使用过滤的GREP访问日志

目录

问题：

环境：思科Web安全工具(WSA)， AsyncOS所有版本

如何能搜索访问注册S系列设备？

从Cisco Web安全工具的命令行界面，您能使用**grep命令**过滤访问日志和确定什么阻塞。这是显示阻塞的所有的示例：

TestS650.wsa.com () **> grep**

目前配置的日志：
1. “accesslog”类型：“访问记录”检索：FTP投票
<… >
18. “welcomeack_logs”类型：“欢迎使用页确认日志”
检索：FTP投票

输入您希望对grep日志的编号。
[]**> 1**

输入常规表示对grep。
[]**> BLOCK_**

是否希望此搜索是不区分的案件？[Y] **> n**

是否要盯梢日志？[N] **> n**

是否要上页数输出？[N] **> n**

(条目将显示)

对于常规表示问题，您能输入**BLOCK_** (没有报价单)表示每请求， WSA阻塞。(警告：此列表可以非常长)。

如果要显示与一个特定站点，涉及的访问长条目您能也输入站点URL的部分。例如-输入常规表示的**windowsupdate将**显示您包含windowsupdate.microsoft.com的Windows更新URL所有访问日志条目。

变得更加先进，如果要显示一个站点的访问日志条目有在URL的windowsupdate的，也阻塞，您可能使用常规表示 windowsupdate.*BLOCK_。