



Guide d'installation de WinGate

Bienvenue dans WinGate !

Ce guide vous aidera à installer et à configurer WinGate.

Nous vous recommandons de le lire entièrement avant la première utilisation du logiciel.

Démarrer



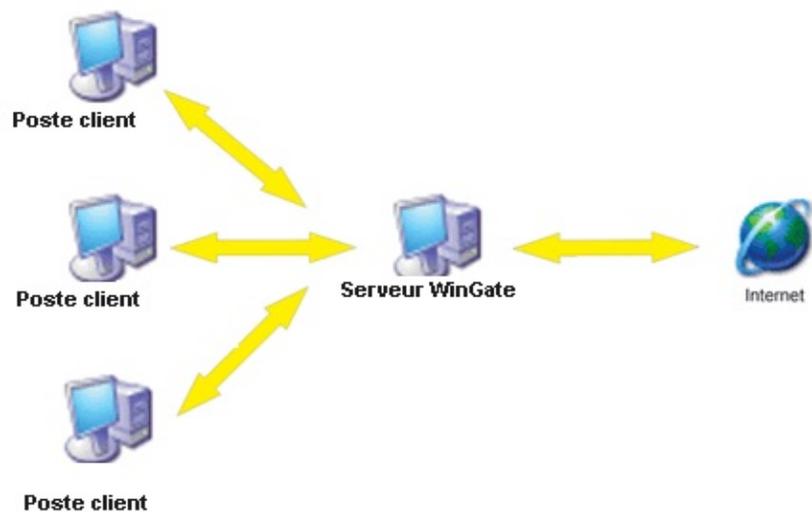
©2005 Qbik New Zealand Limited

WinGate est une marque déposée de Qbik IP Management Limited. Tous les autres produits sont la propriété de leurs éditeurs respectifs.

Quelle est la configuration de votre réseau ?

Configuration 1

(Installation recommandée)

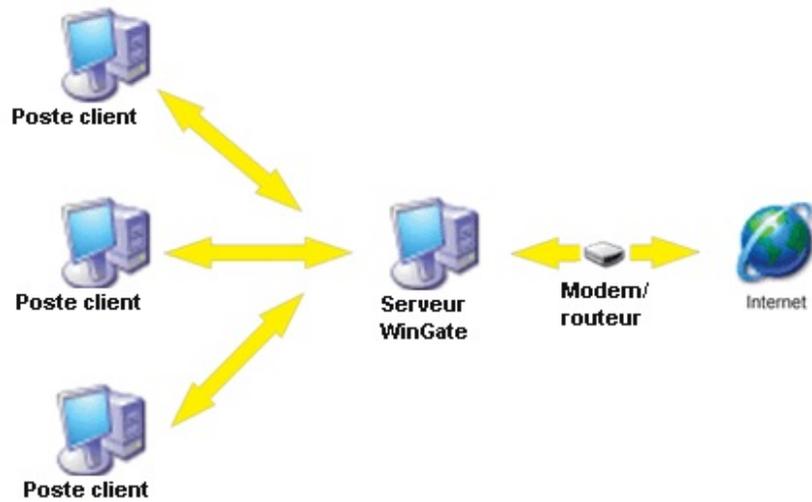


WinGate est installé sur un poste possédant une connexion directe à Internet. Il s'agit de la configuration recommandée et la plus fréquemment utilisée.

[Cliquez ici pour en savoir plus sur ce type de configuration](#)

Configuration 2

(Installation recommandée)



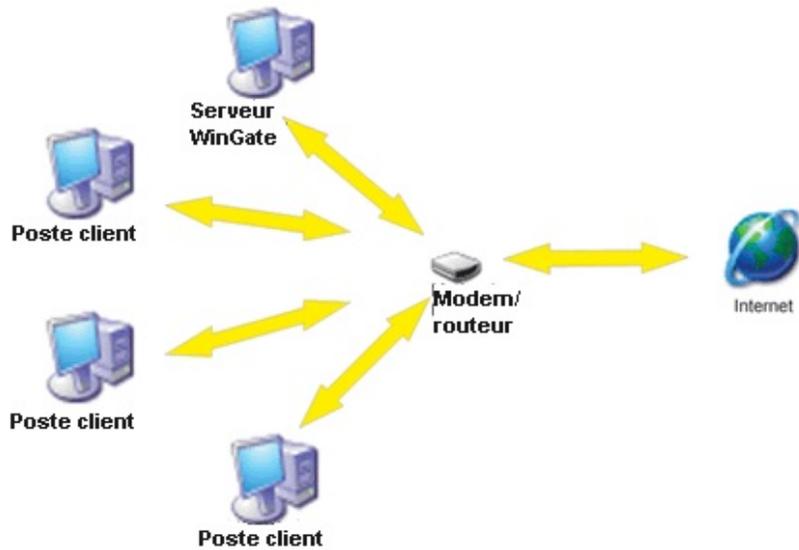
Tous les postes du réseau local se connectent à WinGate, qui accède à Internet par le biais d'un routeur.

Le poste WinGate possède deux interfaces réseau : l'une se connecte au réseau local et l'autre au routeur.

[Cliquez ici pour en savoir plus sur ce type de configuration](#)

Configuration 3

(Installation déconseillée)



Tous les postes du réseau sont connectés au routeur, y compris le serveur WinGate. Cette installation est déconseillée car les clients peuvent plus facilement "échapper" au contrôle de WinGate. Dans la mesure du possible, il est préférable de choisir la [configuration 2](#).

Même si le routeur est directement connecté à Internet, tous les postes clients seront redirigés vers WinGate.

[Cliquez ici pour en savoir plus sur ce type de configuration](#)

©2005 Qbik New Zealand Limited

Étape 1 : configuration requise

Avant d'installer WinGate, assurez-vous de choisir un ordinateur adapté, répondant aux critères de la configuration minimale requise.

WinGate peut être installé sur n'importe quel poste de votre réseau, à condition qu'il possède une connexion directe à Internet.

Nous vous recommandons d'utiliser si possible Windows NT/2000/XP car ces systèmes sont beaucoup mieux sécurisés que Windows 95 ou 98.

Réseau local de petite taille : 2 à 5 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium II 233 Mhz avec 32 Mo de RAM	Pentium 300+ avec 64 Mo de RAM
Windows 95/98	Windows 2000
Modem 56k	DSL
Protocole TCP/IP installé	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés
Winsock 2 installé	Mise à jour Winsock 2 installée (uniquement sous Windows 95a)

Réseau local de taille moyenne : 5 à 20 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium 300+ avec 64 Mo de RAM	Pentium 1000+ avec 128 Mo de RAM
Windows NT +SP4	Windows 2000

Modem 56k	Connexion large bande
TCP/IP et RRAS (Routing and Remote Access Service) installés	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés

Réseau local de grande taille : + de 20 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium 300+ avec 64 Mo de RAM	Pentium 1000+ avec 512 Mo de RAM
Windows 2000	Windows 2000
Connexion ISDN/ Ligne louée/ T1	T1
TCP/IP et RRAS (Routing and Remote Access Service) installés	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés

Étape 2 

©2005 Qbik New Zealand Limited

Étape 2 : configuration de l'interface réseau locale

Le poste WinGate doit posséder une [interface réseau](#) locale qui le relie aux autres postes du réseau local.

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Dans les propriétés TCP/IP, cochez l'option **Utiliser l'adresse IP suivante** et indiquez une adresse comprise dans la même plage que les autres postes du réseau local (adresse IP privée du type 10.0.0.1 ou 192.168.0.1). [Cliquez ici pour en savoir plus sur les adresses IP](#).
5. Remplissez le champ **Masque de sous-réseau** (généralement : 255.255.255.0).
6. Ne remplissez pas le champ **Passerelle par défaut**.
7. Ne remplissez pas le champ **Serveur DNS préféré**.
8. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

©2005 Qbik New Zealand Limited

Étape 3 : configuration de la connexion Internet

Le serveur WinGate étant directement connecté à Internet, deux possibilités s'offrent à vous :

1. Connexion "à la demande"

Connexion par le biais d'une ligne téléphonique, déclenchée par des applications (navigateurs, clients de messagerie) ou manuellement. Cela inclut les connexions commutées, RNIS, modems ADSL, et certaines connexions satellite.

Un profil est créé dans le système d'exploitation lors de l'installation du périphérique. Vous devez ensuite configurer WinGate pour qu'il utilise le profil choisi. ([Cliquez ici pour savoir comment configurer les profils de connexion dans WinGate.](#))

Ces connexions ne possèdent une adresse IP (fournie par le FAI) qu'après s'être connectées à Internet.

Aucune configuration supplémentaire n'est nécessaire. Veuillez toutefois vous assurer du bon fonctionnement de la connexion avant d'installer WinGate.

2. Connexion permanente

Il s'agit généralement de cartes réseau possédant une adresse IP publique attribuée par le fournisseur d'accès. Cela inclut les connexions T1, fibre optique, relais de trames, ou interfaces DSL.

Elles ne possèdent pas de profil associé dans Windows, mais apparaissent dans la liste des connexions réseau.

Les paramètres Internet étant fournis de façon permanente par le FAI, il n'est pas nécessaire de les configurer avant l'installation de WinGate.

WinGate les classe automatiquement en tant que connexions possibles à Internet car elles possèdent une adresse IP publique.

Étape 4 

©2005 Qbik New Zealand Limited

Étape 4 : installation de WinGate

Le procédé d'installation s'effectue de façon très simple, à l'aide d'un assistant. Toutefois, en cas de problème, chaque fenêtre contient un bouton **Help**.

Accord de licence (*Licence agreement*)

Vous devez accepter les termes de l'accord de licence avant d'installer WinGate. Si vous ne les acceptez pas, vous pouvez quitter l'installation.

Type d'installation



Deux possibilités s'offrent à vous : installation du serveur ou du client WinGate (WGIC).

N'oubliez pas que le serveur doit être installé sur un poste possédant un accès direct à Internet.

Une [écran de confirmation](#) s'affiche avant de poursuivre l'installation.

Installation du serveur

Procédure détaillée de l'installation du **serveur** :

1. [Répertoire d'installation](#)
2. [Important](#)
3. [Utilisateurs NT et authentification](#)

4. E-mail
5. ENS
6. Mises à jour automatiques
7. Activation de WinGate
8. Début de l'installation
9. Installation terminée

WinGate est à présent prêt à fonctionner. Il ne vous reste alors qu'à vérifier les divers points mentionnés dans l'étape 5.

Mises à jour

Si vous effectuez une mise à jour, ou si vous installez WinGate sur poste possédant déjà WinGate VPN, une option vous propose de sauvegarder les fichiers remplacés lors de l'installation (***Backup replaced Files***).

Le programme d'installation peut créer des copies de sauvegarde de tous les fichiers remplacés au cours de l'installation. Ces fichiers sont utilisés lorsque le logiciel est désinstallé. Nous vous recommandons de ne pas désactiver cette option car en l'absence de copies de sauvegarde, vous pourrez désinstaller WinGate mais pas restaurer entièrement le système.

Remarque concernant les sauvegardes

Si vous installez WinGate après WinGate VPN, puis décidez de désinstaller WinGate, vous devez prendre certaines précautions afin d'éviter de perdre les paramètres du VPN.

Sauvegarde de la configuration de WinGate VPN

Il est nécessaire de sauvegarder les paramètres de WinGate VPN avant d'installer WinGate. Le programme d'installation de WinGate les enregistre automatiquement dans un fichier appelé **WinGateVPN.reg** (dans le répertoire d'installation). Pour effectuer cette opération manuellement :

1. Démarrez WinGate VPN
2. Dans le menu **Options**, sélectionnez **Avancées**
3. Cliquez sur **Sauvegarder le registre (Save registry settings)**

Restauration de la configuration de WinGate VPN

Pour restaurer WinGate VPN après avoir désinstallé WinGate :

1. Installez **WinGate VPN**
2. **Importez** la configuration que vous avez sauvegardée. Pour cela :

Si vous avez effectué une sauvegarde manuelle : importez le fichier de registre que vous avez enregistré, et écrasez les valeurs présentes dans le registre.

Si vous avez effectué une sauvegarde automatique : importez le fichier "WinGateVPN.reg", et écrasez les valeurs présentes dans le registre.

Étape 5 

Étape 5 : après l'installation

Après avoir installé WinGate, il est recommandé de vérifier les points suivants afin de s'assurer qu'il est correctement configuré.

Icône du moteur de WinGate

Elle s'affiche automatiquement dans la zone de notification (en bas à droite de votre écran) au démarrage de Windows et indique l'état du moteur de WinGate.



Le moteur est en train de démarrer.



Le moteur est actif.



Le moteur est arrêté.

GateKeeper

[GateKeeper](#) est l'interface permettant de configurer le moteur de WinGate

Accès à GateKeeper

1. Effectuez un clic droit sur l'icône du moteur de WinGate dans la zone de notification et sélectionnez **GateKeeper**,

OU BIEN

2. Sélectionnez **GateKeeper** dans le menu démarrer/WinGate.

Première connexion à GateKeeper :

1. Ouvrez **GateKeeper**.
2. Assurez-vous que le nom d'utilisateur soit **Administrator**.
3. Ne remplissez pas le champ du mot de passe et cliquez sur **OK**.
4. Une boîte de dialogue vous invite alors à choisir un mot de passe.
5. Vous êtes à présent connecté à **GateKeeper** en tant qu'**Administrator**.

Remarque :

Si lors de l'installation vous avez coché l'option [Utiliser la base de données du système d'exploitation \(Use Operating System \(Windows\) database\)](#) il n'est pas nécessaire de choisir un mot de passe lors de la première connexion.

Connexions réseau

Une fois connecté à **GateKeeper**, vous devez vérifier si WinGate a correctement identifié et classifié les connexions réseau.

Interface réseau locale et connexion Internet

1. Dans GateKeeper, cliquez sur l'onglet **Réseau (Network)**.
2. Au bas de cet onglet se trouve un panneau appelé **connexions réseau (network connections)** dans lequel figurent toutes les interfaces détectées par WinGate.
3. Double-cliquez sur l'interface reliant WinGate au réseau local : elle doit être définie en tant qu'interface **Interne (Internal)**.
4. Double-cliquez sur la connexion Internet : elle doit être définie en tant qu'interface **Externe (External)**.

Profils de connexion

1. Dans GateKeeper, cliquez sur l'onglet **Réseau (Network)**.
2. Si la connexion Internet possède un profil dans Windows (modem ou connexion commutée), double-cliquez sur son nom pour en configurer les paramètres.
3. Dans les propriétés de l'interface, sélectionnez l'onglet **Numérotation (Auto Dial)**.
4. Assurez-vous que l'option **Autoriser WinGate à utiliser cette connexion (Enable this connection to be used by WinGate)** soit cochée.
5. Indiquez le nom d'utilisateur et le mot de passe correspondant à ce profil.
6. Cliquez sur **OK** pour enregistrer les modifications.

Test de la connectivité des clients

Après vous être assuré que les connexions réseau soient correctement configurées, il ne vous reste plus qu'à vérifier si les postes clients peuvent se connecter à Internet.

Par défaut, tous les utilisateurs peuvent accéder à Internet (ou aux services de WinGate). L'onglet **Activité (Activity)** affiche toutes les connexions des clients.

[Cliquez ici pour savoir comment configurer les postes clients](#) 

Étape 1 : configuration requise

Avant d'installer WinGate, assurez-vous de choisir un ordinateur adapté, répondant aux critères de la configuration minimale requise.

WinGate peut être installé sur n'importe quel poste de votre réseau, à condition qu'il possède une connexion directe à Internet.

Nous vous recommandons d'utiliser si possible Windows NT/2000/XP car ces systèmes sont beaucoup mieux sécurisés que Windows 95 ou 98.

Réseau local de petite taille : 2 à 50 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium II 233 Mhz avec 32 Mo de RAM	Pentium 300+ avec 64 Mo de RAM
Windows 95/98	Windows 2000
Modem 56k	DSL
Protocole TCP/IP installé	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés
Winsock 2 installé	Mise à jour Winsock 2 installée (uniquement sous Windows 95a)

Réseau local de taille moyenne : 50 à 250 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium 300+ avec 64 Mo de RAM	Pentium 1000+ avec 128 Mo de RAM

Windows NT +SP4	Windows 2000
Modem 56k	Connexion large bande
TCP/IP et RRAS (Routing and Remote Access Service) installés	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés

Réseau local de grande taille : + de 250 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium 300+ avec 64 Mo de RAM	Pentium 1000+ avec 512 Mo de RAM
Windows 2000	Windows 2000
Connexion ISDN/ Ligne louée/ T1	T1
TCP/IP et RRAS (Routing and Remote Access Service) installés	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés

Étape 2 

©2005 Qbik New Zealand Limited

Étape 2 : configuration de l'interface réseau locale

Le poste WinGate doit posséder une interface réseau locale qui le relie aux autres postes du réseau local.

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

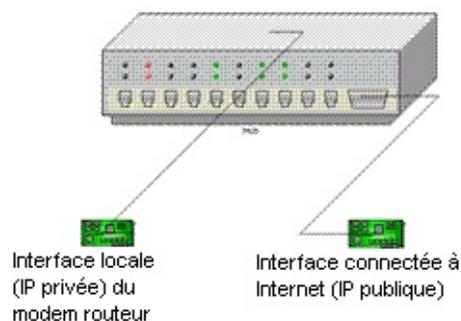
4. Dans les propriétés TCP/IP, cochez l'option **Utiliser l'adresse IP suivante** et indiquez une adresse comprise dans la même plage que les autres postes du réseau local (adresse IP privée du type 10.0.0.1 ou 192.168.0.1). [Cliquez ici pour en savoir plus sur les adresses IP](#).
5. Remplissez le champ **Masque de sous-réseau** (généralement : 255.255.255.0).
6. Ne remplissez pas le champ **Passerelle par défaut**.
7. Ne remplissez pas le champ **Serveur DNS préféré**.
8. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

©2005 Qbik New Zealand Limited

Étape 3 : configuration de l'interface du routeur

Cette étape consiste à configurer l'interface reliant WinGate au modem routeur.

Présentation du routeur



Même si la plupart des modems routeurs ne possèdent pas de carte réseau, ils possèdent deux "interfaces".

1. **Interface Internet**

Interface possédant une adresse IP publique et connectée à Internet.

2. **Interface locale**

Interface possédant une adresse IP privée, à laquelle se connectent les postes du réseau.

Les modems routeurs s'accompagnent généralement d'un service DHCP permettant d'attribuer aux postes clients des adresses IP (privées) comprises dans la même plage que leur interface interne.

Le seul poste directement connecté au routeur et communiquant avec son interface interne est le serveur WinGate. Il sera donc le seul à recevoir les paramètres Internet de son service DHCP.

Ces paramètres seront attribués à l'interface du poste WinGate reliée au routeur.

Configuration de l'interface réseau du serveur WinGate pour qu'il utilise les paramètres Internet fournis par le routeur :

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés** (il s'agit de l'interface connectée au routeur).
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Dans les propriétés TCP/IP, cochez l'option **Obtenir une adresse IP automatiquement**. Tous les paramètres seront alors attribués automatiquement par le routeur.
5. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications

Remarque :

Si vous ne souhaitez pas utiliser le service DHCP du routeur et configurer ces informations manuellement :

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée

4. Dans les propriétés TCP/IP, cochez l'option **Utiliser l'adresse IP suivante** et indiquez une adresse privée comprise dans la même plage que l'interface locale du routeur (du type : 10.0.0.1 ou 192.168.0.1).
5. Dans le champ **Masque de sous-réseau**, indiquez le masque utilisé par l'interface locale du routeur.
6. Dans le champ **Passerelle par défaut**, indiquez l'adresse IP de l'interface locale du routeur.
7. Dans le champ **Serveur DNS préféré**, indiquez l'adresse IP de l'interface locale du routeur.
8. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

Avant d'installer WinGate, assurez-vous que le poste choisi accède correctement à Internet à l'aide du routeur.

Remarque importante :

Après avoir installé WinGate, vous devez indiquer dans GateKeeper que cette interface est une interface externe ([cliquez ici](#) pour en savoir plus)

©2005 Qbik New Zealand Limited

Étape 4 : installation de WinGate

Le procédé d'installation s'effectue de façon très simple, à l'aide d'un assistant. Toutefois, en cas de problème, chaque fenêtre contient un bouton **Help**.

Accord de licence (*Licence agreement*)

Vous devez accepter les termes de l'accord de licence avant d'installer WinGate. Si vous ne les acceptez pas, vous pouvez quitter l'installation.

Type d'installation



Deux possibilités s'offrent à vous : installation du serveur ou du client WinGate (WGIC).

N'oubliez pas que le serveur doit être installé sur un poste possédant un accès direct à Internet.

Une [écran de confirmation](#) s'affiche avant de poursuivre l'installation.

Installation du serveur

Procédure détaillée de l'installation du **serveur** :

1. [Répertoire d'installation](#)
2. [Important](#)
3. [Utilisateurs NT et authentification](#)

4. E-mail
5. ENS
6. Mises à jour automatiques
7. Activation de WinGate
8. Début de l'installation
9. Installation terminée

WinGate est à présent prêt à fonctionner. Il ne vous reste alors qu'à vérifier les divers points mentionnés dans l'étape 5.

Mises à jour

Si vous effectuez une mise à jour, ou si vous installez WinGate sur poste possédant déjà WinGate VPN, une option vous propose de sauvegarder les fichiers remplacés lors de l'installation (***Backup replaced Files***).

Le programme d'installation peut créer des copies de sauvegarde de tous les fichiers remplacés au cours de l'installation. Ces fichiers sont utilisés lorsque le logiciel est désinstallé. Nous vous recommandons de ne pas désactiver cette option car en l'absence de copies de sauvegarde, vous pourrez désinstaller WinGate mais pas restaurer entièrement le système.

Remarque concernant les sauvegardes

Si vous installez WinGate après WinGate VPN, puis décidez de désinstaller WinGate, vous devez prendre certaines précautions afin d'éviter de perdre les paramètres du VPN.

Sauvegarde de la configuration de WinGate VPN

Il est nécessaire de sauvegarder les paramètres de WinGate VPN avant d'installer WinGate. Le programme d'installation de WinGate les enregistre automatiquement dans un fichier appelé **WinGateVPN.reg** (dans le répertoire d'installation). Pour effectuer cette opération manuellement :

1. Démarrez WinGate VPN
2. Dans le menu **Options**, sélectionnez **Avancées**
3. Cliquez sur **Sauvegarder le registre (Save registry settings)**

Restauration de la configuration de WinGate VPN

Pour restaurer WinGate VPN après avoir désinstallé WinGate :

1. Installez **WinGate VPN**
2. **Importez** la configuration que vous avez sauvegardée. Pour cela :

Si vous avez effectué une sauvegarde manuelle : importez le fichier de registre que vous avez enregistré, et écrasez les valeurs présentes dans le registre.

Si vous avez effectué une sauvegarde automatique : importez le fichier "WinGateVPN.reg", et écrasez les valeurs présentes dans le registre.

Étape 5 

Étape 5 : après l'installation

Après avoir installé WinGate, il est recommandé de vérifier les points suivants afin de s'assurer qu'il est correctement configuré.

Icône du moteur de WinGate

Elle s'affiche automatiquement dans la zone de notification (en bas à droite de votre écran) au démarrage de Windows et indique l'état du moteur de WinGate.

 Le moteur est en train de démarrer.

 Le moteur est actif.

 Le moteur est arrêté.

GateKeeper

[GateKeeper](#) est l'interface permettant de configurer le moteur de WinGate

Accès à GateKeeper

1. Effectuez un clic droit sur l'icône du moteur de WinGate dans la zone de notification et sélectionnez **GateKeeper**,

OU BIEN

2. Sélectionnez **GateKeeper** dans le menu démarrer/WinGate.

Première connexion à GateKeeper :

1. Ouvrez **GateKeeper**.
2. Assurez-vous que le nom d'utilisateur soit **Administrator**.
3. Ne remplissez pas le champ du mot de passe et cliquez sur **OK**.
4. Une boîte de dialogue vous invite alors à choisir un mot de passe.
5. Vous êtes à présent connecté à **GateKeeper** en tant qu'**Administrator**.

Remarque :

Si lors de l'installation vous avez coché l'option [Utiliser la base de données du système d'exploitation \(Use Operating System \(Windows\) database\)](#) il n'est pas nécessaire de choisir un mot de passe lors de la première connexion.

Connexions réseau

Une fois connecté à **GateKeeper**, vous devez vérifier si WinGate a correctement identifié et classifié les connexions réseau.

1. Dans GateKeeper, cliquez sur l'onglet **Réseau (Network)**.
2. Au bas de cet onglet se trouve un panneau appelé **connexions réseau (network connections)** dans lequel figurent toutes les interfaces détectées par WinGate.
3. Double-cliquez sur l'interface reliant WinGate au réseau local : elle doit être définie en tant qu'interface **Interne (Internal)**.

Interface reliant WinGate au routeur

1. Double-cliquez sur l'interface servant à connecter WinGate au routeur.
2. Assurez-vous qu'elle soit définie en tant qu'interface **Externe (External)**.
3. Cliquez sur **OK** pour enregistrer les modifications.

Test de la connectivité des clients

Après vous être assuré que les connexions réseau soient correctement configurées, il ne vous reste plus qu'à vérifier si les postes clients peuvent se connecter à Internet.

Par défaut, tous les utilisateurs peuvent accéder à Internet (ou aux services de WinGate). L'onglet **Activité (Activity)** affiche toutes les connexions des clients.

[Cliquez ici pour savoir comment configurer les postes clients](#) 

Étape 1 : configuration requise

Avant d'installer WinGate, assurez-vous de choisir un ordinateur adapté, répondant aux critères de la configuration minimale requise.

WinGate peut être installé sur n'importe quel poste de votre réseau, à condition qu'il possède une connexion directe à Internet.

Nous vous recommandons d'utiliser si possible Windows NT/2000/XP car ces systèmes sont beaucoup mieux sécurisés que Windows 95 ou 98.

Réseau local de petite taille : 2 à 50 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium II 233 Mhz avec 32 Mo de RAM	Pentium 300+ avec 64 Mo de RAM
Windows 95/98	Windows 2000
Modem 56k	DSL
Protocole TCP/IP installé	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés
Winsock 2 installé	Mise à jour Winsock 2 installée (uniquement sous Windows 95a)

Réseau local de taille moyenne : 50 à 250 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium 300+ avec 64 Mo de RAM	Pentium 1000+ avec 128 Mo de RAM
Windows NT +SP4	Windows 2000

Modem 56k	Connexion large bande
TCP/IP et RRAS (Routing and Remote Access Service) installés	TCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés

Réseau local de grande taille : + de 250 utilisateurs

Configuration minimale requise	Configuration recommandée
Pentium 300+ avec 64 Mo de RAM	Pentium 1000+ avec 512 Mo de RAM
Windows 2000	Windows 2000
Connexion ISDN / Ligne louée / T1	T1
TCP/IP et RRAS (Routing and Remote Access Service) installés	TTCP/IP et RRAS (Routing and Remote Access Service - uniquement pour NT) installés

Étape 2 

©2005 Qbik New Zealand Limited

Étape 2 : configuration de l'interface réseau locale

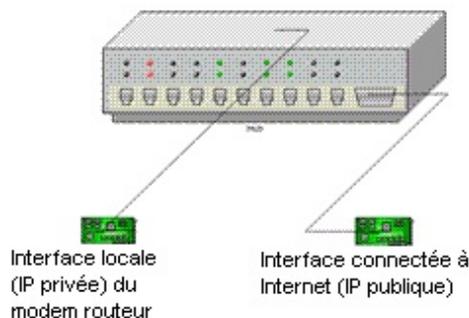
Ce type de configuration est **déconseillé** car tous les postes du réseau étant physiquement reliés à la connexion Internet (le routeur), ils peuvent facilement "échapper" aux mesures de contrôle et de sécurité appliquées par WinGate.

De plus, cela limite les méthodes de connexion pouvant être utilisées : seuls [WGIC](#) et les [proxies](#) seront disponibles. Le [NAT](#) (traduction d'adresses réseau) ne fonctionnera pas correctement.

Afin d'éviter ces problèmes, il est recommandé d'appliquer la [configuration 2](#).

Si toutefois vous souhaitez continuer, configurez l'interface réseau locale comme suit :

Présentation du routeur



Même si la plupart des modems routeurs ne possèdent pas de carte réseau, ils possèdent deux "interfaces".

1. **Interface Internet**

Interface possédant une adresse IP publique et connectée à Internet.

2. **Interface locale**

Interface possédant une adresse IP privée, à laquelle se connectent les postes du réseau.

Les modems routeurs s'accompagnent généralement d'un service DHCP permettant d'attribuer aux postes clients des adresses IP (privées) comprises dans la même plage que leur interface interne.

Puisque tous les postes (y compris le serveur WinGate) sont connectés au routeur, vous pouvez les configurer afin d'utiliser les paramètres Internet fournis par le routeur.

Configuration de l'interface réseau du **serveur WinGate** pour qu'il utilise les paramètres Internet fournis par le routeur :

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés** (il s'agit de l'interface connectée au routeur).
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Dans les propriétés TCP/IP, cochez l'option **Obtenir une adresse IP automatiquement**. Tous les paramètres seront alors attribués automatiquement par le routeur.

5. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

Si vous ne souhaitez pas utiliser le service DHCP du routeur :

1. Désactivez le service sur le routeur.
2. Sur le serveur WinGate, double-cliquez sur **Connexions réseau** dans le **Panneau de configuration**.
3. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
4. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

5. Dans les propriétés TCP/IP, cochez l'option **Utiliser l'adresse IP suivante** et indiquez une adresse privée comprise dans la même plage que l'interface locale du routeur (du type : 10.0.0.1 ou 192.168.0.1).
[Cliquez ici pour en savoir plus sur les adresses IP.](#)
6. Dans le champ **Masque de sous-réseau**, indiquez le masque utilisé par l'interface locale du routeur.
7. Dans le champ **Passerelle par défaut**, indiquez l'adresse IP de l'interface locale du routeur.
8. Dans le champ **Serveur DNS préféré**, indiquez l'adresse IP de l'interface locale du routeur.
9. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

Postes clients

Tous les postes clients étant directement reliés au routeur, il est important de configurer correctement leurs paramètres Internet avant d'installer WinGate.

Nous vous recommandons de configurer ces paramètres **MANUELLEMENT** afin de pouvoir contrôler l'accès au réseau avec WinGate.

N'oubliez pas que seuls **Wingate Internet Client** et les **proxies** seront disponibles avec cette méthode.

1. Sur chaque poste client, dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Dans les propriétés TCP/IP, cochez l'option **Utiliser l'adresse IP suivante** et indiquez une adresse privée comprise dans la même plage que l'interface locale du routeur (du type : 10.0.0.1 ou 192.168.0.1).
[Cliquez ici pour en savoir plus sur les adresses IP.](#)
5. Dans le champ **Masque de sous-réseau**, indiquez le masque utilisé par l'interface locale du routeur.
6. Ne remplissez pas le champ **Passerelle par défaut**.
7. Dans le champ **Serveur DNS préféré**, indiquez l'adresse IP du serveur WinGate.
8. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

©2005 Qbik New Zealand Limited

Étape 3 : configuration de la connexion entre WinGate et le routeur

Avec cette configuration, le serveur WinGate doit être le **SEUL** poste du réseau dont la [passerelle par défaut](#) et les paramètres **DNS** correspondent à l'adresse IP de l'interface locale du routeur.

En effet, si la passerelle par défaut et les paramètres DNS des postes clients correspondent également à l'adresse IP du routeur, rien ne les empêche d'accéder directement à Internet, sans passer par WinGate.

Par conséquent, il est recommandé de désactiver le service DHCP du routeur afin qu'il n'attribue pas automatiquement ces informations aux postes clients. Dans ce cas, les clients doivent être configurés manuellement, comme indiqué dans [l'étape 2](#).

Si vous avez suivi les instructions de l'étape 2 pour la configuration de l'interface interne de WinGate, vous pouvez alors commencer l'installation du logiciel.

Étape 4 

©2005 Qbik New Zealand Limited

Étape 4 : installation de WinGate

Le procédé d'installation s'effectue de façon très simple, à l'aide d'un assistant. Toutefois, en cas de problème, chaque fenêtre contient un bouton **Help**.

Accord de licence (*Licence agreement*)

Vous devez accepter les termes de l'accord de licence avant d'installer WinGate. Si vous ne les acceptez pas, vous pouvez quitter l'installation.

Type d'installation



Deux possibilités s'offrent à vous : installation du serveur ou du client WinGate (WGIC).

N'oubliez pas que le serveur doit être installé sur un poste possédant un accès direct à Internet.

[Une écran de confirmation](#) s'affiche avant de poursuivre l'installation.

Installation du serveur

Procédure détaillée de l'installation du **serveur** :

1. [Répertoire d'installation](#)
2. [Important](#)
3. [Utilisateurs NT et authentification](#)

4. E-mail
5. ENS
6. Mises à jour automatiques
7. Activation de WinGate
8. Début de l'installation
9. Installation terminée

WinGate est à présent prêt à fonctionner. Il ne vous reste alors qu'à vérifier les divers points mentionnés dans l'étape 5.

Mises à jour

Si vous effectuez une mise à jour, ou si vous installez WinGate sur poste possédant déjà WinGate VPN, une option vous propose de sauvegarder les fichiers remplacés lors de l'installation (***Backup replaced Files***).

Le programme d'installation peut créer des copies de sauvegarde de tous les fichiers remplacés au cours de l'installation. Ces fichiers sont utilisés lorsque le logiciel est désinstallé. Nous vous recommandons de ne pas désactiver cette option car en l'absence de copies de sauvegarde, vous pourrez désinstaller WinGate mais pas restaurer entièrement le système.

Remarque concernant les sauvegardes

Si vous installez WinGate après WinGate VPN, puis décidez de désinstaller WinGate, vous devez prendre certaines précautions afin d'éviter de perdre les paramètres du VPN.

Sauvegarde de la configuration de WinGate VPN

Il est nécessaire de sauvegarder les paramètres de WinGate VPN avant d'installer WinGate. Le programme d'installation de WinGate les enregistre automatiquement dans un fichier appelé **WinGateVPN.reg** (dans le répertoire d'installation). Pour effectuer cette opération manuellement :

1. Démarrez WinGate VPN
2. Dans le menu **Options**, sélectionnez **Avancées**
3. Cliquez sur **Sauvegarder le registre (Save registry settings)**

Restauration de la configuration de WinGate VPN

Pour restaurer WinGate VPN après avoir désinstallé WinGate :

1. Installez **WinGate VPN**
2. **Importez** la configuration que vous avez sauvegardée. Pour cela :

Si vous avez effectué une sauvegarde manuelle : importez le fichier de registre que vous avez enregistré, et écrasez les valeurs présentes dans le registre.

Si vous avez effectué une sauvegarde automatique : importez le fichier "WinGateVPN.reg", et écrasez les valeurs présentes dans le registre.

Étape 5 

Étape 5 : après l'installation

Après avoir installé WinGate, il est recommandé de vérifier les points suivants afin de s'assurer qu'il est correctement configuré.

Icône du moteur de WinGate

Elle s'affiche automatiquement dans la zone de notification (en bas à droite de votre écran) au démarrage de Windows et indique l'état du moteur de WinGate.



Le moteur est en train de démarrer.



Le moteur est actif.



Le moteur est arrêté.

GateKeeper

[GateKeeper](#) est l'interface permettant de configurer le moteur de WinGate

Accès à GateKeeper

1. Effectuez un clic droit sur l'icône du moteur de WinGate dans la zone de notification et sélectionnez **GateKeeper**,

OU BIEN

2. Sélectionnez **GateKeeper** dans le menu démarrer/WinGate.

Première connexion à GateKeeper :

1. Ouvrez **GateKeeper**.
2. Assurez-vous que le nom d'utilisateur soit **Administrator**.
3. Ne remplissez pas le champ du mot de passe et cliquez sur **OK**.
4. Une boîte de dialogue vous invite alors à choisir un mot de passe.
5. Vous êtes à présent connecté à **GateKeeper** en tant qu'**Administrator**.

Remarque :

Si lors de l'installation vous avez coché l'option [Utiliser la base de données du système d'exploitation \(Use Operating System \(Windows\) database\)](#) il n'est pas nécessaire de choisir un mot de passe lors de la première connexion.

Connexions réseau

Une fois connecté à **GateKeeper**, vous devez vérifier si WinGate a correctement identifié et classifié les connexions réseau.

1. Dans GateKeeper, cliquez sur l'onglet **Réseau (Network)**.
2. Au bas de cet onglet se trouve un panneau appelé **connexions réseau (network connections)** dans lequel figurent toutes les interfaces détectées par WinGate.
3. Double-cliquez sur l'interface reliant WinGate au réseau local : elle doit être définie en tant qu'interface **Interne (Internal)**.

Désactivation du service NAT (traduction d'adresses réseau)

Comme nous l'avons déjà mentionné précédemment, avec la configuration choisie pour le réseau les clients peuvent facilement "échapper" au contrôle de WinGate et accéder directement à Internet à l'aide du routeur.

Les postes clients doivent donc être configurés afin de se connecter à l'aide de [WinGate Internet Client](#), ou de la méthode [proxy](#).

Le [NAT \(traduction d'adresses réseau\)](#) ne doit pas être utilisé.

Pour désactiver le NAT :

1. Ouvrez **GateKeeper**
2. Cliquez sur l'icône **Général** des propriétés du service ENS (**Extended Networking Services**)
3. Décochez l'option **General Purpose Internet Connection Sharing (NAT)**.
4. Cliquez sur **OK**
5. Redémarrez le moteur de WinGate.

Test de la connectivité des clients

Après vous être assuré que les connexions réseau soient correctement configurées, il ne vous reste plus qu'à vérifier si les postes clients peuvent se connecter à Internet.

Par défaut, tous les utilisateurs peuvent accéder à Internet (ou aux services de WinGate). L'onglet **Activité (Activity)** affiche toutes les connexions des clients.

[Cliquez ici pour savoir comment configurer les postes clients](#) 

Étape 1 : installation du TCP/IP

WinGate ne fonctionne que sur les réseaux TCP/IP. Ce protocole doit donc être installé sur chaque poste client.

Le TCP/IP est installé par défaut avec le système d'exploitation à partir de Windows 2000. Ce protocole est généralement nécessaire au bon fonctionnement des interfaces réseau ou modems installés sur l'ordinateur.

Si le TCP/IP est installé, il est recommandé de vérifier si les clients peuvent communiquer avec le serveur.

[Cliquez ici pour savoir comment tester le TCP/IP.](#)

Si le TCP/IP est installé et fonctionne correctement sur votre réseau, passez à l'étape 2. Sinon, suivez les instructions ci-dessous pour installer ce protocole :

Windows 95 ou 98

1. Cliquez sur **Démarrer / Paramètres / Panneau de configuration**
2. Double-cliquez sur **Connexions réseau**
3. Cliquez sur **Ajouter**
4. Double-cliquez sur **Protocole**, puis sélectionnez **Microsoft**
5. Sélectionnez **TCP/IP** et cliquez sur **OK**
6. Vous serez peut-être amené à redémarrer votre ordinateur

Windows NT 4

1. Cliquez sur **Démarrer / Paramètres / Panneau de configuration**
2. Double-cliquez sur **Connexions réseau**
3. Sélectionnez **Protocole**
4. Cliquez sur **Ajouter**

5. Sélectionnez **Protocole TCP/IP** et cliquez sur **OK**
6. Vous serez peut-être amené à redémarrer votre ordinateur

Windows 2000

1. Cliquez sur **Démarrer**
2. Sélectionnez **Connexions réseau et accès à distance**
3. Effectuez un clic droit sur la connexion pour laquelle vous souhaitez installer TCP/IP, puis cliquez sur **Propriétés**
4. Cliquez sur **Installer**
5. Sélectionnez **Microsoft**, puis **Protocole TCP/IP**
6. Cliquez sur **OK**.
7. Vous serez peut-être amené à redémarrer votre ordinateur

Étape 2 

Étape 2 : adresses IP des clients

WinGate propose un service DHCP afin d'attribuer automatiquement une adresse IP aux clients qui en font la requête, ce qui facilite la configuration de votre réseau. Utilisé en mode entièrement automatique, ce service fournit aux postes clients tous les paramètres Internet nécessaires.

(Pour en savoir plus sur le service DHCP, consultez l'aide de WinGate.)

Si vous possédez déjà un serveur DHCP sur votre réseau et que vous souhaitez l'utiliser, effectuez les modifications suivantes :

1. Désactivation du service DHCP de WinGate

Afin d'éviter les conflits, le service DHCP de WinGate doit être désactivé (cela n'affecte en rien le fonctionnement du logiciel).

Pour cela :

1. Ouvrez **GateKeeper**.
2. Dans l'onglet **Système (System)**, ouvrez les propriétés du service DHCP et cliquez sur l'icône **Général**.
3. Dans le menu déroulant des options de démarrage, sélectionnez **Désactivé (Disabled)**.
4. Cliquez sur **OK** pour enregistrer les modifications.

2. Passerelle par défaut

La **passerelle par défaut** des clients se connectant à WinGate avec la méthode **NAT** doit correspondre à l'adresse IP privée du serveur WinGate. Les serveurs DHCP comportent généralement une option appelée "Passerelle" ou "Routeur" permettant d'attribuer ce paramètre automatiquement.

3. **Serveur DNS préféré**

L'option **Serveur DNS préféré** des clients se connectant à WinGate à l'aide de **WinGate Internet Client** doit également correspondre à l'adresse IP privée du serveur WinGate. Les serveurs DHCP comportent généralement une option appelée "Serveur DNS" permettant d'attribuer ce paramètre automatiquement.

Quel que soit le serveur DHCP choisi, les postes clients doivent être configurés comme suit :

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Dans les propriétés TCP/IP, cochez l'option **Obtenir une adresse IP automatiquement**. Tous les paramètres seront alors attribués automatiquement par le serveur DHCP choisi.
5. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

Si vous ne souhaitez pas utiliser de serveur DHCP sur votre réseau, les paramètres Internet des clients doivent être configurés manuellement :

1. Dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.

2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Dans les propriétés TCP/IP, cochez l'option **Utiliser l'adresse IP suivante** et indiquez une adresse comprise dans la même plage que le serveur.
5. Dans le champ **Masque de sous-réseau**, indiquez l'adresse IP privée du serveur WinGate.
6. Dans le champ **Passerelle par défaut** indiquez l'adresse IP privée du serveur. (Nécessaire avec la méthode de connexion NAT.)
7. Dans le champ **Serveur DNS préféré** indiquez l'adresse IP privée du serveur. (Nécessaire avec la méthode de connexion WinGate Internet Client)
8. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

Passer ensuite à l'étape 3 afin de choisir la méthode de connexion.

Étape 3 

©2005 Qbik New Zealand Limited

Étape 3 : choix de la méthode de connexion

Vous devez à présent choisir la méthode utilisée par les clients pour accéder à Internet.

Avec WinGate, vous disposez de trois méthodes :

1. [NAT \(traduction d'adresses réseau\) : présentation](#)
2. [WinGate Internet Client : présentation](#)
3. [Méthode proxy : présentation](#)

Après avoir choisi une méthode, les postes clients doivent être configurés afin de l'utiliser :

1. [NAT \(traduction d'adresses réseau\) : configuration](#)
2. [WinGate Internet Client : configuration](#)
3. [Méthode proxy : configuration](#)

Après avoir choisi, configuré et testé la méthode de connexion, vous êtes prêt à utiliser WinGate.

©2005 Qbik New Zealand Limited

WinGate dans un réseau local ou un groupe de travail

Cette procédure concerne les réseaux personnels, de petites entreprises et les environnements n'ayant pas de domaine. Le paramétrage de WinGate dans ce type de réseau est très simple.

Configuration du réseau

WinGate ne fonctionne que dans les réseaux TCP/IP. Il doit être installé sur un poste possédant un accès direct à Internet et un système d'exploitation Windows.

Adresses IP

Dans ce type de réseau, les postes communiquent généralement à l'aide d'adresses IP privées comprises dans une même étendue (10.0.0.*, 172.16.0.*, 192.168.1.*).

Puisque les clients adressent les requêtes à WinGate, leurs paramètres Internet (passerelle par défaut et serveur DNS) doivent être configurés avec l'adresse IP privée du serveur. (La configuration des paramètres Internet dépend avant tout de la méthode de connexion utilisée.)

DHCP

WinGate propose un serveur DHCP afin d'attribuer automatiquement les paramètres Internet aux postes clients.

Serveur

1. Vérifiez la configuration requise avant d'installer WinGate.
2. Installez WinGate sur le poste possédant une connexion Internet.
3. Assurez-vous que son interface interne possède une IP privée statique comprise dans la même étendue que les autres postes du réseau (il n'est pas nécessaire d'indiquer une passerelle par défaut et un serveur DNS sur cette interface).
4. Après l'installation, configurez le service DHCP si vous souhaitez qu'il attribue les adresses aux postes clients.

5. Vérifiez dans GateKeeper que WinGate a correctement identifié et classifié les connexions réseau (interface locale = interne et connexion Internet = externe).

Clients

1. Assurez-vous que l'interface interne des clients possède une adresse IP privée comprise dans la même étendue que le serveur.
2. Selon la méthode de connexion utilisée, vérifiez que l'adresse IP de WinGate soit définie en tant que passerelle par défaut et serveur DNS.

Sécurité

Dans ce type d'environnement, chaque poste est responsable de la protection de ses ressources.

WinGate propose une base de données d'utilisateurs afin de contrôler l'accès, exiger l'authentification et appliquer des droits et restrictions selon vos besoins.

WinGate dans un environnement Active Directory

WinGate est conçu pour fonctionner dans un environnement Active Directory. Toutefois, il est recommandé de prendre connaissance des considérations ci-dessous avant de le configurer.

Présentation d'Active Directory

Lorsque WinGate est installé en mode natif dans un environnement Active Directory, cela affecte la façon dont il doit être configuré.

Le serveur DNS AD dispose d'une fonctionnalité de transfert (onglet Redirecteurs) afin que les clients puissent bénéficier de la résolution d'adresses dans Active Directory. Il peut ainsi transférer les requêtes extérieures à son domaine vers un autre serveur DNS sur Internet. Lorsque cette option est activée, les postes clients utilisent le serveur DNS AD pour les requêtes du domaine de Active Directory, et les requêtes Internet sont transférées au serveur DNS choisi.

Active Directory et WinGate

Utilisation de WinGate pour les vérifications DNS des clients

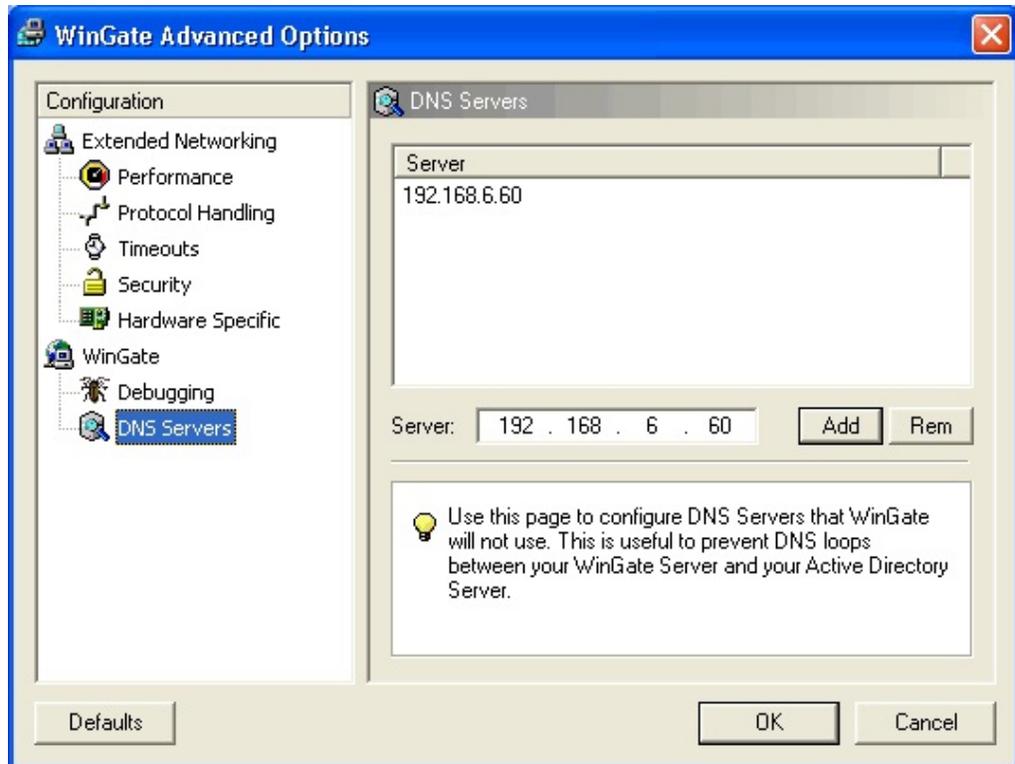
Si le serveur DNS AD ne possède pas une connexion directe à Internet ou ne peut pas résoudre les requêtes des clients, il peut donc être configuré afin de transférer les requêtes à WinGate :

Pour cela :

1. L'adresse IP privée du serveur WinGate doit figurer dans les propriétés du serveur DNS AD (dans l'onglet Redirecteurs).

Ainsi, les requêtes peuvent être transférées à WinGate.

2. Dans les **Options avancées de WinGate** (menu démarrer/WinGate), cliquez sur l'icône **Serveurs DNS (DNS servers)** et indiquez l'adresse IP interne du serveur AD.



Masquer

Cela permet d'éviter les boucles DNS entre WinGate et le serveur DNS d'Active Directory.

Utilisation du serveur DNS d'Active Directory pour les requêtes DNS

Dans un environnement Active Directory, les paramètres DNS des clients sont déjà configurés pour utiliser le serveur DNS AD. Aucune configuration supplémentaire n'est nécessaire.

Installation de WinGate sur le même poste que le serveur DNS d'Active Directory

Si WinGate se trouve sur le même poste que le serveur DNS d'Active Directory, vous devez **désactiver** le service DNS de WinGate.

DHCP

Avec Active Directory, les adresses IP (et autres paramètres réseau) sont attribuées dans la plupart des cas à l'aide d'un serveur DHCP Microsoft sur le réseau.

Si un client utilise le service NAT de WinGate, l'administrateur doit s'assurer que l'option routeur (passerelle) du serveur DHCP Microsoft est configurée de façon à attribuer aux clients l'adresse IP interne du serveur WinGate.

Le service DHCP étant couramment utilisé dans Active Directory, il est recommandé de le désactiver dans WinGate afin d'éviter les conflits.

Base de données d'utilisateurs

Si vous possédez une licence WinGate Enterprise, vous pouvez utiliser la base de données du domaine Active Directory afin de mieux contrôler vos utilisateurs et groupes.

(Pour choisir la base de données, cliquez sur **Base de données (Database options)** dans l'onglet **Utilisateurs (Users)**.)

Termes couramment employés

A B C D E F G H I J L M N O P Q R S T U V
W X Y Z

A

Adresse IP

Chaque poste d'un réseau **TCP/IP** (y compris Internet) possède une adresse unique, appelée adresse IP, permettant de l'identifier.

Ces adresses sont formées de 4 séries de chiffres (ou 4 octets) compris entre 1 et 255, par exemple : 192.168.6.5.

Elles se divisent en 5 catégories :

Classe	Plage	Utilisation
A	de 0.0.0.0 à 127.255.255.255	Généralement utilisée par les réseaux étendus.
B	de 128.0.0.0 à 191.255.255.255	Utilisée par les réseaux de taille moyenne comme ceux des universités.
C	de 192.0.0.0 à 223.255.255.255	Utilisée sur des réseaux locaux, et par les FAI afin d'attribuer une adresse à leurs clients lorsqu'ils se connectent à Internet.
D	de 224.0.0.0 à 239.255.255.255	Non disponible, réservée pour la recherche
E	de 240.0.0.0 à 255.255.255.255	Non disponible, réservée pour la recherche

Adresses IP privées

Les adresses IP privées sont, comme leur nom l'indique, réservées pour les communications au sein de réseaux privés. Ces adresses ne peuvent être utilisées qu'à l'intérieur d'un réseau local, et donc pas sur Internet.

Cela comprend les adresses suivantes :

De 10.0.0.0 à 10.255.255.255

De 172.16.0.0 à 172.31.255.255

De 192.168.0.0 à 192.168.255.255

Adresses IP publiques

Lorsqu'un ordinateur possède une interface connectée à Internet (modem, câble...), celle-ci doit obligatoirement posséder une adresse IP publique afin de pouvoir communiquer. Cela comprend toutes les adresses disponibles, sauf les plages réservées aux adresses [privées](#) mentionnées ci-dessus.

D

DHCP

Dynamic Host Control Protocol. [Protocole](#) utilisé par les serveurs DHCP comme celui de WinGate pour attribuer automatiquement les paramètres Internet ([adresse IP](#), serveur [DNS](#) et [passerelle](#) par défaut) aux postes clients. Cela simplifie l'administration des réseaux car il n'est pas nécessaire de configurer chaque poste manuellement.

DNS

Domain Name System. DNS protocole permettant de convertir des noms d'hôtes, c'est à dire des URL (www.abc.com) ou noms de domaines (qbik.com) en adresses IP afin d'accéder plus facilement aux sites requis.

Exemple :

Si vous saisissez dans votre navigateur une adresse telle que www.abc.com, le DNS identifie l'adresse IP correspondant à cette URL afin de pouvoir envoyer au

serveur une requête pour la page souhaitée.

En effet, il est plus simple de mémoriser une URL du type `www.abc.com`, qu'une adresse IP.

Domaine

Un domaine est un groupe d'ordinateurs ou de réseaux situés dans un même emplacement. Sur les réseaux privés, on utilise généralement des domaines NT ou Active Directory.

Sur Internet, un domaine (ou nom de domaine) désigne l'emplacement d'un site web ou d'un réseau (par exemple : `qbik.com` ou `wingate.com`). Il suffit généralement d'indiquer ce nom dans un navigateur pour accéder au domaine ou au site qu'il héberge.

Les domaines sur Internet sont répartis sur plusieurs niveaux, afin de faciliter leur identification. Les noms de domaine de premier niveau correspondent aux caractères situés après le dernier point de l'URL (par exemple : `.com`, `.net`, `.org`, etc.). Des noms de domaine tels que : `.fr`, `.es`, `.de`, `.it`, etc. permettent de déterminer le pays dans lequel est hébergé le site.

F

FAI

Fournisseur d'accès Internet. Les FAI sont connectés à Internet et proposent des connexions commutées ou directes à leurs clients. En règle générale, ils disposent de nombreux modems auxquels les utilisateurs peuvent se connecter à l'aide d'un compte PPP. La plupart d'entre eux proposent à présent des connexions permettant d'améliorer la vitesse, comme ISDN T1.

G

Groupe de travail

Réseau sur lequel chaque poste est responsable de ses propres ressources ainsi que de sa sécurité. Lorsqu'un utilisateur souhaite se connecter à un autre poste, son identité est vérifiée dans une base de données locale sur le poste concerné (contrairement aux domaines où la base de données d'utilisateurs est centralisée).

H

HTTP

Hyper Text Transfer Protocol. Protocole utilisé pour transmettre les ressources aux clients sur le [web](#). Ainsi, lorsqu'un navigateur effectue une requête pour une page, celle-ci est souvent sous la forme : `http://www.wingate.com`

I

Interface

Également appelée "connexion réseau", une interface est une carte ou un périphérique permettant à un ordinateur de communiquer avec d'autres. Cela inclut les modems et les connexions Internet telles que le câble, les modems DSL, les connexions RNIS...

Afin de pouvoir communiquer (via le protocole [TCP/IP](#)) toutes les interfaces réseau doivent posséder une adresse IP. Celle-ci peut être configurée manuellement (on parle alors d'adresse IP statique) ou bien attribuée automatiquement par un serveur DHCP (adresse IP dynamique).

Ipconfig

Petit utilitaire présent dans toutes les versions de Windows indiquant les détails de l'adresse IP actuellement utilisée par chaque interface. Il est généralement exécuté à l'aide de l'invite de commandes (pour en savoir plus, consultez l'aide de Windows).

L

Localhost

Adresse IP utilisée par le système d'exploitation pour "faire référence" à lui-même. Elle est toujours égale à 127.0.0.1.

En effectuant une requête ping sur cette adresse, vous pouvez ainsi vérifier que le protocole TCP/IP fonctionne correctement sur un poste.

P

Paquet

Les données transmises entre des ordinateurs sur un réseau TCP/IP sont fractionnées sous forme de "paquets". Un paquet de données est similaire à un "colis". Si vous souhaitez envoyer un colis à quelqu'un vous devez respecter certaines règles : indiquer le nom et l'adresse du destinataire et l'adresse de l'expéditeur, utiliser des timbres et un emballage. Cependant, le contenu du colis ne dépend que de vous. La transmission de paquets fonctionne de façon analogique.

Pare-feu

Dispositif destiné à protéger les ordinateurs possédant une interface réseau connectée à Internet contre les tentatives d'intrusion. Un pare-feu peut également être utilisé afin d'assurer la sécurité du trafic entre deux sous-réseaux.

En règle générale, les pare-feu bloquent les requêtes entrantes sur tous les [ports](#). En effet, les pirates utilisent souvent des programmes permettant d'analyser les ports et de déterminer ceux qui sont vulnérables (ouverts ou acceptant des connexions entrantes).

Si vous ne possédez pas de pare-feu, les ports ouverts sont très vulnérables lorsque votre ordinateur est connecté à Internet.

La plupart des pare-feu ouvrent automatiquement les ports nécessaires lorsque les clients effectuent des requêtes et les referment une fois les sessions

terminées.

Passerelle

Dans un réseau TCP/IP, la passerelle (ou passerelle par défaut) correspond à l'adresse IP du poste possédant une interface externe. La passerelle possède habituellement deux interfaces réseau : une interface interne (connectée au réseau local) et une interface externe.

Pilote

Programme associé à un périphérique et indiquant son emplacement et son fonctionnement au système d'exploitation.

Ping

Utilitaire inclus dans Windows et destiné à tester la connectivité sur un réseau (pour en savoir plus, consultez l'aide de Windows ou [cliquez ici](#)).

Port

Canal de communication d'un ordinateur. Les paquets de données ne sont pas seulement adressés à un ordinateur, ils sont destinés à un port spécifique. Le principe est comparable à celui d'un poste de radio, à la différence qu'un ordinateur peut écouter chacun des 65000 canaux possibles en même temps ! En termes plus techniques, un port est une connexion logique TCP/IP. En effet, les programmes utilisant ce protocole doivent utiliser un port pour communiquer avec un autre programme ou un ordinateur. Par exemple, pour afficher une page web, votre navigateur envoie une requête au serveur sur le port 80.

[Cliquez ici pour une liste des ports les plus fréquemment utilisés.](#)

Protocole

Ensemble de règles et de spécifications devant être respectées par les fabricants de matériel informatique et les développeurs de logiciels afin que tous les

produits puissent communiquer entre eux.

Il existe de nombreux protocoles, à tous les niveaux de communication. Les principaux protocoles réseau sont : TCP, IP, UDP, DHCP, NETBIOS et DNS.

[Cliquez ici pour une liste des protocoles les plus fréquemment utilisés.](#)

Proxy

Proxy signifie littéralement "mandataire", c'est à dire une personne effectuant une action au nom d'une autre personne (le terme "serveur mandataire" est d'ailleurs parfois utilisé). Ainsi, WinGate est un programme effectuant des actions (requêtes Internet) au nom d'autres programmes (clients).

Avec un serveur proxy tel que WinGate, toutes les connexions Internet du réseau local sont effectuées à l'aide de [l'adresse IP publique](#) du poste WinGate, ce qui assure une sécurité maximale pour les postes clients.

R

Routeur

Périphérique ou logiciel effectuant la liaison entre deux réseaux différents. Afin de pouvoir assurer cette liaison, le routeur possède une interface connectée à chaque réseau. Par conséquent, le terme "passerelle" est parfois employé.

Les routeurs sont souvent utilisés pour partager une connexion Internet dans un réseau local. Dans ce cas, ils possèdent une interface avec une adresse IP privée (connectée au réseau local) et une interface avec une adresse IP publique (connectée à Internet).

WinGate peut être configuré afin de jouer le rôle de routeur entre deux sous-réseaux.

S

Sous-réseau

Partie d'un réseau constituée d'un groupe d'ordinateurs partageant la même plage d'adresses IP.

Les masques de sous-réseau sont utilisés en association avec l'adresse IP afin de distinguer quelle partie de l'adresse désigne le sous-réseau et quelle partie désigne l'ordinateur.

Le fonctionnement des masques de sous-réseau est assez complexe, mais il peut se résumer de la façon suivante : chacun des 4 octets d'un masque de sous-réseau correspond à un octet de l'adresse IP.

Exemple :

192.168.4.1

255.255.255.0

T

TCP/IP

Transmission Control Protocol/Internet Protocol.

TCP/IP désigne communément un ensemble de [protocoles](#) permettant la communication entre les différents postes des réseaux (y compris sur Internet). Le TCP/IP est installé par défaut avec Windows à partir de Windows 98.

TCP (Transmission Control Protocol)

Protocole le plus fréquemment utilisé pour assurer les communications dans les réseaux TCP/IP. Lorsque deux ordinateurs établissent une connexion à l'aide de ce protocole, il permet d'en assurer le bon déroulement. En effet, chaque poste vérifie que les données ont été correctement reçues par l'autre partie et lorsque la session est terminée, un signal est envoyé indiquant que la connexion peut être arrêtée.

UDP (User Datagram Protocol)

Protocole également utilisé dans les réseaux TCP/IP. Contrairement au TCP, le protocole UDP est non orienté connexion : il ne garantit pas que les paquets atteignent leur destination.

IP (Internet Protocol)

Assure le transport des sessions TCP et UDP et les "dirige" d'un point à un autre.

U

URL

Uniform Resource Locator. Format standard permettant d'indiquer l'emplacement d'une ressource sur Internet. Par exemple : <http://www.qbik.com/index.html> signifie que l'on utilise le protocole HTTP pour se connecter au serveur www.qbik.com afin de consulter le document [index.html](http://www.qbik.com/index.html).

W

WinSock

Windows Sockets. Partie de Windows fournissant les Sockets pour le TCP/IP.

WWW

World Wide Web. Ensemble des millions de serveurs fournissant des pages web et autres ressources par le biais du protocole HTTP.

©2005 Qbik New Zealand Limited

Protocoles et ports fréquemment employés

De nombreux protocoles existent afin de permettre aux applications de communiquer entre elles. Pour cela, elles doivent "écouter" le trafic sur un port spécifique. Par exemple, pour envoyer un e-mail, le client de messagerie envoie une requête au serveur à l'aide du protocole SMTP sur le port 25.

Le tableau ci-dessous décrit les principaux protocoles utilisés dans les communications TCP/IP.

Protocole	Port	TCP/UDP	Description
HTTP	80	TCP	Hypertext Transfer Protocol. Envoi et réception de pages web et autres ressources sur Internet. Protocole utilisé par quasiment tous les navigateurs pour surfer sur Internet.
FTP	21	TCP	File Transfer Protocol. Transferts de fichiers sur Internet.
SMTP	25	TCP	Simple Mail Transfer Protocol. Envoi d'e-mails. La plupart des serveurs de messagerie l'utilisent pour envoyer les messages de leurs clients.
POP3	110	TCP	Post Office Protocol. Troisième version du protocole POP, utilisé pour la réception d'e-mails.
Telnet	23	TCP	Utilisé pour établir des connexions d'administration à distance avec d'autres serveurs Telnet sur Internet.

DNS	53	UDP	Domain Name Service. Conversion d'URL ou noms de domaine en adresses IP.
DHCP	67	UDP	Dynamic Host Control Protocol. Attribution automatique des adresses IP et paramètres Internet aux postes d'un réseau.
SSL	443	TCP	Secure Sockets Layer. Sécurisation du trafic HTTP. Utilisé par exemple pour sécuriser les paiements par carte bancaire.
SOCKS	1080	TCP	SOCKEt Secure. Protocole utilisé par de nombreuses applications TCP/IP pour communiquer par le biais d'un proxy/pare-feu.
RDP	3389	TCP	Remote Desktop Protocol. Administration d'ordinateurs à distance.

©2005 Qbik New Zealand Limited

Installation : sélection du répertoire d'installation



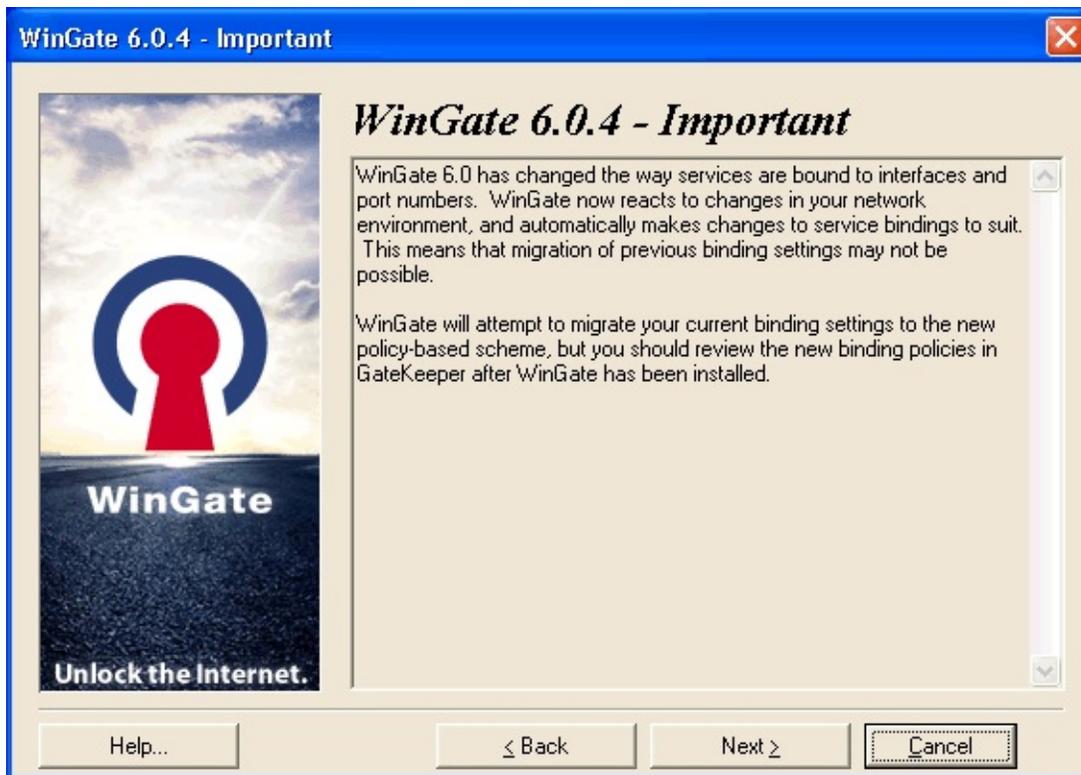
Il s'agit du répertoire dans lequel les fichiers exécutables et ressources de WinGate sont installés.

Répertoire par défaut : **C:\Program Files\Wingate**

Vous pouvez choisir un autre emplacement, à condition qu'il se trouve sur un disque local du serveur WinGate. Le programme d'installation indique l'espace disponible sur le disque.

©2005 Qbik New Zealand Limited

Installation : important



WinGate détecte à présent automatiquement les interfaces réseau et les classe automatiquement en fonction de leur adresse IP en tant qu'interface :

Interne

Interface possédant une adresse IP privée (sauf si WinGate se trouve derrière un routeur NAT), utilisée par les services proxy pour écouter les requêtes des clients sur le réseau local.

Externe

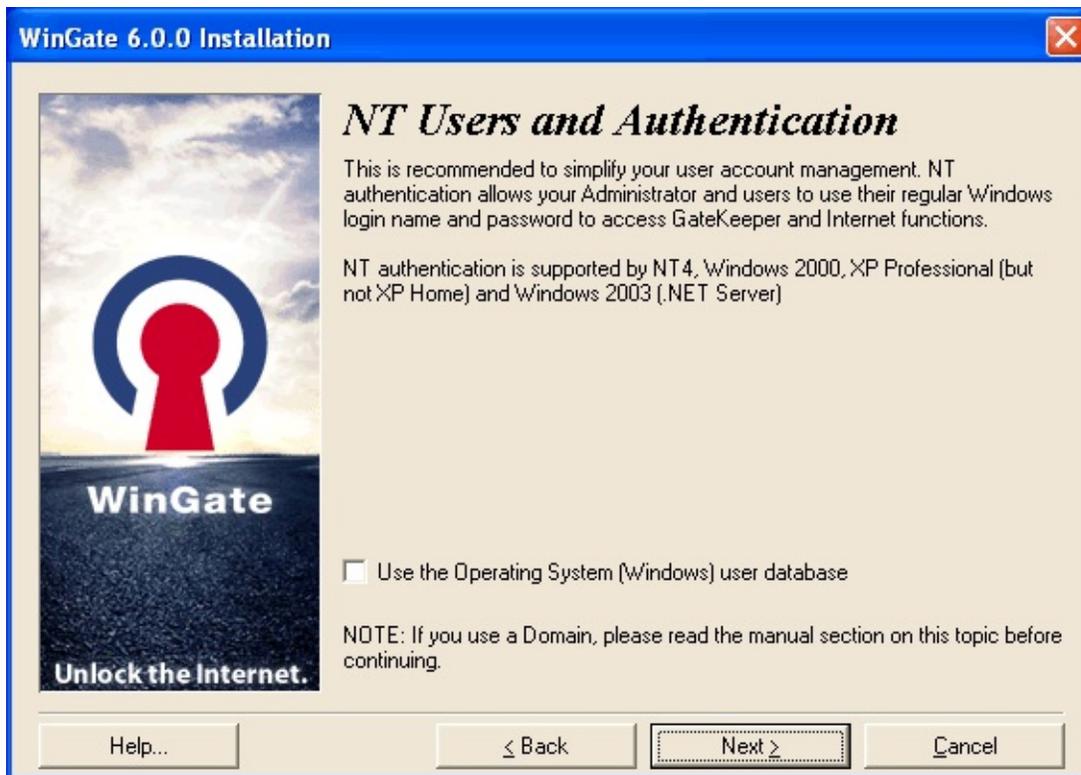
Interface possédant une adresse IP publique et donc considérée comme connexion Internet, utilisée pour exécuter les requêtes des clients.

Si vous effectuez une mise à jour, vérifiez que les interfaces réseau soient correctement liées aux services.

Pour en savoir plus sur la gestion des connexions réseau dans WinGate, consultez le fichier d'aide.

©2005 Qbik New Zealand Limited

Installation : utilisateurs NT et authentification



Cet écran s'affiche si vous installez WinGate sous Windows NT, 2000, XP Pro, ou .NET Server.

Si vous sélectionnez l'option **Utiliser la base de données du système d'exploitation (Windows)** les utilisateurs et groupes créés dans WinGate seront synchronisés avec votre base de données NT/2000/XP.

La gestion des utilisateurs est facilitée.

Vous bénéficiez de l'authentification NT.

Remarque :

Cette option n'est pas disponible sous Windows 95, 98 et Millénium.

©2005 Qbik New Zealand Limited

WinGate Installation : e-mail



Cette option, cochée par défaut, permet d'utiliser le serveur de messagerie de WinGate.

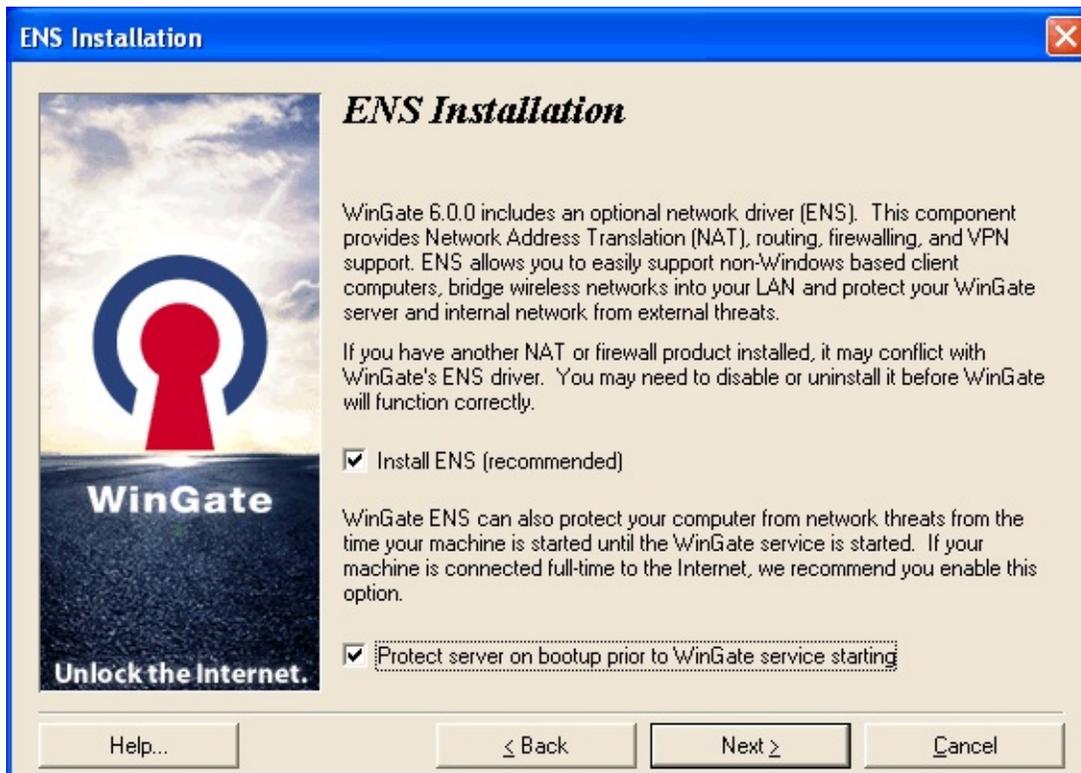
Si elle n'est pas cochée, les serveurs SMTP et POP3 ne seront pas démarrés après l'installation.

Remarque :

Si votre licence le permet, vous pouvez utiliser le serveur de messagerie aussitôt après avoir installé WinGate.

©2005 Qbik New Zealand Limited

Installation : ENS (Extended Network Services)



Ce service fournit entre autres le NAT (Network Address Translation) et le pare-feu. Il est donc recommandé de l'installer.

Avec le NAT, vous partagez votre connexion Internet avec les postes clients quelles que soient l'application et la plateforme utilisées (Windows, MacOS, Unix et Linux).

Si vous utilisez le service DHCP, cela ne requiert AUCUNE configuration spécifique.

Protéger le serveur avant le démarrage du service WinGate (*Protect server on bootup prior to WinGate service starting*)

Protège votre connexion Internet dès le démarrage du serveur.

©2005 Qbik New Zealand Limited

Installation : mises à jour automatiques



Cette option, activée par défaut, recherche automatiquement les mises à jour disponibles.

Vous pouvez la désactiver à tout moment dans GateKeeper.

©2005 Qbik New Zealand Limited

Installation : activation de WinGate



Il est à présent obligatoire d'activer le logiciel avant de pouvoir l'utiliser.

Si vous effectuez la mise à jour d'une licence non activée, vous devrez également effectuer cette opération.

Toutefois, toutes les licences (y compris les versions d'évaluation 6.0) peut être activées après l'installation du logiciel.

A partir de la version 6.0, WinGate affiche un message indiquant que vous devez activer une licence (d'évaluation ou complète) pour bénéficier des fonctionnalités du logiciel.

Remarque :

Vous ne pouvez utiliser qu'une licence par installation. Si vous devez migrer WinGate sur un autre poste, la licence sera désactivée lors de la désinstallation.

Procédé d'activation

Cliquez sur le bouton **Activer (Activate)**.

Ancienne licence (non activée)

1. Surlignez la licence.
2. Cliquez sur le bouton **Activer (Activate)**.
3. Une fois l'opération effectuée, vous devrez redémarrer le moteur de WinGate.

Requête d'une nouvelle licence d'évaluation

1. Cliquez sur **Ajouter (Add New)**.
2. Cochez l'option "**Request trial for any product...**".
3. Sélectionnez **WinGate** dans le menu déroulant.
4. Cliquez sur **next** pour activer la licence d'évaluation.
5. Une fois l'opération effectuée, vous devrez redémarrer le moteur de WinGate.

©2005 Qbik New Zealand Limited

Installation : début de l'installation



Commence la copie des fichiers sur votre ordinateur et la création d'entrées dans le registre.

WinGate étant installé en tant que service, il démarre dès l'installation terminée.

©2005 Qbik New Zealand Limited

Installation : installation terminée



Indique que l'installation de WinGate est terminée et fournit des informations sur ses modules additionnels :

PureSight

Filtre de contenu permettant aux administrateurs de contrôler les droits d'accès des clients aux sites sensibles (par exemple pornographiques).

Kaspersky AntiVirus for WinGate

Logiciel d'analyse antivirus. Améliore la sécurité sur votre réseau.

Lorsque vous cliquez sur Terminer (*Finish*), une **boîte de dialogue** vous propose

de redémarrer l'ordinateur. Cette opération doit être effectuée avant la première utilisation de WinGate.

©2005 Qbik New Zealand Limited

Méthodes de connexion : WinGate Internet Client (WGIC)

WinGate Internet Client est un logiciel indépendant à installer sur chaque ordinateur du réseau, à l'exception du serveur qui possède GateKeeper.

Lorsque WGIC est installé sur un poste client, toutes les requêtes provenant d'applications [WinSock](#) (la plupart des programmes fonctionnant sous Windows) sont interceptées par WinGate. Les administrateurs contrôlent ainsi de façon efficace les applications utilisées par les clients pour accéder à Internet.

Avantages

Permet de contrôler efficacement l'utilisation d'Internet et d'exécuter des applications du serveur.

Possibilité d'exiger l'authentification des utilisateurs souhaitant accéder à Internet. Il peut être configuré de façon à demander l'authentification d'un utilisateur la première fois qu'il accède à Internet (ce qui permet de surveiller l'activité).

Permet de contrôler les politiques de façon centralisée dans WinGate (service WRP).

Avec WinGate Enterprise, l'accès Internet et les opérations des utilisateurs de WGIC peuvent être contrôlés depuis GateKeeper.

Le programme d'installation étant au format MSI, WGIC peut être installé de façon automatique sur les postes des domaines Active Directory.

Inconvénients

Il est nécessaire de l'installer sur chaque poste client.

Ne fonctionne que sous Windows.

Conclusion

Nous vous recommandons d'utiliser WGIC si vous possédez un réseau LAN de clients Windows de petite ou moyenne taille et souhaitez contrôler l'utilisation

d'Internet.

[Cliquez ici pour retourner à l'étape 3](#)

©2005 Qbik New Zealand Limited

Méthodes de connexion : proxy

Cette méthode consiste à configurer chaque application sur le poste client (navigateur, client de messagerie, messagerie instantanée...) pour qu'elle accède à Internet par le biais des services proxy de WinGate.

La plupart des programmes fonctionnant avec le TCP/IP possèdent une option permettant d'utiliser un serveur proxy dans laquelle vous devez indiquer le nom ou l'adresse IP du serveur WinGate.

Les services proxy de WinGate (HTTP, FTP, Telnet...) servent à contrôler les connexions entre les applications clientes et les serveurs sur Internet.

Avec l'essor de WinGate Internet Client (système WRP) et du système NAT, les proxies sont de moins en moins employés.

Vous pouvez toutefois choisir de les utiliser pour exercer un contrôle par service sur les politiques. Mais depuis l'apparition de la [redirection transparente](#), toutes les fonctionnalités des proxies sont également disponibles avec les deux autres méthodes.

Avantages

Permet de contrôler au mieux les données circulant dans votre réseau. Toutefois, avec la redirection transparente, ces avantages sont également possibles avec le NAT et WGIC.

Inconvénients

Ne fonctionne qu'avec les protocoles déjà existants. Si un nouveau protocole apparaît, vous ne pouvez pas l'utiliser car il n'y aura pas de service correspondant dans WinGate.

[Cliquez ici pour retourner à l'étape 3](#)

©2005 Qbik New Zealand Limited

Méthodes de connexion : NAT

Cette méthode est la plus simple à configurer et à utiliser.

Les clients envoient les requêtes Internet à WinGate, qui se connecte à son tour au serveur concerné. Lors de cette opération, il remplace l'adresse IP d'origine par son adresse publique, de telle sorte que la requête semble provenir directement de WinGate.

Puis, lorsque le serveur distant envoie à WinGate les données requises, il remplace son adresse par celle du poste ayant émis la requête afin qu'il reçoive ces informations. Tout cela s'effectue de façon transparente pour les postes clients.

Avantages

Permet le partage d'une connexion Internet de façon rapide, sûre et continue. Il s'agit de la méthode la plus simple, car toutes les requêtes passent par WinGate, quelle que soit l'application utilisée.

Très flexible : permet de partager une connexion Internet sur toutes les plateformes utilisant le TCP/IP (Windows, Mac, Unix, Linux), contrairement à WinGate Internet Client qui ne fonctionne que sous Windows.

Toutes les requêtes passant par le poste WinGate, elles peuvent être envoyées depuis n'importe quelle application cliente utilisant le TCP/IP (navigateurs, clients de messagerie, de nouvelles, clients FTP...) sans aucune configuration supplémentaire.

Il n'est pas nécessaire d'installer de logiciel supplémentaire ou de configurer les applications.

Grâce à la redirection transparente, le NAT s'intègre facilement avec les services proxy de WinGate.

Inconvénients

Comme ce système fonctionne en tant que pilote de bas niveau, il peut y avoir des problèmes de compatibilité en fonction du matériel.

Le NAT ne permet pas de contrôler les clients utilisant WGIC, ou exécutant des applications directement à l'aide des proxies de WinGate. Ce problème peut toutefois être limité à l'aide de la redirection transparente.

Conclusion

Pour de nombreux utilisateurs, le NAT est la solution idéale. Il convient particulièrement aux réseaux LAN possédant différentes plateformes (Windows, Mac, Unix, Linux) et où l'administrateur ne veut pas être obligé d'installer de logiciels supplémentaires et/ou de configurer des applications sur plusieurs ordinateurs.

[Cliquez ici pour retourner à l'étape 3](#)

Configuration des clients avec WinGate Internet Client (WGIC)

Avant de procéder à l'installation de WGIC, installez le serveur WinGate, assurez-vous que le service WRP fonctionne et soit activé, et que les ordinateurs clients répondent aux exigences suivantes :

Système d'exploitation : Windows 95, 98, NT4, 2000 ou XP

Le serveur WinGate ne se trouve pas sur cet ordinateur

Si l'ordinateur fonctionne sous Windows 95, vous devez installer [WinSock 2](#)

Programme d'installation

Si l'ordinateur répond aux critères ci-dessus, vous pouvez installer WGIC.

1. Exécutez l'un des deux fichiers suivants sur le poste client :
 - **Wingate.exe**
(également utilisé pour l'installation du serveur)
ou
 - **WGIC.msi** (programme d'installation du client se trouvant dans le dossier WinGate\Client sur le poste serveur)
2. Le programme détecte le serveur et vous propose d'installer le client. Dans le cas contraire, vous devez le préciser.

La procédure d'installation est très simple, et il n'est pas nécessaire de redémarrer l'ordinateur lorsqu'elle est terminée.

Tout comme le serveur, WGIC fonctionne en tant que service Windows. Cela signifie qu'il est toujours actif, même si vous n'êtes pas connecté. Pour en modifier la configuration, exécutez l'applet WGIC se trouvant dans le [Panneau de configuration](#).

Configuration des applications

Une fois l'installation terminée, aucune configuration n'est nécessaire : vos applications peuvent se connecter à Internet (à condition que le service WRS soit actif sur le serveur). WGIC leur fournit un accès continu.

Si vous utilisiez des proxies avant d'installer WGIC, nous vous recommandons d'en supprimer les paramètres. En effet, vos applications doivent être configurées pour se connecter **directement** à Internet.

Si vous ne supprimez pas ces paramètres, vos applications fonctionneront, mais par le biais des proxies de WinGate et non de WGIC.

[Cliquez ici pour retourner à l'étape 3](#)

Configuration des clients avec la méthode proxy

Pour que les ordinateurs clients se connectent à l'aide de la méthode proxy, vous devez configurer l'application choisie sur l'ordinateur client pour qu'elle soit dirigée vers WinGate (en indiquant l'adresse IP privée du serveur WinGate et le numéro de port du service proxy). Pour plus d'informations, reportez-vous à la documentation de l'application utilisée.

Remarque :

Les applications configurées pour employer cette méthode seront connectées au service proxy correspondant. Les autres méthodes (NAT et WGIC) ne seront pas utilisées, même si elles fonctionnent sur le poste client.

Depuis l'introduction du **NAT** et de la [redirection transparente](#) dans WinGate, il n'est presque plus nécessaire d'utiliser de proxy de façon directe.

[Cliquez ici pour retourner à l'étape 3](#)

Comment tester le TCP/IP ?

La requête "ping" est un utilitaire couramment utilisé permettant de vérifier de façon simple et rapide si un autre ordinateur est en ligne. Cela consiste à envoyer un message composé de quatre paquets ICMP à l'adresse IP ou au nom de domaine à tester. Si l'autre ordinateur est en ligne et en mesure de répondre, il renvoie les mêmes paquets.

En cas d'échec, vous pouvez vérifier si des erreurs se sont produites dans l'Observateur d'évènements.

Tester le poste local

Si vous souhaitez vous assurer que le TCP/IP fonctionne correctement sur votre ordinateur, il suffit d'envoyer une requête ping sur votre adresse loopback (127.0.0.1). En cas d'échec, assurez-vous que le TCP/IP soit installé et correctement configuré.

Tester un ordinateur du réseau

(a) Le serveur WinGate

Dans l'invite de commandes, saisissez :

ping 192.168.0.1 (en remplaçant 192.168.0.1 par l'adresse IP de votre serveur).

Vous devriez obtenir pour chaque ordinateur de votre réseau une réponse du type :

Envoi d'une requête ping sur [192.168.0.1] avec 32 octets de données

Réponse de 192.168.0.1: octets=32 temps < =10ms TTL=32

Cela confirme que le TCP/IP fonctionne correctement entre le client et le serveur. Vous pouvez ensuite le paramétrer.

Remarque :

Si la réponse est du type :

Impossible de joindre l'hôte de destination

ou

Mauvaise IP,

vérifiez les paramètres du TCP/IP.

(b) Un ordinateur sur Internet

Remarque :

Cela ne fonctionnera que si WinGate est installé sur votre réseau (car le service DNS est nécessaire à la résolution des URL en adresses IP).

Dans l'invite de commandes, saisissez :

```
ping www.cnn.com (ou tout autre site fiable)
```

Vous devriez obtenir pour chaque ordinateur de votre réseau (sauf le serveur WinGate) une réponse du type :

```
Envoi d'une requête ping sur cnn.com [207.25.71.29] avec 32 octets de données  
Délati d'attente de la demande dépassé.  
Délati d'attente de la demande dépassé.  
Délati d'attente de la demande dépassé.  
Délati d'attente de la demande dépassé.
```

Si vous avez défini une passerelle par défaut, avec par exemple l'adresse IP 192.168.0.4, la réponse doit être :

```
Envoi d'une requête ping sur cnn.com [207.25.71.29] avec 32 octets de données  
Réponse de 192.168.0.4: Impossible de joindre l'hôte de destination.  
Réponse de 192.168.0.4: Impossible de joindre l'hôte de destination.  
Réponse de 192.168.0.4: Impossible de joindre l'hôte de destination.  
Réponse de 192.168.0.4: Impossible de joindre l'hôte de destination.
```

Cela signifie que le service DNS de WinGate fonctionne correctement : il a identifié l'IP correspondant au nom d'hôte. Lorsque la requête ping est envoyée à un ordinateur distant (sur Internet) depuis un client WinGate, le temps de réponse n'est jamais indiqué.

©2004 Qbik New Zealand Limited

Configuration des clients avec la méthode NAT

La procédure est très simple.

1. Sur chaque poste client, dans le **Panneau de configuration**, double-cliquez sur **Connexions réseau**.
2. Effectuez un clic droit sur l'icône **Connexion au réseau local** puis cliquez sur **Propriétés**.
3. Sélectionnez **Protocole Internet (TCP/IP)** puis cliquez sur le bouton **Propriétés**.

Remarque :

Le nom de l'adaptateur figure en haut de la fenêtre **Propriétés de Connexion au réseau local**, ce qui vous permet de vous assurer qu'il s'agit bien de l'interface souhaitée.

4. Indiquez l'adresse IP privée de WinGate dans le champ **Passerelle par défaut**.
5. Dans le champ **Serveur DNS préféré**, indiquez également l'adresse IP de WinGate.
6. Cliquez sur **OK** dans toutes les fenêtres ouvertes afin d'enregistrer les modifications.

Si vous ne souhaitez pas configurer manuellement chaque poste, ces paramètres peuvent être attribués automatiquement par le serveur DHCP.

Pour cela :

1. Ouvrez **GateKeeper**
2. Double cliquez sur le **Service DHCP (DHCP Service)** dans l'onglet **Système**.
3. Cliquez sur l'icône **Mode DHCP (DHCP Modes)** et assurez-vous que

l'option **Entièrement automatique** (*Fully Automatic*) soit cochée.

4. Cliquez sur **OK** pour enregistrer les modifications.

Ainsi, il n'est pas nécessaire de configurer les postes clients pour qu'ils se connectent à WinGate à l'aide du NAT.

[Cliquez ici pour retourner à l'étape 3](#)

Redirection transparente

Elle permet d'intercepter les requêtes destinées aux serveurs : web (port par défaut : 80), POP3 (port par défaut : 110), de fichiers journaux (port 8010) ou Telnet (port par défaut : 23). Ces requêtes sont ensuite dirigées vers le service correspondant, quelle que soit la méthode de connexion du client (WGIC, le NAT ou bien les proxies).

Le numéro de port contenu dans une requête permet à WinGate de déterminer vers quel service elle doit être dirigée.

Lorsque cette fonctionnalité n'était pas disponible, il était nécessaire de configurer les paramètres proxy des applications clientes sur chaque poste afin de pouvoir utiliser les services de WinGate.

Pour utiliser la redirection transparente :

1. Ouvrez GateKeeper.
2. Connectez-vous à l'aide du compte **Administrator**.
3. Ouvrez le service pour lequel vous souhaitez activer cette fonctionnalité.
4. Cliquez sur l'icône [Sessions](#).
5. Cochez l'option **Intercepter les connexions NAT, WGIC, ou SOCKS sur les ports suivants** (*Intercept connections made via ENS, the WinGate Client, or SOCKS server on the following ports*)
6. Cliquez sur **Ajouter (Add)**.
7. Dans la fenêtre qui s'affiche ensuite, assurez-vous que l'option **Activer l'interception (Interception enabled)** soit cochée et que le numéro de port soit indiqué (il s'agit généralement du même port que le service).
8. Cliquez sur **OK**.

Principaux avantages :

Avec PureSight for WinGate

Ce filtre de contenu utilise une technologie basée sur l'intelligence artificielle, qui consulte le contenu des sites et bloque l'accès si nécessaire. Cette solution fonctionne en association avec le serveur proxy web. Par conséquent, si les clients se connectent à l'aide de WGIC ou du NAT, il est essentiel que la redirection transparente soit activée sur ce serveur..

Avec Kaspersky AntiVirus for WinGate

Face au nombre croissants de menaces, il est à présent indispensable de posséder une solution bloquant les virus à tous les niveaux. Kaspersky AntiVirus for WinGate, développé par Kaspersky Labs est une solution efficace et sûre. Ce module fonctionne au niveau des proxies, c'est pourquoi la redirection transparente doit être activée si les clients se connectent à l'aide de WGIC ou du NAT.

Gestion des politiques simplifiée

Lorsque cette fonctionnalité est activée sur le service web, il est possible d'exiger l'authentification Java, quelle que soit la méthode de connexion du client. Ainsi, les droits et restrictions concernant l'utilisation d'Internet peuvent être créés dans la politique du proxy web pour tous les utilisateurs et groupes.

Installation de Winsock 2

Winsock 2 n'est pas installé dans certaines versions de Windows 95 (il est intégré dans les versions ultérieures de Windows).

Il doit être présent sur votre ordinateur avant de procéder à l'installation de WinGate.

WinSock 2 offre une fonctionnalité réseau particulière à vos applications. Vous pouvez le télécharger gratuitement sur le site web de Microsoft (www.microsoft.com).