GREP を使用したアクセス ログのフィルタリング

目次

質問：

環境： Cisco Web セキュリティ アプライアンス（WSA）、AsyncOS のすべてのバージョン

どのようにログオンします S シリーズ アプライアンスをアクセスを検索できますか。

Cisco Web セキュリティ アプライアンスのコマンド ライン インターフェースから、アクセス ログをフィルタリングし、ブロックされているものが判別する **grep コマンドを**使用できます。 ブロックされていることをすべてに示す例はここにあります:

TestS650.wsa.com（ ）> **グレップ**

現在設定されたログ:
1. 「アクセスログ」型: 「ログ」に検索アクセスして下さい: ポーリングを FTP して下さい
<... >
18. 「welcomeack_logs」型: 「ウェルカム画面 確認応答ログ」
検索: FTP ポーリング

グレップに希望するログの数を入力して下さい。
[] > **1**

グレップに正規表現を入力して下さい。
[] > **BLOCK_**

Do you want this search to be case insensitive?（この検索で大文字小文字を区別しますか？）[Y] > **n**

Do you want to tail the logs?（ログの最後を表示しますか？）[N] > **n**

Do you want to paginate the output?（出力をページングしますか？）[N] > **n**

（エントリは表示されます）

正規表現質問の場合、WSA がブロックしたことを（引用符なしで）各要求に示すために **BLOCK_ を**入力することができます。 （警告します: このリストは非常に長い場合もあります）。

特定のサイトに関するアクセス長いエントリを表示したいと思う場合またサイト URL の一部を入力することができます。 たとえば-正規表現用の **windowsupdate を**入力することは windowsupdate.microsoft.com の Windows アップデート URL が含まれているすべてのアクセス Log エントリを示します。

またブロックされた URL の windowsupdate が付いているサイトのためのアクセス Log エントリを表示したいと思ったらやや高度になって、正規表現 **windowsupdate.*BLOCK_を**使用する可能性があります。