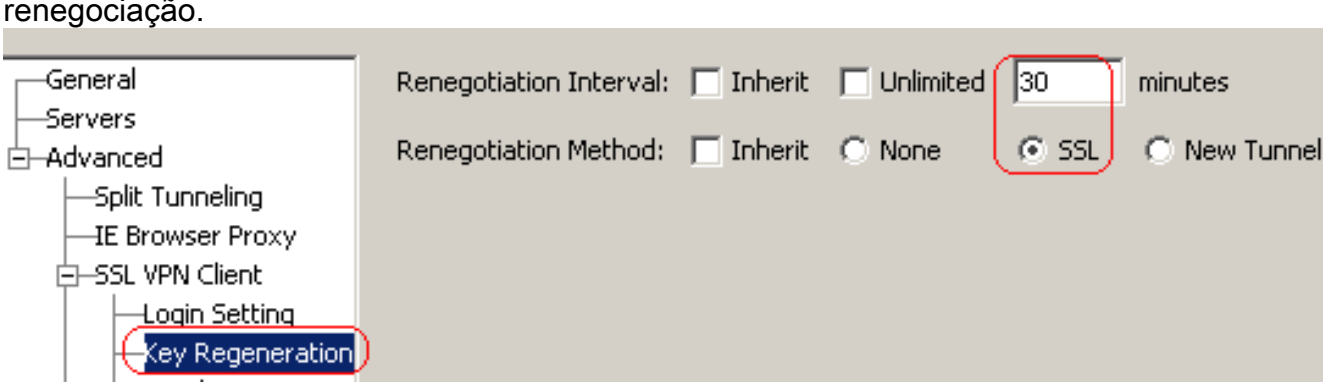
Na página principal, clique em **Apply** e em Send (se necessário) para enviar os comandos ao ASA.Configure as opções da **VPN SSL** no modo de política de grupo.Para a opção Keep Installer on Client System, desmarque a caixa de seleção **Inherit** e clique no botão de opção **Yes**.Esta ação permite 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.



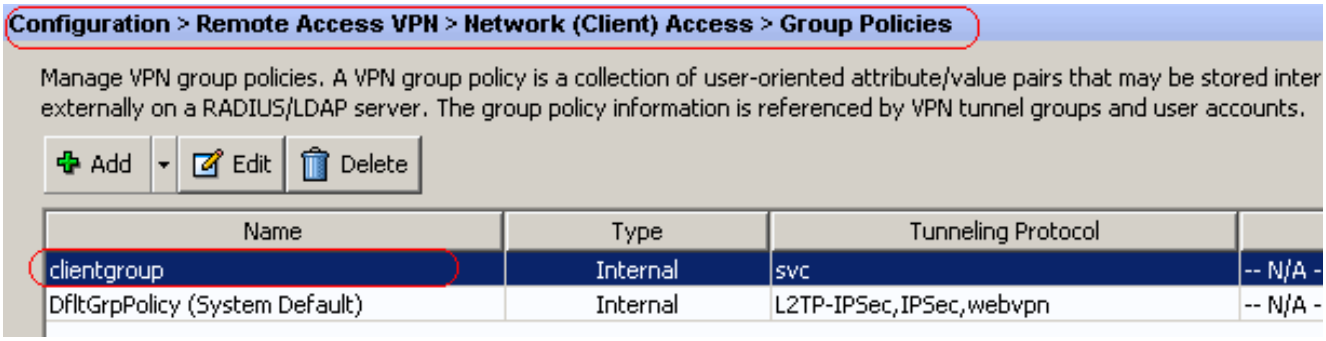
Clique em **Login Setting** para definir as opções **Post Login Setting** e **Default Post Login Selection** conforme mostrado.



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 aumentada com a definição de limites no intervalo de tempo durante o qual 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.

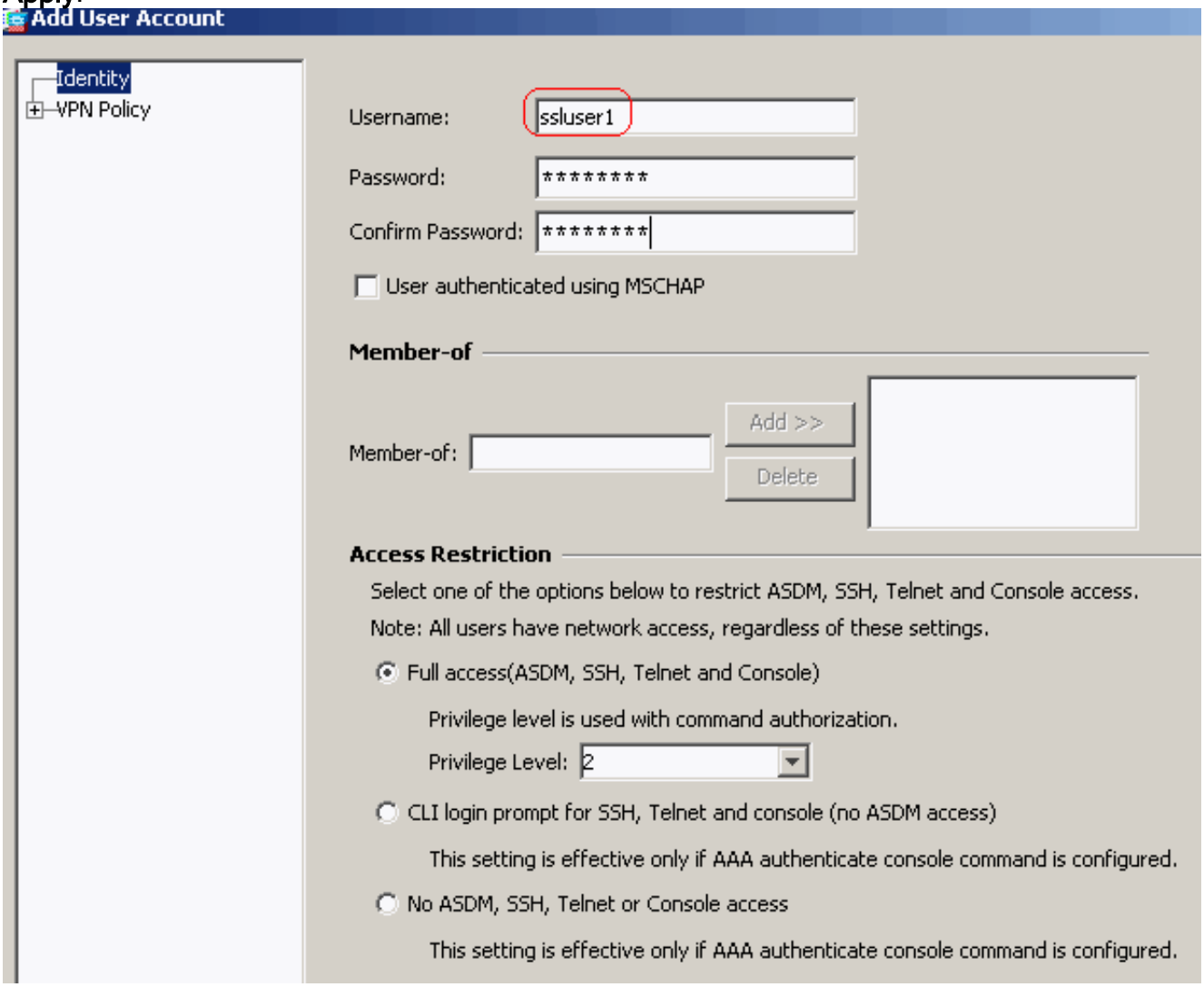


Clique em **OK** e, em seguida, em **Apply**.



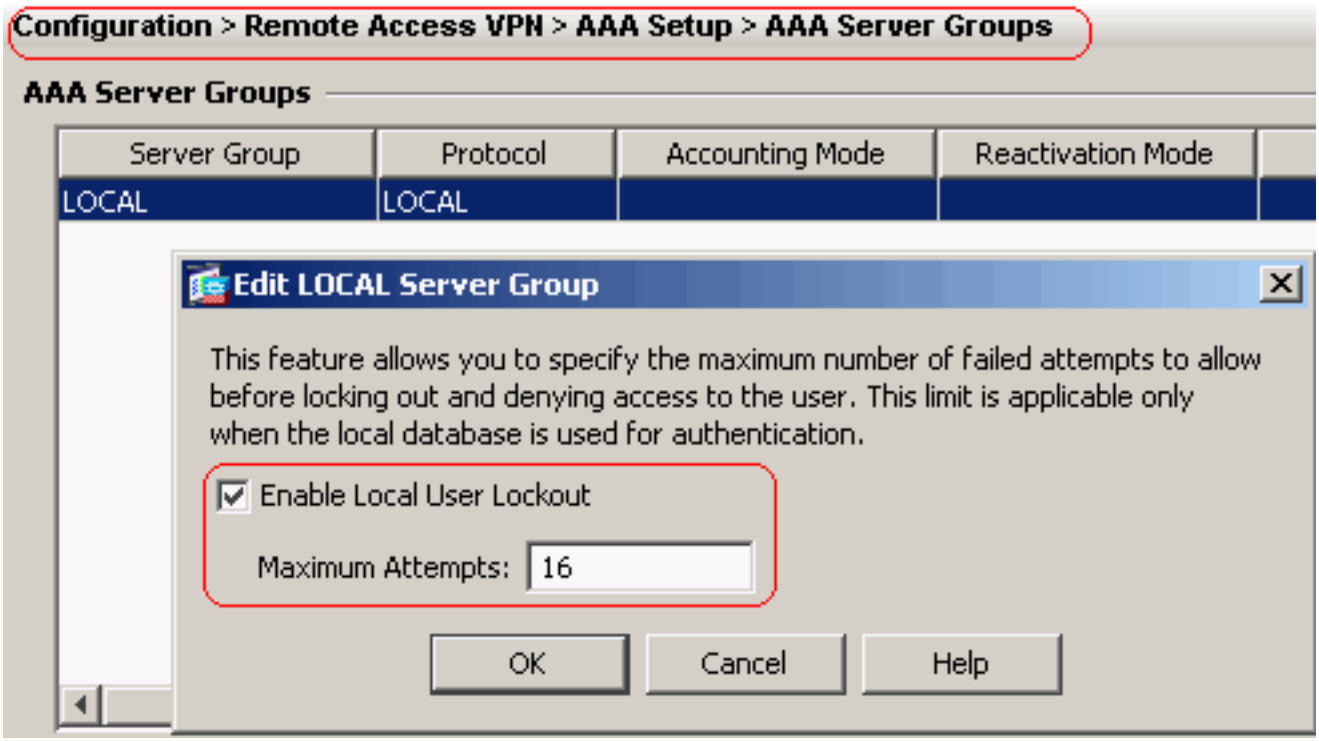
Configuração via CLI Equivalente:

5. Selecione **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** para criar uma nova conta de usuário **ssluser1**. Clique em **OK** e, em seguida, em **Apply**.

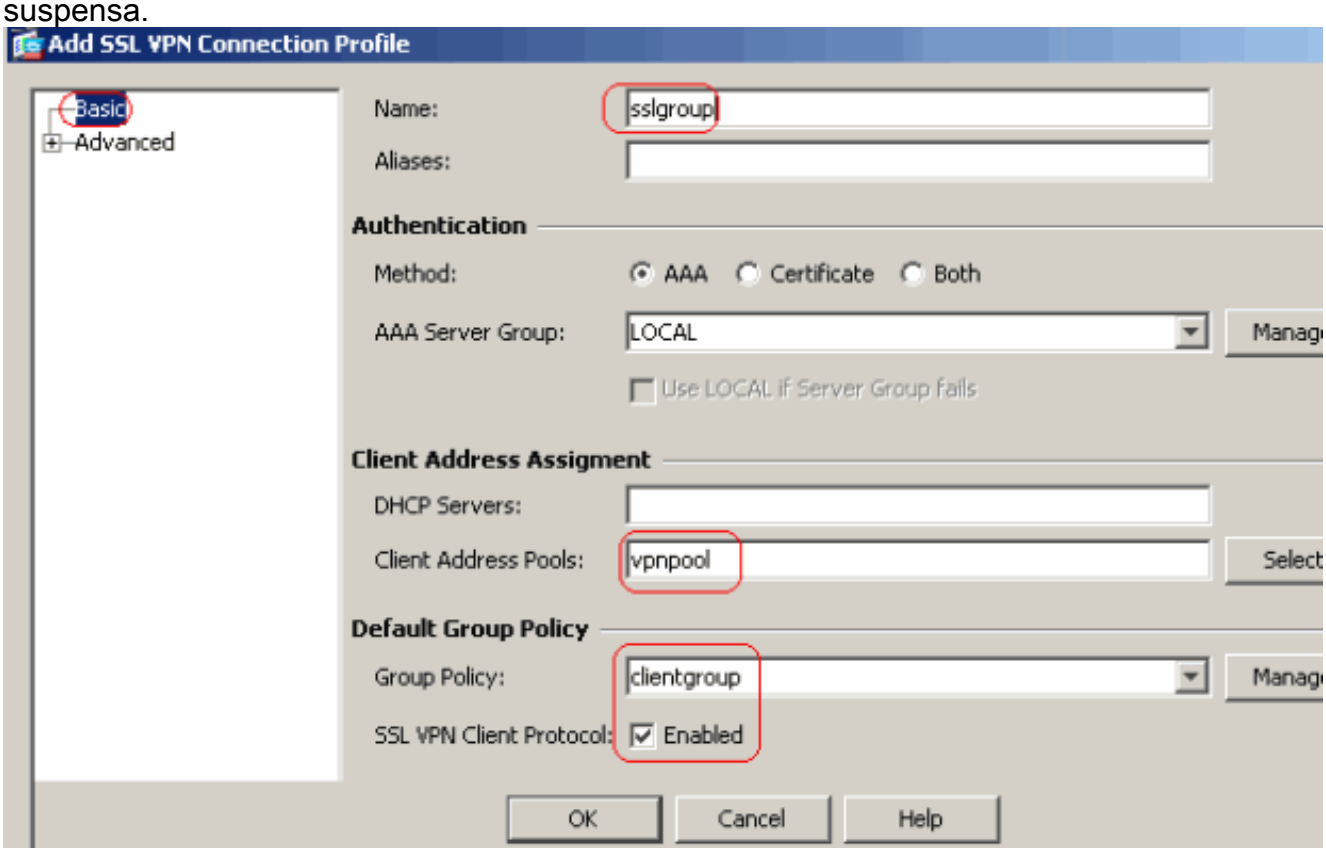


Configuração via CLI Equivalente:

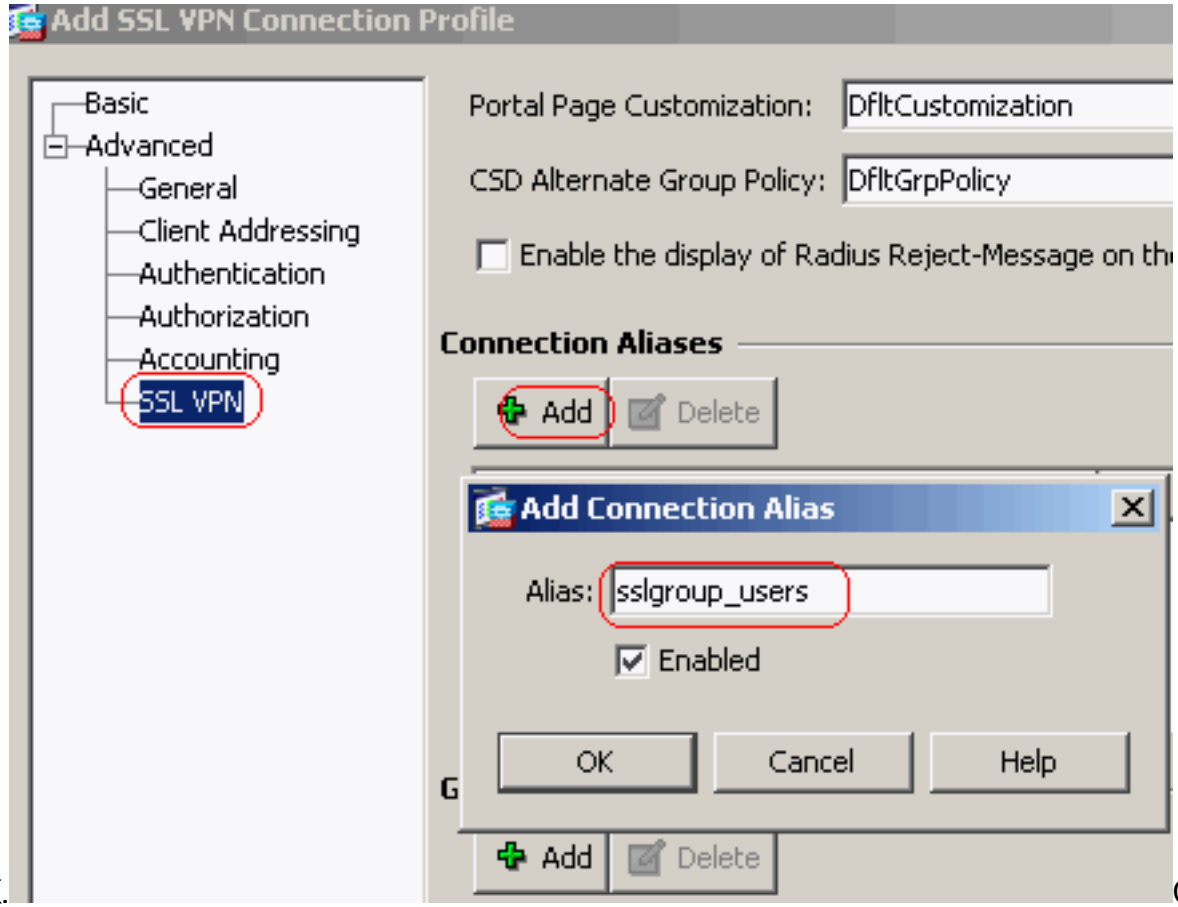
6. Selecione **Configuration > Remote Access VPN > AAA Setup > AAA Servers Groups > Edit** para modificar o grupo de servidores LOCAL padrão ao marcar a caixa de seleção **Enable Local User Lockout** com o valor máximo de tentativas igual a **16**.



7. Clique em **OK** e, em seguida, em **Apply**.**Configuração via CLI Equivalente:**
8. Configure o Grupo de Túneis.Selecione **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles Connection Profiles > Add** para criar um novo grupo de túneis **sslgroup**.Na guia **Basic**, você pode executar a lista de configurações como mostrado:Nomeie o grupo de túneis como **sslgroup**.Sob Client Address Assignment, selecione o pool de endereços **vpnpool** na lista suspensa.Em Default Group Policy, selecione a política de grupo **clientgroup** na lista suspensa.

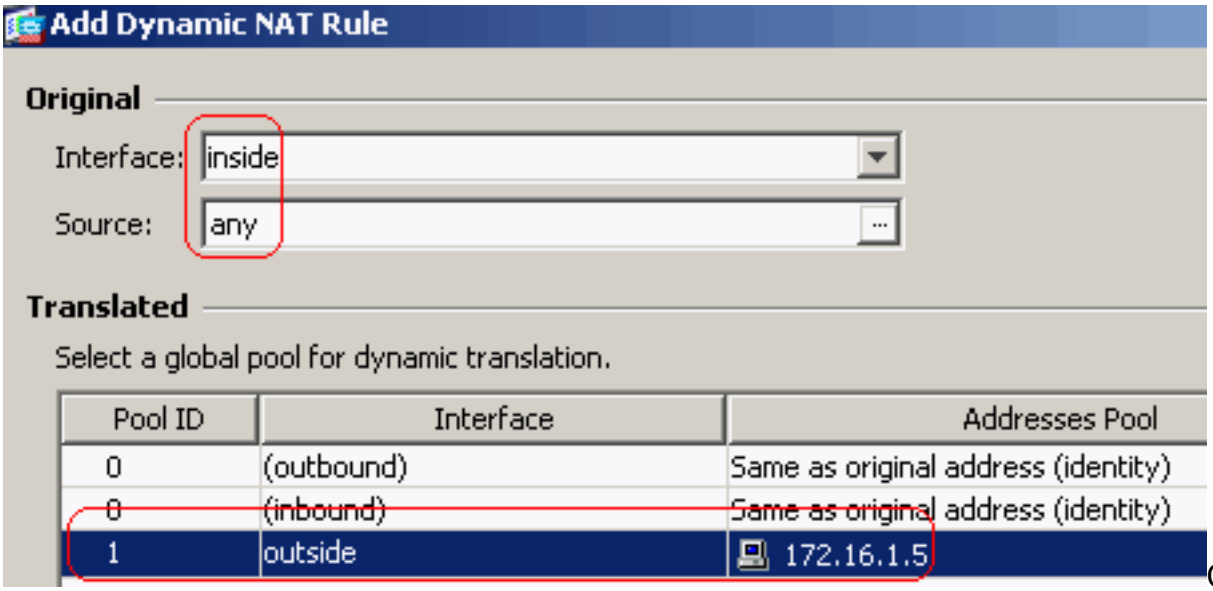


Na guia **SSL VPN > Connection Aliases**, especifique o nome do alias de grupo como **sslgroup_users** e clique em

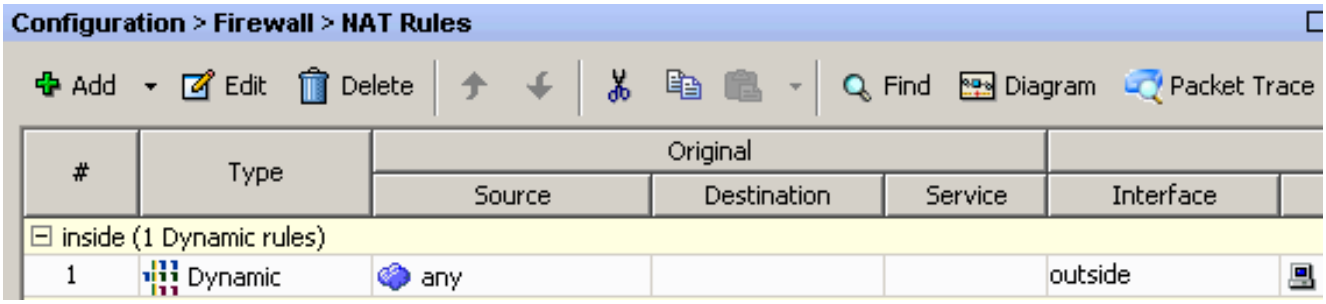


OK. Clique em **OK** e, em seguida, em **Apply**.**Configuração via CLI Equivalente:**

9. Configure o NAT.Selecione **Configuration > Firewall > NAT Rules > Add Dynamic NAT Rule** para que o tráfego proveniente da rede interna possa ser convertido com o endereço IP externo
172.16.1.5.



Clique em **OK**.Clique em
OK.



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

10. Configurar a NAT-isenção para o tráfego de retorno do interior da rede ao 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 via CLI

Cisco ASA 8.0(2)

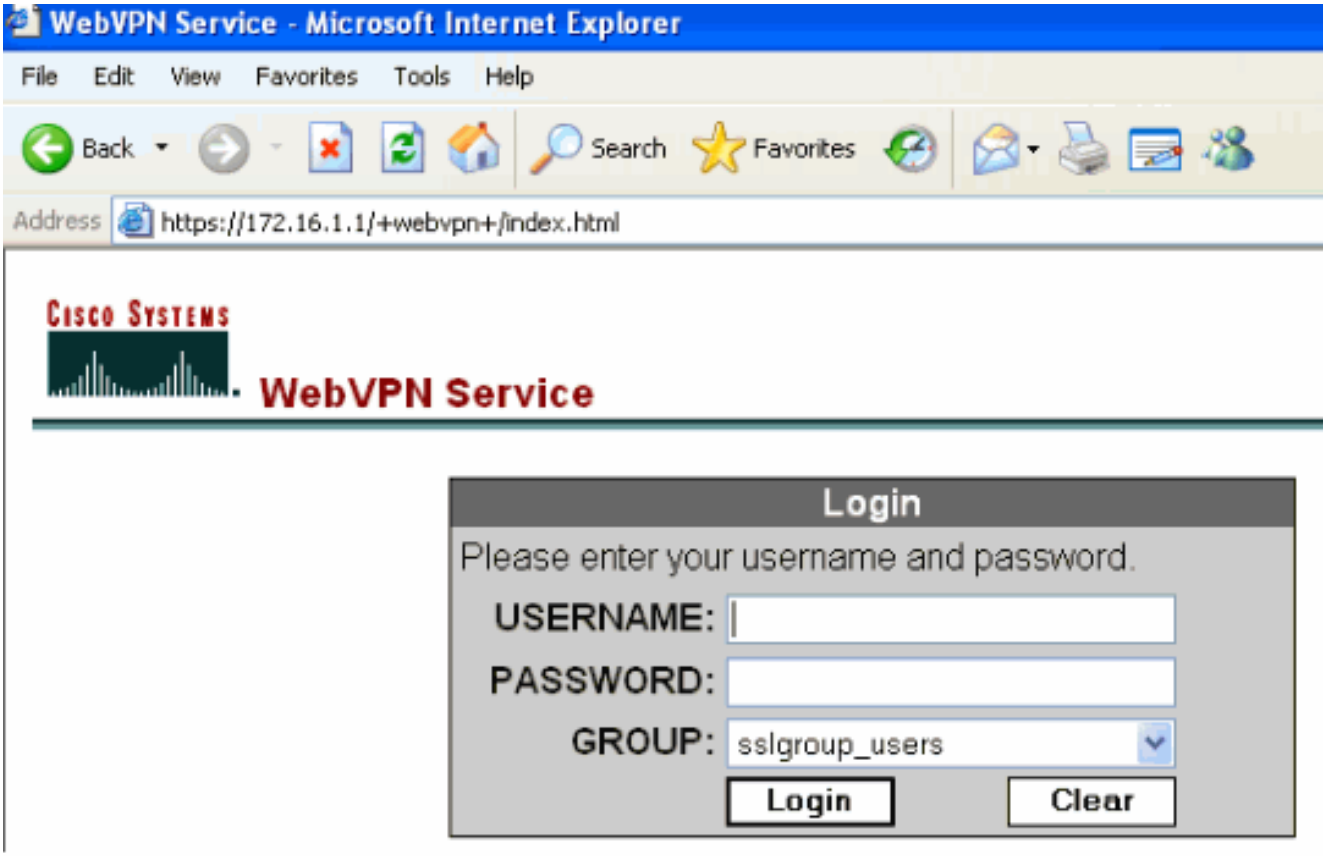
```
ciscoasa(config)#show running-config : Saved : ASA
Version 8.0(2) ! hostname ciscoasa domain-name
default.domain.invalid enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif inside
security-level 100 ip address 10.77.241.142
255.255.255.192 ! interface Ethernet0/1 nameif 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 boot system
disk0:/asa802-k8.bin ftp mode passive clock timezone IST
5 30 dns server-group DefaultDNS domain-name
default.domain.invalid 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
logging enable logging asdm informational mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The
address pool for the Cisco AnyConnect SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-602.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 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 0:05:00 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 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 no crypto isakmp nat-traversal telnet
```

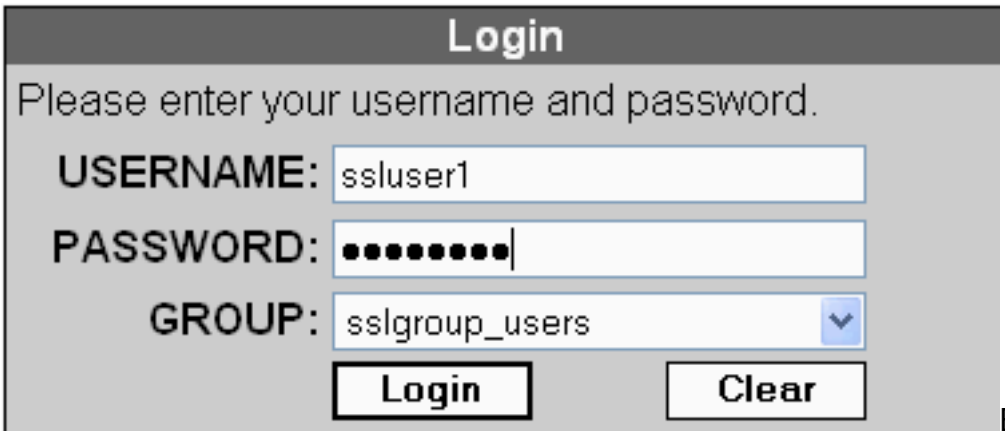
```
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
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 webvpn enable outside !---
Enable WebVPN on the outside interface svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1 !--- Assign an
order to the AnyConnect SSL VPN Client 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 group-policy clientgroup internal !---
Create an internal group policy "clientgroup" group-
policy clientgroup attributes vpn-tunnel-protocol svc !-
-- Specify SSL as a permitted VPN 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 keep-
installer installed !--- When the security appliance and
the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing 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. svc ask none default svc
username ssluser1 password ZRhW85jZqEaVd5P. encrypted !-
-- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access !--- Create a tunnel group
"sslgroup" with type as remote access 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 prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#
```

Estabeleça a conexão VPN SSL com o SVC

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

1. Insira 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>`



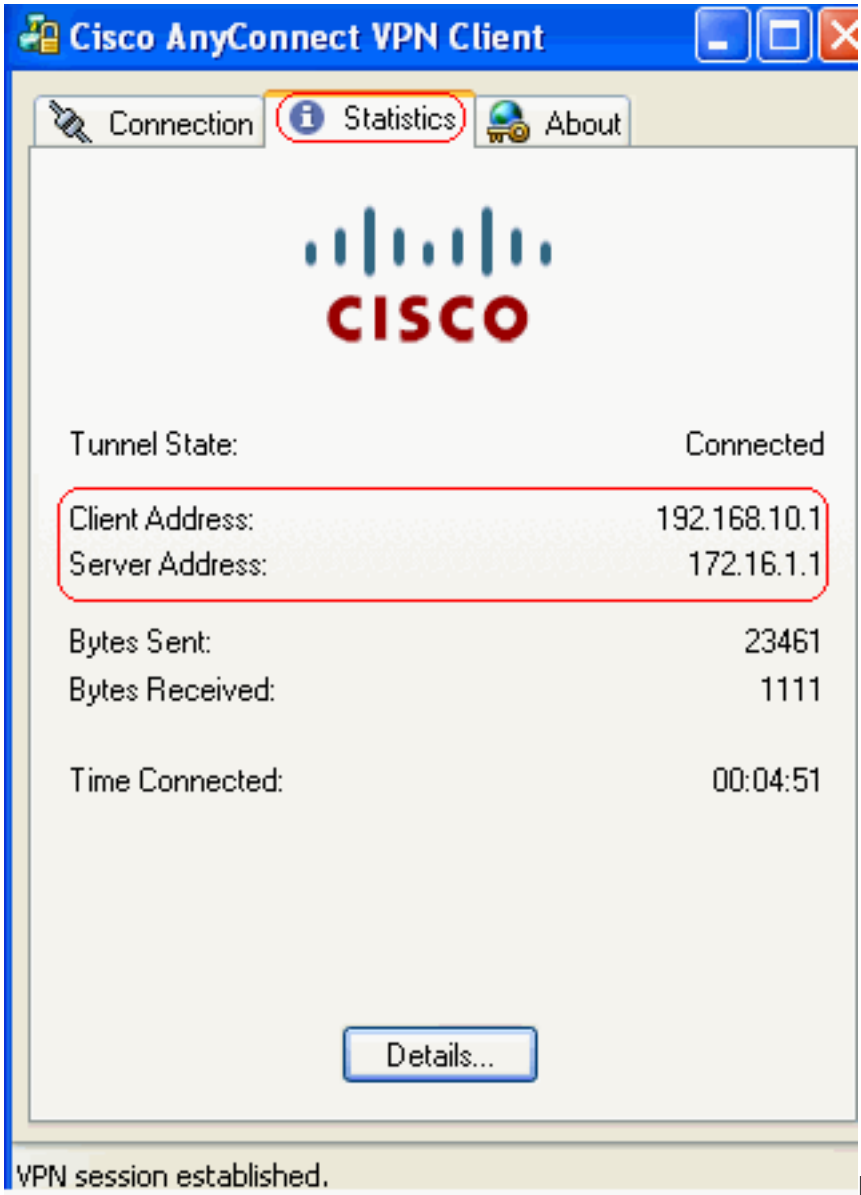
2. Insira seu nome de usuário e senha. Escolha também seu grupo respectivo na lista suspensa conforme mostrado. 

Esta janela é mostrada antes da conexão VPN SSL ser estabelecida.

ota: O software ActiveX deve ser instalado em seu computador antes do SVC ser baixado.Esta janela é mostrada assim que a conexão é estabelecida.

3. Clique no cadeado mostrado na barra de tarefas de seu

computador. Esta janela é mostrada e fornece informações sobre a conexão SSL. Por exemplo, **192.168.10.1** é o IP



atribuído pelo ASA, etc. Esta janela mostra as informações de versão do Cisco AnyConnect VPN

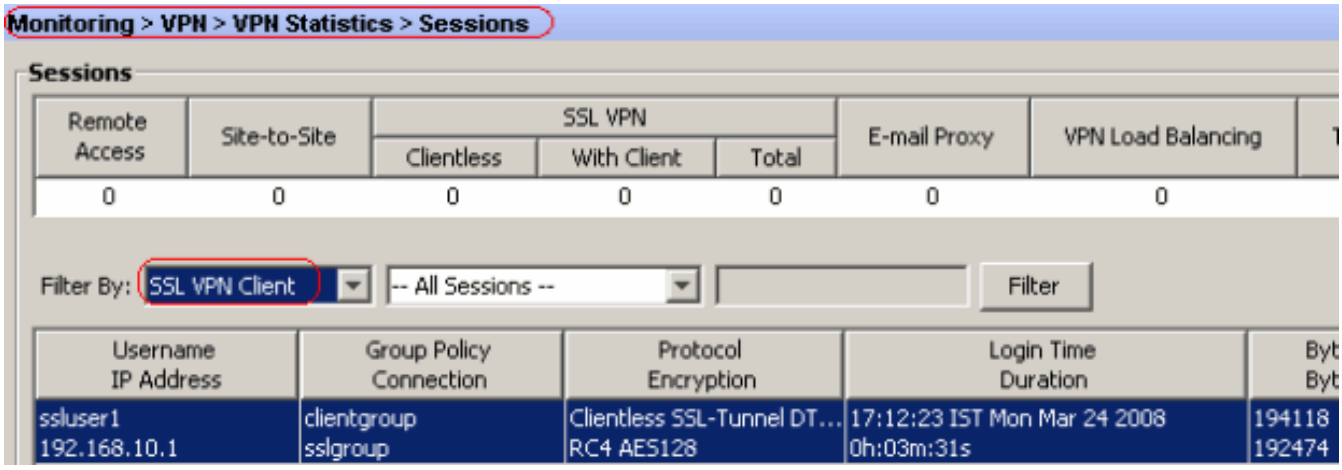
Client.

Verificar

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

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.

- **show webvpn svc** — Mostra as imagens do SVC armazenadas na memória flash do ASA.`ciscoasa#show webvpn svc 1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1 CISCO STC win2k+ 2,0,0343 Mon 04/23/2007 4:16:34.63 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 : 12 Assigned IP : 192.168.10.1 Public IP : 192.168.1.1 Protocol : Clientless SSL-Tunnel DTLS-Tunnel Encryption : RC4 AES128 Hashing : SHA1 Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : clientgroup Tunnel Group : sslgroup Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none`
- **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, selecione **Monitoring > VPN > VPN Statistics > Sessions** para saber quais são as sessões de WebVPN no ASA.



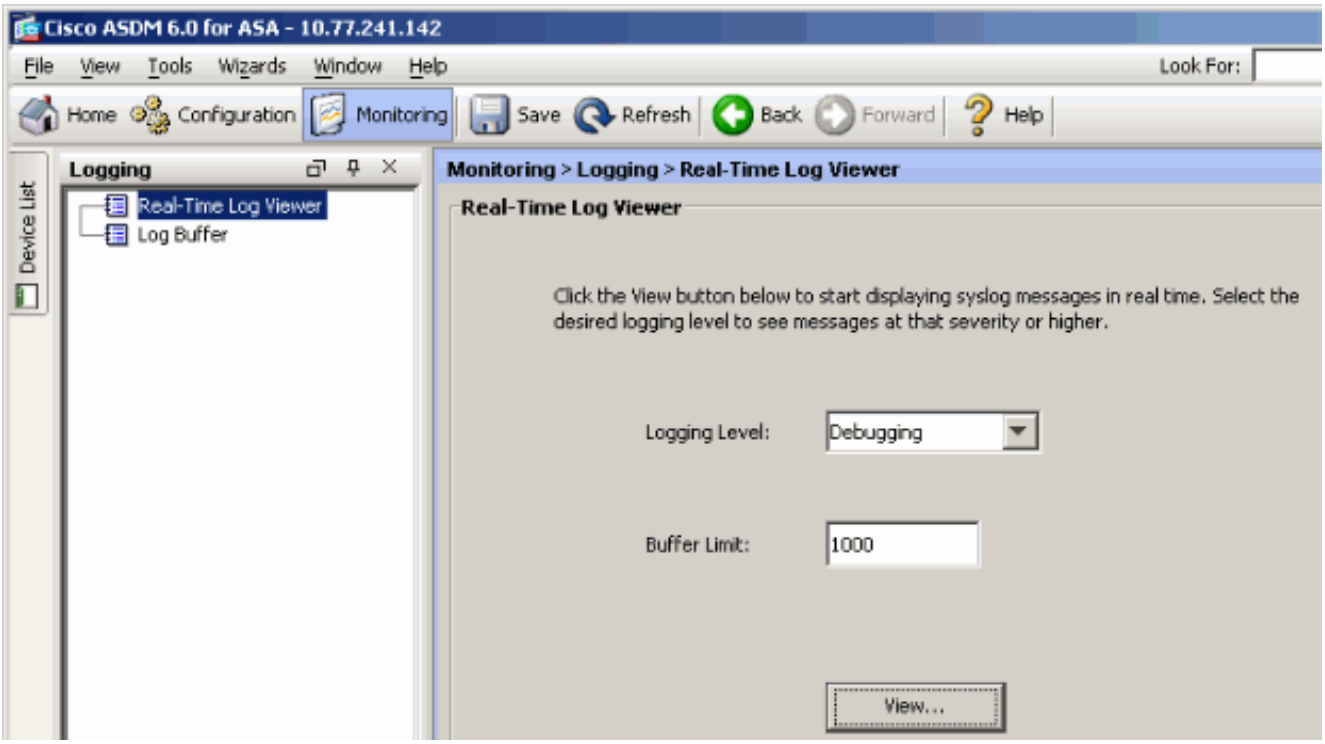
Troubleshooting

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

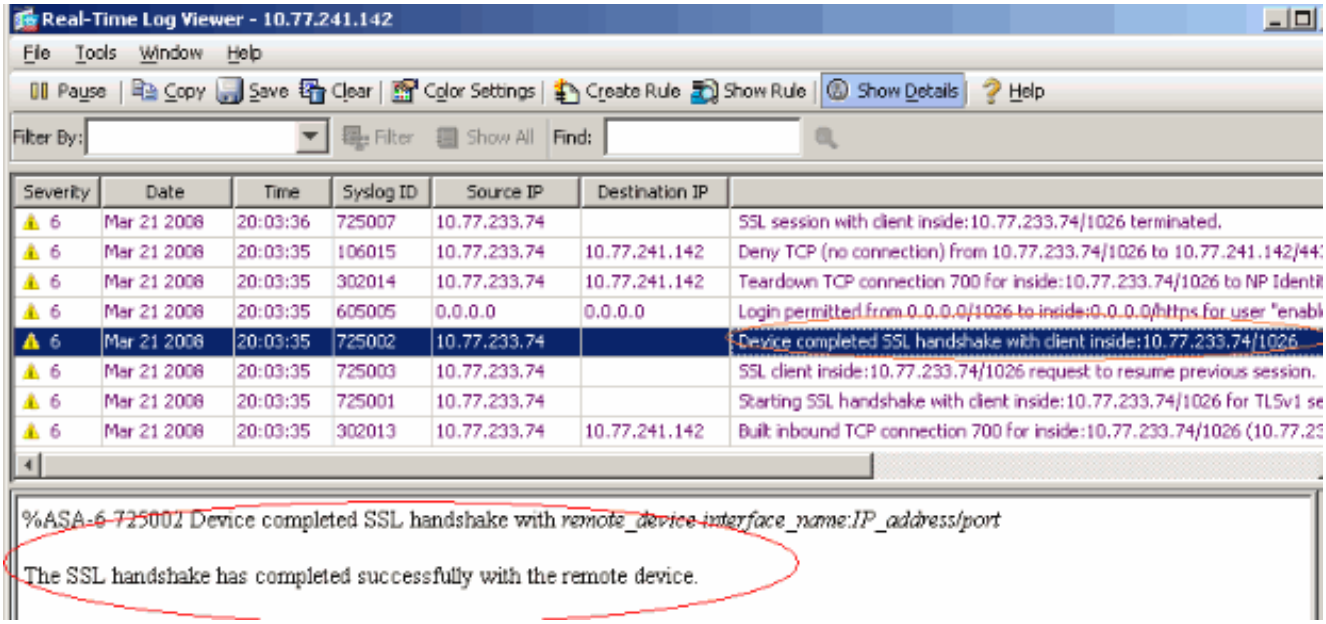
1. **vpn-sessiondb logoff name *<username>*** — Comando para desconectar a sessão VPN SSL para o nome de usuário específico.`ciscoasa#`**`vpn-sessiondb logoff name ssluser1`** `Do you want to logoff the VPN session(s)? [confirm]` **`Y INFO: Number of sessions with name "ssluser1" logged off : 1`** `ciscoasa#`**`Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL np_svc_destroy_session(0xB000)`** De forma semelhante, você pode utilizar o comando **vpn-sessiondb logoff svc** para encerrar todas as seções do SVC.
2. **Nota:** Se o PC entrar no 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, e tc) Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL np_svc_destroy_session(0xA000)` `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`** `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 AnyConnect VPN Client 2, 0, 0343' Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343 ' Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B 7D75F4EDEF26' Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8 625B92C1338D631B08B7D75F4EDEF26' Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B 08B7D75F4EDEF26' WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7 5F4EDEF26' 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: 'X-CSTP-MTU: 1206' Processing CSTP header line: 'X-CSTP-MTU: 1206' webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Address-Type: IPv4' Processing CSTP header line: 'X-CSTP-Address-Type: IPv4' webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40 642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693' Processing CSTP header line: 'X-DTLS-`

```
Master-Secret: CE151BA2107437EDE5EC4F5EE6AE
BAC12031550B1812D40642E22C6AFCB9501758FF3B7B5545973C06F6393C92E59693'
webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-
CBC3-SHA:DES-CBC-SHA' Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-
SHA:DES-CBC3 -SHA:DES-CBC-SHA' 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 np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessmgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTP state = CONNECTED
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy
```

4. No ASDM, selecione **Monitoring > Logging > Real-time Log Viewer > View** para ver os eventos em tempo
real.



Este exemplo mostra que a sessão de SSL foi estabelecida com o dispositivo de head end.



Informações Relacionadas

- Página de Suporte do Cisco 5500 Series Adaptive Security Appliance
- Release Notess do AnyConnect VPN Client, Release 2.0
- 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