Chapitre 3
Sécurité réseau sous Windows

1. Le pare-feu Windows

1.1 Introduction

Les systèmes d'exploitation Windows et Windows Server intègrent un pare-feu, ou *firewall* en anglais. Il s'agit d'un pare-feu logiciel nommé Pare-feu Windows Defender sur les systèmes de Microsoft.

Il sert à contrôler quels sont les flux autorisés ou interdits, que ce soit les flux entrants ou sortants, au niveau de la machine locale.

Pour communiquer sur le réseau, chaque service ou application utilise un ou plusieurs ports réseau. C'est en contrôlant l'accès sur les ports que l'on va pouvoir déterminer si l'on autorise ou non une connexion.

Le pare-feu de Windows est capable de contrôler les connexions sur les ports TCP et UDP, en ICMP, mais aussi les connexions d'un programme.

Il prend en charge la création de règles avec des paramètres communs que l'on retrouve sur les firewalls de façon générale :

– adresse IP locale ;
– adresse IP distante ;
– port local ;
– port distant ;
– type de protocole.

À cela s'ajoutent des conditions avancées pour contrôler les connexions sur une application, un service, ou sur un type de connexion spécifique (accès distant, réseau sans fil et réseau local) ou pour certains ordinateurs autorisés uniquement.

1.2 La notion de profils

Le pare-feu Windows intègre trois profils : **Domaine**, **Privé** et **Public**. Le système sélectionne automatiquement le profil de pare-feu adapté selon le réseau sur lequel vous êtes connecté.

– Le **profil de domaine** s'applique aux réseaux où la machine Windows peut s'authentifier auprès d'un contrôleur de domaine. C'est un cas fréquent en entreprise lorsque les machines sont intégrées à un domaine Active Directory.
– Le **profil privé** est un profil attribué par l'utilisateur, utile pour le réseau à son domicile.
– Le **profil public**, qui est le **mode par défaut**, utilisé pour désigner les réseaux publics. Ce profil s'applique lorsque vous êtes connecté à votre domicile en Wi-Fi, ou lorsque vous êtes connecté depuis un hôtel, un train, un aéroport, etc.

Cette notion de profil est importante car chaque règle de filtrage peut s'appliquer sur un ou plusieurs profils.

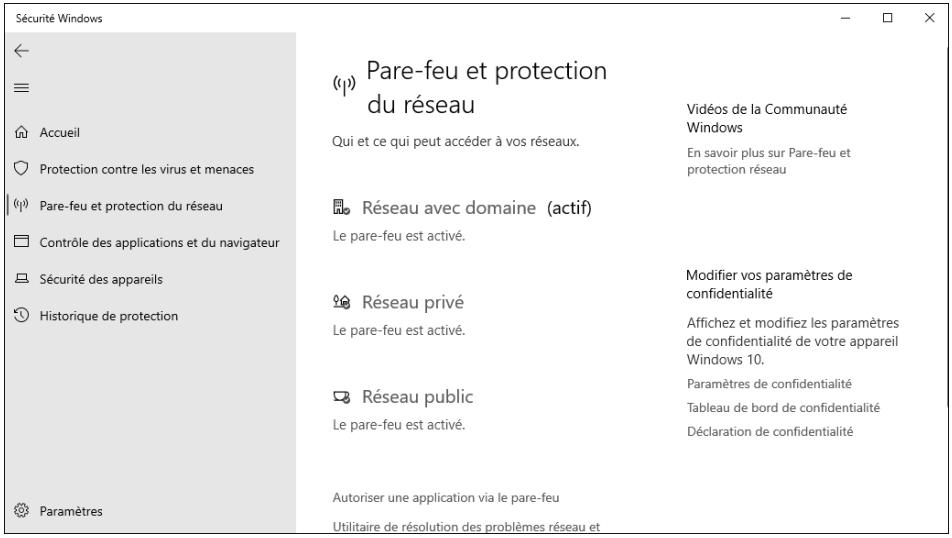
Ce qui permet d'autoriser une connexion lorsque le pare-feu est en mode domaine, ce qui est le cas lorsque l'utilisateur est connecté au réseau de l'entreprise, tout en refusant cette même connexion lorsque la machine est connectée sur un réseau public.

1.3 Visualiser l'état du pare-feu

1.3.1 Avec l'interface graphique

Sous Windows Server 2022, l'accès à l'application Sécurité Windows permet de visualiser l'état du pare-feu Windows.

Cette application contient une section nommée Pare-feu et protection du réseau. Vous pouvez visualiser l'état de chaque profil, le profil actif et gérer les règles.



Par ailleurs, le Panneau de configuration classique de Windows donne aussi accès à la gestion du pare-feu. Les deux chemins d'accès sont liés mais Microsoft a entamé la modernisation de l'interface des paramètres du système depuis plusieurs années.

1.3.2 Avec PowerShell

Le module PowerShell nommé NetSecurity, intégré à Windows, sert à gérer le pare-feu en ligne de commande et à afficher son statut.

La commande ci-dessous sert à afficher le statut de chaque profil du pare-feu :

```
Get-NetFirewallProfile | Format-Table Name,Enabled
```

Si tous les profils sont associés à la valeur `True`, cela signifie que le pare-feu est activé sur l'ensemble des profils.

```
PS C:\> Get-NetFirewallProfile | Format-Table Name,Enabled

Name    Enabled
----    -------
Domain     True
Private    True
Public     True
```

Toutefois, cette commande n'indique pas quel est le profil actif actuellement. Pour obtenir cette information, il faut s'appuyer sur une autre commande :

```
Get-NetFirewallSetting -PolicyStore ActiveStore | Select-Object
-ExpandProperty ActiveProfile
```

Cette commande retournera le nom du profil actif. Par exemple, la valeur Domain si le profil domaine est actif.

1.3.3 Avec la commande netsh

La commande `netsh`, présente sous Windows avant même la création de PowerShell, peut aussi rendre des services pour gérer le pare-feu et simplement afficher son statut.

La commande ci-dessous affiche les paramètres de chaque profil, et la propriété `État` indique si le profil est activé ou désactivé :

```
netsh advfirewall show allprofiles
```

La commande ci-dessous affiche les paramètres du profil actif :

```
netsh advfirewall show currentprofile
```

La première ligne de la configuration indique l'état du profil :

```
PS C:\> netsh advfirewall show currentprofile

Paramètres Profil de domaine :
----------------------------------------------------------------------
État                                  Actif
Stratégie de pare-feu                 BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (magasin d'objets de stratégie de groupe uniquement)
LocalConSecRules                      N/A (magasin d'objets de stratégie de groupe uniquement)
InboundUserNotification               Désactiver
RemoteManagement                      Désactiver
UnicastResponseToMulticast            Activer

Journalisation :
LogAllowedConnections                 Désactiver
LogDroppedConnections                 Désactiver
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096

Ok.
```

1.4 Créer une règle de pare-feu

En tant qu'administrateur, vous pourriez être amené à créer une règle de pare-feu dans Windows ou à éditer une règle de pare-feu existante.

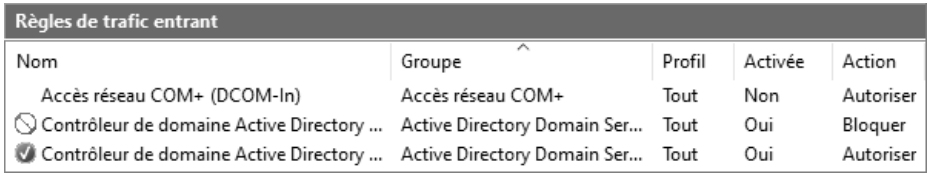
Pour créer une règle de pare-feu à partir de l'interface graphique de Windows et avoir accès à l'ensemble des options, il faut accéder à la console Pare-feu Windows Defender avec fonctions avancées de sécurité, à partir des Paramètres ou du Panneau de configuration.

Avant de commencer, sachez qu'il n'est pas toujours nécessaire de créer une règle de toute pièce. Windows est livré avec un ensemble de règles, certaines sont activées, d'autres désactivées mais prêtes à l'emploi.

En regardant les règles de trafic entrant et de trafic sortant, on peut différencier trois types de règles :

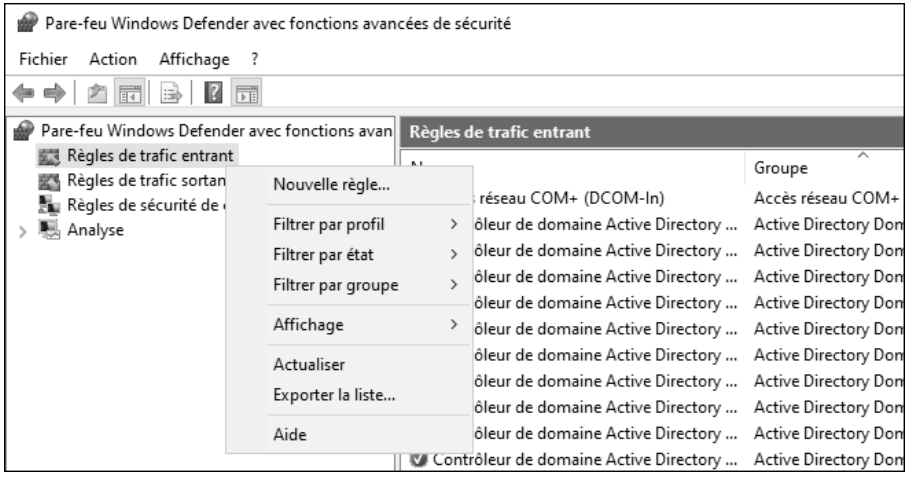
– règle activée pour autoriser une connexion ;
– règle activée pour bloquer une connexion ;
– règle de blocage ou d'autorisation existante mais non activée.

Un indicateur visuel présent à gauche du nom de la règle indique son état :



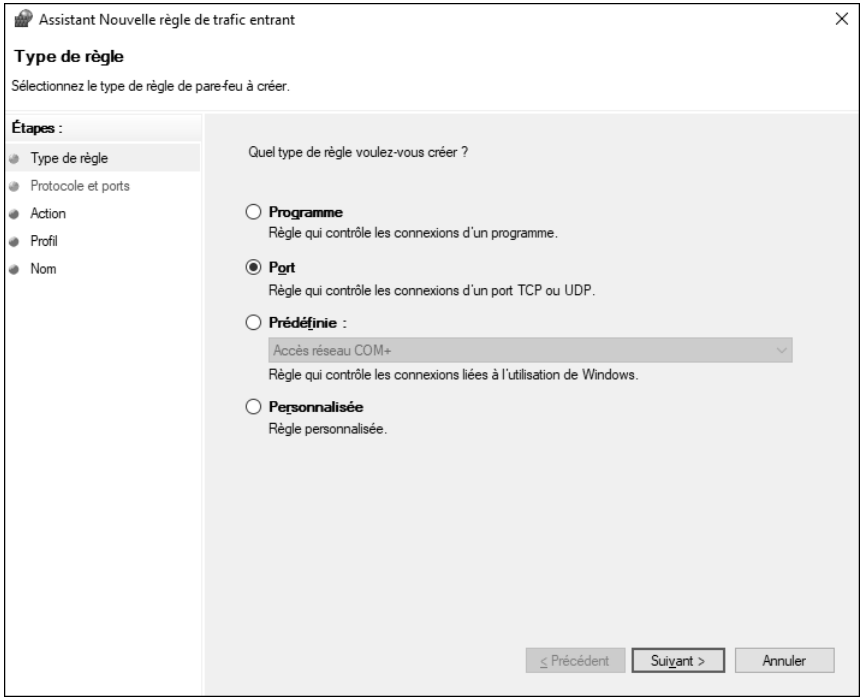
Par exemple, si vous souhaitez autoriser l'accès **Bureau à distance** (port 3389), il n'est pas nécessaire de créer votre propre règle car il y a déjà des règles prédéfinies pour ce service.

Si vous avez besoin de créer une règle spécifique, pour une application tierce par exemple, vous devez effectuer un clic droit sur **Règles de trafic entrant** ou **Règles de trafic sortant**, selon la direction du flux, et cliquer sur **Nouvelle règle...**.



Puis, suivez l'assistant de manière à créer votre règle pour autoriser l'application ou le port correspondant à votre besoin.

Le type de règle **Personnalisée** est le plus complet car il donne accès à plus d'options (notamment les restrictions sur les adresses IP source et destination).



En ligne de commande, vous pouvez utiliser :

– la commande PowerShell `New-NetFirewallRule` ;
– la commande `netsh` (`netsh advfirewall firewall add rule`).

1.5 Bonnes pratiques

1.5.1 L'état du pare-feu

Sur les postes de travail, les serveurs membres et les contrôleurs de domaine Active Directory, il est fortement recommandé d'activer le pare-feu Windows Defender et de prendre le temps de le configurer.

Le pare-feu doit être activé sur les trois profils : **Domaine**, **Privé** et **Public**.

1.5.2 Les connexions sortantes

Même s'il peut sembler plus prudent de bloquer les connexions sortantes dans le pare-feu Windows afin d'autoriser uniquement celles dont on a besoin, dans la pratique c'est différent.

Remarque

Une connexion sortante signifie que c'est la machine locale qui émet du trafic à destination d'une autre machine. Le flux réseau sort de la machine locale.

Il sera nécessaire de passer un temps important à configurer les règles de pare-feu et à gérer les exceptions (un poste de travail sur lequel une application spécifique a besoin d'une autorisation sur un port non autorisé jusqu'ici, par exemple).

Par ailleurs, si un attaquant a compromis le système et obtenu des droits d'administration, il pourra de toute façon réviser les règles du pare-feu.

Il est préférable de s'intéresser davantage aux règles de connexions entrantes.

Dans la configuration du pare-feu, le mode **Autoriser (par défaut)** permet d'autoriser les connexions sortantes.

1.5.3 Les connexions entrantes

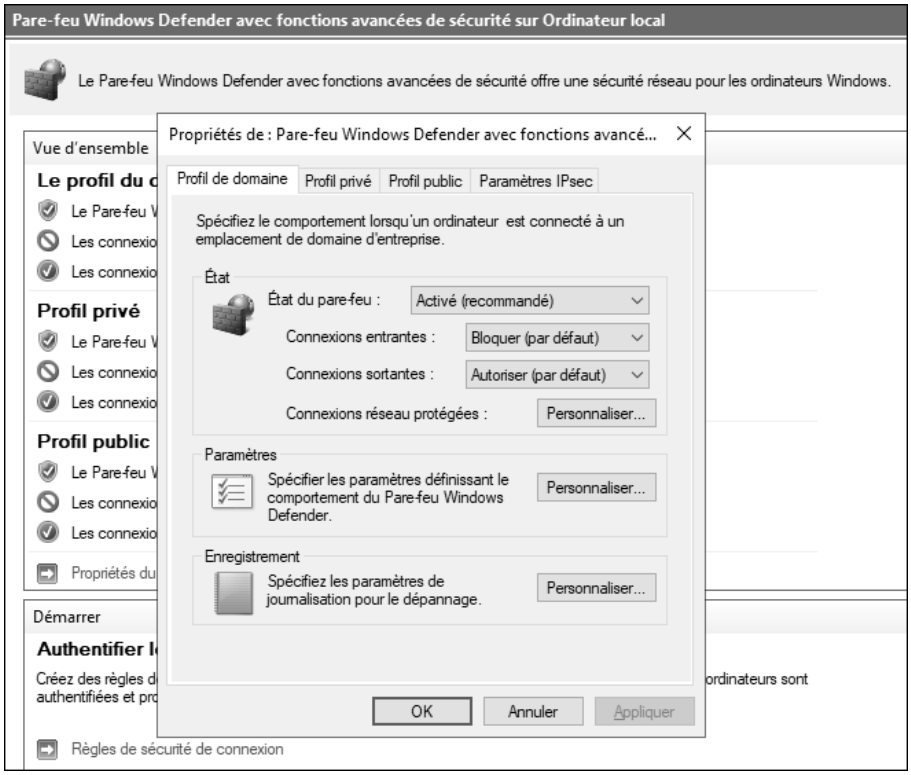
Pour les connexions entrantes, donc à destination de notre machine locale, la bonne pratique consiste à appliquer la stratégie **Bloquer (par défaut)**, qui est différente de la stratégie **Tout bloquer**.

Microsoft a introduit un ensemble de règles pour empêcher la majorité des connexions entrantes afin de protéger les services réseau.

En limitant les connexions entrantes, vous réduisez votre surface d'attaque donc un attaquant aura plus de difficultés à effectuer des mouvements latéraux à partir d'une machine compromise.

Remarque

Nous insistons sur le fait d'avoir un pare-feu actif et bien configuré sur les serveurs et postes de travail.



1.5.4 La gestion centralisée des paramètres de pare-feu

Pour que la configuration du pare-feu soit homogène sur les différents types de machines, il convient de gérer la configuration à l'aide de stratégies de groupe (en environnement Active Directory).

Pour les environnements Cloud chez Microsoft, l'administrateur peut s'appuyer sur le service Microsoft Intune pour gérer les règles du pare-feu Windows.

Ainsi, les règles seront distribuées et imposées par une stratégie de groupe.