GREP를 사용하여 액세스 로그 필터링

목차

질문:

환경:Cisco WSA(Web Security Appliance), 모든 버전의 AsyncOS

S 시리즈 어플라이언스에서 액세스 로그를 검색하려면 어떻게 해야 합니까?

Cisco Web Security Appliance의 명령줄 인터페이스에서 grep 명령을 사용하여 액세스 로그를 필터링하고 차단되는 항목을 확인할 수 있습니다.다음은 차단 중인 모든 항목을 표시하는 예입니다.

—
TestS650.wsa.com ()> **grep**

현재 구성된 로그:
1."accesslogs" 유형:"액세스 로그" 검색:FTP 폴링
<...>
18. "welcome_logs" 유형:"시작 페이지 승인 로그"
검색:FTP 폴링

그리려는 로그 번호를 입력합니다.
[]> **1**

grep할 정규식을 입력합니다.
[]> **블록_**

이 검색을 대/소문자를 구분하지 않도록 하시겠습니까?[Y]> **n**

로그를 미닫으시겠습니까?[N]> **n**

출력을 페이징하시겠습니까?[N]> **n**

(항목이 표시됩니다.)
—

정규식 질문의 경우 BLOCK_(따옴표 제외)를 입력하여 WSA에서 차단한 모든 요청을 표시할 수 있습니다.(경고:이 목록은 매우 길어질 수 있습니다.)

특정 사이트와 관련된 액세스 긴 항목을 표시하려면 사이트 URL의 일부를 입력할 수도 있습니다.예 - **windowsupdate**를 정규식에 입력하면 windowsupdate.microsoft.com의 Windows Update URL이 포함된 모든 액세스 로그 항목이 표시됩니다.

좀 더 고급 기능을 사용하면 URL에 windowsupdate가 있는 사이트에 대한 액세스 로그 항목을 표시할 수 있습니다. 또한 차단되어 있는 경우 정규식 windowsupdate를 사용할 수 있습니다.*BLOCK_.