



FLM-ANT Version 5.5

Release Notes



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

FLM-ANT Release Notes

Release Date: January 11, 2010

Release Build Number: 6732

Replaces: All previous versions... All previous file formats are supported. This version will not communicate with previous versions of FLM-ANT. C3 and Sensor must both be upgraded at once.

What's New

FLMv1 communication using ports 22229 and 22230 have been removed.
FLMv2 communication now uses port 22231 on the FLM sensor and uses TLSv1 in FIPS mode.

Juniper.pl script now uses less strict checking for host key on Juniper router.

Log window wraps long lines rather than using the horizontal scroll bar.

The complete results of the 'commit' statement to the Juniper are now shown in the logs.

The total amount of history data shown in the log window has been significantly increased.

The "Load from Router Configuration" item now supports JunOS format as well as Cisco IOS format.

The "Deployment History" and "Live Filter Editor" now update only after a successful router commit. This replaces the previous behavior where they were updated immediately prior to the router commit.

Changed deployment history dialog to allow rolling back checked circuits. This replaces the previous behavior where the same button rolled back all of the circuits on the sensor.

Removed button in history dialog that rolled back highlighted circuit

Filter is now deployed under "family inet" of the firewall section of the Juniper config.

Fixes

1. "*pdcontrol stop*" now also stops *pdtauth* authentication daemon.

Known Issues

None

Release Date: July 30, 2009

Release Build Number: 6557

Replaces: All previous versions... All previous file formats are supported. This version will not communicate with previous versions of FLM-ANT. C3 and Sensor must both be upgraded at once.

What's New

Deploy history now available which includes filenames.
Choose rollback list based on filename. Rollback Ingress/Egress separately.
Live Access List Window now shows filename of deployed access list.
Juniper.pl script now has a 5 minute SCP timeout
Log messages modified to include "Ingress" / "Egress" during commit process.
C3 config page now has an option to override connection type on sensors to use dedicated connections only.
Now any SCP error message from perl module is written to syslog.
Release notes link added to help menu.
Added a "dedicatedOnly" configuration option for the sensor to disable/enable the original communication protocol.

Fixes

2. Fixed problem where automatic update may have caused the saved window position preferences to be lost in C3.
3. Deploy of "Ingress" list no longer re-enters current "Egress" list. This was unnecessary.
4. Fixed problem that may have caused unnecessary CPU on the sensor usage after a deployment over the dedicated connection type.

Known Issues

None

Release Date: May 6, 2009

Release Build Number: 6465

Replaces: Build Number 6448 and all other previous versions

What's New

Juniper.pl script now only modifies the ingress or egress filter if only one of the two had been deployed from the C3.

Juniper DNS and ICMP access list terms are now combined before deployment when the combining terms option is turned on.

Dedicated communication protocol no longer allows SSL v2, now uses SSL v3 exclusively.

Fixes

5. Authentication may have failed when using one-time tokens for a deployment to two circuits on the same sensor. This was caused by authenticating the two requests separately in some cases.
6. Pdtacauth is now completely restarted when using “pdcontrol stop” and when changing sensor configuration from the C3.

Known Issues

None

Release Date: April 20, 2009

Release Build Number: Sensor:6429 / Deployed with C3:5246

Replaces: All other previous versions

What's New

1. The juniper.pl script no longer makes a backup copy of the router config during access list deployments.
2. The pdauth authentication program has been outmoded completely by pdtacauth and has been removed from all future updates.
3. auth_cmd config item now defaults to /usr/local/sensor/pdtacauth
4. Improved error reporting and handling in juniper.pl script.
5. pdcontrol program now has a 'log' function
6. FLM-ANT sensor now has a commit_command config item that can be used to change the commit call from 'commit synchronize' to 'commit' via the sensor config file.

Fixes

1. The previous release of pdtacauth incorrectly checked login/pass with the tacacs server when deploying to a multi-circuit sensor. This second check was not necessary and could cause problems when single-use passwords are used.
2. Graph polling frequency has been shortened from 5 minutes to 1 minute. This may correct some problems with timeouts on VPN connected controllers.

3. Corrected problem with legacy communication schema where an internal inter-device message may have rarely been dropped due to a slow network connection.
4. Juniper.pl may have incorrectly displayed a user name in log messages during deployment. This has been fixed by not using the “logger” system command in the juniper.pl script.

Known Issues

None

Release Date: June 2, 2008

Release Build Number: 5450

Replaces: Build Number 5246 and all other previous versions

What's New

1. This is a maintenance release for the sensor only that addresses problems with the port optimization.

Fixes

Problem causing incorrect handling of destination ports when using port 80 access list optimization feature.

Known Issues

None

Release Date: April 25, 2008

Release Build Number: 5246

Replaces: Build Number 4788 and all other previous versions

What's New

2. This is a maintenance release that addresses delays experienced in some cases when using the dedicated connection option added in Build Number 4449.

Fixes

Problem causing delays before sensor status and log messages were updated when communicating with some sensors over a dedicated connection.

Known Issues

None

Release Date: February 21, 2008

Release Build Number: 4788

Replaces: Build Number 4449 and all other previous versions

What's New

1. Elapsed time shown in log during commits now calculates from time sensor receives the new ACL.
2. Authentication system improved to better handle operations on multiple sensors which may use different passwords.

Fixes

Problem causing some log lines to displayed twice or not at all in CMS.
Restarting pdserver no longer causes "Could not connect to 127.0.0.1" message.
The spurious message "User Name Required - Access Denied" is fixed.

Known Issues

None

Release Date: January 30, 2008

Release Build Number: 4449

Replaces: Build Number 4061 and all other previous versions

What's New

1. A new communications option between controller and sensor is supported which maintains an open connection so opening connections from the sensor to the controller is not required.
2. DNS special case marking has been modified to only apply to UDP protocol rules, not TCP protocol rules.

3. A feature has been added which allows loading a previous version of sensor's ACL to the ACL editor without having to rollback to that version.
4. The interfaces stats command has been removed.
5. All references to "selected sensor" in user interface have been changed to say "highlighted interface" to avoid confusion.

Fixes

None

Known Issues

None

Release Date: November 14, 2007

Release Build Number: 4061

Replaces: Build Number 3900 and all other previous versions

What's New

1. Special case has been added for ICMP protocol entries similar to what was already handled for DNS entries.
2. DNS and ICMP special case handling can be controlled by setting configuration entries now instead of editing the device script. See the configuration entry table near the end of the user manual for more information.

Fixes

None

Known Issues

None

Release Date: October 15, 2007

Release Build Number: 3900

Replaces: Build Number 3670 and all other previous versions

What's New

1. New option for authorization, pdtauth, now allows TACACS+ authentication without using PAM. The previous method using pdauth is still supported for backwards compatibility.
2. Router configurations are no longer backed up automatically for performance reasons.

Fixes

Using pdtauth for authorization instead of pdauth prevents redundant authorization attempts during deployments.

Known Issues

None

Release Date: October 2, 2007

Release Build Number: 3670

Replaces: Build Number 3560 and all other previous versions

What's New

1. Supports auto insertion of a filter term at the beginning of the list to send a TCP reset to anyone trying to connect to SMTP on a list of IP addresses supplied in a configuration entry.
2. Deployment process now allows commit to be run once for multiple simultaneous deployments to the same router for different interfaces.
3. Progress is now logged periodically to the sensor log during deployment.
4. Router configurations are now backed up to the sensor and rotated with each deployment.
5. The compare with sensors' ACL feature now compares egress filters as well.

Fixes

None

Known Issues

None

Release Date: August 6, 2007

Release Build Number: 3560

Replaces: Build Number 3460 and all other previous versions

What's New

1. The color coding in the FLM-ANT log viewer has been improved so that problems are color coded red and successes are color coded green which will make the software easier to use.
2. Rate limit ACL entries (which are not being used by DOD installations) are now not listed as an option when creating access lists.

Fixes

None

Known Issues

None

Release Date: July 19, 2007

Release Build Number: 3460

Replaces: Build Number 3400 and all other previous versions

What's New

1. Improvements with the temporary ACL entries. The previous version only allowed adding temp entries to the beginning of the ACL but now you can add them anywhere in the list.
2. When specifying the duration of a temporary ACL entry, the operator can now use shortcuts such as "1 day", "5 hours", "17:56", etc.

Fixes

1. The mechanism that removed access list entries via the Live Filter Editor had previously assumed that an identical entry already in the ACL should be removed prior to adding the new entry. This assumption was not always best and in some cases may confuse the operator. Now ACL entries are manipulated exactly as specified by the operator.

2. A problem existed such that the drag/drop feature for the device list would activate when the operator selected a device and then selected another device while the Live Filter Editor was loading a long ACL. This has been corrected.

Known Issues

None