

Configuration du réseau privé virtuel (VPN) du client de groupe sur la passerelle sur les routeurs RV320 et RV325

Objectif

Un réseau privé virtuel (VPN) est un réseau privé utilisé pour connecter virtuellement les périphériques de l'utilisateur distant via le réseau public afin d'assurer la sécurité. Un des types de VPN est un VPN client-passerelle. Avec client-passerelle, vous pouvez connecter à distance différentes filiales de votre entreprise situées dans différentes zones géographiques pour transmettre et recevoir les données entre les zones de manière plus sécurisée. Le VPN de groupe facilite la configuration du VPN car il élimine la configuration du VPN pour chaque utilisateur. La gamme de routeurs VPN RV32x peut prendre en charge un maximum de deux groupes VPN.

L'objectif de ce document est d'expliquer comment configurer un client de groupe à un VPN de passerelle sur les routeurs VPN de la gamme RV32x .

Périphériques pertinents

Routeur VPN double WAN · RV320

Routeur VPN double WAN Gigabit · RV325

Version du logiciel

•v 1.1.0.09

Configurer le client de groupe sur le VPN de passerelle

Étape 1. Connectez-vous à l'utilitaire de configuration du routeur et choisissez **VPN > Client to Gateway**. La *page Client to Gateway* s'ouvre :

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

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 Client Setup

Remote Security Gateway Type:

IP Only

IP Address

:

Étape 2. Cliquez sur la case d'option **Group VPN** pour ajouter un VPN client-passerelle de groupe.

Client to Gateway

Add a New Group VPN

Tunnel **Group VPN** Easy VPN

Group No. 1

Tunnel Name:

Interface:

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type:

IP Address:

Subnet Mask:

Remote Client Setup

Remote Client:

Domain Name:

Ajouter un nouveau tunnel

Étape 1. Entrez le nom du tunnel dans le champ *Nom du tunnel*.

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

Note: Numéro de groupe : représente le numéro du groupe. Il s'agit d'un champ généré automatiquement.

Étape 2. Choisissez l'interface appropriée par laquelle le groupe VPN se connecte à la passerelle dans la liste déroulante *Interface*.

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1
WAN1
WAN2
USB1
USB2

Keying Mode:

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

Étape 3. Cochez la case **Enable** pour activer le VPN passerelle à passerelle. Par défaut, il est activé.

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

Note: Keying Mode : affiche le mode d'authentification utilisé. IKE avec clé prépartagée est la seule option, ce qui signifie que le protocole IKE (Internet Key Exchange) est utilisé pour générer et échanger automatiquement une clé prépartagée afin d'établir une communication authentifiée pour le tunnel.

Étape 4. Pour enregistrer les paramètres dont vous disposez jusqu'à présent et laisser le reste comme valeur par défaut, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration du groupe local

Étape 1. Choisissez l'utilisateur ou le groupe d'utilisateurs LAN local approprié qui peut accéder au tunnel VPN dans la liste déroulante *Local Security Group Type*. La valeur par défaut est « Subnet » (sous-réseau).

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: Subnet

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

Les options disponibles sont définies comme suit :

- IP : un seul périphérique LAN spécifique peut accéder au tunnel. Si vous choisissez cette option, saisissez l'adresse IP de l'appareil LAN dans le champ IP Address (adresse IP). L'adresse IP par défaut est 192.168.1.0.
- Subnet : tous les périphériques LAN d'un sous-réseau spécifique peuvent accéder au tunnel. Si vous choisissez cette option, saisissez l'adresse IP et le masque de sous-réseau des appareils LAN dans les champs IP Address (adresse IP) et Subnet Mask (masque de sous-réseau) respectivement. Le masque par défaut est 255.255.255.0.
- IP Range : une gamme de périphériques LAN peut accéder au tunnel. Si vous choisissez cette option, entrez les première et dernière adresses IP de la plage dans les champs *Start IP* et *End IP* respectivement. La plage par défaut est comprise entre 192.168.1.0 et 192.168.1.254.

Étape 2. Pour enregistrer les paramètres dont vous disposez jusqu'à présent et laisser le reste comme valeur par défaut, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration du client distant

Étape 1. Choisissez l'utilisateur ou le groupe d'utilisateurs LAN distants appropriés qui peuvent accéder au tunnel VPN dans la liste déroulante *Type de groupe de sécurité à distance*.

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: IP

IP Address: 192.168.3.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name: DomainName(FQDN)

Email Address(USER FQDN)
 Microsoft XP/2000 VPN Client

Les options disponibles sont définies comme suit :

Authentification · nom de domaine (FQDN) : l'accès au tunnel est possible via un domaine enregistré. Si vous choisissez cette option, saisissez le nom du domaine enregistré dans le champ Domain Name (nom de domaine).

Authentification · adresse de messagerie (USER FQDN) : l'accès au tunnel est possible par le biais d'une adresse de messagerie. Si vous choisissez cette option, saisissez l'adresse courriel dans le champ Email Address.

·Client VPN Microsoft XP/2000 — L'accès au tunnel est possible via un logiciel client intégré Microsoft XP ou 2000 Client VPN.

Étape 2. Pour enregistrer les paramètres dont vous disposez jusqu'à présent et laisser le reste comme valeur par défaut, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration IPSec

Étape 1. Choisissez le groupe Diffie-Hellman (DH) approprié dans la liste déroulante *Phase 1 DH Group*. La phase 1 est utilisée pour établir le simplex, l'association de sécurité logique (SA) entre les deux extrémités du tunnel afin de prendre en charge la communication sécurisée de l'authentification. Diffie-Hellman est un protocole d'échange de clés cryptographiques utilisé dans la connexion de phase 1 pour partager une clé secrète afin d'authentifier la communication.

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Les options disponibles sont définies comme suit :

- Group1 (768 bits) : calcule la clé le plus rapidement, mais est la moins sécurisée.
- Group2 (1024 bits) : calcule la clé plus lentement, mais elle est plus sécurisée que Group1.
- Group5 (1536 bits) : calcule la clé le plus lentement, mais c'est la clé la plus sécurisée.

Étape 2. Choisissez la méthode de chiffrement appropriée pour chiffrer la clé dans la liste déroulante *Phase 1 Encryption*. AES-128 est recommandé pour sa sécurité élevée et ses performances rapides. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption :

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Les options disponibles sont définies comme suit :

- DES - Data Encryption Standard (DES) est une ancienne méthode de cryptage 56 bits qui n'est pas une méthode de cryptage très sécurisée, mais qui peut être requise pour la rétrocompatibilité.
- 3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits utilisée pour augmenter la taille de la clé, car elle chiffre les données trois fois. Cela offre plus de sécurité que DES, mais moins de sécurité qu'AES.
- AES-128 — Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le chiffrement AES. AES est plus rapide et plus sécurisé que DES. En général, AES est également plus rapide et plus sécurisé que 3DES. La norme AES-128 est plus rapide mais moins sécurisée que les normes AES-192 et AES-256.
- AES-192 — AES-192 utilise une clé 192 bits pour le chiffrement AES. La norme AES-192 est plus lente mais plus sécurisée que la norme AES-128, et plus rapide mais moins sécurisée que la norme AES-256.
- AES-256 — AES-256 utilise une clé de 256 bits pour le chiffrement AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 3. Choisissez la méthode d'authentification appropriée dans la liste déroulante *Authentification de phase 1*. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Les options disponibles sont définies comme suit :

·MD5 — Message Digest Algorithm-5 (MD5) représente une fonction de hachage de 128 bits qui fournit une protection aux données contre les attaques malveillantes par le calcul de la somme de contrôle.

·SHA1 — Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage 160 bits, qui est plus sécurisée que MD5.

Étape 4. Dans le champ *Durée de vie de l'association de sécurité de phase 1*, saisissez la durée en secondes pendant laquelle le tunnel VPN reste actif dans la phase 1. La durée par défaut est de 28 800 secondes.

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Étape 5. (Facultatif) Pour protéger davantage les clés, cochez la case **Perfect Forward Secrecy**. Cette option vous permet de générer une nouvelle clé si une clé est compromise. Il s'agit d'une action recommandée, car elle fournit plus de sécurité.

Remarque : si vous décochez **Perfect Forward Secrecy** à l'étape 5, vous n'avez pas besoin de configurer le groupe DH de phase 2.

Étape 6. Choisissez le groupe DH approprié dans la liste déroulante *Phase 2 DH Group*.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Les options disponibles sont définies comme suit :

- Group1 (768 bits) : calcule la clé le plus rapidement, mais est la moins sécurisée.
- Group2 (1024 bits) : calcule la clé plus lentement, mais elle est plus sécurisée que Group1.
- Group5 (1536 bits) : calcule la clé le plus lentement, mais c'est la clé la plus sécurisée.

Étape 2. Choisissez la méthode de chiffrement appropriée pour chiffrer la clé dans la liste déroulante *Phase 1 Encryption*. AES-128 est recommandé pour sa sécurité élevée et ses performances rapides. Le tunnel VPN doit utiliser la même méthode de chiffrement pour ses deux extrémités.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Les options disponibles sont définies comme suit :

- DES - Data Encryption Standard (DES) est une ancienne méthode de cryptage 56 bits qui n'est pas une méthode de cryptage très sécurisée, mais qui peut être requise pour la rétrocompatibilité.
- 3DES - La norme 3DES (Triple Data Encryption Standard) est une méthode de cryptage simple de 168 bits utilisée pour augmenter la taille de la clé, car elle chiffre les données trois fois. Cela offre plus de sécurité que DES, mais moins de sécurité qu'AES.
- AES-128 — Advanced Encryption Standard avec clé 128 bits (AES-128) utilise une clé 128 bits pour le chiffrement AES. AES est plus rapide et plus sécurisé que DES. En général, AES est également plus rapide et plus sécurisé que 3DES. La norme AES-128 est plus rapide mais moins sécurisée que les normes AES-192 et AES-256.
- AES-192 — AES-192 utilise une clé 192 bits pour le chiffrement AES. La norme AES-192 est plus lente mais plus sécurisée que la norme AES-128, et plus rapide mais moins sécurisée que la norme AES-256.
- AES-256 — AES-256 utilise une clé de 256 bits pour le chiffrement AES. AES-256 est plus lent mais plus sécurisé que AES-128 et AES-192.

Étape 8. Choisissez la méthode d'authentification appropriée dans la liste déroulante *Authentification de phase 2*. Le tunnel VPN doit utiliser la même méthode d'authentification pour ses deux extrémités.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Les options disponibles sont définies comme suit :

- MD5 — Message Digest Algorithm-5 (MD5) représente une fonction de hachage de 128 bits qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.
- SHA1 — Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage de 160 bits plus sécurisée que MD5.

Étape 9. Dans le champ *Durée de vie de l'association de sécurité de phase 2*, saisissez la durée en secondes pendant laquelle le tunnel VPN reste actif dans la phase 2. La durée par défaut est de 3 600 secondes.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Étape 10. (Facultatif) Si vous souhaitez activer le testeur de résistance de la clé pré-partagée, cochez la case **Complexité minimale de la clé pré-partagée**.

Note: Si vous activez la case à cocher **Complexité de clé prépartagée minimale**, le *compteur de résistance de clé prépartagée* affiche la force de la clé prépartagée via des barres de couleur. Le rouge indique une résistance faible, le jaune indique une résistance acceptable et le vert indique une résistance forte.

Étape 11. Entrez la clé souhaitée dans le champ *Clé prépartagée*. Jusqu'à 30 hexadécimaux peuvent être utilisés comme clé prépartagée. Le tunnel VPN doit utiliser la même clé prépartagée pour ses deux extrémités.

Note: Il est fortement recommandé de modifier fréquemment la clé pré-partagée entre les homologues IKE afin que le VPN reste sécurisé.

Étape 12. Pour enregistrer les paramètres dont vous disposez jusqu'à présent et laisser le reste comme valeur par défaut, faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres.

Configuration avancée

Étape 1. Cliquez sur **Avancé** pour configurer les paramètres avancés.

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced +

La zone *Avancé* apparaît avec de nouveaux champs disponibles.

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal

Étape 2. (Facultatif) Cochez la case **Mode agressif** si la vitesse de votre réseau est faible. Aggressive Mode échange les ID des points d'extrémité du tunnel en texte clair pendant la connexion SA, ce qui nécessite moins de temps pour l'échange mais est moins sécurisé.

Étape 3. (Facultatif) Cochez la case **Compress (Support IP Payload Compression Protocol(IPComp))** si vous voulez compresser la taille des datagrammes IP. IPComp est un protocole de compression IP utilisé pour compresser la taille des datagrammes IP si la vitesse du réseau est faible et si l'utilisateur veut transmettre rapidement les données sans perte.

Étape 4. (Facultatif) Cochez la case **Keep-Alive** si vous voulez toujours que la connexion du tunnel VPN reste active. Keep-Alive permet de rétablir immédiatement les connexions si une connexion devient inactive.

Étape 5. (Facultatif) Cochez la case Algorithme de hachage AH si vous souhaitez que l'authentification à l'origine des données, l'intégrité des données par le biais de la somme de contrôle et la protection soit étendue à l'en-tête IP. Choisissez ensuite la méthode d'authentification appropriée dans la liste déroulante. Le tunnel doit avoir le même algorithme pour les deux côtés.

Les options disponibles sont définies comme suit :

- MD5 — Message Digest Algorithm-5 (MD5) représente une fonction de hachage de 128 bits qui protège les données contre les attaques malveillantes par le calcul de la somme de contrôle.
- SHA1 — Secure Hash Algorithm version 1 (SHA1) est une fonction de hachage de 160 bits plus sécurisée que MD5.

Étape 6. Cochez la case **NetBIOS Broadcast** si vous voulez autoriser le trafic non routable via le tunnel VPN. La case est décochée par défaut. NetBIOS est utilisé pour détecter les ressources réseau telles que les imprimantes, les ordinateurs, etc. dans le réseau via des applications logicielles et des fonctionnalités Windows telles que Network Neighborhood.

Étape 7. (Facultatif) Cochez la case **NAT Traversal** si vous souhaitez accéder à Internet à partir de votre réseau local privé via une adresse IP publique. La traversée NAT est utilisée pour faire apparaître les adresses IP privées des systèmes internes comme des adresses IP publiques afin de protéger les adresses IP privées contre toute attaque ou découverte malveillante.

Étape 8. Cliquez sur **Save pour enregistrer les paramètres.**