

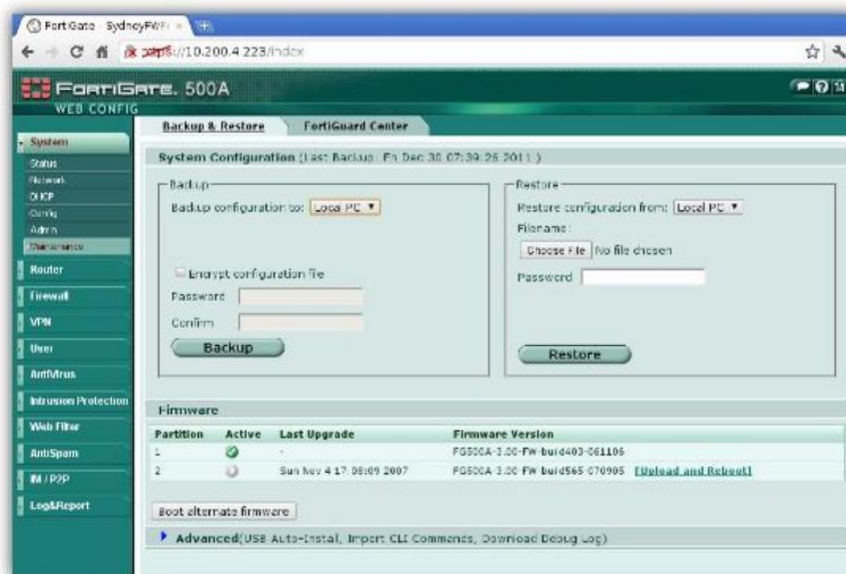
Fortinet Fortigate Devices

There are multiple different methods of extracting the configuration from your Fortinet Fortigate devices; this guide outlines two of those methods.

Using HTTP(S)

We would recommend using HTTPS rather than HTTP for transferring your devices configuration as the latter provides no encryption. The procedure for getting the configuration from the device using HTTP(S) is as follows:

1. Using your favorite web browser, connect to the HTTP(S) service provided by your Fortinet Fortigate device for remote management. You can do this by entering "https://" (recommended) or "http://" followed by your devices IP address.
2. Logon using your administration username and password.
3. Select the "Systems" tab, then the "Maintenance" option.
4. Click the "Backup" button to save the configuration to your computer



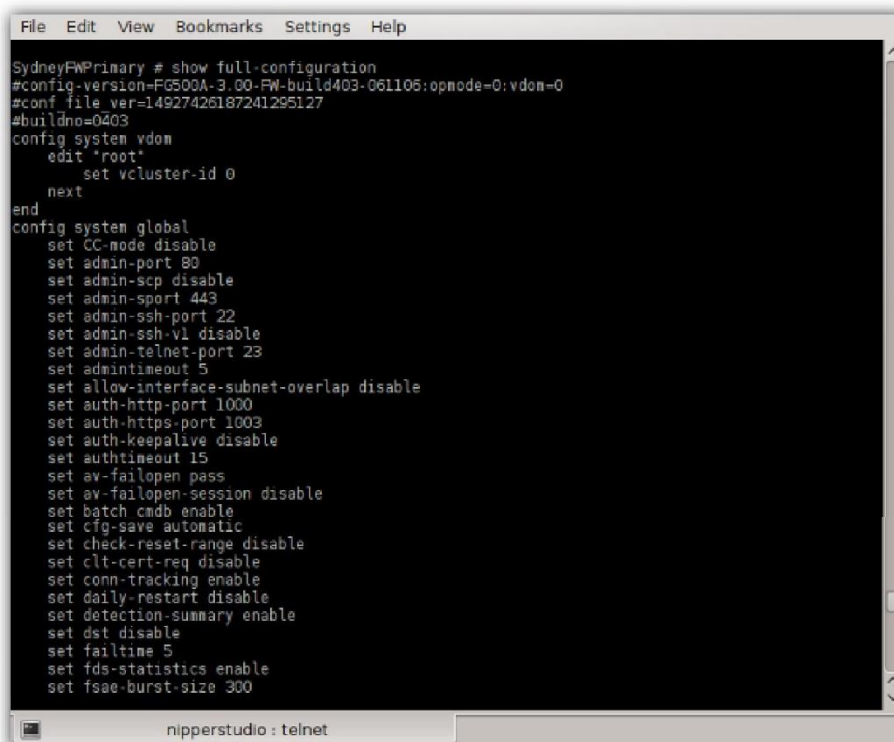
Using SSH, Telnet or the Console

For this procedure you will be using the Command Line Interface (CLI) of your Fortinet Fortigate device using an SSH client (such as OpenSSH or Putty), Telnet or through the console port. We would recommend using either SSH (for remote connections) or using a direct connection to the console port. Telnet provides no encryption of the communications and therefore your authentication credentials and configuration would be vulnerable if a malicious user were to monitor your connection.

1. Connect to the Fortinet Fortigate using your favorite SSH client, Telnet or a direct console connection.
2. Logon using your administration authentication credentials.
3. Execute the following CLI command and capture the output (possibly using the cut and paste facility):

show full-configuration

4. Save the captured output to a file and remove any visible page lines (i.e. -- More--).

A screenshot of a terminal window with a dark background and light text. The window title bar includes 'File Edit View Bookmarks Settings Help'. The terminal content shows the output of the 'show full-configuration' command, starting with 'SydneyFWPrimary # show full-configuration' and listing various system and global configuration parameters such as version, build number, system vdom settings, and global system settings. The window title at the bottom reads 'nipperstudio : telnet'.

```
File Edit View Bookmarks Settings Help
SydneyFWPrimary # show full-configuration
#config-version-FG500A-3.00-FW-build403-061105.opmode=0.vdom=0
#conf file ver=14927426187241295127
#buildno=0403
config system vdom
  edit 'root'
    set vcluster-id 0
  next
end
config system global
  set CC-mode disable
  set admin-port 80
  set admin-scp disable
  set admin-sport 443
  set admin-ssh-port 22
  set admin-ssh-v1 disable
  set admin-telnet-port 23
  set admintimeout 5
  set allow-interface-subnet-overlap disable
  set auth-http-port 1000
  set auth-https-port 1003
  set auth-keepalive disable
  set authtimeout 15
  set av-failopen pass
  set av-failopen-session disable
  set batch-cmdb enable
  set cfg-save automatic
  set check-reset-range disable
  set clt-cert-req disable
  set conn-tracking enable
  set daily-restart disable
  set detection-summary enable
  set dst disable
  set failtime 5
  set fds-statistics enable
  set fsae-burst-size 300
```