

ASA/PIX 8.x: Autorização RADIUS (ACS 4.x) para a utilização do acesso VPN ACL baixável com CLI e exemplo da configuração ASDM

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o acesso remoto VPN \(o IPsec\)](#)

[Configuração do ASA/PIX com a CLI](#)

[Configuração de Cisco VPN Client](#)

[Configurar o ACS para ACL baixável para o usuário individual](#)

[Configurar o ACS para ACL baixável para o grupo](#)

[Configurar ajustes do RADIUS IETF para um grupo de usuário](#)

[Verificar](#)

[Comandos show crypto](#)

[ACL baixável para o usuário/grupo](#)

[ID de filtro ACL](#)

[Troubleshooting](#)

[Cancele associações de segurança](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o mecanismo de segurança para autenticar usuários para o acesso de rede. Já que é possível habilitar autorizações RADIUS implicitamente, esta sessão não contém qualquer informação sobre a configuração da autorização RADIUS no mecanismo de segurança. Ela fornece informações sobre como o mecanismo de segurança lida com as informações da lista de acesso recebidas dos servidores RADIUS.

Você pode configurar um servidor Radius para transferir uma lista de acessos à ferramenta de segurança ou um nome da lista de acessos na altura da autenticação. O usuário é autorizado fazer somente o que é permitido na lista de acessos específica de usuário.

As Listas de acesso carregável são os meios os mais escaláveis quando você usa o Cisco Secure ACS para fornecer as Listas de acesso apropriadas para cada usuário. Para obter mais informações sobre dos recursos de lista de acesso carregável e do Cisco Secure ACS, refira [configurar um servidor Radius para enviar as listas de controle de acesso carregável](#) e [IP carregável ACL](#).

Refira [ASA 8.3 e mais atrasado: Autorização RADIUS \(ACS 5.x\) para a utilização do acesso VPN ACL baixável com CLI e exemplo da configuração ASDM](#) para a configuração idêntica em Cisco ASA com versões 8.3 e mais recente.

[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 do Cisco Adaptive Security Device Manager
- Versão Cliente VPN Cisco 4.x e mais tarde
- Serviço de controle de acesso Cisco Secure 4.x

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](#)

Você pode usar IP carregável ACL para criar grupos de definições de ACL que você pode aplicar a muitos usuários ou grupos de usuário. Estes grupos de definições de ACL são chamados

índices ACL. Também, quando você incorpora NAFs, você controla os índices ACL que são enviados ao cliente de AAA de que um usuário procura o acesso. Isto é, um IP carregável ACL compreende umas ou várias definições do índice ACL, cada qual seja associado com um NAF ou (à revelia) associado a todos os clientes de AAA. O NAF controla a aplicabilidade de índices especificados ACL de acordo com o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA. Para obter mais informações sobre de NAFs e como regulam IP carregável ACL, veja [sobre filtros do acesso de rede](#).

O IP carregável ACL opera esta maneira:

1. Quando o ACS concede um acesso de usuário à rede, o ACS determina se um IP carregável ACL está atribuído a esse usuário ou ao grupo do usuário.
2. Se o ACS encontra um IP carregável ACL que esteja atribuído ao usuário ou ao grupo do usuário, determina se uma entrada do índice ACL está associada com o cliente de AAA que enviou o pedido da autenticação RADIUS.
3. O ACS envia, como parte da sessão do usuário, de um pacote de aceitação acesso do RAIO, de um atributo que especifique o ACL nomeado, e da versão do ACL nomeado.
4. Se o cliente de AAA responde que não tem a versão atual do ACL em seu esconderijo, isto é, o ACL é novo ou mudou, o ACS envia o ACL (novo ou atualizado) ao dispositivo.

O IP carregável ACL é uma alternativa à configuração dos ACL no atributo [26/9/1] do Cisco-av-pair de Cisco do RAIO de cada usuário ou grupo de usuário. Você pode criar um IP carregável ACL uma vez, dá-lhe um nome, e atribui-o então o IP carregável ACL a cada usuário ou grupo de usuário aplicável se você provê seu nome. Este método é mais eficiente do que se você configura o atributo do Cisco-av-pair de Cisco do RAIO para cada usuário ou grupo de usuário.

Mais, quando você emprega NAFs, você pode aplicar índices diferentes ACL ao mesmo usuário ou grupo de usuários com respeito ao cliente de AAA que usam. Nenhuma configuração adicional do cliente de AAA é necessária depois que você configurou o cliente de AAA para usar IP carregável ACL do ACS. Os ACL carregável são protegidos pelo regime do backup ou da replicação que você estabeleceu.

Quando você incorpora as definições de ACL à interface da WEB ACS, não use a palavra-chave ou as entradas de nome; em todos respeitos restantes, sintaxe e semântica padrão de comando `acl` do uso para o cliente de AAA em que você pretende aplicar o IP carregável ACL. As definições de ACL que você incorpora no ACS compreendem uns ou vários comandos `acl`. Cada comando `acl` deve estar em uma linha separada.

Você pode adicionar uns ou vários índices do ACL nomeado a um IP carregável ACL. À revelia, cada índice ACL aplica-se a todos os clientes de AAA, mas, se você definiu NAFs, você pode limitar a aplicabilidade de cada índice ACL aos clientes de AAA que são alistados no NAF que você lhe associa. Isto é, quando você emprega NAFs, você pode fazer cada índice ACL, dentro de um único IP carregável ACL, aplicável aos dispositivos de rede ou aos grupos de dispositivo de rede diferentes múltiplos de acordo com sua estratégia da segurança de rede.

Também, você pode mudar a ordem dos índices ACL em um IP carregável ACL. O ACS examina os índices ACL, partindo da parte superior da tabela, e transfere o primeiro índice ACL que encontra com um NAF que inclui o cliente de AAA que é usado. Quando você ajusta a ordem, você pode assegurar a eficiência de sistema se você posiciona o mais extensamente os índices aplicáveis ACL mais altamente sobre a lista. Você deve realizar que, se seu NAFs inclui populações dos clientes de AAA que sobrepõem, você deve continuar do mais específico ao mais geral. Por exemplo, o ACS transfere todos os índices ACL com o ajuste NAF dos Todo-AAA-clientes e não considera alguns que forem mais baixos na lista.

A fim usar um IP carregável ACL em um cliente de AAA particular, o cliente de AAA deve seguir estes sentidos:

- Use o RADIUS de autenticação
- Apoie IP carregável ACL

Estes são exemplos dos dispositivos Cisco que apoiam IP carregável ACL:

- ASA e dispositivos de PIX
- VPN 3000 series concentrators
- Dispositivos Cisco que executam a Versão do IOS 12.3(8)T ou mais tarde

Este é um exemplo do formato que você deve usar para incorporar VPN 3000/ASA/PIX 7.x+ ACL à caixa das definições de ACL:

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

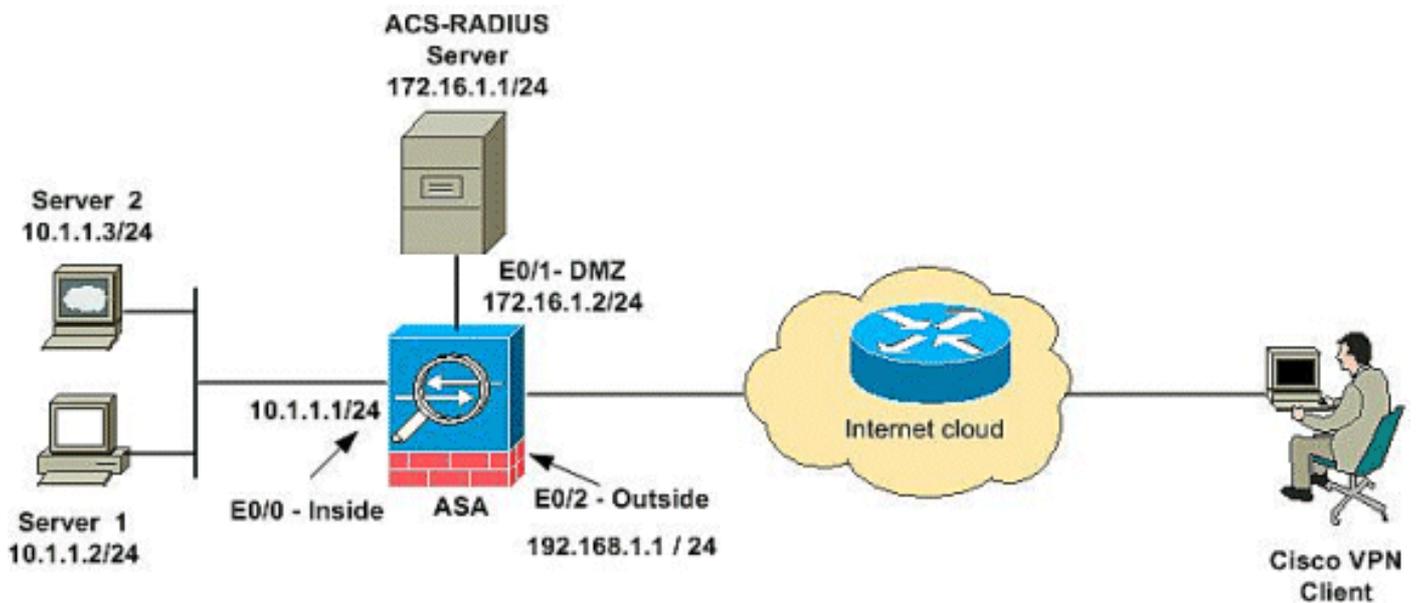
[Configurar](#)

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:



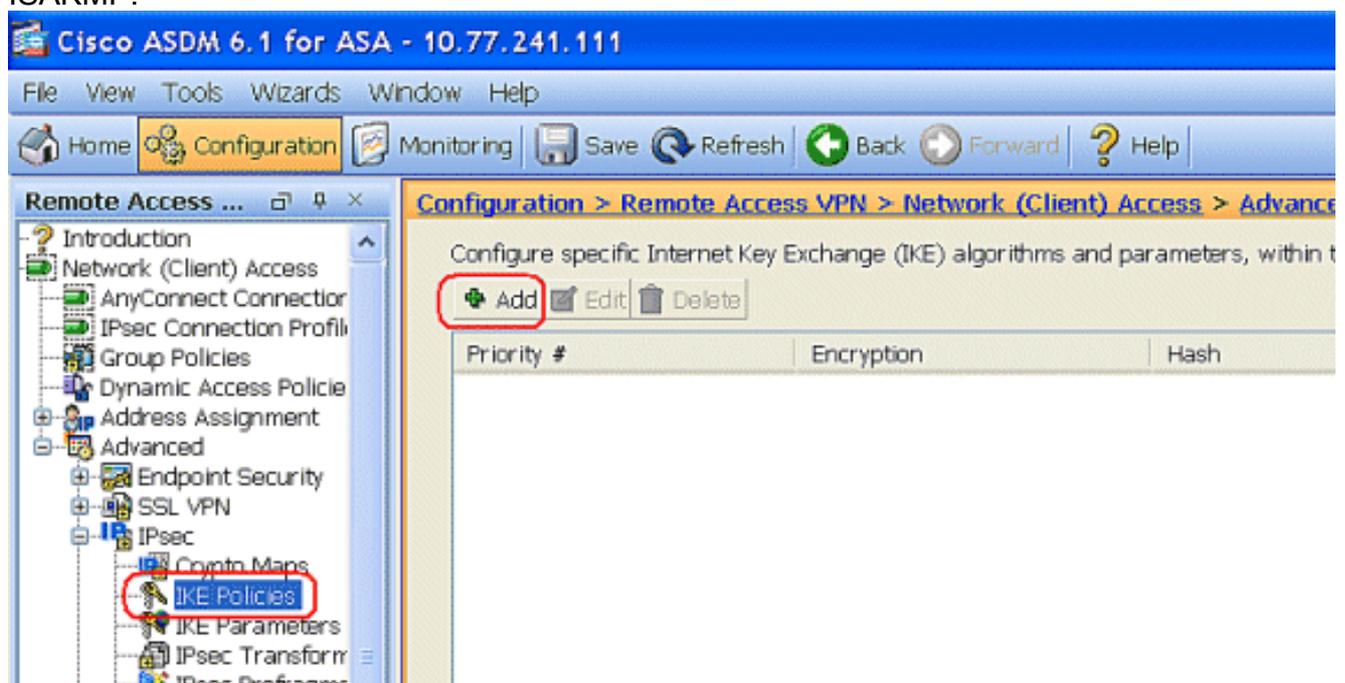
Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

[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 > IPsec > IKE Polícies> adicionam a fim criar uma política de ISAKMP.**

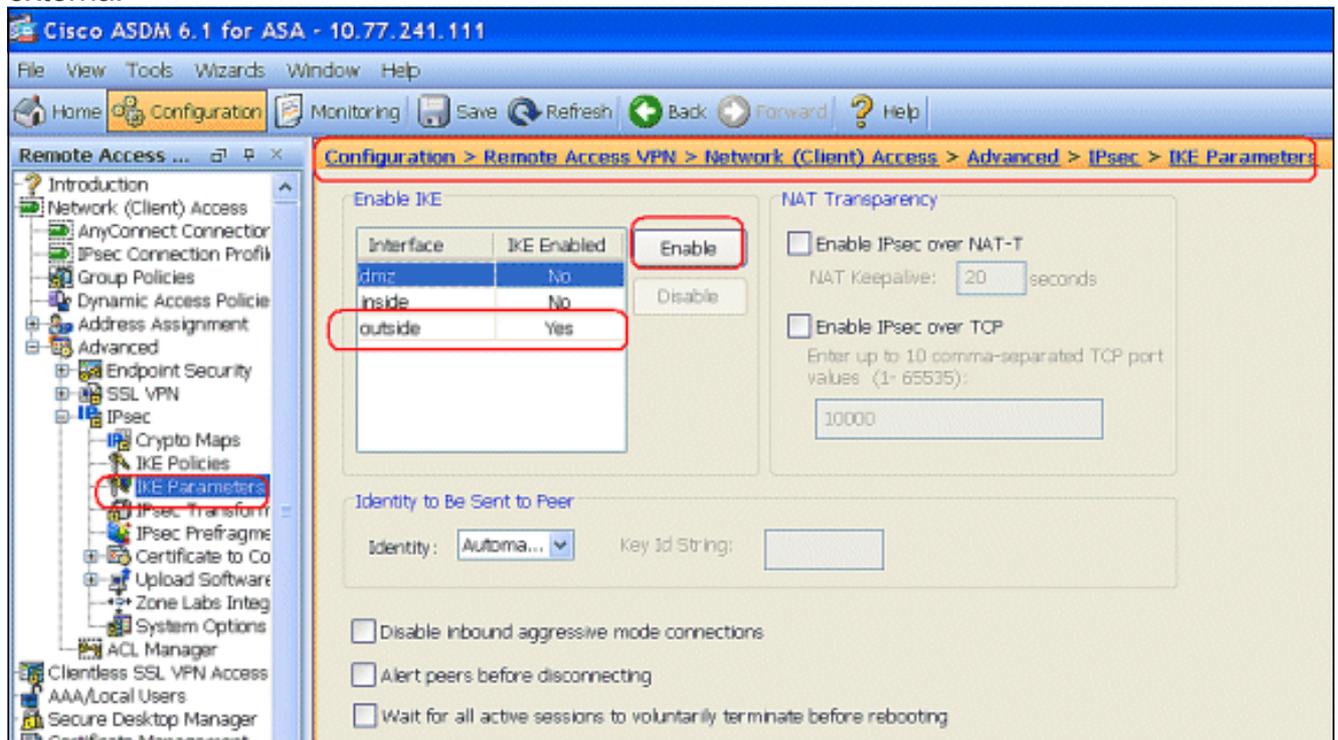


2. Forneça os detalhes da política de ISAKMP como mostrado.



Clique a **APROVAÇÃO** e aplique-a.

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



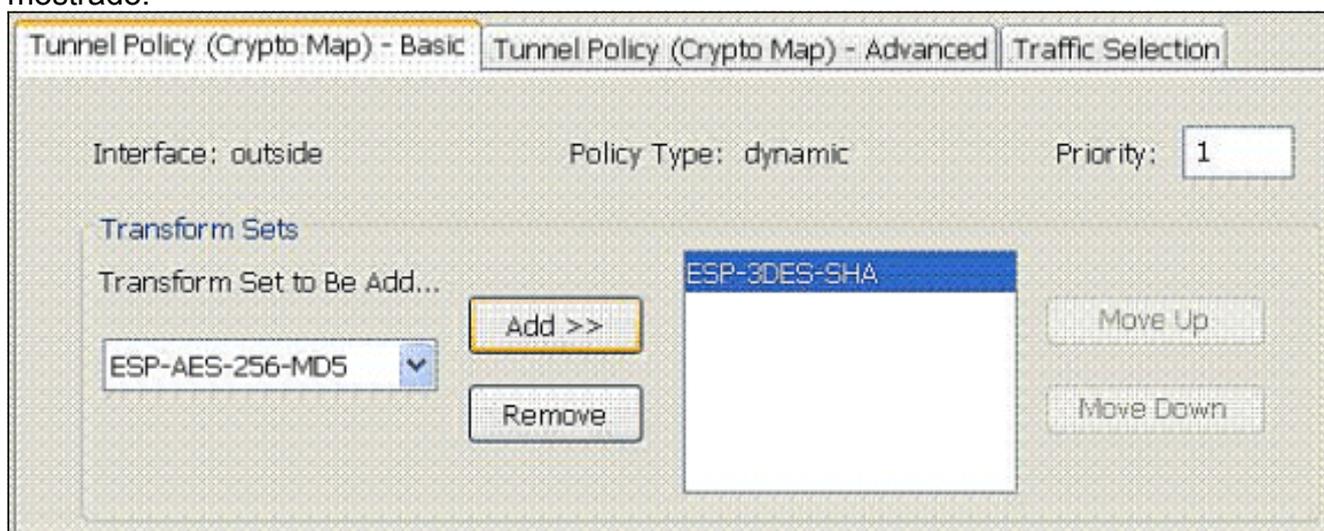
- Escolha a configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > IPsec transformam o > Add dos grupos a fim criar o ESP-3DES-SHA transformam o grupo, como mostrado.



Clique a

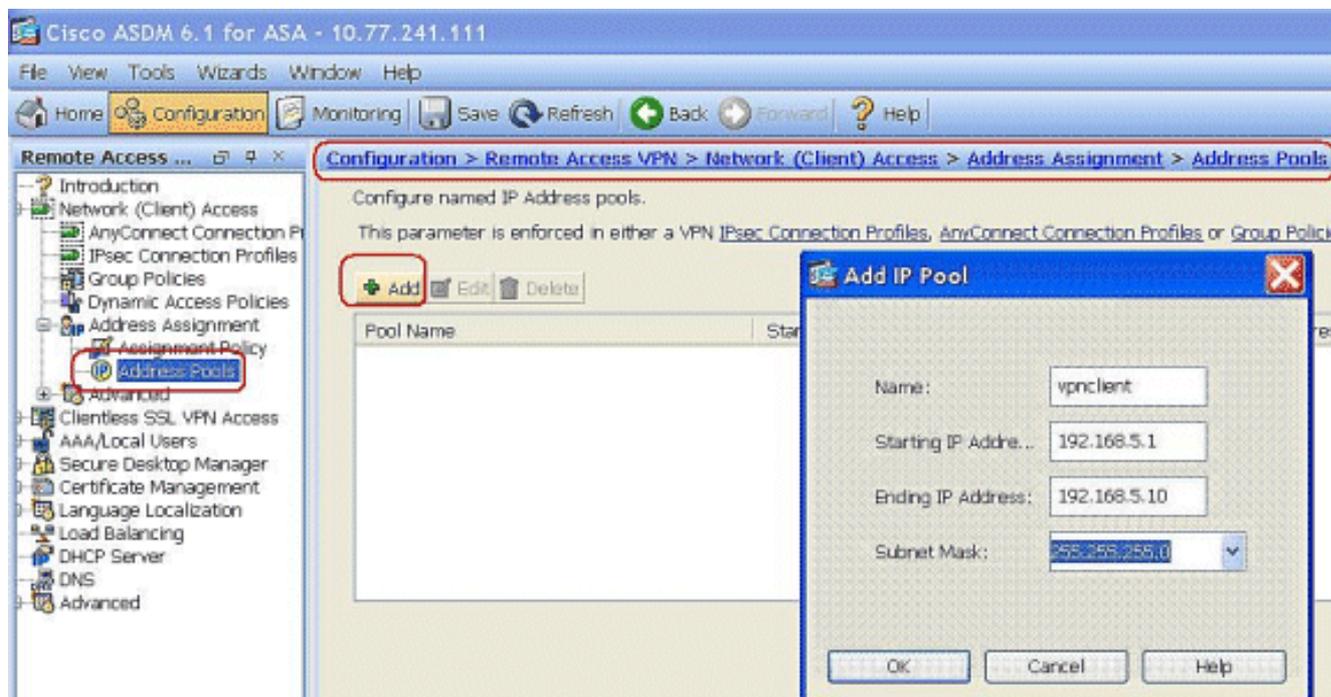
APROVAÇÃO e aplique-a.

- 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.

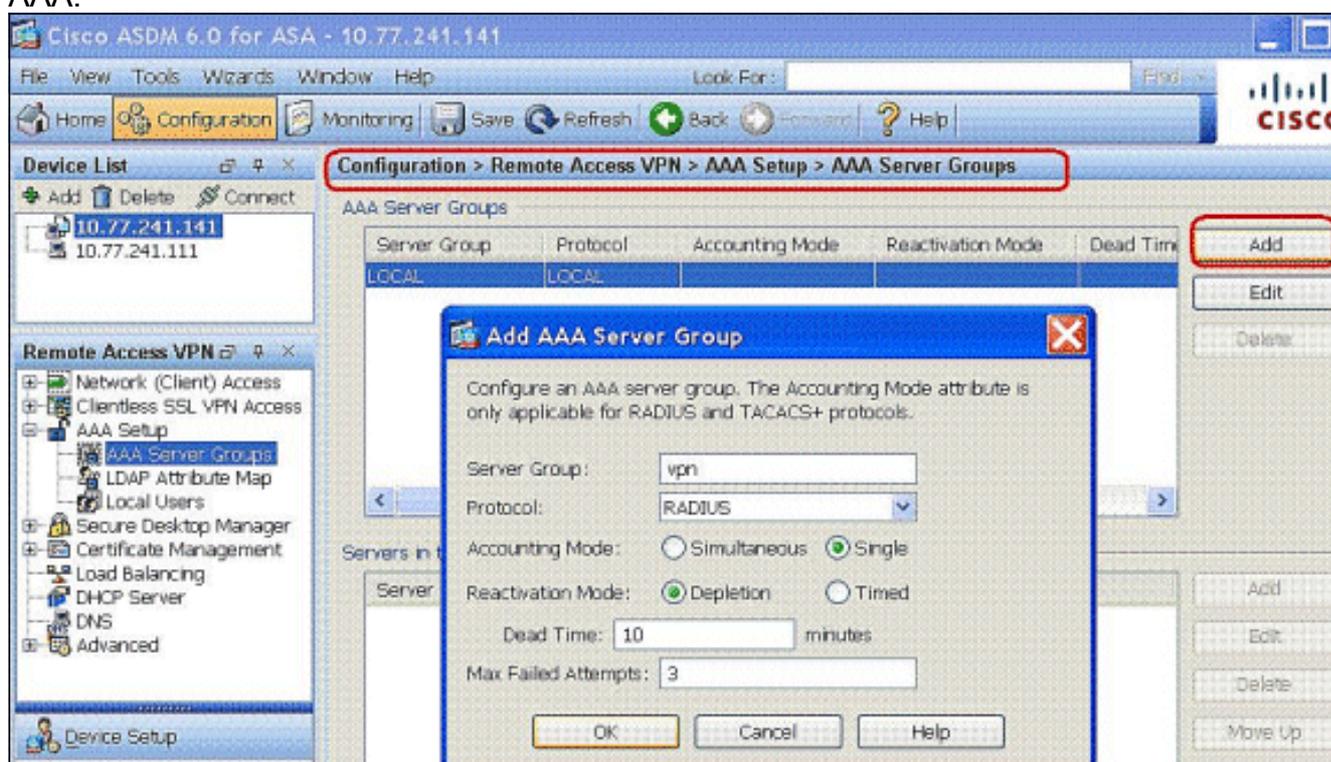


Clique a **APROVAÇÃO** e aplique-a.

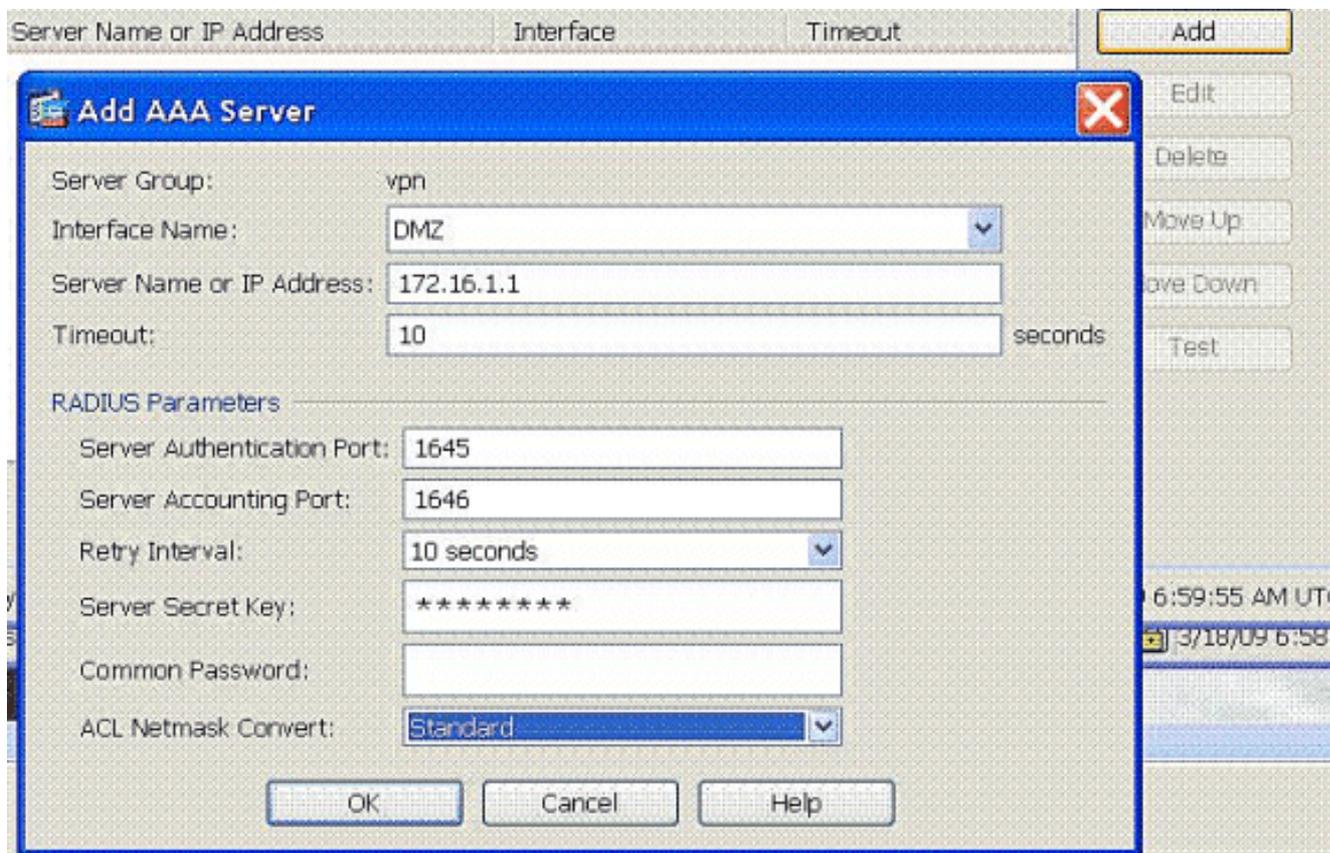
- Escolha a **configuração > o acesso remoto VPN > o acesso > a atribuição de endereço > os conjuntos de endereços da rede (cliente)** e o clique **adiciona** para adicionar o cliente VPN para os usuários de cliente VPN.



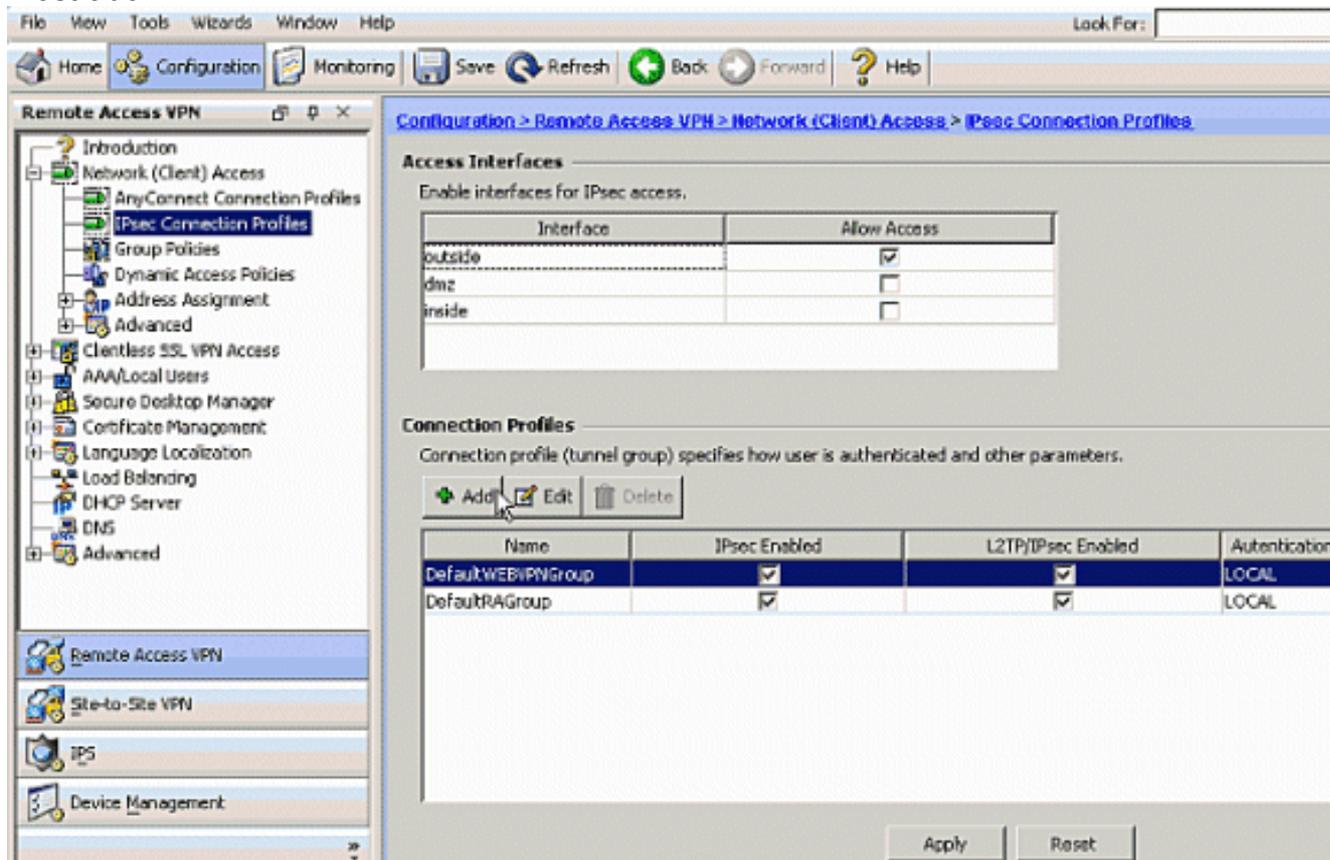
7. Escolha a configuração > o acesso remoto VPN > o AAA Setup > Grupos de servidores AAA e o clique adiciona para adicionar o nome e o protocolo de Grupo de servidores AAA.



Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor AAA (ACS) e a relação que conecta. Igualmente adicionar a chave do segredo de servidor na área de parâmetros radius. Clique em OK.

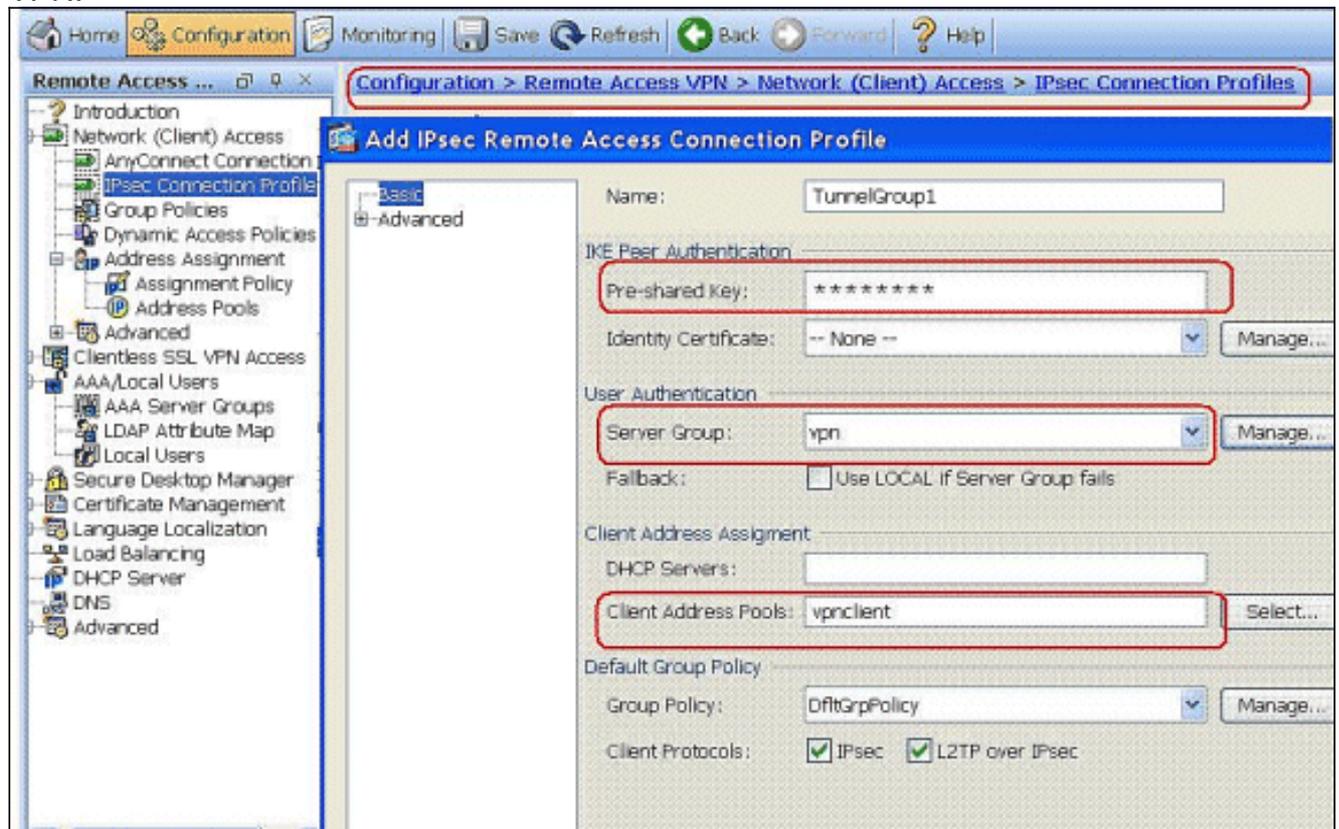


8. Escolha a configuração > o acesso remoto VPN > do acesso > da conexão IPsec da rede (cliente) > Add dos perfis a fim adicionar um grupo de túneis, por exemplo, TunnelGroup1 e a chave Preshared como o cisco123, como mostrado.



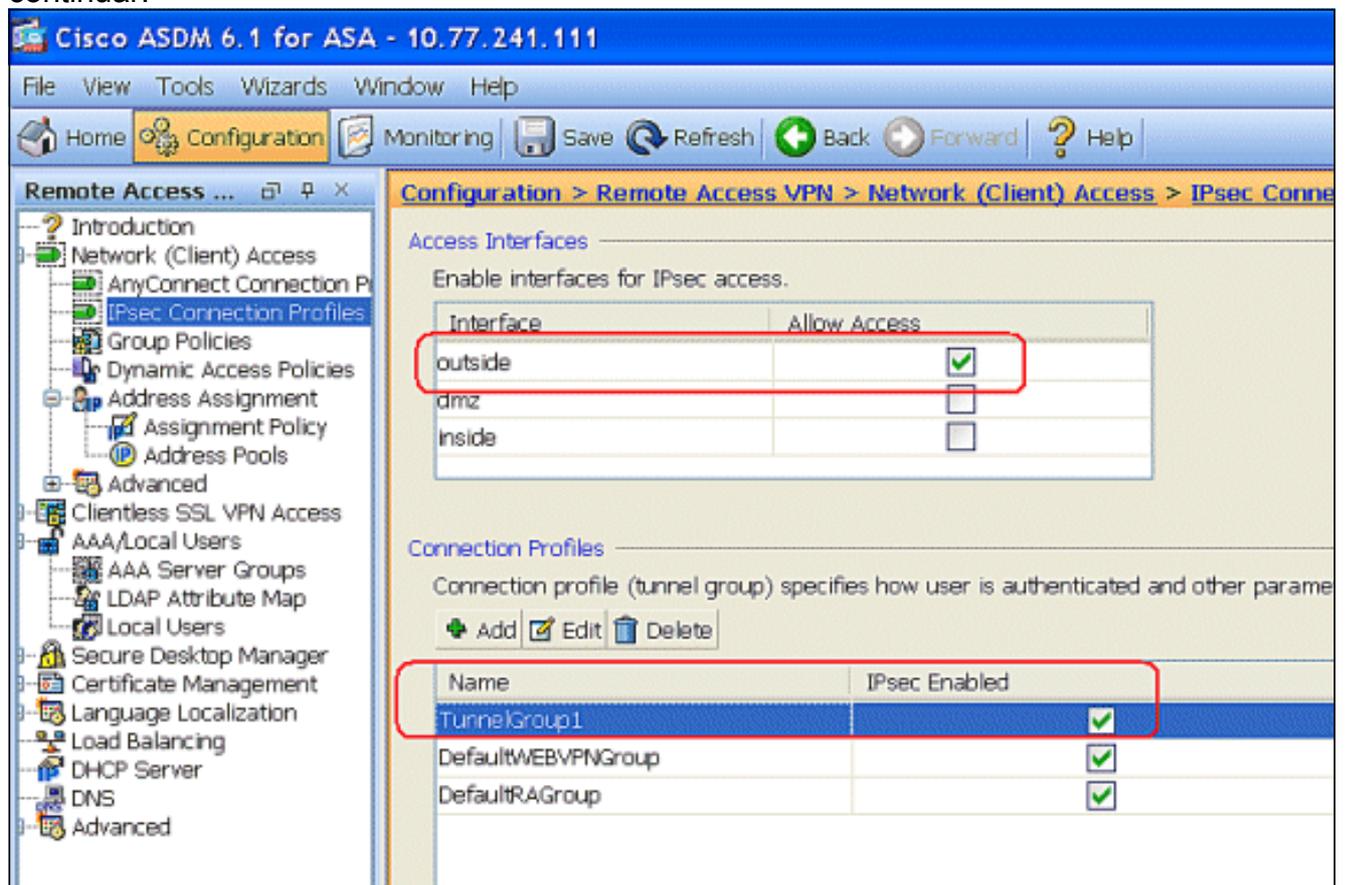
Sob a aba básica, escolha o grupo de servidor como o **vpn** para o campo da autenticação de usuário. Escolha **vpncient** como as associações do endereço de cliente para os usuários de cliente

VPN.



Clique em OK.

9. 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 DMZ security-level 100 ip
address 172.16.1.2 255.255.255.0 ! interface Ethernet0/2
nameif outside security-level 0 ip address 192.168.1.1
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 !---
Radius Attribute Filter access-list new extended deny ip
any host 10.1.1.2 access-list new extended permit ip any
any pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.1-192.168.5.10
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
(outside) 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 !---
Create the AAA server group "vpn" and specify the
protocol as RADIUS. !--- Specify the CSACS server as a
member of the "vpn" group and provide the !--- location
and key. aaa-server vpn protocol radius max-failed-
attempts 5 aaa-server vpn (DMZ) host 172.16.1.1 retry-
interval 1 timeout 30 key cisco123 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 !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. !--- A Triple DES encryption with !---
the sha hash algorithm is used. crypto ipsec transform-
set ESP-3DES-SHA esp-3des esp-sha-hmac !--- Defines a
dynamic crypto map with !--- the specified encryption
settings. crypto dynamic-map outside_dyn_map 1 set
transform-set ESP-3DES-SHA !--- Binds the dynamic map to
the IPsec/ISAKMP process. 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
```

```

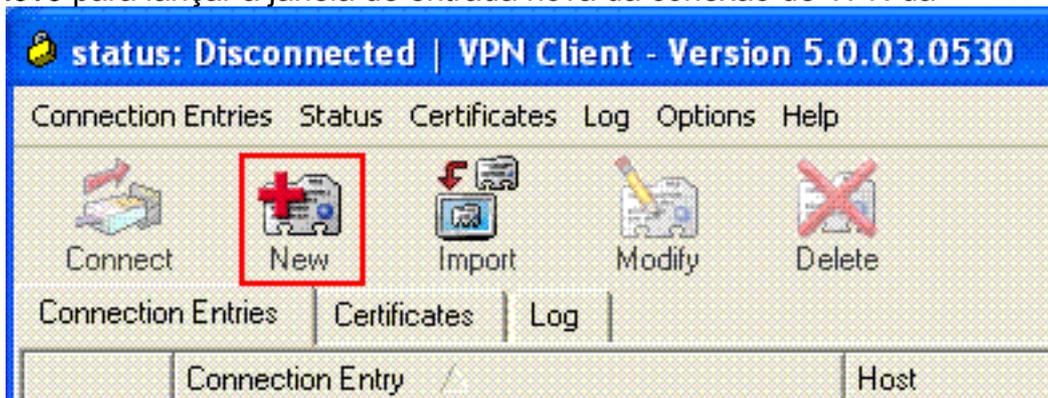
configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 2 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 no
crypto isakmp nat-traversal telnet timeout 5 ssh timeout
5 console timeout 0 threat-detection 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
esmtip 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
!--- Associate the vpnclient pool to the tunnel group
using the address pool. !--- Associate the AAA server
group (VPN) with the tunnel group. tunnel-group
TunnelGroup1 type remote-access tunnel-group
TunnelGroup1 general-attributes address-pool vpnclient
authentication-server-group vpn !--- 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

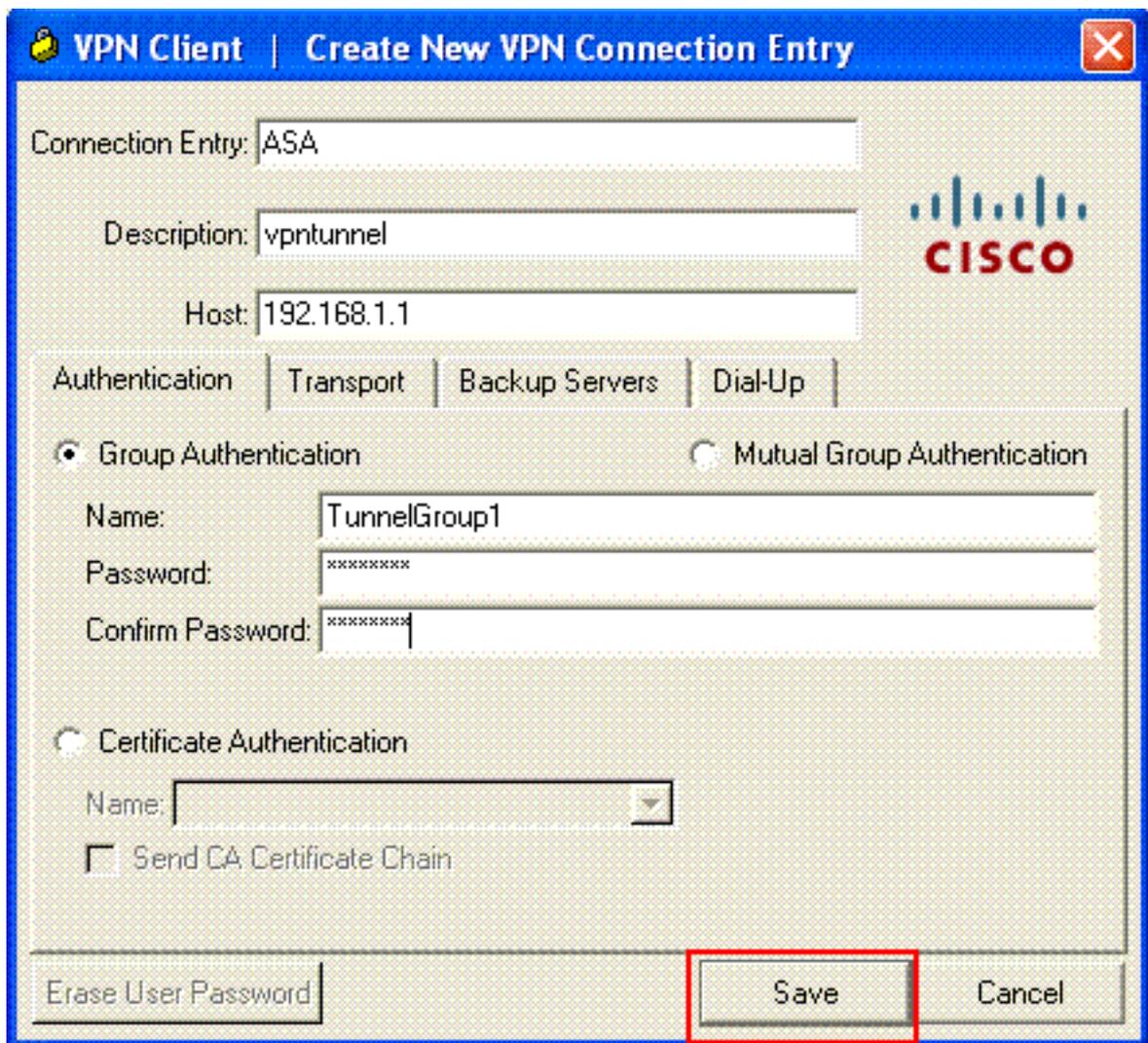
Tente conectar a Cisco ASA com o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

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



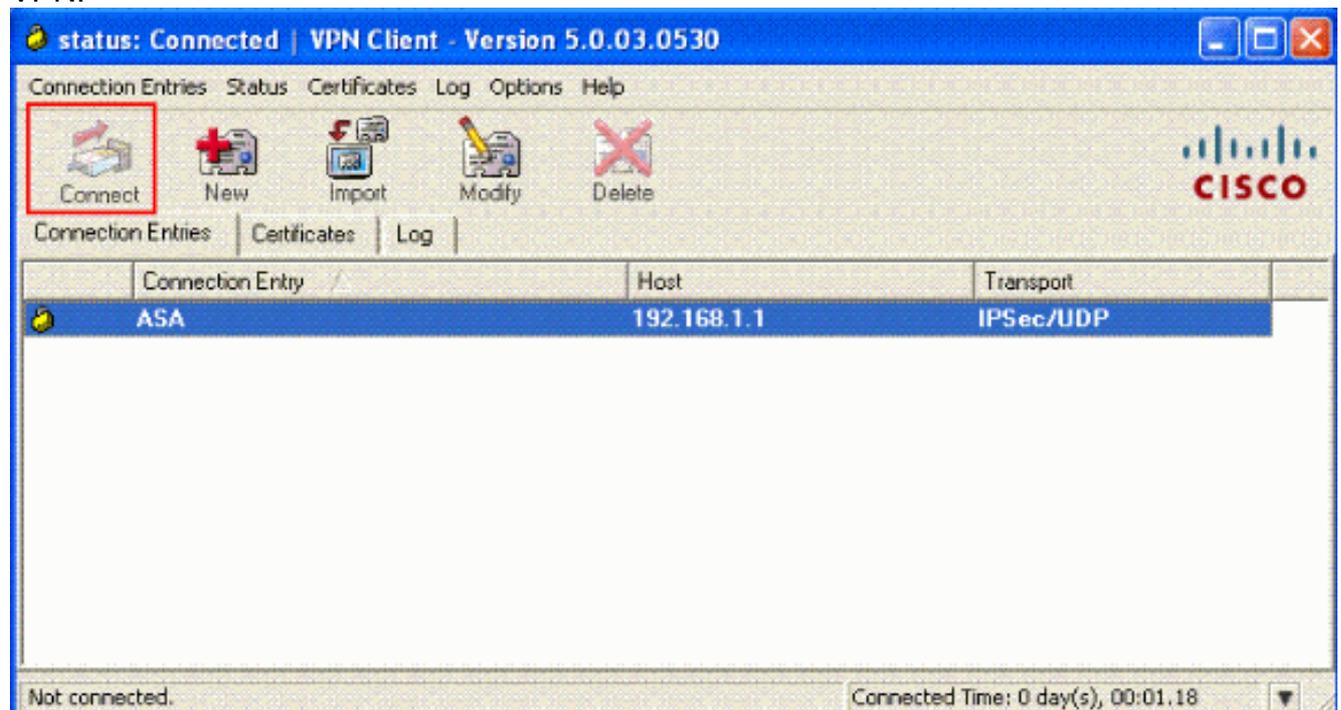
criação.

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

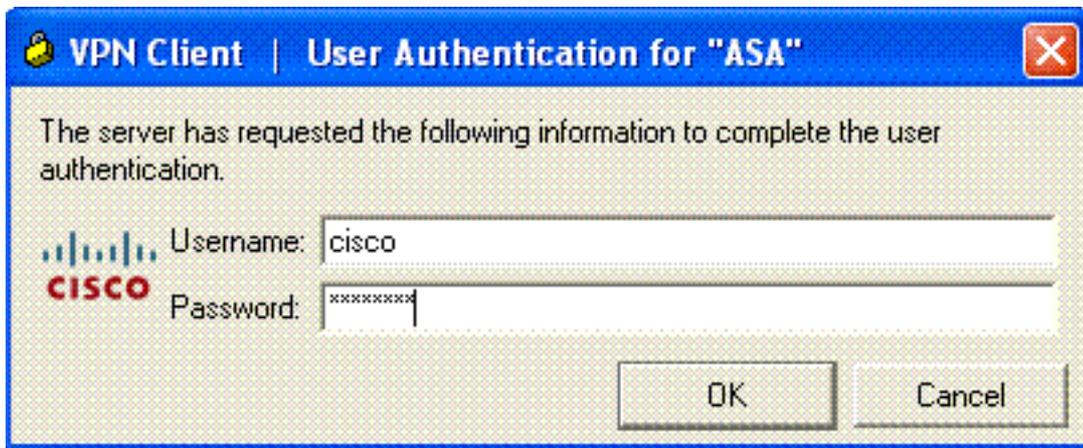


Salvar.

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

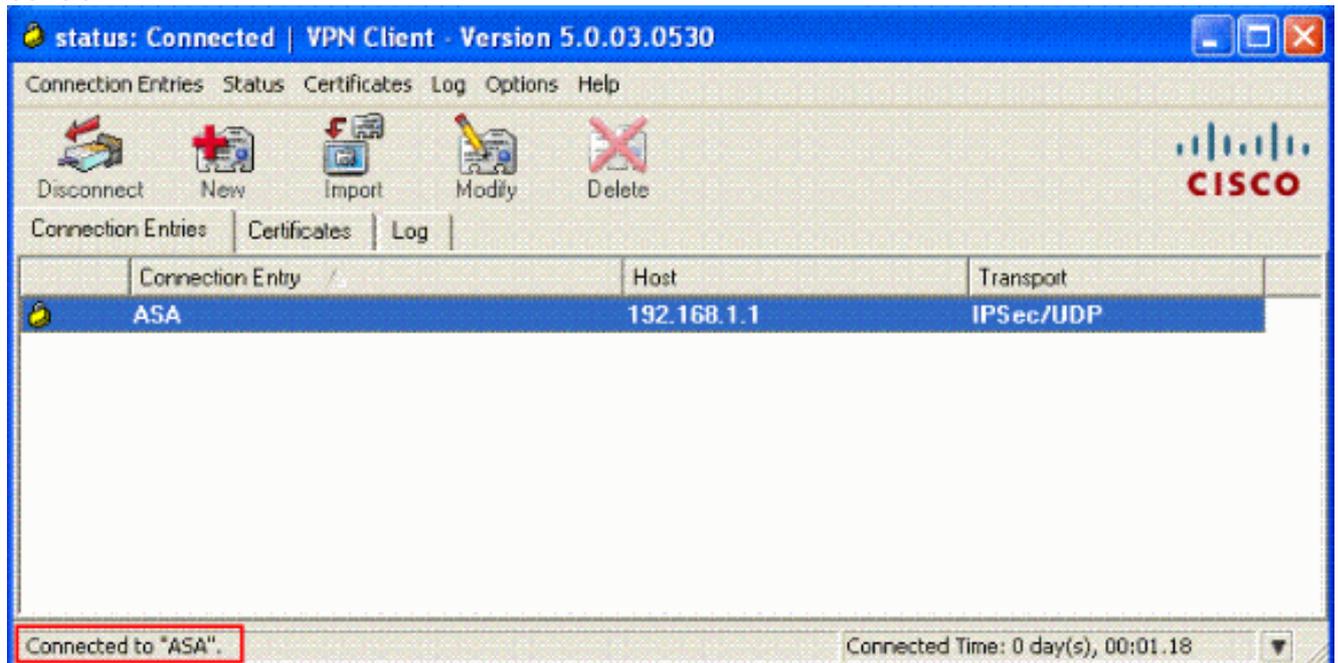


5. Quando alertado, incorpore o **username: Cisco** e **senha: password1** como configurado no ASA para o Xauth, e **APROVAÇÃO** do clique a conectar à rede

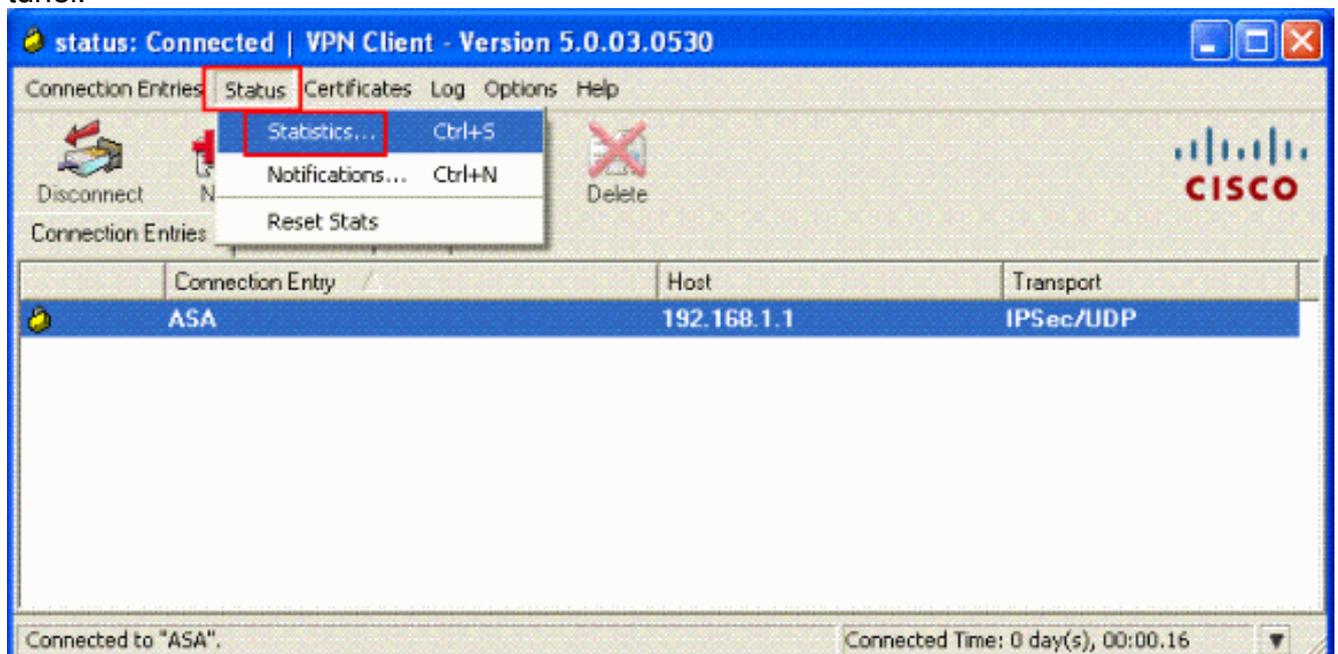


remota.

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.



[Configurar o ACS para ACL baixável para o usuário individual](#)

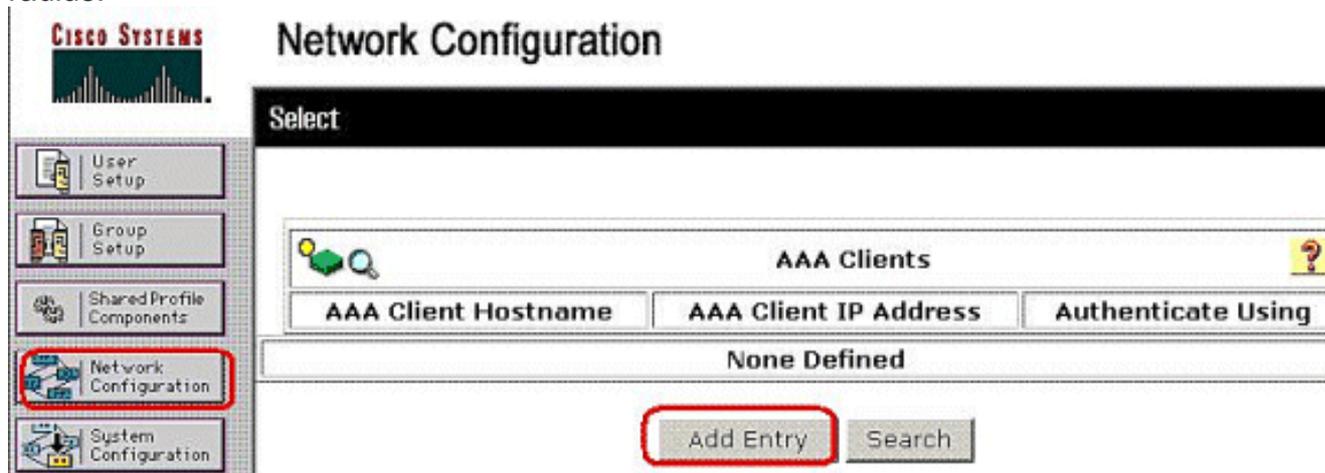
Você pode configurar Listas de acesso carregável no Cisco Secure ACS como um componente de perfil compartilhado e atribui então a lista de acessos a um grupo ou a um usuário individual.

A fim executar listas de acesso dinâmica, você deve configurar o servidor Radius para apoiá-lo. Quando o usuário autentica, o servidor Radius envia uma lista de acessos ou um nome carregável da lista de acessos à ferramenta de segurança. O acesso a um dado serviço é permitido ou negado pela lista de acessos. A ferramenta de segurança suprime da lista de acessos quando a sessão da autenticação expira.

Neste exemplo, o usuário “Cisco” do IPSec VPN autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário “Cisco” pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, veja o [ACL baixável para o usuário/seção de grupo](#).

Termine estas etapas a fim configurar o RAIO em um Cisco Secure ACS.

1. Escolha a **configuração de rede** à esquerda, e o clique **adiciona a entrada** para adicionar uma entrada para o ASA na base de dados do servidor radius.



2. Inscreva **172.16.1.2** no campo de endereço IP cliente, e incorpore "**cisco123**" para o campo de chave secreta compartilhado. Escolha o **RAIO (Cisco VPN 3000/ASA/PIX 7.x+)** na *autenticação usando a caixa suspensa*. O clique **submete-se**.



Network Configuration

Edit

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code
Key

Key Input Format

ASCII Hexadecimal

Authenticate Using

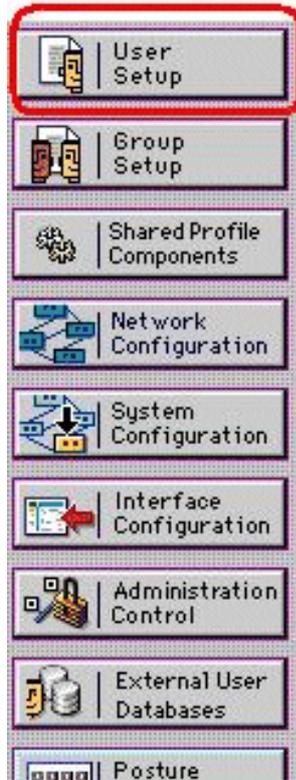
Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

- Incorpore o username ao campo do usuário no base de dados seguro de Cisco, e o clique **adiciona/edita**. Neste exemplo, o username é **Cisco**.



User Setup

Select



User:

List users beginning with letter/number:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9			

4. Na próxima janela, incorpore a senha para "Cisco". Neste exemplo, a senha é igualmente **password1**. Quando você termina, o clique **submete-se**.



User Setup

User: cisco

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

ACS Internal Database 

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

5. Você usa a página avançada das opções para determinar qual avançou opções que o ACS indica. Você pode simplificar as páginas que se publicam em outras áreas da interface da WEB ACS se você esconde as opções avançadas que você não usa. Clique a **configuração da interface**, e clique então **opções avançadas** para abrir a página avançada das opções.

CISCO SYSTEMS

Interface Configuration

Advanced Options

Note: Only the selected options will appear in the user interface.

- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs**
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs**
- Group-Level Password Aging

Verifique a caixa para ver se há o nível de usuário ACL carregável e o Grupo-nível ACL carregável. Nível de usuário ACL carregável - Quando escolhida, esta opção permite a seção carregável ACL (listas de controle de acesso) na página da instalação de usuário. Grupo-nível ACL carregável - Quando escolhida, esta opção permite a seção carregável ACL na página da instalação de grupo.

6. Na barra de navegação, clique **componentes de perfil compartilhado**, e clique **IP carregável ACL**. **Nota:** Se o *IP carregável ACL* não aparece nos componentes de perfil compartilhado página, você deve permitir o nível de usuário opção carregável carregável ACL, de Grupo-nível ACL, ou ambos na página avançada das opções da seção de configuração da

CISCO SYSTEMS

Shared Profile Components

Select

- [Downloadable IP ACLs](#)
- [Network Access Filtering](#)
- [RADIUS Authorization Components](#)
- [Shell Command Authorization Sets](#)
- [PIX/ASA Command Authorization Sets](#)

interface.

7. Clique em Add. A página carregável IP ACL publica-

Shared Profile Components

Select

Downloadable IP ACLs	
Name	Description
None Defined	

Add

Cancel

se.

8. Na caixa de nome, datilografe o nome do IP novo ACL. **Nota:** O nome de um IP ACL pode conter até 27 caracteres. O nome não deve conter espaços ou quaisquer um caracteres: hífen (-), suporte esquerdo ([), right bracket (]), corte (/), corte traseiro (\), citações ("), suporte de ângulo esquerdo (<), suporte de ângulo adequado (>), ou traço (-). Na caixa da descrição, datilografe uma descrição do IP novo ACL. A descrição pode ser até 1,000

Shared Profile Components

Edit

Downloadable IP ACLs

Name:

Description:

ACL Contents

Network Access Filtering

No ACLs

Add

Up

Down



Back to Help

Submit

Cancel

caráteres.

A

fim adicionar um índice ACL ao IP novo ACL, o clique **adiciona**.

9. Na caixa de nome, datilografe o nome do índice novo ACL. **Nota:** O nome de um índice ACL pode conter até 27 caracteres. O nome não deve conter espaços ou qualquer um dos seguintes caracteres: hífen (-), suporte esquerdo ([), right bracket (]), corte (/), corte traseiro (\), citações ("), suporte de ângulo esquerdo (<), suporte de ângulo adequado (>), ou traço (-). Na caixa das definições de ACL, datilografe a definição de ACL nova. **Nota:** Quando você incorpora as definições de ACL à interface da WEB ACS, não use a palavra-chave ou as entradas de nome; um pouco, comece com uma palavra-chave do permit or deny. A fim salvar o índice ACL, o clique **submete**-

Shared Profile Components

Edit

Downloadable IP ACL Content

Name:

VPN_Client

ACL Definitions

```
permit ip any host 10.1.1.2  
deny ip any any
```



Back to Help

Submit

Cancel

se.

10. A página carregável IP ACL publica-se com o satisffeito novo ACL alistado por nome na coluna dos índices ACL. A fim associar um NAF ao índice ACL, escolha um NAF da caixa de filtração do acesso de rede à direita do índice novo ACL. À revelia, NAF é (Todo-AAA-clientes). Se você não atribui um NAF, o ACS associa o índice ACL a todos os dispositivos de rede, que é o

Shared Profile Components

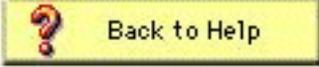
Edit

Downloadable IP ACLs

Name:

Description:

	ACL Contents	Network Access Filtering
<input checked="" type="radio"/>	VPN_Client	(All-AAA-Clients) ▼



padrão.

A fim ajustar a ordem dos índices ACL, clique o botão de rádio para uma definição de ACL, e clique-o então **para cima** ou **para baixo** para reposicioná-la na lista. A fim salvar o IP ACL, o clique **submete-se**. **Nota:** A ordem de índices ACL é significativa. De cima para baixo, o ACS transfere somente a primeira definição de ACL que tem um ajuste NAF aplicável, que inclua a configuração padrão dos Todo-AAA-clientes, se usado. Tipicamente, sua lista de índices ACL continua de esse com o NAF (o mais estreito) o mais específico a esse com (Todo-AAA-clientes) o NAF o mais geral. **Nota:** O ACS incorpora o IP novo ACL, que toma o efeito imediatamente. Por exemplo, se o IP ACL é para o uso com Firewall PIX, está disponível para ser enviado a todo o PIX Firewall que tenta a autenticação de um usuário que tenha esse IP carregável ACL atribuído a seu usuário ou perfil de grupo.

11. Vá à página da instalação de usuário e edite a página de usuário. Sob os ACL carregável seccione, clique o **IP ACL da atribuição**: caixa de verificação. Escolha um IP ACL da lista. Se você terminou a configuração das opções da conta de usuário, o clique **submete-se** para gravar as

User Setup

Account Disable

Never

Disable account if:

Date exceeds: Apr 15 2009

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL: VPN_Access

opções.

[Configurar o ACS para ACL baixável para o grupo](#)

Termine etapas 1 com 9 [configurar ACS para ACL baixável para o usuário individual](#) e siga estas etapas a fim configurar ACL baixável para o grupo em um Cisco Secure ACS.

Neste exemplo, o usuário "Cisco" do IPSec VPN pertence aos grupos de VPN. As políticas do grupo de VPN são aplicadas para todos os usuários no grupo.

O usuário "Cisco" do grupo de VPN autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário "Cisco" pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, refira o [ACL baixável para o usuário/seção de grupo](#).

1. Na barra de navegação, clique a **instalação de grupo**. A página seleta da instalação de grupo

abre.

The screenshot shows the Cisco Systems logo and the title "Group Setup". On the left is a navigation menu with "Group Setup" highlighted. The main content area has a "Select" header and a box containing a dropdown menu for "Group" set to "1: Group 1", and buttons for "Users in Group", "Edit Settings", and "Rename Group".

2. Rebatize o grupo1 ao VPN, e o clique **submete-se**.

The screenshot shows the "Group Setup" page with the "Group Setup" menu item highlighted. A dialog box titled "Renaming Group: Group 1" is displayed, containing a text input field with "VPN" and "Submit" and "Cancel" buttons.

3. Da lista do grupo, escolha um grupo, e clique-o então **editam**

The screenshot shows the "Group Setup" page with the "Group Setup" menu item highlighted. The main content area has a "Select" header and a box containing a dropdown menu for "Group" set to "1: VPN (1 user)", and buttons for "Users in Group", "Edit Settings", and "Rename Group".

ajustes.

4. Sob os ACL carregável secione, clique a caixa de verificação **IP ACL da atribuição**. Escolha um IP ACL da

Group Setup

Jump To Access Restrictions

Sessions available to users of this group

Unlimited

IP Assignment ?

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

Downloadable ACLs ?

Assign IP ACL:

lista.

5. A fim salvar as configurações de grupo que você apenas fez, o clique **submete-se**.

6. Vá à instalação de usuário e edite o usuário que você gostaria de adicionar dentro ao grupo: **VPN**. Quando você termina, o clique **submete-se**.



User Setup

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

VPN ▼

Agora o ACL baixável configurado para o grupo de VPN é aplicado para este usuário.

7. A fim continuar a especificar outras configurações de grupo, execute outros procedimentos neste capítulo, como aplicáveis

[Configurar ajustes do RADIUS IETF para um grupo de usuário](#)

A fim transferir um nome para uma lista de acessos que você já crie na ferramenta de segurança do servidor Radius quando um usuário autentica, configurar o atributo do ID de filtro do RADIUS IETF (número de atributo 11) como segue:

```
filter-id=acl_name
```

O usuário "Cisco" do grupo de VPN autentica com sucesso, e o servidor Radius transfere um nome ACL (novo) para uma lista de acessos que você já crie na ferramenta de segurança. O usuário "Cisco" pode alcançar todos os dispositivos que são rede interna do ASA **exceto** o server de 10.1.1.2. A fim verificar o ACL, veja a [seção ACL do ID de filtro](#).

Conforme o exemplo, o novo nomeado ACL é configurado filtrando no ASA.

```
access-list new extended deny ip any host 10.1.1.2 access-list new extended permit ip any any
```

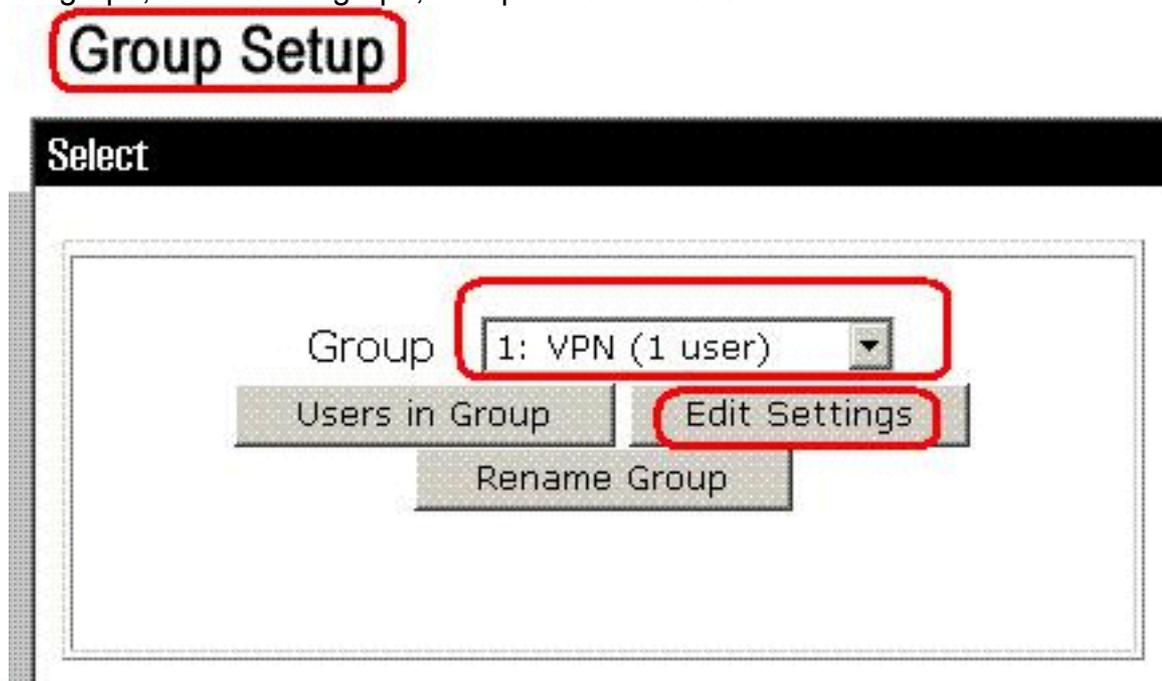
Estes parâmetros aparecem somente quando estes são verdadeiros. Você configurou

- Cliente de AAA para usar um dos protocolos de raio na configuração de rede
- atributos RADIUS do Grupo-nível na página do RAO (IETF) na seção de configuração da interface da interface da WEB

Os atributos RADIUS são enviados como um perfil para cada usuário do ACS ao cliente de AAA de pedido.

A fim configurar ajustes do atributo de raio de IETF para aplicar-se como uma autorização para cada usuário no grupo atual, execute estas ações:

1. Na barra de navegação, clique a **instalação de grupo**.A página seleta da instalação de grupo abre.
2. Da lista do grupo, escolha um grupo, e clique-o então **editam**



ajustes.

nome do grupo aparece na parte superior da página das configurações de grupo.

3. Rolo aos atributos RADIUS IETF. Para cada atributo de raio de IETF, você deve autorizar o grupo atual. Verifique a caixa de verificação do atributo do **ID de filtro [011]**, e adicionar então o name(new) definido ASA ACL na autorização para o atributo no campo. Refira as *saídas de configuração running da mostra*

Group Setup

Jump To Access Restrictions

IETF RADIUS Attributes

[006] Service-Type

Authenticate only

[007] Framed-Protocol

Ascend MPP

[009] Framed-IP-Netmask

0.0.0.0

[010] Framed-Routing

None

[011] Filter-Id

new

[012] Framed-MTU (64..65535)

ASA.

4. A fim salvar as configurações de grupo que você apenas fez e para as aplicar imediatamente, o clique **submete-se** e **aplica-se**. **Nota:** A fim salvar suas configurações de grupo e aplicá-las mais tarde, o clique **submete-se**. Quando você está pronto para executar as mudanças, escolha a **configuração de sistema > o controle de serviço**. Escolha então o **reinício**.

Verificar

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

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

Comandos show crypto

- **show crypto isakmp sa** – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente. `ciscoasa# sh 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: 192.168.10.2 Type : user Role : responder Rekey : no State : AM_ACTIVE ciscoasa#
- **mostre IPsec cripto sa** — Mostra os ajustes usados por SA atuais. `ciscoasa# sh crypto ipsec sa` interface: outside Crypto map tag: outside_dyn_map, seq num: 1, local addr: 192.168.1.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0) current_peer: 192.168.10.2, username: cisco dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 65, #pkts encrypt: 65, #pkts digest: 65 #pkts decaps: 65, #pkts decrypt: 65, #pkts verify: 65 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 4, #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.: 192.168.1.1, remote crypto endpt.: 192.168.10.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: EEF0EC32 inbound esp sas: spi: 0xA6F92298 (2801345176) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xEEF0EC32 (4008766514) transform: esp-3des esp-sha-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 86016, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 28647 IV size: 8 bytes replay detection support: Y

[ACL baixável para o usuário/grupo](#)

Verifique o ACL baixável para o usuário Cisco. Os ACL obtêm transferidos do CSACS.

```
ciscoasa(config)# sh access-list access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300 access-list 101; 1 elements access-list 101 line 1 extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0 255.255.255.0 (hitcnt=0) 0x8719a411 access-list #ACSACL#-IP-VPN_Access-49bf68ad; 2 elements (dynamic) access-list #ACSACL#-IP-VPN_Access-49bf68ad line 1 extended permit ip any host 10.1.1.2 (hitcnt=2) 0x334915fe access-list #ACSACL#-IP-VPN_Access-49bf68ad line 2 extended deny ip any any (hitcnt=40) 0x7c718bd1
```

[ID de filtro ACL](#)

O ID de filtro [011] aplicou-se para o grupo - o VPN, e os usuários do grupo são filtrados conforme o ACL (novo) definido no ASA.

```
ciscoasa# sh access-list
access-list cached ACL log flows: total 0,
    denied 0 (deny-flow-max 4096)
    alert-interval 300
access-list 101; 1 elements
access-list 101 line 1 extended permit ip 10.1.1.0
    255.255.255.0 192.168.5.0 255.255.255.0
    (hitcnt=0) 0x8719a411
access-list new; 2 elements
access-list new line 1 extended deny ip any host 10.1.1.2 (hitcnt=4) 0xb247fec8 access-list new
line 2 extended permit ip any any (hitcnt=39) 0x40e5d57c
```

[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, refira [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](#)
- [Cisco Adaptive Security Device Manager](#)
- [Página de Suporte de Negociação IPsec/Protocolos IKE](#)
- [Página de Suporte do Cisco VPN Client](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)