Configurazione di un profilo IPSec (Internet Protocol Security) su un router serie RV34x

Obiettivo

IPSec (Internet Protocol Security) fornisce tunnel protetti tra due peer, ad esempio due router. I pacchetti considerati sensibili e da inviare attraverso questi tunnel sicuri, nonché i parametri da utilizzare per proteggere questi pacchetti sensibili, devono essere definiti specificando le caratteristiche di questi tunnel. Quindi, quando il peer IPsec rileva un pacchetto sensibile di questo tipo, configura il tunnel sicuro appropriato e invia il pacchetto attraverso questo tunnel al peer remoto.

Quando il protocollo IPsec viene implementato in un firewall o in un router, offre una protezione avanzata che può essere applicata a tutto il traffico che attraversa il perimetro. Il traffico all'interno di un'azienda o di un gruppo di lavoro non comporta il sovraccarico dell'elaborazione relativa alla sicurezza.

Lo scopo di questo documento è mostrare come configurare il profilo IPSec su un router serie RV34x.

Dispositivi interessati

- Serie RV34x

Versione del software

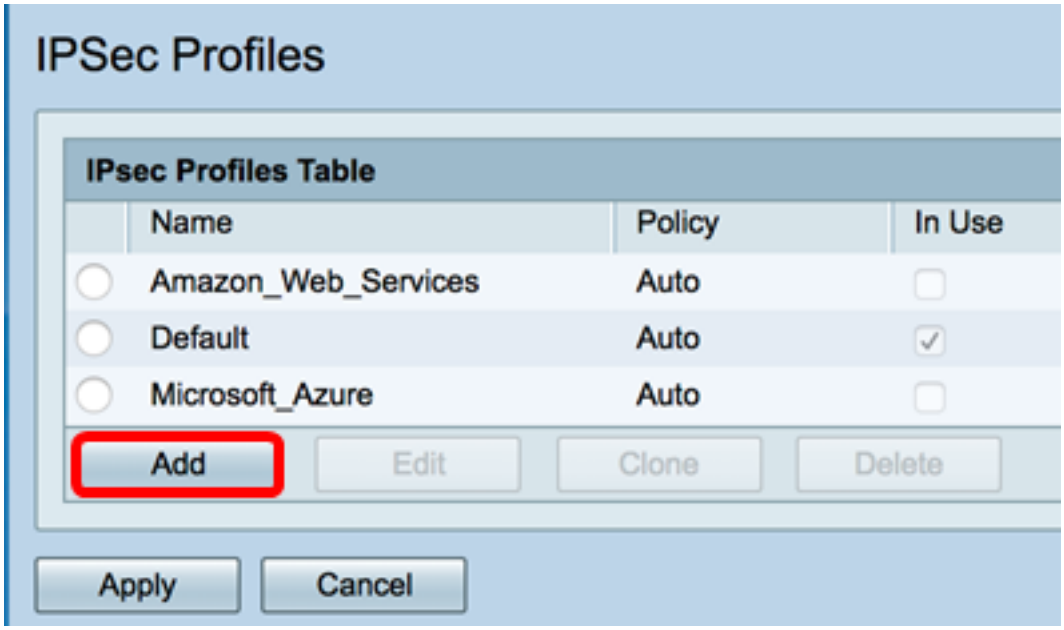
- 1.0.1.16

Configura profilo IPSec

Creazione di un profilo IPSec

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **VPN > Profili IPSec**.

Passaggio 2. La tabella Profili IPSec mostra i profili esistenti. Fare clic su **Aggiungi** per creare un nuovo profilo.



Passaggio 3. Creare un nome per il profilo nel campo *Nome profilo*. Il nome del profilo deve contenere solo caratteri alfanumerici e un carattere di sottolineatura (_) per i caratteri speciali.

Nota: Nell'esempio, il nome del profilo IPSec è IPSec_VPN.

Passaggio 4. Fare clic su un pulsante di opzione per determinare il metodo di scambio delle chiavi che verrà utilizzato dal profilo per l'autenticazione. Le opzioni sono:

- Auto — i parametri dei criteri vengono impostati automaticamente. Questa opzione utilizza un criterio IKE (Internet Key Exchange) per l'integrità dei dati e gli scambi di chiavi di crittografia. Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri automatici sono attivate. Fare clic qui per configurare le impostazioni di Auto.
- Manuale: questa opzione consente di configurare manualmente le chiavi per la crittografia e l'integrità dei dati per il tunnel VPN (Virtual Private Network). Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri manuali sono attivate. Fare clic qui per configurare le impostazioni manuali.

Nota: Per questo esempio è stato scelto Auto.

Configurazione delle impostazioni automatiche

Passaggio 1. Nell'area Opzioni fase 1, scegliere il gruppo Diffie-Hellman (DH) appropriato da utilizzare con la chiave nella fase 1 dall'elenco a discesa Gruppo DH. Diffie-Hellman è un protocollo di scambio chiave crittografica utilizzato nella connessione per lo scambio di set di chiavi già condivisi. La forza dell'algoritmo è determinata dai bit. Le opzioni sono:

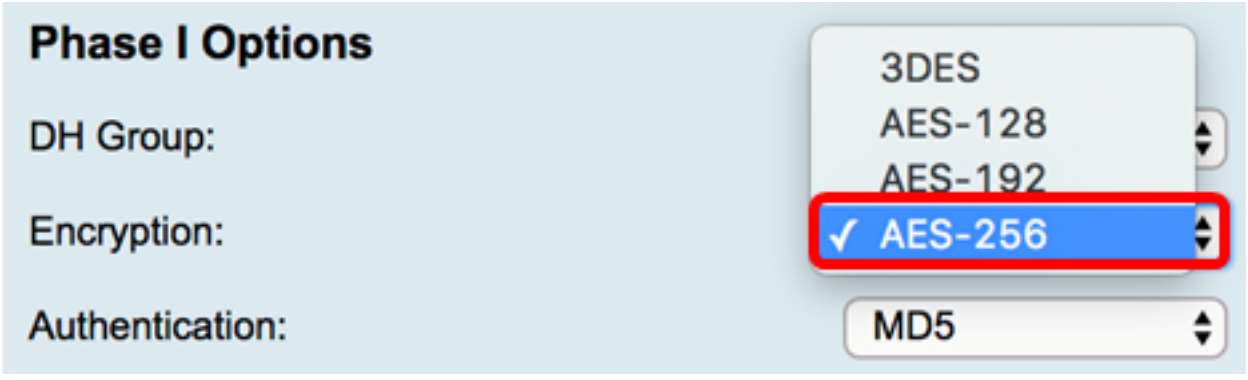
- Gruppo2 - 1024 bit: calcola la chiave più lentamente, ma è più sicuro di Gruppo1.
- Gruppo5 - 1536 bit: calcola la chiave più lentamente, ma è la più sicura.

Nota: Nell'esempio, viene scelto Group2-1024 bit.

Passaggio 2. Dall'elenco a discesa Crittografia, scegliere il metodo di crittografia appropriato per crittografare e decrittografare Encapsulating Security Payload (ESP) e Internet Security Association and Key Management Protocol (ISAKMP). Le opzioni sono:

- 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 ottenere prestazioni e sicurezza maggiori. L'aumento della lunghezza della chiave AES aumenta la sicurezza con un calo delle prestazioni. Per questo esempio, viene scelto AES-256.



Passaggio 3. Dal menu a discesa Autenticazione, scegliere un metodo di autenticazione che

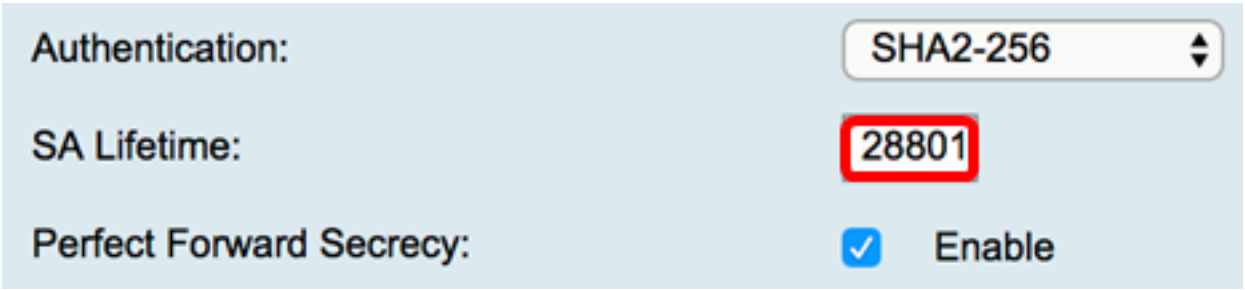
determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

- MD5 — Message Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algoritmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algoritmo hash sicuro con un valore hash a 256 bit.

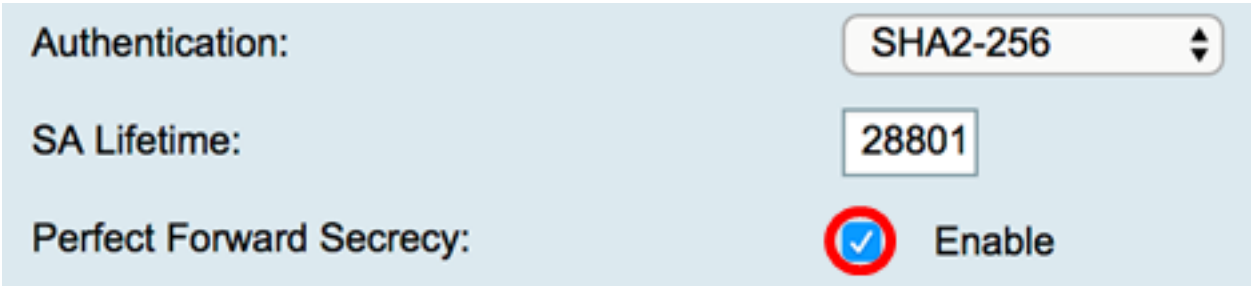
Nota: MD5 e SHA sono entrambe funzioni hash crittografiche. Prendono un dato, lo compattano e creano un output esadecimale unico che in genere non è riproducibile. Nell'esempio, viene scelto SHA2-256.

Passaggio 4. Nel campo *Durata SA* immettere un valore compreso tra 120 e 86400. Questo valore indica il periodo di tempo durante il quale l'associazione di sicurezza IKE (Internet Key Exchange) rimarrà attiva in questa fase. Il valore predefinito è 28800.

Nota: nell'esempio viene usato 2801.

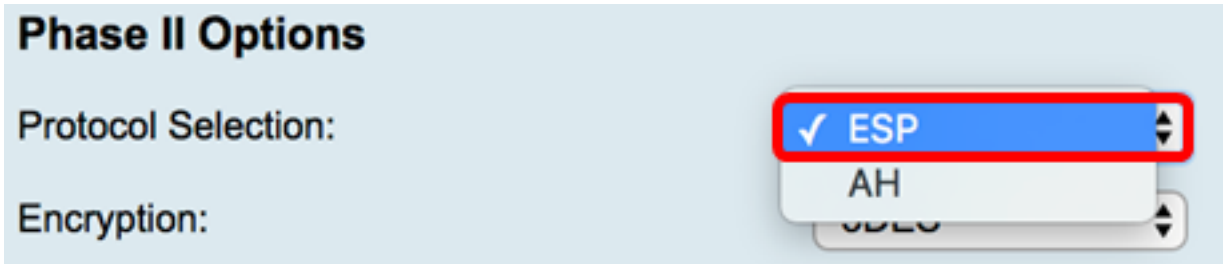


Passaggio 5. (Facoltativo) Selezionare la casella di controllo **Abilita segreto inoltro** corretto per generare una nuova chiave per la crittografia e l'autenticazione del traffico IPSec.



Passaggio 6. Dal menu a discesa Selezione protocollo nell'area Opzioni fase II, scegliere un tipo di protocollo da applicare alla seconda fase della negoziazione. Le opzioni sono:

- ESP: se si sceglie questa opzione, andare al passaggio 7 per scegliere un metodo di crittografia per la crittografia e la decrittografia dei pacchetti ESP. Protocollo di sicurezza che fornisce servizi di privacy dei dati, autenticazione dei dati opzionale e servizi anti-replay. ESP incapsula i dati da proteggere.
- AH — Authentication Header (AH) è un protocollo di sicurezza che fornisce l'autenticazione dei dati e i servizi opzionali anti-replay. AH è incorporato nei dati da proteggere (datagramma IP completo). Se è stato scelto questo comando, andare al passaggio 8.



Passaggio 7. Se nel passaggio 6 è stato scelto ESP, scegliere il metodo di crittografia appropriato per crittografare e decrittografare ESP e ISAKMP dall'elenco a discesa Crittografia. Le opzioni sono:

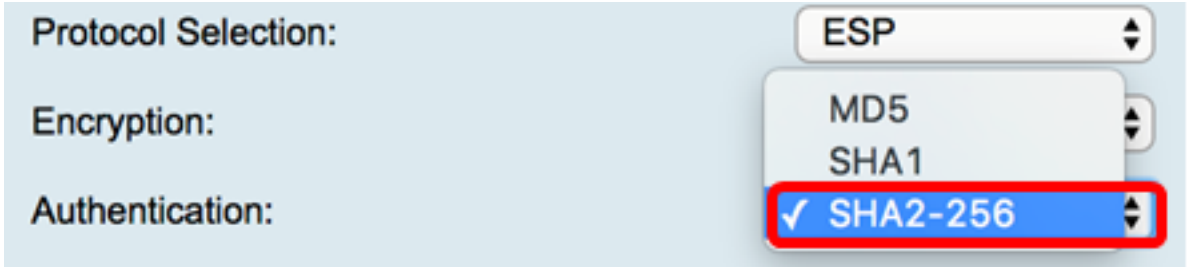
- 3DES: standard per la crittografia tripla dei dati.
- AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit.
- AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.
- AES-256 — Advanced Encryption Standard utilizza una chiave a 256 bit.

Nota: Nell'esempio, viene scelto AES-256.

Passaggio 8. Dal menu a discesa Autenticazione, scegliere un metodo di autenticazione che determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

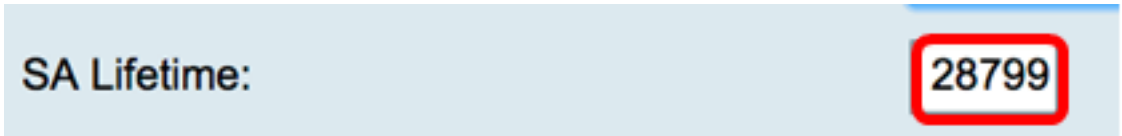
- MD5 — Message Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algoritmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algoritmo hash sicuro con un valore hash a 256 bit.

Nota: Nell'esempio viene utilizzato SHA2-256.



Passaggio 9. Nel campo *Durata associazione di protezione* immettere un valore compreso tra 120 e 2800. Questo valore indica il periodo di tempo durante il quale l'associazione di protezione IKE rimarrà attiva in questa fase. Il valore predefinito è 3600.

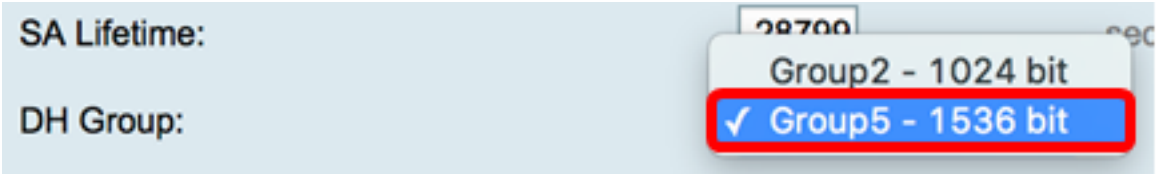
Nota: Nell'esempio viene utilizzato 28799.



Passaggio 10. Dall'elenco a discesa Gruppo DH, scegliere il gruppo Diffie-Hellman (DH) appropriato da utilizzare con la chiave nella Fase 2. Le opzioni sono:

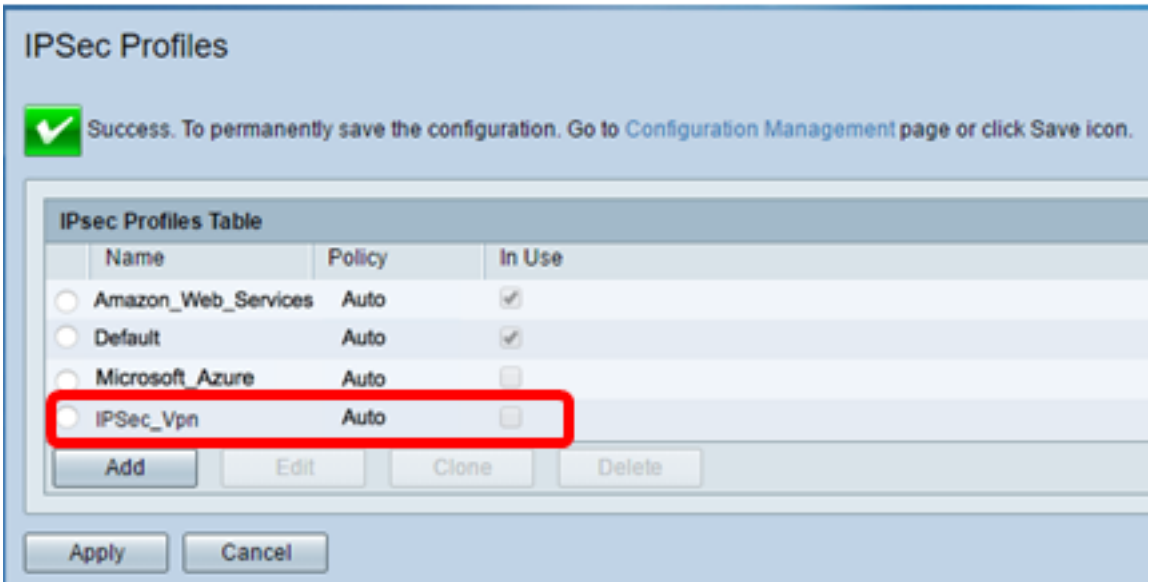
- Gruppo2 - 1024 bit: calcola la chiave più lentamente, ma è più sicuro di Gruppo1.
- Gruppo5 - 1536 bit: calcola la chiave più lentamente, ma è la più sicura.

Nota: Nell'esempio, viene scelto Gruppo 5 - 1536 bit.



Passaggio 11. Fare clic su Apply.

Nota: Verrà visualizzata di nuovo la tabella Profili IPSec e verrà visualizzato il nuovo profilo IPSec.



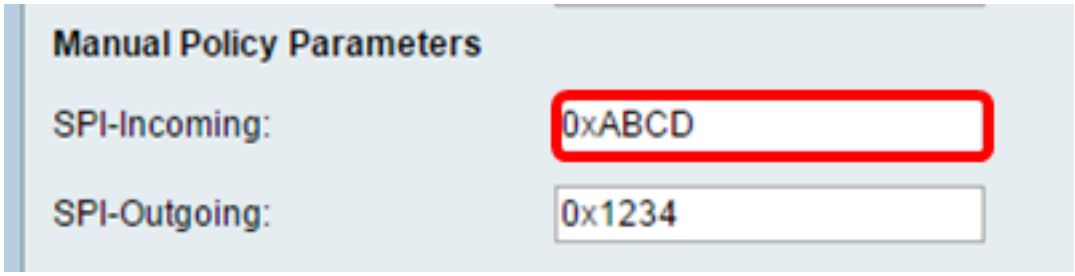
Passaggio 12. (Facoltativo) Per salvare la configurazione in modo permanente, andare alla pagina Copia/Salva configurazione o fare clic sull'icona Save nella parte superiore della pagina.

A questo punto, è necessario configurare correttamente un profilo IPSec automatico su un router serie RV34x.

Configurazione delle impostazioni manuali

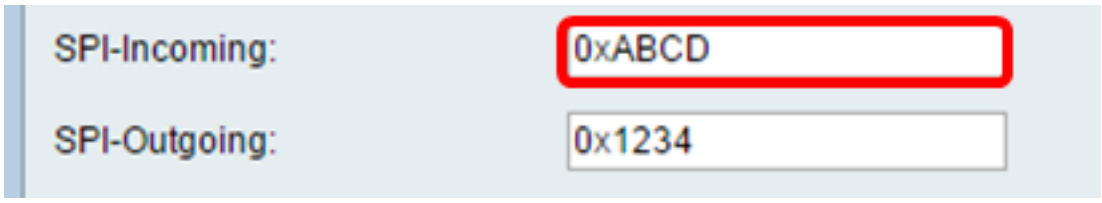
Passaggio 1. Nel campo *SPI-Incoming*, immettere un numero esadecimale compreso tra 100 e FFFFF per il tag SPI (Security Parameter Index) per il traffico in entrata sulla connessione VPN. Il tag SPI viene utilizzato per distinguere il traffico di una sessione dal traffico di altre sessioni.

Nota: Nell'esempio, viene usato 0xABCD.



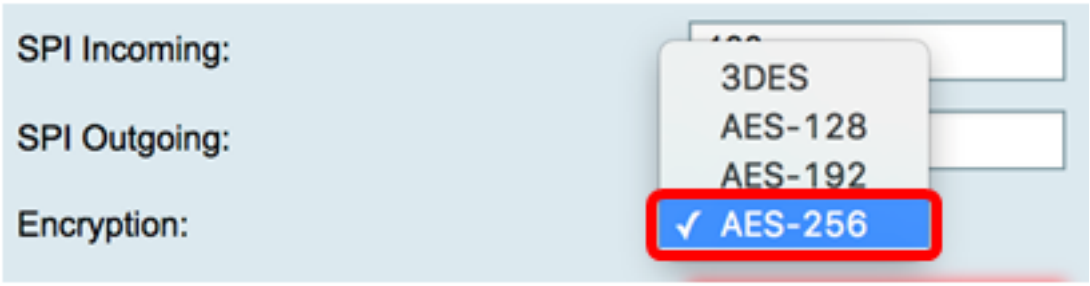
Passaggio 2. Nel campo *SPI-Outgoing*, immettere un numero esadecimale compreso tra 100 e FFFFF per il tag SPI per il traffico in uscita sulla connessione VPN.

Nota: Nell'esempio viene usato 0x1234.



Passaggio 3. Scegliere un'opzione dall'elenco a discesa Crittografia. Le opzioni sono 3DES, AES-128, AES-192 e AES-256.

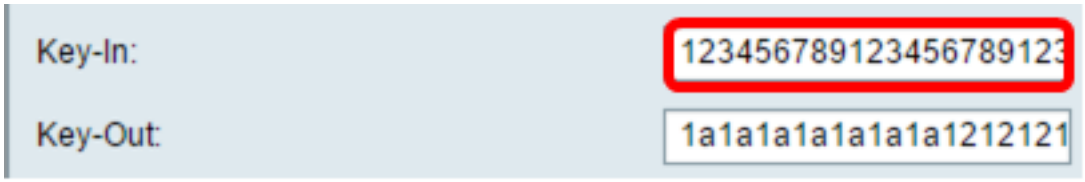
Nota: Nell'esempio, viene scelto AES-256.



Passaggio 4. Nel campo *Chiave in ingresso*, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

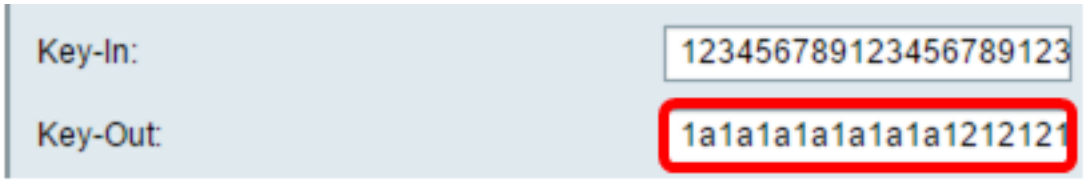
- 3DES utilizza un tasto di 48 caratteri.
- AES-128 utilizza un tasto di 32 caratteri.
- AES-192 utilizza un tasto di 48 caratteri.
- AES-256 utilizza un tasto a 64 caratteri.

Nota: Nell'esempio viene utilizzato 123456789123456789123...



Passaggio 5. Nel campo *Esclusione* immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 3.

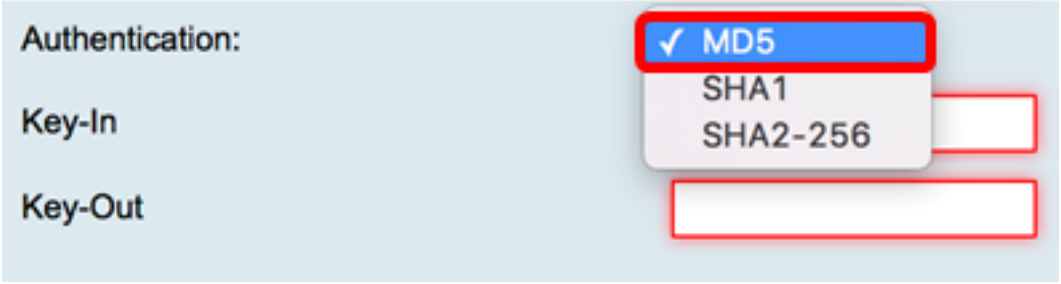
Nota: Nell'esempio viene utilizzato 1a1a1a1a1a1a1a1a1a121212....



Passaggio 6. Scegliere un'opzione dall'elenco a discesa Algoritmo di integrità manuale.

- MD5: utilizza un valore hash a 128 bit per l'integrità dei dati. MD5 è meno sicuro ma più veloce rispetto a SHA-1 e SHA2-256.
- SHA-1: utilizza un valore hash a 160 bit per l'integrità dei dati. SHA-1 è più lento ma più sicuro di MD5 e SHA-1 è più veloce ma meno sicuro di SHA2-256.
- SHA2-256: utilizza un valore hash a 256 bit per l'integrità dei dati. SHA2-256 è più lento ma sicuro di MD5 e SHA-1.

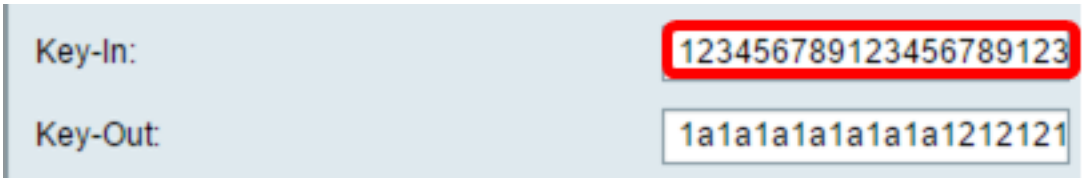
Nota: In questo esempio, viene scelto MD5.



Passaggio 7. Nel *campo Chiave in ingresso*, immettere una chiave per il criterio in ingresso. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

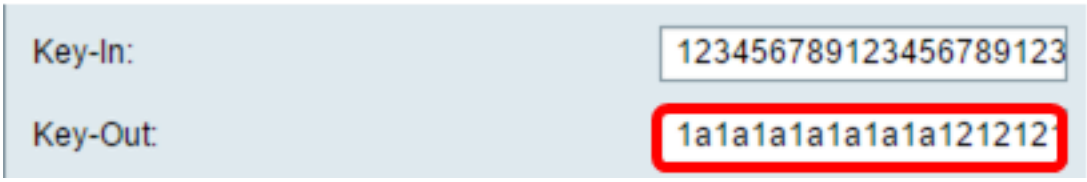
- MD5 utilizza un tasto di 32 caratteri.
- SHA-1 utilizza un tasto di 40 caratteri.
- SHA2-256 utilizza un tasto a 64 caratteri.

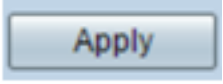
Nota: Nell'esempio viene utilizzato 123456789123456789123...



Passaggio 8. Nel *campo Esclusione*, immettere una chiave per il criterio in uscita. La lunghezza della chiave dipende dall'algoritmo scelto nel passaggio 6.

Nota: Nell'esempio viene utilizzato 1a1a1a1a1a1a1a1a1a121212....

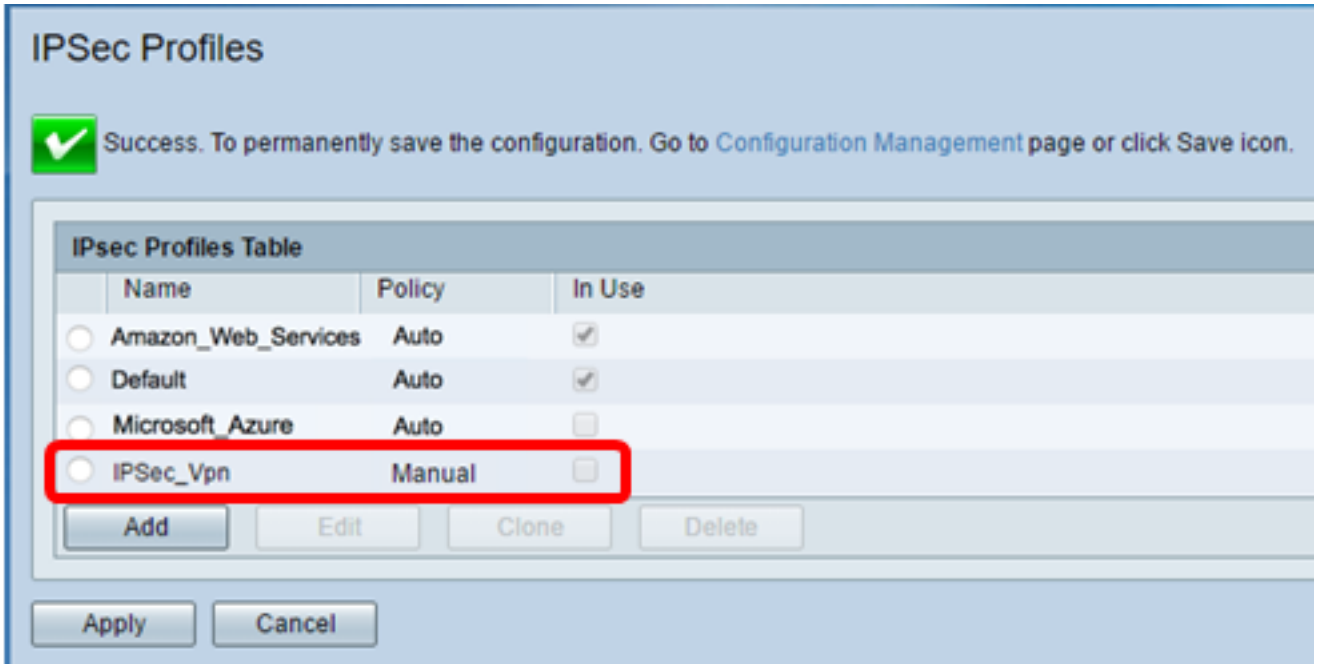


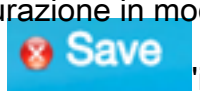
Passaggio 9. Fare clic su 

.

Nota: Verrà visualizzata di nuovo la tabella Profili IPSec e verrà visualizzato il nuovo profilo

IPSec.



Passaggio 10. (Facoltativo) Per salvare la configurazione in modo permanente, andare alla pagina Copia/Salva configurazione o fare clic sull 

'icona nella parte superiore della pagina.

A questo punto, è necessario configurare un profilo IPSec manuale su un router serie RV34x.