

IOS Router: Autenticação de proxy de autenticação de entrada com ACS para configuração de cliente IPsec e VPN

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Configuração de VPN Client 4.8](#)

[Configurar o servidor TACACS+ usando o Cisco Secure ACS](#)

[Configurar o recurso de retorno](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

O recurso de proxy de autenticação permite que os usuários façam login em uma rede ou acessem a Internet via HTTP, com seus perfis de acesso específicos automaticamente recuperados e aplicados de um servidor TACACS+ ou RADIUS. Os perfis de usuário estão ativos somente quando há tráfego ativo dos usuários autenticados.

Essa configuração é projetada para ativar o navegador de Web em 10.1.1.1 e apontá-lo para 10.17.17.17. Como o VPN Client está configurado para passar pelo ponto de extremidade do túnel 10.31.1.111 para chegar à rede 10.17.17.x, o túnel IPsec é criado e o PC obtém o endereço IP do pool RTP-POOL (já que a configuração do modo é executada). A autenticação é solicitada pelo Cisco 3640 Router. Depois que o usuário digitar o nome de usuário e a senha (armazenados no servidor TACACS+ em 10.14.14.3), a lista de acesso passada do servidor é adicionada à lista de acesso 118.

Prerequisites

Requirements

Antes de tentar esta configuração, verifique se estes requisitos são atendidos:

- O Cisco VPN Client é configurado para estabelecer um túnel IPsec com o Cisco 3640 Router.
- O servidor TACACS+ está configurado para proxy de autenticação. Consulte a seção

"Informações relacionadas" para obter mais informações.

Componentes Utilizados

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

- Cisco IOS? Software versão 12.4
- Cisco 3640 Router
- Cisco VPN Client para Windows versão 4.8 (qualquer VPN Client 4.x ou posterior deve funcionar)

Observação: o comando `ip auth-proxy` foi introduzido no Cisco IOS Software Release 12.0.5.T. Esta configuração foi testada com o Cisco IOS Software Release 12.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

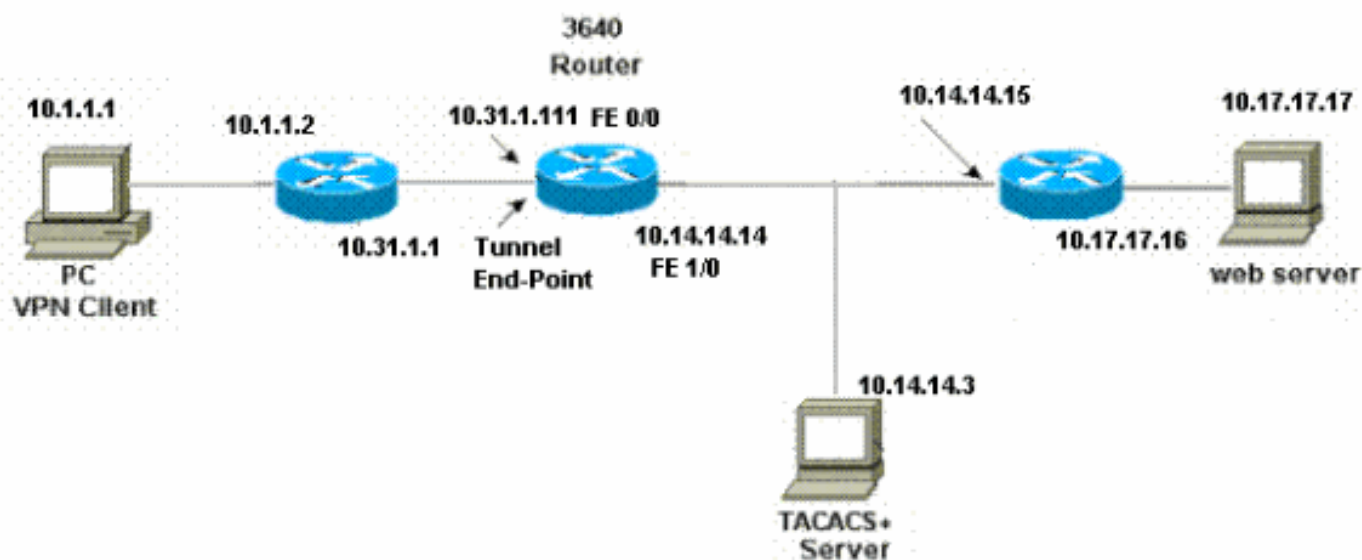
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a [ferramenta Command Lookup Tool](#) (somente clientes [registrados](#)).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração

3640 Router

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
!--- The username and password is used during local
authentication. username rtpuser password 0 rtpuserpass

!--- Enable AAA. aaa new-model

!--- Define server-group and servers for TACACS+. aaa
group server tacacs+ RTP
server 10.14.14.3
!

!--- In order to set authentication, authorization, and
accounting (AAA) authentication at login, use the aaa
authentication login command in global configuration
mode

aaa authentication login default group RTP local
aaa authentication login userauth local
aaa authorization exec default group RTP none
aaa authorization network groupauth local
aaa authorization auth-proxy default group RTP
enable secret 5 $1$CQHC$R/07uQ44E2JgVuCsOUWdG1
enable password ww
!
ip subnet-zero
!
!--- Define auth-proxy banner, timeout, and rules. ip
auth-proxy auth-proxy-banner http ^C
Please Enter Your Username and Password:
^C
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
!--- Define ISAKMP policy. crypto isakmp policy 10
hash md5
authentication pre-share
group 2

!--- These commands define the group policy that !--- is
enforced for the users in the group RTPUSERS. !--- This
group name and the key should match what !--- is
configured on the VPN Client. The users from this !---
group are assigned IP addresses from the pool RTP-POOL.
crypto isakmp client configuration group RTPUSERS
key cisco123
pool RTP-POOL
!
```

```

!--- Define IPSec transform set and apply it to the
dynamic crypto map. crypto ipsec transform-set RTP-
TRANSFORM esp-des esp-md5-hmac
!
crypto dynamic-map RTP-DYNAMIC 10
  set transform-set RTP-TRANSFORM
!
!--- Define extended authentication (X-Auth) using the
local database. !--- This is to authenticate the users
before they can !--- use the IPSec tunnel to access the
resources. crypto map RTPCLIENT client authentication
list userauth

!--- Define authorization using the local database. !---
This is required to push the 'mode configurations' to
the VPN Client. crypto map RTPCLIENT isakmp
authorization list groupauth
crypto map RTPCLIENT client configuration address
initiate
crypto map RTPCLIENT client configuration address
respond
crypto map RTPCLIENT 10 ipsec-isakmp dynamic RTP-DYNAMIC
!
interface FastEthernet0/0
  ip address 10.31.1.111 255.255.255.0
  ip access-group 118 in
  no ip directed-broadcast

!--- Apply the authentication-proxy rule to the
interface. ip auth-proxy list_a
  no ip route-cache
  no ip mroute-cache
  speed auto
  half-duplex

!--- Apply the crypto-map to the interface. crypto map
RTPCLIENT
!
interface FastEthernet1/0
  ip address 10.14.14.14 255.255.255.0
  no ip directed-broadcast
  speed auto
  half-duplex
!
!--- Define the range of addresses in the pool. !--- VPN
Clients will have thier 'internal addresses' assigned !-
-- from this pool. ip local pool RTP-POOL 10.20.20.25
10.20.20.50
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.15
ip route 10.1.1.0 255.255.255.0 10.31.1.1

!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list
118 permits communication !--- between the TACACS+
server and the 3640 router to enable !--- authentication
and authorization. All other traffic is denied. access-
list 118 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111

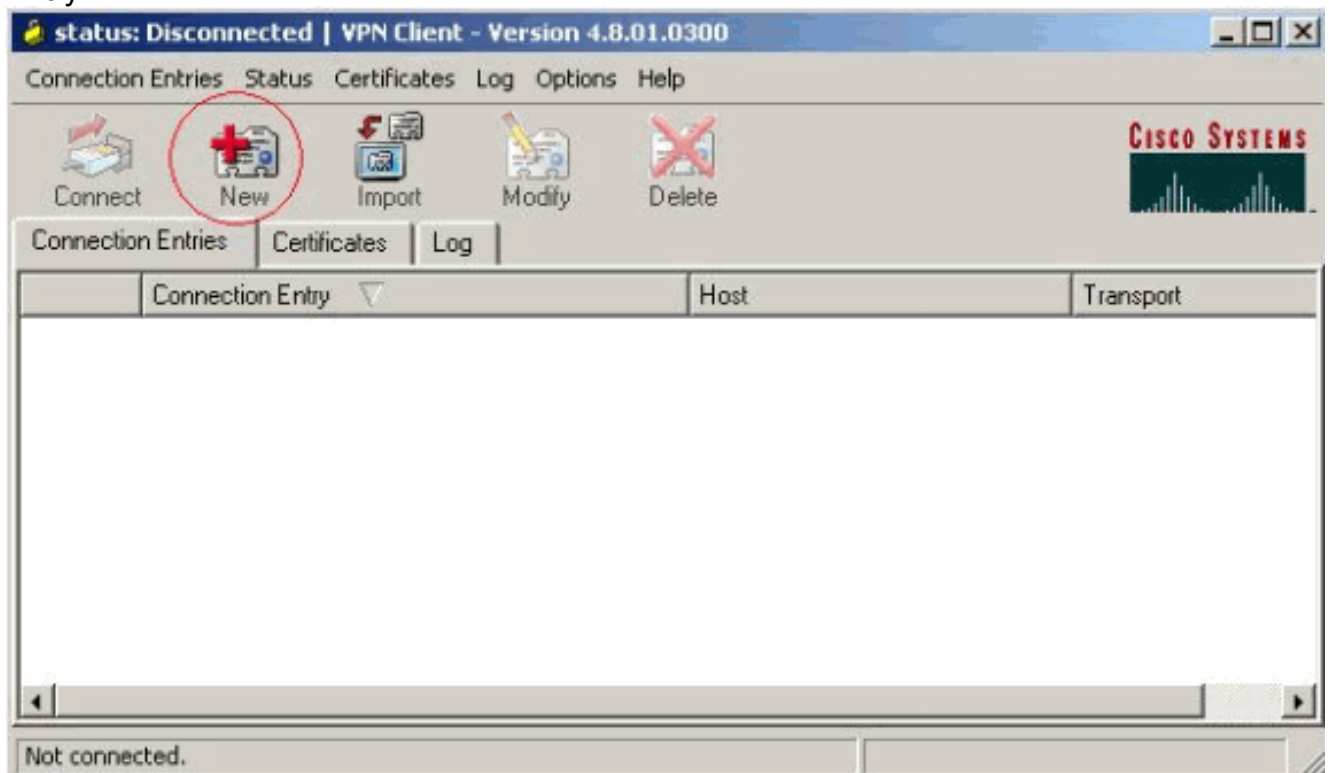
```

```
access-list 118 permit udp 10.1.1.0 0.0.0.255 host
10.31.1.111 eq isakmp
access-list 118 permit tcp host 10.14.14.3 host
10.31.1.111
!
!--- Define the IP address and the key for the TACACS+
server. tacacs-server host 10.14.14.3 key cisco
!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
!
end
```

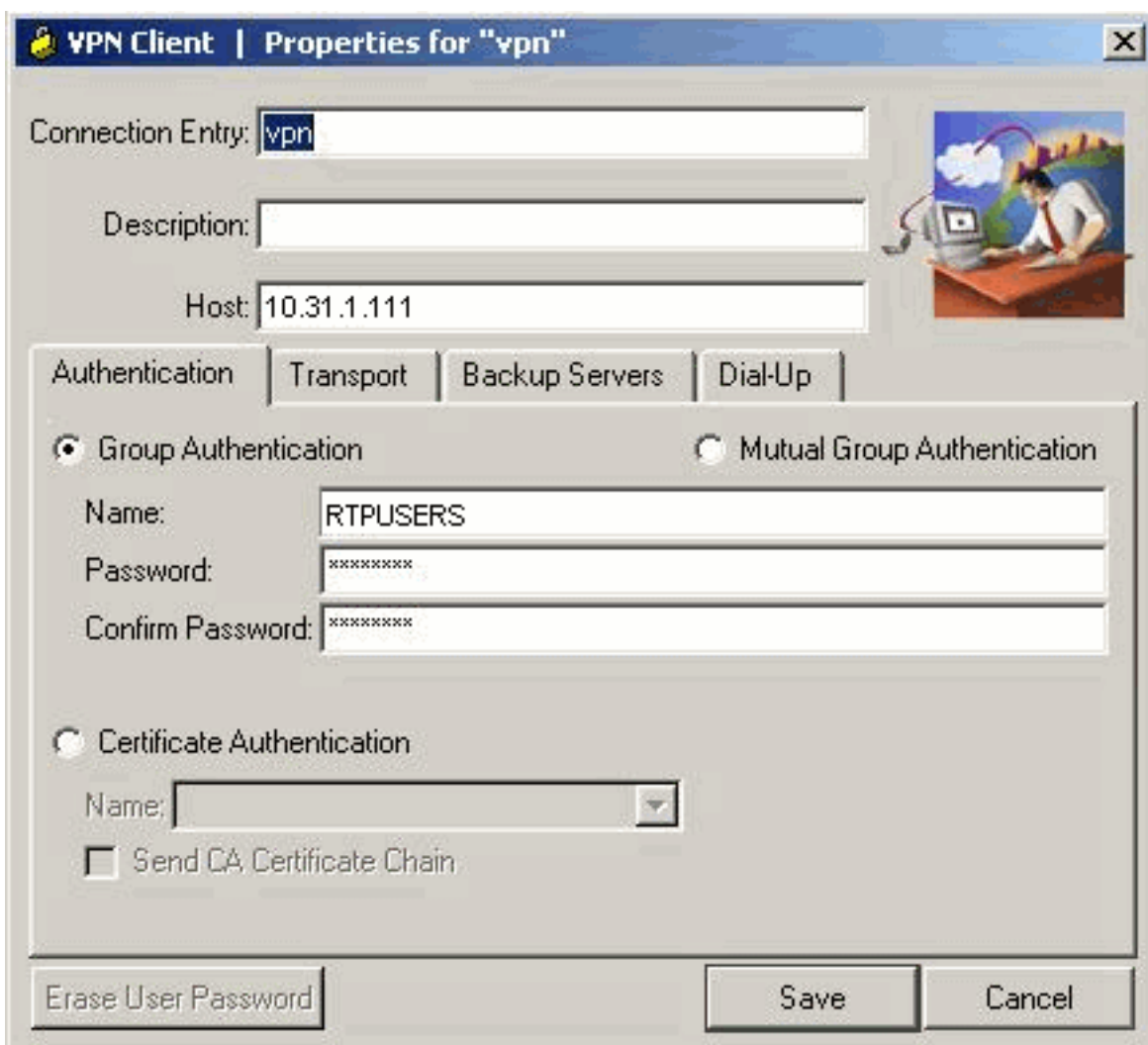
Configuração de VPN Client 4.8

Conclua estes passos para configurar o VPN Client 4.8:

1. Escolha **Iniciar > Programas > Cisco Systems VPN Client > VPN Client**.
2. Clique em **New** para iniciar a janela Create New VPN Connection Entry.

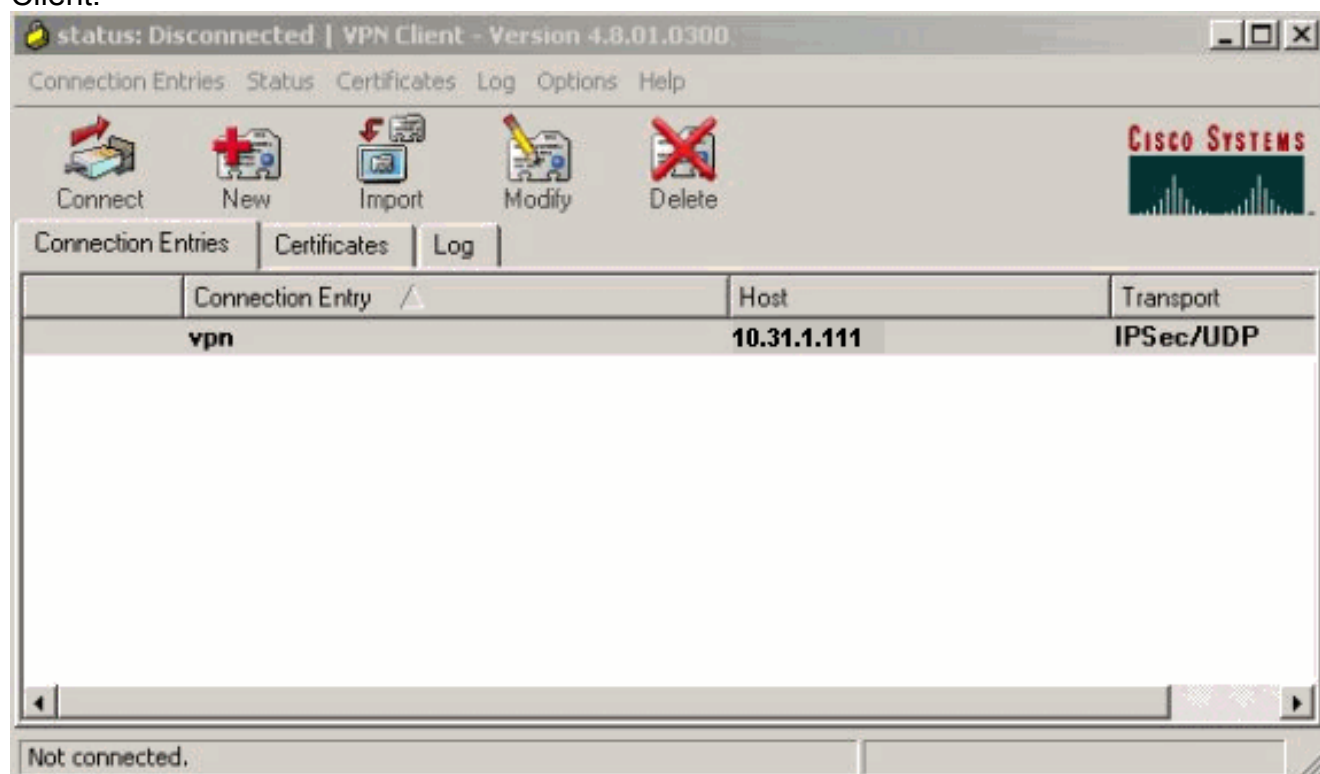


3. Insira o nome da entrada do Connection junto com uma descrição. Insira o endereço IP externo do roteador na caixa Host. Em seguida, digite o nome e a senha do grupo VPN e clique em

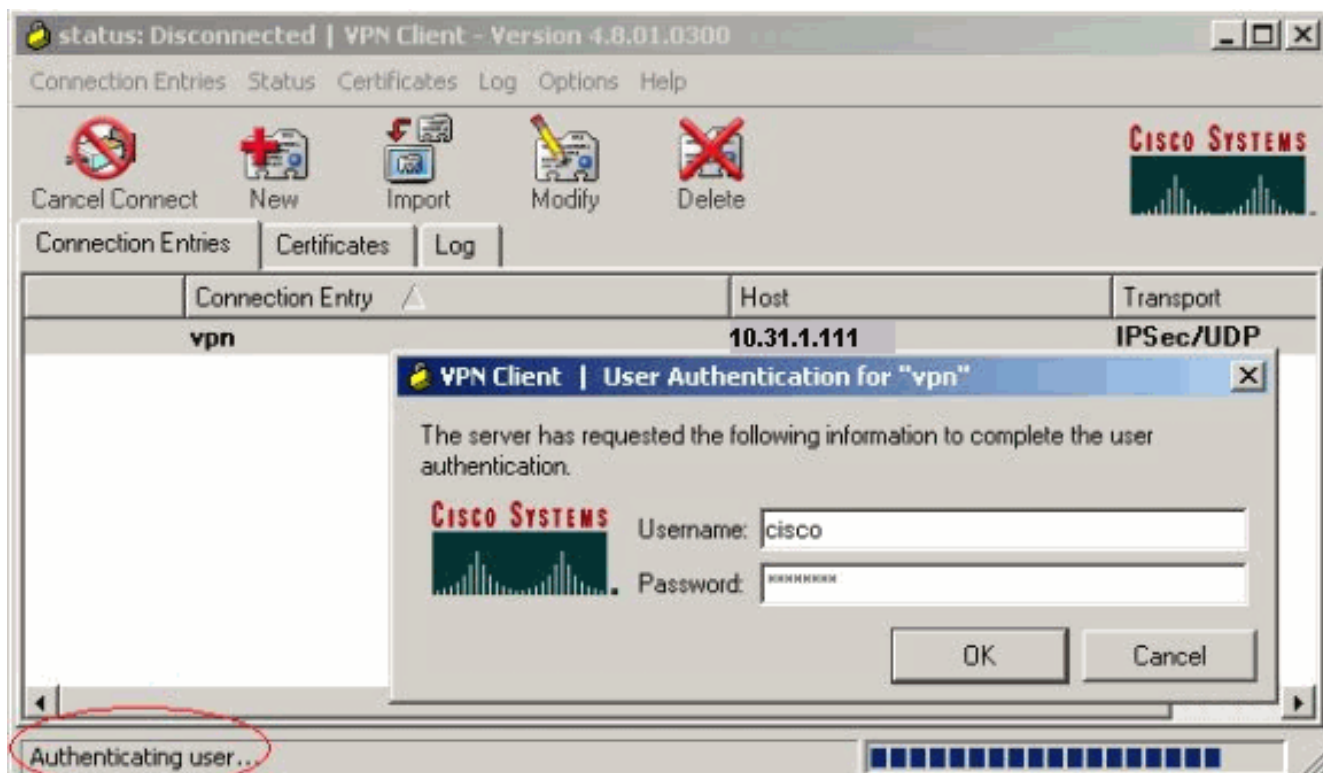


Salvar.

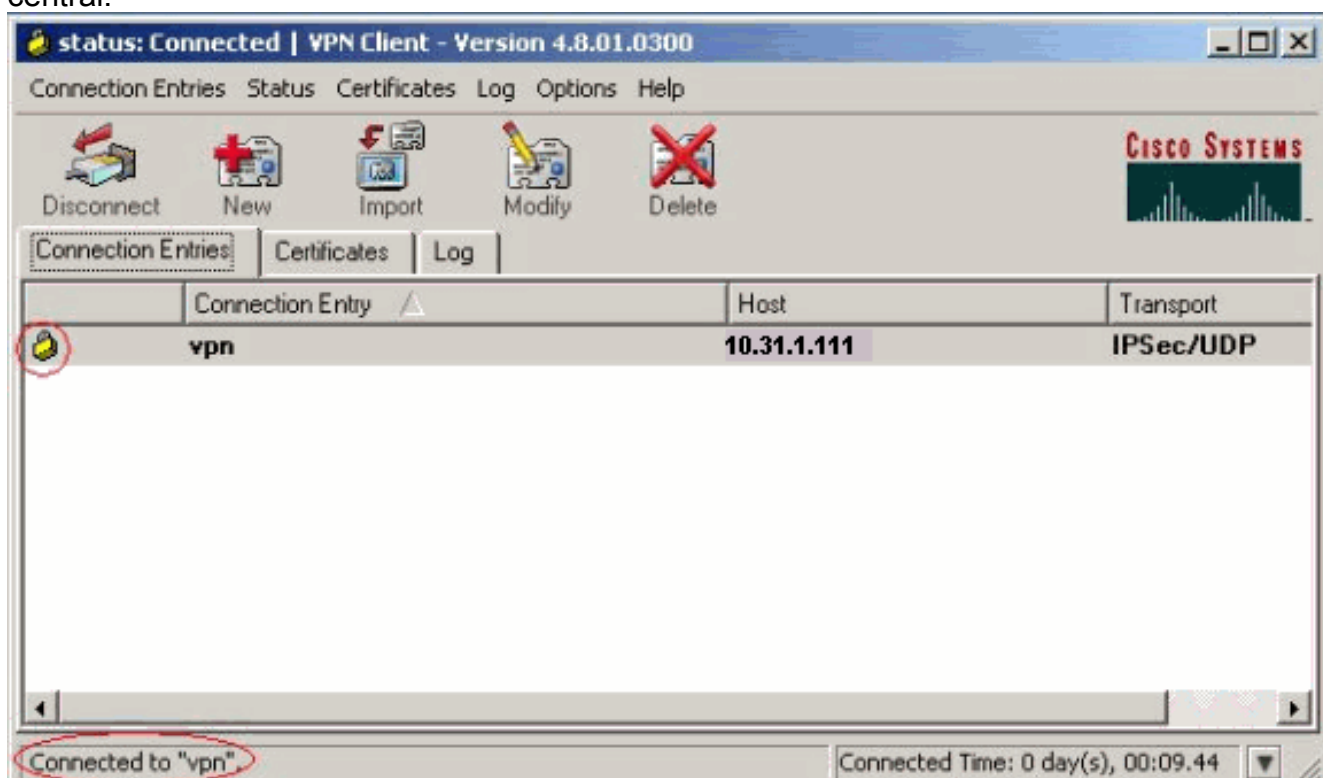
4. Clique na conexão que deseja usar e clique em **Connect** na janela principal do VPN Client.



5. Quando solicitado, introduza o nome de usuário e senha para Xauth e clique em OK para conectar-se à rede remota.



O VPN Client é conectado ao roteador no local central.



Configurar o servidor TACACS+ usando o Cisco Secure ACS

Conclua estes passos para configurar o TACACS+ em um Cisco Secure ACS:

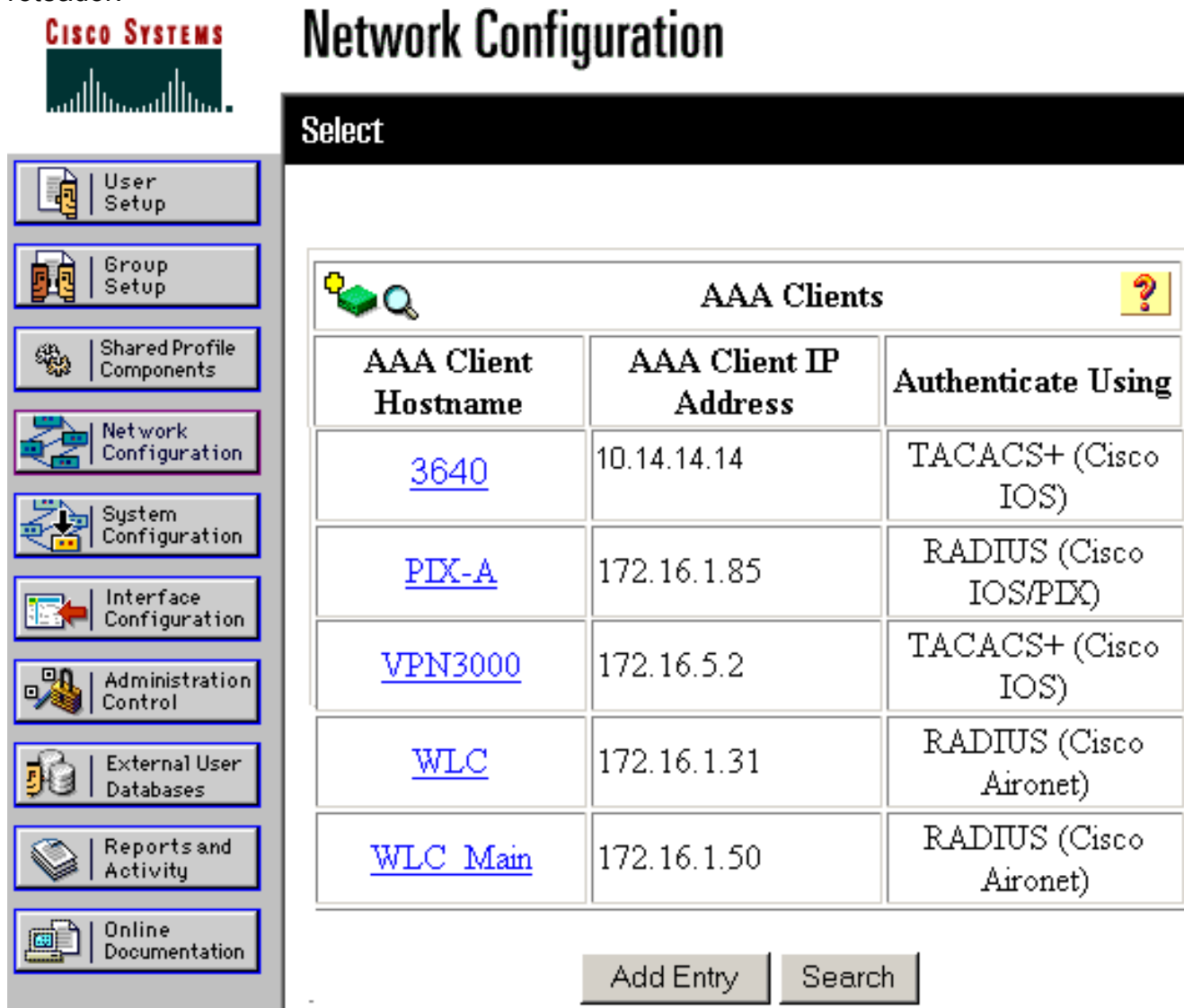
1. Você deve configurar o roteador para localizar o Cisco Secure ACS para verificar as credenciais do usuário. Por exemplo:

```
3640 (config) #
```

```
aaa group server tacacs+ RTP
```

```
3640 (config) #
```

2. Escolha **Network Configuration** à esquerda e clique em **Add Entry** para adicionar uma entrada para o roteador no banco de dados do servidor TACACS+. Escolha o banco de dados do servidor de acordo com a configuração do roteador.



CISCO SYSTEMS

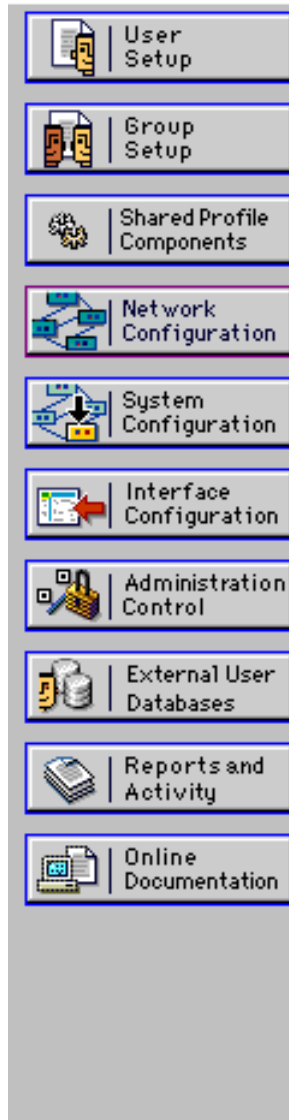
Network Configuration

Select

| AAA Client Hostname | AAA Client IP Address | Authenticate Using |
|--------------------------|-----------------------|------------------------|
| 3640 | 10.14.14.14 | TACACS+ (Cisco IOS) |
| PIX-A | 172.16.1.85 | RADIUS (Cisco IOS/PDX) |
| VPN3000 | 172.16.5.2 | TACACS+ (Cisco IOS) |
| WLC | 172.16.1.31 | RADIUS (Cisco Aironet) |
| WLC Main | 172.16.1.50 | RADIUS (Cisco Aironet) |

Add Entry Search

3. A chave é usada para autenticar entre o 3640 Router e o Cisco Secure ACS Server. Se quiser selecionar o protocolo TACACS+ para autenticação, escolha **TACACS+ (Cisco IOS)** no menu suspenso Authenticate Using (Autenticar usando).



Add AAA Client

| | |
|--------------------------|---|
| AAA Client Hostname | <input type="text" value="3640"/> |
| AAA Client IP Address | <input type="text" value="10.14.14.14"/> |
| Key | <input type="text" value="cisco123"/> |
| Authenticate Using | <input type="text" value="TACACS+ (Cisco IOS)"/> |
| <input type="checkbox"/> | Single Connect TACACS+ AAA Client (Record stop in accounting on failure). |
| <input type="checkbox"/> | Log Update/Watchdog Packets from this AAA Client |
| <input type="checkbox"/> | Log RADIUS Tunneling Packets from this AAA Client |
| <input type="checkbox"/> | Replace RADIUS Port info with Username from this AAA Client |

Submit

Submit + Restart

Cancel

4. Insira o nome de usuário no campo Usuário no banco de dados Cisco Secure e clique em **Adicionar/Editar**. Neste exemplo, o nome de usuário é rtpuser.



User Setup

Select

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

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](#)

5. Na próxima janela, digite a senha para colocar. Neste exemplo, a senha é rtpuserpass. É possível mapear a conta de usuário para um grupo, se desejado. Quando terminar, clique em Submit.



User Setup

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

Supplementary User Info

Real Name:

Description:

User Setup

Password Authentication:

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

Configurar o recurso de retorno

Quando o servidor RADIUS primário se tornar indisponível, o roteador realizará failover para o próximo servidor RADIUS de backup ativo. O roteador continuará a usar o servidor RADIUS secundário para sempre, mesmo que o servidor primário esteja disponível. Geralmente, o servidor primário é de alto desempenho e o preferido. Se o servidor secundário não estiver disponível, o banco de dados local pode ser usado para autenticação usando o comando [aaa authentication login default group RTP local](#).

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

Estabeleça um túnel IPSec entre o PC e o Cisco 3640 Router.

Abra um navegador no PC e aponte-o para <http://10.17.17.17>. O Cisco 3640 Router intercepta esse tráfego HTTP, aciona o proxy de autenticação e solicita um nome de usuário e uma senha. O Cisco 3640 envia o nome de usuário/senha para o servidor TACACS+ para autenticação. Se a autenticação for bem-sucedida, você poderá ver as páginas da Web no servidor Web em 10.17.17.17.

A [Output Interpreter Tool \(somente clientes registrados\) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.](#)

- [show ip access-lists](#) —Exibe as ACLs padrão e estendidas configuradas no roteador de firewall (inclui entradas de ACL dinâmicas). As entradas dinâmicas da ACL são adicionadas e removidas periodicamente com base na autenticação ou não do usuário. Esta saída mostra a lista de acesso 118 antes do proxy de autenticação ter sido disparado:

```
3640#show ip access-lists 118
Extended IP access list 118
 10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (321 matches)
 20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (276 matches)
 30 permit tcp host 10.14.14.3 host 10.31.1.111 (174 matches)
```

Esta saída mostra a lista de acesso 118 depois que o proxy de autenticação foi acionado e o usuário autentica com êxito:

```
3640#show ip access-lists 118
Extended IP access list 118
permit tcp host 10.20.20.26 any (7 matches)
permit udp host 10.20.20.26 any (14 matches)
permit icmp host 10.20.20.26 any
 10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (379 matches)
 20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (316 matches)
 30 permit tcp host 10.14.14.3 host 10.31.1.111 (234 matches)
```

As três primeiras linhas da lista de acesso são as entradas definidas para esse usuário e baixadas do servidor TACACS+.

- [show ip auth-proxy cache](#) —Exibe as entradas de proxy de autenticação ou a configuração de proxy de autenticação em execução. A palavra-chave cache para listar o endereço IP do host, o número da porta de origem, o valor de tempo limite para o proxy de autenticação e o estado das conexões que usam proxy de autenticação. Se o estado do proxy de autenticação for ESTAB, a autenticação do usuário será um sucesso.

```
3640#show ip auth-proxy cache
Authentication Proxy Cache
Client IP 10.20.20.26 Port 1705, timeout 5, state ESTAB
```

Troubleshoot

Para obter os comandos de verificação e depuração, juntamente com outras informações de solução de problemas, consulte [Proxy de Autenticação de Troubleshooting](#).

Observação: antes de inserir o comando **debug**, consulte [Informações importantes sobre os comandos debug](#).

Informações Relacionadas

- [Configurando o proxy de autenticação](#)

- [Configurações de proxy de autenticação no Cisco IOS](#)
- [Implementando o proxy de autenticação em servidores TACACS+ e RADIUS](#)
- [Página de Suporte do Cisco VPN Client](#)
- [Página de suporte de firewall do IOS](#)
- [Página de suporte do IPSec](#)
- [Página de suporte RADIUS](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Página de Suporte do TACACS/TACACS+](#)
- [TACACS+ na Documentação do IOS](#)
- [Suporte Técnico - Cisco Systems](#)