

L2TP over IPsec tra Windows 2000/XP PC e PIX/ASA 7.2 utilizzando un esempio di configurazione a chiave già condivisa

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione client Windows L2TP/IPsec](#)

[Server L2TP in configurazione PIX](#)

[L2TP con configurazione ASDM](#)

[Microsoft Windows 2003 Server con configurazione IAS](#)

[Autenticazione estesa per L2TP su IPsec tramite Active Directory](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Output di esempio del comando debug](#)

[Risoluzione dei problemi con ASDM](#)

[Problema: Disconnessioni frequenti](#)

[Risoluzione dei problemi di Windows Vista](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare L2TP (Layer 2 Tunneling Protocol) su IP Security (IPsec) da client Microsoft Windows 2000/2003 e XP remoti a una sede aziendale di PIX Security Appliance utilizzando chiavi già condivise con Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server per l'autenticazione degli utenti. Per ulteriori informazioni, fare riferimento al documento [Microsoft - Elenco di controllo: Configurazione di IAS per accesso remoto e VPN](#) per ulteriori informazioni su IAS.

Il vantaggio principale della configurazione di L2TP con IPsec in uno scenario di accesso remoto è che gli utenti remoti possono accedere a una VPN su una rete IP pubblica senza un gateway o

una linea dedicata. Ciò consente l'accesso remoto praticamente da qualsiasi luogo con POTS. Un ulteriore vantaggio è che l'unico requisito del client per l'accesso VPN è l'utilizzo di Windows 2000 con Microsoft Dial-Up Networking (DUN). Non è necessario alcun software client aggiuntivo, ad esempio il software Cisco VPN Client.

In questo documento viene descritto anche come usare Cisco Adaptive Security Device Manager (ASDM) per configurare le appliance di sicurezza PIX serie 500 per L2TP su IPsec.

Nota: [Il protocollo L2TP \(Layer 2 Tunneling Protocol\) su IPsec](#) è supportato sul software Cisco Secure PIX Firewall versione 6.x e successive.

Per configurare L2TP over IPsec tra PIX 6.x e Windows 2000, fare riferimento alla [configurazione di L2TP over IPsec tra PIX Firewall e Windows 2000 PC con certificati](#).

Per configurare L2TP su IPsec dai client remoti Microsoft Windows 2000 e XP a un sito aziendale utilizzando un metodo crittografato, fare riferimento alla [configurazione di L2TP su IPsec da un client Windows 2000 o XP a un concentratore Cisco VPN serie 3000 utilizzando chiavi già condivise](#).

Prerequisiti

Requisiti

Prima di stabilire il tunnel sicuro, è necessario che esista una connettività IP tra i peer.

Verificare che la porta UDP 1701 non sia bloccata in alcun punto del percorso della connessione.

Usare solo il gruppo di tunnel predefinito e i criteri di gruppo predefiniti su Cisco PIX/ASA. I criteri e i gruppi definiti dall'utente non funzionano.

Nota: l'appliance di sicurezza non stabilisce un tunnel L2TP/IPsec con Windows 2000 se è installato Cisco VPN Client 3.x o Cisco VPN 3000 Client 2.5. Disabilitare il servizio VPN Cisco per Cisco VPN Client 3.x o il servizio WANetIKE per Cisco VPN 3000 Client 2.5 dal pannello Servizi di Windows 2000. A tale scopo, scegliere **Start > Programmi > Strumenti di amministrazione > Servizi**, riavviare il servizio Agente criteri IPsec dal pannello Servizi e riavviare il computer.

Componenti usati

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

- PIX Security Appliance 515E con software versione 7.2(1) o successive
- Adaptive Security Device Manager 5.2(1) o versioni successive
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional con SP2
- Windows 2003 Server con IAS

Nota: se si aggiorna PIX 6.3 alla versione 7.x, assicurarsi di aver installato SP2 in Windows XP (client L2TP).

Nota: le informazioni riportate nel documento sono valide anche per le appliance di sicurezza

ASA.

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche con Cisco ASA serie 5500 Security Appliance 7.2(1) o versioni successive.

Convenzioni

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

Premesse

Completare questa procedura per configurare L2TP su IPsec.

1. Configurare la modalità di trasporto IPsec per abilitare IPsec con L2TP. Il client L2TP/IPsec di Windows 2000 utilizza la modalità di trasporto IPsec. Viene crittografato solo il payload IP e le intestazioni IP originali rimangono invariate. Il vantaggio di questa modalità è che aggiunge solo pochi byte a ciascun pacchetto e consente ai dispositivi della rete pubblica di vedere l'origine e la destinazione finali del pacchetto. Pertanto, per consentire ai client Windows 2000 L2TP/IPsec di connettersi all'appliance di sicurezza, è necessario configurare la modalità di trasporto IPsec per una trasformazione (vedere il passaggio 2 nella [configurazione ASDM](#)). Con questa funzionalità (trasporto), è possibile abilitare un'elaborazione speciale (ad esempio, QoS) sulla rete intermedia in base alle informazioni contenute nell'intestazione IP. Tuttavia, l'intestazione di layer 4 è crittografata, il che limita l'esame del pacchetto. Purtroppo, la trasmissione dell'intestazione IP in modalità di trasporto non crittografata consente a un utente non autorizzato di eseguire un'analisi del traffico.
2. Configurare L2TP con un gruppo VPDN (Virtual Private Dial-up Network).

La configurazione di L2TP con IPsec supporta certificati che utilizzano chiavi già condivise o metodi di firma RSA e l'utilizzo di mappe crittografiche dinamiche (anziché statiche). La chiave già condivisa viene utilizzata come autenticazione per stabilire il tunnel L2TP su IPsec.

Configurazione

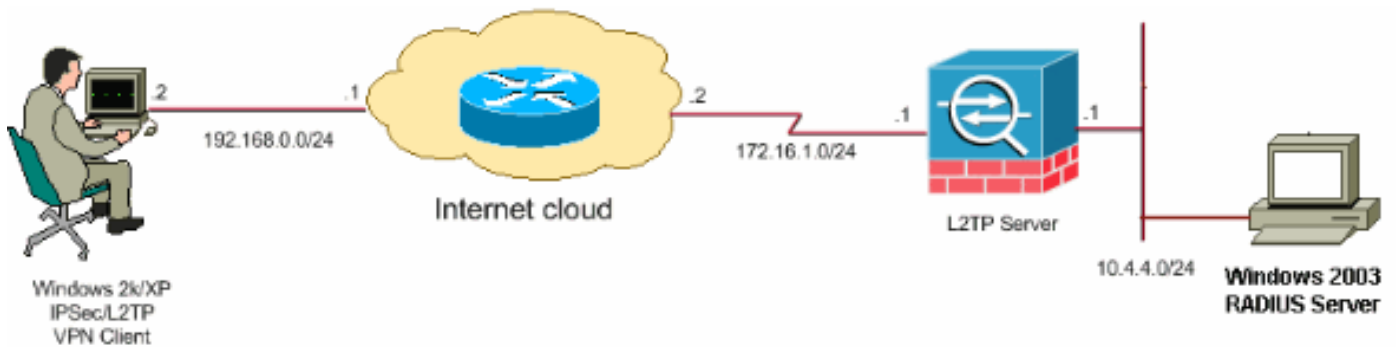
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

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.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- [Configurazione client Windows L2TP/IPsec](#)
- [Server L2TP in configurazione PIX](#)
- [L2TP con configurazione ASDM](#)
- [Microsoft Windows 2003 Server con configurazione IAS](#)

Configurazione client Windows L2TP/IPsec

Completare questa procedura per configurare L2TP over IPsec su Windows 2000. Per Windows XP ignorare i passaggi 1 e 2 e iniziare dal passaggio 3:

1. Aggiungere questo valore del Registro di sistema al computer con Windows 2000:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

2. Aggiungere il valore del Registro di sistema alla chiave:

```
Value Name: ProhibitIpSec
```

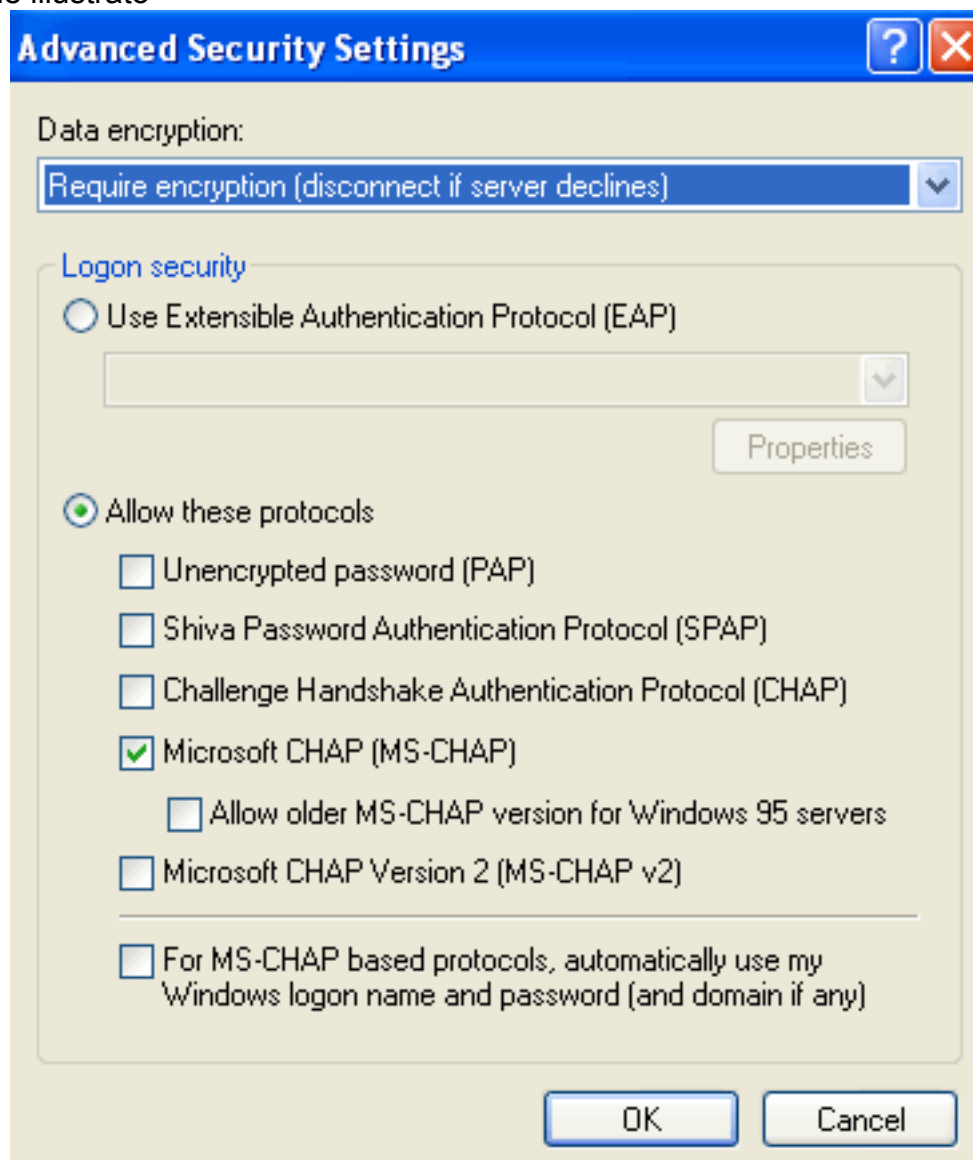
```
Data Type: REG_DWORD
```

```
Value: 1
```

Nota: in alcuni casi (Windows XP Sp2), l'aggiunta di questa chiave (**Valore: 1**) sembra interrompere la connessione in quanto il box XP negozia solo L2TP anziché L2TP con connessione IPsec. È obbligatorio aggiungere un criterio IPsec insieme alla chiave del Registro di sistema. Se viene visualizzato l'errore 800 quando si tenta di stabilire una connessione, rimuovere la chiave (Valore: 1) per ottenere la connessione per lavorare. **Nota:** per rendere effettive le modifiche è necessario riavviare il computer con Windows 2000/2003 o XP. Per impostazione predefinita, il client Windows tenta di utilizzare IPsec con un'Autorità di certificazione (CA). La configurazione di questa chiave del Registro di sistema impedisce il verificarsi di questa condizione. A questo punto, è possibile configurare un criterio IPsec sulla stazione Windows in modo che corrisponda ai parametri desiderati sull'appliance PIX/ASA. Per una configurazione dettagliata del criterio IPsec di Windows, consultare il documento sulla [configurazione di una connessione L2TP/IPsec con autenticazione con chiave già condivisa \(Q240262\)](#). Per ulteriori informazioni, fare riferimento a [Configurazione di una chiave già condivisa da utilizzare con le connessioni del protocollo di tunneling di layer 2 in](#)

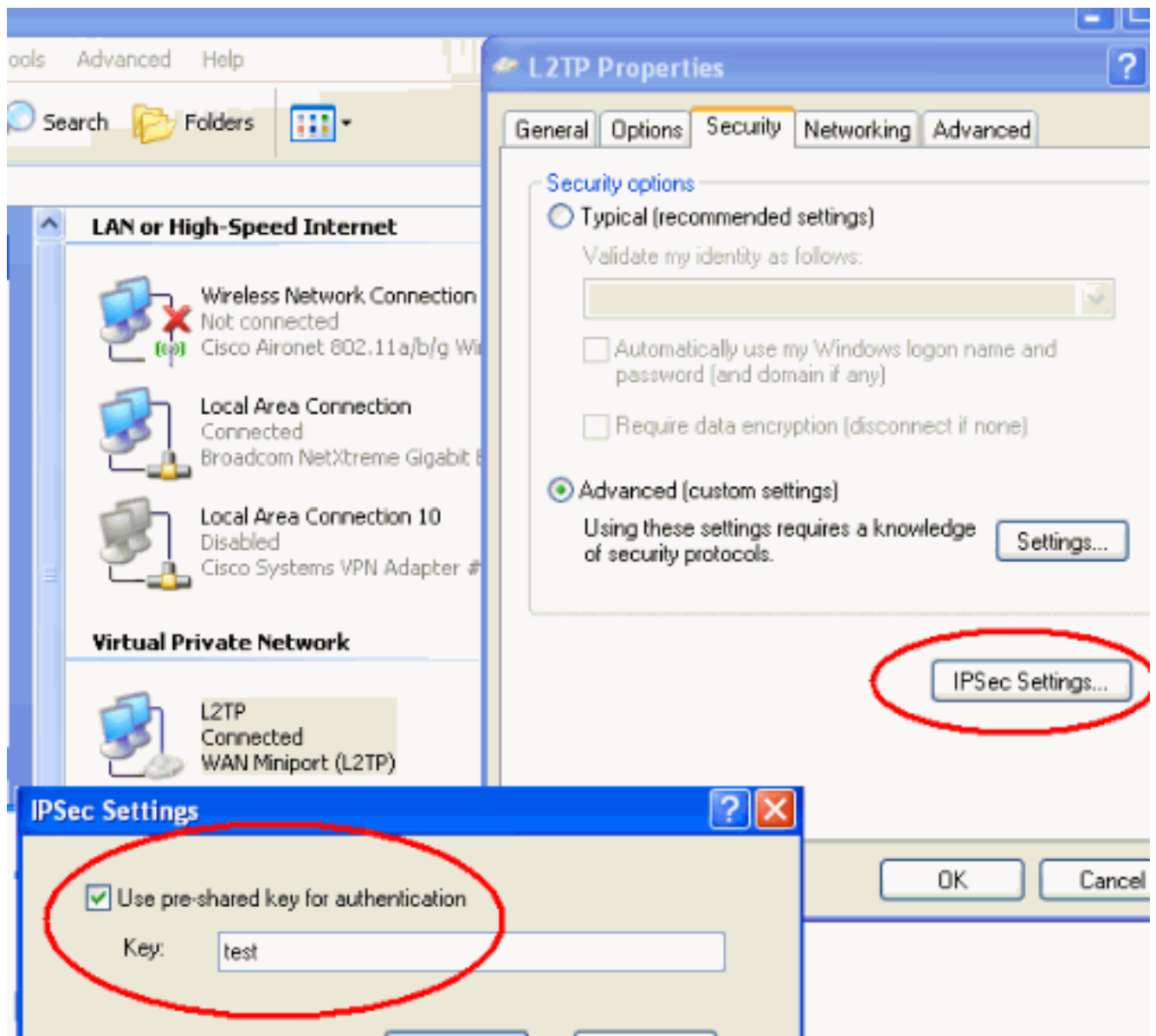
[Windows XP \(Q28155\)](#) .

3. Creare la connessione.
4. In Rete e connessioni remote, fare clic con il pulsante destro del mouse sulla connessione e scegliere **Proprietà**. Andare alla scheda Protezione e fare clic su **Avanzate**. Scegliere i protocolli come illustrato



nell'immagine.

5. **Nota:** Questo passaggio è valido solo per Windows XP. Fare clic su **Impostazioni IPsec**, selezionare **Usa chiave già condivisa per l'autenticazione** e digitare la chiave già condivisa per impostarla. Nell'esempio, test viene utilizzato come chiave già condivisa.



Server L2TP in configurazione PIX

PIX 7.2

```
pixfirewall#show run

PIX Version 7.2(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside and inside interfaces.
interface Ethernet0 nameif outside security-level 0 ip
address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0
nat (inside) 0 access-list nonat

pager lines 24
```

```

logging console debugging
mtu outside 1500
mtu inside 1500

!--- Creates a pool of addresses from which IP addresses
are assigned !--- dynamically to the remote VPN Clients.
ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0

no failover
asdm image flash:/asdm-521.bin
no asdm history enable
arp timeout 14400

!--- The global and nat command enable !--- the Port
Address Translation (PAT) using an outside interface IP
!--- address for all outgoing traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

!--- Create the AAA server group "vpn" and specify its
protocol as RADIUS. !--- Specify the IAS server as a
member of the "vpn" group and provide its !--- location
and key. aaa-server vpn protocol radius
aaa-server vpn host 10.4.4.2
key radiuskey

!--- Identifies the group policy as internal. group-
policy DefaultRAGroup internal
!--- Instructs the security appliance to send DNS and !-
-- WINS server IP addresses to the client. group-policy
DefaultRAGroup attributes
wins-server value 10.4.4.99
dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec
default-domain value cisco.com
!--- Configure usernames and passwords on the device !--
- in addition to using AAA. !--- If the user is an L2TP
client that uses Microsoft CHAP version 1 or !---
version 2, and the security appliance is configured !---
to authenticate against the local !--- database, you
must include the mschap keyword. !--- For example,
username

username test password DLauIAX3178qgoB5c7iVNw== nt-

```

encrypted

vpn-tunnel-protocol l2tp-ipsec

http server enable

http 0.0.0.0 0.0.0.0 inside

no snmp-server location

no snmp-server contact

snmp-server enable traps snmp authentication linkup

linkdown coldstart

!--- Identifies the IPsec encryption and hash algorithms

!--- to be used by the transform set. crypto ipsec

transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac

!--- Since the Windows 2000 L2TP/IPsec client uses IPsec

transport mode, !--- set the mode to transport. !--- The

default is tunnel mode. crypto ipsec transform-set

TRANS_ESP_3DES_MD5 mode transport

!--- Specifies the transform sets to use in a dynamic

crypto map entry. crypto dynamic-map outside_dyn_map 20

set transform-set TRANS_ESP_3DES_MD5

!--- Requires a given crypto map entry to refer to a

pre-existing !--- dynamic crypto map. crypto map

outside_map 20 ipsec-isakmp dynamic outside_dyn_map

!--- Applies a previously defined crypto map set to an

outside interface. crypto map outside_map interface

outside

crypto isakmp enable outside

crypto isakmp nat-traversal 20

!--- Specifies the IKE Phase I policy parameters. crypto

isakmp policy 10

authentication pre-share

encryption 3des

hash md5

group 2

lifetime 86400

!--- Creates a tunnel group with the tunnel-group

command, and specifies the local !--- address pool name

used to allocate the IP address to the client. !---

Associate the AAA server group (VPN) with the tunnel

group.

tunnel-group DefaultRAGroup general-attributes

address-pool clientVPNpool

authentication-server-group vpn

!--- Link the name of the group policy to the default

tunnel !--- group from tunnel group general-attributes

mode. default-group-policy DefaultRAGroup

!--- Use the tunnel-group ipsec-attributes command !---

in order to enter the ipsec-attribute configuration


```
mode. !--- Set the pre-shared key. !--- This key should
be the same as the key configured on the Windows
machine.
```

```
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key *
```

```
!--- Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode.
```

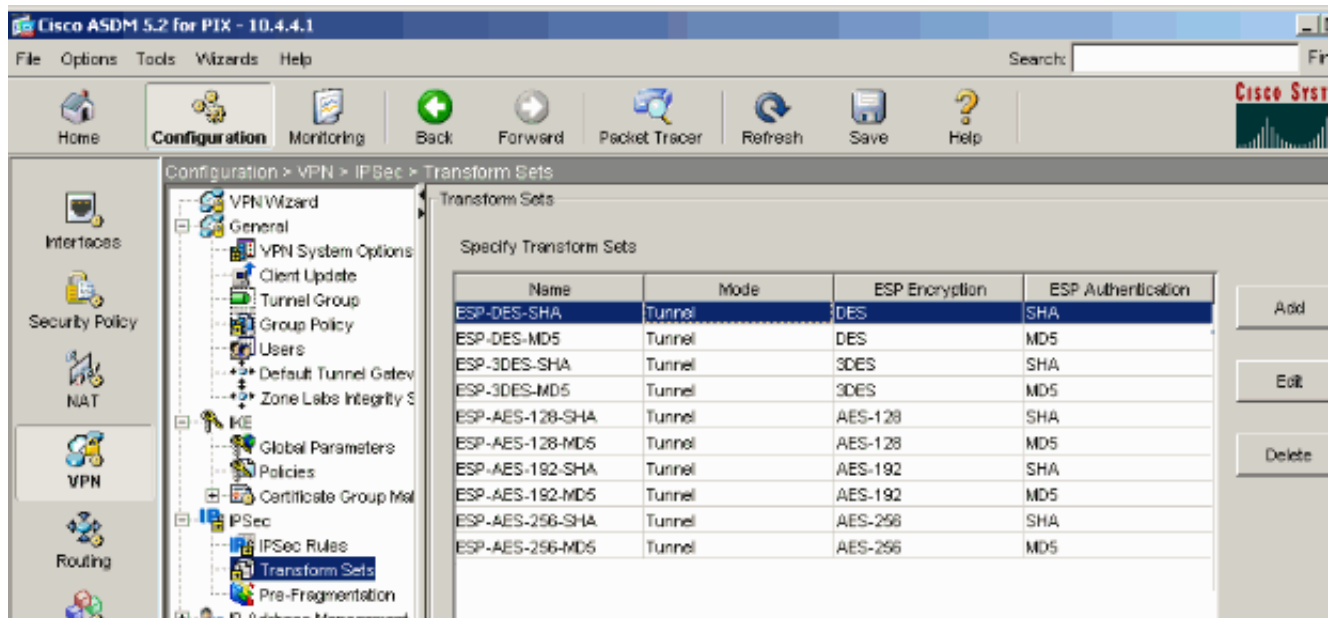
```
tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:ele0730fa260244caa2e2784f632accd
: end
```

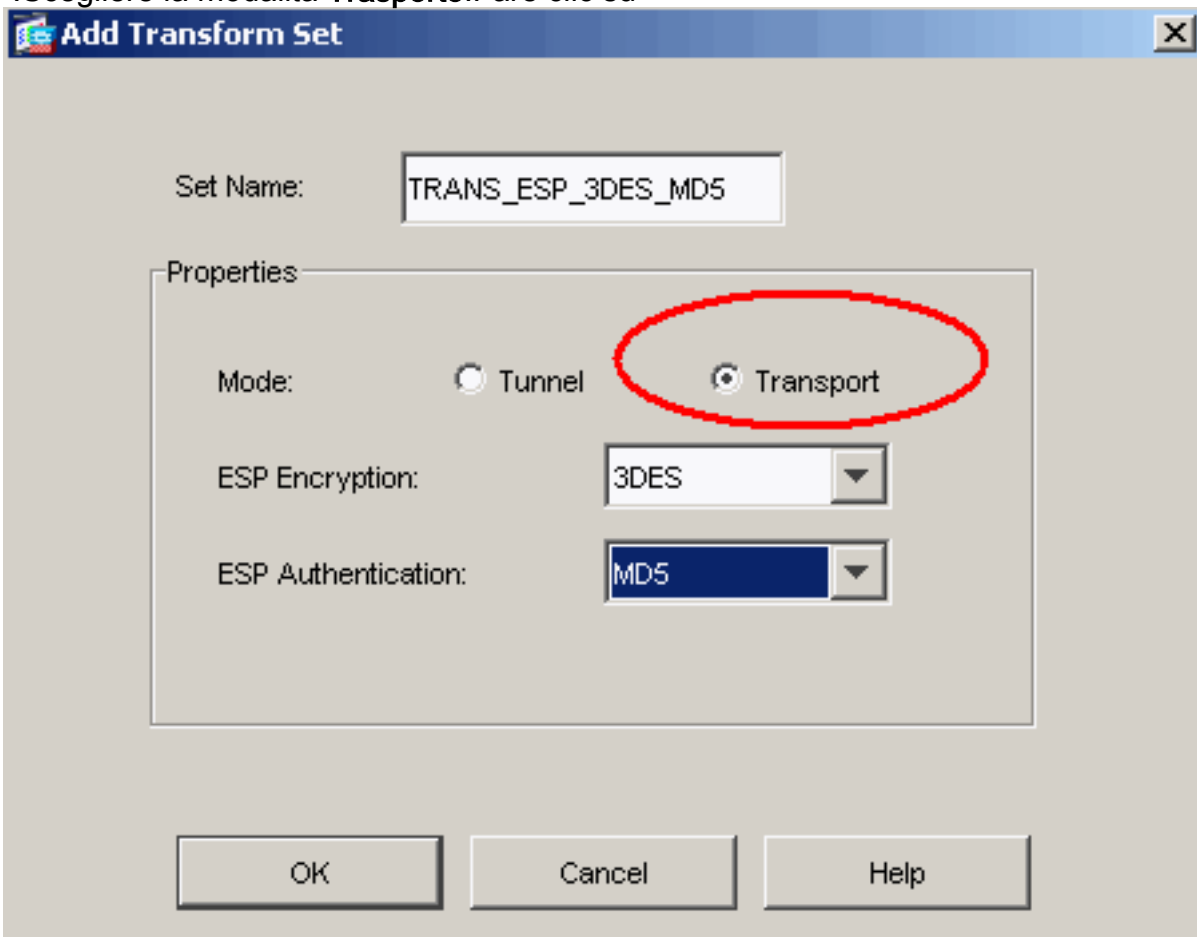
[L2TP con configurazione ASDM](#)

Per configurare l'appliance di sicurezza in modo che accetti le connessioni L2TP su IPsec, completare la procedura seguente:

1. Aggiungere un set di trasformazioni IPsec e specificare IPsec per utilizzare la modalità di trasporto anziché la modalità tunnel. A tale scopo, scegliere **Configurazione > VPN > IPsec > Set di trasformazioni** e fare clic su **Aggiungi**. Viene visualizzato il riquadro Set trasformazioni.

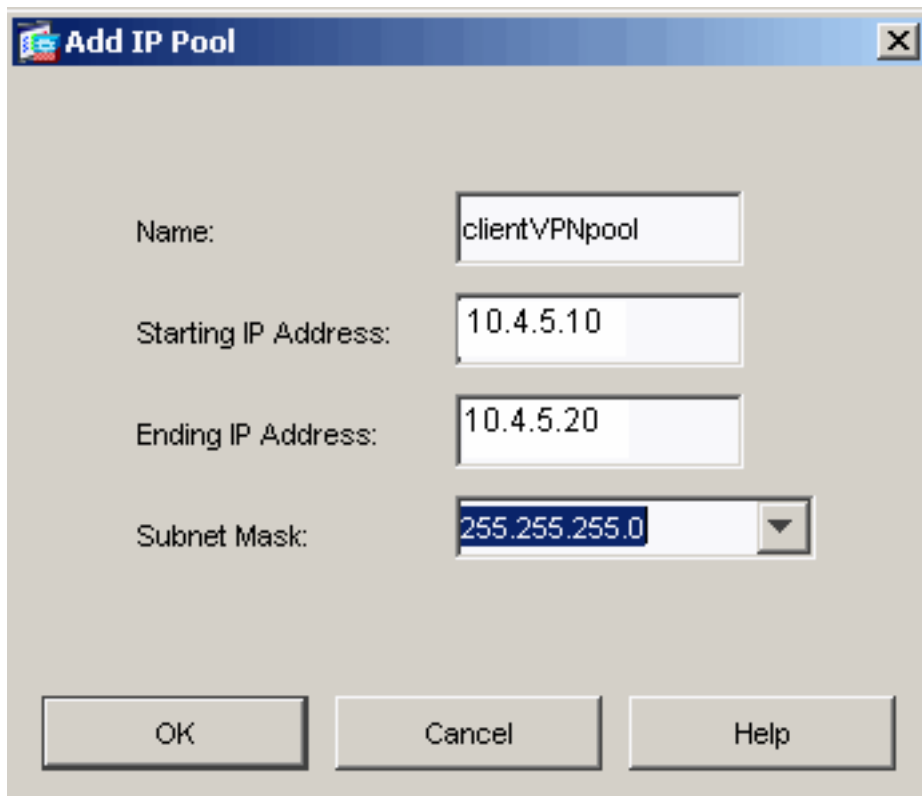


2. Per aggiungere un set di trasformazioni, completare i seguenti passaggi: Immettere un nome per il set di trasformazioni. Scegliere i metodi Crittografia ESP e Autenticazione ESP. Scegliere la modalità **Trasporto**. Fare clic su



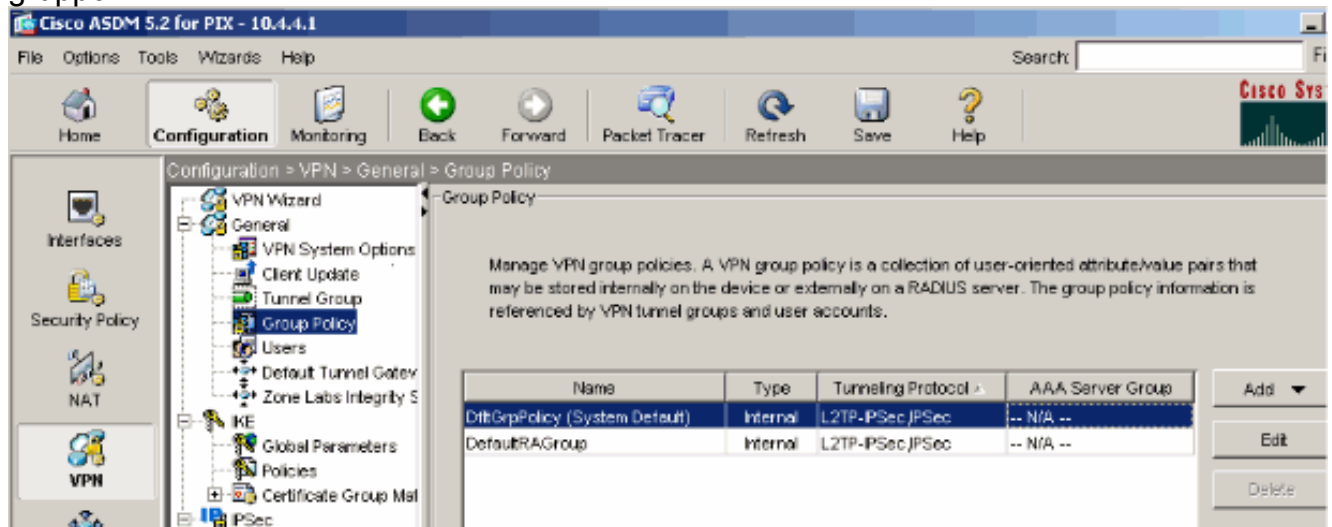
OK.

3. Completare questa procedura per configurare un metodo di assegnazione degli indirizzi. In questo esempio vengono utilizzati pool di indirizzi IP. Scegliere **Configurazione > VPN > Gestione indirizzi IP > Pool IP**. Fare clic su **Add**. Verrà visualizzata la finestra di dialogo **Aggiungi pool IP**. Immettere il nome del nuovo pool di indirizzi IP. Immettere gli indirizzi IP iniziale e finale. Immettere la subnet mask e fare clic su

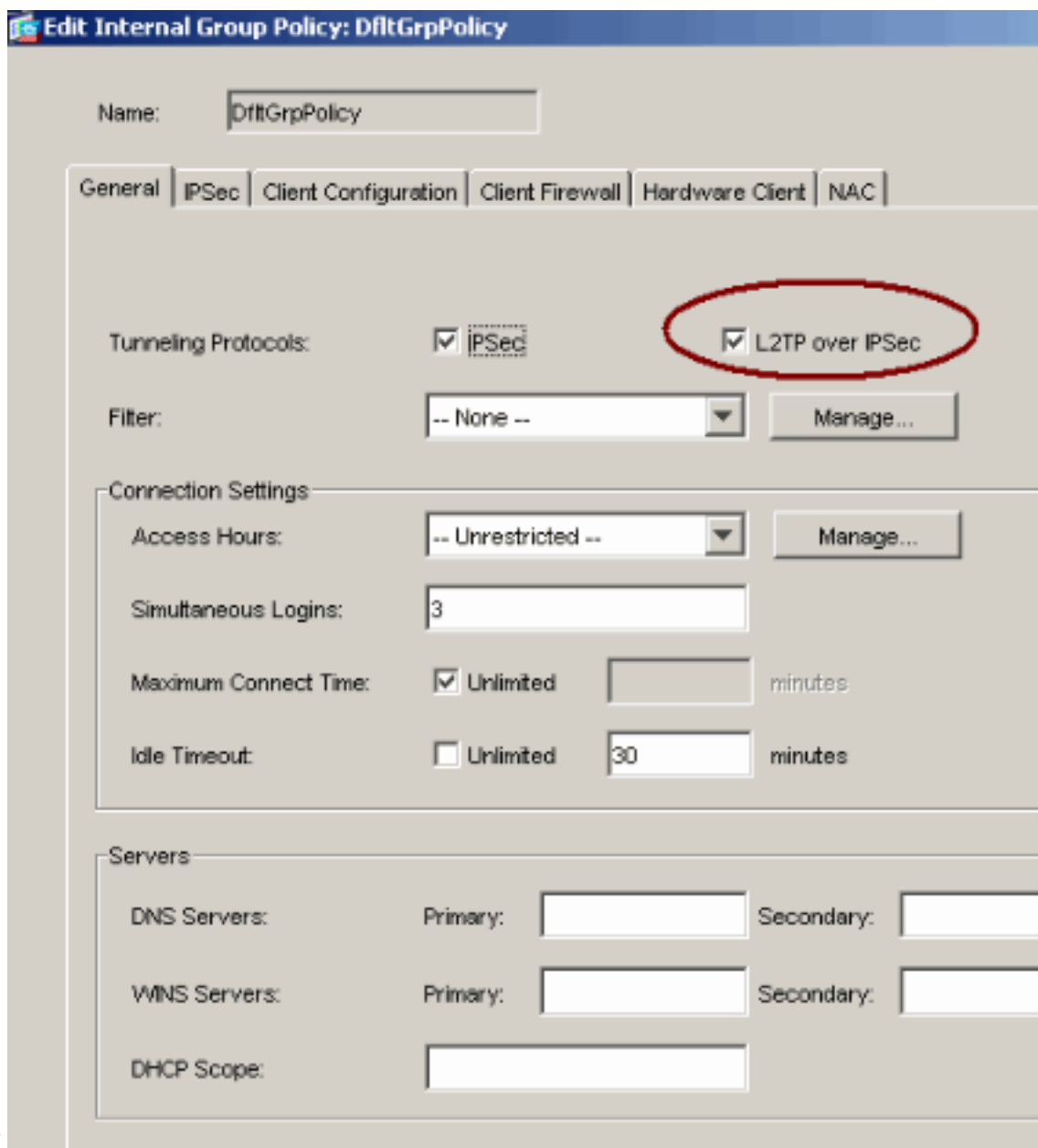


OK.

4. Scegliere **Configurazione > VPN > Generale > Criteri di gruppo** per configurare L2TP su IPsec come protocollo di tunneling VPN valido per i Criteri di gruppo. Verrà visualizzato il riquadro Criteri di gruppo.

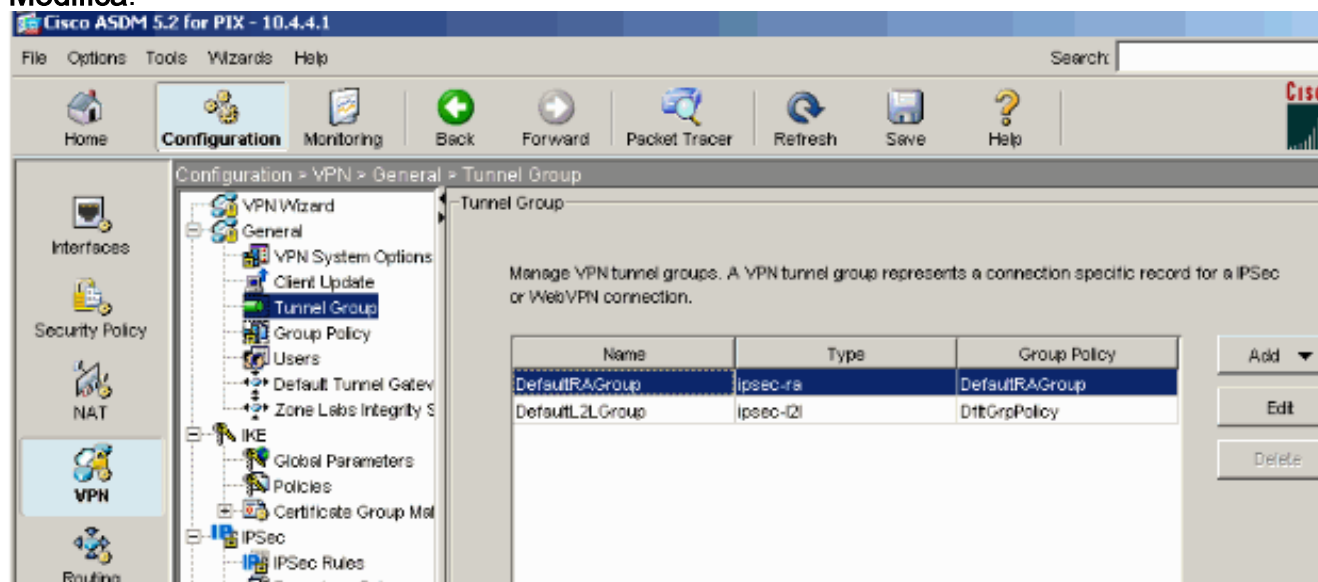


5. Selezionare un criterio di gruppo (DiffGrpPolicy) e fare clic su **Modifica**. Verrà visualizzata la finestra di dialogo Modifica Criteri di gruppo. Selezionare **L2TP su IPsec** per abilitare il protocollo per i Criteri di gruppo e quindi fare clic su

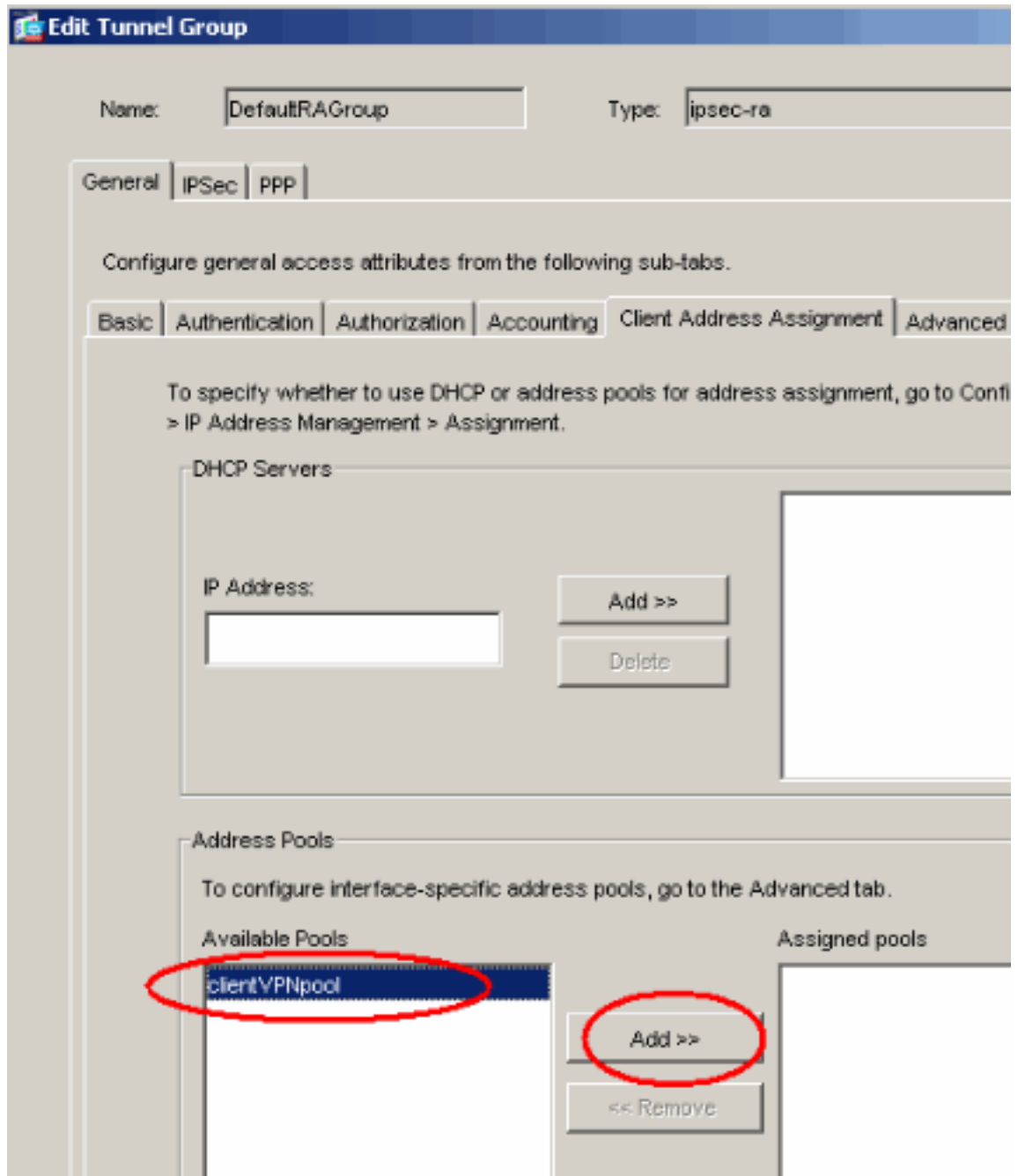


OK.

- Per assegnare il pool di indirizzi IP a un gruppo di tunnel, completare i seguenti passaggi: Scegliere **Configurazione > VPN > Generale > Gruppo di tunnel**. Dopo la visualizzazione del riquadro Gruppo di tunnel, selezionare un gruppo di tunnel (DefaultRAGroup) nella tabella. Fare clic su **Modifica**.



7. Completare questi passaggi quando viene visualizzata la finestra Modifica gruppo di tunnel: Dalla scheda Generale passare alla scheda Assegnazione indirizzo client. Nell'area Pool di indirizzi scegliere un pool di indirizzi da assegnare al gruppo di tunnel. Fare clic su **Add**. Il pool di indirizzi viene visualizzato nella casella Pool



assegnati.

8. Per impostare la chiave già condivisa, andare alla scheda IPsec, immettere la **chiave già condivisa** e fare clic su **OK**.

Edit Tunnel Group

Name: Type:

General | IPsec | **PPP**

Pre-shared Key: Trustpoint Name:

Authentication Mode: IKE Peer ID Validation:

Enable sending certificate chain

ISAKMP Keepalive

Disable keepalives

Monitor keepalives

Confidence Interval: (seconds) Retry Interval: (seconds)

Head end will never initiate keepalive monitoring

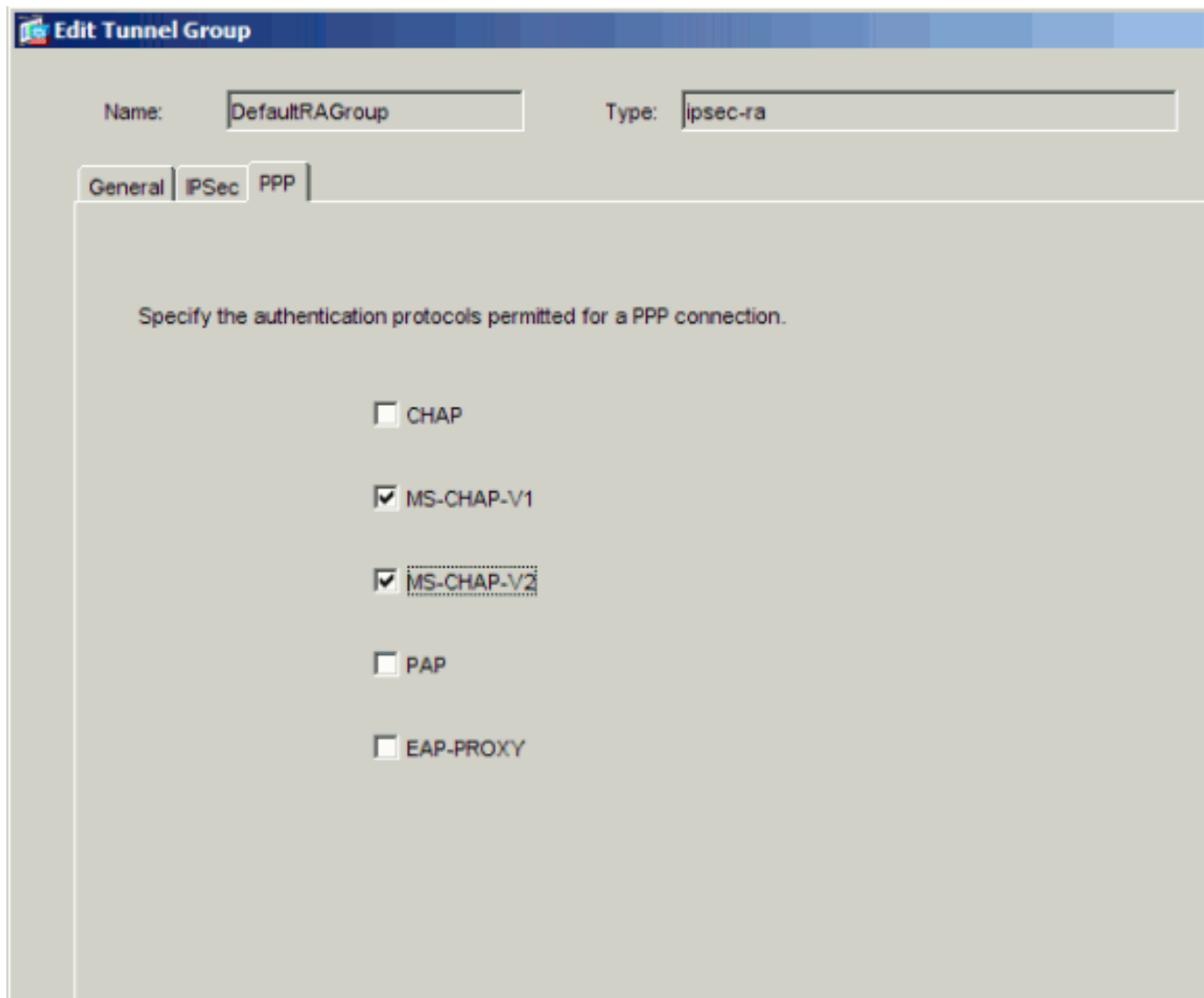
Interface-Specific Authentication Mode

Interface: Add >>

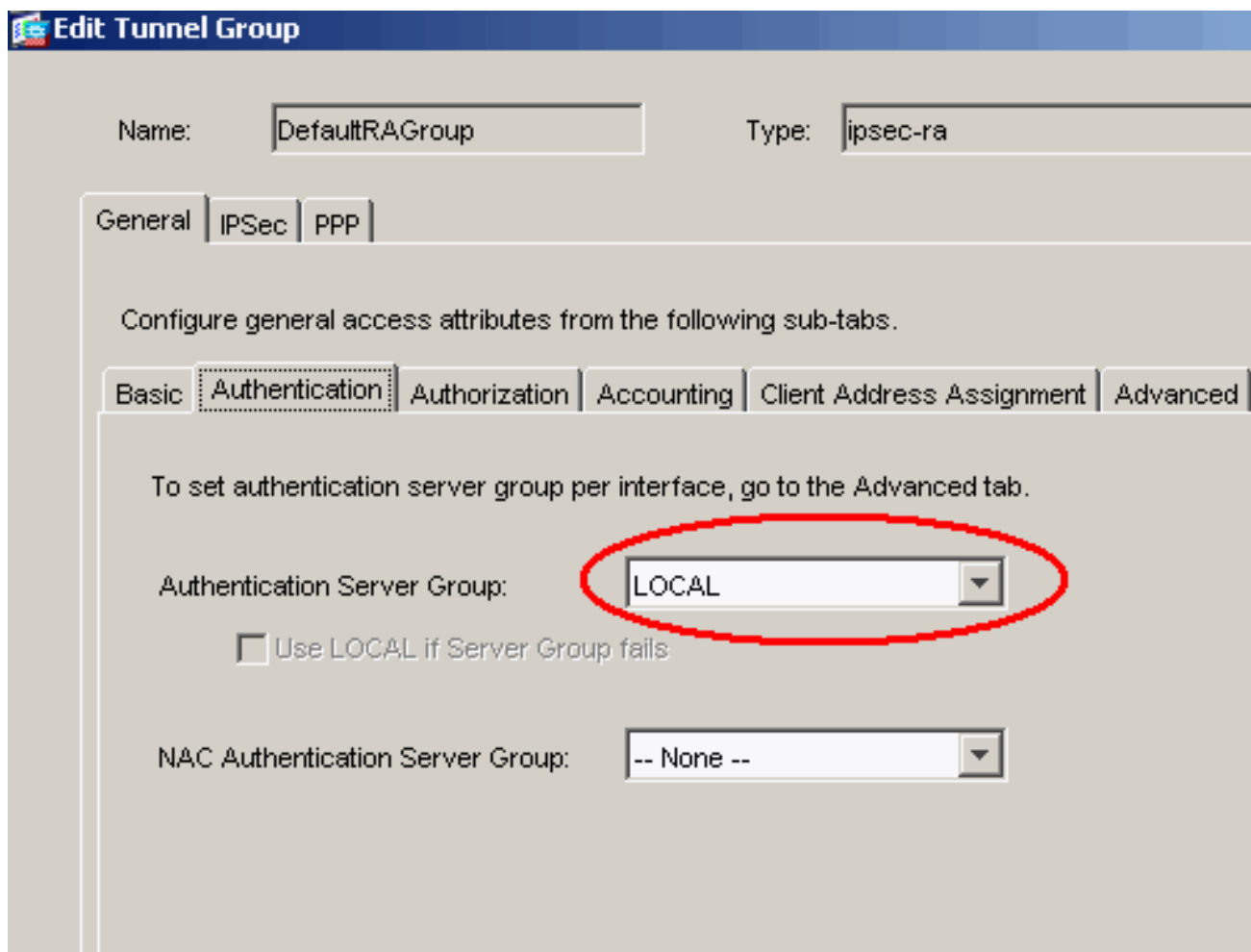
Authentication Mode: << Remove

| Interface | Authentication Mode |
|-----------|---------------------|
| | |

9. L2TP over IPsec utilizza protocolli di autenticazione PPP. Specificare i protocolli consentiti per le connessioni PPP nella scheda PPP del gruppo di tunnel. Selezionare il protocollo **MS-CHAP-V1** per l'autenticazione.



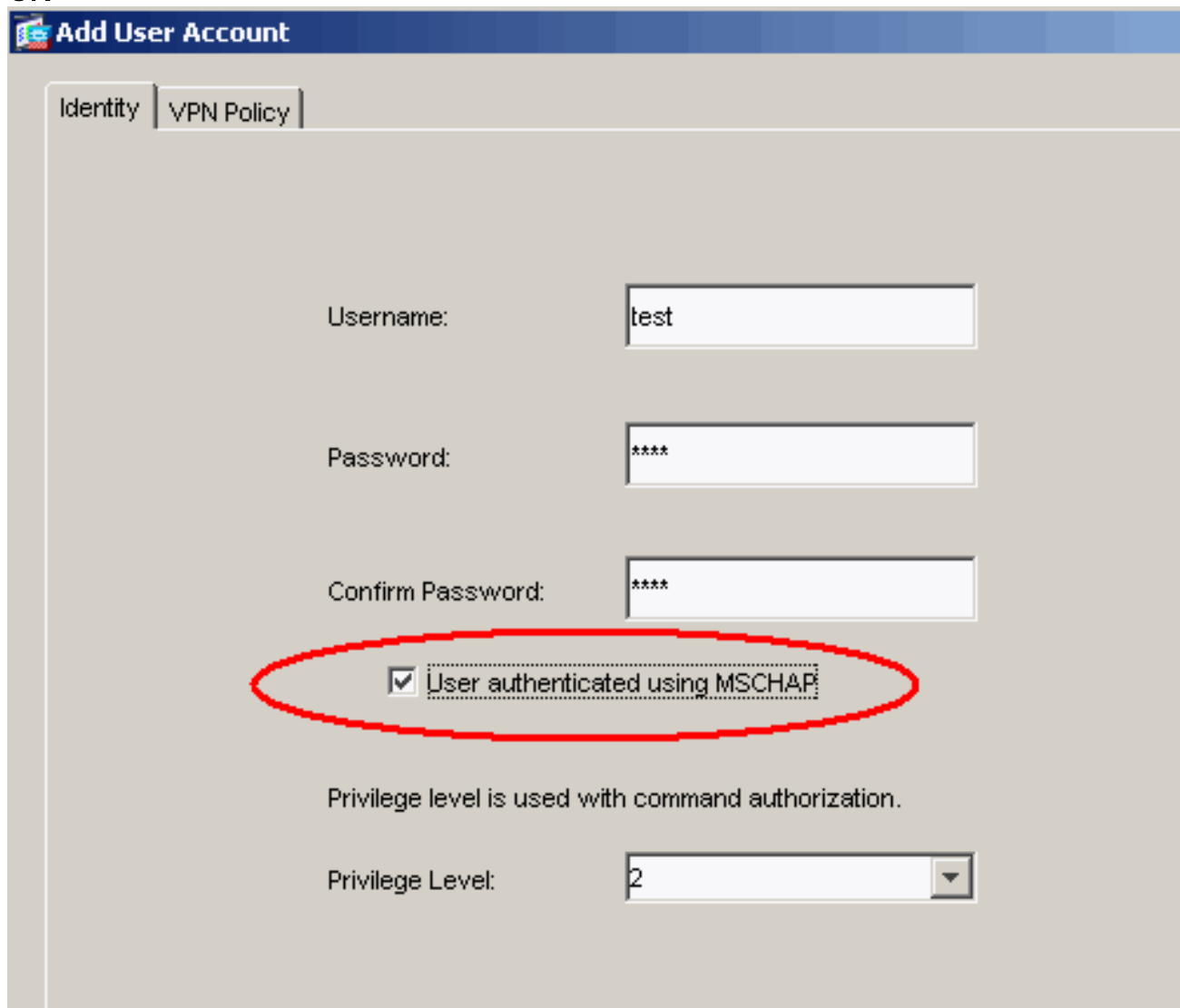
10. Specificare un metodo per autenticare gli utenti che tentano connessioni L2TP su IPsec. È possibile configurare l'accessorio di protezione in modo che utilizzi un server di autenticazione o un database locale. A tale scopo, passare alla scheda Autenticazione del gruppo di tunnel. Per impostazione predefinita, l'accessorio di protezione utilizza il database locale. Nell'elenco a discesa Authentication Server Group (Gruppo server di autenticazione) viene visualizzato LOCAL (LOCALE). Per utilizzare un server di autenticazione, selezionarne uno dall'elenco. **Nota:** l'accessorio di protezione supporta solo le autenticazioni PPP PAP e la protezione CHAP Microsoft versioni 1 e 2 nel database locale. EAP e CHAP vengono eseguiti dai server di autenticazione proxy. Pertanto, se un utente remoto appartiene a un gruppo di tunnel configurato con EAP o CHAP e l'appliance di sicurezza è configurata per l'utilizzo del database locale, tale utente non sarà in grado di connettersi.



Nota: scegliere **Configurazione > VPN > Generale > Gruppo di tunnel** per tornare alla configurazione del gruppo di tunnel in modo da poter collegare i Criteri di gruppo al gruppo di tunnel e abilitare Tunnel Group Switching (facoltativo). Quando viene visualizzato il riquadro Gruppo di tunnel, scegliere il gruppo di tunnel e fare clic su **Modifica**. **Nota:** la funzionalità Tunnel Group Switching consente all'appliance di sicurezza di associare diversi utenti che stabiliscono connessioni L2TP su IPsec a diversi gruppi di tunnel. Poiché ogni gruppo di tunnel dispone di un proprio gruppo di server AAA e di pool di indirizzi IP, gli utenti possono essere autenticati tramite metodi specifici del proprio gruppo di tunnel. Con questa funzionalità, invece di inviare solo un nome utente, l'utente invia un nome utente e un nome di gruppo nel formato `username@group_name`, dove "@" rappresenta un delimitatore che è possibile configurare e il nome del gruppo è il nome di un gruppo di tunnel configurato sull'appliance di sicurezza. **Nota:** la funzionalità Tunnel Group Switching è abilitata dall'elaborazione Strip Group, che consente all'appliance di sicurezza di selezionare il gruppo di tunnel per le connessioni utente ottenendo il nome del gruppo dal nome utente presentato dal client VPN. L'accessorio di protezione invia quindi all'utente solo la parte del nome utente per l'autorizzazione e l'autenticazione. In caso contrario (se disattivato), l'appliance di sicurezza invia l'intero nome utente, compreso il realm. Per abilitare Tunnel Group Switching, selezionare **Rimuovi il realm dal nome utente prima di passarlo al server AAA**, quindi selezionare **Rimuovi il gruppo dal nome utente prima di passarlo al server AAA**. Quindi fare clic su **OK**.

11. Per creare un utente nel database locale, completare i seguenti passaggi: Scegliere **Configurazione > Proprietà > Amministrazione periferica > Account utente**. Fare clic su **Add**. Se l'utente è un client L2TP che utilizza Microsoft CHAP versione 1 o 2 e l'appliance di sicurezza è configurata per l'autenticazione sul database locale, è necessario selezionare

Autenticato dall'utente tramite MSCHAP per abilitare MSCHAP. Fare clic su OK.



Add User Account

Identity | VPN Policy

Username: test

Password: ****

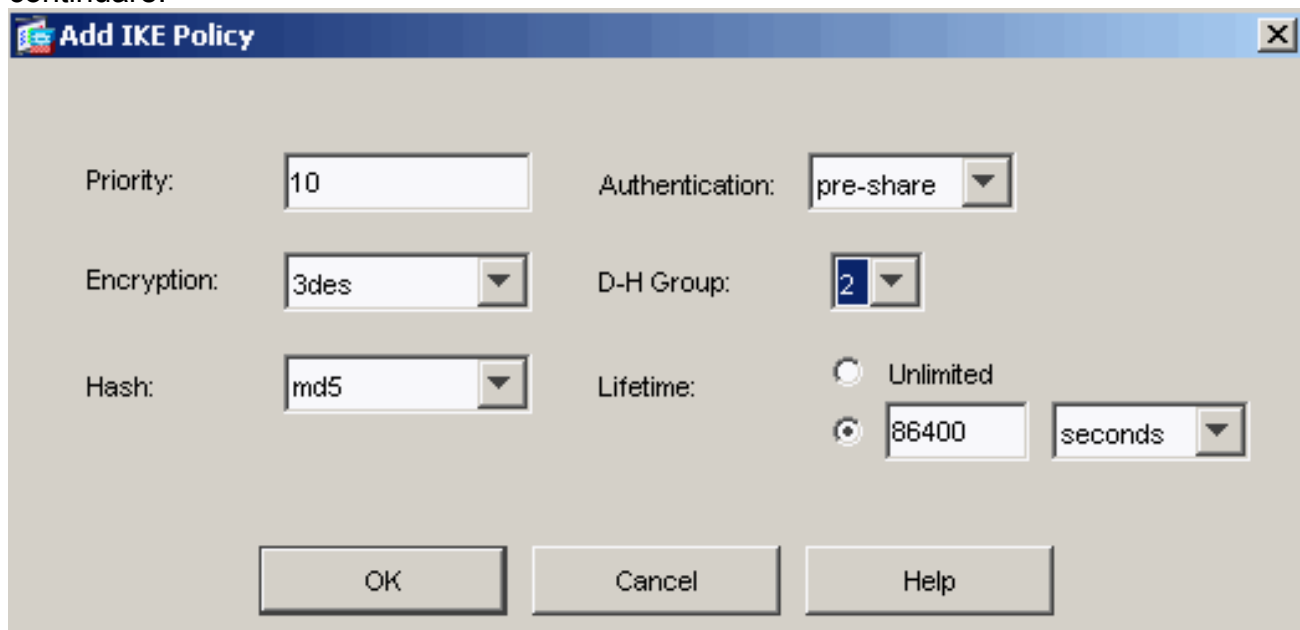
Confirm Password: ****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

12. Scegliere **Configurazione > VPN > IKE > Criteri** e fare clic su **Aggiungi** per creare un criterio IKE per la fase I. Fare clic su **OK** per continuare.



Add IKE Policy

Priority: 10

Authentication: pre-share

Encryption: 3des

D-H Group: 2

Hash: md5

Lifetime: Unlimited 86400 seconds

OK Cancel Help

13. (Facoltativo) Se si prevede che più client L2TP dietro un dispositivo NAT tentino

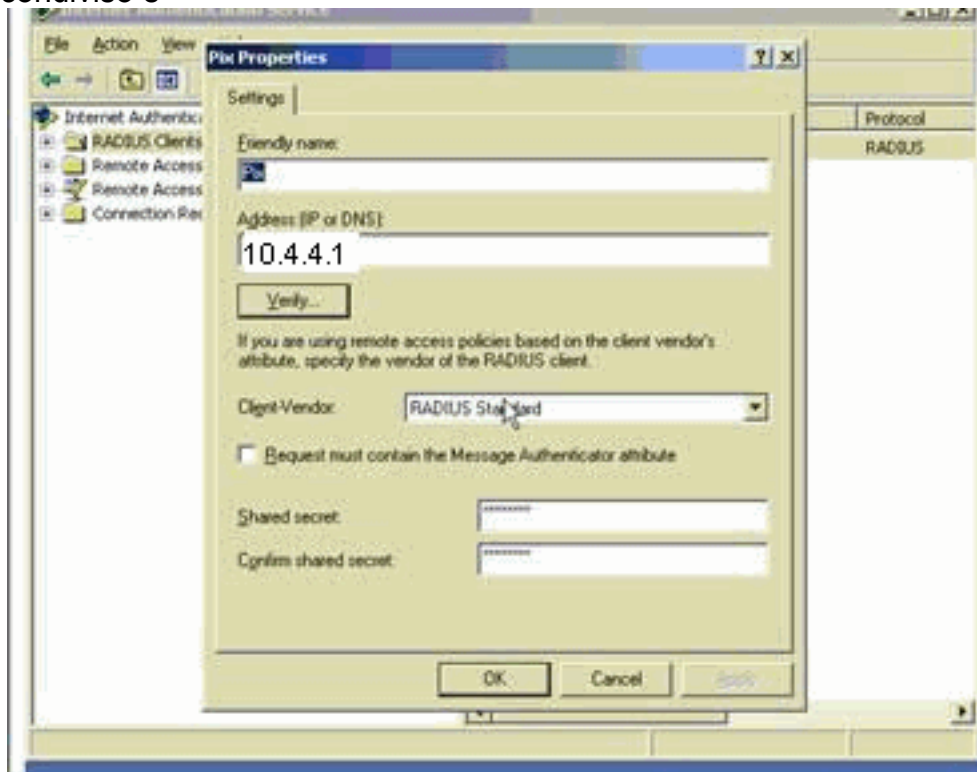
connessioni L2TP su IPsec all'appliance di sicurezza, è necessario abilitare l'attraversamento NAT in modo che i pacchetti ESP possano passare attraverso uno o più dispositivi NAT. A tale scopo, completare i seguenti passaggi: Scegliere **Configurazione > VPN > IKE > Parametri globali**. Verificare che **ISAKMP** sia abilitato su un'interfaccia. Selezionare **Enable IPsec over NAT-T**. Fare clic su **OK**.

[Microsoft Windows 2003 Server con configurazione IAS](#)

Completare questa procedura per configurare il server Microsoft Windows 2003 con IAS.

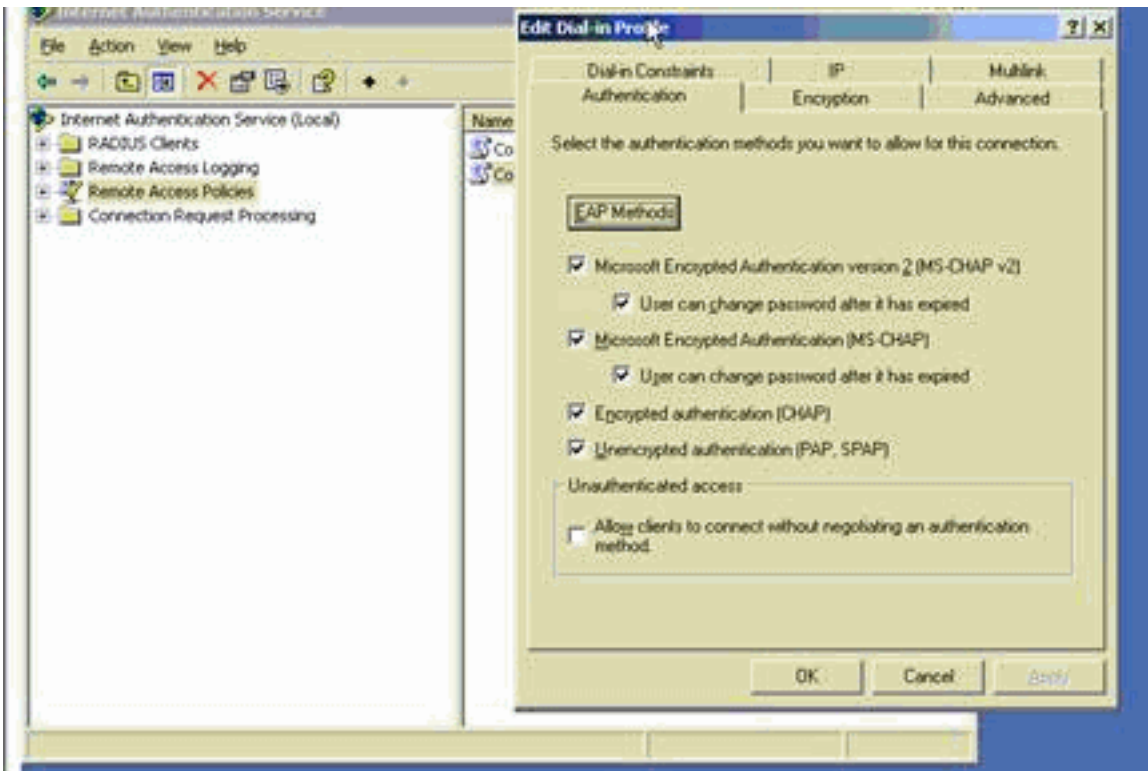
Nota: in questa procedura si presuppone che IAS sia già installato nel computer locale. In caso contrario, aggiungerlo tramite **Pannello di controllo > Installazione applicazioni**.

1. Scegliere **Strumenti di amministrazione > Servizio di autenticazione Internet** e fare clic con il pulsante destro del mouse su **Client RADIUS** per aggiungere un nuovo client RADIUS. Dopo aver digitato le informazioni sul client, fare clic su **OK**. Nell'esempio viene mostrato un client denominato "Pix" con indirizzo IP 10.4.4.1. Client-Vendor è impostato su **RADIUS Standard** e il segreto condiviso è



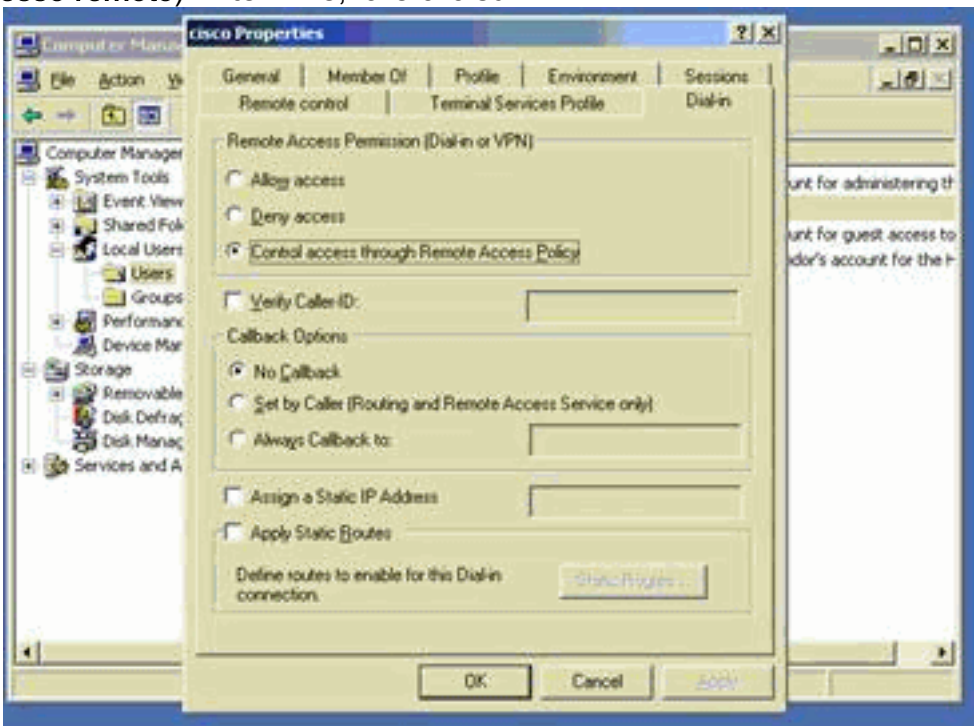
radiuskey.

2. Scegliere **Criteri di accesso remoto**, fare clic con il pulsante destro del mouse su **Connessioni ad altri server di accesso** e selezionare **Proprietà**.
3. Verificare che l'opzione **Concedi autorizzazioni di accesso remoto** sia selezionata.
4. Fare clic su **Modifica profilo** e verificare le seguenti impostazioni: Nella scheda **Autenticazione** selezionare **Autenticazione non crittografata (PAP, SPAP)**. Nella scheda **Crittografia** verificare che l'opzione **Nessuna crittografia** sia selezionata. Al termine, fare clic su



OK.

5. Scegliere **Strumenti di amministrazione > Gestione computer > Utilità di sistema > Utenti e gruppi locali**, fare clic con il pulsante destro del mouse su **Utenti** e selezionare **Nuovi utenti** per aggiungere un utente all'account del computer locale.
6. Aggiungere un utente con password Cisco **password1** e controllare le seguenti informazioni del profilo: Nella scheda **Generale**, assicurarsi che l'opzione **Password Never Expired** (Password non scaduta) sia selezionata anziché l'opzione **User Must Change Password** (Modifica password obbligatoria). Nella scheda **Connessione remota** selezionare l'opzione **Consenti accesso** (o lasciare l'impostazione predefinita **Controlla accesso tramite Criteri di accesso remoto**). Al termine, fare clic su



OK.

[Autenticazione estesa per L2TP su IPSec tramite Active Directory](#)

Utilizzare questa configurazione sull'appliance ASA per consentire l'autenticazione della connessione L2tp da Active Directory:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup
ppp-attributes
ciscoasa(config-ppp)# authentication pap
```

Inoltre, sul client L2tp, passare a **Impostazioni di sicurezza avanzate (Personalizzate)** e scegliere solo l'opzione per **Password non crittografata (PAP)**.

Verifica

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

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

- **show crypto ipsec sa:** visualizza tutte le associazioni di sicurezza IKE correnti in un peer.

```
pixfirewall#show crypto ipsec sa
interface: outside
  Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1

  access-list 105 permit ip host 172.16.1.1 host 192.168.0.2
  local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0)
  remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701)
  current_peer: 192.168.0.2, username: test
  dynamic allocated peer ip: 10.4.5.15

#pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
#pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: C16F05B8

inbound esp sas:
  spi: 0xEC06344D (3959829581)
  transform: esp-3des esp-md5-hmac
  in use settings = {RA, Transport, }
  slot: 0, conn_id: 3, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (sec): 3335
  IV size: 8 bytes
  replay detection support: Y

outbound esp sas:
  spi: 0xC16F05B8 (3245278648)
  transform: esp-3des esp-md5-hmac
  in use settings = {RA, Transport, }
  slot: 0, conn_id: 3, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (sec): 3335
  IV size: 8 bytes
```

replay detection support: Y

- **show crypto isakmp sa:** visualizza tutte le associazioni di protezione IKE correnti in un peer.

```
pixfirewall#show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 192.168.0.2
  Type      : user           Role      : responder
  Rekey     : no            State     : MM_ACTIVE
```

- **show vpn-sessiondb:** include i filtri di protocollo che è possibile utilizzare per visualizzare informazioni dettagliate sulle connessioni L2TP su IPsec. Il comando full dalla modalità di configurazione globale è **show vpn-sessiondb detailed remote filter protocol L2tpOverIPsec**. Nell'esempio vengono mostrati i dettagli di una singola connessione L2TP su IPsec:

```
pixfirewall#show vpn-sessiondb detail remote filter protocol L2TPOverIPSec
```

Session Type: Remote Detailed

```
Username      : test
Index         : 1
Assigned IP   : 10.4.5.15           Public IP     : 192.168.0.2
Protocol      : L2TPOverIPSec      Encryption    : 3DES
Hashing       : MD5
Bytes Tx      : 1336               Bytes Rx      : 14605
Client Type   :                    Client Ver    :
Group Policy  : DefaultRAGroup
Tunnel Group  : DefaultRAGroup
Login Time    : 18:06:08 UTC Fri Jan 1 1993
Duration      : 0h:04m:25s
Filter Name   :
NAC Result    : N/A
Posture Token :
```

```
IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1
```

IKE:

```
Session ID    : 1
UDP Src Port  : 500                 UDP Dst Port  : 500
IKE Neg Mode  : Main                Auth Mode     : preSharedKeys
Encryption    : 3DES                Hashing       : MD5
Rekey Int (T): 28800 Seconds        Rekey Left(T): 28536 Seconds
D/H Group     : 2
```

IPSec:

```
Session ID    : 2
Local Addr    : 172.16.1.1/255.255.255.255/17/1701
Remote Addr   : 192.168.0.2/255.255.255.255/17/1701
Encryption    : 3DES                Hashing       : MD5
Encapsulation: Transport
Rekey Int (T): 3600 Seconds          Rekey Left(T): 3333 Seconds
Idle Time Out: 30 Minutes            Idle TO Left  : 30 Minutes
Bytes Tx      : 1336                 Bytes Rx      : 14922
Pkts Tx       : 25                   Pkts Rx       : 156
```

L2TPOverIPSec:

```
Session ID    : 3
```

```
Username      : test
Assigned IP   : 10.4.5.15
Encryption    : none
Idle Time Out: 30 Minutes
Bytes Tx      : 378
Pkts Tx      : 16
Auth Mode     : msCHAPV1
Idle TO Left  : 30 Minutes
Bytes Rx      : 13431
Pkts Rx      : 146
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Viene visualizzato anche l'output di esempio del comando debug.

Comandi per la risoluzione dei problemi

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

Nota: consultare le [informazioni importanti sui comandi di debug](#) e sulla [risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug](#) prima di usare i comandi di **debug**.

- **debug crypto ipsec 7:** visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp 7:** visualizza le negoziazioni ISAKMP della fase 1.

Output di esempio del comando debug

PIX Firewall

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess
age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V
ID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform
# 2 acceptable Matches global IKE entry # 2
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID
+ extended capabilities payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa
```

yload

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group DefaultRAGroup

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating keys for Responder...

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group DefaultRAGroup

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previously allocated memory for authorization-dn-attributes

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing ID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing dpd vid payload

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 80

!--- Phase 1 completed successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE 1 COMPLETED**

ETED

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection: None

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer does not support keep-alives (type = None)

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Starting P1 rekey timer: 21600 seconds.

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 164

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing nonce payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remote Proxy Host data in ID Payload: Address 192.168.0.2, Protocol 17, Port 1701

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received local Proxy Host data in ID Payload: Address 172.16.1.1, Protocol 17, Port 1701

!--- PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **L2TP/IPsec session detected.**

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed old sa not found by addr

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Peer configured for crypto map: outside_dyn_map

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing IPsec SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPsec SA Proposal # 1, Transform # 1 acceptable Matches global IPsec SA entry # 20

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesting SPI!

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got SPI from key engine: SPI = 0xce9f6e19

!--- Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, **oakley constructing quick mode**

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing blank hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec nonce payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing proxy ID

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmitting Proxy Id:

Remote host: 192.168.0.2 Protocol 17 Port 1701

Local host: 172.16.1.1 Protocol 17 Port 1701

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing qm hash payload

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=elb84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 144

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=elb84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading all IPSEC SAs

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security negotiation complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI = 0xd08f711b

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xd08f711b

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher: received KEY_UPDATE, spi 0xce9f6e19

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Starting P2 rekey timer: 3059 seconds.

!--- Phase 2 completes successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPLETED (msgid=0elb84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.168.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto ipsec 7**

pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09

Rule ID: 0x028D78D8
IPSEC: Deleted inbound permit rule, SPI 0x71933D09
Rule ID: 0x02831838
IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
Rule ID: 0x029134D8
IPSEC: Deleted inbound VPN context, SPI 0x71933D09
VPN handle: 0x0048B284
IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA
Rule ID: 0x028DAC90
IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA
Rule ID: 0x02912AF8
IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA
VPN handle: 0x0048468C
IPSEC: New embryonic SA created @ 0x01BFCF80,
SCB: 0x01C262D0,
Direction: inbound
SPI : 0x45C3306F
Session ID: 0x0000000C
VPIF num : 0x00000001
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x0283A3A8,
SCB: 0x028D1B38,
Direction: outbound
SPI : 0x370E8DD1
Session ID: 0x0000000C
VPIF num : 0x00000001
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x370E8DD1
IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
Flags: 0x00000205
SA : 0x0283A3A8
SPI : 0x370E8DD1
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x028D1B38
Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
VPN handle: 0x0048C164
IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.0.2
Dst mask: 255.255.255.255
Src ports
Upper: 1701
Lower: 1701
Op : equal
Dst ports
Upper: 1701
Lower: 1701
Op : equal
Protocol: 17
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1
Rule ID: 0x02826540
IPSEC: New outbound permit rule, SPI 0x370E8DD1
Src addr: 172.16.1.1

Src mask: 255.255.255.255
Dst addr: 192.168.0.2
Dst mask: 255.255.255.255
Src ports
 Upper: 0
 Lower: 0
 Op : ignore
Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x370E8DD1
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x370E8DD1
 Rule ID: 0x028D78D8
IPSEC: Completed host IBSA update, SPI 0x45C3306F
IPSEC: Creating inbound VPN context, SPI 0x45C3306F
 Flags: 0x00000206
 SA : 0x01BF8CF80
 SPI : 0x45C3306F
 MTU : 0 bytes
 VCID : 0x00000000
 Peer : 0x0048C164
 SCB : 0x01C262D0
 Channel: 0x01693F08
IPSEC: Completed inbound VPN context, SPI 0x45C3306F
 VPN handle: 0x0049107C
IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1
 Flags: 0x00000205
 SA : 0x0283A3A8
 SPI : 0x370E8DD1
 MTU : 1500 bytes
 VCID : 0x00000000
 Peer : 0x0049107C
 SCB : 0x028D1B38
 Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
 VPN handle: 0x0048C164
IPSEC: Completed outbound inner rule, SPI 0x370E8DD1
 Rule ID: 0x02826540
IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1
 Rule ID: 0x028D78D8
IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F
 Src addr: 192.168.0.2
 Src mask: 255.255.255.255
 Dst addr: 172.16.1.1
 Dst mask: 255.255.255.255
 Src ports
 Upper: 1701
 Lower: 1701
 Op : equal
 Dst ports
 Upper: 1701
 Lower: 1701
 Op : equal
 Protocol: 17
 Use protocol: true
 SPI: 0x00000000
 Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F
 Rule ID: 0x02831838
IPSEC: New inbound decrypt rule, SPI 0x45C3306F

```
Src addr: 192.168.0.2
Src mask: 255.255.255.255
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0x45C3306F
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
  Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
  Src addr: 192.168.0.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.1
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x45C3306F
  Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
  Rule ID: 0x02912E50
```

[Risoluzione dei problemi con ASDM](#)

È possibile utilizzare ASDM per abilitare il log e visualizzarne i log.

1. Per abilitare la registrazione, scegliere **Configurazione > Proprietà > Registrazione > Impostazione registrazione**, selezionare **Abilita registrazione** e fare clic su **Applica**.
2. Scegliere **Monitoraggio > Log > Buffer di log > Al livello di log**, selezionare **Buffer di log** e fare clic su **Visualizza** per visualizzare i log.

[Problema: Disconnessioni frequenti](#)

Timeout di inattività/sessione

Se il timeout di inattività è impostato su 30 minuti (impostazione predefinita), significa che il tunnel viene scartato dopo che non è attraversato dal traffico per 30 minuti. Il client VPN si disconnette dopo 30 minuti indipendentemente dall'impostazione del timeout di inattività e rileva il messaggio di errore `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Configurare il timeout di inattività e il timeout di sessione come nessuno in modo che il tunnel sia sempre attivo e che non venga mai scartato.

Immettere il comando **vpn-idle-timeout** in modalità di configurazione criteri di gruppo o in modalità di configurazione nome utente per configurare il periodo di timeout utente:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-idle-timeout none
```

Configurare un periodo di tempo massimo per le connessioni VPN con il comando **vpn-session-timeout** in modalità di configurazione criteri di gruppo o in modalità di configurazione nome utente:

```
hostname(config)#group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#vpn-session-timeout none
```

[Risoluzione dei problemi di Windows Vista](#)

Utente simultaneo

In Windows Vista L2TP/IPsec sono state introdotte alcune modifiche architetturali che impediscono a più utenti simultanei di essere connessi a un'appliance PIX/ASA headend. Questo comportamento non si verifica in Windows 2K/XP. Cisco ha implementato una soluzione per questa modifica a partire dalla versione 7.2(3) e successive.

Impossibile connettersi a Vista PC

Se il computer Windows Vista non è in grado di connettere il server L2TP, verificare di aver configurato SOLO mschap-v2 con gli attributi ppp sul gruppo predefinito RAG.

[Informazioni correlate](#)

- [Soluzioni per la risoluzione dei problemi più comuni di VPN IPsec di L2L e ad accesso remoto](#)
- [Cisco PIX serie 500 Security Appliance](#)
- [Cisco ASA serie 5500 Adaptive Security Appliance](#)
- [Supporto dei prodotti software Cisco PIX Firewall](#)
- [Riferimenti per i comandi di Cisco Secure PIX Firewall](#)
- [Pagina di supporto RADIUS](#)
- [Pagina di supporto per la negoziazione IPsec/i protocolli IKE](#)
- [RFC \(Requests for Comments\)](#)
- [L2TP \(Layer Two Tunnel Protocol\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)