Configurazione di un server VPN IPSec su RV130 e RV130W

Obiettivo

IPSec VPN (Virtual Private Network) consente di ottenere l'accesso remoto sicuro alle risorse aziendali tramite la creazione di un tunnel crittografato su Internet.

Lo scopo di questo documento è mostrare come configurare un server VPN IPSec su RV130 e RV130W.

Nota: Per informazioni su come configurare un server VPN IPSec con Shrew Soft VPN Client su RV130 e RV130W, fare riferimento all'articolo *Use Shrew Soft VPN Client con IPSec VPN Server su RV130 e RV130W*.

Dispositivi interessati

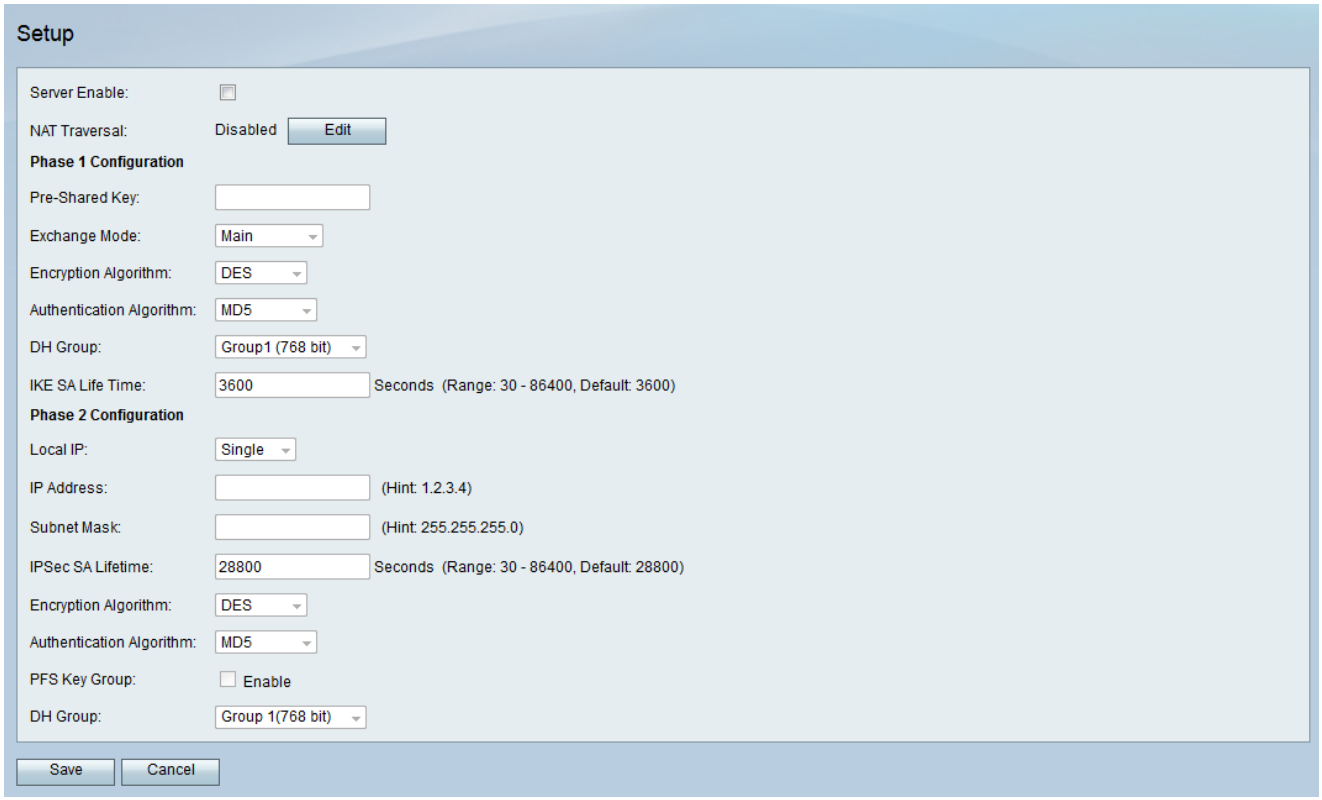
·RV130W Wireless-N VPN Firewall
· RV130 VPN Firewall

Versione del software

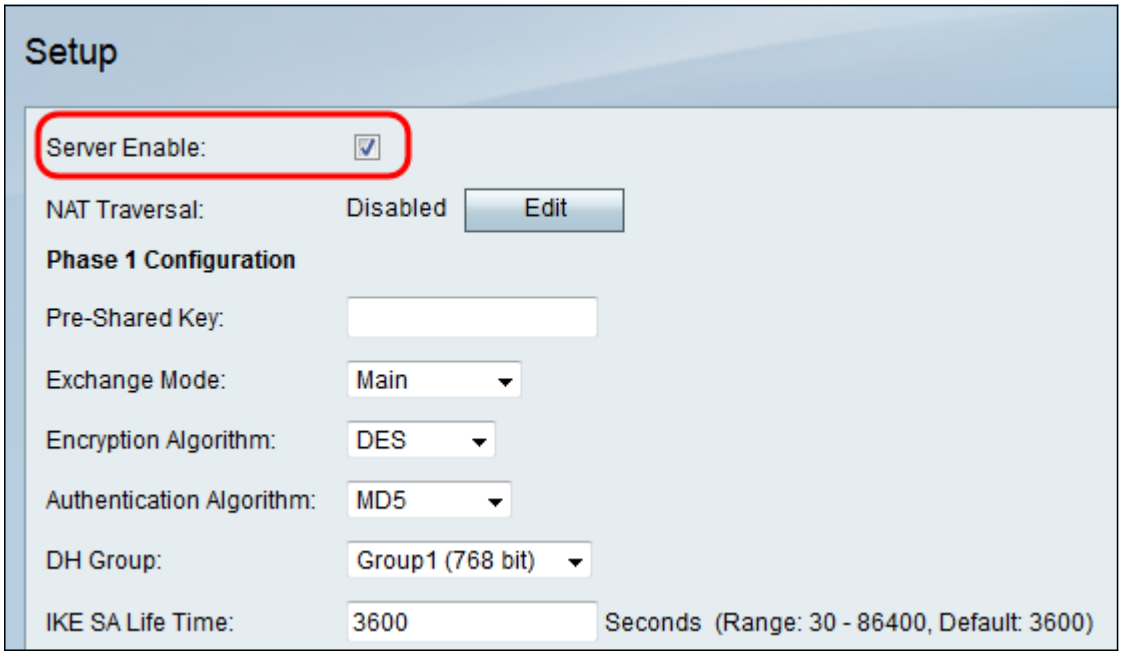
·v1.0.1.3

Configurazione server VPN IPSec

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

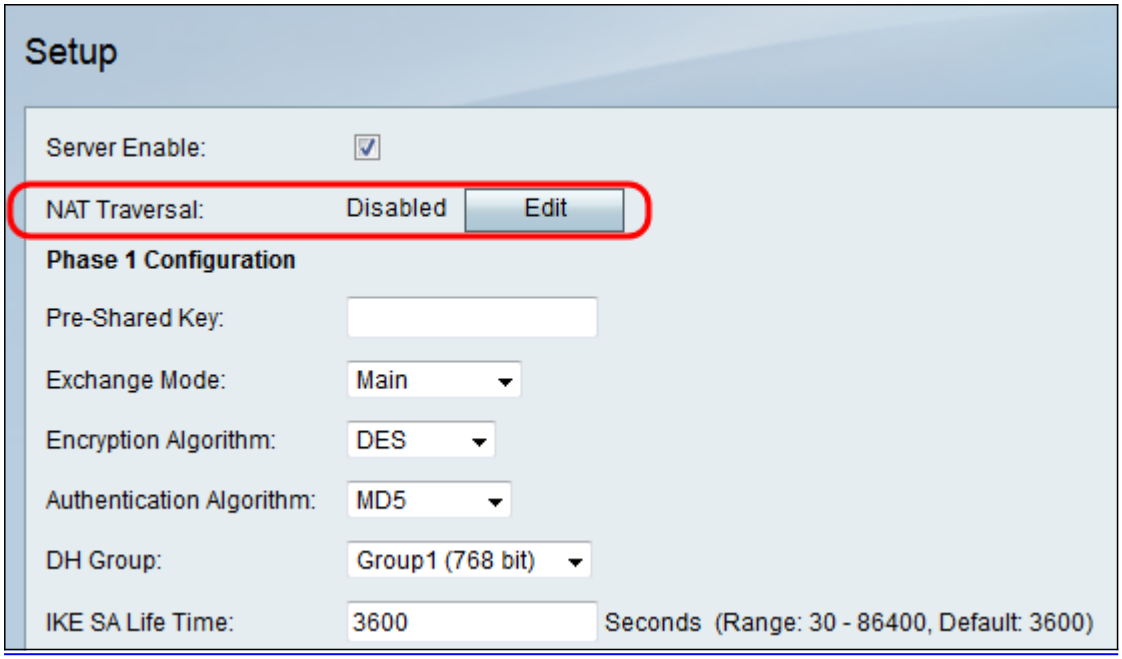


Passaggio 2. Selezionare la casella di controllo **Abilita server** per abilitare il certificato.

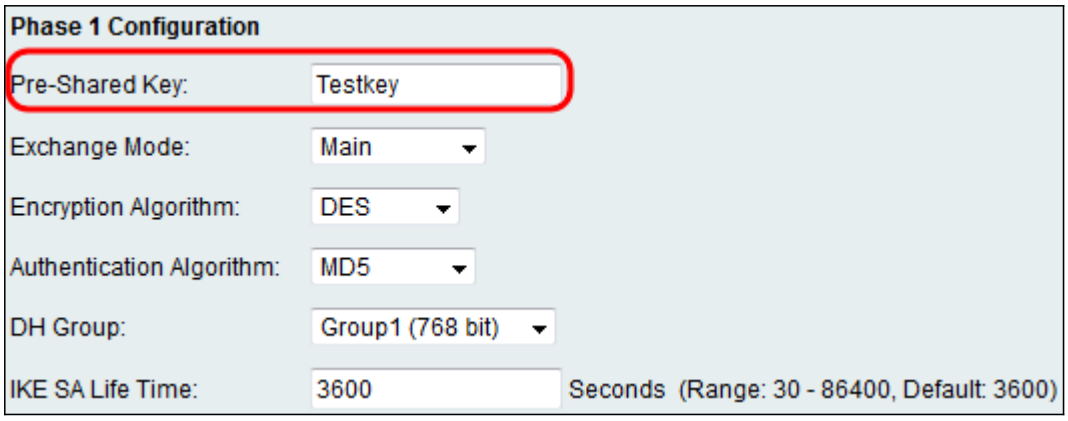


Passaggio 3. (Facoltativo) Se il router o il client VPN è protetto da un gateway NAT, fare clic su **Edit** (Modifica) per configurare NAT Traversal. In caso contrario, lasciare NAT Traversal disabilitato.

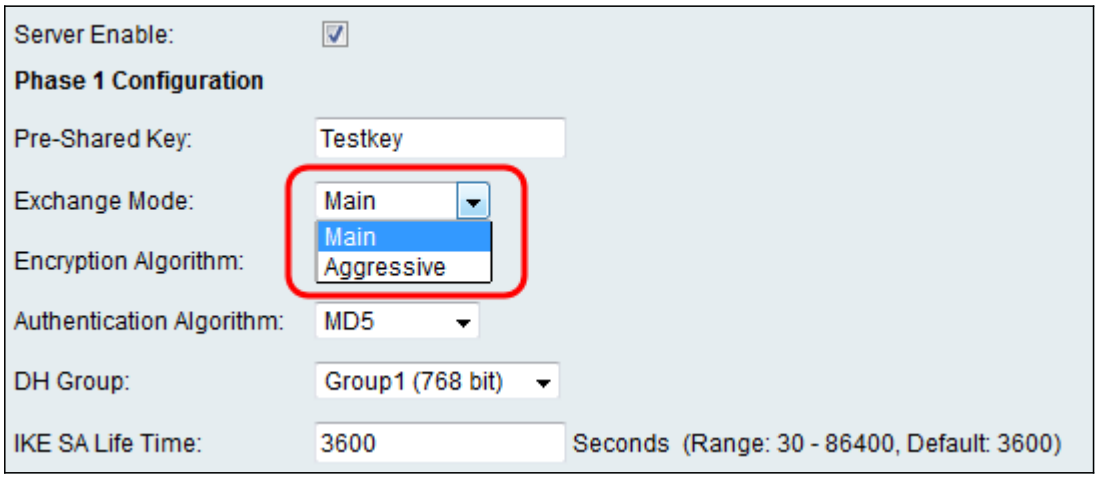
Nota: Per ulteriori informazioni su come configurare le impostazioni di NAT Traversal, fare riferimento alle *impostazioni dei criteri IKE (Internet Key Exchange) sui router VPN RV130 e RV130W.*



Passaggio 4. Immettere una chiave di lunghezza compresa tra 8 e 49 caratteri che verrà scambiata tra il dispositivo e l'endpoint remoto nel campo *Chiave già condivisa*.

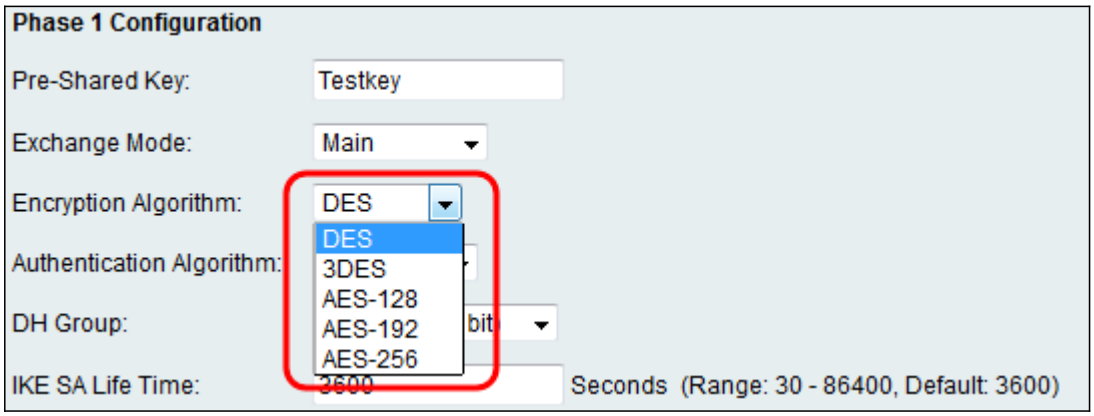


Passaggio 5. Dall'elenco a discesa *Modalità Exchange* scegliere la modalità per la connessione VPN IPSec. **Principale** è la modalità predefinita. Tuttavia, se la velocità della rete è bassa, scegliere la modalità **aggressiva**.



Nota: La modalità aggressiva scambia gli ID degli endpoint del tunnel in testo non crittografato durante la connessione, operazione che richiede meno tempo per lo scambio ma meno sicura.

Passaggio 6. Dall'elenco a discesa **Encryption Algorithm**, scegliere il metodo di crittografia appropriato per crittografare la chiave già condivisa nella fase 1. AES-128 è consigliato per la sua elevata sicurezza e le prestazioni elevate. 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.

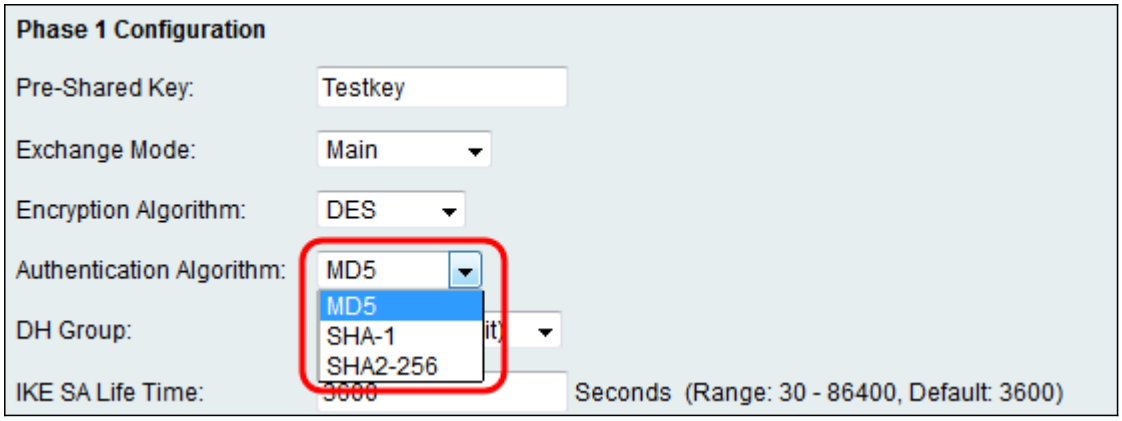
·3DES: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit utilizzato per aumentare le dimensioni della chiave, in quanto esegue la crittografia dei dati tre volte. Ciò garantisce una maggiore sicurezza rispetto a DES ma una minore sicurezza rispetto a AES.

·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 7. Dall'elenco a discesa *Authentication Algorithm*, scegliere il metodo di autenticazione appropriato per determinare la modalità di convalida dei pacchetti dell'intestazione del protocollo Encapsulating Security Payload (ESP) nella fase 1. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità della connessione.



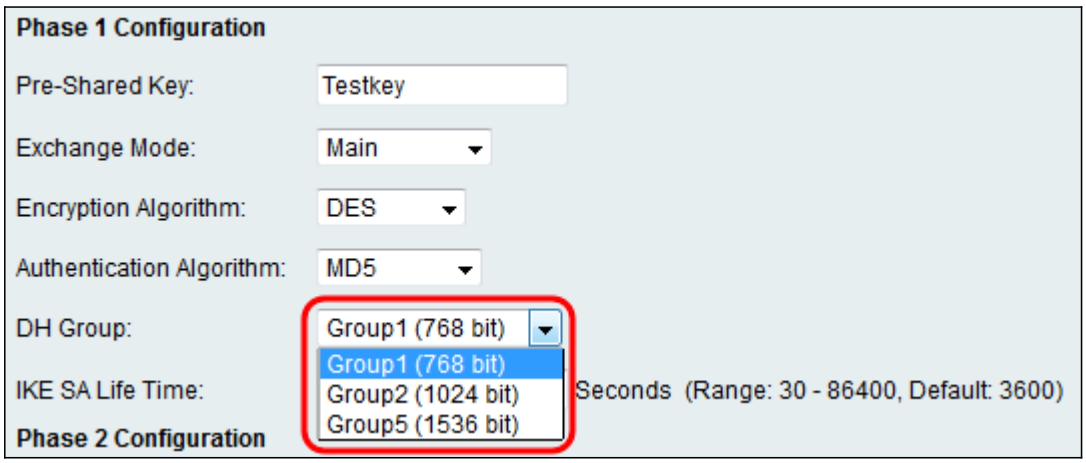
Le opzioni disponibili sono definite come segue:

·MD5 — MD5 è un algoritmo hash unidirezionale che produce un digest a 128 bit. MD5 è più veloce di SHA-1, ma meno sicuro di SHA-1. MD5 non è consigliato.

·SHA-1 — SHA-1 è un algoritmo hash unidirezionale che produce un digest a 160 bit. SHA-1 è più lento di MD5, ma più sicuro di MD5.

·SHA2-256 — specifica l'algoritmo di hash sicuro SHA2 con il digest a 256 bit.

Passaggio 8. Dall'elenco a discesa *Gruppo DH*, scegliere il gruppo Diffie-Hellman (DH) appropriato da utilizzare con la chiave nella fase 1. Diffie-Hellman è un protocollo di scambio di chiave crittografica utilizzato nella connessione per lo scambio di set di chiavi già condivise. La forza dell'algoritmo è determinata dai bit.



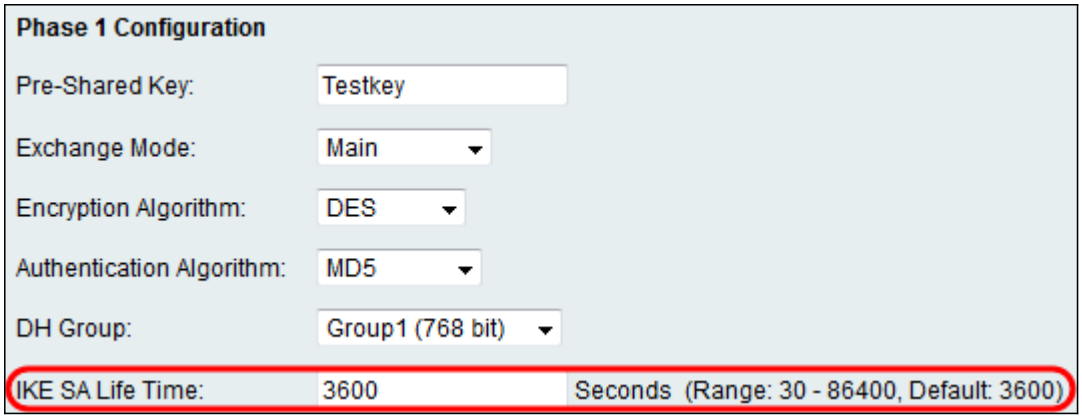
Le opzioni disponibili sono definite come segue:

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

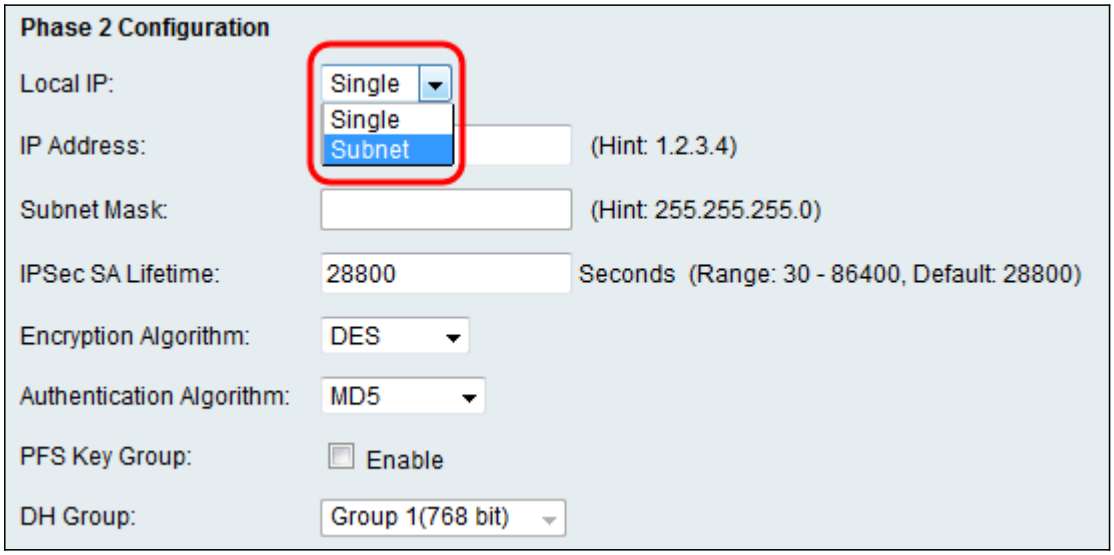
·Gruppo2 (1024 bit): calcola la chiave più lentamente, ma è più sicuro di Gruppo1.

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

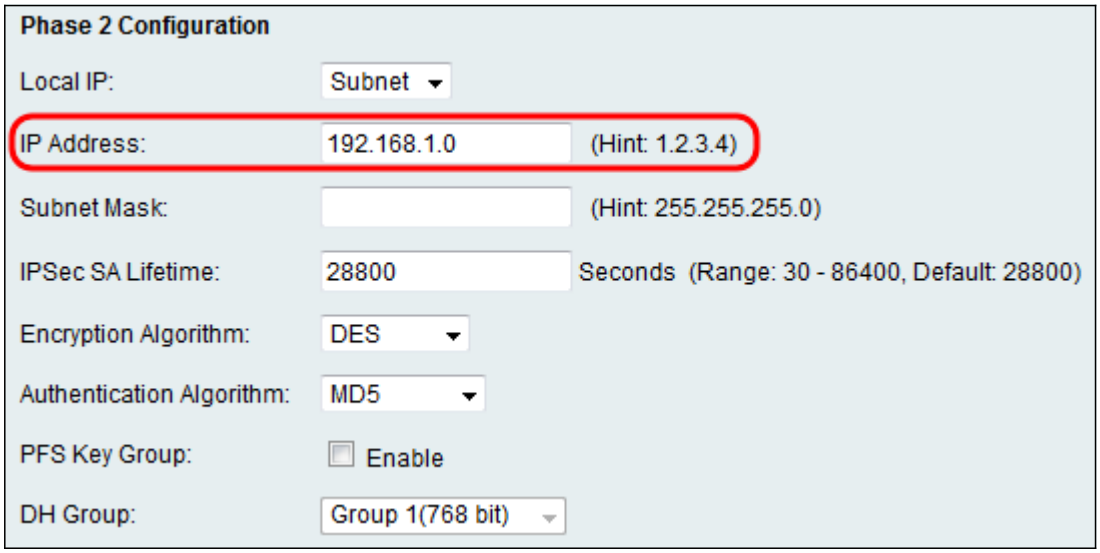
Passaggio 9. Nel campo *Durata associazione di protezione IKE* immettere il periodo di tempo in secondi durante il quale la chiave IKE automatica è valida. Allo scadere di questo periodo, viene negoziata automaticamente una nuova chiave.



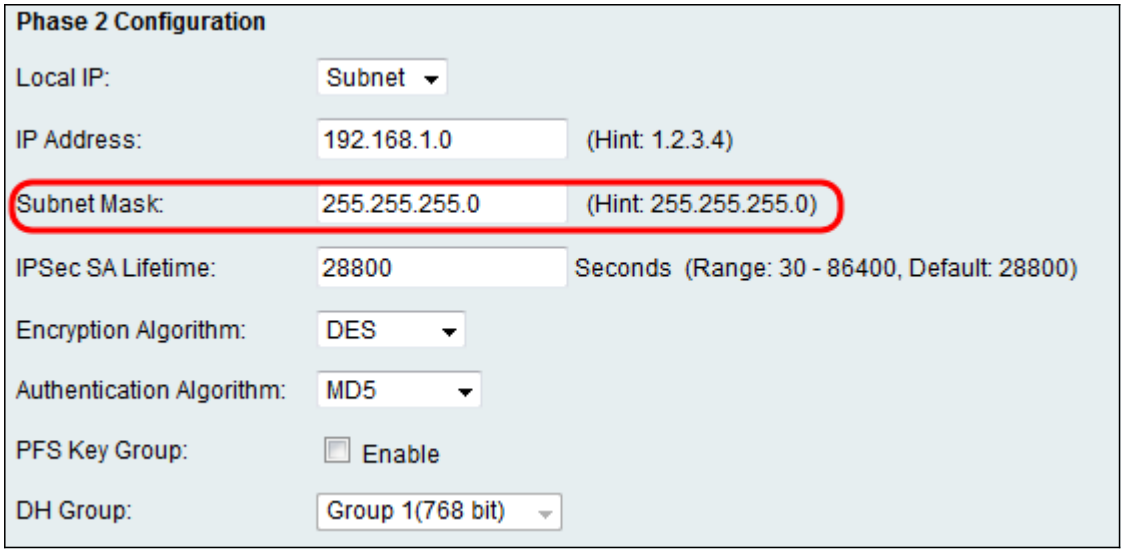
Passaggio 10. Dall'elenco a discesa *IP locale*, scegliere **Singolo** se si desidera che un singolo utente LAN locale acceda al tunnel VPN, oppure scegliere **Subnet** se si desidera che più utenti possano accedervi.



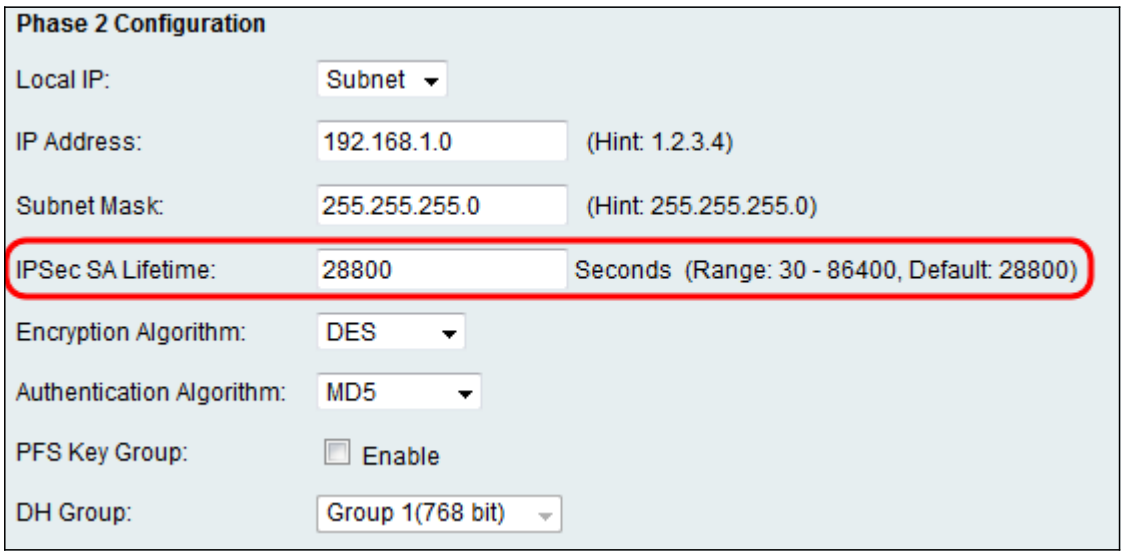
Passaggio 11. Se nel passaggio 10 è stata scelta la **subnet**, immettere l'indirizzo IP di rete della subnet nel campo Indirizzo IP. Se nel passaggio 10 è stato scelto **Single**, immettere l'indirizzo IP del singolo utente e andare al passaggio 13.



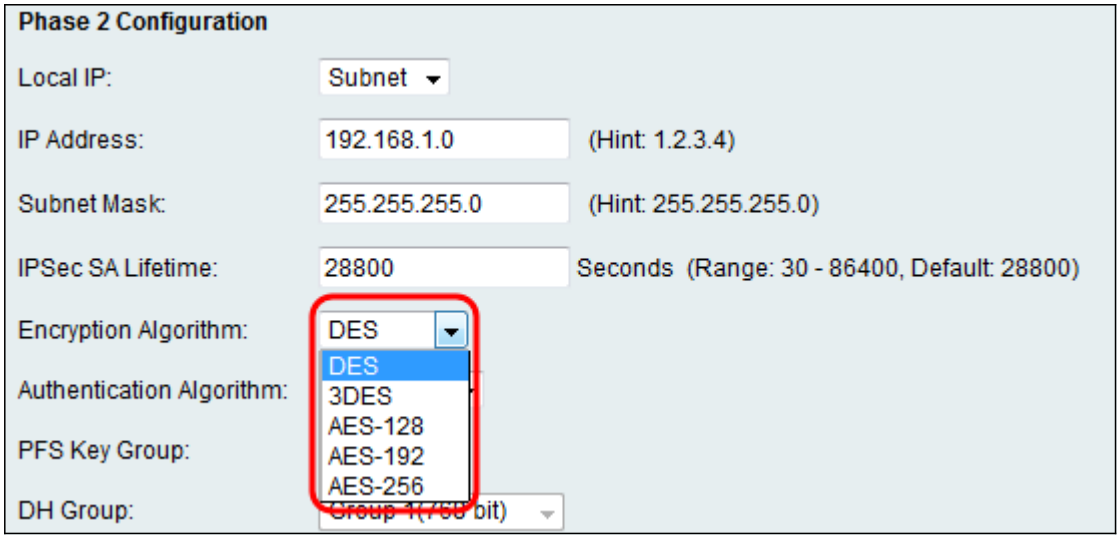
Passaggio 12. (Facoltativo) Se nel passaggio 10 è stata scelta **Subnet mask**, immettere la subnet mask della rete locale nel campo *Subnet mask*.



Passaggio 13. Nel campo *Durata SA IPSec*, immettere il periodo di tempo in secondi durante il quale la connessione VPN rimane attiva nella fase 2. Alla scadenza di questo periodo, l'associazione di sicurezza IPSec per la connessione VPN viene rinegoziata.



Passaggio 14. Dall'elenco a discesa *Encryption Algorithm*, scegliere il metodo di crittografia appropriato per crittografare la chiave già condivisa della fase 2. AES-128 è consigliato per la sua elevata sicurezza e le prestazioni elevate. 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 meno sicuro, ma potrebbe essere necessario per garantire la compatibilità con le versioni precedenti.

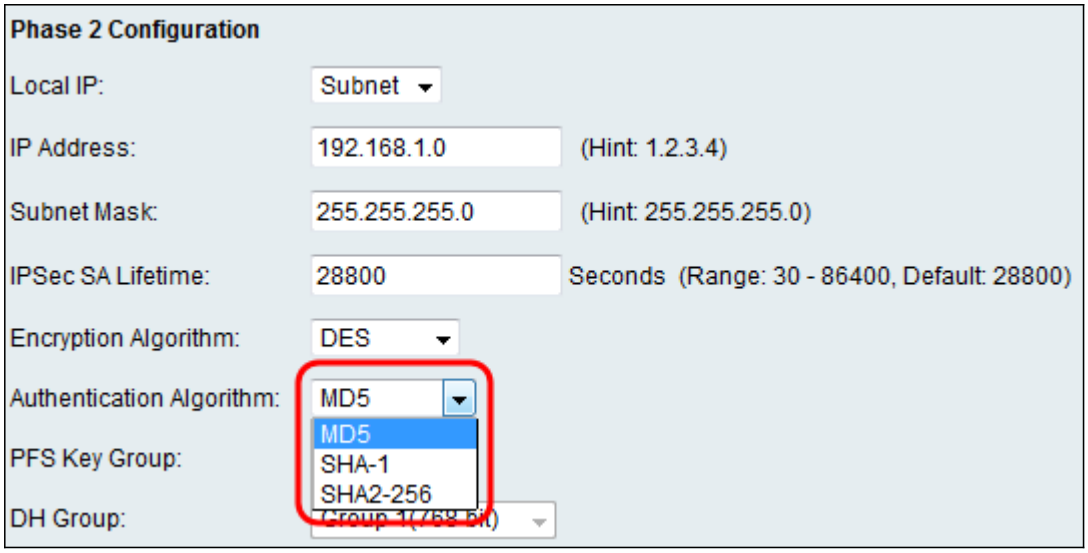
·3DES: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit utilizzato per aumentare le dimensioni della chiave, in quanto esegue la crittografia dei dati tre volte. Ciò garantisce una maggiore sicurezza rispetto a DES ma una minore sicurezza rispetto a AES.

·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 15. Dall'elenco a discesa *Authentication Algorithm* (*Algoritmo di autenticazione)*, scegliere il metodo di autenticazione appropriato per determinare come i pacchetti dell'intestazione del protocollo Encapsulating Security Payload (ESP) vengono convalidati nella fase 2. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.



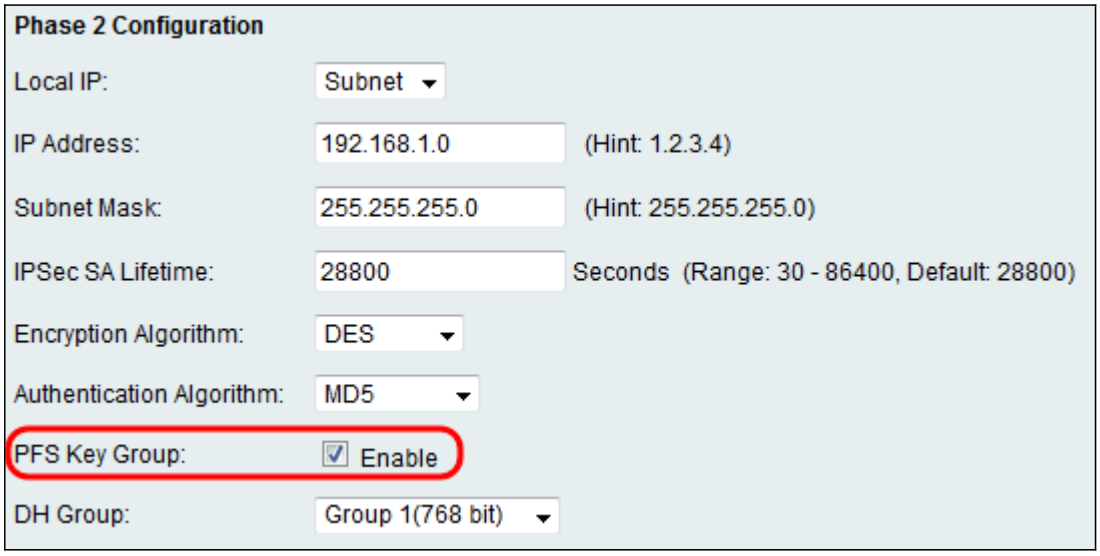
Le opzioni disponibili sono definite come segue:

·MD5 — MD5 è un algoritmo hash unidirezionale che produce un digest a 128 bit. MD5 è più veloce di SHA-1, ma meno sicuro di SHA-1. MD5 non è consigliato.

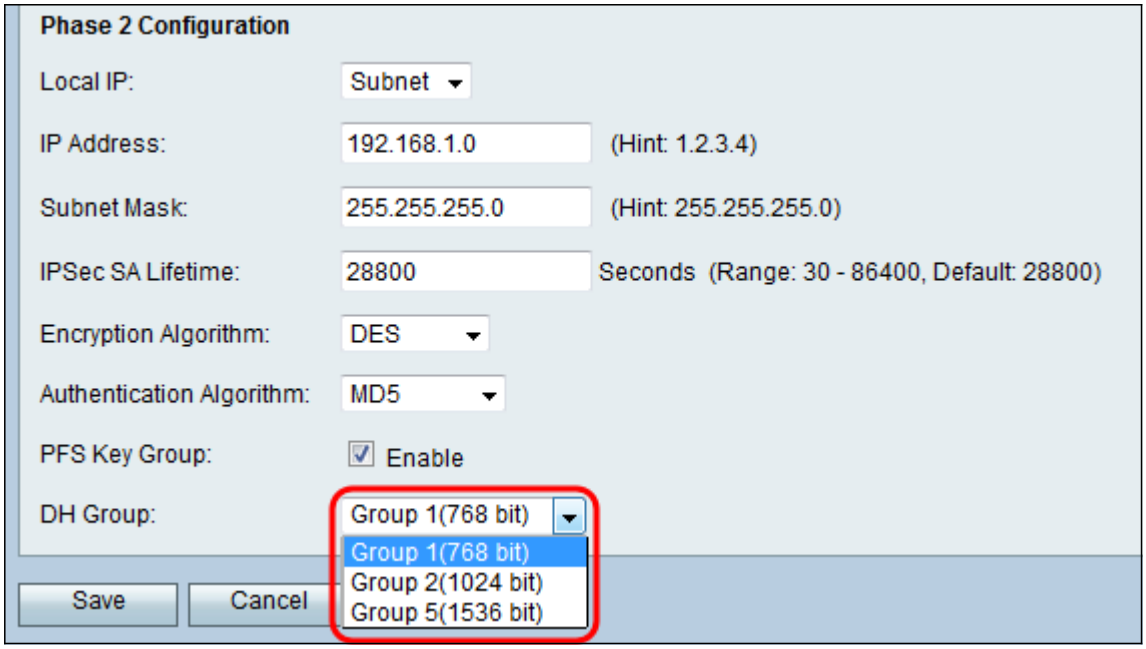
·SHA-1 — SHA-1 è un algoritmo hash unidirezionale che produce un digest a 160 bit. SHA-1 è più lento di MD5, ma più sicuro di MD5.

·SHA2-256 — specifica l'algoritmo di hash sicuro SHA2 con il digest a 256 bit.

Passaggio 16. (Facoltativo) Nel campo *Gruppo chiavi PFS* selezionare la casella di controllo **Abilita**. Perfect Forward Secrecy (PFS) crea un ulteriore livello di sicurezza nella protezione dei dati garantendo una nuova chiave DH nella fase 2. Il processo viene eseguito nel caso in cui la chiave DH generata nella fase 1 venga compromessa durante la trasmissione.



Passaggio 17. Dall'elenco a discesa *Gruppo DH*, scegliere il gruppo Diffie-Hellman (DH) appropriato da utilizzare con la chiave nella fase 2.



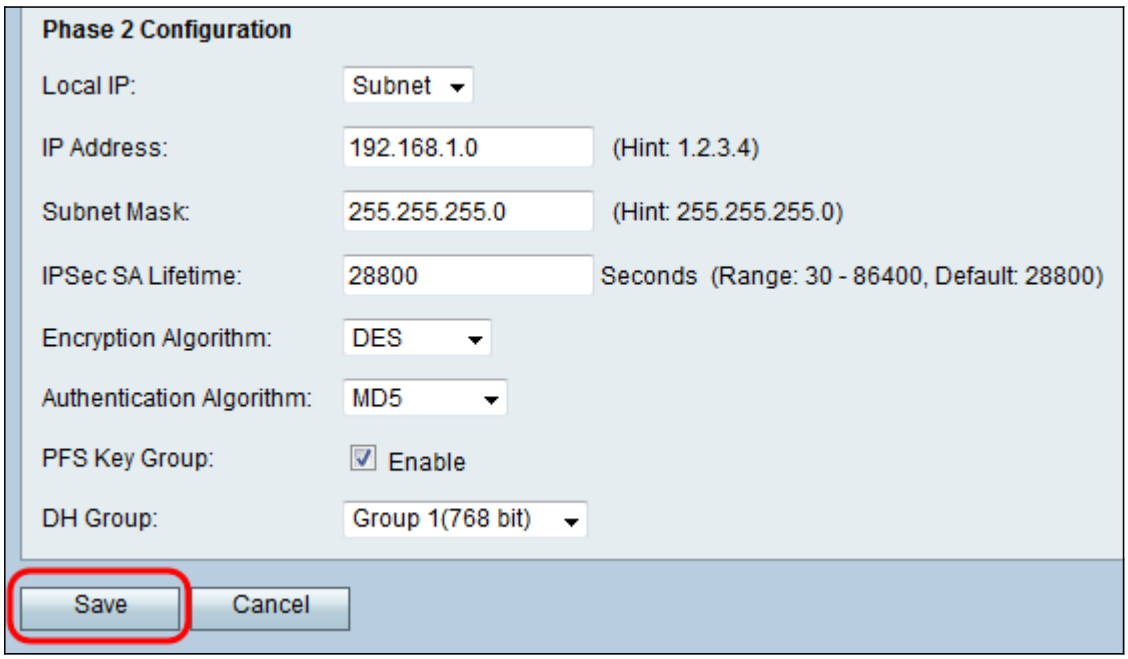
Le opzioni disponibili sono definite come segue:

·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 18. Fare clic su **Salva** per salvare le impostazioni.



Per ulteriori informazioni, consultare la seguente documentazione:

- RV130 Data sheet - spiega le funzionalità VPN per i router serie RV130
- Pagina del prodotto RV130 - include link per tutti gli articoli di Cisco sulla RV130

Informazioni su questa traduzione

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