IKE-Richtlinieneinstellungen (Internet Key Exchange) für RV130- und RV130W-VPN-Router

Ziel

Internet Key Exchange (IKE) ist ein Protokoll, das eine sichere Kommunikation zwischen zwei Netzwerken herstellt. Bei IKE werden Pakete mit Schlüsseln, die von zwei Parteien verwendet werden, verschlüsselt, gesperrt und entsperrt.

Sie müssen eine Internet Key Exchange-Richtlinie erstellen, bevor Sie eine VPN-Richtlinie konfigurieren können. Weitere Informationen finden Sie unter *VPN Policy Configuration on RV130 and RV130W* (Konfiguration der *VPN-Richtlinien* für den *RV130 und RV130W*).

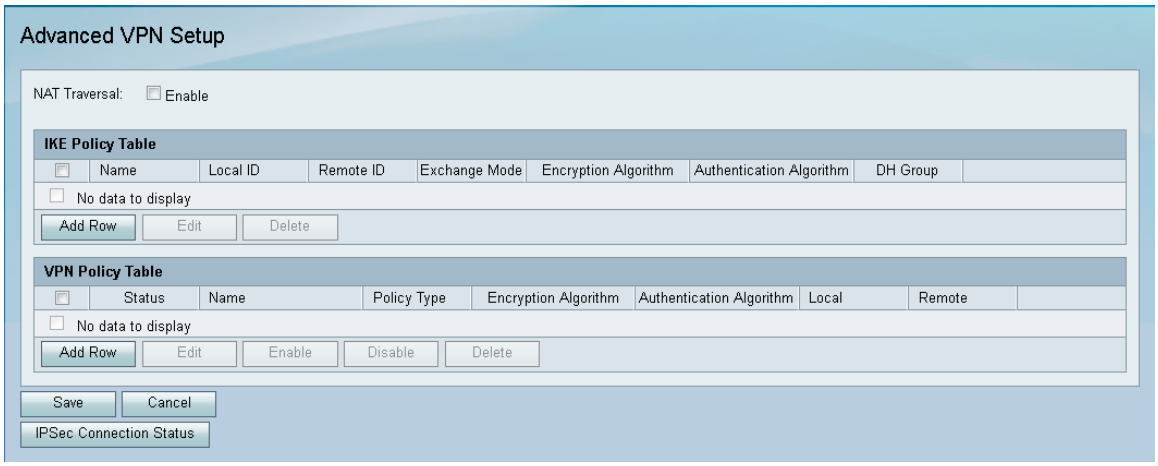
In diesem Dokument wird erläutert, wie Sie RV130- und RV130W-VPN-Routern ein IKE-Profil hinzufügen.

Unterstützte Geräte

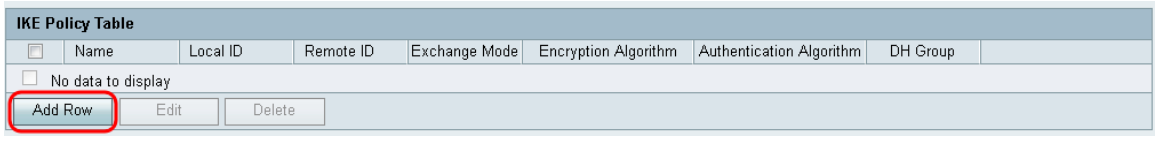
- RV130
- RV130W

Verfahrensschritte

Schritt 1: Wählen Sie im Menü links im Router-Konfigurationsprogramm **VPN > Site-to-Site IPSec VPN > Advanced VPN Setup (Erweitertes VPN-Setup)** aus. Die Seite *Advanced VPN Setup* wird angezeigt:

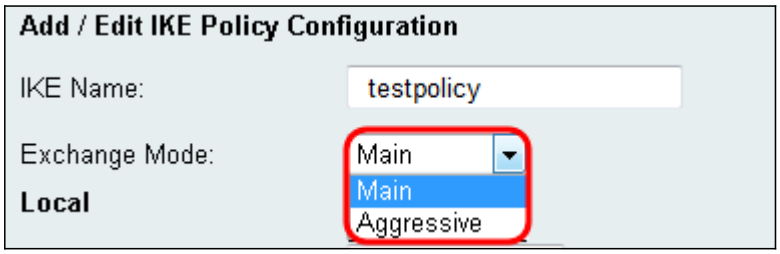


Schritt 2: Klicken Sie in der IKE-Richtlinientabelle auf **Zeile hinzufügen**. Ein neues Fenster wird angezeigt:



Schritt 3: Geben Sie einen Namen für die IKE-Richtlinie in das Feld *IKE-Name ein*.

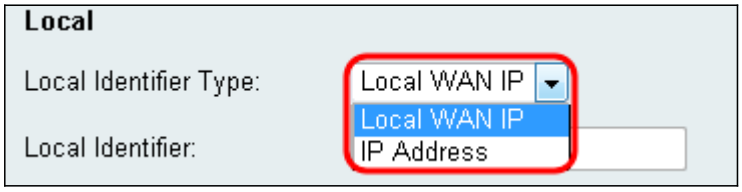
Schritt 4: Wählen Sie aus dem Dropdown-Menü *Exchange Mode (Austauschmodus*) den Modus aus, in dem ein Schlüsselaustausch zum Aufbau einer sicheren Kommunikation verwendet wird.



Die verfügbaren Optionen sind wie folgt definiert:

- Main (Hauptmodus): Schützt die Identität von Peers zur Erhöhung der Sicherheit.
- Aggressiv - Kein Schutz der Peer-Identität, aber schnellere Verbindungen

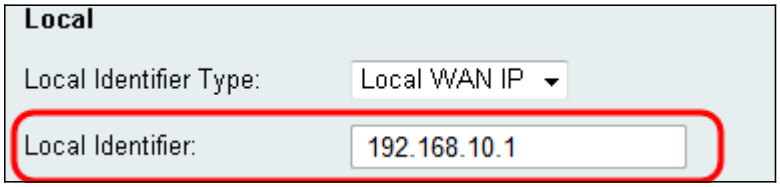
Schritt 5: Wählen Sie aus dem Dropdown-Menü *Local Identifier Type (Lokaler Identifikationstyp*) den Identitätstyp, über den das Profil verfügt.



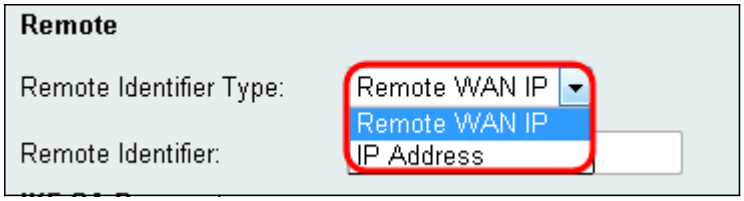
Die verfügbaren Optionen sind wie folgt definiert:

- Lokale WAN (Internet) IP - Verbindung über das Internet.
- IP-Adresse - Eindeutige Zeichenfolge von Zahlen, die durch Punkte getrennt sind und jeden Computer identifiziert, der das Internet-Protokoll für die Kommunikation über ein Netzwerk verwendet.

Schritt 6. (Optional) Wenn in Schritt 5 in der Dropdown-Liste eine **IP-Adresse** ausgewählt ist, geben Sie die lokale IP-Adresse in das Feld *Lokale ID ein*.



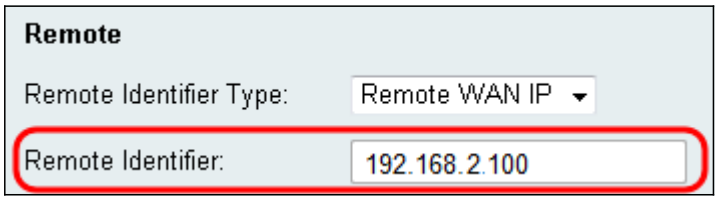
Schritt 7: Wählen Sie aus dem Dropdown-Menü *Remote Identifier Type (Remote-Identifizierertyp*) den Identitätstyp aus, über den das Profil verfügt.



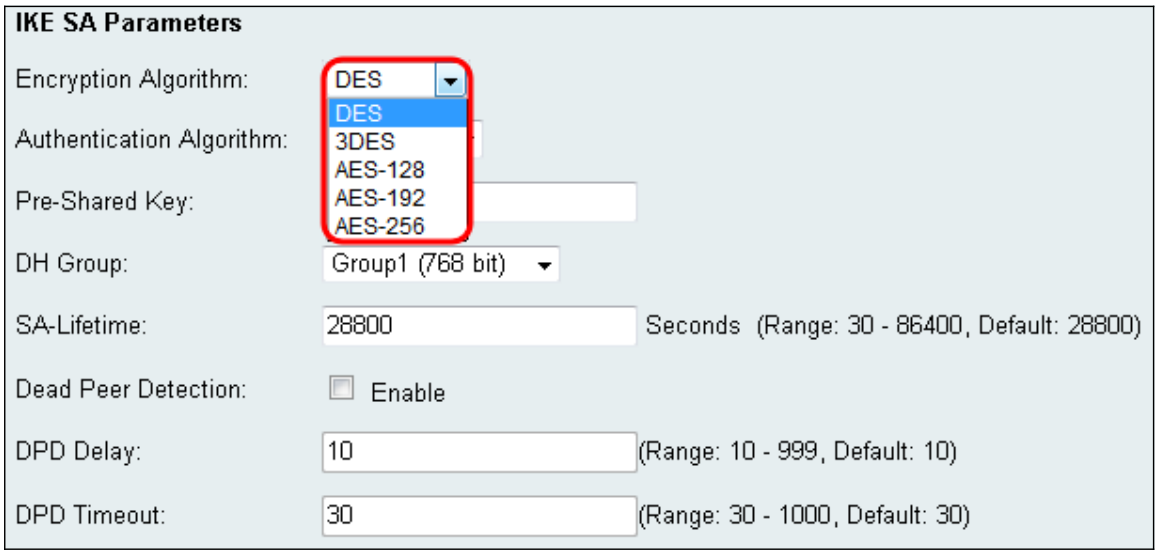
Die verfügbaren Optionen sind wie folgt definiert:

- Lokale WAN (Internet) IP - Verbindung über das Internet.
- IP-Adresse - Eindeutige Zeichenfolge von Zahlen, die durch Punkte getrennt sind und jeden Computer identifiziert, der das Internet-Protokoll für die Kommunikation über ein Netzwerk verwendet.

Schritt 8. (Optional) Wenn in Schritt 7 in der Dropdown-Liste die Option **IP-Adresse** ausgewählt ist, geben Sie die Remote-IP-Adresse in das Feld *Remote Identifier (Remote-Kennung) ein*.



Schritt 9: Wählen Sie im Dropdown-Menü *Encryption Algorithm* (Verschlüsselungsalgorithmus) einen Algorithmus zur Verschlüsselung Ihrer Kommunikation aus. **AES-128** wird als Standard ausgewählt.

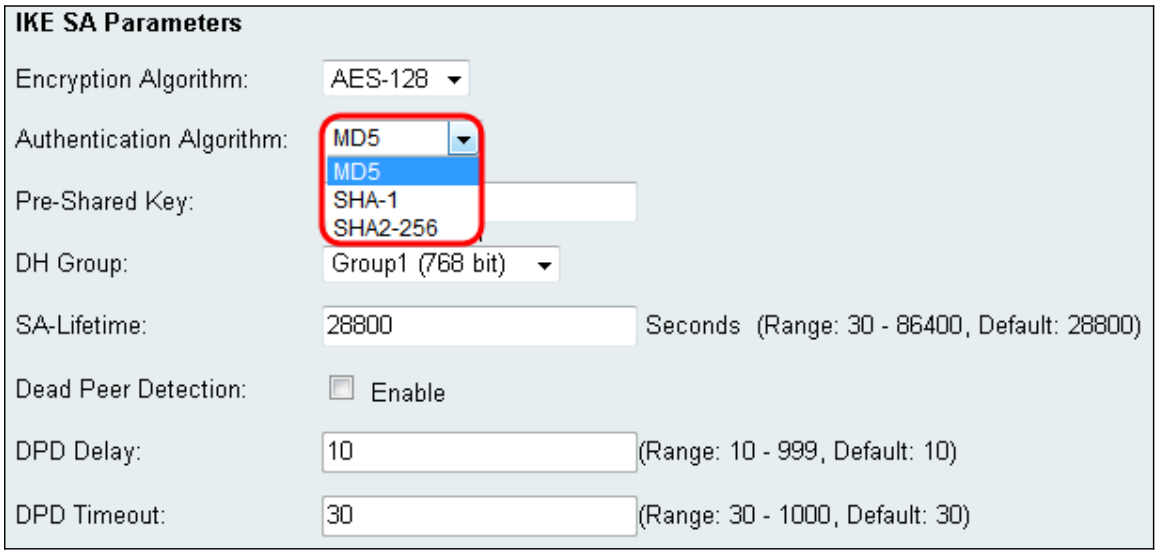


Die verfügbaren Optionen sind für die kleinste bis größte Sicherheit wie folgt aufgeführt:

- DES - Data Encryption Standard.
- 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.

Anmerkung: AES ist die Standardmethode für die Verschlüsselung über DES und 3DES für eine höhere Leistung und Sicherheit. Durch die Verlängerung des AES-Schlüssels wird die Sicherheit erhöht und gleichzeitig die Leistung verringert. AES-128 wird empfohlen, da es den besten Kompromiss zwischen Geschwindigkeit und Sicherheit bietet.

Schritt 10: Wählen Sie aus dem Dropdown-Menü *Authentifizierungsalgorithmus* einen Algorithmus zur Authentifizierung der Kommunikation aus. **SHA-1** wird als Standard ausgewählt.

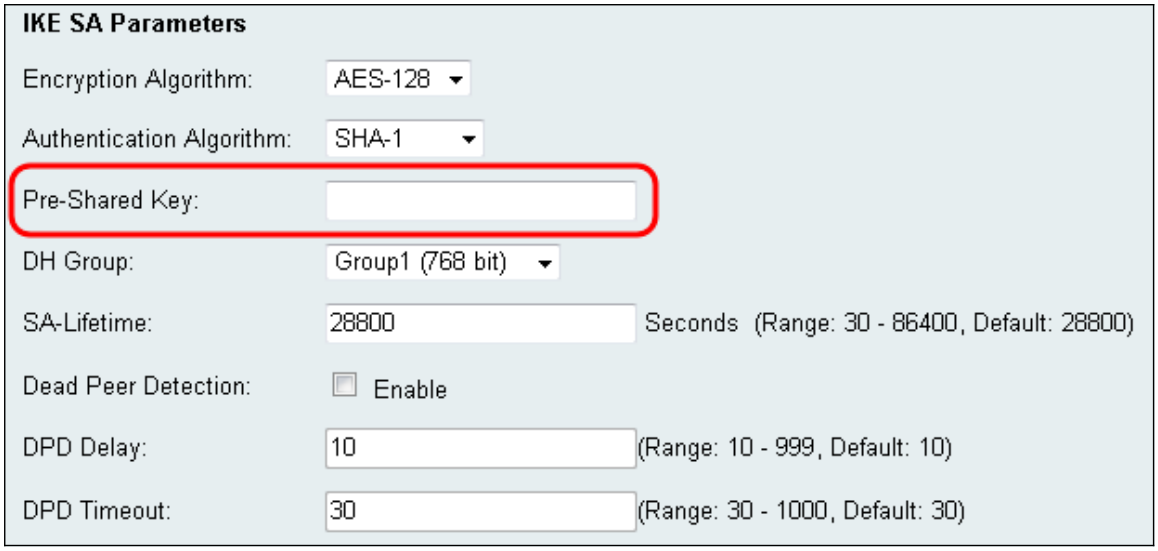


Die verfügbaren Optionen sind wie folgt definiert:

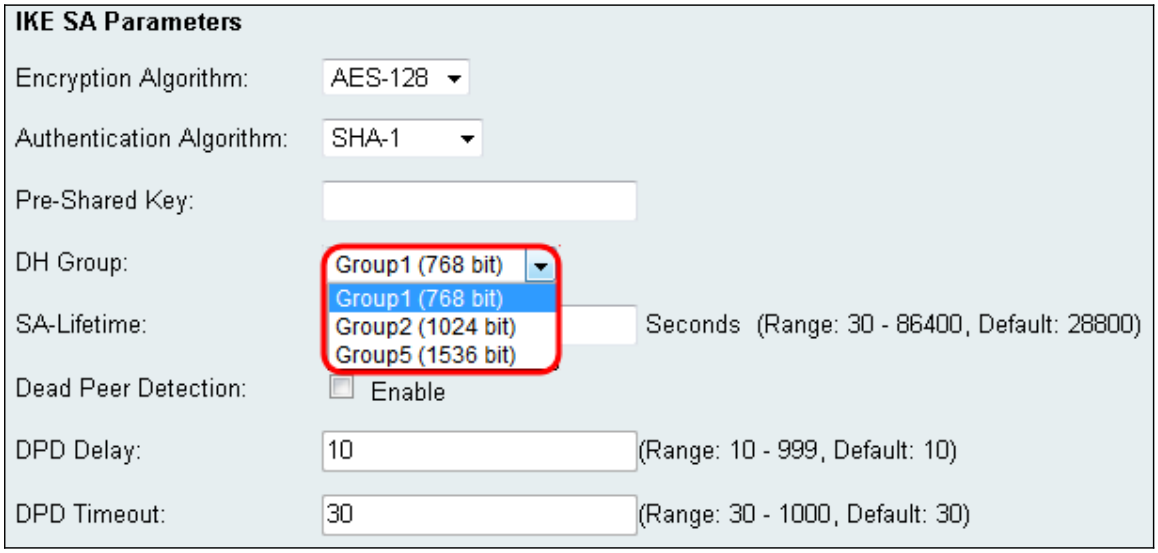
- MD5 - Message Digest Algorithm hat einen 128 Bit Hash-Wert.
- SHA-1 - Secure Hash Algorithm hat einen 160-Bit-Hash-Wert.
- SHA2-256: Sicherer Hash-Algorithmus mit einem 256-Bit-Hash-Wert.

Anmerkung: MD5 und SHA sind beide kryptografische Hashfunktionen. Sie nehmen ein Datenelement, kompaktieren es und erzeugen eine einzigartige Hexadezimalausgabe, die normalerweise nicht reproduzierbar ist. MD5 bietet im Wesentlichen keine Sicherheit gegen Hashing-Kollisionen und sollte nur in Umgebungen kleiner und mittlerer Unternehmen eingesetzt werden, in denen eine Kollisionsabwehr nicht erforderlich ist. SHA1 ist eine bessere Wahl als der MD5, da er bessere Sicherheit bei vernachlässigbar langsameren Geschwindigkeiten bietet. Für optimale Ergebnisse hat SHA2-256 keine bekannten Angriffe von praktischer Relevanz und bietet die beste Sicherheit. Wie bereits erwähnt, bedeutet höhere Sicherheit langsamere Geschwindigkeiten.

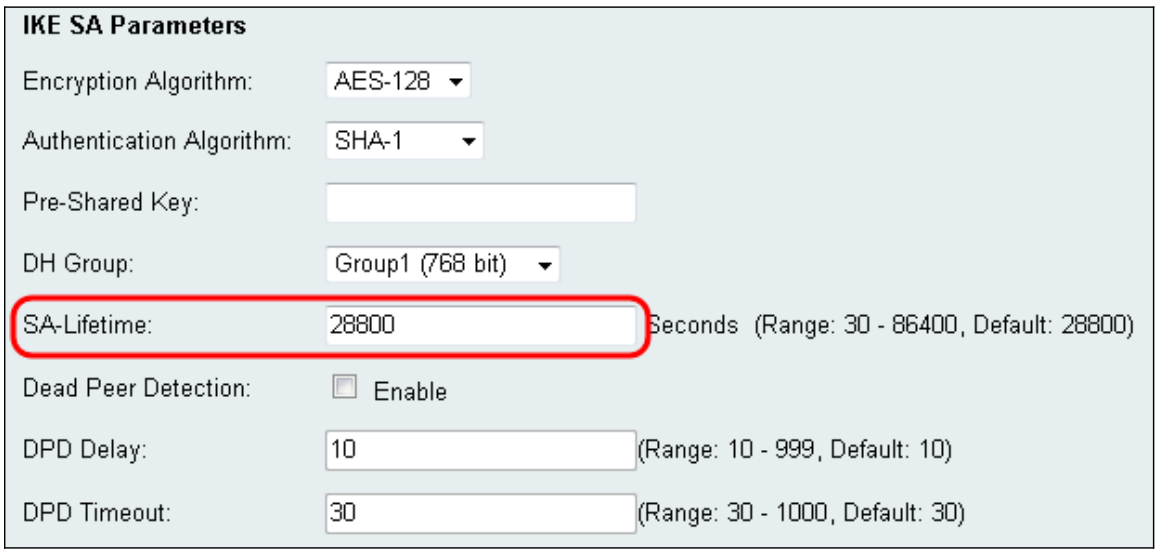
Schritt 11: Geben Sie im Feld "*Pre-Shared Key*" ein Kennwort mit einer Länge zwischen 8 und 49 Zeichen ein.



Schritt 12: Wählen Sie aus dem Dropdown-Menü *DH Group* (DH-Gruppe) eine DH-Gruppe aus. Die Anzahl der Bit gibt die Sicherheitsstufe an. Beide Enden der Verbindung müssen derselben Gruppe angehören.

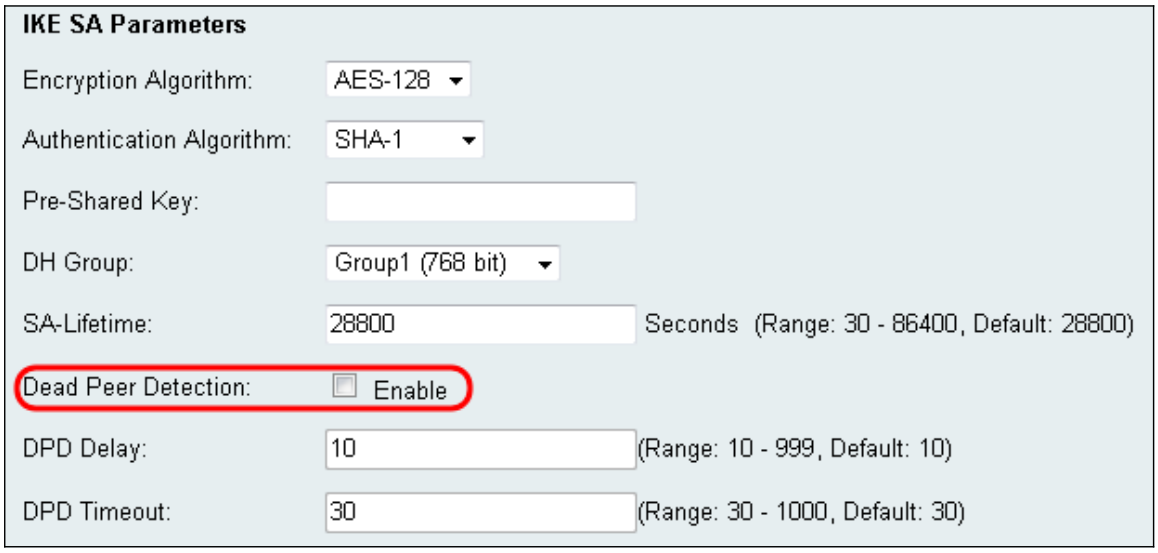


Schritt 13: Geben Sie im Feld *SA-Lifetime* (*SA-Lebensdauer*) an, wie lange die Sicherheitszuordnung in Sekunden gültig sein soll. Der Standardwert ist 28800 Sekunden.

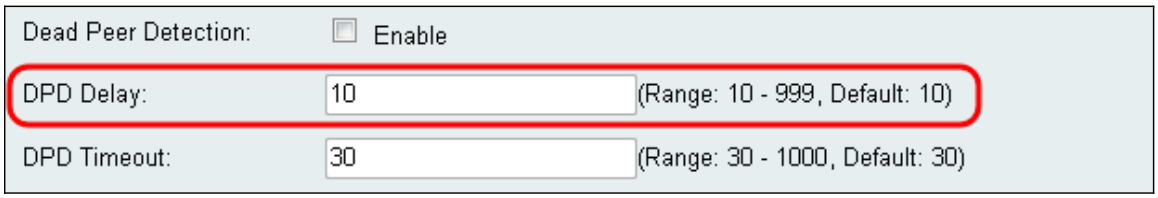


Schritt 14. (Optional) Aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld *Dead Peer*

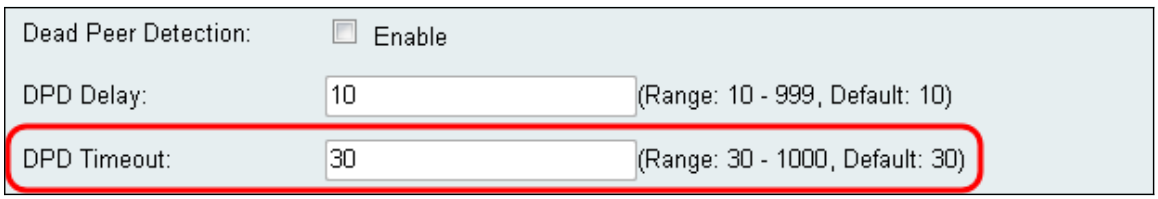
Detection (Dead Peer-Erkennung), wenn Sie eine Verbindung mit inaktivem Peer deaktivieren möchten. Fahren Sie mit Schritt 17 fort, wenn Sie die Dead peer Detection nicht aktiviert haben.



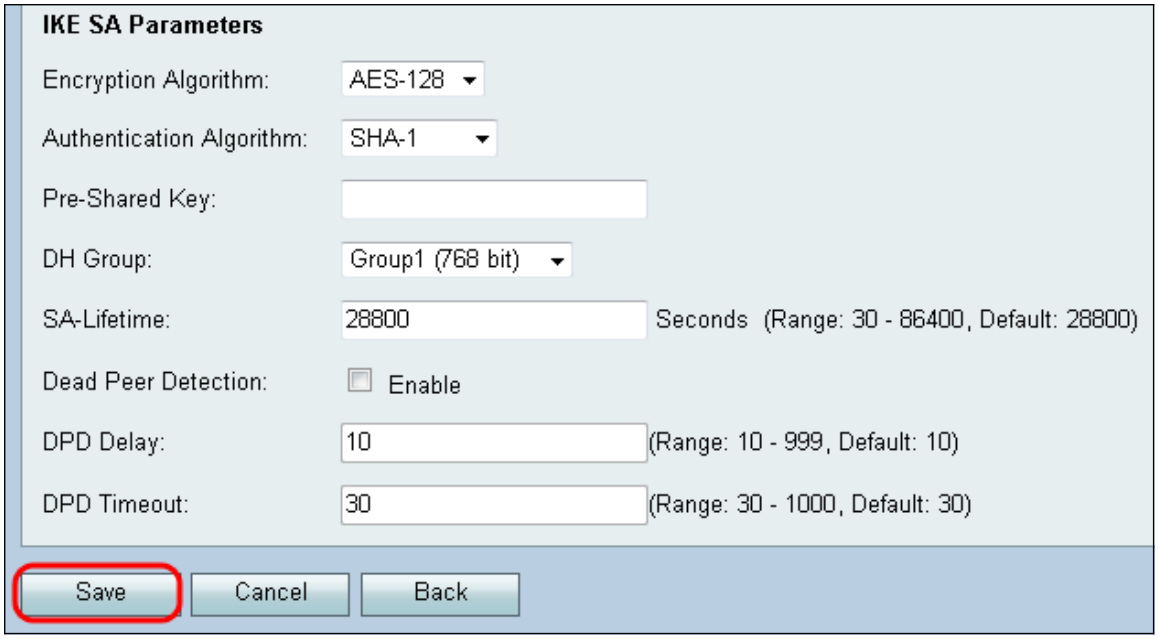
Schritt 15: (Optional) Wenn Sie die Dead Peer Detection (DPD-Erkennung) aktiviert haben, geben Sie einen Wert in das Feld *DPD Delay (DPD-Verzögerung) ein*. Dieser Wert gibt an, wie lange der Router auf die Überprüfung der Client-Verbindung wartet.



Schritt 16: (Optional) Wenn Sie die Dead Peer Detection (DPD-Erkennung) aktiviert haben, geben Sie im Feld *DPD-Zeitüberschreitung* einen Wert ein. Dieser Wert gibt an, wie lange der Client verbunden bleibt, bis das Zeitlimit erreicht ist.



Schritt 17: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.


IKE SA Parameters
Encryption Algorithm:
AES-128
Authentication Algorithm:
SHA-1
Pre-Shared Key:
DH Group:
Group1 (768 bit)
SA-Lifetime:
28800
Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:
Enable
DPD Delay:
10
(Range: 10 - 999, Default: 10)
DPD Timeout:
30
(Range: 30 - 1000, Default: 30)
Save
Cancel
Back

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.