

Paramètres de stratégie IKE (Internet Key Exchange) sur les routeurs VPN RV130 et RV130W

Objectif

Le protocole IKE (Internet Key Exchange) établit une communication sécurisée entre deux réseaux. Avec IKE, les paquets sont chiffrés, verrouillés et déverrouillés avec des clés utilisées par deux parties.

Vous devez créer une stratégie d'échange de clés Internet avant de configurer une stratégie VPN. Référez-vous à [Configuration de la stratégie VPN sur RV130 et RV130W](#) pour plus d'informations.

L'objectif de ce document est de vous montrer comment ajouter un profil IKE aux routeurs VPN RV130 et RV130W.

Périphériques pertinents

- RV130
- RV130W

Étapes de la procédure

Étape 1. Utilisez l'utilitaire de configuration du routeur pour sélectionner **VPN > Site-to-Site IPsec VPN > Advanced VPN Setup** dans le menu de gauche. La page *Advanced VPN Setup* s'affiche :

Advanced VPN Setup

NAT Traversal: Enable

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								

<input type="checkbox"/>	Status	Name	Policy Type	Encryption Algorithm	Authentication Algorithm	Local	Remote	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>								

[IPsec Connection Status](#)

Étape 2. Sous la table de stratégie IKE, cliquez sur **Add Row**. Une nouvelle fenêtre apparaît :

<input type="checkbox"/>	Name	Local ID	Remote ID	Exchange Mode	Encryption Algorithm	Authentication Algorithm	DH Group	
<input type="checkbox"/>	No data to display							
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>								

Étape 3. Entrez un nom pour la stratégie IKE dans le champ *IKE Name*.

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Étape 4. Dans le menu déroulant *Exchange Mode*, choisissez le mode dans lequel un échange de clés est utilisé pour établir une communication sécurisée.

Add / Edit IKE Policy Configuration

IKE Name:

Exchange Mode:

Local

Main
Main
Aggressive

Les options disponibles sont définies comme suit :

- Principal — Protège l'identité des pairs pour une sécurité accrue.
- Agressif : aucune protection de l'identité des homologues, mais une connexion plus rapide.

Étape 5. Dans le menu déroulant *Local Identifier Type*, sélectionnez le type d'identité du profil.

Local

Local Identifier Type:

Local Identifier:

Les options disponibles sont définies comme suit :

- Local WAN (Internet) IP : se connecte via Internet.
- IP Address : chaîne unique de chiffres séparés par des points qui identifie chaque machine utilisant le protocole Internet pour communiquer sur un réseau.

Étape 6. (Facultatif) Si **IP Address** est sélectionné dans la liste déroulante de l'étape 5, saisissez l'adresse IP locale dans le champ *Local Identifier*.

Local

Local Identifier Type:

Local Identifier:

Étape 7. Dans le menu déroulant *Remote Identifier Type*, choisissez le type d'identité du profil.

Remote

Remote Identifier Type: Remote WAN IP ▼

Remote Identifier: Remote WAN IP
IP Address

Les options disponibles sont définies comme suit :

- Local WAN (Internet) IP : se connecte via Internet.
- IP Address : chaîne unique de chiffres séparés par des points qui identifie chaque machine utilisant le protocole Internet pour communiquer sur un réseau.

Étape 8. (Facultatif) Si **IP Address** est sélectionné dans la liste déroulante de l'étape 7, saisissez l'adresse IP distante dans le champ *Remote Identifier*.

Remote

Remote Identifier Type: Remote WAN IP ▼

Remote Identifier: 192.168.2.100

Étape 9. Dans le menu déroulant *Encryption Algorithm*, choisissez un algorithme pour chiffrer vos communications. **AES-128** est sélectionné par défaut.

IKE SA Parameters

Encryption Algorithm: DES ▼

Authentication Algorithm: DES

Pre-Shared Key: AES-128

DH Group: Group1 (768 bit) ▼

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

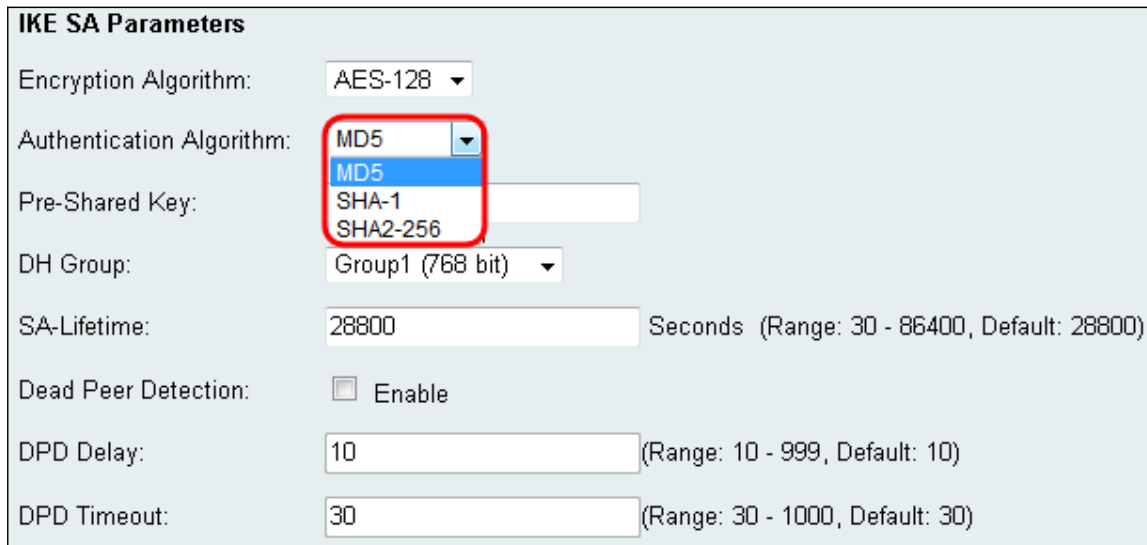
Les options disponibles sont répertoriées comme suit, de la sécurité minimale à la sécurité maximale :

- DES : norme de chiffrement des données.
- 3DES — Triple Data Encryption Standard.
- AES-128 - Advanced Encryption Standard utilise une clé de 128 bits.
- AES-192 — Advanced Encryption Standard utilise une clé de 192 bits.
- AES-256 - Advanced Encryption Standard utilise une clé de 256 bits.

Note: AES est la méthode standard de cryptage sur DES et 3DES pour ses performances et sa sécurité accrues. L'allongement de la clé AES augmentera la sécurité avec une

baisse des performances. AES-128 est recommandé car il offre le meilleur compromis entre vitesse et sécurité.

Étape 10. Dans le menu déroulant *Authentication Algorithm*, choisissez un algorithme pour authentifier vos communications. **SHA-1** est sélectionné par défaut.



IKE SA Parameters

Encryption Algorithm: AES-128

Authentication Algorithm: MD5 (highlighted in blue, with a red box around the dropdown menu)

Pre-Shared Key: [text input field]

DH Group: Group1 (768 bit)

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Les options disponibles sont définies comme suit :

- MD5 — L'algorithme Message Digest a une valeur de hachage de 128 bits.
- SHA-1 : l'algorithme de hachage sécurisé a une valeur de hachage de 160 bits.
- SHA2-256 — Algorithme de hachage sécurisé avec une valeur de hachage de 256 bits.

Note: MD5 et SHA sont des fonctions de hachage cryptographique. Ils prennent une donnée, la compactent et créent une sortie hexadécimale unique qui n'est généralement pas reproductible. MD5 ne fournit pratiquement aucune sécurité contre les collisions de hachage et ne doit être utilisé que dans un environnement de petite entreprise où la résistance aux collisions n'est pas nécessaire. SHA1 est un meilleur choix que le MD5 car il offre une meilleure sécurité à des vitesses légèrement plus lentes. Pour des résultats optimaux, SHA2-256 n'a pas d'attaques connues d'intérêt pratique et offrira la meilleure sécurité. Comme mentionné précédemment, une sécurité accrue implique des vitesses plus lentes.

Étape 11. Dans le champ *Pre-Shared Key*, saisissez un mot de passe comportant entre 8 et 49 caractères.

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Étape 12. Dans le menu déroulant *Groupe DH*, sélectionnez un groupe DH. Le nombre de bits indique le niveau de sécurité. Les deux extrémités de la connexion doivent se trouver dans le même groupe.

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: **Group1 (768 bit) ▾**
Group1 (768 bit)
Group2 (1024 bit)
Group5 (1536 bit)

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Étape 13. Dans le champ *SA-Lifetime*, saisissez la durée de validité de l'association de sécurité en secondes. 28800 secondes sont établies par défaut.

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: 10 (Range: 10 - 999, Default: 10)

DPD Timeout: 30 (Range: 30 - 1000, Default: 30)

Étape 14. (Facultatif) Cochez la case **Enable** dans le champ *Dead Peer Detection* si vous

souhaitez désactiver une connexion avec un homologue inactif. Passez à l'étape 17 si vous n'avez pas activé Dead peer Detection.

IKE SA Parameters	
Encryption Algorithm:	AES-128 ▾
Authentication Algorithm:	SHA-1 ▾
Pre-Shared Key:	<input type="text"/>
DH Group:	Group1 (768 bit) ▾
SA-Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)
Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	10 (Range: 10 - 999, Default: 10)
DPD Timeout:	30 (Range: 30 - 1000, Default: 30)

Étape 15. (Facultatif) Si vous avez activé la détection des homologues morts, saisissez une valeur dans le champ *Délai DPD*. Cette valeur indique la durée pendant laquelle le routeur attend de vérifier la connectivité du client.

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	10 (Range: 10 - 999, Default: 10)
DPD Timeout:	30 (Range: 30 - 1000, Default: 30)

Étape 16. (Facultatif) Si vous avez activé la détection des homologues morts, saisissez une valeur dans le champ *Délai d'expiration DPD*. Cette valeur indique combien de temps le client restera connecté jusqu'à expiration du délai d'attente.

Dead Peer Detection:	<input type="checkbox"/> Enable
DPD Delay:	10 (Range: 10 - 999, Default: 10)
DPD Timeout:	30 (Range: 30 - 1000, Default: 30)

Étape 17. Cliquez sur **Save** pour enregistrer les modifications.

IKE SA Parameters

Encryption Algorithm: AES-128 ▾

Authentication Algorithm: SHA-1 ▾

Pre-Shared Key:

DH Group: Group1 (768 bit) ▾

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 28800)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

Save

Cancel

Back

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.