

Travail de groupe

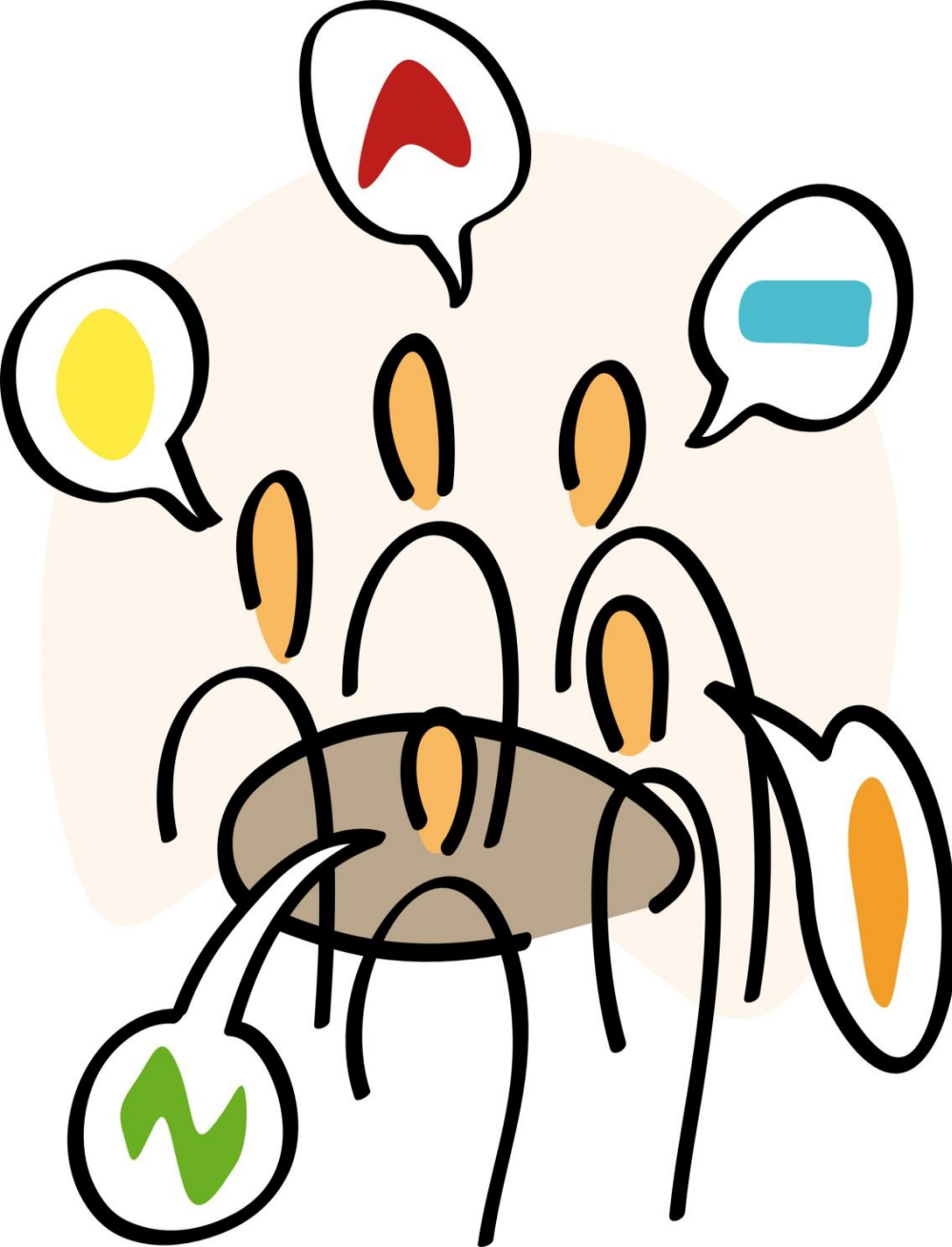
Groupe 1: Pare-feu

Groupe 2: Pare-feu Windows

Groupe 3: Règles du trafic

Groupe 4: Profils : Domaine, Privé & Public

Groupe 5: Configuration d'une règle



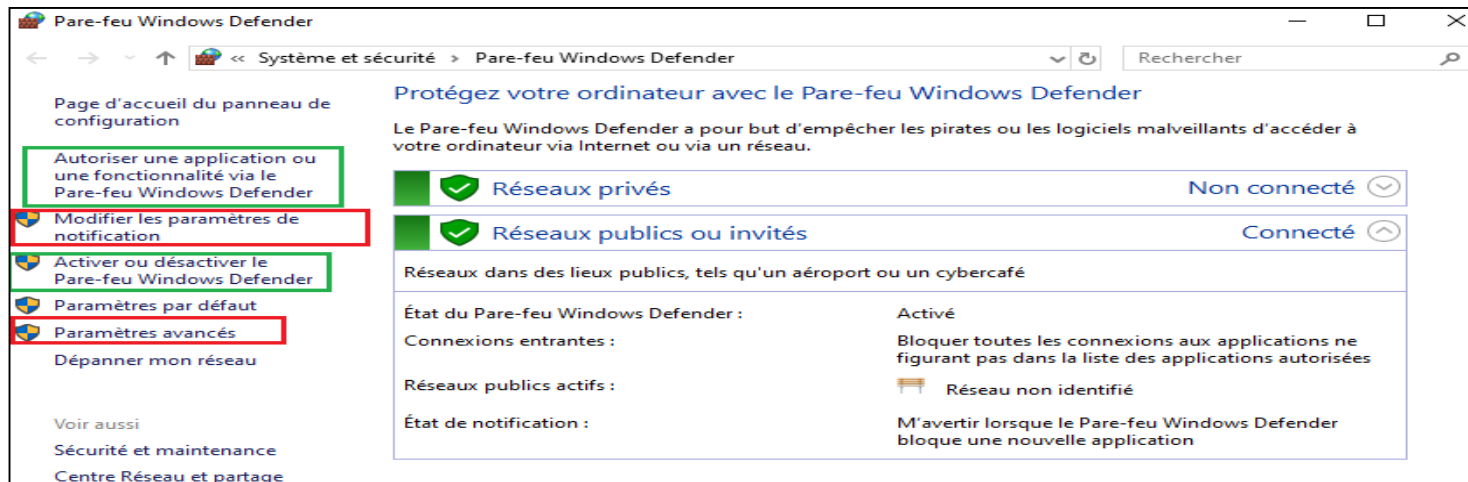
Qu'est-ce qu'un pare-feu

- Parmi les éléments qui peuvent nuire à la sécurité d'un ordinateur on trouve les paquet échangés entre ce dernier et les autres machines.
- Afin de filtrer ces paquets on utilise les pare-feu. Un pare-feu (de l'anglais firewall) est un logiciel et/ou un matériel permettant de protéger un ordinateur ou un réseau des intrusions provenant d'un réseau tiers (notamment internet). Il permet de filtrer les paquets entrantes ou sortantes.
- Windows 10 intègre le pare-feu Windows Defender qui a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via internet ou via un réseau.
- Le pare-feu Windows Defender est activé par défaut

Configuration des paramètres de base du pare-feu Windows

La **configuration de base** du pare-feu Windows Defender consiste à :

- **Activer ou désactiver** le pare-feu Windows
- **Ajouter, modifier ou supprimer** des **programmes autorisés**
- Configurer **les notifications** du pare-feu Windows
- **Créer des règles personnalisées** afin d'autoriser ou bloquer un trafic
- ...

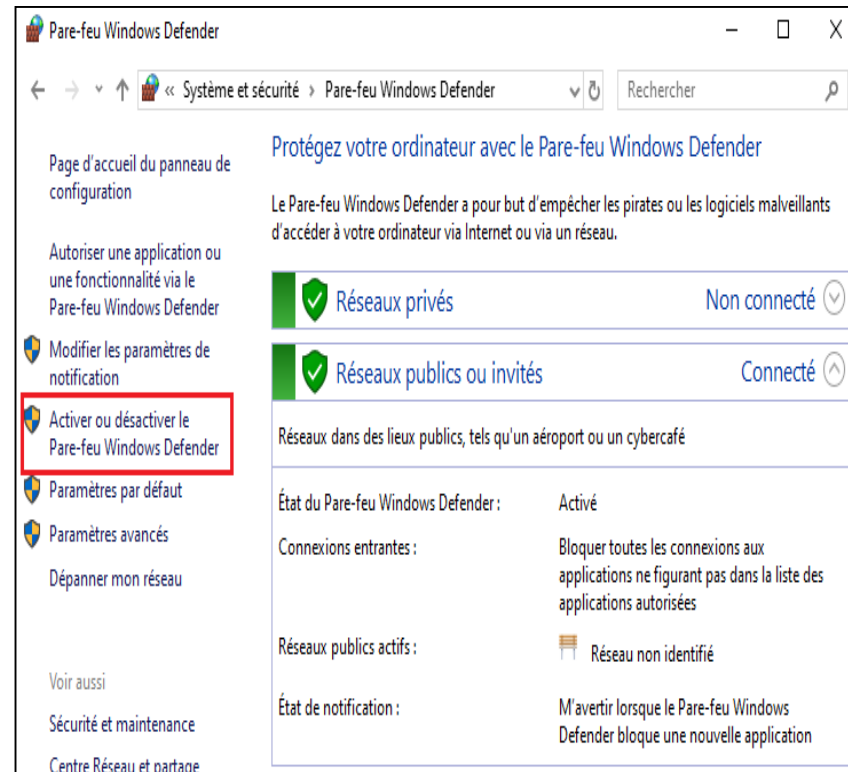


Configuration des paramètres de base du pare-feu Windows

Activer ou désactiver le pare-feu

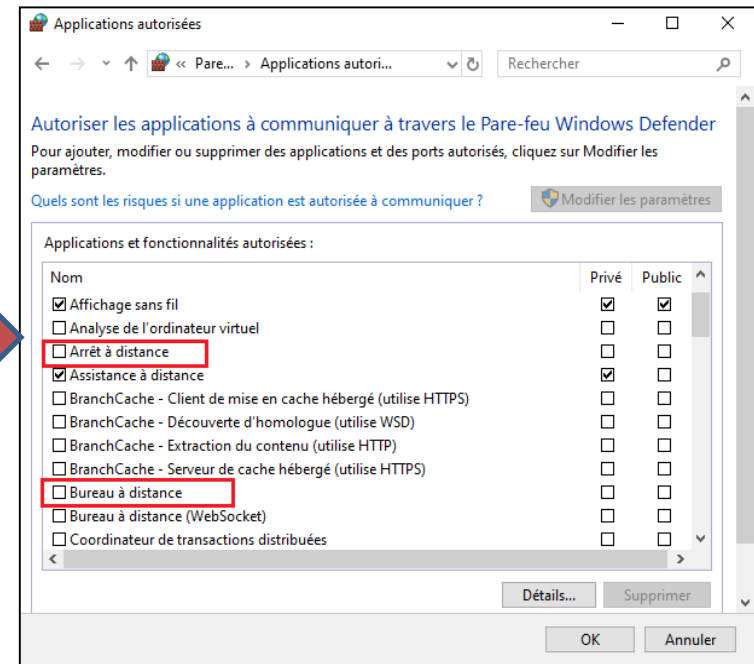
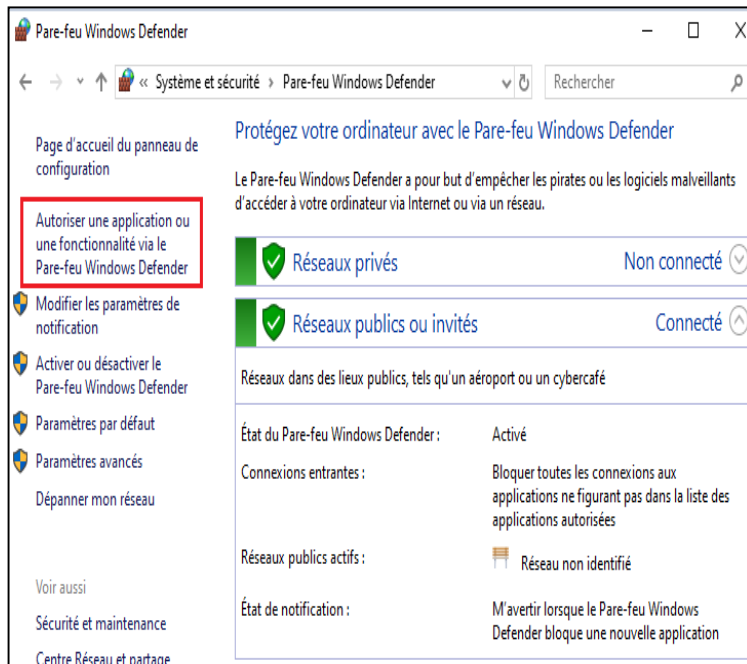
- Pour activer ou désactiver le pare-feu dans Windows 10.

Panneau de configuration → système et sécurité → pare-feu Windows Defender → activer ou désactiver le pare-feu Windows Defender.



Configuration des paramètres de base du pare-feu Windows

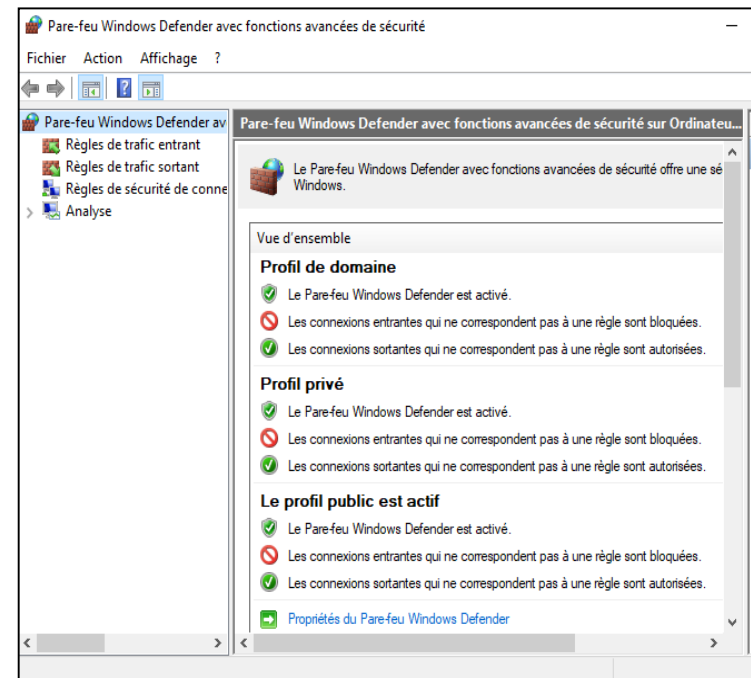
Autoriser les programmes à communiquer à travers le pare feu Windows



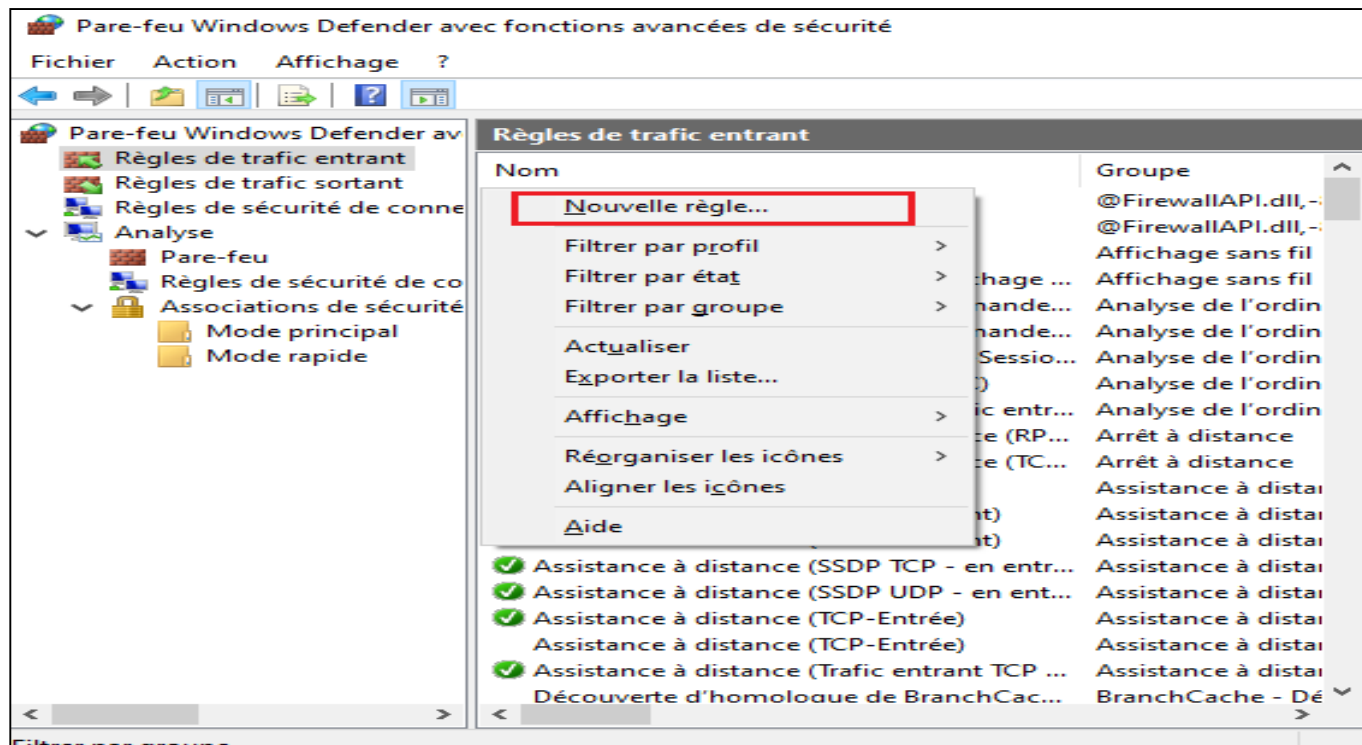
Paramètres du Pare-feu Windows Defender avec fonctions avancées de sécurité

La configuration avancée du pare-feu Windows Defender consiste à créer :

- **Les règles du trafic entrant:**
 - autorisent ou bloquent le trafic destiné à la machine et correspondant à leurs critères.
 - Dans le cas par défaut, le trafic entrant est bloqué.
- **Les règles du trafic sortant**
 - autorisent ou bloquent le trafic provenant de l'ordinateur et correspondant à leurs critères.
 - Dans le cas par défaut, le trafic sortant est autorisé.

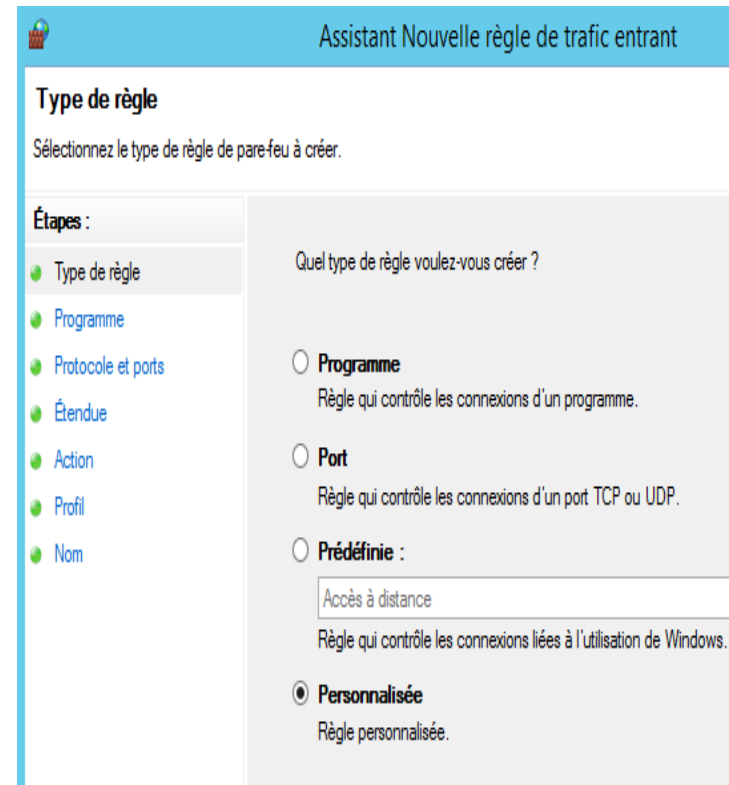


Configuration du Pare-feu Windows avec fonctions avancées de sécurité



Configuration du Pare-feu Windows avec fonctions avancées de sécurité

- **Type de règle :**
 - **Programme** : la règle du pare feu contrôle le trafic en se basant sur le **nom du programme**.
 - **Ports** : la règle du pare feu contrôle le trafic en se basant **le numéro de port**.
 - **Personnalisée** : la règle du pare feu contrôle le trafic en se basant sur le **nom du programme**, le **numéro de port**, l'adresse **IP source** et l'adresse **IP destination**.



Configuration du Pare-feu Windows Defender avec fonctions avancées de sécurité

- **Action**

Spécifie si le trafic sera autorisé ou bloqué

The screenshot shows the 'Assistant Nouvelle règle de trafic entrant' (New Inbound Rule Wizard) in Windows Firewall. The 'Action' step is selected in the 'Étapes' (Steps) list on the left. The main area asks 'Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?' (What action to take when a connection meets the specified conditions?). There are three radio button options: 'Autoriser la connexion' (Allow the connection), 'Autoriser la connexion si elle est sécurisée' (Allow the connection if it is secure), and 'Bloquer la connexion' (Block the connection). The 'Autoriser la connexion' option is selected. Below it, a 'Personnaliser...' (Customize...) button is visible.

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
- Protocole et ports
- 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.

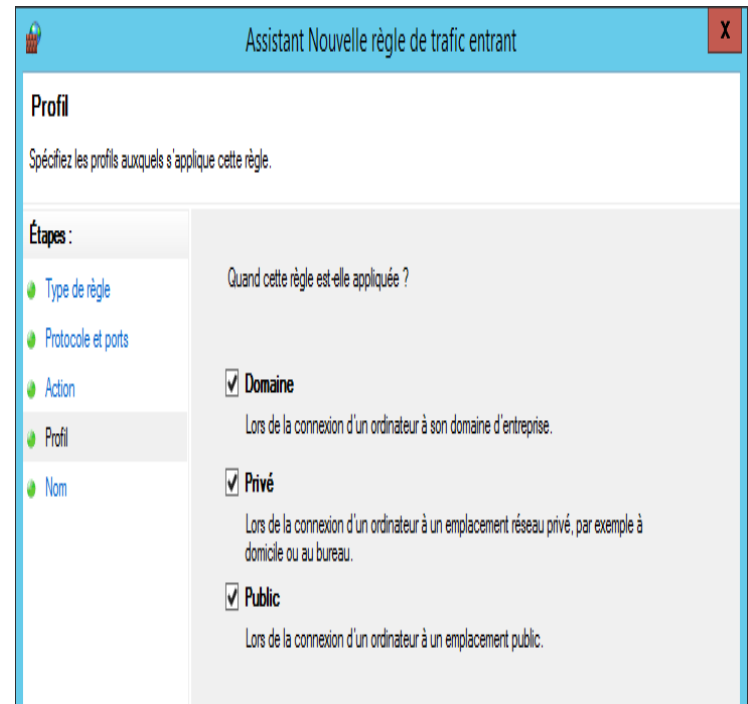
☐ **Autoriser la connexion si elle est sécurisée**
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

Configuration du Pare-feu Windows Defender avec fonctions avancées de sécurité

- **profil**

- **Domaine** : Appliqué lorsqu'un ordinateur est connecté à un réseau sur lequel réside le compte de domaine de l'ordinateur.
- **Privé** : Appliqué lorsqu'un ordinateur est connecté à un réseau sur lequel ne réside pas le compte de domaine de l'ordinateur, tel qu'un réseau domestique
- **Public** : Appliqué lorsqu'un ordinateur est connecté à un domaine par un réseau public, par exemple ceux disponibles dans les aéroports et dans les cafés.



Configuration du Pare-feu Windows Defender avec fonctions avancées de sécurité

- Désactiver le pare feu Windows

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled False
```

- Activer le pare feu Windows

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
```

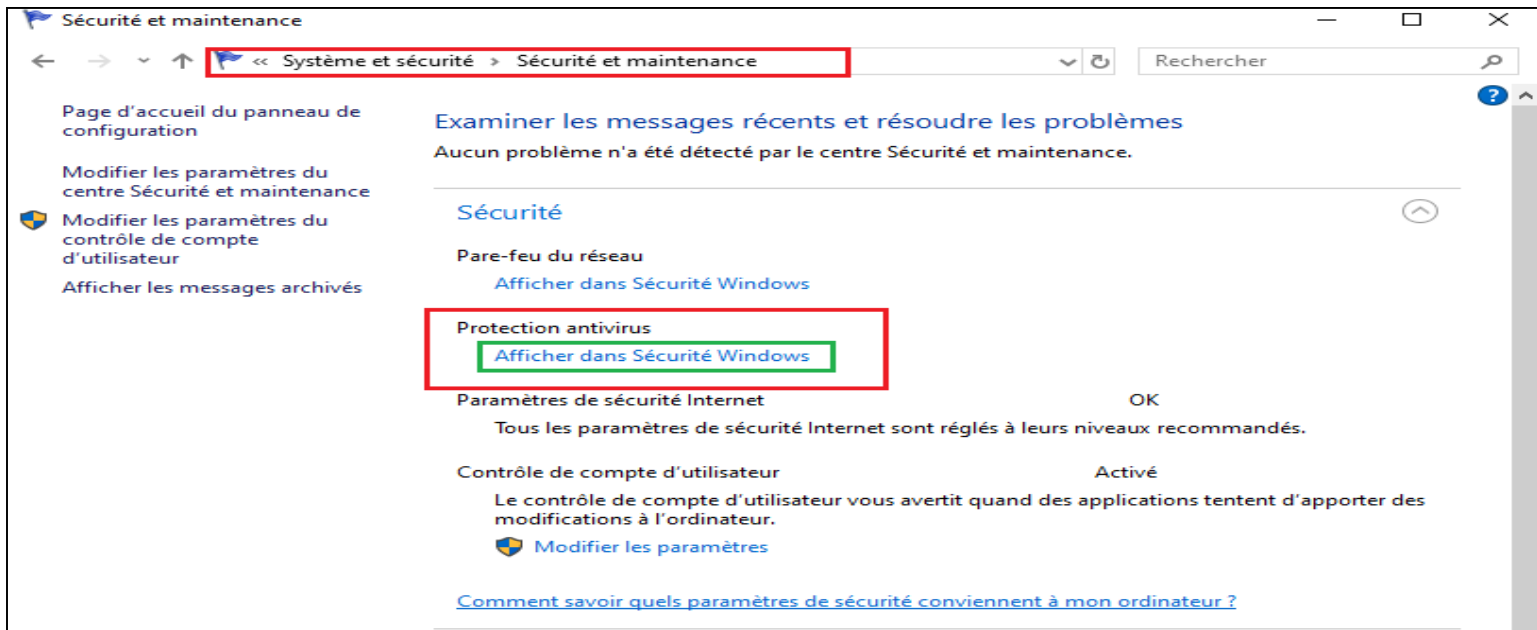
Protection contre les logiciels malveillants

- Windows 10 intègre aussi **Windows Defender** permettant de protéger l'ordinateur contre les menaces de sécurité en détectant et en supprimant les logiciels malveillants.
- Un logiciel malveillant est un logiciels conçus pour nuire à un ordinateur
 - Les logiciels malveillants incluent :
 - Virus
 - Vers informatiques
 - Chevaux de Troie
 - Logiciels espions
 - Logiciels de publicité
 - Les logiciels malveillants entraînent :
 - Une baisse de performances
 - Une perte de données
 - Des accès non autorisés aux d'informations confidentielles
 - Des modifications non autorisées au niveau de la configuration de l'ordinateur

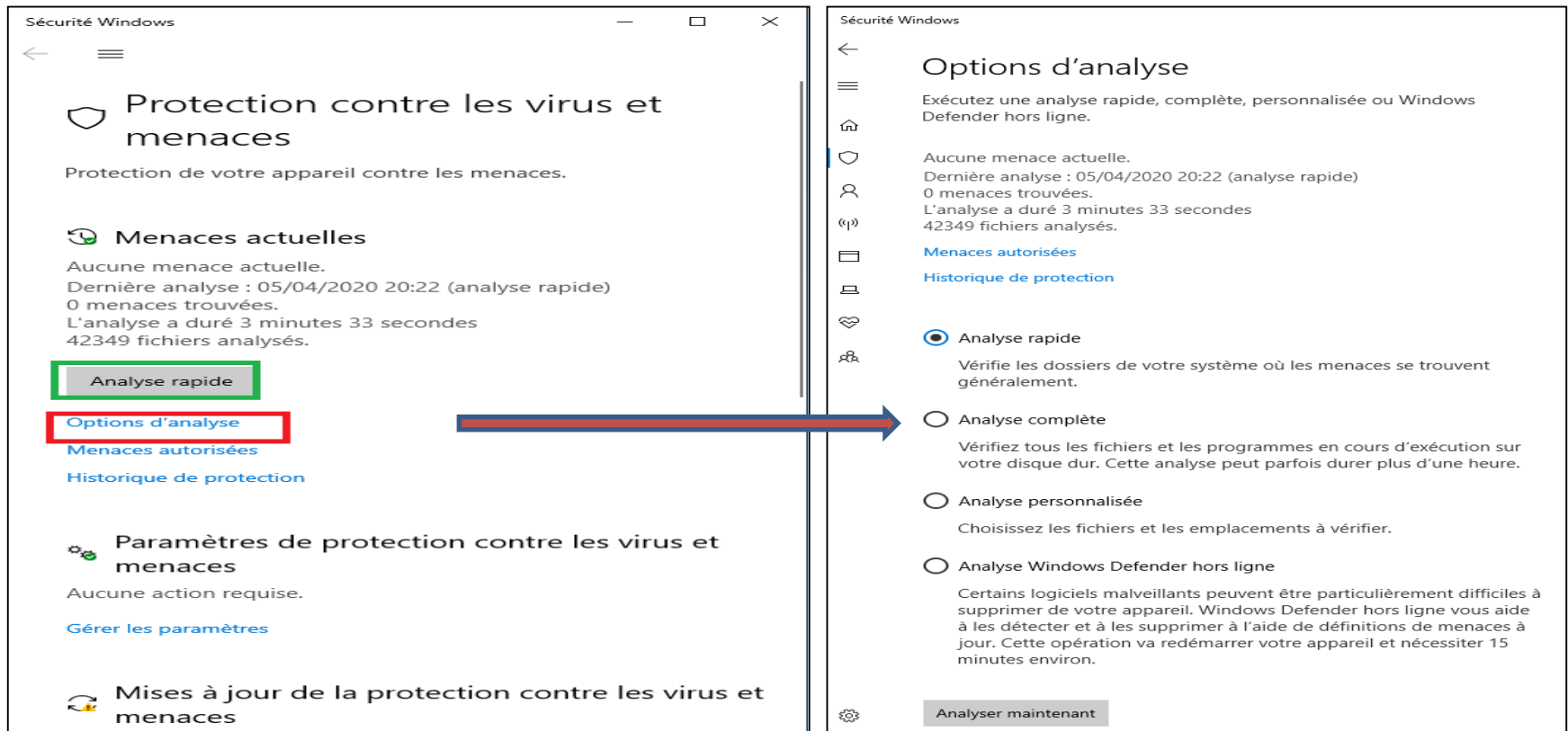
RQ : si vous installer un autre antivirus la protection Windows contre les logiciels malveillants se désactive automatiquement

Protection contre les logiciels malveillants

Pour accéder à la protection antivirus à partir du panneau de configuration → sécurité et système
→ sécurité et maintenance → sécurité



Protection contre les logiciels malveillants



Exercice 5

1. Définir les profils de réseau suivants : Privé, public & domaine.
2. Quelle est la nature d'un pare-feu ?
3. comment fonctionne le pare-feu Windows Defender ?
4. Comment puis-je activer ou désactiver le pare-feu Windows Defender ?
5. Citer les principales fonctionnalités offertes par le pare-feu Windows Defender.
6. Réfléchir sur les principales utilités d'un domaine.

TP N° 6 : Configuration de la connectivité réseau

TP N° 7 : Configuration de la sécurité Windows en utilisant le pare-feu

TP N° 8 : Configuration du pare-feu avec PowerShell