FlowPro Documentation

Release 16.8

Plixer

Oct 23, 2018

FlowPro

Welcome to the on-line FlowPro manual. *Click Here* for online troubleshooting or FAQs. This manual is also available in .pdf format.

Important: Don't struggle, contact Plixer support!

CHAPTER 1

What is FlowPro

The FlowPro Series comes in a variety of flavors. Below is an explanation of the differences between each option available.

1.1 FlowPro

Complete visibility of network traffic is key to managing your network, protecting your assets, and investigating security incidents. Whether you need to monitor traffic in remote offices, in an isolated data closet, or in a data center, FlowPro provides the information you need to perform root-cause analysis of both network performance and security events.

1.2 FlowPro APM (Application Performance Monitor)

FlowPro APM (Application Performance Monitoring) captures network traffic and creates flow data to send to an IPFIX collector to monitor traffic where visibility is limited. In addition to network traffic, FlowPro APM passively monitors traffic and performs three operations depending on the configuration:

1. Latency information on clients, servers, and Layer 7 applications through Deep Packet Inspection (DPI)
2. Traffic metrics related to SIP/RTPs and voice quality
3. Operates in both modes at the same time

1.3 FlowPro Defender Primary Operations

FlowPro Defender captures network traffic to provide additional visibility into the traffic within or transiting the organization. It passively monitors the traffic and can perform two operations on the data:

1. Creating flow data to send to an IPFIX collector to monitor traffic where visibility is limited. When operating in this manner, FlowPro Defender simply captures the network traffic and generates IPFIX records of the traffic without performing any additional processing.

2. Monitoring DNS traffic to identify indicators of malware compromise, including BotNet detection, DNS lookups of domains that are likely associated with malware and identification of malware utilizing DNS for data exfiltration and / or command and control.

In this mode, FlowPro Defender is processing the DNS traffic, comparing DNS Queries to a domain reputation list and matching DNS queries with responses to identify abnormal DNS traffic. Examples of traffic monitored include detection of no existing domain (NXDOMAIN) responses and identification of long and complete DNS names that do not properly resolve.

Additional FlowPro Defender Capabilities

- monitors other types of DNS messages, such as the use of DNS TXT messaging as a means to bypass firewall restrictions and allow direct communications between an outside host and an internal asset.
- allows the user to create their own "white lists" to prevent allowed domains from triggering alerts, as well as their own "blacklist" to augment the Plixer-supplied domain reputation lists.
- can be used in either or both modes simultaneously in any combination on any or all of the available monitoring ports. FlowPro Defender is available as an appliance appropriately sized to the user's network or as a Virtual Appliance download.

CHAPTER 2

Installation

There are several types of appliances available. A valid or evaluation key is required with each install. A key can be obtained from Plixer International, Inc. or a local reseller.

The steps below describe the process of installing hardware and virtual appliances. Although the screen captures show FlowPro Defender, the same steps are performed for each flavor of FlowPro.

2.1 Hardware Appliance

Once the hardware appliance is installed in a network rack, power it on and follow the steps below:

1. Using an SSH client, remotely login using the username root and password flowpro. The hardware appliance will perform a quick setup and immediately reboot

```
CentOS release 6.5 (Final)
Kernel 2.6.32-431.3.1.e16.x86_64 on an x86.64

localhost login: root
Password: _
```

2. Login to the hardware appliance again using the username root and password flowpro. Answer a few brief questions. The hardware appliance will reboot to apply the necessary settings.

```
********************************
FlowPro Hardware Appliance
Initial Configuration
********************************

What is the appliances static IP Address?
10.1.2.3
What is the appliances Netmask?
255.255.255.0
What is the appliances gateway?
```

(continues on next page)

(continued from previous page)

```
10.1.1.1
What is the hostname for this appliance?
flowpro-defender1

What is the IP Address to your DNS?
This will allow the FlowPro to resolve IP addresses.

*Login to the hardware appliance again and answer a few brief questions*
```

3. Login to the hardware appliance command line with the flowpro username and password. Apply the license key by issuing the license set command.
4. In the new window, beside *license*= paste in the license key

```
FlowPro Defender (TM) v15.5.5.277
[2018-04-24 15:01:05 -0400 (Wed, 24 Apr 2018)]
Copyright (C) 2012 - 2018 Plixer, All rights reserved.
Plixer
Need an IPFIX Collector? Download Scrutinizer at http://www.plixer.com

         Machine ID : 6YZ6XEPT669PBA664A14561Q
    Licensed Verson : 15.5
      Licensed Type : valid
         Expiration : Tue Apr 12 2019
License expires in 342 day(s)

FLOW PRO> help license

+-------------------------------------------------+

license <set|update|check|status>

    license update can be used to apply a license key to this flowpro.
    license check or status will give details about the current license key.

+-------------------------------------------------+

FLOWPRO> license set_
```

5. Press CTRL+X to save

FlowPro is now ready for operations

2.2 Virtual Appliance - ESX

The FlowPro Virtual Appliance (FVA) is packaged as an all-in-one virtual machine template known as an OVF template. For VMware deployments, ESXESXi 5.0 or higher is required. VMware Tools will be required to shut down the FVA through the VMware vSphere Client.

System Requirements

Component	in Specifications
RAM	2GB
Disks	5GB
Processor	1 CPU 2 Core 2GHz+
Operating System	ESXi5

Deploying the OVF Template

1. Connect to the ESX host using VMware vSphere, or vCenter.
2. Select File then Deploy OVF Template.
3. Select Deploy from File, browse to the OVF Template, and click Next.
4. Review the OVF template details and click Next.
5. Define the name of the FlowPro Virtual Appliance and click Next.
6. Select a datastore and click Next.
7. Select the disk format and click Next.
8. Select the Network Mapping and click Next.
9. Review the Virtual Settings and click Finish to import the OVF Template.
10. The virtual machine itself has both network adapters and eth1 (or mon1) is already in promiscuous mode. By default, it will start listening for traffic on the default virtual network, but it may not be the correct virtual network that needs to be monitored. If a user wants to monitor something different, they will have to set up a mirror port of a Virtual Distributed Switch or a mirror port using a physical NIC on the ESXi host.
11. Right click on the FlowPro virtual machine and power it on.
12. Navigate to the Console tab and login using the username root and password flowpro. The virtual appliance will perform a quick setup and immediately reboot.
13. Login to the virtual appliance again using the username root and password flowpro. Answer a few brief questions. The virtual appliance will reboot to apply the necessary settings.

```
********************************
FlowPro Hardware Appliance
Initial Configuration
********************************

What is the appliances static IP Address?
10.1.2.3
What is the appliances Netmask?
255.255.255.0
What is the appliances gateway?
10.1.1.1
What is the hostname for this appliance?
flowpro-defender1

What is the IP Address to your DNS?
This will allow the FlowPro to resolve IP addresses.
```

14. Login to the virtual appliance command line with the flowpro username and password. Apply the license key by issuing the license set command.

```
FlowPro Defender (TM) v15.5.5.277
[2018-04-24 15:01:05 -0400 (Wed, 24 Apr 2018)]
Copyright (C) 2012 - 2018 Plixer, All rights reserved.
Plixer
Need an IPFIX Collector? Download Scrutinizer at http://www.plixer.com

         Machine ID : 6YZ6XEPT669PBA664A14561Q
    Licensed Verson : 15.5
      Licensed Type : valid
         Expiration : Tue Apr 12 2019
License expires in 342 day(s)

FLOW PRO> help license

+------------------------------------------------+

license <set|update|check|status>

    license update can be used to apply a license key to this flowpro.
    license check or status will give details about the current license key.

+------------------------------------------------+

FLOWPRO> license set_
```

15. In the new window, beside license= paste in the license key
16. Press CTRL+X to save

The FlowPro is now ready for configuration.

2.3 Installing VMware Tools

VMware Tools are not required for proper function of the virtual appliance. However, there are certain advantages to deploying it on each virtual appliance. See VMware's documentation for more details.

VMware Tools are not installed by default because each version of ESX installs a different VMware Tools package. A script is included with the Virtual FlowPro to simplify the install process.

1. In the VMware vSphere Client, right click on the FlowPro virtual machine and select Guest then Install/Upgrade VMware Tools.
2. Login to the console of the FlowPro Virtual Appliance as the root user and run the command /home/flowpro/conf/vmwareToolsInstall.sh.

2.4 Upgrading the Virtual Machine Hardware Version

The FlowPro Virtual Appliance is built on Virtual Machine Hardware Version 8 to maintain backwards compatibility with ESXi 5.0 hypervisors. While the virtual machine is powered off, in vSphere (or vCenter) right click on the virtual machine and select Upgrade Virtual Hardware.

2.5 Virtual Machine - Hyper-V

System Requirements

Component	Min Specifications
RAM	2GB
Disks	5GB
Processor	1 CPU 2 Core 2GHz+
Operating System	MS Windows Server 2012

2.5.1 Importing a Virtual Machine

1. Download the latest Plixer FlowPro Appliance
2. Unzip the file on the Hyper-V server
3. Open Hyper-V Manager and select Import Virtual Machine
4. Specify the FlowPro Appliance System Folder
5. Select the Virtual Machine
6. Choose the import type
7. Go to Setting
8. Select the Network Adapter and assign it to the appropriate Virtual Switch FlowPro Appliance requires a mirrored port to be associated with eth1 (or mon1). To set up a mirrored port, reference:

   http://blogs.technet.com/b/networking/archive/2015/01/06/settingup-port-mirroring-to-capture-mirrored-traffic-on-a-hyper-v-vir
   aspx
9. Expand the Network Adapter section, select Advanced Features, set the MAC Address to Static, enter in a unique MAC Address, and then press “OK”.
10. Start the Virtual Machine.
11. Right Click on the Virtual Machine and click Connect to login to the Plixer FlowPro Appliance using root/flowpro. The server will perform a quick setup and immediately reboot.

CHAPTER 3

FlowPro : Features and Functionality

This section describes the specific features and functionality of the FlowPro.

3.1 Getting Started

Using an SSH Client, ssh to the FlowPro and log in as the flowpro user using the password configured during the installation process.

```
[root@VA_DC_5 ~]# ssh flowpro@10.1.4.31
Password:
Last login: Mon May  4 12:25:11 2015 from 10.1.10.65
FlowPro (TM) v15.4.30.277 [2015-04-30 16:01:05 -0400 (Thu, 30 Apr 2015)]
Copyright (C) 2012 - 2015 Plixer International, Inc. All rights
reserved.
Plixer
Need an IPFIX Collector? Download Scrutinizer at http://www.plixer.com
Machine ID  : xxxxxxxxxxxxxxx
Licensed Version : 15.5
Licensed Type : standard
Expiration  : Tue Apr 12 2016

License expires in 343 day(s)

FLOWPRO>
```

The *FLOWPRO>* prompt indicates the FlowPro is ready for commands. If the initial steps are done correctly, the FlowPro is already processing traffic and sending feedback to the IPFIX collector specified.

3.2 Server Maintenance

3.2.1 Hardware Failure

If any hardware malfunctions occur, contact technical support for assistance.

3.2.2 Applying Security Patches

Although efforts are made to minimize the risk for security breaches on the appliance, updates to core OS components may be applied.

It is recommended that updates are not installed unless technical support advises or assists. For more information, contact technical support.

3.2.3 Upgrades

Customers are entitled to upgrades provided that maintenance is active. For further instructions, contact technical support.

3.2.4 Backing up the FlowPro

The FlowPro stores all its details in the plixer.ini file. From the FLOWPRO> prompt, type edit plixer.ini and copy the file contents to a safe location.

3.2.5 Restoring a FlowPro from Backup

To restore the FlowPro backup, use ssh to log into the appliance. From the FLOWPRO> prompt, type edit plixer.ini and hit enter. Overwrite the contents of the file with the backed up plixer.ini content. Save the changes. FlowPro will rebuild the appropriate files and begin operations.

If a new server is being used or server configurations have changed, a new license key may need to be applied.

3.3 Commands

3.3.1 clear

The clear command clears log files from the FlowPro. These log files contain details pertaining to the operation of flowpro.

- EXAMPLE clear log <logfile>
- FLOWPRO> clear log dns1yaf.log

By executing clear log by itself, FlowPro will show a list of available logs.

3.3.2 edit

The edit command is used to modify system files used in the day to day operations of FlowPro.

- EXAMPLE edit <plixer.ini>

The plixer.ini file is the main configuration file for FlowPro. It contains settings used by FlowPro to configure licensing, reputation lists, listening interfaces, IPFIX collector, and more.

- FLOWPRO> edit plixer.ini

3.3.3 license

The license command is used to manage the FlowPro license key. Applying a license will upgrade a FlowPro to FlowPro Defender or FlowPro APM. A license is not required to run FlowPro.

To generate a license key, Plixer or the reseller will need the FlowPro's unique machine ID. The machine ID is displayed when issuing the license check command.

The following command can be used to show licensing details:

license <*check*|*status*>

```
FLOWPRO> license check
        Machine ID : 5YZ6XEPV66C766369M8DBN2A
  Licensed Version : 15.5
     Licensed Type : valid
        Expiration : Thu Jul 28 2016

License expires in 730 day(s)
```

The license key can be configured on the FlowPro using the license set command.

license <*set*|*update*>

```
FLOWPRO> license set
```

When applying the license key, it must be one continuous string without any line feeds or carriage returns on the same line as the *license*=.

```
[flowpro]
collector=10.1.4.94:2055
enableDomainReputationList=1
monitorTraffic=mon1
monitorDNS=mon2
license=Nb7RuIh35R1Uv9uOWTWhBUuLX4mLNtYCxfqlL0j3IEV2r//␣
↪hkHhl3EnTTFdZZPK+0jprzFIlW10dmIN7sZOiwlCcA+L5g6HTzQJ/␣
↪b8l6hLeLEsoHiYXgj0SsWkKeCu2IBb6Alpv3msIf1k+ps2cbf8abUR/ kdLVkwOwAwozq2kY7/RzTwvj7$
```

In the new window, beside license= paste in the license key and Press CTRL+X to save. Issuing the license check or license status will verify the key is properly installed.

Contact technical support to acquire a new license key.

3.3.4 password

The *password* command will change the password used for the flowpro username.

```
FLOWPRO> password
(current) UNIX password:
New password:
Retype new password:
Successful password changes will be applied to the next log in.
```

This password is used when logging in remotely or on the server directly

3.3.5 service

The service command can be used to manually start, stop, or restart the FlowPro service.

service <service_name> <start|stop|restart>

```
FLOWPRO> service flowpro restart
```

3.3.6 set

The set command is used to set certain system parameters. At this time, it is used to set the IPFIX Collector. It is primarily an alias to the command edit plixer.ini.

```
FLOWPRO> set collector
```

Future versions of FlowPro may allow users to utilize the set command without modifying the full configuration.

3.3.7 show

The show command is used to display state or list details available for modification and customization by the user.

The show log command lists the available logs to view. By specifying a log file name after the show log command, it will display its contents.

The show realtime command lists the available logs to watch in real time. By specifying a log file name after the show realtime command, it will show new content added to the log file as it happens.

The show status command displays all running components of the FlowPro system, the state of those services, and the current license details.

```
FLOWPRO> show status
+-------------------------------------------------------------------+
| FlowPro                       ACTIVE
| FlowPro Process Monitor       ACTIVE
| (Traffic) mon1                ACTIVE
| FlowPro License               Free
+-------------------------------------------------------------------+
```

3.3.8 snoop

The snoop command can be used to verify that packets are being received by or sent from the FlowPro for a certain IP address or interface.

- snoop ip <ip_address>
- snoop interfaces <interface_name>

```
FLOWPRO> snoop ip 10.1.1.1
FLOWPRO> snoop interfaces mon1
```

Press CTRL+C to exit the snoop command.

3.3.9 system

The system command is used to change state of the FlowPro. The directive change is used to change the host name or IP address.

system <change|restart|shutdown>

```
FLOWPRO> system change FLOWPRO> system restart
FLOWPRO> system shutdown
```

3.4 Ingress, Egress and Observation Domain Configuration

The default behavior for traffic monitoring is to label the flows from each interface as its own ingress and egress. (mon1 = ingress on 1, egress on 1). By default, the observation domain is fixed at 42. However, FlowPro can be configured to label the flows as coming from any licensed ingress and egress interface, and/or from any observation domain.

For example: Users may want to label traffic monitoring so ingress is mon1 (i.e. 1) and egress is mon2 (i.e. 2).

This is done by modifying the plixer.ini

```
FLOWPRO> edit plixer.in
```

In the editor, locate the following line:

```
monitorTraffic=mon1
```

When specified in this format, mon1 is configured for ingress of 1 and egress of 1. By modifying this setting in the following format, FlowPro will configure mon1 to have an ingress of 1 and egress of 2.

```
monitorTraffic=mon1:1:2
```

The format to use is monX:ingress:egress. Once the necessary configuration changes have been made, save the plixer.ini file. FlowPro will then restart the services with the new configuration. Note that the values for ingress and egress are limited to the maximum number of licensed interfaces.

To define a different observation domain for an interface, modify the plixer.ini file as before using the format monX:ingress:egress:observation_domain. To set the observation domain, the ingress and egress labels must also be set. To change the observation domain for mon1 to 45, while using the ingress and egress values set above, modify the setting above to read as:

```
monitorTraffic=mon1:1:2:45
```

Or, to use the default values for mon1 with an observation domain of 45:

```
monitorTraffic=mon1:1:1:45
```

CHAPTER 4

FlowPro Defender : Features and Functionality

This section describes the specific features and functionality of the FlowPro Defender.

4.1 Getting Started

Using an SSH Client, ssh to the FlowPro Defender and log in as the flowpro user using the password configured during the installation process.

```
[root@VA_DC_5 ~]# ssh flowpro@10.1.4.31
Password:
Last login: Mon May  4 12:25:11 2015 from 10.1.10.65

FlowPro Defender (TM) v15.4.30.277
[2015-04-30 16:01:05 -0400 (Thu, 30 Apr 2015)]
Copyright (C) 2012 - 2015 Plixer All rights reserved.
Plixer
Need an IPFIX Collector? Download Scrutinizer at http://www.plixer.com

          Machine ID  : xxxxxxxxxxxxxxx
     Licensed Version : 15.5
        Licensed Type : valid
          Expiration  : Tue Apr 12 2016

License expires in 343 day(s)

FLOWPRO>
```

The *FLOWPRO>* prompt indicates the FlowPro Defender is ready for commands. If the initial steps are done correctly, the FlowPro Defender is already processing traffic and sending feedback to the IPFIX collector specified.

4.2 Trusted Domain List

A "trusted domain list", often called a whitelist, is preconfigured on FlowPro Defender to suppress alarms involving specific domains. The default whitelist contains five entries that can added or removed as best fits a user's environment.

- Mcafee.com
- Sophos.com
- Sophosxl.net
- webcfs03.com
- apple.com

Mcafee.com suppresses DNS Data Leak alarms from McAfee AntiVirus software. McAfee encodes information from the anti-virus clients on the network into very long and complex DNS names and captures this information at their DNS server. This is exactly the type of behavior that the DNS Data Leak algorithm is looking for as this technique is also used by some forms of malware. Sophos.com and sophosxl.net are related to the Sophos Anti-virus software, and it uses multiple techniques to get information in and out of a network using DNS. In addition to using the same technique as McAfee to send information back to their servers, they also use DNS TXT messages to send information back into the clients on the network. Use of DNS TXT messages to exchange information with an external host is also used by some malware families, and the DNS Command and Control algorithm will alarm on this type of activity. This will prevent Sophos from generating either DNS Data Leak or DNS Command and Control alarms.

- Webcfs03.com belongs to SonicWALL and will also generate DNS Data Leak alarms.
- Apple.com uses DNS TXT messages to apparently exchange settings with their NTP server. This will alarm as a DNS Command and Control alarm.

There may be other authorized software on internal networks that use DNS to bypass the firewall for data communications. If so, add the domain(s) involved to the Trusted Domain list. Once configured, any other traffic using DNS to communicate will be worth additional investigation.

Use the edit command to modify the trusteddomains list.

4.3 Untrusted Domain Lists

FlowPro Defender supports both the use of a domain reputation list that is downloaded from Plixer, as well as allowing a user to create or edit custom lists.

4.3.1 Plixer Domain Reputation List

FlowPro Defender can download a list of domains from Plixer once each hour. These are domains that have been determined to be "bad domains" with a high probability, and this list is used in the "Domain Reputation" and "Malware Behavior Detection" algorithms.

To provide maximum protection, FlowPro Defender must update the domain reputation list that it uses each hour. During setup, please verify a network route exists from FlowPro Defender to nba.plixer.com. The Domain Reputation algorithm will not detect any malware if FlowPro Defender is unable to connect to nba.plixer.com, however, all other features will operate normally. Use of this list can be controlled through FlowPro Defender.

To enable or disable the use of this list:

1. Remotely log on to the FlowPro Defender
2. Type at the FLOWPRO> prompt edit plixer.ini

3. To enable (default is enabled), set the value enableDomainReputationList=1 or, to disable the list, set the value enableDomainReputationList=0
4. Save changes and exit the editor

4.3.2 User Defined Domain Lists

Users may augment the Plixer Domain Reputation list and create one or more domain lists that contain domains to monitor. Domains entered must follow the rules below:

- The DNS name must contain at least 2 labels, which is often called a second level domain, or 2LD for short (for example, google.com) and no more than 3 labels (maps.google.com), or a 3LD.
- The labels must contain between 1 and 63 characters, as is required to be a legitimate domain name.

Entries that do not match these requirements will be ignored. To create a custom list of domains to detect domainReputation alarms:

1. Log on to the FlowPro Defender
2. At the FLOWPRO> prompt type edit my_domain_list_name NOTE: DO NOT enter a file extension. This will be automatically assigned.
3. Add, remove, or modify the file contents as desired
4. Save changes and exit the editor

To enable or disable custom domain lists, use the enable and disable commands.

4.3.3 Scrutinizer Flow Analytics Algorithms

FlowPro Defender will send data to the specified IPFIX Collector. Plixer's Scrutinizer Incident Response System has additional capabilities to check for malicious behavior and bad actors.

BotNet Detection This alarm is generated when a large number of unique DNS name lookups have failed. When a DNS lookup fails, a reply commonly known as NXDOMAIN is returned. By monitoring the number of NXDOMAINs detected as well as the DNS name looked up, behavior normally associated with a class of malware that uses Domain Generation Algorithms (DGAs) can be detected.

The default threshold is 100 unique DNS lookup failures (NXDOMAIN) messages in five minutes. Either the source or destination IP address can be excluded from triggering this alarm.

DNS Command and Control This algorithm monitors the use of DNS TXT messages traversing the network perimeter as detected by FlowPro Defender. DNS TXT messages provide a means of sending information into and out of the protected network over DNS, even when the user has blocked use of an external DNS server. This technique is used by malware as a method of controlling compromised assets within the network and to extract information back out. Additionally, some legitimate companies also use this method to communicate as a means to "phone home" from their applications to the developer site.

The algorithm will detect inbound, outbound, and bidirectional communications using DNS TXT messages. Thresholds may be set based either on the number of DNS TXT messages or the number of bytes observed in the DNS TXT messages within a five minute period. The default setting is for any detected traffic to alarm, and alarm aggregation defaults to 120 minutes.

To suppress alarms from authorized applications in the network, the user may add the domain generating the alarm message to the "trusted.domains" list on FlowPro Defender. See the discussion on "trusted.domains" list below.

DNS Data Leak This algorithm monitors the practice of encoding information into a DNS lookup message that has no intention of returning a valid IP address or making an actual connection to a remote device. When this happens, the local DNS server will fail to find the DNS name in its cache, and will pass the name out of the network to where

it will eventually reach the authoritative server for the domain. At that point, the owner of the authoritative server can decode the information embedded in the name, and may respond with a "no existing domain" response, or return a non-routable address.

FlowPro defender reviews all DNS queries and responses using proprietary logic to uncover unwanted communications. Odd behaviors are sent to Scrutinizer where they are further processed by the DNS Data Leak algorithm. Thresholds may be set based either on the number of DNS TXT messages or the number of bytes observed in the DNS TXT messages within a five minute period. The default setting is for any detected traffic to alarm, and alarm aggregation defaults to 120 minutes.

Domain Reputation Plixer is introducing domain reputation with 15.5. Domain reputation provides much more accurate alarming with a dramatic decrease in the number of false positive alarms as compared to IP based Host Reputation. The domain list is provided by Plixer and is updated each hour and currently contains over 400,000 known bad domains.

To provide maximum protection, FlowPro Defender must update the domain reputation list that it uses each hour. During setup, please verify a network route exists from FlowPro Defender to nba.plixer.com. The Domain Reputation algorithm will not detect any malware if FlowPro Defender is unable to connect to nba.plixer.com, however, all other features will operate normally.

FlowPro Defender performs the actual monitoring, and when it detects a domain with poor reputation, it passes the information to Scrutinizer for additional processing. The default setting is for any detected traffic to alarm, and alarm aggregation defaults to disabled so that all DNS lookups observed will result in a unique alarm.

To suppress alarms from authorized applications in the network, the user may add the domain generating the alarm message to the "Trusted Domain" list on FlowPro Defender. See the discussion on FlowPro Defender for additional details.

Malware Behavior Detection This is the first algorithm to demonstrate Plixer's cyber threat correlation capability. Correlation of multiple network behaviors over a long time period provides detection systems with more information allowing for a higher accuracy with fewer false positive alarms.

This specific alarm is correlating IP address lookups (i.e. what is my IP address) activity which is commonly performed by malware shortly after the initial compromise with the detection of the BotNet alarm or with a Domain Reputation alert. In other words, this algorithm looks for the following correlation:

- IP address lookup combined with a Domain Reputation trigger
- IP address lookup combined with a BotNet trigger

When either of the two events is detected, this algorithm triggers an alert as this behavior is a very strong indicator of a compromised asset.

Adding FlowPro Defender to the Algorithms In Scrutinizer's Flow Analytics Configuration interface, the FlowPro Appliance(s) must be associated to the Algorithms the user wishes to utilize.

In Scrutinizer: Navigate to the Admin Tab > Settings > Flow Analytics Configuration. Clicking the numbers in the exporter column will allow users to include the FlowPro Defender Exporter into that Algorithm. Violations and Alarms will show up in the Alarms Tab

4.4 Server Maintenance

4.4.1 Hardware Failure

If any hardware malfunctions occur, contact technical support for assistance.

4.4.2 Applying Security Patches

Although efforts are made to minimize the risk for security breaches on the appliance, updates to core OS components may be applied.

It is recommended that updates are not installed unless technical support advises or assists. For more information, contact technical support.

4.4.3 Upgrades

Customers are entitled to upgrades provided that maintenance is active. For further instructions, contact technical support.

4.4.4 Backing up the FlowPro Defender

The FlowPro Defender stores all its details in the plixer.ini file. From the FLOWPRO> prompt, type edit plixer.ini and copy the file contents to a safe location.

4.4.5 Restoring a FlowPro Defender from Backup

To restore the FlowPro Defender backup, use SSH to log into the appliance. From the FLOWPRO> prompt, type edit plixer.ini and hit enter. Overwrite the contents of the file with the backed up plixer.ini content. Save the changes. FlowPro Defender will rebuild the appropriate files and begin operations.

If a new server is being used or server configurations have changed, a new license key may need to be applied.

4.5 Commands

At any time running the command help, help <command>, <command> ?, or ? will display help in the interface.

4.5.1 check

The *check* command is used to test access to the Domain Reputation lists hosted on nba.plixer.com.

```
FLOWPRO> check replist
```

The output will indicate whether access is available to the domain lists. If access isn't available, the problem usually is that the FlowPro Defender does not have access to the internet.

4.5.2 clear

The *clear* command clears log files from the FlowPro Defender. These log files contain details pertaining to the operation of flowpro.

EXAMPLE clear log <logfile>

```
FLOWPRO> clear log dns1yaf.log
```

By executing clear log by itself, FlowPro Defender will show a list of available logs

4.5.3 delete

The *delete* command is used to permanently remove domain lists from the FlowPro Defender.

EXAMPLE delete <domainlist_name>

```
FLOWPRO> delete mylist
```

To see all domain lists, use the show command.

4.5.4 disable

The *disable* command is used to temporarily ignore domains in particular domain lists from the FlowPro Defender. This list will remain on the FlowPro Defender Appliance until it is removed.

EXAMPLE disable <domainlist_name>

```
FLOWPRO> disable mylist
```

To see all domain lists, use the show command.

4.5.5 edit

The *edit* command is used to modify system files used in the day to day operations of FlowPro Defender.

EXAMPLE edit <plixer.ini|domainlist_name>

The plixer.ini file is the main configuration file for FlowPro Defender. It contains settings used by FlowPro to configure licensing, reputation lists, listening interfaces, IPFIX collector, and more.

```
FLOWPRO> edit plixer.in.
```

The other function of edit is to update any custom domain lists used by FlowPro Defender to check for bad actors.

```
FLOWPRO> edit mylist
```

Newly created lists will be enabled once saved. Lists can be disabled using the disable command.

4.5.6 enable

The *enable* command is used to re-enable a disabled domain list.

```
FLOWPRO> enable mylist
```

4.5.7 license

The *license* command is used to manage the FlowPro Defender license key. To generate a license key, Plixer or the reseller will need the FlowPro Defender's unique machine ID. The machine ID is displayed when issuing the license check command.

The following command can be used to show licensing details:

license <check|status>

```
FLOWPRO> license check
        Machine ID : 5YZ6XEPV66C766369M8DBN2A
  Licensed Version : 15.5
     Licensed Type : valid
        Expiration : Thu Jul 28 2016

License expires in 730 day(s)
```

The license key can be configured on the FlowPro Defender using the license set command.

license <set|update>

```
FLOWPRO> license set
```

When applying the license key, it must be one continuous string without any line feeds or carriage returns on the same line as the *license=*.

```
[flowpro]
collector=10.1.4.94:2055
enableDomainReputationList=1
monitorTraffic=mon1
monitorDNS=mon2
license=Nb7RuIh35R1Uv9uOWTWhBUuLX4mLNtYCxfqlL0j3IEV2r//␣
↪hkHhl3EnTTFdZZPK+0jprzFIlW10dmIN7sZOiwlCcA+L5g6HTzQJ/␣
↪b8l6hLeLEsoHiYXgj0SsWkKeCu2IBb6Alpv3msIf1k+ps2cbf8abUR/
kdLVkwOwAwozq2kY7/RzTwvj7$
```

In the new window, beside license= paste in the license key and Press CTRL+X to save. Issuing the license check or license status will verify the key is properly installed.

Contact technical support to acquire a new license key.

4.5.8 password

The *password* command will change the password used for the flowpro username.

```
FLOWPRO> password
(current) UNIX password:
New password:
Retype new password:

Successful password changes will be applied to the next log in.
```

This password is used when logging in remotely or on the server directly.

4.5.9 service

The *service* command can be used to manually start, stop, or restart the FlowPro Defender service.

service <service_name> <start|stop|restart>

```
FLOWPRO> service flowpro restart
```

4.5.10 set

The *set* command is used to set certain system parameters. At this time, it is used to set the IPFIX Collector. It is primarily an alias to the command edit plixer.ini.

```
FLOWPRO> set collector
```

Future versions of FlowPro Defender may allow users to utilize the set command without modifying the full configuration.

4.5.11 show

The *show* command is used to display state or list details available for modification and customization by the user.

The *show domainlist* command displays all available domain lists that are both enabled and disabled.

```
FLOWPRO> show domainlist

FLOWPRO> show domainlists

mylist (enabled)
trusted (disabled)

2 list(s) Found ...
```

The *show log* command lists the available logs to view. By specifying a log file name after the show log command, it will display its contents.

The *show realtime* command lists the available logs to watch in real time. By specifying a log file name after the show realtime command, it will show new content added to the log file as it happens.

The *show status* command displays all running components of the FlowPro Defender system, the state of those services, and the current license details.

```
FLOWPRO> show status
+-------------------------------------------------------------------+
| FlowPro Defender              ACTIVE
| Super Mediator                ACTIVE
| FlowPro Process Monitor       ACTIVE
| (Traffic) mon1                ACTIVE
| (DNS) mon1                    ACTIVE
| FlowPro License               License expires in 343 day(s)
+-------------------------------------------------------------------+
```

4.5.12 snoop

The *snoop* command can be used to verify that packets are being received by or sent from the FlowPro Defender for a certain IP address or interface

snoop ip <ip_address> Snoop interfaces <interface_name>

```
FLOWPRO> snoop ip 10.1.1.1
FLOWPRO> snoop interfaces mon1
```

Press CTRL+C to exit the snoop command.

4.5.13 system

The *system* command is used to change state of the FlowPro Defender. The directive change is used to change the host name or IP address.

system <change|restart|shutdown>

```
FLOWPRO> system change FLOWPRO> system restart
FLOWPRO> system shutdown
```

4.6 Ingress, Egress, and Observation Domain Configuration

The default behavior for traffic monitoring is to label the flows from each interface as its own ingress and egress. (mon1 = ingress on 1, egress on 1). By default, the observation domain is fixed at 42. However, FlowPro Defender can be configured to label the flows as coming from any licensed ingress and egress interface, and/or from any observation domain.

For example: Users may want to label traffic monitoring so ingress is mon1 (i.e. 1) and egress is mon2 (i.e. 2).

This is done by modifying the plixer.ini

```
FLOWPRO> edit plixer.ini
```

In the editor, locate the following line:

```
monitorTraffic=mon1
```

When specified in this format, mon1 is configured for ingress of 1 and egress of 1. By modifying this setting in the following format, FlowPro will configure mon1 to have an ingress of 1 and egress of 2.

```
monitorTraffic=mon1:1:2
```

The format to use is *monX:ingress:egress*. Once the necessary configuration changes have been made, save the plixer.ini file. FlowPro Defender will then restart the services with the new configuration. Note that the values for ingress and egress are limited to the maximum number of licensed interfaces.

To define a different observation domain for an interface, modify the plixer.ini file as before using the format *monX:ingress:egress:observation_domain* To set the observation domain, the ingress and egress labels must also be set. To change the observation domain for mon1 to 45, while using the ingress and egress values set above, modify the setting above to read as:

```
monitorTraffic=mon1:1:2:45
```

Or, to use the default values for mon1 with an observation domain of 45:

```
monitorTraffic=mon1:1:1:45
```

CHAPTER 5

FlowPro APM Administration

5.1 Getting Started

Using an SSH Client, ssh to the FlowPro APM and log in as the flowpro user using the password configured during the installation process.

```
[root@VA_DC_5 ~]# ssh flowpro@10.1.4.31
Password:
Last login: Mon May  4 12:25:11 2015 from 10.1.10.65
FlowPro Application Performance Monitor (TM) v15.4.30.277
[2015-04-30 16:01:05 -0400 (Thu, 30 Apr 2015)]
Copyright (C) 2012 - 2015 Plixer
All rights reserved. Plixer
Need an IPFIX Collector? Download Scrutinizer at http://www.plixer.com
           Machine ID  : xxxxxxxxxxxxxxxx-xxxxxxxxx
      Licensed Version : 15.8
         Licensed Type : valid
           Expiration  : Tue Apr 12 2016
License expires in 343 day(s)
```

FLOWPRO>

The *FLOWPRO>* prompt indicates the FlowPro APM is ready for commands. If the initial steps are done correctly, the FlowPro APM is already processing traffic and sending feedback to the IPFIX collector specified.

5.2 Server Maintenance

5.2.1 Hardware Failure

If any hardware malfunctions occur, contact technical support for assistance.

5.2.2 Applying Security Patches

Although efforts are made to minimize the risk for security breaches on the appliance, updates to core OS components may be applied.

It is recommended that updates are not installed unless technical support advises or assists. For more information, contact technical support.

5.2.3 Upgrades

Customers are entitled to upgrades provided that maintenance is active. For further instructions, contact technical support.

5.2.4 Backing up the FlowPro APM

The FlowPro APM stores all its details in the plixer.ini file. From the FLOWPRO> prompt, type edit plixer.ini and copy the file contents to a safe location.

5.2.5 Restoring a FlowPro APM from Backup

To restore the FlowPro APM backup, use ssh to log into the appliance. From the FLOWPRO> prompt, type edit plixer.ini and hit enter. Overwrite the contents of the file with the backed up plixer.ini content. Save the changes. FlowPro APM will rebuild the appropriate files and begin operations.

If a new server is being used or server configurations have changed, a new license key may need to be applied.

5.3 Commands

At any time running the command help, help <command>, <command> ?, or ? will display help in the interface.

5.3.1 disable

The disable command is used to stop collection of the specified interface.

```
FLOWPRO> disable mgmt
```

5.3.2 edit

The edit command is used to modify system files used in the day to day operations of FlowPro APM. The plixer.ini file is the main configuration file for FlowPro APM. It contains settings used by FlowPro to configure licensing, IPFIX collector, and more.

```
FLOWPRO> edit plixer.ini
```

5.3.3 enable

The enable command can be used to enable metrics collection on the specified interface.

```
FLOWPRO> enable <interface_name> <voip|latency|both>
```

A list of interfaces is available by using the show command. The modes available to FlowPro APM are latency, VoIP, or both.

```
FLOWPRO> enable mgmt latency
```

The above example enables latency monitoring on the mgmt interface.

5.3.4 license

The license command is used to manage the FlowPro APM license key. To generate a license key, Plixer or the reseller will need the FlowPro APM's unique machine ID. The machine ID is displayed when issuing the license check command.

The following command can be used to show licensing details:

license <*check*|*status*>

```
FLOWPRO> license check
        Machine ID : 5YZ6XEPV66C766369W8DBN2A-XSAAAAASSSWW
  Licensed Version : 15.8
     Licensed Type : valid
        Expiration : Thu Jul 28 2016
License expires in 730 day(s)
```

The license key can be configured on the FlowPro APM using the license set command.

license <*set*|*update*>

```
FLOWPRO> license set
```

When applying the license key, it must be one continuous string without any line feeds or carriage returns on the same line as the *license*=.

```
[flowpro] collector=10.1.4.94:2055
trackProcessMetrics=0
apmMode=mgmt-latency;
license=Nb7RuIh35R1Uv9uOWTWhBUuLX4mLNtYCxfqlL0j3IEV2r//
hkHhl3EnTTFdZZPK+0jprzFIlW10dmIN7sZOiwlCcA+L5g6HTzQJ/
b8l6hLeLEsoHiYXgj0SsWkKeCu2IBb6Alpv3msIf1k+ps2cbf8abUR/
kdLVkwOwAwozq2kY7/RzTwvj7$
```

In the new window, beside license= paste in the license key and Press CTRL+X to save. Issuing the license check or license status will verify the key is properly installed.

Contact technical support to acquire a new license key

5.3.5 password

The password command will change the password used for the flowpro username.

```
FLOWPRO> password
(current) UNIX password:
New password:
Retype new password:
```

Successful password changes will be applied to the next log in. This password is used when logging in remotely or on the server directly.

5.3.6 service

The service command can be used to manually start, stop, or restart the FlowPro APM service/

service <service_name> <start|stop|restart>

```
FLOWPRO> service flowpro restart
```

5.3.7 set

The set command is used to set certain system parameters At this time, it is used to set the IPFIX Collector. It is primarily an alias to the command edit plixer.ini.

```
FLOWPRO> set collector
```

Future versions of FlowPro APM may allow users to utilize the set command without modifying the full configuration.

5.3.8 show

The show command is used to display state or list details available for modification and customization by the user.

The show interfaces command lists the available network interfaces that the FlowPro can utilizes for its operations.

```
FLOWPRO> show interfaces
 mgmt
 mon1
2 interface(s) available
```

The show status command displays all running components of the FlowPro APM system, the state of those services, and the current license details.

```
FLOWPRO> show status
+-------------------------------------------------------------------+
| (mgmt) Latency             ACTIVE
| FlowPro Process Monitor    ACTIVE
| FlowPro License            License expires in 343 day(s)
+-------------------------------------------------------------------+
```

5.3.9 snoop

The snoop command can be used to verify that packets are being received by or sent from the FlowPro APM for a certain IP address or interface.

snoop ip <ip_address> Snoop interfaces <interface_name>

```
FLOWPRO> snoop ip 10.1.1.1
FLOWPRO> snoop interfaces mgmt
```

Press CTRL+C to exit the snoop command.

5.3.10 system

The system command is used to change state of the FlowPro APM. The directive change is used to change the host name or IP address.

system <change|restart|shutdown>

```
FLOWPRO> system change
FLOWPRO> system restart
FLOWPRO> system shutdown
```

CHAPTER 6

Troubleshooting

6.1 Support

Technical support is available provided maintenance is active. Contact our support team at:

- +1(207)324-8805
- https://www.plixer.com/support/contact/

CHAPTER 7

FlowPro Change Log

For more details on the new features below, reference the Plixer website and FlowPro documentation.

KEY: ACTION: (Bug Ticket Number) description

Ex. ADDED: (1640) Thresholds based on outbound traffic

7.1 Change Log History

7.1.1 Version 18.5 - 5/22/2018

FIXED: (25173) FlowPro monitor interfaces not entering promiscuous mode
FIXED: (25634) Replace the EULA.txt in FlowPro
FIXED: (25639) FlowPro needs to support subscription license
FIXED: (25119) FlowPro APM Install/Upgrades need updating
FIXED: (25526) Can't upgrade nProbe due to package dependencies
FIXED: (25557) Update nProbe Version On APM
FIXED: (25627) Undefined address error on deployment
FIXED: (25710) Default Defender Plixer.ini is missing a field on fresh installs
FIXED: (25742) Rewrite the FlowPro manual
FIXED: (25880) FlowPro User Manual typo
FIXED: (25881) FlowPro PDF User Manual header says Plixer documentation
FIXED: (25913) APM won't start nProbe for more than one interface

7.1.2 Version 16.8 - 8/16/2016

ADDED: (13509) Defender now exports HTTP Header Fields
FIXED: (21010) Domain Exclusion List – Now Applies to BotNet Detection

CHAPTER 8

Third Party Attributions

Certain open source or other third-party software components are integrated and/or redistributed FlowPro software. The licenses are reproduced here in accordance with their licensing terms, these terms only apply to the libraries themselves, not FlowPro software.

8.1 libcap

http://www.tcpdump.org/ Copyright (c) The Tcpdump Group Licensed under the GNU GPL 2.0 License – see Licenses Directory

8.2 libfixbuf

http://aircert.sourceforge.net/fixbuf/ Copyright (c) 2005-2006 Carnegie Mellon University Licensed under the GNU GPL 2.0 License – see Licenses Directory

8.3 libtldl

http://www.gnu.org/software/libtool/ Copyright (c) 1999, 2003, 2011-2015 Free Software Foundation, Inc. Written by Thomas Tanner, 1999 Licensed under the GNU LGPL 2.1 License – see Licenses Directory

8.4 PF_RING

https://www.ntop.org/products/packet-capture/pf_ring/ Copyright (c) 2004-2014 ntop.org Licensed under the GNU GPL 2.0 License – see Licenses Directory

8.5 Pof

http://lcamtuf.coredump.cx/p0f3/ Copyright (c) 2000-2006 by Michal Zalewski Licensed under the GNU LGPL 2.1 License – see Licenses Directory

8.6 super_mediator

http://tools.netsa.cert.org/super_mediator/ Copyright (c) 2004-2014 Carnegie Mellon University Licensed under the GNU GPL 2.0 License – see Licenses Directory

8.7 tcpdump

http://www.tcpdump.org/ Copyright (c) The Tcpdump Group Licensed under the BSD 3-clause License – see Licenses Directory

8.8 YAF

https://tools.netsa.cert.org/yaf/ Copyright (c) 2005-2013 Carnegie Mellon University Licensed under the GNU GPL 2.0 License – see Licenses Directory