Bloqueio e chave: Listas de Acesso Dinâmicas

Índice

Introdução

O acesso lock-and-key permite configurar listas de acesso dinâmicas que concedem acesso para cada usuário a um host específico de origem/destino por meio de um processo de autenticação de usuários. O acesso de usuário é permitido com um Firewall do ® do Cisco IOS dinamicamente, sem nenhum acordo nas restrições de segurança.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Neste caso, o ambiente de laboratório consistiu em um 2620 Router que executa o Software Release 12.3(1) de Cisco IOS®. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Considerações sobre falsificação

O acesso bloqueio e chave permite que um evento externo coloque uma abertura no Cisco IOS Firewall. Quando essa abertura existir, o roteador ficará suscetível à falsificação do endereço de origem. A fim impedir isto, forneça o suporte de criptografia que usa a criptografia IP a autenticação ou a criptografia.

Falsificação é um problema de todas as listas de acesso existentes. O acesso de chave e bloqueio não soluciona esse problema.

Como o acesso chave e bloqueio introduz um caminho potencial através do firewall de rede, é necessário considerar o acesso dinâmico. Um outro host, falsificação seu endereço autenticado, acede atrás do Firewall. Com acesso dinâmico, há a possibilidade que um host não autorizado, falsificação seu endereço autenticado, acede atrás do Firewall. O acesso bloqueio e chave não causa o problema da falsificação de endereço. O problema é aqui identificado somente em consideração ao usuário.

Desempenho

O desempenho é afetado nestas duas situações.

- Cada lista de acesso dinâmico obriga uma reconstrução de lista de acesso no silicon switching engine (SSE). Isto faz o caminho de switching SSE ficar temporariamente lento.
- As listas de acesso dinâmica exigem a facilidade do idle timeout (mesmo se o intervalo é deixado para optar). Consequentemente, as listas de acesso dinâmica não podem ser SSE comutado. Estas entradas são seguradas no caminho de switching rápido do protocolo.

Olhe as configurações do roteador de borda. Os usuários remotos criam entradas de lista de acesso no roteador de borda. A lista de acessos cresce e encolhe dinamicamente. As entradas são dinamicamente removidas da lista depois do timeout ocioso ou do timeout máximo expirar. Listas de acesso grandes degradam o desempenho da switching de pacotes.

Quando usar o acesso chave e bloqueio

Dois exemplos de quando você usa o acesso bloqueio e chave são alistados aqui:

- Quando você quiser um host remoto poder alcançar um host em sua rede interna através do Internet. O acesso bloqueio e chave limita o acesso além de seu Firewall em uma base do host individual ou da rede.
- Quando quiser que um subconjunto de hosts em uma rede acesse um host em uma rede remota protegida por um firewall. Com o acesso lock-and-key, você pode habilitar apenas um conjunto desejado de hosts para obter acesso, fazendo com que eles se autentiquem por meio de um servidor TACACS+ ou RADIUS.

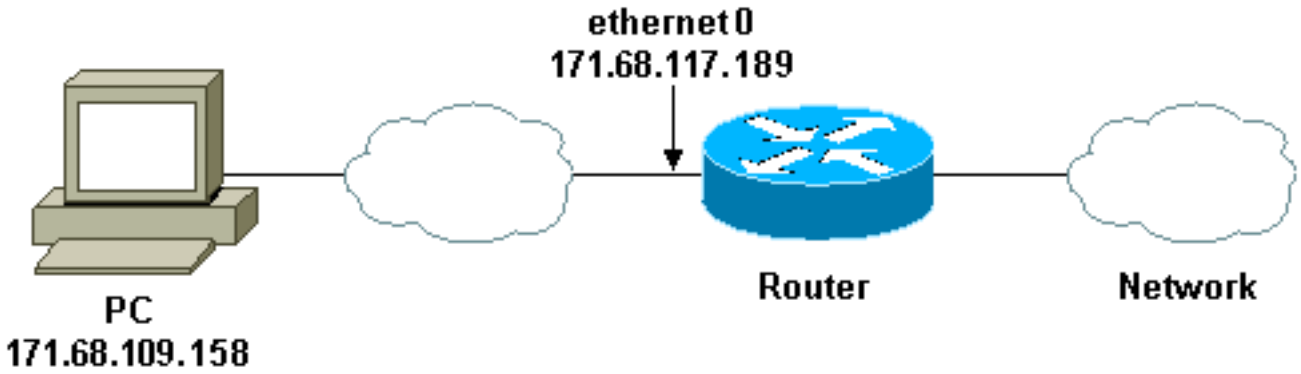
Operação de acesso de chave e bloqueio

Este processo descreve a operação de acesso de chave e bloqueio.

1. Um usuário abre uma sessão Telnet com um roteador de borda configurado para acesso lock-and-key.
2. O Cisco IOS Software recebe o pacote de Telnet. Executa um processo de autenticação de usuário. O usuário deve realizar a autenticação antes do acesso ser permitido. O processo de autenticação é feito pelo roteador ou por um servidor de acesso central tal como um TACACS+ ou um servidor Radius.

Exemplo de Configuração e Troubleshooting

Diagrama de Rede



Cisco recomenda que você usa um server TACACS+ para seu processo da pergunta da autenticação. O TACACS+ fornece serviços de autenticação, autorização e conta. Igualmente fornece o suporte de protocolo, a especificação de protocolo, e um base de dados de segurança centralizado.

Você pode autenticar o usuário no roteador ou com um TACACS+ ou um servidor Radius.

Nota: Estes comandos são globais salvo indicação contrária.

No roteador, você precisa um **username** para o usuário para a autenticação local.

```
username test password test
```

A presença de **login local nas** linhas vty faz com que este username seja usado.

```
line vty 0 4
login local
```

Se você não confia o usuário para emitir o **comando access-enable**, você pode fazer uma de duas coisas:

- Associe o intervalo com o usuário em uma base do usuário per.
  ```
  username test autocommand access-enable host
  timeout 10
  ```
  ou

- Force todos os usuários esse telnet dentro a ter o mesmo intervalo.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

Nota: O 10 na sintaxe é o *idle timeout da* lista de acessos. É cancelado pelo timeout absoluto na lista de acesso dinâmica.

Defina uma lista de acesso extendida que seja aplicada quando um usuário (algum usuário) registra no roteador e no comando access-enable é emitido. O momento absoluto máximo para este “furo” no filtro é ajustado a 15 minutos. Após 15 minutos, o furo fecha-se mesmo se qualquer um o usa. O testlist do nome precisa de existir mas ser não significativo. Limite as redes a que o usuário tem o acesso configurando o endereço de origem ou de destino (aqui, o usuário não é limitado).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Defina a lista de acessos necessária obstruir tudo a não ser que a capacidade ao telnet no roteador (a fim abrir um furo, o usuário precisa o telnet ao roteador). O endereço IP de Um ou Mais Servidores Cisco ICM NT aqui é o endereço IP de Ethernet do roteador.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Há um implícito nega tudo na extremidade (não entrada aqui).

Aplique esta lista de acessos à relação em que os usuários vêm.

```
interface ethernet1
       ip access-group 120 in
```

Você é feito.

Este é o que o filtro olha como no roteador agora:

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Os usuários que obtêm o acesso a sua rede interna não podem ver qualquer coisa até eles telnet ao roteador.

Nota: O 10 aqui é o *idle timeout da* lista de acessos. É cancelado pelo timeout absoluto na lista de acesso dinâmica.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

O filtro olha como este.

```
Router#show access-lists
```

```
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Há um furo no filtro para este um usuário baseado no endereço IP de origem. Quando alguma outra pessoa faz este, você vê *dois furos*.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Estes usuários podem ter o acesso IP completo a todo o endereço IP de destino de seu *endereço IP de origem*.

Utilizando TACACS+

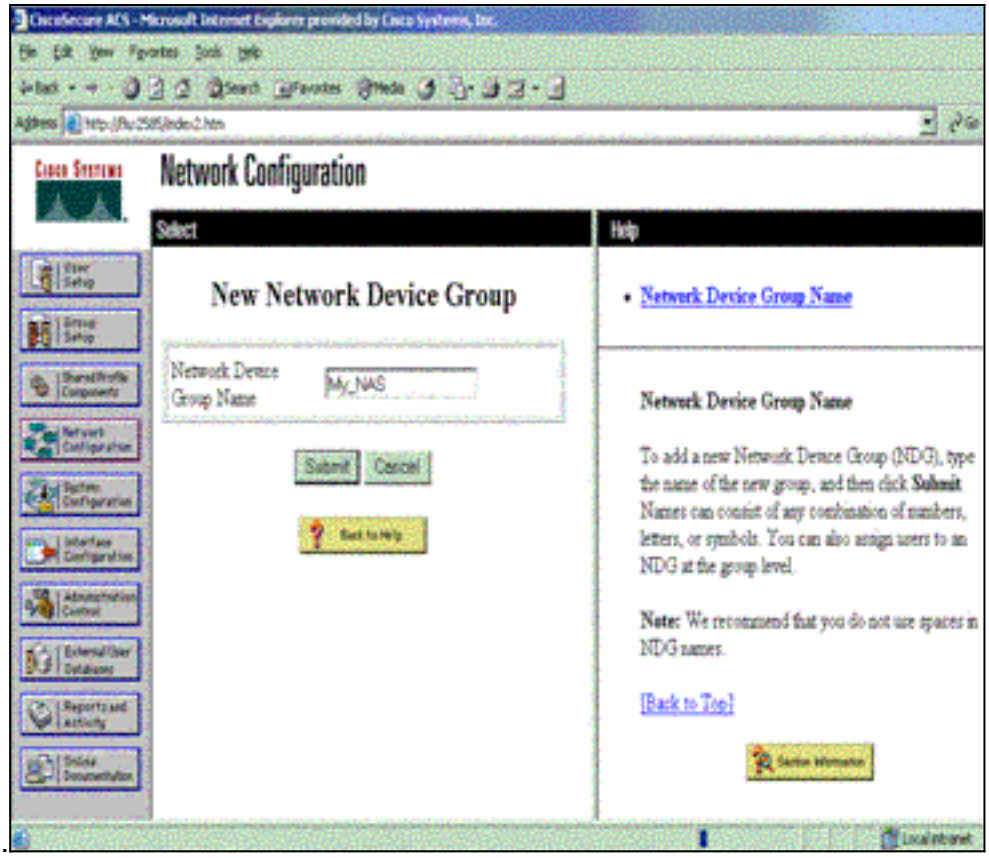
Configurar o TACACS+

Configurar um server TACACS+ para forçar a authentication e autorização para ser feito no server TACACS+ a fim usar o TACACS+, como esta saída mostra:

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

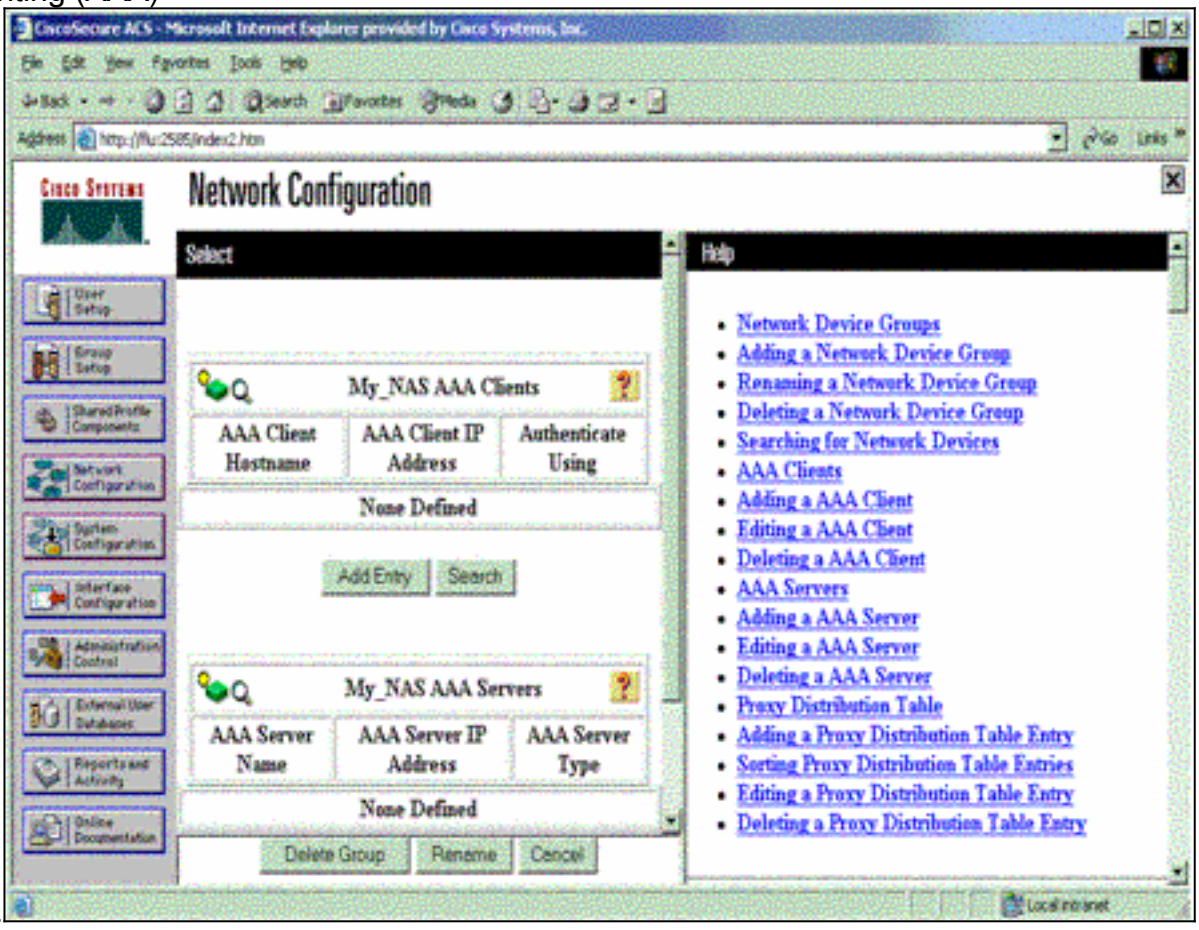
Termine estas etapas para configurar o TACACS+ no Cisco Secure ACS for Windows:

1. Abra um navegador da Web. Incorpore o endereço de seu servidor ACS, que é sob a forma dos *<IP_address de* **http://** *ou do DNS_name>:2002*. (Este exemplo usa uma porta padrão de 2002.) Entre como o admin.
2. Clique em Network Configuration. O clique **adiciona a entrada** para criar um grupo de dispositivo de rede que contenha os servidores do acesso de rede (NAS). Dê entrada com um nome para o grupo e o clique **submete-**



se.

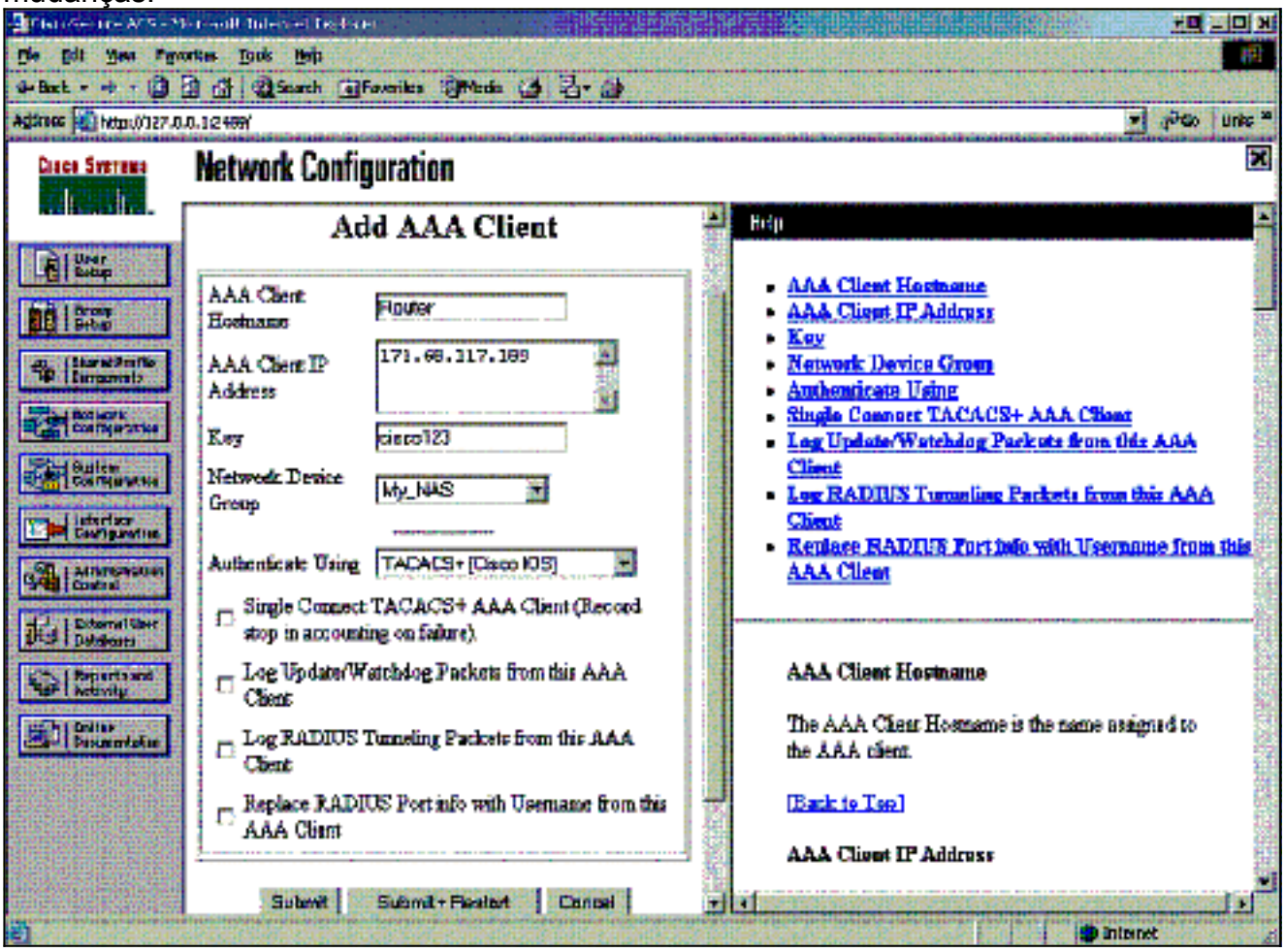
3. O clique **adiciona a entrada** para adicionar um cliente do Authentication, Authorization, and Accounting (AAA)



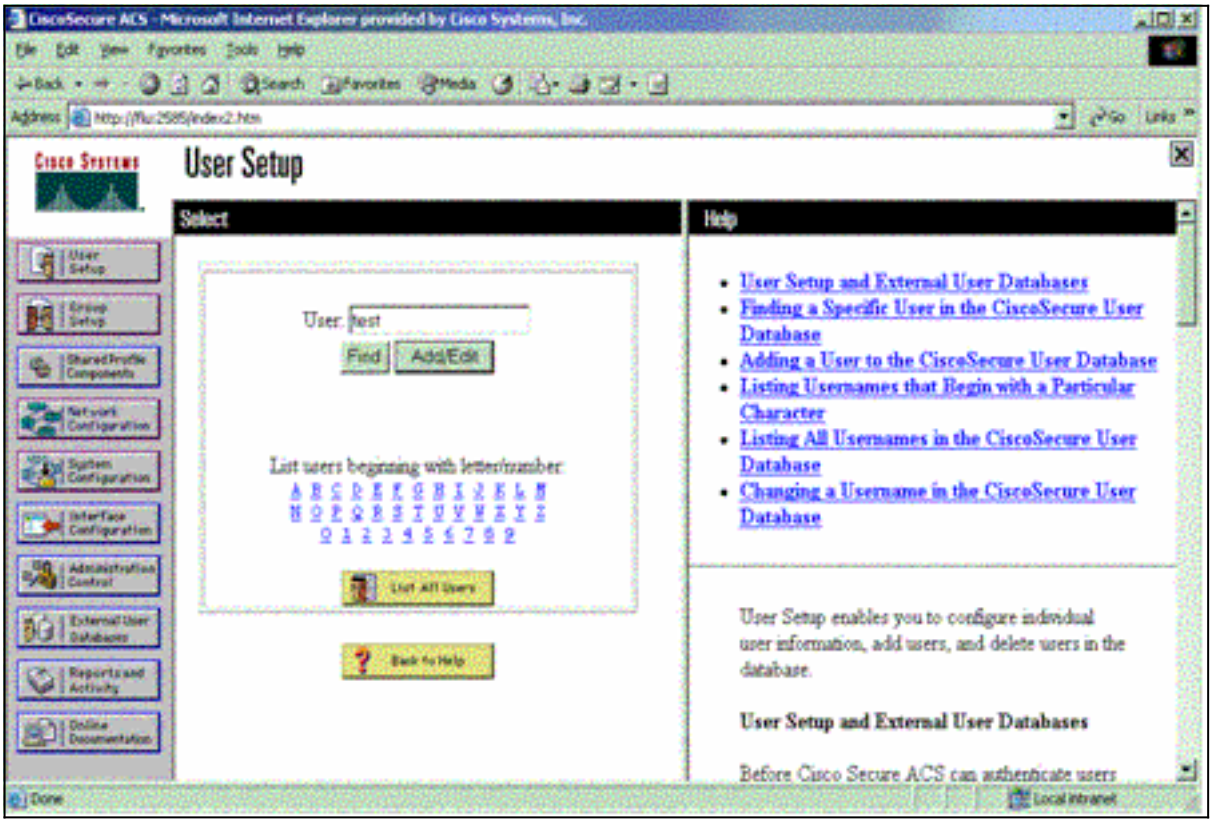
(NAS).

4. Incorpore o nome de host, o endereço IP de Um ou Mais Servidores Cisco ICM NT, e a chave usada para cifrar uma comunicação entre o servidor AAA e o NAS. Selecione **TACACS+ (Cisco IOS)** como o método de autenticação. Quando você é terminado, o clique **submete +Restart** para aplicar as

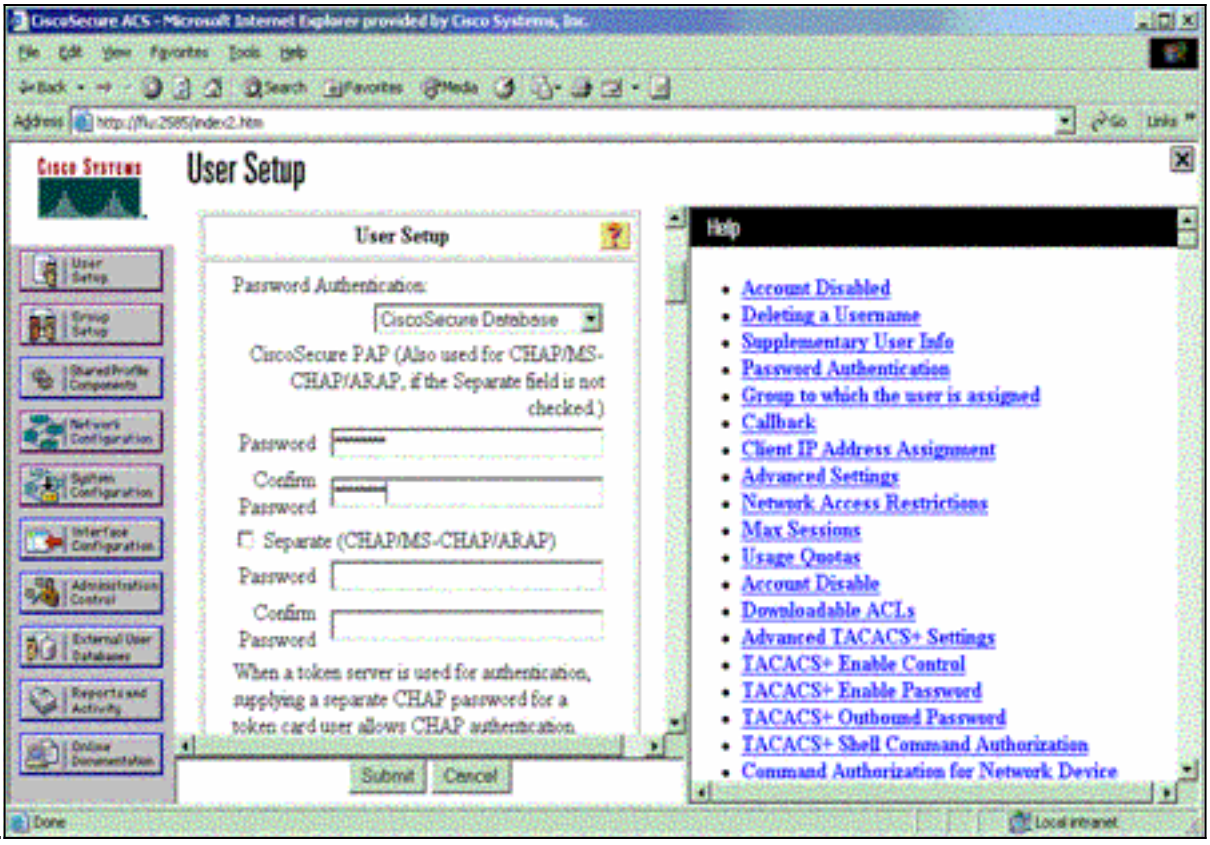
mudanças.



5. Clique a **instalação de usuário**, inscreva um usuário - a identificação, e o clique **adicionam/editam**.

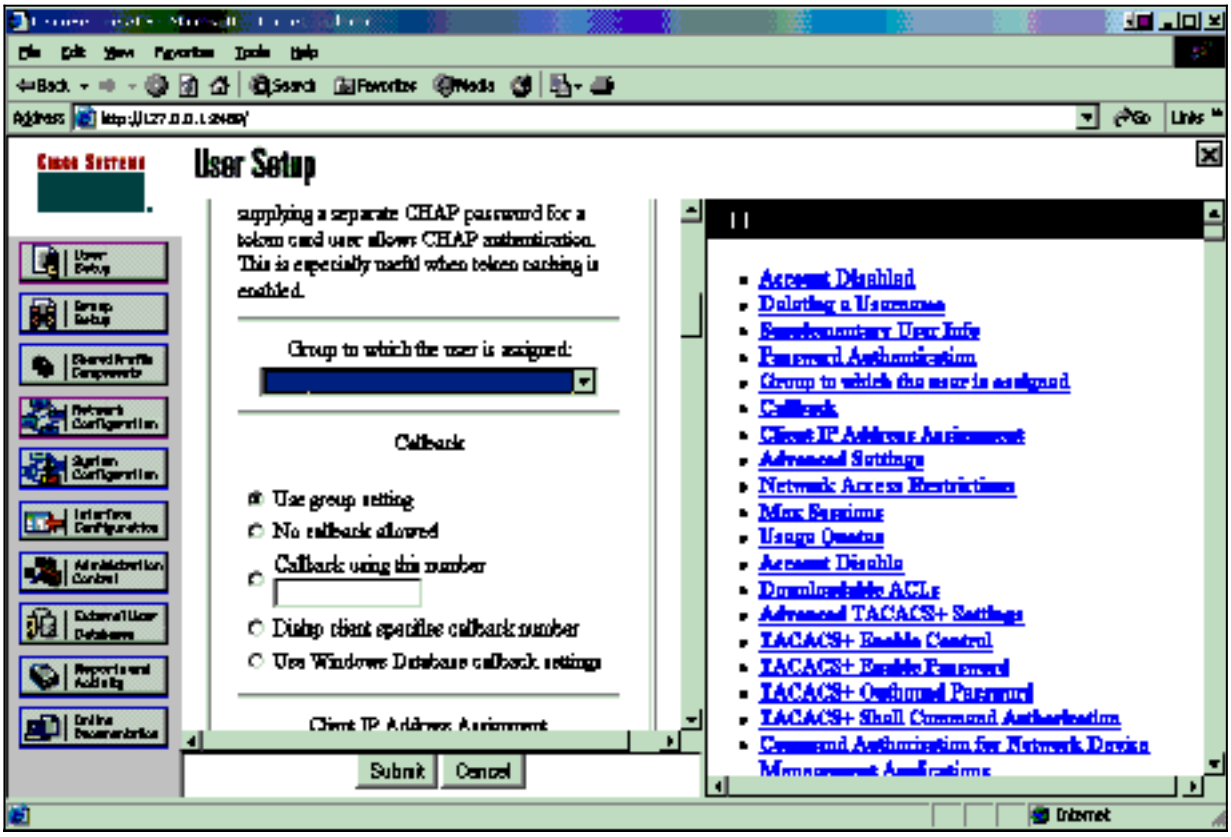


6. Escolha um base de dados autenticar o usuário. (Neste exemplo, o usuário é “teste” e o base de dados interno do ACS é usado para a autenticação). Incorpore uma senha para o usuário, e confirme a

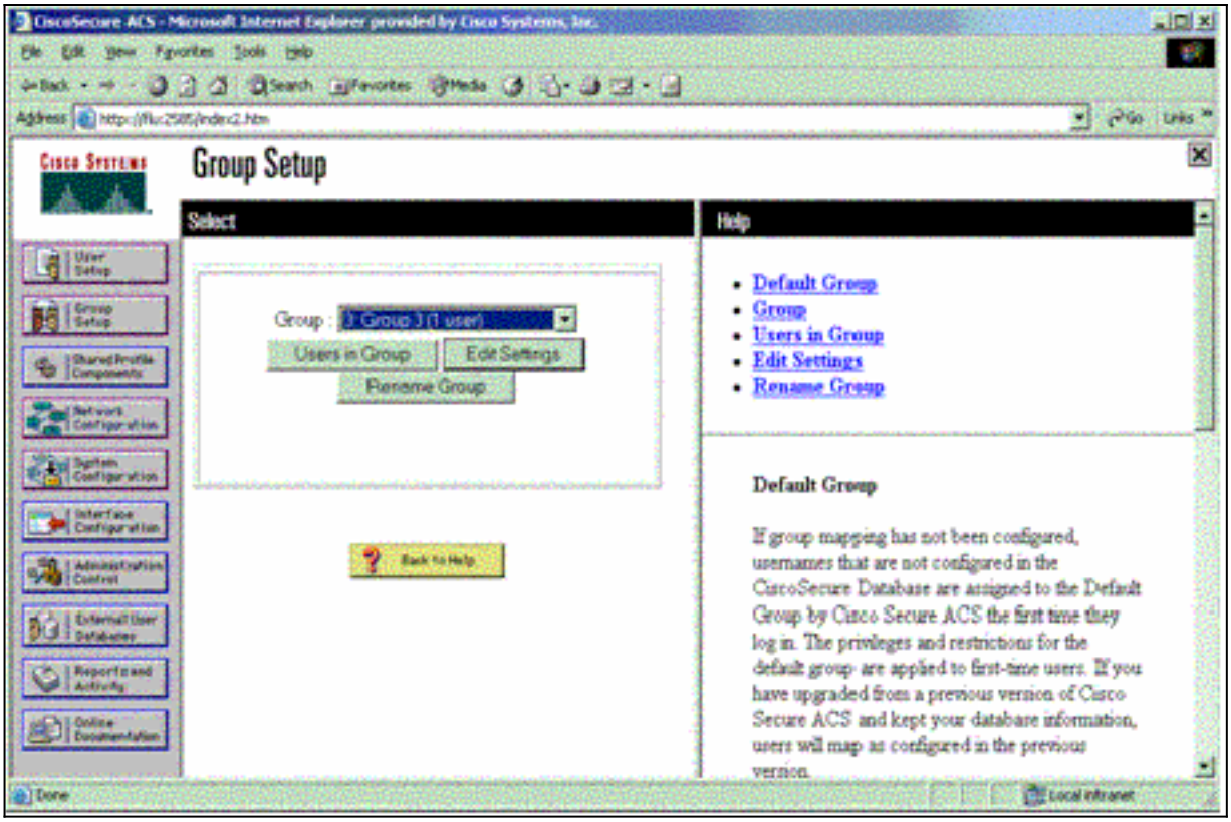


senha.

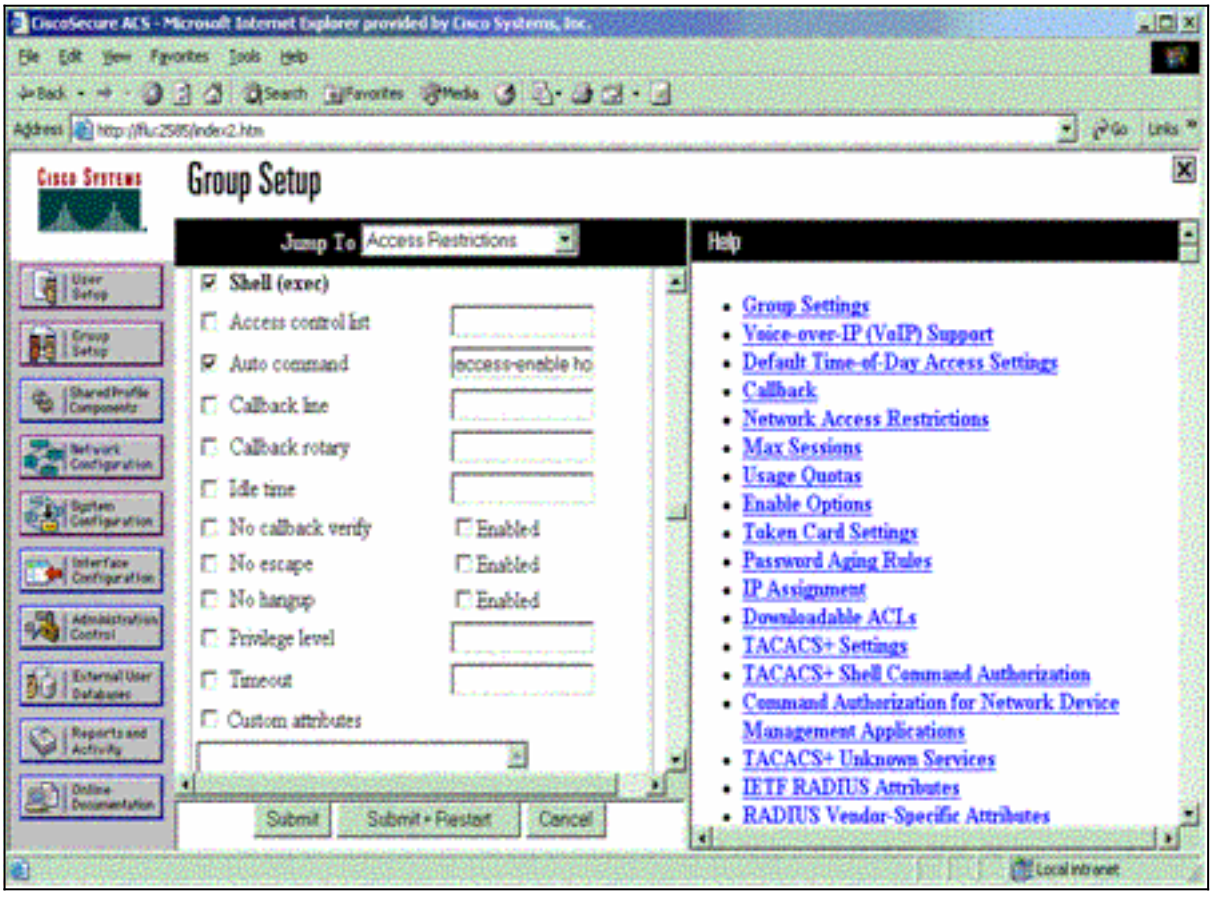
7. Escolha o grupo a que o usuário é atribuído e verifique a **configuração de grupo do uso**. Clique em
Submit.



8. **Instalação de grupo do** clique. Selecione o grupo a que o usuário foi atribuído no clique de etapa 7. **edita**
ajustes.



9. Enrole para baixo a seção dos ajustes TACACS+. Verifique a caixa para ver se há o **executivo de shell**. Verifique a caixa para ver se há o **comando auto**. Inscreva o Comando automático ser executado em cima da autorização bem sucedida do usuário. (Este exemplo usa o **comando 10 do intervalo do host da acesso-possibilidade**.) Clique **Submit+Restart**.



[Pesquise defeitos o TACACS+]

Use estes **comandos debug no** NAS pesquisar defeitos problemas TACACS+.

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

- **debugar a autenticação TACACS** — Indica a informação no processo de autenticação TACACS+. Somente disponível em algumas versões de software. Se não disponível, o uso **debuga tacacs** somente.
- **debugar a autorização dos tacacs** — Informação dos indicadores no processo da autorização TACACS+. Somente disponível em algumas versões de software. Se não disponível, o uso **debuga tacacs** somente.
- **debugar eventos dos tacacs** — Informação dos indicadores do processo do ajudante TACACS+. Somente disponível em algumas versões de software. Se não disponível, o uso **debuga tacacs** somente.

Use estes comandos pesquisar defeitos problemas AAA:

- debug aaa authentication — Exibe informações sobre autenticação AAA/TACACS+.
- debug aaa authorization — Exibe informações sobre autorização AAA/TACACS+.

O exemplo de debug aqui mostra uma autenticação bem sucedida e um processo da autorização no server ACS TACACS+.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
```

```
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Usando RADIUS

Configurar o RAIO

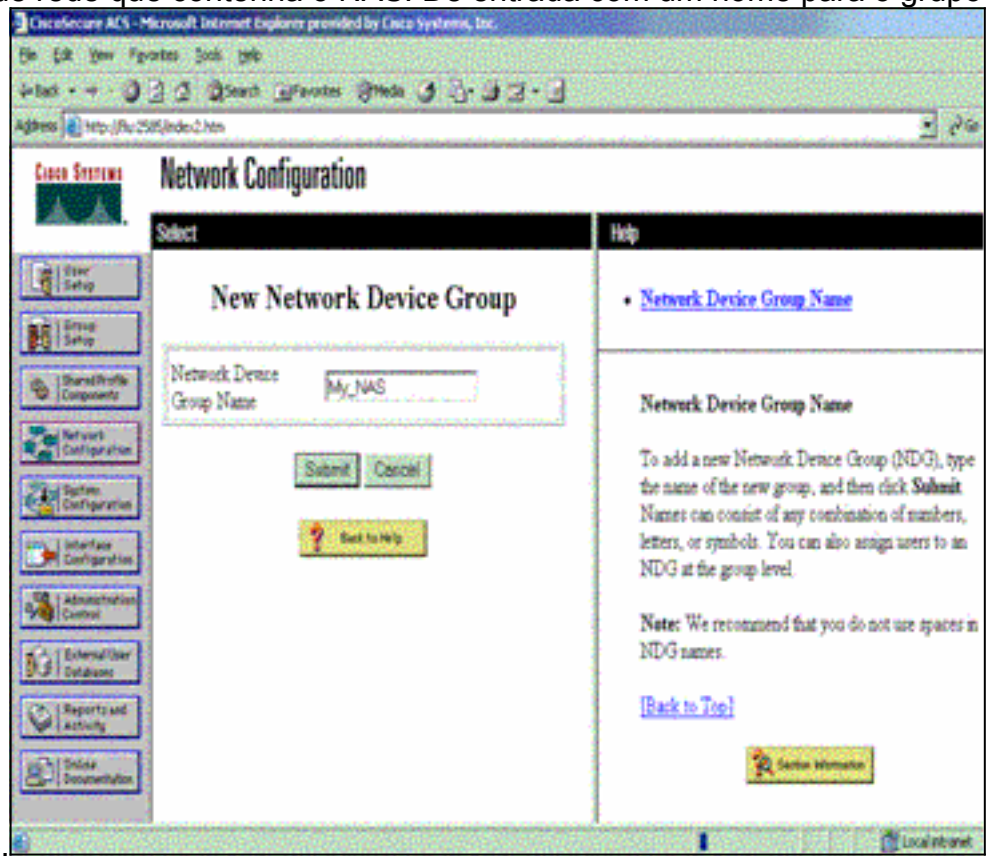
A fim usar o RAIO, configurar um servidor Radius para forçar a autenticação para ser feito no servidor Radius com os parâmetros de autorização (comando automático) a ser enviados para baixo no atributo específico de fornecedor 26, como mostrado aqui:

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
```

```
TPLUS: Authentication start packet created for 9()
TPLUS: Using server 10.48.66.53
TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

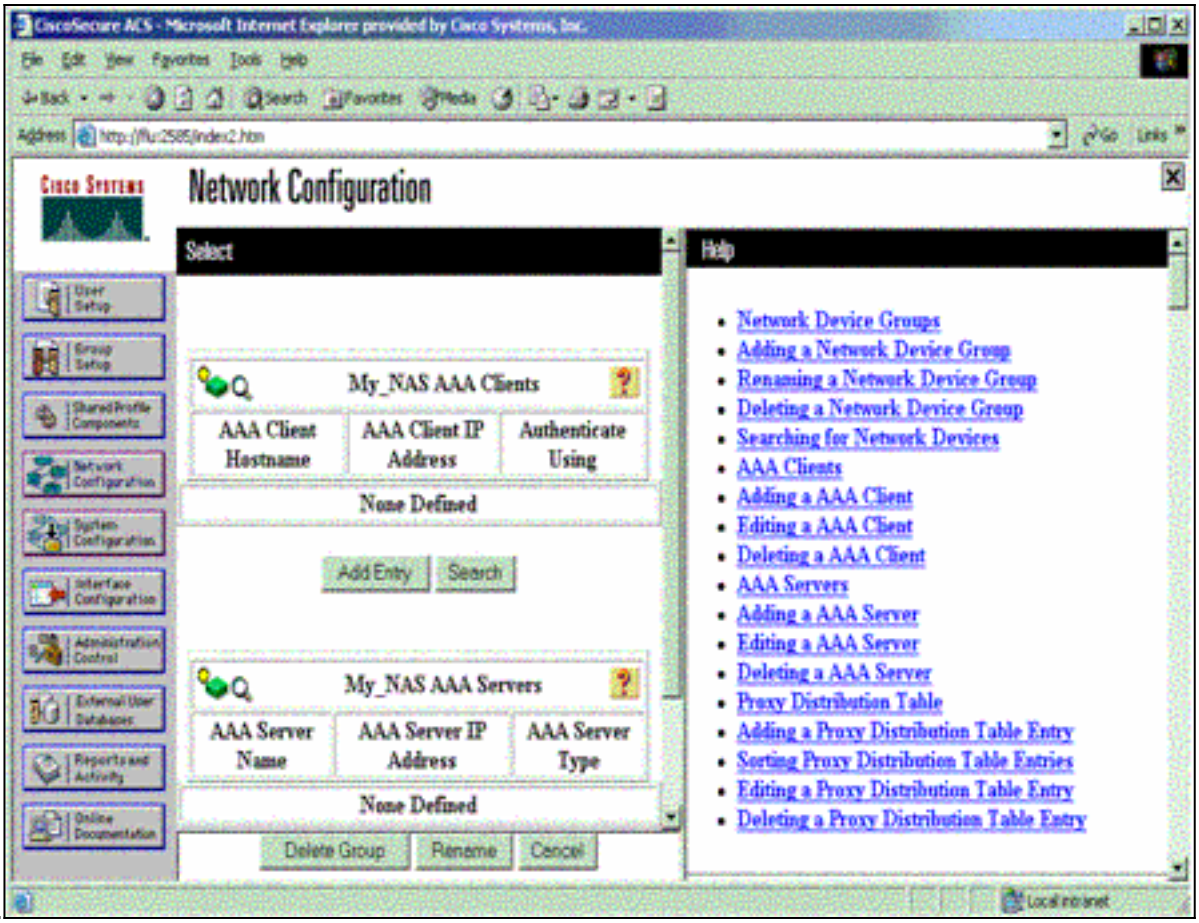
Termine estas etapas para configurar o RAIO no Cisco Secure ACS for Windows:

1. Abra um navegador da Web e incorpore o endereço de seu servidor ACS, que é sob a forma dos ***<IP_address de* http:// *ou do DNS_name>:2002***. (Este exemplo usa uma porta padrão de 2002.) Entre como o admin.
2. Clique em Network Configuration. O clique **adiciona a entrada** para criar um grupo de dispositivo de rede que contenha o NAS. Dê entrada com um nome para o grupo e o clique **submete-se**.

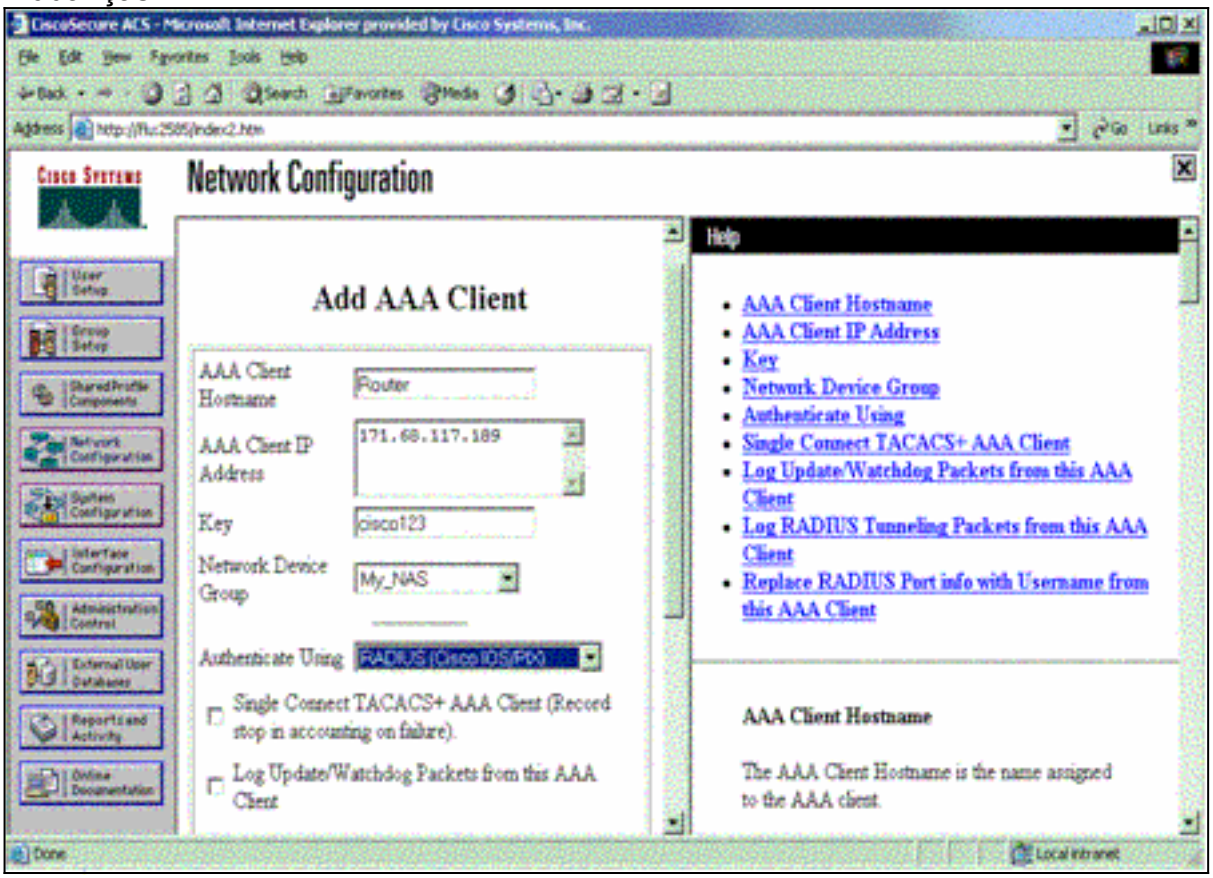


3. O clique **adiciona a entrada** para adicionar um cliente de AAA

(NAS).

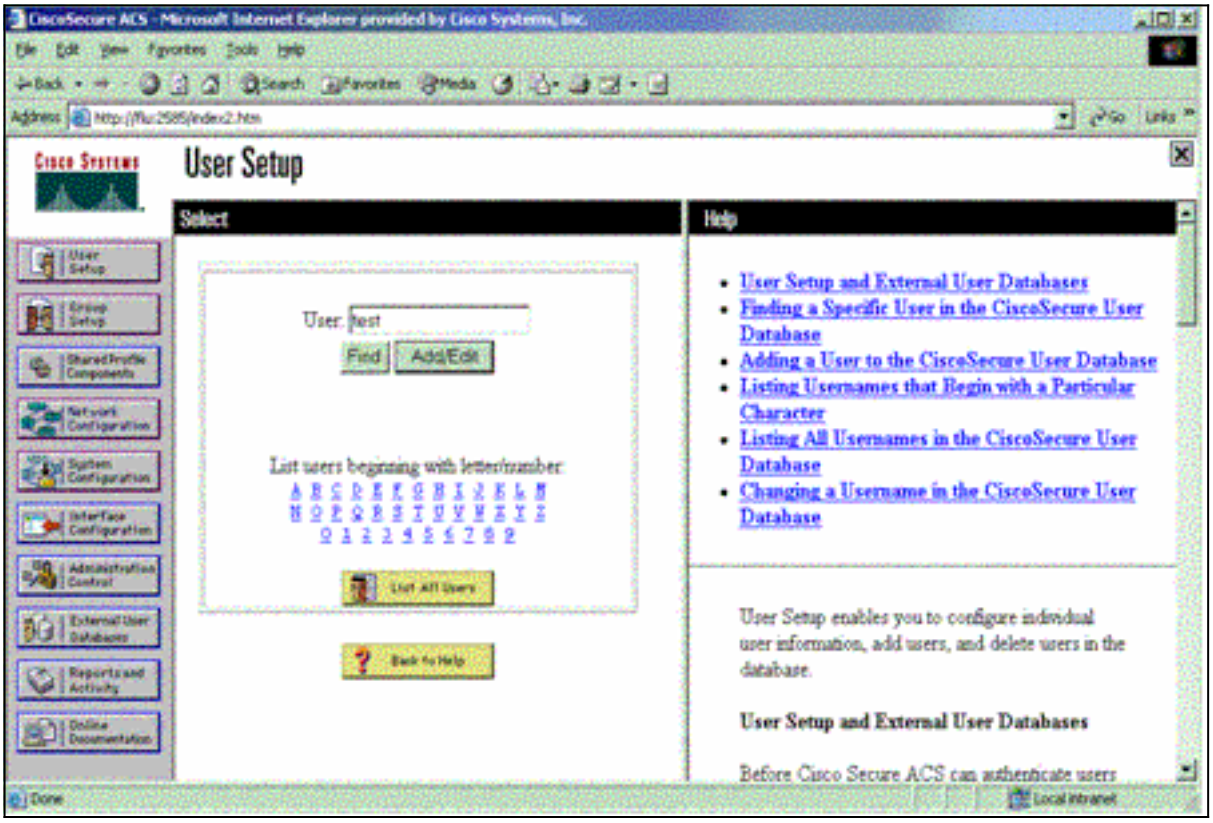


4. Incorpore o nome de host, o endereço IP de Um ou Mais Servidores Cisco ICM NT, e a chave usada para cifrar uma comunicação entre o servidor AAA e o NAS. Selecione o **RAIO (Cisco IOS/PIX)** como o método de autenticação. Quando você é terminado, o clique **submete +Restart** para aplicar as mudanças.

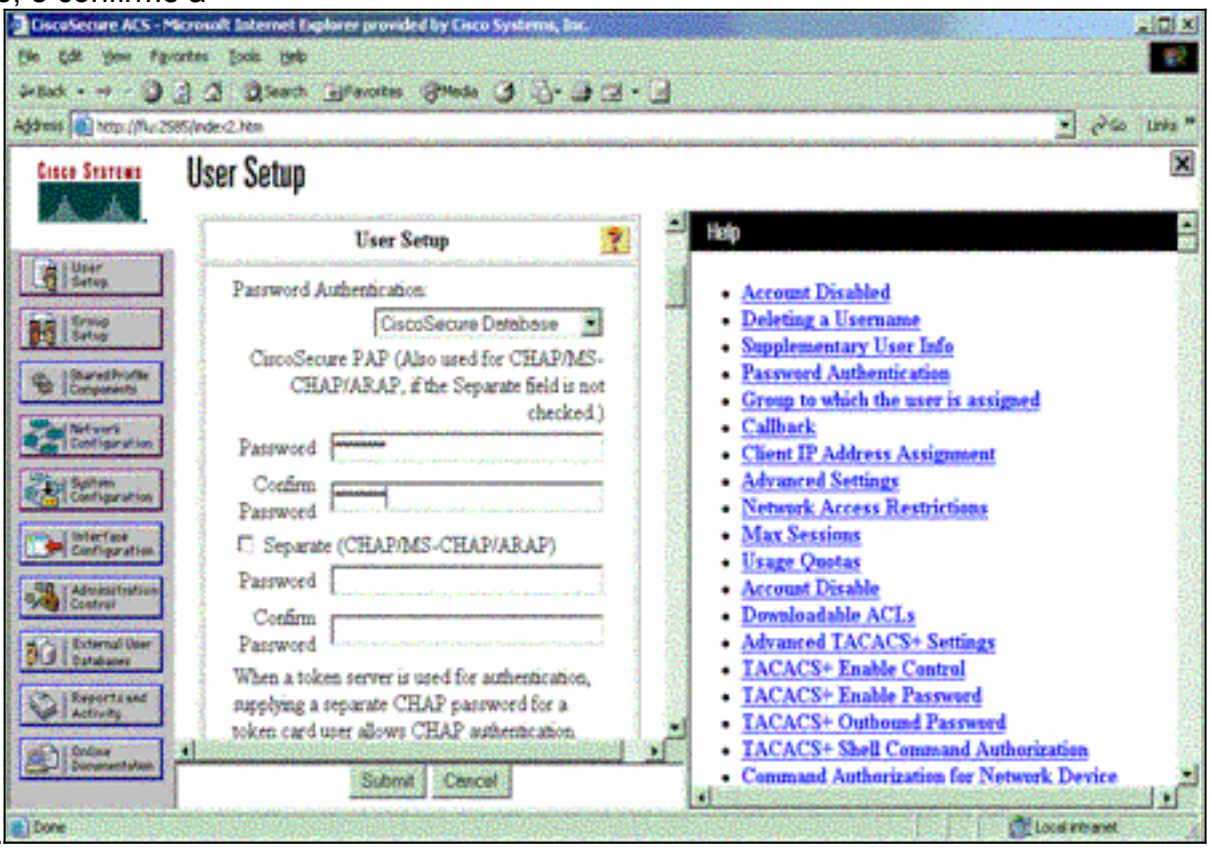


5. Clique a **instalação de usuário**, inscreva um usuário - a identificação, e o clique

adicionam/editam.

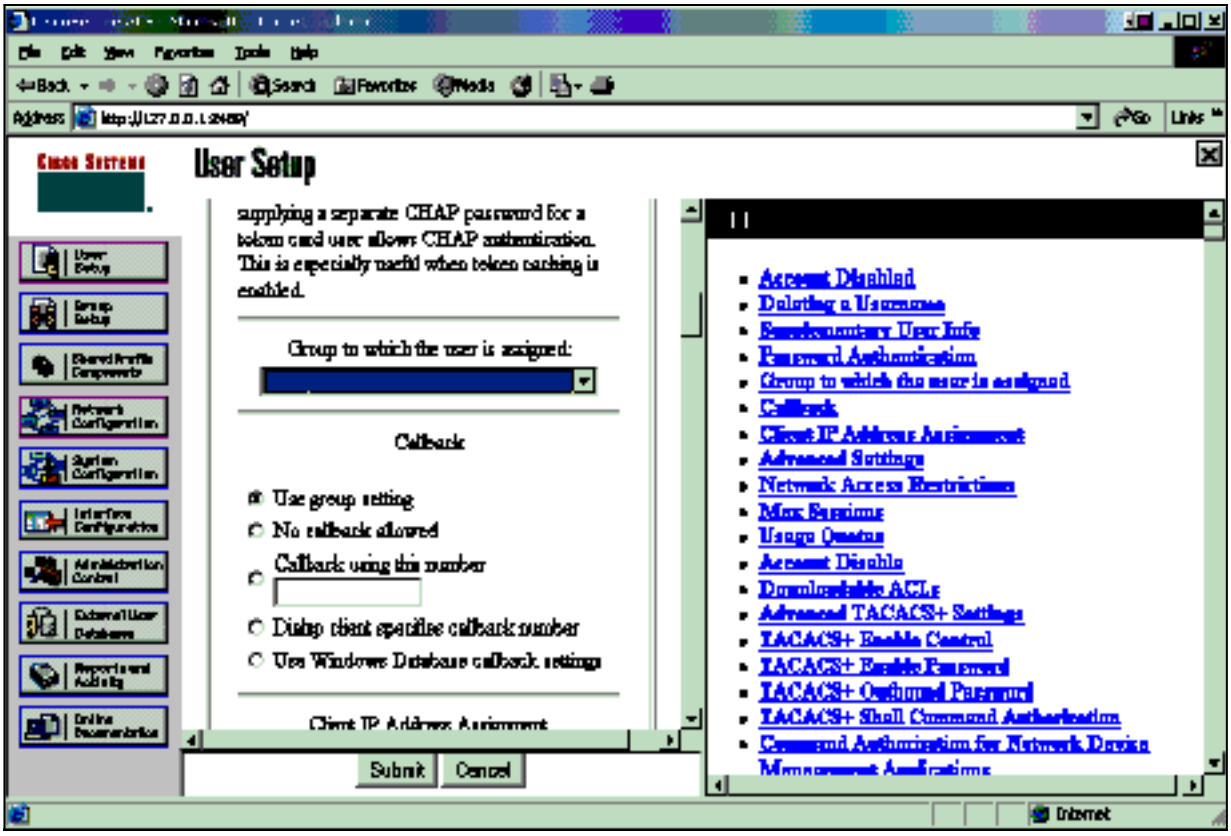


6. Escolha um base de dados autenticar o usuário. (Neste exemplo, o usuário é “teste” e o base de dados interno do ACS é usado para a autenticação). Incorpore uma senha para o usuário, e confirme a

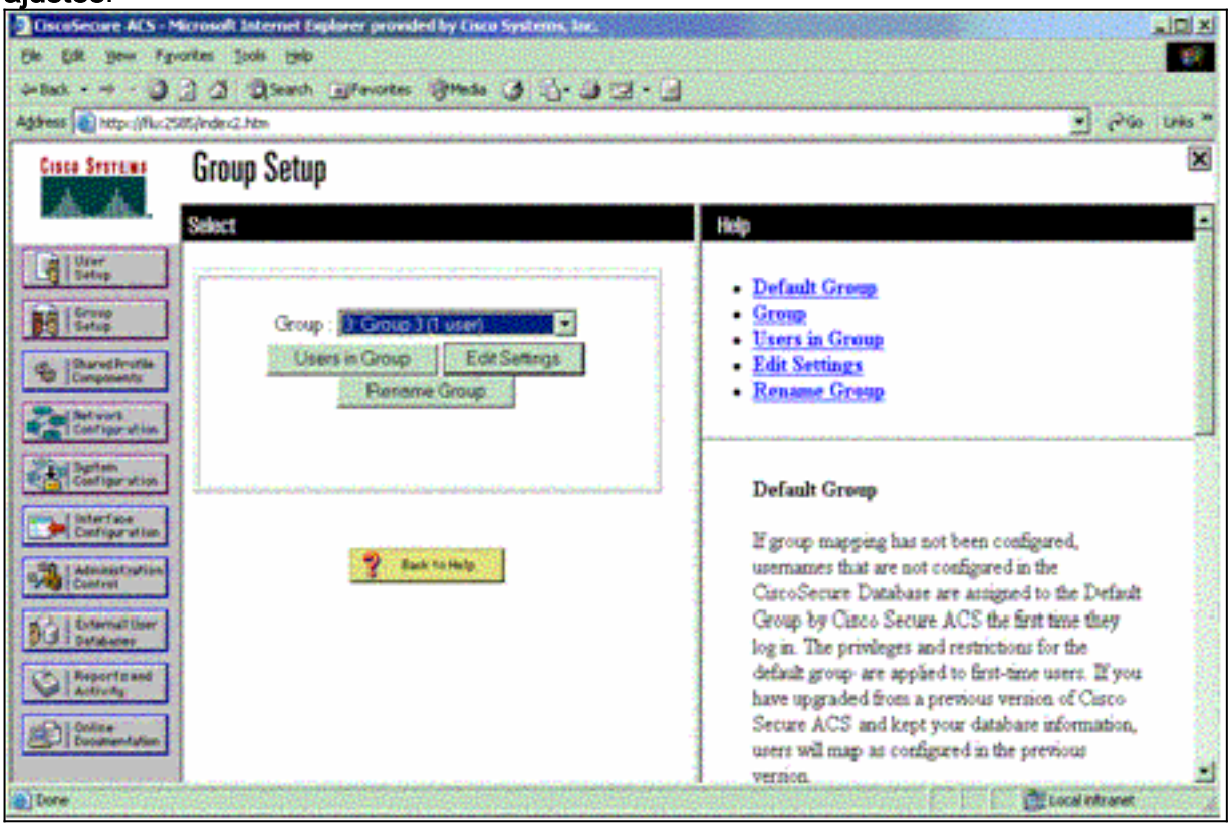


senha.

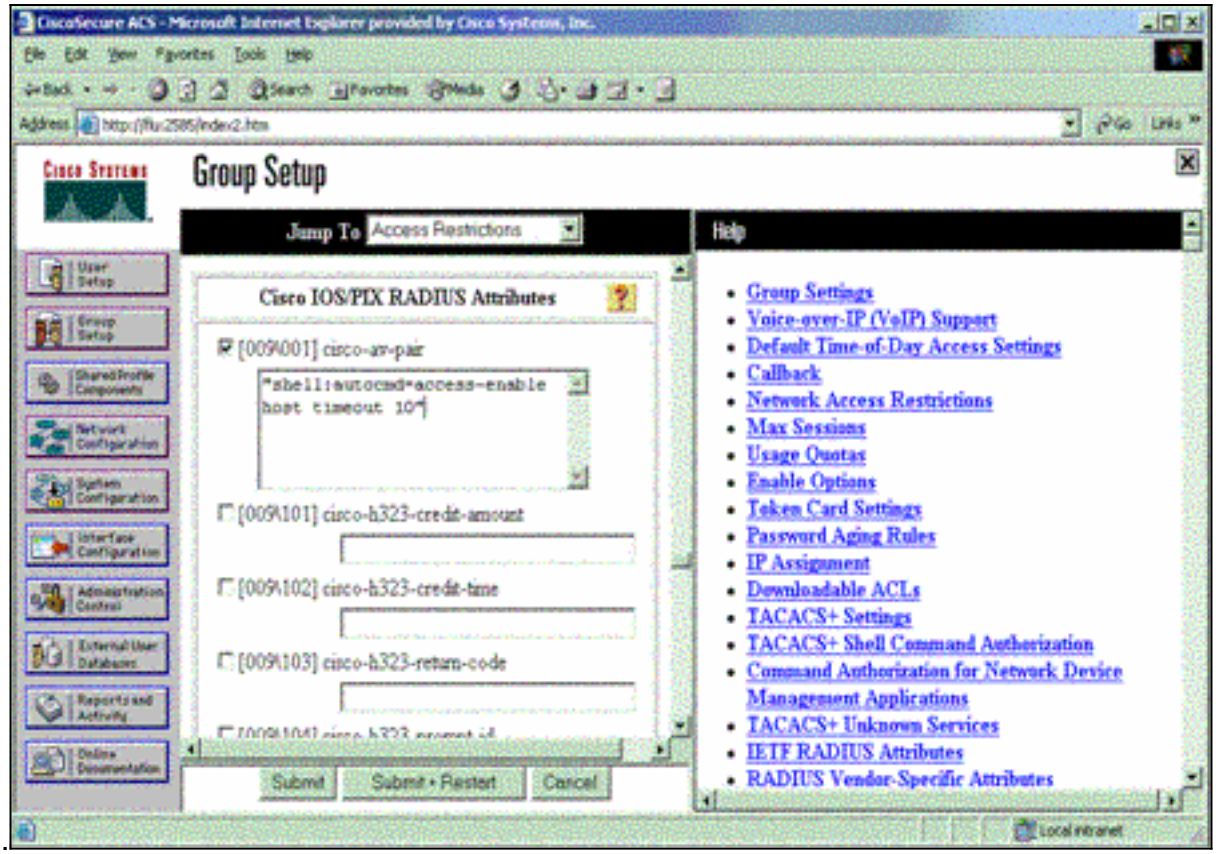
7. Escolha o grupo a que o usuário é atribuído e verifique a **configuração de grupo do uso**. Clique em
Submit.



8. Clique a **instalação de grupo** e selecione o grupo a que o usuário foi atribuído na etapa precedente. O clique **edita ajustes**.



9. Enrole para baixo a seção dos atributos RADIUS de Cisco IOS/PIX. Verifique a caixa para ver se há o **Cisco-av-pair**. Inscreva o **comando shell** ser executado em cima da autorização bem sucedida do usuário. (Este exemplo usa o **shell:** clique **autocmd=access-enable Submit+Restart do intervalo 10. do**

host). 

Pesquise defeitos o RAIO

Use estes **comandos debug no** NAS pesquisar defeitos problemas de RADIUS.

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

- debug radius – Exibe informações associadas ao RADIUS.

Use estes comandos pesquisar defeitos problemas AAA:

- debug aaa authentication — Exibe informações sobre autenticação AAA/TACACS+.
- debug aaa authorization — Exibe informações sobre autorização AAA/TACACS+.

O exemplo de debug aqui mostra uma autenticação bem sucedida e um processo da autorização no ACS configurado para o RAIO.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=======================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                        [tty]
```

```
RADIUS(00000003): Storing nasport 66 in rad_db
RADIUS/ENCODE(00000003): dropping service type,
  "radius-server attribute 6 on-for-login-auth" is off
RADIUS(00000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(00000003): acct_session_id: 1
RADIUS(00000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
  BE B5 07 BD E9 05 5B 5D
RADIUS:  User-Name           [1]   7   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port            [5]   6   66
RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
  Access-Accept, len 93
RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
  68 4B C3 FC 25 21 47 CD
RADIUS:  Vendor, Cisco       [26]  51
RADIUS:   Cisco AVpair       [1]   45
  "shell:autocmd=access-enable host timeout 10"
RADIUS:  Class               [25]  22
RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
RADIUS:   31 2F 36 36                [1/66]
RADIUS(00000003): Received from id 21645/1
AAA/AUTHOR/EXEC(00000003): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

Informações Relacionadas

- Segurança bloqueio e chave do Cisco IOS
- Página de Suporte do TACACS/TACACS+
- TACACS+ na Documentação do IOS
- Página de suporte RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems