Erweitertes VPN-Setup auf der RV215W

Ziel

Ein Virtual Private Network (VPN) ist eine sichere Verbindung innerhalb eines Netzwerks oder zwischen Netzwerken. VPNs dienen dazu, den Datenverkehr zwischen bestimmten Hosts und Netzwerken vom Datenverkehr nicht autorisierter Hosts und Netzwerke zu isolieren. In diesem Artikel wird die Konfiguration des erweiterten VPN-Setups auf der RV215W erläutert.

Anwendbare Geräte

RV215W

Softwareversion

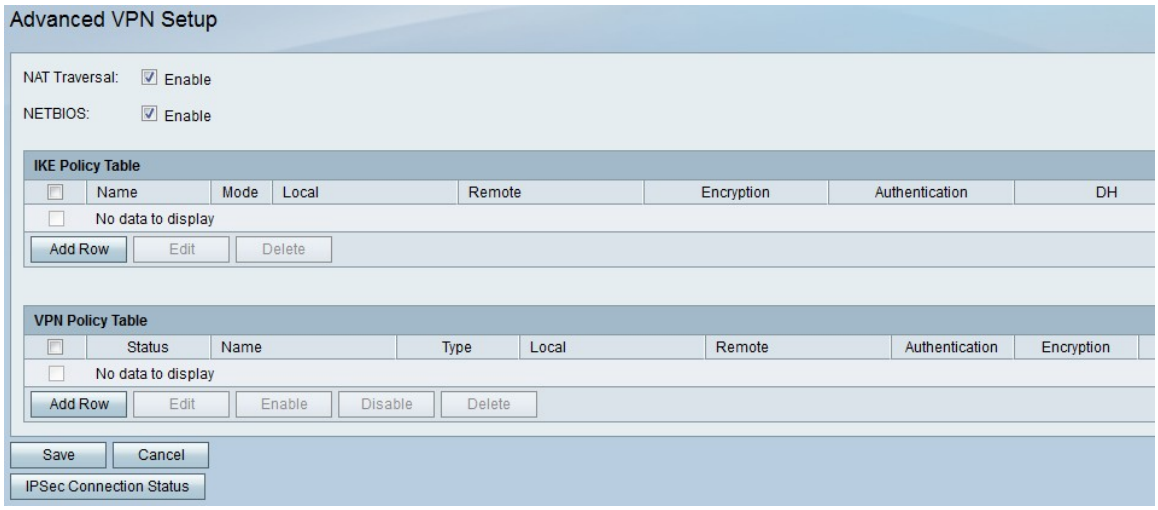
·1.1.0.5

Erweiterte VPN-Einrichtung

Ersteinstellungen

In diesem Verfahren wird erläutert, wie die ursprünglichen Einstellungen für das erweiterte VPN-Setup konfiguriert werden.

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



Schritt 2: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld 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 aus, wenn Ihre VPN-Verbindung über ein NAT-fähiges Gateway verläuft.

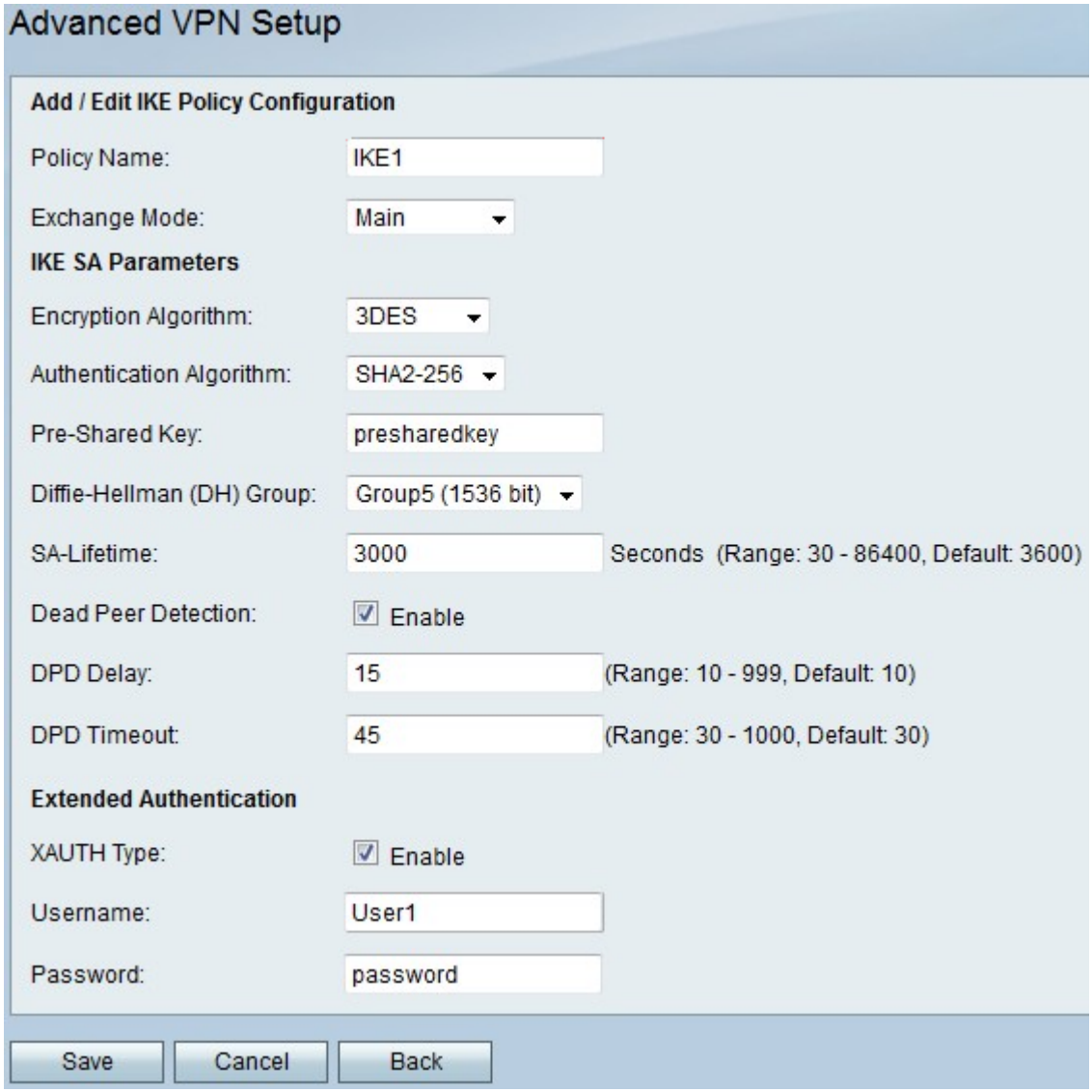
Schritt 3: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld NETBIOS, wenn Sie das Senden von Network Basic Input/Output System (NetBIOS)-Broadcasts über die

VPN-Verbindung aktivieren möchten. NetBIOS ermöglicht Hosts die Kommunikation untereinander in einem LAN.

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: Klicken Sie in der IKE-Richtlinientabelle auf **Zeile hinzufügen**, um eine neue IKE-Richtlinie zu erstellen. Um eine IKE-Richtlinie zu bearbeiten, aktivieren Sie das Kontrollkästchen für die Richtlinie, und klicken Sie auf **Bearbeiten**. Die Seite *Advanced VPN Setup* wird wie folgt geändert:



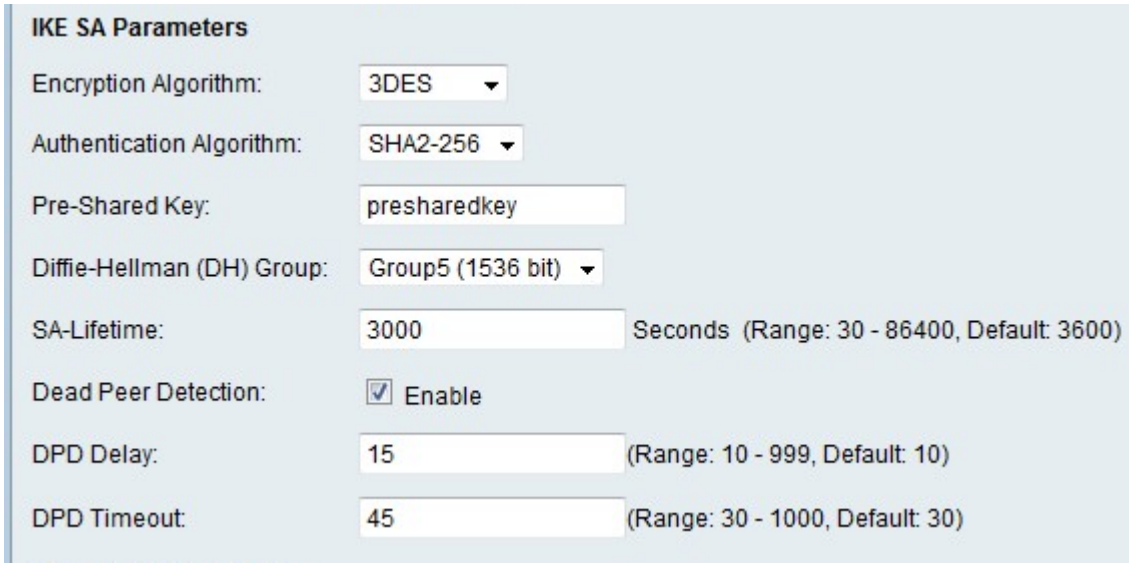
Schritt 2: Geben Sie im Feld Policy Name (Richtlinienname) einen Namen für die IKE-Richtlinie ein.

Schritt 3: Wählen Sie aus der Exchange Mode-Dropdown-Liste eine Option aus.

·Main (Hauptmodus): Mit dieser Option kann die IKE-Richtlinie sicherer, aber langsamer als

der aggressive Modus arbeiten. Wählen Sie diese Option aus, wenn eine sicherere VPN-Verbindung erforderlich ist.

·Aggressive (Aggressiv): Mit dieser Option kann die IKE-Richtlinie schneller, aber weniger sicher als der Hauptmodus ausgeführt werden. Wählen Sie diese Option aus, wenn eine schnellere VPN-Verbindung erforderlich ist.



Schritt 4: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus.

·DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die zwar keine sehr sichere Verschlüsselungsmethode ist, aber für die Abwärtskompatibilität erforderlich sein kann.

·3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode zur Erhöhung der Schlüsselgröße, 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 AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller und sicherer als 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 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 5: Wählen Sie in der Dropdown-Liste Authentication Algorithm (Authentifizierungsalgorithmus) eine Option aus.

·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 sicher als MD5 und SHA-1.

Schritt 6: Geben Sie im Feld Pre-Shared Key (Vorinstallierter Schlüssel) einen vorinstallierten Schlüssel ein, den die IKE-Richtlinie verwendet.

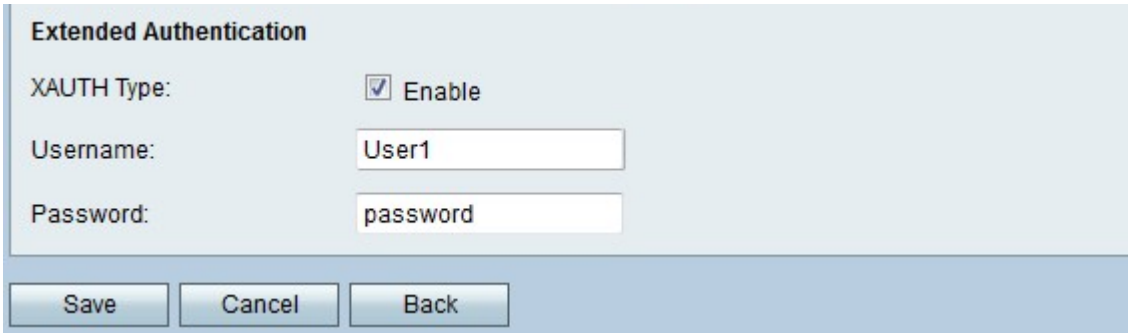
Schritt 7: Wählen Sie aus der Dropdown-Liste Diffie-Hellman (DH) Group (DH-Gruppe) aus, welche DH-Gruppe von der IKE verwendet wird. Hosts in einer DH-Gruppe können Schlüssel austauschen, ohne einander zu kennen. Je höher die Bitnummer der Gruppe ist, desto sicherer ist die Gruppe.

Schritt 8: Geben Sie im Feld SA-Lifetime (SA-Lebensdauer) an, wie lange ein SA für das VPN in Sekunden dauert, bevor die SA verlängert wird.

Schritt 9: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Dead Peer Detection (DPD), um Dead Peer Detection (DPD) zu aktivieren. Die DPD überwacht IKE-Peers, um festzustellen, ob ein Peer nicht mehr funktioniert. DPD verhindert die Verschwendung von Netzwerkressourcen bei inaktiven Peers.

Schritt 10: (Optional) Wenn Sie in Schritt 9 DPD aktiviert haben, geben Sie ein, wie oft (in Sekunden) der Peer im Feld DPD Delay (DPD-Verzögerung) auf Aktivität überprüft wird.

Schritt 11: (Optional) Wenn Sie in Schritt 9 die DPD aktiviert haben, geben Sie die Anzahl der Sekunden ein, die gewartet werden muss, bevor ein inaktiver Peer im Feld DPD Timeout (DPD-Timeout) verworfen wird.



Schritt 12: (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld XAUTH Type (XAUTH-Typ), um die erweiterte Authentifizierung (XAUTH) zu aktivieren. Mit XAUTH können mehrere Benutzer eine einzelne VPN-Richtlinie anstelle einer VPN-Richtlinie für jeden Benutzer verwenden.

Schritt 13: (Optional) Wenn Sie XAUTH in Schritt 12 aktiviert haben, geben Sie den Benutzernamen für die Richtlinie in das Feld Benutzername ein.

Schritt 14: (Optional) Wenn Sie XAUTH in Schritt 12 aktiviert haben, geben Sie das Kennwort für die Richtlinie in das Feld Kennwort ein.

Schritt 15: Klicken Sie auf **Speichern**. Die ursprüngliche Seite *Advanced VPN Setup* wird erneut angezeigt.

VPN-Richtlinieneinstellungen

In diesem Verfahren wird erläutert, wie eine VPN-Richtlinie für die zu verwendende VPN-Verbindung konfiguriert wird. Damit ein VPN ordnungsgemäß funktioniert, müssen die VPN-Richtlinien für beide Endpunkte identisch sein.

Schritt 1: Klicken Sie in der VPN Policy Table (VPN-Richtlinientabelle) auf **Add Row (Zeile hinzufügen**), um eine neue VPN-Richtlinie zu erstellen. Um eine VPN-Richtlinie zu bearbeiten, aktivieren Sie das Kontrollkästchen für die Richtlinie, und klicken Sie auf **Bearbeiten**. Die Seite *Advanced VPN Setup* wird wie folgt geändert:

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

Schritt 2: Geben Sie im Feld Policy Name (Richtlinienname) einen Namen für die VPN-Richtlinie ein.

Schritt 3: Wählen Sie in der Dropdown-Liste Policy Type (Richtlinientyp) eine Option aus.

·Manual Policy (Manuelle Richtlinie): Mit dieser Option können Sie die Schlüssel für Datenverschlüsselung und -integrität konfigurieren.

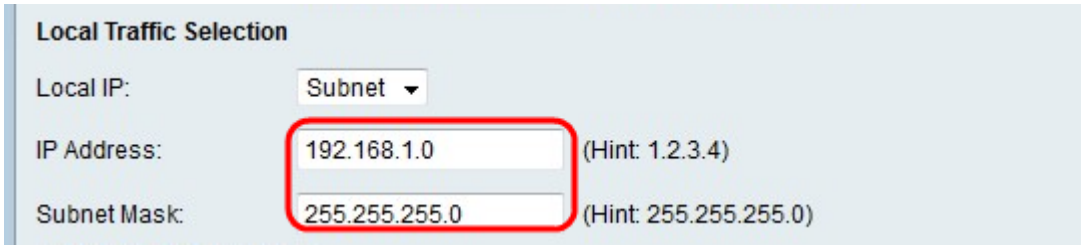
·Auto Policy (Automatische Richtlinie): Diese Option verwendet eine IKE-Richtlinie für Datenintegrität und den Austausch von Verschlüsselungsschlüsseln.

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

·IP Address (IP-Adresse): Diese Option identifiziert das Remote-Netzwerk über eine öffentliche IP-Adresse.

·FQDN - Diese Option verwendet einen FQDN (Fully Qualified Domain Name), um das Remote-Netzwerk zu identifizieren.

Schritt 5: Geben Sie im Textfeld unter der Dropdown-Liste "Remote Endpoint" entweder die öffentliche IP-Adresse oder den Domänennamen der Remote-Adresse ein.



Schritt 6: Wählen Sie aus der Dropdown-Liste Local IP (Lokale IP) eine Option aus.

·Single (Einzel): Diese Option verwendet einen einzelnen Host als lokalen VPN-Verbindungspunkt.

·Subnetz - Diese Option verwendet ein Subnetz des lokalen Netzwerks als lokalen VPN-Verbindungspunkt.

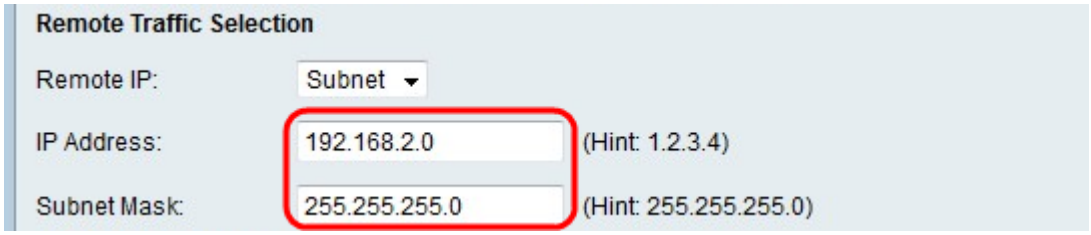
Schritt 7: Geben Sie im Feld IP-Adresse den Host oder die Subnetz-IP-Adresse des lokalen Subnetzes oder Hosts ein.

Schritt 8: (Optional) Wenn Sie in Schritt 6 Subnet (Subnetz) auswählen, geben Sie die Subnetzmaske für das lokale Subnetz in das Feld Subnetzmaske ein.

Schritt 9: Wählen Sie in der Dropdown-Liste Remote IP (Remote-IP) eine Option aus.

·Single (Einzel): Diese Option verwendet einen einzelnen Host als Remote-VPN-Verbindungspunkt.

·Subnetz - Diese Option verwendet ein Subnetz des Remote-Netzwerks als Remote-VPN-Verbindungspunkt.



Schritt 10: Geben Sie im Feld IP-Adresse den Host oder die Subnetz-IP-Adresse des Remote-Subnetzes oder -Hosts ein.

Schritt 11: (Optional) Wenn Sie in Schritt 9 Subnet (Subnetz) auswählen, geben Sie die Subnetzmaske für das Remote-Subnetz in das Feld Subnetzmaske ein.

Hinweis: Wenn Sie in Schritt 3 die Option Manual Policy (Manuelle Richtlinie) ausgewählt haben, führen Sie die Schritte 12 bis 19 aus. Andernfalls überspringen Sie Schritt 20.

Schritt 12: Geben Sie im Feld SPI-Incoming (SPI-Incoming) drei bis acht Hexadezimalzeichen 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.

Schritt 13: Geben Sie im Feld SPI-Outgoing (SPI-Ausgang) drei bis acht Hexadezimalzeichen für SPI-Tag für ausgehenden Datenverkehr an der VPN-Verbindung ein.

Schritt 14: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus.

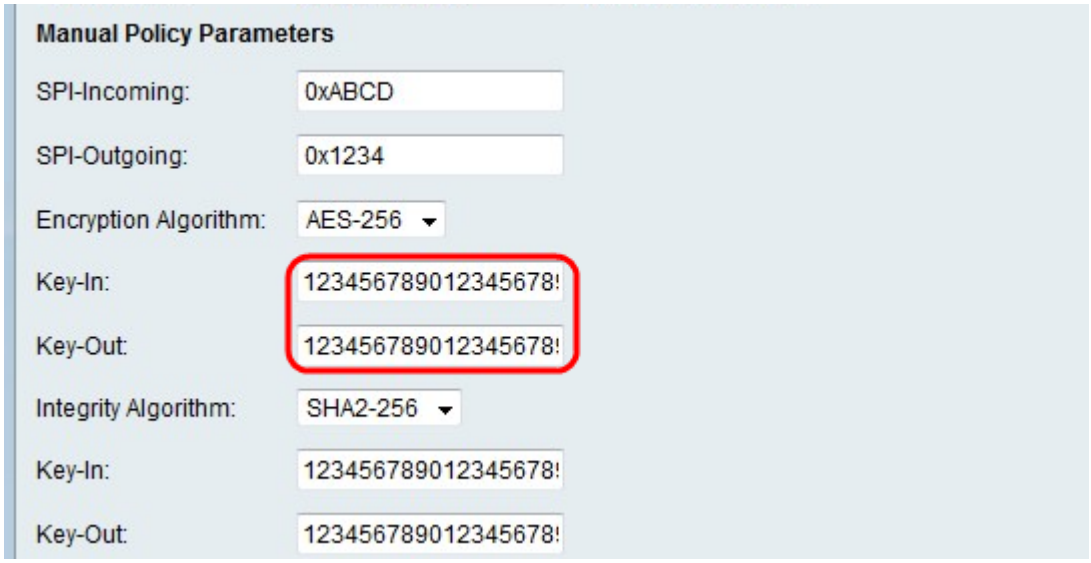
·DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die zwar keine sehr sichere Verschlüsselungsmethode ist, aber für die Abwärtskompatibilität erforderlich sein kann.

·3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode zur Erhöhung der Schlüsselgröße, 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 AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller und sicherer als 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 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 15: Geben Sie im Feld Key-In (Schlüsseleingabe) einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 14 gewählten Algorithmus ab.

·DES verwendet einen 8-stelligen Schlüssel.

·3DES verwendet einen 24-stelligen Schlüssel.

·AES-128 verwendet einen 12-stelligen Schlüssel.

·AES-192 verwendet einen 24-stelligen Schlüssel.

·AES-256 verwendet einen 32-stelligen Schlüssel.

Schritt 16: Geben Sie im Feld "Key-Out" (Schlüssel für das Löschen) einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 14 gewählten Algorithmus ab. Die Schlüssellängen entsprechen denen von Schritt 15.

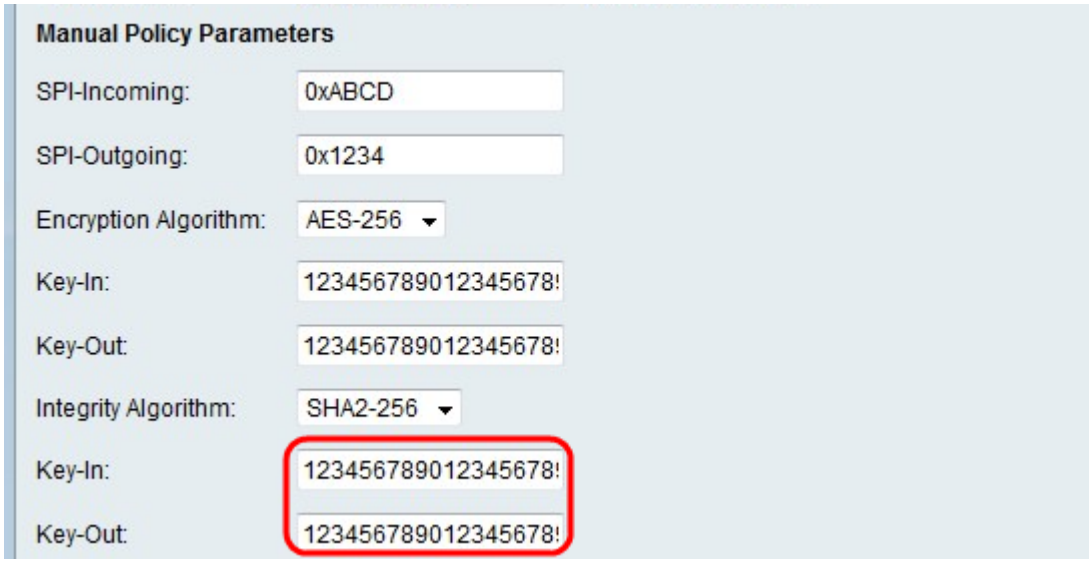
Schritt 17: Wählen Sie in der Dropdown-Liste Integrity Algorithm (Integritätsalgorithmus) eine Option aus.

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



Schritt 18: Geben Sie im Feld Key-In (Schlüsseleingabe) einen Schlüssel für die eingehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 17 gewählten Algorithmus ab.

·MD5 verwendet einen 16-stelligen Schlüssel.

·SHA-1 verwendet einen 20-stelligen Schlüssel.

·SHA2-256 verwendet einen 32-stelligen Schlüssel.

Schritt 19: Geben Sie im Feld "Key-Out" (Schlüssel für das Löschen) einen Schlüssel für die ausgehende Richtlinie ein. Die Schlüssellänge hängt von dem in Schritt 17 gewählten Algorithmus ab. Die Schlüssellängen entsprechen denen von Schritt 18.

Hinweis: Wenn Sie in Schritt 3 die Option "Auto Policy" (Automatische Richtlinie) ausgewählt haben, führen Sie die Schritte 20 bis 25 aus. Fahren Sie andernfalls mit Schritt 26 fort.

Schritt 20: Geben Sie im Feld SA-Lifetime (SA-Lebensdauer) ein, wie lange die SA-Lebensdauer in Sekunden vor der Verlängerung dauert.

Schritt 21: Wählen Sie in der Dropdown-Liste Verschlüsselungsalgorithmus eine Option aus.

·DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die zwar keine sehr sichere Verschlüsselungsmethode ist, aber für die Abwärtskompatibilität

erforderlich sein kann.

·3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode zur Erhöhung der Schlüsselgröße, 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 AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller und sicherer als 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 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 22: Wählen Sie in der Dropdown-Liste Integrity Algorithm (Integritätsalgorithmus) eine Option aus.

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

Schritt 23: 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 24: (Optional) Wenn Sie PFS in Schritt 23 aktiviert haben, wählen Sie eine Diffie-Hellman (DH)-Gruppe, der Sie beitreten möchten, um die folgende Dropdown-Liste aufzurufen. Je höher die Gruppennummer ist, desto sicherer ist die Gruppe.

Schritt 25: Wählen Sie in der Dropdown-Liste Select IKE Policy (IKE-Richtlinie auswählen) aus, welche IKE-Richtlinie für die VPN-Richtlinie verwendet werden soll.

Hinweis: Wenn Sie auf **Ansicht** klicken, werden Sie auf der *Seite* für die *erweiterte VPN-Einrichtung* zum Abschnitt für die IKE-Konfiguration weitergeleitet.

Schritt 26: Klicken Sie auf **Speichern**. Die ursprüngliche Seite *Advanced VPN Setup* wird erneut angezeigt.

Schritt 27: Klicken Sie auf **Speichern**.