Configurar o tráfego de retorno do AnyConnect VPN Client no ASA 9.X

Contents

Introduction

Este documento descreve como configurar um Cisco Adaptive Security Appliance (ASA) Release 9.X para permitir que ele reverta o tráfego de VPN. Ele abrange este cenário de configuração: Retorne o tráfego de clientes de acesso remoto.

> **Note**: Para evitar uma sobreposição de endereços IP na rede, atribua um pool completamente diferente de endereços IP ao VPN Client (por exemplo, 10.x.x.x , 172.16.x.x e 192.168.x.x). Esse esquema de endereços IP é útil para solucionar problemas da sua rede.

Grampos de cabelo ou curva em U

Esse recurso é útil para o tráfego VPN que entra em uma interface, mas é roteado para fora dessa mesma interface. Por exemplo, se você tiver uma rede VPN hub-and-spoke em que o dispositivo de segurança é o hub e as redes VPN remotas são spokes, para que um spoke se comunique com outro tráfego spoke, ele deve ir para o dispositivo de segurança e sair novamente para o outro spoke.

Digite o **same-security-traffic** para permitir que o tráfego entre e saia da mesma interface.

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

Prerequisites

Requirements

A Cisco recomenda que você atenda a estes requisitos antes de tentar executar esta configuração:

- O ASA Security Appliance do hub precisa executar a versão 9.x.
- Cisco AnyConnect VPN Client 3.x**Note**: Baixe o pacote AnyConnect VPN Client (anyconnect-win*.pkg) no Download de Software da Cisco (somente clientes registrados). Copie o AnyConnect VPN Client para a memória flash do Cisco ASA, que deve ser baixada para os computadores de usuários remotos para estabelecer a conexão VPN SSL com o ASA. Consulte a seção Conexões do AnyConnect VPN 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 9.1(2)
- Cisco AnyConnect SSL VPN Client para Windows versão 3.1.05152
- Um PC que executa um sistema operacional suportado de acordo com as plataformas VPN suportadas, Cisco ASA Series.
- Cisco Adaptive Security Device Manager (ASDM) versão 7.1(6)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

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 esteja configurado para redirecionar **http://** pedidos de **https://**, os usuários devem inserir a URL no formato **https://**

.Depois que a URL é inserida, o navegador se conecta a essa interface e exibe a tela de logon. Se o usuário satisfizer o login e a autenticação e o Security Appliance identificar o usuário como necessitando do cliente, ele fará o download do cliente que corresponde ao sistema operacional do computador remoto. Após o download, o cliente se instala e configura sozinho, estabelece uma conexão SSL segura e permanece ou se desinstala (isso depende 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 com o Transport Layer Security (TLS) e também usa o Datagram Transport Layer Security (DTLS). O DTLS evita problemas de latência e largura de banda associados a algumas conexões SSL e melhora o desempenho de aplicativos em tempo real que são sensíveis a atrasos de pacotes.O AnyConnect Client pode ser obtido do Security Appliance ou pode ser instalado manualmente no PC remoto pelo administrador do sistema. Para obter mais informações sobre como instalar o cliente manualmente, consulte o Guia do Administrador do Cisco AnyConnect Secure Mobility Client.O Security Appliance faz o download do cliente com base na política de 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.***Note**: Os exemplos usados neste documento usam IPv4. Para o tráfego IPv6 de retorno, as etapas são as mesmas, mas usam os endereços IPv6 em vez do IPv4.*

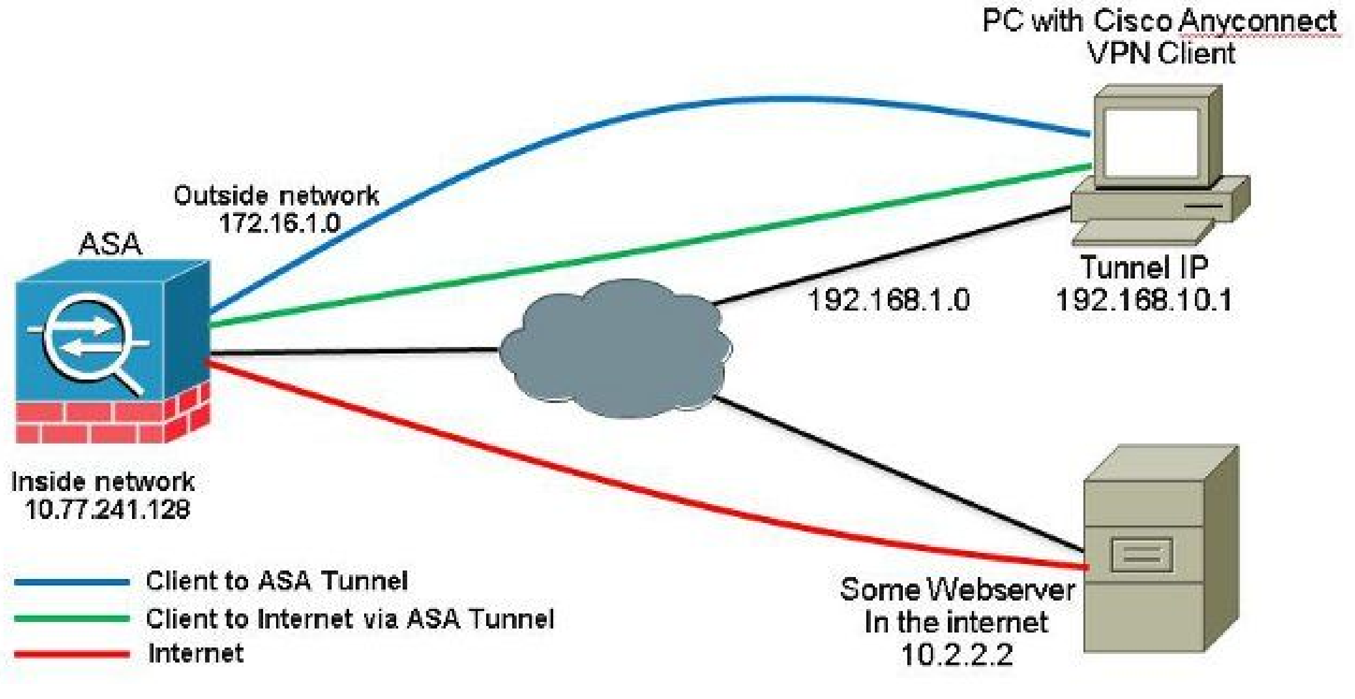
Configurar o tráfego de acesso remoto que gira em U

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.Note: Use os guias Referências de comando para obter mais informações sobre os comandos usados nesta seção.

Exemplo de configuração do AnyConnect VPN Client para VPN de Internet pública em um stick

Diagrama de Rede

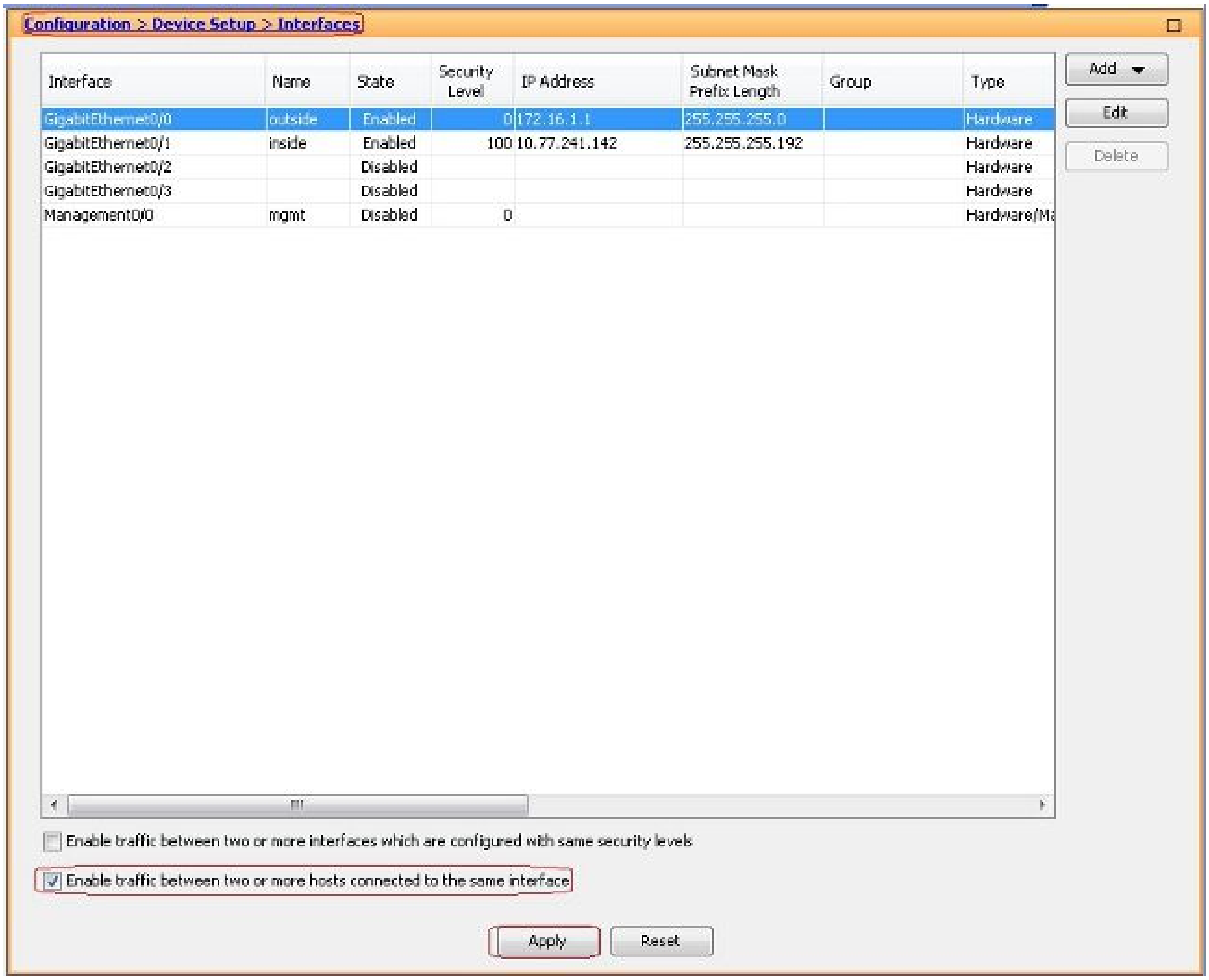
Este documento utiliza a seguinte configuração de rede:


PC with Cisco Anyconnect VPN Client
Outside network 172.16.1.0
ASA
Tunnel IP 192.168.10.1
192.168.1.0
Inside network 10.77.241.128
Client to ASA Tunnel
Client to Internet via ASA Tunnel
Internet
Some Webserver In the internet 10.2.2.2

ASA Versão 9.1(2) Configurações com ASDM Versão 7.1(6)

Este documento pressupõe que a configuração básica, como a configuração de interface, já esteja concluída e funcione corretamente.Note: Consulte Configuração do Acesso de Gerenciamento para permitir que o ASA seja configurado pelo ASDM.Note: Na versão 8.0(2) e posterior, o ASA oferece suporte a sessões VPN SSL (WebVPN) sem cliente e sessões administrativas ASDM simultaneamente na porta 443 da interface externa. Em versões anteriores à Versão 8.0(2), o WebVPN e o ASDM não podem ser ativados na mesma interface 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 estas etapas para configurar a VPN SSL em um cabo no ASA:

1. *Escolher* **Configuration > Device Setup > Interfaces** *e verifique a* **Enable traffic between two or more hosts connected to the same interface** *para permitir que o tráfego VPN SSL entre e saia da mesma interface. Clique em* **Apply***.*



Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	Group	Type
GigabitEthernet0/0	outside	Enabled	0	172.16.1.1	255.255.255.0		Hardware
GigabitEthernet0/1	inside	Enabled	100	10.77.241.142	255.255.255.192		Hardware
GigabitEthernet0/2		Disabled					Hardware
GigabitEthernet0/3		Disabled					Hardware
Management0/0	mgmt	Disabled	0				Hardware/Ma

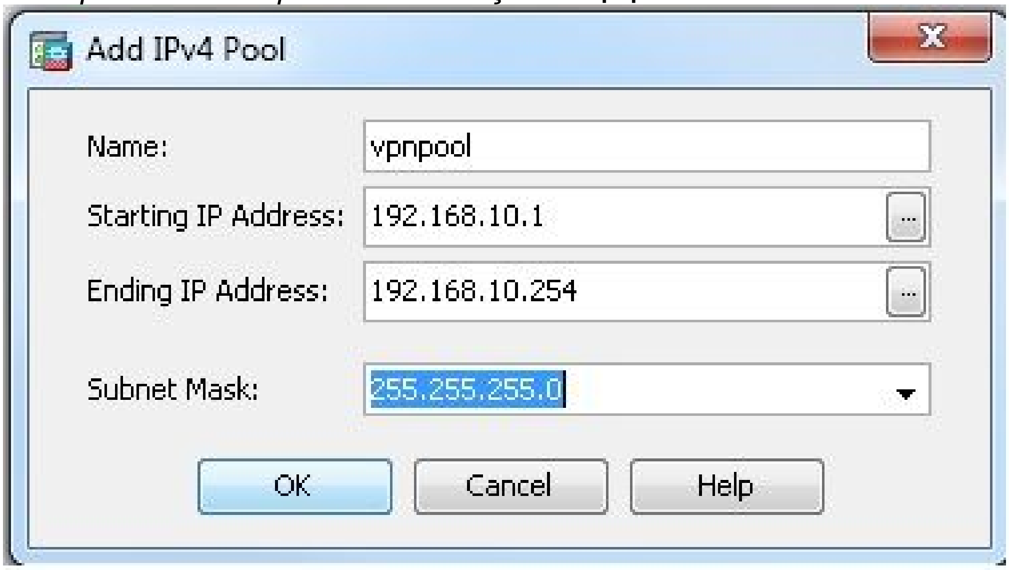
□ Enable traffic between two or more interfaces which are configured with same security levels

☑ Enable traffic between two or more hosts connected to the same interface

Configuração via CLI Equivalente:

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

2. *Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *para criar um pool de endereços IP* **vpnpool**.



Add IPv4 Pool

Name: vpnpool

Starting IP Address: 192.168.10.1

Ending IP Address: 192.168.10.254

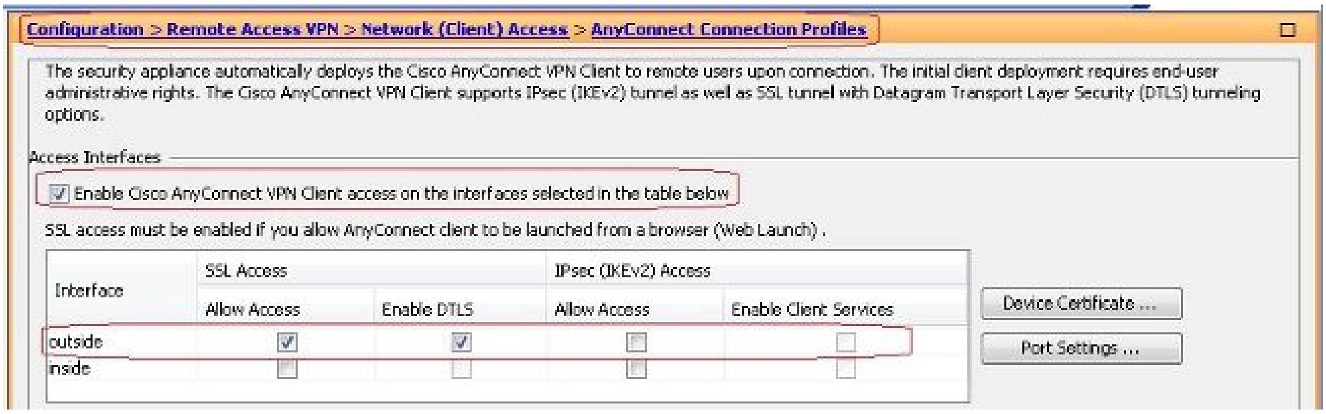
Subnet Mask: 255.255.255.0

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

```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

4. *Ative o WebVPN. Escolher* **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 access on the interfaces selected in the table below** *para habilitar a VPN SSL na interface*

externa.



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

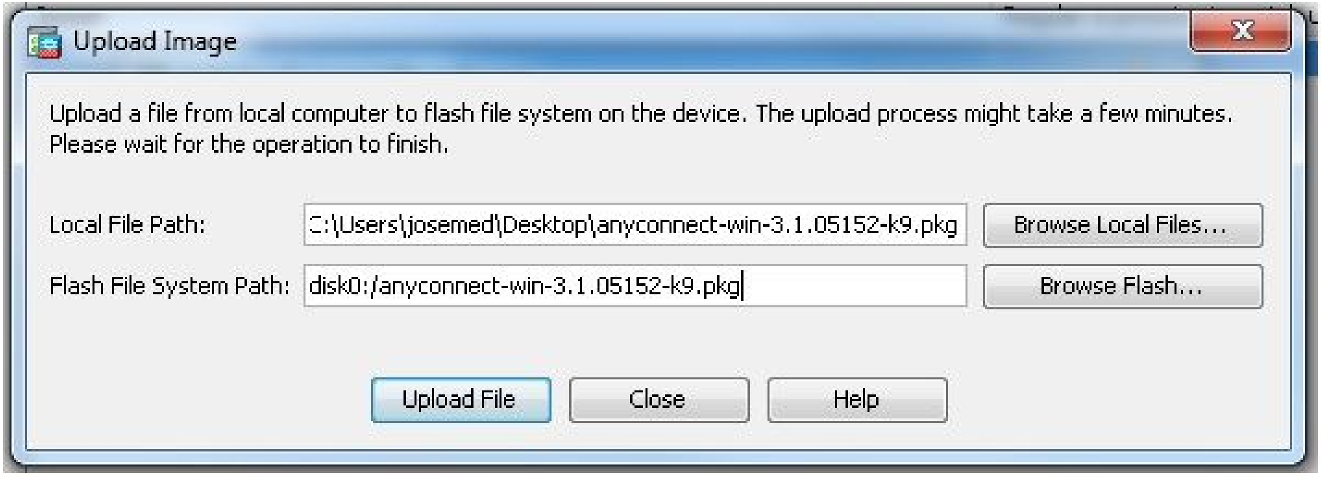
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☐	☐
inside	☐	☐	☐	☐

Clique em **Apply**.*Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *para adicionar a imagem do Cisco AnyConnect VPN Client da memória flash do ASA, conforme mostrado.*

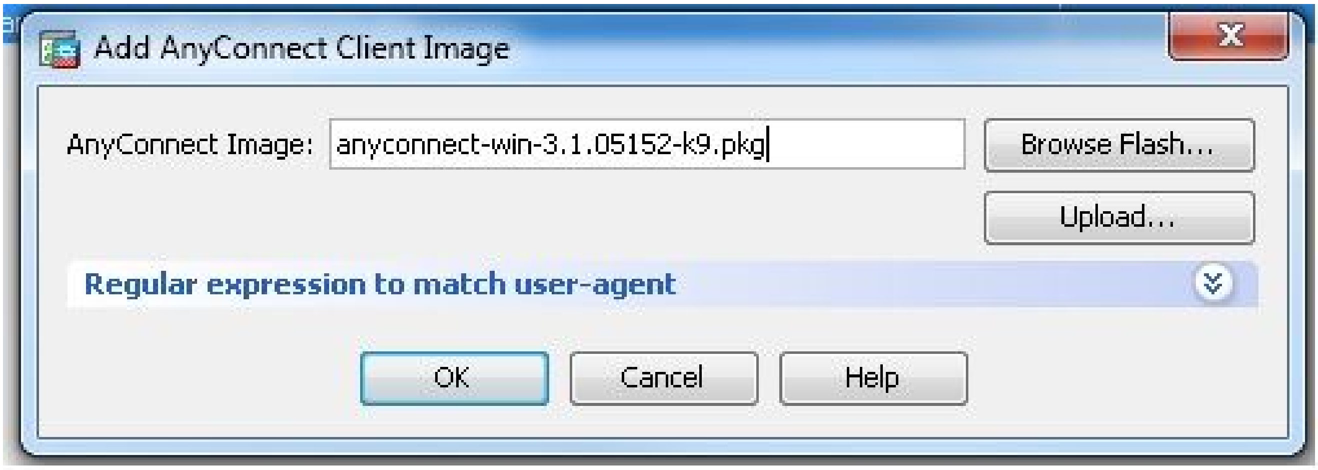


Upload Image

Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Local File Path: C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg

Flash File System Path: disk0:/anyconnect-win-3.1.05152-k9.pkg



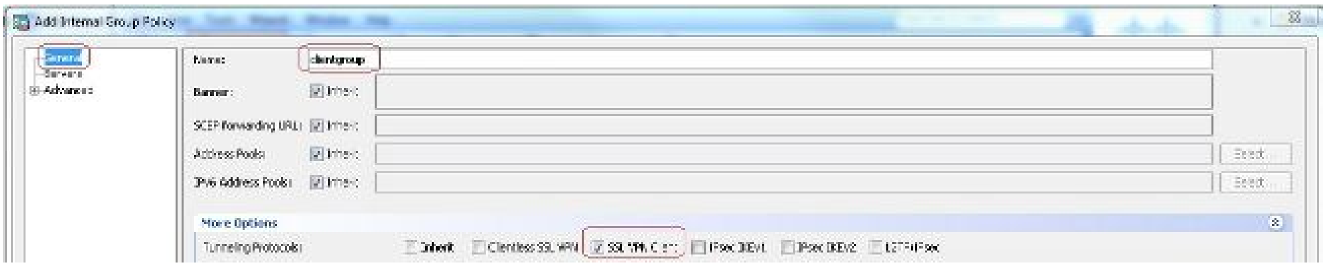
Add AnyConnect Client Image

AnyConnect Image: anyconnect-win-3.1.05152-k9.pkg

Configuração via CLI Equivalente:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

5. *Configure a Política de Grupo. Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *para criar uma política de grupo interna* **clientgroup**. *Sob a* **General** *selecione a guia* **SSL VPN Client** *para habilitar a WebVPN como protocolo de túnel.*



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

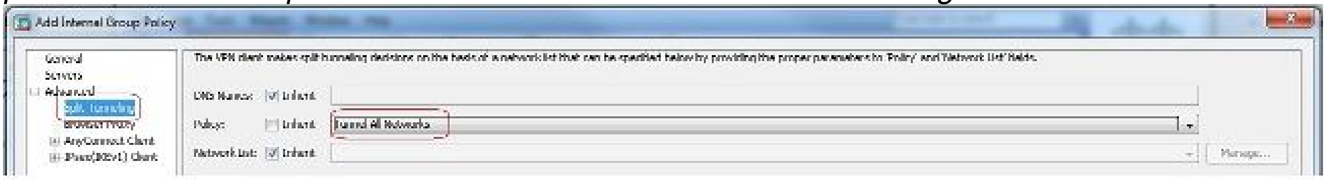
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

No **Advanced > Split Tunneling** *, escolha* **Tunnel All Networks** *na lista suspensa Política da Política para fazer todos os pacotes do PC remoto através de um túnel seguro.*



Add Internal Group Policy

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameters to 'Policy' and 'Network List' fields.

DNS Names: ☑ Inherit

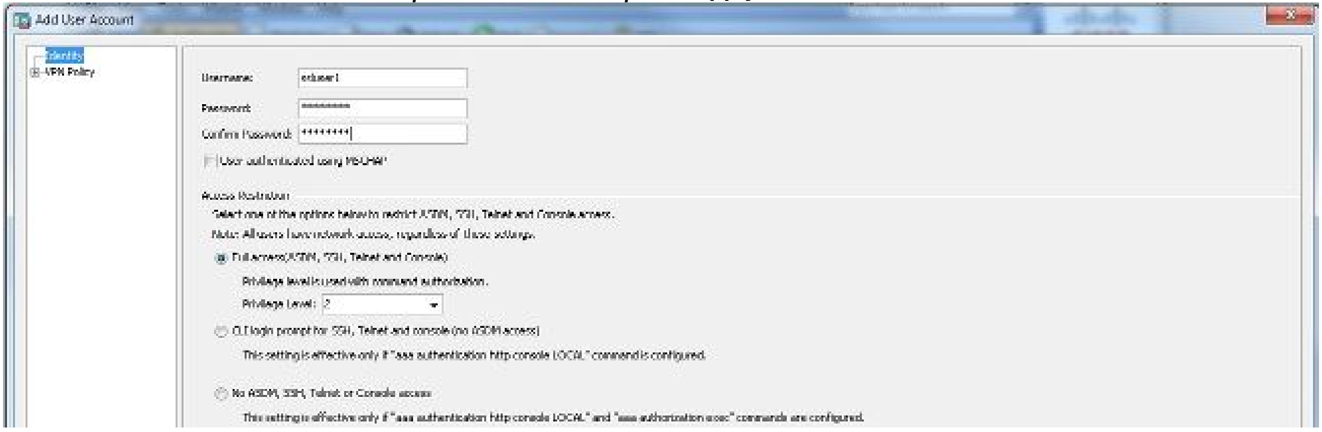
Policy: □ Inherit Tunnel All Networks

Network List: ☑ Inherit

Configuração via CLI Equivalente:

```
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policyclientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelall
```

6. *Escolher* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *para criar uma nova conta de usuário* **ssluser1***. Clique em* **OK** *e depois* **Apply***.*



Add User Account

Username: ssluser1

Password: *********

Confirm Password: ********

□ User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

● Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 2

○ CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

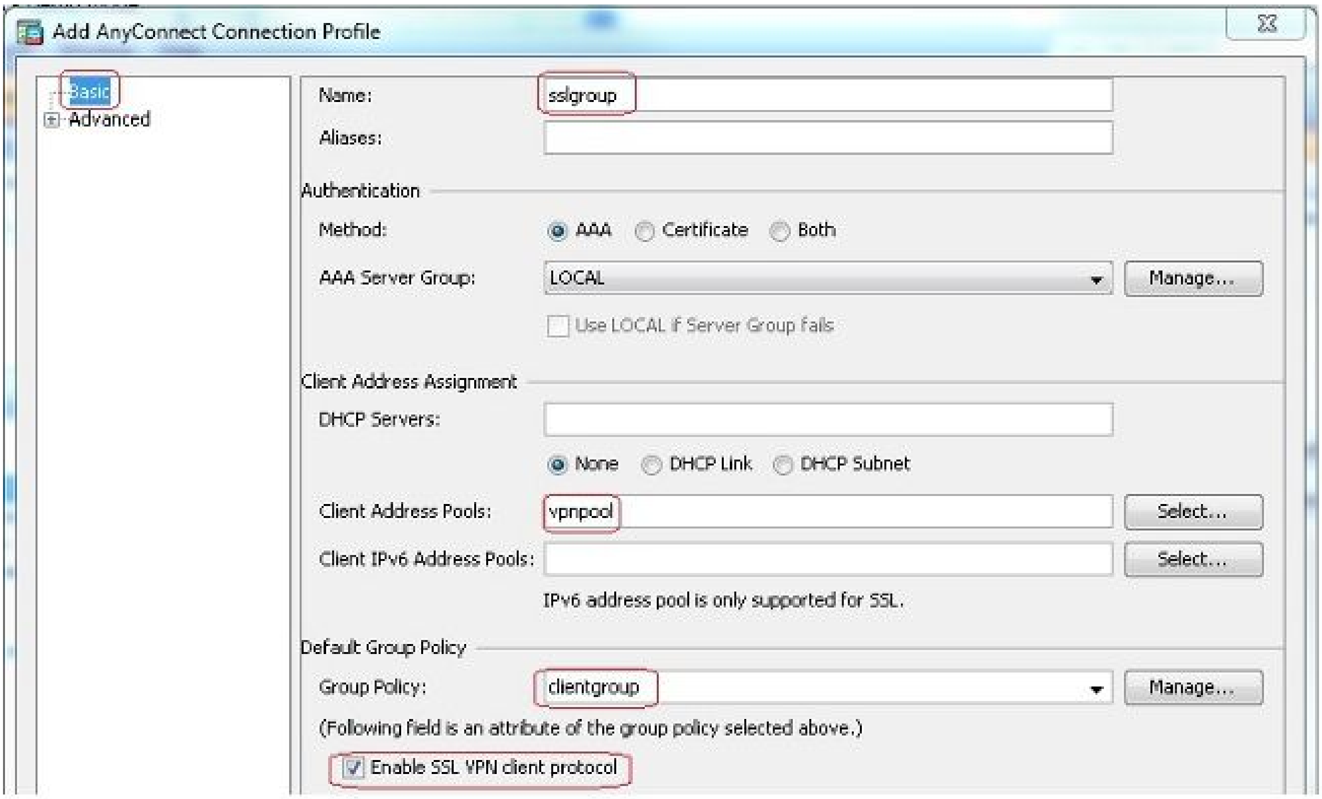
○ No ASDM, SSH, Telnet or Console access

This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

Configuração via CLI Equivalente:

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

7. *Configure o Grupo de Túneis. Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *para criar um novo grupo de túneis* **sslgroup***.No* **Basic** *, você pode executar a lista de configurações como mostrado: Nomear o grupo de túneis como* **sslgroup***.Sob* **Client Address Assignment***, escolha o pool de endereços* **vpnpool** *nos* **Client Address Pools** *lista suspensa.Sob* **Default Group Policy***, escolha a política de grupo* **clientgroup** *nos* **Group Policy** *lista suspensa.*



Name: sslgroup

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: vpnpool

Client IPv6 Address Pools:

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: clientgroup

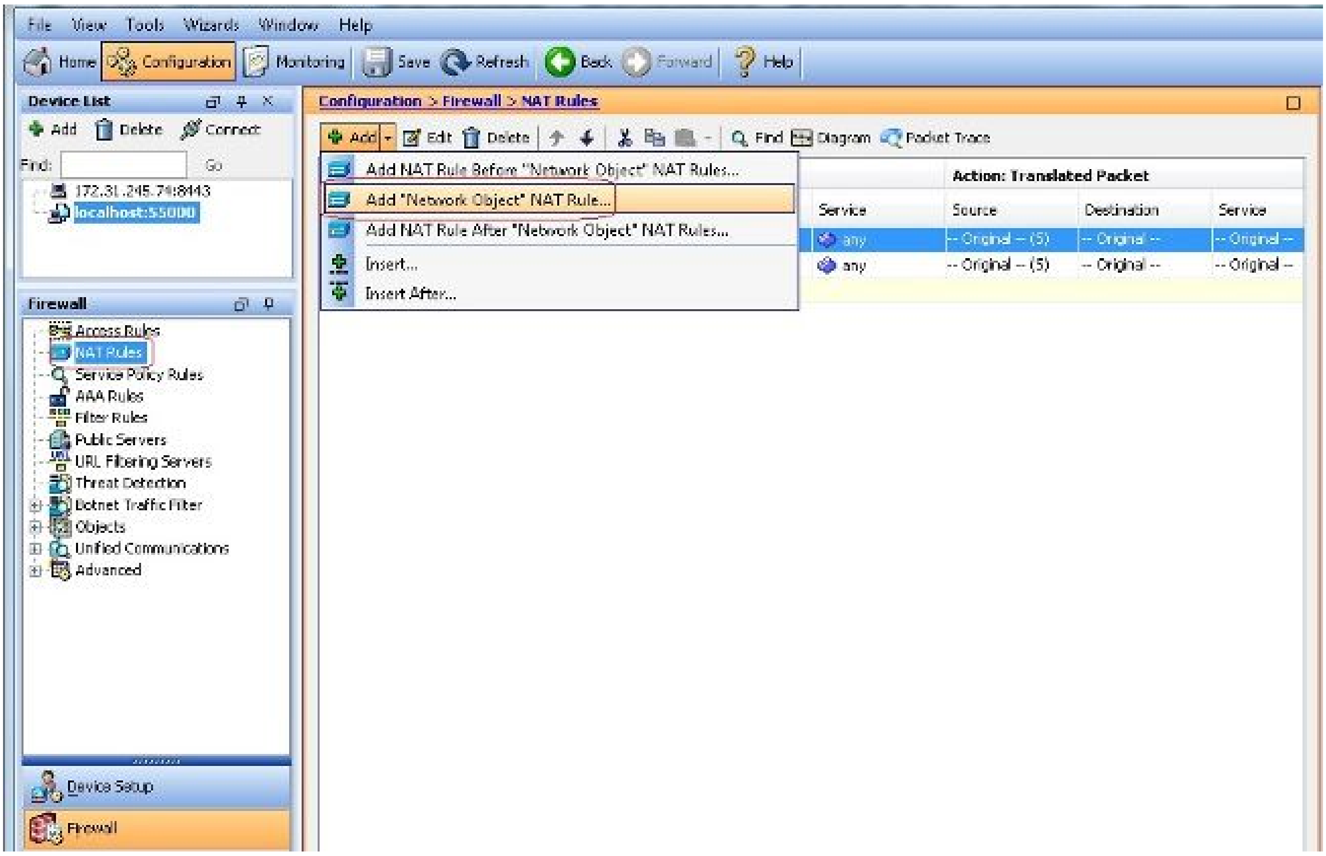
(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

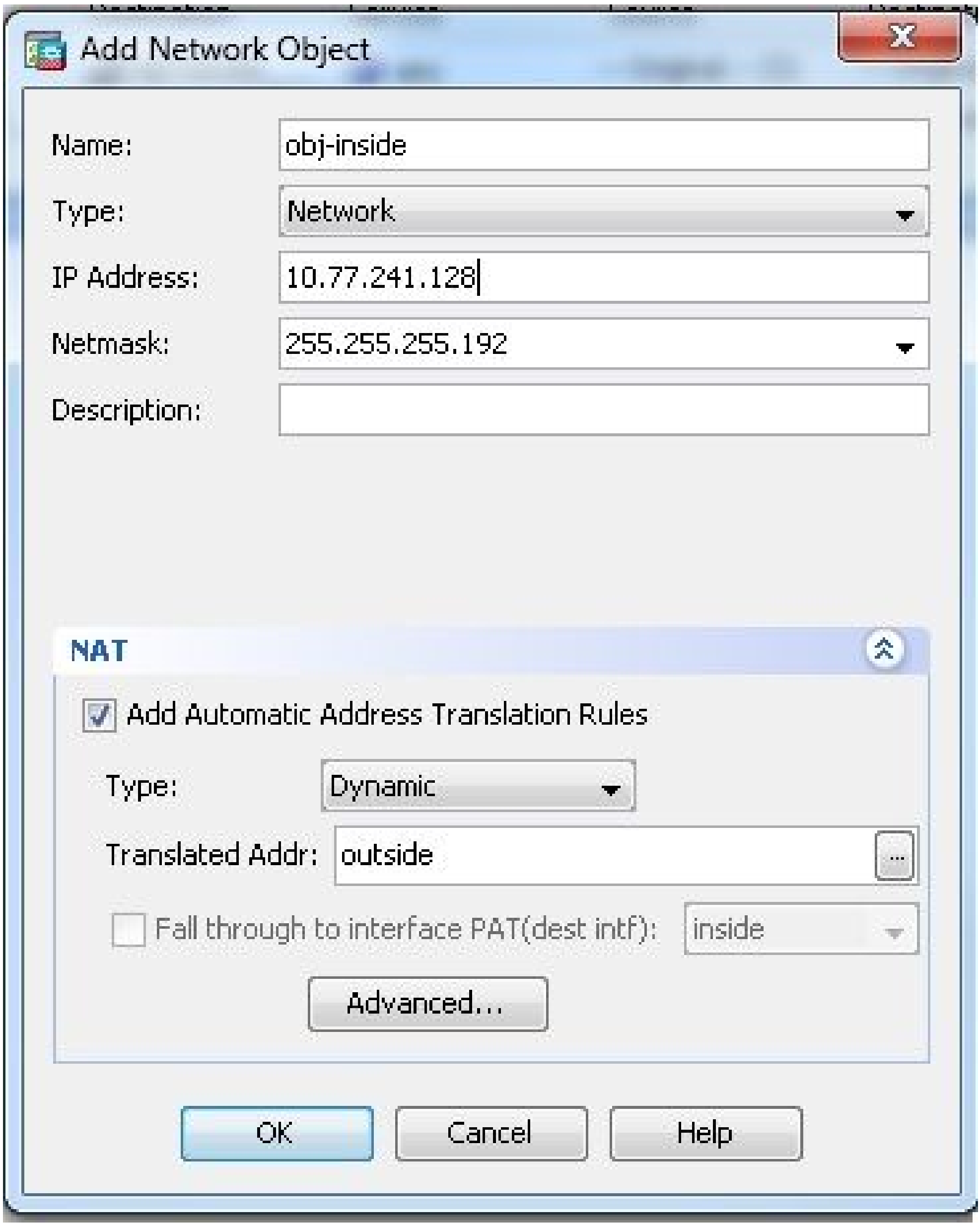
Sob a **Advanced** > **Group Alias/Group URL** *especifique o nome do alias do grupo como* **sslgroup_users** *e clique em* **OK**. ***Configuração via CLI Equivalente:***

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

8. *Configure o NAT Escolher* **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *assim, o tráfego que vem da rede interna pode ser convertido com o endereço IP externo 172.16.1.1.*


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
Find: Go
172.31.245.74:8443
localhost:55000
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Botnet Traffic Filter
Objects
Unified Communications
Advanced
Device Setup
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Add NAT Rule Before "Network Object" NAT Rules...
Add "Network Object" NAT Rule...
Add NAT Rule After "Network Object" NAT Rules...
Insert...
Insert After...

	Action: Translated Packet		
Service	Source	Destination	Service
any	-- Original -- (5)	-- Original --	-- Original --
any	-- Original -- (5)	-- Original --	-- Original --



Add Network Object

Name: obj-inside

Type: Network

IP Address: 10.77.241.128

Netmask: 255.255.255.192

Description:

NAT

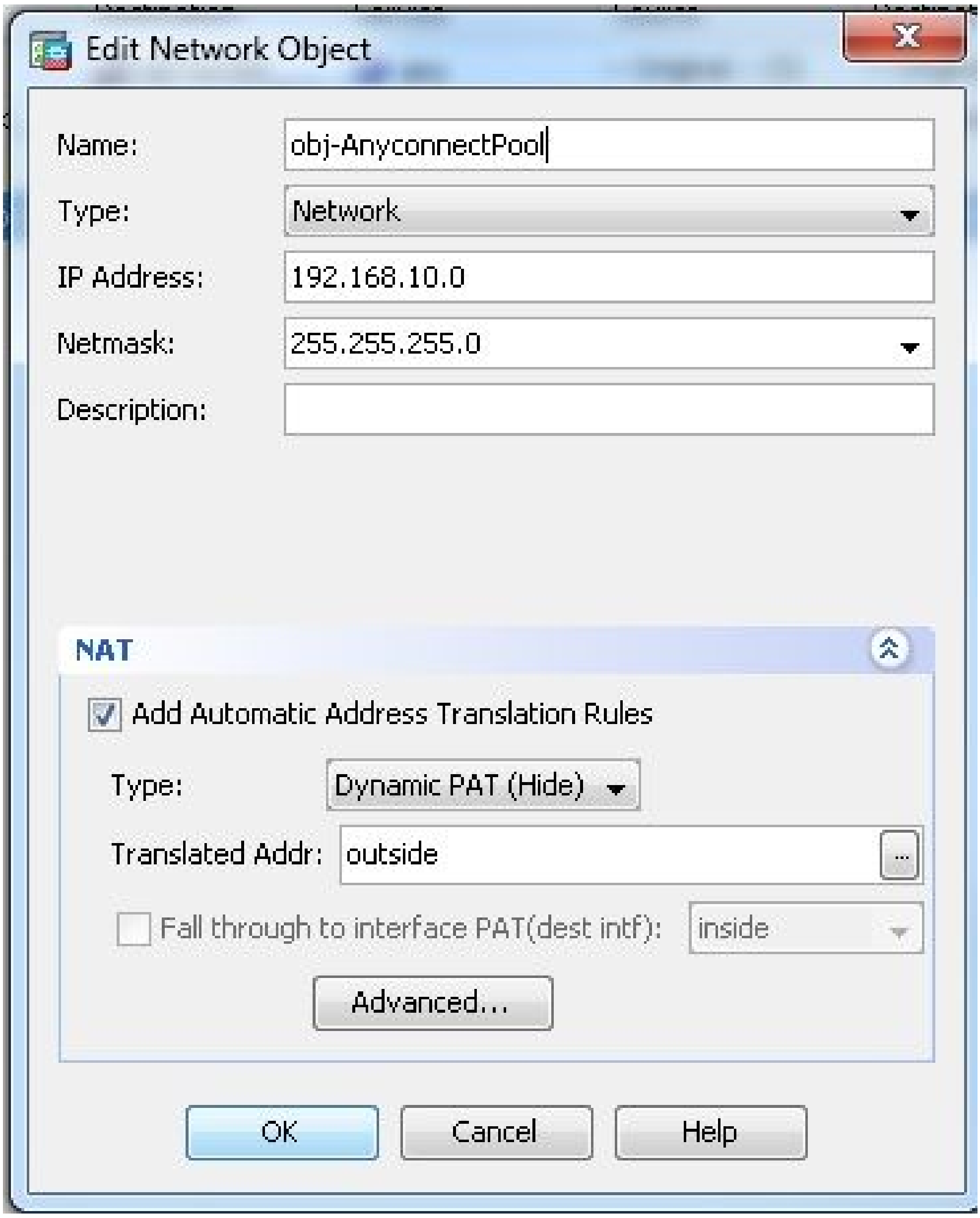
☑ Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: outside

□ Fall through to interface PAT(dest intf): inside

Escolher **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *assim, o tráfego de VPN proveniente da rede externa pode ser convertido com o endereço IP externo 172.16.1.1.*



Name: obj-AnyconnectPool

Type: Network

IP Address: 192.168.10.0

Netmask: 255.255.255.0

Description:

NAT

☑ Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

□ Fall through to interface PAT(dest intf): inside

Configuração via CLI Equivalente:

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

Configuração do ASA versão 9.1(2) na CLI

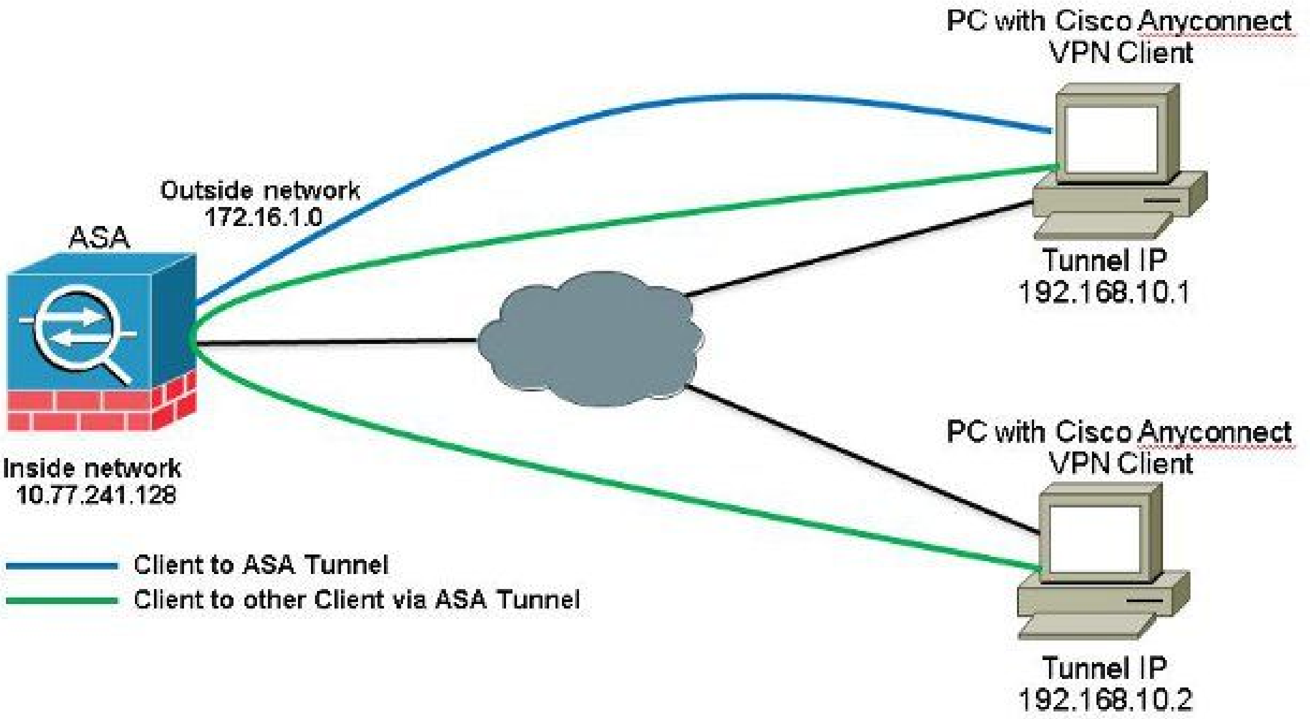
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
```

```
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated
when going to the Anyconnect Pool.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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
```

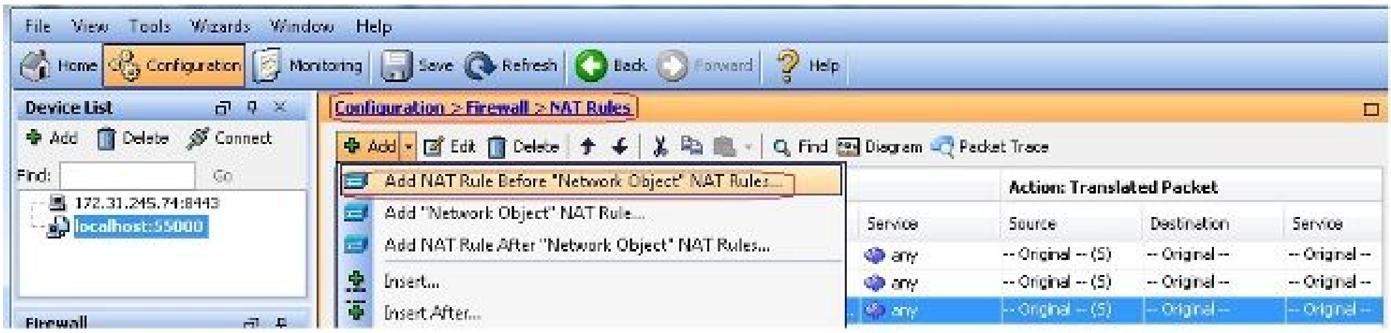
```
group-policy clientgroup internal


!--- Create an internal group policy "clientgroup"


group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

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)#
```

Permitir comunicação entre clientes AnyConnect VPN com a configuração TunnelAll estabelecida

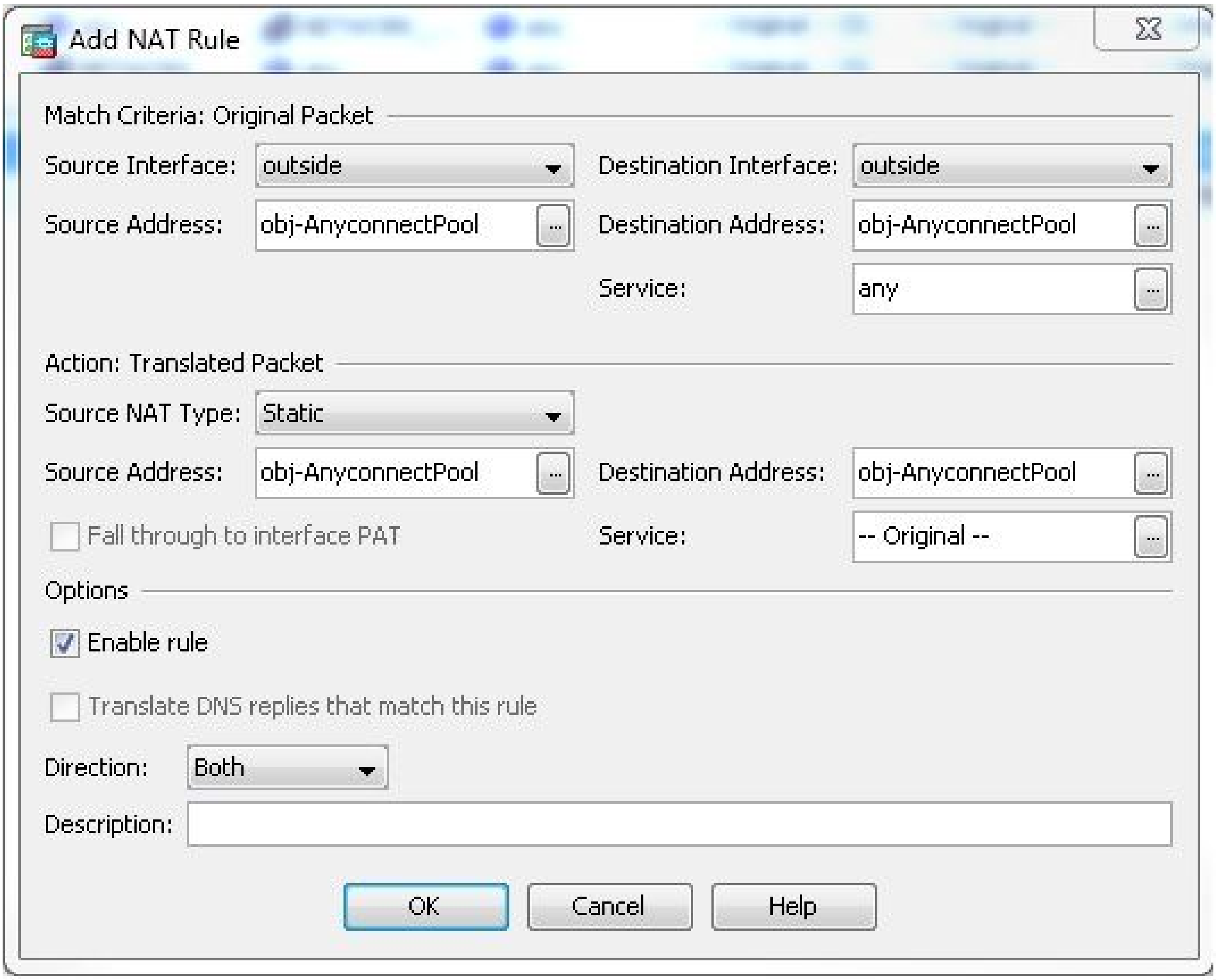
Diagrama de Rede



Se a comunicação entre clientes Anyconnect for necessária e o NAT para Internet Pública em um Stick estiver em vigor; um NAT manual também é necessário para permitir a comunicação bidirecional.Esse é um cenário comum quando os clientes do Anyconnect usam serviços telefônicos e devem ser capazes de ligar uns para os outros.ASA Versão 9.1(2) Configurações com ASDM Versão 7.1(6)Escolher Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules assim, o tráfego que vem da rede externa (Anyconnect Pool) e é destinado a outro Anyconnect Client do mesmo pool não é convertido com o endereço IP externo 172.16.1.1.


File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device List
Add Delete Connect
Find: Go
172.31.245.74:8443
localhost:55000
Firewall
Configuration > Firewall > NAT Rules
Add Edit Delete Find Diagram Packet Trace
Add NAT Rule Before "Network Object" NAT Rules...
Add "Network Object" NAT Rule...
Add NAT Rule After "Network Object" NAT Rules...
Insert...
Insert After...

	Action: Translated Packet		
Service	Source	Destination	Service
any	-- Original -- (S)	-- Original --	-- Original --
any	-- Original -- (S)	-- Original --	-- Original --
any	-- Original -- (S)	-- Original --	-- Original --



Match Criteria: Original Packet

Source Interface: outside

Destination Interface: outside

Source Address: obj-AnyconnectPool

Destination Address: obj-AnyconnectPool

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: obj-AnyconnectPool

Destination Address: obj-AnyconnectPool

□ Fall through to interface PAT

Service: -- Original --

Options

☑ Enable rule

□ Translate DNS replies that match this rule

Direction: Both

Description:

Configuração via CLI Equivalente:

```
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination
static obj-AnyconnectPool obj-AnyconnectPool
```

Configuração do ASA versão 9.1(2) na CLI

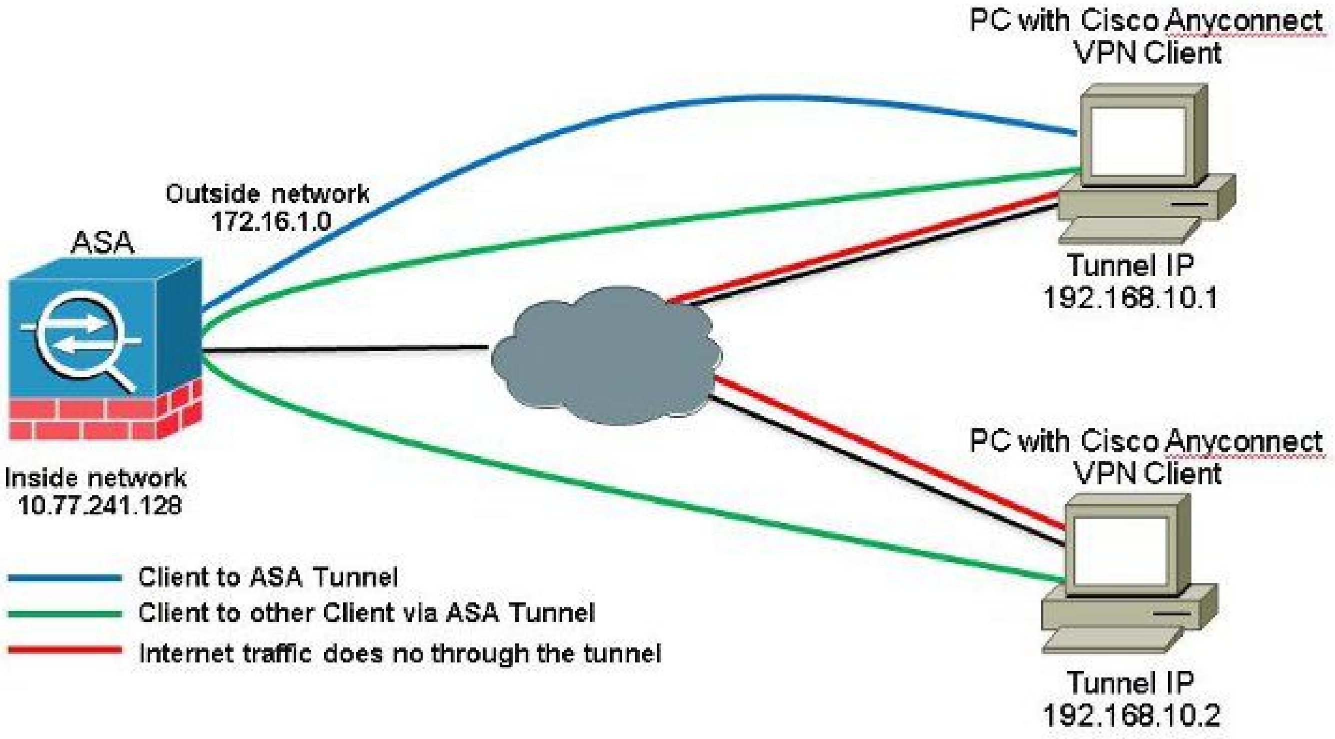
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool
destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network
destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined
to another Client within the same pool does not get translated.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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 ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

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)#
```

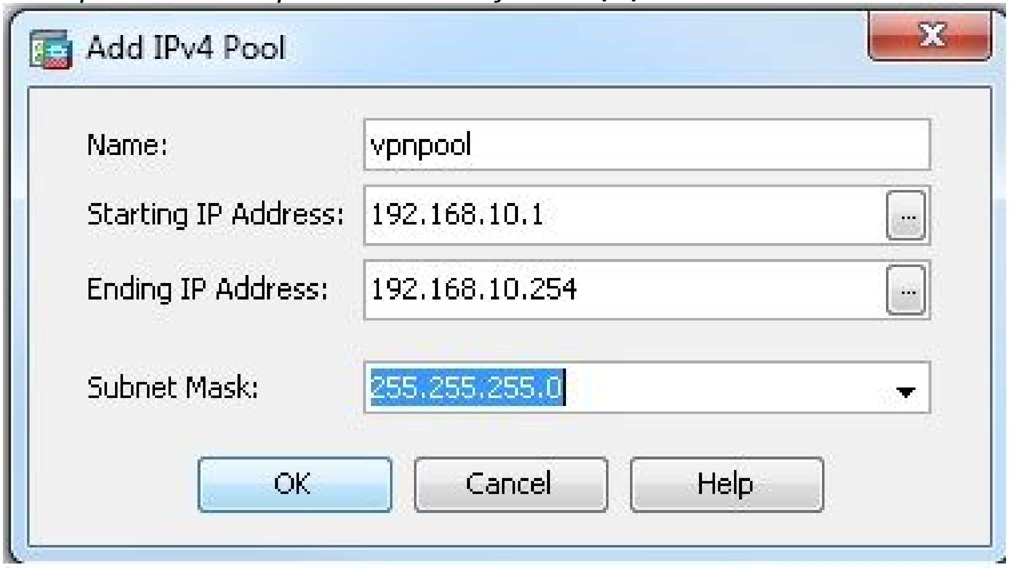
Permitir comunicação entre clientes AnyConnect VPN com Túnel Dividido

Diagrama de Rede


PC with Cisco Anyconnect VPN Client
Outside network 172.16.1.0
ASA
Tunnel IP 192.168.10.1
Inside network 10.77.241.128
PC with Cisco Anyconnect VPN Client
Client to ASA Tunnel
Client to other Client via ASA Tunnel
Internet traffic does no through the tunnel
Tunnel IP 192.168.10.2

Se a comunicação entre clientes Anyconnect for necessária e Split-Tunnel for usado; nenhum NAT manual é necessário para permitir a comunicação bidirecional, a menos que haja uma regra de NAT que afete esse tráfego configurado. No entanto, o Anyconnect VPN Pool deve ser incluído na ACL Split-Tunnel.Esse é um cenário comum quando os clientes do Anyconnect usam serviços telefônicos e devem ser capazes de ligar uns para os outros.ASA Versão 9.1(2) Configurações com ASDM Versão 7.1(6)

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



Add IPv4 Pool

Name: vpnpool

Starting IP Address: 192.168.10.1

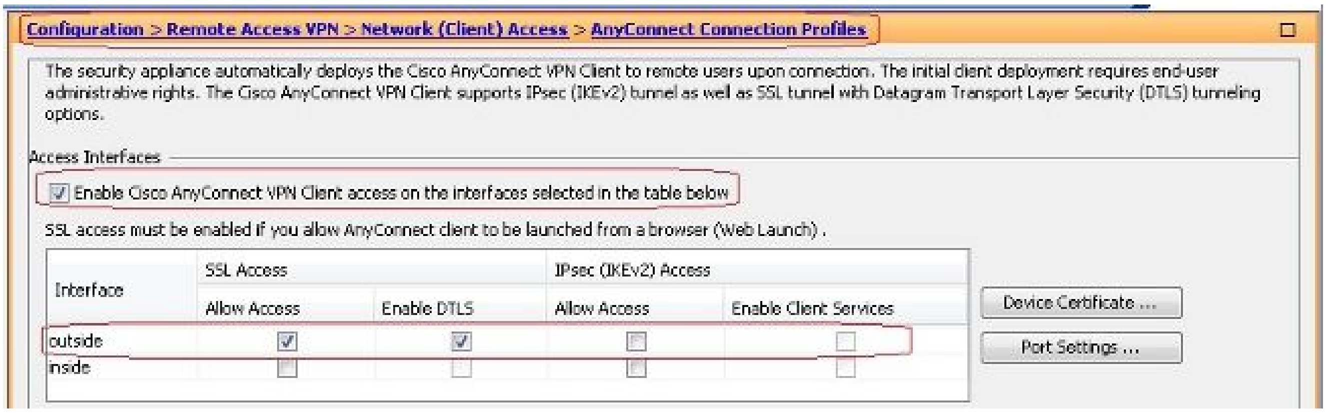
Ending IP Address: 192.168.10.254

Subnet Mask: 255.255.255.0

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

```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

3. *Ative o WebVPN. Escolher* **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 access on the interfaces selected in the table below** *para habilitar a VPN SSL na interface externa.*



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.

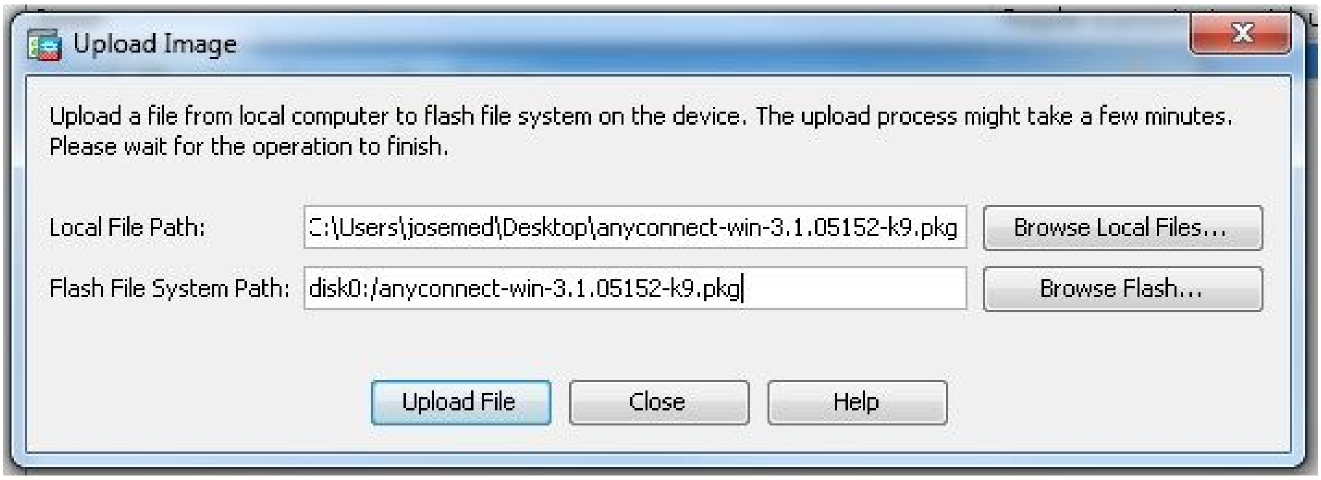
Access Interfaces

☑ Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below

SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch).

Interface	SSL Access		IPsec (IKEv2) Access	
	Allow Access	Enable DTLS	Allow Access	Enable Client Services
outside	☑	☑	☐	☐
inside	☐	☐	☐	☐

Clique em **Apply**.*Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *para adicionar a imagem do Cisco AnyConnect VPN Client da memória flash do ASA, conforme mostrado.*

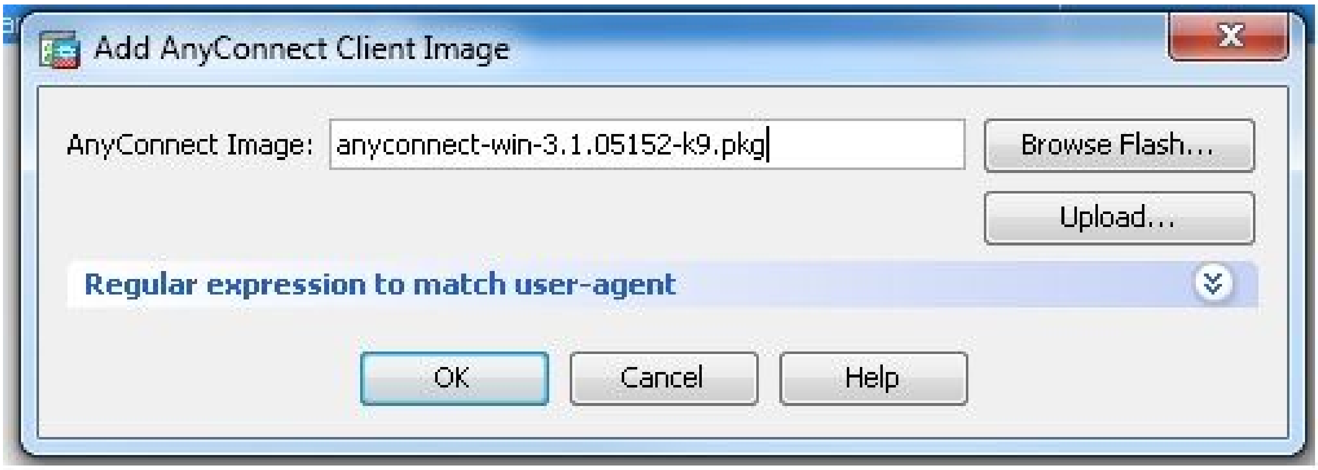


Upload Image

Upload a file from local computer to flash file system on the device. The upload process might take a few minutes. Please wait for the operation to finish.

Local File Path: C:\Users\josemed\Desktop\anyconnect-win-3.1.05152-k9.pkg

Flash File System Path: disk0:/anyconnect-win-3.1.05152-k9.pkg



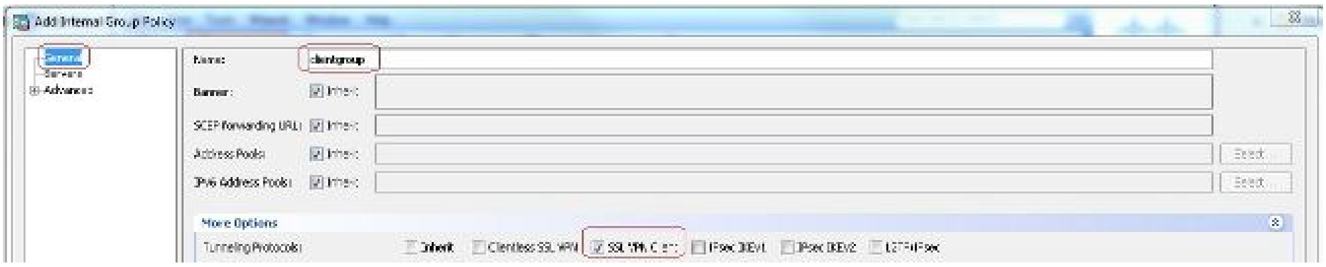
Add AnyConnect Client Image

AnyConnect Image: anyconnect-win-3.1.05152-k9.pkg

Configuração via CLI Equivalente:

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

4. *Configure a Política de Grupo. Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *para criar uma política de grupo interna* **clientgroup**. *Sob a* **General** *selecione a guia* **SSL VPN Client** *para habilitar a WebVPN como um protocolo de túnel permitido.*



Add Internal Group Policy

Name: clientgroup

Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

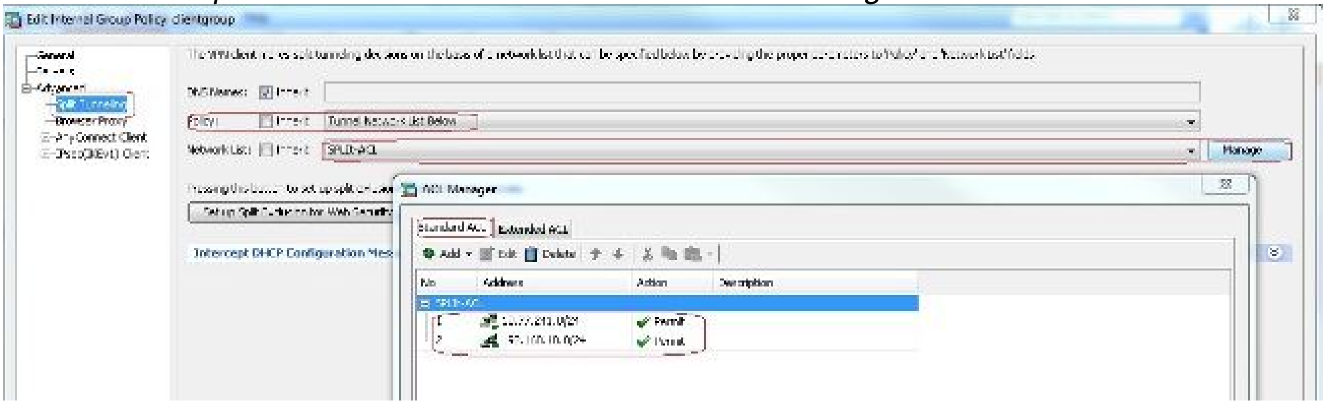
Address Pools: ☑ Inherit

IPv6 Address Pools: ☑ Inherit

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec IKEv1 □ IPsec IKEv2 □ L2TP/IPsec

No **Advanced > Split Tunneling** *, escolha* **Tunnel Network List Below** *na lista suspensa Política para fazer todos os pacotes do PC remoto através de um túnel seguro.*



Edit Internal Group Policy: clientgroup

Policy: □ Inherit Tunnel Network List Below

Network List: □ Inherit SPLIt-ACL

ACL Manager

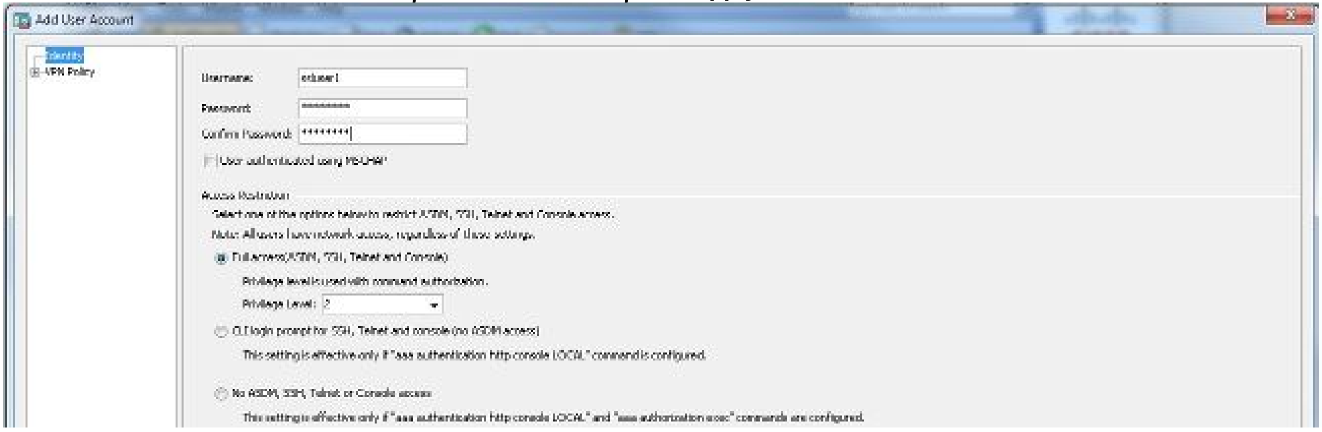
Standard ACL | Extended ACL

No	Address	Action	Description
SPLIt-ACL			
1	10.77.241.0/24	✓ Permit	
2	192.168.10.0/24	✓ Permit	

Configuração via CLI Equivalente:

```
ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policy clientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL
```

5. *Escolher* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *para criar uma nova conta de usuário* **ssluser1***. Clique em* **OK** *e depois* **Apply***.*



Add User Account

Username: ssluser1

Password: *********

Confirm Password: *********

Access Restriction

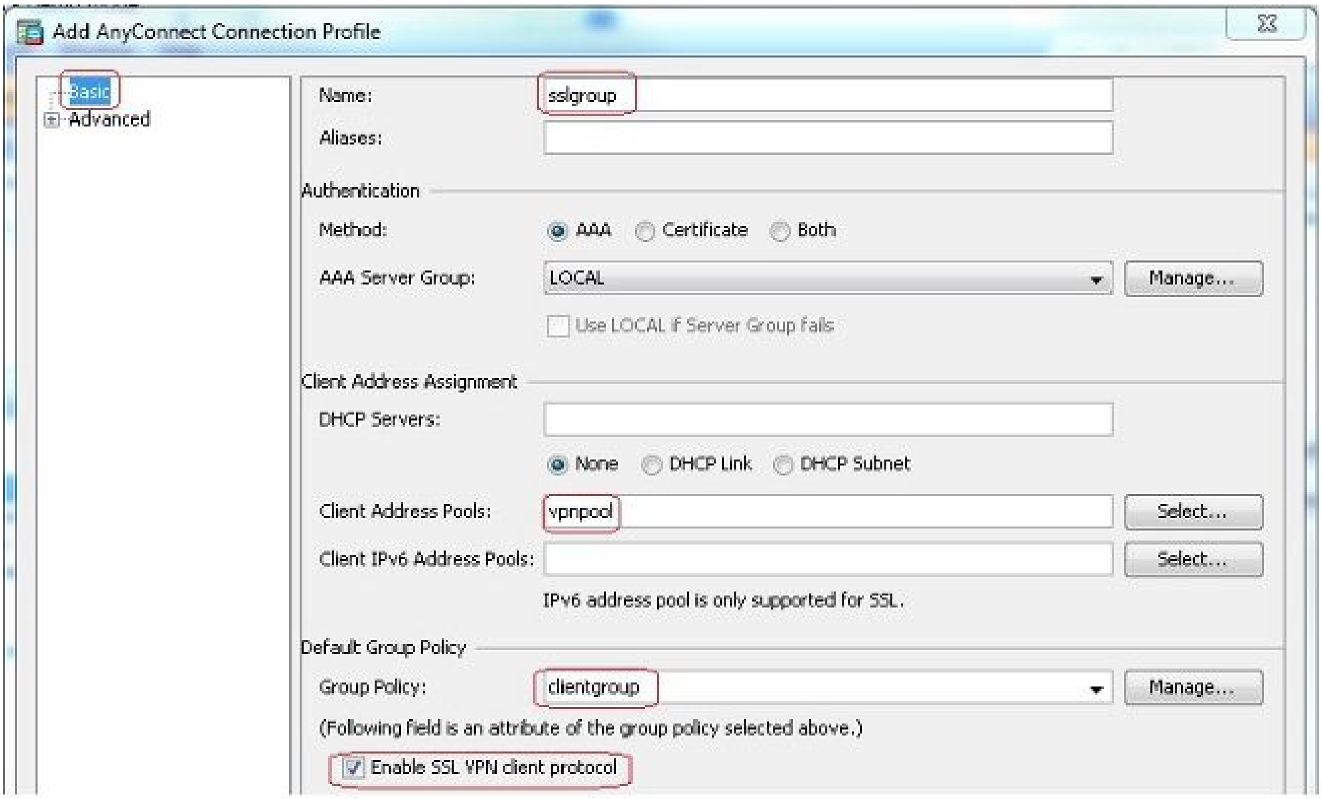
● Full access(ASDM, SSH, Telnet and Console)

Privilege Level: 2

Configuração via CLI Equivalente:

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

6. *Configure o Grupo de Túneis. Escolher* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *para criar um novo grupo de túneis* **sslgroup***.No* **Basic** *, você pode executar a lista de configurações como mostrado: Nomear o grupo de túneis como* **sslgroup***.Sob* **Client Address Assignment***, escolha o pool de endereços* **vpnpool** *nos* **Client Address Pools** *lista suspensa.Sob* **Default Group Policy***, escolha a política de grupo* **clientgroup** *nos* **Group Policy** *lista suspensa.*



Name: sslgroup

Aliases:

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: vpnpool

Client IPv6 Address Pools:

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: clientgroup

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

Sob a **Advanced > Group Alias/Group URL** *especifique o nome do alias do grupo como* **sslgroup_users** *e clique em* **OK**. ***Configuração via CLI Equivalente:***

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

Configuração do ASA versão 9.1(2) na CLI

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

!--- Standard Split-Tunnel ACL that determines the networks that should travel the
Anyconnect tunnel.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when
going to the Anyconnect Pool

object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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 ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol
```

```
split-tunnel-policy tunnelspecified


!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL
VPN Clients.


split-tunnel-network-list value SPLIt-ACL


!--- Defines the previosly configured ACL to the split-tunnel policy.

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)#
```

Verificar

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

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

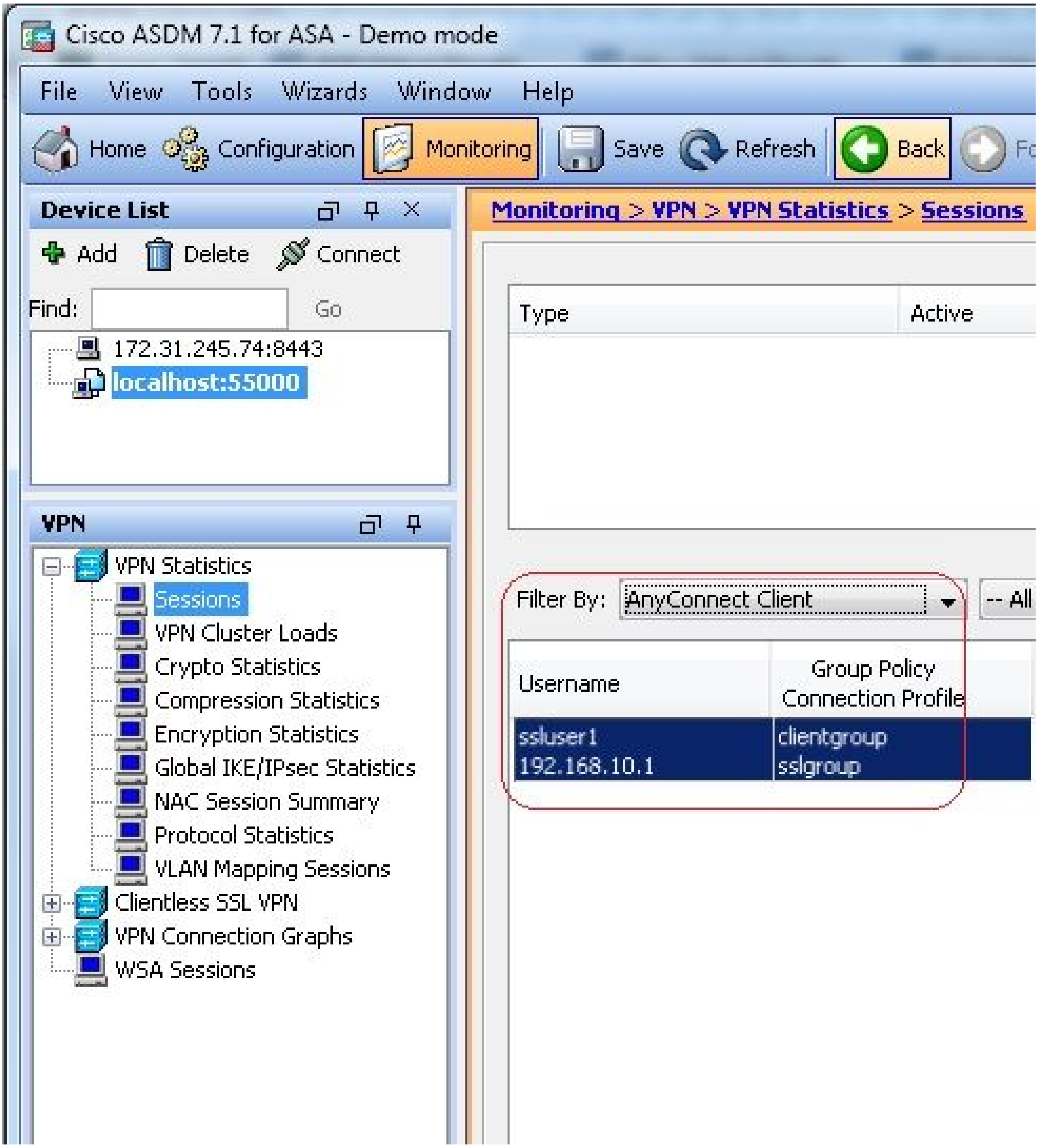
  ```
  ciscoasa#show vpn-sessiondb anyconnect

  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, escolha* **Monitoring > VPN > VPN Statistics > Sessions** *para conhecer as sessões atuais no ASA.*



Type	Active

Filter By: AnyConnect Client -- All

Username	Group Policy Connection Profile
ssluser1 192.168.10.1	clientgroup sslgroup

Troubleshoot

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

- **vpn-sessiondb logoff name** - *Comando para encerrar 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)
```

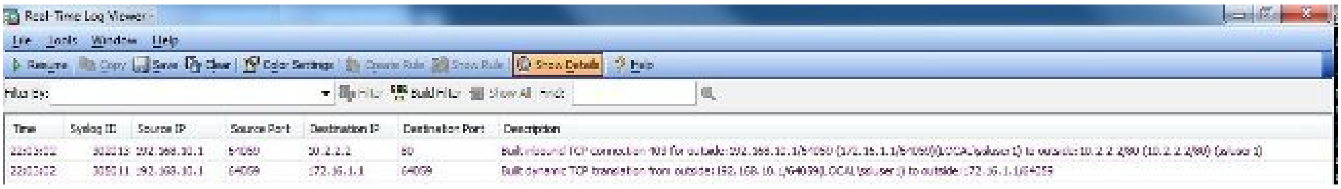
Da mesma forma, você pode usar o comando **vpn-sessiondb logoff anyconnect** *para encerrar todas as sessões do AnyConnect.*

- **debug webvpn anyconnect <1-255>** *- Fornece os eventos webvpn em tempo real para estabelecer a sessão.*

```
Ciscoasa#debug webvpn anyconnect 7

CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
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: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
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'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
```

```
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
No SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260(mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt

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
```

- *No ASDM, escolha* **Monitoring > Logging > Real-time Log Viewer > View** *para ver os eventos em tempo real. Este exemplo mostra as informações de sessão entre o AnyConnect 192.168.10.1 e o Telnet Server 10.2.2.2 na Internet via ASA 172.16.1.1.*



Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port	Description
22:03:02	302013	192.168.10.1	64059	10.2.2.2	80	Built inbound TCP connection 403 for outside:192.168.10.1/64059 (172.16.1.1/64059)(LOCAL\ssluser1) to outside:10.2.2.2/80 (10.2.2.2/80) (ssluser1)
22:03:02	305011	192.168.10.1	64059	172.16.1.1	64059	Built dynamic TCP translation from outside:192.168.10.1/64059(LOCAL\ssluser1) to outside:172.16.1.1/64059

Informações Relacionadas

- *Firewalls Cisco ASA 5500-X Series*
- *Exemplo de Configuração de PIX/ASA e VPN Client para VPN de Internet Pública em um Stick*
- *Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM*
- *Suporte Técnico e Documentação - Cisco Systems*