Firewall Function Configuration and Application

Version: <1.0>
Release date: <2018-06-01>

Contents

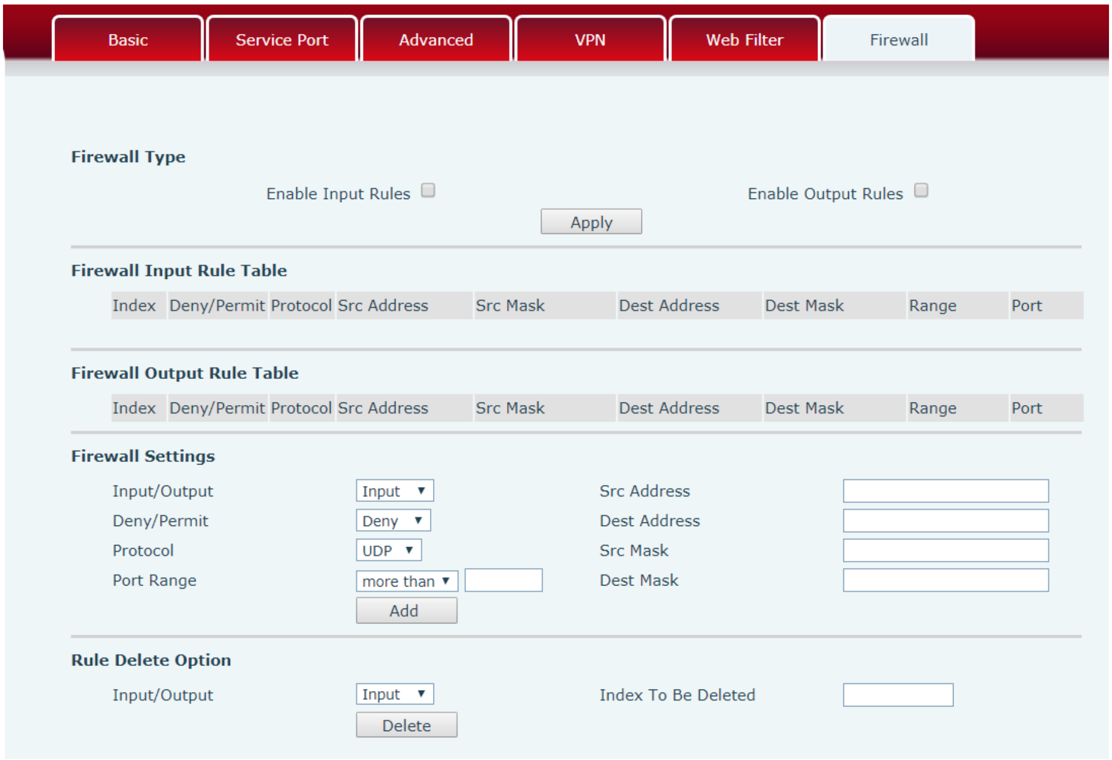
1 Introduction

1.1 Purpose of Firewall

Input and output rules can be configured on the firewall to prevent malicious access to the network or restrict the access permission of internal users to external network resources, improving network security.

1.2 Firewall Configuration

Web-based configuration of firewall



Firewall Type

Enable Input Rules □ Enable Output Rules □

Firewall Input Rule Table

Index	Deny/Permit	Protocol	Src Address	Src Mask	Dest Address	Dest Mask	Range	Port

Firewall Output Rule Table

Index	Deny/Permit	Protocol	Src Address	Src Mask	Dest Address	Dest Mask	Range	Port

Firewall Settings

Input/Output	Input ▾	Src Address	
Deny/Permit	Deny ▾	Dest Address	
Protocol	UDP ▾	Src Mask	
Port Range	more than ▾	Dest Mask	

Rule Delete Option

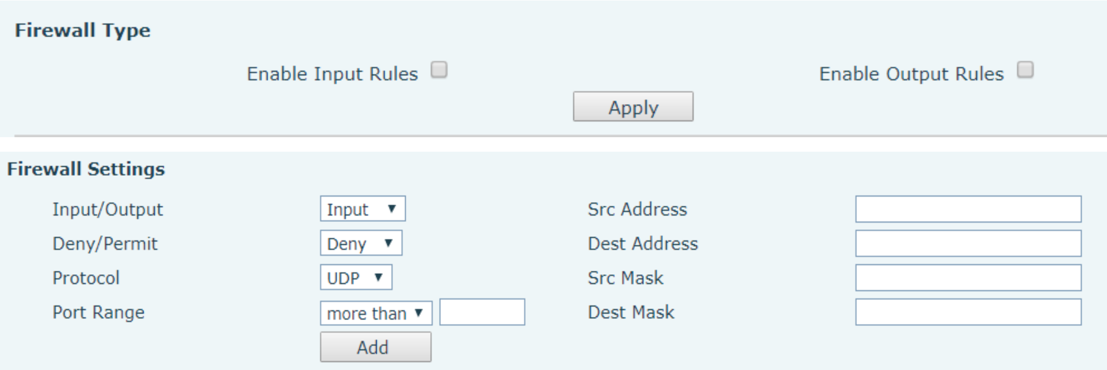
Input/Output: Input ▾ Index To Be Deleted:

Firewall configuration description

Firewall

On this webpage, you can choose whether to enable input and output firewalls. This function supports two types of rules: input and output rules. Each rule has an index. A maximum of 10 rules can be configured for each type.

Firewall configuration is complicated. The following is an example.



Firewall Type

Enable Input Rules □ Enable Output Rules □

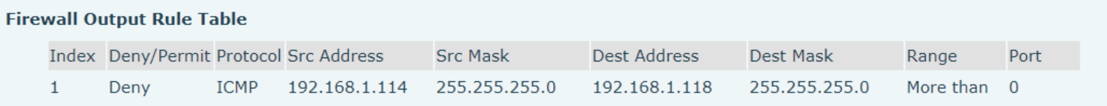
Firewall Settings

Input/Output	Input ▼	Src Address	
Deny/Permit	Deny ▼	Dest Address	
Protocol	UDP ▼	Src Mask	
Port Range	more than ▼	Dest Mask	

Field	Description
Enable Input Rules	Enable the input rule function.
Enable Output Rules	Enable the output rule function.
Input/Output	Choose to add an input or output rule.
Deny/Permit	Set the rule to deny or permit.
Protocol	Type of protocol to be filtered, including TCP, UDP, ICMP, and IP.
Port Range	Range of filtered ports.
Src Address	Source address. The source address can be host address, network address, any address (0.0.0.0), or network address in *.*.*.0 format, such as 192.168.1.0.
Dest Address	Destination address. The destination address can be IP address, any address (0.0.0.0), or network address in *.*.*.0 format, such as 192.168.1.0.
Src Mask	Source address mask. When the mask is set to 255.255.255.255, a specific host is filtered. When the value is set to a subnet mask such as 255.255.255.0, a subnet is filtered.
Dest Mask	Destination address mask. When the mask is set to 255.255.255.255, a specific host is filtered. When the value is set to a subnet mask such as 255.255.255.0, a subnet is filtered.

Local phone IP address: 192.168.1.114.

After the settings, click **Add**. A new rule is added to the output rule table, as shown below:



Firewall Output Rule Table

Index	Deny/Permit	Protocol	Src Address	Src Mask	Dest Address	Dest Mask	Range	Port
1	Deny	ICMP	192.168.1.114	255.255.255.0	192.168.1.118	255.255.255.0	More than	0

Then select **Enable Output Rules** and click **Submit**.

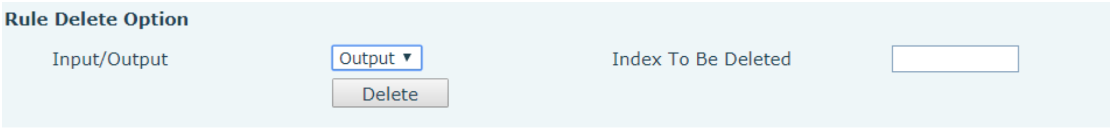
Configuration procedure and symptom:

1. Run the ping 192.168.1.118 command on the phone (192.168.1.114). The ping packet cannot be sent to 192.168.1.118 because it is denied by the rule.

2. Run the ping 192.168.1.0-192.168.1.255 commands on the phone (192.168.1.114). Other IP addresses on the subnet cannot send ICMP packets.

3. Run the ping 192.168.1.114 command on the phone (192.168.1.118). According to the packet capturing result, you can find that the phone (192.168.1.118) has sent the ICMP packet and the device 192.168.1.114 has received the packet, but 192.168.1.114 does not reply due to the deny output rule.

Note: To use the ping function of the phone, open the LCD menu and choose **Application** > **Ping**.



Rule Delete Option

Input/Output: Output ▼

Index To Be Deleted:

To delete a rule, enter the rule index and click **Delete**.