CLOISONNEMENT DES RÉSEAUX

1 2 3

Fiche pratique pour la mise en oeuvre de votre plan d'actions cyber dans votre collectivité.

Description rapide de l'objectif visé :

Le pare-feu local est activé et les communications entrantes sont bloquées.

Coût estimé :

0€

Niveau de difficulté de l'action :

Simple

Ressources nécessaires :

Ordinateur, tableur

Niveau d'accompagnement :

Basique

Temps estimé :

1 jour

Public visé pour l'action :

Responsable informatique
Personne en charge de l'informatique

Organisation conseillée pour la mise en œuvre dans votre collectivité :

1. Qui fait quoi ? Définir les rôles et responsabilités.
Qui a la responsabilité de paramétrer les ordinateurs sur les éléments de sécurité ?

2. Pourquoi ?
L'absence de pare feu permet le libre échange des données entre votre matériel et le reste des équipements qu'ils soient interne ou externe à la collectivité. Il est donc nécessaire de filtrer pour n'autoriser que les communications de programmes légitimes.

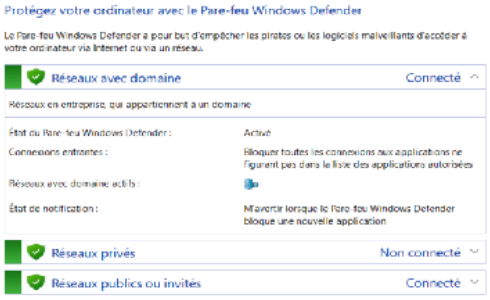
3. Comment ?
Planifier entre 15 et 30 minutes avec les utilisateurs pour réaliser le paramétrage sur leurs postes selon le questionnement de l'utilisateur.

4. Combien ?
Une fois par an pour contrôle de l'activation du pare feu.

5. Quand ?
Le plus tôt possible.

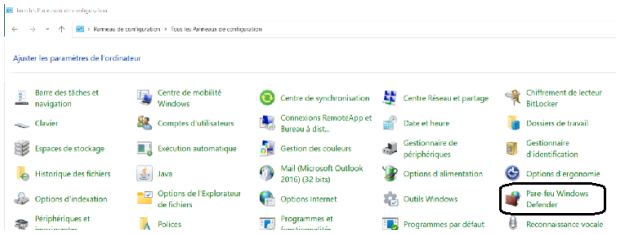
Livrable de l'action terminée :

Etat du pare-feu : activé
Connexions entrantes : Bloquer toutes les connexions aux applications ne figurant pas dans la liste des applications autorisées

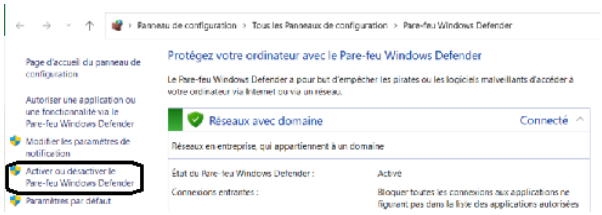


Description étape par étape pour la mise en œuvre :

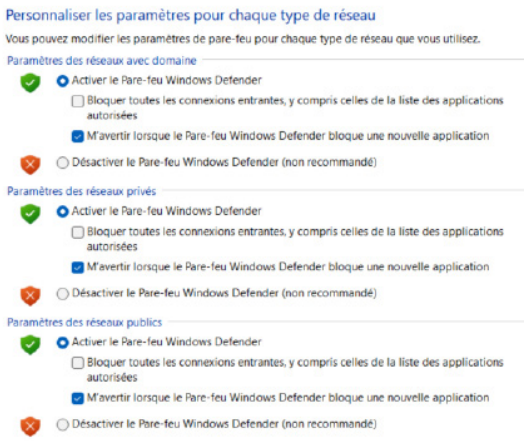
1. Une fois sur le poste de l'utilisateur, parcourir le « panneau de configuration » afin d'aller dans le dossier « Pare-feu Windows defender »



2. Ensuite, cliquer sur « Activer ou désactiver le Pare-feu Windows Defender » :



3. Paramétrer le Pare-feu comme ci-dessous :



Pour aller plus loin :

ANSSI :
- Guide des bonnes pratiques de l'ANSSI
- Cartographie du système d'information

Cybermalveillance :
- Recommandations pour l'administration sécurisée des SI