



CHAPITRE 3

ASSURER LA SÉCURITÉ DU CLIENT WINDOWS

Ce que vous allez apprendre dans ce chapitre :

- Gérer l'authentification dans Windows
- Gérer les permissions et le partage de ressources
- Assurer la protection, le sauvegarde et la restauration des données locales
- Gérer les outils de sécurité sous Windows



15 heures

CHAPITRE 3

ASSURER LA SÉCURITÉ DU CLIENT WINDOWS

1. **Gérer l'authentification dans Windows**
2. Gérer les permissions et le partage de ressources
3. Assurer la protection, le sauvegarde et la restauration des données locales
4. Gérer les outils de sécurité sous Windows



03 – Assurer la sécurité du client Windows

Gérer l'authentification dans Windows



Gérer l'authentification dans Windows

Afin d'assurer la sécurité du client Windows, Windows permet de gérer les comptes utilisateurs, c'est-à-dire la gestion des mots de passe et des paramètres de comptes d'utilisateur pour les utilisateurs qui partagent l'ordinateur. Il permet de modifier le type de compte, et aussi de supprimer des comptes utilisateurs. De plus, il permet la gestion des informations d'identification Web et Windows. On distingue généralement deux types d'utilisateurs : ou un utilisateur simple ou un groupe, et pour chaque type, un compte est associé.

Un compte utilisateur :

Définit les tâches qui peuvent être effectuées par un utilisateur. Il existe deux types de comptes :

- Compte administrateur
- Compte limité

Un groupe :

Permet d'organiser les comptes utilisateurs sous forme de groupes avec la gestion des droits d'accès pour chaque groupe. Cela simplifie la gestion des droits en les attribuant à des groupes plutôt qu'à des utilisateurs spécifiques.

03 – Assurer la sécurité du client Windows

Gérer l'authentification dans Windows

Gestion des comptes utilisateurs

Pour gérer les comptes utilisateurs sous-Windows 10, on doit ouvrir l'application “**panneau de configuration**” et choisir l'onglet “**Comptes utilisateurs**” (Voir la **Figure 73**)

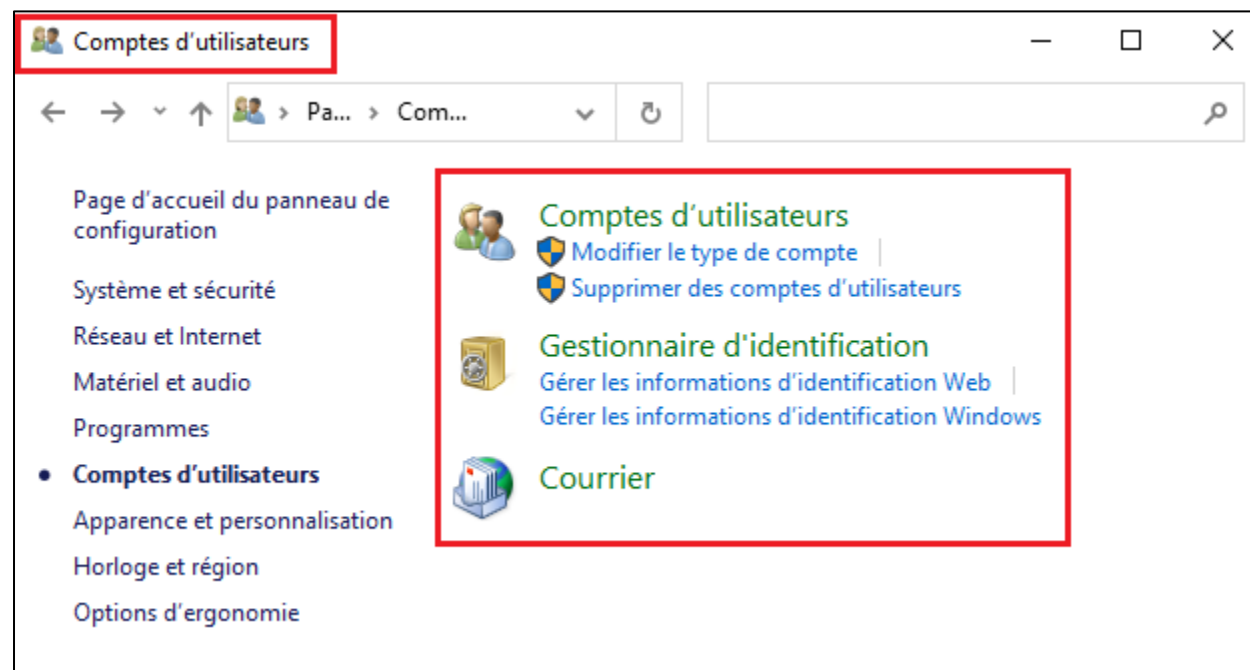


Figure 73: Interface « Comptes d'utilisateur ».

03 – Assurer la sécurité du client Windows

Gérer l'authentification dans Windows

La **Figure 74** illustre l'interface fournie par Windows permettant à l'utilisateur de gérer son compte utilisateur.

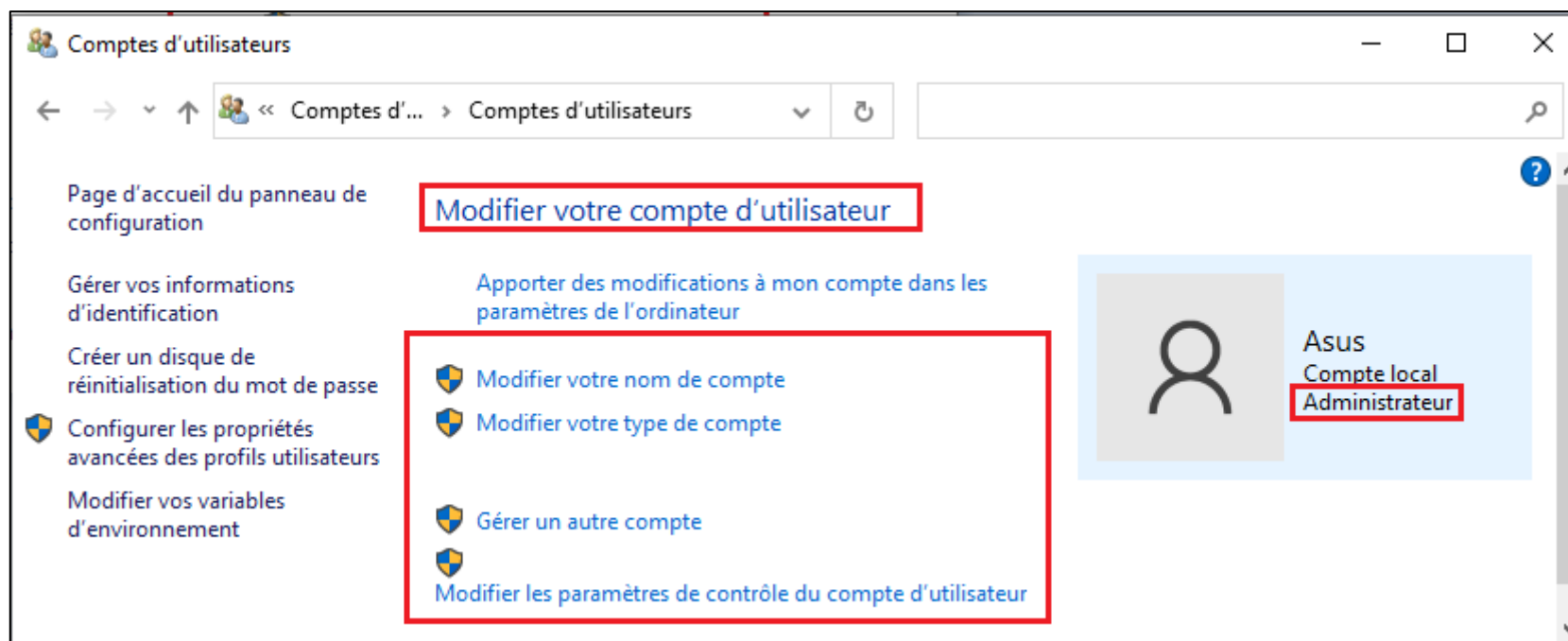


Figure 74: Interface «modifier votre Compte d'utilisateur ».

03 – Assurer la sécurité du client Windows

Gérer l'authentification dans Windows

Si l'utilisateur choisit de modifier son nom de compte, une interface s'affiche, qui lui permet de mettre à jour le nom de son compte (Voir Figure 75 et 76).

Si l'utilisateur choisit de modifier le type de compte, une interface s'affiche qui lui permet de sélectionner le nouveau type de compte soit **Standard** soit **Administrateur**.

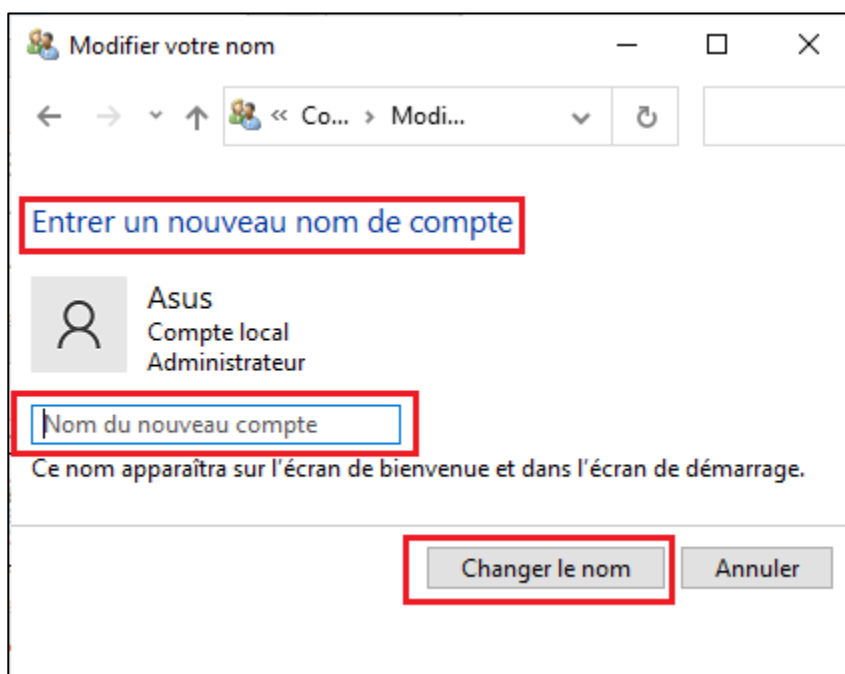


Figure 75 : Interface «Modifier votre nom ».

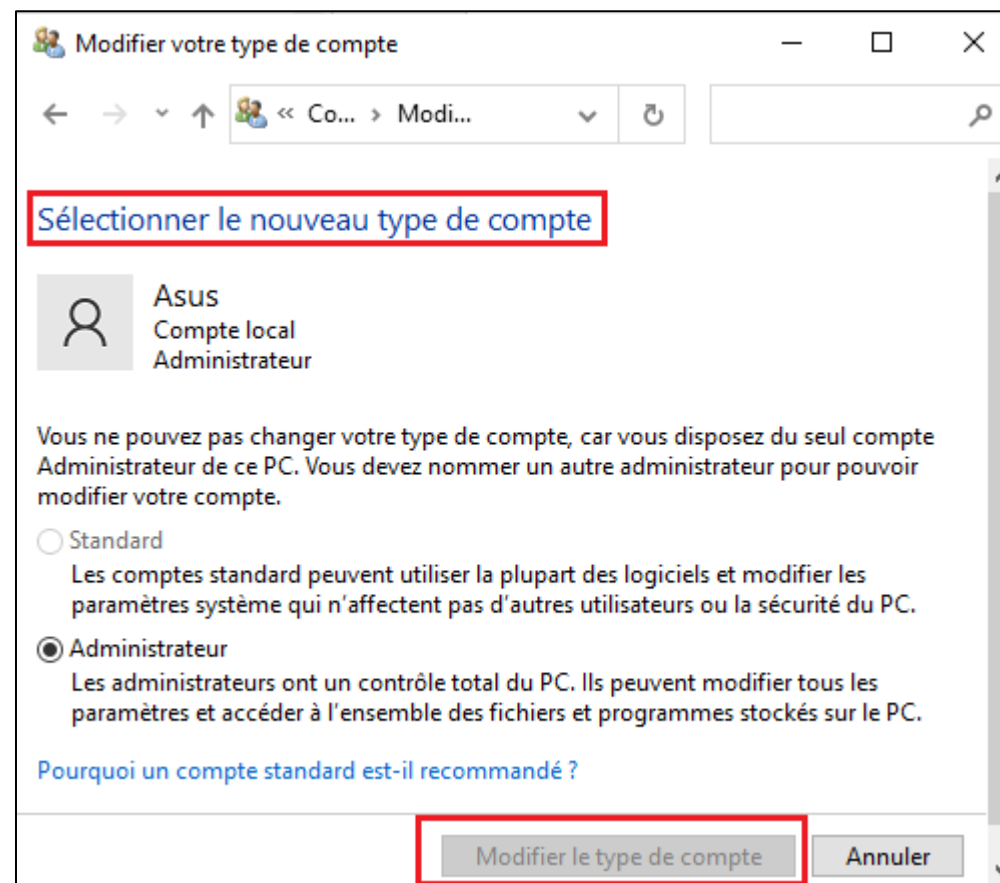


Figure 76 : Interface «Modifier votre type de compte ».

03 – Assurer la sécurité du client Windows

Gérer l'authentification dans Windows

Gestion d'identification

Pour gérer ses informations d'identification Web ou Windows, l'utilisateur doit choisir « Gestionnaire d'identification » (Voir **Figure 77**).

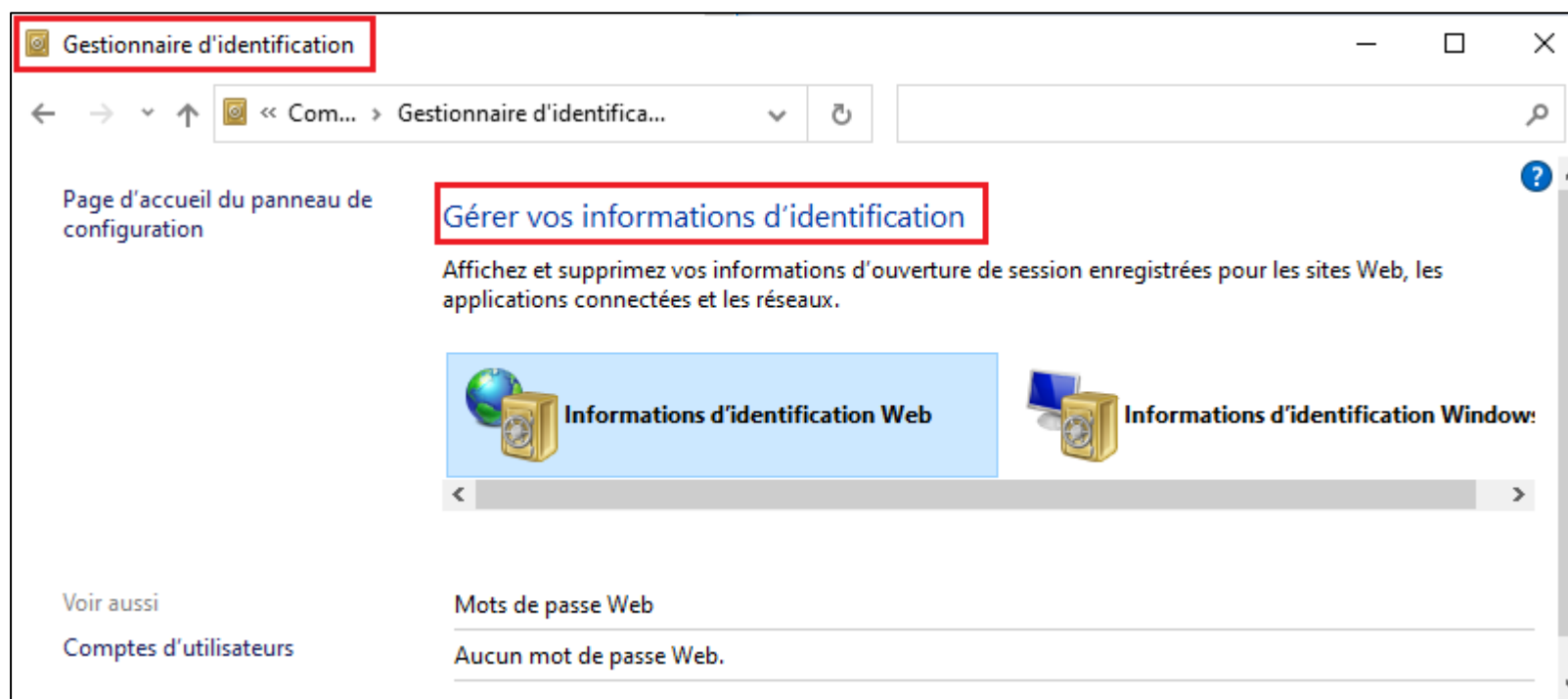


Figure 77: Interface «Gérer vos informations d'identification ».

L'utilisateur peut afficher et supprimer ces informations d'ouverture de session enregistrées pour les sites Web, les applications connectées et les réseaux.

03 – Assurer la sécurité du client Windows

Gérer l'authentification dans Windows

L'authentification des utilisateurs est assurée par :

- **Active Directory** afin d'ouvrir une session sur le domaine (Voir Figure 78).
- **Une base de comptes** afin d'ouvrir une session locale.

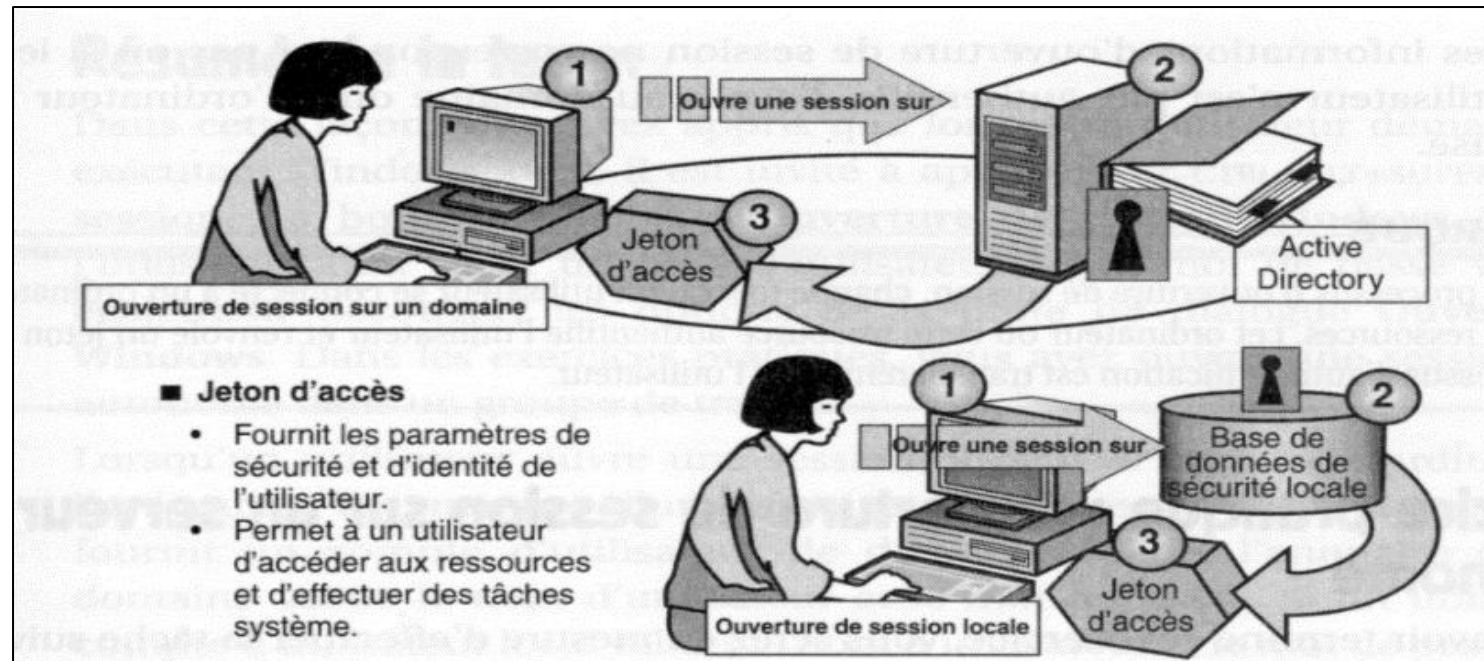


Figure 78 : Etapes d'ouverture de session sur un domaine ou session locale .

CHAPITRE 3

ASSURER LA SÉCURITÉ DU CLIENT WINDOWS

1. Gérer l'authentification dans Windows
2. **Gérer les permissions et le partage de ressources**
3. Assurer la protection, le sauvegarde et la restauration des données locales
4. Gérer les outils de sécurité sous Windows



03 – Assurer la sécurité du client Windows

Gérer les Permissions et le partage de ressources

Gérer les Permissions et le partage de ressources

Windows permet aux utilisateurs de permettre l'accès à leurs fichiers ou ressources comme imprimante par d'autres personnes via le réseau. Pour permettre le partage des ressources, l'utilisateur doit ouvrir le panneau de configuration et choisir **Réseaux et Internet** puis **Centre Réseau et partage** (Voir Figure 79)

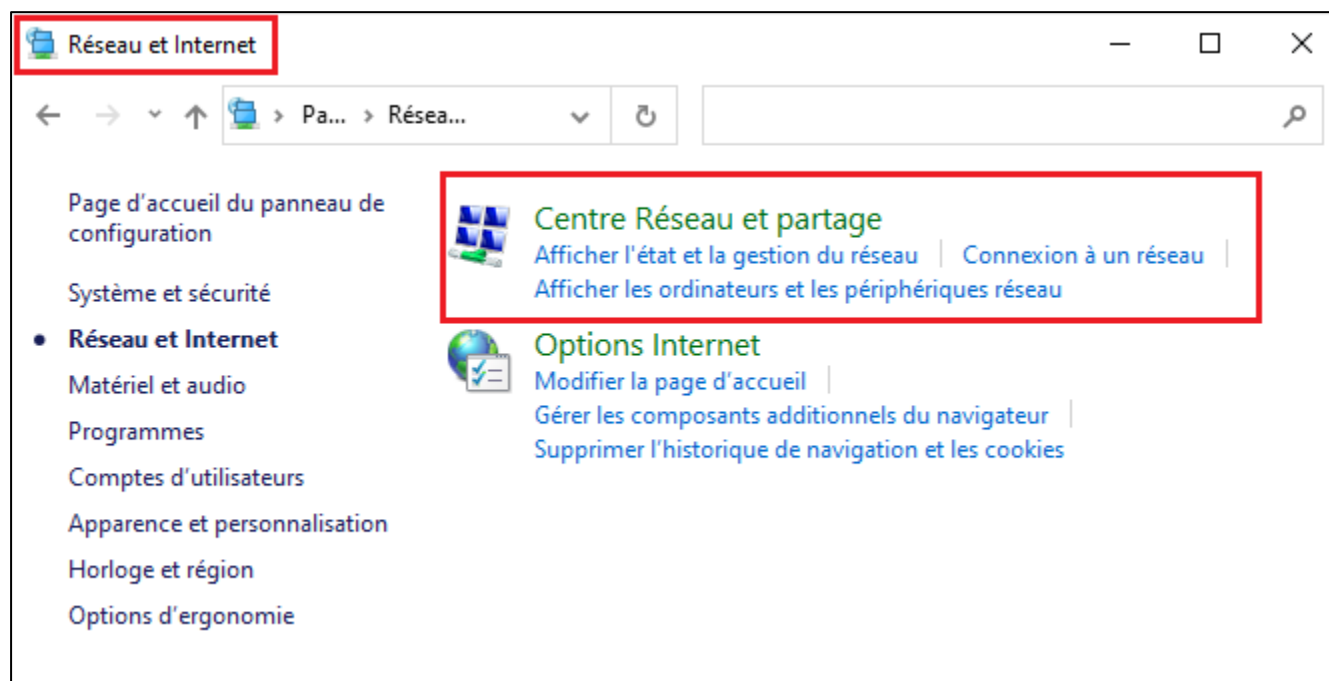


Figure 79 : Interface Réseau et Internet.

03 – Assurer la sécurité du client Windows

Gérer les Permissions et le partage de ressources

Si l'utilisateur souhaite modifier les paramètres de partage il clique sur **Modifier les paramètres de partage avancés** (voir Figure 80).

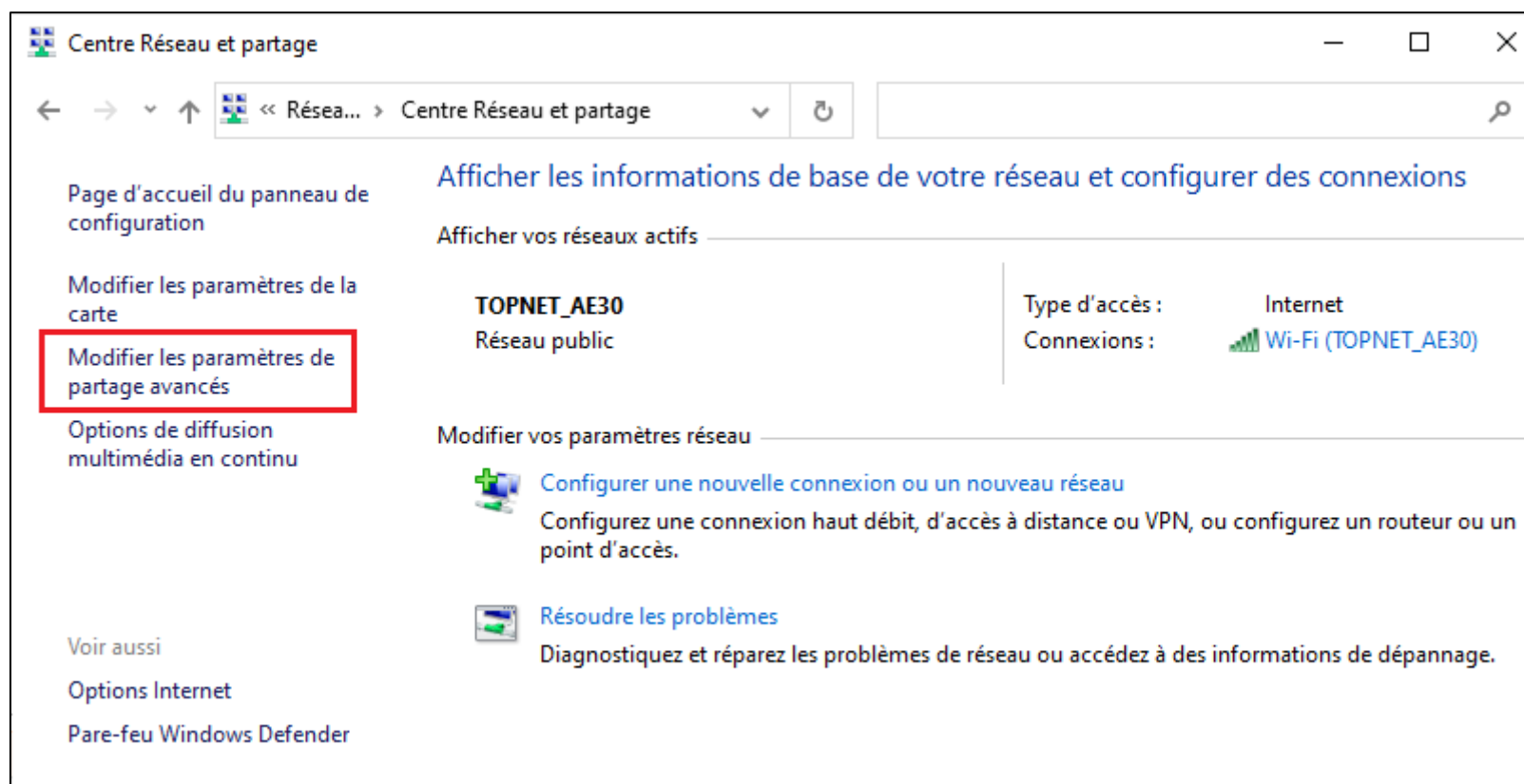


Figure 80 : Interface Centre Réseau et partage

03 – Assurer la sécurité du client Windows

Gérer les Permissions et le partage de ressources

L'utilisateur peut donc activer ou désactiver le partage de fichiers et d'imprimantes, comme il peut activer ou désactiver la découverte de réseau (voir la **Figure 82**). Maintenant pour partager un fichier sauvegardé dans n'importe quel endroit dans son ordinateur, l'utilisateur doit sélectionner le fichier qu'il souhaite partagé et cliquer sur le bouton de droite puis choisir l'onglet partager (voir **Figure 81 (a)**).

L'interface de la **Figure 81 (b)** s'affiche.

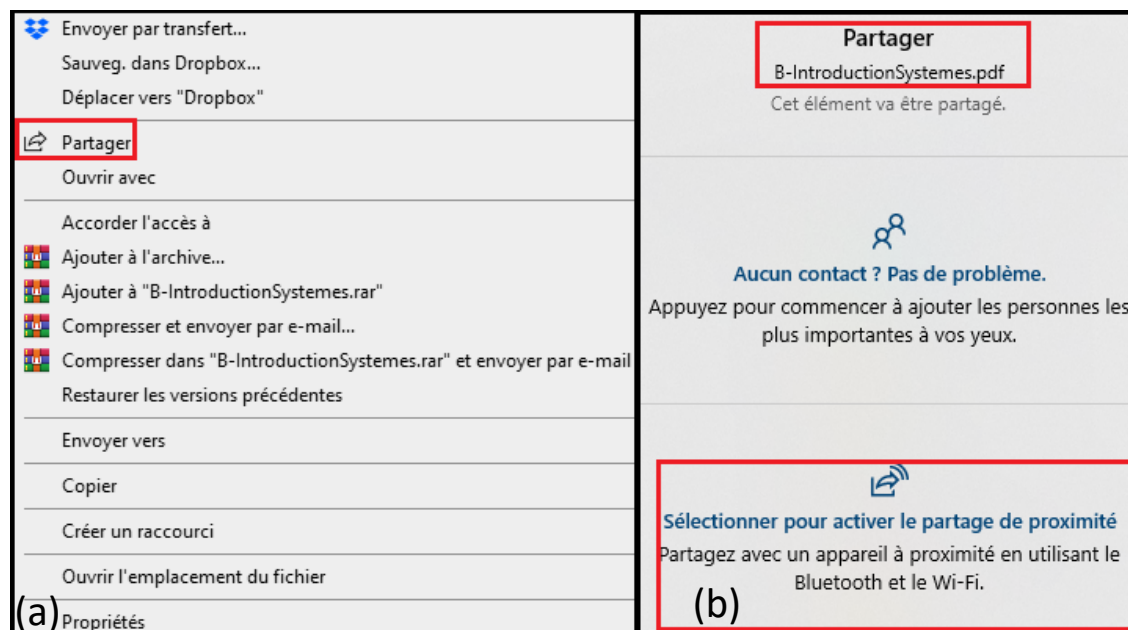


Figure 81: Interface partager

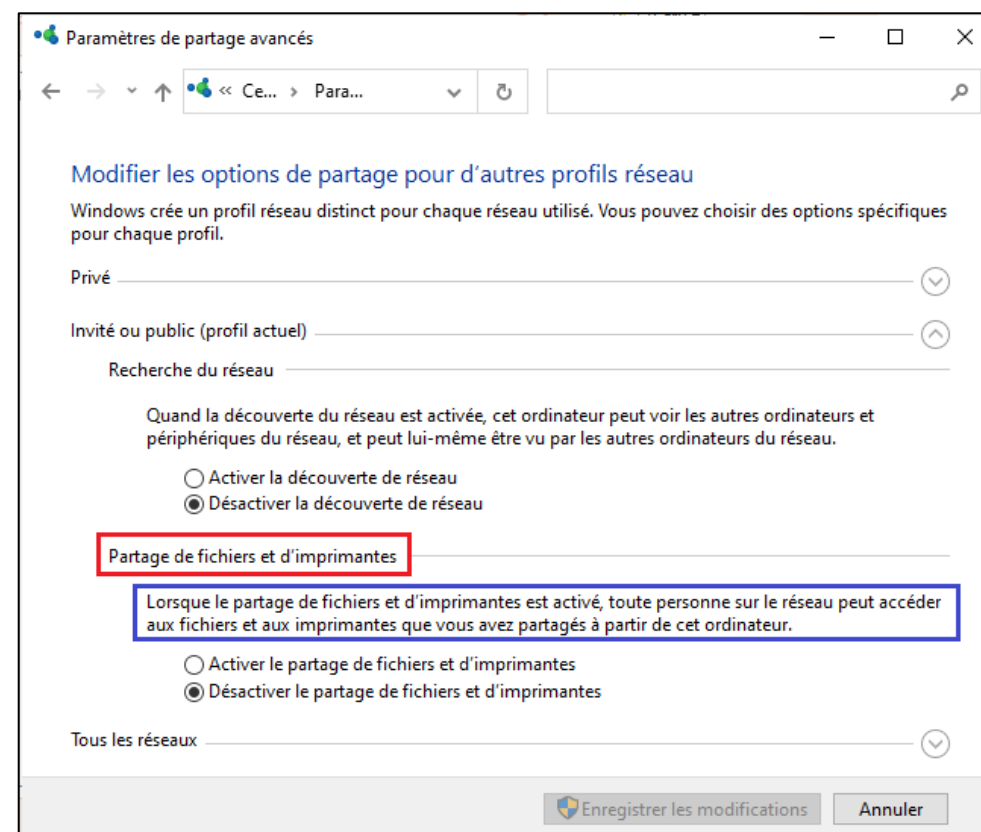


Figure 82 : Interface Paramètre de partage avancé

CHAPITRE 3

ASSURER LA SÉCURITÉ DU CLIENT WINDOWS

1. Gérer l'authentification dans Windows
2. Gérer les permissions et le partage de ressources
- 3. Assurer la protection, le sauvegarde et la restauration des données locales**
4. Gérer les outils de sécurité sous Windows



03 – Assurer la sécurité du client Windows

Protection, sauvegarde et restauration des données locales



Data Protection Manager :

C'est un outil qui assure la protection et la récupération de données d'entreprise de Microsoft System Center.

En particulier, il assure les fonctionnalités suivantes :

- Centralisation de la sauvegarde ;
- Planification de la sauvegarde ;
- Sauvegarde dans le Cloud.

03 – Assurer la sécurité du client Windows

Protection, sauvegarde et restauration des données locales



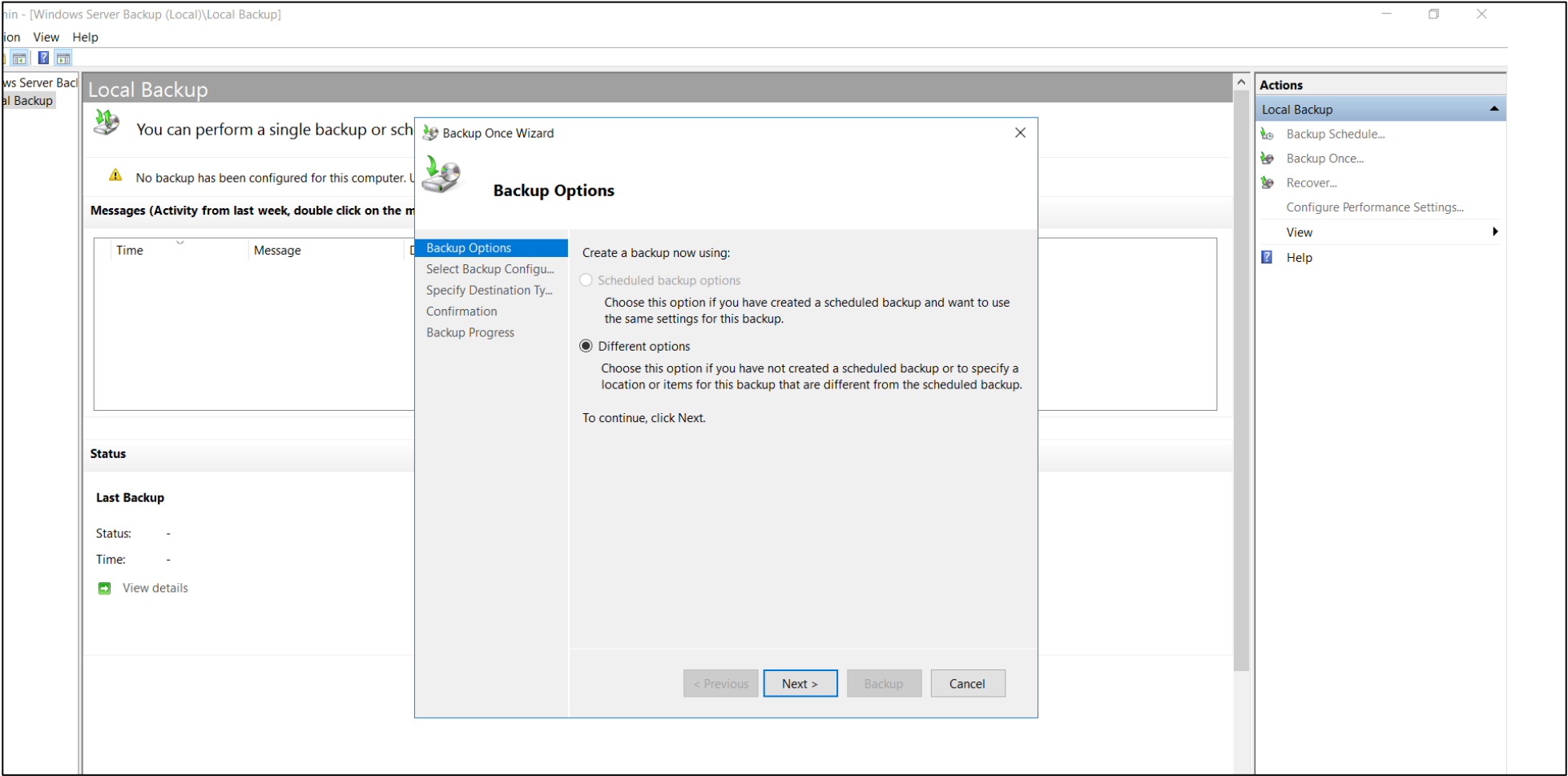
L'Assistant de récupération de la Sauvegarde Windows offre plusieurs options :

- **Destination de récupération.** Dans l'option Destination de récupération, l'utilisateur spécifie l'emplacement de la sauvegarde.
- **Résolution des conflits.** La restauration de données à partir d'une sauvegarde crée fréquemment des conflits avec des versions existantes des données. En cas de conflit, il est possible de choisir l'une des options suivantes :
 - Créer des copies et conserver les deux versions ;
 - Remplacer la version existante par la version récupérée ;
 - Ne pas récupérer les éléments s'ils existent déjà dans l'emplacement de récupération.
- **Paramètres de sécurité.** Cette option est utilisée pour restaurer des autorisations aux données en cours de récupération.

Voir les différentes Figures des diapos 175, 176, 177 et 178 décrivant les étapes de sauvegarde et de restauration des données locales.

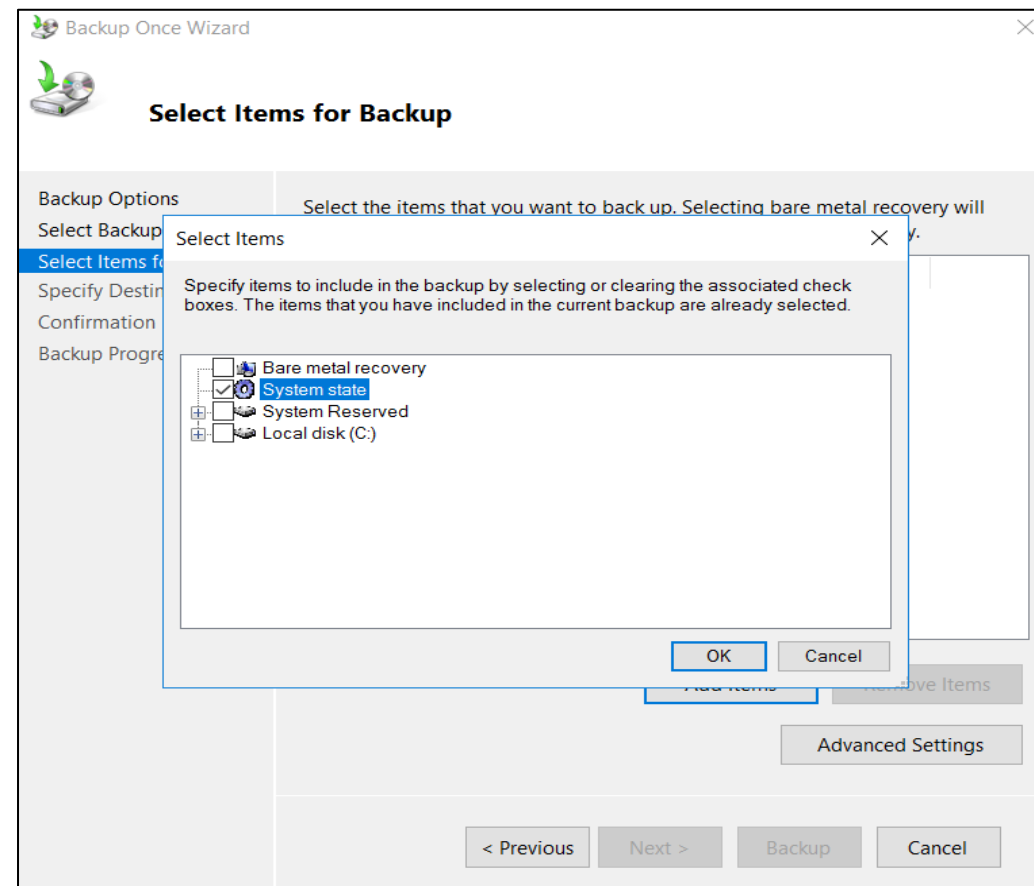
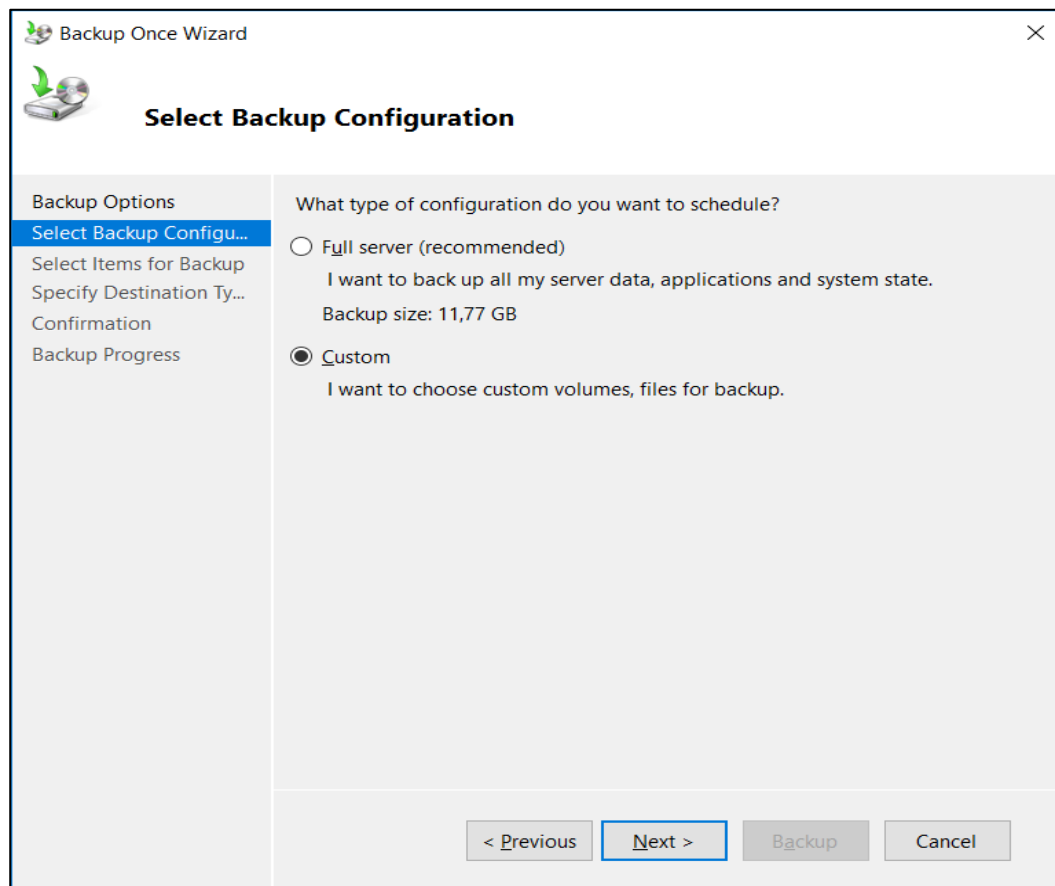
03 – Assurer la sécurité du client Windows

Protection, sauvegarde et restauration des données locales



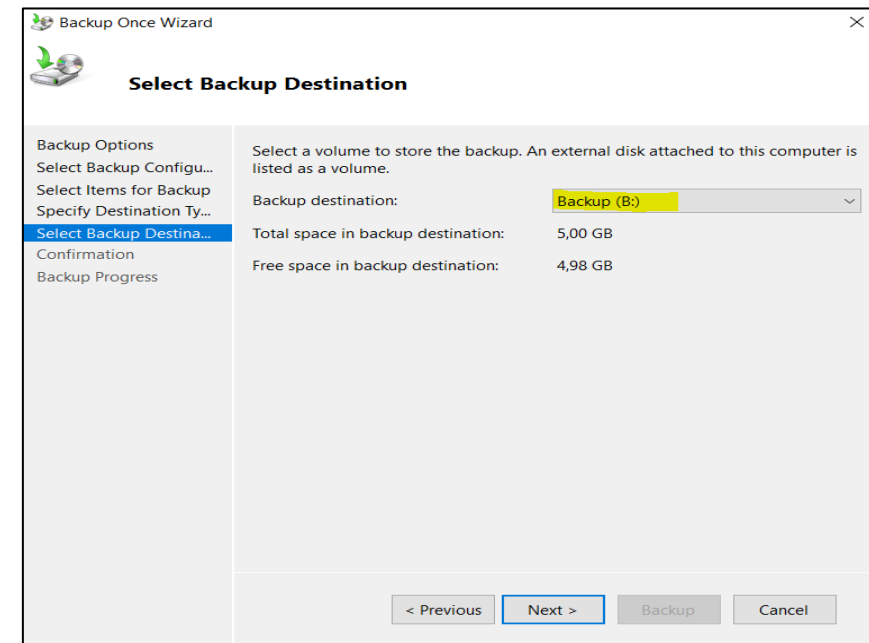
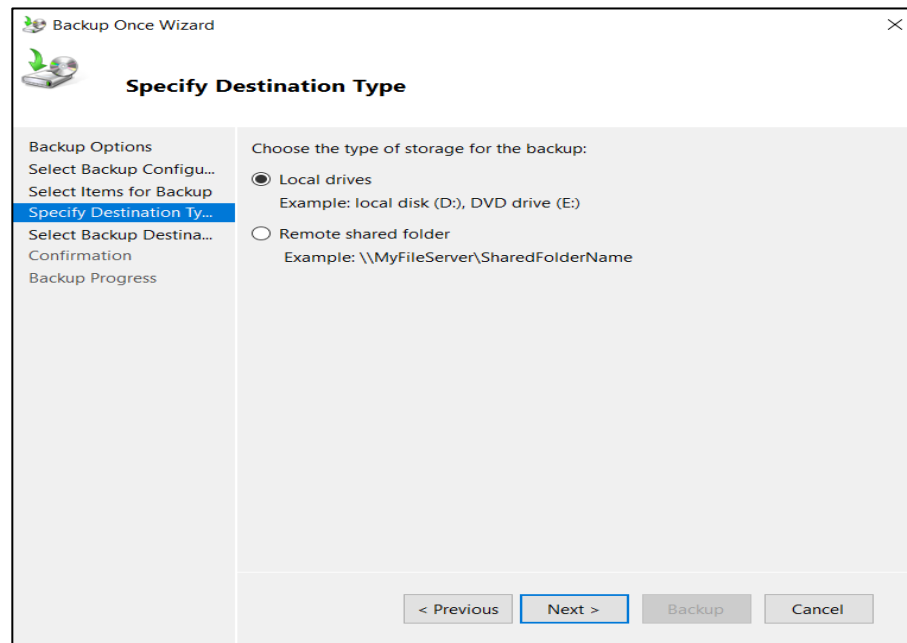
03 – Assurer la sécurité du client Windows

Protection, sauvegarde et restauration des données locales



03 – Assurer la sécurité du client Windows

Protection, sauvegarde et restauration des données locales



03 – Assurer la sécurité du client Windows

Protection, sauvegarde et restauration des données locales



Backup Once Wizard

Backup Progress

Backup Options

Select Backup Configu...

Select Items for Backup

Specify Destination Ty...

Select Backup Destina...

Confirmation

Backup Progress

Status: 29 % of backup completed for System Writer...

Status details

Backup location: B:

Data transferred: 2,35 GB

Items

Item	Status	Data transferred
System state	29 % of backup...	2,35 GB of 8,07 ...

You may close this wizard and the backup operation will continue to run in the background.

< Previous

Next >

Close

Cancel

CHAPITRE 3

ASSURER LA SÉCURITÉ DU CLIENT WINDOWS

1. Gérer l'authentification dans Windows
2. Gérer les permissions et le partage de ressources
3. Assurer la protection, le sauvegarde et la restauration des données locales
4. **Gérer les outils de sécurité sous Windows**



03 – Assurer la sécurité du client Windows

Gérer les outils de sécurité sous Windows



Windows offre un ensemble d'outils de sécurité, qui permettent à l'utilisateur de s'assurer de la sécurité et de la protection de son système et de ses fichiers contre les intrusions et les virus.

On va se concentrer sur l'outil Pare-feu Windows Defender fourni par Windows qui a pour but d'empêcher les pirates ou les logiciels malveillants d'accéder à l'ordinateur via Internet ou un réseau :

- Il améliore la sécurité de Windows ;
- Il protège le système contre les programmes malveillants ;
- La configuration des règles peut se faire manuellement ou à l'aide d'une stratégie de groupe ;
- Il présente plusieurs profils que nous pouvons appliquer à différents réseaux.

Pour ouvrir le Pare-feu Windows Defender, l'utilisateur doit aller vers le panneau de configuration, choisir Système et sécurité puis choisir Pare-feu Windows Defender (Voir la **Figure 83**).

03 – Assurer la sécurité du client Windows

Outils de sécurité sous Windows (Pare-feu, Windows Defender)

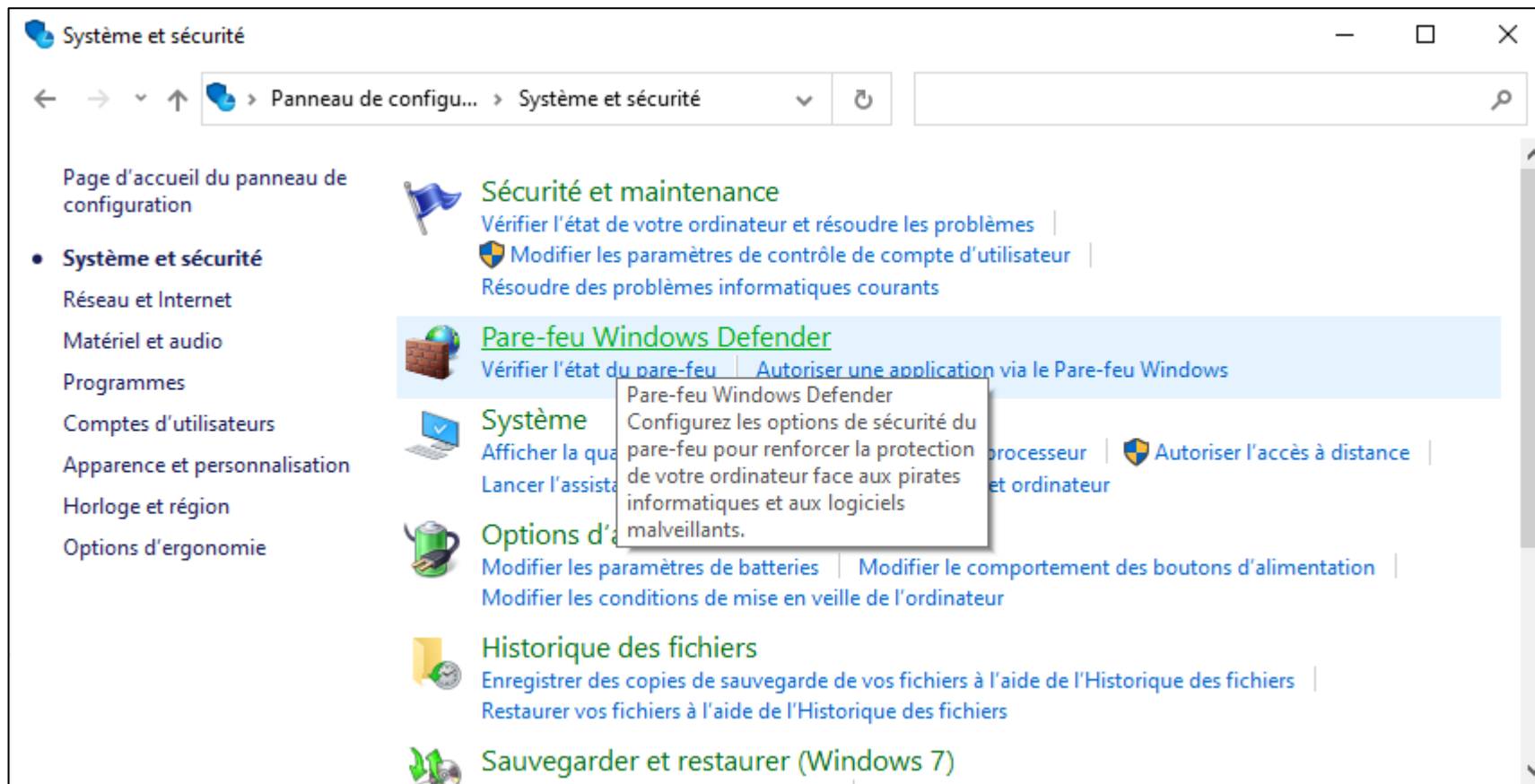


Figure 83 : Interface Système et sécurité

03 – Assurer la sécurité du client Windows

Gérer les outils de sécurité sous Windows

Comme il est illustré dans la **Figure 84**, l'outil Pare-feu Windows Defender permet à l'utilisateur d'autoriser une application ou une fonctionnalité, modifier les paramètres de notification, activer ou désactiver le pare-feu.

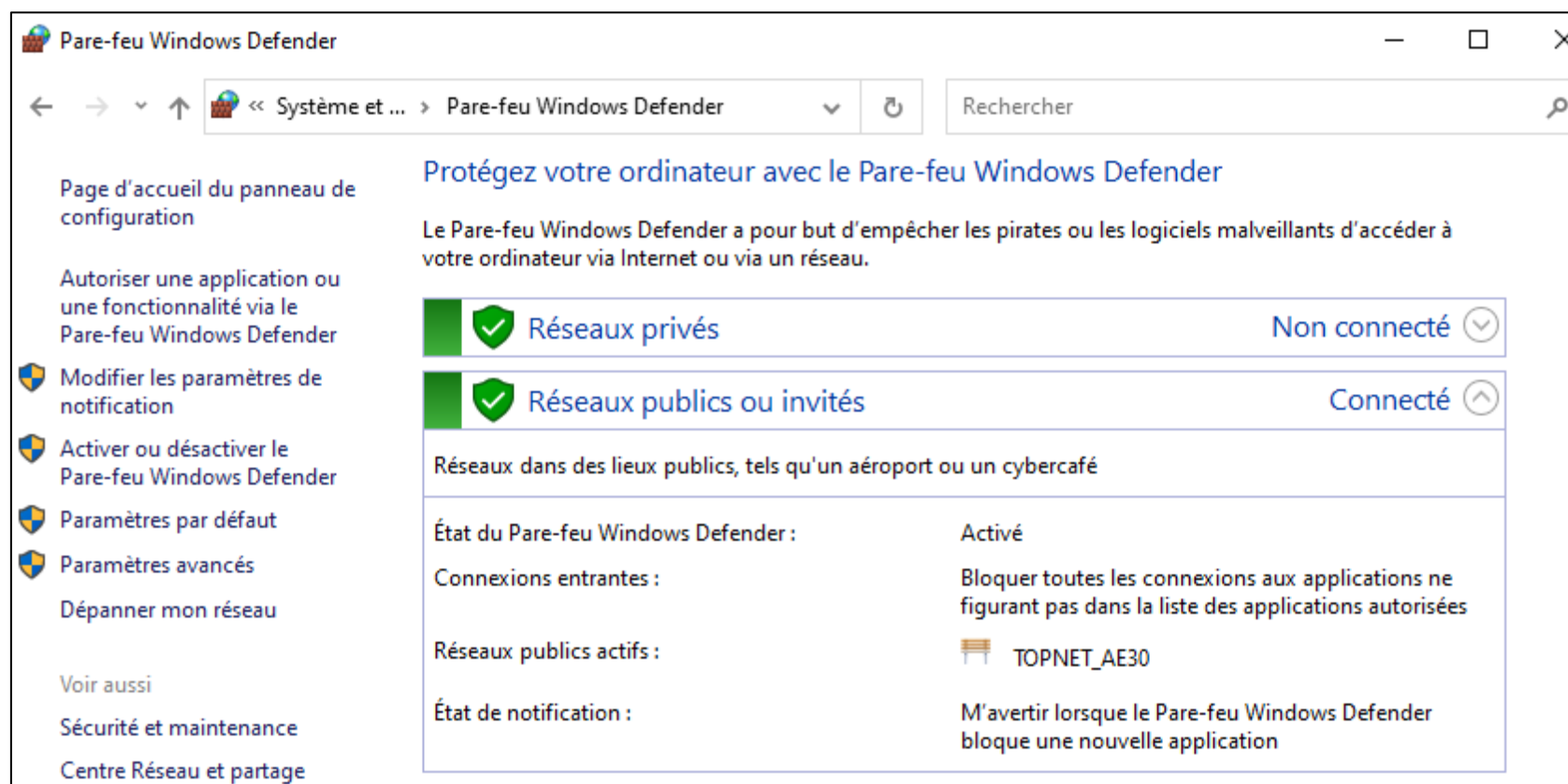


Figure 84 : Interface Pare-feu Windows Defender

03 – Assurer la sécurité du client Windows

Gérer les outils de sécurité sous Windows

Si l'utilisateur veut par exemple activer le Pare-feu, il clique sur Activer ou Désactiver, et l'interface présentée dans la **Figure 85** s'affiche.

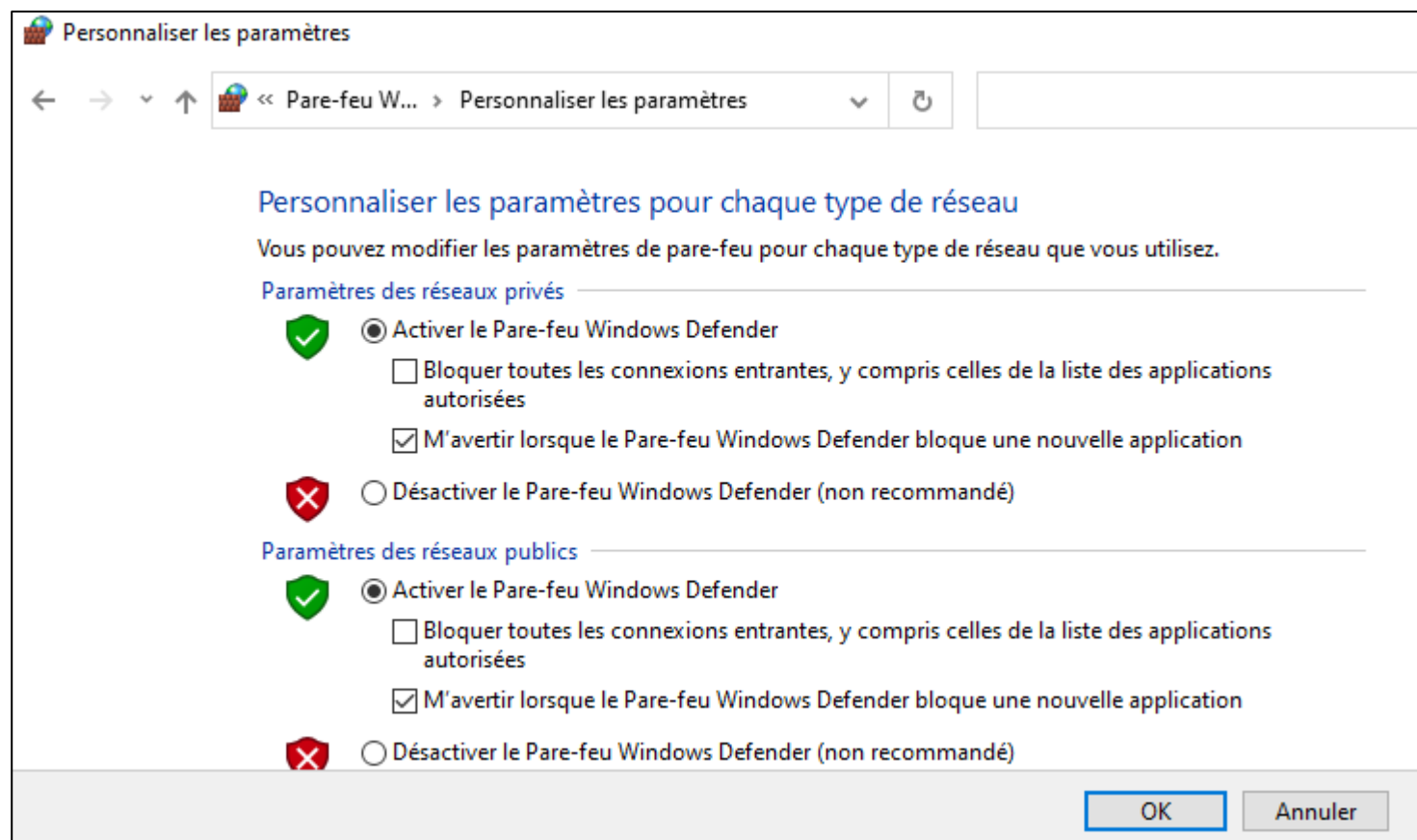


Figure 85: Interface Personnaliser les paramètres

03 – Assurer la sécurité du client Windows

Gérer les outils de sécurité sous Windows



Le suivi et le contrôle des communications initialisées par un équipement sur le réseau sont assurés par les règles de trafic. Il y'a des règles de trafic entrant et sortant.

Règles de trafic entrant :

- Dans le cas par défaut, le trafic entrant est **bloqué**.
- Les échanges qui entrent ne sont autorisés qu'à travers une règle de trafic entrant.

Règles de trafic sortant :

- Le système **autorise** toute communication sortante à l'exception du trafic qui est explicitement bloqué par une règle de trafic sortant.

03 – Assurer la sécurité du client Windows

Gérer les outils de sécurité sous Windows

Windows Defender

Il est intégré par défaut dans Windows 10, il offre un niveau de sécurité élevé en utilisant des signatures sur le cloud. Pour assurer la sécurité de son ordinateur, l'utilisateur doit ouvrir l'interface **Sécurité Windows** illustrée dans la **Figure 86**.

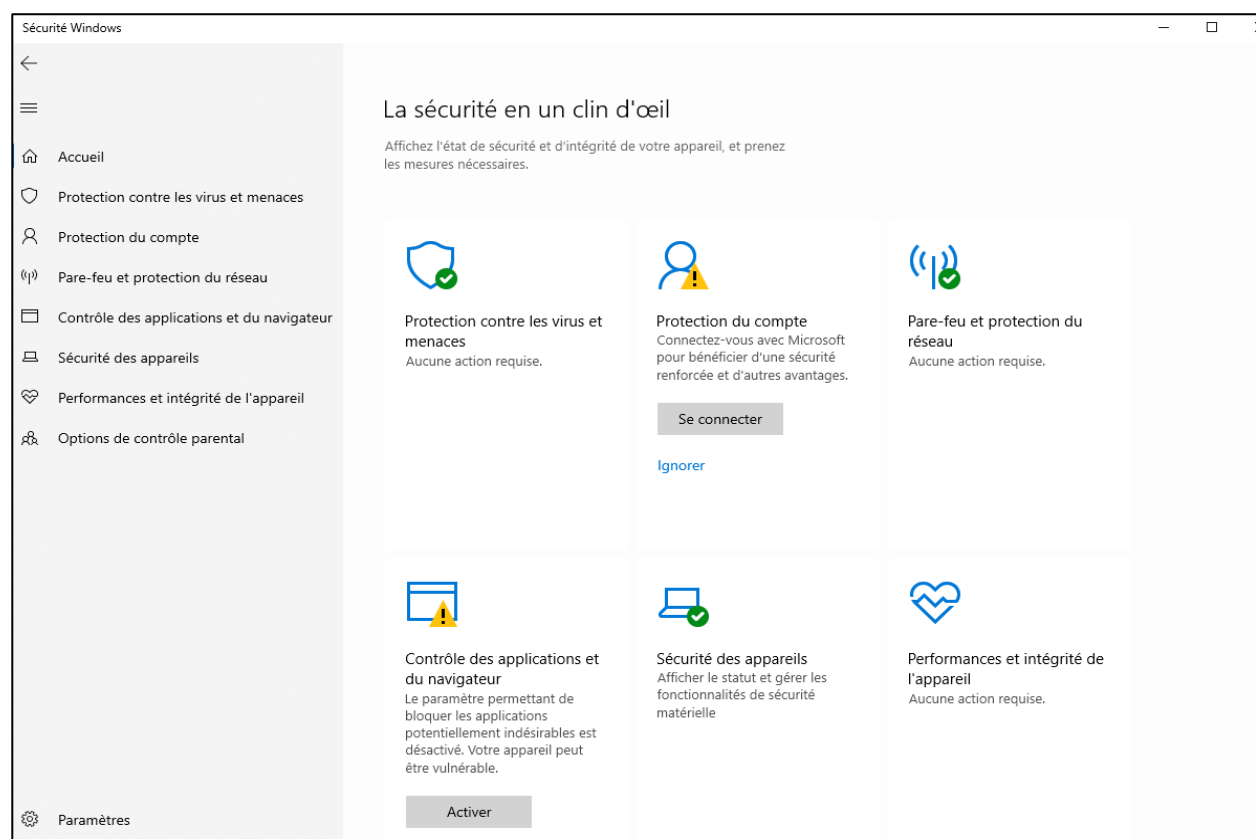


Figure 86: Interface Sécurité Windows