www.hongdian.com

HONGDIAN

Application Guide

Hongdian Router-Filtering Rules-FAQs

Contents

Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Doc Version	Product	Release Data	Details
V1.0	Hongdian Router	2017.09.30	First Release

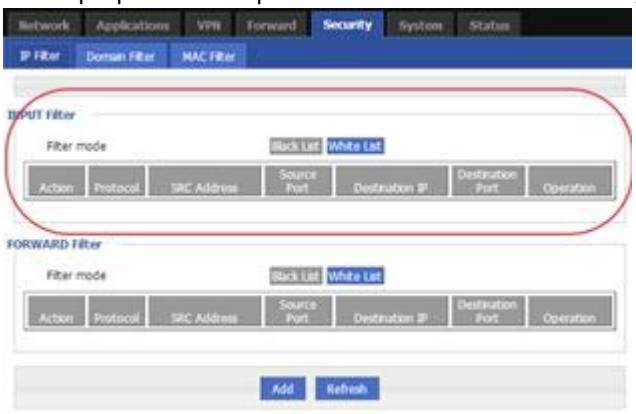
1 Overview

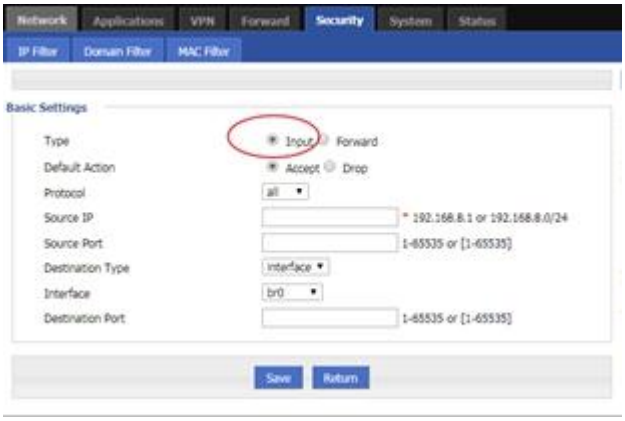
This is the FAQs(Frequently Asked Questions) for the filtering rules of Hongdian routers, which is the security function of Hongdian router including IP filtering, domain filtering and MAC filtering. The filtering rules can build up the firewall for the router.

2 FAQs

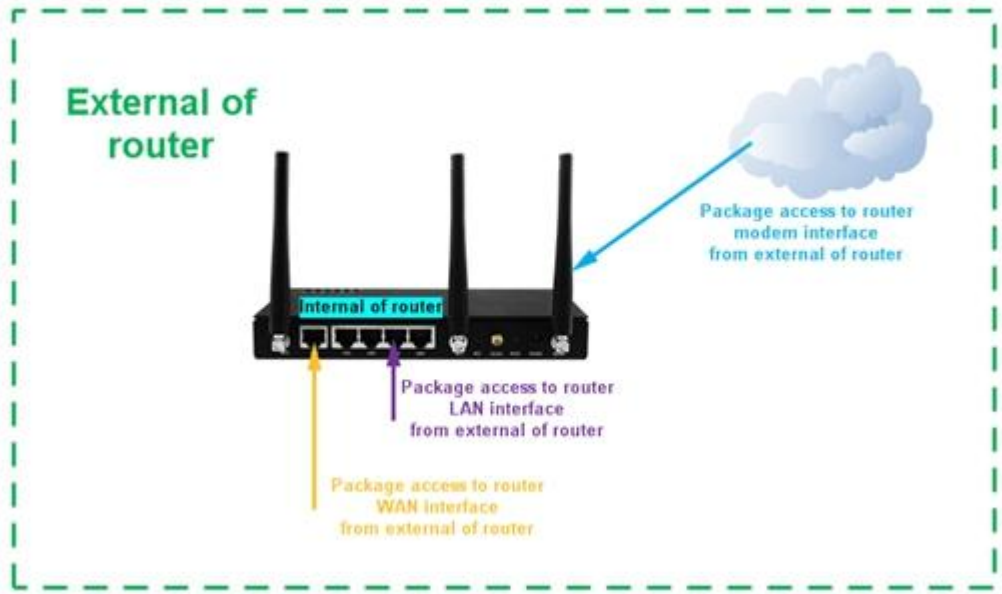
What is the INPUT filter function?

A: The purpose of setup INPUT filter rule is to limit users/IP/PC etc to access router from all router interfaces.



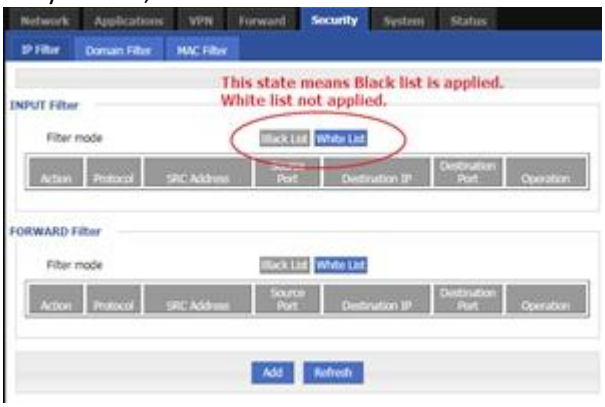


Purpose: Filter all packets sent from external of router to internal of router. Control access to router like visiting GUI, CLI etc.

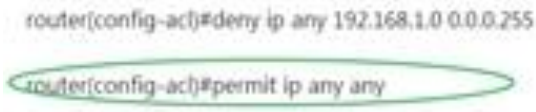


How to setup black list ?

A: By default, filter mode is **Blacklist mode**.



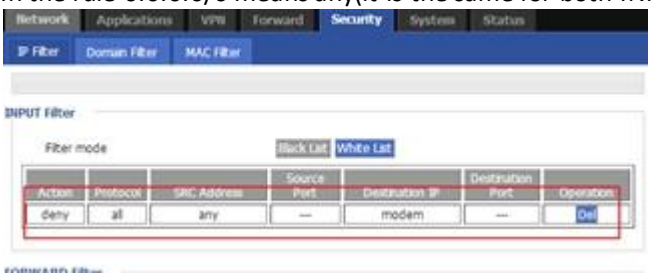
It means there is an ACL rule permit ip any any always at the end of all rules. Whenever rule is updated, this permit ip any any rule will be added at the end of the rule list automatically.



Sample1: Block 192.168.8.0/24 to limit access to router from LAN interface.

Sample2: Block all IP to limit access to router modem interface

In the rule 0.0.0.0/0 means any(it is the same for both INPUT filter and Forward filter)



How to setup white list?

A:

(1) The Blacklist and White list applies to whole router, all interfaces. By default is Black list, which means permit all in all interfaces. If switch to White list, then means deny all on all interface.

(2) To enable White list, need to setup a rule in black list earlier, and then switch from black list to white list. The rule we setup before we enable White list, should be an Accept rule, which accept IP to visit router from outside. If not have this accept rule, when switch to white list, then all IP unable to visit router. We need to avoid this. So earlier rule to setup should be like this:

When switch from Black list to White list, it does nothing to the rule we added in the table. The router just change

From: permit ip any any

To: deny ip any any

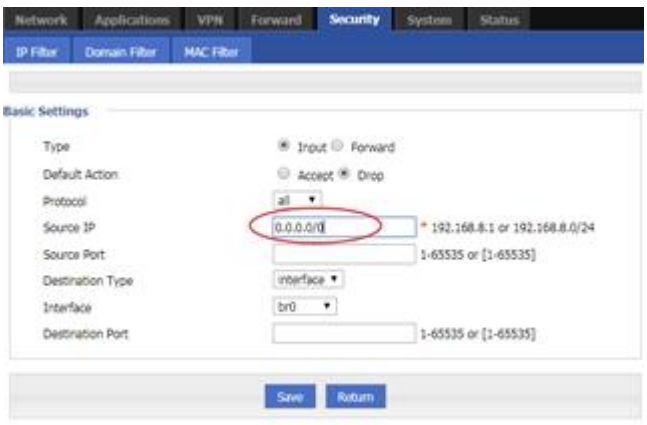
(3) So when we click to switch rule, it will have a permit rule in the table which all IP to access br0, while deny any is applied. If there is no permit rule in the table to permit access to router, then no IP will be able to access to router unless reset router to factor default.

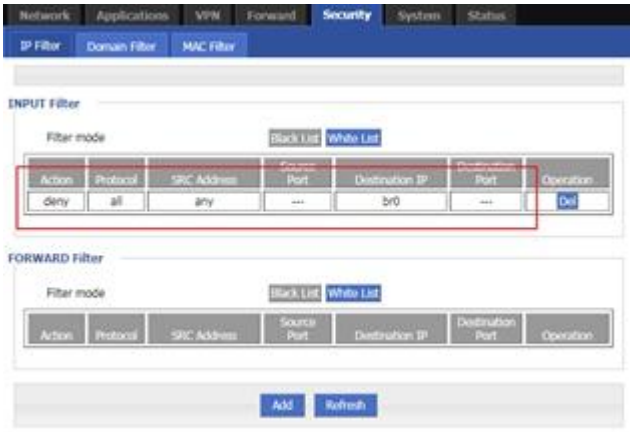
How to block IP or subnet to access router?

A: Need to setup INPUT rule, and select interface as you wish.

Sample1:

Block any IP to access router from LAN





How to block IP or subnet to access internet?

A: Need to use Forward filter

If INPUT rule already block IP and subnet, whether the blocked IP and subnet still be able to pass forward through router?

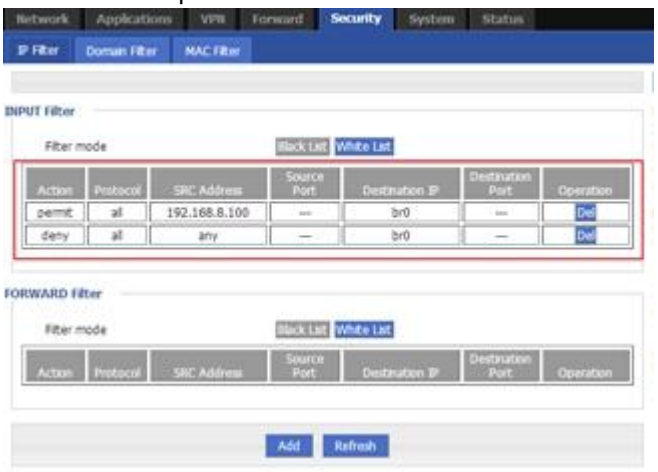
A: Yes, forwarding for IP still will work. But domain will not work, because router doesn't reply to DNS resolution request anymore.

Why still have permit/accept rule in Blacklist?

A: It is necessary to have it, here is an example:

Sample1: A user want to visit router from LAN interface by 192.168.8.100 only. But want to block all other IP and subnets to access router from LAN.

Here is the setup:



In this case, all IP and subnet unable access to router from LAN interface but 192.168.8.100.

We are using Black list, because we only controlling the LAN interface access for now. For WAN or Modem or other virtual interface like IPSec, still they need Blacklist. If we use White list, then means the Deny IP any any rule is applied to all interface. It is not we are trying to setup here.

How does rule take effect if confliction happens in rule?

A: The one added earlier will take effect for the conflicted part.

Whether complete opposite rule can be added?

A: Yes, the rule added earlier, will take effect.

What if complete the same rule added several times?

A: The earlier time added rule will take effect. The priority of it won't change.

How to check the priority of rules already added in router?

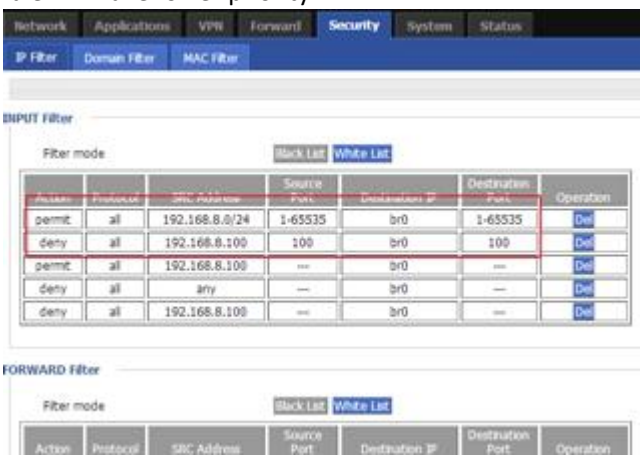
A: Check on the GUI, the one on the top up has higher priority than the one below it.

Sample: in sample below, the permit rule has the top priority and middle on less priority, and the one at the bottom has lowest priority.

Why does the new added rule sometimes go to up in the rules queue with higher priority than old rules?

A: The rule which specify port number always has higher priority than those doesn't have specific port number specified.

When both rule specify specific port number, it still queue according the time when rule is added. New added rule will have lower priority.



HONGDIAN

Create smart things

Contact us

F14 - F16, Tower A, Building 14, No.12, Ganli 6th Road, Longgang District, Shenzhen 518112, China.

+86-755-88864288-5

+86-755-83404677

hongdianchina

www.hongdian.com

sales@hongdian.com

Hongdian_China