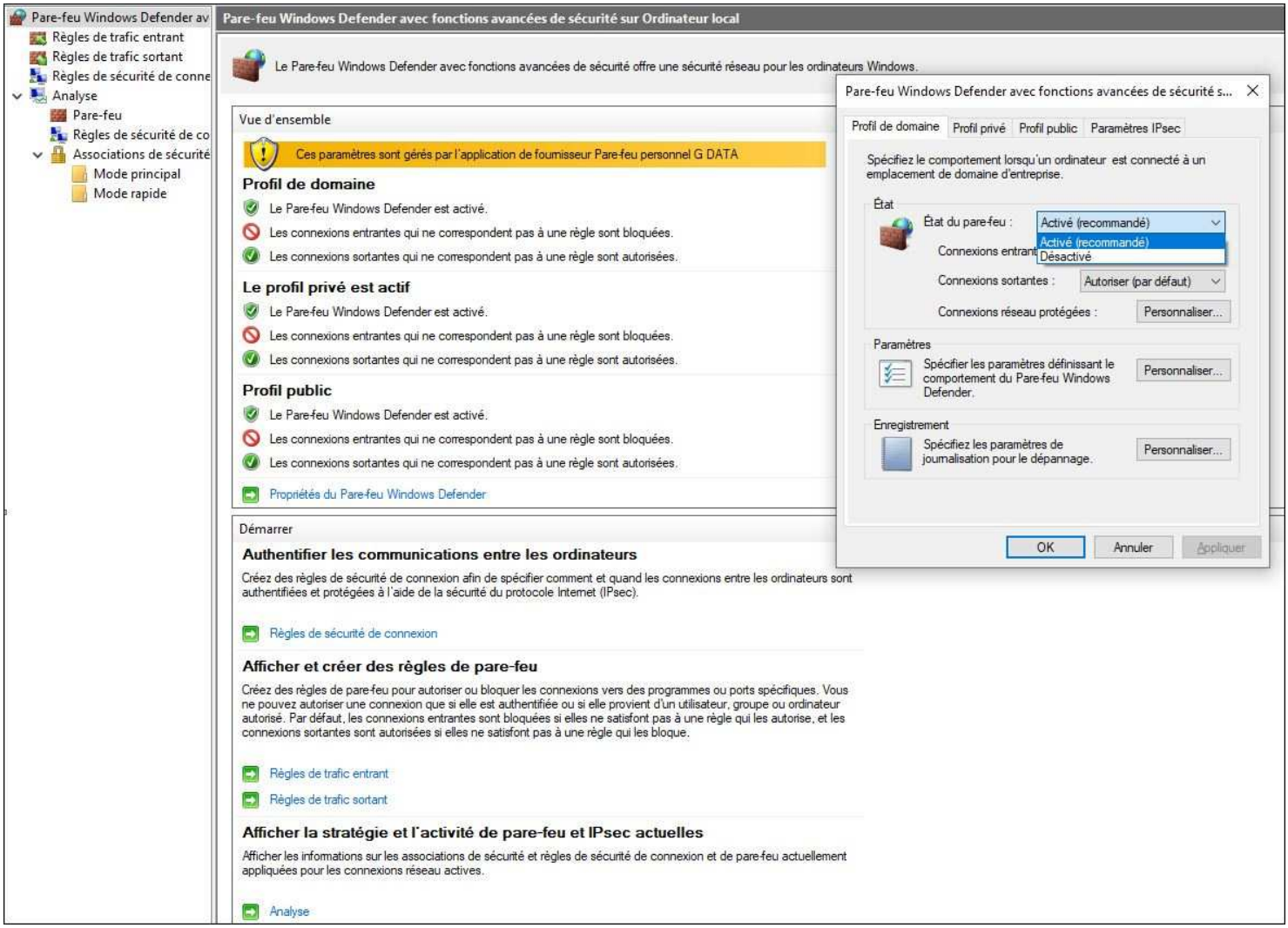

Pare-feu Windows Defender
Panneau de configuration › Système et sécurité › Pare-feu Windows Defender
Page d'accueil du panneau de configuration
Autoriser une application ou une fonctionnalité via le Pare-feu Windows Defender
Modifier les paramètres de notification
Activer ou désactiver le Pare-feu Windows Defender
Paramètres par défaut
Paramètres avancés
Dépanner mon réseau
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.
Ces paramètres sont gérés par l'application du fournisseur Pare-feu personnel G DATA
Réseaux privés
Connecté
Réseaux publics ou invités
Non connecté


Pare-feu Windows Defender av
Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de conne
Analyse
Pare-feu
Règles de sécurité de co
Associations de sécurité
Mode principal
Mode rapide
Pare-feu Windows Defender avec fonctions avancées de sécurité sur Ordinateur local
Le Pare-feu Windows Defender avec fonctions avancées de sécurité offre une sécurité réseau pour les ordinateurs Windows.
Vue d'ensemble
Ces paramètres sont gérés par l'application de fournisseur Pare-feu personnel G DATA
Profil de domaine
Le Pare-feu Windows Defender est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Le profil privé est actif
Le Pare-feu Windows Defender est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Profil public
Le Pare-feu Windows Defender est activé.
Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.
Propriétés du Pare-feu Windows Defender
Démarrer
Authentifier les communications entre les ordinateurs
Créez des règles de sécurité de connexion afin de spécifier comment et quand les connexions entre les ordinateurs sont authentifiées et protégées à l'aide de la sécurité du protocole Internet (IPsec).
Règles de sécurité de connexion
Afficher et créer des règles de pare-feu
Créez des règles de pare-feu pour autoriser ou bloquer les connexions vers des programmes ou ports spécifiques. Vous ne pouvez autoriser une connexion que si elle est authentifiée ou si elle provient d'un utilisateur, groupe ou ordinateur autorisé. Par défaut, les connexions entrantes sont bloquées si elles ne satisfont pas à une règle qui les autorise, et les connexions sortantes sont autorisées si elles ne satisfont pas à une règle qui les bloque.
Règles de trafic entrant
Règles de trafic sortant
Afficher la stratégie et l'activité de pare-feu et IPsec actuelles
Afficher les infomations sur les associations de sécurité et règles de sécurité de connexion et de pare-feu actuellement appliquées pour les connexions réseau actives.
Analyse
Pare-feu Windows Defender avec fonctions avancées de sécurité s...
Profil de domaine
Profil privé
Profil public
Paramètres IPsec
Spécifiez le comportement lorsqu'un ordinateur est connecté à un emplacement de domaine d'entreprise.
État
État du pare-feu :
Activé (recommandé)
Désactivé
Connexions entrantes :
Connexions sortantes :
Autoriser (par défaut)
Connexions réseau protégées :
Personnaliser...
Paramètres
Spécifier les paramètres définissant le comportement du Pare-feu Windows Defender.
Personnaliser...
Enregistrement
Spécifiez les paramètres de journalisation pour le dépannage.
Personnaliser...
OK
Annuler
Appliquer