

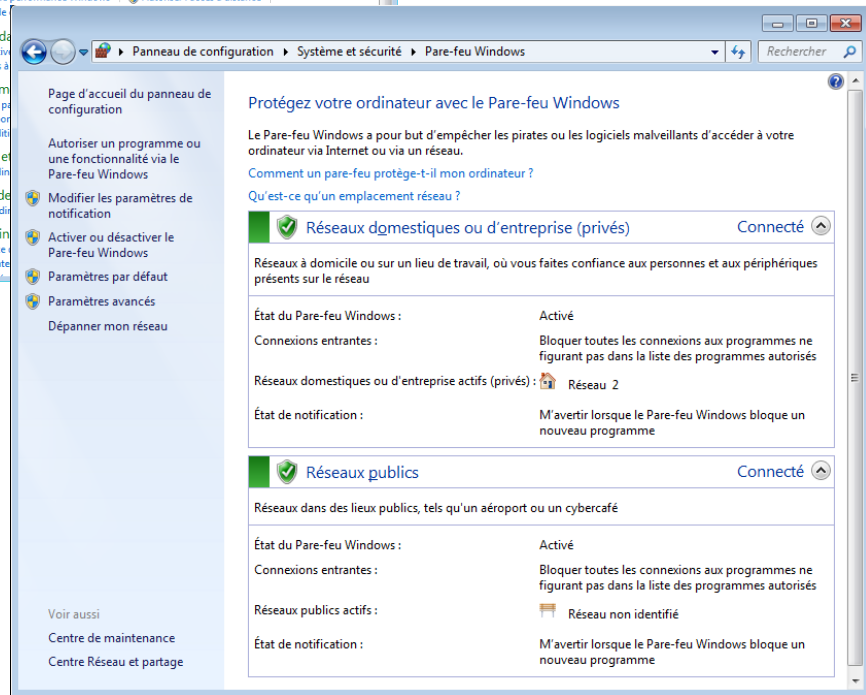
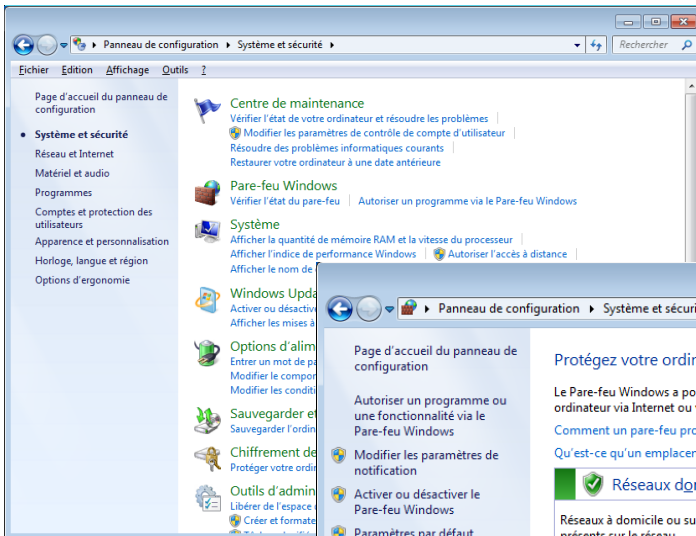
	<h1>HoMIDoM</h1>	V1.0
<h2>Configuration du pare-feu</h2>		

# Configuration du pare feu

Afin de permettre le dialogue entre le serveur et les clients distants (Android, Web ou lourd), il est impératif de configurer le pare feu Windows sur le poste exécutant le service HoMIDoM.

Pour cela, lancer le panneau de configuration – système et sécurité

en « Pare-Feu »

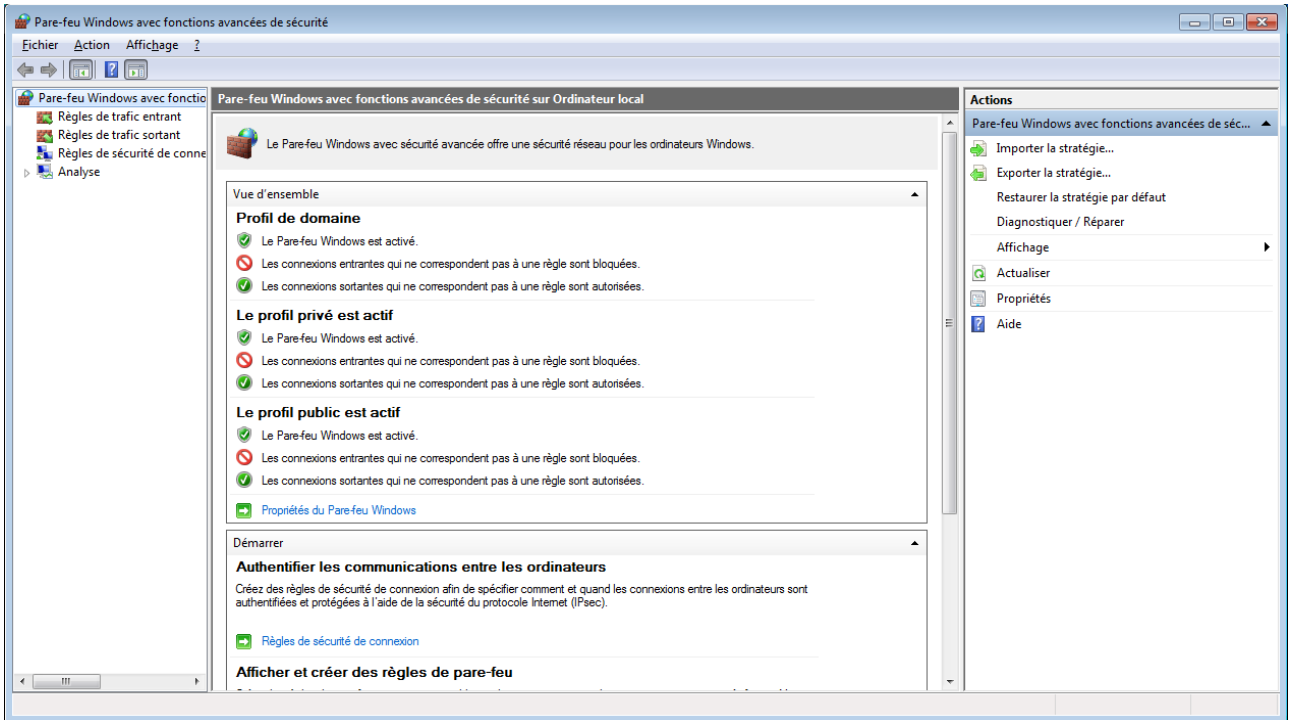


La fenêtre montre les différentes configurations définies pour le Pare-

feu.

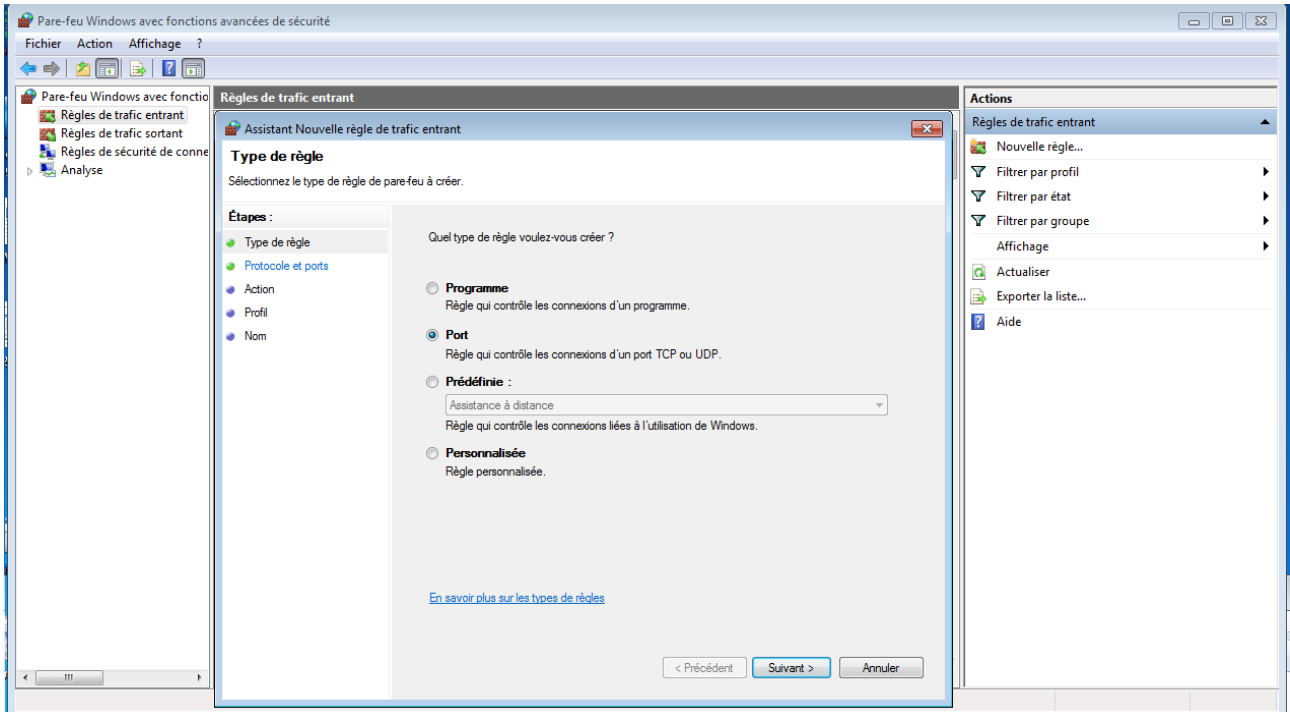
	<h1>HoMIDoM</h1>	V1.0
<h2>Configuration du pare-feu</h2>		

Cliquer sur le bouton « Paramètres avancés »



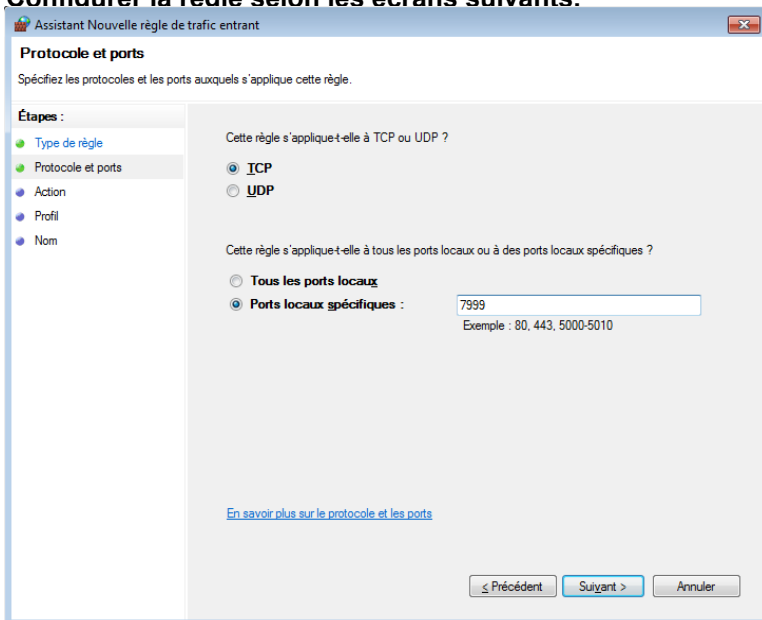
Créer une nouvelle règle, en sélectionnant le groupe « règles de trafic entrant » (fenêtre de gauche) et en cliquant sur le bouton « Nouvelle règle » dans la fenêtre de droite.

	<h1>HoMIDoM</h1>	V1.0
<h2>Configuration du pare-feu</h2>		



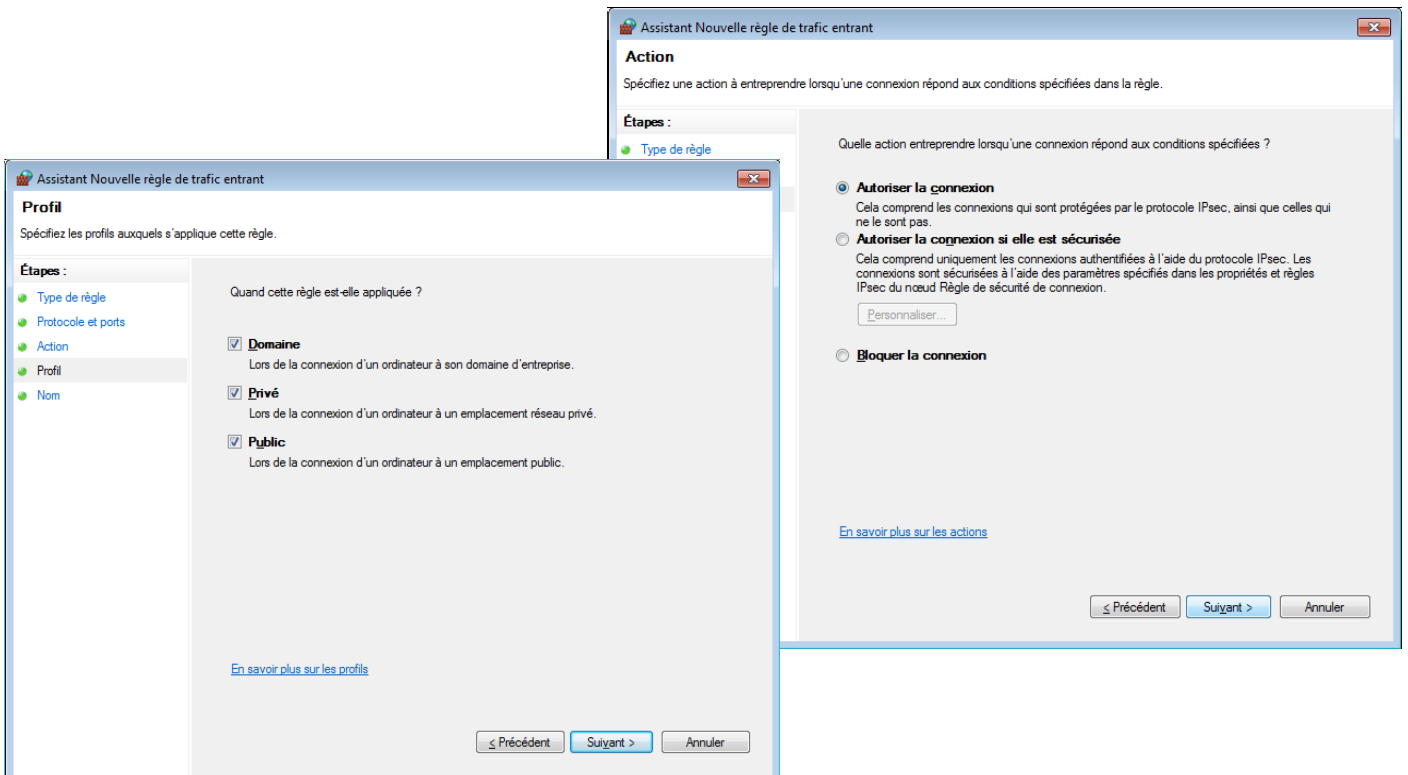
**Configurer la règle, pour filtrer sur le port (comme décrit ci dessus)**

**Configurer la règle selon les écrans suivants.**



	<h1>HoMIDoM</h1>	V1.0
<h2>Configuration du pare-feu</h2>		

Cliquer sur suivant pour changer d'écran



**Assistant Nouvelle règle de trafic entrant**

**Profil**  
Spécifiez les profils auxquels s'applique cette règle.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Quand cette règle est-elle appliquée ?

- Domaine**  
Lors de la connexion d'un ordinateur à son domaine d'entreprise.
- Privé**  
Lors de la connexion d'un ordinateur à un emplacement réseau privé.
- Public**  
Lors de la connexion d'un ordinateur à un emplacement public.

[En savoir plus sur les profils](#)

≤ Précédent   Suivant >   Annuler

---

**Assistant Nouvelle règle de trafic entrant**

**Action**  
Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :

- Type de règle

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

- Autoriser la connexion**  
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.
- Autoriser la connexion si elle est sécurisée**  
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.
- Bloquer la connexion**

[En savoir plus sur les actions](#)

≤ Précédent   Suivant >   Annuler

	<h1>HoMIDoM</h1>	V1.0
	<h2>Configuration du pare-feu</h2>	

**Nommer la règle en HoMIDom-Service**

**Puis cliquer sur Terminer.**

