Cyber ACL
Access Control Lists

User Manual

Cyber Operations Inc.
http://www.CyberOperations.com
153 Cahaba Valley Parkway
Pelham, AL 35124
Ph: 205-403-2923
Fax: 205-403-6508

Table of Contents

Introduction

Thanks

Thanks for choosing **CYBER ACL**, and we hope you enjoy its powerful features for managing your organizations network access 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 CYBER ACL

CYBER ACL 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

Processor/OS: Sparc/Solaris or Intel/Linux.
Hardware: The processing / RAM / disk drive requirements may vary depending on the expected usage.
Database: Oracle or PostgreSQL
Authentication/Authorization: TACACS+, Radius, or LDAP. Also, CYBER ACL can be configured to use local accounts or it can use its own internal Authentication system.
Webserver: Typically apache 2.x but is compatible with most others. CAC/PKI supported.
Devices: Cisco IOS based routers, Juniper routers, Cisco PIX firewalls, Cisco ASA devices, Aruba mobility controllers, Force 10 routers, and Netscreen firewalls. You can also control your organization's iptables and deploy via Cyber Operations FLM-ANT sensors.
Communication to Devices: SSH, SCP, Telnet, TFTP
Logging: Syslog compatible. Many other options are configurable.
Notifications: SNMP traps and Email Notifications

Customization is available. If you have integration requirements for other Linux distributions or UNIX variants, you require the use of another database system, you need to integrate with a different authorization system, or you need support for another type of router or firewall please contact us at Cyber Operations so that we can assist you.

Additional Resources

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

Setup

CYBER ACL Installation

Installing **CYBER ACL** on a server consists of unpacking the gzip'ed tar file containing the distribution, then running the provided install script. Below is an example of the required commands you would need to run with root access.

  gunzip acl.tar.gz
  tar –xvf acl.tar
  cd acl
  ./installacl

This will install to the directory **/usr/local/acl**.

NOTE: All relative path names used in this manual are from the ***/usr/local/acl*** directory.

Read the file **INSTALL** for detailed information on setup and configuration.

Updating CYBER ACL

CYBER ACL has a built-in auto-update mechanism. To check for and install an upgrade to the system, run the command:

cgi-bin/aclserver update.

To install from a file rather than over the internet:
cgi-bin/aclserver update <update-file>

System Configuration

By default, the system configuration file is:
/etc/aclserver.conf
Override this file by creating */usr/local/acl/aclserver.conf*
For future reference, the original is located at */usr/local/acl/aclserver.conf.original*

Use the configuration file to set up the database, authentication, logging, and many other options. **You must set up the database and authentication in the configuration file in order to use CYBER ACL!**

The config file uses standard syntax:
Key=Value
 # Lines starting with # are comments

Syntax Notes:
Keys are case insensitive
Fields that are a time duration understand the words: "second", "minute", "hour", "day", "month", "year"
AuthIdleTimeout = 90 minutes
          is the same as:
AuthIdleTimeout = 1 hour 30 minutes
Fields that are a server address can use dot notation or domain name.

Setup the Database

After the database is configured, run the following command to initialize with the tables that CYBER ACL will need.

cgi-bin/aclserver database init

Setup the Web Server

Set the root directory to **/usr/local/**acl/html and the cgi-bin directory to **/usr/local/acl/cgi-bin.**

This example uses Apache:

In the **httpd.conf** file:

> *DocumentRoot "/usr/local/acl/html"*
>
> *<Directory "/usr/local/acl/html/">*
>   *AllowOverride None*
>   *Options None*
>   *Order allow,deny*
>   *Allow from all*
> *</Directory>*
>
> *ScriptAlias /cgi-bin/ "/usr/local/acl/cgi-bin/"*

<Directory "/usr/local/acl/cgi-bin">
  AllowOverride None
  Options None
  Order allow,deny
  Allow from all
</Directory>

Run the command:
apachectl restart

Configure Authorization

When the user begins an action, an Authorization request is sent to the AAA server.

For TACACS+ or Radius Authorization Use: <command> <argument>

Commands Are: read,write,sync

Arguments Are:
device: includes devices, interfaces, trackers,
deployment logs, deployment reports, and schedules
acl: includes ACL's, networks, services, groups,
ACL tests, ACL logs and ACL reports
admin: includes global device account, email notifcations and administrative tasks
includes user settings in 'db' or 'unix' AuthType mode

When AuthType is set to "db" or "unix", users and authorization can be configured from the "Admin" menu of CYBER ACL.

For Radius use:
Attribute: 26 (Vendor Specific)
Vendor: 9 (Cisco)
Sub-Type: 1 (avpair)

set allowcmds to a comma separated list of allowed commands

for a read only user:
allowcmds=read acl, read device

also you can use wildcards

allowcmds=*

Access Lists

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. CYBER ACL 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

Conflicts and Entries With No Effect

CYBER ACL highlights entries which have no effect with a gray background color, and if you let your cursor hover over the entry it will show you the index of the entry which causes the highlighted entry to have no effect.

Likewise, entries which conflict with other entries are highlighted using a darker, nearly black background.   An example of a conflicting entry would be trying to permit traffic that was completely blocked by an earlier entry. If you let your cursor hover over the entry it will show you the index of the entry which causes the conflict.

Importing

From the "List Entries" page you can also import entries from existing access lists, or export access lists.

You can also click the "Import Access Lists" link from the navigation menu which will give you a larger selection of options when importing, as well as the ability to import all lists from configuration sources containing multiple access lists. From the Import page, you can also import directly from the device.
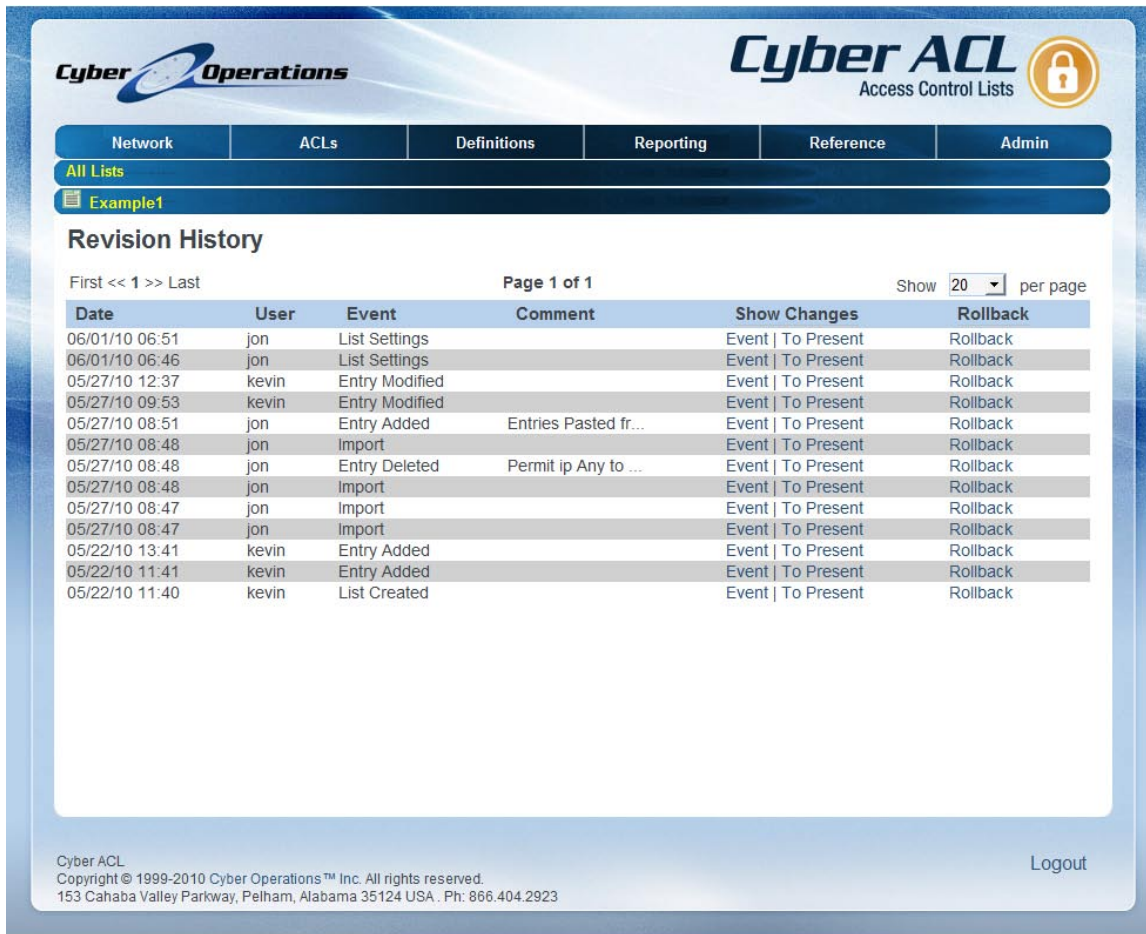

Figure 2 - Importer

If you are importing from a file that contains more than one access list you will be presented with a menu to select which access list you would like to import.

Exporting

ACL's can be exported to several formats by clicking one of the Export options in the Export Navbar from the Edit Access List page.

History and Rollback

There is an automatic history maintained of all changes made to each access list in **CYBER ACL**. In order to access this history, click the link titled "Revision History" Navbar from the Edit Access List page.

Figure 3 – Revision History

Comparing Access Lists

You can compare any two access lists within CYBER ACL. Go to the "Edit List" page of the first access list you would like to compare, select the second access list from the popup menu by clicking on the "Compare List" link in the Navbar. You will be presented with a page detailing the differences between the two access lists.

Figure 4 – Access List Comparison

The revision history page will present you with a history of modifications to the list from most recent to least recent. If you click on the date or event columns of a change, you will be taken to a comparison of the list immediately prior and immediately after the change. If you click the "Rollback" link for a change, the list will be rolled back (restored) to its state immediately prior to that change.

A list that has been deleted can be restored with the Rollback feature.

Using Sublists

In addition to regular access list entries, you can also add references to other lists, known as sublists. Whenever the list is sent to a device (synchronized), the actual sublist will be substituted in place of the sublist entry. This works recursively, which means that the sublist may itself have sublists.

This feature is very useful if you have some common rules for multiple devices and interfaces, but you also have rules which may be common across some are all of your

interfaces. You can create a sublist containing the entries which are common across a group of interfaces, then have each interface's list include your common list as a sublist. Whenever your common list is modified, any interface with a list that includes it as a sublist will automatically be marked in need of synchronization.

Figure 5 - A Sublist

Defining Groups, Networks, and Services

CYBER ACL allows you to create custom defined values which can be used from within your access lists to more easily manage your network access policies. These consist of Networks, Services, and Groups. Networks are predefined combinations of network address ranges; services are combinations of ports and port ranges; and groups are combinations of devices, targets, and other groups which also allow you to define an access list to be included by each group member automatically.

Networks

CYBER ACL allows you to create Network definitions which can then be used within access lists. The currently defined networks can be viewed by clicking on the "Networks" navigation link.

Figure 6 – Network Setup

The "Add Network Address" link will prompt you for a network and mask as well as a comment for the network address you are adding. Additionally, there will be a menu allowing you to select whether this address will be included in or excluded from your network definition. For example, you could create a network definition that included all of the 10.0.0.0 class A private IP block except for the class C beginning with 10.0.1 by adding the address and mask 10.0.0.0/8 to be included, and adding the network address and mask 10.0.1.0/24 to be excluded.

Network Overrides

You can override a network's definition for a specific device or specific interface so that when an ACL is sent to (synchronized with) that interface or device, the device or interface specific definition is used instead of the global definition.

If a device and an interface both override a network definition, then the interface definition will take precedence.

To view or edit the network definitions for a device or interface click the network under "Override These Networks" on the "Device Setup" or "Interface Setup" page respectively.

Services

The services feature allows you to define groups of ports and port ranges that can be used when defining access list entries. To view defined services click on the "Services" link from the navigation menu.

A port or port range can be added to a service definition by clicking the "Add Service" link. You will be asked to select "Include" or "Exclude", indicating whether you want this port or port range included or excluded from your service definition. You will also need to enter the service name, port number, or range, etc. in the "Service or Port Range" field. You can also enter a descriptive comment in the "Comment" field. Click save when you are through entering the fields to return to the "Edit Service" page.

Groups

Groups are custom defined combinations of devices, interfaces, and other groups which also allow you to define an access list to be included by each group member automatically.

You can view your groups by clicking on the "Groups" navigation link. Clicking the "Add New Group" link takes you to the edit group after you enter a name for your group in the given field.

On the "Edit Group" page there are three tabbed areas. The "Devices" area allows you to add or remove devices to your group. The "Interfaces" area allows you to add or remove interfaces to your group. Finally, the "Groups" area allows you to add other groups to your group, effectively nesting them within one another.

Within each tabbed area the left area labeled "Members" shows the items that are currently included in the group, and the right area labeled "Non-Members" shows all items that are not included.

To add items select them on the right side under "Non-Members" and click the "Add" button. To remove items select them on the left side under "Members" and click the "Remove" button. You can select multiple items at a time for adding or removing.

You can remove all items from the group or add all items by clicking the "Remove All" or "Add All" buttons respectively.

When you have finished including devices, interfaces, or other groups in your group click the "Save" button to save your new group.

Figure 7 – Group Setup

Groups each have an associated access list. From the "Edit Group" page this access list can be accessed by clicking the "Group Common ACL Entries" link. This will take you to the "Edit ACL" which is discussed in the section "Access Lists" of this manual. The access list for a group is automatically included as a sublist of each member of the group. This means that any access list entry you add to a group's access list is effectively added to the access list of any device or interface included in that group, as well as any members of other groups included within that group.

Importing Existing Lists

You can import access lists from Cyber Operations internal format which is used by both *FLM-ANT* and *ACL Manager*, and you can also import lists from many router formats.

Using the Importer

If you need to import multiple access lists at a time or need more flexible options then you can use the importer interface by clicking the link "Import Access Lists" from the navigation menu. See the section "Importing" for more information.

Import Directly from a Device

You can import access lists directly from some types of devices. From the "Edit Device" page of the appropriate device you click the link "Import from Device" and you will be taken to the importer interface, but instead of requesting you to select a file you will be able to import directly from the device.

Dependencies

CYBER ACL allows you to view all lists which reference a specific list, service or network. On the "Access List", "Edit Network", and "Edit Service" pages use the "Referenced By" bar, with links on the right titled, "Any", "Lists", "Interfaces", "Devices", "Groups". Clicking on any one of these links will take you to the dependency browser page and will show you all lists of the selected type that reference that network, list or service.

For example if you went to the network "My Network" and clicked the "Groups" link across from "Referenced By" you would be shown all group access-lists which contained entries referencing "My Network". This also includes lists which include sublists that reference "My Network". Similarly, if you had clicked the "Any" link instead you would see access lists of any type referencing "My Network"

Working with Devices

Devices

Within **CYBER ACL** a *device* represents a physical networking device such as a router or firewall. For each device a description, internet address, and information required to access the device is maintained in the database.

A device also has an associated ACL which is automatically included as a sublist for each interface on the device. You can edit this list to add any entries that you want included for all interfaces.

Figure 8 – All Devices

When you click "Add New Device" you will be taken to a page asking you for the basic configuration values for the device. Below are the fields which you must enter to setup your device.

- **Description** – This will be the name of your device within *CYBER ACL.*
- **Type** – This menu allows you to select one of the supported device types.
- **Address** – This is the network address of the device. Specifically, the address of the interface on the device that *CYBER ACL* will use to communicate with the device.
- **Protocol** – For some devices, more than one communication protocol for interoperating with the device is supported. Select the protocol that you wish to use to communicate with the device. You must have the device configured to allow this protocol. See the table 'Protocols' for a more complete description of each option.
- **Folder** – Enter the path to be displayed on the Network Tree Page. Folders allow grouping of devices for easier management on the Network Tree. (Figure 10)
- **Device Authorization** – If 'Static' then the login and password are set on this page for this particular device. If 'Global Authorization', then the login password from the admin menu are used. If 'Prompt' then the operator is asked for a

password when synchronization is initiated. RSA Key Device Authorization is also supported.

- **Device Login Name** – The login name for the device if using static authorization.
- **Device Password** – Password when logging into the device using static authorization. This field is ignored when using an RSA key.
- **Enable Password** – Password to enable management features on the device. This does not apply to all device types. This is only used if using static authorization.
- **Advanced** – This lets you set more advanced configuration options that may also be specific to certain device types.

When you are through entering the values for your device, save it by clicking the "Save" button. In order to send an access list to a device, you must define one or more interfaces on that device.

Figure 9 – Device Setup

Figure 10 – Network Tree

Change Trackers

Creating a **Change Tracker** for a device allows you to automatically import a list from the device whenever it is modified on the device.
In order to create a Change Tracker, click the "New" link from the Change Tracking navbar on the Device Setup page, and then enter the name of the access-list or filter on the device in the "Device ACL Name" field and the name you want the imported list to have in the "Local List" field.

NOTE: Change Trackers are imported at regular intervals by the **aclserver** daemon so you will not see changes take effect immediately. The interval can be set on the Device Setup page for a specific device.

Interfaces

An **Interface** represents an interface and/or named ACL or filter on a device which can be used as a interface for synchronization. Whether a specific network interface is specified as part of an **Interface** depends on the type of device the **Interface** is on.

Figure 11 – Interface Summary

An **Interface** has an associated ACL which allows you to control the access list entries which are sent to the device each time it is synchronized. The device list of the parent device of the **Interface** is automatically included as a sublist in the interface list. You can add entries directly to the **Interface** list, or you can include other access lists as sublists.

Interfaces also support specifying a *device script*. A device script is a script you specify which can modify the access list for the device before it is sent to the device during synchronization. Device scripts are specified per **Interface** on the device. The device script must be in the *scripts* folder on the server running *CYBER ACL*. When the device script is called it will be passed the list, in the native syntax of the device as standard input via a UNIX pipe, and the output of the device script written to standard out will be used by *CYBER ACL* as the modified version of an access list to be sent to the device.

The directory *samples/sample_dev_scripts* contains some example device scripts for your convenience.

Figure 12 – Interface Setup

Device Type Specifics

The "Device Filter Name" and "Device Interface Names" take on different meanings depending on the type of parent device.

Device Type	Device Filter Name	Device Interface Names
Juniper JunOS	Specifies the firewall filter that will be created or modified in the JunOS configuration.	Not used.
Cisco IOS Cisco PIX Cisco ASA/PIX 7.x Aruba Force10 FTOS	Specifies the name of the access-list that will be created or modified in the IOS configuration.	Only used if device Protocol is "Telnet" or "SSH" and the "Device Interface Names" field is not blank, in which case it

Force10 E-Series Force10 SFTOS		specifies the router interface for a "ip access-group" or "ipv6 traffic-filter" command to be inserted into the interface configuration.
Netscreen	Not used.	Interface must specify the source and destination "zones" for the access list rules to apply to in the form <srczone>:<dstzone>.
iptables ip6tables	Not used.	Not used.

Figure 1 – Device Filter Name Usage

Dummy Devices

The device type 'Dummy Device' is a special type of device used for testing and experimenting with access-list policies when you do not want to use an actual network device.

Rotating Device Filter Names

Some devices have a smoother transition if the entire new access list is loaded before the interface is changed to the new ACL. For Cisco IOS, PIX, ASA, Aruba, and all Force 10 device types, it is possible to rotate the access-list used on the device. To take advantage of this feature, simply enter the access-list names you would like to use separated by a comma "," or semi-colon ";" in the "Device Filter" field.

Additionally, if you enter two numeric values or two names both ending in a number, then *CYBER ACL* will rotate through all the intermediate numbers as well.

Here are some examples:

firstName,secondName – Synchronizations will alternate between "firstName" and "secondName" as the access-list name on the device.
name101; name102; name103 – Synchronizations will cycle through name101, name102, etc. and wrap back around to name101.

IP v6 Access-Lists

For devices which support it, the 'IPv6' checkbox selects whether an IPv6 or IPv4 access-list is generated for the interface.

Standard versus Extended Access-Lists on IOS Devices

The 'Extended' option applies only to Cisco IOS and Aruba devices, and a standard access list is generated if this option is not checked. Also, if you specify a number for the access-list name, and this number falls into the ranges used by Cisco IOS for

numbered, standard access-lists, then a standard access-list will be generated instead of an extended list, regardless of the setting of the 'Extended' checkbox.

Standard access lists allow limiting traffic only based on the source address.

Traffic Direction

If the device protocol is 'SSH' or 'Telnet' and the device type is either Cisco IOS, Cisco ASA/PIX 7.x, or Aruba, then the Traffic Direction radio items will control whether the access-list is applied to inbound, outbound, or all (both) traffic.

Previewing Lists

It is possible to preview the device specific syntax generated for an **Interface's** access list without sending it to the device. To do so, click the Preview link from the Interface Setup page for the appropriate interface. This will take you to a page containing the textual list data that would be sent to the **Interface** during an actual synchronization so that you can preview any changes you have made.

Figure 13 - Preview ACL

Synchronizing

Within **CYBER ACL**, synchronization is the sending of the appropriate access list or lists to a **Interface** or **Interfaces**. For each **Interface** and its access list the system maintains synchronization times and modification times so that the system knows if a list or any of its sublists or any networks or services it references have been modified since the last time the interface was synchronized. When viewing the "**Interfaces**" page, each interface that needs to be synchronized will have an icon in the "Synchronize" column that looks like a circle with two arrows. Clicking on the synchronize icon for a interface will begin the synchronization process for that interface. All synchronizations take place in separate processes from the interface, so you can continue your work within **CYBER ACL** while interfaces are being synchronized. Any **Interface** that is currently being synchronized will show a barber pole type progress animation in the "Synchronize" column.

If you view an **Interface** in the "**Interface Setup**" page by clicking its name from the "**Interface**" page or from its parent's "Device Setup" page you will see a horizontal bar stating "**Interface** NOT synchronized" if the **Interface** is not up to date with its access list. The "Synchronize" button starts the deployment in the background in the same manner as clicking the sync icon on the "**All Interfaces**" page would.

When synchronization is in progress the "Synchronize" button on the "**Interface Setup**" page will be replaced by a "Cancel Sync" button with a barber pole type progress indicator next to it.

When synchronization begins a deployment log entry will be added for the **Interface** indicating that it has a deployment in progress showing the user initiating the action and any comment they entered. Upon completion, cancellation, or failure of synchronization to an **Interface** the deployment log entry will updated to indicate the result and the message. The result will either be "Success" or "Failed". Cancelled synchronizations are marked failed. The "Message" field contains the text "Cancelled" for cancellations, and for errors it will contain the text of any error messages indicating what problems occurred.

Management Features

Schedules

You can schedule synchronizations to take place at a later date or time or on a recurring schedule. To view the scheduled synchronizations click on the "Schedules" link in the navigation menu.

Simply click "Add New Synchronization Schedule" to create a new scheduled synchronization. You will be prompted to enter a name for the Schedule, select the **Interface** (or all **Interfaces**) that the schedule applies to, and a date for the schedule to begin. If you click the "Recurring Schedule" checkbox then you will also need to set the interval which can be either hourly, daily, weekly, monthly, or other which allows you to specify a number of minutes between synchronizations.

When entering the "Date/Time" value you can enter relative amounts of time from the present. For example you could enter "+1day" to schedule a synchronization 24 hours away. Or you could enter "+30mins" or "+2hours".

If you click on the name of a Schedule on the "Schedules" page then you will be able to change any of the values for an existing schedule or delete that schedule.

Searching

There are two different types of searches supported by the system. Textual searches allow you to search the textual representation of a list, and advanced searches allow you to search list entries based on specific parameters for entry fields.

Textual Searches

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. To search within a list, you must be on the "List Entries" page of the appropriate list. 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 hilited with a yellow 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"

Advanced Search

From the "List Entries" page the "Advanced Search" link takes you to the "Advanced Search" page where you can specify ACL entry values to match against entries in the list while searching. All fields are the same as the fields from the "Edit Entry" page where you define access list entry values with the exceptions that there are no search fields for "Log", "Reflect", "Evaluate Reflect", or "Established", and at the top there is an additional field named "Match Type" where you specify the relationship the entry must have to the search values to be considered a match. The choices are:

- **Intersection** – If there is any overlap between the entry and the search settings the entry will be considered a match. For example, TCP and UDP do not intersection, but IP and TCP do, and 192.168.1.0 and 10.0.0.0 do not intersect, but 192.168.0.0/16 and 192.168.1.0/24 do intersect.
- **Superset** – The list entry must be a superset of the search values to match. This means that each value must be the same or less restrictive in the list entry. For example, IP is a superset of TCP as a protocol, and 192.168.0.0/16 is a superset of 192.168.1.0/24 as a Source Net/Mask.
- **Subset** – This is the opposite of superset, meaning that the search values must be a superset of the list entry values.
- **Exact** – Only match entries that match each field in the search parameters exactly.

Any field not specified on the "Advanced Search" page defaults to include any value, meaning that leaving "Source Net/Mask" or "Destination Net/Mask" blank defaults to any source or destination address, and that leaving "Port/Service" blank defaults to any port.

Once you have entered all of your search parameters click the "Search" button and you will be returned to the "List Entries" page with all matching entries highlighted in yellow.

Figure 14 - Advanced Search

Testing

CYBER ACL includes a feature which allows you to test what would happen to a theoretical packet as it is processed by an access list. Clicking the "Test" button on the "Advanced Search" page of an access list will run your test case.

When you have entered your parameters, click the "Test" button. You will be taken to the "List Entries" page with the entry which matched your sample values highlighted. This is the terminal entry for those values in the list, meaning that it is the entry which finally permitted or denied the packet.

Figure 15 - Matching Entry

CYBER ACL also includes the ability to create lists of test entries to be run against defined access lists to create test reports.

Reports

CYBER ACL supports two types of reports, deployment reports cover all synchronizations which have taken place and list reports which cover all changes made to access lists.
Reports viewed by clicking the Reports links from the navigational menu.

Dates are specified in the form **MM/DD/YYYY** or **MM/DD/YYYY HH:MM** and can also be specified as offsets backwards such as **-30days** or **-1hrs** or **-30mins**.

After you have selected parameters for your report click the "Filter" button to refresh the data.

Logging

CYBER ACL maintains two types of logs. The first type of log saves a history of all synchronizations performed by any user to any interface.   The second type of log saves a history of all modifications made to the database by users. These logging features allow you to better track user actions, and troubleshoot any problems with your lists or devices.

Deployment Logs

On the "Edit **Interface**" page the deployment log is shown for that particular **Interface** with the time, user, note, result, finish time, and any message for each synchronization.

A separate page showing all deployment logs can be viewed by clicking the "Deployment Logs" link in the navigational menu. This page shows the **Interface**, device, user, note, start time, finish time, result, and any message for each deployment.

Deployment logs also provide the data used for generating deployment reports as discussed in the "Reports" section of this manual.

Revision History

ACL Revision History documents all the changes made to access lists by the users of the system.   The most recent modification log entries for an access list are displayed by clicking the "Revision History" link for that list.   For each log entry the date, user, event (action taken), and comment entered are shown. The "Revision History" is discussed in the section "History and Rollback" in this manual.

Notification

CYBER ACL supports email, snmp notification when certain types of events take place. This feature is controlled via the "Notifications" page.

Syslog

Syslog, file logging, tracing, etc. are documented in the aclserver.conf file and can be configured there.

SNMP Traps

SNMP trap destinations and options are configured in the /etc/aclserver.conf file. This includes the hostname for the SNMP trap server, version, and other options. Minimally, the *SNMPHost* configuration value must be set.

Next, in the Admin->Notifications menu of **CYBER ACL,** configure which events should send traps to the trap server.

The MIB, **CYBER-SNMP-MIB**, is located on the **CYBER ACL** application server and also is available in the downloads and support section of http://www.cyberoperations.com.

Command Line Tools

CYBER ACL also includes an extensive command line tool that allows the user access to much of the features available via the web interface from the command line, as well as some things not available from the web interface. Please see the extensive built-in help by running the command "**aclserver help**".

Web Services

CYBER ACL also includes web services so that the product can be controlled programmatically. The WSDL is located at:

https://<yourServerName>/cgi-bin/aclserver?page=wsdl
Web services must be enabled and configured in the /etc/aclserver.conf file. See that file for instructions.

Branding and Customization

Edit the *html/custom/login.html* and *html/custom/welcome.html* files to enter messages that will be shown on the login and welcome page respectively. These are in html format and are inserted into the page.

Custom links can be added to the "Reference" menu. Instructions are in the *aclserver.conf* file.

Many of the images in the **html/images** folder can be overridden by creating a file of the same name in **html/custom/images.** In general, the replacement image should be the same width/height as the original.
These are: main_bg.jpg, bg_header_login.jpg, bg_header.jpg, welcome.png, reportheader.jpg

Documents can be added to the "Additional Resources" area by adding the file to the **html/custom/resources** folder.

Support

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

Technical Support

Monday - Friday, 8am - 5pm CST

24 by 7 Support Contracts Available

Phone: 205-403-2923

Email: support@CyberOperations.com

Website: www.CyberOperations.com