Configurazione di IKEv2 sul router serie RV34x

Obiettivo

Lo scopo di questo documento è quello di mostrare come configurare il profilo IPsec con IKEv2 sui router serie RV34x.

Introduzione

Il firmware versione 1.0.02.16 per i router serie RV34x supporta ora Internet Key Exchange versione 2 (IKEv2) per VPN da sito a sito e da client a sito. 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). IKE fornisce l'autenticazione dei peer IPSec, negozia le chiavi IPSec e le associazioni di protezione IPSec.

IKEv2 utilizza ancora la porta UDP 500, ma sono state apportate alcune modifiche. La funzionalità DPD (Dead Peer Detection) viene gestita in modo diverso e ora è integrata. La negoziazione della Security Association (SA) è ridotta a 4 messaggi. Il nuovo aggiornamento supporta anche l'autenticazione EAP (Extensible Authentication Protocol), che ora può utilizzare un server AAA e la protezione Denial of Service.

Nella tabella seguente vengono illustrate ulteriormente le differenze tra IKEv1 e IKEv2

IKEv1	IKEv2
Negoziazione in due fasi SA (modalità principale e modalità aggressiva)	Negoziazione singola fase SA (semplificata)
	Supporto certificati locale/remoto
	Migliore gestione delle collisioni
	Meccanica di rigenerazione delle chiavi migliorata
	NAT traversal incorporato
	Supporto EAP per server AAA

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 in una rete VPN (Virtual Private Network) e viene implementato al livello IP, che contribuisce ad aggiungere sicurezza a 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 inoltre 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. Un 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 di Fase I e II in modalità automatica e in modalità di codifica manuale. La fase I stabilisce le chiavi già condivise per creare una comunicazione autenticata sicura. La fase II prevede la crittografia del traffico. È possibile configurare la maggior parte dei parametri IPSec, ad esempio il protocollo (ESP (Encapsulation Security Payload), l'intestazione AH (Authentication Header), la modalità (tunnel, trasporto), gli algoritmi (crittografia, integrità, Diffie-Hellman), PFS (Perfect Forward Secrecy), la durata SA e il protocollo di gestione delle chiavi (Internet Key Exchange (IKE) - IKEv1 e IKEv2).

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

È importante notare che quando si configura la VPN da sito a sito, il router remoto richiede la stessa configurazione del profilo IPsec del router locale.

Di seguito è riportata una tabella della configurazione del router locale e del router remoto. In questo documento, verrà configurata la porta locale con il router A.

Campi	Router locale (Router A)	Router remoto (Router B)
Nome profilo	Ufficio domestico	Ufficio remoto
Modalità trasparenza	Auto	Auto
Versione IKE	IKEv2	IKEv2
Opzioni fase I	**Opzioni fase I**	**Opzioni fase I**
Gruppo DH	Group2 - 1024 bit	Group2 - 1024 bit
Crittografia	AES-192	AES-192
Autenticazione	SHA2-256	SHA2-256
Durata SA	28800	28800
Opzioni fase II	**Opzioni fase II**	**Opzioni fase II**
Selezione protocollo	ESP	ESP
Crittografia	AES-192	AES-192
Autenticazione	SHA2-256	SHA2-256
Durata SA	3600	3600
Perfect Forward Secrecy	Attivato	Attivato
Gruppo DH	Group2 - 1024 bit	Group2 - 1024 bit

Per informazioni su come configurare la VPN da sito a sito sulla RV34x, fare clic sul collegamento: Configurazione della VPN da sito a sito sull'RV34x.

Dispositivi interessati

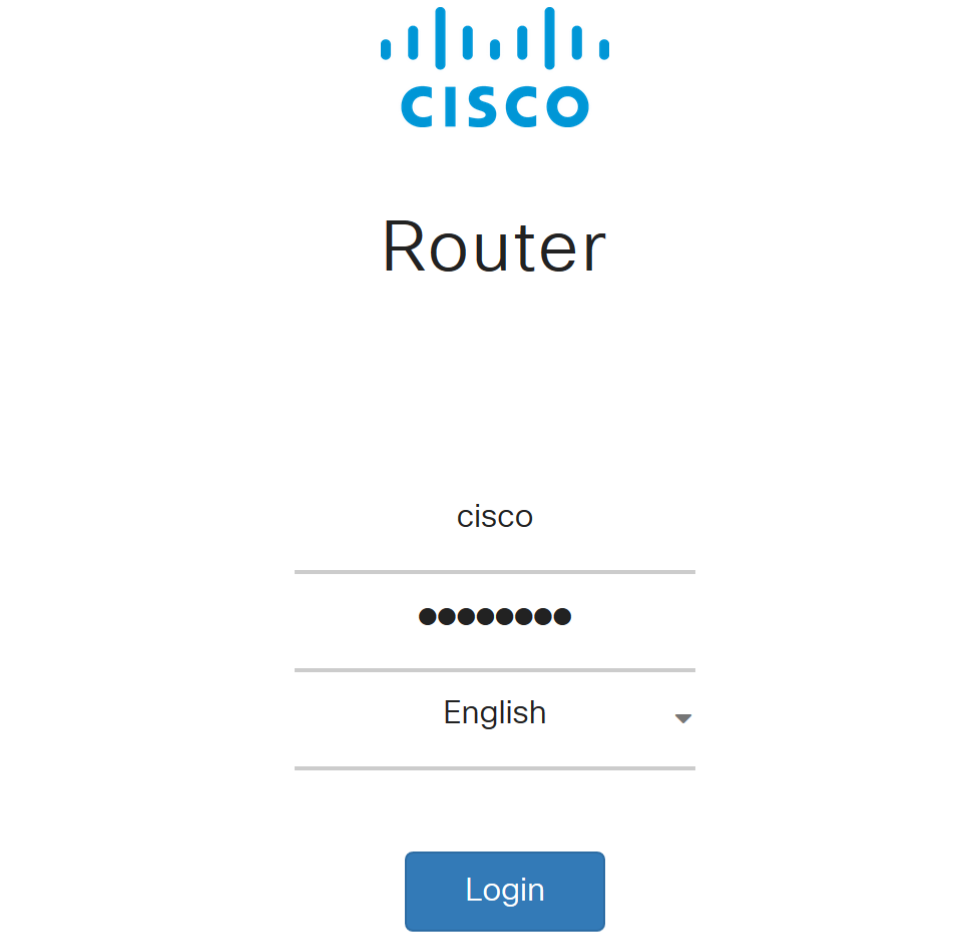
- RV34x

Versione del software

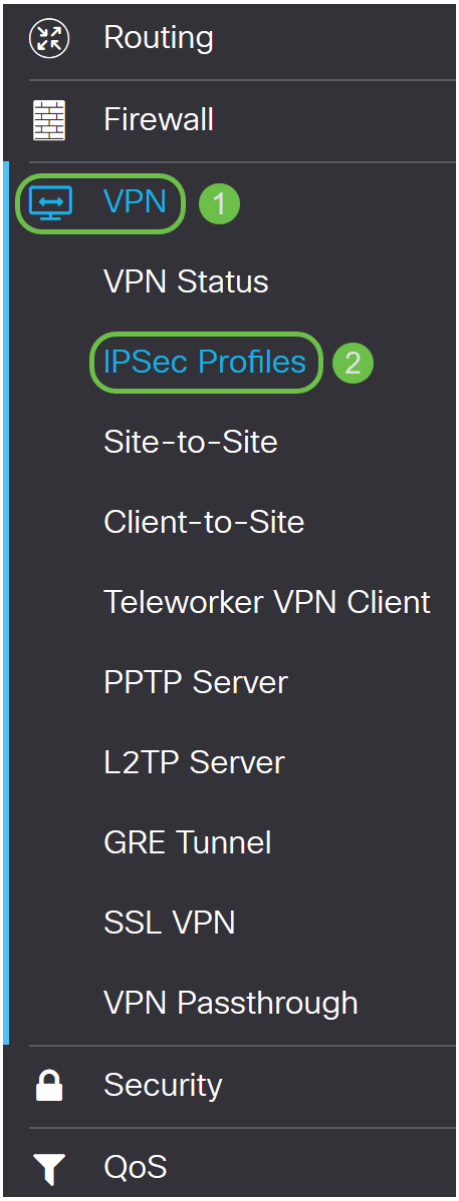
- 1.0.02.16

Configurazione del profilo IPsec con IKEv2

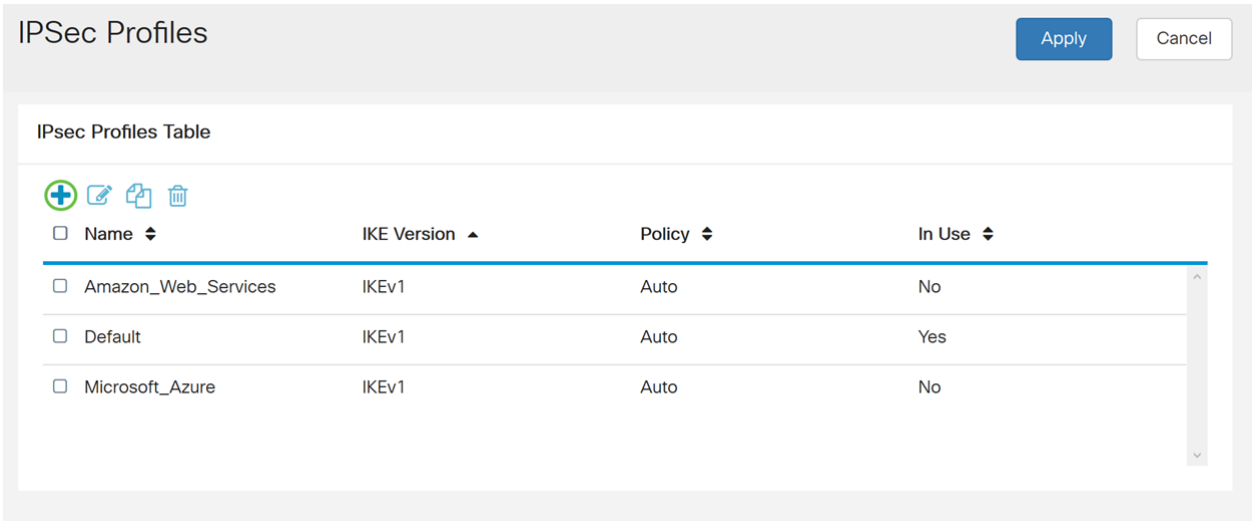
Passaggio 1. Accedere alla pagina di configurazione Web del router locale (Router A).



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



Passaggio 3. Nella tabella *Profili IPSec*, fare clic su **Aggiungi** per creare un nuovo profilo IPSec. Sono inoltre disponibili opzioni per modificare, eliminare o clonare un profilo. La clonazione di un profilo consente di duplicare rapidamente un profilo già esistente nella *tabella Profili IPSec*. Se è necessario creare più profili con la stessa configurazione, la duplicazione consente di risparmiare tempo.

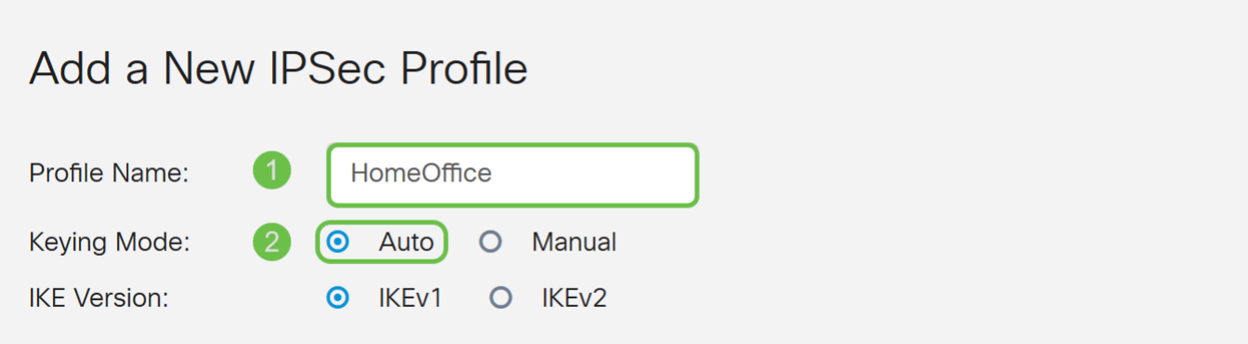


Passaggio 4. Inserire un nome di profilo e selezionare la modalità di applicazione della chiave

(Automatica o Manuale). Il nome del profilo non deve corrispondere all'altro router, ma la modalità di impostazione chiavi deve corrispondere.

HomeOffice viene immesso come *Nome profilo*.

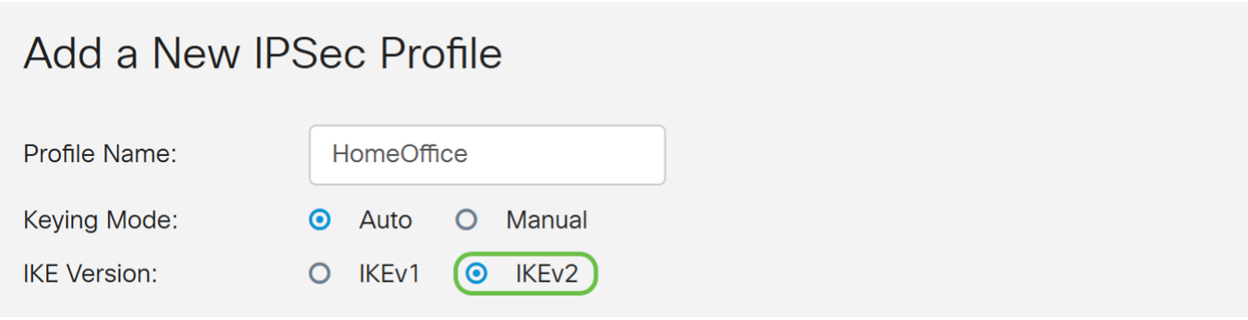
Auto è selezionato per la *modalità trasparenza*.



Passaggio 5. Scegliere **IKEv1** o **IKEv2** come *versione IKE*. IKE è un protocollo ibrido che implementa lo scambio di chiavi Oakley e Skeme nel framework ISAKMP. Oakley e Skeme definiscono entrambi come derivare il materiale per le chiavi autenticato, ma Skeme include anche un rapido aggiornamento delle chiavi. IKEv2 è più efficiente perché richiede meno pacchetti per lo scambio delle chiavi e supporta più opzioni di autenticazione, mentre IKEv1 esegue solo l'autenticazione basata su chiave condivisa e certificati.

Nell'esempio, **IKEv2** è stato selezionato come versione IKE.

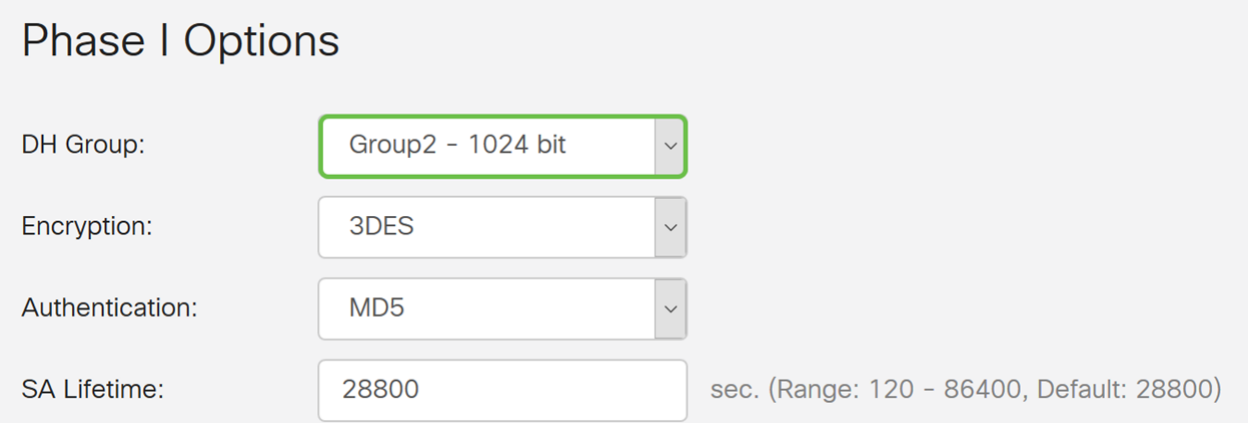
Nota: Se i dispositivi in uso supportano IKEv2, è consigliabile utilizzare IKEv2. Se i dispositivi in uso non supportano IKEv2, utilizzare IKEv1.



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 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 è stato selezionato il **gruppo 2 -** 1024 bit.

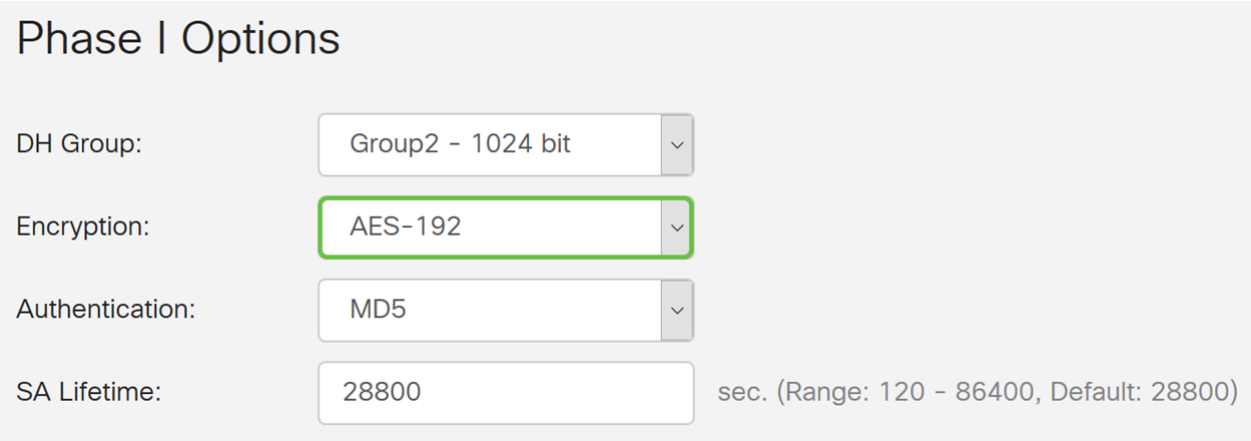
Nota: Per velocizzare le operazioni e ridurre la protezione, scegliere Gruppo 2. Per velocità più lente e maggiore protezione, scegliere Gruppo 5. Gruppo 2 è selezionato come predefinito.



Passaggio 7. Selezionare un'opzione di crittografia (**3DS, 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. Lo standard 3DES (Triple Data Encryption Standard) utilizza la crittografia DES tre volte, ma è ora un algoritmo legacy e dovrebbe essere utilizzato solo quando non esistono altre alternative, 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". 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.

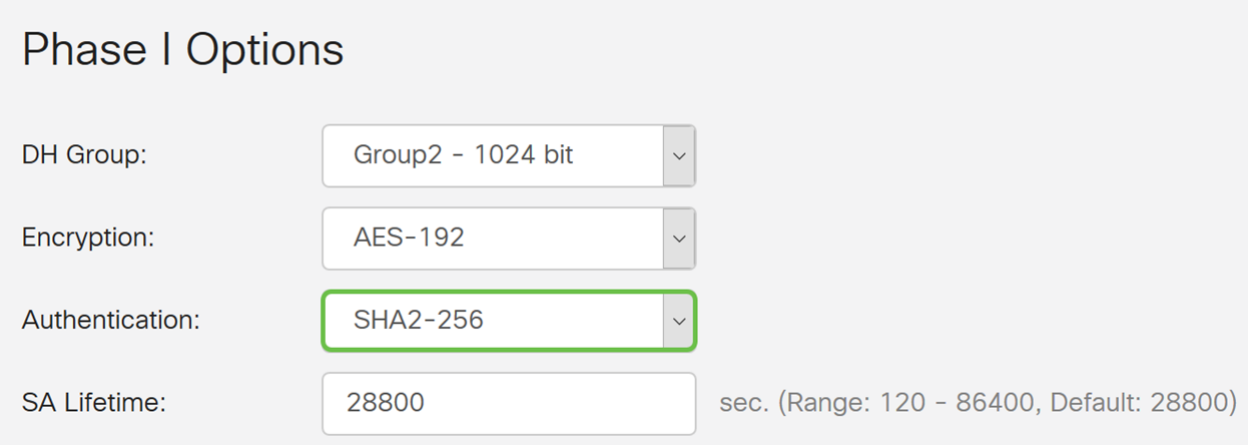
Nell'esempio, abbiamo selezionato **AES-192** come opzione di crittografia.

Nota: Fare clic sui collegamenti ipertestuali per ulteriori informazioni sulla configurazione della sicurezza per le VPN con IPsec o crittografia di nuova generazione.



Passaggio 8. Il metodo di autenticazione determina la modalità di convalida dei pacchetti dell'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**).

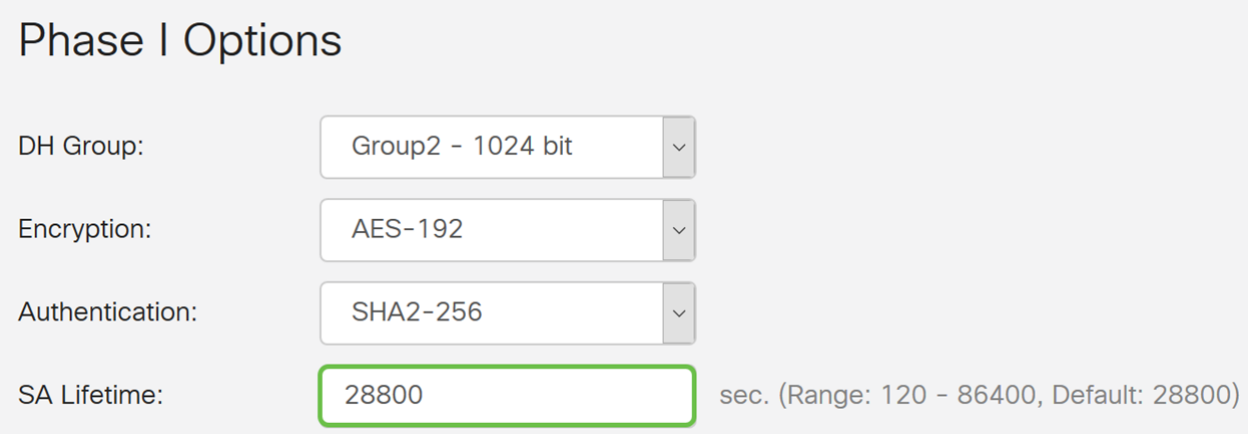
Per questo esempio è stato selezionato **SHA2-256**.



Passaggio 9. La *durata dell'associazione di protezione (sec)* indica la quantità di tempo durante la quale un'associazione di protezione IKE è attiva. 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.

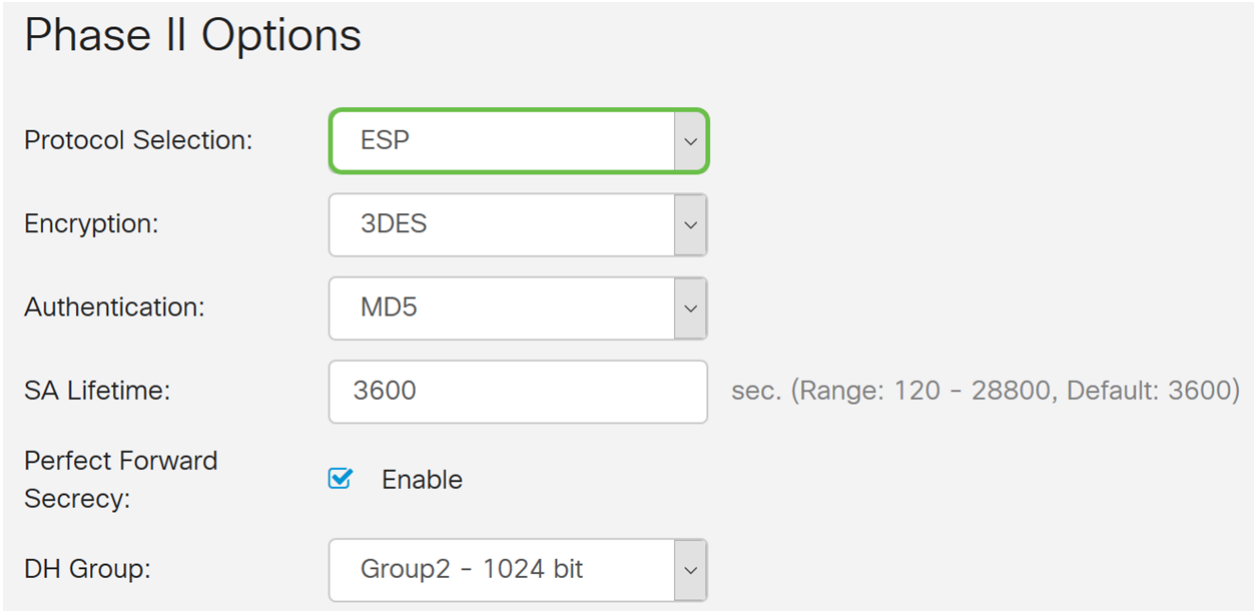


Passaggio 10. La fase II prevede la crittografia dei dati trasmessi. In *Opzioni fase 2*, selezionare un protocollo dall'elenco a discesa:

- 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.

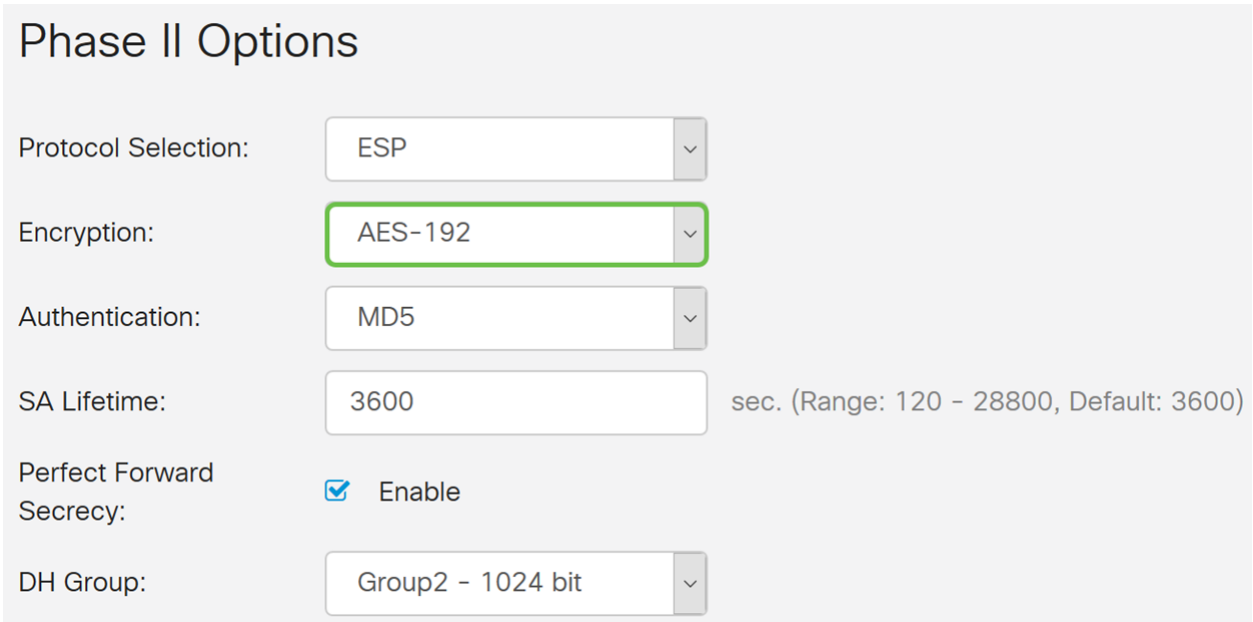
In questo esempio verrà utilizzato **ESP** come *selezione del protocollo*.



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.

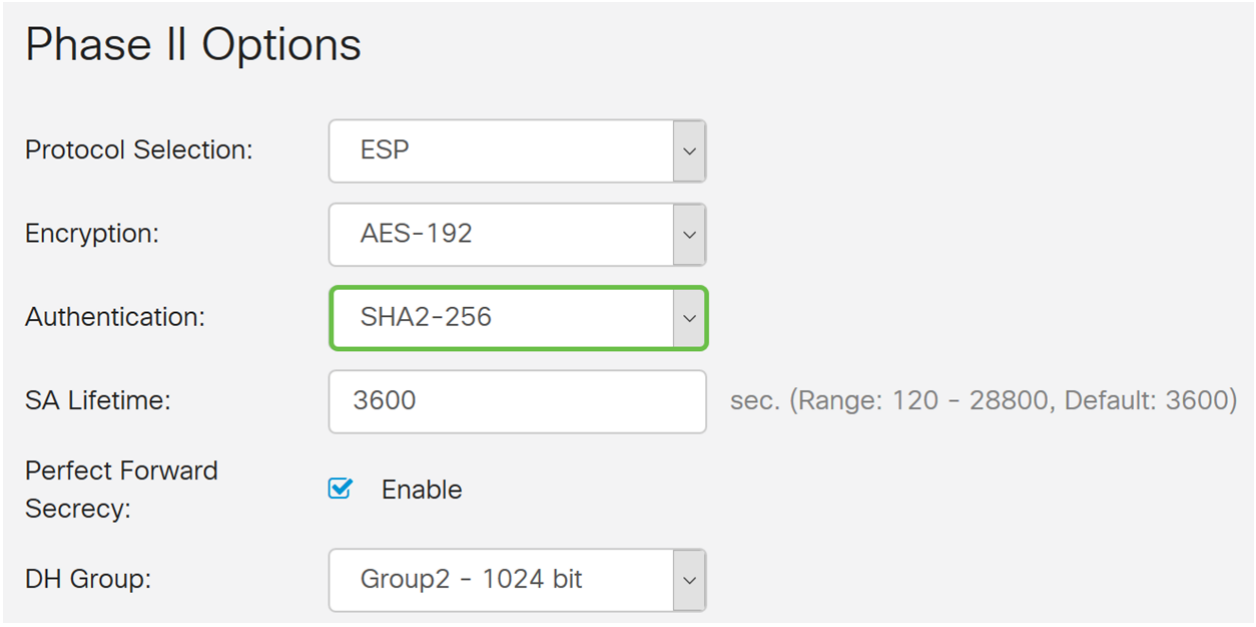
Nell'esempio, utilizzeremo **AES-192** come opzione di crittografia.

Nota: Fare clic sui collegamenti ipertestuali per ulteriori informazioni sulla configurazione della sicurezza per le VPN con IPsec o crittografia di nuova generazione.

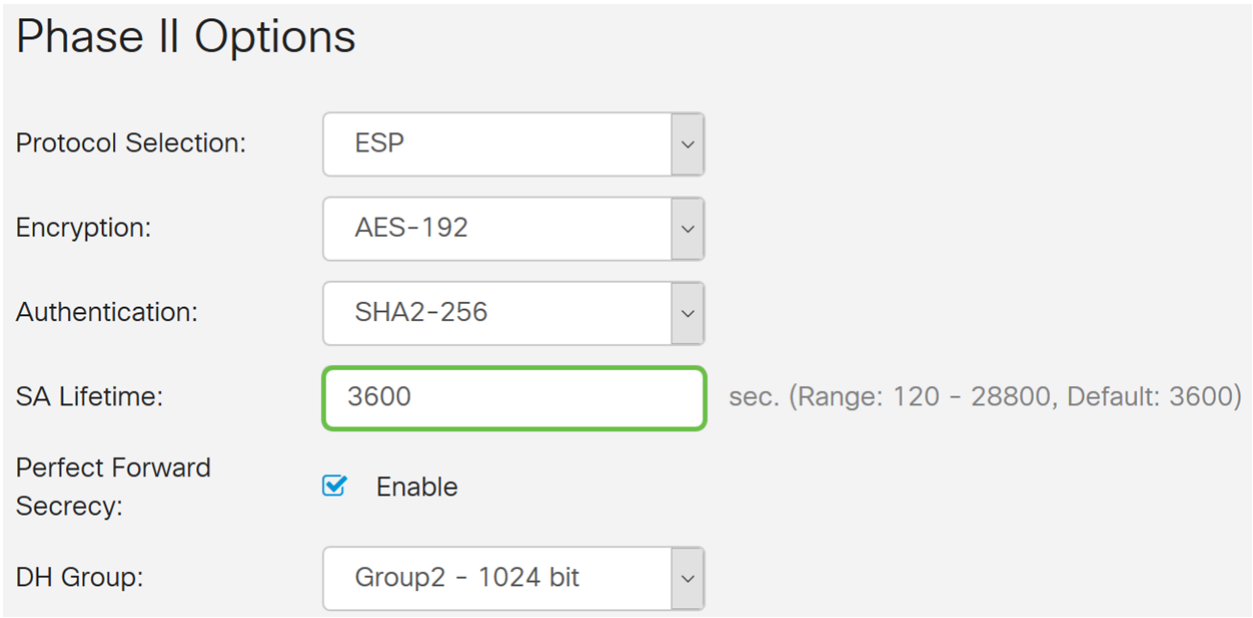


Passaggio 12. Il metodo di autenticazione determina la modalità di convalida dei pacchetti di intestazione Encapsulating Security Payload Protocol (ESP). Selezionare un'autenticazione (**MD5, SHA1** o **SHA2-256**).

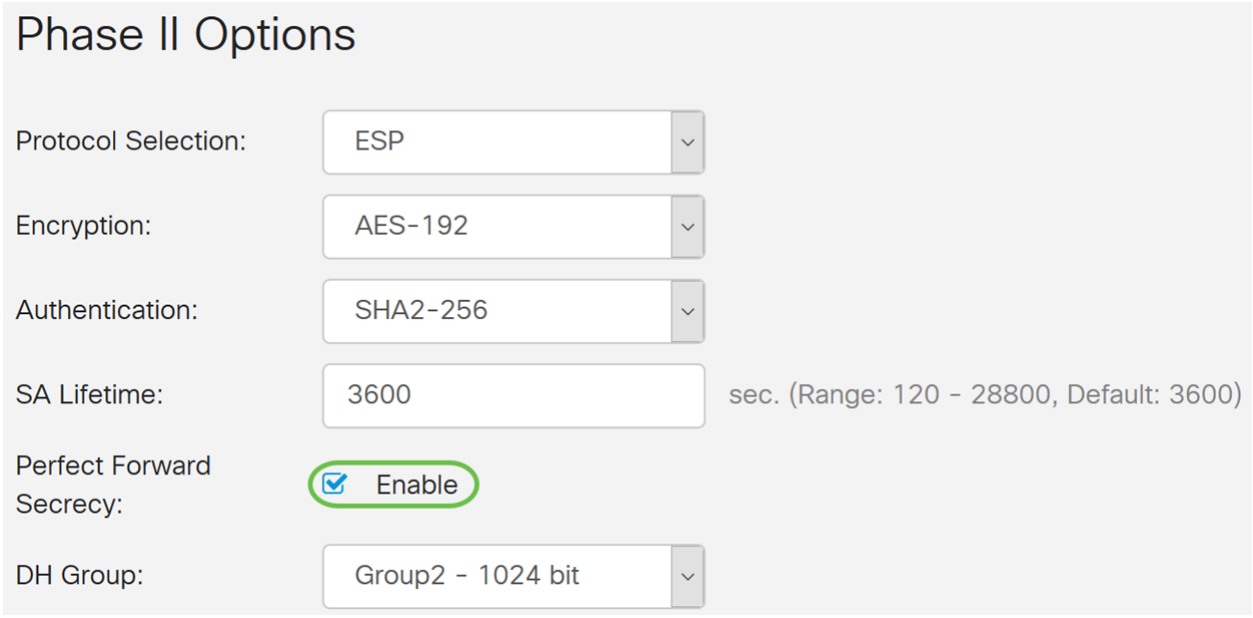
Per questo esempio è stato selezionato **SHA2-256**.



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.

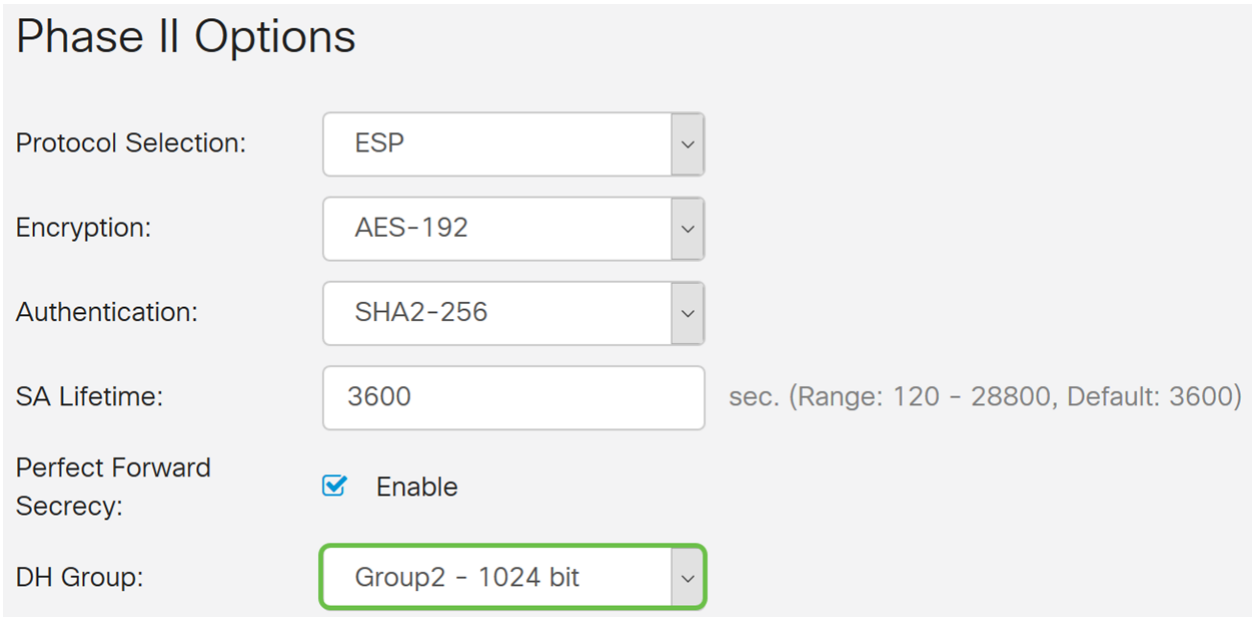


Passaggio 14. Selezionare **Abilita** per abilitare la segretezza di inoltro perfetta. Quando PFS (Perfect Forward Secrecy) è abilitato, la negoziazione IKE fase 2 genera nuovo materiale della chiave per la crittografia e l'autenticazione del traffico IPsec. PFS è utilizzato per migliorare la sicurezza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

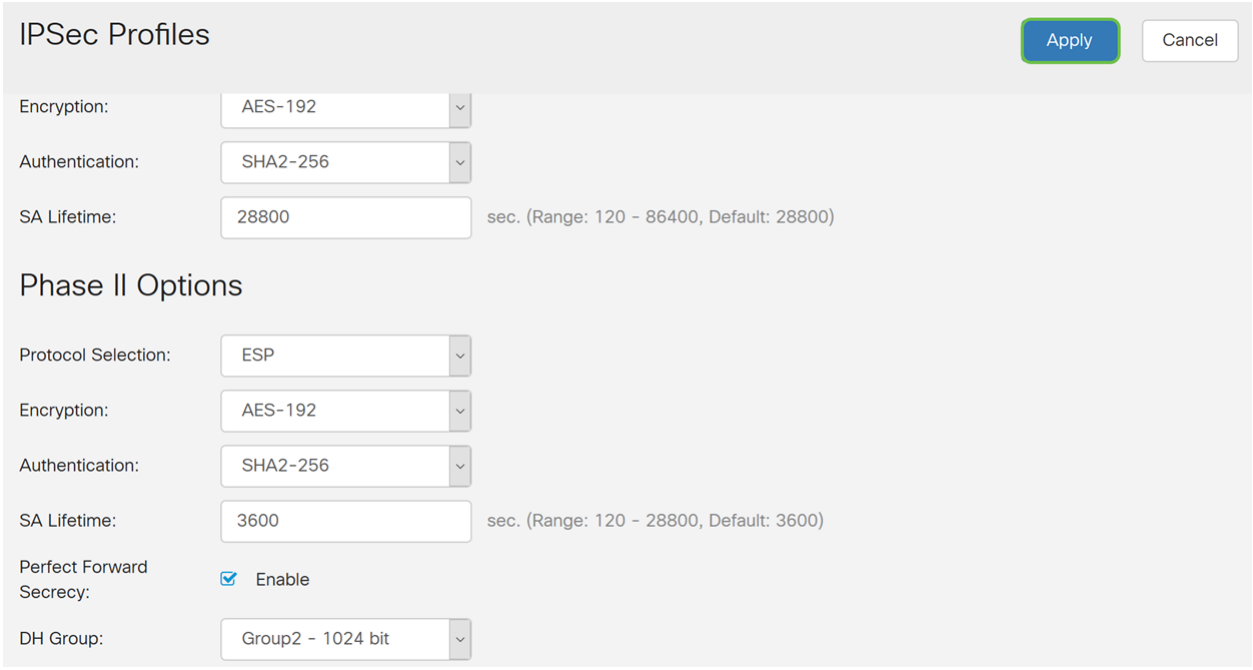


Passaggio 15. Selezionare un gruppo Diffie-Hellman (DH). DH è un protocollo di scambio di chiavi, con due gruppi di diverse lunghezze di chiavi primarie, **Gruppo 2 - 1024 bit** e **Gruppo 5 - 1536 bit**. Per questa dimostrazione, abbiamo selezionato **Gruppo 2 - 1024 bit**.

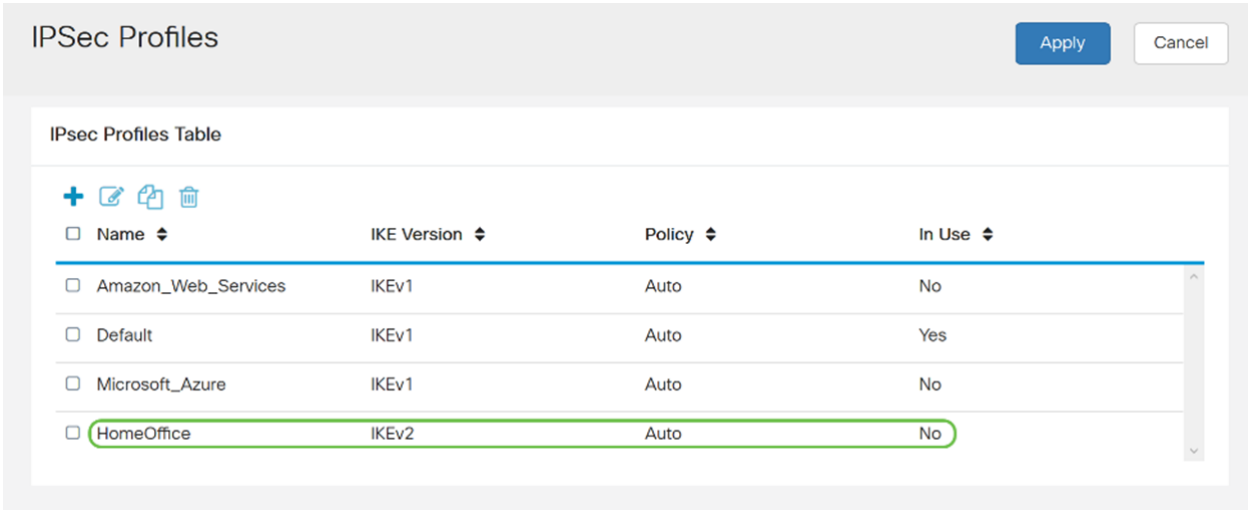
Nota: Per velocizzare le operazioni e ridurre la protezione, scegliere Gruppo 2. Per velocità più lente e maggiore protezione, scegliere Gruppo 5. Gruppo 2 è selezionato per impostazione predefinita.



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

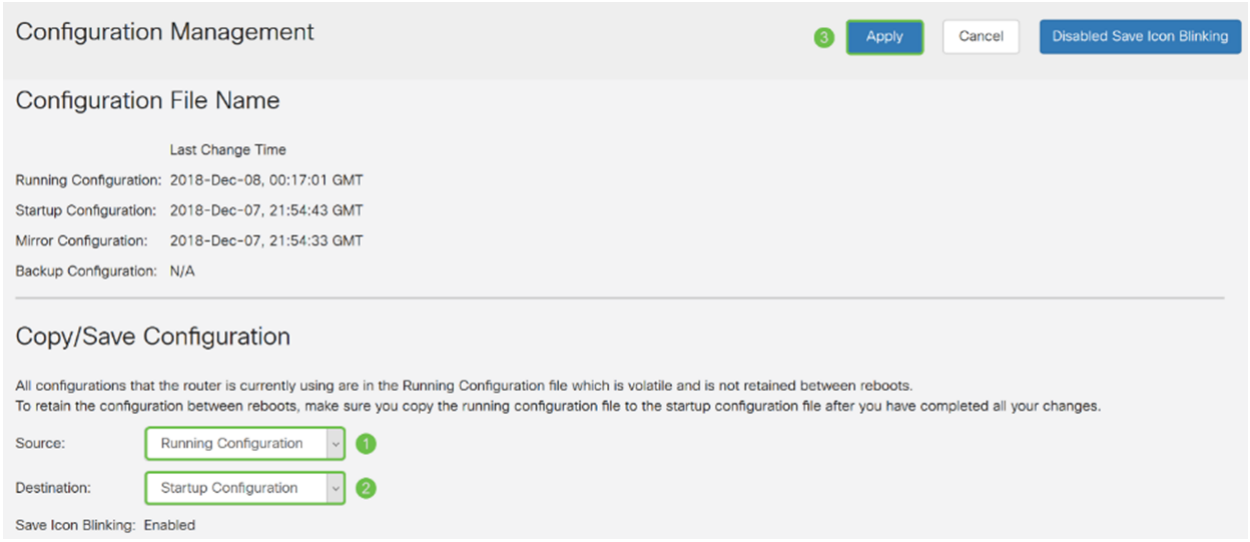


Passaggio 17. Dopo aver fatto clic su *Apply*, viene aggiunto il nuovo profilo IPSec.



Passaggio 18. Nella parte superiore della pagina, fare clic sull'icona **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 19. 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. Tutte le configurazioni attualmente utilizzate dal router si trovano nel file della configurazione in esecuzione, che è volatile e non viene conservato tra un riavvio e l'altro. Se si copia il file della configurazione in esecuzione nel file della configurazione di avvio, tutte le configurazioni verranno mantenute tra un riavvio e l'altro.



Passaggio 20. Seguire nuovamente tutti i passaggi per configurare il router B.

Conclusioni

È ora necessario creare un nuovo profilo IPsec utilizzando IKEv2 come versione IKE per entrambi i router. È ora possibile configurare una VPN da sito a sito.