Konfigurieren der erweiterten VPN-Einrichtung auf einem RV130- oder RV130W-Router

Ziel

Ein Virtual Private Network (VPN) ist eine sichere Verbindung, die innerhalb eines Netzwerks oder zwischen Netzwerken hergestellt wird. VPNs dienen dazu, den Datenverkehr zwischen angegebenen Hosts und Netzwerken vom Datenverkehr nicht autorisierter Hosts und Netzwerke zu isolieren. Ein Site-to-Site (Gateway-to-Gateway)-VPN verbindet ganze Netzwerke miteinander. Die Sicherheit wird dadurch gewährleistet, dass ein Tunnel über eine öffentliche Domäne (das Internet) erstellt wird. Jeder Standort benötigt nur eine lokale Verbindung zum gleichen öffentlichen Netzwerk, wodurch Kosten für lange private Mietleitungen eingespart werden−.

VPNs sind für Unternehmen insofern von Vorteil, als sie hochgradig skalierbar sind, die Netzwerktopologie vereinfachen und die Produktivität steigern, da sie die Reisezeit und die Kosten für Remote-Benutzer verringern.

Internet Key Exchange (IKE) ist ein Protokoll zum Herstellen einer sicheren Verbindung für die Kommunikation in einem VPN. Diese sichere Verbindung wird als Sicherheitszuordnung (Security Association, SA) bezeichnet. Sie können IKE-Richtlinien erstellen, um die in diesem Prozess zu verwendenden Sicherheitsparameter wie Peer-Authentifizierung, Verschlüsselungsalgorithmen usw. zu definieren. Damit ein VPN ordnungsgemäß funktioniert, sollten die IKE-Richtlinien für beide Endpunkte identisch sein.

In diesem Artikel wird erläutert, wie die erweiterte VPN-Einrichtung auf einem RV130- oder RV130W-Router konfiguriert wird. Dabei werden die IKE-Richtlinieneinstellungen und die VPN-Richtlinieneinstellungen behandelt.

Unterstützte Geräte

- RV130
- RV130W

Software-Version

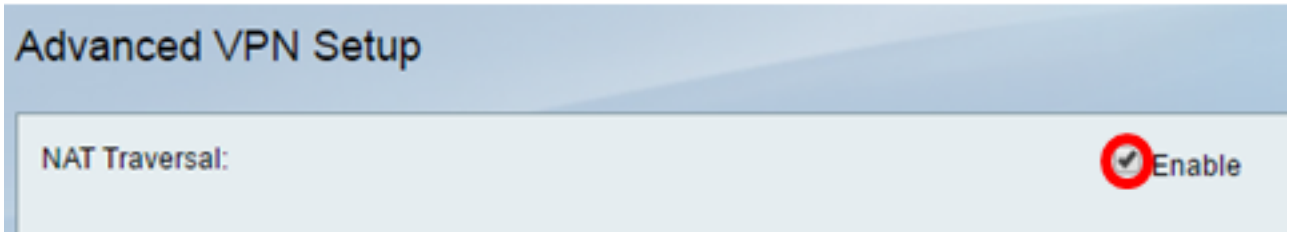
- 1.0.3.22

Erweiterte VPN-Einrichtung konfigurieren

IKE-Richtlinieneinstellungen (Internet Key Exchange) hinzufügen/bearbeiten

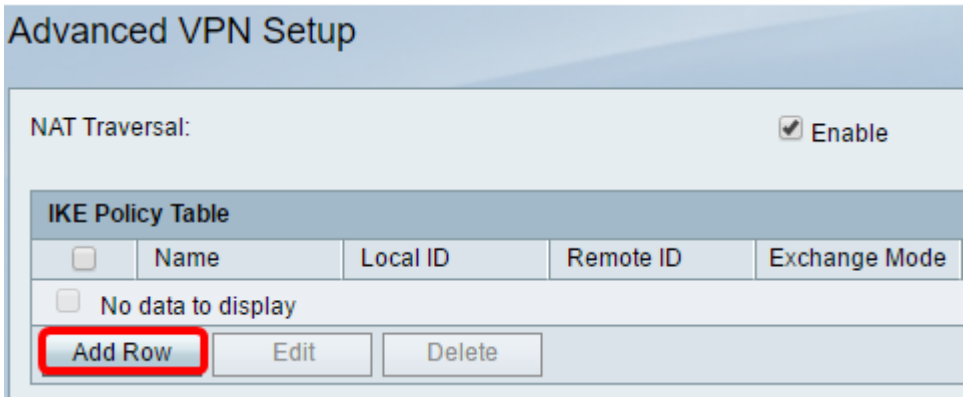
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup**.

Schritt 2. (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** in NAT Traversal, wenn Sie Network Address Translation (NAT) Traversal für die VPN-Verbindung aktivieren möchten. NAT-Traversal ermöglicht die Herstellung einer VPN-Verbindung zwischen Gateways, die NAT verwenden. Wählen Sie diese Option, wenn Ihre VPN-Verbindung über ein NAT-aktiviertes Gateway verläuft.



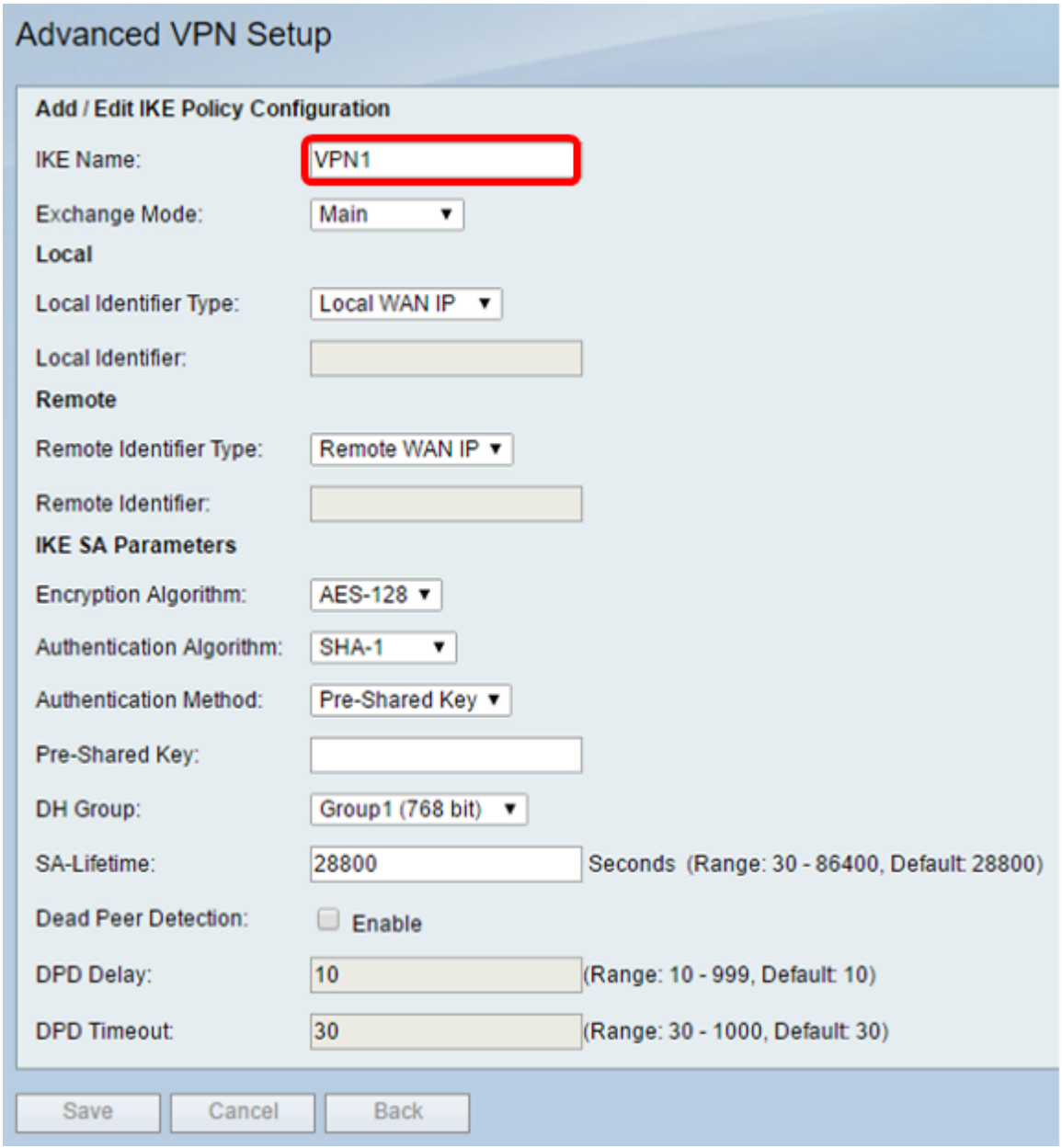
Schritt 3: Klicken Sie in der IKE-Richtlinientabelle auf **Zeile hinzufügen,** um eine neue IKE-Richtlinie zu erstellen.

Anmerkung: Wenn die grundlegenden Einstellungen konfiguriert wurden, enthält die folgende Tabelle die erstellten grundlegenden VPN-Einstellungen. Sie können eine vorhandene IKE-Richtlinie bearbeiten, indem Sie das Kontrollkästchen für die Richtlinie aktivieren und auf **Bearbeiten** klicken. Die Seite für die erweiterte VPN-Einrichtung ändert sich:



Schritt 4: Geben Sie im Feld *IKE*-Name einen eindeutigen Namen für die IKE-Richtlinie ein.

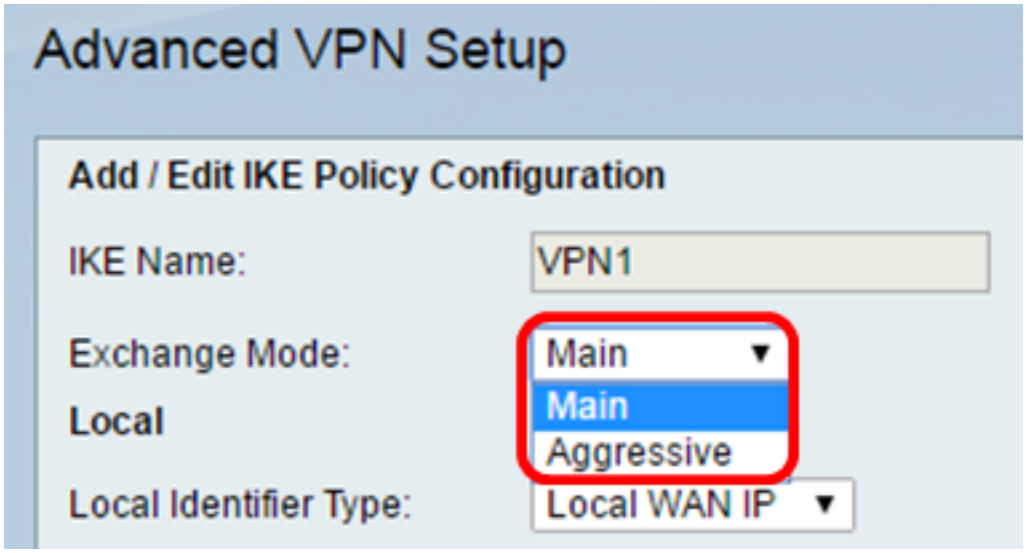
Anmerkung: Wenn die Grundeinstellungen konfiguriert wurden, wird der erstellte Verbindungsname als IKE-Name festgelegt. In diesem Beispiel ist VPN1 der ausgewählte IKE-Name.



Schritt 5: Wählen Sie in der Dropdown-Liste "Exchange Mode" eine Option aus.

- Main (Hauptmodus): Diese Option ermöglicht der IKE-Richtlinie, den VPN-Tunnel mit höherer Sicherheit als im aggressiven Modus auszuhandeln. Klicken Sie auf diese Option, wenn eine sicherere VPN-Verbindung Vorrang vor einer Verhandlungsgeschwindigkeit hat.
- Aggressive (Aggressiv) - Mit dieser Option kann die IKE-Richtlinie eine schnellere, aber weniger sichere Verbindung herstellen als der Hauptmodus. Klicken Sie auf diese Option, wenn eine schnellere VPN-Verbindung Vorrang vor einer hohen Sicherheit hat.

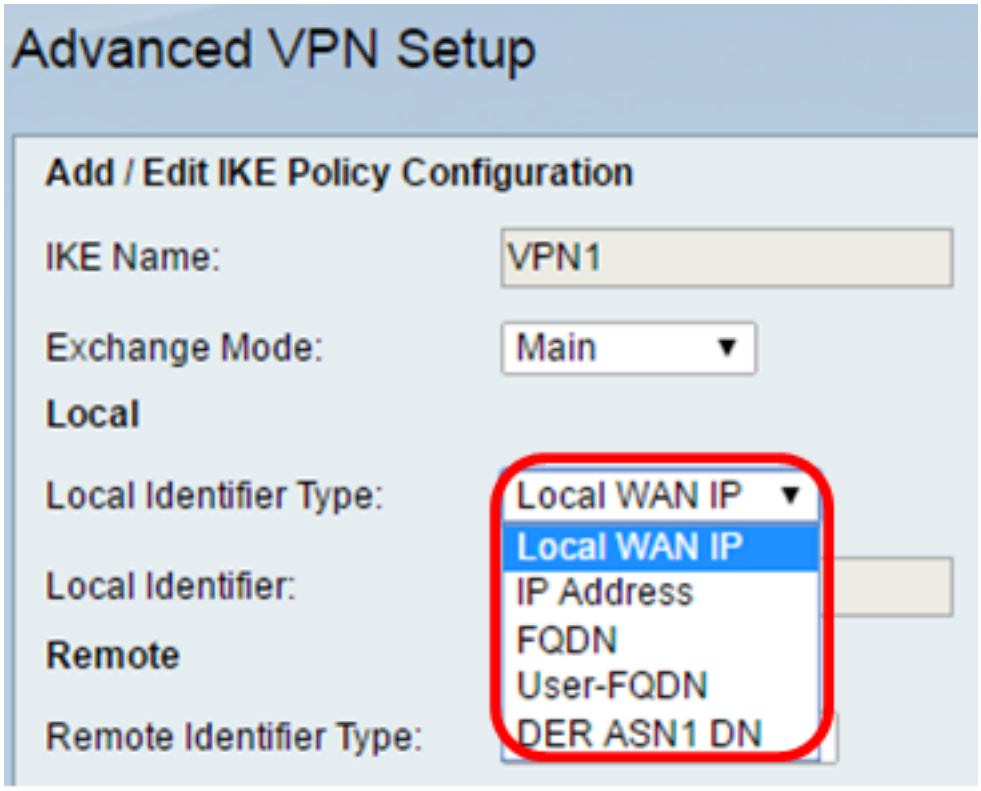
Anmerkung: In diesem Beispiel wird Main ausgewählt.



Schritt 6: Wählen Sie aus der Dropdown-Liste Local Identifier Type (Lokaler Identifizierertyp) die Internet Security Association and Key Management Protocol (ISAKMP) des lokalen Routers aus, um diese zu identifizieren oder anzugeben. Folgende Optionen sind verfügbar:

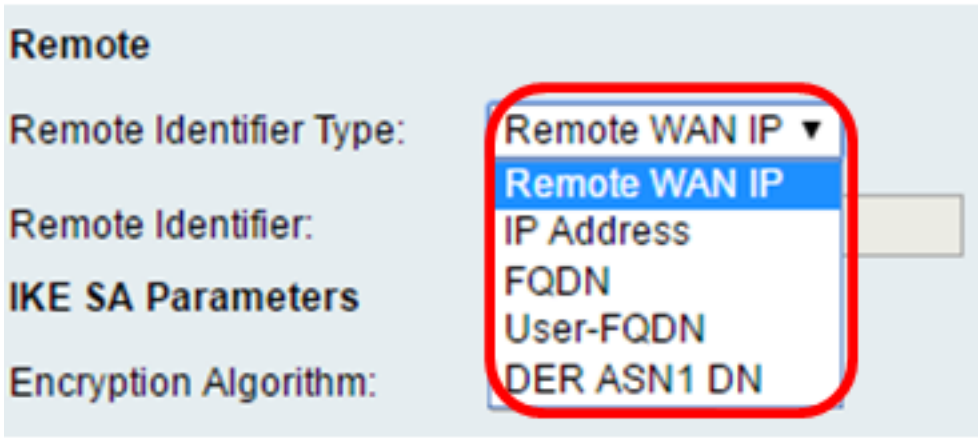
- Lokale WAN-IP - Der Router verwendet die WAN-IP (Local Wide Area Network) als Hauptbezeichner. Diese Option stellt eine Verbindung über das Internet her. Durch Auswahl dieser Option wird das Feld *Lokale Kennung* unten deaktiviert.
- IP-Adresse - Wenn Sie auf diese Schaltfläche klicken, können Sie eine IP-Adresse in das Feld *Lokaler Bezeichner* eingeben.
- FQDN - Ein FQDN (Fully Qualified Domain Name) oder Ihr Domänenname wie http://www.example.com ermöglicht Ihnen, Ihren Domänennamen oder Ihre IP-Adresse in das Feld *Local Identifier (Lokale Kennung)* einzugeben.
- Benutzer-FQDN — Diese Option ist eine Benutzer-E-Mail-Adresse wie user@email.com. Geben Sie einen Domänennamen oder eine IP-Adresse in das Feld *Lokale ID ein*.
- DER ASN1 DN: Diese Option ist ein Bezeichnungstyp für den Distinguished Name (DN), der zur Übertragung von Informationen die Distinguished Encoding Rules Abstract Syntax Notation One (DER ASN1) verwendet. Dies geschieht, wenn der VPN-Tunnel einem Benutzerzertifikat zugeordnet ist. Wenn diese Option ausgewählt ist, geben Sie einen Domänennamen oder eine IP-Adresse in das Feld *Lokale ID ein*.

Anmerkung: In diesem Beispiel wird Local WAN IP (Lokale WAN-IP) ausgewählt.



Schritt 7: Wählen Sie in der Dropdown-Liste "Remote Identifier Type" (Remote-Identifizierertyp) die Option aus, die Internet Security Association and Key Management Protocol (ISAKMP) des Remote-Routers zu identifizieren oder anzugeben. Die Optionen sind Remote-WAN-IP, IP-Adresse, FQDN, Benutzer-FQDN und DER ASN1 DN.

Anmerkung: In diesem Beispiel wird Remote WAN IP ausgewählt.



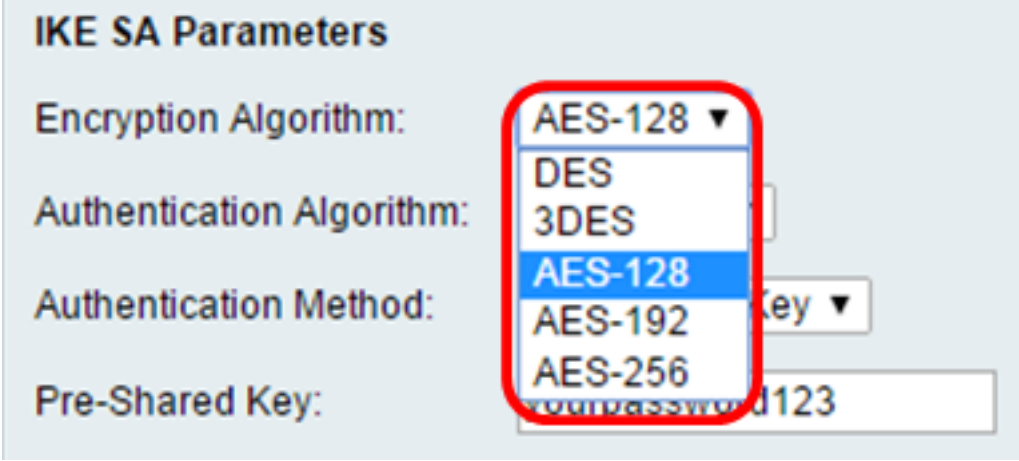
Schritt 8: Wählen Sie eine Option aus der Dropdown-Liste Verschlüsselungsalgorithmus.

- DES - Data Encryption Standard (DES) ist eine alte 56-Bit-Verschlüsselungsmethode, die keine besonders sichere Verschlüsselungsmethode ist, aber möglicherweise für die Abwärtskompatibilität erforderlich ist.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode zur Erhöhung der Schlüssellänge, da sie die Daten dreimal verschlüsselt. Dies bietet mehr Sicherheit als DES, aber weniger Sicherheit als AES.
- AES-128: Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für die AES-Verschlüsselung. AES ist schneller und sicherer als DES. Generell ist AES auch schneller und sicherer als 3DES. AES-128 ist der Standard-

Verschlüsselungsalgorithmus, der schneller, aber weniger sicher als AES-192 und AES-256 ist.

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

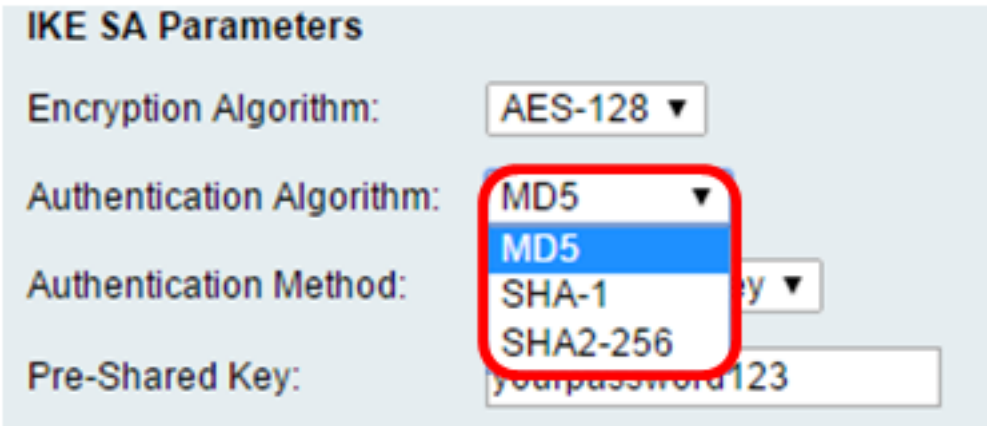
Anmerkung: In diesem Beispiel ist AES-128 ausgewählt.



Schritt 9: Wählen Sie aus der Dropdown-Liste "Authentifizierungsalgorithmus" eine der folgenden Optionen aus:

- MD5 - Message Digest 5 (MD5) ist ein Authentifizierungsalgorithmus, der einen 128-Bit-Hashwert für die Authentifizierung verwendet. MD5 ist weniger sicher, aber schneller als SHA-1 und SHA2-256.
- SHA-1: SHA-1 (Secure Hash Function 1) verwendet einen 160-Bit-Hash-Wert für die Authentifizierung. SHA-1 ist langsamer, aber sicherer als MD5. SHA-1 ist der Standardauthentifizierungsalgorithmus und schneller, aber weniger sicher als SHA2-256.
- SHA2-256: Secure Hash Algorithm 2 mit einem 256-Bit-Hash-Wert (SHA2-256) verwendet einen 256-Bit-Hash-Wert für die Authentifizierung. SHA2-256 ist langsamer, aber sicherer als MD5 und SHA-1.

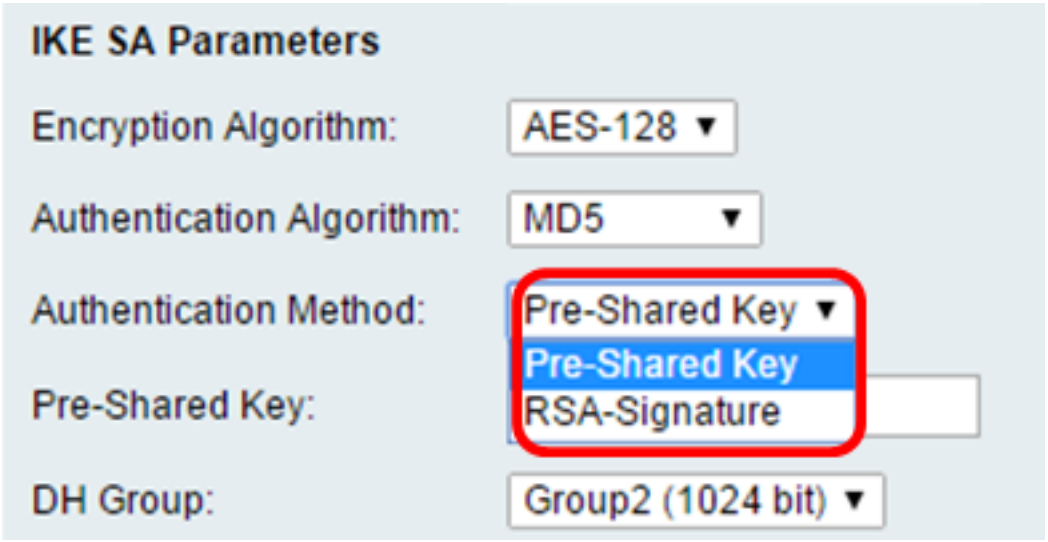
Anmerkung: In diesem Beispiel wird MD5 ausgewählt.



Schritt 10: Wählen Sie in der Dropdown-Liste "Authentifizierungsmethode" eine der folgenden Optionen aus:

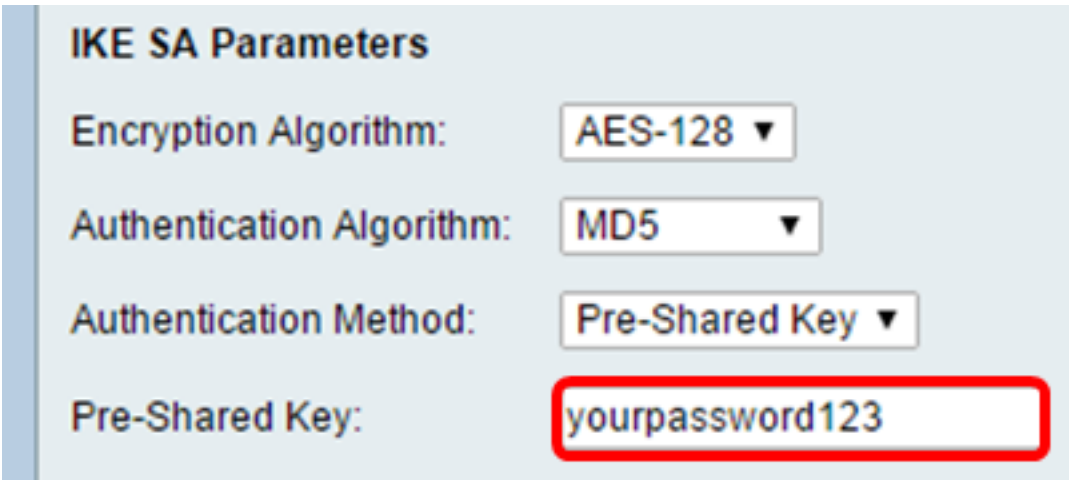
- Pre-Shared Key (Vorläufiger gemeinsamer Schlüssel) - Für diese Option ist ein Kennwort erforderlich, das gemeinsam mit dem IKE-Peer genutzt wird.
- RSA-Signature — Diese Option verwendet Zertifikate zur Authentifizierung der Verbindung. Wenn diese Option ausgewählt ist, ist das Feld für den vorinstallierten Schlüssel deaktiviert. Fahren Sie mit Schritt 12 fort.

Anmerkung: In diesem Beispiel wird der vorinstallierte Schlüssel ausgewählt.



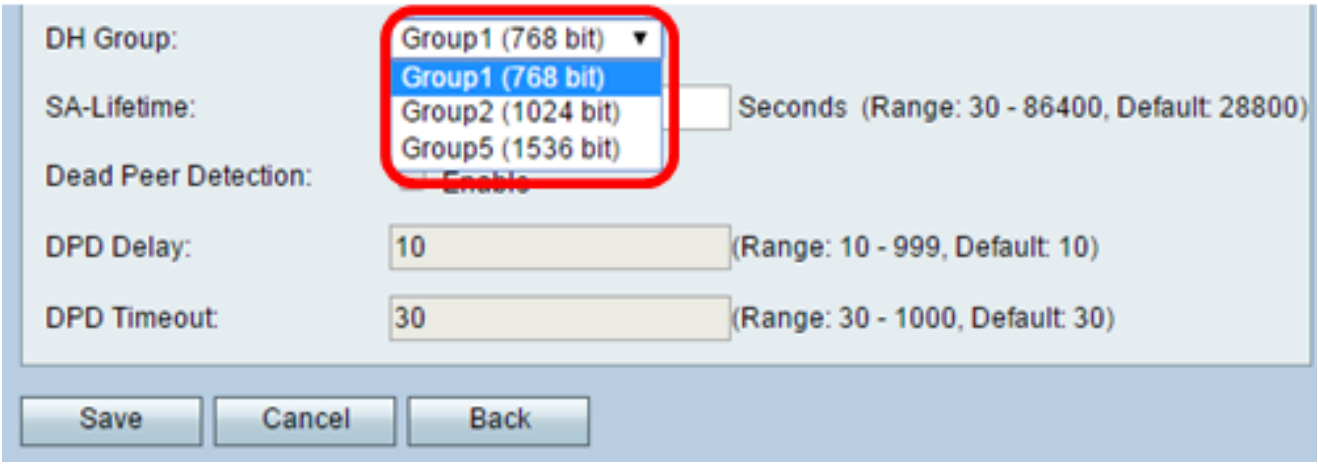
Schritt 11: Geben Sie im Feld "*Pre-Shared Key*" ein Kennwort mit einer Länge zwischen 8 und 49 Zeichen ein.

Anmerkung: In diesem Beispiel wird password123 verwendet.

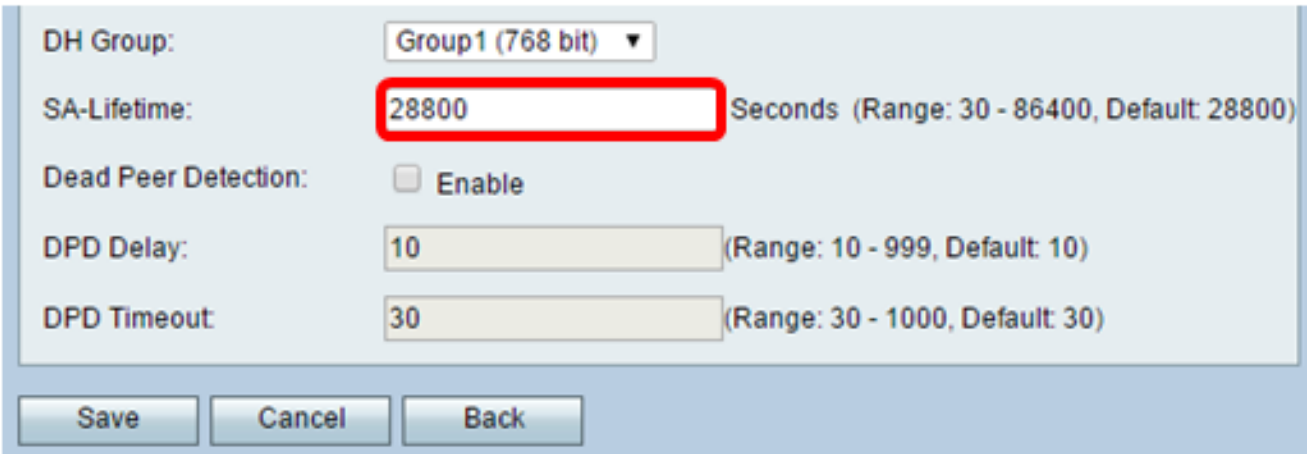


Schritt 12: Wählen Sie aus der Dropdown-Liste "DH Group" (DH-Gruppe) den von IKE verwendeten Diffie-Hellman-Gruppenalgorithmus (DH-Gruppenalgorithmus) aus. Hosts in einer DH-Gruppe können Schlüssel austauschen, ohne sich gegenseitig zu kennen. Je höher die Gruppenbitzahl, desto besser die Sicherheit.

Anmerkung: In diesem Beispiel wird Group1 ausgewählt.

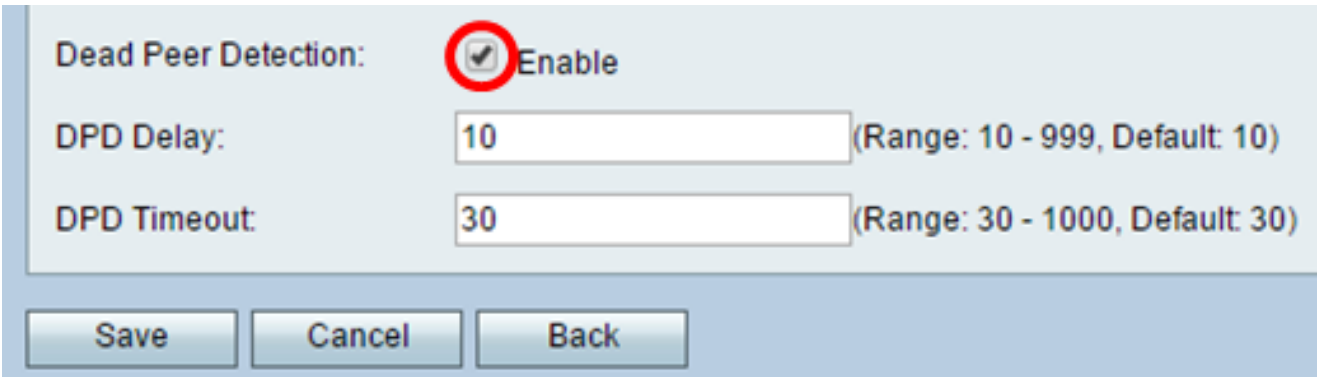


Schritt 13: Geben Sie im Feld *SA-Lifetime (SA-Lebensdauer*) an, wie lange (in Sekunden) eine SA für das VPN dauert, bevor die SA erneuert wird. Der Bereich liegt zwischen 30 und 86400 Sekunden. Der Standardwert ist 28800.



Schritt 14: Aktivieren Sie das Kontrollkästchen Dead Peer Detection (DPD) **aktivieren**. Die DPD überwacht IKE-Peers, um festzustellen, ob ein Peer nicht mehr funktioniert oder noch aktiv ist. Wenn der Peer als ausgefallen erkannt wird, löscht das Gerät die IPsec- und IKE-Sicherheitszuordnung. DPD verhindert die Verschwendung von Netzwerkressourcen für inaktive Peers.

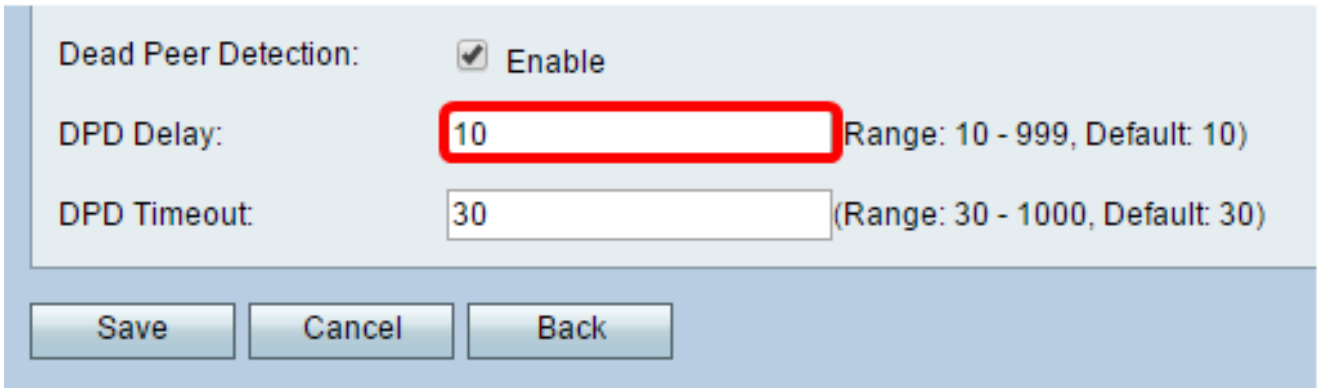
Anmerkung: Wenn Sie die Dead Peer Detection nicht aktivieren möchten, fahren Sie mit Schritt 17 fort.



Schritt 15. (Optional) Wenn Sie DPD in Schritt 14 aktiviert haben, geben Sie in das Feld *DPD-Verzögerung* ein, wie oft (in Sekunden) der Peer auf Aktivitäten überprüft wird.

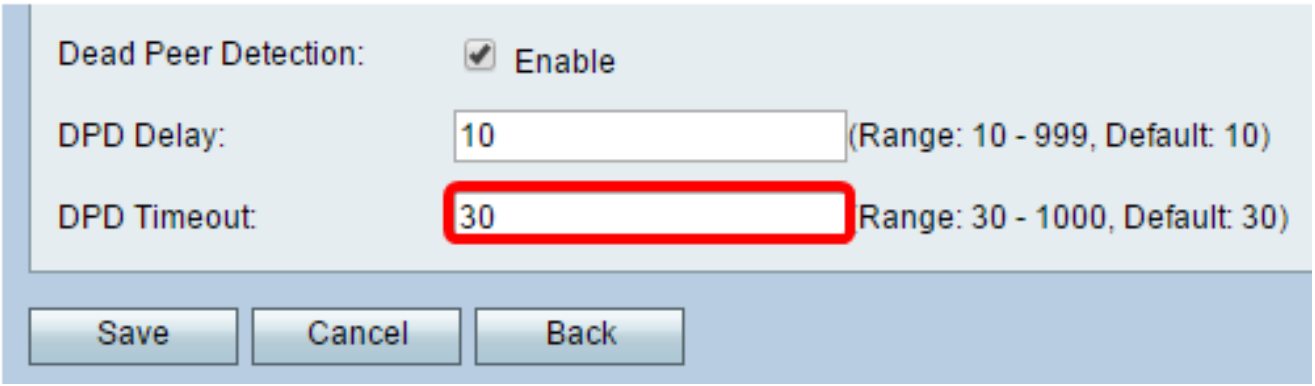
Anmerkung: Die DPD-Verzögerung ist das Intervall in Sekunden zwischen aufeinander

folgenden DPD R-U-THERE-Nachrichten. DPD R-U-THERE-Nachrichten werden nur gesendet, wenn der IPsec-Datenverkehr inaktiv ist. Der Standardwert ist 10.

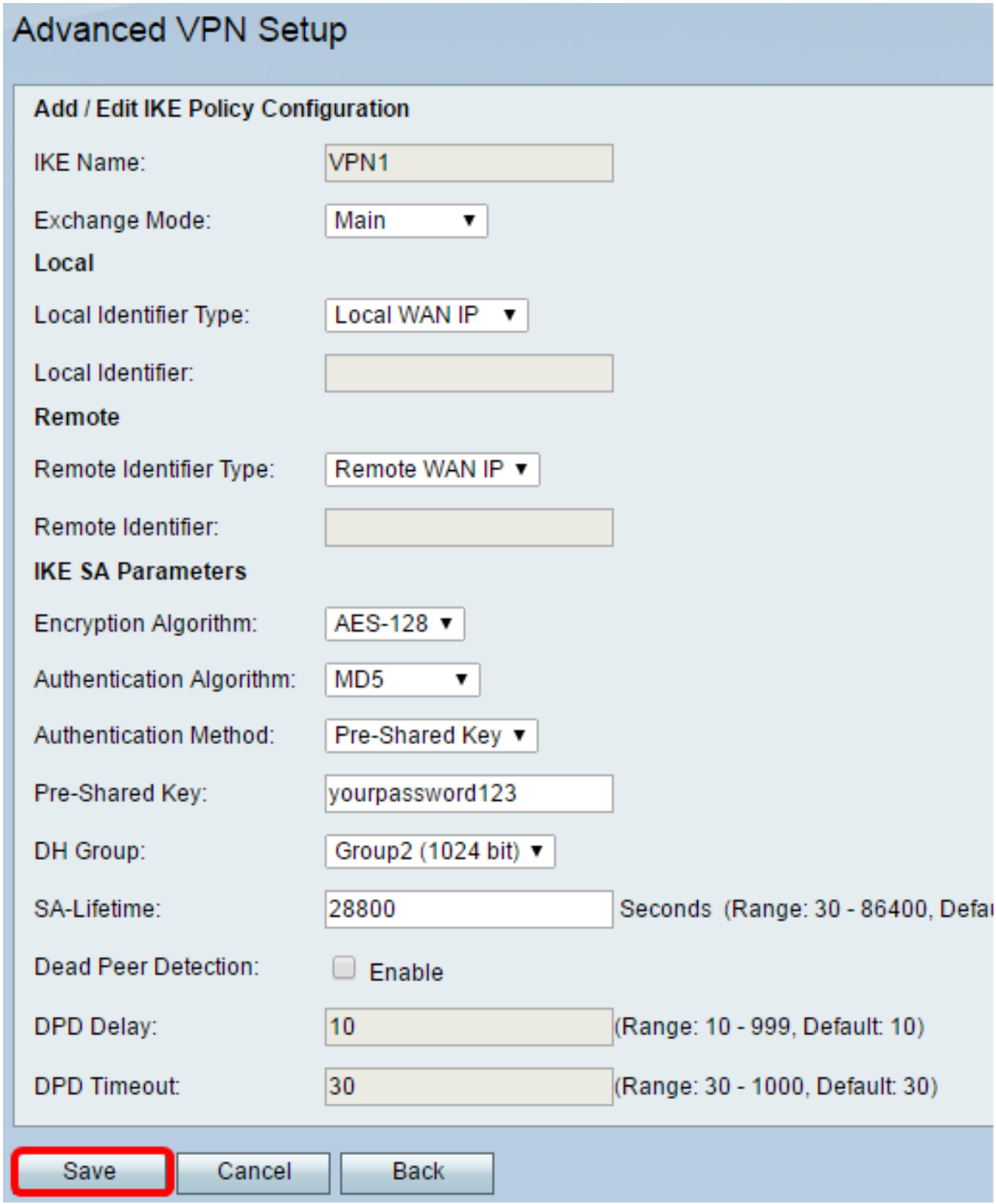


Schritt 16. (Optional) Wenn Sie DPD in Schritt 14 aktiviert haben, geben Sie im Feld *DPD-Zeitüberschreitung* an, wie viele Sekunden gewartet werden soll, bis ein inaktiver Peer gelöscht wird.

Anmerkung: Dies ist die maximale Zeit, die das Gerät auf den Empfang einer Antwort auf die DPD-Nachricht warten darf, bevor es den Peer als ausgefallen betrachtet. Der Standardwert ist 30.



Schritt 17: Klicken Sie auf **Speichern**.



Anmerkung: Die Hauptseite für die erweiterte VPN-Einrichtung wird erneut angezeigt.

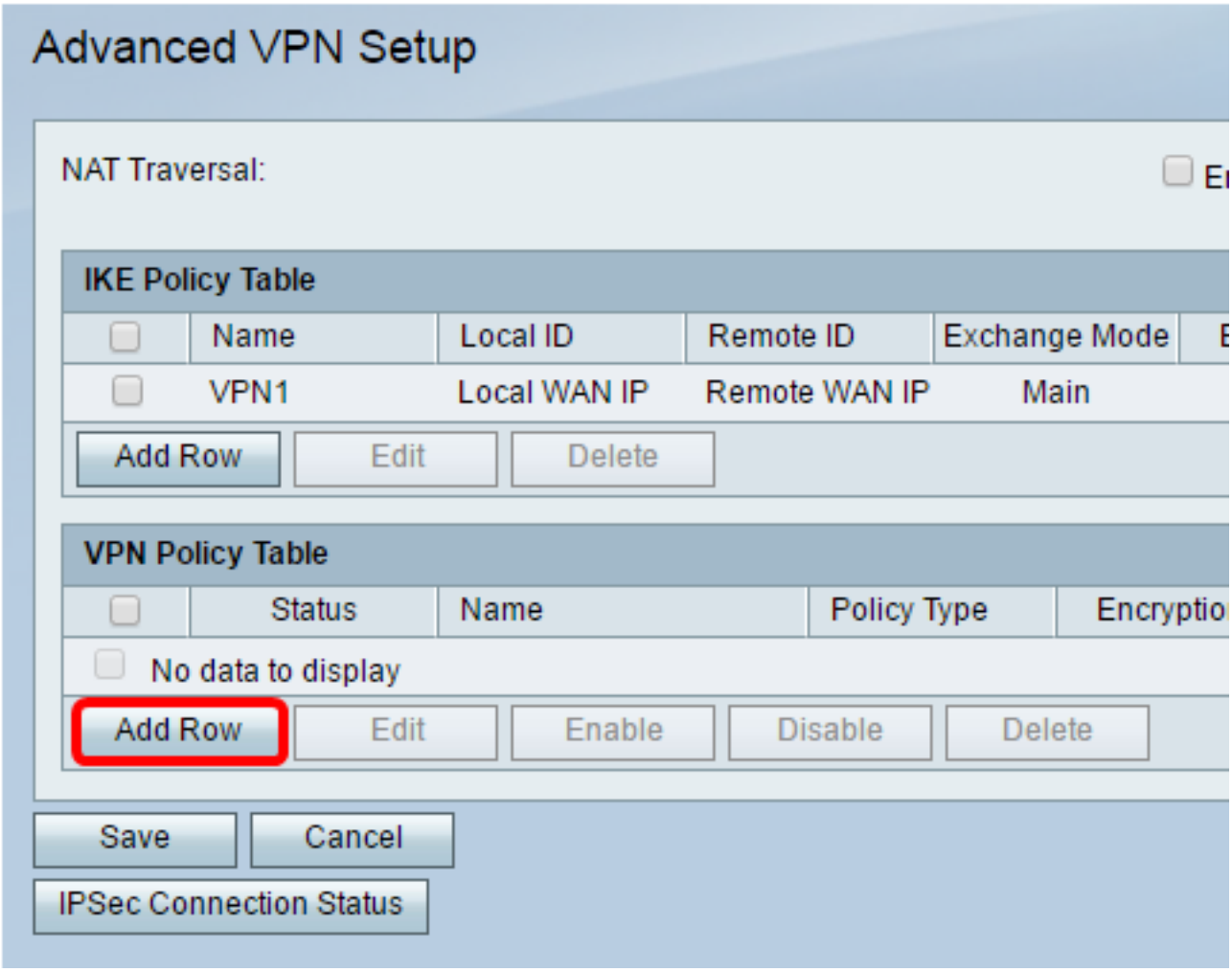
Sie sollten jetzt die IKE-Richtlinieneinstellungen auf Ihrem Router erfolgreich konfiguriert haben.

VPN-Richtlinieneinstellungen konfigurieren

Hinweis: Damit ein VPN ordnungsgemäß funktioniert, sollten die VPN-Richtlinien für beide Endpunkte identisch sein.

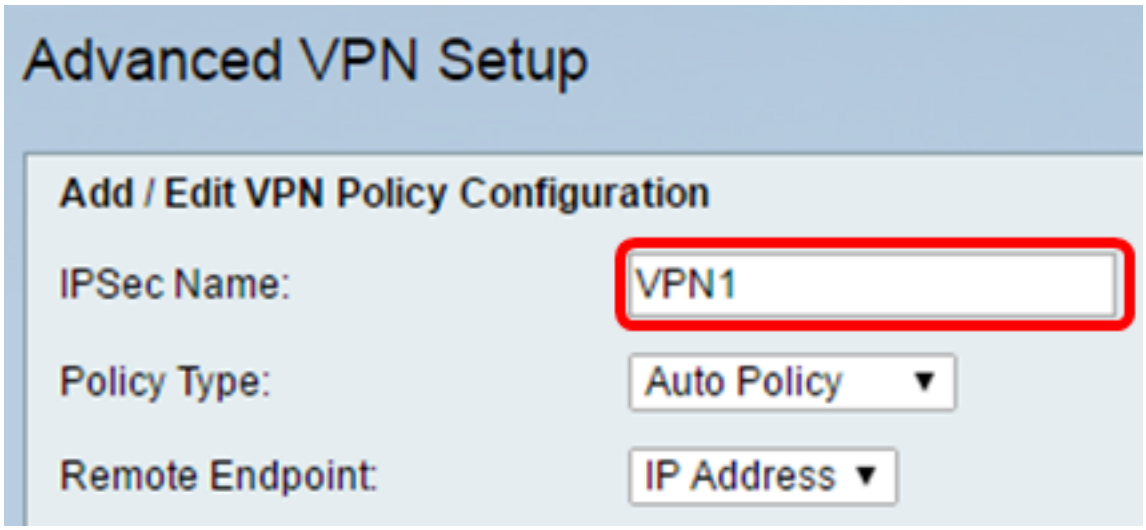
Schritt 1: Klicken Sie in der VPN-Richtlinientabelle auf **Zeile hinzufügen,** um eine neue VPN-Richtlinie zu erstellen.

Anmerkung: Sie können eine VPN-Richtlinie auch bearbeiten, indem Sie das Kontrollkästchen für die Richtlinie aktivieren und auf **Bearbeiten** klicken. Die Seite "Advanced VPN Setup" wird angezeigt:



Schritt 2: Geben Sie im Feld *IPSec-Name* unter dem Bereich "VPN-Konfiguration hinzufügen/bearbeiten" einen Namen für die VPN-Richtlinie ein.

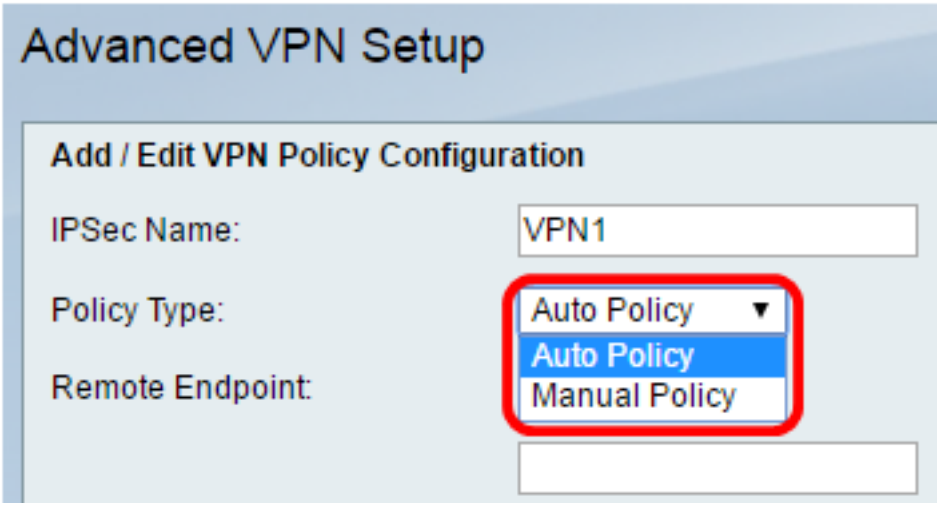
Anmerkung: In diesem Beispiel wird VPN1 verwendet.



Schritt 3: Wählen Sie in der Dropdown-Liste Richtlinientyp eine Option aus.

- Manual Policy (Manuelle Richtlinie) - Mit dieser Option können Sie die Schlüssel für Datenverschlüsselung und -integrität für den VPN-Tunnel manuell konfigurieren. Wenn diese Option ausgewählt ist, werden die Konfigurationseinstellungen im Bereich "Parameter für manuelle Richtlinien" aktiviert. Fahren Sie mit den Schritten bis zur Auswahl des Remote-Datenverkehrs fort. Klicken Sie hier, um die Schritte zu erfahren.
- Automatische Richtlinie - Richtlinienparameter werden automatisch festgelegt. Diese Option verwendet eine IKE-Richtlinie für die Datenintegrität und den Austausch von Verschlüsselungsschlüsseln. Wenn diese Option ausgewählt ist, werden die Konfigurationseinstellungen im Bereich "Auto Policy Parameters" (Parameter für automatische Richtlinie) aktiviert. Klicken Sie hier, um die Schritte zu erfahren. Stellen Sie sicher, dass das IKE-Protokoll automatisch zwischen den beiden VPN-Endpunkten verhandelt.

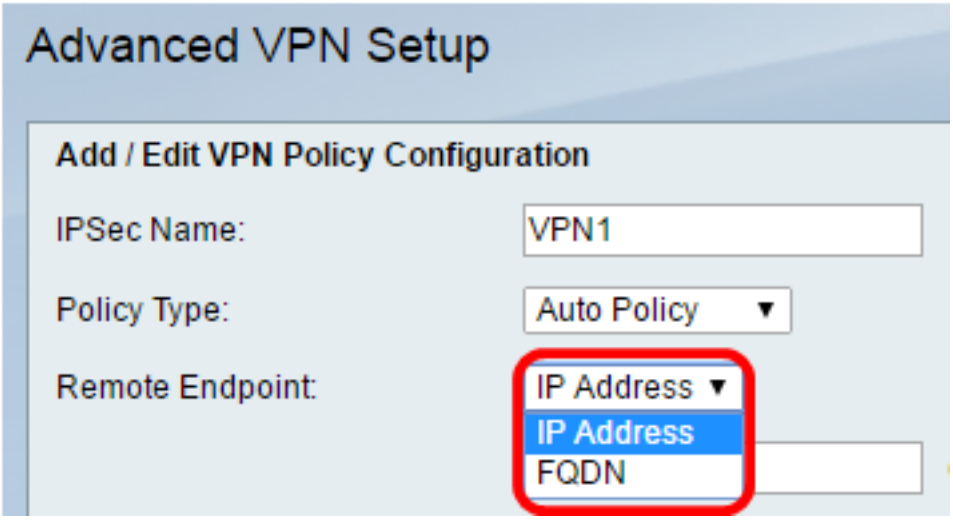
Anmerkung: In diesem Beispiel wird Auto Policy (Automatische Richtlinie) ausgewählt.



Schritt 4: Wählen Sie in der Dropdown-Liste "Remote Endpoint" eine Option aus.

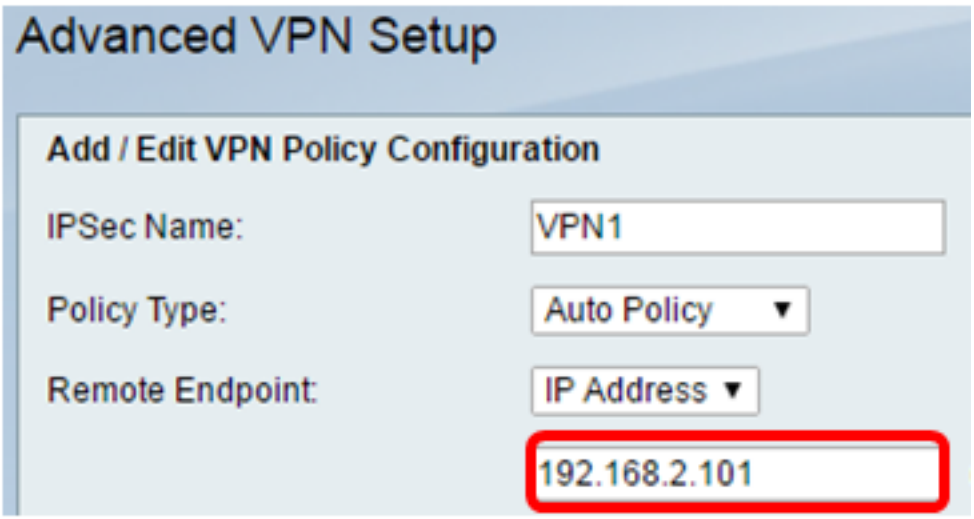
- IP-Adresse - Diese Option identifiziert das Remote-Netzwerk durch eine öffentliche IP-Adresse.
- FQDN - Vollständiger Domänenname für einen bestimmten Computer, Host oder das Internet. Der FQDN besteht aus zwei Teilen: den Hostnamen und den Domänennamen. Diese Option kann nur aktiviert werden, wenn in Schritt 3 die **automatische Richtlinie** ausgewählt ist.

Anmerkung: Für dieses Beispiel wird die IP-Adresse ausgewählt.

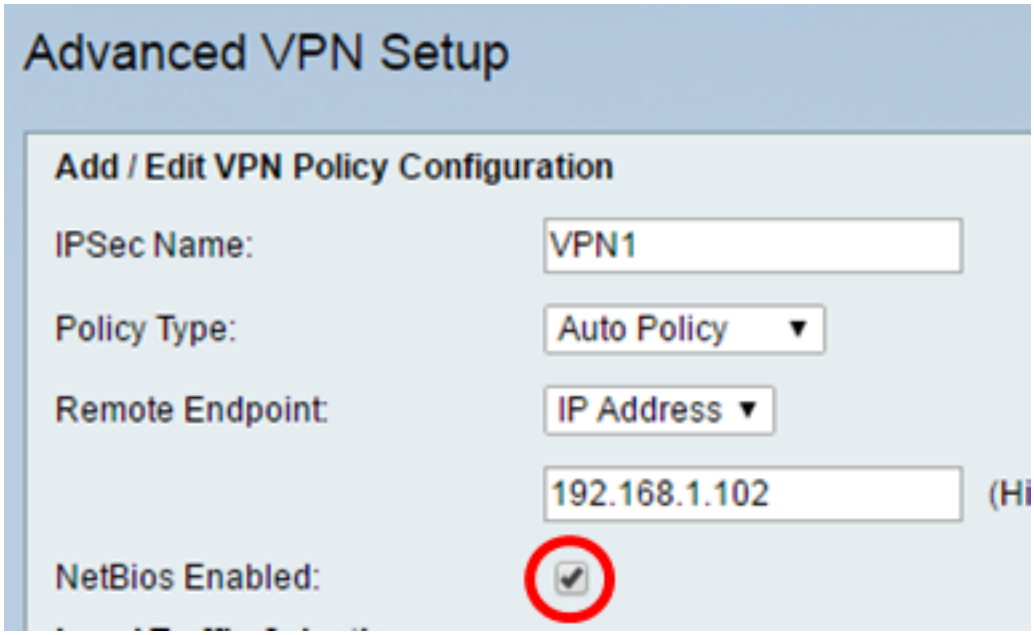


Schritt 5: Geben Sie im Feld "*Remote Endpoint*" entweder die öffentliche IP-Adresse oder den Domänennamen der Remote-Adresse ein.

Anmerkung: In diesem Beispiel wird 192.168.2.101 verwendet.



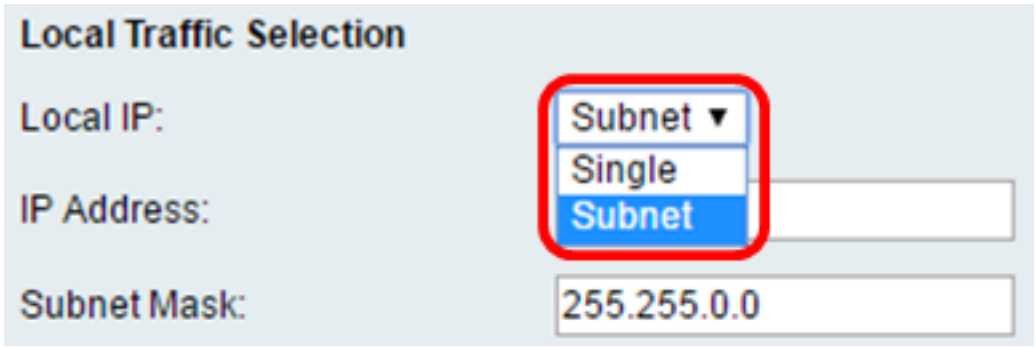
Schritt 6: Aktivieren Sie das Kontrollkästchen **NetBIOS aktiviert,** wenn über die VPN-Verbindung Network Basic Input/Output System (NetBIOS)-Broadcasts gesendet werden sollen. NetBIOS ermöglicht Hosts die Kommunikation untereinander innerhalb eines LAN (Local Area Network).



Schritt 7: Wählen Sie im Bereich zur Auswahl des lokalen Datenverkehrs in der Dropdown-Liste "Lokale IP" eine Option aus.

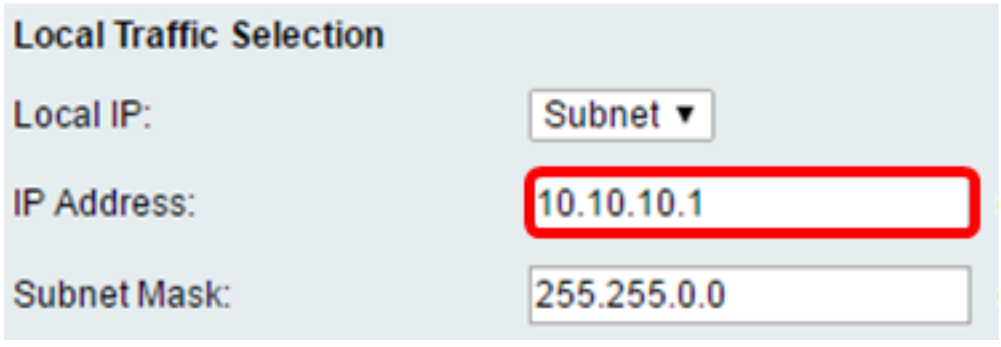
- Single (Einzeln): Die Richtlinie wird auf einen Host beschränkt.
- Subnetz - Ermöglicht Hosts innerhalb eines IP-Adressbereichs, sich mit dem VPN zu verbinden.

Anmerkung: In diesem Beispiel wird "Subnet" ausgewählt.



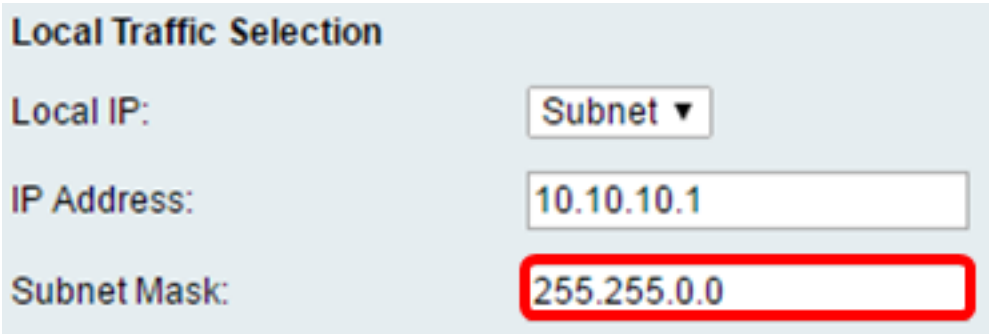
Schritt 8: Geben Sie im Feld "IP Address" (IP-Adresse) die IP-Adresse des Hosts oder Subnetzes des lokalen Subnetzes oder Hosts ein.

Anmerkung: In diesem Beispiel wird die lokale Subnetz-IP-Adresse 10.10.10.1 verwendet.



Schritt 9. (Optional) Wenn in Schritt 7 Subnetz ausgewählt ist, geben Sie die Subnetzmaske des Clients in das Feld *Subnetzmaske ein*. Das Feld "Subnetzmaske" ist deaktiviert, wenn in Schritt 1 die Option Einzeln ausgewählt wird.

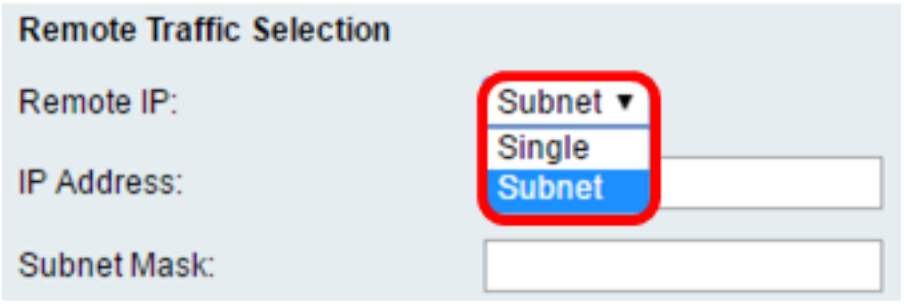
Anmerkung: In diesem Beispiel wird die Subnetzmaske 255.255.0.0 verwendet.



Schritt 10: Wählen Sie in der Dropdown-Liste Remote IP (Remote-IP) im Bereich Remote Traffic Selection (Remote-Datenverkehrsauswahl) eine Option aus.

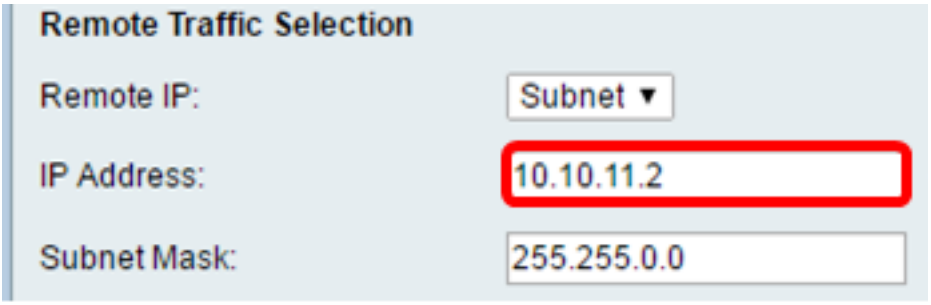
- Single (Einzeln): Die Richtlinie wird auf einen Host beschränkt.
- Subnetz - Ermöglicht Hosts innerhalb eines IP-Adressbereichs, sich mit dem VPN zu verbinden.

Anmerkung: In diesem Beispiel wird "Subnet" ausgewählt.



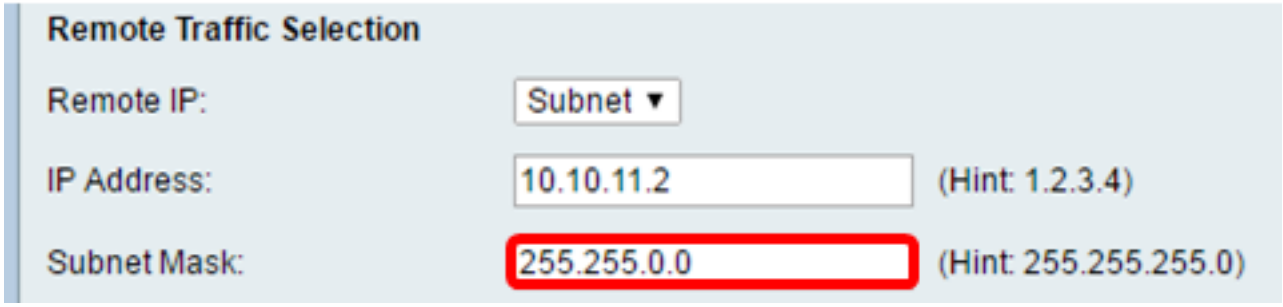
Schritt 11: Geben Sie den IP-Adressbereich des Hosts, der Teil des VPN sein soll, in das Feld *IP-Adresse ein*. Wenn in Schritt 10 die Option **Single** (Einzeln) ausgewählt ist, geben Sie eine IP-Adresse ein.

Anmerkung: Im folgenden Beispiel wird 10.10.11.2 verwendet.



Schritt 12. (Optional) Wenn in Schritt 10 **Subnetz** ausgewählt ist, geben Sie die Subnetzmaske der Subnetz-IP-Adresse in das Feld *Subnetzmaske ein*.

Anmerkung: Im folgenden Beispiel wird 255.255.0.0 verwendet.

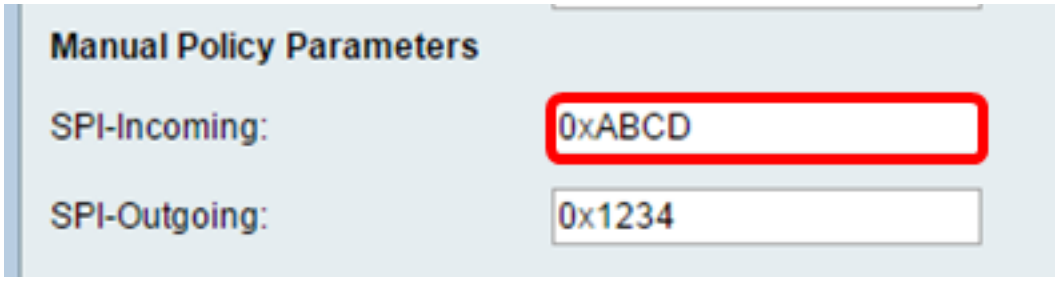


Manuelle Richtlinie Parameter

Hinweis: Diese Felder können nur bearbeitet werden, wenn **Manuelle Richtlinie** ausgewählt ist.

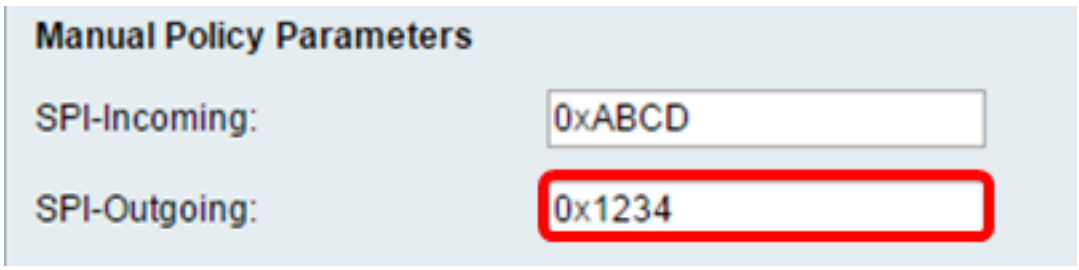
Schritt 1: Geben Sie im Feld *SPI-Incoming (SPI eingehend)* drei bis acht Hexadezimalzeichen für das Security Parameter Index (SPI)-Tag für eingehenden Datenverkehr über die VPN-Verbindung ein. Das SPI-Tag wird verwendet, um den Datenverkehr einer Sitzung vom Datenverkehr anderer Sitzungen zu unterscheiden.

Anmerkung: Für dieses Beispiel wird 0xABCD verwendet.



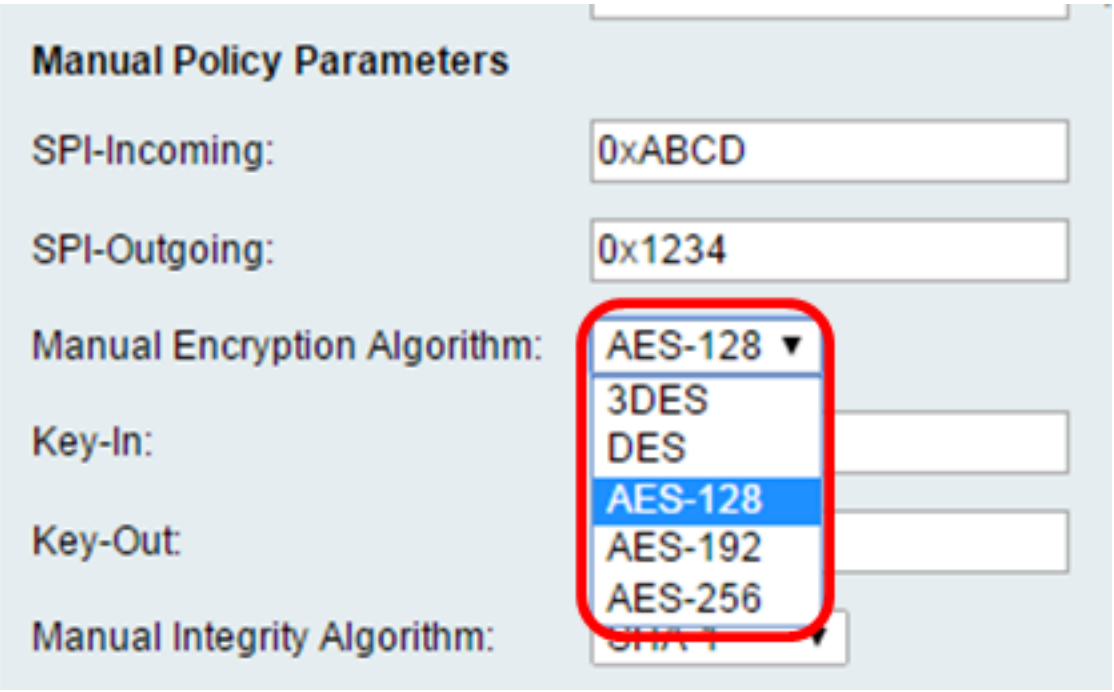
Schritt 2: Geben Sie im Feld *SPI-Outgoing (SPI - Ausgehend)* drei bis acht Hexadezimalzeichen für den SPI-Tag für ausgehenden Datenverkehr auf der VPN-Verbindung ein.

Anmerkung: Für dieses Beispiel wird 0x1234 verwendet.



Schritt 3: Wählen Sie in der Dropdown-Liste Manual Encryption Algorithm (Manueller Verschlüsselungsalgorithmus) eine Option aus. Die Optionen sind DES, 3DES, AES-128, AES-192 und AES-256.

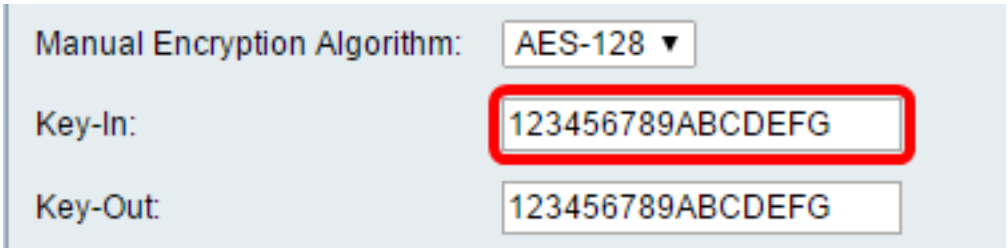
Anmerkung: In diesem Beispiel wird AES-128 ausgewählt.



Schritt 4: Geben Sie im Feld *Key-In* einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 3 gewählten Algorithmus ab.

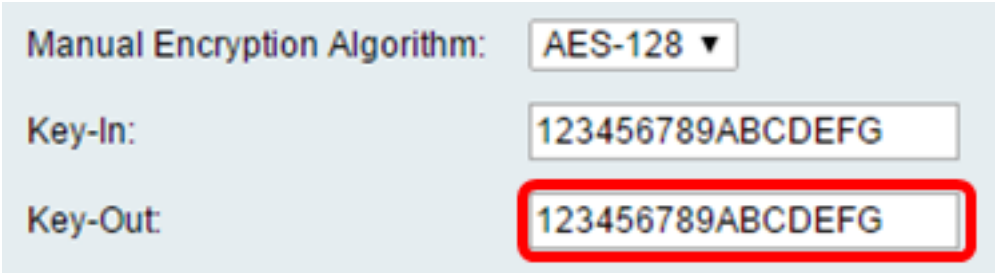
- DES verwendet einen aus 8 Zeichen bestehenden Schlüssel.
- 3DES verwendet eine 24-Zeichen-Taste.
- AES-128 verwendet eine 16-Zeichen-Taste.
- AES-192 verwendet eine 24-Zeichen-Taste.
- AES-256 verwendet eine 32-Zeichen-Taste.

Anmerkung: In diesem Beispiel wird 123456789ABCDEFG verwendet.



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

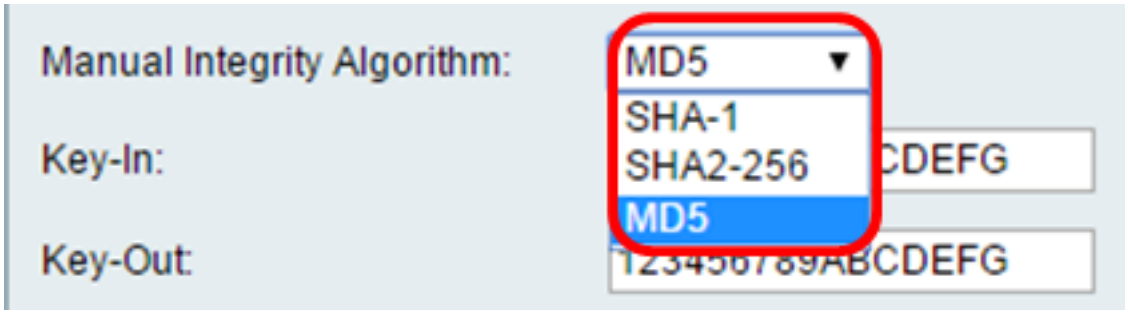
Anmerkung: In diesem Beispiel wird 123456789ABCDEFG verwendet.



Schritt 6: Wählen Sie aus der Dropdown-Liste Manual Integrity Algorithm (Manueller Integritätsalgorithmus) eine Option aus.

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

Anmerkung: In diesem Beispiel wird MD5 ausgewählt.



Schritt 7: Geben Sie im *Feld Key-In* einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 6 gewählten Algorithmus ab.

- MD5 verwendet eine Taste mit 16 Zeichen.
- SHA-1 verwendet eine 20-Zeichen-Taste.
- SHA2-256 verwendet eine 32-Zeichen-Taste.

Anmerkung: In diesem Beispiel wird 123456789ABCDEFG verwendet.

Schritt 8: Geben Sie im *Feld Key-Out* einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 6 gewählten Algorithmus ab.

Anmerkung: In diesem Beispiel wird 123456789ABCDEFG verwendet.

AUTo Richtlinienparameter

Hinweis: Stellen Sie vor dem Erstellen einer automatischen VPN-Richtlinie sicher, dass Sie die IKE-Richtlinie erstellen, auf deren Grundlage Sie die automatische VPN-Richtlinie

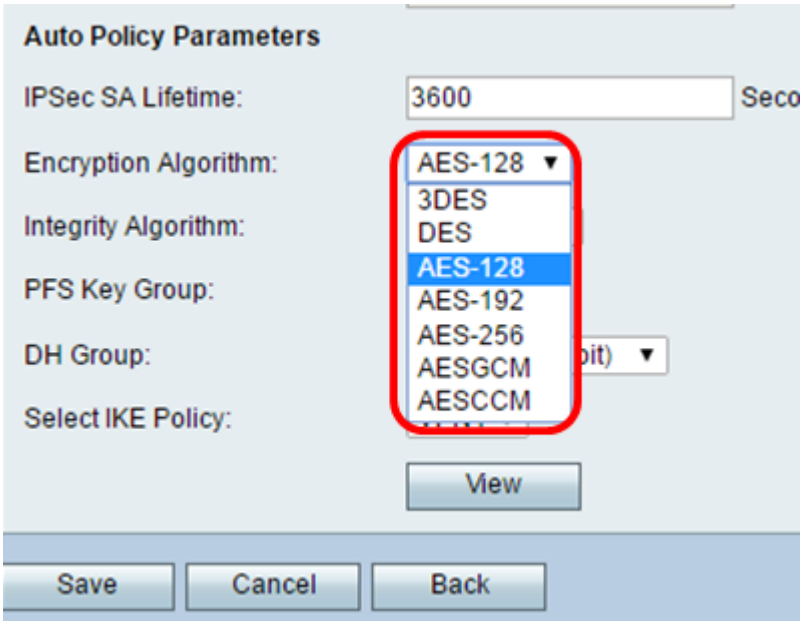
erstellen möchten.Diese Felder können nur bearbeitet werden, wenn in Schritt 3 **Automatische Richtlinie** ausgewählt ist.

Schritt 1: Geben Sie im *Feld IPSec SA-Lifetime (SA-Lebensdauer*) an, wie lange (in Sekunden) die SA vor der Verlängerung dauert. Der Bereich liegt zwischen 30 und 86400. Der Standardwert ist 3600.

Schritt 2: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus. Folgende Optionen sind verfügbar:

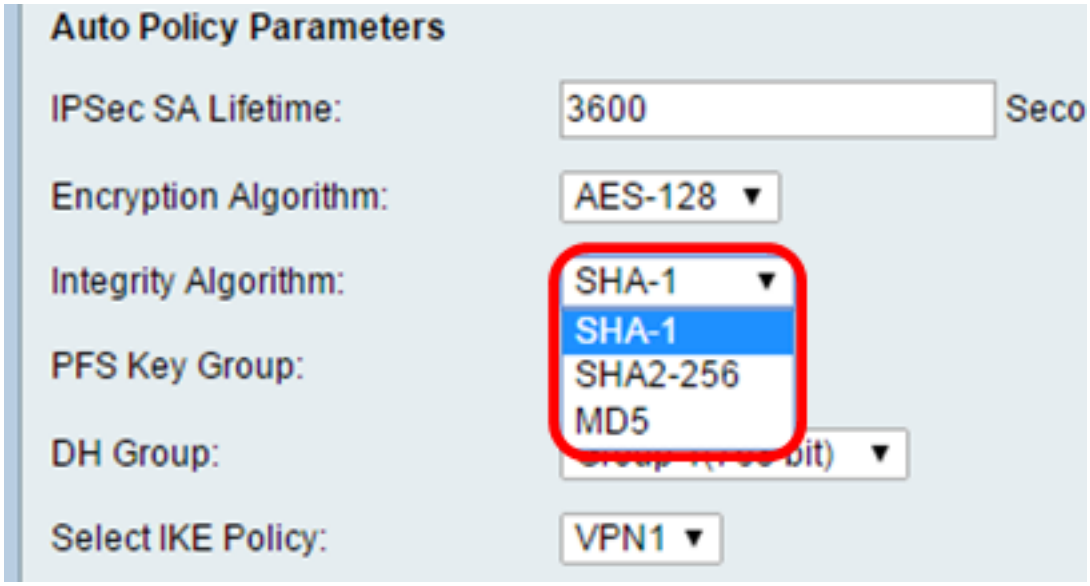
Anmerkung: In diesem Beispiel wird AES-128 ausgewählt.

- DES - Eine 56-Bit alte Verschlüsselungsmethode, die keine besonders sichere Verschlüsselungsmethode ist, aber möglicherweise für die Abwärtskompatibilität erforderlich ist.
- 3DES - Eine einfache 168-Bit-Verschlüsselungsmethode, die verwendet wird, um die Schlüssellänge zu vergrößern, da sie die Daten dreimal verschlüsselt. Dies bietet mehr Sicherheit als DES, aber weniger Sicherheit als AES.
- AES-128: Verwendet einen 128-Bit-Schlüssel für die AES-Verschlüsselung. AES ist schneller und sicherer als DES. Generell ist AES auch schneller und sicherer als 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.
- AES-192 - Verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128 und schneller, aber weniger sicher als 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.
- AESGCM — Advanced Encryption Standard Galois Counter Mode ist ein generischer authentifizierter Verschlüsselungsblockverschlüsselungsmodus. Die GCM-Authentifizierung verwendet Operationen, die sich besonders gut für eine effiziente Implementierung in der Hardware eignen und daher besonders für Hochgeschwindigkeitsimplementierungen oder für Implementierungen in einer effizienten und kompakten Schaltung attraktiv sind.
- AESCCM — Advanced Encryption Standard Counter with CBC-MAC Mode ist ein generischer Verschlüsselungsmodus mit authentifizierter Verschlüsselung. CCM eignet sich hervorragend für den Einsatz in kompakten Software-Implementierungen.

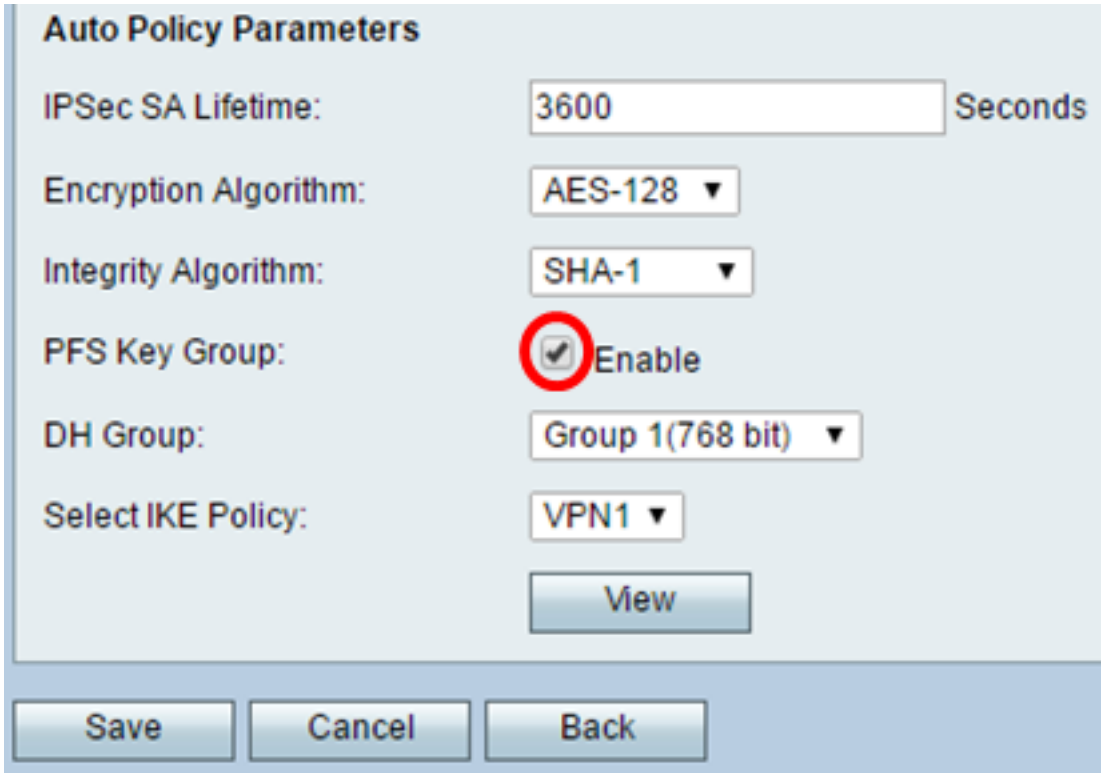


Schritt 3: Wählen Sie aus der Dropdown-Liste "Integritätsalgorithmus" eine Option aus. Die Optionen sind MD5, SHA-1 und SHA2-256.

Anmerkung: In diesem Beispiel wird SHA-1 ausgewählt.

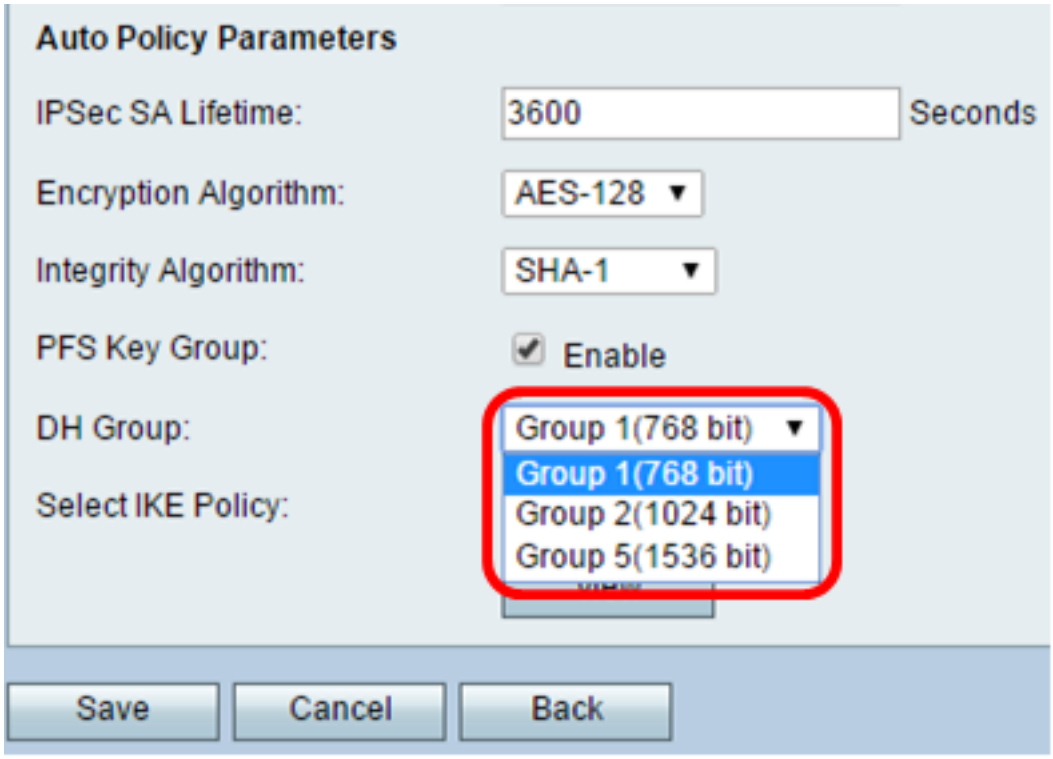


Schritt 4. Aktivieren Sie das Kontrollkästchen **Aktivieren** in der PFS-Schlüsselgruppe, um Perfect Forward Secrecy (PFS) zu aktivieren. PFS erhöht die VPN-Sicherheit, verlangsamt jedoch die Verbindungsgeschwindigkeit.



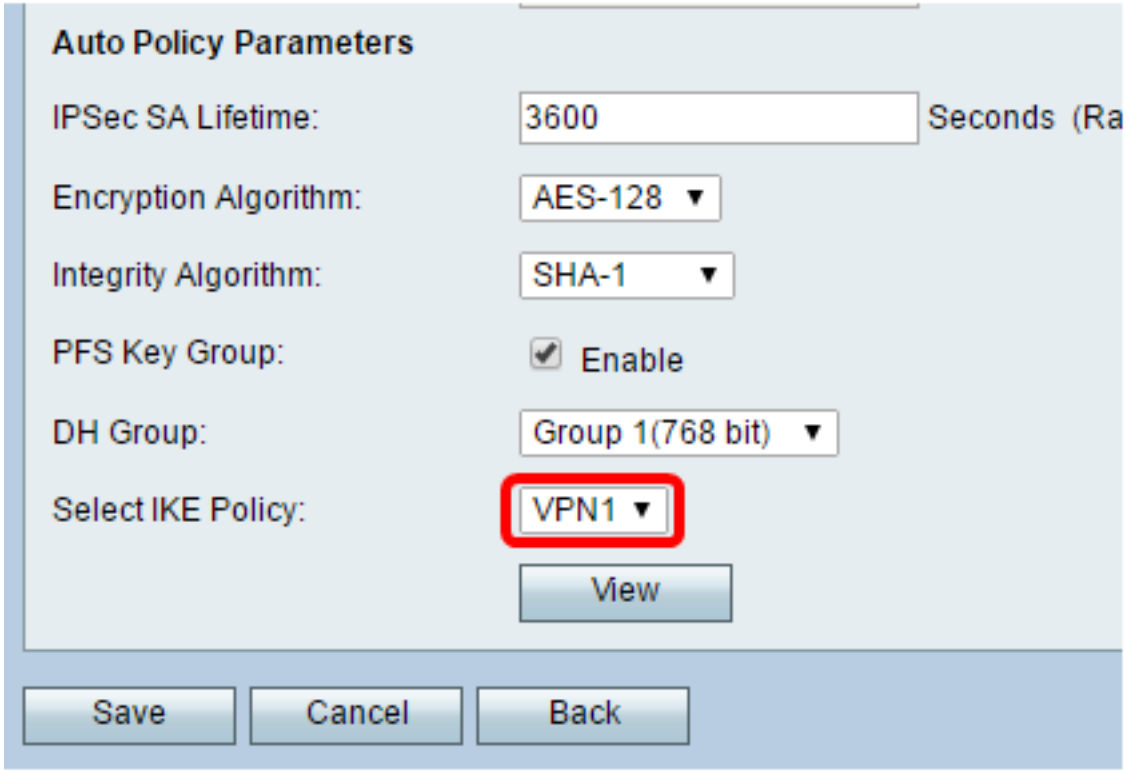
Schritt 5. (Optional) Wenn Sie PFS in Schritt 4 aktivieren möchten, wählen Sie aus der Dropdown-Liste "DH-Gruppe" eine DH-Gruppe aus, der Sie beitreten möchten. Je höher die Gruppennummer, desto besser die Sicherheit.

Anmerkung: Für dieses Beispiel wird Gruppe 1 ausgewählt.

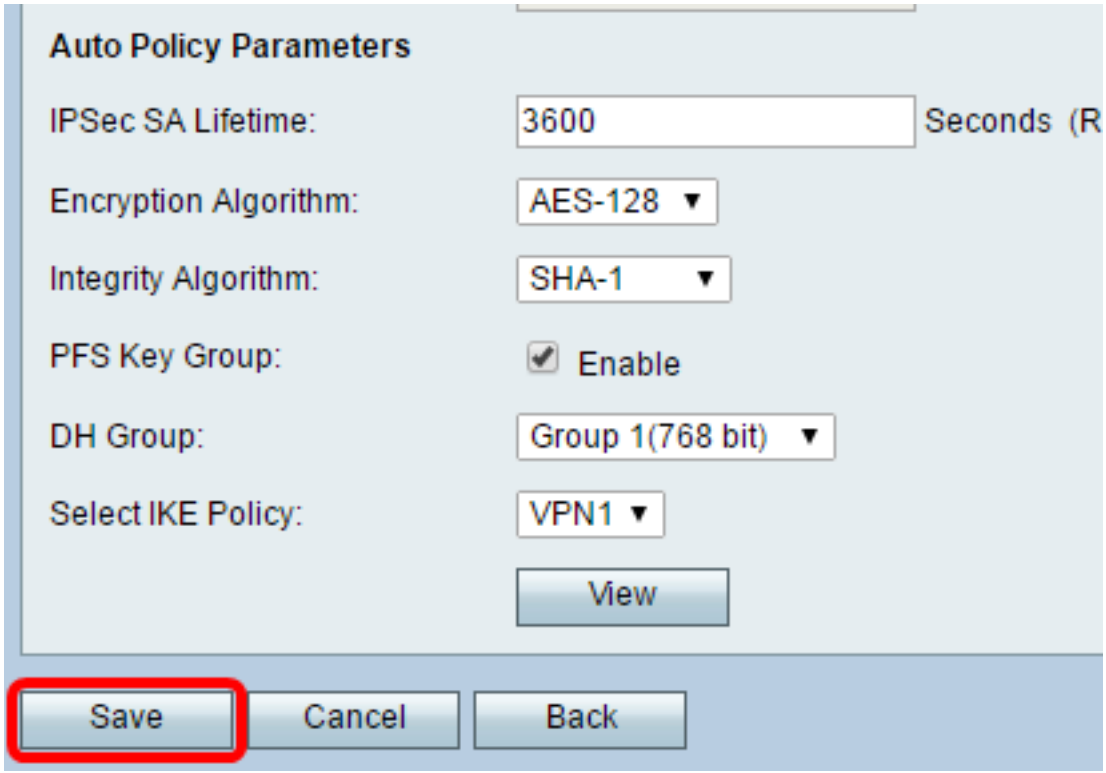


Schritt 6: Wählen Sie aus der Dropdown-Liste IKE-Richtlinie auswählen die IKE-Richtlinie aus, die für die VPN-Richtlinie verwendet werden soll.

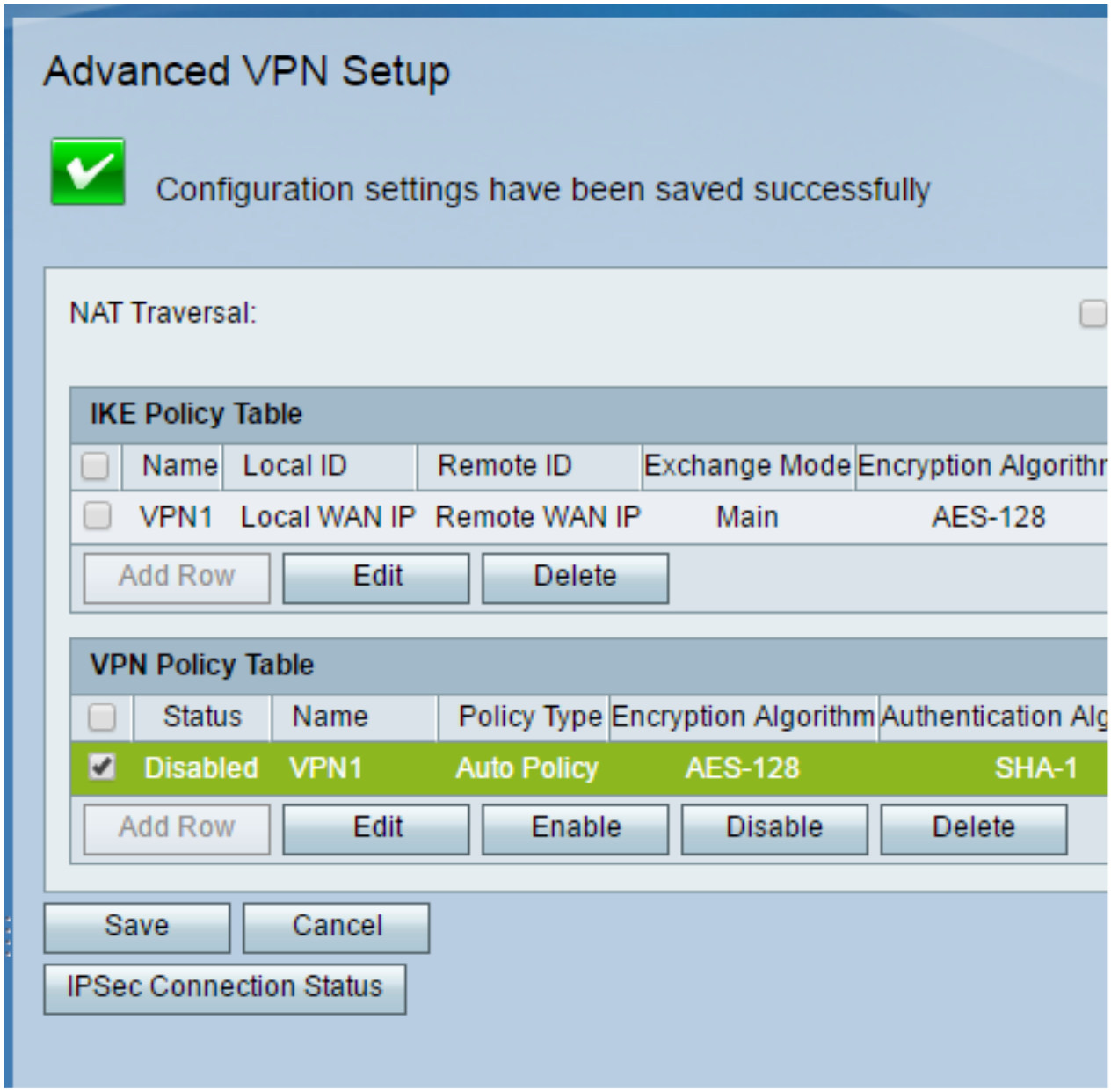
Anmerkung: In diesem Beispiel wurde nur eine IKE-Richtlinie konfiguriert, sodass nur eine Richtlinie angezeigt wird.



Schritt 7: Klicken Sie auf **Speichern**.

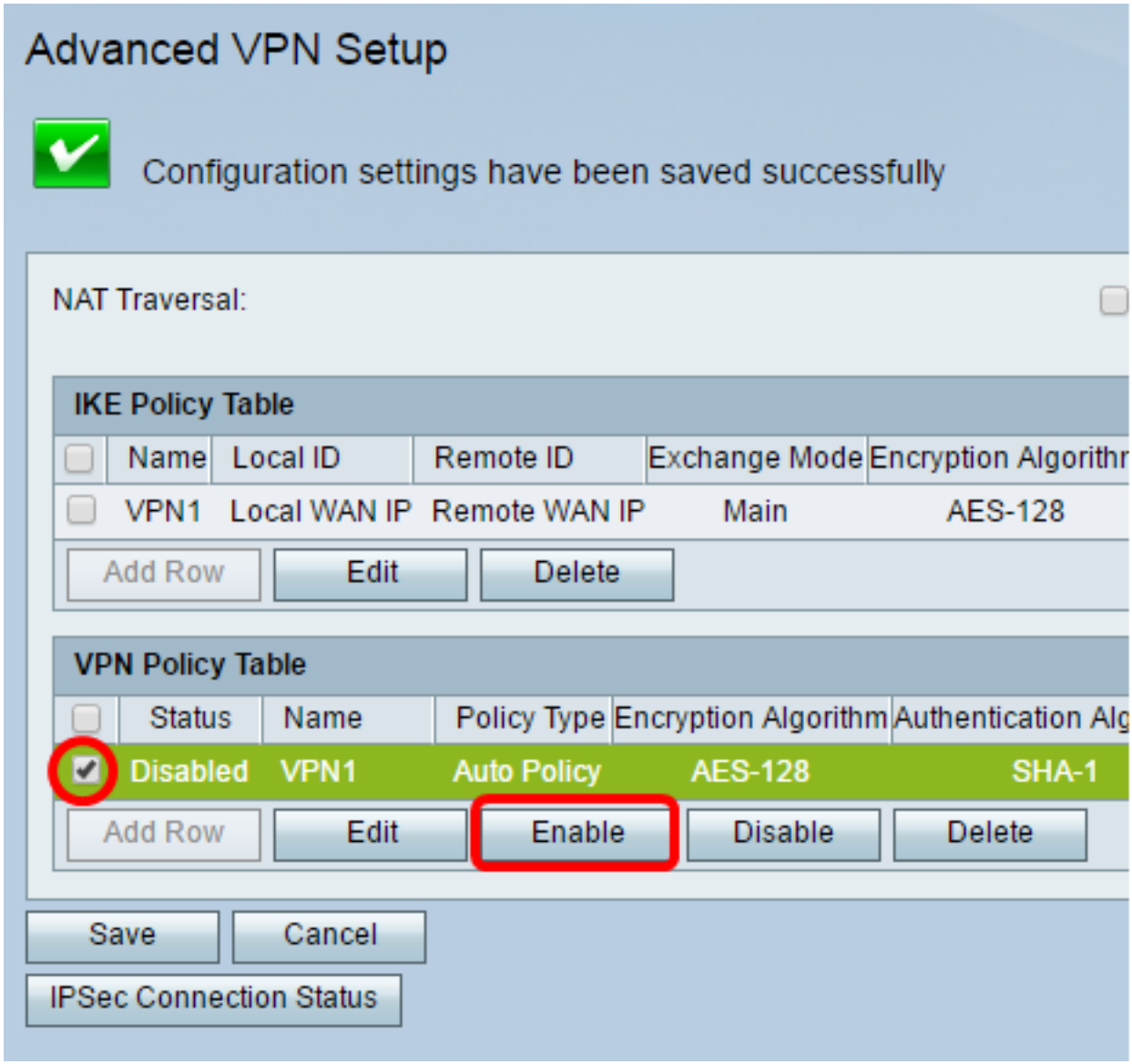


Anmerkung: Die Hauptseite für die erweiterte VPN-Einrichtung wird erneut angezeigt. Eine Bestätigungsmeldung, dass die Konfigurationseinstellungen erfolgreich gespeichert wurden, wird angezeigt.

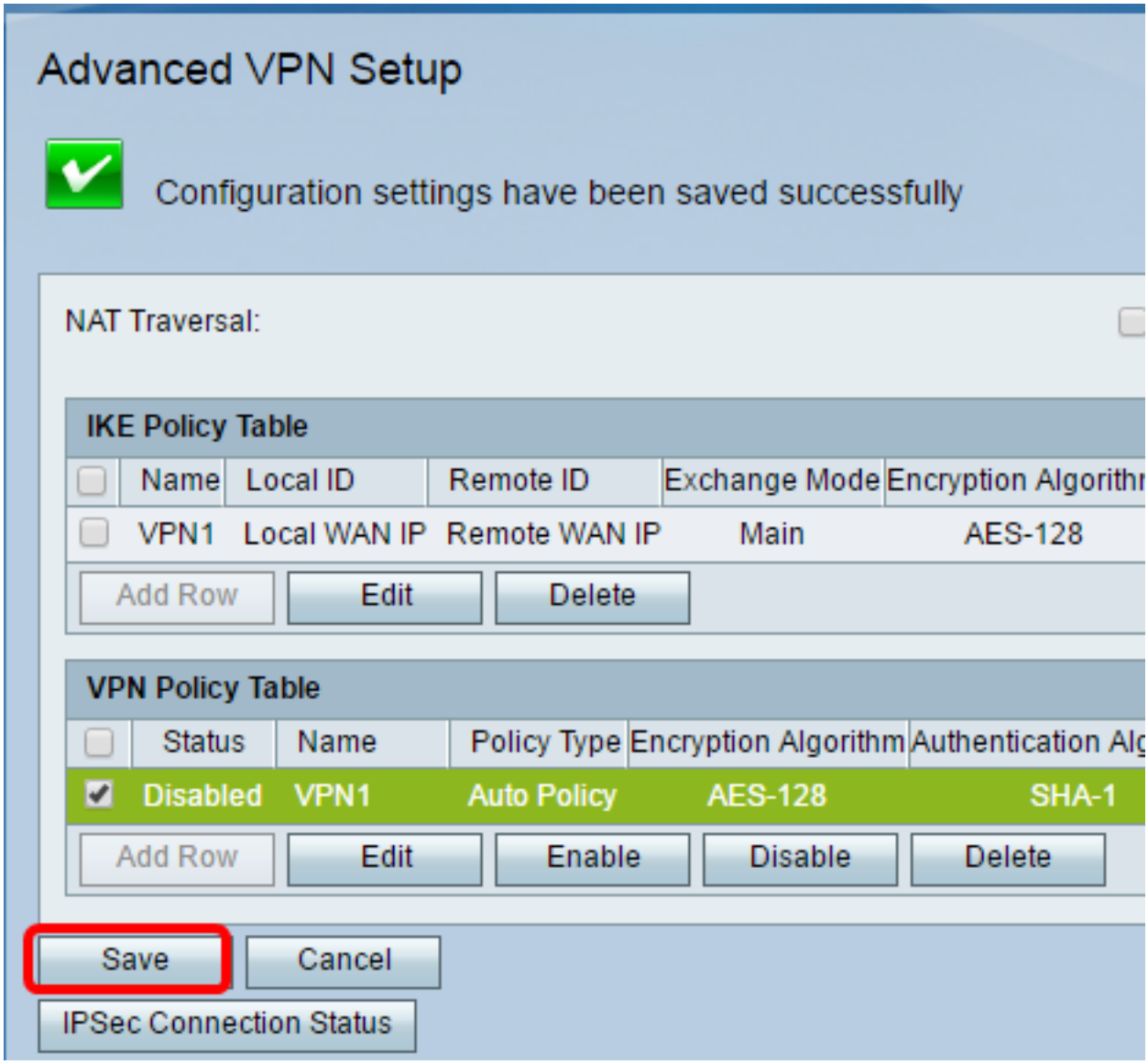


Schritt 8: Aktivieren Sie in der Tabelle "VPN Policy" ein Kontrollkästchen, um ein VPN auszuwählen, und klicken Sie auf **Enable**.

Anmerkung: Die konfigurierte VPN-Richtlinie ist standardmäßig deaktiviert.



Schritt 9: Klicken Sie auf **Speichern**.



Sie sollten nun erfolgreich eine VPN-Richtlinie auf Ihrem RV130 oder RV130W Router konfiguriert haben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.