Usando o GREP para filtrar os logs do acesso

Índice

Pergunta:

Ambiente: Ferramenta de segurança da Web de Cisco (WSA), todas as versões de AsyncOS

Como posso eu procurar o acesso entro o dispositivo da série S?

Da interface da linha de comando da ferramenta de segurança da Web de Cisco, você pode usar o **comando grep** filtrar os logs do acesso e determinar o que está sendo obstruído. Está aqui um exemplo para mostrar a todo o que está sendo obstruído:

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

Logs atualmente configurados:
1. tipo dos “accesslogs”: “Alcance recuperação dos logs”: Votação FTP
<… >
18. tipo dos “welcomeack_logs”: Da “logs do reconhecimento página de boas-vindas”
Recuperação: Votação FTP

Incorpore o número do log que você deseja ao grep.
[]> **1**

Incorpore a expressão regular ao grep.
[]> **BLOCK_**

Você quer esta busca ser não diferenciando maiúsculas e minúsculas? [Y] **> n**

Você quer atar os logs? [N] **> n**

Você quer paginar a saída? [N] **> n**

(as entradas serão indicadas)

Para a pergunta da expressão regular, você pode incorporar **BLOCK_** (sem as citações) para mostrar a cada pedido que WSA obstruiu. (Advertindo: esta lista pode ser muito longa).

Você pode igualmente incorporar partes do local URL se você quer indicar as entradas longas do acesso relativas a um local específico. Por exemplo - Incorporar o **windowsupdate** para a expressão regular mostrar-lhe-á todas as entradas de registro do acesso que contêm Windows

Update URL de windowsupdate.microsoft.com.

Obtendo um pouco de mais avançado, se você quis indicar as entradas de registro do acesso para um local com windowsupdate na URL, que foram obstruídas igualmente, você poderia usar a expressão regular windowsupdate.*BLOCK_.