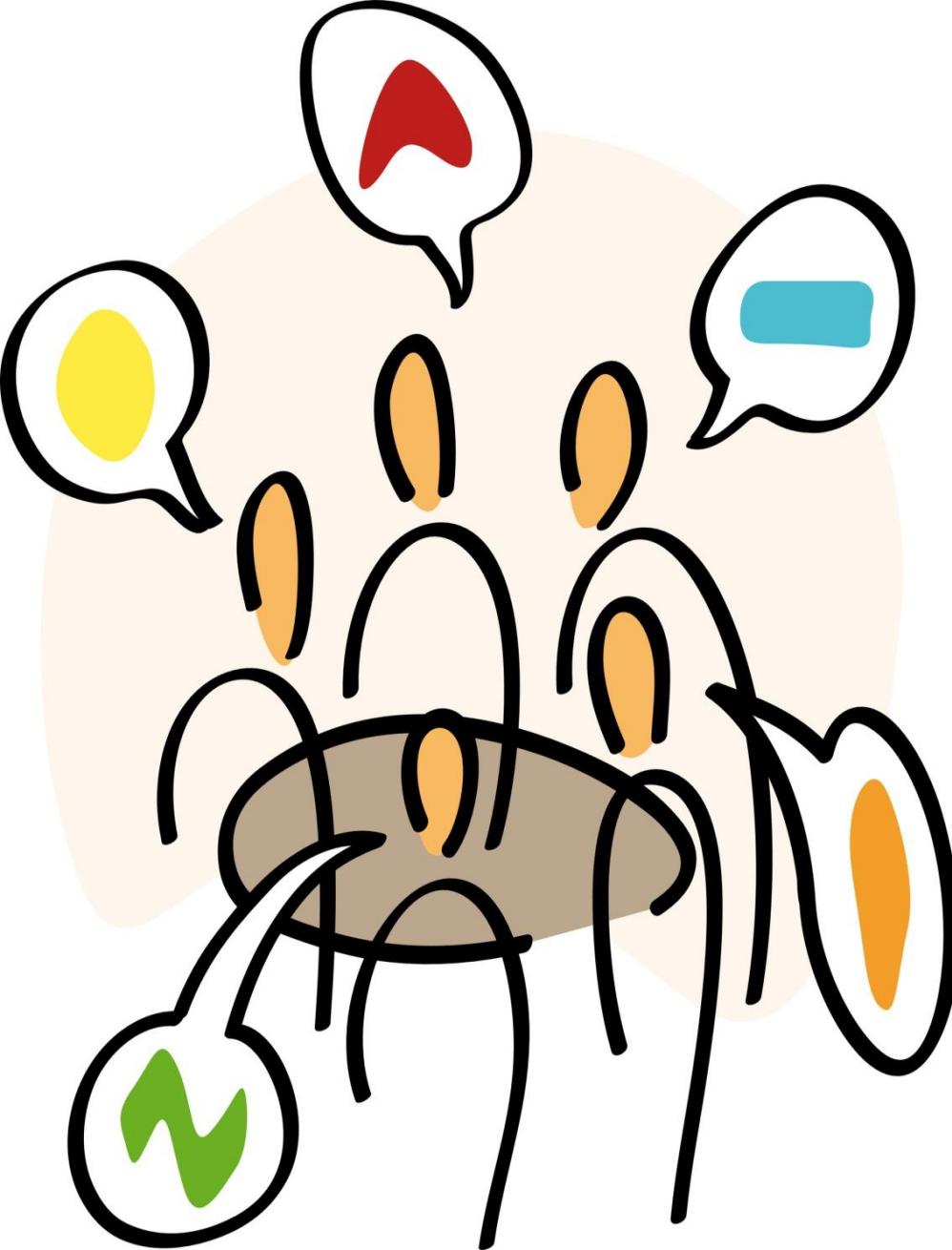


Travail de groupe



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

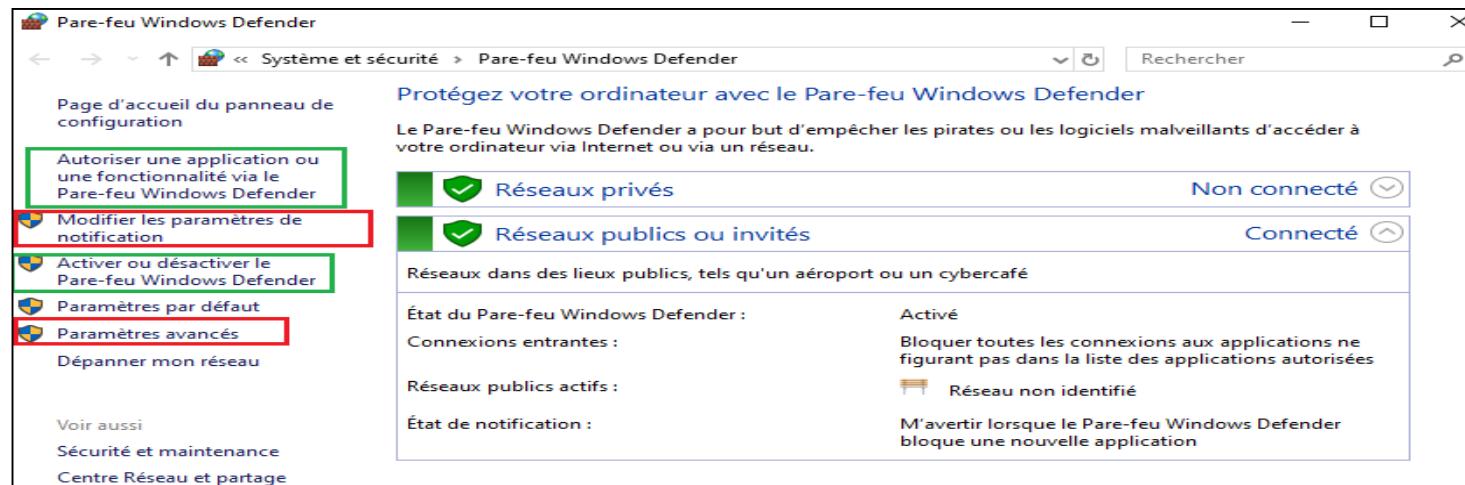
Qu'est-ce qu'un pare-feu

- 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
- ...

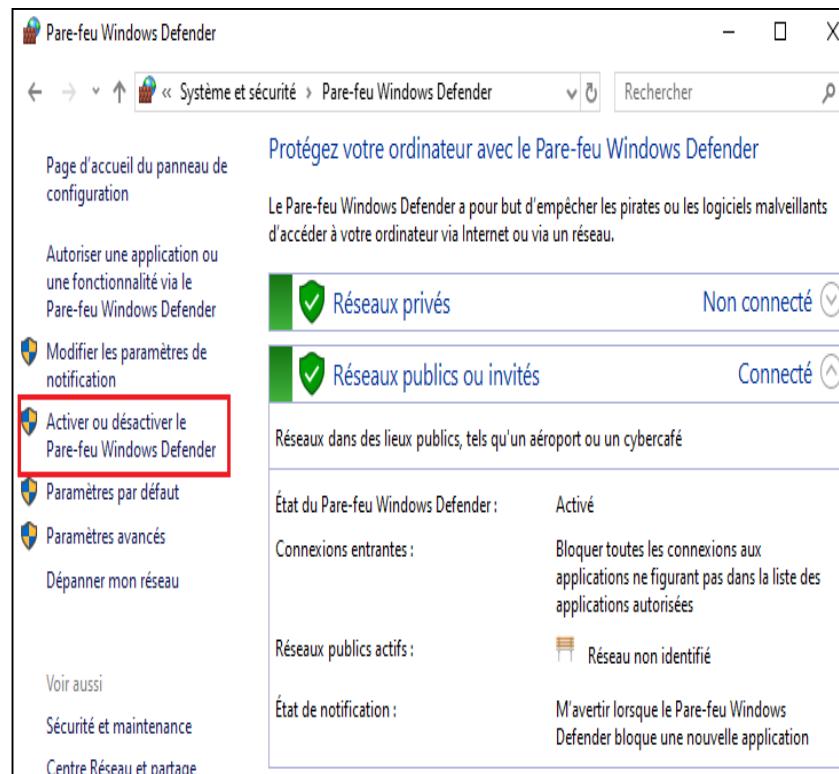


Configuration des paramètres de base du pare-feu Windows

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

The image shows two windows side-by-side. On the left is the 'Pare-feu Windows Defender' configuration window. The 'Autoriser une application ou une fonctionnalité via le Pare-feu Windows Defender' link in the sidebar is highlighted with a red box. A large red arrow points from the bottom right of this window to the top right of the second window. The second window is titled 'Applications autorisées' and shows a list of services with checkboxes for 'Privé' and 'Public'. Two specific items are highlighted with red boxes: 'Arrêt à distance' and 'Bureau à distance'.

Pare-feu Windows Defender

Page d'accueil du panneau de configuration

Protégez votre ordinateur avec le Pare-feu Windows Defender

Le Pare-feu Windows Defender a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à votre ordinateur via Internet ou via un réseau.

Réseaux privés Non connecté

Réseaux publics ou invités Connecté

Réseaux dans des lieux publics, tels qu'un aéroport ou un cybercafé

État du Pare-feu Windows Defender : Activé

Connexions entrantes : Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées

Réseaux publics actifs : Réseau non identifié

État de notification : M'avertir lorsque le Pare-feu Windows Defender bloque une nouvelle application

Applications autorisées

Autoriser les applications à communiquer à travers le Pare-feu Windows Defender

Pour ajouter, modifier ou supprimer des applications et des ports autorisés, cliquez sur Modifier les paramètres.

Quels sont les risques si une application est autorisée à communiquer ?

Modifier les paramètres

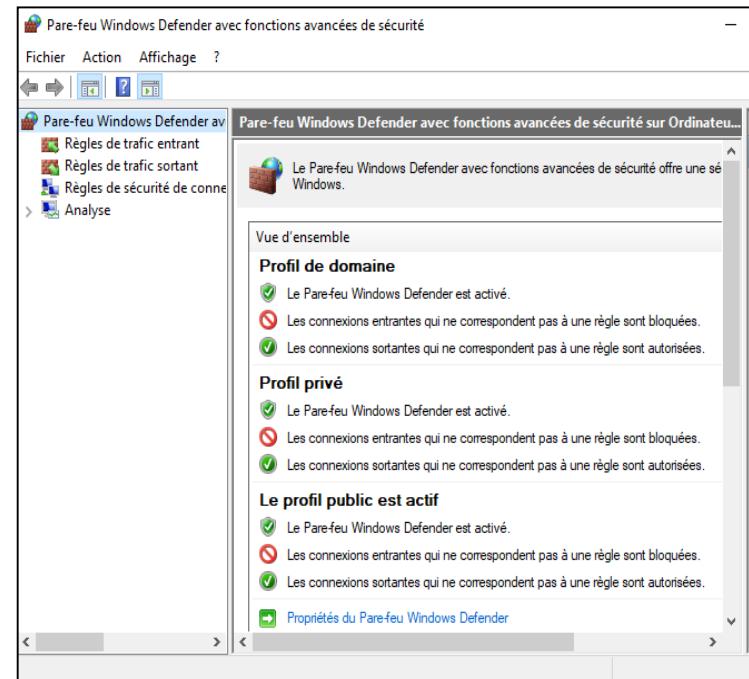
Applications et fonctionnalités autorisées :	Privé	Public
Affichage sans fil	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Analyse de l'ordinateur virtuel	<input type="checkbox"/>	<input type="checkbox"/>
Arrêt à distance	<input type="checkbox"/>	<input type="checkbox"/>
Assistance à distance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BranchCache - Client de mise en cache hébergé (utilise HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
BranchCache - Découverte d'homologue (utilise WSD)	<input type="checkbox"/>	<input type="checkbox"/>
BranchCache - Extraction du contenu (utilise HTTP)	<input type="checkbox"/>	<input type="checkbox"/>
BranchCache - Serveur de cache hébergé (utilise HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
Bureau à distance	<input type="checkbox"/>	<input type="checkbox"/>
Bureau à distance (WebSocket)	<input type="checkbox"/>	<input type="checkbox"/>
Coordoniateur de transactions distribuées	<input type="checkbox"/>	<input type="checkbox"/>

Détails... Supprimer OK Annuler

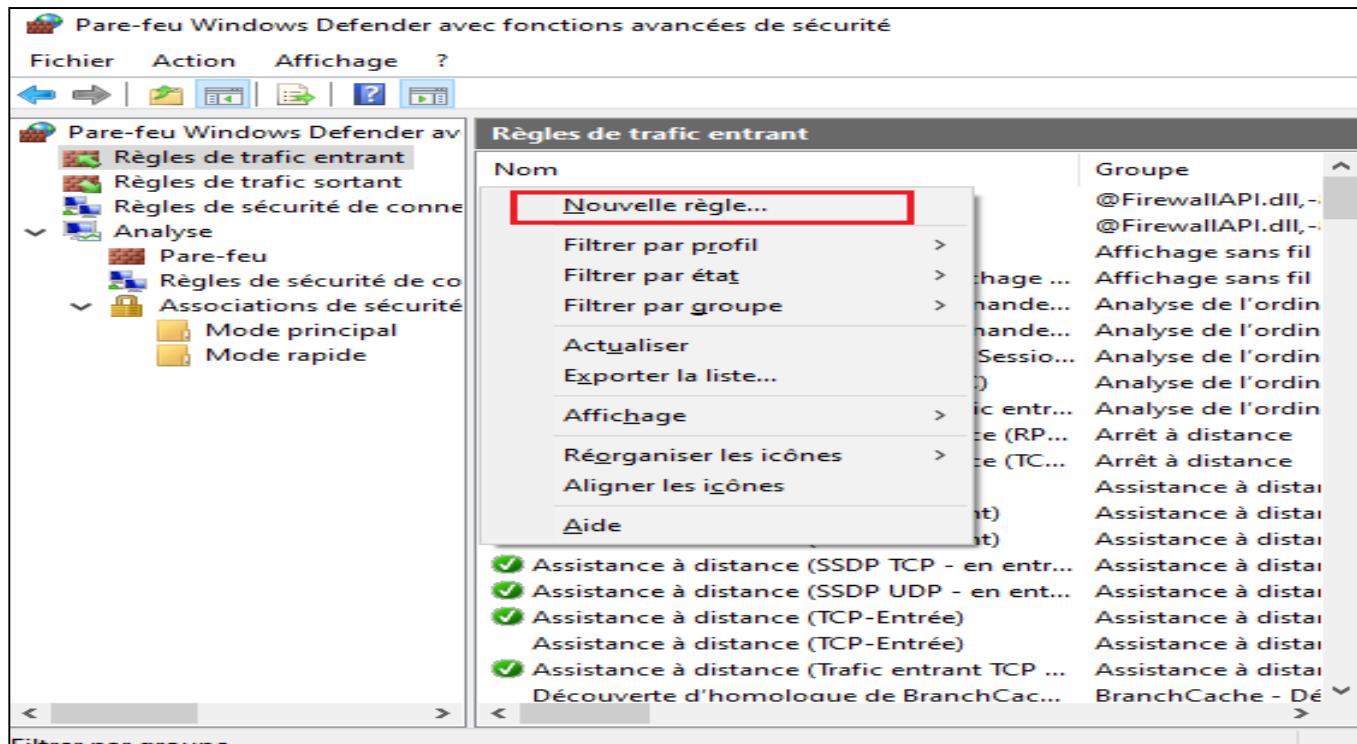
Paramètres du Pare-feu Windows Defender avec fonctions avancées de sécurité

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**.

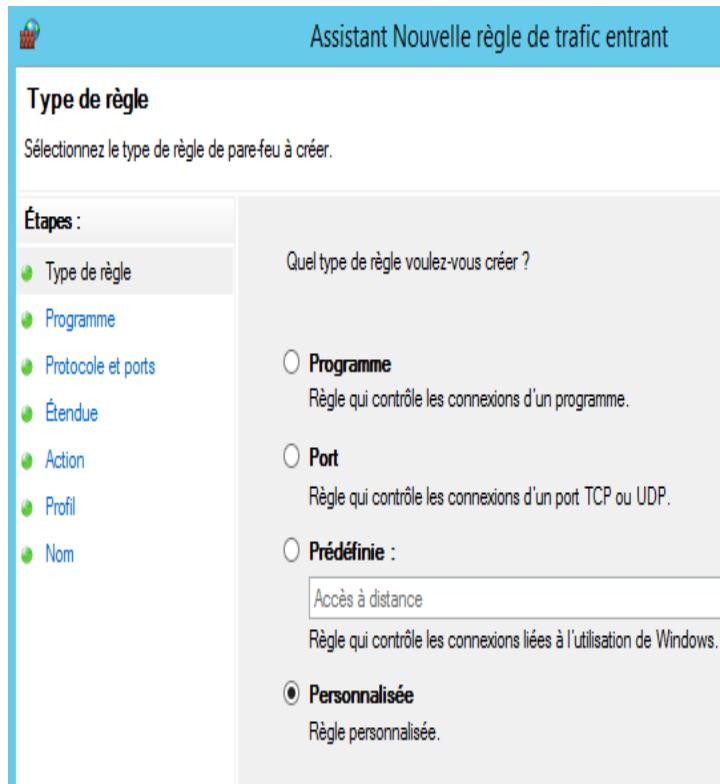


Configuration du Pare-feu Windows avec fonctions avancées de sécurité



Configuration du Pare-feu Windows avec fonctions avancées de sécurité

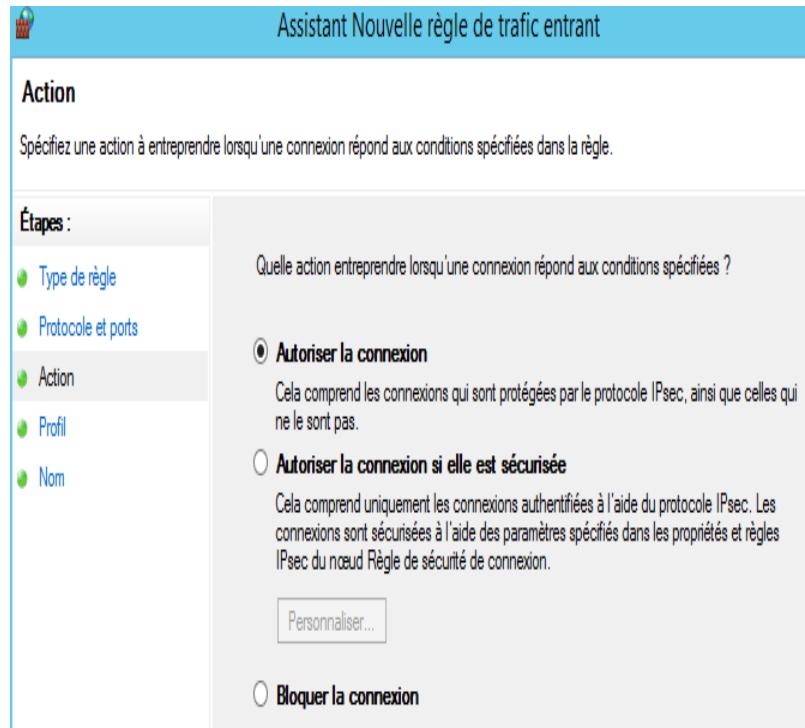
- **Type de règle :**
 - **Programme** : la règle du pare feu contrôle le trafic **en se basant** sur le **nom du programme**.
 - **Ports** : la règle du pare feu contrôle le trafic **en se basant** **le numéro de port**.
 - **Personnalisée** : la règle du pare feu contrôle le trafic en se basant sur 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

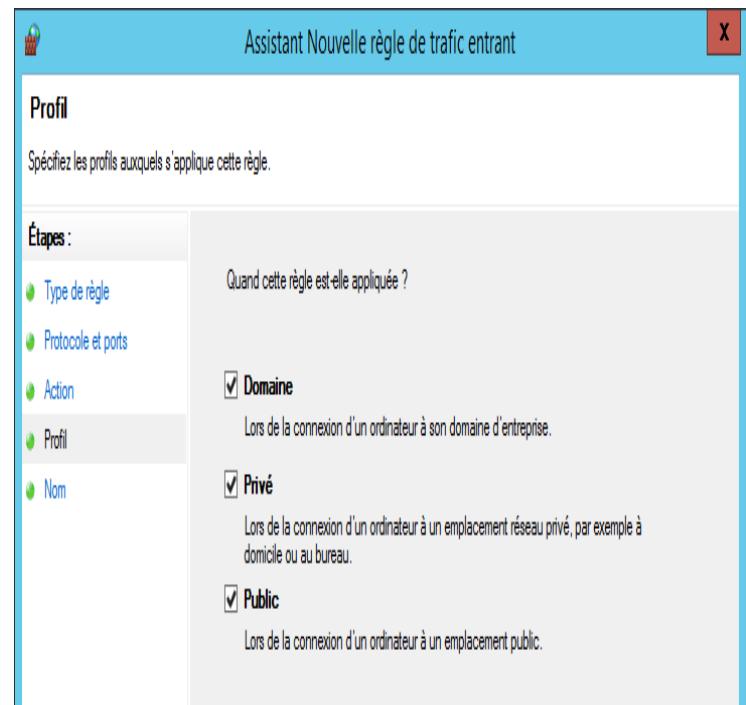
- **Action**

Spécifie si le trafic sera autorisé ou bloqué



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
```

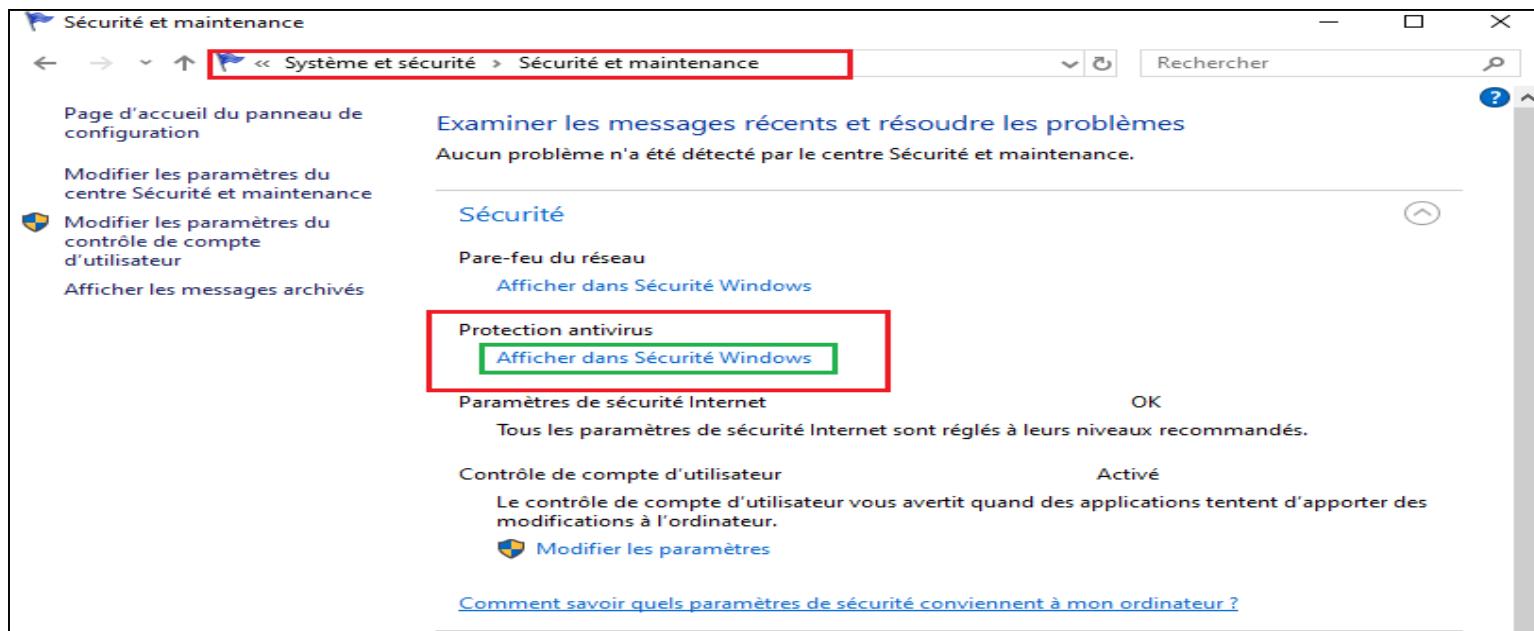
Protection contre les logiciels malveillants

- 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 :**
 - **Les logiciels malveillants entraînent :**
- | | |
|--|---|
| <ul style="list-style-type: none">• Virus• Vers informatiques• Chevaux de Troie• Logiciels espions• Logiciels de publicité | <ul style="list-style-type: none">• 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

The image shows two screenshots of the Windows Security app side-by-side.

Left Screenshot: The main interface of the Windows Security app. It displays the following sections:

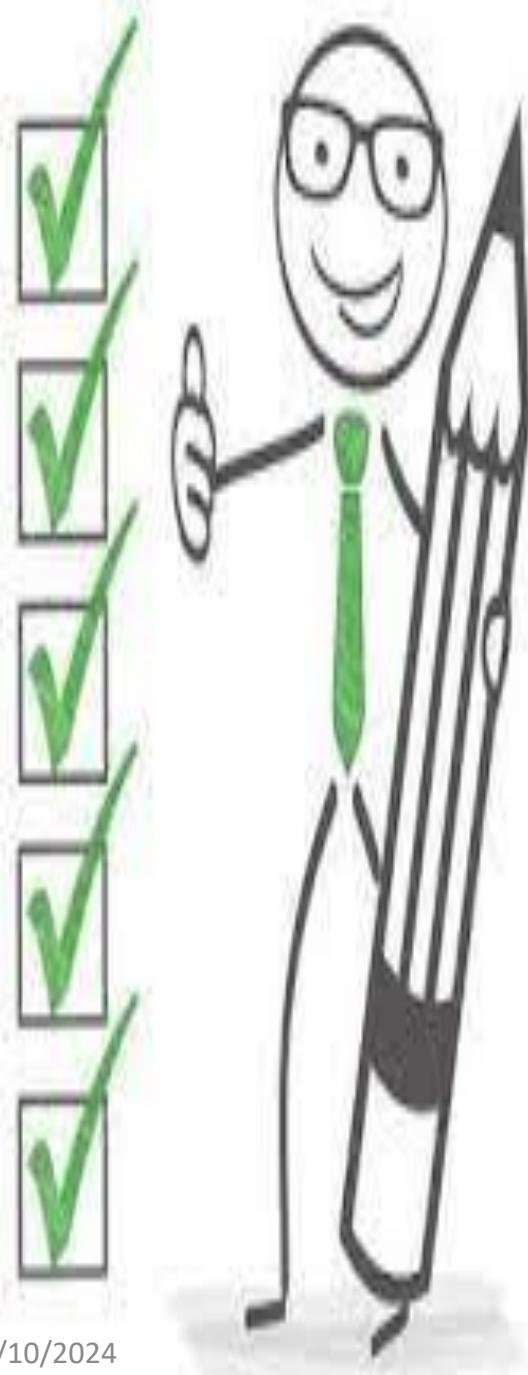
- Protection contre les virus et menaces:** Shows "Protection de votre appareil contre les menaces".
- Menaces actuelles:** Shows "Aucune menace actuelle.", "Dernière analyse : 05/04/2020 20:22 (analyse rapide)", "0 menaces trouvées.", "L'analyse a duré 3 minutes 33 secondes", and "42349 fichiers analysés".
- Options d'analyse:** A button labeled "Analyse rapide" is highlighted with a green border. Other options include "Options d'analyse" (highlighted with a red border), "Menaces autorisées", and "Historique de protection".
- Paramètres de protection contre les virus et menaces:** Shows "Aucune action requise." and a link "Gérer les paramètres".
- Mises à jour de la protection contre les virus et menaces:** Shows a circular icon with arrows.

Right Screenshot: The "Options d'analyse" (Scan Options) section. It includes:

- A sidebar with icons for File, Network, Firewall, Task Manager, and Help.
- Options d'analyse:** Sub-sections include "Exécutez une analyse rapide, complète, personnalisée ou Windows Defender hors ligne.", "Aucune menace actuelle.", "Dernière analyse : 05/04/2020 20:22 (analyse rapide)", "0 menaces trouvées.", "L'analyse a duré 3 minutes 33 secondes", and "42349 fichiers analysés".
- Menaces autorisées** and **Historique de protection**.
- Analyse rapide** (selected): "Vérifie les dossiers de votre système où les menaces se trouvent généralement."
- Analyse complète**: "Vérifiez tous les fichiers et les programmes en cours d'exécution sur votre disque dur. Cette analyse peut parfois durer plus d'une heure."
- Analyse personnalisée**: "Choisissez les fichiers et les emplacements à vérifier."
- Analyse Windows Defender hors ligne**: "Certains logiciels malveillants peuvent être particulièrement difficiles à supprimer de votre appareil. Windows Defender hors ligne vous aide à les détecter et à les supprimer à l'aide de définitions de menaces à jour. Cette opération va redémarrer votre appareil et nécessiter 15 minutes environ."

A large blue arrow points from the "Options d'analyse" section in the left screenshot to the "Analyse rapide" section in the right screenshot.

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