

IOS ルータ : IPsec および VPN クライアントの ACS に関する Auth-proxy 認証着信

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[VPN Client 4.8 の設定](#)

[Cisco Secure ACSを使用したTACACS+サーバの設定](#)

[フォールバック機能の設定](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

概要

認証プロキシ機能を使用すると、ユーザはネットワークにログインしたり、HTTPを介してインターネットにアクセスしたりできます。また、特定のアクセスプロファイルが自動的に取得され、TACACS+またはRADIUSサーバから適用されます。そのユーザプロファイルは、認証済みユーザからのアクティブなトラフィックが存在する間だけ有効です。

この設定は、10.1.1.1でWebブラウザを起動し、10.17.17.17を目指すように設計されています。VPN Clientはトンネルのエンドポイント10.31.1.111を経由して10.17.17.xネットワークに到達するように設定されているため、IPSecトンネルが構築され、PCはプールRTP POOLからアドレスを取得します。その後、Cisco 3640ルータによって認証が要求されます。ユーザが（10.14.14.3のTACACS+サーバに格納されている）ユーザ名とパスワードを入力した後、サーバから渡されるアクセスリストは、アクセスリスト118に追加されます。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- Cisco VPN Clientは、Cisco 3640ルータとのIPSecトンネルを確立するように設定されています。
- TACACS+サーバが認証プロキシ用に設定されている。詳細については、「関連情報」セクションを参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS?ソフトウェアリリース12.4
- Cisco 3640 ルータ
- Cisco VPN Client for Windows バージョン 4.8 (任意の VPN Client 4.x 以降で使用可能)

注 : ip auth-proxy コマンドは、Cisco IOSソフトウェアリリース12.0.5.Tで導入されました。この設定は、Cisco IOSソフトウェアリリース12.4でテストされています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、「[シスコテクニカルティップスの表記法](#)」を参照してください。

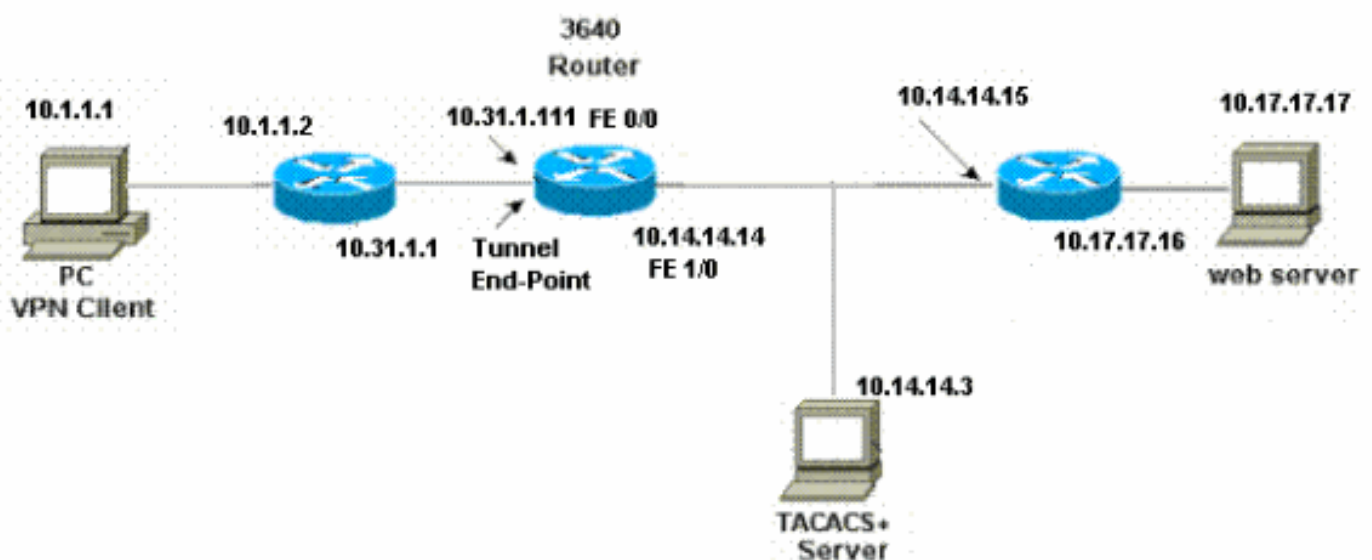
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注 : この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください (登録ユーザのみ) 。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



コンフィギュレーション

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

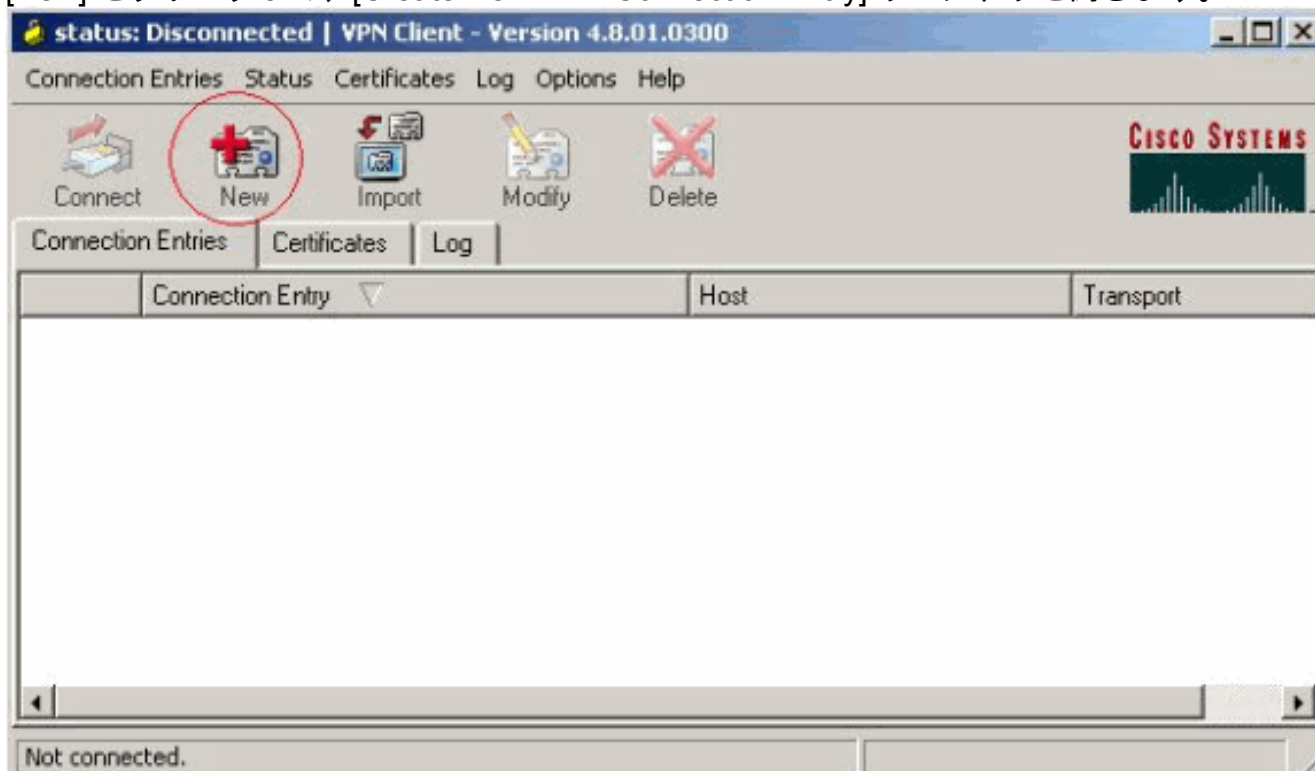
```

```
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
```

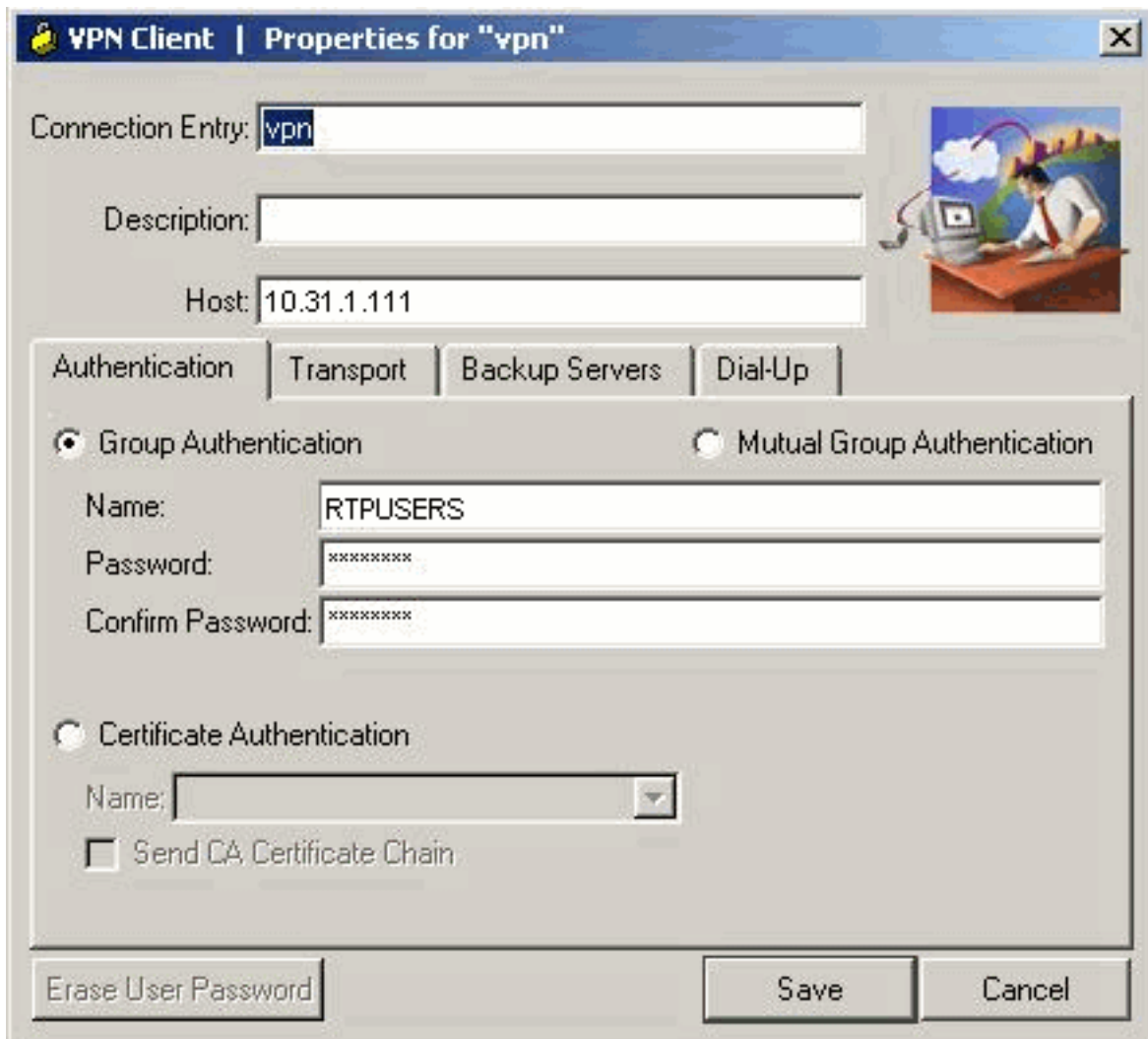
VPN Client 4.8 の設定

VPN Client 4.8 を設定するには、次の手順を実行します。

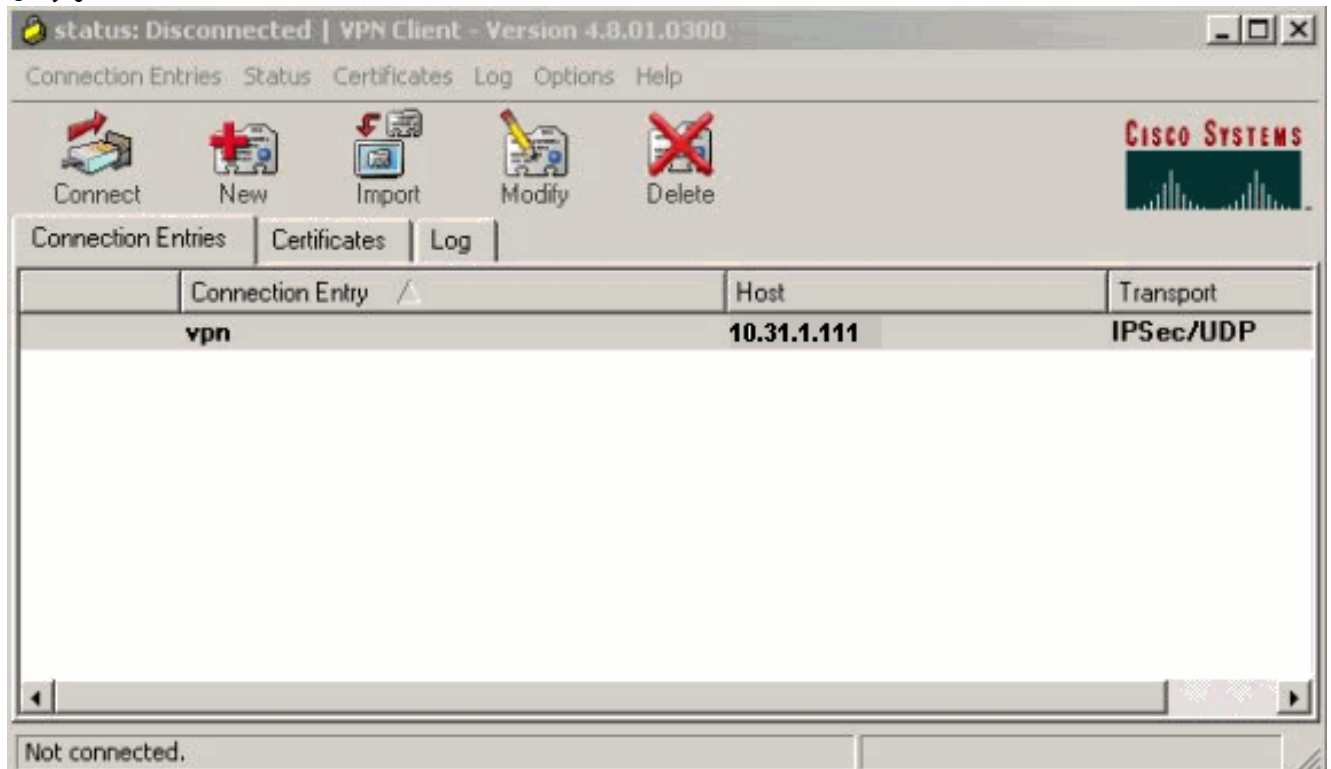
1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択します。
2. [New] をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。



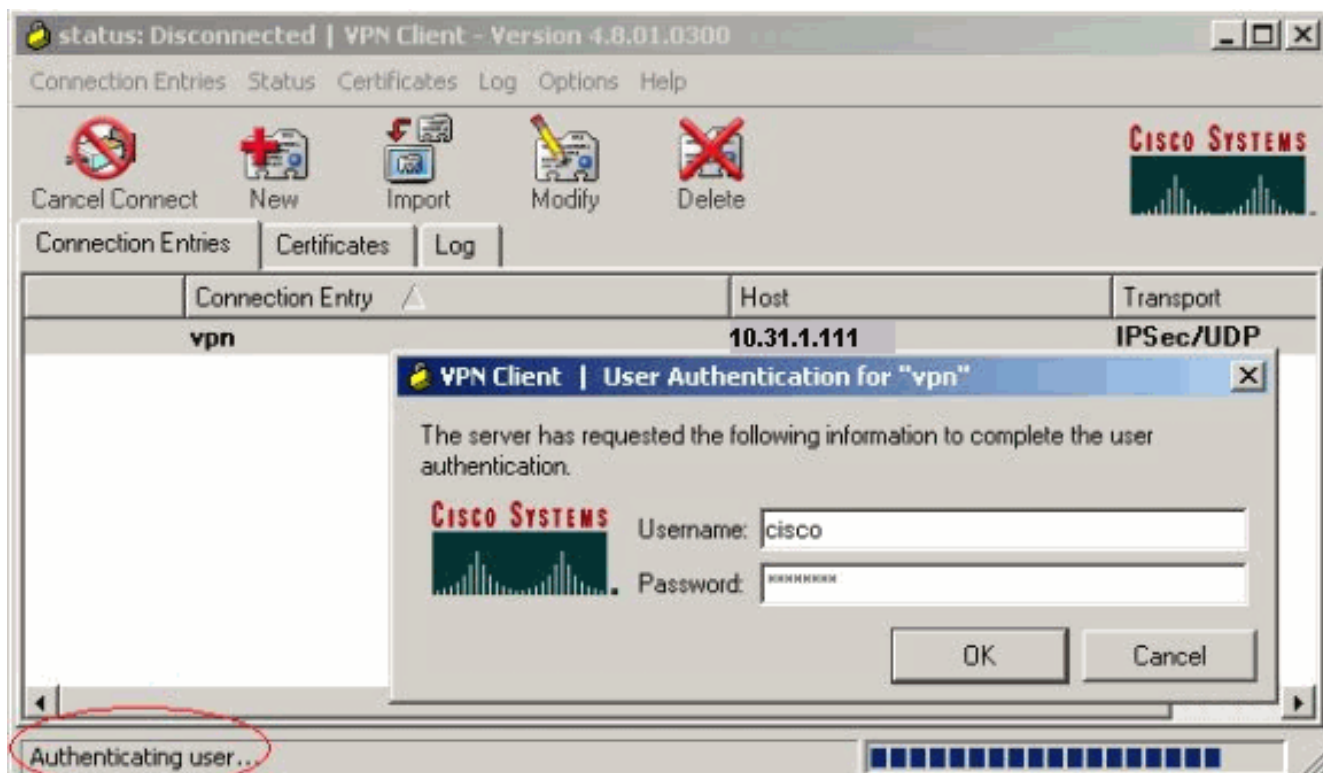
3. 接続エントリの名前と説明を入力します。Host ボックスに、ルータの Outside の IP アドレスを入力します。次に、VPN グループ名とパスワードを入力し、[Save] をクリックします



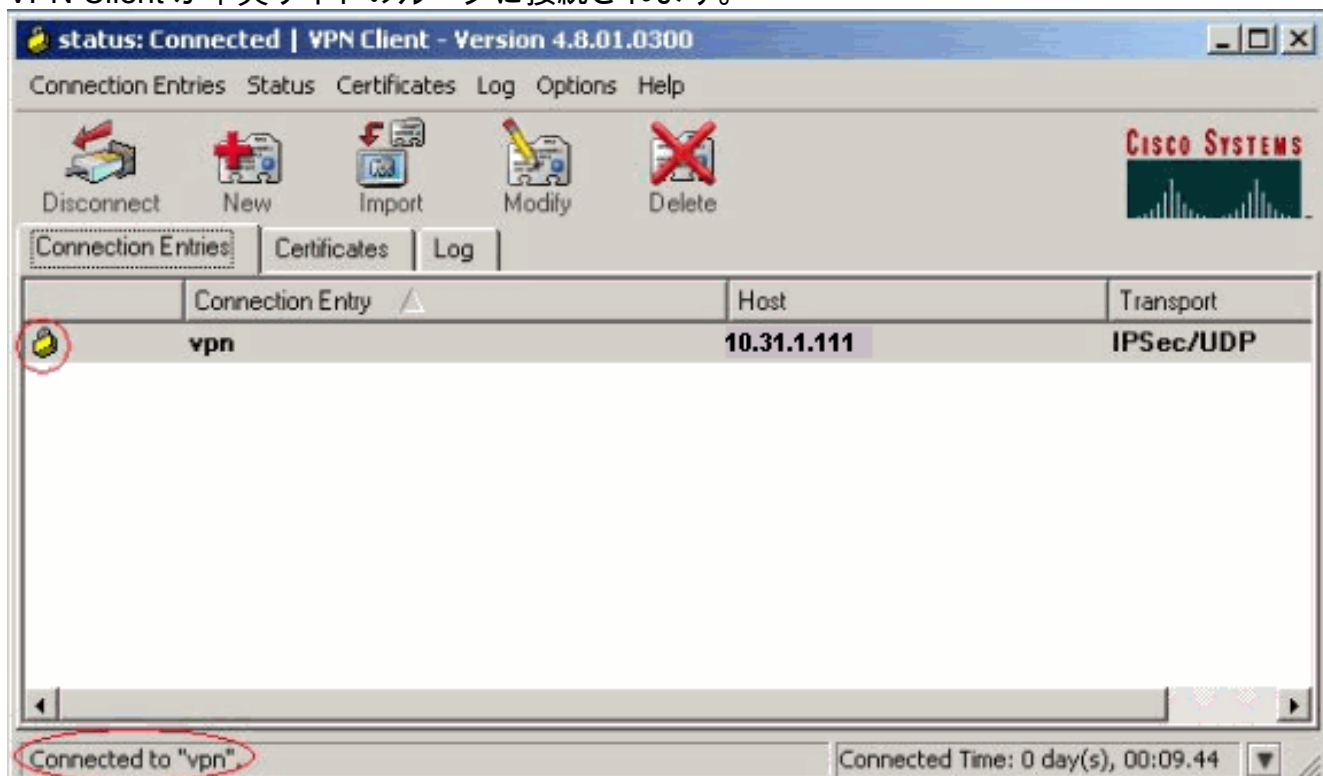
4. 使用する接続をクリックし、VPN Client のメイン ウィンドウから [Connect] をクリックします。



5. ダイアログボックスが表示されたら、Xauth のユーザ名とパスワード情報を入力して [OK] をクリックし、リモート ネットワークに接続します。



VPN Client が中央サイトのルータに接続されます。




Cisco Secure ACSを使用したTACACS+サーバの設定

Cisco Secure ACSでTACACS+を設定するには、次の手順を実行します。

1. ユーザのクレデンシャルを確認するには、Cisco Secure ACSを検索するようにルータを設定する必要があります。以下に、いくつかの例を示します。

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

2. 左側の[Network Configuration]を選択し、[Add Entry]をクリックして、TACACS+サーバデータベースのいずれかにルータのエントリを追加します。ルータの設定に従ってサーバデータベースを選択します。



Network Configuration

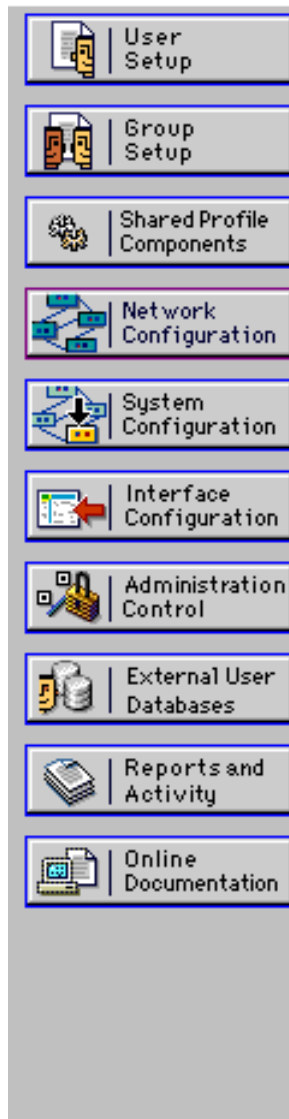
Select

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

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. キーは、3640ルータとCisco Secure ACSサーバ間の認証に使用されます。認証にTACACS+ プロトコルを選択する場合、Authenticate Using ドロップダウンメニューでTACACS+(Cisco IOS)を選択します。



Add AAA Client

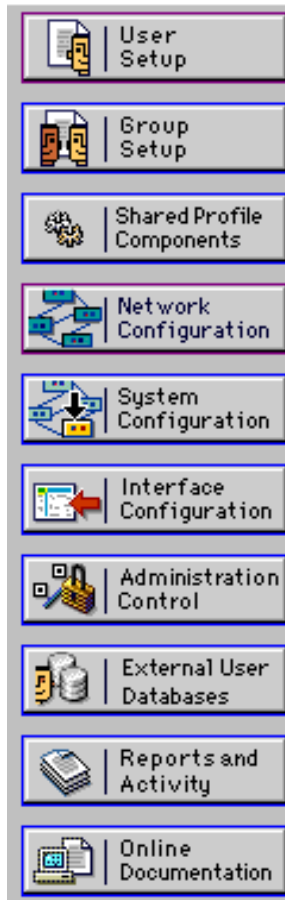
AAA Client Hostname	<input type="text" value="3640"/>
AAA Client IP Address	<input type="text" value="10.14.14.14"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in 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. Cisco Secure データベースの User フィールドにユーザ名を入力してから、Add/Edit をクリックします。この例では、ユーザ名はrtuserです。

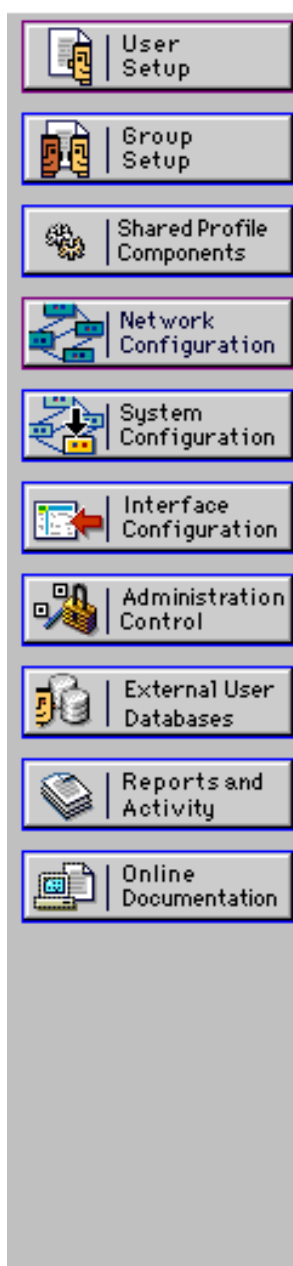


User:

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. 次のウィンドウで、rtpuserのパスワードを入力します。この例では、パスワードはrtpuserpassです。必要であれば、ユーザ アカウントをグループにマップできます。完了したら、[Submit] をクリックします。



Supplementary User Info	
Real Name	<input type="text" value="rtpuser"/>
Description	<input type="text"/>

User Setup	
Password Authentication:	
	<input type="text" value="CiscoSecure Database"/>
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)	
Password	<input type="text" value="XXXXXXXXXXXXXXXXXXXX"/>
Confirm Password	<input type="text" value="XXXXXXXXXXXXXXXXXXXX"/>
<input type="checkbox"/> Separate (CHAP/MS-CHAP/ARAP)	
Password	<input type="text"/>
Confirm Password	<input type="text"/>
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is	
<input type="button" value="Submit"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

フォールバック機能の設定

プライマリ RADIUS サーバが使用不能になると、ルータは次にアクティブなバックアップ RADIUS サーバにフェールオーバーします。ルータは、プライマリ サーバが使用可能になっても、永続的にセカンダリ RADIUS サーバを使用し続けます。通常プライマリ サーバは、パフォーマンスに優れており、優先して使用されるサーバです。セカンダリサーバが使用できない場合は、[aaa authentication login default group RTP local](#) コマンドを使用して、ローカルデータベースを認証に使用することができます。

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

PCとCisco 3640ルータ間にIPSecトンネルを確立します。

PCでブラウザを開き、<http://10.17.17.17>をポイントします。Cisco 3640ルータはこのHTTPトラフィックを代行受信し、認証プロキシをトリガーし、ユーザ名とパスワードの入力を求めます。Cisco 3640は、認証のためにユーザ名/パスワードをTACACS+サーバに送信します。認証に成功すると、Webサーバの10.17.17.17にWebページが表示されます。

一部の show コマンドは[アウトプット インタープリタ ツールによってサポートされています \(登録ユーザ専用 \)](#)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- [show ip access-lists](#) : ファイアウォールルータに設定されている標準および拡張ACL (ダイナミックACLエントリを含む) を表示します。ダイナミック ACL エントリは、ユーザが認証されるかどうかに応じて、定期的に追加および削除されます。次の出力は、auth-proxyがトリガーされる前のaccess-list 118を示しています。

```
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)
```

次の出力は、auth-proxyがトリガーされ、ユーザが正常に認証された後のaccess-list 118を示しています。

```
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)
```

アクセスリストの最初の3行は、このユーザに定義され、TACACS+サーバからダウンロードされたエントリです。

- [show ip auth-proxy cache](#) : [認証プロキシ エントリまたは実行中の認証プロキシ設定を表示します](#)。cache キーワードを使って、ホスト IP アドレス、送信元ポート番号、認証プロキシのタイムアウト値、および認証プロキシを使用する接続の状態を一覧表示します。認証プロキシの状態がESTABの場合、ユーザ認証は成功します。

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

トラブルシューティング

検証コマンドとデバッグコマンド、およびその他のトラブルシューティング情報については、「[認証プロキシのトラブルシューティング](#)」を参照してください。

注 : debugコマンドを発行する前に、『[debugコマンドの重要な情報](#)』を参照してください。

関連情報

- [認証プロキシの設定](#)
- [Cisco IOSでの認証プロキシの設定](#)
- [TACACS+およびRADIUSサーバでの認証プロキシの実装](#)

- [Cisco VPN Client に関するサポート ページ](#)
- [IOS ファイアウォールのサポート ページ](#)
- [IPSec に関するサポート ページ](#)
- [RADIUS に関するサポート ページ](#)
- [Requests for Comments \(RFCs\)](#)
- [TACACS/TACACS+ サポート ページ](#)
- [IOS での TACACS+ に関するドキュメント](#)
- [テクニカルサポート - Cisco Systems](#)