# Configuring a FortiGate 80C Firewall with 3CX

**edit 13**

set name sip

set protocol 17

.

# Introduction

This document describes the configuration of FortiGate 80C Firewall. In general Fortigate routers are known to be complicated to configure correctly for use as a gateway in front of a 3CX.



# Step 1: Disable SIP ALG

The SIP ALG functionality seems to be harder to disable (even if it is disabled via WEB Interface) and varies greatly between models. In addition, the type of NAT may break correct functionality or re-enable SIP ALG. On devices running FortiOs, you will need to disable this in multiple places as shown below:

1. Open the Fortigate CLI from the dashboard.
2. Enter the following commands in FortiGate’s CLI:

## config system settings

set sip-helper disable

set sip-nat-trace disable reboot the device

1. Reopen the FortiGate CLI and enter the following commands (do not enter text after //) config system session-helper

show //you need to find the entry for SIP, usually 12, but it may vary delete 12 //or the number that you identified from the previous command

1. Create a rule and set the **“Protection Profile”** to **“Unfiltered”**
2. Reboot the device and you should be ready to use your FortiGate 80C with the 3CX Phone System without any issues.

# Step 2: Removing the Session Helper

1. Run the following commands:

## config system session-helper

Show

1. Amongst the displayed settings will be one similar to the following example:

set port 5060

1. In this example the next commands would be:

## delete 13

end

# Step 3: Change the default –voip –alg-mode

1. Run the following commands:

## config system settings

set default-voip-alg-mode kernel-helper based end

1. If Version 5.2 and above continue

## config voip profile

edit default config sip

set status enable/disable end

end

# Step 4: Clear Sessions or Reboot

To clear sessions:

Ideally you would only delete sessions related to VoIP traffic. However, in the case of SIP, this means not only deleting the SIP control sessions but also all sessions opened to handle the audio (RTP) traffic. If you know the port-range used for the audio traffic, you can be selective with your session clear by first applying a filter.

* diagnose system session filter ...

The command to clear sessions applies to ALL sessions unless a filter is applied, and therefore will interrupt traffic.

* diagnose system session clear

Alternatively, reboot the FortiGate using either GUI or CLI. The CLI command is:

* execute reboot

# Step 5: Validating Your Setup

Log into your 3CX Management Console → Dashboard → Firewall and run the 3CX Firewall Checker. This will validate if your firewall is correctly configured for use with 3CX.

.