Usando el GREP para filtrar los registros del acceso

Contenido

Pregunta:

Entorno: Dispositivo de seguridad de la red de Cisco (WSA), todas las versiones de AsyncOS

¿Cómo puedo buscar el acceso abro una sesión el dispositivo de la serie S?

De la interfaz de línea de comando del dispositivo de seguridad de la red de Cisco, usted puede utilizar el **comando grep** de filtrar los registros del acceso y de determinar se está bloqueando qué. Aquí está un ejemplo para mostrar a todo el que se está bloqueando:

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

Registros actualmente configurados:
1. tipo de los “accesslogs”: El “acceso registra” la extracción: Encuesta FTP
<… >
18. tipo de los “welcomeack_logs”: “Registros del acuse de recibo de la página de Bienvenida” Extracción: Encuesta FTP

Ingrese el número del registro que usted desea al grep.
[]**> 1**

Ingrese la expresión normal al grep.
[]**> BLOCK_**

¿Usted quisiera que esta búsqueda fuera sin diferenciación entre mayúsculas y minúsculas? [y] **> n**

¿Usted quiere atar los registros? [n] **> n**

¿Usted quiere paginar la salida? [n] **> n**

(las entradas serán visualizadas)

Para la pregunta de la expresión normal, usted puede ingresar **BLOCK_** (sin las citas) para mostrar a cada petición que WSA ha bloqueado. (Advirtiendo: esta lista puede ser muy larga).

Usted puede también ingresar el sitio URL de las partes de si usted quiere visualizar las entradas largas del acceso relacionadas con un sitio específico. Por ejemplo - Ingresar el **windowsupdate** para la expresión normal le mostrará todas las entradas de registro del acceso que contienen la actualización URL de Windows de windowsupdate.microsoft.com.

Consiguiendo un poco más avanzado, si usted quiso visualizar las entradas de registro del acceso para un sitio con el windowsupdate en el URL, que también fueron bloqueadas, usted podría utilizar la expresión normal **windowsupdate.*BLOCK_**.