Konfigurieren der erweiterten Einstellungen für Gateway-to-Gateway-VPN auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Ein Virtual Private Network (VPN) ist ein privates Netzwerk, das verwendet wird, um Geräte des Remote-Benutzers virtuell über ein öffentliches Netzwerk zu verbinden, um Sicherheit zu gewährleisten. Insbesondere ermöglicht eine Gateway-to-Gateway-VPN-Verbindung, dass zwei Router sicher miteinander verbunden sind und dass ein Client an einem Ende logisch Teil desselben Remote-Netzwerks am anderen Ende zu sein scheint. So können Daten und Ressourcen einfacher und sicherer über das Internet gemeinsam genutzt werden. Auf beiden Seiten der Verbindung muss eine identische Konfiguration vorgenommen werden, damit eine erfolgreiche Gateway-to-Gateway-VPN-Verbindung aufgebaut werden kann.

Die erweiterte Gateway-to-Gateway-VPN-Konfiguration bietet die Flexibilität, optionale Konfigurationen für den VPN-Tunnel zu konfigurieren, um die Benutzerfreundlichkeit für die VPN-Benutzer zu erhöhen. Die erweiterten Optionen sind nur für IKE mit dem Modus "Vorinstallierter Schlüssel" verfügbar. Die erweiterten Einstellungen sollten auf beiden Seiten der VPN-Verbindung identisch sein.

In diesem Dokument wird erläutert, wie Sie erweiterte Einstellungen für den Gateway-to-Gateway-VPN-Tunnel auf den VPN-Routern RV016, RV042, RV042G und RV082 konfigurieren.

Hinweis: Weitere Informationen zum Konfigurieren eines Gateway-zu-Gateway-VPN finden Sie im Artikel *Konfiguration von Gateway-zu-Gateway-VPN auf RV016-, RV042-, RV042G- und RV082-VPN-Routern.*

Unterstützte Geräte

RV016
â€¢RV042
ãƒ» RV042G
RV082

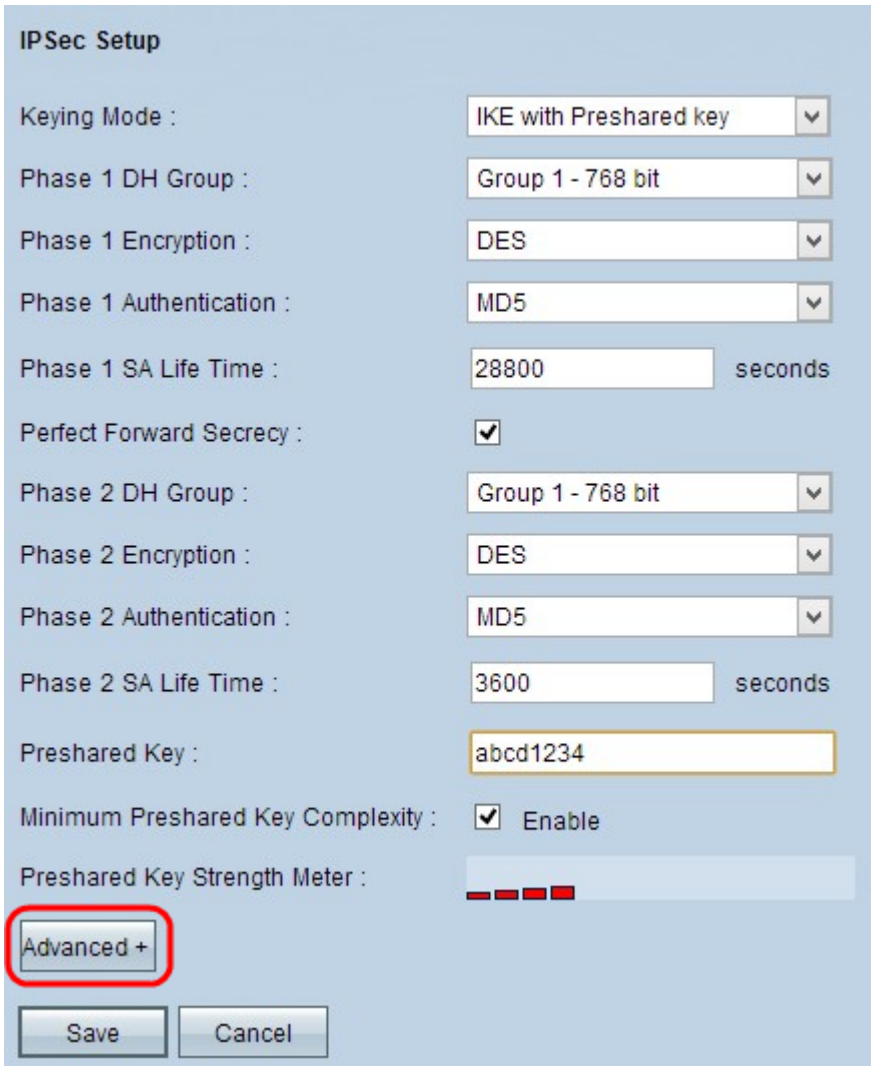
Software-Version

ãƒ» v4.2.2.08

Konfiguration der erweiterten Einstellungen für Gateway-to-Gateway-VPN

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **VPN > Gateway To Gateway aus**. Die Seite *Gateway To Gateway* wird geöffnet:

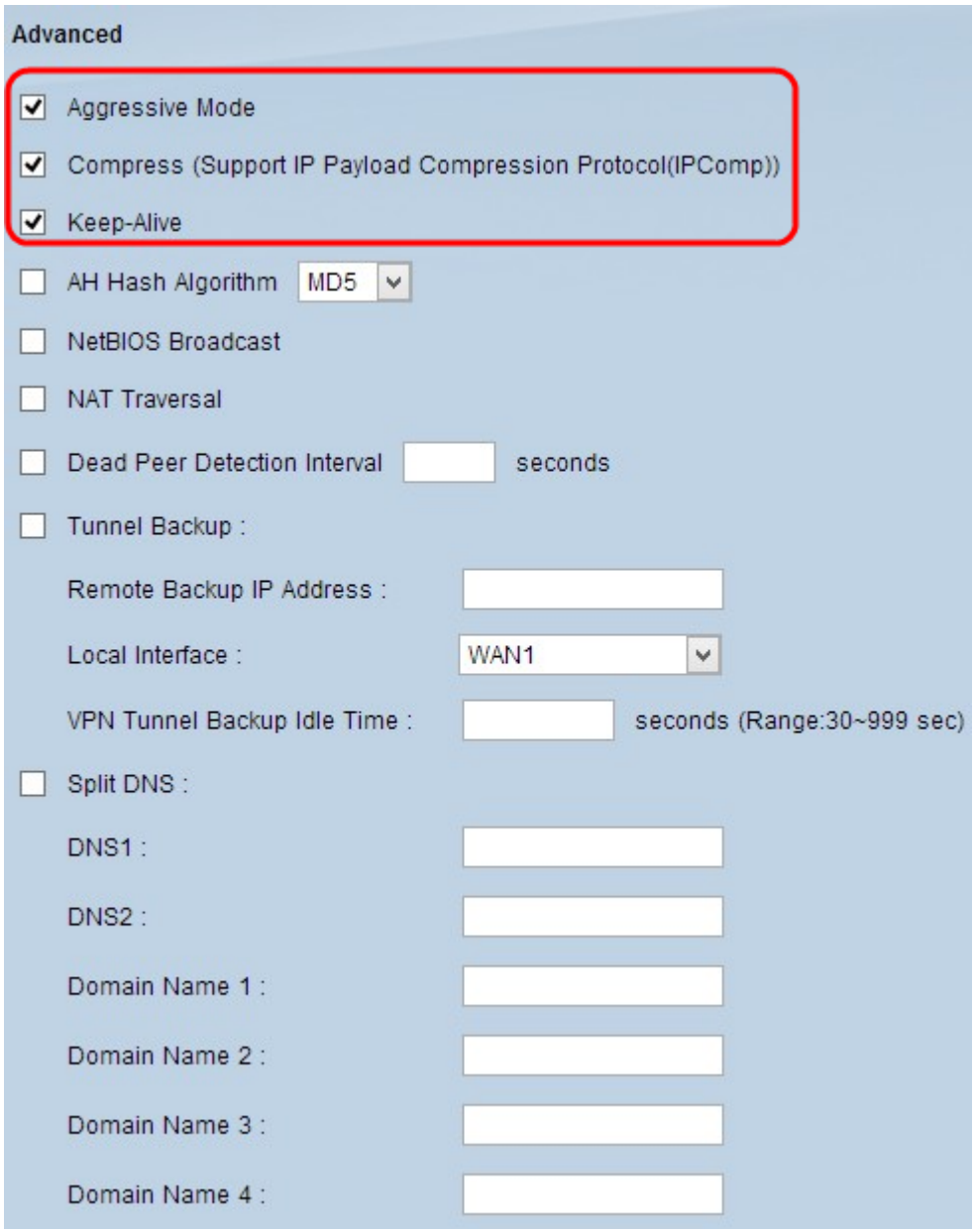
Schritt 2: Blättern Sie nach unten zum Abschnitt *IPSec-Setup*, und klicken Sie auf **Advanced +**. Der Bereich *Erweitert* wird angezeigt:



Schritt 3: Aktivieren Sie das Kontrollkästchen **Aggressive Mode** (Aggressiver Modus), wenn Ihre Netzwerkgeschwindigkeit niedrig ist. Dadurch werden die IDs der Endpunkte des Tunnels während der SA-Verbindung (Phase 1) im Klartext ausgetauscht, was weniger Zeit für den Austausch benötigt, aber weniger Sicherheit bietet.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Compress (Support IP Payload Compression Protocol (IPComp))**, wenn Sie die Größe der IP-Datagramme komprimieren möchten. IPComp ist ein IP-Komprimierungsprotokoll, mit dem die Größe von IP-Datagrammen komprimiert wird. Die IP-Komprimierung ist nützlich, wenn die Netzwerkgeschwindigkeit niedrig ist und der Benutzer die Daten schnell und ohne Verluste über das langsame Netzwerk übertragen möchte, jedoch keine Sicherheit bietet.

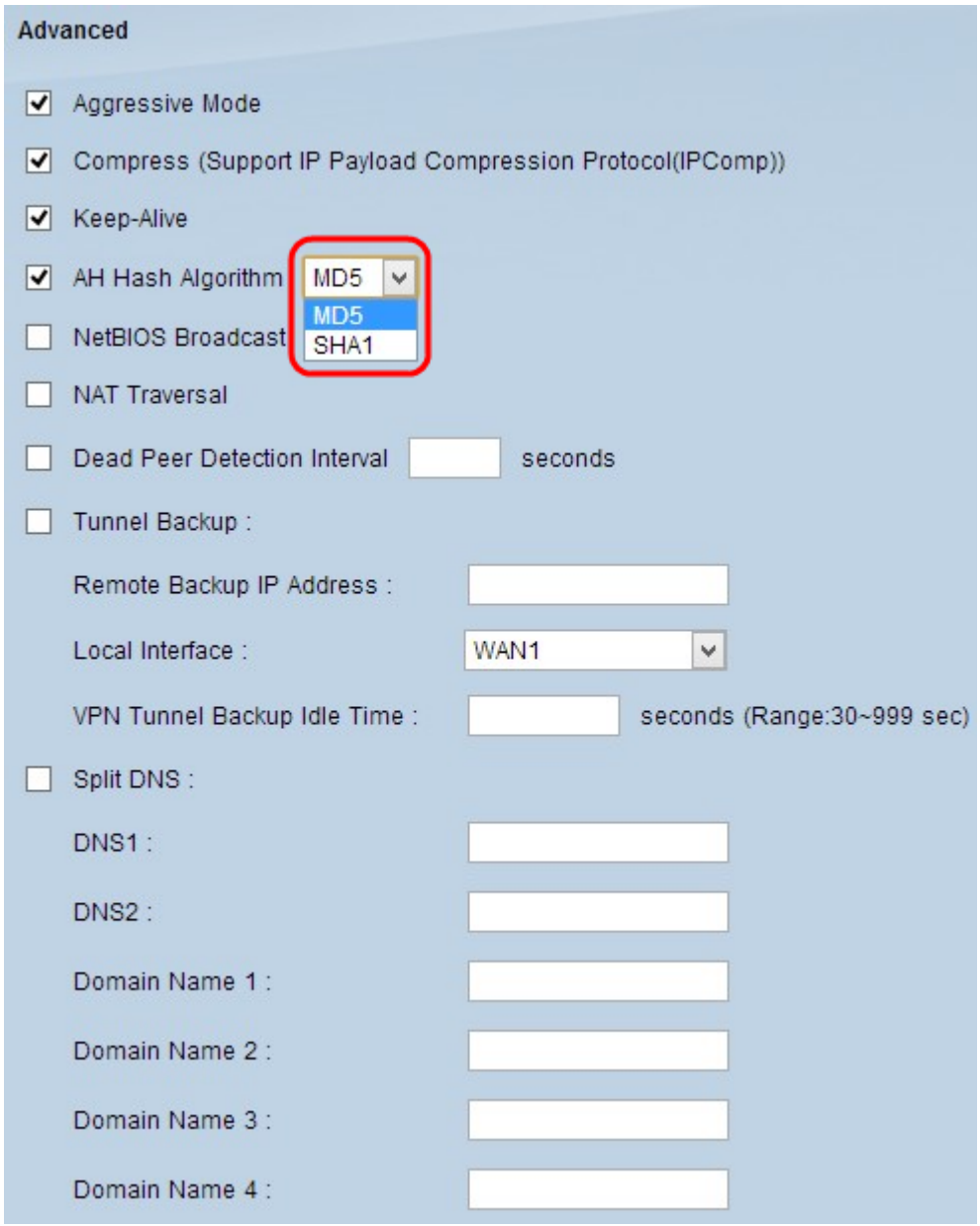
Schritt 5: Aktivieren Sie das Kontrollkästchen **Keep-Alive**, wenn die Verbindung des VPN-Tunnels immer aktiv bleiben soll. Keep-Alive hilft, die Verbindungen sofort wiederherzustellen, wenn eine Verbindung inaktiv wird.



Schritt 6: Aktivieren Sie das Kontrollkästchen **AH Hash Algorithm**, wenn Sie Authenticate Header (AH) aktivieren möchten. AH bietet Authentifizierung für Ursprungsdaten, Datenintegrität durch Prüfsumme und Schutz im IP-Header. Der Tunnel sollte für beide Seiten den gleichen Algorithmus haben.

ãƒ» MD5 â€" Message Digest Algorithm-5 (MD5) ist eine 128-stellige hexadezimale Hash-Funktion, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.

ãƒ» SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5, aber mehr Zeit für die Berechnung benötigt.

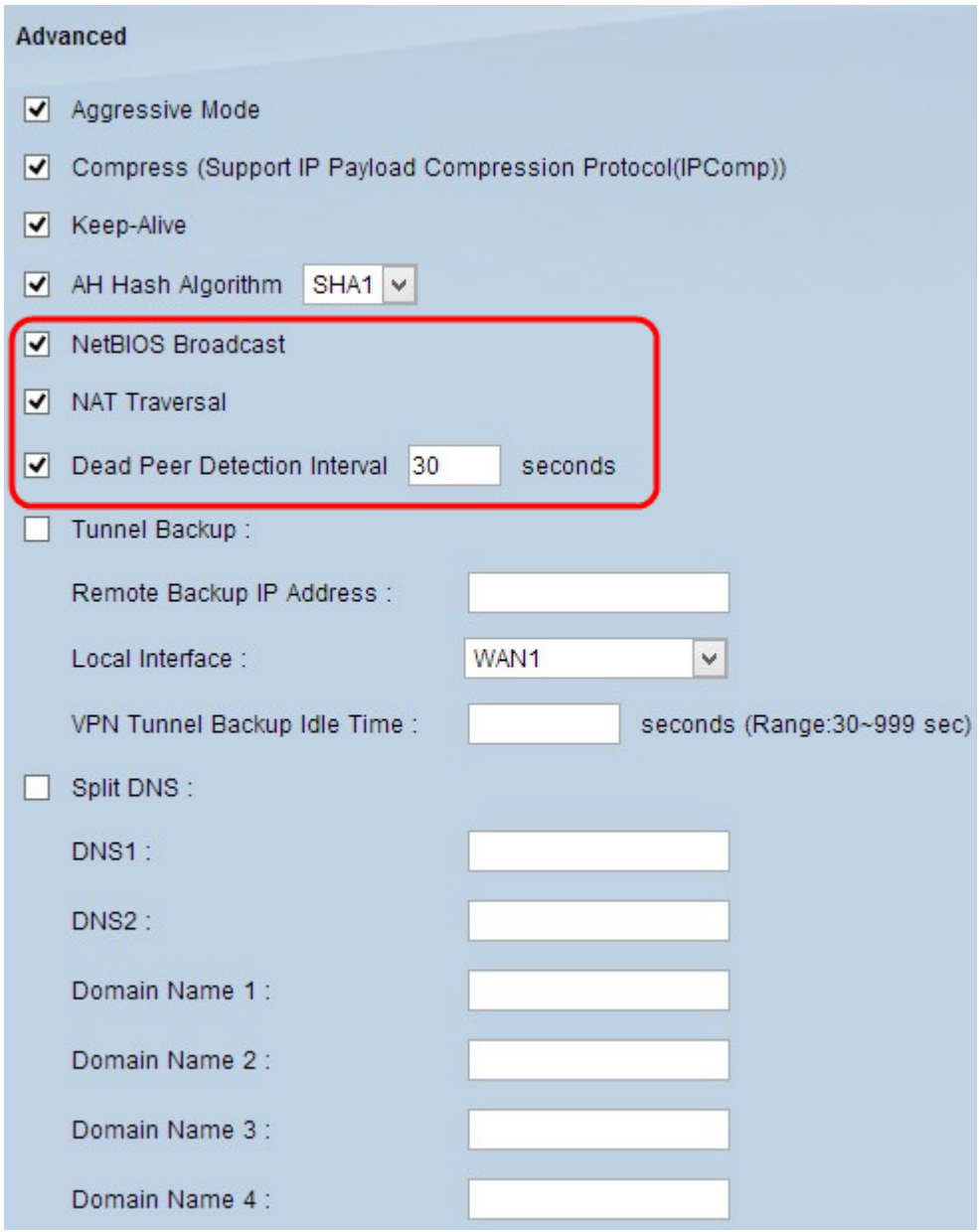


Schritt 7. Aktivieren Sie das Kontrollkästchen **NetBIOS Broadcast** (Nicht routbarer Datenverkehr durch den VPN-Tunnel), wenn Sie nicht routbaren Datenverkehr zulassen möchten. Standardmäßig ist diese Option deaktiviert. NetBIOS wird verwendet, um Netzwerkressourcen wie Drucker und Computer im Netzwerk über einige Softwareanwendungen und Windows-Funktionen wie Netzwerkumgebung zu erkennen.

Schritt 8: Aktivieren Sie das Kontrollkästchen **NAT Traversal**, wenn Sie von Ihrem privaten LAN aus über eine öffentliche IP-Adresse auf das Internet zugreifen möchten. Wenn sich Ihr VPN-Router hinter einem NAT-Gateway befindet, aktivieren Sie dieses Kontrollkästchen, um NAT-Traversal zu aktivieren. Beide Enden des Tunnels müssen die gleichen Einstellungen aufweisen.

Schritt 9. Überprüfen Sie das **Intervall für** die **Erkennung** von **abgestorbenen Peers**, um die Lebhaftigkeit des VPN-Tunnels durch hello oder ACK in regelmäßigen Abständen zu überprüfen. Wenn Sie dieses Kontrollkästchen aktivieren, geben Sie das Intervall (in Sekunden) zwischen den Hello-Nachrichten ein.

Hinweis: Wenn Sie das Dead Peer Detection Interval (Intervall für die Dead Peer-Erkennung) nicht aktivieren, fahren Sie mit Schritt 11 fort.

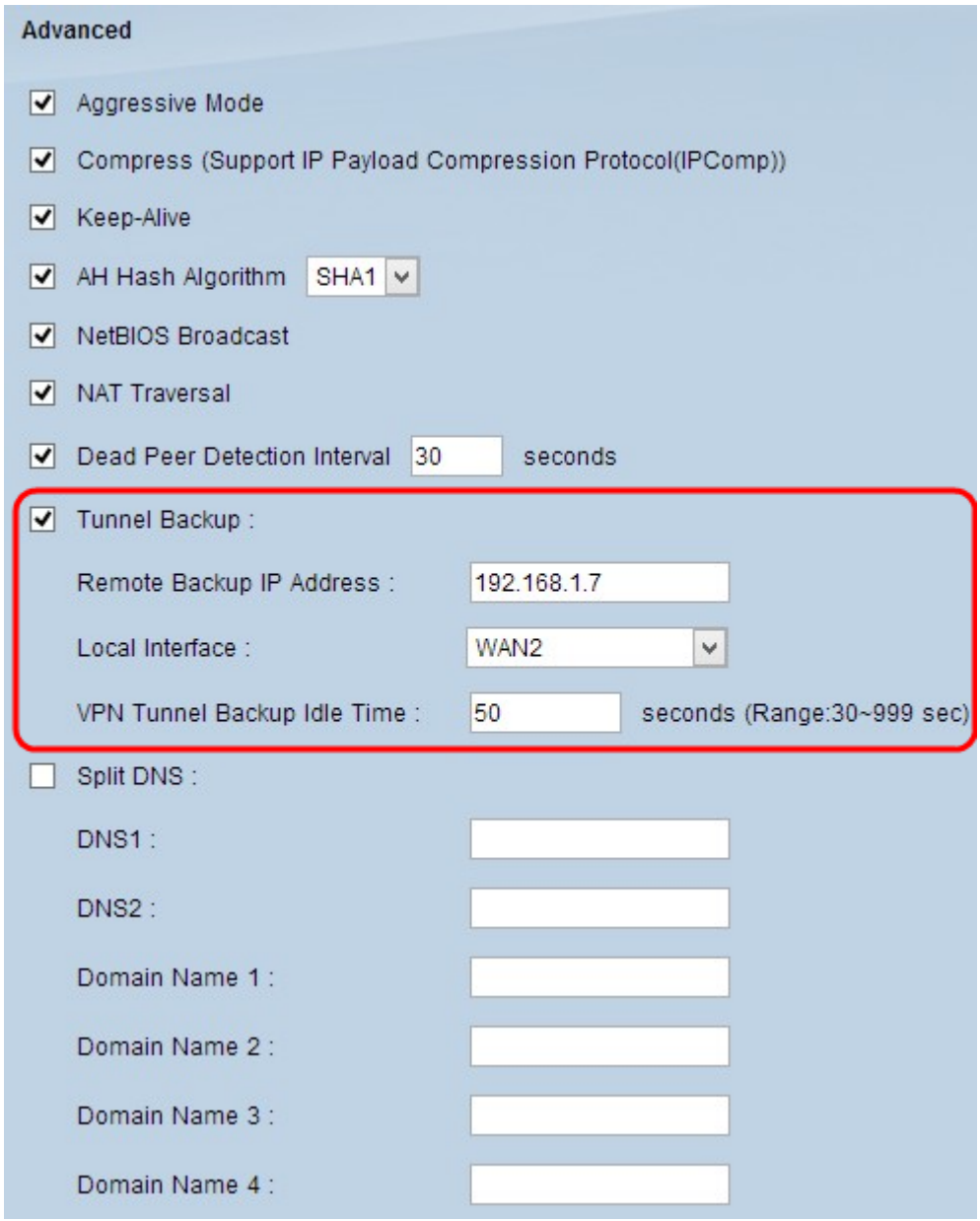


Schritt 10. Aktivieren Sie das Kontrollkästchen **Tunnelsicherung**, um die Tunnelsicherung zu aktivieren. Diese Funktion ist nur verfügbar, wenn das Intervall für die Erkennung von toten Peers aktiviert wurde. Mit dieser Funktion kann das Gerät den VPN-Tunnel über eine alternative lokale WAN-Schnittstelle oder eine Remote-IP-Adresse wiederherstellen.

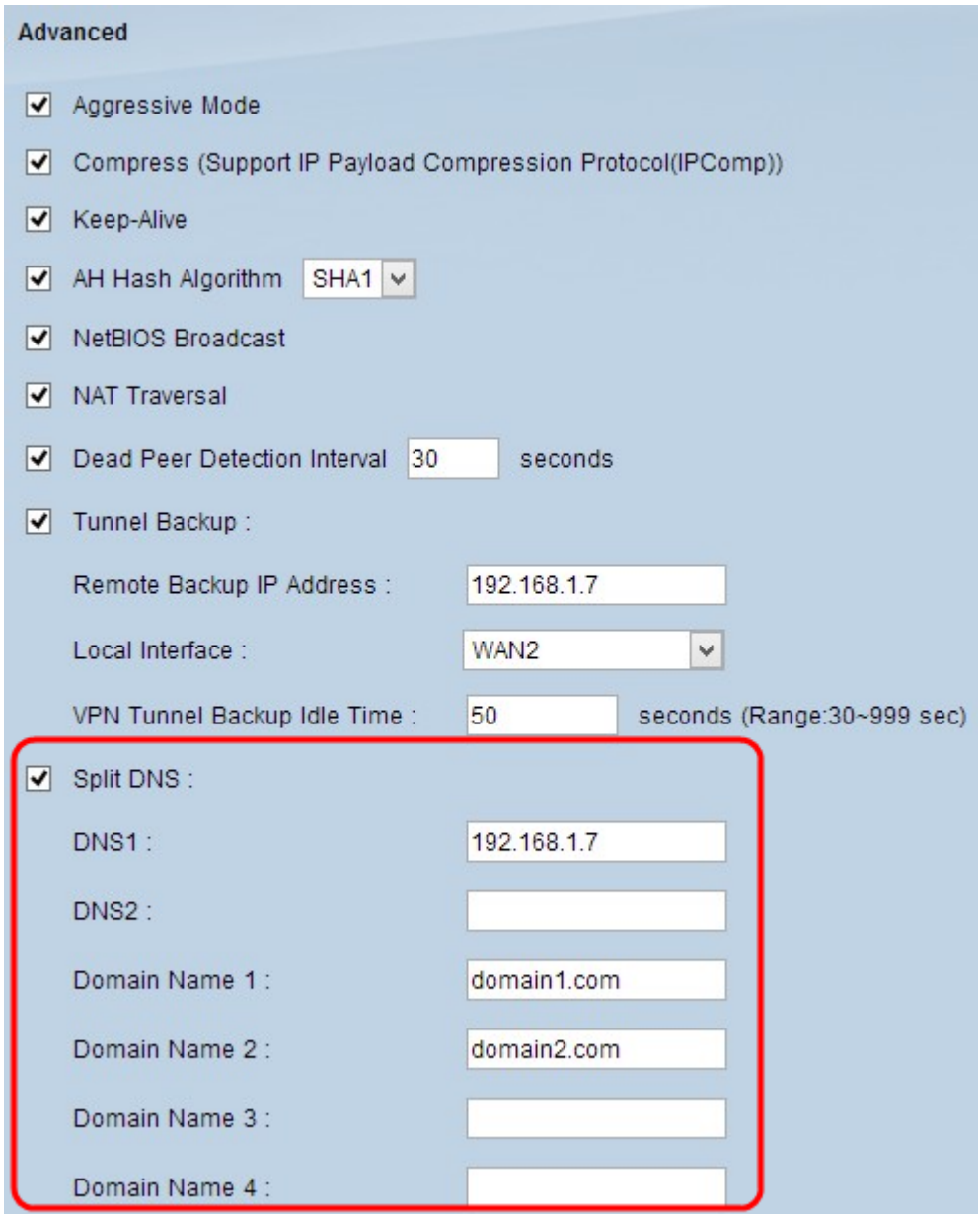
ãƒ» Remote-Backup-IP-Adresse â€" Geben Sie eine alternative IP-Adresse für das Remote-Gateway ein, oder geben Sie die WAN-IP-Adresse ein, die bereits für das Remote-Gateway in diesem Feld festgelegt wurde.

ãƒ» Lokale Schnittstelle - Die WAN-Schnittstelle, die zum Wiederherstellen der Verbindung verwendet wird. Wählen Sie die gewünschte Schnittstelle aus der Dropdown-Liste aus.

ãƒ» Leerlaufzeit des VPN-Tunnels für die Sicherung â€" Geben Sie die Zeit (in Sekunden) ein, die der primäre Tunnel verbinden muss, bevor der Backup-Tunnel verwendet wird.



Schritt 11. Aktivieren Sie das Kontrollkästchen **Split DNS**, um Split DNS zu aktivieren. Mithilfe von Split-DNS können Anforderungen für bestimmte Domänennamen von einem anderen als dem üblicherweise verwendeten DNS-Server verarbeitet werden. Wenn der Router eine DNS-Anforderung vom Client empfängt, überprüft er die DNS-Anforderung und stimmt mit dem Domänennamen überein und sendet die Anforderung an den entsprechenden DNS-Server.



Schritt 12: Geben Sie die IP-Adresse des DNS-Servers in das Feld *DNS1* ein. Wenn ein anderer DNS-Server vorhanden ist, geben Sie die IP-Adresse des DNS-Servers in das Feld *DNS2 ein*.

Schritt 13: Geben Sie die Domänennamen in die Felder *Domänenname 1* bis *Domänenname 4 ein*. Anforderungen für diese Domänennamen werden von den in Schritt 12 angegebenen DNS-Servern verarbeitet.

Schritt 14: Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

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.