

How do I open WebFig for External User in Mikrotik Router

In order to allow connect to Mikrotik Router WebFig remotely, you should add a firewall filter and NAT rule for remote connection in WebFig.

1) Create a firewall filter

The first action you should do is to add filtering option for port 80 at IP Firewall Filter Rules Add New

RouterOS v6.47.3 (stable)

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Add New Reset All Counters

18 items

	#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port
;;; special dummy rule to show fasttrack counters									
- D	0	passthro	forward						
;;; defconf: accept established,related,untracked									
- D	1	accept	input						
;;; allow IPsec NAT									
- D	2	accept	input			17 (udp)		4500	
;;; allow IKE									
- D	3	accept	input			17 (udp)		500	
;;; allow l2tp									
- D	4	accept	input			17 (udp)		1701	
;;; allow pptp									
- D	5	accept	input			6 (tcp)		1723	
;;; allow sstp									
- D	6	accept	input			6 (tcp)		443	
;;; [CK] added for WebFig									
- D	7	accept	input			6 (tcp)		80	
;;; defconf: drop invalid									
- D	8	drop	input						

And then you should make sure if you put following item correctly

<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Remove"/> <input type="button" value="Reset Counters"/>	
not invalid	
Enabled	<input checked="" type="checkbox"/>
Chain	input ▼
Src. Address	▼
Dst. Address	▼
Protocol	<input type="checkbox"/> 6 (tcp) ▼
Src. Port	▼
Dst. Port	<input type="checkbox"/> 80
Any. Port	▼

IP Fragment	▼
Action	accept ▼
Log	<input type="checkbox"/>

Comment	[CK] added for WebFig
---------	-----------------------

You may able to locate above filtering information after #6 like below:

;;; special dummy rule to show fasttrack counters										
-	D	0	passthro	forward						
;;; defconf: accept established,related,untracked										
-	D	1	✓ accept	input						
;;; allow IPsec NAT										
-	D	2	✓ accept	input			17 (udp)	4500		
;;; allow IKE										
-	D	3	✓ accept	input			17 (udp)	500		
;;; allow l2tp										
-	D	4	✓ accept	input			17 (udp)	1701		
;;; allow pptp										
-	D	5	✓ accept	input			6 (tcp)	1723		
;;; allow sstp										
-	D	6	✓ accept	input			6 (tcp)	443		
;; [CK] added for WebFig										
-	D	7	✓ accept	input			6 (tcp)	80		
;;; defconf: drop invalid										
-	D	7	✗ drop	input						
;;; defconf: accept ICMP										
-	D	8	✓ accept	input			1 (icmp)			
;;; defconf: accept to local loopback (for CAPsMAN)										
-	D	9	✓ accept	input		127.0.0.1				
;;; defconf: drop all not coming from LAN										
-	D	10	✗ drop	input						

2) Creating a NAT rule by IP Firewall NAT Add New

CapsMAN

Wireless

Interfaces

Bridge

Switch

PPP

Mesh

IP 1)

ARP

Accounting

Addresses

Cloud

DHCP Client

DHCP Relay

DHCP Server

DNS

Firewall 2)

Hotspot

RouterOS v6.47.3 (stable)

Filter Rules

NAT 3)

Mangle

Raw

Service Ports

Connections

Address Lists

Layer7 Protocols

4)

Add New

Reset All Counters

9 items

	#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf
;;; CK - Service Hairpin to .6 ~ MAIN GATEWAY to 192.168.10.6 (25,80,110,443,20022)										
-	D	0	dst-nat	dstnat	!192.168.10.6	6 (tcp)		25,80,110,4		
;;; Service Hairpin to SSH										
-	D	1	dst-nat	dstnat	!192.168.10.6	6 (tcp)		20022		
;;; defconf: masquerade										
-	D	2	masquerade	srcnat						
;;; masq. vpn traffic										
-	D	3	masquerade	srcnat	192.168.10.0					
;;; SSH to Main Server										

And you should check followings

<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Remove"/> <input type="button" value="Reset Counters"/>	
not invalid	
Enabled	<input checked="" type="checkbox"/>
Chain	dstnat ▼
Src. Address	▼
Dst. Address	▼
Protocol	▲ <input type="checkbox"/> 6 (tcp) ▼
Src. Port	▼
Dst. Port	▲ <input type="checkbox"/> 80
Any. Port	▼
In. Interface	▲ <input type="checkbox"/> ether1-gateway ▼

Note that you can change the connection port number if you want

Action	dst-nat ▼
Log	<input type="checkbox"/>
Log Prefix	▼
To Addresses	▲ 192.168.89.1
To Ports	▲ 80

Comment	[CK] WebFig
---------	-------------

Now you can connect to WebFig remotely.