matériel

Sécurité du réseau

Voici comment protéger votre réseau domestique contre les cyberattaques et les utilisateurs non autorisés en utilisant trois fonctions de sécurité réseau.

Vous pouvez protéger votre réseau domestique :

avec la protection DoS, contre les attaques DoS (Denial of Service) qui inondent votre réseau avec des requêtes serveur

avec le contrôle d'accès, qui bloque ou autorise l'accès à votre réseau à des clients spécifiques

ou en empêchant l'usurpation d'identité ARP et les attaques ARP qui utilisent les liaisons IP & MAC.

Protection de réseau contre les cyberattaques

Le pare-feu SPI peut empêcher les cyberattaques et valider le trafic qui transite par le routeur en fonction du protocole.

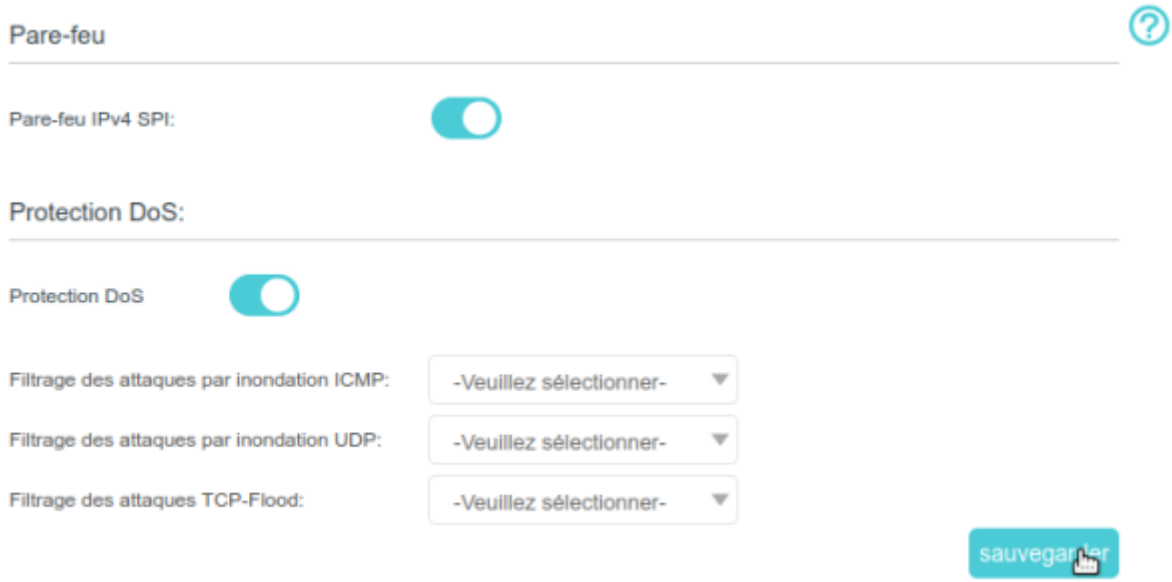
Cette fonction est activée par défaut et il est recommandé de conserver les paramètres par défaut.

La protection DoS peut protéger votre réseau domestique contre les attaques DoS qui inondent votre réseau de requêtes serveur.

Suivez les étapes ci-dessous pour configurer le pare-feu et la protection DoS.

Connectez-vous sur http://tplinkmodem.net avec le mot de passe du routeur.

Onglet **Avancée**, **Sécurité > Pare-feu et protection DoS** (à gauche)



Activez **Pare-feu IPv4 SPI**.

Activez **Protection DoS**. **Remarque** : **Protection DoS** nécessite d'activer aussi **Surveillance du trafic** dans **Outils système > Moniteur de trafic** (à gauche).

Définissez le niveau de protection (faible, moyen ou élevé) pour :
Filtrage des attaques par inondation ICMP : pour empêcher l'attaque par inondation ICMP (Internet Control Message Protocol)

Filtrage des attaques par inondation UDP : pour empêcher l'attaque par inondation UDP (User Datagram Protocol)

Filtrage des attaques TCP-Flood : pour empêcher l'attaque par inondation TCP-SYN (Transmission Control Protocol-Synchronize).
Conseils : Le niveau de protection est basé sur le trafic en nombre de paquets. La protection se déclenche immédiatement lorsque le nombre de paquets dépasse la valeur seuil définie dans la section **Paramètres de niveau de protection Dos** plus bas dans la même page ; l'hôte dangereux s'affiche dans la liste des hôtes DoS bloqués.

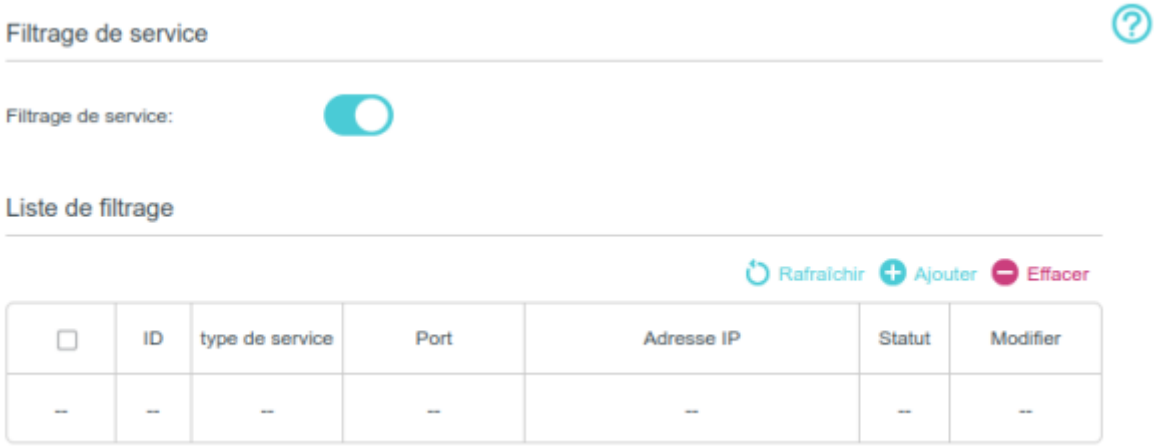
4. **Cliquez sur** **Sauvegarder**

Filtrage des services

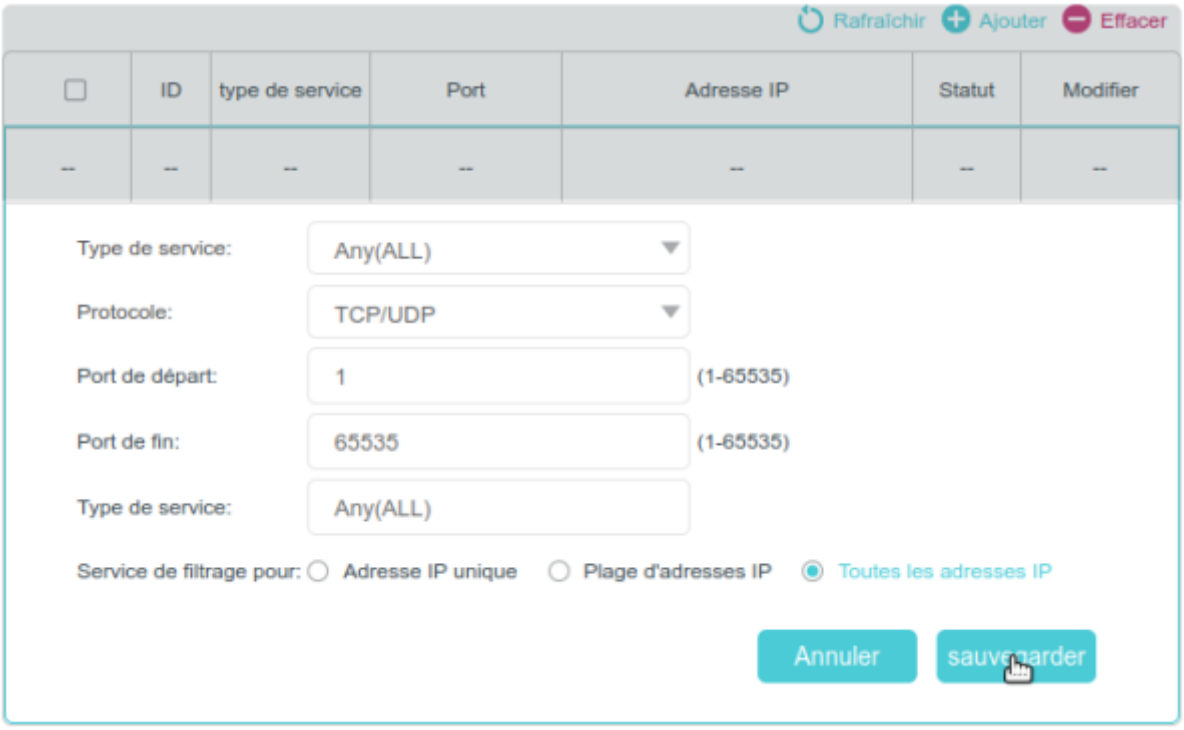
Avec le filtrage des services, vous pouvez empêcher certains utilisateurs d'accéder au service spécifié, voire bloquer complètement l'accès Internet.

Connectez-vous sur http://tplinkmodem.net avec le mot de passe du routeur.

Onglet **Avancée**, **Sécurité > Filtrage de service**, activez **Filtrage de service**



Dans la **Liste de filtrage**, Cliquez sur **Ajouter**.



Type de service : Sélectionnez un type de service dans la liste déroulante → les quatre champs suivants seront automatiquement renseignés. Si le type de service souhaité n'est pas répertorié, sélectionnez **Personnalisé** et saisissez les informations manuellement.

Service de filtrage pour : Spécifiez la ou les adresses IP auxquelles cette règle de filtrage s'appliquera.

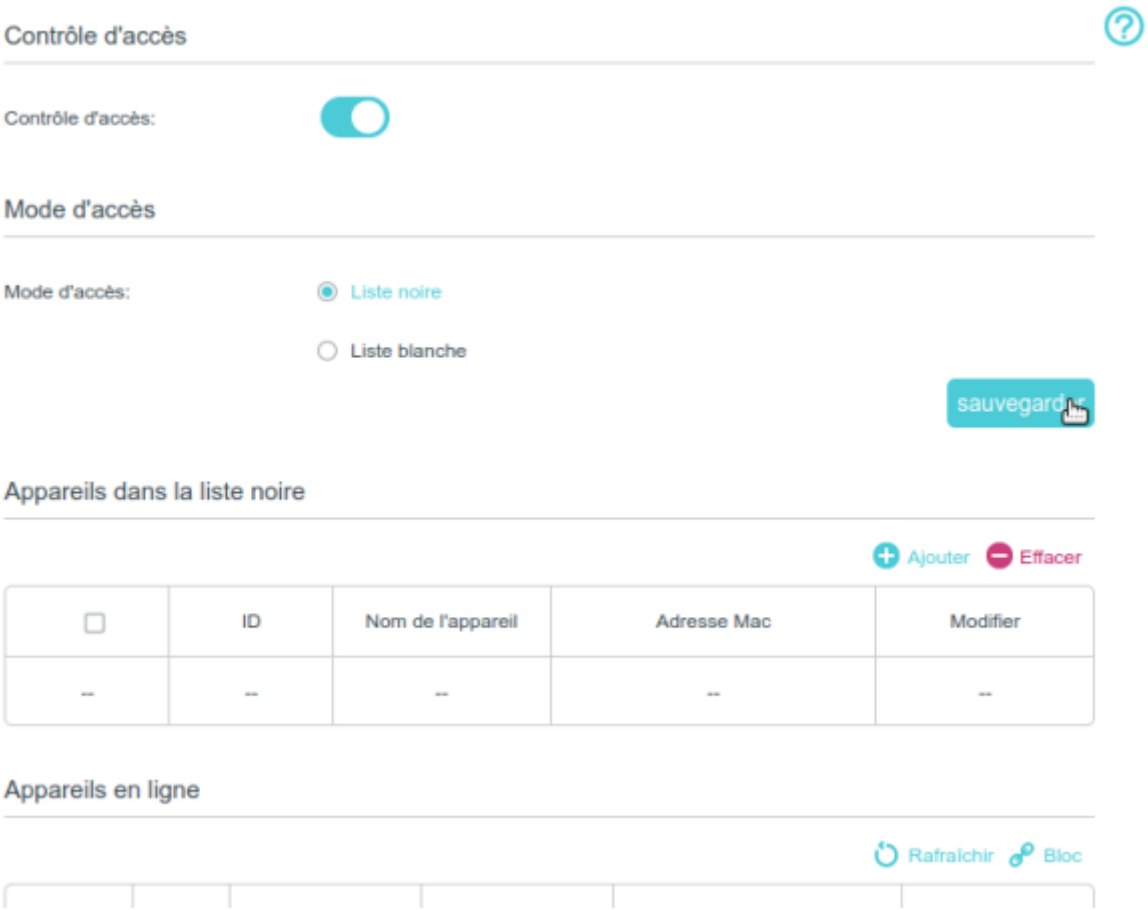
Cliquez sur Sauvegarder.

Contrôle d'accès

Le contrôle d'accès bloque ou autorise des périphériques clients spécifiques à accéder à votre réseau (avec ou sans fil) d'après une liste de périphériques bloqués (liste noire) ou une liste de périphériques autorisés (liste blanche).

Connectez-vous sur http://tplinkmodem.net avec le mot de passe du routeur.

Onglet **Avancée**, **Sécurité > Contrôle d'accès**, activez **Contrôle d'accès**



Pour bloquer un ou plusieurs appareils :
Mode d'accès : *Liste noire* (recommandé) pour bloquer les périphériques dans la liste.

cliquez sur Sauvegarder

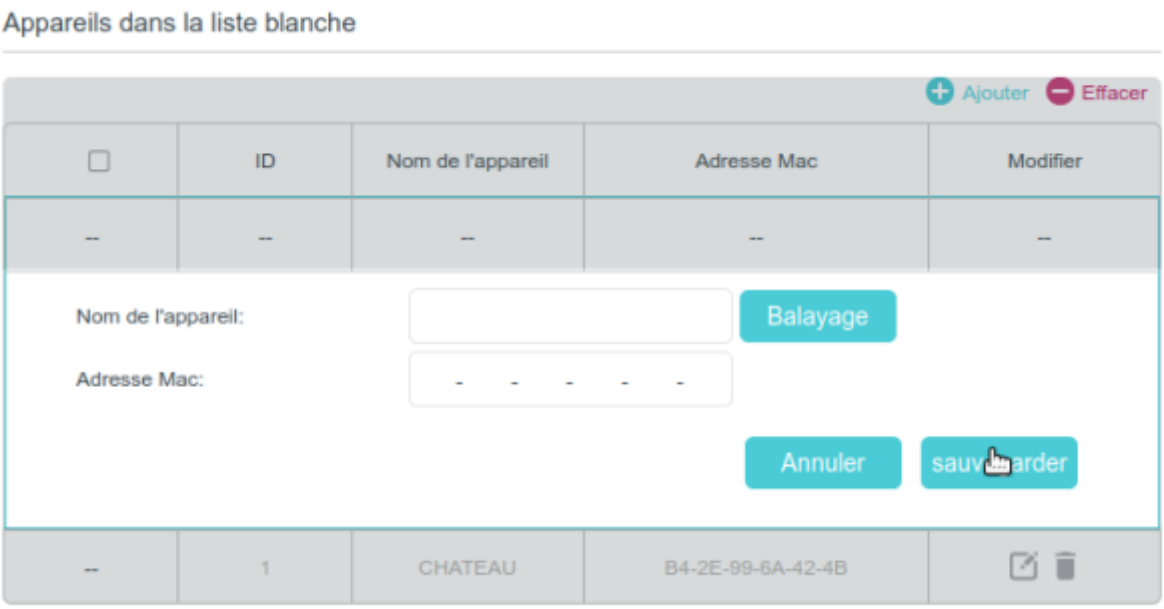
Sélectionnez le ou les appareils à bloquer dans le tableau Appareils en ligne.

Cliquez sur **Bloc** au-dessus du tableau Appareils en ligne. Les appareils sélectionnés seront automatiquement ajoutés aux appareils de la liste noire.

2. Pour autoriser un ou plusieurs appareils :
Mode d'accès : *Liste blanche* pour autoriser les périphériques dans la liste.

cliquez sur Sauvegarder

Cliquez sur **Ajouter** :



Saisissez le nom et l'adresse MAC de l'appareil (vous pouvez vous aider du bouton Balayage si l'appareil est connecté à votre réseau) et cliquez sur Sauvegarder

Vous pouvez désormais bloquer ou autoriser des périphériques clients spécifiques à accéder à votre réseau (par câble ou sans fil) à l'aide de la liste noire ou de la liste blanche.

Liaison IP et MAC

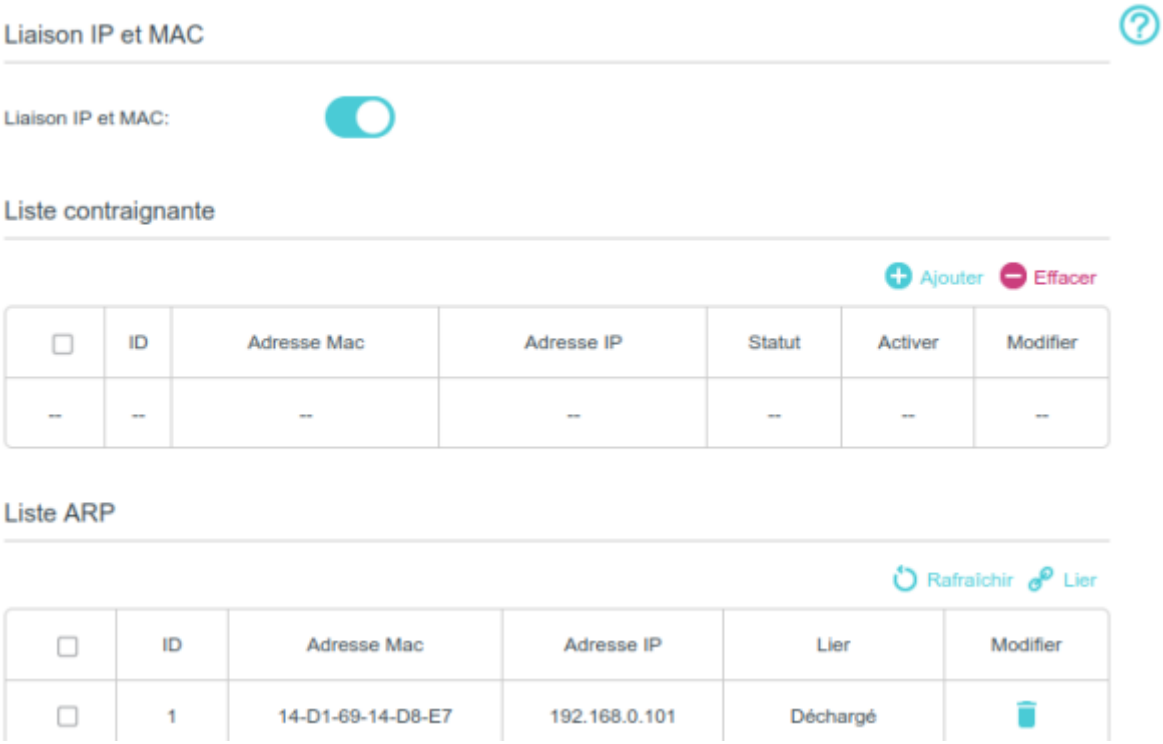
La liaison IP et MAC, (ARP = Address Resolution Protocol), lie l'adresse IP du périphérique réseau à son adresse MAC.

Elle empêche l'usurpation d'identité ARP et d'autres attaques ARP en refusant l'accès réseau à un périphérique dont l'adresse IP correspond dans la liste de liaison, mais dont l'adresse MAC n'est pas reconnue.

Pour cela :

Connectez-vous sur http://tplinkmodem.net avec le mot de passe du routeur.

Onglet **Avancée**, **Sécurité > Liaison IP et MAC** : activez **liaison IP et MAC**.



Liez votre ou vos appareils selon vos besoins :
Pour lier un appareil connecté :
Sélectionnez le ou les appareils à lier dans la liste ARP.

Cliquez sur **Lier** pour ajouter à la liste de liaison.

2. Pour lier un appareil non connecté :
Cliquez sur **Ajouter**.

MAC Ajouter : Saisissez l'adresse MAC à lier.

Adresse IP : Saisissez l'adresse IP à lier

Cochez **Activer l'entrée** et cliquez sur Sauvegarder

Désormais, vous n'avez plus à vous soucier de l'usurpation d'identité ARP et d'autres attaques ARP.

Voir aussi

- **(en)** //www.tp-link.com/us/user-guides/Archer-MR400_V3/

Basé sur « Archer MR400 V3 User Guide » par tp-link.com.

From:
https://www.nfrappe.fr/doc-0/ - **Documentation du Dr Nicolas Frappé**

Permanent link:
https://www.nfrappe.fr/doc-0/doku.php?id=materiel:internet:routeur4g:mr400:uguide:security:start

Last update: **2022/08/13 22:36**