

IOS-router: Verificatie via automatische proxy met ACS voor IPSec en VPN-clientconfiguratie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Configuratie van VPN-client 4.8](#)

[Configuratie van de TACACS+ server met Cisco Secure ACS](#)

[De back-upfunctie configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

De authenticatieproxy-functie stelt gebruikers in staat om in te loggen op een netwerk of via HTTP toegang te krijgen tot het internet, waarbij hun specifieke toegangsprofielen automatisch worden opgehaald en toegepast vanaf een TACACS+ of RADIUS-server. De gebruikersprofielen zijn alleen actief wanneer er actief verkeer is van de geauthentiseerde gebruikers.

Deze configuratie is ontworpen om de webbrowser op 10.1.1.1 te brengen en het te richten op 10.17.17.17. Omdat de VPN-client is ingesteld om door tunneleindpunt 10.31.1.11 te gaan naar het 10.17.17.x-netwerk, wordt de IPSec-tunnel gebouwd en de PC de IP Adres uit de pool RTP-POOL (aangezien de mode-configuratie wordt uitgevoerd). Verificatie wordt vervolgens gevraagd door Cisco 3640-router. Nadat de gebruiker een gebruikersnaam en wachtwoord invoert (opgeslagen op de TACACS+ server op 10.14.14.3) wordt de toegangslijst die van de server wordt doorgegeven toegevoegd aan toegangslijst 118.

Voorwaarden

Vereisten

Zorg er voordat u deze configuratie probeert voor dat u aan deze vereisten voldoet:

- Cisco VPN-client is geconfigureerd voor het maken van een IPSec-tunnel met Cisco 3640 router.
- De TACACS+ server is ingesteld voor een verificatieproxy. Zie het gedeelte "Verwante

informatie" voor meer informatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS? IOS-softwarerelease 12.4
- Cisco 3640 router
- Cisco VPN-client voor Windows versie 4.8 (een VPN-client 4.x en hoger moet werken)

Opmerking: de **ip-opdracht** voor **automatische proxy** is geïntroduceerd in Cisco IOS-softwarerelease 12.0.5.T. Deze configuratie is getest met Cisco IOS-softwarerelease 12.4.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

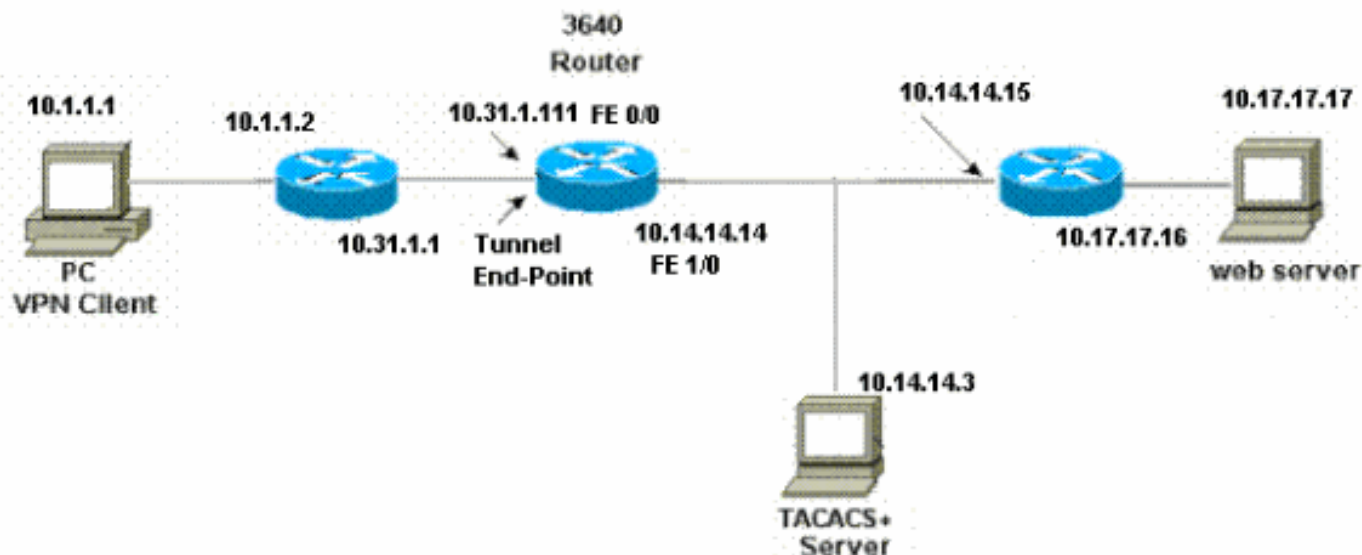
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het [Opdrachtplanningprogramma](#) (alleen [geregistreerd](#) klanten).

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie

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

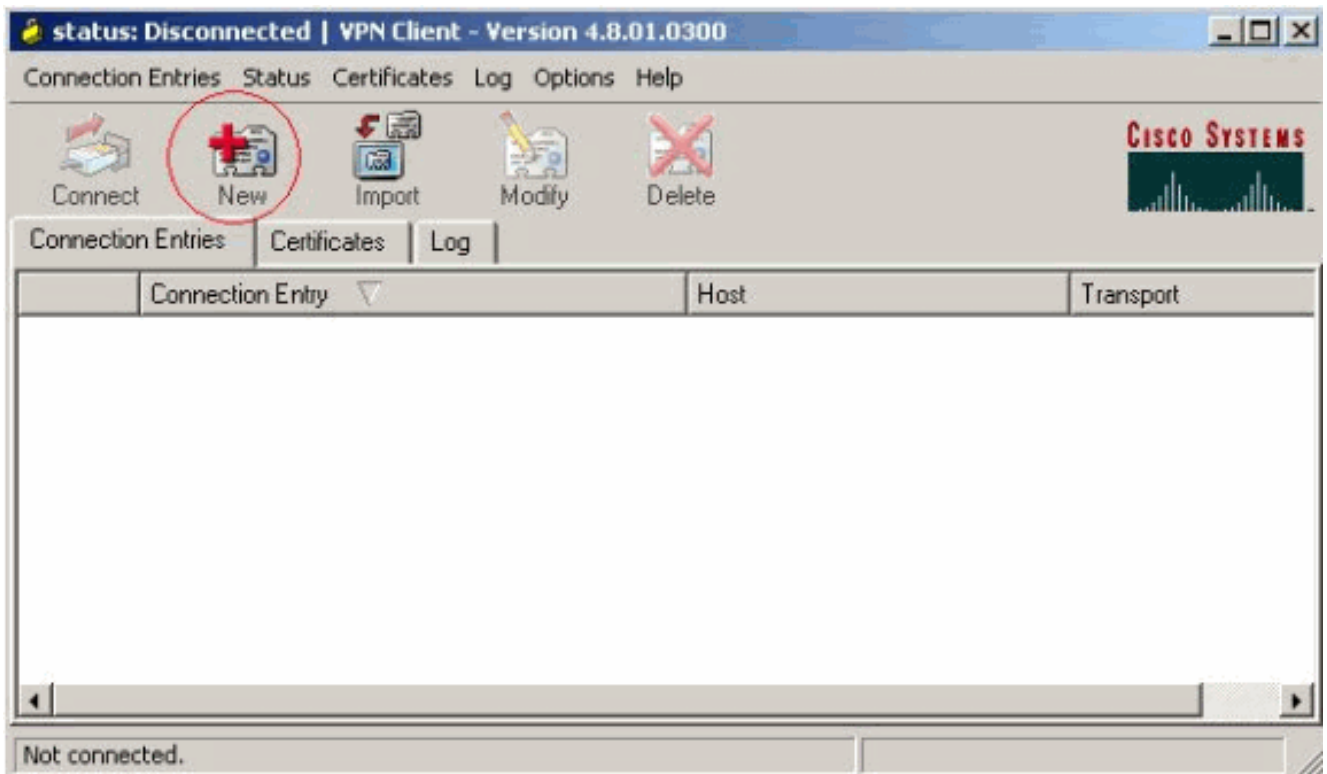
!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list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

```

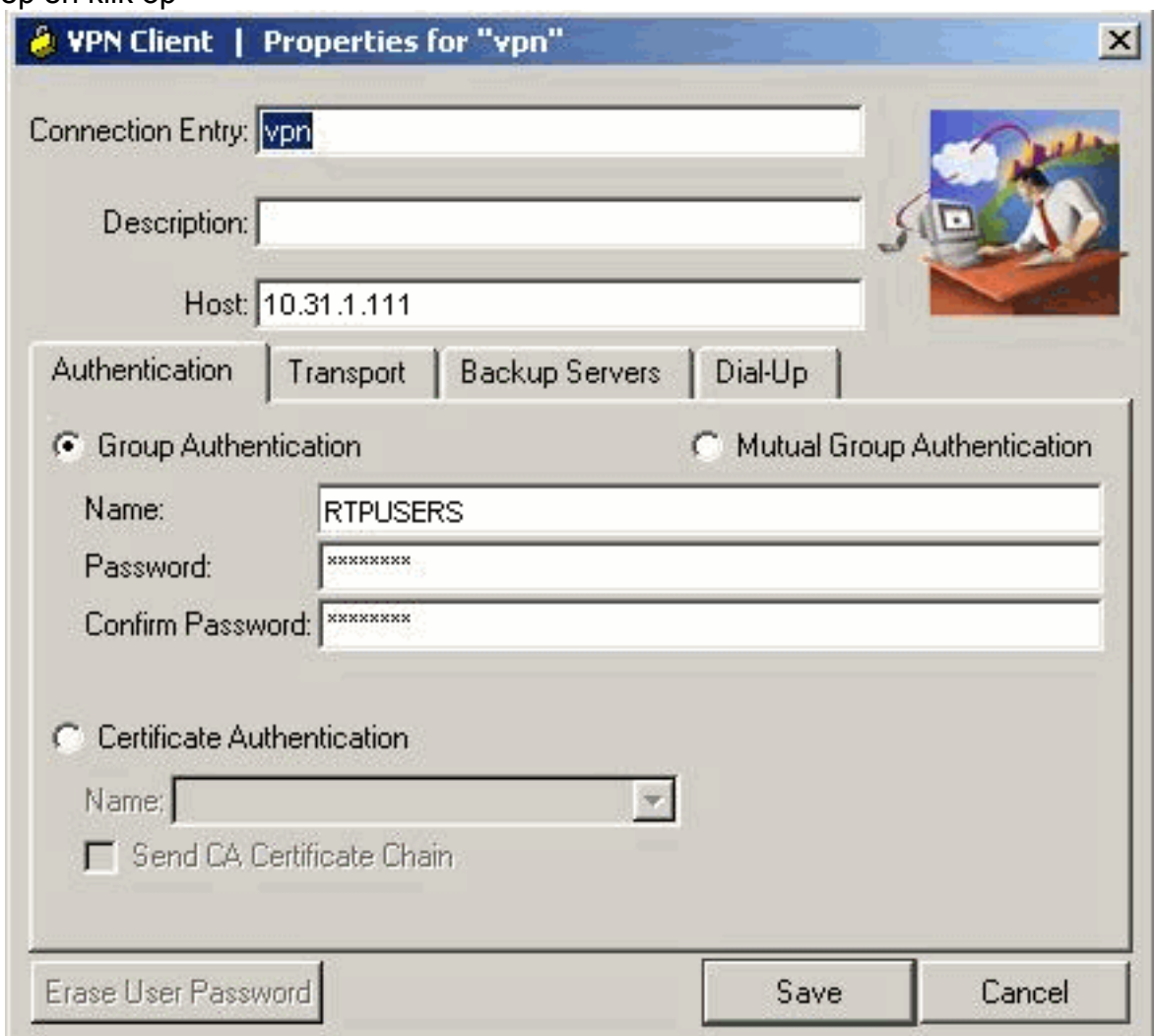
Configuratie van VPN-client 4.8

Voltooi deze stappen om de VPN-client 4.8 te configureren:

1. Kies **Start > Programma's > Cisco Systems VPN-client > VPN-client**.
2. Klik op **New** om het venster Nieuwe VPN-verbinding maken te starten.



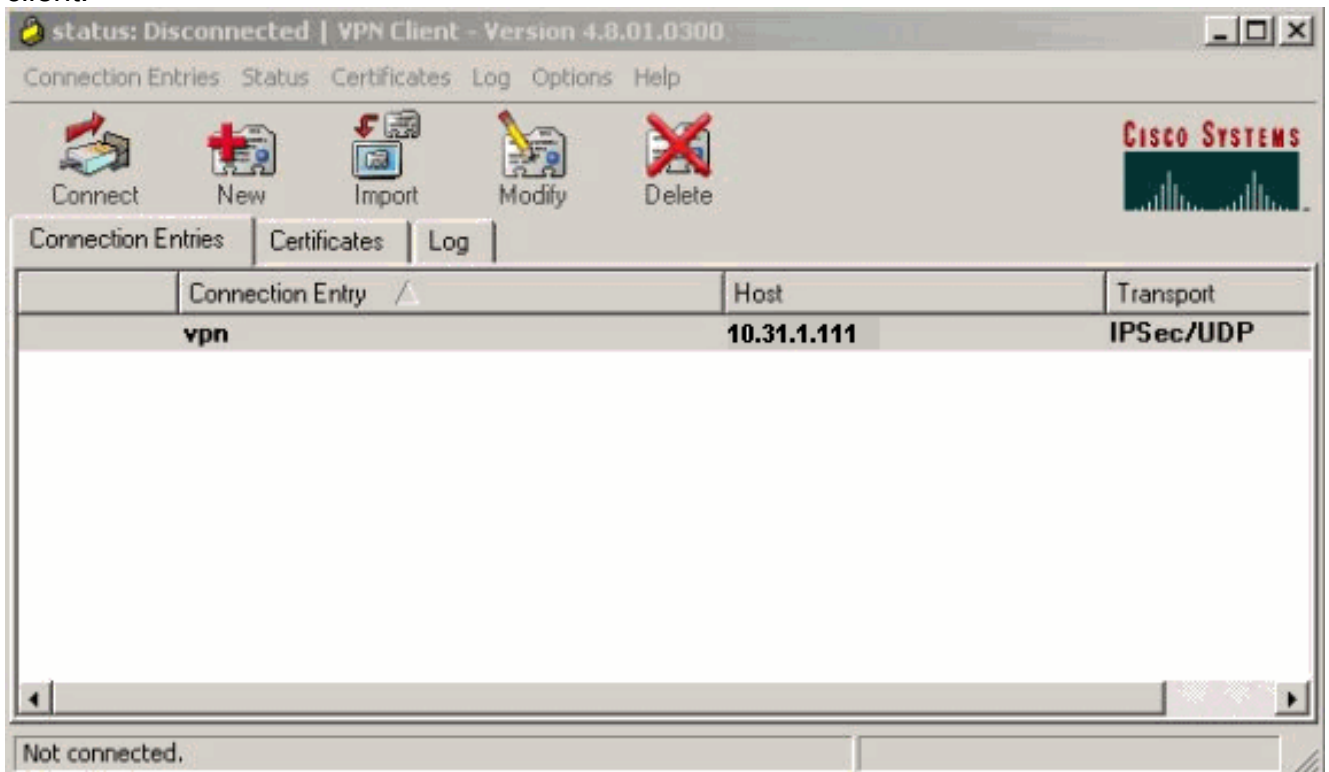
3. Voer de naam van de verbindingsoort in samen met een beschrijving. Voer het externe IP-adres van de router in het host-venster in. Typ vervolgens de naam en het wachtwoord van VPN-groep en klik op



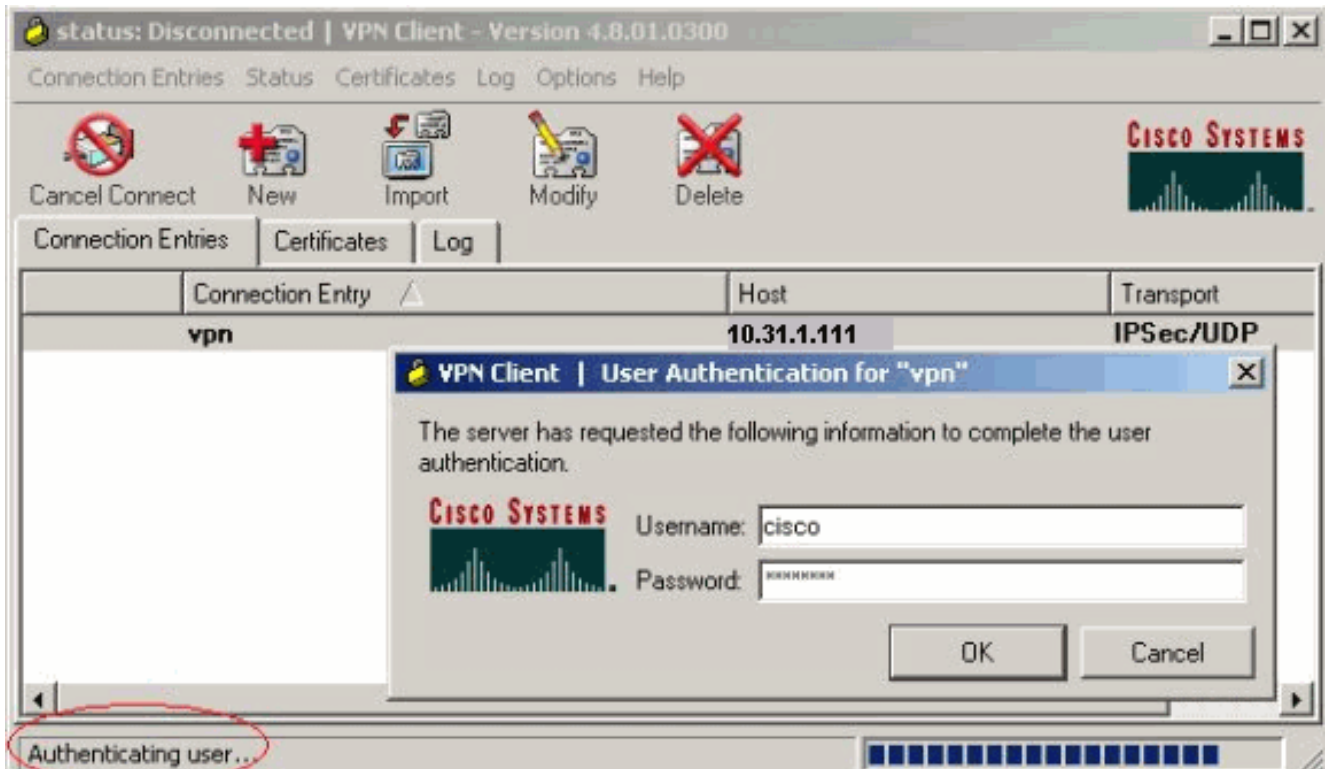
Opslaan.

4. Klik op de verbinding die u wilt gebruiken en klik op **Connect** vanuit het hoofdvenster van VPN-

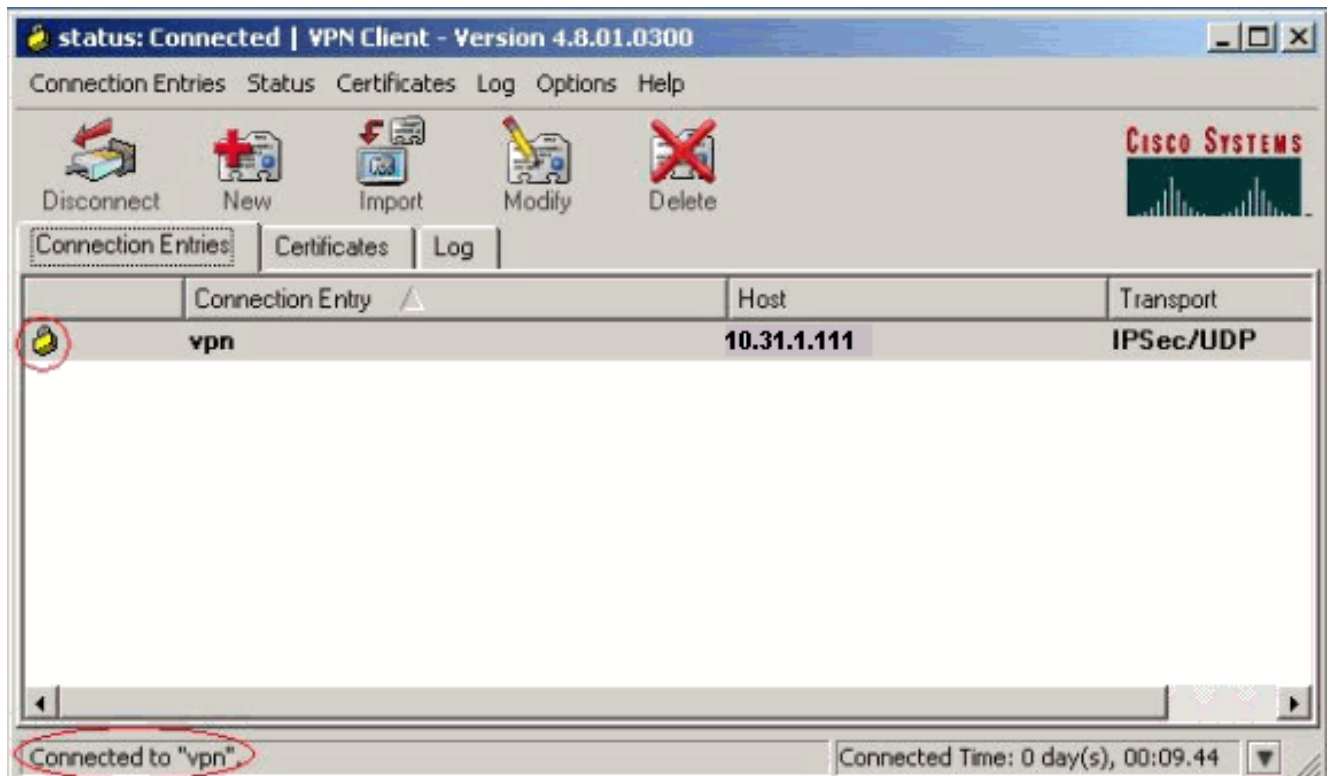
client.



5. Voer desgevraagd de informatie over de naam van de gebruiker en het wachtwoord in en klik vervolgens op **OK** om verbinding te maken met het externe netwerk.



De VPN client wordt verbonden met de router op de centrale site.













Configuratie van de TACACS+ server met Cisco Secure ACS


Voltooi deze stappen om TACACS+ in een Cisco Secure ACS te configureren:

1. U moet de router configureren om de Cisco Secure ACS te lokaliseren om de gebruikersreferenties te controleren. Bijvoorbeeld:

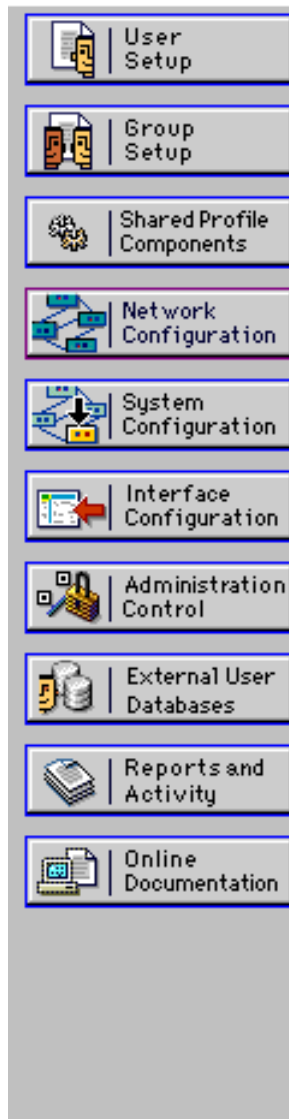
```
3640(config)#  
aaa group server tacacs+ RTP  
3640(config)#  
tacacs-server host 10.14.14.3 key cisco
```
2. Kies **Netwerkconfiguratie** aan de linkerkant en klik op **Toegang toevoegen** om een ingang voor de router in de TACACS+ serverdatabase toe te voegen. Kies de serverdatabase in overeenstemming met de routerconfiguratie.

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. De sleutel wordt gebruikt om tussen de 3640 router en Cisco Secure ACS-server voor verificatie te zorgen. Als u het TACACS+ protocol voor verificatie wilt selecteren, kies dan **TACACS+ (Cisco IOS)** dan in het vervolgkeuzemenu Verificeren met behulp van het TACACS+ protocol.



Add AAA Client

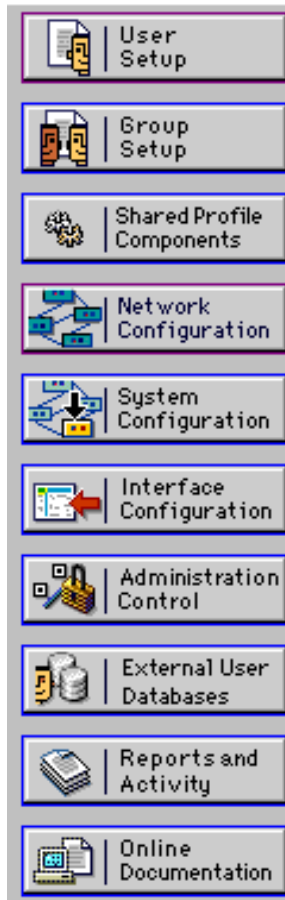
AAA Client Hostname	<input type="text" value="3640"/>
AAA Client IP Address	<input type="text" value="10.14.14.14"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in 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. Voer de gebruikersnaam in het veld Gebruiker in de Cisco Secure-database in en klik vervolgens op **Toevoegen/bewerken**. In dit voorbeeld is de gebruikersnaam een gebruiker.



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. Voer in het volgende venster het wachtwoord voor gebruiker in. In dit voorbeeld is het wachtwoord een gebruikersnaam. U kunt de gebruikersaccount desgewenst aan een groep toewijzen. Klik na voltooiing van het programma op **Inzenden**.



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

De back-upfunctie configureren

Wanneer de primaire RADIUS-server niet beschikbaar wordt, zal de router uitvallen op de volgende actieve RADIUS-server. De router zal de secundaire RADIUS-server altijd blijven gebruiken, zelfs als de primaire server beschikbaar is. De primaire server heeft meestal hoge prestaties en de voorkeursserver. Als de secundaire server niet beschikbaar is, kan de lokale database gebruikt worden voor authenticatie met behulp van de [AAA-authenticatie loginloggroep RTP lokale](#) opdracht.

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Stel een IPSec-tunnel in tussen de PC en Cisco 3640 router.

Open een browser op de PC en verwijder deze naar <http://10.17.17.17>. De Cisco 3640 router onderbreekt dit HTTP verkeer, zet authenticatie proxy in en vraagt u om een gebruikersnaam en wachtwoord. Cisco 3640 verstuurt de gebruikersnaam/het wachtwoord naar de TACACS+ server voor verificatie. Als de authenticatie succesvol is, zou u de webpagina's op de webserver op 10.17.17.17 moeten kunnen zien.

Bepaalde opdrachten met **show** worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). Hiermee kunt u een analyse van de output van opdrachten met **show** genereren.

- [Toon ip toegang-lijsten](#)-Toont de standaard en uitgebreide ACLs die op de firewallrouter zijn ingesteld (omvat dynamische ACL-items). De dynamische ACL-items worden toegevoegd en periodiek verwijderd op basis van of de gebruiker echt is geworden. Deze output toont toegangslijst 118 voordat auth-proxy werd geactiveerd:

```
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)
```

Deze output toont toegangslijst 118 nadat auth-proxy was geactiveerd en de gebruiker met succes authenticceert:

```
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)
```

De eerste drie lijnen van de toegangslijst zijn de items die voor deze gebruiker zijn gedefinieerd en gedownload worden van de TACACS+ server.

- [Toon ip auth-proxy cache](#)-Hiermee geeft u de authenticatie proxy-items of de actieve authenticatie-configuratie weer. Het cache sleutelwoord om een lijst op te geven van het host IP-adres, het bronpoortnummer, de timeout waarde voor de authenticatie proxy en de staat voor verbindingen die authenticatie proxy gebruiken. Als de authenticatieproxy status ESTAB is, is de gebruikersauthenticiteit een succes.

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

Problemen oplossen

Raadpleeg voor de opdrachten verificatie en debugging, samen met andere informatie over probleemoplossing, de [verificatieproxy voor probleemoplossing](#).

Opmerking: Voordat u **debug**-opdrachten afgeeft, raadpleegt u [Belangrijke informatie over Debug Commands](#).

Gerelateerde informatie

- [Verificatieproxy configureren](#)
- [Configuraties van verificatieproxy in Cisco IOS-software](#)
- [Verificatieproxy in TACACS+ en RADIUS-servers uitvoeren](#)
- [Cisco VPN-clientondersteuningspagina](#)
- [IOS-ondersteuningspagina](#)
- [IPsec-ondersteuningspagina](#)
- [RADIUS-ondersteuningspagina](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Ondersteuningspagina voor TACACS/TACACS+](#)
- [TACACS+ in IOS-documentatie](#)
- [Technische ondersteuning - Cisco-systemen](#)