

NQG_039_FR : Utilisation et modification du jeu de filtres Basic Firewall sur routeurs Netopia Série R, 4000 ou Cayman 3300-ENT

Ce guide technique explique comment configurer le filtrage IP sur un routeur Netopia pour permettre l'accès à des serveurs **Telnet**, **SMTP**, **POP3** et **HTTP** (Web).

Ce document est une extension de la note technique [NIR_052 Netopia Router Firewall Features and Configuration](#) qu'il est préférable de lire avant d'essayer de mettre en œuvre la présente note technique.

En règle générale, l'utilisation d'un Firewall n'est nécessaire que lorsque des adresses IP publiques sont utilisées soit directement sur le réseau Ethernet derrière le routeur, soit en utilisant une règle de NAT Statique (voir note technique [NOG_024 : Setting up a Static Map](#)). Si vous utilisez du NAPT (PAT) sur votre connexion Internet, votre réseau est déjà protégé / masqué par une seule IP publique pour connecter les IP privées des ordinateurs sur le réseau derrière le routeur. Utiliser le jeu de filtres **Basic Firewall** est alors en quelque sorte redondant en ce qui concerne la sécurité des postes de travail derrière le routeur. Cependant l'utilisation du filtrage **Basic Firewall** permet de protéger l'accès aux consoles d'administration du routeur.

Si vous désirez utiliser **Basic Firewall** en conjonction avec PAT (**Easy-PAT**) et une Liste de Serveurs (**Easy-Servers**), consultez la note technique [NOG_025 Configurer une liste de serveurs virtuels](#).

Pré-requis :

Ce guide technique suppose que votre routeur utilise un **firmware 4.8.2 ou supérieur**.

Ce guide suppose que vous utilisez de la traduction d'adresses IP sur le routeur.

Pour mettre à jour le firmware de votre routeur, allez sur la [page de mise à jour des firmware](#) sur le site web netopia.

Avant de commencer :

- Etablissez une connexion série sur le port console du routeur en utilisant un programme d'émulation de terminal tel que **HyperTerminal**. Les réglages doivent être:
 - a. Bits par seconde : **9600**
 - b. Bits de données : **8**
 - c. Parité : **Aucune**
 - d. Bits d'arrêt : **1**
 - e. Contrôle de flux : **Aucun**
- Vous pouvez également utiliser **Telnet** pour vous connecter à la console de votre routeur Netopia via le réseau local.

- Pour plus d'informations sur comment vous connecter à votre routeur Netopia via **HyperTerminal** ou **Telnet**, veuillez consulter le guide :

[NQG 100: Démarrer \(Comment établir une connexion Telnet/Console depuis un poste de travail Windows\)](#)

Astuces :

Ne modifiez pas d'autres réglages que ceux cités ci-dessous.

- Taper sur la touche **Entrée** vous conduit à une autre page.
- Taper sur la touche **Echap** vous permet de revenir à la page précédente.
- Taper sur la touche **Entrée** permet de valider la saisie de données.
- Taper sur la touche **Tab** permet de commuter un champ entre deux valeurs.

Contexte :

Ce Guide de Configuration Rapide présente les informations qui vous aideront à personnaliser le filtrage IP de votre routeur Netopia au-delà de la simple utilisation du jeu de filtres **Basic Firewall** sur votre profil de connexion Internet.

Le but de cette note technique est de procurer les instructions pour permettre l'accès Telnet au routeur depuis Internet. Et par répliation de ces instructions, vous découvrirez comment permettre l'accès aux serveurs **SMTP**, **POP3** et **HTTP** connectés au réseau local derrière le routeur. Cette note est fournie comme matériel supplémentaire au chapitre consacré au filtrage IP contenu dans le manuel de référence livré sur le CD et à l'addendum spécifique au firmware retenu.

Notez bien : A partir du firmware 4.8.2, si vous utilisez **Basic Firewall** et la traduction d'adresses IP **Easy-PAT** avec une **IP WAN publique** fixe, vous devez créer une règle de filtrage qui autorise l'accès avec les paramètres suivants :

- La **Destination IP Address** doit être égale à l'adresse **IP WAN publique** du routeur Netopia
- Le **Destination Subnet Mask** doit être **255.255.255.255**.

Veuillez noter que les instructions suivantes ne fonctionneront que si elles sont ajoutées au jeu de filtres pré configuré **Basic Firewall** ou tout autre jeu de filtres similaire.

Créer et activer un jeu de filtres utilisant uniquement les instructions ci-après entraînera l'arrêt du trafic Internet.

Création d'une règle de filtrage pour **Telnet** :

L'outil de création/modification de règles de filtrage est accessible en allant dans le menu suivant :

---> **Quick Menus...**

---> **IP Filter Sets...**

---> **Display/Change IP Filter Set...**

---> **Basic Firewall...**

---> **Add Input Filter to Filter Set...**

Tapez **Entrée** après chaque sélection pour passer à l'étape suivante.

- Conservez **Enabled** positionné sur **Yes**
- Appuyez sur **Tabulation** (TAB) pour changer **Forward** à **Yes**
- Laissez **Source IP Address:** configuré à **0.0.0.0**
- Laissez **Source IP Mask:** configuré à **0.0.0.0**
- Modifiez **Dest. IP Address:** et saisissez **172.20.10.216**
NOTE: Cette adresse est utilisée comme exemple. Remplacez-la avec l'adresse IP attribuée par votre Fournisseur d'accès Internet.
- Modifiez **Dest. IP Mask:** et entrez **255.255.255.255**
- Dans **Protocol Type:** saisissez **TCP**
- Conservez **Source Port Compare...** configuré à **No Compare**
- Conservez **Source Port ID...** configuré à **0**
- Dans **Destination Port Compare...** et choisissez **Equal**
- Modifiez **Destination Port ID...** et entrez **23**
- Laissez **Established TCP Conns. Only:** inchangé à **No**
- Ajoutez le filtre en tapant **Entrée** sur **ADD THIS FILTER NOW**

A la création, cette règle de filtrage est ajoutée à la suite des autres règles. Vous devez la déplacer du bas de la liste à une position située avant les règles autorisant les trafics **TCP** et **UDP** au delà du port **1023**. Pour cela après être retourné dans **Basic Firewall**, allez dans :

---> **Move input filter...**

Tapez **Entrée** et sélectionnez la règle de filtrage que vous venez de créer. Tapez de nouveau sur **Entrée** et utilisez les touches fléchées pour déplacer la règle de filtrage de deux niveaux et tapez à nouveaux **Entrée** pour insérer la règle à sa nouvelle position.

Vous avez maintenant créé une règle de filtrage pour permettre l'accès Telnet à votre routeur depuis Internet lorsque **Basic Firewall** est activé sur votre connexion Internet.

Si vous vérifiez les règles de filtrage depuis le menu **Display/Change Input Filter**, votre filtre sera affiché tel que ci-dessous:

Source IP Address	Source Mask	Destination IP Address	Destination Mask	Protocol	Source Port	Destination Port	On?	Forward
0.0.0.0	0.0.0.0	172.20.10.216	255.255.255.255	TCP	No Compare	=23	Yes	Yes

Si vous avez également un serveur de messagerie (**SMTP/POP3**) ou un serveur Web (**HTTP**) et que vous avez configuré un transfert de ports pour permettre l'accès à des serveurs ayant des IP privées sur le réseau local, il faut également que vous modifiiez le jeu de filtres **Basic Firewall**.

Pour cela, dans le cadre de notre exemple nous allons supposer que le serveur de messagerie a **192.168.1.10** comme adresse IP sur le réseau local, le serveur Web aura quant à lui l'adresse **192.168.1.20**.

Dans l'exemple précédent, vous avez configuré la règle pour un port **TCP 23**. Pour permettre l'accès à un serveur de messagerie il suffira de configurer deux règles pour les ports **TCP 25(SMTP)** et **TCP 110(POP3)**. Pour l'accès à un serveur Web, il faudra configurer une règle identique pour le port **80(HTTP)**.

Les règles de filtrage pour le serveur de messagerie apparaîtront tels que ci-dessous :

Source IP Address	Source Mask	Destination IP Address	Destination Mask	Protocol	Source Port	Destination Port	On?	Forward
0.0.0.0	0.0.0.0	192.168.1.10	255.255.255.255	TCP	No Compare	=25	Yes	Yes
0.0.0.0	0.0.0.0	192.168.1.10	255.255.255.255	TCP	No Compare	=110	Yes	Yes

Les règles de filtrage pour le serveur Web apparaîtront tels que ci-dessous :

Source IP Address	Source Mask	Destination IP Address	Destination Mask	Protocol	Source Port	Destination Port	On?	Forward
0.0.0.0	0.0.0.0	192.168.1.20	255.255.255.255	TCP	No Compare	=80	Yes	Yes

Une fois les filtres déplacés à leur bonne position, si vous allez dans l'écran **Display/Change Input Filter** vous devriez obtenir quelque chose tel que ci-dessous:

```

+---#---Source IP Addr---Dest IP Addr-----Proto--Src.Port--D.Port--On?-Fwd--+
| 1  0.0.0.0      0.0.0.0      TCP    NC      =2000  Yes No
| 2  0.0.0.0      0.0.0.0      TCP    NC      =5000  Yes No
| 3  0.0.0.0      0.0.0.0      ICMP   NC      NC      Yes Yes
| 4  0.0.0.0      172.20.10.216 TCP    NC      =23    Yes Yes
| 5  0.0.0.0      192.168.1.10  TCP    NC      =25    Yes Yes
| 6  0.0.0.0      192.168.1.10  TCP    NC      =110   Yes Yes
| 7  0.0.0.0      192.168.1.20  TCP    NC      =80    Yes Yes
| 8  0.0.0.0      0.0.0.0      TCP    NC      >1023  Yes Yes
| 9  0.0.0.0      0.0.0.0      UDP    NC      >1023  Yes Yes

```

D'autres ports peuvent nécessiter d'être ouvert pour certains services spécifiques. Ils sont listés dans un tableau à la fin de la note technique [NIR_052 Fonctionnalités et configuration du Firewall sur les routeurs Netopia](#)

Conclusion:

Les routeurs Netopia intègrent un filtrage de paquets complet qui permet de bloquer ou de permettre la transmission de trafics IP selon les adresses d'hôte ou de réseau de destination ou sources. Cette fonction de filtrage permet de sécuriser le réseau local contre tout accès non autorisé tout en permettant aux utilisateurs de confiance d'accéder aux ressources de ce même réseau local.