matériel

Redirection NAT

La fonction NAT (Network Address Translation) du routeur permet aux appareils du réseau local d'utiliser la même adresse IP publique pour communiquer sur Internet, ce qui protège le réseau local en masquant les adresses IP des appareils.

Cependant, cela pose également le problème que l'hôte externe ne peut pas initier une communication avec un périphérique spécifié dans le réseau local.

Avec la fonction de transfert, le routeur peut passer l'isolement de NAT et permettre aux hôtes externes sur Internet d'initier une communication avec les périphériques du réseau local, réalisant ainsi certaines fonctions spéciales.

Le routeur TP-Link comprend quatre règles de transfert. Si deux règles ou plus sont définies, la priorité de mise en œuvre de haut en bas est Serveurs virtuels, Déclenchement de port, UPnP et DMZ.

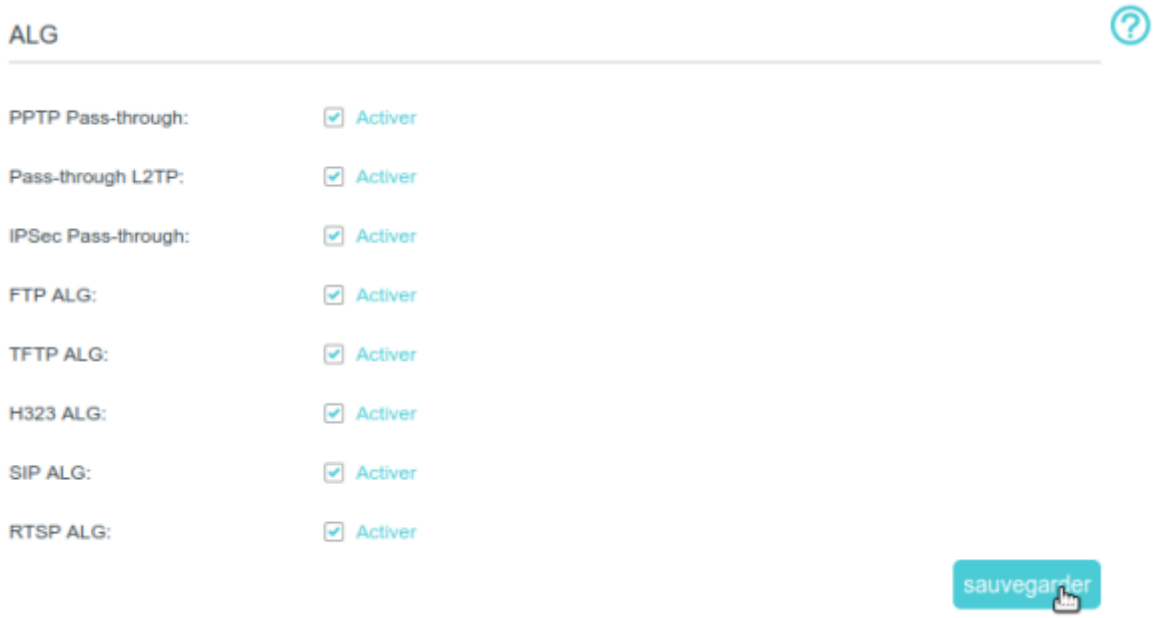
Traduire l'adresse et le port par ALG

ALG (Application Layer Gateway) permet de connecter des filtres personnalisés de transfert NAT (Network Address Translation) à la passerelle pour prendre en charge la traduction d'adresses et de ports pour certains protocoles de « contrôle/données » de la couche d'application : FTP, TFTP, H323, etc.

Il est recommandé d'activer d'ALG.

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

Accédez à **Avancé > Transmission NAT > ALG**. Il est recommandé de conserver les paramètres par défaut.



PPTP Pass-through : si activé, les sessions point à point peuvent être tunnelisées via un réseau IP

et transmises via le routeur.

Pass-through L2TP : si activé, les sessions Layer 2 point à point peuvent être tunnelisées via un réseau IP et passer par le routeur.

IPSec Pass-through : si activé, IPSec (Internet Protocol Security) peut être tunnelisé via un réseau IP et passer par le routeur. IPSec utilise des services de sécurité cryptographiques pour garantir des communications privées et sécurisées sur les réseaux IP.

FTP ALG : si activé, il permet aux clients et serveurs FTP (File Transfer Protocol) de transférer des données via NAT.

TFTP ALG : si activé, il permet aux clients et serveurs TFTP (Trivial File Transfer Protocol) de transférer des données via NAT.

H323 ALG : si activé, il permet aux clients Microsoft NetMeeting de communiquer via NAT.

SIP ALG : si activé, il permet aux clients de communiquer avec les serveurs SIP (Session Initiation Protocol) via NAT.

RTSP ALG : si activé, il permet aux clients et serveurs RTSP (Real-Time Stream Protocol) de transférer des données via NAT.

Partager des ressources locales sur Internet par serveur virtuel

Lorsque vous créez un serveur sur le réseau local et que vous souhaitez le partager sur Internet, Virtual Server peut fournir ce service aux internautes.

En même temps, le serveur virtuel protège le réseau local, car les autres services restent invisibles sur Internet.

Le serveur virtuel permet de configurer des services publics dans votre réseau local, tels que HTTP, FTP, DNS, POP3/SMTP et Telnet.

Les différents services utilisent différents ports de services : Le port 80 est utilisé pour HTTP, le port 21 pour FTP, le port 25 pour SMTP et le port 110 pour POP3.

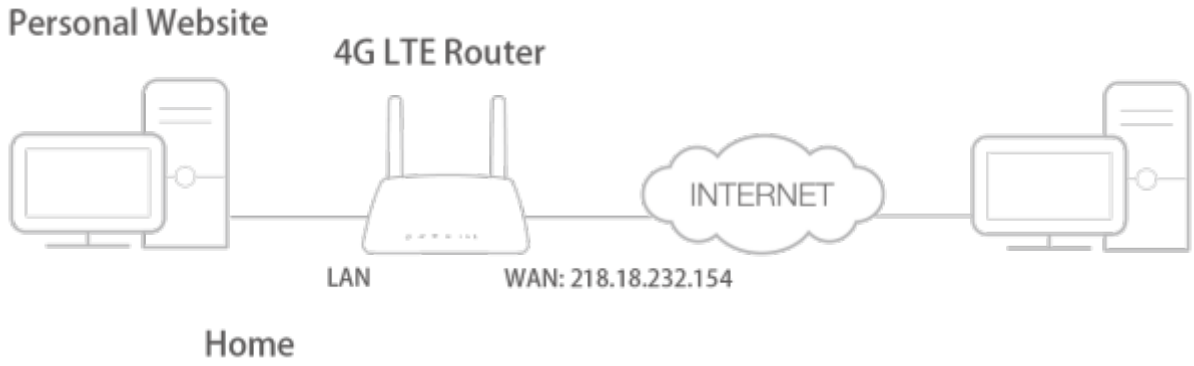
Vérifiez le numéro de port de service avant la configuration.

Il s'agit de partager avec mes amis, via Internet, mon site Web personnel construit en réseau local.

Par exemple, le site Web personnel a été intégré à mon ordinateur personnel (192.168.1.100).

J'espère que mes amis sur Internet pourront visiter mon site Web.

Le PC est connecté au routeur avec l'adresse IP WAN 218.18.232.154.

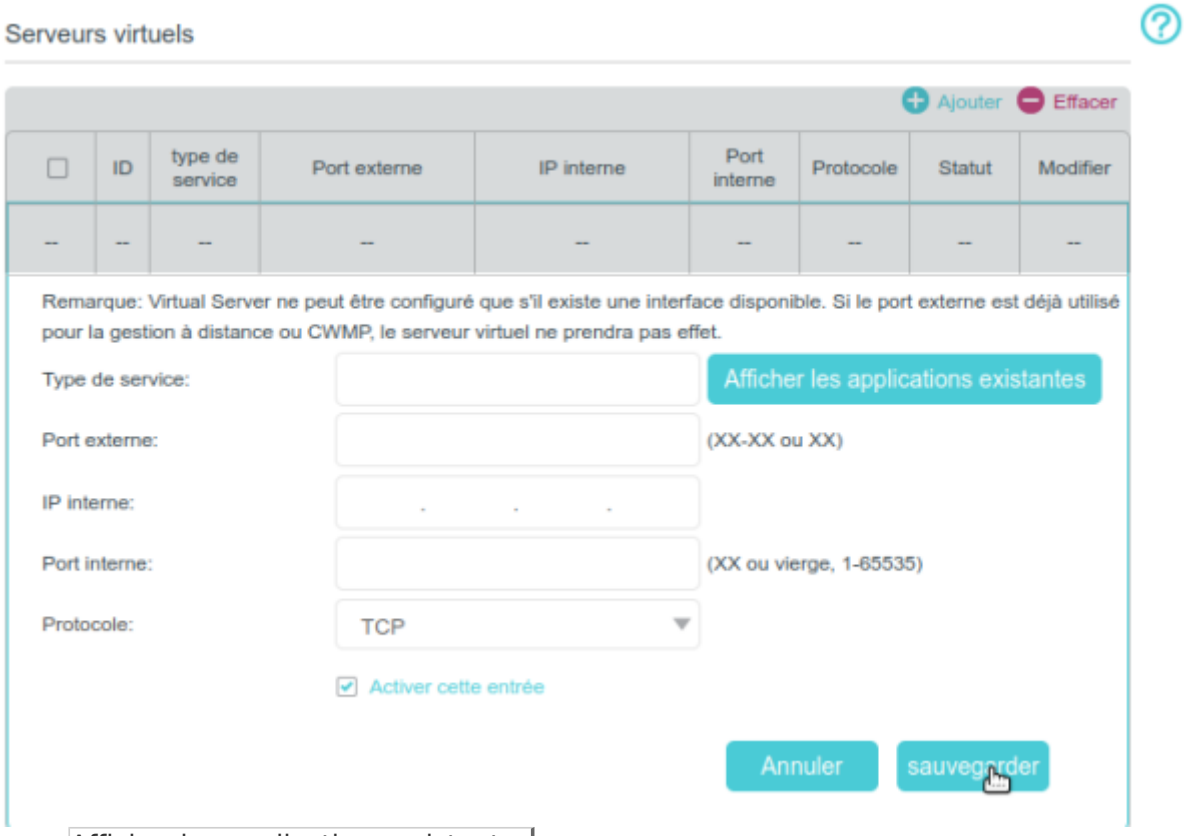


Pour cela :

Attribuez une adresse IP statique à votre PC, par exemple 192.168.1.100.

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

Onglet **Avancée**, **Transmission NAT > Serveurs virtuels**, cliquez sur Ajouter.



Cliquez sur Afficher les applications existantes

choisissez HTTP. Le port externe, le port interne et le protocole seront renseignés automatiquement.
Il est recommandé de conserver les paramètres par défaut du port et du protocole si vous n'êtes pas sûr du port et du protocole à utiliser.

Si le service que vous souhaitez utiliser n'est pas dans les applications existantes, vous pouvez saisir les paramètres correspondants manuellement. Vérifiez le numéro de port dont le service a besoin.

3. **IP interne** : Saisissez l'adresse IP du PC (192.168.1.100).
4. Vous pouvez ajouter plusieurs règles de serveur virtuel si vous souhaitez fournir plusieurs services dans un routeur. Notez que les ports externes ne peuvent pas se chevaucher.
5. Cliquez sur Sauvegarder pour enregistrer les paramètres.

Les utilisateurs d'Internet peuvent maintenant saisir http://WAN IP (dans cet exemple, http://218.18.232.154) pour visiter votre site Web personnel.

WAN IP doit être une adresse IP publique.
Pour que WAN IP soit attribuée dynamiquement par le FAI, enregistrez un nom de domaine pour le WAN par DDNS, et configurez un compte de service DNS dynamique.
Ensuite, vous pouvez utiliser http://nom_de_domaine pour visiter le site Web.

Si vous avez modifié le port externe par défaut, vous devez utiliser http://WAN_IP:External_Port ou http://domain_name:External_Port pour visiter le site Web.

Ouvrir les ports de manière dynamique par déclenchement de port

Le déclenchement de port peut spécifier un port de déclenchement et ses ports externes correspondants.

Lorsqu'un hôte du réseau local initie une connexion sur un port de déclenchement, tous les ports externes seront ouverts pour les connexions suivantes.

Le routeur peut enregistrer l'adresse IP de l'hôte.

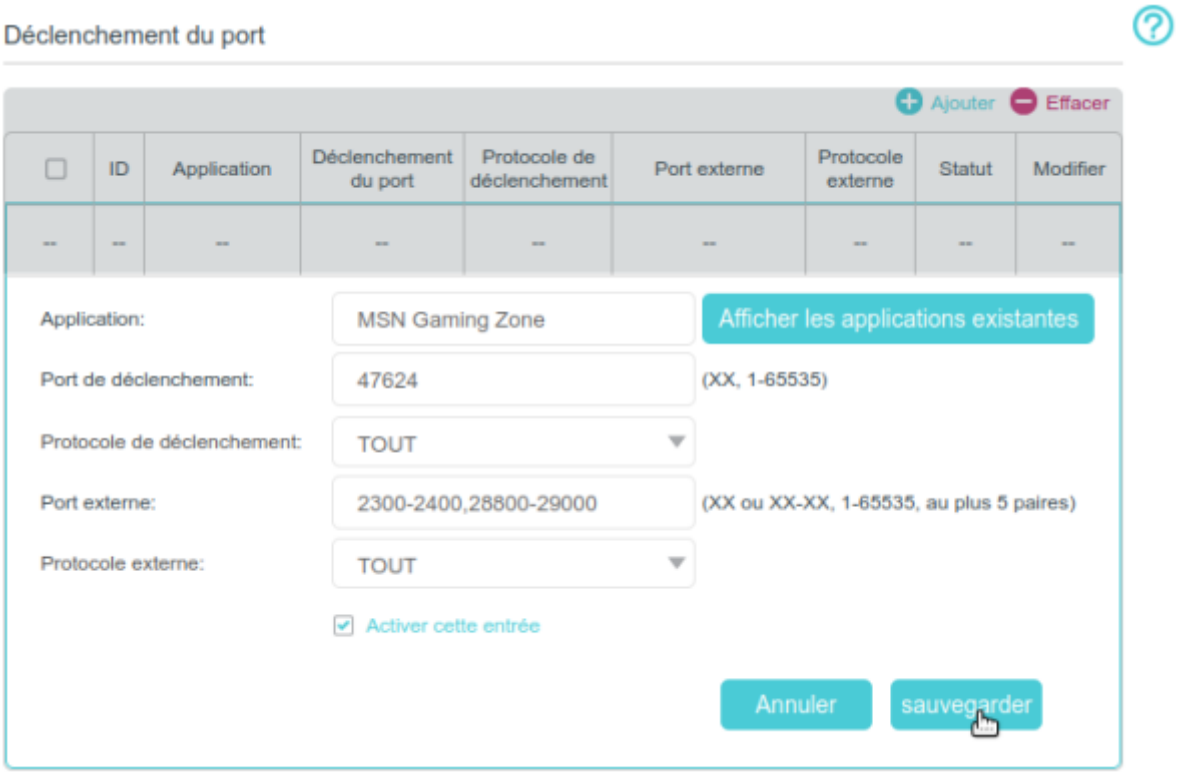
Lorsque les données d'Internet retournent vers les ports externes, le routeur peut les transférer à l'hôte correspondant.

Le déclenchement de port s'applique principalement aux jeux en ligne, VoIP et lecteurs vidéo.

Les applications courantes incluent les lecteurs MSN Gaming Zone, Dialpad et Quick Time 4, etc.

Pour configurer les règles de déclenchement de port :

connectez-vous sur http://tplinkmodem.net avec le mot de passe du routeur.
Accédez à **Avancée > Transmission NAT > Déclenchement du port** et cliquez sur **Ajouter**.



Cliquez sur **Afficher les applications existantes** et sélectionnez l'application souhaitée. Le port et le protocole de déclenchement, le port et le protocole externes seront renseignés automatiquement. Ici, nous prenons l'application **MSN Gaming Zone** comme exemple.

Cliquez sur Sauvegarder pour enregistrer les paramètres.

Vous pouvez ajouter plusieurs règles de déclenchement de port en fonction des besoins de votre réseau.

Si l'application dont vous avez besoin n'est pas répertoriée dans la liste Applications existantes, saisissez les paramètres manuellement. Vous devez d'abord vérifier les ports externes que l'application utilise et les saisir dans le champ Port externe en fonction du format affiché par la page.

Rendre les applications sans restriction de port par DMZ

Lorsqu'un PC est configuré pour être un hôte DMZ (zone démilitarisée) dans le réseau local, il est totalement exposé à Internet, ce qui peut créer une communication bidirectionnelle illimitée entre les hôtes internes et les hôtes externes.

L'hôte DMZ devient un serveur virtuel dont tous les ports sont ouverts.

Lorsque vous ne savez pas exactement quels ports ouvrir dans certaines applications spéciales, comme une caméra IP et un logiciel de base de données, vous pouvez configurer le PC comme hôte DMZ.

DMZ s'utilise surtout quand les utilisateurs ne savent pas

quels ports ouvrir.

Lorsqu'il est activé, l'hôte DMZ est totalement exposé à Internet, ce qui peut entraîner un risque potentiel pour la sécurité.

Si la DMZ n'est pas utilisée, veuillez la désactiver à temps !

Nous voulons que le PC domestique rejoigne le jeu en ligne sur Internet sans restriction de port.

Par exemple quand, en raison de certaines restrictions de port, lorsque vous jouez aux jeux en ligne, vous pouvez vous connecter normalement mais ne pouvez pas rejoindre une équipe avec d'autres joueurs.

Pour résoudre ce problème, configurez votre PC en tant que DMZ avec tous les ports ouverts :

Attribuez une adresse IP statique à votre PC, par exemple 192.168.1.100.
Connectez-vous sur http://tplinkmodem.net avec le mot de passe du routeur.
Onglet **Avancée**, **Transmission NAT > DMZ** et cochez la case pour activer DMZ :

Adresse IP de l'hôte DMZ : Saisissez l'adresse IP (192.168.1.100)
Cliquez sur Sauvegarder pour enregistrer les paramètres.

La configuration est terminée. Vous avez configuré votre PC sur un hôte DMZ et vous pouvez maintenant former une équipe pour jouer avec d'autres joueurs.

Faites en sorte que les jeux Xbox en ligne fonctionnent en douceur grâce à UPnP

Le protocole UPnP (Universal Plug and Play) permet aux applications ou hôtes périphériques de trouver automatiquement le périphérique NAT frontal et de lui demander d'ouvrir les ports correspondants.

Lorsque UPnP est activé, les applications ou les périphériques hôtes des deux côtés du périphérique NAT peuvent communiquer librement les uns avec les autres, réalisant ainsi une connexion transparente du réseau.

Vous devrez peut-être activer l'UPnP pour utiliser des applications pour les jeux multijoueurs, les connexions peer-to-peer, la communication en temps réel (telle que la VoIP ou la conférence

téléphonique) ou l'assistance à distance, etc.

> UPnP est activé par défaut sur ce routeur.
>
> Seule l'application prenant en charge le protocole UPnP peut utiliser cette fonctionnalité.
>
> La fonction UPnP nécessite la prise en charge du système d'exploitation (par exemple, Windows Vista/Windows 7/Windows 8, etc. Certains systèmes d'exploitation doivent installer les composants UPnP).

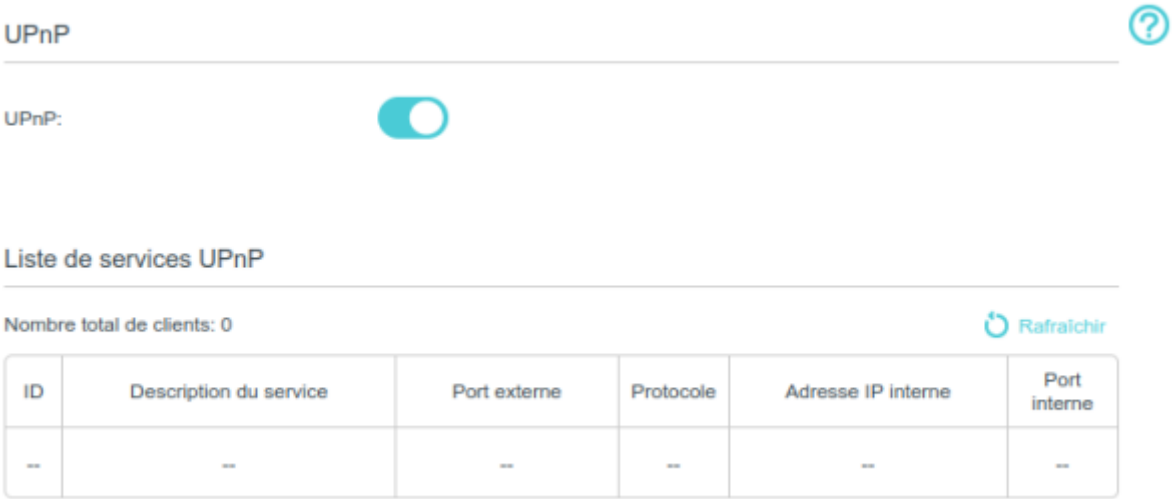
For example, when you connect your Xbox to the router which has connected to the internet to play online games, UPnP will send requests to the router to open the corresponding ports, allowing the following data penetrating the NAT to transmit. Par exemple, lorsque vous connectez votre Xbox au routeur qui s'est connecté à Internet pour jouer à des jeux en ligne, UPnP enverra des requêtes au routeur pour ouvrir les ports correspondants, permettant la transmission des données suivantes par le NAT.

Par conséquent, vous pouvez jouer à des jeux en ligne Xbox sans accroc.

Si nécessaire, pour modifier l'état de l'UPnP :

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

Onglet **Avancée**, **Transmission NAT > UPnP** : activez ou désactivez selon vos besoins.



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

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

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