



WinGate

Solution complète de gestion Internet pour Windows

Bienvenue et merci d'avoir choisi **WinGate 6.1** !

WinGate 6.1 comprend de nombreuses fonctionnalités destinées à faciliter votre utilisation d'Internet, aussi bien en termes de sécurité que de coût et de gestion.

WinGate est un logiciel flexible : vous pouvez vous adapter à un nombre croissant d'utilisateurs sans devoir y consacrer trop de temps ni avoir recours à des techniciens qualifiés.

[Cliquez ici pour en savoir plus sur les fonctionnalités WinGate](#)



©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.

Présentation de WinGate 6.1

Merci d'avoir choisi **WinGate 6.0** par **Qbik New Zealand Ltd** !

WinGate 6.0 comprend de nombreuses fonctionnalités destinées à faciliter votre utilisation d'Internet, aussi bien en termes de sécurité que de coût et de gestion.

WinGate est un logiciel flexible : vous pouvez vous adapter à un nombre croissant d'utilisateurs sans devoir y consacrer trop de temps ni avoir recours à des techniciens qualifiés.

Quelles sont les applications de WinGate ?

Partage de connexions Internet

Lors de sa première publication en octobre 1995, WinGate était le premier proxy de partage de connexion Internet pour MS Windows. Il offrait la possibilité à plusieurs utilisateurs d'accéder à Internet par le biais d'une connexion unique. C'est à présent une solution de connectivité à la fois sophistiquée et simple d'utilisation.

Pare-feu

WinGate joue également le rôle de pare-feu au niveau des paquets : il protège votre réseau des attaques extérieures, et vous signale les risques potentiels. De plus, pour une meilleure flexibilité, il permet un contrôle efficace au niveau des protocoles.

Protection antivirus et filtre de contenu pour les connexions e-mail, web, et FTP

WinGate 6 est compatible avec divers modules additionnels d'analyse de données : PureSight for WinGate (filtre de contenu développé par PureSight Inc.), et Kaspersky AntiVirus for WinGate (solution antivirus de Kaspersky Labs). Vous pouvez ainsi analyser les messages reçus et distribués, les connexions Internet (y compris les téléchargements montants) et les transferts FTP. WinGate analyse même les messages reçus sur un serveur distant. Pour vous informer sur les nouveaux modules disponibles, consultez régulièrement le site Internet de WinGate.

Système de messagerie complet avec des mesures anti-spam avancées

WinGate comprend un serveur de messagerie complet (POP3 et SMTP), facile à configurer et sécurisé (support des connexions et méthodes d'authentification sécurisées). Il apporte également une protection efficace contre le spam. Alors que de nombreux serveurs de messagerie sont complexes et difficiles à gérer, celui de WinGate est à la fois simple, efficace, flexible, rapide et fiable. Il comprend à présent une nouvelle fonctionnalité de rejet des messages provenant d'une adresse usurpée (ce qui représente plus de 90% du spam).

Accès distant à un réseau à l'aide de WinGate VPN (Virtual Private Networking)

WinGate 6 dispose d'une solution VPN entièrement intégrée (licence séparée). Un utilisateur peut se connecter à distance à votre réseau afin de partager des fichiers, imprimer des documents, etc. Avec les licences WinGate VPN, vos utilisateurs pourront accéder aux ressources de votre réseau comme s'ils y étaient directement reliés, qu'ils soient chez eux ou en déplacement (les performances peuvent varier en fonction de la vitesse des connexions Internet). WinGate VPN se configure et s'utilise sans difficulté. C'est un logiciel sûr, flexible et fonctionnel.

Des possibilités infinies

De par sa structure flexible, WinGate peut être utilisé à des fins diverses : protection des services Internet vulnérables (serveurs extranet par exemple), administration automatique du réseau grâce au serveur DHCP : les possibilités sont multiples. N'hésitez pas à nous contacter si vous souhaitez que WinGate propose des fonctionnalités supplémentaires, nous ferons tout notre possible afin de les intégrer dans la prochaine version.

L'administration de WinGate s'effectue à l'aide de l'interface GateKeeper, qui affiche également en temps réel l'activité Internet sur votre réseau.



Qu'est-ce que WinGate ?

WinGate est une solution de connectivité Internet et de pare-feu permettant de partager une (ou plusieurs) connexion(s) Internet avec tous les ordinateurs d'un réseau. Il peut s'agir de quasiment n'importe quel type de connexion : commutée, ISDN, xDSL, modem câble, satellite, ou même T1. Avec WinGate, tous les ordinateurs de votre réseau peuvent accéder simultanément à Internet.

En partageant une seule connexion entre plusieurs ordinateurs, vous n'avez pas besoin d'ajouter de lignes téléphoniques, de souscrire des abonnements Internet supplémentaires, ni d'installer d'autres modems ou du matériel coûteux. Que ce soit pour une utilisation personnelle ou en entreprise, cette solution s'avère économique dès sa mise en œuvre.

WinGate comporte également un pare-feu intégré qui assure la protection de votre réseau contre les tentatives d'intrusion extérieures. Il peut aussi être utilisé dans des réseaux Intranets ou WAN d'entreprise.

Ce logiciel est constitué de différents composants : le moteur WinGate (fonctionne en tant que service sur le poste serveur, c'est à dire de façon "invisible") et GateKeeper (interface permettant de configurer WinGate). Le client WGIC (WinGate Internet Client) fournit l'accès au service WRS (Winsock Redirection Service) aux postes clients.

Après avoir installé WinGate et configuré les postes clients, vous pouvez surfer en toute liberté.

Termes employés

Ce fichier d'aide utilise fréquemment certains termes, dont voici la définition. Pour de détails, consultez le [glossaire](#).

Service Windows

Les services Windows sont des programmes qui s'exécutent dès le démarrage de Windows. Ils ne s'affichent généralement pas à l'écran, et ne s'arrêtent pas lorsqu'un utilisateur ferme sa session. (Par exemple : le programme qui permet à votre souris de fonctionner.)

Moteur WinGate

Il s'agit du composant exécutable de WinGate, fournissant les fonctionnalités du serveur (services WinGate permettant d'accéder à Internet). Il s'exécute de façon "invisible" en tant que service et se configure par le biais de GateKeeper.

Serveur WinGate

L'ordinateur sur lequel le logiciel WinGate est installé. Les autres postes de votre réseau accéderont à Internet via cet ordinateur, il doit donc posséder une connexion Internet.

Ordinateur client

Un ordinateur de votre réseau qui n'est pas connecté à Internet, mais qui y accède par le biais du serveur WinGate. Les ordinateurs clients sont souvent appelés "postes de travail"

GateKeeper

GateKeeper est le programme permettant de contrôler et configurer WinGate à distance. Il s'agit de l'interface utilisateur du moteur WinGate.

Nombre d'utilisateurs

Nombre maximum d'ordinateurs pouvant accéder simultanément à Internet par le biais de GateKeeper : 3, 6, 12, 25, 50, 100, 250, ou + de 250, en fonction de la licence achetée.

Type de licence

Standard, Pro, ou Enterprise.

Application cliente

Programme permettant d'effectuer certaines tâches, comme lire des e-mails ou consulter des pages web (par ex. : Netscape, Eudora etc.).

Serveur

Ordinateur ou programme fournissant un service spécifique (par ex. : serveur de messagerie, serveur web).

Proxy

Programme ou service qui agit pour le compte d'un autre. Intermédiaire entre clients et serveurs. [Cliquez ici pour en savoir plus.](#)

Client WinGate

Le client WinGate, WinGate Internet Client (WGIC) fournit l'accès au service Winsock Redirector Service, permettant aux applications clientes d'utiliser Internet comme si elles étaient directement connectées.

WGIC

WinGate Internet Client.

NAT

Network Address Translation (traduction d'adresses réseau).

ENS

Extended Network Support (Service réseau avancé).

TCP/IP

TCP/IP est un protocole réseau : les ordinateurs d'un réseau l'utilisent pour communiquer entre eux. Protocole le plus répandu sur Internet.

DNS

Domain Name Service. Service permettant de vérifier l'adresse d'un ordinateur sur Internet.

Adresse IP

IP signifie Internet Protocol (protocole Internet). Il s'agit de "l'adresse" d'un ordinateur sur un réseau. Le serveur DHCP de WinGate en attribue une à tous les ordinateurs clients.

Utilisateurs

Les comptes utilisateurs permettent de configurer des droits d'accès et un contrôle individuels. Vous pouvez en ajouter autant que nécessaire.

Groupe

Ensemble d'utilisateurs. Dans WinGate, un groupe peut être lui-même membre d'un autre groupe.

Droits d'accès

Peuvent être attribués à des utilisateurs ou des groupes.

localhost

"localhost" est le nom TCP/IP désignant l'ordinateur que vous utilisez. L'ordinateur utilise ce terme pour "faire référence" à lui-même. Il s'agit du nom que vous employez si vous utilisez un service se trouvant sur votre ordinateur (par ex. : lors de la première connexion à WinGate). L'adresse localhost n'est pas comptabilisée dans le nombre de postes autorisées. Son adresse IP est toujours 127.0.0.1

Interface

"Connexion réseau", c'est à dire la façon de se connecter à un autre ordinateur : carte réseau, profil de connexion, ou votre adresse loopback : localhost.

Liaison

Si un service est lié à une interface, il "écoute" cette dernière. Par défaut, les services de WinGate sont liés à toutes les interfaces.

FAI

Fournisseur d'accès Internet.

WRP

Winsock Redirection Protocol (protocole de redirection Winsock). Protocole utilisé par WGIC et WRS pour fournir les services de redirection Winsock.

WRS

Winsock Redirector Service (service de redirection Winsock).

©2004 Qbik New Zealand Limited

Fonctionnalités de WinGate

Service réseau avancé (*Extended Network Services*)

Le service réseau avancé offre des fonctions complètes aux utilisateurs de votre réseau : partage de l'accès Internet (basé sur NAT), sécurité du pare-feu et des ports et liaison entre plusieurs sous-réseaux (routage).

Redirection transparente

Intercepter le trafic du service réseau avancé et de WIGC permet aux utilisateurs de bénéficier des avantages d'un proxy, tels que la mise en cache et le contrôle avancé de l'accès, tout en profitant de la liberté de configuration offerte par ces deux services. Cette fonctionnalité s'active dans la fenêtre **Session** des services. Le proxy doit obligatoirement utiliser un port standard.

Serveur DNS

Le serveur DNS est un proxy entièrement fonctionnel, capable de gérer l'ensemble des requêtes émises par les clients. Sa fonctionnalité de cache augmente les performances de manière notable. En outre, il peut lire les fichiers de configuration système, les fichiers hosts et LMhosts. Compatible avec le serveur DHCP, le serveur DNS de WinGate autorise les résolutions DNS des noms d'ordinateur sur votre réseau.

Administration à distance avec GateKeeper

GateKeeper vous permet de configurer et de surveiller WinGate depuis n'importe quel emplacement sur Internet. GateKeeper communique avec WinGate via une connexion TCP/IP cryptée. Cette fonctionnalité est disponible dans le Service d'administration à distance (*Remote control service*) fourni avec la version Pro.

DHCP

Le DHCP automatise la configuration réseau des clients de votre réseau local. Disponible en mode manuel ou entièrement automatique, il configure les adresses IP et les DNS de tous vos postes clients.

GDP

Generic Discovery Protocol est un protocole qui détecte les serveurs Internet tels que WinGate. Il est utilisé par WinGate Internet Client (WGIC) et GateKeeper pour rechercher WinGate.

Composeur WinGate (*Dialer*)

Le composeur de WinGate se charge d'établir la connexion à Internet. Plusieurs comptes de fournisseurs d'accès à Internet (FAI) peuvent être configurés, et l'accès restreint par groupes d'utilisateurs, etc.

Journalisation et historique

Toutes les principales informations des services de WinGate sont conservées dans des fichiers journaux de type 'Nomduservice.log' que vous trouverez dans le dossier Program Files/WinGate/Logs (s'ouvrent à l'aide de n'importe quel éditeur de texte).

Icône du moteur de WinGate

Elle se trouve dans la zone de notification et indique si le moteur de WinGate est : en train de démarrer, actif, arrêté ou bien en train de s'arrêter.

Jeux en réseau

WinGate est compatible avec la plupart des jeux sur Internet.

Droits et restrictions

Des droits peuvent être attribués aux utilisateurs pour chaque service ou bien de façon globale. Il peuvent être définis pour chaque requête en fonction de l'utilisateur/groupe, l'emplacement, l'heure ou d'autres paramètres avancés.

Journalisation système

Cette fonctionnalité aide les administrateurs à diagnostiquer et à résoudre les éventuels problèmes se produisant dans WinGate ou sur le réseau.

[Service de redirection Winsock \(Winsock Redirector Service\)](#)

Fonctionne à l'aide du protocole WRP (Winsock Redirection Protocol). Avec ce protocole, quasiment toutes les applications clientes peuvent être exécutées comme si elles étaient directement connectées à Internet. Aucune configuration particulière n'est nécessaire : il suffit d'installer WGIC sur les postes clients. Dans les versions précédentes, chaque application devait être paramétrée manuellement pour fonctionner avec un proxy. (Même si cela n'est plus nécessaire, cette configuration fonctionne toujours).

[Proxy web](#)

Il s'agit d'un serveur proxy compatible avec HTTP/1.0 et possédant une fonction de cache HTTP. Il joue également le rôle de serveur web et supporte les requêtes HTTP et FTP ainsi que les tunnels SSL. Ses fonctionnalités incluent la capacité à gérer les requêtes non proxy, ce qui peut s'avérer utile si vous possédez déjà un serveur web sur votre réseau (vous pouvez ainsi le protéger derrière WinGate). Il peut également être mis en cascade avec un autre proxy ou un serveur SOCKS4.

[Gestion des requêtes non proxy](#)

De nombreux proxies de WinGate acceptent les requêtes non proxy, afin de pouvoir intégrer vos propres serveurs à WinGate de façon transparente et sans risque de conflits. Pour cela, WinGate peut rediriger automatiquement ces requêtes vers un autre serveur. Cela permet également d'en contrôler l'accès.

[Serveur SOCKS](#)

Compatible avec SOCKS 4 et SOCKS 5 (RFC 1928), il supporte la méthode d'authentification RFC1929 pour les utilisateurs de la base de données de WinGate. Ce serveur est capable d'intercepter les requêtes HTTP et de les transmettre au proxy web de WinGate. Ainsi, vos utilisateurs SOCKS bénéficieront des avantages du proxy web (par ex. : la mémoire cache) tout en étant soumis à la politique de ce service.

Proxy FTP

Fournit l'accès aux serveurs FTP, à l'aide de la méthode nomd'utilisateur@nomdedomaine. Il accepte les requêtes non proxy et peut être mis en cascade. De plus, il est possible d'analyser tout le trafic FTP à l'aide des modules additionnels.

Proxy POP3

Fournit l'accès aux serveurs POP3 (collecte du courrier). A l'instar des proxies web et FTP, il accepte les requêtes non proxy et peut être mis en cascade. Possibilité d'analyser tout le trafic POP à l'aide des modules additionnels.

Proxy Telnet

Fournit l'accès aux serveurs Telnet. Ce proxy est compatible avec de nombreux clients Telnet, y compris Unix. Il peut également être mis en cascade. Pour plus de sécurité, il est possible d'exiger l'authentification des utilisateurs.

Proxy RTSP

Le protocole RTSP (Real Time Streaming Protocol) s'utilise pour transférer des données (par exemple audio et vidéo) en temps réel. RealPlayer et QuickTime peuvent être configurés de façon à utiliser le proxy RTSP de WinGate.

Liens mappés

Solution de connectivité pour les applications TCP et UDP n'étant pas compatibles avec les protocoles proxy. Des fonctionnalités avancées permettent de créer des liens mappés en fonction de l'emplacement de l'utilisateur ou de son profil de connexion. Les liens mappés TCP supportent le cryptage "de bout en bout", afin de sécuriser les connexions de WinGate à WinGate sur Internet ou sur votre réseau.

PureSight

Module additionnel de WinGate, ce filtre de contenu est fondé sur la technologie

ACR (artificial content recognition) et bloque les requêtes contenant par exemple les termes "sexe" ou "casino", de façon redoutablement efficace. Il analyse pour cela le contenu des sites à l'aide d'algorithmes "intelligents".

Configuration automatique des proxies

WinGate est compatible avec cette fonctionnalité. Elle se configure dans Internet Explorer en cochant l'option **Détecter automatiquement les paramètres de connexion (Outils / Options Internet / Onglet Connexions / Paramètres réseau)**.

[Base de données d'utilisateurs](#)

Avec la base de données d'utilisateurs de WinGate, il est possible d'enregistrer l'activité de chaque utilisateur. Des droits d'accès peuvent être accordés par utilisateur ou par groupe et pour plus de commodité, un groupe peut être lui-même membre d'un autre groupe.

[Gestion des utilisateurs et authentification avec NT / 2000](#)

Possibilité d'intégrer des bases de données d'utilisateurs NT dans WinGate afin de bénéficier de l'authentification NT et d'une gestion simplifiée.

[Possibilité d'importer / exporter des comptes](#)

Les utilisateurs et groupes peuvent être importés et/ou exportés dans des fichiers texte.

[Authentification sécurisée](#)

De nombreuses méthodes d'authentification sécurisée sont disponibles.

[Support d'interfaces multiples](#)

WinGate peut utiliser plusieurs connexions Internet afin de bénéficier d'une bande passante plus importante et d'un accès plus rapide. Vous pouvez choisir des configurations alliant modem, ISDN et connexion directe pour chaque service.

Proxy VDOLive

Avec ce proxy vos utilisateurs peuvent consulter des vidéos en temps réel (streaming) à l'aide du lecteur VDOLive player de VDONet Corporation. Vous devez pour cela posséder une version qui soit compatible avec les proxies. Si vous possédez un serveur VDO sur votre réseau, vous pouvez le protéger derrière WinGate, car le proxy VDOLive accepte les requêtes non proxy.

Proxy XDMA

Permet le fonctionnement des clients Streamworks sur votre réseau.

©2004 Qbik New Zealand Limited

Proxies : informations générales

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). N'oubliez pas que le serveur proxy est le moteur de WinGate et non GateKeeper.

Exemple d'utilisation d'un proxy :

Un navigateur accède à Internet par le biais d'un serveur proxy (WinGate).

En règle générale, cela n'est pas visible pour l'utilisateur : il semble qu'il communique directement avec le serveur web. Cependant, la procédure est la suivante :

1. Le client se connecte à WinGate.
2. Il envoie une requête non proxy à WinGate (par ex. : "obtenir cette URL").
3. WinGate exécute la requête (si elle est autorisée) et se connecte au serveur correspondant.
4. WinGate envoie ensuite une requête modifiée au serveur, comme si elle provenait directement du navigateur.
5. Le serveur envoie le fichier à WinGate.
6. WinGate transmet le fichier au navigateur.

Les autres proxies de WinGate fonctionnent de la même façon : le client soumet une requête, WinGate l'évalue et l'exécute, et renvoie les données au client si nécessaire.

N'oubliez pas que lorsque vous accédez à Internet par le biais de WinGate, vous n'êtes jamais directement connecté aux ordinateurs extérieurs à votre réseau. Même si vous avez l'impression d'être connecté à Internet, les données proviennent de WinGate qui se connecte pour vous. Ainsi, tous les ordinateurs clients souhaitant se connecter à Internet se connectent en fait au serveur WinGate.

La plupart des applications peuvent indiquer au proxy à quel serveur il doit se

connecter (par ex. : Netscape, WS_FTP) mais certaines ne le peuvent pas (clients IRC, de nouvelles ...). Dans ce cas, vous devez configurer WinGate afin qu'il se connecte à un ordinateur spécifique à l'aide des liens mappés. Ils permettent de déterminer à l'avance sur quel serveur WinGate doit se connecter.

Certains logiciels clients détectent automatiquement les serveurs proxy, mais dans la plupart des cas, vous devrez indiquer l'adresse IP et le numéro de port du serveur de WinGate.

Remarque :

Avec WinGate Internet Client et le NAT, les proxies sont de moins en moins utilisés. Vous pouvez toujours choisir cette méthode afin de contrôler la politique par service. Toutefois, avec la [redirection transparente](#) tout ce qui peut être effectué avec les proxies peut également l'être avec le NAT ou WGIC.

Présentation du service NAT (Network Address Translation)

Deux ordinateurs se trouvant sur le même sous-réseau sont directement connectés : cela signifie que des données peuvent être transmises de l'un à l'autre. Or, s'ils sont situés sur des sous-réseaux différents, cela n'est plus possible car ils ne sont pas directement reliés.

Pour transférer des données entre deux sous-réseaux, on utilise un routeur (il peut s'agir d'un logiciel ou d'un dispositif matériel). Cette méthode est utilisée chaque fois que votre ordinateur essaie de se connecter à un autre sur Internet.

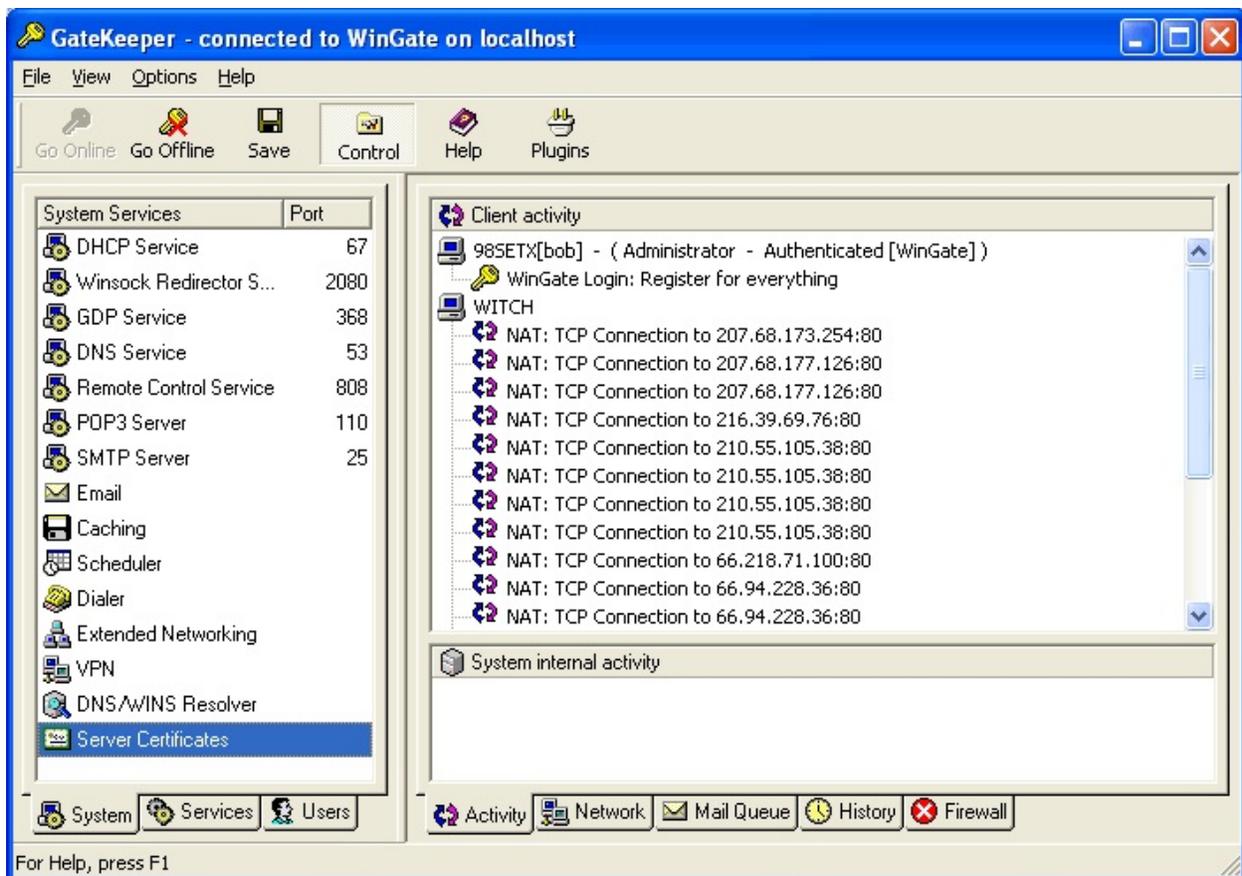
Le NAT est une approche de bas niveau du partage des connexions Internet. Il fonctionne de façon très similaire aux logiciels de routage (si l'on considère qu'Internet est un immense réseau formé de sous-réseaux multiples). Toutefois, une différence essentielle les sépare :

Les routeurs transfèrent les paquets à leurs destinataires car ils disposent de suffisamment d'informations concernant chaque sous-réseau.

Le NAT permet de partager une adresse IP publique unique entre plusieurs ordinateurs clients, chacun possédant sa propre adresse privée. Lorsqu'un client essaie de se connecter ou d'envoyer des données à un ordinateur sur Internet celles-ci sont transmises au NAT, qui remplace alors l'adresse IP privée d'origine du client par la sienne. Puis, l'ordinateur distant renvoie les paquets au poste sur lequel se trouve ce service (ici le serveur WinGate), car pour lui ce poste est l'expéditeur des données.

Le NAT enregistre sur quel port se connecte chaque ordinateur, ce qui lui permet de transférer ensuite les paquets à leurs destinataires.

[Cliquez ici pour voir l'activité du NAT dans GateKeeper](#)



Masquer | Masquer toutes les images

En résumé, le NAT effectue les tâches suivantes :

Remplace l'adresse IP d'origine par sa propre adresse. Ainsi, lorsqu'un ordinateur distant reçoit les données, elles semblent provenir du poste sur lequel se trouve le service NAT.

Enregistre le numéro de port utilisé lors de l'envoi de données.

Transfère au client les données provenant de l'ordinateur distant.

La configuration requise sur les postes clients est minime.

Le TCP/IP contient une passerelle par défaut. Le NAT joue simplement le rôle de passerelle et transfère les données destinées à Internet. Si vous utilisez le service DHCP de WinGate, la passerelle par défaut est configurée automatiquement.

Le NAT fonctionne-t-il avec toutes les applications ?

L'association du NAT et de la redirection transparente répond à quasiment tous les besoins en termes de connectivité sur Internet. Cependant, certaines applications ne permettent pas d'accéder à Internet avec WinGate. Vous trouverez des mises à jour concernant ces problèmes à l'adresse suivante : <http://forums.qbik.com>

Est-il compatible avec les logiciels serveurs ?

Le NAT est compatible avec la plupart des serveurs, à deux conditions :

Le serveur doit avoir une adresse IP statique.

Vous devez créer une redirection dans l'onglet [Sécurité des ports \(Port security\)](#) du service réseau avancé.

Ainsi, les connexions entrantes sont dirigées vers le serveur. Cependant, cette solution risque de ne pas fonctionner si plusieurs transferts de données sont en cours entre le serveur et le client. Les liens mappés sont plus performants.

Pourquoi est-il plus rapide que les autres solutions de connectivité ?

Car son fonctionnement est très simple : il doit simplement modifier quelques champs dans chaque paquet de données, et mémoriser les numéros de ports utilisés. Les autres méthodes sont beaucoup plus complexes.

Avec quels protocoles de transport fonctionne-t-il ?

Le NAT ne lit que les informations des paquets IP. Il est donc compatible avec les protocoles TCP, UDP et ICMP.

Le moteur de WinGate

Il fonctionne en tant que service de Windows et gère toutes les fonctionnalités de WinGate.

Comme tous les services, il s'exécute dès le démarrage de Windows (sauf en cas d'indication contraire).

Il n'est pas possible de le configurer. Pour modifier les paramètres de WinGate, vous devez utiliser GateKeeper.

Lorsqu'il est installé, une [icône](#) située dans la zone de notification indique son statut en temps réel.

Remarque :

Vous ne devriez modifier le fonctionnement de ce service que si vous utilisez l'option **Utiliser une base de données à distance** (*Use remote user database*) dans un environnement **Active Directory**.

([Cliquez ici pour en savoir plus](#))

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.

Elle indique l'état du moteur de WinGate. En effet, lorsque celui-ci est arrêté vous ne partagez plus votre connexion avec les postes clients.



Le service WinGate est actif.



Le service WinGate est arrêté.



Le service WinGate est en train de démarrer ou de s'arrêter.



Il y a un message système en attente.

En cliquant avec le bouton droit de la souris sur cette icône, vous disposez de différentes options :

Démarrer WinGate

Arrêter WinGate

Ouvrir GateKeeper

Présentation de GateKeeper

GateKeeper est l'interface permettant de contrôler et de configurer WinGate, par le biais d'un lien TCP/IP crypté. Toutefois, il n'est pas nécessaire d'utiliser GateKeeper pour accéder à Internet.



Masquer

Il peut être exécuté sur tous les ordinateurs possédant une connexion TCP/IP avec le serveur WinGate (le serveur WinGate lui-même, un poste de votre réseau, ou tout ordinateur connecté à Internet).

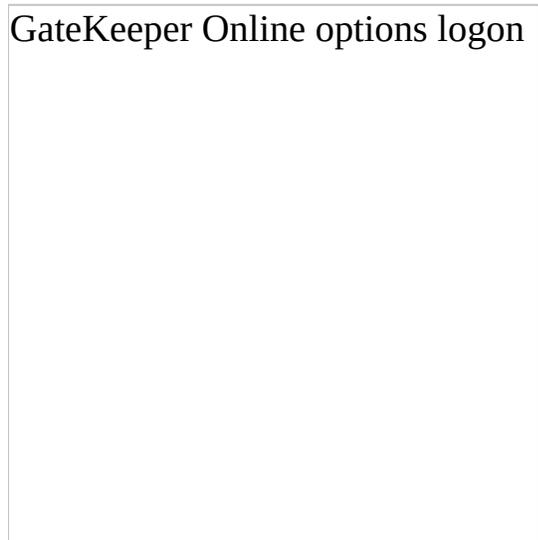
Il est formé d'une barre de menus et deux panneaux : panneau Contrôle et panneau Activité sur la droite).

1. [Panneau contrôle](#)
2. [Panneau activité](#)

Ces panneaux peuvent être ajustés et déplacés à votre convenance.

Authentification dans GateKeeper

Au démarrage de GateKeeper, la **fenêtre** suivante s'affiche :



Masquer | **Masquer toutes les images**

Détails du compte (Account Details)

Nom d'utilisateur (Username

)

Indiquez un nom d'utilisateur valide dans WinGate.

Mot de passe (Password)

Mot de passe correspondant. Laissez ce champ vide lors de votre première connexion à GateKeeper.

Utiliser l'identifiant Windows (Use current Windows login)

Cette option n'est disponible que si vous avez choisi d'utiliser la [base de données du système d'exploitation](#). Elle permet de vous connecter automatiquement, car WinGate utilise votre identifiant et mot de passe

Windows/NT.

Emplacement (WinGate location)

Serveur (Server)

Adresse IP du serveur WinGate

Port

Port utilisé par le [Service d'administration à distance \(Remote Control Service\)](#) pour l'accès à GateKeeper (par défaut : port 808).

Se connecter à l'ordinateur local (Log on to local machine)

Activez cette option pour vous connecter à l'ordinateur sur lequel le serveur WinGate est installé

Enregistrer ces informations pour les prochaines connexions (Use these details next time to login directly)

Activez cette option si vous souhaitez pas indiquer votre identifiant et mot de passe à chaque connexion.

Pour la première connexion à GateKeeper :

1. Ouvrez **GateKeeper**.
2. Indiquez **Administrator** dans le champ **Nom d'utilisateur (Username)**.
3. Ne remplissez pas le champ du mot de passe et cliquez sur **OK**.
4. Un message vous avertit qu'aucun mot de passe n'a été saisi et vous **demande d'en choisir un**.



Masquer | Masquer toutes les images

5. Cliquez sur **OK** pour **saisir votre mot de passe**.



Masquer | Masquer toutes les images

6. Cliquez sur **OK**.
7. Vous êtes à présent connecté à GateKeeper en tant que **Administrator**.

Remarque :

Si lors de l'installation du programme vous cochez l'option [Utiliser la base de données d'utilisateurs du système d'exploitation \(Windows\) \(Use the operating system \(Windows\) user database\)](#), il n'est pas nécessaire de choisir un mot de passe lors de la première connexion à GateKeeper. Vous devrez indiquer le mot de passe de l'administrateur du système d'exploitation.

Voir également :

[Méthodes d'authentification : GateKeeper](#)

Veillez noter que l'accès à GateKeeper à distance n'est possible que si vous

possédez WinGate Pro ou Enterprise, quelle que soit la version.

©2004 Qbik New Zealand Limited

Le panneau Contrôle

Le **panneau Contrôle** est constitué de trois onglets :



Masquer

Systeme (*System*)

Affiche la liste des services système (DHCP, DNS, E-mail, etc.)

Services

Affiche la liste de tous les serveurs proxy.

Utilisateurs (*Users*)

Contient toutes les options relatives aux utilisateurs, groupes, bases de données et la politique système.

Ce panneau est **détachable**.

Pour cela :

1. Cliquez sur le bord du panneau.
2. Effectuez un glisser-déposer sur le bureau.
3. Pour le rattacher à GateKeeper, double-cliquez sur le bord du panneau.

Icônes de GateKeeper

Toutes les icônes de l'onglet **Activité** représentent des **sessions**. Elles s'affichent lorsque les sessions sont actives, et disparaissent lorsqu'elles sont terminées.

Sessions de données

Reflète l'utilisation d'un proxy ou d'un service. Une session de données indique le nom de l'ordinateur (nom Netbios ou IP) et celui de l'utilisateur (ou "Invité").

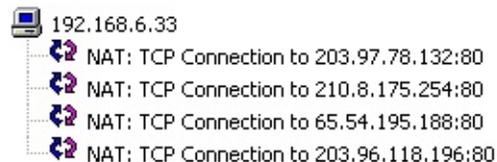
Requêtes proxy (ou NAT/WGIC avec l'option [Proxy transparent \(Transparent Proxy\)](#))

Lorsqu'un client accède à Internet à l'aide de la méthode proxy ou qu'une requête NAT/WGIC est interceptée par l'option de proxy transparent, l'activité s'affiche comme suit :



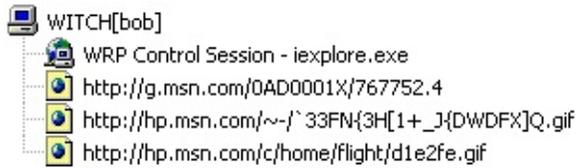
NAT

Lorsqu'un client accède à Internet à l'aide du [NAT](#) l'activité s'affiche comme suit :



Service WRP (connexion avec WinGate Internet Client)

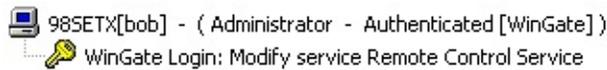
Dans ce cas, l'activité s'affiche comme suit :



Statut/authentification des utilisateurs

Lorsqu'un utilisateur essaie d'utiliser les services de WinGate, l'affichage dépend de la façon dont il s'est authentifié :

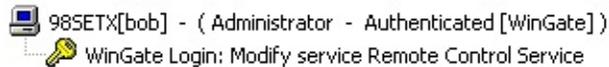
Base de données d'utilisateurs WinGate



Base de données du système d'exploitation/distante



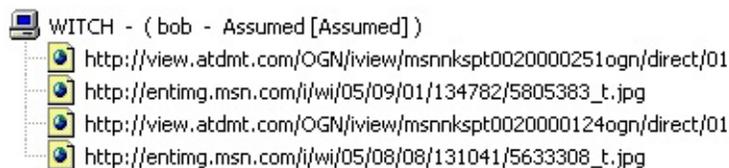
GateKeeper



Authentification Java



Utilisateur présumé



Divers

Poste



Cette icône représente les ordinateurs utilisant WinGate. Elle est suivie du nom Netbios de l'ordinateur (s'il est disponible), ou de son adresse IP.

Session terminée

 WITCH - (bob - Assumed [Assumed])

Lorsqu'un utilisateur arrête sa session, l'icône de l'ordinateur reste grise pendant 30 secondes après la déconnexion, et son nom est suivi de l'indication **Présumé (Assumed)**.

Menus de GateKeeper

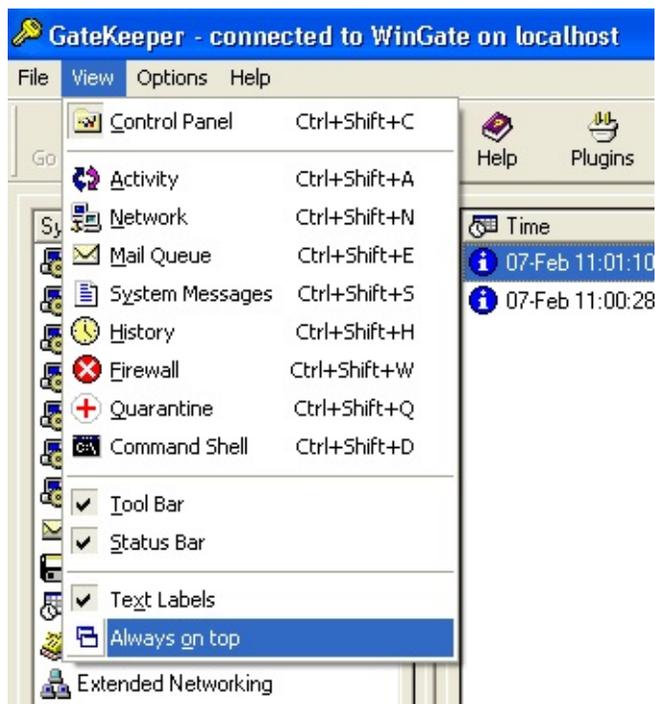
Voici un aperçu des menus de GateKeeper :

Fichier (File)



Masquer | Masquer toutes les images

Affichage (View)



Masquer | Masquer toutes les images

Raccourcis vers les onglets du panneau Activité et options d'affichage.

Options



Masquer | **Masquer toutes les images**

Aide (Help)



Masquer | **Masquer toutes les images**

Barre de menus

Sur la **Barre de menus** se trouvent des icônes permettant un accès rapide aux principales fonctionnalités :



Masquer | Masquer toutes les images

Connexion (Go Online)

Affiche l'interface de GateKeeper. Cette option n'est disponible que lorsque GateKeeper est déconnecté.

Déconnexion (Go Offline)

Lorsque GateKeeper est **déconnecté**, l'interface n'est plus disponible mais le moteur de WinGate continue de fonctionner.

GateKeeper Offline

Masquer | Masquer toutes les images

Enregistrer (Save)

Enregistre les paramètres actuels.

Contrôle (Control)

Affiche ou masque le panneau Contrôle.

Modules (Plugins)

Ouvre le menu de configuration des modules.

Aide (Help)

Affiche l'aide de WinGate.

Administration de WinGate

Pour modifier les paramètres de WinGate, vous devez être connecté à GateKeeper en tant que **Administrator** ou membre du groupe **Administrators**.

En effet, il n'est pas possible de configurer directement le moteur de WinGate.

Remarque :

Pour modifier certaines fonctionnalités, vous devrez redémarrer WinGate. Prenez donc garde aux conséquences sur les opérations du réseau.

Administration en temps réel

Les sessions s'affichant de façon dynamique, les administrateurs peuvent les contrôler en temps réel en effectuant un clic droit sur le nom de la session/de l'utilisateur.

[Cliquez ici pour en savoir plus.](#)

Administration distante

La plupart des tâches d'administration peuvent être effectuées à distance. Il suffit de lier un lecteur au répertoire de WinGate sur le serveur et d'exécuter GateKeeper.exe.

[Cliquez ici pour en savoir plus.](#)

©2005 Qbik New Zealand Limited

Options de l'onglet Activités (*Activity*)

En effectuant un **clic droit** sur l'une des sessions de cet onglet, vous accédez à un menu proposant diverses options :

Masquer

Mettre en pause l'affichage des activités (*Pause activity updates*)

Permet aux administrateurs de "figer" l'affichage des activités dans cet onglet.

Afficher par service (*View by Service*)

Présente l'ensemble des activités classées par service (affichage sélectionné par défaut). Il est possible de le remplacer par **Afficher par ordinateur (*View by Machine*)**.

Afficher par ordinateur

Présente l'ensemble des activités classées par ordinateur.

Arrêter le service d'administration à distance (*Stop Remote Control Service*)

Empêche les utilisateurs d'accéder à GateKeeper par le biais d'une [connexion distante](#).

Propriétés du service (*Service properties*)

Affiche les propriétés du service sélectionné.

Envoyer un message à (*Send message to*)

Permet d'envoyer un message aux utilisateurs connectés à GateKeeper. (L'utilisateur peut répondre au message).

Désactiver l'utilisateur : (*Disable user:*)

Empêche l'utilisateur de procéder à une authentification ou bien d'utiliser WinGate pour accéder à Internet.

Propriétés de l'utilisateur : (*Properties for user:*)

Permet de configurer les propriétés du compte.

Copier l'url dans le presse-papiers (*Copy url to clipboard*)

Permet à l'administrateur de copier une url de l'onglet Activités dans le presse-papiers. Il suffit ensuite de la coller dans un navigateur pour afficher la page ou ressource correspondante.

Propriétés (*properties*)

Affiche diverses propriétés ainsi que les détails de connexion de l'ordinateur sélectionné.

Accès distant à GateKeeper

Il est possible d'accéder à GateKeeper à distance, afin de pouvoir administrer WinGate.

Pour cela :

1. Ouvrez le **Service d'administration à distance (*Remote control service*)** (dans l'onglet **Système** du panneau Contrôle).

2. Cliquez sur l'icône **Liaisons (*Bindings*)**.

Masquer | Masquer toutes les images

3. Assurez-vous que le service soit lié à localhost (127.0.0.1) et à toutes les interfaces réseau internes.
4. Copiez le fichier **GateKeeper.exe** (se trouvant dans le répertoire d'installation de WinGate sur le serveur) et collez-le sur un autre poste.
5. Exécutez ce fichier et indiquez les informations suivantes **lors de la connexion** :

Masquer | Masquer toutes les images

- **Nom d'utilisateur (*Username*) :**

Un compte WinGate possédant des droits d'administration (n'indiquez pas de compte Windows, sauf si vous utilisez la base de données du système d'exploitation).

- **Mot de passe (*Password*) :**

Le mot de passe correspondant.

- **Serveur :**

Le nom ou l'adresse IP de l'ordinateur sur lequel se trouve WinGate.

- **Port :**

Port 808 (sauf si vous avez modifié le numéro de port de ce service).

Remarque :

Si vous souhaitez pouvoir consulter l'onglet **Historique (History)**, créez un **mappage de lecteur réseau** entre l'ordinateur et le répertoire **\WinGate** sur le serveur.

©2004 Qbik New Zealand Limited

Panneau activité

Fournit aux administrateurs un aperçu en temps réel des principales activités de WinGate. Il est formé de **plusieurs onglets** :



Masquer

Activité (*Activity*)

Affiche en temps réel l'activité des sessions par utilisateur ou par ordinateur. Une sous-fenêtre indique également l'activité du système.

Il est possible de modifier ou de supprimer une session dans cet onglet.

Réseau (*Network*)

Permet d'explorer le réseau local ainsi que les connexions WinGate VPN. Une sous-fenêtre indique le statut des connexions réseau (interfaces).

File d'attente (*Mail queue*)

Affiche sous forme de graphique le statut des files d'attente pour le courrier.

Historique (*History*)

Affiche l'historique de l'activité et des évènements de WinGate.

Messages système (*Système messages*)

Informent les administrateurs de divers évènements.

Pare-feu (*Firewall*)

Affiche en temps réel l'activité du pare-feu.

Quarantaine (*Quarantine*)

Affiche les éléments mis en quarantaine par les modules additionnels d'analyse.

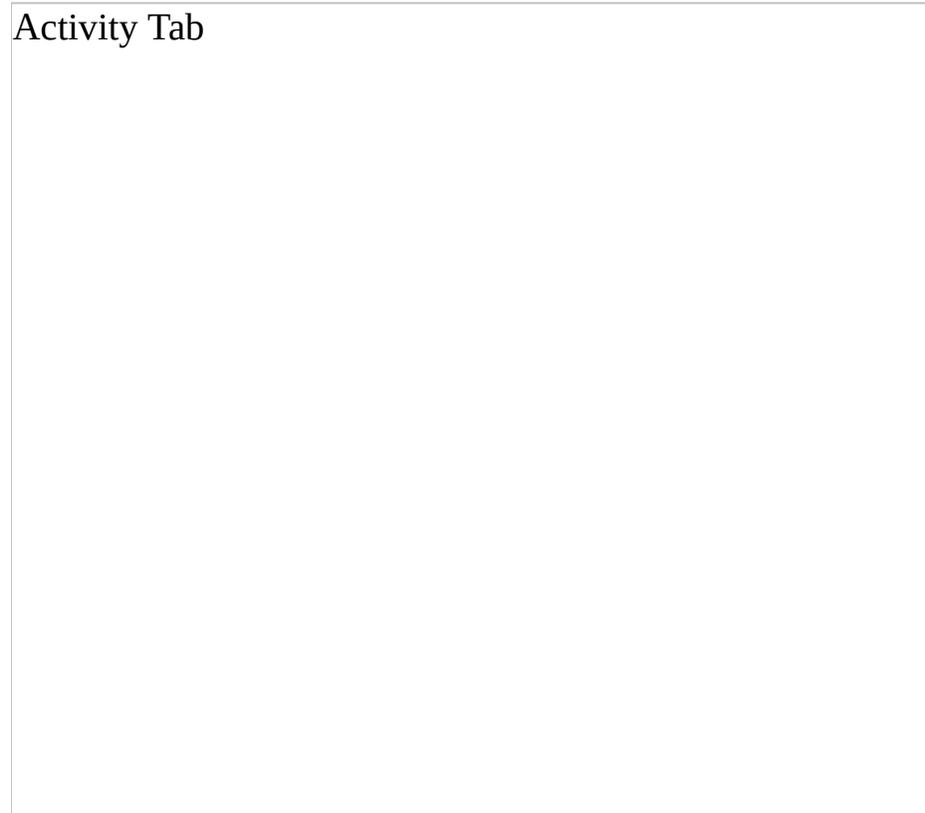
CMD.EXE

Interpréteur de commandes.

©2004 Qbik New Zealand Limited

Onglet Activités (*Activity*)

Cet onglet présente l'activité des utilisateurs de WinGate.



Masquer

Connexions clients

Tous les utilisateurs connectés à WinGate figurent dans l'onglet **Activité (Activity)**.

Diverses informations s'affichent : le nom ou l'adresse IP de l'ordinateur, le nom de l'utilisateur et son statut (entre crochets).

Le statut indique si l'utilisateur est authentifié, et le type d'authentification (WinGate ou NTLM).

Une fois la session terminée, la connexion s'affiche en gris pendant trente secondes avant de disparaître de l'écran.

Sessions

Les sessions s'affichent de façon dynamique et disparaissent une fois terminées.

Les sessions en cours sont affichées en temps réel soit par service, soit par ordinateur (en effectuant un clic droit sur la session : options **Afficher par ordinateur/par service (View by Machine/by Service)**).

Pour obtenir la liste de toutes les sessions effectuées depuis la connexion, cliquez sur l'onglet **Historique (History)**. Pour plus d'informations, consultez les fichiers journaux

Toute personne possédant les droits nécessaires (par exemple un administrateur) peut supprimer une session dans cet onglet.

Sessions de données

Il est possible d'arrêter les sessions de données sans que cela n'affecte les autres activités de l'utilisateur concerné. Cela peut s'avérer utile si la session est interrompue ou si vous estimez que le comportement de l'utilisateur est répréhensible.

Connexion pour l'administration à distance

Si cette connexion est interrompue, les utilisateurs ne seront plus authentifiés, et passeront au statut d'utilisateur présumé (s'ils ont d'autres sessions ouvertes ou s'il existe un mappage), ou bien d'invité.

Entrées "Utilisateur"

Si vous supprimez l'une de ces entrées, toutes les sessions associées à son adresse IP seront interrompues, et ne seront donc plus présentes à l'écran. Dans le cas où l'ordinateur continue de demander l'accès, l'utilisateur apparaîtra en tant qu'invité ou utilisateur présumé.

Menu contextuel

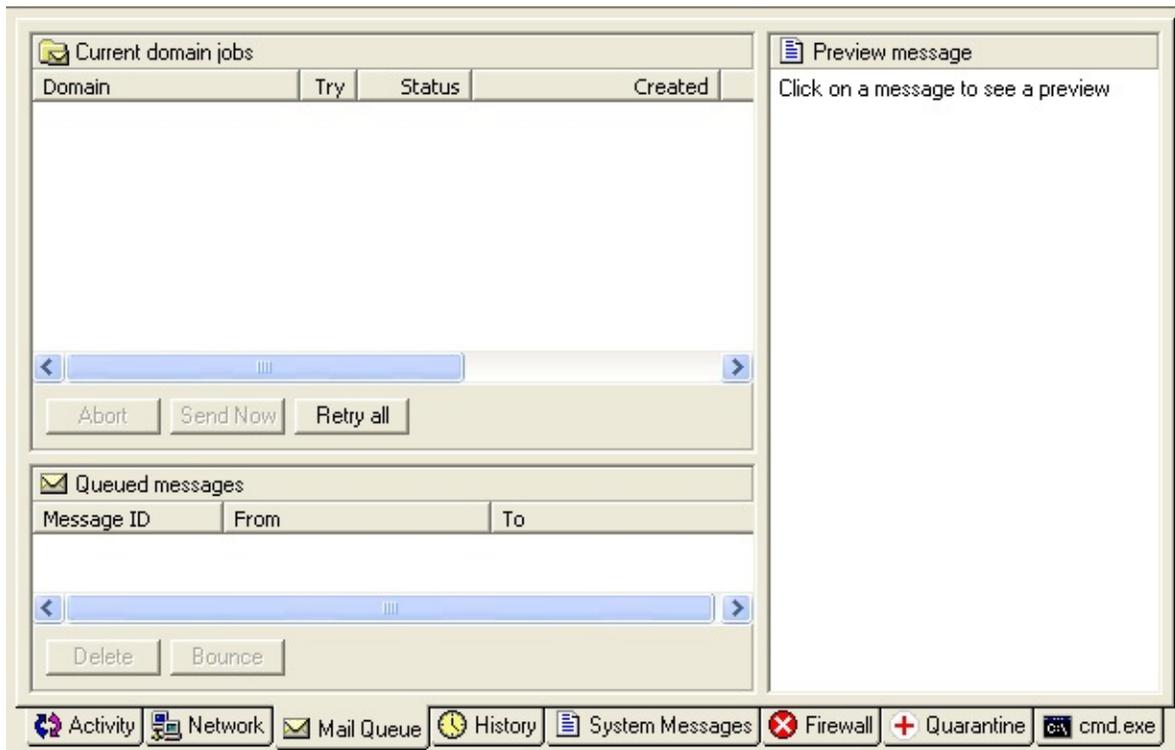
En effectuant un clic droit sur le nom d'un ordinateur ou d'un utilisateur, vous disposez d'un menu contextuel proposant diverses options.

[Cliquez ici pour en savoir plus](#)

©2004 Qbik New Zealand Limited

Onglet File d'attente (*Mail queue*)

L'onglet **File d'attente** affiche en temps réel la file d'attente du courrier distribué avec le serveur de messagerie de WinGate.



Masquer

Remarque :

Seul le courrier qui n'a pas encore été envoyé figure dans cet onglet. Le courrier en train d'être envoyé est affiché dans l'onglet Activité.

Il est constitué de trois panneaux :

1. Domaines

Affiche la liste du courrier en file d'attente par domaine ainsi que le statut.

En sélectionnant un domaine vous pouvez effectuer différentes

actions :

- **Annuler (*Abort*)**

Annule l'envoi du courrier pour ce domaine.

- **Envoyer maintenant (*Send now*)**

Distribue immédiatement le courrier du domaine.

- **Distribuer tout (*Retry all*)**

Essaie d'envoyer à nouveau le courrier de chaque domaine, sans tenir compte des statuts.

2. Messages

Affiche la liste des messages de chaque domaine figurant dans le panneau ci-dessus.

- **Supprimer (*Delete*)**

Supprime le message sélectionné.

- **Retourner (*Bounce*)**

Retourne le(s) message(s) sélectionné(s) à l'expéditeur (si aucun expéditeur n'est trouvé, le message est supprimé).

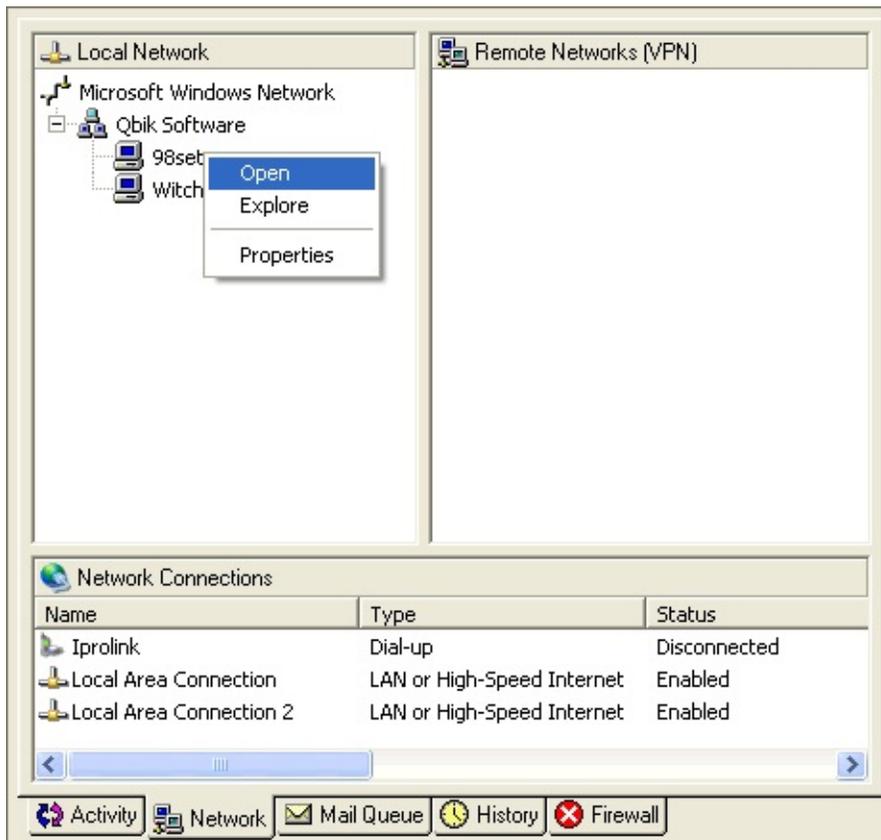
3. Aperçu

Affiche le contenu des messages sélectionnés.

Veillez noter que l'onglet File d'attente n'est disponible qu'à partir de la version 6 de WinGate

Onglet réseau

L'[onglet Réseau](#) affiche les postes du réseau local (LAN), et les réseaux distants accessibles à l'aide de WinGate VPN.



[Masquer](#)

Même si WinGate VPN n'est pas installé, le réseau local du serveur WinGate figure dans cet onglet. Les noms des ordinateurs du réseau local s'affichent au fur et à mesure que WinGate les détecte (l'énumération de noms Netbios est parfois assez longue).

En cliquant avec le bouton droit de la souris sur l'un des ordinateurs de la liste, vous disposez de quatre options :

1. **Ouvrir (*Open*)**
Ouvre l'ordinateur.
2. **Explorer (*Explore*)**

Ouvre l'ordinateur dans l'explorateur Windows.

3. **Tester (*Tester*)**

Teste à nouveau la connectivité avec l'ordinateur (généralement utilisé avec WinGate VPN).

4. **Propriétés (*Properties*)**

Affiche les propriétés de l'ordinateur.

[Cliquez ici pour en savoir plus sur les connexions réseau](#)

©2004 Qbik New Zealand Limited

Onglet Historique (*History*)

L'**onglet Historique** affiche en temps réel de nombreuses informations :

Masquer

En cliquant avec le bouton droit de la souris à l'intérieur de cet onglet, vous disposez d'un menu contextuel contenant les options suivantes :

Modifier les colonnes (*Edit columns*)

Vous pouvez choisir les colonnes à afficher dans l'onglet.

Effacer l'historique (*Clear history*)

Efface définitivement tout le contenu.

Mettre l'IP xxx en liste noire (*Blackhole IP*)

Empêche une adresse spécifique d'accéder à WinGate. [Cliquez ici pour en savoir plus.](#)

Propriétés (*Properties*)

Permet de configurer les paramètres généraux de cet onglet.

Enregistrer l'historique (*Save history*)

Ouvre une fenêtre **Enregistrer sous** et sauvegarde l'historique sous forme de fichier texte.

Informations complémentaires :

Si vous êtes connecté à localhost, vous pouvez consulter l'historique de la session précédente.

Les sessions sont affichées dans l'ordre chronologique (en fonction du moment où elles ont été arrêtées), des plus récentes aux plus anciennes. Comme les requêtes DNS sont très rapides (grâce à la mémoire cache) la durée est généralement de 0.

Si votre système "plante", la base de données risque d'être corrompue. Cela peut

être à l'origine du problème si vous constatez que la connexion à GateKeeper est impossible alors que le moteur fonctionne. Pour vous en assurer, arrêtez WinGate, sauvegardez les deux fichiers de base de données et déplacez-les hors du répertoire de WinGate. Redémarrez WinGate. Si GateKeeper fonctionne, cela signifie que la corruption de la base de données était à l'origine du problème. Dans le cas contraire, remplacez les fichiers dans le répertoire.

Pour pouvoir consulter l'historique avec une connexion à distance, vous devez mapper un lecteur réseau au répertoire de WinGate sur le serveur contenant le fichier GateKeeper.exe utilisé pour la connexion.

Voir également :

[Filtrage de l'historique](#)

©2004 Qbik New Zealand Limited

Activité du pare-feu

GateKeeper possède un **onglet** où s'affichent en temps réel les tentatives d'intrusion sur le réseau bloquées par le pare-feu.



Masquer

De par son architecture, WinGate protège tous les ordinateurs d'un réseau des attaques extérieures car il fait office de bouclier. De plus, le serveur est lui-même protégé par un pare-feu intégré contrôlant tout le réseau.

Ce pare-feu analyse tous les paquets arrivant sur le serveur puis les autorise ou les rejette.

L'activité du pare-feu figure dans cet onglet.

Heure (Time)	Heure à laquelle les données ont été détectées
IP source (Source IP)	IP de l'ordinateur qui demande/envoie des données
Port	Numéro du port sur lequel les données sont arrivées
IP dest (Dest IP)	IP de l'ordinateur destinataire
Protocole	TCP ou UDP
Info	Informations complémentaires sur la nature des données

Messages système

L'onglet **Messages système (System Messages)** est destiné à aider les administrateurs à diagnostiquer les problèmes liés au réseau. Il permet également de les informer de certains événements comme la détection d'un nouveau module, une modification de la licence...

Masquer

Chaque message est précédé d'une icône indiquant sa nature :

- Tout problème ayant empêché un service de démarrer ou de fonctionner correctement.
- Notification d'un événement.
- Tentative de violation du système.
-  Authentification échouée.

Activation des messages système

Les messages système sont toujours activés, et peuvent être à tout moment consultés par les administrateurs. Pour afficher cet onglet, cliquez sur le menu **Affichage (View)/Messages système (System Messages)**.

Lorsqu'un message est généré, il est mis en file d'attente puis envoyé à TOUS les administrateurs connectés ou au premier qui se connecte si aucun n'est présent.

Remarque :

Limitations

Certains évènements peuvent générer un grand nombre de messages (par exemple, les tentatives de violation de sécurité). Le moteur de WinGate acceptera un maximum de 200 messages (en remplaçant les anciens) et GateKeeper en affichera un maximum de 1000 (en remplaçant également les anciens).

[Cliquez ici pour une liste complète des messages de WinGate](#)

©2005 Qbik New Zealand Limited

Onglet Quarantaine

Lorsque les modules d'analyse des données détectent des fichiers potentiellement dangereux (par ex. : un virus), ils sont détruits ou bien conservés dans un endroit sûr, c'est à dire mis en quarantaine.

Lorsqu'un fichier est mis en quarantaine, **cet onglet** affiche les informations suivantes :

Quarantine tab



Masquer

Heure (*Time*)

L'heure exacte à laquelle les données ont été détectées par le module.

Poste (*Computer*)

Nom de l'ordinateur sur lequel les données ont été détectées.

Utilisateur (*WG User*)

Nom de l'utilisateur connecté sur ce poste.

Adresse IP (*IP Address*)

Adresse utilisée lorsque les données ont été détectées.

Numéro (*ID*)

Numéro attribué par WinGate au fichier détecté.

État (*State*)

Le fichier peut être soit maintenu en quarantaine, soit accepté (seulement si vous êtes sûr qu'il n'y a pas de danger).

Taille (*Size*)

Taille du fichier en Ko.

Source

Indique par quel service les données sont entrées sur le réseau : proxy FTP, proxy web, etc.

Contexte

Brève description de l'analyse du fichier.

Raison (*Reason*)

Raison pour laquelle le fichier a été placé en quarantaine (cela peut inclure le nom du virus détecté).

Ces fichiers sont conservés dans le dossier **WinGate\Quarantine**.

Si un fichier est accepté, il sera marqué comme tel et copié dans le dossier **wingate\Quarantine\Release\"Source\"Contexte**.

Par exemple, si un fichier appelé virus.exe est téléchargé de

ftp://serveur.com/mauvais/virus.exe par le proxy FTP, il sera enregistré dans **Wingate\Quarantine\Release\FTPProxy\mauvais\virus.exe**

L'administrateur peut choisir de retourner le fichier à l'expéditeur, à l'exception des e-mails. Si un e-mail mis en quarantaine est accepté, il sera automatiquement remis à son destinataire.

Voir également :

[Options de quarantaine](#)

©2004 Qbik New Zealand Limited

Interpréteur de commandes (*Command Shell*)

L'**Interpréteur de commandes** est une nouvelle fonctionnalité de WinGate, disponible dans GateKeeper. Il permet aux utilisateurs d'exécuter plusieurs instances de l'interpréteur de commandes (cmd.exe) de Windows NT/2000/XP sur le serveur.



Masquer | Masquer toutes les images

Il est similaire à un serveur Telnet, mais plus sécurisé, car toutes les communications sont effectuées via GateKeeper avec le canal de communications crypté de WinGate. Les utilisateurs peuvent donc exécuter des applications consoles sur le serveur WinGate.

Cela peut s'avérer utile pour diverses tâches :

Utiliser **ping** et **tracert** pour vérifier la connectivité de base de l'ordinateur sur lequel WinGate est installé.

Exécuter **route.exe** pour consulter ou modifier la table de routage du système.

Exécuter **ipconfig.exe** pour **renouveler** ou **générer** des adresses pour les adaptateurs réseau, et obtenir des informations sur la configuration TCP/IP.

Exécuter **ps.exe** (composant du kit de ressources posix pour Windows) pour afficher et arrêter les processus en cours.

Utiliser **net.exe** pour parcourir un réseau, mapper un lecteur, etc.

Exécuter **shutdown.exe** pour redémarrer le serveur WinGate, ou des ordinateurs distants.

En résumé, vous pouvez effectuer à distance quasiment les mêmes opérations qu'en exécutant cmd.exe.

Pour utiliser cette fonctionnalité:

1. Cliquez sur **Interpréteur de commandes (*Command Shell*)** dans le

menu **Afficher (View)** de GateKeeper.

2. Dans la **fenêtre de connexion** qui s'ouvre ensuite, indiquez le compte d'utilisateur Windows de l'ordinateur où se trouve WinGate (même si WinGate utilise sa propre base de données d'utilisateurs).



Masquer | Masquer toutes les images

Restrictions :

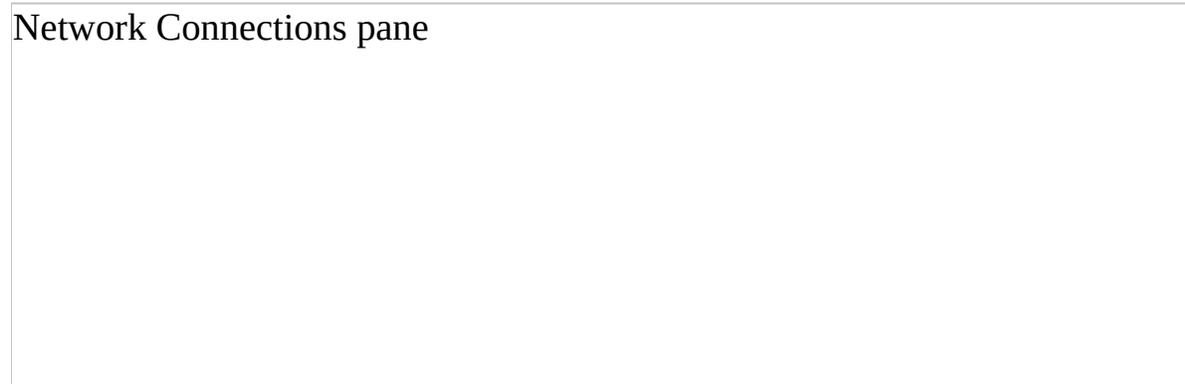
1. Cette fonctionnalité n'est disponible qu'à partir de la version **6.0** de WinGate, pour les licences **WinGate Professional** ou les utilisateurs de **WinGate VPN**.
2. Certaines applications ouvrant automatiquement leur propre fenêtre ne sont pas compatibles avec cette option, par exemple : **telnet.exe**, et **ftp.exe**.

Connexions réseau (*Network Connections*)

Situé au bas de l'onglet **Réseau** (*Network*), **ce panneau** permet de détecter automatiquement les interfaces réseau disponibles (à partir de la version 6.0).

Lorsqu'une interface réseau est détectée, le moteur de WinGate examine son adresse IP afin de déterminer s'il s'agit d'une interface interne (réseau local) ou externe (connexion Internet). Il établit ensuite les **liaisons** (*Bindings*) qui s'y appliquent.

Network Connections pane



Masquer | **Masquer toutes les images**

Nom (*Name*)

Nom donné par le système d'exploitation. (Vous pouvez le modifier dans les propriétés de l'interface réseau).

Type

WinGate distingue les interfaces réseau des connexions commutées.

État (*Status*)

Indique (de façon dynamique) si l'adaptateur réseau est activé ou désactivé.

Usage

Selon les détails de son adresse IP, WinGate détermine si cette connexion est à usage interne ou externe et applique les politiques en conséquence. Vous pouvez modifier manuellement ce paramètre dans l'onglet Général des propriétés de la connexion réseau dans GateKeeper (voir ci-dessous).

Vitesse (*Speed*)

Indique la vitesse de la connexion.

Détails

Contient les détails de fabrication et du modèle.

Propriétés (*Network connection properties*)

Double-cliquez sur une connexion pour en afficher les propriétés :

1. Onglet Général

Indique la vitesse de la connexion et permet aux administrateurs d'indiquer à quel type de réseau se connecte cette interface :

- Détection automatique (en fonction des paramètres de l'adresse IP)
- Réseau interne protégé
- Réseau externe inconnu (par ex. : Internet)
- Réseau externe sécurisé (DMZ)

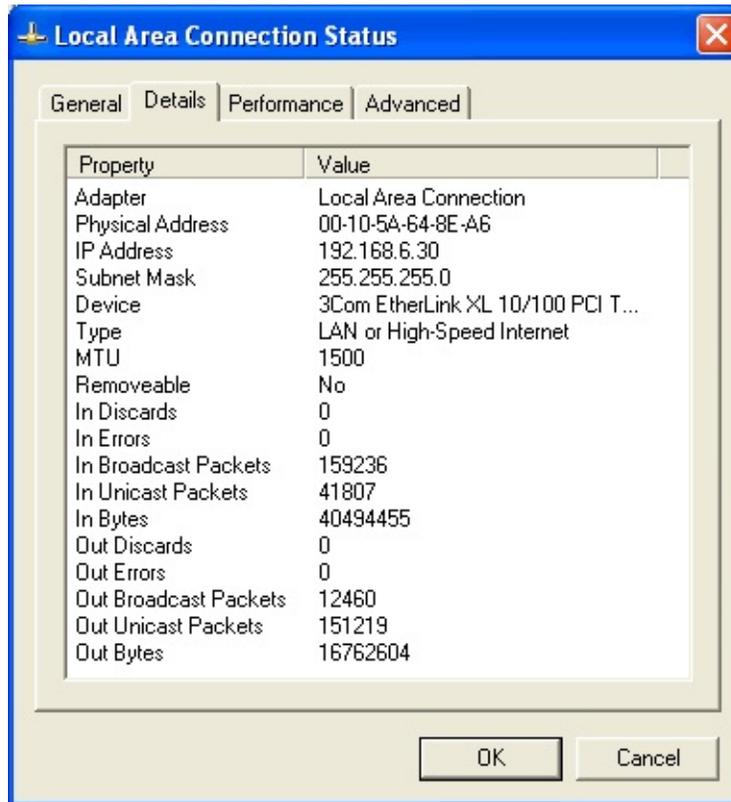
Masquer | **Masquer toutes les images**

Veillez noter que seules les versions WinGate 6 Pro et

Enterprise assurent le support des DMZ (DeMilitarized Zone)

2. Onglet Détails

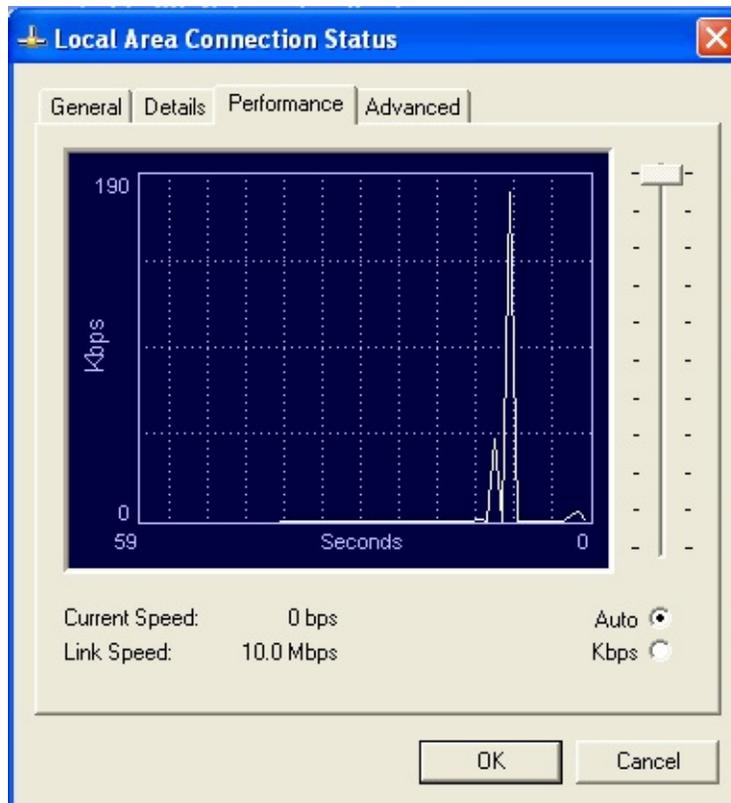
Affiche diverses informations concernant l'interface.



Masquer | Masquer toutes les images

3. Onglet Performances

Permet à l'administrateur de consulter en temps réel l'activité sur son réseau.



Masquer | Masquer toutes les images

Les performances peuvent être affichées de deux façons :

- **Automatique**

La valeur maximum de l'axe des ordonnées (Ko/s) correspond au maximum atteint depuis que la fenêtre est ouverte.

- **Kbps**

Lorsque cette option est cochée, il est possible de modifier manuellement les valeurs de l'axe des ordonnées. Si vous déplacez le curseur vers le haut, ces valeurs diminuent, ce qui permet d'effectuer un "gros plan" sur les données. Inversement, les valeurs augmentent si vous déplacez le curseur vers le bas (maximum 1250 Ko/s).

4. Onglet Avancé

Advanced tab



Masquer | Masquer toutes les images

Outrepasser la MTU de l'interface (*Override interface MTU*)

Indiquez la valeur maximum pour la MTU (Maximum Transmission Unit).

Cela peut s'avérer utile si vous rencontrez des problèmes pour accéder aux ressources VPN ou constatez des pertes de paquets.

Outrepasser la métrique de l'interface (*Override interface metric*)

Vous pouvez modifier la métrique configurée par défaut par le système d'exploitation.

Les valeurs sont comprises entre 0 et 50 (0 correspond à la métrique la plus basse possible, car la valeur minimale utilisée par le système d'exploitation est 1).

Activer le répondeur ARP (*Enable Arp Responder*)

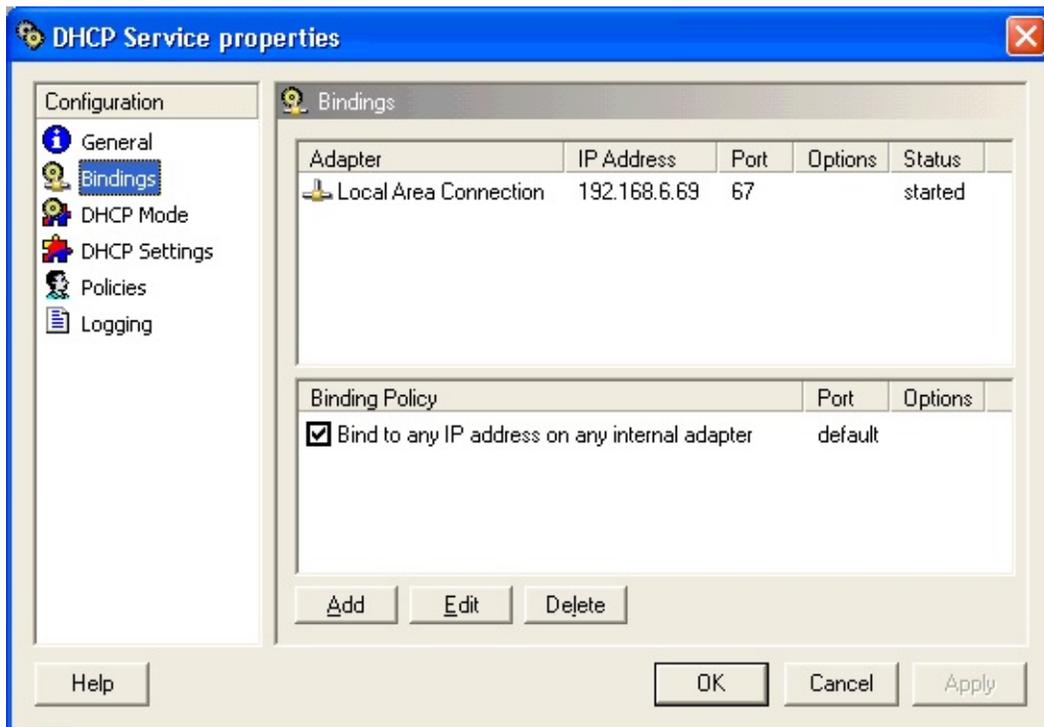
Si cette option est cochée, lorsque l'interface reçoit une requête ARP pour une adresse IP qui n'est pas la sienne, elle répond en envoyant son adresse MAC.

Vous pouvez choisir pour quelles requêtes (adresse IP) l'interface doit envoyer son adresse MAC.

Veillez noter que le répondeur ARP et les liaisons SSL par service ne sont disponibles qu'avec WinGate 6 Enterprise.

Liaisons (*Bindings*)

Cette option, commune à tous les services de WinGate, permet d'en assurer la sécurité et la gestion.



Masquer | **Masquer toutes les images**

Que sont les liaisons ?

Pour accéder à Internet par le biais d'un service spécifique dans WinGate, les clients doivent communiquer avec ce service via l'interface réseau du serveur WinGate connectée au LAN.

Par exemple, pour ouvrir une page web dans le navigateur, les postes clients se connectent au service proxy web (*WWW proxy service*) de WinGate afin que celui-ci exécute les requêtes.

Pour qu'un service puisse exécuter les requêtes des postes clients, il doit être configuré afin d'écouter ces requêtes sur l'interface réseau qui les reçoit. Il s'agit généralement de l'interface LAN, mais il est possible d'accepter les requêtes sur n'importe quelle interface disponible.

Puis, lorsqu'il reçoit une requête, WinGate utilise automatiquement l'interface externe pour accéder à Internet et ainsi l'exécuter.

Il est donc recommandé de ne pas lier une connexion Internet à un service car cela autorise les utilisateurs distants à utiliser les services proxy de WinGate. Attention : si un service n'est lié à aucune interface, les clients ne pourront pas s'y connecter.

En règle générale, les administrateurs souhaitent que le service proxy web ne soit accessible qu'aux utilisateurs du réseau local. Il suffit pour cela de cliquer sur l'icône **Liaisons (Bindings)** dans les propriétés du service et de s'assurer qu'il ne soit lié qu'à la carte LAN (adaptateur interne) et localhost (127.0.0.1).

Remarque :

La liaison avec 127.0.0.1 (localhost) est nécessaire pour que l'ordinateur local puisse utiliser ce service.

Liaisons dynamiques (*Dynamic Bindings*)

Depuis la version 6.0, WinGate supporte les **liaisons dynamiques** : les interfaces disponibles sont automatiquement détectées et classées en tant qu'interface interne ou externe (en fonction des détails de leur adresse IP).

Adaptateur interne (*Internal adapter*)

Il s'agit généralement des interfaces LAN ayant une adresse privée, et donc considérées comme "connues".

Adaptateur externe (*External adapter*)

Connexion Internet ou adaptateur ayant une adresse IP publique, et donc considéré comme "inconnu".

Il est possible de modifier manuellement les propriétés de chaque interface réseau en double-cliquant sur son nom dans l'onglet **Réseau (*Network*)**, panneau

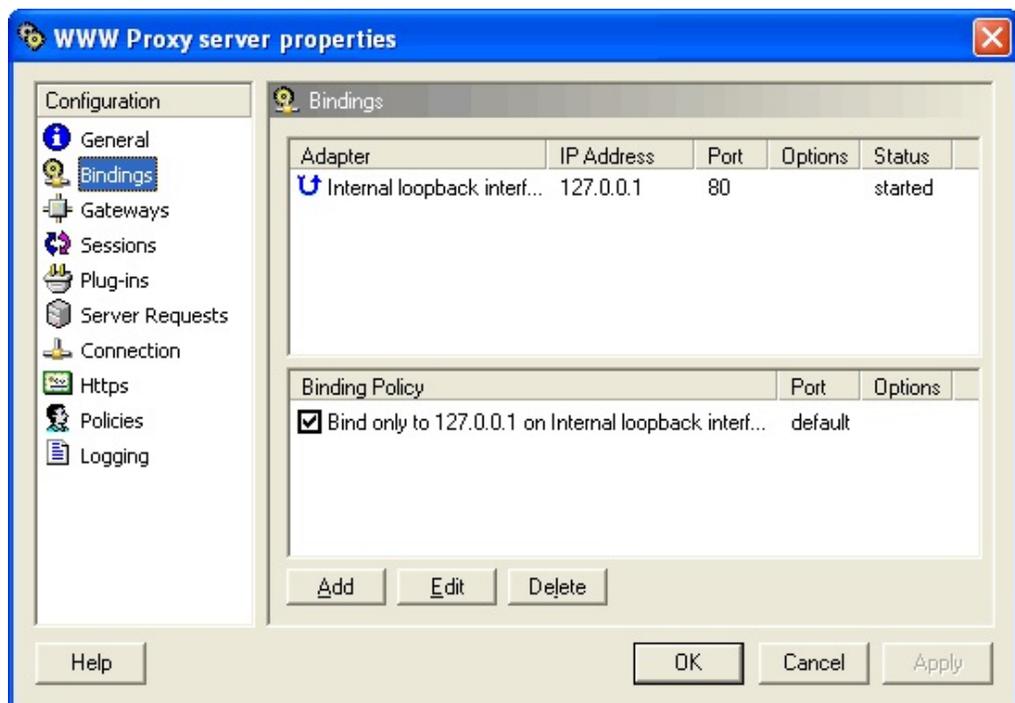
Connexions réseau
(*Network Connections*).

Network Connections

Masquer | Masquer toutes les images

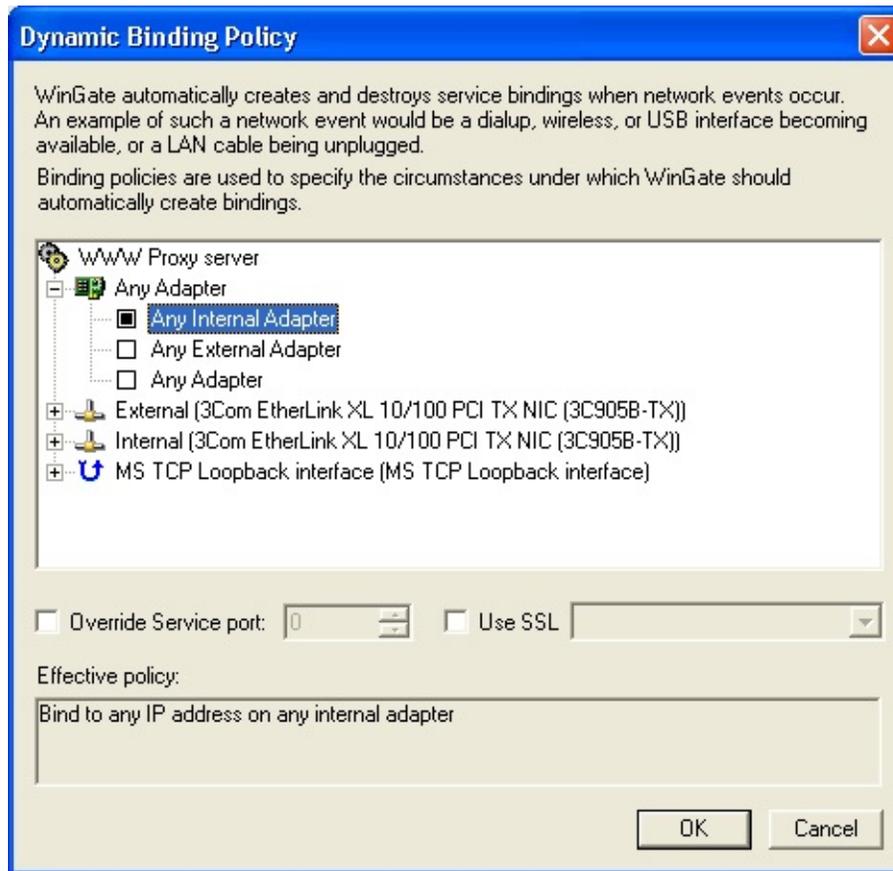
Lier manuellement un service à une interface :

1. Ouvrez **GateKeeper**.
2. Dans les propriétés du service choisi (ici, le service proxy web), cliquez sur l'icône **Liaisons (Bindings)**.



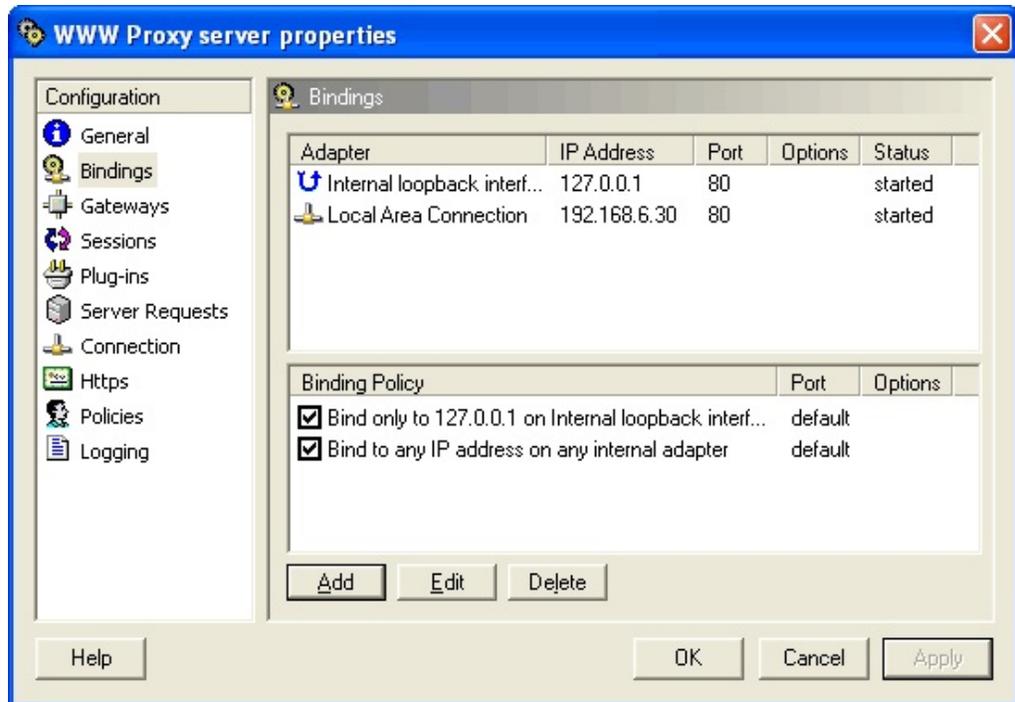
Masquer | Masquer toutes les images

3. Cliquez sur le bouton **Ajouter (Add)**. Une **nouvelle fenêtre** s'ouvre.



Masquer | Masquer toutes les images

4. Cochez la case **Tous les adaptateurs internes (Any Internal adapter)**. Cela permet à WinGate de lier ce service à tous les adaptateurs internes détectés. Vous pouvez également sélectionner l'interface de votre choix.
5. Cliquez sur **OK**.
6. La liaison s'affiche à présent dans les **propriétés du service**.



Masquer | Masquer toutes les images

7. Cliquez sur **OK** pour terminer.

Recommandations :

Ne liez les services qu'aux interfaces LAN.

Les liaisons vers vos profils de connexion sont généralement inutiles.

Après avoir installé WinGate, ou modifié les paramètres des adaptateurs réseau, vérifiez que ces derniers soient correctement classifiés par WinGate.

Conseils de sécurité :

Pour une sécurité optimale, ne liez les services qu'avec votre carte LAN et "localhost". N'autorisez pas de liaisons vers un profil de connexion.

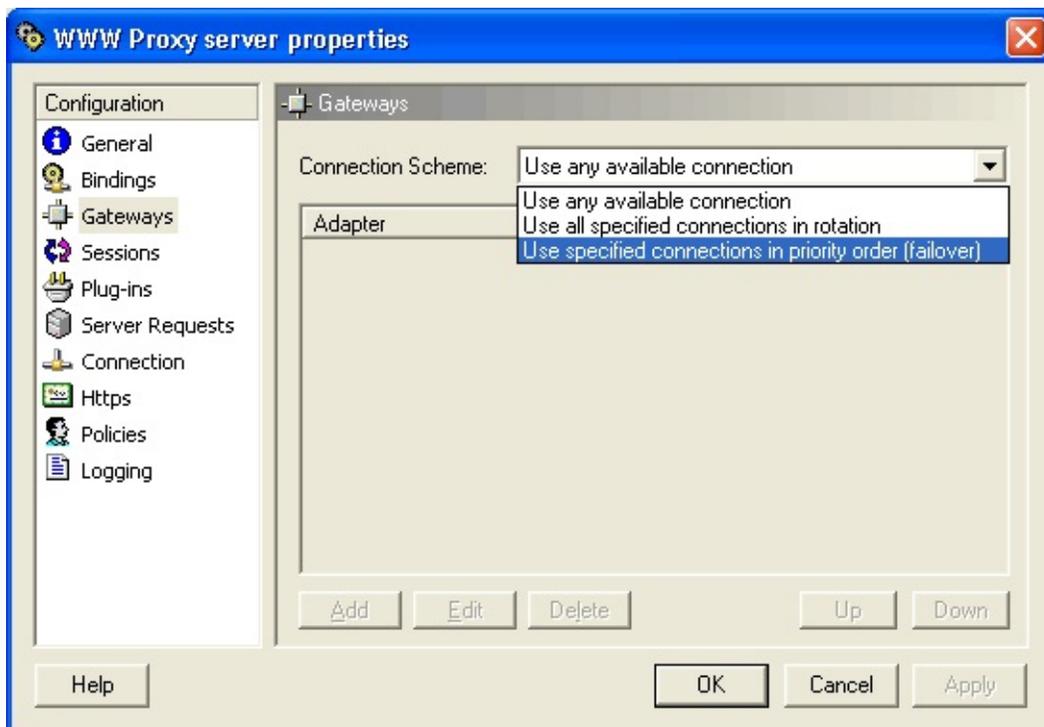
Soyez vigilant lorsque vous liez une interface externe à un service : cela peut éventuellement autoriser l'accès externe à ce service.

©2005 Qbik New Zealand Limited

Passerelles (Gateways)

Commune à tous les services, **cette option** permet de déterminer quelle passerelle le service doit utiliser.

Par défaut, WinGate utilise la passerelle indiquée dans les propriétés réseau de la connexion Internet.



Masquer | Masquer toutes les images

Trois options sont disponibles :

1. **Utiliser toutes les connexions disponibles (*Use any available connection*)**

Option par défaut. WinGate utilise la passerelle indiquée dans les propriétés réseau de la connexion Internet.

2. **Utiliser l'une des connexions indiquées (*Use all Specified connections in rotation*)**

En cliquant sur **Ajouter (Add)**, il est possible de sélectionner les passerelles des interfaces détectées par WinGate (voir ci-dessous).

3. **Utiliser les connexions dans l'ordre de priorité (failover) (Use specified connections in priority order (failover))**

Avec cette option, vous indiquez un ordre de priorité pour l'utilisation des passerelles. Cela permet d'éviter les pannes : si une passerelle n'est plus disponible le service utilise la suivante.

Politique

Cette fenêtre s'affiche lorsque l'on clique sur **Ajouter**.

Masquer | Masquer toutes les images

Dans cette fenêtre figurent toutes les passerelles disponibles.

L'option **Adresse IP source (source IP Address)** permet de choisir l'adresse IP utilisée dans les paquets envoyés à la passerelle choisie. Il peut s'agir de n'importe quelle adresse utilisée par une interface dans le système d'exploitation sur le poste du serveur WinGate.

Remarque : détection de passerelle inactive

Le **service ENS** contient une option de détection de passerelle inactive (*Monitor for dead gateways*) qui facilite la sélection.

Masquer | Masquer toutes les images

Si le service découvre qu'une passerelle est inactive, elle ne peut pas être sélectionnée. De plus, l'interface ne peut être utilisée en tant qu'interface externe pour un service de WinGate car elle n'est pas en mesure d'exécuter les requêtes des clients.

Lorsque cette option n'est pas cochée, toutes les interfaces possédant une passerelle peuvent être sélectionnées, quel que soit leur état.

©2005 Qbik New Zealand Limited

Composeur (*Dialer*) - Général

Dans les **propriétés du composeur**, vous pouvez configurer les profils de connexion que WinGate a identifié dans votre système d'exploitation et permettre leur utilisation pour accéder à Internet. Tous les profils détectés seront automatiquement répertoriés.

Masquer

Vous devez **impérativement** configurer les profils que vous souhaitez utiliser. Pour cela, il suffit de double-cliquer sur un profil ou de le sélectionner puis de cliquer sur Propriétés. Les profils non configurés ne fonctionneront pas correctement.

Autoriser les clients distants à se déconnecter Lorsque cette option est activée, le composeur peut raccrocher (à l'aide de WinGate Dialup Monitor*) une fois que tous les clients sont déconnectés. Décochez cette option si vous souhaitez que le composeur reste connecté en permanence.

(Allow remote clients to disconnect) (Remarque : vous devez alors également décocher "Déconnecter après # secondes d'inactivité").

*WinGate Dialup Monitor - Applet apparaissant à droite de la zone de notification, lorsqu'une connexion Internet est lancée sur le serveur WinGate.

Composer (Dial) Lance la numérotation.

Arrêter (Stop) Interrompt la numérotation ou raccroche si WinGate est en ligne.

Remarques :

Si l'option **Connecter à l'aide de la liste** (*Connect as required using the connection list*) est cochée, le composeur effectuera automatiquement la numérotation pour le client. Dans le cas contraire, la connexion doit être effectuée manuellement.

Le composeur commence la numérotation avec le premier profil de la liste, et réessaie un certain nombre de fois avant de passer au profil suivant. Lorsqu'il atteint la fin de la liste, le cycle est répété autant de fois d'indiqué dans le champ **Recommencer toutes les X fois** (*Retry all X time(s)*).

©2004 Qbik New Zealand Limited

Composeur - Configuration des profils

Tous les profils du système d'exploitation figurent dans la fenêtre **Général** des propriétés du Composeur.

Pour utiliser un profil avec WinGate, vous devez le sélectionner et cliquer sur **Propriétés (Properties)**, puis indiquer les informations requises dans **la fenêtre** qui s'ouvre ensuite.

Masquer

Cochez ensuite l'option **Autoriser WinGate à utiliser cette connexion (*Enable this connection to be used by WinGate*)** et indiquez votre nom d'utilisateur et votre mot de passe. Le champ **Domaine** permet uniquement de s'authentifier sur un domaine NT. En règle générale, vous pouvez laisser ce champ vide, car la plupart des FAI ne l'exigent pas.

Utilisateurs NT/2000 :

La première fois que vous accédez à cette option, votre nom d'utilisateur NT figure déjà dans le champ correspondant.

Vous devez par contre indiquer votre mot de passe.

Utilisateurs 95/98/ME :

Si vous ne remplissez pas les champs du nom d'utilisateur et du mot de passe, WinGate utilise vos identifiants par défaut, s'il les possède.

Ces informations figurent dans les paramètres de connexion de Windows.

©2005 Qbik New Zealand Limited

Composeur - Sites locaux (*Local sites*)

[Cliquez ici pour une copie d'écran](#)

Masquer

Indiquez ici la liste des IP pour lesquelles vous ne souhaitez pas autoriser de connexion. Toute connexion vers un site contenant l'un des mots de la liste sera refusée.

Conseils :

Nous vous recommandons d'inclure dans cette liste : **localhost**, **127.0.0.1**, WinGate (le nom Netbios de votre PC passerelle) et l'IP du serveur WinGate.

Si vous ajoutez des mots comme **micro**, la connexion sera impossible pour microsoft.com ou l'un de ses sous domaines, microtest.com etc.

Si vous ajoutez un point (".") à cette liste, vous n'aurez de connexion pour aucune adresse car tous les noms en contiennent un.

Composeur - Paramètres (*Settings*)

[Cliquez ici pour une copie d'écran](#)

Masquer

Options de journalisation (*Logging*)

Numérote/raccroche

(*Dialing/Hanging up*) Enregistre les modifications du statut de connexion.

Débogage (*Debug*)

Enregistre les messages de débogage. Ne cochez cette option que si vous rencontrez des problèmes avec le composeur.

Options avancées

Intervalle de vérification (*Online status check update interval*)

L'état du composeur est vérifié à la fréquence indiquée. Vous pouvez réduire cette valeur si le risque d'échec est élevé (par exemple si la connexion est mauvaise).

Numérotation Rasdial synchrone (*Use synchronous Rasdial call*)

Utiliser en cas de problème avec le Rasdial.

Annuler la numérotation en cas d'échec après ... secondes (*Abort dial if not completed within ... seconds*)

Cette option, configurable en millisecondes, s'utilise pour les numérotations qui n'aboutissent pas après le temps imparti.

Attendre ... secondes

Si votre FAI est occupé, il est recommandé

avant de réessayer d'attendre quelques instants avant de numéroté à
(Wait ... seconds between nouveau.
redial attempts)

©2004 Qbik New Zealand Limited

Méthodes de connexion des clients

WinGate dispose de trois méthodes différentes :

NAT (Network Address Translation)

WGIC (WinGate Internet Client)

Proxy

Le choix de la méthode est très important, c'est pourquoi nous vous présentons chacune d'entre elles.

NAT

NAT signifie *Network Address Translation*, c'est à dire "traduction d'adresses réseau". L'adresse IP utilisée à l'intérieur d'un réseau est traduite en une adresse connue au sein d'un autre réseau (Internet par exemple). Bien qu'il soit légèrement différent, ce service est parfois appelé ENS (Extended Network Services : Service réseau avancé).

[Cliquez ici pour en savoir plus sur le fonctionnement du NAT.](#)

[Cliquez ici pour en savoir plus sur la configuration des clients avec le NAT.](#)

Avantages

Permet le partage d'une connexion Internet de façon rapide et continue.

Solution la plus facile à utiliser. En effet, ses fonctionnalités sont assez réduites, ce qui diminue d'autant le risque d'erreurs.

Très flexible : toute plateforme supportant les protocoles TCP/IP (Windows, Mac, Unix, Linux) ainsi que quasiment tous les logiciels clients (navigateurs Internet, logiciels de messagerie, forums, FTP, etc.) peuvent bénéficier de connexions partagées.

Il n'est pas nécessaire d'installer un logiciel ou de configurer une application.

L'intégration avec les proxies s'effectue facilement.

Inconvénients

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

Conclusion

Pour de nombreux utilisateurs, le NAT est la solution idéale. Il convient particulièrement aux réseaux LAN de grande taille où l'administrateur ne veut pas être obligé d'installer de logiciels supplémentaires et/ou de configurer des applications sur plusieurs ordinateurs.

WGIC

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

[Cliquez ici pour en savoir plus sur l'installation de WinGate Internet Client.](#)

Avantages

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

Versatile.

Compatible avec un grand nombre de jeux en réseau.

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).

Inconvénients

Il est nécessaire d'installer le logiciel.

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.

Proxy

([Cliquez ici pour en savoir plus sur la configuration des clients avec la méthode proxy](#))

Au sens propre le terme "proxy" signifie "mandataire", c'est à dire une personne qui agit au nom d'une autre personne. Sur Internet, ce mot à la même signification : WinGate est un programme qui agit au nom d'autres programmes.

Plus précisément, il effectue des requêtes sur Internet auprès de serveurs au nom de ses clients. Il s'agit donc d'un intermédiaire entre les utilisateurs et Internet, ce qui présente de nombreux avantages tant au niveau de la sécurité que du contrôle et des possibilités de mise en cache.

N'oubliez pas que c'est WinGate et non GateKeeper qui joue le rôle de mandataire. 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 présents 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.

Les proxies interfèrent davantage avec le trafic : le risque d'erreur est plus élevé.

Conclusion

Puisque le NAT et WGIC disposent à présent des mêmes avantages, il n'est presque plus nécessaire d'utiliser de proxy de façon directe.

Remarque :

Il est possible d'intégrer les trois méthodes. [Cliquez ici pour en savoir plus.](#)

Comparatif des méthodes de connexion pour les clients

Le tableau ci-dessous présente les trois méthodes de connectivité Internet utilisées dans WinGate.

Il vous permettra de choisir la méthode qui correspond le mieux à vos attentes. Lorsque vous connaîtrez suffisamment les avantages et inconvénients de chacune d'entre elles, vous pourrez apprendre à utiliser le NAT avec WGIC et les proxies WinGate.

NAT : meilleure solution en termes de facilité, compatibilité et rapidité.

WGIC : ses principaux avantages sont : la possibilité de recevoir des connexions entrantes, ainsi qu'un contrôle efficace de votre connexion grâce à de nombreuses fonctionnalités, et un niveau de sécurité élevé.

Proxies : se distinguent par leurs fonctionnalités et le niveau de sécurité.

Pour une utilisation optimale vous devez connaître chacune de ces trois méthodes.

Propriétés	NAT	WGIC	Proxies
PC client facile à configurer	***	**	*
Rapide	***	**	**
Sécurisé	**	***	***
Fonctionnalités	*	**	***
Compatible avec les systèmes d'exploitation	***	*	**
Compatible avec les autres logiciels	***	***	**
Accepte les connexions entrantes provenant d'autres ordinateurs	*	***	**

WinGate Internet Client (WGIC)

WGIC est une application qui comme son nom l'indique s'installe sur les postes clients. Il identifie le serveur WinGate sur le réseau à l'aide du protocole GDP (Generic Discovery Protocol), puis communique directement avec ce dernier grâce au service WRP (Winsock Redirector Protocol) de WinGate.

Une fois WGIC installé, toutes les requêtes du poste client provenant d'applications WinSock sont interceptées et exécutées par le service WRP sur le serveur. Les administrateurs contrôlent ainsi de façon efficace l'utilisation d'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 (et surveiller ainsi l'activité).

Permet le contrôle des centralisé des politiques dans WinGate (service WRP).

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

Inconvénients

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

Compatible uniquement avec 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 en savoir plus sur l'installation et l'utilisation de WinGate Internet Client](#)

©2005 Qbik New Zealand Limited

Installation de WinGate Internet Client

Configuration requise

Avant de procéder à l'installation, 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](#)

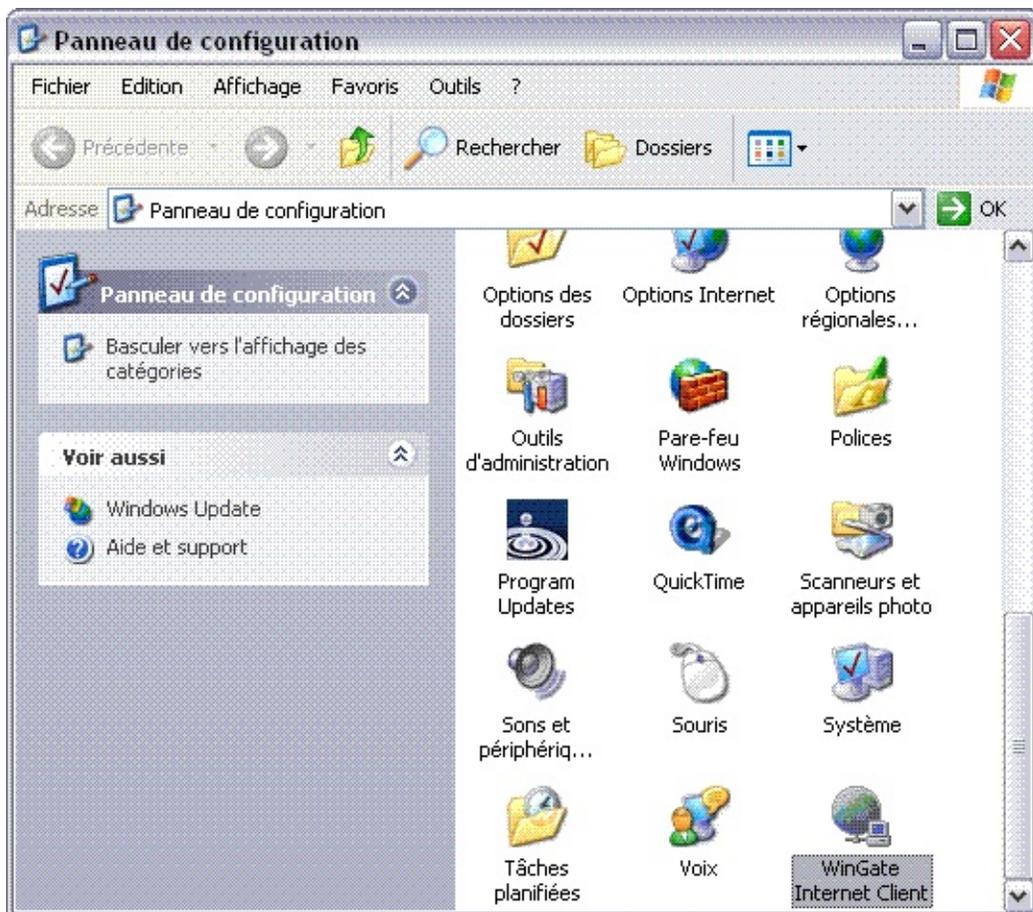
[Le protocole TCP/IP](#) doit être installé et doit [fonctionner correctement](#).

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.

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** (Démarrer/Paramètres/Panneau de configuration).



Masquer

Configuration des applications avec WGIC

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 les supprimez pas, vos applications fonctionneront, mais par le biais des proxies de WinGate et non de WGIC.

Pour utiliser le service NAT, vous devez configurer les postes clients.

([Cliquez ici pour en savoir plus sur l'intégration du NAT avec WGIC.](#))

©2004 Qbik New Zealand Limited

Configuration des clients avec le NAT

La procédure est très simple :

La **passerelle par défaut** - dans les paramètres réseau des ordinateurs clients - doit être configurée sur l'adresse IP privée du serveur WinGate. Ce paramètre fait partie des propriétés TCP/IP et peut être configuré de diverses façons :

Automatiquement, à l'aide du serveur **DHCP de WinGate (méthode recommandée)**.

En utilisant un autre serveur DHCP sur votre réseau, et en paramétrant les options de passerelle (routeur), et DNS sur l'adresse IP privée du serveur WinGate (déconseillé).

En configurant manuellement les paramètres réseau des ordinateurs clients.

Remarque :

Un serveur DNS doit tout de même figurer dans les paramètres réseau des clients NAT, mais cela ne doit pas correspondre obligatoirement à l'adresse IP du serveur WinGate.

Configuration des clients avec les proxies

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 :

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 en savoir plus sur l'intégration des proxies avec le NAT.](#)

Intégration des méthodes de connexion

Dans WinGate, il est possible d'intégrer les différentes méthodes de connexion afin de pouvoir les utiliser simultanément. Ainsi, votre serveur est à même de répondre à quasiment tous les besoins en termes de connectivité sur Internet.

Vous pouvez configurer chaque application en fonction de la méthode qui convient le mieux.

Cela peut être facilement réalisé pour des applications se trouvant sur un même ordinateur ou réseau, car chacune des méthodes (NAT, WGIC et les proxies de WinGate) fonctionne de façon totalement indépendante.

NAT et WGIC

Cette solution convient particulièrement aux postes clients exécutant leurs applications sous Windows.

Le partage de la connexion Internet entre les utilisateurs est optimisé, et vous pouvez contrôler les applications de façon efficace à l'aide de WGIC.

Par défaut, toutes les applications clientes utilisent WGIC pour se connecter à Internet. Si vous souhaitez qu'une application spécifique utilise le NAT vous devez configurer WGIC pour qu'il l'ignore.

Pour utiliser le **NAT** et **WGIC** sur le même poste :

1. Assurez-vous que la passerelle par défaut soit dirigée vers le serveur WinGate (opération effectuée automatiquement par le service **DHCP**).
2. Vérifiez que les applications clientes soient configurées pour se connecter **directement** à Internet.
3. Installez **WGIC** sur le poste client (par défaut, tous les clients l'utilisent).
4. Dans le Panneau de configuration, ouvrez l'applet **WinGate Internet Client**.
5. Cliquez sur **Ajouter** dans l'onglet **Application**.
6. Sélectionnez l'application avec laquelle vous souhaitez utiliser le NAT,

par exemple "Netscape.exe". Cliquez sur **Parcourir** si vous ignorez son nom exact.

7. Cochez l'option **Accès uniquement au réseau local (*Local network access only*)** afin que WGIC ignore cette application.
8. Effectuez cette opération pour chaque application que vous souhaitez utiliser avec le NAT.
9. Cliquez sur **Appliquer** puis sur **OK**.

NAT et proxy

Dans la plupart des cas, le NAT et WGIC suffisent à satisfaire toutes les exigences en matière de partage de connexions Internet. Toutefois, les proxies peuvent parfois s'avérer nécessaires.

Si vous souhaitez utiliser un proxy, vous devez configurer séparément chaque application.

Pour cela, indiquez l'adresse IP du serveur WinGate et le numéro de port utilisé par le service (affiché à côté du service dans GateKeeper).

Avec la [Redirection transparente](#), le NAT peut utiliser des proxies pour les principaux services (comme les serveurs web et FTP).

Remarque :

Si configurez une application pour qu'elle utilise un proxy, elle ne pourra pas accéder au NAT.

La sécurité dans WinGate

WinGate propose un niveau de sécurité élevé, ainsi qu'une comptabilité de l'utilisation d'Internet très flexible.

Les fonctionnalités de sécurité fonctionnent selon différents concepts.

Utilisateurs

Un utilisateur est une personne qui bénéficie des services de WinGate. Vous pouvez créer des utilisateurs et groupes à partir de GateKeeper (ou les importer à partir de NT ou d'un fichier texte), ou bien intégrer une base de données NT/2000 dans WinGate.

Avec WinGate, vous pouvez enregistrer les audits et la comptabilité de chaque utilisateur et gérer leurs droits et privilèges (que ce soit avec une base de données WinGate ou NT).

Les liens ci-dessous renvoient à des informations sur la gestion des bases de données WinGate. Cependant, si votre serveur est sous Windows NT ou 2000, nous vous recommandons d'intégrer une base de données NT (l'authentification est plus sûre et la base de données plus fiable).

[Cliquez ici pour savoir comment ajouter un nouvel utilisateur](#)

[Cliquez ici pour savoir comment ajouter un groupe](#)

[Cliquez ici pour en savoir plus sur la gestion des utilisateurs/groupes en utilisant la base de données de WinGate](#)

Ordinateurs

Il s'agit des postes connectés à WinGate via le réseau local. Chaque ordinateur est identifié en fonction de son adresse IP privée (les adresses ne sont attribuées automatiquement que si vous utilisez le service DHCP).

WinGate peut être configuré afin d'effectuer certaines déductions quant à l'identité de l'utilisateur d'un poste donné. Par exemple, si John est la seule personne à l'utiliser l'ordinateur PCDEJOHN dont l'adresse IP privée est

192.168.0.55, il est possible de présumer que John est responsable de toute l'activité provenant de ce poste (et donc d'appliquer une politique en conséquence).

Cela correspond au niveau d'authentification de l'utilisateur. Par défaut, les utilisateurs non authentifiés sont inconnus, WinGate n'effectue ces "déductions" que lorsque vous le précisez.

Il existe trois niveaux d'authentification :

Niveau	Signification
Inconnu	WinGate ne connaît pas cet utilisateur.
Présumé	WinGate présume l'identité de l'utilisateur, en fonction de l'adresse IP ou du nom de l'ordinateur à partir duquel il se connecte. De plus, les utilisateurs peuvent bénéficier d'une authentification non sécurisée dans Telnet ou SOCKS 5 afin d'avoir le statut "d'utilisateur présumé" (moins sécurisé que le niveau "authentifié").
Authentifié	WinGate a vérifié l'identité de l'utilisateur, car il a fourni un nom d'utilisateur et un mot de passe. Il existe pour cela différentes méthodes.

Remarque :

Avant d'appliquer des politiques, vous devez bien connaître les concepts d'utilisateurs, groupes et niveaux d'authentification dans WinGate .

[Cliquez ici pour en savoir plus sur l'utilisation des politiques dans WinGate.](#)

Choix de la méthode d'authentification pour les bases de données d'utilisateurs

Afin de pouvoir appliquer les politiques de contrôle des utilisateurs et groupes, les administrateurs doivent choisir la base de données à utiliser pour leur authentification.

Il existe deux possibilités :

1. [Base de données d'utilisateurs WinGate](#)
2. [Base de données du système d'exploitation/distante](#)

La base de données de WinGate est sélectionnée par défaut, mais il est possible de modifier ce paramètre en cliquant sur **Bases de données (Database options)** dans l'onglet **Utilisateurs (Users)** de GateKeeper.

Remarques concernant l'authentification :

Les mots de passe NT et WinGate respectent la casse : "motdepasse", "Motdepasse" et "MOTDEPASSE" sont tous différents.

Une fois authentifiés, les utilisateurs ont accès aux services de WinGate pour toute la durée de la session.

Avec l'authentification NT, chaque utilisateur WinGate doit posséder un compte NT. Veuillez noter que si vous choisissez cette méthode, les utilisateurs WinGate ne correspondant à aucun compte NT risquent de disparaître.

WinGate n'enregistre/ne conserve jamais les mots de passe NT. Ils sont vérifiés à chaque connexion.

Il n'est pas possible d'utiliser l'authentification Java avec les mots de passe NT. Cette méthode ne fonctionne qu'avec la base de données d'utilisateurs de WinGate.

L'authentification NT est disponible avec les méthodes suivantes :

Authentification NTLM pour les proxys

Service WRP (via WGIC)

Service d'administration à distance (via GateKeeper).

Serveur POP.

Cependant, elle n'est **PAS** disponible avec (voir remarques ci-dessous) :

le service proxy web (via le client Java)

le proxy SOCKS5 (en texte clair, conformément à la RFC 1929)

le proxy Telnet (en texte clair).

Mots de passe WinGate

Cette fonctionnalité n'est disponible que si vous utilisez la base de données de WinGate (et non celle du système d'exploitation). Lorsque l'authentification est exigée, les noms d'utilisateurs et mots de passe sont comparés à ceux enregistrés sur le serveur.

Remarque :

Si les comptes ont été importés (d'un fichier texte ou de NT) le champ du mot de passe n'est pas rempli, vous devez donc en choisir un. Dans WinGate, les mots de passe sont enregistrés sous forme cryptée.

Mots de passe Windows NT / 2000

Fonctionnalité la plus sécurisée. Elle n'est disponible que si vous utilisez la base de données du système d'exploitation. Les utilisateurs peuvent alors s'authentifier dans WinGate avec leurs identifiants et mots de passe NT. WinGate essaie en premier lieu d'utiliser l'identifiant correspondant à la session actuelle de l'utilisateur, qu'il soit connecté sous Windows NT, 2000, 95, 98 ou ME. En cas d'échec, l'utilisateur devra indiquer son identifiant NT. WinGate vérifie ensuite le mot de passe : les mots de passe NT ne sont jamais enregistrés dans WinGate.

Remarque :

Si les comptes ont été importés (d'un fichier texte ou de NT) le champ du mot de passe n'est pas rempli. Vous devez absolument en attribuer un à chaque utilisateur avant d'avoir recours à cette méthode.

©2004 Qbik New Zealand Limited

Base de données d'utilisateurs de WinGate

La gestion des utilisateurs et des groupes est une fonctionnalité clé de WinGate. Elle permet de créer des politiques de surveillance de l'accès aux principaux services.

Les politiques de WinGate se gèrent à partir d'une ou deux bases de données d'utilisateurs : la base de données de WinGate et/ou la base Windows NT/2000 ([cliquez ici pour en savoir plus sur l'intégration d'une base de données utilisateurs NT.](#))

Cette rubrique indique comment gérer des utilisateurs et groupes avec la base de données de WinGate (pas d'intégration NT / 2000).

Les licences **9x utilisateurs** sont limitées à ce type de gestion.

Remarques à propos des utilisateurs et des groupes :

La définition d'utilisateurs et de groupes n'est pas obligatoire dans WinGate. Cependant, elle améliore considérablement la gestion et le suivi de l'accès Internet.

Avec Windows 9x, vous pouvez utiliser uniquement la base de données de WinGate

Comptes par défaut

Compte Administrator

Le compte Administrator accède à **l'ensemble** des paramètres de configuration de WinGate et ne peut pas être supprimé. Lorsque vous installez WinGate pour la première fois, aucun mot de passe n'est défini pour ce compte et GateKeeper vous demande d'en créer un.

En laissant le champ vide, WinGate vous autorise à vous connecter à GateKeeper en local (localhost) mais pas à distance (en modifiant les liaisons). Cette mesure de sécurité a pour objectif d'empêcher que des utilisateurs non sollicités sur Internet (ou sur votre réseau local) ne piratent

votre configuration.

Un message système vous avertira si les liaisons du **Service d'administration à distance (*Remote control service*)** ont été modifiées.

Compte Guest

Le compte Guest n'est pas associé à un mot de passe par défaut et ne peut pas être supprimé. Il s'agit du compte auquel les utilisateurs inconnus accèdent par défaut. D'une manière générale, il leur ouvre droit à l'ensemble des services mais ne leur octroie pas de droits d'administration. Vous pouvez réduire ou augmenter ces droits selon la politique de sécurité de votre réseau.

Utilisateurs présumés

WinGate est capable de déduire l'identité d'un utilisateur à partir de l'adresse IP ou du nom de réseau de son ordinateur. Cette fonctionnalité est utile si vous souhaitez surveiller vos utilisateurs sans avoir recours à une authentification complète. Elle est d'autant plus pratique si chaque utilisateur du réseau emploie toujours le même ordinateur.

Restriction de l'accès Invité

Le statut d'un utilisateur est défini sur "**Guest**" lorsqu'il se connecte aux services WinGate depuis un emplacement inconnu (entrée vide), sans s'authentifier. Même si vous n'appliquez pas les règles de comptabilité (vous ne facturez pas les services), il peut être utile de savoir qui utilise le plus Internet. Vous pouvez également exiger un solde positif pour certains utilisateurs.

Définir des **comptes utilisateur partagés**, autrement dit des comptes pouvant être utilisés par plusieurs personnes, permet de surveiller les habitudes d'un groupe. Cette configuration est souvent utilisée dans les écoles : une classe entière se sert d'un seul compte utilisateur (ex.: Classe 4) et le professeur dispose de son propre compte et figure dans le groupe Admin. Elle permet de surveiller les habitudes de ce groupe et vous évite de définir plusieurs comptes.

Le statut d'**utilisateur présumé** évite de saisir son identifiant à chaque fois.

Cette fonction est notamment utile lorsqu'un ordinateur est toujours utilisé par la même personne.

Si vous avez défini des liaisons sécurisées, personne ne pourra accéder à votre réseau de l'extérieur.

([En savoir plus sur le statut d'utilisateur présumé](#))

Précautions et autres remarques

Vous pouvez mettre en place les politiques suivantes :

1. Autoriser l'administration seulement à partir du serveur WinGate, ou d'un ordinateur prédéfini sur le réseau.
2. Demander une authentification ou pas.
3. Définir des comptes séparés pour chaque administrateur.
4. Demander une authentification et créer des comptes utilisateurs partagés (ex.: par classe, voir ci-dessous).
5. Appliquer des restrictions de compte aux groupes et aux utilisateurs pour surveiller les accès.
6. Définir des groupes par service (marketing, comptabilité, commercial).

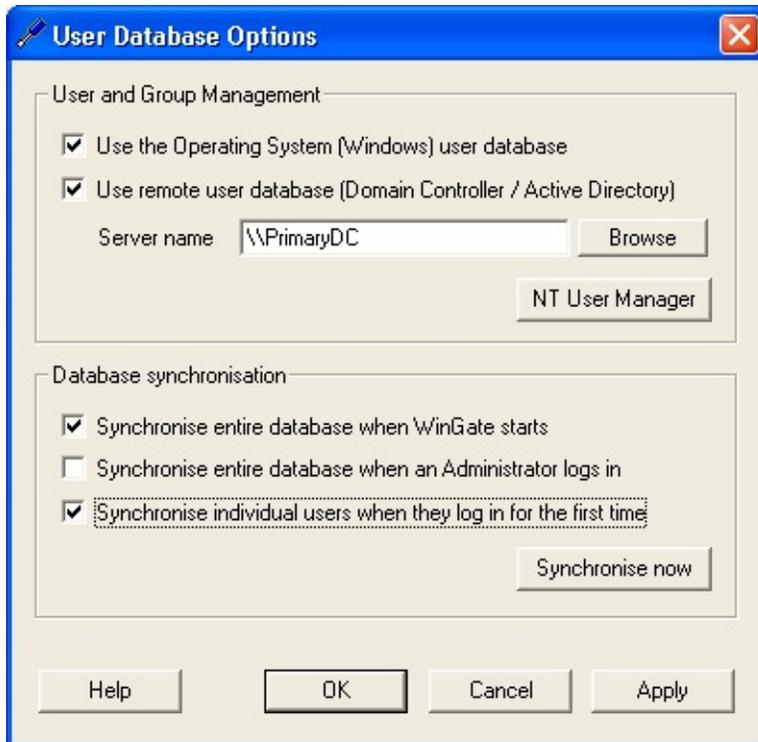
Base de données du système d'exploitation/distante

Les administrateurs ont la possibilité d'utiliser la base de données du système d'exploitation ou bien une base distante afin de contrôler l'activité de WinGate. Toutefois, cette fonctionnalité n'est disponible que sous Windows NT/2000/XP Pro/2003 (.Net server).

Par défaut, WinGate utilise sa propre base de données d'utilisateurs (sauf si lors de l'installation, vous avez coché l'option permettant d'utiliser celle du système d'exploitation).

Pour utiliser la base de données Windows/une base distante :

1. Cliquez sur l'onglet **Utilisateurs (Users)** dans le panneau Contrôle de GateKeeper
2. Double-cliquez sur **Bases de données (Database Options)**.
3. Sélectionnez l'une des options suivantes : **Utiliser la base de données du système d'exploitation (Windows) (Use the operating system (Windows) user database)**, ou **Utiliser une base de données à distance (Active Directory/Contrôleurs de domaine) (Use remote user database)**
4. Choisissez les options de synchronisation souhaitées (ou cliquez sur **Synchroniser (Synchronise now)** pour effectuer immédiatement la synchronisation)
5. Cliquez sur **OK** pour appliquer les modifications
6. Les utilisateurs et groupes de la base de données choisie apparaissent alors dans l'onglet **Utilisateurs** de GateKeeper.



Masquer

Gestion des utilisateurs et groupes (*User and Group management*)

Utiliser la base de données du système d'exploitation (Windows) (*Use the Operating System (Windows) user database*)

Permet d'utiliser la base de données du poste sur lequel WinGate est installé.

Utiliser une base de données à distance (*Use remote user database (Domain Controller/Active Directory)*)

Permet d'utiliser la base de données d'un contrôleur de domaine dans un environnement NT ou Active Directory

(voir ci-dessous)

Gestion des utilisateurs NT (*NT User Manager*)

Ouvre la MMC "Utilisateurs et groupes locaux", afin de gérer directement vos

utilisateurs Windows.

Synchronisation de la base de données (*Database Synchronisation*)

Synchroniser toute la base au démarrage (*Synchronise entire database when WinGate starts*)

La base de données est synchronisée à chaque démarrage de WinGate.

Synchroniser toute la base lorsqu'un administrateur se connecte (*Synchronise entire database when an Administrator logs in*)

La base de données est synchronisée automatiquement à chaque fois qu'un utilisateur se connecte.

Synchroniser les utilisateurs se connectant pour la première fois (*Synchronise individual users when they log in for the first time*)

La synchronisation s'effectue lorsqu'un utilisateur inconnu essaie de s'identifier dans WinGate.

Synchroniser (*Synchronise Now*) :

Cliquez sur ce bouton pour mettre à jour instantanément la base de données.

Remarque :

Les utilisateurs et groupes ne peuvent être contrôlés que dans WinGate. Cette fonctionnalité ne permet pas de modifier les paramètres du système d'exploitation.

Synchronisation des bases de données à distance :

Si vous utilisez un contrôleur de domaine **Active Directory** pour votre base de données, vous devez également effectuer l'opération suivante :

1. Sur le serveur WinGate, allez dans **Panneau de configuration/Outils d'administration/Services et applications** (contient la liste de tous les services).
2. Effectuez un clic droit sur **Qbik WinGate Engine service** et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Connexion**.
4. Dans la section **Ouvrir une session en tant que**, sélectionnez **Ce compte** et indiquez un compte Active Directory possédant des privilèges équivalents à ceux d'un Administrateur de domaine. (Il est recommandé de créer un compte spécifique dans Active Directory, utilisé à cet effet.)
5. Redémarrez WinGate afin que les modifications soient prises en compte.
6. Synchronisez à nouveau la base de données dans GateKeeper.

Avec Active Directory, les utilisateurs et groupes sont gérés à partir de la MMC "Utilisateurs et ordinateurs Active Directory", située dans chaque contrôleur de domaine. La gestion des utilisateurs et groupes locaux n'est pas disponible sur le poste WinGate lorsque l'option **Utiliser la base de données du système d'exploitation (Windows)** est activée.

Veillez noter que l'option de base de données à distance n'est disponible qu'avec WinGate 6 Pro et Enterprise.

Ajouter un utilisateur

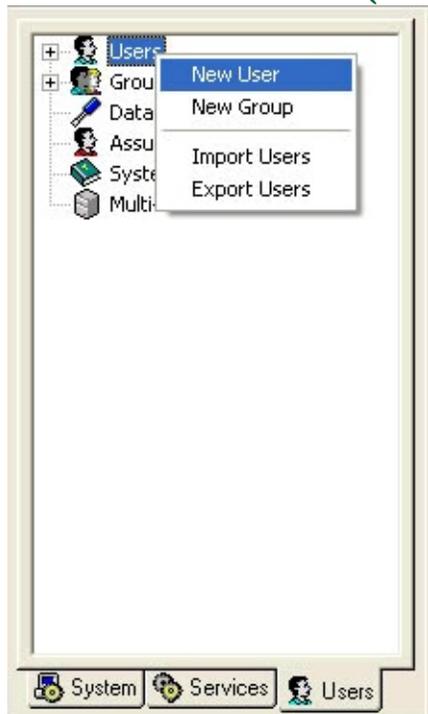
Si vous créez les comptes utilisateurs et groupes dans la base de données de **WinGate**, vous pouvez ensuite instaurer une politique par utilisateur et par groupe.

Cela vous permet de contrôler de façon plus efficace l'accès à Internet depuis vos réseaux, grâce à des fonctionnalités comme : des restrictions appliquées en fonction du lieu/de l'heure, la comptabilité et l'audit.

Créer un nouveau compte :

Lorsque vous créez un nouvel utilisateur, les paramètres sont basés sur un modèle par défaut. Pour modifier ces paramètres :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet Utilisateurs (*Users*) dans le panneau Contrôle.
4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet puis sur **Nouvel utilisateur (New User)**.



Masquer | Masquer toutes images

5. Remplissez le champ **Nom d'utilisateur (Username)**.
6. Indiquez son **Nom réel (Real name) (facultatif)**.
7. Demandez à l'utilisateur d'entrer et de confirmer son **mot de passe**, ou laissez ce champ vide et cochez **L'utilisateur doit changer de mot de passe à la prochaine connexion (User must change password next logon)**.
8. Indiquez sa **description**, par exemple : support technique.
9. Configurez les différentes options.
10. Cliquez sur **OK**.

Remarque :

Les caractères suivants ne peuvent figurer dans le nom d'utilisateur : [] + = \ / : ; , * ? < > " |

Cloner un utilisateur :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet **Utilisateurs** dans le panneau Contrôle.
4. Effectuez un clic droit sur l'un des utilisateurs.
5. Cliquez sur **Cloner**.
6. Indiquez le **nom**, la **description** et le **mot de passe** du nouvel utilisateur.
7. Configurez les options souhaitées puis cliquez sur **OK**.

Modifier le modèle par défaut :

Ce modèle possède une configuration minimale.

Si vous souhaitez en modifier les paramètres, créez un utilisateur appelé : "**default**". Toutes les options sélectionnées le seront ensuite pour chaque nouvel utilisateur.

Procédure à suivre :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte Administrator.
3. Cliquez sur l'onglet **Utilisateurs** dans le panneau Contrôle.
4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet puis sur **Nouvel utilisateur**.
5. Appelez-le "**default**".
6. Modifiez tous les paramètres que vous souhaitez appliquer par défaut.
7. Vous pouvez ainsi instaurer un **mot de passe** par défaut, ainsi que des paramètres de **connexion, groupes, audit** et **comptabilité**.
8. Cliquez sur **OK**.

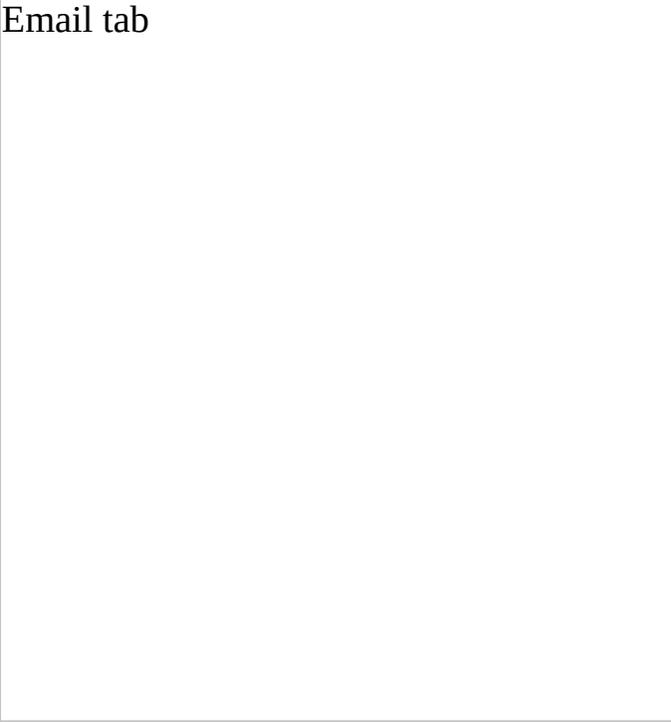
Tous les utilisateurs créés par la suite auront la même configuration que "**default**", vous n'aurez plus qu'à modifier le nom.

Onglet E-mail

Cliquez ici pour une copie d'écran

Dans cet onglet, vous pouvez créer des alias pour les adresses de vos utilisateurs, correspondant aux comptes de la base de données WinGate.

Email tab



Masquer

L'utilisateur possède une boîte sur ce serveur (*This user has an email box on this server*)

Si cette option n'est pas cochée, aucune autre option n'est disponible.

Adresses actuellement utilisées (*Current effective addresses*)

Liste des adresses actives sur ce serveur.

Limiter la capacité de la boîte à ? Mo (*Limit mailbox capacity to ? MB*)

Cette limite est différente pour chaque utilisateur.

Mot de passe POP3 prioritaire (*Override password for POP3*)

Vous pouvez choisir un mot de passe différent pour les comptes POP3.

Options IMAP4

Ces deux options ne sont disponibles que si la boîte aux lettres de l'utilisateur est une boîte IMAP4.

Supprimer les messages marqués comme tels (*Automatically remove messages marked for deletion*)

Certains clients (comme Thunderbird, Outlook ou Outlook Express) ne font que marquer les messages comme supprimés mais ne le suppriment pas. Cochez cette option si vous souhaitez que WinGate supprime automatiquement les messages marqués comme tels.

Corriger les messages envoyés par Eudora (*Clean messages appended by Eudora*)

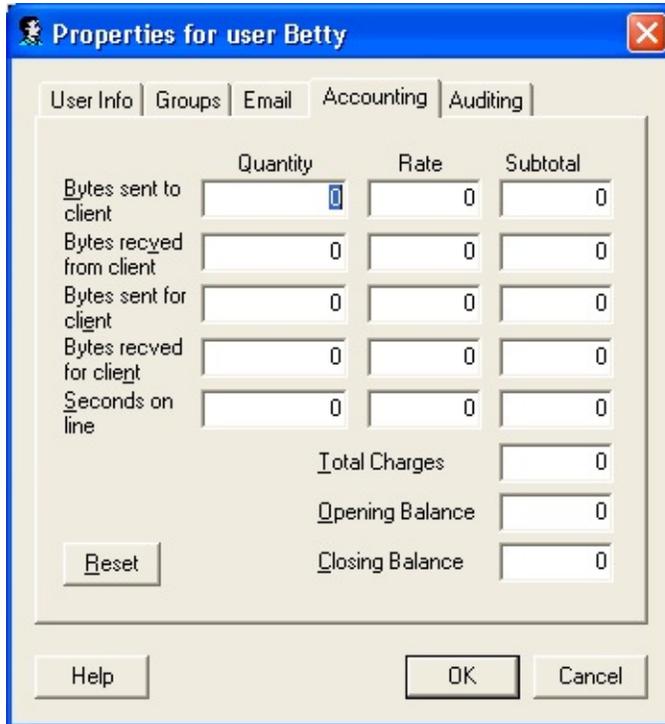
Eudora configure certains en-têtes de façon incorrecte, ce qui peut laisser des balises dans le contenu du message. Par conséquent, les e-mails envoyés avec Eudora ne s'affichent parfois pas correctement dans les autres clients.

Remarque :

Si un utilisateur possède une boîte IMAP4, les messages seront enregistrés dans le dossier **WinGate\Mail\IMAP\"Nomd'utilisateur"**.

Comptabilité

Situé dans les propriétés de chaque utilisateur, **cet onglet** facilite la gestion de votre réseau.



The screenshot shows a Windows-style dialog box titled "Properties for user Betty". It has five tabs: "User Info", "Groups", "Email", "Accounting", and "Auditing". The "Accounting" tab is selected. The dialog contains a table with the following data:

	Quantity	Rate	Subtotal
Bytes sent to client	0	0	0
Bytes recved from client	0	0	0
Bytes sent for client	0	0	0
Bytes recved for client	0	0	0
Seconds on line	0	0	0
		Total Charges	0
		Opening Balance	0
		Closing Balance	0

Below the table is a "Reset" button. At the bottom of the dialog are "Help", "OK", and "Cancel" buttons.

Masquer

Les informations qu'il contient sont mises à jour en temps réel lorsque l'utilisateur est connecté à Internet.

Les totaux sont remis à zéro à la fin de chaque session, et le temps de connexion est remis à zéro lorsque toutes les sessions de données sont terminées. Les tableaux ci-dessous illustrent le fonctionnement de la comptabilité.

Données

Octets

envoyés au client Nombre d'octets que WinGate a envoyés au poste client. En cas d'utilisation du proxy web, ces données proviennent en grande partie de la mémoire cache.
(Bytes sent to client)

Octets reçus du client

(Bytes received from client) Nombre d'octets envoyés par le client à WinGate.

Octets envoyés pour le client

(Bytes sent for client) Données que WinGate envoie aux serveurs pour le compte du client. Cette valeur est généralement différente du nombre d'octets reçus du client.

Octets reçus pour le client
(Bytes received for client)

Données que WinGate reçoit pour le compte du client. Cette valeur est généralement inférieure au nombre d'octets envoyés au client (à cause de la mise en cache).

Tps de connexion (s)
(Seconds online)

Nombre de secondes écoulées depuis que le client est connecté à WinGate. Veuillez noter que cette valeur n'indique pas le temps que l'utilisateur a passé sur Internet. En effet, il est tout à fait possible d'être connecté à WinGate sans pour autant consulter Internet. Cette valeur est remise à zéro lorsque toutes les sessions sont terminées, c'est à dire lorsque l'utilisateur se déconnecte.

Tarifs

Indiquez le tarif applicable par méga-octets ou par secondes. En règle générale, seuls les octets reçus et envoyés POUR le client sont pris en compte.

Total des charges

(Total charges) Montant des charges à payer.

Solde d'ouverture

(Opening Balance) Somme que l'utilisateur a payée jusqu'à présent.

Solde de fermeture

(Closing Balance) Correspond au solde d'ouverture moins le total des charges.

Annuler

(Reset) Remet à zéro tous les champs de la colonne "Quantités". Attention, il n'y a pas de message de confirmation : en cas d'erreur cliquez sur Annuler.

Il est possible de configurer le **Programmateur (Scheduler)** afin d'exporter ou de remettre à zéro les informations concernant l'utilisateur.

Exemples :

Précisez une somme (par ex. : 20 €) que vous attribuez à l'utilisateur. Si la valeur du solde de fermeture est négative, il doit payer cette somme.

L'utilisateur paie une certaine somme (solde d'ouverture). Il peut ensuite utiliser Internet tant que le solde est positif, puis l'accès est coupé dès que cette valeur est égale à zéro. (Solution idéale pour les cybercafés.)

©2004 Qbik New Zealand Limited

Audit des utilisateurs

Les fonctionnalités avancées de contrôle fournissent aux administrateurs des informations complètes sur l'activité de WinGate.

L'activité des utilisateurs est contrôlée à l'aide de l'onglet **Audit** et les informations correspondantes sont enregistrées dans les [fichiers d'audit](#).



Masquer

Ces fichiers sont dans un format délimité par des tabulations et peuvent être consultés dans un éditeur de texte ou bien dans le [serveur de fichiers journaux](#).

Ils sont enregistrés par défaut dans le dossier :

`%WinGate%\audit\nomdel'utilisateur.log`

Ajouter un groupe

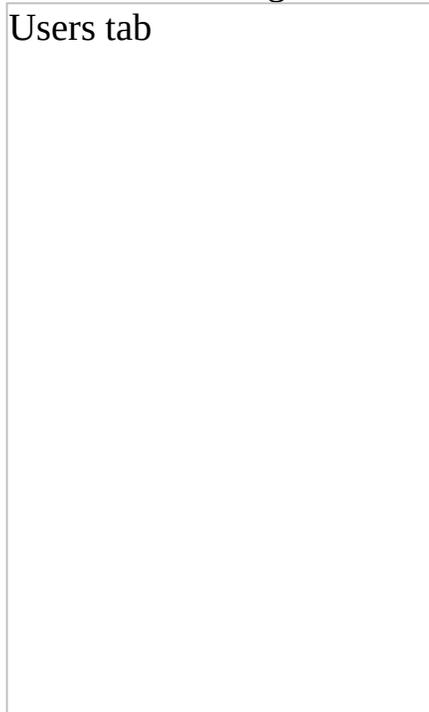
Les groupes sont des utilisateurs possédant des caractéristiques communes.

Un groupe peut contenir un nombre illimité d'utilisateurs, et être lui-même membre d'un autre groupe.

De plus, un utilisateur peut faire partie de plusieurs groupes différents. Les droits d'accès s'attribuent aussi bien par utilisateur que par groupe.

Ajouter un groupe :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Sélectionnez l'onglet **Utilisateurs (Users)** dans le panneau Contrôle.



Masquer | Masquer toutes les images

4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet et sélectionnez **Nouveau groupe (New Group)**.



Masquer | Masquer toutes les images

5. Une fenêtre s'ouvre, permettant de le configurer.
6. Indiquez son **nom** et sa **description**.
7. Double-cliquez sur un utilisateur non membre pour l'ajouter.
8. Cliquez sur **OK**.

Modifier un groupe :

1. Double-cliquez sur son nom dans l'onglet **Utilisateurs**.
2. Double-cliquez sur les **membres** que vous souhaitez **supprimer**.
3. Double-cliquez sur les **non membres** que vous souhaitez **ajouter**.

Remarque :

Si vous utilisez la base de données du système d'exploitation ou une base distante, vous ne pouvez ajouter des groupes qu'à partir de la MMC **Utilisateurs et groupes locaux** dans Windows.

©2004 Qbik New Zealand Limited

Import de comptes

Avec l'**Assistant d'import de comptes (User Import wizard)** vous importez dans votre base de données WinGate des utilisateurs et groupes depuis des fichiers textes. Le format de ces fichiers doit être délimité par des tabulations. WinGate n'est actuellement pas compatible avec les formats délimités par des virgules.

Vous importez autant d'informations que vous le souhaitez : noms d'utilisateurs, descriptions, noms réels, appartenance à des groupes, modèles, etc. (même les données de l'audit si elles ont été exportées dans un fichier texte par WinGate).

Cet outil peut s'avérer utile si vous décidez de migrer votre serveur ou de formater l'ordinateur. Il vous suffit alors d'exporter préalablement votre base de données dans un fichier texte à l'aide de l'**Assistant d'export de comptes (User Export Wizard)**. Il s'agit également d'une solution très rapide pour créer simultanément plusieurs comptes. De plus, l'Assistant peut être utilisé en association avec les modèles afin d'optimiser les performances.

Masquer

Ouvrir (Open)

Cliquez sur ce bouton pour sélectionner le fichier texte contenant les informations à importer (ce fichier doit impérativement être au format délimité par des tabulations).

Supprimer (Delete)

Après avoir sélectionné un fichier, vous pouvez supprimer de la liste les utilisateurs ou groupes que vous ne souhaitez pas importer.

Fusionner les groupes (*Merge Members if group exist*)

Si vous effectuez un import dans une base de données contenant déjà des

utilisateurs, les membres de groupes du même nom seront fusionnés dans un seul groupe.

Exemple :

Marc et Pierre font déjà partie du groupe Administrators. Vous importez un nouveau groupe Administrators contenant un membre appelé Jean. Si cette option est activée, une fois l'import effectué, le groupe Administrators sera composé de trois membres : Marc, Pierre et Jean.

Import d'utilisateurs et groupes :

1. Assurez-vous que les informations à importer soient dans un fichier texte au format souhaité (voir exemple dans le dossier \samples de WinGate).
2. Ouvrez **GateKeeper**.
3. Cliquez sur l'onglet **Utilisateurs (Users)** dans le panneau Contrôle.
4. Effectuez un clic droit à l'intérieur de cet onglet et sélectionnez **Importer (Import Users)**.
5. Dans l'Assistant, cliquez sur **Ouvrir (Open)** et sélectionnez le fichier texte.
6. Si vous ne souhaitez pas importer certains comptes, supprimez-les de la liste avant de cliquer sur **OK**.
7. Un message contenant les détails de l'import s'affiche.
8. Cliquez sur **OK**. Les comptes et groupes importés doivent figurer dans l'onglet **Utilisateurs (Users)**.

Remarques :

Pour des raisons de sécurité, les noms d'utilisateurs et de groupes respectent la casse (par exemple : "Marc", "marc" et "MARC" sont des noms différents).

Si un utilisateur contenu dans un fichier texte est déjà présent dans la base de

données il ne sera PAS importé. Cela permet d'éviter de remplacer des données par accident. Si vous souhaitez réellement remplacer les informations d'un compte, vous devez d'abord le supprimer.

Une fois l'import terminé, il est recommandé de supprimer le fichier texte (pour des raisons de sécurité).

Avant d'effectuer un import dans une base de données existante, il est conseillé de sauvegarder le registre de WinGate afin de pouvoir rétablir la configuration en cas de besoin.

Voir également :

[Export de comptes](#)

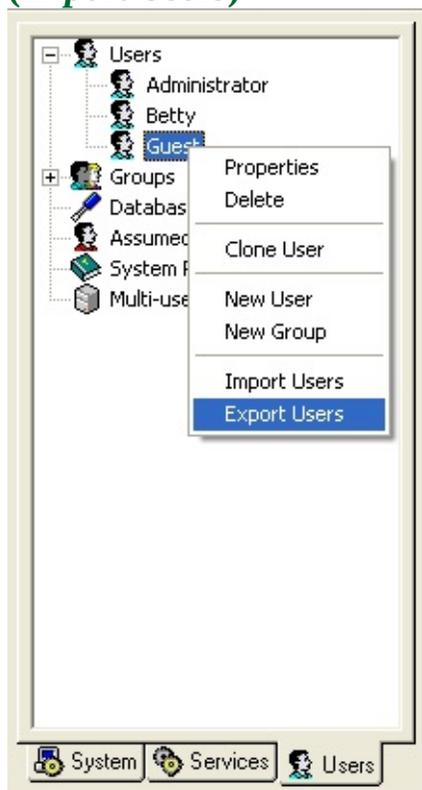
Export de comptes

Avec cette fonctionnalité, il est possible d'exporter les informations concernant tous les comptes dans un seul fichier.

Ce fichier est dans un format délimité par des tabulations afin de faciliter l'import dans une base de données.

Procédure à suivre

1. Ouvrez GateKeeper.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet **Utilisateurs** dans le panneau Contrôle.
4. Cliquez avec le bouton droit de la souris et sélectionnez **Exporter (Export Users)**



Masquer

5. L'**Assistant d'export de comptes** s'ouvre alors.



Masquer

Options de l'assistant :

Exporter dans le fichier (*Export to text file*)

WinGate vous propose un fichier par défaut mais vous pouvez indiquer le nom de fichier et le chemin de votre choix.

Type de fichier (*File Type*)

Format délimité par des virgules ou des tabulations.

Remarque :

WinGate ne peut importer que des informations contenues dans des fichiers au format délimité par des tabulations.

Champs :

Les champs exportés sont les suivants :

Horodatage

Nom d'utilisateur
Nom réel
Envoyé au client (octets)
Reçu du client (octets)
Envoyé au serveur (octets)
Reçu du serveur (octets)
Temps (secondes)
Ouverture
Fermeture

Exemple :

Même si le fichier semble confus, l'espace entre chaque champ correspond à une tabulation : il s'agit d'un format conçu pour l'importation des données.

```
11/11/97 15:44:04 mary-bob 80085 3053 0 0 1455 0 0
11/11/97 15:44:04 invité 194 0 0 0 0 0 0
11/11/97 15:44:04 marc 0 0 0 0 0 0 0
11/11/97 15:44:04 Administrator 173734 12906 0 0 6957 0 0
```

©2004 Qbik New Zealand Limited

Authentification des utilisateurs

Elle peut être effectuée de deux façons :

A l'aide de mots de passe WinGate (si vous utilisez la base de données intégrée de WinGate).

A l'aide de mots de passe Windows NT / 2000/XP Pro/.Net (2003) (si vous utilisez la base de données du système d'exploitation).

L'authentification permet à WinGate de déterminer quel utilisateur se connecte à quel service, et d'appliquer en conséquence la politique choisie par l'administrateur.

Nous vous recommandons de vous informer sur ces deux méthodes avant d'utiliser cette fonctionnalité.

[Choix de la base de données](#)

[Authentification à l'aide de la base de données WinGate](#)

[Authentification à l'aide de la base de données Windows NT / 2000](#)

Les utilisateurs peuvent s'authentifier - c'est à dire fournir un nom d'utilisateur et un mot de passe - pour accéder aux principaux services de WinGate à l'aide de quatre méthodes différentes :

Authentification pour le service WRP à l'aide de la fenêtre de connexion de WinGate Internet Client ([cliquez ici pour en savoir plus](#))

Connexion à distance avec GateKeeper (disponible uniquement avec WinGate Pro et Enterprise) ([cliquez ici pour en savoir plus](#))

Authentification pour un service proxy web à l'aide de l'applet de connexion Java ([cliquez ici pour en savoir plus](#))

Authentification pour un service proxy web à l'aide de l'applet de connexion NTLM dans Internet Explorer (ou tout autre navigateur supportant l'authentification NTLM) ([cliquez ici pour en savoir plus](#))

Remarques :

En complément des méthodes ci-dessus, il est possible de s'authentifier en tant qu'utilisateur présumé pour les services Telnet ou SOCKS 5 par le biais d'une authentification non sécurisée.

L'authentification NTLM pour le proxy web n'est disponible qu'avec les versions WinGate 6 Pro et Enterprise

©2004 Qbik New Zealand Limited

Méthodes d'authentification - GateKeeper

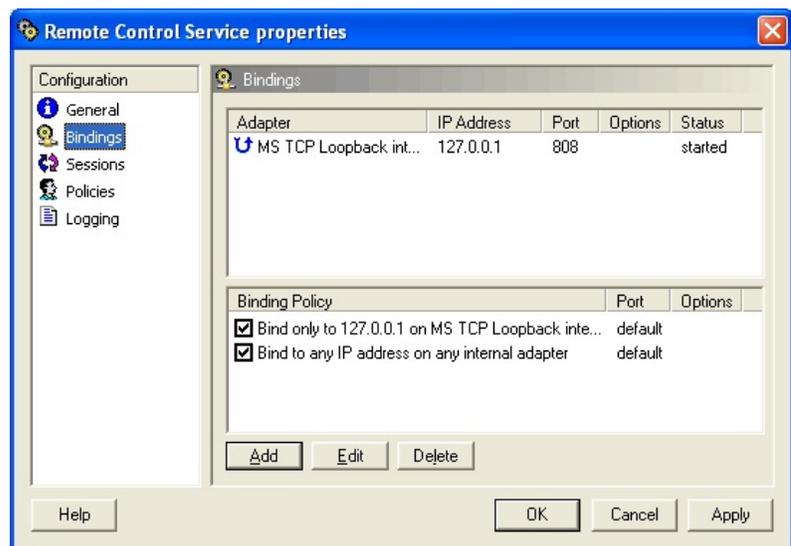
GateKeeper permet de contrôler et de configurer le moteur de WinGate.

Il communique avec le moteur par le biais du [Service d'administration à distance \(Remote control service\)](#), il s'agit donc du service pour lequel vous êtes authentifié (et du niveau d'authentification le plus élevé).

Utilisation de GateKeeper pour l'authentification des utilisateurs :

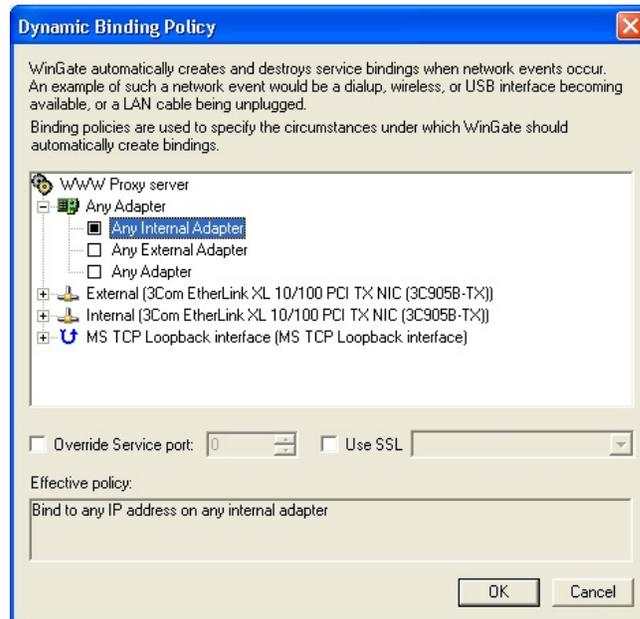
1. Configuration du Service d'administration à distance (*Remote Control Service*)

1. Ouvrez **GateKeeper**.
2. Dans l'onglet **Système**, double-cliquez sur **Service d'administration à distance (Remote Control Service)**.
3. Cliquez sur **Liaisons (Bindings)**, puis si aucune interface interne ne figure dans la fenêtre, cliquez sur **Ajouter (Add)**.



Masquer | Masquer toutes les images

4. Dans **la fenêtre** qui s'ouvre ensuite, sélectionnez une interface interne ou cochez l'option **Tous les adaptateurs internes (Any Internal adapter)**.



Masquer | Masquer toutes les images

5. Cliquez sur **OK**. L'interface figure à présent dans les liaisons.
6. Cliquez à nouveau sur **OK**.

2. Configuration de GateKeeper.exe

1. Copiez le fichier **GateKeeper.exe** du serveur/répertoire d'installation WinGate sur l'ordinateur distant.
2. Exécutez-le (sur l'ordinateur distant).
3. Indiquez les informations suivantes lors de l'**authentification** :



Masquer | Masquer toutes les images

- **Nom d'utilisateur (*Username*) :**

Un compte utilisateur WinGate (n'indiquez un compte Windows que si vous utilisez la base de données du système d'exploitation)

- **Mot de passe (*Password*) :**

Le mot de passe correspondant.

- **Serveur (*Server*) :**

Le nom ou l'adresse IP de l'ordinateur sur lequel se trouve WinGate.

- **Port :**

Port 808 (sauf si vous avez attribué un autre port au Service d'administration à distance).

Une fois authentifiés, les utilisateurs accèdent normalement à Internet sans devoir utiliser GateKeeper. Toutefois, si un utilisateur ne communique pas avec WinGate au-delà du délai défini dans le Service d'administration à distance, il devra à nouveau s'authentifier.

Si vous rencontrez des problèmes lors de la connexion, vérifiez les liaisons du service (assurez-vous que le service soit lié à l'interface sur laquelle vous recevez

votre connexion).

Remarque :

Si vous n'êtes pas connecté en tant qu'administrateur, il est impossible de lier ce service à une interface accessible au public (par ex. : Internet). Cela permet d'éviter que des personnes mal intentionnées ne se connectent à WinGate depuis Internet et modifient votre configuration.

Voir également :

[Accéder à GateKeeper à distance](#)

Méthodes d'authentification - WinGate Internet Client

Vous avez la possibilité d'exiger une authentification sécurisée des utilisateurs avec **WinGate Internet Client**.

Exiger l'authentification des utilisateurs pour le service **WRP** :

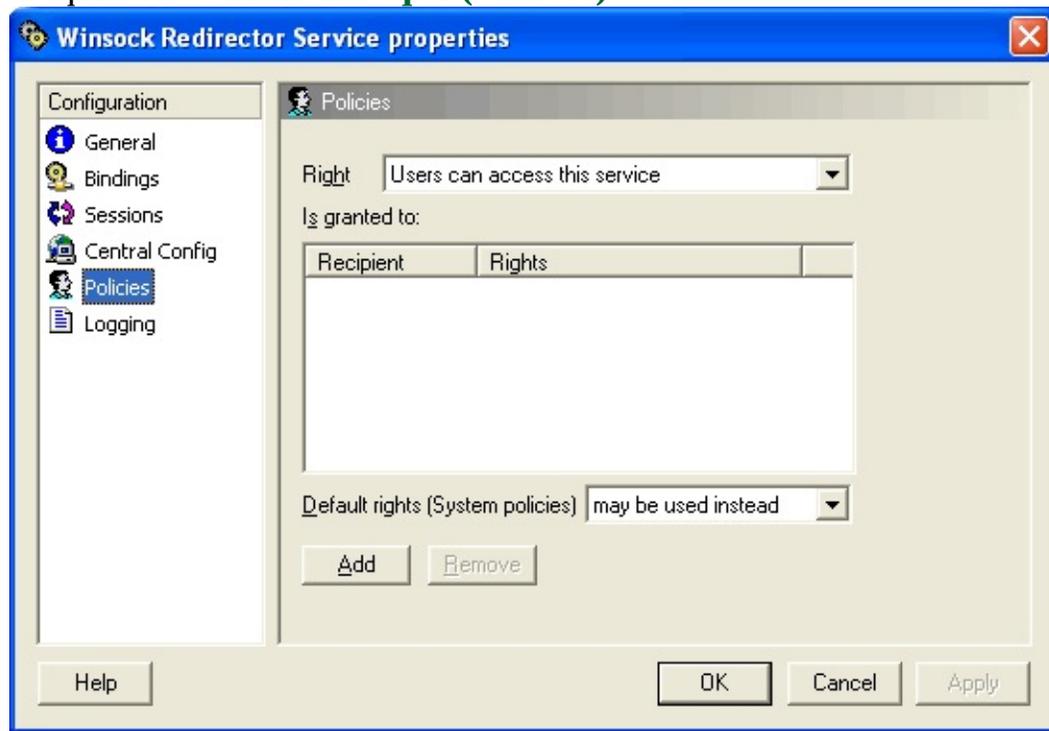
empêche que des utilisateurs non autorisés n'obtiennent un accès Internet sur des postes laissés sans surveillance ;

empêche que les utilisateurs n'installent une copie non autorisée de WinGate Internet Client ;

améliore le contrôle et l'audit.

Pour exiger l'authentification des utilisateurs avec WGIC :

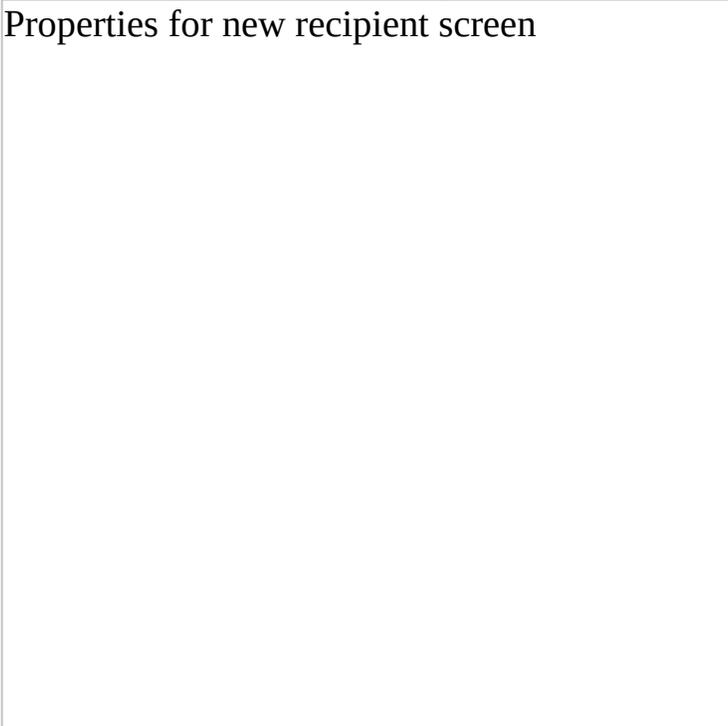
1. Ouvrez **GateKeeper**
2. Ouvrez les propriétés du Service WRP
3. Cliquez sur l'icône **Politique (Policies)**



Masquer | **Masquer toutes les images**

4. Cliquez sur **Ajouter** et indiquez à qui s'applique cette directive (par défaut : **tous les utilisateurs**)

Properties for new recipient screen



Masquer | Masquer toutes les images

5. Cochez l'option **L'utilisateur doit être authentifié** (*User must be authenticated*)
6. Cliquez sur **OK**
7. Dans la fenêtre **Politique** du **service WRP**, sélectionnez **Droits par défaut (politique système) : ignorés** (*Default rights (System Policies) - are ignored*) ou bien l'option souhaitée dans le menu déroulant.

Une fois cette opération effectuée, la **fenêtre de connexion** de WGIC s'affiche la première fois qu'une application essaie de se connecter.



Masquer | Masquer toutes les images

©2004 Qbik New Zealand Limited

Méthodes d'authentification : connexion Java

L'**applet de connexion Java** est un outil multifonctionnel permettant l'authentification des utilisateurs.



Masquer | Masquer toutes les images

Pour que l'applet soit chargée par le navigateur, vous devez :

Configurer le navigateur pour qu'il se connecte à Internet avec le proxy WinGate.

Configurer le service proxy web pour qu'il utilise l'authentification Java (en cochant **Client Java**, dans l'icône **Général** des propriétés du service web).

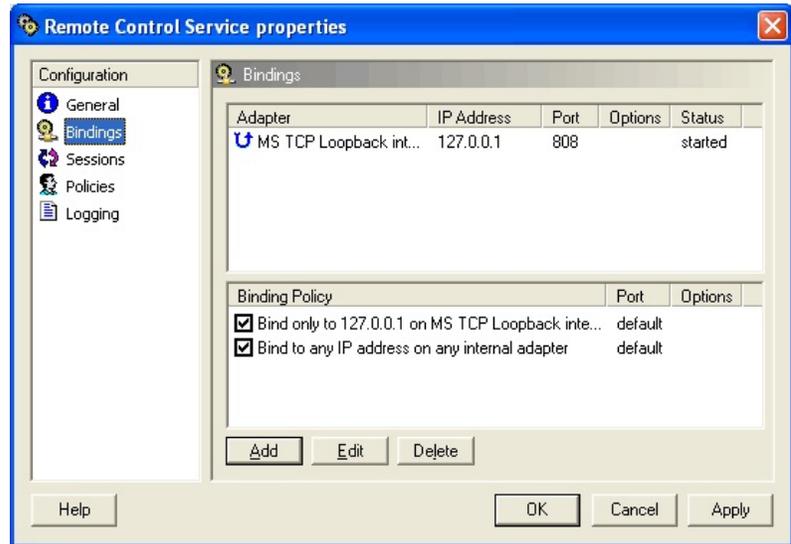
Cocher l'option **L'utilisateur doit être authentifié (User must be authenticated)** (dans les propriétés d'un système ou service, icône **Politique**)

Utilisation de l'applet de connexion Java pour authentifier les utilisateurs du service proxy web (WWW Proxy) de WinGate :

1. Configuration du Service d'administration à distance (*Remote Control Service*) :
 1. Ouvrez **GateKeeper**.
 2. Dans l'onglet **Système**, double-cliquez sur **Service**

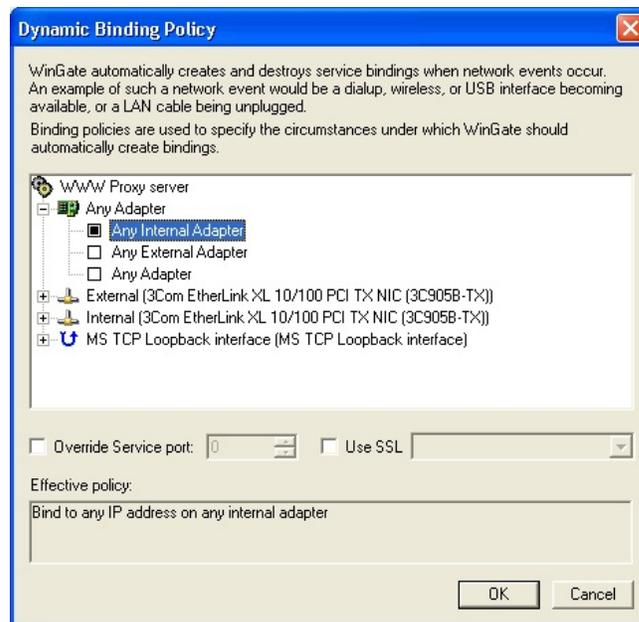
d'administration à distance (*Remote Control Service*).

3. Cliquez sur **Liaisons (Bindings)**, puis si aucune interface interne ne figure dans la fenêtre, cliquez sur **Ajouter (Add)**.



Masquer | Masquer toutes les images

4. Dans **la fenêtre** qui s'ouvre ensuite, sélectionnez une interface interne ou cochez l'option **Tous les adaptateurs internes (Any Internal adapter)**.



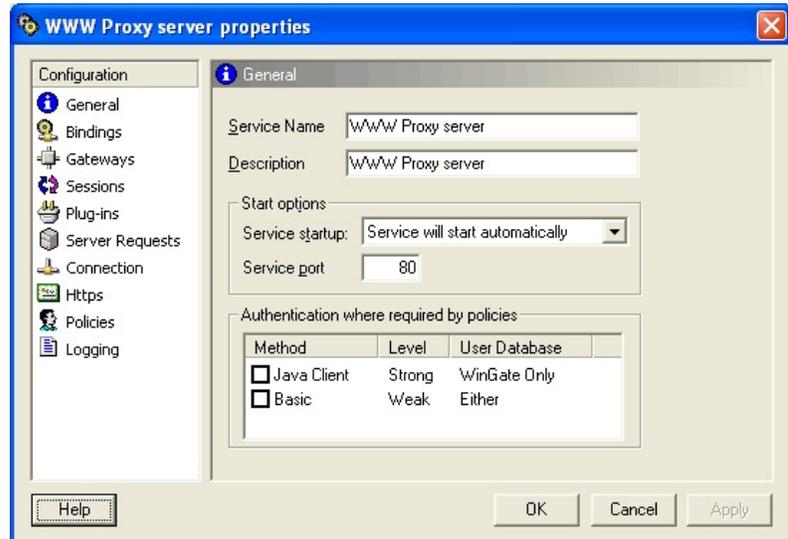
Masquer | Masquer toutes les images

5. Cliquez sur **OK**. L'interface figure à présent dans les liaisons.
6. Cliquez à nouveau sur **OK**.

2. Configuration de la politique pour l'authentification :

1. Double-cliquez sur le **Service proxy web (WWW proxy service)** dans l'onglet **Services** de GateKeeper.
2. Dans la fenêtre **Général**, cochez l'option **Client Java (Java Client)** pour la partie **Méthode d'authentification (si nécessaire) (Authentication where required by policies)**.

(Veuillez noter que cette option n'est pas disponible si vous utilisez la base de données du système d'exploitation ou une base distante, car l'applet Java n'est pas compatible avec l'authentification NTLM.)



Masquer | Masquer toutes les images

3. Cliquez ensuite sur **Politique (Policies)**.

WWW Proxy service policies screen

The screenshot area is currently blank, showing only the title text at the top.

Masquer | Masquer toutes les images

4. Dans le menu déroulant, sélectionnez **L'utilisateur peut accéder au service (*User can access this service*)** puis cliquez sur **Ajouter (*Add*)**.
5. Dans **la fenêtre** qui s'ouvre ensuite, cliquez sur l'onglet **Utilisateur (*Recipient*)**.

Properties for new recipient screen

Masquer | Masquer toutes les images

6. Choisissez l'utilisateur ou groupe auquel s'applique la politique (par défaut : **Tous (*Everyone*)**).
7. Sélectionnez l'option **l'utilisateur doit être authentifié (*user must be authenticated*)**.
8. Configurez les options de votre choix.
9. Cliquez sur **OK**.
10. Dans le menu déroulant **Droits par défaut (*Politique système*) (*Default rights (System policies)*)** sélectionnez **ignorés (*are ignored*)**.
11. Cliquez sur **OK**.

Même s'il est nécessaire d'utiliser un navigateur pour charger l'applet, cette méthode d'authentification fonctionne également avec les autres services (par exemple : FTP).

Si WGIC n'est pas actif, les utilisateurs peuvent s'authentifier en ouvrant leur navigateur et en se connectant dans l'applet Java, pour ensuite utiliser leur client

FTP.

Remarques :

Le **Service d'administration à distance (*Remote control service*)** doit être lié à l'interface locale LAN (adaptateur interne) pour que l'authentification Java fonctionne.

L'applet Java ne s'affiche que lorsque le niveau d'authentification d'un utilisateur est insuffisant pour effectuer une requête. Par exemple, si vous cochez l'option du service proxy web **L'utilisateur peut être présumé (*User may be assumed*)**, elle ne s'affichera que pour les utilisateurs non présumés.

Le **service proxy SOCKS** peut également desservir le client.

La connexion Java **ne fonctionne pas** si WinGate utilise l'authentification NT (elle n'est pas disponible dans les options du proxy web).

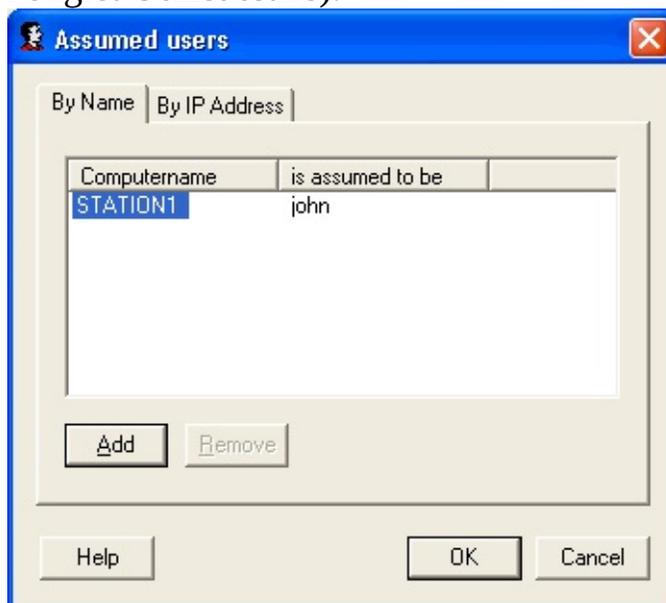
Utilisateurs présumés

Il est possible d'identifier un utilisateur en fonction de son emplacement (sans devoir exiger d'authentification). Vous pouvez donc présumer qu'un utilisateur se connectant à partir d'un emplacement connu est un utilisateur de WinGate.

Avec cette fonctionnalité, les utilisateurs ne sont pas obligés de s'authentifier. Cela peut s'avérer utile si un ordinateur est toujours utilisé par la même personne.

Ajouter un utilisateur présumé

1. Ouvrez GateKeeper.
2. Double-cliquez sur **Utilisateurs présumés (Assumed Users)** (dans l'onglet **Utilisateurs**).



Masquer | Masquer toutes les images

3. Sélectionnez **Adresse IP (by IP Address)**, ou bien **Nom (by Name)** (nom NETBIOS ou Windows de l'ordinateur).
4. Cliquez sur **Ajouter (Add)**. Une **nouvelle fenêtre** s'affiche.



Masquer | Masquer toutes les images

5. Indiquez le nom ou l'adresse IP du poste.
6. Choisissez un utilisateur.
7. Cliquez sur **OK**.

Remarques :

Seuls les clients DHCP peuvent être identifiés en fonction du nom.

Pour les adresses IP, il est possible d'utiliser le caractère joker "*".

WinGate respecte l'ordre de la liste (de haut en bas). La première adresse qui correspond est retenue.

Par exemple :

```
192.168.0.1 pierre
192.168.0.3 alf
192.168.*.* fred
192.168.0.* célia
```

Avec cette liste, Célia n'aura jamais le statut d'utilisateur présumé car la troisième ligne correspond à toutes les adresses commençant par 192.168 (sauf 192.168.0.1 et 192.168.0.3). La liste doit donc être dans l'ordre suivant :

```
192.168.0.1 pierre
192.168.0.3 alf
192.168.0.* célia
192.168.*.* fred
```

L'adresse *.*.* est associée de façon implicite avec le compte "Guest" : cela correspond aux utilisateurs qui ne sont pas encore authentifiés.

©2004 Qbik New Zealand Limited

Méthodes d'authentification : NTLM

Il est possible de bénéficier dans WinGate de l'authentification NTLM (employée par les systèmes d'exploitation Windows).

Pour cela, vous devez utiliser la [base de données du système d'exploitation](#) et non celle de WinGate.

Cette méthode est compatible avec **WinGate Internet Client (WGIC)** et **GateKeeper** mais pas avec [l'authentification Java](#).

Pour bénéficier de l'authentification NTLM dans **WGIC** ou **GateKeeper** :

1. Assurez-vous que WinGate soit paramétré de façon à utiliser la base de données du système d'exploitation (Windows).
2. Configurez les clients afin qu'ils utilisent l'authentification [WGIC](#) ou [GateKeeper](#).
3. Les utilisateurs doivent se connecter à l'aide d'un **nom d'utilisateur** et d'un **mot de passe** valides (provenant de la base de données choisie).
4. Une fois authentifiés, ils figurent dans l'onglet **Activité** (Authenticated [NTLM]).

Utilisation de proxies avec la méthode NTLM

Les clients possédant des navigateurs compatibles avec cette méthode et configurés pour utiliser un serveur proxy (par ex. : Internet Explorer) peuvent bénéficier de l'authentification NTLM dans WinGate.

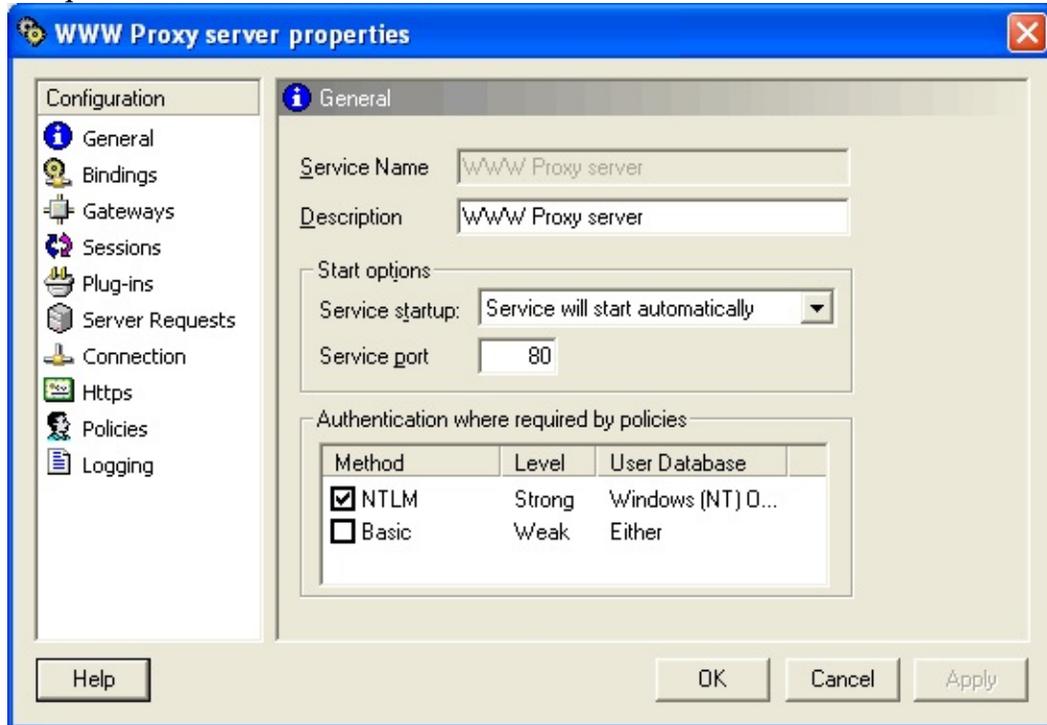
Cela peut s'avérer utile dans un environnement Active Directory où les politiques de groupe sont centralisées dans les paramètres du navigateur (c'est à dire la configuration du serveur proxy par défaut).

Cette politique de groupe pouvant être appliquée à tous les navigateurs du réseau, cela permet de contrôler facilement l'authentification pour l'accès à Internet sans devoir configurer chaque client individuellement. En effet, dans ce cas tous les clients s'authentifient dans WinGate à l'aide de la méthode NTLM.

Procédure à suivre :

Sur le serveur :

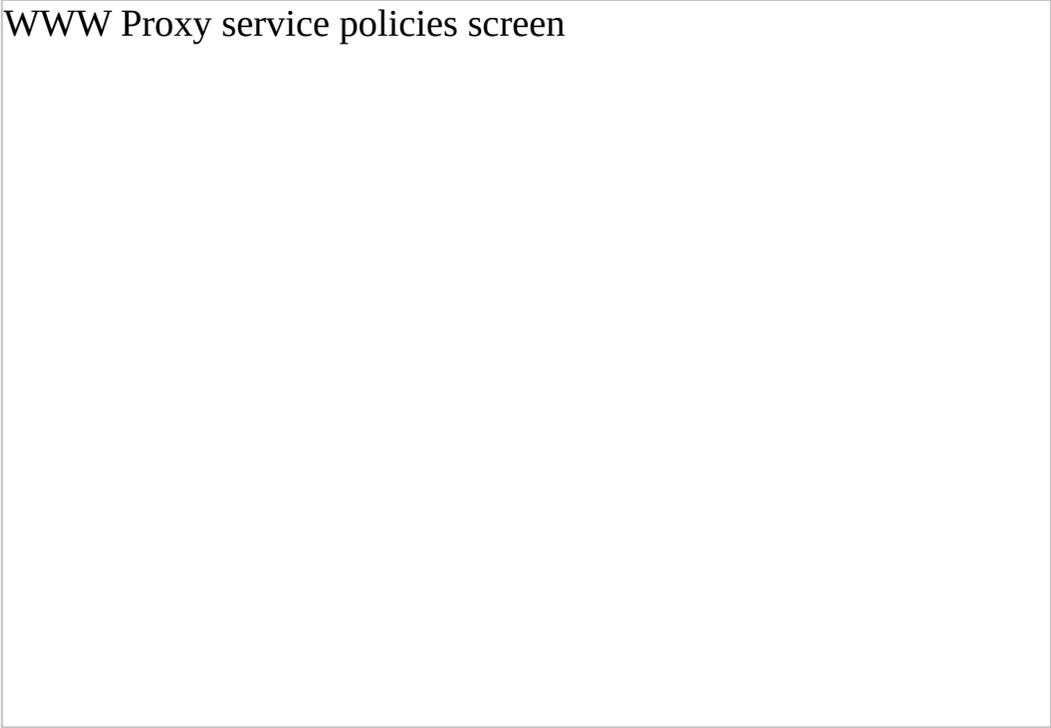
1. Ouvrez **GateKeeper**.
2. Double-cliquez sur le serveur **proxy web (WWW proxy)** (dans l'onglet **Services** du panneau Contrôle).
3. Cliquez sur l'icône **Général**.



Masquer | Masquer toutes les images

4. Dans la section **Méthode d'authentification (si nécessaire)** (*Authentication (where required by policies)*), cochez l'option **NTLM**.
5. Cliquez ensuite sur l'icône **Politique (Policies)**.

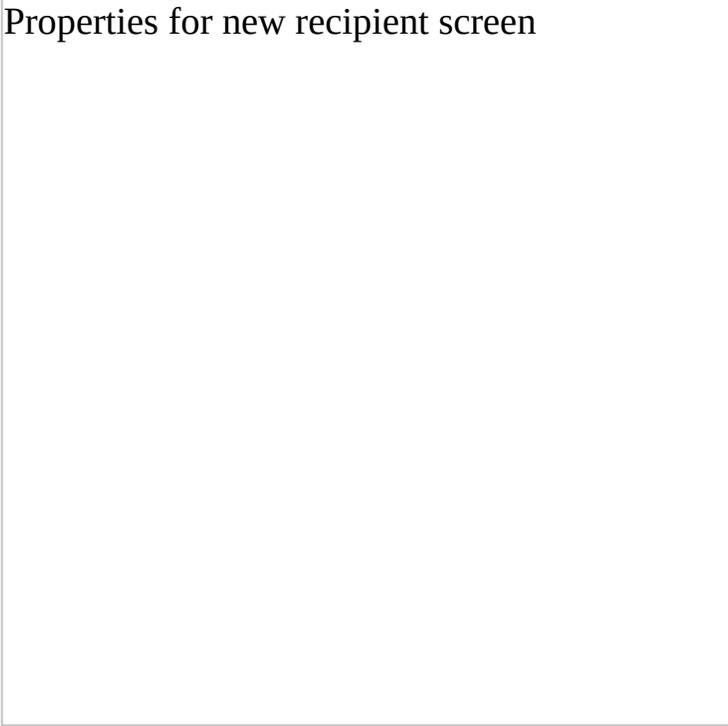
WWW Proxy service policies screen

A large rectangular area that is currently blank, representing the content of the WWW Proxy service policies screen mentioned in the text above it.

Masquer | Masquer toutes les images

6. Cliquez sur **Ajouter (Add)** pour choisir à quels utilisateurs cela s'applique.
7. Dans la **fenêtre qui s'ouvre ensuite**, cochez l'option **L'utilisateur doit être authentifié (User must be authenticated)**.

Properties for new recipient screen



Masquer | Masquer toutes les images

8. Cliquez sur **OK**
9. En fonction de vos besoins, vous pouvez éventuellement configurer l'option **Droits par défaut (politique système) (Defaults rights (System policies))** sur **ignorés (are ignored)**.
10. Cliquez sur **OK**.

Sur le client :

1. Configurez le navigateur de façon à ce qu'il utilise un serveur proxy et indiquez l'IP du serveur WinGate.
2. Sur certains navigateurs, il est possible de modifier les paramètres de sécurité afin que l'utilisateur s'authentifie avec son nom et mot de passe Windows. Ainsi, il n'est plus nécessaire d'indiquer ces informations à chaque fois qu'il ouvre son navigateur. Le nom et le mot de passe utilisés doivent évidemment figurer dans la base de données choisie pour WinGate.

Remarque :

L'authentification NTLM pour le service proxy web n'est disponible qu'avec les versions WinGate 6 Pro et Enterprise

©2004 Qbik New Zealand Limited

Postes multi-utilisateurs (*Multi-user Machines*)

Dans WinGate, plusieurs utilisateurs du même serveur de terminal peuvent s'authentifier simultanément. Auparavant, WinGate considérait généralement qu'il s'agissait d'un seul utilisateur avec des sessions différentes.

Cependant, avec WinGate 6.0 chaque utilisateur peut s'authentifier dans WinGate de façon indépendante.

Dans la fenêtre Postes multi-utilisateurs vous pouvez indiquer les adresses IP des serveurs de terminaux de votre réseau. Ainsi, plusieurs utilisateurs d'un même terminal peuvent s'authentifier individuellement.

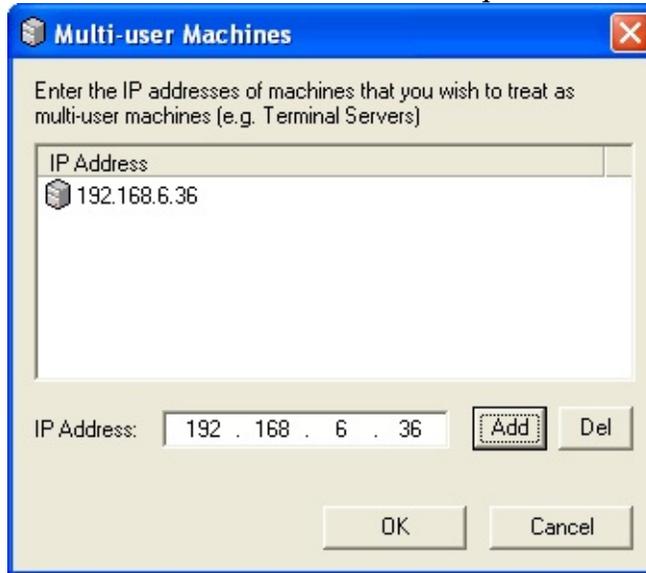
Pour cela :

1. Ouvrez **GateKeeper**.
2. Double-cliquez sur l'icône **Postes multi-utilisateurs (*Multi-user Machines*)** dans l'onglet **Utilisateurs** du panneau Contrôle.



Masquer | Masquer toutes les images

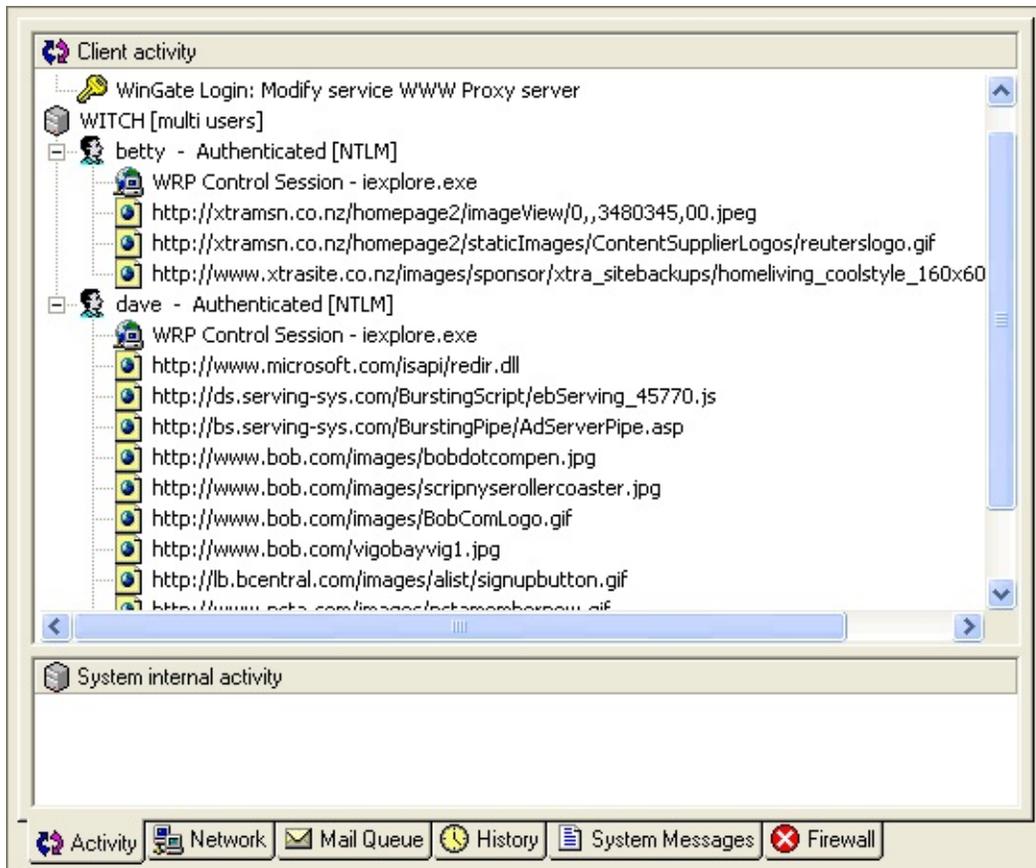
3. Dans la **fenêtre** qui s'ouvre ensuite, indiquez l'adresse IP du poste que vous souhaitez utiliser en tant que serveur de terminal.



Masquer | Masquer toutes les images

4. Cliquez sur **Ajouter**, puis sur **Ok**.
5. Pour supprimer une IP de la liste, sélectionnez-la et cliquez sur **Supprimer**.

Cliquez ici pour un consulter l'affichage de l'onglet Activité



Masquer | Masquer toutes les images

Remarques :

Comme les utilisateurs se connectent individuellement au serveur de terminal (sous Windows), WinGate doit être configuré afin d'utiliser la base de données du système d'exploitation pour l'authentification NTLM.

Cette fonctionnalité n'est disponible qu'avec WinGate 6 Enterprise.

©2004 Qbik New Zealand Limited

Politiques et droits

WinGate est à la fois sécurisé et flexible.

En termes de sécurité, des droits sont attribués à des individus ou des groupes (ils forment ce que l'on appelle des "politiques"). De ce point de vue, WinGate fonctionne de la même manière que la gestion des utilisateurs Windows NT.

Les politiques s'appliquent soit de façon globale, soit par service. Vous pouvez les associer pour sécuriser votre réseau selon vos besoins.

Politique système

La politique système est le premier outil de sécurisation et de contrôle de WinGate. Elle peut être définie par utilisateur, par groupe, par heure et s'appliquer aux requêtes. Cette politique est globale et tient lieu de règle pour l'ensemble des services (sauf si vous définissez une politique de service).

([Cliquez ici pour savoir comment attribuer des droits avec la politique système](#))

Politique de service

Les politiques de service sont le second outil de sécurisation et de contrôle de WinGate. Une politique ne s'applique qu'au service auquel elle est attribuée.

([Cliquez ici pour savoir comment attribuer des droits par service dans GateKeeper](#))

Droits proposés par WinGate

([Cliquez ici pour connaître les droits proposés par WinGate](#))

Configuration d'une politique par utilisateur

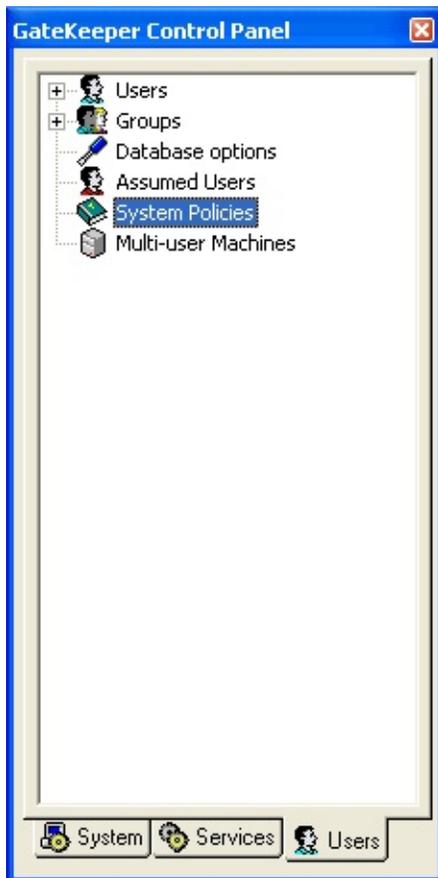
Lorsque vous définissez une politique dans WinGate, vous pouvez définir des droits par utilisateur dans le respect de cette politique.

([Cliquez ici pour savoir comment configurer des droits par utilisateur](#))

©2004 Qbik New Zealand Limited

Politique système (*System Policies*)

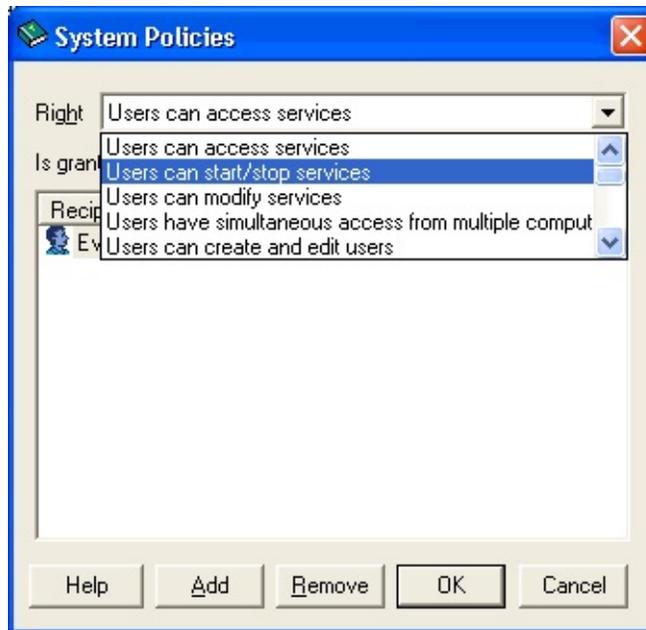
Située dans l'onglet **Utilisateurs (Users)** de GateKeeper, l'icône **Politique système (System policies)**, permet de contrôler l'ensemble des services de WinGate.



Masquer | Masquer toutes les images

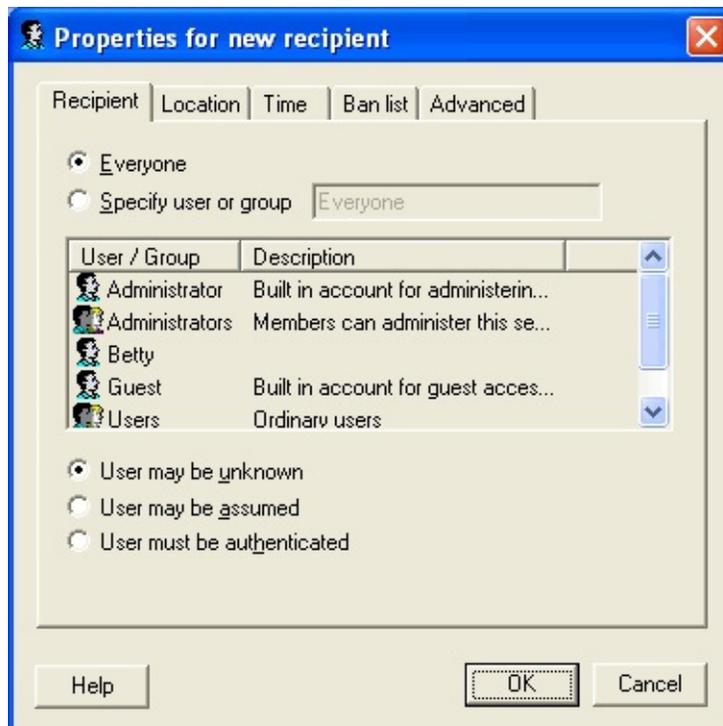
Pour ajouter/modifier des droits :

1. Ouvrez **GateKeeper**
2. Double-cliquez sur l'icône **Politique système (System Policies)**.



Masquer | Masquer toutes les images

3. Sélectionnez un droit dans le menu déroulant.
4. Cliquez sur **Ajouter (Add)** et choisissez l'utilisateur ou groupe auquel vous souhaitez accorder ce droit.



Masquer | Masquer toutes les images

5. Configurez les options de votre choix.
6. Cliquez sur **OK**.

Remarque importante :

Dans WinGate, le droit **Les utilisateurs peuvent accéder aux services/à ce service (*Users can access services/this service*)** est accordé à tous les utilisateurs et groupes (**Everyone**).

Ainsi, tous les services sont disponibles tant que l'administrateur n'a pas imposé de restrictions.

Cela permet également à l'administrateur d'accéder au Service d'administration à distance (*Remote Control service*) lorsqu'il se connecte pour la première fois à GateKeeper. Si ce droit n'est plus accordé à tous les utilisateurs (*Everyone*), le Service d'administration à distance ne sera plus disponible et il sera impossible de s'authentifier dans WinGate, même pour l'administrateur.

Ne modifiez pas ce droit, sauf si l'administrateur possède des droits d'accès spécifiques au Service d'administration à distance. Vous pouvez également configurer la politique de ce service afin d'ignorer la Politique système.

Si ce droit n'est plus accordé à tous les utilisateurs dans la Politique système, suivez les indications suivantes pour le rétablir :

1. Sauvegardez le registre de WinGate.
2. Ouvrez le Registre à l'aide de l'application RegEdit.exe et recherchez la clé suivante HKLM\Qbik Software\WinGate\DefaultRights\Access
3. Ajoutez les entrées suivantes :

Key: [HKEY_LOCAL_MACHINE\SOFTWARE\Qbik Software\WinGate\DefaultRights\Access\Recipient0]

"UserName"="Everyone"

"Description"="Unrestricted rights"

"SpecifyUser"=dword:00000000

"SpecifyLocation"=dword:00000000

"SpecifyTime"=dword:00000000

"SpecifyBan"=dword:00000000

"SpecifyRequest"=dword:00000000

"MinimumSecurityLevel"=dword:00000000

Key:[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik
Software\WinGate\DefaultRights\Access\Recipient0\BanFilter]

"Name"=""

"Description"=""

Key:[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik
Software\WinGate\DefaultRights\Access\Recipient0\ExcludedLoc

Key:[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik
Software\WinGate\DefaultRights\Access\Recipient0\IncludedLoc

Key:[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik
Software\WinGate\DefaultRights\Access\Recipient0\RequestFilter

Key:[HKEY_LOCAL_MACHINE\SOFTWARE\Qbik
Software\WinGate\DefaultRights\Access\Recipient0\TimeFilter]

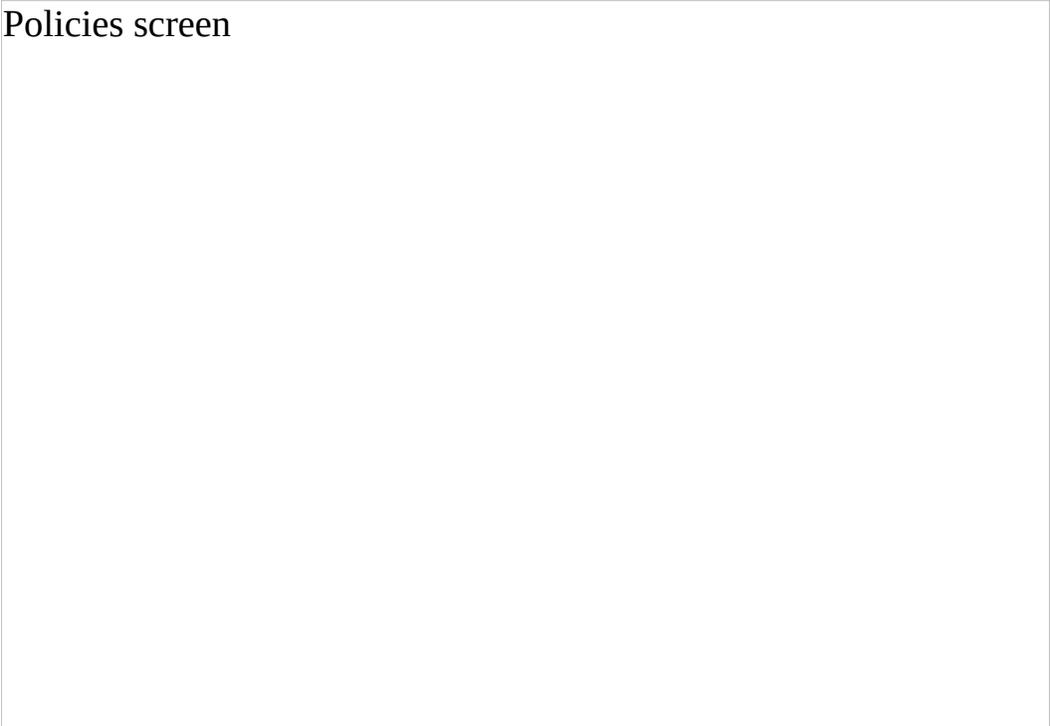
"Name"=""

"Description"=""

Politique de service

En cliquant sur l'icône **Politique (Policies)** d'un service, vous pouvez configurer une politique spécifique à ce service.

Policies screen



Masquer | **Masquer toutes les images**

Pour chaque service, vous pouvez accorder l'un des trois droits suivants :

1. **L'utilisateur peut accéder au service (*User can access this service*)**
Précise quels utilisateurs peuvent accéder au service, ainsi que les requêtes pouvant être effectuées.
2. **L'utilisateur peut modifier le service (*User can modify this service*)**
Précise quels utilisateurs peuvent modifier les paramètres du service ou même le supprimer.
3. **L'utilisateur peut démarrer/arrêter le service (*User can start/stop this service*)**
Précise quels utilisateurs peuvent démarrer ou arrêter le service.

Ces droits sont similaires à ceux de la **Politique système**, mais ils ne s'appliquent qu'au service sélectionné. ([Cliquez ici pour en savoir plus sur l'intégration des politiques système et de service](#))

Configuration de la politique d'un service :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte **Administrator**.
3. Sélectionnez le service souhaité (dans l'onglet **Services**).
4. Cliquez sur l'icône **Politique**.
5. Sélectionnez un droit dans le menu déroulant.
6. Cliquez sur **Ajouter** afin de choisir à qui s'applique ce droit.



Masquer | **Masquer toutes les images**

7. Sélectionnez un utilisateur ou un groupe.
8. Configurez les différentes options.
9. Cliquez sur **OK**.

[Cliquez ici pour en savoir plus](#)

Lorsqu'une requête est effectuée, WinGate vérifie la liste des utilisateurs concernés par cette action.

Si un utilisateur figure sur la liste, le droit correspondant s'applique.

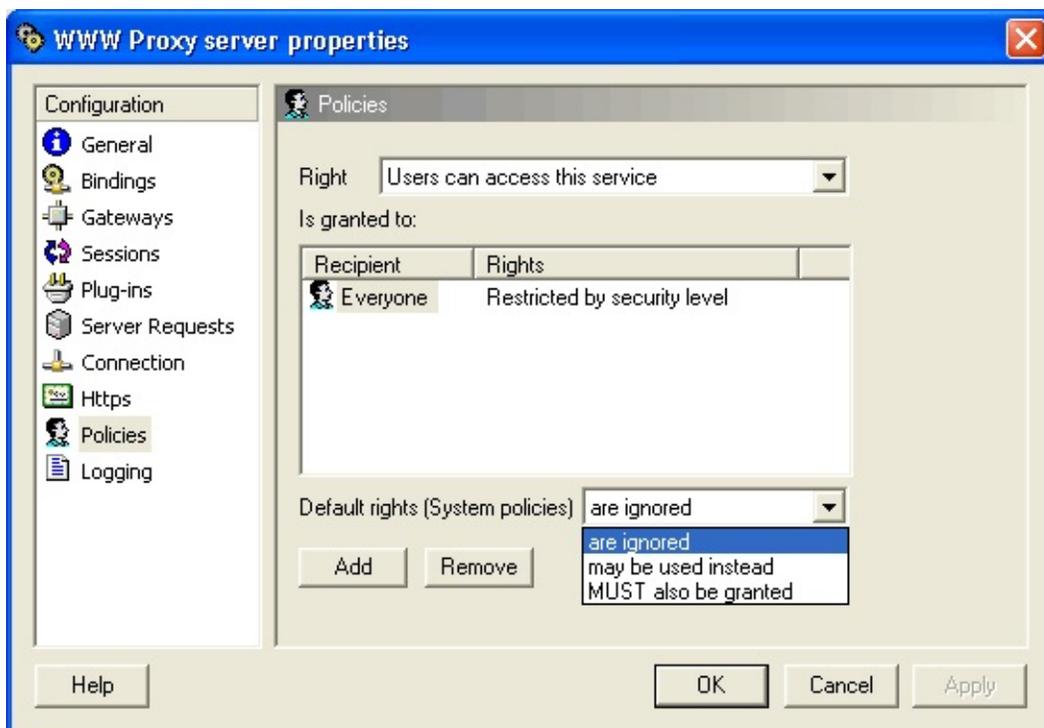
©2004 Qbik New Zealand Limited

Intégration des politiques système et de service

Il s'agit d'un élément capital concernant la sécurité dans WinGate.

Il est important d'intégrer les politiques appliquées par service (**politiques de service**) avec celle s'appliquant à tous (**politique système**).

Ainsi, lors du choix des droits et politiques d'un service vous devez choisir l'une des options ci-dessous. L'option **droits par défaut (politique système) (Default rights (system policy))** se trouve dans la fenêtre **Politique** de chaque service.



Masquer

Droits par défaut (politique système) :

ignorés (are ignored)

Les politiques système ne s'appliquent pas à ce service. Dans ce cas, soyez vigilants quant aux droits accordés car ils constituent la seule mesure de sécurité pour ce service.

peuvent être appliqués (may be used instead) (sélectionné par défaut)

La requête sera acceptée si les règles de l'une des politiques l'autorisent. Ce qui

est permis par la politique d'un service peut être interdit par la politique système.
La sécurité est ainsi assurée sur deux niveaux.

DOIVENT être appliqués (*must be used*)

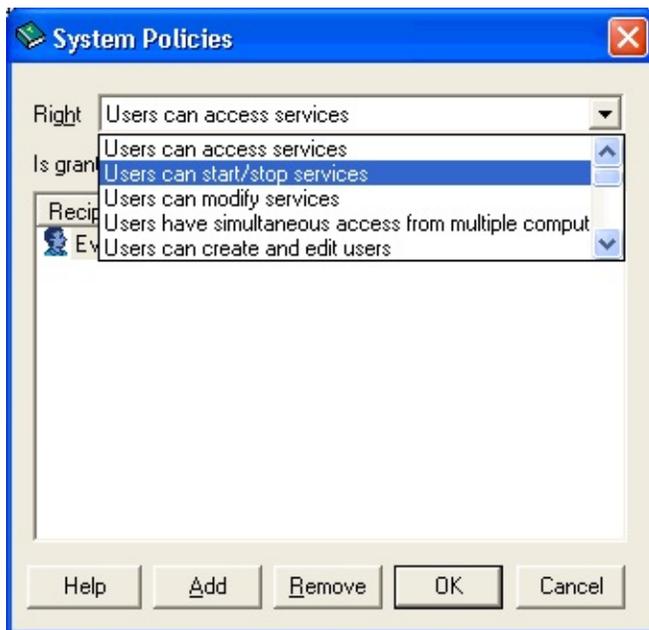
Solution la plus sécurisée mais la moins flexible. En effet, les droits doivent être accordés par chacune des politiques.

©2004 Qbik New Zealand Limited

Politiques et droits

Politique système (*System Policies*)

Définit les droits d'accès par défaut à tous les services de WinGate. **Cette fonctionnalité** se trouve dans l'onglet **Utilisateurs (Users)** du panneau Contrôle.



Masquer | Masquer toutes les images

([Cliquez ici pour en savoir plus](#))

Droits

Les utilisateurs peuvent créer/supprimer des services (*Users can create/delete services*)

Les utilisateurs possédant ce droit peuvent créer ou supprimer des services dans WinGate.

Remarque : Tous les droits relatifs aux services dépendent de celui-ci.

Les utilisateurs peuvent accéder aux services (*Users can access services*)

Précise quels utilisateurs peuvent bénéficier des services ainsi que les requêtes pouvant être effectuées.

Les utilisateurs peuvent modifier les services (*Users can modify services*)

Précise quels utilisateurs peuvent modifier les paramètres des services ou même les supprimer.

Les utilisateurs peuvent démarrer/arrêter les services (*Users can start/stop services*)

Précise quels utilisateurs peuvent démarrer ou arrêter les services.

Les utilisateurs peuvent créer et modifier des comptes (*Users can create and edit users*)

Précise quels utilisateurs peuvent créer ou modifier des utilisateurs et groupes. Remarque : tous les droits relatifs aux utilisateurs dépendent de celui-ci.

Les utilisateurs possèdent des droits d'administration (*Users have power user rights*)

Par défaut, ce droit n'est accordé qu'au groupe "Administrators".

Les utilisateurs peuvent se connecter simultanément depuis plusieurs postes (*Users have simultaneous access from multiple computers*)

Permet d'accéder aux services de WinGate en étant connecté sur plusieurs postes en même temps.

Les utilisateurs peuvent contrôler l'activité du serveur (*Users can monitor activity on this server*)

Précise quels utilisateurs peuvent contrôler l'activité du serveur, c'est à dire consulter le statut de toutes les sessions.

Les utilisateurs peuvent supprimer des sessions (*Users can delete sessions from this server*)

Précise quels utilisateurs peuvent supprimer des sessions.

Les utilisateurs peuvent modifier la politique système (*Users can modify and control system policies*)

Si un utilisateur ne possède pas ce droit, l'icône correspondante ne s'affiche pas.

Les utilisateurs peuvent modifier le Composeur (*Users can modify and control WinGate dialer*)

Précise quels utilisateurs peuvent modifier les paramètres du Composeur.

Les utilisateurs peuvent modifier le cache (*Users can modify and control WinGate cache*)

Précise quels utilisateurs peuvent modifier les paramètres du cache.

Les utilisateurs peuvent arrêter WinGate (*Users can shutdown WinGate*)

Nous vous recommandons de n'accorder ce droit qu'au groupe "Administrators". En effet, le service se démarre à partir du Panneau de configuration (NT) ou du menu démarrer .

Les utilisateurs peuvent modifier la licence de WinGate (*Users can change WinGate license*)

Permet de modifier les détails concernant la licence.

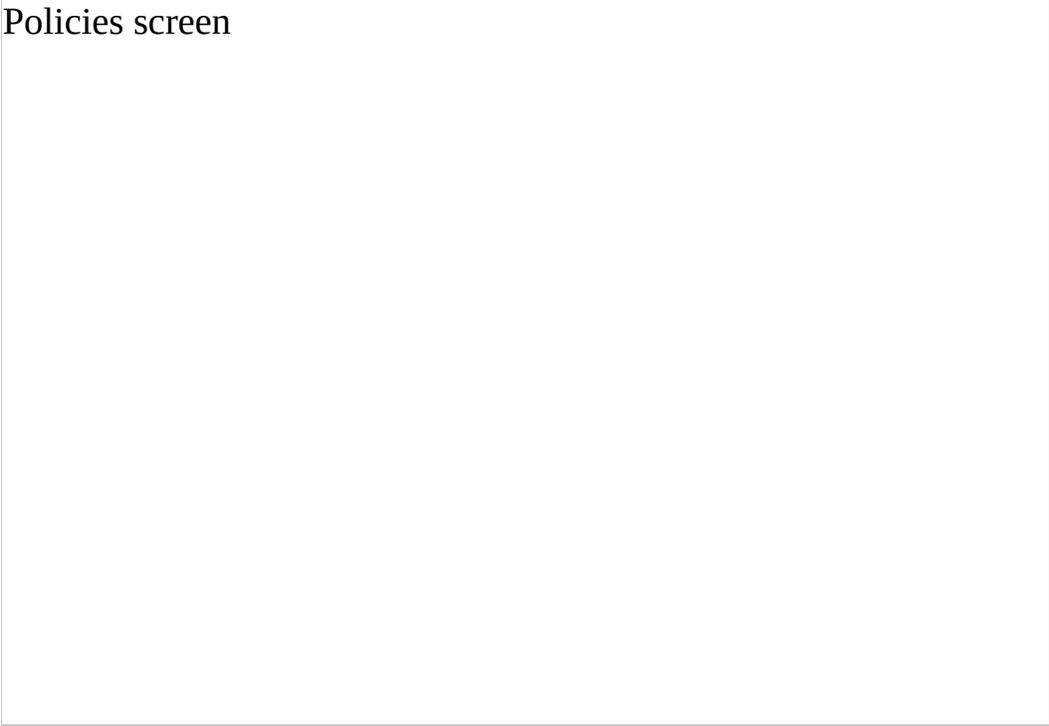
Les utilisateurs peuvent modifier le Programmeur (*Users can change WinGate scheduler*)

Il est préférable de n'accorder ce droit qu'au groupe "Administrators" ou aux utilisateurs responsables de la maintenance.

Politiques de service (*Service Policies*)

En cliquant sur l'icône **Politique** d'un service, vous pouvez configurer une politique spécifique à ce service.

Policies screen



Masquer | Masquer toutes les images

Pour chaque service, vous pouvez accorder l'un des trois droits suivants :

1. **L'utilisateur peut accéder au service (*User can access this service*)**
Précise quels utilisateurs peuvent accéder au service, ainsi que les requêtes pouvant être effectuées.
2. **L'utilisateur peut modifier le service (*User can modify service*)**
Précise quels utilisateurs peuvent modifier les paramètres du service ou même le supprimer.
3. **L'utilisateur peut démarrer/arrêter le service (*User can start/stop service*)**
Précise quels utilisateurs peuvent démarrer ou arrêter le service.

Remarque :

Ces droits sont identiques à ceux de la **Politique système**, cependant ces derniers s'appliquent à tous les services. ([Cliquez ici pour en savoir plus sur l'intégration des politiques système et de service](#))

©2004 Qbik New Zealand Limited

Création de règles

Les règles de WinGate sont très flexibles et permettent d'appliquer diverses politiques, en fonction de vos besoins.

Plusieurs outils utilisent des règles :

1. Les options des politiques système ou de service, onglets [Exclusions \(Ban list\)](#) ou [Avancé \(Advanced\)](#).
2. [La mémoire cache](#)

Exemple de création d'une règle :

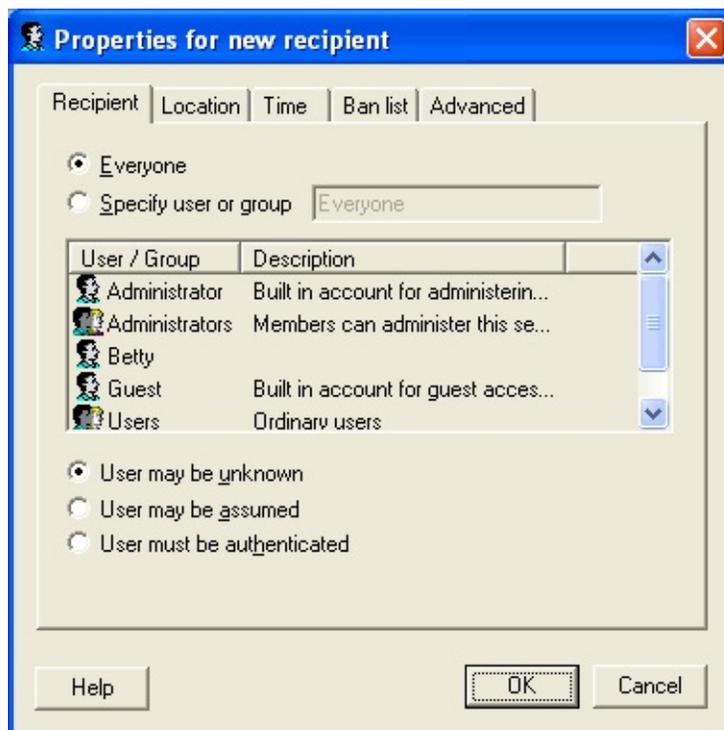
Vous ne souhaitez accorder l'accès qu'à certains sites, par exemple : www.wingate.com.

1. Ouvrez **GateKeeper**
2. Double-cliquez sur le service **proxy web** (dans l'onglet **Services**).
3. Cliquez sur l'icône **Politique (Policies)**.

Policies Configuration

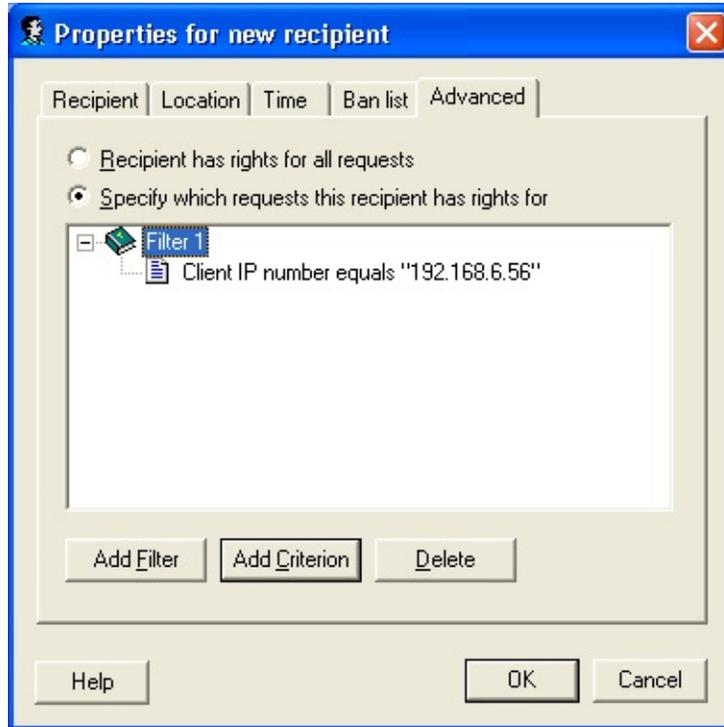
Masquer | Masquer toutes les images

4. Double-cliquez sur un utilisateur de la liste ou cliquez sur **Ajouter**.
5. Cliquez sur l'onglet **Utilisateur (Recipient)** dans la fenêtre qui s'ouvre ensuite.



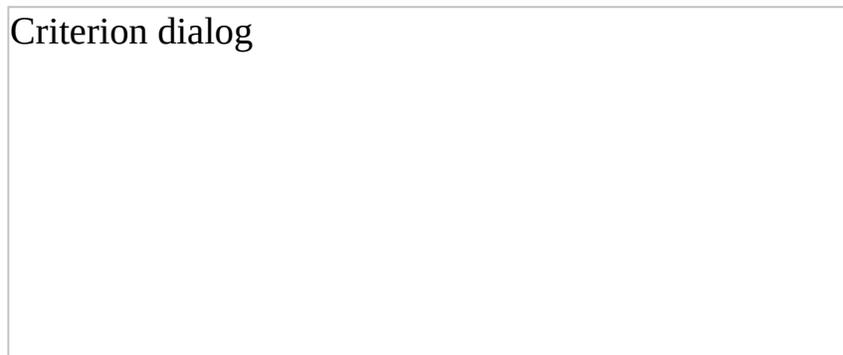
Masquer | Masquer toutes les images

6. Choisissez pour quels utilisateurs la politique s'applique.
7. Cliquez sur l'onglet **Avancé (Advanced)**.



Masquer | Masquer toutes les images

8. Cochez l'option **Indiquer pour quelles requêtes la politique s'applique (Specify which requests this recipient has rights for)**.
9. Cliquez sur **Ajouter un filtre (Add Filter)**.
10. Cliquez sur **Ajouter un critère (Add Criterion)**.



Masquer | Masquer toutes les images

11. Sélectionnez l'option **le critère s'applique si** (*the criterion is met if*).
12. Créez un filtre contenant le critère : **le nom du serveur/ contient/ www.wingate.com** (*server name/ contains/ www.wingate.com*).
13. Pour permettre l'accès à d'autres sites, ajoutez des filtres contenant les critères correspondants.
14. Cliquez sur **OK**.
15. Dans les propriétés du service **Proxy web (WWW service)**, cliquez sur l'icône **Politique (Policy)** et choisissez l'option **Droits par défaut (politique Système) (Default rights(System Policies)) / ignorés (Are ignored)**.



Masquer | Masquer toutes les images

Dans l'exemple ci-dessus, **seules** les pages provenant des sites mentionnés dans les filtres pourront être consultées.

Filtres et règles

Tous les filtres d'une politique sont coordonnés avec l'opérateur **OU**.

Il suffit donc qu'une requête corresponde à l'un des filtres pour que la politique s'applique.

Cependant, tous les critères d'un même filtre sont coordonnés avec l'opérateur **ET**. Ils doivent donc tous être vrais pour que le filtre s'applique.

Les opérateurs fonctionnent de la façon suivante :

ET - Si des critères sont coordonnés avec **ET**, ils doivent tous être vrais pour que la règle s'applique.

OU - Si des critères sont coordonnés avec **OU**, il suffit que l'un d'entre eux soit vrai pour que la règle s'applique.

PAS - La règle s'applique si le critère n'est pas vrai.

Pour définir les critères, vous disposez de nombreuses variables :

(Dans cette liste, **Tous** désigne tous les services sauf le DHCP.)

Variable	Type	Service	Description
L'adresse IP du client (<i>Client IP number</i>)	Chaîne	Tous	Adresse avec laquelle l'utilisateur s'est connecté.
Le numéro de port du client (<i>Client port number</i>)	Nombre	Tous	Numéro de port sur l'ordinateur du client.
Le nom Netbios du client (<i>Client Netbios name</i>)	Chaîne	Tous + DHCP	Nom Netbios du poste connecté.
L'adresse MAC du client (<i>Client MAC address</i>)	Chaîne	Tous + DHCP	Adresse MAC de l'adaptateur réseau du poste client.
Le client est un client DHCP (<i>Client is a DHCP client</i>)	Vrai/Faux	Tous	Indique si l'adresse IP du client a été attribuée par WinGate.
Le nom du serveur (<i>Server name</i>)	Chaîne	Tous	Nom ou IP du serveur auquel le client souhaite se connecter.
Le numéro de port du serveur (<i>Server port number</i>)	Nombre	Tous	Numéro de port du serveur auquel le client souhaite se connecter.
Le nom de l'utilisateur (<i>User:</i>	Chaîne	Tous	Nom de l'utilisateur dans WinGate. Il s'agit du compte pour lequel les données

Username)

seront enregistrées.

Le niveau d'authentification de l'utilisateur (<i>User: Authentication level</i>)	Nombre	Tous	Niveau d'authentification. 0 = inconnu 1 = présumé 2 = authentifié.
Le nombre d'octets envoyés au client (<i>User: Bytes sent to client</i>)	Nombre	Tous	Nombre d'octets que WinGate a envoyés au client pour cet utilisateur.
Le nombre d'octets reçus du client (<i>User: Bytes received from client</i>)	Nombre	Tous	Nombre d'octets que WinGate a reçus du client.
Le nombre d'octets envoyés pour le client (<i>User: Bytes sent for client</i>)	Nombre	Tous	Nombre d'octets que WinGate à envoyé pour le compte du client (par ex. : à des serveurs).
Le nombre d'octets reçus pour le client (<i>User: Bytes received for client</i>)	Nombre	Tous	Nombre d'octets que WinGate a reçus pour le compte du client.
Le temps de connexion (sec.) (<i>User: Time online</i>)	Nombre	Tous	Temps (en secondes) qui s'est écoulé depuis que l'utilisateur est connecté à WinGate.
Le solde de l'utilisateur (<i>User: Account</i>)	Nombre	Tous	Solde de l'utilisateur.

balance)

La description de la session (<i>Session description</i>)	Chaîne	Tous	Description de la session.
Le protocole HTTP (<i>HTTP Protocol</i>)	Chaîne	web	Protocole requis par l'utilisateur dans l'URL.
La méthode HTTP (<i>HTTP method</i>)	Chaîne	web	Commande HTTP envoyée par l'utilisateur, par exemple : GET, HEAD, LIST, PUT, CONNECT, POST.
La ressource HTTP (<i>HTTP resource</i>)	Chaîne	web	Fichier requis par l'utilisateur.
L'URL HTTP (<i>HTTP URL</i>)	Chaîne	web	URL complète.
Les données HTTP POST (<i>HTTP POST data</i>)	Chaîne	web	Contenu des formulaires envoyés à l'aide de la méthode POST.
La chaîne de requête HTTP (<i>HTTP Query string</i>)	Chaîne	web	Contenu de la chaîne (il s'agit généralement du contenu d'un formulaire envoyé à l'aide de la méthode GET).
Le champ d'en-tête HTTP (<i>HTTP Header field</i>)	Chaîne	web	Tout champ d'en-tête de requête HTTP défini dans le protocole HTTP. Vous devez indiquer le nom du champ, par exemple : "User-Agent", "If-Modified-Since", etc.
La requête est non proxy (<i>Is non proxy request</i>)	Vrai/Faux	Tous les proxies	Indique s'il s'agit d'une requête non proxy.
La session a été transférée	Vrai/Faux	web	Indique si la session a été transférée par

(*Session was handed over*)

le serveur SOCKS.

Le nom d'utilisateur POP3 (<i>POP 3 username</i>)	Chaîne	POP3	Nom d'utilisateur de la boîte POP3 à laquelle le client souhaite accéder.
Nom d'utilisateur FTP (<i>FTP username</i>)	Chaîne	FTP	Nom d'utilisateur sur le serveur FTP.
Le fichier VDOLive (<i>VDOLive file</i>)	Chaîne	VDOLive	Nom du fichier requis par VDOLive Player.
La version du protocole SOCKS (<i>SOCKS Protocol version</i>)	Nombre	SOCKS	Numéro de la version du protocole SOCKS (4 ou 5).
La commande SOCKS (<i>SOCKS Command</i>)	Nombre	SOCKS	1 = connect 2 = bind 3 = UDP associate (SOCKS5 seulement).
Type d'adresse SOCKS (<i>SOCKS Address type</i>)	Nombre	SOCKS	Type d'adresse SOCKS (uniquement pour les requêtes SOCKS5) 1 = IP4 2 = Name 3 = IP6 (non supporté).

Si la variable est un nombre, vous disposez de plusieurs possibilités pour définir le critère : inférieur, supérieur ou égal au nombre indiqué.

Si la variable est une chaîne, vous pouvez spécifier : **contient (contains)**, **commence par (begins with)**, **achève par (ends with)** ou **est absent (is empty)**.

©2005 Qbik New Zealand Limited

Options des politiques

Vous disposez de nombreuses options permettant de configurer la façon dont la politique **Système** ou les politiques **de Service** sont appliquées à un utilisateur (en cliquant sur **Ajouter**).

Onglet Utilisateur (*Recipient*)

Cet onglet indique à qui s'applique la politique choisie.

Masquer

Vous pouvez sélectionner **Tous (*Everyone*)**, ou indiquer l'utilisateur ou le groupe de votre choix.

Vous disposez de trois niveaux d'authentification :

L'utilisateur doit être authentifié (*User must be authenticated*)

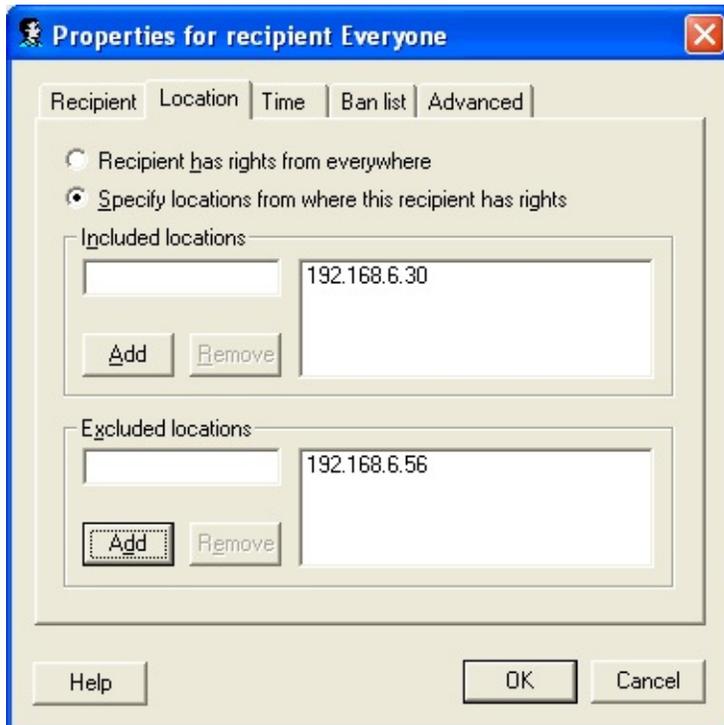
L'utilisateur peut être présumé (*User may be assumed*) : s'applique aux utilisateurs présumés à condition qu'ils soient authentifiés.

L'utilisateur peut être inconnu (*User may be unknown*) : s'applique à tous les utilisateurs.

[Cliquez ici pour en savoir plus la création de règles, les critères et les filtres](#)

Onglet emplacement (*Location*)

Cet onglet indique sur quel poste l'utilisateur doit se trouver.



Masquer

Pour que la politique s'applique, l'utilisateur doit se connecter à partir d'un emplacement inclus. S'il se connecte à partir d'un emplacement exclus, elle ne s'applique pas.

Vous pouvez sélectionner :

Tous les emplacements

Une adresse IP

Une plage d'adresses

Pour que les droits soient accordés, l'adresse IP de l'ordinateur doit correspondre à au moins un emplacement inclus, et aucun emplacement exclu.

Vous pouvez utiliser des caractères joker (par ex. : "?" et "*") pour définir une

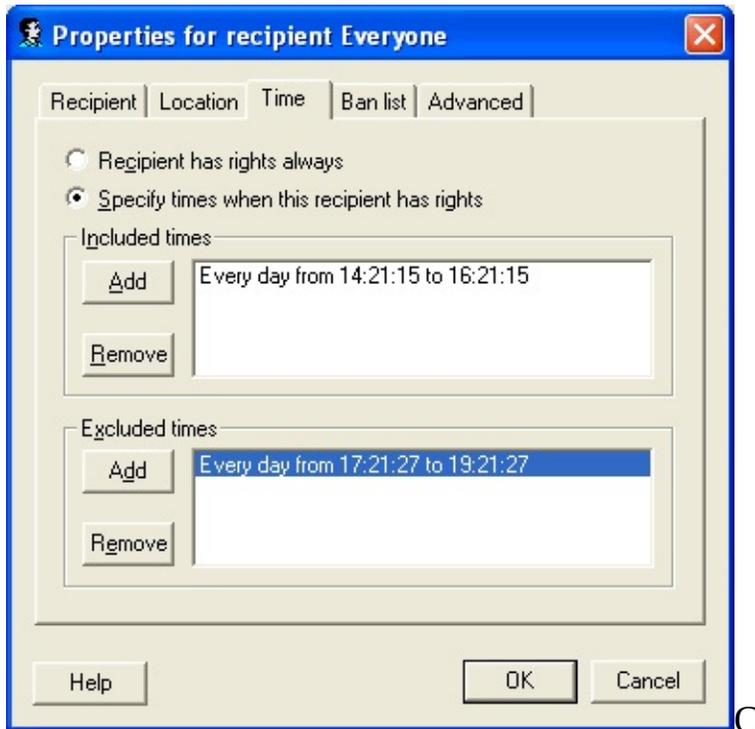
plage d'adresses. Cela permet d'ignorer certaines parties d'une adresse IP lors de la vérification des restrictions.

Leur utilisation est simple : ils fonctionnent de la même façon que pour les noms de fichiers DOS.

©2005 Qbik New Zealand Limited

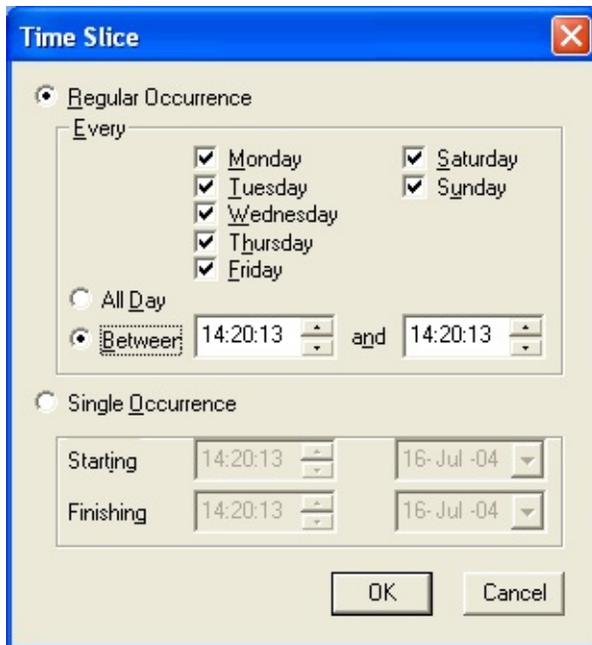
Onglet Horaires (*Time*)

Cet onglet précise à quel moment les droits s'appliquent.



Masquer | Masquer toutes les images

Par défaut, ils s'appliquent tout le temps mais vous pouvez également ne les accorder que certains jours, et même pendant une certaine **plage horaire (time-slice)**.

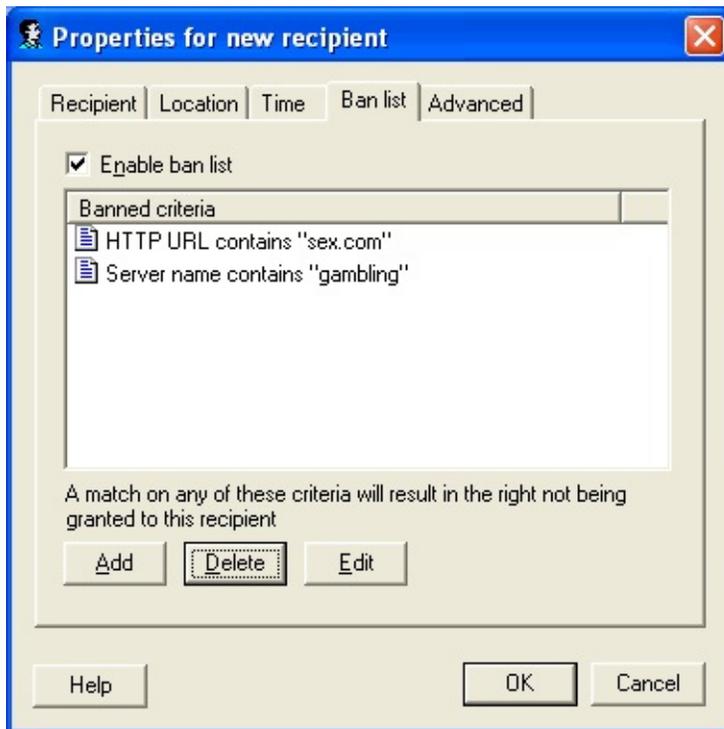


Masquer | Masquer toutes les images

La règle peut s'appliquer de façon continue (par ex. : du lundi au vendredi de 09:00:00 à 17:00:00) ou ponctuelle (par ex. : du 12 janvier 2005 à 12:00:00 au 13 janvier 2005 à 12:00:00).

Onglet Exclusions (*Ban List*)

Cet onglet permet de limiter de façon efficace l'accès des utilisateurs.



Masquer | Masquer toutes les images

Si un élément de cette liste est rencontré, la politique ne s'applique pas. (Cela peut être utilisé de façon globale ou bien par service.)

Exemple

Pour exclure un site spécifique pour tous les services :

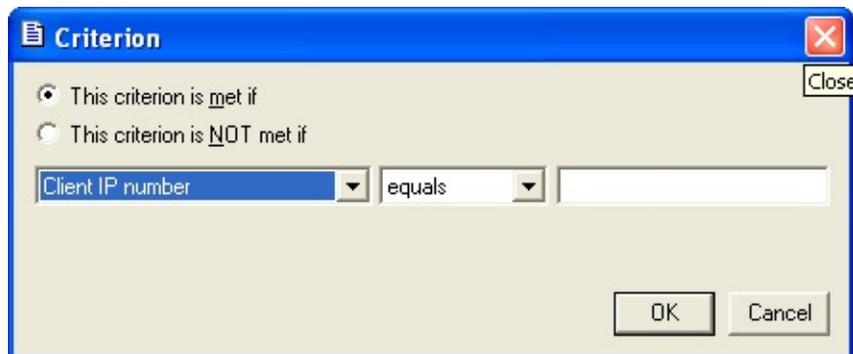
1. Ouvrez **GateKeeper**.

2. Cliquez sur l'onglet **Utilisateurs (Users)** et sélectionnez **Politiques système (System policies)**.



Masquer | Masquer toutes les images

3. Sélectionnez tous les utilisateurs.
4. Cliquez sur l'onglet **Exclusions (Ban list)**.
5. Cochez l'option **Activer la liste des exclusions (Enable ban list)**.
6. Cliquez sur **Ajouter (Add)**.
7. Dans **la fenêtre** qui s'ouvre ensuite, sélectionnez **Le critère s'applique si/ le nom du serveur/ est (This criteria is met if/Server name>equals)** et indiquez le nom du serveur à exclure.



Masquer | Masquer toutes les images

8. Cliquez sur **OK**.

Ce serveur figure alors dans la liste des exclusions.

Remarques :

La politique ne s'applique pas à l'utilisateur si sa requête concerne un élément exclus.

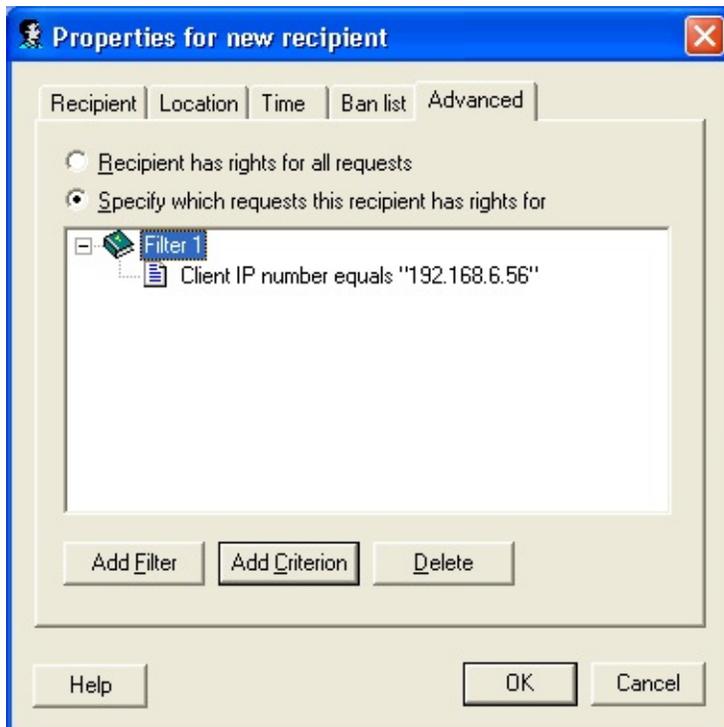
L'utilisateur ne peut donc accéder à aucun des éléments exclus.

Il est plus efficace de rejeter les URL contenant des termes spécifiques que des URL ou sites entiers.

Vous pouvez exclure certaines parties d'un site seulement en refusant l'URL contenant "www.nomduserveur.com/rep1/rep2/" : les autres répertoires du site sont toujours accessibles.

Onglet Avancé (*Advanced*)

Cet onglet permet d'appliquer des restrictions en fonction de la requête envoyée. Vous pouvez associer des critères requis et exclus afin de limiter les requêtes acceptées.



Masquer

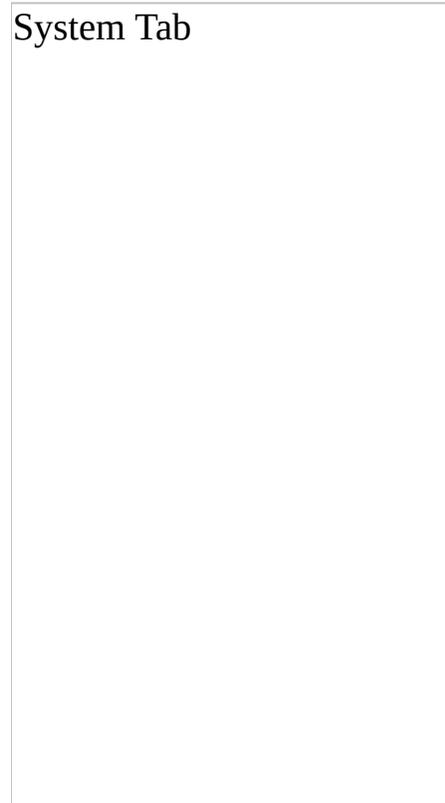
Si vous souhaitez appliquer une restriction, vous devez créer des filtres en fonction de certains critères. Si vous n'ajoutez aucun critère, la restriction n'est pas effective. Ces filtres fonctionnent de la même façon que ceux de la mémoire cache.

[Cliquez ici pour en savoir plus sur la création de règles, les filtres et les critères](#)

©2005 Qbik New Zealand Limited

Services système de WinGate

Les **services système** de WinGate sont efficaces et simples à configurer.



Masquer

Service	Description
DHCP	Fournit automatiquement les adresses IP aux postes clients du réseau.
WRP (<i>WinSock Redirector Service</i>)	Exécute les requêtes Internet provenant de postes sur lesquels WinGate Internet Client est installé.
GDP	Permet à WinGate Internet Client de localiser le

serveur sur le réseau.

DNS	Fournit la résolution DNS aux clients.
Service d'administration à distance (<i>Remote Control Service</i>)	Ce service est utilisé afin de modifier à distance la configuration de WinGate, par le biais d'un lien crypté.
POP3	Fournit les services POP3 au serveur de messagerie de WinGate.
SMTP	Fournit les services SMTP au serveur de messagerie de WinGate.
IMAP4	Fournit les services IMAP4 aux clients possédant des boîtes de ce type sur le serveur de messagerie de WinGate.
E-mail	Options du serveur de messagerie.
Cache (<i>Caching</i>)	Configuration de la mémoire cache du service proxy web (<i>WWW proxy service</i>).
Programmateur (<i>Scheduler</i>)	Permet de programmer divers évènements et les actions effectuées en conséquence.
Composeur (<i>Dialer</i>)	Configuration des profils de connexion disponibles pour l'accès Internet.
ENS (<i>Extended Networking</i>)	Configuration des services ENS de WinGate comme le pare-feu, le routage et le NAT (Network Address Translation).
Résolution DNS/WINS (<i>DNS/WINS Resolver</i>)	Permet de choisir les serveurs DNS et Wins utilisés pour les requêtes des clients.

Certificats (*Server
Certificates*)

Génère des certificats X509 pour les sessions en
SSL.

©2005 Qbik New Zealand Limited

Présentation du service DHCP

Qu'est-ce que le DHCP ?

DHCP signifie "Dynamic Host Configuration Protocol". Il s'agit d'une méthode standard permettant de configurer automatiquement l'accès Internet des ordinateurs clients (attribution d'adresses IP et serveurs DNS). Vous connaissez certainement le concept d'attribution d'adresses IP dynamiques. Lorsqu'un modem effectue une connexion PPP avec un FAI, un numéro IP lui est souvent attribué de façon dynamique.

A quoi sert-il ?

Avec le DHCP, les ordinateurs d'un réseau peuvent obtenir leurs paramètres TCP/IP (comme l'adresse IP) à partir d'un serveur centralisé **de façon automatique**. Le service DHCP de WinGate est différent des autres car il est capable de déterminer quelles sont les adresses à attribuer sans que l'administrateur ne doive prédéfinir des pools d'adresses (étendues). Il peut également déterminer de quelle façon la passerelle du client ainsi que de nombreux autres paramètres doivent être configurés. Ainsi, il n'est pas nécessaire d'avoir des connaissances approfondies pour utiliser ce service. Toutefois, les administrateurs ont également la possibilité de modifier manuellement tous les paramètres s'ils le souhaitent.

Pourquoi est-il recommandé de l'utiliser ?

La configuration TCP/IP ainsi que celle de WinGate sont facilitées. Lorsque ce protocole n'existait pas, une adresse IP statique unique devait être attribuée à tous les ordinateurs d'un réseau et le serveur DNS devait également être paramétré. Les anciens utilisateurs de WinGate se souviendront sans doute que 6 étapes étaient nécessaires à la configuration TCP/IP de chaque ordinateur client. Or, de nombreuses options peuvent poser problème, et il suffit que l'une d'entre elles soit mal paramétrée pour que le client ne puisse pas obtenir l'accès souhaité. Avec le DHCP, il suffit d'installer le TCP/IP et le tour est joué ! Le client DHCP est installé en tant que composant du TCP/IP. Si ce dernier est déjà installé, vous n'avez qu'à sélectionner l'option "Obtenir une adresse IP automatiquement" dans

Paramètres/Panneau de configuration/Connexions réseau/Protocole Internet. Le DHCP est la solution la plus facile : il garantit l'absence de conflits IP et d'erreurs de configuration.

Comment fonctionne-t-il ?

Lors du démarrage de Windows sur un ordinateur client, le client DHCP intégré dans le TCP/IP de Windows envoie sur le réseau un paquet de diffusion contenant une requête d'adresse IP. Lorsqu'un serveur DHCP "entend" cette requête, il envoie une réponse contenant une "proposition" d'adresse IP. Le client choisit alors parmi une série d'adresses IP possibles configurées sur le serveur DHCP. (Chaque série d'adresses est appelée "étendue".) Une fois l'adresse acceptée, les autres informations de configuration (y compris les détails concernant le serveur DNS) sont envoyées au client. Lorsque le bail IP du client est à moitié écoulé, celui-ci effectue une requête pour un nouveau bail. Un numéro IP différent peut alors lui être attribué. WinGate enregistre les détails concernant chaque bail actif et les intègre à ses règles, ce qui vous permet d'obtenir plus d'informations sur les ordinateurs connectés à WinGate.

Qu'en est-il de mes adresses IP statiques ?

Les ordinateurs de votre réseau qui ne peuvent bénéficier du DHCP peuvent toujours utiliser leur adresse IP existante. Avant d'attribuer une adresse, WinGate exécute la commande ping. Si une adresse répond cela signifie qu'elle est utilisée, elle ne sera donc pas affectée sur un autre ordinateur. Vous pouvez également indiquer une liste d'adresses à exclure pour chaque étendue créée (dans Paramètres/Panneau de configuration/Connexions réseau/Protocole Internet - TCP/IP.)

Que sont les réservations ?

Elles permettent de "réserver" une adresse IP à un ordinateur spécifique et d'empêcher qu'elle soit attribuée à un autre. Elles sont utilisées lorsque des applications spécialisées se connectent à des hôtes spécifiques utilisant également le DHCP. Cependant, avec l'intégration du DHCP dans le service DNS de WinGate, cette précaution devient superflue. Vous avez en effet la possibilité de vérifier les adresses IP des ordinateurs en fonction de leur nom

(nom Netbios et non nom d'hôte). Les réservations peuvent également être utilisées pour définir des paramètres TCP/IP par ordinateur.

Comment mettre en place le DHCP ?

La procédure pour passer d'un réseau où les adresses IP sont statiques à un réseau DHCP est très simple. Le serveur DHCP de WinGate est installé avec des paramètres par défaut fiables. Tous les ordinateurs de votre réseau peuvent utiliser le DHCP, sauf le serveur WinGate qui doit avoir des adresses statiques pour ses cartes LAN. Il s'agit d'une règle de base commune à tous les serveurs DHCP. Les adresses IP que vous indiquez pour les cartes LAN de votre serveur WinGate déterminent ensuite les adresses attribuées aux autres ordinateurs du réseau. Par exemple, si vous indiquez 192.168.0.1 pour une carte LAN, tous les ordinateurs directement connectés à cette carte (c'est à dire dans le même sous-réseau) auront des adresses comprises entre 192.168.0.2 et 192.168.0.254. Si vous possédez un réseau LAN avec plusieurs segments séparés par des routeurs, ces routeurs doivent exécuter des agents relais BOOTP. (Ou agents relais DHCP. Le DHCP utilise le format de paquet BOOTP afin que les paquets DHCP puissent être transférés par les agents relais BOOTP.) Pour attribuer les adresses, WinGate utilise l'adresse IP de l'interface d'un agent relais BOOTP sur laquelle une requête a été effectuée. Par conséquent, les adresses sont toujours attribuées dans le sous-réseau correspondant. Les masques réseau sont obtenus à partir de la RFC définissant les séries d'adresses IP. Il suffit de redémarrer les ordinateurs clients pour que le service DHCP fonctionne. (L'adresse attribuée est souvent identique à celles qu'ils possédaient déjà.)

Comment passer d'une attribution manuelle au DHCP ?

Effectuez l'opération suivante sur chaque ordinateur client :

1. Dans Démarrer/Paramètres/Panneau de configuration/Connexions réseau/ Protocole Internet /TCP-IP, décochez l'option **Utilisez l'adresse IP suivante** et cochez **Obtenir une adresse IP automatiquement**
2. Cliquez sur **OK**.
3. Redémarrez. En cas de conflit, redémarrez à nouveau l'ordinateur.

Si vous possédez un autre serveur DHCP sur votre réseau LAN, et que vous souhaitez le remplacer par celui de WinGate, il vous suffit de démarrer le service DHCP de WinGate, et d'arrêter l'autre. Lorsqu'un ordinateur client essaiera de renouveler son bail, il ne pourra pas se connecter avec son ancien serveur. Il devra donc envoyer un paquet de diffusion, ce qui permettra à WinGate de prendre le contrôle du bail.

Information générales

Ce service est automatiquement installé par WinGate et facile à configurer. Son mode de fonctionnement par défaut est "Entièrement automatique" (tout est fourni automatiquement : adresses IP, DNS et autres paramètres). Pour les utilisateurs avancés, le mode manuel permet de configurer tous les paramètres.

Voici une liste de définitions utiles :

Sous-réseau : Groupe d'ordinateurs connectés directement via un câble coaxial ou un concentrateur. Un ordinateur possédant deux adaptateurs réseau appartient à deux sous-réseaux.

Interface : Type de connexion à un réseau : carte réseau, modem, carte ISDN ou tout autre dispositif TCP/IP installé sur l'ordinateur.

Bail : Période au cours de laquelle une adresse IP dynamique peut être utilisée. Le client doit le renouveler auprès du serveur avant son expiration.

Réservation : Garantie qu'une adresse sera toujours attribuée au même ordinateur.

Étendue : Série d'adresses IP, accompagnées des options de configuration TCP/IP associées. Une étendue DHCP contient un pool d'adresses IP disponibles dans un même sous-réseau. Chaque étendue est associée à une interface et dispose de différentes propriétés.

Exclusions : Les adresses exclues ne seront attribuées à aucun ordinateur. Elles doivent faire partie d'une même étendue. En mode automatique, l'adresse IP du serveur WinGate est exclue.

Option : Définit un paramètre qui sera configuré dans le client DHCP (par ex. : le serveur DNS, ou la passerelle par défaut. Les options sont réparties sur trois niveaux : options globales, options d'étendue, et options de réservation. Les options de réservation sont prioritaires sur les options d'étendue, elles-mêmes

prioritaires sur les options globales).

Même en mode entièrement automatique, vous avez la possibilité de configurer manuellement certaines options d'étendue. Ce mode ne fait que définir les tâches effectuées automatiquement. Par conséquent, nous vous recommandons de commencer par utiliser ce mode, puis d'ajouter par la suite vos propres modifications.

Désactivation du service

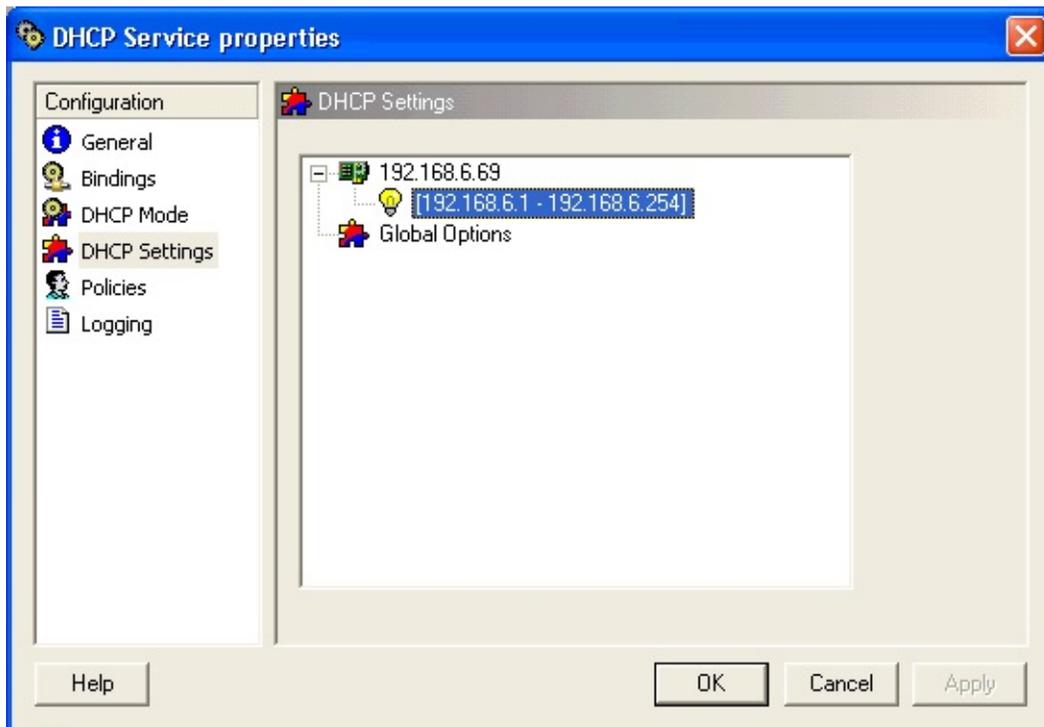
Il est recommandé d'utiliser le serveur DHCP de WinGate, mais il est tout à fait possible d'en utiliser un autre (ou de ne pas en utiliser du tout). Par défaut, le serveur de WinGate est installé et actif.

[Cliquez ici pour savoir comment désactiver le service DHCP](#)

©2004 Qbik New Zealand Limited

Paramètres DHCP

Les **paramètres DHCP** indiquent la configuration DHCP actuelle de votre réseau : carte interface et étendues (plages d'adresses) utilisées.



Masquer

Cette fenêtre affiche l'interface réseau contenant l'étendue utilisée. Il s'agit en règle générale de l'interface connectant le serveur au réseau local.

Au-dessous se trouve l'étendue, c'est à dire la plage d'adresses IP qui seront attribuées aux postes clients.

Double-cliquez sur une **Étendue** (icône représentant une ampoule) pour afficher ou modifier ses propriétés.

Double-cliquez sur une **Réservation** pour afficher ou modifier ses propriétés.

Double-cliquez sur **Options globales (Global Options)** pour configurer les **options DHCP**, s'appliquant à toutes les étendues, sur toutes les interfaces.

Les options par étendue ont priorité sur les options globales et s'appliquent à toutes les réservations d'une étendue. Les options par réservation ont priorité sur les options par étendue et ne s'appliquent qu'à la réservation concernée.

Création et renouvellement du bail

Pour créer et renouveler un numéro IP sur un ordinateur client :

Sous 95, 98 ou ME :

1. Cliquez sur **Démarrer / Exécuter**.
2. Indiquez **winipcfg** puis cliquez sur **OK**.
3. Assurez-vous que la carte réseau (NIC) est sélectionnée (et non l'adaptateur PPP).
4. Exécutez **renew**.
5. Exécutez **release**.

Sous 2000 / NT :

1. Ouvrez **l'invite de commandes**.
2. Exécutez **ipconfig /release** pour afficher les anciens paramètres.
3. Exécutez **ipconfig /renew** pour que les nouveaux paramètres du serveur DHCP soient pris en compte sur l'ordinateur.

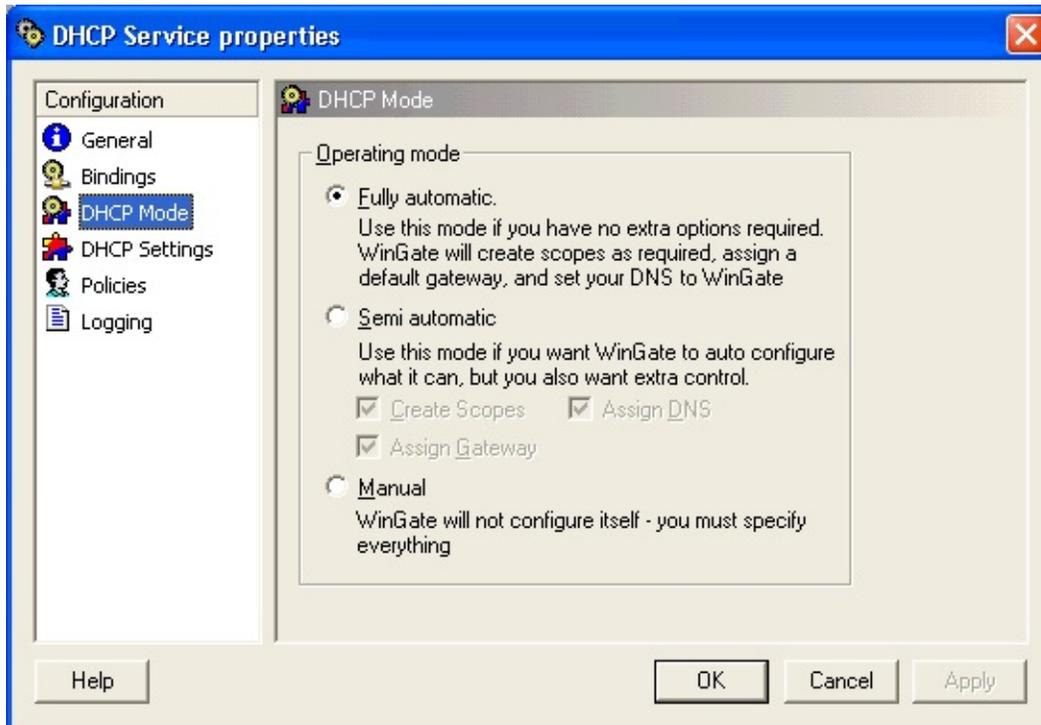
Vous serez probablement amené à redémarrer l'ordinateur.

Remarque :

Lorsqu'une réservation est attribuée à un client ou modifiée, le client ne change pas d'adresse automatiquement. Même dans ce cas il doit envoyer une requête de renouvellement.

Modes DHCP

Choisissez ici le **mode de fonctionnement** de ce service :



Masquer

Entièrement automatique (*Fully automatic*)

Tout s'effectue automatiquement. Tous les paramètres sont standard et fonctionnent dans presque tous les cas de figure. Le DNS est configuré directement sur le serveur WinGate. Il n'y a pas de réservations. La création d'étendues est basée sur l'adresse IP du serveur WinGate ou de l'agent relais DHCP. Ce mode est capable de gérer des agents relais DHCP et plusieurs sous-réseaux. La passerelle par défaut est configurée sur le serveur WinGate (si WinGate fonctionne sur un hôte connecté à plusieurs fournisseurs) ou bien sur l'adresse IP de l'agent relais.

Semi automatique (*Semi automatic*)

Permet de définir quelles tâches seront effectuées automatiquement.

Manuel (*Manual*)

Ne choisissez ce mode que si vous connaissez parfaitement le service DHCP et ses options. Il peut s'avérer utile pour des réseaux complexes comprenant de nombreux ordinateurs ayant des exigences différentes.

©2004 Qbik New Zealand Limited

Étendues DHCP

Ajouter une étendue

1. Dans les propriétés du service DHCP, cliquez sur **Paramètres (DHCP Settings)**.



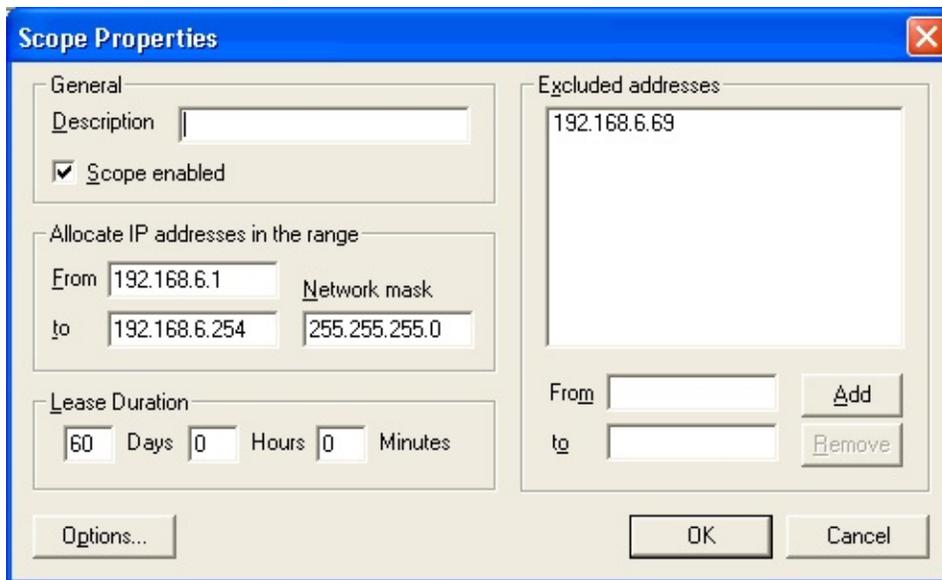
Masquer | **Masquer toutes les images**

2. Effectuez un clic droit sur l'**interface** pour laquelle vous souhaitez ajouter une étendue.
3. Sélectionnez **Nouvelle étendue (New scope)**.
4. Configurez-la comme indiqué ci-dessous.

Configuration

Vous pouvez modifier les paramètres d'une étendue déjà existante. Il est possible de l'augmenter, mais il est conseillé de ne pas la réduire (vous pouvez toutefois exclure des adresses).

1. Cliquez sur **Paramètres**.
2. Double-cliquez sur l'étendue que vous souhaitez modifier.
3. Une **fenêtre** s'ouvre ensuite, vous permettant de configurer l'étendue à votre guise.



Masquer | Masquer toutes les images

Propriétés générales :

Le nom choisi pour une étendue sera affiché dans les propriétés du service DHCP. Vous pouvez autoriser / refuser l'attribution d'adresses de cette étendue.

Attribuer des adresses IP comprises entre ... et ... (*Allocate IP addresses in the range from ... to ...*) :

Indique la plage d'adresses à attribuer. Les valeurs par défaut sont : 192.168.0.* pour les adresses et 255.255.255.0 pour le masque réseau. Les options avancées vous permettent également d'appliquer différents paramètres pour les plages ou masques.

Durée du bail (*Lease duration*) :

La durée par défaut est de 3 jours, ce qui convient pour la plupart des réseaux LAN. Si le nombre d'ordinateurs sur votre réseau LAN est supérieur au nombre d'adresses de l'étendue, il est préférable de raccourcir cette durée afin que tous puissent bénéficier des IP disponibles.

Exclusions :

Adresses IP faisant partie de l'étendue mais qui ne seront pas attribuées. Dans l'exemple ci-dessus, l'adresse 192.168.0.100 ainsi que toutes celles à partir de 220* 240 ne seront pas attribuées.

Ajouter une exclusion :

1. Dans les propriétés de l'étendue, indiquez le numéro IP à exclure dans le champ **de (from)**.
Pour exclure une plage, indiquez une adresse de fin dans le champ **à (to)**.
2. Cliquez sur **Ajouter**.

Supprimer une étendue

Vous pouvez supprimer une étendue du service DHCP lorsque par exemple vous n'utilisez plus un sous-réseau. Avant de supprimer une étendue, désactivez-la puis assurez-vous que tous les baux soient terminés.

1. Effectuez un clic droit sur l'étendue que vous souhaitez supprimer.
2. Cliquez sur **Supprimer (Delete)**.

Appliquer les options DHCP

D'autres options DHCP à imposer aux clients doivent également être configurées pour chaque interface. Ces options peuvent être communes à toutes les étendues (options globales) ou bien définies par étendue, ou par client :

Les options globales s'appliquent toujours lorsqu'elles sont activées, mais peuvent être annulées par celles concernant une étendue ou un client (prioritaires).

Les options d'une étendue s'appliquent à tous les ordinateurs de cette étendue lorsqu'elles sont activées, mais peuvent être annulées par celles d'un client.

Ne configurez que les options que vous connaissez suffisamment. Certaines sont liées entre elles (voir la liste des [Options DHCP](#)).

Pour instaurer une option de configuration DHCP :

1. Double-cliquez sur : l'étendue que vous souhaitez configurer, options globales ou bien une réservation spécifique.
2. Cliquez sur **Options**.

3. Sélectionnez dans la liste **Options disponibles (Available options)** celle que vous souhaitez configurer puis cliquez sur **Ajouter**.

Masquer | Masquer toutes les images

4. Double-cliquez sur une option de la liste **Options utilisées (Options in use)** pour la modifier.
5. Indiquez les informations souhaitées.
6. Cliquez sur **OK**.

Exemple :

Pour préciser les serveurs de nom DNS que les clients doivent utiliser, double-cliquez sur **Serveur DNS (DNS Server)** puis indiquez l'adresse d'un serveur. L'ordre de la liste est important : le premier serveur de la liste sera le premier consulté.

Pour supprimer une option configurée :

1. Sélectionnez-la et cliquez sur **supprimer**.
2. Cliquez sur **OK**.

Remarque :

Si vous désignez un serveur WINS, vous devez également configurer un type de nœud NBT.

Liaisons DHCP

L'option **Liaisons (Bindings)** fonctionne de façon différente pour le service DHCP : il n'est lié qu'à l'adaptateur interne.

Masquer

Pour des raisons de sécurité, le protocole DHCP ne vous autorise pas à effectuer de liaison avec un **modem** ou une interface **non statique**.

De plus, il n'est pas possible de créer une liaison avec localhost. Dans l'exemple, le serveur DHCP n'attribuera des numéros IP qu'aux ordinateurs dont la requête a été reçue sur 192.168.6.69

Remarque :

Vous devez créer une liaison pour toute les interfaces avec lesquelles vous souhaitez utiliser le **DHCP**.

Réservations DHCP

Il est possible de réserver une adresse IP pour un client spécifique, ce qui peut s'avérer utile s'il est nécessaire que son adresse ne change jamais. Cette fonctionnalité n'est pas disponible en mode entièrement automatique.

Remarques :

Si plusieurs serveurs DHCP attribuent des adresses dans une même étendue, la réservation doit être identique pour chaque serveur. Dans le cas contraire, le client recevra une adresse différente en fonction du serveur qui a répondu.

Vous pouvez à tout moment changer les informations concernant la réservation.

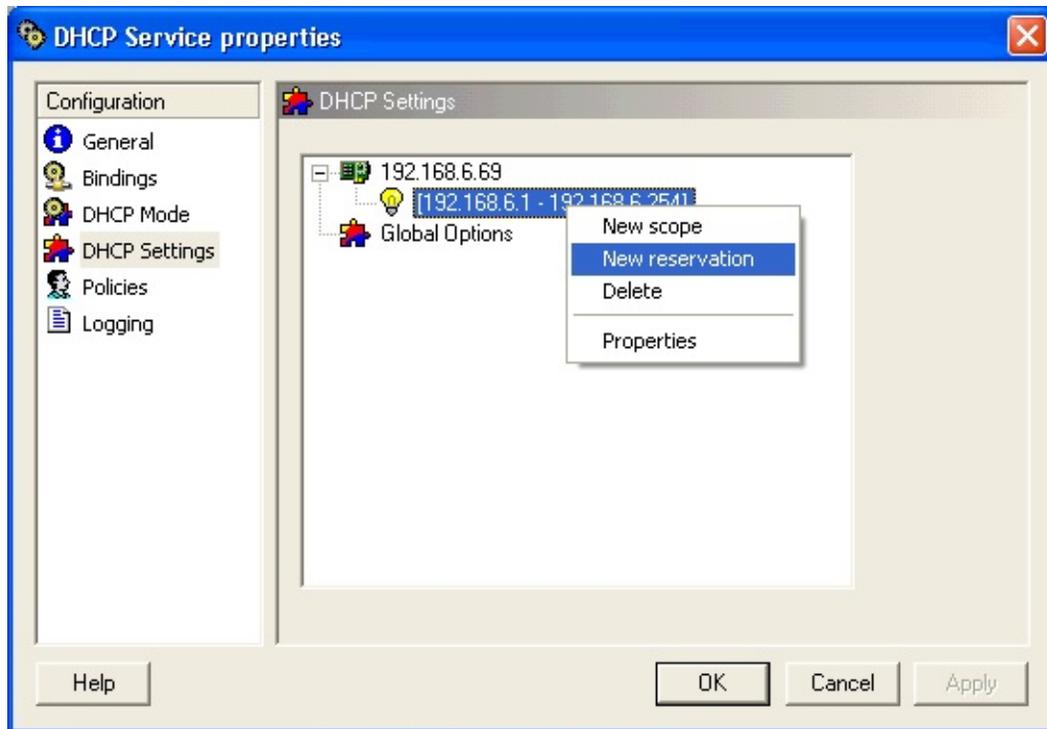
La réservation d'une adresse n'oblige pas le client qui l'utilise à en changer. Avant de réserver une nouvelle adresse, ou une adresse différente de celle actuellement utilisée, assurez-vous qu'elle n'a pas déjà été attribuée. Si l'adresse est déjà utilisée par un client, celui-ci doit la "libérer" à l'aide d'une requête spécifique.

Ajouter une réservation

Le service DHCP de WinGate permet de créer des réservations en fonction du nom de l'ordinateur ou de l'adresse MAC de sa carte LAN. Il est recommandé d'utiliser le nom de l'ordinateur, car même si vous changez de matériel la réservation sera toujours valable.

Procédure à suivre :

1. Dans les propriétés du service DHCP, cliquez sur Paramètres (*DHCP Settings*).
2. Effectuez un clic droit sur l'**étendue** dans laquelle vous souhaitez ajouter la réservation.



Masquer | Masquer toutes les images

3. Sélectionnez **Nouvelle réservation** (*New reservation*).
4. Dans **la fenêtre** qui s'ouvre ensuite, indiquez le client souhaité.



Masquer | Masquer toutes les images

5. Dans le champ **Adresse IP**, indiquez une adresse incluse dans cette étendue (n'importe laquelle, à condition qu'elle ne soit pas utilisée).
6. Vous disposez de deux options pour identifier l'ordinateur client : **nom de l'ordinateur** ou **adresse MAC**. Nous vous recommandons de l'identifier par son nom car ainsi cela fait référence à l'ordinateur lui-même et non uniquement à la carte.
7. Cliquez sur **Ajouter** pour enregistrer la réservation dans la base de

données. Il est possible d'ajouter plusieurs réservations sans devoir fermer la fenêtre.

Déterminer l'adresse MAC d'un ordinateur client :

Sous NT / 2000 : exécutez la commande **ipconfig /all** sur l'ordinateur client.

Sous 95 / 98 / ME : exécutez la commande **winipcfg** puis cliquez sur le bouton **Plus>>**.

Modifier la réservation

Les informations concernant la réservation peuvent être modifiées à tout moment. Ces modifications ne seront effectives qu'après le renouvellement du bail.

Options configurables du service DHCP

Vous trouverez ci-dessous une liste des **options configurables** dans le serveur DHCP de WinGate. La plupart des clients DHCP ignorent ces options. Nous vous recommandons de ne modifier que celles que vous comprenez parfaitement. Cette liste n'est proposée qu'à titre indicatif : en effet, vous ne devriez presque jamais changer ces options.

Masquer

Décalage horaire (*Time offset*)

Indique le décalage avec le temps universel UCT en secondes.

Routeur (*Router*)

Définit une liste d'adresses IP pour les routeurs du sous-réseau du client.

Serveur de temps (*Time server*)

Définit une liste d'adresses IP pour les serveurs de temps auxquels le client a accès.

Serveur de nom (*Name servers*)

Définit une liste d'adresses IP pour les serveurs de nom auxquels le client a accès.

Serveurs DNS (*DNS servers*)

Définit une liste d'adresses IP pour les serveurs DNS auxquels le client a accès.

Serveurs de fichiers journaux (*Log servers*)

Définit une liste d'adresses IP pour les serveurs de fichiers journaux MIT_LCS User Datagram Protocol (UDP) auxquels le client a accès.

Serveurs de cookies (*Cookie servers*)

Définit une liste d'adresses IP pour les serveurs de cookies RFC 865 auxquels le client a accès.

Serveurs de fichiers journaux RCS (*RCS Log servers*)

Définit une liste d'adresses IP pour les serveurs d'impression en ligne RFC 1179 auxquels le client a accès.

Serveurs Impress (*Impress servers*)

Définit une liste d'adresses IP pour les serveurs Imagen Impress auxquels le client a accès.

Serveurs RLP (*RLP servers*)

Définit une liste de serveurs de localisation de ressources RFC 887 auxquels le client a accès.

Nom d'hôte (*Host name*)

Définit un nom d'hôte pour le client (jusqu'à 63 caractères). Le premier caractère doit être une lettre et le dernier un chiffre. De plus, les seuls caractères autorisés sont les lettres, chiffres, et traits d'union. Ce nom peut être qualifié à l'aide du nom de domaine DNS local.

Taille du fichier d'initialisation (*Boot file size*)

Définit la taille du fichier image d'initialisation pour le client, en blocs de 512 octets.

Fichier de vidage Merit (*Merit dump file*)

Définit (en caractères ASCII) le chemin du fichier dans lequel l'image mémoire principale est vidée en cas d'échec.

Nom de domaine (*Domain name*)

Définit le nom de domaine DNS que le client doit utiliser pour les résolutions de nom d'hôte.

Serveur Swap (*Swap server*)

Définit l'adresse IP du serveur Swap du client.

Chemin d'accès racine (*Root path*)

Définit (en caractères ASCII) le nom de chemin du disque racine du client.

Chemin d'accès extensions (*Extensions path*)

Définit un fichier accessible via le protocole TFTP, contenant des informations à interpréter de la même façon que le champ extension fournisseur de la réponse BOOTP. Toutefois, le fichier n'est pas limité dans sa longueur et les références

au Tag 18 sont ignorées.

Réexpédition des couches IP (*IP layer forwarding*)

Active ou désactive la réexpédition des paquets IP pour ce client.

Routage source non local (*Non-local source routing*)

Active ou désactive la réexpédition des paquets avec des routages source non locaux.

Filtre stratégique (*Policy filter masks*)

Définit des filtres stratégiques, constitués d'une liste d'adresses IP et de masques indiquant les paires de masques de destination utilisés pour filtrer les routages source non locaux. Si l'adresse du prochain saut d'un paquet provenant d'un routage source ne correspond pas au filtre, elle sera refusée par le client.

Taille max. de réassemblage des paquets (*Max Datagram reassembly size*)

Définit la taille maximum des paquets pouvant être rassemblés par le client.
Valeur minimum : 576.

Durée de vie par défaut (*Default time-to-live*)

Définit la durée de vie (TTL, *Time to Live*) par défaut que le client utilise pour les paquets sortants. La valeur pour un octet est un nombre compris entre 1 et 255.

Tous les sous-réseaux sont locaux (*All subnets are local*)

Indique si le client doit supposer que tous les sous-réseaux servant en réseau d'interconnexion utilisent la même MTU que le sous-réseau local auquel le client est connecté. 1 = tous les sous-réseaux partagent la même MTU; 0 = le client doit présumer que certains sous-réseaux ont des MTU de taille inférieure.

Adresse de diffusion (*Broadcast address*)

Définit l'adresse de diffusion utilisée dans le sous-réseau du client.

Recherche de masques (*Mask discovery*)

Indique si le client doit utiliser le protocole ICMP (Internet Control Message Protocol) pour rechercher les masques de sous-réseau.

Fournisseur de masques (*Is Mask supplier*)

Indique si le client doit répondre aux demandes de masques de sous-réseau en

utilisant le protocole ICMP.

Recherche de routeurs (*Router discovery*)

Indique si le client doit utiliser la méthode de recherche de routeurs indiquée dans la norme RFC 1256 pour la sollicitation de routeurs.

Adresse de sollicitation de routeurs (*Router solicitation address*)

Définit l'adresse IP à laquelle le client soumet les sollicitations de routeurs.

Encapsulation de code de fin (*Trailer encapsulation*)

Indique si le client doit négocier l'utilisation de codes de fin (RFC 983) lors de l'utilisation du protocole ARP.

Délai de cache ARP (*ARP cache timeout*)

Indique (en secondes) le délai pour les entrées de cache ARP.

Encapsulation Ethernet (*Ethernet encapsulation*)

Indique si le client doit utiliser l'encapsulation Ethernet version 2 (RFC 894) ou IEEE 802.3 (RFC 1042) lorsque l'interface est Ethernet.

Durée de vie par défaut (*Default time-to-live*)

Définit la durée de vie par défaut que le client doit utiliser lorsqu'il envoie des segments TCP. La valeur minimum pour un octet est 1.

Intervalle de conservation de connexion TCP (*Keepalive interval*)

Définit (en secondes) combien de temps le client doit attendre avant d'envoyer un message de conservation de connexion (keepalive) pour une connexion TCP.

Octet de conservation de connexion (*Keepalive garbage*)

Indique si le client doit envoyer des messages de conservation de connexion TCP contenant un octet de données parasites.

Nom de domaine NIS (*NIS domain name*)

Définit le nom de domaine NIS (Network Information Service) sous forme d'une chaîne ASCII.

Serveurs NIS (*NIS servers*)

Indique une liste d'adresses IP pour les serveurs NIS auxquels le client a accès.

Serveurs NTP (*NTP servers*)

Indique une liste d'adresses IP pour les serveurs NTP (Network Time Protocol) auxquels le client a accès.

Serveurs WINS/NBNS (*WINS/NBNS servers*)

Indique une liste d'adresses IP pour les serveurs NBNS (NetBIOS name servers).

NBDD NetBIOS sur TCP/IP (*NetBIOS over TCP/IP NBDD*)

Indique une liste d'adresses IP pour les serveurs NBDD (NetBIOS datagram distribution servers).

Type de nœud WINS/Netbt (*WINS/Netbt node type*)

Permet la configuration du type de nœud client pour les clients NetBIOS sur TCP/IP (NetBT), conformément à la norme RFC 1001/1002. Les options possibles sont b-node, p-node, m-node, et h-node.

ID d'étendue NetBIOS (*NetBIOS scope ID*)

Définit l'identification d'étendue NetBIOS sur TCP/IP utilisée par le client, conformément à la norme RFC 1001/1002.

Serveurs de police X Window (*X Window font server*)

Indique une liste d'adresses IP pour les serveurs X Window auxquels le client a accès.

Serveurs de gestionnaire d'affichage X Window (*X Window system display*)

Indique une liste d'adresses IP pour les serveurs X Window System Display auxquels le client a accès.

Désactivation du service DHCP

Selon la configuration et le fonctionnement de votre réseau, vous serez peut-être amené à désactiver le service DHCP.

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Ouvrez le **service DHCP**.

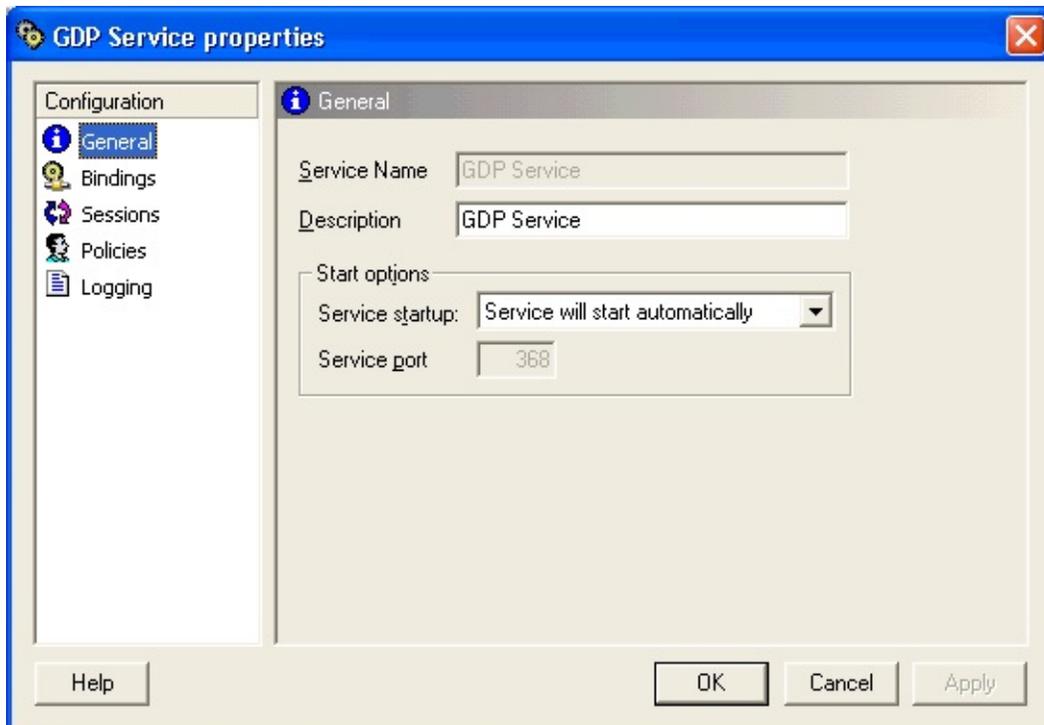
Masquer

4. Dans les options de démarrage (fenêtre **Général**), sélectionnez **désactivé (Service is disabled)**.
5. Cliquez sur **OK** et fermez la fenêtre.

Le service est alors désactivé et ne pourra plus attribuer d'adresses IP aux postes clients.

Service GDP (Generic Discovery Protocol)

Qbik New Zealand a développé le **protocole GDP** afin de pouvoir "rechercher" et identifier les serveurs de connexion à Internet (tels que WinGate). WinGate Internet Client (WGIC) et GateKeeper l'utilisent pour détecter WinGate. Une fois installé, il fonctionne de façon entièrement automatique.



Masquer

Le service GDP recherche les messages de diffusion des clients sur le port 368. Lorsque WGIC est installé sur les postes clients, il envoie une "requête de diffusion" afin d'identifier les serveurs WinGate, dont la liste s'affiche ensuite.

Informations générales :

Un seul service GDP suffit

Il doit être obligatoirement sur le port 368

Les clients WRP l'utilisent pour identifier WinGate automatiquement

Il est recommandé de ne créer de liaisons qu'avec les interfaces internes

Ce service est parfois appelé Gateway Discovery Protocol

©2004 Qbik New Zealand Limited

Service WRP (Winsock Redirection Protocol)

Le **service WRP** (Winsock Redirection Protocol) fonctionne sur le serveur WinGate et permet à vos applications d'agir comme si elles étaient directement reliées à Internet. Une fois WinGate Internet Client (WIC) installé sur les postes clients, aucune configuration logicielle n'est requise.



Masquer

Le service WRP connecte vos applications directement à Internet tout en offrant les avantages d'un serveur proxy et la sécurité d'un pare-feu.

Avec WRP, vos applications clientes peuvent :

Établir des connexions TCP (navigation web)

Accepter des connexions TCP (comme un serveur web)

Envoyer des paquets UDP (pour des lecteurs comme Real Audio)

Accepter des paquets UDP (comme un serveur RA).

Service WRP et applications clientes

Prenons l'exemple d'une application Internet sur le poste client qui tente d'établir une connexion avec un ordinateur sur Internet. Le client WRP détecte cette tentative de connexion et détermine la nature de la requête. S'il s'agit d'une connexion à un ordinateur implanté sur le même réseau, WRP laisse l'application établir la connexion directement.

S'il s'agit d'une tentative de connexion à un ordinateur sur Internet (autrement dit, sur un réseau différent), alors le client WRP "intercepte" la connexion et l'envoie au service WRP de WinGate.

Il n'est pas nécessaire de définir un proxy différent pour chaque service. Il gère les connexions directement, vous n'avez plus à le faire au niveau des applications.

Il fonctionne par défaut sur le port 2080.

Serveurs

Ce service écoute également pour le serveurs les connexions provenant d'Internet sur les clients possédant WGIC.

Exemple :

Si l'un des vos postes clients possède un serveur de messagerie, vous pouvez configurer le service WRP afin qu'il écoute les requêtes provenant d'Internet et les transfère au poste serveur.

[Cliquez ici pour savoir comment ce service gère les applications](#)

©2004 Qbik New Zealand Limited

Configuration centralisée - Onglet Paramètres généraux (*General Settings*)

Cet onglet permet de configurer la gestion par défaut des applications.

Masquer

Paramètres (*Defaults*)

Mode par défaut (*Default Mode*) :

Local (Non LSP) (*Local - No LSP*)

Mixte (connexions uniquement, serveurs refusés) (*Mixed - Connections only, no servers*)

Global (Utiliser LSP) (*Global - Use LSP*)

Accès refusé (pas d'accès Internet) (*Networking denied - No internet access*)

Application refusée (non autorisée) (*Application terminated - Not allowed to run*)

Le mode par défaut est utilisé si l'application est introuvable dans la Liste des applications (onglet Applications) ou si cette liste est désactivée.

Remarque :

En utilisant un mode par défaut qui ferme les applications et en désignant les applications que vos utilisateurs sont autorisés à exécuter, vous évitez que des programmes non autorisés ne soient utilisés sur votre réseau.

[Cliquez ici pour en savoir plus sur les modes du service WRP.](#)

Suivre les connexions (*Track connections*)

Cochez cette case pour suivre les connexions de chaque mode sélectionné.

Informez l'utilisateur si l'accès Internet est refusé (*Inform the user if internet access is denied*)

L'utilisateur est informé par un message système sur le client.

Informez l'utilisateur si une application est fermée (*Inform the user if an application will be terminated*)

L'utilisateur est informé par un message système sur le client.

Général

Vérifier la liste globale des applications (*Check the central applications list*)

Pour les politiques liées à chaque application.

Vérifier la liste des applications du client (*Check the clients applications list*)

Pour les politiques liées à chaque application - l'utilisation de la liste centralisée est plus sécurisée..

Utiliser WGIC pour l'authentification seulement (*Use WGIC for authentication only*)

Permet au serveur de savoir qui est le client ; WGIC n'acceptera ni les applications de socket, ni les autres applications.

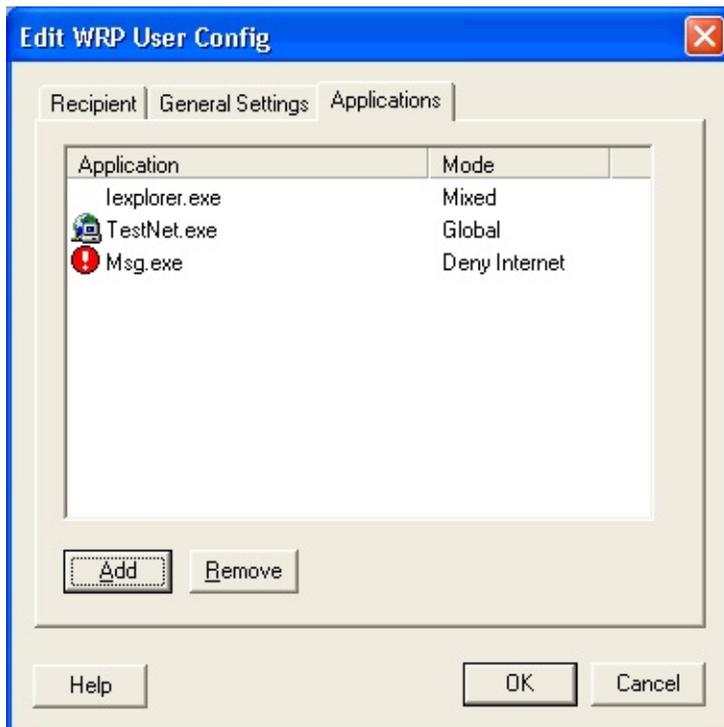
Remarque :

LSP signifie "Layered Service Provider". Il s'agit d'un pilote système relié aux services réseau de Windows. Il accède à l'ensemble des données qui entrent et sortent de l'ordinateur, et possède la capacité de modifier ces données. Certains LSP sont indispensables pour autoriser Windows à vous connecter à d'autres ordinateurs, y compris à Internet.

©2005 Qbik New Zealand Limited

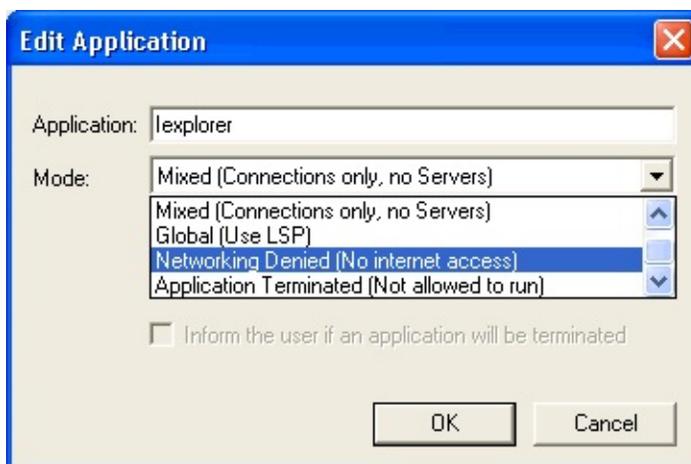
Configuration centralisée - Onglet Applications

Choisissez dans **cet onglet** le mode appliqué aux applications clientes lorsqu'elles effectuent une requête.



Masquer | Masquer toutes les images

Pour cela, cliquez sur **Ajouter (Add)**.



Masquer | Masquer toutes les images

Application :

Nom de l'application souhaitée. Il comporte toujours l'extension .exe. Veillez à entrer seulement le nom de l'application - n'indiquez pas le chemin.

Mode :

Sélectionnez l'une des entrées suivantes :

Mixte (connexions uniquement, serveurs refusés)

Global (Utiliser LSP)

Accès refusé (Pas d'accès Internet)

Application refusée (non autorisée)

Suivre les connexions vers l'application - cochez cette case pour suivre les connexions vers cette application.

Informé l'utilisateur si l'accès à Internet est refusé - par un message système.

Informé l'utilisateur si une application est fermée - par un message système.

[Cliquez ici pour en savoir plus sur les modes.](#)

Remarque :

La configuration centralisée de WRP est seulement disponible avec les licences WinGate 6 Enterprise.

©2005 Qbik New Zealand Limited

Foire aux questions sur WRP

Qu'est-ce que WRP ?

Winsock Redirection Protocol est une spécification conçue pour rediriger les requêtes Winsock. Elle permet aux postes clients d'accéder à Internet sans proxy ni connexion directe.

Qu'est-ce que le service WRP ?

Winsock Redirection Protocol Service correspond au serveur de WinGate qui offre un accès WRP (tout comme un serveur FTP offre un accès FTP).

Qu'est-ce que WGIC ?

WinGate Internet Client est le logiciel qui autorise les postes clients à utiliser le service WRP sur le serveur WinGate. Invisible, il se configure dans le Panneau de configuration.

Quels sont les avantages de WRP ?

Tout d'abord, WRP est simple d'utilisation. Aucune configuration client n'est requise ; une fois installé, le client WinGate se charge de tout. La configuration de WinGate est également simple. Souvent, seuls 5 services au lieu de 15 sont requis.

De plus, WRP est rapide. Une fois installé, vous ne perdez plus de temps à faire fonctionner vos applications.

Quels sont ses inconvénients ?

Comme toutes les connexions s'effectuent à partir du serveur WinGate, sur les ports requis par les applications clients, des conflits de ports peuvent se produire.

Dois-je avoir des connaissances approfondies en matière de réseau ?

Non. Il s'agit là du point fort de ce service : il fonctionne de façon invisible. Une

fois installé, WinGate Internet Client travaille pour vous.

Comment installer WRP ?

Le service WRP doit être installé sur le serveur WinGate (il s'agit d'un service système ordinaire de WinGate installé par défaut). Les postes clients sont autorisés à utiliser ce service simplement en installant WinGate Internet Client.

J'ai lancé l'installation, mais je ne vois pas WinGate Internet Client

C'est normal. WGIC fonctionne en toute transparence : il est toujours prêt mais vous ne le voyez pas. Il ne requiert aucune configuration. Une icône est simplement ajoutée dans le Panneau de configuration.

Mon réseau est-il sécurisé si j'utilise WRP ?

Oui. Le service WRP est entièrement sécurisé. Il fonctionne seulement sur les ordinateurs de votre réseau local. Si, par accident, vous exécutez un serveur sur un ordinateur client, il ne sera accessible depuis Internet que si vous l'autorisez.

Comment configurer WRP pour qu'il bloque toutes les applications sauf celles que j'ai choisies ?

Il suffit d'activer l'option permettant de refuser les applications clientes (apparue dans les versions 3.05 et supérieures).

Ensuite, modifiez la politique du service :

1. Les droits par défaut sont ignorés
2. Ajouter dans la liste de rejet le critère "Not client application name is empty" pour tous les utilisateurs. Ces deux entrées interdisent toutes les applications pour tout le monde. Donc :
3. Ajouter dans cette liste le critère "Not client application name equals X" (X correspond à TELNET.EXE)
4. Ajouter "Not client application name equals Y" (Y correspond à NETSCAPE.EXE). Ces deux critères s'appliquent à tous les utilisateurs.

Maintenant, le client peut seulement exécuter les applications X et Y. Cela permet d'avoir un contrôle centralisé sur ce qu'une application WRP peut et ne peut pas rediriger.

Cependant, il ne s'agit pas d'une solution miracle. Gardez à l'esprit qu'un utilisateur peu scrupuleux peut très bien contourner cette procédure en modifiant le nom du fichier .EXE que vous avez décidé d'interdire (ex.: vous interdisez netscape.exe mais autorisez telnet.exe. En renommant le fichier netscape.exe par telnet.exe, l'utilisateur contourne l'interdiction.)

Est-ce simple à utiliser ?

Très simple. WRP est conçu pour fonctionner sans aucune intervention de l'utilisateur.

Pourquoi utiliser WRP ?

Avec WRP, vous économisez du temps et de l'argent en termes de configuration réseau. WRP est idéal pour les administrateurs réseau puisqu'il n'est plus nécessaire de configurer un pare-feu pour les applications clientes.

WRP fonctionnera-t-il avec mes anciennes applications ?

Oui. Le client WRP permet aux applications TCP et UDP de fonctionner comme si elles étaient directement connectées à Internet.

Joue-t-il le rôle de relais ?

Oui. Les applications TCP et UDP fonctionnent comme si elles étaient directement connectées à Internet

Comment configurer les applications ?

Il n'est pas nécessaire de configurer les applications pour que WRP fonctionne. Finis les paramètres proxy, les liens mappés et les fichiers hosts.

Puis-je utiliser plusieurs versions de WinGate simultanément ?

Oui. Chaque client WRP peut gérer plusieurs moteurs WinGate sur un réseau. La

version la plus adéquate sera utilisée. Si une version est occupée, le client se servira d'une autre.

Qu'est-ce que GDP ?

GDP signifie Generic Discovery Protocol. Ce protocole est un standard Internet enregistré auprès de l'IANA et qui utilise le port 368. Il sert à retrouver des ordinateurs passerelle sur le réseau.

WRP est-il un standard ?

Oui. WRP utilise GDP pour détecter les installations WinGate. WRP est un protocole conçu pour les redirections Winsock. WRP et GDP sont deux spécifications créées et développées par Qbik New Zealand Ltd.

Quel est son niveau de compatibilité ?

WRP est à 100% compatible avec les PC équipés de Windows 95, 98, NT4 ou d'une version supérieure.

WRP sera-t-il compatible avec les Macintosh installés sur mon réseau ?

Le client WRP est seulement compatible avec Windows 95, 98 et NT. Les autres ordinateurs devront être équipés de serveurs proxy WinGate ou du service NAT (NAT a été introduit dans la version 4.0 de WinGate).

Faut-il une formation pour apprendre à s'en servir ?

Non. Aucune formation n'est requise. WRP fonctionne en toute transparence, l'utilisateur n'a pas besoin de savoir comment il fonctionne ni comment il se connecte à Internet.

Puis-je utiliser plusieurs services WRP sur mon réseau ?

Oui. Chaque client WRP peut gérer plusieurs moteurs WinGate sur le réseau. Le serveur WinGate le plus approprié sera utilisé. Si un serveur WinGate est occupé, le client se tournera vers un autre (sauf indication contraire de votre part).

Fonctionnera-t-il avec mes serveurs Intranet ?

Oui. WRP n'affecte pas les connexions aux ordinateurs de votre réseau local.

Que signifie WRP pour les développeurs de logiciels ?

WRP est une avancée : les applications clientes TCP, UDP et les applications serveur fonctionnent sans proxy. De même, la configuration d'un pare-feu n'est plus nécessaire pour accéder à Internet.

©2004 Qbik New Zealand Limited

WRP - Configuration des serveurs

Si vous possédez des serveurs installés sur les postes clients de WinGate, suivez cette procédure afin qu'ils puissent recevoir les requêtes provenant d'Internet :

1. Configuration du pare-feu sur le serveur WinGate :

1. Ouvrez **GateKeeper**.
2. Cliquez sur **Service réseau avancé (*Extended Networking Services*)** dans l'onglet **Systeme**.
3. Cliquez sur l'icône **Sécurité des ports (*Port security*)**.
4. Cliquez sur **Ajouter (*Add*)**.
5. Dans la fenêtre qui s'ouvre ensuite, sélectionnez à quel type de connexion s'applique le filtre (**Connexions provenant d'Internet, *Connections from the Internet***), et le protocole approprié (**TCP** ou **UDP**).
6. Indiquez le numéro de port écouté par l'application serveur (par exemple : 21 pour un serveur FTP) et éventuellement une description.
7. Dans la partie **Action (*Action to take*)** (action à effectuer lorsqu'un paquet arrive sur ce port), sélectionnez **Autoriser (*Allow*)**.
8. Cliquez sur **OK** pour enregistrer les modifications.

2. Configuration du poste client (avec WGIC) :

1. Ouvrez l'applet **WGIC**.
2. Sélectionnez l'onglet **Applications utilisateur (*User Applications*)**.

3. Cliquez sur **Ajouter (Add)** et sélectionnez le fichier exécutable de l'application serveur.
4. Sélectionnez l'option **Global (Global Access)**.
5. Cliquez sur **OK** pour enregistrer les modifications.

A l'attention des développeurs d'applications Winsock

Voici quelques conseils destinés aux développeurs d'applications Winsock 2, afin que les programmes créés soient compatibles avec le service WRP de WinGate (Winsock Redirection Protocol).

1. Évitez d'appliquer des protocoles pour lesquels le client indique au serveur de façon explicite : son adresse IP, le port utilisé pour certaines connexions ou pour retourner des données au serveur. En effet :
 - Dans un système NAT, le client ne connaît probablement pas son IP réelle, et ne possède pas de dispositif permettant de la découvrir.
 - Le serveur peut identifier le client à l'aide de la fonction "getpeername". Il est donc inutile de transmettre ces informations s'il les possède déjà (de plus, cela risque de causer des erreurs).
2. Évitez d'utiliser des numéros de ports fixes dans les applications clientes. Si le client doit accepter une connexion ou recevoir des données sur un port, le numéro doit être attribué par le système d'exploitation (en utilisant la fonction "bind()" avec un numéro de port égal à zéro). Veillez à utiliser cette méthode avec précaution car cela risque d'interférer avec certains systèmes NAT. La meilleure solution consiste à laisser le client demander les connexions nécessaires.
- 3.

N'oubliez pas qu'un ordinateur peut posséder plusieurs adresses IP. Ainsi, si vous appliquez "gethostbyname()" sur le résultat de "gethostname()" et utilisez la première adresse IP renvoyée, cela fait échouer de nombreuses applications. Si vous avez besoin de connaître votre adresse IP, veillez à l'obtenir en fonction de l'interface de l'ordinateur local qui communique avec l'autre hôte. Pour cela :

Si vous disposez d'une connexion ouverte à l'autre hôte, utilisez "getsockname()" sur ce socket afin d'obtenir votre adresse.

Si ne disposez pas d'une telle connexion, établissez une connexion "fictive" avec un service connu de l'autre hôte, et utilisez getsockname() sur le socket.

Si vous ne savez pas à quel service vous connecter, liez un socket "fictif" à chaque interface connue, et essayez de vous connecter à l'hôte sur un port au hasard. Si vous tentez de vous connecter sur une mauvaise interface, la tentative échoue rapidement et indique WSAENETUNREACHABLE. Si vous êtes sur la bonne interface, la connexion réussit ou bien elle est refusée.

Vous pouvez également utiliser le protocole SNMP afin d'obtenir la table de routage de votre ordinateur, et en déduire l'adresse IP.

Enfin, vous pouvez déterminer l'interface à l'aide des appels Winsock 2 .

Remarques :

Si vous utilisez le service WRP et WinGate Internet Client, ou un client et serveur socks, TOUS les postes clients possèdent plusieurs adresses IP. Le point numéro 3 (ci-dessus) est donc particulièrement important.

Certains proxies de niveau circuit ne peuvent pas utiliser getsockname() et getpeername(), et afficher l'interface sur le serveur. Toutefois, avec le WRP et WGIC cette opération est possible.

Service DNS : présentation

Le **service DNS** (Domain Name System) permet de localiser les noms de domaines Internet et de les convertir en adresses IP. Un nom de domaine est une façon de désigner une adresse afin de la retenir plus facilement.

En règle générale, ce service fonctionne de façon presque autonome, mais il est parfois nécessaire de le configurer afin de pouvoir utiliser le serveur SOCKS. Il est recommandé de désactiver le serveur DNS de WinGate si vous utilisez déjà un autre serveur sur cet ordinateur, car cela risque d'entraîner des problèmes.

Masquer

Autoriser les requêtes à démarrer le composeur (*Allow Request to initiate dialer*)

Cochez cette option si vous souhaitez que les requêtes DNS puissent lancer une session Internet.

Remarques :

Si vous possédez déjà un service DNS sur votre réseau interne (avec Active Directory), et souhaitez que les postes clients puissent accéder à Internet par le biais de WinGate, indiquez l'**IP interne** du serveur WinGate dans l'onglet **Forwarders** des propriétés du serveur DNS LAN. Ainsi, toutes les requêtes seront transférées par le serveur DNS LAN vers WinGate afin d'effectuer la résolution. ([Cliquez ici pour en savoir plus sur la configuration du service DNS avec Active Directory](#))

Si vous souhaitez que WinGate utilise un serveur spécifique, indiquez-le dans **Résolution DNS/Wins (*DNS/Wins Resolver*)**.

Un problème survient lors de l'utilisation du protocole SOCKS4 : les requêtes de connexion sont effectuées sous la forme de requêtes de numéro IP. Par conséquent, les clients SOCKS4 doivent pouvoir vérifier les adresses afin de fournir ce numéro IP au serveur SOCKS4. Ce problème a été résolu dans

SOCKS5.

Voir également :

[Désactiver le service DNS de WinGate](#)

[Options DNS](#)

©2004 Qbik New Zealand Limited

Options DNS

Le service DNS permet aux ordinateurs de votre réseau d'effectuer des "vérifications de nom". Vous avez pour cela plusieurs possibilités mais il est recommandé d'utiliser le service DNS de WinGate. Voici les avantages et inconvénients de chaque méthode :

Serveur DNS WinGate

Méthode par défaut, la plus simple et la plus efficace. Il reconnaît automatiquement le nom **wingate** et renvoie l'IP du serveur, ce qui évite d'ajouter des entrées dans les fichiers hosts. Cette méthode ne convient pas si vous souhaitez avoir une résolution externe pour votre site (c'est à dire si vous avez un nom de domaine). Vous devrez alors utiliser un serveur DNS autre que celui de WinGate.

Lien mappé

Méthode décrite dans [Ajouter un lien mappé](#). Un lien mappé UDP sur le port 53 permet de mapper toutes les requêtes DNS vers un serveur externe (généralement celui de votre FAI). Cela vous permet d'accéder au service sans devoir gérer un autre serveur. Cette méthode ne convient pas si vous souhaitez avoir une résolution externe pour votre site (c'est à dire si vous avez un nom de domaine). Vous devrez alors utiliser un serveur DNS autre que celui de WinGate. Cela ne permet pas d'effectuer de vérification pour le nom 'wingate', mais les clients peuvent utiliser des fichiers hosts pour y référer.

Autre serveur DNS

L'utilisation d'un serveur indépendant tel que Bind est nécessaire pour fournir les services DNS aux clients si vous possédez un nom de domaine pour votre serveur. Cette méthode ne permet pas d'effectuer de vérification pour le nom 'wingate', mais les clients peuvent utiliser des fichiers hôtes pour y référer.

Remarque :

Faire fonctionner le DNS sur les ordinateurs clients n'est pas une tâche aisée,

c'est pourquoi il est vivement recommandé d'utiliser les services **DNS** et **DHCP** de WinGate.

©2004 Qbik New Zealand Limited

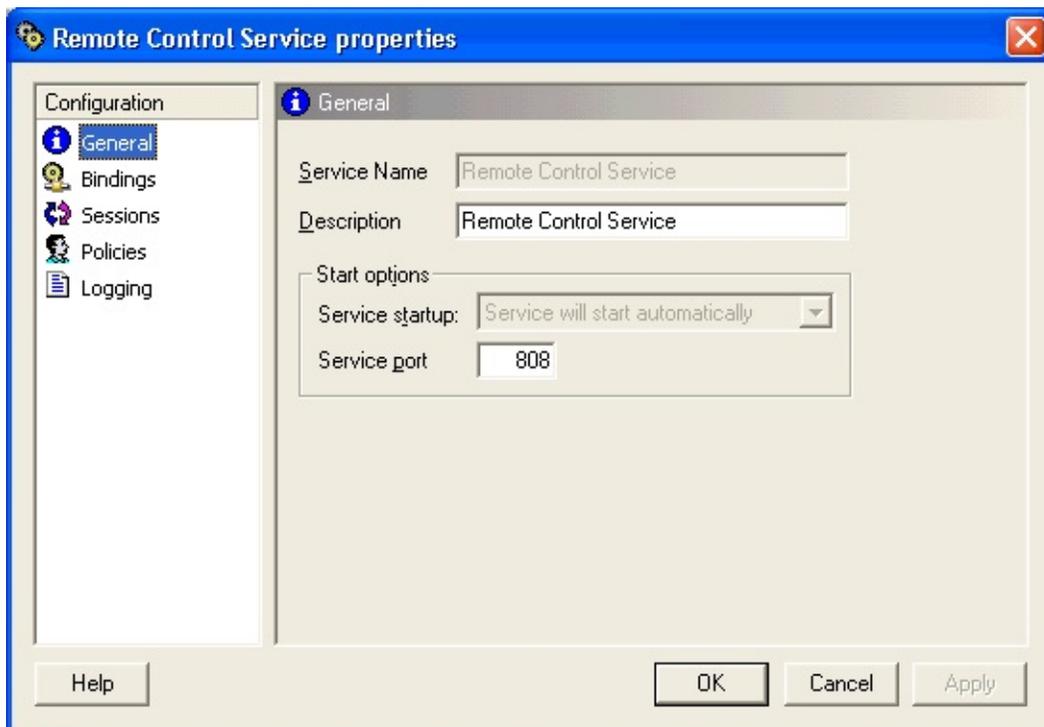
Service d'administration à distance

Le contrôle et la configuration de WinGate s'effectuent à l'aide d'un outil appelé **GateKeeper**.

GateKeeper communique avec WinGate par le biais d'un lien TCP/IP crypté. Cette interface permet de paramétrer WinGate, mais elle n'est pas nécessaire pour accéder à Internet.

Le service d'administration à distance permet d'accéder à GateKeeper depuis n'importe quel ordinateur de votre réseau (à condition de posséder au moins une licence Pro).

Par défaut, ce service est installé et actif. S'il vient à être supprimé ou corrompu, vous pouvez le réinstaller avec les paramètres par défaut.



Masquer | Masquer toutes les images

Il comporte différentes options qu'il n'est quasiment pas nécessaire de modifier.

Le service écoute par défaut le port **808**.

Il est utilisé par les clients souhaitant s'authentifier dans WinGate, y compris

GateKeeper, le client Java (par le biais d'un navigateur) ou toute application utilisant une DLL Qbik pour l'authentification.

Configuration d'une session d'administration à distance :

Par défaut, ce service n'est lié à aucune interface réseau.

Si un administrateur souhaite accéder à GateKeeper à distance, il doit **lier le service** à toutes les interfaces réseau internes.

Pour vous connecter à distance, vous devez exécuter le fichier GateKeeper.exe se trouvant sur le poste serveur de votre réseau (généralement dans le dossier Program Files / WinGate).

Masquer | Masquer toutes les images

Voir également :

[Accès distant à GateKeeper](#)

Veillez noter que ce service n'est disponible qu'avec WinGate Pro ou Enterprise, quelle que soit la version.

Serveur IMAP4

Le serveur IMAP4 est une nouveauté de la version 6.1 de WinGate.

Présentation du protocole IMAP4

Le protocole IMAP (Internet Message Access Protocol) est utilisé pour stocker et récupérer des messages sur un serveur de façon centralisée. Il permet aux clients d'accéder à leur courrier et de le gérer directement sur le serveur par le biais d'un client de messagerie ou d'une interface web.

Puisque le courrier est stocké sur le serveur les utilisateurs y accèdent où qu'ils soient et de n'importe quelle façon.

IMAP4 permet l'intégration des interfaces webmail et des clients de messagerie en local et à distance. Cela évite tout problème de synchronisation car les dossiers sont toujours sur le serveur.

Le serveur IMAP4 de WinGate représente une bonne alternative au serveur POP3, en particulier pour les utilisateurs mobiles.

Différences entre IMAP4 et POP3

Stockage du courrier

IMAP4 : le courrier est conservé de façon centralisé sur le serveur et donc toujours accessible.

POP3 : lorsqu'un client accède à son courrier sur le serveur POP3 le courrier est transféré du serveur vers le client.

Configuration

IMAP4 : lorsqu'un utilisateur crée des dossiers dans son client de messagerie (par ex. :Outlook express, Eudora) ces dossiers sont répliqués sur le serveur.

POP3 : les dossiers créés sont conservés au niveau du client de messagerie mais pas sur le serveur.

Recherche de messages

IMAP4 : les recherches sont effectuées sur le serveur.

POP3 : le courrier étant téléchargé sur le poste client, les recherches sont effectuées par le client.

Accessibilité

IMAP4 : tout le courrier est stocké dans un seul endroit (le serveur IMAP4), les utilisateurs peuvent accéder à leurs dossiers où qu'ils soient sans devoir effectuer de synchronisation.

POP3 : tous les paramètres sont conservés au niveau du client de messagerie.

[Cliquez ici pour savoir comment configurer le serveur IMAP4 de WinGate](#)

Serveur IMAP4

Sa configuration est assez simple, mais nous attirons votre attention sur les points suivants :

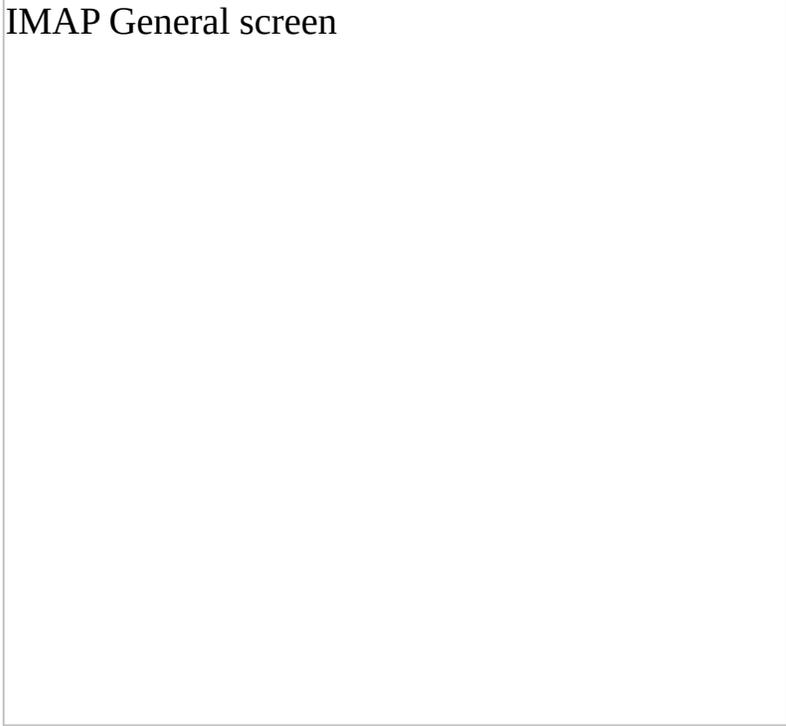
1. Le serveur IMAP4 étant une alternative au serveur POP3 de WinGate, les utilisateurs peuvent posséder soit une boîte POP3 soit une boîte IMAP4 mais pas les deux.
2. L'option de débogage occupant rapidement l'espace disque, ne l'activez qu'avec précaution et uniquement en cas de nécessité absolue.

Configuration du serveur IMAP4

1. Activation du serveur

1. Ouvrez **GateKeeper**.
2. Sélectionnez **Serveur IMAP (*IMAP server*)** dans l'onglet **Système**.
3. Cliquez sur l'icône **Général**.

IMAP General screen



Masquer

4. Dans le menu déroulant **Démarrage (Service Startup)** sélectionnez **Automatique (Service will start automatically)**.
5. Cliquez sur **OK**

Remarque :

Le serveur IMAP4 fonctionne sur le port 143 (TCP) et démarre automatiquement par défaut.

2. Configuration des boîtes IMAP pour les utilisateurs WinGate :

1. Ouvrez **GateKeeper**.
2. Cliquez sur l'onglet **Utilisateurs (Users)**.
3. Cliquez avec le bouton droit de la souris sur le nom de l'utilisateur souhaité, et sélectionnez **Propriétés**

(Properties).



Masquer

4. Dans la fenêtre qui s'ouvre ensuite, cliquez sur l'onglet **E-mail**.



Masquer

5. Sélectionnez **IMAP4** dans le menu déroulant.
6. Cliquez sur **OK**.

Cet utilisateur possède à présent une boîte sur le serveur IMAP4, dans le répertoire **WinGate\Mail\IMAP**"Nomd'utilisateur".

Il suffit alors de configurer les applications clientes pour qu'elles se connectent au serveur IMAP de WinGate.

Remarque :

En règle générale, il n'est pas nécessaire de modifier les paramètres de messagerie car ils s'appliquent essentiellement aux services POP3 et SMTP.

©2005 Qbik New Zealand Limited

Serveur de messagerie de WinGate - Introduction

Le serveur de messagerie de WinGate offre les fonctions POP3 et SMTP.

Ses avantages sont nombreux :

Modules d'analyse des données (ex.: AntiVirus, GateFilter).

Messages acheminés à la vitesse du réseau local (LAN).

Intégration avec la base de données d'utilisateurs WinGate et le composeur WinGate.

Hébergement de plusieurs domaines de messagerie.

Options du serveur de messagerie de WinGate

Le serveur de messagerie de WinGate s'adapte à vos besoins.

Ses possibilités de configuration sont variées :

serveur de messagerie principal

serveur de messagerie supplémentaire sur le réseau local

serveur de messagerie externe pour l'envoi et la réception du courrier

association avec un fournisseur d'accès à Internet (FAI) pour la réception du courrier

etc.

[\(Cliquez ici pour connaître les possibilités de configuration du serveur de messagerie\)](#)

[\(Cliquez ici pour connaître le fonctionnement du serveur de messagerie de WinGate\).](#)

Remarque :

La fonction de messagerie est seulement disponible dans les versions 5.0 et ultérieures de WinGate.

©2004 Qbik New Zealand Limited

E-mail - Options de configuration

Le service E-mail de WinGate peut être configuré pour fonctionner sous diverses formes :

1. Vous utilisez WinGate en tant que serveur de messagerie

Sans héberger de domaine

Il suffit d'installer WinGate pour que cette fonctionnalité soit immédiatement disponible et que les clients utilisent son serveur en tant que serveur SMTP et POP.

Avec un nom de domaine

Cette méthode fonctionne par défaut. Vous devez simplement ajouter les noms de domaines, et configurer vos enregistrements MX pour qu'ils indiquent l'adresse IP externe de l'ordinateur où se trouve WinGate. Si vos informations DNS se trouvent sur votre FAI, vous devrez le contacter pour qu'il les modifie.

2. WinGate sert de passerelle pour un serveur interne

C'est à dire : vous possédez un serveur de messagerie sur l'un des ordinateurs de votre réseau et souhaitez utiliser WinGate en tant que pare-feu et protection antivirus.

Exemple :

Adresses IP de WinGate : 202.10.10.2 (externe) et 192.168.0.1 (LAN)

Adresse du serveur de messagerie : 192.168.0.10

Le courrier circule de la façon suivante :

Internet <-> WinGate <-> Serveur de messagerie <-> Clients

1. Configurez le service E-mail de WinGate afin que le serveur de

courrier local/entrant soit dirigé vers 192.168.0.10

2. Ajoutez les domaines considérés comme locaux.
3. Configurez votre serveur de messagerie afin qu'il utilise l'IP interne de WinGate (192.168.0.1) en tant que passerelle.

Ainsi, votre serveur interne transfère tout le courrier non local vers WinGate.

3. Vous utilisez votre FAI en tant que passerelle

Avec chacune des options ci-dessus, vous avez la possibilité d'utiliser le serveur de votre FAI en tant que passerelle pour le courrier sortant. Cela peut s'avérer utile si votre connexion Internet est lente, car il est plus rapide de transférer le courrier à votre FAI qu'à chaque domaine destinataire. Remarque : Vous devez auparavant obtenir l'autorisation de votre FAI.

Pour appliquer cette méthode, il suffit de choisir **Utiliser une passerelle (Use gateway)** dans les options de distribution et d'indiquer l'adresse IP du serveur de votre FAI.

Le courrier circule de la façon suivante :

Entrant : Internet -> WinGate -> clients

Sortant : Internet < - FAI < - WinGate < - clients

4. Vous n'utilisez WinGate que pour l'envoi de courrier

Si vous possédez des comptes POP sur votre FAI, vous pouvez tout de même envoyer du courrier par le biais de WinGate (fonctionnalité disponible par défaut). WinGate analyse tout le courrier provenant du FAI, même si ces comptes ne sont pas hébergés dans WinGate.

Entrant : Internet - > FAI - > clients

Sortant : Internet < - WinGate < - clients

Dans ce cas, il est également possible d'utiliser votre FAI pour l'envoi de courrier, en le désignant comme passerelle.

Entrant : Internet - > FAI -> clients

Sortant : Internet < - FAI < - WinGate < - clients

©2004 Qbik New Zealand Limited

Fichiers de messages et répertoires de WinGate

WinGate utilise une structure de répertoires simple pour stocker le courrier. Toutes les informations sont enregistrées dans des fichiers pour éviter de perdre des messages. Ce système est avantageux pour l'administrateur car il lui permet d'ajuster ses paramètres au fur et à mesure que le courrier est traité. Les fichiers de messages (.msg) sont conformes à la norme RFC822, et les fichiers de routage (.rcp) utilisent un format lisible par l'utilisateur.

Exemples :

1. Un document important a été envoyé par accident à un mauvais destinataire à l'extérieur de l'entreprise :

Solution - l'administrateur peut rechercher le message dans le répertoire "**Incoming**" et le supprimer. S'il a déjà été mis en file d'attente pour être envoyé au domaine, il peut le supprimer dans le répertoire " **Holding**".

2. Un document important a été envoyé par accident à un mauvais destinataire au sein de l'entreprise :

Solution - l'administrateur peut ouvrir le répertoire "**POP3**" du premier utilisateur, rechercher le fichier et le déplacer dans le répertoire de l'utilisateur voulu.

Pour annuler l'envoi des messages en cours à un domaine :

1. Ouvrez le répertoire **Spool\Domains**.
2. Recherchez le répertoire requis (tout le courrier du domaine "hotmail.com" sera enregistré dans le répertoire "hotmail.com"), supprimez-le ou faites-le glisser dans le répertoire "**Dead**".

Types de fichiers

Il s'agit de fichiers texte que vous pouvez ouvrir et lire à l'aide de n'importe

quelle visionneuse.

fichiers .msg

Messages au format RFC822.

fichiers .rcp

Ces fichiers contiennent des informations sur le destinataire d'un message mais aussi sur la personne qui l'a envoyé.

fichiers .mri

Ces fichiers sont créés pour chaque répertoire de domaine et contiennent des informations telles que la date du premier test d'un domaine, celle du test suivant et le nombre de fois où WinGate a tenté d'envoyer du courrier pour ce domaine.

Répertoires du système de messagerie de WinGate

POP3

Les e-mails des utilisateurs locaux sont enregistrés dans les sous-dossiers de ce répertoire. Par exemple, le courrier de Jean est enregistré dans WinGate\Mail\POP3\Jean. Tous les messages correspondent à des fichiers texte enregistrés au format RFC822.

Spool\Incoming

Ce répertoire accueille les e-mails et les fichiers .rcp lorsqu'ils sont reçus par le service SMTP.

Spool\PostIn

Ce répertoire accueille les e-mails et les fichiers .rcp lorsqu'ils sont acceptés par le préprocesseur. Les fonctionnalités du préprocesseur incluent une analyse des données (recherche de virus ou de matériel inadapté) ainsi qu'une protection contre les boucles de courrier.

Spool\Holding

Les messages sont stockés dans ce répertoire jusqu'à leur distribution.

Remarque : le contenu d'un fichier de messages peut être distribué à plusieurs destinataires issus de domaines différents. Par conséquent, il est préférable de n'enregistrer qu'une seule version du fichier. En supprimant un fichier .msg, vous empêchez la distribution des messages au reste des destinataires prévus.

Spool\Domains\"nomdedomaine"

Ce répertoire est associé à chaque domaine pour lequel des messages sont en attente d'envoi ; il contient un fichier .rcp pour chacun des messages. Si trois messages doivent être envoyés à hotmail.com, le répertoire domains\hotmail.com\ est créé : il inclut trois fichiers .rcp comprenant la liste des destinataires de chaque message (fichier .msg). Un fichier domain.mri est également créé pour recueillir les informations de distribution. S'il est supprimé, le programme d'envoi redémarre (comme si les e-mails venaient d'être envoyés). La suppression d'un fichier .rcp dans un répertoire de domaine empêche la distribution du message aux utilisateurs de ce domaine.

Spool\Sent

Lorsque vous activez l'option d'enregistrement d'une copie des e-mails envoyés, les fichiers .msg sont déplacés dans ce répertoire au lieu d'être supprimés. Cette fonction est pratique si vous rencontrez des problèmes de distribution de courrier. Remarque : la taille du répertoire n'est pas limitée mais l'administrateur doit vérifier que le volume de stockage reste gérable par l'ordinateur.

Spool\Domains\Dead

Ce répertoire regroupe l'ensemble des fichiers qui rentrent dans l'une des catégories suivantes :

Fichiers orphelins :

Si un serveur distant plante ou que votre connexion Internet échoue pendant la

réception du courrier, vous obtenez des fichiers orphelins. On dit également d'un fichier qu'il est orphelin si l'administrateur supprime une partie des éléments constitutifs d'un message. Exemple : si un fichier .rcp n'est pas associé à un fichier .msg, etc.

Fichiers avec erreur :

Si un plantage système se produit lors de l'écriture d'un fichier, une erreur est signalée. Le fichier devient alors incomplet et WinGate ne peut pas distribuer le message.

Autres :

Si le système de messagerie ne peut pas affirmer qu'un e-mail a correctement été envoyé, ce dernier est enregistré dans le répertoire "**Dead**".

La taille de ce répertoire n'est pas limitée (cependant, il ne doit pas être trop volumineux).

Protection contre les boucles de courrier

Le service de messagerie de WinGate assure une protection contre les boucles de courrier.

Une boucle de courrier se produit lorsqu'un message est transféré plusieurs fois par des serveurs de messagerie sans jamais atteindre sa destination finale. WinGate empêche ce problème en limitant la taille totale des en-têtes de messages (ex.: sujet, date, etc.)

Ce système fonctionne de la façon suivante : chaque fois qu'un serveur de messagerie reçoit un e-mail, il ajoute un en-tête "Received" dans lequel sont indiqués la date, l'heure et d'autres informations. S'il reçoit un nombre d'en-têtes trop important, il en déduit qu'une boucle est en cours d'exécution. WinGate déplace le message dans le répertoire "**Dead**" lorsque la taille maximale autorisée est atteinte. Par défaut, cette taille est définie à 8 Ko.

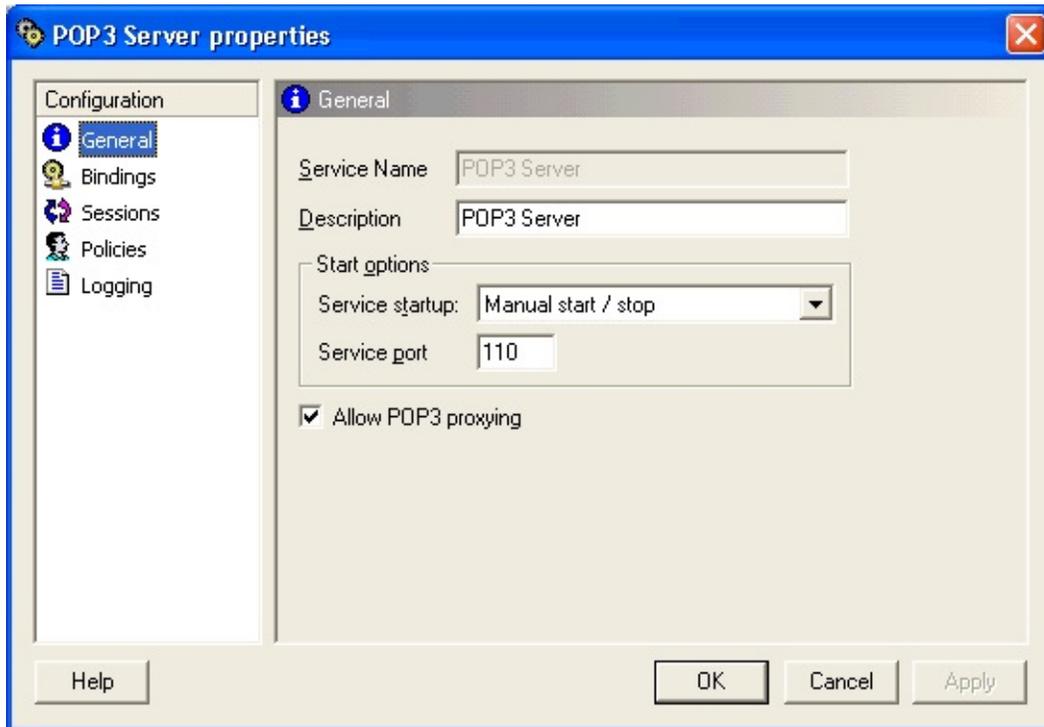
Vous pouvez l'ajuster en modifiant cette valeur dans le registre de WinGate :
WinGate\Settings\Mail REGDWORD:MaxMessageHeaderSize

Pour garantir le traitement des e-mails normaux, WinGate refuse les valeurs inférieures à 2048 octets.

©2004 Qbik New Zealand Limited

Serveur POP3

Depuis la version 5.0, WinGate propose un serveur **Serveur POP3**, accessible dans l'onglet **Système** de GateKeeper.



Masquer

Sa configuration est très simple, mais il convient de noter quelques points :

Le serveur POP3 ne doit être lié à une interface externe que si des clients extérieurs au réseau reçoivent leur courrier sur le serveur de messagerie de WinGate. Par défaut, il est lié à une interface interne, car le serveur de messagerie est généralement utilisé sur le réseau local.

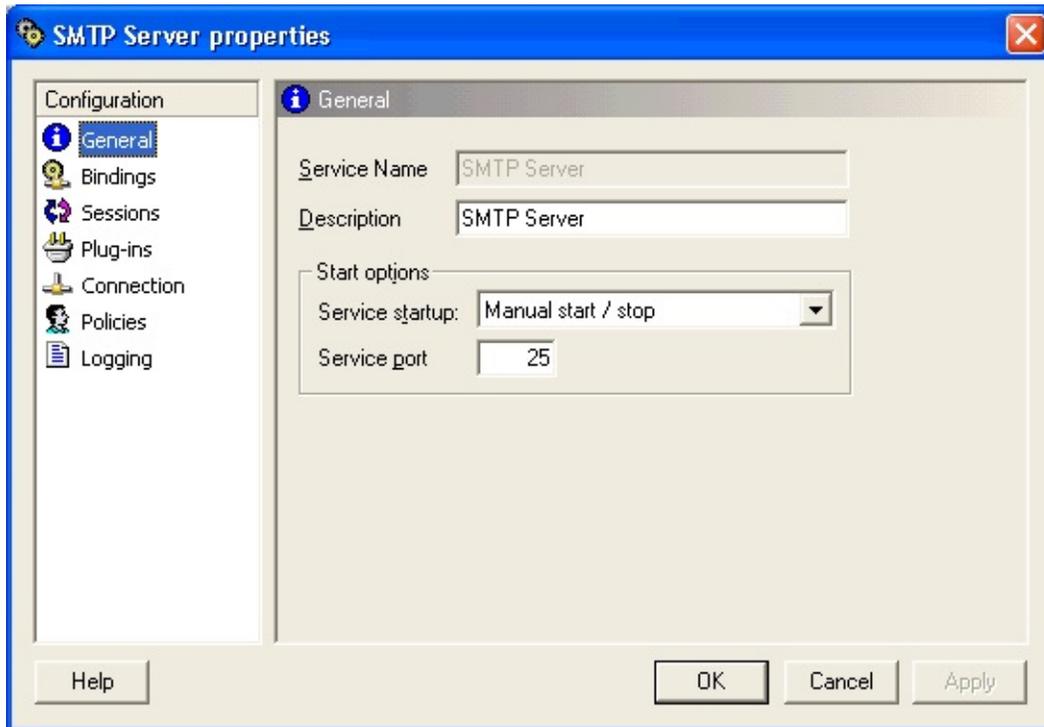
Si l'option **Transmettre au proxy POP3 (Hand over to POP3 Proxy)** est cochée, les clients pourront accéder au [Service proxy POP3](#).

Le serveur POP3 écoute par défaut le port **110** et fonctionne en association avec le service proxy POP3 (mentionné ci-dessus) qui utilise le port **8110**.

©2005 Qbik New Zealand Limited

Serveur SMTP

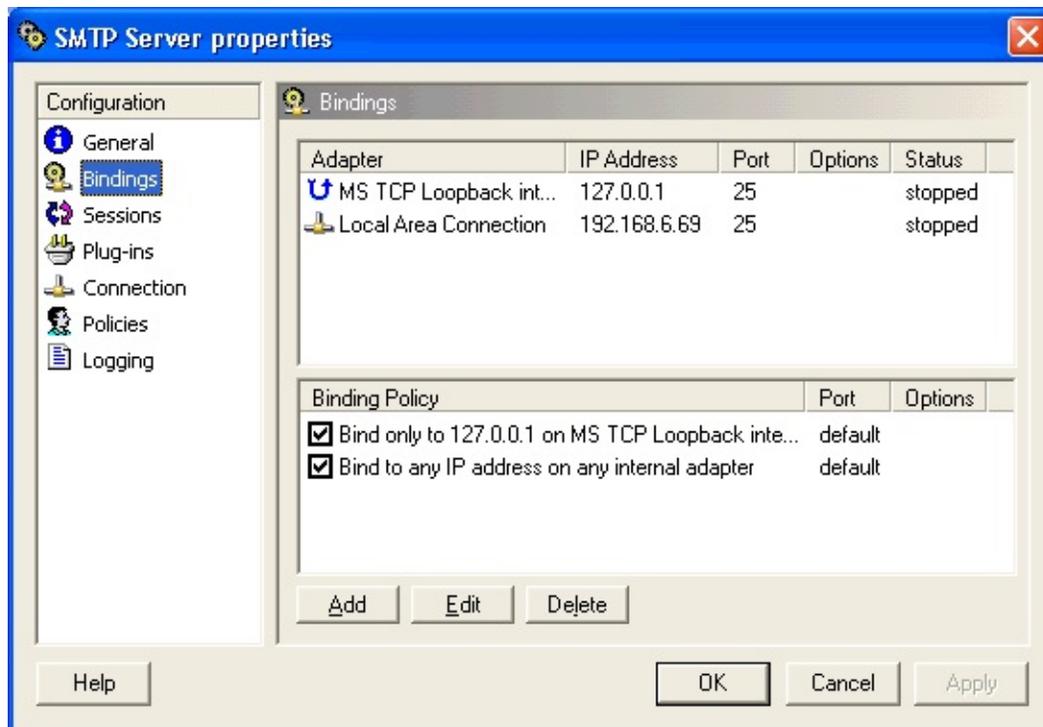
Le **Serveur SMTP** fournit le protocole SMTP au serveur de messagerie de WinGate.



Masquer | **Masquer toutes les images**

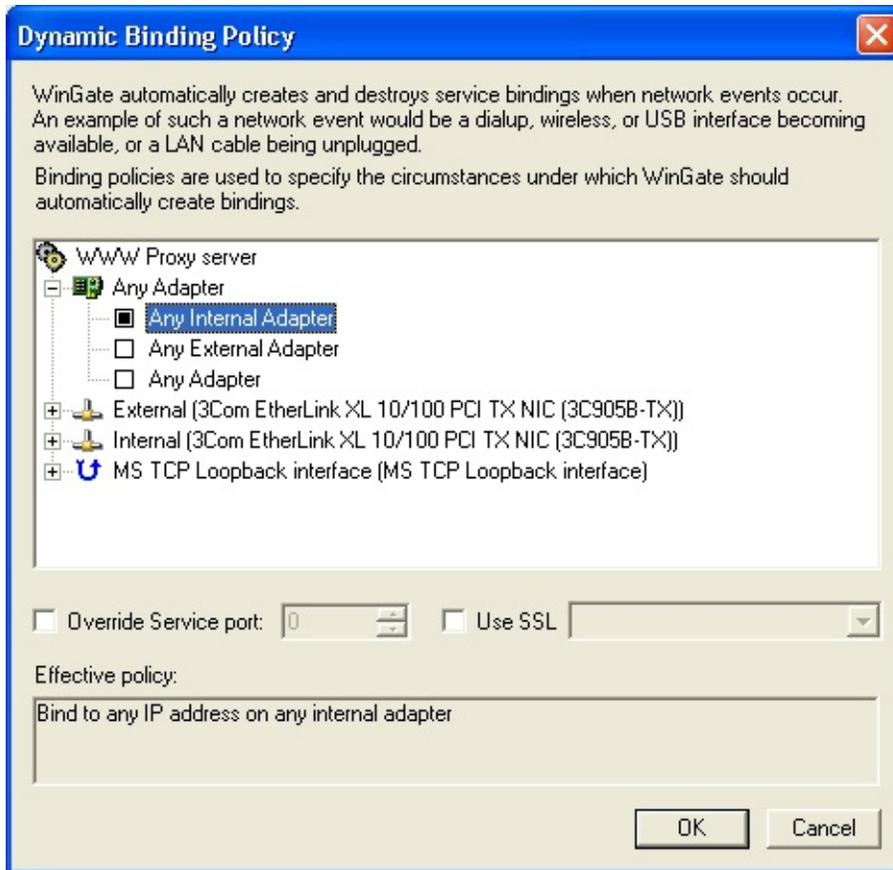
Liaisons (*Bindings*)

Ce serveur doit être lié à une interface interne, afin de pouvoir transférer le courrier des utilisateurs sur le réseau local. Cette option est correctement paramétrée par défaut, mais vous pouvez la modifier en cliquant sur **Liaisons** dans les propriétés du serveur SMTP.



Masquer | Masquer toutes les images

Si vous possédez une licence WinGate Enterprise, vous pouvez utiliser des **Liaisons SSL**.



Masquer | Masquer toutes les images

Modules (*Plug-ins*)

Si des modules d'analyse sont installés, vous pouvez les activer en cliquant sur l'icône **Modules (Plug-ins)**.



Masquer | Masquer toutes les images

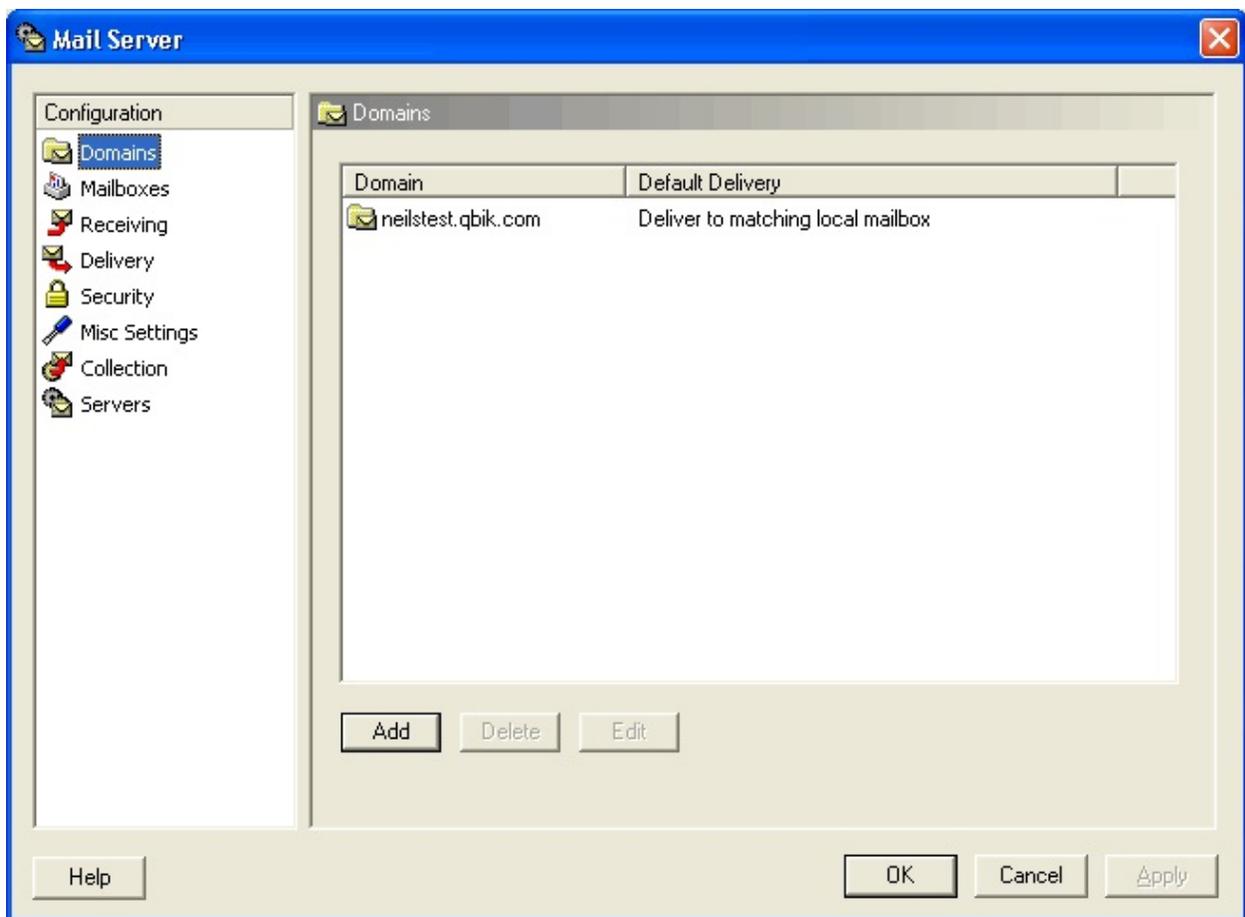
©2005 Qbik New Zealand Limited

E-mail - Domaines

Cette option vous permet de configurer les domaines de votre choix.

Le service E-mail de WinGate est très flexible, c'est pourquoi il est important de comprendre certains concepts clés.

En règle générale, vous serez amené à utiliser cette fonctionnalité si vous souhaitez qu'un domaine soit traité de façon spécifique (accepter le courrier pour les boîtes locales, rediriger vers un autre serveur, appliquer des restrictions supplémentaires ...).



Masquer

Champs :

Domaine (Domain)

Nom du domaine pour lequel WinGate doit effectuer des tâches particulières.

Distribution par défaut (*Default delivery*)

Méthode de distribution par défaut pour le traitement du courrier de ce domaine.

Remarque :

Ce paramètre peut également être appliqué par adresse, auquel cas il est prioritaire.

Boutons :

Ajouter (*Add*)

Cliquez ici pour configurer les paramètres du domaine.

Modifier (*Edit*)

Permet de modifier les données concernant un domaine spécifique.

Supprimer (*Delete*)

Cliquez sur ce bouton pour supprimer un domaine.

Remarques :

Le "domaine" est la partie d'une adresse électronique qui suit le caractère '@'. Par exemple, le domaine de l'adresse "bob@marybob.com" est "marybob.com".

En général la configuration d'un domaine a pour but de permettre la réception du courrier qui lui est destiné et de le distribuer aux boîtes à lettres locales de vos utilisateurs.

Mais cela permet également de :

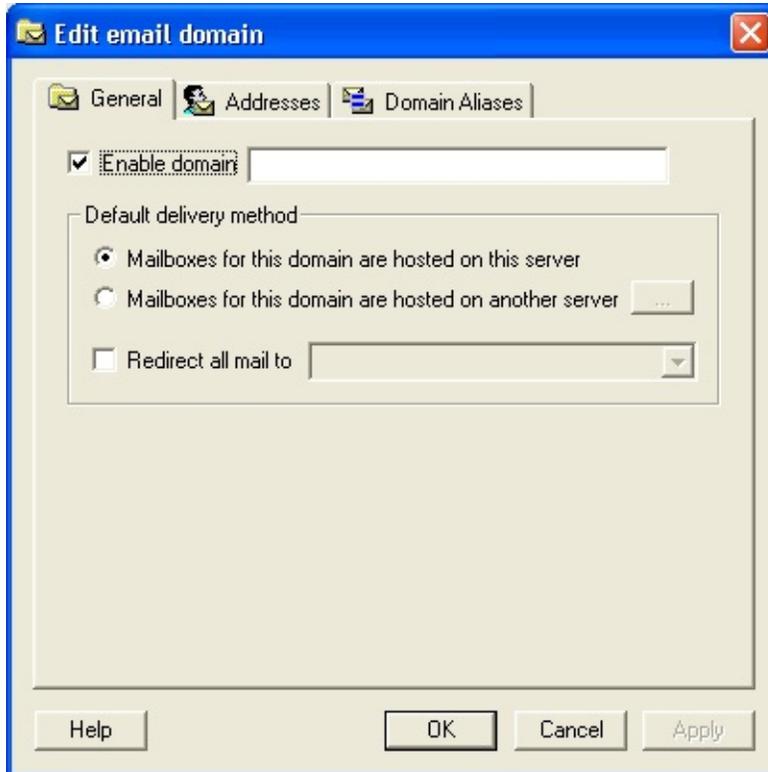
1. Effectuer des tâches particulières pour une adresse spécifique (changer de destinataire, limiter la taille des messages, envoyer une copie des messages reçus à une autre adresse ...). Le service mail étant basé sur les domaines, il est impossible d'assigner une configuration particulière à une adresse sans en paramétrer le domaine. Le courrier peut être reçu directement avec le protocole SMTP, ou bien collecté par le biais du POP3.
2. Autoriser pour certains utilisateurs la réception du courrier provenant de destinataires non vérifiés, même si leur courrier n'est pas hébergé localement.

3. Rediriger tout le courrier sortant destiné à un domaine spécifique.
4. Envoyer tout le courrier reçu pour un domaine dans une seule boîte, ou envoyer la totalité du courrier dans une seule boîte, à l'exception de certaines adresses.

©2004 Qbik New Zealand Limited

Domaines - Onglet Général

Configurez dans **cet onglet** la méthode de distribution par défaut pour ce domaine.



Masquer

Activer le domaine (*Enable Domain*)

Indiquez le nom du domaine pour lequel vous souhaitez que WinGate effectue des tâches spécifiques.

Méthode de distribution par défaut

Cette méthode permet de configurer la distribution du courrier de façon simple et pratique.

WinGate distribue automatiquement tout le courrier d'un domaine dans la boîte locale correspondante. Il n'est pas nécessaire de configurer les adresses e-mail pour chaque adresse acceptée dans votre domaine.

Par exemple, si un utilisateur s'appelle 'info', le courrier adressé à info@qbik.com sera distribué par défaut dans sa boîte.

Si ce compte est désactivé, ou si sa boîte à lettres n'est pas paramétrée, le courrier adressé à info@qbik.com sera rejeté.

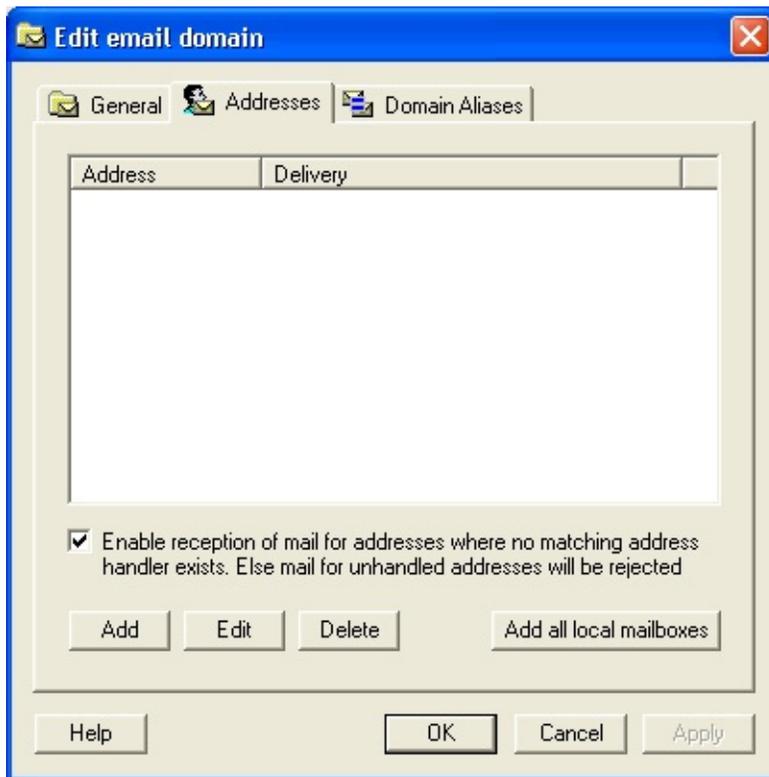
Vous avez également la possibilité de transférer sur un autre compte tout le courrier destiné à info@qbik.com en créant une configuration d'adresse spécifique. Ainsi, il n'est pas nécessaire d'avoir un utilisateur ou une boîte appelés 'info'.

Rediriger tout le courrier vers (*Redirect all mail to*)

Lorsque cette option est cochée, vous pouvez sélectionner dans le menu déroulant une adresse à laquelle tout le courrier du domaine sera transféré.

Domaines - Onglet Adresses

Configurez **dans cet onglet** la liste des adresses et listes de diffusion du domaine.



Masquer | Masquer toutes les images

En cliquant sur **Ajouter (Add)** vous choisissez d'ajouter soit une adresse, soit une liste de diffusion.



Masquer | Masquer toutes les images

Si vous sélectionnez **Ajouter une adresse (Add address)** une fenêtre s'ouvre vous permettant de [paramétrer les adresses](#).

Si vous sélectionnez **Ajouter une liste de diffusion (Add address list)** une fenêtre s'ouvre vous permettant de [paramétrer les listes de diffusion](#).

Cliquez sur **Ajouter toutes les boîtes locales** (*Add all local mailboxes*) pour ajouter directement toutes les boîtes créées par des utilisateurs de WinGate.

Autoriser la réception du courrier pour les adresses ne possédant pas de configuration spécifique (*Enable reception of mail for addresses where no matching address handler exists*)

Cette option influe sur la **Méthode de distribution par défaut** (*Default delivery method*) (définie dans l'onglet **Général**).



Masquer | **Masquer toutes les images**

Si cette option est cochée et que la méthode par défaut est : **Les boîtes à lettres du domaine sont hébergées sur ce serveur** (*Mailboxes for this domain are hosted on this server*), tout le courrier sera distribué aux boîtes correspondantes. Si vous créez des configurations d'adresses, elles seront prioritaires pour chaque adresse concernée.

Si cette option n'est pas cochée, seul le courrier destiné à des adresses possédant une configuration sera accepté.

Associée à **Ajouter toutes les boîtes locales** (*Add all local mailboxes*), cette option permet donc de définir rapidement les adresses qui seront acceptées.

Si la méthode par défaut est : **Les boîtes à lettres du domaine sont hébergées sur un autre serveur (*Mailboxes for this domain are hosted on another server*)**, alors la distribution du courrier dépend des conditions suivantes :

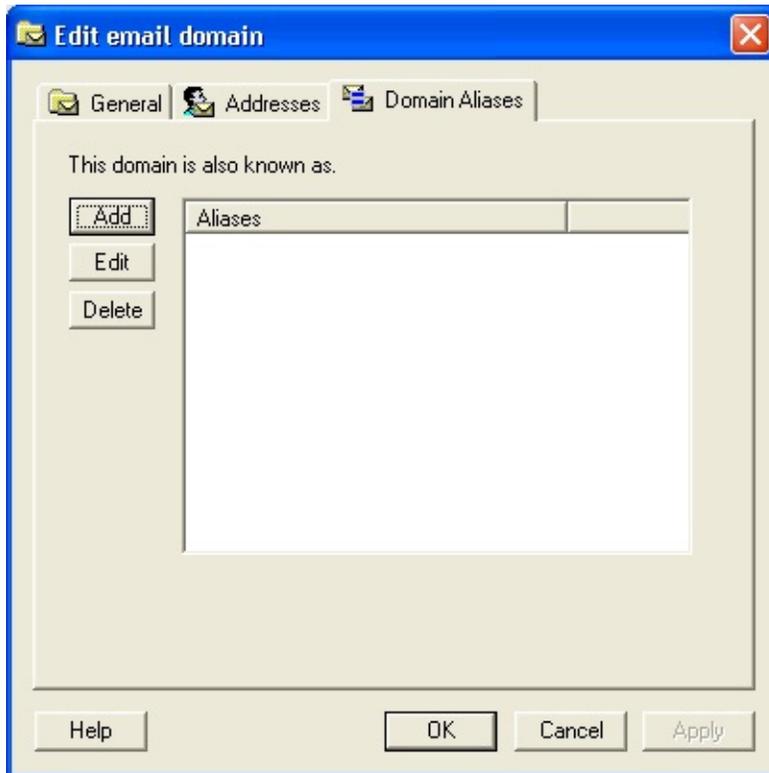
Si l'option est cochée, WinGate ne vérifie pas les adresses et transfère tout le courrier du domaine au serveur distant.

Si l'option n'est pas cochée, WinGate n'accepte que le courrier destiné à des adresses possédant une configuration. Ce courrier est alors transféré au serveur distant, sauf indication contraire des configurations d'adresses.

Ainsi, WinGate peut bloquer tout le courrier destiné à une adresse non existante d'un domaine, même si ce domaine se trouve sur un serveur distant.

Domaines - Onglet Alias de domaine (*Domain Aliases*)

Cet onglet permet de créer et de modifier une liste d'alias pour ce domaine.



Masquer

Le principe des alias peut s'avérer utile pour grouper le courrier de plusieurs domaines. Si vous possédez plusieurs domaines sur votre serveur, mais que vous n'avez qu'un ensemble d'utilisateurs, ayant chacun une adresse électronique dans des domaines différents, les alias facilitent la procédure. En effet, il n'est pas nécessaire de créer des configurations spécifiques à chaque domaine.

Par exemple : les adresses du domaine Qbik.com ont des équivalents dans d'autres domaines. L'adresse info@qbik.com possède la même configuration que info@wingate.com et info@netpatrol.com.

©2005 Qbik New Zealand Limited

E-mail - Configuration d'adresse - Onglet Général (*Address handler - General*)

Dans WinGate, une "configuration d'adresse" est le nom donné à une configuration indiquant la façon de traiter une adresse spécifique. Vous avez ainsi la possibilité de spécifier divers paramètres pour chaque adresse.

Pour **configurer ces paramètres**, cliquez sur **Ajouter (Add)** dans l'onglet **Adresses (Addresses)** des **propriétés du domaine**.

Vous pouvez ainsi : rediriger le courrier adressé à un utilisateur vers un autre emplacement (local ou distant), envoyer une copie des messages reçus à une autre adresse (ou liste d'adresses), limiter la réception des messages en fonction de leur taille ou bloquer toutes les pièces jointes.



Masquer

Activer la configuration d'adresse (*Address handler enabled*)

Cochez cette option pour appliquer une configuration particulière à cette adresse.

Remarque :

En fonction de la méthode de distribution par défaut choisie, le fait de désactiver cette option risque de bloquer la réception de tous les messages destinés à cette adresse. Voir les remarques ci-dessous pour plus d'informations.

Adresse

Nom de l'adresse. Il s'agit de la partie de l'adresse électronique qui précède le caractère '@'. Cela permet d'utiliser des alias de domaines (voir remarques).

Outrepasser les paramètres de distribution du domaine (*Override domain delivery settings*)

Cochez cette option pour annuler les paramètres par défaut du domaine, définis dans **Distribution (Delivery)**. Deux options supplémentaires sont alors disponibles :

Distribuer le courrier dans une boîte locale (*Deliver mail to local mailbox*)

Le courrier de cet utilisateur est distribué dans une boîte du réseau local.

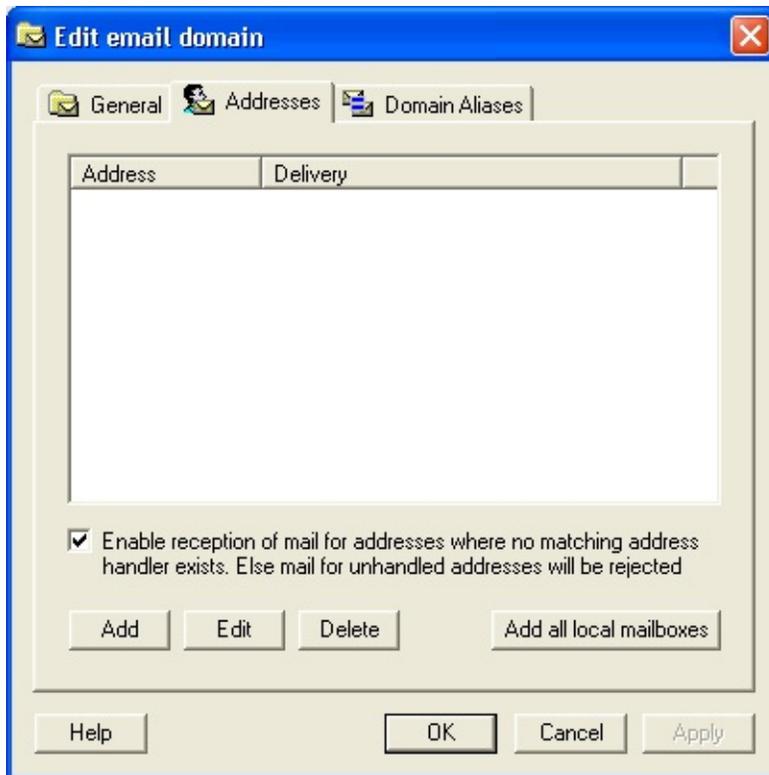
Distribuer le courrier sur un autre serveur (*Deliver mail to another mail server*)

Le courrier adressé à cet utilisateur est distribué dans une boîte se trouvant sur un serveur distant. Lorsque cette option est cochée, vous pouvez cliquer sur le bouton permettant d'ouvrir la fenêtre **Options de distribution à distance (*Remote delivery options*)**. Le courrier est alors distribué sur un serveur spécifique ou bien WinGate effectue une résolution MX pour en trouver un.

Cliquez sur (...) pour définir [la configuration du serveur choisi](#).

Remarques :

Dans l'onglet **Adresses** du domaine se trouve une option appelée **Autoriser la réception du courrier pour les adresses ne possédant pas de configuration spécifique (*Enable reception of mail for addresses where no matching address handler exists*)**.



Masquer

Si elle est cochée, tout le courrier est accepté mais les configurations d'adresses de la liste sont prioritaires.

Si elle n'est pas cochée, seules les adresses possédant une configuration seront acceptées. Dans ce cas, si vous désactivez une configuration, le courrier destiné à l'adresse correspondante sera refusé.

Avec WinGate, il est possible d'utiliser des alias pour un domaine, ainsi une seule configuration peut entraîner la création de plusieurs adresses (une pour chaque alias de domaine).

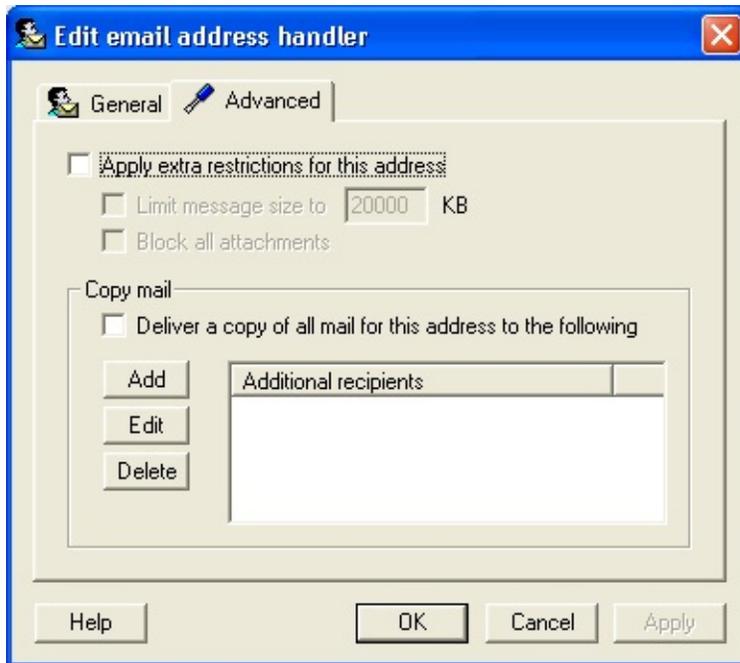
Par exemple : si vous définissez un domaine appelé qbik.com, et créez une configuration d'adresse appelée info, cela équivaut à créer l'adresse info@qbik.com. Puis si vous ajoutez ensuite un alias au domaine qbik.com (par exemple test.com) cela crée un autre adresse : info@test.com.

Si vous choisissez de distribuer le courrier sur un autre serveur, cliquez sur le bouton situé à la droite de cette option afin de définir les paramètres pour le serveur choisi.

©2004 Qbik New Zealand Limited

E-mail - Configuration d'adresse - Onglet avancé (*Address handler - Advanced*)

Dans **cet onglet**, vous pouvez créer des restrictions en fonction de la taille des messages et bloquer les pièces jointes adressées à l'utilisateur.



Masquer

Options

Appliquer des restrictions supplémentaires pour cette adresse (*Apply extra restrictions for this address*)

Cochez cette case pour activer les restrictions ci-dessous.

Limiter la taille des messages à X Ko (*Limit message size to X Kb*)

Cette limite s'applique par message et par utilisateur.

Bloquer toutes les pièces jointes (*Block all attachments*)

Bloque tous les messages contenant des pièces jointes destinés à cet utilisateur.

Copier

Envoyer une copie de tout le courrier adressé à cet utilisateur à (*Deliver a copy of all mail for this address to the following*)

Cochez cette option si vous souhaitez qu'une copie de chaque message envoyé à l'utilisateur soit également envoyée à une adresse spécifique (souvent celle de l'administrateur).

©2004 Qbik New Zealand Limited

Configuration des listes de diffusion - Onglet Général

Avec WinGate 6.1, vous avez la possibilité de créer des **listes de diffusion** pour chaque domaine.

Masquer

Création d'une liste de diffusion :

1. Saisissez l'adresse de la liste dans le champ **Adresse (Address)**.
2. Indiquez dans le champ **Nom (List Name)** l'intitulé de votre choix.
3. Indiquez l'adresse à laquelle doivent être envoyées les erreurs dans le champ **Notif. erreurs (Errors to:)**.
4. Puis, cliquez sur l'onglet **Membres (Members)** pour y ajouter des utilisateurs.

Options

Autor. envoi (Who can post:)

Sélectionnez dans la liste déroulante les personnes autorisées à envoyer des messages sur la liste :

1. Membres uniquement (*Members only*)
2. Administrateur (*List owner*)
3. Tout le monde (*Anyone*)

Réponses (*Replies go*)

Sélectionnez dans la liste déroulante quels utilisateurs recevront les réponses aux messages de la liste :

1. À la liste (*Back to the list*)

Les réponses seront envoyées à tous les membres de la liste.

2. À l'expéditeur (*Back to the sender*)

Si un utilisateur répond à un message de la liste, la réponse ne sera envoyée qu'à l'expéditeur de ce message.

3. À l'administrateur (*Back to the list owner*)

Les réponses aux messages seront envoyées à l'administrateur de la liste.

Configuration des listes de diffusion - Onglet Membres (*Members*)

Cet onglet permet d'ajouter des membres à la liste de diffusion.

Masquer | **Masquer toutes les images**

Pour cela, il suffit de cliquer sur **Ajouter**, puis d'indiquer une adresse e-mail ou simplement un nom d'utilisateur si celui-ci possède une boîte sur le serveur.

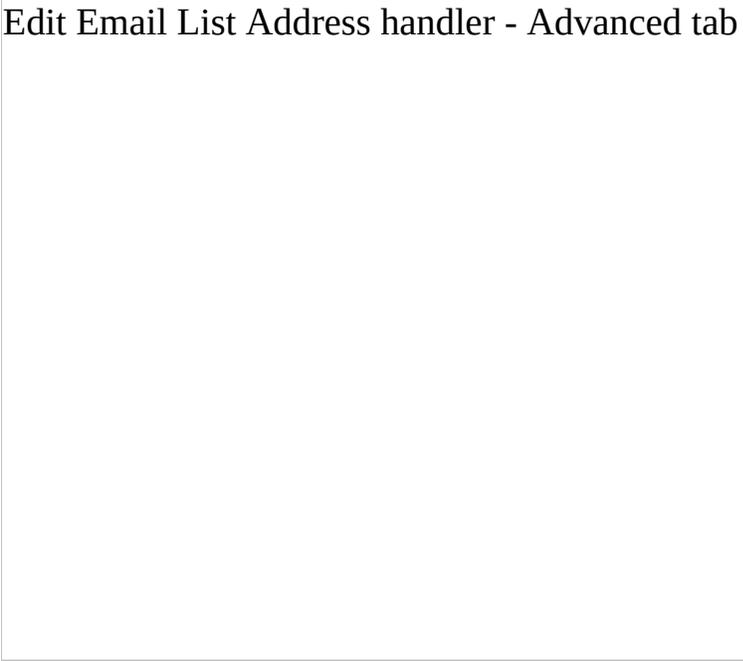
Masquer | **Masquer toutes les images**

Vous pouvez autoriser les membres à envoyer et/ou à recevoir des messages.

Configuration des listes de diffusion - Onglet Avancé

Cet onglet permet d'appliquer des restrictions supplémentaires.

Edit Email List Address handler - Advanced tab



Masquer

Limiter la taille des messages à (*Limit message size to*)

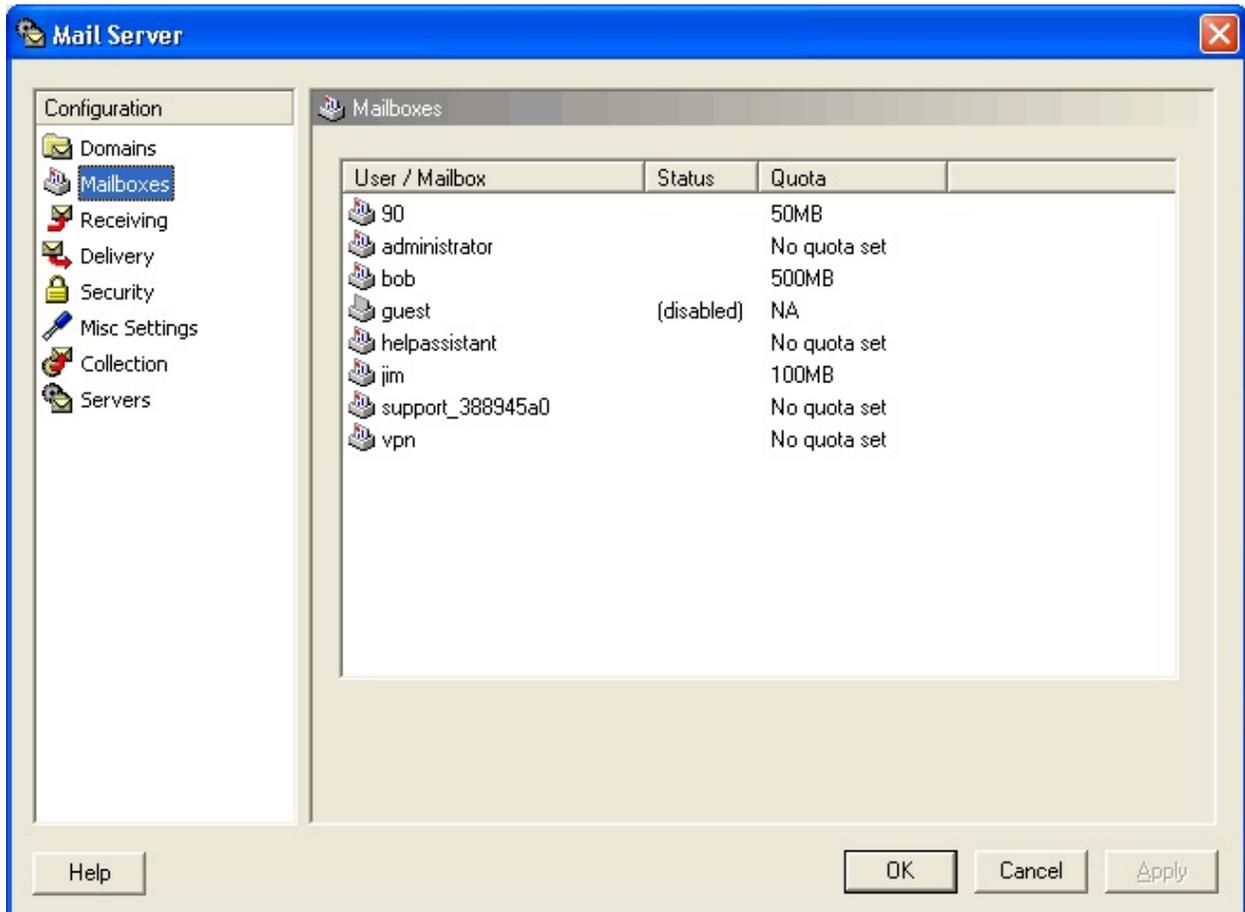
Indiquez la taille maximum des messages pouvant être envoyés à la liste.

Bloquer toutes les pièces jointes (*Block all attachments*)

Empêche les utilisateurs d'envoyer sur la liste des messages contenant des pièces jointes.

E-mail - Boîtes à lettres (*Boxes*)

Cette fenêtre contient la liste de toutes les boîtes à lettres des utilisateurs sur ce serveur, ainsi que des informations concernant leur configuration.



Masquer

Statut

Indique si la boîte est activée ou désactivée.

Quota

Espace maximum attribué pour la boîte (si cette option est activée).

Type

POP3 ou IMAP4 (défini dans l'onglet [E-mail](#) des propriétés de l'utilisateur)

Double-cliquez sur un utilisateur pour en modifier les propriétés. Vous avez la possibilité d'appliquer des quotas, activer/désactiver sa boîte et d'afficher la liste de toutes ses adresses.

©2004 Qbik New Zealand Limited

Email - Réception (*Receiving*)

Diverses options sont configurables pour la **réception** du courrier.

Masquer

Espace libre requis pour la distribution du courrier : X Mo (*Receive mail while X MB free on partition*)

Cette option doit être cochée pour recevoir le courrier. Lorsque le nombre indiqué est atteint, WinGate ne reçoit plus de courrier et ne fait que le distribuer.

Utilisateurs inconnus (*Untrusted Sender*)

Autoriser le relais (*Allow relay*)

Lorsque cette option est cochée, le serveur accepte et envoie des messages pour des domaines non locaux. Remarque : l'activation de cette option peut présenter des risques concernant la sécurité.

Taille maximum du message (*Max Message Size*)

Pour limiter la taille des messages entrants, cochez cette case et remplissez le champ.

Nombre maximum de destinataires (*Max number of recipients*)

Pour limiter le nombre maximum de destinataires d'un message, cochez cette case et remplissez le champ.

Déconnecter après X commandes rejetées (*Disconnect if sender sends X disallowed commands*)

Limite le nombre de commandes pouvant être effectuées avant que le serveur n'arrête la connexion. Indiquez un nombre inférieur si votre connexion Internet est lente.

Refuser les domaines expéditeurs non vérifiés (*Block Invalid Sender Domain*)

Activez cette option pour vérifier la validité des messages entrants. Une vérification DNS et/ou MX est alors effectuée. Cette option vérifie également que les adresses IP et noms de serveur ne sont pas des faux (par exemple : 127.0.0.1 – ou toute autre adresse loopback – sont invalides).

Refuser les messages sans adresse de retour (*Block Blank Return Path*)

Cochez cette case si vous souhaitez rejeter les messages qui ne possèdent pas d'adresse de retour (return path) valide. (Limite le spam.)

Refuser les expéditeurs numériques (*Block Numeric Sender Domains*)

Cochez cette case si vous ne souhaitez pas recevoir de messages contenant une IP dans le champ "adresse". Il s'agit en effet d'une technique de spam couramment utilisée.

Utiliser la détection de relais ouverts (*Use open relay detection*)

Lorsque cette option est activée, vous pouvez indiquer le nom de domaine ou l'IP d'un serveur, afin que celui-ci compare l'adresse IP de l'expéditeur à celles de la liste des serveurs relais ouverts connus. Pour cela, ouvrez la fenêtre [Paramètres de la base de données relais ouverts](#).

Refuser les messages provenant d'adresses usurpées (*Block Spoofed Sender Address*)

Lorsque cette option est activée, vous pouvez vérifier si l'adresse IP de l'expéditeur utilise le même fournisseur d'accès que le serveur responsable du courrier de ce domaine. Pour cela, ouvrez la fenêtre [Paramètres de validation de l'adresse de l'expéditeur](#).

Refuser des pièces jointes (*Block Attachment File Types*)

Il est possible de refuser certaines pièces jointes en fonction de leur extension, car certaines peuvent contenir des virus : .exe, .vbs, .pif, .com, .scr. Indiquez les types d'extensions à refuser dans la fenêtre [Pièces jointes refusées](#).

Utilisateurs connus (*Trusted Sender*)

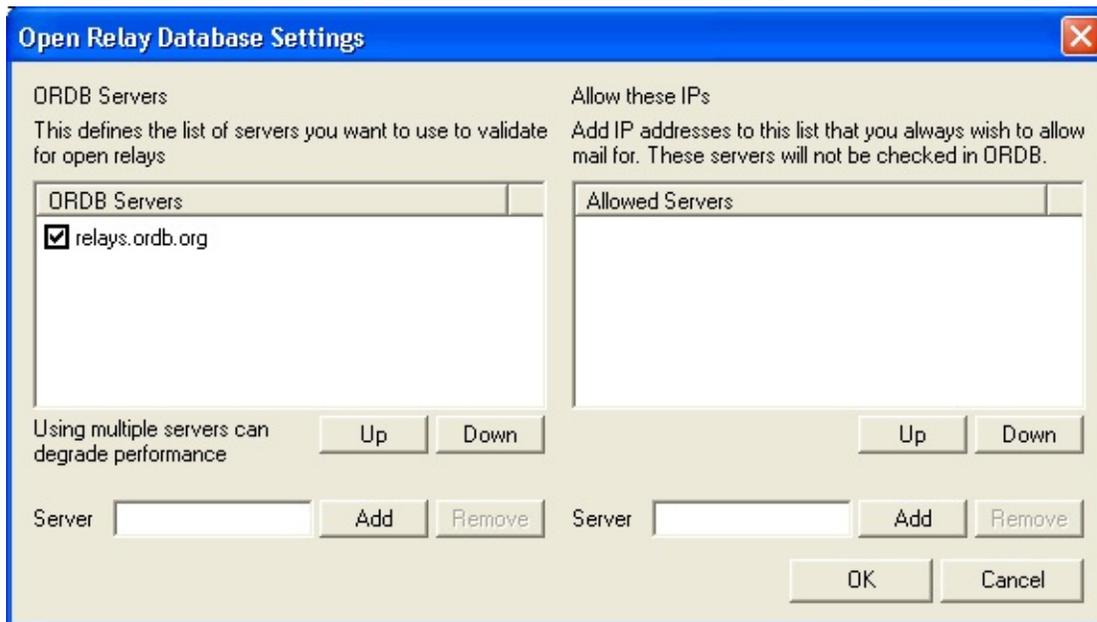
Autoriser le relais (*Allow relay*)

Lorsque cette option est cochée, le serveur accepte et envoie des messages pour des domaines non locaux. Dans la section "Expéditeurs connus", cette option ne présente pas les mêmes risques que dans la section "Expéditeurs inconnus" elle ne s'applique qu'aux utilisateurs de votre réseau LAN.

©2004 Qbik New Zealand Limited

Paramètres de la base de données relais ouverts

Indiquez ici le nom de domaine ou l'IP d'un serveur, afin que celui-ci compare l'adresse IP de l'expéditeur à celles de la liste des serveurs relais ouverts connus.



Masquer

Les serveurs relais ouverts sont souvent utilisés pour l'envoi de spam.

En voici quelques exemples :

inputs.orbz.org

outputs.orbz.org

relays.ordb.org

orbs.dorkslayers.com

dev.null.dk

relays.osirusoft.com

bl.spamcop.net

relays.visi.com

Remarque :

L'emploi de cette fonctionnalité a pour inconvénient le risque de faux positifs (rejet de messages légitimes par le serveur).

Indiquez dans quel ordre ces serveurs seront vérifiés à l'aide des boutons **Haut (Up)** et **Bas (Down)**.

©2004 Qbik New Zealand Limited

E-mail - Pièces jointes refusées

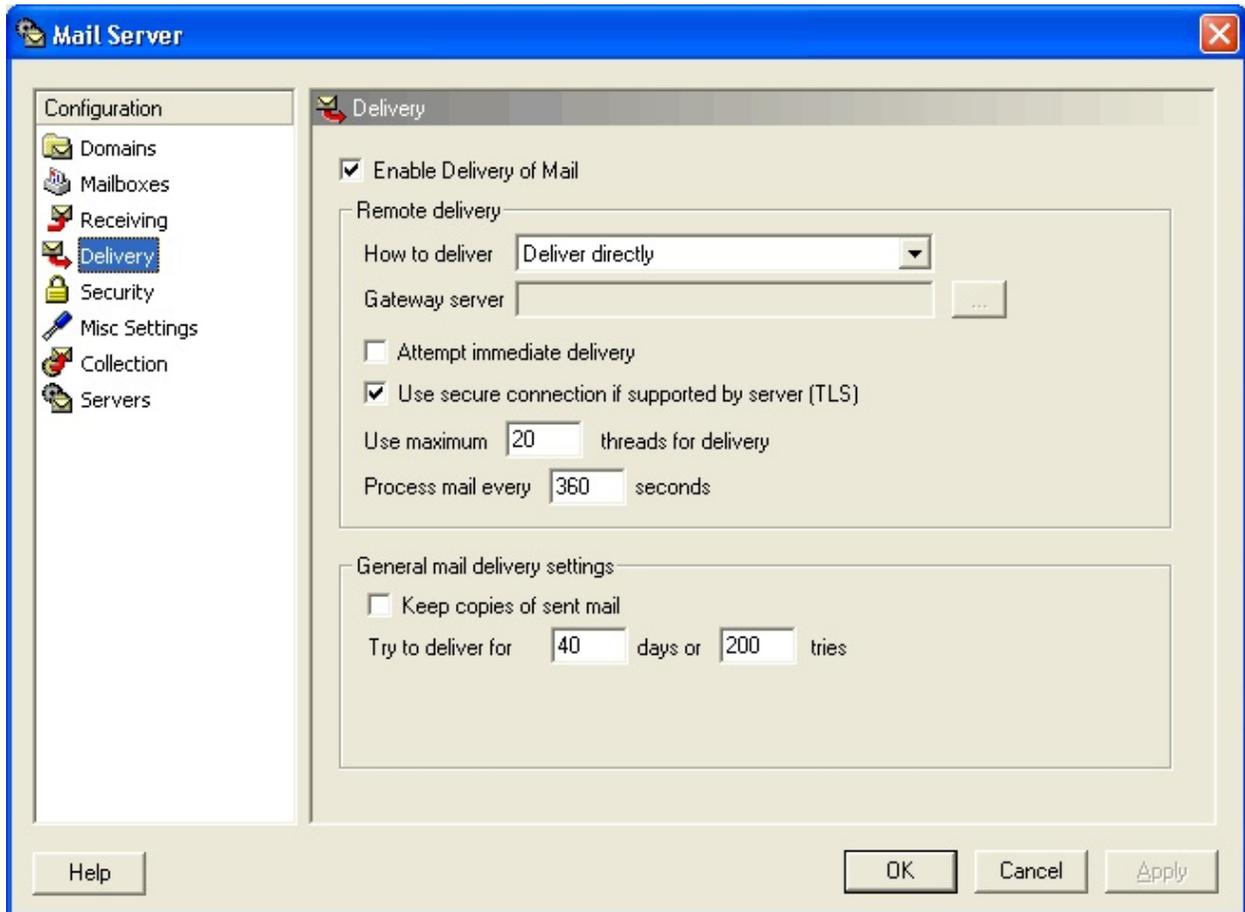
Indiquez ici les types d'extensions qui seront refusées.



Masquer

E-mail - Distribution (*Delivery*)

Cette fonctionnalité vous permet de paramétrer la distribution des messages reçus.



Masquer

Activer la distribution du courrier (*Enable delivery of mail*)

Cette option doit être cochée pour que WinGate distribue le courrier (qu'il soit distant ou local).

Distribution à distance (*Remote delivery*)

Choisissez parmi les options suivantes :

Distribuer directement (*Deliver directly*)

WinGate effectue des requêtes DNS spécifiques (résolutions MX) afin d'identifier automatiquement les serveurs acceptant la distribution du courrier pour les domaines destinataires. Cette option est sélectionnée par défaut et ne nécessite pas l'utilisation d'un autre serveur (comme celui de votre FAI). Elle est généralement utilisée pour les connexions permanentes.

Utiliser une passerelle (*Use gateway*)

Lorsque cette option est sélectionnée, WinGate redirige tout le courrier sortant (qui n'est pas destiné à des boîtes locales ou pour des adresses possédant une configuration spécifique) vers le serveur de votre choix (généralement le serveur SMTP de votre FAI).

Utiliser une passerelle pour le courrier échoué (*Use gateway for undeliverable mail*)

Le serveur essaie de distribuer le courrier directement, mais en cas d'échec il le transfère vers un autre serveur afin que celui-ci essaie à son tour. Cela peut s'avérer utile si votre serveur possède une adresse IP susceptible d'être en liste noire (en effet, les administrateurs mettent parfois certaines adresses commutées en liste noire).

Options

Passerelle (*Gateway server*)

Si vous avez sélectionné "Utiliser une passerelle" ou "Utiliser une passerelle pour le courrier échoué", indiquez ici le serveur à utiliser (identifié par son adresse IP ou nom d'hôte). Pour définir des paramètres supplémentaires cliquez sur le bouton situé sur la droite (par exemple, si le courrier est transféré vers votre FAI et que celui-ci exige une authentification).

Ne pas utiliser plus de X threads (*Use maximum X threads for delivery*)

Indiquez le nombre maximum de threads pouvant être utilisés simultanément pour la distribution. La valeur par défaut convient pour la plupart des cas. Cependant, vous pouvez indiquer une valeur inférieure si votre ordinateur effectue de nombreuses tâches, afin de réduire la puissance de traitement utilisée par la distribution du courrier dans WinGate.

Distribution immédiate (*Attempt immediate delivery*)

Lorsque cette option est cochée, WinGate démarre le processus de distribution dès qu'il reçoit un message. Dans le cas contraire, les messages ne sont traités

qu'à la fréquence indiquée dans l'option ci-dessous.

Traiter le courrier toutes les X secondes (*Process mail every X seconds*)

Indiquez la fréquence à la laquelle WinGate doit effectuer les tâches planifiées.

Essayer de distribuer pendant X jours ou X tentatives (*Try to deliver for X days or X tries*)

Définir après combien de temps ou de tentatives tout les messages non distribués d'un domaine seront retournés à leur expéditeur (il suffit que l'une des deux valeurs expire pour que le courrier soit renvoyé).

La distribution déclenche le composeur (*Allow delivery to trigger dialer*)

Lorsque cette option est cochée et que votre serveur utilise une connexion commutée, le processus de distribution du courrier déclenche le composeur.

Conserver une copie des messages (*Keep copies of sent mail*)

Lorsque cette option est cochée, tous les messages distribués seront copiés dans le dossier \Mail\Spool\Sent du répertoire d'installation de WinGate. Pensez à nettoyer ce dossier régulièrement.

Remarque :

WinGate conserve une trace des messages à distribuer dans le dossier \Mail\Spool.

Il analyse régulièrement ces dossiers afin de vérifier si des messages reçus doivent être distribués.

WinGate possède également une base de données interne contenant des informations sur les tâches planifiées de chaque domaine ayant des messages en attente. Il peut arriver que certaines tâches soient reprogrammées à la suite d'un problème survenant lors de la distribution (par exemple, si un serveur distant est indisponible).

E-mail - Sécurité (*Security*)

Cette fonctionnalité permet de configurer les paramètres de sécurité du service E-mail de WinGate.

Mail Server Security screen



Masquer | Masquer toutes les images

Elle comporte deux applications :

1. Support de l'authentification (protocoles POP3 et SMTP).
2. Support des connexions sécurisées TLS (Transport Layer Security)

Authentification :

Procédé par lequel le client confirme son identité auprès du serveur. Ceci peut être effectué à l'aide de diverses méthodes fonctionnant de façons différentes. On distingue les authentifications sécurisées des authentifications non sécurisées en fonction de la façon dont les mots de passe sont transmis sur le réseau (s'ils peuvent être interceptés ou non).

Le protocole POP3 (réception d'e-mails) nécessite une authentification pour des raisons évidentes : le système en a besoin pour déterminer à quelle boîte l'utilisateur essaie d'accéder. Avec le protocole SMTP (envoi d'e-mails) cela n'est pas indispensable mais présente de nombreux avantages.

En effet, lorsqu'un utilisateur s'authentifie pour le SMTP, il est considéré comme un utilisateur connu et possède donc plus de privilèges (comme l'envoi de courrier par le biais d'un relais).

Par défaut, un utilisateur est considéré comme connu pour l'envoi de courrier s'il répond à l'une des conditions suivantes :

1. Il s'est connecté à WinGate dans une interface "connue" (dans les paramètres avancés : Interfaces)
2. La configuration de son adresse IP l'associe à un compte utilisateur WinGate
3. Il s'est authentifié dans le service SMTP de WinGate

Par conséquent, si vous souhaitez que les utilisateurs externes à votre réseau puissent bénéficier du serveur de messagerie de WinGate, la seule méthode sécurisée est l'authentification (en effet, leur adresse IP risque de changer fréquemment).

WinGate supporte les méthodes d'authentification suivantes :

Non sécurisée : SASL: PLAIN, USER/PASS (POP3 uniquement)

Sécurisée : SASL: NTLM, SASL: CRAM-MD5, APOP (POP3 uniquement)

SASL (Simple Authentication and Security Layer) est un procédé d'authentification pouvant être utilisé avec diverses méthodes. Ainsi les méthodes PLAIN, NTLM et CRAM-MD5 sont supportées avec les protocoles SMTP et POP3. De plus, la méthode USER/PASS ainsi que les commandes

APOP sont supportées pour le POP3.

WinGate vous permet également d'exiger qu'une connexion soit sécurisée (voir ci-dessous) avant d'autoriser certaines méthodes d'authentification, afin d'éviter que les mots de passe ne soient envoyés sur le réseau de façon non sécurisée.

Bases de données d'utilisateurs

En fonction de la base de données d'utilisateurs choisie (celle de WinGate ou du système d'exploitation), certaines méthodes risquent de ne pas être disponibles. En résumé, pour une base de données NT l'authentification doit être de type plaintext, ou SASL NTLM (utilisé dans Outlook). Si vous choisissez la base de données WinGate, la méthode NTLM n'est pas disponible.

Mots de passes POP3 prioritaires

Les paramètres du compte de l'utilisateur ont également une influence sur les mots de passe. Par exemple, si vous avez indiqué que le mot de passe POP3 d'un utilisateur est prioritaire, et que votre programme de messagerie utilise la méthode USER/PASS, ce mot de passe doit être utilisé impérativement. Le mot de passe WinGate ou NT ne fonctionnera pas.

Cependant, avec d'autres méthodes le mot de passe POP3 prioritaire n'est utilisé qu'en deuxième recours (par exemple avec les méthodes APOP et CRAM-MD5 lorsque l'on utilise la base de données NT), car sinon elles ne seraient pas disponibles.

Paramètres

Trois paramètres sont disponibles pour chaque méthode :

1. **Refusé (*Denied*)**

Il n'est pas possible de s'authentifier à l'aide de cette méthode.

2. **Autorisé (*Allowed***

)

Il est possible de s'authentifier avec cette méthode.

3. Connexion sécurisée obligatoire (*Allowed with secure connection*)

La méthode n'est disponible que si la connexion est sécurisée (TLS/SSL).



Masquer | Masquer toutes les images

Connexions sécurisées (TLS/SSL)

Elles permettent de réduire les risques avec les méthodes d'authentification non sécurisées car la connexion est cryptée. Ainsi, vous pouvez utiliser en toute sécurité des méthodes qui présenteraient des risques avec une connexion normale.

De plus, si vous choisissez ce type de connexion les messages sont également envoyés de façon cryptée. Ainsi, même si un pirate utilise un "sniffeur" sur votre réseau ou sur Internet il ne connaîtra pas leur contenu.

Certificats

Pour bénéficier du support TLS, vous devez posséder un certificat (X.509 au format PEM standard). Les certificats ont pour but de valider l'authenticité d'un serveur. Ils sont utilisés depuis de nombreuses années sur les serveurs sécurisés. WinGate peut générer son propre certificat pour le courrier, mais vous pouvez également en obtenir un auprès d'une autorité reconnue. Si vous choisissez de générer un certificat avec WinGate, certains clients de messagerie risquent de ne pas l'accepter. Toutefois, la plupart d'entre eux peuvent être configurés afin de les

obliger à reconnaître le certificat.

Par conséquent, les certificats de WinGate devraient vous suffire, sauf si la configuration des clients s'avère trop fastidieuse. En outre, l'obtention de certificats signés auprès d'une agence n'est généralement pas un service gratuit.

Remarque importante :

Lors de la création d'un certificat vous devez lui attribuer un nom, qui servira à identifier le serveur. La plupart des clients n'acceptent pas que le nom du certificat ne soit pas le même que celui du serveur sur lequel ils sont connectés. Vous avez par contre la possibilité d'utiliser des caractères joker. Par exemple, le serveur de messagerie de Qbik emploie le nom :

*.qbik.com

Les clients peuvent donc accéder à leur courrier en se connectant à n'importe quel nom finissant par qbik.com.

Enfin, WinGate ne supporte que les certificats au format .PEM. Si vous avez obtenu votre certificat auprès d'une agence, il sera éventuellement nécessaire de le convertir (de nombreux outils de conversion sont disponibles sur Internet).

Identité du serveur

Nom servant à désigner le serveur. Par défaut, il s'agit du nom DNS de l'ordinateur sur lequel il se trouve. Par exemple : "qbik.com" pour un serveur sous Windows 2000 Active Directory, ou "WorkPC1" pour des systèmes d'exploitation plus anciens. Ce nom est également utilisé lors de la création de certificats (sauf si vous décidez du contraire), et figure donc dans les programmes de gestion des certificats.

Clients de messagerie

La plupart des clients supportent les connexions sécurisées et/ou l'authentification, à différents niveaux. Voici quelques informations concernant les principaux clients :

Microsoft Outlook et Outlook Express.

Méthodes d'authentification supportées :

POP3 : USER/PASS, NTLM.

SMTP : NTLM

En ce qui concerne les connexions sécurisées, Outlook supporte le TLS pour l'envoi de courrier (SMTP), mais pas pour la réception (POP3).

Si vous spécifiez qu'Outlook doit utiliser une connexion sécurisée pour le POP3, il essaiera de se connecter à un serveur POP3 sécurisé (SPOP) sur le port 995. Or, cela n'est pas supporté dans WinGate.

Qualcomm Eudora

Méthodes d'authentification supportées :

POP3 : USER/PASS, APOP, CRAM-MD5, Kerberos (non disponible)

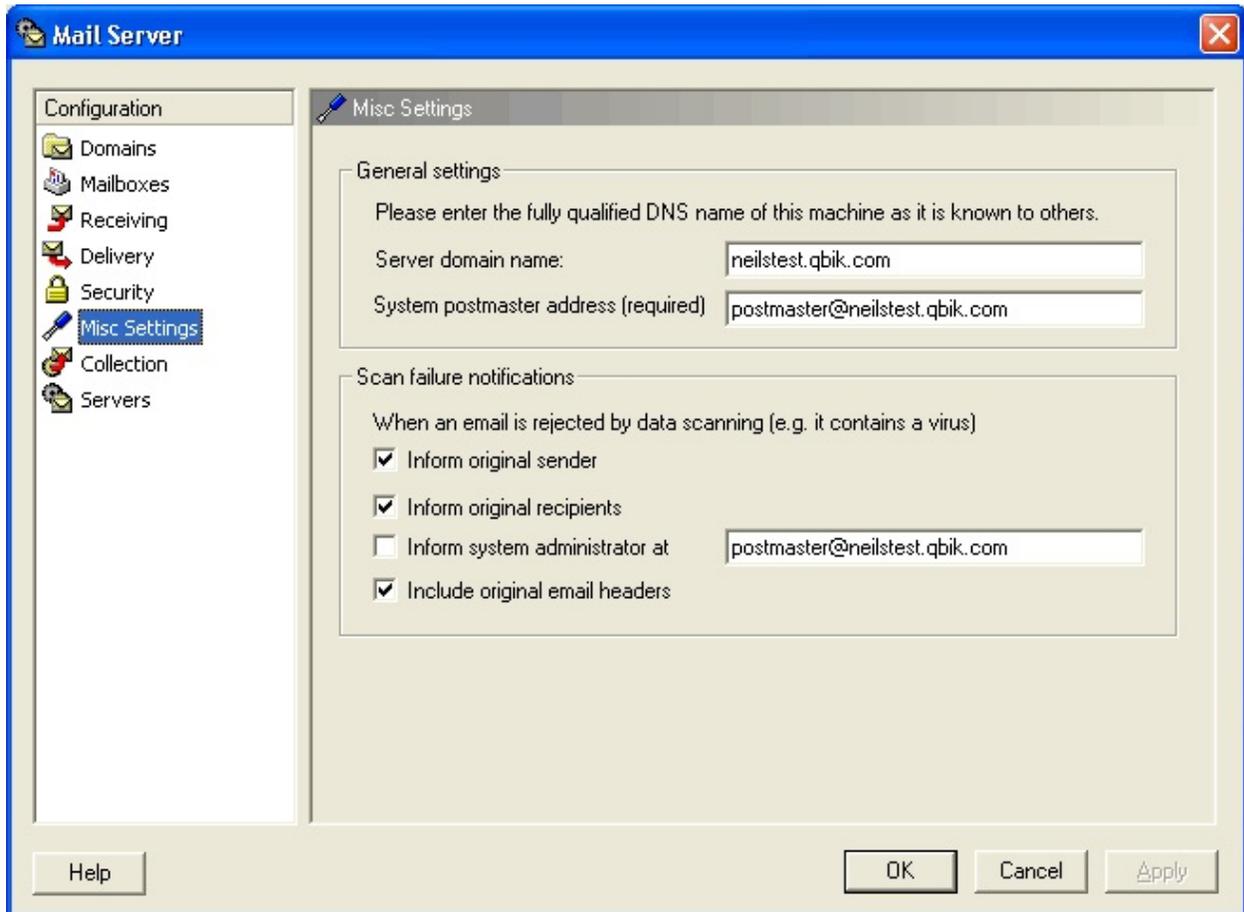
SMTP : CRAM-MD5, Kerberos, PLAIN

Support TLS inclus.

©2004 Qbik New Zealand Limited

E-mail - Divers (*Misc Settings*)

Dans la fenêtre **Divers** vous pouvez choisir diverses options concernant l'analyse du courrier sur votre réseau (par exemple l'analyse antivirus).



Masquer

Général

Adresse du postmaster (obligatoire) (*System postmaster address (required)*)

Vous devez indiquer dans ce champ une adresse valide afin que le serveur puisse fonctionner correctement.

Notifications de rejet

Informez l'expéditeur d'origine (*Inform original sender*)

Un message est envoyé à l'expéditeur afin de l'informer qu'il a envoyé un message contenant un virus.

Informez les destinataires d'origine (*Inform original recipients*)

Un message est envoyé aux destinataires du message infecté, afin de les informer que celui-ci a été rejeté.

Informez l'administrateur système (adresse :) (*Inform system administrator at*)

Un message est envoyé à l'administrateur, afin de l'informer qu'un message a été rejeté. Vous devez pour cela indiquer une adresse e-mail valide.

Incluez les en-têtes d'origine (*Include original email headers*)

Cochez cette option pour inclure les en-têtes d'origine dans le message de notification. Cela permet souvent de déterminer l'origine du message rejeté.

Remarques :

Les paramètres choisis dans "Notifications de rejet" n'auront aucun effet si vous n'avez pas installé le module Data Scanning.

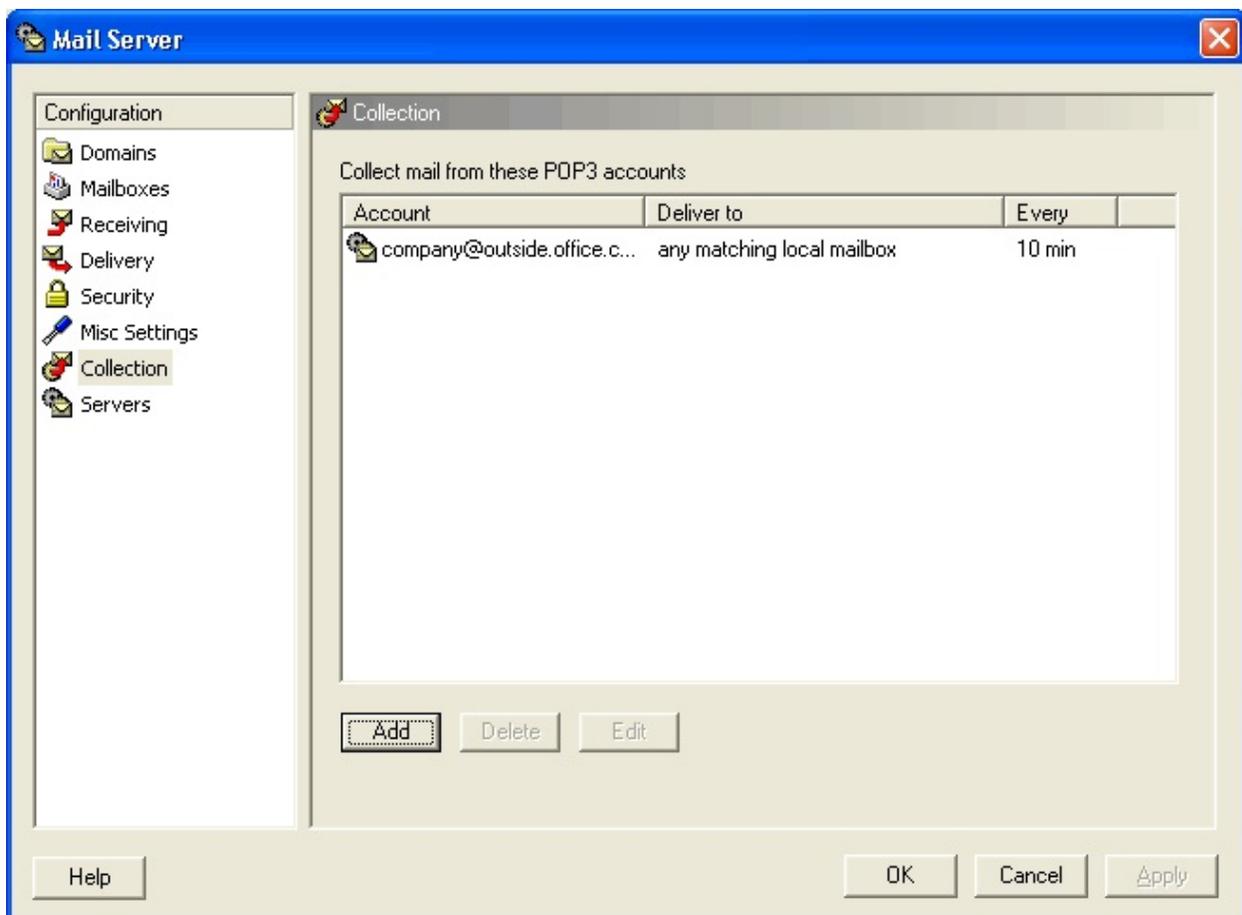
WinGate peut analyser le courrier entrant, si la configuration de la fenêtre [Modules](#) du serveur SMTP le permet. Les analyses recherchent généralement les virus ou les spams. Lorsqu'un message est rejeté, il est possible d'envoyer une notification à l'expéditeur, au destinataire ou à l'administrateur système.

E-mail - Collecte (*Collection*)

Cette fonctionnalité permet de planifier des tâches afin que WinGate se connecte à intervalles réguliers à des serveurs POP3 et collecte le courrier.

Les messages sont ensuite distribués en fonction d'un certain nombre de règles, configurées pour chaque tâche de façon individuelle.

Cela peut s'avérer utile pour le partage de comptes POP3, ou les comptes collecteurs (où tout le courrier d'un domaine est distribué dans une seule boîte à lettres, généralement sur votre FAI).



Masquer

Champs

Compte (*Account*)

Indique le serveur et l'identifiant de la boîte à lettres.

Distribution (*Deliver to*)

Indique la façon dont le courrier collecté sera distribué.

Fréquence (*Every*)

Fréquence (en minutes) à laquelle le serveur vérifie le courrier.

Boutons**Ajouter (*Add*)**

Ouvre la fenêtre "Collecte du courrier", dans laquelle vous pouvez ajouter une tâche et configurer ses propriétés.

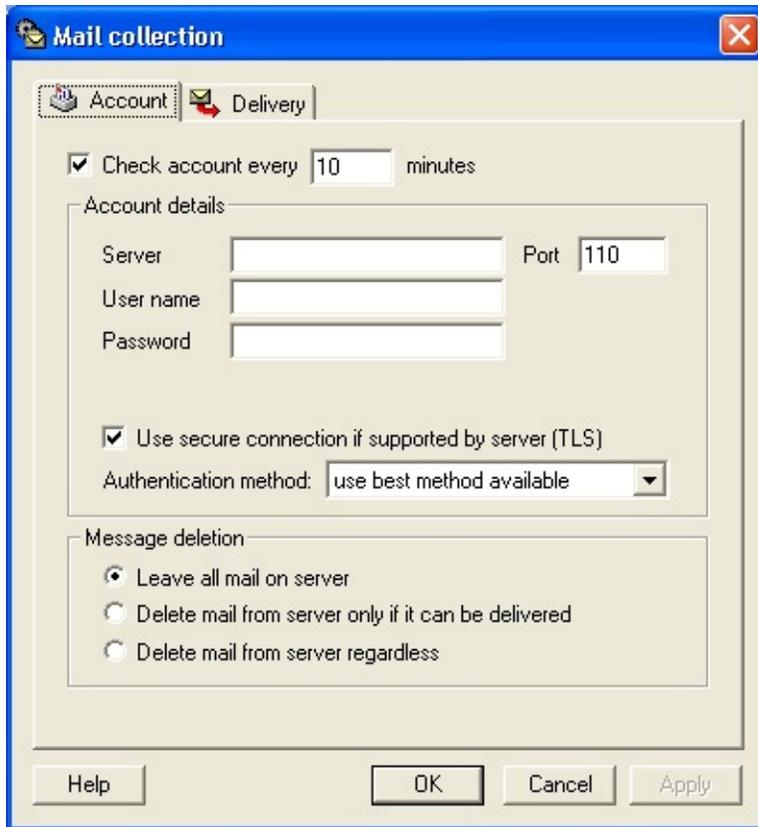
Modifier (*Edit*)

Pour modifier une tâche, sélectionnez-la et cliquez sur ce bouton.

Supprimer (*Delete*)

Cliquez sur ce bouton pour supprimer une tâche.

Collecte - Onglet Compte



Masquer

Vérifier toutes les X minutes (*Check account every X minutes*)

Indiquez à quelle fréquence WinGate doit collecter le courrier de ce compte.

Utiliser une connexion sécurisée (TLS) si le serveur le permet (*Use secure connection if supported by server (TLS)*)

Pour utiliser cette méthode, vous devez générer un certificat (dans la fenêtre Serveurs).

Méthode d'authentification (*Authentication method*)

Par défaut, WinGate recherche la meilleure méthode disponible supportée par le serveur. Toutefois, il peut arriver qu'un serveur n'indique pas correctement les méthodes supportées.

Dans ce cas, il peut s'avérer nécessaire d'indiquer à WinGate celle qu'il doit choisir :

USER/PASS

SASL PLAIN

APOP

CRAM-MD5

NTLM

Suppression des messages (*Message Deletion*)

Conserver tout le courrier sur le serveur (*Leave all mail on server*)

Vous devrez le supprimer manuellement.

Ne supprimer que le courrier distribué (*Delete mail on server only if it can be delivered*)

Cocher cette option garantit que le courrier est bien distribué avant d'être supprimé du serveur.

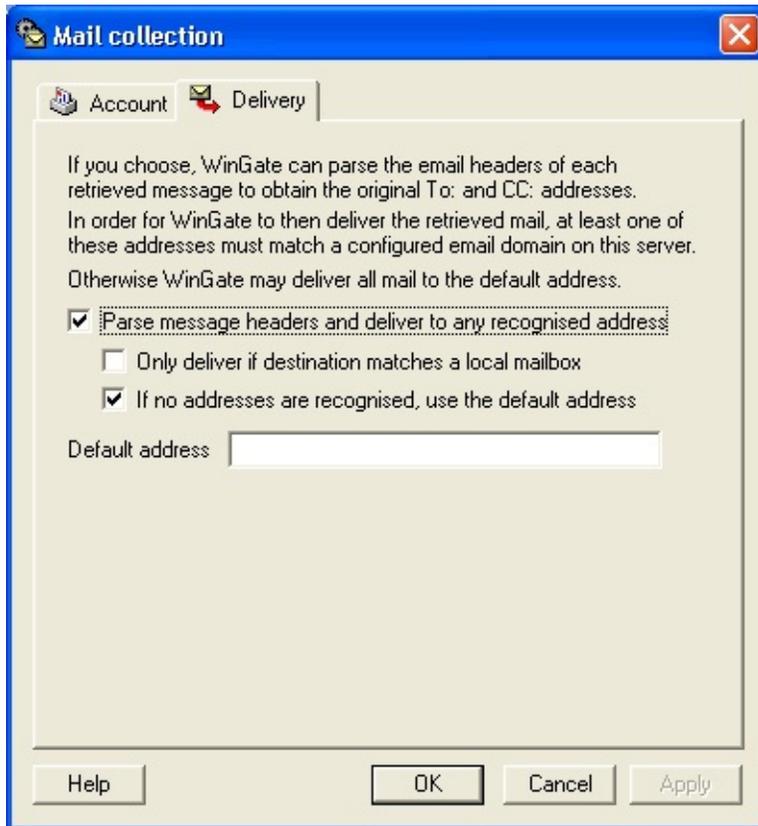
Supprimer tout le courrier (*Delete mail from server regardless*)

Si vous cochez cette option le courrier sera supprimé du serveur, même s'il n'a pas été correctement distribué.

©2005 Qbik New Zealand Limited

Collecte - Onglet Distribution (*Delivery*)

Indiquez ici la façon dont le courrier collecté sera distribué.



Masquer

Analyser les en-têtes des messages et distribuer aux adresses identifiées (*Parse message headers and deliver to any recognised address*)

Si cette option n'est pas cochée, WinGate distribuera tout le courrier à l'adresse par défaut.

Ne distribuer que si le destinataire correspond à une boîte locale (*Only deliver if destination matches a local mailbox*)

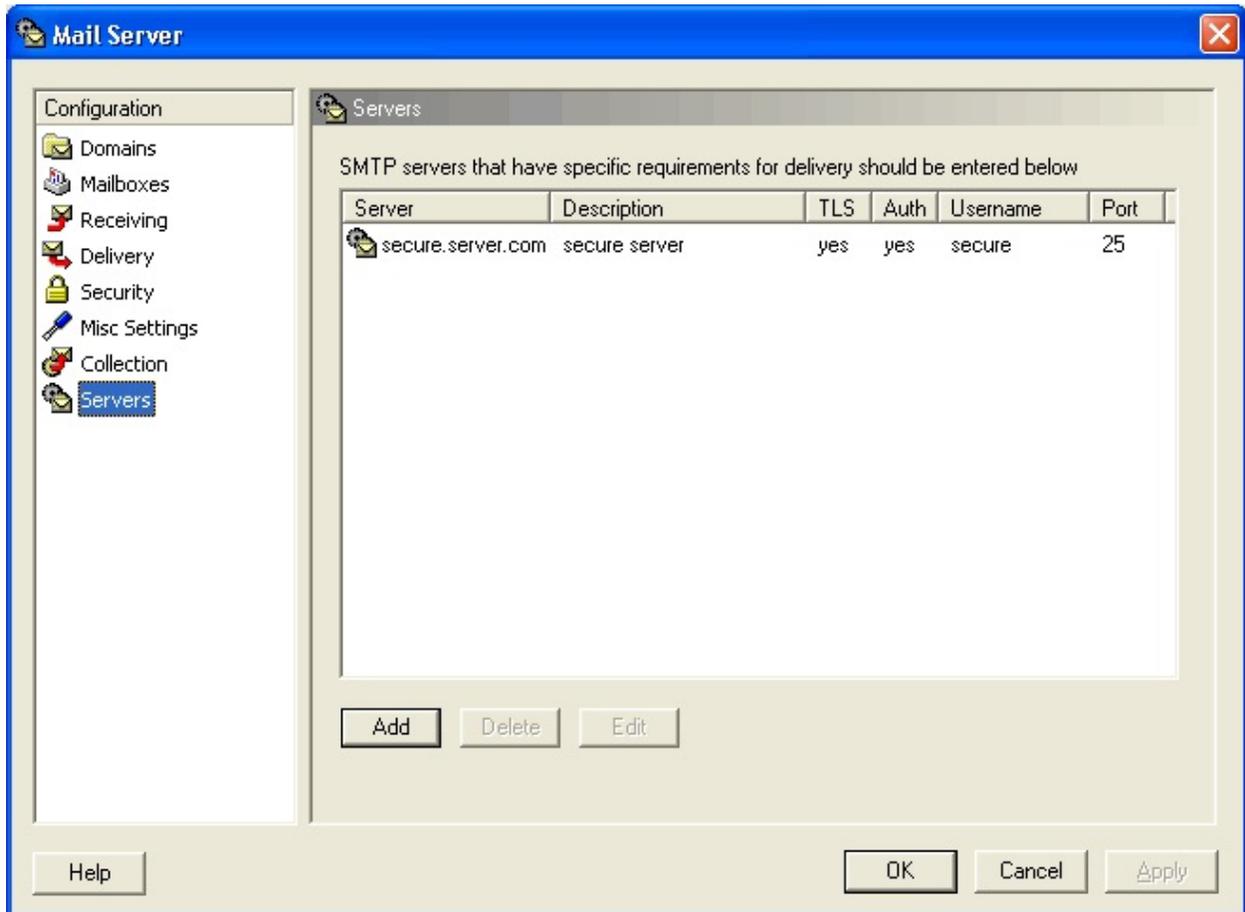
Lorsque cette option est cochée, le courrier qui n'est pas correctement adressé à une boîte locale sera rejeté.

Utiliser l'adresse par défaut si aucune adresse n'est identifiée (*If no addresses are recognised, use the default address*)

Pour que cette option fonctionne, vous devez indiquer une adresse valide dans le champ situé au-dessous.

E-Mail - Serveur (Servers)

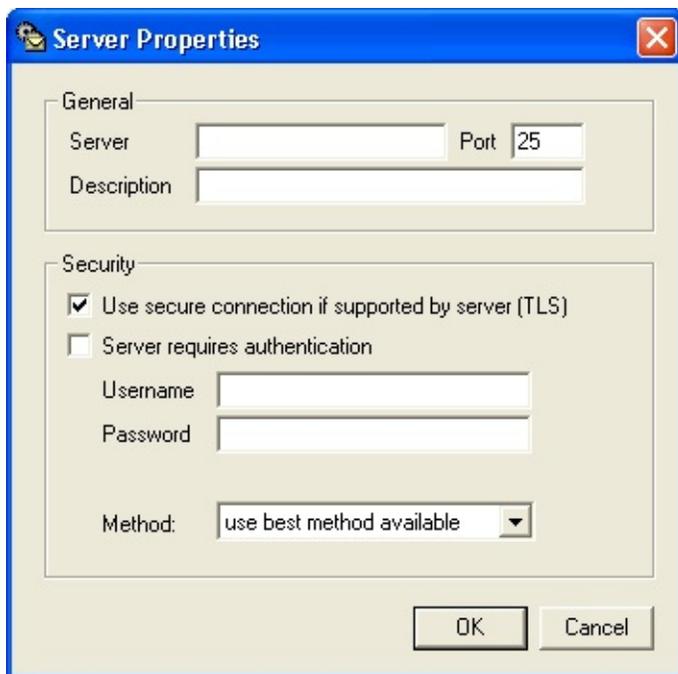
Cette fenêtre affiche la liste des serveurs SMTP ayant des paramètres spécifiques.



Masquer | Masquer toutes les images

Cliquez sur **Ajouter (Add)** pour configurer un nouveau serveur.

Pour modifier ou supprimer un serveur, surlignez-le et cliquez sur **Modifier (Edit)** ou **Supprimer (Delete)**.



Masquer | Masquer toutes les images

Général

Serveur (*Server*)

Nom du serveur.

Description

Indiquez la description de votre choix.

Sécurité (*Security*)

Utiliser une connexion sécurisée (TLS) si le serveur le permet (*Use secure connection if supported by server (TLS)*)

Authentification requise (*Server requires authentication*)

Si votre serveur exige une authentification, cochez cette option et indiquez votre

nom d'utilisateur et votre mot de passe.

Remarque :

Même si l'authentification échoue lors de la distribution, WinGate essaie tout de même de distribuer le courrier car elle n'est que rarement requise.

©2005 Qbik New Zealand Limited

Présentation de la fonction de cache

Qu'est-ce que la mémoire cache ?

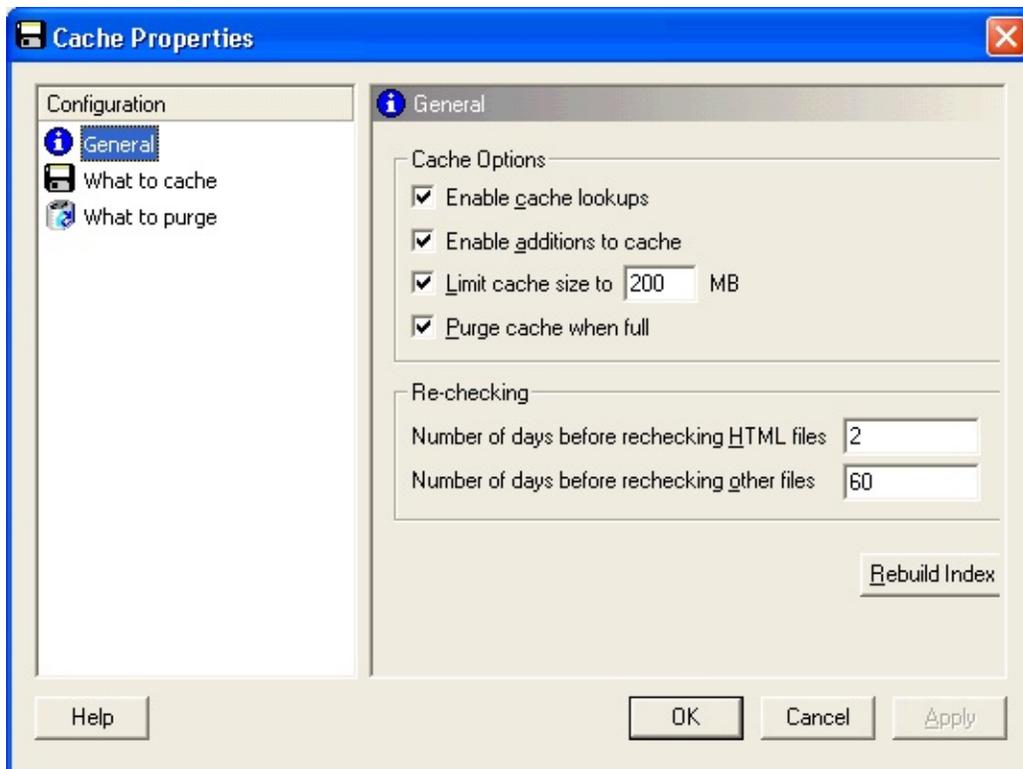
Cela consiste à enregistrer les données utilisées régulièrement de façon à pouvoir y accéder au besoin de façon rapide et simple. WinGate met en cache les informations provenant d'Internet, comme les graphiques, documents HTML, ou autres fichiers si vous utilisez le service proxy web.

Si vous utilisez WinGate Internet Client ou le NAT ces informations ne seront mises en cache que si vous avez coché l'option **Proxy transparent** (en cliquant sur l'icône **Sessions** dans les propriétés du serveur proxy web).

Ainsi, les données fréquemment consultées sont enregistrées sur le disque local, ce qui permet d'améliorer considérablement les performances sur Internet. En effet, ces données sont téléchargées moins souvent. WinGate dispose bien sûr de règles avancées qui déterminent quelles sont les données mises en cache. Vous avez toutefois la possibilité d'obliger votre navigateur à télécharger tout de même les données en cliquant sur **Recharger** (Netscape) ou **Actualiser** (Internet Explorer).

Quelles sont les données mises en cache ?

La **mémoire cache** de WinGate a pour avantage d'être partagée par tous les utilisateurs du service proxy web de votre réseau. Ainsi, si les informations que vous souhaitez obtenir sont souvent consultées par un autre utilisateur, elles seront déjà présentes dans la mémoire cache du serveur. Le processus est donc plus rapide, car il n'est pas nécessaire de les télécharger.



Masquer

Options

Activer le cache (*Enable Cache Lookups*)

Si cette option n'est pas cochée, le cache ne sera pas accessible et les pages seront toujours téléchargées d'Internet.

Vous ne serez amené à la décocher que si vous rencontrez des problèmes avec un document mis à jour.

Autoriser les ajouts (*Enable Additions to the Cache*)

Les pages ajoutées à la mémoire dépendent des paramètres définis en cliquant sur [Mettre en cache \(*What to cache*\)](#).

Limiter la taille à (*Limit cache size to*)

Lorsque la taille de la mémoire cache atteint la limite indiquée (par défaut : 200 Mo), 20 % des données les moins utilisées sont supprimées.

Recommandations :

Tailles minimum recommandées :

1 à 5 utilisateurs, avec un modem 56k : 30 Mo

Jusqu'à 10 utilisateurs, connexion modem ou RNIS : 40 Mo

Plus de 10 utilisateurs avec du haut débit : 50 Mo

Conseils

L'utilisation de la mémoire augmente la vitesse de restitution des données. Si votre cache est de petite taille, en augmentant sa taille d'un tiers il sera 100% plus efficace.

Avec les options de Mettre en cache (*What to cache*)/Supprimer (*What to purge*), vous réduisez significativement l'utilisation de la bande passante et augmentez la vitesse.

Supprimer des éléments lorsque la mémoire est pleine (*Purge cache when full*)

Supprime des éléments inutiles ou superflus lorsque la mémoire est pleine. Veuillez noter que cette option ne supprime pas la totalité des données mise en cache.

Vérifications (*Re-checking*)

Vérifier les fichiers HTML après (jours) (*Number of days before rechecking HTML files*)

Si un fichier a été requis lors des X derniers jours, il ne sera pas vérifié et

actualisé.

Vérification des autres fichiers

Les graphiques et autres fichiers changent moins souvent. L'intervalle de vérification par défaut est donc beaucoup plus long.

Mettre l'index à jour (*Rebuild Index File*)

Cette option permet de mettre à jour l'index de la mémoire cache si vous avez supprimé des entrées manuellement.

Remarque :

WinGate ne met en cache que les requêtes HTTP utilisant la méthode "GET". Les chaînes de requêtes (par ex. : envoi d'un formulaire) et les URL FTP ne sont pas mises en cache. Vous pouvez également créer vos propres règles afin de définir quels éléments seront mis en cache.

Remarque pour les utilisateurs de Windows NT :

Le répertoire cache peut parfois être très volumineux. Même si la plupart des fichiers ne dépassent pas 5 Ko , on en trouve fréquemment plus de 10000. Il peut donc s'avérer utile de conserver le répertoire cache sur un lecteur utilisant le système de fichiers NTFS : cela permet de gagner de l'espace et d'améliorer la vitesse de traitement des données.

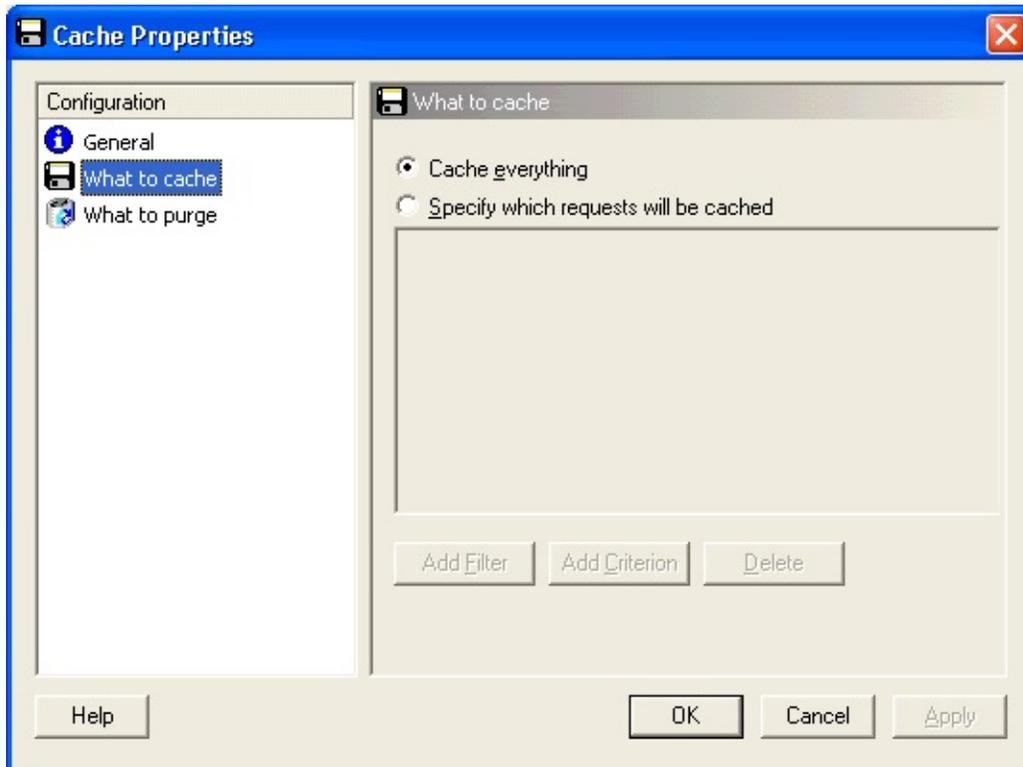
Voir également :

[Mémoire cache - Mettre en cache](#)

[Mémoire cache - Supprimer](#)

Mettre en cache (*What to cache*)

Configurez ici les éléments qui seront mis en cache par WinGate.



Masquer | Masquer toutes les images

Vous pouvez mettre toutes les pages en cache, ou bien créer des filtres afin de déterminer quelles pages le seront.

Création d'un filtre :

1. Ouvrez **GateKeeper**
2. Cliquez sur **Mettre en cache (*What to cache*)** dans les propriétés de la mémoire cache.
3. Cochez l'option **Choisir les requêtes mises en cache (*Specify which requests will be cached*)**.
4. Cliquez sur **Ajouter un filtre (*Add Filter*)**.

5. Cliquez sur **Ajouter un critère (Add Criterion)** pour configurer le filtre.
6. Dans **la fenêtre** qui s'ouvre ensuite, indiquez les données à mettre/ne pas mettre en cache, selon les conditions.

Masquer | Masquer toutes les images

7. Cliquez sur **OK** pour ajouter le critère.
8. Après avoir configuré les filtres, cliquez sur **OK**.

Afin de pouvoir utiliser cette option, il est nécessaire de comprendre le fonctionnement des règles logiques à l'aide des opérateurs **ET**, **OU** et **PAS**.

ET

Si des critères sont coordonnés avec ET, ils doivent tous être vrais pour que la règle s'applique.

OU

Si des critères sont coordonnés avec OU, il suffit que l'un d'entre eux soit vrai pour que la règle s'applique.

PAS

La règle s'applique si le critère n'est PAS vrai.

Pour la mémoire cache, tous les filtres sont coordonnés avec **OU**, et tous les critères d'un même filtre avec **ET** (ils doivent tous être vrais pour que le filtre s'applique). Par conséquent pour qu'une requête soit mise en cache, il faut qu'elle corresponde à tous les critères de l'un des filtres.

Attention aux pièges ! Par exemple : vous souhaitez "ne pas mettre en cache les requêtes de Mary ou Bob" et vous créez donc deux filtres (un avec le critère *Not User: Username equals Mary*, et un autre avec le critère *Not User: Username equals Bob*).

Vous n'obtiendrez pas le résultat escompté : Mary ne passera pas le premier filtre, mais puisque son nom d'utilisateur n'est pas Bob, elle passera le second, et

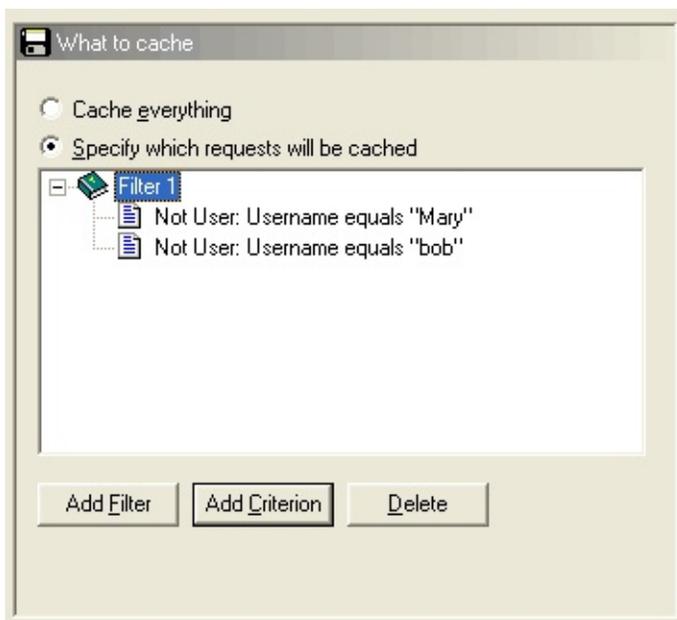
vice-versa (en effet, un utilisateur ne peut pas avoir deux noms différents).

Pour "ne pas mettre en cache pour Mary ou Bob" vous devez créer la règle :
"mettre en cache **NI** pour Mary **NI** pour Bob".

La règle ne fonctionnera que si ces deux critères sont pris en compte. Il doivent donc faire partie d'un même filtre:

1. Ne pas mettre le fichier en cache si la requête provient de Bob
2. Ne pas mettre le fichier en cache si la requête provient de Mary

Exemple



Masquer| Masquer toutes les images

La logique est donc la suivante :

Mettre en cache les fichiers si la requête ne provient **PAS** de Bob **ET PAS** de Mary. Le filtre ainsi créé est illustré ci-dessus.

Remarques sur les règles négatives :

Les règles négatives (où la mise en cache dépend de la non validité d'un critère)

peuvent être assez complexes. L'exemple ci-dessus montre qu'une requête peut être refusée par un filtre mais acceptée par un autre, que ce soit de façon directe ou indirecte (si elle n'est pas refusée).

Si vous utilisez plusieurs règles et souhaitez qu'un critère spécifique soit rejeté, assurez-vous de l'inclure dans chaque filtre. Ceci s'applique à toutes les règles de WinGate (y compris pour l'accès aux services).

©2004 Qbik New Zealand Limited

Mémoire cache - Supprimer (*What to purge*)

Lorsque le répertoire cache atteint sa taille maximum, WinGate peut supprimer des fichiers indésirables ou peu utilisés.

Pour cela, cliquez sur **Supprimer (*What to purge*)** dans les propriétés de la mémoire cache.

Masquer

Trois filtres sont déjà configurés par défaut :

1. Supprimer les fichiers volumineux (*Large Files*)

Il arrive souvent que la plupart de l'espace soit occupé par quelques fichiers très volumineux.

2. Supprimer les fichiers non utilisés (*Unused cache files*)

Supprime les fichiers non utilisés, c'est à dire requis moins d'une fois (hit count = *nombre de requêtes*).

3. Supprimer les fichiers vides (*Zero Length Files*)

Il arrive parfois qu'un problème survienne lors du téléchargement d'un fichier. Cette option évite que des fichiers inutiles n'occupent l'espace du répertoire.

Afin de pouvoir utiliser cette option, il est nécessaire de comprendre le fonctionnement des règles logiques à l'aide des opérateurs **ET**, **OU** et **PAS**.

ET

Si des critères sont coordonnés avec ET, ils doivent tous être vrais pour que la

règle s'applique

OU

Si des critères sont coordonnés avec **OU**, il suffit que l'un d'entre eux soit vrai pour que la règle s'applique.

PAS

La règle s'applique si le critère n'est **PAS** vrai.

Dans cette option, tous les filtres sont coordonnés avec **OU**, et tous les critères d'un même filtre avec **ET** (ils doivent tous être vrais pour que le filtre s'applique). Par conséquent pour qu'un fichier caché soit supprimé, il faut qu'il corresponde à tous les critères de l'un des filtres.

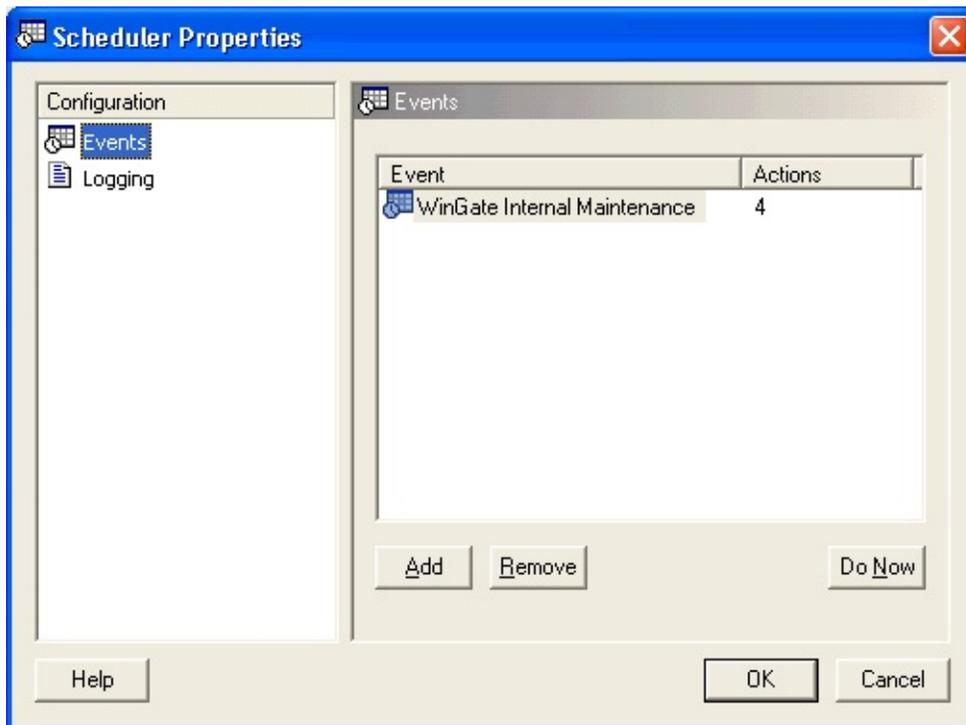
Ces filtres définissent le "profil" des fichiers à supprimer. L'ajout d'un filtre correspond au type de fichier que vous souhaitez supprimer, et en y ajoutant des critères vous précisez plus en détail les conditions à remplir.

Remarque sur les règles négatives :

Les règles négatives (où la suppression dépend de la non validité d'un critère) peuvent être assez complexes. En effet, un fichier peut être refusé par un filtre mais accepté par un autre, que ce soit de façon directe ou indirecte (s'il n'est pas refusé). Si vous utilisez plusieurs règles et souhaitez qu'un critère spécifique soit rejeté, assurez-vous de l'inclure dans chaque filtre.

Programmateur (Scheduler)

Le programmateur est une fonctionnalité clé de WinGate, permettant d'effectuer de nombreuses tâches de façon automatique.



Masquer

Qu'est-ce que le Programmateur ?

Il effectue automatiquement certaines tâches à des moments ou intervalles prédéfinis. Cela comprend de nombreuses fonctions de WinGate, ainsi que l'exécution de programmes en ligne de commande. Les options de programmation vont de quelques minutes à des mois.

A quoi sert-il ?

Il permet d'automatiser les opérations effectuées par WinGate, comme : le renouvellement des fichiers journaux, le nettoyage de la mémoire cache, la numérotation du composeur ou le démarrage et l'arrêt de WinGate. De plus, WinGate peut exécuter des programmes externes, y compris des fichiers batch. Les possibilités d'automatisation de votre système sont donc illimitées : vous pouvez programmer des sauvegardes système, des téléchargements montants et

descendants, etc.

Est-il nécessaire de l'utiliser ?

Vous pouvez l'utiliser à votre guise. Cela vous permet simplement d'éviter d'effectuer plusieurs fois la même opération. Par exemple, si vous avez besoin de renouveler vos fichiers journaux, programmez cette tâche afin qu'elle soit effectuée de façon hebdomadaire. Ainsi, ces fichiers n'atteindront jamais une taille démesurée. En effet, il est généralement plus simple de programmer un évènement que de l'effectuer soi-même !

Il n'est pas obligatoire d'utiliser le Programmeur, mais cela est généralement plus simple, sûr et rapide.

Comment fonctionne-t-il ?

La configuration d'un évènement est très simple. Il suffit de choisir une ou plusieurs actions à effectuer et de préciser à quelle heure ou à quel intervalle l'évènement doit se produire. (Pour en savoir plus, consultez les fichiers suivants). Certaines opérations, comme l'exécution de fichiers batch, permettent de contrôler des tâches ne faisant pas partie de WinGate.

Programmateur - Évènements

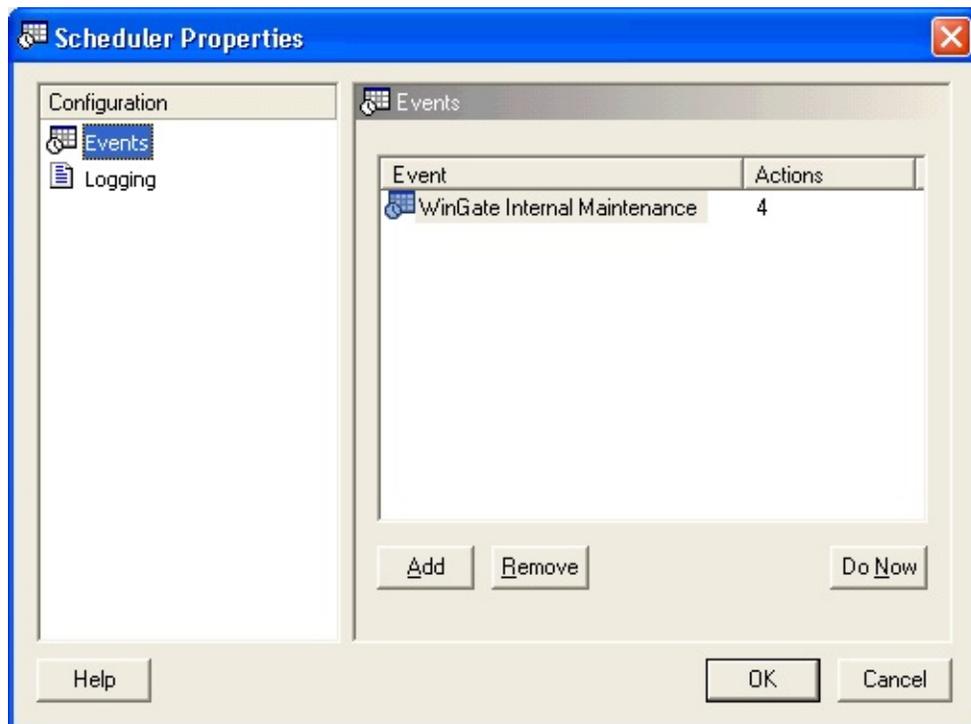
Avec WinGate, vous avez la possibilité de programmer des évènements. Vous devez alors préciser quelles sont les actions à effectuer.

Évènements

Un évènement peut être ponctuel, ou bien programmé afin de se produire de façon régulière (quotidienne, hebdomadaire, mensuelle ou toutes les heures).

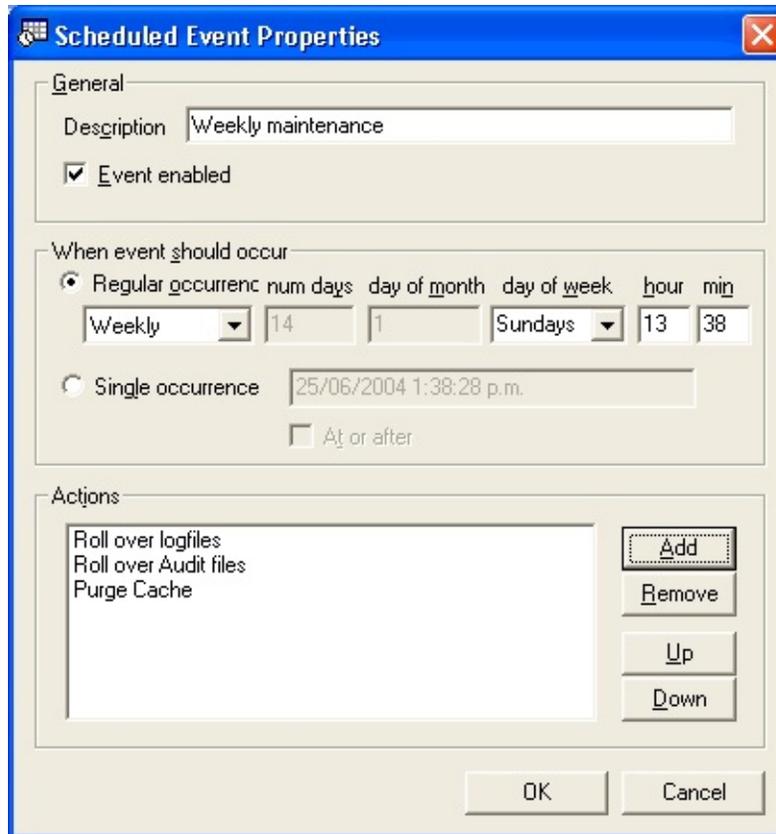
Ajouter un évènement

1. Ouvrez **GateKeeper**.
2. Cliquez sur **Programmateur (Scheduler)** dans les propriétés de l'onglet **Système**.



Masquer | Masquer toutes les images

3. Cliquez sur **Ajouter (Add)**.



Masquer | Masquer toutes les images

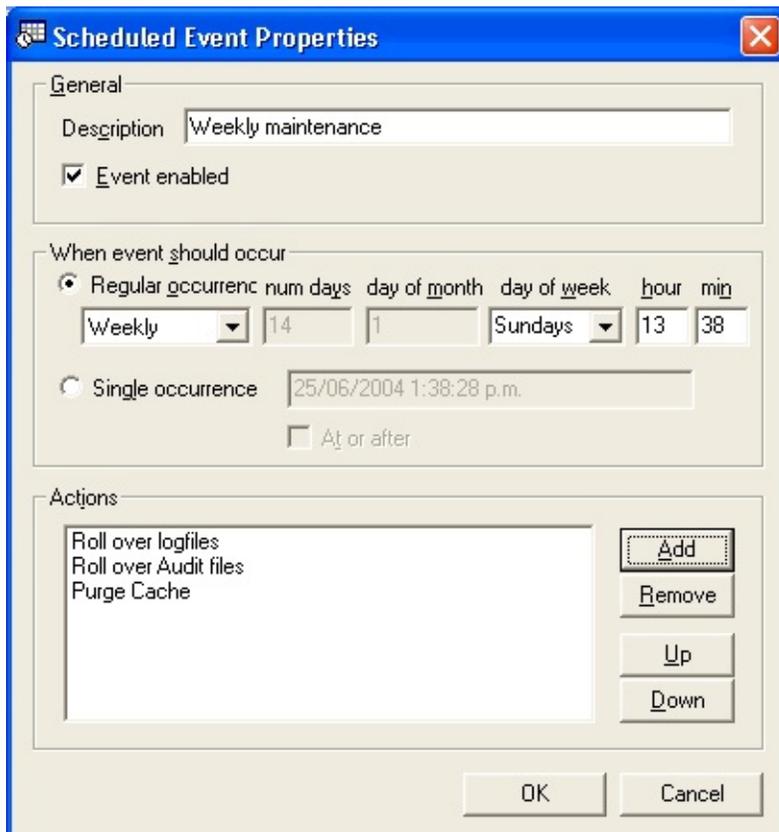
4. Indiquez une description dans le champ prévu à cet effet.
5. Cochez la case **Activer l'évènement (Event Enabled)**.
6. Choisissez à quelle fréquence où à quel moment il doit se produire.
7. Dans la partie **Actions** cliquez sur **Ajouter (Add)** pour choisir les actions à effectuer pour cet évènement.
8. Cliquez sur **OK**.
9. Vérifiez dans les propriétés du Programmateur que l'évènement a bien été ajouté.

[Cliquez ici pour en savoir plus sur les actions pouvant être effectuées](#)

©2005 Qbik New Zealand Limited

Actions du programmeur

La **liste des actions** choisies pour un évènement figure dans les propriétés de cet évènement. Ces actions seront effectuées selon l'ordre de la liste.



Masquer

Vous pouvez modifier cet ordre en cliquant sur les boutons Haut (*Up*) et Bas (*Down*).

De nombreuses actions sont disponibles :

Action	Options	Description
Arrêter le service (<i>Stop service</i>)	Tous les services de WinGate	Arrête le service indiqué.

Démarrer le service <i>(Start service)</i>	Tous les services de WinGate	Démarre le service indiqué.
Arrêter tous les services <i>(Stop all services)</i>	Aucune	Arrête tous les services de WinGate à l'exception du service d'administration à distance.
Démarrer tous les services <i>(Start all services)</i>	Aucune	Démarre tous les services de WinGate.
Numéroter <i>(Dial profile)</i>	Tous les profils de connexion de WinGate	Numérote le profil de connexion sélectionné.
Déconnecter <i>(Hang up profile)</i>	Tous les profils de connexion de WinGate	"Raccroche" le profil sélectionné.
Renouveler les fichiers journaux <i>(Roll over log files)</i>	Aucune	Crée de nouveaux fichiers journaux .log.
Renouveler les fichiers d'audit <i>(Roll over audit files)</i>	Aucune	Crée de nouveaux fichiers d'audit .log.
Exporter les comptes d'utilisateurs <i>(Export user accounts)</i>	Nom du fichier de destination Fusionner	Exporte les paramètres des comptes dans un fichier au format délimité par des tabulations.
Remettre le		<ul style="list-style-type: none"> • Remet à zéro toutes les valeurs de l'onglet Comptabilité. (Nombre d'octets

compte à zéro <i>(Reset user account)</i>	Tous les utilisateurs	envoyés/reçus du client et pour le client, et nombre de secondes en ligne.) • Remplace le solde d'ouverture par le solde de fermeture précédent.
Remettre tous les comptes à zéro <i>(Reset all user accounts)</i>	Aucune	Remet tous les comptes à zéro (voir ci-dessus).
Nettoyer le cache <i>(Purge cache)</i>	Aucune	Supprime des fichiers de la mémoire cache, comme si vous aviez cliqué sur "Supprimer maintenant" dans les options du cache.
Arrêter toutes les sessions <i>(Terminate all sessions)</i>	Aucune	Interrompt toutes les sessions en cours.
Exécuter une ligne de commande <i>(Execute command line)</i>	Lignes de commande Exécuter en arrière-plan	Exécute une ligne de commande de façon visible ou invisible. Cette action peut exécuter des programmes en ligne de commande sur le serveur. Si vous souhaitez exécuter plusieurs programmes, vous pouvez utiliser un fichier batch.
Envoyer un message aux clients <i>(Send message to clients)</i>	Uniquement lors de la connexion à GateKeeper	Affiche un message sur les postes clients.
Mémo <i>(Reminder)</i>	Message souhaité	Affiche un message dans GateKeeper.
Activer un utilisateur	Tous les utilisateurs	Active le compte sélectionné (s'il est

<i>(Enable user)</i>		désactivé).
Désactiver un utilisateur <i>(Disable user)</i>	Tous les utilisateurs	Désactive le compte sélectionné (s'il est activé).
Sauvegarder le registre <i>(Backup the WinGate registry)</i>	Aucune	Sauvegarde le registre de WinGate.
Connecter un VPN <i>(Connect a VPN)</i>	Nom du VPN	Effectue une connexion avec le VPN sélectionné.
Déconnecter un VPN <i>(Disconnect a VPN)</i>	Nom du VPN	Déconnecte le VPN sélectionné.
Traiter le courrier en file d'attente <i>(Force mail queue)</i>	Aucune	Distribue immédiatement tout le courrier en file d'attente.
Remettre à zéro les tentatives de distribution <i>(Reset mail try counts)</i>	Aucune	Remet à zéro le nombre de tentatives de distribution du courrier en file d'attente.
Mettre à jour les modules <i>(Run update for plugins)</i>	Aucune	Exécute lorsque c'est possible un fichier de mise à jour pour le module sélectionné.

©2004 Qbik New Zealand Limited

Service réseau avancé - Général (*Extended networking*)

Le service réseau avancé fournit aux utilisateurs de votre réseau des possibilités de partage Internet efficaces. Ces services offrent un accès aux informations du réseau au niveau des paquets, ce qui permet à WinGate de proposer les fonctionnalités suivantes :

([Cliquez ici pour une copie d'écran](#))

NAT

Le moteur NAT (Network Address Translation) permet aux ordinateurs du réseau d'accéder directement à une connexion Internet avec votre serveur WinGate. Il n'est pas nécessaire de configurer le proxy manuellement, ni d'installer de logiciel supplémentaire. De plus, il fonctionne avec quasiment tous les systèmes d'exploitation à une vitesse très performante.

Support de sous-réseaux multiples (routeur)

Cette option permet de partager des lecteurs, fichiers et autres ressources entre des ordinateurs connectés sur des sous réseaux différents. Si WinGate possède une interface connectée à chaque sous-réseau, il achemine les données TCP et UDP entre les ordinateurs. *Remarque : si vous désactivez cette option, l'icône "Routage" disparaît.

Protection pare-feu

Système de filtrage des paquets protégeant le serveur WinGate contre les attaques extérieures : déni de service, "pings of death" (pings de la mort), analyses de ports, chevaux de Troie ainsi que de nombreuses failles de Windows.

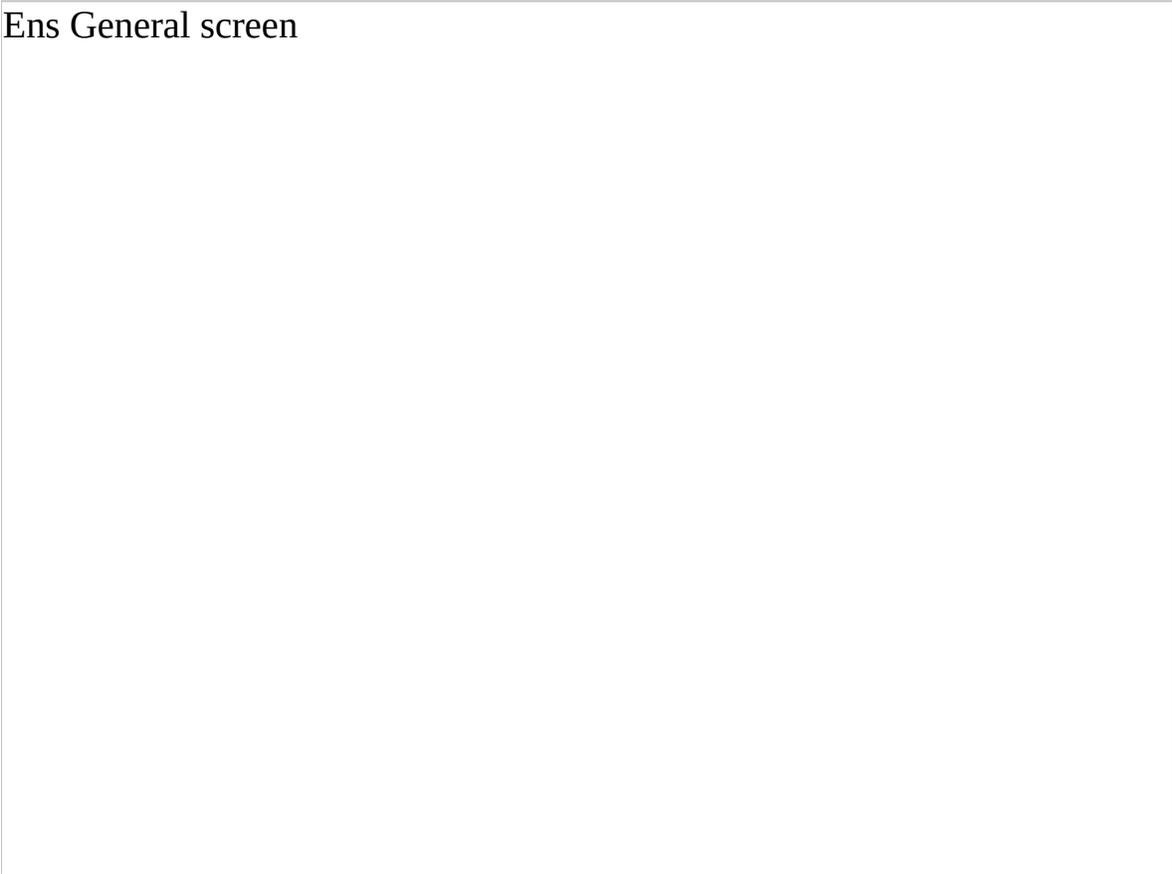
Remarque :

Cette fonctionnalité n'est disponible qu'à partir de la version 4 de WinGate.

Service réseau avancé (*Extended Networking Services*) - Général

Cette fenêtre permet de configurer les options du service ENS.

Ens General screen



Masquer

Statut :

Indique si le pilote est installé et actif. Cliquez sur "... " pour modifier le statut.

Activer le pilote ENS (*Enable Extended Network Driver*)

Si cette case n'est pas cochée, les services NAT,VPN, etc. ne seront plus disponibles.

Options

Service NAT (*General Purpose Internet sharing*)

Cochez cette case pour que le service ENS puisse fournir le NAT.

Support de sous-réseaux multiples (*Support for Multiple Subnetworks*)

Permet à WinGate de fonctionner en tant que routeur et de transférer des données entre des sous-réseaux différents. Pour cela, WinGate doit avoir une interface sur chaque sous-réseau.

Si cette option est désactivée, l'icône [Routage \(Routing\)](#) ne s'affiche pas.

Activer le contrôle de la bande passante (*Enable Bandwidth Control*)

Affiche l'icône [Bande passante \(Bandwidth control\)](#).

Détecter les passerelles inactives (*Monitor for Dead Gateways*)

Si le service découvre qu'une passerelle est inactive, elle ne peut pas être sélectionnée. De plus, l'interface ne peut être utilisée en tant qu'interface externe pour un service de WinGate car elle n'est pas en mesure d'exécuter les requêtes des clients.

Lorsque cette option n'est pas cochée, toutes les interfaces possédant une passerelle peuvent être sélectionnées, quel que soit leur état.

[Cliquez ici pour en savoir plus sur les passerelles.](#)

Pare-feu

Désactiver le pare-feu (*Disable the WinGate Firewall*)

Désactive entièrement le pare-feu de WinGate : le serveur n'est plus protégé.

Bas (*Low*) : Permet aux serveurs de fonctionner avec le pare-feu. Autorise : les serveurs Telnet, web, FTP, SMTP, NNTP et POP3 ainsi que les connexions TCP & UDP sur les ports 1024 à 4096 et sur les interfaces internes.

Moyen (*Medium*) : Pour les jeux et applications Internet. Autorise : les connexions TCP & UDP sur les ports 1024 à 4096 et les connexions TCP & UDP sur les interfaces internes.

Haut (*High*) : Refuse toutes les connexions extérieures. Autorise : les connexions TCP & UDP sur les interfaces internes.

Personnalisé (*Custom*) : Pour les utilisateurs avancés.

Le mode personnalisé permet d'ajouter vos propres paramètres à l'un des autres modes. Pour cela, sélectionnez le mode souhaité (bas, moyen ou haut) puis sauvegardez les paramètres de GateKeeper. Sélectionnez ensuite **Personnalisé** et ajoutez des filtres dans la fenêtre Sécurité des ports (*Port security*).

(IMPORTANT : tous les paramètres personnalisés s'ajoutent à ceux du dernier mode choisi).

Service réseau avancé - Régulation de la bande passante

La régulation de la bande passante permet aux administrateurs système de limiter ou de hiérarchiser le flux de trafic des machines.

Lorsque le trafic atteint un certain seuil, cette fonctionnalité joue le rôle de "file d'attente" et retarde ou abandonne l'envoi de paquets provenant d'un client/destinés à un utilisateur spécifique.

Elle peut être appliquée à différents niveaux :

1. Au niveau de l'application

La régulation de la bande passante au niveau de l'application agit sur son protocole, par ex. : HTTP pour la navigation sur le web ou SMTP pour la distribution du courrier. Cela ne prend pas en compte les protocoles de niveau inférieur (comme les en-têtes de paquets) ni les relances/envois groupés, etc. , qui augmentent pourtant le trafic.

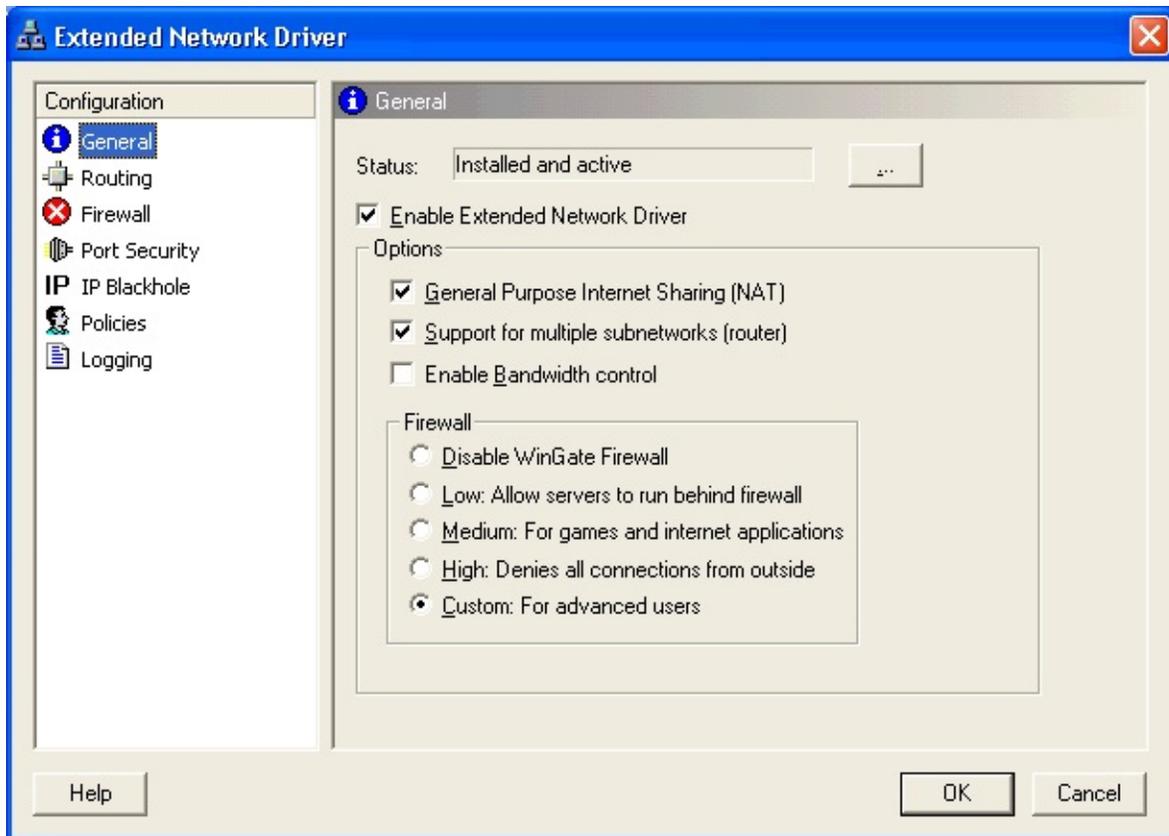
2. Au niveau des paquets

La régulation au niveau des paquets est plus flexible mais beaucoup plus complexe à appliquer et à contrôler. Ses règles sont établies en fonction de l'adresse IP de l'expéditeur/du destinataire, du numéro de port, du type de protocole, etc. Par défaut, toutes les relances ou multiplications de paquets sont prises en compte. Cependant, ce type de régulation entraîne souvent des changements soudains au niveau du trafic, pouvant être atténués en modifiant les caractéristiques des paquets.

WinGate utilise la régulation au niveau des paquets. Le pilote examine tous les paquets interceptés avant de décider si le paquet doit être retardé/mis en file d'attente ou distribué immédiatement.

Comment activer la régulation de la bande passante

Cette fonctionnalité s'active dans les propriétés du **Service réseau avancé (Extended network services)** (icône Général).

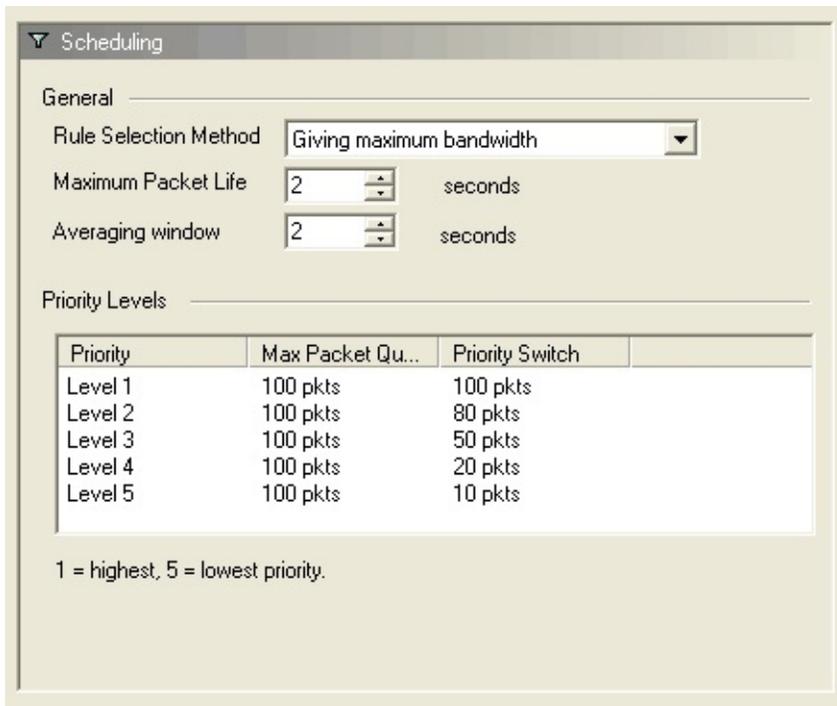


Masquer | Masquer toutes les images

Une fois l'option cochée, l'icône **Bande passante** (*Bandwidth control*) s'affiche.

Réglages

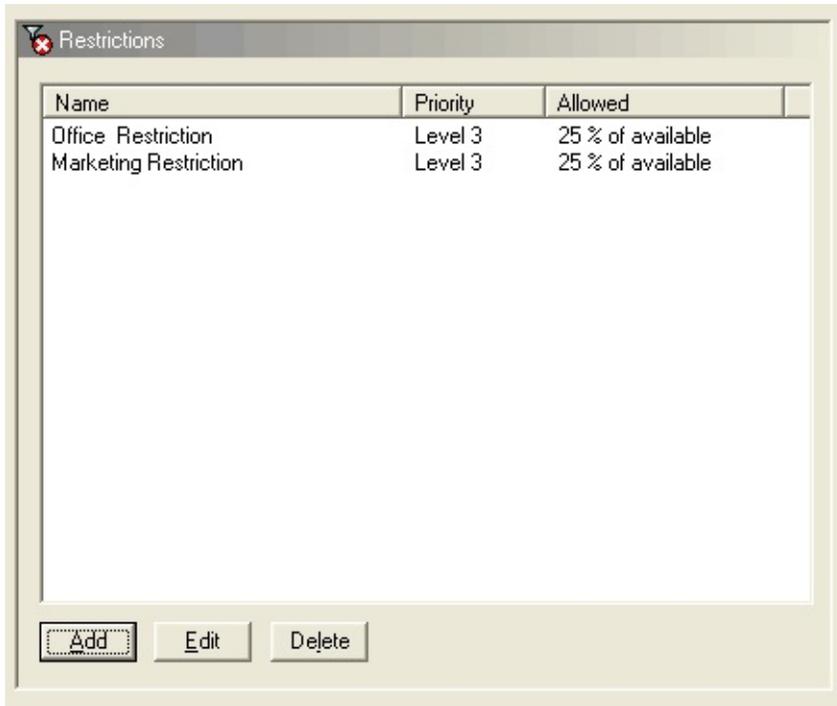
En cliquant sur l'icône **Réglages** (*Scheduling*) vous contrôlez la gestion de la bande passante lorsque plusieurs règles sont établies.



Masquer | Masquer toutes les images

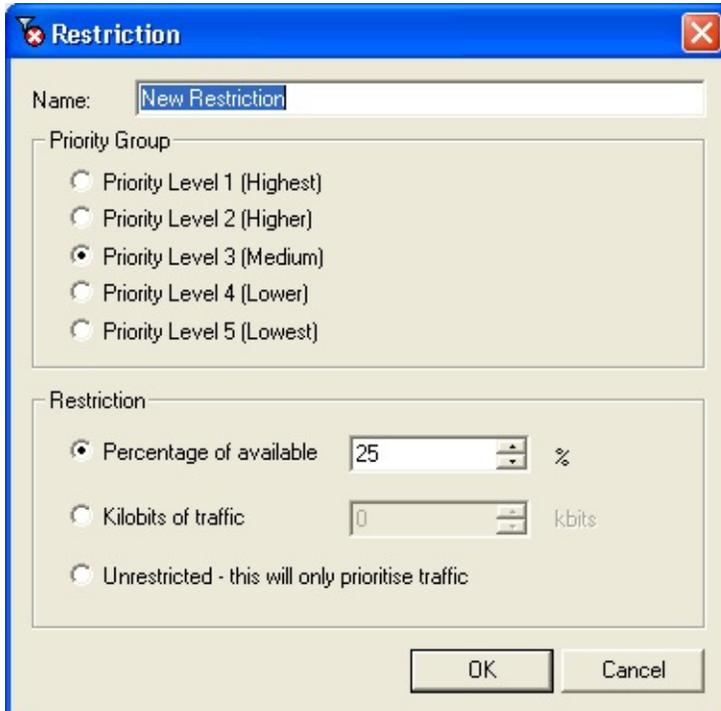
Restrictions

En cliquant sur l'icône **Restrictions** vous pouvez créer des règles de restriction pour certaines opérations et les hiérarchiser.



Masquer | Masquer toutes les images

Cliquez sur **Ajouter** pour créer une **nouvelle restriction**.



Masquer | Masquer toutes les images

Nom

Attribuez-lui un nom

Niveau de priorité

Indiquez son niveau de priorité par rapport aux autres règles.

Restriction

Définit la règle selon différents critères :

Pourcentage disponible (*Percentage of available*)

Pourcentage de bande passante disponible.

Kilobits (*Kilobits of traffic*)

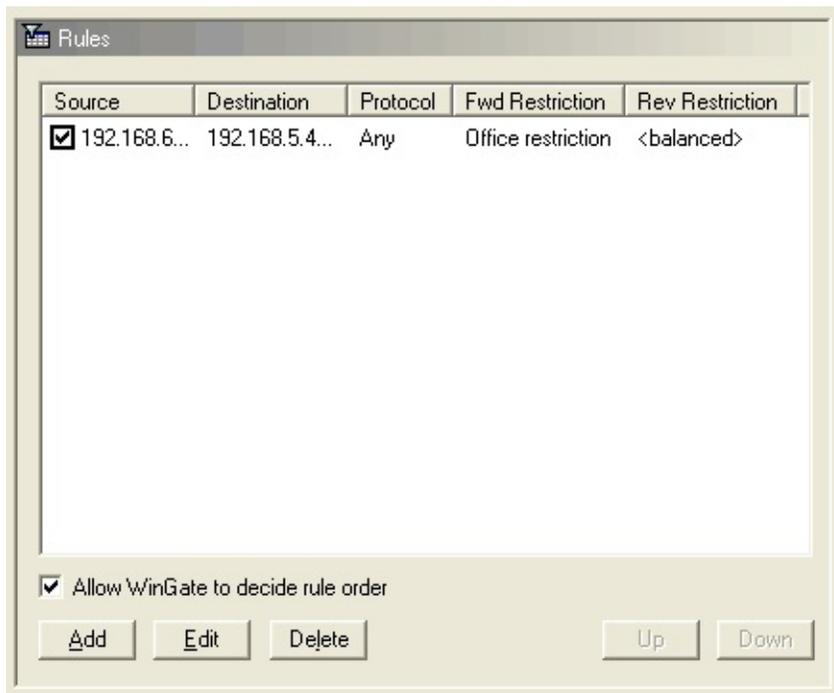
Restriction en fonction du nombre de kilobits.

Pas de restriction (*Unrestricted*)

Seul le trafic est hiérarchisé.

Règles

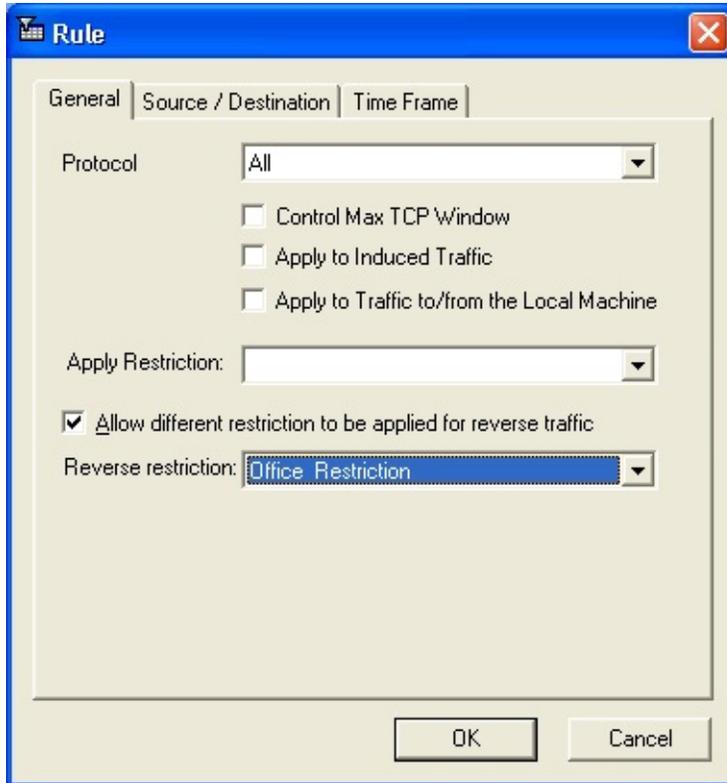
En cliquant sur l'icône **Règles**, vous pouvez créer les règles appliquées pour la restriction.



Masquer | Masquer toutes les images

Cliquez sur **Ajouter** pour créer une nouvelle règle.

Général



Masquer | Masquer toutes les images

Protocole

Les règles peuvent être établies en fonction du protocole : TCP, UDP ou les deux. De nombreuses options sont disponibles : taille maximum de la fenêtre TCP, application des règles au trafic induit (trafic secondaire pour les connexions TCP/UDP, par ex. : canaux de contrôle FTP).

Appliquer la restriction (*apply restriction*)

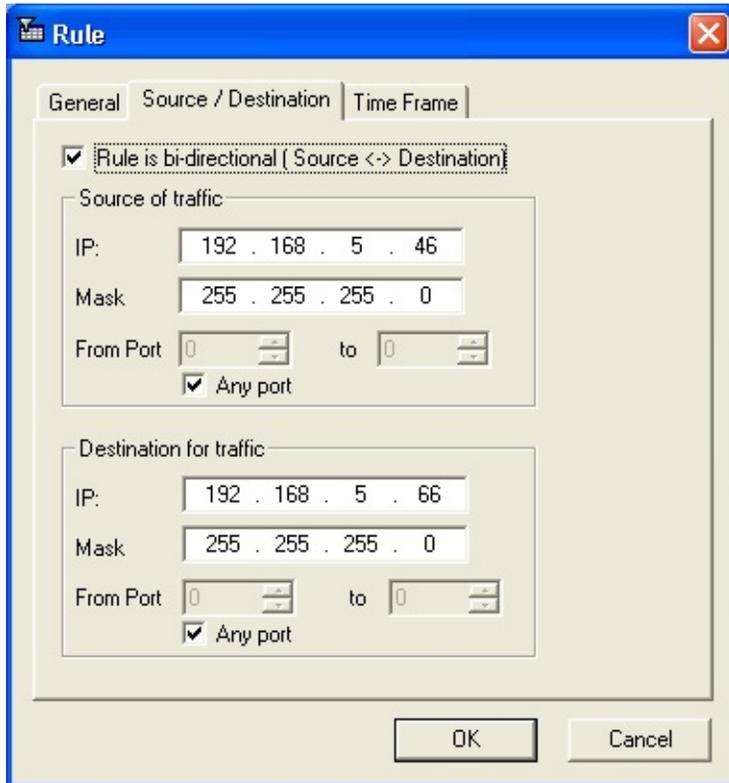
Applique une restriction (voir ci-dessus).

Appliquer une restriction pour le trafic inverse (*Allow different restriction to be applied for reverse traffic*)

Vous permet de choisir une restriction spécifique pour le trafic inverse

Source/Destinataire (*Source/Destination*)

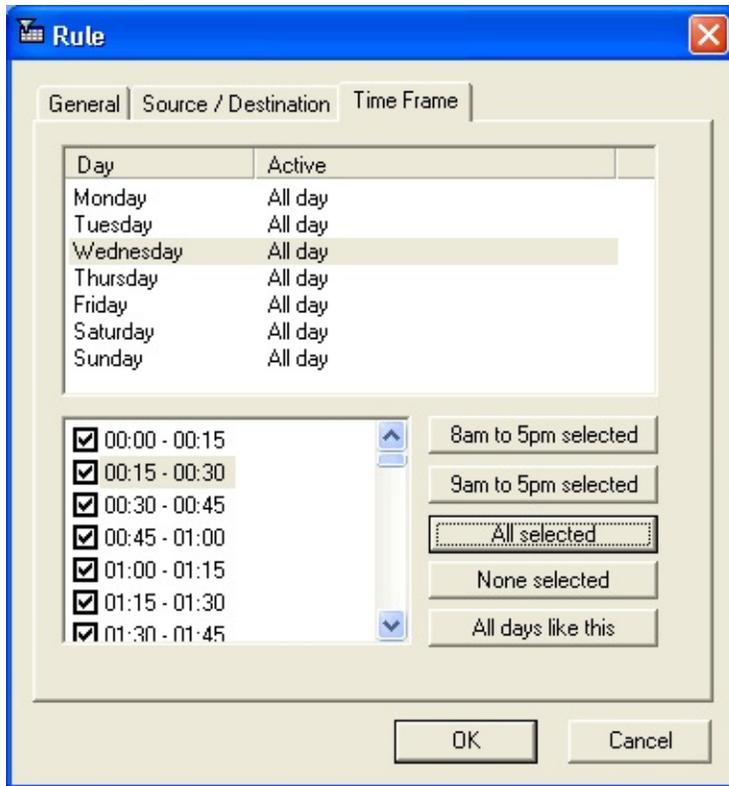
Indiquez ici les adresses IP sources et destinataires concernées par les règles.



[Close](#) | [Close all images](#)

Horaires (*Time frame*)

Diverses options vous permettent de configurer l'heure et la durée d'application des règles.



Masquer | Masquer toutes les images

Veillez noter que la régulation de la bande passante n'est disponible qu'avec WinGate 6 Pro et Enterprise

©2004 Qbik New Zealand Limited

Service réseau avancé - Pare-feu (*Extended network services - Firewall*)

A propos du pare-feu de WinGate

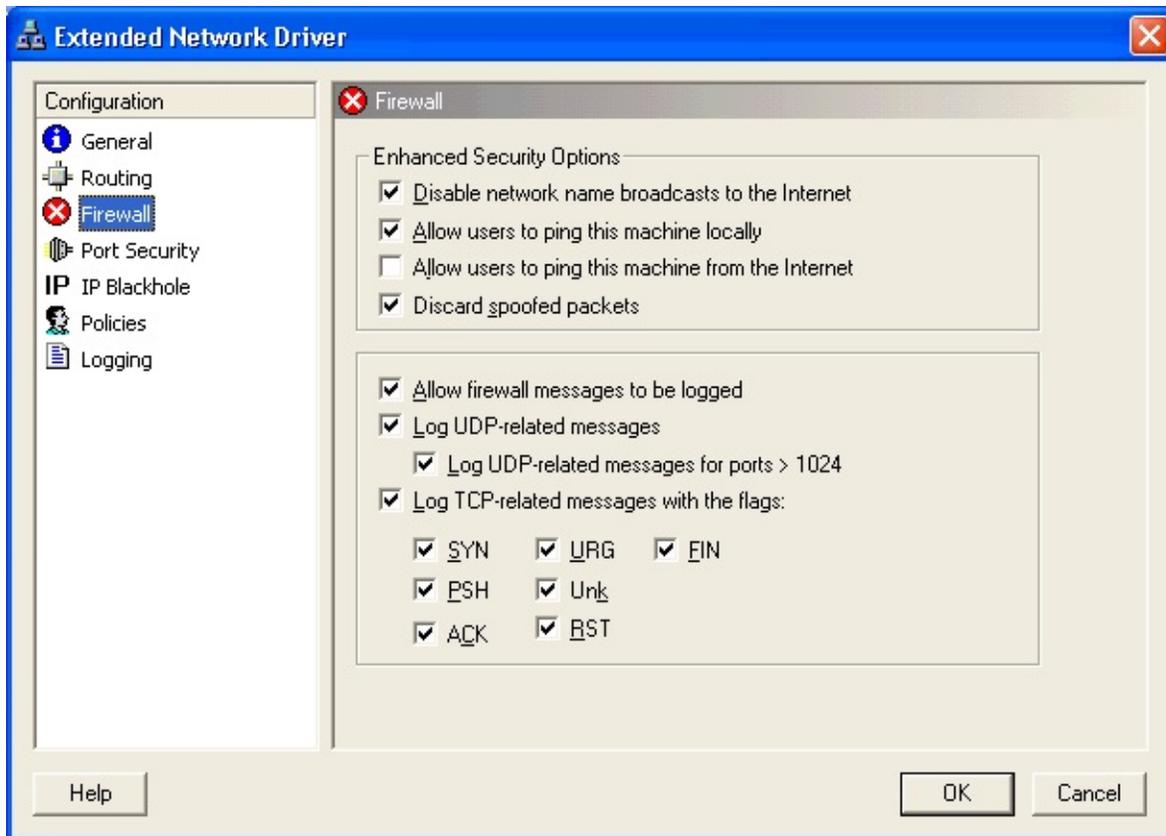
Il s'agit d'une solution qui intervient au niveau des paquets, bien plus performante que le pare-feu proxy des versions précédentes. Cette fonctionnalité assure de façon efficace la protection de votre ordinateur passerelle (ainsi que de tout votre réseau) contre les attaques extérieures. Les mesures de sécurité sont appliquées là où elles sont vraiment nécessaires : au niveau de la couche réseau.

Ainsi, tous les services, applications et fichiers qui se trouvent derrière le pare-feu sont protégés. De plus, il s'intègre de façon "transparente" dans n'importe quel environnement. Toutes les données TCP et UDP sont rigoureusement analysées avant de pouvoir atteindre la pile de protocoles, puis vos applications et données.

Ses principales fonctionnalités sont :

1. **Options de sécurité avancées.** Fournissent la sécurité et la protection de base et peuvent être activées ou désactivées individuellement. Une fonctionnalité intégrée par défaut fonctionne en permanence et protège votre ordinateur contre les principales attaques.
2. **Filtrage avancé au niveau des paquets.** Les paquets peuvent être filtrés en fonction du protocole, de l'interface et du port ; puis autorisés, refusés ou redirigés vers un autre ordinateur (voir [Sécurité des ports](#)).
3. **Journalisation des intrusions.** Vous êtes immédiatement averti des tentatives d'intrusion ou des activités suspectes grâce à un message système (voir [Sécurité des ports](#)).

Le **pare-feu** dispose de nombreuses options :



Masquer

Options de sécurité avancée (*Enhanced Security Options*)

Désactiver la diffusion du nom Netbios sur Internet (*Disable network name broadcasts to the Internet*)

Empêche la diffusion du nom Netbios du poste WinGate sur une interface externe et sur Internet.

Autoriser les utilisateurs à envoyer un Ping en local (*Allow users to ping this machine locally*)

Autorise les utilisateurs du réseau local à effectuer une requête Ping sur le serveur WinGate (pour tester la connectivité des postes par exemple).

Autoriser les utilisateurs à envoyer un Ping depuis Internet (*Allow users to ping this machine from the Internet*)

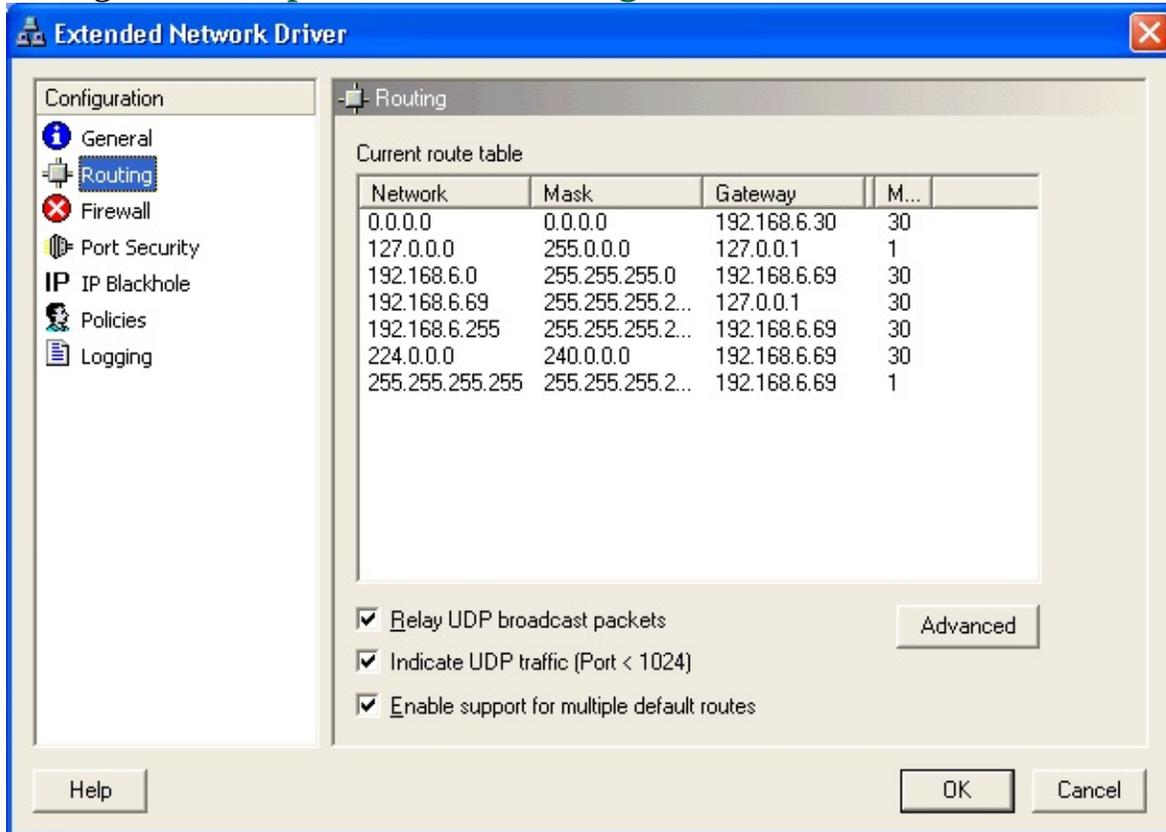
Autorise les utilisateurs sur Internet à effectuer une requête Ping sur le serveur WinGate. Pour des raisons de sécurité, cette option n'est pas cochée par défaut.

Ignorer les paquets usurpés (*Discard spoofed packets*)

Lorsque cette option est activée, WinGate vérifie que l'adresse IP source indiquée dans l'en-tête des paquets correspond bien au poste ayant émis la requête. Si elle est différente, les paquets seront ignorés.

Service réseau avancé - Routage (*Routing*)

Configurez ici les **paramètres de routage**.



Masquer

Acheminer les paquets de diffusion UDP (*Relay UDP broadcast packets*)

Cette option indique si le serveur WinGate doit acheminer les paquets de diffusion UDP entre les sous-réseaux. Si elle est désactivée, il est impossible d'explorer un ordinateur situé sur un sous-réseau différent.

Ces paquets sont généralement utilisés afin de :

Fournir aux ordinateurs du sous-réseau des informations concernant votre poste lors du démarrage (nom Netbios, adresse IP, système d'exploitation et principaux services).

S'informer sur les autres ordinateurs du réseau (par exemple, déterminer où se

trouve le contrôleur de domaine principal ou le serveur DHCP).

Nous vous recommandons de ne pas désactiver cette option.

Indiquer le trafic UDP (ports < 1024) (*Indicate UDP Traffic (Port < 1024)*)

Par défaut, le service NAT informe le moteur de WinGate du trafic UDP sur les ports inférieurs à 1024 dès qu'il se produit. Ce trafic n'est indiqué que s'il reste actif pendant une certaine période (20 secondes avec au moins 10 secondes depuis la dernière activité).

Lorsque le volume de trafic UDP du NAT (par ex. : redirections DNS) est important, cela peut augmenter la taille de la mémoire utilisée. Cette option vous permet donc de décider si les sessions UDP sur les ports 1024 et inférieurs seront répertoriées.

Même si cette option est cochée, le trafic UDP ne sera indiqué que s'il s'agit d'une [redirection transparente](#) ou si le trafic est actif pendant une certaine période (cela concerne tous les ports).

Autoriser plusieurs routages par défaut (*Enable support for multiple default routes*)

Lors d'une connexion commutée, une autre passerelle par défaut est ajoutée au routeur. Elle possède un ordre de priorité supérieur à la passerelle normale, ce qui entraîne des problèmes pour le routage entre plusieurs sous-réseaux. En effet, les paquets adressés à un sous-réseau sont envoyés à la passerelle possédant le plus haut niveau de priorité (c'est à dire l'adaptateur connecté à Internet).

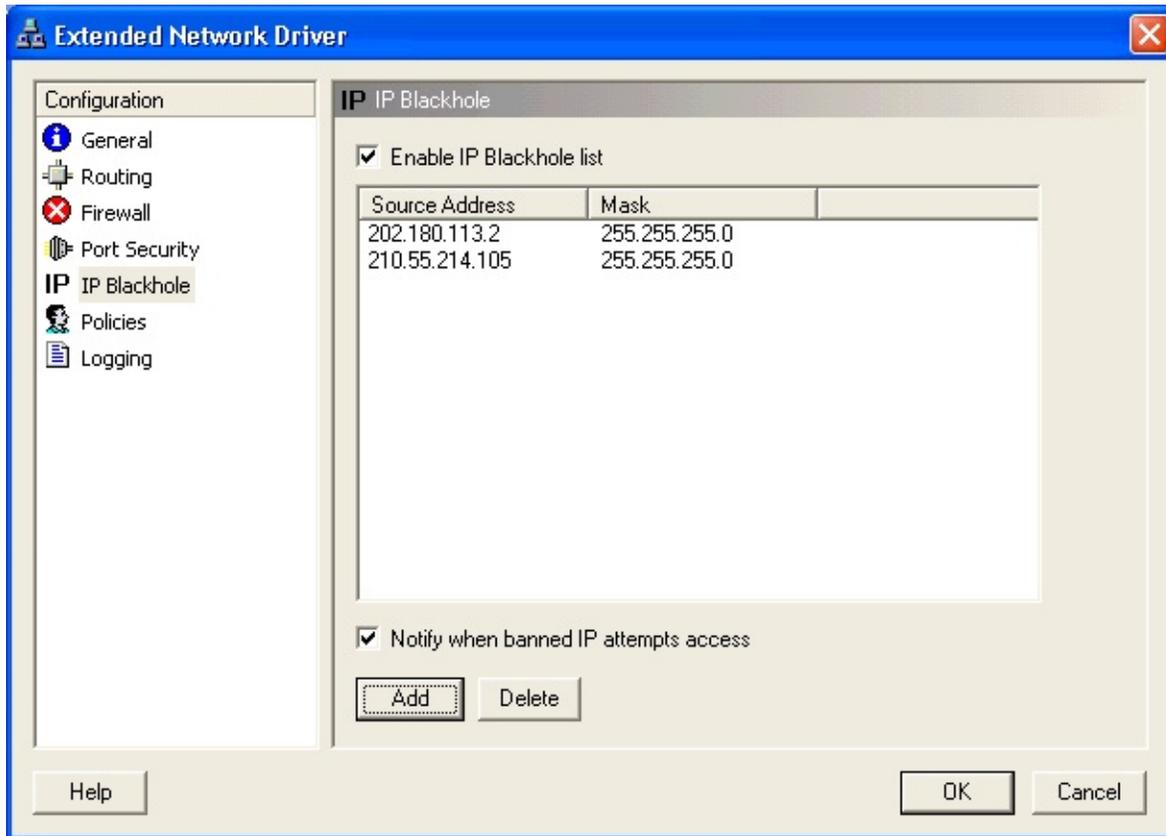
Si cette option est activée, WinGate intercepte les paquets envoyés d'un sous-réseau à l'autre et les renvoie vers la passerelle d'origine, afin qu'ils puissent être correctement transférés. Par conséquent, lorsque l'option est désactivée, le routage entre des sous-réseaux risque de ne pas fonctionner si l'ordinateur passerelle utilise une connexion commutée pour accéder à Internet.

En cliquant sur **Avancé (*Advanced*)**, vous pouvez configurer les [Paramètres avancés des ports de diffusion](#) et choisir quels ports seront utilisés pour les diffusions UDP sur le réseau local.

©2004 Qbik New Zealand Limited

Service réseau avancé - Liste noire IP (*IP Blackhole*)

La **liste noire** permet d'empêcher certaines IP d'accéder à votre réseau.



Masquer

Vous disposez pour cela de deux méthodes :

Cliquez sur **Ajouter** dans l'option "Liste noire IP" puis saisissez l'adresse et cliquez sur **OK**.

Vous avez également la possibilité de supprimer une adresse de cette liste.

Mettre une plage d'adresses en liste noire

Exemple : si vous indiquez une adresse et un masque terminant par un "0", l'accès est refusé à tous les ordinateurs se trouvant sur le même sous-réseau.

Remarque :

Assurez-vous que l'option **Activer la liste noire** (*Enable IP Blackhole list*) soit cochée. Dans le cas contraire, les adresses mises en liste noire pourront toujours accéder à votre réseau.

Dans les onglets **Activité** ou **Historique** effectuez un clic droit sur une adresse et sélectionnez "Mettre l'IP xxx en liste noire" pour ajouter cette adresse à la liste. (Il s'agit de la méthode la plus couramment utilisée)

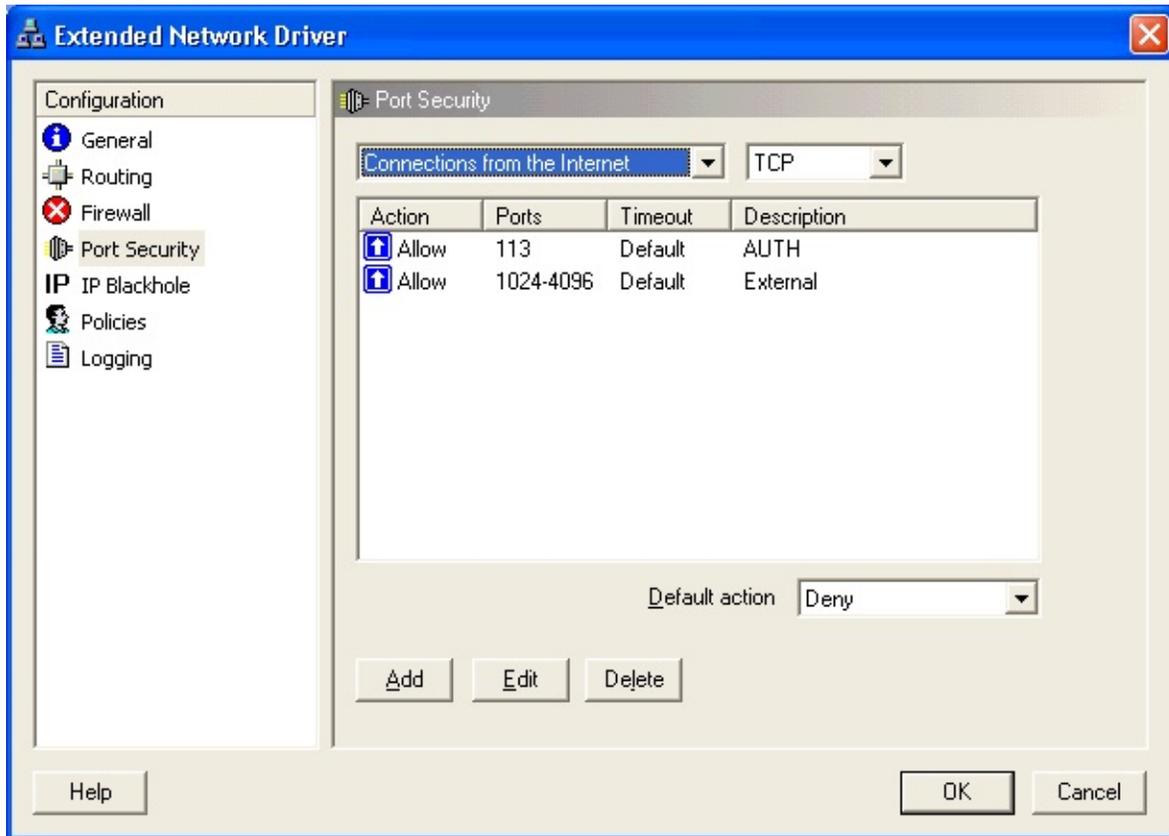
Remarque :

Avec la deuxième méthode, assurez-vous que l'adresse sélectionnée ne fait pas partie de votre réseau.

©2004 Qbik New Zealand Limited

Service réseau avancé - Sécurité des ports (*Port Security*)

Configurez ici les paramètres de sécurité des ports du pare-feu de WinGate.



Masquer

Il s'agit des propriétés avancées du pare-feu. Les utilisateurs peuvent configurer une action par défaut.

Cela signifie qu'il est possible de définir une "action" s'appliquant à tous les paquets pour une combinaison spécifique interface/protocole (voir ci-dessous).

Vous pouvez également paramétrer des filtres de sécurité afin de contrôler certains intervalles de ports.

Les paquets correspondant aux critères définis seront autorisés, refusés ou redirigés (selon votre choix).

Action(s) par défaut

Pour une protection optimale, nous vous recommandons d'utiliser les paramètres par défaut (ci-dessous).

Interface	Protocole	Action par défaut
Connexions provenant d'Internet (externe -> interne) (<i>Connections from the Internet</i>)	TCP	Refuser (<i>Deny</i>)
	UDP	Refuser
Connexions LAN à l'ordinateur WinGate (interne -> interne) (<i>LAN connections to WinGate PC</i>)	TCP	Autoriser (<i>Allow</i>)
	UDP	Autoriser
Connexions LAN à Internet (interne - > externe) (<i>LAN connections to Internet</i>)	TCP	Autoriser
	UDP	Autoriser

En cliquant sur **Ajouter (Add)**, vous avez également la possibilité de créer des "trous" dans le pare-feu ou de rediriger les paquets (à l'aide des filtres de sécurité) afin de répondre aux besoins de votre LAN.

Remarque :

Lorsque le pare-feu est activé, l'administrateur doit ouvrir/fermer manuellement certains intervalles de ports afin d'assurer le fonctionnement des serveurs présents sur le LAN.

Le pare-feu assure une protection optimale contre les attaques provenant d'Internet (car tous les paquets destinés au LAN sont analysés au niveau de l'interface externe).

Il apporte une excellente flexibilité aux utilisateurs Internet de votre LAN (car tous les paquets sortants sont autorisés).

Avec la liste noire IP, vous pouvez également refuser des IP spécifiques.

Filtres de sécurité

([Cliquez ici pour en savoir plus sur la création de filtres de sécurité](#))

Avec les filtres de sécurité, votre pare-feu est mieux contrôlé et plus flexible, sans pour autant compromettre la sécurité de votre réseau. Les administrateurs peuvent ainsi :

Créer des **trous** dans le pare-feu afin que les utilisateurs sur Internet puissent accéder aux serveurs de votre LAN. Remarque : lorsqu'un service de WinGate est lié à une combinaison interface/port bloquée par le pare-feu, WinGate vous propose de créer un "trou" (il est recommandé d'accepter). Dès la suppression du service ou de la liaison, ce "trou" sera évidemment à nouveau bloqué automatiquement.

Refuser les paquets sur certains ports ou intervalles (cette action ferme les ports). Par défaut, tous les ports non utilisés sont masqués.

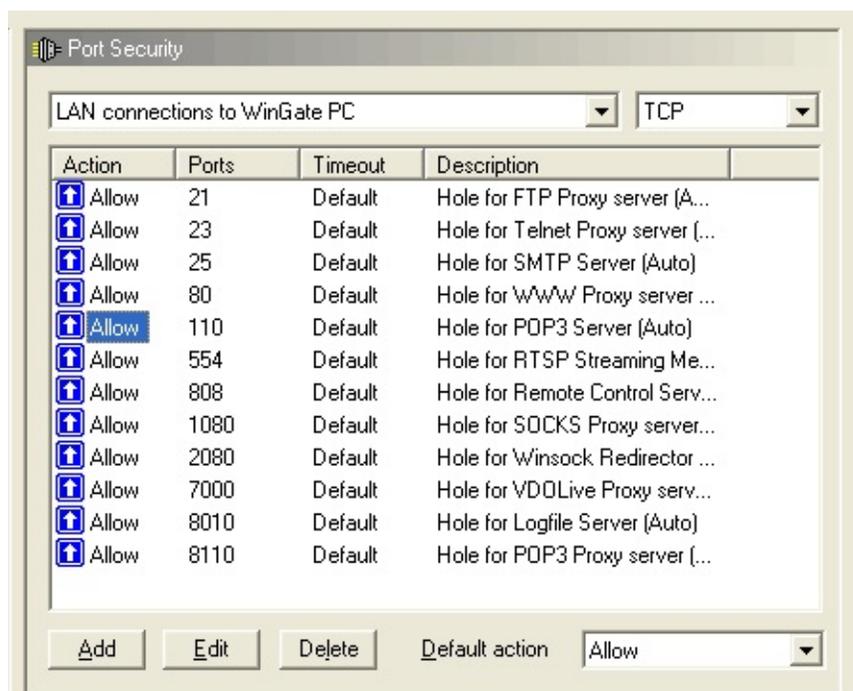
Rediriger les paquets vers un autre ordinateur, qu'il soit derrière le pare-feu ou pas.

Configuration automatique des ports

Si vous utilisez les ports configurés par défaut pour chaque service (comme le port 80 pour le service proxy web (*WWW service*), port 21 pour le proxy FTP, etc.), vous disposez d'options permettant d'en ajuster les paramètres pour le pare-feu.

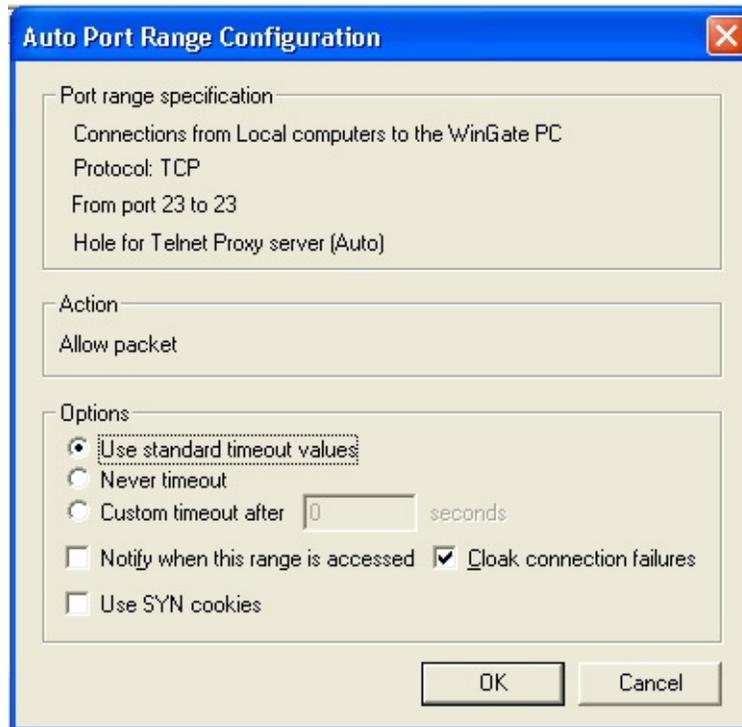
Pour cela :

1. Cliquez sur **Sécurité des ports (*Port Security*)** dans les propriétés du service ENS et sélectionnez **Connexions LAN au poste WinGate (*LAN connections to the WinGate PC*)** dans le menu déroulant du haut.



Masquer | Masquer toutes les images

2. Double-cliquez sur l'entrée que souhaitez configurer, ou bien sélectionnez-la et cliquez sur **Modifier (*Edit*)**.



Masquer | Masquer toutes les images

Diverses options sont disponibles : configuration de délais de déconnexion, notifications lorsque le port est utilisé et cookies SYN.

Remarque :

Pour en savoir plus sur ces options, consultez l'article sur la [création de filtres de sécurité](#).

Diffusion UDP - Avancé

Cette fonctionnalité est disponible en cliquant sur [Routage \(Routing\)](#), puis **Avancé (Advanced)** dans les propriétés du service ENS.

Masquer | Masquer toutes les images

Vous pouvez choisir les ports utilisés pour les diffusions UDP sur le réseau local. Par défaut, les ports 137 et 138 sont activés pour la diffusion Netbios.

Même si cette fonctionnalité est destinée à faciliter la diffusion UDP sur des réseaux étendus avec WinGate VPN, elle peut également être utilisée pour le service DHCP et les jeux en réseau (sur un réseau local).

Pour ajouter un port de diffusion UDP :

1. Cliquez sur l'icône **Routage (Routing)** dans les propriétés du service ENS.
2. Cliquez sur **Avancé (Advanced)** puis sur **Ajouter (Add)** dans la fenêtre qui s'ouvre ensuite.
3. Indiquez le numéro du port et sa description.
4. Assurez-vous que la case **Activé (Enabled)** soit cochée, puis cliquez sur **OK**.

Ce port doit alors figurer dans la liste.

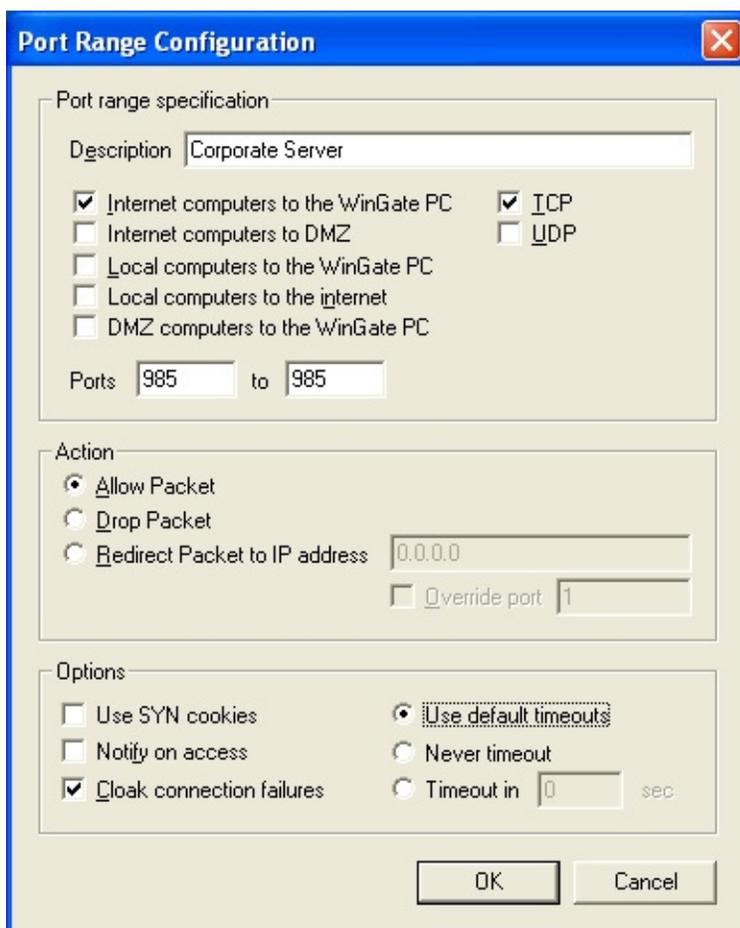
©2005 Qbik New Zealand Limited

Service réseau avancé (ENS) - Création de filtres de sécurité

Il n'est pas nécessaire de configurer des filtres de sécurité pour que WinGate gère toutes les requêtes Internet des clients. Il ouvre les ports nécessaires et les referme une fois la connexion terminée.

Cependant, lorsque qu'un utilisateur distant envoie une requête sur votre réseau (par exemple sur serveur web installé derrière WinGate), vous devez créer des filtres afin qu'elles soient acceptées par le pare-feu de WinGate. En effet, toutes les connexions entrantes sont bloquées par défaut.

Pour créer des filtres, cliquez sur **Sécurité des ports (Port Security)**, puis sur **Ajouter (Add)**



The screenshot shows the "Port Range Configuration" dialog box. It is divided into three main sections: "Port range specification", "Action", and "Options".

- Port range specification:** The "Description" field contains "Corporate Server". There are six checkboxes for traffic types: "Internet computers to the WinGate PC" (checked), "Internet computers to DMZ" (unchecked), "Local computers to the WinGate PC" (unchecked), "Local computers to the internet" (unchecked), "DMZ computers to the WinGate PC" (unchecked), "ICP" (checked), and "UDP" (unchecked). The "Ports" field is set to "985" to "985".
- Action:** The "Allow Packet" radio button is selected. Other options are "Drop Packet" and "Redirect Packet to IP address" (with a text box containing "0.0.0.0"). There is also an "Override port" checkbox with a text box containing "1".
- Options:** There are four checkboxes: "Use SYN cookies" (unchecked), "Notify on access" (unchecked), "Cloak connection failures" (checked), "Use default timeouts" (selected), "Never timeout" (unchecked), and "Timeout in" (with a text box containing "0" and "sec" next to it).

At the bottom of the dialog are "OK" and "Cancel" buttons.

Masquer

Intervalle de ports (*Port range specification*)

Connexions Internet au poste WinGate (*Internet connections to the WinGate PC*)

S'applique si un paquet provenant d'une connexion inconnue est reçu sur une interface externe. Cette option s'utilise pour les connexions entrantes (provenant d'Internet).

Connexions Internet sur une DMZ (*Internet computers to DMZ*)

S'applique aux paquets reçus sur une interface externe du serveur WinGate et destinés à un adaptateur en DMZ (Demilitarized Zone).

Connexions locales au poste WinGate (*Local computers to WinGate PC*)

S'applique aux paquets reçus sur une interface interne du serveur et destinés à l'adresse IP interne du poste WinGate.

Connexions locales vers Internet (*Local Computers to the Internet*)

S'applique aux paquets reçus sur une interface interne ou DMZ du serveur mais destinés à une interface externe ou DMZ.

Connexions DMZ au poste WinGate (*DMZ Computers to the WinGate PC*)

S'applique aux paquets envoyés par des postes connectés à un adaptateur en DMZ et destinés à l'adresse IP interne du poste WinGate..

Critère	Description
---------	-------------

Protocole	TCP ou UDP
Port	Port sur lequel le paquet est reçu (indiquez un numéro de port ou un intervalle)

Actions

Action	Description
Autoriser (<i>Allow</i>)	Le paquet est "autorisé" à passer la pile TCP/IP.
Refuser (<i>Deny</i>)	Le paquet est refusé à l'entrée du réseau. Cette action équivaut à fermer/désactiver le port
Rediriger (<i>Redirect</i>)	Le paquet est redirigé vers un autre ordinateur ou port. (Fonctionne de la même façon que les liens mappés de WinGate mais à un niveau inférieur)

Options

Utiliser des cookies Syn (*Use Syn cookies*)

Ils permettent à WinGate de contrôler une session de paquets avant même qu'ils ne soient autorisés à entrer sur le port, en conservant une trace des requêtes ACK valides provenant d'un hôte sur Internet. Cela évite que des faux paquets (utilisés pour des attaques appelées SynFlood) ne pénètrent dans WinGate.

Par défaut, cette option n'est pas cochée afin d'optimiser la compatibilité entre les sessions. Ne l'utilisez que si vous possédez suffisamment de connaissances sur les mécanismes des sessions TCP.

Afficher les tentatives de connexion (*Notify when this range is accessed*)

Affiche dans l'onglet **Pare-feu (*Firewall*)** les tentatives de connexion sur l'interface indiquée.

Masquer les connexions échouées (*Cloak connection failures*)

Cette option est cochée par défaut. Ainsi, lorsqu'un pirate recherche des ports vulnérables sur le serveur WinGate, le statut des ports est masqué. Par conséquent, ils ne sont pas détectés par l'analyseur.

Remarque :

Lorsqu'un port (ou un intervalle) est ouvert, WinGate dirige les paquets acceptés sur le port correspondant pour qu'il soient traités par la pile TCP/IP puis transmis au système d'exploitation ou à l'application concernée. Or, le système d'exploitation répond systématiquement aux requêtes de connexion, même si aucune application n'écoute le port. Dans ce cas, il renvoie un paquet TCP RST (connexion refusée).

Si le système d'exploitation envoie un paquet TCP RST et que l'option ci-dessus est activée, WinGate intercepte le paquet et l'abandonne.

Ainsi, si vous ouvrez un intervalle de ports qui n'est écouté par aucune application les tentatives d'analyse ne recevront aucune réponse.

Cependant, si une application écoute les ports ouverts, les utilisateurs pourront s'y connecter normalement.

Utiliser les délais d'expiration par défaut (*Use default timeouts*)

Cette option est cochée par défaut et en règle générale, il n'est pas nécessaire de la modifier. Dans tous les cas, il est recommandé de ne pas activer l'option **La session n'expire jamais (*Never timeout*)** car cela peut s'avérer dangereux.

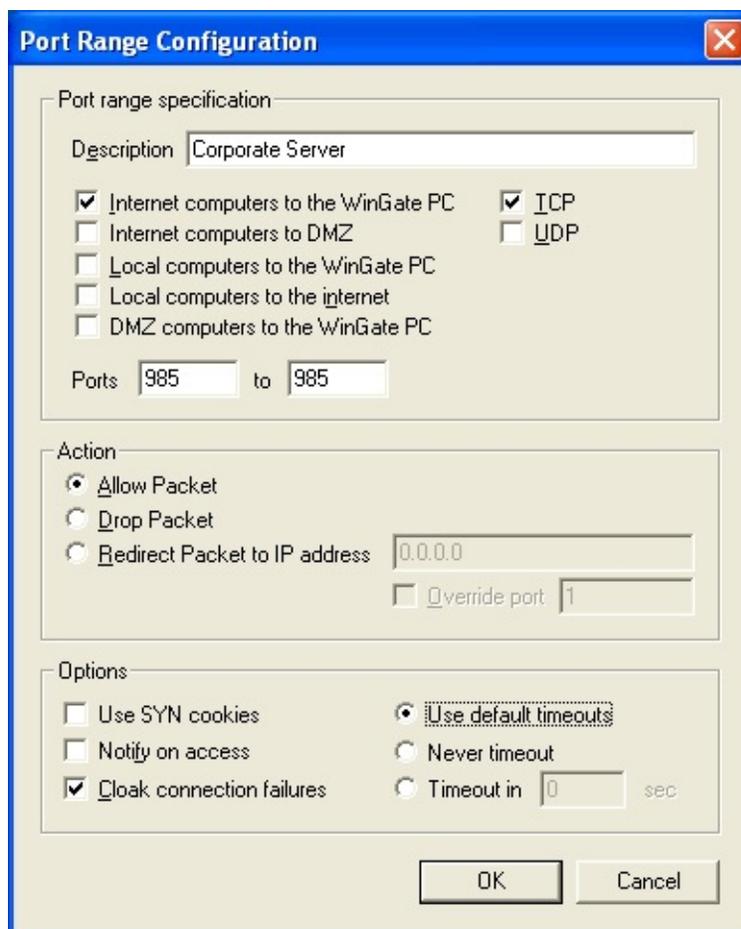
Remarque :

Lorsqu'un service de WinGate est lié à une combinaison interface/port bloquée par le pare-feu, WinGate vous propose de créer un "trou" (il est recommandé d'accepter). Dès la suppression du service ou de la liaison, ce "trou" sera

évidemment à nouveau bloqué automatiquement.

Création d'un filtre de sécurité :

1. Ouvrez **GateKeeper**.
2. Cliquez sur **Sécurité des ports (Port security)** dans les propriétés du service ENS.
3. Cliquez sur **Ajouter (Add)**



Masquer

4. Dans la fenêtre qui s'ouvre ensuite, indiquez la description du filtre afin de pouvoir l'identifier plus facilement.
5. Indiquez à quel(s) type(s) de connexion s'applique le filtre, ainsi que le protocole (TCP ou UDP).

6. Indiquez le **port** (ou l'intervalle).
7. Sélectionnez l'action à effectuer lorsqu'un paquet utilise le port spécifié : **autoriser**, **abandonner**, ou **rediriger** vers une autre adresse IP (par exemple si vous possédez un serveur web derrière WinGate).
8. Cliquez sur **OK**.

Résolution DNS/WINS - DNS (*DNS/Wins Resolver - DNS*)

Avec **cette fonctionnalité**, vous avez la possibilité de choisir les serveurs utilisés par WinGate pour la résolution de noms de domaine (DNS).

Masquer

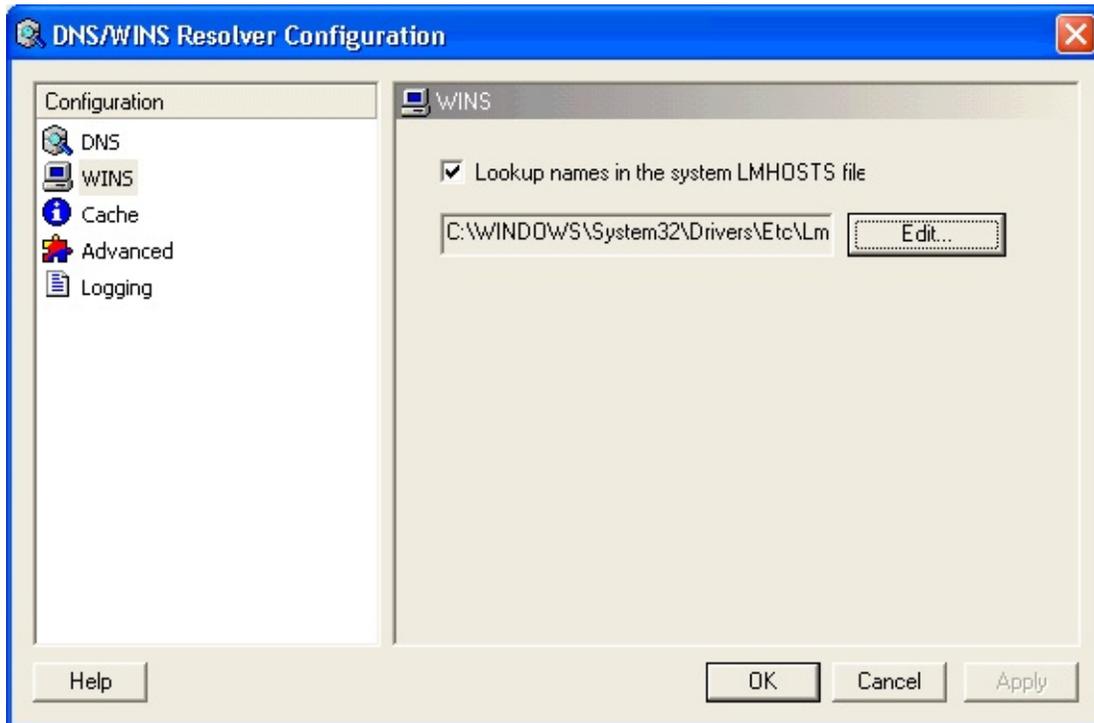
Sélectionnez-les à l'aide des boutons **Ajouter (Add)** et **Supprimer (Delete)**.

Vérifier les noms dans le fichier système HOSTS (*Lookup names in the system HOST file*)

Cochez cette option si vous souhaitez effectuer les résolutions dans un fichier hôte contenu dans un répertoire de votre ordinateur (par exemple : C:\WINDOWS\Hosts). Cliquez sur **Modifier (Edit)** pour changer de répertoire.

Résolution DNS/WINS - WINS (*DNS/Wins Resolver - Wins*)

Cette fonctionnalité permet à WinGate d'utiliser le fichier LMHosts lors de la conversion des noms Netbios en adresses IP.



Masquer

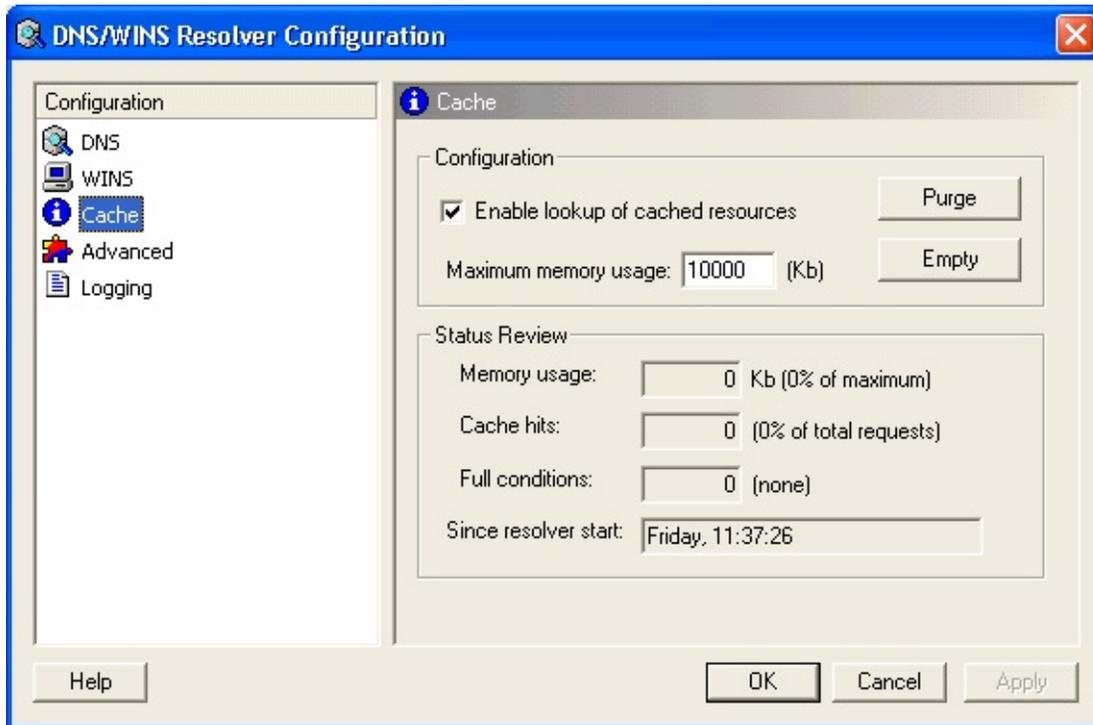
Vérifier les noms dans le fichier LMHOSTS (*Lookup names in the system LMHOSTS file*)

Cochez cette case pour effectuer la résolution des noms Netbios dans un fichier hôte contenu dans un répertoire de votre ordinateur (par exemple : C:\WINDOWS\LMhosts).

Cliquez sur **Modifier** pour changer de répertoire.

Résolution DNS/WINS - Cache

Configurez ici les options de cache DNS.



Masquer

Configuration

Autoriser la vérification des données en cache (*Enable lookup of cached resources*)

Cochez cette option pour activer la fonction de cache du service DNS.

Taille maximum de la mémoire (*Maximum memory usage*)

Détermine la quantité maximum d'informations pouvant être mises en cache avant d'être supprimées. Par défaut : 10000 Ko (ou 10 Mo).

Supprimer (*Purge*)

Supprime des données du cache afin de ne pas dépasser la taille maximum autorisée.

Vider (*Empty*)

Supprime la totalité des données.

Mémoire utilisée (*Memory usage*)

Quantité de mémoire utilisée par le cache DNS.

Requêtes cache (*Cache hits*)

Nombre exact de requêtes DNS utilisant le cache.

Mémoire pleine (*Full conditions*)

Nombre de fois où la mémoire cache a été pleine au cours de la session.

Démarrage session (*Since resolver start*)

Date et heure à laquelle la session de résolution DNS a démarré.

Résolution DNS/WINS - Avancé (*DNS/Wins Resolver - Advanced*)

[Cliquez ici pour une copie d'écran](#)

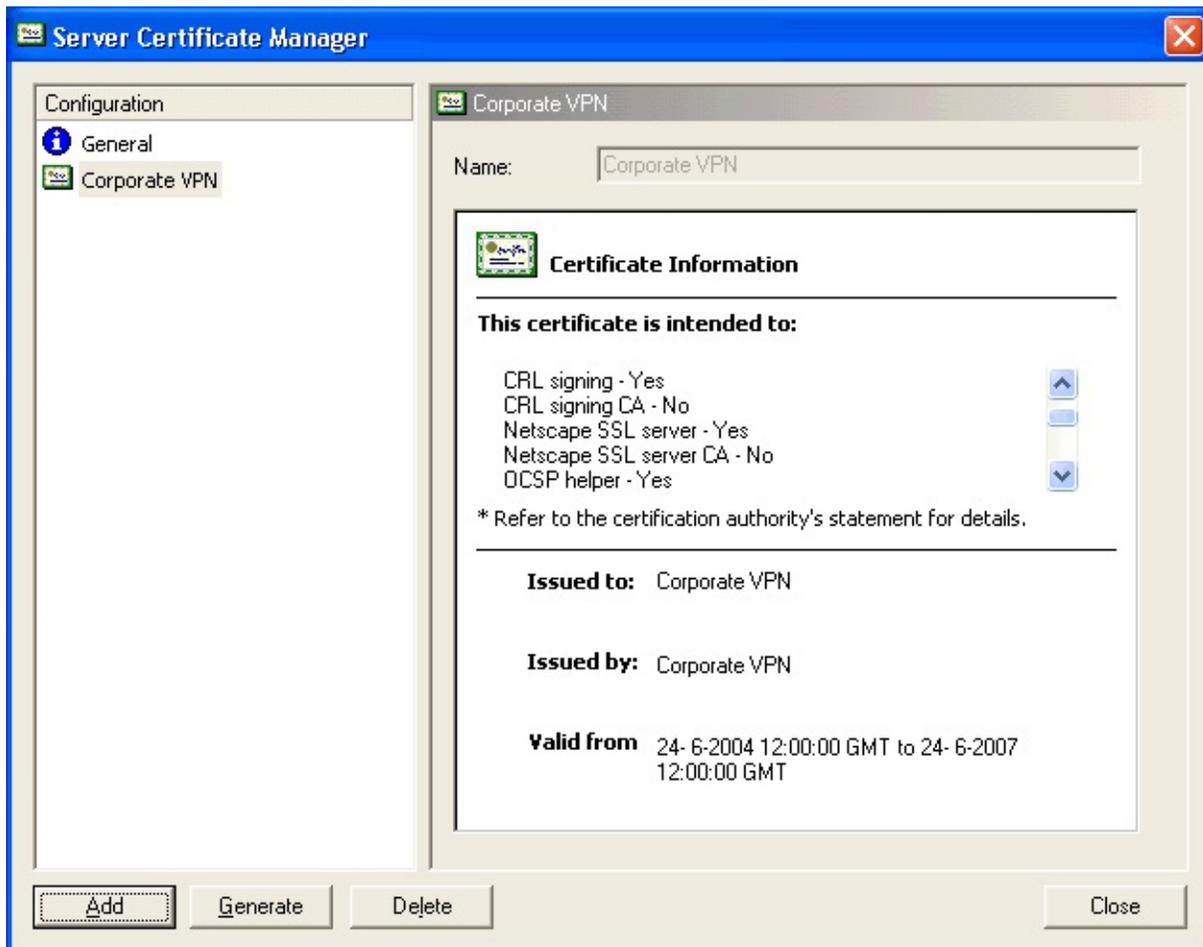
Masquer

Ajouter le domaine DHCP aux noms de label uniques (*Add DHCP domain to single label names*)

Cochez cette option si vous souhaitez créer des adresses e-mail n'ayant qu'un seul nom (par exemple @mail), ou si votre FAI a attribué un domaine DNS par défaut à votre serveur via le DHCP (par exemple : modems ATT&T;).

Certificats du serveur

WinGate enregistre tous vos **Certificats X509** au même emplacement, dans le **gestionnaire de certificats (Server certificate manager)**.



Masquer

Les certificats sont utilisés pour les connexions TLS ou SSL et avec WinGate VPN. Ils permettent de garantir l'identité de votre serveur WinGate aux ordinateurs qui s'y connectent.

Dans le cas d'une connexion VPN, le certificat identifie uniquement **l'hôte VPN**, et les clients peuvent le vérifier avant de se connecter au serveur. Cela permet de se protéger des attaques de type "man in the middle".

Pour le **Serveur de messagerie** le certificat permet de sécuriser les connexions entre le client et le serveur. Attention : la plupart des clients n'acceptent pas que le nom mentionné dans le certificat soit différent de celui du serveur.

Si vous mettez WinGate à jour, et que vous possédez déjà des certificats pour vos VPN ou votre serveur de messagerie, la migration s'effectue automatiquement.

[Cliquez ici pour en savoir plus sur la création de certificats](#)

Remarque :

Les liaisons SSL ne sont disponibles qu'avec WinGate Enterprise, à partir de la version 6.0.

Création de certificats

1. Ouvrez **GateKeeper**.
2. Ouvrez le **Gestionnaire de certificats** (onglet **Systeme** du panneau Contrôle).
3. Cliquez sur **Ajouter**.



Masquer | Masquer toutes les images

4. Indiquez le nom du certificat (afin de pouvoir l'identifier plus facilement).
5. Cliquez sur **Générer (Generate)**. Ce bouton n'est disponible qu'après

avoir choisi un nom.

Details of the Certificate

Name or Server: Corporate VPN CN

Email Address: Corporate@Corp.com

Department: Sales OU

Company: Corporation Ltd ON

City: Auckland L

State / Province: ST

Country: New Zealand C

Certificate Expires: 25/06/2007

Encrypt Certificate (Optional)

< Back Next > Cancel Help

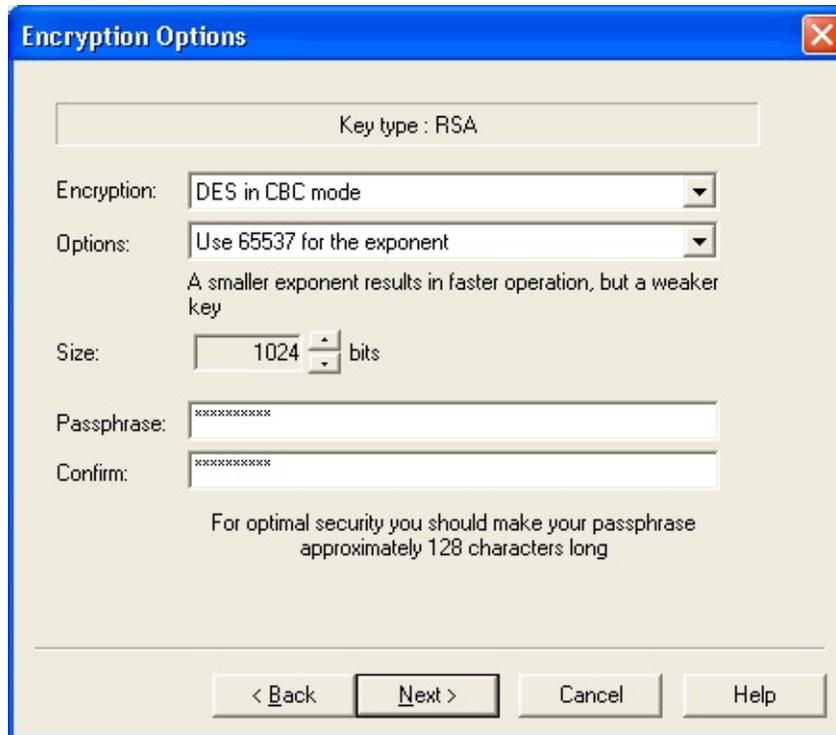
Masquer | Masquer toutes les images

Champ	Requis
Nom ou serveur (<i>Name or Server</i>)	Oui
E-mail (<i>Email Address</i>)	Non
Service (<i>Department</i>)	Non
Société (<i>Company</i>)	Non
Ville (<i>City</i>)	Non
Département (<i>State</i>)	Non

Country (*Pays*)

Non

6. Remplissez les champs nécessaires.
7. Si vous souhaitez enregistrer le certificat sous forme cryptée, cochez la case **Crypter le certificat (*Encrypt certificate*)**.



Masquer | Masquer toutes les images

Options de cryptage

Choisissez un type de cryptage :

1. **DES en mode CBC**
2. **3DES en mode EDE**

Deux types d'exposant sont disponibles : 65537 et 3. Si l'exposant est petit, l'opération est plus rapide mais moins sécurisée.

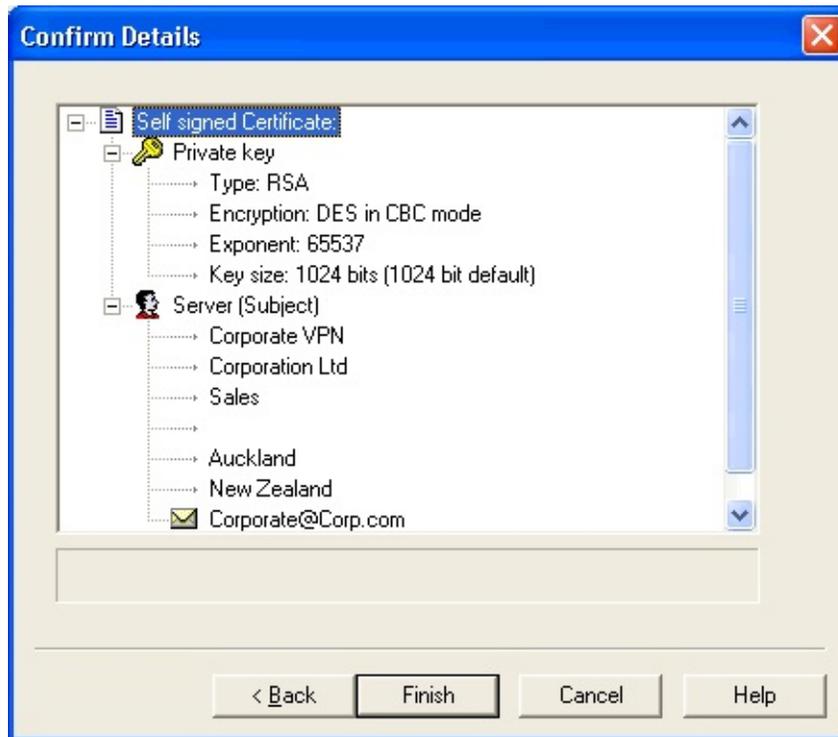
Taille (*Size*)

Taille (en bits) de la clé de cryptage.

Mot de passe (*Passphrase*)

Permet de décrypter la clé privée.

8. Cliquez sur **Suivant (*Next*)**. Les **détails** du certificat s'affichent alors. Tous les champs que vous avez remplis sont affichés.



Masquer | Masquer toutes les images

9. Vérifiez que les informations soient correctes puis cliquez sur **Terminer (*Finish*)**.
10. La requête n'est pas envoyée à WinGate tant que vous n'avez pas cliqué sur **OK**.

Remarque :

Les liaisons SSL ne sont disponibles qu'avec WinGate Enterprise, à partir de la version 6.0.

©2005 Qbik New Zealand Limited

Les services de WinGate

Les **services** sont au centre des opérations de WinGate.



Masquer

Ils sont composés de serveurs proxy pour les protocoles individuels et de liens mappés TCP/UDP.

Ils autorisent les ordinateurs clients à accéder aux serveurs externes des clients de leur choix, mais pas à jouer eux-mêmes le rôle de serveur. Les serveurs proxy se chargent de transmettre les requêtes des clients aux serveurs externes.

WinGate est équipé des proxies suivants : web, POP3 (messagerie électronique), FTP, Telnet, Streamworks, RTSP.

Les canaux sont les services utilisateur les plus courants. Ils redirigent les requêtes vers un autre emplacement. WinGate utilise deux types de canaux : TCP et liens mappés UDP.

Par défaut, le programme d'installation de WinGate configure les services de base et les exécute sur des ports standard. Si vous utilisez déjà une application serveur du même type (un serveur FTP ou web par exemple), vous souhaitez probablement modifier le port du service WinGate (ou du serveur). La section suivante explique comment intégrer des serveurs : elle est utile car une application ne peut écouter qu'un seul port donné à la fois.

[Cliquez ici pour savoir comment intégrer d'autres serveurs sur le même poste que WinGate](#)

Chaque service peut être configuré en tenant compte de ses exigences.

 Icône 	 Service 	 Description
Général	tous	Comporte le nom, la description du service ainsi que le port sur lequel les connexions sont acceptées. Permet également de configurer les options de démarrage (manuel, automatique, désactivé).

Liaisons (<i>Bindings</i>)	tous	Cette fenêtre permet à l'administrateur d'indiquer les interfaces qui acceptent les connexions entrantes pour ce service. Ces interfaces sont prises en charge par le serveur WinGate.
Politique (<i>Policies</i>)	tous	Chaque service est régi par des règles. Une option permet d'activer la politique par défaut (politique système). Si vous l'activez, ces droits s'appliquent également.
Journalisation (<i>Logging</i>)	tous	Tous les services peuvent être suivis ou enregistrés dans un fichier journal. Ces enregistrements détaillent l'utilisation d'un service. L'heure de chaque événement y est enregistrée.
Sessions	tous sauf DHCP	Cette fenêtre permet de définir le temps au bout duquel une session expire. Pour certains services, il est également possible de limiter le nombre de connexions.
Connexion (<i>Connection</i>)	tous les proxy TCP et liens mappés	Dans cette fenêtre, l'administrateur définit le mode de connexion du proxy à Internet. Les options proposées sont : connexion directe, en cascade, SOCKS4 ou SSL.
Requêtes serveur (<i>Server requests</i>)	tous les proxy sauf Telnet	Dans cette fenêtre, l'administrateur ajoute d'autres serveurs dans WinGate, notamment pour le traitement des requêtes non proxy.
Mode DHCP (<i>DHCP Mode</i>)	DHCP	Toutes les options du mode DHCP : de manuel à entièrement automatisé.
Paramètres (<i>DHCP Settings</i>)	DHCP	Plusieurs options sont disponibles pour le service DHCP. En cliquant sur l'icône Paramètres DHCP, vous configurez entre autres les baux et réservations d'adresses IP.
Mappages (<i>Mappings</i>)	Liens mappés	Cette fenêtre permet de configurer les mappages par utilisateur ou par emplacement.
Cryptage (<i>Encryption</i>)	Liens mappés	Cette fenêtre contient l'ensemble des paramètres de cryptage disponibles pour les liens mappés.

Avancé

SOCKS

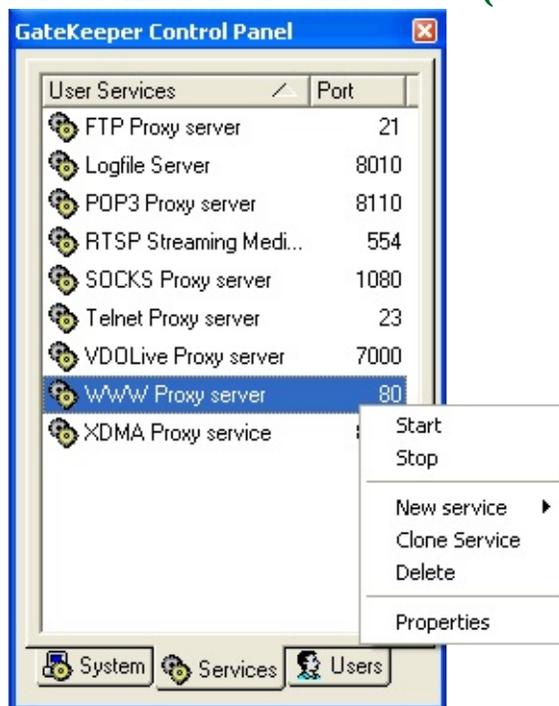
Options avancées de SOCKS, notamment le transfert des requêtes HTTP et des options pour les requêtes SOCKS.

©2004 Qbik New Zealand Limited

Ajouter un service

La procédure est très simple : tous les services sont affichés dans le même panneau.

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet **Services** dans le panneau Contrôle.
4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet et sélectionnez **Nouveau service (New service)**.



Masquer

5. Choisissez le type de service que vous souhaitez ajouter.
6. Indiquez son **nom** et sa **description**.
7. Choisissez un numéro de port ou conservez le numéro par défaut.
8. Cliquez sur **OK**.

Le service est à présent configuré.

Icônes Service

Service actif

Le service est actif.

Service arrêté

Le service est inactif.

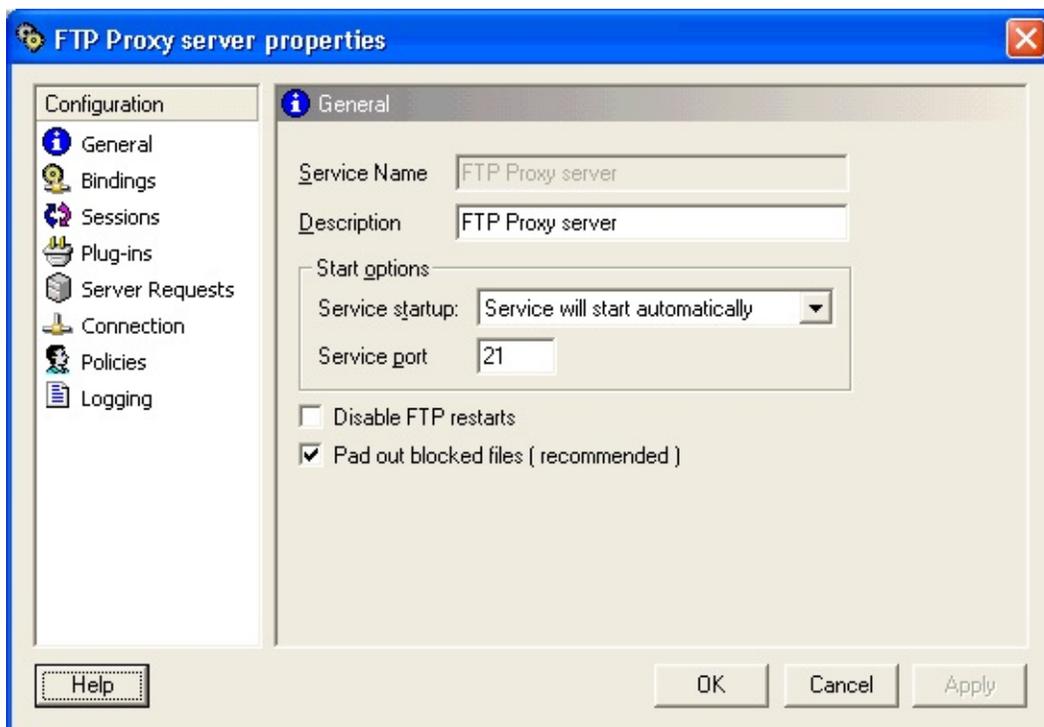
Erreur service

Le service n'a pas pu être démarré, généralement à cause d'un conflit au niveau des ports (deux services essayant de fonctionner sur le même port).

Proxy FTP

Le **serveur proxy FTP** est compatible avec les clients FTP utilisant la méthode d'authentification nomd'utilisateur@nomd'hôte : WS_FTP, CuteFTP, ainsi que les clients FTP en ligne de commande.

Le port FTP est le port 21.



Masquer

Si vous utilisez les modules additionnels au serveur FTP, vous disposez de deux options supplémentaires afin de mieux protéger votre réseau.

Empêcher la reprise des connexions interrompues (*Disable FTP restarts*)

Vous pouvez bloquer la commande **REST**, afin d'empêcher la reprise des téléchargements lorsqu'ils ont été interrompus par une analyse effectuée par les modules. Au contraire, il est possible de continuer à envoyer les données prévues

au client. Elles seront remises à zéro et donc invalides et inutilisables.

Conserver les fichiers bloqués (*Pad out blocked files*)

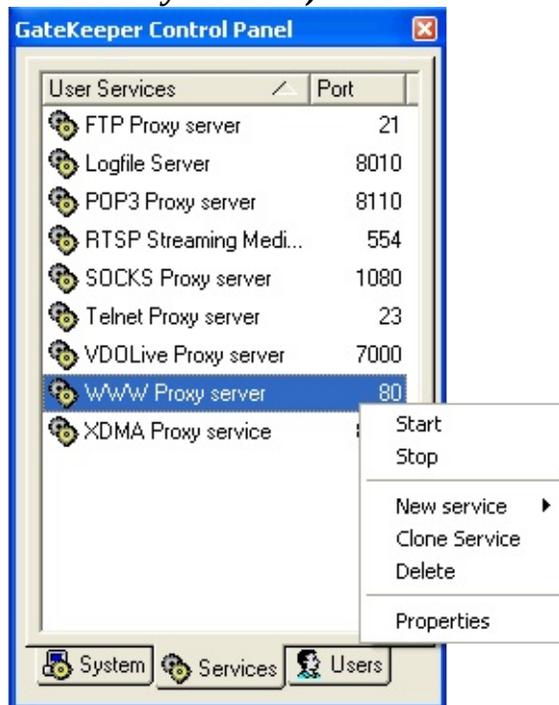
Empêche que les clients FTP ne soient déconnectés lors de l'analyse des données par les modules dans WinGate.

©2004 Qbik New Zealand Limited

Ajouter un proxy FTP

La procédure est assez simple :

1. Ouvrez **GateKeeper**.
2. Cliquez sur l'onglet **Services** dans le panneau Contrôle.
3. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet et sélectionnez **Nouveau service** puis **Service proxy FTP (New Service - FTP Proxy Service)**.

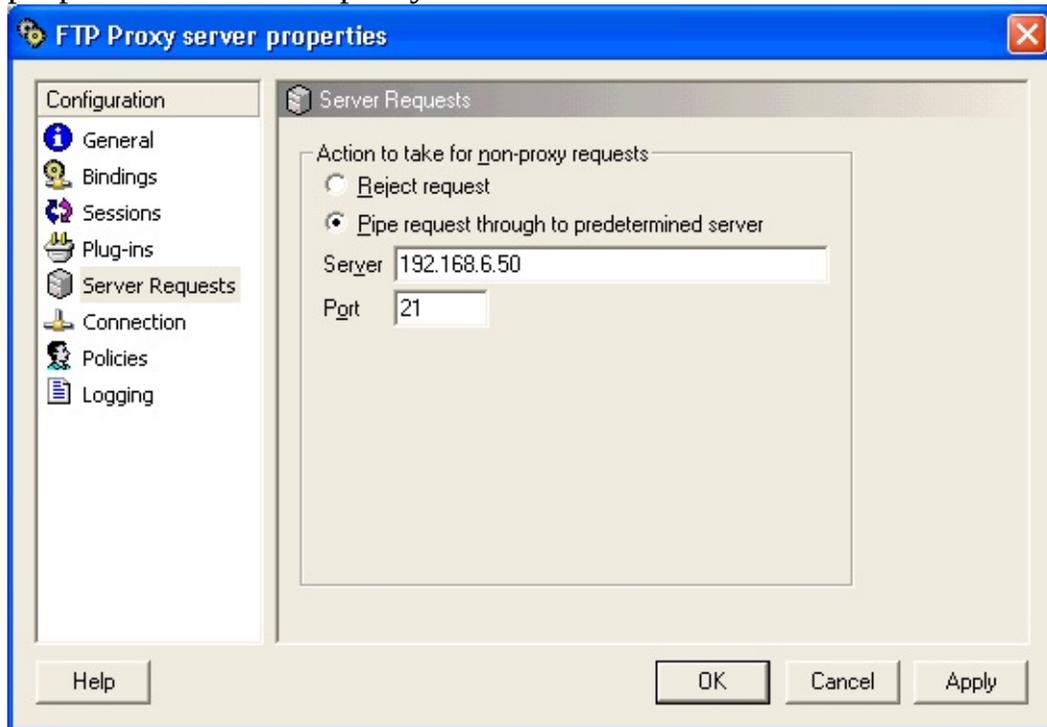


Masquer | Masquer toutes les images

4. Indiquez le numéro de port du service. Il s'agit généralement du **21**, sauf si vous possédez un serveur FTP qui l'utilise, auquel cas vous devrez en choisir un autre.
5. Si vous possédez un pare-feu externe, indiquez le nom d'hôte et le numéro de port et cochez l'option **Utiliser un pare-feu**.
6. Cliquez sur **OK**.

Si vous possédez un serveur FTP sur votre réseau, il est également possible d'autoriser l'accès depuis Internet par le biais de WinGate. Pour cela :

1. Cliquez sur l'icône **Requêtes serveur (Server Requests)** dans les propriétés du serveur proxy FTP.



Masquer | Masquer toutes les images

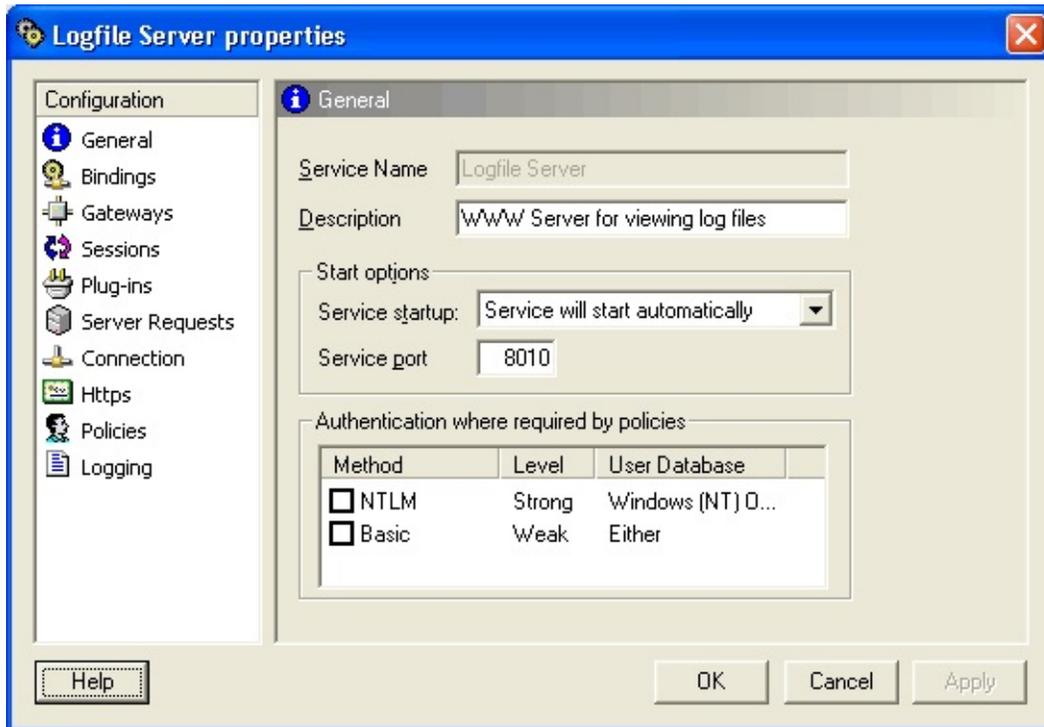
2. Indiquez l'**adresse** et le **numéro de port** de l'ordinateur sur lequel se trouve votre serveur FTP.

Voir également :

[Proxy FTP](#)

Serveur de fichiers journaux (*Logfile server*)

Afin de faciliter la gestion des audits utilisateurs et des fichiers journaux, WinGate inclut un **serveur de fichiers journaux** (installé et actif par défaut).



Masquer | Masquer toutes les images

Il s'agit d'un service proxy web sur le port 8010 permettant d'afficher les audits et fichiers journaux dans un navigateur. Si vous utilisez ce service, veillez à ce que le navigateur soit configuré correctement : il ne doit pas utiliser de proxy pour le serveur WinGate (car il est connecté par votre réseau et non par Internet).

Ajoutez l'entrée suivante à la liste des services qui ne doivent pas utiliser de proxy :

wingate:8010

(ou bien l'adresse IP/le nom que vous avez attribué au serveur WinGate).

Affichage des fichiers journaux dans un navigateur

Il suffit de copier et coller l'une des URL suivantes dans la barre d'adresses :

http://wingate:8010 (remplacez "wingate" par le nom que vous avez choisi pour votre serveur)

OU

http://192.168.0.1:8010 (remplacez "192.168.0.1" par l'adresse IP privée de votre serveur)

Le fichier index.htm, situé dans le répertoire d'installation de WinGate, s'affiche alors.

Il contient quatre liens :

Fichiers journaux des services (*Service logs*)

Audits utilisateurs (*User audits*)

Informations générales (*Information*)

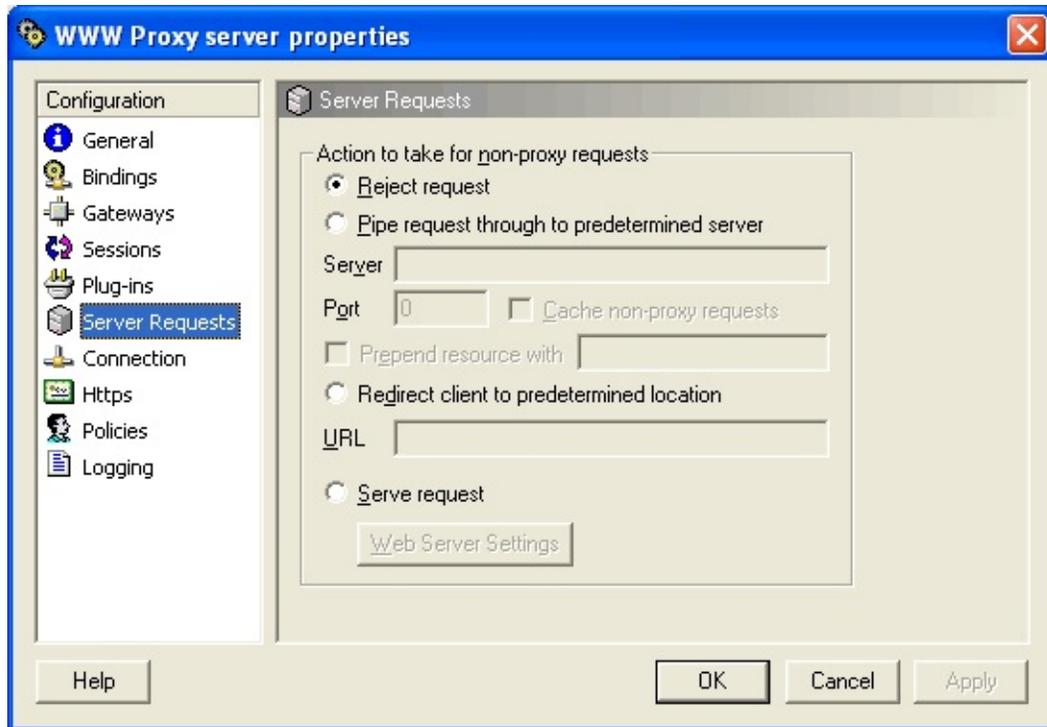
GateKeeper.exe

Les deux premiers liens affichent des dossiers contenant les fichiers journaux ou d'audits. Le dernier permet d'installer GateKeeper sur le poste. Il est donc préférable de limiter l'accès à ce serveur aux administrateurs (en effet, des utilisateurs mal intentionnés pourraient installer GateKeeper afin de modifier les paramètres de WinGate).

Autres applications

Il est possible d'ajouter des serveurs de fichiers journaux supplémentaires

1. Dans GateKeeper, ajoutez un service proxy web (*WWW proxy service*) sur un port libre.
2. Cliquez sur l'icône **Requêtes serveur (*Server requests*)**.



Masquer | Masquer toutes les images

3. Cochez l'option **Exécuter la requête (Serve request)**.
4. Cliquez sur **Paramètres du serveur (Web server settings)**.
5. Dans **la fenêtre** qui s'ouvre ensuite, indiquez le répertoire de WinGate dans le champ **Répertoire racine du serveur (Server root directory)**.

Masquer | Masquer toutes les images

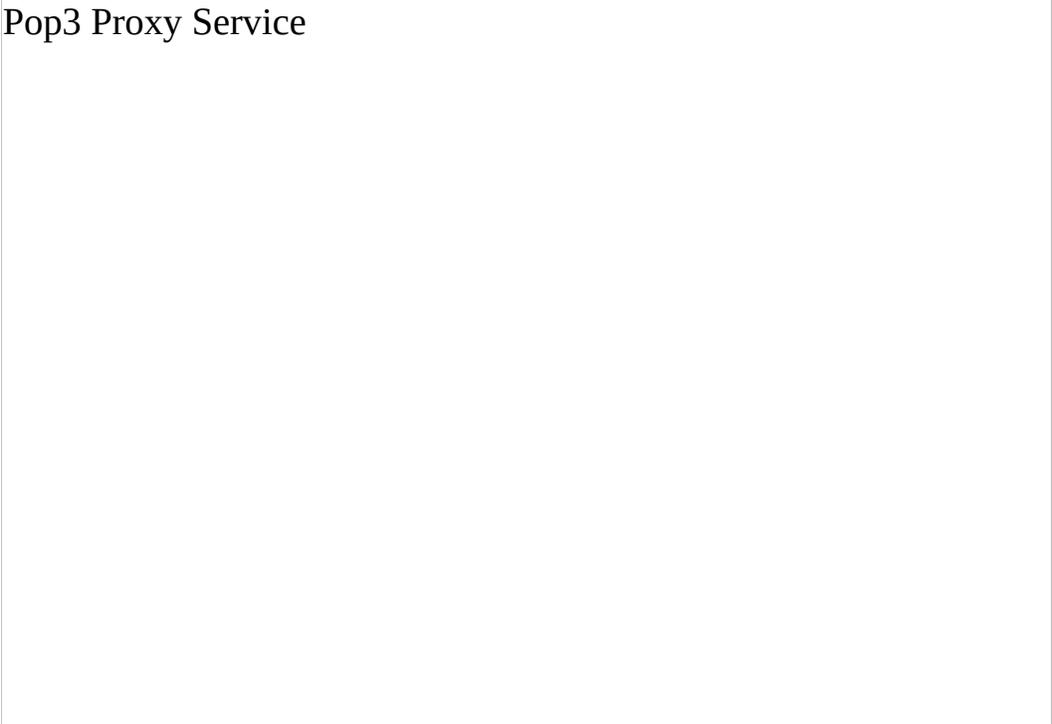
6. Dans le champ **Fichier par défaut (Default filename)**, indiquez **index.htm**.
7. Cochez l'option **Autoriser l'exploration du répertoire (Permit directory browsing)**.
8. Cliquez sur **OK**.

Créez ensuite votre page HTM sur le modèle du fichier index.htm. Ces serveurs peuvent avoir diverses applications, y compris la publication de vos pages Intranet/Internet.

Proxy POP3

Le serveur proxy POP3 peut s'avérer nécessaire si vous souhaitez pouvoir consulter le courrier sur un compte à distance.

Pop3 Proxy Service



Masquer | Masquer toutes les images

Il peut se connecter sur différents ports (110 par défaut). Dans les propriétés du proxy, vous pouvez utiliser un délimiteur. Il s'agit généralement du signe "#" (voir exemple ci-dessous).

Pour utiliser le proxy POP3 :

Dans le programme de messagerie sur le poste client, indiquez l'adresse IP interne du serveur WinGate dans les paramètres du serveur POP3, et modifiez votre nom d'utilisateur POP3 comme suit :

Nom d'utilisateur POP3 + délimiteur + Nom du serveur POP3.

Exemple :

Le nom d'utilisateur POP3 est **pierredupond** et le nom du serveur de messagerie est **mail.qbik.com**.

Dans Netscape, MS Mail, Pegasus mail, etc. vous devez indiquer **pierredupond#mail.qbik.com** pour le nom d'utilisateur et **l'adresse IP du serveur WinGate** dans les propriétés SMTP/POP3.

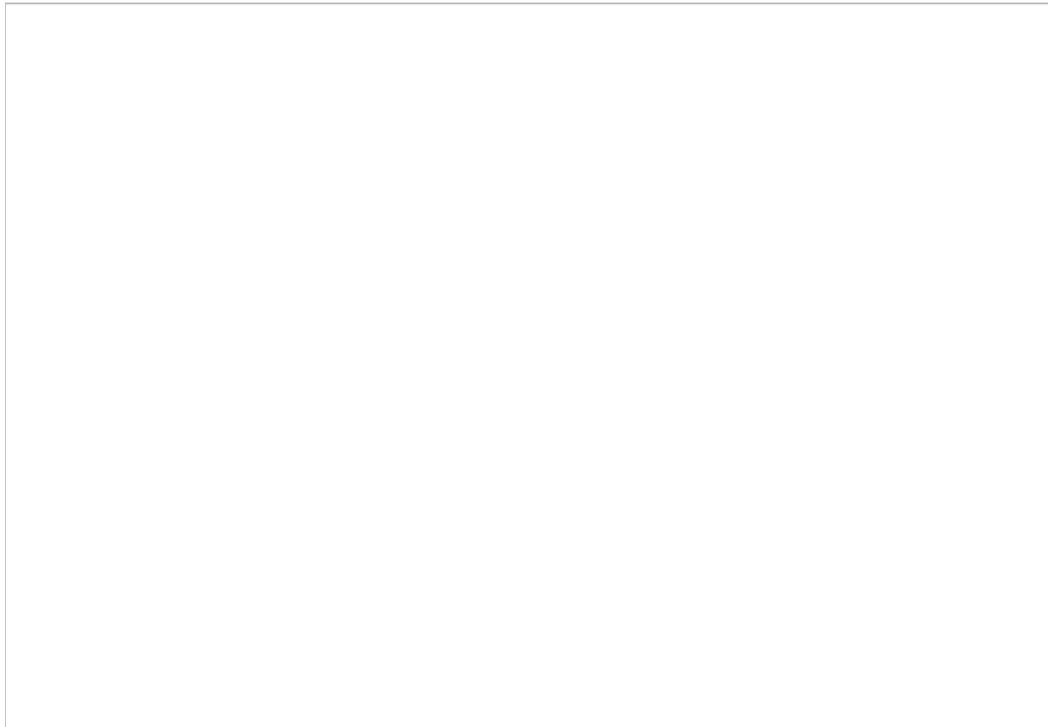
Remarque :

Si vous n'indiquez aucune adresse de retour, l'adresse par défaut est **pierredupond#mail.qbik.com@wingate**.

Assurez-vous que l'adresse de retour soit bien votre adresse e-mail.

Remarque :

Si vous utilisez le serveur de messagerie, les connexions sur le port **110** pourront être redirigées vers le serveur proxy POP3 sur le port **8110** à condition que l'option **Transmettre au serveur de messagerie interne (*Handover to Internal Mail server*)** soit sélectionnée dans les **propriétés du service proxy POP3**.

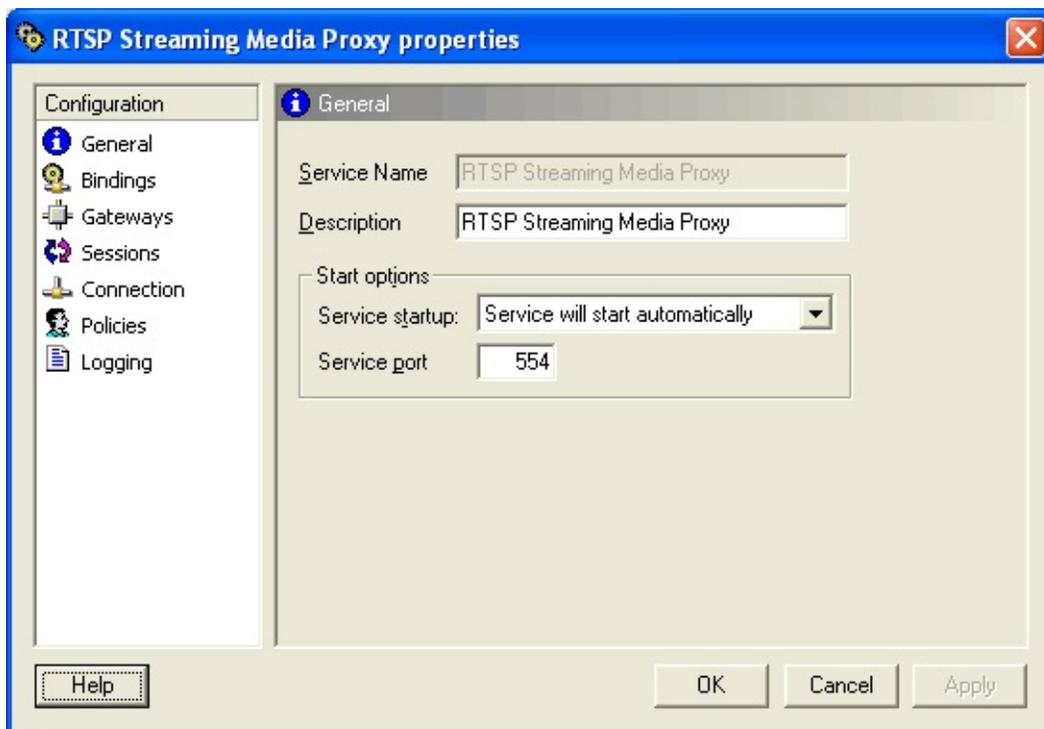


Masquer | Masquer toutes les images

©2005 Qbik New Zealand Limited

Proxy RTSP

Le protocole RTSP (Real Time Streaming Protocol) permet de transférer des données (audio et vidéo) en temps réel. RealPlayer et QuickTime peuvent être configurés de façon à utiliser le **proxy RTSP** de WinGate.



Masquer

Ce service transfère les données par le biais de sockets UDP de façon plus efficace que le NAT. En effet, ce dernier a tendance à diffuser les données en continu à l'aide d'une connexion TCP. Ainsi, lorsqu'il s'agit de données en temps réel, il en transmet plus que nécessaire.

Le proxy gère les connexions UDP de façon plus efficace car il "comprend" mieux le protocole RTSP, ce qui le rend plus performant.

Configuration de RealPlayer

1. Cliquez sur Outils -> Préférences -> Proxy.
2. Cochez l'option "Utiliser un proxy RTSP" et indiquez l'adresse du serveur WinGate ainsi que le numéro de port du proxy RTSP (par défaut : 554). En cas de doute, contactez votre administrateur système.

RealAudio et RealPlayer sont des marques déposées de RealNetworks, Inc.

Configuration de QuickTime

1. Cliquez sur Édition -> Préférences -> Préférences de QuickTime et sélectionnez "Proxy d'enchaînement" dans la liste déroulante.
2. Indiquez l'adresse du serveur WinGate ainsi que le numéro de port du proxy RTSP (par défaut : 554).

QuickTime est une marque déposée de Apple Computer, Inc., aux États-unis et dans d'autres pays.

©2004 Qbik New Zealand Limited

Proxy Socks

Le **serveur proxy SOCKS** de WinGate fournit les services de connectivité Socks et AutoSocks aux postes clients de votre réseau local.

Masquer

SOCKS est un protocole de communication Internet permettant d'effectuer des connexions de base à travers un pare-feu.

Il est compatible avec de nombreuses applications capables de se connecter à travers à un pare-feu : la plupart des navigateurs, certains clients FTP et applications IRC... Les logiciels clients compatibles avec ce protocole fonctionnent généralement de façon transparente, c'est à dire comme s'ils étaient connectés directement à Internet.

De plus, il existe des logiciels (par exemple : **AutoSOCKS**) permettant d'intégrer **SOCKS** automatiquement dans des applications qui ne sont pourtant pas compatibles avec ce protocole. Le logiciel client **AutoSOCKS** est disponible auprès de nombreux vendeurs.

Si vous possédez ce logiciel, les proxies de WinGate ne sont pas nécessaires (le proxy SOCKS suffit à répondre à vos besoins). Les autres services de WinGate peuvent toutefois s'avérer utiles si vous possédez un serveur de messagerie/FTP/web ou si vous souhaitez que les utilisateurs s'authentifient.

Le numéro de port par défaut est : **1080**.

Versions

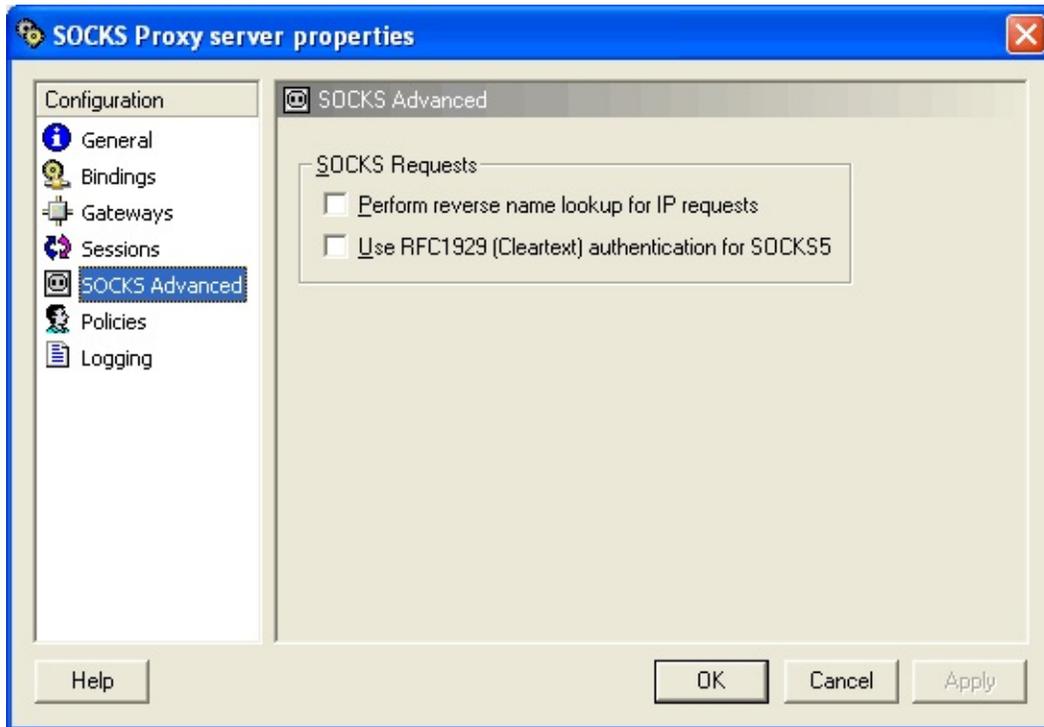
Deux versions de SOCKS sont actuellement utilisées sur Internet : **SOCKS 4** et **5**. SOCKS 5 inclut des fonctionnalités supplémentaires, telles que : le support de l'authentification des clients SOCKS et le support du protocole UDP.

Le serveur SOCKS de WinGate est compatible avec chacune de ces versions.

©2004 Qbik New Zealand Limited

Socks - Avancé

Copie d'écran



Masquer

En cliquant sur cette icône, vous disposez de deux options :

1. **Effectuer des vérifications inverses pour les requêtes (*Perform reverse name lookups for IP requests*)**

Lorsque cette option est cochée, WinGate convertit en noms de domaine les adresses IP utilisées dans les requêtes. Cela améliore les performances de la mémoire cache car si un nom est présent, il peut être utilisé directement.

2. **Utiliser l'authentification RFC1929 pour Socks5 (*Use RFC1929 (Cleartext) Authentication for Socks5*)**

- Certains clients SOCKS5 sont compatibles avec la méthode d'authentification "RFC1929", avec laquelle un nom d'utilisateur et un mot de passe sont transmis en texte clair. Lorsqu'un utilisateur se connecte, WinGate évalue son niveau d'authentification : Inconnu

(*Unknown*), Présumé (*Assumed*) ou Authentifié (*Authenticated*), en fonction des informations qu'il possède.

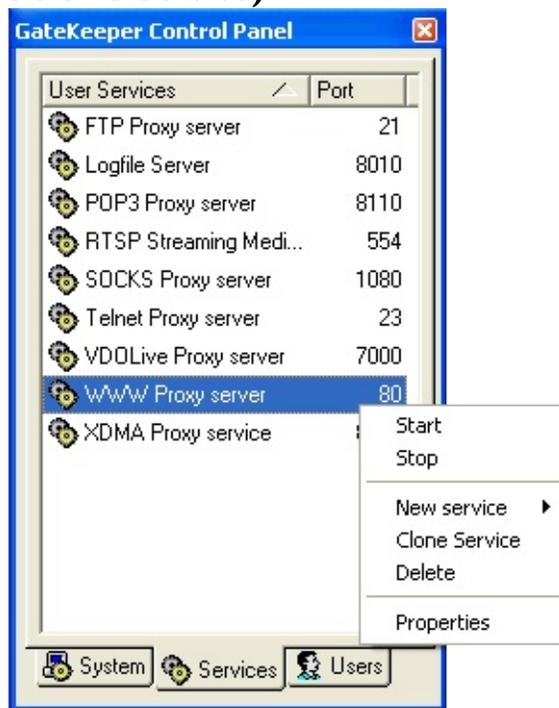
- Si un utilisateur est inconnu et que cette option est cochée, il devra utiliser la méthode "RFC1929" afin d'acquérir le statut d'utilisateur présumé. Dans les autres cas le client ne sera pas obligé de l'utiliser.
- Si un utilisateur présumé ne dispose pas de droits d'accès au serveur SOCKS il pourra tout de même s'authentifier à l'aide de cette méthode (à condition que le nom et le mot de passe fournis correspondent à un compte possédant les droits nécessaires).
- Cette méthode n'étant pas sécurisée, les utilisateurs qui l'emploient obtiennent seulement le statut "présumé" (et non "authentifié"). De plus, en raison de sa vulnérabilité, il est recommandé de ne pas l'utiliser sur un réseau inconnu comme Internet.

Si vos applications clientes utilisent SOCKS4, vous devez posséder un service DNS sur votre réseau (pouvant être configuré à l'aide du DHCP). Avec SOCKS5, cela n'est généralement pas nécessaire. De nombreux produits sont compatibles avec SOCKS5, mais SOCKS4 est encore souvent employé par les navigateurs et certains clients.

Le serveur SOCKS de WinGate est capable de reconnaître et de transmettre les requêtes HTTP au proxy web afin de permettre la mise en cache et l'application de la politique spécifique à ce service.

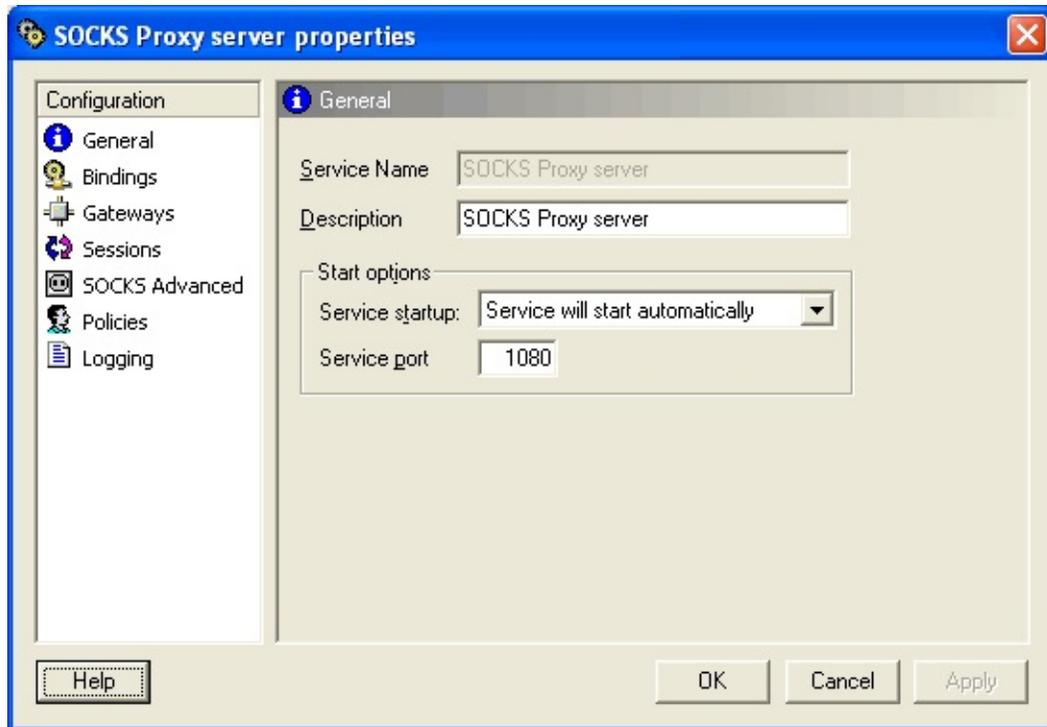
Ajouter un serveur SOCKS

1. Ouvrez GateKeeper.
2. Connectez-vous à l'aide du compte **Administrator**.
3. Cliquez sur l'onglet **Services** dans le panneau Contrôle.
4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet et sélectionnez **Nouveau service - Service SOCKS (New service - SOCKS Service)**



Masquer | Masquer toutes les images

5. Dans **la fenêtre** qui s'ouvre ensuite, indiquez le **nom** et la **description** du service, ou conservez les paramètres par défaut.



Masquer | Masquer toutes les images

6. Indiquez le numéro de **port** à utiliser, ou conservez le numéro par défaut.

Remarque :

Le nom choisi doit être différent pour chaque service.

Vous pouvez aussi conserver les options avancées par défaut, ou bien les configurer vous-même.

Voir également :

[Serveur SOCKS 5](#)

Proxy Telnet

Telnet étant un service essentiellement en ligne de commande, il n'est pas nécessaire de configurer le client pour l'utilisation du **proxy Telnet**. Toutefois, vous devez toujours commencer par vous connecter au serveur WinGate sur le port choisi pour ce service.

Le numéro de port par défaut est **23**.

Masquer | **Masquer toutes les images**

Options

Utiliser l'authentification requise par la politique système (*Use login as required by system policies*)

Lorsque cette option est cochée, vous devez vous authentifier pour utiliser ce service.

Exécuter en tant qu'interpréteur de commandes (*Run as Command Shell*)

Permet d'accéder à certaines fonctionnalités de WinGate par le biais d'une invite de commandes Telnet. Pour des raisons de sécurité, il est recommandé de ne cocher cette option que si vous possédez suffisamment de connaissances dans ce domaine.

Nous vous recommandons également de créer un nouveau service Telnet appelé par exemple **Interpréteur WinGate** sur un port différent (par ex. : 8023) et lié à **aucun** adaptateur externe.

Utilisation du service Telnet dans WinGate

1. Ouvrez l'invite de commandes de Windows.
2. Saisissez **Telnet.exe**

3. Saisissez **Open** puis indiquez l'adresse IP du serveur WinGate ou bien **localhost** si vous travaillez sur le serveur, et connectez-vous sur le port 23 (ou le port attribué au proxy Telnet).

Login :

Saisissez votre nom d'utilisateur WinGate et appuyez sur la touche Entrée.

Password :

Saisissez votre mot de passe et appuyez sur la touche Entrée.

Une fois connecté, l'invite que vous avez choisie s'affiche. Par exemple :

WinGate>

Indiquez le nom de l'hôte auquel vous souhaitez vous connecter (vous pouvez préciser un numéro de port mais cela n'est obligatoire). Par exemple :

```
WinGate>ftp.freddy-anne.com
```

ou

```
WinGate>ftp.billy-sue.com 1023
```

WinGate affiche "Connecting to" ..." puis "Connected" lorsque vous êtes connecté à l'ordinateur distant.

Quelques modifications ont été apportées à ce proxy. Cela risque de perturber les clients utilisant des commandes Telnet (par exemple : les clients EWAN, simpterm, et UNIX). Un double écho se produit parfois lorsque vous saisissez le nom d'hôte. Ce problème se résout généralement de lui-même une fois connecté.

En cas de problème avec la touche Entrée, essayez Ctrl + J ou Ctrl + Entrée, ou attribuez un autre numéro de port au service. Cela empêche les clients de déterminer qu'il s'agit d'un serveur Telnet. Par conséquent ils n'envoient pas de commandes risquant de causer des erreurs.

Remarque :

Le service Telnet de WinGate permet **uniquement** de se connecter à un "vrai" serveur Telnet. Il ne propose pas les autres fonctions généralement associées à ce service.

Si vous vous connectez toujours au même hôte, il est préférable d'utiliser un lien

mappé : cela évite de devoir indiquer le nom de l'hôte à chaque connexion.

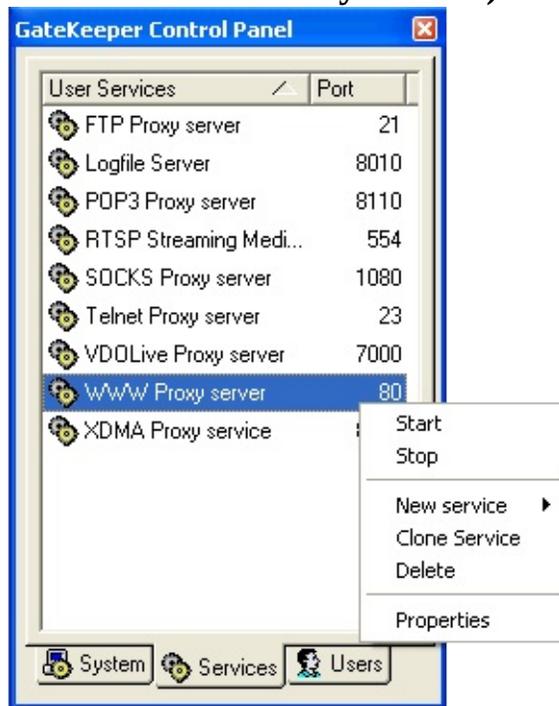
Veillez noter que cette fonctionnalité n'est disponible qu'avec les versions Pro et supérieures.

©2004 Qbik New Zealand Limited

Ajouter un proxy Telnet

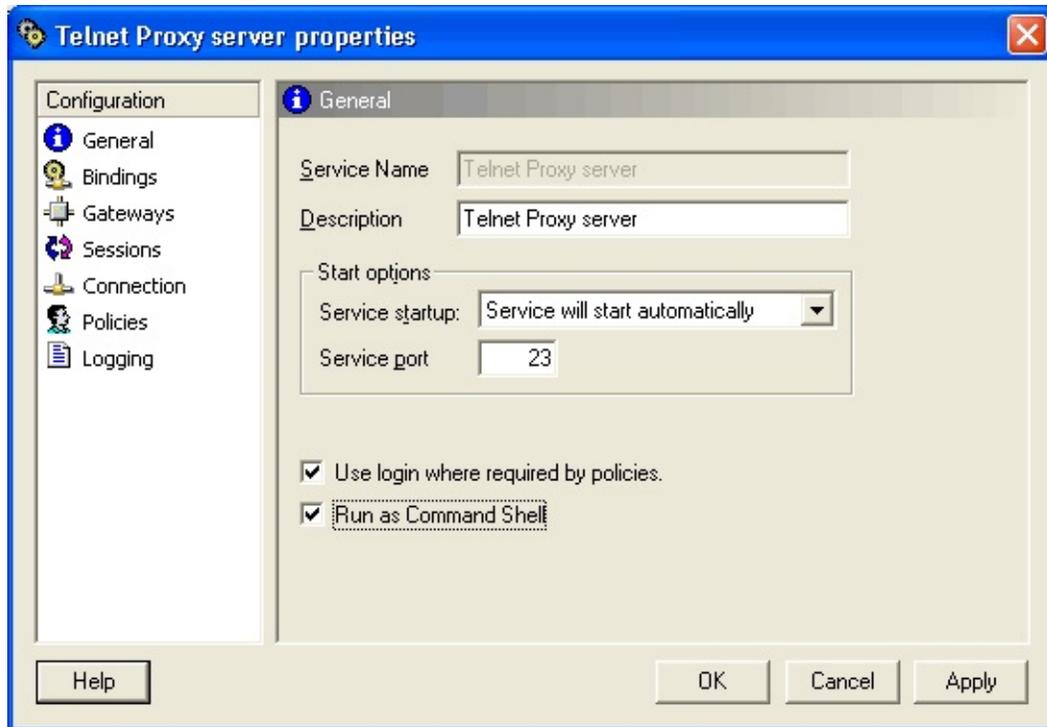
Le port utilisé est généralement le **23**. Pour ajouter un proxy Telnet :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet **Services** du panneau Contrôle.
4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet et sélectionnez **Nouveau service** puis **Service proxy Telnet (New service - Telnet Proxy Service)**



Masquer | **Masquer toutes les images**

5. Indiquez le numéro de port (par défaut : **23**).
6. Cliquez sur **OK**.



Masquer | Masquer toutes les images

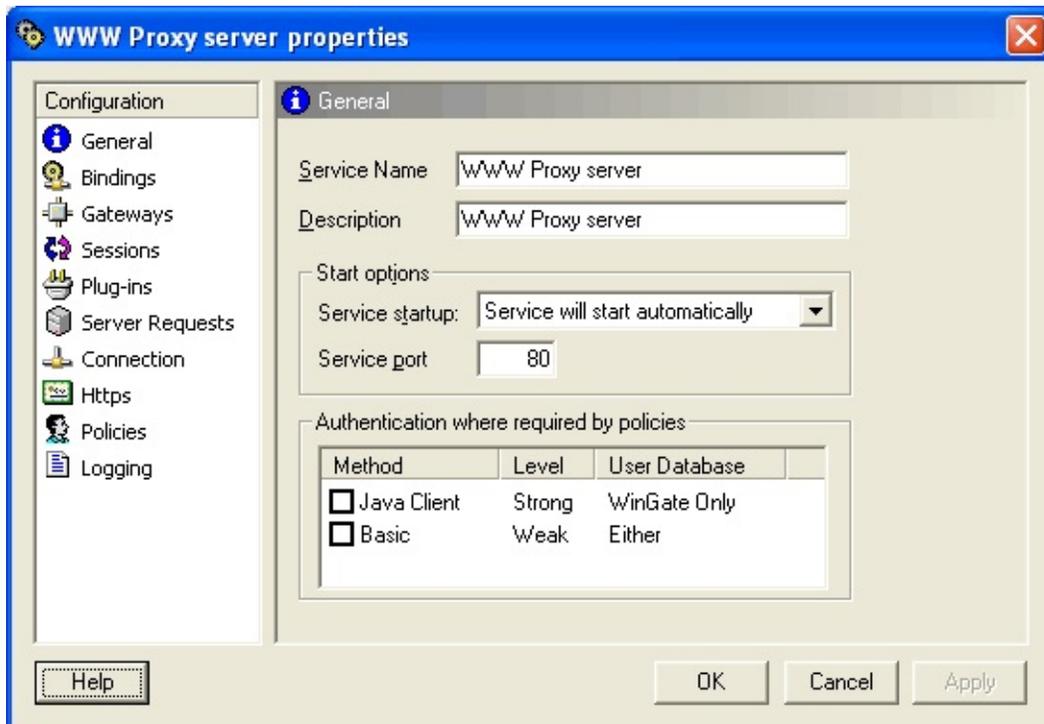
Voir également :

[Proxy Telnet](#)

Proxy web

Le serveur **proxy web** permet aux clients qui utilisent le protocole HTTP d'accéder à Internet.

Si cela concerne principalement les navigateurs, d'autres applications reposent également sur HTTP (ex.: RealPlayer et le lecteur VIVO).



Masquer | Masquer toutes les images

Quelques données :

Le proxy web de WinGate est compatible avec les protocoles HTTP, SHTTP et FTP.

Il utilise le port 80 (possible de le configurer).

Les serveurs web fonctionnent également sur le port 80.

Le proxy supporte la gestion en cascade et les requêtes ne provenant pas de serveurs proxy (cf. "Requêtes serveur" ci-dessous).

Les utilisateurs équipés d'un navigateur Java peuvent s'authentifier dans

WinGate à l'aide du [Client Java](#)

Les utilisateurs équipés d'un navigateur compatible peuvent s'authentifier avec NTLM.

Plusieurs proxy web peuvent être configurés sur différents ports, mais chacun doit porter un nom différent.

Méthode d'authentification (si nécessaire) (*Authentication where required by policies*)

Sélectionnez le type d'authentification à mettre en place pour sécuriser l'accès au proxy web.

Trois méthodes sont possibles : Plain, Authentification Java et NTLM.

Plain

Système d'authentification le moins sécurisé.

Authentification Java

Disponible pour les navigateurs compatibles avec l'authentification Java.

NTLM

Autorise les clients à s'authentifier avec NTLM, méthode employée par les systèmes d'exploitation Windows NT.

Remarque :

L'authentification NTLM n'apparaît que si vous utilisez la base de données d'utilisateurs du système d'exploitation (Windows).

Mise en cache

Le proxy web de WinGate inclut un cache HTTP dans lequel sont stockés les graphiques, documents HTML, Applets Java et autres fichiers Internet récemment consultés pour les retrouver rapidement si un utilisateur en fait la demande depuis un ordinateur du réseau.

Seules les requêtes de type "GET" sont mises en cache. Les requêtes FTP, celles

qui contiennent une chaîne (réponse suite à un modèle soumis par exemple) et les pages Web qui requièrent une authentification ne sont pas concernées par cette fonctionnalité. Vous pouvez par ailleurs configurer des règles pour définir ce que WinGate est autorisé à mettre en cache.

([En savoir plus sur la gestion du cache](#))

Ordre des tentatives de connexion

Si l'URL demandée n'existe pas, le proxy web essaie de se connecter aux URL basées sur ce nom. Ainsi, vous pouvez obtenir la page "microsoft.com" simplement en saisissant "microsoft" ou "tf1.fr" en saisissant "tf1". L'ordre de recherche se définit dans le registre et correspond au modèle suivant :

http://site/

http://site.com/

http://www.site.com/

etc.

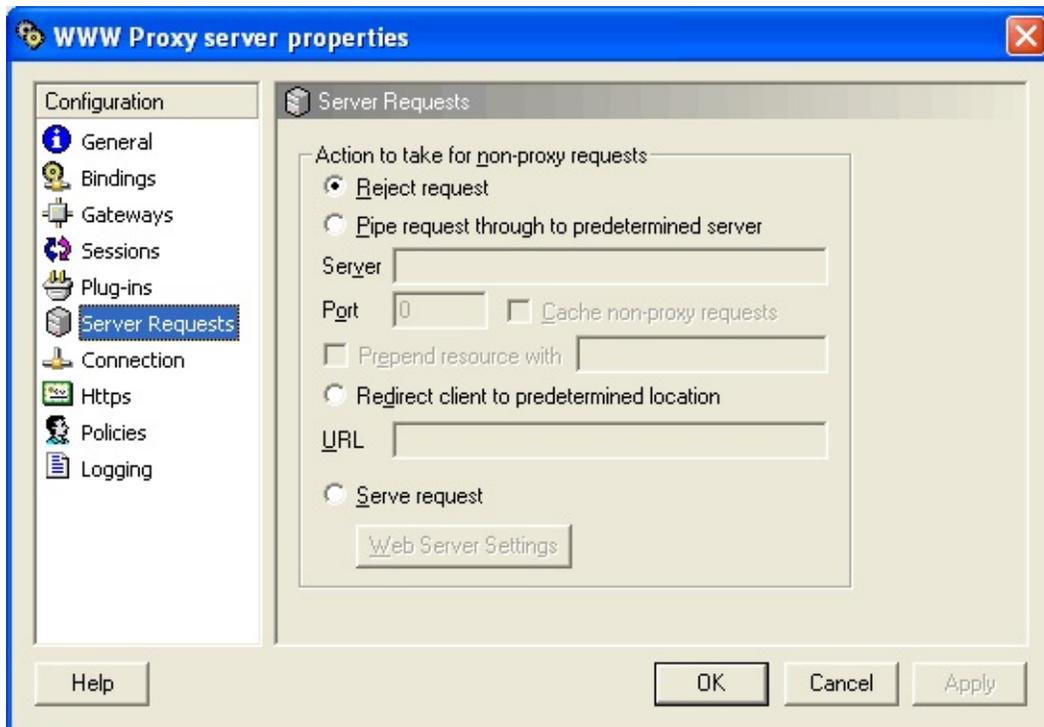
Pour ajouter d'autres types de recherche, reportez-vous à la [configuration avancée](#) de WinGate

Voir également :

[Ajouter un serveur proxy](#)

Requêtes serveur (*Server Requests*)

Cette fonctionnalité permet de configurer la gestion des requêtes non proxy pour les services FTP, WWW, POP3, XMDA, VDO et le serveur de fichiers journaux.



Masquer | Masquer toutes les images

Rejeter la requête (*Reject request*)

Par défaut, WinGate rejette toutes les requêtes qui ne proviennent pas d'un proxy.

Rediriger la requête vers un serveur prédéterminé (*Pipe request through a predetermined server*)

En sélectionnant cette option, WinGate transfère la requête vers un autre serveur.

Souvent, il s'agit d'un serveur web sur le réseau ou sur Internet. Il existe en fait un lien mappé qui écoute sur le même port que le proxy web.

Mettre en cache les requêtes non proxy (*Cache non-proxy requests*)

Cette option est recommandée si vous redirigez les requêtes vers un autre ordinateur sur le réseau local. Lorsqu'elle est activée, WinGate enregistre les ressources les plus demandées en cache afin de les retrouver rapidement la fois suivante.

Compléter la ressource avec (*Prepend resource with*)

Activez cette option pour utiliser un répertoire différent de celui enregistré à la racine du serveur. Par exemple, si la racine est "C:\root" et que vous préférez diriger les utilisateurs vers "C:\root\public\company\", activez l'option puis entrez "\public\company" dans le champ **Compléter la ressource**.

Options disponibles uniquement le service proxy web (WWW proxy service) et le serveur de fichiers journaux :

Rediriger le client vers un emplacement prédéterminé (*Redirect client to predetermined location*)

En activant cette option, WinGate "redirige" chaque requête entrante vers une URL particulière. Cette option est semblable à celle intitulée "Rediriger la requête vers un serveur prédéterminé" à deux différences près : elle considère que la requête provient d'un navigateur web et elle autorise l'utilisateur à indiquer une page.

Cette option permet également d'accepter et de rediriger les requêtes d'un site Web à partir d'un domaine, alors qu'il est en fait hébergé par un autre (Ex. : votre domaine est www.mycompany.com mais votre site est hébergé par www.someISP.com) - vos utilisateurs sont autorisés à se connecter à votre site à partir de www.mycompany.com.

Exécuter la requête (*Serve request*)

Vous pouvez configurer le service proxy web de WinGate pour qu'il joue le rôle

de serveur web même lorsqu'une requête entrante ne provient pas d'un proxy. À réception d'une requête de ce type, il fournira au client la ressource demandée (normalement une page web).

Quand cette fonction est-elle utilisée dans WinGate ?

Elle est utile si vous souhaitez servir le site Web d'une entreprise publique ou un Intranet privé réservé aux seuls utilisateurs du réseau local. Dans l'exemple donné, le service proxy web est configuré pour "servir" la page index.htm à partir du répertoire C:\webserve (ou de n'importe quel sous-dossier).

Ainsi, lorsqu'un utilisateur pointe son navigateur sur le serveur WinGate (avec une adresse IP ou un nom de domaine externe s'il en possède un), son navigateur affiche la page index.html.

Configuration du service proxy web (WWW proxy service) pour qu'il exécute les requêtes :

1. Ouvrez le service proxy web et cliquez sur l'icône **Requêtes serveur (Server Requests)**.
2. Cochez l'option **Exécuter la requête (Serve Request)**.
3. Cliquez sur le bouton **Paramètres du serveur (Web server settings)**.
4. Dans l'onglet **Général**, indiquez l'emplacement du répertoire utilisé pour exécuter les requêtes.



Masquer | Masquer toutes les images

[Cliquez ici pour en savoir plus](#)

Remarque :

Les autres liens de la page index.htm risquent de diriger le navigateur vers des

pages qui ne sont pas stockées sur le serveur WinGate.

©2005 Qbik New Zealand Limited

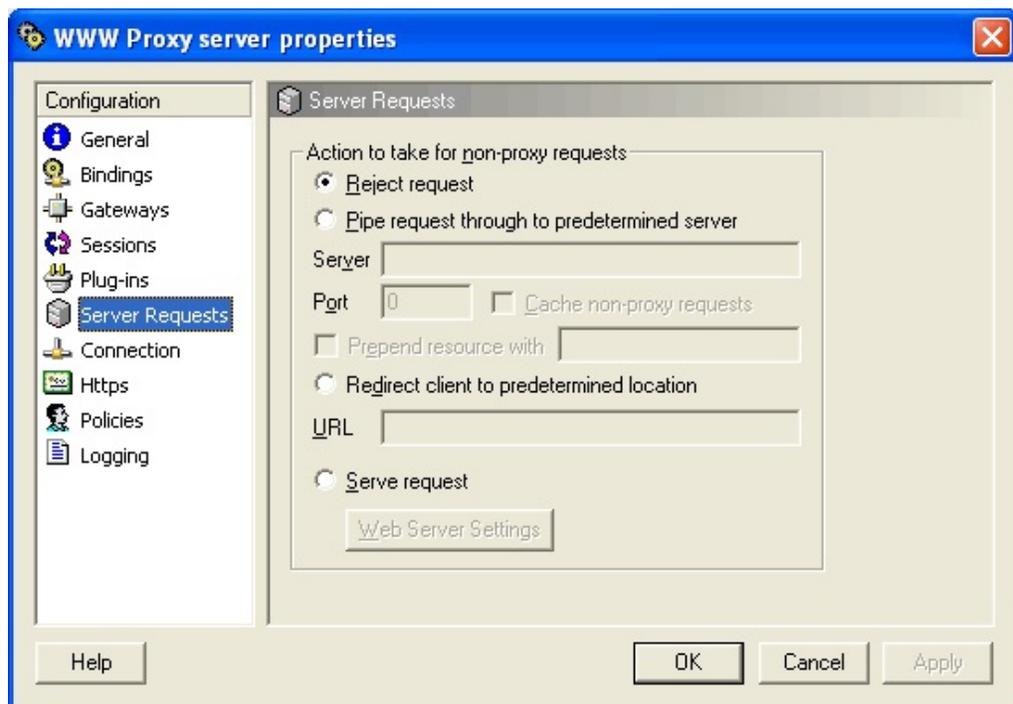
Paramètres du serveur web

Le service proxy web (*WWW Proxy Service*) peut être configuré de façon à exécuter les requêtes entrantes non proxy. Lorsqu'il reçoit ce type de requête, il essaie alors de "servir" la ressource demandée (généralement une page html).

A partir de la version 6.0, WinGate peut même servir d'autres types de ressources comme les pages .php.

Pour configurer ces paramètres :

1. Ouvrez **GateKeeper**.
2. Cliquez sur l'icône **Requêtes serveur (*Server Requests*)** dans les propriétés du service proxy web.



Masquer | Masquer toutes les images

3. Cochez l'option **Exécuter la requête (*Serve request*)**, puis cliquez sur **Paramètres du serveur (*Web Server settings*)**.

La fenêtre comprenant les paramètres du serveur est constituée de trois onglets :

1. Général

Masquer | **Masquer toutes les images**

Répertoire racine du serveur (*Server root directory*)

Répertoire racine sur le disque local (généralement appelé www root) où sont conservées toutes les ressources. Tous les sous-répertoires indiqués dans des URL sont ajoutés au nom de ce chemin.

Fichier par défaut (*Default filename*)

Page html "servie" lorsque l'URL n'indique aucune page. Il s'agit généralement de la page d'accueil.

Répertoire CGI (*CGI Directory*)

Chemin du répertoire sur le disque local dans lequel sont conservés les scripts CGI (généralement un sous-répertoire de www root).

Préfixe des CGI (*CGI URL Prefix*)

Nom du répertoire sur le disque local dans lequel sont conservés les scripts CGI. Les scripts ne s'exécuteront que s'ils se trouvent à la racine de ce répertoire.

2. Associations de fichiers (*File Associations*)

Masquer | **Masquer toutes les images**

Choisissez les exécutables à utiliser pour ouvrir des fichiers ayant des extensions spécifiques.

3. Variables d'environnement (Environment Variables)

Masquer | Masquer toutes les images

Configurez ici les variables d'environnement pour les exécutables choisis dans l'onglet précédent.

Remarque :

CGI (Common Gateway Interface) est une norme Internet conçue pour les petits programmes installés sur le serveur web : les scripts. Les pages web contiennent souvent des **modèles** (formulaires, champs que vous remplissez et menus déroulants dans lesquels vous sélectionnez des éléments.)

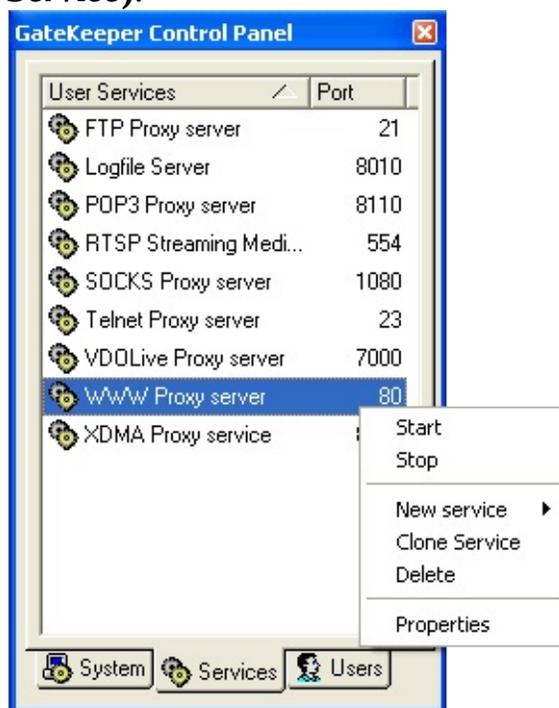
Lorsqu'un utilisateur clique sur le bouton pour valider les informations saisies dans un modèle, le serveur web exécute le script indiqué et lui transmet les informations à traiter. Le travail du script consiste à entrer ces informations dans la base de données, ou à générer une nouvelle page HTML à partir des informations saisies par l'utilisateur.

Notez bien que si le script génère une nouvelle page HTML, il doit générer une page entière comprenant toutes les informations de l'en-tête (NPH only – Non-Parsed Headers). Certains serveurs Web génèrent les informations de l'en-tête avant même d'ouvrir la page, mais ce n'est pas le cas avec cette implémentation de WinGate.

©2005 Qbik New Zealand Limited

Ajouter un serveur proxy web

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet **Services** du panneau Contrôle.
4. Effectuez un clic droit à l'intérieur de cet onglet puis sélectionnez **Nouveau service - Service proxy web (New service - WWW Proxy Service)**.



Masquer | Masquer toutes les images

5. Indiquez son **nom** et sa **description** ou bien conservez les valeurs par défaut.
6. Indiquez le **port** à utiliser, ou conservez le numéro par défaut.
7. Cliquez sur **OK**.

Remarque :

Le nom choisi doit être différent pour chaque service.

Vous pouvez conserver les options avancées par défaut ou bien les configurer

vous-même.

Voir également :

[Proxy web](#)

©2004 Qbik New Zealand Limited

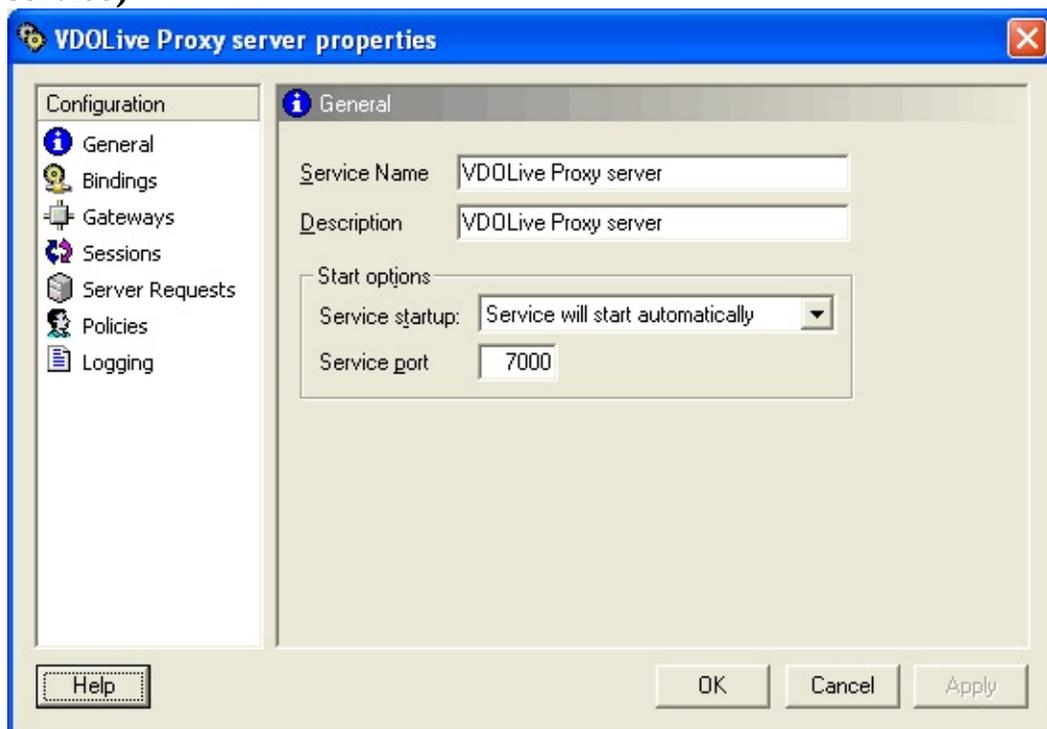
Proxy VDOLIVE

Il permet aux utilisateurs de WinGate de visionner des vidéos en temps réel. Ce proxy est compatible avec les versions 3.22 et ultérieures de VDOLive player.

Remarque : ce standard est plus ancien que le proxy RTSP. Dans la plupart des cas, il est préférable d'utiliser VDOLive.

La procédure est simple :

1. Ouvrez GateKeeper.
2. Connectez-vous à l'aide du compte "Administrator".
3. Effectuez un clic droit dans l'onglet **Services** sélectionnez **Nouveau service - Service proxy VDOLive (New service - VDOLive proxy service)**



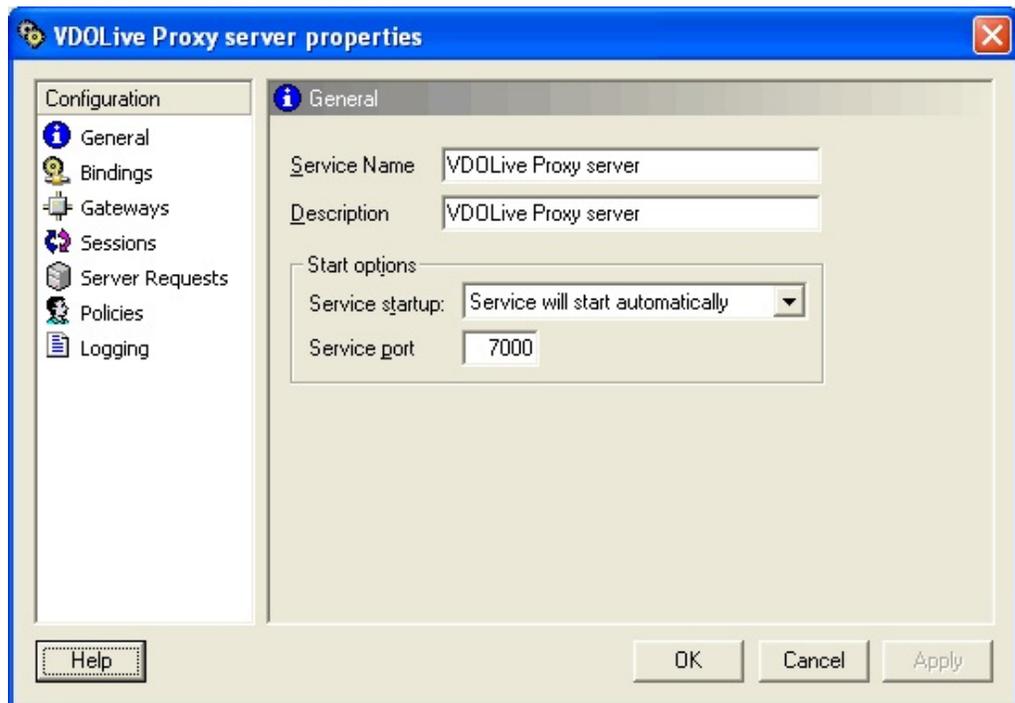
Masquer | Masquer toutes les images

4. Choisissez un **nom** et une **description**, ou conservez les valeurs par défaut.

5. Indiquez le numéro de port (par défaut : 7000).
6. Cliquez sur **OK**.

Si vous possédez sur votre réseau un serveur ainsi qu'un proxy VDOLive :

1. Cliquez sur l'onglet **Requêtes serveur (Server Requests)**
2. Cochez l'option **Rediriger la requête vers un serveur prédéterminé (Pipe request through to predetermined server)**



Masquer | Masquer toutes les images

3. Indiquez l'adresse et le numéro de port de l'ordinateur sur lequel se trouve votre serveur.

Proxy XDMA

WinGate inclut un proxy XDMA pour garantir un accès complet à Internet.

Veillez noter que Streamworks n'est plus géré par Xing Technology Corporation.

Nous vous recommandons d'utiliser le port 8000 par défaut pour ce proxy. Cette configuration s'effectue dans Streamworks.

Pour ajouter un proxy XDMA dans WinGate :

1. Dans GateKeeper : effectuez un clic droit dans l'onglet **Services** du panneau **Contrôle**
2. Cliquez sur **Nouveau service - Proxy XDMA** (*New service - XDMA Proxy*)

Masquer

3. Acceptez les paramètres ou modifiez le numéro de port puis cliquez sur **OK**.

Pour faire fonctionner un proxy XDMA dans Streamworks :

1. Dans le lecteur Streamworks, cliquez sur **Settings/Network...**
2. Cochez la case "**Use Application firewall**"
3. Entrez les valeurs :
 - Proxy Host: 192.168.0.1
 - Proxy Port: 8000
4. Cliquez sur **OK**

Remarque : ces paramètres sont stockés dans le fichier swplayer.ini du répertoire Streamworks.

Liens mappés

Les liens mappés sont sans doute la façon la plus simple de créer une passerelle.

Ils ne sont pas aussi flexibles que les services proxy car il s'agit d'un simple transfert de données. Vous devez donc indiquer à quel hôte distant l'ordinateur doit se connecter.

Vous pouvez configurer un hôte distant et un numéro de port sur chaque poste du réseau, ou bien choisir un hôte et un port par défaut pour tous les ordinateurs se connectant à la passerelle. Il est possible d'utiliser des liens mappés sur tous les réseaux TCP/IP : Internet, réseau WAN d'entreprise ou bien réseau local personnel/professionnel.

WinGate contrôle les données circulant sur ces liens et affiche les détails de la session de données formant le "lien". Les liens mappés TCP affichent dans l'onglet **Activité (Activity)** les données des sessions suivantes :

SMTP : envoi de courrier

POP3 : réception de courrier

NNTP : connexion aux serveurs de nouvelles

HTTP : navigation sur Internet

FTP : accès aux serveurs FTP

TELNET : connexion aux serveurs Telnet

Lorsque l'un des protocoles est utilisé via un lien mappé TCP, des détails s'affichent dans GateKeeper (à l'exception évidemment des commandes relatives aux mots de passe). Des détails supplémentaires sont fournis pour les sessions HTTP, POP3 et SMTP.

Exemple : lien mappé vers un serveur de nouvelles (les serveurs de nouvelles

utilisent le port port 119)

WinGate ne possédant pas de proxy pour ce service, vous devez utiliser un lien mappé. Pour cela, choisissez un serveur (par exemple : news.cnn.com) et un numéro de port (par exemple : 119). Créez alors un lien mappé sur le port 119 avec l'hôte par défaut : news.cnn.com, et assurez-vous qu'il soit activé.

Pour accéder aux nouvelles, vous vous connectez à 'wingate', et non à news.cnn.com, car vous communiquez avec le serveur par le biais de WinGate.

Il est possible de créer des mappages spécifiques selon l'utilisateur ou l'emplacement. Ainsi, les utilisateurs peuvent par exemple choisir des serveurs de nouvelles différents.

[Cliquez ici pour en savoir plus sur les mappages spécifiques](#)

Délais de déconnexion

Pour les services TCP (c.à.d. tous sauf DNS, XDMA, et mappages UDP) ces délais ne sont qu'une protection contre d'éventuels problèmes. En effet, les sessions se ferment automatiquement une fois terminées. Cependant, il peut arriver qu'elles restent ouvertes et inactives. Dans ce cas les délais permettent d'éviter d'occuper inutilement le modem.

Au contraire, les sessions UDP ne se ferment pas automatiquement. L'utilisation d'un délai de déconnexion est donc le seul moyen de les arrêter.

Ajouter un lien mappé

L'ajout d'un lien mappé (appelé également proxy ou service de mappage) est simple à effectuer : il suffit de suivre la procédure ci-dessous.

N'oubliez pas qu'un lien mappé ne peut se connecter qu'à un seul ordinateur, vous devez donc savoir avant de commencer de quel ordinateur il s'agit et le port que vous allez utiliser.

Sélectionnez tout d'abord le type de Socket (généralement **TCP**, mais certaines applications utilisent l'**UDP** - c'est à dire les services DNS - auquel cas vous en serez informé).

Suivez ensuite les étapes suivantes :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'onglet **Services** dans le panneau Contrôle.
4. Cliquez avec le bouton droit de la souris à l'intérieur de cet onglet et sélectionnez **Nouveau service** - puis **Service de mappage TCP (ou UDP) (New service - TCP/UDP mapping service)**.



Masquer

5. Indiquez le **numéro du port** à utiliser sur l'ordinateur local.
6. Sélectionnez **Activer le mappage par défaut sur (Enable default mapping to)**.
7. Indiquez le **nom** de l'ordinateur distant (par ex. : news.iprolink.co.nz).
8. Indiquez le **port** à utiliser sur l'ordinateur distant*
9. Cliquez sur **OK** .

* Il s'agit presque toujours du même port que pour l'étape 5.

Principaux mappages

Voici quelques exemples de mappages ainsi que leur fonction.

Service	Port	Fonction
Internet/Usenet News	119	Configure un lien mappé TCP sur le port 119 avec votre serveur de nouvelles sur le même port.
IRC Chat	6667	Configure un lien mappé TCP sur le port 6667 avec votre serveur IRC sur le même port.
SMTP (envoi de courrier)	25	Configure un lien mappé TCP sur le port 25 avec votre serveur SMTP sur le même port.
DNS	53	Configure un lien mappé UDP vers un serveur DNS (probablement celui de votre FAI) sur le port 53. Peut remplacer le service DNS de WinGate.

Voir également :

[Ajouter un mappage spécifique](#)

Ajouter un mappage spécifique

Si vous utilisez un mappage par défaut, cela signifie que tout ordinateur de votre réseau se connectant au numéro de port correspondant sera dirigé vers le poste que vous avez indiqué. Or, il peut arriver qu'un utilisateur souhaite se connecter à un serveur différent sur ce port.

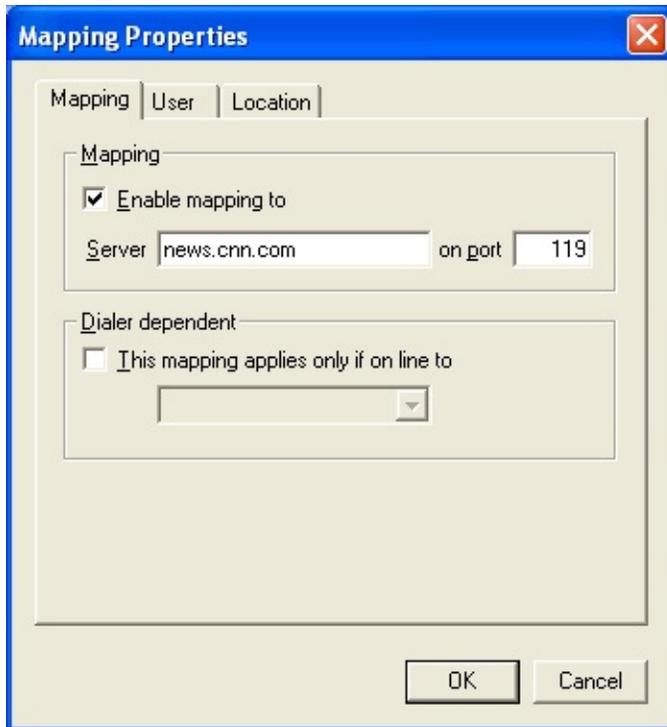
Vous pouvez pour cela configurer des mappages spécifiques par **adresse IP**, **utilisateur** ou **profil de connexion**.

Mappage par adresse IP

Exemple : Un utilisateur travaille sur le poste 192.168.0.5 et souhaite utiliser news.cnn.com au lieu du serveur de nouvelles par défaut. Voici la procédure à suivre pour modifier son mappage :

1. Ouvrez **GateKeeper**.
2. Connectez-vous avec le compte Administrator.
3. Double-cliquez sur le lien mappé que vous souhaitez modifier (dans l'onglet **Services** du panneau Contrôle).
4. Cliquez sur l'icône **Mappages (Mappings)**, puis sur **Ajouter**.
5. Une nouvelle fenêtre s'ouvre : indiquez-y le nom du **serveur** (ici : news.cnn.com).
6. Saisissez le numéro de **port** à utiliser (119 pour les nouvelles).
7. Cliquez sur l'onglet **Emplacement (Location)** et indiquez 192.168.0.5.
8. Cliquez sur **OK**.

Exemple



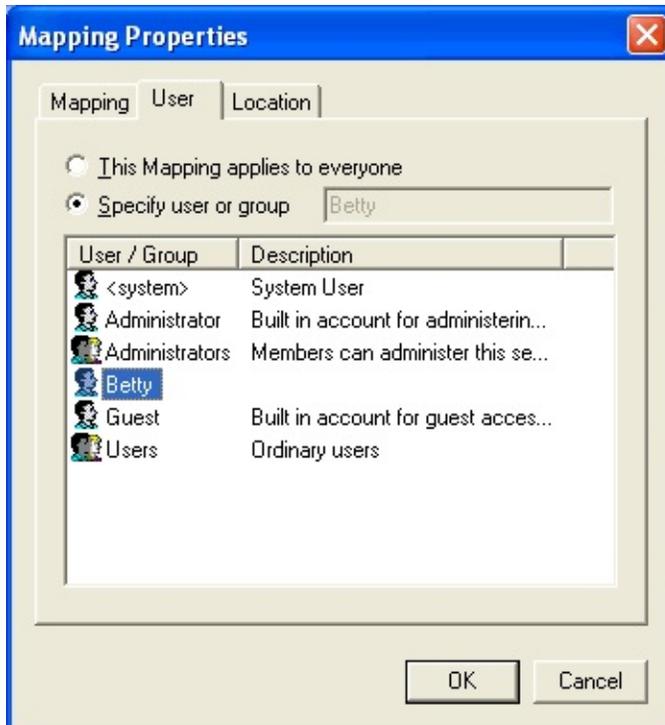
Masquer | Masquer toutes les images

Mappage par nom d'utilisateur

Exemple : Un utilisateur n'emploie pas le serveur de nouvelles par défaut mais news.domaine.com. Voici la procédure à suivre pour modifier son mappage :

1. Double-cliquez sur le lien mappé que vous souhaitez modifier.
2. Cliquez sur l'icône **Mappages**, puis sur **Ajouter**.
3. Une nouvelle fenêtre s'ouvre : indiquez-y le nom du **serveur** (ici : news.domaine.com)
4. Saisissez le numéro de **port** à utiliser (119 pour les nouvelles).
5. Cliquez sur l'onglet **Utilisateur** et indiquez le nom de cet utilisateur.
6. Cliquez sur **OK** .

Exemple



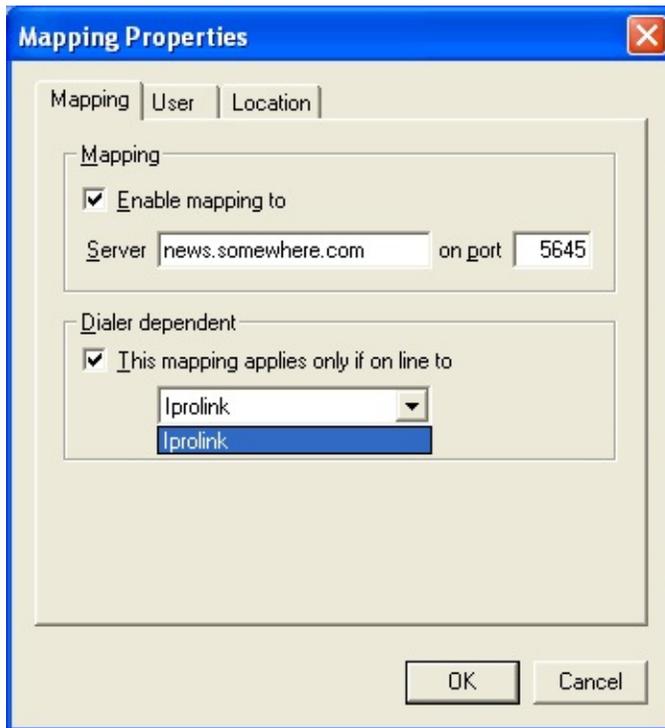
Masquer | Masquer toutes les images

Mappage par profil de connexion

Si vous disposez de deux profils de connexion, utilisant deux FAI différents, et que vous souhaitez configurer un serveur de nouvelles pour chaque profil :

1. Double-cliquez sur le lien mappé du serveur de nouvelles que vous souhaitez modifier.
2. Le mappage par défaut est normalement celui du serveur de nouvelles du premier FAI.
3. Cliquez sur l'icône **Mappages**, puis sur **Ajouter**.
4. Dans la nouvelle fenêtre, cochez l'option **Ne s'applique qu'avec la connexion suivante (This mapping applies only if online to)** puis sélectionnez le deuxième FAI dans la liste déroulante.
5. Indiquez le nom du serveur de nouvelles du deuxième FAI.
6. Indiquez le numéro de **port** à utiliser (ici : 5645).
7. Cliquez sur **OK** .

Exemple



Masquer | Masquer toutes les images

Liens mappés : fonctionnalités avancées

Les liens mappés sont plus limités que les autres proxies sous certains aspects mais plus flexibles sous d'autres :

Ils peuvent être établis selon les besoins de chaque utilisateur et paramétrés en fonction du nom de l'utilisateur, de l'adresse IP ou du profil de connexion.

Il est possible de crypter les mappages TCP (c'est à dire sécuriser les données transmises de façon à ce que seul le destinataire puisse les décoder).

Configuration d'un mappage crypté

Permet de sécuriser les données transférées par le biais des liens mappés de WinGate.

De nombreuses entreprises possèdent des serveurs de messagerie, Telnet, HTTP ou FTP dont le contenu (souvent confidentiel) est à disposition des employés et/ou des clients.

Or, ces informations sont transmises en clair. Cela signifie qu'une personne mal intentionnée munie d'un "sniffeur" de paquets peut intercepter les mots de passe et accéder aux données.

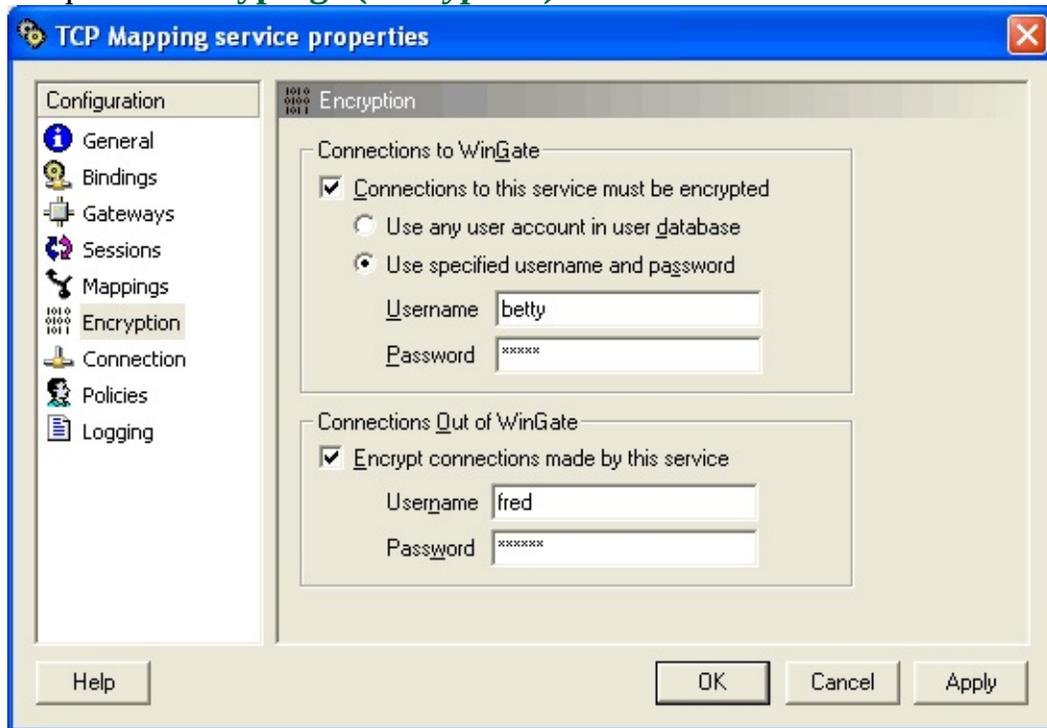
Afin d'assurer un accès sécurisé à leurs serveurs, certaines entreprises ont recours à des lignes louées ou des serveurs commutés afin que les communications ne s'effectuent pas sur Internet. Toutefois, cette solution s'avère souvent très onéreuse.

Avec WinGate, vous pouvez crypter toutes les données envoyées depuis votre réseau sur Internet ou un réseau externe. Elles sont transmises à un autre serveur WinGate, puis décodées (ne fonctionne qu'avec les liens mappés). Cette fonctionnalité permet donc aux entreprises d'assurer un accès sécurisé à leurs serveurs.

Ajouter un lien mappé crypté

1. [Ajoutez un lien mappé TCP](#), et attribuez-lui un nom (par ex. : "lien TCP crypté")

2. Sélectionnez un **port**. Il est généralement plus sûr d'utiliser des ports **supérieurs à 10 000**.
3. Cliquez sur **Cryptage (Encryption)**.



Masquer

4. Choisissez les options souhaitées pour les connexions entrantes et sortantes.

Exemple 1 - Accès sécurisé à des serveurs de fichiers

Vous possédez deux bureaux : l'un à Paris et l'autre à Londres, et souhaitez accéder en toute sécurité aux fichiers se trouvant sur le serveur à Londres.

Procédure à suivre :

A Londres :

1. Installez un serveur web sur le serveur de fichiers.
2. Créez un lien mappé dans WinGate (par exemple sur le port 3080) avec ce serveur.

A Paris :

1. Créez un lien mappé sur le port 3080, avec le serveur WinGate de Londres.
2. Pour accéder aux fichiers contenus sur le serveur, il suffit d'indiquer l'URL suivante dans votre navigateur : `http://wingate:3080`

Le navigateur se connecte au serveur WinGate de Paris, qui effectue une connexion cryptée avec celui de Londres afin d'accéder au serveur web. Il est alors possible d'explorer le serveur et de télécharger les fichiers souhaités.

Si votre serveur web est compatible avec la méthode **PUT**, vous pourrez même envoyer des fichiers sur le serveur (téléchargements montants).

Exemple 2 - Accès sécurisé sous Unix

Vous possédez un serveur Unix et souhaitez que vos employés en déplacement (ou même à domicile) puissent y accéder de façon sécurisée.

Procédure à suivre :

Ordinateur principal :

1. Créez un lien mappé crypté (par exemple sur le port 3023) relié au serveur Telnet Unix sur le port 23.

Ordinateur distant :

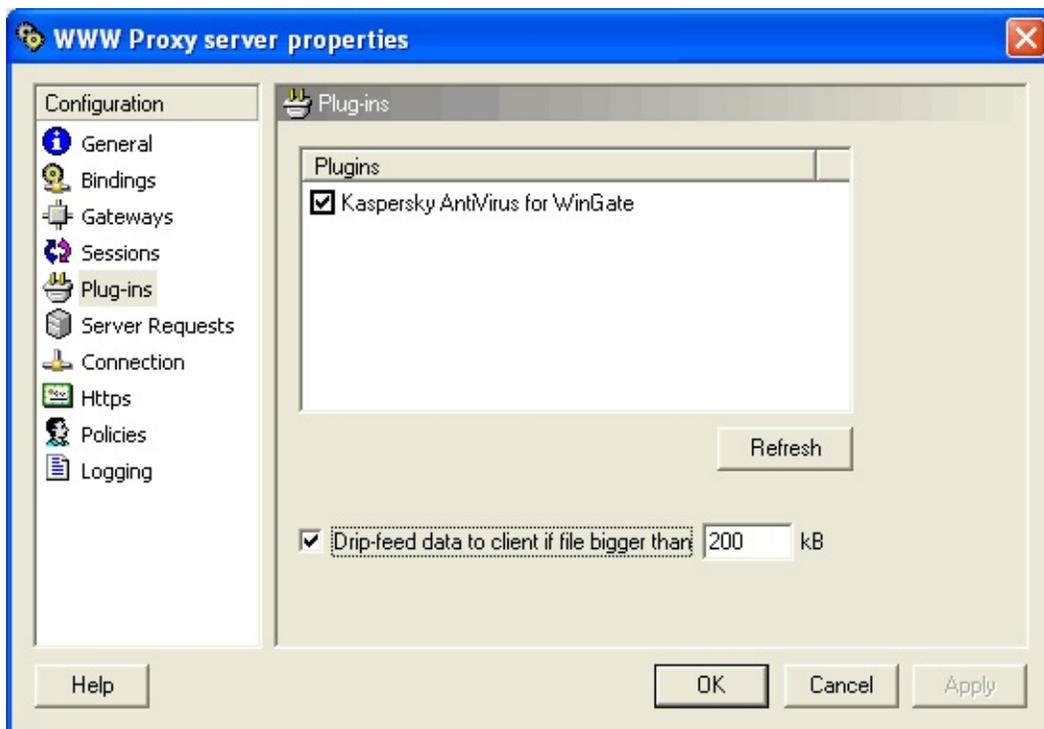
1. Créez un lien mappé crypté sur le port 3023 relié à l'ordinateur principal (sur le port 3023).

Pour se connecter au serveur de l'ordinateur principal, il suffit de se connecter à WinGate sur le port 3023 par le biais du protocole Telnet. Une invite de commandes s'affiche ensuite mais toutes les communications sont cryptées.

©2004 Qbik New Zealand Limited

Modules (*Plug-ins*)

En cliquant sur l'icône **Modules**, vous pouvez activer ou désactiver les modules installés pour chaque service : il suffit de cocher ou décocher la case correspondante.



Masquer

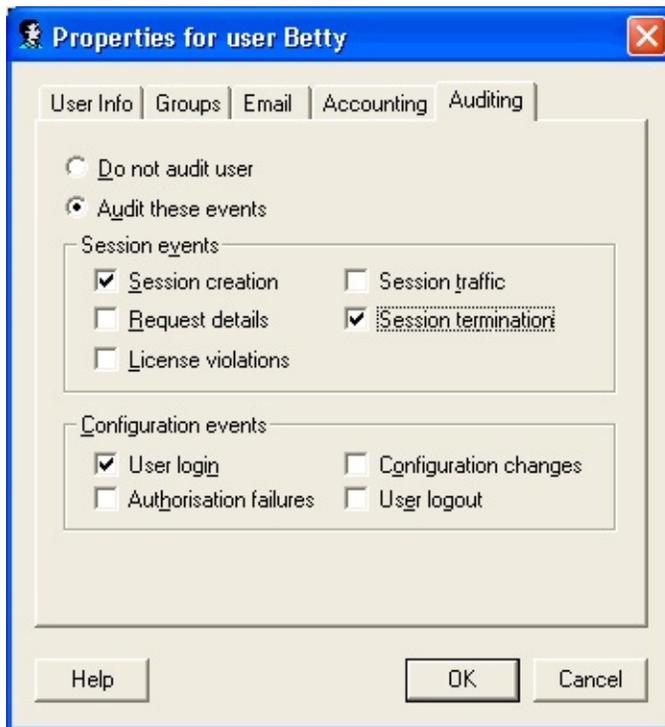
**Transmettre au client les données analysées si le fichier est supérieur à x Ko
(*Drip-feed data to client if file bigger than 'x' kB*)**

Si vous cochez cette option, une partie des données est envoyée au client au cours de l'analyse du fichier. Ainsi, les clients tels que Outlook ou Internet Explorer ne se déconnectent pas automatiquement.

Audits et fichiers journaux

WinGate dispose de fonctionnalités permettant de surveiller son activité :

- Onglet **Audit (Auditing)** dans les propriétés des utilisateurs.

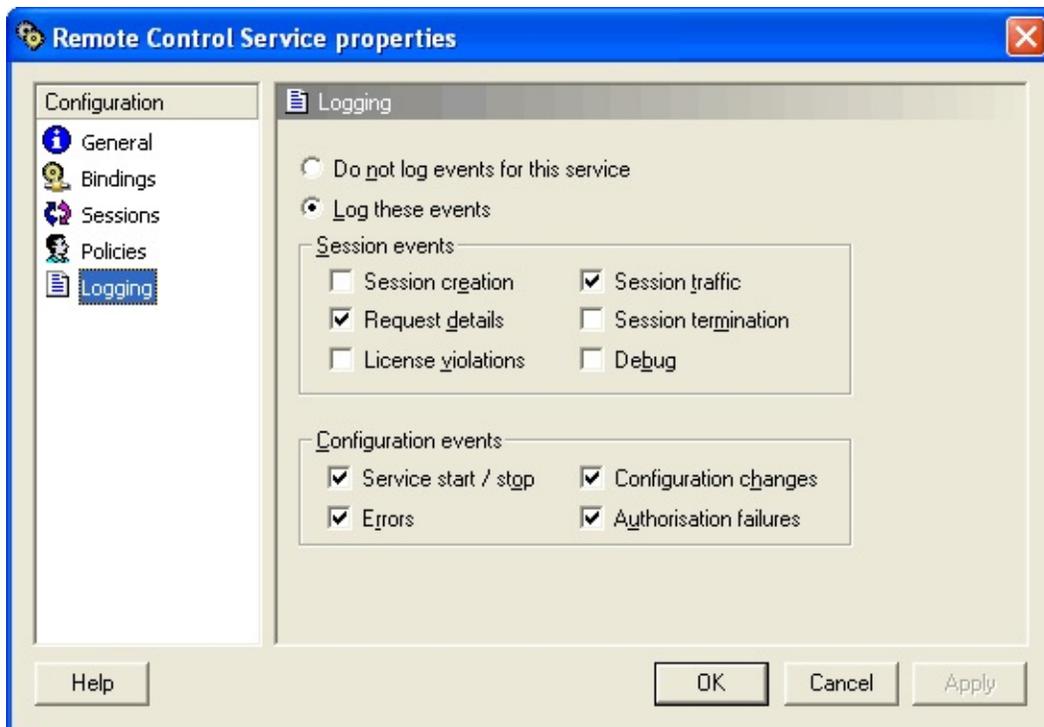


Masquer | Masquer toutes les images

Par défaut, les audits des utilisateurs sont enregistrés dans le fichier :

%WinGate%\audit\nomdel'utilisateur.log

- Icône **Journalisation (Logging)** dans les propriétés des services.



Masquer | Masquer toutes les images

Par défaut, les fichiers journaux des services sont enregistrés dans le fichier :
 %WinGate%\logs\nomduservice.log.

L'activité des utilisateurs est enregistrée dans les fichiers d'audit, et celle des services dans les fichiers journaux,

tous deux sous un format délimité par des tabulations.

Vous pouvez les consulter dans un éditeur de texte ou à l'aide du [Serveur de fichiers journaux \(Logfile Server\)](#).

Le format des fichiers est le suivant :

Date	Heure	Adresse IP	Numéro de session	Type d'évènement	Détails évènement
12/02/96	15:01:25	192.168.0.1	0000006100	Modification	utilisateur John

Les évènements des fichiers journaux/audits sont divisés en deux parties. Différentes options sont à la disposition des administrateurs ; vous trouverez ci-dessous la configuration par défaut.

Évènements de session

Type d'évènement	Paramètres par défaut	Description
Création	Désactivé	Enregistre les détails concernant la création des sessions (le type de service est mentionné, par ex. :http). Cette option est souvent utilisée pour rechercher la source d'un problème.
Fermeture	Désactivé	Arrête toutes les sessions en cours, ce qui peut s'avérer utile si vous rencontrez des problèmes lors de la fermeture. Il est également possible d'identifier une session spécifique à partir de sa création et d'effectuer une requête pour l'arrêter.
Détail des requêtes	Activé	Enregistre le détail des requêtes de chaque session. Pour les sessions en http, les URL demandées seront conservées.
Débogage	Désactivé	Enregistre les éventuels messages de débogage.
Violations de la licence	Désactivé	Toute violation de la licence est enregistrée.
Trafic	Activé	Enregistre les informations concernant le trafic : envoyé à, reçu de, envoyé pour, reçu pour (en octets) ainsi que le nombre de secondes en ligne.

Évènements de configuration

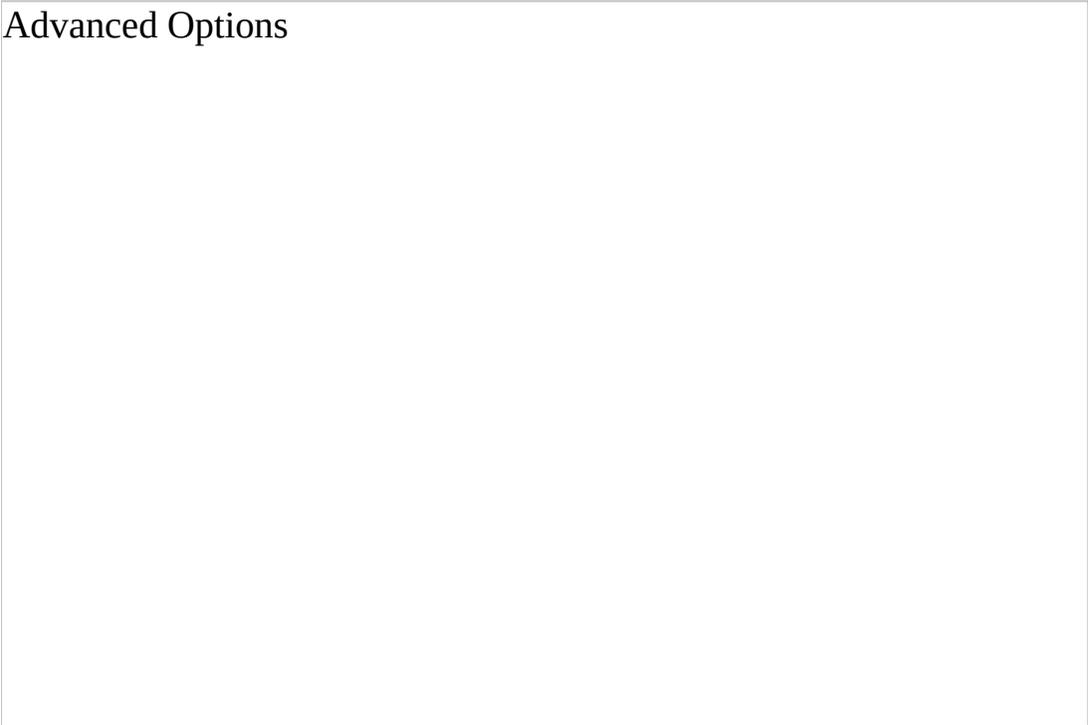
Type **Paramètres par**

d'évènement	défaut	Description
Autorisation refusée	Activé	Si un utilisateur saisit un mot de passe incorrect, l'évènement est enregistré.
Erreurs	Activé	Enregistre les détails concernant toutes les erreurs.
Démarrage/arrêt du service	Activé	Le démarrage et l'arrêt du service sont consignés dans le fichier.
Changements de configuration	Activé	Toute modification apportée aux paramètres d'un service/utilisateur est enregistrée.
Connexion utilisateur	Activé	La connexion de chaque utilisateur est consignée.
Déconnexion utilisateur	Activé	La déconnexion de chaque utilisateur est consignée.

Options avancées (*Advanced options*)

Dépannage (*Troubleshooting*)

Advanced Options



Masquer | **Masquer toutes les images**

Rapport de configuration (*Configuration Report*)

Affiche un rapport contenant la configuration actuelle de WinGate et des informations comme : le numéro de version, les interfaces réseaux, la configuration des services, etc. Il est possible d'enregistrer ce rapport dans un fichier texte en cliquant sur **Enregistrer le rapport (*Save report*)**.

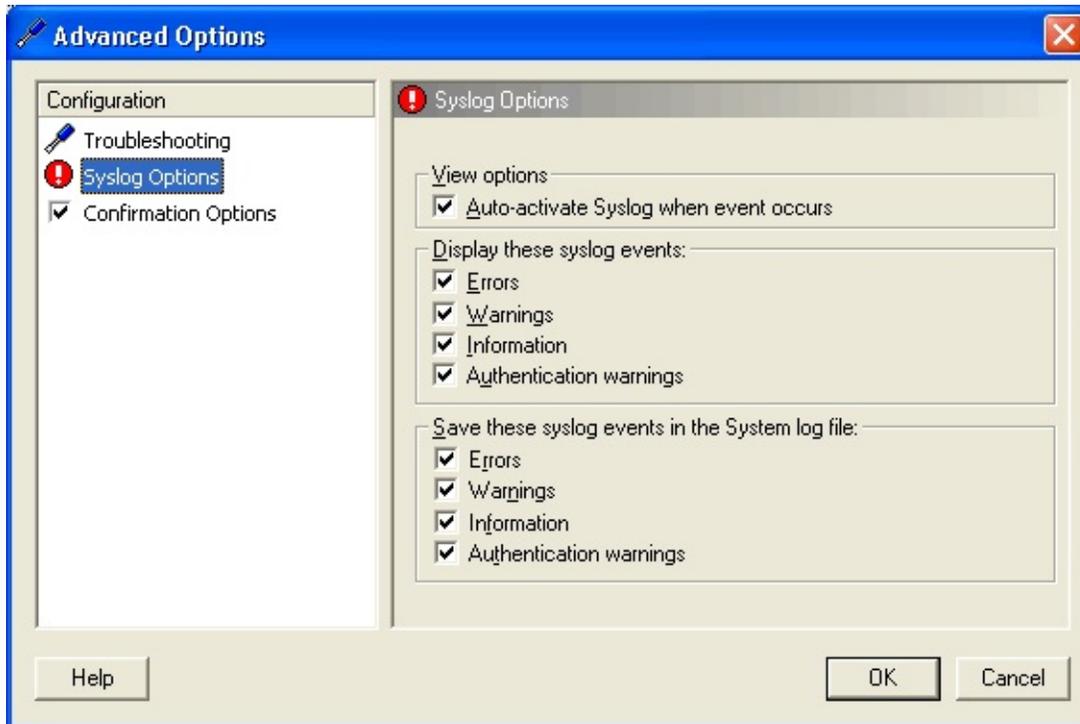
La liste déroulante contient divers éléments qu'il est possible d'inclure (ou pas) dans le fichier. Il suffit pour cela de cocher les cases correspondantes.

Sauvegarder les paramètres du registre (*Save Registry Settings*)

Cliquez sur ce bouton pour enregistrer les paramètres actuels du registre dans le fichier de votre choix. Cette fonctionnalité est utilisée afin d'examiner la configuration de WinGate ou bien d'effectuer une sauvegarde avant de la modifier. Ce bouton ne s'affiche que lorsque GateKeeper est exécuté sur le poste

serveur.

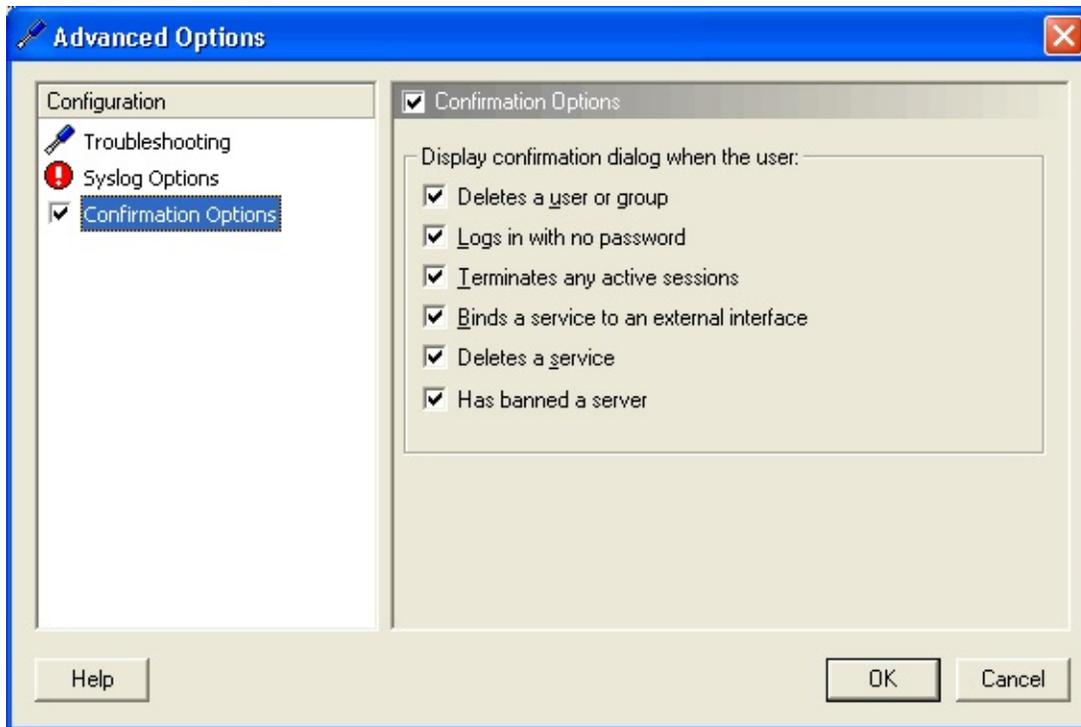
Journal système (Syslog Options)



Masquer | Masquer toutes les images

Configurez ici la façon dont s'affichent les événements dans l'onglet [Messages système \(System Messages\)](#) de GateKeeper et le type d'évènements enregistrés.

Options de confirmation (Confirmation Options)



Masquer | Masquer toutes les images

Vous pouvez choisir d'afficher un message de confirmation lorsqu'un utilisateur modifie la configuration de WinGate.

Messages système

Message	Composant	ID	
NO VALID LICENCE REVERT TO ONE USER	Moteur	(0x0001)	<p>La vérification de la licence au mode "utilisateur unique" (sing Cet utilisateur devant être local serveur.</p> <p>Si vous possédez des licences v fonctionner.</p> <p>Dans le cas contraire vous deve sur votre réseau. Si vous pensez contacter votre revendeur.</p>
NO CONFIG FOUND USING DEFAULT	Moteur	(0x0004)	<p>Aucune information concernant registre. WinGate va utiliser les</p>
NO SNMP SUPPORT	Moteur	(0x0005)	<p>Erreur lors de l'initialisation du SNMPAPI.DLL soit absent de v corrompu.</p> <p>De nombreuses fonctionnalités support SNMP.</p> <p>Le SNMP est normalement inst</p>
INTERNAL DIALER RESTART	Moteur	(0x0006)	<p>Les requêtes envoyées au comp inconnues trop important.</p> <p>Le composeur va redémarrer.</p>
			<p>Erreur lors de l'initialisation du</p> <p>Le fichier ICMP.DLL est absen</p>

NO ICMP SUPPORT	Moteur	(0x0007) corrompu. De nombreuses fonctionnalités sans support ICMP, en particulier ping pour vérifier les adresses I
AFFINITY SETTING	Moteur	(0x0008) L'affinité du processus a été out
SCHEDULED SYSTEM REMINDER	Moteur	(0x0009) Message système du Programm
SCHEDULED REMINDER	Moteur	(0x000A) Message de rappel programmé déconnecter. Fermeture du syst
TRIAL LICENCE EXPIRED	Moteur	(0x000B) Votre période d'évaluation est e précédente.
OLD LICENCE	Moteur	(0x000C) La version de votre licence est : certaines fonctionnalités ne son
NO ROUTE TO INTERNET	Moteur	(0x000D) Pas de profil de connexion ni de WinGate en tant que passerelle Internet.
AUTOUPDATE CURRENT	Moteur	(0x000E) Vérification de la version : pas
AUTOUPDATE NEWER AVAILABLE	Moteur	(0x000F) Vérification de la version : une
AUTOUPDATE FAILED	Moteur	(0x0010) Vérification de la version : éche

NEED MANUAL DNS	Moteur	(0x0012)	Les serveurs DNS doivent être
DNS CACHE DISABLED	Moteur	(0x0014)	Échec et désactivation du cache surcharge. Les requêtes sont toutes en local : des messages sont envoyés.
INTERFACE DETECTED	Moteur	(0x0015)	Nouvelle interface détectée.
WWW CACHE CANNOT OPEN CACHE FILE	Cache	(0x0016)	Impossible d'ouvrir l'index de la cache.
NO PRO LICENCE BUT OTHER USERS	Base de données d'utilisateurs	(0x0101)	Des utilisateurs ne faisant pas partie de la licence ne vous permet pas d'utiliser ce produit. Cela se produit généralement lors de l'installation de la licence Standard après avoir utilisé une licence Standard. Pour ne plus obtenir ce message, modifiez le registre, dans : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Winlogon\Parameters\LegalNoticeCaption Supprimez toutes les entrées sautées par l'Administrateur. Si ces clés sont supprimées par erreur, vous pouvez les recréer à nouveau, mais les informations ne peuvent pas être rétablies.
DEFAULT USER NOT FOUND CREATED	Base de données d'utilisateurs	(0x0102)	Un compte par défaut (Administrateur) n'a pas été créé. Cela peut se produire si vous avez supprimé le compte par défaut de vos paramètres ont été perdus.
DEFAULT GROUP NOT FOUND	Base de données	(0x0103)	Un groupe par défaut (Administrateurs) n'a pas été créé. Cela peut se produire si vous avez supprimé le groupe par défaut de vos paramètres ont été perdus.

CREATED	d'utilisateurs		vos paramètres ont été perdus.
NT INTEGRATION BUT NO 4 LICENSE	Base de données d'utilisateurs	(0x0104)	Vous avez sélectionné l'option c vous ne pouvez l'utiliser que si ultérieure.
REMOTE CONTROL SERVICE NOT FOUND CREATED	Services	(0x0201)	Le Service d'administration à di manquant et a été ajouté. Cela peut se produire si vous dé vos paramètres ont été perdus.
AUTHENTICATION ACCESS PERMISSION DENIED	Authentification	(0x0301)	Un utilisateur a essayé d'effectue WinGate. Il est parfois nécessaire de vérif souhaitées.
CONNECTOID REMOVED	Composeur	(0x0401)	Un profil de connexion a été su plus disponible dans WinGate. Pour les versions Standard et Pi Certains paramètres dépendent vérifier : 1. Si dans les paramètre que connexion princij 2. Le profil configuré pc 3. Si des mappages TCF 4. Si aucune règle n'a de
CONNECTOID ADDED	Composeur	(0x0402)	Nouveau profil de connexion di WinGate, modifiez les paramètr
			Aucune interface disponible n'a Le service ne fonctionnera pas.

NO VALID INTERFACES AVAILABLE	Services	(0x0501)	<p>N'oubliez pas que :</p> <ul style="list-style-type: none"> • Le DNS ne peut pas être lié à l'interface • Le service DHCP ne peut pas être utilisé si l'adresse est attribuée automatiquement
BINDING OPTION INVALID FOR SERVICE)	Services	(0x0502)	<p>La méthode de liaison est invalide. Le service va effectuer automatiquement :</p> <ol style="list-style-type: none"> a) valide pour ce type de service b) NON accessible depuis l'interface
NO SPECIFIC BINDING SPECIFIED	Services	(0x0503)	<p>Les options de liaison du service sont définies dans l'interface, mais celle-ci n'est pas valide. Le service va effectuer automatiquement :</p> <ol style="list-style-type: none"> a) valide pour ce type de service b) NON accessible depuis l'interface
BINDING NO LONGER AVAILABLE	Services	(0x0504)	<p>WinGate a déterminé qu'une liaison a été supprimée de la liste pour ce service. Cela se produit généralement lorsque :</p> <ol style="list-style-type: none"> 1. Une interface a été supprimée 2. Votre adresse IP a été attribuée automatiquement par WinGate
BINDING NOT VALID FOR SERVICE	Services	(0x0505)	<p>WinGate a déterminé qu'une liaison n'est plus valide. Elle a donc été supprimée de la liste. Ce message s'affiche parfois si l'adresse n'est pas attribuée automatiquement ou fixe.</p>

START UP ERROR	Services	(0x0506)	Échec lors du démarrage du service DHCP. Le service DHCP n'est lié à aucune interface réseau. Les adresses IP privées sont des adresses réservées sur Internet. Il est vivement recommandé d'utiliser des adresses IP publiques. Le service DHCP de WinGate a été configuré sur l'adaptateur réseau connecté au serveur DHCP.
DHCP NO PRIVATE INTERFACES BOUND	Service DHCP	(0x0601)	Le serveur DHCP a reçu une requête pour des adresses IP publiques mais sa configuration est configurée pour des adresses IP privées. Par mesure de sécurité, le serveur DHCP refuse de fournir des adresses IP publiques. Si vous utilisez des adresses IP publiques, vous devez : 1. Modifier la configuration de votre serveur DHCP pour lui permettre de fournir des adresses IP publiques (à l'aide du serveur DHCP) OU 2. Modifier les paramètres de votre serveur DHCP pour lui permettre de fournir des adresses IP publiques. Dans ce cas, vérifiez également que votre serveur DHCP soit lié à aucune interface réseau avec votre FAI.
DHCP CLIENT DENIED NON PRIVATE ALLOCATION	Service DHCP	(0x0602)	
DHCP ACCESS DENIED	DHCP	(0x0603)	L'accès au serveur DHCP a été refusé. S'il s'agit d'un poste de votre réseau local, vérifiez que le service DHCP est activé sur votre carte réseau, ou bien modifiez ses paramètres.
DHCP NO			

ACCEPTABLE OFFER AVAILABLE	DHCP	(0x0604)	Le serveur DHCP n'a pas pu en
BAD NAT DRIVER VERSION	NAT	(0x0701)	Le pilote utilisé pour fournir le version de WinGate. Le pilote doit être mis à jour.
NAT NETWORK ADAPTOR CHANGE	ENS	(0x0702)	Une modification a été détectée risque de ne pas fonctionner cor Lancez l'Assistant Configuratio (démarrer/Programmes/Accesso
ENS DRIVER/NAT REFUSED LOAD (BOOT SAFETY)	ENS	(0x0703)	Le pilote ENS a refusé de déma plusieurs échecs de démarrage c Par mesure de sécurité, le pilote démarrage. Cela permet d'évite Différents facteurs peuvent être Si vous avez récemment installé WinGate cela signifie que le pil matériel de votre ordinateur. <ul style="list-style-type: none"> • Si le service ENS fonctionnait c nouveau logiciel sur votre ordi parfois de redémarrer le service • Si vous avez éteint l'ordinateur l'avoir allumé, vous avez peut-ê moteur de WinGate et le pilote
ENS DRIVER FAILED TO LOAD (UNKNOWN REASON)	ENS	(0x0704)	Le pilote ENS n'a pas pu démar Signifie que le pilote est manqu système d'exploitation. Le fichi choisi de ne pas le lancer lors d commence par "QbikHk").

			Si vous n'avez pas démarré en r service ENS, ou bien contactez
NAT BUFFERS EXHAUSTED	ENS	(0x0705)	Le pilote ENS manque de mém avec le fonctionnement du rése Toutes les fonctionnalités de ce disponibles.
NAT MANUALLY DISABLED	ENS	(0x0706)	Le pilote ENS a été désactivé n <ol style="list-style-type: none"> 1. Ouvrez GateKeeper 2. Assurez-vous que l'op Network Driver) soit 3. Cliquez sur OK. 4. Redémarrez l'ordinateur
There is no Administrator password, this service is being reconfigured for local access only	Service d'administration à distance <i>(Remote Control Service)</i>	(0x0801)	Le compte Administrator ne po sécurité, le service a été reconfi poste local. Si vous souhaitez que ce service devez indiquer un mot de passe
VPN ACCESS TO DOMAIN DENIED	VPN	(0x0901)	Un utilisateur a essayé d'accéder refusé.
INFO NTUDB REFLECTED	Base de données d'utilisateurs	(0x0A01)	La base de données d'utilisateur groupes ont été ajoutés à la base
INFO NTUDB NET API 32 DLL LOAD FAIL	Base de données d'utilisateurs	(0x0A02)	Erreur lors de la synchronisation fichier NETAPI32.DLL est peu pas effectuer de synchronisation

INFO COMPONENT NOT SUPPORTED		(0x0B01)	Le composant \"(Composant(s) votre système.
SMTP RELAY DENIED	Serveur de messagerie	(0x0c01)	Une tentative de relais a été dét il peut s'avérer nécessaire de pr
SMTP SILENT DISCARD	Serveur de messagerie	(0x0c02)	Une tentative de relais a été dét de tentatives répétées, il peut s' contre leurs auteurs.
SMTP PROBE EMAIL RELAYED	Serveur de messagerie	(0x0c02)	Une tentative de relais a été dét serveur SMTP apparaîtra en tan devez bloquer les relais au lieu
FIREWALL ATTACK BLOCKED	Pare-feu	(0x0c04)	Le pare-feu a bloqué une tentati port.....attaque de virus connu
PLUGIN LICENSE INVALID	Modules	(0x0c05)	La licence de %s a expiré ou es disponibles.
SMTP OPEN RELAY BLOCKED	Serveur de messagerie	(0x0c06)	
SMTP DETECTED NON PROXY REQUEST	Serveur de messagerie	(0x0c07)	
SMTP DEFAULTING TO COMPUTERNAME	Serveur de messagerie	(0x0c08)	
HISTORY CORRUPTED	Moteur	(0x0c09)	

©2005 Qbik New Zealand Limited

Configuration avancée

La configuration avancée s'effectue à l'aide du registre, avec regedit.exe ou regedt32.exe.

Ces opérations doivent être effectuées avec précaution car il est difficile de les annuler.

Il est recommandé de sauvegarder le registre de WinGate avant de le modifier.

Clés du registre

Tous les paramètres sont enregistrés sous la clé :

HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik Software\Wingate

dont voici quelques détails :

Clé	Description
Cache	Contient les paramètres du cache.
Default rights	Droits par défaut. Si vous bloquez accidentellement l'accès aux droits d'accès de modification ou de démarrage des services, il suffit de modifier l'entrée correspondante pour rétablir les droits par défaut.
DHCP (NE PAS MODIFIER)	Contient les baux attribués par le serveur DHCP, ainsi que le détail des utilisateurs présumés en fonction du nom de l'ordinateur.
ErrorStrings	Chaînes des messages. Vous pouvez personnaliser les valeurs qu'elles contiennent mais prenez garde de ne pas modifier le nom de la valeur.

Voir détails ci-dessous.

Locations

Contient le détail des utilisateurs présumés en fonction de l'adresse IP.

MimeTypes

Les valeurs sont enregistrées au format **Nom** <nomdel'extension> **Valeur** <typedemime>.

Par exemple, le type de mime GIF sera enregistré sous le nom GIF et la valeur image/gif. Pour créer de nouveaux types il suffit d'ajouter le nom de l'extension et une icône au répertoire des ressources.

Services

Contient tous les services de WinGate.

Settings

Contient les répertoires utilisés pour les audits, la journalisation et la mémoire cache.

Audit Files

Pour modifier le répertoire des fichiers d'audit, ouvrez :

HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik Software\Wingate\Settings\

et créez une valeur appelée AuditDirectory. Configurez ensuite le chemin souhaité.

Clés appelées **FormatX** contenant la liste des noms de sites recherchés lorsque WinGate reçoit des requêtes HTTP.

Procédure:

1. WinGate recherche le site '%s', (par exemple qbik)
2. S'il ne le trouve, il lit la valeur Format0 et remplace "%s", par exemple qbik.com

3. La procédure continue jusqu'à ce qu'un site soit trouvé ou qu'il n'y ait plus de formats.

"%s" représente le site requis.

HTTPSearchOrder

La clé HTTPSearchOrder contient normalement les entrées suivantes :

```
"Format0"="www.%s.com"
```

```
"Format1"="%s.com"
```

```
"Format2"="www.%s"
```

Exemple de recherche complète :

```
"Format0"="www.%s.com"
```

```
"Format1"="%s.com"
```

```
"Format2"="www.%s"
```

```
"Format3"="www.%s.net"
```

```
"Format4"="%s.net"
```

```
"Format5"=" www.qbik.com/Titles?qt=%s"
```

Log Files

Pour modifier le répertoire des fichiers journaux des services, ouvrez :

```
HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik  
Software\WinGate\Settings\
```

et créez une valeur appelée LogFileDirectory.
Configurez ensuite le chemin souhaité.

Pour modifier le répertoire des fichiers de la mémoire cache :

Cache directory

HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik
Software\WinGate\Cache\

et créez une valeur appelée CacheDirectory.
Configurez ensuite le chemin souhaité.

Remarque concernant les chemins :

Si vous utilisez un lecteur réseau, vous devez employer un nom UNC. En effet, la lettre désignant le nom du lecteur n'est valide que lorsqu'un utilisateur est connecté.

Messages d'erreur

Liste des messages d'erreur pouvant être modifiés :

[HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik
Software\WinGate>ErrorStrings\HTTP]

"AccessDeniedTitle"="Access Denied"

"AccessDeniedDescription"="You do not have sufficient rights for access to this resource"

[HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik
Software\WinGate>ErrorStrings\SocketErrors]

"HostnameLookupFailed"="Host name lookup for '%s' failed"

"RecvLineTimeout"="Timeout in recvline function"

[HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik
Software\WinGate>ErrorStrings\SOCKS]

"AccessDenied"="SOCKS4 connect to %s:%u failed - denied by SOCKS server"

"NoResponse"="SOCKS4 connect to %s:%u failed - no response from SOCKS server"

[HKEY_LOCAL_COMPUTER\SOFTWARE\Qbik Software\WinGate\ErrorStrings\SSL]

"BadResponse"="SSLTunnelling connect to %s:%u failed - bad response from HTTP server"

Autres clés

Attention :

Il est déconseillé de modifier les clés suivantes. Nous vous recommandons de configurer les services à l'aide des Outils d'administration de Windows et de désinstaller WinGate si vous souhaitez supprimer le service.

Windows 95/98

La clé suivante permet d'exécuter WinGate en tant que service :

HKEY_LOCAL_COMPUTER\SOFTWARE\Microsoft\Windows\Current version\Run Services\WinGate

Si vous la supprimez, WinGate ne se lancera pas au démarrage de Windows.

Windows NT/2000

Les informations concernant le service WinGate sont enregistrées dans :

HKEY_LOCAL_COMPUTER\SYSTEM\CurrentControlSet\Services\WinGateE

Toutes les versions de Windows :

HKEY_LOCAL_COMPUTER\Software\Microsoft\Windows\CurrentVersion\App Paths\gatekeeper.exe : chemin d'accès à GateKeeper.

HKEY_CURRENT_USER\Software\Qbik Software\GateKeeper : paramètres de GateKeeper.

Informations complémentaires

Si vous bloquez par accident votre accès à GateKeeper, ne réinstallez pas WinGate.

Deux facteurs peuvent être en cause :

1. Votre compte est corrompu. Si tel est le cas, connectez-vous en tant qu'Administrator et modifiez votre compte, ou bien supprimez l'entrée du registre. Si le compte Administrator est corrompu supprimez son entrée du registre.
2. Vous avez bloqué l'accès pour votre propre compte. Connectez-vous en tant qu'Administrator et rétablissez les droits d'accès, ou bien modifiez le registre afin de supprimer les règles qui vous empêchent d'accéder à GateKeeper (règles du Service d'administration à distance (*Remote control service*) et politique système (*System policies*)).

L'article "The Bug Report" publié dans le magazine InfoWorld du 10/20/97 (page 31), décrit une modification du registre pour les utilisateurs de Novell NetWare Client 32 et Internet Explorer 4. IE 4 fonctionne avec les serveurs proxy en ajoutant la clé :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings\DontU
= (REG_DWORD) 1.

Diverses options en ligne de commande sont disponibles avec le fichier **WinGate.EXE**.

Pour afficher la liste de ces options, saisissez : wingate.exe -? dans l'invite de commandes.

L'une de ces options est -clean.

Elle a pour effet d'arrêter et de désinstaller le service et de supprimer toutes les entrées du registre. Ne l'utilisez que si vous souhaitez vraiment perdre tous les paramètres.

©2005 Qbik New Zealand Limited

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  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.  
Délai d'attente de la demande dépassé.  
Délai 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

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*)**.)

[Cliquez ici pour savoir comment configurer WinGate dans un environnement Active Directory](#)

©2005 Qbik New Zealand Limited

Configuration de WinGate dans un environnement Active Directory

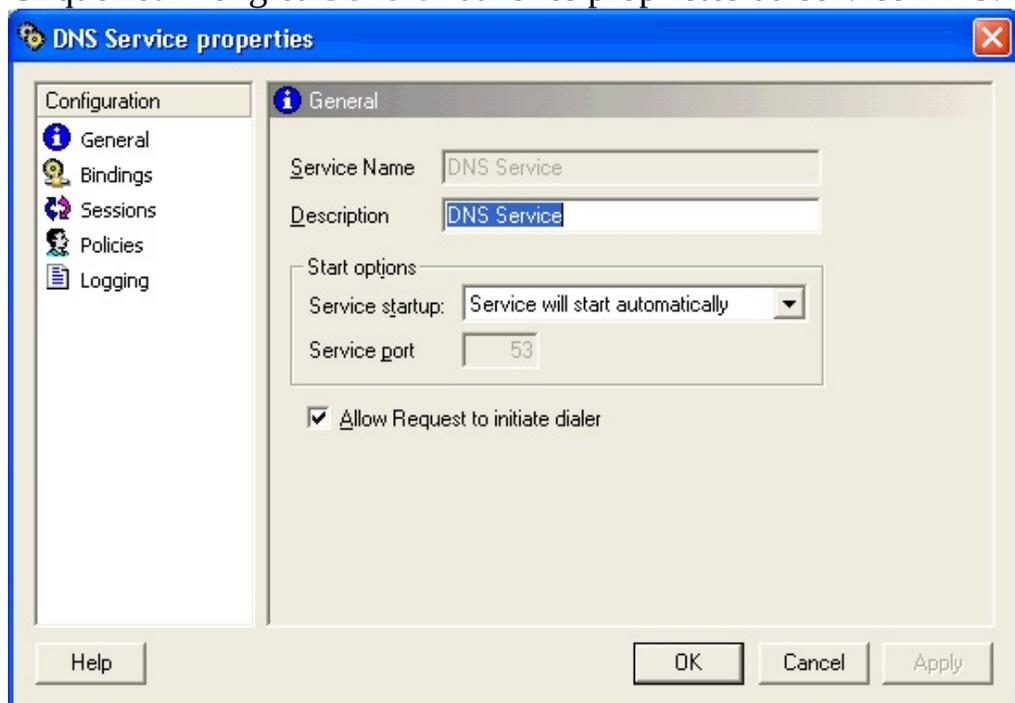
WinGate est conçu pour fonctionner dans un environnement Active Directory. Toutefois, même si la configuration des domaines Active Directory peut varier, certaines conditions sont nécessaires au bon fonctionnement de WinGate.

Sur le serveur WinGate

DNS

Si WinGate est installé sur le **MÊME** poste que le serveur DNS d'Active Directory :

1. Ouvrez **GateKeeper**.
2. Cliquez sur l'onglet **Général** dans les propriétés du service DNS.



Masquer | Masquer toutes les images

3. Dans le menu déroulant des options de démarrage, sélectionnez **Désactivé (*Service is disabled*)**.
4. Cliquez sur **OK**.

Le service DNS de WinGate est alors arrêté, afin d'éviter tout conflit avec Active Directory.

Un autre serveur DNS en amont est configuré dans les paramètres de l'interface externe (connexion Internet). WinGate l'utilise si le serveur AD ne peut pas résoudre les requêtes. Aucune configuration supplémentaire n'est nécessaire.

Si WinGate **n'est pas installé sur le même poste** qu'Active Directory, les deux solutions sont possibles (serveur DNS WinGate ou serveur DNS AD).

Utilisation de WinGate pour les vérifications DNS des clients :

1. Ouvrez la MMC du **Serveur DNS d'Active Directory**.
2. Effectuez un clic droit sur le serveur DNS et sélectionnez propriétés.
3. Cliquez sur l'onglet **Redirecteurs**.
4. Indiquez l'adresse IP interne du serveur **WinGate**.
5. Cliquez sur **OK** pour enregistrer les modifications.

Ainsi, les requêtes ne pouvant être résolues sont transférées à WinGate. Cela peut s'avérer utile si le serveur DNS d'Active Directory n'est pas connecté à Internet.

Sur le serveur WinGate :

1. 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 | Masquer toutes les images

2. Indiquez l'adresse IP interne du serveur DNS d'Active Directory.
3. Cliquez sur **OK**.

Cette étape est importante car elle 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.

DHCP

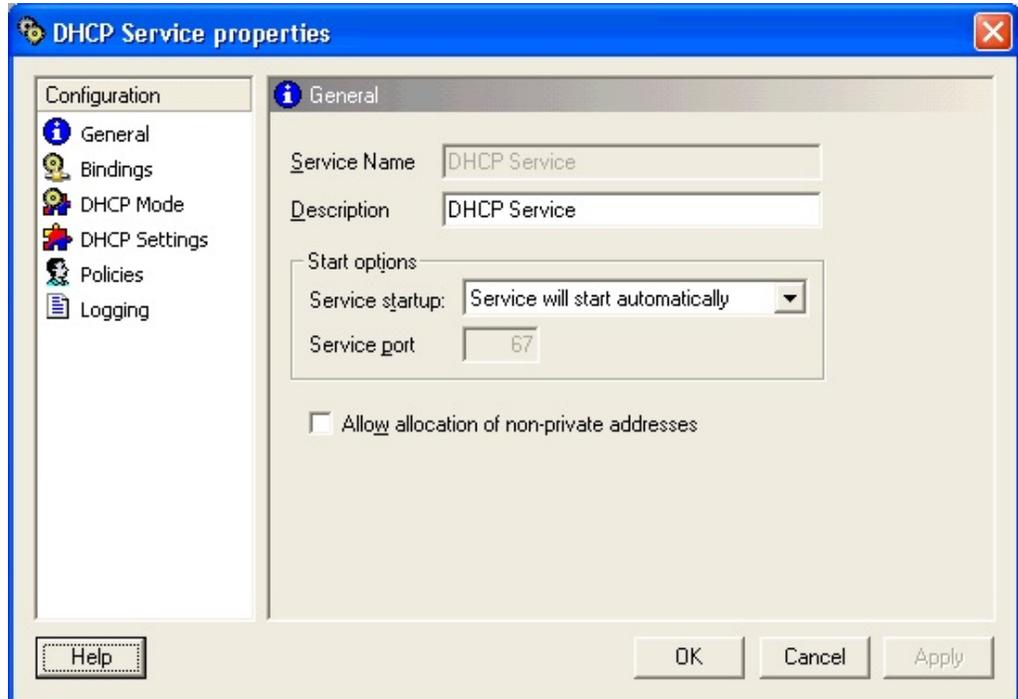
Avec Active Directory, les adresses IP (et autres paramètres réseau) sont attribuées dans la plupart des cas à l'aide d'un serveur DHCP Microsoft sur le réseau.

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.

Désactivation du service DHCP de WinGate :

1. Ouvrez **GateKeeper**.
2. Cliquez sur l'onglet **Général** dans les propriétés du service DHCP.



Masquer | Masquer toutes les images

3. Dans le menu déroulant des options de démarrage, sélectionnez **Désactivé (Service is disabled)**.
4. Cliquez sur **OK**.

Les postes clients de WinGate se connectant à Internet avec la méthode NAT (Network Address Translation) doivent indiquer l'adresse IP du serveur WinGate en tant que passerelle par défaut.

Cette opération peut être effectuée automatiquement à l'aide du service DHCP.

Base de données d'utilisateurs Active Directory dans WinGate

Afin de mieux contrôler vos utilisateurs et groupes, vous pouvez bénéficier de la base de données Active Directory dans WinGate.

Remarque :

[Les bases de données distantes](#) ne sont disponibles qu'avec une licence **WinGate Enterprise**.

Pour accéder à cette base de données, le service WinGate doit pouvoir se connecter au domaine avec un compte possédant des droits d'administration.

Il est recommandé de créer un compte dans Active Directory réservé à cet usage (par exemple : un utilisateur appelé WinGateEngine et membre du groupe Administrateurs.)

Une fois le compte créé :

1. Sur le serveur WinGate, ouvrez la MMC **Gestion de l'ordinateur** (dans Panneau de configuration/Outils d'administration).
2. Double-cliquez sur **Services et applications**.
3. Effectuez un clic droit sur le service **Qbik WinGate Engine** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Connexion**.
5. Dans la section **Ouvrir une session en tant que** cochez l'option **Ce compte**, puis cliquez sur **Parcourir** et sélectionnez le compte que vous venez de créer.
6. Redémarrez le moteur de WinGate.

©2005 Qbik New Zealand Limited

Glossaire de WinGate

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

A

Application cliente

Application se connectant à d'autres ordinateurs sur Internet afin d'obtenir des services : envoi ou réception de courrier, consultation de pages web, etc. Les principales applications clientes sont les navigateurs (comme Netscape et IE), les programmes de messagerie et les programmes FTP. Un même ordinateur peut être à la fois client et serveur selon les applications exécutées.

B

Bail

Période au cours de laquelle les adresses IP attribuées par le service DHCP peuvent être utilisées. Le client doit envoyer une demande de renouvellement au serveur avant son expiration.

BSOD

Blue Screen Of Death (littéralement : écran bleu de la mort). Lorsque Windows rencontre de sérieux problèmes et "plante", il sauvegarde le contenu de sa mémoire dans un fichier. Un écran bleu apparaît alors vous demandant de contacter votre administrateur système et la seule solution consiste à redémarrer l'ordinateur. Cet écran est connu sous le nom de "Blue Screen of Death".

C

Cache

Le serveur proxy web de WinGate comprend une fonctionnalité de cache HTTP. Cela consiste à enregistrer sur le serveur les fichiers récemment consultés sur Internet (graphiques, pages HTML, etc.) afin de pouvoir y accéder plus rapidement par la suite. La mémoire cache de WinGate vérifie quotidiennement que les documents soient à jour, mais il est également possible d'effectuer cette opération manuellement en cliquant sur "Actualiser" dans votre navigateur. Les

URL comprenant le caractère '?' (c'est à dire les documents contenant des CGI) ne sont pas enregistrées dans la mémoire cache.

Cascade

La mise en cascade consiste à se connecter à un proxy à l'aide d'un autre proxy. Ce procédé est généralement utilisé lorsqu'un FAI met un proxy web à la disposition de ses utilisateurs. Si vous souhaitez mettre le serveur de WinGate en cascade avec celui de votre FAI, sélectionnez l'option "Via un serveur proxy en cascade" (en cliquant sur l'icône **Connexion** dans les propriétés du proxy web) puis indiquez les informations concernant votre FAI.

CGI

Common Gateway Interface. Petits programmes (appelés scripts), situés et exécutés sur un serveur web, et souvent utilisés pour traiter les informations contenues dans les formulaires html. Les moteurs de recherche en utilisent également beaucoup.

Composeur

Logiciel indiquant au modem à quel moment il doit effectuer la numérotation. WinGate possède un composeur intégré.

Connexion

Ce terme peut avoir plusieurs significations : union de deux appareils à l'aide d'un câble, d'une prise, etc. ; numérotation à l'aide d'un modem ou bien canal de communication entre un client et un serveur.

Connexion permanente

Une connexion est dite permanente lorsque l'utilisateur reçoit une adresse IP (ou une plage d'adresses) pour son réseau. Il en existe différentes sortes : ISDN, modem et Ethernet. Cela garantit l'accès à Internet.

Cryptage

Procédé permettant de sécuriser les données transmises de façon à ce que seul le destinataire puisse les décoder.

D

DHCP

Dynamic Host Configuration Protocol. Service permettant de configurer

automatiquement les paramètres TCP/IP des postes clients de votre réseau.

Droits

Les administrateurs attribuent des droits à chaque utilisateur afin de décider s'ils peuvent accéder à WinGate (et de quelle façon) et éventuellement en modifier la configuration.

DUN

Dial-Up-Networking (réseau commuté). Terme désignant la partie du système d'exploitation permettant aux modems de communiquer.

E

ENS

Extended Network Support (service réseau avancé) : voir NAT

Étendue

Plage d'adresses IP ayant des propriétés communes. En mode automatique, le serveur DHCP utilise l'étendue : 192.168.0.1 à 192.168.0.254 . Une étendue DHCP comprend un groupe d'ordinateurs clients d'un même sous-réseau.

Exclusions

Dans le service DHCP, il est possible d'exclure des plages d'adresses IP : elles ne sont attribuées à aucun ordinateur (la plage doit faire partie d'une même étendue). L'IP du serveur WinGate est automatiquement exclue.

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.

Fichier hosts

Le fichier hosts se trouve dans le dossier "drivers" du système d'exploitation Windows et "relie" les noms d'hôtes aux adresses IP. Avec le DHCP, les fichiers hosts ne sont plus nécessaires.

FTP (File Transfer Protocol)

Protocole de transfert de fichiers. Permet de télécharger/envoyer des fichiers sur Internet (en utilisant un logiciel client la procédure est très simple).

G

GDP

Generic (ou Gateway) Discovery Protocol. Protocole permettant de rechercher et d'identifier les ordinateurs passerelle d'un réseau. Il est enregistré auprès de l'IANA (port : 368).

Groupe

Ensemble d'utilisateurs ayant des caractéristiques communes. Si une règle s'applique à un groupe, elle s'applique à tous ses membres. Un utilisateur peut appartenir à un, plusieurs ou tous les groupes mais peut également ne faire partie d'aucun.

H

HTTP

Protocole utilisé pour naviguer sur Internet, bien qu'à présent de nombreux autres programmes l'utilisent également. Le proxy web de WinGate offre un accès HTTP à ses utilisateurs.

HTTPS

HTTP sécurisé, parfois appelé SHTTP. Des navigateurs comme Netscape possèdent un système de cryptage intégré afin de rendre les échanges de données plus sûrs. Il est utilisé pour les achats en ligne, en particulier les paiements par carte bleue.

I

IANA (Internet Assigned Numbers Authority)

Organisation contrôlant l'attribution des numéros de port IP. Les ports inférieurs à 1024 sont appelés des ports système. Les développeurs de logiciels serveurs utilisant ces ports doivent auparavant déposer une demande auprès de l'IANA. De nombreux numéros de port ont déjà été attribués.

ICMP (Internet Control Message Protocol)

Extension de bas niveau du protocole IP.

Interface

Une interface est une "connexion réseau". Il peut s'agir d'une carte réseau, d'un profil de connexion, ou de l'adresse loopback ("localhost").

IP

Internet Protocol. Une adresse IP est un moyen d'identifier un ordinateur sur Internet.

IRC (Internet Relay Chat)

Application permettant à plusieurs utilisateurs de "dialoguer" avec d'autres sur Internet.

L

Liaison

Obligation d'utiliser quelque chose. Un service (ou un protocole) n'écoute que l'interface à laquelle il est lié. Par défaut, les services de WinGate sont liés à toutes les interfaces "non externes". Cela élimine les risques de liaison avec des interfaces non existantes.

Licence

Les licences de WinGate varient en fonction de la version (WinGate Plus, Pro ou Enterprise) et du nombre d'utilisateurs (3, 6, 12, 25, 50, 100, 250 ou illimité). Il s'agit du nombre maximum de postes pouvant être connectés simultanément à WinGate. Cela ne correspond donc pas au nombre d'ordinateurs sur votre réseau, ni au nombre de comptes d'utilisateurs. Par exemple, sur un réseau comprenant plus de 10 postes, une licence de 6 utilisateurs permet de limiter l'utilisation d'Internet. Les licences peuvent être obtenues auprès de revendeurs. Vous pouvez également obtenir une version d'évaluation contenant un compte intégré.

Localhost

Terme spécifique au TCP/IP. Il s'agit de l'interface loopback (127.0.0.1) d'un ordinateur. Cette interface ne correspond pas à un périphérique physique.

LSP (Layered Service Provider)

Ce système fait partie des extensions de Winsock 2. Il permet le chaînage de certaines fonctions de Winsock. WinGate Internet Client est un LSP.

M

Moteur de WinGate

Il s'agit du programme wingate.exe (le serveur). Il fonctionne de façon "invisible", en tant que service Windows.

N

NAT

Le NAT (Network Address Translation, ou traduction d'adresses réseau) est l'un des éléments principaux du service réseau avancé. Il fonctionne de la même façon qu'un routeur mais remplace son adresse IP publique par l'adresse interne de ses clients dans les paquets qu'il transfère. Cela permet aux ordinateurs d'un réseau de partager une connexion Internet quelles que soient l'application et la plateforme utilisées (Windows, MacOS, Unix ou Linux).

NIC

Network Interface Card, c'est à dire carte d'interface réseau.

P

Paquet

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. Les paquets de données fonctionnent de façon très similaire. La façon dont les données sont "emballées" est codifiée, mais vous décidez du contenu. Différents types de paquets sont utilisés sur Internet, mais tous suivent le même modèle.

Pare-feu

Barrière entre votre réseau et Internet, ne pouvant être traversée que par le trafic autorisé. Le pare-feu examine les données circulant entre un réseau et Internet et refuse tout ce qui n'a pas été expressément autorisé. Pour créer des règles de permission ou de refus, il suffit d'indiquer le service, l'adresse IP ou l'hôte que vous souhaitez autoriser ou refuser. En règle générale, les pare-feu analysent le trafic entre le réseau interne d'une entreprise et Internet. Cependant, il est également possible d'en placer un entre deux parties d'un même réseau, ce qui permet par exemple de protéger le service comptabilité des autres utilisateurs.

Ping

Commande disponible sur la plupart des systèmes compatibles TCP/IP y compris DOS. Elle teste la connexion TCP entre deux emplacements et renvoie des informations sur la rapidité du lien. Utilisation : ping [-t] [-a] [-n échos] [-l taille] [-f] [-i vie] [-v TypServ] [-r NbSauts] [-s NbSauts] [[-j ListeHôtes] | [-k ListeHôtes] [-w Délai] NomCible. Options : "-t" : envoie la requête ping sur l'hôte spécifié jusqu'à interruption, "-a" : transforme les adresses en noms d'hôtes, "-n échos" : nombre de requêtes écho à envoyer, "-l size" : envoie la taille du tampon, "-f" : active l'indicateur Ne pas fragmenter dans le paquet, "-i" : durée de vie, "-v" : type de service, "-r " : enregistre l'itinéraire pour le nombre de sauts, "-s" : dateur pour le nombre de sauts, "-j" : itinéraire source libre parmi la liste d'hôtes, "-k" : itinéraire source strict parmi la liste d'hôtes, "-w" : délai d'attente pour chaque réponse en millisecondes.

Par exemple, pour tester la connexion à "ftp.microsoft.com", exécutez la commande : ping ftp.microsoft.com

Si votre ordinateur est directement connecté à Internet, la réponse est la suivante :

Envoi d'une requête ping sur [198.105.232.1] avec 32 octets de données

Réponse de [198.105.232.1] : Octets=32 temps 40ms

Réponse de [198.105.232.1] : Octets=32 temps 20ms

Réponse de [198.105.232.1] : Octets=32 temps 20ms

Réponse de [198.105.232.1] : Octets=32 temps 30ms

Remarque : le nom a été converti en adresse IP par le service DNS. Sans ce service, il n'est possible d'effectuer des requêtes ping que sur des IP.

Si l'ordinateur est connecté à Internet par le biais de WinGate, la réponse sera du type :

Envoi d'une requête ping sur [198.105.232.1] avec 32 octets de données

Impossible de joindre l'hôte de destination

Cela signifie que le service DNS fonctionne. WinGate ne peut pas transférer les paquets, par conséquent vous n'obtiendrez pas d'autres données.

Si le résultat est du type :

Mauvaise adresse IP ftp.microsoft.com

cela signifie que le service DNS ne fonctionne pas correctement. Assurez-vous qu'il soit bien paramétré.

Politiques

Permettent aux administrateurs de contrôler l'accès à WinGate, et d'accorder certains droits aux utilisateurs.

POP3

Protocole (précédé des versions POP et POP2) utilisé pour accéder au courrier sur les serveurs de messagerie. Les clients de messagerie communiquent avec les serveurs à l'aide de ce protocole.

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. Certains ports sont réservés à des opérations spécifiques, par exemple le port 80 pour le protocole HTTP.

Protocole

Méthode selon laquelle deux ou plusieurs entités communiquent ou organisent leur communication. Les protocoles réseaux sont très stricts. Si une application ne respecte pas les règles définies, elle risque de ne pas pouvoir communiquer. Ces "règles" concernent : la façon de "saluer" le serveur, la connexion avec un nom d'utilisateur et un mot de passe, les requêtes et envois d'informations, etc. Les serveurs proxy ont généralement besoin d'un proxy par protocole. Exemples : POP3 (Post Office Protocol) ou http (HyperText Transfer Protocol).

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).

R

RAS (Remote Access Service)

Accès réseau distant. Technologie similaire au DUN. Il s'agit du programme permettant de contrôler les modems dans Windows.

Requête non proxy

Le terme requête non proxy est employé lorsqu'un programme s'adresse directement à un port comme s'il s'agissait d'un serveur, sans utiliser le protocole proxy. La plupart des serveurs proxy ne sont pas compatibles avec ce type de requête, mais certains services de WinGate les acceptent.

Requête proxy

Action effectuée lorsqu'un programme "s'adresse" à un proxy et lui demande des ressources.

Ressource

Terme désignant tout type de données ou du matériel de traitement/stockage. Les ressources d'un ordinateur sont la mémoire, l'espace disque, ou le temps de traitement. Sur Internet il peut s'agir d'un graphique, une page HTM, un fichier à télécharger, etc.

S

Serveur

Application qui "écoute" les connexions entrantes et les requêtes provenant d'autres ordinateurs, et leur fournit des services (d'où le terme "serveur"). Les principaux types de serveurs sont : les serveurs web (fournissent des documents html aux clients), ftp (fournissent tous types de fichiers) et SMTP/POP3 (réception et envoi de courrier). Remarque : pour qu'un serveur puisse entendre les requêtes provenant d'ordinateurs sur Internet il doit être lié à un port sur une interface publique (un port du serveur WinGate).

Service

Dispositif qui facilite ou permet certaines opérations. Les proxies de WinGate sont des services qui facilitent la connexion à Internet.

Service actif

Service qui est en train de fonctionner (c'est à dire qui écoute les requêtes TCP/IP).

SMTP

Simple Mail Transfer Protocol. Méthode utilisée pour l'envoi de courrier sur Internet.

SOCKS

Protocole de négociation pour les pare-feu. WinGate possède un serveur SOCKS intégré.

Sous-réseau

Groupe d'ordinateurs directement connectés entre eux via un câble coaxial ou un concentrateur. Si un ordinateur possède deux adaptateurs réseau, il est présent sur deux sous-réseaux. De plus, il est possible de trouver plusieurs sous-réseaux virtuels sur un seul sous-réseau physique.

SSL

SSL (Secure Socket Layer). Protocole permettant de sécuriser les connexions. Son rôle est très important car de plus en plus d'informations confidentielles (comme les numéros de cartes de crédit) sont transmises sur Internet.

T

TCP/IP

Transmission Control Protocol / Internet Protocol. Méthode standard pour l'envoi de données sur Internet, basée sur des formats de paquets de données spécifiques (y compris les adresses de l'expéditeur et du destinataire). Pour utiliser Internet ou WinGate, ce protocole doit être présent sur chaque ordinateur du réseau. TCP et IP sont en fait deux protocoles différents, mais le terme TCP/IP est couramment employé car ils sont très proches.

Telnet

Programme en ligne de commande permettant d'accéder à un ordinateur distant et d'y exécuter des applications (utilisé aux débuts d'Internet). WinGate possède

un proxy Telnet.

Terminateur

Petit élément situé à chaque extrémité d'un réseau relié par câble co-axial.

U

UDP

User Datagram Protocol. Protocole non orienté connexion, permettant d'envoyer des datagrammes de la même façon que le TCP, mais qui - à l'instar du protocole IP - ne garantit pas que les paquets atteignent leur destination.

Unix

Ensemble de systèmes d'exploitations multitâche, dont le plus répandu est Linux. Malgré quelques défauts, les systèmes Unix sont flexibles et plus sécurisés que les autres SE. Chaque système étant différent, des protocoles ont été établis afin de permettre aux ordinateurs de communiquer entre eux.

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).

Utilisateur

Dans WinGate, il est possible de créer des comptes d'utilisateurs auxquels vous accordez des droits afin de : contrôler leur accès à WinGate, leur permettre (ou pas) d'en modifier la configuration, et connaître la quantité de données transmises. WinGate comporte deux comptes par défaut, qu'il est impossible de supprimer : "Administrator" et "Guest".

Utilisateur présumé

Personne utilisant les services de WinGate sans être authentifiée, mais ayant fourni certaines informations : l'adresse MAC de la carte LAN de son ordinateur, ou mieux encore son nom Netbios.

W

WGIC

WinGate Internet Client. Logiciel client de WinGate (donne l'accès au service de redirection Winsock).

Winsock

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

WRP (Winsock Redirection Protocol)

Protocole utilisé par WGIC et le service WRS afin de fournir les services de redirection Winsock.

WRS (Winsock Redirector Service)

Service de WinGate permettant la redirection Winsock.

A propos de Qbik New Zealand

WinGate est la propriété de **Qbik** - entreprise de développement de logiciels spécialisée dans les solutions innovatrices pour Internet.

Nos bureaux se trouvent à Auckland, en Nouvelle Zélande.

Pour en savoir plus sur Qbik et les différents produits disponibles :

<http://www.Qbik.com>

Un support en ligne est disponible à l'adresse suivante :

<http://www.wingate.com>

Pour toute question générale, commerciale, ou technique, consultez la page [Contact](#).

Nous tenons également à remercier tous ceux qui ont consacré du temps et de l'énergie à tester et à soutenir les versions bêtas de WinGate. Leur contribution a permis à WinGate de devenir aussi performant.



©2004 Qbik New Zealand Limited

Contact

Pour le support technique, adressez-vous à la personne qui vous a vendu le logiciel. Si vous possédez une clé d'évaluation et que vous souhaitez acquérir une licence, adressez-vous au revendeur qui vous a fourni cette clé.

Plus d'informations sur WinGate par **Qbik New Zealand Ltd** sont disponibles à l'adresse suivante :

<http://www.wingate.com>

Pour toute autre question, adressez-vous à :

info@wingate.com

La documentation de WinGate est régulièrement modifiée et améliorée. En consultant notre site, vous trouverez la documentation à jour ainsi que d'autres informations utiles.

La liste complète des distributeurs de WinGate par pays est disponible à l'adresse suivante :

<http://wingate.com/resellers>



©2004 Qbik New Zealand Limited

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 (serveur proxy web, POP3, de fichiers journaux ou Telnet).
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**.

Le numéro de port à intercepter s'affiche alors dans la liste.

Principaux avantages :

Avec le module PureSight - 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 le module AntiVirus - 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.

Jeux

Afin de pouvoir jouer en ligne avec WinGate, vous devez vérifier :

1. **La configuration requise indiquée dans le manuel du jeu.**
2. **La configuration de WinGate.**

Remarque :

Pour la plupart des jeux, il n'est pas possible que plusieurs joueurs se trouvent sur le même client WGIC. En effet, une seule adresse IP est utilisée pour se connecter à WinGate : le serveur du jeu ne voit donc qu'un seul joueur.

Remarque :

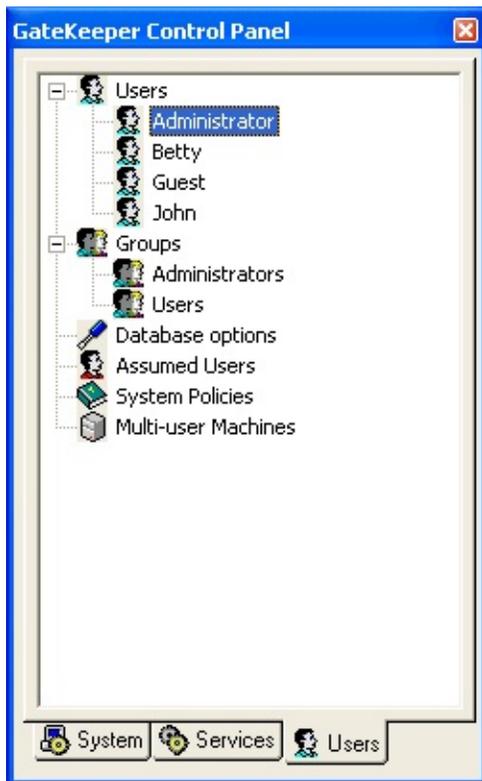
WinGate intègre à présent **Direct Play** par le biais des connexions **ENS/NAT**. Plusieurs utilisateurs peuvent jouer simultanément à un même jeu.

Voici quelques instructions à suivre :

1. Assurez-vous que votre ordinateur soit paramétré afin de pouvoir accéder à Internet par le biais de WinGate.
2. Configurez le pare-feu en mode [Moyen : pour les jeux et applications Internet \(Medium\)](#).
3. Installez le jeu conformément aux instructions de son manuel. Vous serez peut-être amené à ouvrir un port dans le **Pare-feu** (en cliquant sur [Sécurité des ports \(Port security\)](#) dans le Service réseau avancé).

The Users tab

The **Users tab** on the GateKeeper control panel provides easy access to the tools used to manage users, groups, user databases and system policies in WinGate.



Close

Options on the User tab include:

Option	Description
Users	This lists all of the current users that are known and used by WinGate. (Regardless of what user database has been used). Double clicking on a user allows you to configure details for the user in the user properties.

Groups

This lists all of the current groups that are used by WinGate.(Regardless of what user database has been used)

Database Options

The Database option allows you to select whether or not to use the Operating system/Remote user database for implementing policies and control in WinGate. (The built in WinGate user database is used by default)

Note:

When using the Operating System or Remote user database option, once the users and groups are listed in WinGate, then all WinGate related policy and control over these users and groups is performed inside of GateKeeper.

Local Network/Domain user and group control (i.e. access to shares, permissions etc) is still controlled by the Operating System/Domain Controller.

WinGate management for user and group control and policies relates only to WinGate operations.

System Policies

The System Policies option is where you can configure policies that will be used throughout WinGate, as opposed to Service policies which are configured on a service by service basis.

Assumptions

The Assumptions option allows you to configure location assumptions for WinGate. You can set WinGate to assume that if a connection is recieved from a particular IP address or computer name,

then it is deemed to be a particular user connecting.

Multi User Machines

The Multi user machines option (available only with a WinGate Enterprise license) allows you to specify Multi user machines (e.g. Terminal Server machines, "thin client" servers) on your network, so that WinGate will be able to authenticate and identify individual login client sessions from the Multi user machine.

Note:

The Multi User machines option only supports Multi User machines that use NTLM authentication.

NAT

NAT stands for Network Address Translation. It is used to share a single public IP between multiple client computers on the LAN, each using their own unique private class IP address.

When a client attempts to connect or send data to a machine on the Internet it forwards the data to the WinGate server(running NAT). The WinGate server then substitutes the original private IP in the packet sent from the client with its own (the external Public class IP address it uses for the Internet) and carries out the clients original request.

The remote Internet computer/server/site sends packets back to the WinGate server, because they think that the WinGate server was the source of the data sent. Since NAT keeps a record of which client computers sent packets on which ports, it is able to pass the incoming packets back to the correct LAN computer that initially made the request.

[Click here to find out more about how NAT works](#)

[Click here to find out how to configure clients to use NAT](#)

Pros

NAT provides fast and seamless low-level sharing of a connection to the internet. It is the simplest approach to sharing an internet connection. With little overhead, it is very reliable.

It is also extremely flexible as it gives access to shared connection for any platform that supports TCP/IP (e.g. Windows, Mac, Unix, Linux) and virtually any client application (web browsers, mail programs, newsgroups, FTP etc.)

There is no software to install and no applications to configure.

Easy integration with proxies.

©2005 Qbik New Zealand Limited

Filtrage de l'historique

Cette fonctionnalité permet de choisir les éléments enregistrés dans l'historique, afin de ne pas encombrer votre disque dur avec des données inutiles.

Masquer | Masquer toutes les images

Filtres d'affichage (View Filter Settings)

Affiche les données enregistrées. La structure des fichiers journaux "classiques" de WinGate permet de créer des filtres déterminant les éléments à afficher. Vous retrouvez ainsi rapidement les informations recherchées.

Il existe deux types de filtres :

1. Filtre simple (Simple Filter)

Masquer | Masquer toutes les images

Avec cet outil, vous créez facilement des filtres en sélectionnant un critère dans le menu déroulant de gauche. Par exemple, le filtre ci-dessus affiche uniquement l'historique de l'utilisateur Bob. Les données concernant les autres utilisateurs sont bien enregistrées mais ne s'affichent pas.

2. Filtre personnalisé (Free-Hand Filter)

Masquer | Masquer toutes les images

S'adressant aux utilisateurs avancés, cet outil est extrêmement flexible : il permet d'associer tous les critères et toutes les valeurs disponibles dans des instructions logiques (à l'aide d'opérateurs booléens comme OR, AND, NOT...).

Exemples :

username="bob" affiche tous les éléments concernant l'utilisateur "bob"

username="t?m" affiche tous les éléments concernant les utilisateurs dont le nom commence par "t" et termine par "m".

username<>"tim" AND username<>"b??" AND (compname <>"b*" OR IP <> "192.168.*") (((type<> DNS) or (type<>RCS)) = FALSE) AND (bytesin > 4096))

N'affiche que les sessions dont le trafic est supérieur à 4Ko (sauf les sessions RCS et DNS), pour les utilisateurs ayant un nom composé de 3 lettres qui ne commence pas par "b" ou égal à "tim". Exclut également les sessions provenant d'ordinateurs dont le nom Netbios commence par "b" ou dont l'adresse IP est comprise dans l'étendue 192.168.*.*.

Vous pouvez utiliser des parenthèses pour grouper des expressions.

Types de comparaison	Description
<	Inférieur à
>	Supérieur à
=	Egal à

==	Identique à
<=	Inférieur ou égal à
>=	Supérieur ou égal à
AND	"Et" booléen : les deux opérateurs doivent être vérifiés (TRUE)
OR	"Or" booléen : au moins l'un des opérateurs doit être vérifié (TRUE)
XOR	"Xor" booléen : un seul des opérateurs doit être vérifié TRUE
ISU	Le critère s'applique si l'opérateur 1 contient l'opérateur 2 (ne respecte pas la casse)
IS	Chaîne correspondante (respecte la casse)

Opérateurs

Les opérateurs peuvent éventuellement être utilisés dans des expressions :

+ : Addition numérique et concaténation de chaînes

- : Soustraction

* : Multiplication d'expressions numériques, par ex. : 3*5

/ : Division

Types de données

Constantes

TRUE : le critère est vérifié

FALSE : le critère n'est pas vérifié

<Type de constante> : voir ci-dessous

Caractères joker :

* : remplace toute chaîne composée de 0 caractères ou plus

? : remplace un seul caractère

Chaînes :

Une chaîne peut être élaborée comme suit

"nouvelle chaîne"

Vous pouvez utiliser des caractères joker et effectuer des concaténations

"str" + "ing"

Types de chiffres

Nombres entiers : {...,-2, -1, 0, 1, 2, ...}

Nombre réels : {1.2, 3.9, -4.6, etc. }

Variables disponibles

Toutes les valeurs doivent être entre guillemets (" ").

Variable	Type	Description
USERNAME	Chaîne	Nom Netbios de l'utilisateur ayant ouvert la session. Si celui-ci est inconnu, le champ sera

vide

WGUSERNAME	Chaîne	Identifiant WinGate de l'utilisateur ayant ouvert la session. Si celui-ci est inconnu, le champ sera vide
COMPNAME	Chaîne	Nom Netbios de l'ordinateur (s'il est connu)
IPNUMBER	Chaîne	Adresse IP du client
APPNAME	Chaîne	Nom de l'application ayant ouvert la session, si le service WRP possède cette information
DESCRIPTION	Chaîne	Description de l'activité de la session
DURATION	Nombre entier	Durée en secondes de la session
BYTESIN	Nombre entier	Données envoyées au client (en octets)
BYTESOUT	Nombre entier	Données envoyées pour le client (en octets)
TYPE	Constante prédéfinie	L'un des protocoles suivants : NONE, RCS, DNS, WRP, PLUG, HTTP, FTP, POP3, SMTP, NNTP, TELNET, REALPLAYER, VDO, SOCKS4, SOCKS5, XDMA, VPN

©2005 Qbik New Zealand Limited

Options de quarantaine

Pour configurer les options de quarantaine, effectuez un clic droit à l'intérieur de l'onglet et cliquez sur Propriétés (*Quarantine properties*).

[Cliquez ici pour une copie d'écran](#)

Stockage :

Taille maximum (*Maximum size*)

Lorsque le dossier contenant les fichiers en quarantaine atteint la taille indiquée (en Mo) des fichiers sont supprimés.

Durée maximum (*Maximum age*)

Période au cours de laquelle un fichier reste en quarantaine avant d'être supprimé.

Nbre max. de fichiers (*Maximum items*)

Nombre maximum de fichiers pouvant être mis en quarantaine.

Divers :

Afficher l'onglet si un fichier est mis en quarantaine (*Autoactivate when an item is quarantined*)

Lorsque cette option est cochée, l'onglet s'affiche automatiquement dès qu'un élément mis en quarantaine.

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).

©2004 Qbik New Zealand Limited

Installation du service TCP/IP

Remarque :

Windows installe presque toujours le TCP/IP par défaut. Il n'est donc nécessaire de modifier ces paramètres que s'il n'a pas été installé pour une raison spécifique.

Avant de configurer les ordinateurs clients, assurez-vous que le moteur de WinGate fonctionne.

Si le TCP/IP est déjà installé, vous pouvez [vérifier qu'il fonctionne correctement](#). En cas de problème, il est possible de le supprimer puis de le réinstaller en suivant la procédure ci-dessous.

En règle générale, il fait partie du système d'exploitation.

Remarque importante :

Si vous possédez un modem connecté à Internet cela signifie que le TCP/IP est déjà présent sur votre ordinateur.

Vous serez peut être amené à insérer un CD (celui du système d'exploitation).

Sous 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

Sous Windows NT4

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

Sous 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

Modes du service WRP

Ces modes sont configurables depuis l'applet WGIC sur les postes clients, ou bien directement à partir du serveur si vous possédez une licence WinGate Enterprise.

Modes des applications

Local

Ce mode empêche le service WRP de répondre aux requêtes provenant de l'application sélectionnée.

Les applications configurées en mode local seront ignorées par WGIC et devront effectuer leurs requêtes par d'autres moyens.

Si vous souhaitez bénéficier de la rapidité du NAT pour vos applications nécessitant uniquement des connexions sortantes, il suffit de les configurer en mode local.

Remarques :

Pour que cela fonctionne, le service NAT/ENS de WinGate doit être activé sur le serveur.

Les applications en mode local utilisent le NAT (à condition que la passerelle par défaut dans les propriétés TCP/IP du poste client corresponde au serveur WinGate ; et que l'application ne soit pas configurée pour utiliser des proxies). Veuillez noter que le NAT n'est utilisable que par les applications clientes (et non les serveurs).

Mixte

Ce mode est à la fois sûr et fonctionnel.

Il permet aux applications des postes clients d'effectuer des connexions sortantes par le biais du WRP, mais les serveurs hébergés sur ces mêmes postes ne pourront recevoir de connexions entrantes que si elles proviennent d'ordinateurs situés sur le même réseau. Cela convient particulièrement pour les serveurs web ou FTP intranet.

Par mesure de sécurité ce mode est attribué automatiquement aux applications essayant d'écouter un port système (c.à.d. inférieur à 1024). Elles ne sont accessibles depuis l'extérieur que si vous choisissez le mode global.

Global

Utilisez ce mode si vous possédez des serveurs (web ou FTP par exemple) sur des postes clients de WinGate, afin qu'ils puissent recevoir des requêtes provenant d'Internet.

[Cliquez ici pour savoir comment configurer le service pour qu'il supporte les applications serveurs sur les postes clients](#)

Configuration du réseau

Informations générales

Avant d'installer WinGate, assurez-vous que votre réseau TCP/IP fonctionne correctement.

Pour cela, effectuez une requête ping sur chaque ordinateur du réseau.

[\(Cliquez ici pour en savoir plus\)](#)

Remarque :

Le TCP est installé par défaut avec Windows (à partir de Windows 98). Une fois votre réseau configuré, vous pouvez installer WinGate.

Domaines Active Directory

Informations générales

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

Le service Active Directory nécessite un serveur DNS (DDNS, DNS dynamique) afin d'enregistrer les détails concernant l'adresse IP du client. Il peut recevoir ces informations d'un serveur DHCP Microsoft lorsqu'une adresse IP est attribuée au client, ou être configuré afin de les recevoir directement du client.

Les clients ont également besoin de serveurs DNS afin de s'informer sur les contrôleurs de domaine de AD. Lorsqu'un contrôleur de domaine est correctement paramétré, il enregistre les informations spécifiques à AD (par le biais d'enregistrements SRV) à l'aide du serveur DDNS de Microsoft.

Le serveur DDNS dispose d'une fonctionnalité de transfert 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 DDNS pour les requêtes du domaine de Active Directory, et les requêtes Internet

sont transférées au serveur DNS choisi.

Lors de l'installation du serveur DDNS de Microsoft (serveur DNS Active Directory) il arrive parfois qu'il ne détecte pas les autres serveurs. Il est alors paramétré en tant que serveur racine pour toutes les requêtes de nom de domaine, ce qui désactive l'option de transfert. Si tel est le cas, consultez l'aide de Microsoft afin de pouvoir activer cette option.

Active Directory et WinGate

DNS

Lorsque WinGate est utilisé dans un environnement Active Directory, le serveur (D)DNS d'Active Directory doit être paramétré afin de transférer les requêtes Internet des clients vers le serveur WinGate.

Il est cependant nécessaire que les paramètres réseaux des clients indiquent le serveur DNS d'Active Directory. Les requêtes Internet seront ensuite transférées au serveur de WinGate.

Remarque :

Si WinGate ne se trouve pas sur le même poste que le serveur DNS d'Active Directory il n'est pas nécessaire de modifier sa configuration DNS.

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 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.

©2004 Qbik New Zealand Limited

Désactiver le service DNS de WinGate

Vous pouvez utiliser soit le serveur DNS de WinGate, soit un lien mappé UDP sur le port 53. Le serveur DNS de WinGate est installé et activé par défaut.

Pour désactiver ce service :

1. Ouvrez **GateKeeper**.
2. Connectez-vous à l'aide du compte "Administrator".
3. Cliquez sur l'icône **Général** dans les propriétés du **Service DNS**.
4. Dans les options de démarrage, sélectionnez **désactivé (Service is disabled)**.
5. Cliquez sur **OK**.
6. Effectuez un clic droit sur le **service DNS** puis sélectionnez **Arrêter**.
Le service est alors arrêté et la liaison avec l'interface interrompue.

Email - Paramètres de validation de l'adresse de l'expéditeur

[Cliquez ici pour une copie d'écran](#)

Indiquez ici si vous souhaitez effectuer une vérification inverse pour les serveurs de messagerie qui se connectent au votre.

©2004 Qbik New Zealand Limited

Intégration de serveurs avec les proxies de WinGate

Certains ordinateurs possèdent des serveurs indépendants qui fonctionnent dans WinGate.

Gardez toujours à l'esprit que vous ne pouvez exécuter qu'une seule application sur un même port.

Vous disposez pour cela de deux solutions :

Proxy :

Modifiez le numéro de port du service WinGate en conflit.

Vous devrez ensuite modifier les informations concernant le proxy dans les paramètres du client ou utiliser les fichiers **PAC** ; ou bien les utilisateurs seront contraints d'indiquer le numéro de port dans l'URL.

Exemple :

Une entreprise possède un serveur FTP et dispose d'une connexion permanente à Internet.

1. L'administrateur installe WinGate et ouvre GateKeeper.
2. Dans GateKeeper, il constate que le démarrage du service FTP de WinGate sur le **port 21** a échoué.
3. Il attribue alors le port **8021** à ce service.
4. Toutes les applications clientes sont paramétrées pour utiliser le service FTP sur le port **8021** et le serveur FTP de l'entreprise utilise toujours le port **21**.

Non proxy :

Modifiez le numéro de port du serveur (et non celui du service WinGate).

En règle générale, on ajoute 8000 au numéro initial (8080 pour les serveurs web,

ou 8110 pour les serveurs POP3). Il suffit alors d'apporter quelques modifications aux paramètres du proxy pour que les deux services fonctionnent, c'est pourquoi nous vous recommandons d'utiliser cette méthode.

Exemple :

Une entreprise possède un serveur web pour son site et dispose d'une connexion permanente à Internet.

L'administrateur décide d'installer WinGate.

1. Il ouvre GateKeeper et constate que le démarrage du proxy web sur le **port 80** a échoué.
2. Il modifie le port de son serveur, et lui attribue le **port 8080**.
3. Dans les propriétés du proxy web, il clique sur l'icône **Requêtes serveur (Server requests)**.
4. Il sélectionne l'option **Rediriger la requête vers un serveur prédéterminé (Pipe requests through predetermined server)**, puis indique l'adresse IP de son serveur et le **port 8080**
5. Il sauvegarde la configuration et redémarre le service.
6. La configuration des clients est la même que pour l'utilisation de n'importe quel proxy et l'accès au site s'effectue normalement.

Utilisation de serveurs sur des postes différents

Vos serveurs de messagerie, FTP ou web situés des postes différents peuvent être connectés à Internet via WinGate. La procédure est simple et sécurisée.

Vous disposez de trois possibilités :

1. Créer un **lien mappé** entre le port du service de WinGate et le poste de l'autre serveur.
2. Rediriger les requêtes non proxy vers le poste du serveur (dans **Requêtes serveur**).
3. Utiliser les fonctionnalités de **redirection** et de **relais** du **Service réseau avancé** pour rediriger les paquets vers le serveur correspondant.

Il est plus avantageux d'avoir recours au Service réseau avancé ou à la solution non proxy car cela permet de recevoir des requêtes proxy et non proxy sur un même port.

©2004 Qbik New Zealand Limited