

## NQG\_023 : Configurer un Réseau Privé Virtuel / tunnel PPTP entre deux routeurs Netopia

Cette notice technique explique en détail la configuration d'un tunnel PPTP entre deux routeurs Netopia. Pour les instructions de configuration d'un routeur Netopia en tant que serveur PPTP, veuillez vous référer au Guide de configuration rapide suivant :

[NQG\\_022: Installer et configurer un Réseau Privé Virtuel\(VPN\) entre un client PPTP Windows et un routeur Netopia](#)

Pour les instructions de configuration d'un tunnel IPsec avec IKE entre deux routeurs, veuillez vous référer au Guide de configuration rapide suivant :

[NQG\\_053: Configuration des routeurs Netopia pour IPsec avec IKE](#)

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 PPTP) 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.

---

## 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	4.8.4 et supérieur
Routeurs Série 4000	5.3.7 et supérieur
Routeurs Cayman Série 3300-ENT	8.0.9 et supérieur

Pour mettre à jour le firmware (microcode/logiciel) de votre routeur, consultez la page [firmware update](#).

## 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:

- a. Bits par seconde : **9600**
- b. Bits de données : **8**
- c. Parité : **Aucune**
- d. Bits d'arrêt : **1**
- e. 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'information 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.

---

### 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 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 **PPTP**.
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 **Data Link Encapsulation** (ou **Encapsulation Type** selon la version de firmware), changez le protocole d'encapsulation à **PPTP** et allez dans **Data Link Options Options** (ou **Encapsulation Options** selon la version de firmware) pour modifier les options d'encapsulation.

```

PPTP Tunnel Options

PPTP Partner IP Address:      172.20.17.1

Authentication...            MS-CHAP
Data Encryption...           MPPE

Send Host Name:               Routeur A
Send Secret:                  *****
Receive Host Name:
Receive Secret:

Initiate Connections:        Yes
On Demand:                   Yes

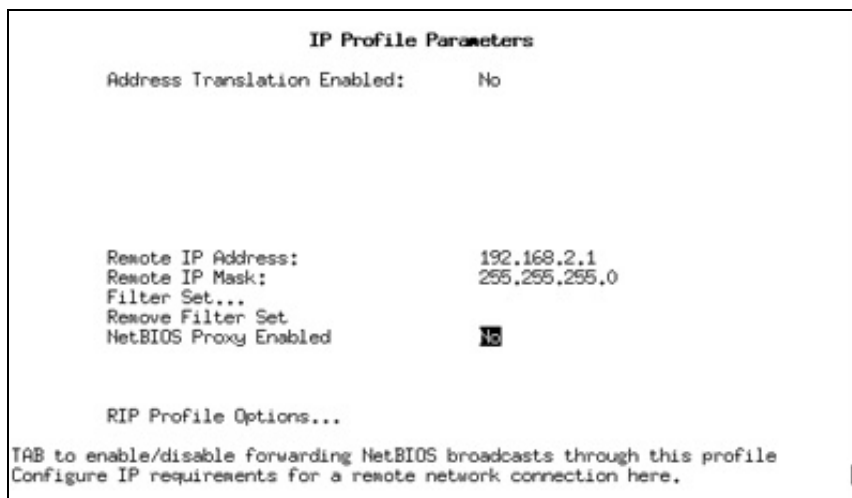
Optional Windows NT Domain Name:

Idle Timeout (seconds):      300

Enter Domain Name if the PPTP tunnel destination is an NT server.
```

4. Entrez l'adresse **IP WAN du routeur B** distant dans le champ **PPTP Partner IP Address**. 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 **PPTP Partner IP Address**.
5. Puis choisissez le **type d'authentification** pour le tunnel. Si vous désirez sécuriser votre connexion en activant le cryptage, vous devez choisir **MS-CHAP** comme authentification. Vous aurez alors le choix entre None (aucune) ou **MPPE (Cryptage Microsoft Point à Point)** dans le champs **Data Encryption**. MPPE intègre compression et cryptage pour un haut niveau de sécurité, cependant cela ralentira la transmission de données.
6. Si au contraire vous choisissez **PAP** ou **CHAP** comme type d'authentification, vous pourrez choisir le type de compression de données dans le champ **Data Compression**. Vous aurez alors le choix entre **None** (aucune) ou **Standard LZS**.
7. Si le **routeur A** est conduit à **initier la connexion PPTP** vers le **routeur B**, entrez un identifiant de connexion dans **Send Host Name** ainsi qu'un mot de passe dans **Send Password** (ou **Secret**) puis positionnez **Initiate Connections** sur **Yes** (oui).
8. Si à l'inverse c'est le **routeur B** qui **initie la connexion** vers le **routeur A**, entrez un identifiant de connexion dans **Receive Host Name** ainsi qu'un mot de passe dans **Receive Password** (ou **Secret**).
9. Si vous désirez que le Routeur A initie une connexion PPTP vers le **routeur B** à chaque fois qu'il y a une demande d'accès à une ressource du réseau situé derrière le **routeur B**, assurez-vous que **On Demand** est positionné sur **Yes**.

10. Vous pouvez modifier l'expiration du délai d'attente (**Idle Timeout**), il s'agit de régler au bout de combien de temps le routeur A doit déconnecter le tunnel PPTP lorsqu'il n'y a pas de trafic. Vous pouvez changer le **délai d'attente à 0 seconde** pour que la **connexion PPTP n'expire pas en absence de trafic**.
11. Tapez sur **Echap** pour retourner à l'écran **Add Connection Profile**.
12. Selon la version de firmware (microcode/logiciel) utilisé sur le routeur, vous pouvez être amené à activer IP dans le profil de connexion en positionnant **IP Enabled** sur **Yes**.
13. Allez dans le menu **IP Profile Parameters**. Désactivez la traduction d'adresse IP en commutant **Address Translation Enabled** sur **No** (Rappel : Utilisez la touche Tab pour commuter entre Yes et No. Tapez sur **Entrée** pour valider le changement).



14. Configurez les champs **Remote IP Address** et **Remote IP Mask** avec l'adresse IP Ethernet du routeur B **192.168.2.1** et son masque de sous-réseau **255.255.255.0**.  
**Attention :** si l'adresse IP Ethernet du routeur B est différente, entrez cette dernière.
15. Ne choisissez pas de jeu de filtres (**Filter Set**) et au besoin si un jeu de filtres est déjà configuré, tapez sur **Entrée** après avoir sélectionné **Remove Filter Set** pour le désactiver. Il est possible d'utiliser des filtres sur une connexion PPTP, cependant les jeux de filtres pré configurés sont peu adaptés à cet usage. Si vous désirez filtrer le trafic sur votre tunnel PPTP, veuillez vous référer à la note technique [NIR\\_052\\_FR : Description et configuration du Firewall des routeurs Netopia](#).
16. Désactivez RIP en réglant **Receive RIP** sur **Off** (notez que ce menu est accessible directement dans les paramètres IP ou dans le menu **RIP Profile Options...**). N'activez RIP que si vous disposez de routeurs derrières les Netopia ayant eux-mêmes RIP actif.
17. Tapez sur **Echap** pour retourner à l'écran **Add Connection Profile** et allez sur **Add Profile Now** puis tapez **Entrée**.

18. Depuis l'écran **Connection Profiles**, tapez de nouveau **Echap** pour revenir à **Quick Menus**.
19. Sélectionnez **ATMP/PPTP Default Profile** ou **VPN Default Answer Profile** (pour les firmwares inférieurs à 4.8).
20. Réglez sur **Yes Answer ATMP/PPTP Connections** ou **Answer VPN Connections** (pour les firmwares inférieurs à 4.8).
21. Dans **PPTP Configuration Options**, allez sur **Receive Authentication** et choisissez le même type d'authentification que celle utilisée dans le profil de connexion.
22. Tapez **Echap** pour revenir dans **Quick Menus**.
23. Choisissez le menu **WAN Default Profile**.
24. Changez le champ **Must Match a Defined Profile** à **Yes**.  
Notez que les routeurs dotés d'interface WAN Ethernet tels que R910 et R9100 ne disposent pas de ce menu. Dans ce cas ignorez cette étape et passez à la suivante.
25. Tapez sur **Echap** deux fois pour revenir au menu principal et allez dans le menu **Utilities and Diagnostics**.
26. Choisissez **Restart System**. Cela termine la configuration du routeur A.

#### **Configuration du routeur B :**

1. Pour configurer le routeur B, procédez de la même manière que pour la configuration du routeur A.
2. 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 PPTP.
3. 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).
4. Dans le champ **Data Link Encapsulation** (ou **Encapsulation Type** selon la version de firmware), changez le protocole d'encapsulation à **PPTP** et allez dans **Data Link Options Options** (ou **Encapsulation Options** selon la version de firmware) pour modifier les options d'encapsulation.
5. Entrez l'adresse IP WAN du routeur B distant dans le champ **PPTP Partner IP Address**. 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 son adresse IP Ethernet dans le champ **PPTP Partner IP Address**.
6. Puis choisissez le **type d'authentification** pour le tunnel. Si vous désirez sécuriser votre connexion en activant le cryptage, vous devez choisir **MS-CHAP** comme authentification. Vous aurez alors le choix entre **None** (aucune) ou **MPPE (Cryptage Microsoft Point à Point)** dans le champ **Data Encryption**. **MPPE**

intègre compression et cryptage pour un haut niveau de sécurité, cependant cela ralentira la transmission de données.

7. Si au contraire vous choisissez **PAP** ou **CHAP** comme type d'authentification, vous pourrez choisir le type de compression de données dans le champ **Data Compression**. Vous aurez alors le choix entre None (aucune) ou **Standard LZS**.
8. Si le routeur B est conduit à **initier la connexion PPTP** vers le **routeur A**, entrez un identifiant de connexion dans **Send Host Name** ainsi qu'un mot de passe dans **Send Password** (ou **Secret**) puis positionnez **Initiate Connections** sur **Yes** (oui).
9. Si à l'inverse c'est le **routeur A** qui **initie la connexion** vers le **routeur B**, entrez un identifiant de connexion dans **Receive Host Name** ainsi qu'un mot de passe dans **Receive Password** (ou **Secret**).
10. Si vous désirez que **le Routeur B initie une connexion PPTP** vers le **Routeur A** à chaque fois qu'il y a une demande d'accès à une ressource du réseau situé derrière le routeur A, assurez-vous que **On Demand** est positionné sur **Yes**.
11. Vous pouvez modifier l'expiration du **délai d'attente (Idle Timeout)**, il s'agit de régler au bout de combien de temps le routeur A doit déconnecter le tunnel PPTP lorsqu'il n'y a pas de trafic. Vous pouvez changer le **délai d'attente à 0 seconde** pour que la connexion PPTP n'expire pas en absence de trafic.
12. Tapez sur **Echap** pour retourner à l'écran **Add Connection Profile**.
13. Selon la version de firmware (microcode) utilisé sur le routeur, vous pouvez être amené à activer IP dans le profil de connexion en positionnant **IP Enabled** sur **Yes**.
14. Allez dans le menu **IP Profile Parameters**. Désactivez la traduction d'adresse IP en commutant **Address Translation Enabled** sur **No** (Rappel : Utilisez la touche Tab pour commuter entre Yes et No. Tapez sur Entrée pour valider le changement).
15. Configurez les champs **Remote IP Address** et **Remote IP Mask** avec l'adresse IP Ethernet du routeur A soit **192.168.1.1** et son masque de sous-réseau **255.255.255.0**. Notez que si l'adresse IP Ethernet du routeur A est différente, entrez celle-ci.
16. Ne choisissez pas de jeu de filtres (**Filter Set**) et au besoin si un jeu de filtres est déjà configuré, tapez sur entrée après avoir sélectionné **Remove Filter Set** pour le désactiver (il est possible d'utiliser des filtres sur une connexion PPTP, cependant les jeu de filtres pré configurés sont peu adaptés à cet usage. Si vous désirez filtrer le trafic sur votre tunnel PPTP, veuillez vous référer à la note technique [NIR\\_052\\_FR : Description et configuration du Firewall des routeurs Netopia](#)).
17. Désactivez RIP en réglant **Receive RIP** sur **Off** (notez que ce menu est accessible directement dans les paramètres IP ou dans le menu **RIP Profile Options...**). N'activez RIP que si vous disposez de routeurs derrière les Netopia ayant eux-mêmes RIP actif.
18. Tapez sur **Echap** pour retourner à l'écran **Add Connection Profile** et allez sur **Add Profile Now** puis tapez **Entrée**.

19. Depuis l'écran **Connection Profiles**, tapez à nouveau **Echap** pour revenir à **Quick Menus**.
20. Sélectionnez **ATMP/PPTP Default Profile** ou **VPN Default Answer Profile** (pour les firmwares inférieurs à 4.8).
21. Réglez sur **Yes, Answer ATMP/PPTP Connections** ou **Answer VPN Connections** (pour les firmwares inférieurs à 4.8).
22. Dans **PPTP Configuration Options**, allez sur **Receive Authentication** et choisissez le même type d'authentification que celle utilisée dans le profil de connexion.
23. Tapez **Echap** pour revenir dans **Quick Menus**.
24. Choisissez le menu **WAN Default Profile**.
25. Changez le champ **Must Match a Defined Profile** à **Yes**.  
Notez que les routeurs dotés d'interface WAN Ethernet tels que R910 et R9100 ne disposent pas de ce menu. Dans ce cas ignorez cette étape et passez à la suivante.
26. Tapez sur **Echap** deux fois pour revenir au menu principal et allez dans le menu **Utilities et Diagnostics**.
27. Choisissez **Restart System**. Cela termine la configuration du routeur B.

### Test de la connexion VPN :

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

1. **Le premier test** que vous pouvez réaliser est de **connecter manuellement le profil de connexion PPTP**. Sur le routeur qui doit initier la connexion (ex : routeur A) établissez manuellement la connexion. Pour ce faire, depuis le menu principal allez dans **Quick Menu** puis dans **Connection Profiles**. Choisissez **Establish WAN Connection** et sélectionnez le profil de connexion PPTP puis appuyez sur **Entrée**. Le routeur va alors essayer de se connecter. Dans l'écran **Call Status**, la connexion doit passer par les étapes :
  - **Attempting** (le routeur essaye de contacter le routeur B)
  - **Acquiring** (le routeur a contacté le routeur B et négocie les paramètres PPTP)
  - **Connected** (la connexion PPTP est établie)
 Si vous n'arrivez pas à l'étape **Connected**, contrôlez les paramètres des profils de connexion PPTP et essayez de nouveau. Si cela n'est toujours pas concluant, contactez l'Assistance Technique.  
Tapez **Echap** pour revenir à **Connection Profiles** et encore deux fois pour revenir au menu principal.
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 (si la connexion PPTP est initiée 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 10 dans **Packets to Send** pour le nombre de paquets ICMP à envoyer. 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 la connexion PPTP est fonctionnelle, 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 de la connexion PPTP**. Pour cela, allez dans le menu **Quick View** puis dans **VPN Quick View**. Vérifiez que les compteurs **Rx Pckts** et **Tx Pckts** 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 la connexion PPTP.