ASA/PIX: Servidor de VPN remoto com o NAT de entrada para o tráfego do cliente VPN com CLI e exemplo da configuração ASDM

Índice

Introdução

Este documento descreve como configurar o Cisco 5500 Series Adaptive Security Appliance (ASA) para atuar como um servidor de VPN remoto usando o Adaptive Security Device Manager (ASDM) ou CLI e NAT para o tráfego de entrada do cliente VPN. O ASDM oferece gerenciamento de segurança de nível mundial e monitoramento através de uma interface de gerenciamento baseada na Web intuitiva e fácil de usar. Uma vez que a configuração ASA Cisco está completa, pode-se verificar através do Cisco VPN Client.

Pré-requisitos

Requisitos

Este documento supõe que o ASA é plenamente operacional e configurado para permitir que Cisco ASDM ou CLI faça alterações de configuração. O ASA é suposto igualmente para ser configurado para o NAT de partida. Consulte para permitir o acesso dos host internos às redes externas com o uso da PANCADINHA para obter mais informações sobre de como configurar o NAT de partida.

Nota: Refira permitir o acesso HTTPS para ASDM ou PIX/ASA 7.x: SSH no exemplo de configuração da interface interna e externa para permitir que o dispositivo seja configurado remotamente pelo ASDM ou pelo Shell Seguro (ssh).

Componentes Utilizados

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

- Versão de software adaptável 7.x da ferramenta de segurança de Cisco e mais tarde
- Versão 5.x e mais recente adaptável do Security Device Manager
- Versão Cliente VPN Cisco 4.x e mais tarde

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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão 7.x e mais recente da ferramenta de segurança de Cisco PIX.

Convenções

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

Informações de Apoio

As configurações do Acesso remoto fornecem o Acesso remoto seguro para Cisco VPN Client, tais como usuários móveis. Um acesso remoto VPN deixa usuários remotos firmemente alcançar recursos de rede centralizada. O Cisco VPN Client segue com o protocolo IPSec e é projetado especificamente trabalhar com a ferramenta de segurança. Contudo, a ferramenta de segurança pode estabelecer conexões IPSec com muitos clientes protocolo-complacentes. Refira manuais de configuração ASA para obter mais informações sobre do IPsec.

Os grupos e os usuários são conceitos do núcleo no Gerenciamento da Segurança dos VPN e na configuração da ferramenta de segurança. Especificam os atributos a que determine o acesso de usuários e o uso do VPN. Um grupo é uma coleção de usuários tratada como uma entidade única. Os usuários obtêm seus atributos das políticas do grupo. Os grupos de túneis identificam a política do grupo para conexões específicas. Se você não atribui uma política do grupo particular aos usuários, a política do grupo padrão para a conexão aplica-se.

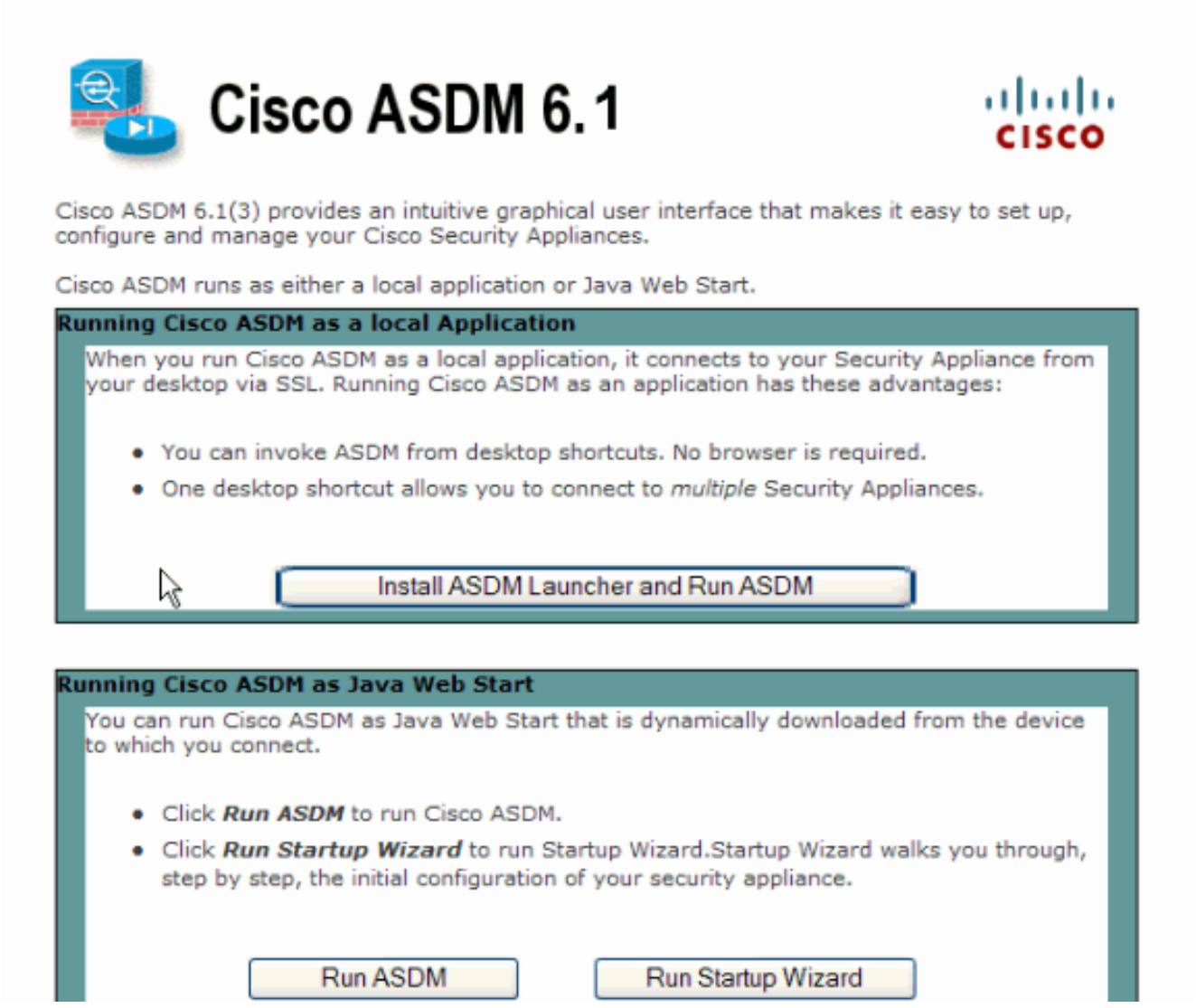
Um grupo de túneis consiste em um grupo de registros que determine políticas da conexão de túnel. Estes registros identificam os server a que os usuários do túnel são autenticados, assim como os servidores de contabilidade, eventualmente, a que a informação de conexão é enviada. Igualmente identificam uma política do grupo padrão para as conexões, e contêm parâmetros de conexão do específico de protocolo. Os grupos de túneis incluem um pequeno número de atributos que se referem a criação do túnel própria. Os grupos de túneis incluem um ponteiro a uma política do grupo que defina atributos USER-orientados.

Configurações

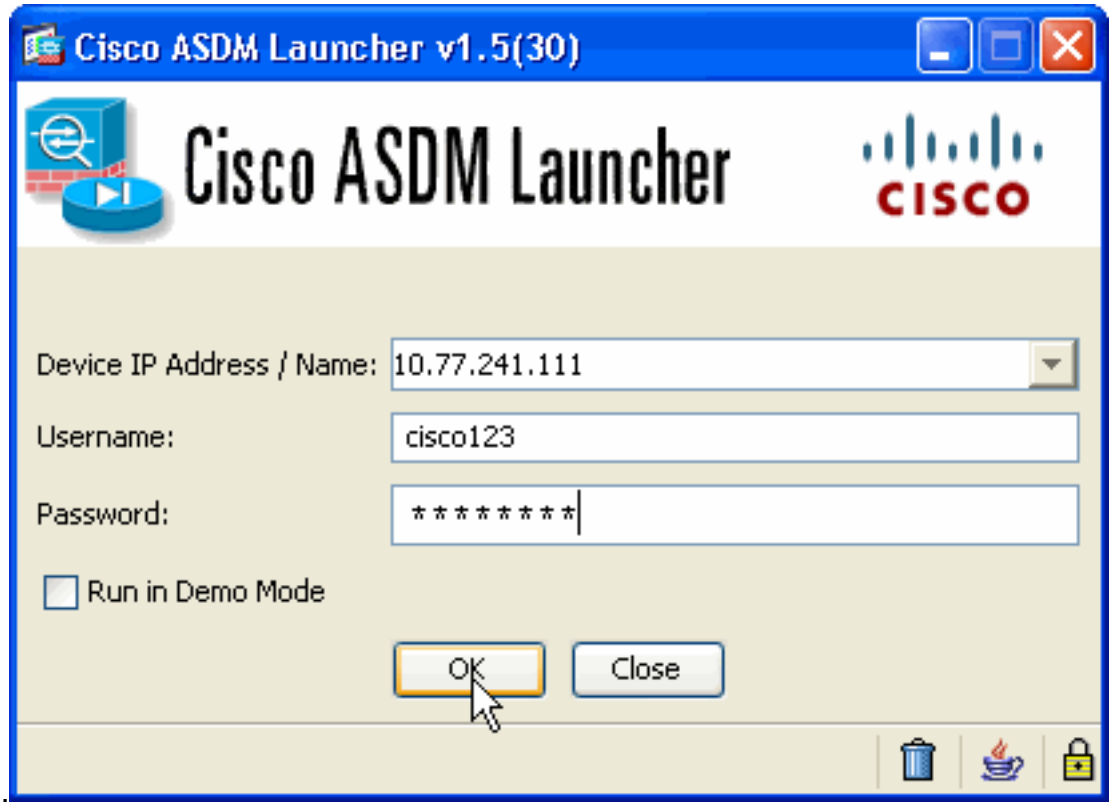
Configurar o ASA/PIX como um servidor de VPN remoto com ASDM

Termine estas etapas a fim configurar Cisco ASA como um servidor de VPN remoto com ASDM:

1. Abra seu navegador e incorpore **<IP_Address de https:// da relação do ASA que foi configurado para ASDM Access>** a fim alcançar o ASDM no ASA.Certifique-se autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O ASA apresenta este indicador para permitir a transferência do aplicativo ASDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java applet.

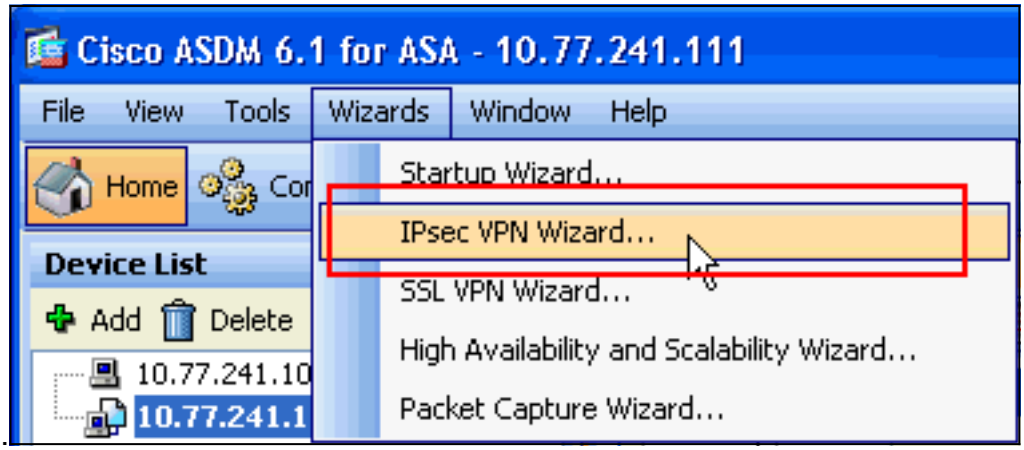


2. Clique a **launcher ASDM da transferência e comece o ASDM** a fim transferir o instalador para o aplicativo ASDM.
3. Uma vez as transferências da launcher ASDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador ASDM Cisco.
4. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação que você configurou com o **HTTP -** comande, e um nome de usuário e senha se você especificou um.Este exemplo usa o **cisco123** como o username e o **cisco123** como a



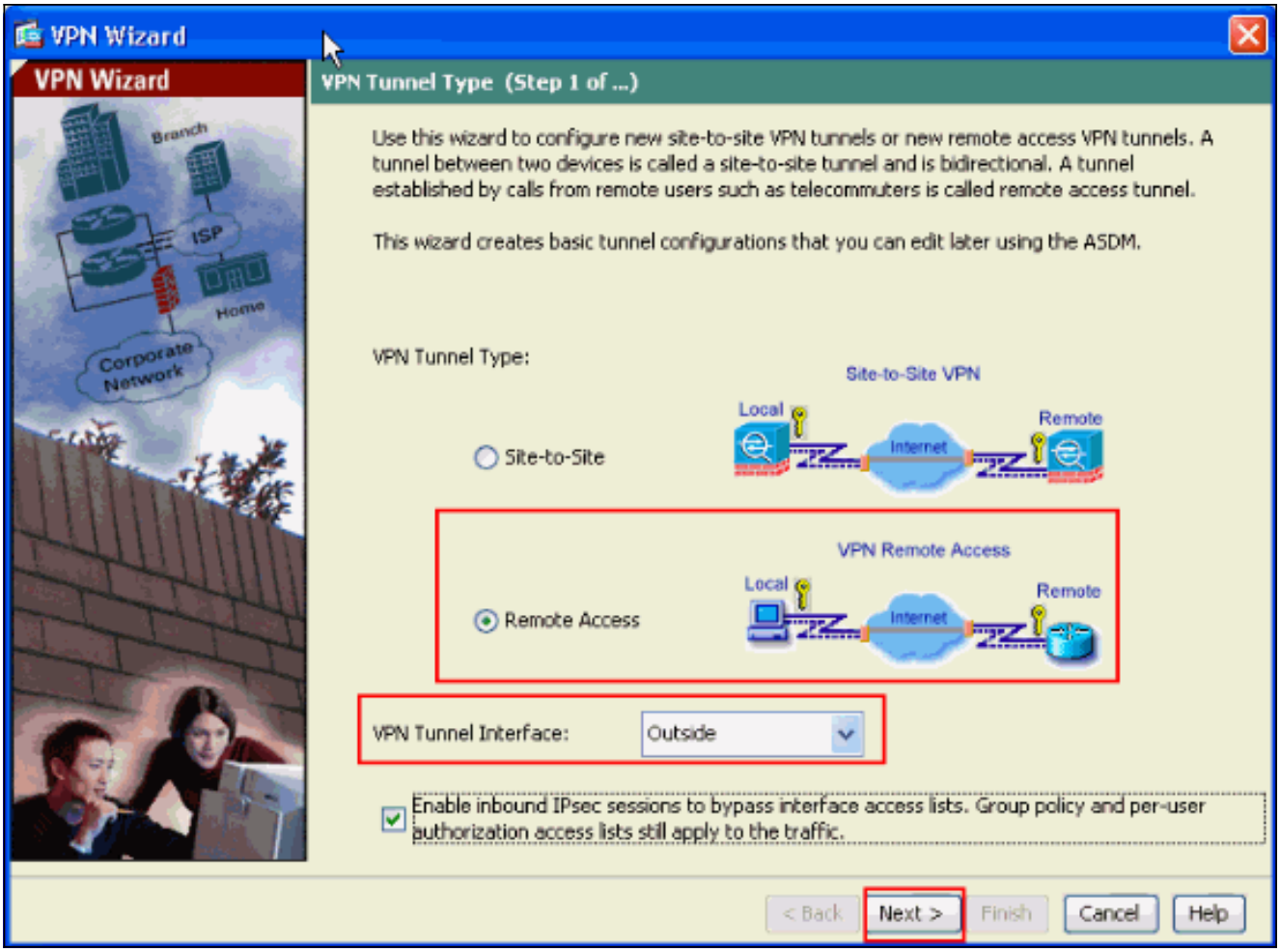
senha.

5. Selecione **assistentes > assistente do IPSec VPN do** indicador

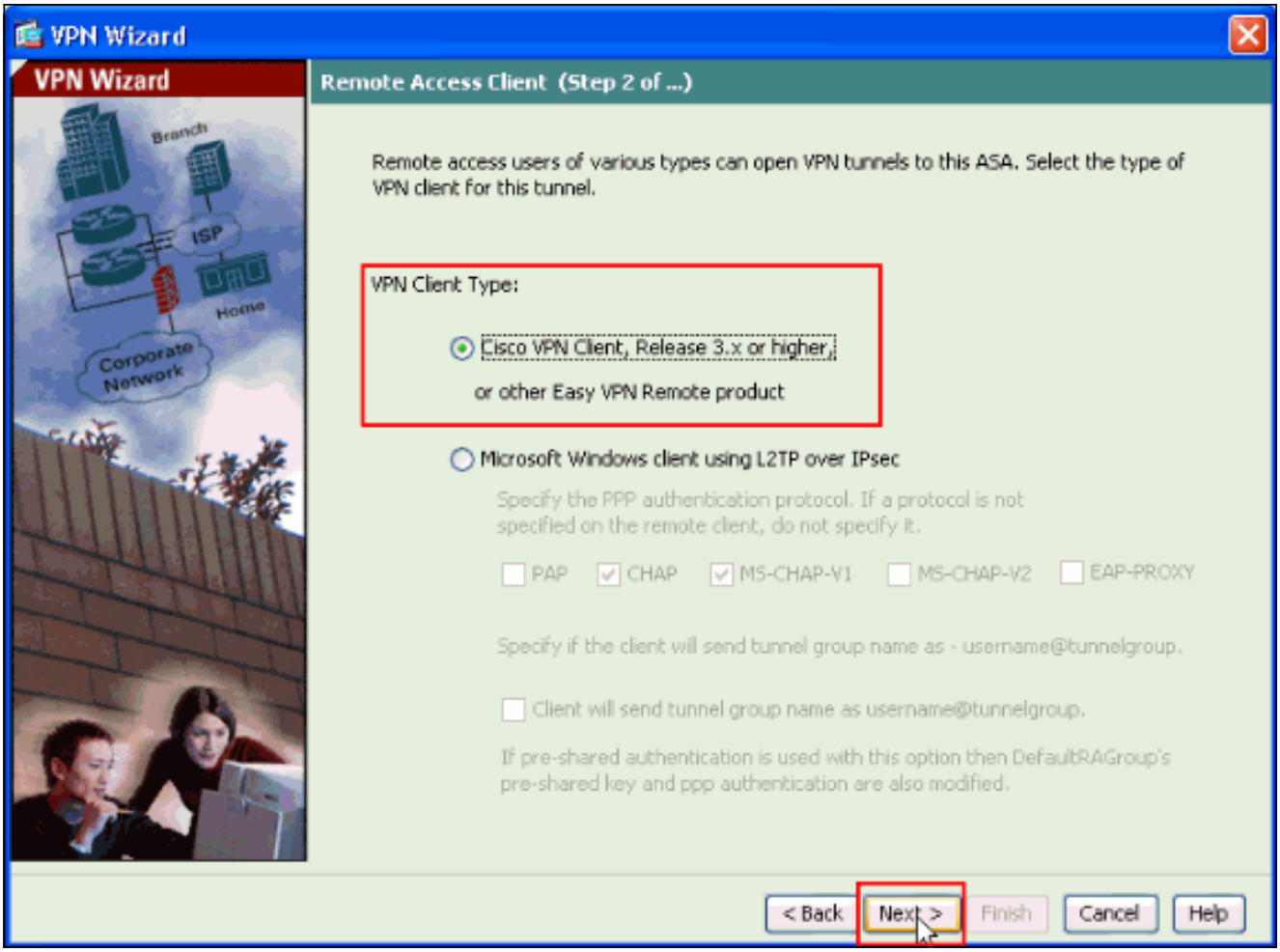


home.

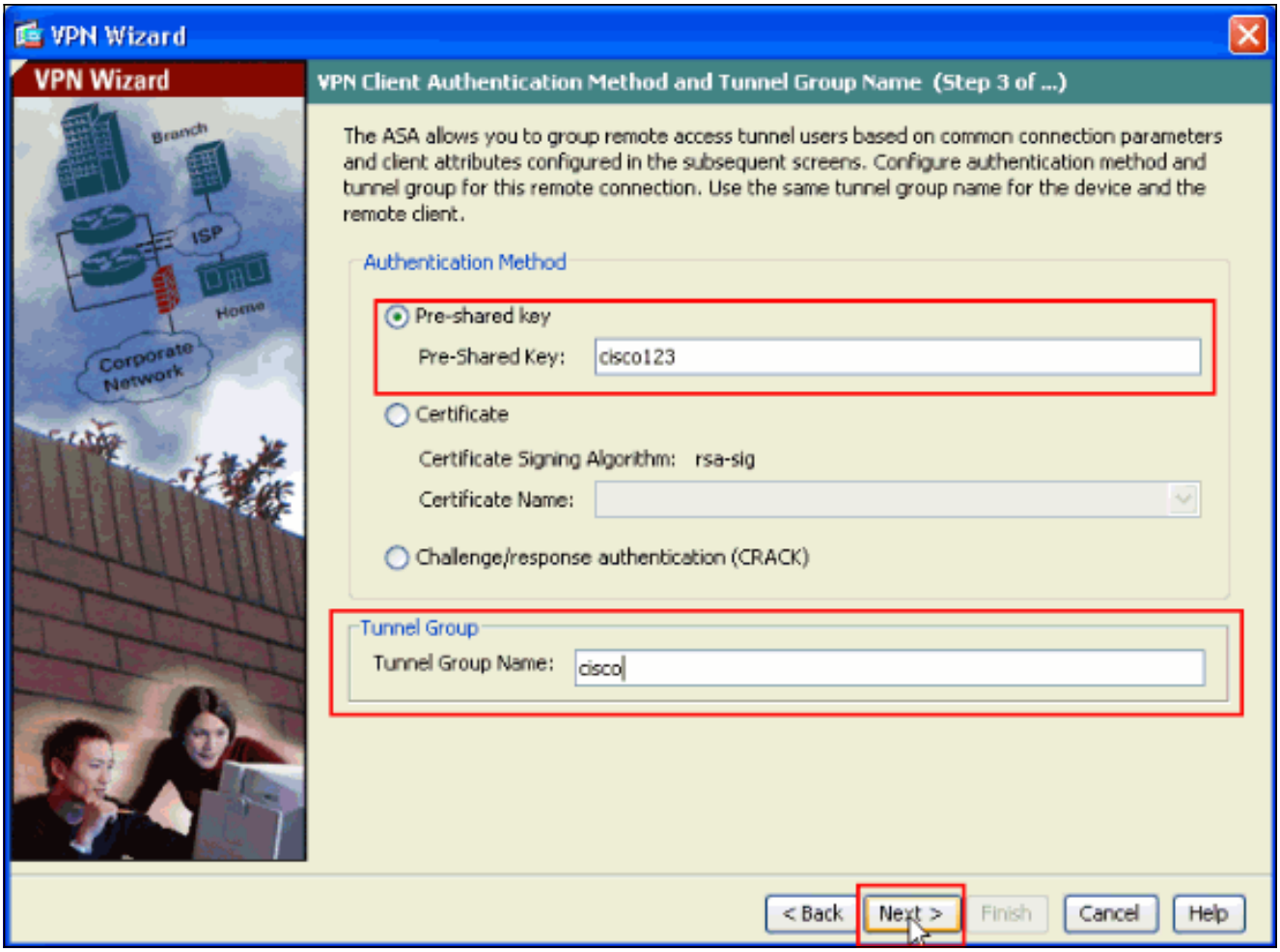
6. Selecione o tipo de túnel do **acesso remoto VPN** e assegure-se de que a interface de túnel VPN esteja ajustada como desejada, e clique-se **em seguida** como mostrado aqui.



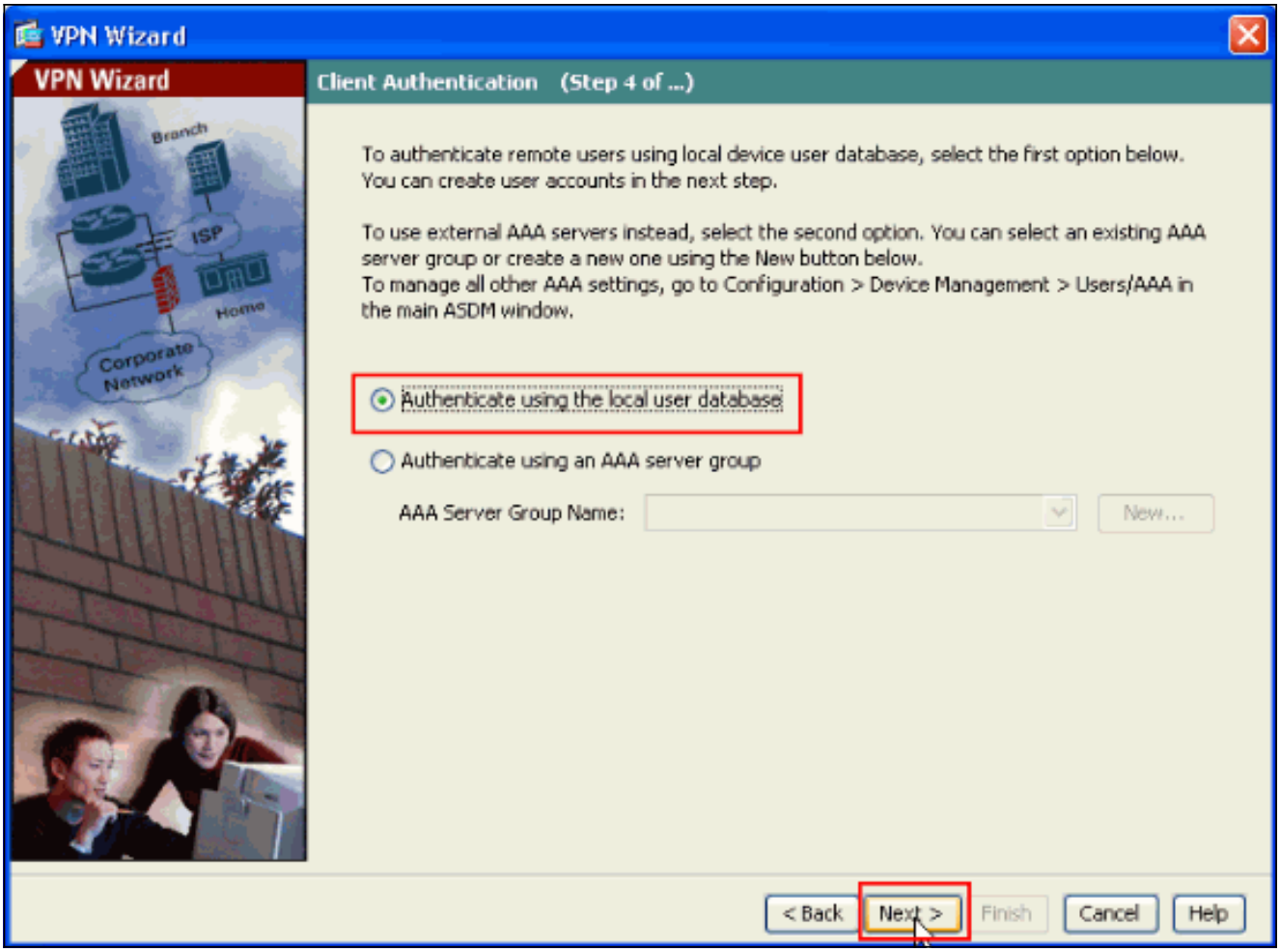
7. O tipo do cliente VPN é escolhido, como mostrado. **O Cisco VPN Client** é escolhido aqui. Clique em
   Next.



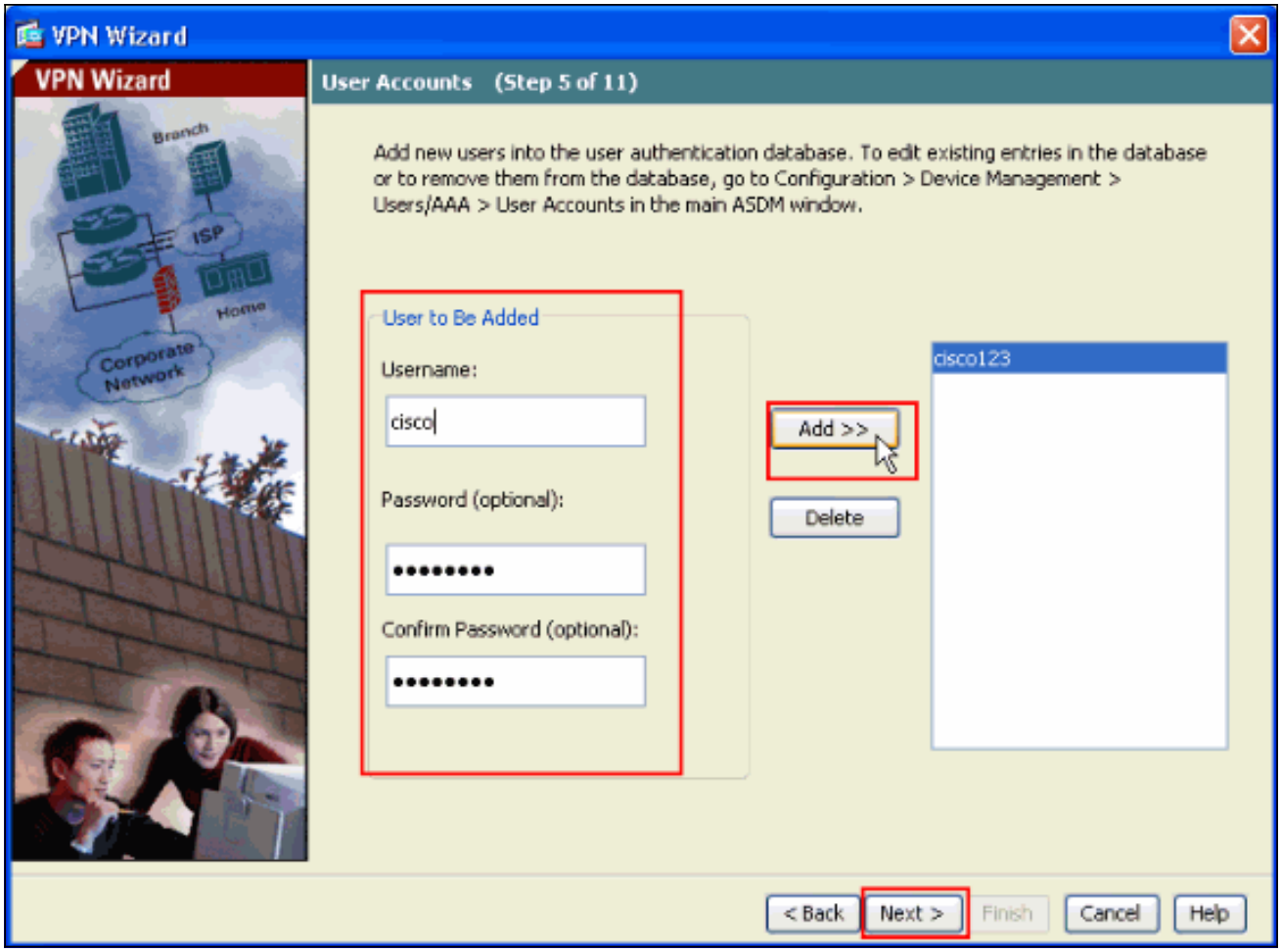
8. Dê entrada com um nome para o **nome de grupo de túneis**. Incorpore a informação da autenticação para usar-se, que é a **chave pré-compartilhada n**este exemplo. A chave pré-compartilhada usada neste exemplo é **cisco123**. O nome de grupo de túneis usado neste exemplo é **Cisco**. Clique em
Next.



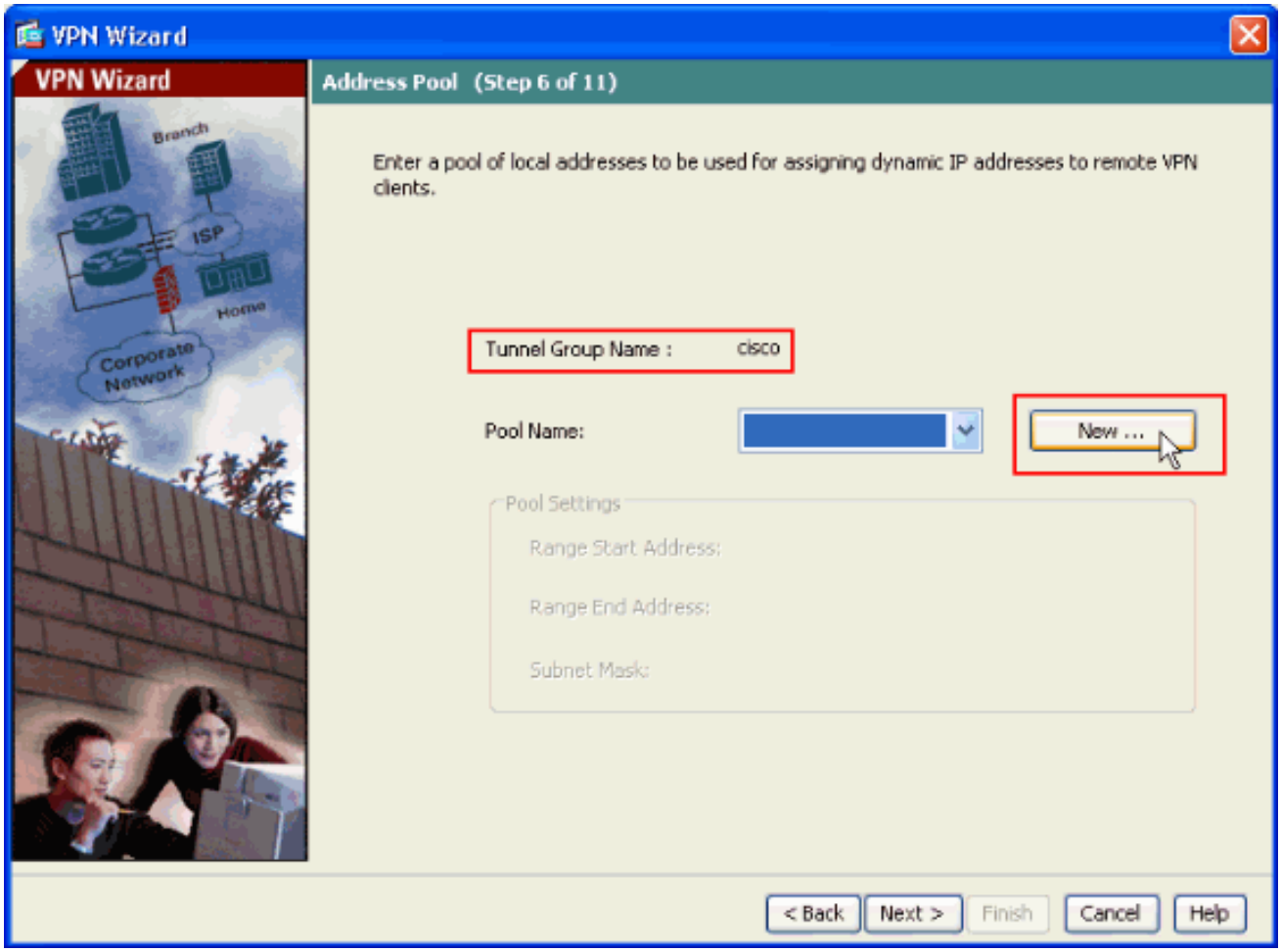
9. Escolha se você quer usuários remotos ser autenticado à base de dados de usuário local ou a um Grupo de servidores AAA externo.**Nota:** Você adiciona usuários à base de dados de usuário local na etapa 10.**Nota:** Refira [grupos de servidor da authentication e autorização PIX/ASA 7.x para usuários VPN através do exemplo da configuração ASDM] para obter informações sobre de como configurar um Grupo de servidores AAA externo com ASDM.



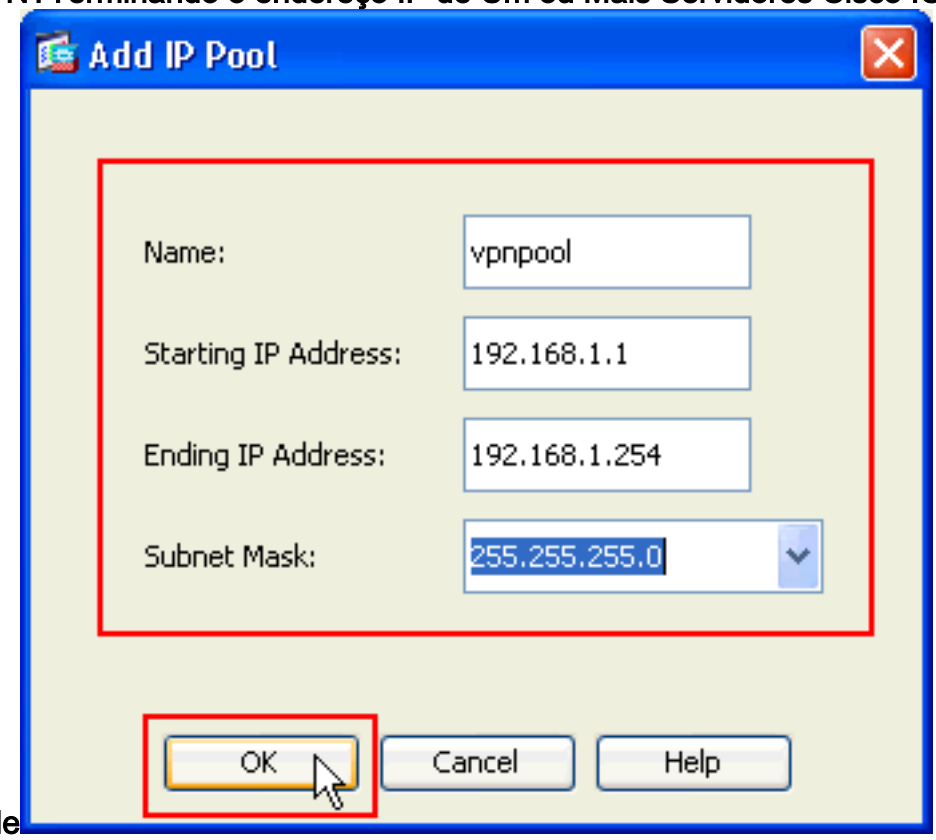
10. Forneça um **username** e a **senha** e o clique opcionais **adicionam** a fim adicionar novos usuários ao base de dados de autenticação de usuário. Clique em Next.**Nota:** Não remova os usuários existentes deste indicador. Selecione a **configuração > o Gerenciamento de dispositivos > o Users/AAA > as contas de usuário na** janela principal de ASDM para editar entradas existentes no base de dados ou para removê-las do base de dados.



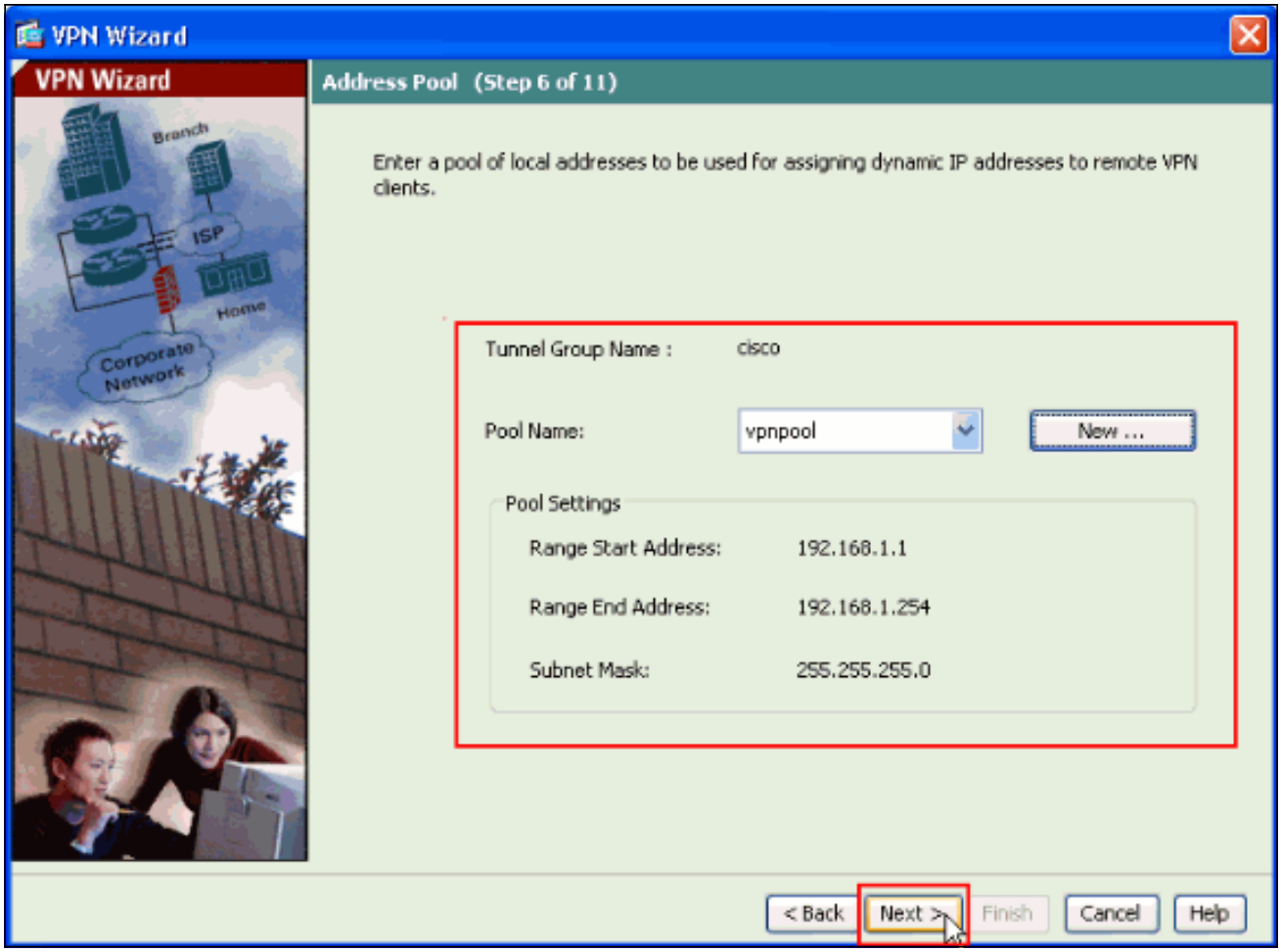
11. A fim definir um pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos, clique **novo** para criar um **IP pool** novo.



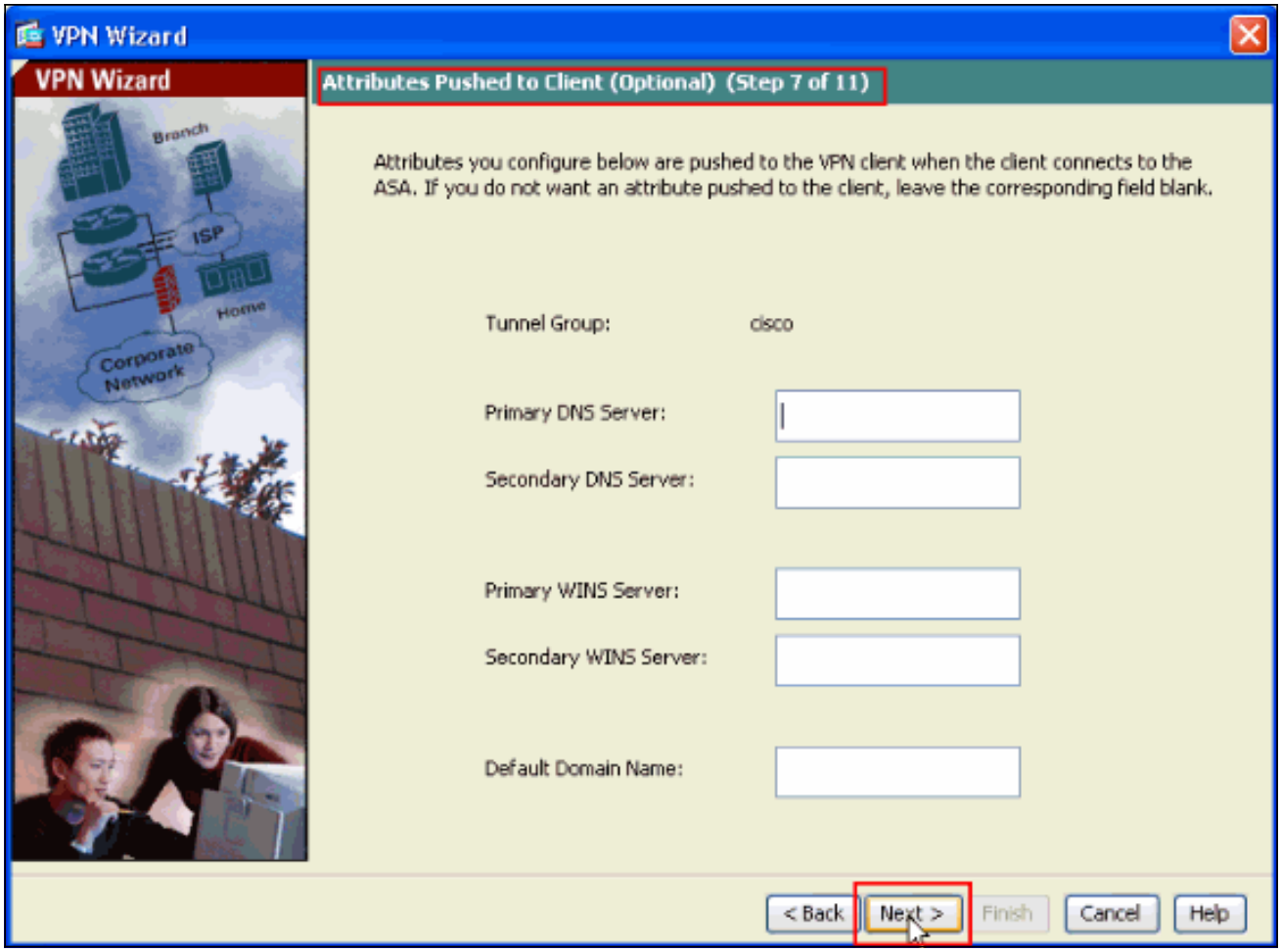
12. Na nova janela intitulada **adicionar o IP pool** fornecem esta informação, e clicam a **APROVAÇÃO.Nome do IP poolComeçando o endereço IP de Um ou Mais Servidores Cisco ICM NTTerminando o endereço IP de Um ou Mais Servidores Cisco ICM NTMáscara de sub-rede**



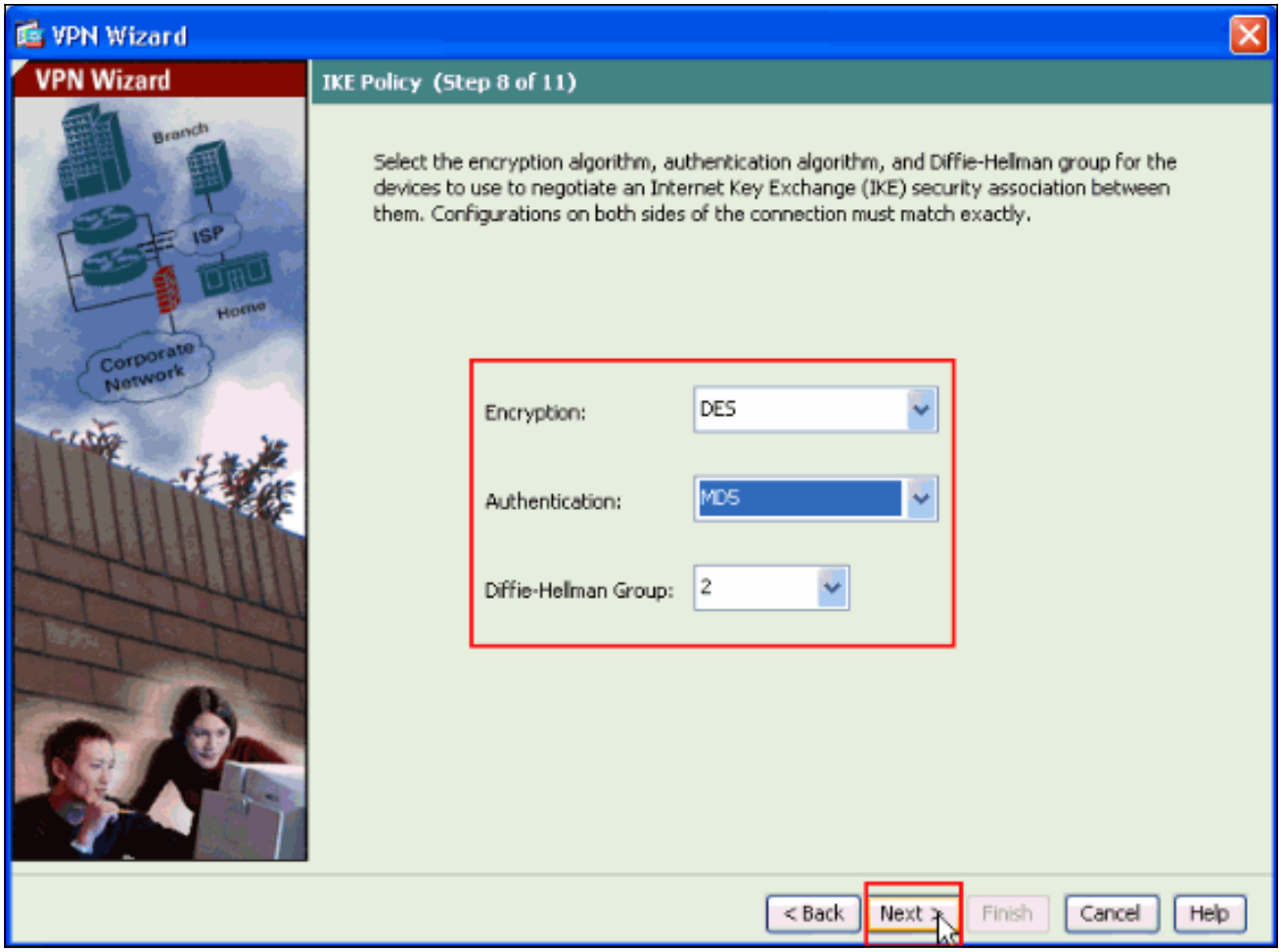
13. Depois que você define o pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos quando conectam, clique **em seguida.**



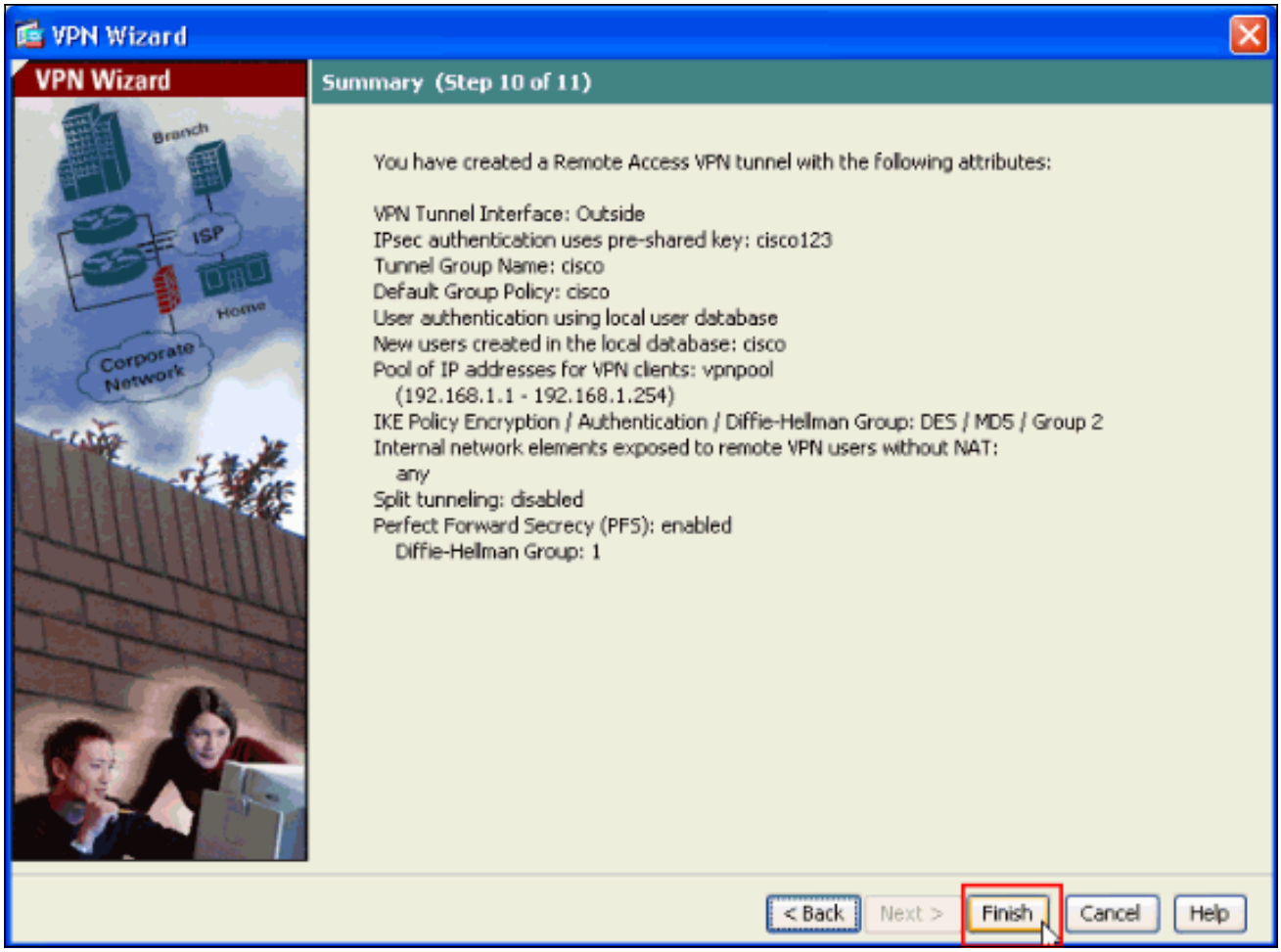
14. *Opcional:* Especifique o DNS e GANHE a informação do servidor e um Domain Name do padrão a ser empurrado para clientes VPN remotos.



15. Especifique os parâmetros para o IKE, igualmente conhecidos como a fase 1. IKE.As configurações em ambos os lados do túnel devem combinar exatamente. Contudo, o Cisco VPN Client seleciona automaticamente a configuração apropriada para se. Consequentemente, nenhuma configuração de IKE é necessária no PC cliente.



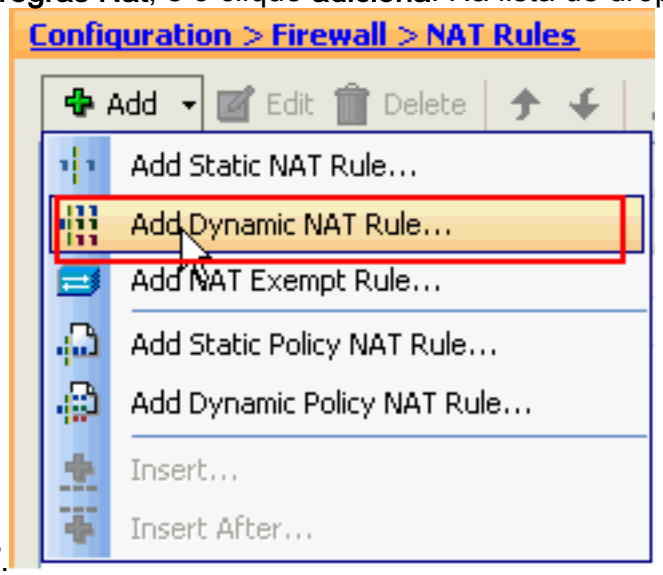
16. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.



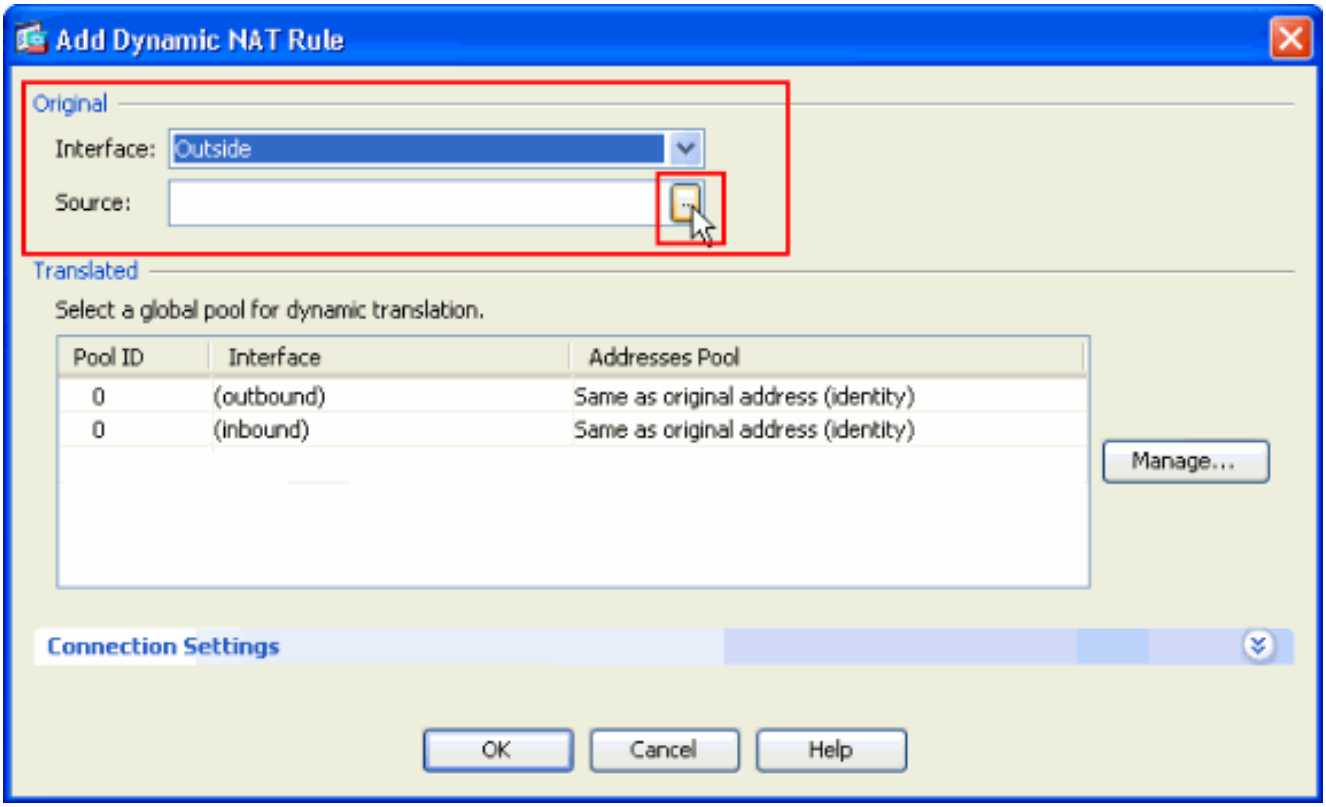
Configurar o ASA/PIX ao tráfego do cliente VPN da entrada de NAT com ASDM

Termine estas etapas a fim configurar Cisco ASA ao tráfego do cliente VPN da entrada de NAT com ASDM:

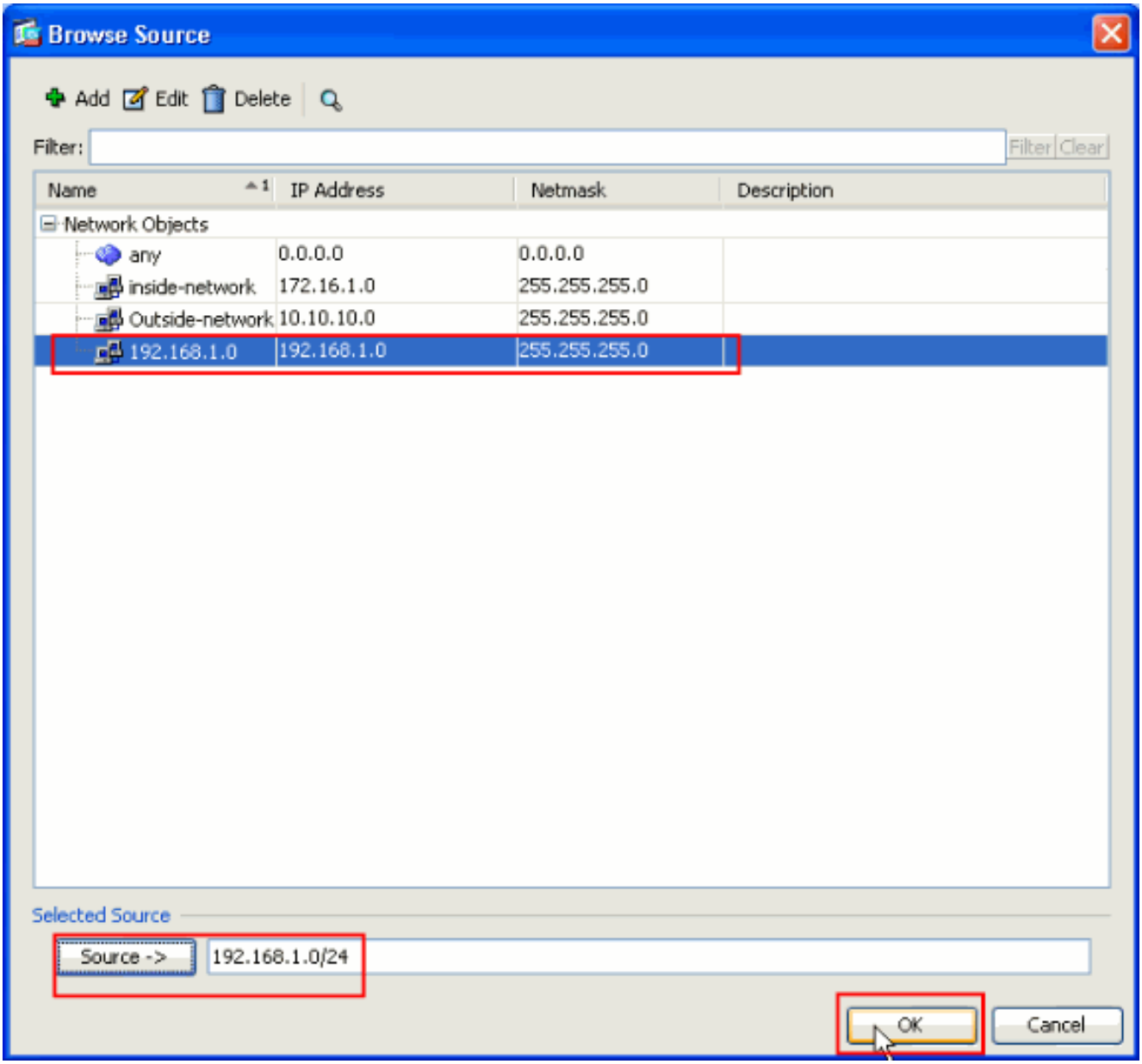
1. Escolha a **configuração > o Firewall > regras Nat**, e o clique **adiciona**. Na lista de drop-down, seleta **adicionar a regra dinâmica NAT**.



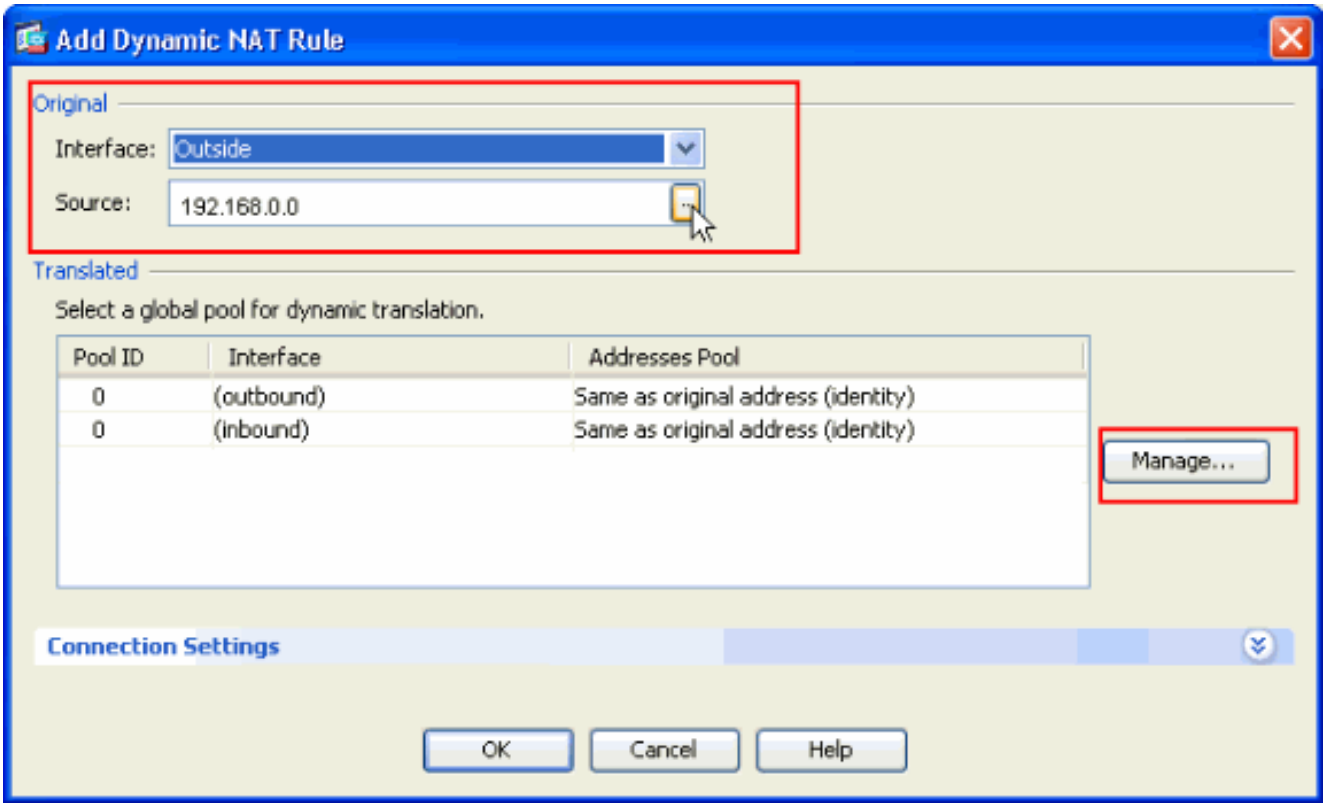
2. No indicador **dinâmico da regra adicionar NAT**, escolha a **parte externa** como a relação, e clique o botão Browse ao lado da caixa da **fonte**.



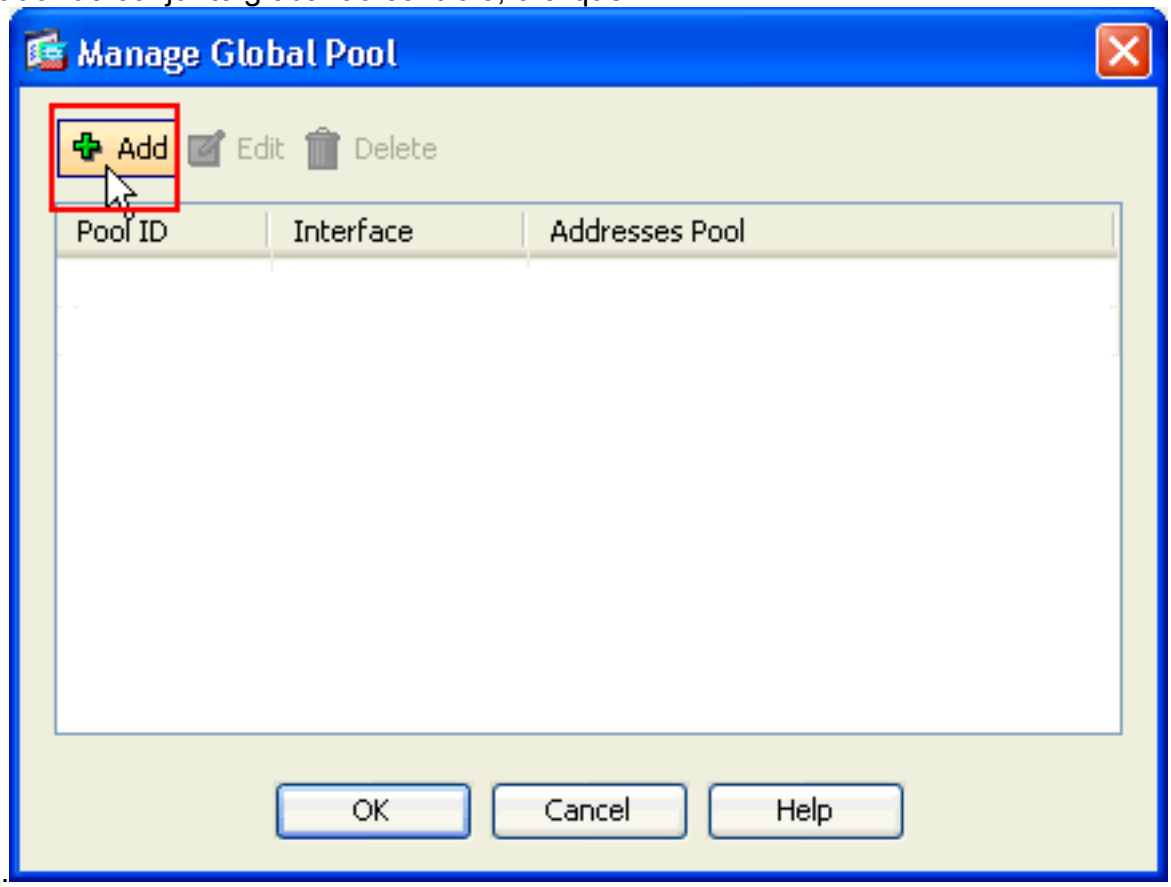
3. No indicador da fonte da consultação, selecione os objetos de rede adequada e igualmente escolha a **fonte** sob a seção selecionada da fonte, e clique a **APROVAÇÃO**. O objeto de rede de 192.168.1.0 é escolhido
aqui.



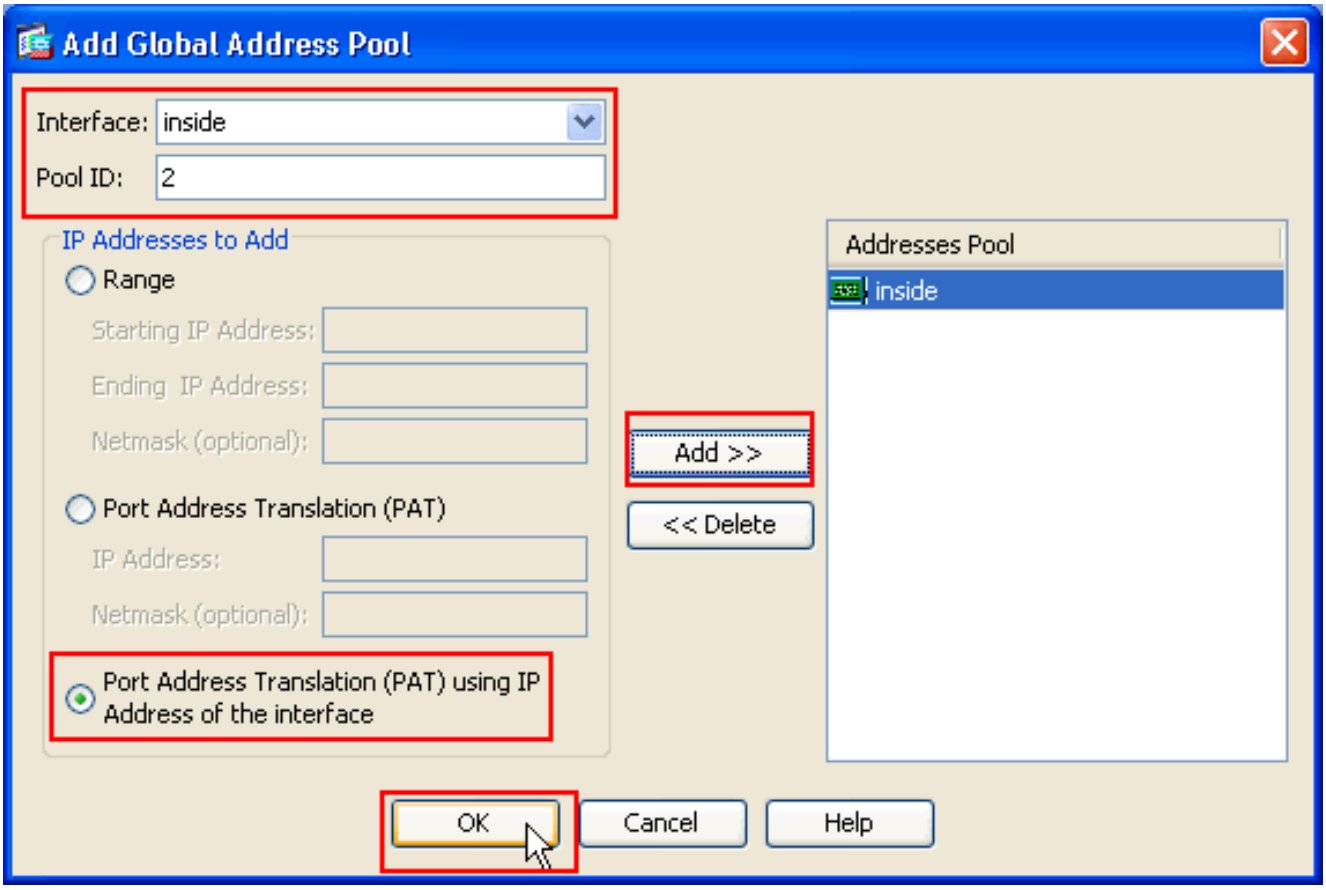
4. O clique **controla**.



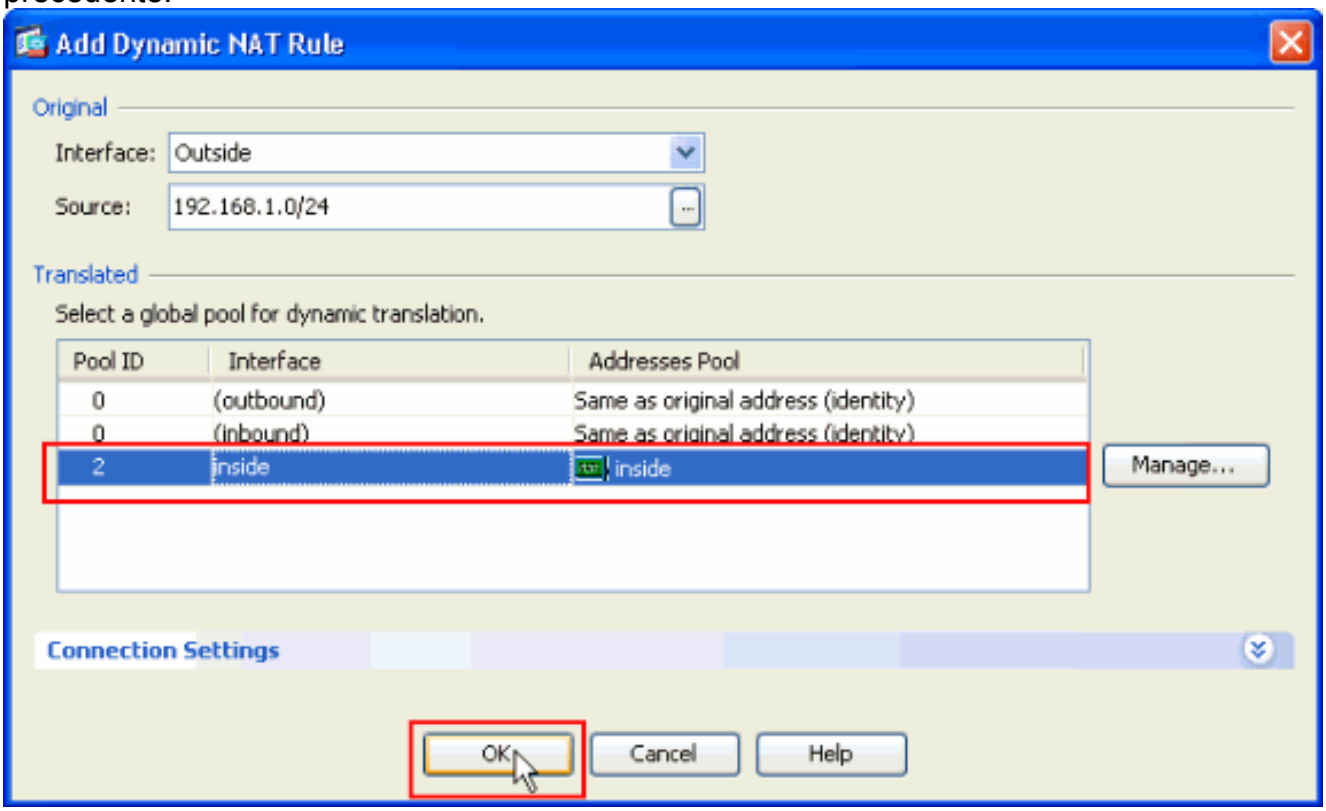
5. No indicador do conjunto global do controlo, o clique **adiciona**.



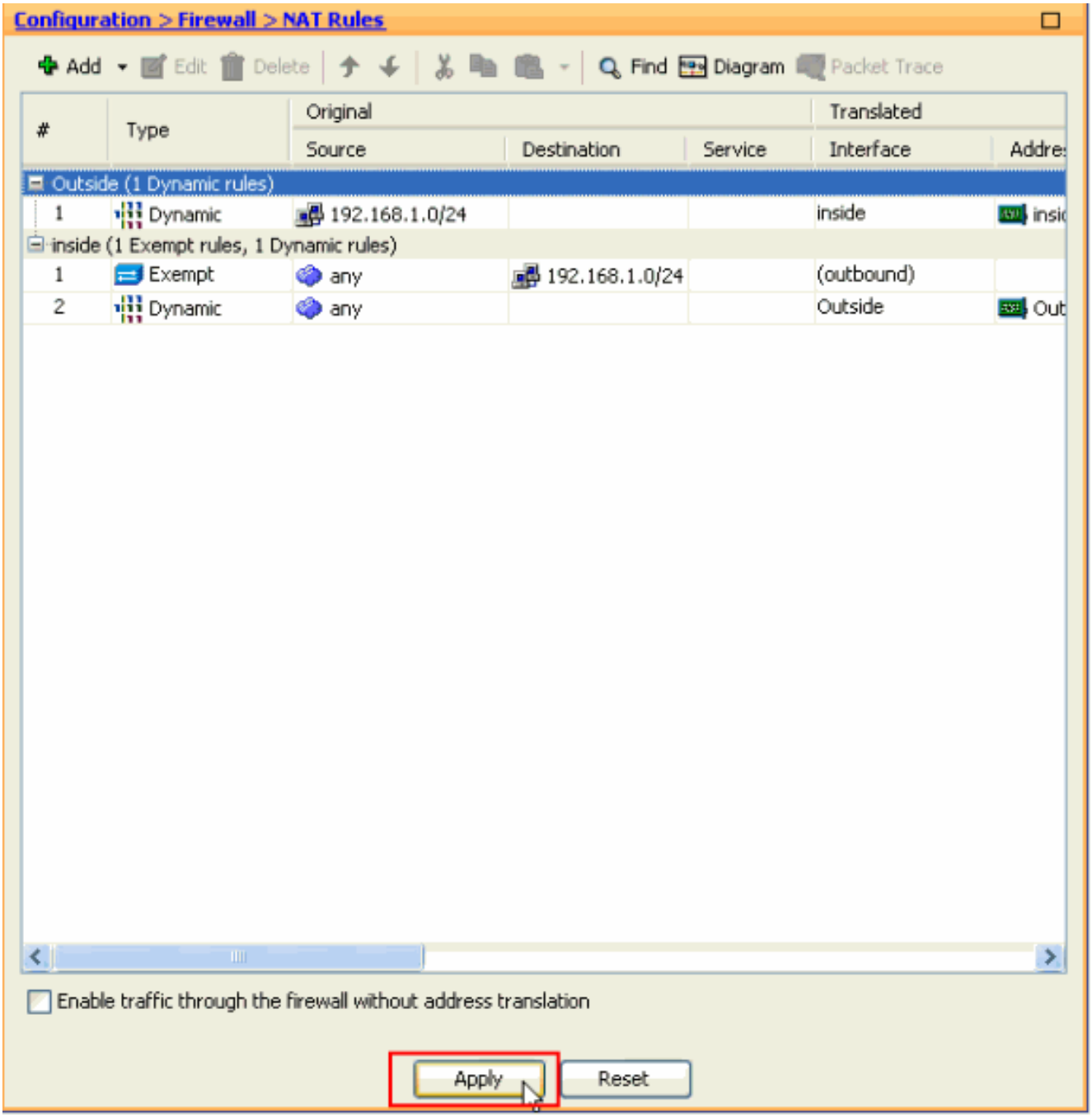
6. No indicador do conjunto de endereço global adicionar, escolha o **interior** como a relação e os **2** como o **pool ID**. Igualmente certifique-se de que o botão de rádio ao lado da **PANCADINHA que usa o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação** está selecionado. Clique **Add>>**, e clique então a **APROVAÇÃO**.



7. Clique a **APROVAÇÃO** depois que você seleciona o conjunto global com o **pool ID 2** configurado na etapa
precedente.



8. Agora o clique **aplica-se** de modo que a configuração seja aplicada ao ASA.This termine a configuração.



Configurar o ASA/PIX como um servidor de VPN remoto e para o NAT de entrada com o CLI

Configuração running no dispositivo ASA
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 ! ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 **ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control **global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2**

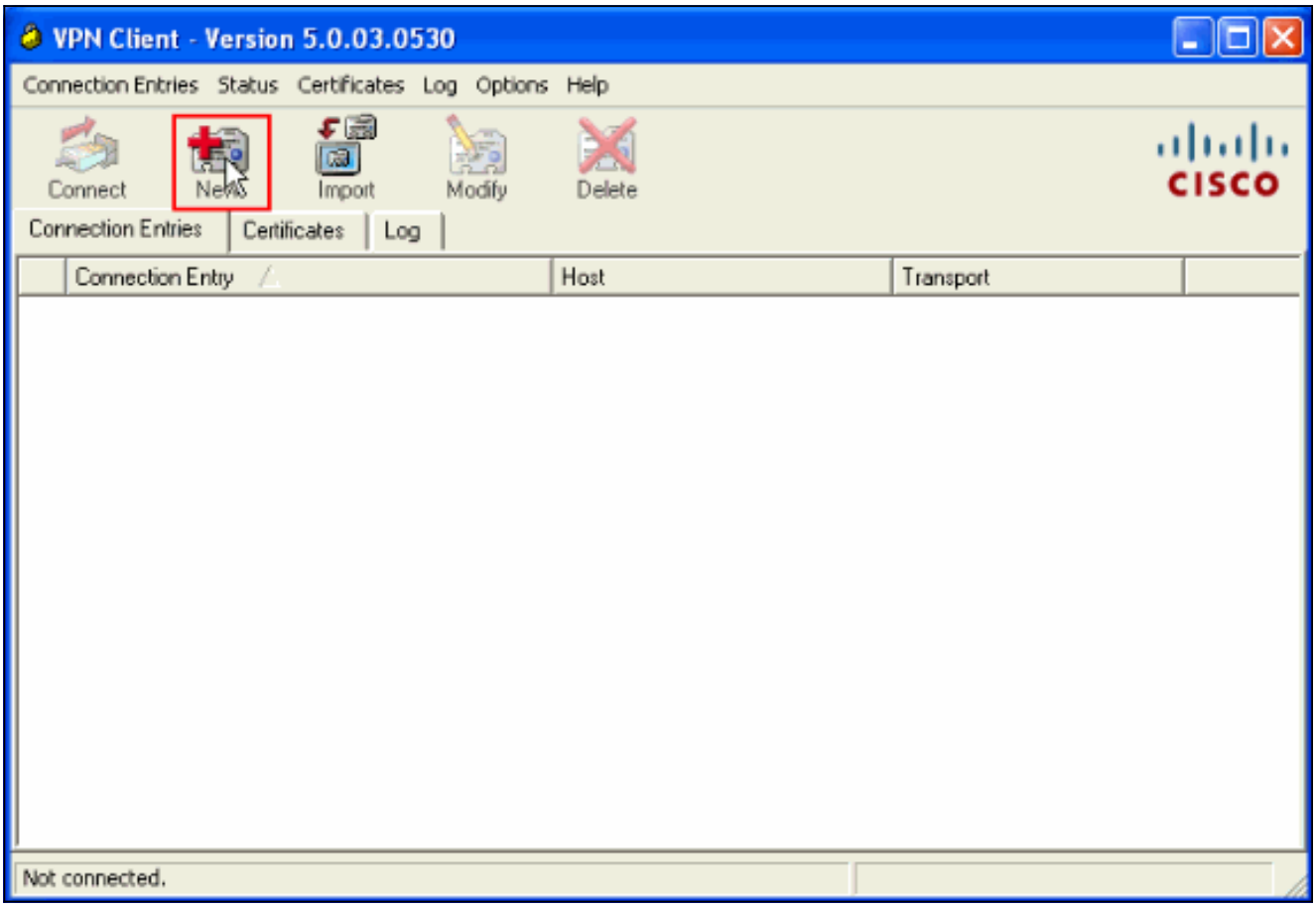
```
192.168.1.0 255.255.255.0 outside nat (inside) 0 access-
list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 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 no snmp-server location no snmp-server
contact !--- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto
ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP
65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto
map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map
interface Outside crypto isakmp enable Outside !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and !--- Policy
details are hidden as the default values are chosen.
crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 2 lifetime 86400 crypto
isakmp policy 30 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 telnet timeout 5 ssh
timeout 60 console timeout 0 management-access inside
threat-detection basic-threat threat-detection
statistics access-list group-policy cisco internal
group-policy cisco attributes vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 0 username
cisco attributes vpn-group-policy cisco tunnel-group
cisco type remote-access tunnel-group cisco general-
attributes address-pool vpnpool default-group-policy
cisco !--- Specifies the pre-shared key "cisco123" which
must !--- be identical at both peers. This is a global
!--- configuration mode command. tunnel-group cisco
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns migrated_dns_map_1
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
migrated_dns_map_1 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 prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end
ciscoasa#
```

Verificar

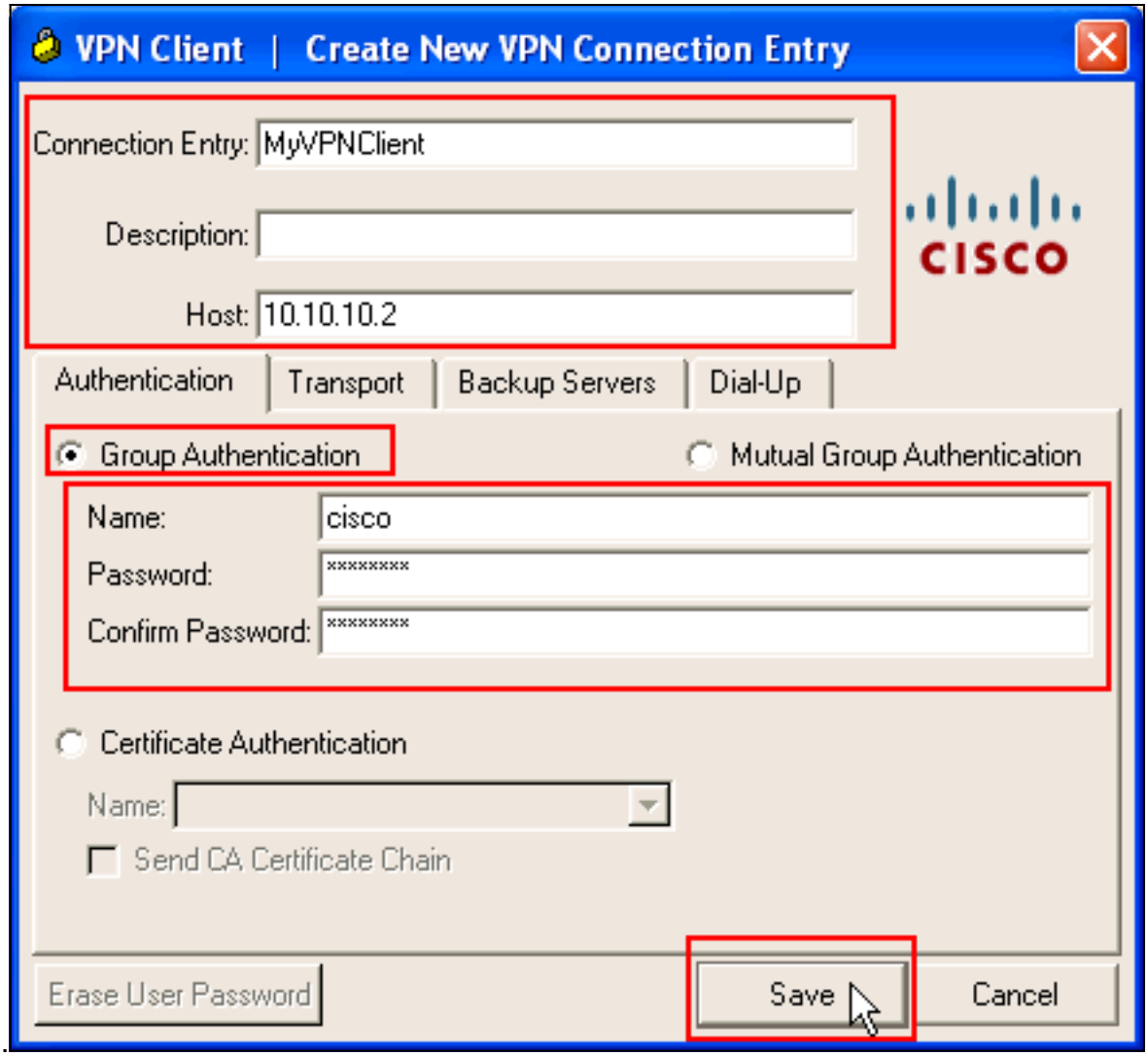
Tente conectar a Cisco ASA através do Cisco VPN Client a fim verificar que o ASA está

configurado com sucesso.

1. Clique em
   New.

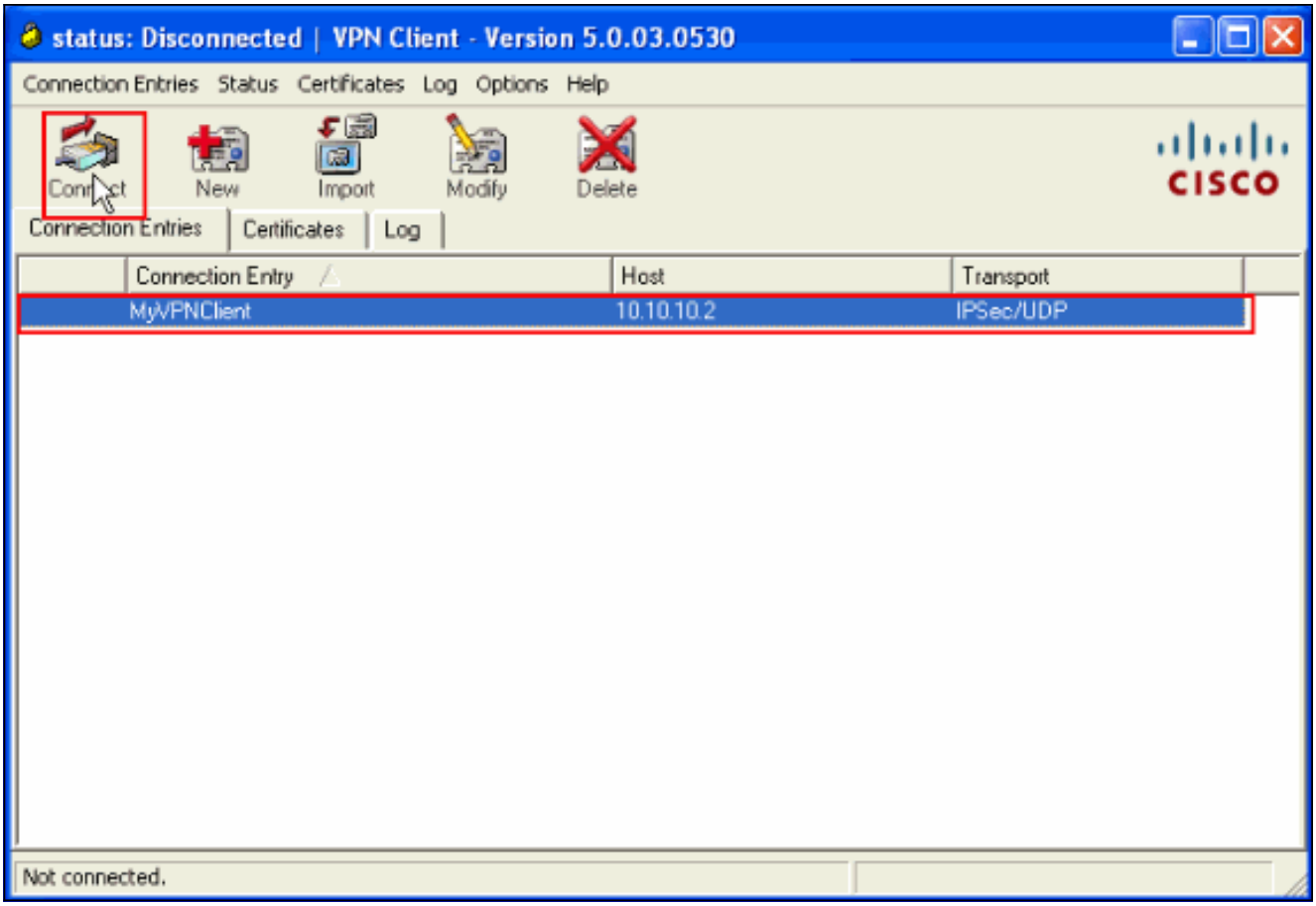


2. Preencha os detalhes de sua nova conexão.O campo do host deve conter o endereço IP ou nome do host de Cisco previamente configurado ASA. A informação da autenticação do grupo deve corresponder àquela usada na **salvaguarda do** clique de **etapa 4.** quando você é

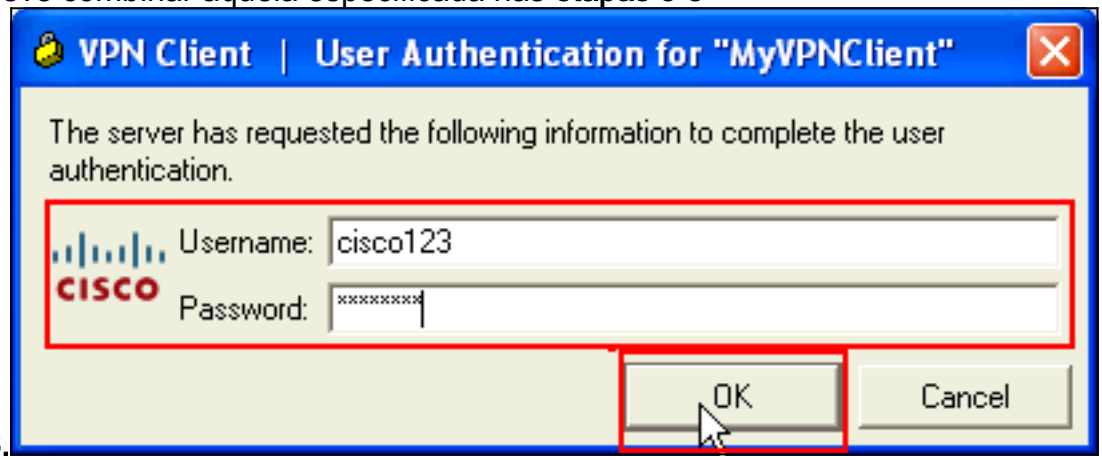


terminado.

3. Selecione a conexão recém-criado, e o clique **conecta**.

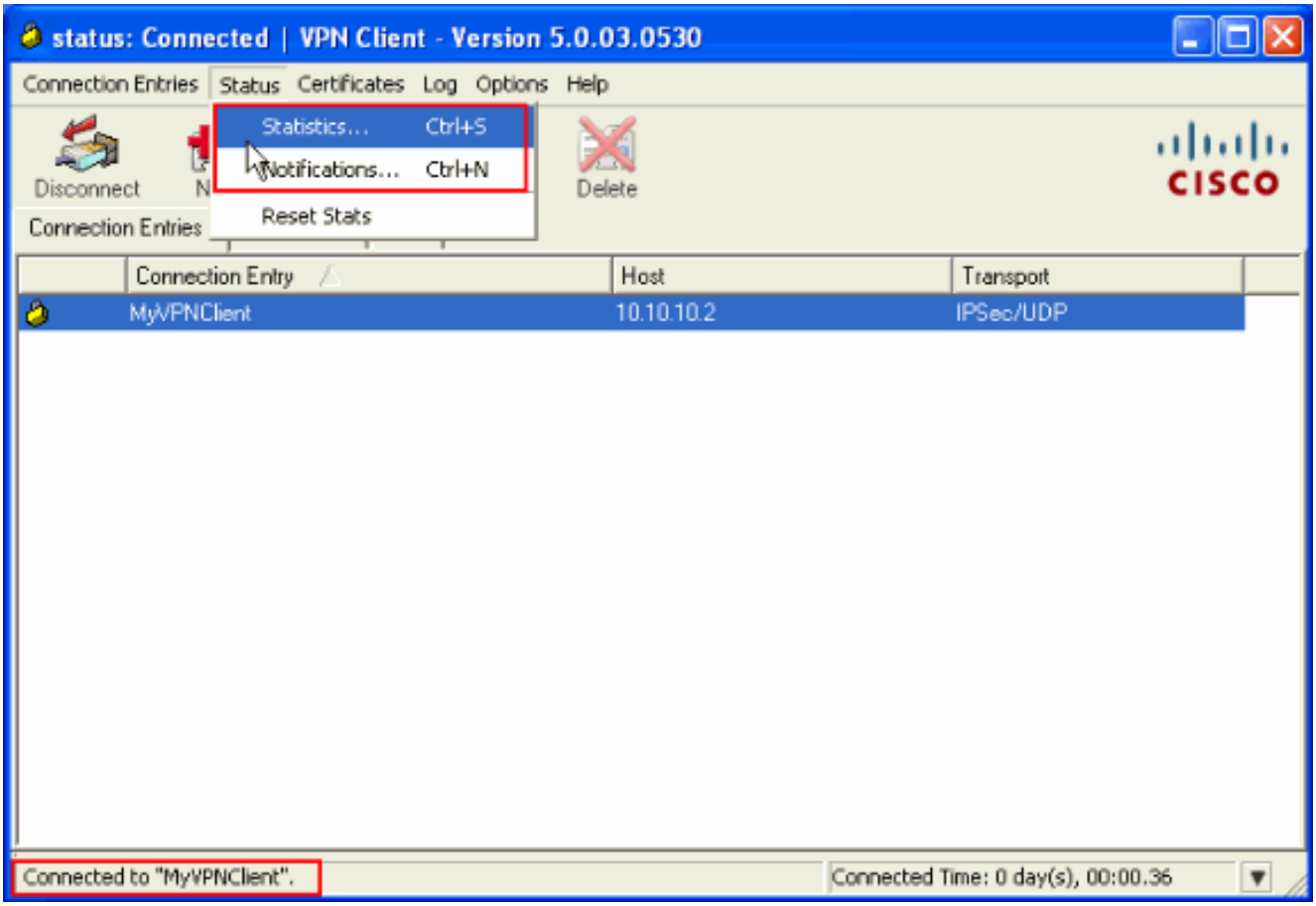


4. Incorpore um nome de usuário e senha para a autenticação extendida. Esta informação deve combinar aquela especificada nas **etapas 5 e**

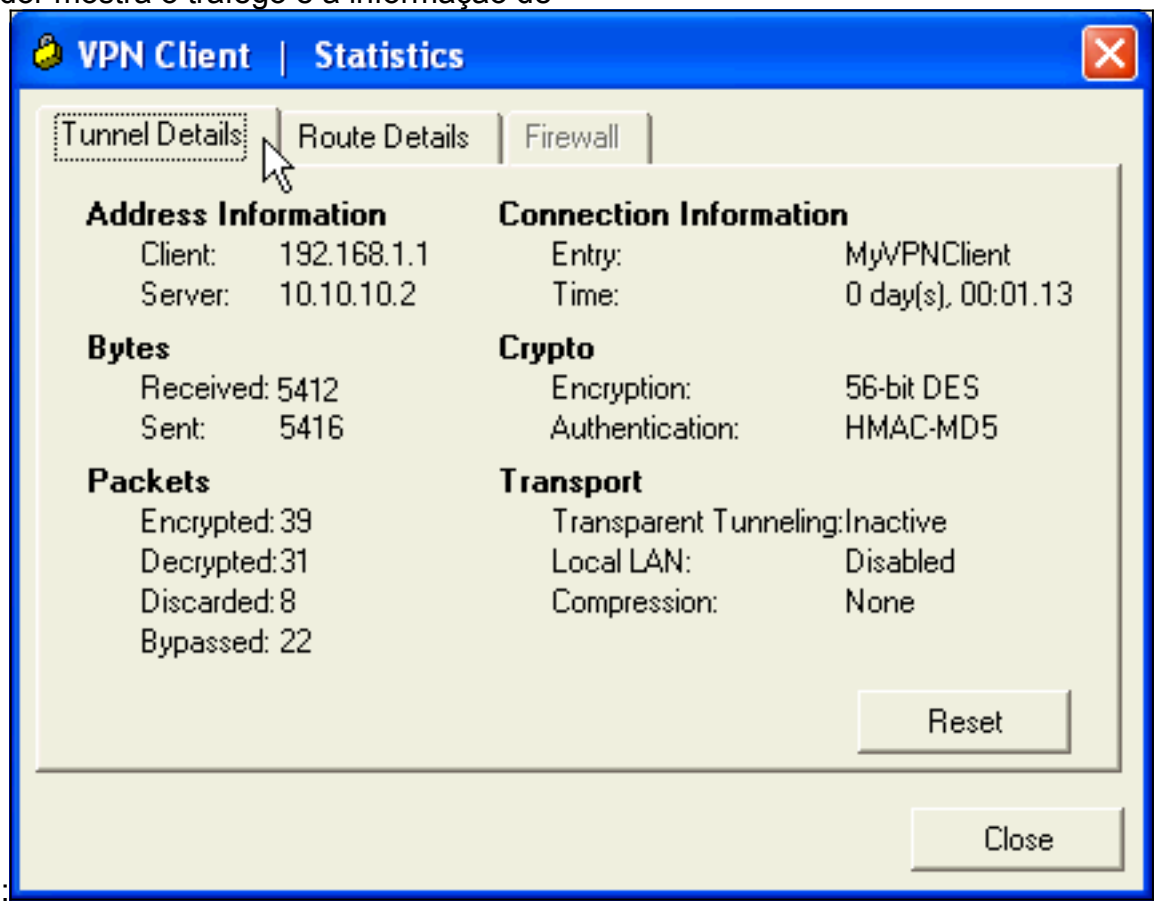


6.

5. Uma vez que a conexão é estabelecida com sucesso, escolha **estatísticas do** menu de status a fim verificar os detalhes do
túnel.

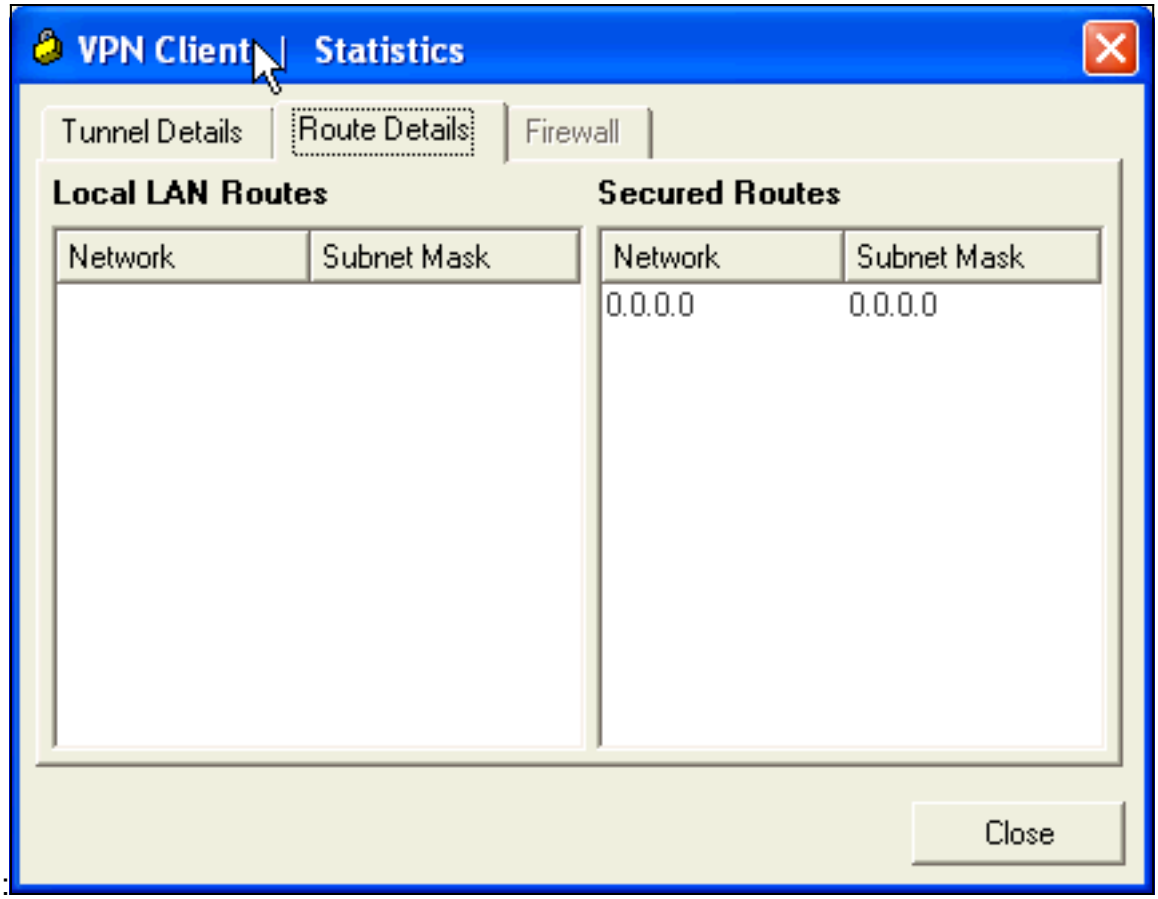


Este indicador mostra o tráfego e a informação de criptografia:



Este indicador mostra a informação do Split

Tunneling:



Ferramenta de segurança ASA/PIX - comandos show

- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.ASA#**show crypto isakmp sa** Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE
- **mostre IPsec cripto sa** — Mostra todo o sas de IPSec atual em um par.ASA#**show crypto ipsec sa** interface: Outside **Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0** #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 **local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1** path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#**debug icmp trace** *!--- Inbound Nat Translation is shown below for Outside to Inside* **ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1** ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 *!--- Inbound Nat Translation is shown below for Inside to Outside* **ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768** ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from

```
172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to
172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768
seq=8960 len=32
```

Troubleshooting

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

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

Refira a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções para obter mais informações sobre de como pesquisar defeitos o Local-local VPN.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Adaptive Security Device Manager
- O Dispositivos de segurança adaptáveis Cisco ASA série 5500 pesquisa defeitos e alertas
- Suporte Técnico e Documentação - Cisco Systems