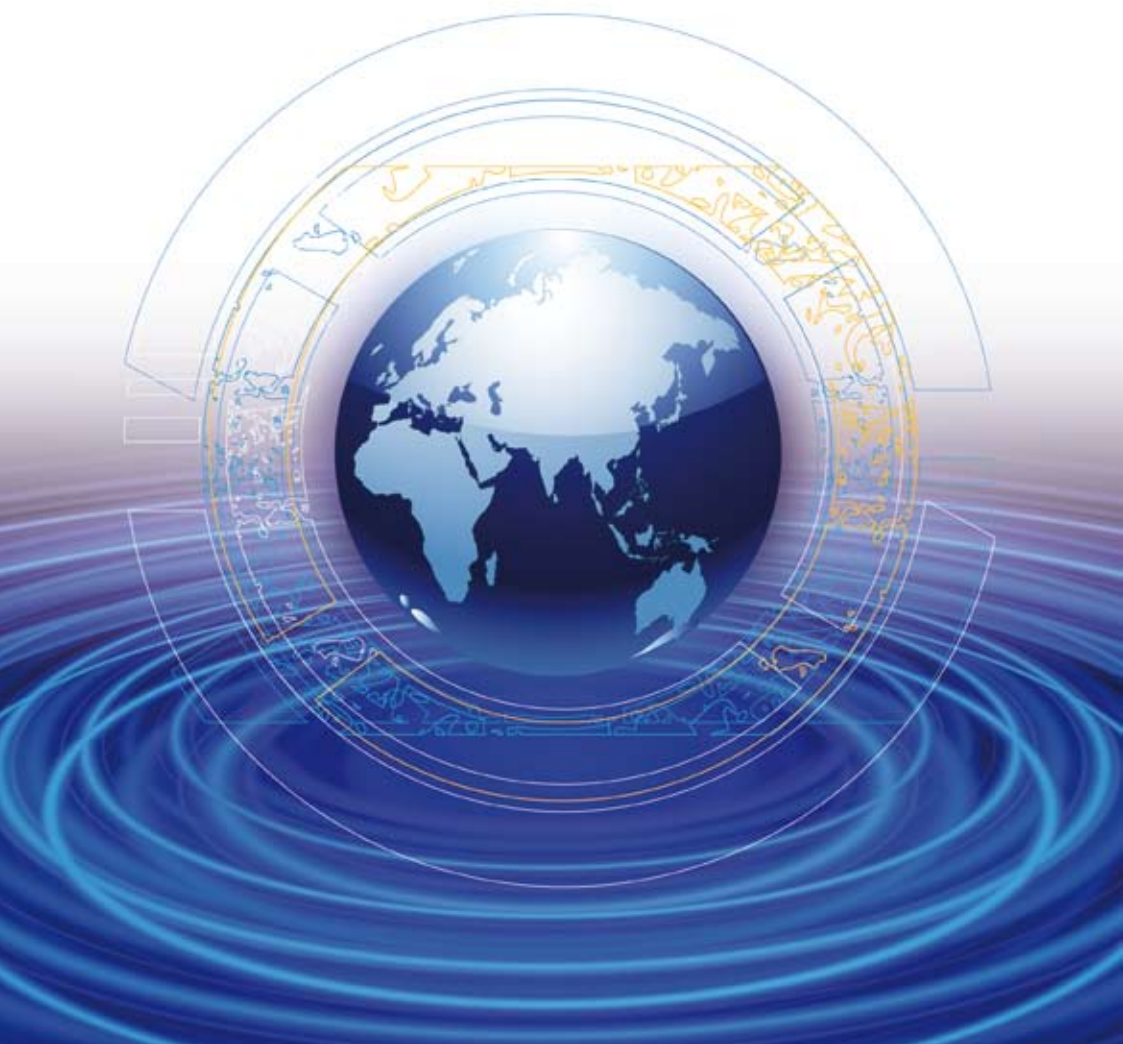


# PROFIL NETWORK FILTER

La réponse globale aux risques numériques liés au facteur humain



MANUEL UTILISATEUR





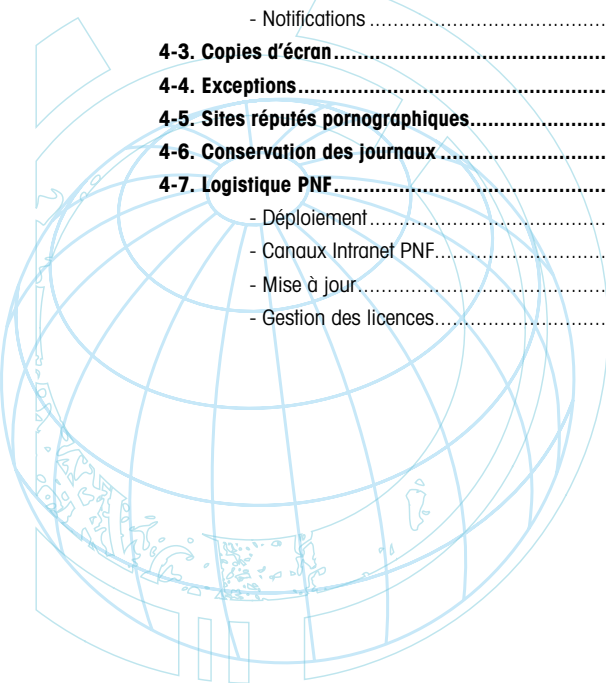
<b>1 - PRÉSENTATION .....</b>	<b>4</b>
<b>1-1. Caractéristiques du produit.....</b>	<b>5</b>
<b>1-2. Configuration requise.....</b>	<b>5</b>
<b>2 - PRISE EN MAIN DU LOGICIEL.....</b>	<b>6</b>
<b>2-1. Installation de Profil Network Filter .....</b>	<b>6</b>
<b>2-2. Déploiement de l'agent de sécurité .....</b>	<b>6</b>
- Déploiement centralisé.....	7
- Déploiement individuel .....	7
<b>2-3. Règles et politiques de sécurité .....</b>	<b>7</b>
- Exemple 1 : Envoi d'e-mail .....	8
- Exemple 2 : Téléchargements.....	9
- Exemple 3 : Accès au Web .....	10
- Exemple 4 : Disques amovibles.....	11
<b>2-4. La console d'administration .....</b>	<b>12</b>
- Lancement de la console .....	12
- Les principales fonctionnalités .....	12
- Interface de la console d'administration .....	13
Barre de menus.....	13
Les fenêtres de la console.....	13
<b>3 - QUOI ? POUR QUI ? QUAND ?.....</b>	<b>16</b>
<b>3-1. Les éléments à surveiller .....</b>	<b>16</b>
- Utilisation générale.....	16
Accès à Internet .....	16
Accès à l'ordinateur .....	16
- Données sensibles.....	17
Coordonnées fiscales et bancaires.....	17
Coordonnées postales et téléphoniques.....	17
- Listes de contacts .....	17
- Listes de sites Internet.....	17
- Filtrage des contenus Internet .....	18
Catégories .....	18
Langues et jeux de caractères .....	18
Détection des images pornographiques.....	18
- Téléchargements Internet.....	19
- Entrées et sorties réseau .....	19



- Système Windows..... 19
  - Types de disques..... 19
  - Types de dossiers..... 20
  - Programmes et types de fichiers..... 20
  - Sécurité système..... 20
- 3-2. Utilisateurs, ordinateurs, groupes, domaines..... 20**
  - Les utilisateurs et les domaines gérés par Windows..... 21
  - Les utilisateurs gérés par PNF..... 22
  - Les ordinateurs..... 22
- 3-3. Les plages horaires..... 22**
- 3-4. Règles et politiques..... 22**

**4 - LA PANOPLIE DE L'ADMINISTRATEUR..... 24**

- 4-1. Rapports..... 24**
- 4-2. Alertes..... 24**
  - Messages de blocage..... 24
  - Notifications..... 25
- 4-3. Copies d'écran..... 25**
- 4-4. Exceptions..... 25**
- 4-5. Sites réputés pornographiques..... 25**
- 4-6. Conservation des journaux..... 26**
- 4-7. Logistique PNF..... 26**
  - Déploiement..... 26
  - Canaux Intranet PNF..... 26
  - Mise à jour..... 27
  - Gestion des licences..... 27





## 1 - PRÉSENTATION

Profil Network Filter (PNF) est un système de filtrage conçu pour optimiser la gestion du réseau local de votre entreprise en s'adaptant à vos besoins en termes de limitation des accès **à Internet** et **aux ordinateurs** de vos usagers et collaborateurs.

Avec Profil Network Filter vous pouvez filtrer les accès Internet que vous estimez contestables ou «dissipateurs» et réguler l'accès de vos utilisateurs au réseau d'entreprise.

Le filtrage pour une ou plusieurs stations de travail est défini par l'administrateur au niveau de la **console** de Profil Network Filter, puis implanté au niveau de chaque station de travail par des **agents de sécurité déployés**.

Les agents de sécurité PNF agissent en transparence par rapport aux applications métier et généralistes installées sur les stations de travail, qui de ce fait n'ont pas besoin d'être re-configurées.

Le filtrage porte sur un large éventail d'**éléments à surveiller**, liés à la fois à l'usage de l'Internet et à l'usage de la station de travail à proprement parler. Les éléments à surveiller sont aussi variés qu'une donnée sensible (par exemple le numéro d'une carte bancaire d'entreprise) ou la possibilité de brancher un lecteur externe (mini-carte mémoire, clé USB). Pour une liste complète, voir **Les éléments à surveiller**.

Pour devenir opérationnel, un élément sous surveillance doit être appliqué à un ou plusieurs ordinateurs ou à un ou plusieurs utilisateurs et éventuellement associé à une étendue dans le temps. La conjonction des trois définit une règle de sécurité :

**Règle de sécurité** = **Élément à surveiller** + **Utilisateur(s)** + **Plage horaire**  
 («Quoi ?») «Pour qui ?» «Quand ?»

A leur tour, les règles de sécurité peuvent être agrégées pour former des politiques de sécurité.

L'ensemble donne à l'administrateur du réseau d'entreprise les moyens d'accomplir les missions qui lui reviennent en matière de sécurité :

- analyse des besoins et mise en place des consignes des dirigeants de l'entreprise
- définition des règles à construire en fonction des événements à contrôler
- paramétrage personnalisé des différents types d'objets de sécurité proposés.

La souplesse du système offre à l'administrateur tous les moyens de réagir rapidement aux événements.

Lorsqu'un utilisateur enfreint une règle qui lui a été affectée, une notification, ou alerte de sécurité, peut être transmise par courrier électronique à l'administrateur. Peuvent également être générés des rapports récapitulants les accès, les alertes de sécurité, etc.

Profil Network Filter utilise des techniques d'intelligence artificielle pour catégoriser les documents envoyés et reçus (pages web, courrier électronique). Au-delà des catégories prédéfinies (une trentaine), l'administrateur peut définir des catégories personnalisées à partir de mots et d'expressions présents dans les documents.

Enfin, Profil Network Filter dispose d'un mécanisme de mise à jour en ligne du serveur, de la console et des postes clients. L'ensemble est paramétrable à partir de la console.



## 1-1. Caractéristiques du produit

- Gestion des topologies réseau orientées domaine et groupe de travail
- Catégorisation automatique
- Filtrage multi-protocoles (Web, FTP, e-mail, messageries instantanées)
- Création de listes d'urls personnalisées
- Création de listes de contacts
- Gestion des données sensibles (interdites d'envoi)
- Sécurité sur les dossiers clients
- Détection automatique d'images pornographiques

## 1-2. Configuration requise

### Serveur :

- 1GB RAM par tranche de 100 utilisateurs
- 400 Mo d'espace disque dur disponible
- Microsoft Windows (32 bits) 2000, XP, 2003, Vista Pro.

### Console (si installée séparément du serveur) :

- 256 Mo de RAM
- 50 Mo d'espace disque dur disponible
- Microsoft Windows (32 bits) 2000, XP, 2003, Vista Pro.

### Ordinateurs sous contrôle :

- 256 Mo RAM
- 20 Mo d'espace disque dur disponible
- Microsoft Windows (32 bits) 2000, XP, 2003, Vista Pro, XP Home\*, Vista Home\*.

\* Les éditions Home ne permettent pas le déploiement centralisé (voir Déploiement de l'agent de sécurité).



## 2 - PRISE EN MAIN DU LOGICIEL

### 2-1. Installation de Profil Network Filter

Profil Network Filter est composé de trois applications distinctes :

- une console d'administration
- un serveur de règles définies à l'aide de la console
- des agents de sécurité déployés, qui viendront chercher auprès du serveur les politiques à implanter.

Bien que les deux premiers soient conceptuellement indissociables dans le processus de création de règles, vous pouvez néanmoins choisir de les dissocier en termes d'installation, par exemple en installant la console d'administration sur l'ordinateur de l'administrateur et la base de règles sur un serveur d'applications. Afin de vous le permettre, l'installation de Profil Network Filter présente les possibilités ci-dessous :

- installation complète
- installation de la console uniquement
- installation du service seul.

La liste des éléments à renseigner sera donc plus ou moins fournie selon l'installation choisie dans une étape donnée :

- l'identifiant et le mot de passe d'un accès administrateur sur l'ordinateur d'installation du service sont nécessaires à ce dernier pour accomplir des tâches indépendamment de toute session ouverte
- le cas échéant, les coordonnées de l'annuaire Active Directory sont nécessaires pour formuler les demandes d'information sur les utilisateurs associés
- le port d'écoute du serveur est le carrefour de transit des règles imposées vers les agents et - dans le sens inverse - des retours d'information (alertes, journalisation etc.)

Bien entendu, toutes les informations saisies lors de l'installation seront ensuite accessibles pour modification depuis la console d'administration (voir aussi **Canaux Intranet PNF**).

### 2-2. Déploiement de l'agent de sécurité

C'est à l'agent de sécurité d'implanter les politiques définies à la console, et de ce fait il doit être présent sur chacune des stations de travail protégées.

La génération d'un agent de sécurité se fait de façon assistée à partir de la console, avec des options portant sur le comportement de l'agent au moment de son installation :

- notification de l'utilisateur de la station du début de l'installation
- déroulement automatique ou non de l'installation
- options de re-démarrage

Ainsi que sur le comportement général de l'agent en cas d'impossibilité de contacter le serveur central :

- accès à l'ordinateur (conforme au plus récent jeu de règles sauvegardé localement), ou
- refus de tout accès à l'ordinateur en attendant le rétablissement du lien avec la base centrale PNF.

Dans le premier cas, la remontée pour journalisation des événements produit pendant l'absence de lien aura lieu au prochain rétablissement de la communication avec la base centrale.

Pour déployer et respectivement retirer les agents de sécurité des ordinateurs, utilisez le menu **Outils > Déploiement de Profil Network Filter**. Selon les versions du système Windows sur les ordinateurs de votre réseau, deux méthodes de



déploiement vous sont proposées :

- la première, centralisée, vous permet d'effectuer depuis la console un déploiement (ou une désinstallation) à distance sur les postes clients. Elle fonctionne pour des stations de travail sous Windows 2000, XP Pro, Vista Pro
- la seconde, vous permet de créer un empaquetage d'installation pour un déploiement (ou une désinstallation). Dans ce cas, il s'agit de mettre un fichier **.EXE** ou **.ZIP** à la disposition des postes clients afin qu'ils soit exécuté ultérieurement. Cette méthode est utilisable quel que soit la version de Windows sur les ordinateurs ciblés (voir **Configuration requise**).

## **Déploiement centralisé**

Le déploiement centralisé fonctionne pour des stations de travail sous Windows 2000, XP Pro, Vista Pro.

L'assistant de déploiement centralisé passe par le choix des ordinateurs ciblés, sachant que chaque ordinateur doit être au moins allumé (avec ou sans session utilisateur active).

Si vous voulez ajouter un ordinateur qui n'appartient à aucun domaine ou groupe de travail, cliquez sur **Ajouter** et remplissez tous les champs le concernant.

Ensuite, vous pouvez suivre le déroulement du transfert et de l'installation de l'agent sur chaque station de travail sélectionnée.

## **Déploiement individuel**

La création d'un empaquetage d'installation ou de désinstallation individuelle d'agent n'exige pas d'information sur les ordinateurs ciblés, en revanche il vous appartient de lui choisir un endroit de sauvegarde, de préférence dans un espace accessible ultérieurement au lancement individuel depuis chaque ordinateur.

De même, selon les politiques de sécurité déjà en place dans votre réseau, vous pouvez choisir entre la génération d'un empaquetage sous la forme d'un exécutable **.EXE** ou d'une archive **.ZIP**.

## **2-3. Règles et politiques de sécurité**

Les cinq exemples qui suivent pourront vous aider à rapidement tirer parti de la console de Profil Network Filter, en vous présentant quelques-unes de ses fonctions les plus utiles :

- créer et configurer un élément à surveiller
- créer une règle à partir des éléments que vous aurez créés
- affecter une règle à des utilisateurs ou groupes d'utilisateurs.

Ces exemples ne vous proposent, en général, qu'un seul moyen d'accomplir certaines tâches. Nous vous suggérons donc de consulter les chapitres qui traitent de chaque aspect en détail (**Quoi ? Pour qui ? Quand ?**, ainsi que **La panoplie de l'administrateur**).

Envoi de courrier électronique : **Exemple 1 : Envoi d'e-mail**

Téléchargements sur Internet : **Exemple 2 : Téléchargements**



Accès au Web (par liste et par détection de contenu) : **Exemple 3 : Accès au Web**

Accès aux disques/lecteurs d'un ordinateur : **Exemple 4 : Disques amovibles**

## **Exemple 1 : Envoi d'e-mail**

**Objectif** : limiter l'envoi de courriers électroniques aux adresses internes de l'entreprise.

- 1 - Dans le volet **Quoi ?** de la console d'administration, développez l'arborescence **Éléments à surveiller**, puis sélectionnez **Listes de contacts**.
- 2 - Double-cliquez sur **Nouvelle liste de contacts** dans le volet central.
- 3 - Introduisez **Adresses internes** dans le champ **Nom** correspondant.
- 4 - Introduisez une adresse e-mail générique correspondant au domaine de votre entreprise, par exemple : **\*@entreprise.fr**, puis cliquez sur **Ajouter**.
- 5 - Afin d'utiliser le nouvel élément à surveiller **Adresses internes**, faites un clic droit sur la racine du volet **Politiques**, puis choisissez **Nouveau > Politique Internet**.
- 6 - Le volet central contient maintenant la politique nouvellement créée. Nommez-la **E-mail en interne**.
- 7 - A droite dans le volet central, appuyez sur le bouton **+**, puis choisissez **Nouvelle règle** dans le menu qui apparaît.
- 8 - Dans le volet central, pour chaque colonne de la nouvelle règle, cliquez et déployez la liste correspondante, de façon à obtenir la configuration ci-dessous :

<b>Etat</b>	<b>Ordinateur</b>	<b>Flux</b>	<b>Élément à surveiller</b>	<b>Plage horaire</b>
Icône verte («Permis»)	Tous	E-mail sortant	Adresses internes	Aucune

- 9 - Dans le volet **Politiques**, faites un clic droit sur la nouvelle politique **E-mail en interne** et choisissez **Affecter la politique aux utilisateurs**.
- 10 - Utilisez les deux volets du dialogue qui s'ouvre pour choisir des utilisateurs et/ou des groupes de travail concernés, puis validez avec **OK**.
- 11 - Enregistrez la nouvelle configuration en utilisant le menu principal de la console **Fichier > Enregistrer**.



## Exemple 2 : Téléchargements

**Objectif :** Autoriser uniquement le téléchargement depuis l'Internet des fichiers de type document (texte, .DOC et .PDF).

1 - Dans le volet **Quoi ?** de la console d'administration, développez l'arborescence **Éléments à surveiller**, puis sélectionnez **Téléchargements Internet**.

2 - Double-cliquez sur **Nouvel objet téléchargements Internet** dans le volet central.

3 - Introduisez **Textes via Internet** dans le champ **Nom** correspondant.

4 - Dans le panneau inférieur, cochez les options **Textes** et **.PDF** respectivement.

5 - Afin d'utiliser le nouvel élément à surveiller **Textes via Internet**, faites un clic droit sur la racine du volet **Politiques**, puis choisissez **Nouveau > Politique Internet**.

6 - Le volet central contient maintenant la politique nouvellement créée. Nommez-la **Téléchargement de textes**.

7 - A droite dans le volet central, appuyez sur le bouton +, puis choisissez **Nouvelle règle** dans le menu qui apparaît.

8 - Dans le volet central, pour chaque colonne de la nouvelle règle, cliquez et déployez la liste correspondante, de façon à obtenir le configuration ci-dessous :

Etat	Ordinateur	Flux	Élément à surveiller	Plage horaire
Icône verte («Permis»)	Tous	HTTP	Textes via Internet	Aucune

9 - Dans le volet **Politiques**, faites un clic droit sur la nouvelle politique **Téléchargement de textes** et choisissez **Affecter la politique aux utilisateurs**.

10 - Utilisez les deux volets du dialogue qui s'ouvre pour choisir des utilisateurs et/ou des groupes de travail concernés, puis validez avec **OK**.

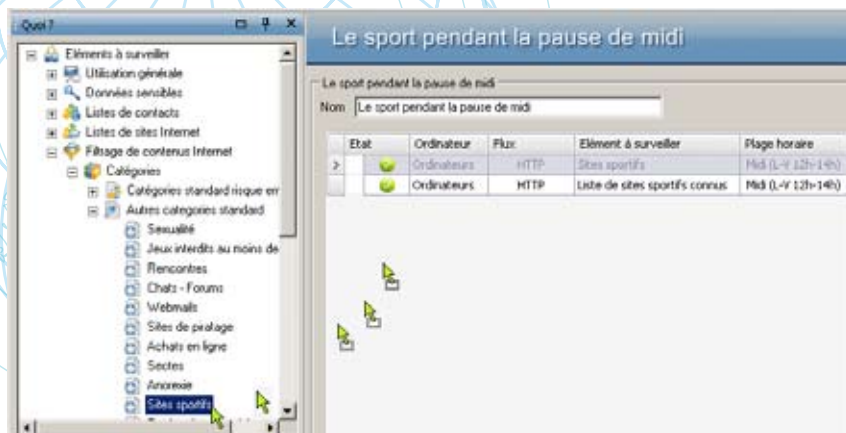
11 - Enregistrez la nouvelle configuration en utilisant le menu principal de la console **Fichier > Enregistrer**.



## Exemple 3 : Accès au Web

**Objectif :** Autoriser l'accès aux sites sportifs uniquement entre 12h et 14h.

- 1 - Dans le volet **Quoi ?** de la console d'administration, développez l'arborescence **Éléments à surveiller**, puis sélectionnez **Accès aux sites Web**.
- 2 - Double-cliquez sur **Nouvelle liste d'URL** dans le volet central.
- 3 - Introduisez **Liste de sites sportifs connus** dans le champ **Nom** correspondant.
- 4 - Dans le panneau inférieur, introduisez tour à tour les sites ci-dessous, en utilisant le bouton **Ajouter** :  
 www.lequipe.fr  
 sports.fr  
 fr.sports.yahoo.fr  
 sport365.fr  
 ...
- 5 - Faites un clic droit sur la racine du volet **Politiques** (à droite de l'écran), puis choisissez **Nouveau > Politique Internet**.
- 6 - Le volet central contient maintenant la politique nouvellement créée. Nommez-la **Le sport pendant la pause de midi**.
- 7 - A droite dans le volet central, appuyez sur le bouton +, puis choisissez Nouvelle règle dans le menu qui apparaît, afin d'introduire l'élément **Liste de sites sportifs connu**.
- 8 - Dans le volet **Quoi ?** de la console d'administration, développez l'arborescence **Éléments à surveiller**, puis sélectionnez **Filtrage des contenus Internet > Catégories > Autres catégories standard**. Cliquez sur l'entrée, puis sans relâcher le bouton de la souris, glissez et lâchez la catégorie **Sites sportifs** dans le volet central :





9 - Dans le volet central, pour chaque colonne de la nouvelle règle, cliquez et déployez la liste correspondante, de façon à obtenir le configuration ci-dessous :

État	Ordinateur	Flux	Élément à surveiller	Plage horaire
Icône verte («Permis»)	Tous	HTTP	Liste de sites sportifs	Pause midi
Icône verte («Permis»)	Tous	HTTP	Pages à contenu sportif	Pause midi

10 - Dans le volet **Politiques**, faites un clic droit sur la nouvelle politique **Le sport pendant la pause de midi** et choisissez **Affecter la politique aux utilisateurs**.

11 - Utilisez les deux volets du dialogue qui s’ouvre pour choisir des utilisateurs et/ou des groupes de travail concernés, puis validez avec **OK**.

12 - Enregistrez la nouvelle configuration en utilisant le menu principal de la console **Fichier > Enregistrer**.

### Exemple 4 : Disques amovibles

**Objectif :** Interdire l’accès aux disques amovibles

1 - Dans le volet **Quoi ?** de la console d’administration, développez l’arborescence **Éléments à surveiller**, puis sélectionnez **Système Windows > Types de disques**.

2 - Double-cliquez sur **Nouvel objet types de disques** dans le volet central.

3 - Introduisez **Disques à risque** dans le champ **Nom** correspondant.

4 - Dans le panneau inférieur, cochez les options **Disquettes** et **Lecteurs CD** et **Disques amovibles** respectivement.

5 - Afin d’utiliser le nouvel élément à surveiller **Disques à risque**, faites un clic droit sur la racine du volet **Politiques**, puis choisissez **Nouveau > Politique ordinateur**.

6 - Le volet central contient maintenant la politique nouvellement créée. Nommez-la **Supports de données amovibles**.

7 - A droite dans le volet central, appuyez sur le bouton **+**, puis choisissez **Nouvelle règle** dans le menu qui apparaît.

8 - Dans le volet central, pour chaque colonne de la nouvelle règle, cliquez et déployez la liste correspondante, de façon à obtenir le configuration ci-dessous :

Etat	Ordinateur	Flux	Élément à surveiller	Plage horaire
Icône rouge («Interdit»)	Tous	Tous	Supports de données amovibles	Aucune

9 - Dans le volet **Politiques**, faites un clic droit sur la nouvelle politique **Supports de données amovibles** et choisissez **Affecter la politique aux utilisateurs**.

10 - Utilisez les deux volets du dialogue qui s’ouvre pour choisir des utilisateurs et/ou des groupes de travail concernés, puis validez avec **OK**.

11 - Enregistrez la nouvelle configuration en utilisant le menu principal de la console **Fichier > Enregistrer**.



## 2-4. La console d'administration

La console d'administration peut être utilisée directement au niveau du serveur mais également à distance. Elle est protégée par un mot de passe afin d'éviter toute administration non autorisée. Pour accéder à la console d'administration, vous pouvez utiliser le raccourci créé dans le **Dossier Enterprise Filter Network** du menu **Démarrer**.

### Lancement de la console

Depuis le serveur : lors du premier lancement, vous devrez préciser le mot de passe administration ainsi qu'une éventuelle question/réponse vous permettant de retrouver le mot de passe en cas d'oubli, à partir de la boîte de dialogue ci-dessous.

Lors des accès ultérieurs à la console, vous devrez saisir le mot de passe. Si le mot de passe saisi est erroné, vous aurez alors accès à la boîte de saisie de la réponse à la question entrée lors de la première connexion.

Depuis un autre poste : lors du premier lancement, vous devrez dans un premier temps préciser les paramètres de connexion au serveur :

- 1 - Sélectionnez les paramètres de la connexion à distance.
- 2 - Sélectionnez le numéro du port.
- 3 - Si vous utilisez un proxy, cochez la case **Connexion par proxy** et entrez ses paramètres.

Une fois les paramètres de connexion saisis, ceux-ci seront sauvegardés et considérés comme les paramètres de connexion à utiliser à chaque démarrage de la console. Ils pourront être modifiés en lançant la commande **Fichier > Se connecter au serveur**.

Les étapes suivantes sont identiques à celles de la connexion directe depuis le serveur.

### Les principales fonctionnalités

La console d'Enterprise Filter Network vous permet de gérer les cinq grandes familles d'objets qui participent du fonctionnement de l'application :

- éléments à surveiller
- utilisateurs, ordinateurs, groupes de travail, domaines, annuaires
- plages horaires
- règles et politiques
- rapports, alertes, statistiques

Et d'effectuer des tâches administratives :

- déploiement de l'agent de sécurité sur les postes du réseau
- création d'empaquetages d'installation et de désinstallation
- mise à jour des composants d'Enterprise Filter Network
- gestion des licences d'utilisation
- communication avec le serveur Enterprise Filter Network.



## Interface de la console d'administration

### Barre de menus

Les commandes générales de la console de Enterprise Filter Network sont accessibles par menu centralisé et reprises en barre à boutons.

**Fichier > Se connecter au serveur** : établir explicitement une connexion avec le serveur Enterprise Filter Network. Par défaut, la console tente dès son lancement la connexion avec le serveur de règles, dans les conditions (local, distant, port, etc.) en vigueur à la session précédente. Cette commande vous permet de reprendre contact avec le serveur en cas de changement d'infrastructure (topologie du réseau ou de l'installation).

De même, cette commande permet à un administrateur gérant les réseaux de plusieurs entreprises de se connecter de façon explicite au serveur PNF dans chaque réseau.

**Fichier > Enregistrer** : enregistrer immédiatement l'état des données au niveau du serveur PNF. De façon générale, les actions explicites d'enregistrement portent sur l'assignation de règles à des utilisateurs et non pas sur les changements des autres objets, ces derniers étant enregistrés en permanence.

**Fichier > Enregistrement programmé le...** : enregistrement planifié des modifications. Ce type de fonctionnement est utile dans tous les cas où l'imposition de nouvelles règles sur les ordinateurs ne doit pas interférer avec des opérations en cours. Avec cette commande vous avez la possibilité d'effectuer la sauvegarde des règles soit en différé une fois, soit de programmer une sauvegarde automatique, par exemple tous les soirs à minuit.

**Fichier > Quitter** : pour fermer la console Enterprise Filter Network.

**Edition > Précédent** : option de navigation pour afficher la fenêtre précédente.

**Edition > Suivant** : option de navigation pour afficher la fenêtre suivante dans l'ordre des fenêtres précédemment affichées.

**Edition > Nouveau** : pour créer un nouvel objet dans le contexte de la fenêtre active.

**Edition > Supprimer** : pour supprimer l'objet sélectionné.

**Edition > Accueil** : pour afficher dans la fenêtre principale les racines des hiérarchies d'objets.

**Affichage > Utilisateurs connectés** : présente la liste de tous les utilisateurs actuellement sous la surveillance de Profil Network Filter. Ceci permet de vérifier en temps réel l'utilisation des postes clients.

**Affichage > Historique des mises à jour** : permet d'obtenir la liste de toutes les mises à jour effectuées au cours des sept derniers jours.

**Affichage > Fenêtres** : pour sélectionner les fenêtres de gestion à afficher ou à cacher.

**Déploiement > Déployer l'agent et Retirer l'agent** : pour installer et respectivement retirer de façon centralisée l'agent



responsable de l'implantation des politiques de sécurité sur les stations de travail (voir **Déploiement centralisé**).

**Déploiement > Créer un empaquetage d'installation et Créer un empaquetage de désinstallation** : pour mettre un fichier .EXE ou .ZIP à la disposition des postes clients afin qu'ils soit exécuté ultérieurement (voir **Déploiement individuel**).

**Déploiement > Configuration...** : pour paramétrer l'identifiant et le mot de passe qui seront nécessaires pour le déploiement centralisé.

**Rapports > Nouveau rapport application**

**Rapports > Nouveau rapport Internet**

**Rapports > Nouveau rapport connexions**

**Rapports > Nouveau rapport Copies d'écran**

Pour créer respectivement un nouveau modèle du type souhaité, à l'aide d'un assistant pour sélectionner le contenu, la portée et la période (voir **Rapports**).

**Rapports > Personnalisation des rapports ...** : pour «signer» visuellement les rapports avec un nom de structure, un logo etc.

## Les fenêtres de la console

Par défaut, la console affiche sept fenêtres : les cinq fenêtres de gestion, la fenêtre d'aide et la fenêtre principale.

Six fenêtres sont ancrées de part et d'autre de la fenêtre principale. A gauche, de haut en bas :

**Éléments à surveiller**

**Utilisateurs**

**Plages horaires**

A droite, de haut en bas :

**Politique**

**Activité**

**Aide**

La largeur de chacune de ces deux colonnes de fenêtres peut être augmentée ou réduite en agissant sur les barres de redimensionnement.

La hauteur de chaque fenêtre peut être augmentée ou réduite de façon individuelle en agissant sur la barre de redimensionnement de la fenêtre.

Le point d'ancrage d'une fenêtre peut être déplacé verticalement dans la colonne où elle se trouve. Pour ce faire, sélectionnez la fenêtre à déplacer en cliquant sur sa barre de titre, puis glissez-la vers la nouvelle position souhaitée.

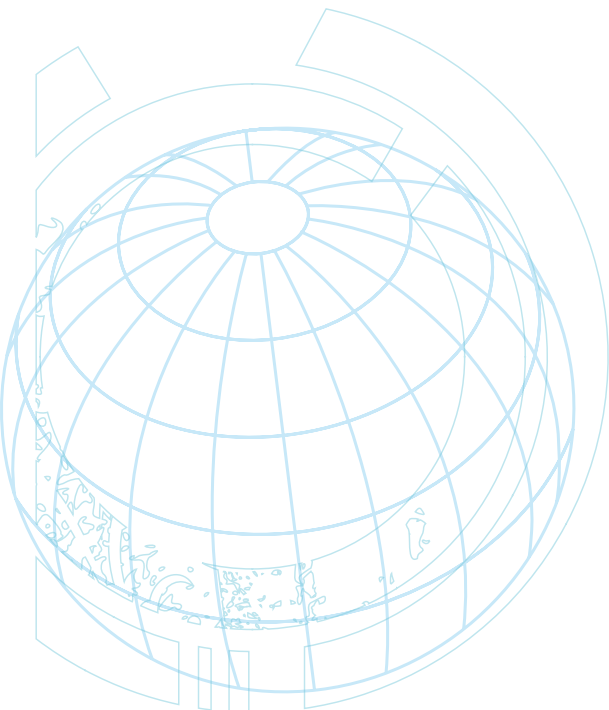
Le point d'ancrage d'une fenêtre peut être déplacé horizontalement d'une colonne de fenêtres à l'autre. Pour ce faire, sélectionnez la fenêtre à déplacer en cliquant sur sa barre de titre, puis glissez-la vers la colonne et la position



souhaitées.

De même, les fenêtres peuvent être ancrées en colonnes, en lignes ou les deux.

Pour afficher/cacher une fenêtre, sélectionnez **Affichage > Fenêtres**, puis sélectionnez / désélectionnez la case correspondante.





## 3 - QUOI ? POUR QUI ? QUAND ?

Dans l'approche de Profil Network Filter, une règle de sécurité se définit comme étant la conjonction d'un élément à surveiller, d'un champ d'application et d'une étendue dans le temps :

**Règle de sécurité** = **Élément à surveiller** + **Utilisateur(s)** + **Plage horaire**  
 («Quoi ?» «Pour qui ?» «Quand ?»)

C'est par l'interface de définition, de manipulation et d'agrégation de ces entités que l'administrateur définit le périmètre de fonctionnement de Profil Network Filter.

### 3-1. Les éléments à surveiller

De façon générale, un élément à surveiller est une entité informatique dont l'accès ou le transit pourraient avoir un impact sur la sécurité de l'entreprise. Le concept couvre des notions aussi variées qu'une information sensible (comme un numéro de carte bancaire d'entreprise), un type de contenu Web ou encore un lecteur externe de cartes mémoire.

(En ce sens, Profil Network Filter est bien plus qu'un surveillant de trafic Internet, tout comme la sécurité physique de l'entreprise ne saurait être réduite au digicode de sa porte d'entrée.)

Pour des raisons de cohérence d'organisation de l'interface, Profil Network Filter différencie les éléments à surveiller qui ont partie liée à l'Internet et ceux qui relèvent strictement de l'utilisation locale de l'ordinateur.

Les noms des éléments à surveiller (prédéfinis dans le logiciel ou créés par l'administrateur) se retrouveront dans les notifications de blocage, les rapports et les statistiques.

#### Utilisation générale

Profil Network Filter vous offre la possibilité de restreindre très sévèrement l'utilisation de tout ou partie des ordinateurs de l'entreprise, en spécifiant des horaires strictes d'accès à Internet ou directement aux ressources locales de l'ordinateur.

#### Accès à Internet

La restriction de l'accès global d'un ordinateur à Internet (aux heures de bureau, par exemple) est un moyen simple de limiter l'usage de l'accès Internet de l'entreprise. Toutes les ressources locales de l'ordinateur (disques durs, ports USB, imprimante, partages au travers du réseau local) restent disponibles.

#### Accès à l'ordinateur

L'interdiction d'accès aux ordinateurs équivaut à un interrupteur intelligent et sélectif de leur alimentation électrique, car en dehors des horaires spécifiés aucune utilisation n'en sera possible.



## **Données sensibles**

Dans l'acception de Profil Network Filter, les données sensibles sont des chaînes de caractères que le logiciel aura pour tâche de détecter dans l'ensemble des échanges de type Internet : formulaires Web, e-mail, messagerie instantanée. Plusieurs catégories sont pré-définies (avec des contraintes de format qui facilitent leur détection), mais vous pouvez en définir des nouvelles, dont le nom apparaîtra de plein droit dans les notifications, les rapports et les statistiques.

## **Coordonnées fiscales et bancaires**

Il s'agit d'une catégorie prédéfinie de chaîne de caractères, avec des contraintes de format qui facilitent la détection sans confusion dans un flux d'échanges. Dans le cas d'un numéro de carte bancaire notamment, les deux groupes de quatre chiffres doivent être correctement remplis afin de déclencher la ou les règles correspondantes.

## **Coordonnées postales et téléphoniques**

Il s'agit d'une catégorie prédéfinie de chaîne de caractères, avec des contraintes de format qui facilitent la détection sans confusion dans un flux d'échanges.

Bien entendu, rien n'empêche d'en créer plusieurs autres afin de gagner en visibilité dans les rapports et dans les notifications, par exemple pour détailler «Lignes directes DRH».

## **Listes de contacts**

Les adresses e-mail présentes dans les listes de contact seront détectées dans les flux de messagerie, et le cas échéant les messages correspondants seront filtrés ou autorisés, selon les règles définies. La présence du caractère générique \* est autorisée à gauche du caractère @ afin de pouvoir spécifier «toutes les adresses du domaine».

## **Listes de sites Internet**

A chaque fois qu'un ordinateur soumis à une règle portant sur une liste de sites formule une demande d'accès, l'adresse demandée est confrontée avec la liste et le cas échéant la règle est déclenchée.

La recherche a lieu quelle que soit l'origine de la requête : navigateur (frappe au clavier ou clic de souris), action utilisateur dans une autre application, requête automatique venant d'un logiciel.

Une liste peut contenir des noms complets de sites (www.domain.com) ou des noms de domaine (domain.com).

Vous pouvez définir autant de listes que vous le souhaitez, afin de détailler le texte des interdictions, les rapports, etc.



## **Filtrage des contenus Internet**

Contrairement aux listes d'accès aux sites, le filtrage sur le contenu attend la réponse du serveur, qu'il analyse ensuite à la volée.

Dans sa version actuelle, Profil Network Filter dispose de deux angles d'attaque différents pour analyser le contenu retourné par le serveur, à savoir le texte et les images.

### **Catégories**

Schématiquement parlant, l'analyse thématique répond à la question « Cette page, de quoi parle-t-elle ? ». (Plusieurs réponses sont possibles, bien qu'en général une catégorie se détache du reste).

Dans un élément à surveiller basé sur les catégories, vous pouvez en choisir une ou plusieurs parmi la trentaine proposée par Profil Network Filter, afin d'interdire ou d'autoriser de façon explicite l'accès à un univers thématique.

Vous pouvez même y rajouter de nouvelles catégories, chacune étant définie par le nombre d'apparitions d'une expression dans le texte. Utilisez pour cela l'entrée **Filtrage des contenus Internet > Catégories personnalisées** dans l'arbre des **Éléments à surveiller**.

Ensuite, vous pouvez panacher les catégories prédéfinies et les vôtres afin de préciser un univers thématique à interdire ou à autoriser.

Notez toutefois qu'une catégorie définie en vertu de la seule présence (unique ou multiple) d'une expression dans un texte ne saurait approcher la finesse de l'analyse que le moteur d'intelligence artificielle de PNF met en oeuvre afin de détecter une de ses catégories prédéfinies.

### **Langues et jeux de caractères**

La détection de contenu Web basée sur la langue employée est un moyen simple de cantonner le flux Web entrant à des contenus en rapport avec le spécifique de l'activité de l'entreprise.

Profil Network Filter vous donne la possibilité de définir autant d'éléments **Langues et jeux de caractères** qu'il vous seront utiles, avec des cases à cocher correspondant aux langues à interdire ou à autoriser.

Les options sont structurées en faisceaux et cercles concentriques en partant de la France, les langues officielles de l'Union Européenne en tête.

### **Détection des images pornographiques**

Profil Network Filter propose trois modes de détection des images pornographiques, avec des comportements distincts

- la détection **en tâche de fond** analyse les images des sites nouveaux et alimente en temps réel une liste noire de sites pornographiques, utilisée pour l'ensemble des utilisateurs de cette détection dans l'entreprise. De ce fait, les accès suivants à un site détecté comme étant à caractère pornographique seront bloqués dès l'envoi de la requête
- la détection en **mode normal** privilégie la vitesse de traitement



- la détection en **mode strict** effectue une analyse complète de chaque image, sans aucune contrainte de temps de réponse d'affichage (temps d'attente utilisateur).

## **Téléchargements Internet**

Le contrôle des types de documents téléchargés depuis l'Internet a pour point d'ancrage la déclaration de type qui précède le document à proprement parler dans la réponse du serveur Web à une requête utilisateur. En définissant un nouvel objet à partir de **Éléments à surveiller > Téléchargements Internet** vous pourrez :

- choisir un ou plusieurs types parmi ceux proposés
- définir de nouveaux types, en tant qu'extension de nom de fichier ou encore en tant que type Internet MIME.

## **Entrées et sorties réseau**

Le contrôle des entrées et sorties réseau porte sur les connexions au sens large qu'un ordinateur peut établir. Cette approche du contrôle des échanges suit de près l'architecture TCP/IP des échanges réseau. De ce fait, on y retrouvera ses concepts de base, à savoir l'adresse IP du distant et le port de communication.

Vous pourrez donc y définir en tant qu'élément à surveiller l'établissement d'une connexion avec :

- une adresse unique
- une classe d'adresses
- toute adresse distante

En utilisant :

- tout numéro de port
- un intervalle de numéros de port, par exemple : de 81 à 8079 (inclus, soit 7999 valeurs)
- une liste de numéros de port, par exemple : 22, 25, 443, 1010 (soit quatre valeurs).

## **Système Windows**

Profil Network Filter déploie sa palette de moyens de surveillance au plus près de l'utilisateur, ce qui lui permet d'aller bien au-delà du contrôle des échanges Internet, pour sécuriser l'utilisation des postes de travail et des contenus locaux.

## **Types de disques**

Un élément Type de disque vous permet de définir un contrôle d'accès à un ou plusieurs disques, identifiés soit par leur appartenance à une classe de périphériques (en cochant la case correspondante) :

- lecteur de disquettes
- lecteur de CD-ROM / DVD-ROM
- lecteur amovible, par exemple clé USB ou lecteur de mémoire SD/SDHC
- lecteur réseau

Soit par identification système, en spécifiant une ou plusieurs lettres de volume.

## **Types de dossiers**



Un élément **Type de dossier** vous permet de définir une contrôle portant sur l'accès à des répertoires génériques du système Windows :

- Ma musique
- Mes images
- Mes vidéos
- Menu **Démarrer**
- Mes Documents
- Voisinage réseau

Ainsi qu'à des répertoires propres, dont il vous appartient d'en saisir les noms.

## Programmes et types de fichiers

Un élément de type **Programmes et types de fichiers** vous permet de définir un contrôle de l'accès à des applications et à l'ouverture de certains types de fichiers.

Dans les deux cas, les plus connus sont présentés en tant que cases à cocher, mais vous pouvez également en saisir d'autres, afin d'obtenir une liste personnalisée.

## Sécurité système

Les éléments de type **Sécurité système** vous permettent de contrôler de façon très fine des aspects propres aux systèmes d'exploitation Microsoft Windows.

Il s'agit d'une trentaine d'éléments, allant de l'affichage des icônes habituellement présentes sur le bureau virtuel Windows jusqu'à l'accès à l'invité de commandes ou encore la possibilité de modifier directement la base de registres du système.

## 3-2. Utilisateurs, ordinateurs, groupes, domaines

Conceptuellement, Profil Network Filter vous permet d'appliquer des règles de surveillance à deux catégories d'entités :

- des utilisateurs identifiés en tant que tels, quels que soient les différents ordinateurs sur lesquels ils travaillent dans l'entreprise
- des ordinateurs reconnus comme tels dans le réseau, quels que soient leurs utilisateurs respectifs.

En sélectionnant un utilisateur ou un ordinateur dans le volet **Pour qui ?** les éléments le concernant apparaissent dans le volet central :

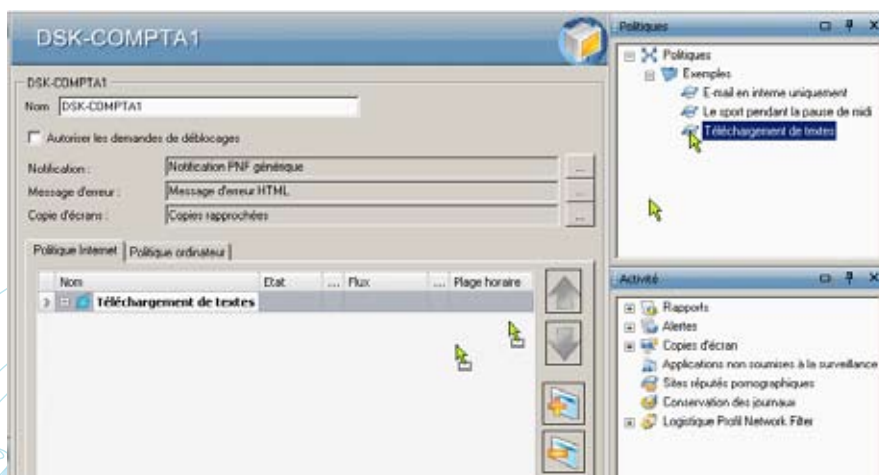
- l'option **Autoriser les demandes de déblocage**. Cocher l'option fera apparaître un bouton **Demander le déblocage** dans l'alerte de blocage sur l'écran contrôlé. Un appui sur le bouton enverra à l'administrateur une demande par e-mail contenant les informations relatives au blocage



- le nom du modèle de **Notification** qui sera employé pour notifier l'administrateur de chaque blocage (voir **Notifications**)
- le nom du modèle **Message de blocage** qui sera employé pour altérer le flux bloqué, selon le cas page HTML, e-mail entrant, e-mail sortant (voir **Messages de blocage**)
- le modèle d'action **Copie d'écran** qui sera employé pour l'ordinateur concerné (voir **Copies d'écran**).

De façon générale, **pour introduire des règles et des politiques** :

- sélectionnez un groupe ou un utilisateur individuel dans cette hiérarchie, de façon à ce que les détails le concernant apparaissent dans le volet central de la console, puis
- glissez-lâchez des règles/politiques dans le volet central depuis le volet **Politiques**.



**!** Dans le volet central les politiques appliquées sont séparées dans deux onglets selon leur portée, **Politiques ordinateur** et **Politiques Internet** respectivement. Les mécanismes de glisser-lâcher y sont sensibles : mettez en avant l'onglet **Politiques ordinateur** avant d'y ajouter par glisser-lâcher une règle de type **Ordinateur** etc.

La présentation des deux catégories dans le volet **Pour qui ?** prend également en compte les différentes variantes de mise en réseau selon Windows.

## Les utilisateurs et les domaines gérés par Windows

Cette branche correspond à la structure d'un réseau Windows à contrôleur de domaine / Active Directory. Si un réseau de ce type est présent dans l'entreprise, cette branche du volet **Pour qui ?** n'en est rien d'autre que le miroir, prêt à accueillir des règles et des politiques de sécurité.

Utilisez la commande **Rechercher de nouveaux utilisateurs et groupes** disponible en clic droit sur chaque domaine afin de mettre à jour la vue par rapport à la configuration en temps réel du réseau.



## Les utilisateurs gérés par PNF

Afin d'offrir la richesse fonctionnelle des utilisateurs itinérants en absence d'un réseau Windows orienté utilisateurs, Entreprise Network Filter peut gérer directement des utilisateurs et des groupes d'utilisateurs, avec des noms et des mots de passe qui seront vérifiés au démarrage de chaque session locale sur les ordinateurs contrôlés. Dans ce cas, il vous appartient de les créer et éventuellement de les distribuer dans des groupes, avant de leur imposer des politiques et de règles de sécurité (voir **Utilisateurs, ordinateurs, groupes, domaines**).

Une fois sélectionné dans le volet **Pour qui**, la caractéristique de ce type d'utilisateur est la présence dans le volet central des zones de saisie **Mot de passe** et **Confirmation du mot de passe**, qu'il vous appartient de renseigner.

## Les ordinateurs

Cette branche reprend la structure d'un réseau Windows orienté ordinateurs et groupes de travail, mais vous pouvez également en créer d'autres, avant de leur imposer des politiques et des règles de sécurité (voir **Utilisateurs, ordinateurs, groupes, domaines**).

## 3-3. Les plages horaires

Le volet **Quand ?** présente un jeu standard de plages horaires, auxquelles vous pouvez rajouter celles qui expriment au mieux les besoins de votre entreprise en termes d'application des politiques de sécurité. Comme pour tous les autres volets, le clic droit est le point d'ancrage de toutes les commandes applicables localement.

Pour créer une nouvelle plage horaire, commencez par un clic droit et faites **Copier**, puis **Coller** à partir d'un objet prédéfini. Ensuite, sélectionnez le nouvel objet et modifiez à la souris sa grille de créneaux horaires, affichée dans le volet central.

## 3-4. Règles et politiques

Le volet **Politiques** concentre l'ensemble des règles et groupes de règles en vigueur dans l'entreprise.

En sélectionnant une politique, vous obtenez dans le volet central l'ensemble des règles dont elle est composée. Pour chaque règle, vous avez la possibilité de définir ou redéfinir ses composantes:

- la décision : interdit, permis, règle neutralisée
- le champ d'application (utilisateurs ou ordinateurs)
- l'élément à surveiller
- les flux d'entrée-sortie concernés (si l'élément à surveiller porte sur des échanges Internet)
- la plage horaire d'application.

Pour chaque composante d'une règle, un clic sur la colonne correspondante commande l'apparition d'une liste déroulante avec l'ensemble des choix applicables.

**Toujours dans le volet central** qui détaille une politique, vous pouvez utiliser les boutons flèches verticales pour changer l'ordre d'application des règles. A la fin d'une session de travail sur les règles, n'oubliez pas d'enregistrer les modifications (voir **Barre de menus**), afin que celle-ci soit répercutées au niveau des agents qui travaillent sur chaque ordinateur contrôlé.



## 4 - LA PANOPLIE DE L'ADMINISTRATEUR

Le volet **Activité** regroupe les éléments généraux de configuration du logiciel, ainsi que les retours d'information à l'intention de l'administrateur.

### 4-1. Rapports

Au vu du caractère multi-dimension de son travail (types de surveillance, utilisateurs, périodes), l'approche de Profil Network Filter en matière de rapports consiste à décliner des modèles de rapport par type de surveillance, pour vous laisser ensuite le soin de fixer à l'intérieur d'un modèle les autres paramètres à l'aide d'assistants spécialisés.

Vous commencerez donc par choisir parmi les variantes ci-dessous :

- **Rapports applications**
- **Rapports Internet**
- **Rapports sessions de travail**
- **Rapports copies d'écran**

Pour restreindre ensuite le champ d'application du rapport par groupes, ordinateurs, utilisateurs etc., puis par période, en sélectionnant au passage des éléments de contenu spécifiques à chaque type de rapport.

A la fin du processus, il convient de donner au rapport nouvellement créé un nom explicite en accord avec sa vocation (par ex. «Groupe compta, durées applis sur une semaine»), de sorte à le retrouver facilement au besoin.

Une fois le rapport créé, il suffira de cliquer sur son nom dans le volet, pour le voir s'afficher avec des données à jour, prêtes à être imprimées.

Des moyens de personnalisation de votre rapport sont également disponibles, à partir du menu général **Rapports > Personnalisation des rapports ...**

### 4-2. Alertes

Les **Alertes** regroupent les modèles de retour d'information immédiat de la part de Profil Network Filter. A chaque fois qu'une règle de sécurité déclenche un blocage, l'agent de sécurité envoie des «signaux» :

- à l'utilisateur concerné, en remplaçant la page Web qu'il attendait par un message détaillant les causes du blocage ou en modifiant la teneur d'un échange de courrier électronique
- à l'administrateur de Profil Network Filter, par l'intermédiaire d'un e-mail.

#### **Messages de blocage**

La branche **Alertes > Messages de blocage** vous permet de créer et de modifier les modèles de «messages» que l'utilisateur recevra au déclenchement d'une règle le concernant.



Par la suite, vous pouvez choisir un modèle pour chaque utilisateur ou ordinateur sous surveillance (voir **Utilisateurs, ordinateurs, groupes, domaines**).

De ce fait, un modèle contient l'ensemble des éléments susceptibles d'être altérés au déclenchement d'une règle, selon le flux concerné : page Web, e-mail entrant, e-mail sortant.

## **Notifications**

La branche **Alertes > Notifications** vous permet de créer et de modifier les modèles de «messages» que l'administrateur PNF recevra au déclenchement d'une règle au sein du réseau surveillé.

Par la suite, vous pouvez choisir un modèle pour chaque utilisateur ou ordinateur sous surveillance (voir **Utilisateurs, ordinateurs, groupes, domaines**).

Les éléments qui définissent un modèle de notification assurent une grande flexibilité du fonctionnement, allant jusqu'à la délégation des tâches d'administration pour un groupe d'utilisateurs, sous-réseau etc., car dans chaque modèle vous pouvez définir un destinataire différent, voire une plate-forme de messagerie (serveur SMTP) spécifique.

## **4-3. Copies d'écran**

L'entrée **Copies d'écran** regroupe les modèles applicables (voir **Utilisateurs, ordinateurs, groupes, domaines**) pour prendre des photos d'écran d'un ordinateur placé sous surveillance. Trois modèles sont fournis en standard :

**Copies rapprochées** : une photo toutes les 5 secondes

**Copies sommaires** : une photo toutes les 5 minutes

**Pas de copies** : l'enregistrement de l'écran est désactivé

Vous pouvez également définir de nouveaux modèles, avec d'autres périodicités en adéquation avec vos besoins.

## **4-4. Exceptions**

Il vous appartient d'introduire dans la liste des **Applications non soumises à la surveillance** toutes les applications métier dont les entrées-sorties réseau ne doivent pas être contrôlées d'aucune façon par Entreprise Network Filter. La liste admet des noms d'applications à chemin complet ou relatif et des masques de saisie contenant le méta-caractère \* (étoile).

## **4-5. Sites réputés pornographiques**

La liste des **Sites réputés pornographiques** s'enrichit au fur et à mesure du fonctionnement de la **Détection des images pornographiques** en mode **tâche de fond** sur les ordinateurs où celle-ci est appliquée (voir **Détection des images pornographiques**).

Vous pouvez bien entendu y ajouter vos propres entrées. Le filtrage résultant est appliqué de suite à la navigation Web sur les ordinateurs concernés.



## 4-6. Conservation des journaux

Les durées de conservation des constats effectués par PNF sont déclinées par catégorie et fixées par défaut à 5 semaines.

En y effectuant d'éventuels changements, gardez à l'esprit le besoin de «matière» pour les modèles de rapports d'activité que vous avez définis.

En effet, le contenu d'un rapport portant sur un mois en arrière se verra amputé de moitié si les journaux sur lesquels il s'appuie ne sont conservés que deux semaines etc.

## 4-7. Logistique PNF

### Déploiement

L'arborescence **Déploiement** est un rappel de la structure par groupe d'ordinateurs du réseau de l'entreprise. Une fois sélectionné, un groupe présente dans le volet central sa liste d'ordinateurs, avec des informations propres à l'état du déploiement de l'agent de sécurité :

- **Adresse IP**, pour information
- **Administrateur**, l'identifiant d'une session administrateur sur l'ordinateur concerné. Attention, cette information est essentielle au processus de déploiement de l'agent
- **Mot de passe**, le mot de passe de la session administrateur (voir supra)
- **État**, rappel de l'état déployé ou encore à déployer sur l'ordinateur.

### Canaux Intranet PNF

Le volet **Canaux Intranet PNF** regroupe l'information dont les différentes parties de l'application ont besoin pour se parler :

- le **Port d'accès au politiques** est la porte de communication entre les agents déployés sur les postes surveillés et le serveur central.
- le **Mot de passe** est celui qui donne accès à la console d'administration
- le couple **Question - Réponse** sert d'alternative en cas d'oubli du mot de passe ci-dessus.



**Il vous appartient de vérifier que les différentes solutions de sécurité en service dans l'entreprise laissent passer un trafic HTTP standard par le canal de communication **Port d'accès aux politiques**.**



## **Mise à jour**

Le volet **Mise à jour** regroupe les paramètres et les commandes qui régissent la mise à jour des composants du logiciel, notamment :

- la périodicité de la mise à jour automatique ou a contrario l'option de mettre à jour manuellement (en appuyant sur le bouton correspondant)
- les paramètres d'un éventuel proxy d'accès Web vers l'extérieur, selon l'endroit où se trouve le composant et la topologie de votre accès Internet.

Par défaut, la mise à jour est configurée en mode automatique avec recherche des nouveautés une fois par semaine.

## **Gestion des licences**

Le volet **Gestion des licences** présente l'ensemble des licences PNF présentées au logiciel, avec l'affichage pour chacune du nombre des postes couverts et de la date d'expiration. Vous pouvez en introduire d'autres au fur et à mesure des besoins, et de ce fait garder votre investissement dans la solution PNF en phase avec les évolutions de votre réseau d'entreprise.

