

IOS-Router: Authentifizierungsproxy-eingehende Authentifizierung mit ACS für IPSec- und VPN-Client-Konfiguration

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Konfiguration](#)

[Konfiguration des VPN-Clients 4.8](#)

[Konfigurieren des TACACS+-Servers mit Cisco Secure ACS](#)

[Konfigurieren der Fallback-Funktion](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Die Authentifizierungsproxyfunktion ermöglicht es Benutzern, sich bei einem Netzwerk anzumelden oder über HTTP auf das Internet zuzugreifen, wobei ihre spezifischen Zugriffsprofile automatisch von einem TACACS+- oder RADIUS-Server abgerufen und angewendet werden. Die Benutzerprofile sind nur aktiv, wenn der aktive Datenverkehr der authentifizierten Benutzer vorhanden ist.

Diese Konfiguration soll den Webbrowser am 10.1.1.1 aufrufen und auf 10.17.17.17 richten. Da der VPN-Client so konfiguriert ist, dass er den Tunnel-Endpunkt 10.31.1.11 durchläuft, um zum 10.17.17.x-Netzwerk zu gelangen, wird der IPSec-Tunnel erstellt, und der PC erhält die IP-Adresse aus dem RTP-POOL-Pool (da die Moduskonfiguration durchgeführt wird). Die Authentifizierung wird dann vom Cisco Router 3640 angefordert. Nachdem der Benutzer einen Benutzernamen und ein Kennwort eingegeben hat (auf dem TACACS+-Server unter 10.14.14.3 gespeichert), wird die vom Server übergebene Zugriffsliste der Zugriffsliste 118 hinzugefügt.

Voraussetzungen

Anforderungen

Stellen Sie vor dem Versuch dieser Konfiguration sicher, dass Sie die folgenden Anforderungen erfüllen:

- Der Cisco VPN Client ist so konfiguriert, dass ein IPSec-Tunnel mit dem Cisco 3640 Router eingerichtet wird.
- Der TACACS+-Server ist für den Authentifizierungsproxy konfiguriert. Weitere Informationen finden Sie im Abschnitt "Zugehörige Informationen".

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS? Softwareversion 12.4
- Cisco Router 3640
- Cisco VPN Client für Windows 4.8 (alle VPN Client 4.x und höher sollten funktionieren)

Hinweis: Der Befehl `ip auth-proxy` wurde in Version 12.0.5.T der Cisco IOS-Software eingeführt. Diese Konfiguration wurde mit Version 12.4 der Cisco IOS-Software getestet.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

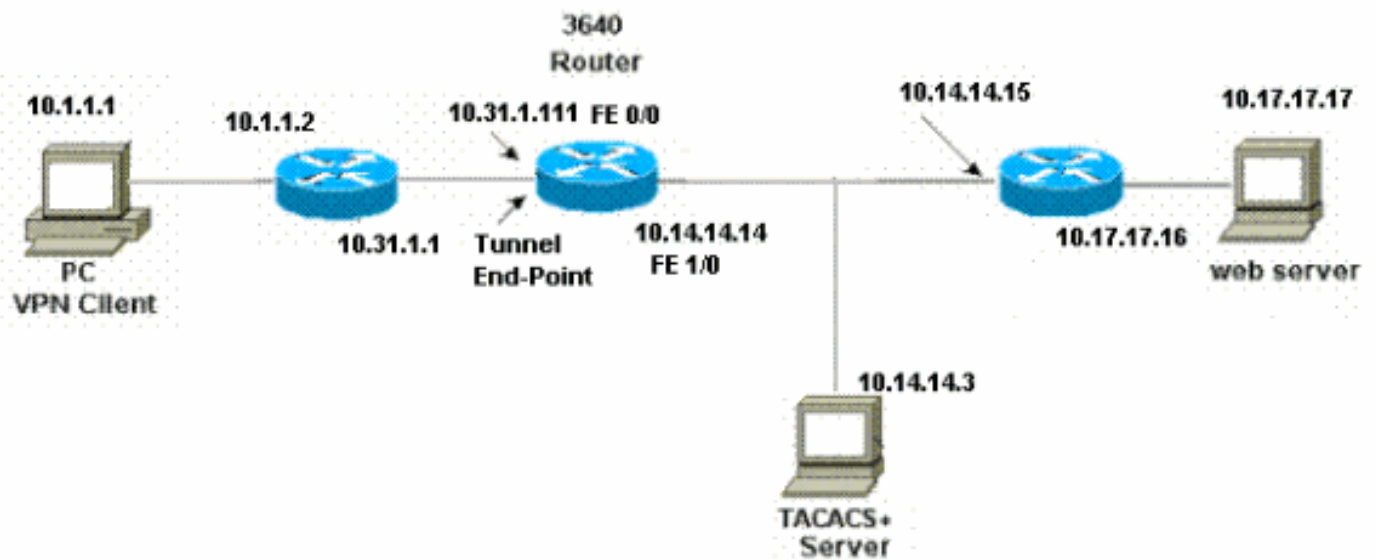
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte](#) Kunden).

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration

Router 3640

```

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

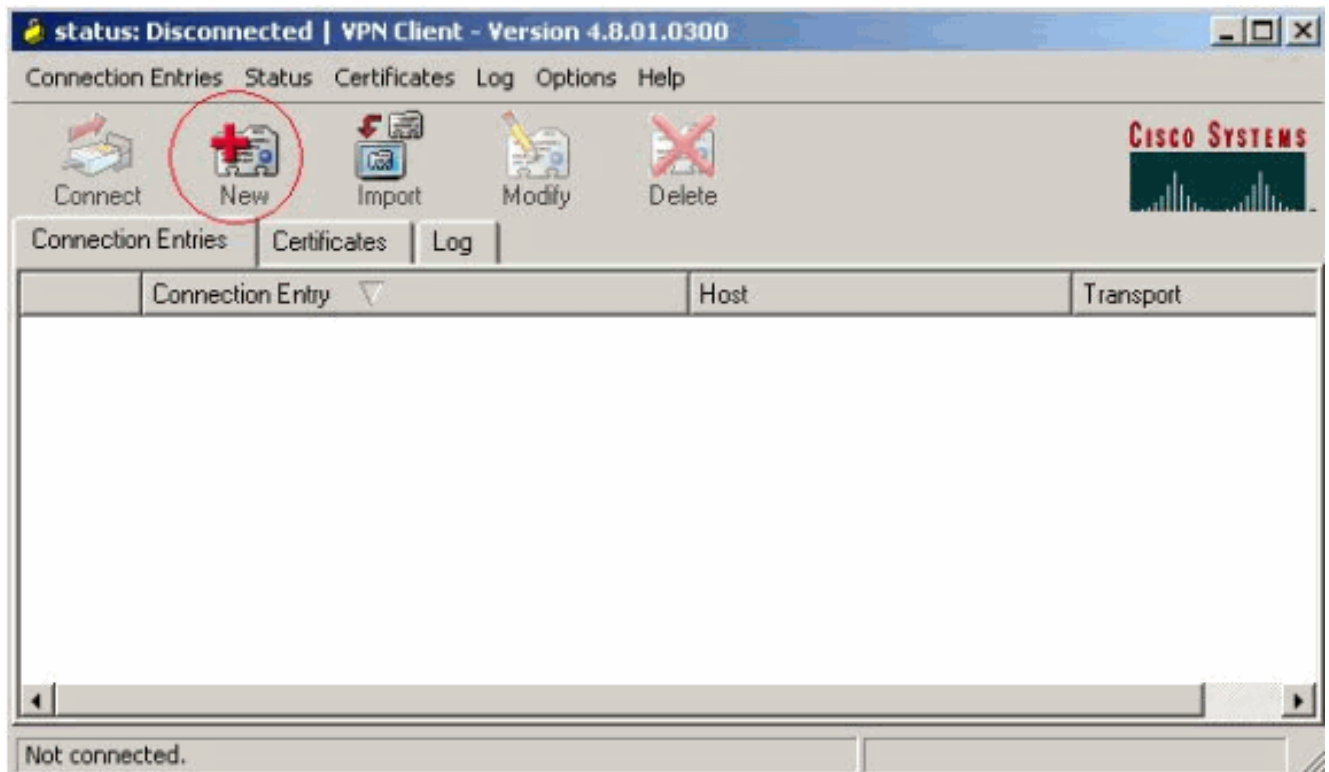
!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list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

```

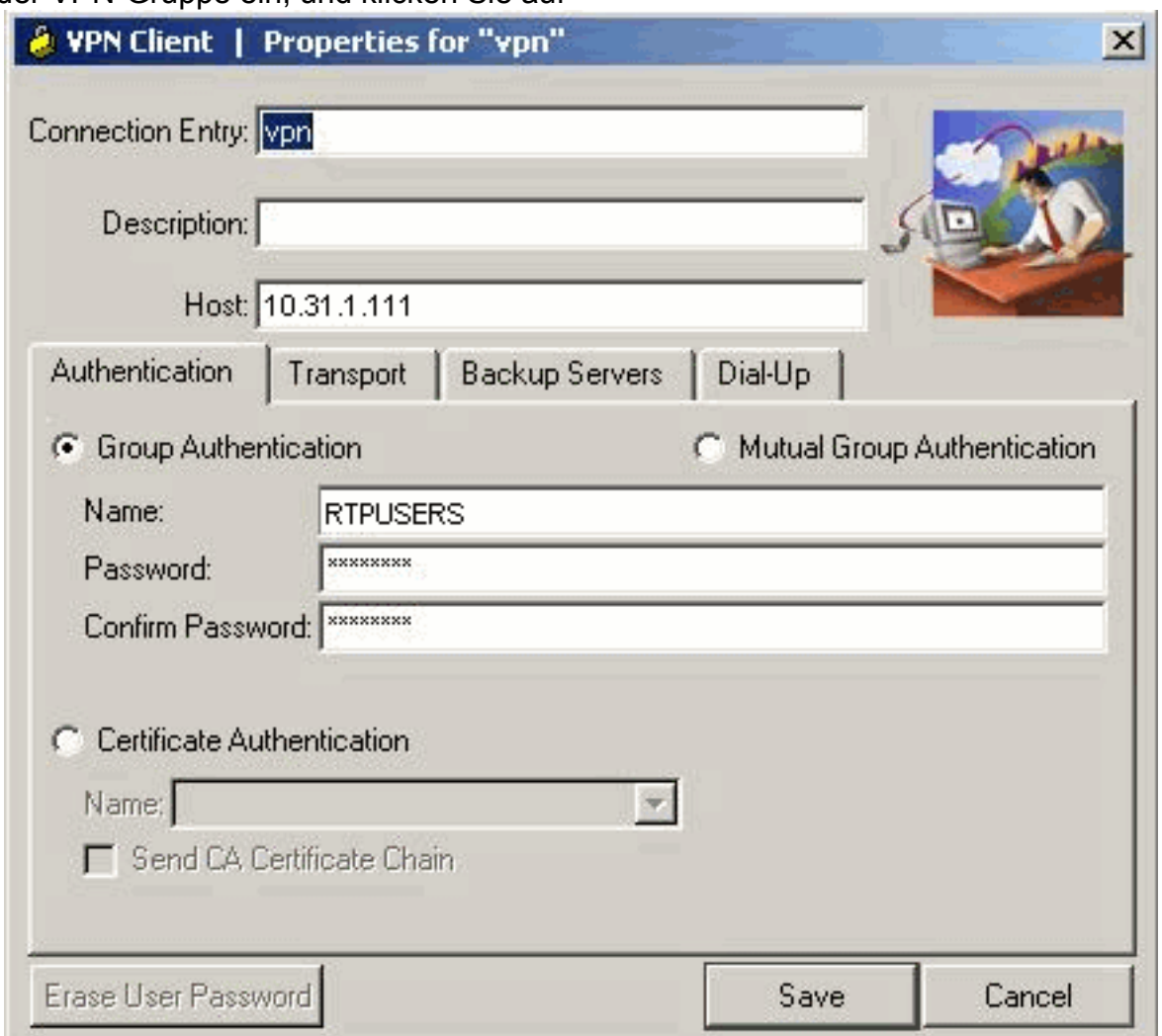
Konfiguration des VPN-Clients 4.8

Gehen Sie wie folgt vor, um den VPN Client 4.8 zu konfigurieren:

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client** aus.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-Verbindung erstellen) zu öffnen.



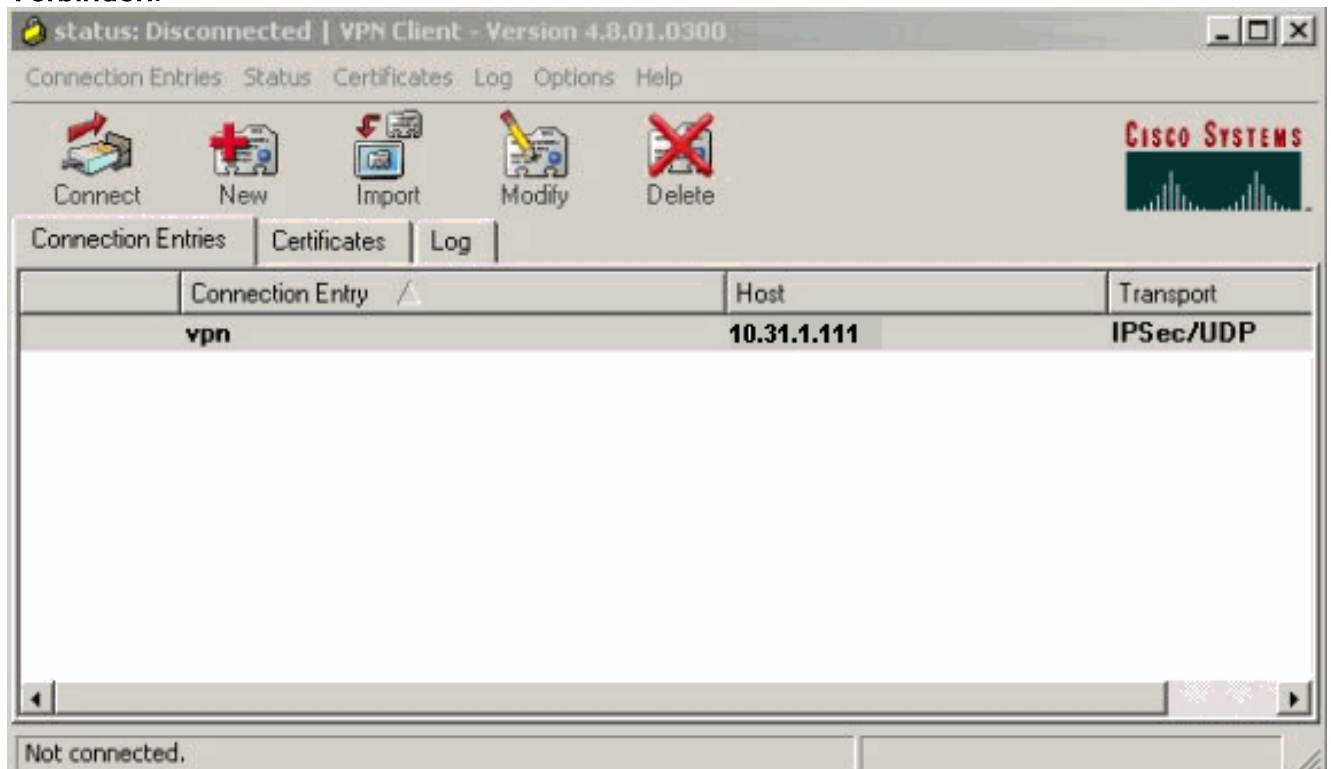
3. Geben Sie den Namen des Verbindungseintrags und eine Beschreibung ein. Geben Sie die externe IP-Adresse des Routers in das Feld Host ein. Geben Sie dann den Namen und das Kennwort der VPN-Gruppe ein, und klicken Sie auf



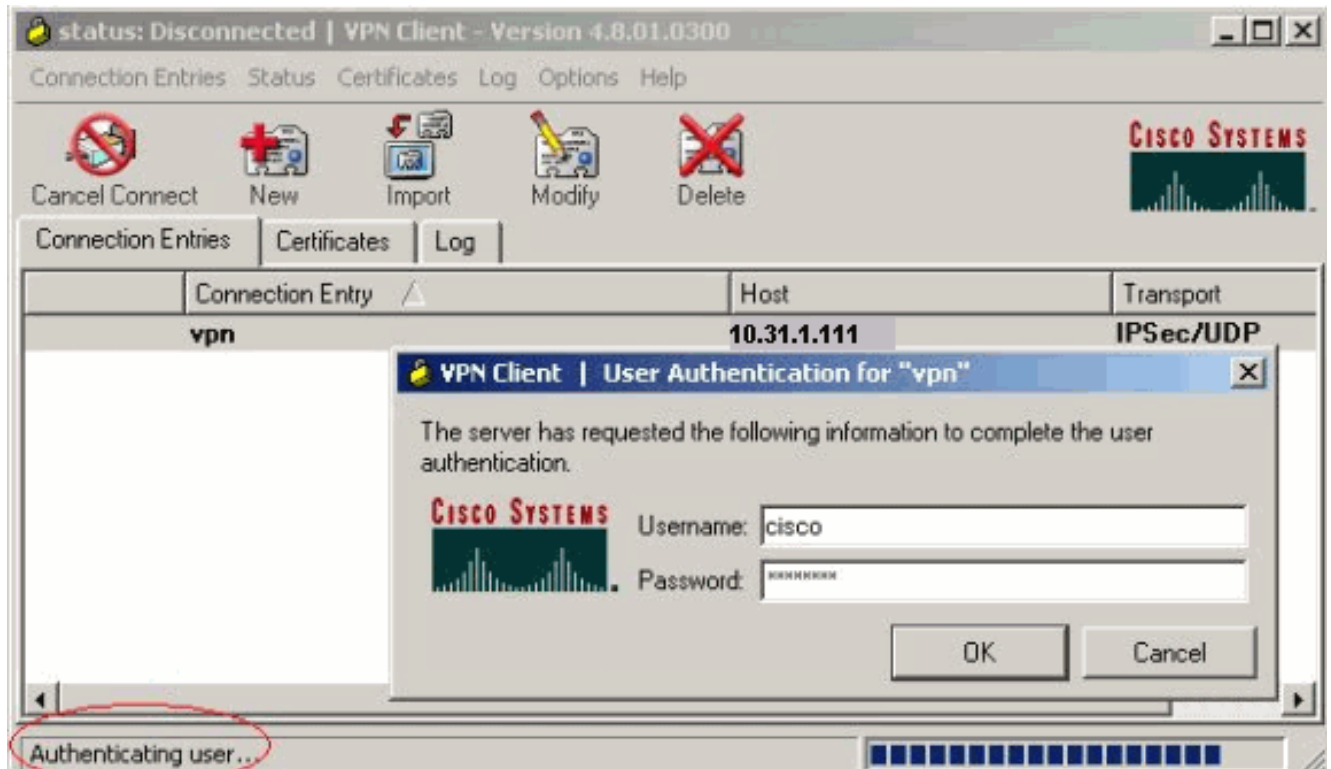
Speichern.

4. Klicken Sie auf die Verbindung, die Sie verwenden möchten, und klicken Sie im Hauptfenster des VPN-Clients auf

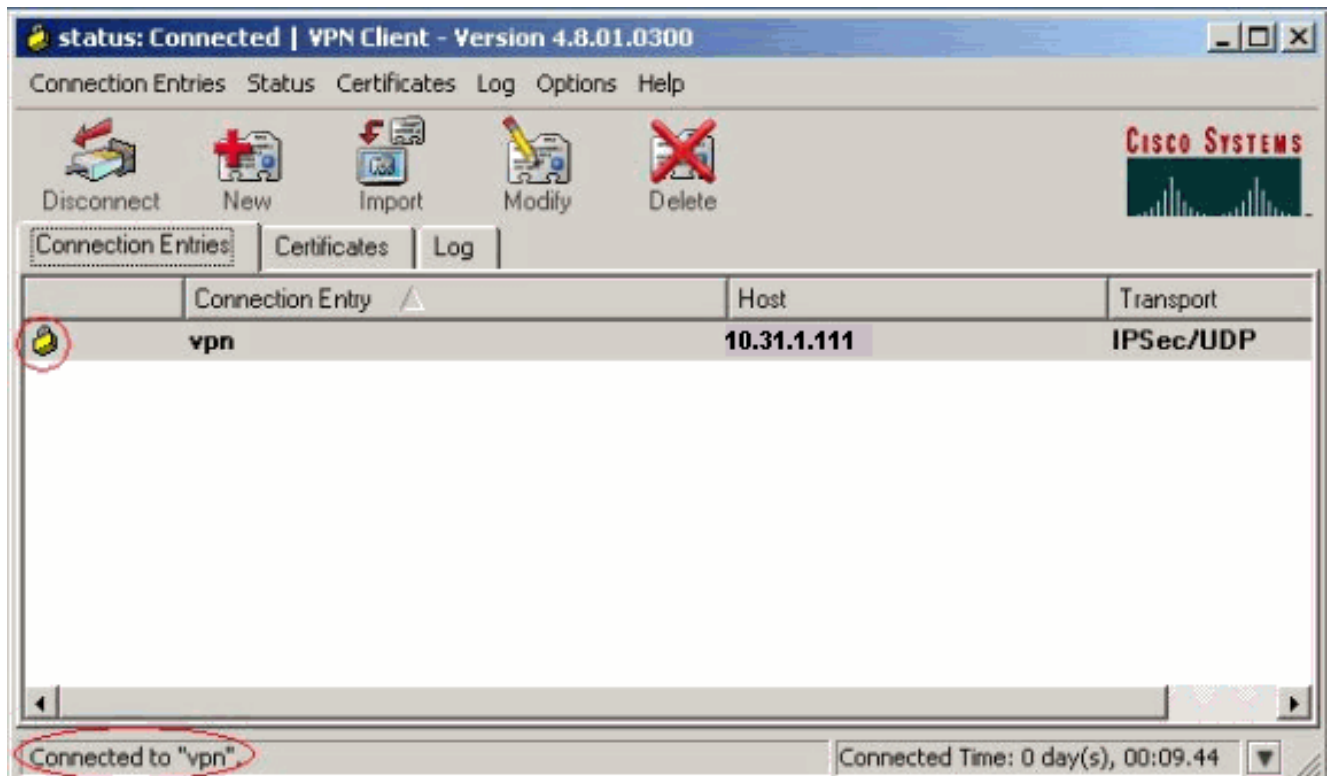
Verbinden.



5. Geben Sie bei Aufforderung die Benutzernamen- und Kennwortinformationen für xauth ein, und klicken Sie auf **OK**, um eine Verbindung zum Remote-Netzwerk herzustellen.



Der VPN-Client wird mit dem Router in der Zentrale verbunden.



Konfigurieren des TACACS+-Servers mit Cisco Secure ACS

Gehen Sie wie folgt vor, um TACACS+ in einem Cisco Secure ACS zu konfigurieren:

1. Sie müssen den Router so konfigurieren, dass er den Cisco Secure ACS ausfindig macht, um die Benutzeranmeldeinformationen zu überprüfen. Beispiel:

```
3640(config)#
```











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


```
3640(config)#
```

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

2. Wählen Sie **Netzwerkconfiguration** links aus, und klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um einen Eintrag für den Router in der TACACS+-Serverdatenbank hinzuzufügen. Wählen Sie die Serverdatenbank entsprechend der Router-Konfiguration aus.

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. Der Schlüssel dient zur Authentifizierung zwischen dem Router 3640 und dem Cisco Secure ACS-Server. Wenn Sie das TACACS+-Protokoll für die Authentifizierung auswählen möchten, wählen Sie **TACACS+ (Cisco IOS)** im Dropdown-Menü Authenticate Using (Authentifizieren über) aus.

- 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

AAA Client IP Address

Key

Authenticate Using

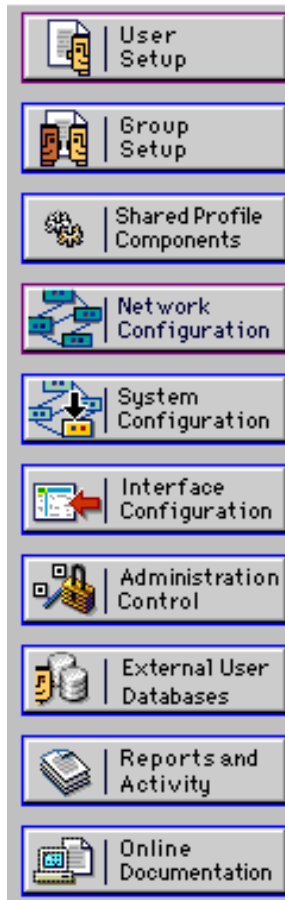
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

Submit

Submit + Restart

Cancel

4. Geben Sie den Benutzernamen in das Feld Benutzer in der Cisco Secure-Datenbank ein, und klicken Sie dann auf **Hinzufügen/Bearbeiten**. In diesem Beispiel ist der Benutzername "rtpuser".



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. Geben Sie im nächsten Fenster das Kennwort für rtpuser ein. In diesem Beispiel lautet das Kennwort rtpuserpass. Sie können das Benutzerkonto einer Gruppe zuordnen, wenn Sie möchten. Wenn Sie fertig sind, klicken Sie auf **Senden**.

Erstellen Sie einen IPSec-Tunnel zwischen dem PC und dem Cisco 3640 Router.

Öffnen Sie einen Browser auf dem PC, und zeigen Sie auf <http://10.17.17.17>. Der Cisco 3640 Router fängt diesen HTTP-Datenverkehr ab, löst einen Authentifizierungsproxy aus und fordert Sie zur Eingabe eines Benutzernamens und Kennworts auf. Der Cisco 3640 sendet den Benutzernamen/das Kennwort zur Authentifizierung an den TACACS+-Server. Wenn die Authentifizierung erfolgreich ist, sollten Sie die Webseiten auf dem Webserver unter 10.17.17.17 sehen können.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- [show ip access-lists](#): Zeigt die auf dem Firewall-Router konfigurierten Standard- und erweiterten ACLs an (einschließlich dynamischer ACL-Einträge). Die dynamischen ACL-Einträge werden regelmäßig hinzugefügt und entfernt, je nachdem, ob sich der Benutzer authentifiziert oder nicht. Diese Ausgabe zeigt die Zugriffsliste 118 an, bevor der Authentifizierungsproxy ausgelöst wurde:

```
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)
```

Diese Ausgabe zeigt die Zugriffsliste 118 an, nachdem der Authentifizierungsproxy ausgelöst und der Benutzer erfolgreich authentifiziert wurde:

```
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)
```

Die ersten drei Zeilen der Zugriffsliste sind die Einträge, die für diesen Benutzer definiert und vom TACACS+-Server heruntergeladen wurden.

- [show ip auth-proxy cache](#): Zeigt entweder die Authentifizierungsproxyeinträge oder die aktuelle Authentifizierungsproxykonfiguration an. Das Cache-Schlüsselwort, um die Host-IP-Adresse, die Quell-Port-Nummer, den Timeout-Wert für den Authentifizierungsproxy und den Status für Verbindungen aufzulisten, die den Authentifizierungsproxy verwenden. Wenn der Authentifizierungsproxystatus ESTAB lautet, ist die Benutzerauthentifizierung ein Erfolg.

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

Fehlerbehebung

Die Befehle zur Überprüfung und zum Debuggen sowie weitere Informationen zur Fehlerbehebung finden Sie unter [Troubleshooting Authentication Proxy](#).

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie [Wichtige Informationen über Debug-Befehle](#).

Zugehörige Informationen

- [Konfigurieren des Authentifizierungsproxys](#)
- [Authentifizierungsproxykonfigurationen in Cisco IOS](#)
- [Implementieren des Authentifizierungsproxys in TACACS+- und RADIUS-Servern](#)
- [Support-Seite für Cisco VPN-Clients](#)
- [Support-Seite für IOS-Firewall](#)
- [IPSec-Support-Seite](#)
- [RADIUS-Support-Seite](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Support-Seite für TACACS/TACACS+](#)
- [TACACS+ in der IOS-Dokumentation](#)
- [Technischer Support - Cisco Systems](#)