

Router IOS: Autenticazione proxy in entrata con ACS per configurazione client IPsec e VPN

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Configurazione VPN Client 4.8](#)

[Configurazione del server TACACS+ con Cisco Secure ACS](#)

[Configurazione della funzione di fallback](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

La funzione proxy di autenticazione consente agli utenti di accedere a una rete o a Internet tramite HTTP, con i relativi profili di accesso specifici recuperati e applicati automaticamente da un server TACACS+ o RADIUS. I profili utente sono attivi solo quando è attivo il traffico proveniente dagli utenti autenticati.

Questa configurazione è stata progettata per attivare il browser Web sulla versione 10.1.1.1 e puntare alla versione 10.17.17.17. Poiché il client VPN è configurato per passare attraverso l'endpoint del tunnel 10.31.1.111 e raggiungere la rete 10.17.17.x, il tunnel IPsec viene generato e il PC ottiene l'indirizzo IP dal pool RTP-POOL (poiché viene eseguita la configurazione della modalità). L'autenticazione viene quindi richiesta dal router Cisco 3640. Dopo che l'utente ha immesso un nome utente e una password (memorizzati sul server TACACS+ alla versione 10.14.14.3), l'elenco degli accessi passato dal server viene aggiunto all'elenco degli accessi 118.

Prerequisiti

Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Il client VPN Cisco è configurato per stabilire un tunnel IPsec con il router Cisco 3640.
- Il server TACACS+ è configurato per il proxy di autenticazione. Per ulteriori informazioni, vedere la sezione "Informazioni correlate".

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS? Software release 12.4
- Cisco 3640 Router
- Cisco VPN Client per Windows versione 4.8 (qualsiasi client VPN versione 4.x e successive dovrebbe funzionare)

Nota: il comando **ip auth-proxy** è stato introdotto nel software Cisco IOS versione 12.0.5.T. Questa configurazione è stata testata con il software Cisco IOS versione 12.4.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

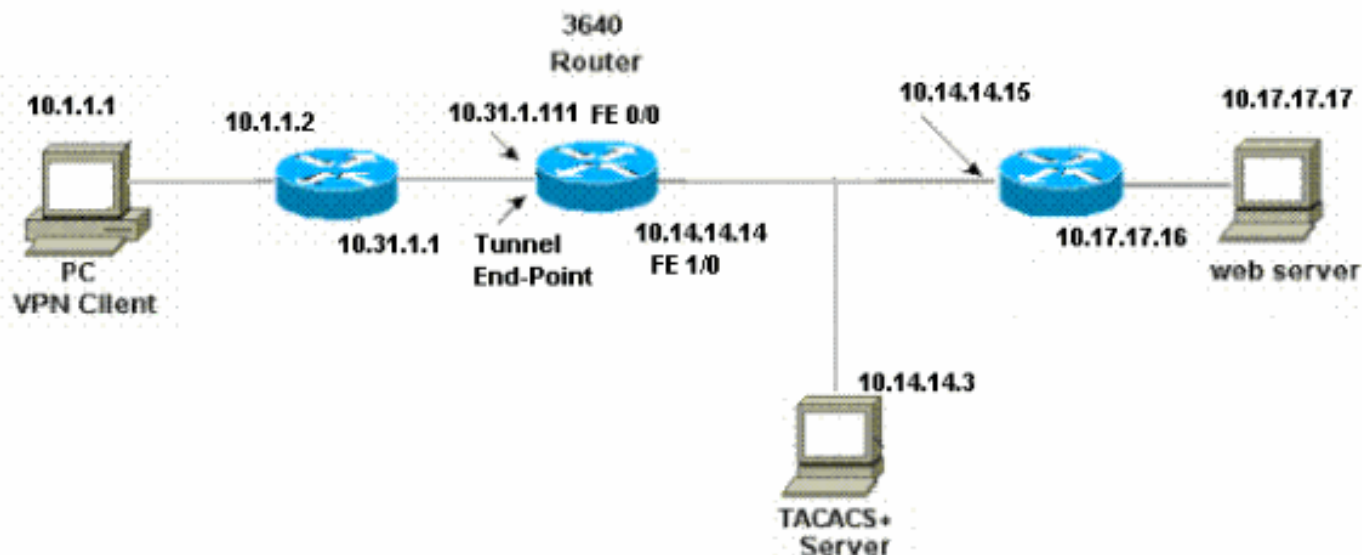
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca dei comandi](#) (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazione

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

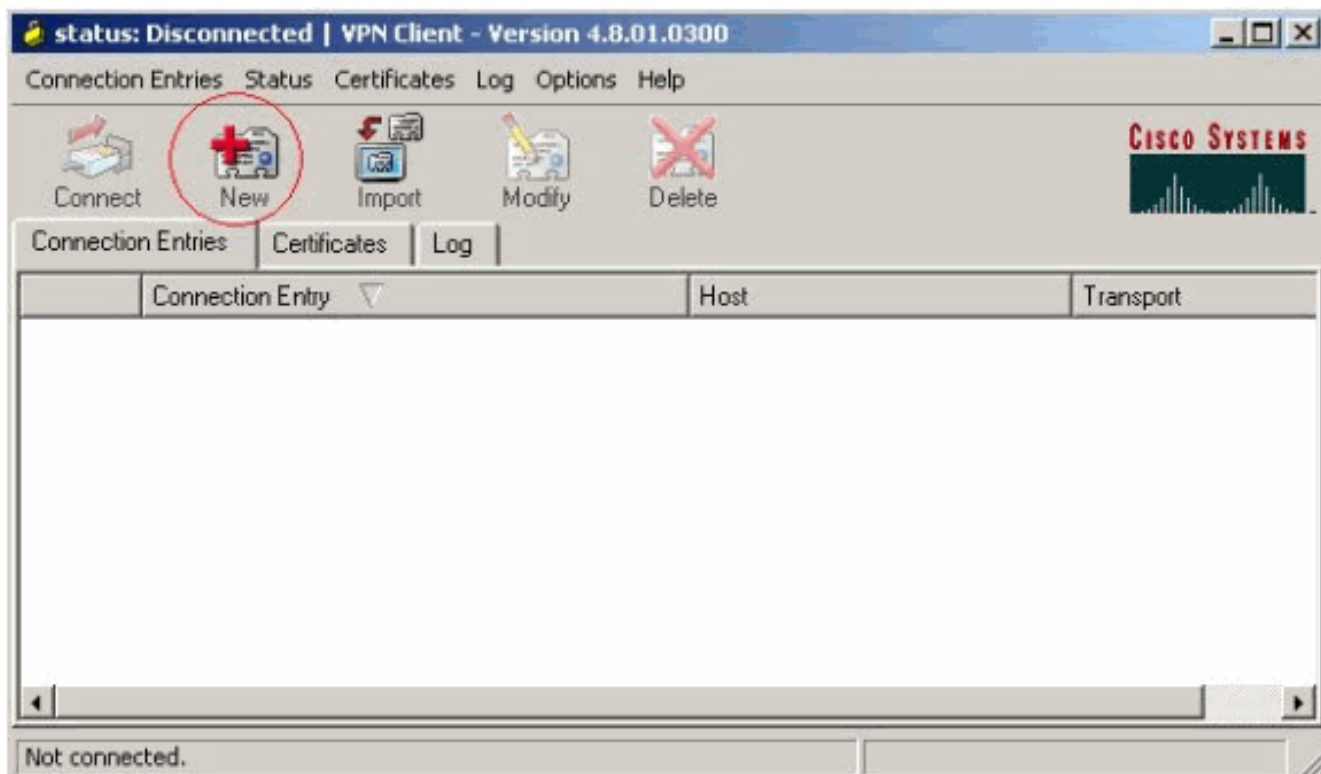
!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list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

```

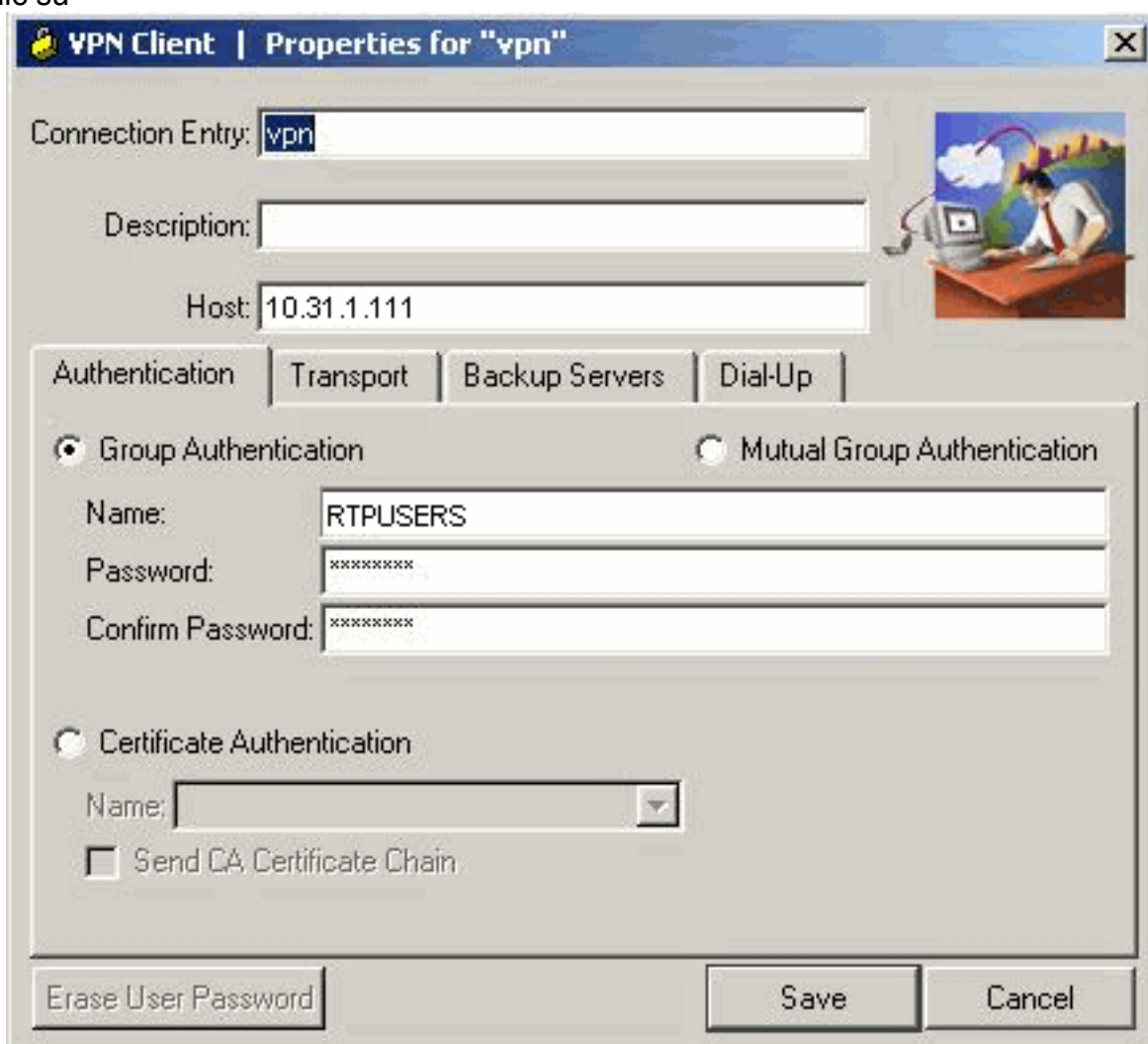
Configurazione VPN Client 4.8

Completare questa procedura per configurare il client VPN 4.8:

1. Scegliere **Start > Programmi > Cisco Systems VPN Client > VPN Client**.
2. Fare clic su **Nuovo** per avviare la finestra Crea nuova voce di connessione VPN.



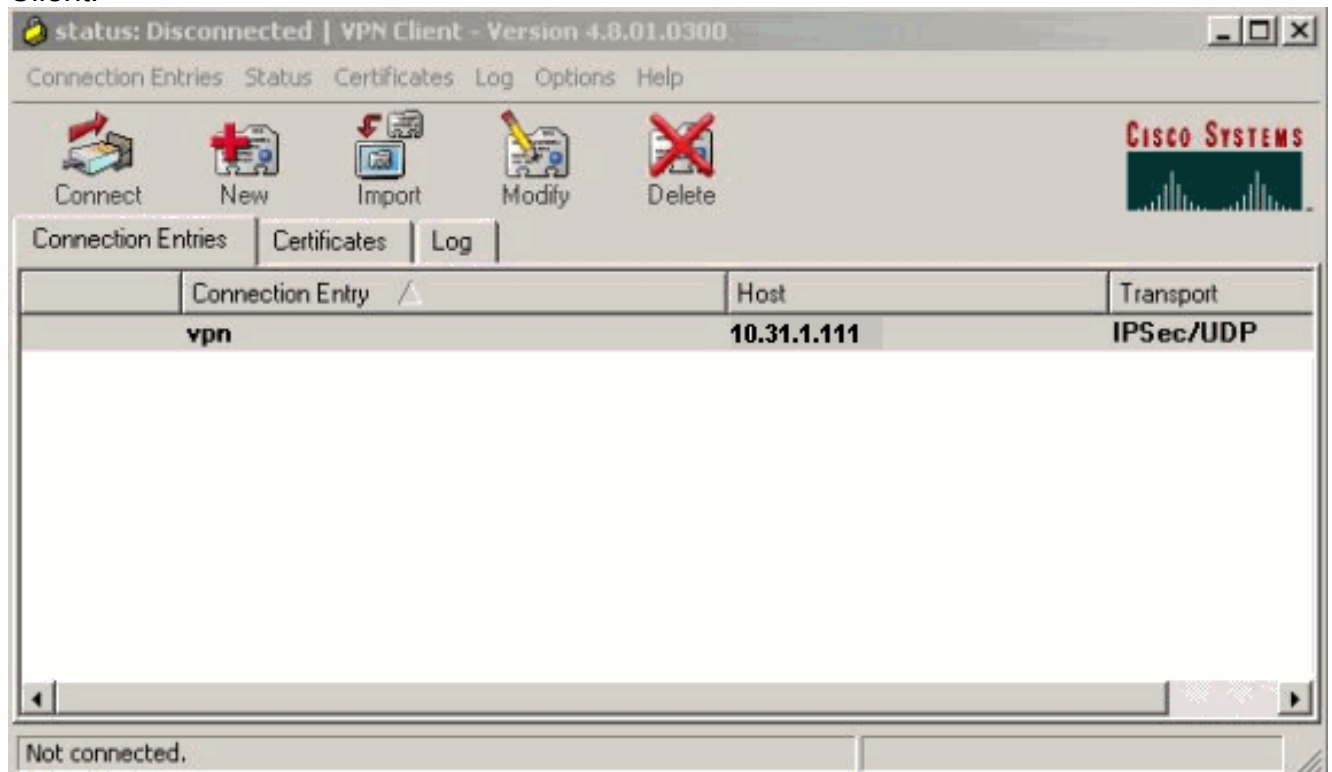
3. Immettere il nome della voce di connessione insieme a una descrizione. Immettere l'indirizzo IP esterno del router nella casella Host. Immettere il nome e la password del gruppo VPN e fare clic su



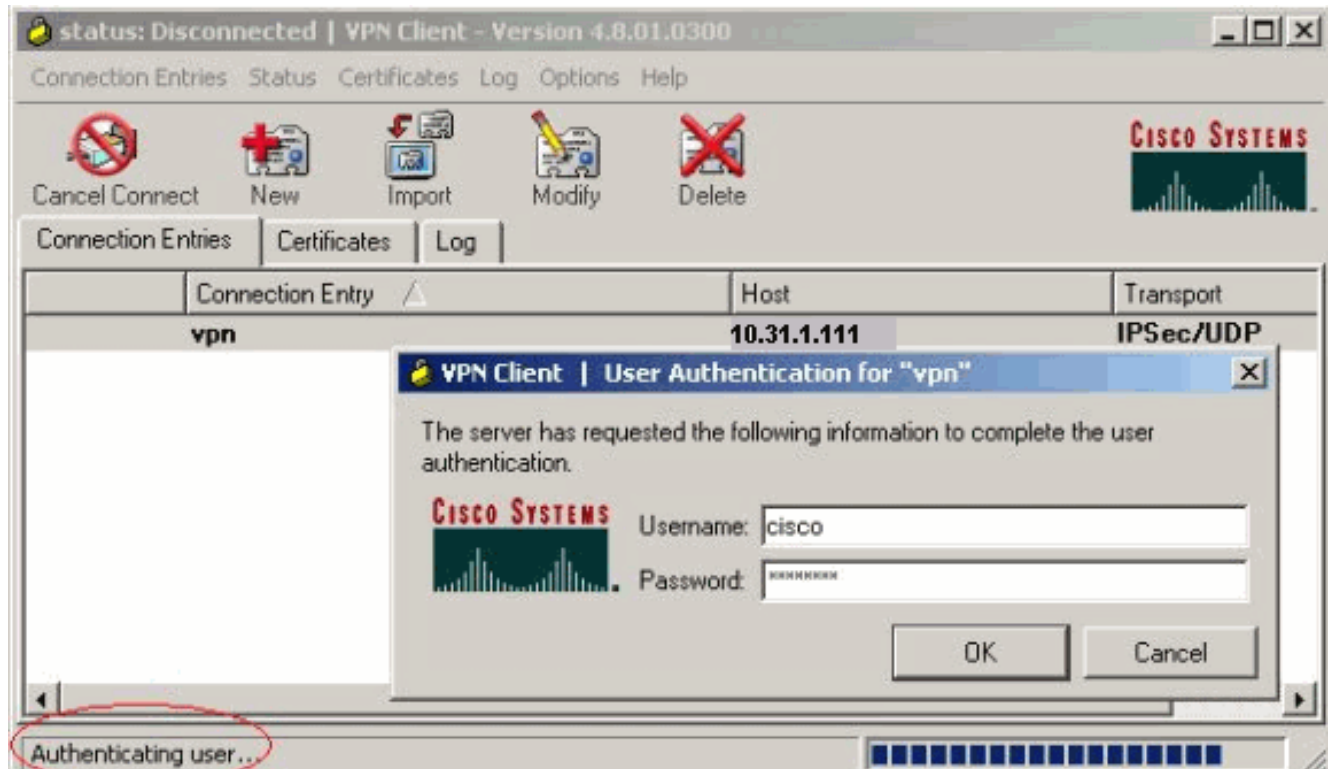
Salva.

4. Fare clic sulla connessione che si desidera utilizzare e fare clic su **Connetti** dalla finestra principale di VPN

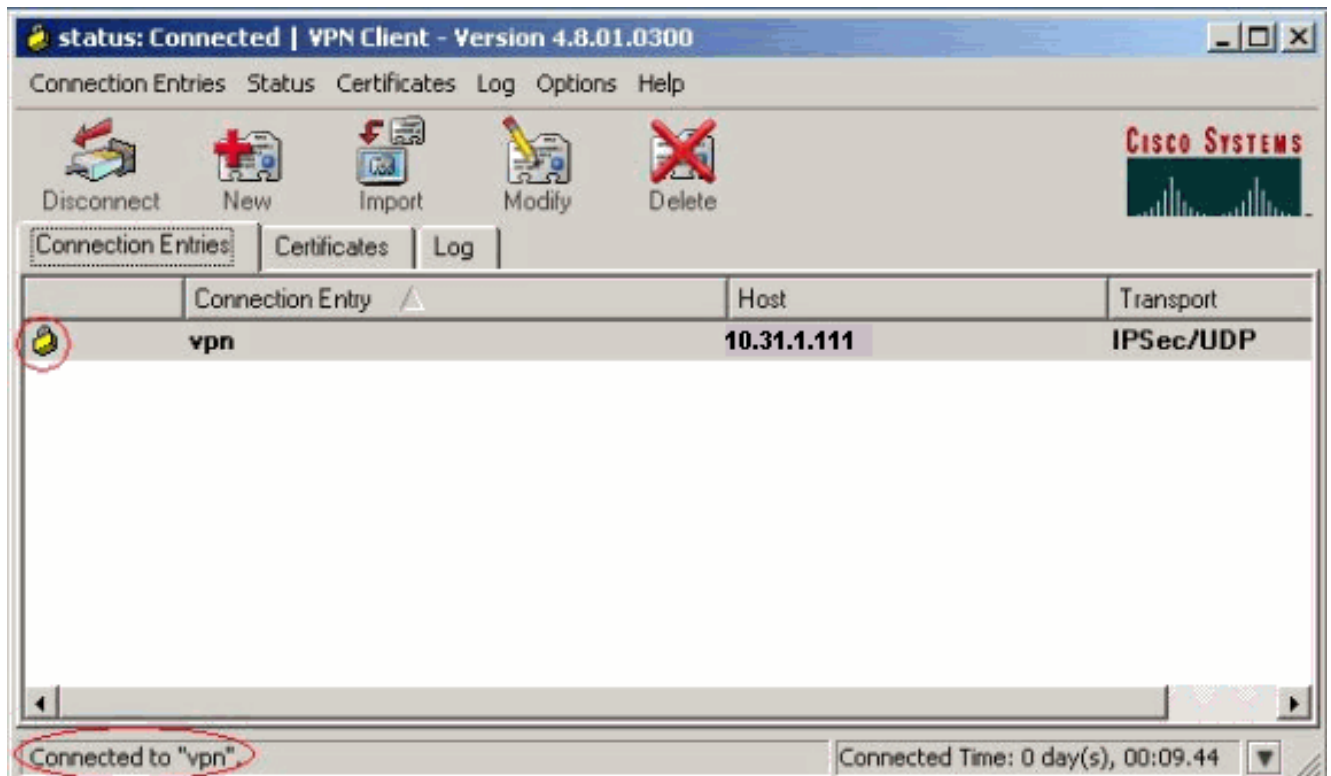
Client.



5. Quando richiesto, immettere il nome utente e la password per xauth e fare clic su OK per connettersi alla rete remota.



Il client VPN si connette al router sul sito centrale.



Configurazione del server TACACS+ con Cisco Secure ACS

Completare questa procedura per configurare TACACS+ in un Cisco Secure ACS:

1. È necessario configurare il router per individuare il Cisco Secure ACS e controllare le credenziali dell'utente. Ad esempio:

```
3640(config)#
```











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


```
3640(config)#
```

```
tacacs-server host 10.14.14.3 key cisco
```

2. Scegliere **Configurazione di rete** a sinistra e fare clic su **Aggiungi voce** per aggiungere una voce per il router nel database del server TACACS+. Scegliere il database del server in base alla configurazione del router.

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 Clients 		
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/PDQ)
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)

3. La chiave viene utilizzata per autenticare il router 3640 e il server Cisco Secure ACS. Per selezionare il protocollo TACACS+ per l'autenticazione, scegliere **TACACS+ (Cisco IOS)** dal menu a discesa Autentica con.

- 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

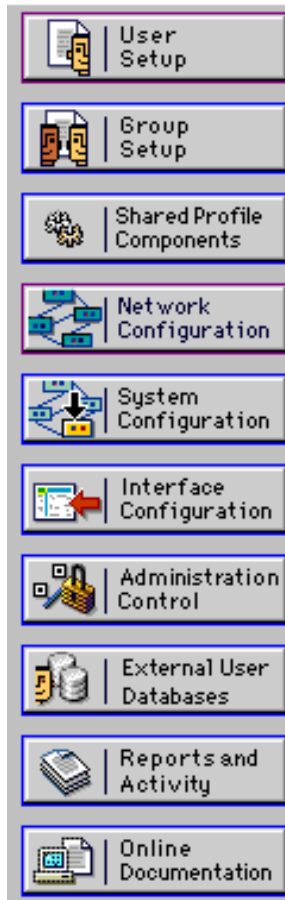
Submit

Submit + Restart

Cancel

4. Immettere il nome utente nel campo Utente nel database Cisco Secure, quindi fare clic su **Aggiungi/Modifica**. Nell'esempio, il nome utente è rtpuser.

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. Nella finestra successiva, immettere la password per rtpuser. Nell'esempio, la password è rtpuserpass. Se lo si desidera, è possibile mappare l'account utente a un gruppo. Al termine, fare clic su **Invia**.



- 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	<input style="width: 70%;" type="text" value="rtpuser"/>
Description	<input style="width: 70%;" type="text"/>

User Setup ?

Password Authentication:

CiscoSecure Database ▼

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

Password	<input style="width: 70%;" type="password" value="XXXXXXXXXXXXXXXX"/>
Confirm Password	<input style="width: 70%;" type="password" value="XXXXXXXXXXXXXXXX"/>

Separate (CHAP/MS-CHAP/ARAP)

Password	<input style="width: 70%;" type="password"/>
Confirm Password	<input style="width: 70%;" type="password"/>

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is

Configurazione della funzione di fallback

Quando il server RADIUS primario diventa non disponibile, il router eseguirà il failover sul successivo server RADIUS di backup attivo. Il router continuerà a utilizzare il server RADIUS secondario per sempre anche se il server primario è disponibile. In genere, il server principale è il server preferito e offre prestazioni elevate. Se il server secondario non è disponibile, il database locale può essere utilizzato per l'autenticazione usando il comando [aaa authentication login default group RTP local](#).

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Stabilire un tunnel IPsec tra il PC e il router Cisco 3640.

Aprire un browser sul PC e puntarlo a <http://10.17.17.17>. Il router Cisco 3640 intercetta il traffico HTTP, attiva il proxy di autenticazione e richiede un nome utente e una password. Cisco 3640 invia nome utente/password al server TACACS+ per l'autenticazione. Se l'autenticazione ha esito positivo, sarà possibile visualizzare le pagine Web sul server Web al numero 10.17.17.17.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- [show ip access-lists](#): visualizza gli ACL standard ed estesi configurati sul router firewall (include le voci ACL dinamiche). Le voci ACL dinamiche vengono aggiunte e rimosse periodicamente a seconda che l'utente esegua o meno l'autenticazione. Questo output visualizza l'elenco degli accessi 118 prima dell'attivazione del proxy di autenticazione:

```
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)
```

Questo output visualizza l'elenco degli accessi 118 dopo l'attivazione del proxy di autenticazione e l'autenticazione corretta da parte dell'utente:

```
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)
```

Le prime tre righe dell'elenco degli accessi sono le voci definite per questo utente e scaricate dal server TACACS+.

- [show ip auth-proxy cache](#): visualizza le voci del proxy di autenticazione o la configurazione del proxy di autenticazione in esecuzione. La parola chiave cache per elencare l'indirizzo IP dell'host, il numero della porta di origine, il valore di timeout per il proxy di autenticazione e lo stato delle connessioni che utilizzano il proxy di autenticazione. Se lo stato del proxy di autenticazione è ESTAB, l'autenticazione utente avrà esito positivo.

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

Risoluzione dei problemi

Per i comandi di verifica e debug, insieme ad altre informazioni sulla risoluzione dei problemi, vedere [Risoluzione dei problemi del proxy di autenticazione](#).

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

Informazioni correlate

- [Configurazione del proxy di autenticazione](#)
- [Configurazioni del proxy di autenticazione in Cisco IOS](#)

- [Implementazione del proxy di autenticazione nei server TACACS+ e RADIUS](#)
- [Pagina di supporto per Cisco VPN Client](#)
- [Pagina di supporto di IOS Firewall](#)
- [Pagina di supporto per IPSec](#)
- [Pagina di supporto RADIUS](#)
- [RFC \(Requests for Comments\)](#)
- [Pagina di supporto TACACS/TACACS+](#)
- [Documentazione relativa a TACACS+ in IOS](#)
- [Supporto tecnico – Cisco Systems](#)