Configuring FortiGate® for FortiVoice™

Configuring FortiGate® for FortiVoice™

Revision 1

August 30, 2012

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

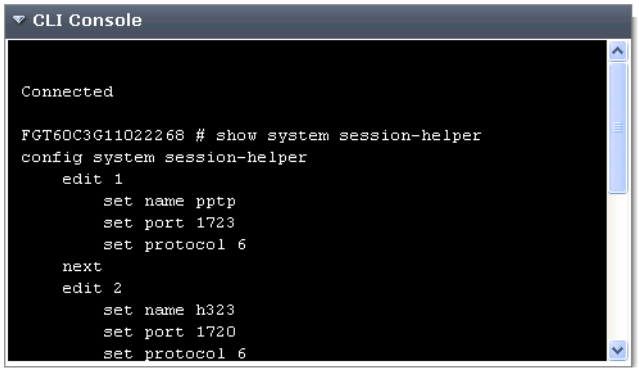
Configuring FortiGate® for FortiVoice™

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`.



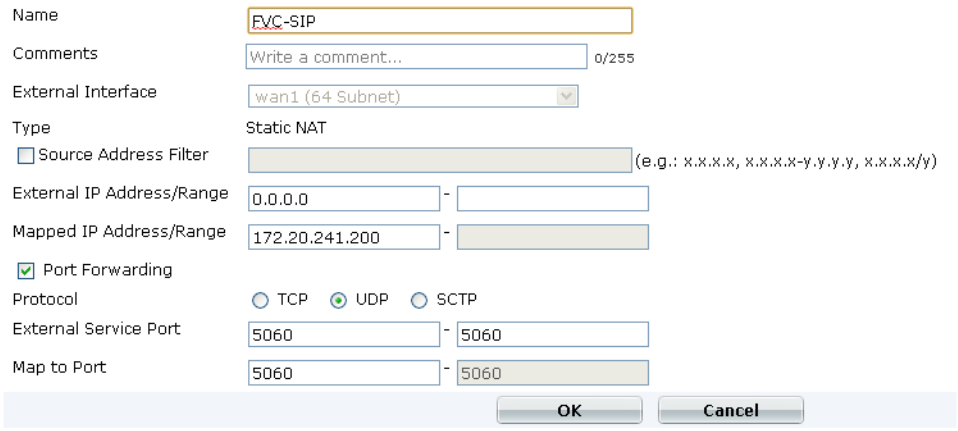
4. Find the SIP session *set name SIP*, and check its session number. For example, *Edit 3*.
5. Enter `delete 3`.
6. Reboot the FortiGate.

Creating Routing Rules

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

Create a rule for SIP

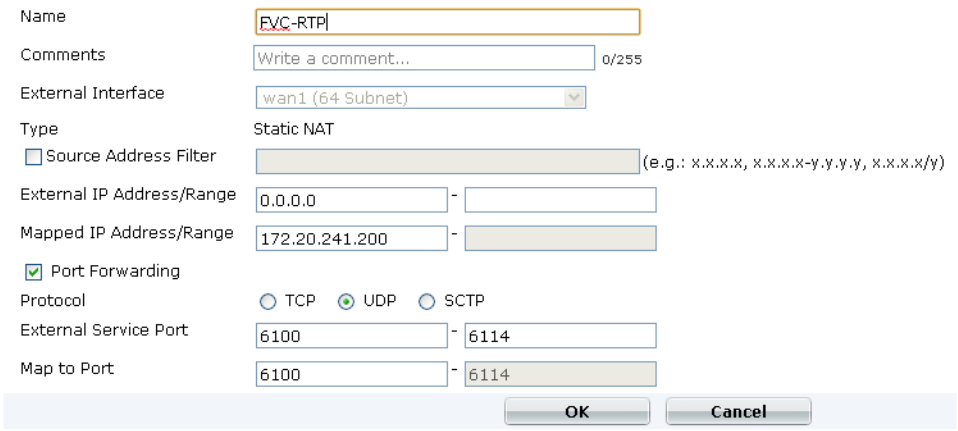
1. In the FortiGate web browser, go to *Firewall Objects* > *Virtual IP* > *Virtual IP*.
2. Select *Create New*.



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*.

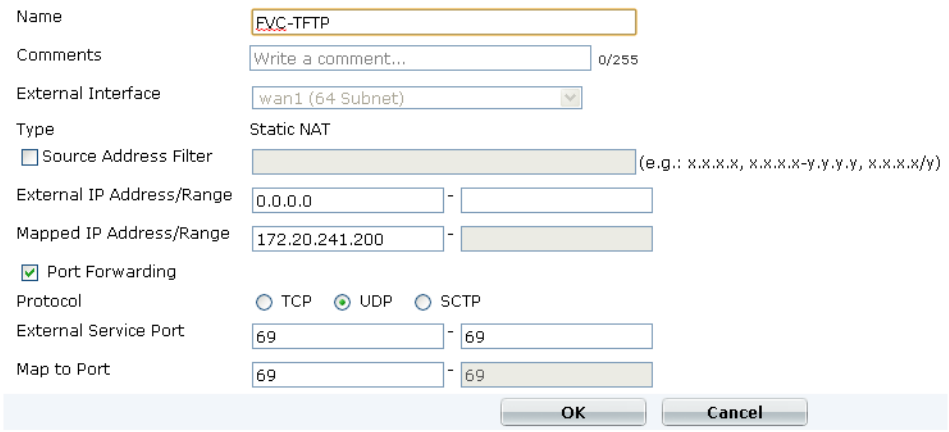


2. Name the rule *FVC-RTP*.
3. Enter the FortiVoice system IP address in the *Mapped IP Address/Range*.
4. Set the *Protocol* to *UDP*.
5. Set the *External Service Port* to *6100 – 6114*.
6. Set the *Map to Port* to *6100*.

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

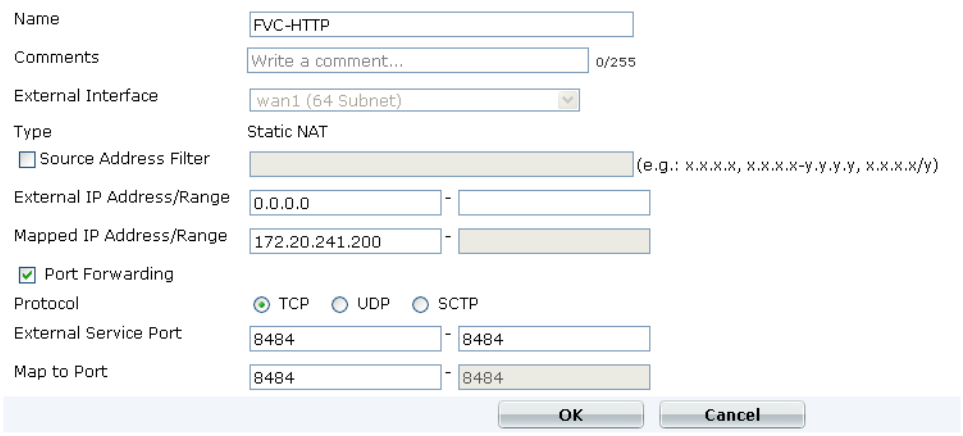
1. Select *Create New*.



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

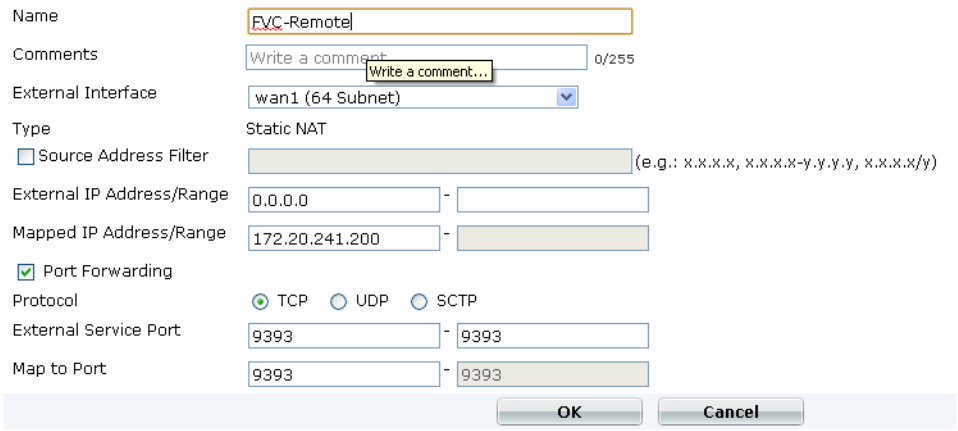
1. Select *Create New*.



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

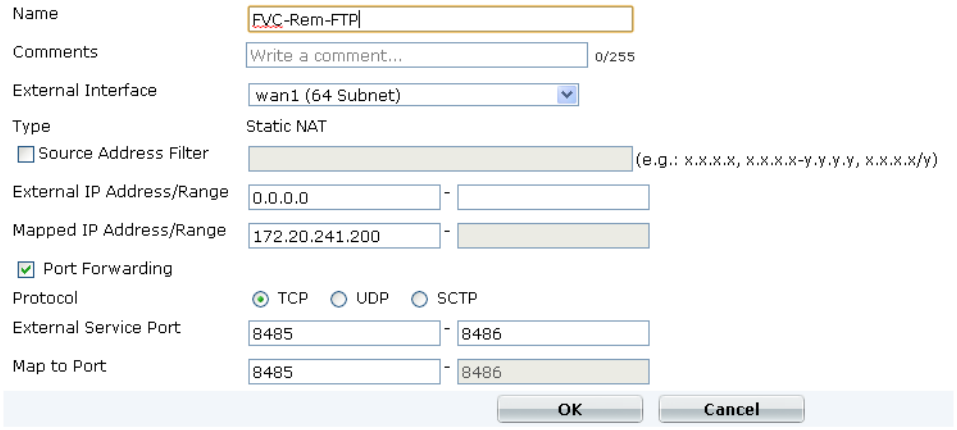
1. Select *Create New*.



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

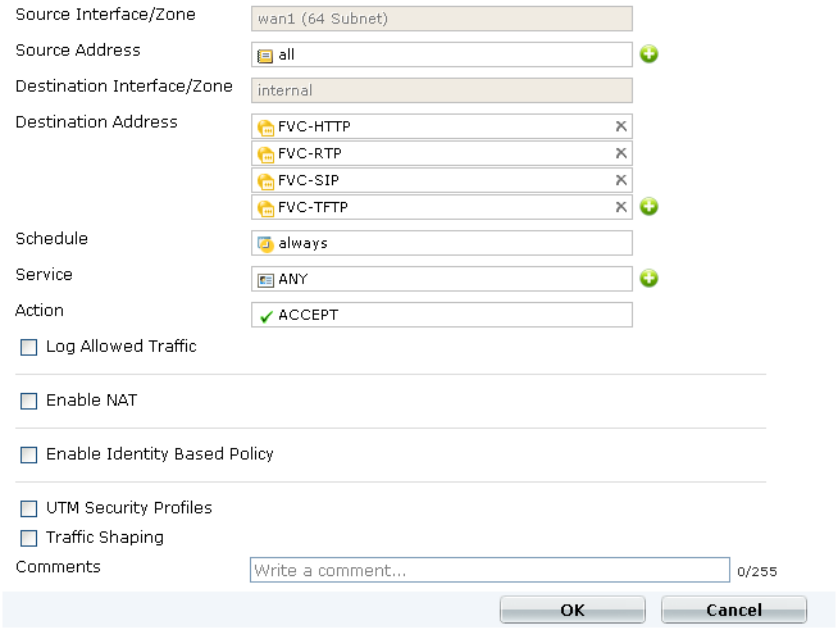
1. Select Create New.



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*.



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.