Utilizzare Show Soft VPN Client per connettersi con IPSec VPN Server su RV130 e RV130W

Obiettivo

La VPN IPSec (Virtual Private Network) consente di ottenere risorse remote in modo sicuro tramite la creazione di un tunnel crittografato su Internet.

RV130 e RV130W funzionano come server VPN IPSec e supportano il client Shrew Soft VPN.

Accertarsi di scaricare l'ultima versione del software client.

·Mostrare Soft (https://www.shrew.net/download/vpn)

Nota: Per configurare correttamente il client VPN Show Soft con un server VPN IPSec, è necessario innanzitutto configurare il server VPN IPSec. Per informazioni su come eseguire questa operazione, fare riferimento all'articolo *Configurazione di un server VPN IPSec su RV130 e RV130W.*

L'obiettivo di questo documento è mostrare come utilizzare il client Show Soft VPN per connettersi a un server VPN IPSec sui modelli RV130 e RV130W.

Dispositivi interessati

·RV130W Wireless-N VPN Firewall

·RV130 VPN Firewall

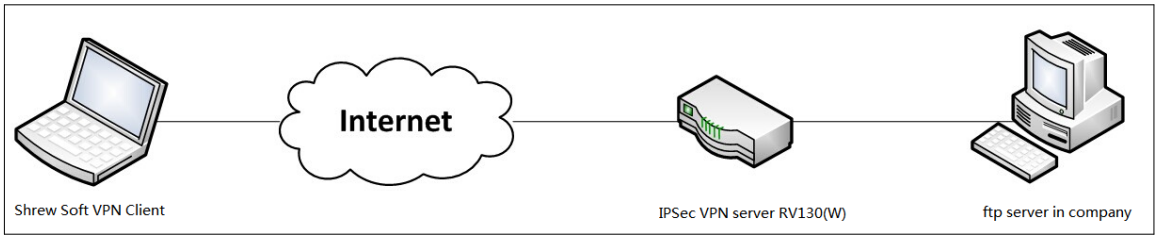
Requisiti di sistema

·Sistemi a 32 o 64 bit

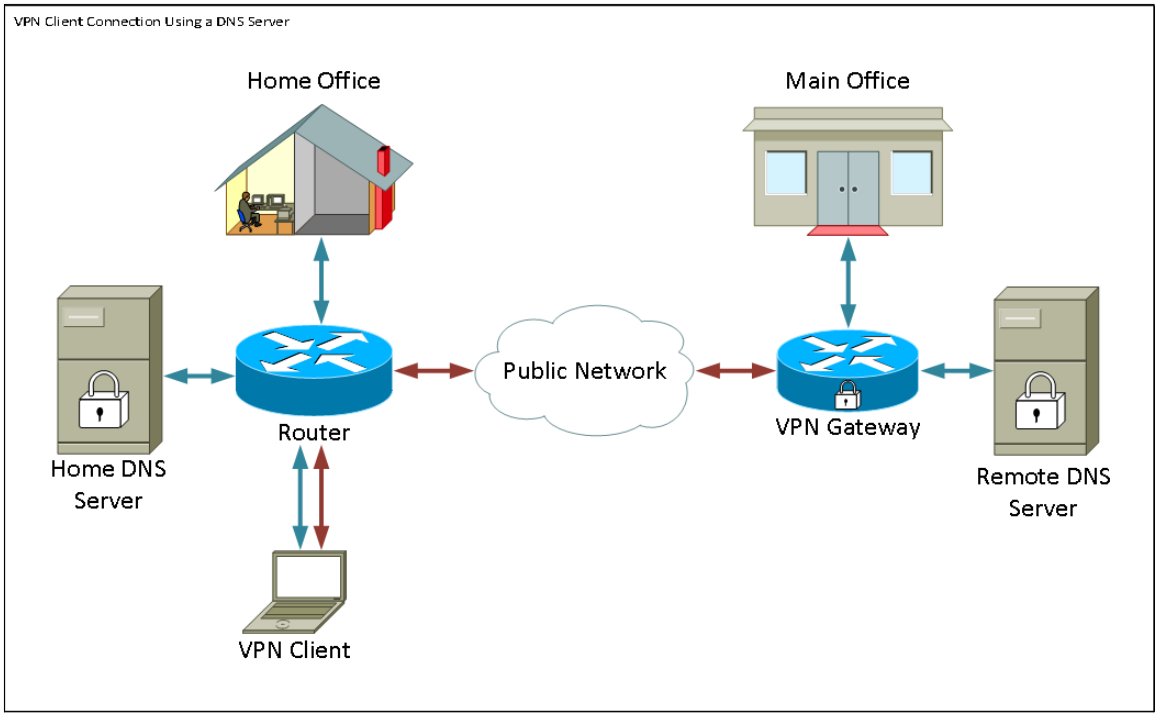
·Windows 2000, XP, Vista o Windows 7/8

Topologia

Di seguito è riportata una topologia di livello superiore che illustra i dispositivi coinvolti nella configurazione di un client Shrewsoft per il sito.



Di seguito è riportato un diagramma di flusso più dettagliato che illustra il ruolo dei server DNS in un ambiente di rete per piccole imprese.



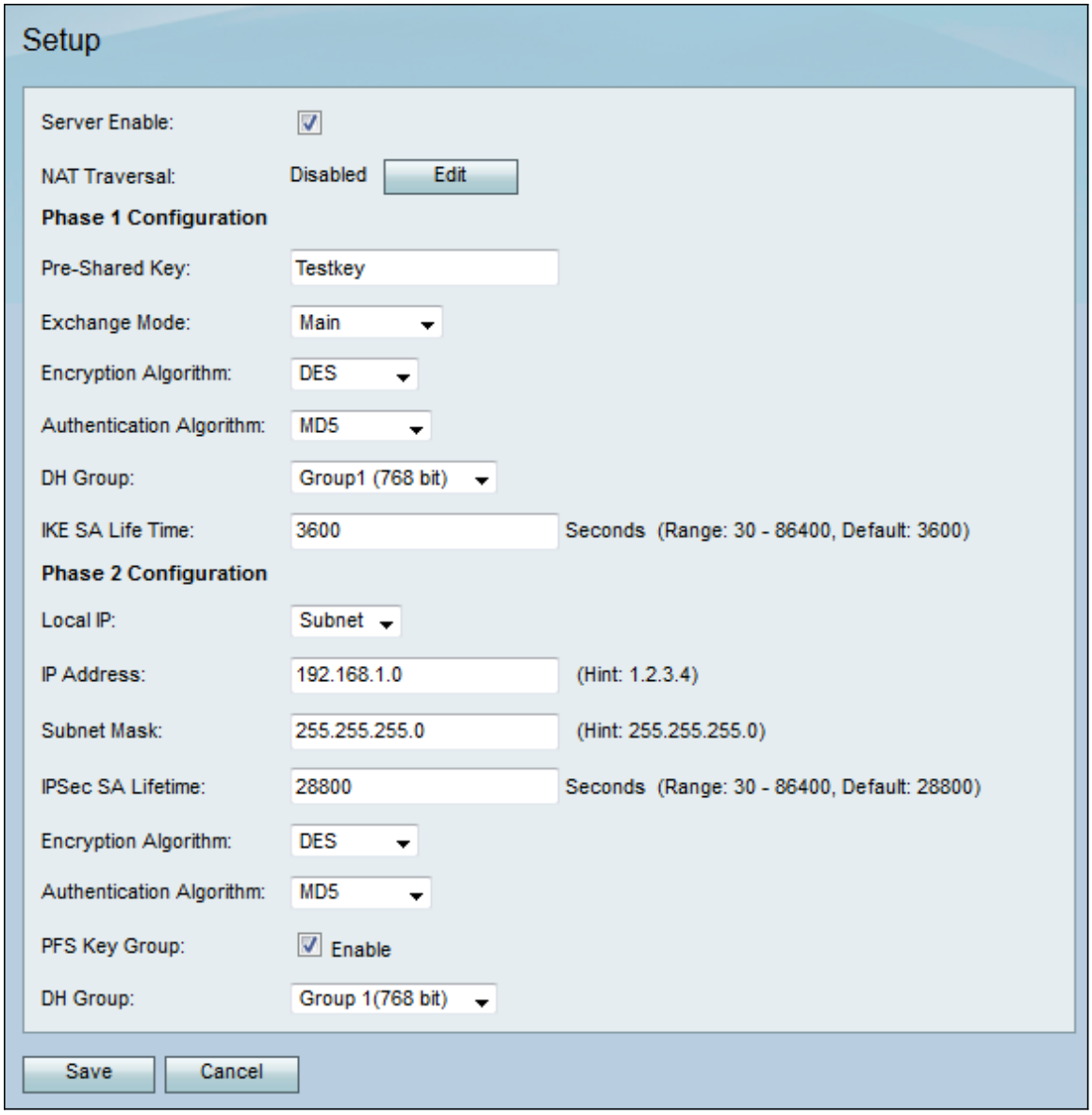
Versione del software

- 1.0.1.3

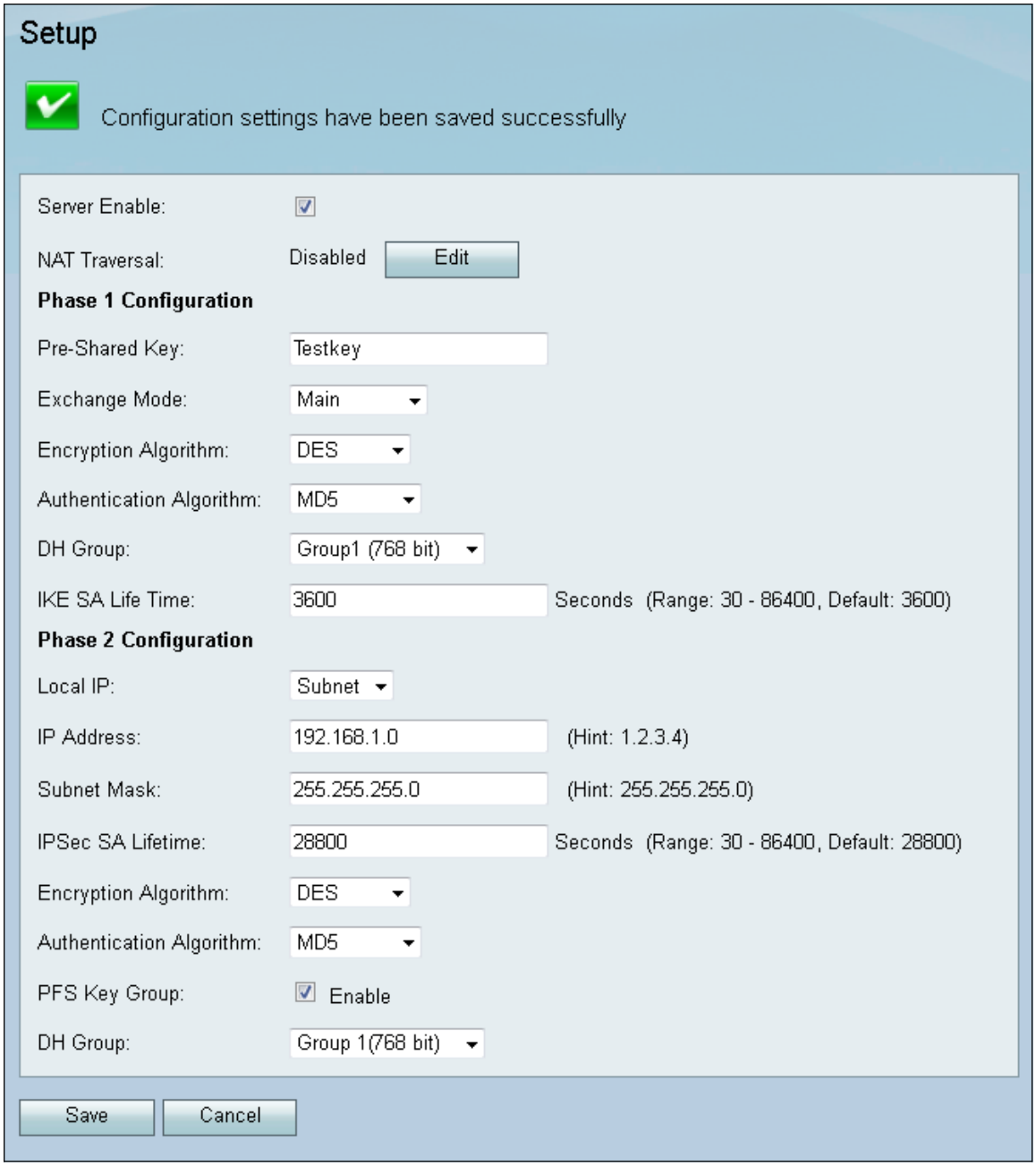
Configurazione client VPN avanzata

Configurazione e configurazione utente della VPN IPSec

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **VPN > Server VPN IPSec > Configurazione**. Viene visualizzata la pagina *Setup* (Impostazione).

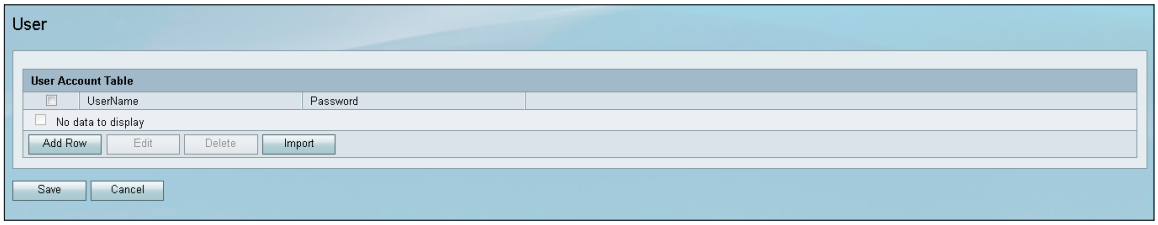


Passaggio 2. Verificare che il server VPN IPSec per RV130 sia configurato correttamente. Se il server VPN IPSec non è configurato o non è configurato correttamente, vedere *Configurazione di un server VPN IPSec sugli switch RV130 e RV130W* e fare clic su **Salva**.

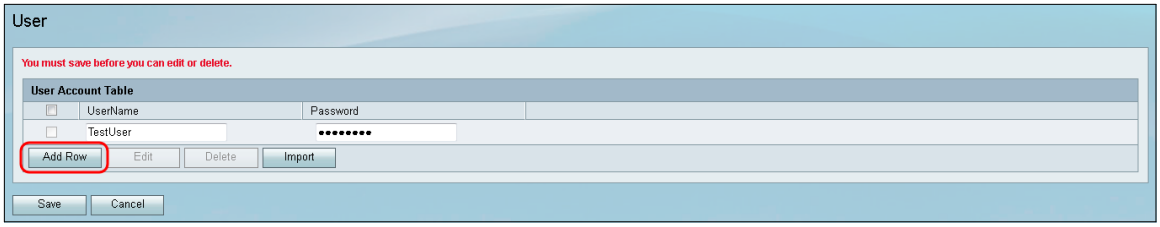


Nota: Le impostazioni precedenti sono un esempio di configurazione di un server VPN IPSec RV130/RV130W. Le impostazioni sono basate sul documento *Configurazione di un server VPN IPSec su RV130 e RV130W* e verranno usate nei passaggi successivi.

Passaggio 3. Passare a **VPN > IPSec VPN Server > Utente**. Viene visualizzata la pagina *User*.



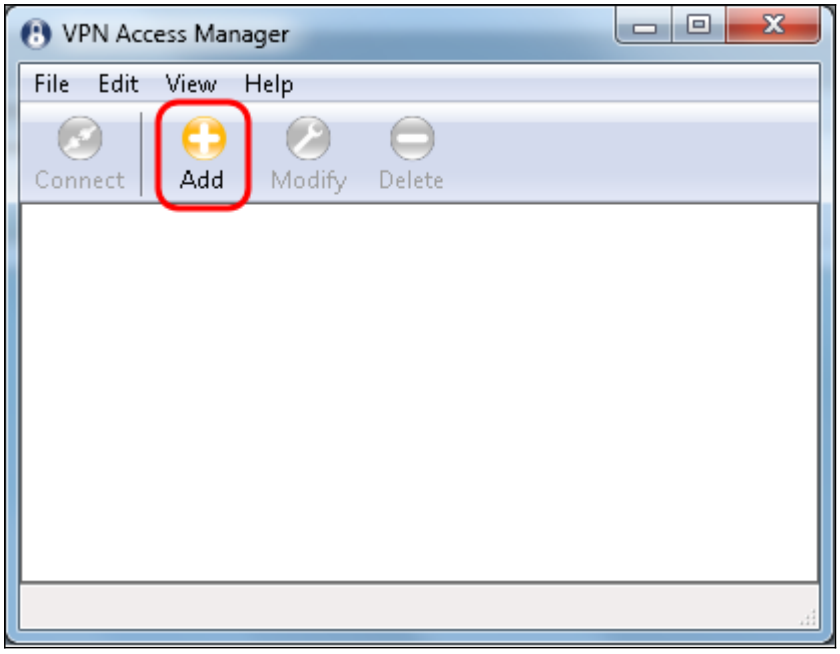
Passaggio 4. Fare clic su **Aggiungi riga** per aggiungere gli account utente utilizzati per autenticare i client VPN (autenticazione estesa) e immettere il nome utente e la password desiderati negli appositi campi.



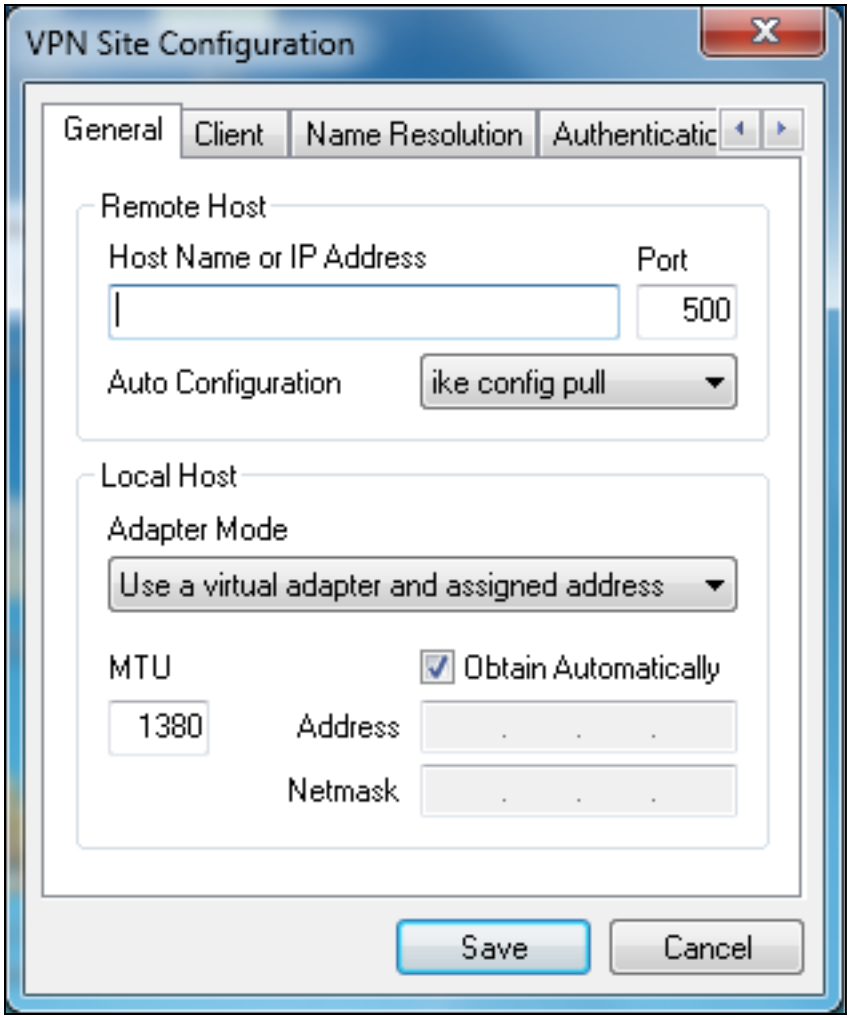
Passaggio 5. Fare clic su **Save** per salvare le impostazioni.

Configurazione client VPN

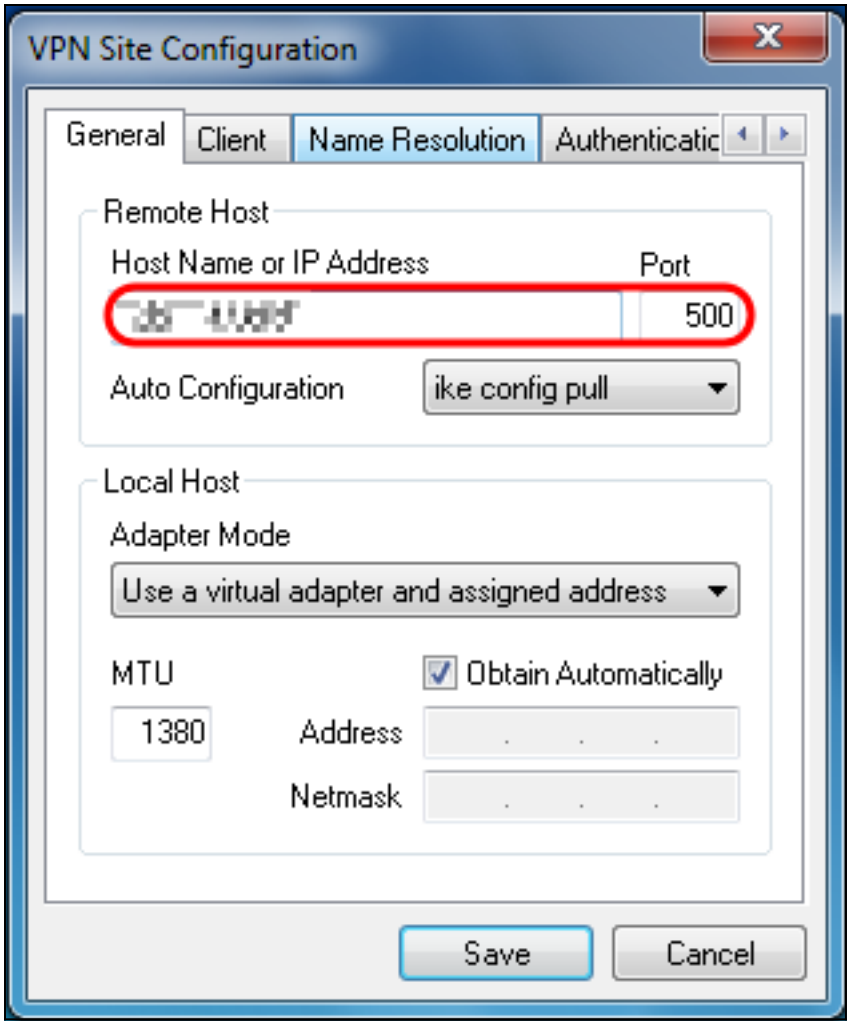
Passaggio 1. Aprire Show VPN Access Manager e fare clic su **Add** (Aggiungi) per aggiungere un profilo.



Viene visualizzata la finestra *Configurazione sito VPN*.

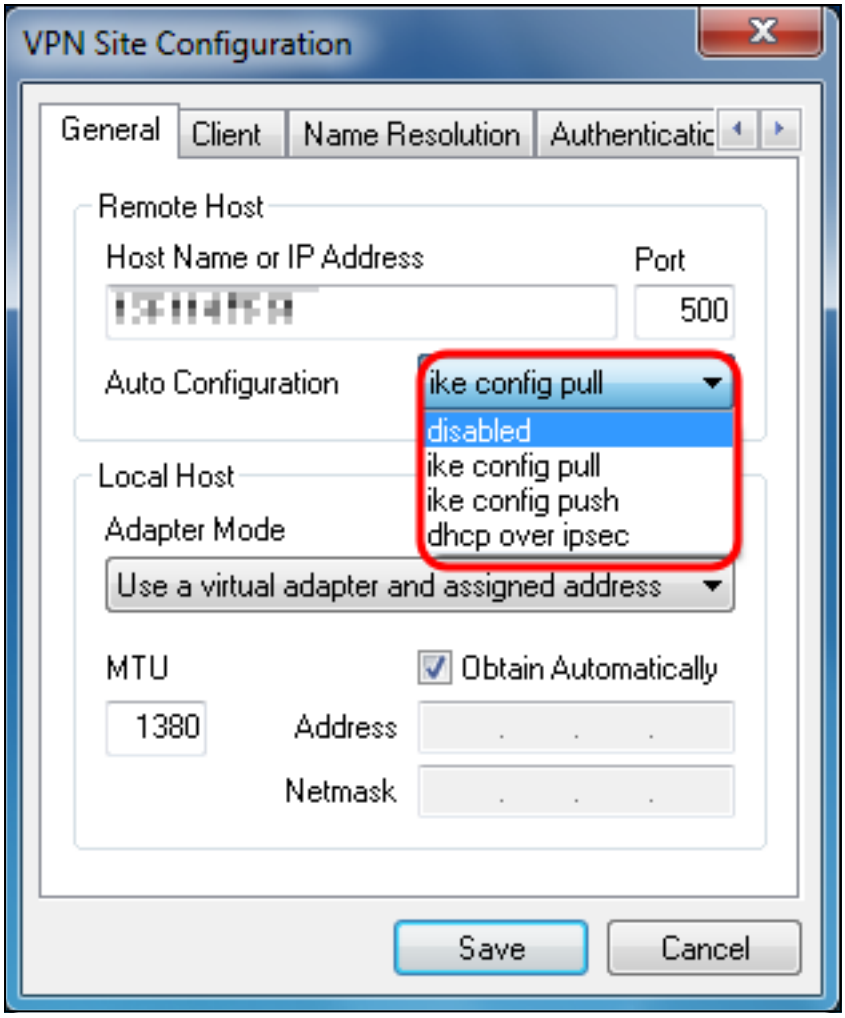


Passaggio 2. Nella sezione *Host remoto* della scheda *Generale*, immettere il nome host pubblico o l'indirizzo IP della rete a cui si sta tentando di connettersi.



Nota: Verificare che il numero di porta sia impostato sul valore predefinito 500. Affinché la VPN funzioni, il tunnel utilizza la porta UDP 500 che deve essere impostata in modo da consentire l'inoltro del traffico ISAKMP nel firewall.

Passaggio 3. Nell'elenco a discesa *Configurazione automatica*, scegliere **disabilitato**.



Le opzioni disponibili sono definite come segue:

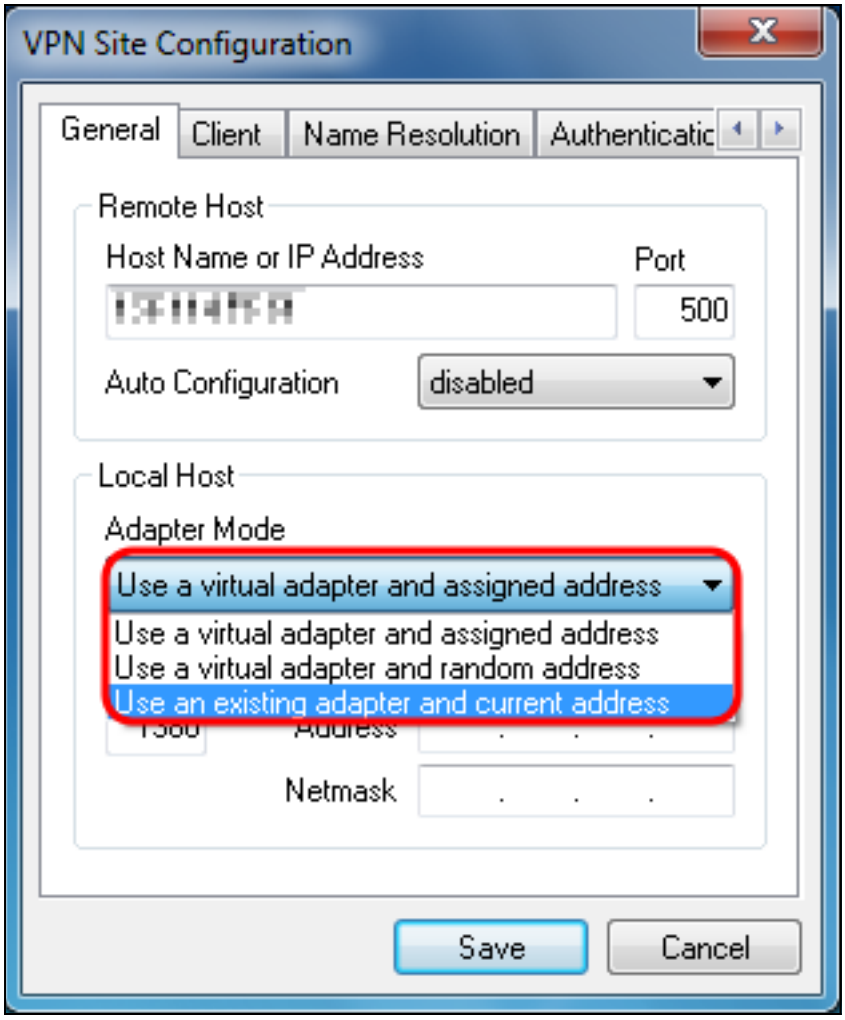
·Disattivato: disattiva qualsiasi configurazione client automatica.

·IKE Config Pull: consente al client di impostare le richieste da un computer. Se il computer supporta il metodo Pull, la richiesta restituisce un elenco di impostazioni supportate dal client.

·IKE Config Push: fornisce a un computer l'opportunità di offrire impostazioni al client attraverso il processo di configurazione. Se il computer supporta il metodo Push, la richiesta restituisce un elenco di impostazioni supportate dal client.

·DHCP over IPSec: consente al client di richiedere le impostazioni al computer tramite DHCP su IPSec.

Passaggio 4. Nella sezione *Host locale*, scegliere **Utilizza un adattatore esistente e l'indirizzo corrente** nell'elenco a discesa *Modalità adattatore*.



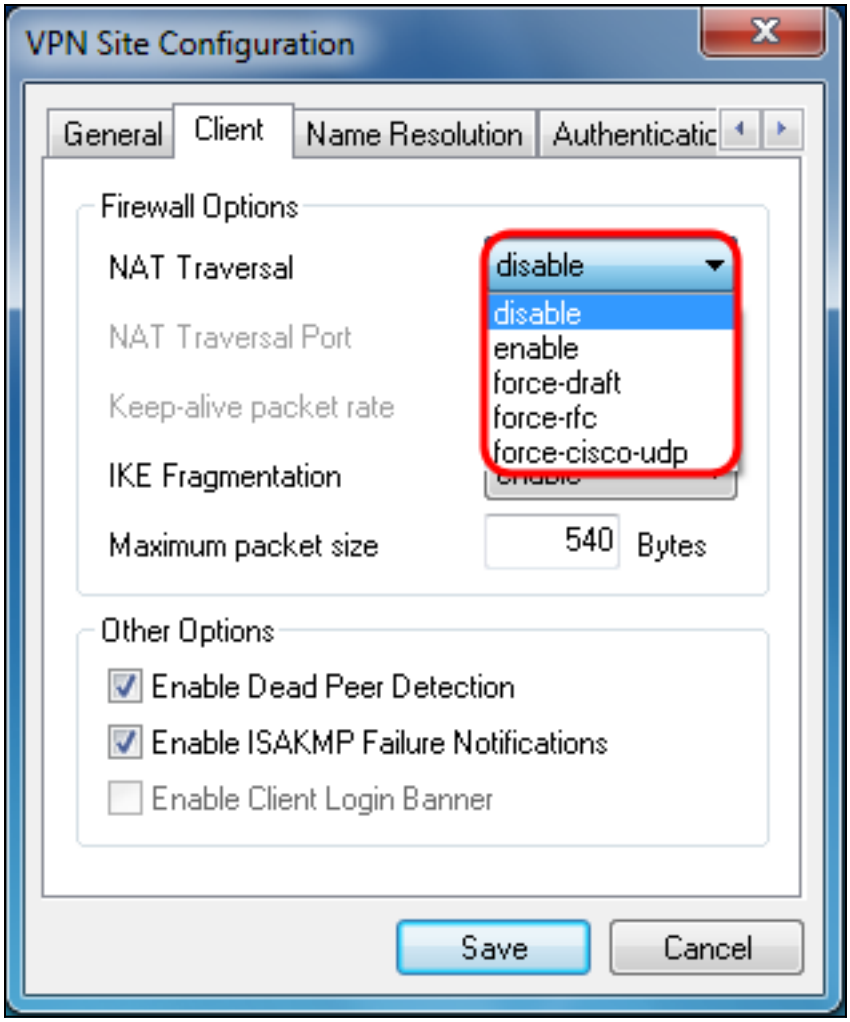
Le opzioni disponibili sono definite come segue:

·Utilizza una scheda virtuale e un indirizzo assegnato - Consente al client di utilizzare una scheda virtuale con un indirizzo specificato come origine per le comunicazioni IPsec.

·Utilizza una scheda virtuale e un indirizzo casuale: consente al client di utilizzare una scheda virtuale con un indirizzo casuale come origine delle comunicazioni IPsec.

·Utilizza una scheda esistente e l'indirizzo corrente: consente al client di utilizzare solo la scheda fisica esistente con l'indirizzo corrente come origine per le comunicazioni IPsec.

Passaggio 5. Fare clic sulla scheda *Client*. Nell'elenco a discesa *NAT Traversal*, selezionare la stessa impostazione configurata sull'RV130/RV130W per NAT Traversal nell'articolo *Configuration of an IPSec VPN Server on RV130 and RV130W.*



Le opzioni di menu disponibili per NAT (Network Address Translation) sono definite come segue:

·Disabilita: le estensioni del protocollo NAT non verranno utilizzate.

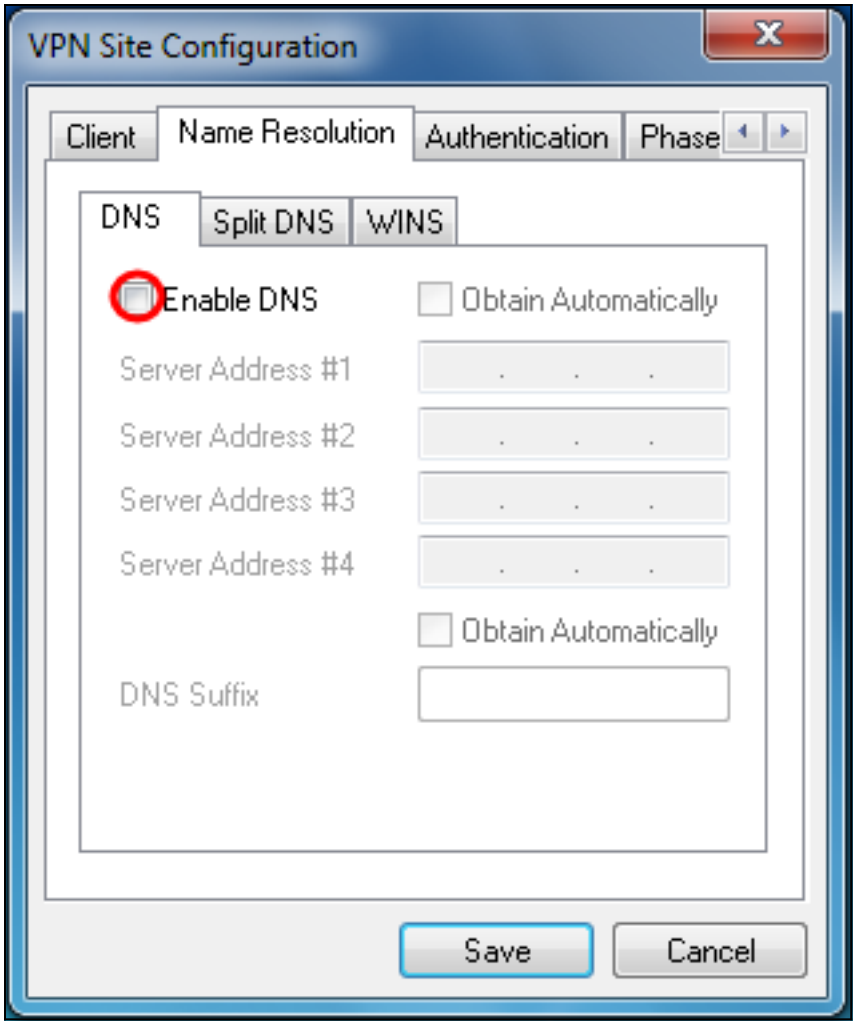
·Abilita: le estensioni del protocollo NAT verranno utilizzate solo se il gateway VPN indica il supporto durante le negoziazioni e se viene rilevato NAT.

·Force-Draft: la versione bozza delle estensioni del protocollo NAT verrà utilizzata indipendentemente dal fatto che il gateway VPN indichi o meno il supporto durante le negoziazioni o che venga rilevato NAT.

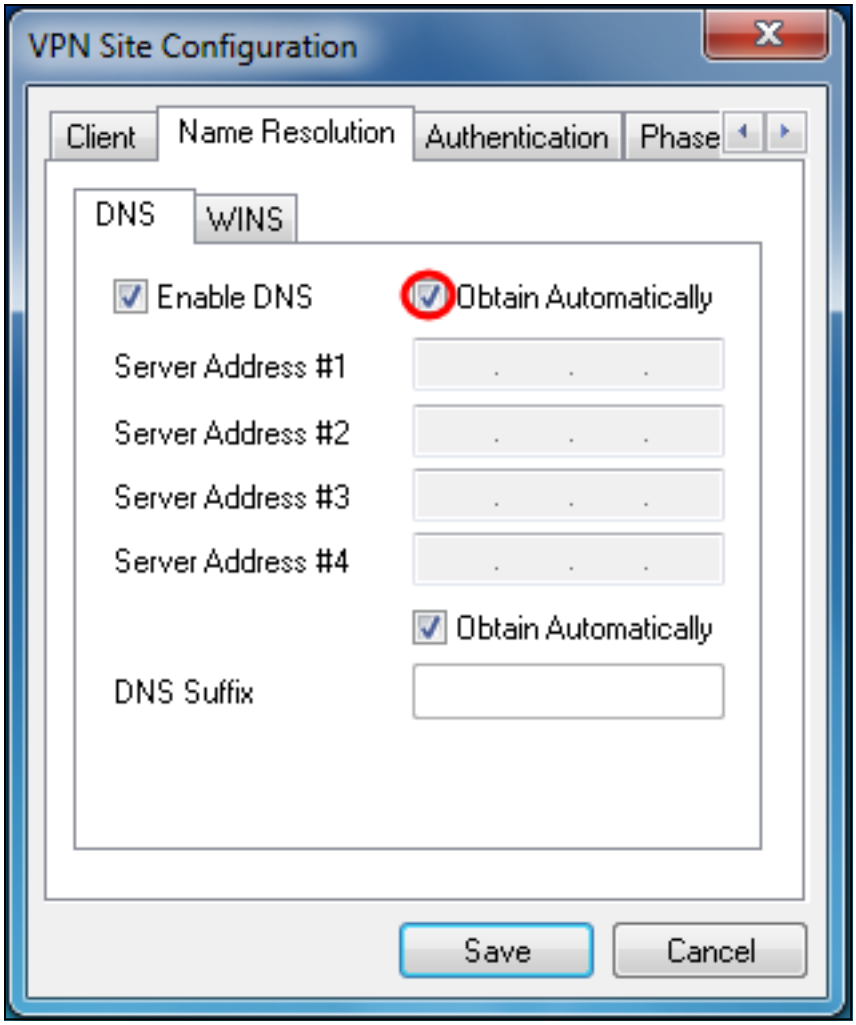
·Force-RFC: la versione RFC del protocollo NAT verrà utilizzata indipendentemente dal fatto che il gateway VPN indichi o meno il supporto durante le negoziazioni o che sia stato rilevato NAT.

·Force-Cisco-UDP: forza l'incapsulamento UDP per i client VPN senza NAT.

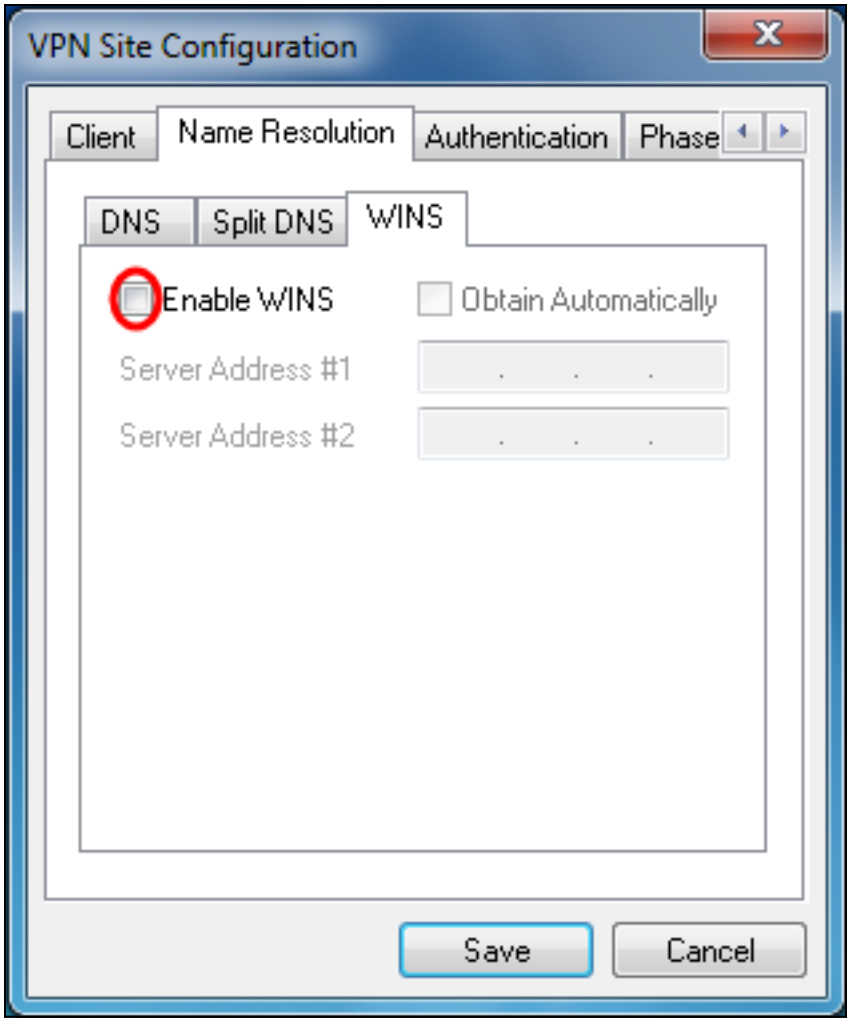
Passaggio 6. Fare clic sulla scheda *Risoluzione nomi* e selezionare la casella di controllo **Abilita DNS** se si desidera abilitare il DNS. Se per la configurazione del sito non sono necessarie impostazioni DNS specifiche, deselezionare la casella di controllo **Abilita DNS**.



Passaggio 7. (Facoltativo) Se il gateway remoto è configurato per supportare Configuration Exchange, il gateway è in grado di fornire automaticamente le impostazioni DNS. In caso contrario, verificare che la casella di controllo **Ottieni automaticamente** sia deselezionata e immettere manualmente un indirizzo server DNS valido.

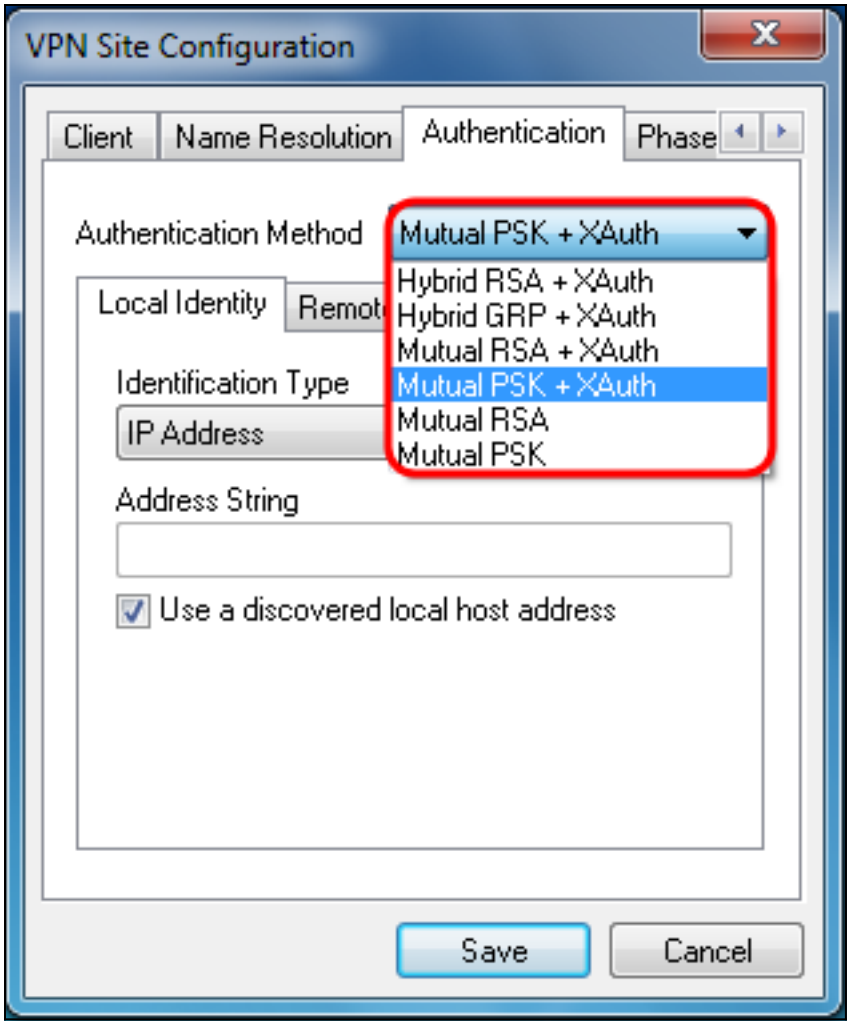


Passaggio 8. (Facoltativo) Fare clic sulla scheda *Risoluzione nome*, selezionare la casella di controllo **Abilita WINS** se si desidera abilitare Windows Internet Name Server (WINS). Se il gateway remoto è configurato per supportare Configuration Exchange, il gateway è in grado di fornire automaticamente le impostazioni WINS. In caso contrario, verificare che la casella di controllo **Ottieni automaticamente** sia deselezionata e immettere manualmente un indirizzo di server WINS valido.



Nota: Fornendo informazioni sulla configurazione di WINS, un client sarà in grado di risolvere i nomi WINS utilizzando un server situato nella rete privata remota. Ciò è utile quando si tenta di accedere a risorse di rete di Windows remote utilizzando un nome percorso Uniform Naming Convention. Il server WINS appartiene in genere a un controller di dominio di Windows o a un server Samba.

Passaggio 9. Fare clic sulla scheda *Authentication* (Autenticazione) e selezionare **Mutual PSK + XAuth** nell'elenco a discesa *Authentication Method* (Metodo di autenticazione).



Le opzioni disponibili sono definite come segue:

·Hybrid RSA + XAuth: credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno nel formato dei file di certificato PEM o PKCS12 o del tipo dei file di chiave.

·Hybrid GRP + XAuth: credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno sotto forma di file di certificato PEM o PKCS12 e di una stringa segreta condivisa.

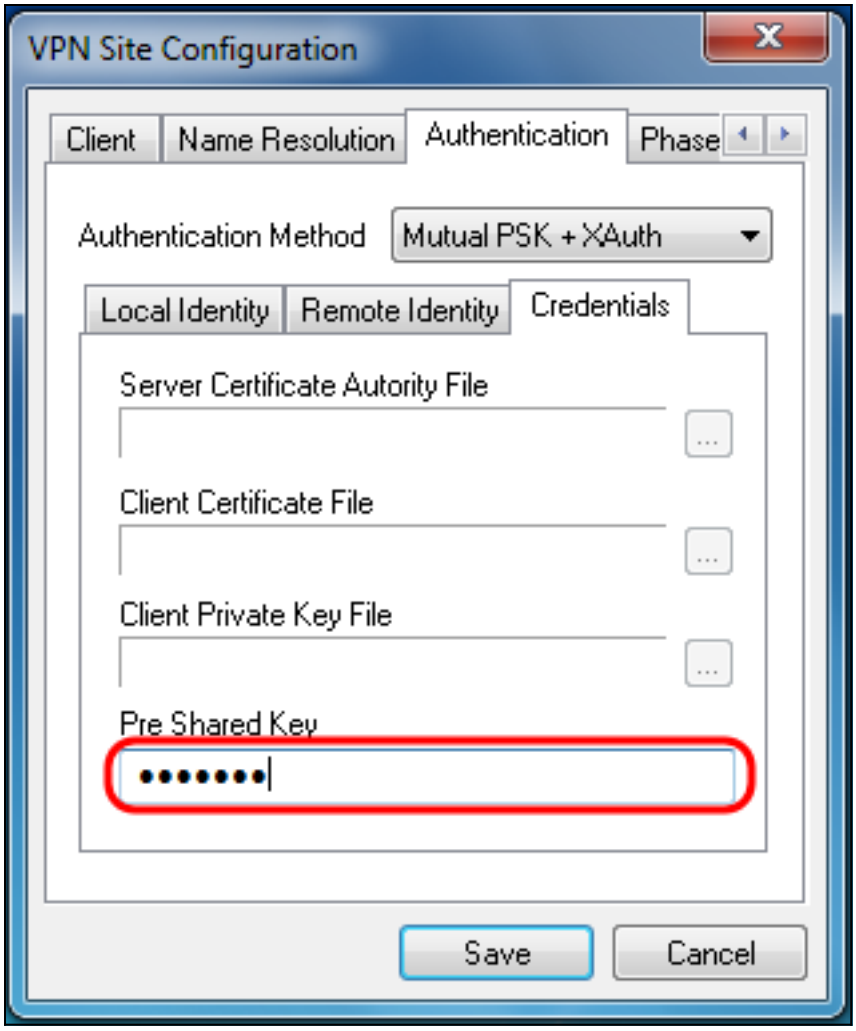
·RSA + XAuth reciproci: client e gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in formato PEM o PKCS12, file di certificato o tipo di chiave.

·PSK reciproco + XAuth: il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.

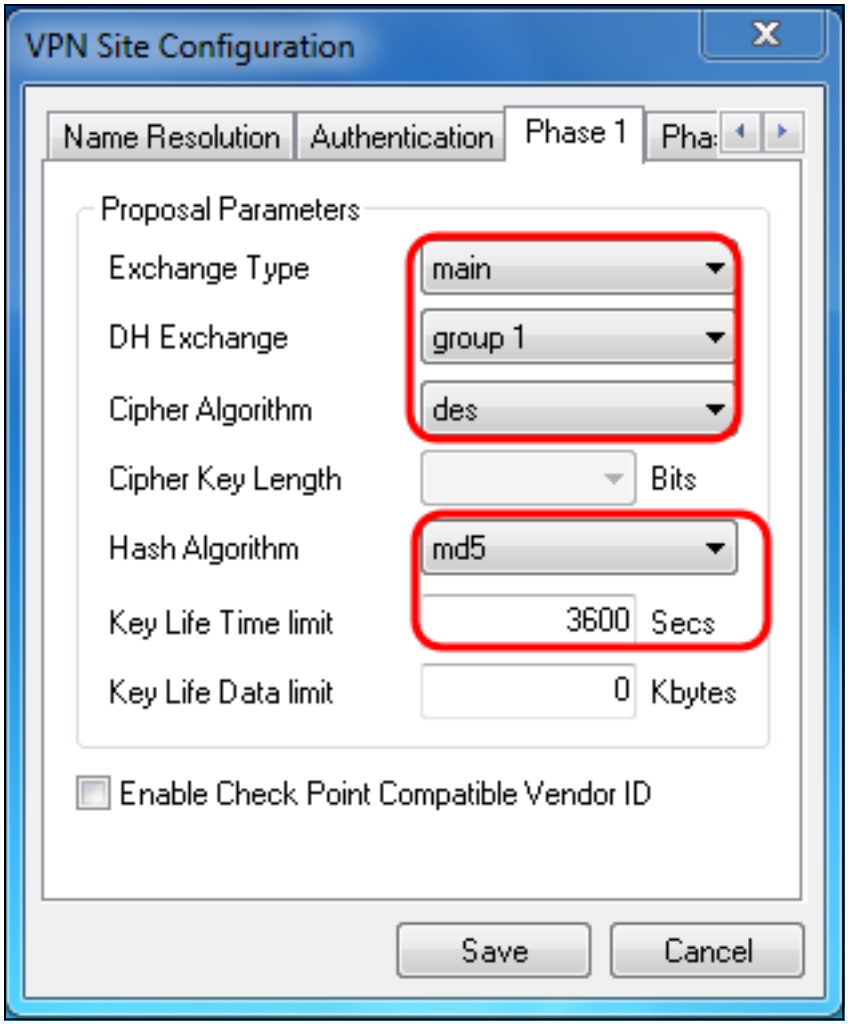
·RSA reciproca: client e gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in formato PEM o PKCS12, file di certificato o tipo di chiave.

·PSK reciproco: il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.

Passaggio 10. Nella sezione *Autenticazione*, fare clic sulla scheda secondaria *Credenziali* e immettere la stessa chiave precondivisa configurata nella pagina *IPsec VPN Server Setup* del campo *Chiave precondivisa*.



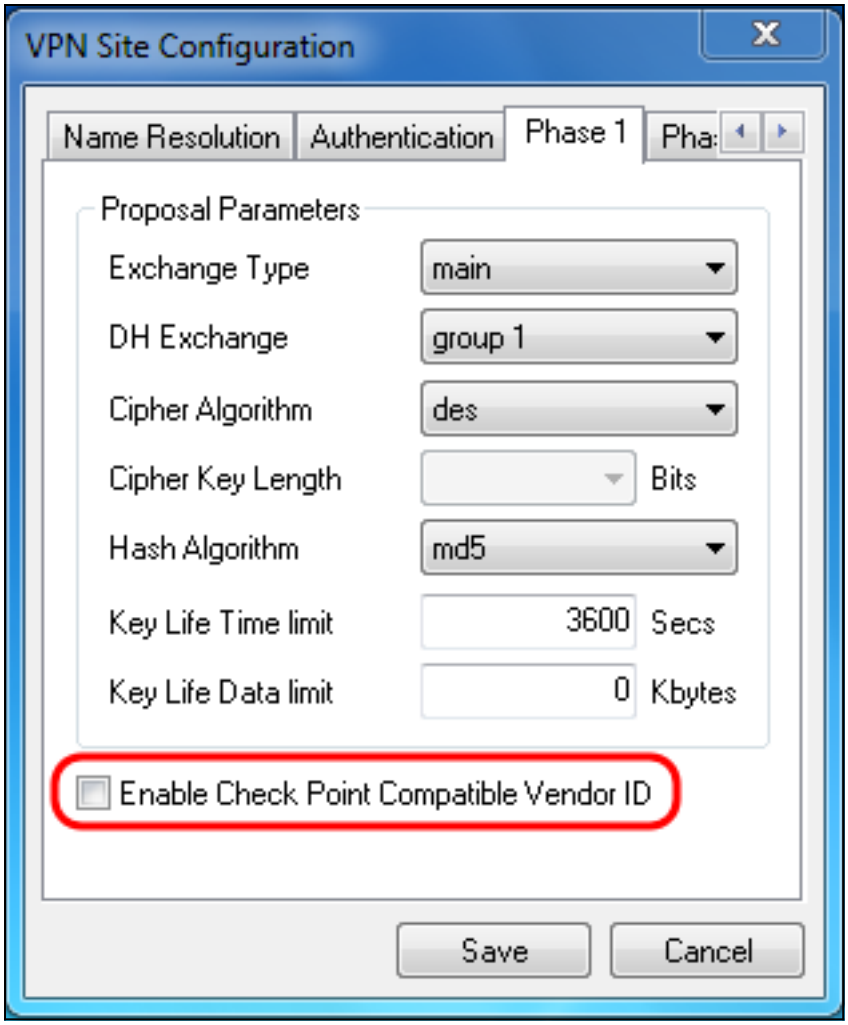
Passaggio 11. Fare clic sulla scheda *Fase 1*. Configurare i seguenti parametri in modo che abbiano le stesse impostazioni configurate per RV130/RV130W nel passaggio 2 della sezione *IPSec VPN Server User Configuration* di questo documento.



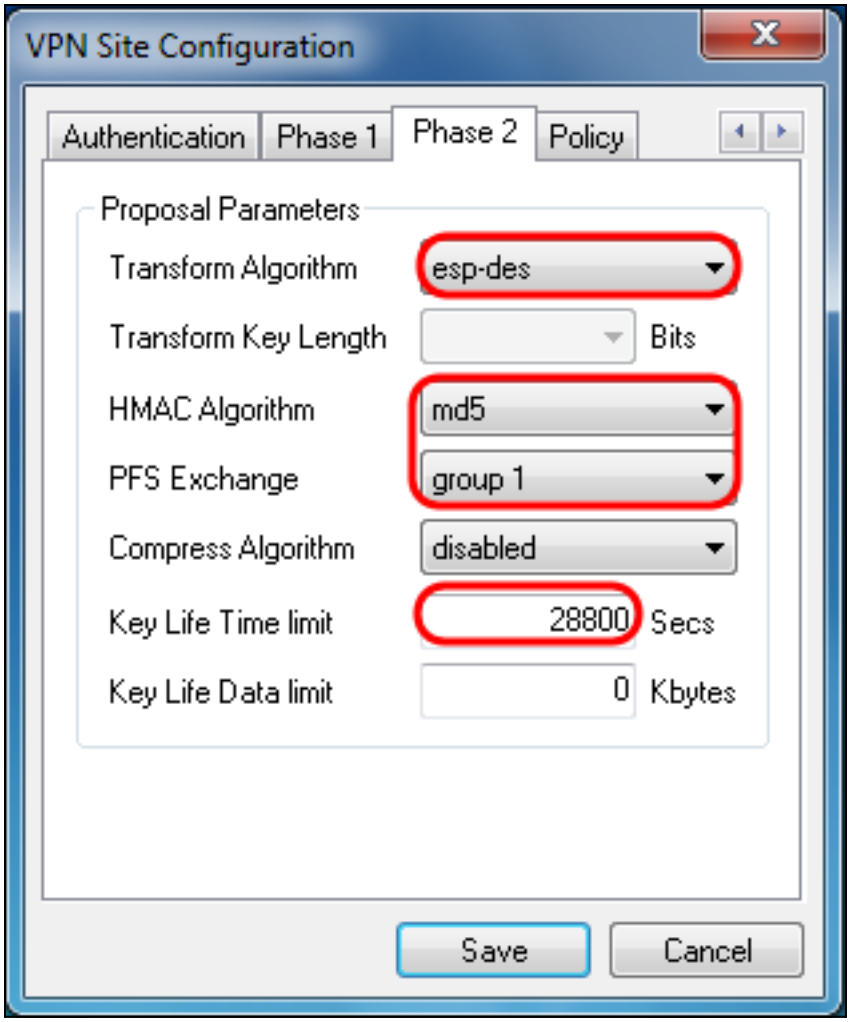
I parametri in Shrew Soft devono corrispondere alle configurazioni RV130/RV130W nella fase 1 come segue:

- "Exchange Type" deve corrispondere a "Exchange Mode".
- "DH Exchange" deve corrispondere a "DH Group".
- "Cipher Algorithm" deve corrispondere a "Encryption Algorithm".
- "Hash Algorithm" deve corrispondere a "Authentication Algorithm".

Passaggio 12. (Facoltativo) Se il gateway offre un ID fornitore compatibile con Cisco durante le negoziazioni della fase 1, selezionare la casella di controllo **Abilita ID fornitore compatibile con checkpoint**. Se il gateway non funziona o non si è certi, lasciare deselezionata la casella di controllo.



Passaggio 13. Fare clic sulla scheda *Fase 2*. Configurare i seguenti parametri in modo che abbiano le stesse impostazioni configurate per RV130/RV130W nel passaggio 2 della sezione *IPSec VPN Server User Configuration* di questo documento.



I parametri in Shrew Soft devono corrispondere alle configurazioni RV130/RV130W nella fase 2 come segue:

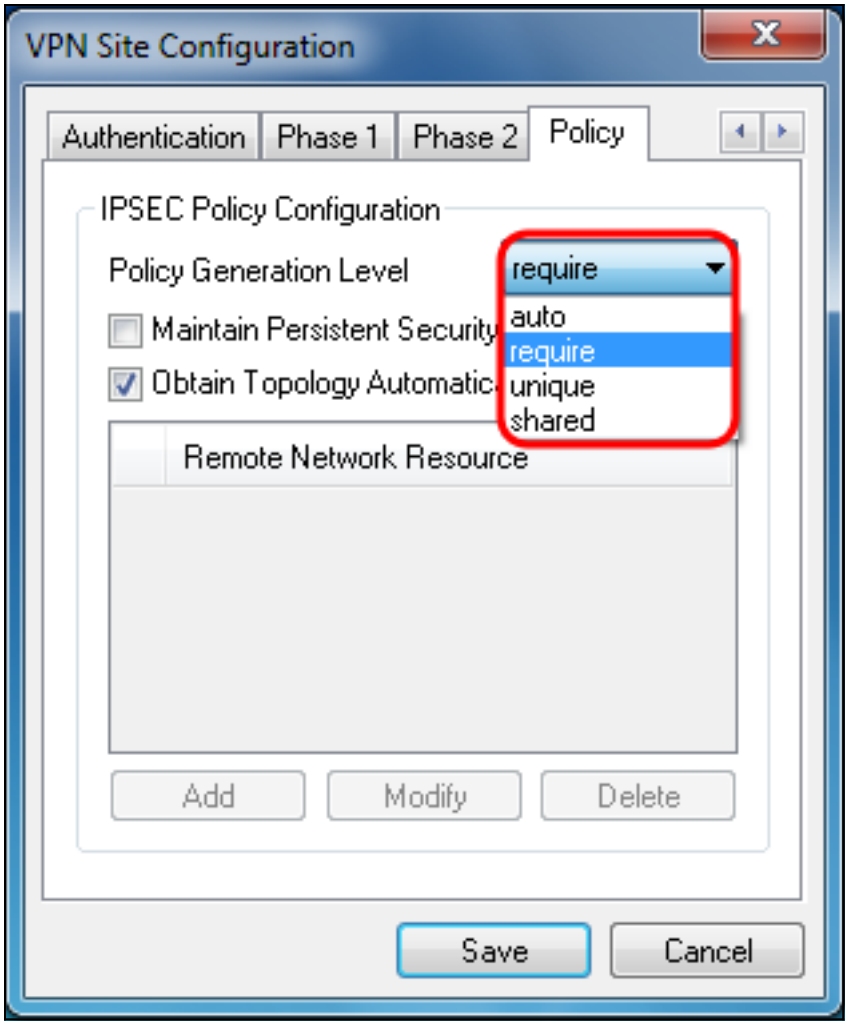
·"Transform Algorithm" deve corrispondere a "Encryption Algorithm".

·"HMAC Algorithm" deve corrispondere a "Authentication Algorithm".

·PFS "Exchange" deve corrispondere a "DH Group" se PFS Key Group è abilitato su RV130/RV130W. In caso contrario, selezionare **Disattivato**.

·"Key Life Time limit" deve corrispondere a "IPSec SA Lifetime".

Passaggio 14. Fare clic sulla scheda *Criterio* e selezionare **obbligatorio** nell'elenco a discesa *Livello di generazione criteri*. L'opzione *Policy Generation Level* (Livello di generazione criteri) consente di modificare il livello di generazione dei criteri IPSec. I diversi livelli forniti nell'elenco a discesa corrispondono ai comportamenti di negoziazione delle associazioni di protezione IPSec implementati da diverse implementazioni di fornitori.



Le opzioni disponibili sono definite come segue:

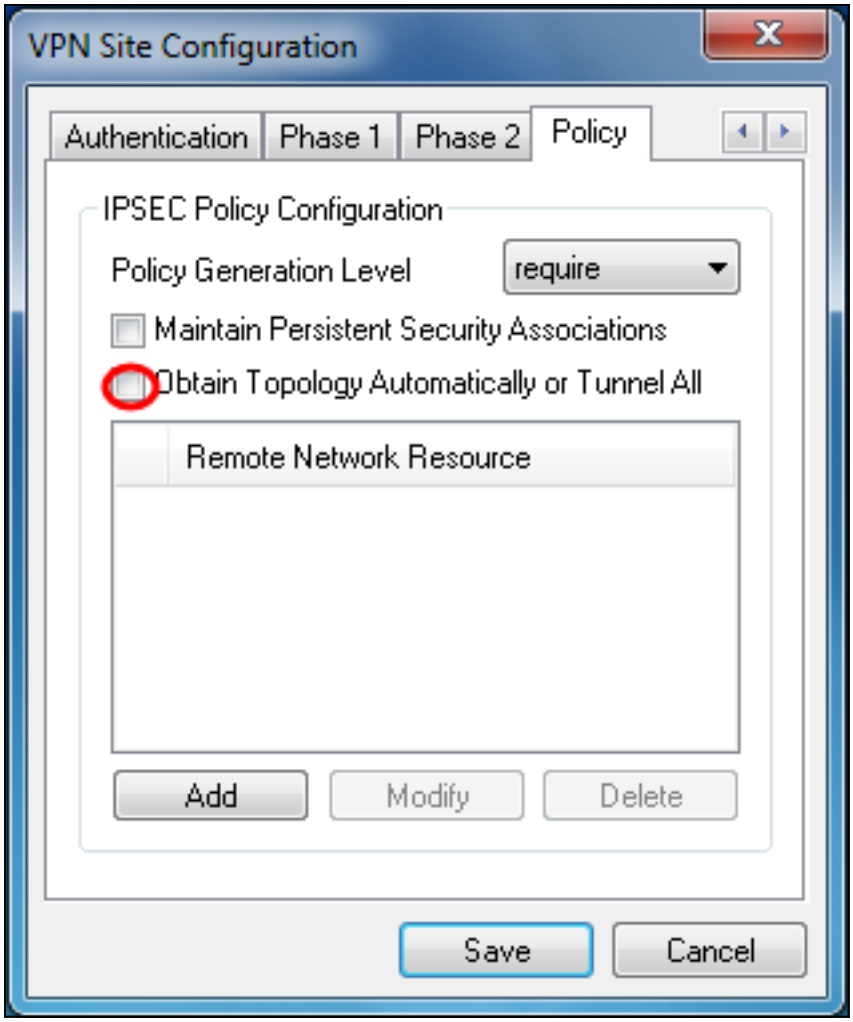
·Automatico: il client determina automaticamente il livello di criteri IPSec appropriato.

·Richiedi: il client non negozierà un'associazione di sicurezza (SA) univoca per ogni criterio. I criteri vengono generati utilizzando l'indirizzo pubblico locale come ID dei criteri locali e le risorse di rete remota come ID dei criteri remoti. La proposta per la fase 2 utilizzerà gli ID dei criteri durante la negoziazione.

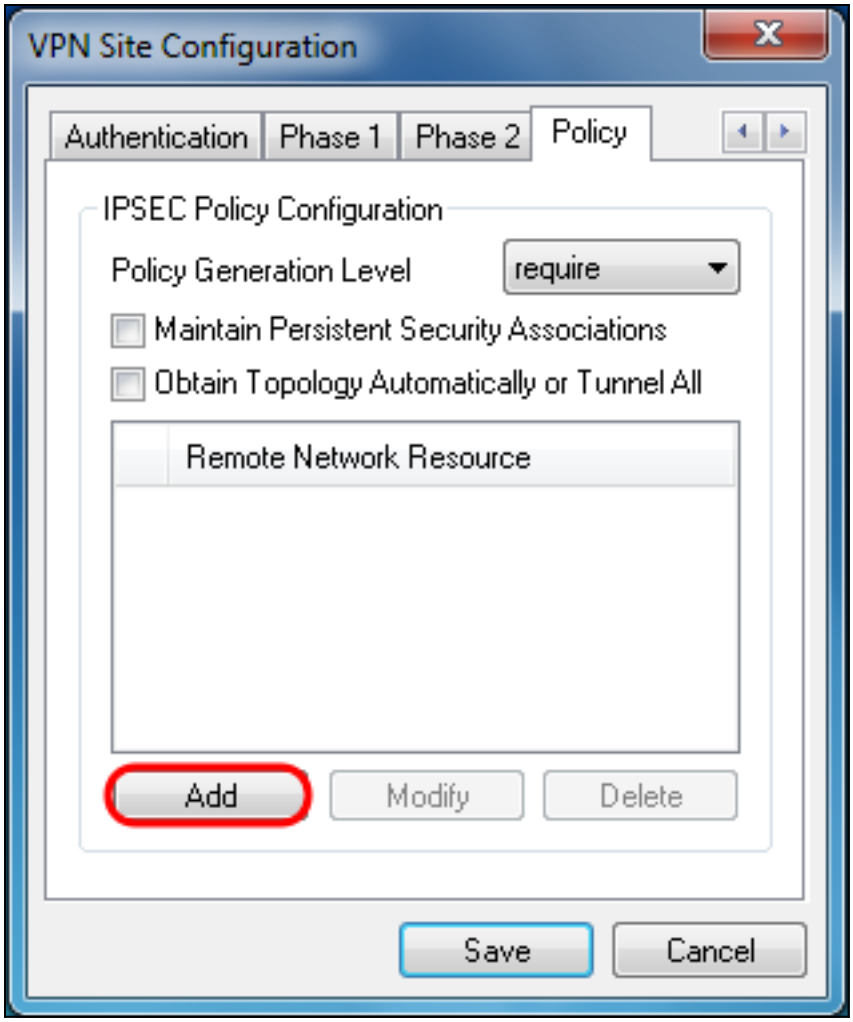
·Univoco: il client negozia un'associazione di protezione univoca per ogni criterio.

·Condiviso: le policy vengono generate al livello richiesto. La proposta per la fase 2 utilizzerà l'ID del criterio locale come ID locale e Any (0.0.0.0/0) come ID remoto durante la negoziazione.

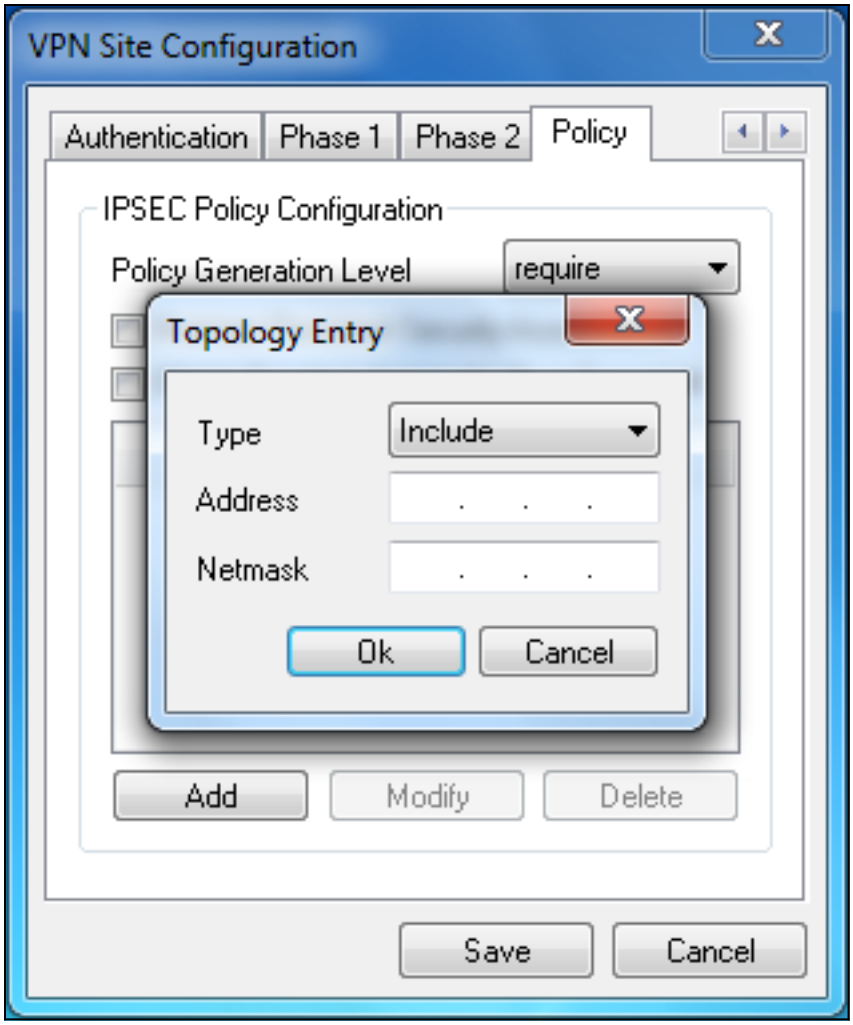
Passaggio 15. Deselezionare la casella di controllo **Ottieni topologia automaticamente o Tunnel tutto**. Questa opzione modifica la modalità di configurazione dei criteri di sicurezza per la connessione. Quando è disattivato, è necessario eseguire la configurazione manuale. Se questa opzione è abilitata, viene eseguita la configurazione automatica.



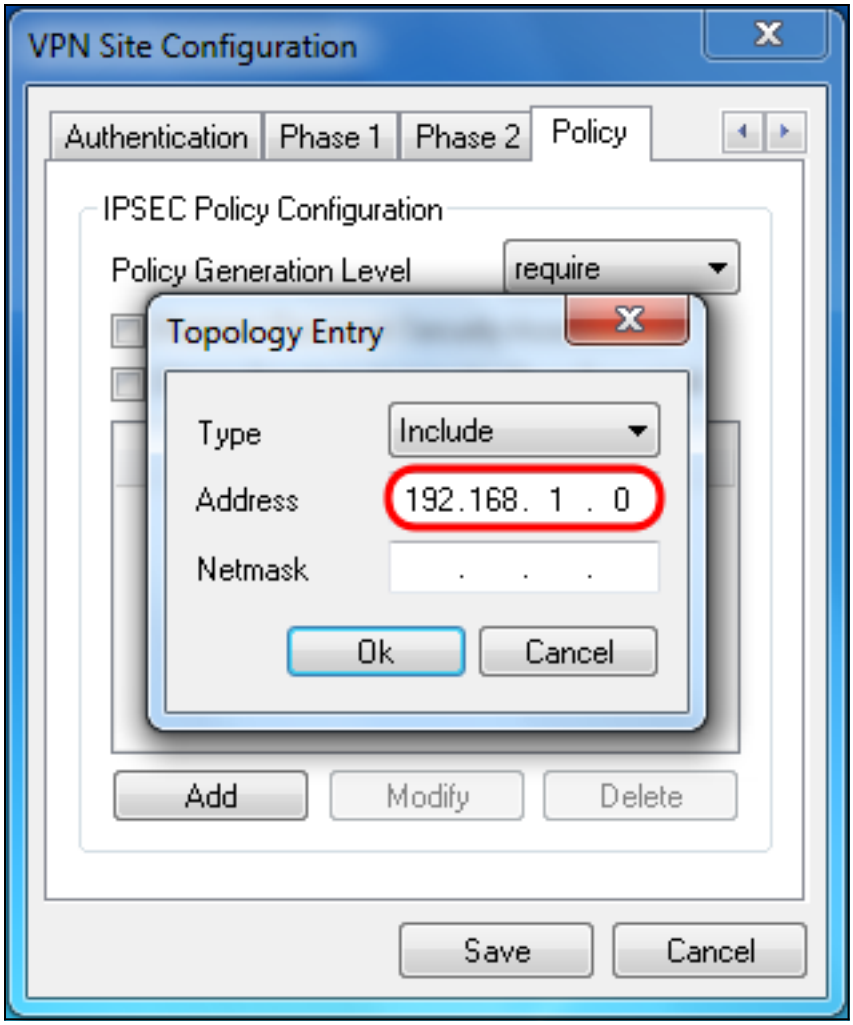
Passaggio 16. Per aggiungere la risorsa di rete remota a cui si desidera connettersi, fare clic su **Add** (Aggiungi). Le risorse di rete remote includono l'accesso remoto ai desktop, le risorse di reparto, le unità di rete e la posta elettronica protetta.



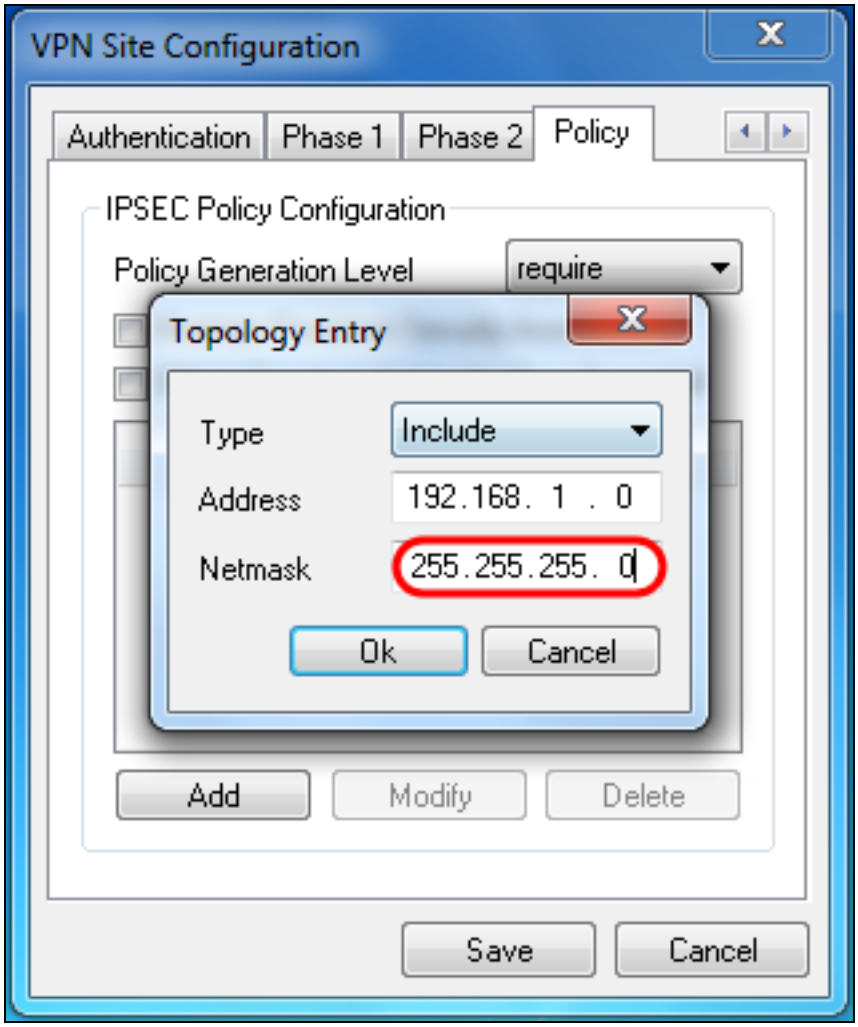
Viene visualizzata la finestra *Voce topologia*:



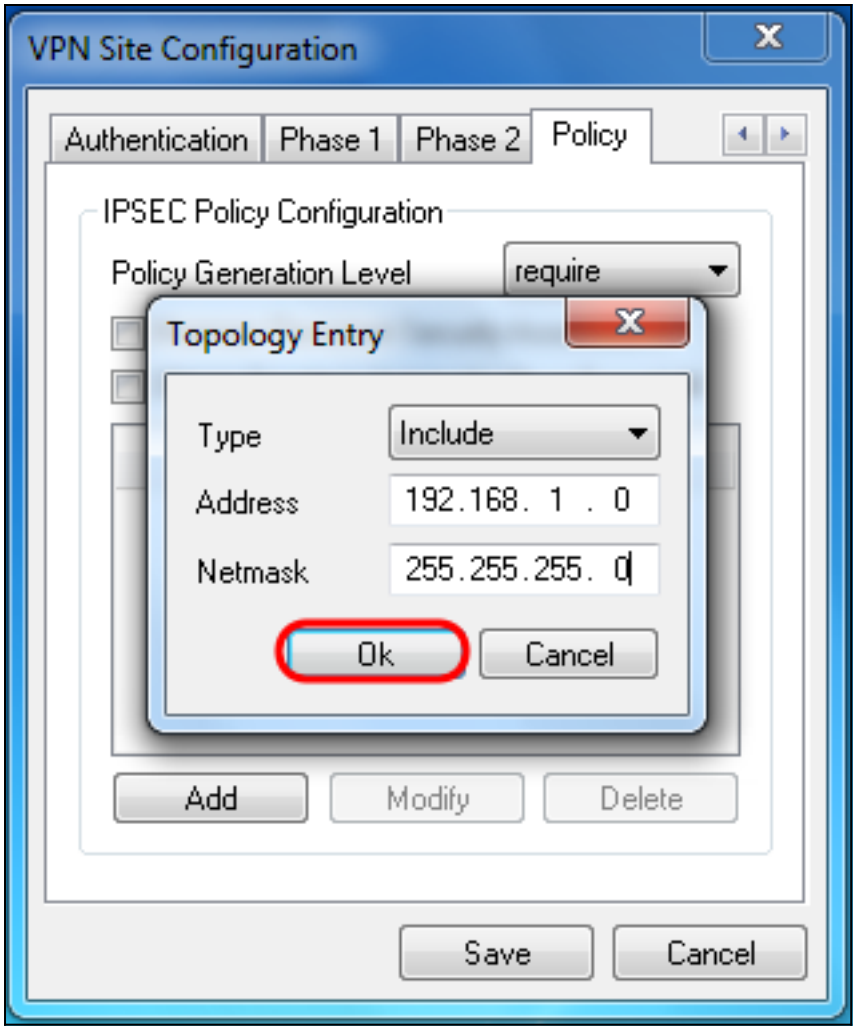
Passaggio 17. Nel campo *Address* (Indirizzo), immettere l'ID subnet della RV130/RV130W. L'indirizzo deve corrispondere al campo *IP Address* nel passaggio 2 della sezione *IPSec VPN Server Setup and User Configuration* di questo documento.



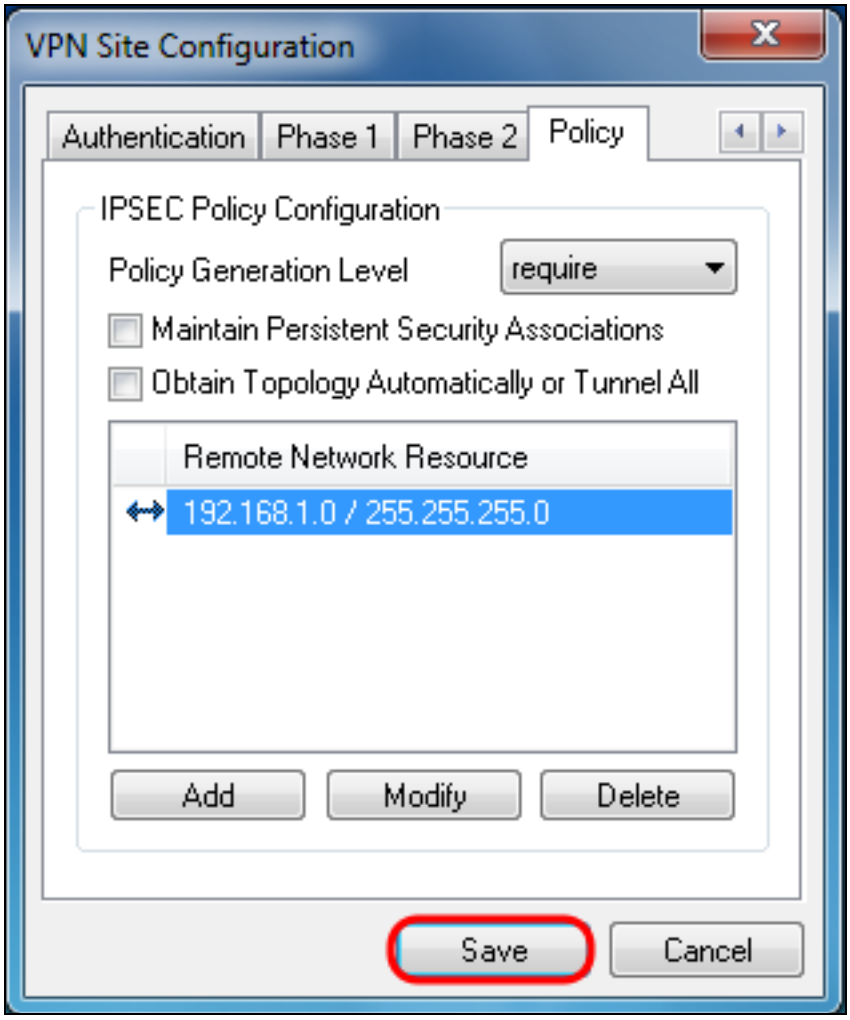
Passaggio 18. Nel campo *Netmask*, immettere la subnet mask della rete locale dell'RV130/RV130W. La netmask deve corrispondere al campo *Subnet Mask* nel passaggio 2 della sezione *IPSec VPN Server User Configuration* in questo documento.



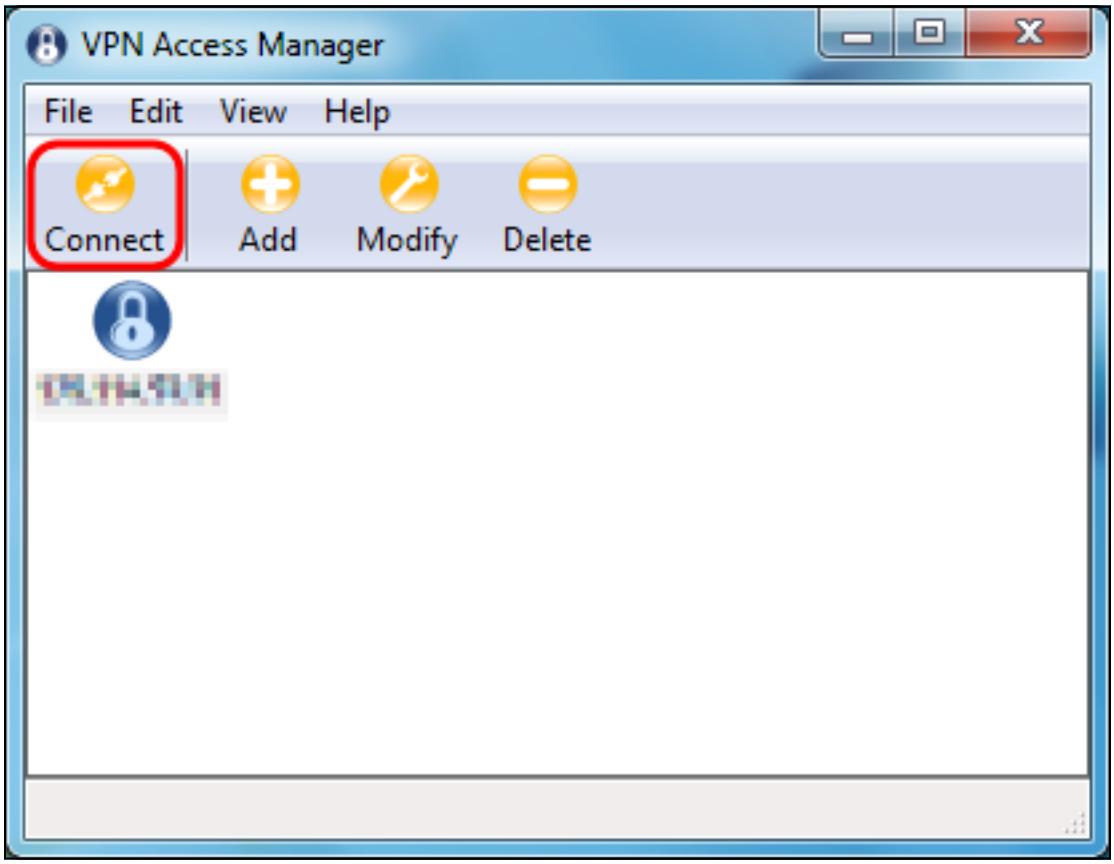
Passaggio 19. Fare clic su **OK** per completare l'aggiunta della risorsa di rete remota.



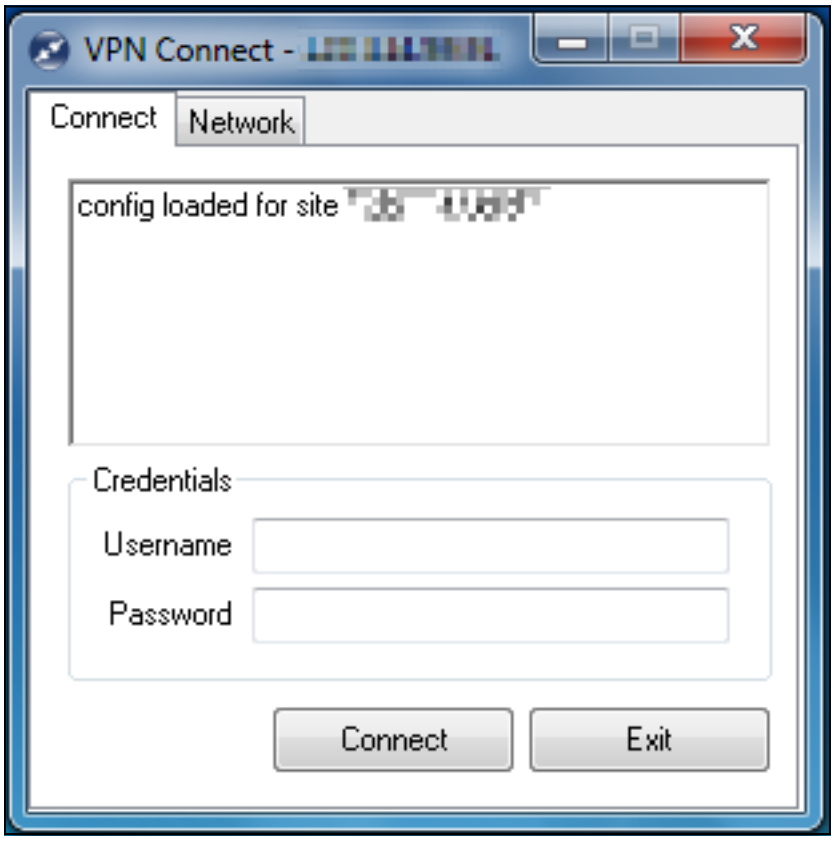
Passaggio 20. Fare clic su **Save** per salvare le configurazioni per la connessione al sito VPN.



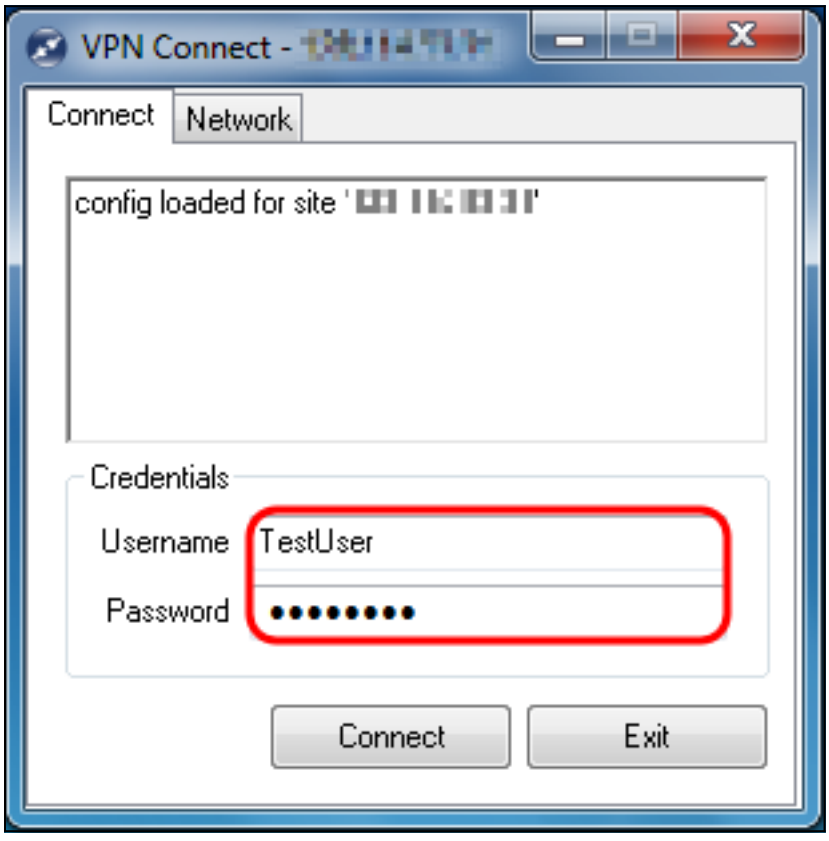
Passaggio 21. Tornare alla finestra *VPN Access Manager* per selezionare il sito VPN configurato e fare clic sul pulsante **Connect**.



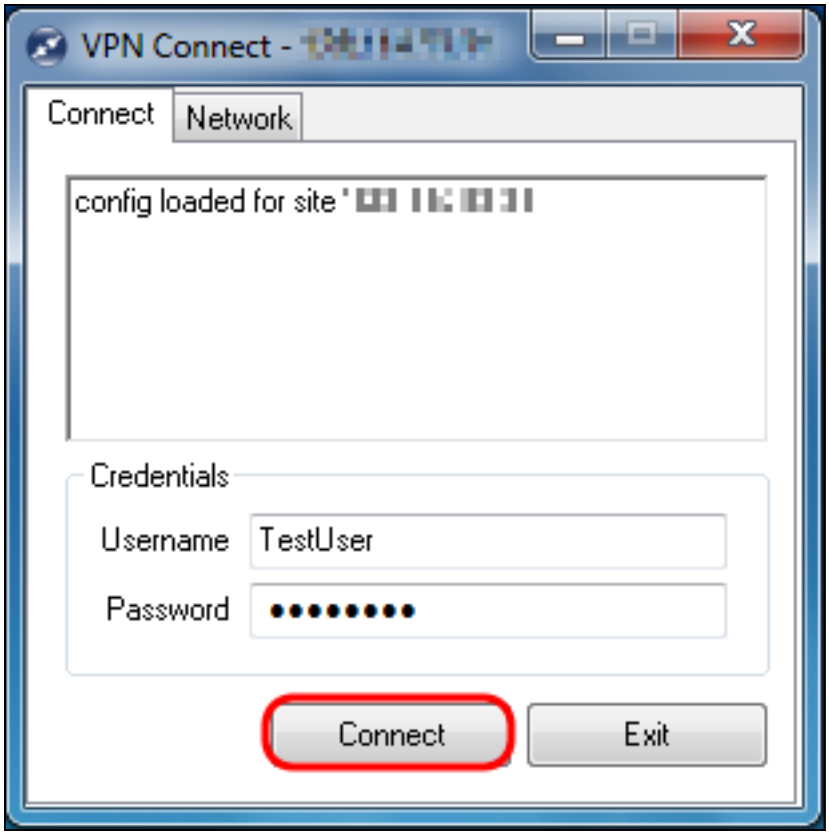
Viene visualizzata la finestra *VPN Connect*.



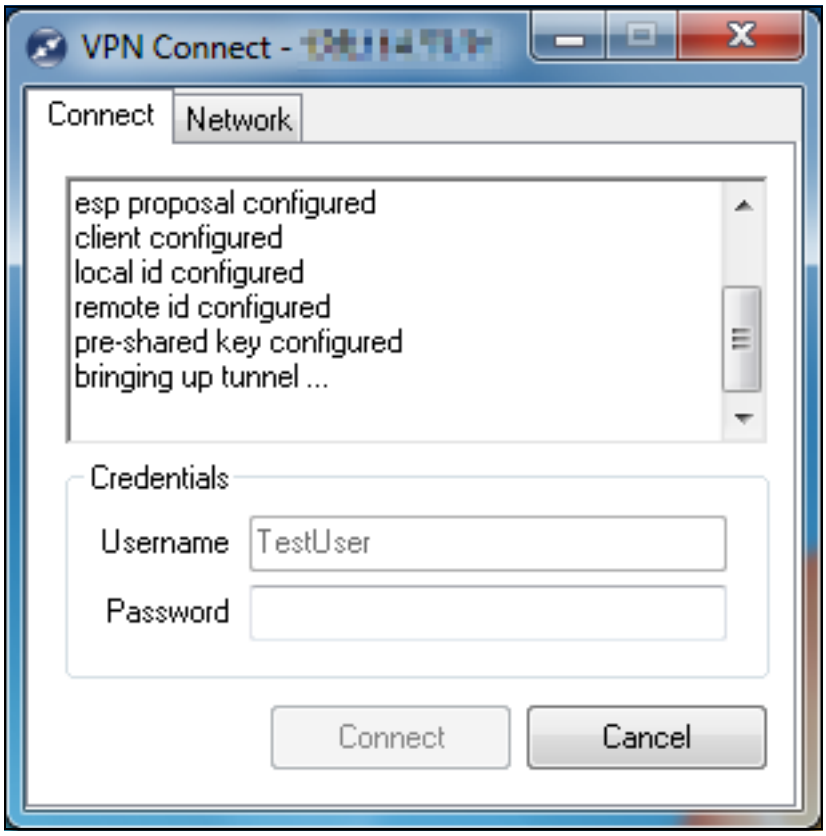
Passaggio 2. Nella sezione *Credenziali*, immettere il nome utente e la password dell'account configurato nel passaggio 4 della sezione *Configurazione utente server VPN IPSec* di questo documento.

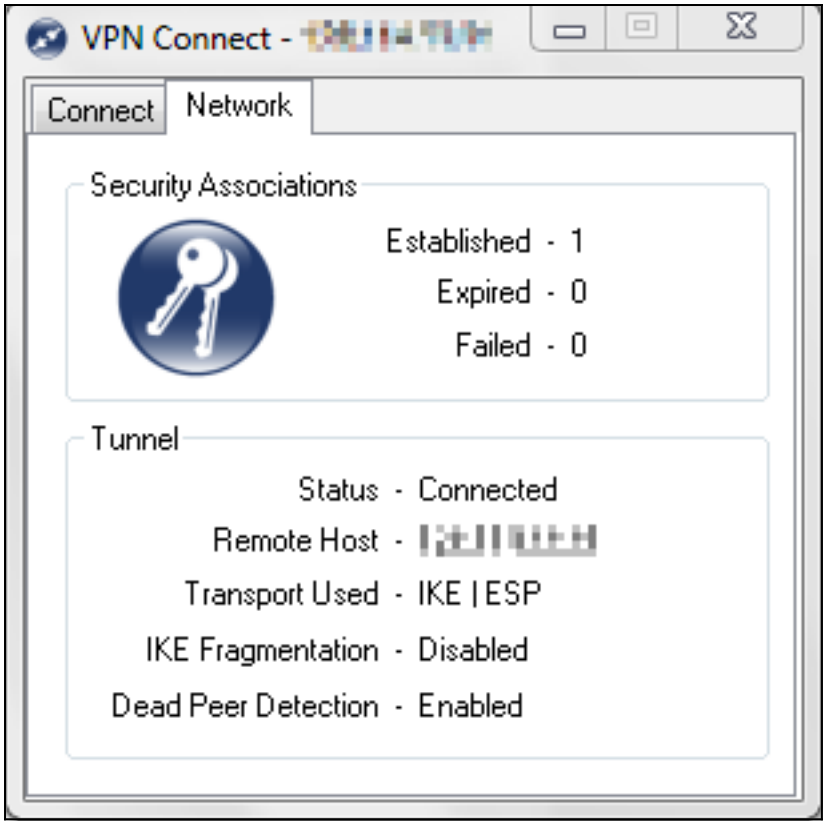


Passaggio 23. Fare clic su **Connect** to VPN (Connetti a VPN) in RV130/RV130W.



Il tunnel VPN IPSec viene stabilito e il client VPN può accedere alla risorsa sottostante la LAN RV130/RV130W.





Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).