Configurazione dei profili IPSec (modalità di impostazione automatica della trasparenza) sugli switch RV160 e RV260

Obiettivo

In questo documento viene spiegato come creare un nuovo profilo IPsec (Internet Protocol Security) con la modalità di impostazione automatica delle chiavi sui router serie RV160 e RV260.

Introduzione

IPsec garantisce comunicazioni private protette su Internet. Offre a due o più host privacy, integrità e autenticità per la trasmissione di informazioni riservate su Internet. IPsec viene comunemente utilizzato nelle reti VPN (Virtual Private Network) e viene implementato a livello IP e può essere utilizzato per supportare molte applicazioni non sicure. Una VPN viene utilizzata per fornire un meccanismo di comunicazione sicuro per dati sensibili e informazioni IP trasmesse tramite una rete non protetta, ad esempio Internet. Offre una soluzione flessibile per gli utenti remoti e l'organizzazione per proteggere le informazioni riservate da altre parti sulla stessa rete.

Affinché le due estremità di un tunnel VPN possano essere crittografate e stabilite correttamente, entrambe devono concordare i metodi di crittografia, decrittografia e autenticazione. Il profilo IPsec è la configurazione centrale di IPsec che definisce algoritmi quali la crittografia, l'autenticazione e il gruppo Diffie-Hellman (DH) per la negoziazione nelle fasi I e II in modalità automatica e in modalità di generazione manuale delle chiavi. La fase 1 stabilisce le chiavi già condivise per creare una comunicazione autenticata sicura. La fase 2 prevede la crittografia del traffico. È possibile configurare la maggior parte dei parametri IPSec, ad esempio protocollo, modalità, algoritmo, PFS (Perfect Forward Secrecy), durata associazione di sicurezza (SA, Security Association) e protocollo di gestione delle chiavi.

Quando si configura la VPN da sito a sito, il router remoto deve avere le stesse impostazioni di profilo del router locale.

Ulteriori informazioni sulla tecnologia Cisco IPsec sono disponibili in questo collegamento: Introduzione alla tecnologia Cisco IPSec.

Per configurare il profilo IPsec e la VPN da sito a sito utilizzando la Configurazione guidata VPN, fare clic sul collegamento: Configurazione della Configurazione guidata VPN su RV160 e RV260.

Per configurare la VPN da sito a sito, vedere il documento: Configurazione della VPN da sito a sito sugli switch RV160 e RV260.

Dispositivi interessati

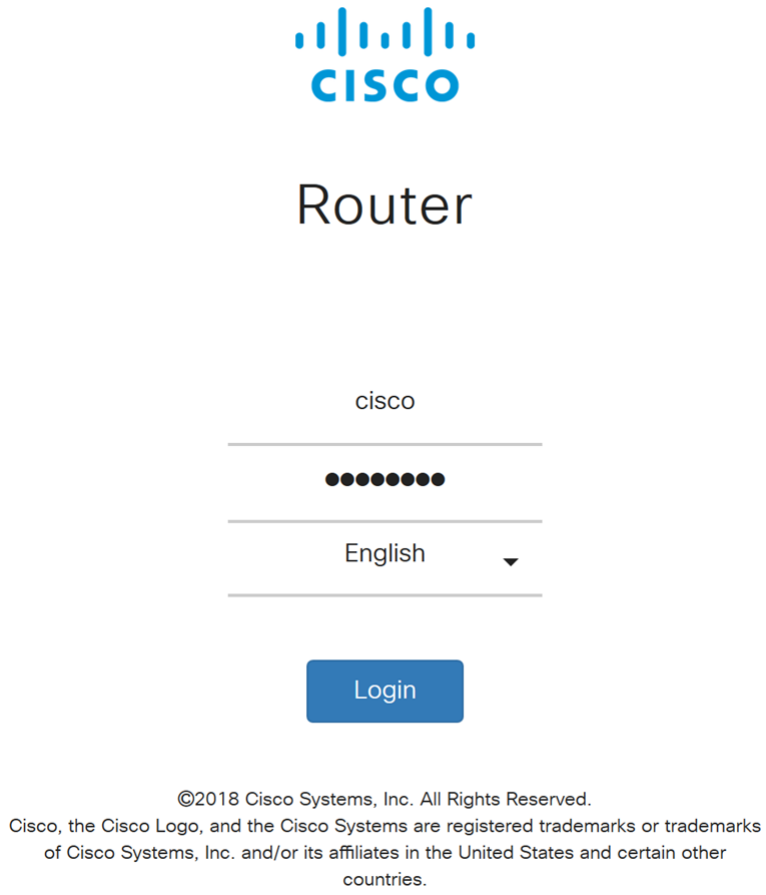
- RV160
- RV260

Versione del software

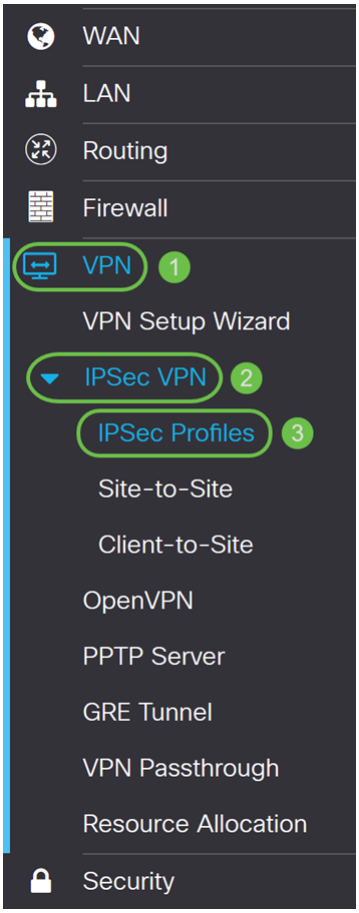
- 1.0.00.13

Configurazione dei profili IPsec

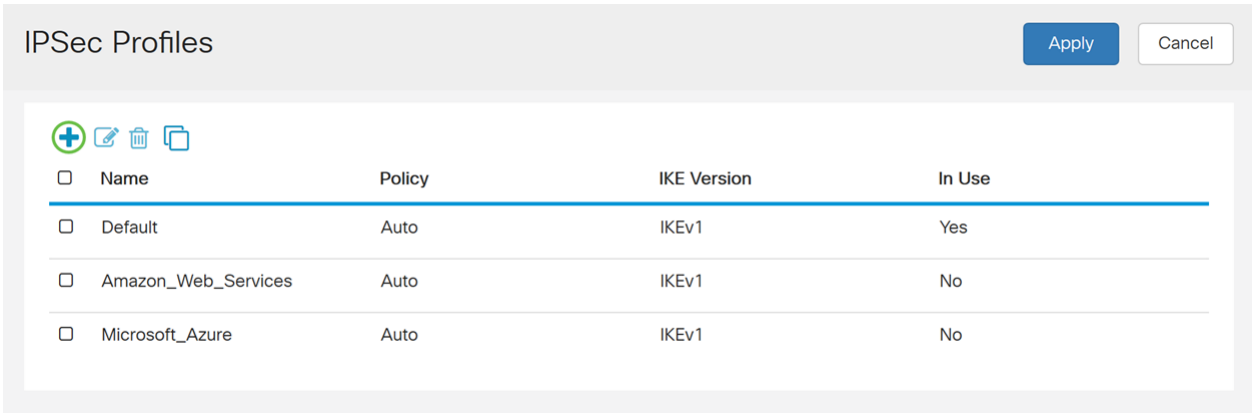
Passaggio 1. Accedere alla pagina di configurazione Web sul router.



Passaggio 2. Passare a **VPN > VPN IPSec > Profili IPSec**.



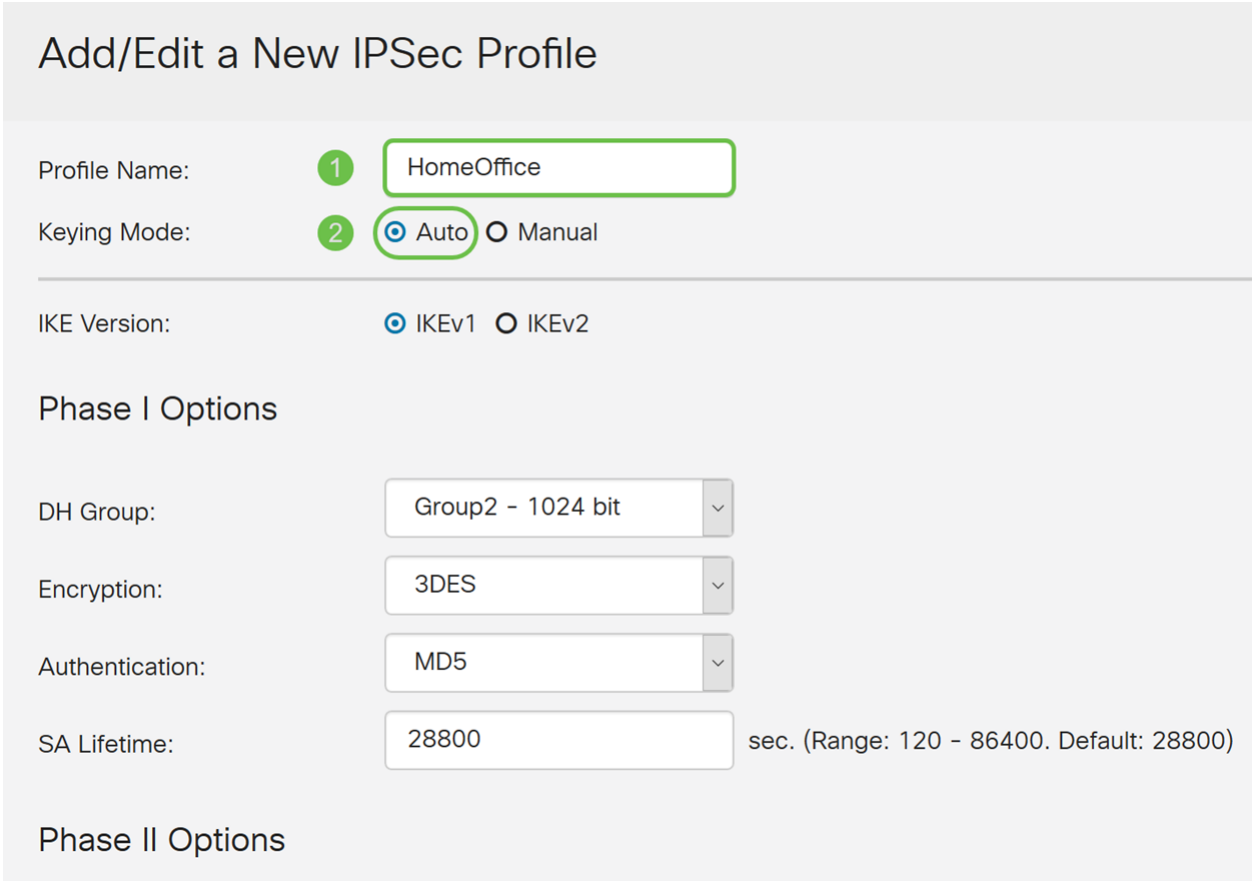
Passaggio 3. Nella tabella *Profili IPSec*, fare clic su **Aggiungi** per creare un nuovo profilo IPSec. È inoltre possibile modificare, eliminare o clonare un profilo.



Passaggio 4. Inserire un nome di profilo e selezionare la modalità di applicazione della chiave (Automatica o Manuale).

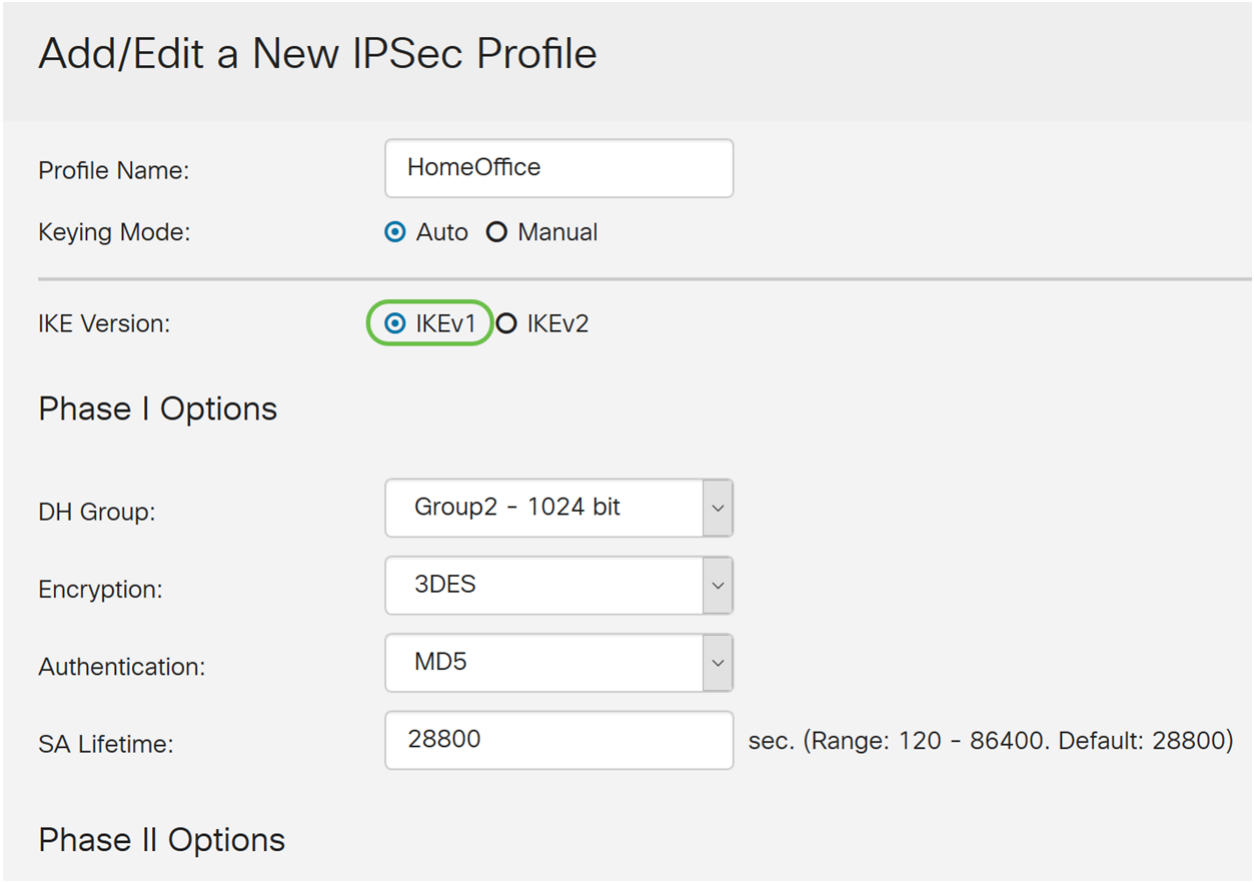
HomeOffice viene immesso come *Nome profilo*.

Auto è selezionato per la *modalità trasparenza*.



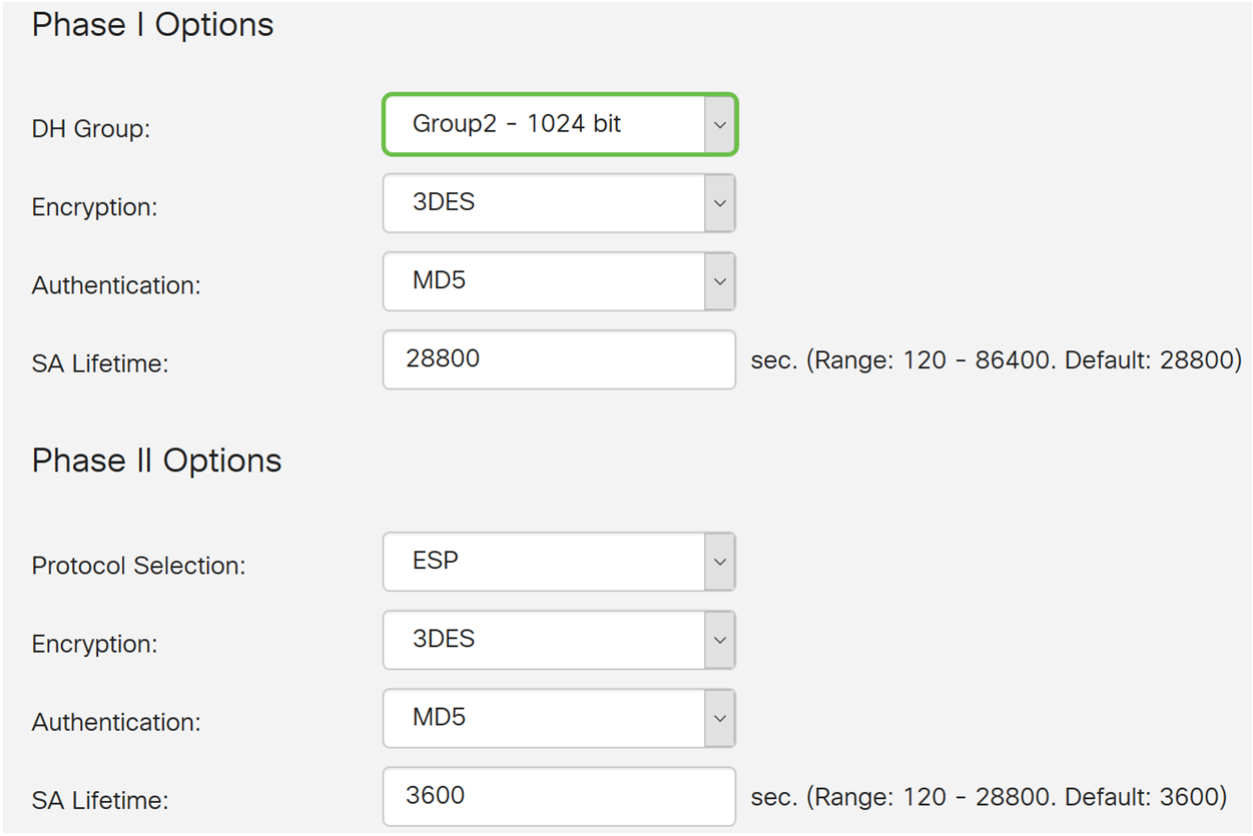
Passaggio 5. Scegliere *Internet Key Exchange versione 1* (*IKEv1)* o *Internet Key Exchange versione 2 (IKEv2)* come versione IKE. IKE è un protocollo ibrido che implementa lo scambio di chiavi Oakley e Skeme all'interno della struttura ISAKMP (Internet Security Association and Key Management Protocol). Oakley e Skeme definiscono entrambi come derivare il materiale per le chiavi autenticato, ma Skeme include anche un rapido aggiornamento delle chiavi. IKE fornisce l'autenticazione dei peer IPSec, negozia le chiavi IPSec e le associazioni di protezione IPSec. IKEv2 è più efficiente perché richiede meno pacchetti per lo scambio di chiavi, supporta più opzioni di autenticazione, mentre IKEv1 esegue solo l'autenticazione basata su chiave condivisa e certificati. Nell'esempio, **IKEv1** è stato selezionato come versione IKE.

Nota: Se il dispositivo supporta IKEv2, è consigliabile utilizzare IKEv2. Se il dispositivo non supporta IKEv2, utilizzare IKEv1.



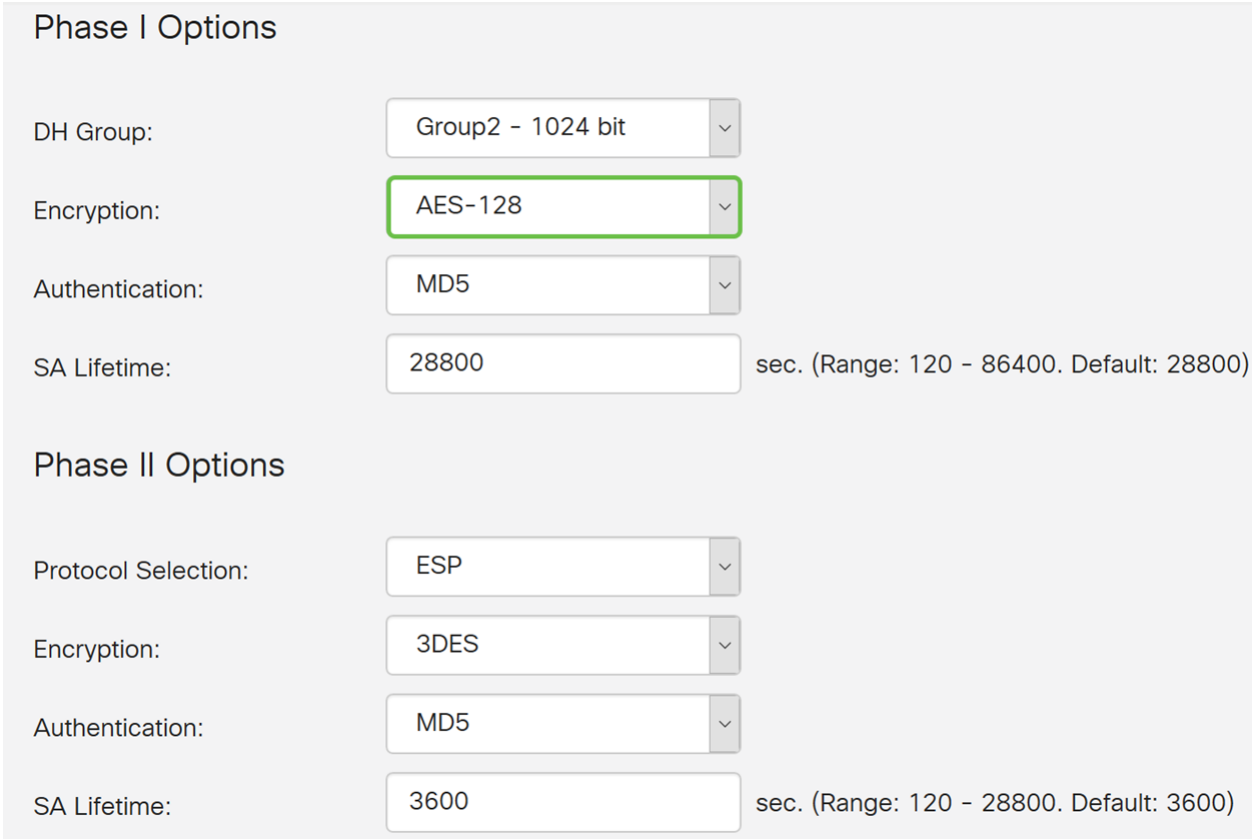
Passaggio 6. La fase I configura e scambia le chiavi che verranno utilizzate per crittografare i dati nella fase II. Nella sezione *Fase I* , selezionare un gruppo Diffie-Hellman (DH). DH è un protocollo di scambio di chiavi, con due gruppi di diverse lunghezze di chiavi primarie, **Gruppo 2 - 1024 bit** e **Gruppo 5 - 1536 bit**. Per questa dimostrazione, abbiamo selezionato **Gruppo 2 - 1024 bit**.

Nota: Per velocizzare le operazioni e ridurre la protezione, scegliere Gruppo 2. Per velocità più lente e maggiore protezione, scegliere Gruppo 5. Gruppo 2 è selezionato come predefinito.



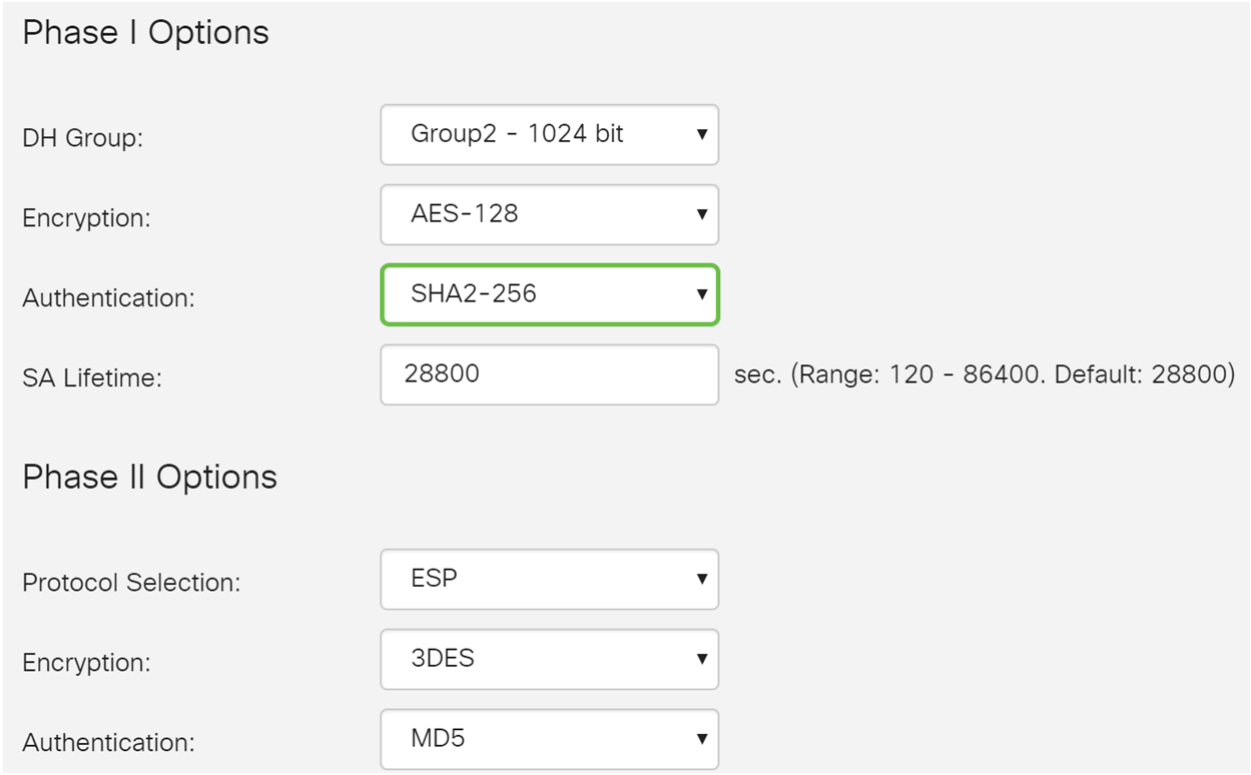
Passaggio 7. Selezionare un'opzione di crittografia (**3DES**, **AES-128**, **AES-192** o **AES-256**) dall'elenco a discesa. Questo metodo determina l'algoritmo utilizzato per crittografare e decrittografare i pacchetti ESP/ISAKMP. Triple Data Encryption Standard (3DES) utilizza la crittografia DES tre volte, ma è ora un algoritmo legacy. Ciò significa che dovrebbe essere utilizzato solo quando non ci sono alternative migliori, in quanto fornisce ancora un livello di sicurezza marginale ma accettabile. Gli utenti dovrebbero utilizzarlo solo se necessario per la compatibilità con le versioni precedenti, in quanto è vulnerabile ad attacchi di tipo "collisione di blocco". Non è consigliabile utilizzare 3DES in quanto non è considerato sicuro. Advanced Encryption Standard (AES) è un algoritmo di crittografia progettato per essere più sicuro di DES. AES utilizza una chiave di dimensioni maggiori che garantisce che l'unico approccio noto per decrittografare un messaggio sia che un intruso possa provare tutte le chiavi possibili. Se il dispositivo in uso è in grado di supportarlo, si consiglia di utilizzare l'AES. Nell'esempio, abbiamo selezionato **AES-128** come opzione di crittografia.

Nota: Di seguito sono riportate alcune risorse aggiuntive che possono essere utili: Configurazione della sicurezza per le VPN con crittografia IPsec e di nuova generazione.



Passaggio 8. Il metodo di autenticazione determina la modalità di convalida dei pacchetti di intestazione ESP. Questo è l'algoritmo di hashing usato nell'autenticazione per convalidare che il lato A e il lato B sono realmente ciò che dicono di essere. MD5 è un algoritmo di hashing unidirezionale che produce un digest a 128 bit ed è più veloce di SHA1. SHA1 è un algoritmo di hashing unidirezionale che produce un digest a 160 bit, mentre SHA2-256 produce un digest a 256 bit. SHA2-256 è consigliato perché più sicuro. Verificare che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione. Selezionare un'autenticazione (**MD5, SHA1** o **SHA2-256**).

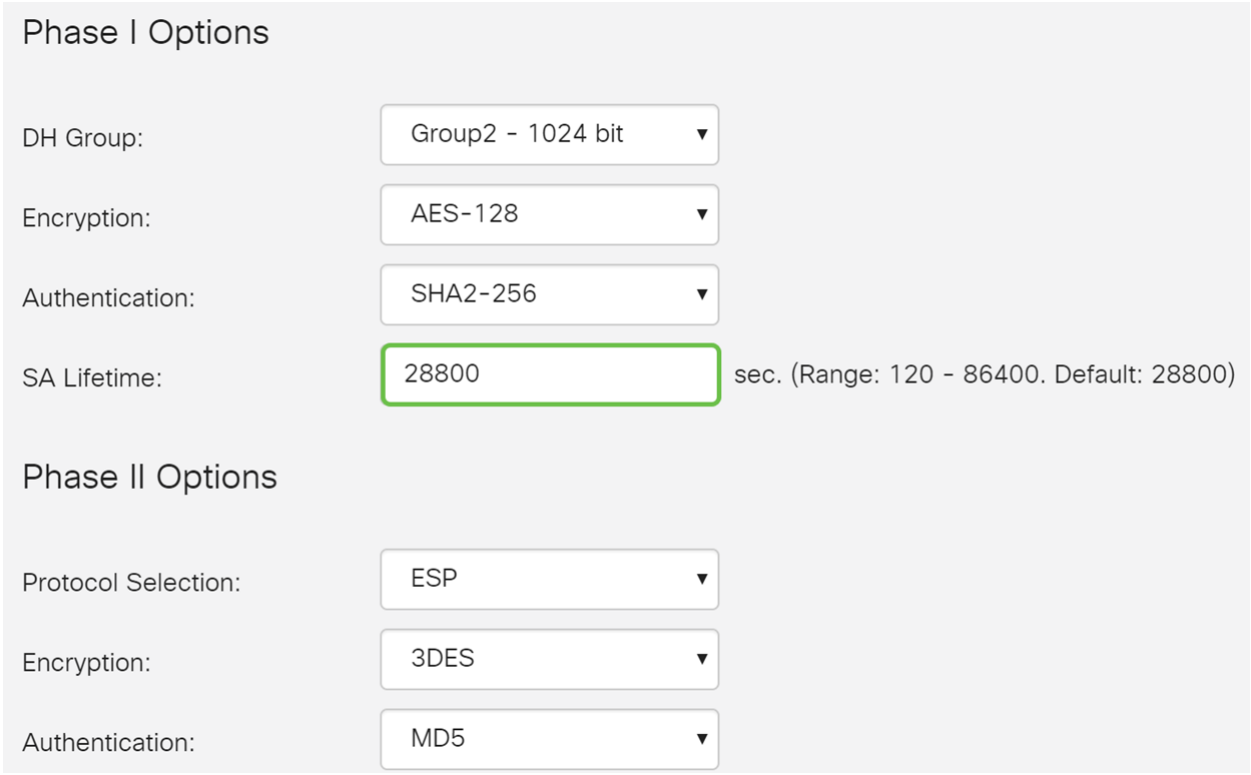
Per questo esempio è stato selezionato **SHA2-256**.



Passaggio 9. La *durata dell'associazione di protezione (sec)* indica la quantità di tempo durante la quale un'associazione di protezione IKE è attiva in questa fase. Quando l'associazione di protezione scade dopo la rispettiva durata, viene avviata una nuova negoziazione per una nuova associazione. L'intervallo è compreso tra 120 e 86400 e il valore predefinito è 28800.

Per la Fase I verrà utilizzato il valore predefinito di **2800** secondi.

Nota: Si consiglia che la durata dell'ASA nella Fase I sia maggiore della durata dell'ASA nella Fase II. Se si rende la Fase I più breve della Fase II, sarà necessario rinegoziare il tunnel frequentemente in senso inverso rispetto al tunnel di dati. Il tunnel dei dati è ciò che richiede maggiore sicurezza, quindi è meglio avere una durata di vita inferiore nella Fase II rispetto alla Fase I.

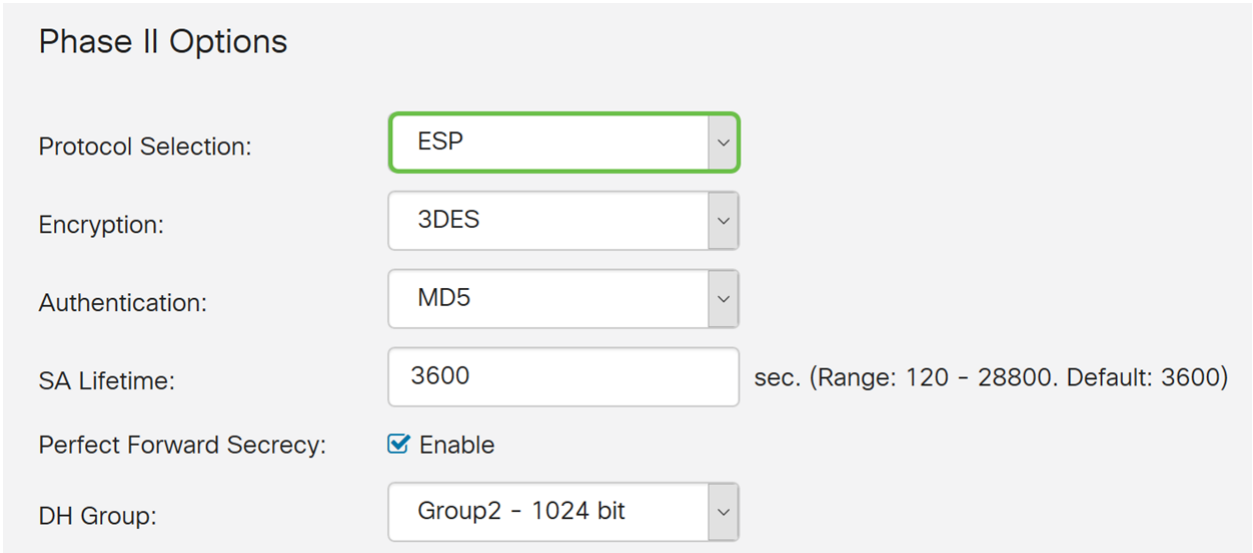


Passaggio 10. La fase II prevede la crittografia dei dati trasmessi. Nell'elenco a discesa *Phase 2 Options* (Opzioni fase 2), Select a protocol (Seleziona un protocollo), le opzioni sono:

- Encapsulating Security Payload (ESP): selezionare ESP per la crittografia dei dati e immettere la crittografia.

- AH (Authentication Header): selezionare questa opzione per garantire l'integrità dei dati quando i dati non sono segreti, ovvero non sono crittografati ma devono essere autenticati. Viene usata solo per convalidare l'origine e la destinazione del traffico.

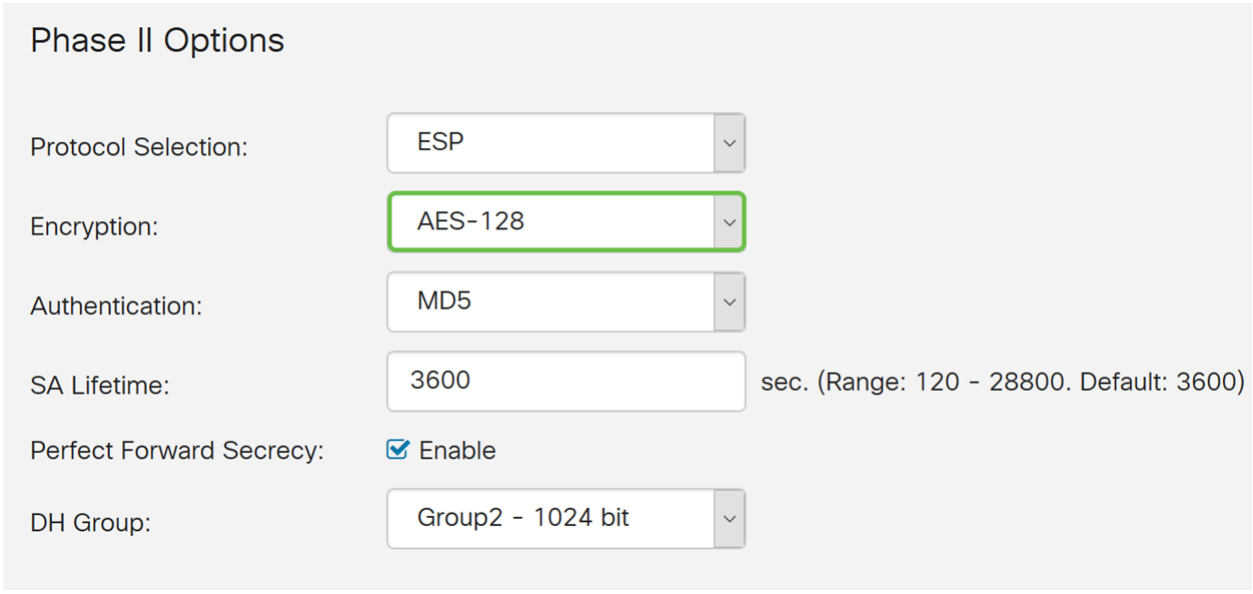
In questo esempio verrà utilizzato **ESP** come *selezione del protocollo*.



Passaggio 11. Selezionare un'opzione di crittografia (**3DES**, **AES-128**, **AES-192** o **AES-256**) dall'elenco a discesa. Questo metodo determina l'algoritmo utilizzato per crittografare e decrittografare i pacchetti ESP/ISAKMP.

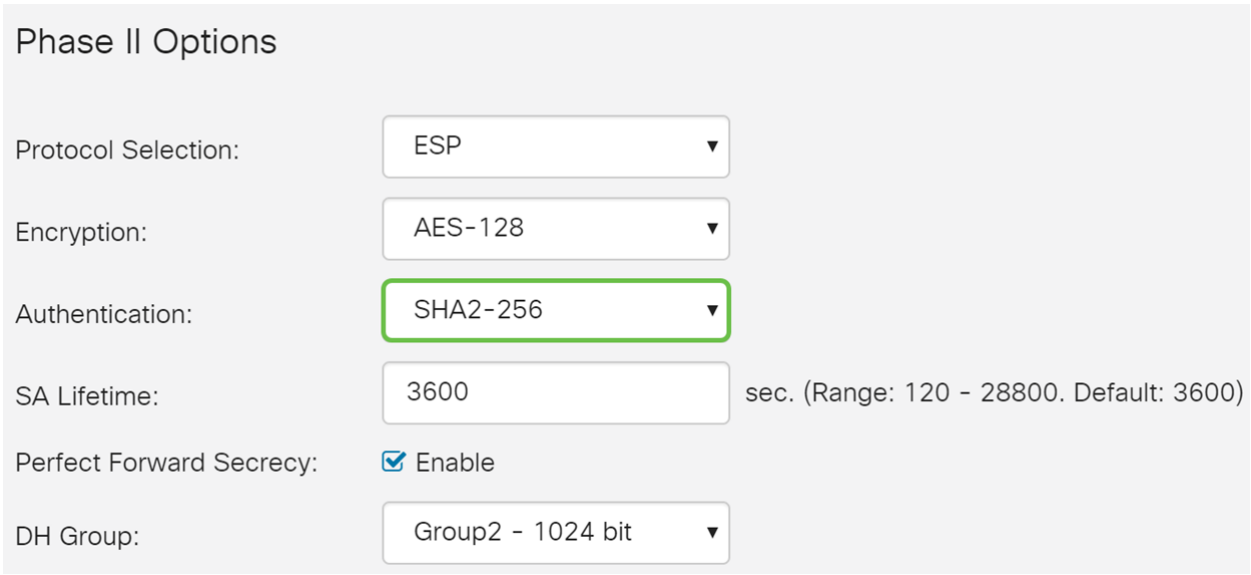
Nell'esempio, utilizzeremo **AES-128** come opzione di crittografia.

Nota: Di seguito sono riportate alcune risorse aggiuntive che possono essere utili: Configurazione della sicurezza per le VPN con crittografia IPsec e di nuova generazione.

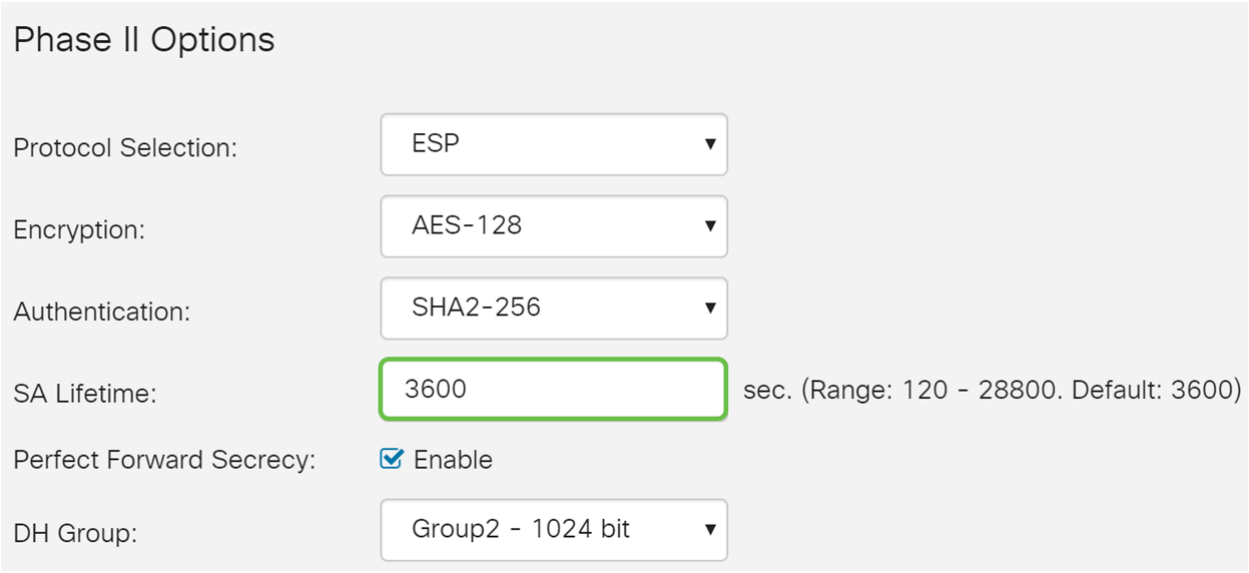


Passaggio 12. Il metodo di autenticazione determina la modalità di convalida dei pacchetti di intestazione Encapsulating Security Payload Protocol (ESP). Selezionare un'autenticazione (**MD5, SHA1** o **SHA2-256**).

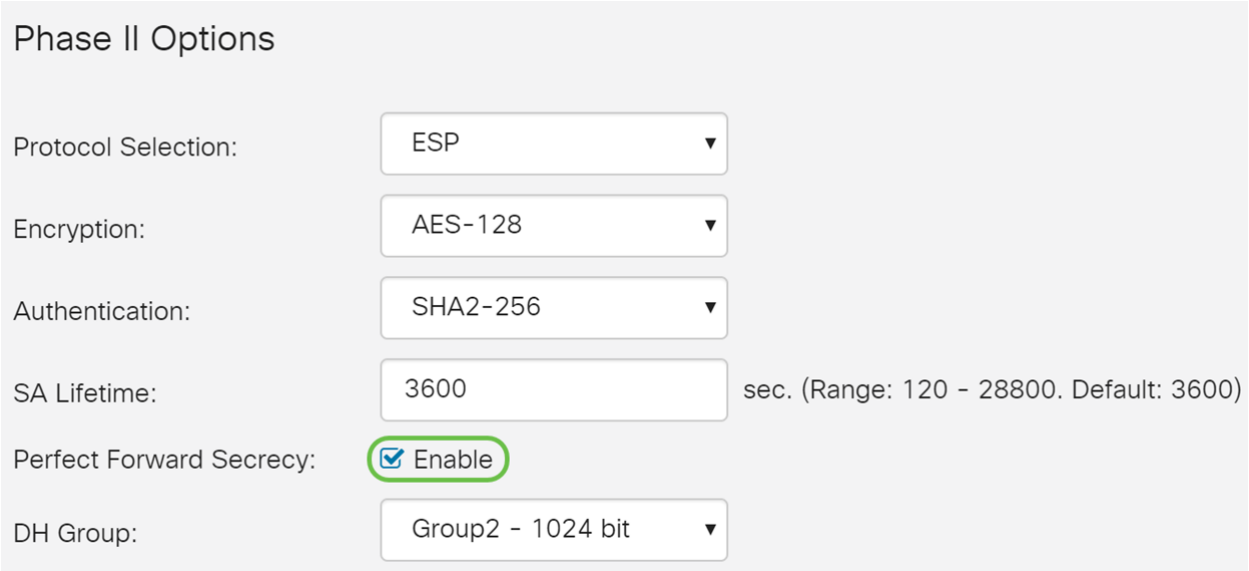
Per questo esempio è stato selezionato **SHA2-256**.



Passaggio 13. Immettere il periodo di tempo durante il quale un tunnel VPN (SA IPsec) è attivo in questa fase. Il valore predefinito per la Fase 2 è 3600 secondi. Per questa dimostrazione verrà utilizzato il valore predefinito.

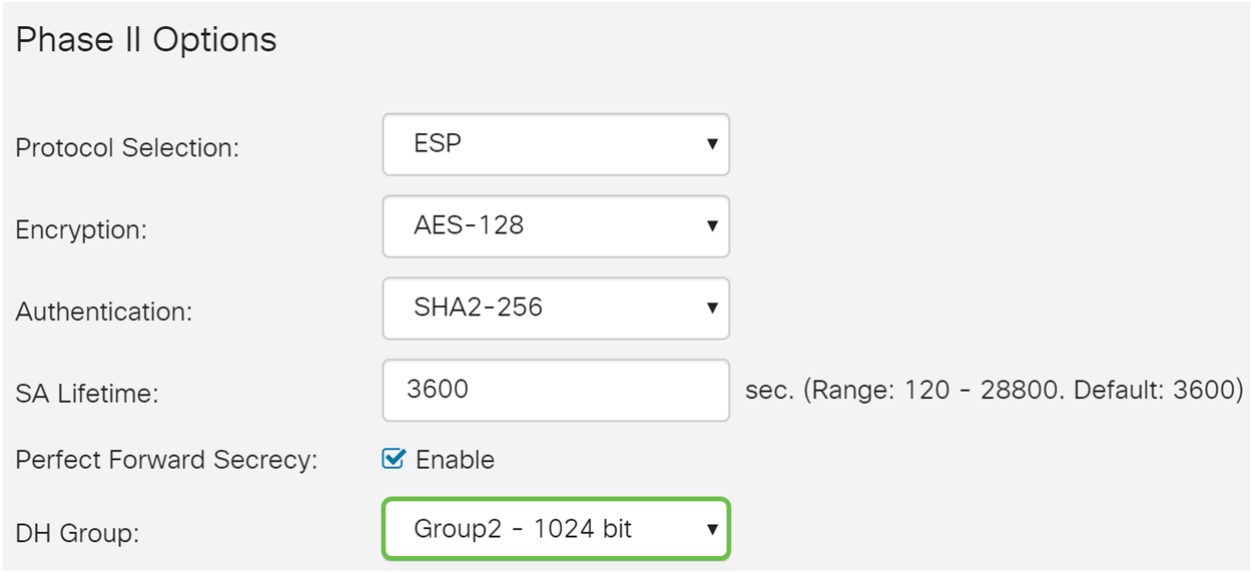


Passaggio 14. Selezionare **Abilita** per abilitare la segretezza di inoltro perfetta. Quando PFS (Perfect Forward Secrecy) è abilitato, la negoziazione IKE fase 2 genera nuovo materiale della chiave per la crittografia e l'autenticazione del traffico IPsec. PFS è utilizzato per migliorare la sicurezza delle comunicazioni trasmesse tramite Internet utilizzando la crittografia a chiave pubblica. Questa opzione è consigliata se il dispositivo lo supporta.

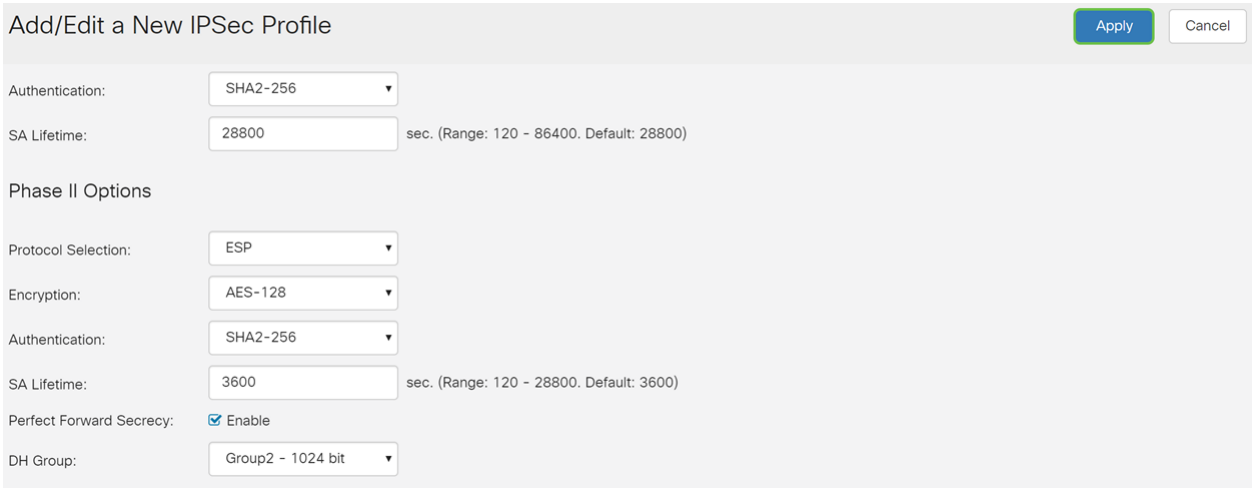


Passaggio 15. Selezionare un gruppo Diffie-Hellman (DH). DH è un protocollo di scambio di chiavi, con due gruppi di diverse lunghezze di chiavi primarie, **Gruppo 2 - 1024 bit** e **Gruppo 5 - 1536 bit**. Per questa dimostrazione, abbiamo selezionato **Gruppo 2 - 1024 bit**.

Nota: Per velocizzare le operazioni e ridurre la protezione, scegliere Gruppo 2. Per velocità più lente e maggiore protezione, scegliere Gruppo 5. Gruppo 2 è selezionato per impostazione predefinita.



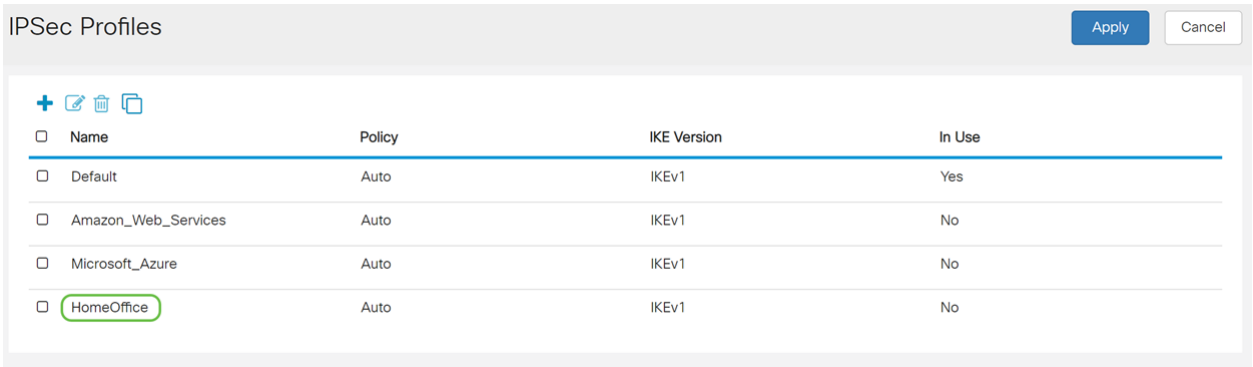
Passaggio 16. Fare clic su **Apply** (Applica) per aggiungere un nuovo profilo IPSec.



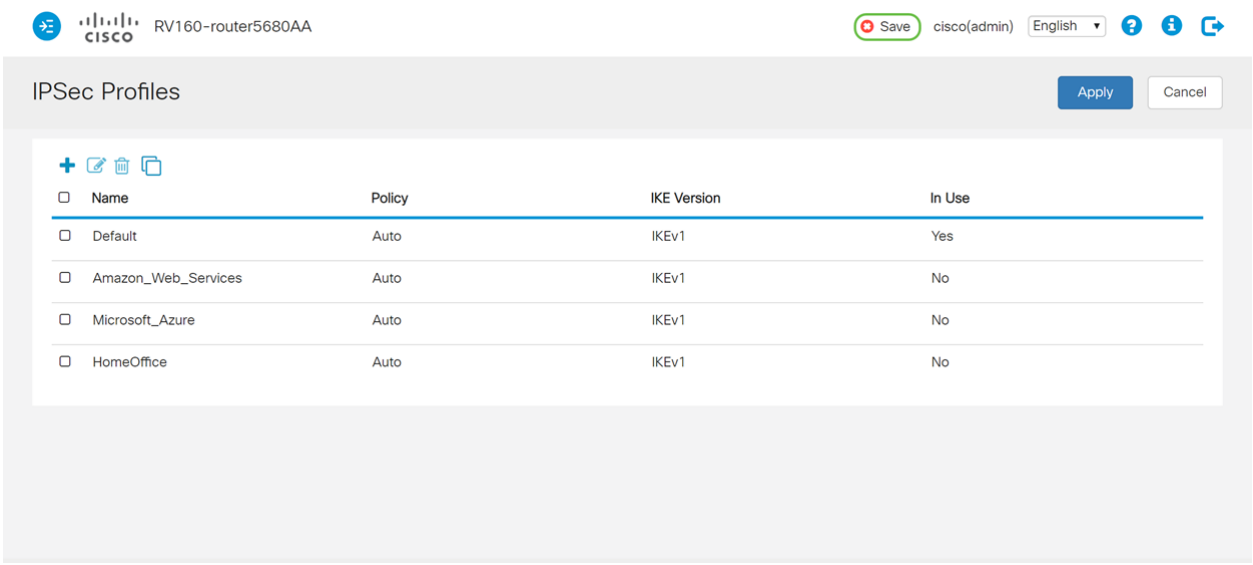
Conclusioni

Creazione del nuovo profilo IPSec completata. Continuare di seguito per verificare che il profilo IPsec sia stato aggiunto. È inoltre possibile eseguire la procedura per copiare il file della configurazione di esecuzione nel file della configurazione di avvio, in modo da mantenere tutta la configurazione tra un riavvio e l'altro.

Passaggio 1. Dopo aver fatto clic su *Apply*, viene aggiunto il nuovo profilo IPSec.



Passaggio 2. Nella parte superiore della pagina, fare clic sul pulsante **Save** (Salva) per accedere a *Configuration Management* (Gestione configurazione) e salvare la configurazione in esecuzione nella configurazione di avvio. In questo modo, la configurazione viene conservata tra un riavvio e l'altro.



Passaggio 3. Nella gestione della configurazione, verificare che l'*origine* sia **Configurazione in esecuzione** e che la *destinazione* sia **Configurazione di avvio**. Quindi, premere **Apply** per salvare la configurazione in esecuzione nella configurazione di avvio. Tutta la configurazione attualmente in uso sul router si trova nel file della configurazione in esecuzione, che è volatile e non viene conservata tra un riavvio e l'altro. Se si copia il file della configurazione di esecuzione nel file della configurazione di avvio, tutte le configurazioni verranno mantenute tra un riavvio e l'altro.