

# IOS路由器：用於IPSec和VPN客戶端配置的使用ACS的入站身份驗證代理身份驗證

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[組態](#)

[VPN客戶端4.8配置](#)

[使用Cisco Secure ACS配置TACACS+伺服器](#)

[配置回退功能](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

驗證代理功能允許使用者登入網路或透過HTTP存取網際網路，並自動從TACACS+或RADIUS伺服器擷取和應用其特定存取設定檔。僅當存在來自已驗證使用者的活動流量時，使用者配置檔案才處於活動狀態。

此配置設計為在10.1.1.1上啟用Web瀏覽器，並將目標設為10.17.17.17。由於VPN客戶端配置為通過隧道端點10.31.1.111到達10.17.17.x網路，因此會構建IPSec隧道，並且PC會從池RTP-POOL獲取IP地址（因為執行模式配置）。然後，Cisco 3640路由器會請求身份驗證。使用者輸入使用者名稱和密碼後（儲存在10.14.14.3處的TACACS+伺服器上），從伺服器向下傳遞的存取清單會新增到存取清單118中。

## 必要條件

## 需求

嘗試此設定之前，請確保符合以下要求：

- Cisco VPN客戶端配置為與Cisco 3640路由器建立IPSec隧道。
- TACACS+伺服器已配置為身份驗證代理。有關詳細資訊，請參閱「相關資訊」部分。

## 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS?軟體版本12.4
- 思科3640路由器
- 適用於Windows版本4.8的Cisco VPN客戶端 ( 任何VPN客戶端4.x及更高版本都應工作 )

**注意：** ip auth-proxy指令是在Cisco IOS軟體版本12.0.5中匯入，此配置已使用Cisco IOS軟體版本12.4進行測試。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

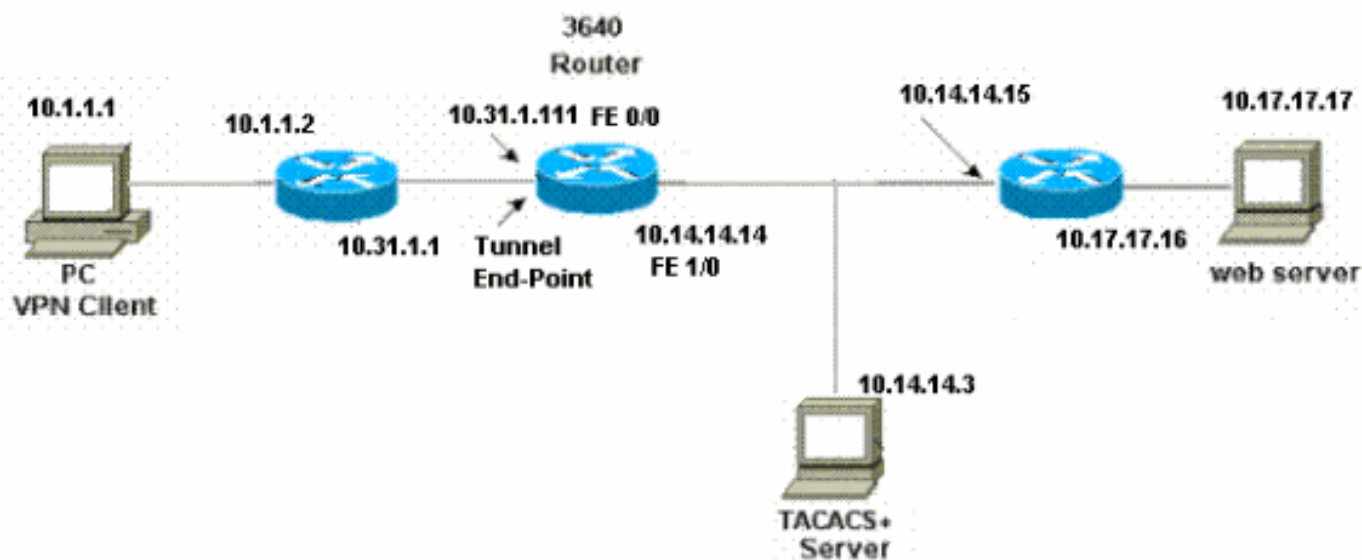
## 設定

本節提供用於設定本文件中所述功能的資訊。

**注意：** 要查詢有關本文檔中使用的命令的其他資訊，請使用[命令查詢工具](#)([僅限註冊客戶](#))。

## 網路圖表

本檔案會使用以下網路設定：



## 組態

### 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

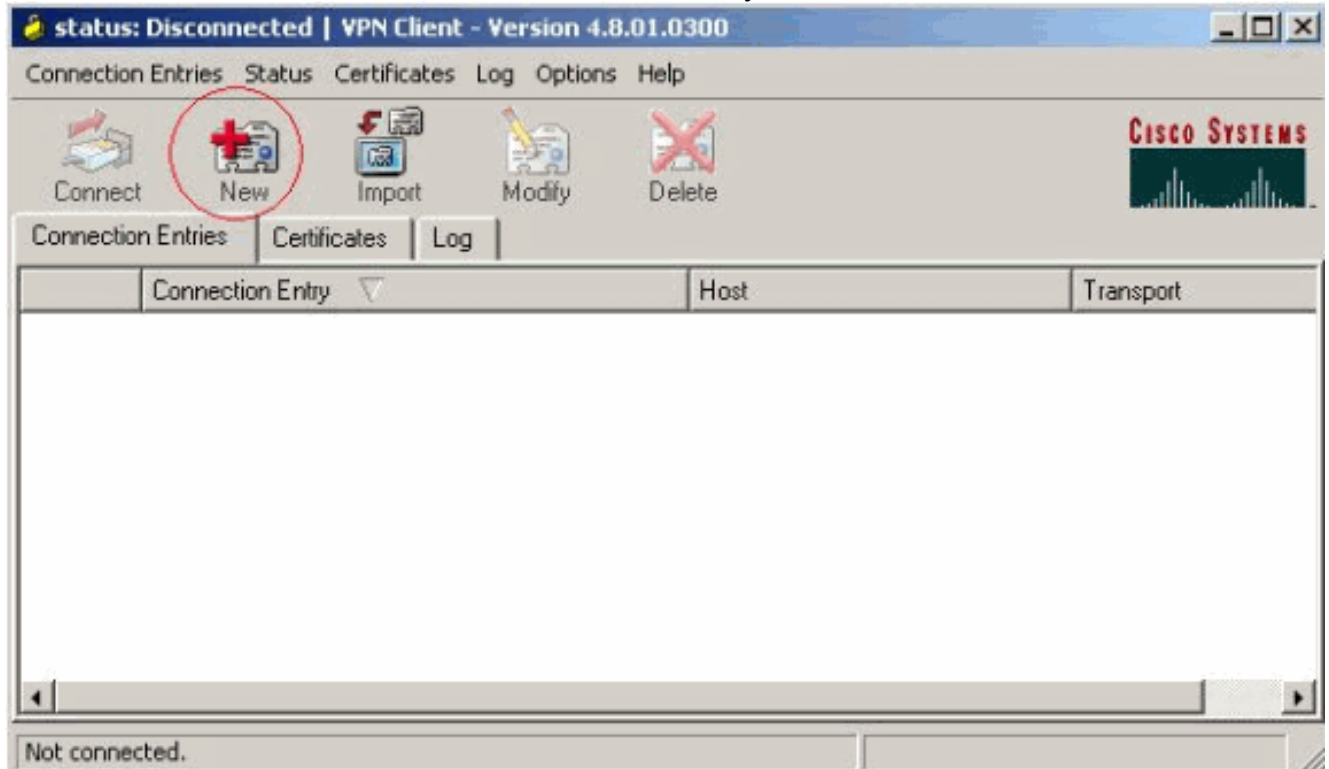
!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPsec
packets !--- to enable the Cisco VPN Client to establish
the IPsec tunnel. !--- The last line of the access-list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

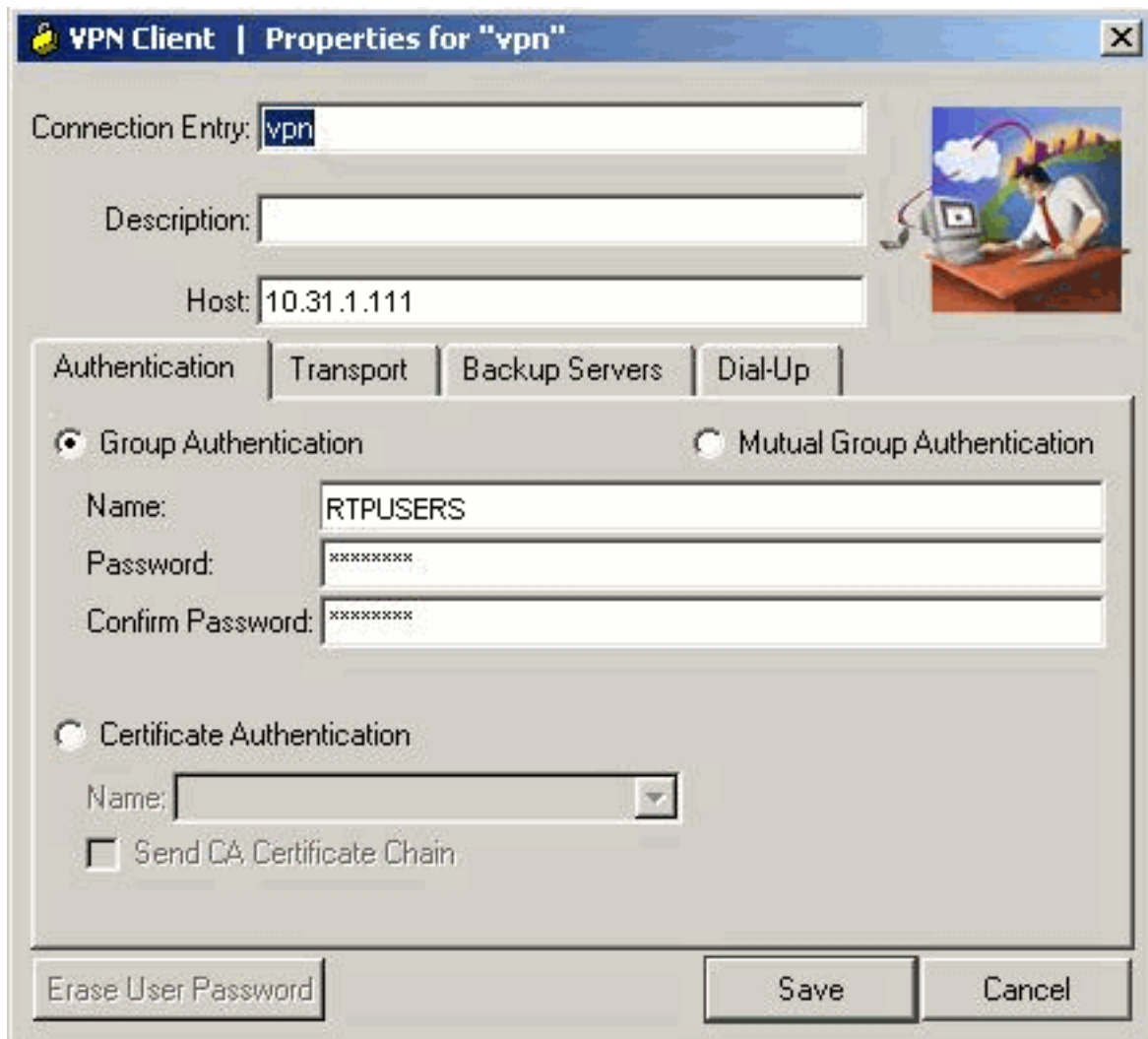
## VPN客戶端4.8配置

完成以下步驟以配置VPN客戶端4.8:

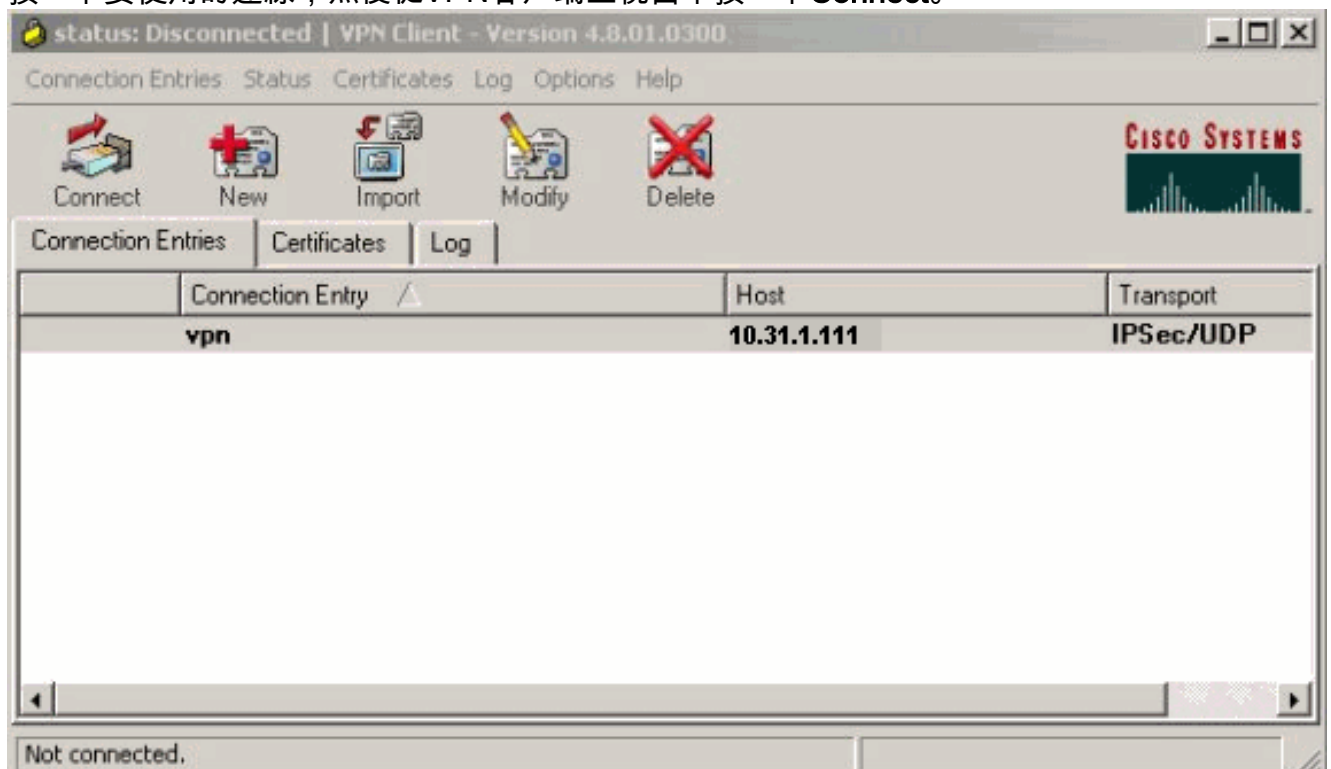
1. 選擇**Start > Programs > Cisco Systems VPN Client > VPN Client**。
2. 按一下**New**以啟動Create New VPN Connection Entry視窗。



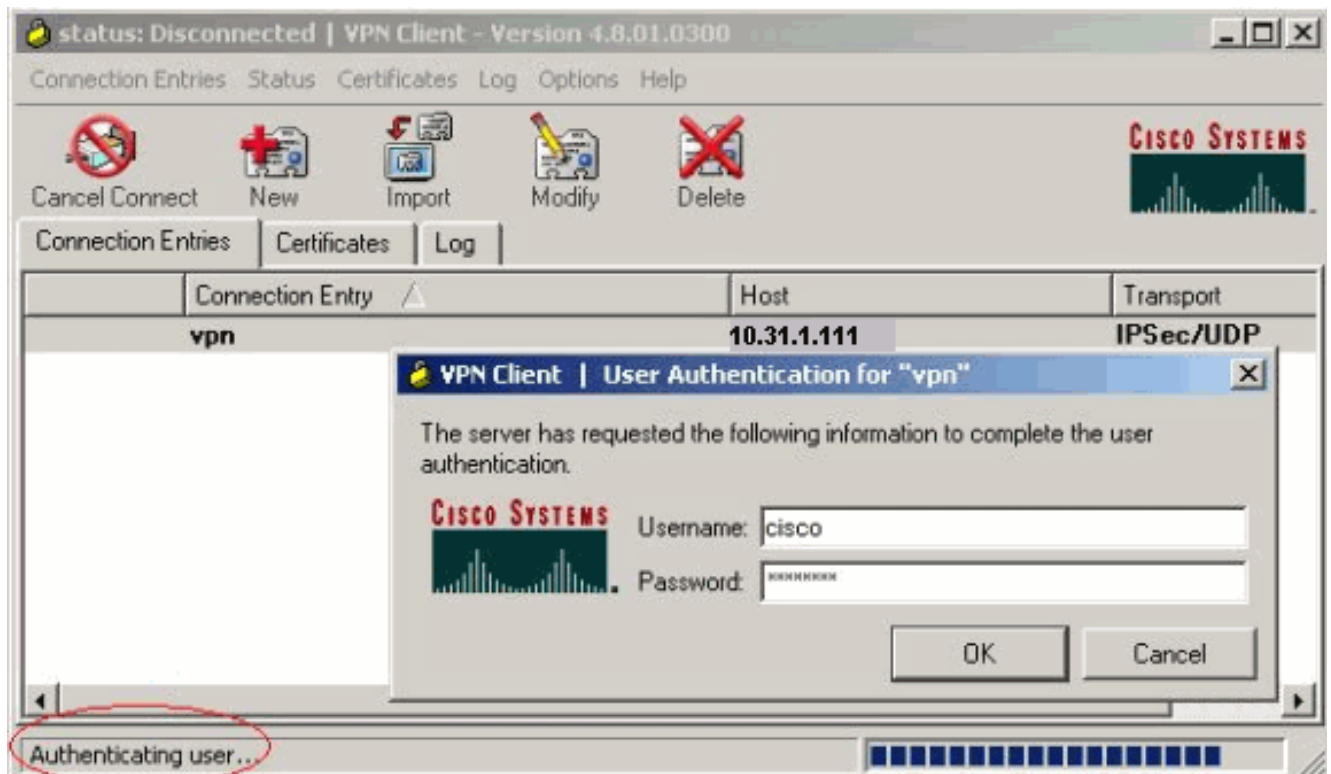
3. 輸入連線條目的名稱和說明。在Host (主機) 框中輸入路由器的外部IP地址。然後輸入VPN組名稱和密碼，然後按一下**Save**。



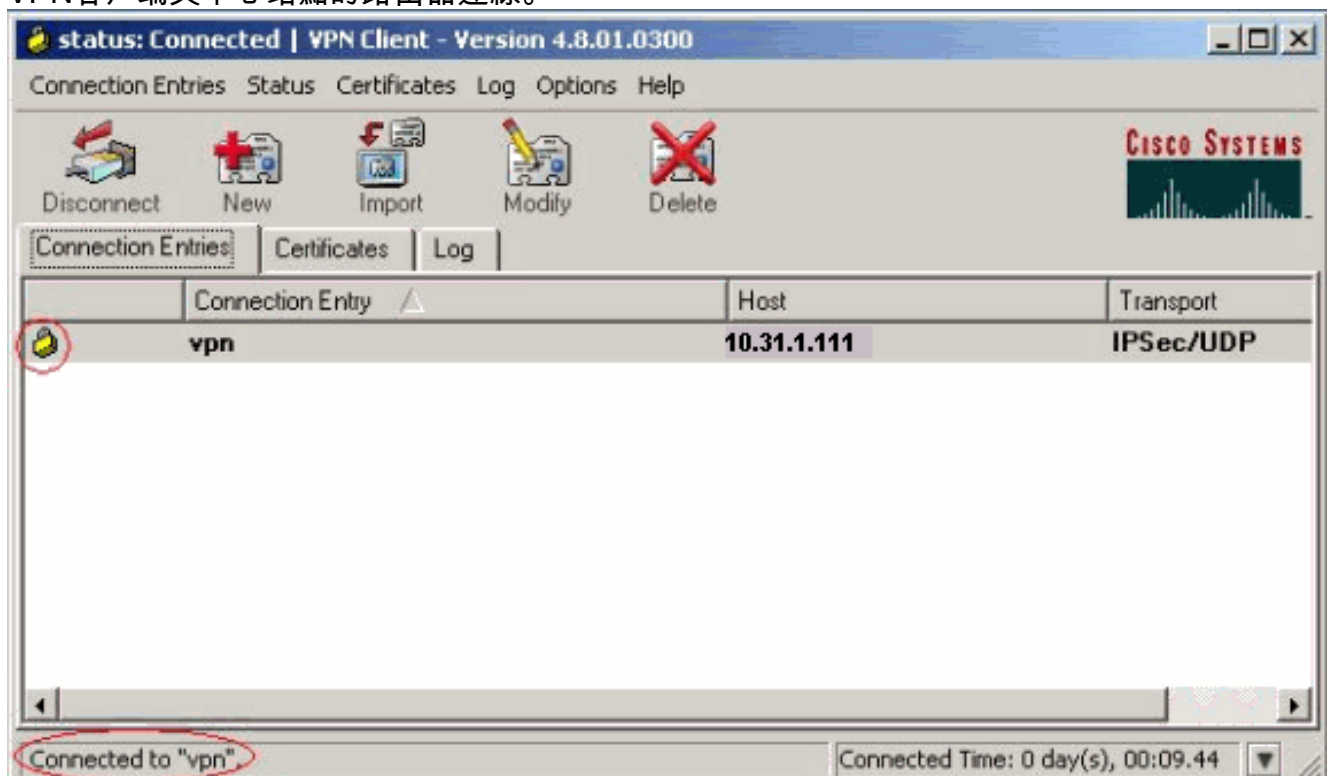
4. 按一下要使用的連線，然後從VPN客戶端主視窗中按一下**Connect**。



5. 出現提示時，輸入xauth的使用者名稱和密碼資訊，然後按一下**OK**連線到遠端網路。



VPN客戶端與中心站點的路由器連線。



## 使用Cisco Secure ACS配置TACACS+伺服器

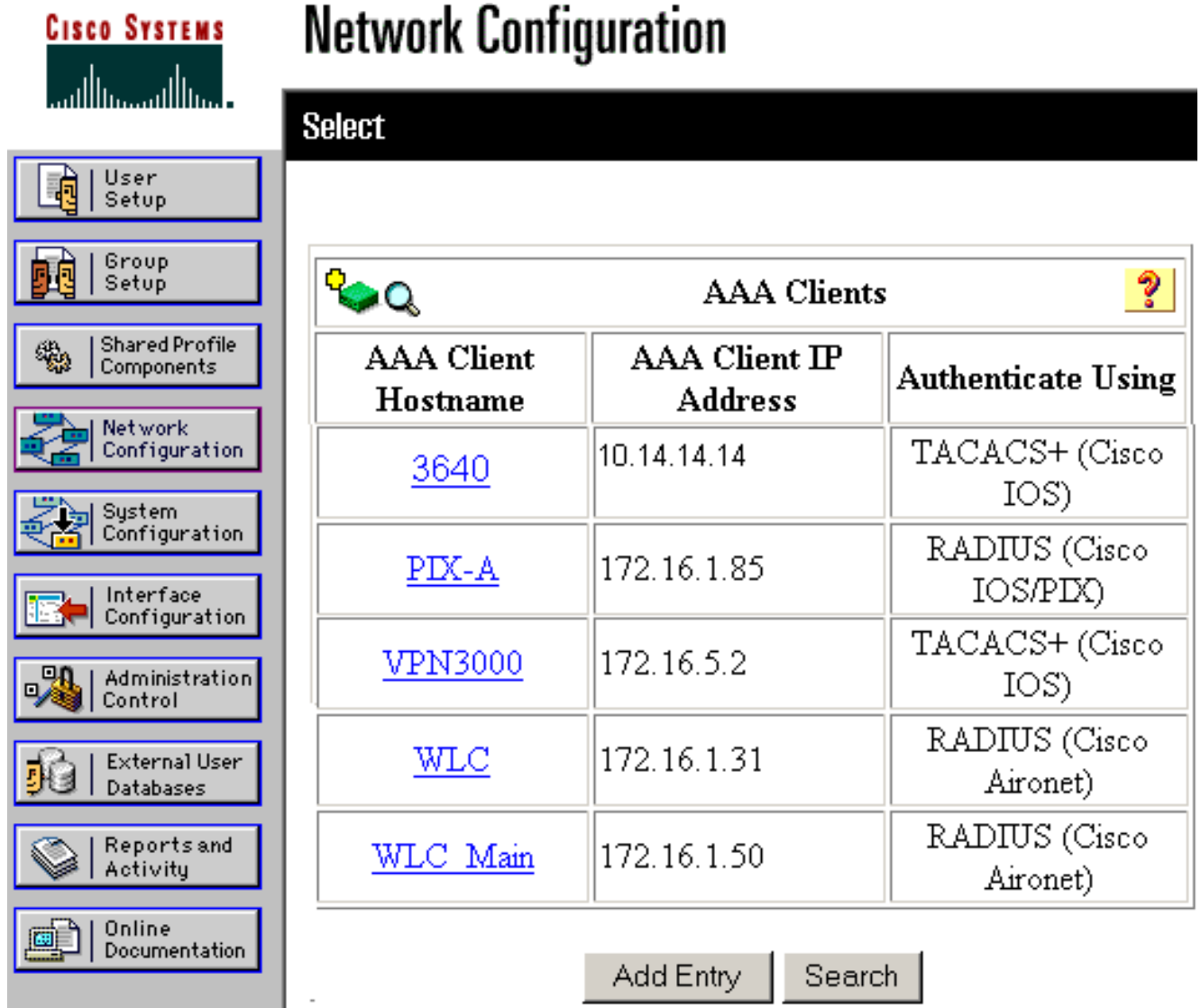
完成以下步驟，以便在Cisco Secure ACS中設定TACACS+：

1. 您必須將路由器配置為定位Cisco Secure ACS以檢查使用者憑證。例如：

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



2. 在左側選擇Network Configuration，然後按一下Add Entry，在TACACS+伺服器資料庫中為路由器新增條目。根據路由器配置選擇伺服器資料庫。



The screenshot shows the Cisco Network Configuration interface. On the left is a navigation menu with the following items: 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 content 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. 金鑰用於在3640路由器和Cisco Secure ACS伺服器之間進行身份驗證。如果要選擇TACACS+通訊協定進行驗證，請在「Authenticate Using」下拉選單中選擇TACACS+(Cisco IOS)。





# Network Configuration

Edit

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

## 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	

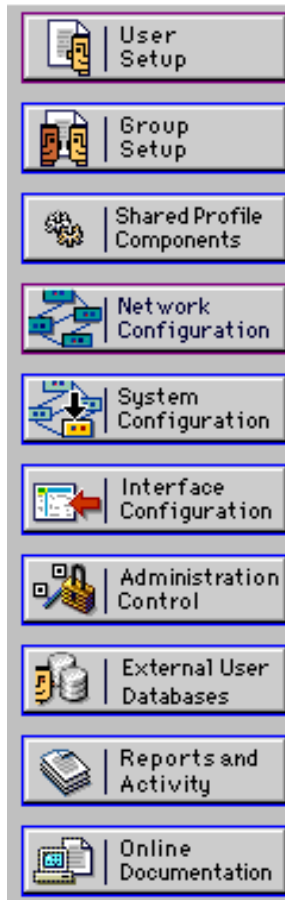
Submit

Submit + Restart

Cancel

4. 在Cisco Secure資料庫的User欄位中輸入使用者名稱，然後按一下Add/Edit。在本例中，使用者名稱是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. 在下一個視窗中，輸入rtpuser的口令。在本例中，口令為rtpuserpass。如果需要，可以將使用者帳戶對映到組。完成後，按一下**Submit**。



在PC上開啟瀏覽器並將其指向<http://10.17.17.17>。Cisco 3640路由器會攔截此HTTP流量，觸發身份驗證代理，並提示您輸入使用者名稱和密碼。Cisco 3640將使用者名稱/密碼傳送到TACACS+伺服器以進行驗證。如果驗證成功，您應該能夠在Web伺服器10.17.17.17上看到網頁。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- [show ip access-lists](#) — 顯示防火牆路由器上配置的標準型和延伸型ACL (包括動態ACL條目)。動態ACL條目將根據使用者是否進行身份驗證定期新增和刪除。此輸出顯示觸發驗證代理之前的存取清單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)
```

此輸出顯示auth-proxy觸發且使用者成功進行驗證後access-list 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)
```

存取清單的前三行是為此使用者定義並從TACACS+伺服器下載的專案。

- [show ip auth-proxy cache](#) — 顯示驗證代理條目或執行中的驗證代理配置。cache關鍵字，用於列出主機IP地址、源埠號、身份驗證代理的超時值和使用身份驗證代理的連線狀態。如果身份驗證代理狀態為ESTAB，則使用者身份驗證成功。

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

## 疑難排解

如需驗證和偵錯指令，以及其他疑難排解資訊，請參閱[驗證代理疑難排解](#)。

注意：發出debug命令之前，請參閱[有關Debug命令的重要資訊](#)。

## 相關資訊

- [配置身份驗證代理](#)
- [Cisco IOS中的驗證代理配置](#)
- [在TACACS+和RADIUS伺服器中實作驗證代理](#)
- [Cisco VPN使用者端支援頁面](#)
- [IOS防火牆支援頁面](#)
- [IPSec支援頁面](#)
- [RADIUS 支援頁面](#)
- [要求建議 \(RFC\)](#)
- [TACACS/TACACS+ 支援頁面](#)
- [IOS 文件中的 TACACS+](#)
- [技術支援 - Cisco Systems](#)