FlowPro Documentation

Release 19.1.2

Plixer

Mar 14, 2024

VERSION 19.1.2

Welcome to the Plixer FlowPro online manual.

Click here to view the full Plixer FlowPro command list, or download this documentation in PDF format here.

Tip: For questions or concerns, contact Plixer Technical Support.

CHAPTER

ONE

PLIXER FLOWPRO - OVERVIEW

1.1 What is Plixer FlowPro?

Plixer FlowPro is a network monitoring solution that ensures your IT teams always have access to the information they need to investigate and analyze network performance and security events, despite infrastructure limitations.

1.2 How does Plixer FlowPro work?

Because traffic transparency is a vital to efficient asset management and proactive threat defense, network visibility limtations can severely hamper efforts to identify and respond to issues.

Plixer FlowPro enables visibility in a network's blind spots by capturing network traffic, generating the corresponding IPFIX records, and forwarding the data to a suitable flow collector, such as Plixer Scrutinizer.

Plixer FlowPro is available as a rack-mountable hardware appliance or in virtualized ESX-, Hyper-V-, or KVM-based packages.

1.3 Licensing

Plixer FlowPro is offered in the following license options:

Plixer FlowPro

The core Plixer FlowPro license enables complete network visibility by generating flow data for otherwise invisible traffic and forwarding it to an IPFIX Collector without requiring additional processing.

Plixer FlowPro APM

The **APM** (Application Performance Monitoring) enables application visibility from Layers 2 through 7 and allows Plixer FlowPro to capture and include the following application-level data in flows sent:

- Latency data on clients, servers, and Layer 7 applications through Deep Packet Inspection
- Traffic metrics related to SIP, RTP, and voice quality
- Latency + traffic metrics (dual mode)

Plixer FlowPro Defender

With the **Defender** license, Plixer FlowPro can leverage DNS monitoring techniques to provide enhanced visibility and malware detection through the following features:

- BotNet detection
- DNS lookups of domains likely associated with malware

- Data exfiltration detection
- Command and control detection

DNS queries are compared against a domain reputation list and matched with known responses to identify potentially malicious traffic, such as *no existing domain* (NXDOMAIN) and long, complete DNS names that do not properly resolve. Plixer FlowPro Defender is also able to monitor other types of DNS messages, such as DNS TXT messaging to bypass firewall restrictions, and supports user-defined domain whitelists and blacklists.

Plixer FlowPro APM-Defender

The **APM-Defender** license combines the functions included in the *APM* and *Defender* licenses and allows Plixer FlowPro to deliver valuable network and security insights while enabling complete visibility in any type of environment.

Note: All Plixer FlowPro license levels support the disabling (and later re-enabling) of individual features as needed. To learn more, see the *Advanced Services section* of this manual.

CHAPTER

TWO

DEPLOYMENT GUIDES

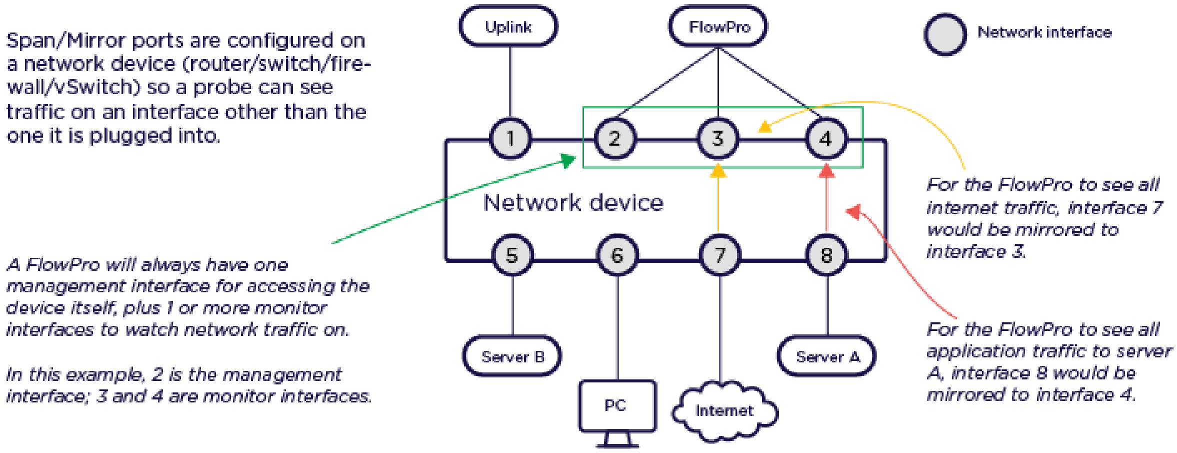
This section covers the deployment procedure of Plixer FlowPro hardware and virtual appliances.

Note: A valid production or evaluation license key is required with each install. A key can be obtained from *Plixer Support* or a local reseller.

2.1 Span Configuration

This section covers how and where to deploy *Plixer FlowPro*, *Plixer FlowPro APM*, and *Plixer FlowPro Defender*.

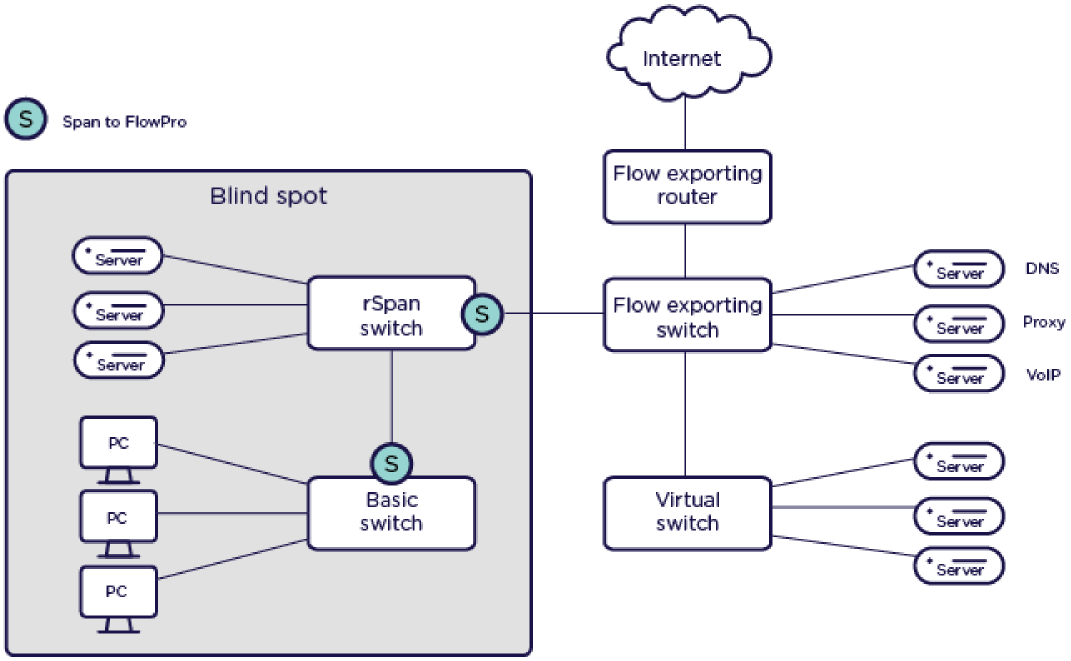
2.1.1 Span ports


Span/Mirror ports are configured on a network device (router/switch/firewall/vSwitch) so a probe can see traffic on an interface other than the one it is plugged into.
Uplink
FlowPro
Network interface
1
2
3
4
Network device
5
6
7
8
For the FlowPro to see all internet traffic, interface 7 would be mirrored to interface 3.
A FlowPro will always have one management interface for accessing the device itself, plus 1 or more monitor interfaces to watch network traffic on.
In this example, 2 is the management interface; 3 and 4 are monitor interfaces.
Server B
PC
Internet
Server A
For the FlowPro to see all application traffic to server A, interface 8 would be mirrored to interface 4.

Note: Monitoring a 1Gb interface requires two (2) 1Gb spans to the Plixer FlowPro: one for ingress and one for egress flows (see *Ingress, Egress, and Observation Domain Configuration* for more information).

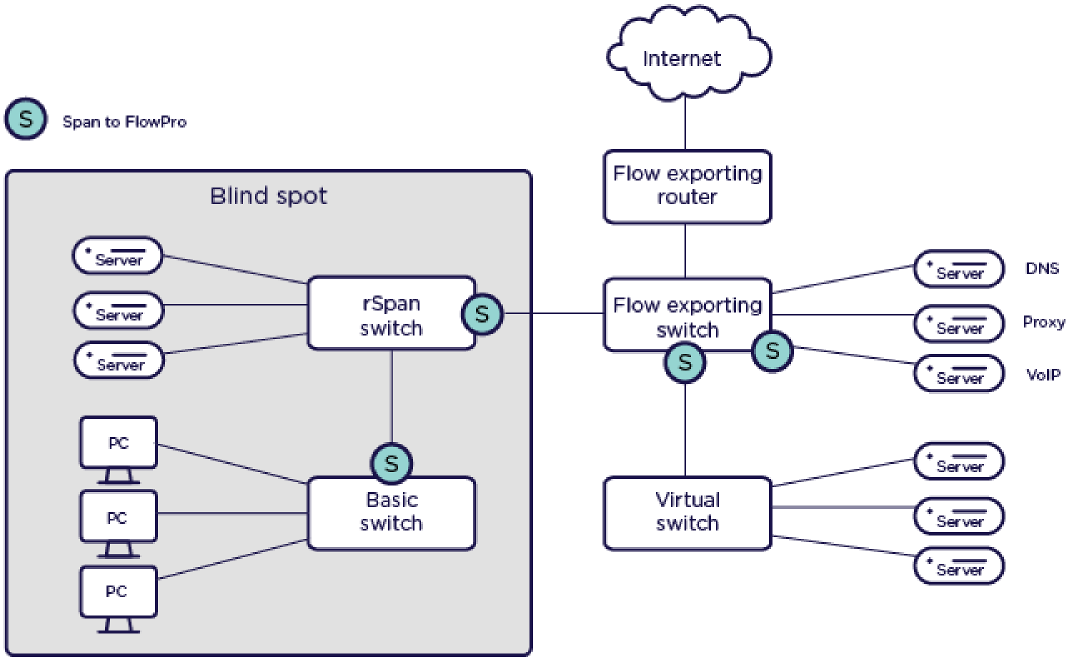
2.1.2 Plixer FlowPro

Visibility where you need it.



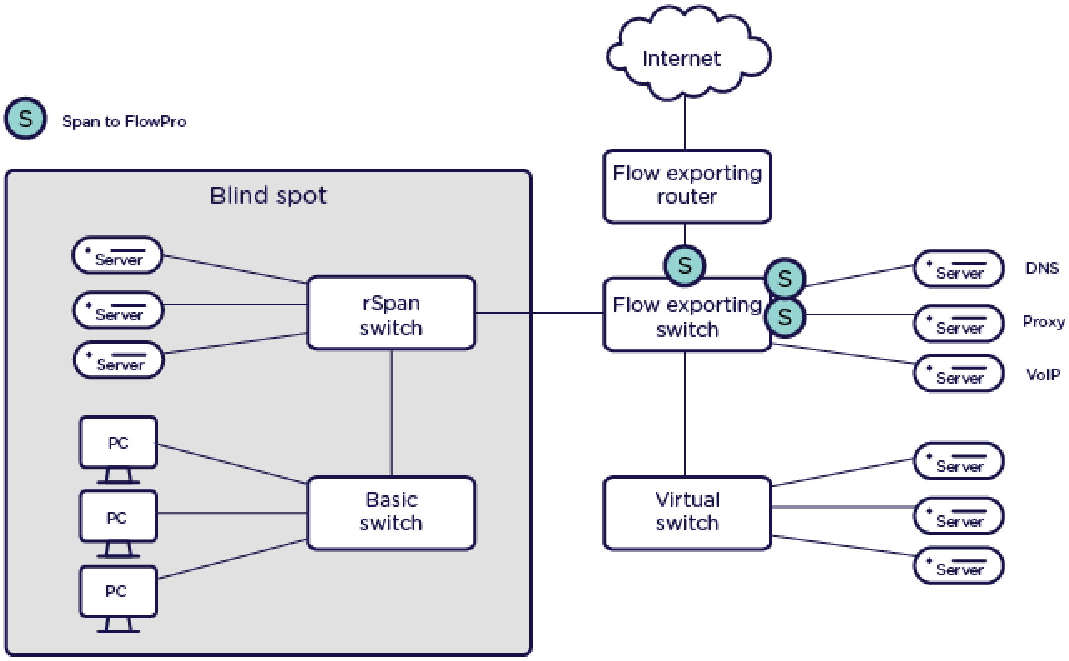
2.1.3 Plixer FlowPro APM

Application Performance Monitoring



2.1.4 Plixer FlowPro Defender

Security through watching DNS and HTTP traffic



2.2 Hardware Appliance

To deploy the Plixer FlowPro hardware appliance, follow these steps after it has been mounted in a server or network rack:

1. Using an SSH client, login remotely at the default IP address of 192.168.168.168/24, with the username `flowpro` and password `flowpro` and wait for the appliance to execute a quick setup routine and immediately reboot.
2. Login again using the username `flowpro` and password `flowpro` and enter the answers to the configuration questions that follow.
3. After the Plixer FlowPro reboots to apply the new settings, login with the new credentials entered during the previous step.
4. Issue the `edit license` command to enter the license key.
5. Paste the license key between the EOT markers after the label `license=` in the [Client] section of the plixer.ini file. The license key may span multiple lines.
6. Press CTRL+X to save your settings.
7. The interface must be enabled for the Plixer FlowPro process that will run on that interface using the *enable command*.

   For example, to activate Plixer FlowPro Defender monitoring on mon1: `enable defender mon1`

   The commands to enable the other Plixer FlowPro processes on a specific interface are:

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

2.3 Virtual Appliance

Plixer FlowPro is available in standard virtual appliance packages for VMware ESX, Microsoft Hyper-V, and KVM environments.

All types of Plixer FlowPro virtual appliances are available through Plixer or a local reseller, who will assist you with acquiring the evaluation or subscription license key required to activate the product.

To deploy the virtual appliance of your choice, follow the corresponding guide below:

2.3.1 Virtual Appliance - ESX

To deploy the Plixer FlowPro virtual appliance for ESX environments, take note of the following additional requirements and proceed with the subsequent setup process:

Note: The Plixer FlowPro virtual appliance for ESX is provided as an all-in-one OVF template to streamline the deployment process.

2.3.1.1 System Requirements

Component	Minimum Specifications
Memory	4GB DDR3
Storage	20GB SATA drive
Processor	2.0 GHz Quad Core CPU
Operating System	ESXi 5.5

2.3.1.2 Deploying the OVF Template

1. After downloading the latest version of the Plixer FlowPro virtual appliance, connect to the ESX host where the appliance will be deployed using VMware, vSphere, or vCenter.
2. Select **File > Deploy OVF Template**.
3. Select **Deploy from File**, navigate to the OVF Template, and click **Next**.
4. Review the OVF template details and click **Next**.
5. Provide a name for the Plixer Scrutinizer virtual appliance and continue to follow the deployment wizard.
6. Review the **Virtual Settings**, and click **Finish** to complete importing the OVF Template.

Note: The virtual appliance is configured with 2 network adapters (mgmt and mon1), with mon1 already in promiscuous mode. By default, it will start listening for traffic on the default virtual network. A mirror port of a Virtual Distributed Switch or a mirror port using a physical NIC on the ESXi host will have to be configured if a different network needs to be monitored.

7. Power on the Plixer FlowPro virtual machine.
8. Navigate to the **Console** tab and log in using the username `flowpro` and password `flowpro`.
9. After the machine performs a quick setup and reboots, log in again with the same credentials and enter the answers to the configuration questions that follow.

10. After the Plixer FlowPro reboots to apply the new settings, log in with the new credentials entered during the previous step.
11. Issue the `edit license` command to enter the license key.
12. Paste the license key between the EOT markers after the label `license=` in the [Client] section of the plixer.ini file. The license key may span multiple lines.
13. Press CTRL+X to save.
14. The interface must be enabled for the Plixer FlowPro processes that will run on that interface using the *enable command*.

    For example, to activate Plixer FlowPro Defender montoring on mon1: `enable defender mon1`

    The commands to enable the other Plixer FlowPro processes on specific interfaces are:

    ```
    enable apm \<interface\> \<apmMode\> <enable_apm> enable flowpro \<interface\
    > <enable_flowpro>
    ```

Note: When *adding additional monitoring interfaces* to the virtual appliance, be sure to use the interface naming convention monX so that Plixer FlowPro recognizes them as monitoring interfaces (for example: mon1, mon2).

2.3.1.3 Upgrading the Virtual Machine Hardware Version

To upgrade the Virtual Machine hardware version:

1. Shut down the virtual machine.
2. Right-click on the virtual machine in vSphere (or vCenter) and select **Upgrade Virtual Hardware**.

2.3.2 Virtual Appliance - Hyper-V

To deploy the Plixer FlowPro virtual appliance for Hyper-V environments, take note of the following additional requirements and proceed with the subsequent setup process:

2.3.2.1 System Requirements

Component	Minimum Specifications
Memory	4GB DDR3
Storage	20GB SATA drive
Processor	2.0 GHz Quad Core CPU
Operating System	Hyper-V 2012

2.3.2.2 Importing a Virtual Machine

1. After downloading the latest version of the Plixer FlowPro virtual appliance, unzip the package on the Hyper-V server.
2. Open **Hyper-V Manager**, right-click the virtual machine, and select **Import Virtual Machine**.
3. Browse to the location of the Plixer FlowPro appliance system folder.
4. Select the virtual machine and import type.
5. Go to **Settings**, select the network adapter, and assign it to the appropriate virtual switch.

Note: The Plixer FlowPro appliance comes with two interfaces: 'mgmt': for virtual appliance management and 'mon1': the default monitoring interface. It requires a mirrored port to be associated with 'mon1'. To set up a mirrored port, refer to the latest Hyper-V documentation.

6. In the network adapter's **Advanced Features** section, set the MAC address to **Static**, enter a unique MAC Address, and click **OK**.
7. Start the virtual machine, right-click on it, and select **Connect**.
8. Log in with the username `flowpro` and password `flowpro` and wait for the server to reboot after a quick setup.
9. Issue the `edit license` command to enter the license key.
10. Paste the license key between the EOT markers after the label `license=` in the [Client] section of the plixer.ini file. The license key may span multiple lines.
11. Press CTRL+X to save.

Note: When *adding additional monitoring interfaces* to the virtual appliance, be sure to use the interface naming convention 'monX' so that Plixer FlowPro recognizes them as monitoring interfaces (for example: mon1, mon2).

2.3.3 Virtual Appliance - KVM

To deploy the Plixer FlowPro virtual appliance for KVM environments, take note of the following additional requirements and proceed with the subsequent setup process:

2.3.3.1 System Requirements

Component	Minimum Specifications
Memory	4GB DDR3
Stprage	20GB SATA drive
Processor	2.0 GHz Quad Core CPU
Operating System	KVM 14

2.3.3.2 Importing a Virtual Machine

1. Create a directory for your install by entering `mkdir kvm/FlowPro_VM/`.
2. Download the latest version of the Plixer FlowPro KVM Virtual Appliance and place in the install directory.

   Note: Contact *Plixer Support* to obtain the latest Plixer FlowPro KVM image.

3. Unzip the file in the install directory on your KVM server by entering `sudo tar xvzf FlowPro_KVM_Image.tar.gz`.
4. Enter `sudo ./deploy-flowpro.sh` to run the install script.
5. Log in to the virtual appliance and use the `virsh console Plixer FlowPro` command to get to the console.
6. Log in with the username `flowpro` and the password `flowpro` and wait for the virtual machine to reboot.
7. When prompted, log in again and follow the shell script to enter the networking settings for the virtual appliance.
8. Issue the `edit license` command to enter the license key.
9. Paste the license key between the EOT markers after the label `license=` in the [Client] section of the plixer.ini file. The license key may span multiple lines.
10. Press CTRL+X to save.

2.4 Adding Additional Interfaces

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

The Plixer FlowPro appliance comes with two interfaces by default:

- ‘mgmt’: for virtual appliance management
- ‘mon1’: the default monitoring interface

Follow the instructions below to add additional interfaces to the Plixer FlowPro appliance and rename them from the default ‘ethX’ to ‘monX’.

Important: Take a snapshot of the virtual machine before making any changes.

2.4.1 CentOS 7

This section outlines the process of adding and renaming a new interface for a Plixer FlowPro appliance running on CentOS 7.

2.4.1.1 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’.
4. Run the following command:

```
$ ~flowpro/util/configure_new_adapter
```

CHAPTER

THREE

FEATURES AND FUNCTIONALITY

3.1 Plixer FlowPro Defender Functionality

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

3.1.1 Trusted Domain List

A trusted domain list, or whitelist, is preconfigured on Plixer FlowPro to suppress alarms involving specific domains. The default whitelist contains five entries that can added or removed depending on the customer environment.

- mcafee.com
- sophos.com
- sophosxl.net
- webcfs03.com
- apple.com
- aaplimg.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 stores this information on 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 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 exchange settings with their NTP server. This will trigger 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 those domains to the trusted domain list. Once configured, any other traffic communicating via DNS should be investigated.

Use the *edit domainlist* command to modify the trusted domain list.

3.1.2 Untrusted Domain Lists

Plixer FlowPro supports the use of a domain reputation list downloaded from Plixer as well as user-defined domain lists.

3.1.2.1 Plixer Domain Reputation List

Plixer FlowPro can be configured 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, Plixer FlowPro periodically updates the domain reputation list. During setup, please verify a network route exists from Plixer FlowPro to `nba.plixer.com`. The Domain Reputation algorithm will not detect any malware if Plixer FlowPro is unable to connect to `nba.plixer.com` - however, all other features will function normally.

Use the following Plixer FlowPro commands to control the use of this list:

- *enable domainreputationlist* to enable
- *disable domainreputationlist* to disable

3.1.2.2 Plixer JA3 Signatures

Plixer FlowPro can be configured to download a list of JA3 Signatures from Plixer.

Use the following Plixer FlowPro commands to control the use of this signature list:

- *enable domainreputationlist* to enable
- *disable domainreputationlist* to disable

3.1.2.3 User-defined Domain Lists

Users may supplement the Plixer domain reputation list by creating one or more domain lists that contain user-defined domains to monitor. Domain names in the list must adhere to the following rules:

- DNS names must contain at least 2 (2LD) but no more than 3 (3LD) labels. For example: google.com (2LD) and maps.google.com (3LD)
- Labels must contain between 1 and 63 characters to form a legitimate domain name
- One DNS name per line

Entries that do not match these requirements will be ignored.

Use the following Plixer FlowPro command to create or edit a custom list of domains to trigger Domain Reputation alarms:

- *edit domainlist*

Use the following Plixer FlowPro commands to enable or disable custom domain lists:

- *enable domainlist* to enable
- *disable domainlist* to disable

3.1.2.4 User-defined JA3 Signature Lists

The JA3 blacklist functionality supports custom blacklists specified in either a *bin* or *csv* format.

To import the user-defined JA3 blacklist CSV file, use the filename and path: `/home/flowpro/conf/domains/ja3-custom.csv`

The expected format is one MD5 hash in hexadecimal, without leading 0x, per line. Once you upload the CSV file containing signatures to the `/home/flowpro/conf/domains/` directory, Plixer FlowPro will then check for an updated JA3 list every minute and reload it if there are any changes.

Important: Contact *Plixer Technical Support* for assistance with the JA3 bin import option.

3.1.3 Plixer Scrutinizer Flow Analytics Algorithms

Plixer FlowPro will send data to the specified IPFIX Collector. Plixer Scrutinizer provides additional functionality to check for malicious behavior and bad actors, and to generate alarms when detected.

3.1.3.1 BotNet Detection

This alarm is generated when a large number of unique DNS name lookups have failed. When a DNS lookup fails, a NXDOMAIN reponse is returned. Plixer Scrutinizer is able to identify a class of malware that uses Domain Generation Algorithms (DGAs) by monitoring the number of NXDOMAINs detected as and the actual DNS name looked up.

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

3.1.3.2 DNS Command and Control

This algorithm monitors the use of DNS TXT messages traversing the network perimeter as detected by Plixer FlowPro. DNS TXT messages can be used to send information into and out of the protected network over DNS, even when the use of external DNS servers has been blocked. Malware uses this technique to control compromised assets within the network and to extract information back out. Additionally, some legitimate software also uses this method to communicate back to the developer site.

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

The domain generating the alarm message may be added to the trusted domains list in Plixer FlowPro to suppress alarms from authorized applications on the network. See the information regarding the trusted domains list below.

3.1.3.3 DNS Data Leak

This algorithm monitors for information encoded into a DNS lookup message that has no intention of returning a valid IP address or making an actual connection to a remote device. As a result, 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.

Plixer FlowPro reviews all DNS queries and responses using proprietary logic to detect unwanted communications. Odd behaviors are sent to Plixer Scrutinizer where they are further processed by the DNS Data Leak algorithm. Thresholds can be set based on either 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 trigger an alarm and alarm aggregation defaults to 120 minutes.

3.1.3.4 DNS Server Detection

The algorithm detects new DNS servers being used on or by your network through analysis of the DNS packets being exchanged between the client and the server. Exclude DNS servers that are authorized for use on the network.

3.1.3.5 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 provided by Plixer is updated periodically and currently contains over 400,000 known bad domains.

To provide maximum protection, the Plixer FlowPro must be able to update its domain reputation list periodically. For that purpose, during setup, please verify a network route exists from Plixer FlowPro to nba.plixer.com. The Domain Reputation algorithm will not detect any malware if the Plixer FlowPro is unable to connect to nba.plixer.com - however, all other features will function normally.

The Plixer FlowPro performs the actual monitoring, and when it detects a domain with poor reputation, it passes the information to Plixer Scrutinizer for additional processing. The default setting is for any detected traffic to trigger an 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 domain generating the alarm message can be added to the trusted domain list in Plixer FlowPro. See the *User-defined Domain Lists* section for details.

3.1.3.6 JA3 Fingerprinting

The JA3 fingerprinting functionality leverages the unique characteristics of the TLS handshake to identify the software generating encrypted traffic by comparing it against a list of known signatures. If a positive match is made, Plixer FlowPro Defender will send the details of that connection to Plixer Scrutinizer.

3.1.3.7 Malware Behavior Detection

This algorithm demonstrate Plixer's cyber threat correlation capability. Correlation of multiple network behaviors over a long time period provides detection systems with more information resuting in higher accuracy with fewer false positive alarms.

This specific alarm correlates IP address lookup (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 a Domain Reputation alert.

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.

3.1.3.8 Adding Plixer FlowPro to the Algorithms

The Plixer FlowPro appliance(s) must be linked to the algorithms the user wishes to use in the Plixer Scrutinizer Flow Analytics configuration settings:

- Navigate to the Admin Tab > Settings > Flow Analytics Configuration
- Click the numbers in the exporter column to associate the Plixer FlowPro exporter with that algorithm
- Violations and alarms will be displayed in the Alarms tab

3.2 ERSPAN

ERSPAN is the acronym for Encapsulated Remote Switched Port Analyzer. It 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), which 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 Plixer FlowPro appliance.

3.2.1 Configuration

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

3.2.1.1 Prerequisites

The order of configuration (Plixer FlowPro or the ERSPAN/GRE device first) is not critical, as long as the information listed here is gathered first. The configuration of each device requires information from the other device (Plixer FlowPro and ERSPAN device).

This information should be determined prior to starting the configuration:

Plixer FlowPro ERSPAN configuration

- Monitor port: for example ‘mon1’.
- Monitor port IP and CIDR: for example ‘10.30.15.50/16’ (do NOT use /32 CIDR)
- Monitor port gateway: for example ‘10.30.1.1’
- Peer IP Address: the ERSPAN source IP defined below - for example ‘10.30.1.203’

ERSPAN device configuration

- ERSPAN Source IP - an IP address on the device (switch or router) or the ESXi host IP address (VDS): for example ‘10.30.1.203’
- Destination IP - Plixer FlowPro monitor port IP address (not the Plixer FlowPro management IP): for example ‘10.30.15.50’
- Source Interface(s) to SPAN - the example in step 6 of VMWare VDS configuration below shows 3 sources selected

Note: Plixer FlowPro provides support for GRE type 2.

The following pages detail how to configure *Plixer FlowPro*, a *Cisco switch*, and a *VMware VDS*.

Note: Specific commands and configuration options may vary between devices and versions. Command syntax should be verified with vendor documentation for the specific device being configured.

3.2.2 Plixer 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 Plixer FlowPro for ERSPAN.

Note: Each monitoring interface on the Plixer FlowPro supports only one ERSPAN configuration. Multiple ERSPAN configurations on the same interface, for example mon1, may produce unpredictable results.

3.2.3 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 Plixer FlowPro monitor␣
↪interface
source interface port-channel1 both       # Port(s) to be sniffed
no shut                                   # enable
```

(continues on next page)

(continued from previous page)

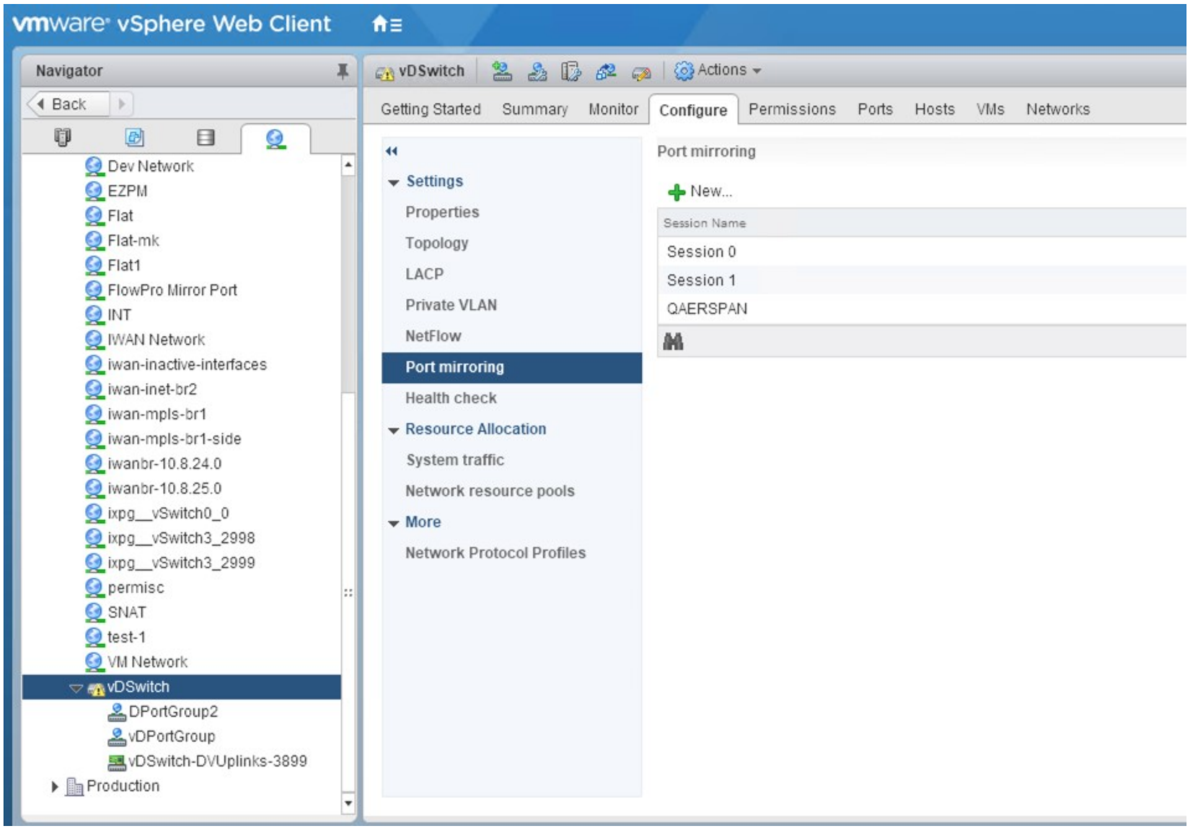
```
monitor erspan origin ip-address 10.1.2.1 global
```

3.2.4 VMware VDS

Note: This requires the VMware Enterprise Plus license and a configured vSphere Distributed Switch.

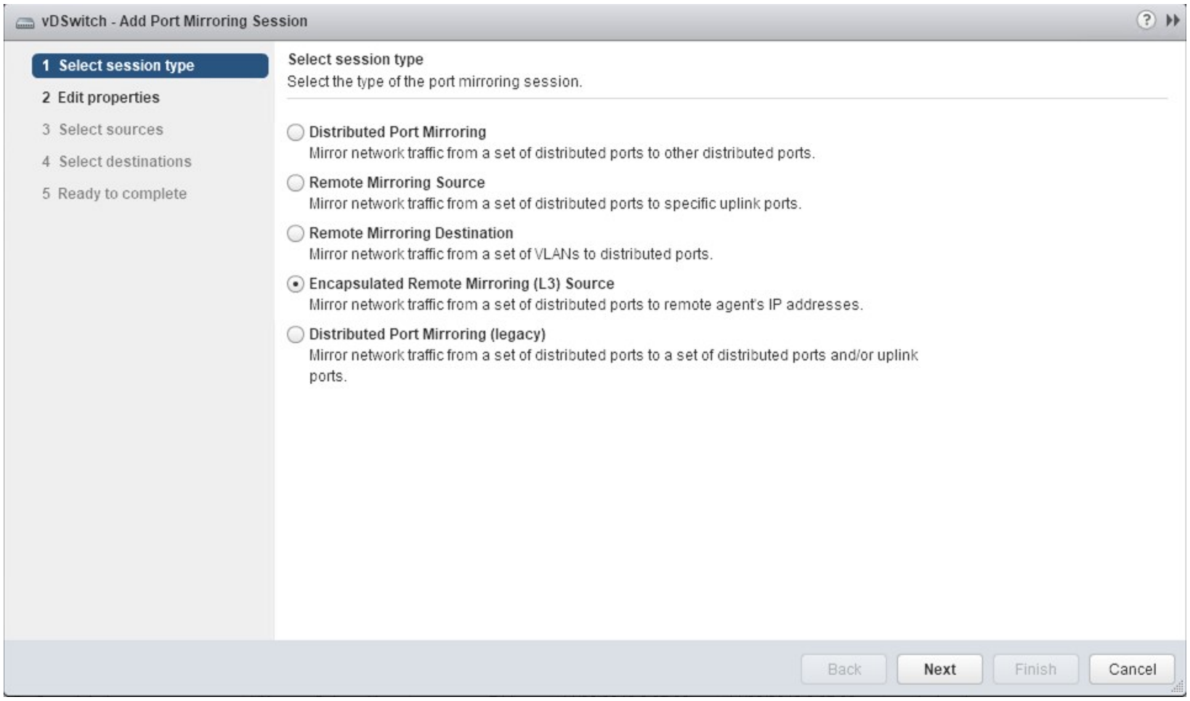
From the VMware web console:

1. Select the VDS from the list of networks.
2. Select *Port mirroring* on the **Configure** tab.
3. Select *New. . .* to create a new session.



Session Name
Session 0
Session 1
QAERSPAN

4. Select *Encapsulated Remote Mirroring (L3) Source*, and then click **Next**.



Select session type

Select the type of the port mirroring session.

○ Distributed Port Mirroring
Mirror network traffic from a set of distributed ports to other distributed ports.

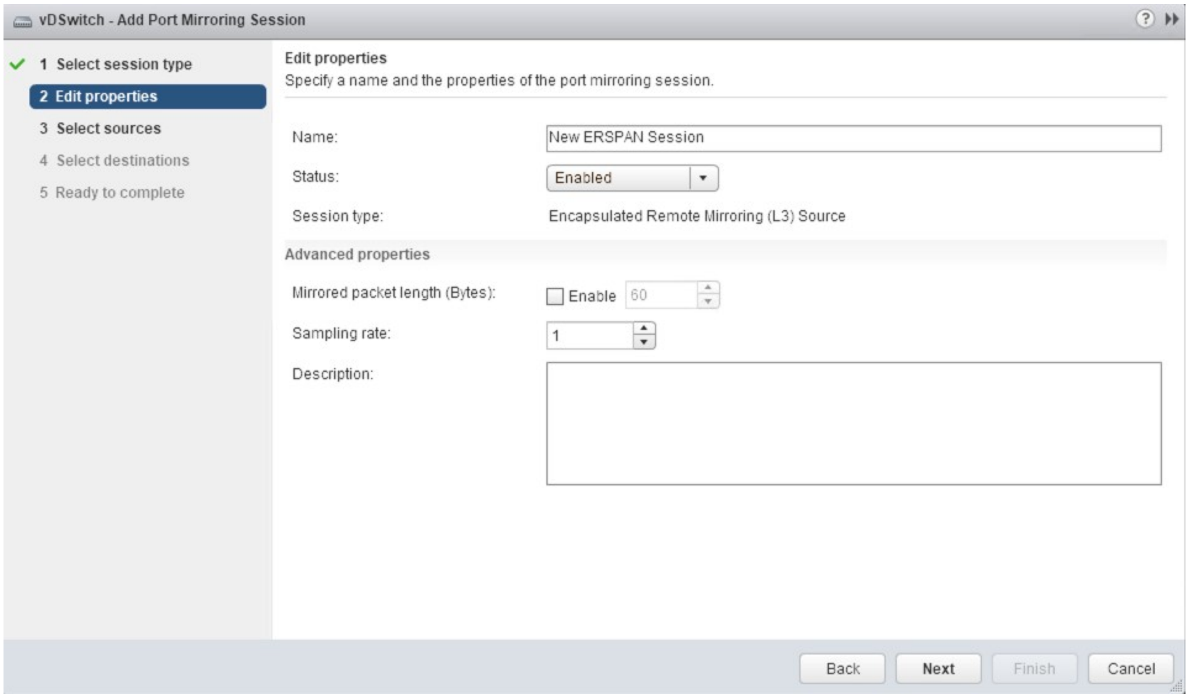
○ Remote Mirroring Source
Mirror network traffic from a set of distributed ports to specific uplink ports.

○ Remote Mirroring Destination
Mirror network traffic from a set of VLANs to distributed ports.

● Encapsulated Remote Mirroring (L3) Source
Mirror network traffic from a set of distributed ports to remote agent's IP addresses.

○ Distributed Port Mirroring (legacy)
Mirror network traffic from a set of distributed ports to a set of distributed ports and/or uplink ports.

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



Edit properties

Specify a name and the properties of the port mirroring session.

Name: New ERSPAN Session

Status: Enabled

Session type: Encapsulated Remote Mirroring (L3) Source

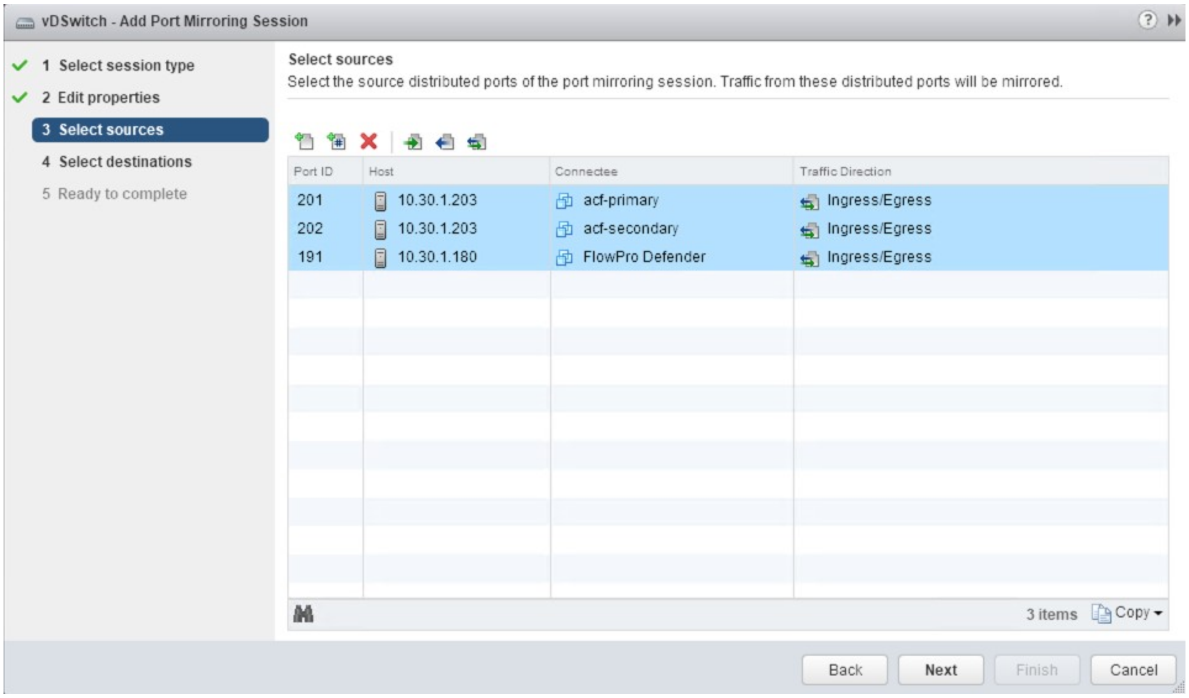
Advanced properties

Mirrored packet length (Bytes): □ Enable 60

Sampling rate: 1

Description:

6. Add the ports intended to mirror to the probe, and then click **Next**.



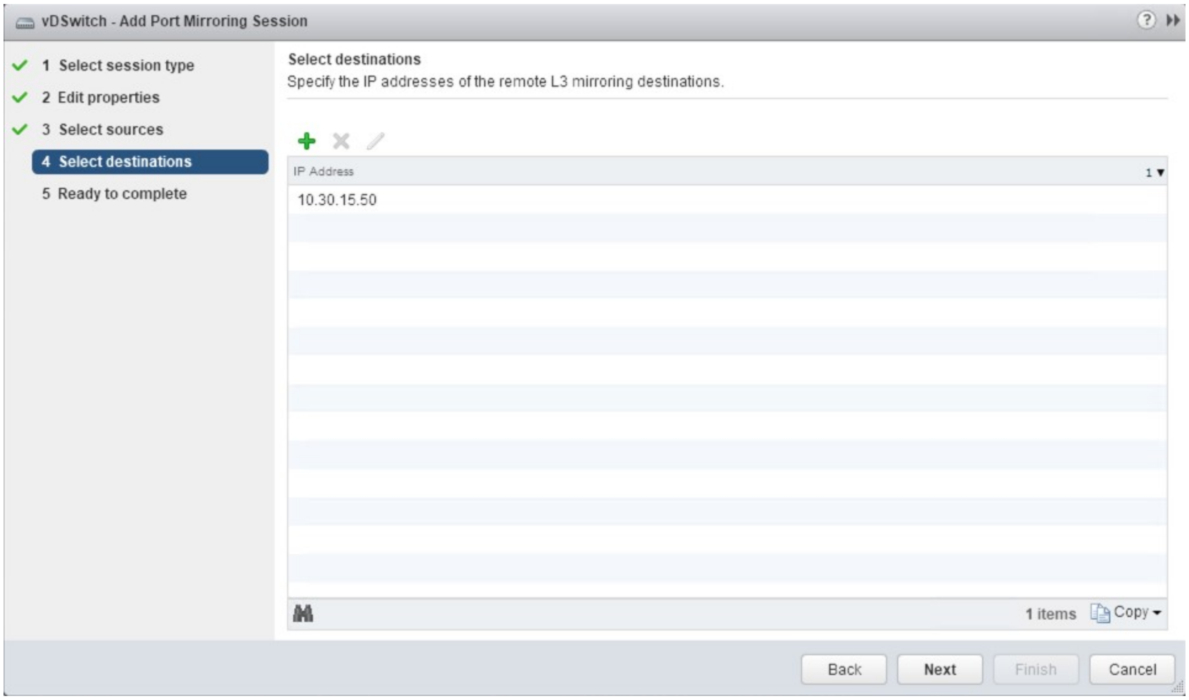
vDSwitch - Add Port Mirroring Session

Select sources

Select the source distributed ports of the port mirroring session. Traffic from these distributed ports will be mirrored.

Port ID	Host	Connectee	Traffic Direction
201	10.30.1.203	acf-primary	Ingress/Egress
202	10.30.1.203	acf-secondary	Ingress/Egress
191	10.30.1.180	FlowPro Defender	Ingress/Egress

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



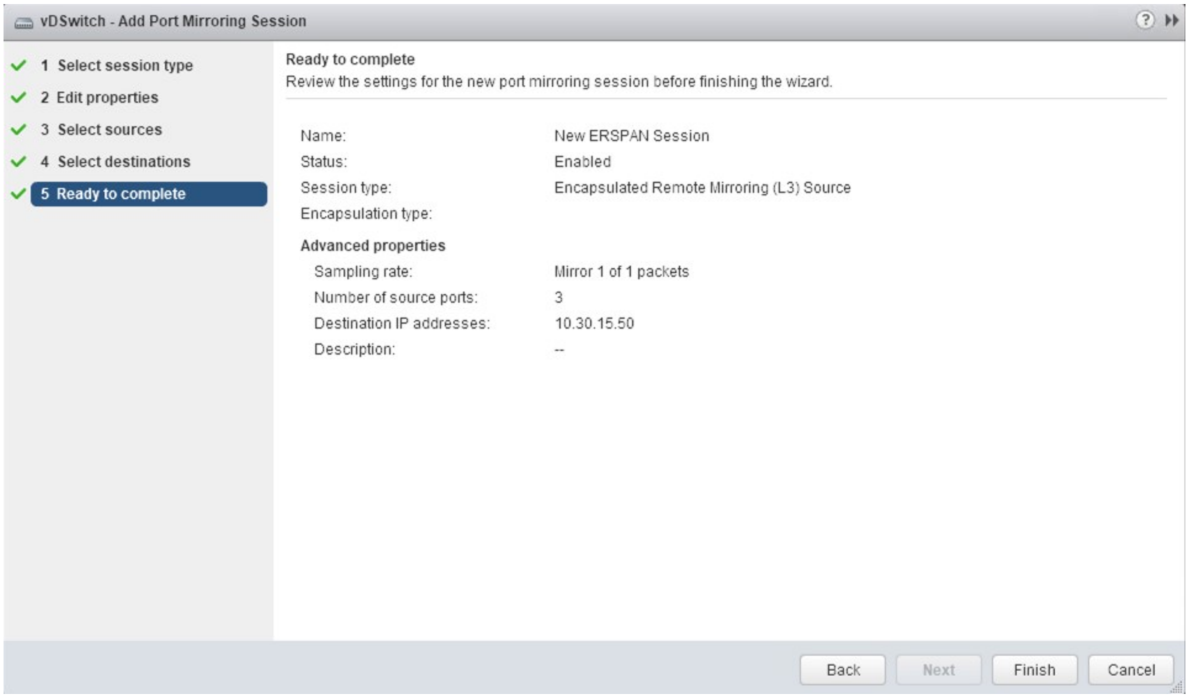
vDSwitch - Add Port Mirroring Session

Select destinations

Specify the IP addresses of the remote L3 mirroring destinations.

IP Address
10.30.15.50

8. Verify the configuration, and then click **Finish** to start the session.



Ready to complete

Review the settings for the new port mirroring session before finishing the wizard.

Name:	New ERSPAN Session
Status:	Enabled
Session type:	Encapsulated Remote Mirroring (L3) Source
Encapsulation type:	
Advanced properties	
Sampling rate:	Mirror 1 of 1 packets
Number of source ports:	3
Destination IP addresses:	10.30.15.50
Description:	--

CHAPTER

FOUR

ADVANCED SERVICES

4.1 Commands

The Plixer FlowPro command set provides numerous configuration and maintenance utilities required for device management and technical support purposes and are available in the Plixer FlowPro user interface.

4.1.1 Logging in to User Interface

Connect to Plixer FlowPro over SSH and log in as the `flowpro` user with the password configured during the installation process.

The *FLOWPRO>* prompt indicates that Plixer FlowPro is ready to accept commands. If the initial configuration steps have been completed correctly, Plixer FlowPro is already processing traffic and sending data to the designated IPFIX collector.

4.1.2 Command List

The following are the top level commands:

- *check*
- *clear*
- *disable*
- *edit*
- *enable*
- *service*
- *set*
- *show*
- *system*

Note: Each top level command may have several extended commands or sub-commands.

4.1.3 check

Note: This feature requires the *Plixer FlowPro Defender license*.

Function	Verifies different settings and configurations on the Plixer FlowPro appliance.
Syntax	• *check replist* - Checks the ability for the Plixer FlowPro to reach **nba.plixer.com** to download the reputation lists. If this appliance does not have access to the internet, contact *Plixer Technical Support* for help.

4.1.4 clear

Warning: These commands will alter Plixer FlowPro's functions and should be used with caution.

Note: This feature requires the *Plixer FlowPro Defender license*.

Function	Cleans up or removes data from a system.
Syntax	• *clear domainlist <domain_list>* - Removes a domain list from the system. Use with caution. Use the *show domainlist* command to list all active domain lists.

4.1.5 disable

Function	Disables settings.
Syntax	• *disable apm <interface> <apmMode>* - Disables either monitoring of Latency, VOIP or both on an interface. The specified interface must be active. The valid <apmMode> options are: `voip`, `latency`, or `both`. This feature requires the *Plixer FlowPro APM license*. To display a list of currently enabled interfaces, use the *show configuration* command. • *disable defender* <interface> - Disables DNS monitoring on an interface. The specified interface must be active. This feature requires the *Plixer FlowPro Defender license*. To display a list of currently enabled interfaces, use the *show configuration* command. • *disable domainlist <domain_list>* - Disables a custom domain reputation list. The disabled domain list will not be removed and can be re-enabled using the *enable domainlist* command. This feature requires the *Plixer FlowPro Defender license*. • *disable domainReputationList* - Disables checking against the domain reputation lists configured on the system. This feature requires the *Plixer FlowPro Defender license*. To display the available domain lists, use the *show domainlist* command. • *disable erspan <interface>* - Disables traffic monitoring on an interface. To display a list of currently enabled interfaces, use the *show configuration* command. • *disable http_mon* - Disables the HTTP monitoring. This feature requires the *Plixer FlowPro Defender license*. • *disable trackProcessMetrics* - Disables Plixer FlowPro process metrics.

4.1.6 edit

Function	Edits the Plixer FlowPro configuration files.
Syntax	• *edit domainlist <domain_list>* - Edits a custom domain reputation list. The name specified in *<domain_list>* will create a new list with 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 or three layer domain (2LD/3LD). Domain names that do not contain 2 or 3 layers are ignored. This feature requires the *Plixer FlowPro Defender license*. • *edit license* - Opens the **plixer.ini** file where the license key is stored. The plixer.ini file also stores the Plixer FlowPro configuration information. After editing the **plixer.ini** file, Plixer FlowPro will restart services to load the changes made. • *edit plixer.ini* - Opens the **plixer.ini** file for edit. The **plixer.ini** file stores the Plixer FlowPro configuration information. After editing the **plixer.ini** file, Plixer FlowPro will restart services to load the changes made.

4.1.7 enable

Function	Enables monitoring options. All settings can be edited in the configuration file using the *edit plixer.ini* command.
Syntax	• *enable apm <interface> <apmMode>* - Enables the monitoring of Latency, VOIP, or both on an interface. The specified interface must be active. The valid *<apmModes>* options are: `voip`, `latency`, or `both`. This feature requires the *Plixer FlowPro APM license*. To display a list of available monitoring interfaces, use the *show interfaces* command. • *enable defender <interface>* - Enables DNS monitoring on an interface. The specified interface must be active. This feature requires the Plixer FlowPro Defender license. To display a list of available monitoring interfaces, use the *show interfaces* command. • *enable domainlist <domain_list>* - Enables a custom domain reputation list. Custom user-defined reputation lists can be created to supplement the known compromised domain list provided by Plixer. To create a new list, use the *edit domainlist <domain_list_name>* command. • *enable domainReputationList* - Enables Plixer FlowPro to download an updated list of known compromised domains. This list will be periodically downloaded from **nba.plixer.com**. To verify access to the list, use the *check replist* command. • *enable erspan <interface> <ipaddress/cidr> <gateway> <peerIPaddress>* - Configures a monitor interface to receive traffic from an ERSPAN/GRE tunnel. This configuration supports all types of GRE tunnels. The following parameters are required: – <interface> - Monitors the ERSPAN/GRE tunnel traffic. This interface must be one of the monitoring interfaces displayed by the *show interfaces* command. – <interface><ipaddress/cidr> - The IP address dedicated to the ERSPAN/GRE tunnel. This IP must be routable from the monitoring interface to the network device configured to send ERSPAN/GRE. Both the IP address and CIDR are required, which must be unique to this interface. – <interface><gateway> - Used by the monitoring interface to create a route to keep the outgoing traffic from the ERSPAN/GRE tunnel localized to the monitoring interface. – <interface><peerIPaddress> - The external address of the network device configured to send ERSPAN/GRE. If the device is a VMware VDS, enter the IP address of the VMware host. **Note:** For instructions on how to configure the ERSPAN/GRE device, refer to the *ERSPAN configuration* section.

4.1.8 service

Function	Controls the Plixer FlowPro service daemon.
Syntax	• *service flowpro <start|stop|restart>*

4.1.9 set

Function	Changes various settings for the Plixer FlowPro appliance.
Syntax	• *set activeDomainResendSeconds <seconds>* - Sets the number of seconds to resend the active domain list to your collector. The active domain list is the list of domains seen by the Plixer FlowPro Defender HTTP module since the last time the list was sent. Run the enable http_mon command to enable the HTTP monitoring. The <*seconds*> parameter must be set to a whole number between 300 (5 minutes) and 86400 (24 hours). • *set collector <ip> <port>* - Configures the collector IP address and port number for the Plixer FlowPro to send flows to. The collector IP and port are required. The flows will not be collected by the collector if it is not configured to listen on that port number. • *set hostname <hostname>* - Changes the hostname of the Plixer FlowPro appliance. The <*hostname*> parameter is required. A reboot is required for this change to take effect. • *set license* - Opens the **plixer.ini** file where the license key is stored. The **plixer.ini** file also stores the Plixer FlowPro configuration information. After editing the **plixer.ini** file, Plixer FlowPro will restart services to load the changes made. **Note:** The *set license* command is an alias of the *edit license* command as defined in the interactive command help. • *set password* - Changes the password for the *flowpro* operating system user.

4.1.10 show

Function	Displays Plixer FlowPro information or settings.
Syntax	• *show configuration* - Shows the current Plixer FlowPro configuration settings. • *show domainlist* - Shows all the custom domain lists configured on the system. To edit the custom domain list, use the *edit domainlist* command. • *show erspan* - Shows current ERSPAN configuration information. Only one ERSPAN tunnel can be configured per interface. • *show features* - Shows licensed Plixer FlowPro features. • *show interfaces* - Shows available interfaces that can be configured to monitor mirrored traffic. • *show license* - Shows the current license information. • *show machine_id* - Shows the machine id of the Plixer FlowPro appliance. • *show status* - Shows the status of Plixer FlowPro processes.

4.1.11 system

Function	Changes state of the Plixer FlowPro operating system.
Syntax	• *system restart* - Restarts the operating system. • *system shutdown* - Shuts down the operating system.

4.2 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). However, Plixer 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 and egress is mon2. This is done by modifying the `plixer.ini` file.

Note: If you are using the basic Plixer FlowPro license, the observation domain is fixed at 42 by default.

To do this, follow these steps:

1. Open the editor from the FLOWPRO> prompt: `FLOWPRO> edit plixer.ini`.
2. In the editor, locate the line: `monitorTraffic=mon1`. When specified in this format, mon1 is configured for ingress of 1 and egress of 1.

3. To allow Plixer FlowPro to configure mon1 to have an ingress of 1 and egress of 2, modify the setting in the following format: `monitorTraffic=mon1:1:2`. The format to use is `monX:ingress:egress`.
4. Save the `plixer.ini file`. Plixer 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.

The observation domain ID identifies the source of the IPFIX flows to the collector, which in this case is the Plixer FlowPro appliance. In most cases, there is no need to change the default value.

To define a different observation domain for an interface, follow these steps:

1. Modify the `plixer.ini` file as before using the format monX:ingress:egress:observation_domain. The ingress and egress labels must also be set when setting the observation domain.
2. To change the observation domain for mon1 from the default to 45, while keeping the ingress and egress values set above, modify the configuration setting specified above to read as: `monitorTraffic=mon1:1:2:45`.
3. To use the default ingress/egress values for mon1 but change the observation domain to 45: `monitorTraffic=mon1:1:1:45`.

4.3 Server Maintenance

4.3.1 Hardware Failure

Contact *Plixer Technical Support* for assistance if any hardware malfunctions occur.

4.3.2 Applying Security Patches

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

Updates should not be installed unless Plixer Technical Support advises or assists. For more information, contact *Plixer Technical Support*.

4.3.3 Backing Up Plixer FlowPro

Plixer FlowPro stores all of its configuration data in the plixer.ini file.

To backup the Plixer FlowPro configuration data, make a copy of the `/home/flowpro/conf/plixer.ini` file.

4.3.4 Restoring Plixer FlowPro from Backup

To restore the Plixer FlowPro configuration data backup, follow these steps:

1. Copy the backed up `plixer.ini` file to `/home/flowpro/conf/plixer.ini`.
2. To rebuild the appropriate files and begin operations, issue the following command: `$ manage -verbose -flowproSH`.

If a new host server is being deployed, or the server hardware configuration has changed, a new license key will need to be applied.

CHAPTER

FIVE

ADDITIONAL RESOURCES

5.1 Change Log

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

KEY: ACTION: (Bug Ticket Number) description

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

5.1.1 Change Log History

5.1.1.1 Version 19.1.2 - (10/2023)

FIXED: Addressed various security issues
FIXED: (229): APM nprobe services not starting

5.1.1.2 Version 19.1.1 - (09/2023)

FIXED: Addressed various security issues
FIXED: (206): Malformed DNS crashes FlowPro Defender

5.1.1.3 Version 19.1.0 - (10/2022)

FIXED: (56): Hardware 10Gb FlowPro APM Understating
FIXED: (97): FlowPros Deploying with only 1 network
FIXED: (114): yum update breaks flowpro APM
FIXED: (117): Separate Observation domains per monitor interface by default to fix high MFSN's

---

5.1.1.4 Version 19.0.0 - 10/2020

ADDED: (55) Custom JA3 Blacklist Support
ADDED: (63) JA3 Fingerprinting Support

FIXED: (43) Make FlowPro licensed features clearly understandable
FIXED: (56) Hardware 10Gb FlowPro APM understating
FIXED: (61) /home/flowpro/conf/vmwareToolsInstall.sh is missing
FIXED: (64) Add the FlowPro version to FlowPro prompt

5.1.1.5 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

5.1.1.6 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

---

5.1.1.7 Version 16.8 - 8/16/2016

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

---

5.2 Plixer Technical Support

Plixer Technical support is available with an active maintenance contract. Contact our support team at:

- +1 (207) 324-8805 ext 4
- https://www.plixer.com/support/

5.3 Glossary

5.3.1 Plixer FlowPro Terms

BotNet
A network of private computers infected with malicious software and controlled as a group without the owners' knowledge

Command and Control
Command and Control cyberattacks (C2 or C&C) happen when bad actors infiltrate a system and install malware that lets them remotely send commands from a C2 server to infected devices

Data exfiltration
Unauthorized data transfer, either manually from a device or over a network

DGA (Domain Generation Algorithms)
Algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used as rendezvous points with the command and control servers

DNS Data Leak
DNS server requests that are visible to third parties

Domain Reputation List
List of domains that have been determined, with a high probability, to be "bad domains"

DPI (Deep Packet Inspection)
An advanced method of examining and managing network traffic, functioning at the application layer of the OSI model

JA3 Signature
A method to fingerprint an SSL/TLS client connection based on fields in the Client Hello message from the SSL/TLS handshake. So named as it was first published by John Althouse, Jeff Atkinson, and Josh Atkins from Salesforce in 2017.

NXDOMAIN (No Existing Domain)
Error message indicating that the domain is either not registered or invalid

Observation Domain
A value used by the collector device to group devices when receiving data sessions

plixer.ini
Plixer FlowPro configuration file.

Trusted Domain list
List of domains that are allowed on the network (whitelisted)

5.3.2 General Networking Terms

2LD (Second-level Domain)
Part of the naming convention domain names. For example, in example.com, *example* is the second-level domain of the .com TLD (Top level domain)

3LD (Third-level Domain)
For example, in www.mydomain.com, *www* is the third-level domain

API (Application Programming Interface)
A software component that allows applications to share data and functionality

CA (Certification Authority)
A trusted entity that issues, signs, and stores digital certificates

CIDR (Classless Inter-Domain Routing)
An Internet Protocol addressing method that improves the efficiency of allocating IP addresses. The general way of representing the CIDR IP address is `a.b.c.d/n` with `n` representing the number of bits used for the identification of the network.

CLI (Command-line Interface)
A text-based interface for applications and operating systems that allows a user to enter commands and receive

Collector
SIEMs, Flow Collectors, SNMPTrap Receivers, or other network management systems that analyze data forwarded by the Plixer Replicator from other networked devices

DNS (Domain Name System)
The system by which computers and other devices on the Internet or Internet Protocol networks are uniquely identified using names matched to their IP addresses

Egress
Traffic that exits a device or network

ERSPAN (Encapsulated Remote Switched Port Analyzer)
A Cisco proprietary feature that brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains

Exporter
A networked device such as a router, switch, or server that generates data and sends it to the Plixer Replicator for replication and forwarding

Fault tolerance
A system's ability to continue operating without interruptions in the event of a hardware or software failure

FQDN (Fully Qualified Domain Name)
The comple domain name of a specific computer, host, or online presence. For example, Plixer's website's FQDN would be *www.plixer.com*

GRE (Generic Routing Encapsulation)
A tunneling protocol developed by Cisco Systems

IP address
A unique numerical label assigned to a networked device

IPFIX (Internet Protocol Flow Information Export)
A protocol that standardizes Internet Protocol flow information from networked devices

Latency
The latency of a network is the time it takes for a data packet to be transferred from its source to the destination

LDAP (Lightweight Directory Access Protocol)
An open, cross platform protocol used to authenticate and store information about users, groups, and applications

MAC (Media Access Control) address
A unique hardware identifier typically assigned by manufacturers to network adapters and devices

NIC (Network Interface Card)
Adapter that provides devices network connections, either wired or wireless

OVF (Open Virtualization Format)
An open-source standard for packaging and distributing virtual machines and software applications

Packet
A block of data transmitted across a network

Redundancy
Duplicated or alternative network devices and connections meant to serve as a failsafes against the primary service becoming unavailable

Router
A device that forwards or routes data packets to devices on a network

Server
A system or device that provides resources, data, services, or applications to other devices over a network

SIP/RTP (Session Initiation Protocol/Real Time Protocol)
SIP is the control protocol, and RTP is the payload protocol used to send and receive Voice over IP (VoIP)

SSH (Secure Shell Protocol)
A network communication protocol that allows network services to be used securely over an unsecured network

SSL (Secure Sockets Layer)
A protocol for establishing secure connections between networked devices

Switch
A device that connects devices in a network and allows them to communicate with each other

Syslog
A standard for message logging that allows a wide variety of networked devices to share the same repositories and management systems

TLS handshake (Transport Layer Security)
TLS is a network protocol used to ensure secure and private communications over the internet. A TLS handshake is the process that kicks off a communication session that uses TLS encryption

UDP (User Datagram Protocol)
A communication protocol used by applications to send messages to other hosts on an Internet Protocol network via low-latency, loss-tolerating connections

Virtual appliance
A pre-configured virtual machine image with pre-installed software meant to serve a specific function

VoIP (Voice over Internet Protocol)
A technology that allows voice calls using an internet connection

5.4 Third-party licenses

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

5.4.1 libcap

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

5.4.2 libfixbuf

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

5.4.3 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

5.4.4 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

5.4.5 Pof

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

5.4.6 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

5.4.7 tcpdump

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

5.4.8 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