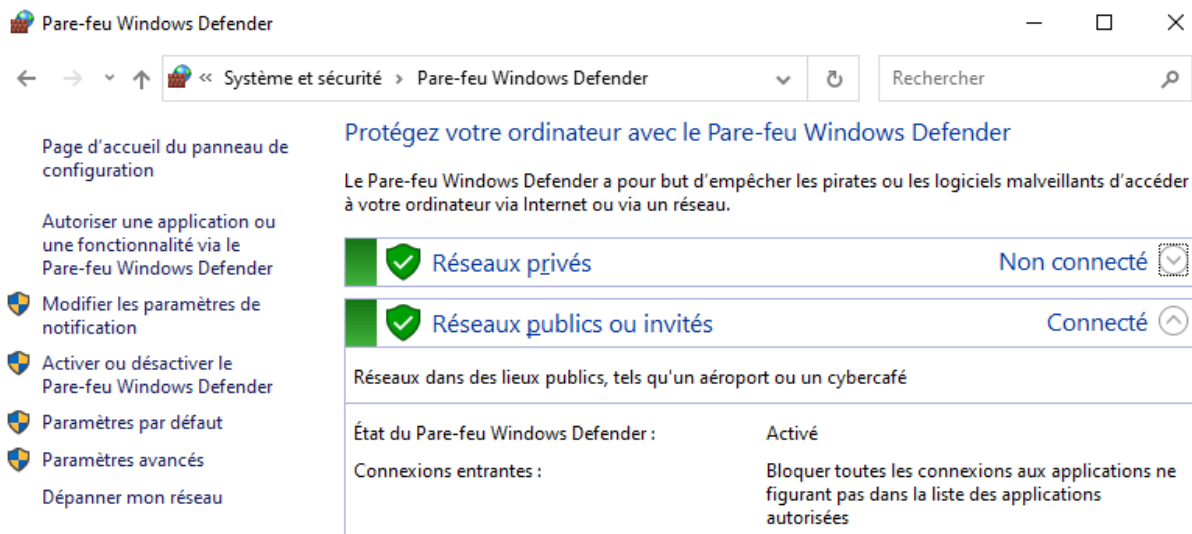


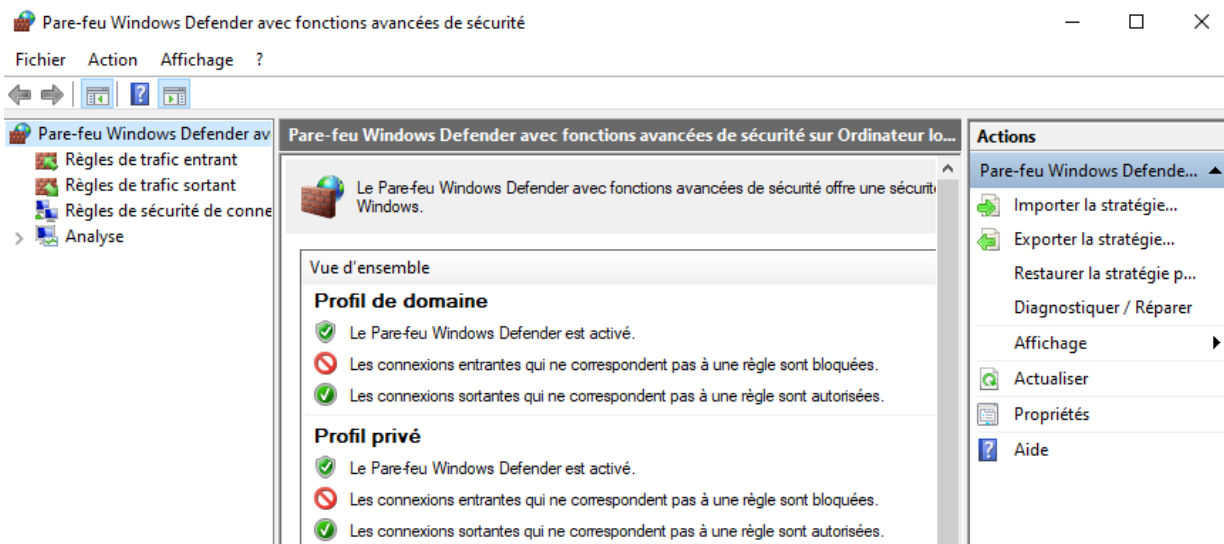
## Appendix A: Allowing ICMP Traffic Through a Firewall (Activity 1.5.4)

### Part 1: Create a new inbound rule allowing ICMP traffic through the firewall.

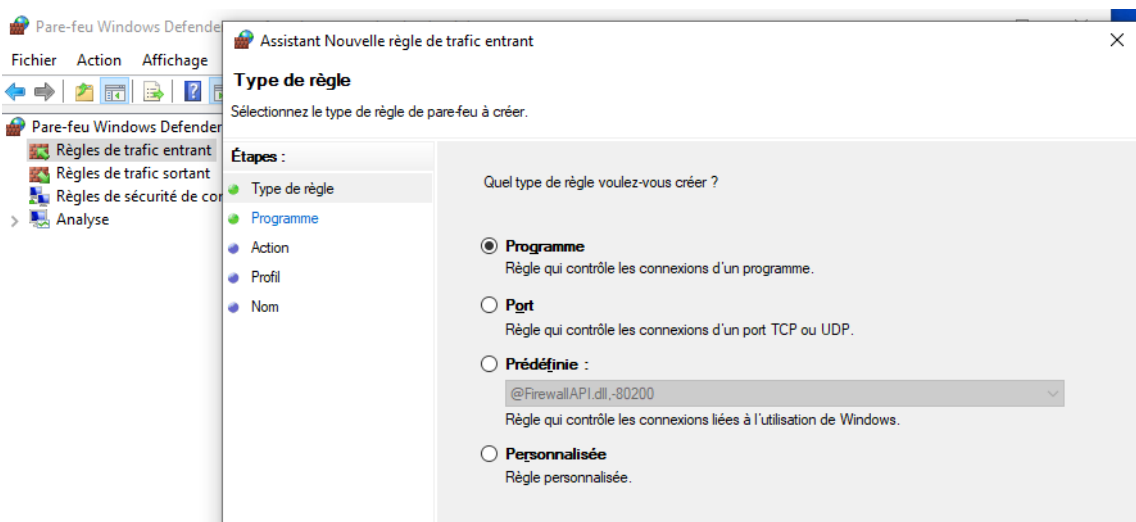
- a. Navigate to the **Control Panel** and click the **System and Security**, then **Windows Defender Firewall** or **Windows Firewall** (Pare-feu Windows Defender).



- b. Click Advanced settings (Parametres avancés), a new window will open:



- c. Click the **Inbound Rules** (Regles de trafic entrant) option on the left sidebar and then click **New Rule** (Nouvelle Regle)... on the right sidebar. This launches the **New Inbound Rule** wizard.



- d. On the **Rule Type** screen, click the **Custom** (Personnalisée) radio button and click **Next (Suivant)**.

The screenshot shows the 'Assistant Nouvelle règle de trafic entrant' (New Incoming Traffic Rule Wizard) at the 'Type de règle' (Rule Type) step. The left pane shows the 'Étapes' (Steps) list with 'Type de règle' selected. The main area asks 'Quel type de règle voulez-vous créer ?' (What type of rule do you want to create?). There are four radio button options: 'Programme' (Rule that controls connections of a program), 'Port' (Rule that controls connections of a TCP or UDP port), 'Prédéfinie' (Rule that controls connections related to Windows usage, with a dropdown menu showing '@FirewallAPI.dll,-80200'), and 'Personnalisée' (Custom rule), which is selected. At the bottom, there are three buttons: '≤ Précédent' (Previous), 'Suivant >' (Next), and 'Annuler' (Cancel).

- e. In the left pane, click the **Protocol and Ports** (Protocole et ports) option and using the **Protocol Type** (Type de protocole) drop-down menu, select **ICMPv4**, and then click **Next**.

The screenshot shows the 'Assistant Nouvelle règle de trafic entrant' (New Incoming Traffic Rule Wizard) at the 'Protocole et ports' (Protocol and Ports) step. The left pane shows the 'Étapes' (Steps) list with 'Protocole et ports' selected. The main area asks 'À quels ports et protocoles cette règle s'applique-t-elle ?' (To which ports and protocols does this rule apply?). It contains several fields: 'Type de protocole' (Protocol type) set to 'ICMPv4', 'Numéro de protocole' (Protocol number) set to '1', 'Port local' (Local port) set to 'Tous les ports' (All ports), and 'Port distant' (Remote port) set to 'Tous les ports' (All ports). There are also example ranges for ports: 'Exemple : 80, 443, 5000-5010'. At the bottom, there is a section for 'Paramètres ICMP (Internet Control Message Protocol)' with a 'Perso...' button. At the bottom right, there are three buttons: '≤ Précédent' (Previous), 'Suivant >' (Next), and 'Annuler' (Cancel).

- f. Verify that **Any IP address** (Toute adresse IP) for both the local and remote IP addresses are selected. Click **Next** to continue.

Assistant Nouvelle règle de trafic entrant

×

### Étendue

Spécifiez les adresses IP locales et distantes auxquelles s'applique cette règle.

Étapes :

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

**A quelles adresses IP locales cette règle s'applique-t-elle ?**

☒ Toute adresse IP

☐ Ces adresses IP :

Ajouter...  
Modifier...  
Supprimer

Personnaliser les types d'interfaces auxquels cette règle s'applique : Perso...

**A quelles adresses IP distantes cette règle s'applique-t-elle ?**

☒ Toute adresse IP

☐ Ces adresses IP :

Ajouter...  
Modifier...  
Supprimer

≤ Précédent **Suivant >** Annuler

- g. Select **Allow the connection** (Autoriser la connexion). Click **Next** to continue.

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
- Programme
- Protocole et ports
- Étendue
- Action
- Profil
- Nom

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.

Personnaliser...

☐ **Bloquer la connexion**

≤ Précédent **Suivant >** Annuler

h. By default, this rule applies to all the profiles. Click **Next** to continue.

Assistant Nouvelle règle de trafic entrant

**Profil**

Spécifiez les profils auxquels s'applique cette règle.

Étapes :

- Type de règle
- Programme
- Protocole et ports
- Étendue
- 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, par exemple à domicile ou au bureau.
- ☒ **Public**  
Lors de la connexion d'un ordinateur à un emplacement public.

≤ Précédent   Suivant >   Annuler

i. Name the rule with **Allow ICMP Requests**. Click **Finish** (Terminer) to continue. This new rule should allow your team members to receive ping replies from your PC.

Assistant Nouvelle règle de trafic entrant

**Nom**

Spécifier le nom et la description de cette règle.

Étapes :

- Type de règle
- Programme
- Protocole et ports
- Étendue
- Action
- Profil
- Nom**

Nom :  
Allow ICMP Request

Description (facultatif) :

≤ Précédent   Terminer   Annuler

## Part 2: Disabling or deleting the new ICMP rule.

After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of inbound rules.

- On the **Advanced Security** window, click **Inbound Rules** in the left pane and then locate the rule you created previously.
- Right-click the ICMP rule and select **Disable Rule** if so desired. You may also select **Delete** if you want to permanently delete it. If you choose this option, you must re-create the rule again to allow ICMP replies.

