

# Konfigurieren eines IPSec-Profiles (Internet Protocol Security) auf einem Router der Serie RV34x

## Ziel

Internet Protocol Security (IPSec) bietet sichere Tunnel zwischen zwei Peers, z. B. zwei Routern. Pakete, die als sensibel gelten und über diese sicheren Tunnel gesendet werden sollten, sowie die Parameter, die zum Schutz dieser sensiblen Pakete verwendet werden sollten, sollten durch Angabe der Merkmale dieser Tunnel definiert werden. Wenn dann der IPsec-Peer ein derart sensibles Paket sieht, richtet er den entsprechenden sicheren Tunnel ein und sendet das Paket durch diesen Tunnel an den Remote-Peer.

Wenn IPsec in einer Firewall oder in einem Router implementiert wird, bietet es starke Sicherheit, die auf den gesamten Perimeter überschreitenden Datenverkehr angewendet werden kann. Der Datenverkehr innerhalb eines Unternehmens oder einer Arbeitsgruppe verursacht keine Kosten für die sicherheitsbezogene Verarbeitung.

In diesem Dokument wird erläutert, wie Sie das IPSec-Profil auf einem Router der Serie RV34x konfigurieren.

## Anwendbare Geräte

- Serie RV34x

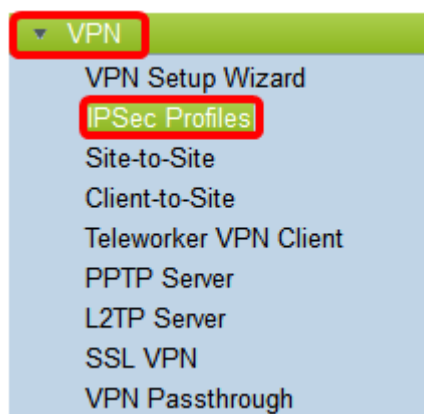
## Softwareversion

- 1,0/1,16

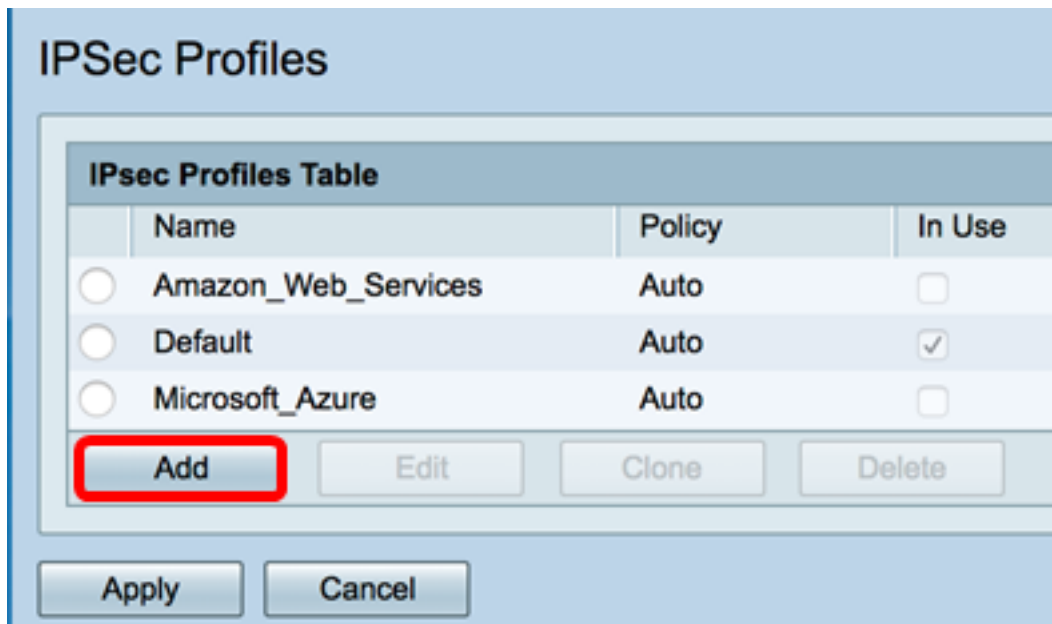
## Konfigurieren des IPSec-Profiles

### IPSec-Profil erstellen

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Routers an, und wählen Sie **VPN > IPSec Profiles** aus.

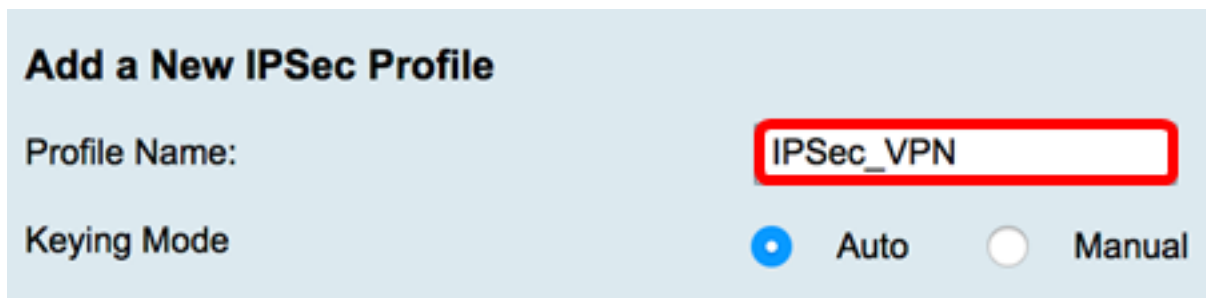


Schritt 2: Die IPsec-Profiltable zeigt die vorhandenen Profile. Klicken Sie auf **Hinzufügen**, um ein neues Profil zu erstellen.



Schritt 3: Erstellen Sie im Feld *Profilname* einen Namen für das Profil. Der Profilname darf nur alphanumerische Zeichen und ein Unterstrich (\_) für Sonderzeichen enthalten.

**Hinweis:** In diesem Beispiel wird IPsec\_VPN als IPsec-Profilname verwendet.



Schritt 4: Klicken Sie auf ein Optionsfeld, um die Schlüsselaustauschmethode für die Authentifizierung des Profils festzulegen. Folgende Optionen stehen zur Verfügung:

- Auto (Automatisch): Richtlinienparameter werden automatisch festgelegt. Diese Option verwendet eine IKE-Richtlinie (Internet Key Exchange) für Datenintegrität und Verschlüsselungsschlüssel-Austausch. Wenn diese Option ausgewählt ist, sind die Konfigurationseinstellungen im Bereich Auto Policy Parameters (Parameter für automatische Richtlinie) aktiviert. Klicken Sie [hier](#), um die Auto-Einstellungen zu konfigurieren.
- Manual (Manuell): Mit dieser Option können Sie die Schlüssel für Datenverschlüsselung und -integrität im VPN-Tunnel (Virtual Private Network) manuell konfigurieren. Wenn diese Option ausgewählt ist, werden die Konfigurationseinstellungen im Bereich "Manuelle Richtlinienparameter" aktiviert. Klicken Sie [hier](#), um die manuellen Einstellungen zu konfigurieren.

**Hinweis:** Für dieses Beispiel wurde Auto ausgewählt.

## Add a New IPsec Profile

Profile Name:

IPsec\_VPN

Keying Mode



Auto



Manual

### Konfigurieren der automatischen Einstellungen

Schritt 1: Wählen Sie im Bereich Phase 1-Optionen die entsprechende Diffie-Hellman (DH)-Gruppe aus der Dropdown-Liste DH Group (DH-Gruppe) aus, die mit dem Schlüssel in Phase 1 verwendet werden soll. Diffie-Hellman ist ein kryptografisches Schlüsselaustauschprotokoll, das bei der Verbindung zum Austausch von vorinstallierten Schlüsselsätzen verwendet wird. Die Stärke des Algorithmus wird durch Bits bestimmt. Folgende Optionen stehen zur Verfügung:

- Group2 - 1024 bit (Gruppe2 - 1024 Bit): Berechnet den Schlüssel langsamer, ist aber sicherer als Group1.
- Gruppe5 - 1536-Bit - Berechnet den Schlüssel am langsamsten, ist aber am sichersten.

**Hinweis:** In diesem Beispiel wird das Bit Group2-1024 ausgewählt.

### Phase I Options

DH Group:

✓ Group2 - 1024 bit

Group5 - 1536 bit

Encryption:

Schritt 2: Wählen Sie in der Dropdown-Liste Verschlüsselung die entsprechende Verschlüsselungsmethode zum Verschlüsseln und Entschlüsseln der Encapsulating Security Payload (ESP) und des Internet Security Association and Key Management Protocol (ISAKMP) aus. Folgende Optionen stehen zur Verfügung:

- 3DES - Triple Data Encryption Standard.
- AES-128 - Advanced Encryption Standard verwendet einen 128-Bit-Schlüssel.
- AES-192 - Advanced Encryption Standard verwendet einen 192-Bit-Schlüssel.
- AES-256 - Advanced Encryption Standard verwendet einen 256-Bit-Schlüssel.

**Hinweis:** AES ist die Standardmethode der Verschlüsselung über DES und 3DES für mehr Leistung und Sicherheit. Durch die Verlängerung des AES-Schlüssels wird die Sicherheit durch eine geringere Leistung erhöht. Für dieses Beispiel wird AES-256 ausgewählt.

**Phase I Options**

DH Group:

Encryption: 3DES  
AES-128  
AES-192  
✓ AES-256

Authentication: MD5

Schritt 3: Wählen Sie im Dropdown-Menü Authentication (Authentifizierung) eine Authentifizierungsmethode aus, die bestimmt, wie ESP und ISAKMP authentifiziert werden. Folgende Optionen stehen zur Verfügung:

- MD5 - Message Digest Algorithm hat einen 128-Bit-Hashwert.
- SHA-1 - Secure Hash Algorithm hat einen 160-Bit-Hashwert.
- SHA2-256 - Sicherer Hash-Algorithmus mit einem Hashwert von 256 Bit.

**Hinweis:** MD5 und SHA sind beide kryptografische Hashfunktionen. Sie nehmen Daten, kompilieren sie und erstellen eine eindeutige Hexadezimalausgabe, die normalerweise nicht reproduzierbar ist. In diesem Beispiel wird SHA2-256 ausgewählt.

DH Group: Group2 - 1024 bit

Encryption:

Authentication: MD5  
SHA1  
✓ SHA2-256

Schritt 4: Geben Sie im Feld *SA Lifetime (SA-Lebensdauer)* einen Wert zwischen 120 und 86400 ein. Dies ist die Dauer, die die Internet Key Exchange (IKE) Security Association (SA) in dieser Phase aktiv bleiben wird. Der Standardwert ist 28800.

**Hinweis:** In diesem Beispiel wird 28801 verwendet.

Authentication: SHA2-256

SA Lifetime: 28801

Perfect Forward Secrecy:  Enable

Schritt 5: (Optional) Aktivieren Sie das Kontrollkästchen **Enable Perfect Forward Secrecy** (Perfektes Weiterleiten-**Geheimnis aktivieren**), um einen neuen Schlüssel für die Verschlüsselung und Authentifizierung des IPSec-Datenverkehrs zu generieren.

Authentication:	SHA2-256
SA Lifetime:	28801
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable

Schritt 6: Wählen Sie im Dropdown-Menü Protocol Selection (Protokollauswahl) im Bereich Phase II Options (Optionen für Phase II) einen Protokolltyp aus, der auf die zweite Verhandlungsphase angewendet werden soll. Folgende Optionen stehen zur Verfügung:

- ESP: Wenn Sie diese Option auswählen, fahren Sie mit [Schritt 7](#) fort, um eine Verschlüsselungsmethode für die Verschlüsselung und Entschlüsselung der ESP-Pakete auszuwählen. Ein Sicherheitsprotokoll, das Datenschutz-Services, optionale Datenauthentifizierung und Anti-Replay-Services bereitstellt. ESP kapselt die zu schützenden Daten.
- AH — Authentication Header (AH) ist ein Sicherheitsprotokoll, das Datenauthentifizierung und optionale Anti-Replay-Dienste bietet. AH ist in die zu schützenden Daten eingebettet (ein vollständiges IP-Datagramm). Fahren Sie mit [Schritt 8](#) fort, wenn Sie diese Option ausgewählt haben.

<b>Phase II Options</b>	
Protocol Selection:	✓ ESP
Encryption:	AH

[Schritt 7](#): Wenn in Schritt 6 ESP ausgewählt wurde, wählen Sie die entsprechende Verschlüsselungsmethode aus, um ESP und ISAKMP zu verschlüsseln und zu entschlüsseln. Wählen Sie dazu die entsprechende Verschlüsselungsmethode in der Dropdown-Liste Verschlüsselung aus. Folgende Optionen stehen zur Verfügung:

- 3DES - Triple Data Encryption Standard.
- AES-128 - Advanced Encryption Standard verwendet einen 128-Bit-Schlüssel.
- AES-192 - Advanced Encryption Standard verwendet einen 192-Bit-Schlüssel.
- AES-256 - Advanced Encryption Standard verwendet einen 256-Bit-Schlüssel.

**Hinweis:** In diesem Beispiel wird AES-256 ausgewählt.

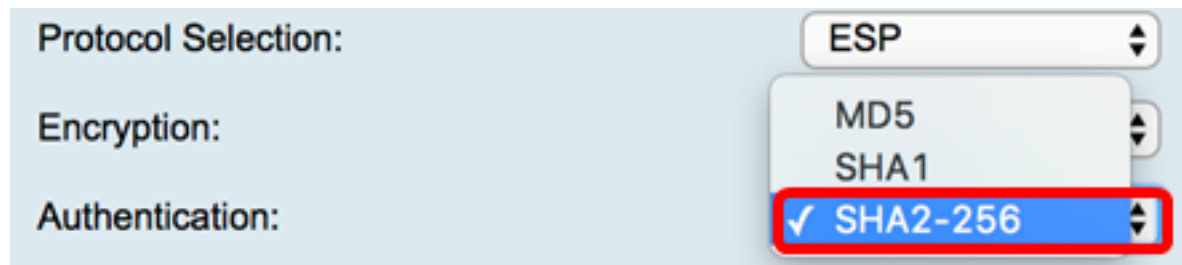
<b>Phase II Options</b>	
Protocol Selection:	
Encryption:	3DES
	AES-128
	AES-192
	✓ AES-256

[Schritt 8](#): Wählen Sie im Dropdown-Menü Authentication (Authentifizierung) eine Authentifizierungsmethode aus, die bestimmt, wie ESP und ISAKMP authentifiziert werden.

Folgende Optionen stehen zur Verfügung:

- MD5 - Message Digest Algorithm hat einen 128-Bit-Hashwert.
- SHA-1 - Secure Hash Algorithm hat einen 160-Bit-Hashwert.
- SHA2-256 - Sicherer Hash-Algorithmus mit einem Hashwert von 256 Bit.

**Hinweis:** In diesem Beispiel wird SHA2-256 verwendet.



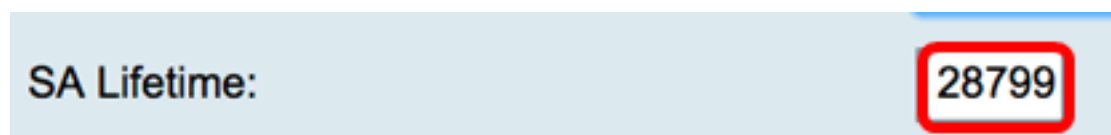
Protocol Selection: ESP

Encryption: MD5, SHA1

Authentication: ✓ SHA2-256

Schritt 9: Geben Sie im Feld *SA Lifetime* (SA-Lebensdauer) einen Wert zwischen 120 und 28800 ein. Dies ist die Dauer, die die IKE SA in dieser Phase aktiv bleiben wird. Der Standardwert ist 3600.

**Hinweis:** In diesem Beispiel wird 28799 verwendet.

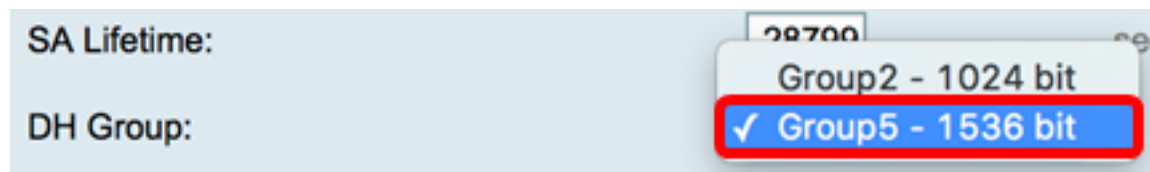


SA Lifetime: 28799

Schritt 10: Wählen Sie in der Dropdown-Liste "DH Group" (DH-Gruppe) die entsprechende DH-Gruppe (Diffie-Hellman) aus, die mit dem Schlüssel in Phase 2 verwendet werden soll. Folgende Optionen stehen zur Verfügung:

- Group2 - 1024 bit (Gruppe2 - 1024 Bit): Berechnet den Schlüssel langsamer, ist aber sicherer als Group1.
- Gruppe5 - 1536 Bit - Berechnet den Schlüssel am langsamsten, ist aber am sichersten.

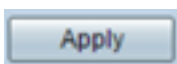
**Hinweis:** In diesem Beispiel wird Gruppe5 - 1536 Bit ausgewählt.



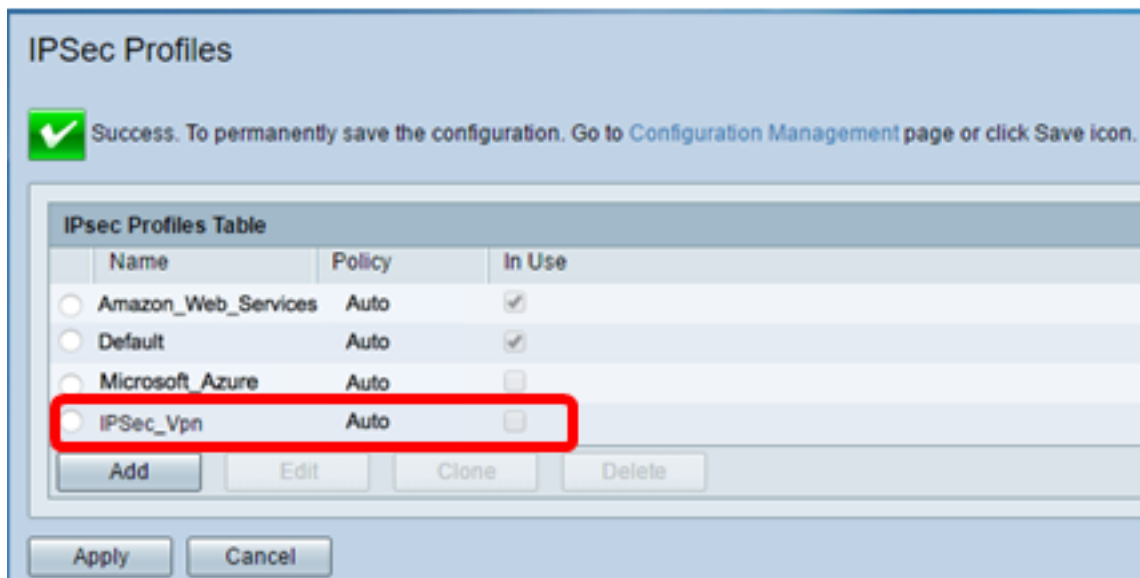
SA Lifetime: 28799


DH Group: ✓ Group5 - 1536 bit

Schritt 11: Klicken Sie



**Hinweis:** Sie werden zur IPSec-Profiltable zurückgeleitet, und das neu erstellte IPSec-Profil sollte jetzt angezeigt werden.



Schritt 12: (Optional) Um die Konfiguration dauerhaft zu speichern, öffnen Sie die Seite "Copy/Save Configuration" (Konfiguration kopieren/speichern), oder klicken Sie auf das  Symbol oben auf der Seite.

Sie sollten jetzt ein Auto IPsec-Profil auf einem Router der Serie RV34x erfolgreich konfiguriert haben.

### Konfigurieren der manuellen Einstellungen

Schritt 1: Geben Sie im Feld *SPI-Incoming* (SPI-Incoming) eine Hexadezimalnummer zwischen 100 und FFFFFFFF für das SPI-Tag (Security Parameter Index) für eingehenden Datenverkehr an der VPN-Verbindung ein. Der SPI-Tag wird verwendet, um den Datenverkehr einer Sitzung vom Datenverkehr anderer Sitzungen zu unterscheiden.

**Hinweis:** In diesem Beispiel wird 0xABCD verwendet.

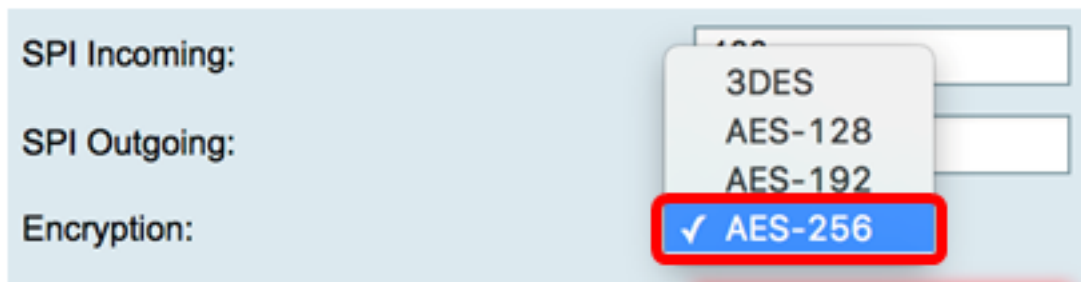
Schritt 2: Geben Sie im Feld *SPI-Outgoing* (SPI-Ausgang) eine Hexadezimalnummer zwischen 100 und FFFFFFFF für das SPI-Tag für ausgehenden Datenverkehr an der VPN-Verbindung ein.

**Hinweis:** In diesem Beispiel wird 0x1234 verwendet.

Schritt 3: Wählen Sie eine Option aus der Dropdown-Liste Verschlüsselung aus. Die

Optionen sind 3DES, AES-128, AES-192 und AES-256.

**Hinweis:** In diesem Beispiel wird AES-256 ausgewählt.

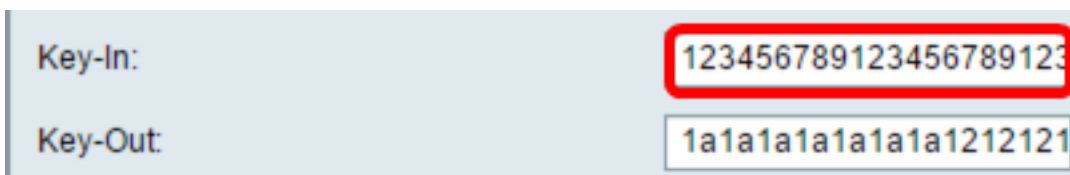


Screenshot of a configuration interface showing encryption options. The options are 3DES, AES-128, AES-192, and AES-256. The AES-256 option is selected and highlighted with a red box.

Schritt 4: Geben Sie im Feld *Key-In* (Schlüssel für eingehende Richtlinie) einen Schlüssel ein. Die Schlüssellänge hängt vom in [Schritt 3](#) gewählten Algorithmus ab.

- 3DES verwendet einen 48-stelligen Schlüssel.
- AES-128 verwendet einen 32-stelligen Schlüssel.
- AES-192 verwendet einen 48-stelligen Schlüssel.
- AES-256 verwendet einen 64-stelligen Schlüssel.

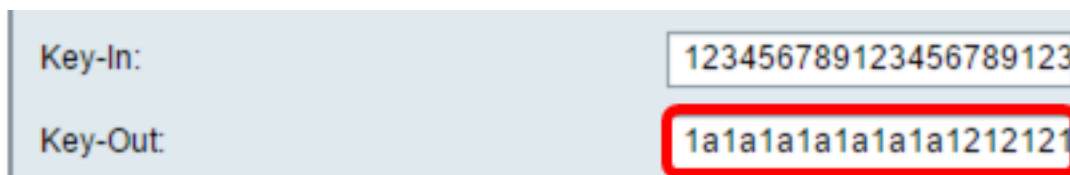
**Hinweis:** In diesem Beispiel wird 123456789123456789123... verwendet.



Screenshot of a configuration interface showing key input fields. The Key-In field contains the value 123456789123456789123 and is highlighted with a red box. The Key-Out field contains the value 1a1a1a1a1a1a1a1a1212121.

Schritt 5: Geben Sie im Feld *Key-Out* (*Tastenbelegung*) einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 3 gewählten Algorithmus ab.

**Hinweis:** In diesem Beispiel wird 1a1a1a1a1a1a1a1a121212.. verwendet.



Screenshot of a configuration interface showing key input fields. The Key-In field contains the value 123456789123456789123. The Key-Out field contains the value 1a1a1a1a1a1a1a1a1212121 and is highlighted with a red box.

[Schritt 6:](#) Wählen Sie eine Option aus der Dropdown-Liste Manual Integrity Algorithm (Manueller Integrity-Algorithmus) aus.

- MD5 - Verwendet einen 128-Bit-Hashwert für Datenintegrität. MD5 ist weniger sicher, aber schneller als SHA-1 und SHA2-256.
- SHA-1 - Verwendet einen 160-Bit-Hashwert für Datenintegrität. SHA-1 ist langsamer, aber sicherer als MD5, und SHA-1 ist schneller, aber weniger sicher als SHA2-256.
- SHA2-256 - Verwendet einen 256-Bit-Hashwert für Datenintegrität. SHA2-256 ist langsamer, aber sicherer als MD5 und SHA-1.

**Hinweis:** In diesem Beispiel wird MD5 gewählt.



Authentication:	<input checked="" type="radio"/> MD5
Key-In	<input type="radio"/> SHA1
Key-Out	<input type="radio"/> SHA2-256

Schritt 7: Geben Sie im *Feld Key-In (Schlüssel)* einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt vom in [Schritt 6](#) gewählten Algorithmus ab.

- MD5 verwendet einen 32-stelligen Schlüssel.
- SHA-1 verwendet einen 40-stelligen Schlüssel.
- SHA2-256 verwendet einen 64-stelligen Schlüssel.

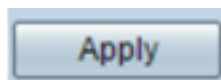
**Hinweis:** In diesem Beispiel wird 123456789123456789123... verwendet.

Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121

Schritt 8: Geben Sie im *Feld "Key-Out"* einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt vom in [Schritt 6](#) gewählten Algorithmus ab.

**Hinweis:** In diesem Beispiel wird 1a1a1a1a1a1a1a1a121212.. verwendet.


Key-In:	123456789123456789123
Key-Out:	1a1a1a1a1a1a1a1a1212121



Schritt 9: Klicken Sie auf .

**Hinweis:** Sie werden zur IPSec-Profiltable zurückgeleitet, und das neu erstellte IPSec-Profil sollte jetzt angezeigt werden.

## IPSec Profiles

 Success. To permanently save the configuration, Go to [Configuration Management page](#) or click Save icon.

IPsec Profiles Table		
Name	Policy	In Use
<input type="radio"/> Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>
<input type="radio"/> Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/> Microsoft_Azure	Auto	<input type="checkbox"/>
<input type="radio"/> IPSec_Vpn	Manual	<input type="checkbox"/>

Schritt 10: (Optional) Um die Konfiguration dauerhaft zu speichern, öffnen Sie die Seite "Copy/Save Configuration" (Konfiguration kopieren/speichern), oder klicken Sie auf das



Symbol oben auf der Seite.

Sie sollten jetzt ein manuelles IPSec-Profil auf einem Router der Serie RV34x erfolgreich konfiguriert haben.