Configurazione di Group Client per Gateway VPN (Virtual Private Network) su RV320 e RV325 VPN Router

Obiettivo

Una rete privata virtuale (VPN) è una rete privata utilizzata per connettere virtualmente i dispositivi dell'utente remoto tramite la rete pubblica per garantire la sicurezza. Uno dei tipi di VPN è una VPN da client a gateway. Grazie al collegamento da client a gateway, è possibile collegare in remoto diverse filiali della società situate in aree geografiche diverse per trasmettere e ricevere i dati tra le aree in modo più sicuro. Group VPN offre una semplice configurazione della VPN in quanto elimina la configurazione della VPN per ogni utente. La serie RV32x VPN Router può supportare un massimo di due gruppi VPN.

L'obiettivo di questo documento è spiegare come configurare un client di gruppo per gateway VPN sui router VPN serie RV32x.

Dispositivi interessati

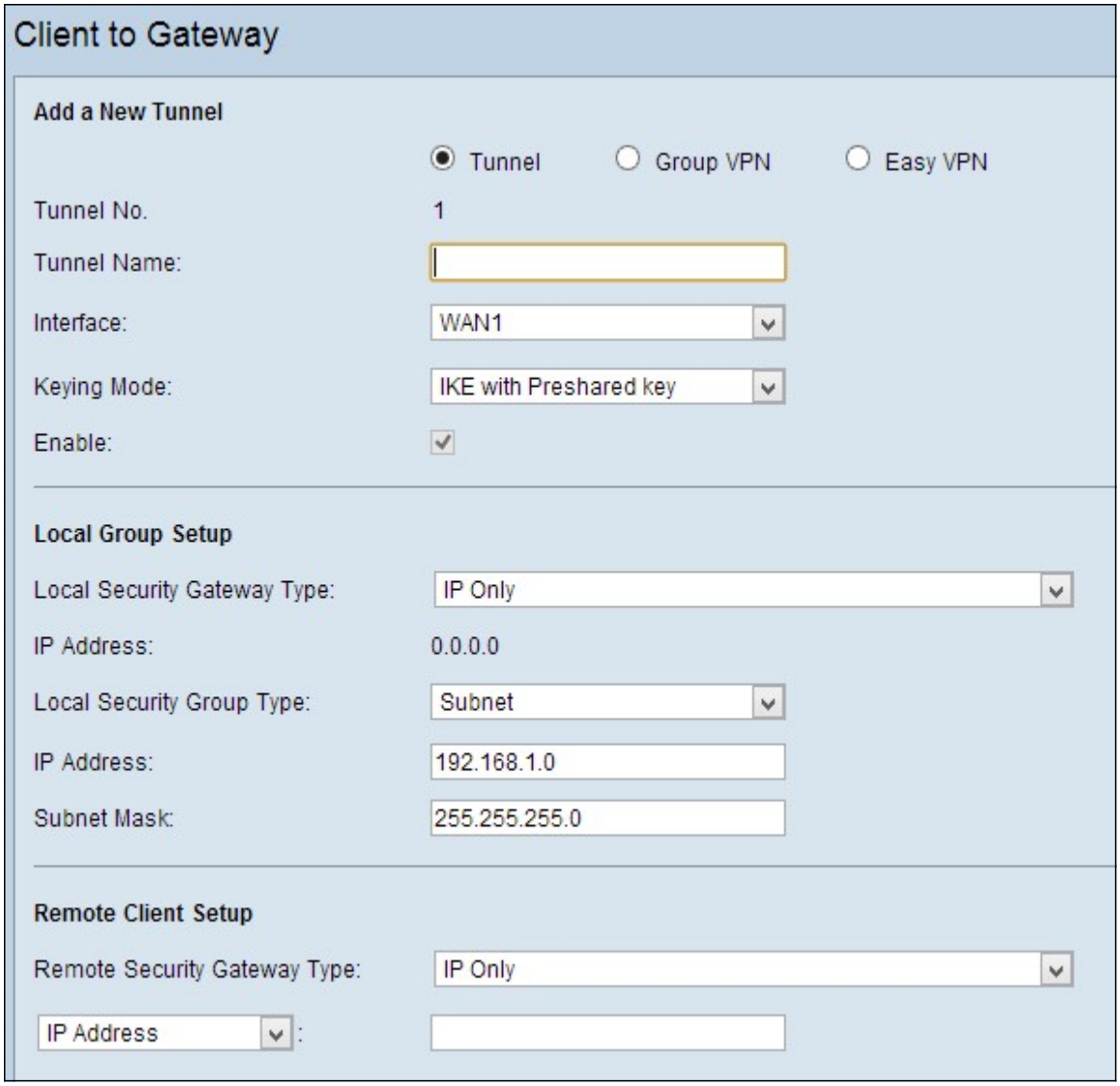
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

Versione del software

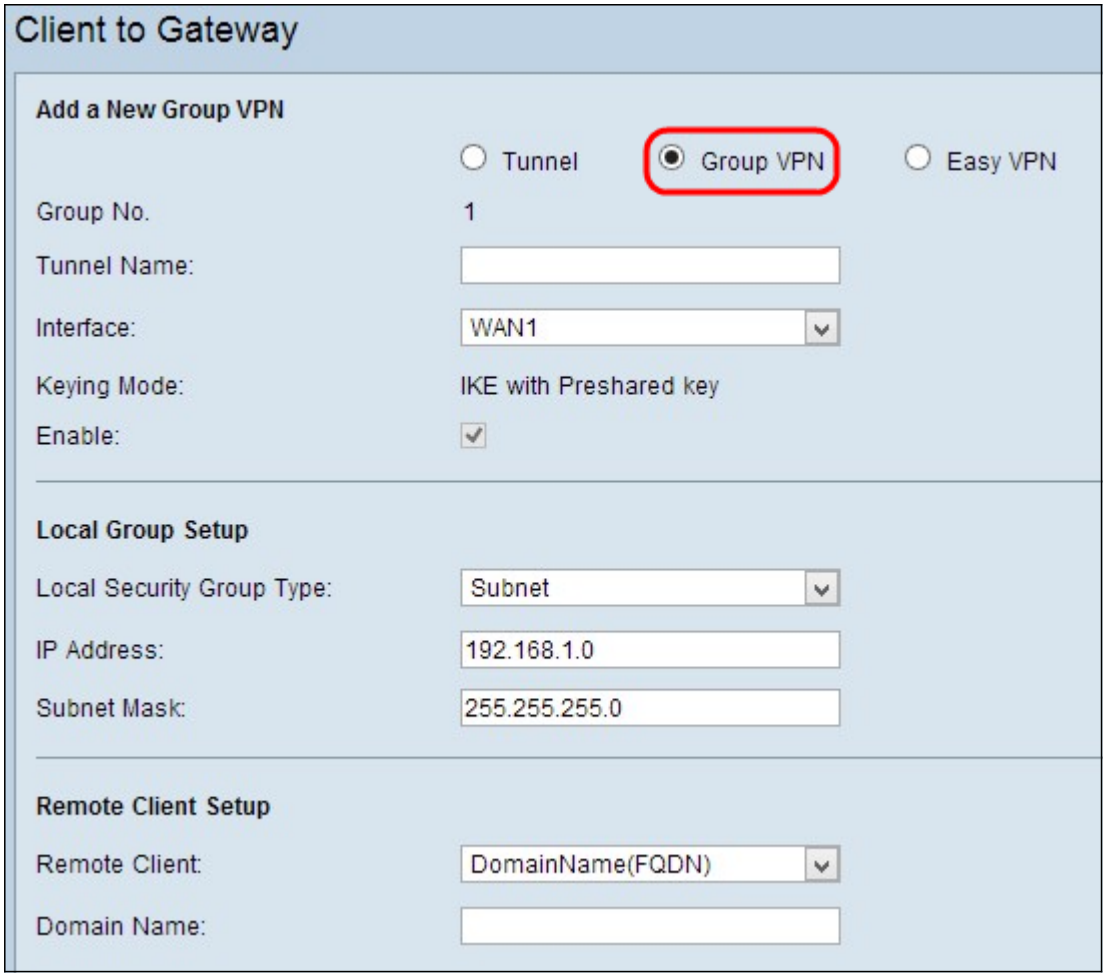
·v1.1.0.09

Configurare il client del gruppo per la VPN del gateway

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

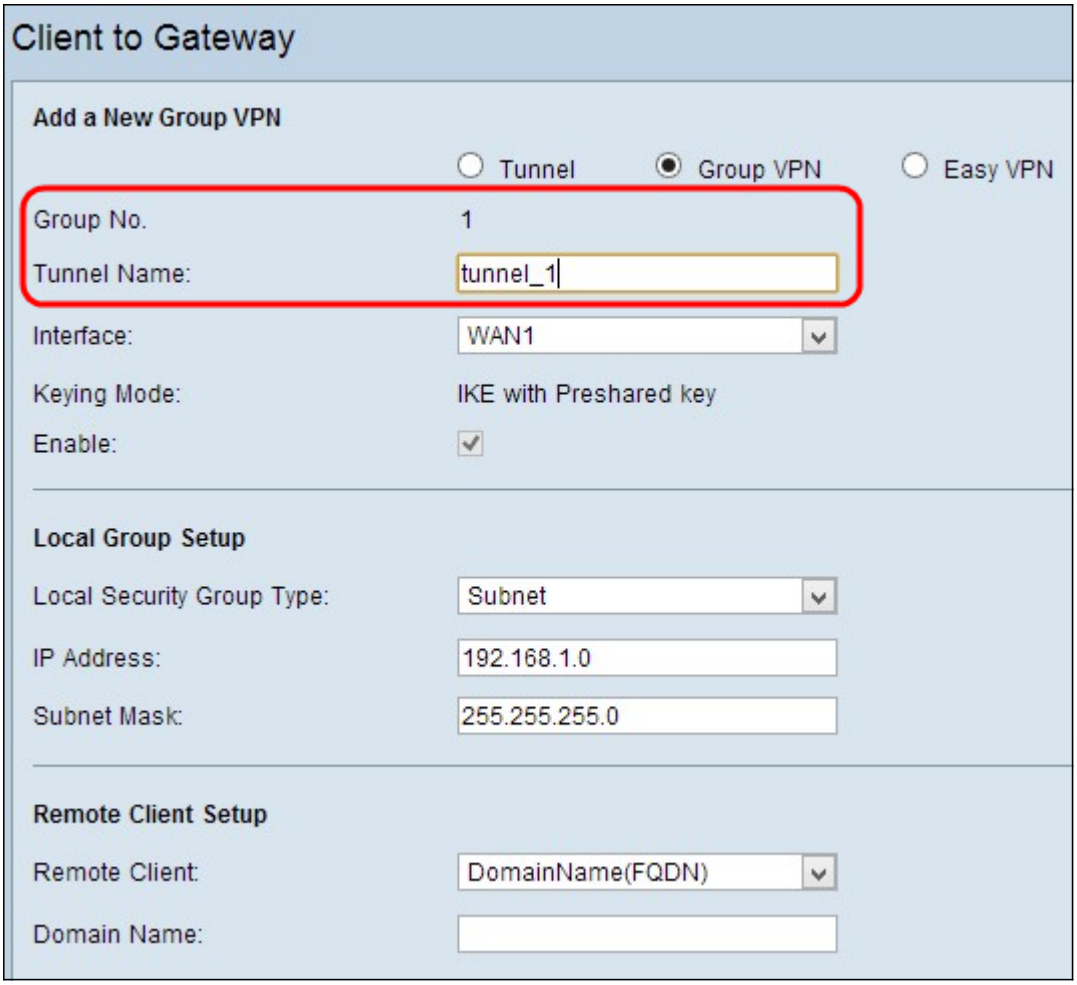


Passaggio 2. Fare clic sul pulsante di opzione **Group VPN** per aggiungere una VPN da client a gateway di gruppo.



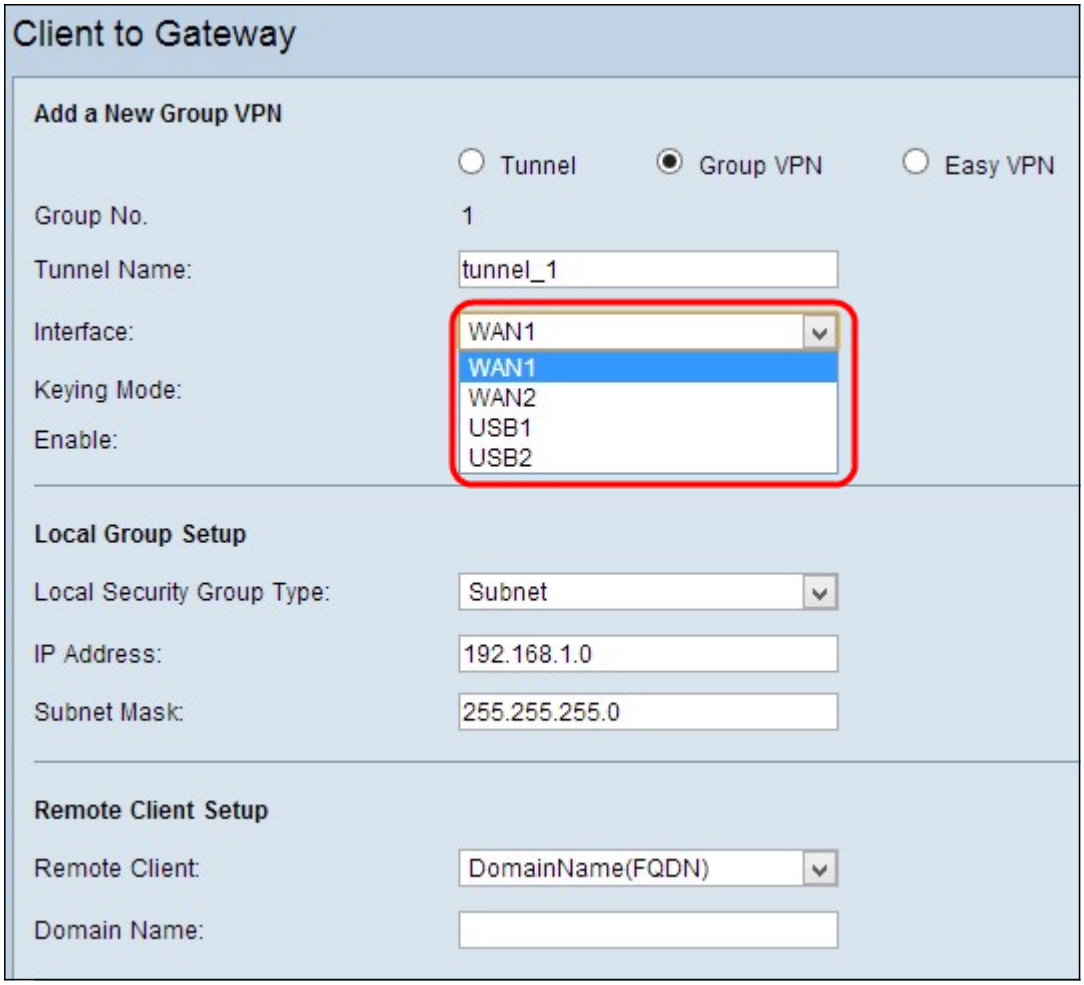
Aggiungi nuovo tunnel

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

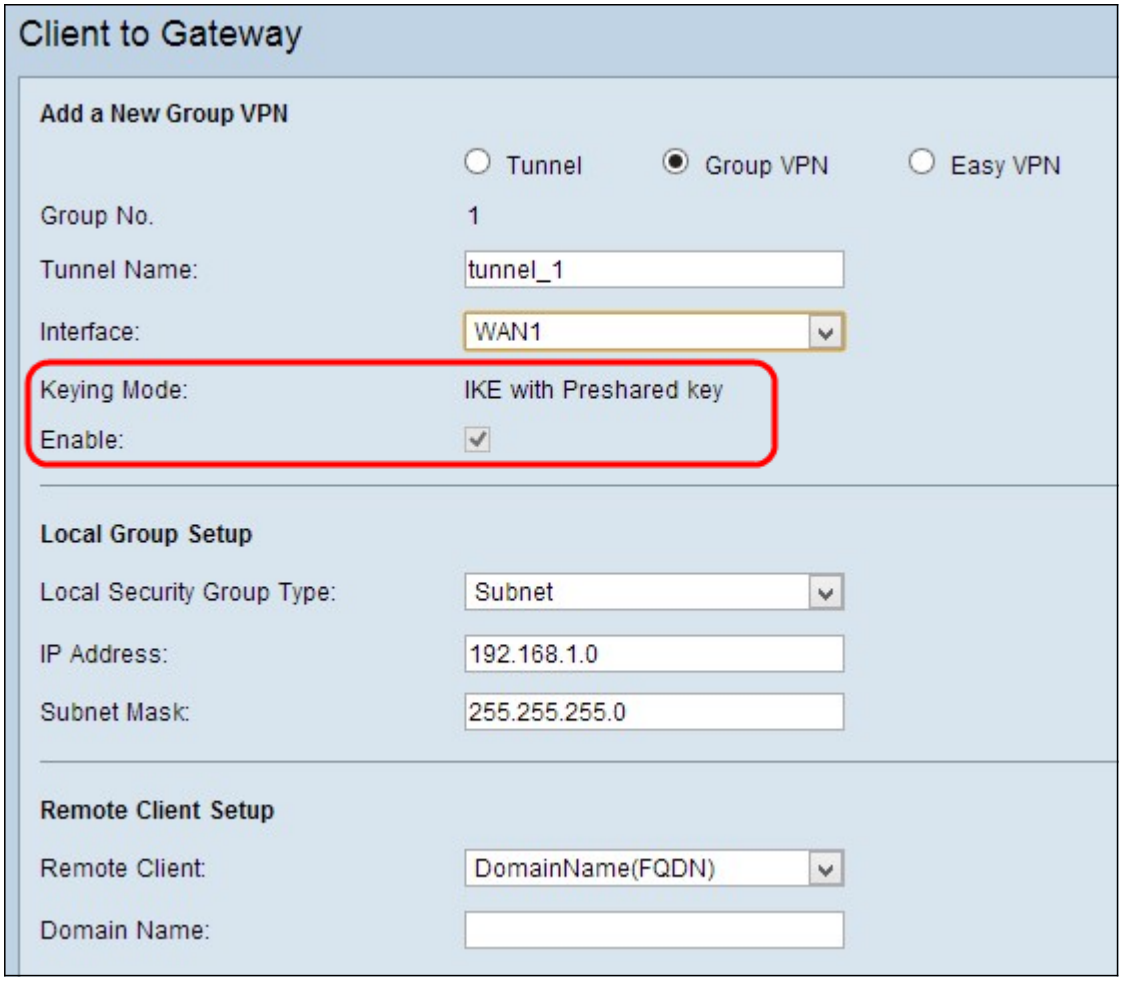


Nota: N. gruppo: rappresenta il numero del gruppo. Si tratta di un campo generato automaticamente.

Passaggio 2. Selezionare l'interfaccia appropriata tramite la quale il gruppo VPN si connette al gateway dall'elenco a discesa *Interface*.



Passaggio 3. Selezionare la casella di controllo **Abilita** per abilitare la VPN da gateway a gateway. Per impostazione predefinita è attivata.

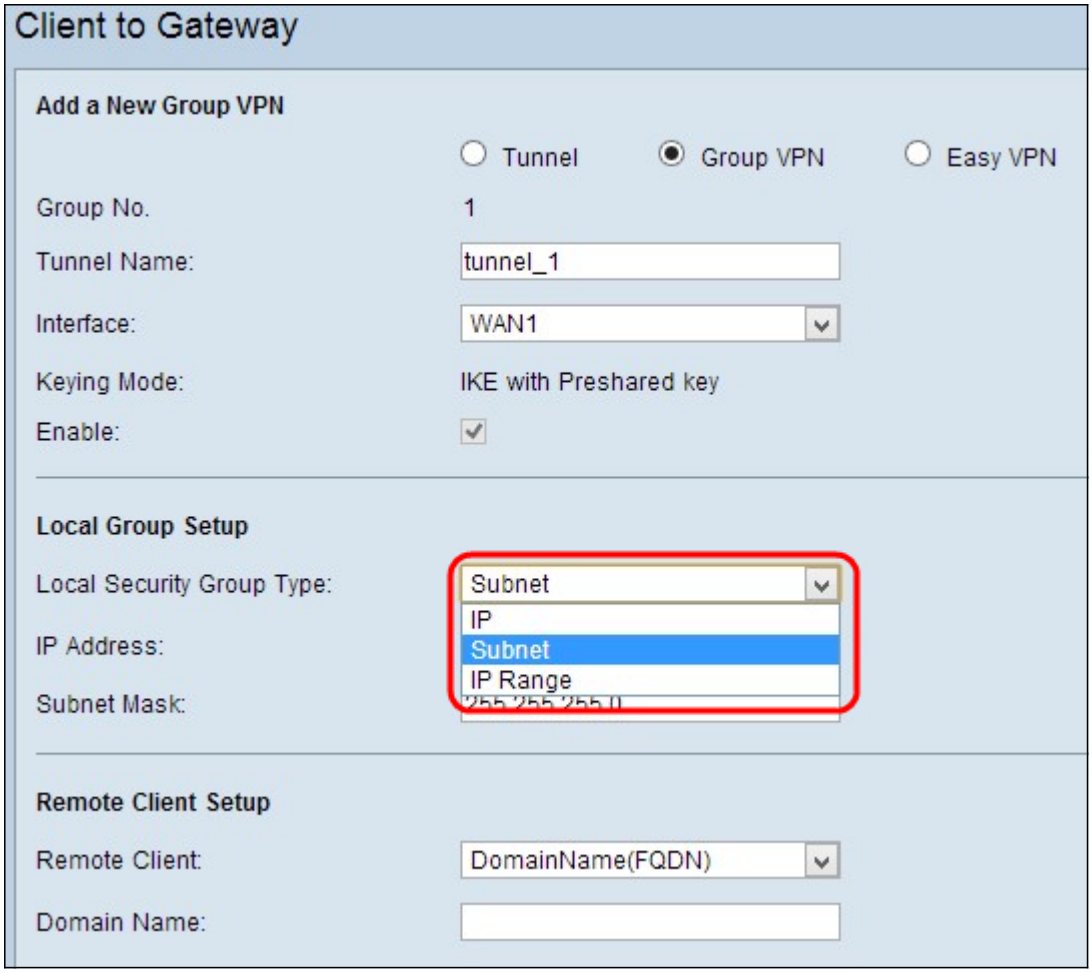


Nota: Modalità impostazione chiavi: visualizza la modalità di autenticazione utilizzata. IKE con chiave già condivisa è l'unica opzione disponibile, ovvero il protocollo IKE (Internet Key Exchange) viene utilizzato per generare e scambiare automaticamente una chiave già condivisa per stabilire la comunicazione autenticata per il tunnel.

Passaggio 4. Per salvare le impostazioni correnti e lasciare le altre predefinite, scorrere verso il basso e fare clic su **Salva** per salvare le impostazioni.

Installazione gruppo locale

Passaggio 1. 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.



Le opzioni disponibili sono definite come segue:

·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.

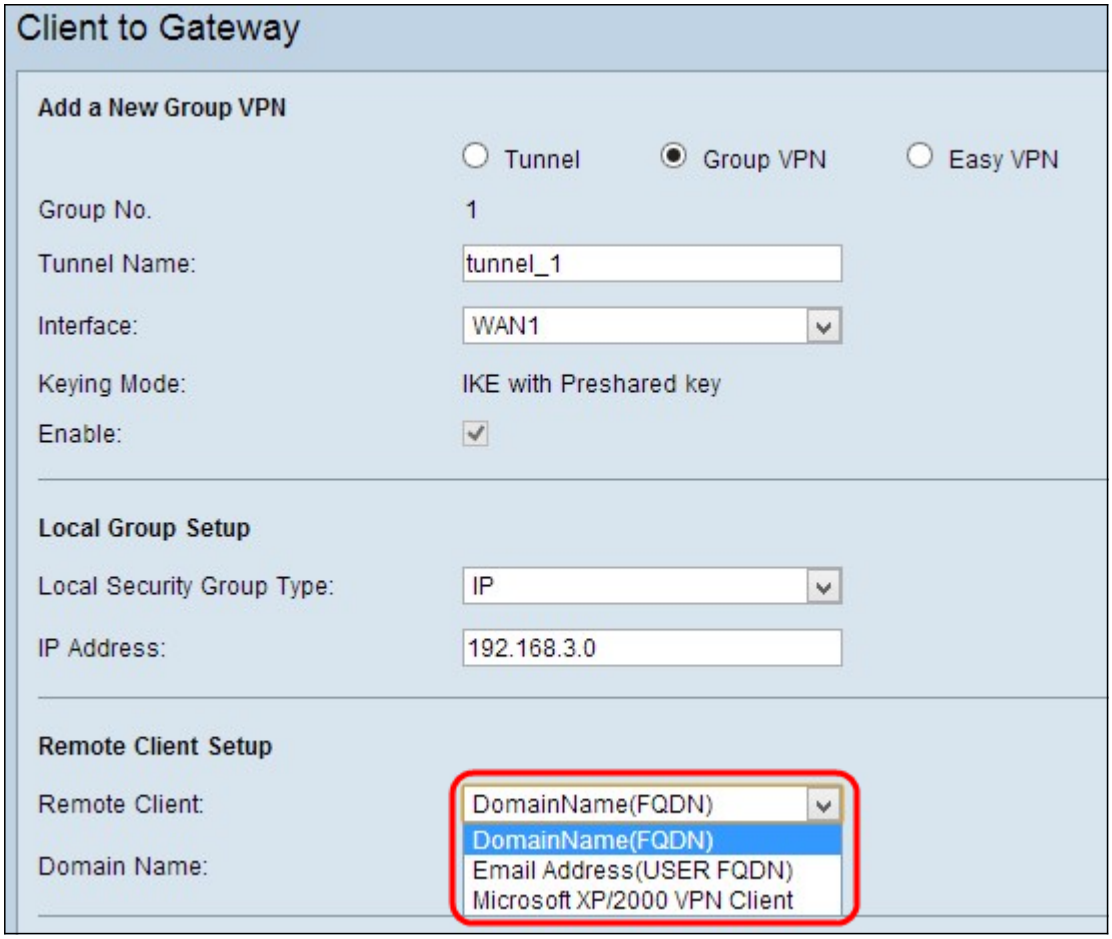
·Subnet: tutti i dispositivi LAN su una subnet specifica possono accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP e la subnet mask dei dispositivi LAN rispettivamente nei campi *Indirizzo IP* e *Subnet mask*. La maschera predefinita è 255.255.255.0.

·Intervallo IP: una serie di dispositivi LAN può accedere al tunnel. Se si sceglie questa opzione, immettere il primo e l'ultimo indirizzo IP dell'intervallo rispettivamente nei campi *IP iniziale* e *IP finale*. L'intervallo predefinito è compreso tra 192.168.1.0 e 192.168.1.254.

Passaggio 2. Per salvare le impostazioni correnti e lasciare le altre predefinite, scorrere verso il basso e fare clic su **Salva** per salvare le impostazioni.

Installazione client remota

Passaggio 1. Selezionare l'utente o il gruppo di utenti LAN remoti appropriato che può accedere al tunnel VPN dall'elenco a discesa *Tipo gruppo di sicurezza remoto*.



Le opzioni disponibili sono definite come segue:

·Autenticazione con nome di dominio (FQDN): è possibile accedere al tunnel tramite un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo *Nome dominio*.

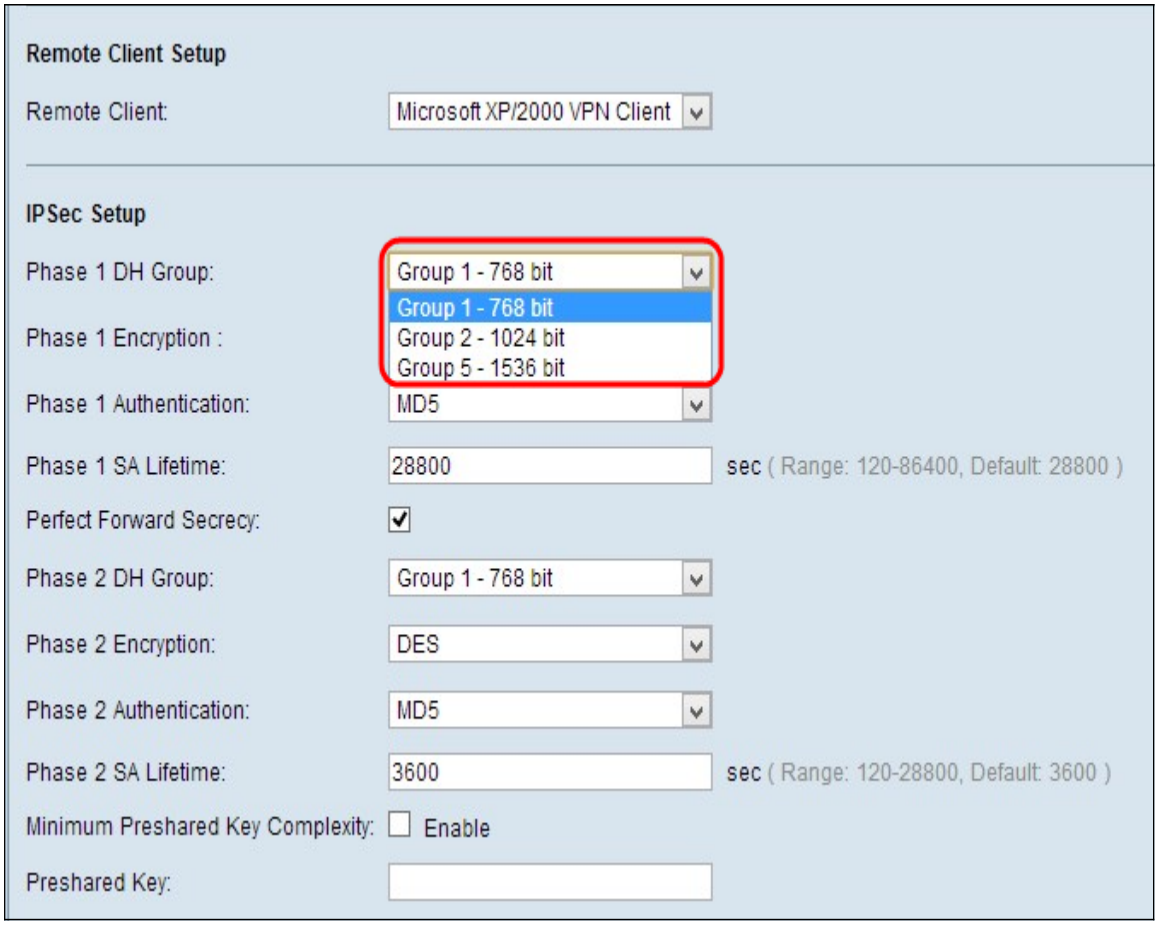
·Autenticazione indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo e-mail. Se si sceglie questa opzione, immettere l'indirizzo e-mail nel campo *Indirizzo e-mail*.

·Client VPN per Microsoft XP/2000: l'accesso al tunnel è possibile tramite un software client integrato in Microsoft XP o 2000 VPN Client.

Passaggio 2. Per salvare le impostazioni correnti e lasciare le altre predefinite, scorrere verso il basso e fare clic su **Salva** per salvare le impostazioni.

Installazione di IPSec

Passaggio 1. Scegliere il gruppo Diffie-Hellman (DH) 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 la comunicazione di autenticazione protetta. Diffie-Hellman è un protocollo di scambio chiave crittografica utilizzato nella connessione della fase 1 per condividere una chiave segreta al fine di autenticare la comunicazione.



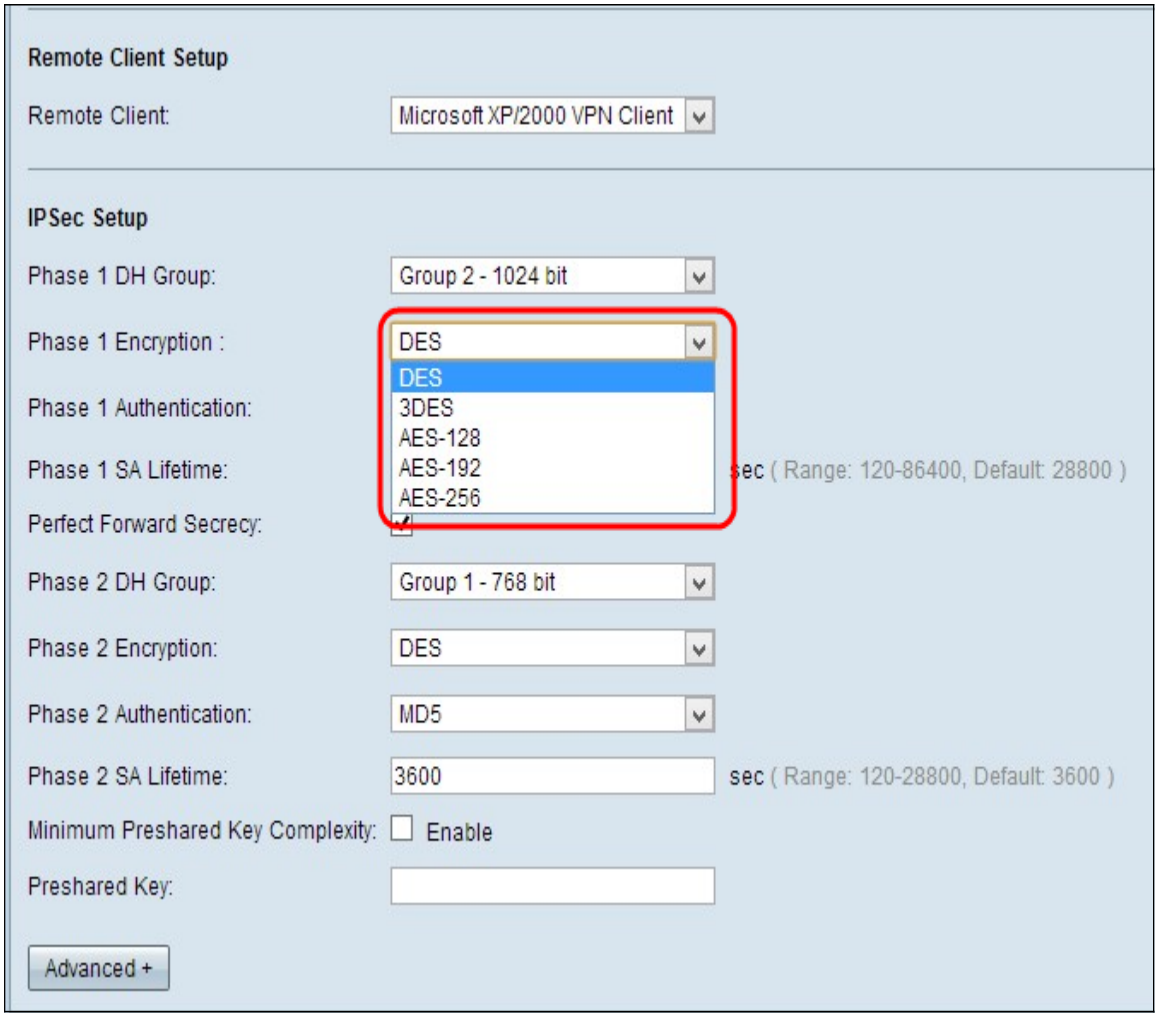
Le opzioni disponibili sono definite come segue:

·Gruppo 1 (768 bit): calcola la chiave più velocemente, ma è la meno sicura.

·Gruppo2 (1024 bit): calcola la chiave più lentamente, ma è più sicuro di Gruppo1.

·Gruppo 5 (1536 bit): calcola la chiave più lentamente, ma è la più sicura.

Passaggio 2. Scegliere il metodo di crittografia appropriato per cifrare la chiave dall'elenco a discesa *Crittografia fase 1*. AES-128 è consigliato per l'alta sicurezza e le prestazioni veloci. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.



Le opzioni disponibili sono definite come segue:

·DES: Data Encryption Standard (DES) è un vecchio metodo di crittografia a 56 bit che non è molto sicuro, ma potrebbe essere necessario per garantire la compatibilità con le versioni precedenti.

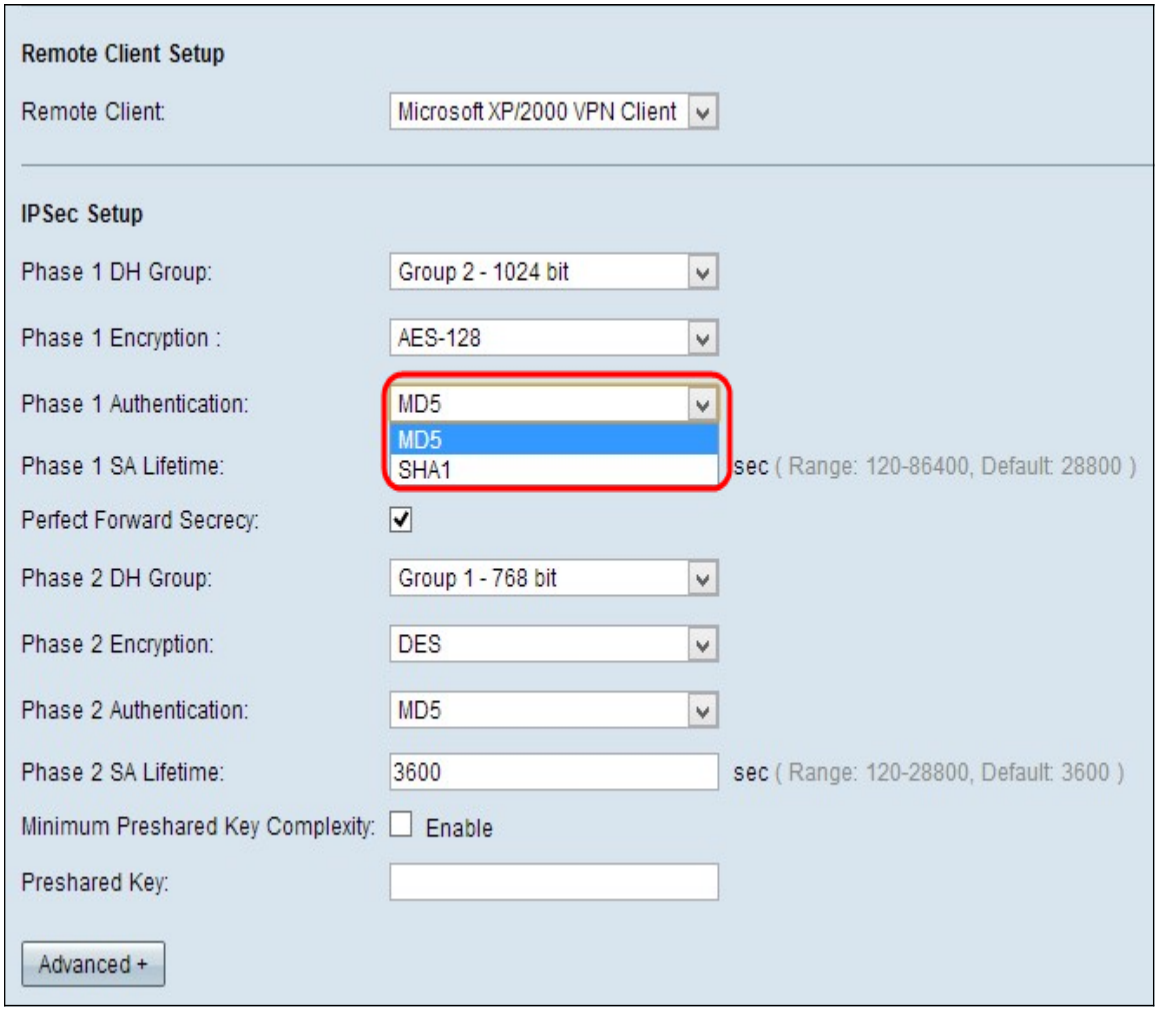
·3DES: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit utilizzato per aumentare le dimensioni della chiave, in quanto esegue la crittografia dei dati tre volte. Ciò garantisce una maggiore sicurezza rispetto a DES ma una minore sicurezza rispetto a AES.

·AES-128 — Advanced Encryption Standard con chiave a 128 bit (AES-128) utilizza una chiave a 128 bit per la crittografia AES. AES è più veloce e sicuro rispetto a DES. In generale, AES è anche più veloce e più sicuro di 3DES. AES-128 è più veloce ma meno sicuro di AES-192 e AES-256.

·AES-192 - AES-192 utilizza una chiave a 192 bit per la crittografia AES. AES-192 è più lento ma più sicuro di AES-128 e più veloce ma meno sicuro di AES-256.

·AES-256 - AES-256 utilizza una chiave a 256 bit per la crittografia AES. AES-256 è più lento ma più sicuro di AES-128 e AES-192.

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

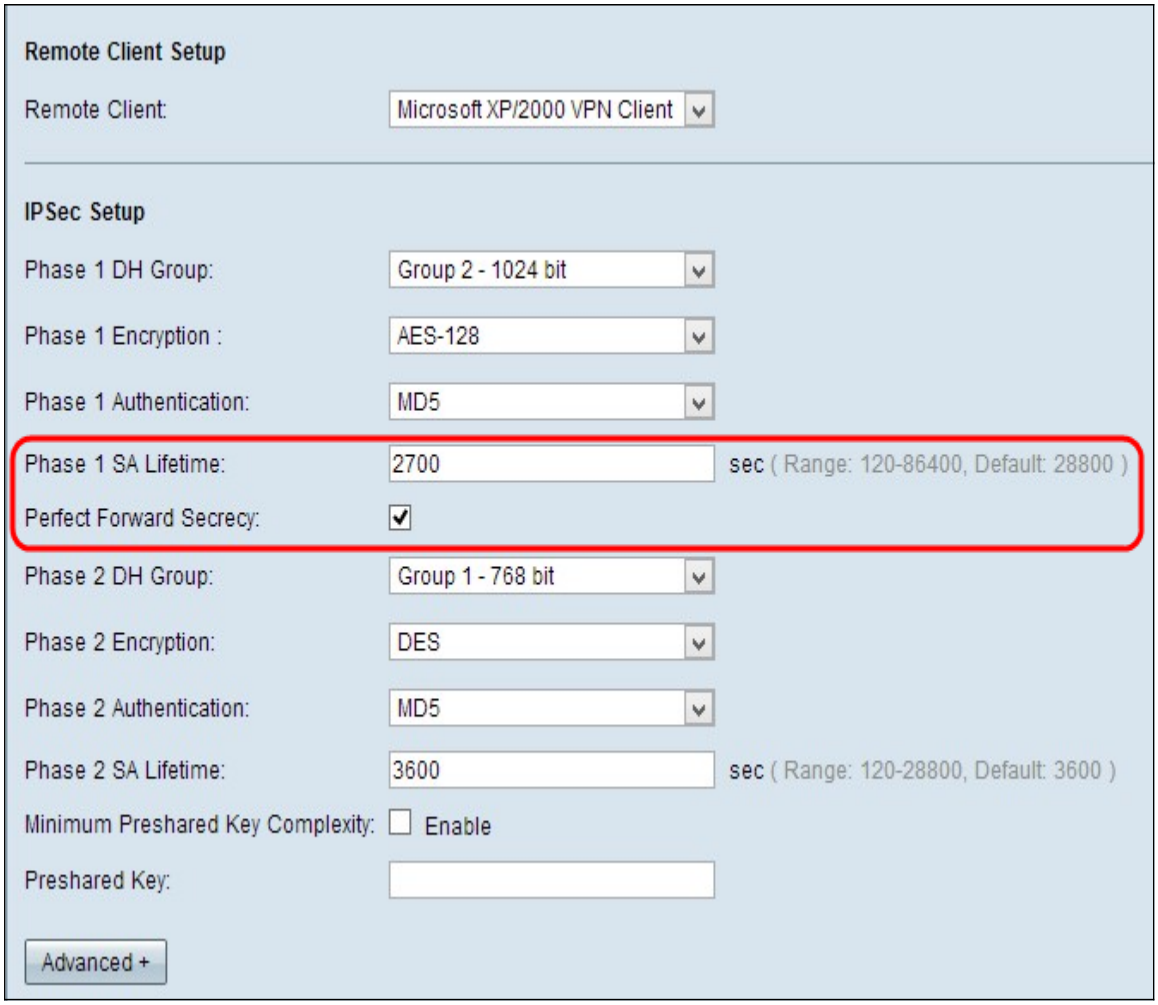


Le opzioni disponibili sono definite come segue:

·MD5 — Message Digest Algorithm-5 (MD5) rappresenta una funzione hash a 128 bit 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.

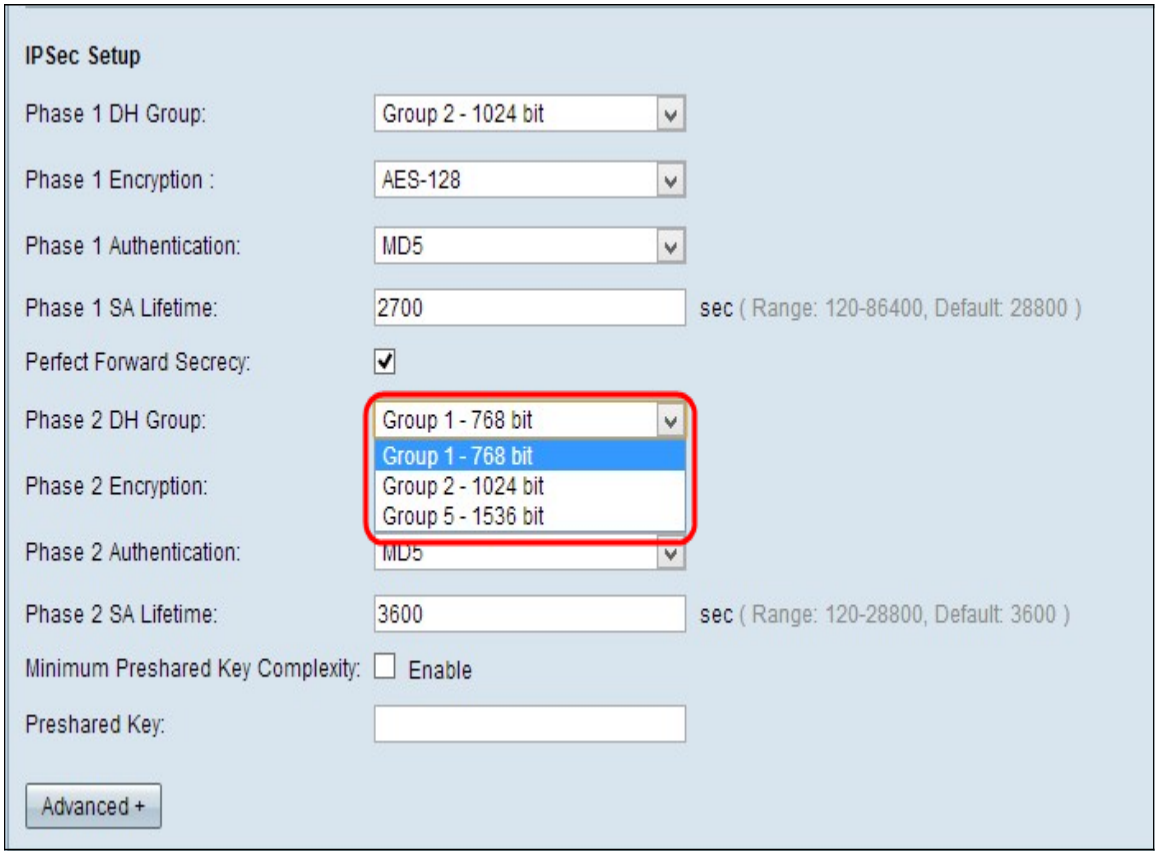
Passaggio 4. Nel campo *Durata ASA fase 1*, immettere il periodo di tempo in secondi durante il quale il tunnel VPN rimane attivo nella fase 1. Il tempo predefinito è 28.800 secondi.



Passaggio 5. (Facoltativo) Per proteggere ulteriormente le chiavi, selezionare la casella di controllo **Perfect Forward Secrecy**. Questa opzione consente di generare una nuova chiave se una delle chiavi è compromessa. Si tratta di un'azione consigliata in quanto offre maggiore protezione.

Nota: se si deseleziona **Perfect Forward Secrecy** nel passaggio 5, non è necessario configurare il gruppo DH per la fase 2.

Passaggio 6. Scegliere il gruppo DH appropriato dall'elenco a discesa *Gruppo DH fase 2*.



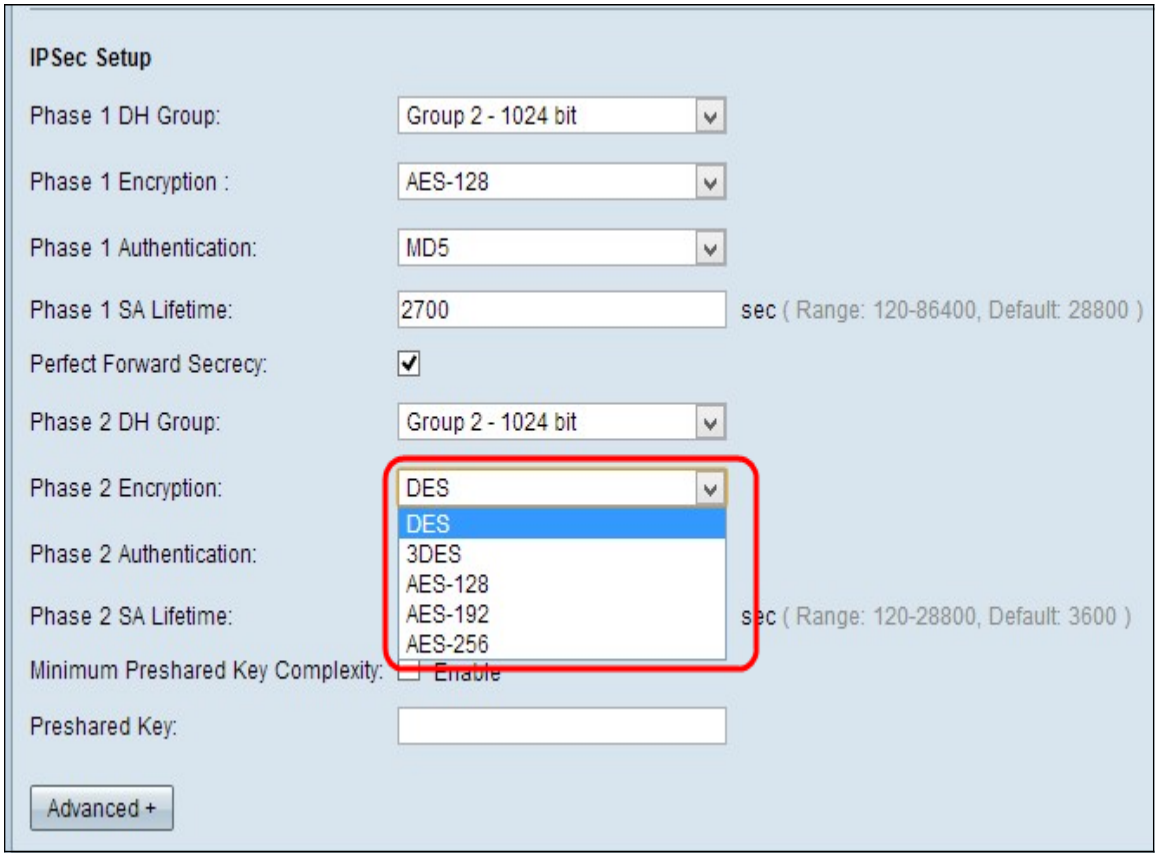
Le opzioni disponibili sono definite come segue:

·Gruppo 1 (768 bit): calcola la chiave più velocemente, ma è la meno sicura.

·Gruppo2 (1024 bit): calcola la chiave più lentamente, ma è più sicuro di Gruppo1.

·Gruppo 5 (1536 bit): calcola la chiave più lentamente, ma è la più sicura.

Passaggio 2. Scegliere il metodo di crittografia appropriato per cifrare la chiave dall'elenco a discesa *Crittografia fase 1*. AES-128 è consigliato per l'alta sicurezza e le prestazioni veloci. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.



Le opzioni disponibili sono definite come segue:

·DES: Data Encryption Standard (DES) è un vecchio metodo di crittografia a 56 bit che non è molto sicuro, ma potrebbe essere necessario per garantire la compatibilità con le versioni precedenti.

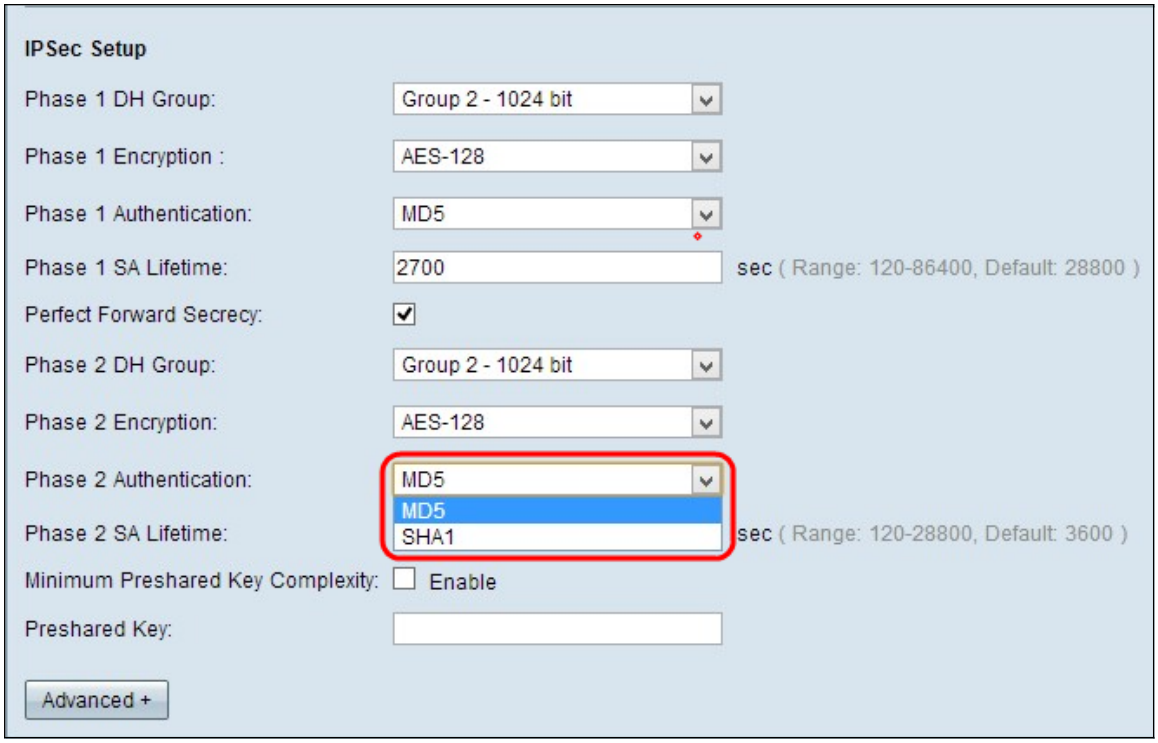
·3DES: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit utilizzato per aumentare le dimensioni della chiave, in quanto esegue la crittografia dei dati tre volte. Ciò garantisce una maggiore sicurezza rispetto a DES ma una minore sicurezza rispetto a AES.

·AES-128 — Advanced Encryption Standard con chiave a 128 bit (AES-128) utilizza una chiave a 128 bit per la crittografia AES. AES è più veloce e sicuro rispetto a DES. In generale, AES è anche più veloce e più sicuro di 3DES. AES-128 è più veloce ma meno sicuro di AES-192 e AES-256.

·AES-192 - AES-192 utilizza una chiave a 192 bit per la crittografia AES. AES-192 è più lento ma più sicuro di AES-128 e più veloce ma meno sicuro di AES-256.

·AES-256 - AES-256 utilizza una chiave a 256 bit per la crittografia AES. AES-256 è più lento ma più sicuro di AES-128 e AES-192.

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.

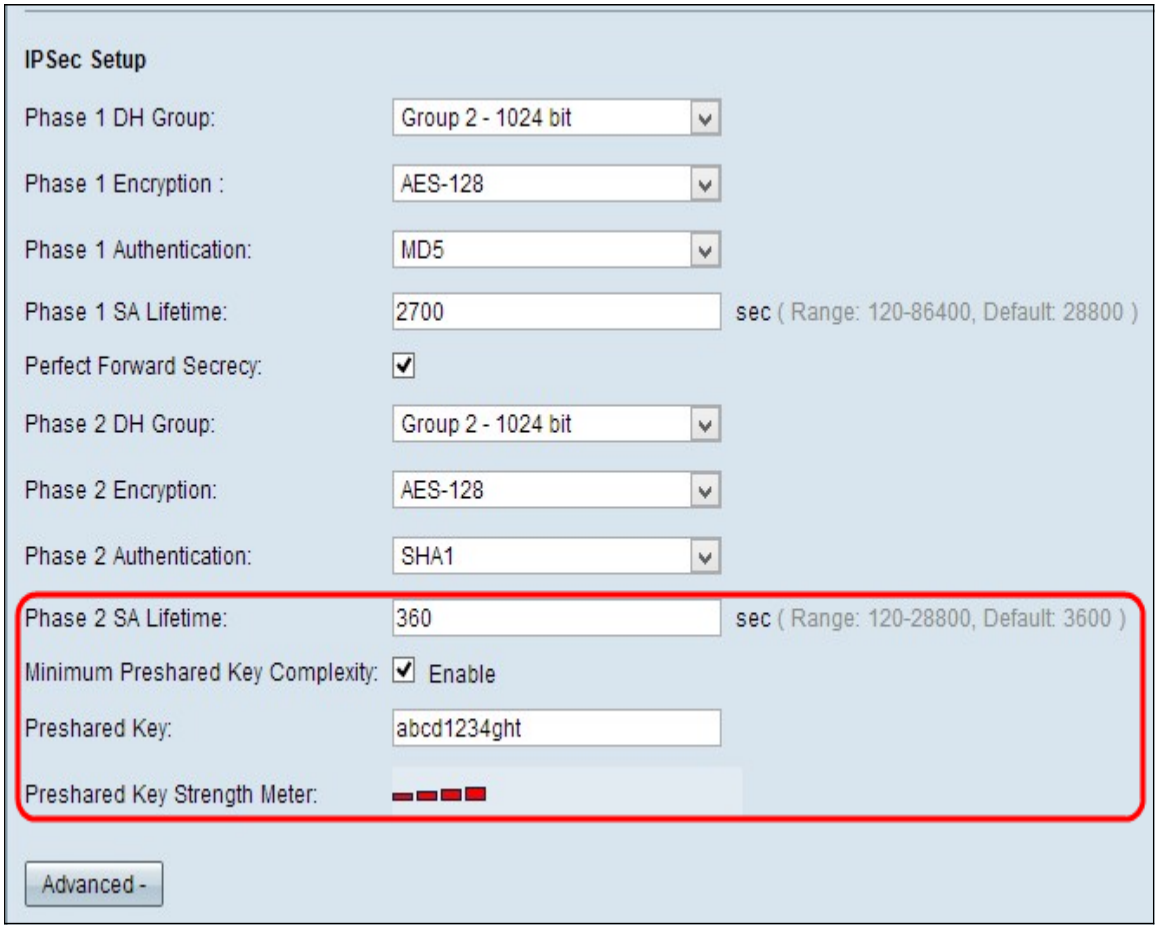


Le opzioni disponibili sono definite come segue:

·MD5 — Message Digest Algorithm-5 (MD5) rappresenta una funzione hash a 128 bit 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 9. Nel campo *Durata associazione di sicurezza fase 2*, immettere il periodo di tempo in secondi durante il quale il tunnel VPN rimane attivo nella fase 2. Il tempo predefinito è 3600 secondi.



Passaggio 10. (Facoltativo) Se si desidera attivare il misuratore di affidabilità per la chiave già condivisa, selezionare la casella di controllo **Complessità minima chiave già condivisa**.

Nota: Se si seleziona la casella di controllo **Complessità minima chiave già condivisa**, il *misuratore dell'intensità della chiave già condivisa* visualizza 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.

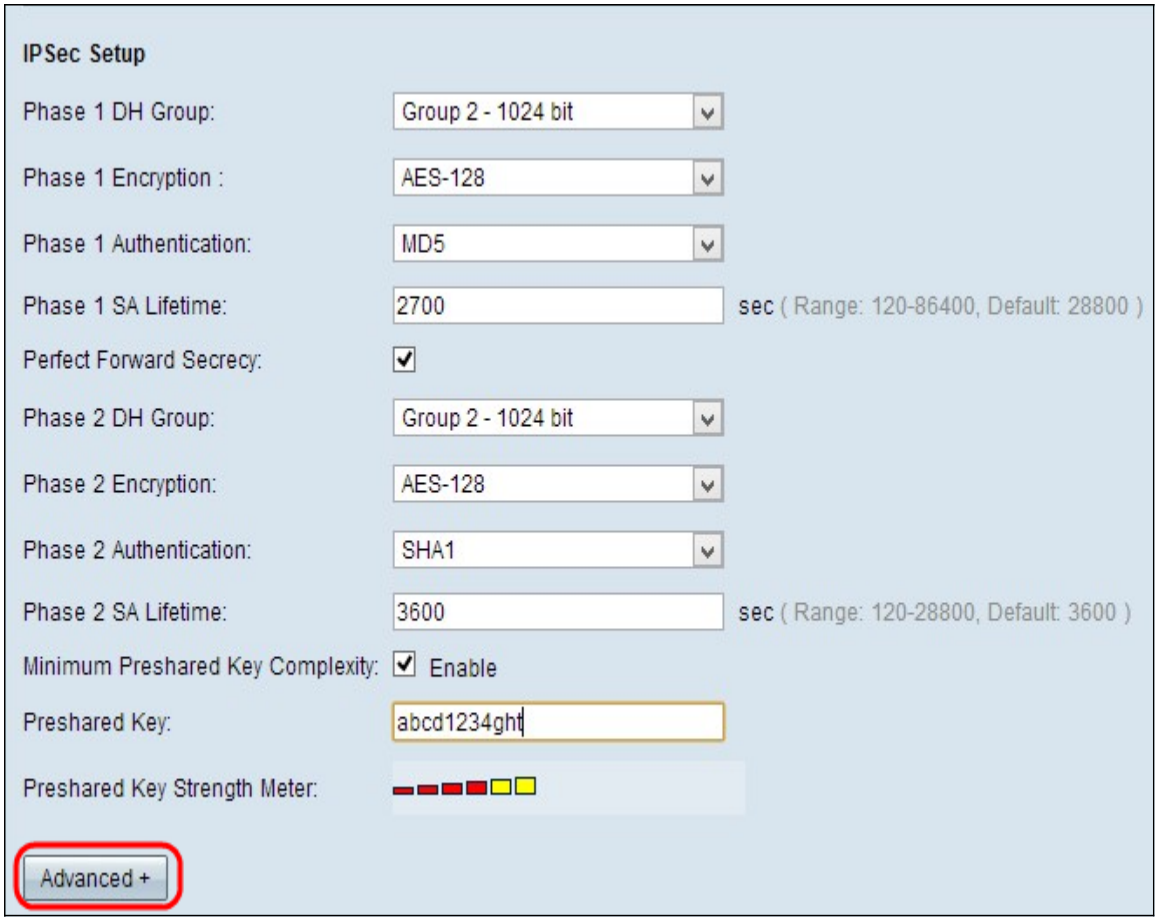
Passaggio 11. Immettere la chiave desiderata nel campo *Chiave già condivisa*. È possibile utilizzare fino a 30 caratteri esadecimali come chiave già condivisa. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.

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

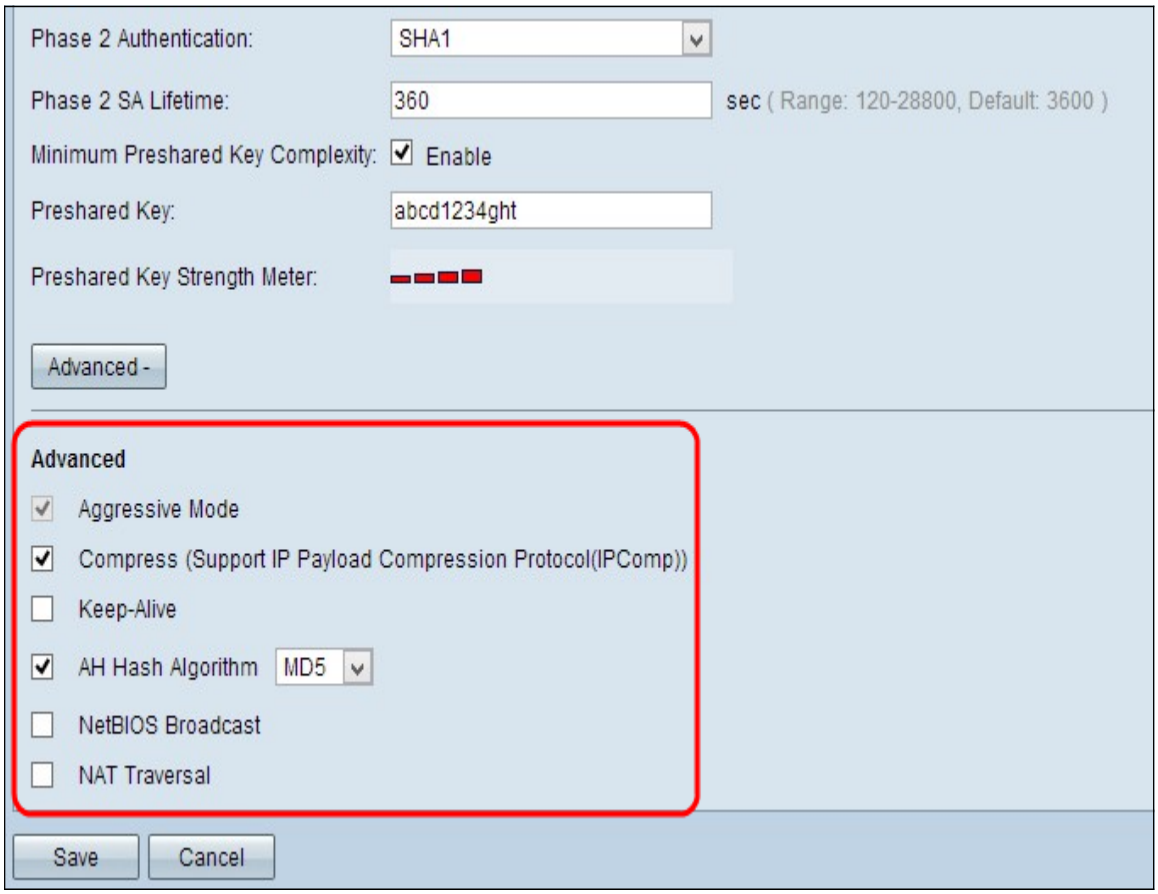
Passaggio 12. Per salvare le impostazioni correnti e lasciare le altre predefinite, scorrere verso il basso e fare clic su **Salva** per salvare le impostazioni.

Configurazione avanzata

Passaggio 1. Fare clic su **Advanced** (Avanzate) per configurare le impostazioni avanzate.



Viene visualizzata l'area *Avanzate* con i nuovi campi disponibili.



Passaggio 2. (Facoltativo) Selezionare la casella di controllo **Modalità aggressiva** se la velocità della rete è bassa. La modalità aggressiva scambia gli ID degli endpoint del tunnel in testo non crittografato durante la connessione SA, operazione che richiede meno tempo

per lo scambio ma meno sicura.

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

Passaggio 4. (Facoltativo) Selezionare la casella di controllo **Keep-Alive** se si desidera che la connessione del tunnel VPN rimanga sempre attiva. Keep-Alive consente di ristabilire immediatamente le connessioni nel caso in cui una connessione diventi inattiva.

Passaggio 5. (Facoltativo) Selezionare la casella di controllo Algoritmo hash AH se si desidera estendere l'autenticazione all'origine dati, l'integrità dei dati tramite checksum e la protezione all'intestazione IP. Quindi scegliere il metodo di autenticazione appropriato dall'elenco a discesa. Il tunnel deve avere lo stesso algoritmo per entrambi i lati.

Le opzioni disponibili sono definite come segue:

·MD5 — Message Digest Algorithm-5 (MD5) rappresenta una funzione hash a 128 bit 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 la casella di controllo **Trasmissione NetBIOS** per 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 applicazioni software e funzionalità di Windows come Risorse di rete.

Passaggio 7. (Facoltativo) Selezionare la casella di controllo **NAT Traversal** per accedere a Internet dalla LAN privata tramite l'indirizzo IP pubblico. L'attraversamento NAT viene utilizzato per fare in modo che gli indirizzi IP privati dei sistemi interni vengano visualizzati come indirizzi IP pubblici per proteggere gli indirizzi IP privati da attacchi dannosi o da rilevamenti.

Passaggio 8. Fare clic su **Save** per salvare le impostazioni.