Configurazione di Shrew Soft VPN Client con RV160 e RV260

Obiettivo

L'obiettivo di questo documento è mostrare come configurare le impostazioni necessarie per connettere il client Show Soft VPN con router serie RV160 o RV260.

Introduzione alle nozioni di base della VPN

Una rete privata virtuale (VPN) è un ottimo modo per connettere utenti remoti a una rete protetta. Stabilisce una connessione crittografata su una rete meno sicura come Internet.

Un tunnel VPN stabilisce una rete privata in grado di inviare i dati in modo sicuro utilizzando la crittografia e l'autenticazione. Le filiali utilizzano spesso una connessione VPN, in quanto è utile e necessario per consentire ai dipendenti di accedere alle risorse interne, anche se si trovano fuori sede.

Il router RV160 supporta fino a 10 tunnel VPN, mentre il router RV260 ne supporta fino a 20.

In questo documento viene descritto come configurare il router RV160/RV260 e il client Show Soft VPN. Verrà illustrato come creare un gruppo di utenti, un account utente, un profilo IPSec e un profilo da client a sito. Sul client Soft VPN, viene illustrato come configurare le schede Generale, Client, Risoluzione nome, Autenticazione, Fase 1 e Fase 2.

Quali sono i pro e i contro se voglio usare una VPN?

Le VPN risolvono scenari di utilizzo reali comuni a molti settori e tipi di aziende. La tabella seguente mostra alcuni dei pro e dei contro dell'utilizzo di una VPN.

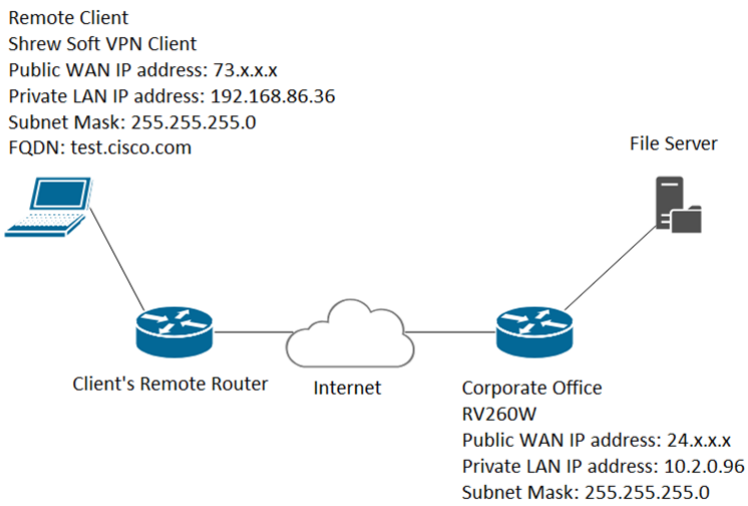
Pro	Svantaggi
Garantisce comunicazioni sicure, comodità e accessibilità con diritti di accesso personalizzati per singoli utenti, ad esempio dipendenti, collaboratori esterni o partner.	Può verificarsi una velocità di connessione lenta. La crittografia avanzata richiede tempo e risorse per garantire l'anonimato e la sicurezza. La crittografia del traffico di rete in genere richiede un maggiore sovraccarico. È possibile trovare un paio di provider VPN che mantengono una buona velocità di connessione mantenendo l'anonimato e la sicurezza, ma di solito sono servizi a pagamento.
Aumenta la produttività estendendo la rete e le applicazioni aziendali.	Potenziale rischio per la sicurezza dovuto a configurazioni errate. La progettazione e l'implementazione di una VPN può essere complicata.

	È necessario affidare a un professionista esperto la configurazione della VPN per assicurarsi che la rete non venga compromessa.
Riduce i costi di comunicazione e aumenta la flessibilità.	Se si verifica una situazione in cui è necessario aggiungere una nuova infrastruttura o una nuova serie di configurazioni, possono verificarsi problemi tecnici dovuti all'incompatibilità, in particolare se si tratta di prodotti o fornitori diversi da quelli già in uso.
L'effettiva posizione geografica degli utenti è protetta e non esposta al pubblico o alle reti condivise come Internet.	
Protezione dei dati e delle risorse di rete riservati.	
Una VPN consente di aggiungere nuovi utenti o un gruppo di utenti senza la necessità di componenti aggiuntivi o una configurazione complessa.	

Topologia

Questa è una semplice topologia della rete.

Nota: L'indirizzo IP della WAN pubblica è sfocato.



Dispositivi interessati

- RV160

- RV260

Versione del software

- 1.0.0.xx (RV160 e RV260)

- Si consiglia 2.2.1 in quanto la versione 2.2.2 potrebbe presentare problemi di connettività con i router (Shrew Soft VPN Client Download)

Sommario

Creazione di gruppi di utenti

Nota importante: Lasciare l'account amministratore predefinito nel gruppo di amministratori e creare un nuovo account utente e un nuovo gruppo di utenti per Shrew Soft. Se si sposta l'account amministratore in un gruppo diverso, non sarà possibile accedere al router.

Passaggio 1. Accedere alla pagina di configurazione Web.

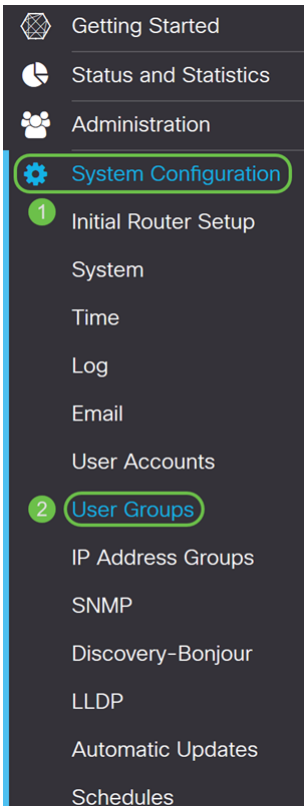
Router

cisco

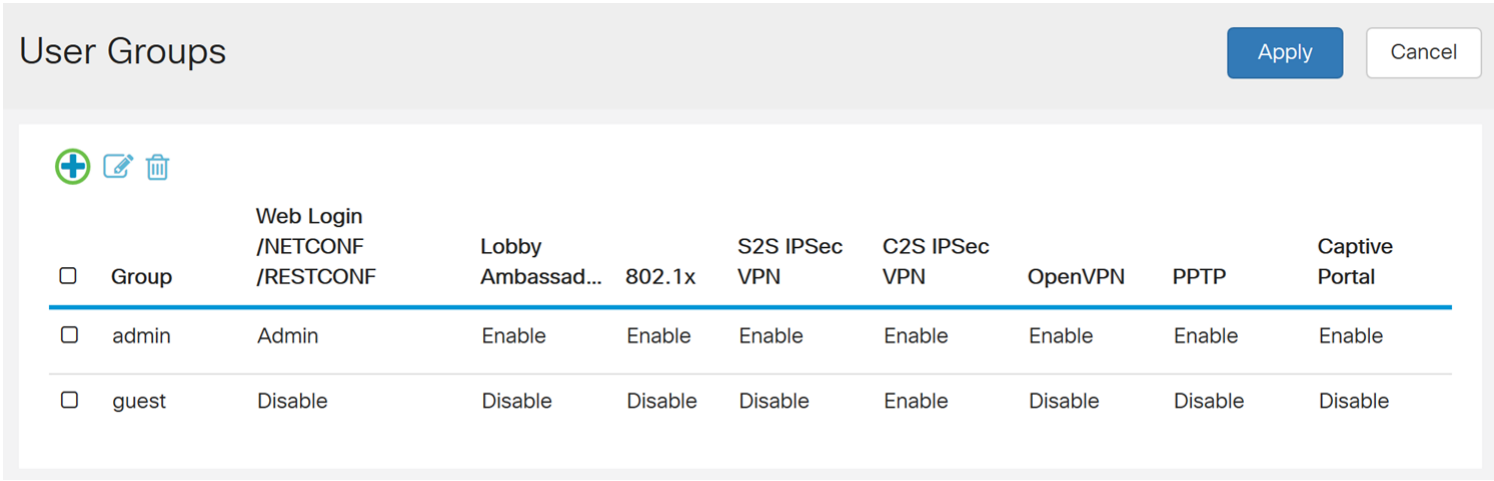
English

Login

Passaggio 2. Passare a **Configurazione di sistema > Gruppi di utenti**.



Passaggio 3. Fare clic sull'icona **più** per aggiungere un nuovo gruppo di utenti.



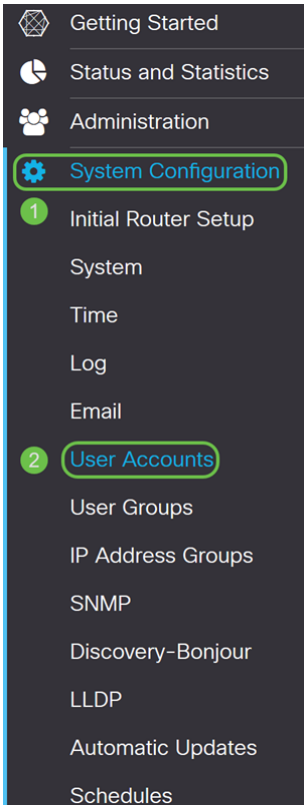
Passaggio 4. Inserire un nome per il gruppo nel campo *Nome gruppo*.

Verrà utilizzato **ShrewSoftGroup** come esempio.

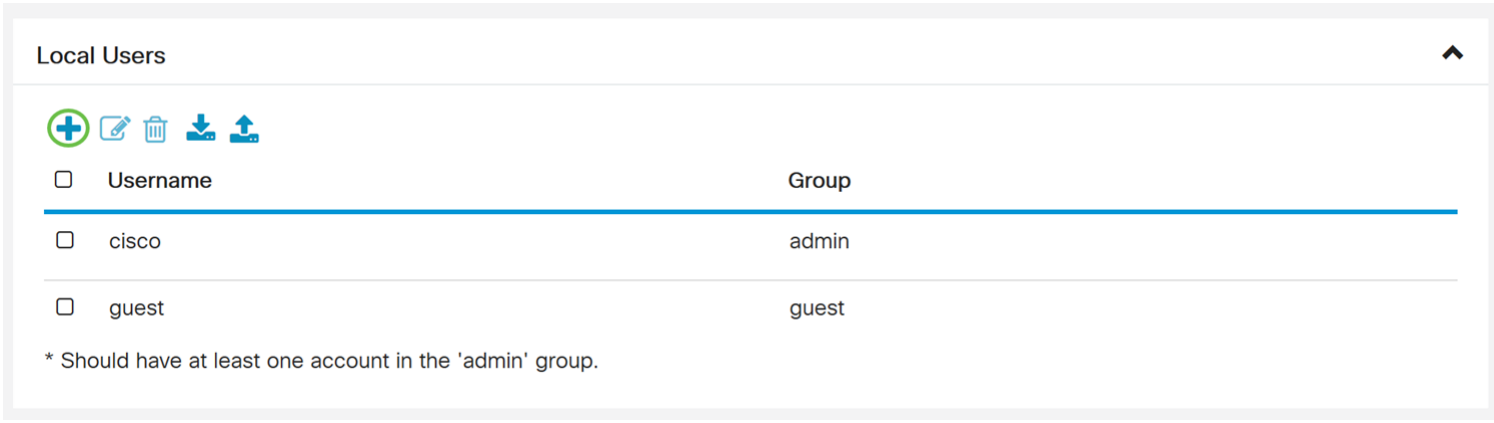
Passaggio 5. Premere **Applica** per creare un nuovo gruppo.

Creazione di account utente

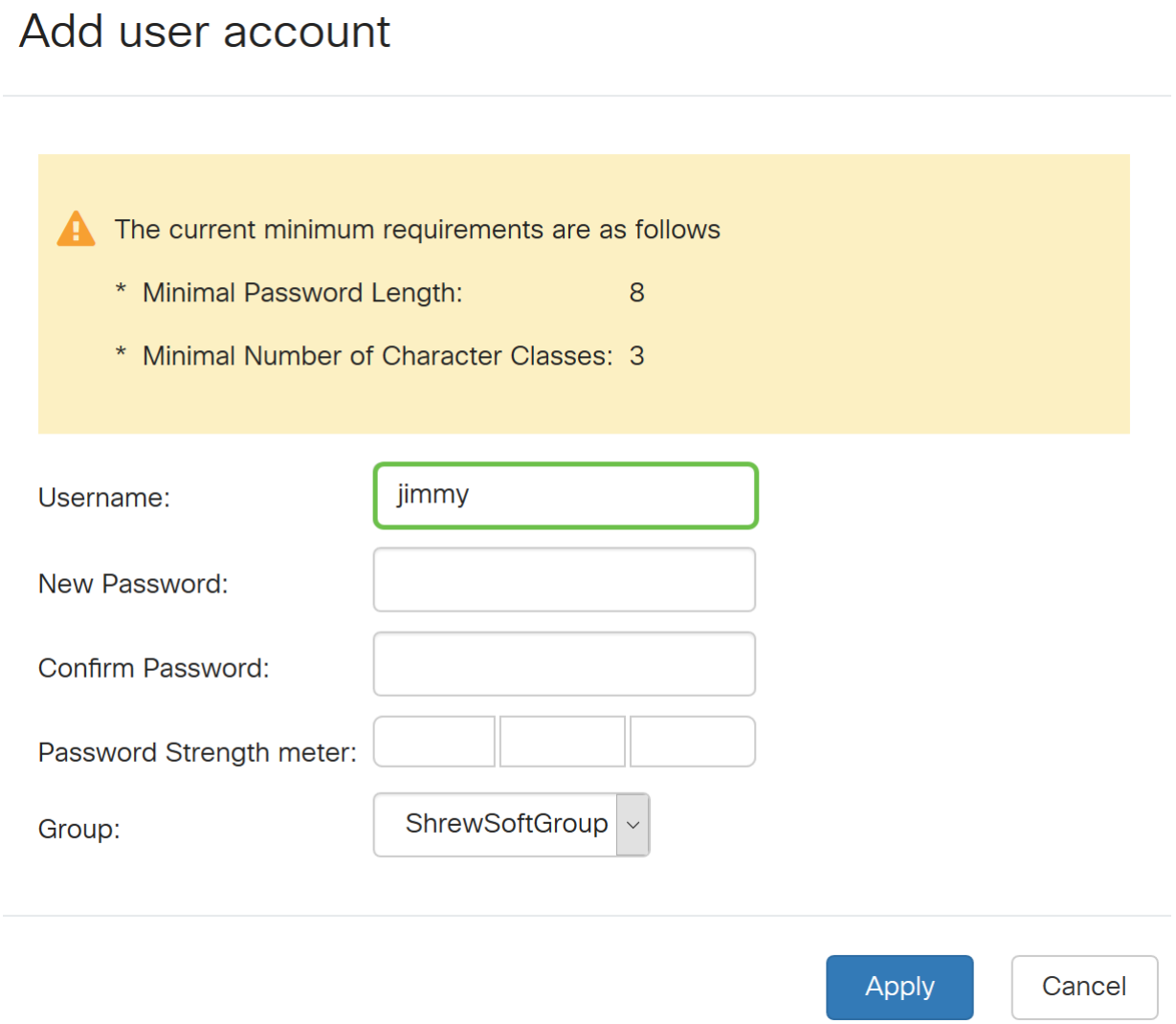
Passaggio 1. Passare a **Configurazione di sistema > Account utente**.



Passaggio 2. Scorrere verso il basso fino alla tabella *Utenti locali* e premere l'icona **più** per aggiungere un nuovo utente.

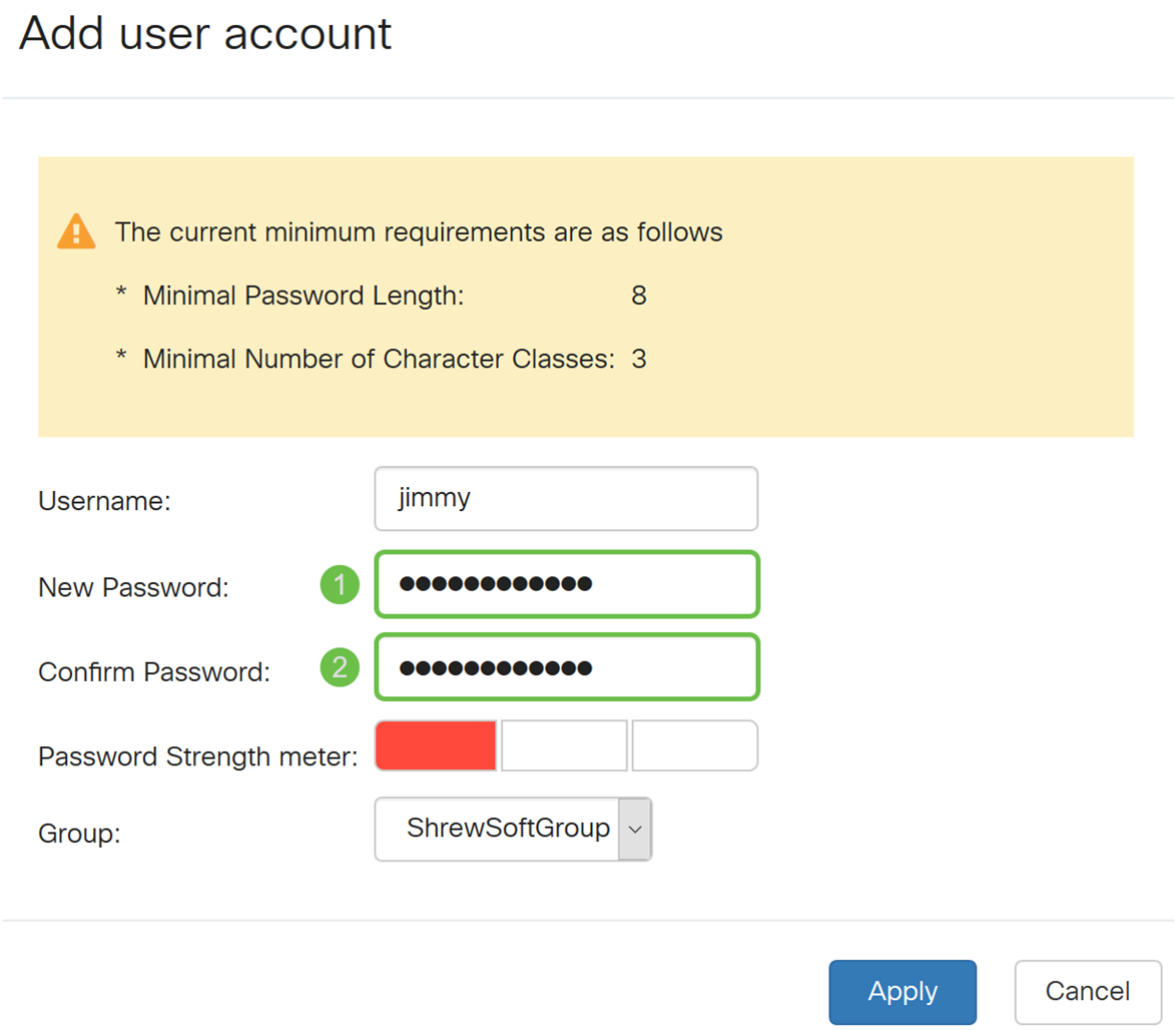


Passaggio 3. Viene visualizzata la pagina *Aggiungi account utente*. Immettere un nome utente per l'utente.

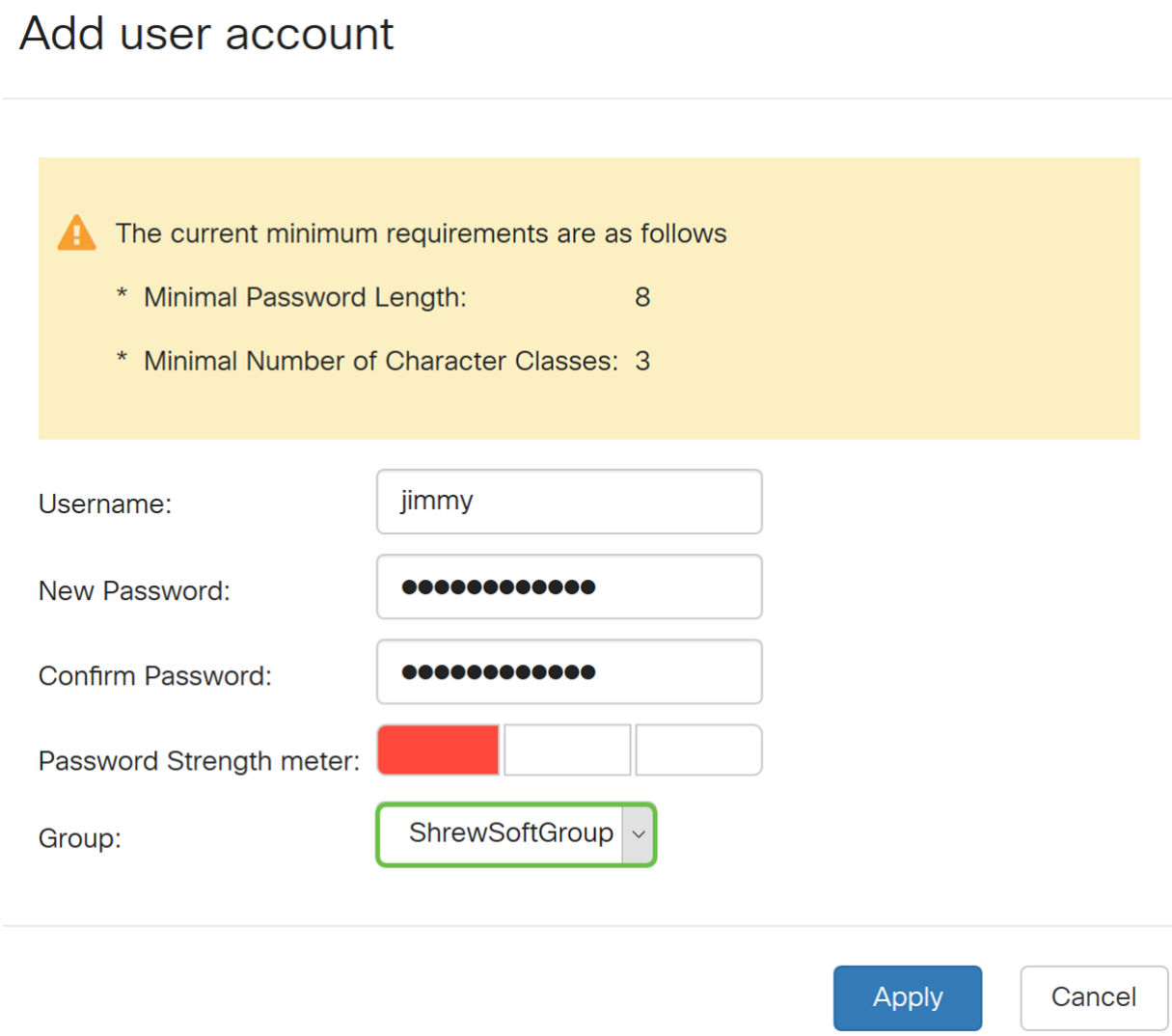


Passaggio 4. Immettere una password nel campo *Nuova password*. Immettere nuovamente la stessa password nel campo *Conferma password*. Nell'esempio, verrà utilizzata la password **CiscoTest123**.

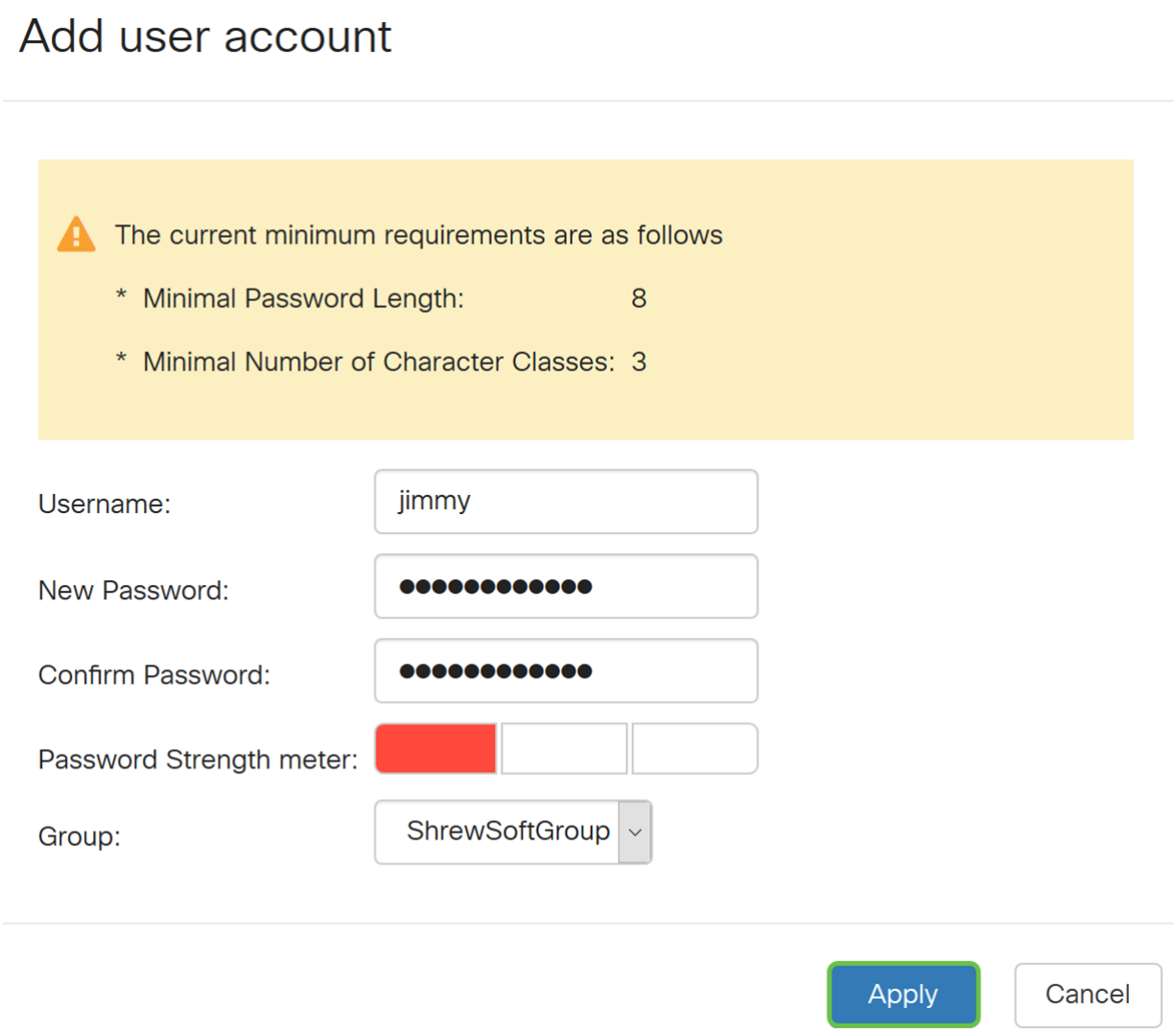
Nota: La password utilizzata è un esempio. È consigliabile rendere la password più complessa.



Passaggio 5. Nell'elenco a discesa *Gruppo* selezionare un gruppo in cui si desidera che l'utente si trovi.

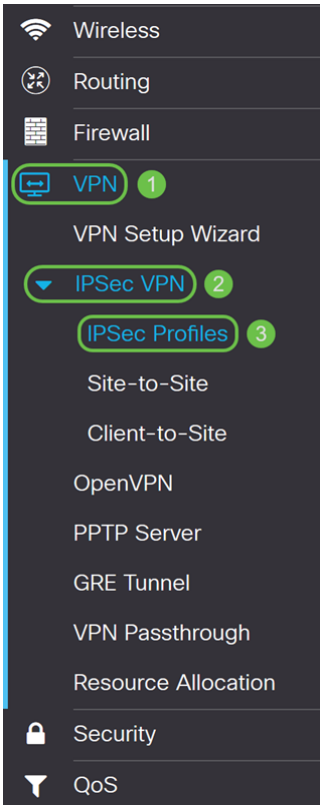


Passaggio 6. Premere **Applica** per creare un nuovo account utente.



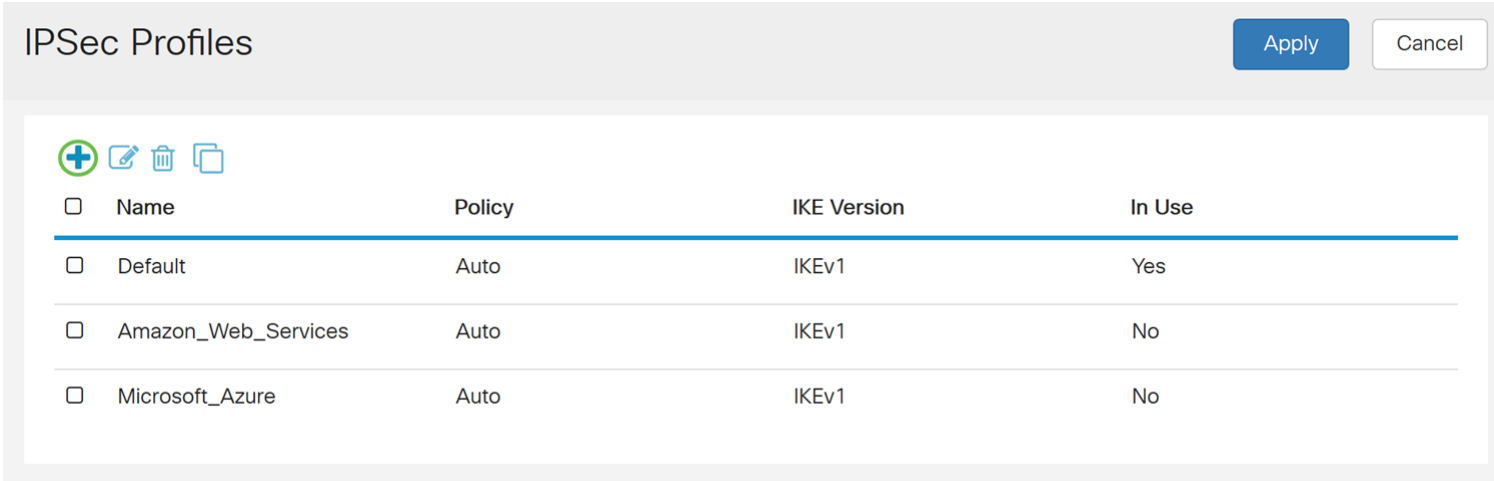
Configurazione del profilo IPsec

Passaggio 1. Passare a **VPN > VPN IPSec > Profili IPSec**.

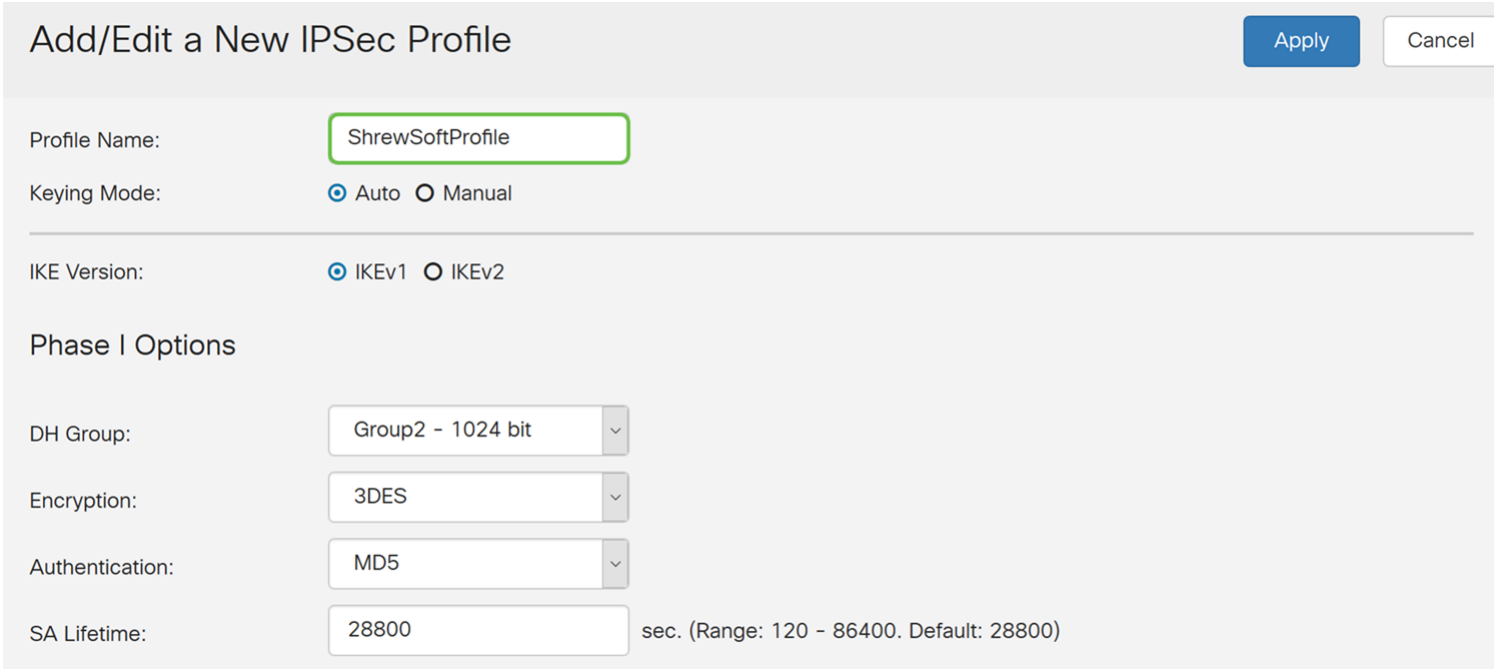


Nota: Per ulteriori informazioni su come configurare i profili IPSec, fare clic sul collegamento per visualizzare l'articolo: [Configurazione dei profili IPsec (modalità di impostazione automatica della chiave) sui router RV160 e RV260]

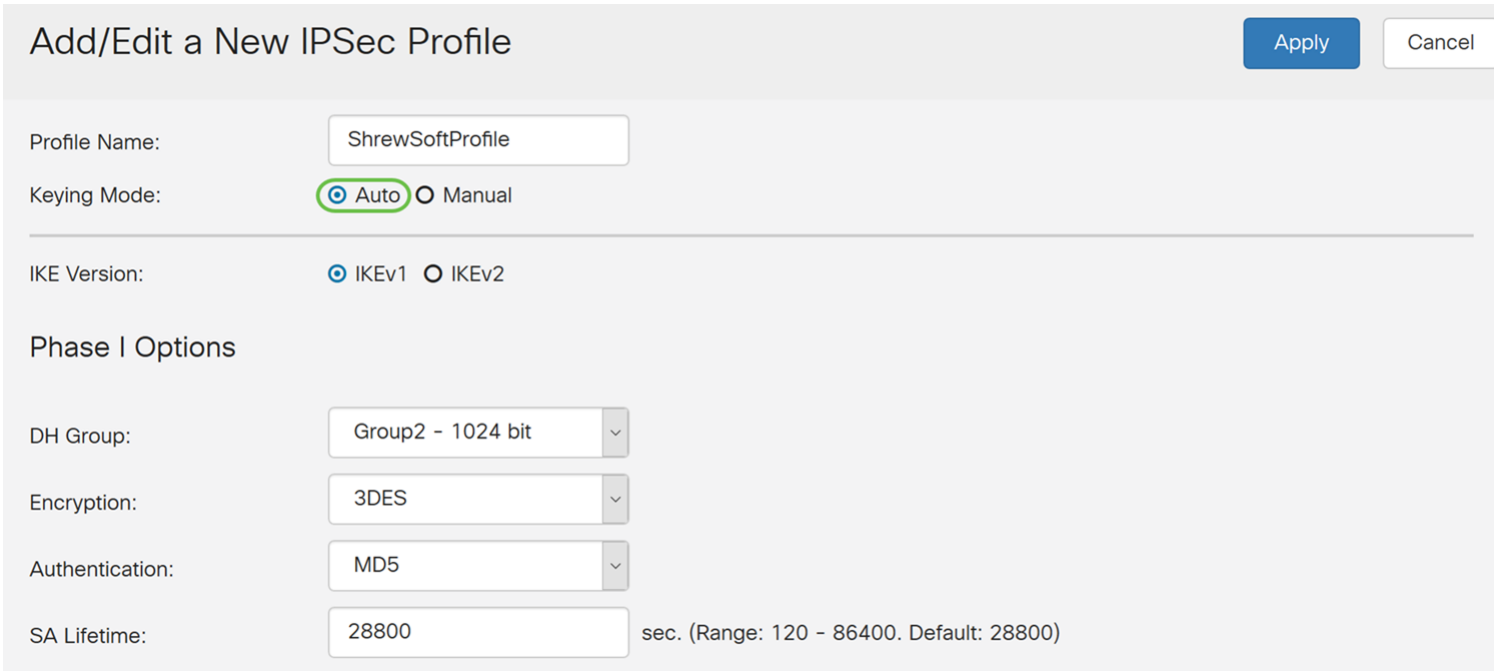
Passaggio 2. Fare clic sul pulsante **più** per aggiungere un nuovo profilo IPSec.



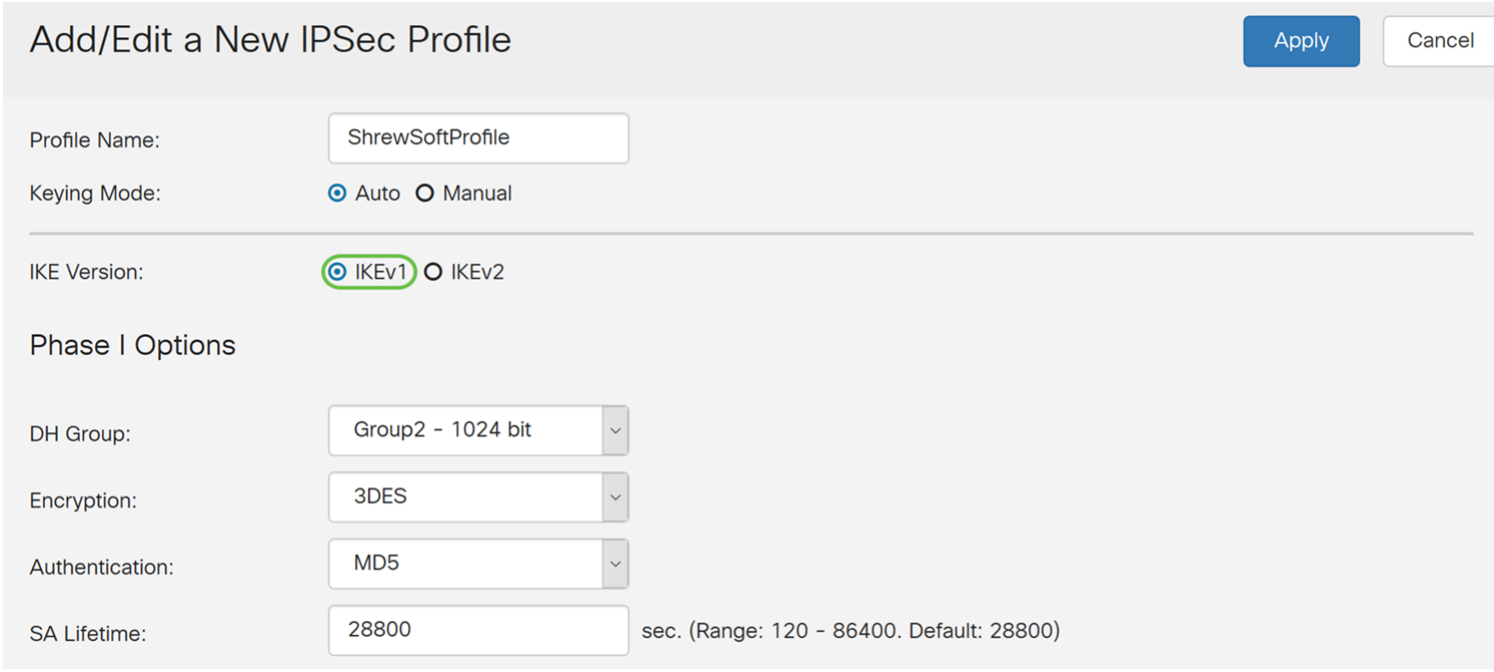
Passaggio 3. Inserire un nome per il profilo nel campo *Nome profilo*. Verrà immesso **ShrewSoftProfile** come nome del profilo.



Passaggio 4. Selezionare **Automatico** per *Modalità trasparenza*.



Passaggio 5. Selezionare **IKEv1** o **IKEv2** come *versione IKE*. Nell'esempio riportato di seguito è stato selezionato IKEv1.



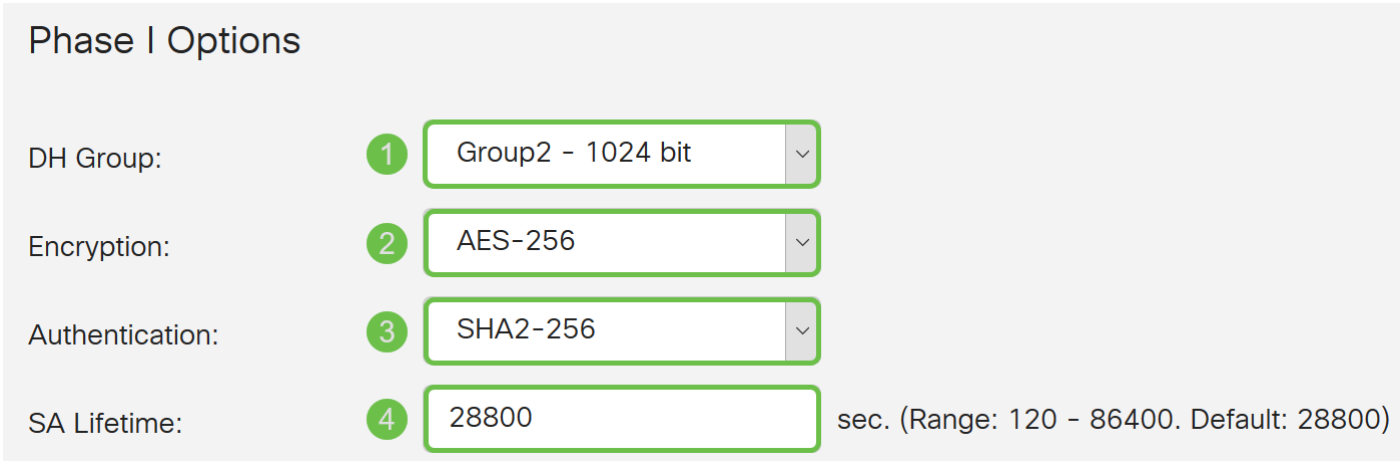
Passaggio 6. Nella sezione *Opzioni Fase I* questo è quanto è stato configurato per questo articolo.

Gruppo DH: **Group2 - 1024 bit**

Crittografia: **AES-256**

Autenticazione: **SHA2-256**

Durata SA: **28800**



Passaggio 7. In *Opzioni fase II*, questo è ciò che abbiamo configurato per questo articolo.

Selezione protocollo: **ESP**

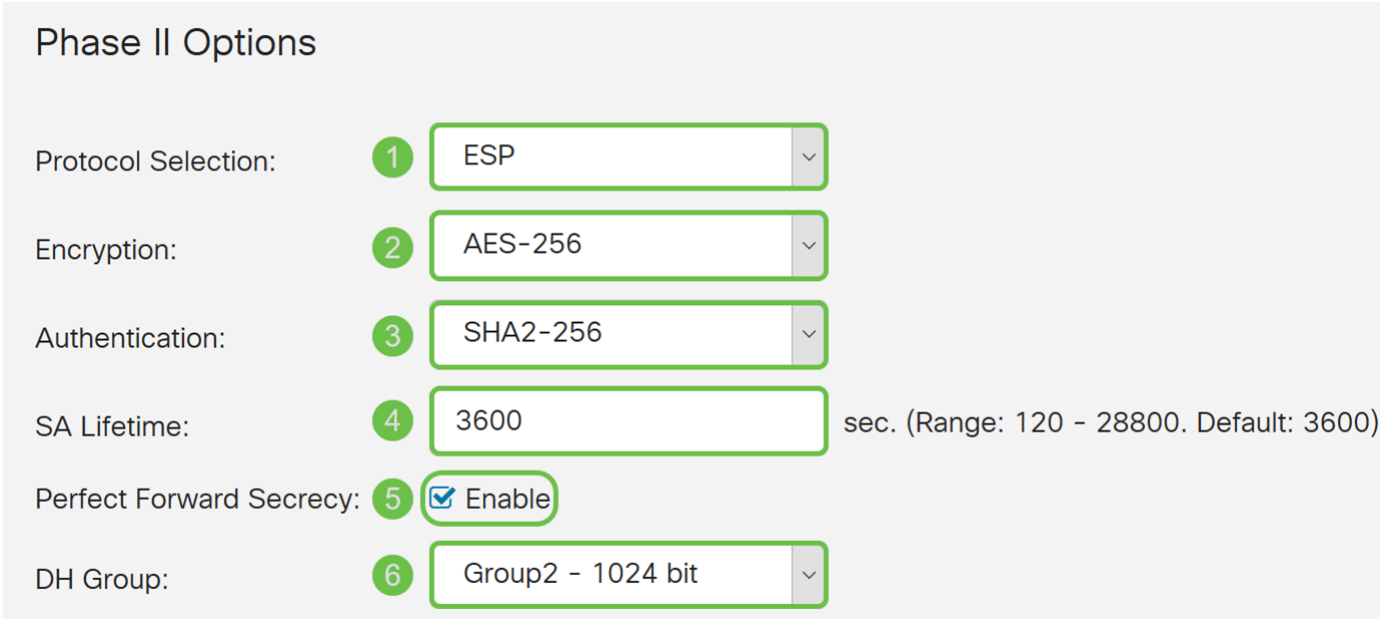
Crittografia: **AES-256**

Autenticazione: **SHA2-256**

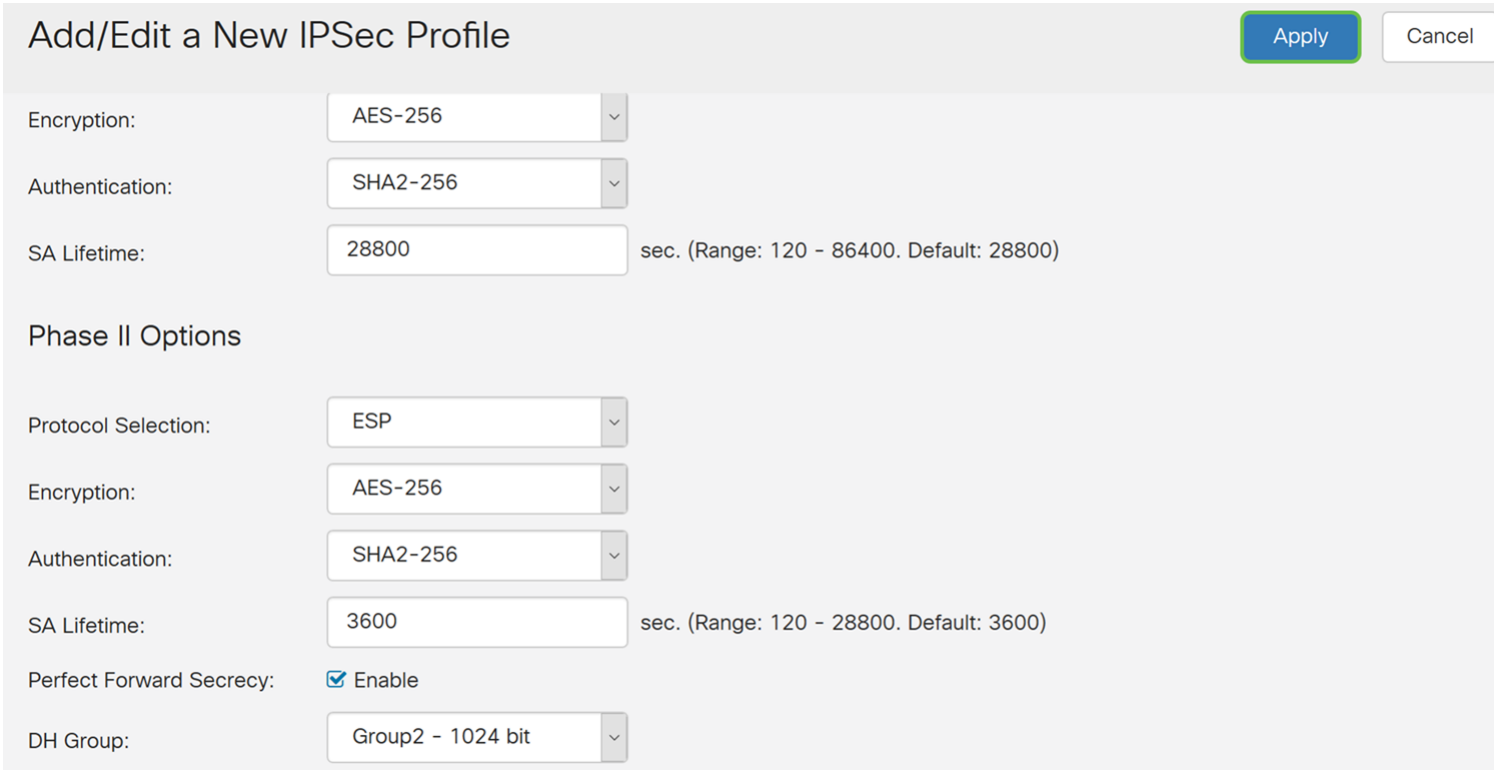
Durata SA: **3600**

Perfect Forward Secrecy: **Attivato**

Gruppo DH: **Group2 - 1024 bit**

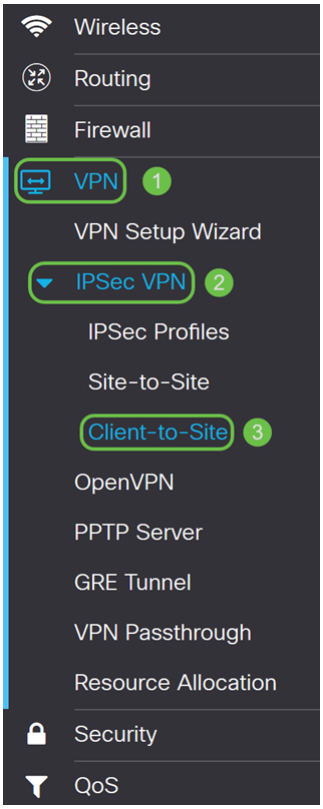


Passaggio 8. Fare clic su **Apply** (Applica) per creare il nuovo profilo IPSec.

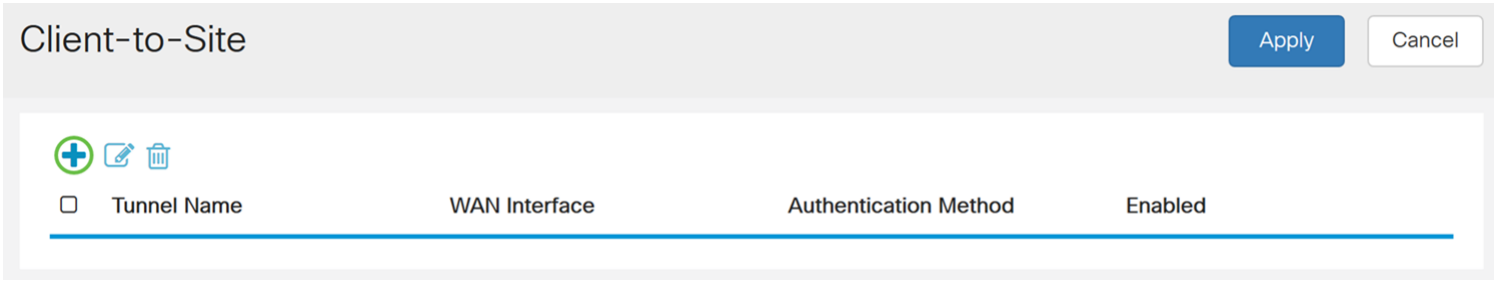


Configurazione da client a sito

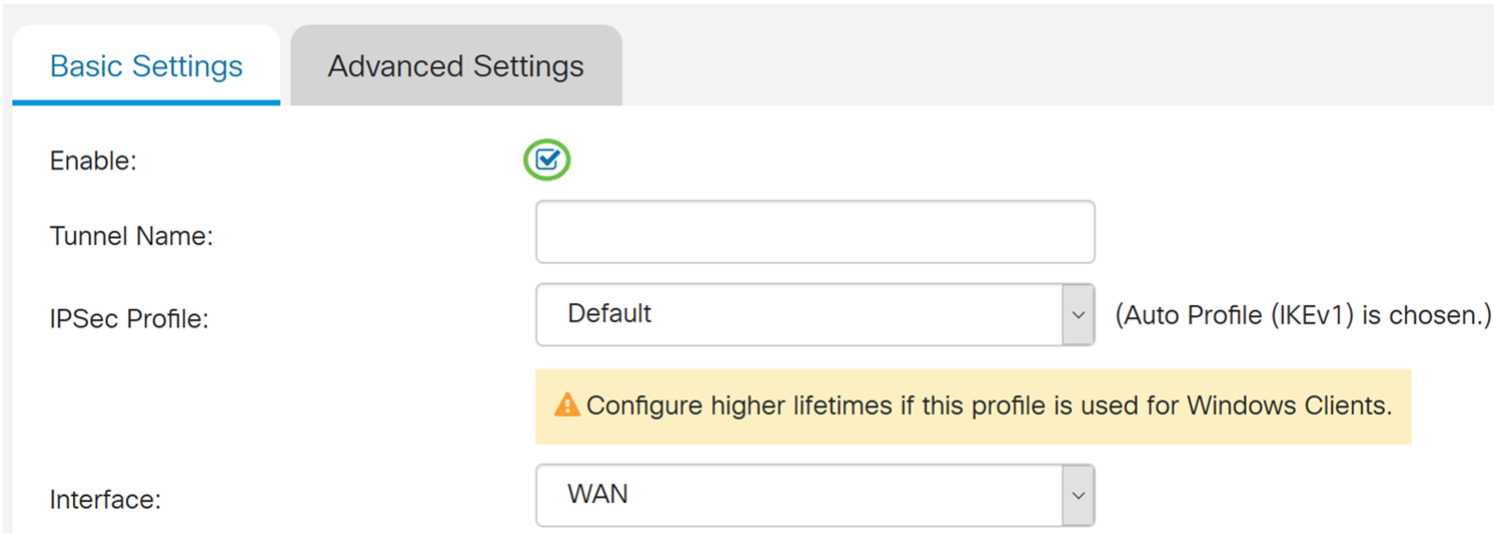
Passaggio 1. Passare a **VPN > IPSec VPN > Da client a sito**.



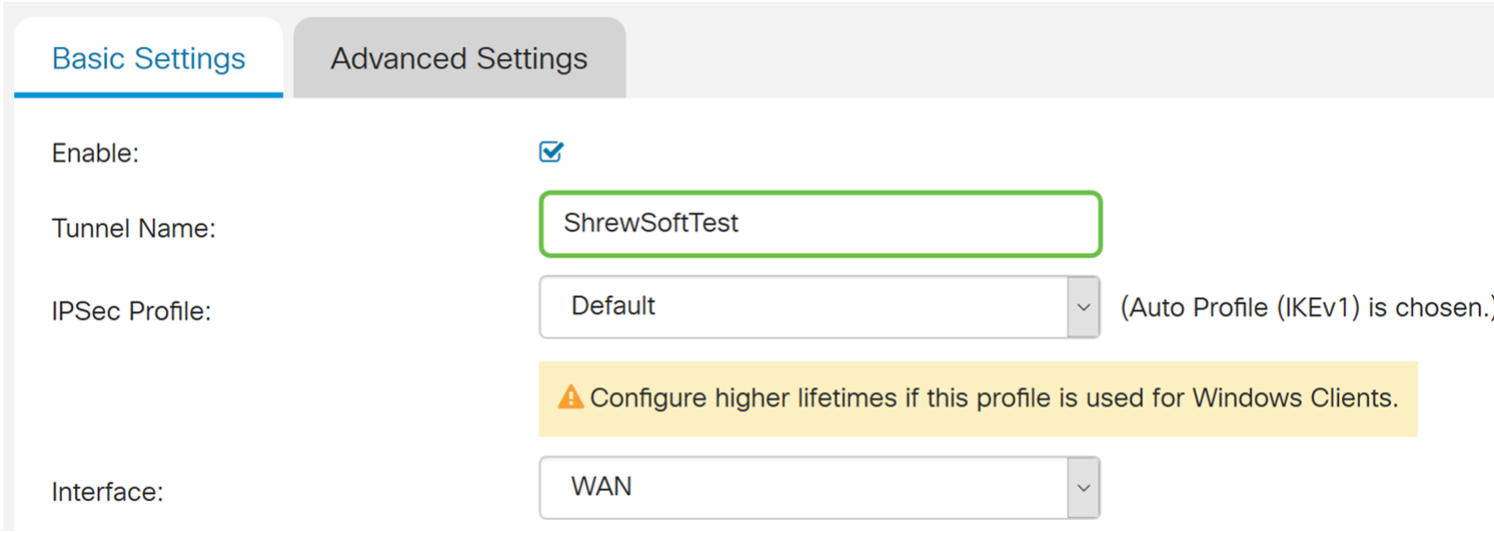
Passaggio 2. Fare clic sul pulsante **più** per aggiungere un nuovo tunnel.



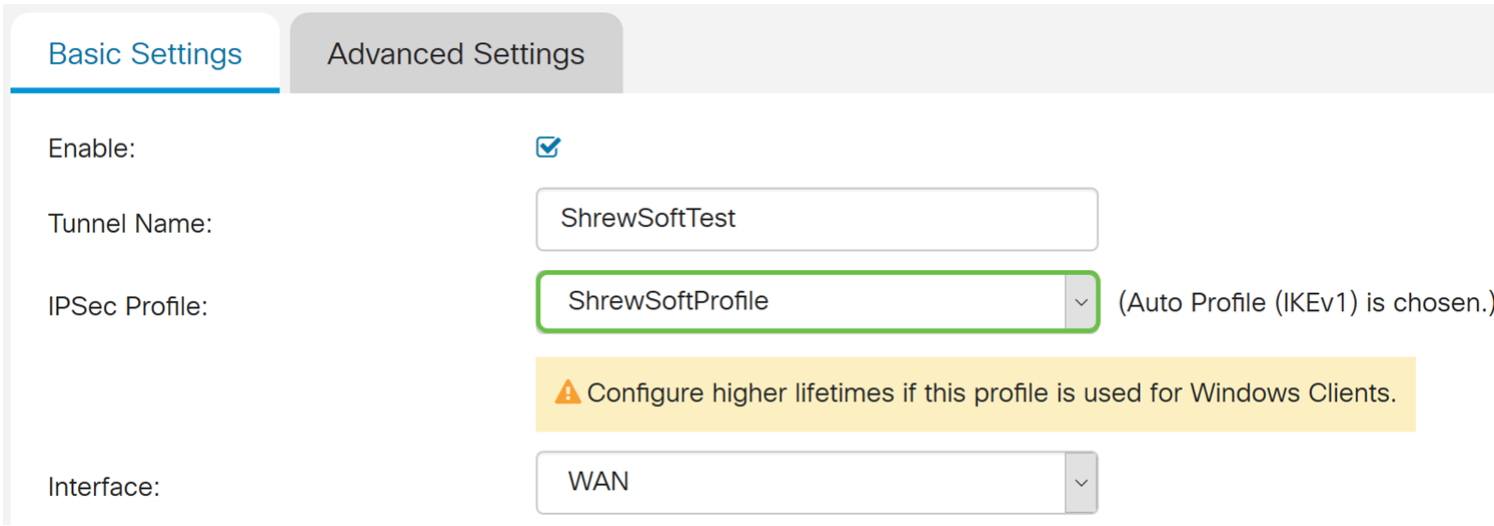
Passaggio 3. Selezionare la casella di controllo **Abilita** per abilitare il tunnel.



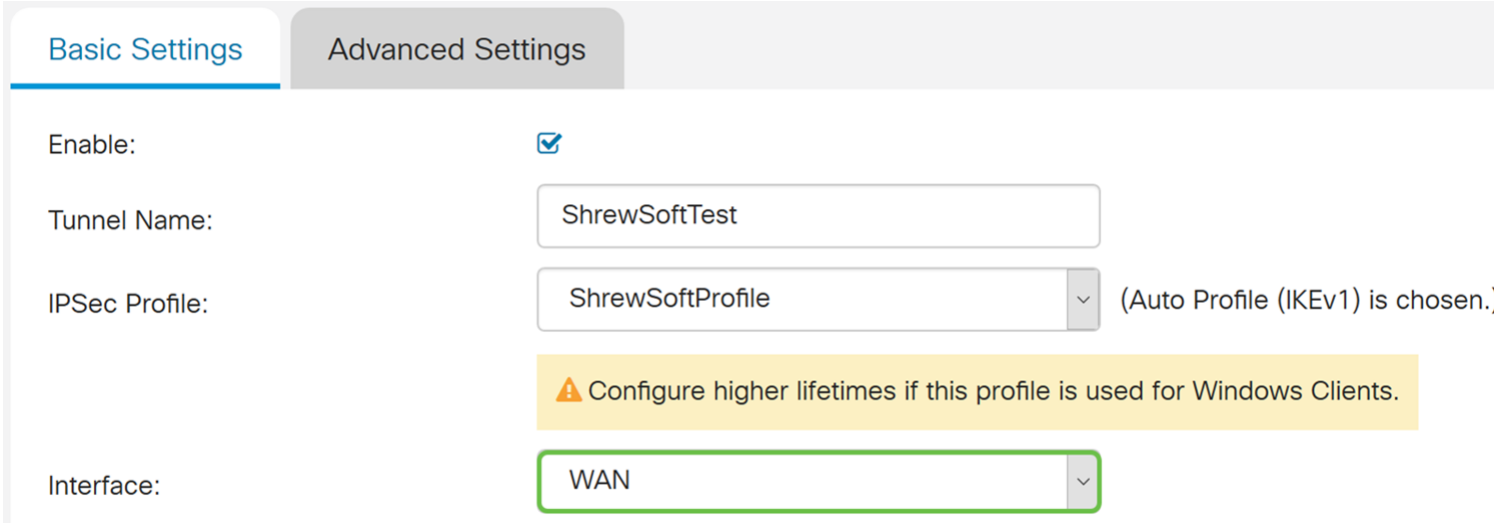
Passaggio 4. Immettere un nome per il tunnel nel campo *Nome tunnel*.



Passaggio 5. Nell'elenco a discesa *Profilo IPSec* selezionare il profilo che si desidera utilizzare. Verrà selezionato ShrewSoftProfile creato nella sezione precedente: Configurazione del profilo IPsec.



Passaggio 6. Dall'elenco a discesa *Interfaccia*, selezionare l'interfaccia che si desidera utilizzare. Utilizzeremo la rete **WAN** come interfaccia per collegare il tunnel.

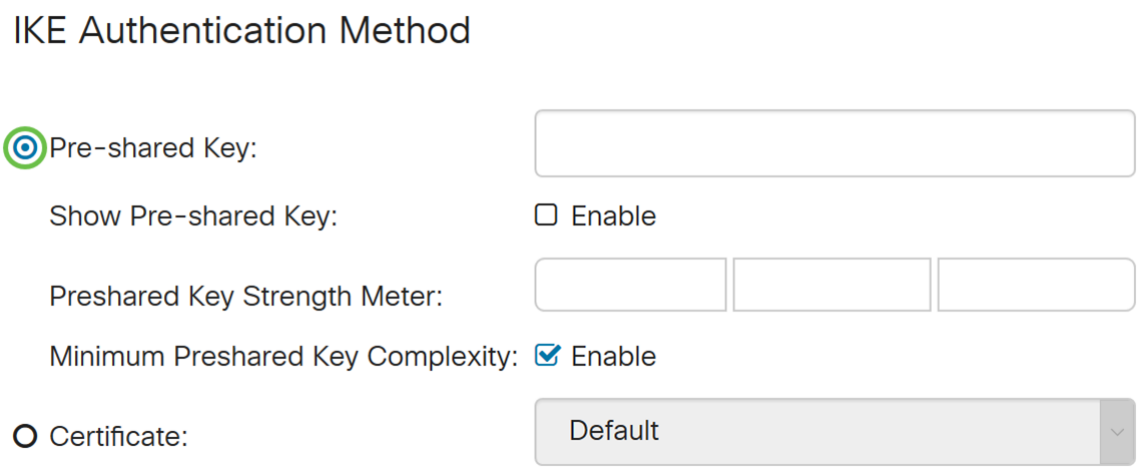


Passaggio 7. Nella sezione *Metodo di autenticazione IKE* selezionare *Chiave già condivisa* o *Certificato*. Verrà utilizzata la **chiave già condivisa** come metodo di autenticazione IKE.

Nota: I peer IKE si autenticano a vicenda tramite il calcolo e l'invio di un hash di dati con chiave che include la chiave precondivisa. Se il peer ricevente è in grado di creare lo stesso

hash in modo indipendente utilizzando la propria chiave già condivisa, sa che entrambi i peer devono condividere lo stesso segreto, autenticando così l'altro peer. Le chiavi già condivise non sono scalabili correttamente perché ogni peer IPsec deve essere configurato con le chiavi già condivise di ogni altro peer con cui stabilisce una sessione.

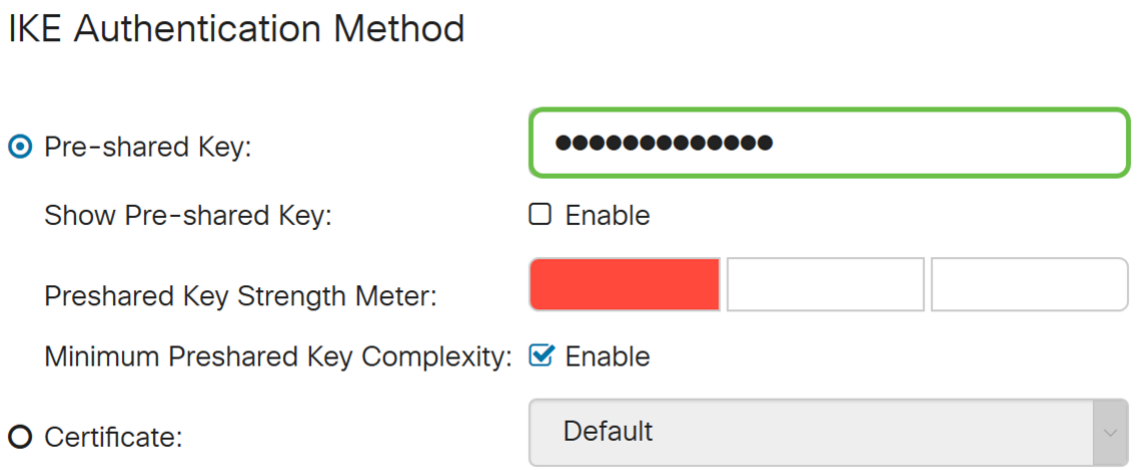
Il certificato utilizza un certificato digitale che contiene informazioni quali il nome, l'indirizzo IP, il numero di serie, la data di scadenza del certificato e una copia della chiave pubblica del titolare del certificato.



Passaggio 8. Immettere la chiave già condivisa che si desidera utilizzare per l'autenticazione. La chiave già condivisa può essere qualsiasi cosa si desideri. La chiave precondivisa configurata sul client Show Soft VPN deve essere uguale a quella qui configurata.

In questo esempio verrà utilizzato **CiscoTest123!** come chiave già condivisa.

Nota: La chiave già condivisa immessa qui è un esempio. È consigliabile immettere una chiave già condivisa più complessa.



Passaggio 9. Selezionare l'*identificatore locale* dall'elenco a discesa. Le opzioni seguenti sono definite come:

- IP WAN locale: questa opzione utilizza l'indirizzo IP dell'interfaccia WAN (Wide Area Network) del gateway VPN

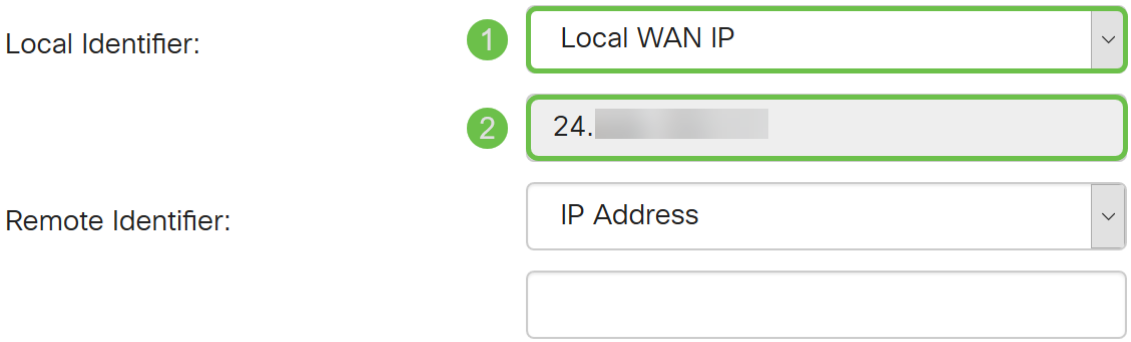
- Indirizzo IP - Questa opzione consente di immettere manualmente un indirizzo IP per la connessione VPN. È necessario immettere l'indirizzo IP WAN del router sul sito (ufficio).

- FQDN: questa opzione utilizza il nome di dominio completo (FQDN) del router quando si stabilisce la connessione VPN.

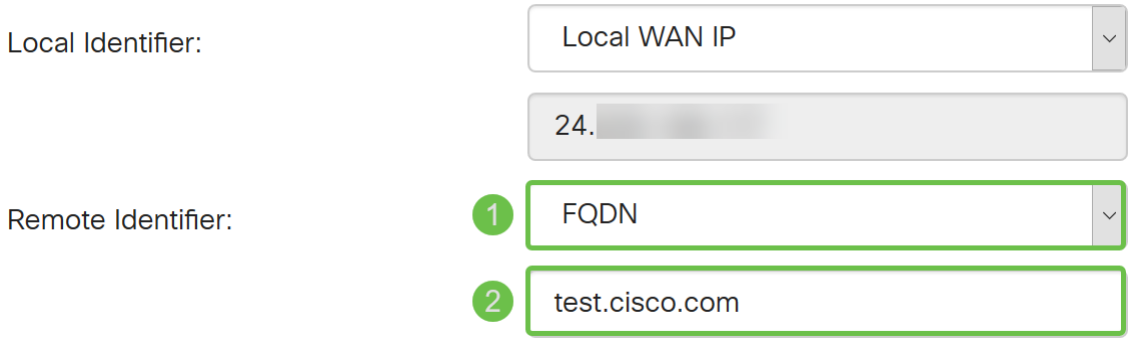
- FQDN utente: questa opzione consente di utilizzare un nome di dominio completo per un utente specifico su Internet.

Nell'esempio, verrà selezionato **Local WAN IP** come identificatore locale.

Nota: L'indirizzo IP WAN locale del router verrà compilato automaticamente.

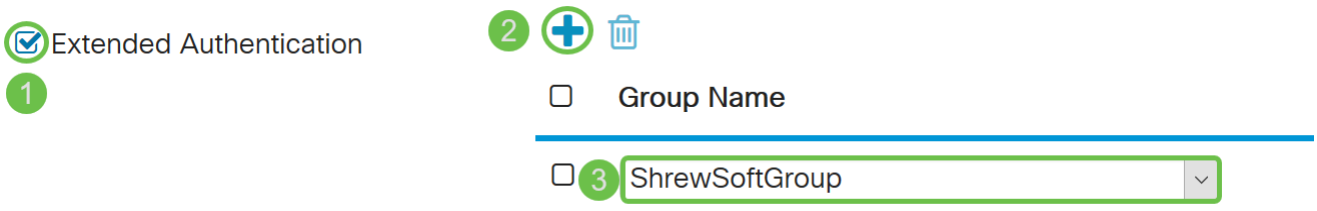


Passaggio 10. Nell'elenco a discesa *Identificatore remoto* selezionare **Indirizzo IP**, **FQDN** o **FQDN utente**. Immettere quindi la risposta appropriata da quanto selezionato. Nell'esempio, selezioneremo **FQDN** e immetteremo **test.cisco.com**.



Passaggio 11. Selezionare la casella di controllo **Autenticazione estesa** per abilitarla. Ciò fornirà un ulteriore livello di autenticazione che richiederà agli utenti remoti di inserire le proprie credenziali prima di ottenere l'accesso alla VPN.

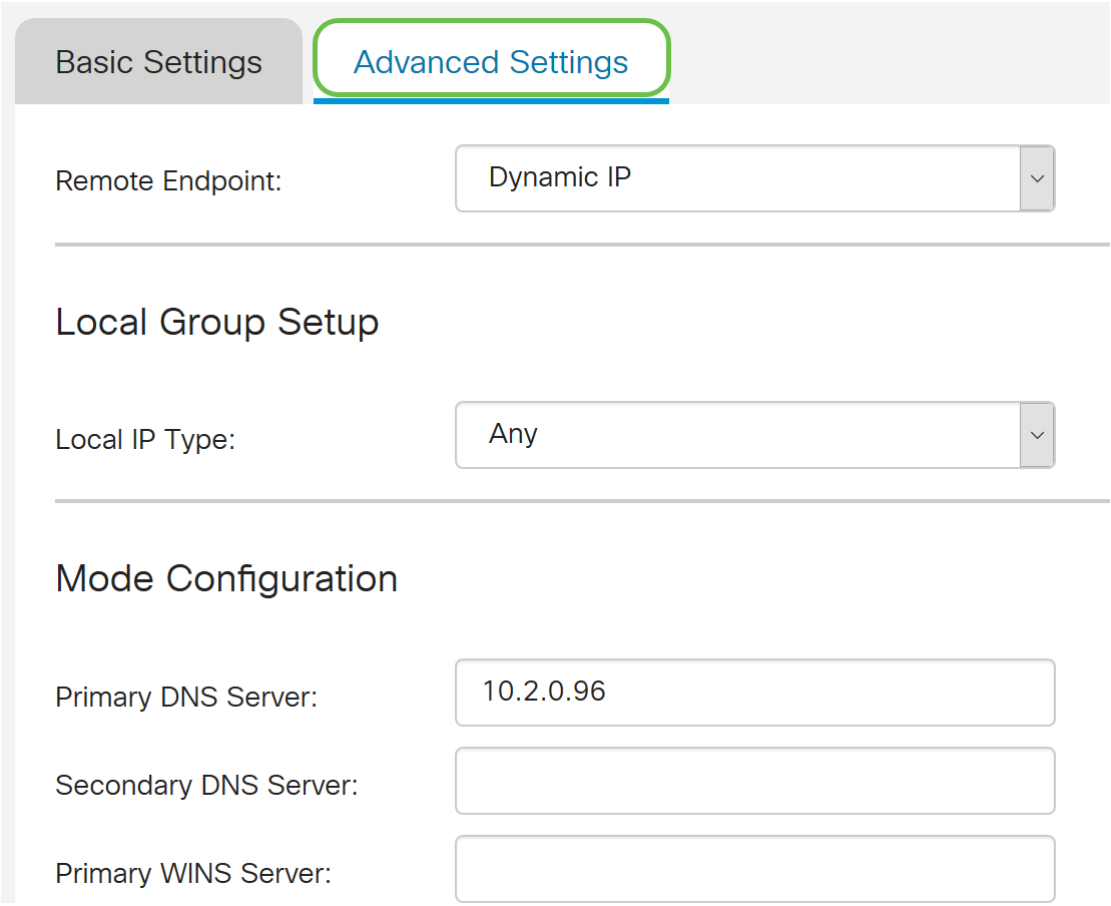
Se è stata abilitata l'opzione *Autenticazione estesa*, fare clic sull'icona **più** per aggiungere un gruppo di utenti. Selezionare dall'elenco a discesa il gruppo che si desidera utilizzare per l'autenticazione estesa. Verrà selezionato **ShrewSoftGroup** come gruppo.



Passaggio 12. Nell'*intervallo del pool per la LAN client*, immettere l'intervallo di indirizzi IP che è possibile assegnare a un client VPN nel campo *IP iniziale* e *IP finale*. Deve trattarsi di un pool di indirizzi che non si sovrappone agli indirizzi del sito.

La versione **10.2.1.1** verrà immessa come *IP iniziale* e la **versione 10.2.1.254** come *IP finale*.

Passaggio 13. (Facoltativo) Fare clic sulla scheda **Advanced Settings** (Impostazioni avanzate).



Passaggio 14. (Facoltativo) Qui è possibile specificare l'indirizzo IP dell'endpoint remoto. In questa guida verrà utilizzato l'indirizzo **IP dinamico**, poiché l'indirizzo IP del client finale non è fisso.

Èinoltre possibile specificare quali risorse interne saranno disponibili in *Configurazione gruppo locale*.

Se si seleziona **Qualsiasi**, saranno disponibili tutte le risorse interne.

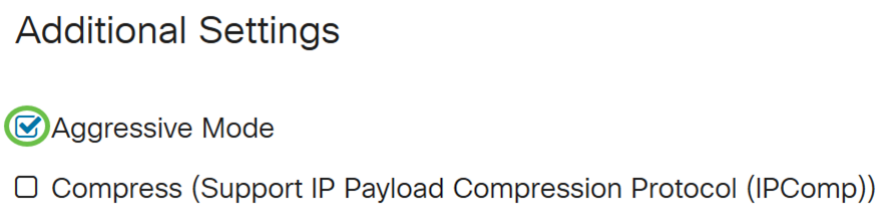
Èinoltre possibile scegliere di utilizzare i server DNS interni e WINS. A tale scopo, è necessario specificarli in *Configurazione modalità*.

Èinoltre possibile utilizzare il tunnel completo o diviso e il DNS suddiviso.

Scorrere fino a *Impostazioni aggiuntive*. Selezionare la casella di controllo **Modalità aggressiva** per abilitare la modalità aggressiva. La modalità aggressiva si ha quando la negoziazione per l'associazione di protezione IKE viene compressa in tre pacchetti, con tutti i dati dell'associazione di protezione che devono essere passati dall'iniziatore. I negoziati sono più rapidi, ma presentano una vulnerabilità di identità di scambio in testo chiaro.

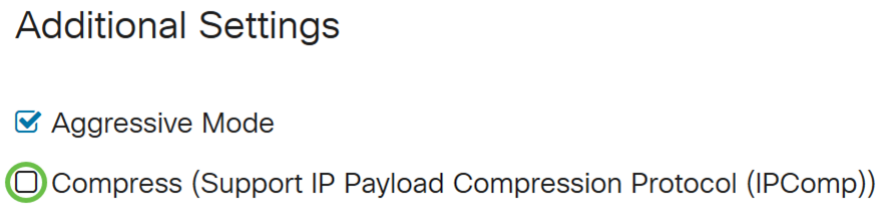
Nota: Per ulteriori informazioni sulla modalità principale o aggressiva, vedere: Modalità Principale E Modalità Aggressiva

In questo esempio verrà attivata la **modalità aggressiva**.

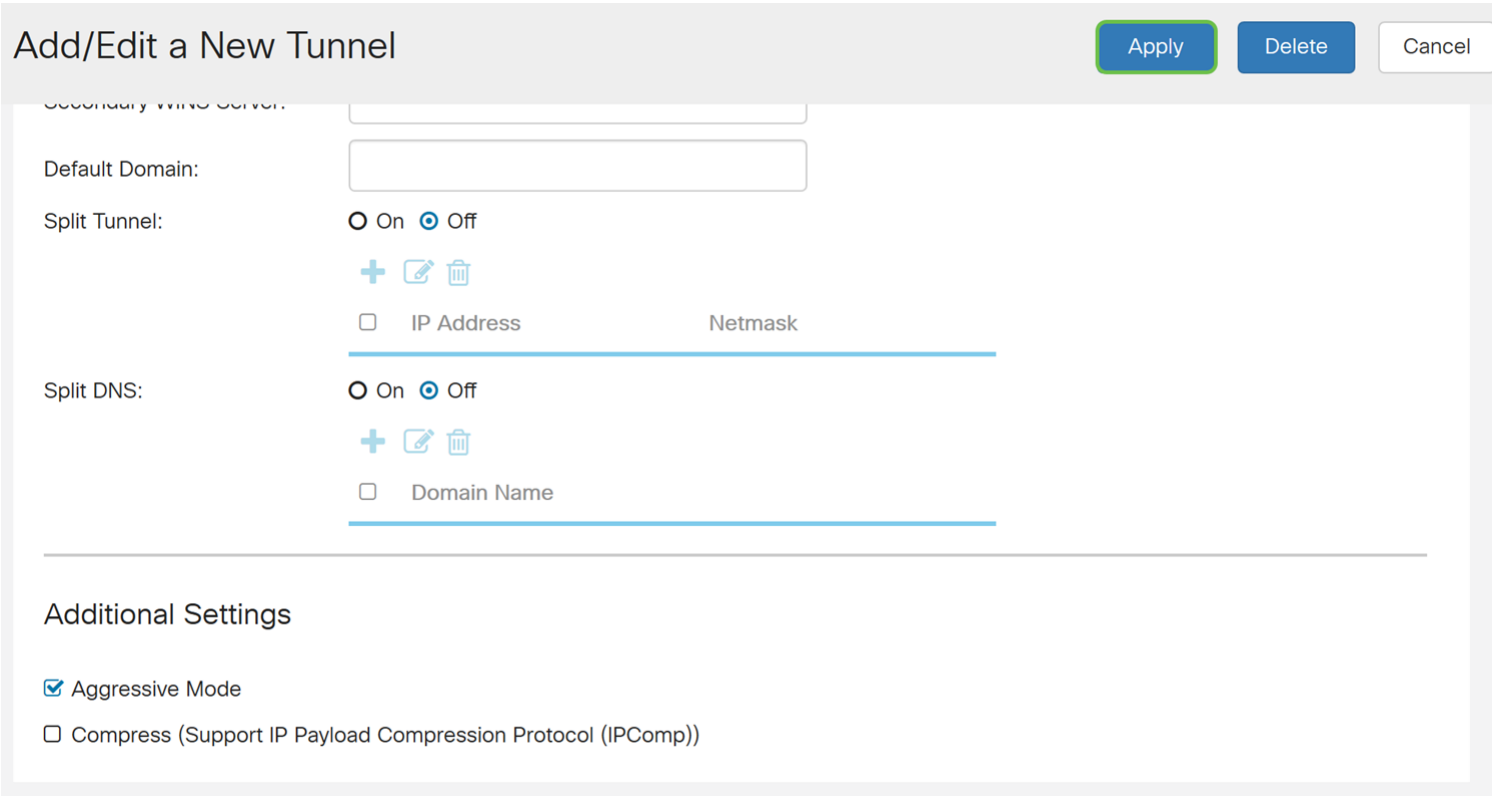


Passaggio 15. (Facoltativo) Selezionare la casella di controllo **Comprimi (Support IP Payload Compression Protocol (IPComp))** per consentire al router di proporre la compressione quando avvia una connessione. Questo protocollo riduce le dimensioni dei datagrammi IP. Se il risponditore rifiuta questa proposta, il router non implementa la compressione. Quando il router è il risponditore, accetta la compressione, anche se non è abilitata.

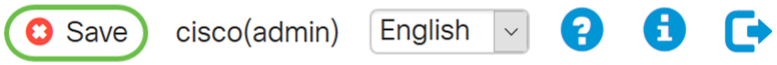
Lasceremo *Compress* non controllato.



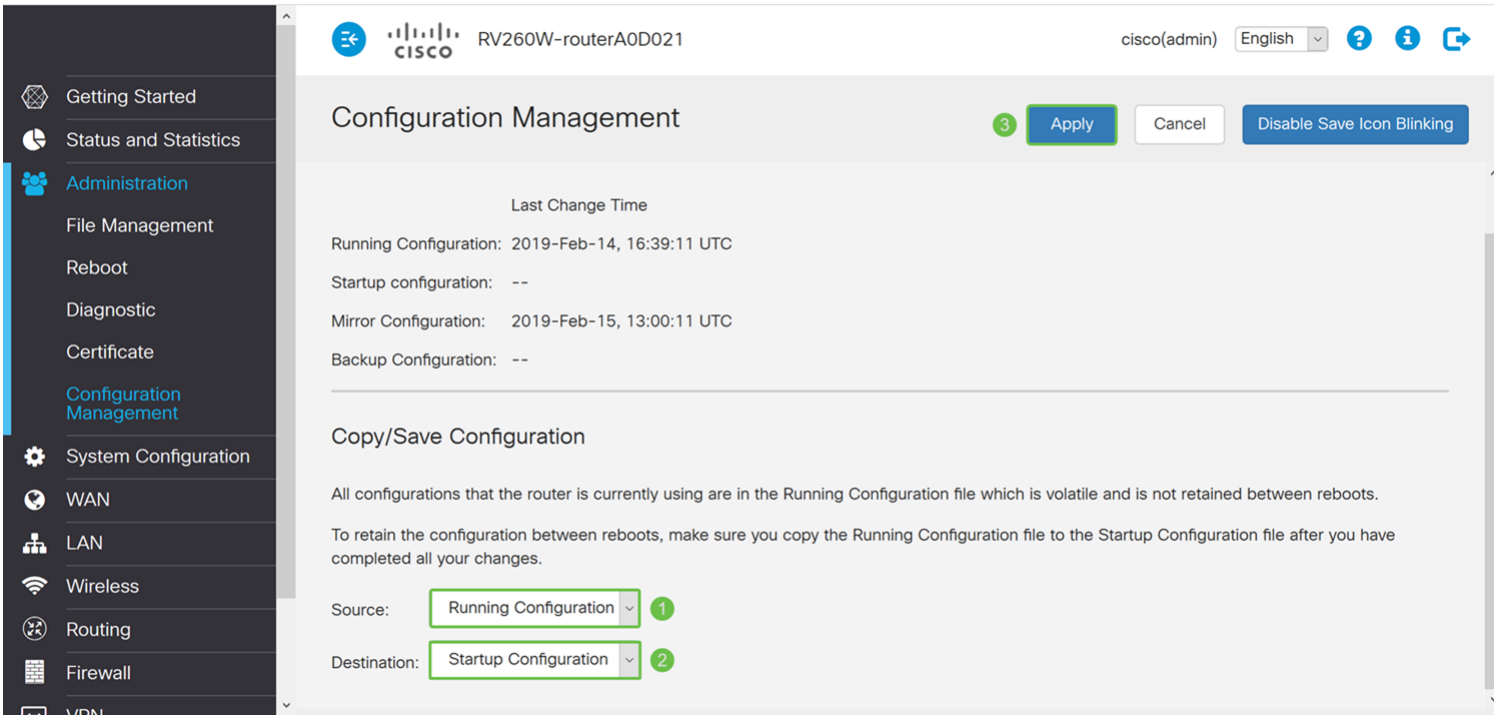
Passaggio 16. Fare clic su **Apply** (Applica) per aggiungere il nuovo tunnel.



Passaggio 17. Fare clic sull'icona **Salva** lampeggiante nella parte superiore della pagina di configurazione Web.



Passaggio 18. Viene visualizzata la pagina *Configuration Management*. Nella sezione Copia/Salva configurazione, verificare che il campo *Origine* abbia **Configurazione in esecuzione** e che il campo *Destinazione* abbia **Configurazione di avvio**. Quindi premere **Applica**. Tutte le configurazioni attualmente utilizzate dal router si trovano nel file della configurazione in esecuzione, che è volatile e non viene conservato tra un riavvio e l'altro. Se si copia il file della configurazione di esecuzione nel file della configurazione di avvio, la configurazione verrà mantenuta tra un riavvio e l'altro.

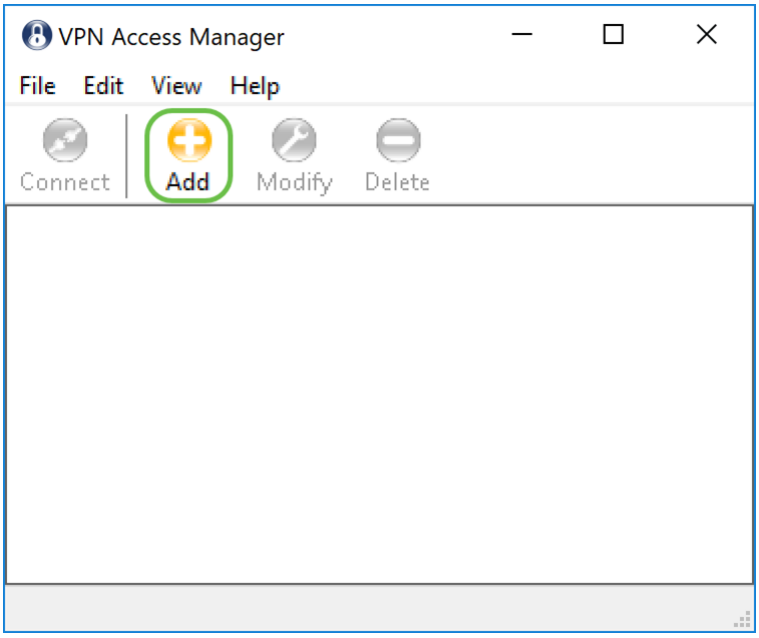


Configurazione di Show Soft VPN Client

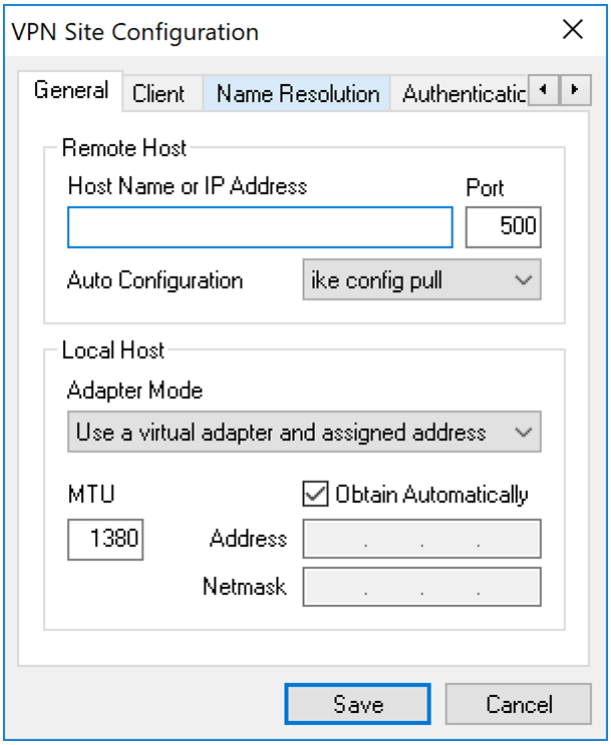
Se non hai ancora scaricato il client Shrew Soft VPN, puoi scaricarlo cliccando su questo link: Mostra client VPN software per Windows. Utilizzeremo l'edizione standard. Se hai già scaricato il client Shrew Soft VPN, puoi passare alla prima fase.

Mostra client VPN software: Scheda Generale

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

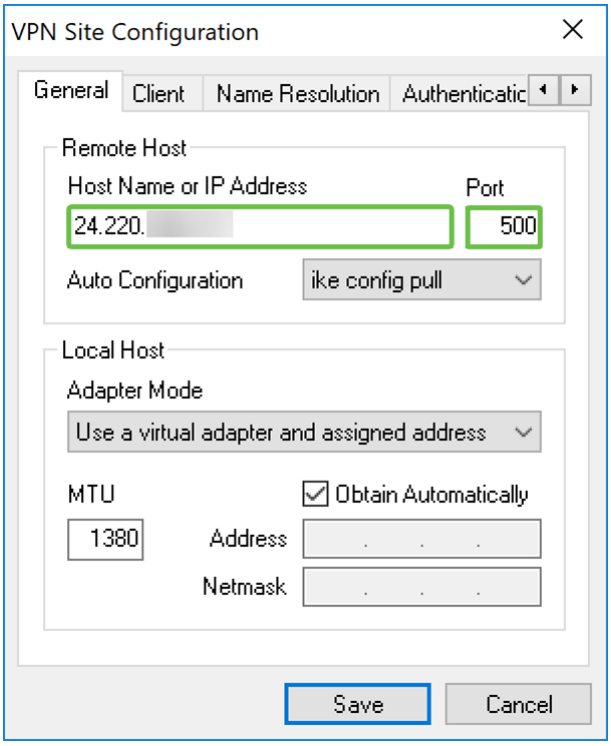


Viene visualizzata la finestra *VPN Site Configuration* (Configurazione sito VPN).



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. In questo esempio, per configurare la connessione, immettere l'indirizzo IP WAN dei router RV160/RV260 in loco.

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 al firewall.



Passaggio 3. Nell'elenco a discesa *Configurazione automatica*, selezionare un'opzione. Le opzioni disponibili sono definite come segue:

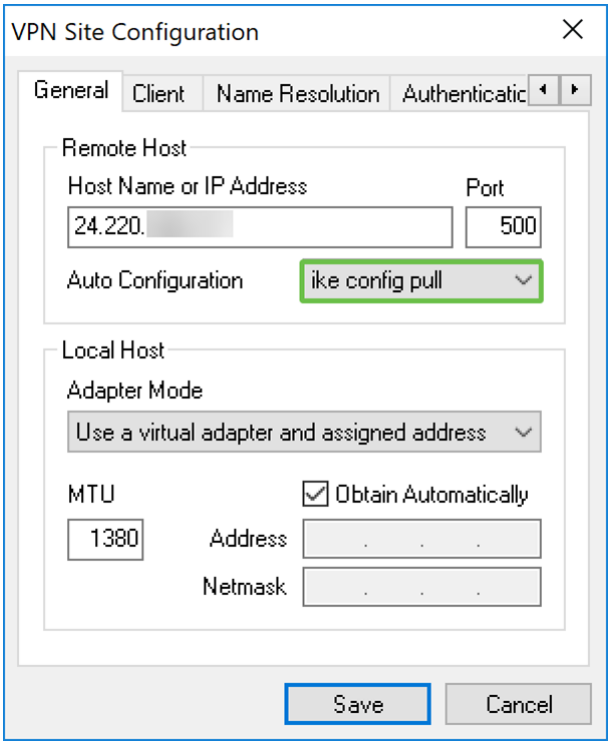
- **Disabilitato** - disabilita qualsiasi configurazione client automatica

- **Ike Config Pull** - Consente le richieste di impostazione da un computer da parte del client. Se il computer supporta il metodo pull, la richiesta restituisce un elenco di impostazioni supportate dal client.

- **Ike Config Push** - Offre a un computer la possibilità 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 dal computer tramite DHCP over IPsec.

Nell'esempio, verrà selezionato **ike config pull**.

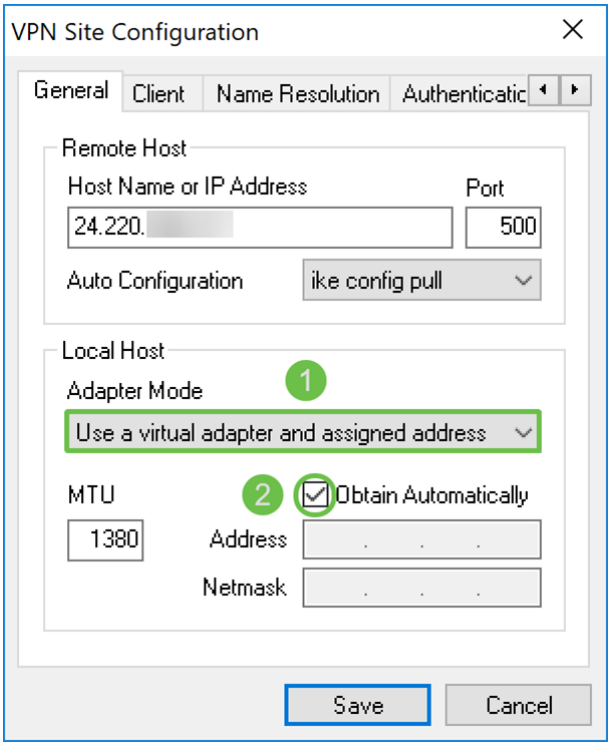


Passaggio 4. Nella sezione *Host locale*, scegliere **Utilizza una scheda virtuale e l'indirizzo assegnato** nell'elenco a discesa *Modalità scheda* e selezionare la casella di controllo **Ottieni automaticamente**. Le opzioni disponibili sono definite come segue:

- **Usa una scheda virtuale e 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.

- **Usa una scheda esistente e indirizzo corrente** - Consente al client di utilizzare solo la scheda fisica esistente con l'indirizzo corrente come origine per le comunicazioni IPsec.



Mostra client VPN software: Scheda Client

Passaggio 1. Fare clic sulla scheda *Client*. Nell'elenco a discesa *NAT Traversal*, selezionare la stessa impostazione configurata sull'RV160/RV260 per NAT Traversal. Le opzioni di menu disponibili di Network Address Traversal (NATT) sono definite come segue:

- **Disabilitato** - Le estensioni del protocollo NAT non verranno utilizzate.

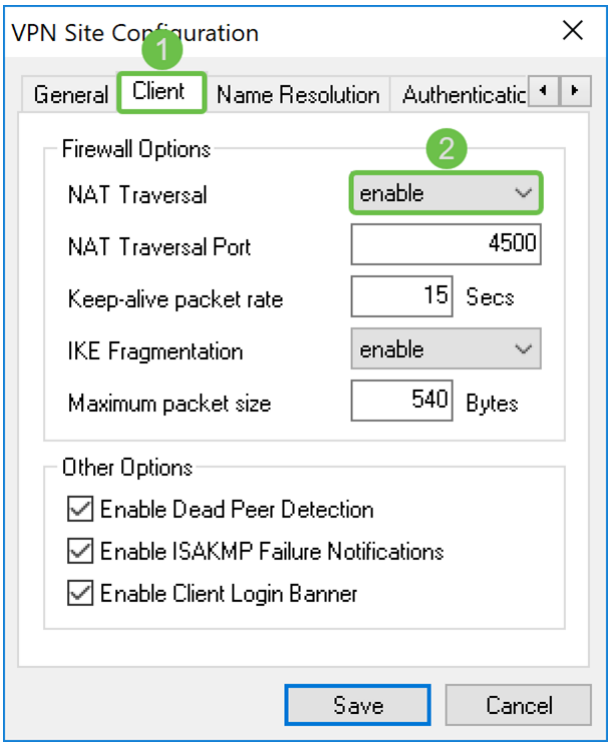
- **Abilitato** - Le estensioni del protocollo NAT verranno utilizzate solo se il gateway VPN indica il supporto durante le negoziazioni e se viene rilevato NAT.

- **Force-Draft** - La versione Draft delle estensioni 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-RFC** - Verrà utilizzata la versione RFC del protocollo NAT 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.

In questo documento, selezioneremo **enable** per NAT Traversal e lasceremo *NAT Traversal Port* e *Keep-alive packet rate* come valore predefinito.



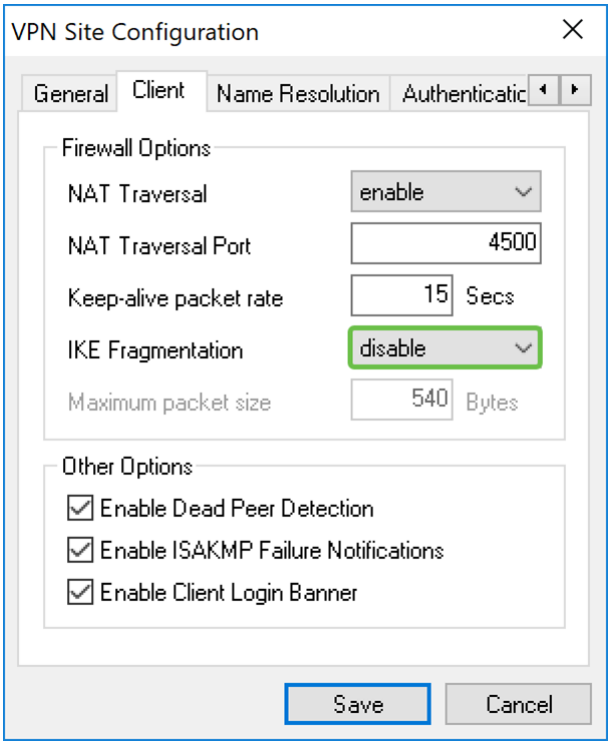
Passaggio 2. Nell'elenco a discesa *Frammentazione IKE* selezionare **Disabilita**, **Abilita** o **Forza**. Le opzioni sono definite come segue:

- **Disable** – Λəεστενσιονε δελ προτοχολλο δι φραμμενταζιονε ΙΚΕ νον ϖερρ◊ υτιλιζζατα.

- **Abilita** - L'estensione del protocollo di frammentazione IKE verrà utilizzata solo se il gateway VPN indica il supporto durante le negoziazioni.

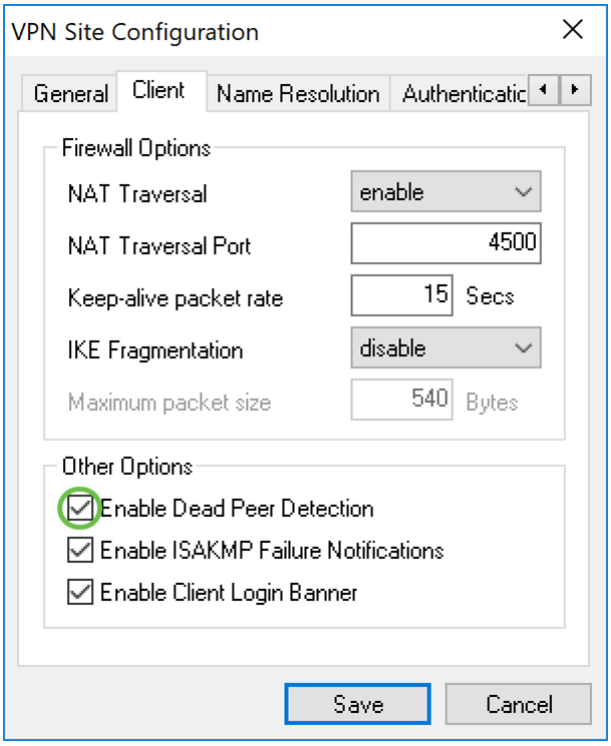
- **Force**: λəεστενσιονε δελ προτοχολλο δι φραμμενταζιονε ΙΚΕ ϖερρ◊ υτιλιζζατα ινδιπενδεντεμεντε δαλ φαττο χηε ιλ γατεωαψ ϛΠΝ ινδιχηι ο μενο ιλ συππορτο δυραντε λε νεγοζιαζιονι.

È stata selezionata l'opzione **disable** per la *frammentazione IKE*.



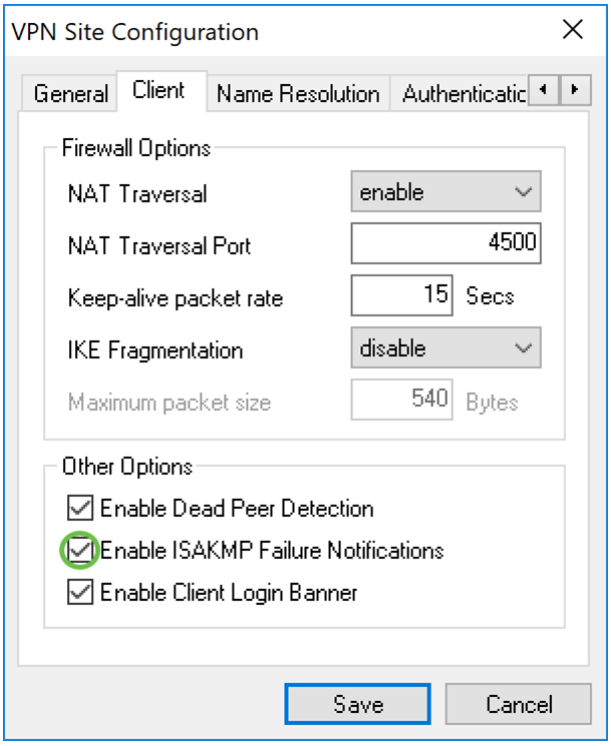
Passaggio 3. Selezionare la casella di controllo **Abilita rilevamento peer inattivo** per abilitare il protocollo Dead Peer Detection. Se questa opzione è abilitata, verrà utilizzata solo se supportata dal router. Questo consente al client e al router di controllare lo stato del tunnel e di rilevare quando un lato non è più in grado di rispondere. Questa opzione è attivata per default.

In questo esempio, lasceremo il Dead Peer Detection controllato.



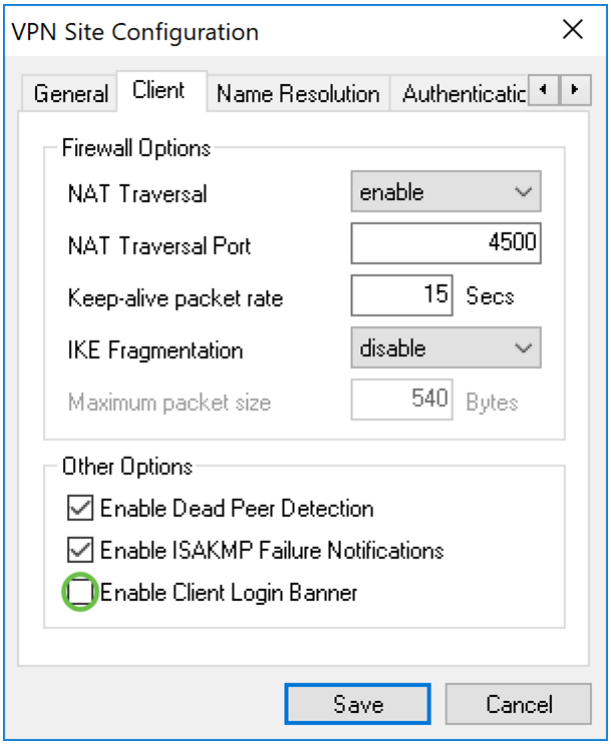
Passaggio 4. Selezionare la casella di controllo **Abilita notifica di errore ISAKMP** per abilitare la notifica di errore ISAKMP dal daemon IPsec del client VPN. L'opzione è abilitata per impostazione predefinita.

In questo esempio, lasceremo il controllo ISAKMP Failure Notification.



Passaggio 5. Deselezionare la casella **Enable Client Login Banner** (Abilita accesso client) per disabilitarla. Dopo aver stabilito il tunnel con il router, verrà visualizzato un banner di accesso. Il router deve supportare Transaction Exchange e deve essere configurato per inoltrare un banner di accesso al client. Questo valore è attivato per impostazione predefinita.

Il banner di accesso client verrà deselezionato.

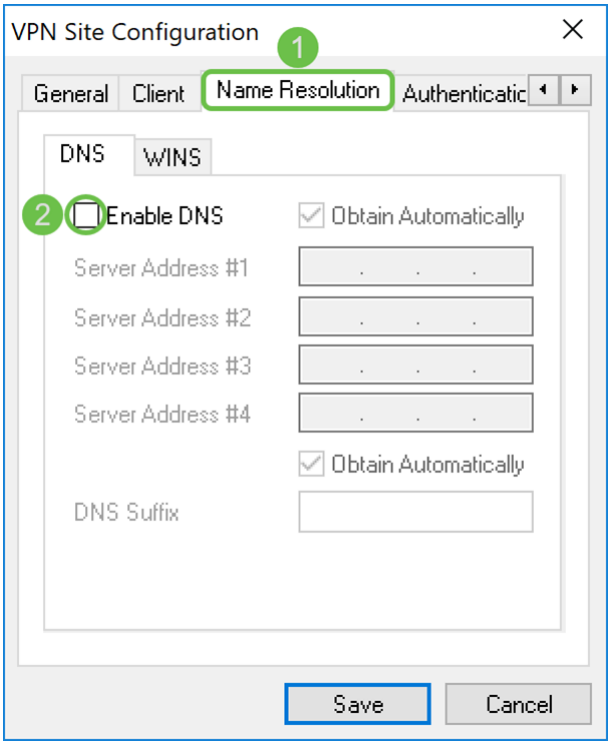


Mostra client VPN software: Scheda Risoluzione nome

Passaggio 1. 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**.

Se l'opzione *Abilita DNS* è selezionata e il gateway remoto è configurato per il supporto di 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.

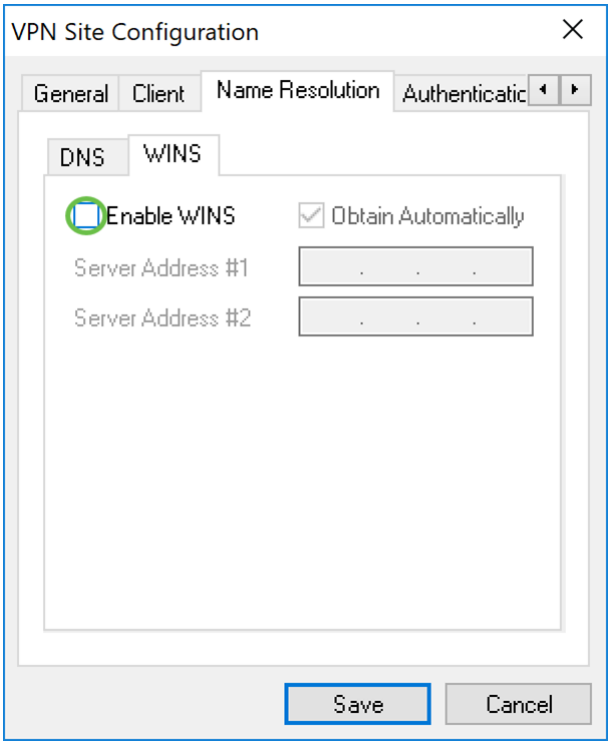
In questo esempio, l'opzione **Abilita DNS** è deselezionata.



Passaggio 2. 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.

Nell'esempio, l'opzione **Enable WINS** è deselezionata.



Mostra client VPN software: Scheda Autenticazione

Passaggio 1. Fare clic sulla scheda *Authentication* (Autenticazione), quindi 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.

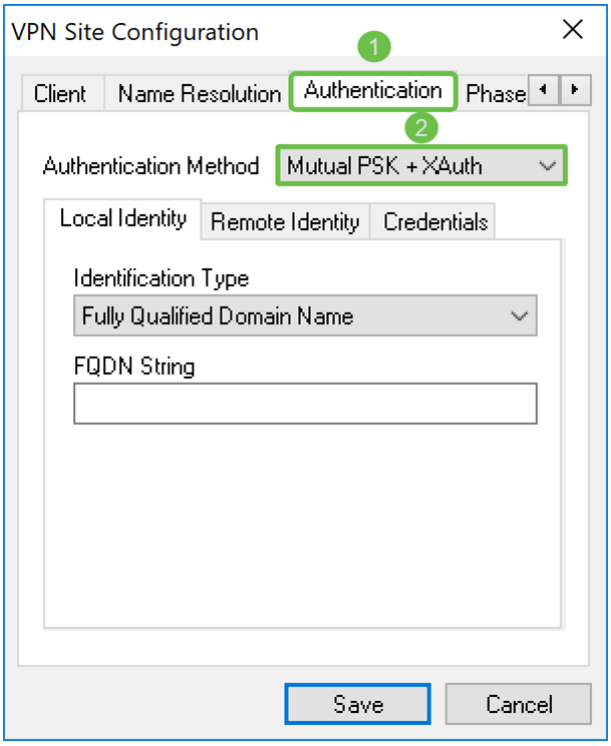
- **Hybrid GRP + XAuth** - Credenziali client non necessarie. Il client autenticherà il gateway. Le credenziali saranno sotto forma di file di certificato PEM o PKCS12 e di una stringa segreta condivisa.

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

- **Mutual PSK + XAuth** - Il client e il gateway richiedono entrambi credenziali per l'autenticazione. Le credenziali saranno in forma di stringa segreta condivisa.

- **RSA reciproca** - Il client e il 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 2. Nella scheda *Identità locale*, selezionare il tipo di identificazione e immettere la stringa appropriata nel campo vuoto. Le opzioni seguenti sono definite come:

- **Any** - Accettato solo nella scheda Identità remota. Il client accetterà qualsiasi tipo di ID e valore. Questa opzione deve essere utilizzata con cautela in quanto ignora parte del processo di identificazione IKE fase 1.

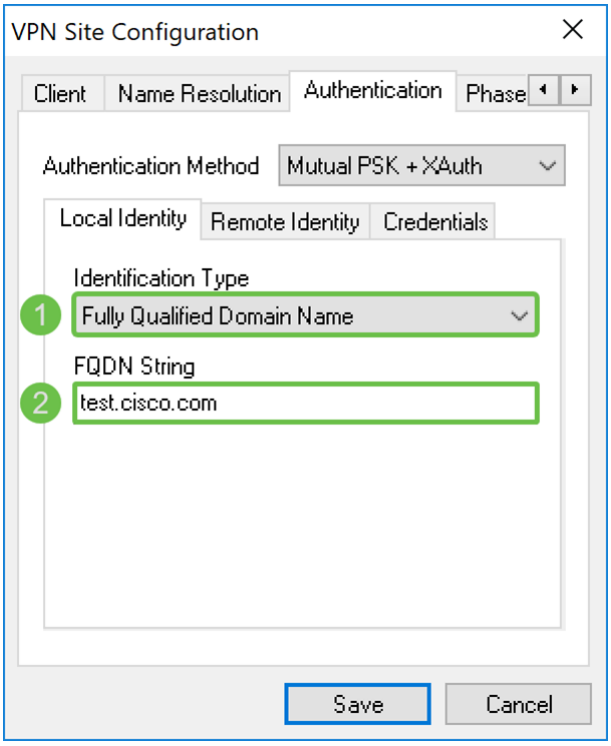
- **Nome di dominio completo** - Questa opzione consente di fornire una stringa FQDN sotto forma di stringa di dominio DNS. Ad esempio, "cisco.com" è un valore accettabile. Il client consente di selezionare questa opzione solo se viene utilizzata una modalità di autenticazione PSK.

- **Nome di dominio completo utente** - È necessario fornire una stringa FQDN utente sotto forma di user@domain. Ad esempio, "dave@cisco.com" è un valore accettabile. Il client consente di selezionare questa opzione solo se viene utilizzata una modalità di autenticazione PSK.

- **Indirizzo IP** - Quando si seleziona Indirizzo IP, la casella di controllo *Usa indirizzo host locale individuato* viene selezionata automaticamente per impostazione predefinita. Ciò significa che il valore verrà determinato automaticamente. Deselezionare la casella di controllo se si desidera utilizzare un indirizzo diverso da quello della scheda di rete utilizzata per comunicare con il gateway client. Immettere quindi una stringa di indirizzo specifica. Il client consentirà di selezionare questa opzione solo se viene utilizzata una modalità di autenticazione PSK.

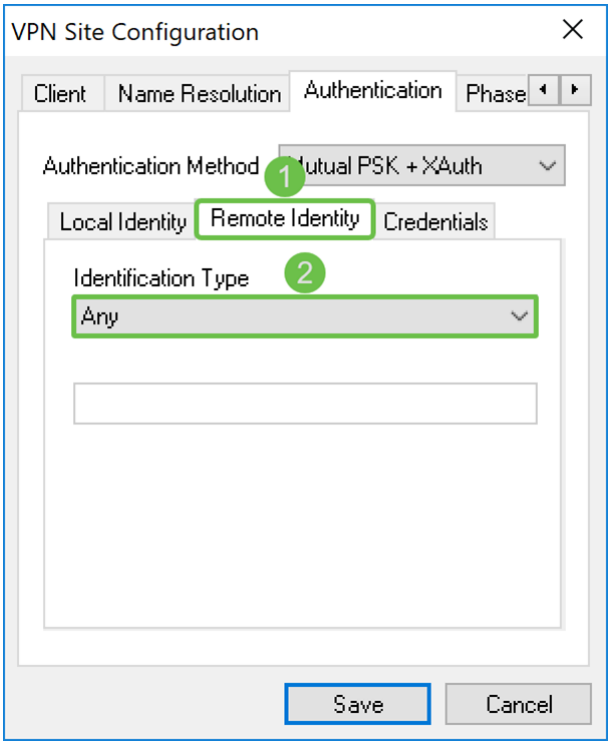
- **Identificatore chiave** - Quando questa opzione è selezionata, è necessario fornire una stringa di identificazione.

In questo esempio, selezioneremo **Full Qualified Domain Name** (Nome di dominio completo) e immetteremo **test.cisco.com** nel campo *FQDN String* (Stringa FQDN).



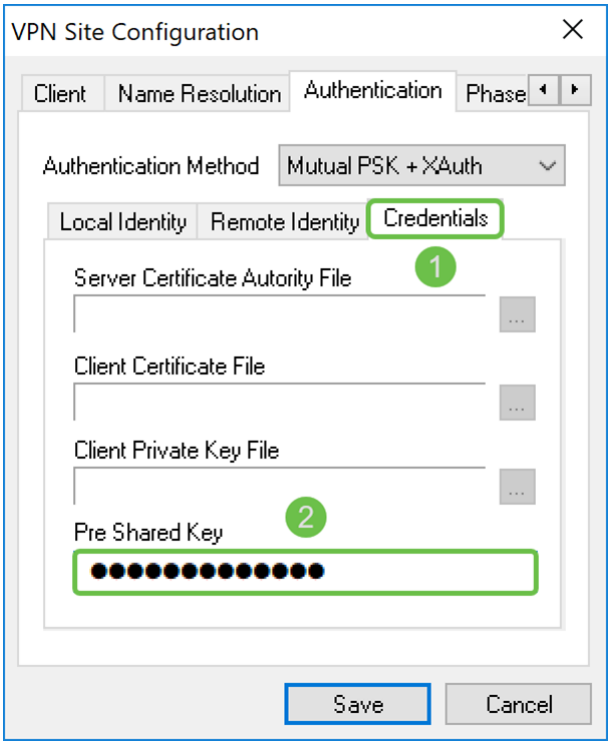
Passaggio 3. Fare clic sulla scheda *Identità remota* e selezionare il tipo di identificazione. Le opzioni includono: Qualsiasi nome di dominio completo, nome di dominio completo dell'utente, indirizzo IP o identificatore della chiave.

Nel presente documento, verrà utilizzato **Any** come tipo di identificazione.



Passaggio 4. Fare clic sulla scheda *Credenziali* e immettere la stessa chiave precondivisa configurata sull'RV160/RV260.

Entreremo in **CiscoTest123!** nel campo *Chiave già condivisa*.

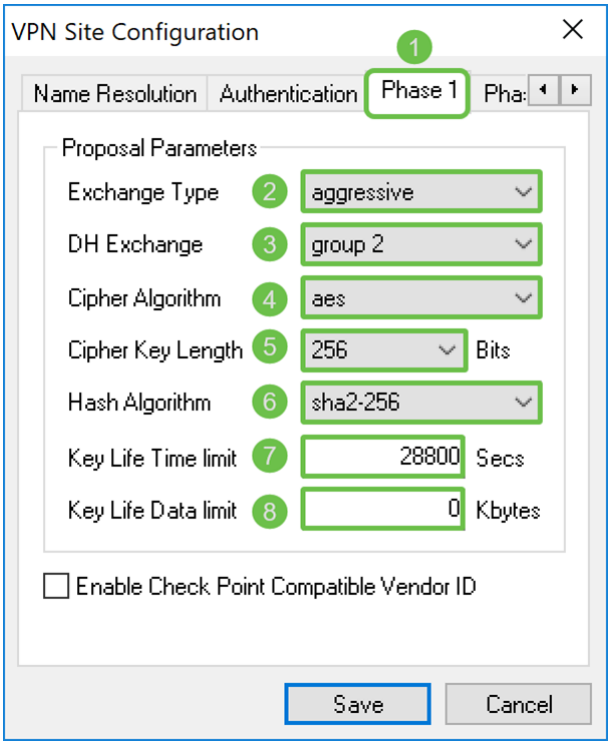


Mostra client VPN software: Scheda Fase 1

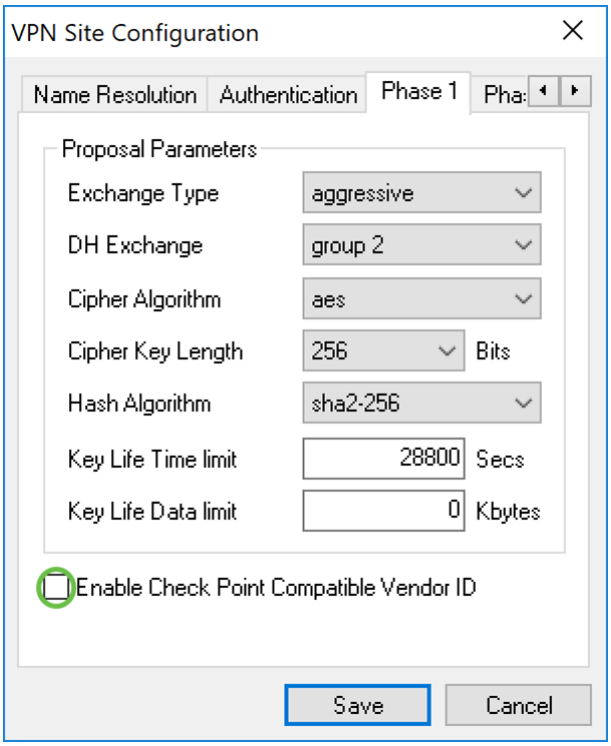
Passaggio 1. Fare clic sulla scheda *Fase 1*. Configurare i seguenti parametri in modo che abbiano le stesse impostazioni configurate per RV160/RV260.

I parametri di Shrew Soft devono corrispondere alla configurazione di RV160/RV260 selezionata nella fase 1. In questo documento, i parametri di Shrew Soft verranno impostati come segue:

- Tipo di scambio: **aggressivo**
- DH Exchange: **gruppo 2**
- Algoritmo di crittografia: **aes**
- Lunghezza della chiave di crittografia: **256**
- Algoritmo hash: **sha2-256**
- Durata massima chiave: **28800**
- Limite dati durata chiave: **0**



Passaggio 2. (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 gate non offre un ID fornitore compatibile con Cisco o non si è certi, lasciare la casella di controllo deselezionata. La casella di controllo rimarrà deselezionata.



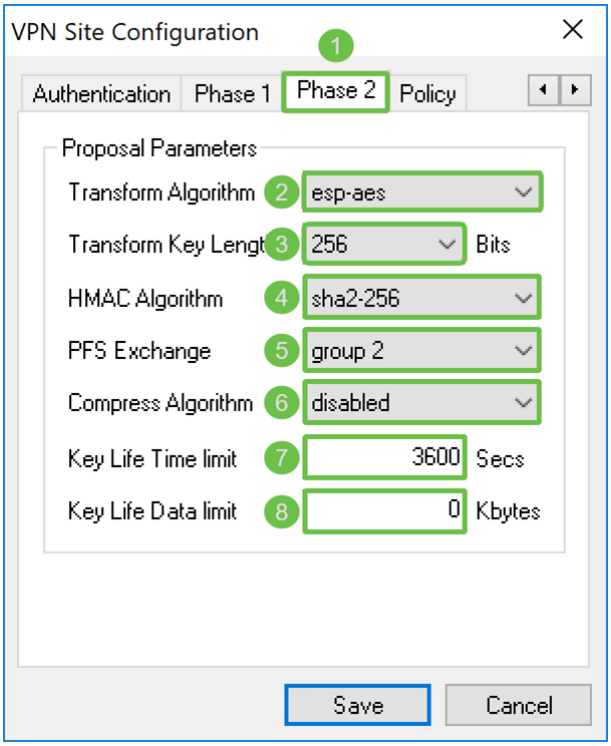
Mostra client VPN software: Scheda Fase 2

Passaggio 1. Fare clic sulla scheda *Fase 2*. Configurare i seguenti parametri in modo che abbiano le stesse impostazioni configurate per RV160/RV260.

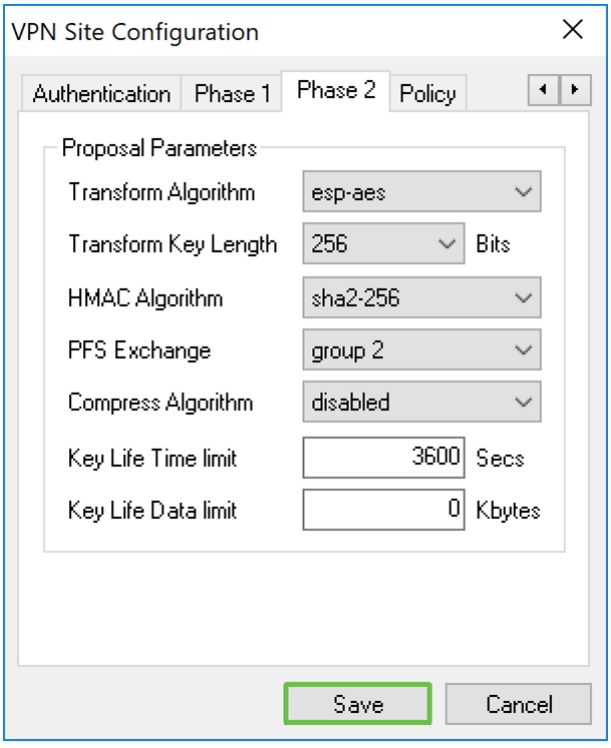
I parametri devono corrispondere alla configurazione di RV160/260 nella fase 2 come segue:

- Algoritmo di trasformazione: **esp-aes**

- Lunghezza chiave di trasformazione: **256**
- Algoritmo HMAC: **sha2-256**
- Scambio PFS: **gruppo 2**
- Algoritmo di compressione: **disattivato**
- Durata massima chiave: **3600**
- Limite dati durata chiave: **0**



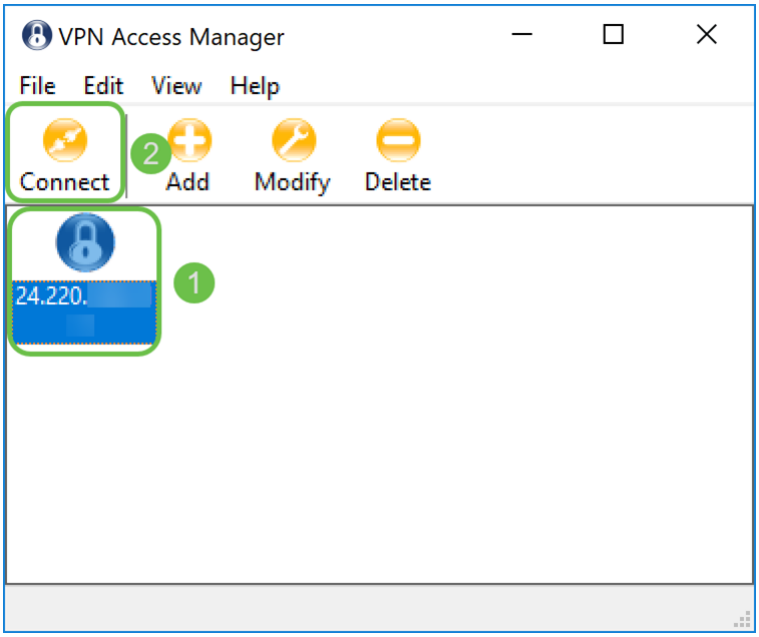
2. Premere il pulsante **Save** in fondo alla pagina per salvare la configurazione.



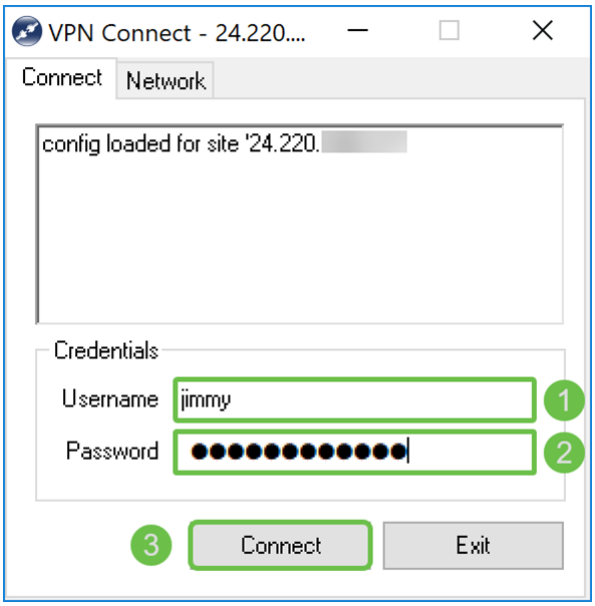
Mostra client VPN software: Connessione

Passaggio 1. In *VPN Access Manager*, selezionare il profilo VPN appena creato. Quindi premere **Connect** (Connetti).

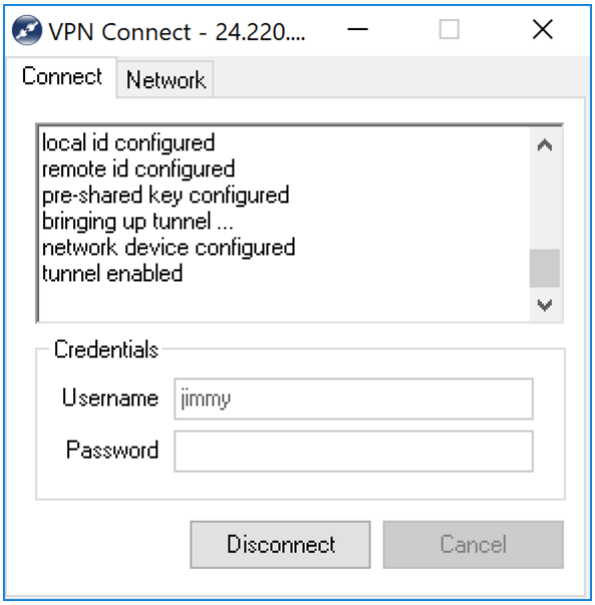
Nota: Per rinominare il profilo VPN, fare clic con il pulsante destro del mouse su di esso e selezionare **Rinomina**. Parte dell'indirizzo IP nel profilo è sfocata per proteggere la rete.



Passaggio 2. Viene visualizzata la finestra *VPN Connect*. Immettere il nome utente e la password creati nella sezione *Creazione account utente*. Quindi premere **Connect** (Connetti).

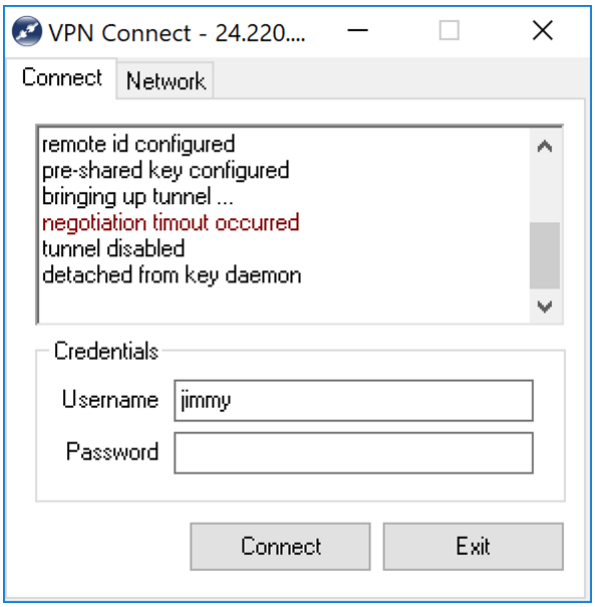


Passaggio 3. Dopo aver premuto *Connect*, le informazioni di configurazione vengono passate al daemon IKE insieme a una richiesta di comunicazione. Nella finestra di output vengono visualizzati diversi messaggi relativi allo stato della connessione. Se la connessione ha esito positivo, verrà visualizzato il messaggio "dispositivo di rete configurato" e "tunnel abilitato". Il pulsante *Connessione* diventerà il pulsante *Disconnetti*.

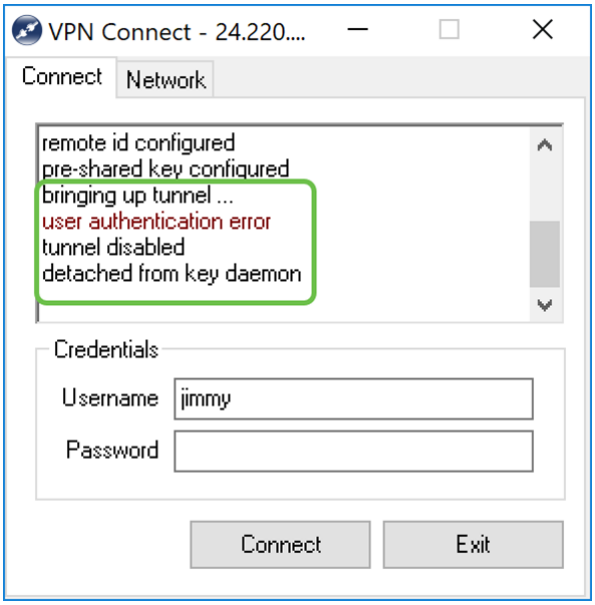


Suggerimenti per la risoluzione dei problemi di connessione VPN

Se vengono visualizzati messaggi di errore nei quali è indicato che si è verificato il timeout della negoziazione, che il tunnel è stato disabilitato e che il daemon della chiave è stato scollegato. È possibile verificare due volte la configurazione sul router e sul client Show Soft VPN per verificare che corrispondano.

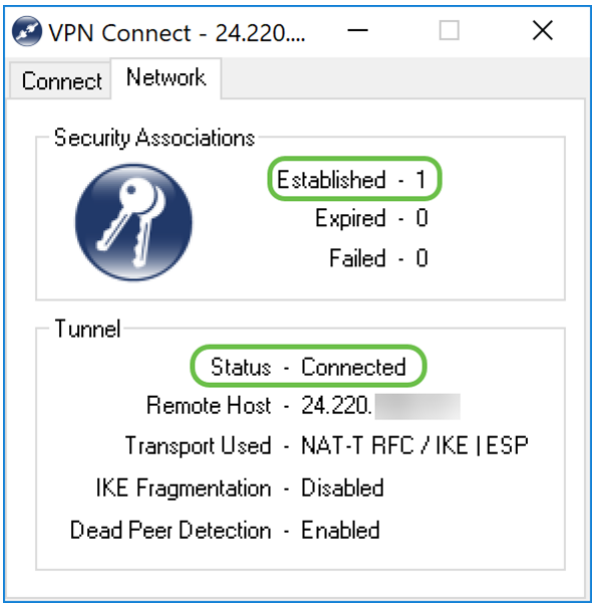


Se viene visualizzato il messaggio di errore "user authentication error" (Errore di autenticazione utente), significa che è stata immessa una password errata per quel nome utente. Verificare le credenziali dell'utente e che siano state configurate e immesse correttamente.

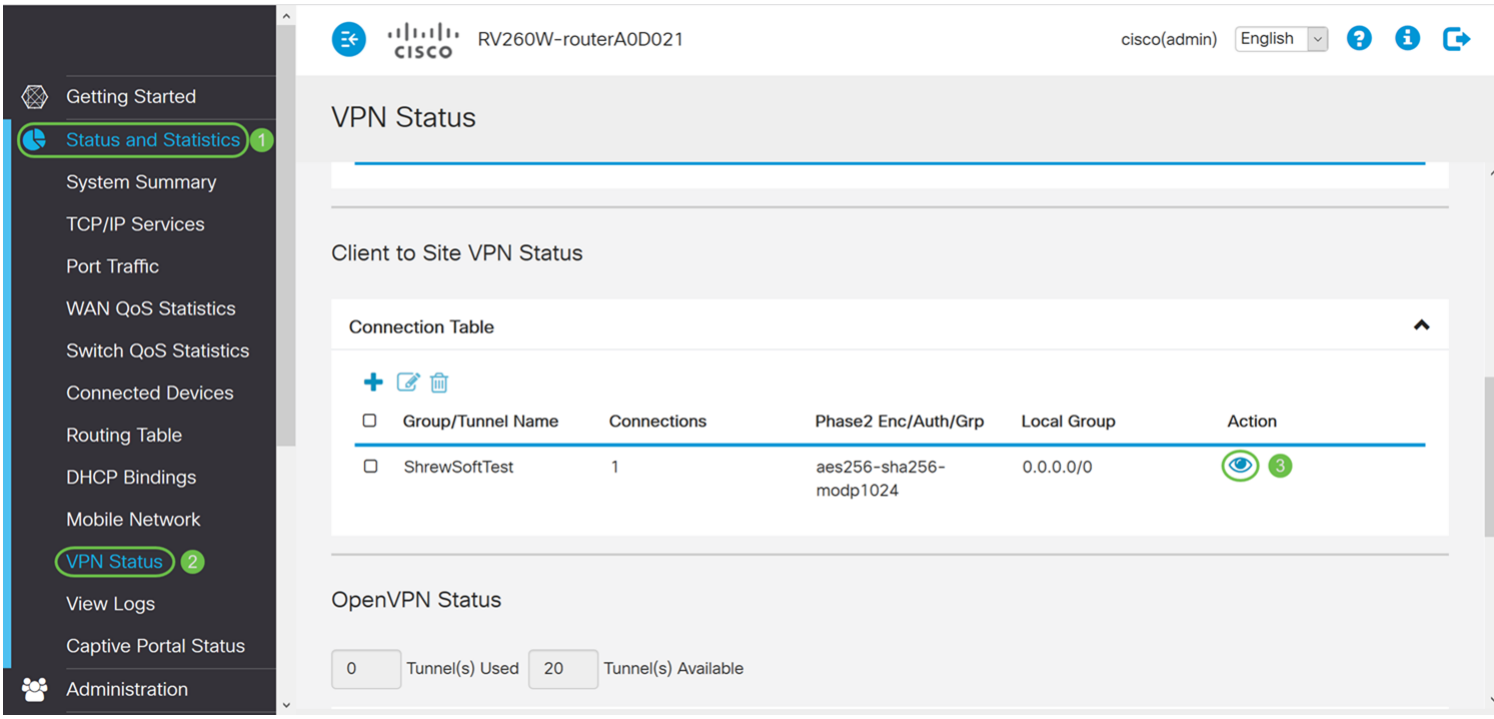


Verifica

Passaggio 1. Fare clic sulla scheda *Network* (Rete) nella finestra *VPN connect* (Connessione VPN). In questa scheda dovrebbe essere possibile visualizzare le statistiche di rete correnti per la connessione. Nella sezione *Tunnel*, è visualizzato *Connesso* come stato.

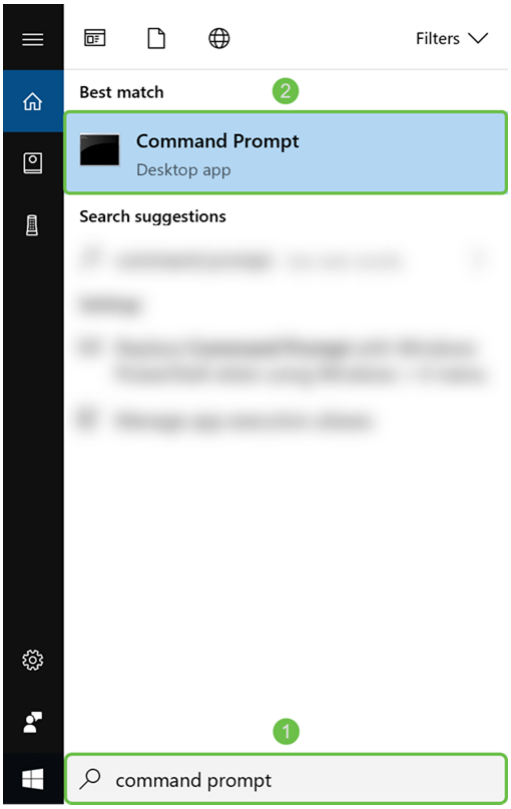


Passaggio 2. Sul router, selezionare **Status and Statistics > VPN Status** (Stato e statistiche). Nella pagina *Stato VPN* scorrere verso il basso fino alla sezione *Stato VPN da client a sito*. In questa sezione è possibile visualizzare tutte le connessioni da client a sito. Fare clic sull'icona **occhio** per visualizzare ulteriori dettagli.



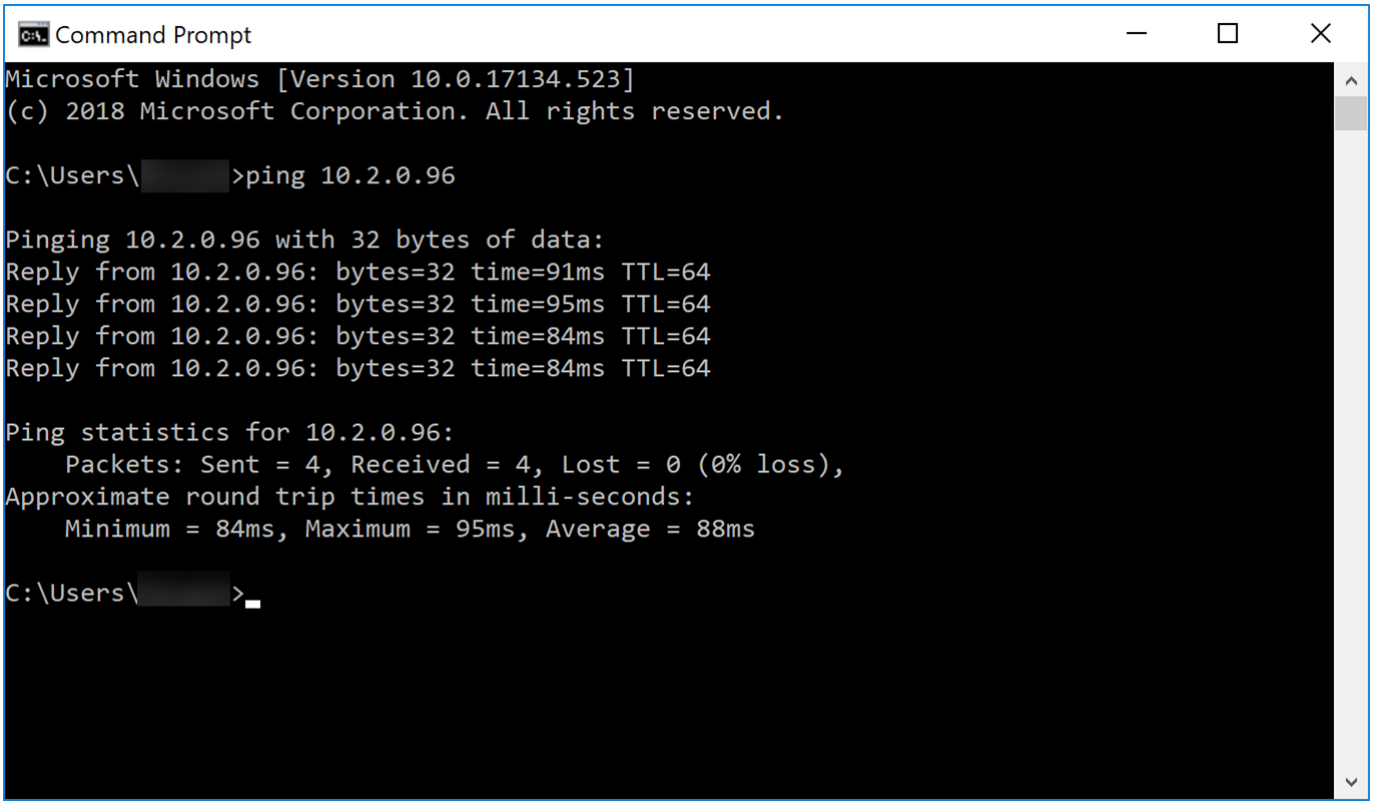
Passaggio 3. Passare alla barra di ricerca sulla barra delle applicazioni e cercare **Prompt dei comandi**.

Nota: Le seguenti istruzioni sono utilizzate in un sistema operativo Windows 10. Questa impostazione può variare a seconda del sistema operativo in uso.



Passaggio 4. Digitare il comando senza virgolette, "**ping [*indirizzo IP privato del router*]**" ma immettere l'indirizzo IP privato anziché le parole. Dovrebbe essere possibile eseguire correttamente il ping dell'indirizzo IP privato del router.

Nell'esempio, verrà digitato **ping 10.2.0.96**. 10.2.0.96 è l'indirizzo IP privato del router.



Conclusioni

A questo punto, il client Smart Soft VPN dovrebbe essere connesso correttamente a RV160 o RV260.