

## NQG\_053\_FR : Configurer un Réseau Privé Virtuel utilisant IPsec avec IKE entre deux routeurs Netopia

Ce Guide de configuration rapide traite de la configuration d'un profil IPsec utilisant le protocole Internet Key Exchange (IKE – échange automatique de clés) entre deux routeurs Netopia.

---

Des notices techniques supplémentaires sont disponibles dans la section **Utiliser des Réseaux Privés Virtuels** (ou [Using Virtual Private Networking \(VPN\)](#) pour les notes techniques en langue anglaise). Elles procurent des informations sur la compatibilité, la configuration et le diagnostic des problèmes des Réseaux Privés Virtuels sur les routeurs Netopia et en particulier sur les tunnels **IPsec**.

**Veillez noter :** Les services de **Réseau Privé Virtuel** (utilisant IPsec) vers et depuis des routeurs avec des adresses IP WAN non routable ne sont pas supportés par Netopia. La Commission National Internet (NIC) définit les espaces d'adresses IP non routable tel que ci-dessous :

Types d'adresses	Plages de réseaux
Classe <b>A</b>	10.x.x.x
Classe <b>B</b>	172.16.x.x-172.31.x.x
Classe <b>C</b>	192.168.x.x

Même s'il est possible par expérimentation de mettre en œuvre les fonctions Réseau Privé Virtuel dans le cas d'adresses IP WAN non routable, l'Assistance technique Netopia ne peut assurer le support de ce type de configurations. Afin de configurer avec succès des accès Réseau Privé Virtuel sur les routeurs Netopia et Cayman, vérifiez avec votre Fournisseur d'Accès Internet comment obtenir des IP routable à utiliser sur l'interface WAN de votre routeur.

L'exemple de configuration ci-après utilise des Adresses WAN non routable comme modèle uniquement. Modifiez votre configuration en utilisant les adresses IP fournies par votre FAI.

A l'intérieur de cette note technique, il est fait référence aux masques de sous-réseau . Tout comme les espaces d'adresses IP non routable, l'utilisation des masques de sous-réseau est standardisée.

Types de masque	Masque de sous-réseau	Notation dans l'adressage	Jargon
Classe <b>A</b>	255.0.0.0	10.0.0.0 / 8	8 bits ou Slash - 8
Classe <b>B</b>	255.255.0.0	172.20.0.0 / 16	16 bits ou Slash - 16
Classe <b>C</b>	255.255.255.0	192.168.1.0 / 24	24 bits ou Slash - 24
<b>Route d'hôte*</b>	255.255.255.255	192.168.1.50 / 32	32 bits ou Slash - 32

\*Le masque de réseau sur 32 bits permet de spécifier une seule adresse d'hôte et non une adresse de réseau (plusieurs hôtes).

### Paramètres :

Vous trouverez ci-dessous la liste des versions de firmware (logiciel/microcode) et des matériels utilisés pour construire cette note technique.

<u>Matériel</u>	<u>Version de logiciel</u>
Routeurs Série R	4.10.0 et supérieur
Routeurs Série 4000	5.3.4 et supérieur
Routeurs Cayman Série 3300-ENT	8.0.9 et supérieur

Pour mettre à jour le **firmware** (microcode/logiciel) de votre routeur allez à la page [Mise à jour de firmware](#).

### Avant de commencer :

Veillez vous référer à la note technique sur la configuration des tunnels VPN sur les Routeurs Netopia ([Notice on Configuring VPN Tunnels with Netopia Routers](#)).

Etablissez une connexion série sur le port console du routeur en utilisant un programme d'émulation de terminal tel que **HyperTerminal**. Les réglages doivent être:

- Bits par seconde : **9600**
- Bits de données : **8**
- Parité : **Aucune**
- Bits d'arrêt : **1**
- Contrôle de flux : **Aucun**

Vous pouvez également utiliser **Telnet** pour vous connecter sur la console de votre routeur Netopia via le réseau local.

Pour plus d'informations sur comment vous connecter sur votre routeur Netopia via **HyperTerminal** ou **Telnet**, veuillez consulter le guide :

[NOG\\_100: Démarrer \(Comment établir une connexion Telnet/Console depuis un poste de travail Windows\)](#)

### **Astuces :**

Ne modifiez pas d'autres réglages que ceux cités ci-dessous.

- Taper sur la touche **Entrée** vous conduit à une autre page.
- Taper sur la touche **Echap** vous permet de revenir à la page précédente.
- Taper sur la touche **Entrée** permet de valider la saisie de données.
- Taper sur la touche **Tab** permet de commuter un champ entre deux valeurs.

**Veillez noter :** Ce document vous est procuré comme service supplémentaire de l'**Assistance Technique Netopia**. Bien que les configurations décrites ci-dessous ont été utilisées avec succès en de nombreuses occasions pour établir des connexions avec entre des postes de travail équipé de Windows avec des réseaux locaux derrière des routeurs Netopia via des Réseau Privé Virtuel (VPN), nous ne pouvons garantir le succès dans toutes circonstances à cause du nombre de variables et des comportements imprédictibles des Systèmes d'Exploitation Windows. Si suivre les présentes informations ne vous apporte pas le résultat désiré, veuillez consulter votre Service Informatique ou l'Assistance Technique Microsoft directement car Netopia ne peut assurer au-delà de ces notes techniques le support des fonctions du Système Microsoft Windows.

### **Introduction**

Ce Guide de configuration rapide explique comment créer un profil IKE (phase 1) et un profil IPsec (phase 2) dans les Netopia. Sur les routeurs Netopia, toutes les connexions sont gérées au sein de profils (de connexion). Pour vérifier ou modifier un profil IPsec déjà créé, allez dans **Quick Menus** et dans **Change Connection Profile** puis sélectionnez le profil IPsec existant. Si vous désirez vérifier ou modifier un profil IKE, allez **dans Quick Menus** et **IKE Phase 1 Configuration** puis sélectionnez le profil IKE existant. Ne modifiez d'autres réglages que ceux mentionnés dans ce document. Contrairement à d'autre types de profils, il n'y a pas besoin d'établir une connexion IPsec ; une fois les profils IKE et IPsec créés, le tunnel est activé de manière automatique et transparente. Cependant en fonction de votre modèle de routeur et de la présence ou de l'accélérateur VPN, les phases d'authentification jusqu'au transfert des données peuvent prendre jusqu'à deux minutes. Conservez cela en mémoire lorsque vous testerez votre tunnel IPsec avec Ping ou d'autres outils de diagnostic. Dans ce document les routeurs sont configurés avec des adresses IP statiques et NAT n'est pas activée sur le tunnel IPsec en lui-même bien que la traduction d'adresses IP soit activée sur l'interface WAN / connexion Internet.

## Configuration du routeur Pas à Pas :

La configuration mise en place dans l'exemple suivant est basée sur deux routeurs Netopia connectés sur Internet utilisant **NAT (Traduction d'adresses IP)**. Il n'est pas nécessaire que NAT soit activée pour que la solution fonctionne. Les adresses IP locales WAN ne sont fournies qu'à titre d'exemple.

**Notez que** les adresses IP Ethernet utilisées dans cet exemple peuvent être utilisées dans d'autres configurations similaires. L'essentiel étant que les routeurs soient configurés avec des adresses IP Ethernet différentes. Cependant les adresses IP locales WAN devront être remplacées par les adresses IP allouées par votre Fournisseur d'Accès Internet.

Routeur A		Routeur B	
Adresse IP Ethernet :	192.168.1.1	Adresse IP Ethernet :	192.168.2.1
Masque de sous-réseau Ethernet :	255.255.255.0	Masque de sous-réseau Ethernet :	255.255.255.0
Adresse IP locale WAN :	172.20.16.1	Adresse IP locale WAN :	172.20.17.1

## Configuration du routeur A :

1. Une fois connecté à la console de votre routeur, le premier écran qui s'affiche est celui du menu principal. Depuis ce dernier allez dans **Quick Menu** et choisissez **Add Connection Profile** pour ajouter un profil de connexion **IPsec**.

```

                                Add Connection Profile

Profile Name:                    Routeur B
Profile Enabled:                 Yes
Encapsulation Type...           IPsec
Encapsulation Options...

IP Profile Parameters...

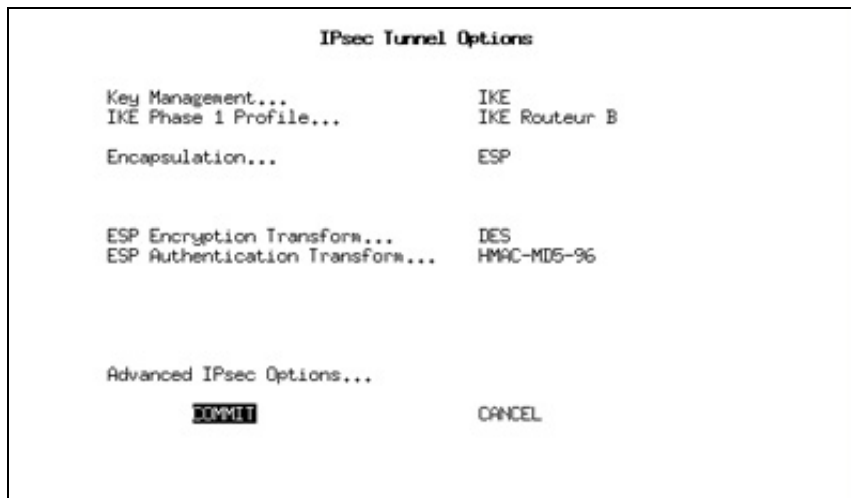
Interface Group...              Any Port

COMMIT                        CANCEL

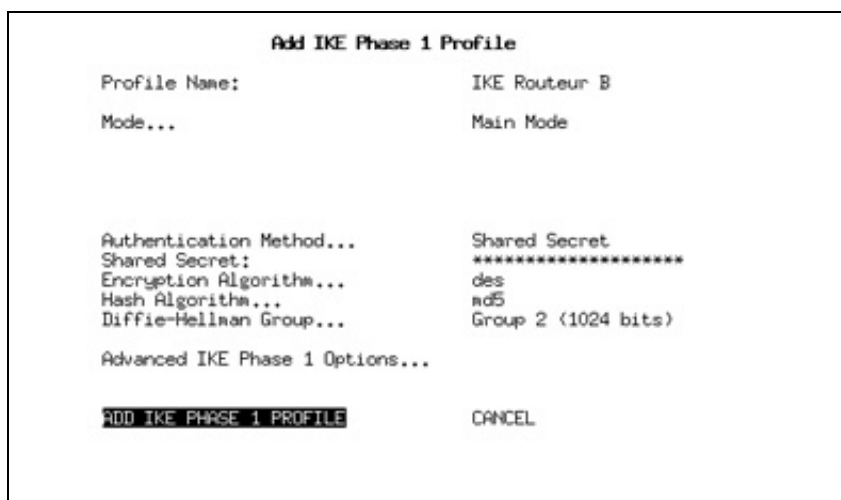
Return/Enter to accept the profile.
Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.
```

2. Dans le champ **Profile Name**, saisissez « **Routeur B** » (ou le nom de votre choix – en principe un nom explicite correspondant à celui du site distant).

3. Dans le champ **Encapsulation Type**, changez le protocole d'encapsulation à **IPsec** et allez dans **Encapsulation Options** pour modifier les options d'encapsulation.

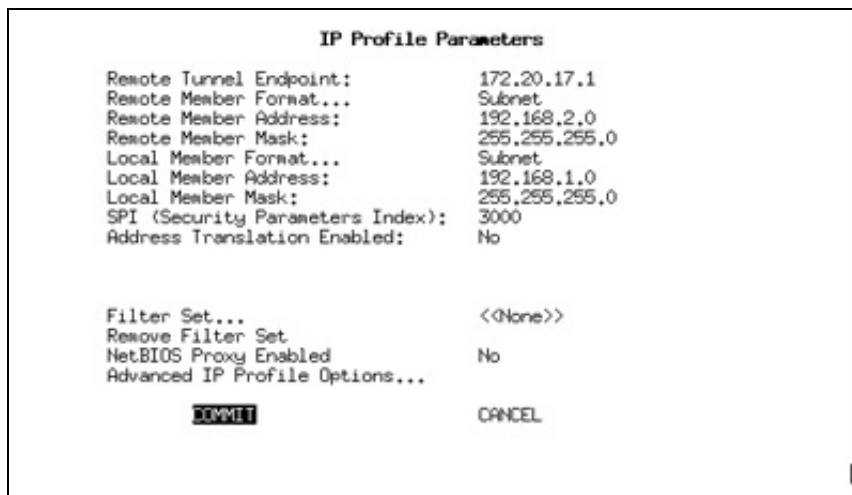


4. Dans le champ **Key Management**, choisissez **IKE**.
5. Allez dans **IKE Phase 1 profile** et choisissez **<<ADD PH1 PROFILE>>**.
6. Dans le champ **Profile Name**, saisissez « **IKE Routeur B** » (ou le nom de votre choix – en principe un nom explicite correspondant à celui du site distant).



7. Laissez le **Mode** configuré à **Main Mode**.
8. Laissez **Authentication Method** à **Shared Secret**.
9. Saisissez une clé (chaîne de caractères alphanumériques) dans le champ **Shared Secret**, il s'agit de la même clé (ex : netopia1234) qui doit être utilisée sur les deux routeurs A et B.
10. Choisissez DES ou 3DES comme algorithme de cryptage (**Encryption Algorithm**). Il est très fortement recommandé d'utiliser une carte accélératrice (XL) VPN si vous désirez choisir 3 DES.

11. Sélectionnez **MD5** ou **SHA1** comme algorithme de hachage dans le champ **Hash Algorithm**.
12. Vous pouvez laisser le champ **Diffie-Hellman Group** sur **Group 2 (1024 bits)**. Cependant dans le cas où le routeur distant ne serait pas un Netopia, vous pouvez être amené à changer pour Group 1 (768 bits).
13. Laissez les options avancés IKE Phase 1 (**Advanced IKE Phase 1 Options...**) inchangées.
14. Allez sur **ADD IKE PHASE 1 PROFILE** et tapez sur **Entrée**.
15. Vous êtes maintenant de retour dans l'écran **IPsec Tunnel Options**.
16. Le profil IKE que vous venez de créer est maintenant listé dans **IKE Phase Profile...** Assurez-vous que celui-ci est bien sélectionné.
17. Conservez le type d'encapsulation (**Encapsulation**) sur **ESP**.
18. Dans le champ **ESP Encryption Transform**, choisissez **DES** ou **3DES** comme algorithme de cryptage. Il est très fortement recommandé d'utiliser une carte accélératrice VPN si vous désirez choisir 3 DES.
19. Régler **ESP Authentication Transform** à **HMAC-MD5-96** ou **HMAC-SHA1-96**. L'essentiel est que le routeur distant soit configuré de la même manière.
20. Si vous disposez d'une carte accélératrice (XL), un autre champ est disponible Compression Type. Dans ce cas, si le routeur distant supporte la compression LZS, vous pouvez choisir **LZS Compression**. Sinon choisissez **None**.
21. Laissez les Options IPsec avancées (**Advanced IPsec Options**) inchangées.
22. Tapez **Entrée** sur **COMMIT**.
23. Vous êtes de retour dans l'écran **Add Connection Profile**.
24. Déplacez-vous avec les touches fléchées sur **IP Profile Parameters** et tapez **Entrée**.
25. Entrez l'adresse **IP WAN du routeur B** distant dans le champ **Remote Tunnel Endpoint**. En se basant sur notre exemple, l'adresse IP à saisir est **172.20.17.1**. Si l'interface WAN du routeur B était configurée avec NAT désactivée et en mode non numérotée (unnumbered), il faudrait alors saisir l'adresse IP Ethernet du **routeur B** dans le champ **Remote Tunnel Endpoint**.



26. Dans **Remote Member Format** choisissez **Subnet** pour établir un tunnel entre deux (sous) réseaux complets.
  27. Dans **Remote Member Address**, entrez l'adresse IP de réseau de l'interface Ethernet LAN du routeur B soit **192.168.2.0**.
  28. Et dans **Remote Member Mask**, saisissez le masque de sous-réseau de l'interface Ethernet LAN du routeur B soit **255.255.255.0**.
  29. Configurez de manière identique le champ **Local Member Format** et choisissez **Subnet**.
  30. Dans le champ **Local Member Address**, saisissez l'adresse de réseau de l'interface Ethernet du routeur A soit **192.168.1.0**.
  31. Et dans **Local Member Mask**, saisissez le masque de sous-réseau de l'interface Ethernet LAN du routeur A soit **255.255.255.0**.
  32. Laissez le champ **Address Translation Enabled** à **No**, ce réglage permet d'activer NAT à l'intérieur du tunnel.
  33. Selon vos besoins, activez **NetBIOS Proxy Enabled** (commutez sur **Yes**). Activez cette fonction si vous désirez supporter les réseaux Microsoft. Elle permet aux postes de travail des réseaux locaux derrière les deux routeurs de se voir dans leur **Voisinage** ou **Favoris réseau**
  34. Laissez également **Filter Set** configuré à **None** et laissez les options avancées du profil IP (**Advanced IP Profile Options...**) inchangées.
  35. Et validez la modification des paramètres IP en vous déplaçant sur **COMMIT** et en tapant sur **Entrée**. Vous êtes de nouveau dans l'écran **Add Connection Profile**. Allez sur **COMMIT** et tapez sur Entrée pour créer le profil IPsec.
  36. Maintenant, tapez **Echap** deux fois pour revenir au menu principal.
- Répétez maintenant l'opération avec le routeur B.

## Configuration du routeur B :

1. Une fois connecté à la console de votre routeur, le premier écran qui s'affiche est celui du menu principal. Depuis ce dernier allez dans **Quick Menu** et choisissez **Add Connection Profile** pour ajouter un profil de connexion **IPsec**.
2. Dans le champ **Profile Name**, saisissez « **Routeur A** » (ou le nom de votre choix – en principe un nom explicite correspondant à celui du site distant).
3. Dans le champ **Encapsulation Type**, changez le protocole d'encapsulation à **IPsec** et allez dans **Encapsulation Options** pour modifier les options d'encapsulation.
4. Dans le champ **Key Management**, choisissez **IKE**.
5. Allez dans **IKE Phase 1 profile** et choisissez **<<ADD PH1 PROFILE>>**.
6. Dans le champ **Profile Name**, saisissez « **IKE Routeur A** » (ou le nom de votre choix – en principe un nom explicite correspondant à celui du site distant).
7. Laissez le **Mode** configuré à **Main Mode**.
8. Laissez **Authentication Method** à **Shared Secret**.
9. Saisissez une clé (chaîne de caractères alphanumériques) dans le champ **Shared Secret**, il s'agit de la même clé (ex : netopia1234) qui doit être utilisée sur les deux routeurs A et B.
10. Choisissez DES ou 3DES comme algorithme de cryptage (**Encryption Algorithm**). Il est très fortement recommandé d'utiliser une carte accélératrice (XL) VPN si vous désirez choisir 3 DES.
11. Sélectionnez **MD5** ou **SHA1** comme algorithme de hachage dans le champ **Hash Algorithm**.
12. Vous pouvez laisser le champ **Diffie-Hellman Group** sur **Group 2 (1024 bits)**.
13. Laissez les options avancés IKE Phase 1 (**Advanced IKE Phase 1 Options...**) inchangées.
14. Allez sur **ADD IKE PHASE 1 PROFILE** et tapez sur **Entrée**.
15. Vous êtes maintenant de retour dans l'écran **IPsec Tunnel Options**.
16. Le profil IKE que vous venez de créer est maintenant listé dans **IKE Phase Profile...** Assurez-vous que celui-ci est bien sélectionné.
17. Conservez le type d'encapsulation (**Encapsulation**) sur **ESP**.
18. Dans le champ **ESP Encryption Transform**, choisissez **DES** ou **3DES** comme algorithme de cryptage. Il est très fortement recommandé d'utiliser une carte accélératrice VPN si vous désirez choisir 3 DES.
19. Régler **ESP Authentication Transform** à **HMAC-MD5-96** ou **HMAC-SHA1-96**. L'essentiel est que le routeur distant soit configuré de la même manière.

20. Si vous disposez d'une carte accélératrice (XL), un autre champ est disponible Compression Type. Dans ce cas, si le routeur distant supporte la compression LZS, vous pouvez choisir **LZS Compression**. Sinon choisissez **None**.
21. Laissez les Options IPsec avancées (**Advanced IPsec Options**) inchangées.
22. Tapez **Entrée** sur **COMMIT**.
23. Vous êtes de retour dans l'écran **Add Connection Profile**.
24. Déplacez-vous avec les touches fléchées sur **IP Profile Parameters** et tapez **Entrée**.
25. Entrez l'adresse **IP WAN du routeur A** distant dans le champ **Remote Tunnel Endpoint**. En se basant sur notre exemple, l'adresse IP à saisir est **172.20.16.1**. Si l'interface WAN du routeur A était configurée avec NAT désactivée et en mode non numérotée (unnumbered), il faudrait alors saisir l'adresse IP Ethernet du **routeur A** dans le champ **Remote Tunnel Endpoint**.
26. Dans **Remote Member Format** choisissez **Subnet** pour établir un tunnel entre deux (sous) réseaux complets.
27. Dans **Remote Member Address**, entrez l'adresse IP de réseau de l'interface Ethernet LAN du routeur A soit **192.168.1.0**.
28. Et dans **Remote Member Mask**, saisissez le masque de sous-réseau de l'interface Ethernet LAN du routeur A soit **255.255.255.0**.
29. Configurez de manière identique le champ **Local Member Format** et choisissez **Subnet**.
30. Dans le champ **Local Member Address**, saisissez l'adresse de réseau de l'interface Ethernet du routeur A soit **192.168.2.0**.
31. Et dans **Local Member Mask**, saisissez le masque de sous-réseau de l'interface Ethernet LAN du routeur A soit **255.255.255.0**.
32. Laissez le champ **Address Translation Enabled** à **No**, ce réglage permet d'activer NAT à l'intérieur du tunnel.
33. Selon vos besoins, activez **NetBIOS Proxy Enabled** (commutez sur **Yes**). Activez cette fonction si vous désirez supporter les réseaux Microsoft et permettre aux postes de travail des réseaux locaux derrière les deux routeurs de se voir dans leur **Voisinage** ou **Favoris réseau**
34. Laissez également **Filter Set** configuré à **None** et laissez les options avancées du profil IP (**Advanced IP Profile Options...**) inchangées.
35. Et validez la modification des paramètres IP en vous déplaçant sur **COMMIT** et en tapant sur **Entrée**. Vous êtes de nouveau dans l'écran **Add Connection Profile**. Allez sur **COMMIT** et tapez sur Entrée pour créer le profil IPsec.
36. Maintenant, tapez **Echap** deux fois pour revenir au menu principal.

## Contrôle et Test du tunnel IPsec :

Une fois les deux routeurs configurés, vous pouvez tester votre Réseau Privé Virtuel. Pour cela vous procéder en trois étapes.

1. Sur chaque routeur, vérifiez que le profil est bien activé en allant dans le menu **Quick View et VPN Quickview**.

VPN Quick View					
Profile Name	Type	Rx Pkts	Tx Pkts	Rx Discard	Remote Address
Routeur B	IPsec	0	0	0	172.20.17.1

2. **Si l'étape 1 s'est déroulée avec succès**, passez au **test IP** en envoyant des **paquets Ping ICMP** vers le routeur B depuis le routeur A. Allez dans le menu **Utilities and Diagnostics**. Dans **Name of Host to Ping** entrez l'adresse IP Ethernet du routeur B soit **192.168.2.1** puis entrez 120 dans **Packets to Send** pour le nombre de paquets ICMP à envoyer (cela permet d'envoyer des paquets Ping pendant 2 minutes soit le temps maximum d'authentification et d'établissement du tunnel IPsec). Changez **Specify source address** à **Yes** et saisissez l'adresse IP Ethernet du routeur A soit **192.168.1.1**. Tapez sur **START PING**. Si Lorsque le tunnel IPsec est fonctionnel, le nombre dans **Packets In** augmente au dessus de 1. Tapez **Echap** deux fois pour revenir au menu principal.
3. **Si l'étape 2 s'est déroulée avec succès**, vous pouvez, maintenant, **vérifier que les paquets ICMP** ont bien été acheminés vers le routeur B **au travers du tunnel IPsec**. Pour cela, allez dans le menu **Quick View** puis dans **VPN Quick View**. Vérifiez que les compteurs **Rx Pkts** et **Tx Pkts** ont été incrémentés des paquets ICMP envoyés lors du test effectué en étape 2. Si les compteurs sont restés à zéro, cela signifie qu'il existe un problème de routage et que les **Pings** n'ont pas été envoyés à travers le tunnel Ipsec.