

Configuration du réseau privé virtuel (VPN) Easy Client to Gateway sur les routeurs RV320 et RV325 VPN

Objectif

Un réseau privé virtuel (VPN) assure la sécurité des utilisateurs distants qui se connectent à Internet à partir d'un réseau public ou non approuvé. 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. Easy VPN permet une configuration et une configuration rapides du VPN via l'utilitaire client VPN Cisco.

L'objectif de ce document est de vous montrer comment configurer un Easy Client to Gateway VPN sur la gamme de routeurs VPN RV32x.

Périphériques pertinents | Version du micrologiciel

- Routeur VPN double WAN RV320 | 1.1.0.09 ([Télécharger la dernière version](#))
- Routeur VPN double WAN Gigabit RV325 | 1.1.0.09 ([Télécharger la dernière version](#))

Configurer Easy Client à Gateway VPN

Étape 1. Connectez-vous à l'utilitaire de configuration Web 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: ▼

Keying Mode: ▼

Enable:

Local Group Setup

Local Security Gateway Type: ▼

IP Address: 0.0.0.0

Local Security Group Type: ▼

IP Address:

Subnet Mask:

Remote Client Setup

Remote Security Gateway Type: ▼

▼ :

Étape 2. Cliquez sur la case d'option **Easy VPN**.

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Remarque : Le *numéro de groupe* représente le numéro du groupe. Il s'agit d'un champ généré automatiquement.

Étape 3. Dans le champ *Nom*, saisissez le nom du tunnel.

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Étape 4. (Facultatif) Si vous souhaitez activer le testeur de résistance pour la clé pré-partagée, cochez la case **Complexité minimale du mot de passe**.

Étape 5. Dans le champ *Mot de passe*, saisissez un mot de passe.

- Password Strength Meter (Compteur de puissance du mot de passe) : indique la force du mot de passe par des barres de couleur. La couleur rouge indique une puissance faible, la couleur jaune, une puissance acceptable et le vert, une puissance élevée. Si vous n'avez pas coché la case **Complexité minimale du mot de passe** à l'étape 4, le compteur d'intensité du mot de passe n'apparaît pas.

Étape 6. Choisissez l'interface appropriée par laquelle le client établit Easy VPN à la passerelle dans la liste déroulante *Interface*.

Client to Gateway

Add a New Easy VPN

Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter:

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Étape 7. Cochez la case **Activer** pour activer le VPN client-passerelle. Par défaut, il est activé.

Client to Gateway

Add a New Easy VPN

Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter:

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Étape 8. Sélectionnez le mode de tunnellation approprié dans la liste déroulante *Tunnel Mode*.

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode: (dropdown menu open showing Full Tunnel, Full Tunnel, Split Tunnel)

IP Address:

Subnet Mask:

Extended Authentication:

Les options disponibles sont définies comme suit :

- Full Tunnel : envoie tout le trafic via le tunnel VPN, ce qui renforce la sécurité du trafic. Si vous choisissez cette option, passez à l'[étape 11](#).
- Tunnel fractionné : permet au client VPN d'accéder simultanément à l'Internet public et aux ressources VPN, ce qui économise la bande passante.

Étape 9. Dans le champ *Adresse IP*, saisissez l'adresse IP que vous souhaitez attribuer à l'interface du Easy VPN.

Client to Gateway

Add a New Easy VPN


Tunnel Group VPN Easy VPN

Group No. 1

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter: 

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Étape 10. Dans le champ *Masque de sous-réseau*, saisissez le masque de sous-réseau de l'adresse IP attribuée à l'interface Easy VPN.

Étape 11. Choisissez l'authentification appropriée pour le client VPN dans la liste déroulante *Extended Authentication* pour utiliser un nom d'utilisateur et un mot de passe d'hôte IPsec pour authentifier les clients VPN, ou pour utiliser la base de données trouvée dans User Management. Cette option doit être activée sur les deux périphériques pour qu'elle fonctionne.

Client to Gateway

Add a New Easy VPN

Tunnel
 Group VPN
 Easy VPN

Group No.

Name:

Minimum Password Complexity: Enable

Password:

Password Strength Meter:

Interface:

Enable:

Tunnel Mode:

IP Address:

Subnet Mask:

Extended Authentication:

Les options disponibles sont définies comme suit :

- 1 - Active Directory - L'authentification est étendue via active directory. Active Directory est un service qui fournit la sécurité réseau sur un réseau de domaine Windows. Cliquez sur **Ajouter/Modifier** si vous voulez ajouter un nouveau répertoire ou modifier le répertoire existant.
- Default - Local Database - L'authentification est effectuée par le routeur. Cliquez sur **Ajouter/Modifier** pour ajouter ou modifier la base de données.

Note: Pour en savoir plus sur l'ajout ou la modification du répertoire actif ou de la base de données locale, reportez-vous au document intitulé [Configuration de la gestion des utilisateurs et des domaines sur les routeurs VPN RV320 et RV325](#).

Étape 12. Cliquez sur **Save** pour enregistrer les paramètres.