

➤ Configurer le pare-feu de Windows XP SP2/Vista pour UserLock

Après l'installation du service pack 2 sur une machine Windows XP toute requête réseau entrante est bloquée par le pare-feu. Il n'y a en conséquence plus aucun moyen de contacter cette machine depuis une autre machine même avec un simple ping. La station de travail devient donc complètement invisible pour tous les outils réseau empêchant ainsi son administration à distance.

Pour corriger cela, le pare-feu nécessite d'être configuré. Vous pouvez le faire directement sur chaque station de travail mais si vous avez à charge un réseau Windows le meilleur moyen est de configurer le pare-feu de tous vos postes Windows XP par le biais des stratégies de groupe ou système.

- - - - -

Configurer le pare-feu via les stratégies de groupe (pour les domaines Windows 2000/2003/2008)

■ Etape 1 : Mettre à jour les objets de stratégie de groupe avec les nouveaux paramètres du pare-feu

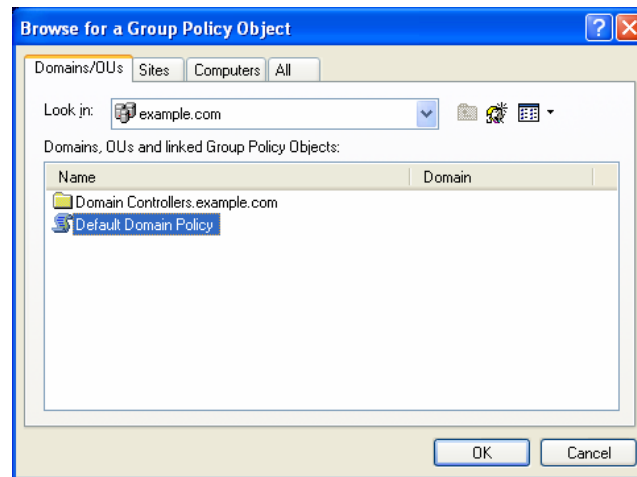
Important : Cette étape n'est pas nécessaire pour Windows server 2003 SP2 ou Windows server 2008.

Cette section est la traduction d'un extrait du document Microsoft "[Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2](#)". Pour plus d'information vous pouvez télécharger le document directement sur le site web de Microsoft.

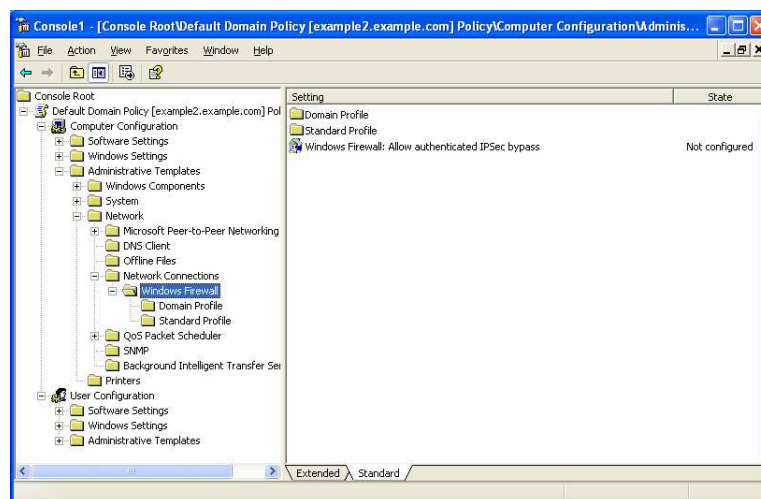
Pour mettre à jour les objets de stratégie de groupe avec les nouveaux paramètres du pare-feu Windows en utilisant le composant logiciel enfichable *Stratégies de groupe* (fourni avec Windows XP), faites comme suit :

1. Installez le service pack 2 sur un ordinateur *Windows XP* membre du domaine contenant les comptes de machines de tous les postes *Windows XP* que vous voulez passer au service pack 2.
2. Redémarrez cet ordinateur et ouvrez une session en tant que membre d'un des groupes suivant: Administrateurs du domaine, Administrateurs de l'entreprise, Propriétaires et créateurs de la stratégie de groupe.
3. Depuis le bureau Windows XP, cliquez **Démarrer**, cliquez **Exécuter**, entrez **mmc**, puis cliquez **OK**.
4. Dans le menu **Fichier**, cliquez **Ajouter/Supprimer un composant logiciel enfichable**.
5. Dans l'onglet **Autonome** cliquez sur **Ajouter**.
6. Dans la liste des composant logiciel enfichable sélectionnez **Editeur d'objet de stratégie de groupe** puis cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Sélection d'un objet de stratégie de groupe** cliquez **Parcourir**.

8. Dans **Rechercher un objet de stratégie de groupe** sélectionnez l'objet de stratégie de groupe que vous voulez mettre à jour avec les nouveaux paramètres du pare-feu Windows. Vous avez un exemple dans la figure ci-dessous.



9. Cliquez **OK**.
10. Cliquez **Terminer** pour terminer l'assistant de stratégie de groupe.
11. Dans la boîte de dialogue **Ajout d'un composant logiciel enfichable autonome** cliquez sur **Fermer**.
12. Dans la boîte de dialogue **Ajouter/Supprimer un composant logiciel enfichable**, cliquez **OK**.
13. Dans l'arborescence de la console ouvrez **Configuration de l'ordinateur, Modèles d'administration, Réseau, Connexions réseau**, et puis **Pare-feu Windows**. Vous avez un exemple dans la figure ci-dessous.



Répétez cette procédure pour chaque objet de stratégie de groupe qui sera utilisée pour appliquer les stratégies de groupe aux ordinateurs Windows XP avec le service pack 2 installé.

► **Note** Pour mettre à jour les stratégies de groupe pour des environnements réseau utilisant l'Active Directory et Windows XP SP1, Microsoft recommande que vous utilisiez la console des stratégies de

groupe téléchargeable librement. Pour plus d'information voir [Group Policy Management Console with Service Pack 1](#).

Fin de l'extrait du document Microsoft "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2"

Si à la suite cette manipulation vous avez le message suivant sur votre serveur lors de l'édition des stratégies de groupe :

« L'entrée suivante de la section [strings] est trop longue et a été tronquée » vous pouvez lire l'article suivant de la base de connaissance Microsoft pour résoudre le problème :

<http://support.microsoft.com/default.aspx?scid=kb;en-us;842933>

■ Etape 2 : Configurer le pare-feu dans les stratégies de groupe

- Editez la stratégie de groupe concernée comme expliqué dans la section précédente et allez dans "Configuration de l'ordinateur/Modèles d'administration/Réseau/Connexions réseau/Pare-feu Windows/Profil du domaine"
- Activer le paramètre "Pare-feu Windows: Autoriser l'exception d'administration à distance"
Pour plus de sécurité vous pouvez restreindre la source à l'adresse IP du serveur (au lieu de * ou localsubnet). Cela fait vos machines XP SP2 ne pourront plus être infectées par des vers de type BLASTER.
- Activer le paramètre "Autoriser les exceptions ICMP" Sélectionnez « Autoriser les requêtes d'écho entrante » et cliquez sur OK.
- Activer le paramètre (Pour UserLock 3 uniquement) "Définir des exceptions de programme", Cliquez sur *Afficher*, cliquez sur *Ajouter* et entrez la ligne suivante: "%SystemRoot%\system32\LogoffAgent.exe:*:Enabled:Userlock"
- Cliquez Ok deux fois.

■ Etape 3: Faites votre premier test sur une station de travail XP SP2

A ce niveau les stratégies de groupe sont configurées mais les paramètres du pare-feu ne sont pas répliqués sur toutes les stations de travail. Vous devez attendre que toutes les stations aient mise à jour les paramètres des stratégies.

Pour faire un test avec une station de travail Windows XP SP2 vous pouvez forcer la mise à jour en lançant la commande *gpupdate*.

Le pare-feu est maintenant configuré sur cette machine vous pouvez donc vérifier si vous êtes en mesure de déployer l'agent UserLock sur cette machine ainsi que de fermer la session de l'utilisateur connecté grâce à la console d'administration UserLock.

- - - - -

Configurer le pare-feu via les stratégies système (pour les domaines Windows NT 4)

■ Etape 1: Mise à jour des stratégies système NT4 avec les nouveaux paramètres du pare-feux

Cette section est la traduction d'un extrait du document Microsoft "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2". Pour plus d'information vous pouvez télécharger le document directement sur le site web de Microsoft.

Les ordinateurs Windows XP qui sont membre d'un domaine Windows NT 4.0 utilisent les stratégies système en lieu et place des stratégies de groupe. Pour déployer les paramètres du pare-feu pour

ces machines, vous devez ajouter le modèle de stratégies du pare-feu (le fichier Wfnt.adm), configurer les paramètres du pare-feu Windows, puis distribuer le nouveau fichier de stratégie système sur tous vos contrôleurs de domaine Windows NT 4.

Les paramètres des stratégies système Windows NT sont stockés dans le fichier *Ntconfig.pol* dans le partage *Netlogon* de vos contrôleurs de domaine Windows NT 4.0. Pour plus d'information à propos des stratégies système Windows NT, voir le document [Implementing Profiles and Policies for Windows NT 4.0](#) à l'adresse suivante :

http://www.microsoft.com/ntserver/techresources/management/prof_policies.asp

Pour configurer les paramètres du pare-feu dans les stratégies système suivez les étapes suivantes:

1. Téléchargez le fichier Wfnt.adm depuis [Le centre de téléchargement Microsoft](#) à l'adresse <http://www.microsoft.com/downloads/details.aspx?FamilyID=d67c7085-4bff-4056-8e7e-3d583214e728&DisplayLang=en>.
2. Si vous administrez les stratégies système Windows NT depuis un poste Windows XP professionnel ou Windows 2000, vous devez installer les outils d'administration Windows 2000 en double cliquant sur le fichier Adminpak.msi dans le répertoire \I386 du CD Windows 2000 serveur si nécessaire. Si vous administrez les stratégies système Windows NT depuis un poste Windows NT 4 vous pouvez sauter cette étape.
3. Cliquez **Démarrer**, cliquez **Exécuter**, entrez **poledit.exe**, puis cliquez **OK**.
4. Depuis l'éditeur des stratégies système, cliquez **Options** puis cliquez sur **Modèles de stratégies**.
5. Dans la boîte de dialogue **Options de modèle de stratégies**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ouvrir un fichier modèle**, sélectionnez le fichier *Wfnt.adm* téléchargé à l'étape 1, et cliquez **OK**.

Fin de l'extrait du document Microsoft "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2"

■ Etape 2: Configurer le pare-feu dans les stratégies système

- Exécuter *poledit.exe*
- Ouvrir le fichier "*Ntconfig.pol*" (créez le si nécessaire) dans le partage *netlogon* (Généralement dans le répertoire *c:\winnt\system32\repl\import\scripts*) du contrôleur de domaine.
- Allez dans "*Ordinateur par défaut/Pare-feu Windows/Profil du domaine*"
- Activer le paramètre "*Pare-feu Windows: Autoriser l'exception d'administration à distance*"
Pour plus de sécurité vous pouvez restreindre la source à l'adresse IP du serveur (au lieu de * ou *localsubnet*). Cela fait vos machines XP SP2 ne pourront pas être infectées par des vers de type BLASTER.
- Activer le paramètre "*Pare-feu Windows: Autoriser l'exception de partage de fichiers et d'imprimantes*"
Pour plus de sécurité configurez une restriction sur la source comme expliqué ci-dessus.
- Activer le paramètre "*Autoriser les exceptions ICMP*" Sélectionnez « *Autoriser les requêtes d'écho rentrante* » et cliquez sur **OK**.
- Activer le paramètre (Pour UserLock 3 uniquement) "*Définir des exceptions de programme*", Cliquez sur **Afficher**, cliquez sur **Ajouter** et entrez la ligne suivante: "*%SystemRoot%\system32\LogoffAgent.exe:*:Enabled:Userlock*"
Cliquez **Ok** deux fois.
- La stratégie système est maintenant configurée, vous devez vous assurer que le fichier *Ntconfig.pol* est bien répliqué sur tous les contrôleurs de domaine.

■ Etape 3: Faites votre premier test sur une station de travail XP SP2

A ce niveau les stratégies système sont configurées mais les paramètres du pare-feu ne sont pas répliqués sur toutes les stations de travail. Vous devez attendre que toutes les stations aient mis à jour les paramètres des stratégies.

Pour faire un test sur une station de travail Windows XP SP2 vous pouvez forcer la mise à jour en redémarrant celle-ci.

Le pare-feu est maintenant configuré sur cette machine vous pouvez donc vérifier si vous êtes en mesure de déployer l'agent UserLock sur cette machine ainsi que de fermer la session de l'utilisateur connecté grâce à la console d'administration UserLock.

- - - - -

Configurer le pare-feu sans les stratégies de groupe ou système

Sur chaque station de travail que vous voulez administrer allez dans le panneau de configuration et affichez « *Pare-feu Windows* ».

Sélectionnez l'onglet *Exceptions* et suivez les points listés ci-dessous :

- **Activez l'exception *Partage de fichiers et d'imprimantes*.**
Pour plus de sécurité vous pouvez restreindre la source à l'adresse IP du serveur (au lieu de * ou *localsubnet*). Cela fait vos machines XP SP2 ne pourront pas être infectées par des vers de type BLASTER.
- **Pour Windows Vista, vous devez également autoriser le ping.** Dans la console de Configuration avancé du pare feu disponible dans les outils d'administration, activez la règle « *réseau- requête d'écho entrante ICMP* ».
- **Ajoutez une exception de port avec *RPC* comme nom (pour UserLock 3 uniquement), 135 comme port et avec *TCP* sélectionné.** Pour plus de sécurité configurez une restriction sur la source comme expliqué ci-dessus.
- **Ajoutez une exception de programme (pour UserLock 3 uniquement) avec *%SystemRoot%\system32\LogoffAgent.exe* comme chemin.** Si vous n'êtes pas autorisé à le faire car le fichier n'est pas présent sur la machine, vous pouvez télécharger et exécuter le fichier .reg disponible à l'adresse suivante :
<http://www.isdecisions.com/download/AllowLogoffAgent.zip>

Le pare-feu est maintenant activé vous pouvez vérifier si vous êtes en mesure de déployer l'agent UserLock sur ces machines ainsi que de fermer des sessions utilisateur grâce à la console d'administration UserLock.

➤ **References :**

Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2

<http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1&displaylang=en>