Pare-feu

Généralités et Pare-feu Windows Server

11:11PM

Topics Covered

Start

Généralités sur les pare-feu

Qu’est-ce qu’un pare-feu et à quoi sert-il dans un réseau informatique ?

Le firewall est un outil de sécurité permettant de sécuriser l'entrée d’un réseau à l'aide de filtrage et de règles.

Quelle est la différence entre un pare-feu matériel et un pare-feu logiciel ?

L’un est matériel tandis que l’autre est immatériel. Le prix semble également être plus important pour ce qui est du firewall matériel

Quelles sont les principales fonctions d'un pare-feu moderne ?

Les pare-feu modernes surpassent les anciens en termes de capacité d'analyse, d'adaptabilité et de protection contre les cybermenaces avancées. Ils sont essentiels face aux défis de la sécurité numérique actuelle

Comment les pare-feu participent-ils à la sécurité des systèmes d'information ?

Les pare-feu sont des gardiens essentiels, offrant une défense proactive et adaptée aux menaces numériques.

Topics Covered

Généralités sur le pare-feu Windows

Quel est le rôle principal du pare-feu Windows Defender sur les systèmes Windows et Windows Server ?

En résumé, il agit comme une barrière protectrice, assurant la sécurité des données et des communications sur les systèmes Windows.

Quels types de connexions le pare-feu Windows est-il capable de contrôler ?

Il existe 2 types de connexion: une connexion entrante comme un accès à distant et une connexion sortante comme un logiciel qui se connecte à internet.

Topics Covered

Profils du pare-feu Windows

3. Profils du pare-feu Windows

Quels sont les trois profils de pare-feu disponibles dans Windows ?

Les profils publics, privés et profils de domaine. Ils offrent un contrôle global sur les flux réseau, qu'ils soient entrants ou sortants, pour renforcer la sécurité.

Quel profil est automatiquement sélectionné lorsqu'un ordinateur s'authentifie sur un contrôleur de domaine ?

Profil réseau domaine reprenant les rôles et spécificités d’une organisation, Kerberos, GPO etc..

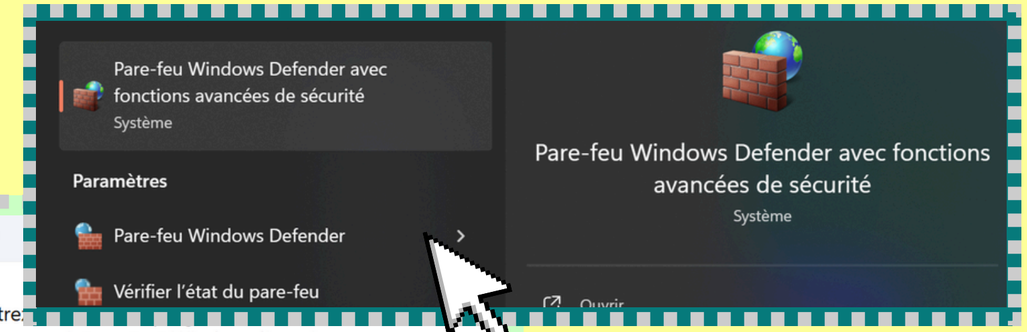
Pourquoi la notion de profil de pare-feu est-elle importante pour la gestion des règles de filtrage ?

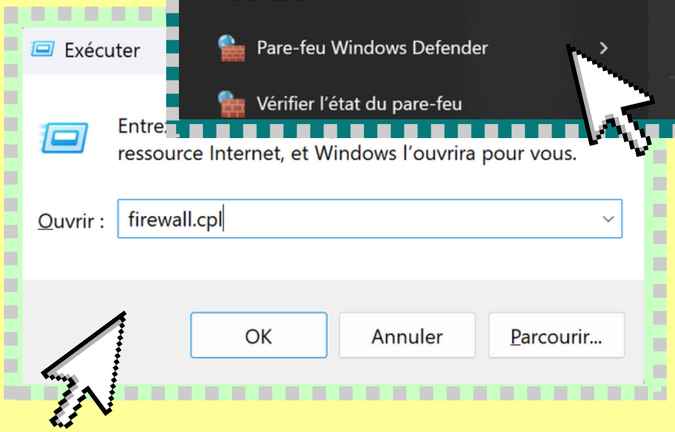
Les profils de pare-feu garantissent une gestion efficace et automatique des règles de filtrage, tout en assurant une sécurité appropriée à chaque environnement.

Topics Covered

Visualisation et gestion du pare-feu

Quels sont les deux moyens principaux pour visualiser l'état du pare-feu sous Windows Server ?





Quelle commande PowerShell permet d'afficher l'état des profils du pare-feu ?

Ouvrir CMD et écrire :

Firewall.cpl

Ou sur Powershell :

Get-NetFirewallProfile

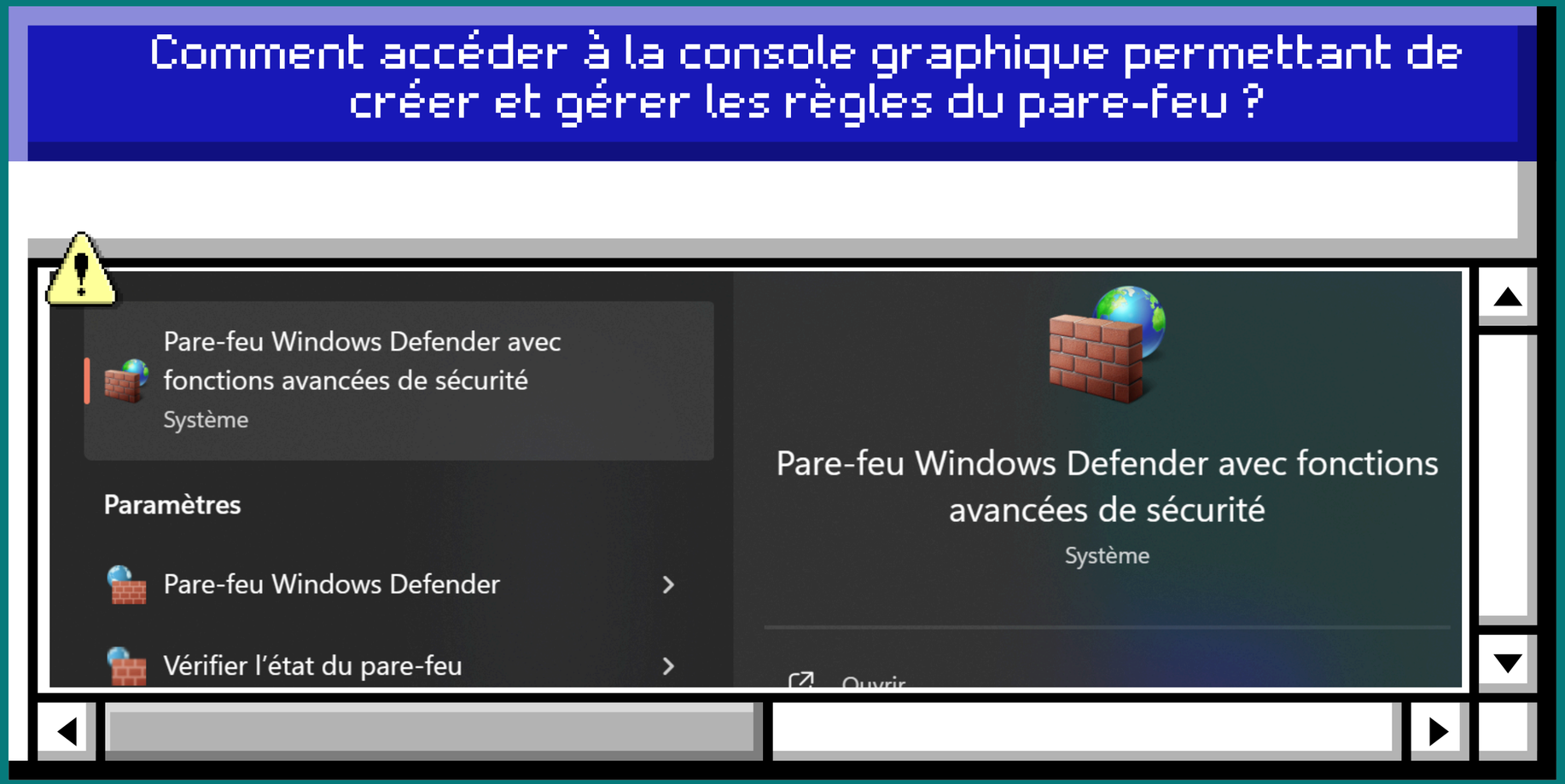
Quelle commande netsh permet d'afficher les paramètres du profil actif du pare-feu ?

netsh advfirewall show currentprofile

Topics Covered

Création et gestion des règles

Comment accéder à la console graphique permettant de créer et gérer les règles du pare-feu ?



Quels sont les trois types de règles que l'on peut trouver dans la console du pare-feu Windows Defender ?

les règles de trafic entrant.

les règles de trafic sortant

les règles de sécurité de connexion (pour les vpn)

Quelle est la commande PowerShell permettant de créer une nouvelle règle de pare-feu ?

New-NetFirewallRule -DisplayName "Autoriser le port 8080" -Direction Inbound -Protocol TCP -LocalPort 8080 -Action Allow

Pourquoi est-il recommandé d’activer le pare-feu sur les postes de travail, serveurs membres et contrôleurs de domaine ?

Pour protéger contre les attaques, limiter les connexions non autorisées et renforcer la sécurité réseau.

Quelle est la stratégie recommandée pour les connexions entrantes et pourquoi ?

La stratégie recommandé est de bloquer par défaut : n’autorise que les connexions nécessaires (ex : un serveur qui héberge un site web a besoin du port 80 ouvert)

Pourquoi bloquer toutes les connexions sortantes peut-il être compliqué à gérer en pratique ?

Beaucoup d'applications légitimes (navigateurs, mise a jours) ont besoin d’internet. il faut alors créer des règles manuelles , ce qui prend du temps

Quelle solution Microsoft permet de gérer les règles du pare-feu dans un environnement Cloud ?

La solution est Azure Firewall, il permet de gérer les par feu à distance dans un environnement cloud

11:11PM


MERCI !
15/20