Содержание

Вопрос:

Среда: Cisco Web Security Appliance (WSA), все версии AsyncOS

Как я могу искать вход в систему доступа устройства серии S?

От интерфейса командной строки Cisco Web Security Appliance можно использовать **команду grep**, чтобы фильтровать журналы доступа и определить то, что блокируется. Вот пример для показа всего, что блокируется:

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

В настоящее время настраиваемые журналы:
1. тип "accesslog": "Извлечение" журналов доступа: опрос FTP
<...>
18. тип "welcomeack_logs": "Журналы подтверждения страницы приветствия"
Извлечение: опрос FTP

Введите номер журнала, которого вы желаете к grep.
[]> **1**

Введите регулярное выражение в grep.
[]> **BLOCK_**

Вы хотите, чтобы этот поиск был нечувствителен к регистру? [Y]> **n**

Вы хотите выследить журналы? [N]> **n**

Вы хотите разбить на страницы выходные данные? [N]> **n**

(записи будут отображены),

Для вопроса о регулярном выражении можно ввести **BLOCK_** (без кавычек) для показа каждого запроса, что заблокировался WSA. % Warning: этот список может быть очень длинным).

Если вы хотите отобразить доступ длинные записи, отнесенные к определенному узлу, можно также ввести части URL узла. Например - Ввод **windowsupdate** для регулярного выражения покажет, что вы все обращаетесь к записям журнала, содержащим URL Windows Update windowsupdate.microsoft.com.

Будучи немного более усовершенствованным, если вы хотели отобразить записи журнала

доступа для узла с windowsupdate в URL, которые были также заблокированы, вы могли использовать регулярное выражение **windowsupdate. *BLOCK_**.