

Konfiguration eines Backup Virtual Private Network (VPN)-Tunnels auf den VPN-Routern RV042, RV042G und RV082

Ziel

Ein VPN ist ein privates Netzwerk, das verwendet wird, um Netzwerke über Tunneling-Protokolle remote und sicher zu verbinden. Ein Backup-VPN-Tunnel stellt sicher, dass eine Verbindung aufrechterhalten wird, wenn der primäre VPN-Tunnel keine Verbindung herstellen kann.

In diesem Dokument wird erläutert, wie Sie einen VPN-Backup-Tunnel zwischen zwei Routern auf den VPN-Routern RV042, RV042G und RV082 konfigurieren.

Hinweis: Weitere Informationen zur Konfiguration von Gateway zu Gateway-VPN finden Sie unter [Konfiguration von Gateway zu Gateway-VPN auf RV016-, RV042-, RV042G- und RV082-VPN-Routern](#).

Unterstützte Geräte

• RV042
• RV042G
• RV082

Konfiguration des Backup-Tunnels

Erweiterte VPN-Konfiguration

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

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2
Tunnel Name :
Interface : WAN1 ▾
Enable :

Local Group Setup

Local Security Gateway Type : IP Only ▾
IP Address : 0.0.0.0
Local Security Group Type : Subnet ▾
IP Address : 192.168.1.0
Subnet Mask : 255.255.255.0

Remote Group Setup

Remote Security Gateway Type : IP Only ▾
IP Address ▾ :
Remote Security Group Type : Subnet ▾
IP Address :
Subnet Mask : 255.255.255.0

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

IPSec Setup

Keying Mode : IKE with Preshared key ▾

Phase 1 DH Group : Group 1 - 768 bit ▾

Phase 1 Encryption : DES ▾

Phase 1 Authentication : MD5 ▾

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit ▾

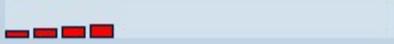
Phase 2 Encryption : DES ▾

Phase 2 Authentication : MD5 ▾

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Advanced +

Save Cancel

Schritt 3: Blättern Sie nach unten zu Dead Peer Detection Interval (Intervall für die **Dead Peer-Erkennung**), und aktivieren Sie das Kontrollkästchen **Dead Peer Detection Interval (Intervall für die Dead Peer-Erkennung)**, um die Lebhaftigkeit des VPN-Tunnels durch Hellos oder ACKs in regelmäßigen Abständen zu überprüfen.

Dead Peer Detection Interval 10 seconds

Tunnel Backup :

Remote Backup IP Address : 192.168.3.131

Local Interface : WAN2 ▾

VPN Tunnel Backup Idle Time : 30 seconds (Range:30~999 sec)

Schritt 4: Geben Sie die gewünschte Dauer oder das gewünschte Intervall für die Hello-Nachrichten in das Feld "Intervall für die Dead Peer-Erkennung" in Sekunden ein. Dies ist der Zeitpunkt, zu dem eine Nachricht gesendet werden soll, um den Status der Tunnelverbindung zu überprüfen.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Tunnel Backup (Tunnelsicherung)**, um den VPN-Tunnel zu sichern.

Schritt 6: Geben Sie im Feld Remote Backup IP Address (IP-Adresse für Remote-Backup) die Backup-IP-Adresse für den Remote-Router ein.

Schritt 7. Wählen Sie in der Dropdown-Liste Local Interface (Lokale Schnittstelle) die passende WAN-Schnittstelle für die Backup-Verbindung aus. Wählen Sie die alternative WAN-Schnittstelle für eine andere Backup-Verbindung als die Haupt-VPN-Verbindung aus. Wenn die Haupt-VPN-Verbindung ausfällt, wird nur diese Backup-Verbindung angezeigt.

Schritt 8: Geben Sie im Feld "VPN Tunnel Backup Idle Time" (Leerlaufzeit für VPN-Tunnel-Backup) die Zeit (in Sekunden) ein, die der Router warten muss, bevor er versucht, eine Verbindung zum Backup-Tunnel herzustellen, nachdem der ursprüngliche VPN-Tunnel ausgefallen ist.

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

Smart Link-Sicherungskonfiguration

Die Backup-Konfiguration für Smart Links ermöglicht die Übernahme einer Backup-Verbindung, wenn die primäre Verbindung ausfällt. Daher wird das Smart Link-Backup nur verwendet, wenn die primäre Verbindung ausfällt.

Schritt 10. Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **System Management > Dual WAN** aus. Die Seite *Dual WAN* wird geöffnet:

Dual WAN

Load Balance

Smart Link Backup : Primary WAN WAN1 (Specify which WAN is Primary , the other one will be backup)

Load Balance (Auto Mode)

Interface Setting

Interface	Mode	Configuration
WAN1	Smart Link Backup	
WAN2	Smart Link Backup	

Hinweis: Weitere Informationen zur Konfiguration von Dual-WAN finden Sie unter *Konfigurieren von Smart Link Backup (Failover) auf RV042-, RV042G- und RV082-VPN-Routern*.

Schritt 11. Klicken Sie auf das Optionsfeld **Smart Link Backup**, um die VPN-Verbindung mit der Backup-VPN-Verbindung fortzusetzen, wenn die Haupt-VPN-Verbindung ausfällt.

Schritt 12: Wählen Sie aus der Dropdown-Liste Primary WAN (Primäres WAN) die WAN-Schnittstelle aus, die Sie für die primäre VPN-Verbindung verwendet haben.

Schritt 13: Klicken Sie auf **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.