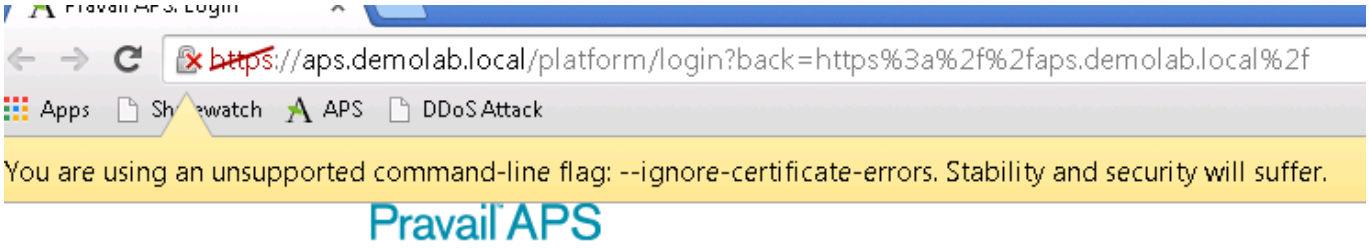
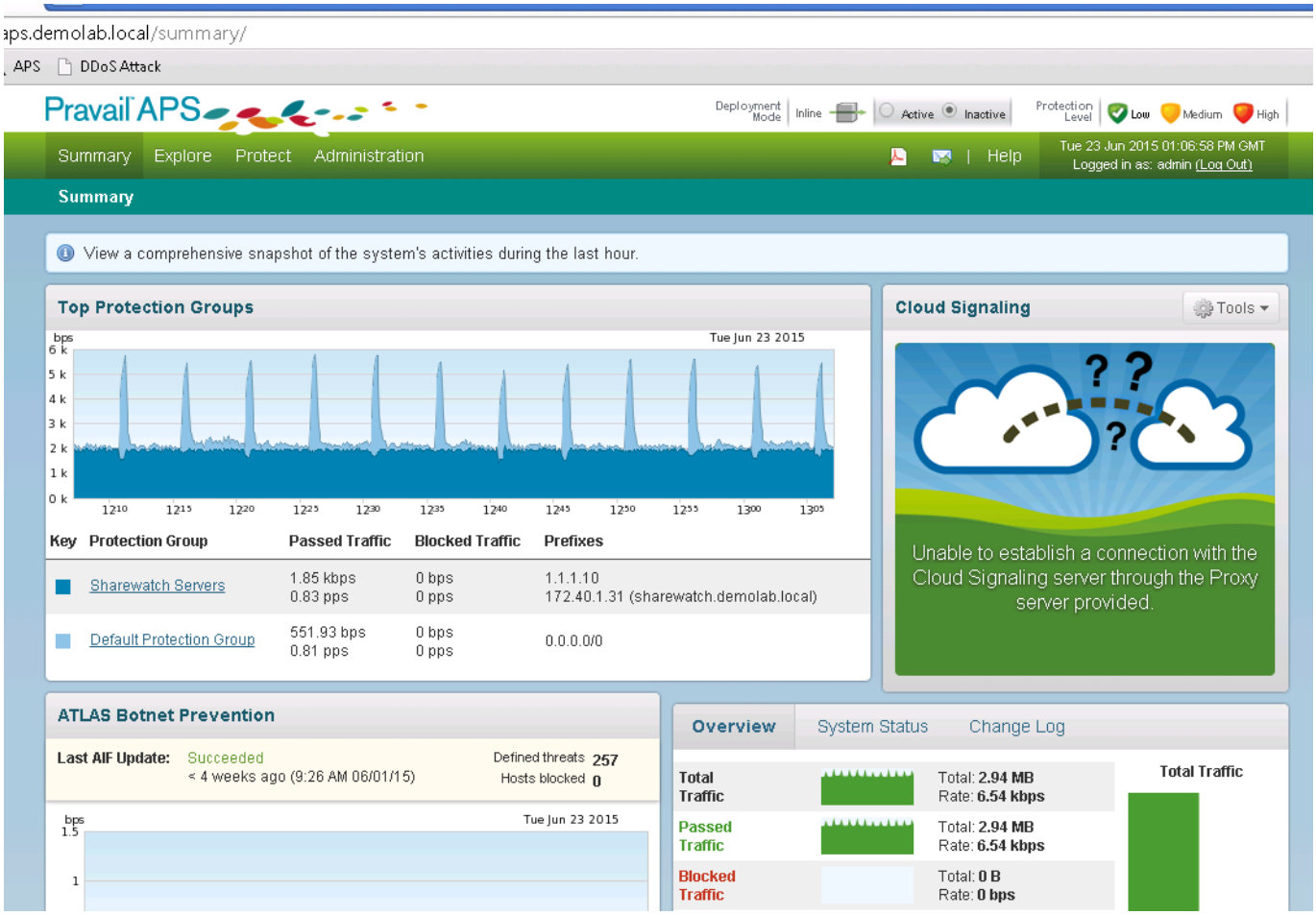
Arbor Lab Walkthrough

Log in to the Arbor Virtual Desktop, open up Chrome from the desktop:

Press the X to acknowledge the use of an unsupported flag in Chrome:



Log in to the Arbor APS appliance using the username **admin** and the password of **arbor**:



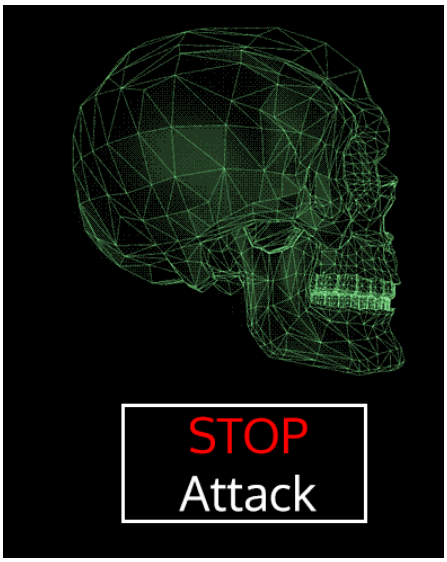
Ensure the APS is in INACTIVE mode at the top right hand corner of the GUI

©Zycko Ltd 2010

Open up Internet Explorer, you should see a Share index window, this will be our tier 1 web application, and also our Hackers target:

Go back to Google Chrome, On the same browser window as the arbor console, right click on the DDoS attack bookmark and open in new tab:

Now you should be able to launch a DDoS against the site, it will send a command to the C&C server to begin the attack.:

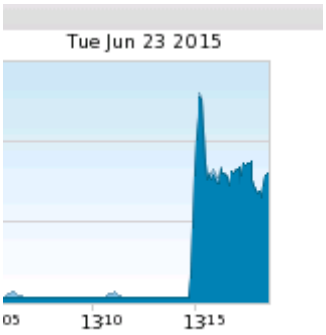


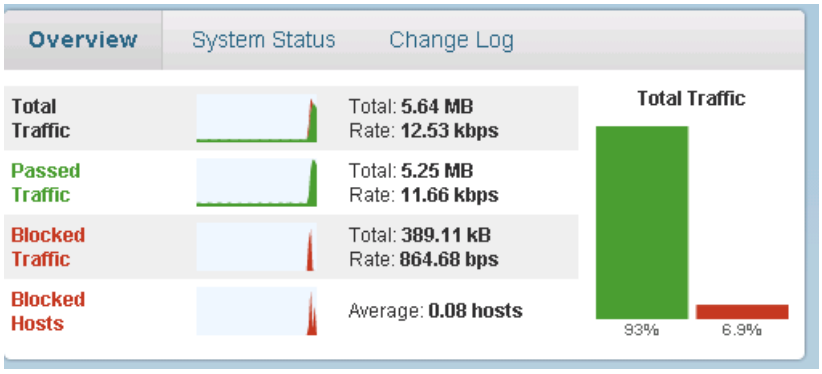
When the attack is running – a skull will rotate across the screen, the attack automatically times out after 15-20 minutes.

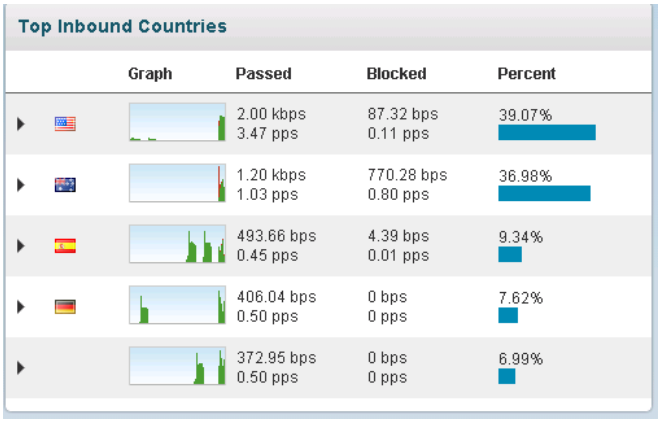
©Zycko Ltd 2010

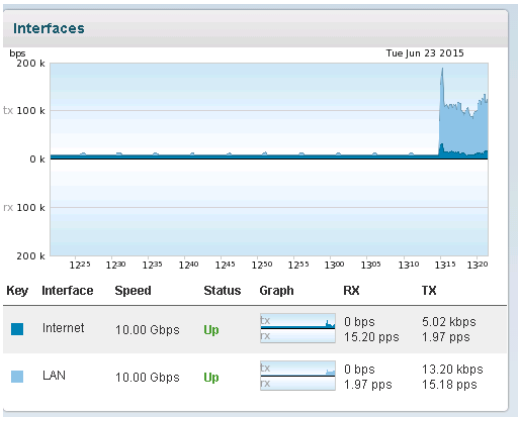
Switch back to the Arbor GUI, and also open up the sharewatch IE window, in a few minutes, the server will be unavailable as the session state table will consume all resources (you may have to hit refresh a few times)

On the APS GUI, you should see a large amount of traffic attacking the server, and you sould also be able to see where those attacks are originating from and the interfaces it is affecting :

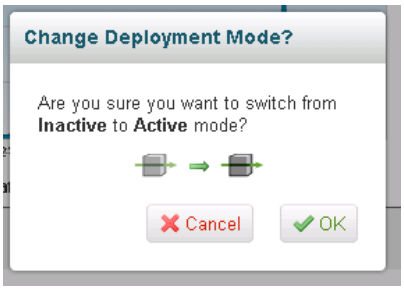






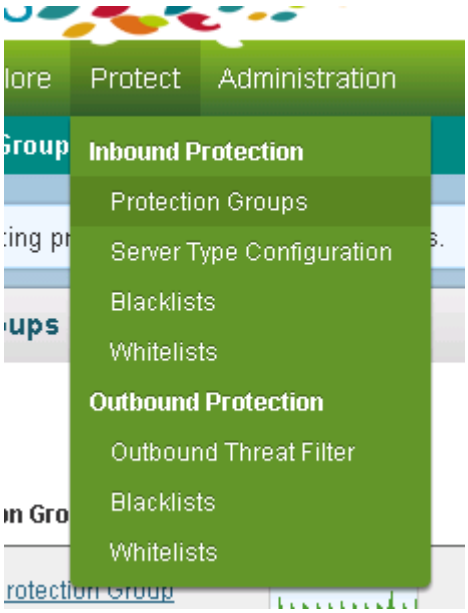


To mitigate against the attack, change the mode to ACTIVE in the top right corner of the gui:



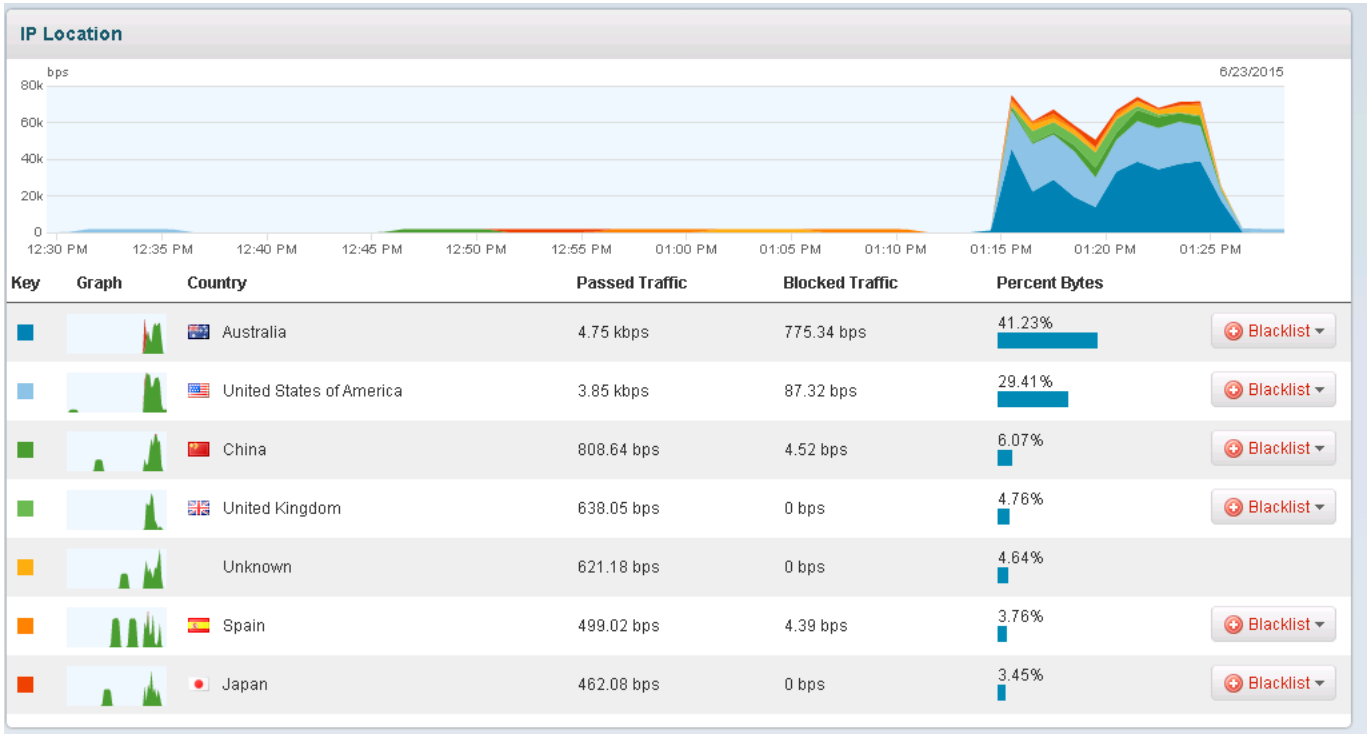
©Zycko Ltd 2010

You can explore the attack in a bit more depth by clicking into the protection group:



Choose the "Sharewatch Servers" group and look at the metrics:

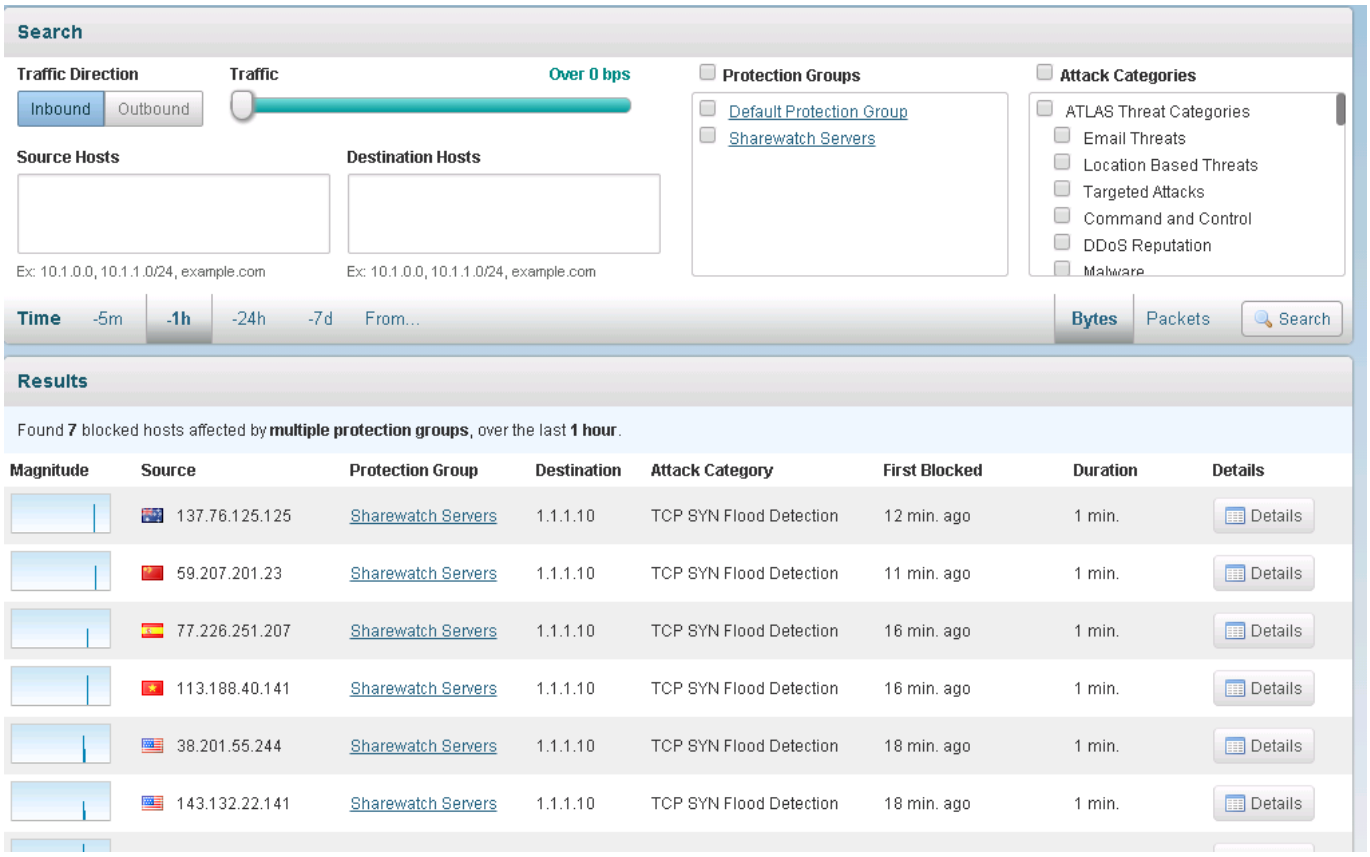
IP Location is a good metric to look at, and you can actively blacklist countries:



Key	Graph	Country	Passed Traffic	Blocked Traffic	Percent Bytes	
		Australia	4.75 kbps	775.34 bps	41.23%	Blacklist
		United States of America	3.85 kbps	87.32 bps	29.41%	Blacklist
		China	808.64 bps	4.52 bps	6.07%	Blacklist
		United Kingdom	638.05 bps	0 bps	4.76%	Blacklist
		Unknown	621.18 bps	0 bps	4.64%	
		Spain	499.02 bps	4.39 bps	3.76%	Blacklist
		Japan	462.08 bps	0 bps	3.45%	Blacklist

Commercial in Confidence
©Zycko Ltd 2010

You can also look at the active blocking list (Blocked Hosts) during the attack:



It will take 5-10 minutes for the sessions on the web server to recover, but you should be able to see that the web site will recover again.

When it does, stop the attack on the DDoS screen.

©Zycko Ltd 2010