



# Configuring FortiGate® for FortiVoice™



## Configuring FortiGate® for FortiVoice™

Revision 1

August 30, 2012

Copyright © 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	<a href="http://docs.fortinet.com">docs.fortinet.com</a>
Knowledge Base	<a href="http://kb.fortinet.com">kb.fortinet.com</a>
Customer Service & Support	<a href="http://support.fortinet.com">support.fortinet.com</a>
Training Services	<a href="http://training.fortinet.com">training.fortinet.com</a>
FortiGuard	<a href="http://fortiguard.com">fortiguard.com</a>
Document Feedback	<a href="mailto:techdocs@fortinet.com">techdocs@fortinet.com</a>

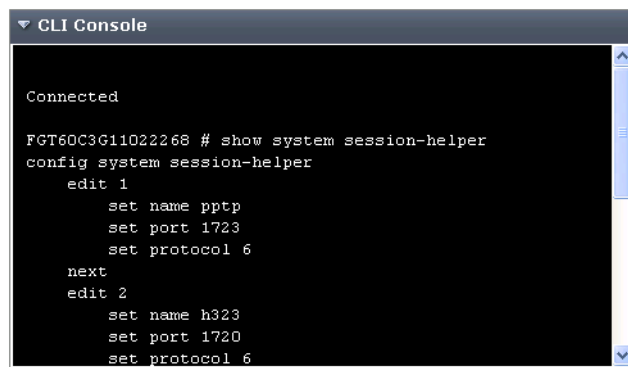
# Configuring FortiGate® for FortiVoice™

This document covers setting up a FortiGate for a FortiVoice phone system. This document assumes that the FortiGate is already set up and working on the network, and the FortiVoice system is using the default port configurations.

## Disabling the SIP session helper

The SIP session helper may cause problems with some providers.

1. Connect to the FortiGate via a web browser.
2. Under *Dashboard* > *Status*, click on the *CLI Console*.
3. Enter `show system session-helper`.



```
CLI Console
Connected
FGT60C3G11022268 # show system session-helper
config system session-helper
edit 1
    set name pptp
    set port 1723
    set protocol 6
next
edit 2
    set name h323
    set port 1720
    set protocol 6
```

4. Find the SIP session *set name SIP*, and check its session number. For example, *Edit 3*.
5. Enter `delete 3`.
6. Reboot the FortiGate.

## Creating Routing Rules

To ensure proper routing, configure Virtual IPs in the FortiGate and write policies for them.

### Create a rule for SIP

1. In the FortiGate web browser, go to *Firewall Objects > Virtual IP > Virtual IP*.
2. Select *Create New*.

The screenshot shows the configuration page for a new Virtual IP rule named 'FVC-SIP'. The 'Name' field is 'FVC-SIP'. The 'Comments' field is 'Write a comment...'. The 'External Interface' is 'wan1 (64 Subnet)'. The 'Type' is 'Static NAT'. The 'Source Address Filter' checkbox is unchecked. The 'External IP Address/Range' is '0.0.0.0'. The 'Mapped IP Address/Range' is '172.20.241.200'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'UDP'. The 'External Service Port' is '5060'. The 'Map to Port' is '5060'. There are 'OK' and 'Cancel' buttons at the bottom.

3. Name the rule *FVC-SIP*.
4. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
5. Set the *Protocol* to *UDP*.
6. Set the *External Service Port* to *5060*.
7. Set the *Map to Port* to *5060*.

### Create a rule for RTP

1. Select *Create New*.

The screenshot shows the configuration page for a new Virtual IP rule named 'FVC-RTP'. The 'Name' field is 'FVC-RTP'. The 'Comments' field is 'Write a comment...'. The 'External Interface' is 'wan1 (64 Subnet)'. The 'Type' is 'Static NAT'. The 'Source Address Filter' checkbox is unchecked. The 'External IP Address/Range' is '0.0.0.0'. The 'Mapped IP Address/Range' is '172.20.241.200'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'UDP'. The 'External Service Port' is '6100 - 6114'. The 'Map to Port' is '6100 - 6114'. There are 'OK' and 'Cancel' buttons at the bottom.

2. Name the rule *FVC-RTP*.
3. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
4. Set the *Protocol* to *UDP*.
5. Set the *External Service Port* to *6100 – 6114*.
6. Set the *Map to Port* to *6100*.

If configuring a multiple-unit deployment, enter the FortiVoice system IP address for Unit #2, and the RTP port range of 6200 – 6214. Refer to the *FortiVoice User Guide* for a complete list of RTP ports for additional systems.

## Create a rule for TFTP if you're using external IP phones

1. Select *Create New*.

Name	<input type="text" value="FVC-TFTP"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
External Interface	<input type="text" value="wan1 (64 Subnet)"/>
Type	Static NAT
<input type="checkbox"/> Source Address Filter	<input type="text" value=""/> (e.g.: x.x.x.x, x.x.x.x-y.y.y.y, x.x.x.x/y)
External IP Address/Range	<input type="text" value="0.0.0.0"/> - <input type="text" value=""/>
Mapped IP Address/Range	<input type="text" value="172.20.241.200"/> - <input type="text" value=""/>
<input checked="" type="checkbox"/> Port Forwarding	
Protocol	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> SCTP
External Service Port	<input type="text" value="69"/> - <input type="text" value="69"/>
Map to Port	<input type="text" value="69"/> - <input type="text" value="69"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

2. Name the rule *FVC-TFTP*.
3. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
4. Set the *Protocol* to *UDP*.
5. Set the *External Port* to 69 – 69.
6. Set the *Map to Port* to 69.

## Create a rule for HTTP for web access and legacy external IP phones

1. Select *Create New*.

Name	<input type="text" value="FVC-HTTP"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
External Interface	<input type="text" value="wan1 (64 Subnet)"/>
Type	Static NAT
<input type="checkbox"/> Source Address Filter	<input type="text" value=""/> (e.g.: x.x.x.x, x.x.x.x-y.y.y.y, x.x.x.x/y)
External IP Address/Range	<input type="text" value="0.0.0.0"/> - <input type="text" value=""/>
Mapped IP Address/Range	<input type="text" value="172.20.241.200"/> - <input type="text" value=""/>
<input checked="" type="checkbox"/> Port Forwarding	
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP
External Service Port	<input type="text" value="8484"/> - <input type="text" value="8484"/>
Map to Port	<input type="text" value="8484"/> - <input type="text" value="8484"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

2. Name the rule *FVC-HTTP*.
3. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
4. Set the *Protocol* to *TCP*.
5. Set the *External Service Port* to 8484 – 8484.
6. Set the *Map to Port* to 8484.

## Create a rule for remote access via TCP

### 1. Select *Create New*.

The screenshot shows the configuration form for a Static NAT rule. The fields are as follows:

Name	FVC-Remote	
Comments	Write a comment... 0/255	
External Interface	wan1 (64 Subnet)	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter	(e.g.: x.x.x.x, x.x.x.x-y.y.y.y, x.x.x.x/y)	
External IP Address/Range	0.0.0.0 -	
Mapped IP Address/Range	172.20.241.200 -	
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	9393 - 9393	
Map to Port	9393 - 9393	

Buttons: OK, Cancel

2. Name the rule *FVC-Remote*.
3. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
4. Set the *Protocol* to *TCP*.
5. Set the *External Service Port* to *9393 – 9393*.
6. Set the *Map to Port* to *9393*.

## Create a rule for remote access via FTP

### 1. Select *Create New*.

The screenshot shows the configuration form for a Static NAT rule. The fields are as follows:









Name	FVC-Rem-FTP	
Comments	Write a comment... 0/255	
External Interface	wan1 (64 Subnet)	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter	(e.g.: x.x.x.x, x.x.x.x-y.y.y.y, x.x.x.x/y)	
External IP Address/Range	0.0.0.0 -	
Mapped IP Address/Range	172.20.241.200 -	
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	8485 - 8486	
Map to Port	8485 - 8486	

Buttons: OK, Cancel

2. Name the rule *FVC-Rem-FTP*.
3. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
4. Set the *Protocol* to *TCP*.
5. Set the *External Service Port* to *8485 – 8486*.
6. Set the *Map to Port* to *8485*.

## Write policies for the new Virtual IPs

1. Go to *Policy > Policy > Policy*.
2. Select *Create New*.

Source Interface/Zone	wan1 (64 Subnet)
Source Address	all 
Destination Interface/Zone	internal
Destination Address	FVC-HTTP  FVC-RTP  FVC-SIP  FVC-TFTP  
Schedule	always
Service	ANY 
Action	ACCEPT 
<input type="checkbox"/> Log Allowed Traffic	
<input type="checkbox"/> Enable NAT	
<input type="checkbox"/> Enable Identity Based Policy	
<input type="checkbox"/> UTM Security Profiles	
<input type="checkbox"/> Traffic Shaping	
Comments	<input type="text" value="Write a comment..."/> 0/255

3. In *Source Interface/Zone*, select the Wan port that you wish to use.
4. Set *Source Address* to *all* (restricting this may cause problems with traffic from various media servers used by VoIP carriers).
5. Set *Destination Interface/Zone* to *Internal*.
6. In *Destination Address*, add all of the Virtual IPs you just created.

