

Configurazione del client Show Soft VPN per la connessione al router serie RV34X

Obiettivo

L'obiettivo di questo documento è mostrare come utilizzare il client Show Soft VPN per connettersi a un router serie RV340.

È possibile scaricare la versione più recente del software client Shrew Soft VPN qui:

<https://www.shrew.net/download/vpn>

Dispositivi interessati | Versione software

RV340 | 1.0.3.17 (scarica la versione più recente)

RV340W | 1.0.3.17 ([scarica la versione più recente](#))

RV345 | 1.0.3.17 ([scarica la versione più recente](#))

RV345P | 1.0.3.17 ([scarica la versione più recente](#))

Introduzione / Use Case

La VPN IPsec (Virtual Private Network) consente di ottenere risorse remote in modo sicuro stabilendo un tunnel crittografato su Internet. I router della serie RV34X funzionano come server VPN IPSEC e supportano il client Show Soft VPN. In questa guida viene illustrata la configurazione iniziale del router e di Show Soft Client per proteggere una connessione a una VPN.

Il documento si compone di due parti:

Configurazione del router serie RV340

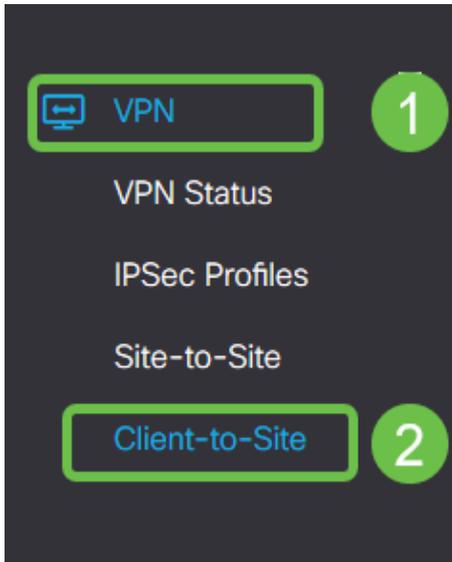
Configurare il client Show Soft VPN

Configurare il router serie RV34X:

Inizieremo configurando la **VPN da client a sito** sulla RV34x

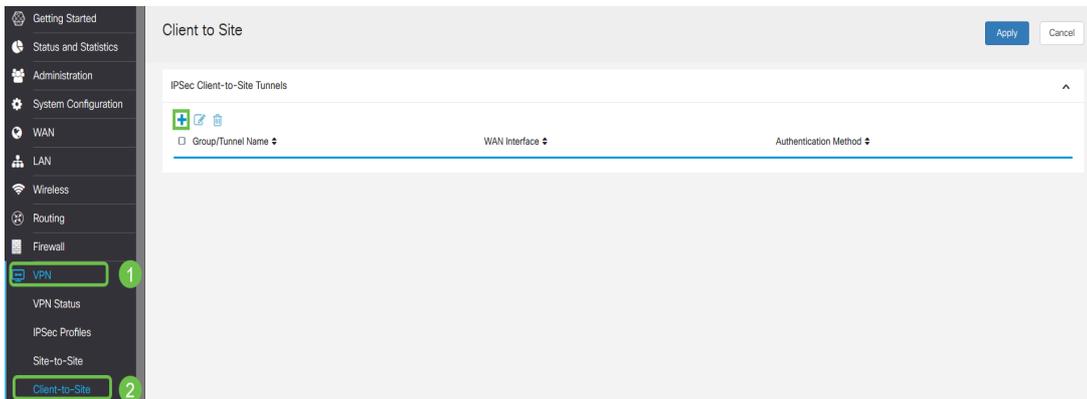
Passaggio 1

In **VPN > Da client a sito**,



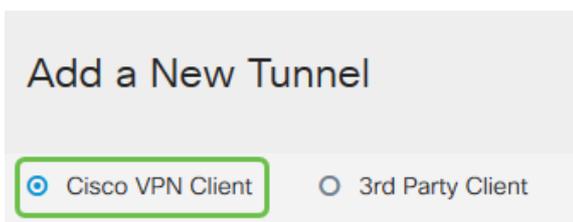
Passaggio 2

Aggiungere un profilo VPN **da client a sito**



Passaggio 3

Selezionare l'opzione **Cisco VPN Client**.



Passaggio 4

Selezionare la casella **Enable** (Abilita) per rendere attivo il profilo client VPN. Inoltre, configureremo il *Nome gruppo*, selezioneremo l'**interfaccia WAN** e immetteremo una **Chiave già condivisa**.

Nota: Prendere nota del *nome del gruppo* e della *chiave già condivisa*, in quanto verranno utilizzati in seguito durante la configurazione del client.

Enable:

Group Name: Clients

Interface: WAN1

IKE Authentication Method

Pre-shared Key: [.....]

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable

Certificate:

Passaggio 5

Per il momento, lasciare vuota la **tabella Gruppo utenti**. Questa operazione è relativa al *gruppo di utenti* sul router, ma non è ancora stata configurata. Verificare che la **modalità** sia impostata su **Client**. Immettere l'**intervallo di pool per la LAN client**. Utilizzeremo da 172.16.10.1 a 172.16.10.10.

Nota: L'intervallo di pool deve utilizzare una subnet univoca che non viene utilizzata in altre posizioni della rete.

User Group:

User Group Table

+ [trash icon]

□ Group Name ↕

Mode: Client NEM

Pool Range for Client LAN

Start IP: 172.16.10.1

End IP: 172.16.10.10

Passaggio 6

Qui è possibile configurare le impostazioni di **Configurazione modalità**. Ecco le impostazioni che utilizzeremo:

Server DNS primario: Se si dispone di un server DNS interno o si desidera utilizzare un server DNS esterno, è possibile immetterlo qui. In caso contrario, per impostazione predefinita viene utilizzato l'indirizzo IP della LAN RV340. Nell'esempio verrà utilizzata l'impostazione predefinita.

Tunnel ripartito: Selezionare per abilitare il tunneling ripartito. Questa opzione viene usata per specificare il traffico che passerà attraverso il tunnel VPN. Nel nostro esempio utilizzeremo

Split Tunnel.

Tabella tunnel suddiviso: Immettere le reti a cui il client VPN deve avere accesso tramite la VPN. In questo esempio viene utilizzata la rete LAN RV340.

Mode Configuration

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain:

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel:

Split Tunnel Table

+ [edit] [delete]

IP Address ⇅ Netmask ⇅

<input checked="" type="checkbox"/> 192.168.1.0	255.255.255.0
---	---------------

Passaggio 7

Dopo aver fatto clic su **Save**, è possibile visualizzare il profilo nell'elenco **IPSec Client-to-Site Groups** (Gruppi client-sito IPSec).

Client to Site

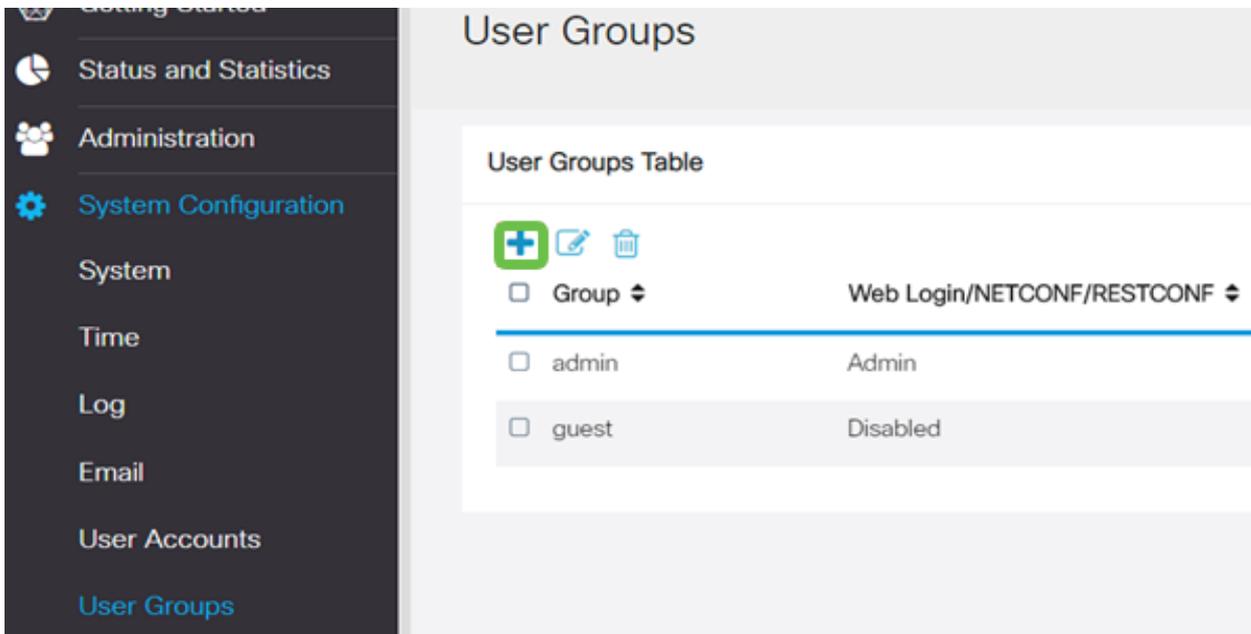
IPSec Client-to-Site Tunnels

+ [edit] [delete]

Group/Tunnel Name ⇅	WAN Interface ⇅	Authentication Method ⇅
<input type="checkbox"/> Clients	WAN1	Pre-shared Key

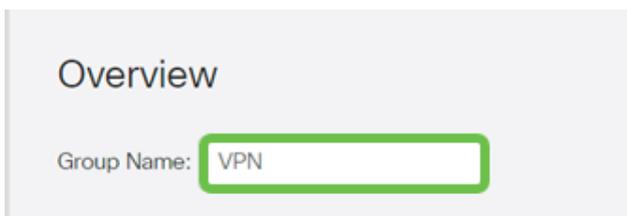
Passaggio 8

Verrà ora configurato un **gruppo di utenti** da utilizzare per l'autenticazione degli utenti client VPN. In **Configurazione di sistema > Gruppi di utenti**, fare clic su '+' per aggiungere un gruppo di utenti.



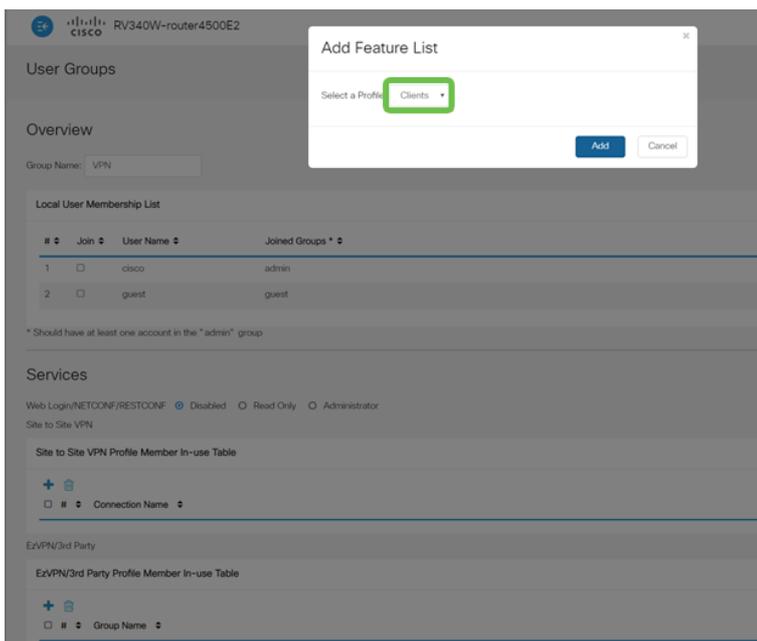
Passaggio 9

Immettere il nome di un gruppo.



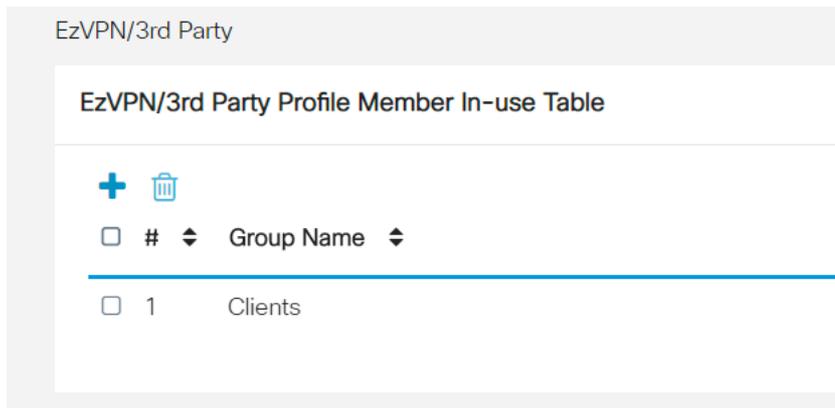
Passaggio 10

Nella sezione **Servizi > EzVPN/terze parti**, fare clic su **Aggiungi** per collegare questo gruppo di utenti al profilo **client-sito** configurato in precedenza.



Passaggio 11

Il nome del gruppo **da client a sito** dovrebbe essere visualizzato nell'elenco di **EzVPN/terze parti**



EzVPN/3rd Party

EzVPN/3rd Party Profile Member In-use Table

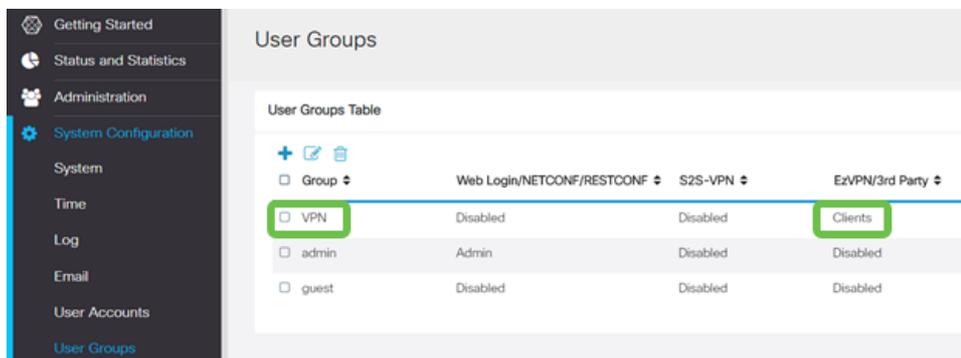
+ 

Group Name

1 Clients

Passaggio 12

Dopo aver **applicato** la configurazione del gruppo di utenti, questa verrà visualizzata nell'elenco **Gruppi di utenti** e mostrerà che il nuovo gruppo di utenti verrà utilizzato con il profilo da client a sito creato in precedenza.



Getting Started

Status and Statistics

Administration

System Configuration

System

Time

Log

Email

User Accounts

User Groups

User Groups

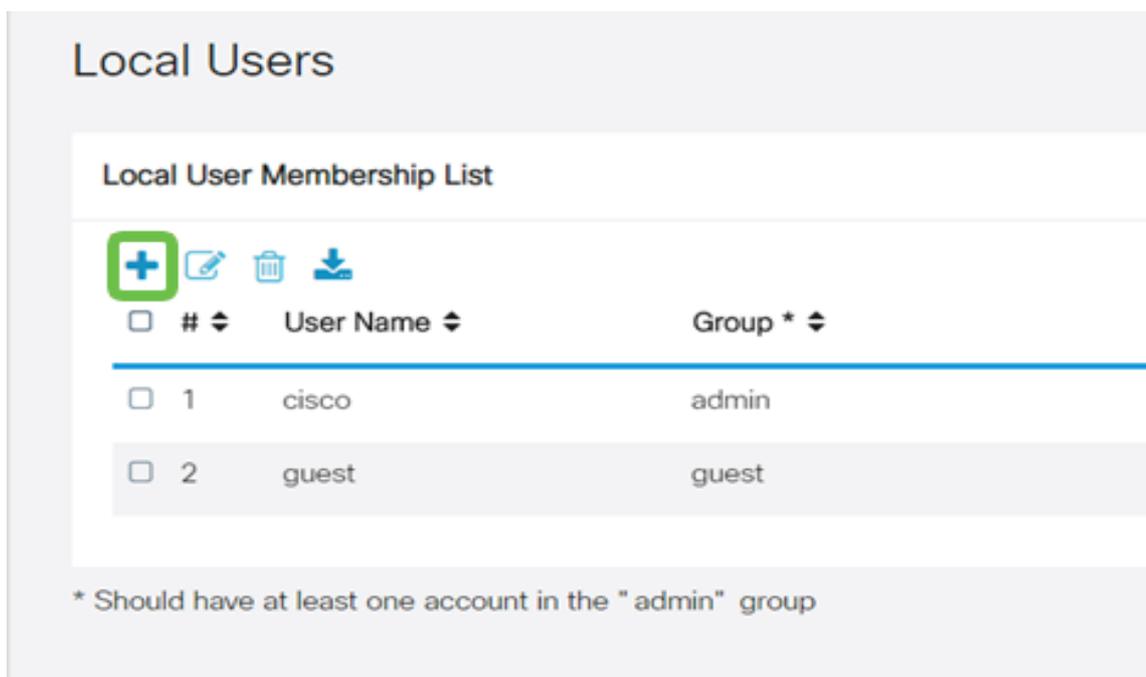
User Groups Table

+  

<input type="checkbox"/> Group <input type="checkbox"/>	Web Login/NETCONF/RESTCONF <input type="checkbox"/>	S2S-VPN <input type="checkbox"/>	EzVPN/3rd Party <input type="checkbox"/>
<input type="checkbox"/> VPN	Disabled	Disabled	Clients
<input type="checkbox"/> admin	Admin	Disabled	Disabled
<input type="checkbox"/> guest	Disabled	Disabled	Disabled

Passaggio 13

Verrà ora configurato un nuovo utente in **Configurazione di sistema > Account utente**. Fare clic su **+** per creare un nuovo utente.



Local Users

Local User Membership List

+   

User Name Group *

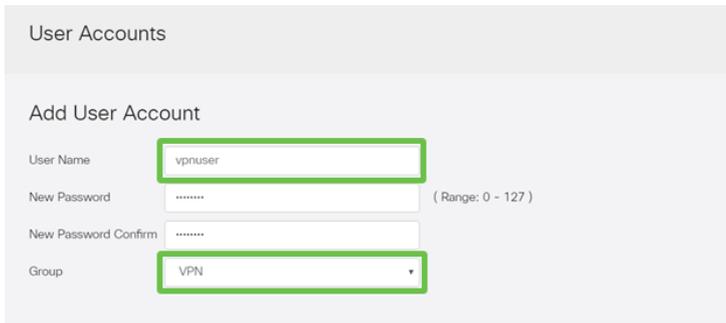
1 cisco admin

2 guest guest

* Should have at least one account in the " admin " group

Passaggio 14

Immettere il nuovo **nome utente** insieme alla **nuova password**. Verificare che il **gruppo** sia impostato sul nuovo **gruppo utenti** appena configurato. Al termine, fare clic su **Apply** (Applica).



User Accounts

Add User Account

User Name

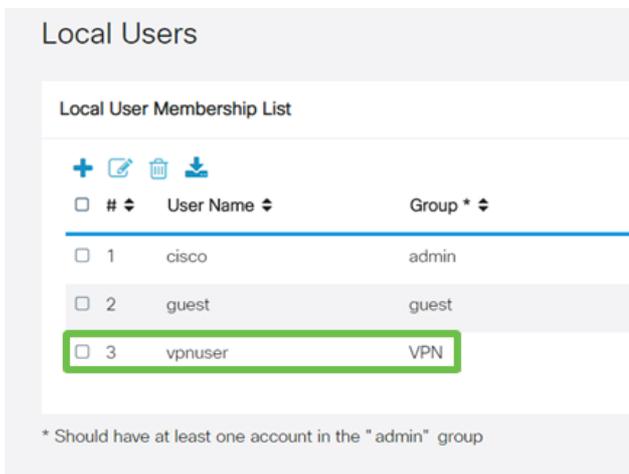
New Password (Range: 0 - 127)

New Password Confirm

Group

Passaggio 15

Il nuovo **utente** verrà visualizzato nell'elenco degli **utenti locali**.



Local Users

Local User Membership List

+ ✎ 🗑️ ⬇️

<input type="checkbox"/>	#	User Name	Group *
<input type="checkbox"/>	1	cisco	admin
<input type="checkbox"/>	2	guest	guest
<input type="checkbox"/>	3	vpnuser	VPN

* Should have at least one account in the "admin" group

La configurazione del router serie RV340 è completata. Verrà ora configurato il client di Shrew Soft VPN.

Configurare il client VPN ShrewSoft

Verrà ora configurato il client di Shrew Soft VPN.

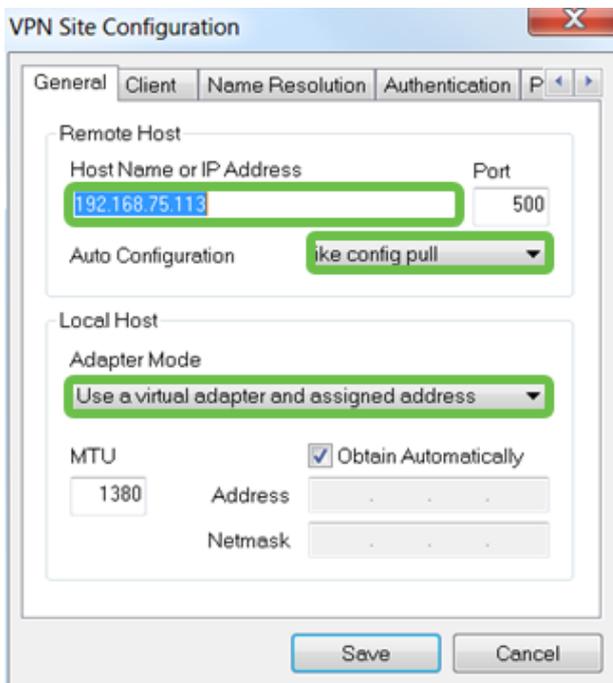
Passaggio 1

Aprire ShrewSoft *VPN Access Manager* e fare clic su **Aggiungi** per aggiungere un profilo. Nella finestra *Configurazione sito VPN* visualizzata, configurare la scheda **Generale**:

Nome host o indirizzo IP: Usare l'indirizzo ip WAN (o il nome host dell'RV340)

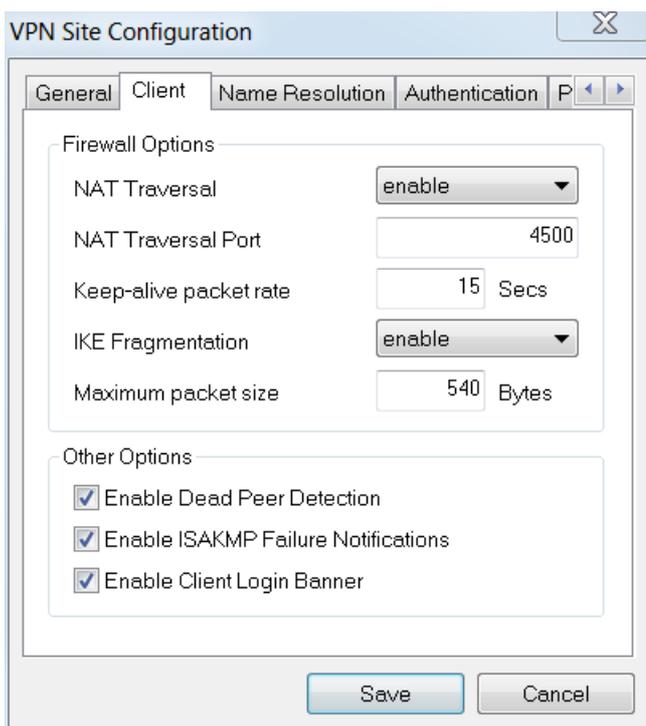
Configurazione automatica: Selezionare **Ike config pull**

Modalità scheda di rete: Selezionare **Usa scheda virtuale e indirizzo assegnato**



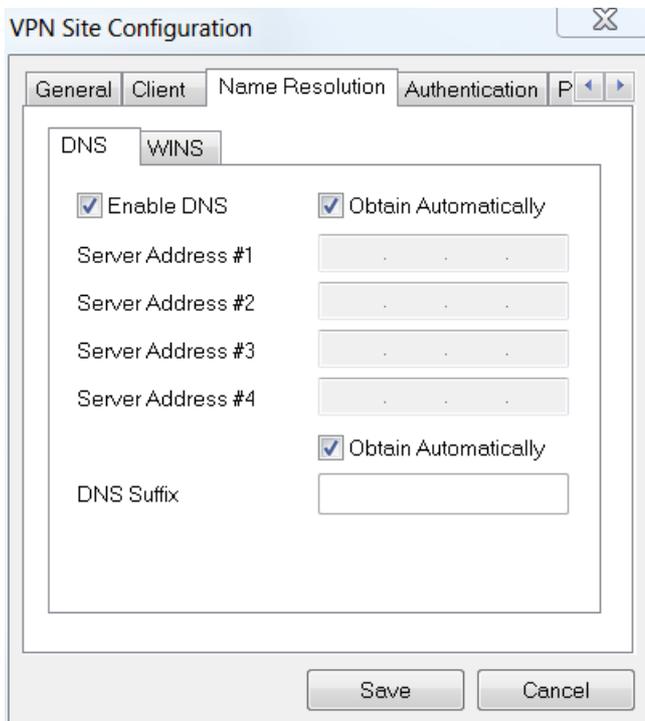
Passaggio 2

Configurare la scheda **Client**. Verranno utilizzate solo le impostazioni predefinite.



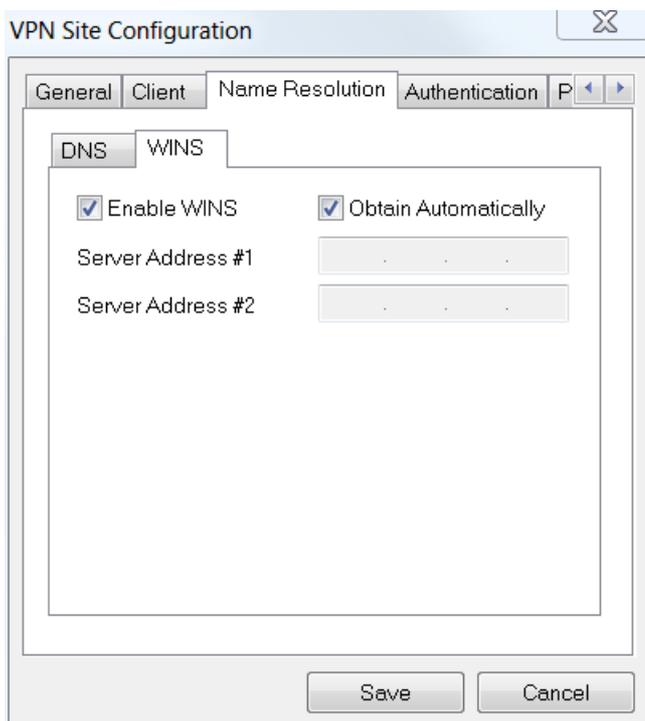
Passaggio 3

Nella scheda **Risoluzione nomi** > scheda **DNS**, selezionare la casella **Abilita DNS** e lasciare selezionate le caselle **Otteni automaticamente**.



Passaggio 4

Nella scheda **Risoluzione nome** > scheda **WINS**, selezionare la casella **Abilita WINS** e lasciare la casella di controllo **Ottieni automaticamente** selezionata.

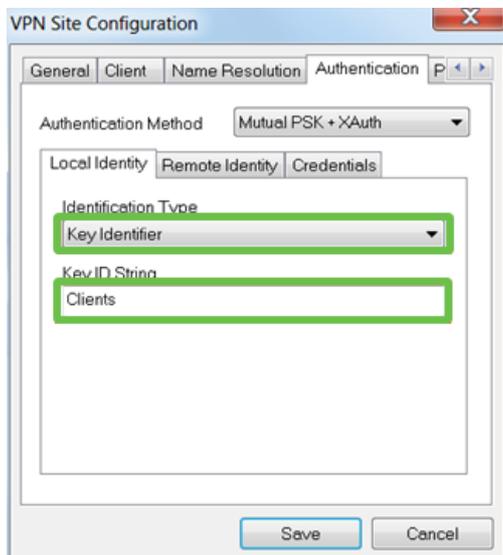


Passaggio 5

Configurare la scheda **Autenticazione** > scheda **Identità locale**:

Tipo di identificazione: Seleziona **identificatore chiave**

Stringa ID chiave: Immettere il **nome del gruppo** configurato sull'RV34x



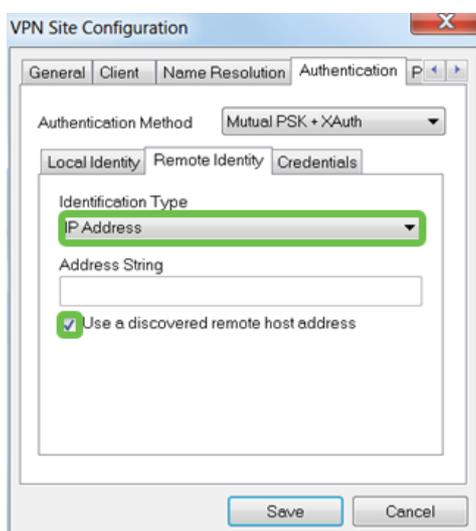
Passaggio 6

Nella scheda **Autenticazione** > **Identità remota**, verranno mantenute le impostazioni predefinite.

Tipo di identificazione: Indirizzo IP

Stringa indirizzo: <vuoto>

Utilizzare la casella dell'indirizzo di un host remoto individuato: Controllato

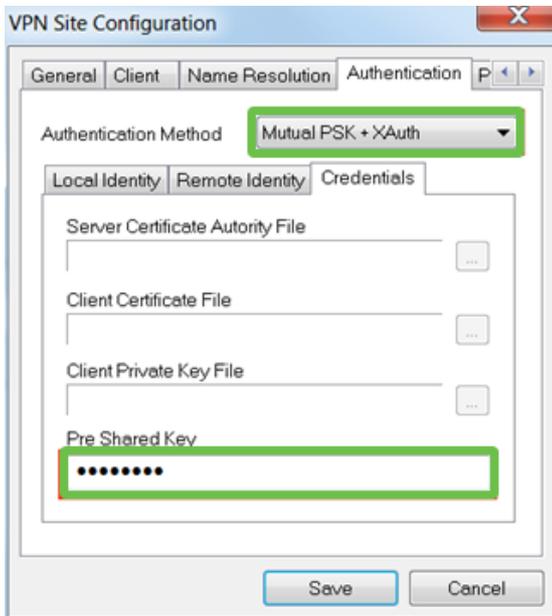


Passaggio 7

Nella scheda **Autenticazione** > scheda **Credenziali**, configurare quanto segue:

Metodo di autenticazione: Selezionare **Mutual PSK + XAuth**

Chiave già condivisa: Immettere la **chiave già condivisa** configurata nel profilo client RV340



Passaggio 8

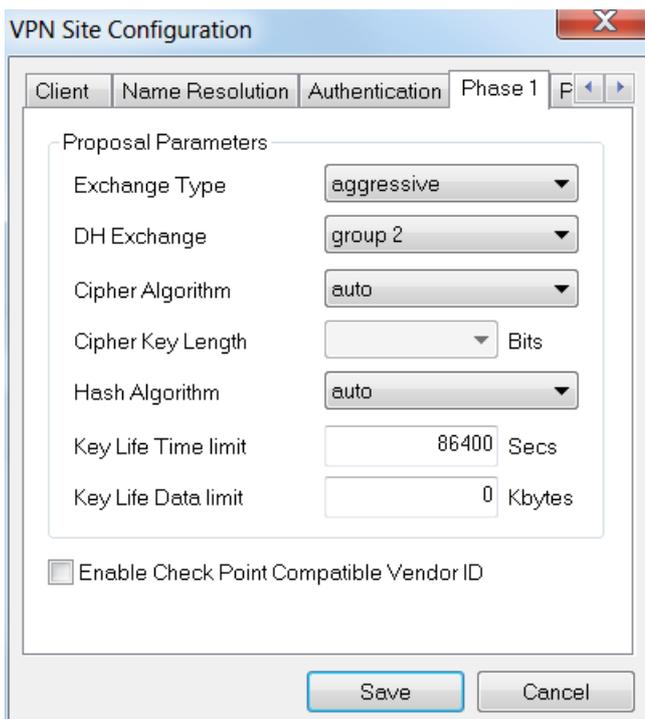
Per la scheda **Fase 1**, verranno mantenute le impostazioni predefinite:

Tipo di scambio: Aggressivo

Scambio DH: gruppo 2

Algoritmo di crittografia: Auto

Algoritmo hash: Auto



Passaggio 9

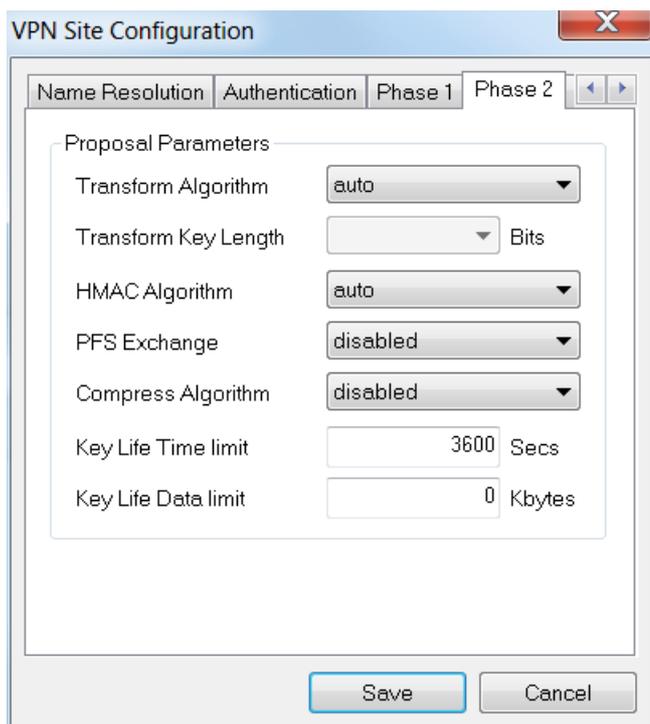
Verranno inoltre utilizzati i valori predefiniti per la scheda **Fase 2**:

Algoritmo di trasformazione: Auto

Algoritmo HMAC: Auto

Scambio PFS: Disattivato

Algoritmo di compressione: Disattivato



Passaggio 10

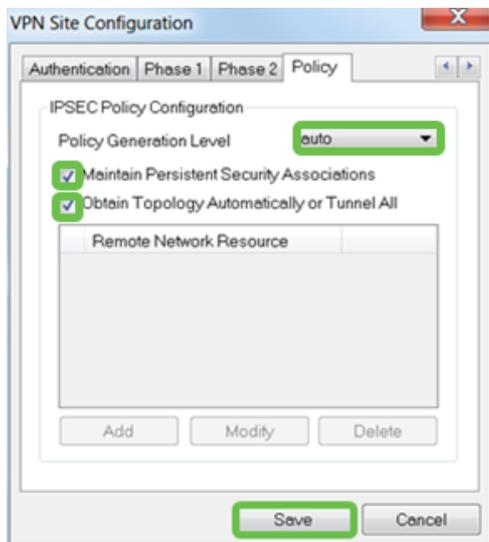
Per la scheda **Criterio** verranno utilizzate le impostazioni seguenti:

Livello generazione criteri: Auto

Gestisci Associazioni Di Sicurezza Persistenti: Controllato

Ottieni topologia automaticamente o Tunnel tutto: Controllato

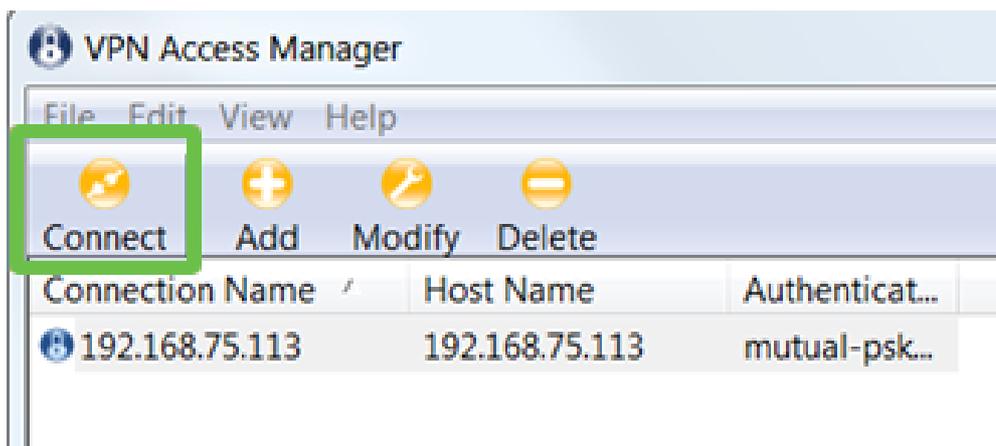
Poiché è stato configurato lo **split-tunneling** sull'RV340, non è necessario configurarlo qui.



Al termine, fare clic su **Salva**.

Passaggio 11

Ora siamo pronti a testare la connessione. In *VPN Access Manager*, evidenziare il profilo di connessione e fare clic sul pulsante **Connect** (Connetti).



Passaggio 12

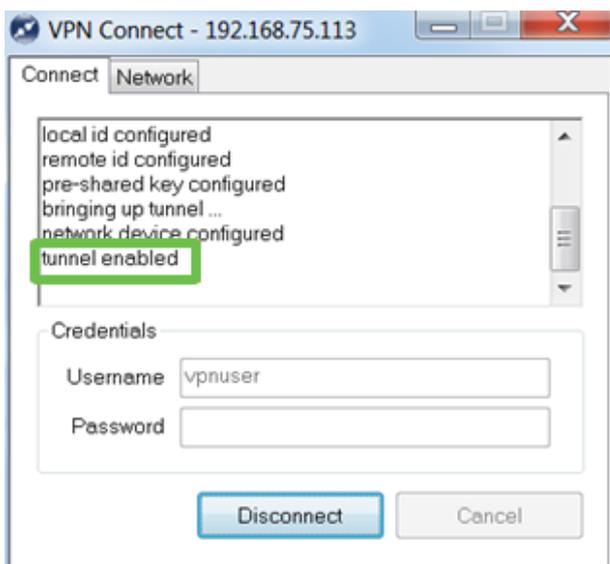
Nella finestra **VPN Connect** che viene visualizzata, immettere il **nome utente** e la **password** usando le credenziali per l'**account utente** creato sull'RV340 (passaggi 13 e 14).



Al termine, fare clic su **Connetti**.

Passaggio 13

Verificare che il tunnel sia collegato. Il **tunnel** dovrebbe essere **abilitato**.



Conclusioni

Ecco, ora è possibile connettersi alla rete tramite VPN.