Tools
for Windows

User Manual

Cyber Operations
https://www.CyberOperations.com
1449 Court Place
Pelham, AL 35124
Ph: 205-733-0901

Table of Contents

Introduction

Thanks

Thank you for choosing ***FLM Tools***, a desktop companion to ***FLM.*** We hope you enjoy its powerful features for managing your organizations network access control list policies. Please let us know if there is any way you feel this product, its documentation, or its support could be improved to better meet your needs.

About FLM

FLM is a system which allows your organization to store, control, and implement all of your organization's network access policies for different brands and types of networking devices from one centrally managed database with revision history and access control. It also provides you advanced tools for creating, analyzing, and deploying your access control policies, including comparison, searching, conflict detection, hierarchal lists, and simultaneous synchronization of devices with the database. The web-based interface allows access from any platform, and allows you to configure the system to suit your organization's needs.

System Requirements

OS: Windows 10 or newer
Hardware: Intel 64bit

Additional Resources

Additional, current information is available on our website:
https://www.cyberoperations.com

Updating FLM Tools

The latest version of FLM Tools can be downloaded here:
https://www.cyberoperations.com/FLM-Tools.exe

Link to SHA-512 checksum:
https://www.cyberoperations.com/FLM-Tools.sha512.txt

FLM Tools Features

List Basics

Access lists, also known as ACL's, consist of a sequence of entries, each of which specifies whether a certain type or group of packets will be permitted or denied through the filter. **FLM Tools** maintains your access lists in a platform independent format for you so that they can be easily sent to different device types, typically a router or firewall.

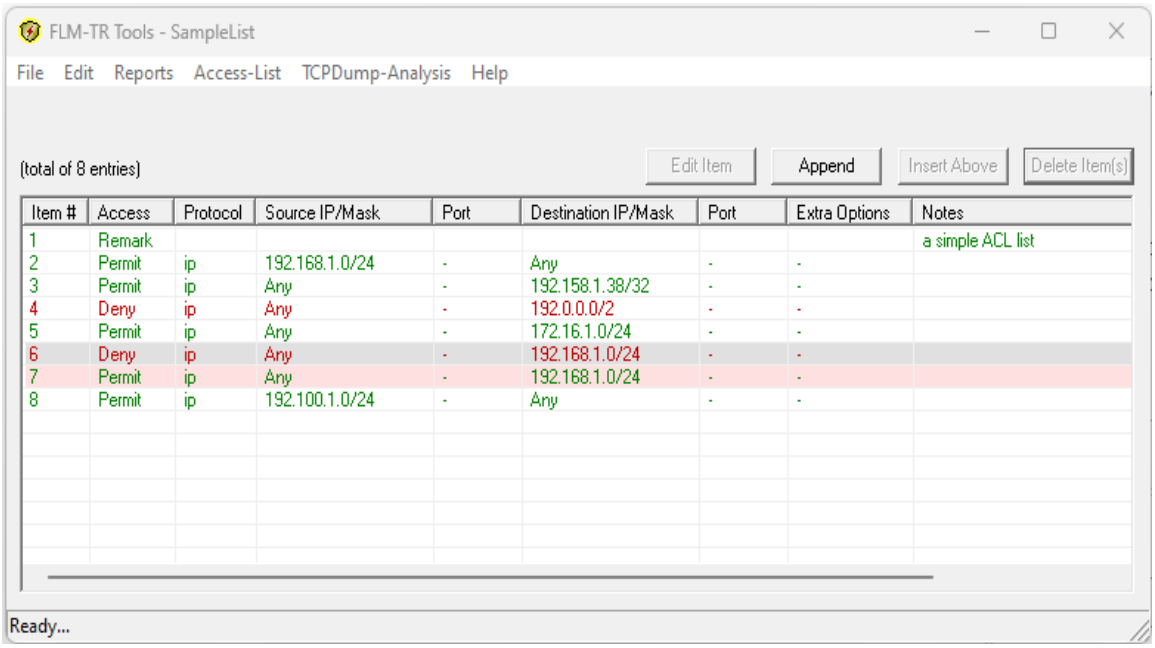

Figure 1 – Access List

Edit Access List

Cut / Copy / Paste

The list supports standard cut, copy, and pasting of input with both key shortcuts and as options from the Edit menubar.

Conflicts and Entries With No Effect

FLM highlights entries which have no effect with a gray background color, and if you open the entry for editing it will tell you the issue which causes the highlighted entry to have no effect.

Likewise, entries which conflict with other entries are highlighted using a pink background. An example of a conflicting entry would be trying to permit traffic that was completely blocked by an earlier entry. If you open the entry for editing it will tell you the issue which causes the highlighted entry to have a conflict.

Searches

There are two different types of searches supported by the system. Find, which is a powerful feature with specific parameters for entry fields, and Find Text, which allows you to search the textual representation of a list.

Edit > Find...

enter in the packet data as specific as possible / source ip , port, etc. click "Intersection Entries" Once you have entered all of your search parameters click the “Find Next” button and dialog will close with all matching entries highlighted in light gray.

Edit > Find Text

The textual search feature allows you to regular expressions to search the textual representation of the list entries. The regular expressions syntax used is that of POSIX 1003.2, and all expression matching is case insensitive. Enter the string or regular expression you wish to search for in the text field to the left of the “Search” button; then click “Search”. All matching entries will be shaded with a light gray background. Below are some examples of regular expression for searching:

- **permit.*udp** – This would match any entry containing the text “udp” somewhere after the text “permit”. The ‘.’ Represents a wildcard matching any character, and the ‘*’ indicates match zero or more of the preceding value.
- **port** – This would simply match any entry containing the port keyword.
- **(tcp)|(udp)** – This would match all entries containing the word “tcp” or the word “udp”

List Comment

Similar to a header, this is an optional comment line for the access list.

Access-List

Load From Router Configuration

You can import an existing list from a junos file, cisco file etc. This router configuration should be in a text file. Choose **Access-List > Load From Router Configuration...** on the menu bar.

Simplify

This feature gets rid of unneeded entries to make the list smaller. It combines entries where possible, but it doesn't change if a packet is permitted or denied.

Merge

Merging is a beneficial tool that combines the entries of two separate access lists and results in one combined list. Note that merging requires a file or access list to already be created and saved in a folder. The manner in which the merge function handles special cases is dependent upon the merge option(s) selected. Details regarding these options are explained below.

Choose **Access-List > Merge ACL into this ACL…**

The following window appears.

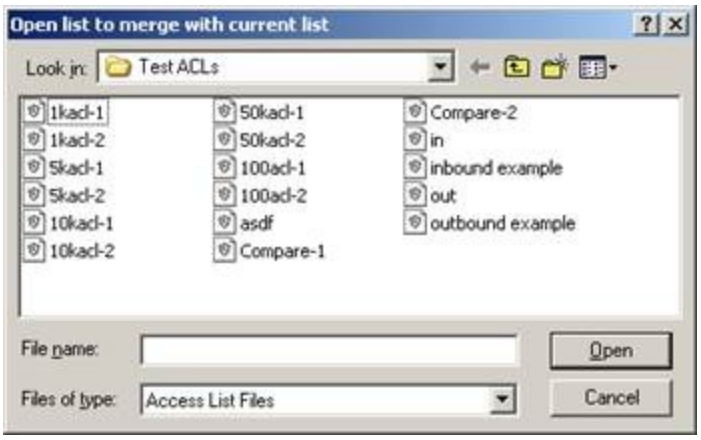

Figure 2 - Select Access List to Merge with Existing Access List

Select the file to be merged with the current list.

Click **Open**. The following **Merge Options** window appears.

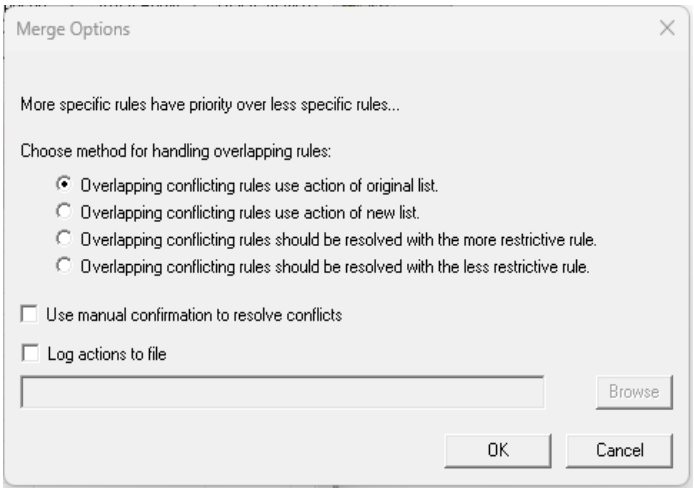

Figure 3 - Merge Options Window

the user will be presented with a set of four options to choose how conflicts will be resolved. These options are:

1. **Overlapping conflicting rules use action of original list.**
2. **Overlapping conflicting rules use action of new list.**
3. **Overlapping conflicting rules should be resolved with the more restrictive rule.**
4. **Overlapping conflicting rules should be resolved with the less restrictive rule.**

If option 1) is selected, then rules in the original list will take precedence over rules in the second input list when there is a conflict.

If option 2) is selected, then rules in the second input list will take precedence, instead, over rules in the original list when there is a conflict.

If option 3) is selected, then the more restrictive rule will take precedence when there is a conflict between the two input lists, regardless of which list it originates from.

If option 4) is selected, then the less restrictive rule will take precedence when there is a conflict, regardless of the list it originates from.

1. There are two check box options which may be enabled:

   a. Use manual confirmation to resolve conflicts.

   b. Log actions to file.

Option a) allows the user to resolve conflicts as they arise. When a conflict arises, the user will be shown the following dialog:

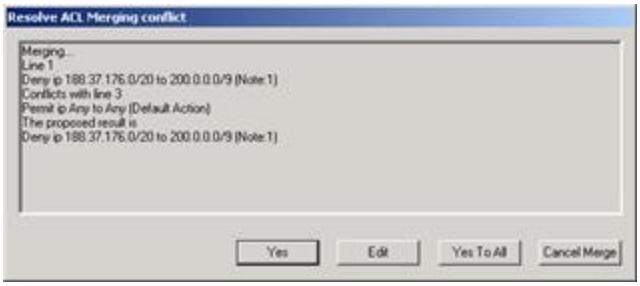

Figure 4 – Resolve ACL Merging Conflict

The user may accept the proposed solution by clicking **Yes**, or **Edit** the entry to resolve it manually. The user may also select **Yes To All** to automatically answer all future conflicts in the merge as **Yes**. Lastly, the entire merge operation may be canceled by clicking the **Cancel Merge** button.

Option b) allows the user to log all actions that take place during a merge. The user is prompted to enter a file name and select the folder location. The file saves a description of all actions taken as a text file (.txt).

Reports

FLM-Tools supports three types of reports, CIDR and network, conflict, and compare two acl files. Reports are viewed in a separate window generated from the navigational menu. Reports can be printed or saved in a text file.

CIDR and Network Report

You can enter one or more IP address or network and this will list relevant entries in a report.

Conflict Report

A report that identifies the status of all highlighted lines and the cause of each.

Figure 5 – Conflict Report

Comparing Access Lists

You can compare any two access lists with FLM Tools. Choose **Reports > Compare two ACL Files...** on the menu bar. You will be propted to open each of the access lists to compare. A report page detailing the differences between the two access lists will be automatically generated.

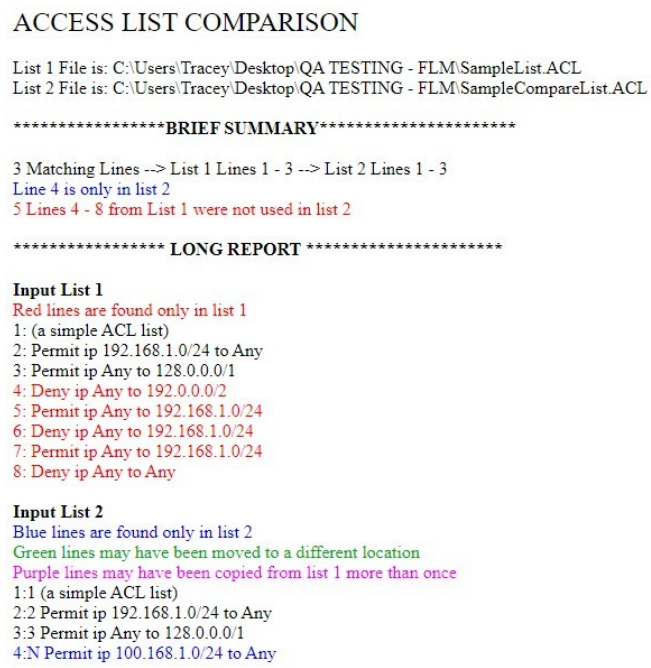

Figure 6 – Access List Comparison

TCPDump-Analysis

Speed Analysis

The "Speed Analysis" option in FLM Tools provides information including the average number of filter list entry lines required to process the packets. This number is a very good metric for determining the speed efficiency of the access list. The lower the average line count, in general, the more packets can be handled by the filter in the router.

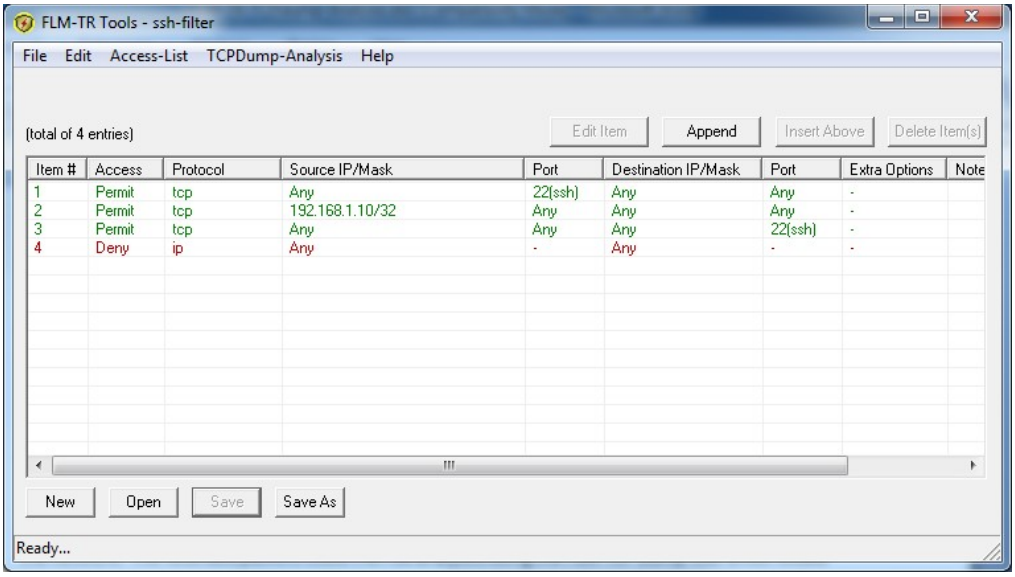

Figure 7 – Sample List For Speed Analysis

After Choosing "Speed Analysis" the following window opens and packets are ready to be loaded:

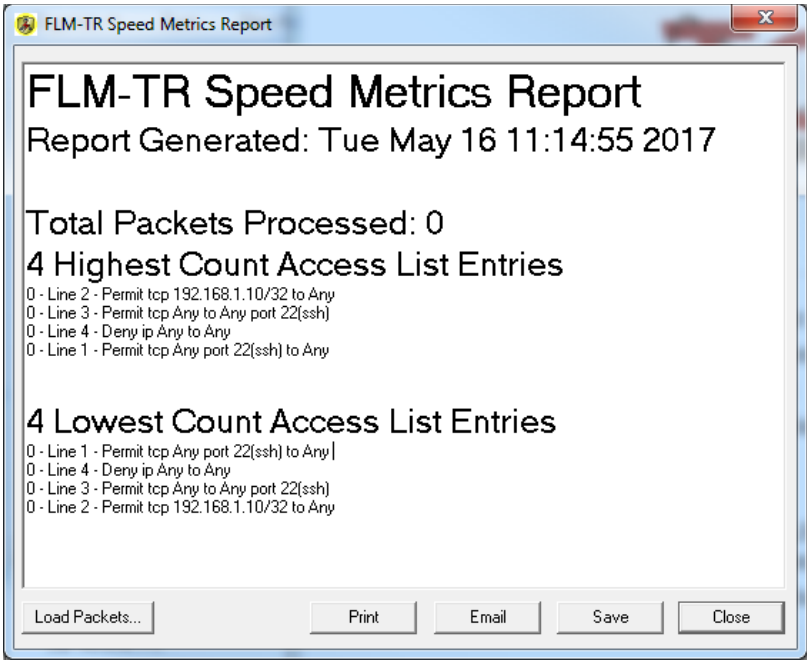

Figure 8 – Speed Metrics Report

After pressing the "Load Packets" button, the tcpdump file is opened and the packets are processed. The report in the window now shows the highest and lowest count entries and the average lines used per packet.

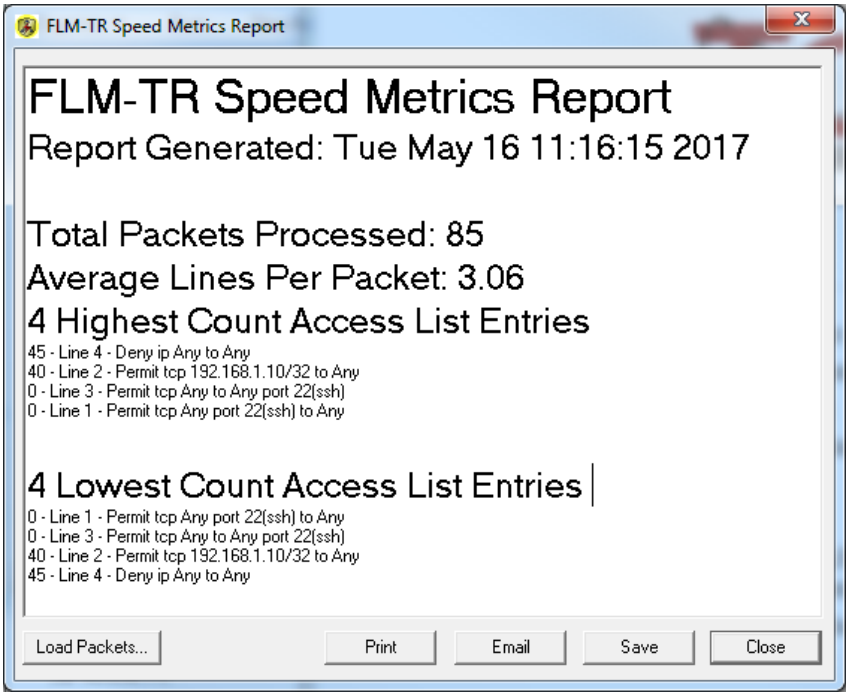

Figure 9 – Speed Metrics Report After Loading Packets

In general the highest count lines would be moved up as far as possible and the lower count lines would be moved down as far as possible in order to reduce the average lines per packet. The packets could then be processed again to show improvement.

Speed Optimize

The speed optimize option can be used to automatically optimize an access list. After selecting "Speed Optimize" from the menu, a packet dump file is chosen. FLM processes the packet file and moves access list entries up or down in the list to improve efficiency. This function will not move an entry in a way that would change the logic of the access list.

The following is a sample report from the "Speed Optimize" function:

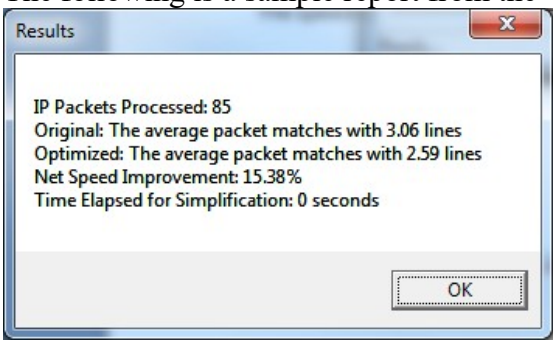

Figure 10 - Results

The new list shows that entry 2 was moved upward to entry 1.

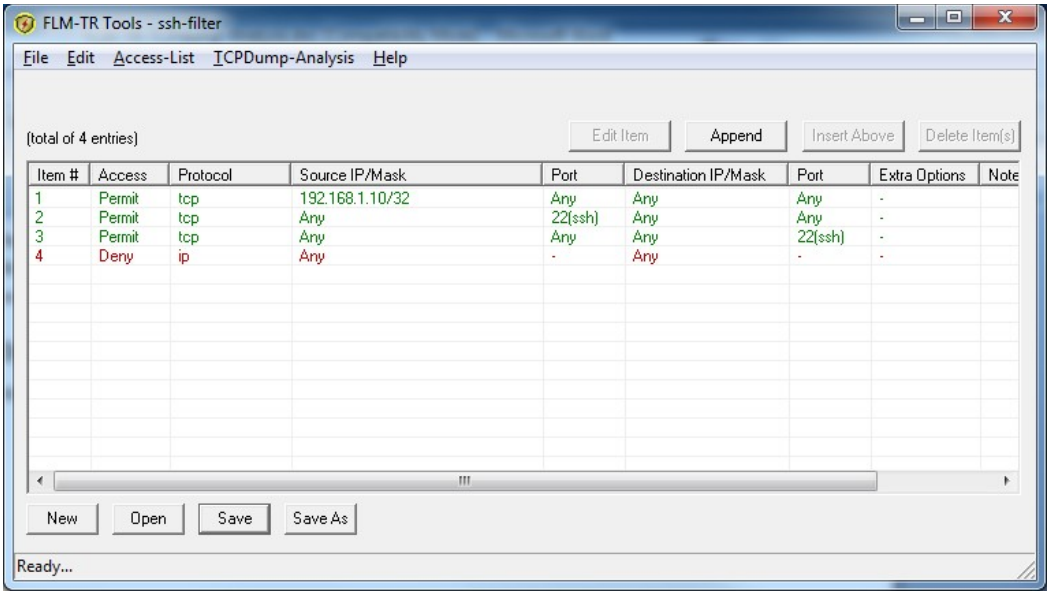

Figure 11 – List After Speed Optimization

Exporting

ACL's can be exported to several formats (JUNOS, Cisco IOS, CSV, and TXT) by clicking one of the Export options in the File menubar.

Support

Please contact us if this manual does not answer your questions, or if you experience any problems while using ***FLM Tools.***

Technical Support

Monday - Friday, 8am - 5pm CST

24 x 7 Support Contracts Available

Phone: 205-733-0901

Website: www.CyberOperations.com

Cyber Operations

INTEGRATED SECURITY TECHNOLOGIES