Impostazioni dei criteri IKE (Internet Key Exchange) su RV130 e RV130W VPN Router

Obiettivo

IKE (Internet Key Exchange) è un protocollo che consente di stabilire comunicazioni protette tra due reti. Con IKE, i pacchetti vengono crittografati, bloccati e sbloccati con le chiavi utilizzate da due parti.

Ènecessario creare un criterio di scambio chiave Internet prima di configurare un criterio VPN. Per ulteriori informazioni, fare riferimento a *Configurazione dei criteri VPN su RV130 e RV130W*.

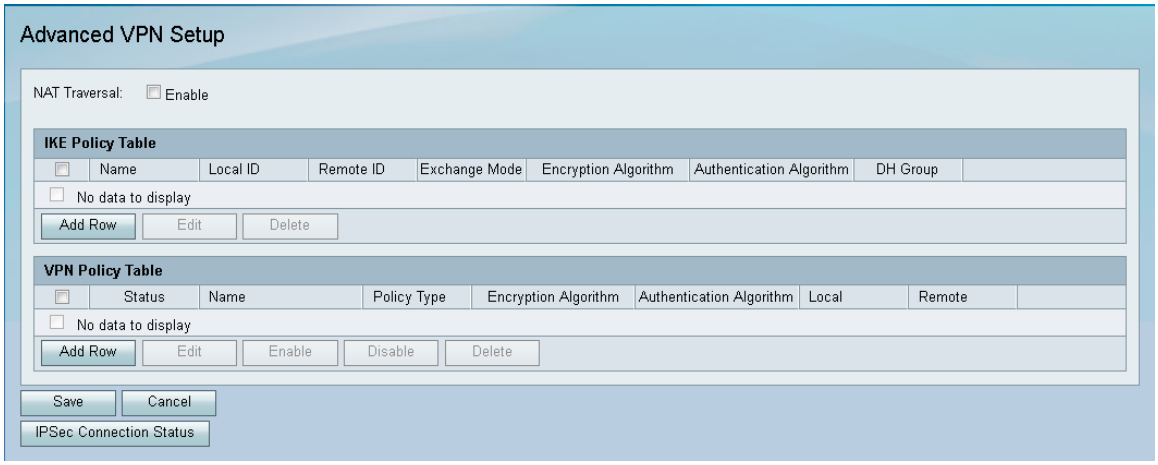
L'obiettivo di questo documento è mostrare come aggiungere un profilo IKE ai router VPN RV130 e RV130W.

Dispositivi interessati

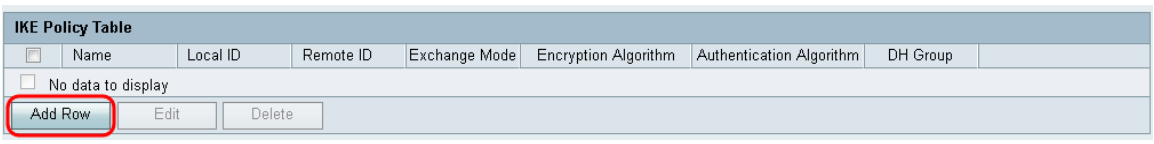
RV130
RV130W

Fasi della procedura

Passaggio 1. Utilizzare l'utilità Configurazione router per scegliere **VPN > VPN IPSec da sito a sito > Configurazione VPN avanzata** dal menu a sinistra. Viene visualizzata la pagina *Advanced VPN Setup*:

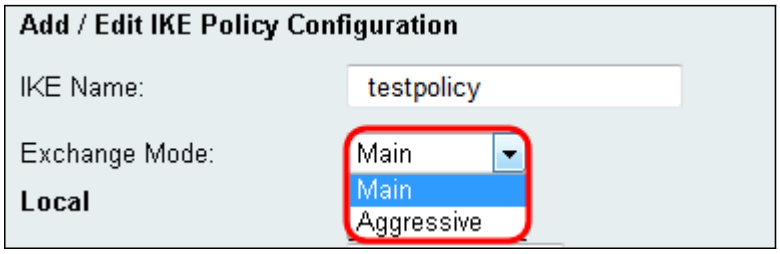


Passaggio 2. Nella tabella dei criteri IKE fare clic su **Aggiungi riga**. Viene visualizzata una nuova finestra:



Passaggio 3. Immettere un nome per il criterio IKE nel campo *Nome IKE*.

Passaggio 4. Dal menu a discesa *Modalità scambio*, scegliere la modalità in cui viene utilizzato lo scambio di chiave per stabilire una comunicazione sicura.

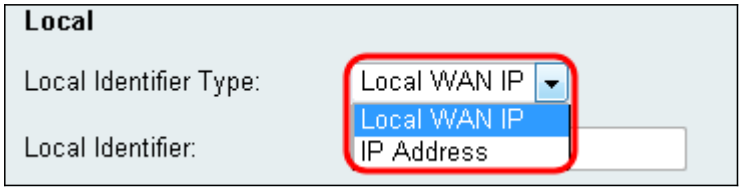


Le opzioni disponibili sono definite come segue:

·Principale: protegge l'identità dei peer per una maggiore sicurezza.

·Aggressivo: nessuna protezione dell'identità peer, ma connessione più rapida.

Passaggio 5. Dal menu a discesa *Tipo di identificatore locale*, scegliere il tipo di identità del profilo.

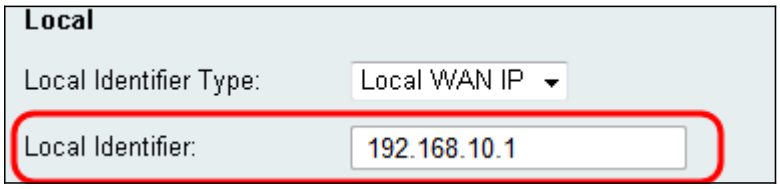


Le opzioni disponibili sono definite come segue:

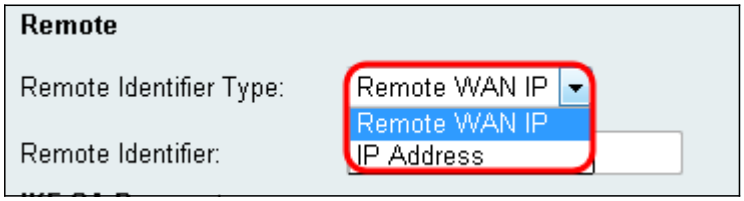
·IP WAN locale (Internet): connessione tramite Internet.

·Indirizzo IP: stringa univoca di numeri separati da punti che identifica ogni computer che utilizza il protocollo Internet per comunicare in rete.

Passaggio 6. (Facoltativo) Se **Indirizzo IP** è selezionato dall'elenco a discesa nel passaggio 5, immettere l'indirizzo IP locale nel campo *Identificatore locale*.



Passaggio 7. Dal menu a discesa *Tipo di identificatore remoto*, scegliere il tipo di identità del profilo.

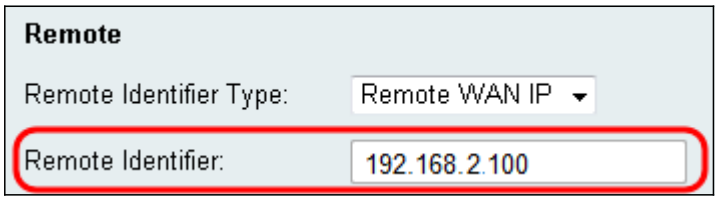


Le opzioni disponibili sono definite come segue:

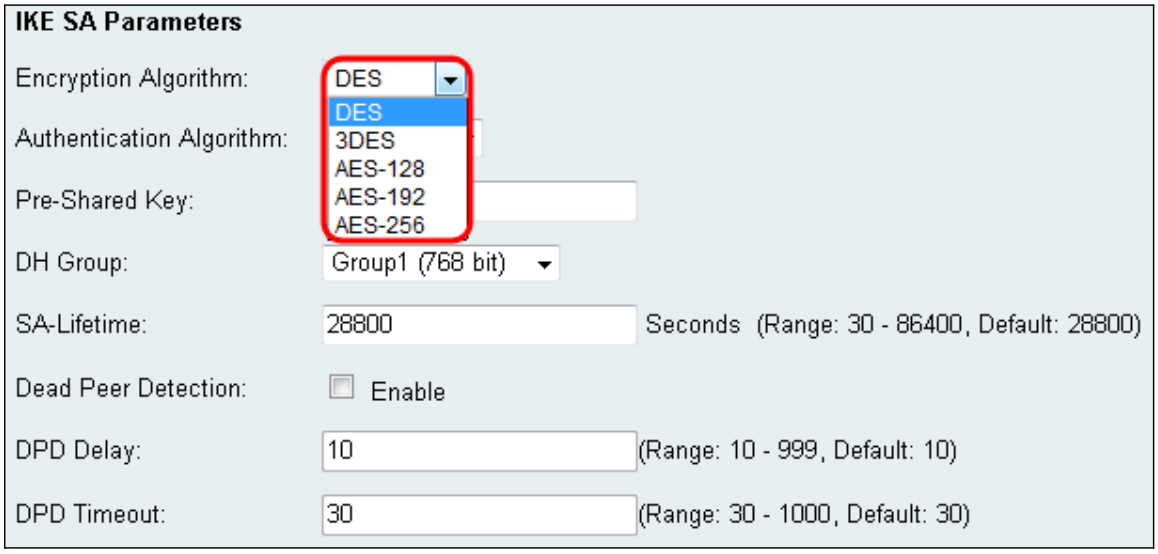
·IP WAN locale (Internet): connessione tramite Internet.

·Indirizzo IP: stringa univoca di numeri separati da punti che identifica ogni computer che utilizza il protocollo Internet per comunicare in rete.

Passaggio 8. (Facoltativo) Se **Indirizzo IP** è selezionato dall'elenco a discesa nel Passaggio 7, immettere l'indirizzo IP remoto nel campo *Identificatore remoto*.



Passaggio 9. Dal menu a discesa *Algoritmo di crittografia*, scegliere un algoritmo per crittografare le comunicazioni. **AES-128** è scelto come predefinito.



Le opzioni disponibili sono elencate come segue, a partire dalla protezione minima alla massima:

·DES: standard per la crittografia dei dati.

·3DES: standard per la crittografia tripla dei dati.

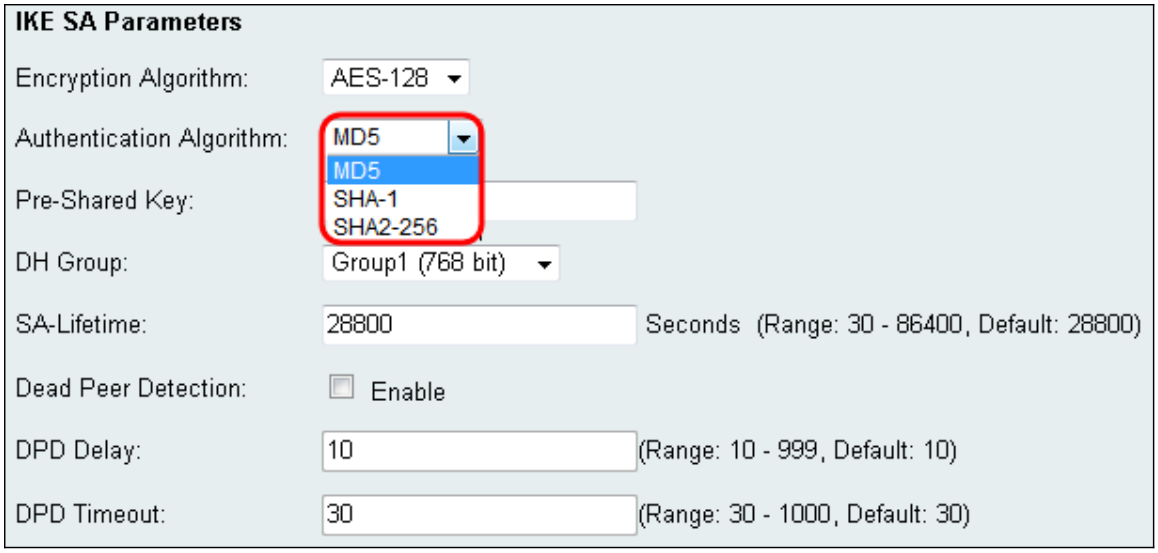
·AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit.

·AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.

·AES-256 - Advanced Encryption Standard utilizza una chiave a 256 bit.

Nota: AES è il metodo standard di crittografia su DES e 3DES per prestazioni e sicurezza più elevate. L'aumento della lunghezza della chiave AES aumenta la sicurezza con un calo delle prestazioni. Si consiglia l'AES-128 perché offre il miglior compromesso tra velocità e sicurezza.

Passaggio 10. Dal menu a discesa *Algoritmo di autenticazione*, scegliere un algoritmo per autenticare le comunicazioni. **SHA-1** è scelto come predefinito.



Le opzioni disponibili sono definite come segue:

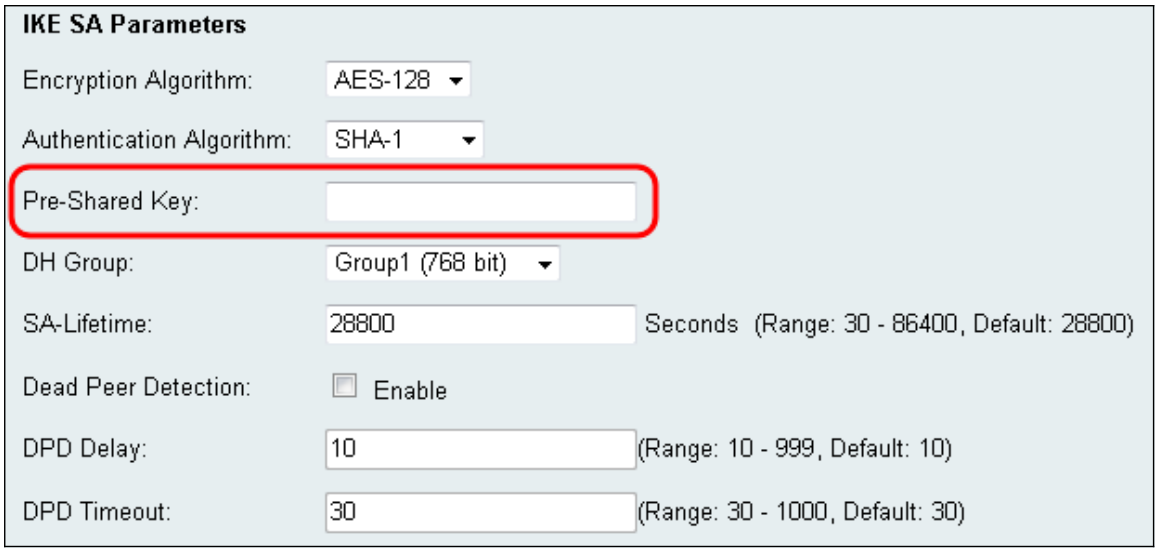
·MD5 — Message Digest Algorithm ha un valore hash di 128 bit.

·SHA-1: Secure Hash Algorithm ha un valore hash di 160 bit.

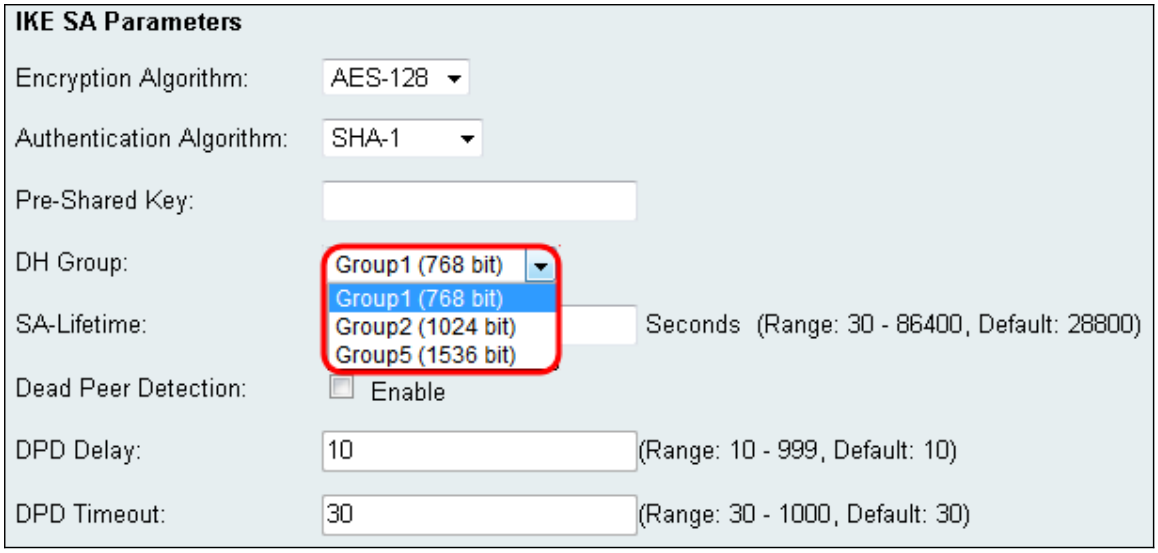
·SHA2-256: algoritmo hash sicuro con valore hash a 256 bit.

Nota: MD5 e SHA sono entrambe funzioni hash crittografiche. Prendono un dato, lo compattano e creano un output esadecimale unico che in genere non è riproducibile. MD5 non fornisce essenzialmente alcuna protezione contro le collisioni di hashing e deve essere utilizzato solo in ambienti di piccole imprese in cui non è necessaria la resistenza alle collisioni. SHA1 è una scelta migliore rispetto a MD5 perché offre una maggiore sicurezza a velocità sensibilmente più lente. Per ottenere i migliori risultati, SHA2-256 non ha attacchi noti di rilevanza pratica e offrirà la migliore sicurezza. Come accennato in precedenza, maggiore sicurezza significa velocità più lente.

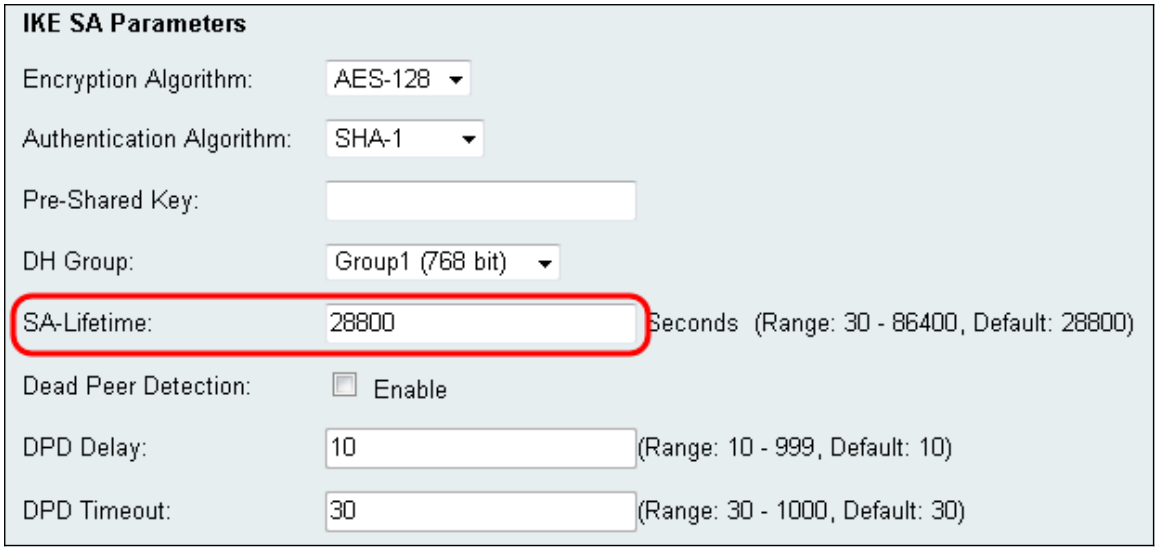
Passaggio 11. Nel campo *Chiave già condivisa*, immettere una password con una lunghezza compresa tra 8 e 49 caratteri.



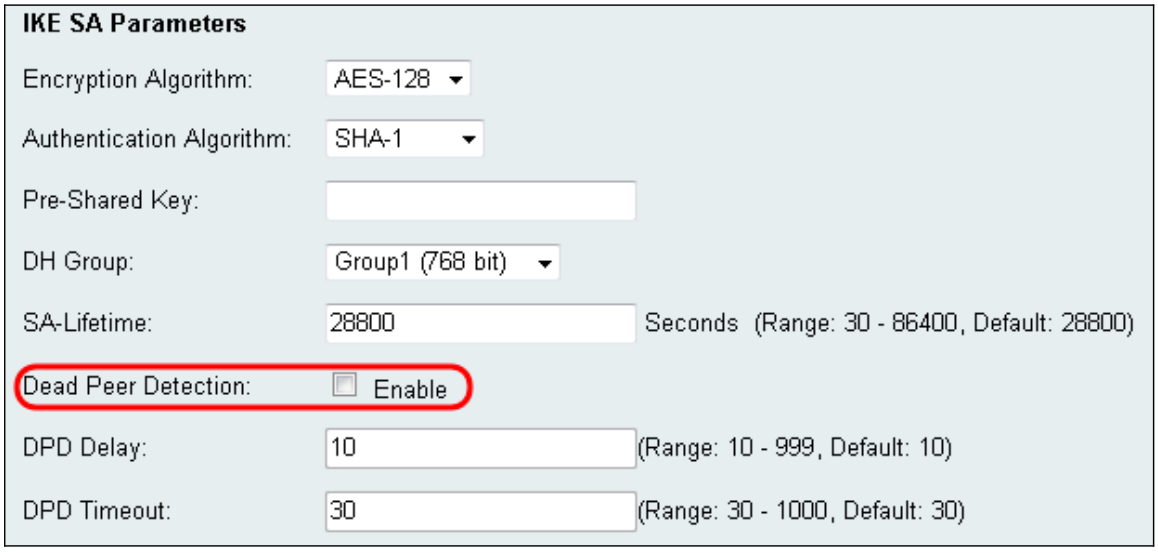
Passaggio 12. Dal menu a discesa *Gruppo DH*, scegliere un gruppo DH. Il numero di bit indica il livello di sicurezza. Entrambe le estremità della connessione devono trovarsi nello stesso gruppo.



Passaggio 13. Nel campo *Durata SA* immettere per quanto tempo l'associazione di sicurezza sarà valida in secondi. L'impostazione predefinita è 28800 secondi.

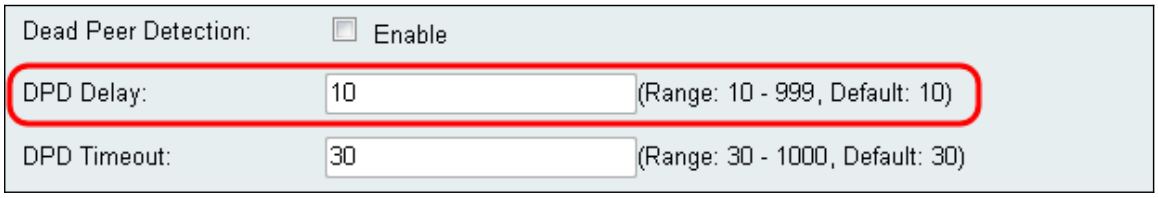


Passaggio 14. (Facoltativo) Selezionare la casella di controllo **Abilita** nel campo *Dead Peer Detection* (Rilevamento peer inattivo) se si desidera disabilitare una connessione con un peer inattivo. Andare al passaggio 17 se non è stato abilitato Dead Peer Detection.



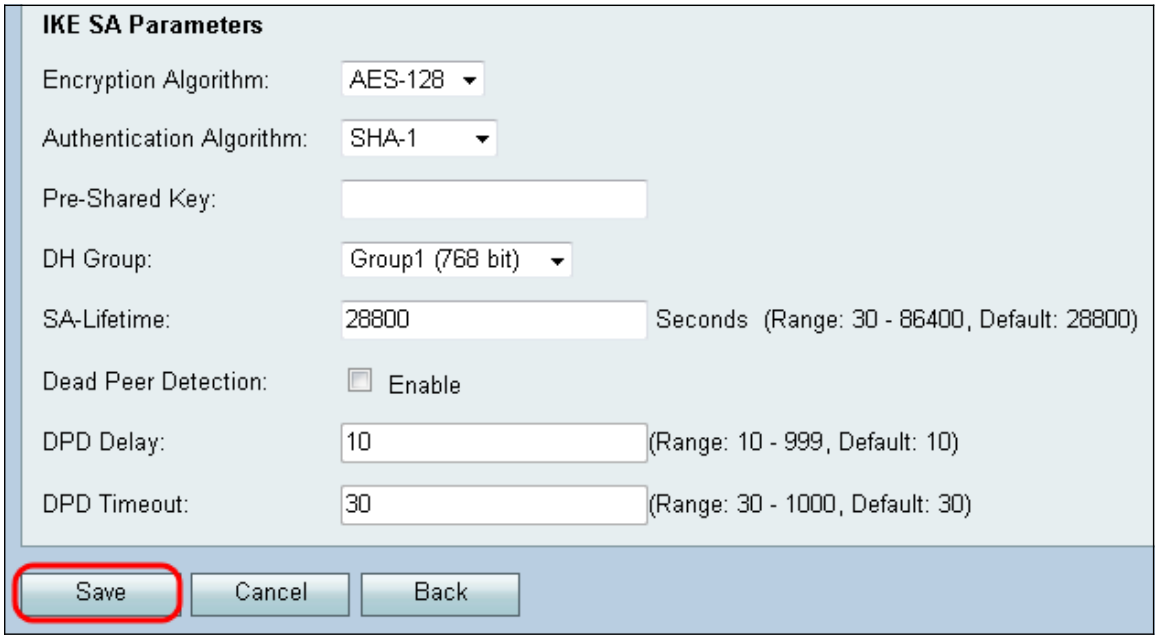
Passaggio 15. (Facoltativo) Se è stato abilitato Dead Peer Detection, immettere un valore

nel campo *DPD Delay*. Questo valore specifica il tempo di attesa del router per il controllo della connettività client.



Passaggio 16. (Facoltativo) Se è stato abilitato Dead Peer Detection, immettere un valore nel campo *Timeout DPD*. Questo valore specifica per quanto tempo il client rimarrà connesso fino al timeout.

Passaggio 17. Fare clic su **Salva** per salvare le modifiche.



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).