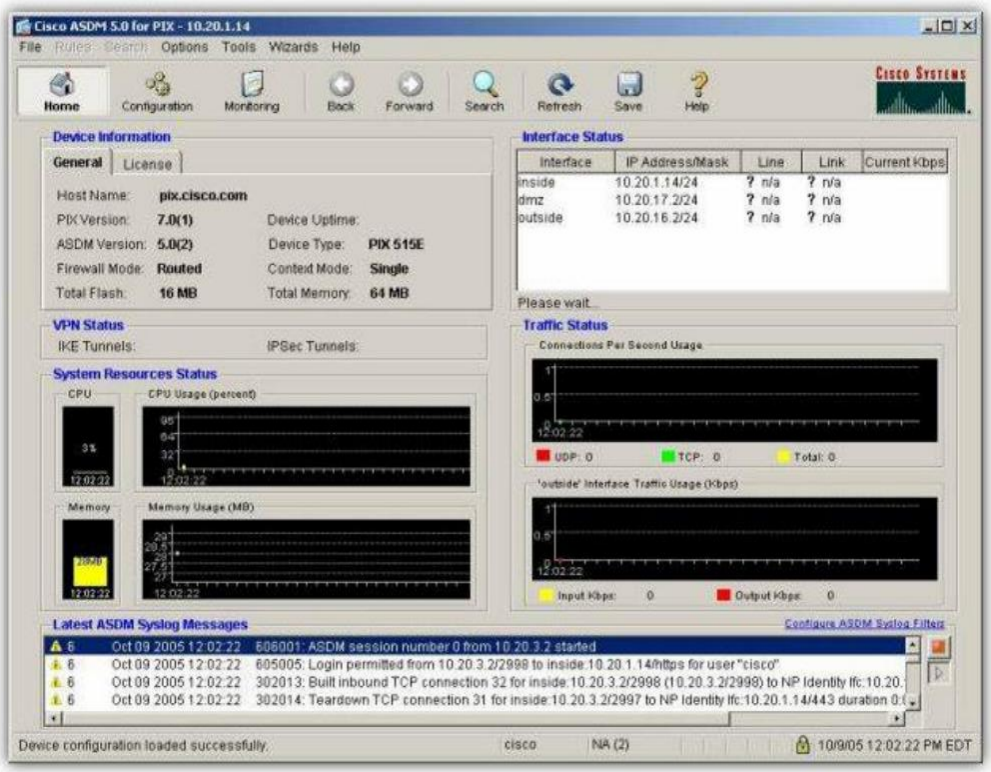
Cisco ASA, PIX and FWSM Firewalls

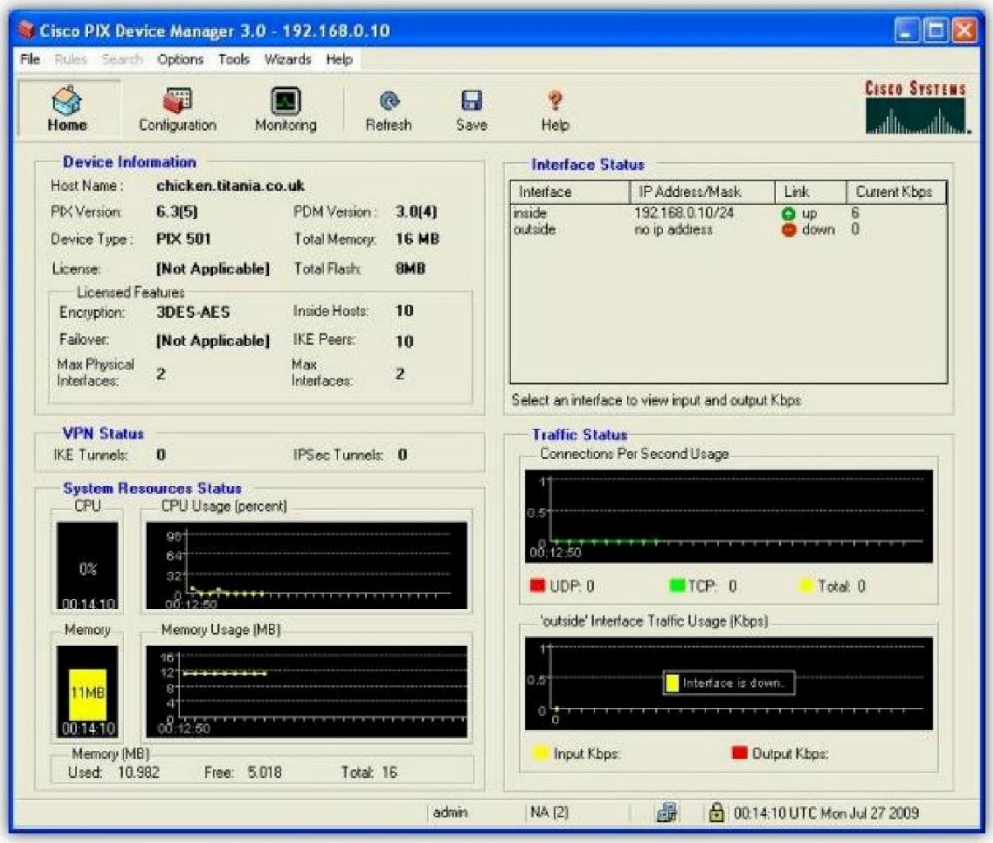
There are multiple different methods of extracting the configuration from your Cisco Security Appliance; this guide outlines just three of those.

Using ASDM and PDM

The ASDM and PDM interfaces can be accessed using a web browser with Java capabilities. Whether you have access to ASDM or PDM will depend on your security appliance (and its age), but the procedure is the same for both. The procedure for getting the configuration from your device is as follows:

1. Using your favourite web browser, connect to the HTTPS service provided by your Cisco device for remote management. You can do this by entering "https://" followed by your devices IP address.
2. On ADSM-capable devices, click on the "Run ADSM as a Java Applet" button.
3. Using your admin user name and password, login.
4. You should now see the ADSM or PDM application, both of which are shown in the screenshots below.
5. You can show the "running-config" using the option on the File menu.
6. Copy and paste the configuration into a file to use with Nipper Studio.





Using TFTP

We do not recommend using TFTP to transfer your configuration due to weaknesses in the protocol; the other methods described in this section are more secure. However, here is the procedure for using TFTP:

Connect to the Cisco device using SSH, Telnet, ASDM, and PDM or through a Console connection.

Login to your Cisco PIX device.

Transfer the configuration using the TFTP command "write net <ip-address> :<filename>"

Using SSH, Telnet or the Console

For this procedure you will be using the Command Line Interface (CLI) of your Cisco 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.

Connect to the Cisco using your favourite SSH client, Telnet, or a direct console connection.

Logon using your administration authentication credentials.

Enter "enable" and type in your enable password.

Execute the following CLI command and capture the output (possibly using the cut and paste facility):

```
show run
```

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