

# Konfigurieren der erweiterten VPN-Einrichtung (Virtual Private Network) auf der RV110W-Firewall

## Ziel

Virtual Private Network (VPN) verwendet das öffentliche Netzwerk oder das Internet, um ein privates Netzwerk für eine sichere Kommunikation einzurichten. Ein Internet Key Exchange (IKE) ist ein Protokoll, das eine sichere Kommunikation zwischen zwei Netzwerken herstellt. Sie wird verwendet, um einen Schlüssel vor dem Datenverkehrsfluss auszutauschen, wodurch die Authentizität für beide Enden des VPN-Tunnels sichergestellt wird.

Beide Enden des VPNs sollten dieselbe VPN-Richtlinie verwenden, um erfolgreich miteinander zu kommunizieren.

In diesem Dokument wird erläutert, wie Sie ein IKE-Profil hinzufügen und die VPN-Richtlinie auf dem RV110W Wireless Router konfigurieren.

## Anwendbare Geräte

·RV110W

## Softwareversion

·1.2.0.9

## IKE-Richtlinieneinstellungen

Internet Key Exchange (IKE) ist ein Protokoll, das verwendet wird, um eine sichere Verbindung für die Kommunikation in einem VPN herzustellen. Diese etablierte, sichere Verbindung wird als Security Association (SA) bezeichnet. In diesem Verfahren wird erläutert, wie Sie eine IKE-Richtlinie für die VPN-Verbindung konfigurieren, die für die Sicherheit verwendet wird. Damit ein VPN ordnungsgemäß funktioniert, müssen die IKE-Richtlinien für beide Endpunkte identisch sein.

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN > Advanced VPN Setup** aus. Die Seite *Advanced VPN Setup* wird geöffnet:

Advanced VPN Setup

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>							

[IPSec Connection Status](#)

**Advanced VPN Setup**

**IKE Policy Table**

<input type="checkbox"/>	Name	Mode	Local	Remote
No data to display				

**Add Row**   **Edit**   **Delete**

**VPN Policy Table**

<input type="checkbox"/>	Status	Name	Type	Local
No data to display				

**Add Row**   **Edit**   **Enable**   **Disable**   **Delete**

**Save**   **Cancel**

**IPSec Connection Status**

Schritt 2: Klicken Sie auf **Zeile hinzufügen**, um eine neue IKE-Richtlinie zu erstellen. Die Seite *Advanced VPN Setup* wird geöffnet:

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

**Save**   **Cancel**   **Back**

Schritt 3: Geben Sie im Feld *Policy Name (Richtliniennamen)* einen Namen für die IKE-Richtlinie ein, um diese leicht zu identifizieren.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode: Main  
Main  
Aggressive

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Schritt 4: Wählen Sie eine Option aus der Dropdown-Liste *Exchange Mode*:

·Main (Hauptmodus): Ermöglicht den sicheren, aber langsameren Betrieb der IKE-Richtlinie als der Modus "Aggressive" (Aggressive Modus). Wählen Sie diese Option aus, wenn eine sicherere VPN-Verbindung erforderlich ist.

·Aggressive (Aggressiv): Ermöglicht den schnelleren, aber weniger sicheren Betrieb der IKE-Richtlinie als im Hauptmodus. Wählen Sie diese Option aus, wenn eine schnellere VPN-Verbindung erforderlich ist.

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm: 

- DES
- 3DES
- AES-128
- AES-192
- AES-256

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Schritt 5: Wählen Sie aus der Dropdown-Liste *Encryption Algorithm* einen Algorithmus aus:

- DES - Data Encryption Standard (DES) verwendet eine 56-Bit-Schlüsselgröße für die Datenverschlüsselung. DES ist veraltet und sollte nur verwendet werden, wenn ein Endpunkt nur DES unterstützt.
- 3DES - Der Triple Data Encryption Standard (3DES) führt DES dreimal durch, variiert jedoch die Schlüssellänge zwischen 168 Bit und 112 Bit und zwischen 112 Bit und 56 Bit, je nach der DES-Runde. 3DES ist sicherer als DES und AES.
- AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller, aber weniger sicher als 3DES, aber einige Hardwaretypen ermöglichen eine schnellere Ausführung von 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.
- AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128, und AES-192 ist schneller, aber weniger sicher als AES-256.
- AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Schritt 6: Wählen Sie die gewünschte Authentifizierung aus der Dropdown-Liste *Authentication Algorithm*:

·MD5 — Message-Digest Algorithm 5 (MD5) verwendet einen 128-Bit-Hashwert für die Authentifizierung. MD5 ist weniger sicher, aber schneller als SHA-1 und SHA2-256.

·SHA-1 - Secure Hash Function 1 (SHA-1) verwendet einen 160-Bit-Hashwert für die Authentifizierung. SHA-1 ist langsamer, aber sicherer als MD5, und SHA-1 ist schneller, aber weniger sicher als SHA2-256.

·SHA2-256 - Secure Hash Algorithm 2 mit einem Hashwert von 256 Bit (SHA2-256) verwendet einen Hashwert von 256 Bit für die Authentifizierung. SHA2-256 ist langsamer, aber sicherer als MD5 und SHA-1.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

**Pre-Shared Key:**

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Schritt 7: Geben Sie im Feld *Vorinstallierter Schlüssel* einen vorinstallierten Schlüssel ein, den die IKE-Richtlinie verwendet.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Schritt 8: Wählen Sie aus der Dropdown-Liste *Diffie-Hellman (DH) Group (DH-Gruppe)* aus, welche DH-Gruppe von IKE verwendet wird. Hosts in einer DH-Gruppe können Schlüssel austauschen, ohne einander zu kennen. Je höher die Bitnummer der Gruppe ist, desto sicherer ist die Gruppe.

·Gruppe 1 - 768 Bit - Der niedrigste Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe. Die Berechnung der IKE-Schlüssel nimmt jedoch weniger Zeit in Anspruch. Diese Option wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.

·Gruppe 2 - 1024 Bit - Der höhere Schlüssel und eine sicherere Authentifizierungsgruppe. Die IKE-Schlüssel müssen jedoch erst nach einiger Zeit berechnet werden.

·Gruppe 5 - 1536 Bit - Stellt den höchsten Stärke-Schlüssel und die sicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert mehr Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit hoch ist.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

Schritt 9: Geben Sie an, wie lange (in Sekunden) eine SA für das VPN dauert, bevor die SA im Feld *SA-Lifetime* verlängert wird.

Schritt 10: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *Dead Peer Detection (Dead-Peer-Erkennung)*, um die Dead Peer Detection (Dead-Peer-Erkennung) zu aktivieren. Die Dead Peer Detection überwacht IKE-Peers, um festzustellen, ob ein Peer nicht mehr funktioniert. Dead Peer Detection verhindert die Verschwendung von Netzwerkressourcen bei inaktiven Peers.

Schritt 11: (Optional) Wenn Sie unter Schritt 9 die Dead Peer Detection aktiviert haben, geben Sie im Feld *Dead Peer Delay (Dead-Peer-Verzögerung)* ein, wie oft (in Sekunden) der Peer auf Aktivitäten überprüft wird.

Schritt 12: (Optional) Wenn Sie unter Schritt 9 die Dead Peer Detection aktiviert haben, geben Sie in das Feld *Dead Peer Detection Timeout (Dead Peer Detection-Timeout)* die Anzahl der Sekunden ein, die gewartet wird, bevor ein inaktiver Peer verworfen wird.

Schritt 13: Klicken Sie auf **Speichern**, um alle Einstellungen zu übernehmen.

## VPN-Richtlinienkonfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **VPN>Advanced VPN Setup** (Erweitertes VPN-Setup). Die Seite *Advanced VPN Setup* wird geöffnet:

Advanced VPN Setup

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
Add Row Edit Delete							

<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
Add Row Edit Enable Disable Delete							

Save Cancel

IPSec Connection Status

Advanced VPN Setup

 Configuration settings have been saved successfully

<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	policy1	Aggressive		
Add Row Edit Delete				

<input type="checkbox"/>	Status	Name	Type	Local
<input type="checkbox"/>	No data to display			
Add Row Edit Enable Disable Delete				

Save Cancel

IPSec Connection Status

Schritt 2: Klicken Sie in der *VPN-Richtlinientabelle* auf Zeile **hinzufügen**. Das Fenster *Advanced VPN Policy Setup* (Erweiterte VPN-Richtlinieneinrichtung) wird angezeigt:

Advanced VPN Setup

### Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:  ▼

Remote Endpoint:  ▼

(Hint: 1.2.3.4 or abc.com)

### Local Traffic Selection

Local IP:  ▼

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

### Remote Traffic Selection

## VPN-Richtlinienkonfiguration hinzufügen/bearbeiten

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

Schritt 1: Geben Sie einen eindeutigen Namen für die Richtlinie im Feld *Policy Name* (*Richtliniennamen*) ein, um sie leicht zu identifizieren.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

Schritt 2: Wählen Sie den entsprechenden Richtlinientyp aus der Dropdown-Liste *Policy Type* (*Richtlinientyp*) aus.

·Auto Policy (Automatische Richtlinie): Die Parameter können automatisch festgelegt werden. In diesem Fall ist es zusätzlich zu den Richtlinien erforderlich, dass das IKE-Protokoll (Internet Key Exchange) zwischen den beiden VPN-Endpunkten ausgehandelt wird.

·Manuelle Richtlinie - In diesem Fall werden alle Einstellungen, die Einstellungen für Schlüssel für den VPN-Tunnel enthalten, für jeden Endpunkt manuell eingegeben.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

Schritt 3: Wählen Sie aus der Dropdown-Liste "Remote Endpoint" den Typ der IP-ID aus, der das Gateway am Remote-Endpunkt identifiziert.

·IP-Adresse - IP-Adresse des Kabelmodems am Remote-Endpunkt. Wenn Sie diese Option wählen, geben Sie die IP-Adresse in das Feld ein.

·FQDN (Fully Qualified Domain Name): Geben Sie den vollqualifizierten Domänennamen des Kabelmodems am Remote-Endpunkt ein. Wenn Sie diese Option wählen, geben Sie den vollqualifizierten Domänennamen in das Feld ein.

## Lokale Datenverkehrsauswahl



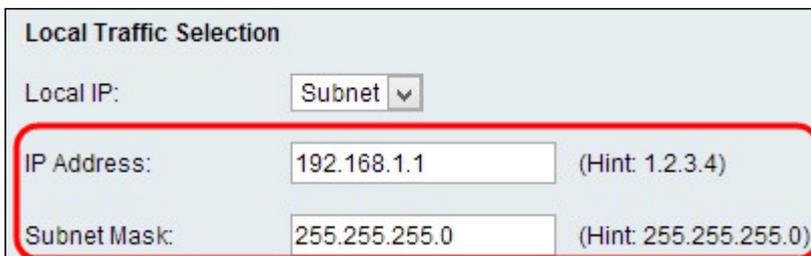
The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is open, with 'Single' selected and highlighted in blue. The 'IP Address:' field is empty, and the 'Subnet Mask:' field is also empty. A red box highlights the dropdown menu.

Schritt 1: Wählen Sie aus der Dropdown-Liste "*Local IP*" (*Lokale IP*) den Typ der ID aus, die Sie für den Endpunkt bereitstellen möchten.



The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is set to 'Single'. The 'IP Address:' field contains the value '192.168.1.1'. The 'Subnet Mask:' field is empty. A red box highlights the 'IP Address:' field.

·Single (Einzel): Dadurch wird die Richtlinie auf einen Host beschränkt. Wenn Sie diese Option wählen, geben Sie die IP-Adresse in das Feld *IP-Adresse* ein.



The screenshot shows the 'Local Traffic Selection' form. The 'Local IP:' dropdown menu is set to 'Subnet'. The 'IP Address:' field contains the value '192.168.1.1'. The 'Subnet Mask:' field contains the value '255.255.255.0'. A red box highlights both the 'IP Address:' and 'Subnet Mask:' fields.

·Subnetz - Dies ist eine Maske, die die Grenzen einer IP definiert. Dadurch können Hosts aus dem angegebenen Subnetz nur eine Verbindung zum VPN herstellen. Um eine VPN-Verbindung herzustellen, wird ein Computer durch einen logischen AND-Vorgang ausgewählt. Ein Computer wird ausgewählt, wenn die IP in den gleichen erforderlichen Bereich fällt. Wenn Sie diese Option wählen, geben Sie die IP-Adresse und das Subnetz in das Feld *IP-Adresse* und *Subnetz* ein.

## RemoteTraffic-Auswahl



The screenshot shows the 'Remote Traffic Selection' form. The 'Remote IP:' dropdown menu is open, with 'Single' selected and highlighted in blue. The 'IP Address:' field is empty, and the 'Subnet Mask:' field is also empty. A red box highlights the dropdown menu.

Schritt 1: Wählen Sie aus der Dropdown-Liste *Local IP* (*Lokale IP*) den Typ der ID aus, die Sie für den Endpunkt bereitstellen möchten:

Remote Traffic Selection	
Remote IP:	Single <input type="button" value="v"/>
IP Address:	192.168.1.5 (Hint: 1.2.3.4)
Subnet Mask:	<input type="text"/> (Hint: 255.255.255.0)

·Single (Einzel): Dadurch wird die Richtlinie auf einen Host beschränkt. Wenn Sie diese Option wählen, geben Sie die IP-Adresse in das Feld *IP-Adresse* ein.

Remote Traffic Selection	
Remote IP:	Subnet <input type="button" value="v"/>
IP Address:	192.168.1.5 (Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)

·Subnetz - Dies ist eine Maske, die die Grenzen einer IP definiert. Dadurch können Hosts aus dem angegebenen Subnetz nur eine Verbindung zum VPN herstellen. Um eine VPN-Verbindung herzustellen, wird ein Computer durch einen logischen AND-Vorgang ausgewählt. Ein Computer wird ausgewählt, wenn die IP in den gleichen erforderlichen Bereich fällt. Wenn Sie diese Option wählen, geben Sie die IP-Adresse und das Subnetz in das Feld *IP-Adresse* und *Subnetz* ein.

## Parameter für manuelle Richtlinien

Um Parameter für die manuelle Richtlinie zu konfigurieren, wählen Sie in der Dropdown-Liste *Policy Type (Richtlinientyp)* in *Schritt 2* des Abschnitts *Konfiguration der VPN-Richtlinie* hinzufügen/bearbeiten aus.

Manual Policy Parameters	
SPI-Incoming:	014C
SPI-Outgoing:	014C
Encryption Algorithm:	AES-128 <input type="button" value="v"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	SHA-1 <input type="button" value="v"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

Schritt 1: Geben Sie im Feld *SPI-Incoming (SPI-Eingang)* einen Hexadezimalwert zwischen 3 und 8 ein. Stateful Packet Inspection (SPI) ist eine Technologie, die als Deep Packet Inspection (Deep Packet Inspection) bezeichnet wird. SPI implementiert eine Reihe von Sicherheitsfunktionen, die dazu beitragen, Ihr Computernetzwerk sicher zu halten. Der Wert für den SPI-Eingang entspricht dem SPI-Ausgang des vorherigen Geräts. Jeder Wert ist akzeptabel, vorausgesetzt, der Remote-VPN-Endpunkt hat in seinem *SPI-Outgoing*-Feld den gleichen Wert.

Schritt 2: Geben Sie im Feld *SPI-Outgoing (SPI-Ausgang)* einen Hexadezimalwert zwischen 3 und 8 ein.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

- 3DES
- DES
- AES-128
- AES-192
- AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Schritt 3: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus den entsprechenden Verschlüsselungsalgorithmus aus.

·DES - Data Encryption Standard (DES) verwendet eine 56-Bit-Schlüsselgröße für die Datenverschlüsselung. DES ist veraltet und sollte nur verwendet werden, wenn ein Endpunkt nur DES unterstützt.

·3DES - Der Triple Data Encryption Standard (3DES) führt DES dreimal durch, variiert jedoch die Schlüssellänge von 168 Bit bis 112 Bit und von 112 Bit bis 56 Bit je nach der DES-Runde. 3DES ist sicherer als DES und AES.

·AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller, aber weniger sicher als 3DES, aber einige Hardwaretypen ermöglichen eine schnellere Ausführung von 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.

·AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128, und AES-192 ist schneller, aber weniger sicher als AES-256.

·AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

**Key-In:**

**Key-Out:**

Integrity Algorithm:

Key-In:

Key-Out:

Schritt 4: Geben Sie den Verschlüsselungsschlüssel der eingehenden Richtlinie in das Feld *Key-In* ein. Die Länge des Schlüssels hängt von dem in Schritt 3 gewählten Algorithmus ab.

Schritt 5: Geben Sie im Feld *Key-Out* den Verschlüsselungsschlüssel der Richtlinie für ausgehenden Datenverkehr ein.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Schritt 6: Wählen Sie den entsprechenden Integritätsalgorithmus aus der Dropdown-Liste *Integrity Algorithm* aus. Dieser Algorithmus überprüft die Integrität der Daten:

·MD5: Dieser Algorithmus gibt die Schlüssellänge auf 16 Zeichen an. Message-Digest Algorithm Five (MD5) ist nicht kollisionssicher und eignet sich für Anwendungen wie SSL-Zertifikate oder digitale Signaturen, die auf dieser Eigenschaft basieren. MD5 komprimiert jeden Byte-Stream in einen 128-Bit-Wert, SHA komprimiert ihn jedoch in einen 160-Bit-Wert. MD5 ist etwas preiswerter zu berechnen, MD5 ist jedoch eine ältere Version des Hash-Algorithmus und ist anfällig für Kollisionsangriffe.

·SHA1 — Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5, aber die Berechnung dauert länger.

·SHA2-256: Dieser Algorithmus gibt die Schlüssellänge auf 32 Zeichen an.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:  ▼

Key-In:

Key-Out:

Integrity Algorithm:  ▼

**Key-In:**

**Key-Out:**

Schritt 7: Geben Sie den Integritätsschlüssel (für ESP mit Integrity-Modus) für die eingehende Richtlinie ein. Die Länge des Schlüssels hängt von dem in Schritt 6 gewählten Algorithmus ab.

Schritt 8: Geben Sie den Integritätsschlüssel der Richtlinie für ausgehenden Datenverkehr in das Feld "Key-Out" ein. Die VPN-Verbindung ist für den ausgehenden an den eingehenden Datenverkehr eingerichtet. Daher müssen die ausgehenden Schlüssel eines Endgeräts mit den eingehenden Schlüsseln am anderen Ende übereinstimmen.

**Hinweis:** Für eine erfolgreiche Verbindung müssen SPI-Eingangs- und Ausgangs-, Verschlüsselungs-Algorithmus, Integrity Algorithm und Keys am anderen Ende des VPN-Tunnels identisch sein.

## Parameter für die automatische Richtlinie

**Auto Policy Parameters**

**SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 28800)**

Encryption Algorithm:  ▼

Integrity Algorithm:  ▼

PFS Key Group:  Enable

▼

Select IKE Policy:  ▼

Schritt 1: Geben Sie die Dauer der Sicherheitszuordnung (Security Association, SA) in Sekunden im Feld SA Lifetime (SA-Lebensdauer) ein. Die SA-Lebensdauer ist, wenn ein Schlüssel seine Lebensdauer erreicht hat. Alle zugehörigen SAs werden automatisch neu verhandelt.

Schritt 2: Wählen Sie den entsprechenden Verschlüsselungsalgorithmus aus der Dropdown-Liste Verschlüsselungsalgorithmus aus:

- DES - Data Encryption Standard (DES) verwendet eine 56-Bit-Schlüsselgröße für die Datenverschlüsselung. DES ist veraltet und sollte nur verwendet werden, wenn ein Endpunkt nur DES unterstützt.

- 3DES - Der Triple Data Encryption Standard (3DES) führt DES dreimal durch, variiert jedoch die Schlüssellänge von 168 Bit bis 112 Bit und von 112 Bit bis 56 Bit je nach der DES-Runde. 3DES ist sicherer als DES und AES.

- AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller, aber weniger sicher als 3DES, aber einige Hardwaretypen ermöglichen eine schnellere Ausführung von 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.

- AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128, und AES-192 ist schneller, aber weniger sicher als AES-256.

- AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 3: Wählen Sie in der Dropdown-Liste Integrity Algorithm (Integritätsalgorithmus) den entsprechenden Integrationsalgorithmus aus. Dieser Algorithmus überprüft die Integrität der Daten.

·MD5: Dieser Algorithmus gibt die Schlüssellänge auf 16 Zeichen an. Message-Digest Algorithm Five (MD5) ist nicht kollisionssicher und eignet sich für Anwendungen wie SSL-Zertifikate oder digitale Signaturen, die auf dieser Eigenschaft basieren. MD5 komprimiert jeden Byte-Stream in einen 128-Bit-Wert, SHA komprimiert ihn jedoch in einen 160-Bit-Wert. MD5 ist etwas preiswerter zu berechnen, MD5 ist jedoch eine ältere Version des Hash-Algorithmus und ist anfällig für Kollisionsangriffe.

·SHA1 — Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5, aber die Berechnung dauert länger.

·SHA2-256: Dieser Algorithmus gibt die Schlüssellänge auf 32 Zeichen an.

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Schritt 4: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im *PFS-Feld Schlüsselgruppe*, um Perfect Forward Secrecy (Perfekte Weiterleitungsgeheimnis) zu aktivieren, um die Sicherheit zu verbessern.

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

Schritt 5: Wenn Sie in Schritt 4 **Aktivieren** aktiviert haben, wählen Sie den entsprechenden Diffie-Hellman-Schlüsselaustausch aus der Dropdown-Liste *PFS Key Group* (Feld *PFS-Schlüsselgruppe*) aus.

·Gruppe 1 - 768 Bit - Stellt den niedrigsten Stärke-Schlüssel und die unsicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert jedoch weniger Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit niedrig ist.

·Gruppe 2 - 1024 Bit - Stellt einen leistungsfähigeren Schlüssel und eine sicherere Authentifizierungsgruppe dar. Die IKE-Schlüssel müssen jedoch erst nach einiger Zeit berechnet werden.

·Gruppe 5 - 1536 Bit - Stellt den höchsten Stärke-Schlüssel und die sicherste Authentifizierungsgruppe dar. Die Berechnung der IKE-Schlüssel erfordert mehr Zeit. Es wird empfohlen, wenn die Netzwerkgeschwindigkeit hoch ist.

**Auto Policy Parameters**

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable  
DH-Group 1(768 bit)

Select IKE Policy: policy1 (selected)  
policy1  
view

Schritt 6: Wählen Sie die entsprechende IKE-Richtlinie aus der Dropdown-Liste *Select IKE Policy (IKE-Richtlinie auswählen)* aus. Internet Key Exchange (IKE) ist ein Protokoll, das verwendet wird, um eine sichere Verbindung für die Kommunikation in einem VPN herzustellen. Diese etablierte, sichere Verbindung wird als Security Association (SA) bezeichnet. Damit ein VPN ordnungsgemäß funktioniert, müssen die IKE-Richtlinien für beide Endpunkte identisch sein.

Schritt 7: Klicken Sie auf **Speichern**, um alle Einstellungen zu übernehmen.

**Hinweis:** Für eine erfolgreiche Verbindung müssen SA-Lifetime, Encryption Algorithm, Integrity Algorithm, PFS Key Group und die IKE Policy am anderen Ende des VPN-Tunnels identisch sein.

Wenn Sie weitere Artikel zur RV110W anzeigen möchten, klicken Sie [hier](#).