Configurazione di VPN (Virtual Private Network) da client singolo a gateway su RV320 e RV325 VPN Router

Obiettivo

L'obiettivo di questo documento è mostrare come configurare un singolo client per gateway con una VPN (Virtual Private Network) sui router VPN serie RV32x.

Introduzione

Una VPN è una rete privata utilizzata per connettere virtualmente un utente remoto tramite una rete pubblica. Un tipo di VPN è una VPN da client a gateway. Una VPN da client a gateway è una connessione tra un utente remoto e la rete. Il client è configurato nel dispositivo dell'utente con software client VPN. Consente agli utenti di connettersi in modo sicuro a una rete in modalità remota.

Dispositivi interessati

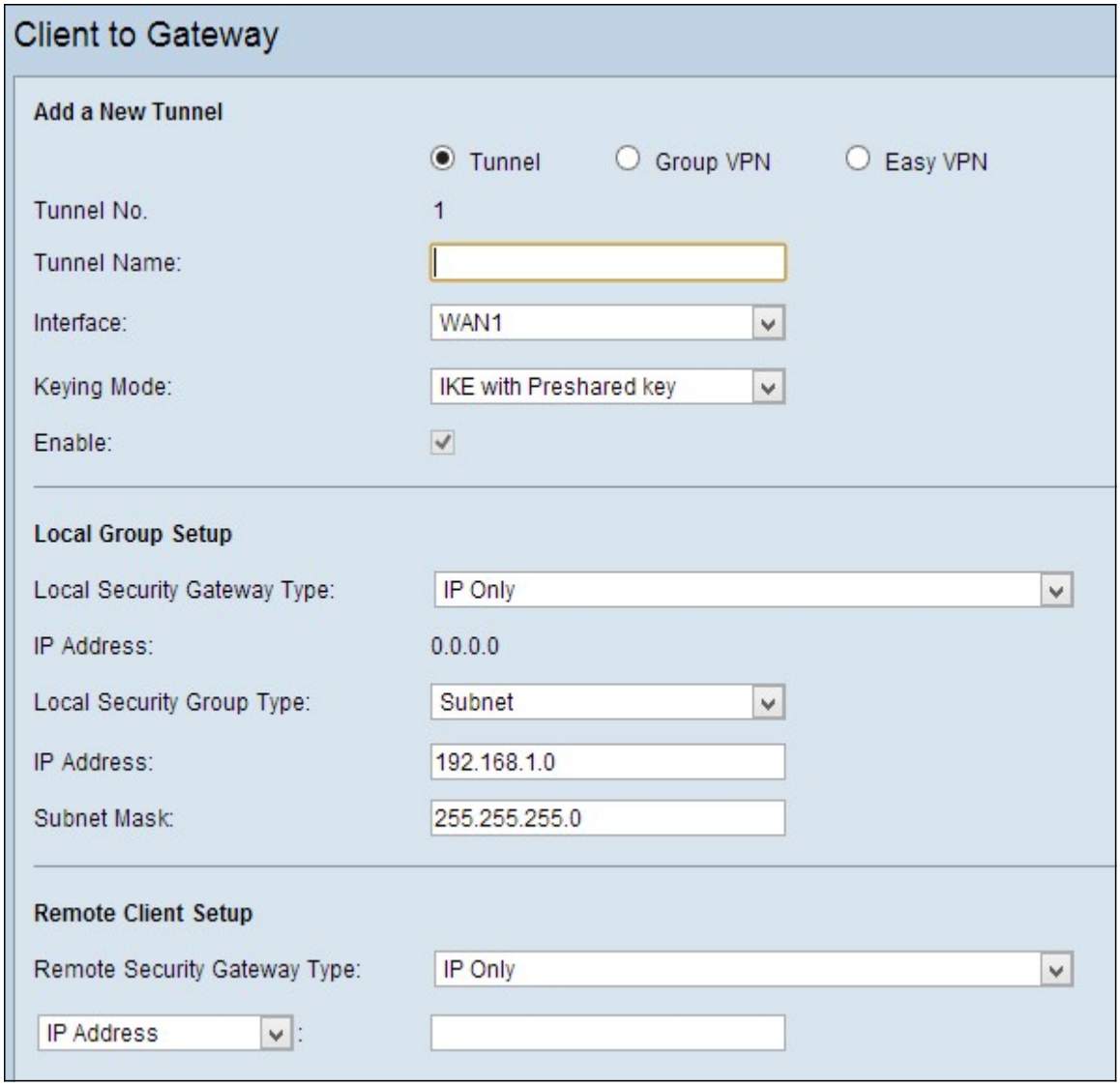
- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

Versione del software

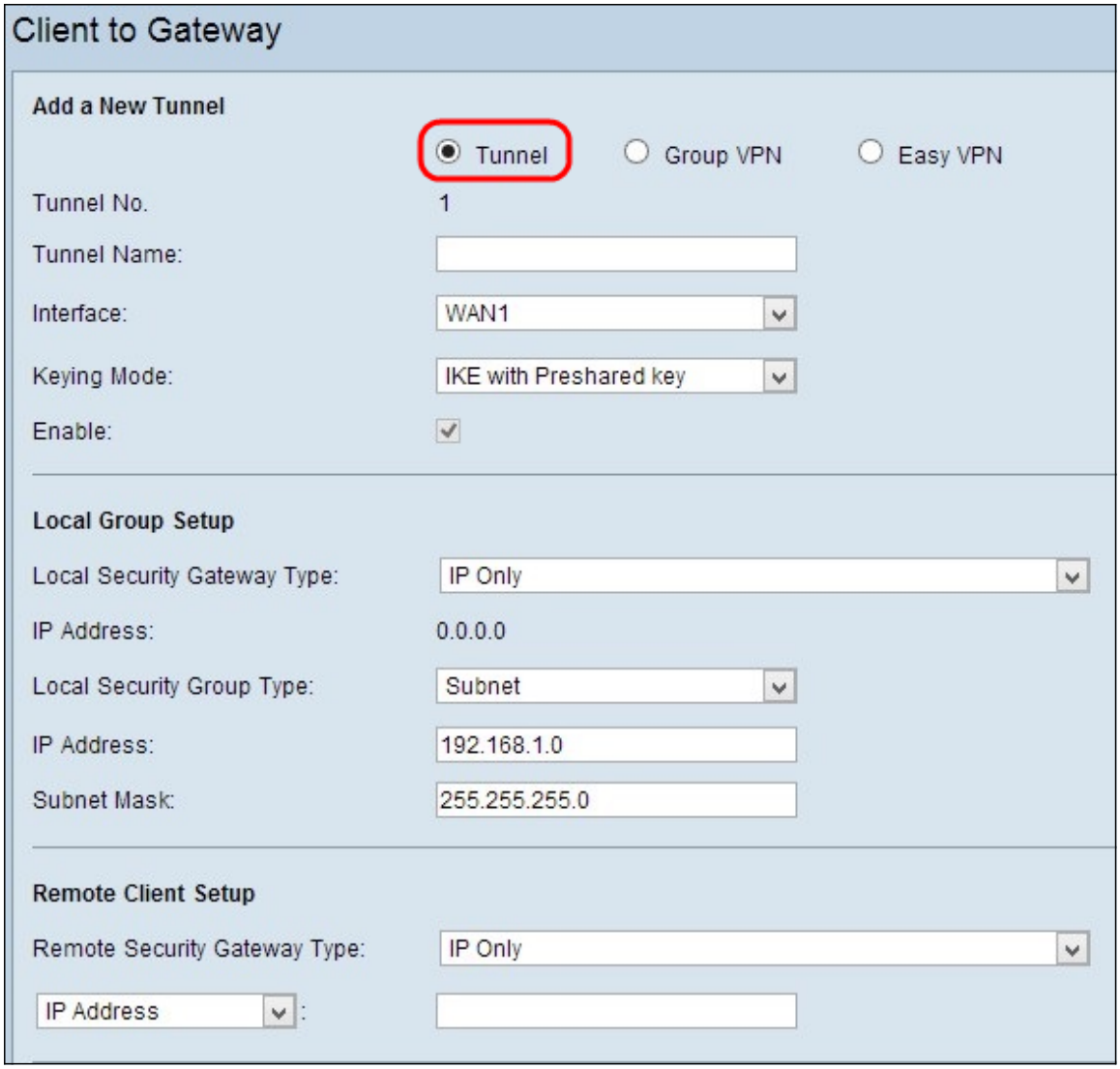
- v1.1.0.09

Configurazione di VPN da client singolo a gateway

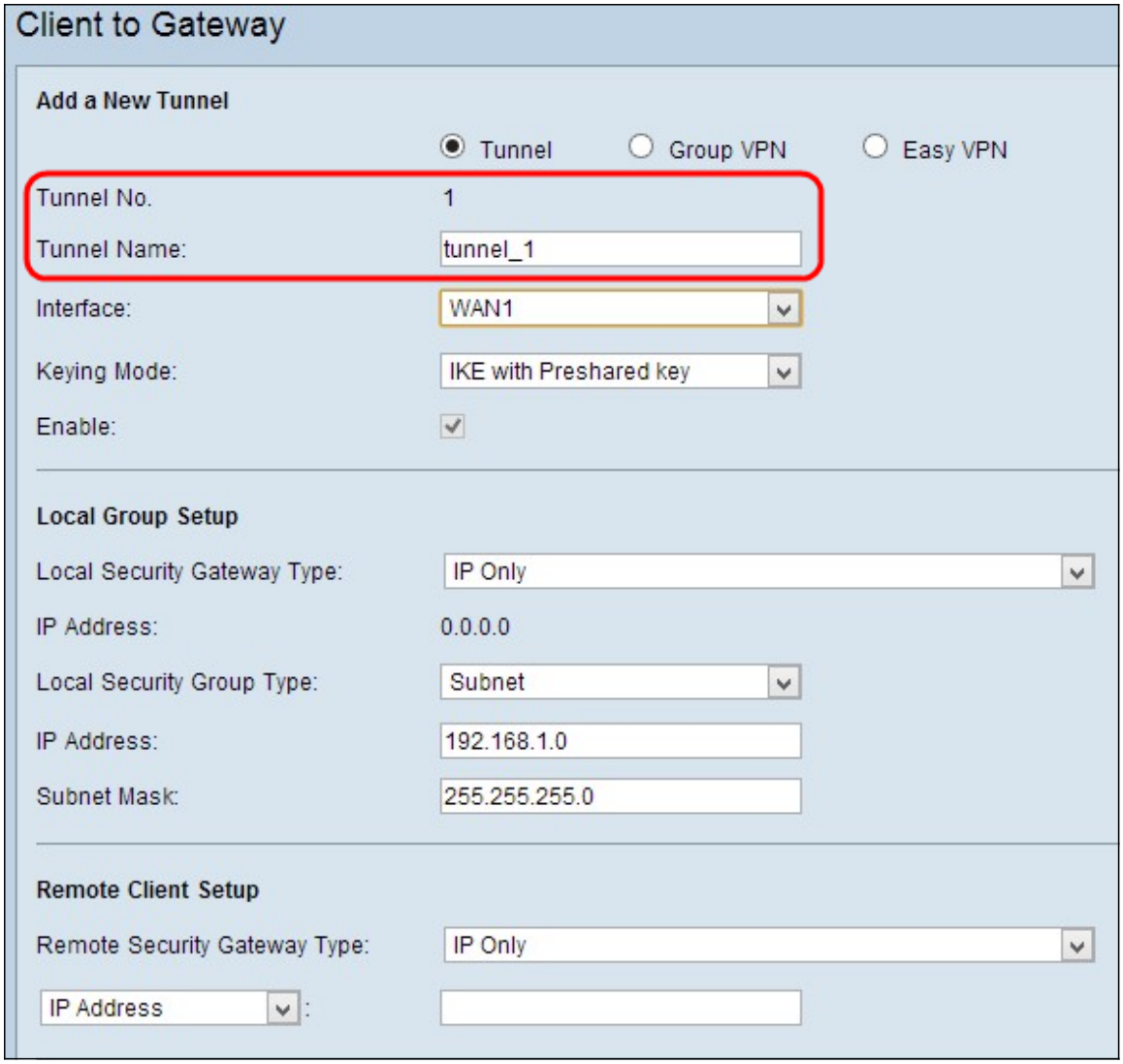
Passaggio 1. Accedere all'utility di configurazione Web e scegliere **VPN > Da client a gateway**. Viene visualizzata la pagina *Da client a gateway*:



Passaggio 2. Fare clic sul pulsante di opzione **Tunnel** per aggiungere un singolo tunnel per la VPN da client a gateway.



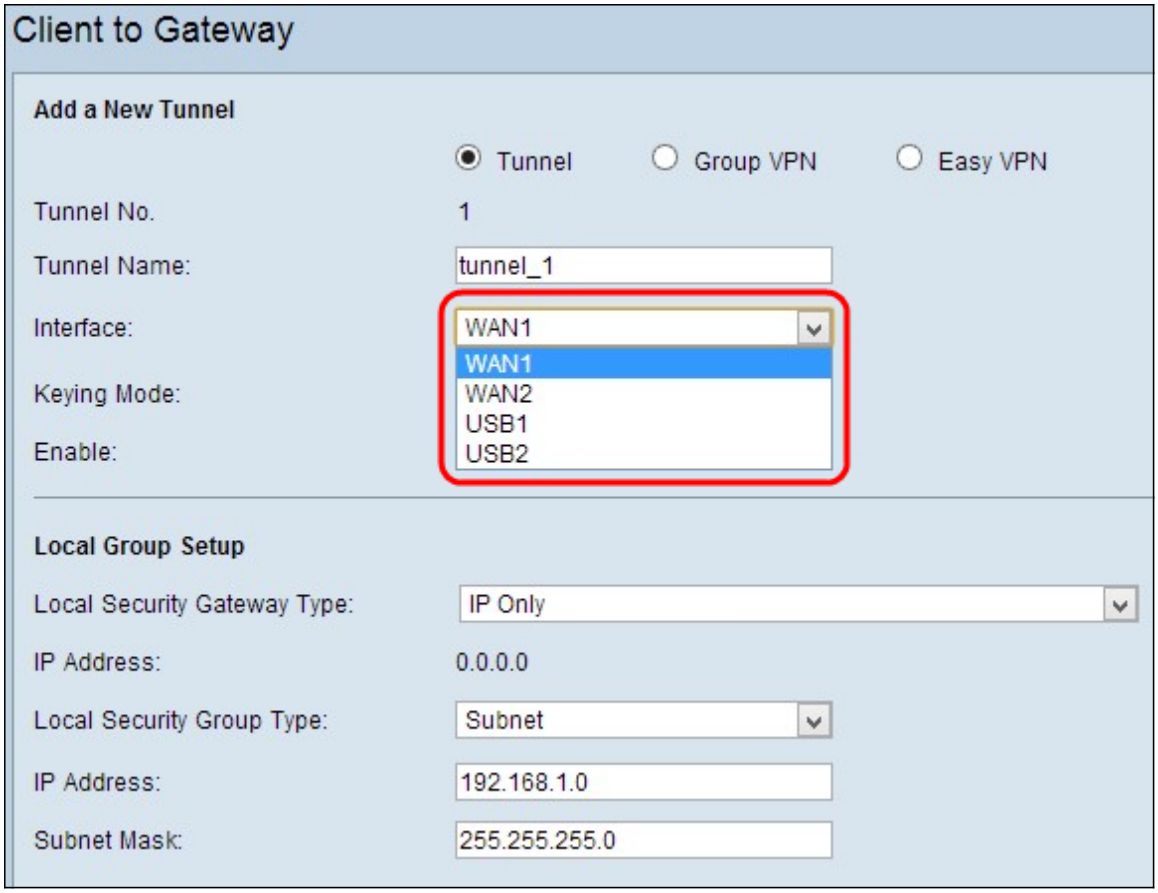
Aggiungi nuovo tunnel



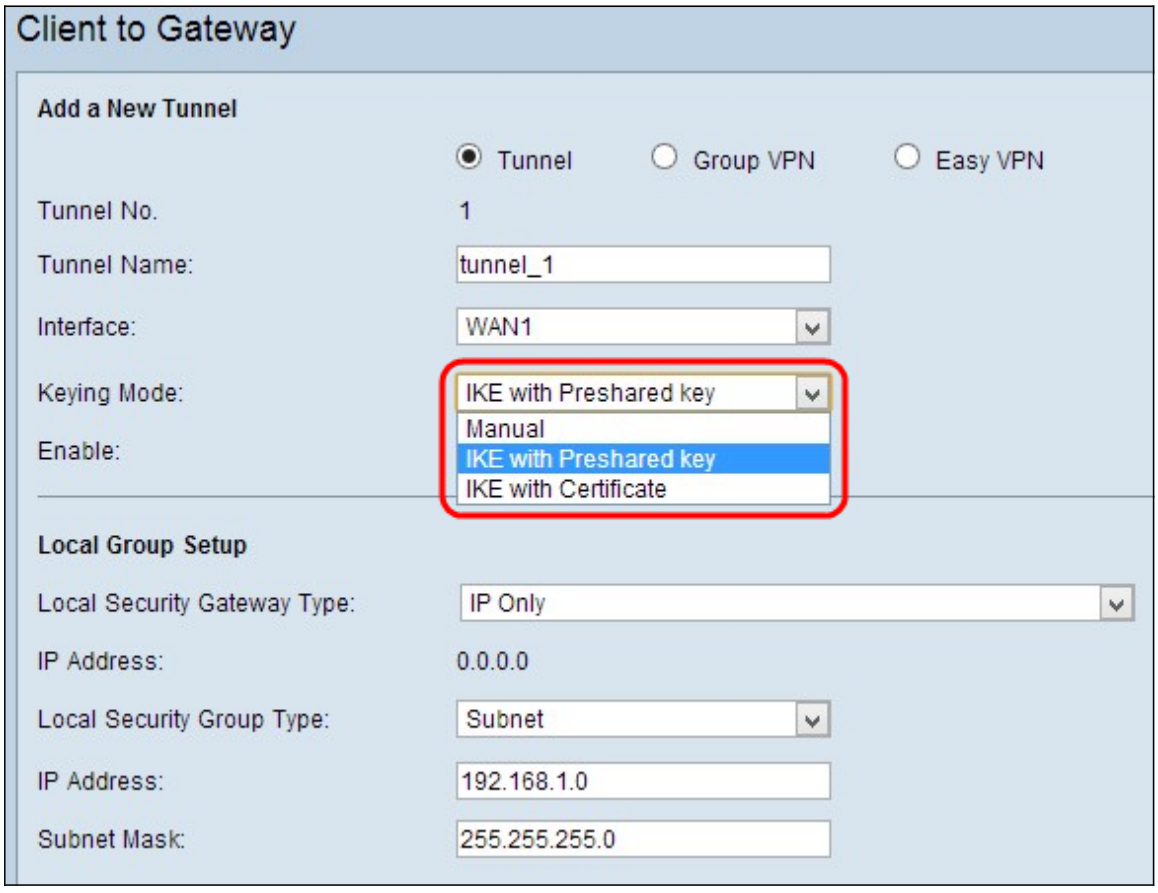
Nota: N. tunnel: rappresenta il numero del tunnel. Questo numero viene generato automaticamente.

Passaggio 1. Immettere il nome del tunnel nel campo *Nome tunnel*.

Passaggio 2. Selezionare l'interfaccia tramite la quale il client remoto accede alla VPN dall'elenco a discesa *Interfaccia*.



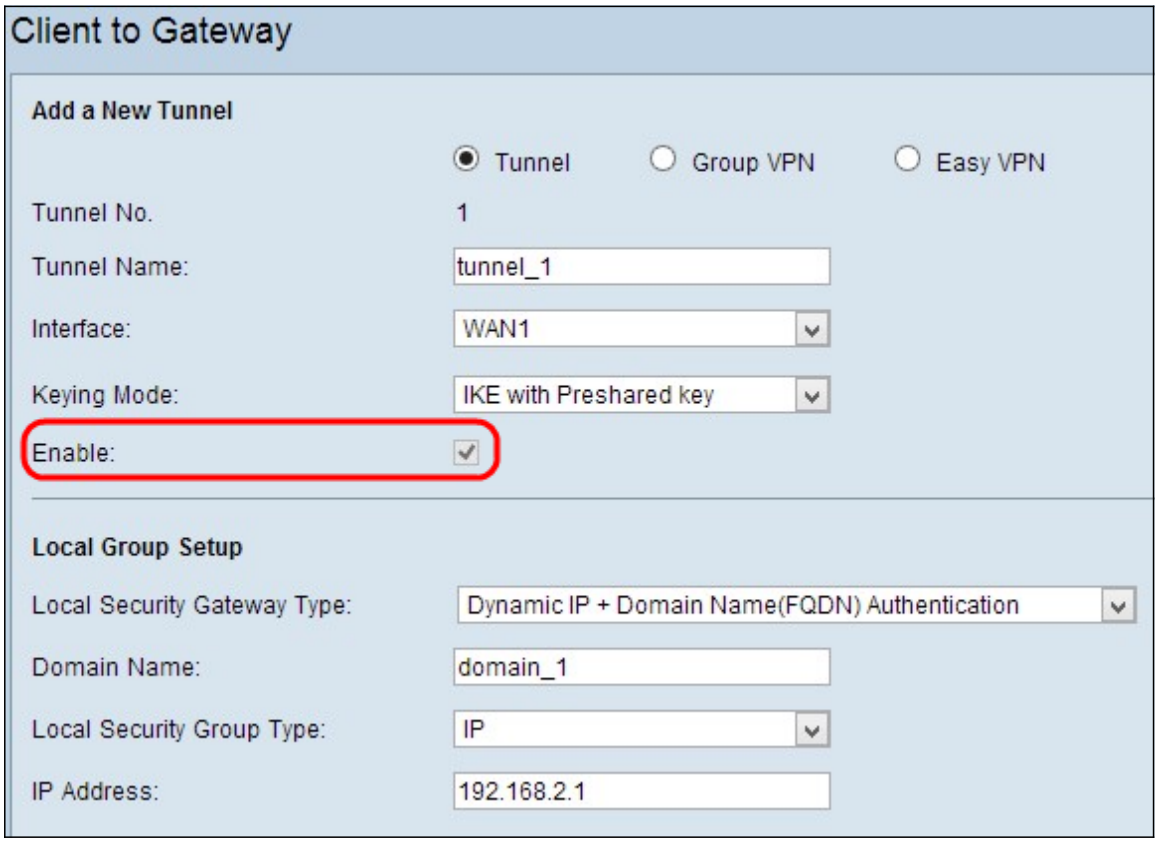
Passaggio 3. Scegliere la modalità di gestione delle chiavi appropriata per garantire la protezione dall'elenco a discesa *Modalità di impostazione chiavi*. La modalità predefinita è IKE con chiave già condivisa.



Le opzioni sono definite come segue:

- Manuale: modalità di protezione personalizzata che consente di generare una nuova chiave di protezione autonomamente e di non eseguire alcuna negoziazione con la chiave. È consigliabile utilizzarlo durante la risoluzione dei problemi o in un ambiente statico di piccole dimensioni.
- IKE con chiave già condivisa: il protocollo IKE (Internet Key Exchange) viene utilizzato per generare e scambiare automaticamente una chiave già condivisa per stabilire la comunicazione autenticata per il tunnel.
- IKE con certificato - Il protocollo IKE (Internet Key Exchange) con certificato è un metodo più sicuro per generare e scambiare automaticamente le chiavi già condivise in modo da garantire una comunicazione più sicura per il tunnel.

Passaggio 4. Selezionare la casella di controllo **Abilita** per abilitare la VPN da client a gateway. È attivata per impostazione predefinita.



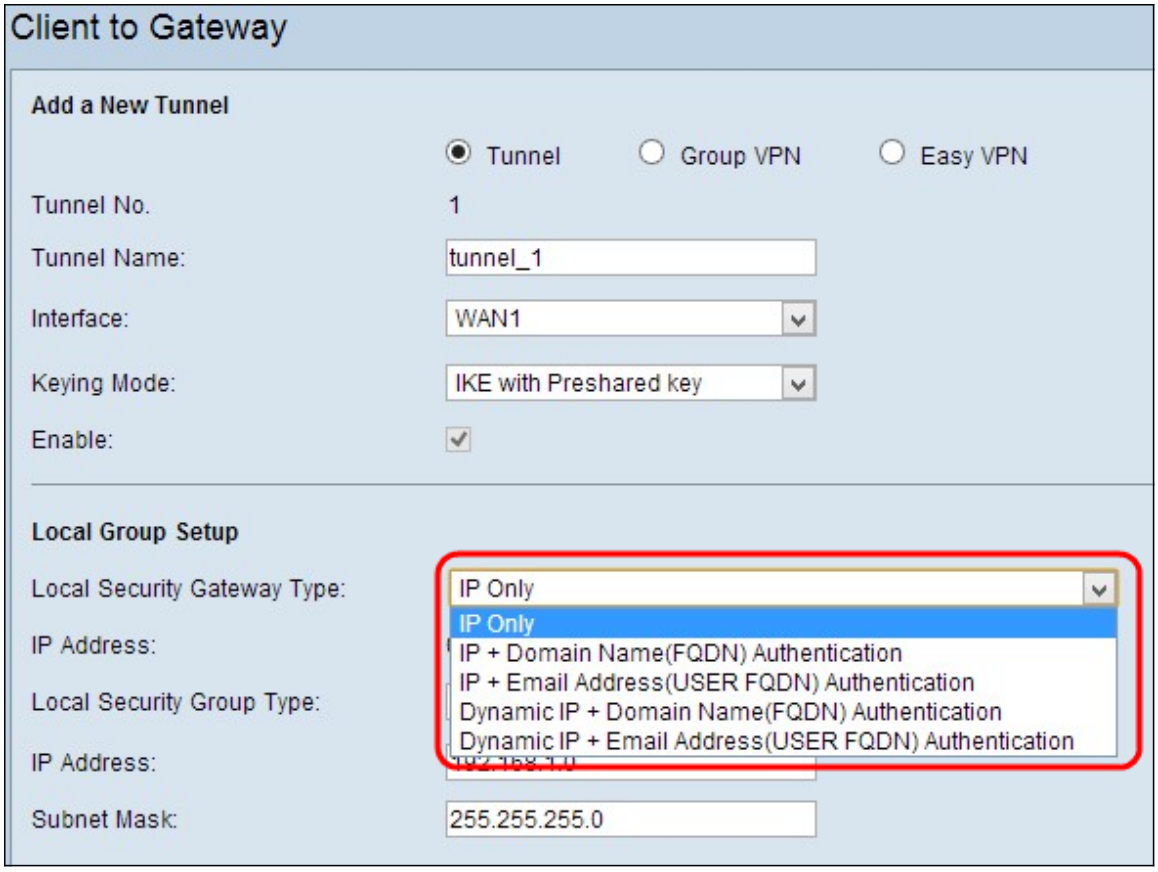
Passaggio 5. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Installazione gruppo locale

Configurazione gruppo locale con manuale o IKE con chiave già condivisa

Nota: Attenersi alla procedura seguente se si sceglie Manuale o IKE con chiave già condivisa dall'elenco a discesa *Modalità di impostazione chiavi* nel Passaggio 3 della sezione *Aggiunta di un nuovo tunnel*.

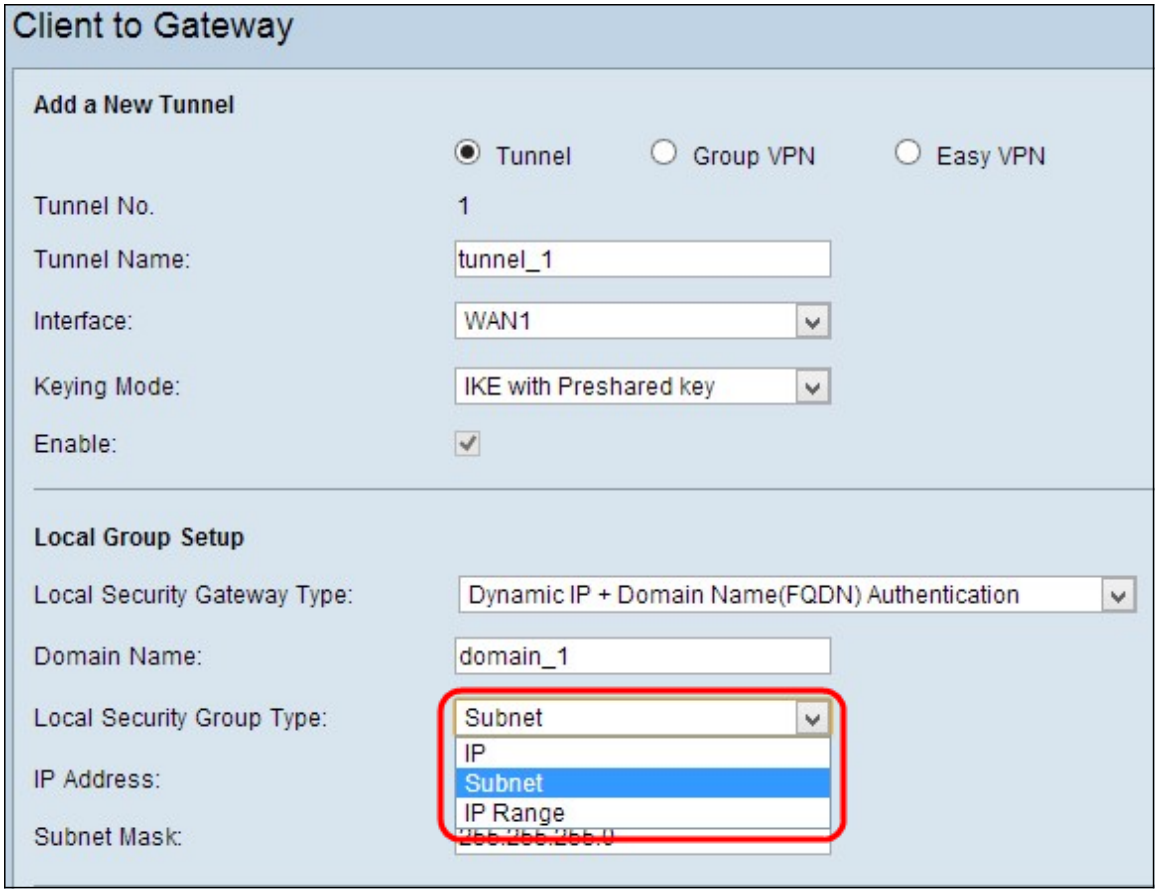
Passaggio 1. Per stabilire un tunnel VPN, selezionare il metodo di identificazione del router appropriato dall'elenco a discesa *Gateway di sicurezza locale*.



Le opzioni sono definite come segue:

- Solo IP: l'accesso al tunnel è possibile solo tramite una rete IP statica WAN. È possibile scegliere questa opzione se solo il router ha un IP WAN statico. L'indirizzo IP statico della WAN viene generato automaticamente.
- Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo *Nome dominio*. L'indirizzo IP statico della WAN viene generato automaticamente.
- Autenticazione IP + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'indirizzo e-mail nel campo *Indirizzo e-mail*. L'indirizzo IP statico della WAN viene generato automaticamente.
- Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo *Nome dominio*.
- Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'indirizzo e-mail nel campo *Indirizzo e-mail*.
- IP Address: rappresenta l'indirizzo IP dell'interfaccia WAN. È un campo di sola lettura.

Passaggio 2. Selezionare l'utente o il gruppo di utenti LAN locale appropriato che può accedere al tunnel VPN dall'elenco a discesa *Tipo di gruppo di sicurezza locale*. Il valore predefinito è Subnet.

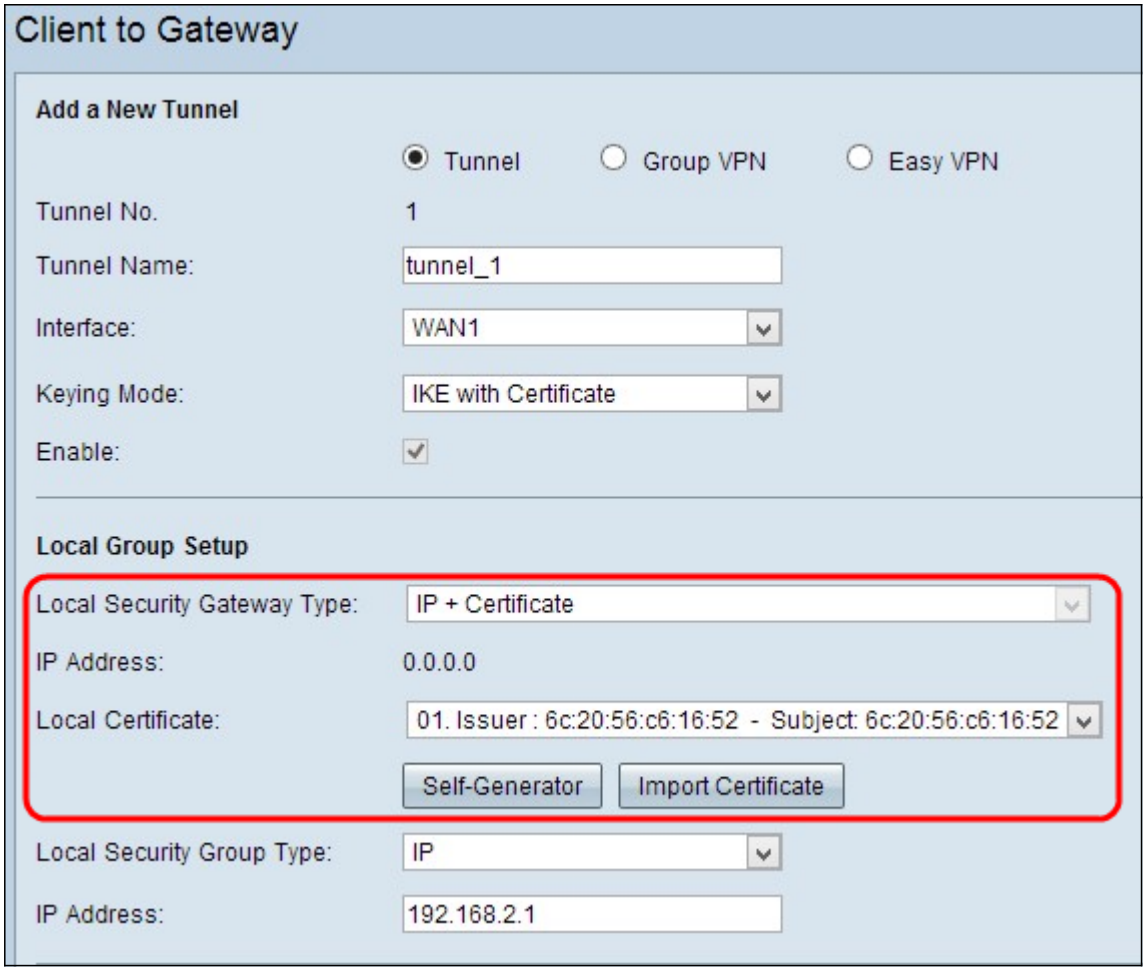


- IP - Solo un dispositivo LAN specifico può accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP del dispositivo LAN nel campo *IP Address* (Indirizzo IP). L'indirizzo IP predefinito è 192.168.1.0.
- Subnet: tutti i dispositivi LAN su una subnet specifica possono accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP e la subnet mask dei dispositivi LAN rispettivamente nei campi *Indirizzo IP* e *Subnet mask*. La maschera predefinita è 255.255.255.0.
- Intervallo IP - Una serie di dispositivi LAN può accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP iniziale e quello finale rispettivamente nei campi *IP iniziale* e *IP finale*. L'intervallo predefinito è compreso tra 192.168.1.0 e 192.168.1.254.

Passaggio 3. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Configurazione gruppo locale con IKE con certificato per VPN tunnel

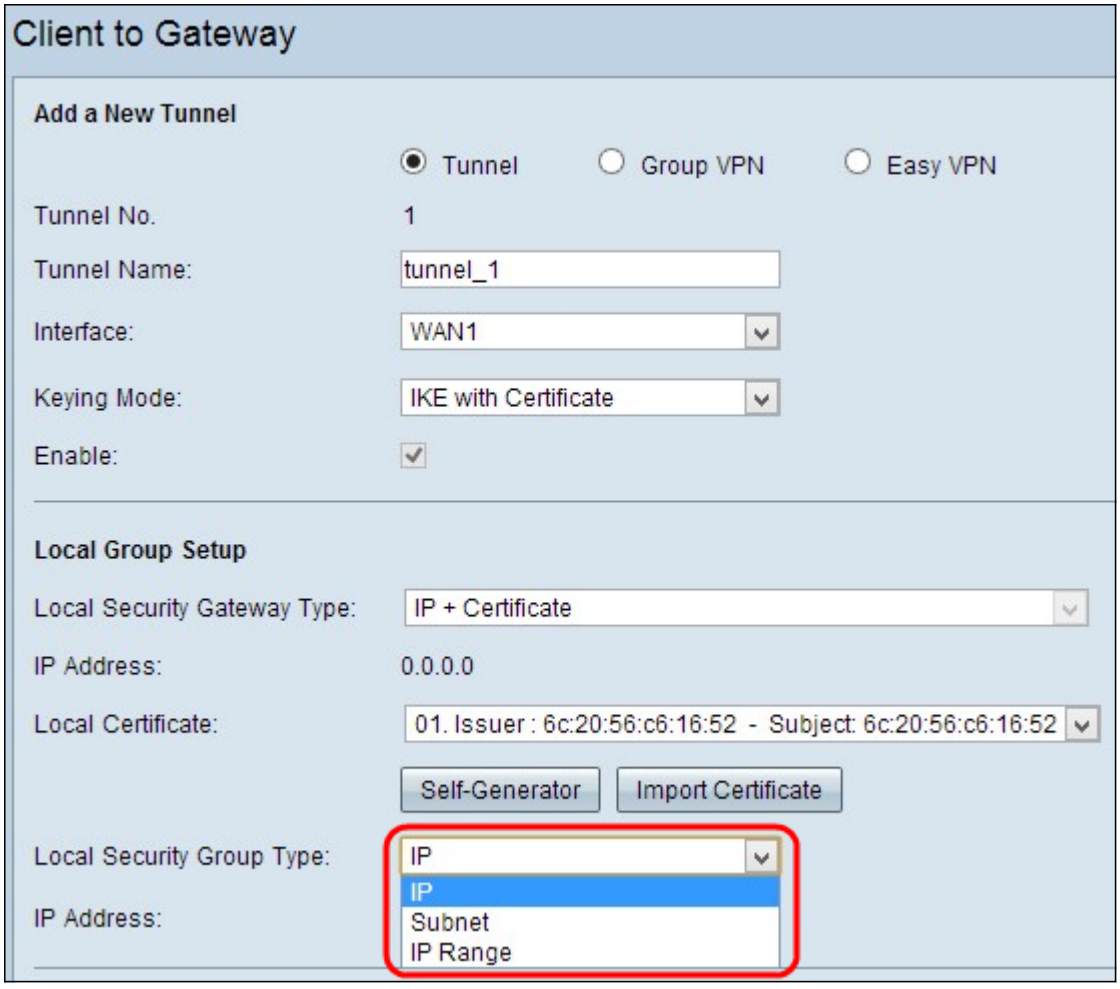
Nota: Se è stato selezionato IKE con certificato dall'elenco a discesa *Modalità di impostazione chiavi* nel passaggio 3 della sezione *Aggiunta di un nuovo tunnel,* eseguire la procedura seguente.



- Tipo di gateway di sicurezza locale: è possibile accedere al tunnel tramite IP con un certificato.
- IP Address: rappresenta l'indirizzo IP dell'interfaccia WAN. È un campo di sola lettura.

Passaggio 1. Scegliere il certificato locale appropriato per identificare il router dall'elenco a discesa *Certificato locale*. Fare clic su **Self-Generator** per generare il certificato automaticamente oppure fare clic su **Importa certificato** per importare un nuovo certificato.

Nota: per ulteriori informazioni su come generare automaticamente i certificati, fare riferimento a *Generazione di certificati su router RV320* e per informazioni su come importare i certificati fare riferimento a *Configurazione del certificato sui router RV320*.



Passaggio 2. Selezionare il tipo appropriato di utente LAN locale o di gruppo di utenti che possono accedere al tunnel VPN dall'elenco a discesa *Tipo di gruppo di sicurezza locale*. Il valore predefinito è Subnet.

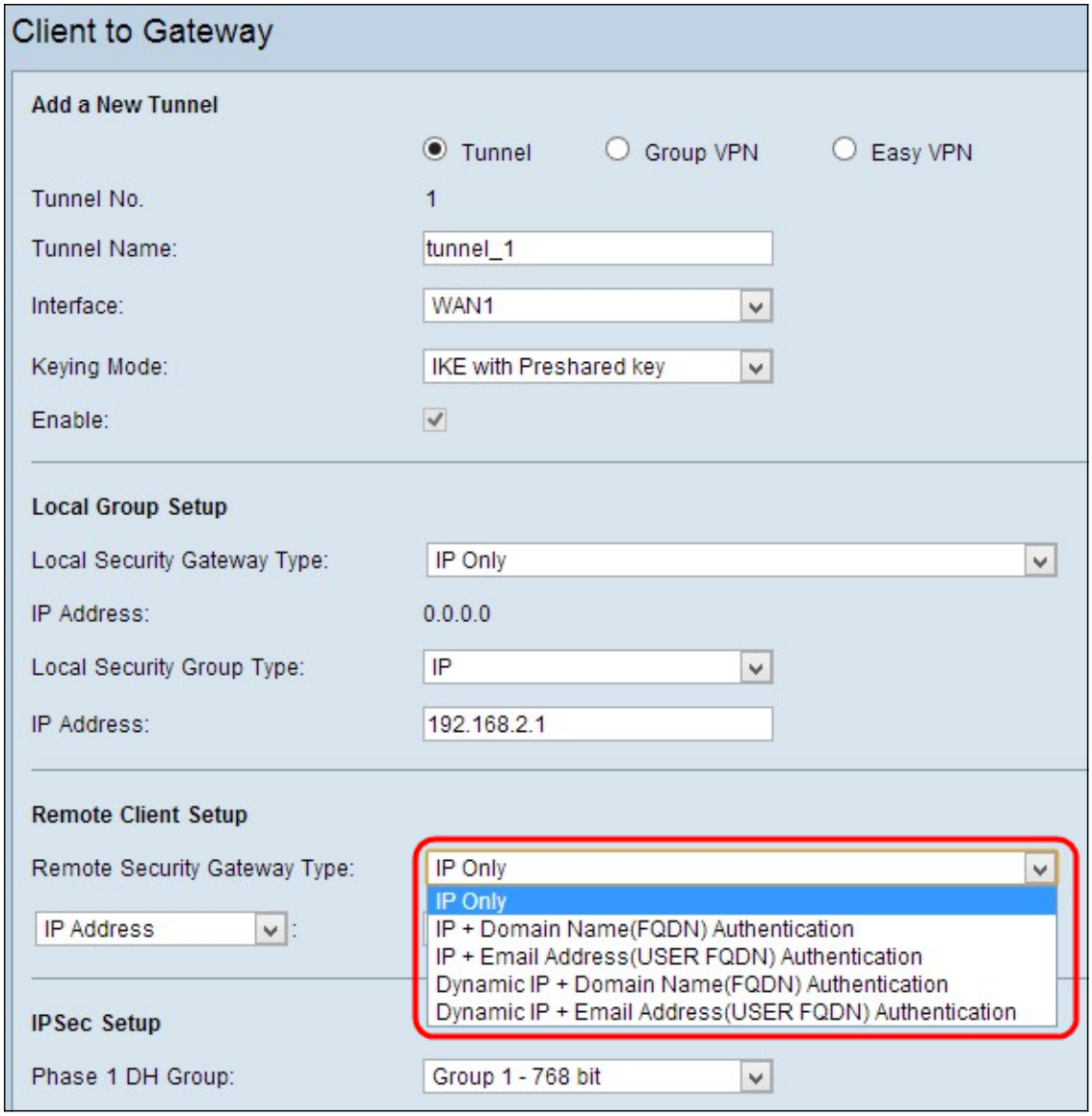
- IP - Solo un dispositivo LAN specifico può accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP del dispositivo LAN nel campo Indirizzo IP. L'indirizzo IP predefinito è 192.168.1.0.
- Subnet: tutti i dispositivi LAN su una subnet specifica possono accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP e la subnet mask dei dispositivi LAN rispettivamente nei campi Indirizzo IP e Subnet mask. La maschera predefinita è 255.255.255.0.
- Intervallo IP - Una serie di dispositivi LAN può accedere al tunnel. Se si sceglie questa opzione, immettere gli indirizzi IP iniziale e finale rispettivamente nei campi IP iniziale e IP finale. L'intervallo predefinito è compreso tra 192.168.1.0 e 192.168.1.254.

Passaggio 3. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Installazione client remota

Installazione client remota con manuale o IKE con chiave già condivisa

Nota: se si sceglie Manuale o IKE con chiave già condivisa dall'elenco a discesa *Modalità di impostazione chiavi* nel passaggio 3 della sezione *Aggiungi nuovo tunnel,* eseguire la procedura seguente.



Passaggio 1. Scegliere il metodo di identificazione del client appropriato per stabilire un tunnel VPN dall'elenco a discesa *Gateway di sicurezza remota*. Il valore predefinito è Solo IP.

- Solo IP: l'accesso al tunnel è possibile solo tramite l'IP WAN statico del client. È possibile scegliere questa opzione solo se si conosce l'IP statico WAN o il nome di dominio del client. Scegliere Indirizzo IP dall'elenco a discesa e immettere l'indirizzo IP statico del client nel campo adiacente oppure scegliere IP da DNS risolto dall'elenco a discesa e immettere il nome di dominio dell'indirizzo IP nel campo adiacente. Tramite il server DNS locale dell'indirizzo IP, il router può recuperare automaticamente l'indirizzo IP.

  Nota: Se si sceglie Manuale dall'elenco a discesa *Modalità di impostazione chiavi* al passaggio 3 della sezione Add a New Tunnel Through Tunnel or Group VPN, questa sarà l'unica opzione disponibile.

- Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico del client e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio. Scegliere Indirizzo IP dall'elenco a discesa e immettere l'indirizzo IP statico del client nel campo adiacente oppure scegliere IP da DNS risolto dall'elenco a discesa e immettere il nome di dominio dell'indirizzo IP nel campo

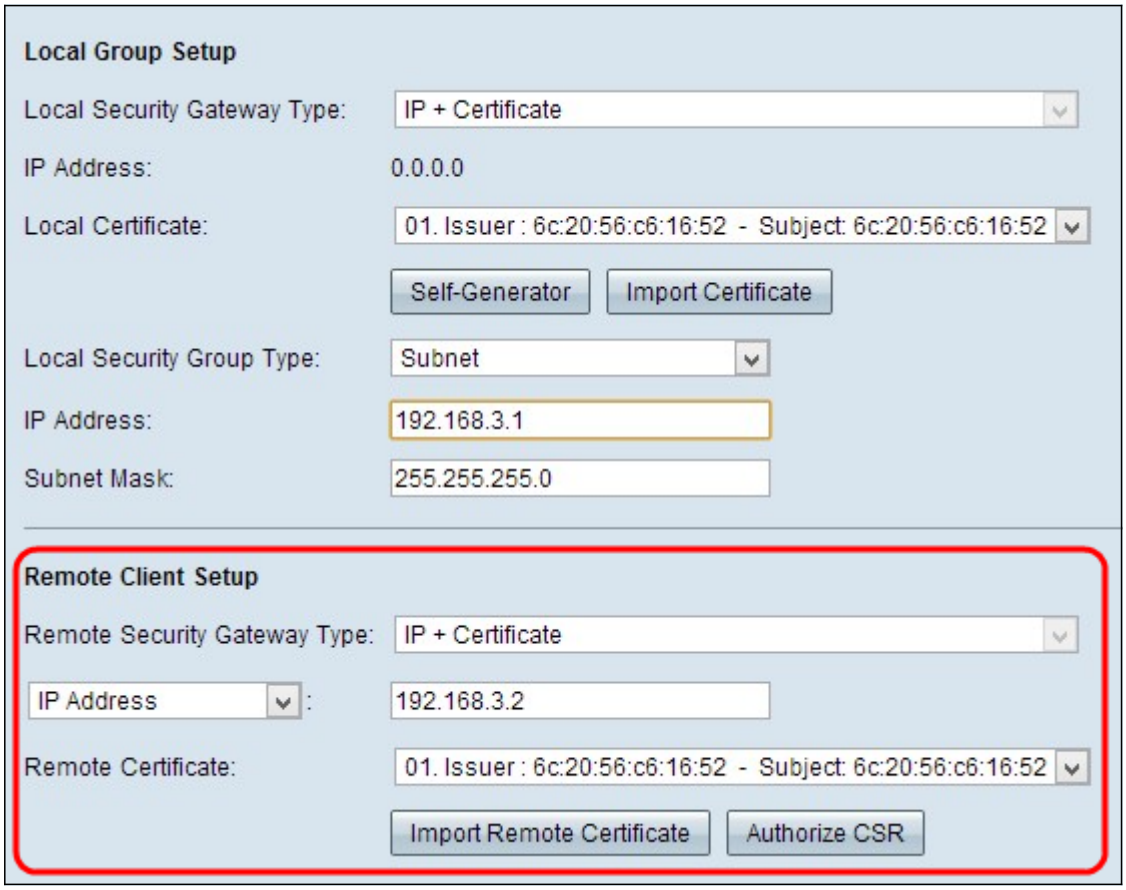
adiacente. Tramite il server DNS locale dell'indirizzo IP, il router può recuperare automaticamente l'indirizzo IP.

- Autenticazione IP + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico del client e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'indirizzo di posta elettronica nel campo Indirizzo di posta elettronica. Scegliere Indirizzo IP dall'elenco a discesa e immettere l'indirizzo IP statico del client nel campo adiacente oppure scegliere IP da DNS risolto dall'elenco a discesa e immettere il nome di dominio dell'indirizzo IP nel campo adiacente. Tramite il server DNS locale dell'indirizzo IP, il router può recuperare automaticamente l'indirizzo IP.
- Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico del client e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.
- Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico del client e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'Indirizzo e-mail nel campo Indirizzo e-mail.

Passaggio 2. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Installazione gruppo remoto con IKE con certificato

Nota: se è stato selezionato IKE con certificato dall'elenco a discesa *Modalità di impostazione chiavi* nel passaggio 3 della sezione *Aggiungi nuovo tunnel,* eseguire la procedura seguente.



- Tipo di gateway di sicurezza remoto: è possibile identificare il client tramite IP con un certificato per stabilire una connessione VPN.

Passaggio 1. Scegliere **Indirizzo IP** o **IP da DNS risolto** dall'elenco a discesa.

- Indirizzo IP: l'accesso al tunnel è possibile solo tramite l'IP WAN statico del client. È possibile scegliere questa opzione solo se si conosce l'IP WAN statico del client. Immettere l'indirizzo IP statico del client nel campo *Indirizzo IP*.
- IP da DNS risolto: utile se non si conosce l'indirizzo IP del client ma si conosce il dominio di tale indirizzo IP. Immettere il nome di dominio dell'indirizzo IP. Tramite il server DNS locale dell'indirizzo IP, il router può recuperare automaticamente l'indirizzo IP.

Passaggio 2. Scegliere il certificato remoto appropriato dall'elenco a discesa *Certificato remoto*. Fare clic su **Importa certificato remoto** per importare un nuovo certificato oppure fare clic su **Autorizza CSR** per identificare un certificato con una richiesta di firma digitale.

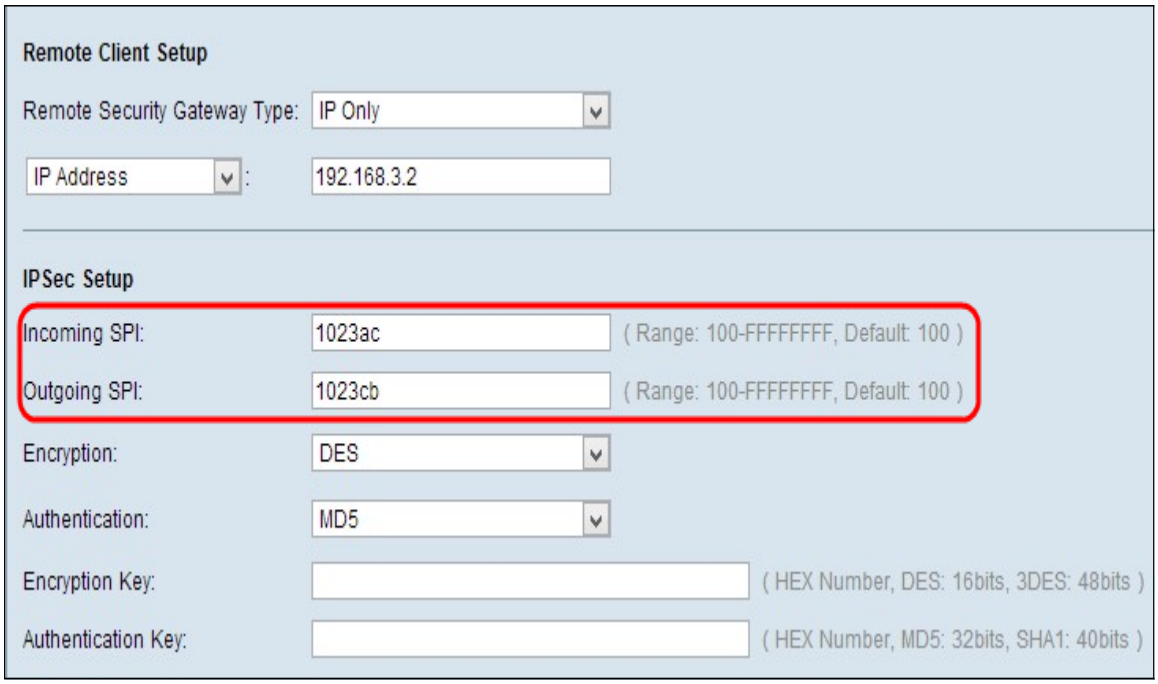
Nota: Per ulteriori informazioni su come importare un nuovo certificato, vedere *Visualizzare/aggiungere un certificato SSL attendibile sui router RV320* e per ulteriori informazioni sull'utilizzo di un certificato protetto (CSR) autorizzato, vedere *Richiesta di firma del certificato (CSR) sui router RV320*.

Passaggio 3. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Installazione di IPSec

Configurazione IPSec con tasto manuale

Nota: se si sceglie Manuale dall'elenco a discesa *Modalità di impostazione chiavi* al passo 3 della sezione *Aggiungi nuovo tunnel,* attenersi alla procedura descritta di seguito.

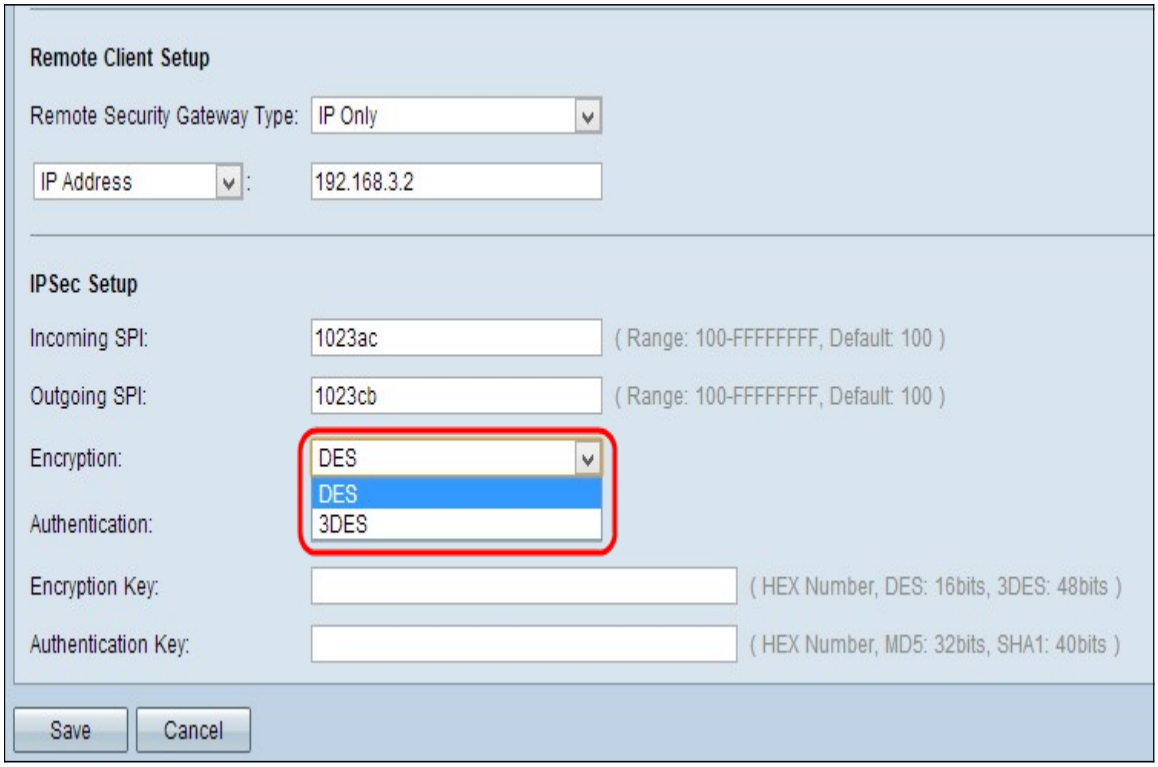


Passaggio 1. Immettere il valore esadecimale univoco per l'indice dei parametri di sicurezza (SPI, Security Parameter Index) in ingresso nel campo *Incoming SPI*. L'indice SPI è contenuto nell'intestazione ESP (Encapsulating Security Payload Protocol), che determina l'associazione di sicurezza (SA) per il pacchetto in ingresso. L'intervallo è compreso tra 100 e ffffffff, il valore predefinito è 100.

Passaggio 2. Immettere il valore esadecimale univoco per l'indice dei parametri di sicurezza

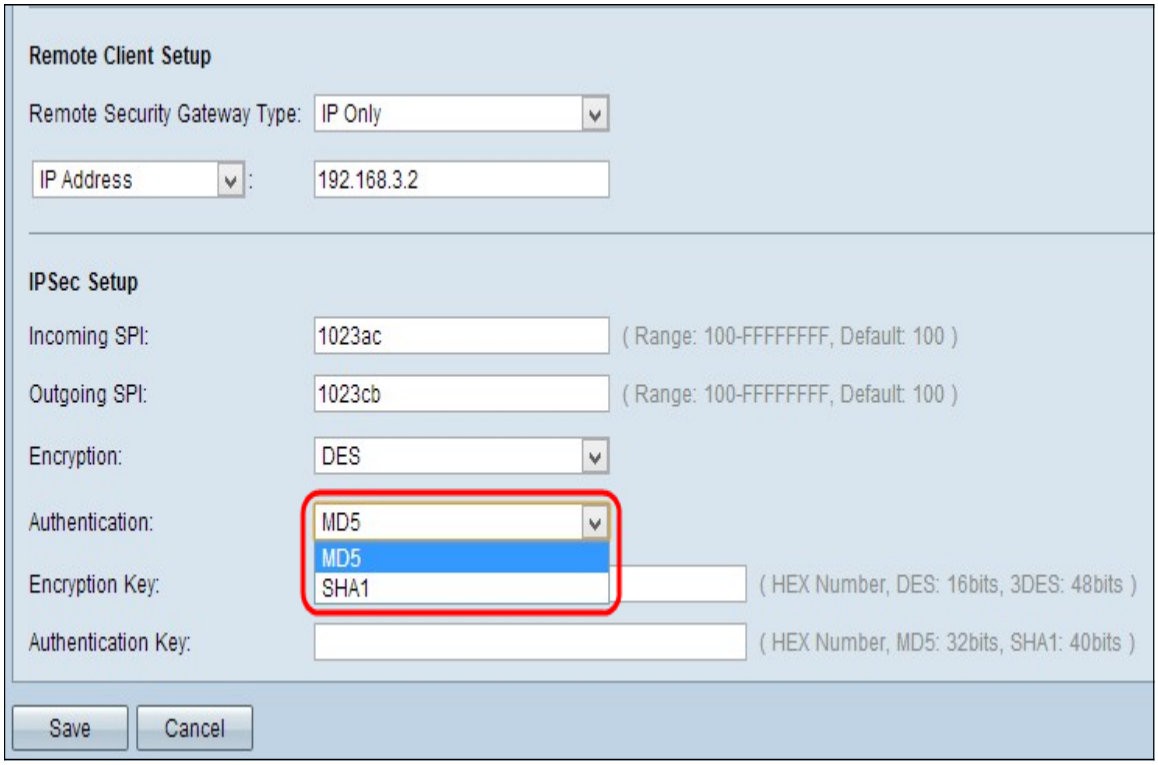
(SPI) in uscita nel campo *SPI in uscita*. L'indice SPI è contenuto nell'intestazione ESP (Encapsulating Security Payload Protocol) che determina l'associazione di sicurezza (SA) per il pacchetto in uscita. L'intervallo è compreso tra 100 e ffffffff, il valore predefinito è 100.

Nota: L'SPI in ingresso del dispositivo connesso e l'SPI in uscita dell'altra estremità del tunnel devono corrispondere per stabilire un tunnel.



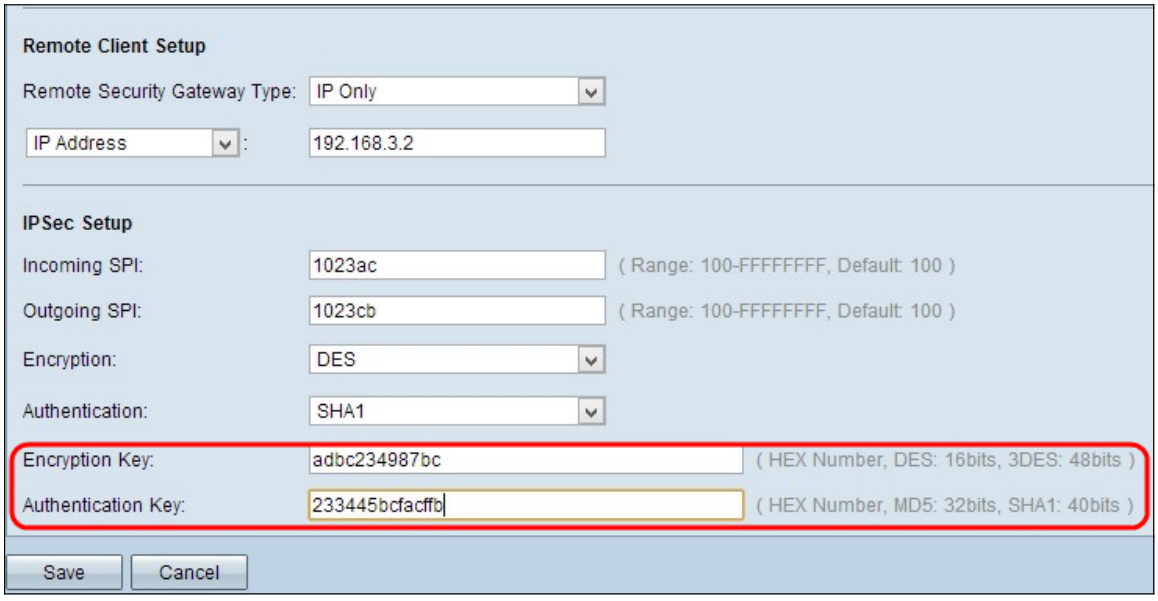
Passaggio 3. Scegliere il metodo di cifratura appropriato dall'elenco a discesa *Cifratura*. La crittografia consigliata è 3DES. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES - Data Encryption Standard (DES) è un metodo di crittografia a 56 bit, vecchio e compatibile con le versioni precedenti, che non è altrettanto sicuro.
- 3DES - Triple Data Encryption Standard (3DES) è un metodo di crittografia semplice a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.



Passaggio 4. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa *Autenticazione*. L'autenticazione consigliata è SHA1. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5.



Passaggio 5. Immettere la chiave per crittografare e decrittografare i dati nel campo *Chiave di crittografia*. Se al passaggio 3 è stato scelto DES come metodo di crittografia, immettere un valore esadecimale a 16 cifre. Se nel passaggio 3 è stato scelto 3DES come metodo di crittografia, immettere un valore esadecimale di 40 cifre.

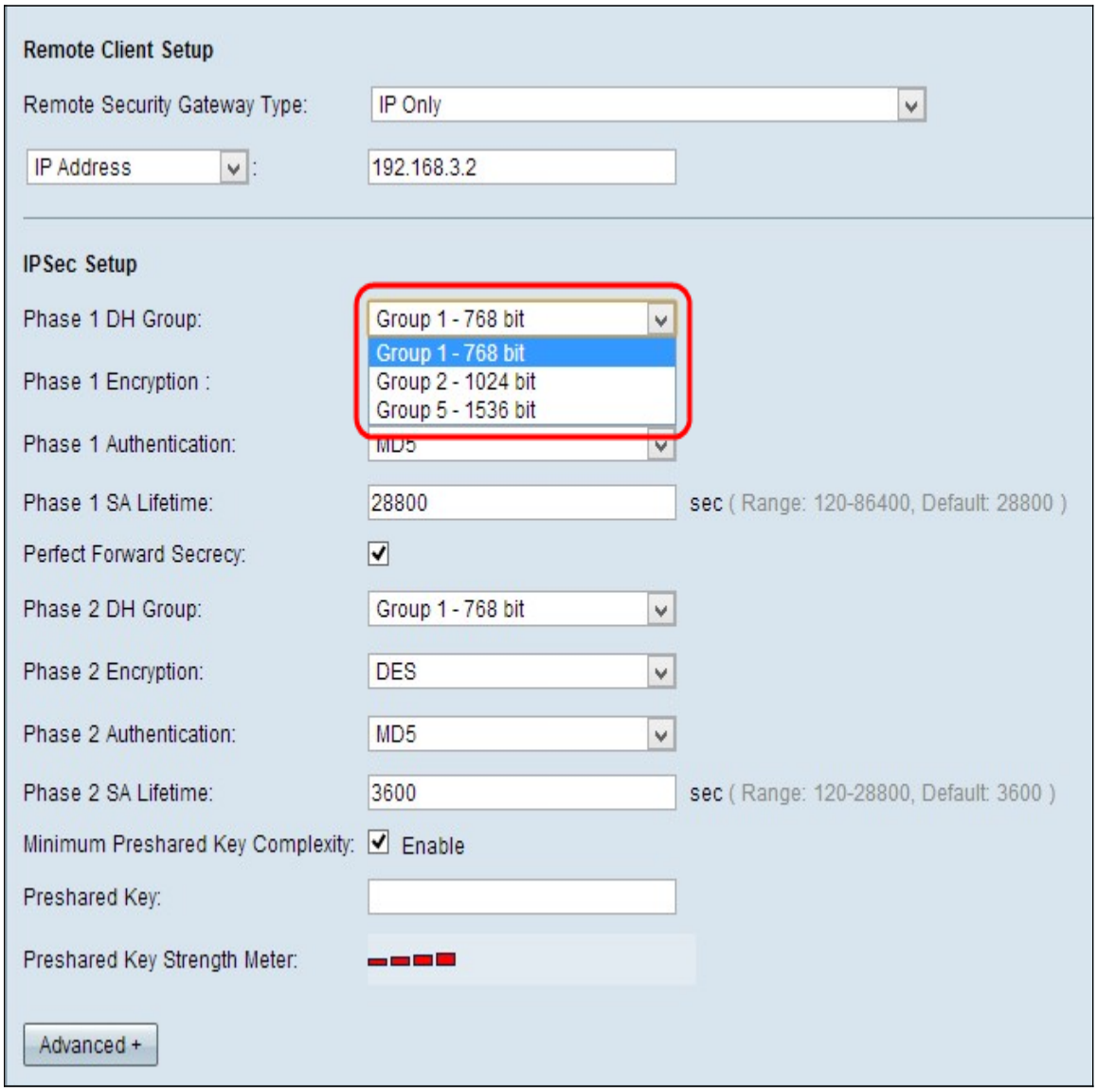
Passaggio 6. Immettere una chiave già condivisa per autenticare il traffico nel campo *Authentication Key* (Chiave di autenticazione). Se al passaggio 4 si sceglie MD5 come

metodo di autenticazione, immettere un valore esadecimale di 32 cifre. Se si sceglie Agente integrità sistema come metodo di autenticazione al passaggio 4, immettere un valore esadecimale di 40 cifre. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.

Passaggio 7. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Installazione di IPSec con IKE con chiave già condivisa o IKE con certificato

Nota: se si sceglie IKE con chiave già condivisa o IKE con certificato dall'elenco a discesa *Modalità di impostazione chiavi* nel passaggio 3 della sezione *Aggiungi nuovo tunnel,* eseguire la procedura seguente.

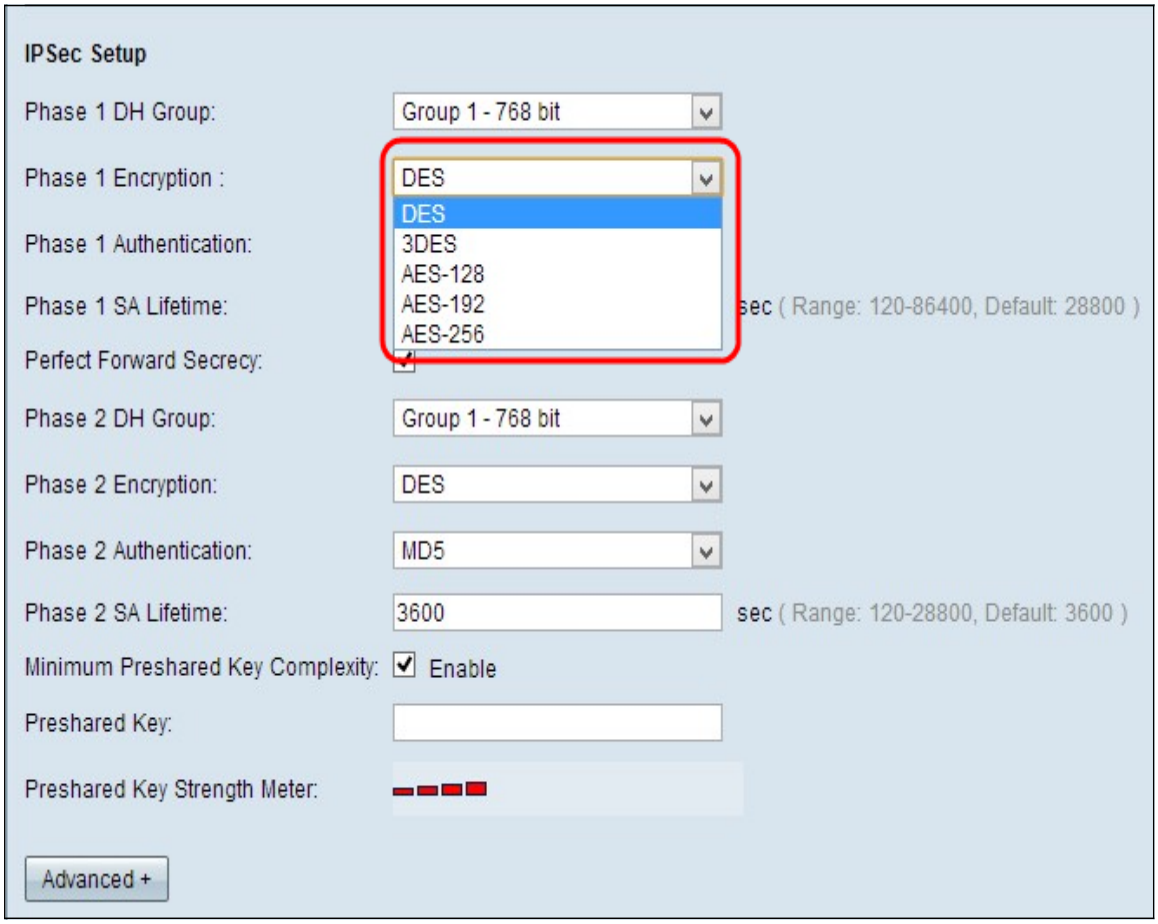


Passaggio 1. Scegliere il gruppo DH Fase 1 appropriato dall'elenco a discesa Gruppo *DH Fase 1*. La fase 1 viene utilizzata per stabilire un'associazione di sicurezza logica (SA, Logical Security Association) semplice tra le due estremità del tunnel per supportare una comunicazione autentica e sicura. Diffie-Hellman (DH) è un protocollo di scambio chiave crittografica utilizzato durante la connessione di Fase 1 per condividere la chiave segreta e autenticare la comunicazione.

- Gruppo 1 - 768 bit - Rappresenta la chiave con il livello di protezione più basso e il gruppo di

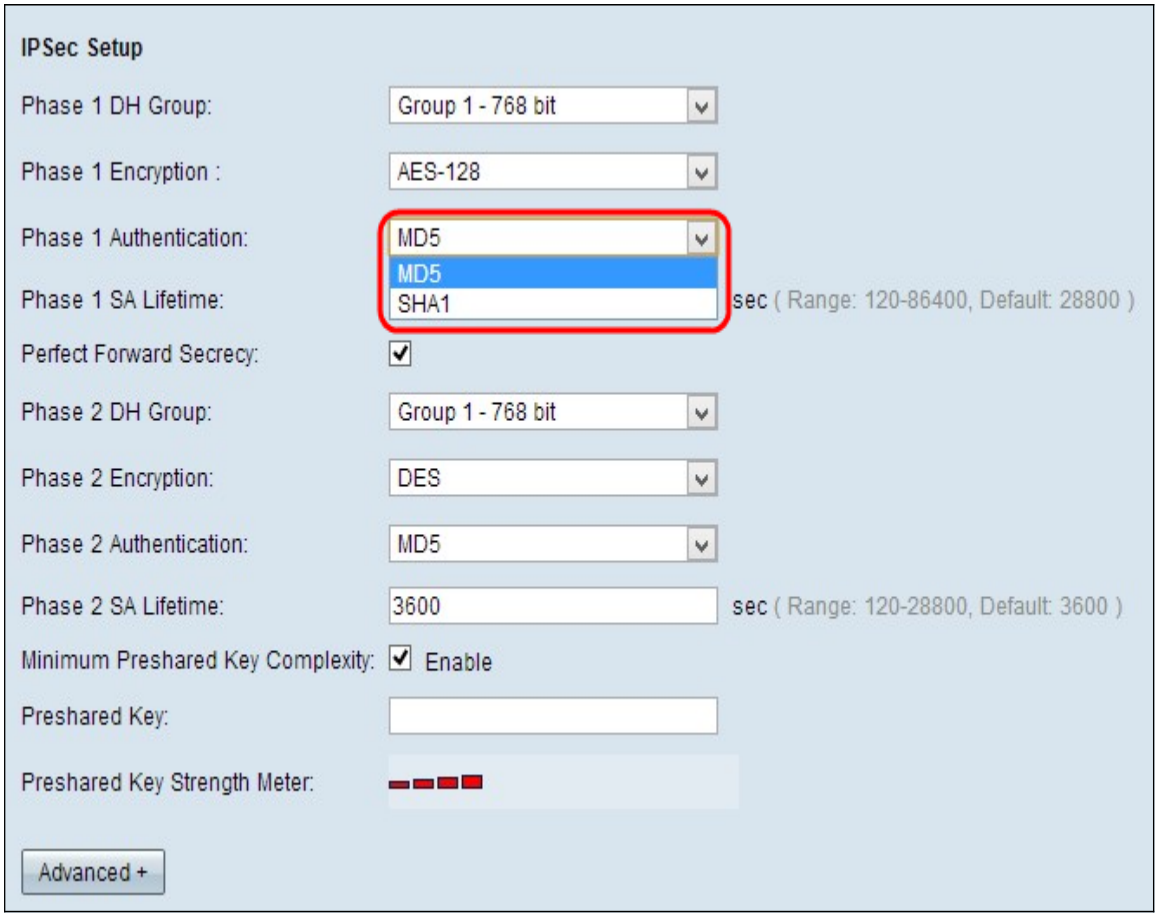
autenticazione con il livello di protezione più basso. Ma ha bisogno di meno tempo per calcolare le chiavi IKE. È preferibile se la velocità della rete è bassa.

- Gruppo 2 - 1024 bit - Rappresenta una chiave di livello superiore e un gruppo di autenticazione più sicuro. Ma ha bisogno di un po' di tempo per calcolare le chiavi IKE.
- Gruppo 5 - 1536 bit - Rappresenta la chiave con il livello di protezione più alto e il gruppo di autenticazione più sicuro. È necessario più tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è elevata.



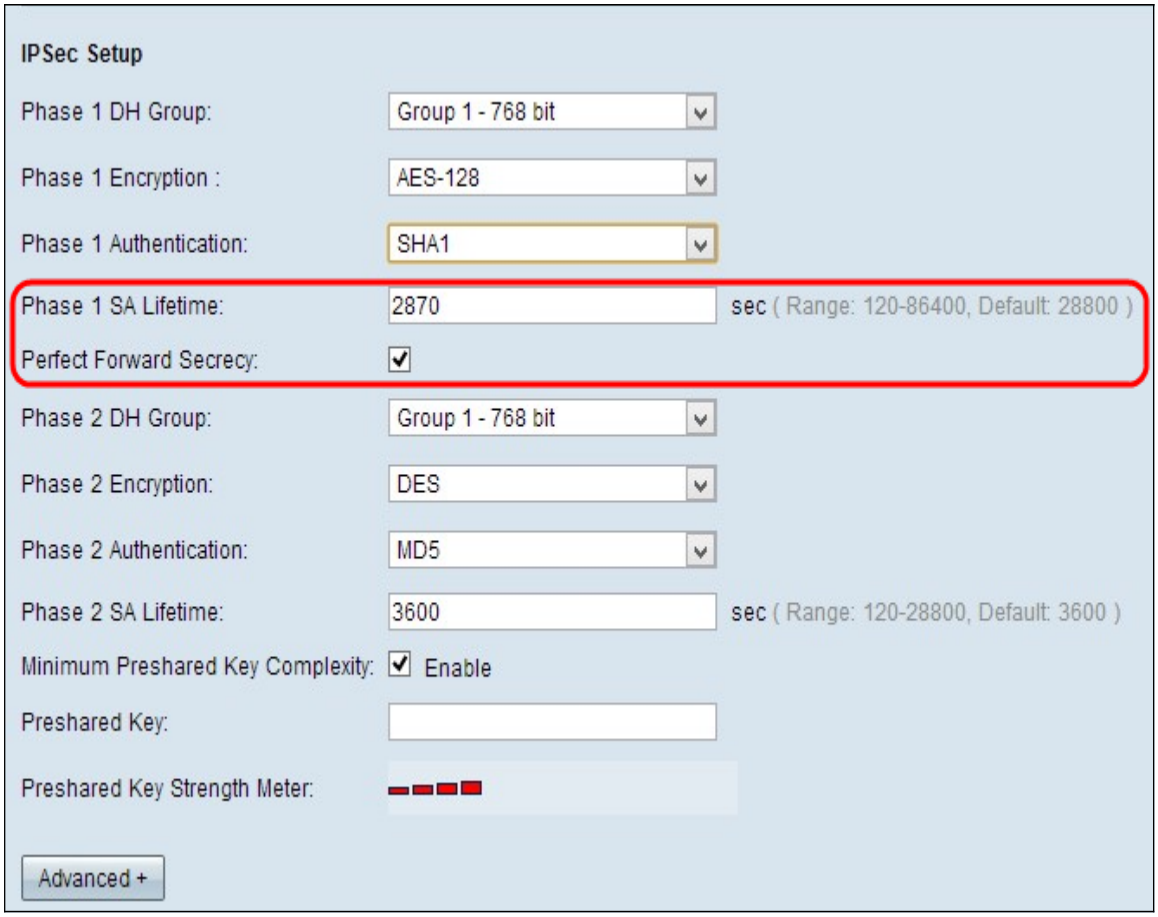
Passaggio 2. Scegliere la crittografia appropriata per la fase 1 per crittografare la chiave dall'elenco a discesa *Crittografia fase 1*. Si consiglia l'AES-256 perché è il metodo di crittografia più sicuro. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES - Data Encryption Standard (DES) è a 56 bit, il vecchio metodo di crittografia che non è molto sicuro.
- 3DES - Triple Data Encryption Standard (3DES) è un metodo di crittografia semplice a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.
- AES-128 - Advanced Encryption Standard (AES) è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso 10 cicli di ripetizione.
- AES-192 - Advanced Encryption Standard (AES) è un metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato attraverso 12 cicli di ripetizione.
- AES-256 - Advanced Encryption Standard (AES) è un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso 14 cicli di ripetizione.



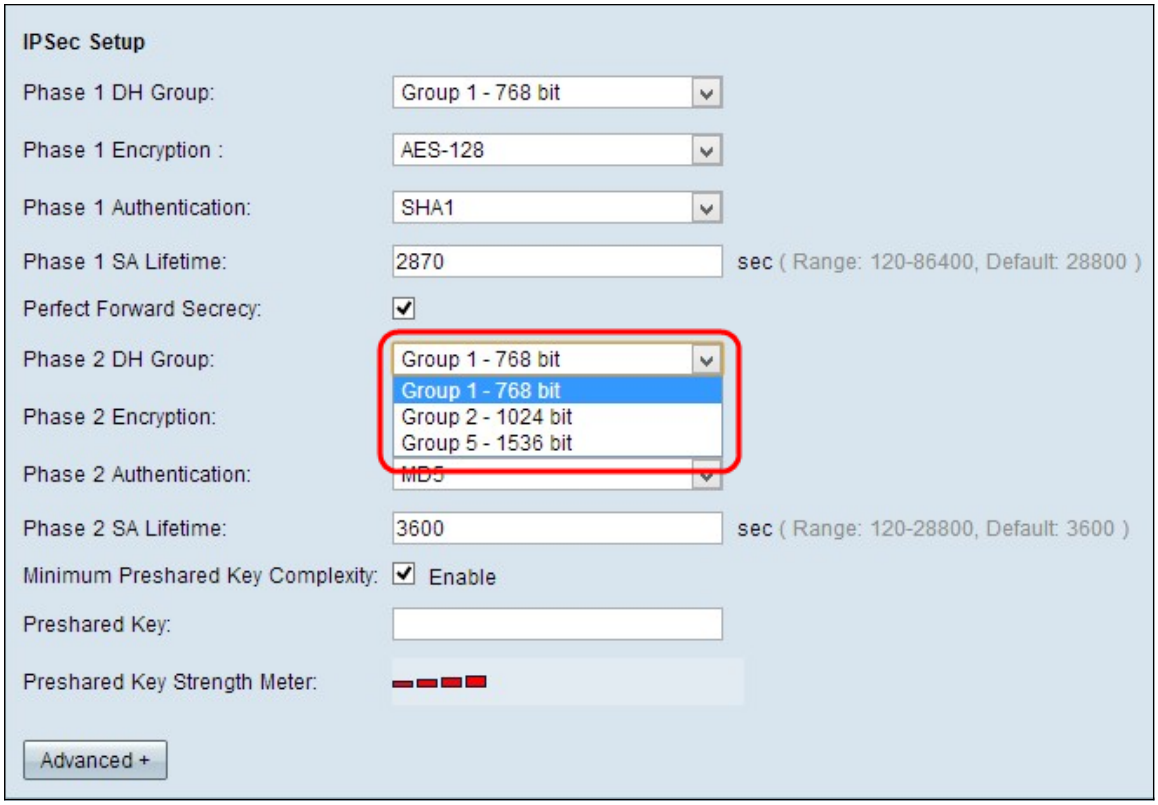
Passaggio 3. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa *Autenticazione fase 1*. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5.



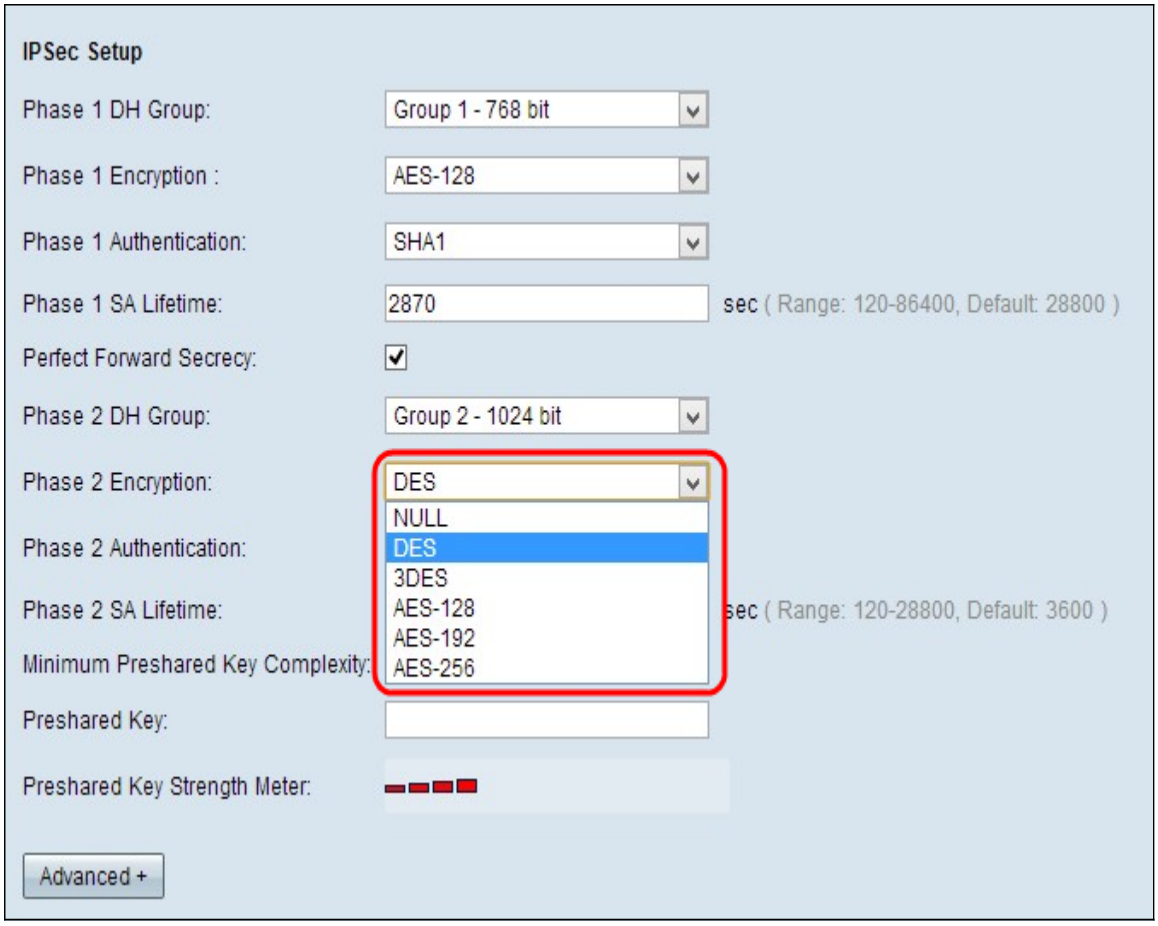
Passaggio 4. Immettere il periodo di tempo in secondi. Nella Fase 1, il tunnel VPN rimane attivo nel campo *Durata SA fase 1*. Il tempo predefinito è 2800 secondi.

Passaggio 5. Selezionare la casella di controllo **Perfect Forward Secrecy** per proteggere ulteriormente le chiavi. Questa opzione consente di generare una nuova chiave in caso di violazione di una chiave. I dati crittografati vengono compromessi solo tramite la chiave compromessa. In questo modo la comunicazione risulta più sicura e autenticata, poiché protegge altre chiavi anche se compromesse. Si tratta di un'azione consigliata in quanto offre maggiore protezione.



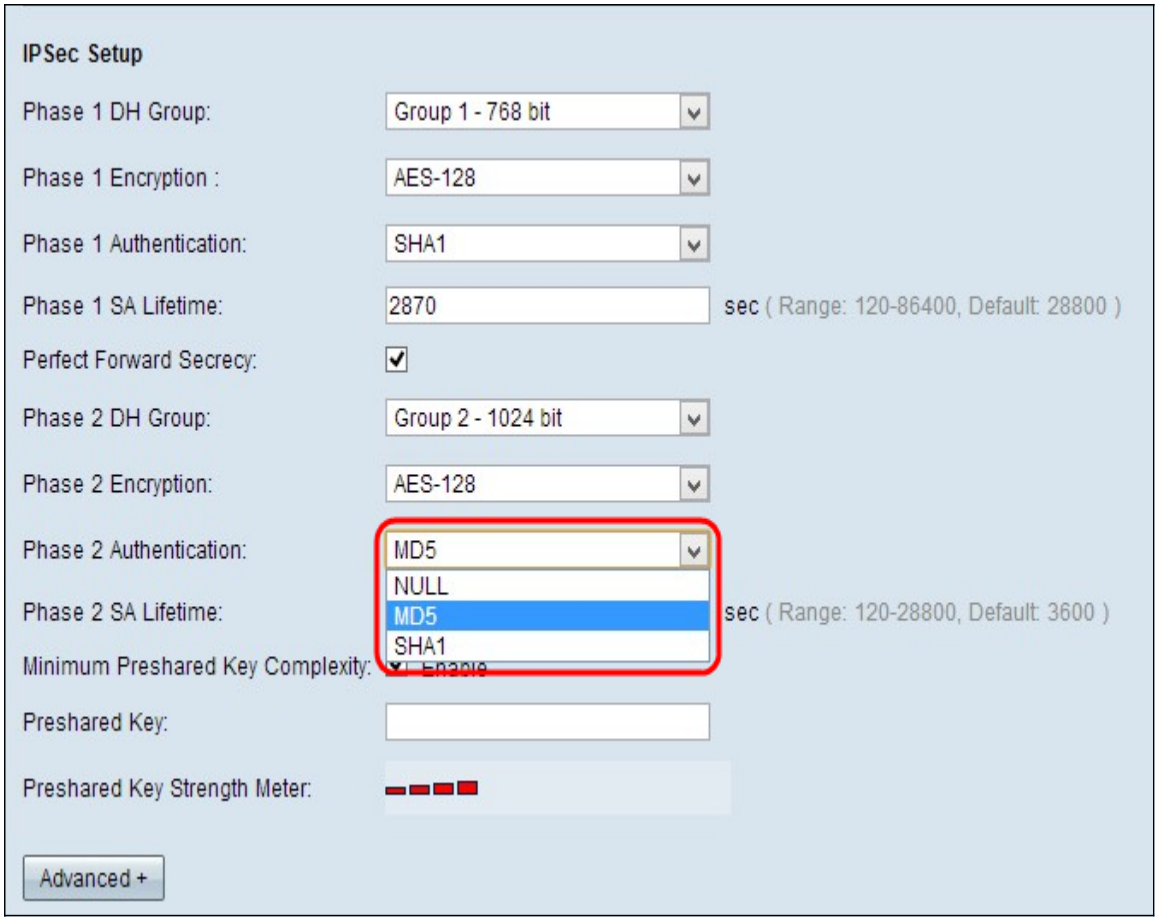
Passaggio 6. Scegliere il gruppo DH Fase 2 appropriato dall'elenco a discesa *Gruppo DH Fase 2*. La fase 1 viene utilizzata per stabilire un'associazione di sicurezza logica (SA, Logical Security Association) semplice tra le due estremità del tunnel per supportare la comunicazione di autenticazione protetta. Diffie-Hellman (DH) è un protocollo di scambio chiave crittografica utilizzato durante la connessione di Fase 1 per condividere la chiave segreta e autenticare la comunicazione.

- Gruppo 1 - 768 bit - Rappresenta la chiave con il livello di protezione più basso e il gruppo di autenticazione con il livello di protezione più basso. Ma ha bisogno di meno tempo per calcolare le chiavi IKE. È preferibile se la velocità della rete è bassa.
- Gruppo 2 - 1024 bit - Rappresenta una chiave di livello superiore e un gruppo di autenticazione più sicuro. Ma ha bisogno di un po' di tempo per calcolare le chiavi IKE.
- Gruppo 5 - 1536 bit - Rappresenta la chiave con il livello di protezione più alto e il gruppo di autenticazione più sicuro. È necessario più tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è elevata.



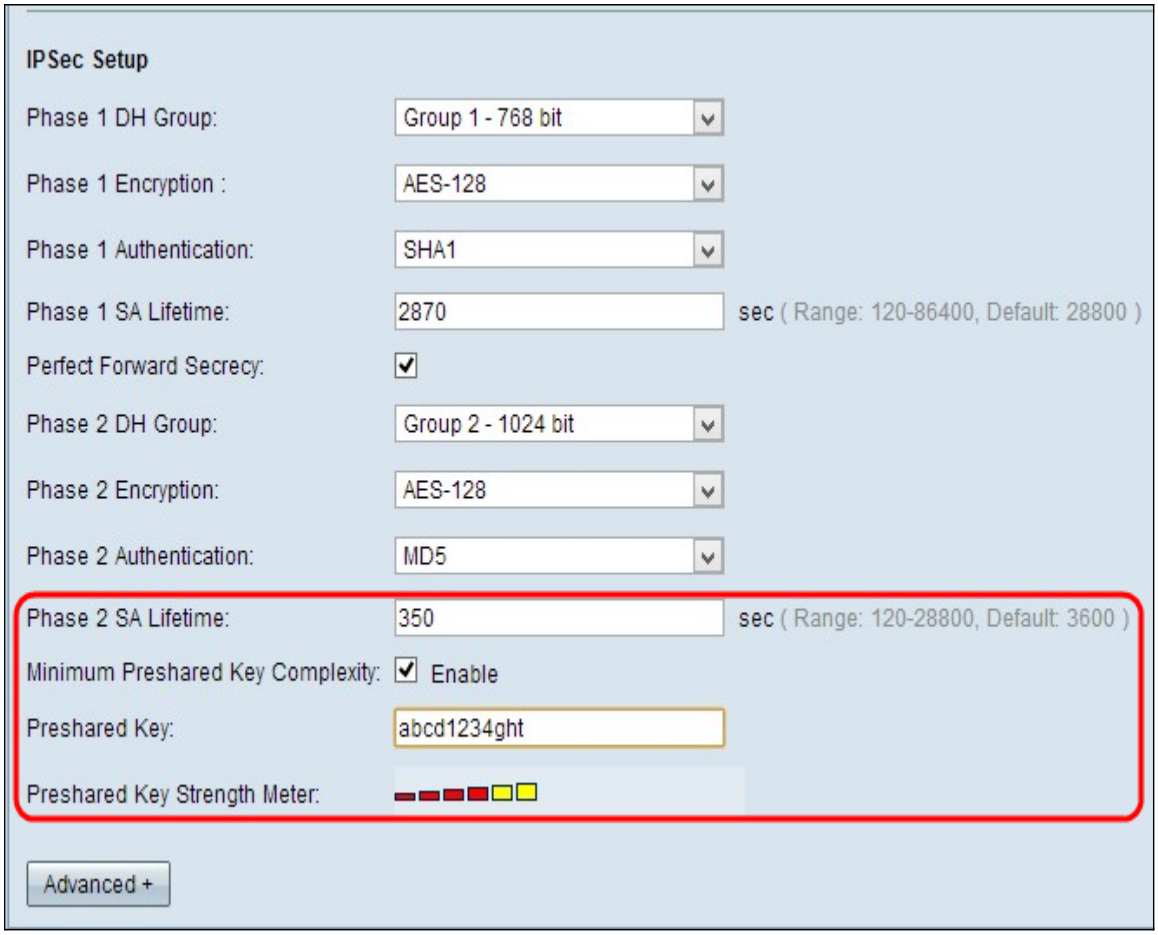
Passaggio 7. Scegliere la crittografia di fase 2 appropriata per crittografare la chiave dall'elenco a discesa *Crittografia fase 2*. Si consiglia l'AES-256 perché è il metodo di crittografia più sicuro. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES - Data Encryption Standard (DES) è a 56 bit, il vecchio metodo di crittografia che non è molto sicuro.
- 3DES - Triple Data Encryption Standard (3DES) è un metodo di crittografia semplice a 168 bit che consente di aumentare le dimensioni della chiave tramite la crittografia dei dati per tre volte, garantendo una maggiore protezione rispetto a DES.
- AES-128 - Advanced Encryption Standard (AES) è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.
- AES-192 - Advanced Encryption Standard (AES) è un metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 12 cicli.
- AES-256 - Advanced Encryption Standard (AES) è un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli.



Passaggio 8. Scegliere il metodo di autenticazione appropriato dall'elenco a discesa *Autenticazione fase 2*. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5.
- Null - Non viene utilizzato alcun metodo di autenticazione.



Passaggio 9. Immettere il periodo di tempo in secondi. Nella Fase 2, il tunnel VPN rimane attivo nel campo *Durata SA fase 2*. Il tempo predefinito è 3600 secondi.

Passaggio 10. Selezionare la casella di controllo **Complessità minima chiave già condivisa** se si desidera abilitare il misuratore di affidabilità per la chiave già condivisa.

Passaggio 11. Immettere una chiave condivisa in precedenza tra i peer IKE nel campo *Chiave già condivisa*. È possibile utilizzare fino a 30 caratteri alfanumerici come chiave già condivisa. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.

Nota: Si consiglia di modificare frequentemente la chiave già condivisa tra i peer IKE in modo che la VPN resti sicura.

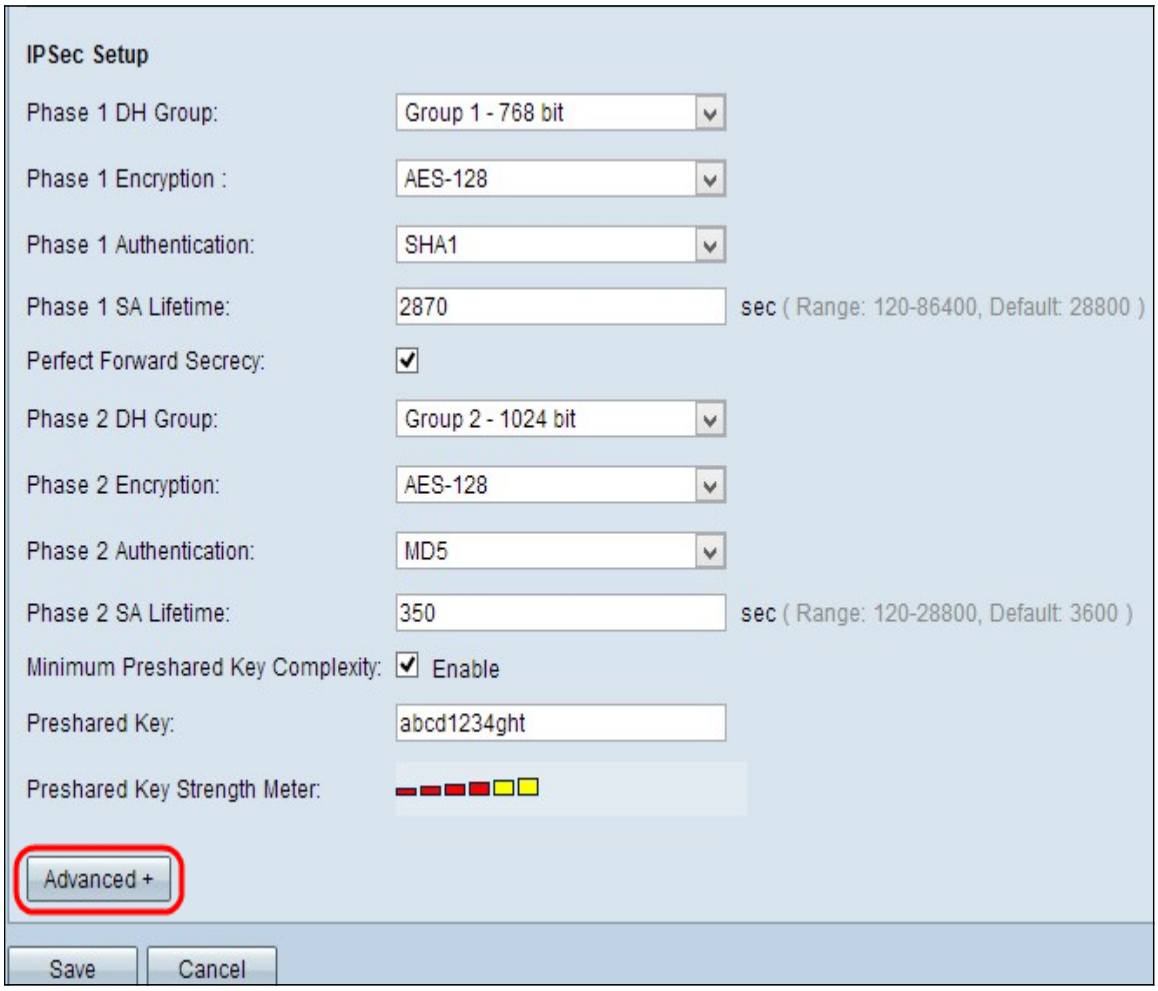
- Misuratore dell'intensità della chiave già condivisa: mostra l'intensità della chiave già condivisa tramite barre colorate. Il rosso indica una forza debole, il giallo indica una forza accettabile e il verde indica una forza forte. Se si seleziona la casella di controllo **Complessità minima chiave già condivisa** nel passaggio 10 della sezione Configurazione di IPSec, verrà visualizzato solo il Misuratore di forza della chiave già condivisa.

  Nota: Se si sceglie IKE con chiave già condivisa dall'elenco a discesa *Modalità di impostazione chiavi* nel passaggio 3 per la sezione *Aggiunta di un nuovo tunnel*, solo l'utente può configurare i passaggi 10 e 11 e visualizzare il misuratore di livello della chiave già condivisa.

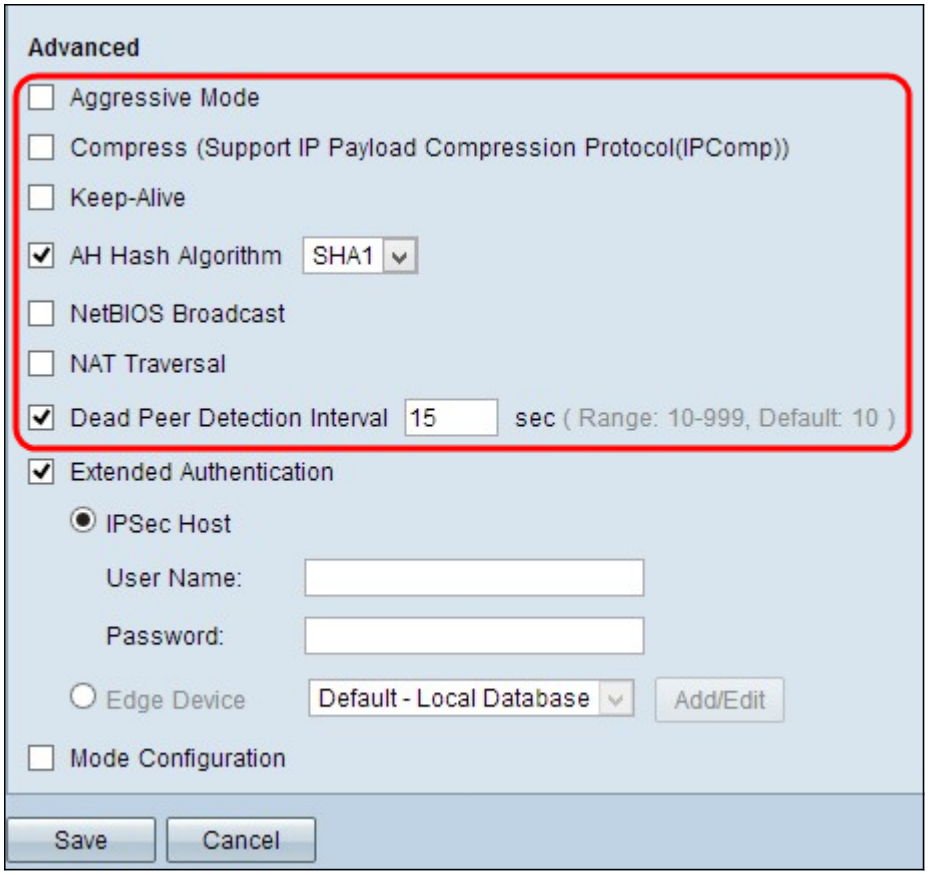
  Passaggio 12. Se si desidera salvare le impostazioni correnti, scorrere verso il basso e fare clic su **Salva** per salvarle.

Installazione avanzata con IKE con chiave già condivisa o IKE con certificato

Le impostazioni avanzate sono possibili solo per IKE con chiave già condivisa e IKE con chiave di certificazione. Per l'impostazione del tasto Manuale non sono disponibili impostazioni avanzate.



Passaggio 1. Fare clic su **Avanzate** per visualizzare le impostazioni avanzate di IKE con chiave già condivisa.



Passaggio 2. Selezionare la casella di controllo **Modalità aggressiva** se la velocità della rete è bassa. Scambia gli ID dei punti finali del tunnel in testo non crittografato durante la connessione SA, operazione che richiede meno tempo per lo scambio ma meno protezione.

Passaggio 3. Selezionare la casella di controllo **Comprimi (Support IP Payload Compression Protocol (IPComp))** se si desidera comprimere le dimensioni del datagramma IP. IPComp è un protocollo di compressione IP che viene utilizzato per comprimere le dimensioni del datagramma IP se la velocità della rete è bassa e l'utente desidera trasmettere rapidamente i dati senza alcuna perdita attraverso la rete lenta.

Passaggio 4.Selezionare la casella di controllo **Keep-Alive** se si desidera che la connessione del tunnel VPN rimanga sempre attiva. Aiuta a ristabilire le connessioni immediatamente se una connessione diventa inattiva.

Passaggio 5. Selezionare la casella di controllo **AH Hash Algorithm** per autenticare l'intestazione AH (Authenticate Header). AH fornisce l'autenticazione all'origine dei dati, l'integrità dei dati tramite checksum e la protezione viene estesa nell'intestazione IP. Il tunnel deve avere lo stesso algoritmo per entrambi i lati.

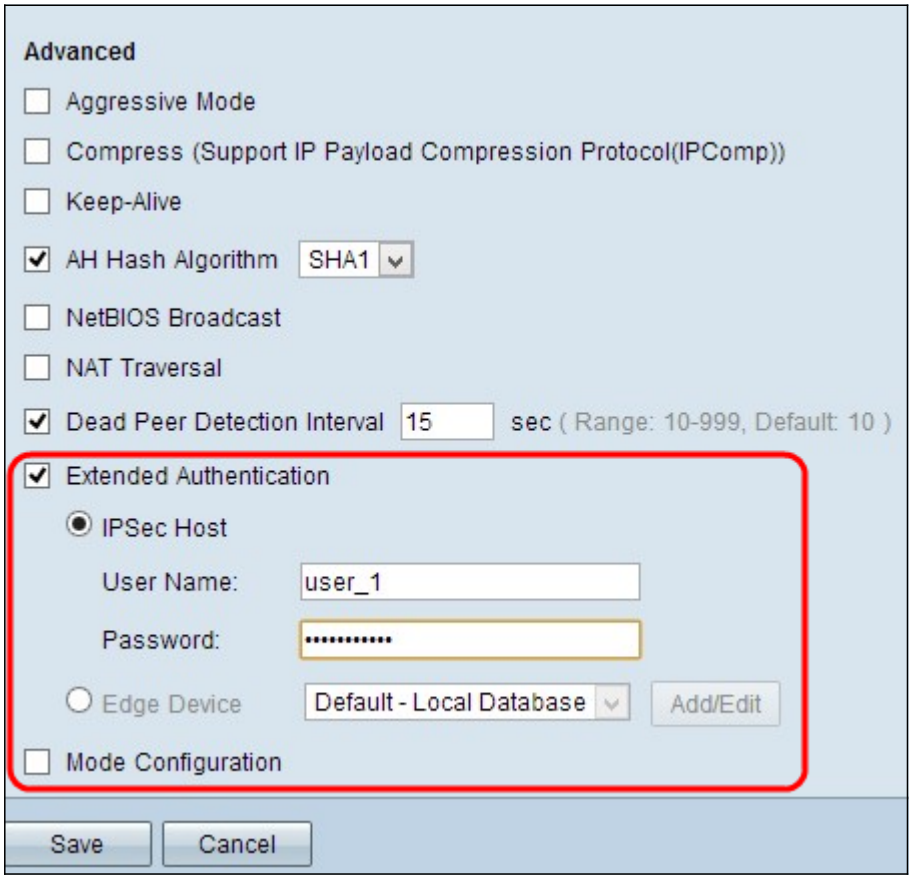
- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 128 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5.

Passaggio 6. Selezionare **NetBIOS Broadcast** se si desidera consentire il traffico non instradabile attraverso il tunnel VPN. L'opzione di default è deselezionata. NetBIOS viene utilizzato per rilevare risorse di rete come stampanti, computer e così via nella rete tramite alcune applicazioni software e funzionalità di Windows come Risorse di rete.

Passaggio 7. Selezionare la casella di controllo **NAT Traversal** se si desidera accedere a

Internet dalla LAN privata tramite l'indirizzo IP pubblico. L'attraversamento NAT viene utilizzato per visualizzare gli indirizzi IP privati dei sistemi interni come indirizzi IP pubblici per proteggere gli indirizzi IP privati da attacchi dannosi o da rilevamenti.

Passaggio 8. Selezionare **Dead Peer Detection Interval** per verificare periodicamente la vivacità del tunnel VPN tramite hello o ACK. Se si seleziona questa casella di controllo, immettere la durata o l'intervallo dei messaggi di benvenuto desiderati.



Passaggio 9. Selezionare **Autenticazione estesa** per fornire maggiore sicurezza e autenticazione alla connessione VPN. Fare clic sul pulsante di opzione appropriato per estendere l'autenticazione della connessione VPN.

- Host IPSec - Autenticazione estesa tramite host IPSec. Se si sceglie questa opzione, immettere il nome utente dell'host IPSec nel campo Nome utente e una password nel campo Password.
- Periferica perimetrale - Autenticazione estesa tramite periferica perimetrale. Se si sceglie questa opzione, scegliere dall'elenco a discesa il database contenente il dispositivo perimetrale. Per aggiungere o modificare il database, fare clic su **Aggiungi/Modifica**.

Nota: Per ulteriori informazioni su come aggiungere o modificare il database locale, vedere *Configurazione della gestione di utenti e domini sul router RV320*.

Passaggio 10. Selezionare **Configurazione modalità** per fornire l'indirizzo IP per il richiedente del tunnel in ingresso.

Nota: I passaggi da 9 a 11 sono disponibili per la modalità di impostazione chiavi già condivise IKE per la VPN tunnel.

Passaggio 11. Fare clic su **Save** per salvare le impostazioni.

Conclusioni

A questo punto, è possibile configurare un singolo client per gateway VPN sui router VPN serie RV32x

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

Fare clic qui per visualizzare altre Tech Talks di Cisco