

Esempio di IPsec tra un concentratore VPN 3000 e un client VPN 4.x per Windows con RADIUS per l'autenticazione utente e la configurazione dell'accounting

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Uso dei gruppi sul concentratore VPN 3000](#)

[Utilizzo degli attributi di gruppo e utente da parte di VPN 3000 Concentrator](#)

[VPN serie 3000 Concentrator Configuration](#)

[Configurazione server RADIUS](#)

[Assegna un indirizzo IP statico all'utente client VPN](#)

[Configurazione client VPN](#)

[Aggiungi accounting](#)

[Verifica](#)

[Verifica di VPN Concentrator](#)

[Verificare il client VPN](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi di VPN Client 4.8 per Windows](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come stabilire un tunnel IPsec tra un concentratore Cisco VPN 3000 e un client Cisco VPN 4.x per Microsoft Windows che utilizza RADIUS per l'autenticazione e l'accounting dell'utente. In questo documento viene consigliato Cisco Secure Access Control Server (ACS) per Windows, in modo da semplificare la configurazione di RADIUS e autenticare gli utenti che si connettono a un concentratore VPN 3000. Un gruppo su un concentratore VPN 3000 è una raccolta di utenti trattati come entità singola. La configurazione dei gruppi, a differenza dei singoli utenti, può semplificare la gestione del sistema e semplificare le attività di configurazione.

Per configurare la connessione VPN di accesso remoto tra un client VPN di Cisco (4.x per Windows) e l'appliance di sicurezza PIX serie 500 7.x che utilizza un server RADIUS Microsoft

Windows 2003, fare riferimento agli [esempi di configurazione dell'autenticazione RADIUS PIX/ASA 7.x e del client VPN di Cisco 4.x per Windows 2003](#) per Windows.

Per configurare una connessione tra un router e il client VPN Cisco 4.x che utilizza RADIUS per l'autenticazione dell'utente, fare riferimento alla [configurazione di IPsec tra un router Cisco IOS e un client VPN Cisco 4.x per Windows](#) che utilizza RADIUS per l'autenticazione dell'utente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure ACS per Windows RADIUS è installato e funziona correttamente con altri dispositivi.
- Cisco VPN 3000 Concentrator è configurato e può essere gestito con l'interfaccia HTML.

Componenti usati

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

- Cisco Secure ACS per Windows con versione 4.0
- Cisco VPN serie 3000 Concentrator con file immagine 4.7.2.B
- Cisco VPN Client 4.x

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

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

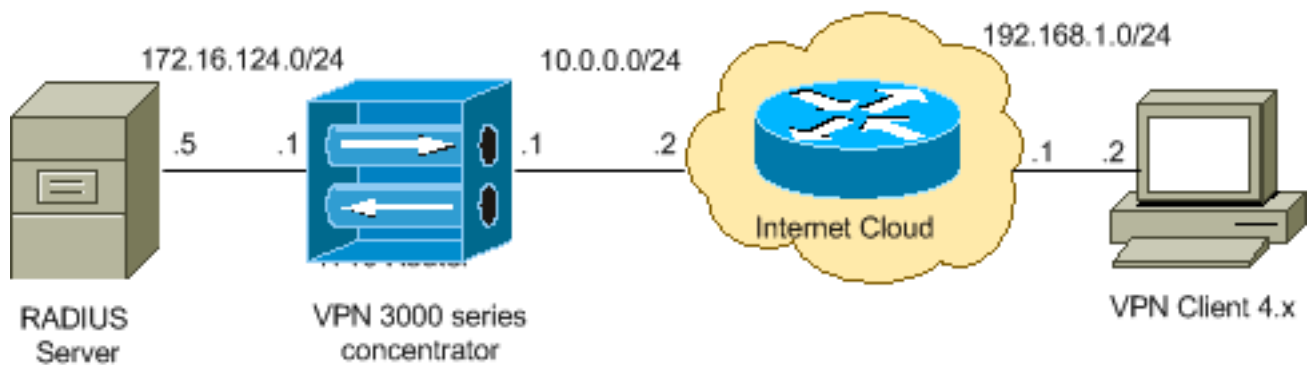
Configurazione

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 questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi [RFC 1918](#) utilizzati in un ambiente lab.

[Uso dei gruppi sul concentratore VPN 3000](#)

I gruppi possono essere definiti sia per Cisco Secure ACS for Windows che per VPN 3000 Concentrator, ma utilizzano gruppi in modo leggermente diverso. Per semplificare le procedure, eseguire le seguenti attività:

- **Configurare un singolo gruppo sul VPN 3000 Concentrator** per quando si stabilisce il tunnel iniziale. Questo viene spesso chiamato Tunnel Group e viene usato per stabilire una sessione IKE (Internet Key Exchange) crittografata con il concentratore VPN 3000 usando una chiave già condivisa (la password del gruppo). Questo è lo stesso nome di gruppo e la stessa password che devono essere configurati su tutti i client VPN Cisco che vogliono connettersi al concentratore VPN.
- **Configurare nel server Cisco Secure ACS per Windows i gruppi** che utilizzano attributi RADIUS standard e attributi specifici del fornitore (VSA) per la gestione dei criteri. Le VSA da utilizzare con il concentratore VPN 3000 sono gli attributi RADIUS (VPN 3000).
- **Configurare gli utenti sul server Cisco Secure ACS per Windows RADIUS e assegnarli a uno dei gruppi** configurati sullo stesso server. Gli utenti ereditano gli attributi definiti per il proprio gruppo e Cisco Secure ACS for Windows invia tali attributi a VPN Concentrator quando l'utente viene autenticato.

[Utilizzo degli attributi di gruppo e utente da parte di VPN 3000 Concentrator](#)

Dopo aver autenticato il gruppo di tunnel con il concentratore VPN e l'utente con RADIUS, VPN 3000 deve organizzare gli attributi ricevuti. VPN Concentrator utilizza gli attributi in questo ordine di preferenza, sia che l'autenticazione venga eseguita in VPN Concentrator o con RADIUS:

1. **Attributi utente** - Questi attributi hanno sempre la precedenza su qualsiasi altro.
2. **Attributi del gruppo di tunnel:** tutti gli attributi non restituiti al momento dell'autenticazione vengono inseriti dagli attributi del gruppo di tunnel.
3. **Attributi del gruppo base:** tutti gli attributi mancanti dagli attributi utente o gruppo tunnel vengono inseriti dagli attributi del gruppo base di VPN Concentrator.

[VPN serie 3000 Concentrator Configuration](#)

Completare la procedura descritta in questa sezione per configurare un concentratore Cisco VPN 3000 per i parametri richiesti per la connessione IPsec e il client AAA per l'autenticazione

dell'utente VPN con il server RADIUS.

In questa impostazione di laboratorio, si accede prima a VPN Concentrator tramite la porta della console e viene aggiunta una configurazione minima, come mostrato nell'output:

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address -----
----- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
----- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPsec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address -----
----- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | -----
----- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

VPN Concentrator viene visualizzato in Configurazione rapida e questi elementi sono configurati.

- Ora/Data
- Interfacce/maschere in **Configurazione > Interfacce** (public=10.0.0.1/24, private=172.16.124.1/24)
- Gateway predefinito in **Configurazione > Sistema > Routing IP > Default_Gateway** (10.0.0.2)

A questo punto, VPN Concentrator è accessibile tramite HTML dalla rete interna.

Nota: se VPN Concentrator è gestito dall'esterno, è anche possibile eseguire i seguenti passaggi:

1. Scegliere **Configurazione > 1-Interfacce > 2-Pubbliche > 4-Selezione filtro IP > 1. Private** (impostazione predefinita).
2. Scegliere **Amministrazione > 7-Diritti di accesso > 2-Lista di controllo di accesso > 1-**

Aggiungi workstation Manager per aggiungere l'indirizzo IP del manager esterno.

Questa procedura è necessaria solo se si gestisce VPN Concentrator dall'esterno.

Dopo aver completato questi due passaggi, il resto della configurazione può essere eseguita dalla GUI utilizzando un browser Web e collegandosi all'IP dell'interfaccia appena configurata. In questo esempio e a questo punto, VPN Concentrator è accessibile tramite HTML dalla rete interna:

1. Scegliere **Configurazione > Interfacce** per ricontrollare le interfacce dopo aver avviato la GUI.

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

2. Completare questa procedura per aggiungere il server Cisco Secure ACS per Windows RADIUS alla configurazione di VPN 3000 Concentrator. Scegliere **Configurazione > Sistema > Server > Autenticazione**, quindi fare clic su **Aggiungi** dal menu a sinistra.

Configure and add a user authentication server.

Server Type Selecting *Internal Server* will let you add users to database. If you are using RADIUS authenticator additional authorization check, do not configure at

Authentication Server Enter IP address or hostname.

Used For Select the operation(s) for which this RADIUS se

Server Port Enter 0 for default port (1645).

Timeout Enter the timeout for this server (seconds).

Retries Enter the number of retries for this server.

Server Secret Enter the RADIUS server secret.

Verify Re-enter the secret.

Scegliere il tipo di server **RADIUS** e aggiungere questi parametri per Cisco Secure ACS for Windows RADIUS server. Lasciate tutti gli altri parametri nello stato predefinito. **Server di autenticazione:** immettere l'indirizzo IP del server Cisco Secure ACS per Windows RADIUS. **Segreto server:** immettere il segreto del server RADIUS. Deve essere lo stesso

segreto utilizzato quando si configura il concentratore VPN 3000 nella configurazione di Cisco Secure ACS per Windows. **Verifica (Verify)** - Immettete nuovamente la password per la verifica. Il server di autenticazione verrà aggiunto alla configurazione globale di VPN 3000 Concentrator. Questo server è utilizzato da tutti i gruppi tranne quando è stato definito in modo specifico un server di autenticazione. Se un server di autenticazione non è configurato per un gruppo, viene ripristinato il server di autenticazione globale.

3. Completare questa procedura per configurare il gruppo di tunnel sul concentratore VPN 3000. Scegliere **Configurazione > Gestione utente > Gruppi** dal menu a sinistra e fare clic su **Aggiungi**. Modificare o aggiungere questi parametri nelle schede Configurazione. Non fare clic su **Applica** finché non si modificano tutti i seguenti parametri: **Nota:** questi parametri rappresentano il minimo necessario per le connessioni VPN di accesso remoto. Per questi parametri si presume inoltre che le impostazioni predefinite nel gruppo base sul concentratore VPN 3000 non siano state modificate. **Identità**

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Identity Parameters

Attribute	Value	Description
Group Name	ipsecgroup	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Add Cancel

Nome gruppo (Group Name) - Digitate un nome per il gruppo. Ad esempio, IPsecUsers. **Password:** immettere una password per il gruppo. Chiave già condivisa per la sessione IKE. **Verifica (Verify)** - Immettete nuovamente la password per la verifica. **Tipo (Type)** - Accettate questa opzione come default: Interno. **IPSec**

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to remain idle before the peer is checked to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Updates are needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for members of this group. This method only applies to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization, select the authorization method. If you configure this method, you must also configure an Authorization Server.

Tipo di tunnel: scegliere **Accesso remoto**. **Autenticazione** - RADIUS. In questo modo si indica a VPN Concentrator il metodo da utilizzare per autenticare gli utenti. **Configurazione modalità (Mode Config)** - Controlla la **configurazione della modalità**. Fare clic su **Apply** (Applica).

4. Completare questa procedura per configurare più server di autenticazione su VPN 3000 Concentrator. Una volta definito il gruppo, evidenziarlo e fare clic su **Server di autenticazione** nella colonna Modifica. È possibile definire singoli server di autenticazione per ogni gruppo anche se non esistono nei server globali.

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<p>Add Group</p> <p>Modify Group</p> <p>Delete Group</p>	<p>ipsecgroup (Internally Configured)</p>	<p>Authentication Servers</p> <p>Authorization Servers</p> <p>Accounting Servers</p> <p>Address Pools</p> <p>Client Update</p> <p>Bandwidth Assignment</p> <p>WebVPN Servers and URLs</p> <p>WebVPN Port Forwarding</p>

Scegliere il tipo di server **RADIUS** e aggiungere questi parametri per Cisco Secure ACS for

Windows RADIUS server. Lasciate tutti gli altri parametri nello stato predefinito. **Server di autenticazione:** immettere l'indirizzo IP del server Cisco Secure ACS per Windows RADIUS. **Segreto server:** immettere il segreto del server RADIUS. Deve essere lo stesso segreto utilizzato quando si configura il concentratore VPN 3000 nella configurazione di Cisco Secure ACS per Windows. **Verifica (Verify)** - Immettete nuovamente la password per la verifica.

5. Scegliere **Configurazione > Sistema > Gestione indirizzi > Assegnazione** e selezionare **Usa indirizzo del server di autenticazione** per assegnare l'indirizzo IP ai client VPN del pool IP creato nel server RADIUS dopo l'autenticazione del client.

Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address Check to use the IP address supplied by the client. This can be overridden by user/group configuration.

Use Address from Authentication Server Check to use an IP address retrieved from an authentication server for the client.

Use DHCP Check to use DHCP to obtain an IP address for the client.

Use Address Pools Check to use internal address pool configuration to obtain an IP address for the client.

IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply Cancel

[Configurazione server RADIUS](#)

In questa sezione del documento viene descritta la procedura richiesta per configurare Cisco Secure ACS come server RADIUS per l'autenticazione degli utenti dei client VPN inoltrata dal client Cisco VPN serie 3000 Concentrator - AAA.

Fare doppio clic sull'icona **ACS Admin** per avviare la sessione di amministrazione sul PC su cui è in esecuzione Cisco Secure ACS per Windows RADIUS server. Eseguire l'accesso con il nome utente e la password corretti, se necessario.

1. Completare questa procedura per aggiungere il concentratore VPN 3000 alla configurazione del server Cisco Secure ACS for Windows. Per aggiungere un client AAA al server RADIUS, selezionare **Configurazione di rete** e fare clic su **Add Entry**.



Network Configuration

Select



AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

Aggiungere questi parametri per il proprio concentratore VPN 3000:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="172.16.124.1"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>
<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	

Nome host client AAA: immettere il nome host del proprio concentratore VPN 3000 (per la risoluzione DNS). **Indirizzo IP client AAA:** immettere l'indirizzo IP del concentratore VPN 3000. **Chiave:** immettere il segreto del server RADIUS. Deve essere lo stesso segreto configurato quando è stato aggiunto il server di autenticazione nel concentratore VPN. **Autentica tramite:** selezionare **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. Questo consente alla VPN 3000 VSA di essere visualizzata nella finestra Configurazione

gruppo. Fare clic su **Invia**. Selezionare **Interface Configuration**, fare clic su **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**, quindi selezionare **Group [26] Vendor-Specific** (Gruppo specifico del fornitore).

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- | | | |
|--------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/001] Access-Hours |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/002] Simultaneous-Logins |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/005] Primary-DNS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/006] Secondary-DNS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/007] Primary-WINS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/008] Secondary-WINS |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/009] SEP-Card-Assignment |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/011] Tunneling-Protocols |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/012] IPSec-Sec-Association |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/013] IPSec-Authentication |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/015] IPSec-Banner1 |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | [026/3076/016] IPSec-Allow-Passwd-Store |

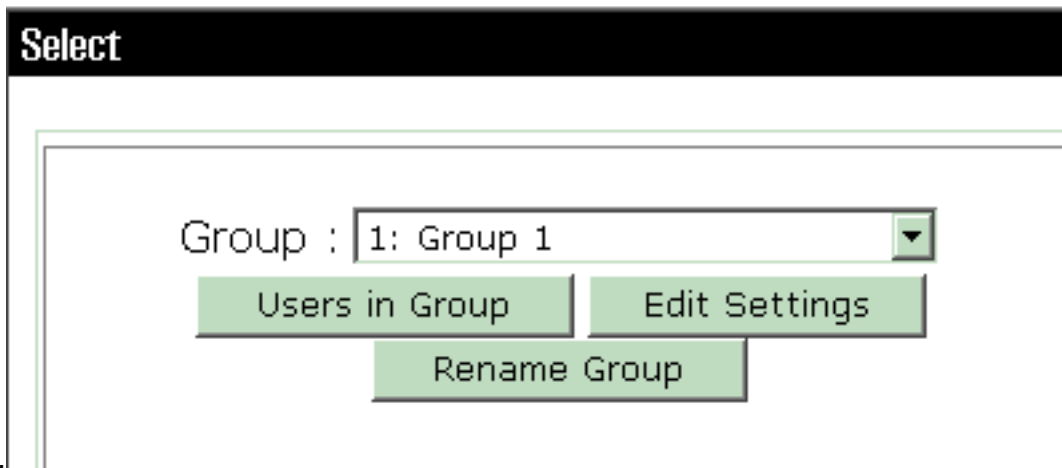
Submit

Cancel

Nota: 'attributo RADIUS 26' si riferisce a tutti gli attributi specifici del fornitore. Ad esempio, scegliere **Configurazione interfaccia > RADIUS (Cisco VPN 3000)** e verificare che tutti gli attributi disponibili inizino con 026. Ciò mostra che tutti questi attributi specifici del fornitore rientrano nello standard IETF RADIUS 26. Per impostazione predefinita, questi attributi non vengono visualizzati nelle impostazioni Utente o Gruppo. Per visualizzare la configurazione nel gruppo, creare un client AAA (in questo caso VPN 3000 Concentrator) che esegua l'autenticazione con RADIUS nella configurazione di rete. Verificare quindi gli attributi da visualizzare in Impostazione utente, Impostazione gruppo o entrambi nella configurazione interfaccia. Per ulteriori informazioni sugli attributi disponibili e sul relativo utilizzo, fare riferimento a [Attributi RADIUS](#). Fare clic su **Invia**.

2. Completare questa procedura per aggiungere gruppi alla configurazione di Cisco Secure ACS per Windows. Scegliere **Imposta gruppo**, quindi selezionare uno dei gruppi di modelli, ad esempio Gruppo 1, e fare clic su **Rinomina**

Group Setup



gruppo.

Modific


are il nome in un nome appropriato per l'organizzazione, ad esempio ipsecgroup. Poiché gli utenti vengono aggiunti a questi gruppi, fare in modo che il nome del gruppo rifletta lo scopo effettivo del gruppo. Se tutti gli utenti fanno parte dello stesso gruppo, è possibile chiamarlo Gruppo Utenti VPN. Fare clic su **Modifica impostazioni** per modificare i parametri nel gruppo appena

Group Setup


Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed

Dialup client specifies callback number

Use Windows Database callback settings (where possible)

rinominato.

Fare clic su **Cisco VPN 3000 RADIUS** e configurare gli attributi consigliati. Questo consente agli utenti assegnati a questo gruppo di ereditare gli attributi Cisco VPN 3000 RADIUS, che consentono di centralizzare i criteri per tutti gli utenti in Cisco Secure ACS for

Group Setup

Jump To IP Address Assignment

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

Windows.


No

ta: per motivi tecnici, gli attributi VPN 3000 RADIUS non devono essere configurati finché il Tunnel Group è configurato nel passaggio 3 della [configurazione del concentratore VPN 3000](#) e il Gruppo di base nel concentratore VPN non cambia rispetto alle impostazioni predefinite originali. **Attributi VPN 3000 consigliati:** **Primary-DNS:** immettere l'indirizzo IP del server DNS primario. **DNS secondario:** immettere l'indirizzo IP del server DNS secondario. **Primary-WINS:** immettere l'indirizzo IP del server WINS principale. **Secondary-WINS:** immettere l'indirizzo IP del server WINS secondario. **Protocolli di tunneling:** scegliere **IPsec**. In questo modo sono consentite *solo* connessioni client IPsec. PPTP o L2TP non sono consentiti. **IPsec-Sec-Association:** immettere **ESP-3DES-MD5**. In questo modo tutti i client IPsec si conatteranno con la crittografia più elevata disponibile. **IPsec-Allow-Password-Store:** selezionare **Disallow** in modo che *non* sia consentito salvare la password nel client VPN. **IPsec-Banner:** immettere un banner di benvenuto da presentare all'utente al momento della connessione. Ad esempio, "Benvenuto nella pagina Accesso VPN per i dipendenti della mia azienda". **Dominio predefinito IPsec:** immettere il nome di dominio della società. Ad esempio, "mycompany.com". Questo insieme di attributi non è necessario.

Tuttavia, in caso di dubbi sulla modifica degli attributi del gruppo base di VPN 3000 Concentrator, Cisco consiglia di configurare i seguenti attributi:**Accessi simultanei:** immettere il numero di accessi simultanei di un utente con lo stesso nome utente. La raccomandazione è 1 o 2.**SEP-Card-Assignment:** scegliere **Any-SEP**.**IPsec-Mode-Config:** scegliere **ON**.**IPsec over UDP:** selezionare **OFF**, a meno che non si desideri che gli utenti di questo gruppo si connettano tramite IPsec sul protocollo UDP. Se si seleziona ON, il client VPN può comunque disabilitare IPsec su UDP e connettersi normalmente.**Porta IPsec over UDP:** selezionare un numero di porta UDP compreso tra 4001 e 49151. Utilizzato solo se IPsec over UDP è attivato.Per poter utilizzare il set di attributi successivo, è prima necessario configurare qualcosa nel concentratore VPN. Questa opzione è consigliata solo per utenti esperti.**Access-Hours:** richiede la configurazione di un intervallo di ore di accesso su VPN 3000 Concentrator in **Configurazione > Gestione delle policy**. Per gestire questo attributo, utilizzare invece le ore di accesso disponibili in Cisco Secure ACS for Windows.**IPsec-Split-Tunnel-List:** è necessario configurare un elenco delle reti sul concentratore VPN in **Configurazione > Gestione policy > Gestione traffico**. Elenco delle reti inviate al client che indicano al client di crittografare i dati solo per le reti presenti nell'elenco.Scegliere **Assegnazione IP in Configurazione gruppo** e selezionare **Assegnato dal pool di server AAA** per assegnare gli indirizzi IP agli utenti client VPN dopo l'autenticazione.

Group Setup

Jump To

IP Assignment 

No IP address assignment
 Assigned by dialup client
 Assigned from AAA Client pool
 Assigned from AAA server pool

Available Pools

->

<-

Selected Pools

pool1

Up


Down

Scegliere

Configurazione di sistema > Pool IP per creare un pool IP per gli utenti VPN Client e fare clic su

System Configuration

Edit

New Pool		
Name	<input type="text" value="pool1"/>	
Start Address	<input type="text" value="10.1.1.1"/>	
End Address	<input type="text" value="10.1.1.10"/>	


Submit

Cancel

Invia.

System Configuration

Select

AAA Server IP Pools				
Pool Name	Start Address	End Address	In Use	
pool1	10.1.1.1	10.1.1.10	0%	

Per salvare la

configurazione e attivare il nuovo gruppo, scegliere **Sottometti > Riavvia**. Ripetere questi passaggi per aggiungere altri gruppi.

3. **Configurare gli utenti su Cisco Secure ACS per Windows.** Scegliere **Configurazione utente**, immettere un nome utente e fare clic su

User Setup

Select

User:

Find

Add/Edit

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](#)

List all users

Remove Dynamic Users

Aggiungi/Modifica.


onfigurare questi parametri nella sezione Impostazione utente:

C

User Setup


User: ipsecuser1 (New User)

Account Disabled


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 especially useful when token caching is enabled.

Group to which the user is assigned:



Autenticazione password: scegliere Database interno ACS. **Cisco Secure PAP - Password:** immettere una password per l'utente. **Cisco Secure PAP - Conferma password** - Reimmettere la password per il nuovo utente. **Gruppo a cui è assegnato l'utente:** selezionare il nome del gruppo creato nel passaggio precedente. Fare clic su **Submit** (Invia) per salvare e attivare le impostazioni utente. Ripetere questi passaggi per aggiungere altri utenti.

[Assegna un indirizzo IP statico all'utente client VPN](#)

Attenersi alla seguente procedura:

1. Creare un nuovo gruppo VPN IPSECGRP.
2. Creare un utente che desideri ricevere l'IP statico e scegliere **IPSECGRP**. Scegliere **Assegna indirizzo IP statico** con l'indirizzo IP statico assegnato in Assegnazione indirizzo IP

User Setup

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 especially useful when token caching is enabled.

Group to which the user is assigned:

IPSECGRP

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

Submit

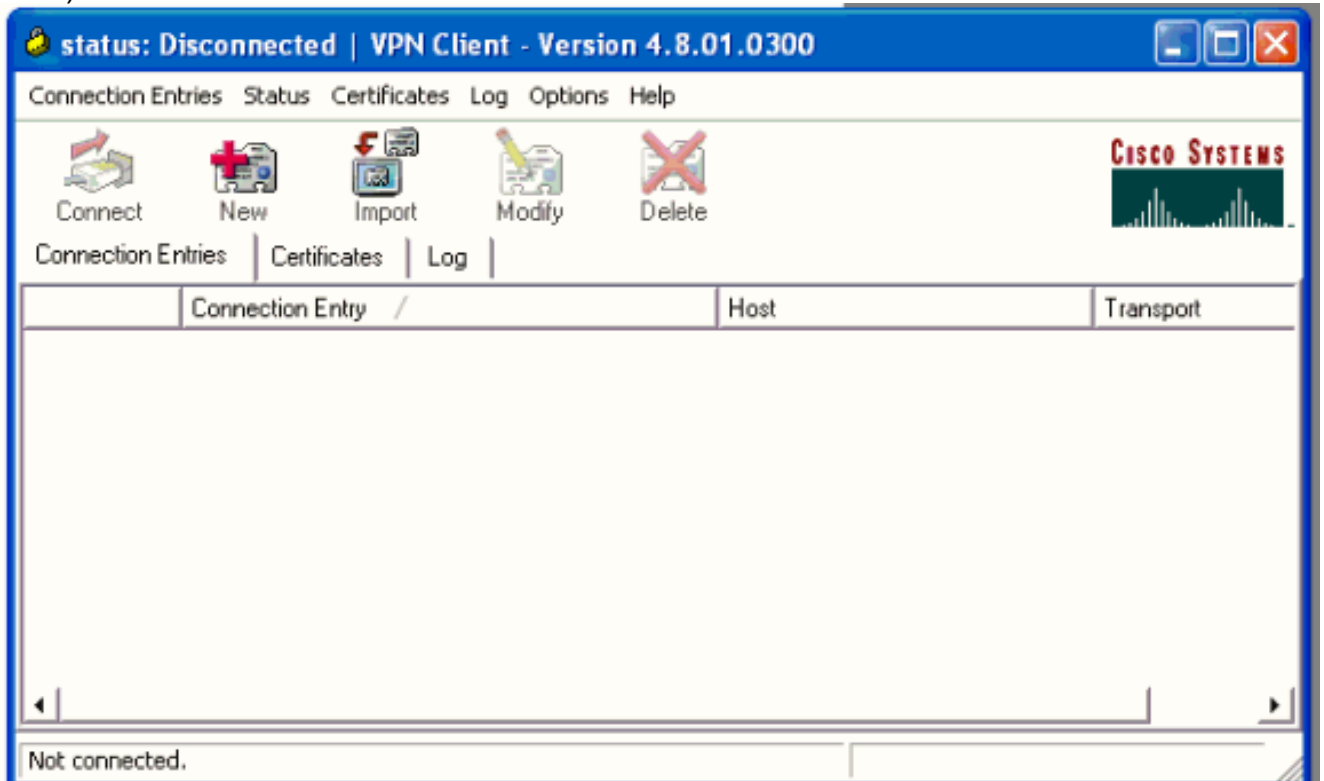
Delete

Cancel

client.

In questa sezione viene descritta la configurazione del lato client VPN.

1. Scegliere **Start > Programmi > Cisco Systems VPN Client > VPN Client**.
2. Fare clic su **New** per avviare la finestra Create New VPN Connection Entry (Crea nuova voce di connessione VPN).



3. Quando richiesto, assegnare un nome alla voce. Se lo si desidera, è inoltre possibile immettere una descrizione. Specificare l'indirizzo IP dell'interfaccia pubblica VPN 3000 Concentrator nella colonna Host e scegliere **Autenticazione gruppo**. Specificare quindi il nome e la password del gruppo. Per completare la nuova voce della connessione VPN, fare clic su **Save**

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: ipsecgroup

Password: xxxxxxxx

Confirm Password: xxxxxxxx

Certificate Authentication

Name: [dropdown]

Send CA Certificate Chain

Erase User Password | Save | Cancel

(Salva).

Not

a: verificare che il client VPN sia configurato per utilizzare lo stesso nome di gruppo e la stessa password configurati in Cisco VPN 3000 Concentrator.

[Aggiungi accounting](#)

Al termine dell'autenticazione, è possibile aggiungere l'accounting.

1. Sulla VPN 3000, scegliere **Configurazione > Sistema > Server > Server di accounting**, quindi aggiungere il server **Cisco Secure ACS per Windows**.
2. È possibile aggiungere singoli server di accounting a ogni gruppo quando si sceglie **Configurazione > Gestione utente > Gruppi**, si evidenzia un gruppo e si fa clic su **Modifica account. Server**. Immettere quindi l'indirizzo IP del server di accounting con il segreto del server.

Configure and add a RADIUS user accounting server.

Accounting Server	<input type="text" value="172.16.124.5"/>	Enter IP address or hostname.
Server Port	<input type="text" value="1646"/>	Enter the server UDP port number.
Timeout	<input type="text" value="1"/>	Enter the timeout for this server (se
Retries	<input type="text" value="3"/>	Enter the number of retries for this
Server Secret	<input type="text" value="*****"/>	Enter the RADIUS server secret.
Verify	<input type="text" value="*****"/>	Re-enter the server secret.

In Cisco Secure ACS for Windows, i record di accounting vengono visualizzati come segue:

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets
10/27/2006	18:38:20	ipseuser1	ipsegroup	192.168.1.2	Start	E8700001	..	Framed	PPP
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Verifica di VPN Concentrator

Sul lato VPN 3000 Concentrator, scegliere **Amministrazione > Amministra sessioni** per verificare che il tunnel VPN sia stato creato in remoto.

Remote Access Sessions

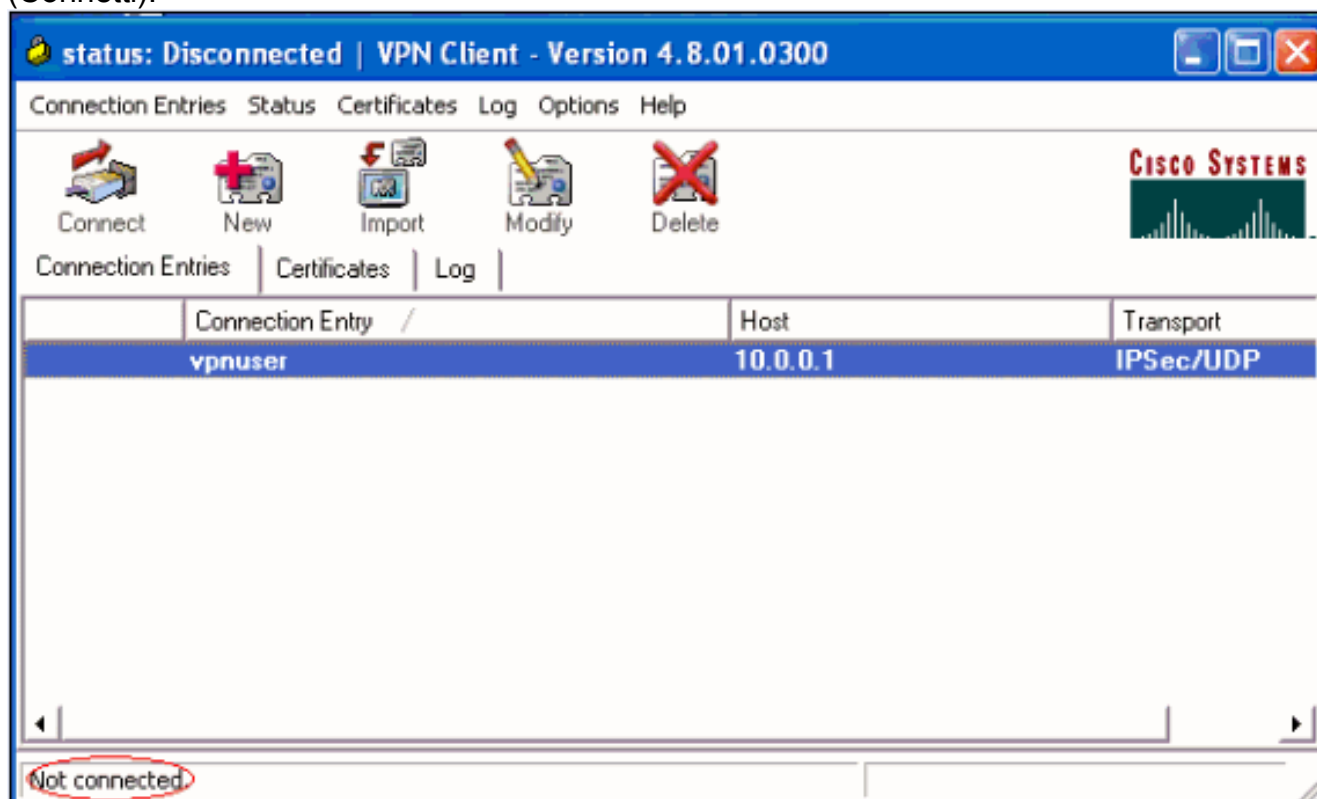
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

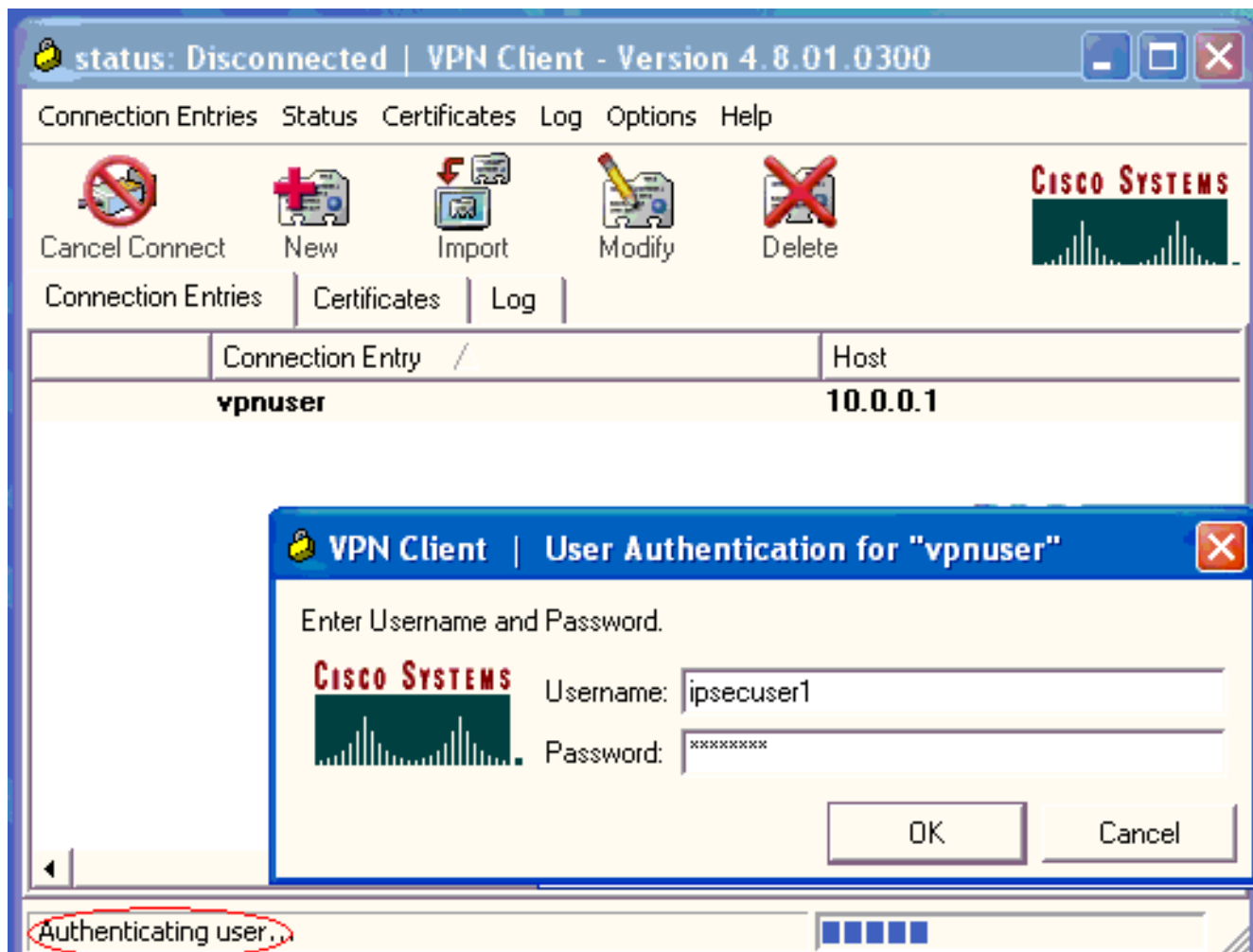
[Verificare il client VPN](#)

Completare questa procedura per verificare il client VPN.

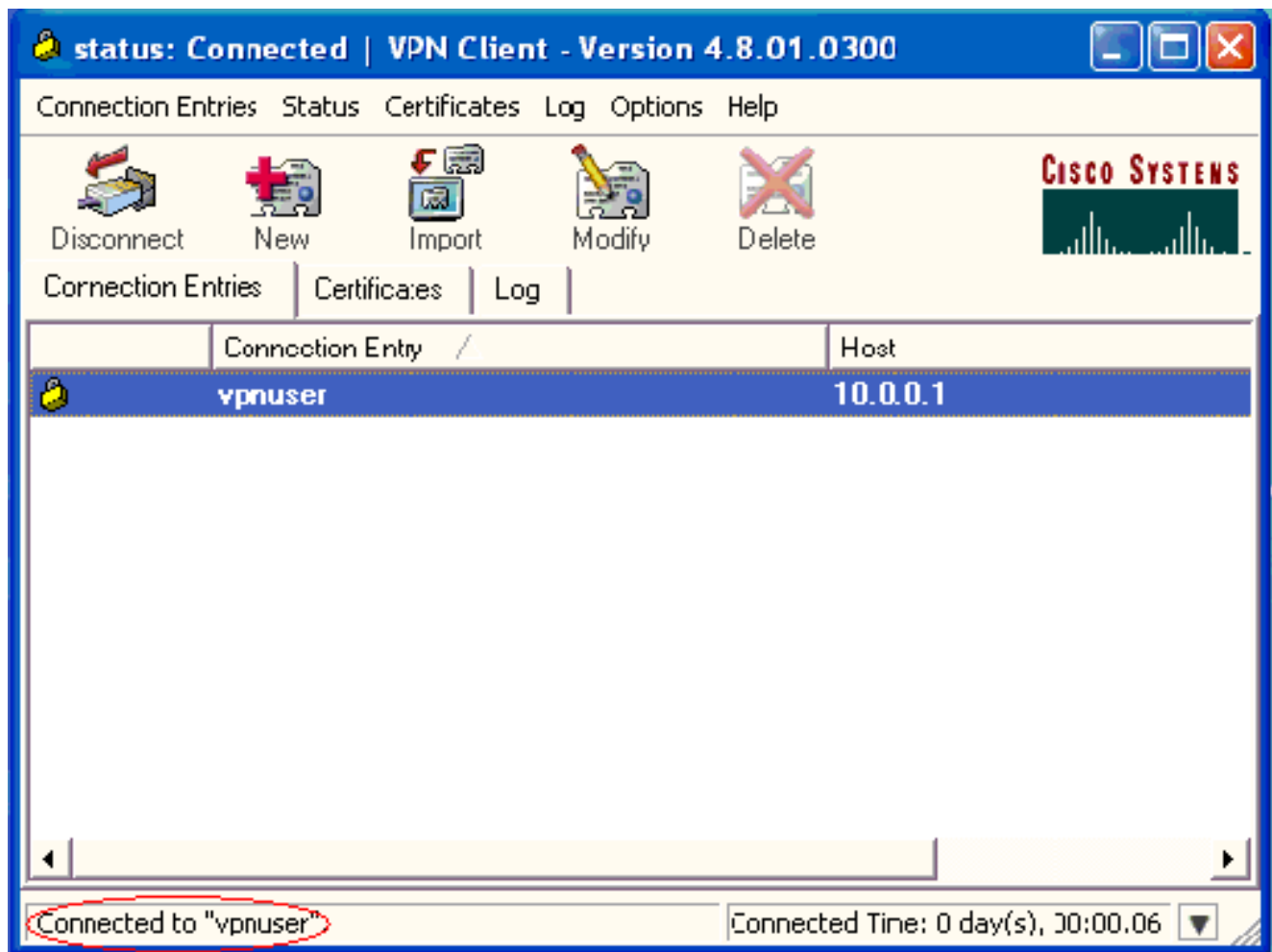
1. Per avviare una connessione VPN, fare clic su **Connect** (Connetti).



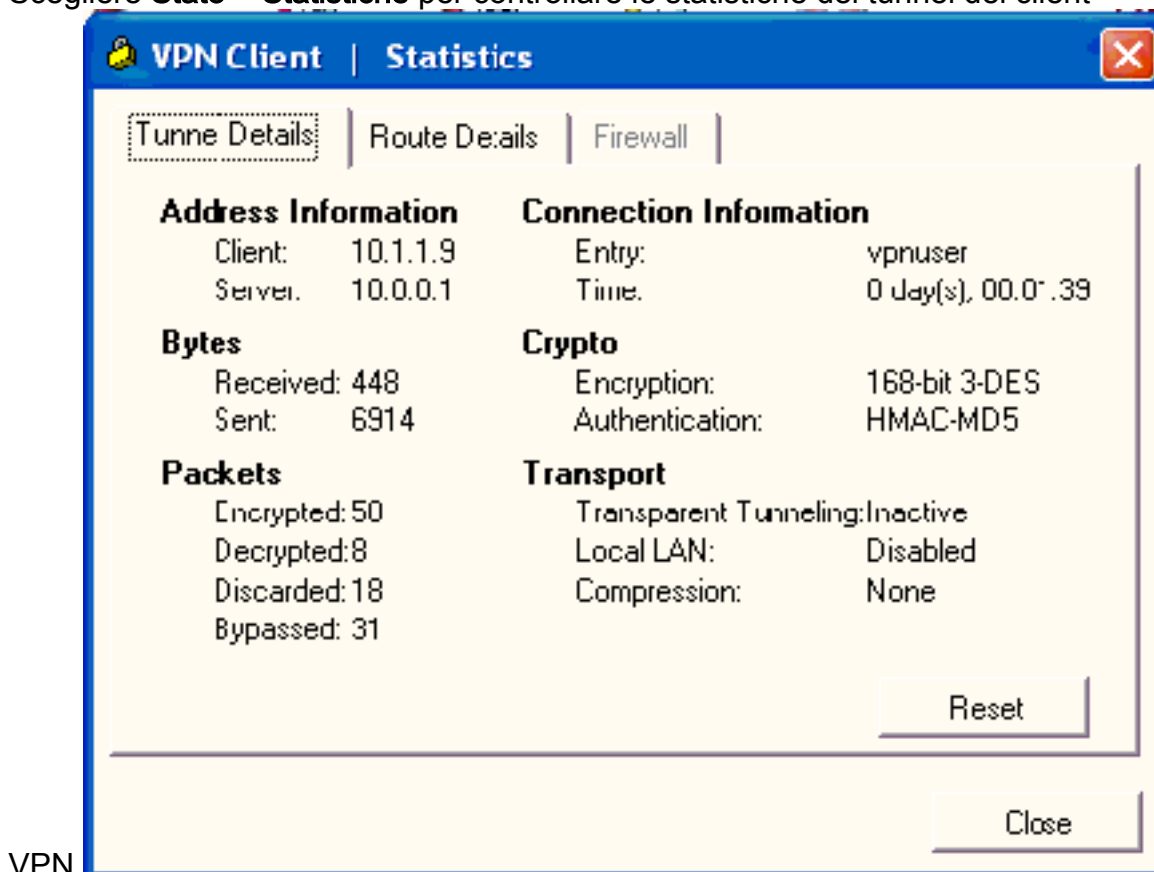
2. Questa finestra viene visualizzata per l'autenticazione dell'utente. Immettere un nome utente e una password validi per stabilire la connessione VPN.



3. Il client VPN si connette al concentratore VPN 3000 sul sito centrale.



4. Scegliere **Stato > Statistiche** per controllare le statistiche del tunnel del client



VPN.

Risoluzione dei problemi

Completare questa procedura per risolvere i problemi relativi alla configurazione.

1. Scegliere **Configurazione > Sistema > Server > Autenticazione** e completare la procedura descritta di seguito per verificare la connettività tra il server RADIUS e il concentratore VPN 3000. Selezionare il server e quindi fare clic su

Test.

Configuration | System | Servers | Authentication

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) Internal (Internal)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/>

Immettere il nome utente e la password RADIUS e fare clic su **OK**.


Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation**

Username

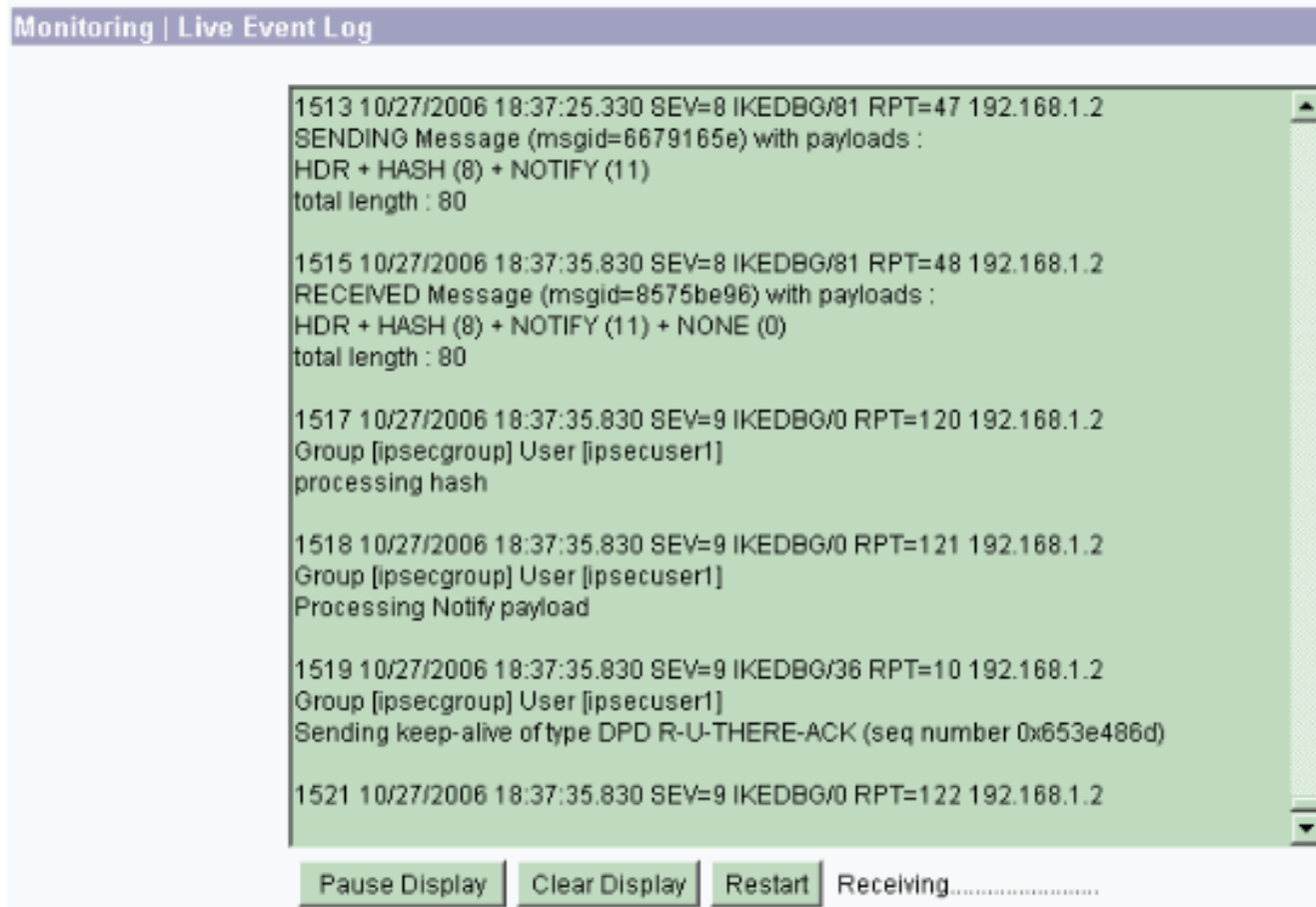
Password

Success

 Authentication Successful

Viene visualizzata un'autenticazione riuscita.

2. In caso di errore, si è verificato un problema di configurazione o di connettività IP. Controllare il registro dei tentativi non riusciti sul server ACS per i messaggi relativi all'errore. Se in questo registro non viene visualizzato alcun messaggio, è probabile che si sia verificato un problema di connettività IP. La richiesta RADIUS non raggiunge il server RADIUS. Verificare che i filtri applicati all'interfaccia VPN 3000 Concentrator appropriata consentano l'ingresso e l'uscita di pacchetti RADIUS (1645). Se il test di autenticazione ha esito positivo, ma il login a VPN 3000 Concentrator continua a non riuscire, controllare il registro eventi filtrabile tramite la porta della console. Se le connessioni non funzionano, è possibile aggiungere le classi di evento AUTH, IKE e IPsec a VPN Concentrator selezionando **Configurazione > Sistema > Eventi > Classi > Modifica (da Gravità a Registro=1-9, da Gravità a Console=1-3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG e IPSECDECODE sono disponibili, ma possono fornire troppe informazioni. Se sono necessarie informazioni dettagliate sugli attributi passati dal server RADIUS, AUTHDECODE, IKEDECODE e IPSECDECODE forniscono tale informazione al livello di gravità da Log=1 a Log=13.
3. Recuperare il registro eventi da **Monitoraggio > Registro eventi**.



```
Monitoring | Live Event Log

1513 10/27/2006 18:37:25.330 SEV=8 IKEDBG/81 RPT=47 192.168.1.2
SENDING Message (msgid=6679165e) with payloads :
HDR + HASH (8) + NOTIFY (11)
total length : 80

1515 10/27/2006 18:37:35.830 SEV=8 IKEDBG/81 RPT=48 192.168.1.2
RECEIVED Message (msgid=8575be96) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0)
total length : 80

1517 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=120 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
processing hash

1518 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=121 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Processing Notify payload

1519 10/27/2006 18:37:35.830 SEV=9 IKEDBG/36 RPT=10 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x653e486d)

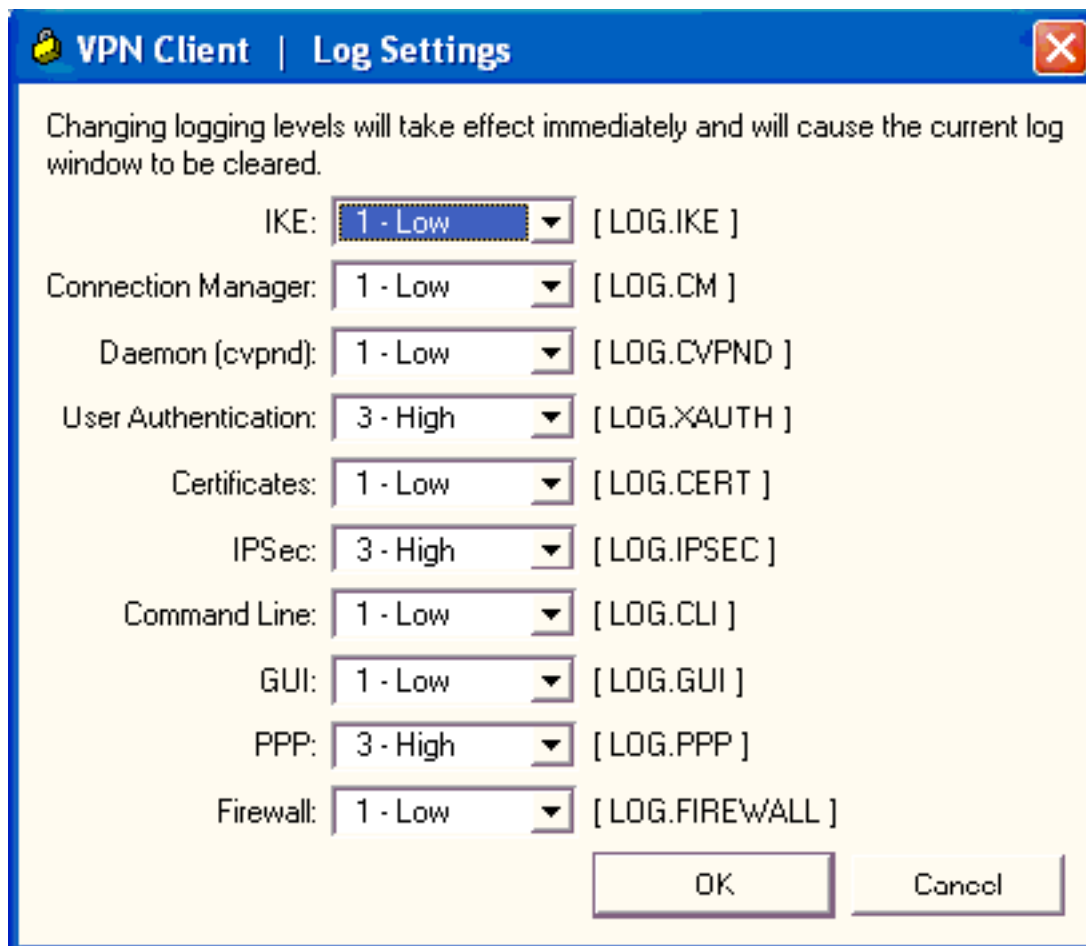
1521 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=122 192.168.1.2

Pause Display Clear Display Restart Receiving.....
```

[Risoluzione dei problemi di VPN Client 4.8 per Windows](#)

Completare questa procedura per risolvere i problemi di VPN Client 4.8 per Windows.

1. Scegliere **Log > Impostazioni log** per abilitare i livelli di log nel client



VPN.

2. Scegliere **Log > Log Window** per visualizzare le voci di log nel client VPN.

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013
AddRoute failed to add a route: code 87
Destination 192.168.1.255
Netmask 255.255.255.255
Gateway 10.1.1.9
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45

Informazioni correlate

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Pagina di supporto per Cisco VPN Client](#)
- [Negoziazione IPsec/protocolli IKE](#)
- [Pagina di supporto di Cisco Secure ACS per Windows](#)
- [Configurazione dei filtri dinamici su un server RADIUS](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)