



# Configurer le firewall Pour MacOs Tigre

Pour plus de sécurité, adoptez les réflexes CASES !

## Table des matières

1. Définition : « FireWall »
2. Configurer le firewall pour MacOS Tigre,
3. Téléchargement et installation,
4. Quelques explications sur l'interface,
5. Détails de l'interface,
  - a) Onglet « Services »,
  - b) Onglet « Coupe-Feu »,
  - c) Onglet « Internet »,
6. Conclusion et aspects sécurité,
7. Résolution des problèmes courants,
8. Définitions secondaires.

Sécuriser le Router Thomson SpeedTouch

Les termes techniques en **rouge** au cours de ce tutoriel sont présentés en fin de document dans la rubrique « 8. Définitions secondaires ».

## 1. Définition « Firewall »

**Firewall** : Mécanisme de sécurité localisé entre une zone de confiance (réseau local ou une machine personnelle) et un réseau externe non digne de confiance (par exemple Internet). La tâche du firewall est de contrôler et de filtrer, d'accepter ou de bloquer, en fonction de règles de sécurité définies par un administrateur, les communications entrantes et sortantes passant par lui. Les firewalls peuvent être de type hardware (firewall physique) mais aussi software (notamment pour la [protection des ordinateurs personnels](#)).

## 2. Configurer le Firewall pour MacOS Tigre

Ce tutoriel permet de comprendre les bases de la configuration du firewall intégré à MacOS Tigre. Il faut cependant noter que, le firewall de MacOS Tigre ne filtre que les connexions entrantes et **laisse passer toute communication sortante**. Ce firewall n'est donc pas une protection efficace contre les Chevaux de Troie.

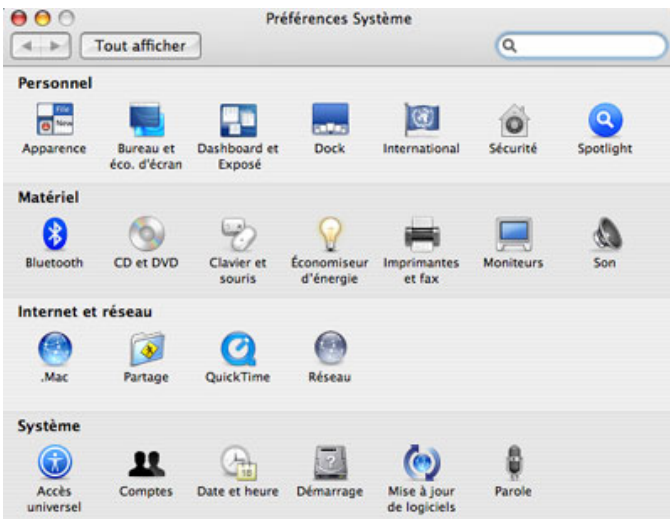
### 3. Téléchargement et installation

Un **firewall** est déjà intégré dans MacOS Tigre. Il n'y a donc aucun nouveau programme à télécharger ou à installer.

Pour activer le firewall, il suffit de se rendre dans les « **Préférences du système** », puis « **Partage** » (Fenêtre 1) et ensuite dans l'onglet « **Coupe-feu** ».



Fenêtre 1



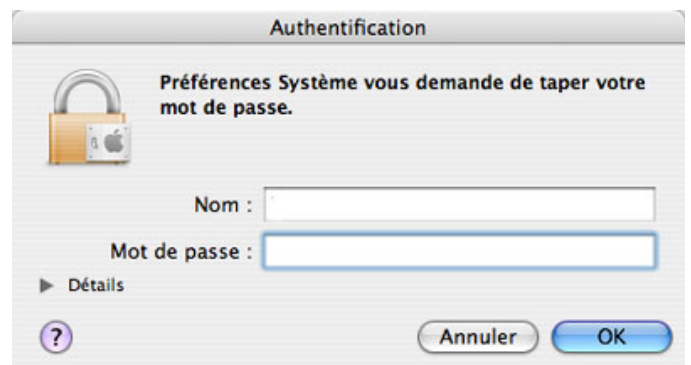
Fenêtre 2

Pour lancer le pare-feu, il suffit de cliquer sur « Démarrer » (Fenêtre 2).

(Page officielle d'Apple sur le sujet :

<http://docs.info.apple.com/article.html?path=Mac/10.4/fr/mh1042.html>)

**NB :** Il est nécessaire de s'authentifier afin de pouvoir démarrer le firewall (c'est aussi nécessaire pour sa configuration), pour cela il suffit de cliquer sur le cadenas situé en bas à gauche (de la fenêtre 2) et d'entrer le mot de passe demandé (Fenêtre 3).

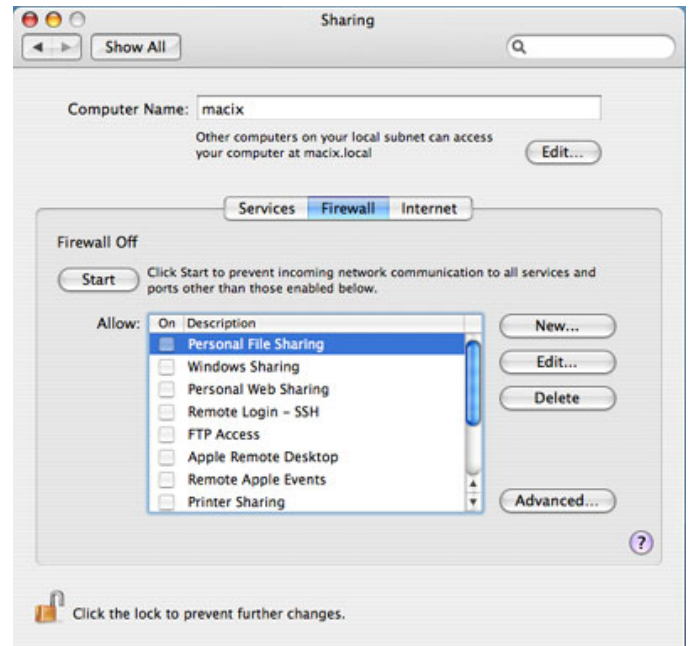


Fenêtre 3

## 4. Quelques explications sur l'interface

Le panneau de contrôle « Partage » comporte 3 onglets : « Services », « Coupe-feu » et « Internet ». Ces 3 panneaux seront détaillés dans la partie suivante.

Dans le firewall de MacOS Tigre, pour gérer les connexions de certains programmes ou services, comme par exemple **FTP (File Transfer Protocol)**, il suffit d'activer le service associé. Si le service est démarré, le firewall est automatiquement configuré pour autoriser les connexions en ouvrant les **ports** nécessaires. Si le service est désactivé ou fermé, les ports associés sont automatiquement fermés pour des raisons de sécurité. De fait il n'est pas possible de modifier ces ports manuellement (Fenêtre 4).



Fenêtre 4

## 5. Détails de l'interface

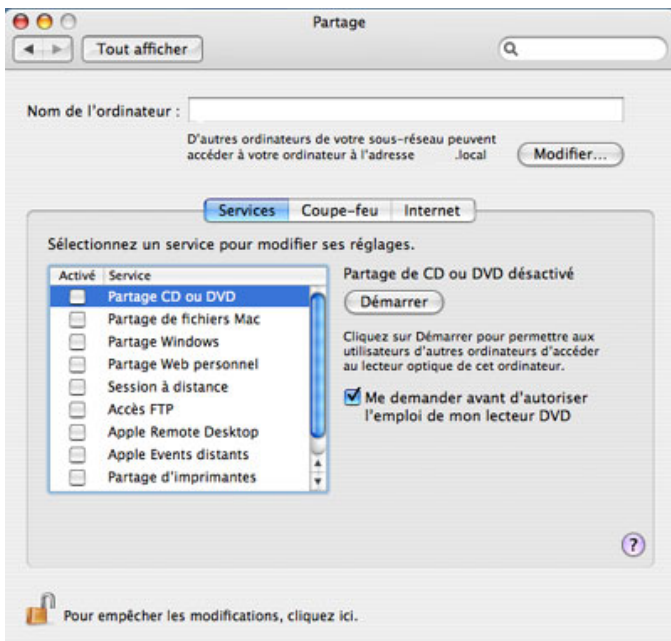
### a. Onglet « Services »

Cet onglet (Fenêtre 5) permet d'activer ou de désactiver les différents services de partage réseau de MacOS Tigre. C'est ici que l'on peut configurer le partage de fichiers par FTP, le partage des imprimantes et d'autres services similaires...

Pour activer un service, il suffit de sélectionner son nom dans la liste et de cliquer sur « Démarrer » à droite de la liste.

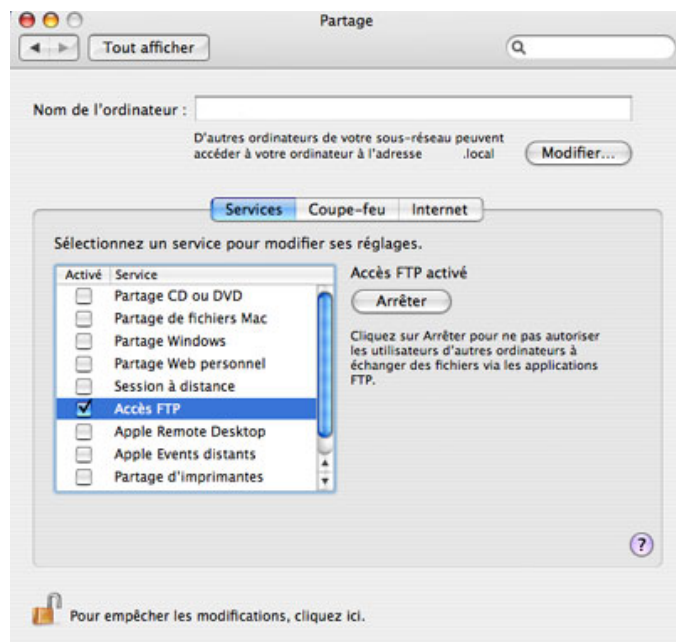
Pour arrêter un service, il suffit de sélectionner son nom dans la liste et de cliquer sur « Stop » à droite de la liste.

Le firewall de MacOS Tigre se charge ensuite de gérer automatiquement l'ouverture et la fermeture des ports associés aux services que l'on demande respectivement d'ouvrir ou de fermer.



Fenêtre 5

Pour connaître les services activés, il suffit de vérifier ceux qui sont « cochés » dans la liste (Fenêtre 6).



Fenêtre 6

## b) Onglet « Coupe-feu »

Cet onglet (Fenêtre 7) permet d'ouvrir ou de fermer des ports pour chacun des programmes de MacOS Tigre.

Comme expliqué précédemment, certains ports sont gérés par l'onglet « Services ».



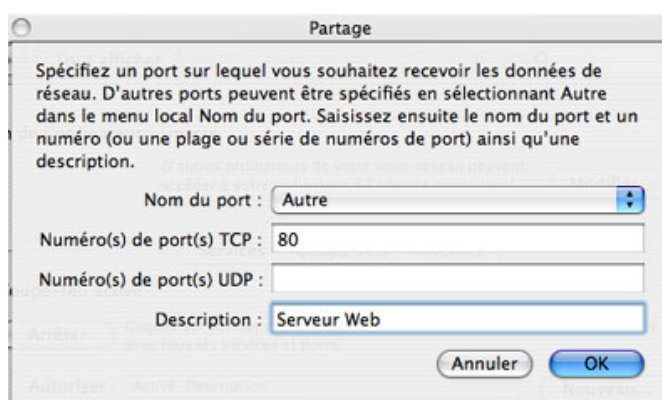
Fenêtre 7

Il est ici possible de créer (Fenêtre 8 et 9), modifier (Fenêtre 10) et de supprimer des connexions vers des ports.

En cliquant sur le bouton « nouveau », un menu apparaît permettant de créer une nouvelle règle d'ouverture de port pour un programme de son choix. Il faut tout d'abord choisir le nom du port, certains noms sont prédéfinis (Fenêtre 8).



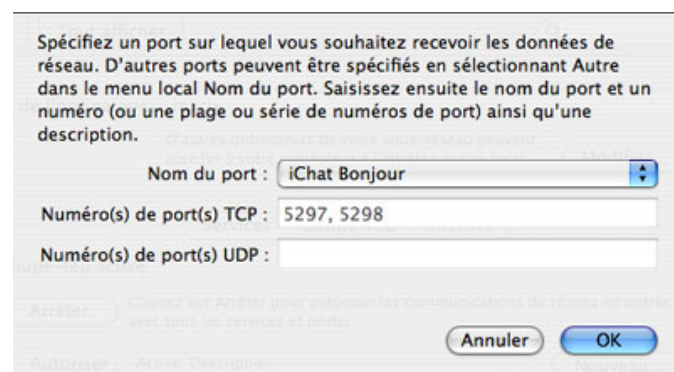
Fenêtre 8



Fenêtre 9

Rien n'empêche de créer une nouvelle connexion en mode *expert* (Fenêtre 9).

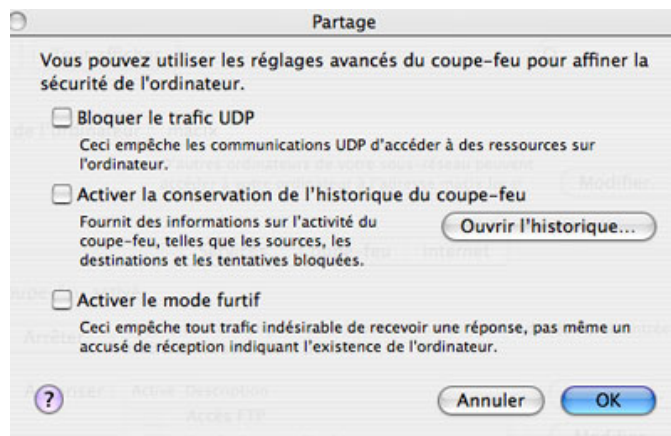
Il est évidemment possible de modifier une entrée existante (Fenêtre 10) en cliquant sur le bouton « Editer ». La modification (Fenêtre 10) fonctionne exactement comme l'ajout.



Fenêtre 10

Enfin, il est possible de changer certaines options du pare-feu en cliquant sur le bouton « Avancé » (Fenêtre 11). Ainsi il est possible de :

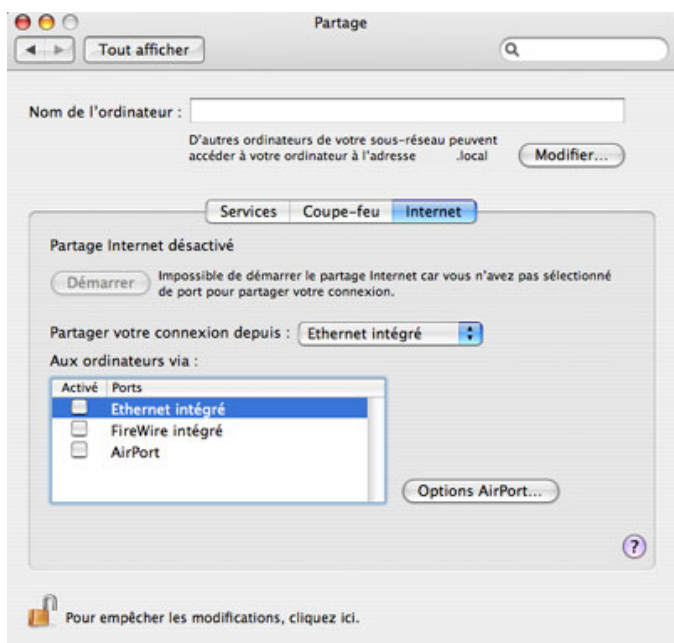
- Bloquer le trafic **UDP** afin de sécuriser les informations de l'ordinateur de l'utilisateur ainsi que de son réseau personnel,
- Activer la conservation de l'historique du coupe-feu afin de garder des traces (fichiers de logs) permettant de revoir les différentes connexions (connexions qui ont réussies ou qui ont échouées) afin de détecter des tentatives d'attaques (pour experts),
- Activer le mode *furtif* pour rendre l'ordinateur "invisible" depuis internet. Un ordinateur "invisible" permet de dissimuler la présence de l'utilisateur pour ne pas attirer l'attention et donc limiter les risques d'être la cible d'attaques.



Fenêtre 11

### c) Onglet « Internet »

Cet onglet (Fenêtre 12) permet de gérer le partage « Internet » de MacOS Tigre. C'est ici qu'il faut faire les réglages nécessaires pour permettre aux autres ordinateurs de son domicile de partager la même connexion Internet pour surfer et envoyer des e-mails.



Fenêtre 12

## 4. Conclusion et aspects sécurité

Il est important de noter que dès qu'un port est ouvert, un programme est susceptible de l'utiliser pour envoyer et recevoir des informations sur Internet. De plus, le firewall de MacOS Tigre Tiger ne filtre **que les connexions entrantes** et laisse passer toute communication sortante. Le firewall de MacOS Tigre n'est pas une protection efficace contre les Chevaux de Troie.

## 5. Résolution des problèmes courants

**J'ai un programme qui communique sur Internet. Il fonctionnait parfaitement jusqu'au jour où j'ai activé le pare-feu de MacOS Tigre, maintenant il ne fonctionne plus :**

- Si le programme est prédéfini dans le firewall intégré de MacOS Tigre, il suffit de procéder à l'ajout d'un programme (voir plus haut).
- Si le programme n'est pas dans la liste, alors il est nécessaire de savoir quel est le port utilisé par celui-ci. Si le programme nécessite un port particulier, cela doit être précisé dans l'aide, il suffira alors de procéder à l'ajout d'un nouveau programme en spécifiant le port utilisé.

## 1. Définitions secondaires

**FTP (File Transfer Protocol)** : Protocole de transfert (envoi ou réception) de fichiers entre deux machines. Le protocole FTP est notamment utilisé sur internet pour mettre à jour les sites web.

**IANA**: IANA signifie *Internet Assigned Numbers Authority*. Il s'agit de l'autorité de gestion et d'attribution des adresses IP, des numéros de [ports de communication](#) aux services, des noms de domaines racines, etc.

**Port (de communication)** : Numéro spécifique normalisé par l' [IANA](#) et attribué à un service particulier sur un réseau d'information et de communication selon la règle qu'à un port correspond un type d'application. Le couple constitué d'une adresse IP associée à un numéro de port permet de spécifier toute application qui fonctionne sur toute [machine](#). Le port est lié à la couche Transport du modèle [OSI](#), il a été normalisé 65536 ports différents puisque la valeur de chaque port est codée sur 16 bits soit  $2^{16} = 65536$  ports différents possibles, répartis de la manière suivante :

- Les ports 0 à 1023 sont les *ports reconnus* ou *réservés* (*Well Known Ports*). Ils sont, de manière générale, réservés aux processus système (démons) ou aux programmes exécutés par des utilisateurs privilégiés. Un administrateur réseau peut néanmoins lier des services aux ports de son choix.
- Les ports 1024 à 49151 sont appelés «ports enregistrés» (*Registered Ports*).
- Les ports 49152 à 65535 sont les «ports dynamiques et/ou privés» (*Dynamic and/or Private Ports*).

Par exemple : port 80 = HTTP pour les pages web, port 25 = SMTP pour les mails, port 21 = FTP pour le transfert de fichiers. Ces derniers font partie des *ports réservés* et sont quelques uns des ports et services les plus connus et utilisés sur [internet](#).

**UDP (User Datagram Protocol)** : Protocole réseau de communication en mode non connecté du niveau Transport du modèle [OSI](#) utilisé pour les transferts rapides de données. L'échange n'est pas sécurisé et UDP n'assure pas les contrôles offerts par [TCP](#) principalement ceux concernant la garantie que tous les paquets émis soient bien arrivés au destinataire.

**TCP (Transmission Control Protocol)** : Protocole réseau de communication en mode connecté du niveau Transport du modèle [OSI](#) répondant à un certain nombre de critères, notamment au niveau du contrôle des erreurs de transmission de données et l'assurance de la transmission de l'ensemble des paquets devant être transmis. TCP assure des services que n'assure pas [UDP](#).

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)