

Configuration d'un tunnel de réseau privé virtuel (VPN) de secours sur les routeurs VPN RV042, RV042G et RV082

Objectif

Un VPN est un réseau privé utilisé pour connecter des réseaux à distance et en toute sécurité via des protocoles de tunnellation. Un tunnel VPN de secours garantit que si le tunnel VPN principal ne parvient pas à se connecter, une connexion est toujours maintenue.

L'objectif de ce document est de vous guider sur la façon de configurer un tunnel de réseau privé virtuel (VPN) de secours entre deux routeurs sur des routeurs VPN RV042, RV042G et RV082.

Remarque : si vous souhaitez en savoir plus sur la configuration du VPN passerelle à passerelle, reportez-vous à la section [Configuration du VPN passerelle à passerelle sur les routeurs VPN RV016, RV042, RV042G et RV082](#).

Périphériques pertinents

- RV042
- RV042G
- RV082

Configuration du tunnel de secours

Configuration avancée du VPN

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez VPN > Gateway To Gateway. La page Gateway To Gateway s'ouvre :

Gateway To Gateway

Add a New Tunnel

Tunnel No.	2
Tunnel Name :	<input type="text"/>
Interface :	WAN1 ▼
Enable :	<input checked="" type="checkbox"/>

Local Group Setup

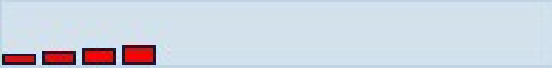
Local Security Gateway Type :	IP Only ▼
IP Address :	0.0.0.0
Local Security Group Type :	Subnet ▼
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only ▼
IP Address ▼ :	<input type="text"/>
Remote Security Group Type :	Subnet ▼
IP Address :	<input type="text"/>
Subnet Mask :	255.255.255.0

Étape 2. Faites défiler jusqu'à la section Advanced et cliquez sur Advanced. La zone Avancé s'affiche.

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 :	<input checked="" type="checkbox"/>	
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 :	<input type="text"/>	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/>	Enable
Preshared Key Strength Meter :		
Advanced +		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Étape 3. Faites défiler jusqu'à Dead Peer Detection Interval et cochez la case Dead Peer Detection Interval pour vérifier la vitalité du tunnel VPN via les paquets Hello ou ACK de manière périodique.

<input checked="" type="checkbox"/>	Dead Peer Detection Interval	<input type="text" value="10"/>	seconds
<input checked="" type="checkbox"/>	Tunnel Backup :		
	Remote Backup IP Address :	<input type="text" value="192.168.3.131"/>	
	Local Interface :	<input type="text" value="WAN2"/>	<input type="button" value="v"/>
	VPN Tunnel Backup Idle Time :	<input type="text" value="30"/>	seconds (Range:30~999 sec)

Étape 4. Entrez la durée ou l'intervalle souhaité des messages Hello dans le champ Dead Peer Detection Interval en secondes. Il s'agit de la fréquence à laquelle un message doit être envoyé pour vérifier l'état de la connexion du tunnel.

Étape 5. Cochez la case Tunnel Backup pour sauvegarder le tunnel VPN.

Étape 6. Dans le champ Remote Backup IP Address, saisissez l'adresse IP de sauvegarde du routeur distant.

Étape 7. Dans la liste déroulante Local Interface, sélectionnez l'interface WAN appropriée pour la connexion de secours. Choisissez l'interface WAN alternative pour une connexion de secours autre que la connexion VPN principale. Si la connexion VPN principale échoue, seule cette connexion de secours apparaît.

Étape 8. Dans le champ VPN Tunnel Backup Idle Time, saisissez la durée (en secondes) pendant laquelle le routeur doit attendre avant d'essayer de se connecter au tunnel de secours après l'échec du tunnel VPN initial.

Étape 9. Cliquez sur Save.

Configuration de sauvegarde Smart Link

La configuration de sauvegarde Smart Link permet à une liaison de sauvegarde de prendre le relais en cas de défaillance de la liaison principale. Par conséquent, la sauvegarde de liaison intelligente est utilisée uniquement en cas de défaillance de la liaison principale.

Étape 10. Connectez-vous à l'utilitaire de configuration Web et choisissez System Management > Dual WAN. La page Dual WAN s'ouvre :



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	

Remarque : si vous souhaitez en savoir plus sur la configuration du double WAN, reportez-vous à la section Configure Smart Link Backup (Failover) on RV042, RV042G and RV082 VPN Routers.

Étape 11. Cliquez sur la case d'option Smart Link Backup pour continuer la connexion VPN avec la connexion VPN de secours si la connexion VPN principale échoue.

Étape 12. Sélectionnez l'interface WAN que vous avez utilisée pour la connexion VPN principale dans la liste déroulante Primary WAN.

Étape 13. Cliquez sur Save.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.