FlowPro Documentation

Release 18.12

Plixer

Jan 22, 2019

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?

1.1 Overview

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.

FlowPro comes with several different licensing options. Explanations of each option are listed below.

1.2 FlowPro license

The basic FlowPro license allows for complete visibility of your network traffic by creating flow data to send to an IPFIX collector to monitor traffic where visibility is limited. FlowPro simply captures the network traffic and generates IPFIX records of the traffic without performing any additional processing.

More features and functionality are available with additional licensing as described below.

1.3 FlowPro APM (Application Performance Monitor) license

With the FlowPro APM (Application Performance Monitoring) licensing, the FlowPro 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

Note: If additional interfaces will be added to the Virtual Appliance, that must be completed prior to requesting the FlowPro APM license.

1.4 FlowPro Defender license

The FlowPro with the FlowPro Defender licensing captures network traffic to provide additional visibility into the traffic within or transiting the organization. It passively monitors the traffic and can perform the following operation on the data:

Monitor 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 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.

1.4.1 Additional Capabilities with the FlowPro Defender license

- Monitor 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 is available as an appliance appropriately sized to the user's network or as a Virtual Appliance download.

1.5 FlowPro APM-Defender license

This licensing option includes the licensing options listed below:

- FlowPro APM (Application Performance Monitoring) licensing
- FlowPro Defender licensing

Enabling and disabling any of the available features and functionality can be performed using the associated *enable* or *disable* command.

CHAPTER 2

Installation

There are several *licensing levels* of the FlowPro available. A valid production or evaluation license key is required with each install. A key can be obtained from Plixer Customer Support or a local reseller.

The steps below describe the process of installing hardware and virtual appliances.

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, connect to the appliance with default IP address of 192.168.168.168/24, and remotely login using the username root and password flowpro. The hardware appliance will perform a quick setup and immediately reboot.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-862.14.4.e17.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

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 edit license command.
4. In the new window, beside *license*=, paste in the license key

```
FlowPro (TM) v18.12 [2018-11-02 19:27:01 -0400 (Fri, 02 Nov 2018)]
Copyright (C) 2012 - 2018 Plixer LLC. All rights reserved.
Need an IPFIX Collector? Download Scrutinizer at https://www.plixer.com

 Install Version : FlowPro (TM) v18.12.14.1235
      Machine ID : 6YZ6XEPT66H66636M95HU54D-1D4621169206AAF2
 License Version :
   Licensed Type :
 Licensed Status : Unlicensed
  Used Mon Ports : 0 of 1
      Expiration : 01/18/2038

 Standard Mode. Type 'edit license' to add a license key.


FLOWPRO> help license


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

[ List of Commands ]

 edit license
 show license

+-------------------------------------------------------------------------+
For more detail type 'help <command>' or '<command> ?'
Full PDF manual can be found at '/home/flowpro/files/flowpro.pdf'
+-------------------------------------------------------------------------+
```

5. Press CTRL+X to save
6. The FlowPro interface(s) must be enabled next for the process that will run on the interface(s), using the *enable command*.

   For example, if the FlowPro is licensed for FlowPro Defender, to activate mon1 for Defender monitoring, enter:

   enable defender mon1

   Other options for enabling the FlowPro interfaces include:

   enable apm <interface> <apmMode> enable flowpro <interface>

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, ESX/ESXi 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	4GB
Disks	20GB
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 Virtual 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
```

(continues on next page)

(continued from previous page)

```
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 edit license command.

```
FlowPro (TM) v18.12 [2018-11-02 19:27:01 -0400 (Fri, 02 Nov 2018)]
Copyright (C) 2012 - 2018 Plixer LLC. All rights reserved.
Need an IPFIX Collector? Download Scrutinizer at https://www.plixer.com

 Install Version : FlowPro (TM) v18.12.14.1235
      Machine ID : 6YZ6XEPT66H66636M95HU54D-1D4621169206AAF2
 License Version :
   Licensed Type :
 Licensed Status : Unlicensed
  Used Mon Ports : 0 of 1
      Expiration : 01/18/2038

 Standard Mode. Type 'edit license' to add a license key.


FLOWPRO> help license


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

[ List of Commands ]

 edit license
 show license

+-------------------------------------------------------------------------+
For more detail type 'help <command>' or '<command> ?'
Full PDF manual can be found at '/home/flowpro/files/flowpro.pdf'
+-------------------------------------------------------------------------+
```

15. In the new window, beside license=, paste in the license key.
16. Press CTRL+X to save
17. The FlowPro interface(s) must be enabled next for the process that will run on the interface(s), using the *enable command*.

    For example, if the FlowPro is licensed for FlowPro Defender, to activate mon1 for Defender monitoring, enter:

        enable defender mon1

    Other options for enabling the FlowPro interfaces include:

        enable apm <interface> <apmMode> enable flowpro <interface>

Note: When *adding additional monitoring interfaces* to the virtual appliance, be sure the interfaces are named using the 'monX' naming convention for the FlowPro to recognize them as monitoring interfaces. ie. mon1, mon2, etc.

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	4GB
Disks	20GB
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. The FlowPro Appliance requires a mirrored port to be associated with 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.

```
********************************
FlowPro Virtual 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

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

Note: When *adding additional monitoring interfaces* to the virtual appliance, be sure the interfaces are named using the 'monX' naming convention for the FlowPro to recognize them as monitoring interfaces. ie. mon1, mon2, etc.

2.6 Adding Additional Interfaces

On the FlowPro appliance, the names of the monitoring interfaces are important. When adding additional interfaces to a virtual appliance, the interfaces must be renamed to something the FlowPro can recognize.

The FlowPro appliance comes with two interfaces by default.

- The 'mgmt' interface is used for management.
- The 'mon1' interface is the first, and by default, the only monitor interface.

When adding additional interfaces to the FlowPro appliance, follow this guide to rename the interfaces from the default 'ethX' to 'monX'.

Important: It is always recommended to take a snapshot of the virtual machine before making any changes.

2.6.1 CentOS 7

This section outlines the process of adding and renaming a new interface for a FlowPro appliance running on CentOS 7. At least a minimal understanding of the CentOS 7 network interface naming is required.

Add a new interface in vmware

1. In vCenter, right click on the VM that the new interface will be added to and select 'Edit Settings...'.

2. From the 'Edit Settings...' window, select 'Add New Device'.
3. From the drop down menu, click on 'Network Adapter'.

Restart the VM

Restarting the VM will make the OS see the newly added interface.

```
$ shutdown -r now
```

Correct the new interface's name

Run these commands to put the mac address for the new interface into the correct ifcfg file.

Important: Before running the last command, verify the interface name is eth0 with the 'ip addr' command.

```
$ cp /etc/sysconfig/network-scripts/ifcfg-mon1 /etc/sysconfig/network-scripts/ifcfg-
↪mon2
$ sed -i 's|mon1|mon2|g' /etc/sysconfig/network-scripts/ifcfg-mon2
$ MAC=$(cat /sys/class/net/eth0/address); sed -i "s|HWADDR=.*|HWADDR=$MAC|g" /etc/
↪sysconfig/network-scripts/ifcfg-mon2
```

Restart the VM, again

Restart the VM so the new name takes effect.

```
$ shutdown -r now
```

After the reboot, verify the interface has the correct name.

```
$ ip addr
```

CHAPTER 3

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.

```
FlowPro (TM) v18.12 [2018-11-02 19:27:01 -0400 (Fri, 02 Nov 2018)]
Copyright (C) 2012 - 2018 Plixer LLC. All rights reserved.
Need an IPFIX Collector? Download Scrutinizer at https://www.plixer.com

 Install Version : FlowPro (TM) v18.12.14.1235
      Machine ID : 6YZ6XEPT66H66636M95HU54D-1D4621169206AAF2
 License Version :
   Licensed Type :
 Licensed Status : Unlicensed
  Used Mon Ports : 0 of 1
      Expiration : 01/18/2038

 Standard Mode. Type 'edit license' to add a license key.


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 Additional Functionality with FlowPro Defender licensing

The following features and functionality are available with the FlowPro Defender (or FlowPro APM-Defender) licensing option.

3.2.1 Trusted Domain List

A "trusted domain list", often called a whitelist, is preconfigured on FlowPro 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 use 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 to 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 domainlist* command to modify the trusteddomains list.

3.2.2 Untrusted Domain Lists

FlowPro 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.

Plixer Domain Reputation List

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

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

Use the *enable domainreputationlist* to enable and the *disable domainreputationlist* to disable the use of this list.

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.
- One DNS name per line.

Entries that do not match these requirements will be ignored.

Use the *edit domainlist* to create (or edit) a custom list of domains to detect domainReputation alarms.

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

Scrutinizer Flow Analytics Algorithms

FlowPro 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 and generate alarms.

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. 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. 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 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 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 every ten minutes and currently contains over 400,000 known bad domains.

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

FlowPro 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. See the *User Defined Domain Lists* section 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 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 exporter into that algorithm. Violations and alarms will show up in the Alarms tab.

3.3 ERSPAN

3.3.1 What is ERSPAN?

ERSPAN is an acronym that stands for Encapsulated Remote Switched Port Analyzer. ERSPAN mirrors traffic on one or more "source" ports and delivers the mirrored traffic to one or more "destination" ports. The traffic is encapsulated in generic routing encapsulation (GRE) and is, therefore, routable across a layer 3 network between the "source" switch and the "destination". In this case, the "destination" is the IP of the monitor interface (e.g. 'mon1') on the FlowPro appliance.

3.3.2 Configuration

Configuration is required on both the FlowPro and the ERSPAN/GRE device.

The order of configuration, whether to configure the FlowPro or the ERSPAN/GRE device first, isn't critical, so long as the prerequisite information listed below is gathered first. Each side of the configuration requires information from the other side (ie. FlowPro and ERSPAN device).

Instructions are provided below for configuring the FlowPro, a Cisco Switch, and a VMWare VDS.

Note: Specific commands and configuration options may vary between devices and versions. It is recommended to verify command syntax with the vendor's documentation for the specific device being configured.

Prerequisites

The following information should be specified prior to starting the configuration.

FlowPro ERSPAN configuration

- Which monitor port? mon1? mon2? The examples in this document will be using 'mon1'.
- Monitor port IP and CIDR (Do not use a /32 CIDR) The examples in this document will be using '10.30.15.50/16'
- Monitor port gateway - The examples in this document will be using '10.30.1.1'
- Peer IP Address - This is the ERSPAN Origin IP defined below. The examples in this document will be using '10.30.1.203'

ERSPAN device configuration

- ERSPAN Origin IP - This should be an IP on the device if it's a switch or a router; if it's a VDS it will be the ESXi host's IP address. The examples in this document are using 10.30.1.203
- Destination IP - This is the FlowPro monitor port IP address (not the FlowPro management IP) The examples in this document are using 10.30.15.50
- Source Interface(s) to SPAN - The example in step 6 of VMWare VDS configuration shows 3 selected.

FlowPro

The monitoring interface(s) must first be enabled as defined in the *Hardware Appliance* or *Virtual Appliance* installation instructions.

Next, refer to the *enable erspan* command for instructions on configuring FlowPro for ERSPAN.

Note: Each monitoring interface on the FlowPro supports only one ERSPAN configuration. Multiple ERSPAN configurations on the same interface (ie. mon1) may produce unpredictable results.

Cisco Switch

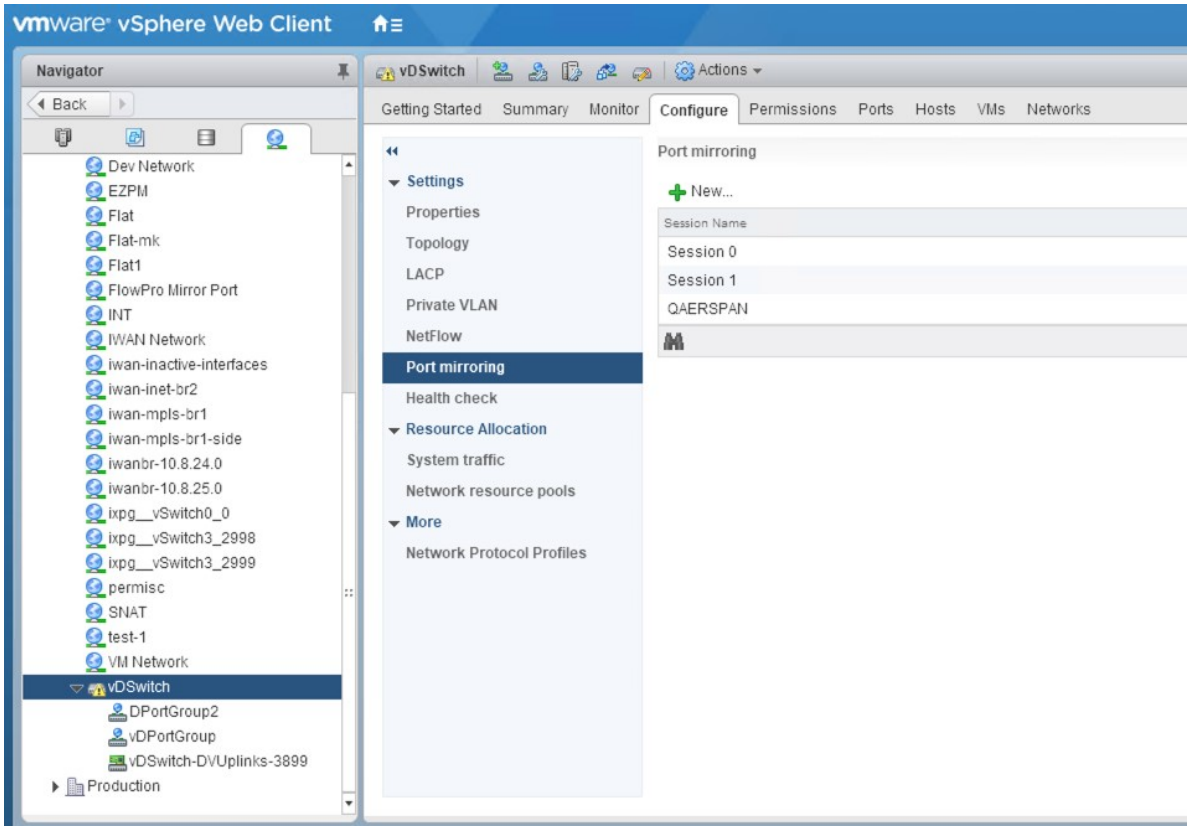
```
monitor session 1 type erspan-source
description ERSPAN direct to FlowPro
erspan-id 32                                # required
vrf default                                 # required
destination ip 10.1.2.3                     # IP address of FlowPro Monitor Interface
source interface port-channel1 both         # Port(s) to be sniffed
no shut                                     # enable

monitor erspan origin ip-address 10.1.2.1 global
```

VMware VDS

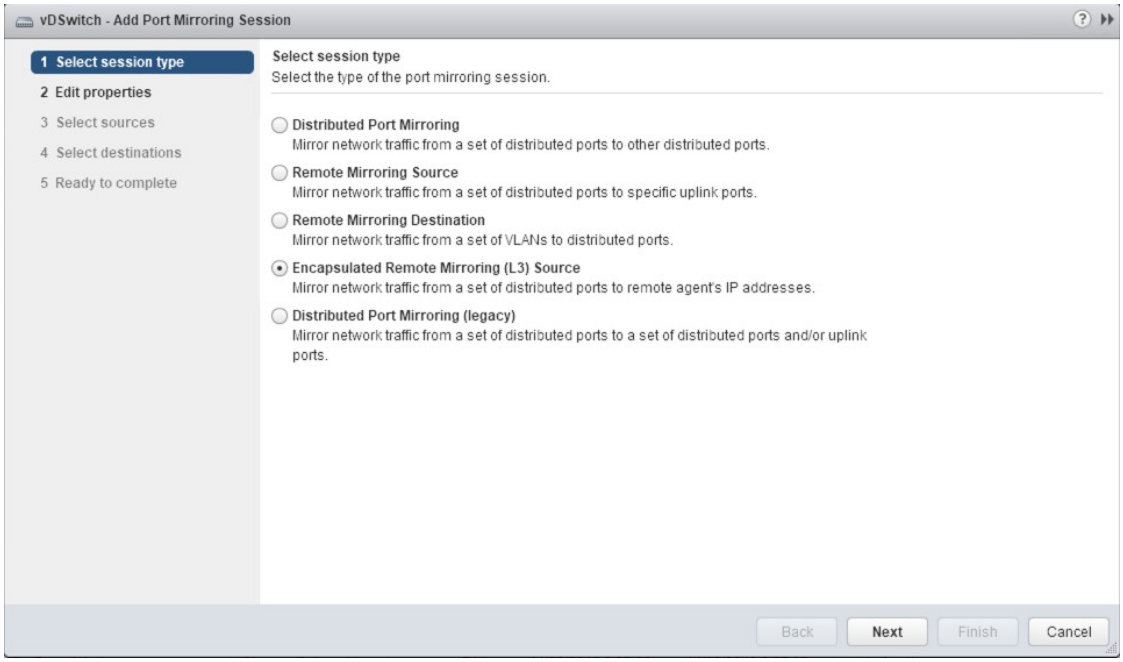
Note: This requires the Enterprise plus license level and a configured virtually distributed switch.

From the web console of VMware:

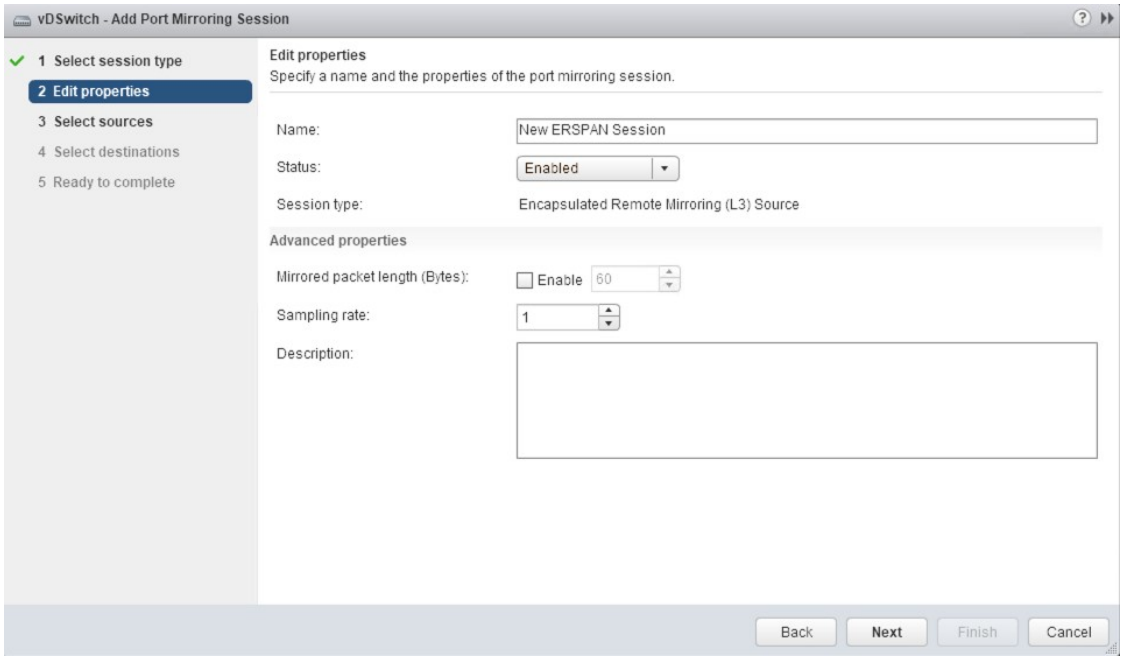
1. Select your VDS from the list of networks.
2. Under the "Configure" tab, select "Port mirroring".
3. Select "New…" to create a new session.



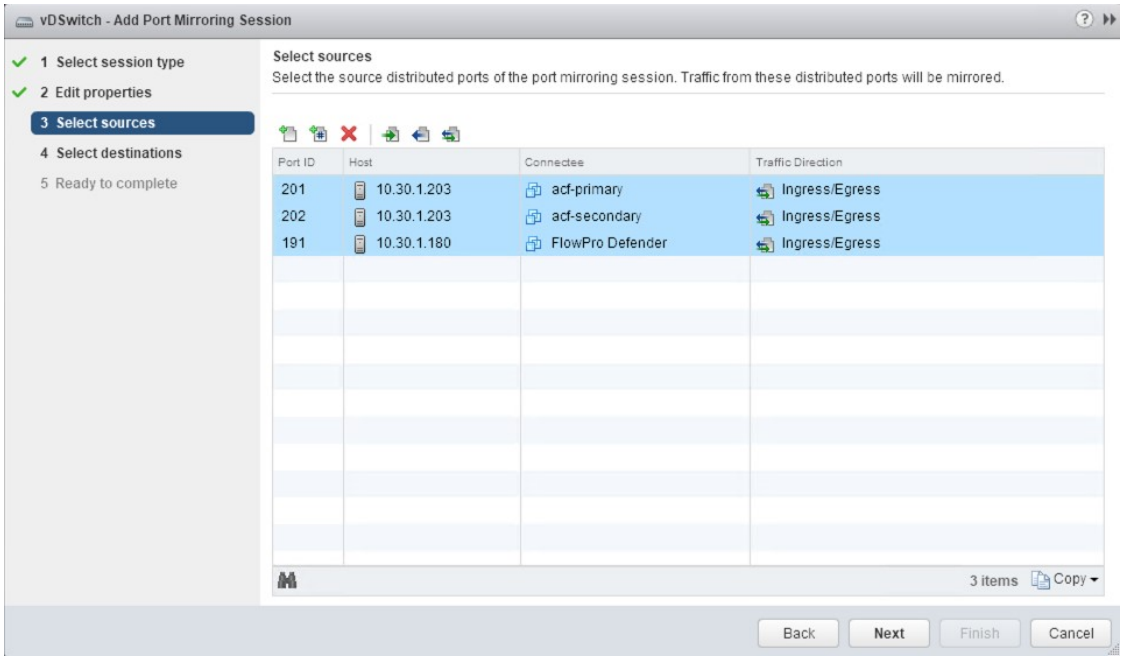
4. Select "Encapsulated Remote Mirroring (L3) Source then click "Next".



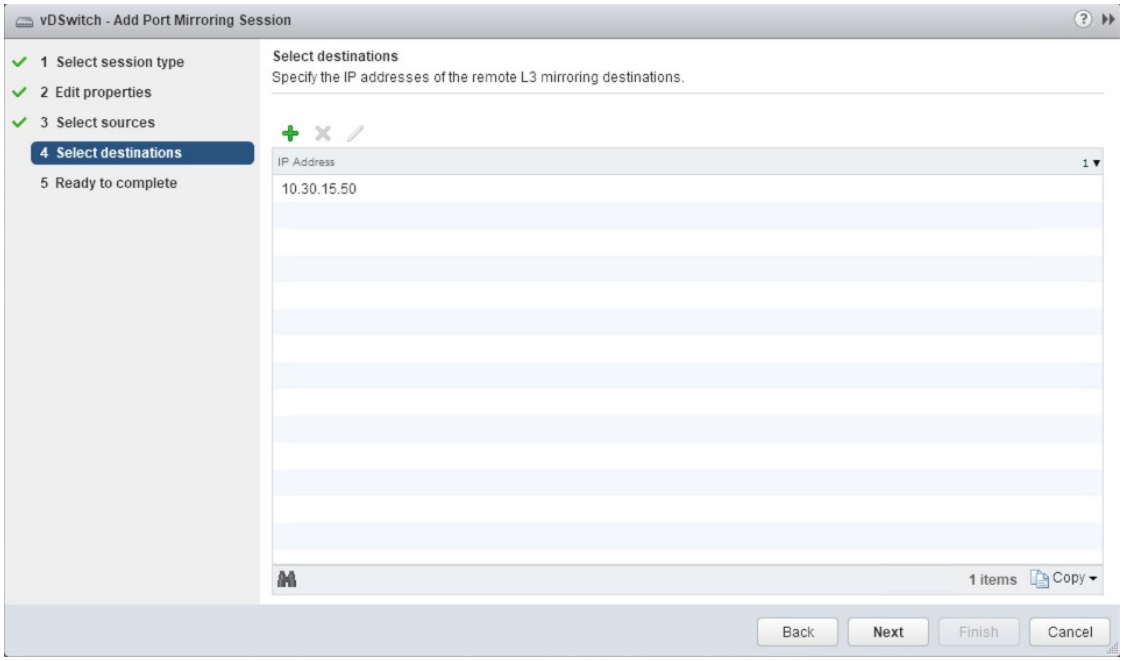
5. Give your new session a name and set the status to Enabled, then click “Next”.



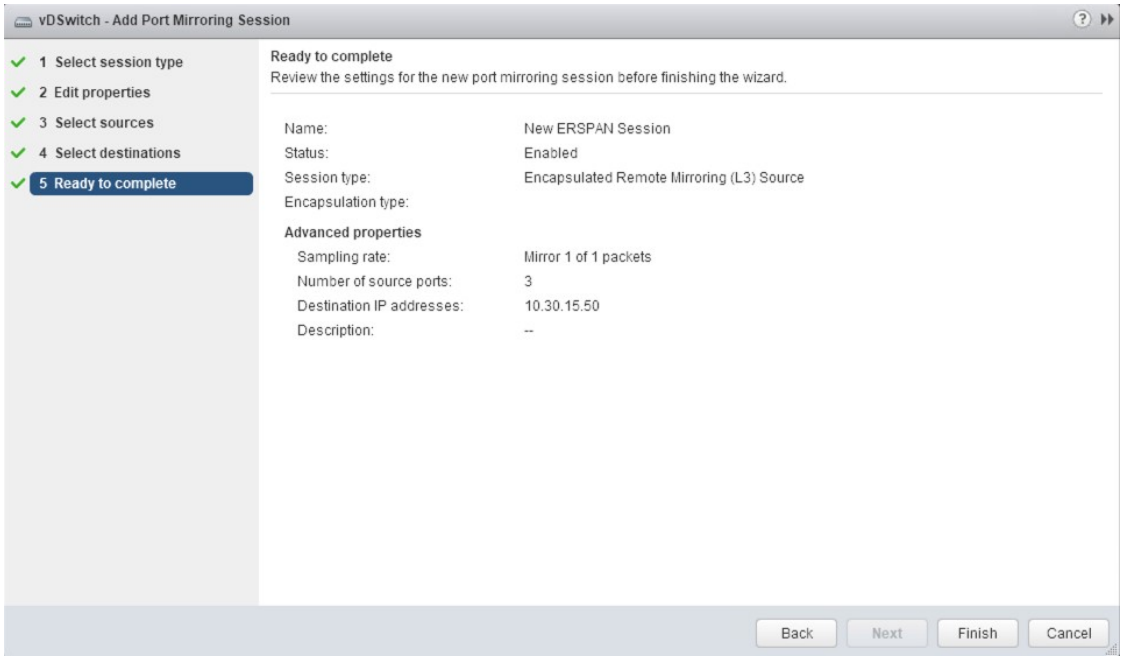
6. Add the ports you wish to mirror to the probe, then click “Next”.



7. Add the IP given to the monitor interface of the probe as the destination of the session, then click “Next”. (not the FlowPro management IP)



8. Verify your configuration and if complete and accurate, select Finish to start the session.



3.4 Server Maintenance

3.4.1 Hardware Failure

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

3.4.2 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*.

3.4.3 Upgrades

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

3.4.4 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.

3.4.5 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.

CHAPTER 4

Commands

4.1 Overview

The FlowPro commands provide access to numerous maintenance utilities, including password changes and other configuration options. Device management utilities are also included in the command list along with many routines to access information required for technical support.

Click on an entry in the Command list table to see the usage of that command.

4.2 Command list

Command	Sub-command
check	*replist*
clear	*domainlist* *log*
disable	*apm* *defender* *domainlist* *domainreputationlist* *erspan* *flowpro* *HTTPMonitoring* *trackProcessMetrics*
edit	*domainlist* *license* *plixer.ini*
enable	*apm* *defender* *domainlist* *domainreputationlist* *erspan* *flowpro* *HTTPMonitoring* *trackProcessMetrics*
service	*flowpro*
set	*activeDomainResendSeconds* *collector* *hostname* *password*
show	*configuration* *domainlist* *erspan* *features* *interfaces* *license* *log* *status*
snoop	*interface* *ipaddress*
system	*restart* *shutdown*

4.3 Command usage

4.3.1 check

Check different settings and configurations on the FlowPro appliance.

check replist

Usage: check replist

Description: Check the ability for FlowPro to reach nba.plixer.com to download the reputation lists every ten minutes. If this appliance does not have access to the internet, contact Plixer's Support for help.

Note: This feature requires the *Defender licensing*.

4.3.2 clear

Clean up or remove data from a system. Use with caution.

clear domainlist

Usage: clear domainlist <domain_list>

Description: Remove a domainlist from the system. Use with caution. Use the *show domainlist* command to see a list of active domainlists.

Note: This feature requires the *Defender licensing*.

---

clear log

Usage: clear log <log_file>

Description: Remove data from a specific log file. Use with caution. To get a list of active logs, use the *show log* command.

Note: You can not remove data from the cli.log file.

EXAMPLE: FLOWPRO> clear log dns1yaf.log

4.3.3 disable

Disable Settings.

disable apm

Usage: disable apm <interface> <apmMode>

Description: Disable either Latency, VOIP or both monitoring on an interface. That interface must be active. Valid apmModes are:

voip latency both

Use the *show configuration* command to get a list of currently enabled interfaces.

Note: This feature requires the *APM licensing*.

---

disable defender

Usage: disable defender <interface>

Description: Disable DNS monitoring on an interface. That interface must be active. Use the *show configuration* command to get a list of currently enabled interfaces.

Note: This feature requires the *Defender licensing*.

disable domainlist

Usage: disable domainlist <domain_list>

Description: Disable a custom domain reputation list. The domain list disabled will not be removed and can be re-enabled with the *enable domainlist* command.

Note: This feature requires the *Defender licensing*.

disable domainreputationlist

Usage: disable domainreputationlist

Description: Disable the check against domain reputation lists configured on the system. To see available domain lists, use the *show domainlist* command.

Note: This feature requires the *Defender licensing*.

disable erspan

Usage: disable erspan <interface>

Description: Disable the ERSPAN configured on a monitoring interface.

disable flowpro

Usage: disable flowpro <interface>

Description: Disable traffic monitoring on an interface. Use the *show configuration* command to get a list of currently enabled interfaces.

disable HTTPMonitoring

Usage: disable HTTPMonitoring

Description: This process keeps track of all domains hit with HTTP. The list of currently active domains is saved for the amount of seconds set by the *set activeDomainResendSeconds* command.

HTTP monitoring will be on the same interfaces that are configured in the *enable defender* command.

Note: This feature requires the *Defender licensing*.

disable trackProcessMetrics

Usage: disable trackProcessMetrics

Description: Disable FlowPro process metrics.

4.3.4 edit

Edit the configuration files used by FlowPro.

edit domainlist

Usage: edit domainlist <domain_list>

Description: Edit a custom domain reputation list. The name of the domain list given on the command line will create a new list of that name if none exists already.

The custom domain reputation list created must contain one domain per line and each domain must contain a two layer domain. Domains that are not at least 2 layers will be ignored.

Note: This feature requires the *Defender licensing*.

---

edit license

Usage: edit license

Description: Opens the plixer.ini file where the license key is stored. The plixer.ini file is where configurations for FlowPro are stored. After editing the plixer.ini file, FlowPro will restart services to pull in any new changes made.

edit plixer.ini

Usage: edit plixer.ini

Description: Opens the plixer.ini file for edit. The plixer.ini file is where configurations for traffic monitoring are stored. After editing the plixer.ini file, FlowPro will restart services to pull in any new changes made.

4.3.5 enable

Enable monitoring options. All settings can be set inside the configuration file using 'edit plixer.ini'.

enable apm

Usage: enable apm <interface> <apmMode>

Description: Enable either Latency, VOIP or both monitoring on an interface. That interface must be active. Valid apmModes are:

voip latency both

Use the *show interfaces* command to get a list of available monitoring interfaces.

Note: This feature requires the *APM licensing*.

---

enable defender

Usage: enable defender <interface>

Description: Enable DNS monitoring on an interface. That interface must be active. Use the *show interfaces* command to get a list of available monitoring interfaces.

Note: This feature requires the *Defender licensing*.

---

enable domainlist

Usage: enable domainlist <domain_list>

Description: Enable a custom domain reputation list. In addition to the known compromised domain list provided by Plixer, you can create your own list.

To create a new list, use the '*edit domainlist* <domain_list_name>' command.

Note: This feature requires the *Defender licensing*.

---

enable domainreputationlist

Usage: enable domainreputationlist

Description: Enable FlowPro to download an updated list of known compromised domains. This list will be downloaded from nba.plixer.com every ten minutes. Use the *check replist* command to check connection to the list.

Note: This feature requires the *Defender licensing*.

---

enable erspan

Usage: enable erspan <interface> <ipaddress/cidr> <gateway> <peerIPaddress>

Description: Configure a monitor interface to receive traffic sent from an ERSPAN/GRE tunnel. This configuration supports all types of GRE tunnels.

All of the following parameters are required:

- interface
- ipaddress/cidr
- gateway
- peerIPaddress

<interface> is which interface to use to monitor the ERSPAN/GRE tunnel traffic. The interface used must be one of the monitor interfaces listed when the command *show interfaces* is used.

<ipaddress/cidr> is the IP address dedicated to the ERSPAN/GRE tunnel. This IP must be routable from the monitoring interface to the device configured to send ERSPAN/GRE. Both an IP address and a cidr are required and must be unique to this interface. Do not use the IP address of the management interface of the FlowPro appliance.

<gateway> is used by the monitor interface and is needed to create a route to keep the outgoing traffic from the ERSPAN/GRE tunnel localized to the monitor interface.

<peerIPaddress> is the external address of the switch configured for ERSPAN/GRE. If the device configured is VMware, the IP address of the host should be used.

Command Example:

enable erspan mon1 10.30.15.50/16 10.30.1.1 10.30.1.203

Go to the *ERSPAN configuration* for instructions on configuring the ERSPAN/GRE device configuration.

enable flowpro

Usage: enable flowpro <interface>

Description: Enable traffic monitoring on an interface. That interface must be active. Use the *show interfaces* command to get a list of available monitoring interfaces.

enable HTTPMonitoring

Usage: enable HTTPMonitoring

Description: This process keeps track of all domains hit with HTTP. The list of currently active domains is saved for the amount of seconds set by the *set activeDomainResendSeconds* command.

HTTP monitoring will be on the same interfaces that are configured in the *enable defender* command.

Note: This feature requires the *Defender licensing*.

---

enable trackProcessMetrics

Usage: enable trackProcessMetrics

Description: Send process information to your collector about the FlowPro processes. Information about cpu and memory usage will be sent to the collector.

4.3.6 service

service flowpro

Usage: service flowpro <start|stop|restart>

Description: Control the FlowPro service daemon.

4.3.7 set

Change various settings for the FlowPro appliance.

set activeDomainResendSeconds

Usage: set activeDomainResendSeconds <seconds>

Description: Set the amount of seconds to resend the active domain list to your collector. The active domain list is a list of domains seen by the defender http module since the last time the list was sent from the FlowPro. To enable the HTTP monitoring, run the *enable HTTPMonitoring* command. Seconds can be set to a whole number between 300 (5 minutes) and 86400 (24 hours).

Note: This feature requires the *Defender licensing*.

---

set collector

Usage: set collector <ip> <port>

Description: Configure the collector and port number for the FlowPro to send flows to. The collector's IP and port are required for this setting. The collector must be configured to listen on the port the FlowPro is sending to or flows will not be collected.

set hostname

Usage: set hostname <hostname>

Description: Change the hostname of the FlowPro appliance. The 'hostname' parameter is required. A reboot is required for this change to take effect.

set password

Usage: set password

Description: Change the password for the 'flowpro' operating system user.

4.3.8 show

Check information or settings from FlowPro.

show configuration

Usage: show configuration

Description: Shows FlowPro's current configuration options and values.

show domainlist

Usage: show domainlist

Description: Shows all custom domainlists configured on the system. To edit the custom domain list, run the *edit domainlist* command.

Note: This feature requires the *Defender licensing*.

---

show erspan

Usage: show erspan

Description: Shows FlowPro's current ERSPAN configuration information. Only one ERSPAN tunnel per interface can be configured at a time.

show features

Usage: show features

Description: Shows FlowPro's current licensed features.

show interfaces

Usage: show interfaces

Description: Shows interfaces available to be configured for monitoring mirrored traffic.

show license

Usage: show license

Description: Shows current license information.

show log

Usage: show log <log_file>

Description: Shows the current log entries for the given log. 'show log' without naming a <log_file> will print out available logs for viewing.

show status

Usage: show status

Description: Shows status of FlowPro processes.

4.3.9 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. This command runs tcpdump with a filter of either an interface or ip address.

snoop interface

Usage: snoop interface <INTERFACE>

Description: Runs tcpdump filtering on a specific interface. Use the *show interfaces* command to see a list of available interfaces. To exit the snoop command, hit CTRL+C.

snoop ipaddress

Usage: snoop ipaddress <IPADDRESS>

Description: Runs tcpdump with a filter of an ip address. To exit the snoop command, hit CTRL+C.

4.3.10 system

The system command is used to change state of the FlowPro operating system.

system restart

Usage: system restart

Description: Restart the operating system.

system shutdown

Usage: system shutdown

Description: Shutdown the operating system.

CHAPTER 5

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.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 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 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

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 18.12.14 - 1/21/2019

ADDED: (14) Consolidated all FlowPro license types to one probe
ADDED: (120) Support for ERSPAN
ADDED: (121) Defender decapsulates GRE packets
ADDED: (376) Weekly log rotation

FIXED: (377) Defender no longer truncates logs on restart

7.1.2 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

---

7.1.3 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