

TermiNET

Pare-feu pour PC

Guide de référence

Table des matières

1	INTRODUCTION	3
1.1	TERMINET – PRESENTATION GENERALE	3
1.2	PRINCIPALES CARACTERISTIQUES	3
2	PRINCIPES DE BASE	3
2.1	INSTALLER TERMINET	3
2.2	CONNEXION A TERMINET	4
2.2.1	<i>Windows 95/98</i>	4
2.2.2	<i>Windows NT/2000</i>	4
2.3	MODE ADMINISTRATEUR	4
2.4	INTERFACE DE TERMINET	4
3	UTILISATEURS ET GROUPES	8
3.1	GERER LES UTILISATEURS ET DES GROUPES	8
3.1.1	<i>Ajouter un utilisateur</i>	8
3.1.2	<i>Créer un groupe</i>	8
4	REGLES	8
4.1	REGLES STANDARD	8
4.2	REGLES AVANCEES	9
4.3	CREER UNE REGLE	10
5	LISTES DE SITES WEB	13
5.1	LISTES NOIRES	13
5.2	LISTES BLANCHES	13
5.3	LISTES GLOBALES ET LOCALES	13
6	PROBLEMES AVEC NETBIOS	14

1 Introduction

1.1 TermiNET – Présentation générale

TermiNET est un pare-feu (firewall) destiné à protéger un PC contre les « attaques » venant de l'extérieur pendant qu'il est connecté à Internet. Lors de l'installation de TermiNET, vous avez le choix entre trois modes de configuration :

1. **Mode Fermé** – Par défaut, bloque tout trafic (entrant et sortant) de votre PC. Votre administrateur peut ensuite définir les accès qui vous sont autorisés, par exemple limiter votre connexion aux transferts FTP, ou vous permettre d'accéder à FTP, à Telnet et au Web. Pour contrôle parental, l'accès du PC peut être limité à certains sites Web. Ces sites Web peuvent être définis explicitement à l'aide de « règles » génériques, ou spécifiés à l'aide d'une « Liste blanche » contenant l'adresse URL des sites Web autorisés.
2. **Mode Ouvert** – Par défaut, n'impose aucune condition de blocage. Votre administrateur peut ensuite interdire l'accès à certains sites par application, par port ou/et par protocole, par exemple en bloquant l'accès à Telnet et à FTP, les communications entrantes du port 25 ou la consultation de certains sites Web. La configuration d'accès de TermiNET peut être définie explicitement à l'aide de « règles » spécifiques ou s'appuyer sur une « Liste noire » contenant l'adresse URL des sites Web interdits.
3. **Mode Protégé** – Permet tout trafic sortant, mais bloque les connexions entrantes qui n'ont pas été émises de votre PC. Dans ce mode, vous pouvez utiliser votre PC normalement pour surfer sur le Web, transférer des fichiers par FTP, etc., mais votre PC est protégé contre toute attaque extérieure pendant que vous êtes connecté à Internet.

TermiNET est une solution de sécurité idéale pour les PME-PMI et pour les utilisateurs privés qui souhaitent se connecter à Internet sans prendre de risques, mais qui ne souhaitent pas investir dans une protection complexe et coûteuse.

1.2 Principales caractéristiques

Les principales caractéristiques de TermiNET sont les suivantes:

- Règles standard et avancées – Activation/désactivation par simple case à cocher.
- Les listes noires et les listes blanches permettent de configurer l'accès au Web en désignant (respectivement) les sites interdits et les sites autorisés.
- La souplesse des règles permet de contrôler les accès par adresses IP, adresses URL, ports et/ou protocoles.
- Les règles peuvent également être configurées de manière à être actives seulement certains jours.
- Similaire aux fenêtres de l'Explorateur Windows, l'interface de TermiNET est intuitive et très simple d'emploi, même pour les utilisateurs à expérience limitée.

2 Principes de base

2.1 Installer TermiNET

Insérez le CD-ROM de TermiNET dans le lecteur de votre PC. L'installation devrait démarrer automatiquement. Si ce n'est pas le cas, choisissez « Démarrer » -> « Exécutez » et entrez « D:\setup » dans la boîte de dialogue qui apparaît (le cas échéant, remplacez « D: » par la lettre d'unité de votre lecteur de CD-ROM). Suivez les instructions qui s'affichent.

Lorsque l'installation est terminée, le PC doit impérativement être redémarré.

2.2 Connexion à TermiNET

2.2.1 Windows 95/98

À chaque démarrage de votre PC, TermiNET active les règles par défaut définies par l'Administrateur. Si plusieurs profils d'utilisateur TermiNET ont été définis, vous disposez de deux solutions pour vous connecter : double-cliquez sur l'icône TermiNET affichée dans la Barre des tâches Windows (zone de l'horloge), ou cliquez avec le bouton droit sur cette icône et choisissez « Connexion » dans le menu qui apparaît. Dans un cas comme dans l'autre, la boîte de dialogue de connexion s'affiche pour vous permettre d'entrer votre nom d'utilisateur et votre mot de passe. (La spécification d'un nom d'utilisateur et d'un mot de passe active le profil de sécurité de l'utilisateur correspondant.)

2.2.2 Windows NT/2000

Les utilisateurs sont automatiquement connectés à TermiNET en fonction du profil de connexion de NT (NT Logon).

2.3 Mode Administrateur

Le mode Administrateur permet d'exécuter les fonctions suivantes : définir un profil de sécurité par défaut pour les utilisateurs, créer un profil pour les nouveaux utilisateurs et spécifier des règles avancées pour certains utilisateurs. Pour passer en mode Administrateur, cliquez avec le bouton droit sur l'icône TermiNET affichée dans la Barre des tâches Windows (zone de l'horloge) et choisissez « Mode Administrateur » dans le menu qui apparaît. Entrez le mot de passe d'Administrateur dans la boîte de dialogue qui s'affiche. L'écran de configuration de TermiNET s'affiche pour vous permettre d'exécuter les fonctions administratives.

Pour quitter le mode Administrateur, fermez l'écran de configuration en choisissant « Fichier » - > « Quitter le mode Administrateur ».

2.4 Interface de TermiNET

L'interface de TermiNET (Figure 1) est accessible uniquement à l'aide du mot de passe Administrateur.

Elle constitue un outil graphique simple d'emploi qui permet de définir les profils de sécurité de chaque machine.

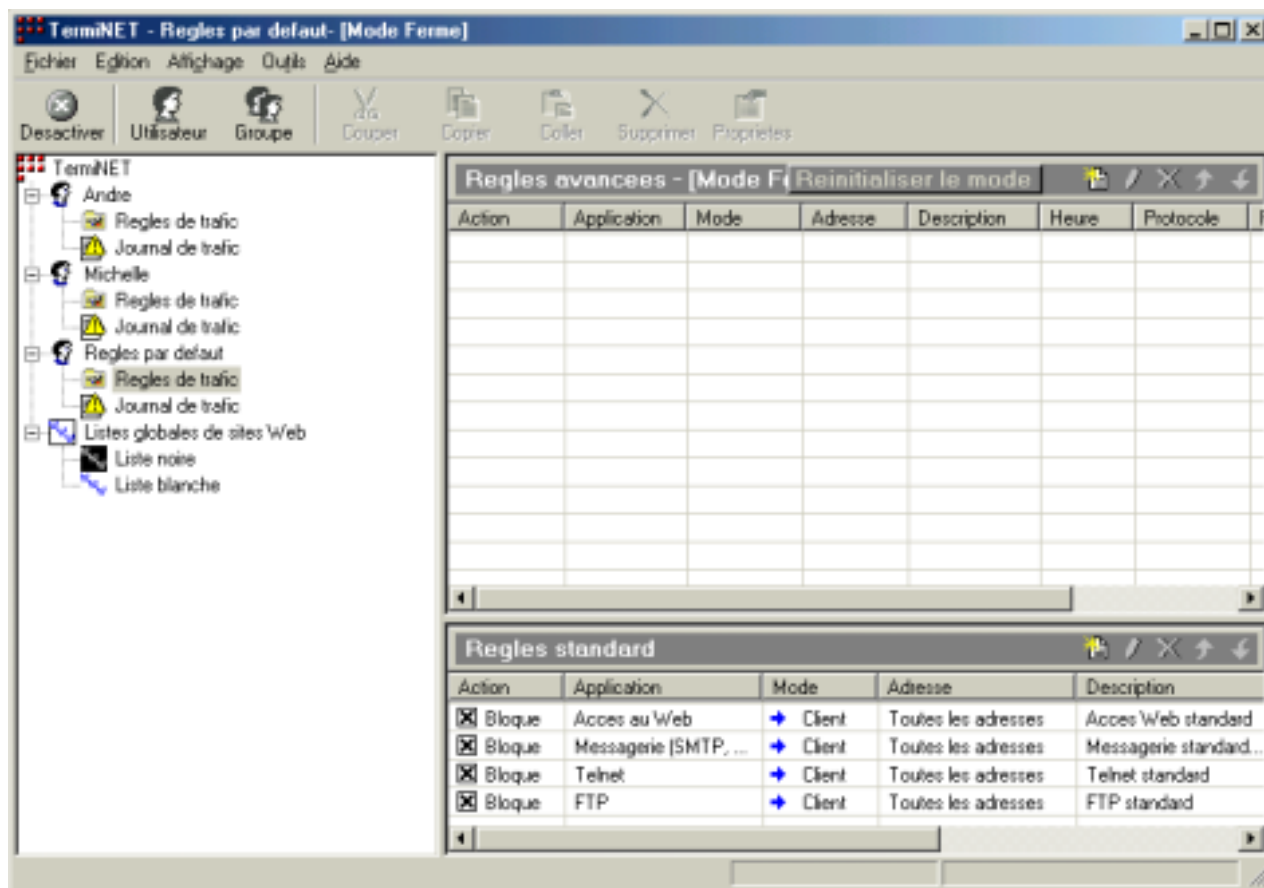


Figure 1

L'interface est divisée en trois fenêtres : la fenêtre de gauche présente l'arborescence du système de sécurité défini pour le PC considéré. La fenêtre inférieure droite présente les « Règles standard », qui sont prédéfinies par le système. La fenêtre supérieure droite présente les règles avancées créées pour le PC considéré. Lorsque vous sélectionnez un utilisateur dans la fenêtre de gauche, les deux fenêtres de droite affichent l'état des règles standard et avancées définies pour cet utilisateur.

Les menus Fichier, Édition et Affichage permettent aux Administrateurs de personnaliser l'interface en fonction de leurs préférences. La séquence « Outils » -> « Options » permet de définir des propriétés générales.

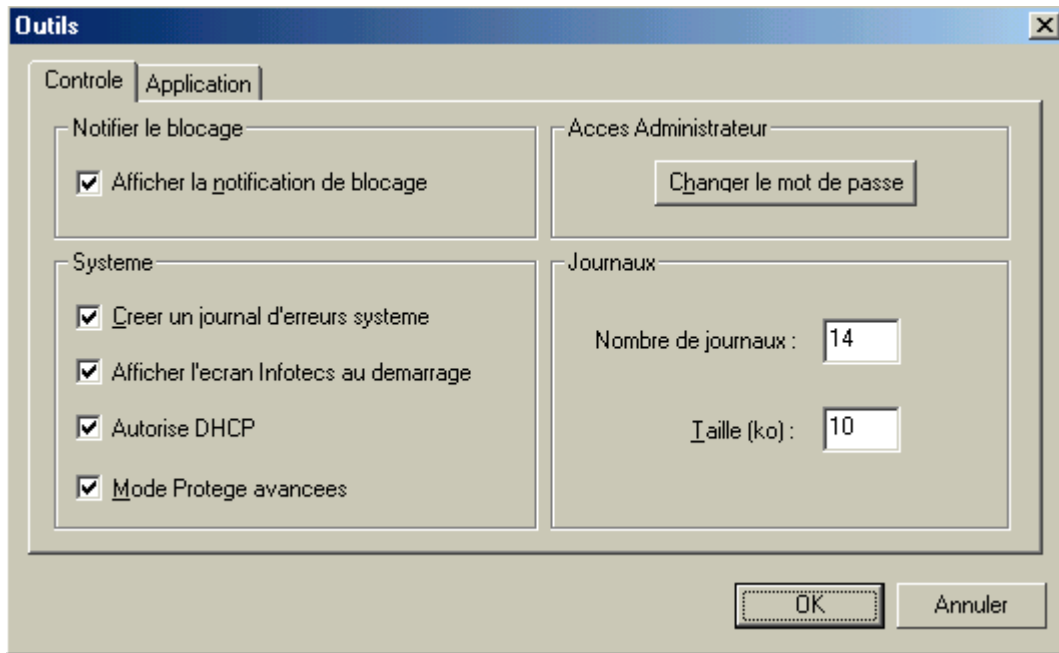


Figure 2

L'onglet Contrôle (Figure 2) contient les options suivantes :

Afficher la notification de blocage	Lorsque cette case est cochée, le journal de trafic affiche les détails du trafic bloqué et du trafic autorisé ; lorsqu'elle est décochée, le journal affiche uniquement les détails du trafic autorisé.
Créer un journal d'erreurs système	Lorsque cette case est cochée, les erreurs système sont enregistrées dans le fichier \Program Files\Infotecs\Terminet\Data\errorlog.txt.
Afficher l'écran INFOTECS au démarrage	Décochez cette case si vous ne souhaitez pas que l'écran d'accueil de TermiNET (logo animé INFOTECS) apparaisse à chaque démarrage de TermiNET.
Changer le mot de passe	Ce bouton permet de changer le mot de passe d'administration.
Nombre de journaux	Spécifie le nombre de journaux de trafic à enregistrer. Lorsque le nombre spécifié est atteint ET que le dernier fichier a atteint la taille maximum spécifiée (voir option suivante), le premier fichier est écrasé.
Taille (ko)	Spécifie la taille maximum autorisée pour chaque journal de trafic. Lorsqu'un journal atteint cette taille, le fichier est enregistré et le système enregistre la suite des données dans le journal suivant.

L'onglet Application (Figure 3) permet de définir de nouvelles applications standard.

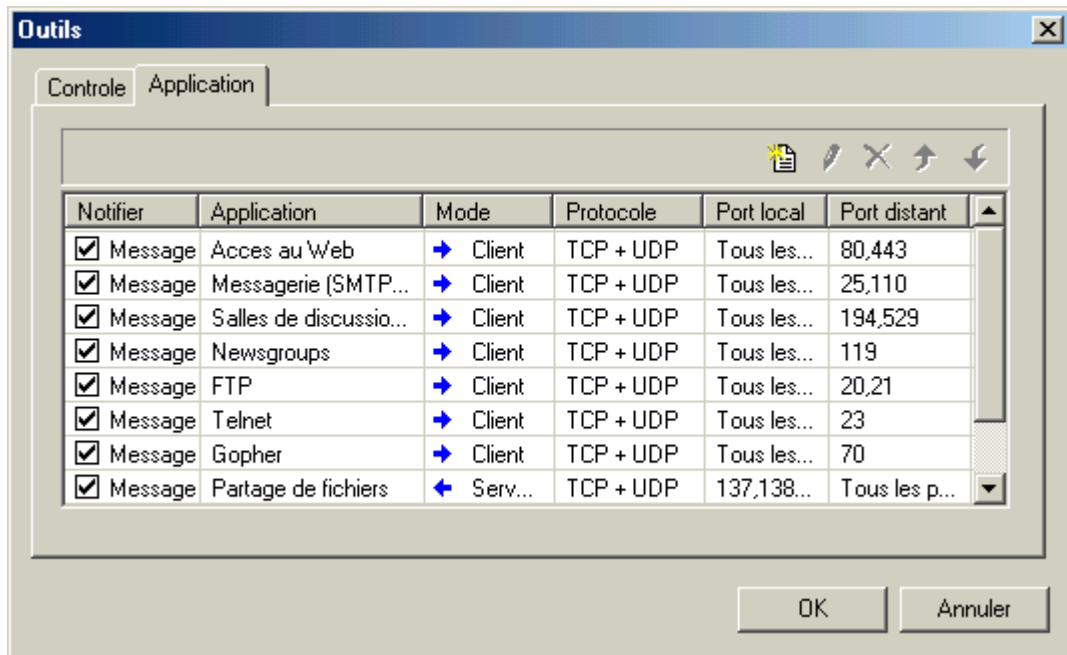


Figure 3

Cliquez sur le bouton Ajouter une application  pour afficher la boîte de dialogue Application personnalisée (Figure 4).

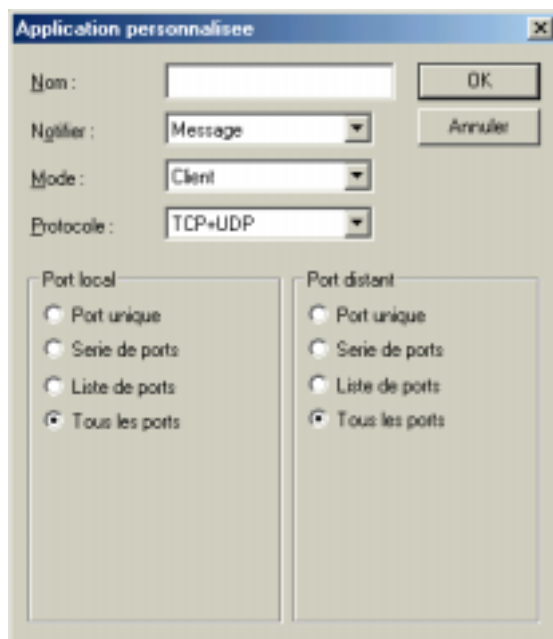


Figure 4

Cette boîte de dialogue permet de définir les options suivantes :

- **Nom:** Spécifiez le nom de la nouvelle application personnalisée.
- **Protocole:** Sélectionnez le protocole à associer à l'application.
- **Notifier:** Sélectionnez Message ou Ignorer. Si vous sélectionnez Message, l'utilisateur verra s'afficher une notification chaque fois qu'un trafic de ce type est bloqué.
- **Direction:** Sélectionnez Entrant ou Sortant.
- **Port distant:** Spécifiez la valeur de port de la machine distante à associer à cette application.
- **Port local:** Spécifiez la valeur de port de la machine locale à associer à cette application.

3 Utilisateurs et groupes

3.1 Gérer les utilisateurs et des groupes

3.1.1 Ajouter un utilisateur

Mode Administrateur uniquement -- Pour ajouter un profil d'utilisateur, cliquez avec le bouton droit sur le niveau le plus élevé de l'arborescence TerMiNET et choisissez « Ajouter un utilisateur » dans le menu qui apparaît (ou cliquez sur le bouton Utilisateur de la barre d'outils). La boîte de dialogue « Propriétés d'utilisateur TerMiNET » apparaît (Figure 5).

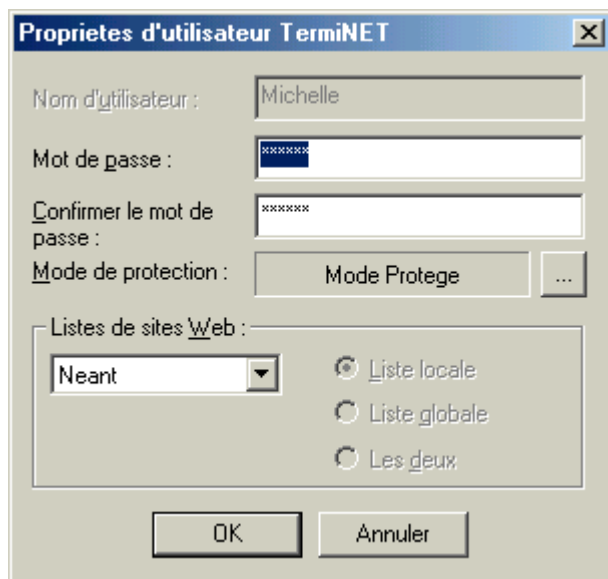


Figure 5

Cette boîte de dialogue permet de définir les options suivantes :

- **Nom d'utilisateur:** Entrez le nom correspondant au nouvel utilisateur.
- **Mot de passe:** Entrez le mot de passe du nouvel utilisateur.
- **Confirmer le mot de passe:** Entrez le mot de passe une deuxième fois.
- **Mode de protection:** Sélectionnez le mode de sécurité par défaut pour cet utilisateur.
- **Listes de sites Web:** Permet selon besoin de limiter l'accès de cet utilisateur à l'aide d'une liste noire ou blanche globale ou locale (voir plus loin).

3.1.2 Créer un groupe

Les groupes permettent d'organiser les utilisateurs présents dans de TerMiNET. Pour créer un groupe, cliquez avec le bouton droit sur le niveau le plus élevé de l'arborescence, choisissez « Ajouter un groupe » dans le menu qui apparaît et tapez le nom de votre choix pour ce nouveau groupe. Pour introduire des utilisateurs dans un groupe, il suffit de faire glisser leur nom dans le groupe requis. Par ailleurs, vous pouvez créer un utilisateur dans un groupe existant en cliquant avec le bouton droit sur le nom de ce groupe dans l'arborescence et en choisissant « Ajouter un utilisateur » dans le menu qui apparaît.

4 Règles

TerMiNET permet de définir des règles de trafic « standard » ou « avancées ».

4.1 Règles standard

Ce type de règle s'applique à **toutes** les adresses IP pour permettre ou interdire l'accès global à certains services. TerMiNET est livré avec quatre règles standard : Accès au Web, Messagerie, FTP et Telnet. Pour ajouter une règle, sélectionnez l'utilisateur requis dans l'arborescence (fenêtre de gauche), cliquez avec le bouton droit dans la fenêtre « Règles standard » et sélectionnez « Ajouter une règle » dans le menu qui apparaît pour afficher la boîte de dialogue d'ajout de règle (Figure 6).

4.2 Règles avancées

Ce type de règle s'applique à **certaines** adresses IP ou URL pour permettre ou interdire l'accès global des sites ou des services correspondants. Pour ajouter une règle, sélectionnez l'utilisateur requis dans l'arborescence (fenêtre de gauche), cliquez avec le bouton droit dans la fenêtre « Règles avancées » et sélectionnez « Ajouter une règle » dans le menu qui apparaît pour afficher la boîte de dialogue d'ajout de règle (Figure 6).

En mode Protégé, seules les règles avancées peuvent être configurées.

4.3 Créer une règle

La boîte de dialogue d'ajout de règle (Figure 6) permet de définir une nouvelle règle.

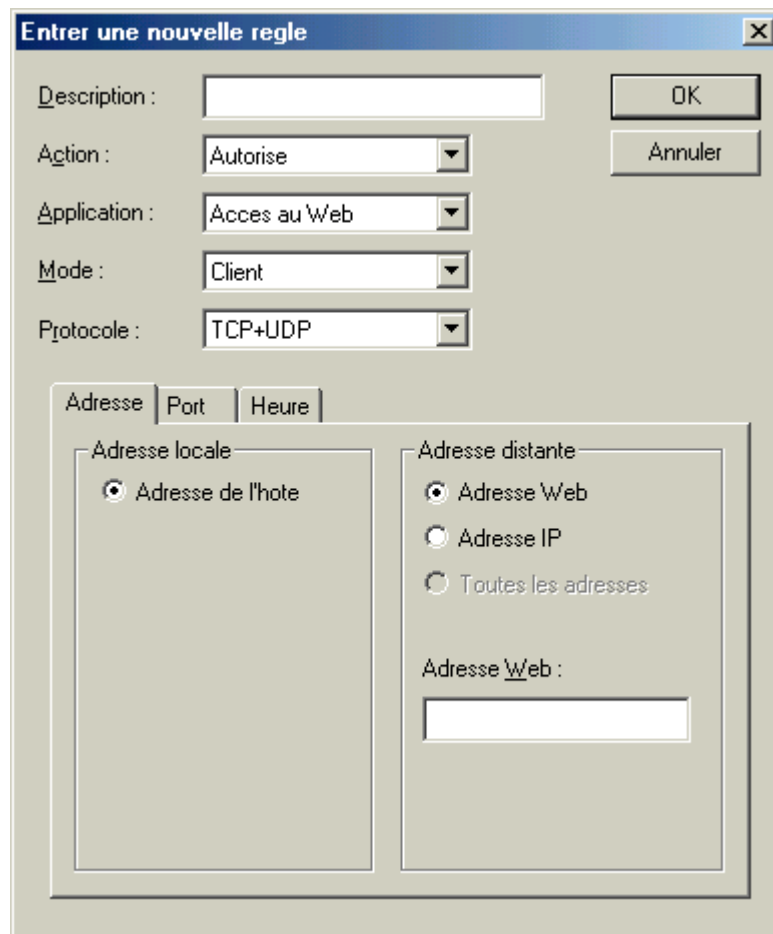


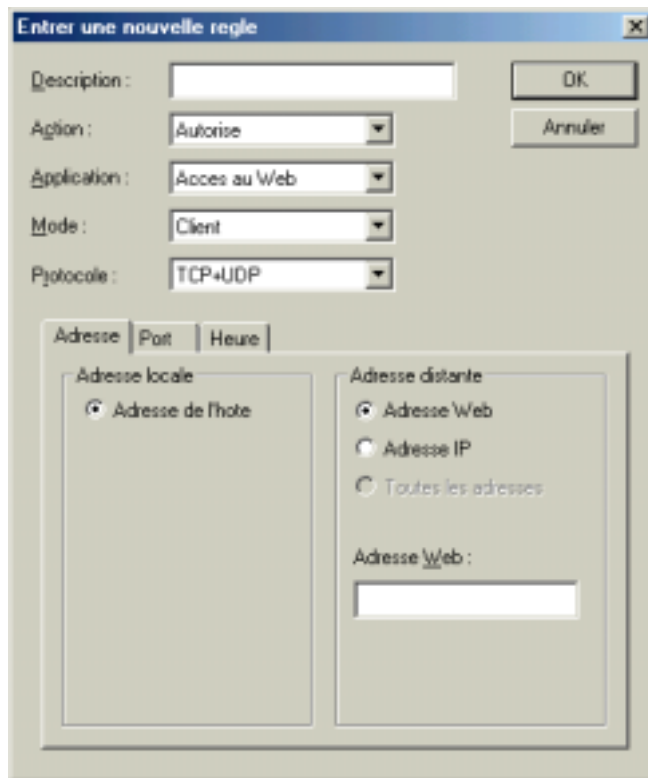
Figure 6

Cette boîte de dialogue contient les options suivantes :

Description	(Facultatif) Tapez la description de la nouvelle règle.
Action	Précisez si cette règle devra Autoriser ou Bloquer le trafic défini dans cette boîte de dialogue.
Application	Sélectionnez l'application à laquelle s'appliquera la nouvelle règle (ou tapez son nom directement).
Mode	Précisez si la machine locale jouera le rôle de client ou de serveur pour cette règle (avec la valeur « Client », la règle sera appliquée au trafic sortant ; avec la valeur « Serveur », elle sera appliquée au trafic entrant).

Les onglets Adresse (Figure 7), Port (Figure 8) et Heure (Figure 9) permettent de définir les paramètres évolués de la règle.

Onglet Adresse:



The screenshot shows a dialog box titled "Entrer une nouvelle règle" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Description:** A text input field.
- Action:** A dropdown menu set to "Autorise".
- Application:** A dropdown menu set to "Accès au Web".
- Mode:** A dropdown menu set to "Client".
- Protocole:** A dropdown menu set to "TCP+UDP".
- Buttons:** "OK" and "Annuler" buttons are located to the right of the "Action" and "Application" fields.
- Address Selection:** A section with three tabs: "Adresse", "Port", and "Heure". The "Adresse" tab is active and contains two columns:
 - Adresse locale:** A radio button labeled "Adresse de l'hôte" is selected.
 - Adresse distante:** Three radio buttons are present: "Adresse Web" (selected), "Adresse IP", and "Toutes les adresses".
 - Adresse Web:** A text input field is located below the "Adresse distante" section.

Figure 7

Règle standard -- La seule valeur disponible est « Toutes les adresses ».

Règle avancée -- Vous pouvez spécifier le site auquel la règle s'applique en indiquant l'adresse URL ou IP de celui-ci.

Vous pouvez activer le bouton « Adresse URL », puis taper l'adresse du site dans le champ « Adresse URL ».

Si vous activez le bouton « Adresse IP », le libellé du champ « Adresse URL » devient « Adresse IP »..

Onglet Port:

Entrez une nouvelle règle

Description :

Action :

Application :

Mode :

Protocole :

Adresse | **Port** | Heure

Port local

Port unique

Serie de ports

Liste de ports

Tous les ports

Port distant

Port unique

Serie de ports

Liste de ports

Tous les ports

Liste des ports:

80
443

Cet onglet permet de spécifier le port ou la série de ports auxquels la règle doit s'appliquer. Les paramètres de port doivent être configurés à la fois sur la machine locale et sur la machine distante. Options disponibles:

- **Port unique:** Pour associer un seul numéro de port à la règle.
- **Série de ports:** Pour associer un ensemble de ports à la règle.
- **Liste de ports:** Pour associer plusieurs ports à la règle.
- **Tous les ports:** Pour associer l'ensemble des ports à la règle.

Figure 8

Heure:



Intervalle	
<input checked="" type="checkbox"/> Lundi	Oui
<input checked="" type="checkbox"/> Mardi	Oui
<input checked="" type="checkbox"/> Mercredi	Oui
<input checked="" type="checkbox"/> Jeudi	Oui
<input checked="" type="checkbox"/> Vendredi	Oui
<input checked="" type="checkbox"/> Samedi	Oui
<input checked="" type="checkbox"/> Dimanche	Oui

Cet onglet permet de limiter l'application de la règle à certains jours de la semaine.

Figure 9

5 Listes de sites Web

Les listes de sites Web permettent de bloquer (liste noire) ou d'autoriser (liste blanche) l'accès aux sites qu'elles spécifient. Ces listes sont mutuellement exclusives : l'utilisateur qui est associé à une liste noire ne peut pas utiliser une liste blanche et vice versa.

5.1 Listes noires

Les listes noires bloquent l'accès à certains sites, même si cet accès est autorisé par une règle. Exemple : une règle standard autorise l'accès à l'ensemble du Web, mais le site `www.site_non.com` figure dans une liste noire ; dans ce cas, l'utilisateur peut visiter tous les sites du Web à l'exception de `www.site_non.com`.

5.2 Listes blanches

Les listes blanches autorisent l'accès à certains sites, même si cet accès est bloqué par une règle. Exemple : une règle standard bloque tout accès au Web, mais le site `www.disney.com` figure dans une liste blanche ; dans ce cas, l'utilisateur ne peut visiter aucun site Web à l'exception de `www.disney.com`.

5.3 Listes globales et locales

Les listes noires et blanches peuvent être de type Local ou Global. Les listes « globales » sont créées par l'Administrateur et peuvent être appliquées à l'ensemble des utilisateurs. Les entrées d'une liste globale sont appliquées à tous les utilisateurs que l'Administrateur a associé à une liste globale. Les listes « locales » sont créées pour un utilisateur donné. Les entrées d'une liste globale sont appliquées uniquement à l'utilisateur pour lequel cette liste a été créée.

6 Problèmes avec NetBIOS

Certaines difficultés peuvent apparaître lors de l'accès à un hôte à l'aide de NetBIOS (via TCP/IP, en mode Protégé). Ces problèmes se produisent lorsque votre PC utilise le mode "diffusion/broadcast" pour déterminer l'adresse IP d'un hôte du réseau. En mode Protégé, TermiNET bloque les messages renvoyés en réponse par les hôtes, ce qui empêche l'établissement de la communication.

Solution -- Créer dans le fichier "HOSTS" une entrée mappant l'adresse IP des hôtes interrogés avec leur nom NetBIOS. "HOSTS" est un fichier texte qui réside généralement dans le dossier C:\windows (98) ou \system32\drivers\etc (NT) ; ce fichier peut être manipulé à l'aide de tout éditeur de texte. Le fichier "hosts.sam" (également présent dans ce dossier) décrit la structure des fichiers. Exemple de mappages déclarés dans un fichier Hosts :

```
192.168.25.2 myserver.myorg.com
192.168.56.10 nt_server_1
```

Autre exemple -- Pour communiquer avec l'hôte "nt_server_2", dont l'adresse IP est 192.168.35.23, éditez le fichier de manière à obtenir ceci :

```
192.168.25.2 myserver.myorg.com
192.168.55.10 nt_server_1
192.168.35.23 nt_server_2
```

Remarque -- Ce problème ne se manifeste pas si votre réseau dispose d'un serveur WINS.