Subject: OT: ApocMedia
Posted by glyde51 on Sat, 19 Mar 2005 05:41:05 GMT
View Forum Message <> Reply to Message

I have anti-hacking stuff, 20 bad requests and you get banned for an hour

Quote:Anti-Hacking Protection

Although Abyss Web Server is secure and has an integrated system to prevent malicious accesses to the server, it was equipped with an automatic anti-hacking protection system to detect clients that are trying to attack the server and to ban them. This system improves the overall security, detects at an early stage denial of service attacks, and saves the bandwidth that could be wasted during attacks.

To configure the anti-hacking system, select Anti-Hacking Protection in the Server Configuration dialog.

The displayed dialog is made of the following items:

* Enable Automatic Anti-Hacking Protection: Check it to enable the automatic anti-hacking protection system.
* Do not monitor requests from: This table contains the IP addresses or IP address ranges that should not be protected against hacking. Refer to "IP Addresses and Ranges Format" appendix for more information about the IP addresses and ranges. Fill this table with trusted IP addresses only.
* Bad requests count before banning: The number of tolerated bad requests before considering the client as attempting to hack the server. A request that results in a reply which HTTP status code is 400 or 401 is counted as a bad request. A request that results in a reply which HTTP status code is 403, 404, 405, or 408 is counted as half a bad request.
* Monitoring Period: The server considers only the bad requests that are generated by a client during the last Monitoring Period to decide whether to ban it or not. The bigger this parameter is, the more memory the anti-hacking system needs to record all the bad requests.
* Banning Duration: How much time a client is banned when it is considered as hacking the server.

In other words, the anti-hacking system works as follows: If a client has generated Bad requests

count before banning bad requests during the last Monitoring Period seconds, then ban it for the next Banning Duration seconds. When a client is banned, the server will not accept connections from it.

Note:: The server preserves the list of banned clients when it is shutdown. So if a client was banned for 2 hours at 10:00, and if the server was stopped at 10:15 and restarted at 11:00, the server will continue to not accept requests from the banned client until 12:00.
