

Esempio di configurazione di IPSec con client VPN (indirizzo IP assegnato statico/dinamico) su VPN 3000 Concentrator

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Configurazione di VPN 3000 Concentrator](#)

[Assegnazione di un indirizzo IP statico a un utente](#)

[Configurare il client VPN](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Problemi che possono verificarsi](#)

[Client VPN](#)

[VPN Concentrator](#)

[VPN 3000 Concentrator - Buono debug di esempio](#)

[Informazioni correlate](#)

[Introduzione](#)

In questa configurazione di esempio viene mostrato come formare un tunnel IPsec da un PC con client VPN Cisco (versione 4.x e successive) (indirizzo IP assegnato statico/dinamico) a un concentratore VPN 3000 di Cisco per consentire all'utente di accedere in modo sicuro alla rete all'interno del concentratore VPN.

Per ulteriori informazioni sullo stesso scenario con l'autenticazione RADIUS con Cisco ACS, consultare il documento sull'[uso di Cisco Secure ACS per Windows con VPN 3000 Concentrator - IPSec](#). Per ulteriori informazioni sullo stesso scenario con l'autenticazione MS-RADIUS, fare riferimento alla [configurazione del concentratore Cisco VPN 3000](#) con MS RADIUS.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

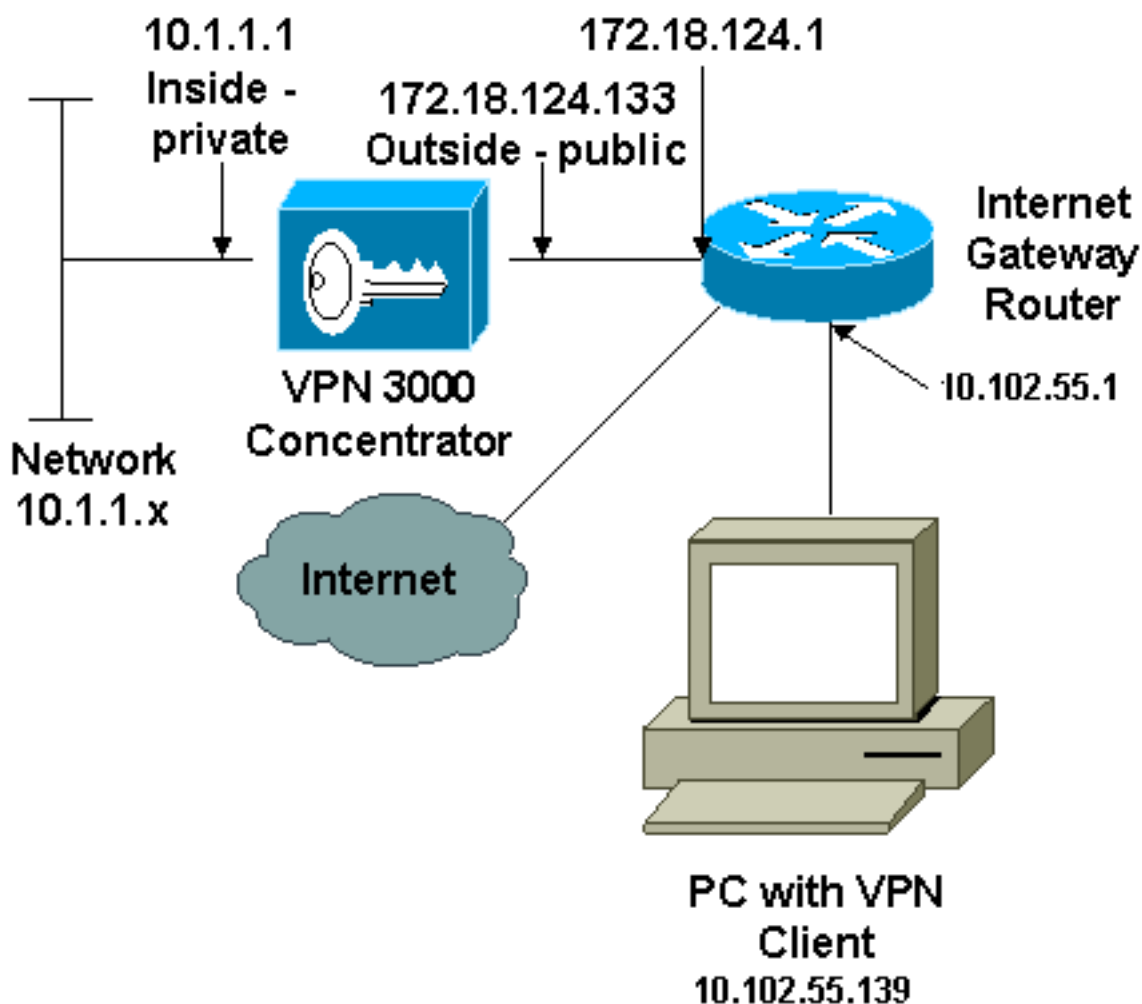
- Cisco VPN 3030 Concentrator versione 4.1.7.A
- Cisco VPN Client versione 4.x e successive

Nota: questa configurazione è stata recentemente testata nuovamente con Cisco VPN Concentrator versione 4.7.2.H.

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.

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.

Convenzioni

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

Configurazione di VPN 3000 Concentrator

Completare questa procedura per configurare il concentratore VPN 3000.

Nota: a causa dei limiti di spazio, alcune schermate mostrano solo schermate parziali.

1. Connettersi alla porta della console VPN Concentrator e verificare che vi siano indirizzi IP assegnati alle interfacce privata (interna) e pubblica (esterna). Verificare inoltre che sia stato assegnato un gateway predefinito in modo che Concentrator possa inoltrare i pacchetti per le destinazioni di cui non è a conoscenza al gateway predefinito (normalmente il router gateway Internet):

```
97 01/21/2005 12:18:50.300 SEV=3 PSH/23 RPT=1
PSH - Console user "admin" failed login
Login: admin
Password:
```

```
                Welcome to
                Cisco Systems
VPN 3000 Concentrator Series
                Command Line Interface
Copyright (C) 1998-2004 Cisco Systems, Inc.
```

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

```
Main -> _
```

```
Cisco Systems
VPN 3000 Concentrator Series
Command Line Interface
Copyright (C) 1998-2004 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

Nella tabella vengono mostrati gli indirizzi IP correnti.

- 5) Tunneling and Security
- 6) Back

Config -> 1

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	UP	10.1.1.1/255.255.255.0	00.90.A4.00.06.94
Ether2-Pub	UP	172.18.124.133/255.255.255.0	00.90.A4.00.06.95
Ether3-Ext	Not Configured	0.0.0.0/0.0.0.0	

DNS Server(s): 10.1.0.121, 10.1.0.122

DNS Domain Name:

Default Gateway: 172.18.124.1

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies
- 5) Back

Interfaces ->

DNS Domain Name:
Default Gateway: 172.18.124.1

- 1) Configure Ethernet #1 (Private)
- 2) Configure Ethernet #2 (Public)
- 3) Configure Ethernet #3 (External)
- 4) Configure Power Supplies

5) Back

Interfaces -> 5

- 1) Interface Configuration
- 2) System Management
- 3) User Management
- 4) Policy Management
- 5) Tunneling and Security
- 6) Back

Config -> 2

- 1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
- 2) Address Management
- 3) IP Routing (static routes, OSPF, etc.)
- 4) Management Protocols (Telnet, TFTP, FTP, etc.)
- 5) Event Configuration
- 6) General Config (system name, time, etc.)
- 7) Client Update
- 8) Load Balancing Configuration
- 9) Back

System -> 3_

- 8) Load Balancing Configuration
- 9) Back

System -> 3

- 1) Static Routes
- 2) Default Gateways

- 3) OSPF
- 4) OSPF Areas
- 5) DHCP Parameters
- 6) Redundancy
- 7) Reverse Route Injection
- 8) DHCP Relay
- 9) Back

Routing -> 1

Static Routes

Destination	Mask	Metric	Destination
0.0.0.0	0.0.0.0	1	172.18.124.1
10.0.0.0	255.0.0.0	10	10.1.16.111
192.168.0.0	255.255.0.0	10	10.1.16.111

- 1) Add Static Route
- 2) Modify Static Route
- 3) Delete Static Route
- 4) Back

Routing ->

```
8) Load Balancing Configuration
9) Back

System -> 3

1) Static Routes
2) Default Gateways

3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back

Routing -> 1

Static Routes
-----
Destination      Mask           Metric Destination
-----
0.0.0.0          0.0.0.0       1 172.18.124.1

1) Add Static Route
2) Modify Static Route
3) Delete Static Route
4) Back

Routing ->
```

2. Accertarsi di scegliere l'opzione di filtro **Public** per l'interfaccia Public.

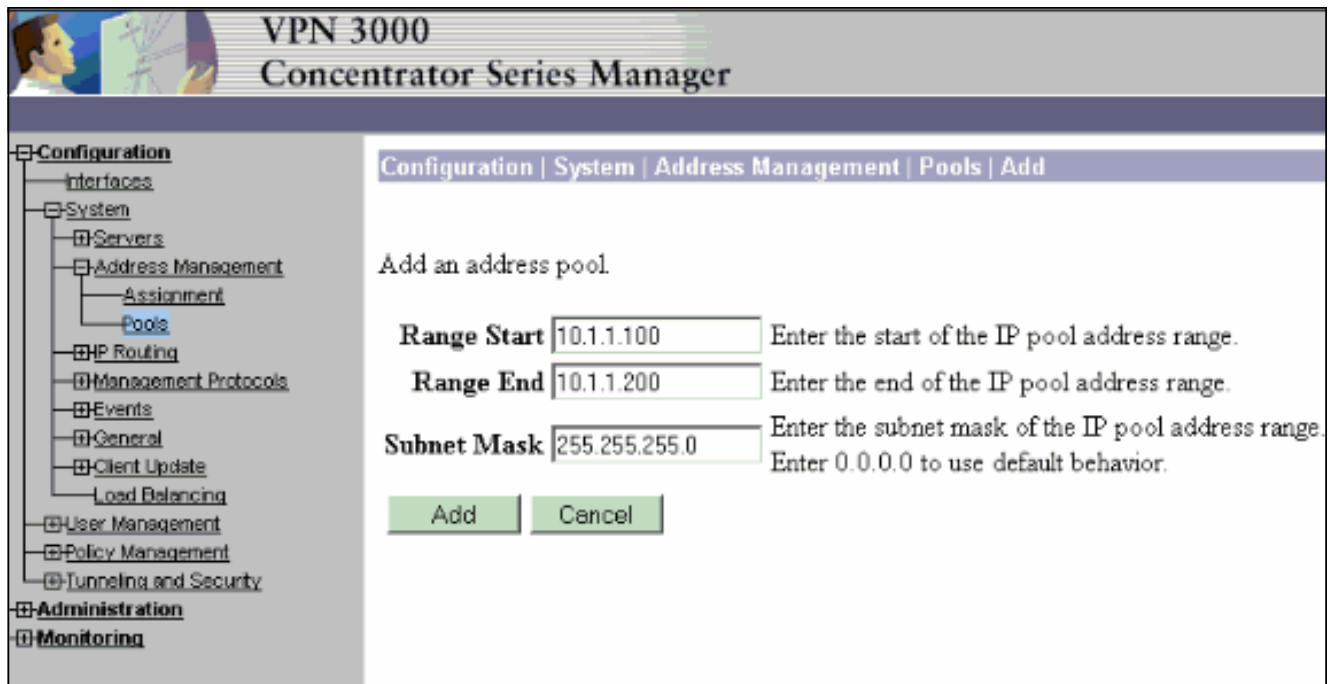


You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

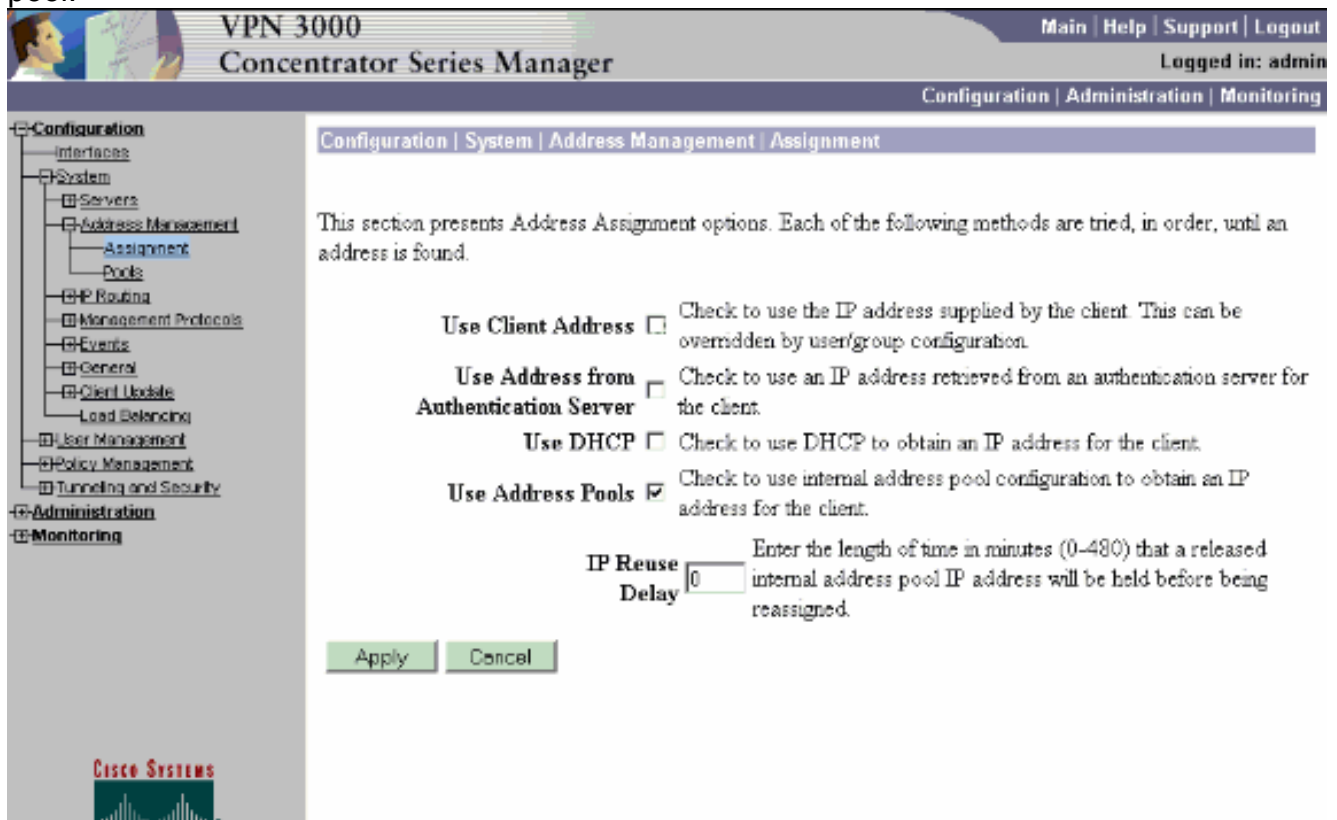
Configuring Ethernet Interface 2 (Public).

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask.
	IP Address	192.168.1.2	Enter the IP Address and Subnet Mask for this interface.
	Subnet Mask	255.255.255.0	
	Public Interface	<input checked="" type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.89.BF.D1	The MAC address for this interface.
	Filter	2. Public (Default)	Select the filter for this interface.
	Speed	10/100 auto	Select the speed for this interface.

- Puntare un browser all'interfaccia interna del concentratore VPN e scegliere Configurazione > Sistema > Gestione indirizzi > Pool di indirizzi > Aggiungi per assegnare un intervallo di indirizzi IP disponibile. Specificare un intervallo di indirizzi IP che non sia in conflitto con altri dispositivi nella rete interna: **Nota:** queste immagini mostrano la gestione dell'interfaccia pubblica esterna perché sono stati aggiunti filtri per consentire questa operazione solo in un'impostazione lab.



4. Scegliere Configurazione > Sistema > Gestione indirizzi > **Assegnazione**, selezionare la casella **Utilizza pool di indirizzi** e fare clic su **Applica** per indicare a VPN Concentrator di utilizzare il pool.



5. Scegliere **Configurazione > Gestione utente > Gruppi > Aggiungi gruppo** per configurare un gruppo IPsec per gli utenti e definire un nome e una password per il gruppo. In questo esempio viene utilizzato group="ipsecgroup" con password/verify="cisco123":

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

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

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	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

CISCO SYSTEMS

6. Nella scheda Generale del gruppo verificare che IPsec sia selezionato.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Add

Secondary DNS	<input type="text"/>	<input checked="" type="checkbox"/>	secondary DNS server.
Primary WINS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec <input checked="" type="checkbox"/> WebVPN	<input checked="" type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

CISCO SYSTEMS

7. Nella scheda IPsec del gruppo verificare che l'autenticazione sia impostata su **Interno**. Scegliere **Configurazione > Gestione utenti > Gruppi > Modifica gruppo** e selezionare **ipsecgroup** dall'opzione Gruppi correnti.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

- Configuration
 - Interfaces
 - System
 - Servers
 - Address Management
 - Assignment
 - Pools
 - IP Routing
 - Management Protocols
 - Events
 - General
 - Client Update
 - Load Balancing
 - User Management
 - Base Group
 - Groups
 - Users
 - Policy Management
 - Tunneling and Security
- Administration
- Monitoring

Confidence Interval: 300

Tunnel Type: Remote Access

Remote Access Parameters

Group Lock:

Authentication: Internal

Authorization Type: None

...a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.

Select the type of tunnel for this group. Update the Remote Access parameters below as needed.

Lock users into this group.

Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.

If members of this group need authorization in addition to authentication, select an authorization method. If you configure

CISCO SYSTEMS

8. Scegliere Configurazione > Gestione utente > Utenti > Aggiungi e aggiungere un utente al gruppo definito in precedenza. Nell'esempio, l'utente è "ipsecuser" con la password "xyz12345" nel gruppo "ipsecgroup":

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

- Configuration
 - Interfaces
 - System
 - User Management
 - Base Group
 - Groups
 - Users
 - Policy Management
 - Tunneling and Security
- Administration
- Monitoring

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPsec | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Username	ipsecuser	Enter a unique username.
Password	XXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXX	Verify the user's password.
Group	ipsecgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add Cancel

CISCO SYSTEMS

[Assegnazione di un indirizzo IP statico a un utente](#)

Per assegnare un indirizzo IP statico per l'utente VPN remoto ogni volta che si connette a VPN 3000 Concentrator, scegliere **Configurazione > Gestione utenti > Utenti > Modifica ipsecuser2 > Identità**. In questa configurazione per l'utente (ipsecuser2), l'indirizzo IP statico 10.2.2.1/24 viene assegnato ogni volta che l'utente si connette.

Configuration | User Management | Users | Modify ipsecuser2

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

Identity Parameters		
Attribute	Value	Description
Username	ipsecuser2	Enter a unique username.
Password	XXXXXXXXXXXXXXXXXXXX	Enter the user's password. The password must satisfy the group password re.
Verify	XXXXXXXXXXXXXXXXXXXX	Verify the user's password.
Group	ipsecgroup	Enter the group to which this user belongs.
IP Address	10.2.2.1	Enter the IP address assigned to this user.
Subnet Mask	255.255.255.0	Enter the subnet mask assigned to this user.

Apply Cancel

Nota: accertarsi di passare a **Configurazione > Sistema > Gestione indirizzi > Assegnazione** per assicurarsi che VPN Concentrator esegua il provisioning dell'indirizzo IP assegnato. Selezionare **Usa indirizzo del server di autenticazione** per assegnare gli indirizzi IP recuperati da un server di autenticazione per singolo utente. L'indirizzo IP e la subnet mask immessi nella scheda Parametri identità nella finestra **Gestione utenti > Utenti > Aggiungi o modifica** vengono considerati come appartenenti al server di autenticazione interno.

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.

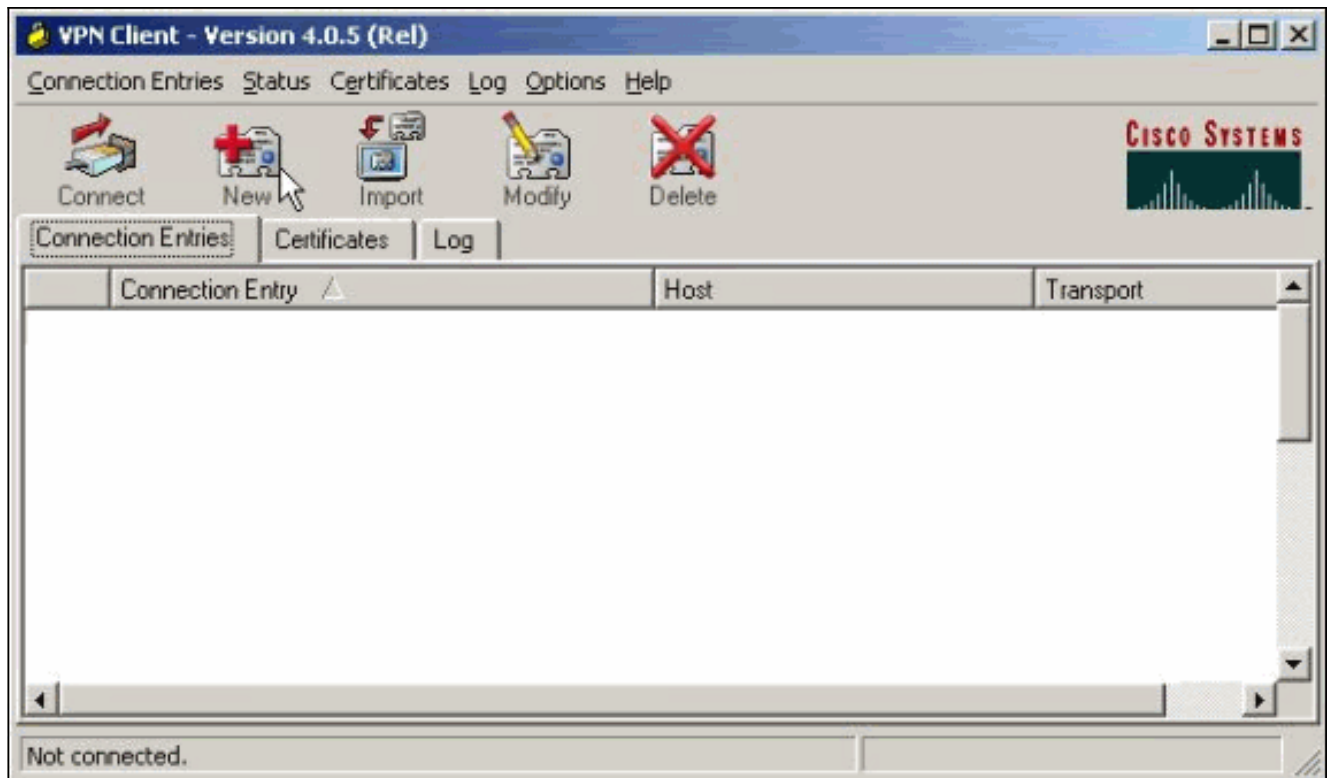
IP Reuse Delay Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply Cancel

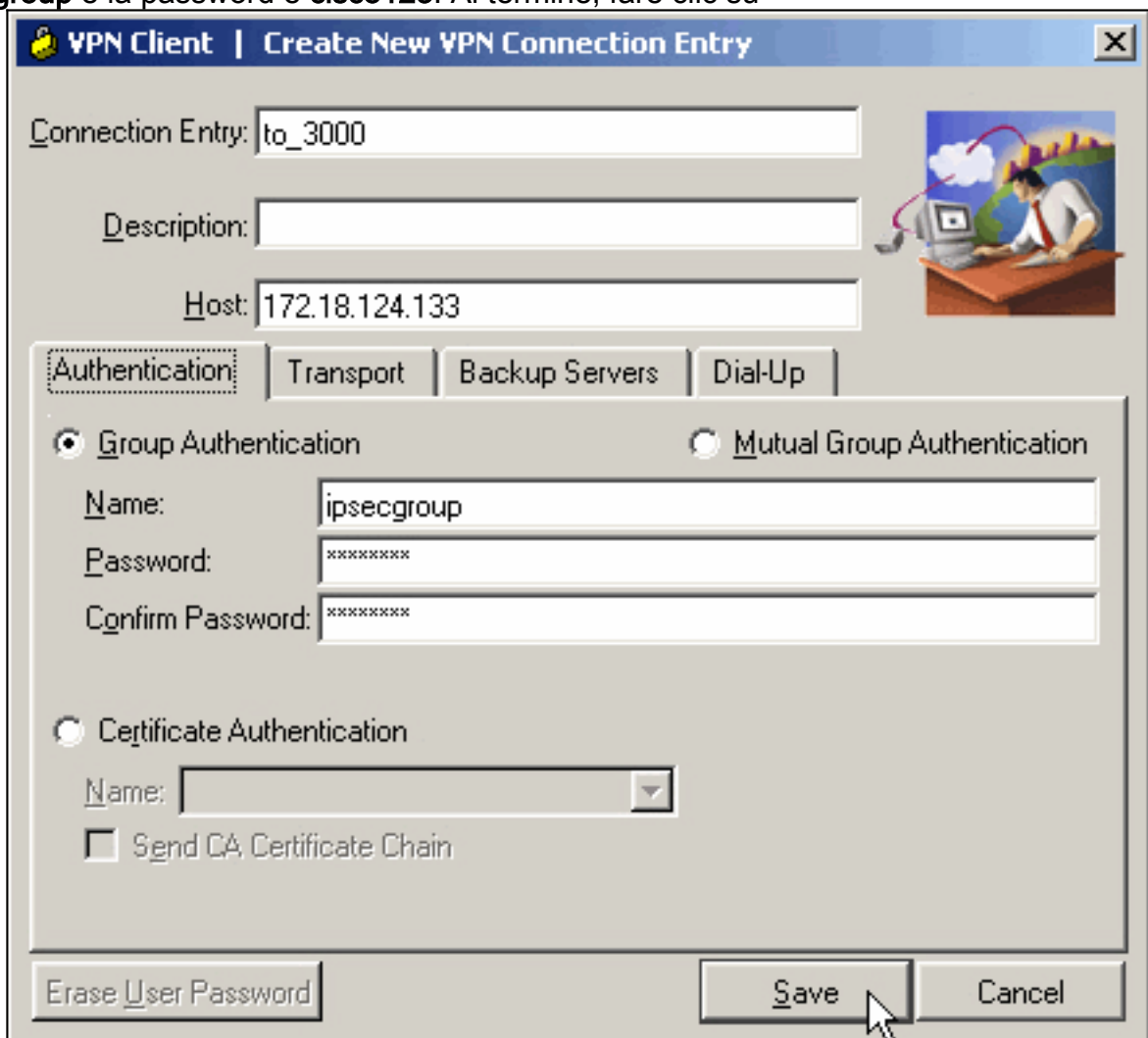
Configurare il client VPN

Completare questa procedura per configurare il client VPN.

1. Per creare una nuova voce di connessione, fare clic su **Nuovo**.



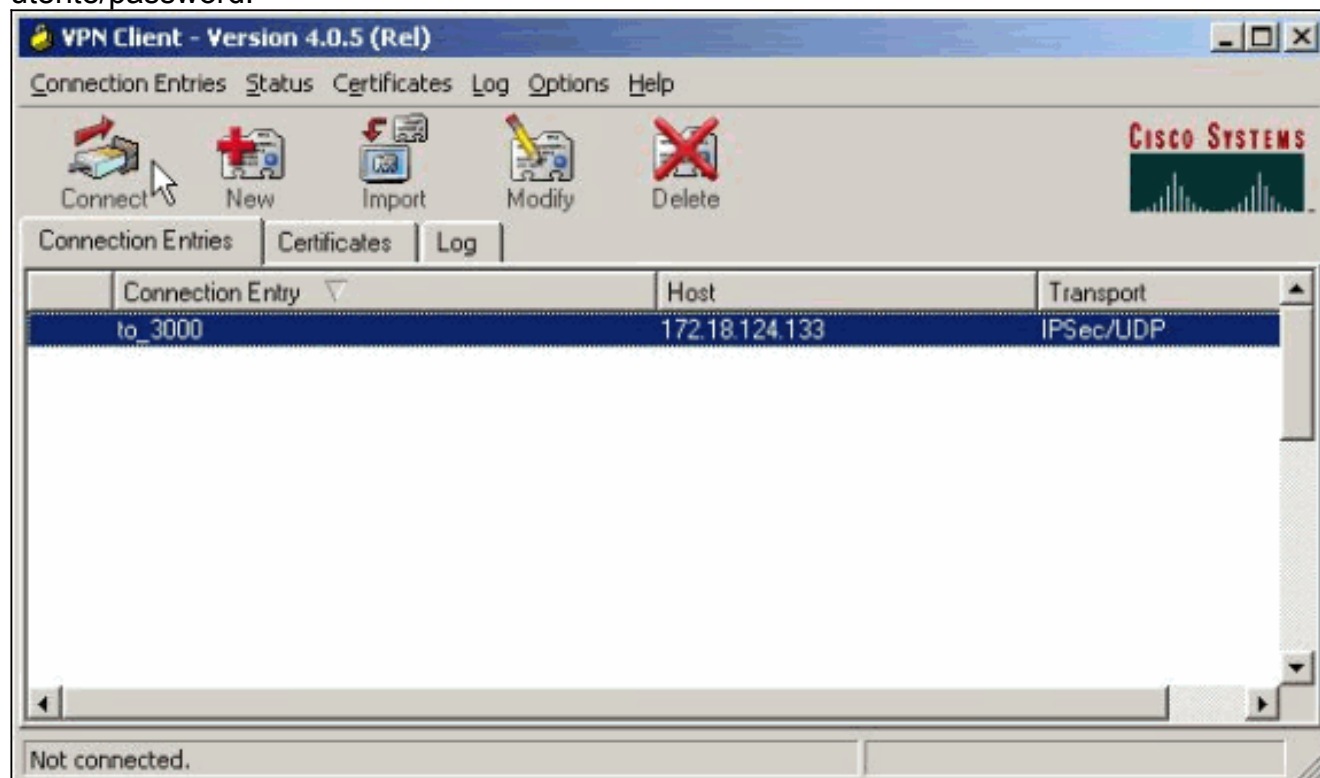
2. Assegnare un nome alla connessione, immettere l'indirizzo IP dell'interfaccia pubblica del concentratore VPN e specificare le credenziali del gruppo. In questo caso, il nome è **ipsegroup** e la password è **cisco123**. Al termine, fare clic su



Salva.

3. Selezionare la voce di connessione dall'elenco e fare clic su **Connetti**. Quando viene richiesto il nome utente/password, immettere il nome

utente/password.



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in queste sezioni permettono di risolvere i problemi relativi alla configurazione.

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

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

Problemi che possono verificarsi

Si tratta di potenziali errori che possono verificarsi. Per le soluzioni a questi errori, vedere le sezioni [VPN Client](#) e [VPN Concentrator](#).

- Un utente riceve il messaggio Impossibile negoziare IPSec oppure l'host non risponde. Il debug di VPN 3000 mostra:

```
14 02/20/2001 08:59:29.100 SEV=4 IKE/22 RPT=5 10.102.55.139  
No Group found matching badgroup for Pre-shared key peer 10.102.55.139
```

Causa normale: L'utente tenta di connettersi con un nome di gruppo non configurato.

- Un utente non può connettersi e il debug di VPN 3000 mostra:

```
Filter missing on interface 2, IKE data from Peer x.x.x.x dropped
```

Causa normale: Filtro mancante nell'interfaccia pubblica. Di solito si tratta del filtro "pubblico"

(ma può essere il filtro privato; "none" non valido). Scegliere **Configurazione > Interfacce > Ethernet 2 > Filtro** e rendere il filtro "pubblico" o un altro valore (ossia, non "nessuno"). Per ulteriori informazioni su come configurare il filtro, vedere la [sezione configurazione](#) di questo documento.

- Un utente non può connettersi e viene visualizzato il messaggio `Impossibile negoziare IPsec` oppure `l'host non risponde`. Il debug di VPN 3000 mostra:

```
Terminating connection attempt: IPSEC not permitted for group >group<
```

Causa normale: IPsec non è selezionato nel gruppo. Scegliere **Configurazione > Gestione utenti > Gruppi > <gruppo> > Modifica > Generale** e verificare che **IPsec** sia selezionato in **Protocolli di tunneling**.

- Un utente non può connettersi dopo numerosi tentativi e vede `Autenticazione utente non riuscita`. Il debug di VPN 3000 mostra:

```
Authentication rejected: Reason = User was not found handle = 14, server = Internal, user = <user>
```

Causa normale: L'utente non esiste nel database utenti. Assicurarsi di immettere il nome utente corretto quando viene visualizzata la finestra di autenticazione utente.

- Gli utenti non possono connettersi e il debug di VPN 3000 mostra:

```
Filter missing on interface 0, IKE data from Peer x.x.x.x dropped
```

Causa normale: Route predefinita mancante. Verificare che nella configurazione sia presente un percorso predefinito. Scegliere **Configurazione > Sistema > Instradamento IP > Gateway predefinito** e specificare il gateway predefinito.

- Un utente non è in grado di connettersi e vede che `la connessione IPsec è stata interrotta dal peer remoto`. Il debug di VPN 3000 mostra:

```
User [ <user> ]  
IKE rcv'd FAILED IP Addr status!
```

Causa normale: Nessuna opzione selezionata per assegnare al client VPN un indirizzo IP. Scegliere **Configurazione > Sistema > Gestione indirizzi > Assegnazione indirizzi** e selezionare un'opzione.

- Un utente non è in grado di connettersi e vede che `l'autenticazione dell'utente non è riuscita`. Il debug di VPN 3000 mostra:

```
The calculated HASH doesn't match the received value
```

Causa normale: La password del gruppo sul client VPN è diversa dalla password configurata sul concentratore VPN. Controllare la password sia sul client VPN che sul concentratore.

- È stato configurato il pool VPN per le risorse associate a VPN Concentrator. È possibile accedere alle risorse ma non è possibile eseguirne il ping. **Causa normale:** C'è un PIX dietro il VPN Concentrator che blocca i pacchetti ICMP. Accedere al PIX e applicare un **elenco degli accessi** per abilitare i pacchetti ICMP.

- Non sono presenti debug di VPN Concentrator e tutti o alcuni utenti non possono connettersi. Il filtro pubblico predefinito di VPN Concentrator contiene le regole per consentire questo traffico: `Protocollo = UDP, porta = 500` `Protocollo = UDP, porta = 10000` `Protocollo = ESP` `Protocollo = AH` Se i filtri di VPN Concentrator consentono questo traffico, è possibile che un dispositivo tra il client VPN e VPN Concentrator blocchi alcune di queste porte (ad esempio un firewall). Per procedere alla verifica, provare a connettersi al concentratore VPN dalla rete immediatamente all'esterno del concentratore VPN. Se il problema persiste, un dispositivo tra il PC client VPN e il concentratore VPN blocca il traffico.

- Un utente non può connettersi e visualizza i seguenti registri:

```
07/10/2006 11:48:59.280 SEV=4 IKE/0 RPT=141 10.86.190.92
```

```
Group [NYMVPN]
```

```
received an unencrypted packet when crypto active!! Dropping packet
```

Causa normale: Nome di gruppo o password non definiti correttamente. Ricreare il nuovo

- nome e la nuova password del gruppo sul concentratore VPN 3000 per il client VPN.
- Un utente può eseguire il ping o la connessione Telnet a un host dietro il concentratore VPN, ma non può utilizzare Remote Desktop (9RDP) o applicazioni simili. **Causa comune:** il filtro Public non è abilitato sull'interfaccia Public. Vedere il passaggio 2 nella sezione [Configurazione di VPN 3000 Concentrator](#) in questo documento.
 - Un utente può connettersi, ma il traffico non viene passato attraverso il tunnel VPN. **Causa normale:** NAT-Transparency non abilitato. In molti casi il client VPN è dietro un dispositivo PAT. PAT si basa sui numeri di porta TCP e UDP per preservare lo spazio degli indirizzi. Tuttavia, ESP, che incapsula il traffico VPN, è un protocollo separato da TCP o UDP. Ciò significa che molti dispositivi PAT non sono in grado di gestire il traffico ESP. NAT-T incapsula i pacchetti ESP in pacchetti UDP consentendo loro di passare facilmente attraverso un dispositivo PAT. Pertanto, per consentire il flusso del traffico ESP attraverso un dispositivo PAT, è necessario abilitare NAT-T sul concentratore. per ulteriori informazioni, fare riferimento a [Configurazione della modalità trasparente NAT per IPSec sul concentratore VPN 3000](#).

[Client VPN](#)

Per visualizzare il visualizzatore dei log, scegliere **Start > Programmi > Cisco Systems VPN 3000 Client > Log Viewer**.

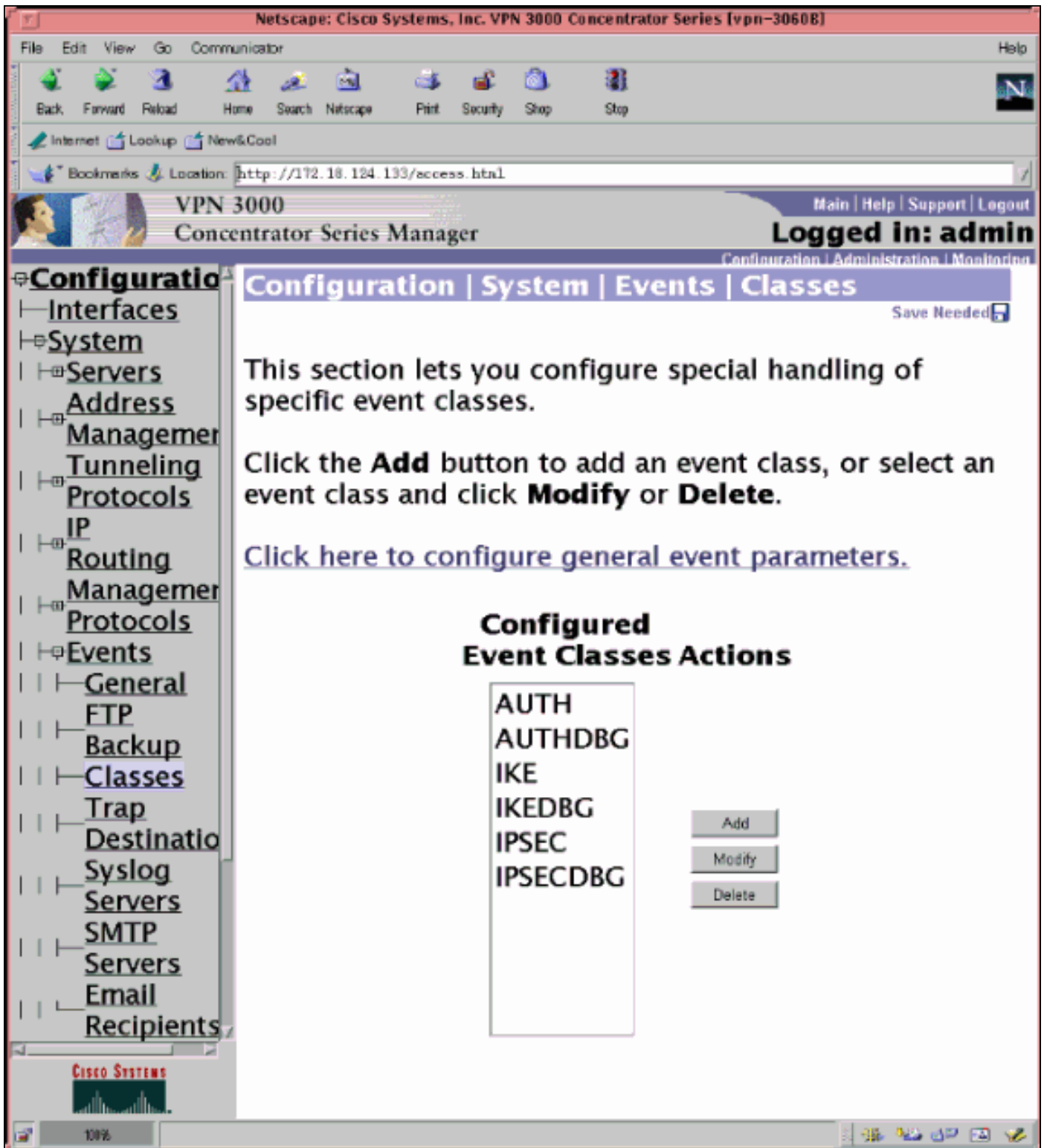
[VPN Concentrator](#)

Scegliere **Configurazione > Sistema > Eventi > Classi** per attivare questo debug in caso di errori di connessione degli eventi:

- AUTH - Gravità del log 1-13
- AUTHDBG - Gravità da registrare 1-13
- IKE - Gravità da registrare 1-13
- IKEDBG - Gravità da registrare 1-13
- IPSEC - Gravità da registrare 1-13
- IPSECDBG - Gravità da registrare 1-13

Nota: se necessario, è possibile aggiungere AUTHDECODE, IKEDECODE, IPSECDECODE in un secondo momento.

Per ulteriori informazioni sulla risoluzione dei problemi, fare riferimento a [Risoluzione dei problemi di connessione su VPN 3000 Concentrator](#).



Scegliere Monitoraggio > Registro eventi filtrabile per visualizzare il registro.

[VPN 3000 Concentrator - Buono debug di esempio](#)

```
1 02/07/2002 08:00:13.320 SEV=8 IKEDBG/0 RPT=69 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) ... total length : 562
```

```
4 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=70 172.18.124.241
processing SA payload
```


5 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=71 172.18.124.241
processing ke payload

6 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=72 172.18.124.241
processing ISA_KE

7 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=7 172.18.124.241
processing nonce payload

8 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=8 172.18.124.241
Processing ID

9 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=4 172.18.124.241
processing VID payload

10 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=4 172.18.124.241
Received xauth V6 VID

11 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=5 172.18.124.241
processing VID payload

12 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=5 172.18.124.241
Received DPD VID

13 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=6 172.18.124.241
processing VID payload

14 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=6 172.18.124.241
Received Cisco Unity client VID

15 02/07/2002 08:00:13.320 SEV=9 IKEDBG/23 RPT=2 172.18.124.241
Starting group lookup for peer 172.18.124.241

16 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/1 RPT=2
AUTH_Open() returns 136

17 02/07/2002 08:00:13.320 SEV=7 AUTH/12 RPT=2
Authentication session opened: handle = 136

18 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/3 RPT=2
AUTH_PutAttrTable(136, 728a84)

19 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/6 RPT=2
AUTH_GroupAuthenticate(136, 9b143bc, 482fb0)

20 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/59 RPT=2
AUTH_BindServer(9a08630, 0, 0)

21 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/69 RPT=2
Auth Server 16b3fa0 has been bound to ACB 9a08630, sessions = 1

22 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/65 RPT=2
AUTH_CreateTimer(9a08630, 0, 0)

23 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/72 RPT=2
Reply timer created: handle = 3B2001B

24 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/61 RPT=2
AUTH_BuildMsg(9a08630, 0, 0)

25 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/64 RPT=2
AUTH_StartTimer(9a08630, 0, 0)

26 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/73 RPT=2

Reply timer started: handle = 3B2001B, timestamp = 10085308, timeout = 30000

27 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/62 RPT=2
AUTH_SndRequest(9a08630, 0, 0)

28 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/50 RPT=3
IntDB_Decode(62b6d00, 115)

29 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=3
IntDB_Xmt(9a08630)

30 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/71 RPT=2
xmit_cnt = 1

31 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=4
IntDB_Xmt(9a08630)

32 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/49 RPT=2
IntDB_Match(9a08630, 2ebe71c)

33 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/63 RPT=2
AUTH_RcvReply(9a08630, 0, 0)

34 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/50 RPT=4
IntDB_Decode(2ebe71c, 44)

35 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/48 RPT=2
IntDB_Rcv(9a08630)

36 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/66 RPT=2
AUTH_DeleteTimer(9a08630, 0, 0)

37 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/74 RPT=2
Reply timer stopped: handle = 3B2001B, timestamp = 10085318

38 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/58 RPT=2
AUTH_Callback(9a08630, 0, 0)

39 02/07/2002 08:00:13.420 SEV=6 AUTH/41 RPT=2 172.18.124.241
Authentication successful: handle = 136, server = Internal, group = ipsecgroup

40 02/07/2002 08:00:13.420 SEV=7 IKEDBG/0 RPT=73 172.18.124.241
Group [ipsecgroup]
Found Phase 1 Group (ipsecgroup)

41 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/4 RPT=2
AUTH_GetAttrTable(136, 728c4c)

42 02/07/2002 08:00:13.420 SEV=7 IKEDBG/14 RPT=2 172.18.124.241
Group [ipsecgroup]
Authentication configured for Internal

43 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/2 RPT=2
AUTH_Close(136)

44 02/07/2002 08:00:13.420 SEV=9 IKEDBG/0 RPT=74 172.18.124.241
Group [ipsecgroup]
processing IKE SA

45 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=75 172.18.124.241
Group [ipsecgroup]
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:

Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

53 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=76 172.18.124.241
Group [ipsecgroup]
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

53 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=77 172.18.124.241
Group [ipsecgroup]
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

57 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=78 172.18.124.241
Group [ipsecgroup]
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

61 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=79 172.18.124.241
Group [ipsecgroup]
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 7

65 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=80 172.18.124.241
Group [ipsecgroup]
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

68 02/07/2002 08:00:13.420 SEV=7 IKEDBG/28 RPT=2 172.18.124.241
Group [ipsecgroup]
IKE SA Proposal # 1, Transform # 2 acceptable
Matches global IKE entry # 1

70 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/60 RPT=2
AUTH_UnbindServer(9a08630, 0, 0)

71 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/70 RPT=2
Auth Server 16b3fa0 has been unbound from ACB 9a08630, sessions = 0

72 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/10 RPT=2
AUTH_Int_FreeAuthCB(9a08630)

73 02/07/2002 08:00:13.420 SEV=7 AUTH/13 RPT=2
Authentication session closed: handle = 136

74 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=81 172.18.124.241

Group [ipsecgroup]
constructing ISA_SA for isakmp

75 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=82 172.18.124.241
Group [ipsecgroup]
constructing ke payload

76 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=9 172.18.124.241
Group [ipsecgroup]
constructing nonce payload

77 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=83 172.18.124.241
Group [ipsecgroup]
Generating keys for Responder...

78 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=10 172.18.124.241
Group [ipsecgroup]
constructing ID

79 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=84
Group [ipsecgroup]
construct hash payload

80 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=85 172.18.124.241
Group [ipsecgroup]
computing hash

81 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=5 172.18.124.241
Group [ipsecgroup]
constructing Cisco Unity VID payload

82 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=6 172.18.124.241
Group [ipsecgroup]
constructing xauth V6 VID payload

83 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=7 172.18.124.241
Group [ipsecgroup]
constructing dpd vid payload

84 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=8 172.18.124.241
Group [ipsecgroup]
constructing VID payload

85 02/07/2002 08:00:13.450 SEV=9 IKEDBG/48 RPT=2 172.18.124.241
Group [ipsecgroup]
Send Altiga GW VID

86 02/07/2002 08:00:13.450 SEV=8 IKEDBG/0 RPT=86 172.18.124.241
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 344

89 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=87 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 76

91 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=88 172.18.124.241
Group [ipsecgroup]
processing hash

92 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=89 172.18.124.241
Group [ipsecgroup]
computing hash

93 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=90 172.18.124.241
Group [ipsecgroup]
Processing Notify payload

94 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=91 172.18.124.241
Group [ipsecgroup]

constructing blank hash

95 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=92 172.18.124.241
Group [lipsecgroup]
constructing qm hash

96 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=93 172.18.124.241
SENDING Message (msgid=ec88ba81) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 100

98 02/07/2002 08:00:21.810 SEV=8 IKEDBG/0 RPT=94 172.18.124.241
RECEIVED Message (msgid=ec88ba81) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

100 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=11
process_attr(): Enter!

101 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=12
Processing MODE_CFG Reply attributes.

102 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/1 RPT=3
AUTH_Open() returns 137

103 02/07/2002 08:00:21.810 SEV=7 AUTH/12 RPT=3
Authentication session opened: handle = 137

104 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/3 RPT=3
AUTH_PutAttrTable(137, 728a84)

105 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/5 RPT=1
AUTH_Authenticate(137, 50093bc, 4b5708)

106 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/59 RPT=3
AUTH_BindServer(9b1544c, 0, 0)

107 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/69 RPT=3
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

108 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/65 RPT=3
AUTH_CreateTimer(9b1544c, 0, 0)

109 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/72 RPT=3
Reply timer created: handle = 3B4001A

110 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/61 RPT=3
AUTH_BuildMsg(9b1544c, 0, 0)

111 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/64 RPT=3
AUTH_StartTimer(9b1544c, 0, 0)

112 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/73 RPT=3
Reply timer started: handle = 3B4001A, timestamp = 10086157, timeout = 30000

113 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/62 RPT=3
AUTH_SndRequest(9b1544c, 0, 0)

114 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/50 RPT=5
IntDB_Decode(62b6d00, 102)

115 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=5
IntDB_Xmt(9b1544c)

116 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/71 RPT=3
xmit_cnt = 1

117 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=6
IntDB_Xmt(9b1544c)

118 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/49 RPT=3
IntDB_Match(9b1544c, 2ebe71c)

119 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/63 RPT=3
AUTH_RcvReply(9b1544c, 0, 0)

120 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=6
IntDB_Decode(2ebe71c, 62)

121 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/48 RPT=3
IntDB_Rcv(9b1544c)

122 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/66 RPT=3
AUTH_DeleteTimer(9b1544c, 0, 0)

123 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/74 RPT=3
Reply timer stopped: handle = 3B4001A, timestamp = 10086167

124 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/58 RPT=3
AUTH_Callback(9b1544c, 0, 0)

125 02/07/2002 08:00:21.910 SEV=6 AUTH/4 RPT=1 172.18.124.241
Authentication successful: handle = 137, server = Internal, user = ipsecuser

126 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/3 RPT=4
AUTH_PutAttrTable(137, 1861c60)

127 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/60 RPT=3
AUTH_UnbindServer(9b1544c, 0, 0)

128 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/70 RPT=3
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

129 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/59 RPT=4
AUTH_BindServer(9b1544c, 0, 0)

130 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/69 RPT=4
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

131 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/65 RPT=4
AUTH_CreateTimer(9b1544c, 0, 0)

132 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/72 RPT=4
Reply timer created: handle = 3B5001A

133 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/61 RPT=4
AUTH_BuildMsg(9b1544c, 0, 0)

134 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/64 RPT=4
AUTH_StartTimer(9b1544c, 0, 0)

135 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/73 RPT=4
Reply timer started: handle = 3B5001A, timestamp = 10086167, timeout = 30000

136 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/62 RPT=4
AUTH_SndRequest(9b1544c, 0, 0)

137 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=7
IntDB_Decode(2ec5350, 44)

138 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=7
IntDB_Xmt(9b1544c)

139 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/71 RPT=4
xmit_cnt = 1

140 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=8
IntDB_Xmt(9b1544c)

141 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/49 RPT=4
IntDB_Match(9b1544c, 2ec3f64)

142 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/63 RPT=4
AUTH_RcvReply(9b1544c, 0, 0)

143 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=8
IntDB_Decode(2ec3f64, 44)

144 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/48 RPT=4
IntDB_Rcv(9b1544c)

145 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/66 RPT=4
AUTH_DeleteTimer(9b1544c, 0, 0)

146 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/74 RPT=4
Reply timer stopped: handle = 3B5001A, timestamp = 10086177

147 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/58 RPT=4
AUTH_Callback(9b1544c, 0, 0)

148 02/07/2002 08:00:22.010 SEV=6 AUTH/41 RPT=3 172.18.124.241
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

149 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/3 RPT=5
AUTH_PutAttrTable(137, 1861c60)

150 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/60 RPT=4
AUTH_UnbindServer(9b1544c, 0, 0)

151 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/70 RPT=4
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

152 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/59 RPT=5
AUTH_BindServer(9b1544c, 0, 0)

153 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/69 RPT=5
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

154 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/65 RPT=5
AUTH_CreateTimer(9b1544c, 0, 0)

155 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/72 RPT=5
Reply timer created: handle = 3B6001A

156 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/61 RPT=5
AUTH_BuildMsg(9b1544c, 0, 0)

157 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/64 RPT=5
AUTH_StartTimer(9b1544c, 0, 0)

158 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/73 RPT=5
Reply timer started: handle = 3B6001A, timestamp = 10086177, timeout = 30000

159 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/62 RPT=5
AUTH_SndRequest(9b1544c, 0, 0)

160 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=9
IntDB_Decode(2ec39ec, 44)

161 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=9
IntDB_Xmt(9b1544c)

162 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/71 RPT=5
xmit_cnt = 1

163 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=10
IntDB_Xmt(9b1544c)

164 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/49 RPT=5
IntDB_Match(9b1544c, 2ec5350)

165 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/63 RPT=5
AUTH_RcvReply(9b1544c, 0, 0)

166 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/50 RPT=10
IntDB_Decode(2ec5350, 44)

167 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/48 RPT=5
IntDB_Rcv(9b1544c)

168 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/66 RPT=5
AUTH_DeleteTimer(9b1544c, 0, 0)

169 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/74 RPT=5
Reply timer stopped: handle = 3B6001A, timestamp = 10086187

170 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/58 RPT=5
AUTH_Callback(9b1544c, 0, 0)

171 02/07/2002 08:00:22.110 SEV=6 AUTH/41 RPT=4 172.18.124.241
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

172 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=3
AUTH_GetAttrTable(137, 729c04)

173 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=4
AUTH_GetAttrTable(137, 728c4c)

174 02/07/2002 08:00:22.110 SEV=7 IKEDBG/14 RPT=3 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Authentication configured for Internal

175 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/2 RPT=3
AUTH_Close(137)

176 02/07/2002 08:00:22.110 SEV=4 IKE/52 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
User (ipsecuser) authenticated.

177 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=95 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

178 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=96 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

179 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=97 172.18.124.241
SENDING Message (msgid=4cc78f4e) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 60

181 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/60 RPT=5
AUTH_UnbindServer(9b1544c, 0, 0)

182 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/70 RPT=5
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

183 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/10 RPT=3
AUTH_Int_FreeAuthCB(9b1544c)

184 02/07/2002 08:00:22.110 SEV=7 AUTH/13 RPT=3
Authentication session closed: handle = 137

185 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=98 172.18.124.241
RECEIVED Message (msgid=4cc78f4e) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

187 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=13
process_attr(): Enter!

188 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=14
Processing cfg ACK attributes

189 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=99 172.18.124.241
RECEIVED Message (msgid=38a7c320) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 154

191 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=15
process_attr(): Enter!

192 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=16
Processing cfg Request attributes

193 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=1
MODE_CFG: Received request for IPV4 address!

194 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=2
MODE_CFG: Received request for IPV4 net mask!

195 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=3
MODE_CFG: Received request for DNS server address!

196 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=4
MODE_CFG: Received request for WINS server address!

197 02/07/2002 08:00:22.180 SEV=6 IKE/130 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received unsupported transaction mode attribute: 5

199 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=5
MODE_CFG: Received request for Application Version!

200 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=6
MODE_CFG: Received request for Banner!

201 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=7
MODE_CFG: Received request for Save PW setting!

202 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=8
MODE_CFG: Received request for Default Domain Name!

203 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=9
MODE_CFG: Received request for Split Tunnel List!

204 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=10
MODE_CFG: Received request for PFS setting!

205 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=11
MODE_CFG: Received request for FWTYPE!

206 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=12
MODE_CFG: Received request for UDP Port!

207 02/07/2002 08:00:22.180 SEV=9 IKEDBG/31 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Obtained IP addr (10.1.1.100) prior to initiating Mode Cfg (XAuth enabled)

209 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=100 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

210 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=101 172.18.124.241
0000: 00010004 0A010164 F0010000 F0070000d.....
0010: 00070062 43697363 6F205379 7374656D ...bCisco System
0020: 732C2049 6E632E2F 56504E20 33303030 s, Inc./VPN 3000
0030: 20436F6E 63656E74 7261746F 72205665 Concentrator Ve
0040: 7273696F 6E20332E 352E5265 6C206275 rsion 3.5.Rel bu
0050: 696C7420 62792076 6D757270 6879206F ilt by vmurphy o

216 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=102 172.18.124.241
0000: 6E204E6F 76203237 20323030 31203131 n Nov 27 2001 11
0010: 3A32323A 3331 :22:31

218 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=103 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

219 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=104 172.18.124.241
SENDING Message (msgid=38a7c320) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 174

221 02/07/2002 08:00:22.190 SEV=9 IKEDBG/21 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

223 02/07/2002 08:00:22.190 SEV=4 AUTH/22 RPT=86
User ipsecuser connected

224 02/07/2002 08:00:22.190 SEV=7 IKEDBG/22 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

226 02/07/2002 08:00:22.200 SEV=4 IKE/119 RPT=68 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 1 COMPLETED

227 02/07/2002 08:00:22.200 SEV=6 IKE/121 RPT=1 172.18.124.241
Keep-alive type for this connection: DPD

228 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=105 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Starting phase 1 rekey timer: 82080000 (ms)

229 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=106 172.18.124.241
Group [ipsecgroup] User [ipsecuser]

sending notify message

230 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=107 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

231 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=108 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

232 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=109 172.18.124.241
SENDING Message (msgid=be237358) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 88

234 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=110 172.18.124.241
RECEIVED Message (msgid=472c326b) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 792

237 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=111 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

238 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=112 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing SA payload

239 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=17 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing nonce payload

240 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=18 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

241 02/07/2002 08:00:22.200 SEV=5 IKE/25 RPT=62 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received remote Proxy Host data in ID Payload:
Address 10.1.1.100, Protocol 0, Port 0

244 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=19 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

245 02/07/2002 08:00:22.200 SEV=5 IKE/24 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received local Proxy Host data in ID Payload:
Address 172.18.124.133, Protocol 0, Port 0

248 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=113
QM IsRekeyed old sa not found by addr

249 02/07/2002 08:00:22.200 SEV=5 IKE/66 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

251 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=114 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing IPSEC SA

252 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=115
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
Phase 2 failure:

Mismatched attr types for class HMAC Algorithm:

Rcv'd: SHA

Cfg'd: MD5

256 02/07/2002 08:00:22.200 SEV=7 IKEDBG/27 RPT=1 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

IPSec SA Proposal # 3, Transform # 1 acceptable

258 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=116 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

IKE: requesting SPI!

259 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/6 RPT=1

IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 129, err 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, dsId 300

263 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/1 RPT=1

Processing KEY_GETSPI msg!

264 02/07/2002 08:00:22.200 SEV=7 IPSECDBG/13 RPT=1

Reserved SPI 1037485220

265 02/07/2002 08:00:22.200 SEV=8 IKEDBG/6 RPT=1

IKE got SPI from key engine: SPI = 0x3dd6c4a4

266 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=117 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

oakley constructing quick mode

267 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=118 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

constructing blank hash

268 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=119 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

constructing ISA_SA for ipsec

269 02/07/2002 08:00:22.200 SEV=5 IKE/75 RPT=121 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

271 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=20 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

constructing ipsec nonce payload

272 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=21 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

constructing proxy ID

273 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=120 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

Transmitting Proxy Id:

Remote host: 10.1.1.100 Protocol 0 Port 0

Local host: 172.18.124.133 Protocol 0 Port 0

277 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=121 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

Sending RESPONDER LIFETIME notification to Initiator

279 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=122 172.18.124.241

Group [ipsecgroup] User [ipsecuser]

constructing qm hash

280 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=123 172.18.124.241
SENDING Message (msgid=472c326b) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 172

283 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=124 172.18.124.241
RECEIVED Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 796

286 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=125 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

287 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=126 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing SA payload

288 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=22 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing nonce payload

289 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=23 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

290 02/07/2002 08:00:22.210 SEV=5 IKE/25 RPT=63 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received remote Proxy Host data in ID Payload:
Address 10.1.1.100, Protocol 0, Port 0

293 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=24 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

294 02/07/2002 08:00:22.210 SEV=5 IKE/34 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received local IP Proxy Subnet data in ID Payload:
Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

297 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=127
QM IsRekeyed old sa not found by addr

298 02/07/2002 08:00:22.210 SEV=5 IKE/66 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

300 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=128 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing IPSEC SA

301 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=129
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
Phase 2 failure:
Mismatched attr types for class HMAC Algorithm:
Rcv'd: SHA
Cfg'd: MD5

305 02/07/2002 08:00:22.210 SEV=7 IKEDBG/27 RPT=2 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IPSec SA Proposal # 3, Transform # 1 acceptable

307 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE: requesting SPI!

308 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 130, err
0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 300

312 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_GETSPI msg!

313 02/07/2002 08:00:22.210 SEV=7 IPSECDBG/13 RPT=2
Reserved SPI 1517437317

314 02/07/2002 08:00:22.210 SEV=8 IKEDBG/6 RPT=2
IKE got SPI from key engine: SPI = 0x5a724185

315 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=131 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
oakley constructing quick mode

316 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=132 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

317 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=133 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ISA_SA for ipsec

318 02/07/2002 08:00:22.210 SEV=5 IKE/75 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

320 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=25 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ipsec nonce payload

321 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=26 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing proxy ID

322 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=134 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Transmitting Proxy Id:
Remote host: 10.1.1.100 Protocol 0 Port 0
Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0

326 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=135 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Sending RESPONDER LIFETIME notification to Initiator

328 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=136 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

329 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=137 172.18.124.241
SENDING Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 176

332 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=138 172.18.124.241
RECEIVED Message (msgid=472c326b) with payloads :

HDR + HASH (8) + NONE (0) ... total length : 48

334 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=139 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

335 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=140 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
loading all IPSEC SAs

336 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=27 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

337 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=28 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

338 02/07/2002 08:00:22.220 SEV=7 IKEDBG/0 RPT=141 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Loading host:
 Dst: 172.18.124.133
 Src: 10.1.1.100

340 02/07/2002 08:00:22.220 SEV=4 IKE/49 RPT=129 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Security negotiation complete for User (ipsecuser)
Responder, Inbound SPI = 0x3dd6c4a4, Outbound SPI = 0x8104887e

343 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 8104887e, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

347 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=3
Processing KEY_ADD msg!

348 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=4
key_msghdr2secassoc(): Enter

349 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=5
No USER filter configured

350 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=6
KeyProcessAdd: Enter

351 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: Adding outbound SA

352 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: src 172.18.124.133 mask 0.0.0.0, dst 10.1.1.100 mask 0.0.0.0

353 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=9
KeyProcessAdd: FilterIpsecAddIkeSa success

354 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=4
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 3dd6c4a4, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

358 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=10
Processing KEY_UPDATE msg!

359 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=11
Update inbound SA addresses

360 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=12
key_msghdr2secassoc(): Enter

361 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=13
No USER filter configured

362 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=14
KeyProcessUpdate: Enter

363 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=15
KeyProcessUpdate: success

364 02/07/2002 08:00:22.220 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD msg for SA: SPI = 0x8104887e

365 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=142
pitcher: rcv KEY_UPDATE, spi 0x3dd6c4a4

366 02/07/2002 08:00:22.220 SEV=4 IKE/120 RPT=129 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=472c326b)

367 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=143 172.18.124.241
RECEIVED Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

369 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=144 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

370 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=145 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
loading all IPSEC SAs

371 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=29 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

372 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=30 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

373 02/07/2002 08:00:22.280 SEV=7 IKEDBG/0 RPT=146 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Loading subnet:
Dst: 0.0.0.0 mask: 0.0.0.0
Src: 10.1.1.100

375 02/07/2002 08:00:22.280 SEV=4 IKE/49 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Security negotiation complete for User (ipsecuser)
Responder, Inbound SPI = 0x5a724185, Outbound SPI = 0x285e6ed0

378 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=5
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 285e6ed0, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

382 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=16

Processing KEY_ADD msg!

383 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=17
key_msghdr2secassoc(): Enter

384 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=18
No USER filter configured

385 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=19
KeyProcessAdd: Enter

386 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=20
KeyProcessAdd: Adding outbound SA

387 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=21
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 10.1.1.100 mask 0.0.0.0

388 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=22
KeyProcessAdd: FilterIpsecAddIkeSa success

389 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=6
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 5a724185, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

393 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=23
Processing KEY_UPDATE msg!

394 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=24
Update inbound SA addresses

395 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=25
key_msghdr2secassoc(): Enter

396 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=26
No USER filter configured

397 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=27
KeyProcessUpdate: Enter

398 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=28
KeyProcessUpdate: success

399 02/07/2002 08:00:22.280 SEV=8 IKEDBG/7 RPT=2
IKE got a KEY_ADD msg for SA: SPI = 0x285e6ed0

400 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=147
pitcher: rcv KEY_UPDATE, spi 0x5a724185

401 02/07/2002 08:00:22.280 SEV=4 IKE/120 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=64c59a32)

[Informazioni correlate](#)

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Cisco VPN serie 3000 Client Support Page](#)
- [Negoziatore IPSec/protocolli IKE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)