ASA/PIX: IP Estático que endereça para o cliente do IPSec VPN com CLI e exemplo da configuração ASDM

Índice

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável do Cisco 5500 Series (ASA) para fornecer o endereço IP estático ao cliente VPN o Security Device Manager adaptável (ASDM) ou o CLI. 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 com o Cisco VPN Client.

Refira PIX/ASA 7.x e Cisco VPN Client 4.x com exemplo da configuração de autenticação do RAIO de Windows 2003 IAS (contra o diretório ativo) a fim estabelecer a conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500. O usuário de cliente VPN remoto autentica contra o diretório ativo com um servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refira PIX/ASA 7.x e Cisco VPN Client 4.x para o exemplo da configuração de autenticação do Cisco Secure ACS a fim estabelecer uma conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500 com um Serviço de

controle de acesso Cisco Secure (versão de ACS 3.2) para a autenticação extendida (XAUTH).

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.

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.

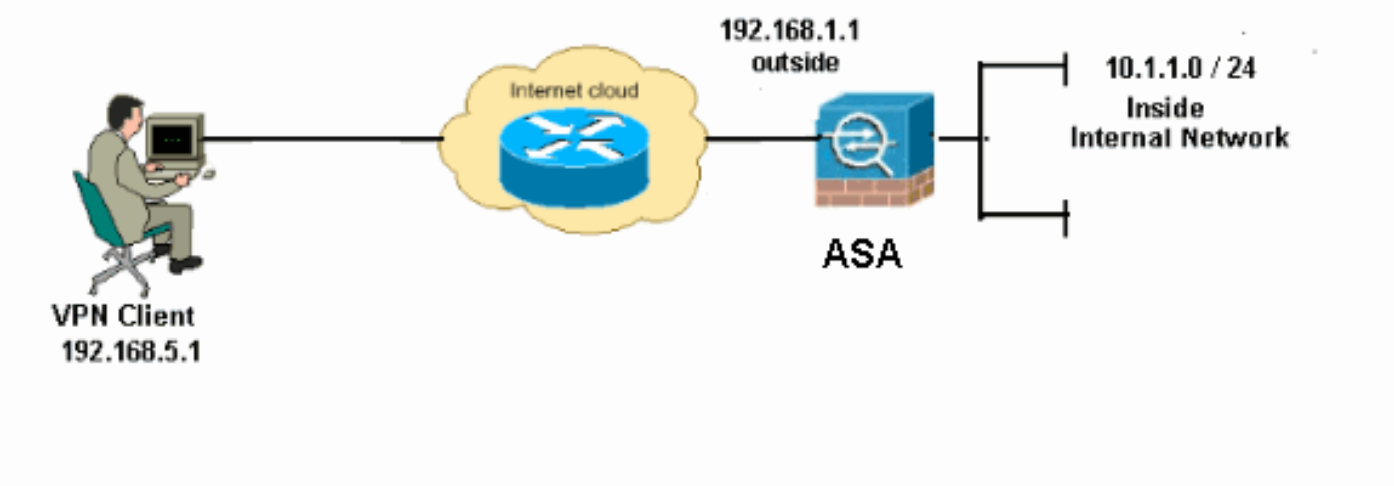
Configurar

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:



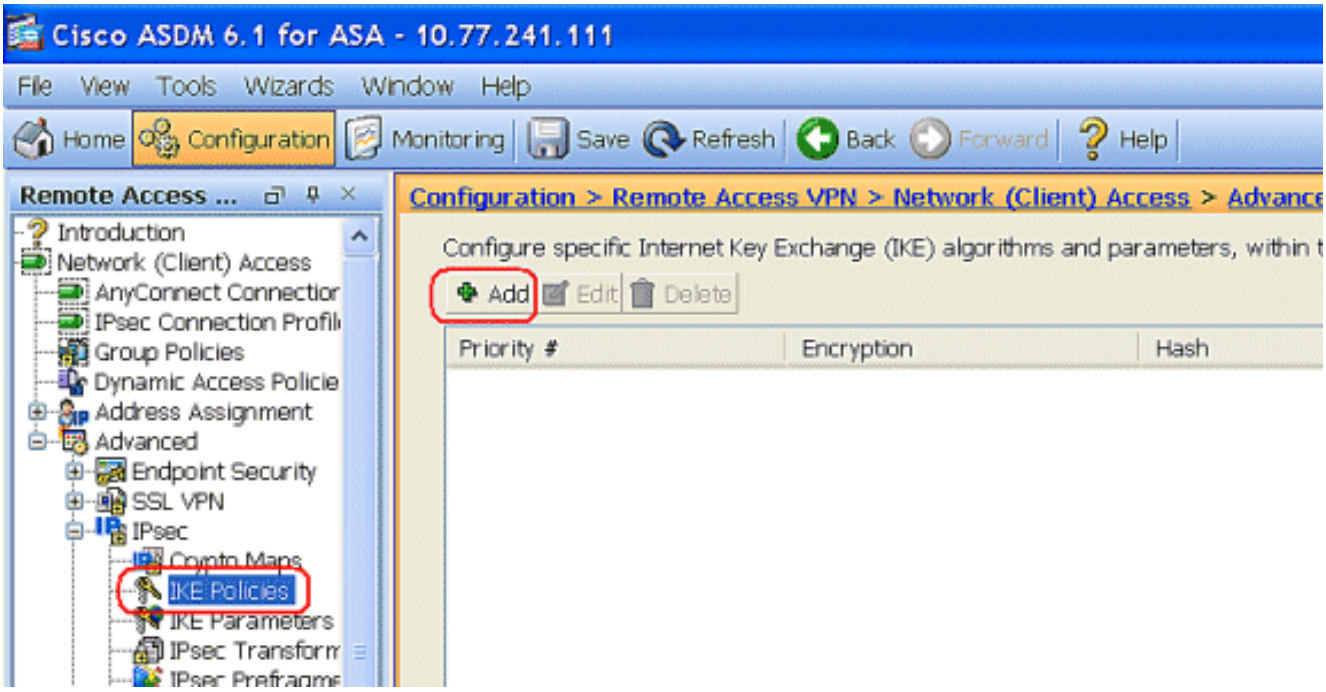
Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

Configurar o acesso remoto VPN (o IPsec)

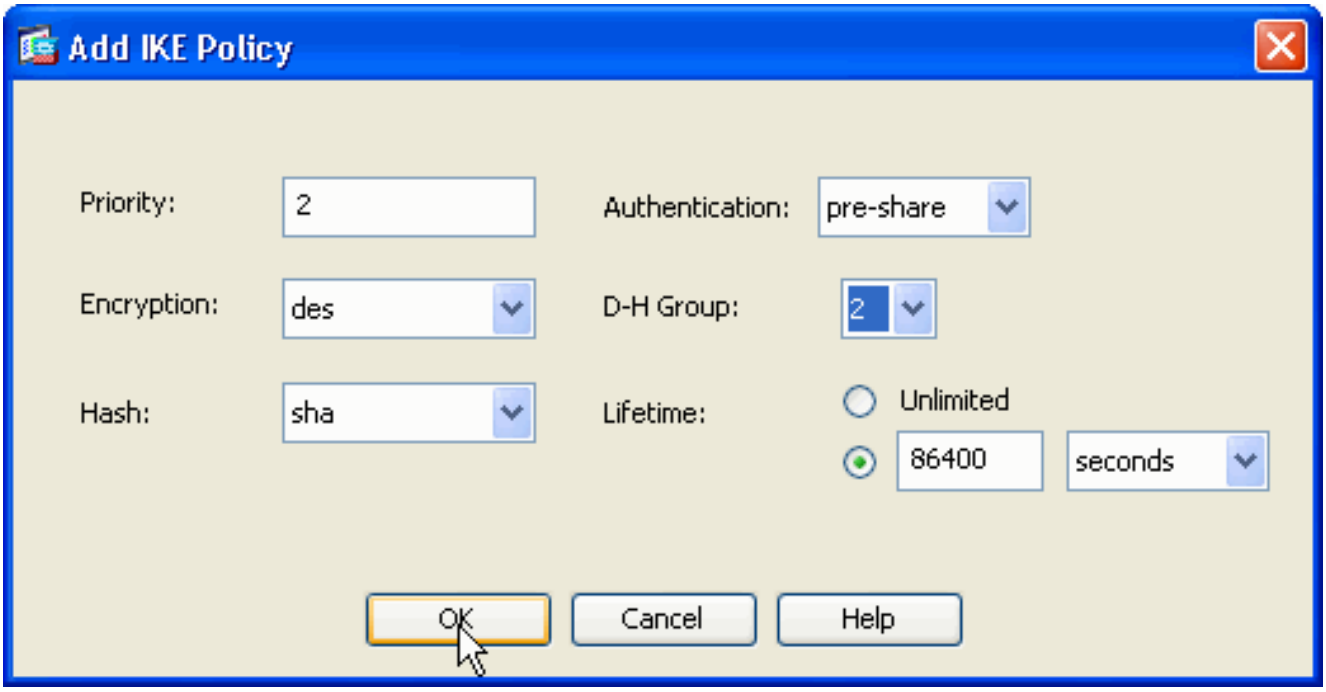
Procedimento ASDM

Termine estas etapas a fim configurar o acesso remoto VPN:

1. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > das políticas de IKE** a fim criar uma política de ISAKMP.

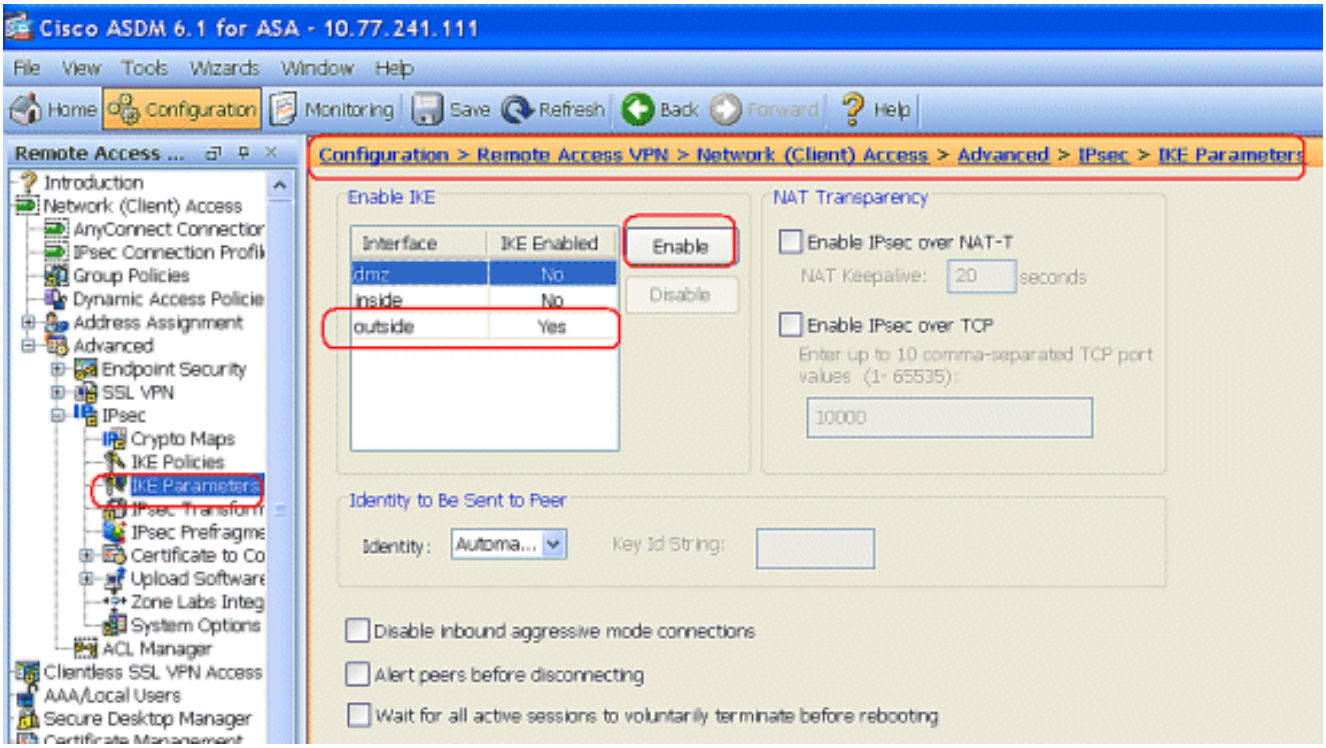


2. Forneça os detalhes da política de ISAKMP.

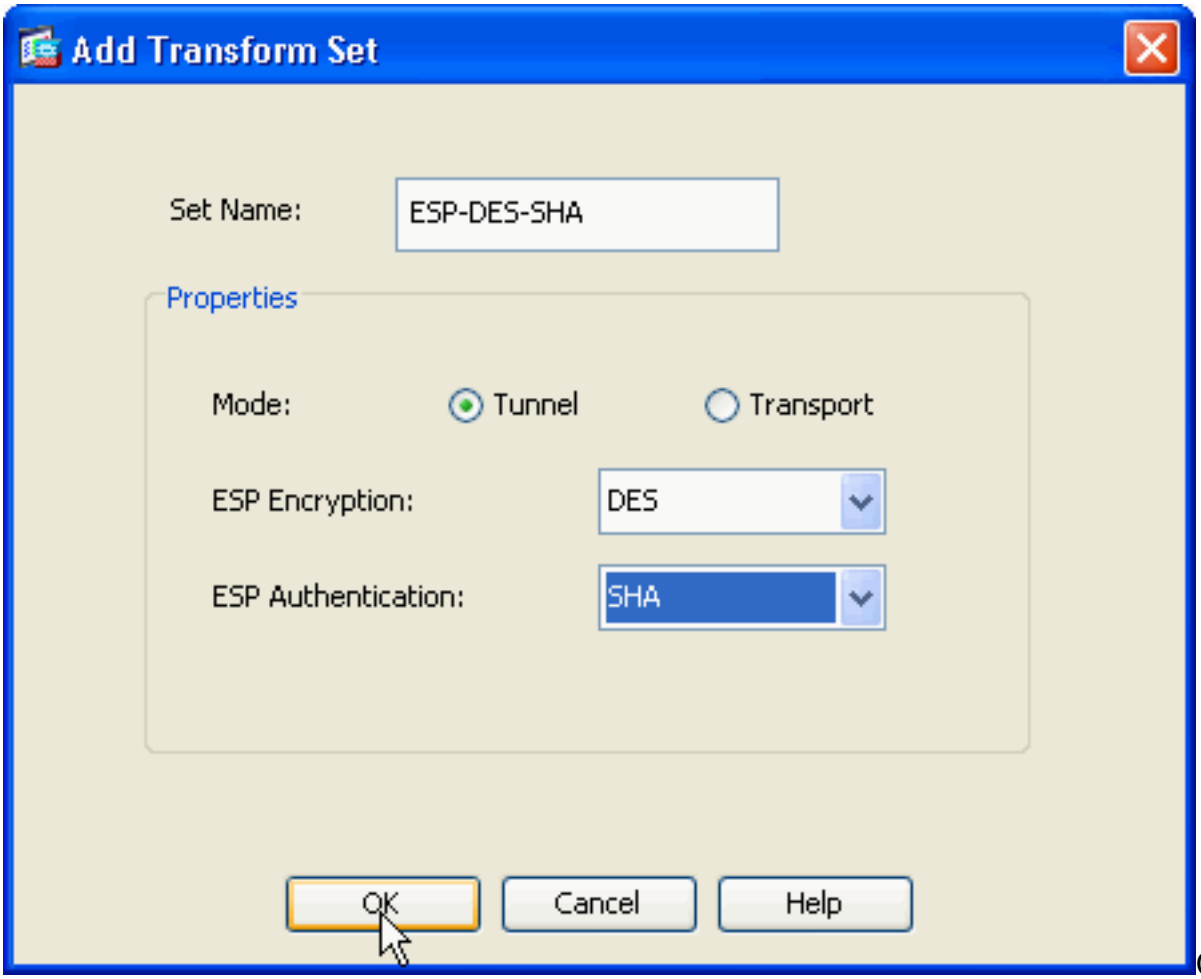


Clique a **APROVAÇÃO** e **aplique-a**.

3. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > parâmetros IKE** para permitir o IKE na interface externa.

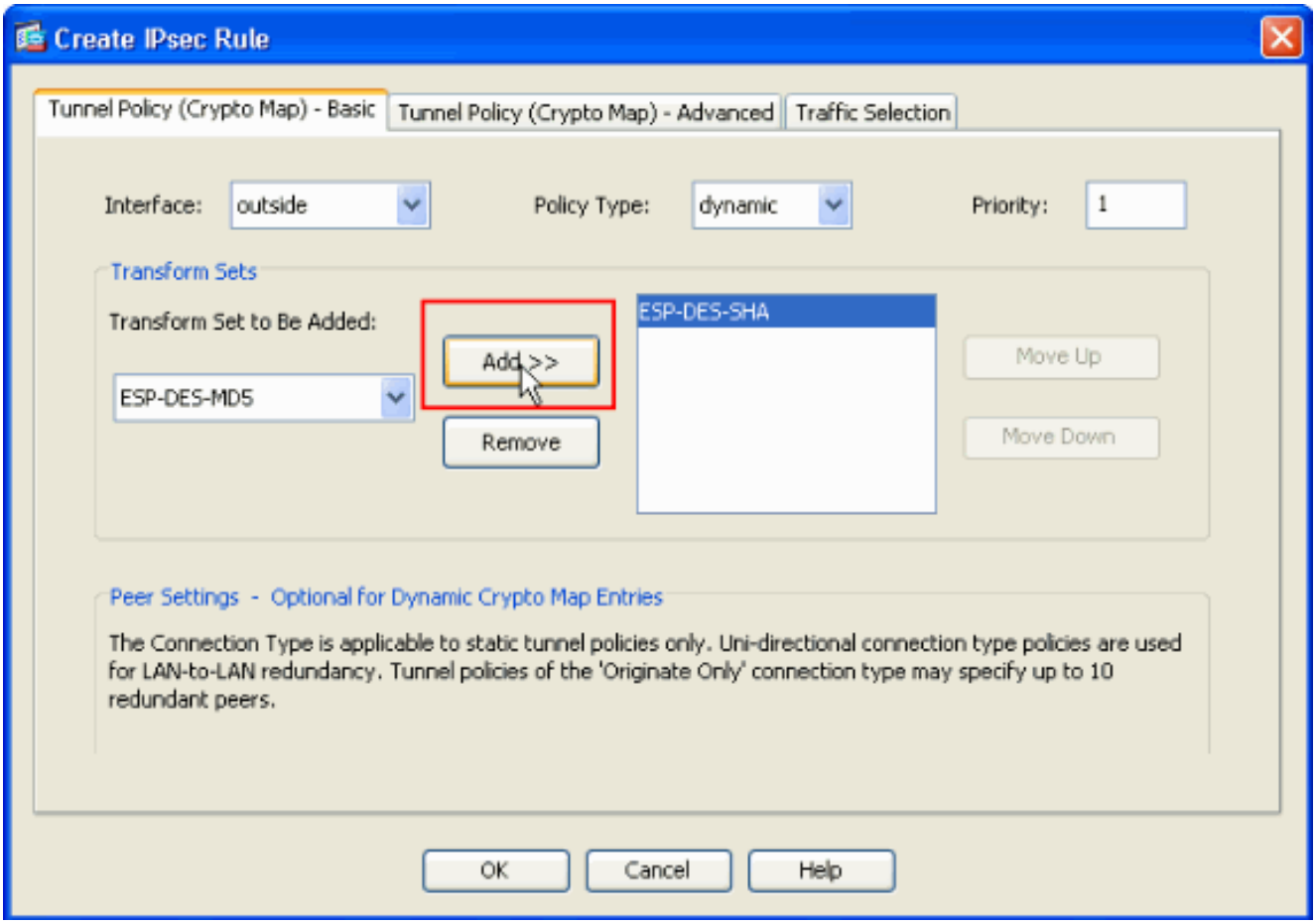


4. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > IPsec transformam o > Add dos grupos** a fim criar o **ESP-DES-SHA** transformam o grupo, como mostrado.



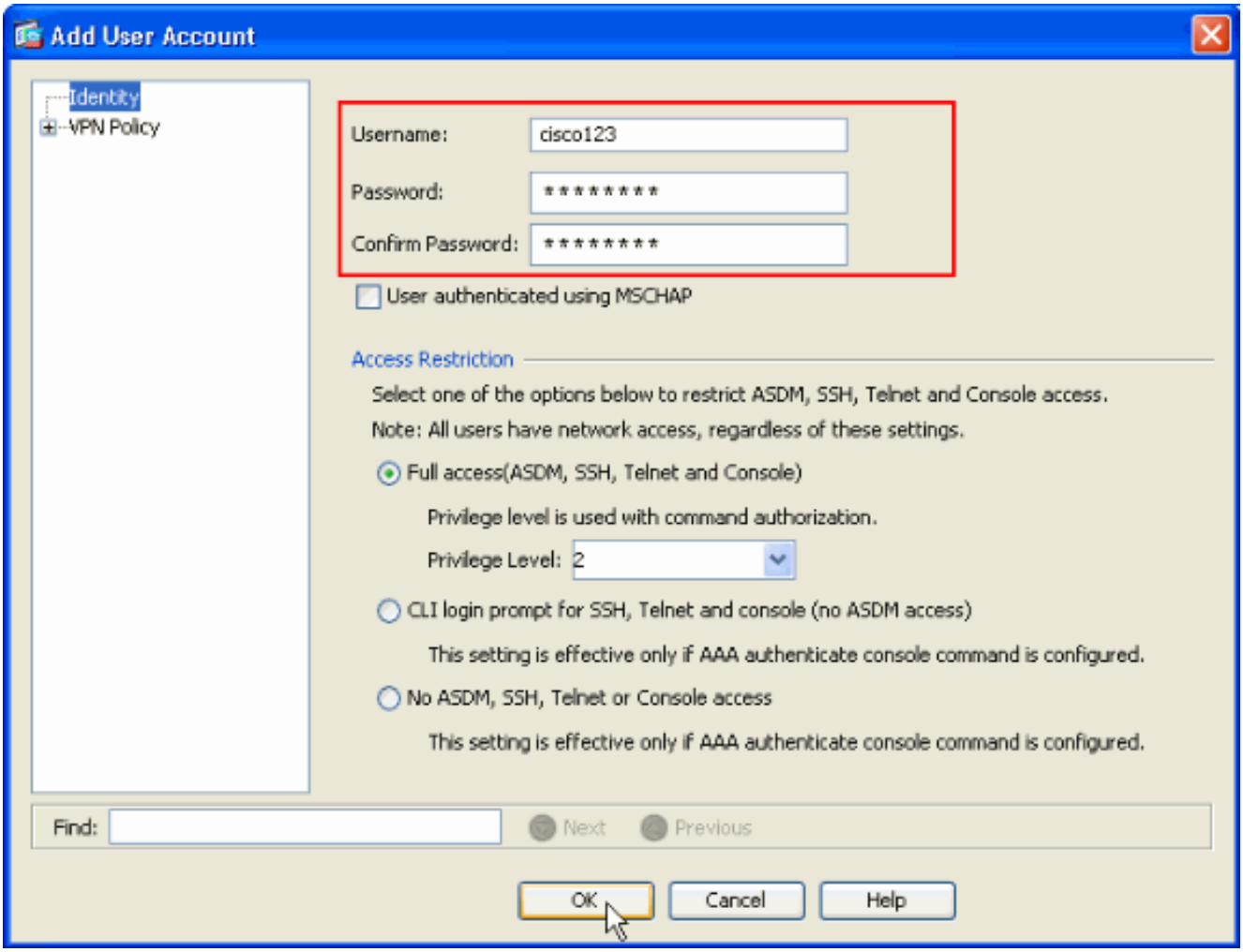
Clique a **APROVAÇÃO** e **aplique-a**.

5. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > dos crypto map** a fim criar um crypto map com a política dinâmica da prioridade 1, como
mostrado.

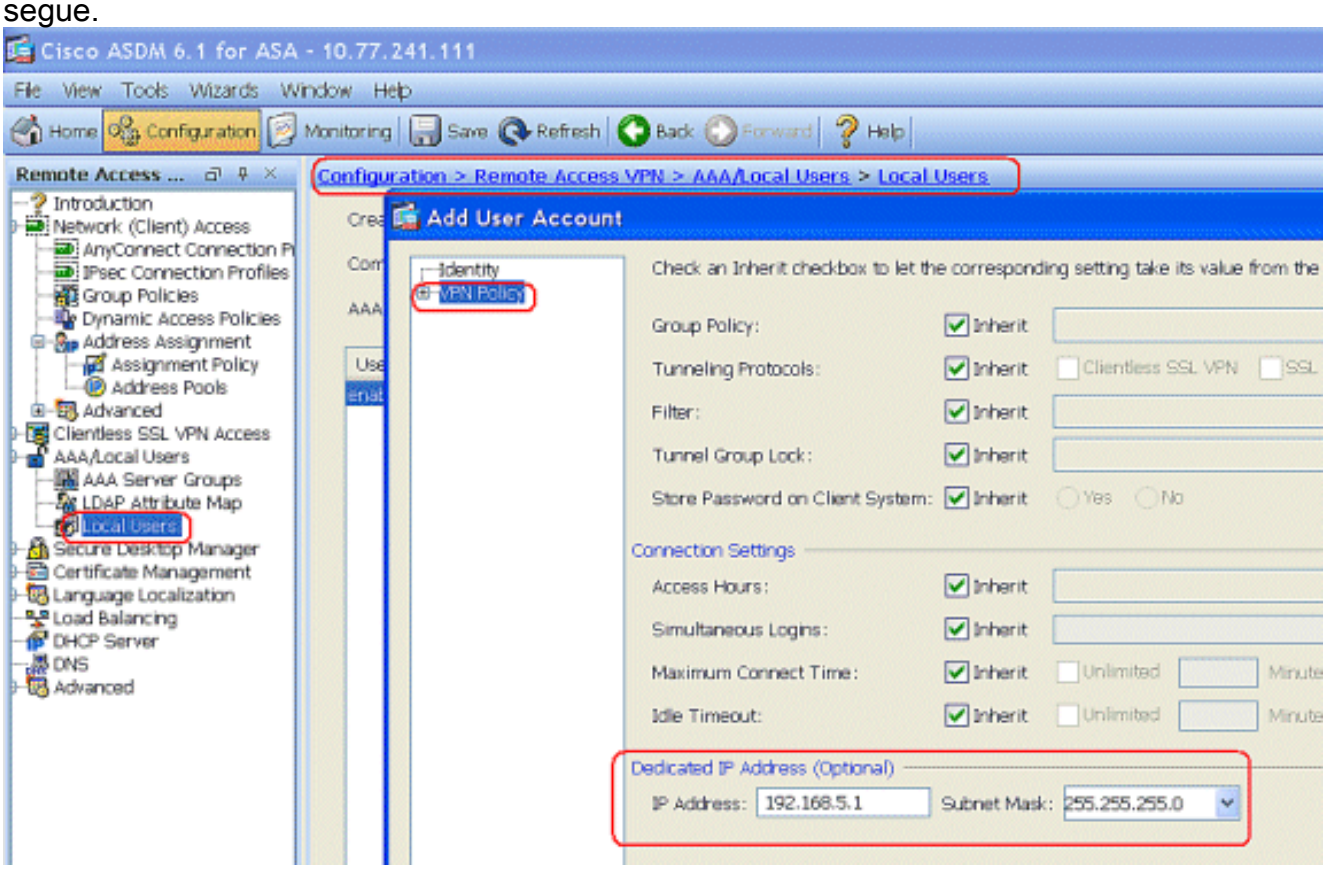


Clique a **APROVAÇÃO** e **aplique-a**.

6. Escolha a **configuração > o acesso remoto VPN > o AAA Setup > > Add dos usuários locais** a fim criar a conta de usuário (por exemplo, username - cisco123 e senha - cisco123) para o acesso de cliente
VPN.

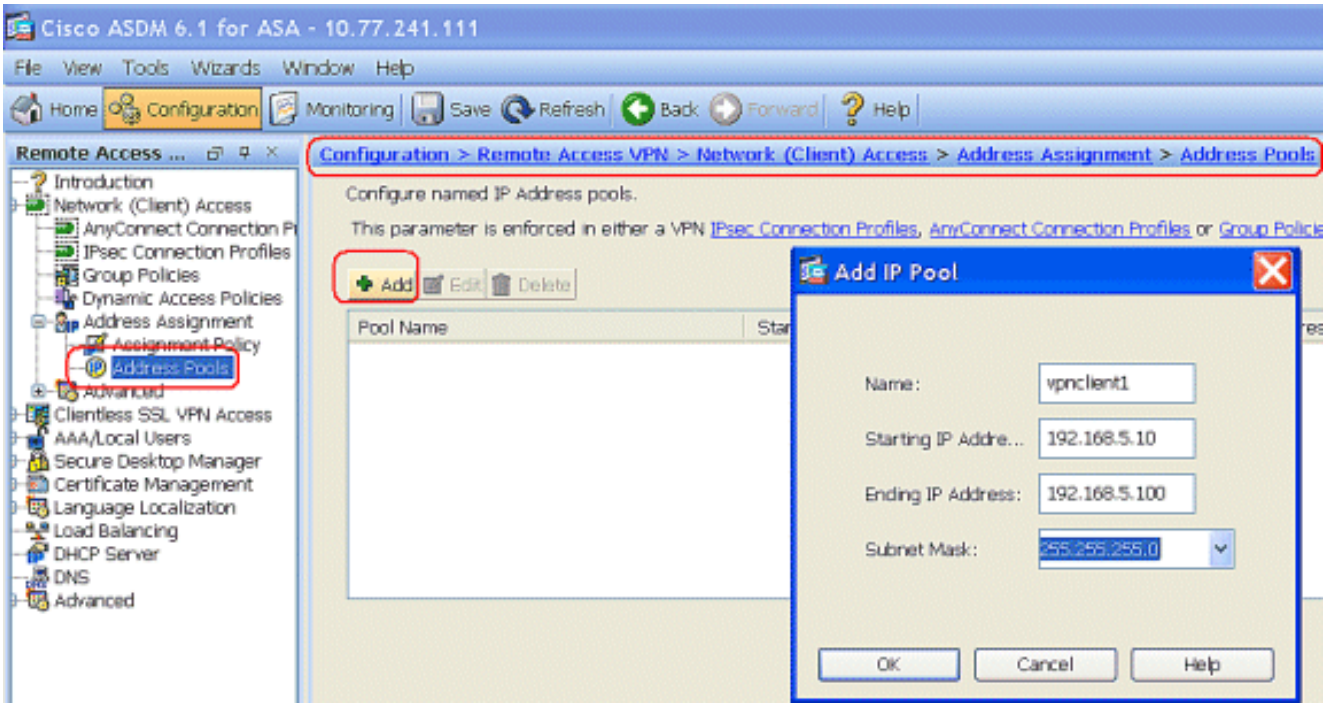


7. Vá à **política de VPN** e adicionar o **estático/dedicou o endereço IP de Um ou Mais Servidores Cisco ICM NT** para o usuário "cisco123," como segue.

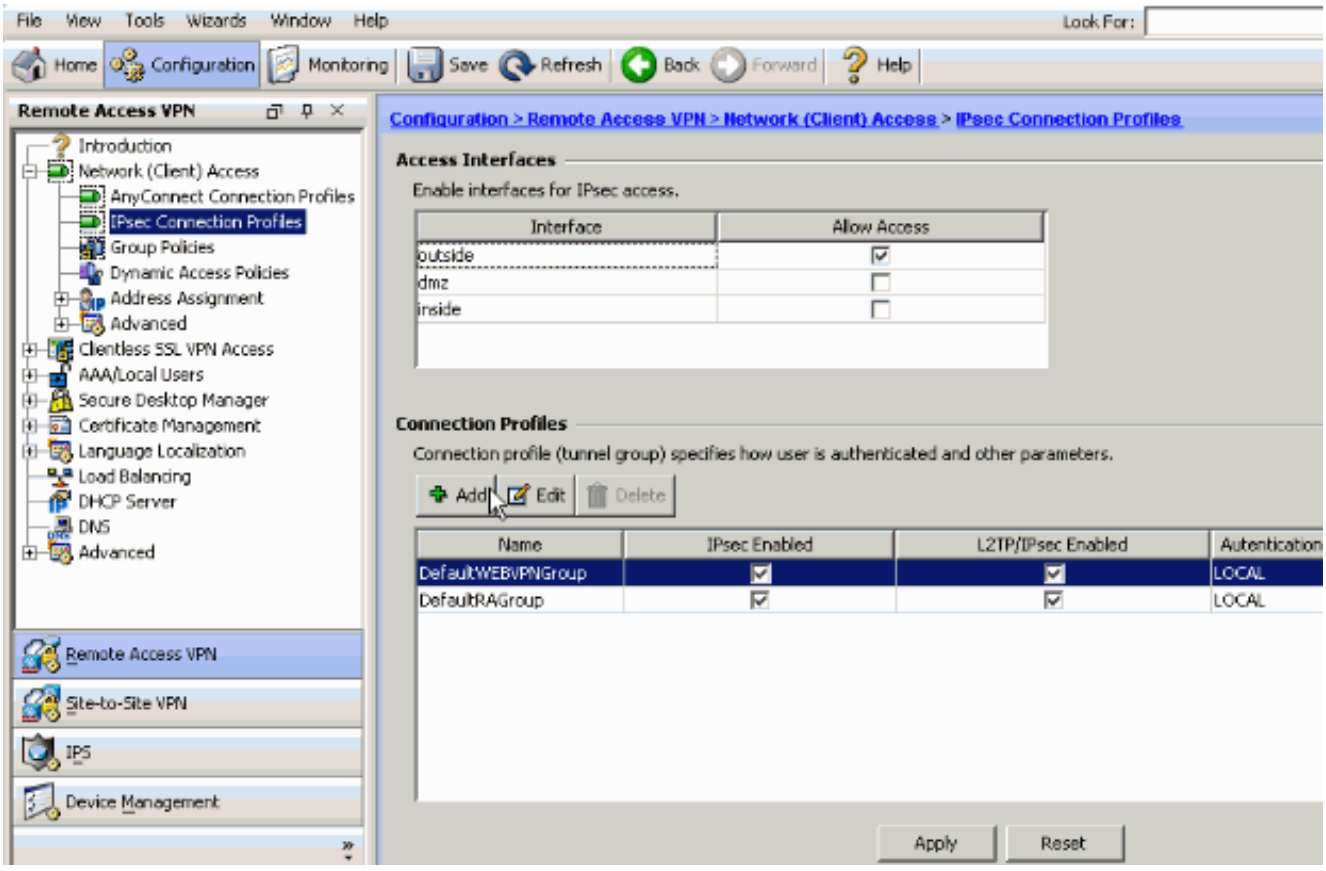


8. Escolha a **configuração > o acesso remoto VPN > o acesso > a atribuição de endereço > os**

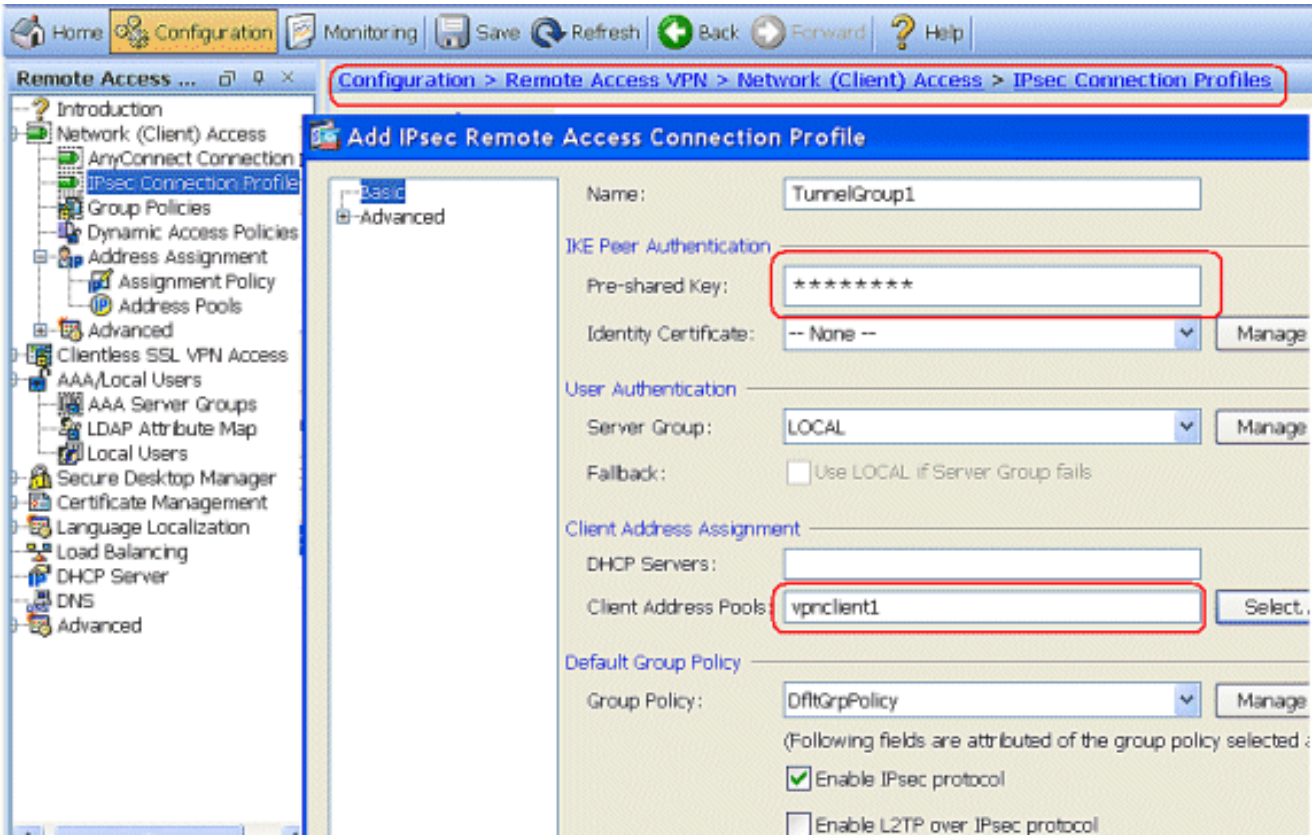
conjuntos de endereços da rede (cliente) e o clique **adiciona** para adicionar o cliente VPN para usuários de cliente
VPN.



9. Escolha a **configuração > o acesso remoto VPN > do acesso > da conexão IPSec da rede (cliente) > Add dos perfis** a fim adicionar um grupo de túneis (por exemplo, TunnelGroup1 e a chave Preshared como o cisco123), como
mostrado.

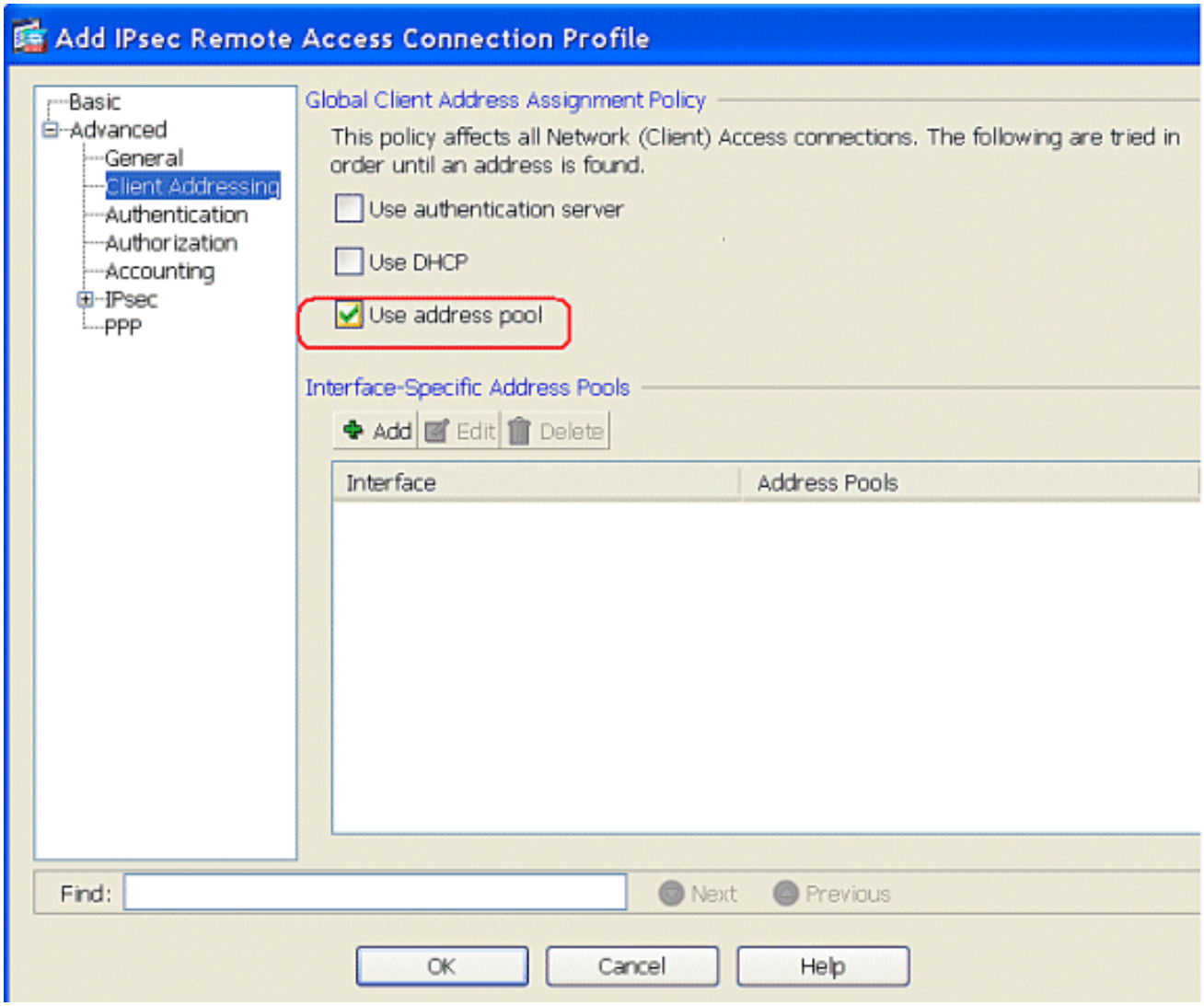


Sob a aba **básica**, escolha o grupo de servidor como o **LOCAL** para o campo da autenticação de usuário.Escolha **vpnclient1** como as associações do endereço de cliente para os usuários de cliente
VPN.



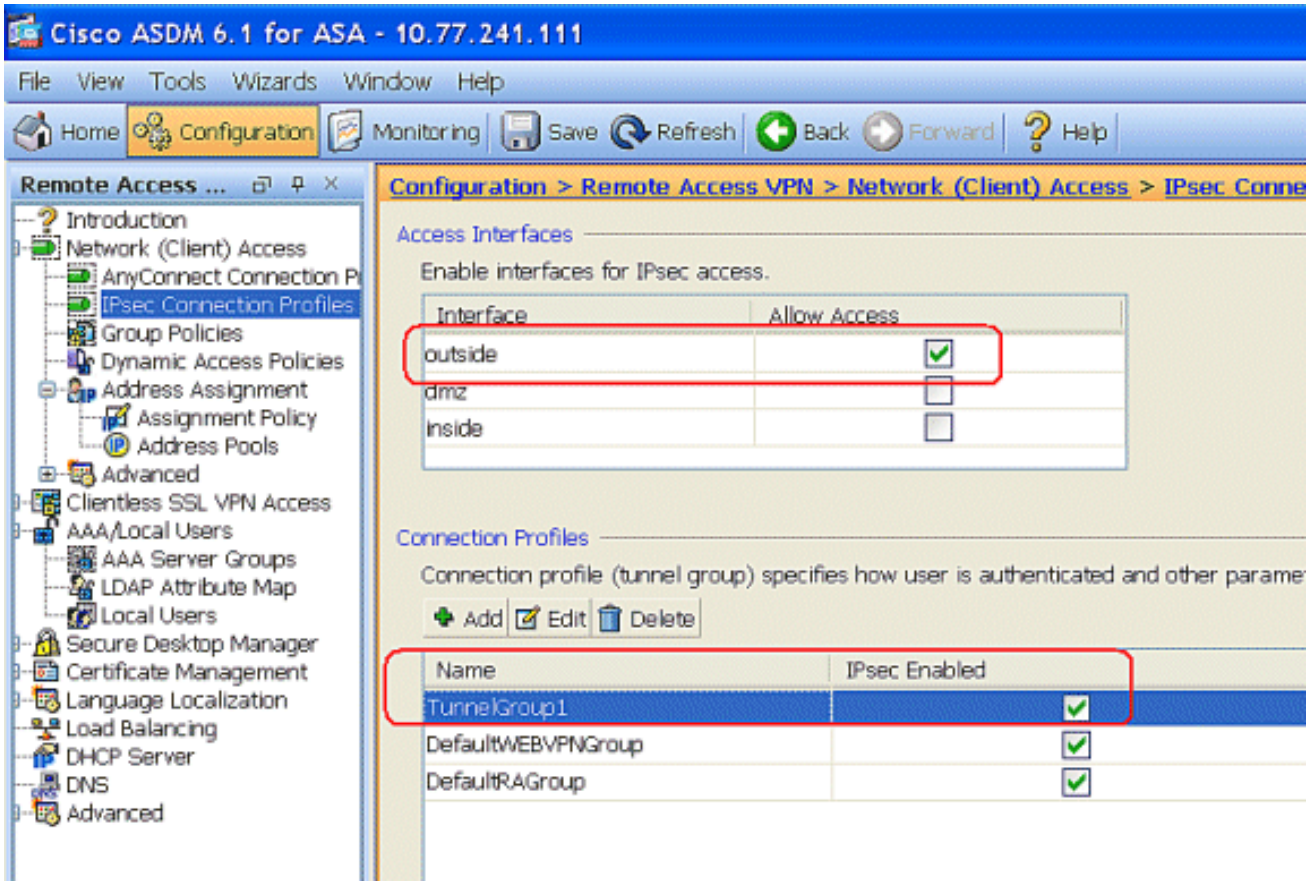
Clique em **OK**.

10. Escolha **avançado > endereçamento do cliente** e verifique a caixa de verificação do **conjunto de endereços do uso** para atribuir o endereço IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN.**Nota:** Certifique-se desmarcar as caixas de seleção para o **Authentication Server do uso** e **usar o DHCP**.



Clique em **OK**.

11. Permita a **interface externa** para o acesso do IPsec. O clique **aplica-se** para continuar.



Configuração do ASA/PIX com a CLI

Termine estas etapas a fim configurar o servidor DHCP para fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN da linha de comando. Refira configurar referências adaptáveis do Dispositivo-comando da Segurança do 5500 Series dos acessos remoto VPN ou do Cisco ASA para obter mais informações sobre de cada comando que é usado.

Configuração running no dispositivo ASA

```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0 no failover icmp unreachable rate-
limit 1 burst-size 1 !--- Specify the location of the
ASDM image for ASA to fetch the image for ASDM access.
asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 global (outside) 1 192.168.1.5 nat
(inside) 0 access-list 101 nat (inside) 1 0.0.0.0
```

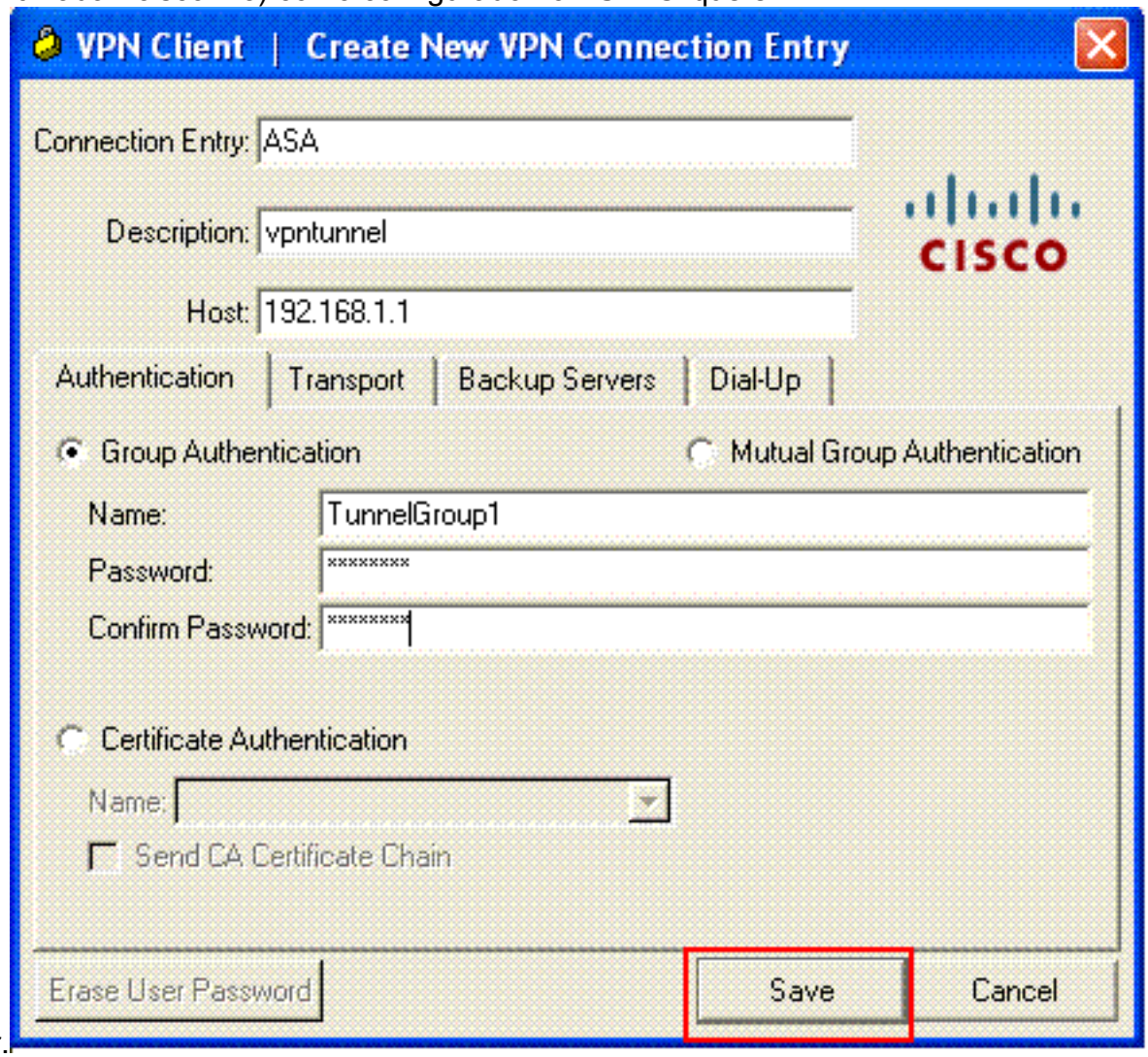
```
0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 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 crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the local and not by AAA or dhcp. The CLI
vpn-addr-assign local for VPN address assignment through
ASA is hidden in the CLI provided by show run command.
no vpn-addr-assign aaa no vpn-addr-assign dhcp 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 ! group-policy DfltGrpPolicy
attributes vpn-tunnel-protocol IPSec webvpn group-policy
GroupPolicy1 internal !--- In order to identify remote
access users to the Security Appliance, !--- you can
also configure usernames and passwords on the device. !-
-- specify the IP address to assign to a particular
user, use the vpn-framed-ip-address command !--- in
username mode username cisco123 password
ffIRPGpDSOJh9YLq encrypted username cisco123 attributes
vpn-framed-ip-address 192.168.5.1 255.255.255.0 !---
Create a new tunnel group and set the connection !---
type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

Configuração de Cisco VPN Client

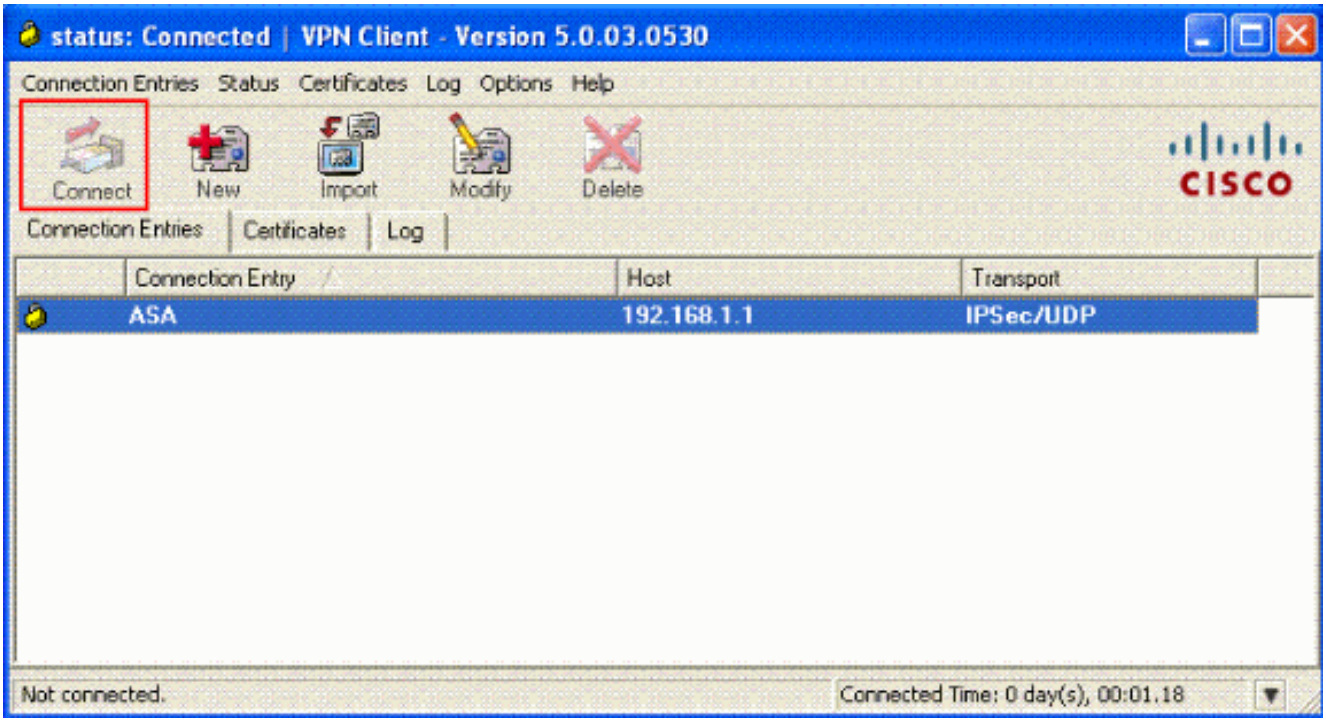
Tente conectar a Cisco ASA com o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN**.
2. Clique **novo** para lançar a janela de entrada nova da conexão de VPN da criação.

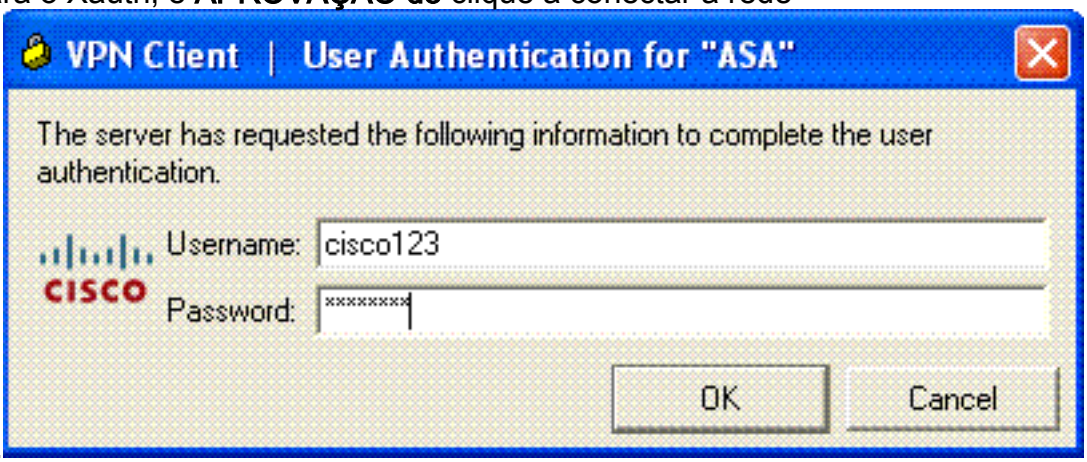
3. Preencha os detalhes de sua nova conexão.Dê entrada com o nome da entrada de conexão junto com uma descrição. Incorpore o **endereço IP externo do ASA à** caixa do host. Incorpore então o nome de grupo de túneis VPN (TunnelGroup1) e a senha (chave pré-compartilhada - cisco123) como configurado no ASA. Clique em Salvar.



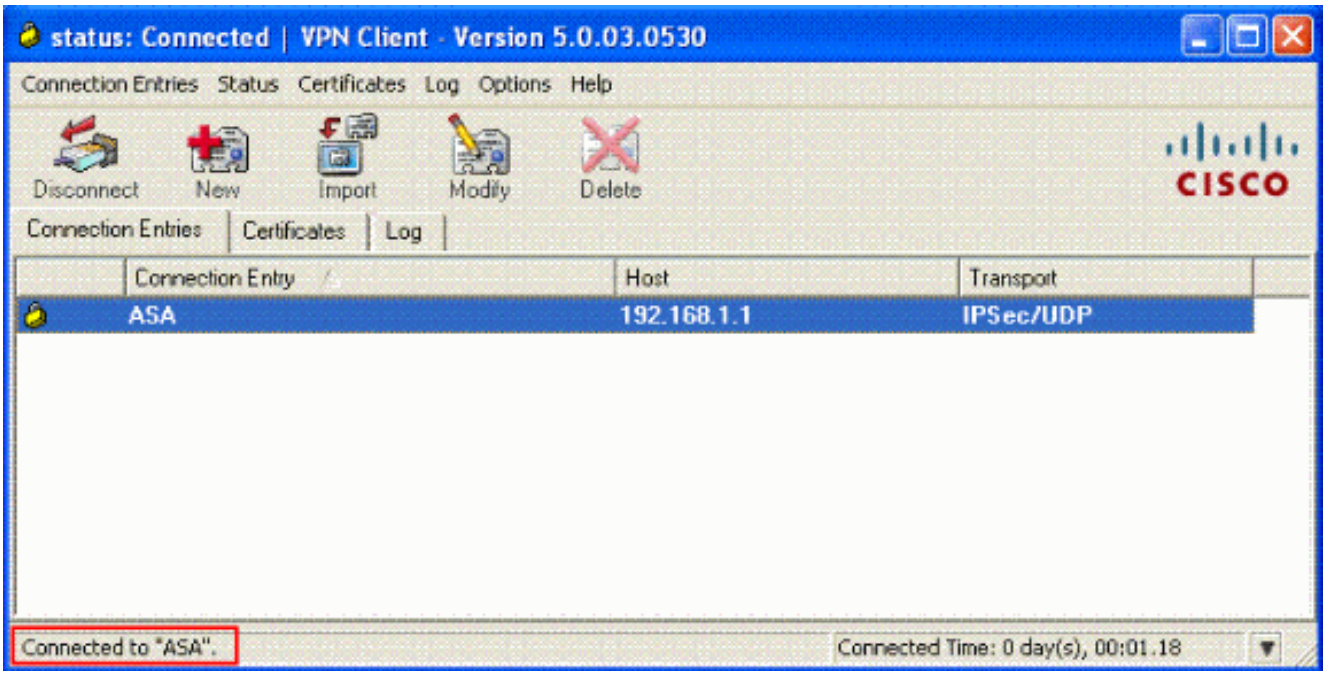
4. Clique a conexão que você quer usar, e o clique **conecta da** janela principal do cliente VPN.



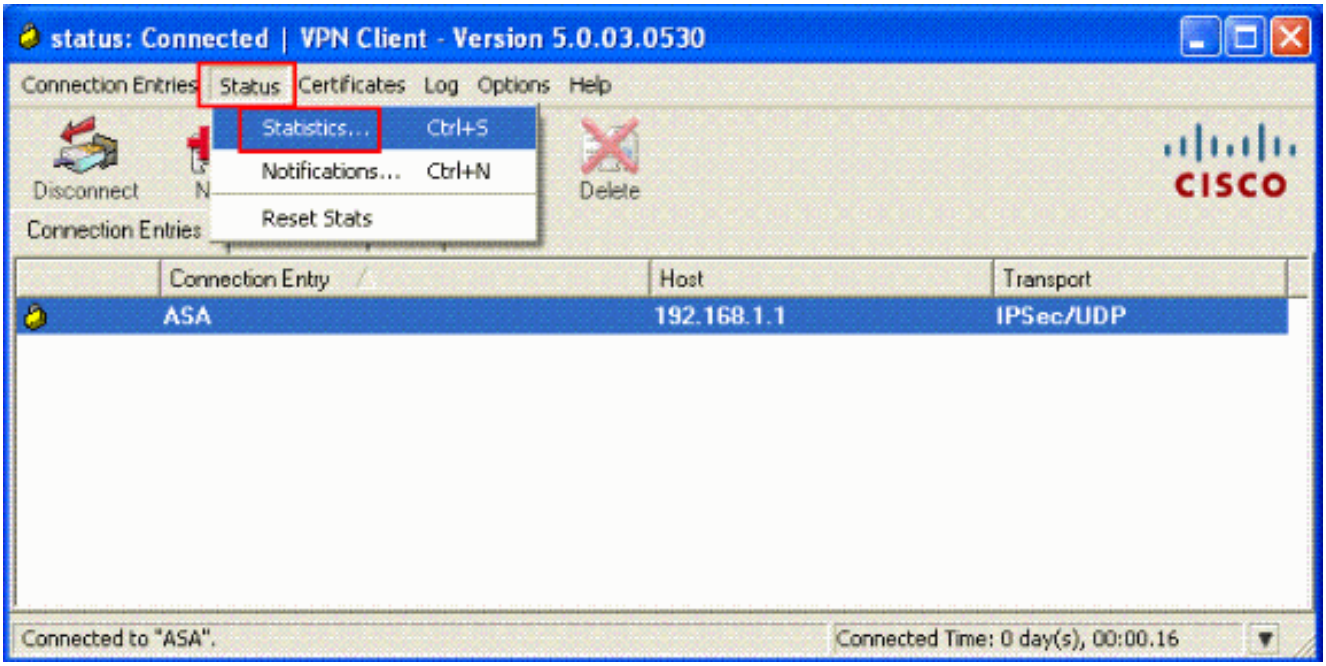
5. Quando alertado, incorpore o **username: cisco123** e **senha: cisco123** como configurado no ASA para o Xauth, e **APROVAÇÃO do** clique a conectar à rede remota.



6. O cliente VPN é conectado com o ASA na instalação central.



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



Verificar

comandos show

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 crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.
- **mostre IPsec cripto sa** — Mostra os ajustes usados por SA atuais.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. O exemplo de debug é mostrado igualmente.

Nota: Para obter mais informações sobre do IPSec VPN do Acesso remoto do Troubleshooting consulte a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções.

Cancele associações de segurança

Quando você pesquisa defeitos, certifique-se cancelar associações de segurança existentes depois que você faz uma mudança. No modo privilegiado do PIX, use estes comandos:

- **clear [crypto] ipsec sa** — Suprime do IPSec ativo SA. As palavras-chave crypto são

opcionais.
- **clear [crypto] isakmp sa** — Suprime do IKE ativo SA. As palavras-chave crypto são opcionais.

Comandos para Troubleshooting

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.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **IPsec 7 do debug crypto** — Indica as negociações de IPSEC de fase 2.
- **isakmp 7 do debug crypto** — Indica as negociações de ISAKMP de fase 1.

Informações Relacionadas

- Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances
- Referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Página de Suporte dos Cisco PIX 500 Series Security Appliances
- Referência de comandos do Dispositivos de segurança Cisco PIX série 500
- Cisco Adaptive Security Device Manager
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Página de Suporte do Cisco VPN Client
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems