

# IOS 路由器：带ACS for IPSec的认证代理验证入站与和VPN客户端配置

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[VPN 客户端 4.8 配置](#)

[使用 Cisco Secure ACS 配置 TACACS+ 服务器](#)

[配置后退功能](#)

[验证](#)

[故障排除](#)

[相关信息](#)

## 简介

认证代理功能允许用户登录到网络或通过 HTTP 访问互联网，并会自动从 TACACS+ 或 RADIUS 服务器检索并应用其特定的访问配置文件。只有验证的用户有活动的流量时，用户配置文件才是有效的。

此配置旨在在 10.1.1.1 上启用 Web 浏览器，并将其目标定为 10.17.17.17。由于 VPN 客户端配置为通过隧道端点 10.31.1.11 到达 10.17.17.x 网络，因此 IPSec 隧道是并且 PC 从池 RTP-POOL 获取 IP 地址（因为执行了模式配置）。然后，Cisco 3640 路由器会请求进行认证。用户输入用户名和口令（存储在 10.14.14.3 处的 TACACS+ 服务器上）之后，会将从服务器向下传递的访问列表添加到访问列表 118。

## 先决条件

## 要求

在尝试此配置前，请保证您符合这些要求：

- Cisco VPN 客户端配置为与 Cisco 3640 路由器之间建立 IPSec 隧道。
- TACACS+ 服务器配置用于认证代理。有关详细信息，请参阅“相关信息”部分。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS?软件版本12.4
- Cisco 3640 路由器
- Cisco VPN 客户端 for Windows 4.8 版 ( 所有 VPN 客户端 4.x 和更高版本均应适用 )

**注意：**在Cisco IOS软件版本12.0.5.T中引入了ip auth-proxy命令。已使用 Cisco IOS 软件版本 12.4 对此配置进行了测试。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 ( 默认 ) 配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

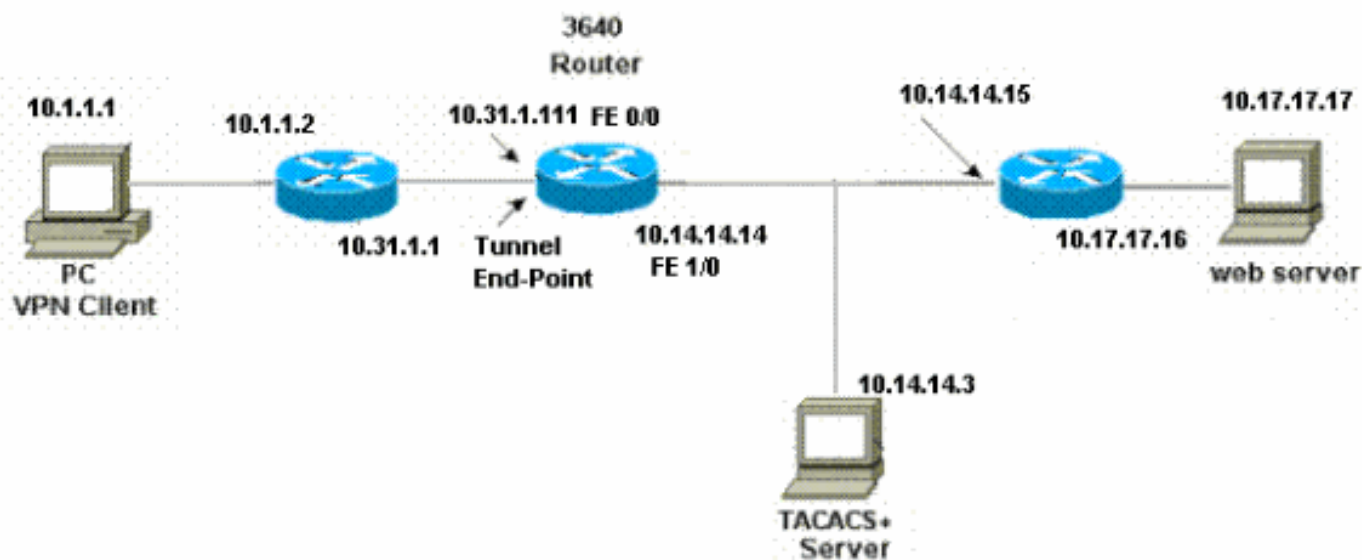
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注：**要查找有关本文档中使用的命令的其他信息，请使用命令[查找工具](#)([仅注册客户](#))。

## 网络图

本文档使用以下网络设置：



## 配置

### 3640路由器

```
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

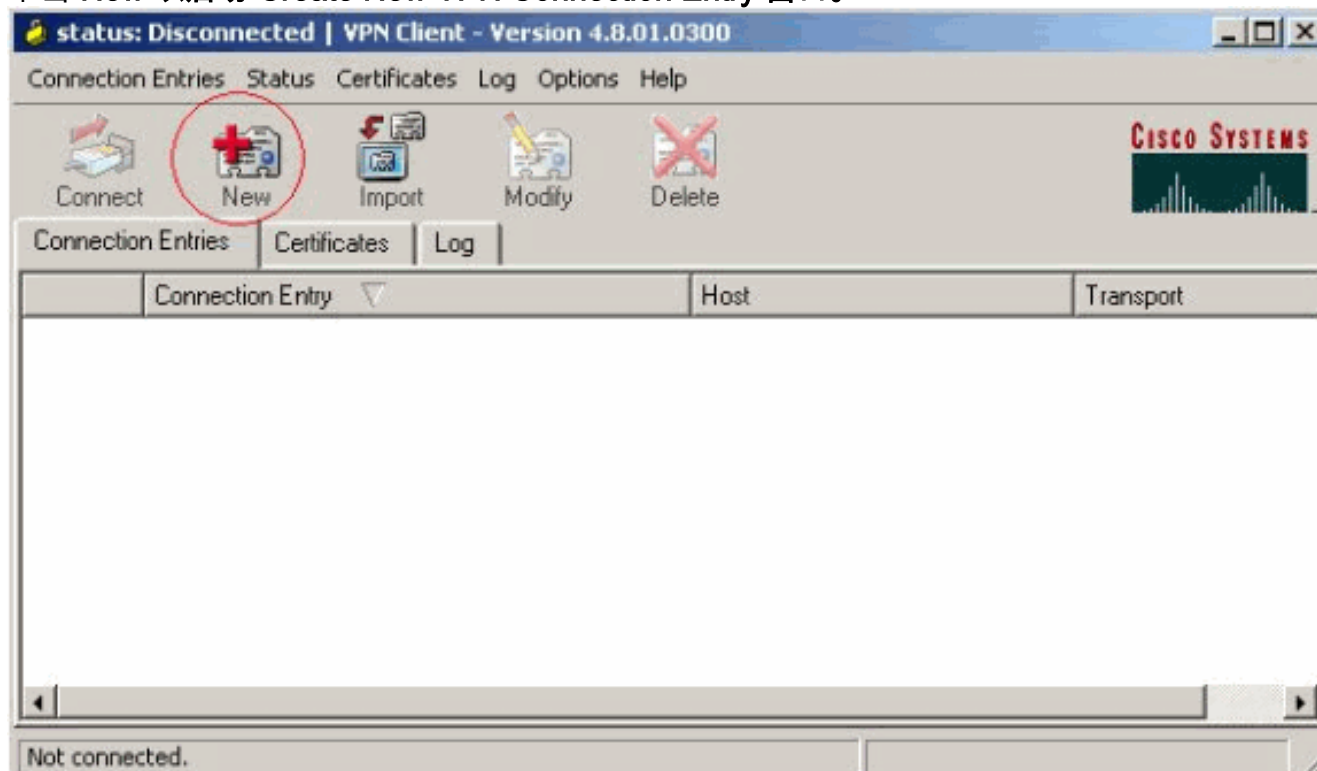
!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPsec
packets !--- to enable the Cisco VPN Client to establish
the IPsec tunnel. !--- The last line of the access-list
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
```

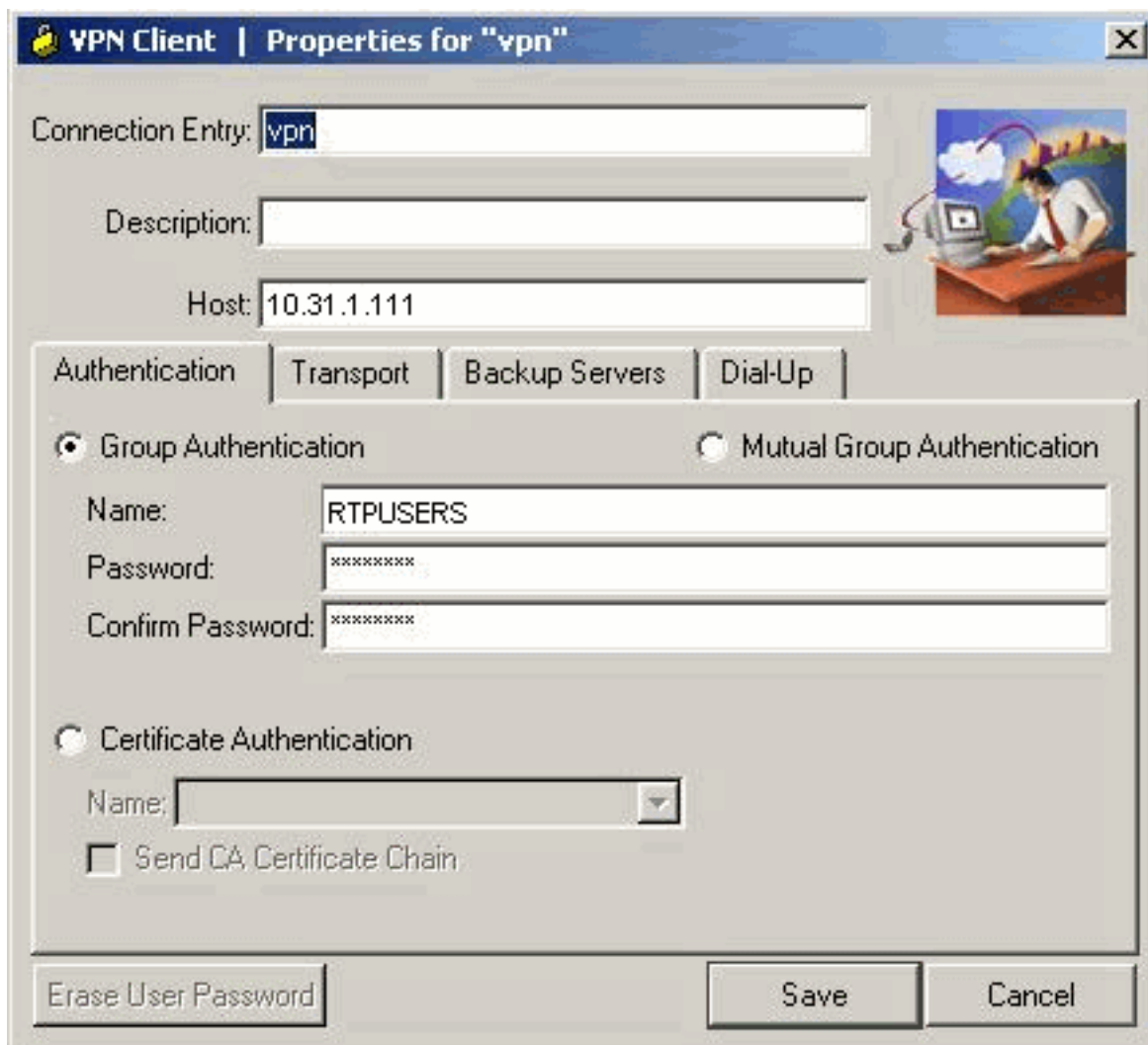
## VPN 客户端 4.8 配置

完成下列步骤以配置 VPN Client 4.8 :

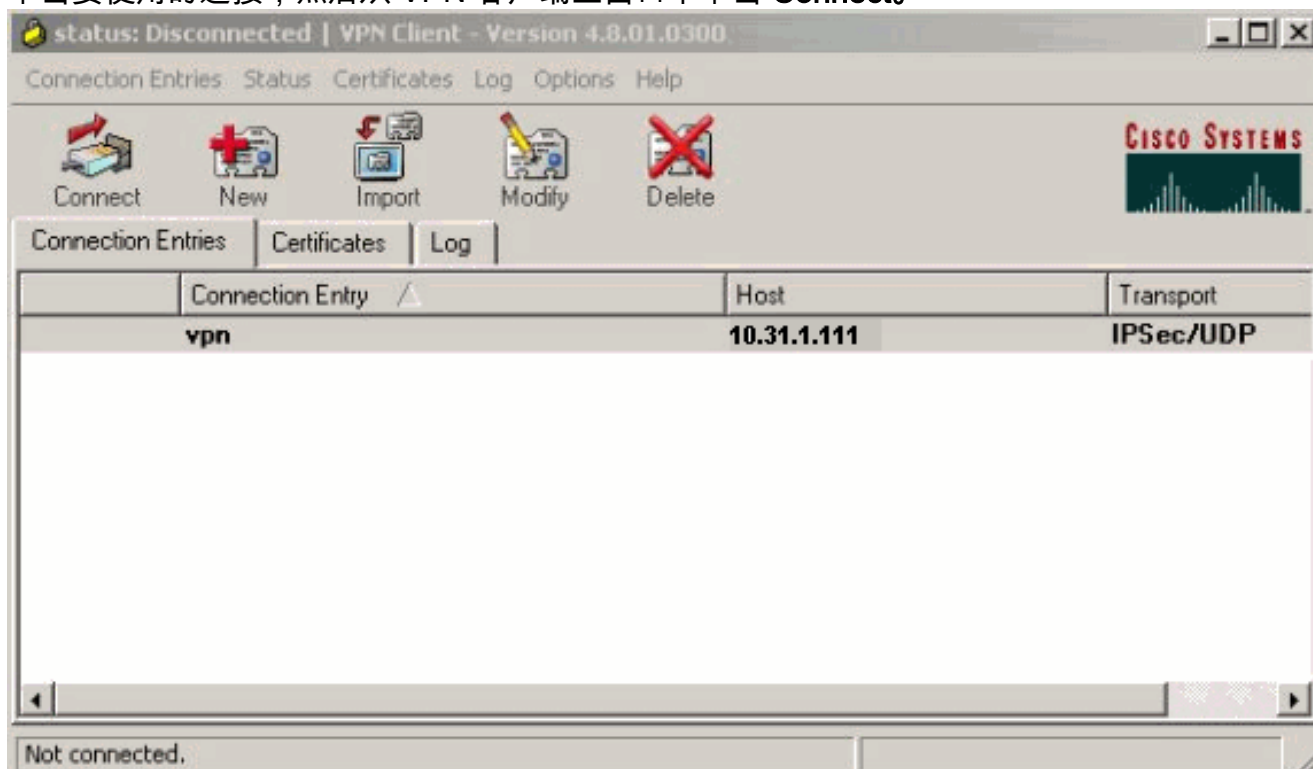
1. 选择开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端。
2. 单击 **New** 以启动 **Create New VPN Connection Entry** 窗口。



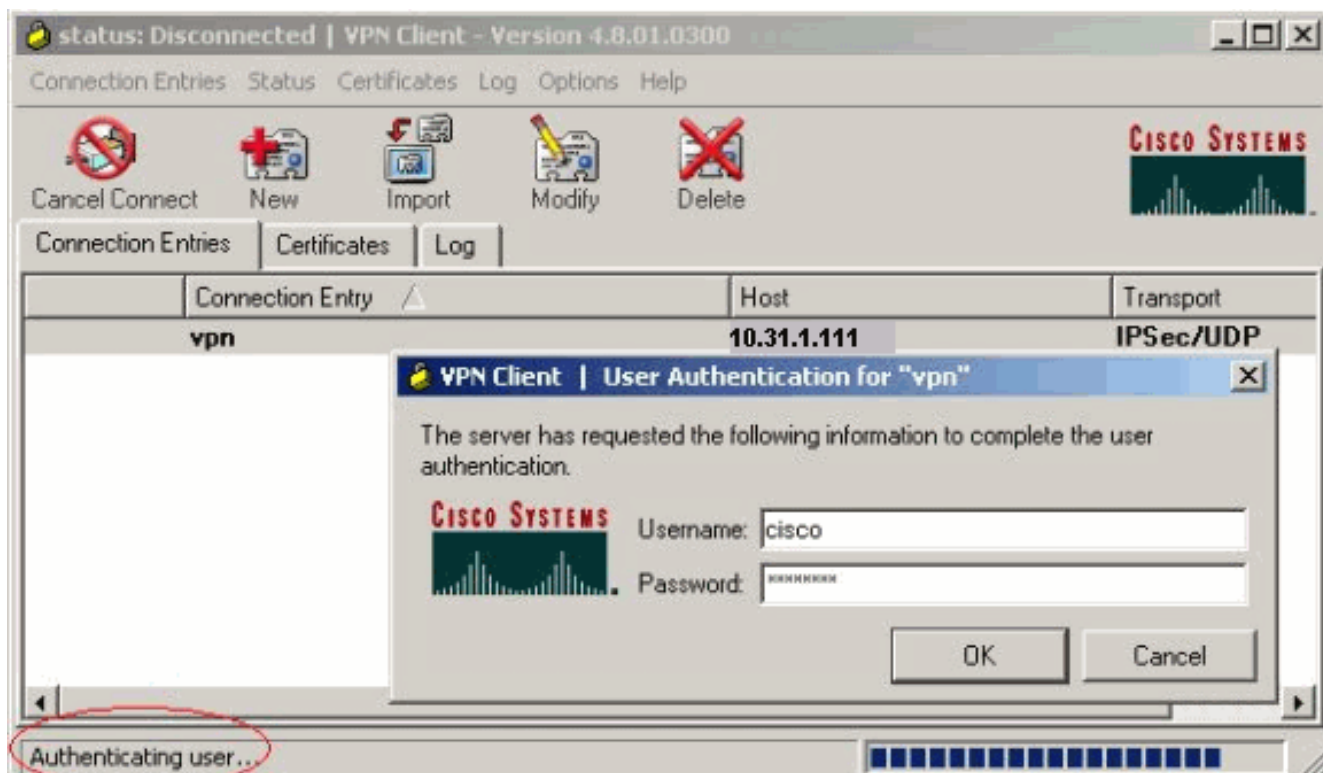
3. 输入 Connection Entry 的名称与说明。在“Host”框中输入路由器的外部 IP 地址。然后输入 VPN 组名称和口令，并单击 **Save**。



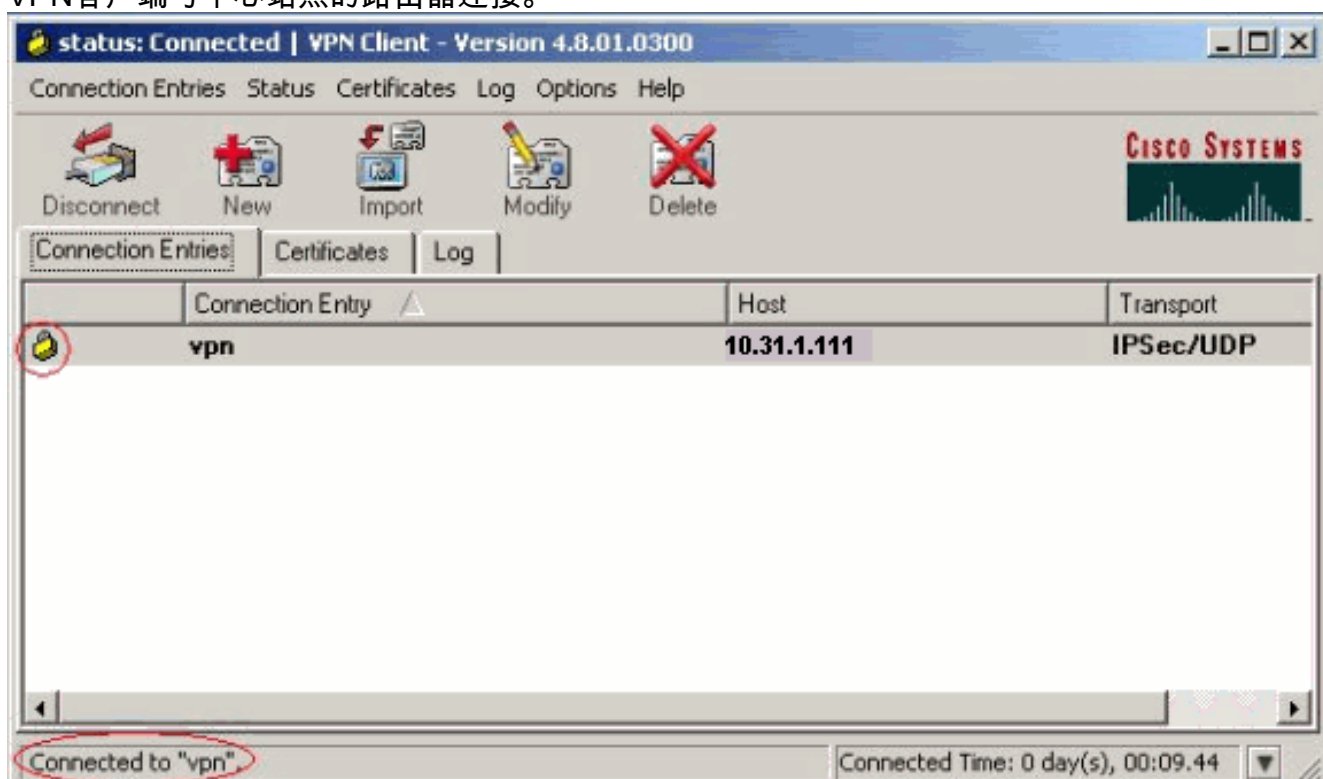
4. 单击要使用的连接，然后从 VPN 客户端主窗口中单击 **Connect**。



5. 出现提示时，输入用于 xauth 的 Username 和 Password 信息，然后单击 OK 以连接远程网络。



VPN客户端与中心站点的路由器连接。



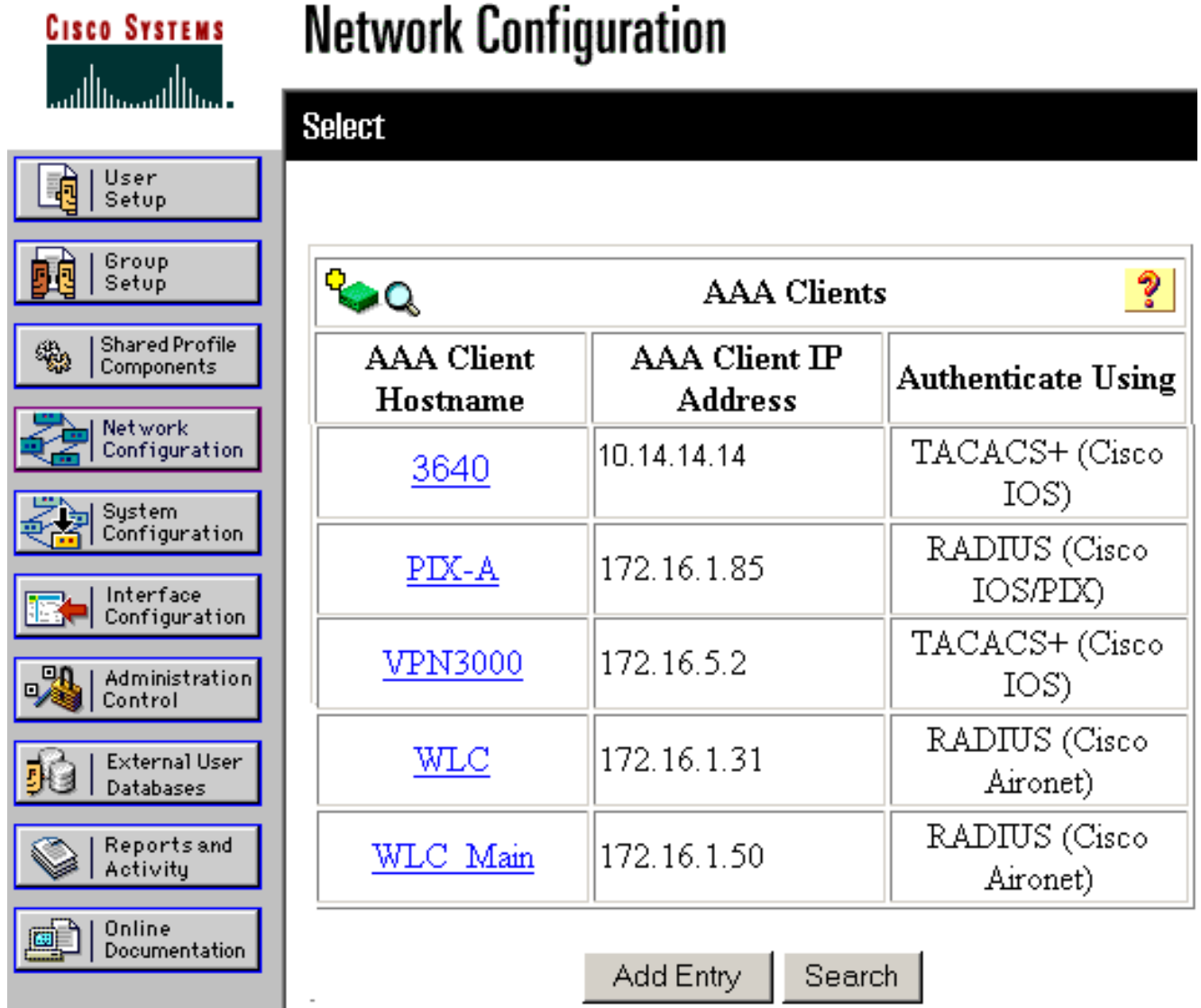
## 使用 Cisco Secure ACS 配置 TACACS+ 服务器

完成下列步骤以便在 Cisco Secure ACS 中配置 TACACS+ :

1. 您必须将路由器配置为查找 Cisco Secure ACS , 以检查用户凭据。例如 :

```
3640(config)#  
aaa group server tacacs+ RTP  
3640(config)#  
tacacs-server host 10.14.14.3 key cisco
```

2. 在左侧选择 Network Configuration，然后单击 Add Entry，在任一 TACACS+ 服务器数据库中为路由器添加一个条目。根据路由器配置选择服务器数据库。

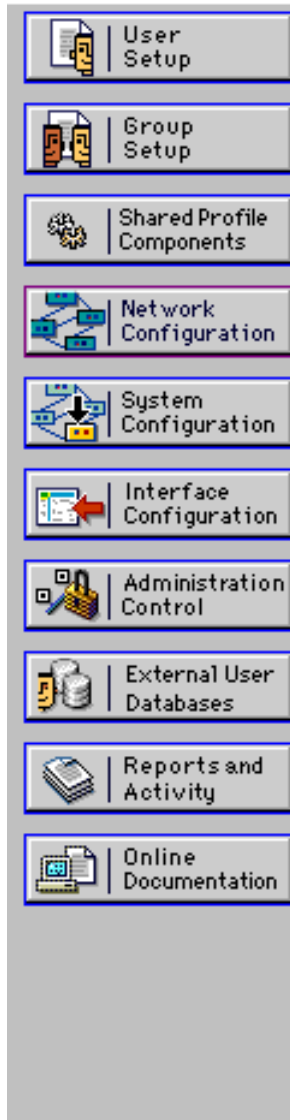


The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled 'Select' and displays a table of AAA Clients. The table has three columns: AAA Client Hostname, AAA Client IP Address, and Authenticate Using. Below the table are 'Add Entry' and 'Search' buttons.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">3640</a>	10.14.14.14	TACACS+ (Cisco IOS)
<a href="#">PIX-A</a>	172.16.1.85	RADIUS (Cisco IOS/PDX)
<a href="#">VPN3000</a>	172.16.5.2	TACACS+ (Cisco IOS)
<a href="#">WLC</a>	172.16.1.31	RADIUS (Cisco Aironet)
<a href="#">WLC Main</a>	172.16.1.50	RADIUS (Cisco Aironet)

3. 密钥用于在 3640 路由器与 Cisco Secure ACS 服务器之间进行认证。如果要选择 TACACS+ 协议进行身份验证，则在 Authenticate Using 下拉菜单中选择 TACACS+ (Cisco IOS)。



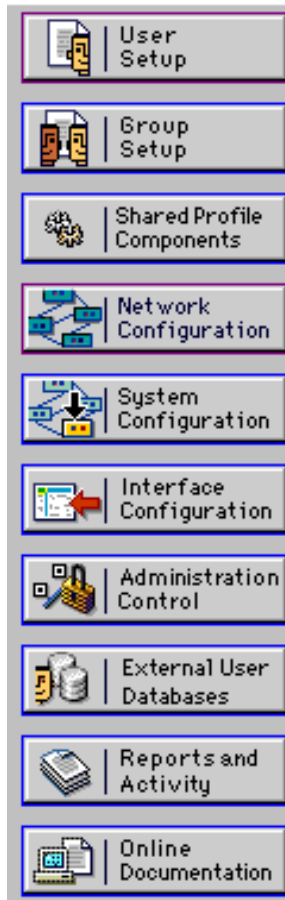


## Add AAA Client

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	

4. 在 User 字段中，输入 Cisco Secure 数据库中的用户名，然后单击 **Add/Edit**。在本例中，用户名为 rtuser。

## 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](#)

5. 在下一个窗口中，输入 rtuser 的口令。在本例中，口令为 rtuserpass。如果需要，可将用户帐户映射到组。完成后，单击 **Submit**。



在PC上打开浏览器并将其指向<http://10.17.17.17>。Cisco 3640路由器拦截此HTTP流量，触发身份验证代理，并提示您输入用户名和密码。Cisco 3640 会将用户名/口令发送到 TACACS+ 服务器以进行认证。如果认证成功，您应该能够在 10.17.17.17 处看到 Web 服务器的网页。

[命令输出解释程序工具 \(仅限注册用户\) 支持某些 show 命令](#)，使用此工具可以查看对 show 命令输出的分析。

- [show ip access-lists](#) — 显示在防火墙路由器上配置的标准和扩展 ACL (包括动态 ACL 条目)。动态 ACL 条目会根据是否进行用户身份验证来定期添加和删除。此输出会在认证代理触发之前显示访问列表 118。

```
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)
```

此输出会在认证代理触发且用户认证成功后显示访问列表 118。

```
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)
```

访问列表的前三行是针对此用户定义并从 TACACS+ 服务器下载的题目。

- [show ip auth-proxy cache](#) - 显示认证代理条目或运行中的认证代理配置。缓存关键字，用于列出主机 IP 地址、源端口号、认证代理超时值以及使用认证代理的连接的状态。如果认证代理状态为“ESTAB”，则表示用户身份验证成功。

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

## 故障排除

有关验证和调试命令以及其他故障排除信息，请参阅[对认证代理进行故障排除](#)。

注意：在发出debug命令之前，请[参阅有关Debug命令的重要信息](#)。

## 相关信息

- [配置认证代理](#)
- [Cisco IOS 中的认证代理配置](#)
- [在 TACACS+ 和 RADIUS 服务器中实施认证代理](#)
- [Cisco VPN 客户端支持页](#)
- [IOS防火墙支持页面](#)
- [IPSec 支持页面](#)
- [RADIUS 支持页](#)
- [请求注解 \(RFC\)](#)
- [TACACS/TACACS+支持页面](#)
- [IOS 文档中的 TACACS+](#)
- [技术支持 - Cisco Systems](#)