FlowPro Documentation

Release 19.1.2

Plixer

Apr 22, 2024

VERSION 20.0.0

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

- Selective packet capture
- Threat Feed based event detection
- Custom NIDS rule event detection
- DNS lookups of domains likely associated with malware
- DNS Start of Authority
- Transfered file info and hashes
- HTTP connection reporting
- TLS and JA3 signature reporting

- Data exfiltration detection
- BotNet & Command and control detection
- Plus many more with NIDS rules traffic inspection

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.

Note: The Plixer FlowPro APM and Plixer FlowPro APM-Defender licenses are currently only available in version 19, but will be available in a future version 20.x release.

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 Plixer FlowPro Licensing

To obtain a Plixer FlowPro license, contact and provide *Plixer Technical Support* with the Customer ID and Machine ID found in **Admin > Plixer > FlowPro Licensing**.

Note: Before deploying the appliance, you must apply the license and define Plixer FlowPro in Plixer Scrutinizer first.

Plixer FlowPro license management is done via the admin interface in Plixer Scrutinizer.

1. In the Plixer Scrutinizer web interface, navigate to **Admin > Plixer > FlowPro Licensing**.
2. Enter the license details provided for your Plixer FlowPro.
3. After providing your license details, navigate to **Admin > Resources > Manage FlowPros**.
4. Click the **+** icon to add a Plixer FlowPro probe. Assign a unique name and enter the Plixer FlowPro MGMT interface IP address.

   Note: This IP address must be used in the inital MGMT setup of the appliance on first boot.

5. Enable the **Default NIDS Rules** to allow the use of open-source threat feed NIDS rules for network event reporting.
6. Click **Save**, and then proceed to setting up the appliance.

2.2 System Requirements

CPU and RAM requirements scale with the expected traffic aggregate volume.

Disk requirements scale with selective packet capture workloads. This value can be approximated using: `$ ~/flowpro/flowpro-settings.yaml`

- The `$pcap.server_capture_depth` value determines how many payload observations will be maintined per capture
- The `$pcap.server_ttl_hours` value determines how long captures are stored after the last observation
- The maximum MTU of monitored interfaces

Required Storage Bytes = Capture Depth * MTU * Expected Source Host - Well Known Port - Destination Host combinations stored during TTL time duration

The VM Deploys by default with:

Default VM Configuration	
CPU	8 cores
RAM	8 GB
Disk	100GB

2.2.1 Resource Scaling Recommendations

MEDIUM TRAFFIC (Up to 1 GBIT PER SECOND)	
CPU	6-10 cores
RAM	10-18GB
Disk	100GB+

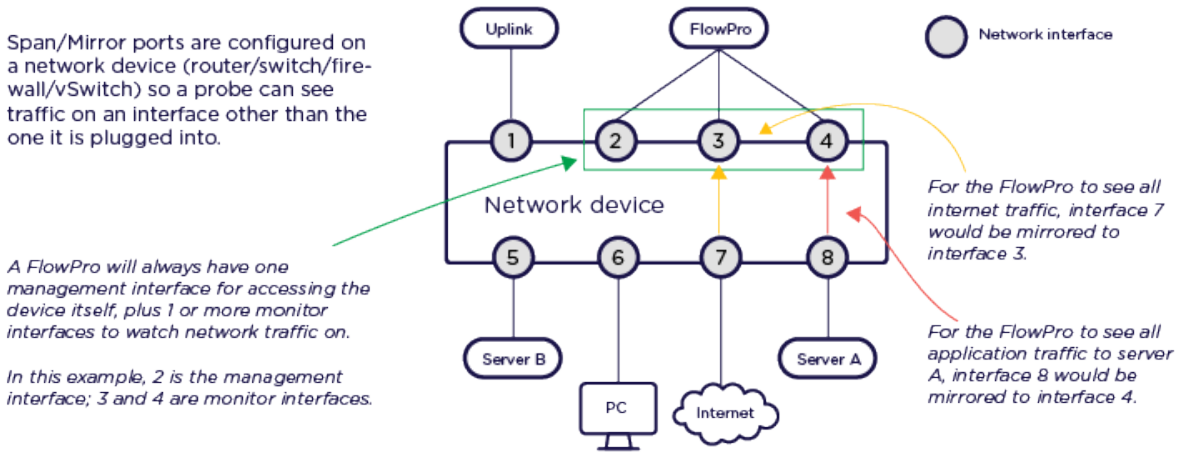
HIGH TRAFFIC (1 - 10 GBITS PER SECOND)	
Recommendation	Hardware Solution Recommended
CPU	10-18 cores
RAM	18-34GB
Disk	100GB+

Note: Scale the disk to meet the specific requirements for selective PCAP usage.

2.3 Span Configuration

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

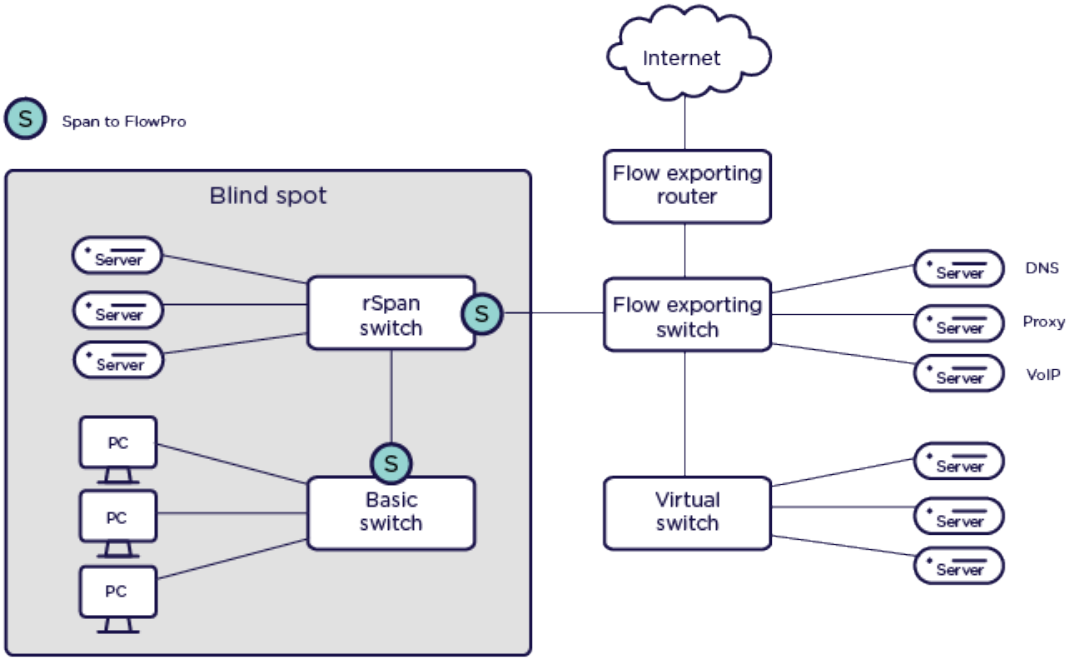
2.3.1 Span ports



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).

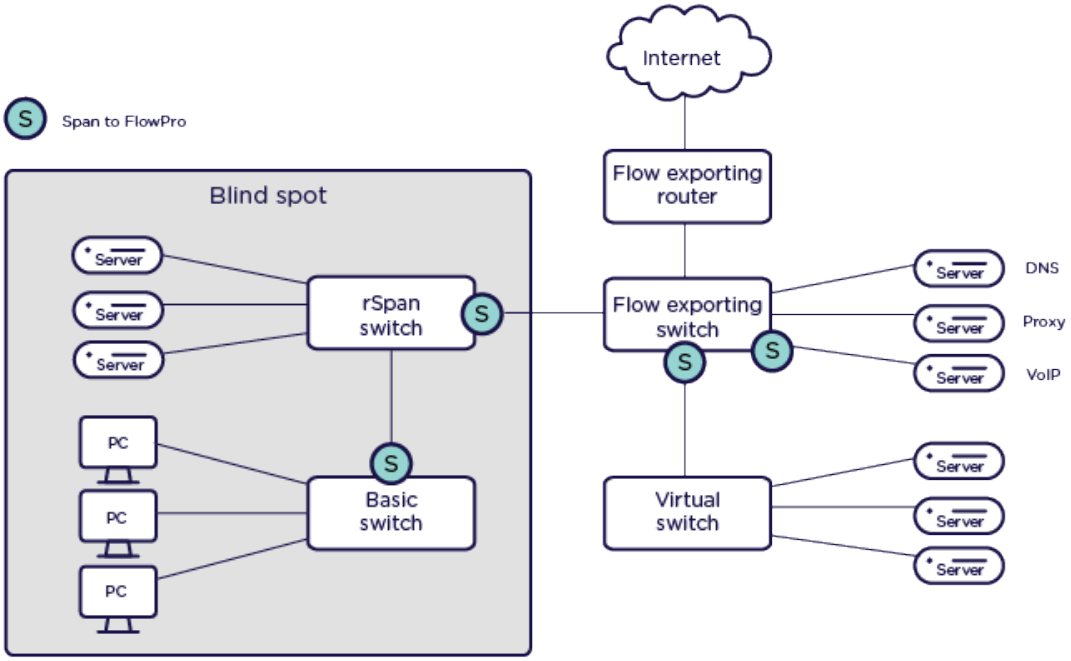
2.3.2 Plixer FlowPro

Visibility where you need it.



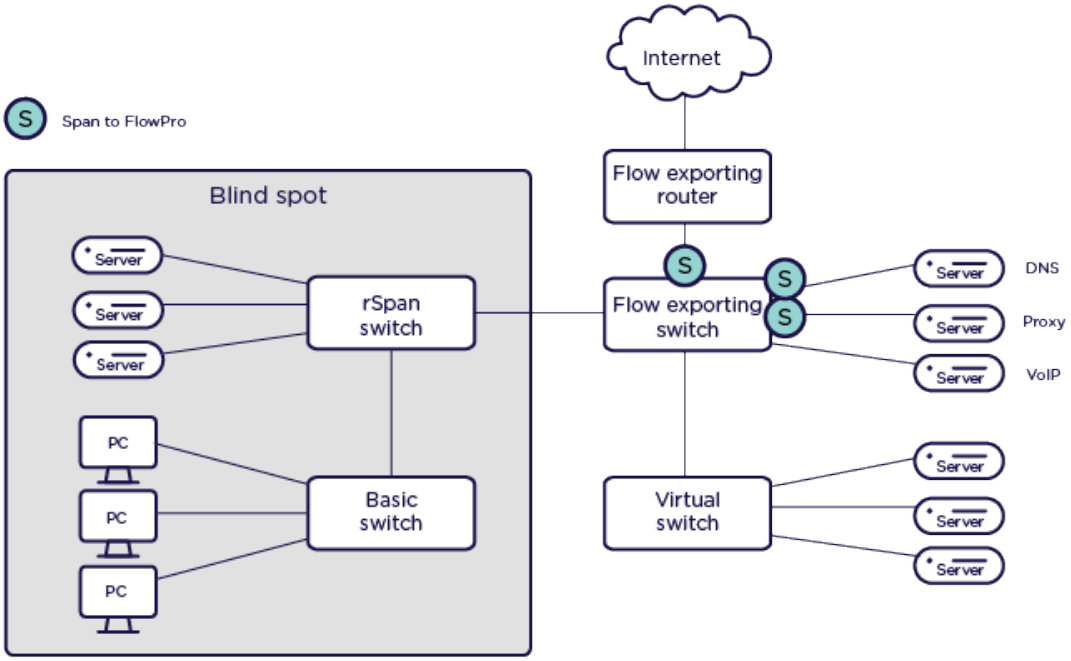
2.3.3 Plixer FlowPro APM

Application Performance Monitoring



2.3.4 Plixer FlowPro Defender

Security through watching DNS and HTTP traffic



2.4 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:

2.4.1 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:

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

2.4.1.1 Deploying the OVA 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 OVA Template**.
3. Select **Deploy from File**, navigate to the OVA Template, and click **Next**.
4. Review the OVA 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 OVA Template.
7. *Add additional network adapters* via vCenter by editing the settings of the VM. Use **Add New Device** to install a *Network Adapter*, and then connect these to the desired observation point.

Note: The virtual appliance is configured with 1 network adapter (mgmt), additional interfaces will be labeled monX during setup. By default, it will start listening for traffic on all attached monX interfaces. This can be verified in `Flowpro.Interfaces` in `~/flowpro/flowpro-settings.yaml` after setup. 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.

---

8. Power on the Plixer FlowPro virtual machine.

Once the Plixer FlowPro appliance is powered on, navigate to the *Setup Utility* page to continue with the initial deployment.

2.4.2 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:

2.4.2.1 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.
6. *Add additional network adapters* to monitor interfaces.
7. Start the virtual machine, right-click on it, and select **Connect**.

Once the Plixer FlowPro appliance is powered on, navigate to the *Setup Utility* page to continue with the initial deployment.

2.4.3 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:

2.4.3.1 System Requirements

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

2.4.3.2 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.

2.5 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>

2.6 Adding Additional Interfaces

2.6.1 Add a new interface in VMware

1. In vCenter, right click on the VM that the new interface will be added to, and then select **Edit Settings…**.
2. From the **Edit Settings…** window, select **Add New Device**.
3. From the dropdown menu, click **Network Adapter**.
4. Connect to SPAN Network or standard network which can receive GRE traffic from network infrastructure for ERSPAN.
5. Run the *setup utility* to begin monitoring.
   - On a new deployment that has not been configured: `$ sudo ~/flowpro/setup.sh`.
   - To add interface to existing configuration: `$ sudo ~/flowpro/setup.sh --monitor-ports`.
   - For use as ERSPAN destination: `$ sudo ~/flowpro/setup.sh --erspan-config`.

2.6.2 Add a new interface in Hyper-V

1. Power off the Plixer FlowPro VM.
2. In Hyper-V Manager, right click on the VM that the new interface will be added to, and then select **Settings…**.
3. From the **Settings…** window, select **Add Hardware**.
4. From the dropdown menu, click **Network Adapter**.
5. Connect to SPAN Network or standard network which can receive GRE traffic from network infrastructure for ERSPAN.
6. Power on the Plixer FlowPro VM.
7. Run the *setup utility* to begin monitoring.
   - On a new deployment that has not been configured: `$ sudo ~/flowpro/setup.sh`.
   - To add interface to existing configuration: `$ sudo ~/flowpro/setup.sh --monitor-ports`.
   - For use as ERSPAN destination: `$ sudo ~/flowpro/setup.sh --erspan-config`.

2.7 Setup Utility

The Setup Utility found in `~/flowpro/setup.sh` is responsible for interface management and Plixer FlowPro configuration.

1. From the Hyper-Visor, launch the virtual console, and then log in to the Plixer FlowPro as the `root` user and password `plixer`.
2. Accept the **FlowPro End User Agreement**, and then proceed with the initial setup.
3. When prompted, enter the values for the following:
    - Flowpro Hostname (this must be a fully qualified hostname)
    - IP Address
    - CIDR (provide the CIDR mask only (i.e. 8,16,24,etc.))
    - Gateway
    - DNS IP
    - `root` user's new password
    - `plixer` user's new password

    Note: The system will reboot after all the information is provided.

4. After the system reboots, you can now SSH to the newly configured IP address using the `plixer` user and password that you set in the previous step.
5. Run the following command to setup Plixer FlowPro: `$ sudo /home/plixer/flowpro/setup.sh`.
6. When prompted, enter the values for the following:
    - `plixer` user's current password
    - Primary Plixer Scrutinizer reporter address
    - Plixer Scrutinizer Collector address (This should be the Collector that will receive flows from the Plixer FlowPro appliance. This can be the same as the reporter address.)
    - Plixer Scrutinizer admin auth_token (This is important as part of the initial Plixer FlowPro licensing steps.)
7. When prompted, enter the values for the following to generate a new SSL certificate:
    - Country Name (2-letter country code)
    - State or Province Name (Complete state or province name)
    - Locality Name (Complete locality or city name)
    - Organizational Unit Name (Section)
    - Common Name (Server FQDN or your name)
    - DNS alternative name 1

    Note: Press Enter to stop adding values.

8. When prompted, enter if your Plixer FlowPro appliance has internet access.
    - If yes, proceed with the next steps that follow. This may require a docker account.

- If no, the setup will be done locally.

9. When prompted, confirm if you will be configuring an ERSPAN.
10. If setting up ERSPAN, enter the following details when prompted:
    - IP address to assign to a monX interface
    - ERSPAN source IP
    - ERSPAN destination IP
    - ERSPAN ID and key

Note: For more information, refer to the *ERSPAN* section.

Flow data and/or events should begin to populate in Plixer Scrutinizer with an exporter address of the local MGMT interface IP.

2.7.1 Setup Utility Runmodes

After inital setup, Plixer Flowpro configuration changes can be made by running the whole setup utility or individual sections.

`$ sudo ~/flowpro/setup.sh` - Full application re-configuration

`$ sudo ~/flowpro/setup.sh --monitor-ports` - Re-configuration of monitor ports, used when adding additonal interface post-deployment

`$ sudo ~/flowpro/setup.sh --exporter-config` - Re-configuration of flow export and destination Scrutinizer

`$ sudo ~/flowpro/setup.sh --cert-generation` - Regeneration of local certificates

`$ sudo ~/flowpro/setup.sh --container-setup` - Update suricata execution container

`$ sudo ~/flowpro/setup.sh --erspan-config` - IP and configure erspan destination post-deployment

`$ sudo ~/flowpro/setup.sh --firewall-mgmt` - Reset Firewall to default posture

2.7.2 Plixer FlowPro service

The operation is orchestrated through the Plixer FlowPro system service and can be controlled using the following command: `service flowpro [start|stop|restart]`.

Note: The setup will generate a certificate signing request `~flowpro/server.csr`. Sign this request and replace the existing `~/flowpro/server.crt` file. Then, restart the Plixer FlowPro service to avoid self-signed operation.

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 Custom Rules

Custom rules that are added to `/home/plixer/flowpro/rules/custom.rules` are considered by Suricata.

A rule consists of the following:

- **Action**: Determines what happens when the rule matches.
- **Header**: Defines the protocol, IP addresses, ports and direction of the rule.
- **Rule options**: Defines the specifics of the rule.

The command `suricata-update` can be used to manage the running rule set if a custom source is available via HTTPS.

The custom Suricata rules file uses the following format (newline delimited):

Note: General rules are used in the following example for demonstration. In high-performance environments, rules should be as specific as possible.

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 8080 (msg:"This rule alerts on traffic from the␣
↪internal network to the external network over 8080/tcp"; classtype:web-application-
↪activity; sid:2000010;)
alert http 10.1.2.3 any -> any any (msg:"HTTP GET request to example.com detected from␣
↪10.1.2.3"; classtype:trojan-activity; flow:established,to_server; http.method; content:
↪"GET"; http.host; content:"example.com"; nocase; sid:3000001; rev:1;)
alert tcp any any -> any 22 (msg:"SSH protocol version 2 detected"; flow:established,to_
↪server; content:"SSH-2.0"; startswith; sid:3000002; rev:1;)
alert dns any any -> any 53 (msg:"DNS query for malicious-domain.com detected";␣
↪classtype:targeted-activity; dns.query; content:"malicious-domain.com"; nocase;␣
↪sid:3000003; rev:1;)
alert http any any -> any any (msg:"Download of malicious.exe detected";␣
↪classtype:suspicious-filename-detect; flow:established,to_server; http.request_uri;␣
↪content:"/malicious.exe"; endswith; sid:3000004; rev:1;)
alert tls any any -> any any (msg:"TLS 1.0 usage detected"; classtpye:non-standard-
```

(continues on next page)

(continued from previous page)

```
↪protocol; tls.version:"TLS 1.0"; sid:3000005; rev:1;)
#alert tcp any any -> any any (msg:"A commented out rule to temporarily disable";␣
↪classtype:example; sid:3000005; rev:1;)
```

The following are the minimum required fields for Plixer FlowPro events to be sent to Plixer Scrutinizer. The following class types will map to a specific policy in Scrutinizer:

EVENT CODE	DESCRIPTION
attempted-recon	Attempted information leak
successful-recon-limited	Information leak
successful-recon-largescale	Large-scale information leak
attempted-dos	Attempted Denial of Service
successful-dos	Denial of Service
attempted-user	Attempted User Privilege Gain
unsuccessful-user	Unsuccessful User Privilege Gain
successful-user	Successful User Privilege Gain
successful-admin	Successful Administrator Privilege Gain
rpc-portmap-decode	Decode of an RPC Query
shellcode-detect	Executable code was detected
suspicious-filename-detect	A suspicious filename was detected
suspicious-login	An attempted login using a suspicious username
system-call-detect	A system call was detected
trojan-activity	A Network Trojan was detected
unusual-client-port-connection	A client was using an unusual port
network-scan	Detection of a Network Scan
denial-of-service	Detection of a Denial of Service Attack
non-standard-protocol	Detection of a non-standard protocol or event
web-application-activity	Access to a potentially vulnerable web app
web-application-attack	Web application attack
default-login-attempt	Attempt to login by a default username/password
targeted-activity	Targeted malicious activity was detected
exploit-kit	Exploit kit activity detected
external-ip-check	Device retrieving external IP Address detected
domain-c2	Domain observed used for C2 detected
pup-activity	Possibly unwanted program detected
credential-theft	Successful credential theft detected
social-engineering	Possible social engineering attempted
coin-mining	Crypto currency mining activity detected
command-and-control	Malware command and control activity detected

3.1.2 Rule Updates

The command `suricata-update` can be used to manage the running rule set if a custom source is available via HTTPS.

The `suricata-rule-update` file is located at `/home/plixer/flowpro/rules/suricata-rule-update.yaml`.

This file is comprised of the following sections:

- **disable-conf**: A path to a file containing match statments for conditional rule exclusion. See the Example Configuration to Disable Rules for more information.

- **ignore**: A list used to exclude local custom filenames from duplication. This can be absolute path or local if located in `/home/plixer/flowpro/rules`.
- **sources**: The URL pointing to a custom Suricata rule source.

All other `suricata-rule-update` configuration entries are managed by the system.

3.1.3 Selective Packet Capture

Selective packet capture is the targeted capturing of specific network packets based on predefined criteria, such as source/destination IP addresses, port numbers, or protocol types. Rather than capturing all traffic, this method helps conserve storage space and allows for focused analysis on packets relevant to troubleshooting, security monitoring, or network performance analysis.

User capture rules are configured directly in psql in the Plixer Scrutinizer reporter.

Important: Use minimal matching criteria for rules in a high-volume environment.

```
-- Example 1
INSERT INTO flowpro.nids_rules
(source_ip, destination_ip, protocol, source_port, destination_port, sid, msg)
VALUES
('1.1.1.1', '192.168.1.10', 'UDP', '53', 'any', '2000001', 'Dns Response from 1.1.1.1');

-- Example 2
INSERT INTO flowpro.nids_rules
(source_ip, destination_ip, protocol, source_port, destination_port, sid, msg)
VALUES
('192.168.1.10', '1.1.1.1', 'UDP', 'any', '53', '2000002', ' DNS query detected');

-- Example 3
INSERT INTO flowpro.nids_rules
(source_ip, destination_ip, protocol, source_port, destination_port, sid, msg)
VALUES
('1.1.1.1', '192.168.1.10', 'TCP', '2022', '2022', '2000003', 'Potential encrypted␣
↪tunneling detected');

-- Example 4
INSERT INTO flowpro.nids_rules
(source_ip, destination_ip, protocol, source_port, destination_port, sid)
VALUES
('1.1.1.1', '192.168.1.10', 'ICMP', 'NA', 'NA', '2000004');

-- Note: For protocols like ICMP, the concept of "ports" does not apply. Thus, 'NA'␣
↪should be used.
```

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

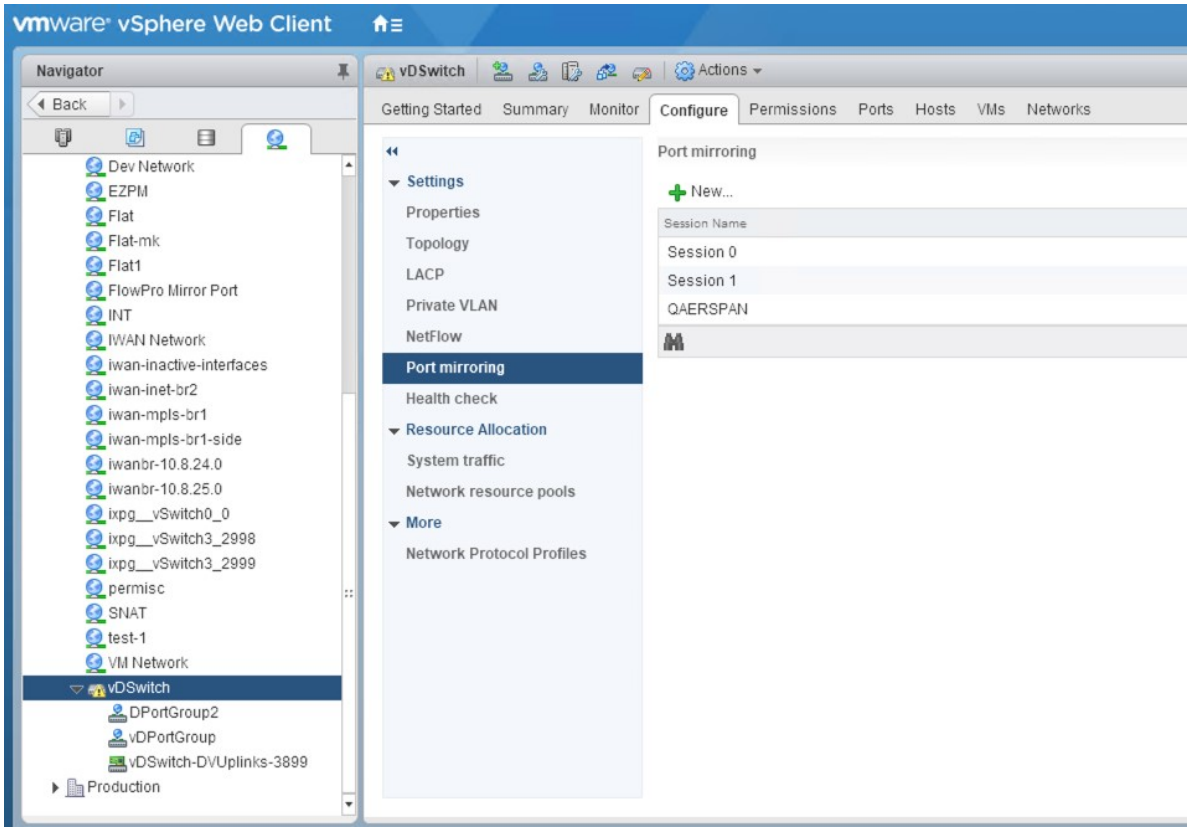
```
monitor session 1 type erspan-source
description ERSPAN direct to FlowPro
erspan-id 32                                # required
vrf default                                 # required
destination ip 10.1.2.3                     # IP address of Plixer FlowPro monitor␣
↪interface
source interface port-channel1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

monitor erspan origin ip-address 10.1.2.1 global
```

3.2.4 VMware VDS

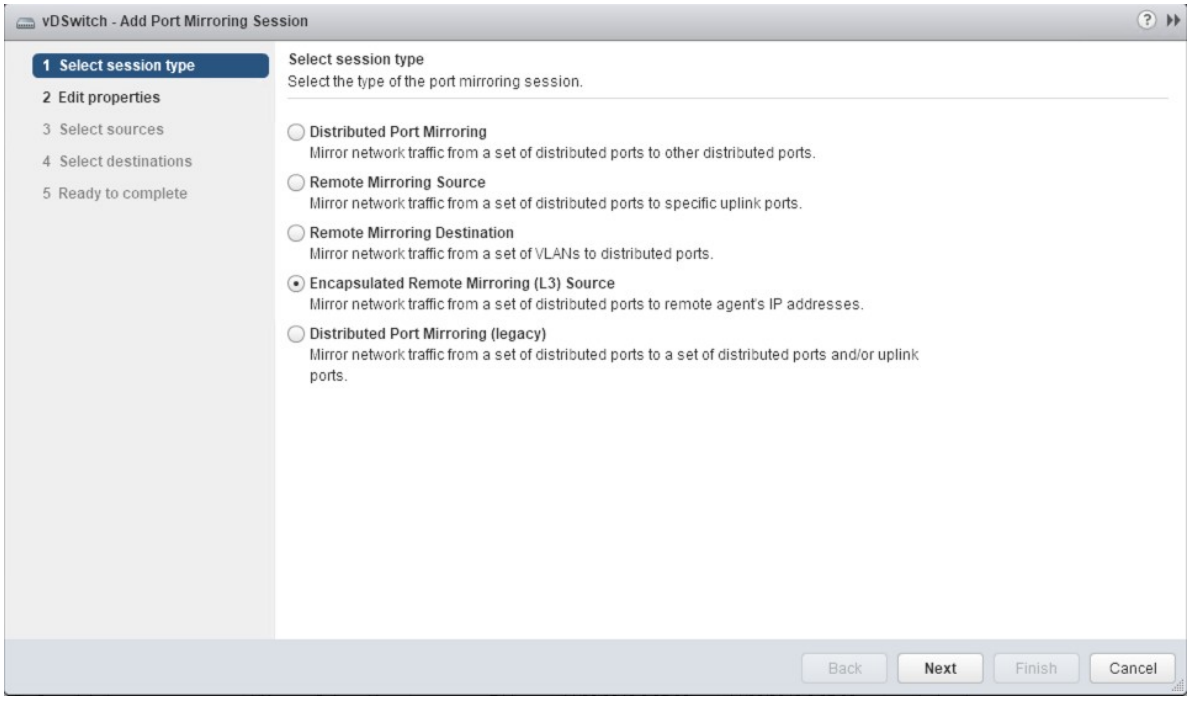
Note: This requires the VMware Enterprise Plus license and a configured vSphere Distributed Switch.

From the VMware web console:

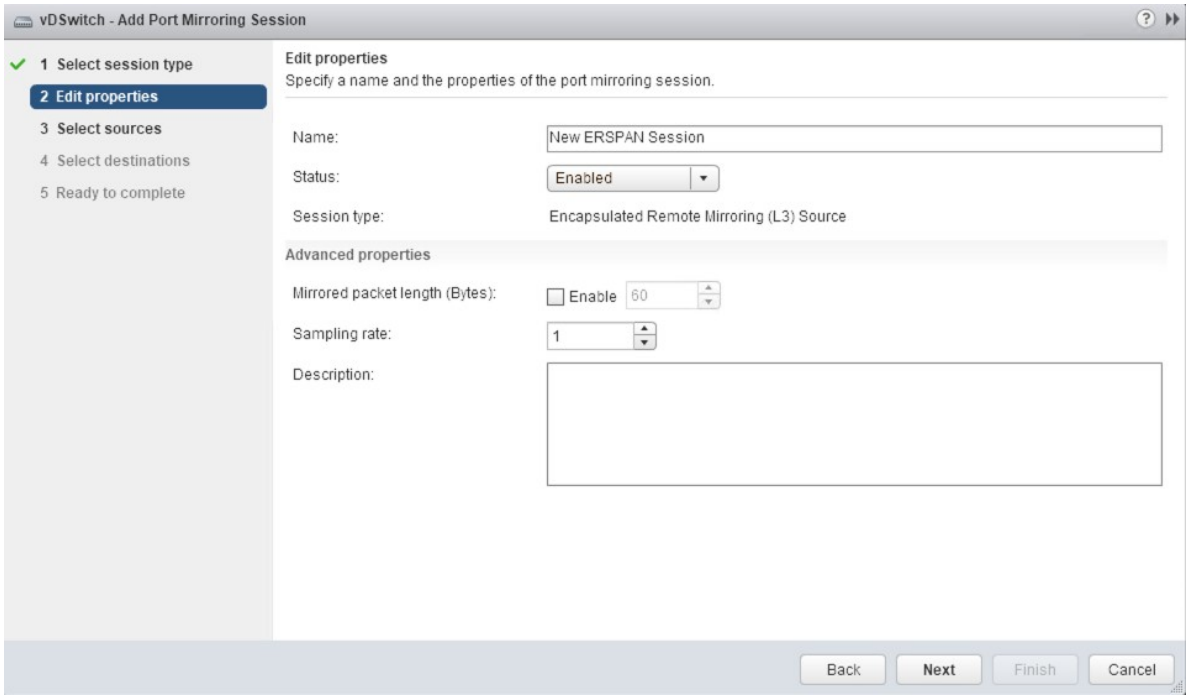
1. Select the VDS from the list of networks.
2. Select *Port mirroring* on the **Configure** tab.
3. Select *New...* to create a new session.



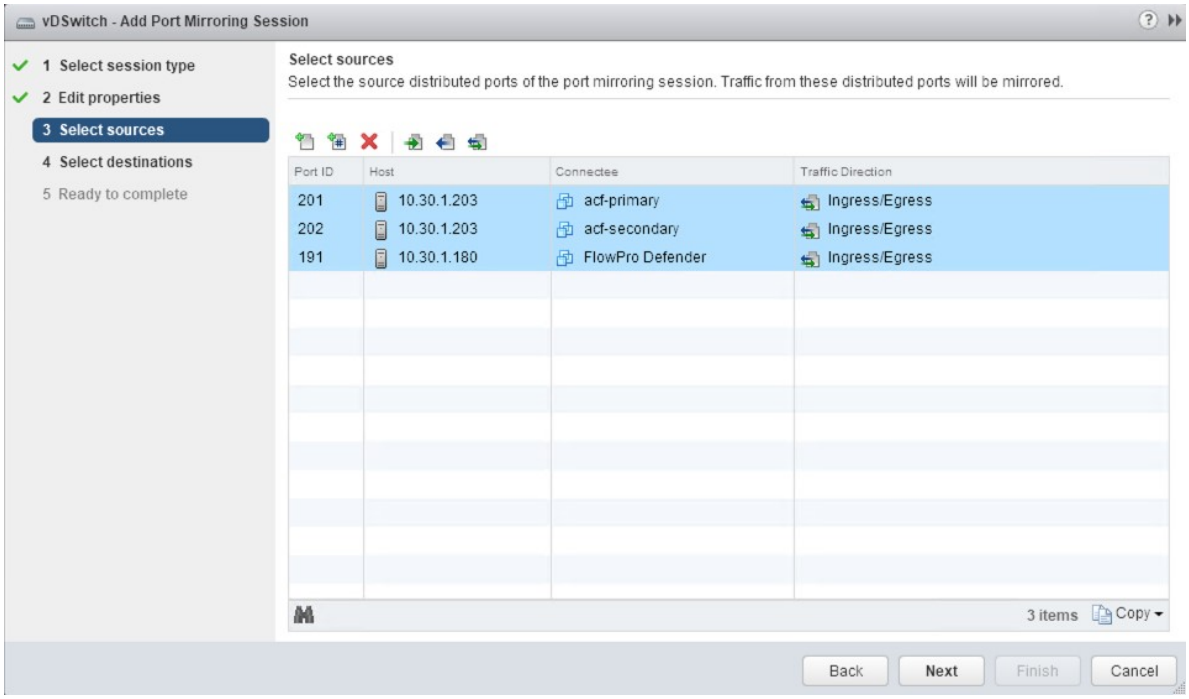
4. Select *Encapsulated Remote Mirroring (L3) Source*, and then click **Next**.



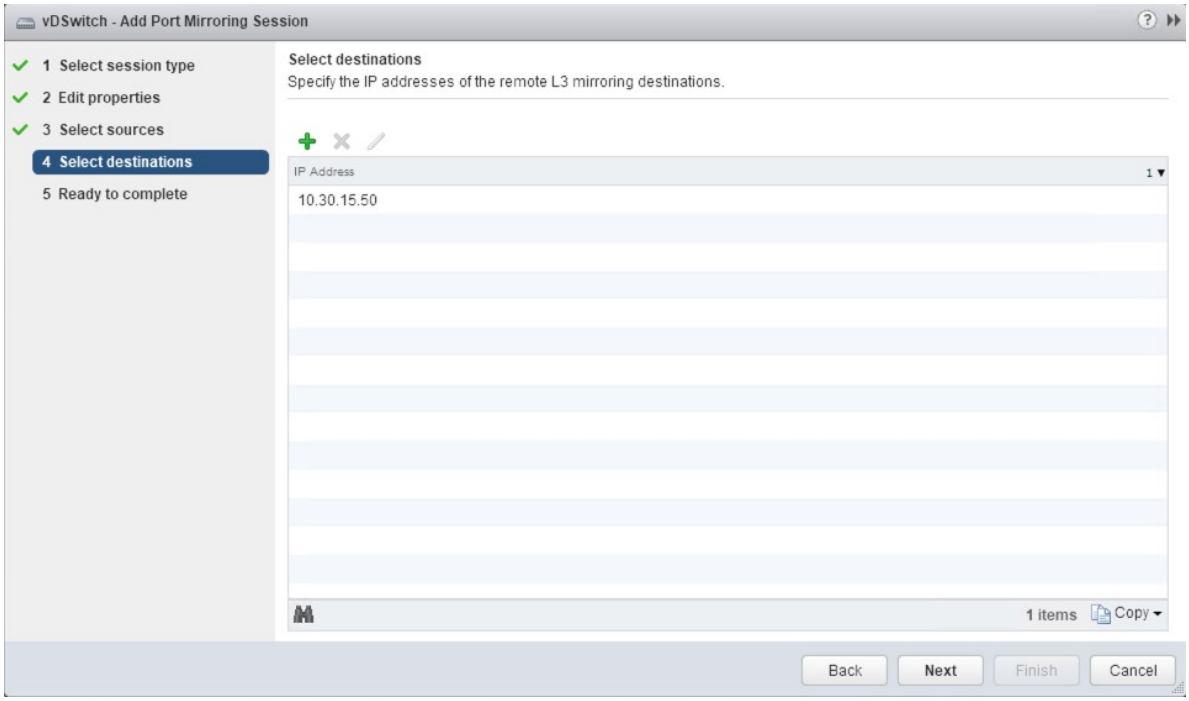
5. Give the new session a name and set the status to *Enabled*, and then click **Next**.



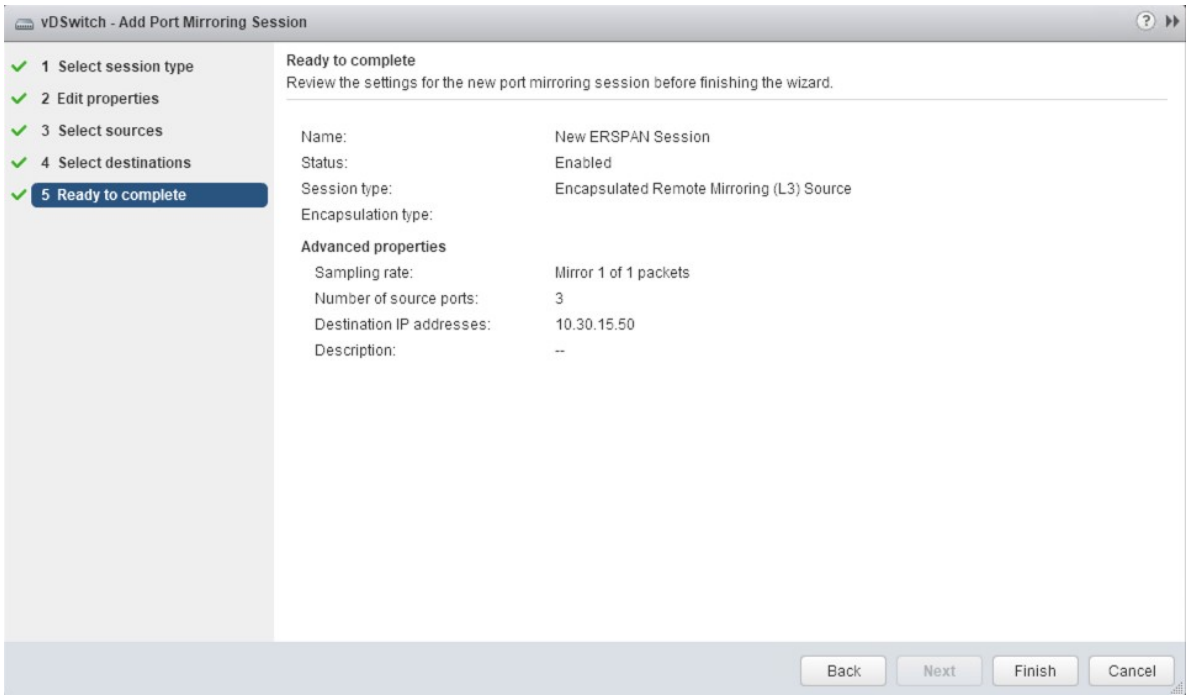
6. Add the ports intended to mirror to the probe, and then click **Next**.



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**.



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



CHAPTER

FOUR

ADDITIONAL RESOURCES

4.1 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

4.1.1 Change Log History

4.1.1.1 Version 20.0.0 - (03/2024)

ADDED: (8): Custom Inspection Rule Support for Detection
ADDED: (196): Selective Event Based Packet Capture
ADDED: (180): Replace Inspection/Detection Engine with Suricata

---

4.1.1.2 Version 19.1.2 - (10/2023)

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

4.1.1.3 Version 19.1.1 - (09/2023)

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

4.1.1.4 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

---

4.1.1.5 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

4.1.1.6 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

4.1.1.7 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

---

4.1.1.8 Version 16.8 - 8/16/2016

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

---

4.2 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/

4.3 Glossary

4.3.1 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)

4.3.2 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

4.4 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.

Suricata
https://suricata.io/
Copyright (c) 2016-2024, OISF
Licensed under the GNU GPL 2.0 License

Golang
https://go.dev/
Copyright (c) 2009-2024, The Go Authors
Licensed under the BSD 3-Clause License

Badger
https://dgraph.io/badger
Copyright (c) dgraph
Licensed under Apache v2 License

ET/Open Emerging Threats Open Ruleset
https://rules.emergingthreats.net/open/
Copyright (c) Proofpoint
Licensed under MIT License

Docker
https://www.docker.com/
Copyright (c) 2012-2018 Docker, Inc
Licensed under Apache v2 License

Gorilla Mux
https://github.com/gorilla/mux
Copyright (c) 2023 The Gorilla Authors.
Licensed under the BSD 3-Clause License