Configurazione di L2TP over IPsec tra PC con Windows 8 e ASA con chiave già condivisa

Sommario

Introduzione

In questo documento viene descritto come configurare il protocollo L2TP (Layer 2 Tunneling Protocol) su IPsec utilizzando una chiave già condivisa tra Cisco Adaptive Security Appliance (ASA) e il client nativo di Windows 8.

L2TP over Internet Protocol Security (IPsec) consente di distribuire e amministrare una soluzione L2TP Virtual Private Network (VPN) insieme ai servizi VPN e firewall IPsec in un'unica piattaforma.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Connettività IP tra il computer client e l'appliance ASA. Per verificare la connettività, provare a eseguire il ping tra l'indirizzo IP dell'appliance ASA e l'endpoint del client e viceversa
- Verificare che le porte UDP 500 e 4500 e il protocollo Encapsulating Security Payload (ESP)

non siano bloccati in alcun punto del percorso della connessione

Restrizioni

- L2TP su IPsec supporta solo IKEv1. IKEv2 non è supportato.
- L2TP con IPsec sull'appliance ASA consente all'LNS di interagire con i client VPN nativi integrati in sistemi operativi come Windows, MAC OS X, Android e Cisco IOS. Solo L2TP con IPsec è supportato, l'L2TP nativo non è supportato sull'appliance ASA.
- La durata minima delle associazioni di protezione IPSec supportata dal client Windows è di 300 secondi. Se la durata dell'appliance ASA è impostata su un valore inferiore a 300 secondi, il client Windows la ignora e la sostituisce con una durata di 300 secondi.
- L'ASA supporta solo le autenticazioni PPP (Point-to-Point Protocol), il protocollo PAP (Password Authentication Protocol) e il protocollo CHAP (Microsoft Challenge-Handshake Authentication Protocol), versioni 1 e 2, sul database locale. EAP (Extensible Authentication Protocol) e CHAP vengono eseguiti dai server di autenticazione proxy. Pertanto, se un utente remoto appartiene a un gruppo di tunnel configurato con i comandi **authentication eap-proxy** o **authentication chap** e l'ASA è configurata per utilizzare il database locale, tale utente non può connettersi.

Tipi di autenticazione PPP supportati

Le connessioni L2TP su IPsec sull'appliance ASA supportano solo i tipi di autenticazione PPP mostrati nella tabella

Supporto server AAA e tipi di autenticazione PPP

Tipo di server AAA	Tipi di autenticazione PPP supportati
LOCALE	PAP, MSCHAPv1, MSCHAPv2
RAGGIO	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TACACS+	PAP, CHAP, MSCHAPv1
LDAP	PAP
NT	PAP
Kerberos	PAP
SDI	SDI

Caratteristiche del tipo di autenticazione PPP

Parola chiave	Tipo di autenticazione	Caratteristiche
tizio	CHAP	In risposta alla richiesta di verifica del server, il client restituisce il nome utente crittografato [richiesta più password] con un nome utente non crittografato. Questo protocollo è più sicuro del protocollo PAP, ma non crittografa i dati.
eap-proxy	EAP	Abilita il protocollo EAP che consente all'appliance di sicurezza di inoltrare il processo di autenticazione PPP a un server di autenticazione RADIUS esterno.
ms-chap-v1 **ms-chap-v2**	Microsoft CHAP, versione 1 CHAP Microsoft, versione, 2	Simile alla protezione CHAP ma più sicuro, in quanto il server archivia e confronta solo le password crittografate anziché quelle non crittografate come nella protezione CHAP. Questo protocollo genera anche una chiave per la crittografia dei dati da parte di MPPE.
pap	PAP	Passa nome utente e password non crittografati durante l'autenticazione e non è sicuro.

Componenti usati

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

- Cisco serie 5515 ASA con software versione 9.4(1)
- Client L2TP/IPSec (Windows 8)

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 8.3(1) o versioni successive.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici

Premesse

L2TP (Layer 2 Tunneling Protocol) è un protocollo di tunneling VPN che consente ai client remoti di utilizzare la rete IP pubblica per comunicare in modo sicuro con i server della rete aziendale privata. L2TP utilizza il protocollo PPP su UDP (porta 1701) per eseguire il tunnel dei dati.

Il protocollo L2TP si basa sul modello client/server. La funzione è divisa tra il server di rete L2TP (LNS) e l'Access Concentrator L2TP (LAC). In questo caso, l'LNS viene in genere eseguito su un gateway di rete, ad esempio l'ASA, mentre il LAC può essere un server di accesso alla rete (NAS) per la connessione remota o un dispositivo endpoint con un client L2TP in dotazione, ad esempio Microsoft Windows, Apple iPhone o Android.

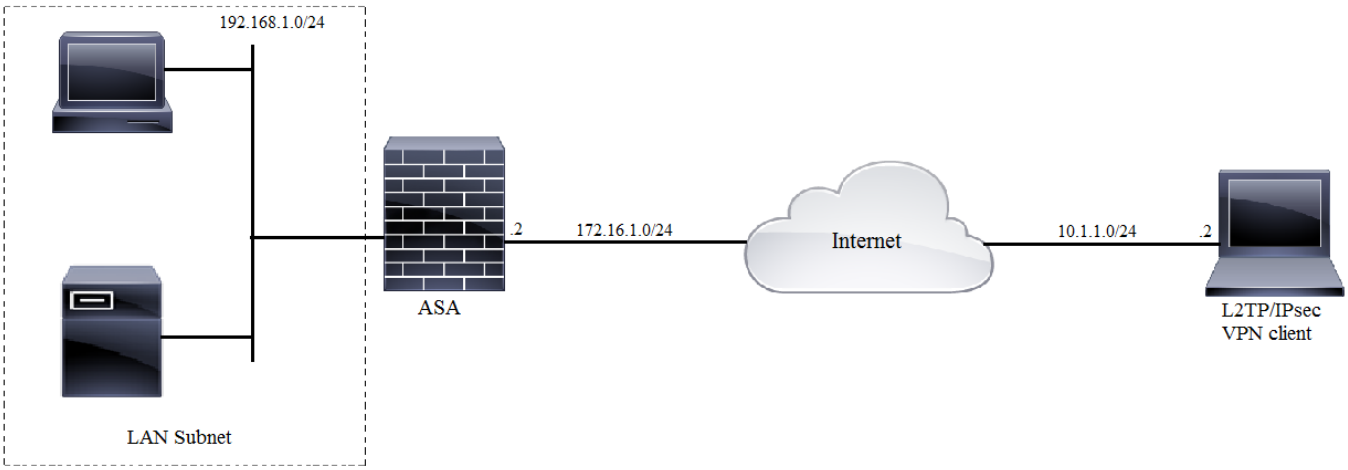
Configurazione

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 indirizzabili legalmente su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Esempio di rete

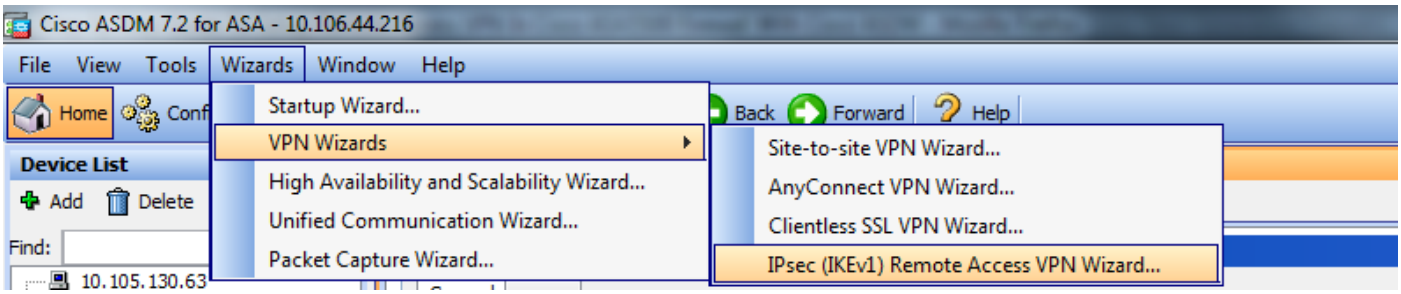


Configurazione tunnel completo

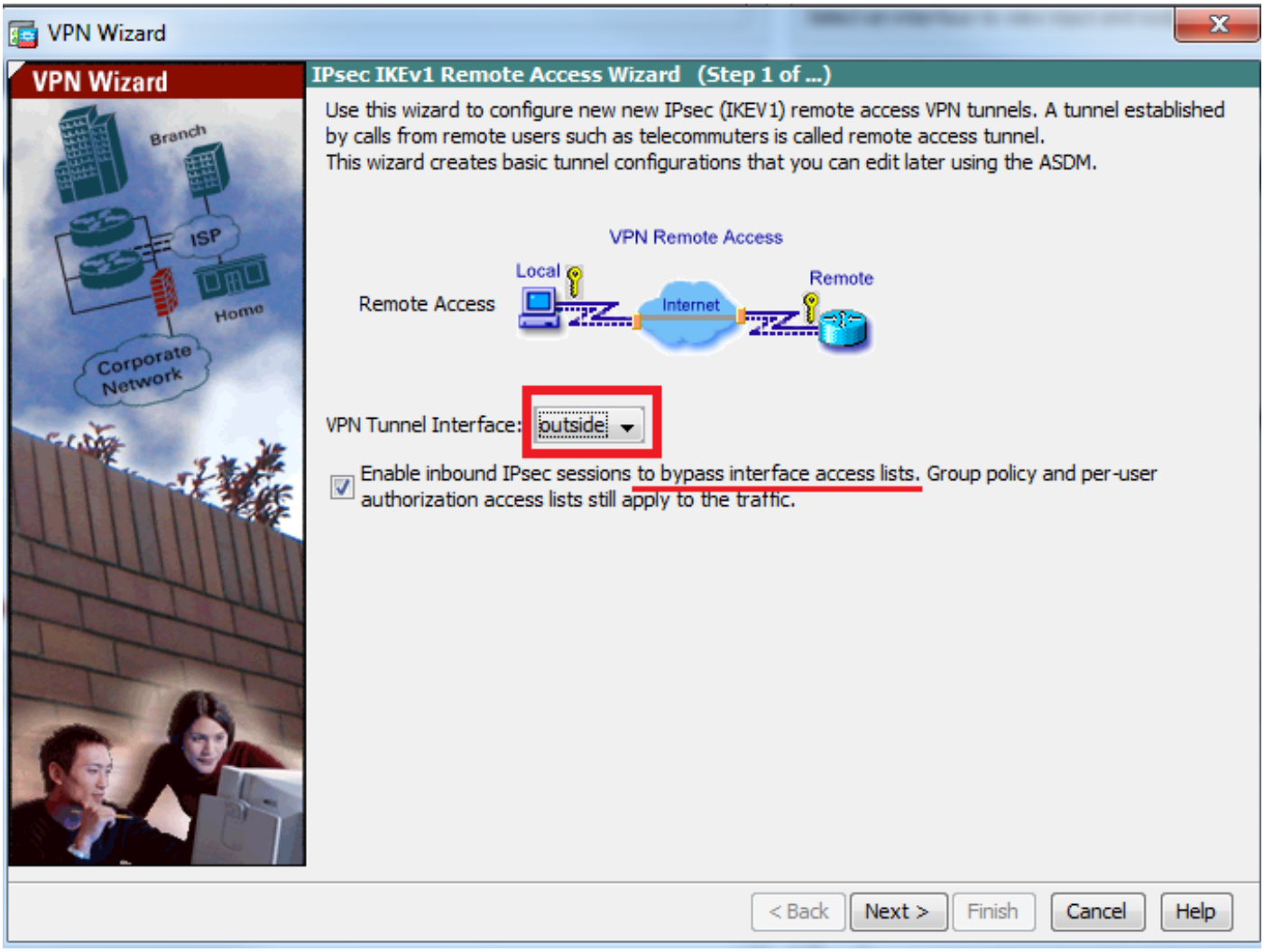
Configurazione ASA con Adaptive Security Device Manager (ASDM)

Attenersi alla seguente procedura:

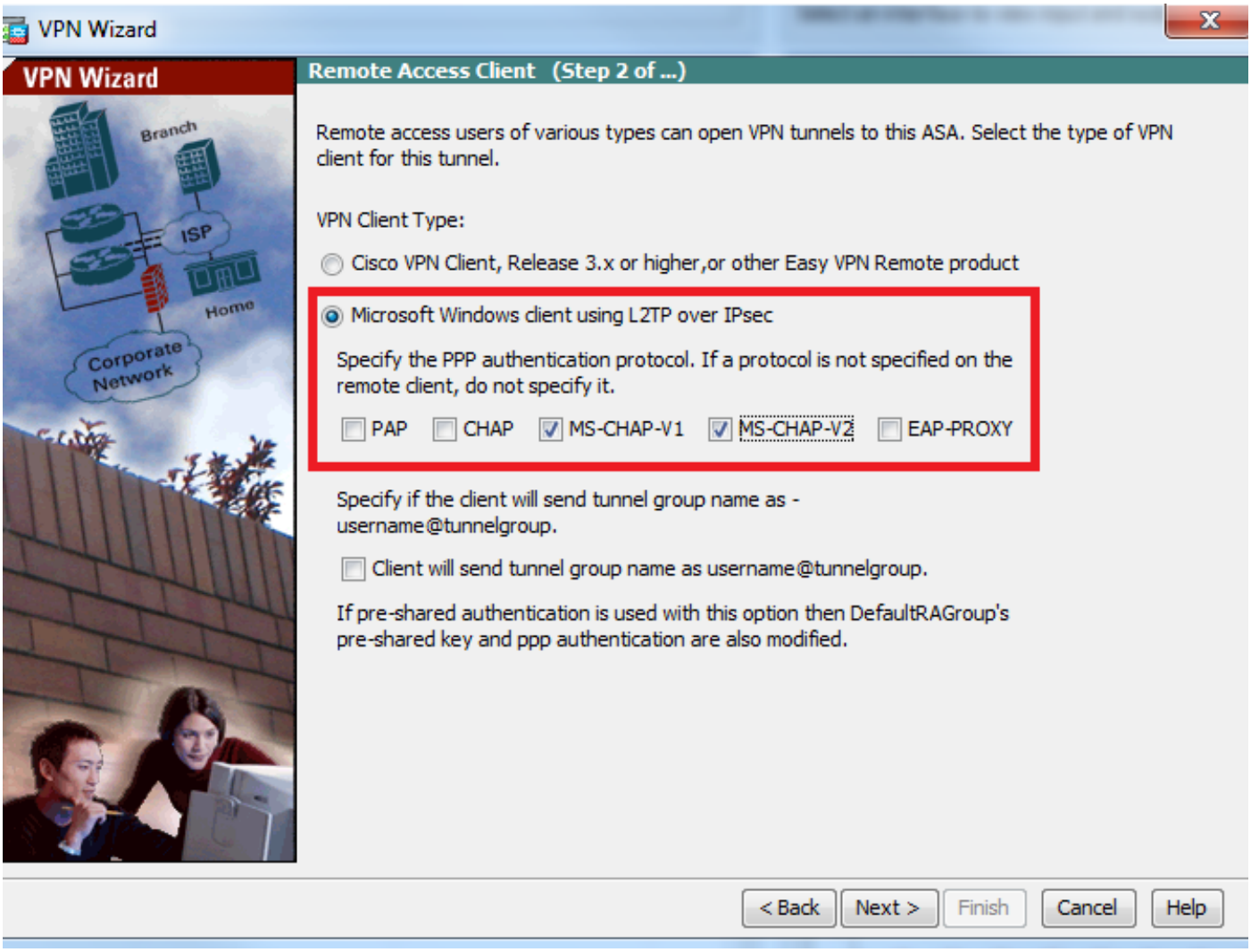
Passaggio 1. Accedere ad ASDM e selezionare **Wizards > VPN Wizard > Ipsec (IKEv1) Remote Access VPN Wizard**.



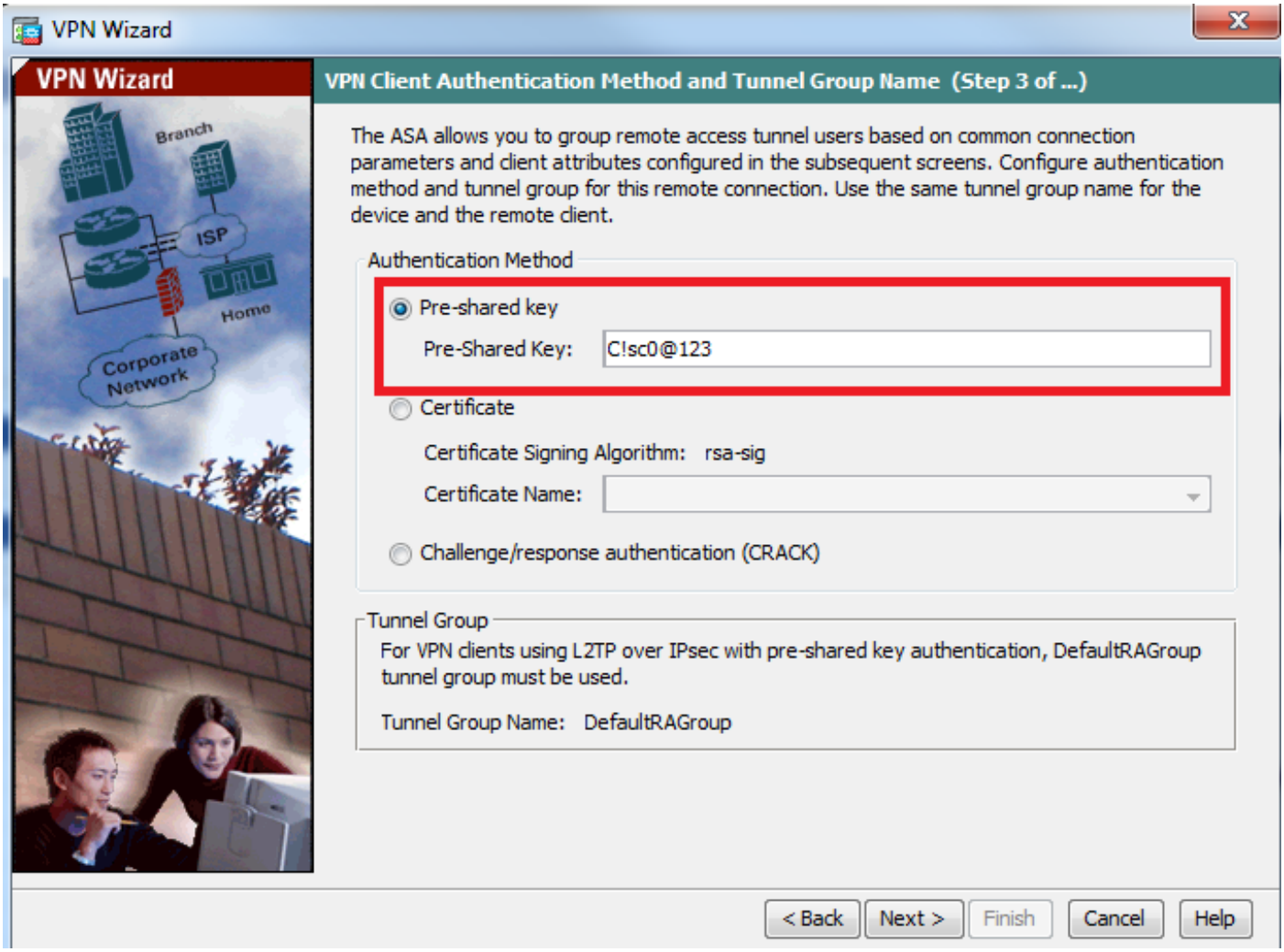
Passaggio 2. Viene visualizzata una finestra di configurazione della VPN ad accesso remoto. Dall'elenco a discesa, scegliere l'interfaccia su cui terminare il tunnel VPN. In questo esempio, l'interfaccia esterna è connessa alla WAN e quindi termina i tunnel VPN su questa interfaccia. Selezionare la casella di controllo **Abilita le sessioni IPSec in ingresso per ignorare gli elenchi degli accessi all'interfaccia. I Criteri di gruppo e gli elenchi degli accessi con autorizzazione per utente continuano ad essere applicati al traffico** controllato in modo che non sia necessario configurare il nuovo elenco degli accessi sull'interfaccia esterna per consentire ai client di accedere alle risorse interne. Fare clic su **Next** (Avanti).



Passaggio 3. Come mostrato in questa immagine, scegliere il tipo di client come **client Microsoft Windows utilizzando L2TP su IPSec** e **MS-CHAP-V1** e **MS-CHAP-V2** come protocollo di autenticazione PPP poiché PAP non è sicuro e altri tipi di autenticazione non sono supportati con il database LOCALE come server di autenticazione e fare clic su **Avanti**.

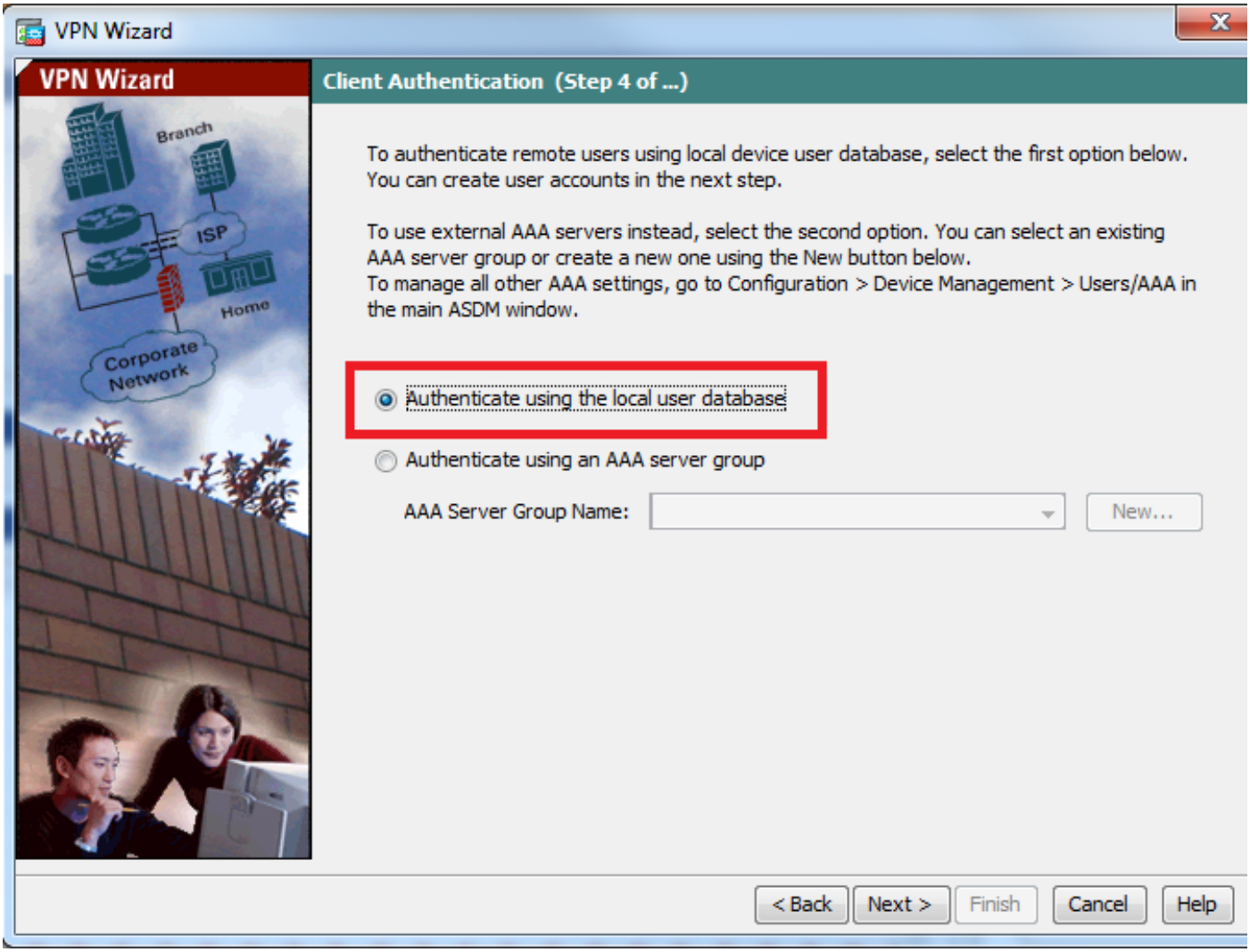


Passaggio 4. Scegliere il metodo di autenticazione come **Preshared-key** e digitare la pre-shared-key che deve essere uguale anche sul lato client, quindi fare clic su **Avanti**, come mostrato nell'immagine.

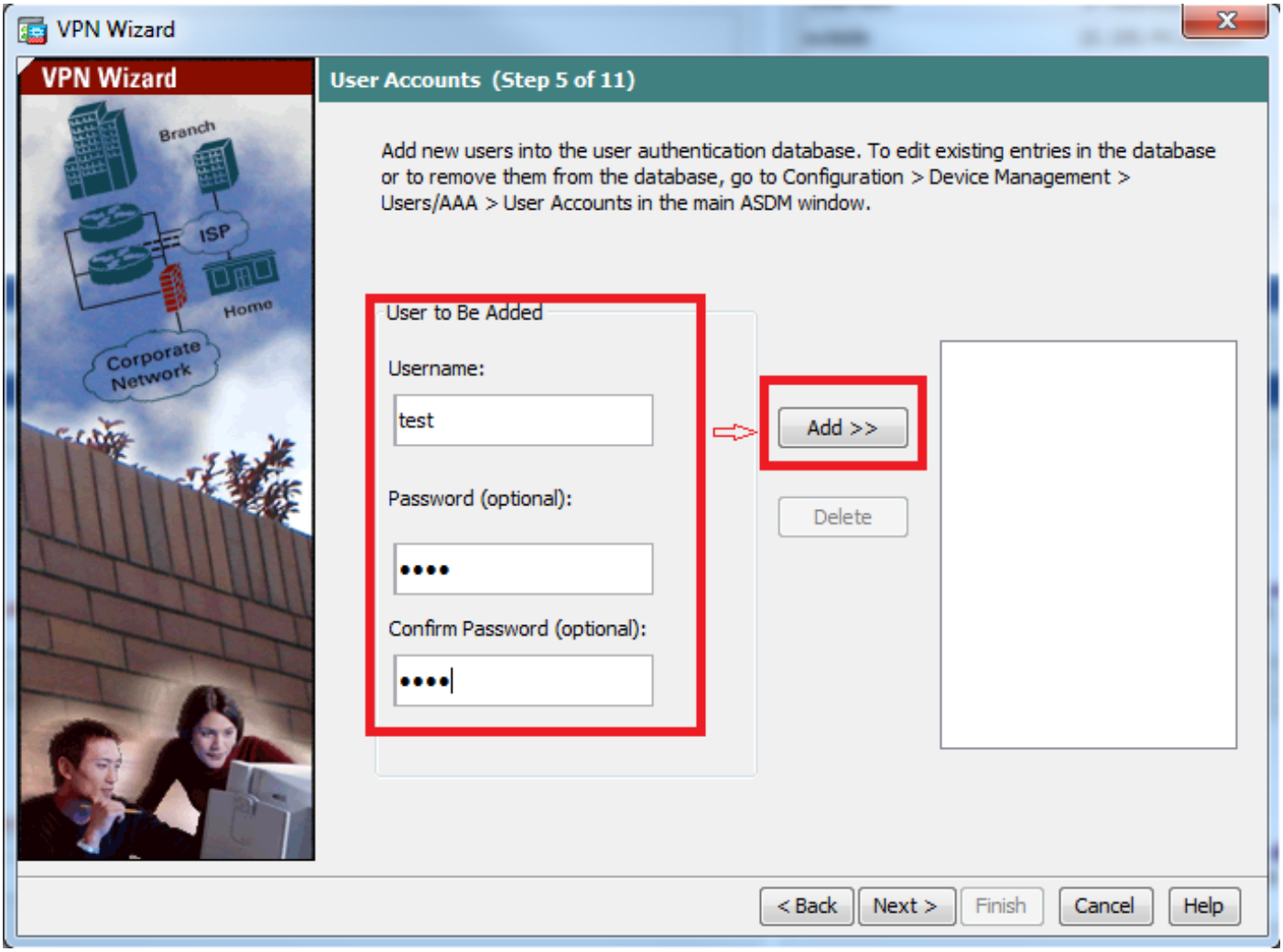


Passaggio 5. Specificare un metodo per autenticare gli utenti che tentano connessioni L2TP su IPSec. È possibile utilizzare un server di autenticazione AAA esterno o il relativo database locale. Scegliere **Autentica utilizzando il database locale** se si desidera autenticare i client sul database locale dell'appliance ASA e fare clic su **Avanti.**

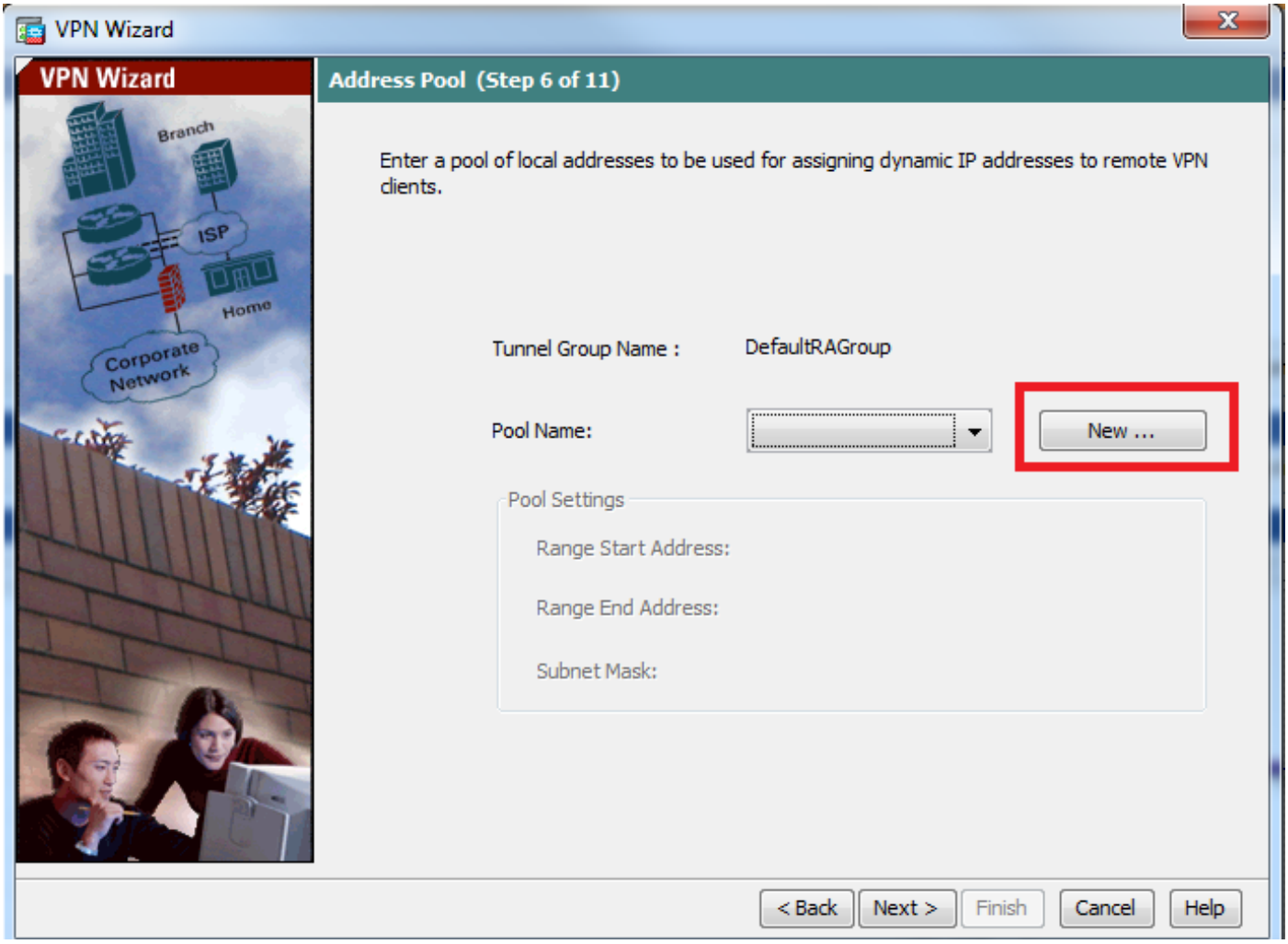
> **Nota:** Per autenticare gli utenti che usano un server AAA esterno, consultare il documento sulla configurazione dell'autenticazione RADIUS per gli utenti VPN.



Passaggio 6. Per aggiungere nuovi utenti al database locale per l'autenticazione degli utenti, immettere il nome utente e la password, quindi fare clic su **AGGIUNGI** oppure è possibile utilizzare gli account utente esistenti nel database, come mostrato nell'immagine. Fare clic su **Next (Avanti).**

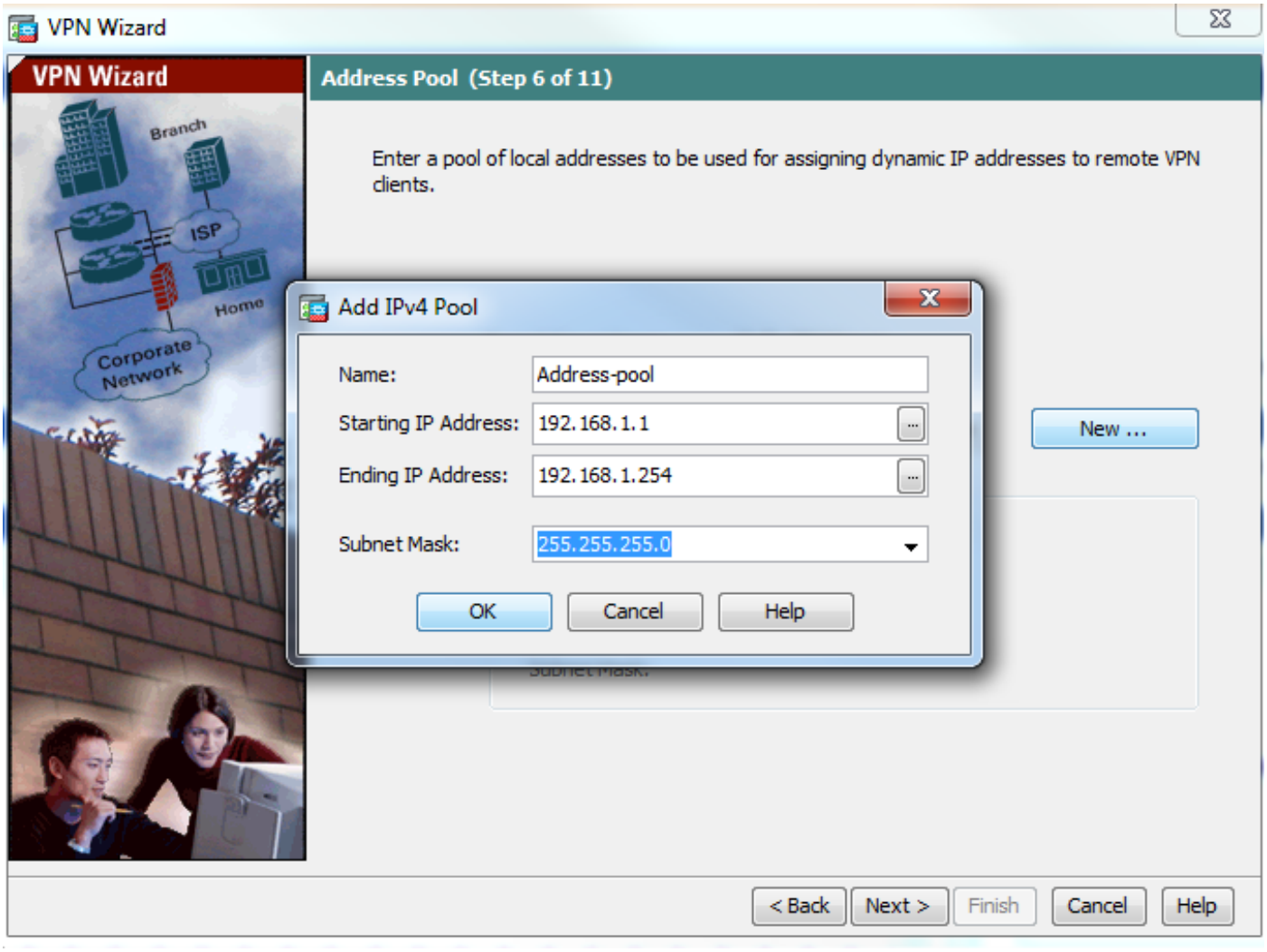


Passaggio 7. Dall'elenco a discesa, scegliere il pool di indirizzi da utilizzare per assegnare l'indirizzo IP ai client. Per creare un nuovo pool di indirizzi, fare clic su **Nuovo,** come mostrato nell'immagine.

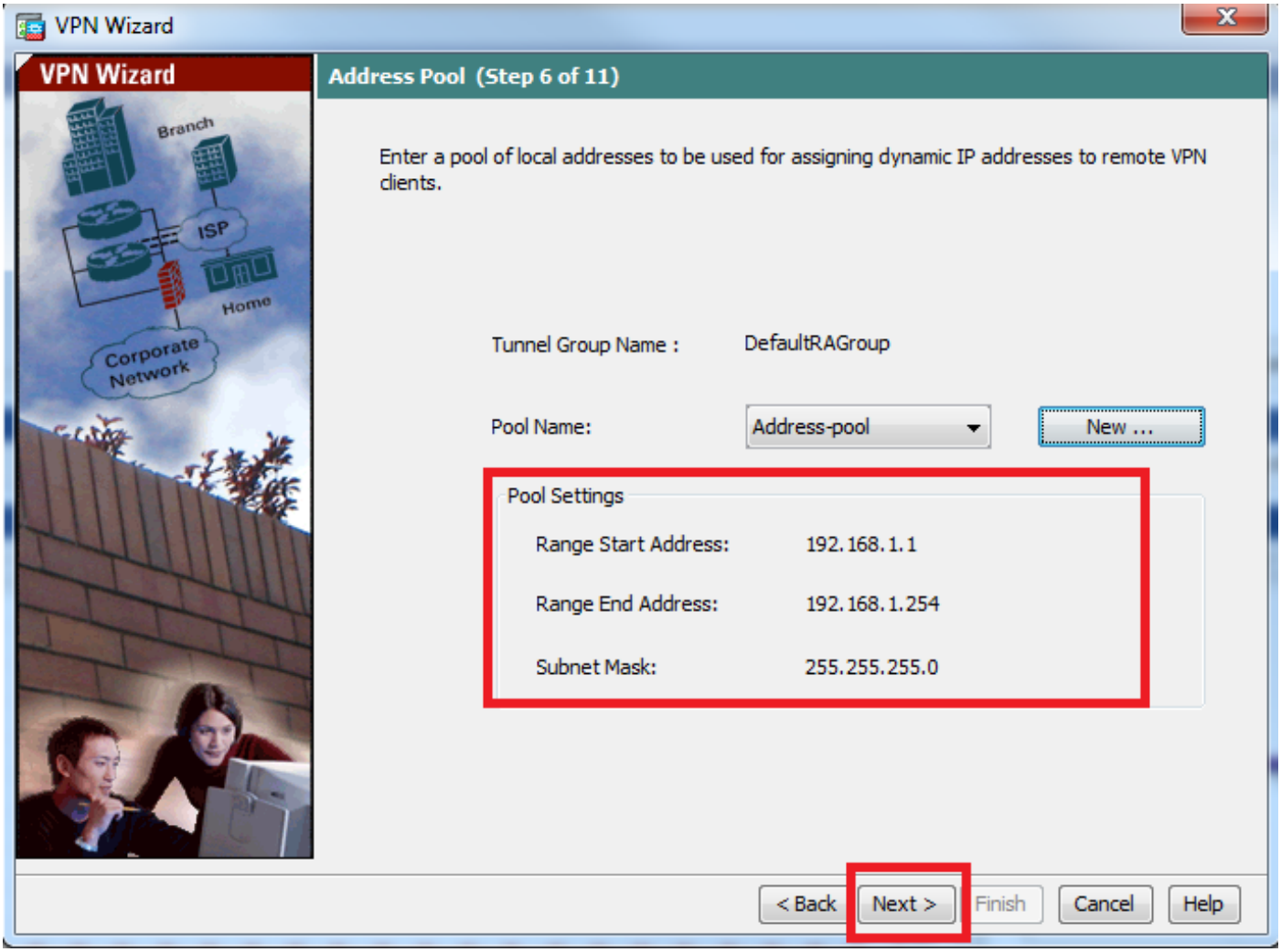


Passaggio 8. Viene visualizzata la finestra di dialogo **Aggiungi pool IPv4**.

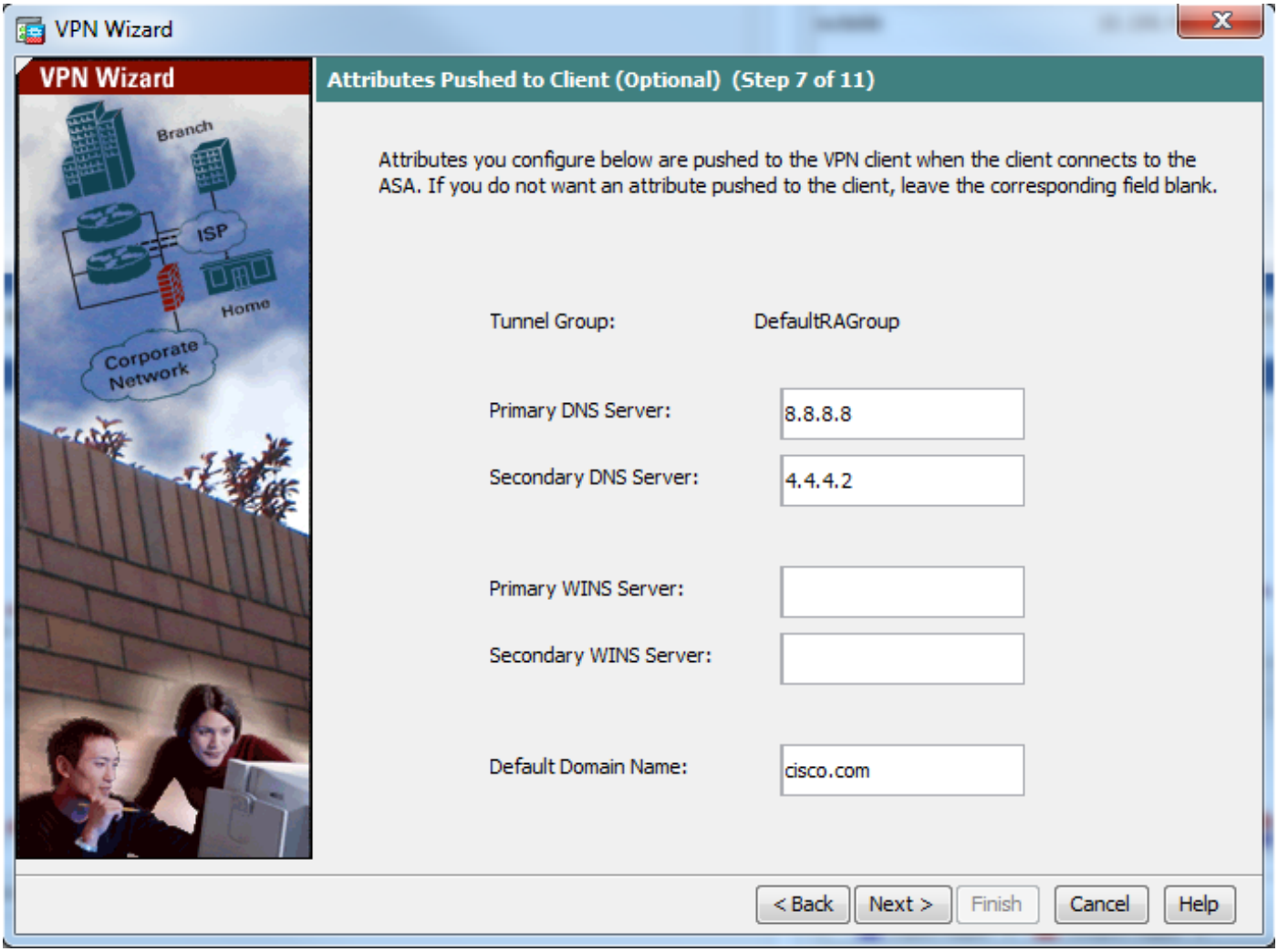
1. Immettere il nome del nuovo pool di indirizzi IP.
2. Immettere gli indirizzi IP iniziale e finale.
3. Immettere la subnet mask e fare clic su **OK**.



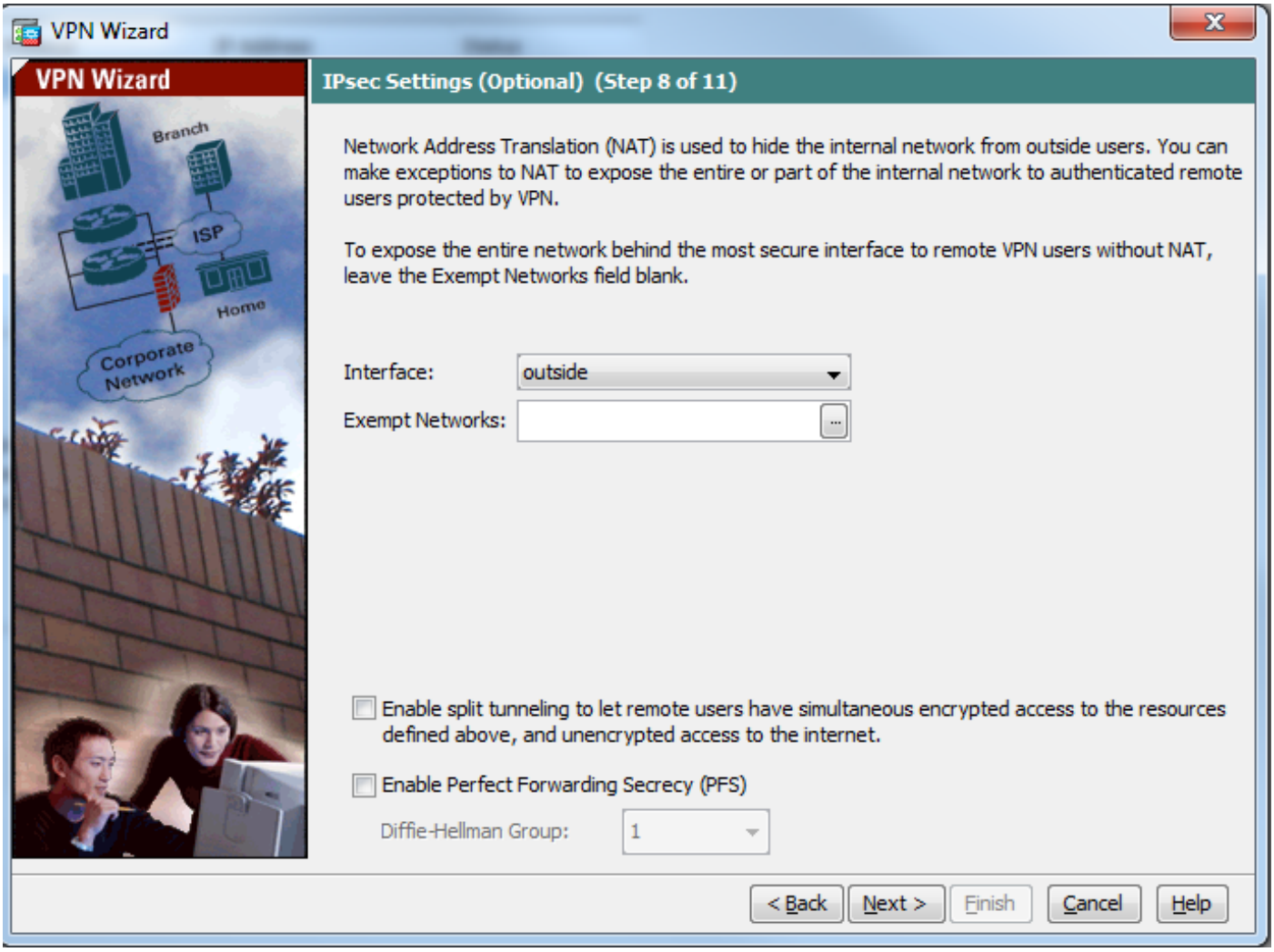
Passaggio 9. Verificare le impostazioni del pool e fare clic su **Avanti.**



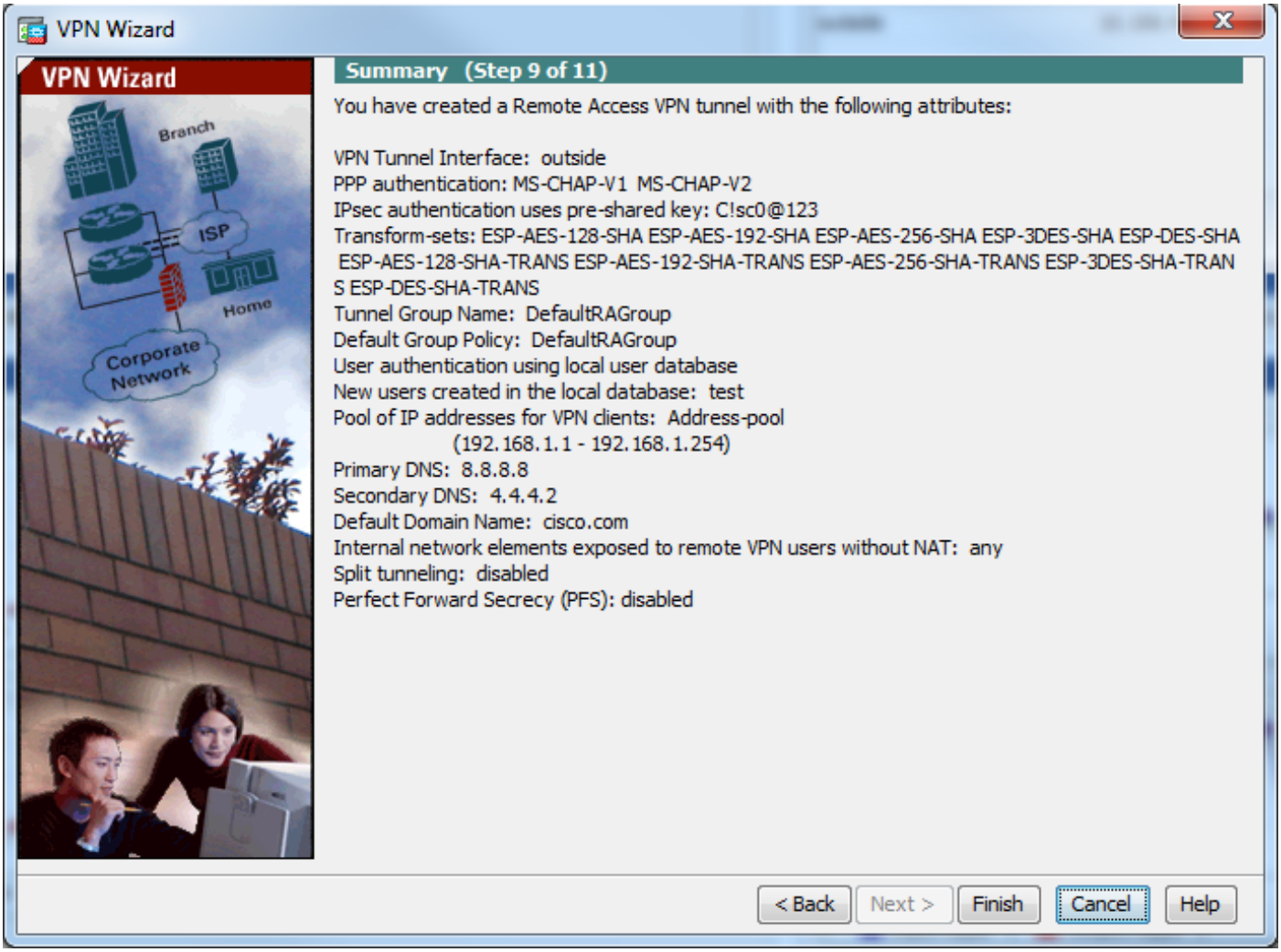
Passaggio 10. Configurare gli attributi da inviare ai client o lasciarli vuoti e fare clic su **Avanti.**



Passaggio 11: Verificare che la casella di controllo **Abilita PFS (Perfect Forwarding Secrecy)** sia deselezionata, in quanto alcune piattaforme client non supportano questa funzione. **Abilitare il tunneling suddiviso per consentire agli utenti remoti di accedere contemporaneamente in modalità crittografata alle risorse definite in precedenza e** deselezionare **l'accesso non crittografato alla** casella **Internet.** Ciò significa che è abilitato il tunneling completo, in cui tutto il traffico (incluso il traffico Internet) dal computer client verrà inviato all'ASA sul tunnel VPN. Fare clic su **Next (Avanti).**



Passaggio 12. Esaminare le informazioni di riepilogo e quindi fare clic su **Fine.**



Configurazione di ASA con CLI

Passaggio 1. Configurare i parametri dei criteri IKE fase 1.

Questo criterio viene utilizzato per proteggere il controllo del traffico tra peer, ovvero per proteggere la chiave già condivisa e le negoziazioni della fase 2

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
```

Passaggio 2. Configurare Transform-set.

Contiene i parametri dei criteri IKE fase 2 utilizzati per proteggere il traffico di dati. Poiché il client Windows L2TP/IPsec utilizza la modalità di trasporto IPSec, impostare la modalità su Trasporto. Il valore predefinito è la modalità tunnel

```
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport
```

Passaggio 3. Configurare la mappa dinamica.

Poiché i client Windows ottengono l'indirizzo IP dinamico dall'ISP o dal server DHCP locale (ad

esempio, il modem), l'ASA non è in grado di rilevare l'indirizzo IP del peer e ciò crea un problema nella configurazione di un peer statico sull'estremità ASA. È quindi necessario avvicinarsi alla configurazione della crittografia dinamica, in cui tutti i parametri non sono necessariamente definiti e i parametri mancanti vengono successivamente appresi in modo dinamico, come risultato della negoziazione IPSec da parte del client.

```
ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-
SHA
```

Passaggio 4. Associare la mappa dinamica alla mappa crittografica statica, applicare la mappa crittografica e abilitare IKEv1 sull'interfaccia esterna

Impossibile applicare la mappa crittografica dinamica a un'interfaccia. Associarla quindi alla mappa crittografica statica. I set di crittografia dinamici devono essere le mappe crittografiche con la priorità più bassa nel set di mappe crittografiche (ossia, devono avere i numeri di sequenza più alti) in modo che l'ASA valuti per prima le altre mappe crittografiche. Esamina il set di mappe crittografiche dinamiche solo quando le altre voci (statiche) della mappa non corrispondono.

```
ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
ciscoasa(config)#crypto map outside_map interface outside
ciscoasa(config)#crypto ikev1 enable outside
```

Passaggio 5. Creazione del pool di indirizzi IP

Creare un pool di indirizzi da cui gli indirizzi IP vengono assegnati dinamicamente ai client VPN remoti. Ignorare questo passaggio per usare il pool esistente sull'appliance ASA.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
```

Passaggio 6. Configurare i criteri di gruppo

Identificare i Criteri di gruppo come interni, ovvero gli attributi vengono estratti dal database locale.

```
ciscoasa(config)#group-policy L2TP-VPN internal
```

> **Nota:** Le connessioni L2TP/IPsec possono essere configurate con Criteri di gruppo predefiniti (DfltGrpPolicy) o definiti dall'utente. In entrambi i casi, è necessario configurare i Criteri di gruppo per l'utilizzo del protocollo di tunneling L2TP/IPsec. configurare l2tp-ipsec sull'attributo del protocollo VPN nei criteri di gruppo predefiniti, che verranno ereditati dai criteri di gruppo definiti dall'utente se l'attributo vpn-protocol non è configurato su di esso.

Configurare gli attributi come il protocollo del tunnel vpn (nel nostro caso, l2tp-ipsec), il nome di dominio, l'indirizzo IP dei server DNS e WINS e i nuovi account utente

```
ciscoasa(config)#group-policy L2TP-VPN attributes
ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2
ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec
ciscoasa(config-group-policy)#default-domain value cisco.com
```

Configurare nomi utente e password sul dispositivo, oltre a usare il server AAA. Se l'utente è un client L2TP che utilizza Microsoft CHAP versione 1 o versione 2 e l'appliance ASA è configurata per l'autenticazione sul database locale, è necessario includere la parola chiave mschap. Ad esempio, username <username> password <password> mschap.

```
ciscoasa(config-group-policy)# username test password test mschap
```

Passaggio 7. Configurare il gruppo di tunnel

Creare un gruppo di tunnel con il comando **tunnel-group** e specificare il nome del pool di indirizzi locale utilizzato per allocare l'indirizzo IP al client. Se il metodo di autenticazione è pre-shared-key, il nome del gruppo di tunnel deve essere DefaultRAGroup in quanto il client non dispone di un'opzione per specificare il gruppo di tunnel e pertanto viene eseguito solo sul gruppo di tunnel predefinito. Associare i criteri di gruppo a tunnel-group utilizzando il comando default-group-policy

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

> **Nota:** È necessario configurare il profilo di connessione predefinito (gruppo di tunnel) DefaultRAGroup se viene eseguita l'autenticazione basata su chiave già condivisa. Se viene eseguita l'autenticazione basata sui certificati, è possibile scegliere un profilo di connessione definito dall'utente in base agli identificativi dei certificati

Per impostare la chiave già condivisa, usare il comando **tunnel-group ipsec-attributes** per accedere alla modalità di configurazione dell'attributo ipsec.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)#  ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

Configurare il protocollo di autenticazione PPP con il comando **authentication type** dalla modalità ppp-attributes del gruppo di tunnel. Disabilitare la protezione CHAP che è abilitata per impostazione predefinita perché non è supportata se il server AAA è configurato come database locale.

```
ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes
ciscoasa(config-ppp)#no authentication chap
ciscoasa(config-ppp)#authentication ms-chap-v2
ciscoasa(config-ppp)#exit
```

Passaggio 8. Configurare l'esenzione NAT

Configurare l'esenzione NAT in modo che i client possano accedere alle risorse interne connesse alle interfacce interne (in questo esempio, le risorse interne sono connesse all'interfaccia interna).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
```

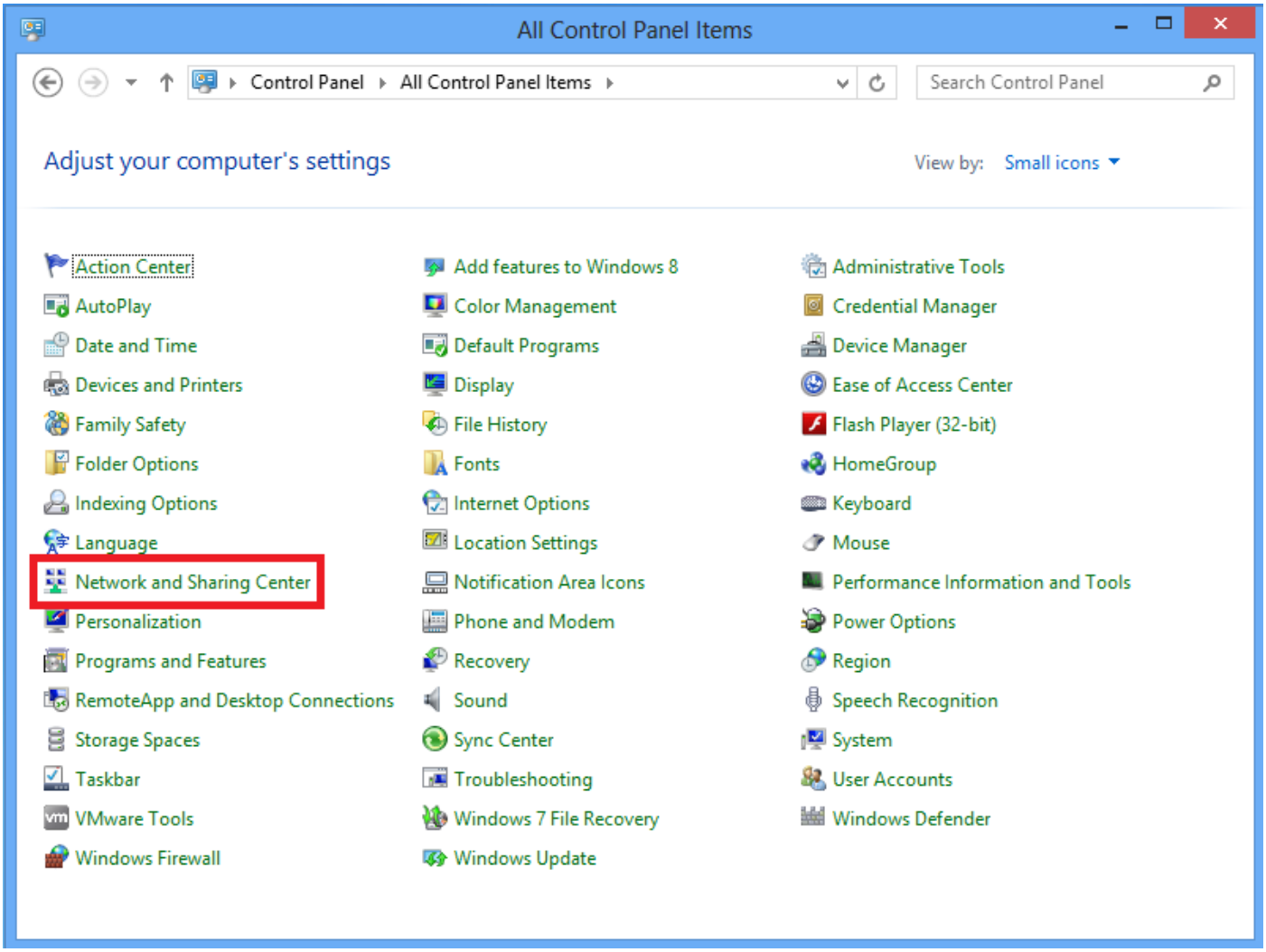
Completa configurazione di esempio

```
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
exit
```

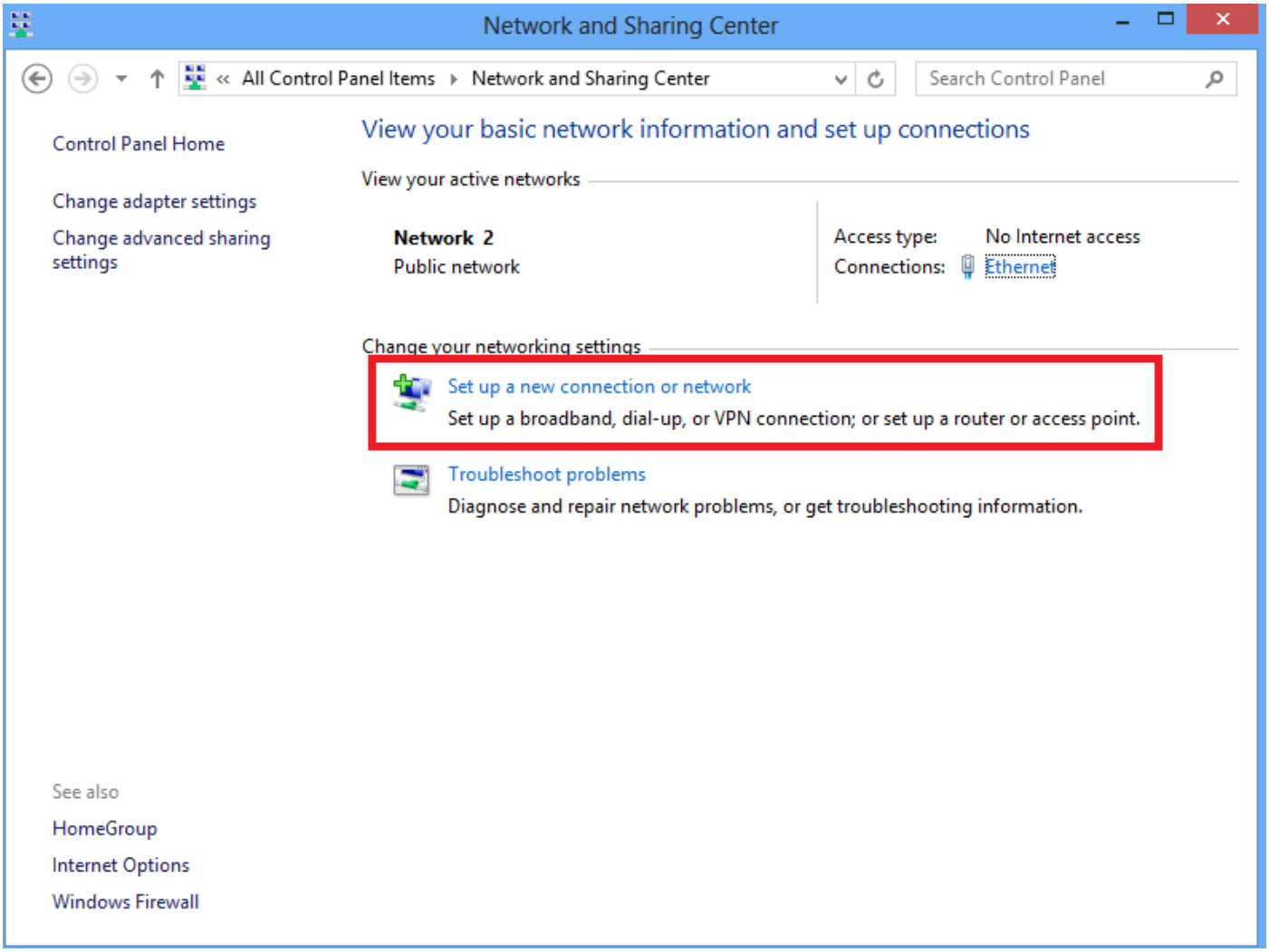
```
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport

crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
crypto ikev1 enable outside

ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0

group-policy L2TP-VPN internal
group-policy L2TP-VPN attributes
vpn-tunnel-protocol l2tp-ipsec
default-domain value cisco.com
username test password test mschap
exit

tunnel-group DefaultRAGroup general-attributes
address-pool Address-pool
default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

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

object network L2TP-Pool
subnet 192.168.1.0 255.255.255.0
exit
nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup
```

Configurazione client Windows 8 L2TP/IPsec

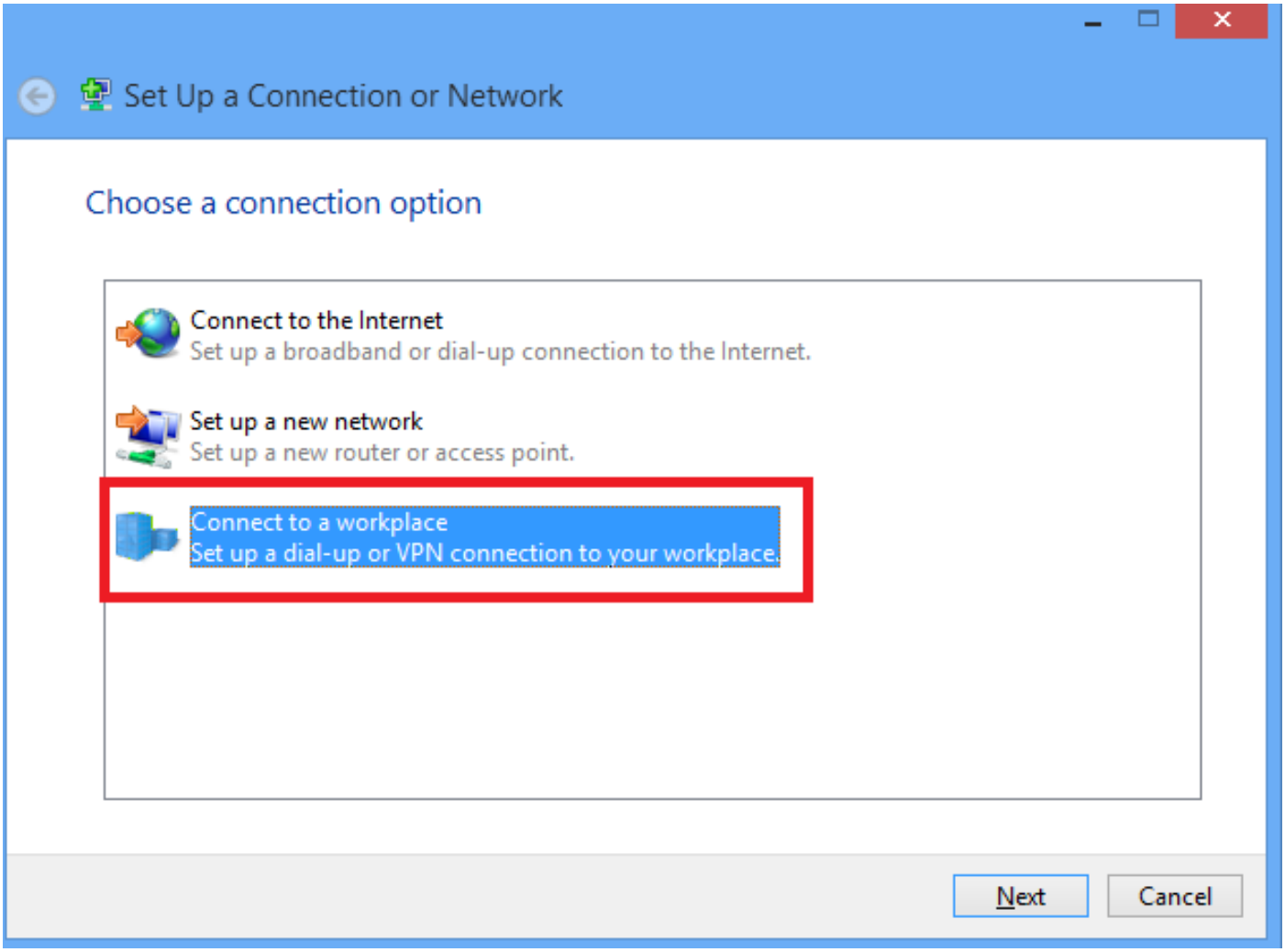
1. Aprire il Pannello di controllo e selezionare Centro connessioni di rete e condivisione.



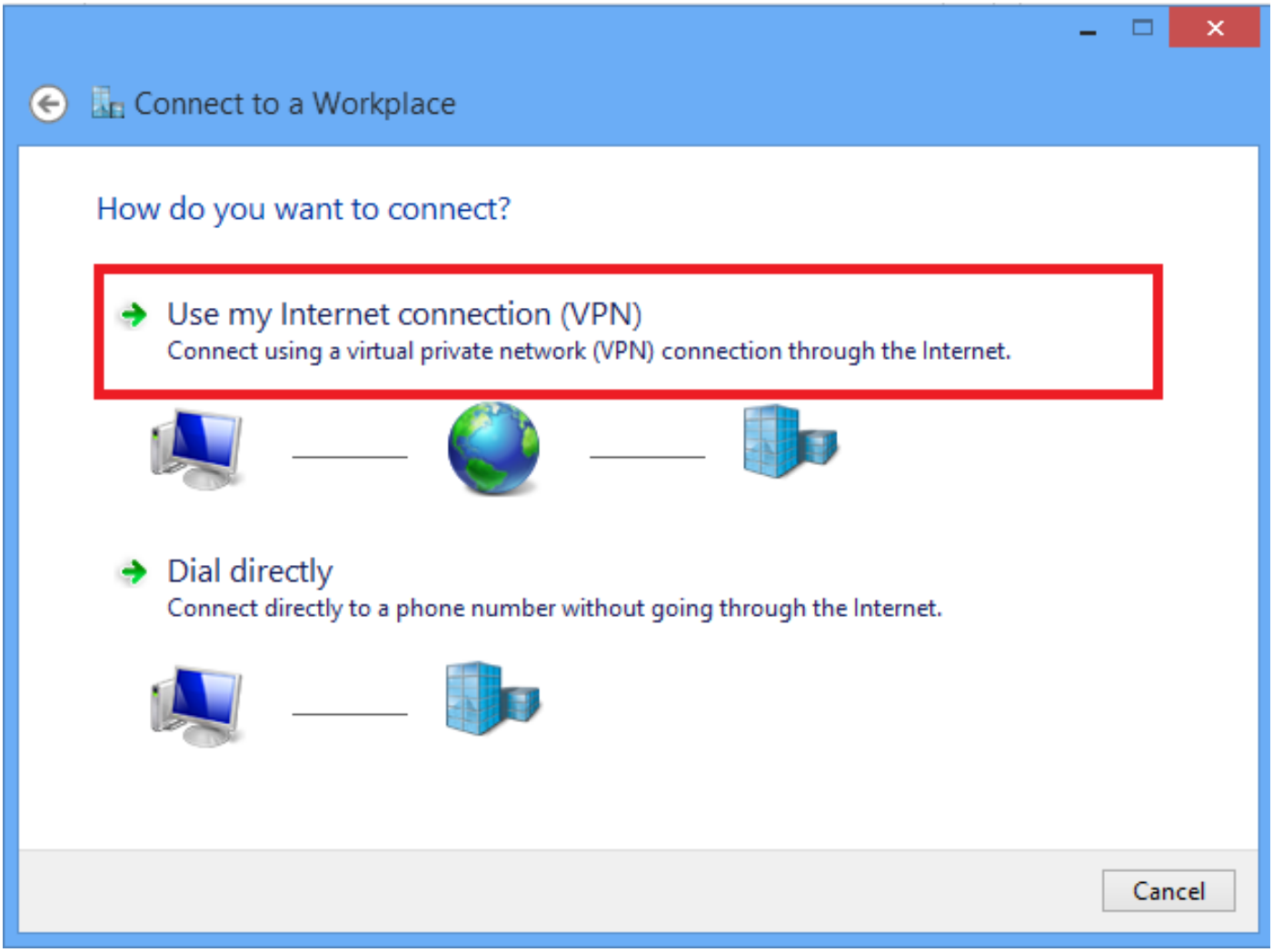
2. Scegliere **Configura nuova connessione o** opzione **di rete**.



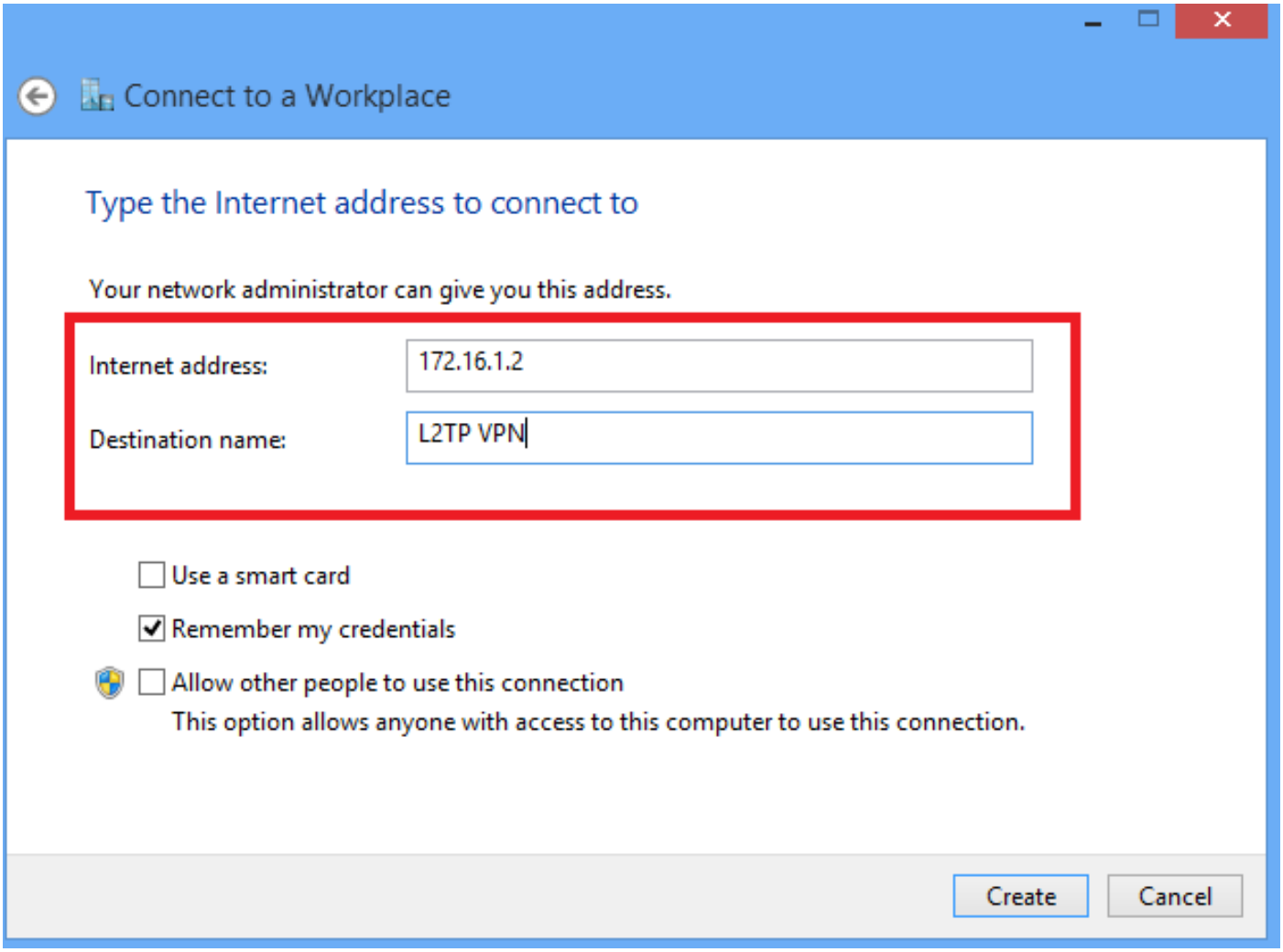
3. Scegliere **Connetti a una rete aziendale** e fare clic su **Avanti.**



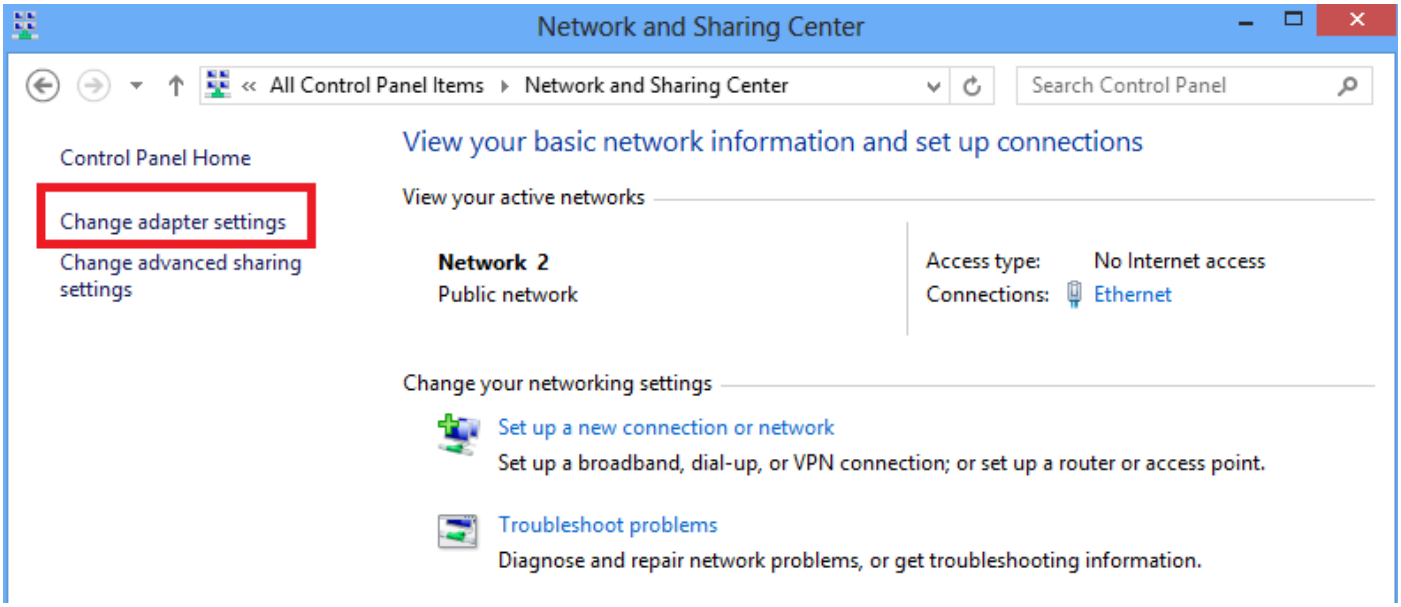
4. Fare clic sull'opzione **Usa connessione Internet (VPN)**.



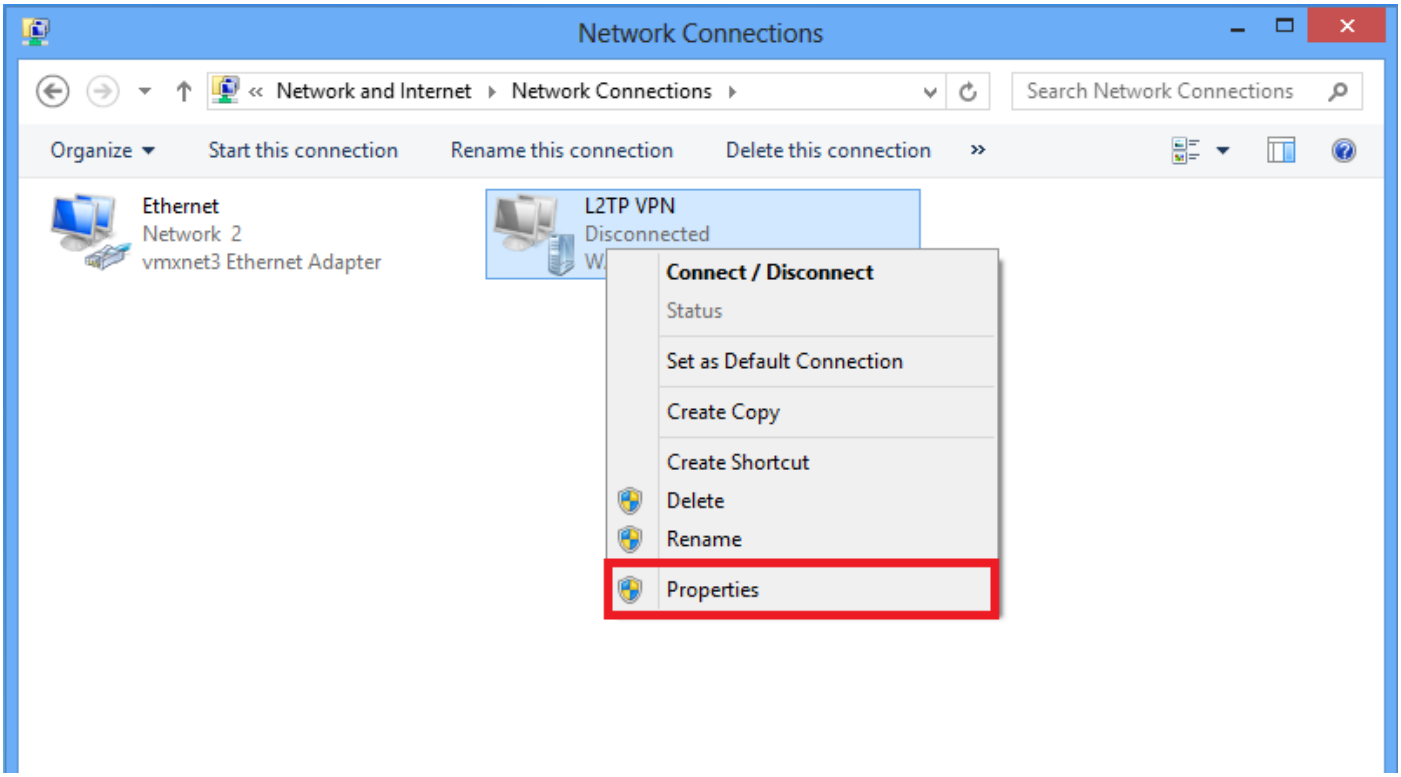
5. Immettere l'indirizzo IP dell'interfaccia WAN o dell'FQDN dell'ASA e un nome qualsiasi per la scheda VPN che sia significativo a livello locale, quindi fare clic su **Crea.**



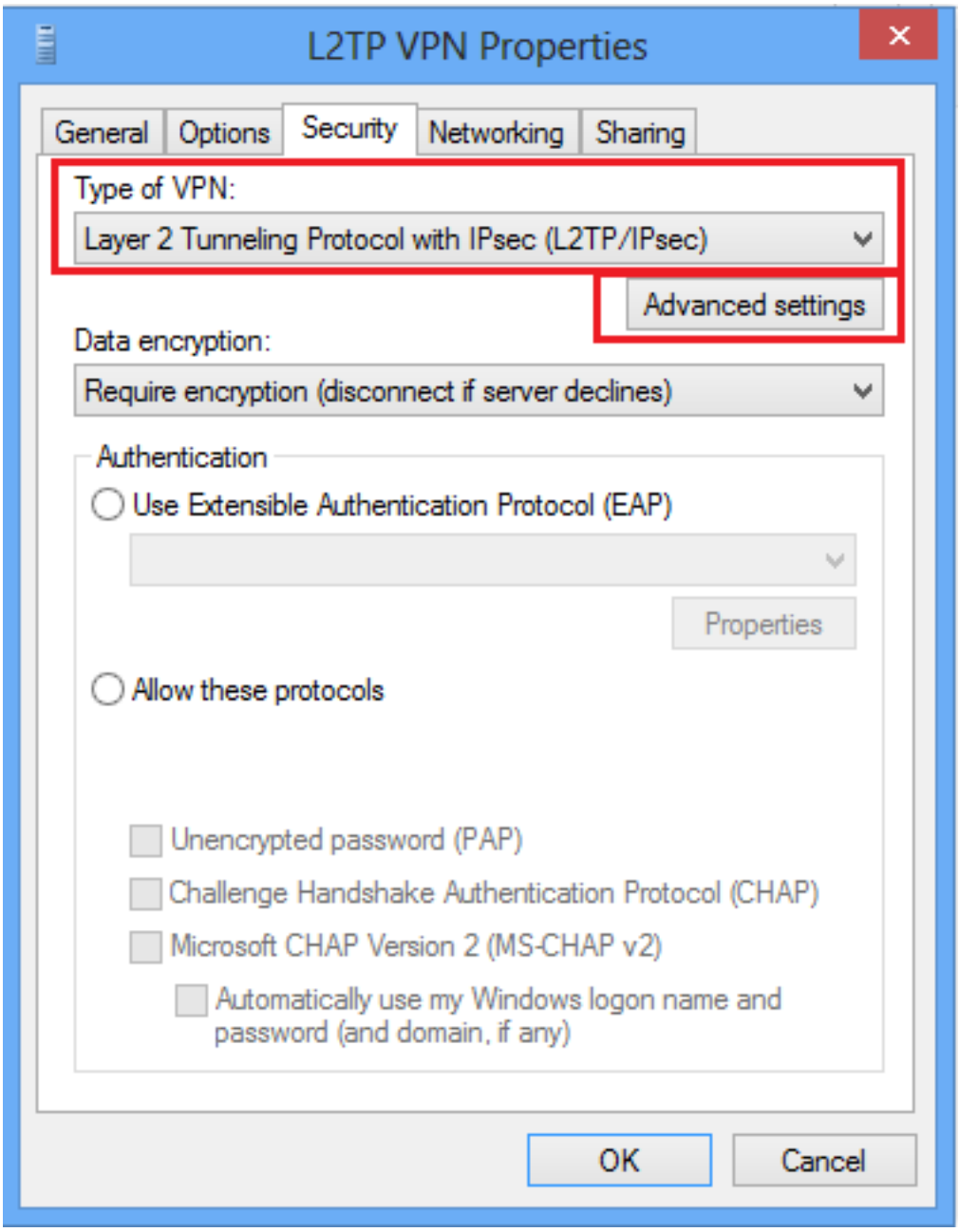
6. In Centro connessioni di rete e condivisione scegliere l'opzione **Modifica impostazioni scheda** nel riquadro sinistro della finestra.



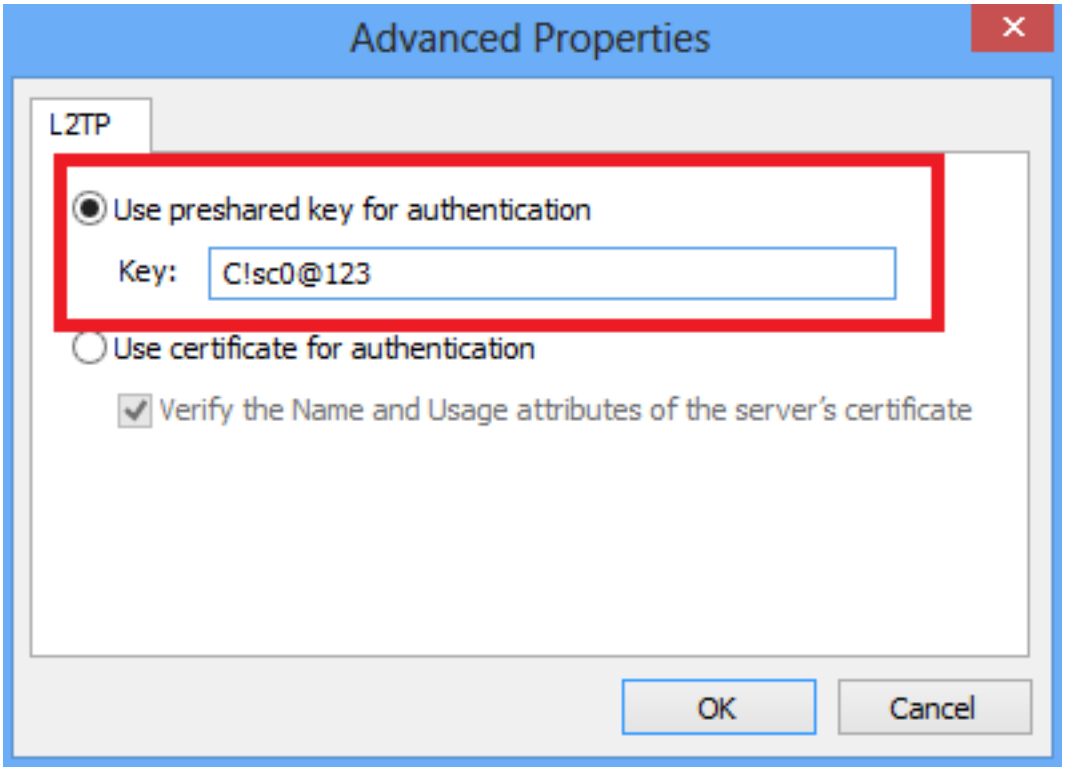
7. Fare clic con il pulsante destro del mouse sulla scheda creata di recente per L2TP VPN e scegliere **Proprietà.**



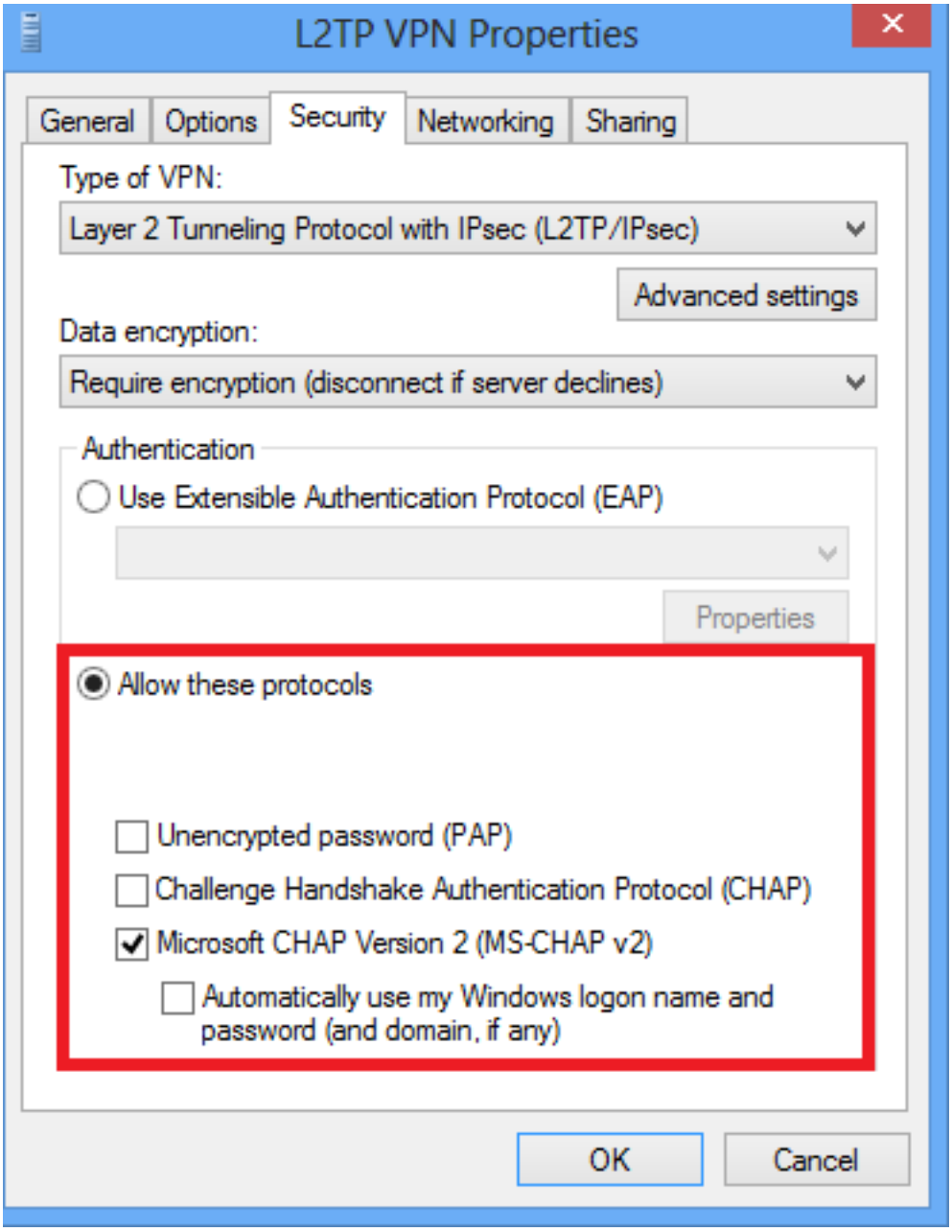
8. Passare alla scheda **Sicurezza**, scegliere il Tipo di VPN come **Layer 2 Tunneling Protocol con IPsec (L2TP/IPsec)** e quindi fare clic su **Impostazioni avanzate.**



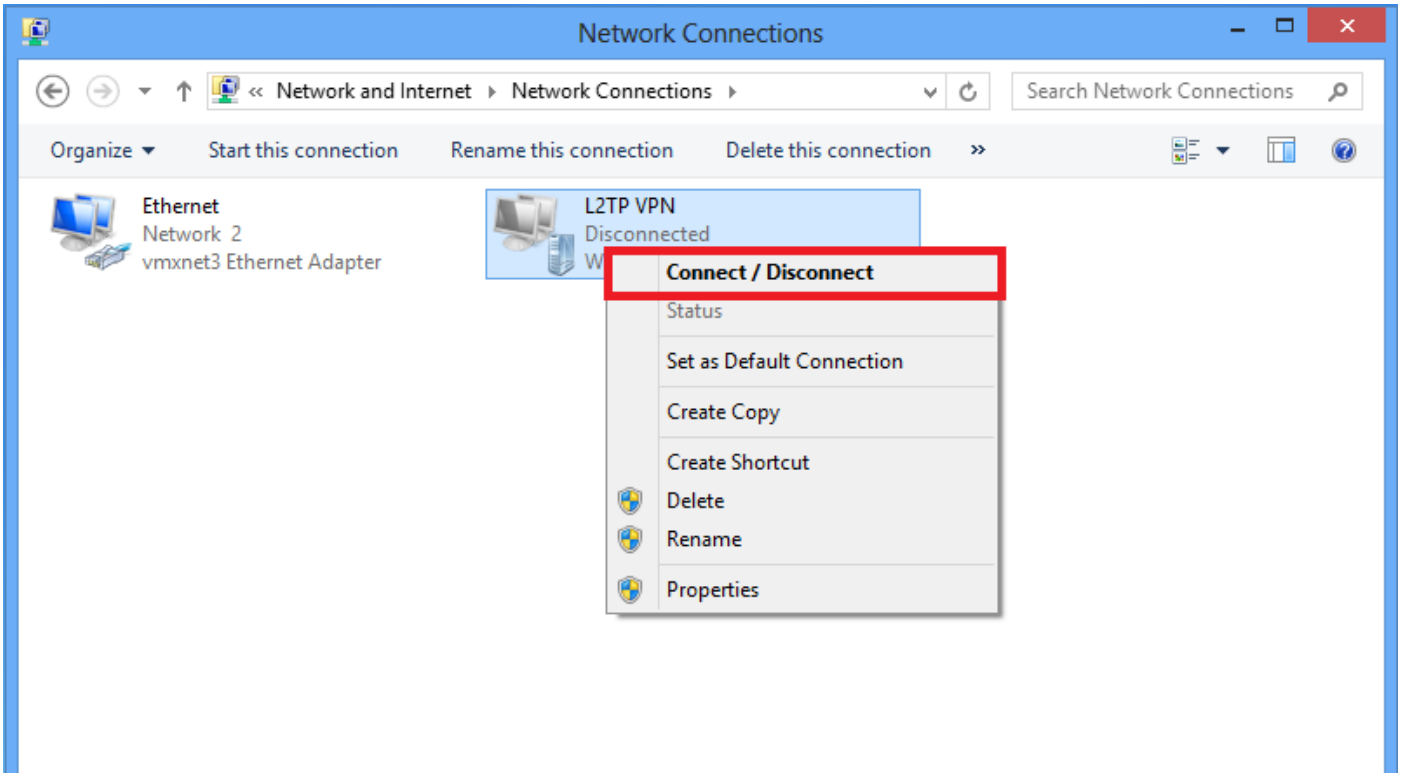
9. Immettere la chiave già condivisa indicata nel gruppo di tunnel **DefaultRAGroup** e fare clic su **OK**. Nell'esempio, la chiave già condivisa è C!sc0@123.



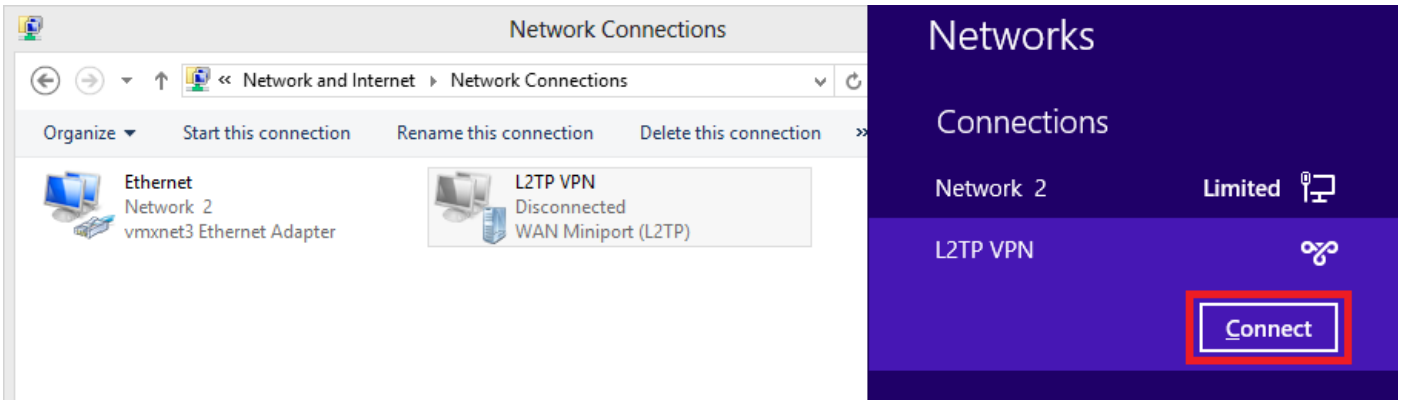
10. Scegliere il metodo di autenticazione come Consenti questi protocolli e assicurarsi che la casella di controllo "**Microsoft CHAP versione 2 (MS-CHAP v2)** sia selezionata e fare clic su **OK**.



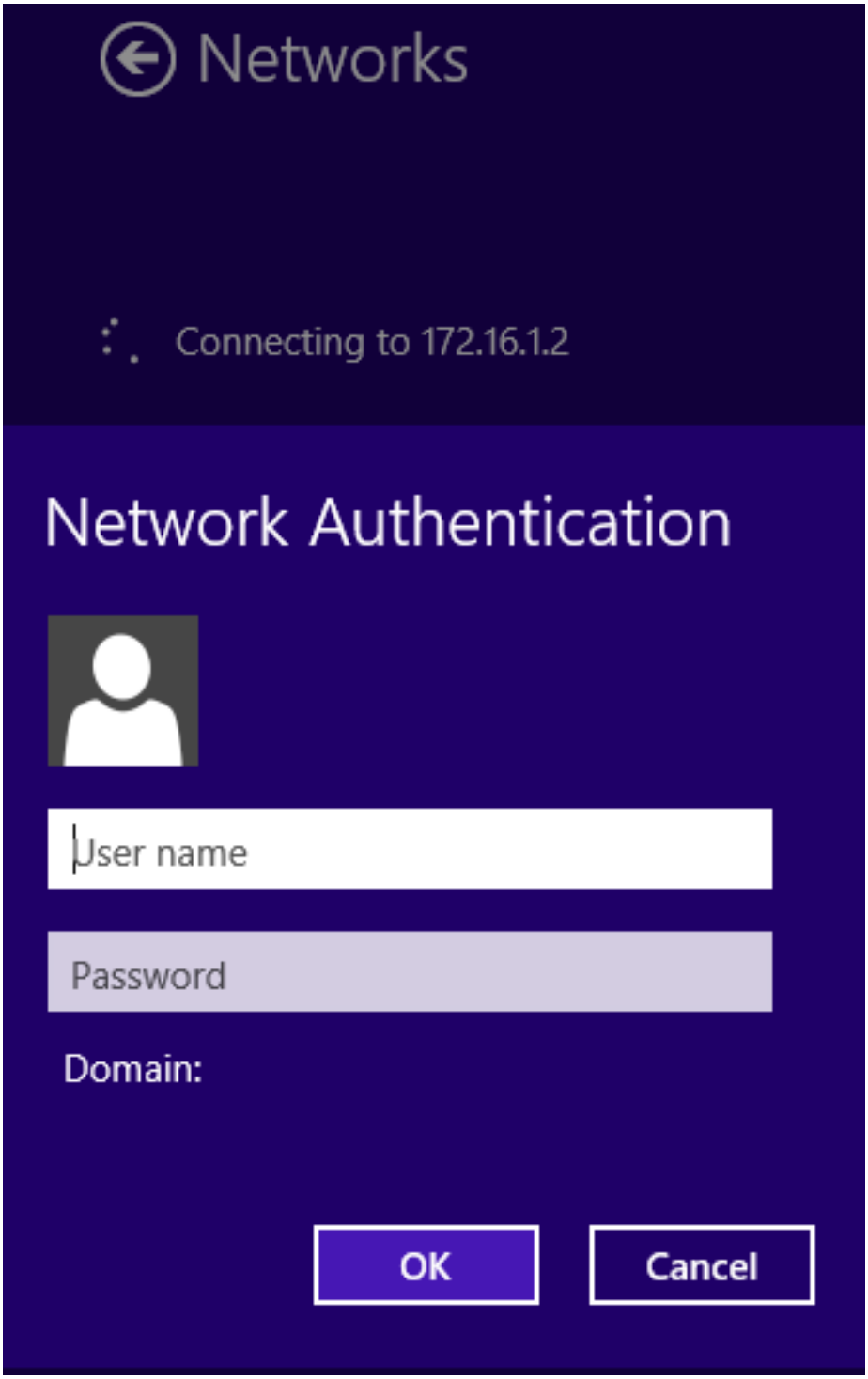
11. In Connessioni di rete, fare clic con il pulsante destro del mouse sulla scheda VPN L2TP e scegliere **Connetti/Disconnetti.**



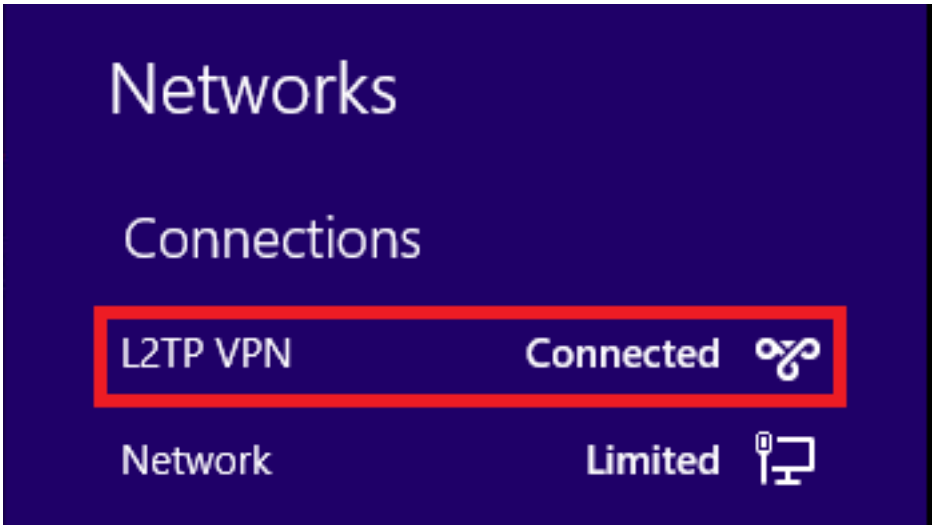
12. Verrà visualizzata l'icona Reti e fare clic su **Connetti** sulla connessione VPN L2TP.



13. Immettere le credenziali utente e fare clic su **OK**.



Se i parametri richiesti vengono associati su entrambe le estremità, verrà stabilita la connessione L2TP/IPsec.



Configurazione tunnel suddiviso

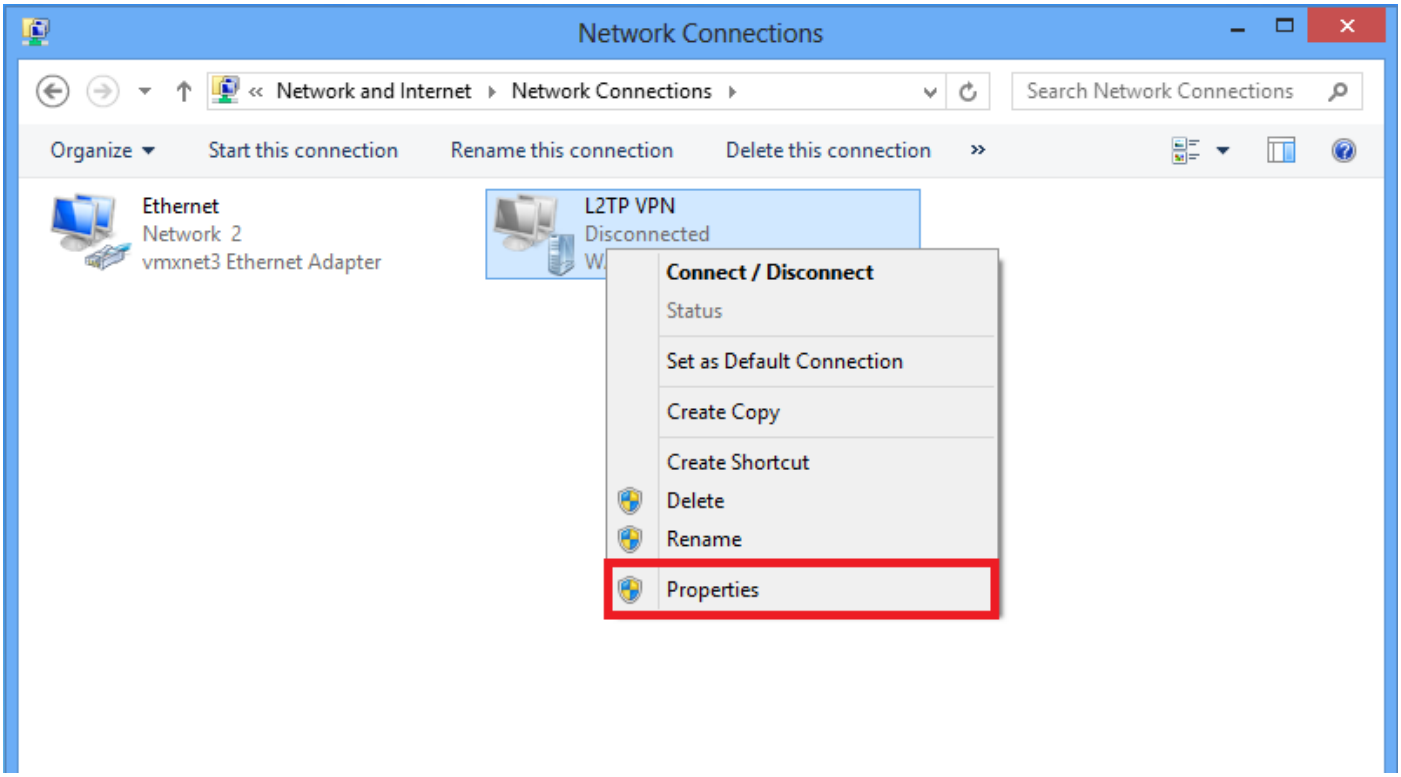
Il tunneling ripartito è una funzione che può essere utilizzata per definire il traffico delle subnet o degli host che devono essere crittografati. Questa operazione richiede la configurazione di un Access Control List (ACL) associato a questa funzione. Il traffico per le subnet o gli host definiti in questo ACL viene crittografato sul tunnel dall'estremità client e le route per queste subnet vengono installate nella tabella di routing del PC. ASA intercetta il messaggio DHCPINFORM da un client e risponde con la subnet mask, il nome di dominio e le route statiche senza classe.

Configurazione sull'appliance ASA

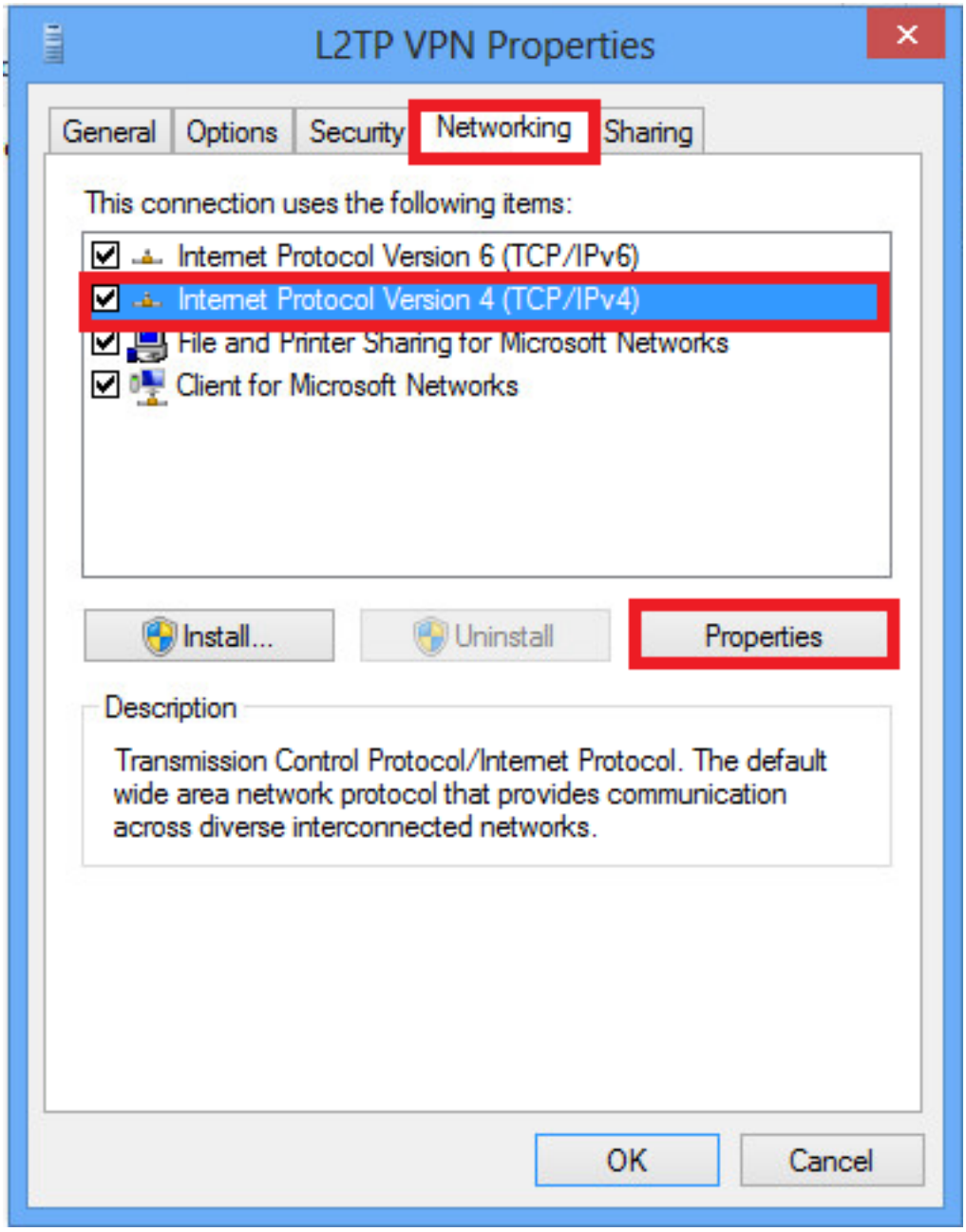
```
ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0

ciscoasa(config)# group-policy DefaultRAGroup attributes
ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT
ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable
```

Configurazione sul client L2TP/IPsec

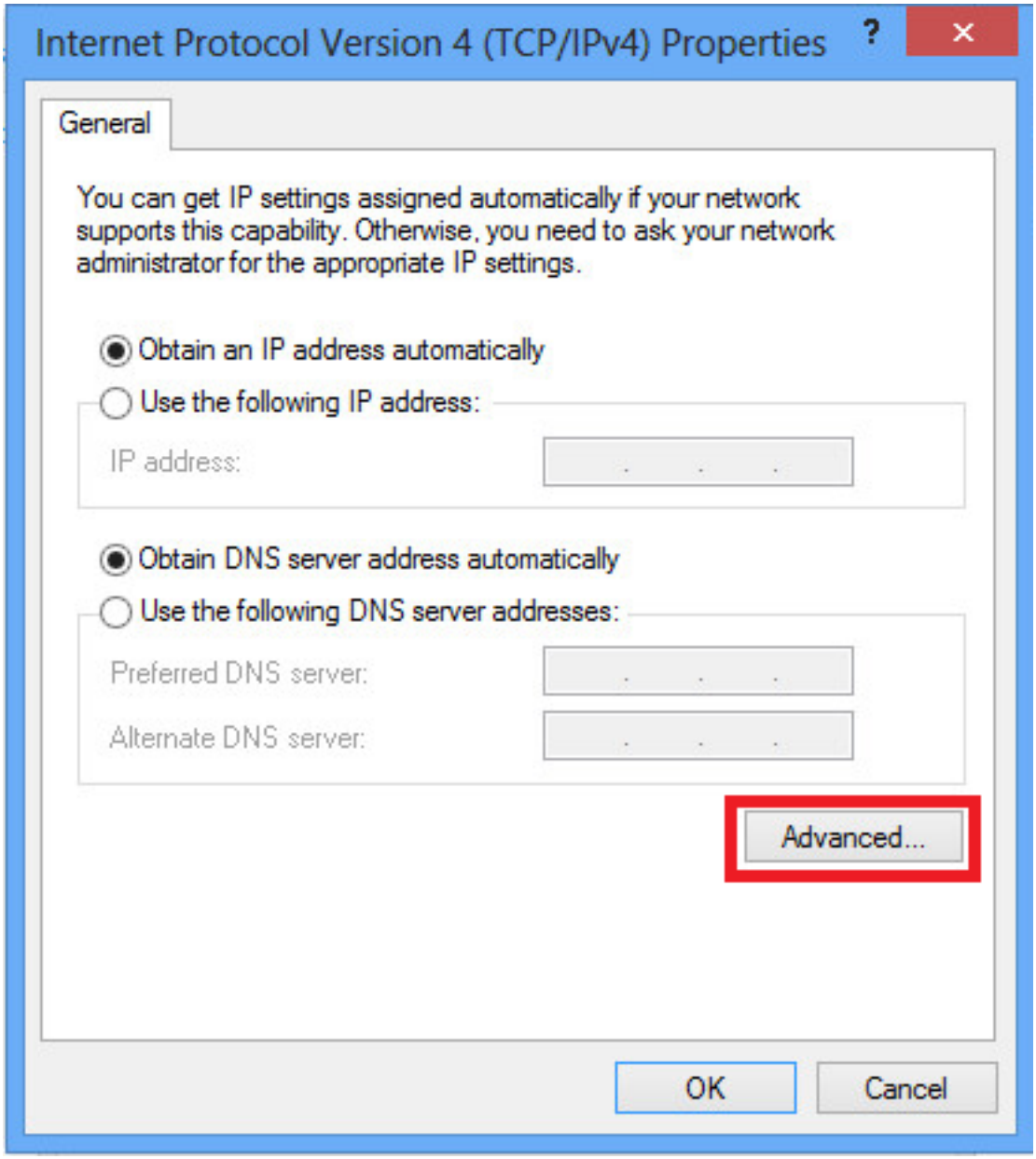
1. Fare clic con il pulsante destro del mouse sulla scheda VPN L2TP e scegliere **Proprietà.**



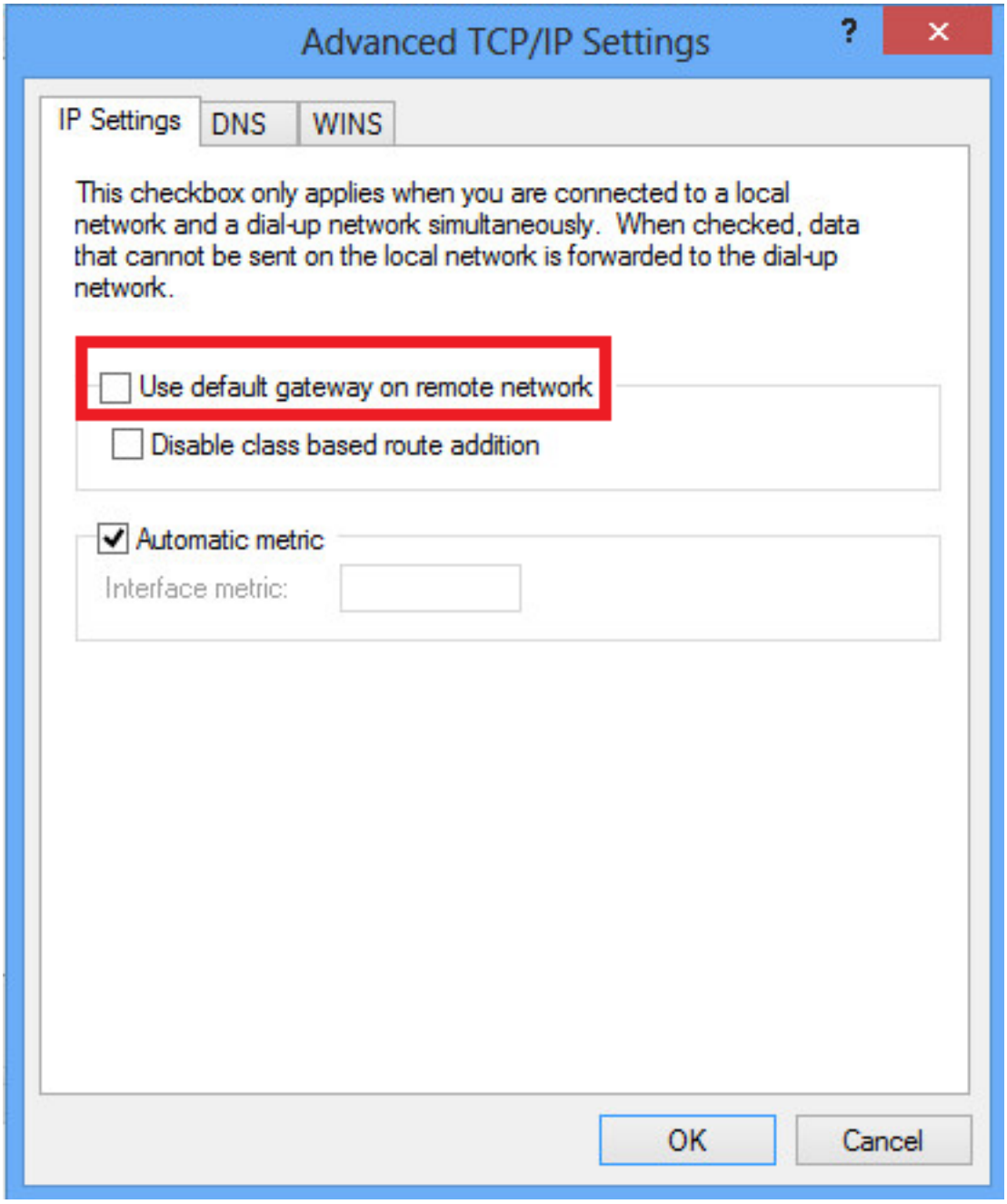
2. Passare alla scheda Rete, scegliere Protocollo Internet versione 4 (TCP/IPv4), quindi fare clic su **Proprietà.**



3. Fare clic su **Avanzate** opzione.



4. Deselezionare l'opzione **Usa gateway predefinito sulla rete remota** e fare clic su **OK**.



Verifica

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

> **Nota:** Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

- **show crypto ikev1 sa**: visualizza tutte le associazioni di protezione IKE correnti a un peer.

```
ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

  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:
```

10.1.1.2

```
   Type    : user            Role    : responder
   Rekey   : no
```

State   : MM_ACTIVE

- show crypto ipsec sa: visualizza tutte le associazioni di protezione IPsec correnti in un peer.

```
ciscoasa# show crypto ipsec sa
interface: outside
   Crypto map tag:
```

outside_dyn_map

```
, seq num: 10, local addr: 172.16.1.2

     local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/
```

17/1701

```
)
     remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/
```

17/1701

```
)
```

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

```
     dynamic allocated peer ip(ipv6): 0.0.0.0
```

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

```
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 29, #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
```

```
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
    path mtu 1500, ipsec overhead 58(36), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: E8AF927A
    current inbound spi : 71F346AB

  inbound esp sas:
    spi: 0x71F346AB (1911768747)
       transform: esp-3des esp-sha-hmac no compression
       in use settings ={RA, Transport, IKEv1, }
       slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
       sa timing: remaining key lifetime (kB/sec): (237303/3541)
       IV size: 8 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000003
  outbound esp sas:
    spi: 0xE8AF927A (3903820410)
       transform: esp-3des esp-sha-hmac no compression
       in use settings ={RA, Transport, IKEv1, }
       slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
       sa timing: remaining key lifetime (kB/sec): (237303/3541)
       IV size: 8 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

- **show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec - Mostra informazioni dettagliate sulle connessioni L2TP su IPsec.**

```
ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed


Username     : test

                  Index        : 1


Assigned IP  : 192.168.1.1           Public IP    : 10.1.1.2


Protocol     : IKEv1 IPsec L2TPOverIPsec
License      : Other VPN
Encryption   : IKEv1: (1)3DES  IPsec: (1)3DES  L2TPOverIPsec: (1)none
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1  L2TPOverIPsec: (1)none
Bytes Tx     : 1574                  Bytes Rx     : 12752
Pkts Tx      : 29                    Pkts Rx      : 118
Pkts Tx Drop : 0                     Pkts Rx Drop : 0


Group Policy : L2TP-VPN              Tunnel Group : DefaultRAGroup


Login Time   : 23:32:48 UTC Sat May 16 2015
```

```
Duration     : 0h:04m:05s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                     VLAN         : none
Audt Sess ID : 0a6a2577000010005557d3a0
Security Grp : none

IKEv1 Tunnels: 1
IPsec Tunnels: 1
L2TPOverIPsec Tunnels: 1
```

IKEv1:

```
 Tunnel ID    : 1.1
 UDP Src Port : 500                     UDP Dst Port : 500
 IKE Neg Mode : Main                    Auth Mode    : preSharedKeys
 Encryption   : 3DES                    Hashing      : SHA1
 Rekey Int (T): 28800 Seconds           Rekey Left(T): 28555 Seconds
 D/H Group    : 2
 Filter Name  :
```

IPsec:

```
 Tunnel ID    : 1.2
 Local Addr   : 172.16.1.2/255.255.255.255/17/1701
 Remote Addr  : 10.1.1.2/255.255.255.255/17/1701
 Encryption   : 3DES                    Hashing      : SHA1
 Encapsulation: Transport
 Rekey Int (T): 3600 Seconds            Rekey Left(T): 3576 Seconds
 Rekey Int (D): 250000 K-Bytes          Rekey Left(D): 250000 K-Bytes
 Idle Time Out: 30 Minutes              Idle TO Left : 29 Minutes
 Bytes Tx     : 1574                    Bytes Rx     : 12752
 Pkts Tx      : 29                      Pkts Rx      : 118
```

L2TPOverIPsec:

```
 Tunnel ID    : 1.3
```

Username : test

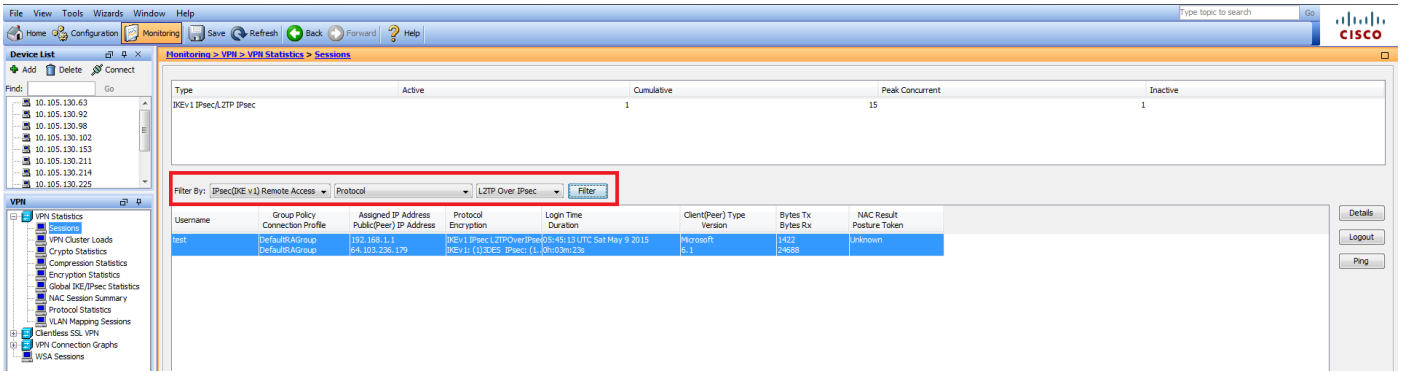
Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

```
 Encryption   : none                    Hashing      : none
```

```
Auth Mode     : msCHAPV2

Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
Client OS     : Microsoft
Client OS Ver: 6.2
Bytes Tx      : 475                   Bytes Rx     : 9093
Pkts Tx       : 18                    Pkts Rx      : 105
```

Su ASDM, in **Monitoraggio > VPN > Statistiche VPN > Sessioni** è possibile visualizzare le informazioni generali relative alla sessione VPN. Le sessioni L2TP su IPsec possono essere filtrate in base ad **Accesso remoto IPsec (IKEv1) > Protocollo > L2TP su IPsec**.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

> **Attenzione:** Sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene utilizzato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug potrebbe aumentare. Procedere con cautela, soprattutto negli ambienti di produzione!

Usare i seguenti **comandi di debug con cautela** per risolvere i problemi con il tunnel VPN

- **debug crypto ikev1**: visualizza le informazioni di debug su IKE
- **debug crypto ipsec**: visualizza le informazioni di debug su IPsec

Di seguito viene riportato l'output del comando debug per una connessione L2TP su IPSec riuscita:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NONE (0) total length : 408
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
```

```
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure:  Mismatched attribute types for class Group
Description:  Rcv'd: Unknown  Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended
capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,
```

Connection landed on tunnel_group DefaultRAGroup

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for
Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D
(20) + NONE (0) total length : 304
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
```

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keep-alives (type = None)
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds.
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

PSec SA Proposal # 2, Transform # 1 acceptable

  Matches global IPSec SA entry # 10
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI!
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI   : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine: SPI = 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick mode
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;

```
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007fffe1c75c00,
   SCB: 0xE13ABD20,
   Direction: outbound
   SPI      : 0x8C14FD70
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x8C14FD70
IPSEC: Creating outbound VPN context, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
   Peer : 0x00000000
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: New outbound encrypt rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   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 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
   Src addr: 172.16.1.2
   Src mask: 255.255.255.255
   Dst addr: 10.1.1.2
   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: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User ()  Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
   Direction: inbound
   SPI      : 0x7AD72E0D
   Session ID: 0x00001000
   VPIF num  : 0x00000002
   Tunnel type: ra
   Protocol   : esp
   Lifetime   : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x00000206
   SA   : 0x00007fffe13ab260
   SPI  : 0x7AD72E0D
   MTU  : 0 bytes
   VCID : 0x00000000
   Peer : 0x000028D4
   SCB  : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x0000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA   : 0x00007fffe1c75c00
   SPI  : 0x8C14FD70
   MTU  : 1500 bytes
   VCID : 0x00000000
```

```
   Peer : 0x00004174
   SCB  : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
   VPN handle: 0x00000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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 inbound tunnel flow rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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: 0x7AD72E0D
   Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
   Src addr: 10.1.1.2
   Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
   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: 0x7AD72E0D
   Use SPI: true
```

```
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
   Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

PHASE 2 COMPLETED

```
 (msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1

In questa tabella vengono illustrati alcuni degli errori più comuni relativi alla VPN nel client Windows

Codice errore	Soluzione possibile
691	Verificare che il nome utente e la password immessi siano corretti
789,835	Verificare che la chiave precondivisa configurata sul computer client sia la stessa dell'appliance
800	1. Verificare che il tipo VPN sia impostato su "Layer 2 Tunneling Protocol (L2TP)" 2. Assicurarsi che la chiave già condivisa sia configurata correttamente
809	Verificare che la porta UDP 500, 4500 (nel caso in cui il client o il server si trovi dietro un dispos NAT) e il traffico ESP non sia stato bloccato

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Soluzioni per la risoluzione dei problemi più comuni di VPN IPsec L2L e ad accesso remoto
- Documentazione e supporto tecnico – Cisco Systems