FlowPro Docs

Release 20.1.1

Plixer, LLC

Apr 20, 2026

VERSION 20.1.1

1 Getting started **1**

2 Using FlowPro **3**

3 Advanced Services **5**

4 Help and references **7**

4.1 Deployment Guides . . . 7
4.1.1 Pre-deployment . . . 8
4.1.1.1 License and probe registration . . . 8
4.1.1.2 SPAN configuration . . . 9
4.1.1.3 FlowPro (core probe functions) . . . 10
4.1.1.4 Updating the Scrutinizer reporter . . . 10
4.1.2 Virtual appliances . . . 10
4.1.2.1 CPU and RAM . . . 10
4.1.2.2 Storage . . . 11
4.1.3 Hardware appliance . . . 14
4.1.4 Initial configuration . . . 14
4.1.4.1 Appliance setup . . . 14
4.1.4.2 Registering and connecting interfaces . . . 15
4.1.4.3 Configuring ERSPAN . . . 16
4.1.4.4 Setup utility runmodes . . . 16
4.1.4.5 FlowPro service management . . . 17
4.2 Features and Functionality . . . 17
4.2.1 FlowPro functionality overview . . . 17
4.2.1.1 Custom rules . . . 18
4.2.1.2 Rule updates . . . 20
4.2.1.3 Selective packet capture . . . 20
4.2.1.4 FlowPro exclusions . . . 21
4.2.1.5 Untrusted domain lists . . . 21
4.2.2 ERSPAN . . . 22
4.2.2.1 Configuration . . . 22
4.2.2.2 FlowPro ERSPAN configuration . . . 22
4.2.2.3 Device-specific configuration . . . 24
4.3 Advanced Services . . . 28
4.3.1 Version upgrades . . . 28
4.3.1.1 Upgrading to v20.1.1 . . . 28
4.4 Additional Resources . . . 29
4.4.1 FlowPro changelogs . . . 30
4.4.1.1 Version 20.1.1 - (06/2025) . . . 30

4.4.1.2 Version 20.1.0 - (01/2025) . . . 30
4.4.1.3 Version 20.0.0 - (03/2024) . . . 31
4.4.1.4 Version 19.1.2 - (10/2023) . . . 31
4.4.1.5 Version 19.1.1 - (09/2023) . . . 31
4.4.1.6 Version 19.1.0 - (10/2022) . . . 31
4.4.1.7 Version 19.0.0 - 10/2020 . . . 32
4.4.1.8 Version 18.12.14 - 1/21/2019 . . . 32
4.4.1.9 Version 18.5 - 5/22/2018 . . . 32
4.4.1.10 Version 16.8 - 8/16/2016 . . . 33
4.4.2 Glossary . . . 33
4.4.2.1 FlowPro . . . 33
4.4.2.2 General networking . . . 34
4.4.3 Third-party atttributions . . . 38
4.4.3.1 Suricata . . . 38
4.4.3.2 Golang . . . 38
4.4.3.3 Badger . . . 38
4.4.3.4 ET/Open Emerging Threats Open Ruleset . . . 38
4.4.3.5 Docker . . . 38
4.4.3.6 Gorilla Mux . . . 38

CHAPTER

ONE

GETTING STARTED

Virtual appliances

Deploy your ESXi, Hyper-V, or KVM virtual appliance

Virtual appliances **Hardware appliance**

Deploy your hardware appliance

Hardware appliance **Appliance setup**

Complete initial setup and licensing after deployment

Initial configuration

CHAPTER

TWO

USING FLOWPRO

Custom rules

Enable and manage NIDS rules on FlowPro and custom Suricata rules

Custom rules **Rule updates**

Manage and customize Suricata rules

Rule updates **Selective packet capture**

Configure FlowPro to capture specific network packets for targeted traffic analysis

Selective packet capture **FlowPro exclusions**

Exclude trusted hosts or networks from FlowPro detections

FlowPro exclusions **Untrusted domain lists**

Configure domain reputation rules using external or custom domain lists for threat detection

Untrusted domain lists **ERSPAN**

Configure ERSPAN to mirror and route traffic over GRE to the FlowPro monitor interface

ERSPAN

CHAPTER

THREE

ADVANCED SERVICES

Version upgrades

Upgrade procedures and instructions

Version upgrades

CHAPTER

FOUR

HELP AND REFERENCES

Changelog

Version history and release notes

FlowPro changelogs **Glossary**

Glossary of terms used in FlowPro

Glossary **Attributions**

Open source and third-party licenses

Third-party atttributions About FlowPro

FlowPro is an advanced module of the Plixer One platform that delivers network visibility and actionable insights across both performance and security. It allows your team to capture, analyze, and forward enriched flow data even in environments with infrastructure constraints.

- Selective packet capture for targeted traffic analysis
- Event detection using a threat feed and custom NIDS rules
- DNS monitoring, including:
  - Identifying domains likely associated with malware
  - Analyzing DNS Start of Authority and DNS TXT messaging to identify potentially suspicious behavior
  - Supporting user-defined domain whitelists and blacklists
- Malware and botnet detection, including:
  - Monitoring for data exfiltration and command-and-control traffic
  - TLS and JA3 signature reporting
  - Reporting on HTTP connections and transferred file hashes

For further questions, contact *Plixer Technical Support*.

4.1 Deployment Guides

FlowPro is available in deployment packages for ESXi, Hyper-V, and KVM. *Hardware appliances* are also available upon request.

Contact *Plixer Technical Support* or a local reseller for availability and licensing or visit www.plixer.com to learn more.

Note

- FlowPro 20.1.0 requires Scrutinizer 19.5.x or higher.
- Before deploying any type of FlowPro appliance, complete *these steps* to add a license via the Scrutinizer web interface.

On this page:

Pre-deployment *Pre-deployment* Virtual appliances *Virtual appliances* Hardware appliance *Hardware appliance* Initial configuration *Initial configuration*

4.1.1 Pre-deployment

As part of the installation process, the following preparatory steps should be completed before deploying the FlowPro appliance. Review the subsections below for optimal deployment locations, recommended resource allocation, and licensing instructions.

4.1.1.1 License and probe registration

Before a FlowPro appliance is deployed, it must first be licensed and registered through the Scrutinizer web interface.

Adding a license

Note

If the following steps have already been completed, proceed to reviewing the resource requirements and deployment recommendations below.

To obtain and set up a new FlowPro license, follow these steps:

1. Contact *Plixer Technical Support* and provide them with the **Customer ID** and **Machine ID** found under Admin > Plixer > FlowPro Licensing in the Scrutinizer web interface.
2. Paste the key in the *License Key* field on the same page.
3. Click **Save**.

After a license key has successfully been added, the page will display the number of probes supported by the license as well as registered and deployed probe counts.

Registering a new probe

After a license key has been added, the FlowPro appliance/probe can be registered as follows:

1. Navigate to **Admin > Resources > FlowPro Probes** in the Scrutinizer web interface.
2. Click the **+** button and enter the following details in the **Add Probe** tray:
   - A name to identify the probe in Scrutinizer
   - The probe's MGMT interface IP address
   - The Scrutinizer collector to assign the probe to
3. [Optional] Leave *Default NIDS Rules* enabled to import NIDS rules from open-source threat feeds for network event reporting.
4. Click the **Save** button to register the probe configuration.

5. [Optional] To deploy multiple appliances, repeat the above steps until they have all been registered.

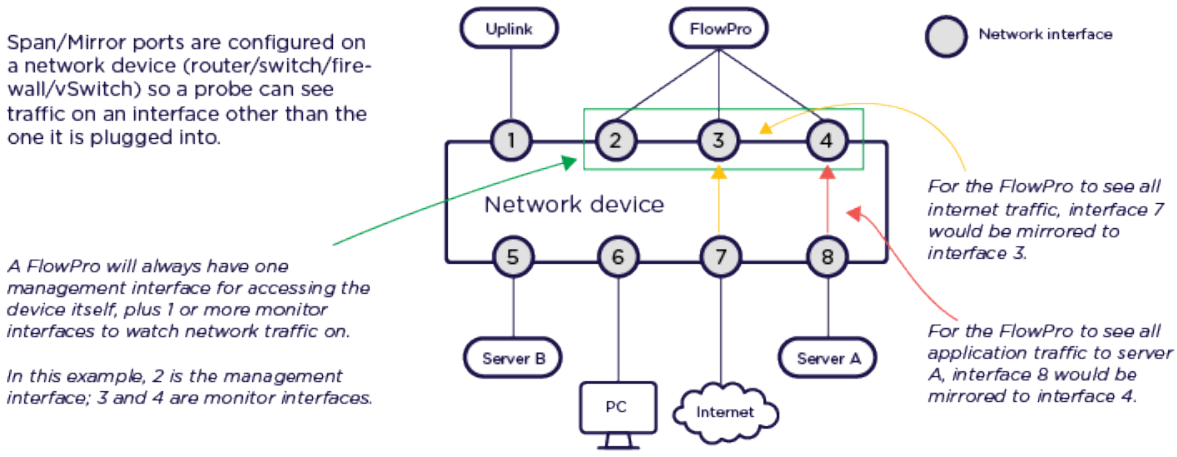
Confirm that the probe has been correctly registered in the main **FlowPro Probes** view, and then proceed to deploying the *hardware* or *virtual* appliance.

Note

- A license key and probe must be registered in Scrutinizer **before** the FlowPro appliance(s) is deployed. The MGMT IP address configured in Scrutinizer must also match the address assigned during the initial setup process after the appliance's first boot.
- If the *Default NIDS Rules* option is disabled, the probe will send only basic IPFIX observations, unless *custom rules* are manually added to the probe.
- FlowPro keys can be obtained from *Plixer Technical Support* and entered via the probe management page (for Scrutinizer versions below 19.6.0, the FlowPro key must be be entered via the FlowPro CLI).

4.1.1.2 SPAN configuration

By default, the monitor interfaces of a FlowPro appliance are set to promiscuous mode and can be connected directly to a mirrored port. This allows the appliance to be deployed in the optimal location for maximizing coverage and functionality.

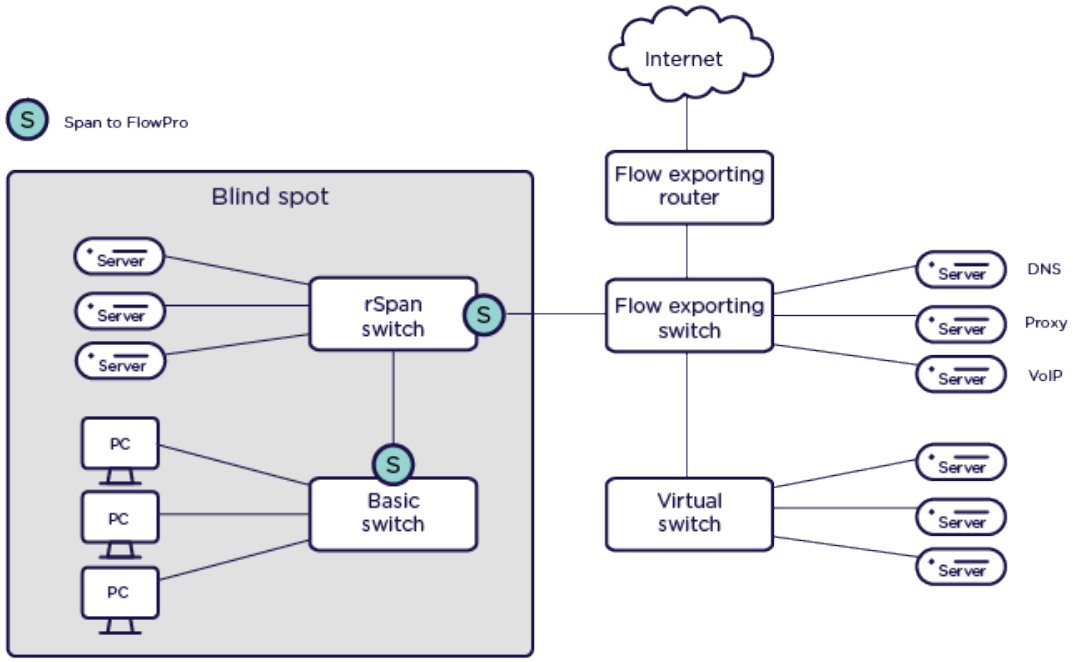


Note

- For remote SPAN (RSPAN) configuration instruction, see *this guide*.
- A 1 GB interface can be monitored using either separate SPAN interfaces for Rx/ingress and Tx/egress traffic or a single SPAN interface for both directions. Using dedicated SPANs for Rx and Tx traffic is recommended to allow for better traffic distribution and avoid potential bottlenecks. Rx and Tx SPAN interfaces can be configured as part of the FlowPro appliance's *initial setup* process.

The image below shows the recommended deployment locations for FlowPro based on the functions/features that will be enabled:

4.1.1.3 FlowPro (core probe functions)



4.1.1.4 Updating the Scrutinizer reporter

If the original primary Scrutinizer reporter in a high-availability configuration becomes permanently unavailable, FlowPro probes will need to be updated to point to the new primary reporter as follows:

1. SSH to the FlowPro server using the `plixer:flowpro` credentials.
2. Run the following command to stop the FlowPro service:

```
sudo service flowpro stop
```

3. Update the `.collector.reporter_address` in the `/home/plixer/flowpro/flowpro-settings.yaml` file.
4. Then run the following command to restart the FlowPro service:

```
sudo service flowpro start
```

4.1.2 Virtual appliances

See below for recommended resource scaling for FlowPro virtual appliances:

4.1.2.1 CPU and RAM

Default VM configuration	Medium traffic (up to 1 Gb/s)	High traffic (up to 10 Gb/s)
8 CPU cores8 GB RAM	6-10 CPU cores8-18 GB RAM	10-18 CPU cores18-34 GB RAM

4.1.2.2 Storage

Storage requirements scale with selective packet capture workloads and can be approximated using the following formula:

```
Capture depth * Max MTU of monitored interfaces * Expected number of source host:well-
↪known port:destination host combinations that will be stored for the specified␣
↪retention duration
```

The values above are stored in `~/flowpro/flowpro-settings.yaml`, where:

- Capture depth (`$pcap.server_capture_depth`) is the number of payload observations to be maintained per capture.
- Retention duration (`$pcap.server_ttl_hours`) is the number of hours captures are stored after the last observation.

ESXi deployment

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

Deploying the OVA Template

To deploy the FlowPro virtual appliance in ESXi, follow these steps:

1. Contact *Plixer Technical Support* and use the link they provide (`https://files.plixer.com/PACKAGE_PATH_AND_FILENAME`) to download the latest VMware virtual appliance package.
2. Extract the contents of the package to a location on the ESXi server.
3. In vSphere or vCenter, right-click the host to deploy the appliance to, and then select **Deploy OVF Template** from the menu.
4. Select **Local file** and browse to the FlowPro OVF and VMDK files before clicking **Next**.
5. Provide a name for the FlowPro virtual appliance and continue to follow the deployment wizard.
6. When prompted, select the datastore, set the disk format to **Thick Provision**, and then click **Next**.
7. Select the network to be used by the virtual appliance, and then verify the configuration in the summary before clicking **Finish** to import the Scrutinizer virtual appliance. This may take a few moments.

After the FlowPro virtual appliance has been successfully deployed, add the necessary monitoring interfaces (as explained below) before proceeding with the *initial appliance configuration*.

Adding new interfaces

After the appliance is deployed, at least one additional interface will need to be created for monitoring.

To add a new interface to the FlowPro virtual appliance, follow these steps:

1. In vCenter, right click on the FlowPro VM, and then select **Edit Settings…**.
2. Select **Add New Device**, and then select **Network Adapter** from the dropdown.

Available interfaces can be verified by checking `Flowpro.Interfaces` in `~/flowpro/flowpro-settings.yaml` after the *initial appliance configuration* is completed.

Note

- The virtual appliance will be configured with one network adapter (MGMT) by default.

- To monitor a different network, a mirror port of a virtual distributed switch or a mirror port using a physical NIC on the ESXi server will need to be configured.
- Monitoring interfaces can also be created at a later time. Follow *these steps* to register and connect additional interfaces.

Hyper-V deployment

The FlowPro virtual appliance for Hyper-V is provided as an all-in-one VHD template to streamline the deployment process.

Importing the virtual machine

To deploy the FlowPro virtual appliance in Hyper-V, follow these steps:

1. Contact *Plixer Technical Support* and use the link they provide (`https://files.plixer.com/PACKAGE_PATH_AND_FILENAME`) to download the latest Hyper-V virtual appliance package.
2. Extract the contents of the package to a location on the Hyper-V server.
3. Open **Hyper-V Manager**, right-click the virtual machine, and then select **Import Virtual Machine**.
4. Browse to the location of the FlowPro appliance folder.
5. Select the FlowPro virtual machine and click **Next**.
6. Use the radio buttons to select the import operation type and click **Next**.
7. Verify the settings in the summary and click **Finish** to import the virtual machine.

After the FlowPro virtual appliance has been successfully deployed, add the necessary monitoring interfaces (as explained below) before proceeding with the *initial appliance configuration*.

Adding new interfaces

After the appliance is deployed, at least one additional interface will need to be created for monitoring.

To add a new interface to the FlowPro virtual appliance, follow these steps:

1. After downloading the latest version of the FlowPro virtual appliance, unzip the package on the Hyper-V server.
2. In Hyper-V Manager, right click on the VM, and then select **Settings…**.
3. From the **Settings…** window, select **Add Hardware**.
4. From the dropdown menu, click **Network Adapter**.

Available interfaces can be verified by checking `Flowpro.Interfaces` in `~/flowpro/flowpro-settings.yaml` after the *initial appliance configuration* is completed.

Note

- The virtual appliance will be configured with one network adapter (MGMT) by default.
- To monitor a different network, a mirror port of a virtual distributed switch or a mirror port using a physical NIC on the Hyper-V server will need to be configured.
- Monitoring interfaces can also be created at a later time. Follow *these steps* to register and connect additional interfaces.

KVM deployment

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

Importing the virtual machine

To deploy the FlowPro virtual appliance in KVM, follow these steps:

1. Contact *Plixer Technical Support* and use the link they provide to download the latest KVM virtual appliance package:

```
curl -k -o PACKAGE_FILENAME.tar.gz https://files.plixer.com/PACKAGE_PATH/PACKAGE_
↪FILENAME.tar.gz
```

2. Create a directory for the install:

```
mkdir /kvm/flowpro
```

3. Extract the contents of the package to the new directory:

```
sudo tar xvzf PACKAGE_FILENAME.tar.gz -C /kvm/flowpro/
```

4. Run the installation script in the new directory:

```
cd /kvm/flowpro/PACKAGE_FILENAME
sudo ./deploy-flowpro.sh
```

5. Wait for the confirmation that the virtual machine has been created from the image.

After the FlowPro virtual machine has been created, add the necessary monitoring interfaces (as explained below) before proceeding with the *initial appliance configuration*.

Adding new interfaces

After the appliance is deployed, at least one additional interface will need to be created for monitoring.

To add a new interface to the FlowPro virtual appliance, follow these steps:

```
virsh attach-interface --domain <VM_NAME> --type network --source default --model virtio␣
↪--config --live
```

Available interfaces can be verified by checking `Flowpro.Interfaces` in `~/flowpro/flowpro-settings.yaml` after the *initial appliance configuration* is completed.

Note

- The virtual appliance will be configured with one network adapter (MGMT) by default.
- To monitor a different network, a mirror port of a virtual distributed switch or a mirror port using a physical NIC on the KVM server will need to be configured.
- Monitoring interfaces can also be created at a later time. Follow *these steps* to register and connect additional interfaces.

4.1.3 Hardware appliance

After removing the FlowPro hardware appliance from its packaging, verify that all accompanying accessories (rack-mount kit, appliance-locking bezel and keys, and power cord) are included. The appliance can be mounted in a standard 19-inch rack or cabinet.

> **Important**
>
> If your box arrives torn, dented, or otherwise damaged, the appliance itself seems damaged, or there are missing parts, *contact Plixer Technical Support* immediately and **do not attempt to install the unit**.

From there, follow these steps to set up the FlowPro hardware appliance:

1. Connect the power cable to one of the power supply sockets and plug the other end to a grounded AC outlet or UPS. To take advantage of the redundant PSUs, ensure that each socket is connected to an independent power source.
2. Connect the appliance to the network using the MGMT port.
3. Refer to *these deployment location recommendations*, and then connect the necessary cables to the monitoring ports.
4. Connect the iDRAC port to a remote access controller using an RJ-45 cable to enable remote console access for hardware management and monitoring. *Contact Plixer Technical Support* for help with configuring alerts for hardware-related events.

After the FlowPro hardware appliance has been racked and cabled, proceed to *configuring the appliance*.

4.1.4 Initial configuration

Once the FlowPro appliance has been deployed and the necessary monitoring interfaces have been added, power it on and log into the console using the credentials `root:plixer`. The appliance will go through a quick initialization sequence and then reboot.

> **Note**
>
> - For hardware appliances, SSH to 192.168.168.168/24 using the credentials `plixer:flowpro` instead. KVM appliances should run `virsh console Plixer FlowPro` and log in with the credentials `plixer:flowpro`.
> - Before proceeding, review *these pre-deployment notes* and complete the *licensing process*.

4.1.4.1 Appliance setup

After the reboot, log in again and follow the initial setup prompts:

View instructions

1. Review and accept the EULA.
2. Configure the networking properties and user credentials for the appliance:
   - Appliance hostname (must be a fully qualified hostname)
   - Static IP address (must match the address registered for the probe in Scrutinizer)
   - CIDR (mask only - 8, 16, etc.)
   - Gateway

- DNS IP
- New password for the `root` user
- New password for the `plixer` user

3. Wait for the appliance to reboot, and then SSH to the IP address entered as the `plixer` user with the new password.
4. Provide the following Scrutinizer details:
   - Current password for the `plixer` user
   - IP address of the Scrutinizer server (or the primary reporter in distributed clusters)
   - Destination collector address (either same standalone server as above, a remote collector in a distributed cluster, or a Replicator instance)
   - Authentication token generated after the probe was registered in Scrutinizer
5. Enter the following details 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
   - Alternative DNS name 1 (press Enter to stop adding)
6. Select whether the appliance can access the Internet or to continue the setup locally, and then follow any additional instructions.
7. If a FlowPro key has not been entered via the Scrutinizer web interface, select **Yes** to enter it when prompted.
8. Enter the address of the NTP server to use for clock-syncing.

After the initial appliance setup has been completed, monitoring interfaces should be registered and connected to observation points.

> **Note**
>
> The setup script automatically generates both a self-signed certificate and a certificate signing request (`~/flowpro/server.csr`). After getting the request signed by a certificate authority, overwrite the existing `~/flowpro/server.crt`. To continue using the self-signed certificate, navigate to `https://<FLOWPRO_MGMT_IP>:8080` on each user browser and accept the security exception.

4.1.4.2 Registering and connecting interfaces

Once the appliance is running, all monitoring interfaces must be registered and connected to observation points as follows:

View instructions

> **Note**
>
> Monitoring interfaces can be added at any time following the corresponding instructions for *ESXi*, *Hyper-V*, or *KVM* deployments. The steps below must be completed after new monitoring interfaces are added.

1. Register all additional interfaces as `monX` interfaces:

```
cd flowpro
sudo ./setup.sh --monitor-ports
```

2. Create one or more observation points by specifying Rx and Tx interface pairs for monitoring:

```
sudo ./setup.sh --create-observation-point
```

To verify that the interfaces have been successfully registered and connected, check `Flowpro.Interfaces` in `~/flowpro/flowpro-settings.yaml`.

4.1.4.3 Configuring ERSPAN

To configure traffic mirroring via ERSPAN, do the following:

View instructions

1. After the monitoring interfaces have been added and registered, run the following command:

```
sudo ./setup.sh --erspan-config
```

2. Then enter the following details for the configuration:
   - IP address to assign to a monX interface
   - Source IP
   - Destination IP
   - ERSPAN ID and key

4.1.4.4 Setup utility runmodes

After the initial setup process, you can manually execute `~/flowpro/setup.sh` to re-run the entire setup utility.

You can also run a specific configuration task by running the following command:

```
sudo ./setup.sh [OPTION]
```

Then replace `[OPTION]` with the specific flag that corresponds to the service you want to configure.

The following optional flags are available for this process:

View content

Reset `/home/plixer/flowpro/flowpro-settings.yaml` to its default state	`--reset-config`
Back up the current configuration	`--reconfigure`
Register all interfaces as monX interfaces	`--monitor-ports`
Configure exporter settings, including MGMT IP, Scrutinizer server/reporter IP, collector IP, and authentication token; configure Kafka if ML Engine ETA IP is provided	`--exporter-config`
Configure SSL certificate details and re-create the self-signed certificate and certificate signing request	`--cert-generation`
Pull Suricata image from Dockerhub and set up Docker environment (also supports offline setup with a local Docker image)	`--container-setup`
Configure ERSPAN settings	`--erspan-config`
Reset firewall settings to default	`--firewall-mgmt`
Configure Rx and Tx interface pairs for monitoring	`--create-observation-point`
Add/edit a FlowPro key (written to `/etc/nprobe.license`)	`--set-apm-key`
Configure NTP server details (written to `/etc/ntp.conf`) and restart the service	`--set-ntp`

4.1.4.5 FlowPro service management

The FlowPro service is managed using the following command:

```
service flowpro [start|stop|restart]
```

4.2 Features and Functionality

Custom rules

Enable and manage NIDS rules on FlowPro and custom Suricata rules

Custom rules **Rule updates**

Manage and customize Suricata rules

Rule updates **Selective packet capture**

Configure FlowPro to capture specific network packets for targeted traffic analysis

Selective packet capture **FlowPro exclusions**

Exclude trusted hosts or networks from FlowPro detections

FlowPro exclusions **Untrusted domain lists**

Configure domain reputation rules using external or custom domain lists for threat detection

Untrusted domain lists **ERSPAN**

Configure ERSPAN to mirror and route traffic over GRE to the FlowPro monitor interface

ERSPAN

4.2.1 FlowPro functionality overview

When FlowPro is enabled, it leverages deep packet inspection (DPI) and advanced traffic analysis techniques to detect potential security threats and alert you when your assets may be compromised by malware.

By monitoring DNS traffic, FlowPro provides critical insights into data entering and leaving your network, helping to identify malicious activity and prevent data exfiltration.

The following features and functionalities are available when the FlowPro functionality is enabled:

- **DNS Traffic Analysis:** Gain visibility into DNS queries and responses to identify potentially malicious domains or unusual behavior.
- **Threat Detection:** Utilize selective packet capture, threat feeds, and custom network intrusion detection system (NIDS) rules for identifying suspicious activity, such as command-and-control traffic or DNS tunneling.
- **TLS and JA3 Signature Reporting:** Monitor encrypted traffic to detect anomalous patterns and potential misuse of encryption protocols.
- **HTTP Connection Reporting:** Identify and track HTTP requests for enhanced visibility into application-layer behavior.
- **File Hash Analysis:** Capture information on transferred files and calculate hashes to detect potential malware.
- **DNS Reputation Checks:** Compare DNS queries against domain reputation lists to uncover threats such as NXDOMAIN responses and suspiciously long DNS names.
- **Customizable Whitelists and Blacklists:** Define trusted and restricted domains to tailor detection to your organization's needs.
- **Botnet and Command-and-Control Detection:** Identify and mitigate traffic associated with known botnets or malicious command-and-control servers.

4.2.1.1 Custom rules

For online appliances, FlowPro is pre-equipped with the ability to implement a large set of detection and prevention rules from the *Emerging Threats* ruleset collection of known potentially malicious or suspect traffic. This can be enabled when adding or editing a FlowPro integration by toggling the *Default NIDS Rules* option via **Admin > Resources > FlowPro Probes** in the Scrutinizer web UI. In addition to this, users can define custom rules in the `/home/plixer/flowpro/rules/custom.rules` file to be 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; rev:1;)
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"; nocase; 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;)
```

(continues on next page)

(continued from previous page)

```
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"; classtype:non-standard-
↪protocol; tls.version:1.0; sid:3000005; rev:1;)
#alert tcp any any -> any any (msg:"A commented out rule to temporarily disable";␣
↪classtype:example; sid:3000006; rev:1;)
```

The following fields are the minimum required for FlowPro events to be sent to Scrutinizer. Each class type corresponds to a specific policy in Scrutinizer.

View content

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

4.2.1.2 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 statements 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.

4.2.1.3 Selective packet capture

When deployed as part of the Plixer One platform, FlowPro enables selective capturing of network packets based on user-defined rules. This allows for targeted sampling of network traffic, which can result in more efficient analysis/investigation as well as optimal resource utilization.

> **Note**
>
> The steps described below require Scrutinizer 19.6.0 or higher. For assistance with other versions, contact *Plixer Technical Support*.

Selective packet capture rules can be defined via the Scrutinizer web interface as follows:

1. Navigate to **Admin > Resources > FlowPro Capture Rules**.
2. Click the **+** button and configure the following details in the tray:
    - **Name**: A name for the capture rule
    - **Client IP**: Client/source IP address of packets to capture
    - **Server IP**: Server/destination IP address of packets to capture
    - **Well-Known Port**: Well-known port to monitor for packets
    - **Max Packets**: Maximum number of packets to capture
    - **Stops On**: End date for capturing packets
    - **Retain Until**: End date for retaining captured packet data
3. [Optional] Use the *Enabled* toggle to disable the rule to start capturing packets at a later time.
4. Click the **Save** button to create the rule.

Packets will start being captured as soon as a rule is saved (if enabled). Rules with captured data will be indicated by a check in the *Data* column.

> **Note**
>
> The timezones configured on the Scrutinizer server and the FlowPro probe must be the same for the *Stops On* rule to be correctly observed.

Downloading PCAP files via Scrutinizer

Captures can be downloaded by clicking **Download PCAP** for events under the *FlowPro Event Capture* policy in the Scrutinizer Alarm Monitor views.

Because these download requests are redirected to the FlowPro appliance, an exception for the default self-signed certificate must be added to Scrutinizer user browsers. To do this, navigate to `https://<FLOWPRO_MGMT_IP>:8080`, and then accept the security exception.

Rule management

Once the maximum number of packets has been captured, or the defined end date has been reached, the rule will automatically be disabled. Inactive rules will be marked with a yellow indicator in the main view/table instead of green (enabled/active).

To continue capturing packets, click on the rule name, make the necessary changes (*Max Packets* or *Stops On*) in the configuration tray, and then re-enable the rule.

Rules that are no longer needed can instead be deleted. To do this, use the checkboxes to select one or more rules to be deleted, and then use the **Delete** option in the *Bulk Actions* menu/tray.

4.2.1.4 FlowPro exclusions

To exclude hosts from FlowPro detections, you can add them to the *FlowPro Exclusions* IP group. This group allows flexibility in defining exclusions by supporting individual IP addresses, entire subnets, or other IP groups.

Once added, traffic from these hosts will no longer trigger detections, ensuring they are excluded from monitoring while maintaining overall security visibility.

This feature is useful for trusted systems, testing environments, or specific infrastructure components that may generate benign traffic resembling threats.

Administrators should carefully manage this group to prevent accidental exclusion of potentially malicious activity, balancing security and operational requirements effectively.

4.2.1.5 Untrusted domain lists

FlowPro supports the use of a domain reputation review downloaded from external and user-defined domain lists.

Domain reputation

FlowPro enforces domain reputation review through the use of domain aware network intrusion detection rules.

On service start, FlowPro will integrate all rule sources in `/home/plixer/flowpro/rules/suricata-update.yaml`, violations are attributed to a rule class and forwarded Scrutinizer events.

JA3 signatures

FlowPro enforces JA3 signature review through the use of TLS aware network intrusion detection rules.

On service start, FlowPro will integrate all rule sources in `/home/plixer/flowpro/rules/suricata-update.yaml`, violations are attributed to a rule class and forwarded Scrutinizer events.

User-defined domain lists

You can load the custom domains via `/home/plixer/flowpro/importDomainRep.sh`, and then save it locally in your FlowPro as `domains.csv`.

Then run the following command to convert the domain list into DNS domain reputation detection rules in `/home/plixer/flowpro/rules/custom.rules`:

```
./home/plixer/flowpro/importDomainRep.sh path_to_domain.csv
```

User-defined JA3 signature lists

This will produce events in Scrutinizer under the *Device Retrieving External IP Address Detected* policy, alerting when DNS requests are made for the untrusted domains.

Finally, run the following command to restart the FlowPro service to enter the events into the detection engine:

```
sudo service flowpro restart
```

4.2.2 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 FlowPro appliance.

On this page:

FlowPro ERSPAN configuration *FlowPro ERSPAN configuration* Cisco switch configuration *Cisco switch* VMware VDS configuration *VMware VDS*

4.2.2.1 Configuration

Configuration is required on both the FlowPro and the ERSPAN/GRE device, as each device's setup requires information from the other.

Prerequisites

The following information should be determined prior to starting the configuration:

ERSPAN device configuration

- **ERSPAN Source IP**: The IP address on the device (switch or router) or the ESXi host IP address (VDS).
- **Destination IP**: The FlowPro monitor port IP address (not the FlowPro management IP).
- **ERSPAN Type/Version**: Legacy ERSPAN = Type 1/Ver 0, Type II = Ver 1, Type III = Ver 2

> **Note**
>
> ERSPAN Versions 1 and 2 will prompt to set up the ERSPAN destination interface. FlowPro also provides support for GRE type 2.

4.2.2.2 FlowPro ERSPAN configuration

1. Run the following command:

   ```
   sudo ./setup.sh --erspan-config
   ```

2. Confirm whether you need to assign an IP address to a monitoring interface to receive ERSPAN.

   ```
   Do you need to IP a monitor interface to receive ERSPAN? (yes/no): yes
   ```

3. Enter the monitoring interface name to assign an IP address as the ERSPAN destination.

```
Monitor Interfaces Available:
mon1
mon2
mon3
############################
Enter the interface name to IP for ERSPAN Destination: mon1
```

4. Then, enter the IP address of the monitoring interface.

```
Enter the IP address (with CIDR notation, e.g., x.x.x.x/yy) for mon1: 192.168.1.24/
↪24
```

5. Verify the ERSPAN version.

```
Do you need to set up a Virtual Type II/III ERSPAN destination? (yes/no):
```

6. If yes, enter a name for the ERSPAN mon port. If no, the ERSPAN traffic will go directly to the configured interface, completing the ERSPAN setup.

```
Enter a name for this ERSPAN MON port [fp_erspan_x]:
```

> **Important**
>
> Take note of this interface name as it will need to be added to an observation interface pair after setup.

7. Re-enter the ERSPAN source for the virtual interface peer.

```
Enter your Local ERSPAN destination IP (Not MGMT IP):
```

8. Enter the ERSPAN version.

```
############################################################
ERSPAN Version Map: ERSPAN Type II = 1, ERSPAN Type III = 2
############################################################
Enter your ERSPAN Version:
```

9. Enter the ERSPAN ID.
10. Once you complete the setup, run the following command for either the virtual or physical interface configured to receive ERSPAN:

```
sudo ./setup.sh --create-observation-point
```

Command reference

The monitoring interface(s) must first be enabled as defined in the hardware appliance or virtual appliance installation instructions.

Next, connect to FlowPro over SSH, and then use the `enable erspan` command to configure FlowPro for ERSPAN.

- `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

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

4.2.2.3 Device-specific configuration

Cisco switch

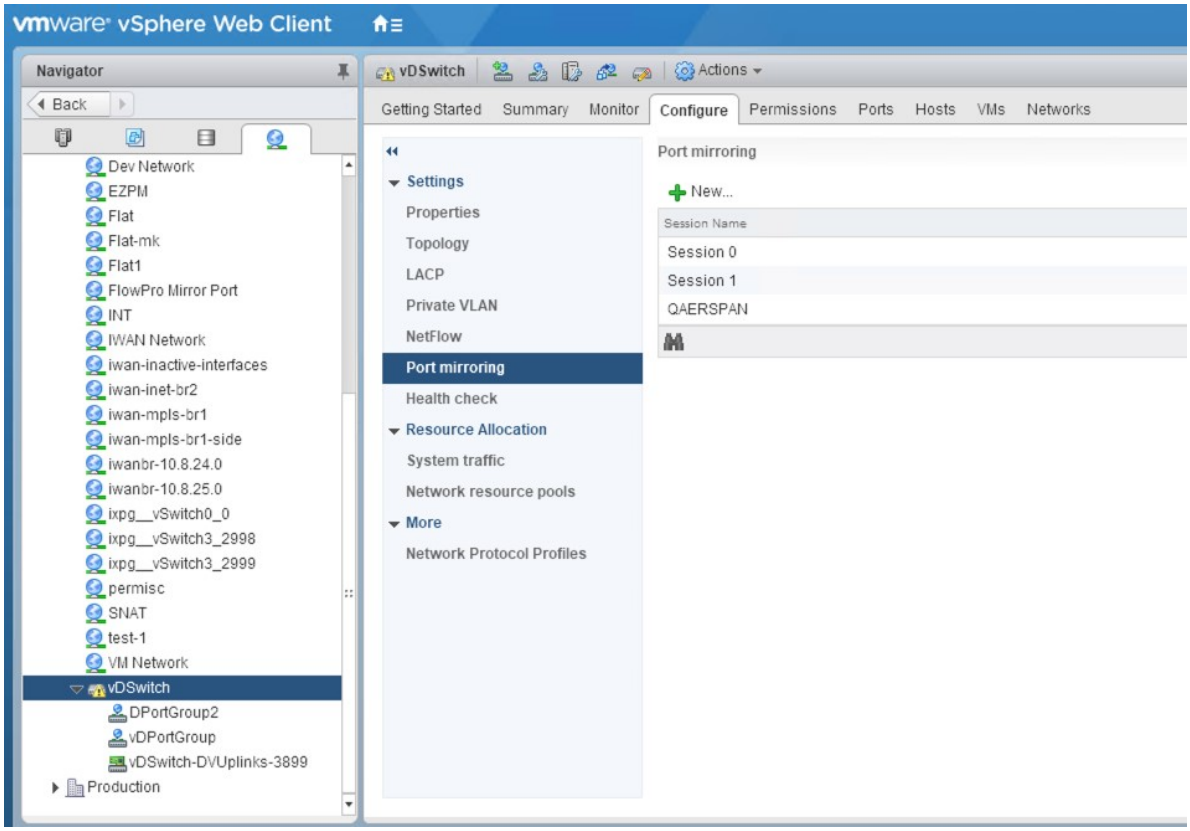
```
monitor session 1 type erspan-source
description ERSPAN direct to FlowPro
erspan-id 32                              # required
vrf default                               # required
destination ip 10.1.2.3                   # IP address of FlowPro monitor interface
source interface port-channel1 both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

monitor erspan origin ip-address 10.1.2.1 global
```

VMware VDS

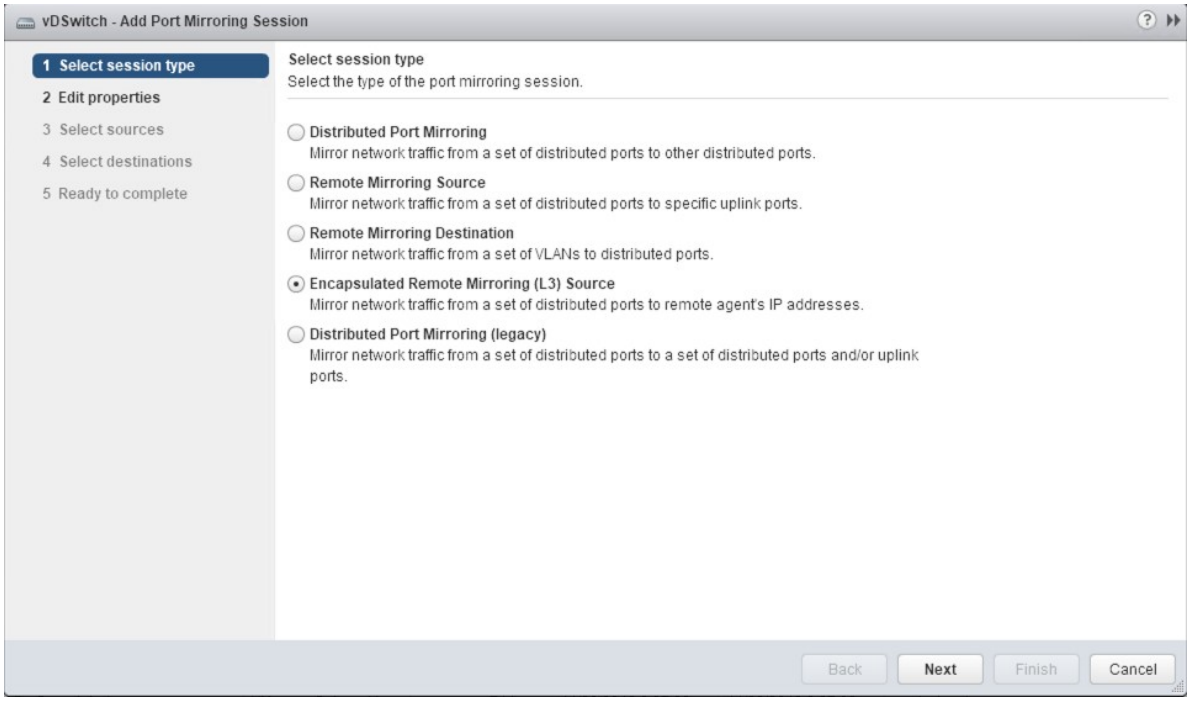
> **Note**
>
> This requires the VMware Enterprise Plus license and a configured vSphere Distributed Switch.

From the VMware web console, do the following:

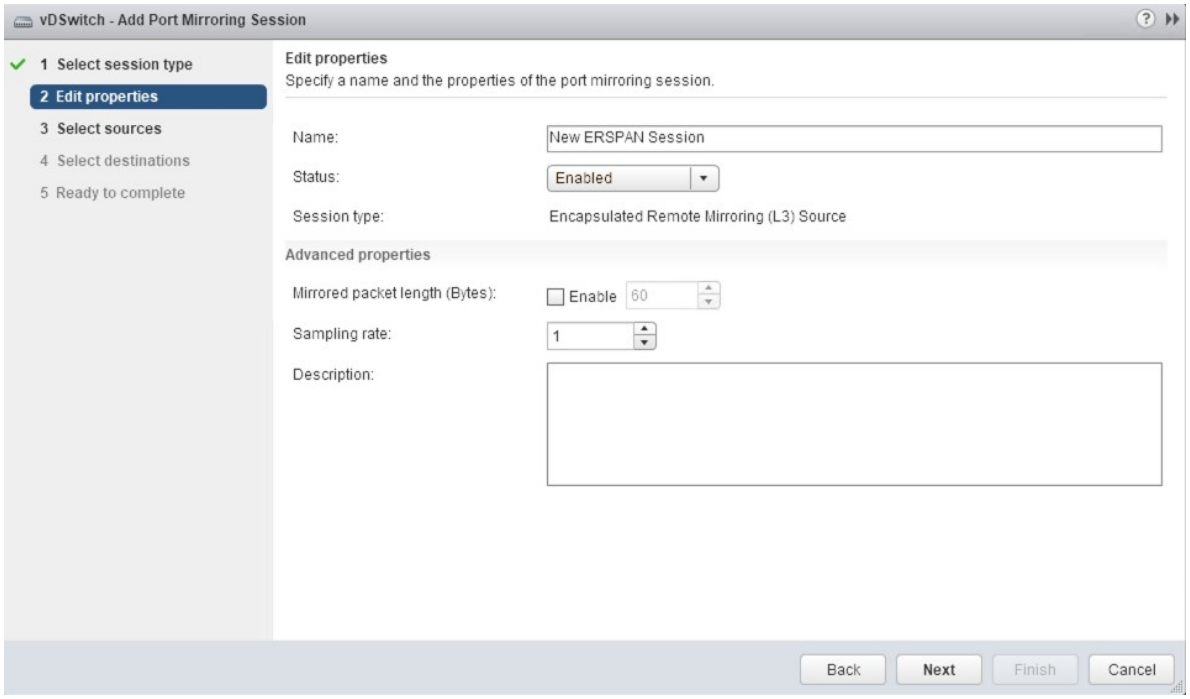
1. Select the VDS from the list of networks.
2. Select **Port mirroring** on the *Configure* tab.
3. Select **New…** to create a new session.



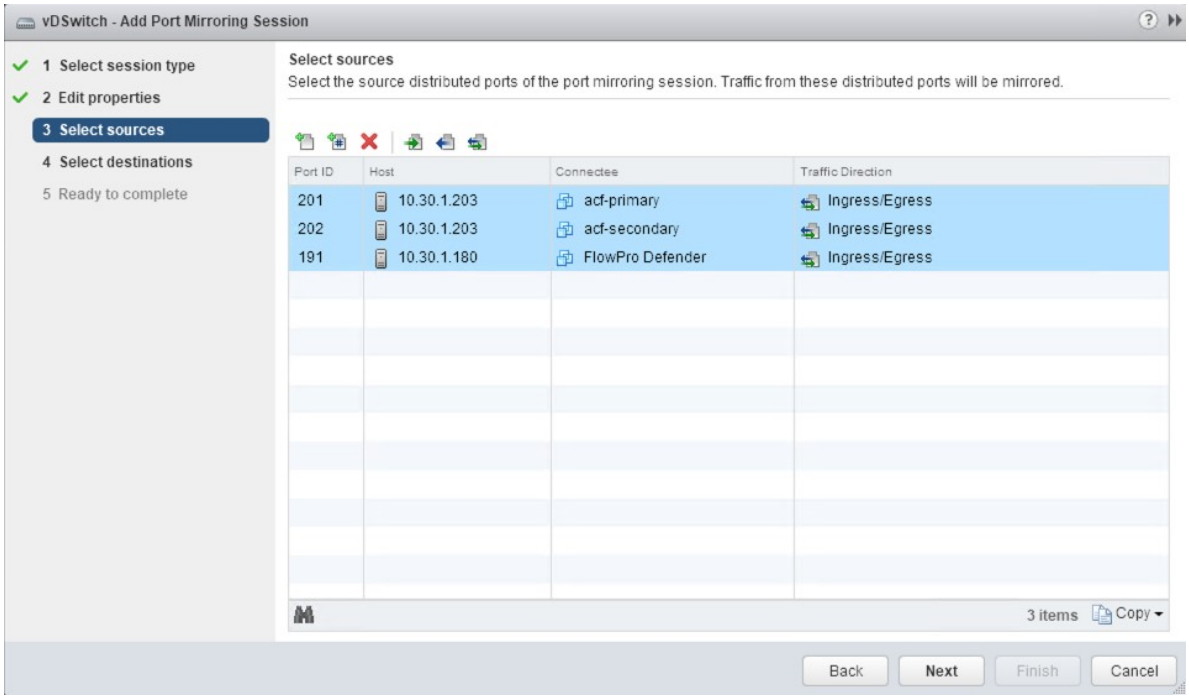
4. Select **Encapsulated Remote Mirroring (L3) Source**, and then click **Next**.



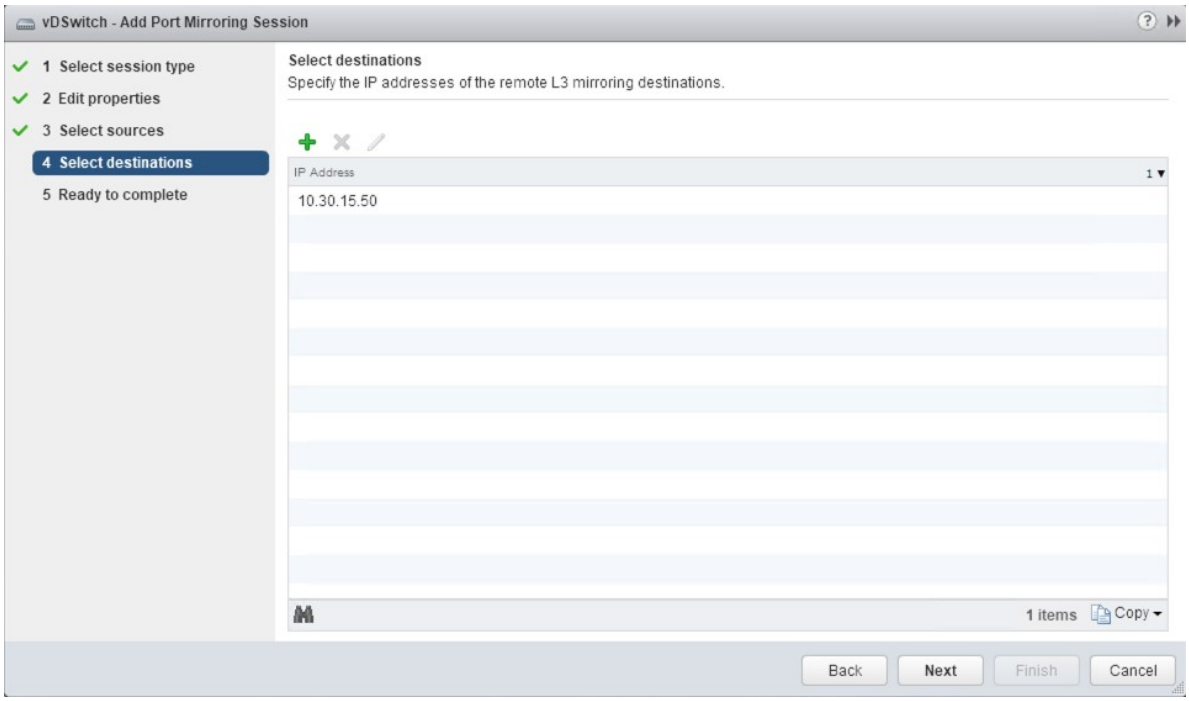
5. Give the new session a name, set the status to **Enabled**, and then click **Next**.



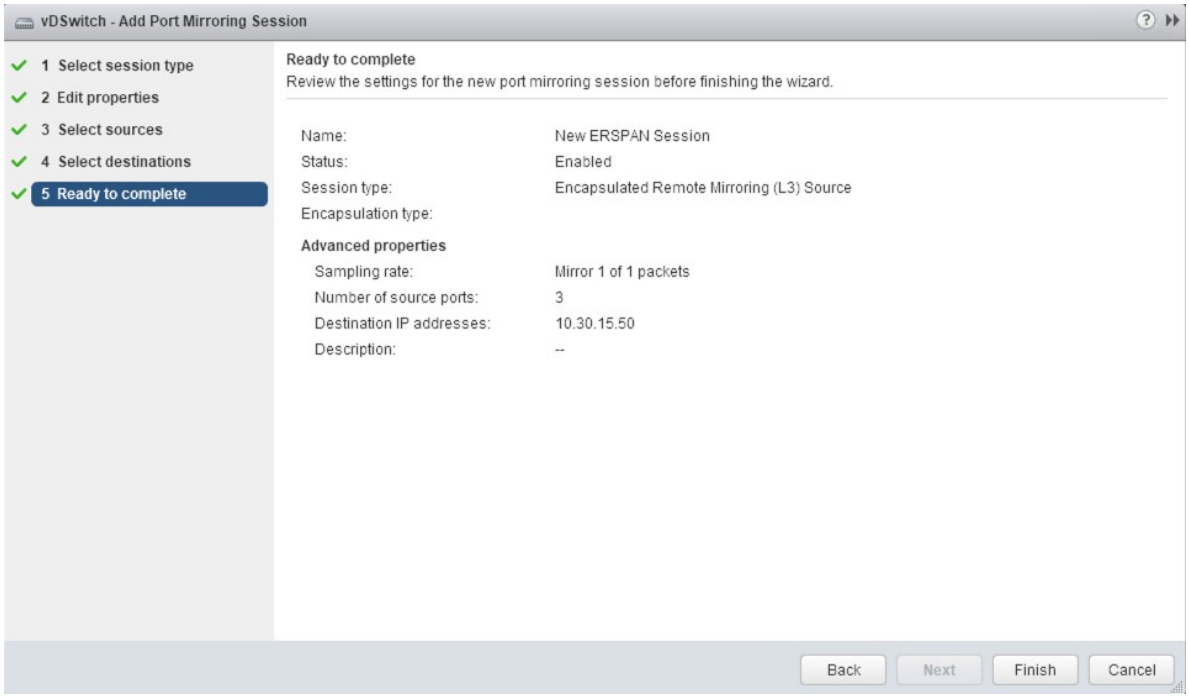
6. Add the ports intended to mirror to the probe, and then click **Next**.



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



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



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.

4.3 Advanced Services

Certain advanced functions/services, such as the interactive CLI, are currently unavailable in FlowPro 20.1.1.

4.3.1 Version upgrades

Version upgrades may include additional functionality, performance enhancements, and/or other improvements over previous versions. Fixes for certain types of issues will also be included in these updates.

4.3.1.1 Upgrading to v20.1.1

The update to FlowPro 20.1.1 requires the current instance to be on v20.0.0 or higher.

Important

While it is possible to install FlowPro update packages without assistance, it is highly recommended to contact *Plixer Technical Support* and allow our engineers to guide you through the process.

Pre-upgrade preparation

Before attempting to install any type of update package, the following procedures should be observed:

- Verify that the version currently installed can be upgraded to the target version.
- Delete any older update files/packages from the home directory for the `plixer` user.

- [Scrutinizer 19.5.x and below only] Save an external copy of your FlowPro key (if applicable).

Upgrade process

Once all preparation steps have been completed, follow these steps to upgrade the appliance:

View instructions

1. Ensure that a backup of the current install has been saved to an external location, as part of the *recommended preparatory procedures*.
2. SSH to the FlowPro instance as the `plixer` user and start a new tmux session:

```
tmux new -s upgrade
```

3. Download the update package for FlowPro 20.1.1:

```
curl -k -o update-flowpro-20-1-1.sh https://files.plixer.com/downloads/flowpro/20/update-
↪flowpro-20-1-1.sh
```

4. Set the correct permissions for the update script:

```
sudo chmod +x update-flowpro-20-1-1.sh
```

5. Run the update script:

```
sudo ./update-flowpro-20-1-1.sh -s release
```

Once the script completes running, the system must be rebooted to update the kernel and complete the upgrade to FlowPro 20.1.1.

Note

On Scrutinizer 19.5.x and below, the FlowPro key will need to be re-entered after the probe is upgraded.

Offline upgrades

To update a FlowPro instance that cannot access the Internet, follow these steps:

View instructions

1. Download the update package from a system with Internet access.
2. Copy the package to the home directory of the `plixer` user.
3. Follow the online update procedure above starting from step 4.

Once the script completes running and the system reboots, the FlowPro instance will be on v20.1.1.

4.4 Additional Resources

Changelog

FlowPro updates and version history

FlowPro changelogs **Glossary**

Glossary of terms used in FlowPro

Glossary **Attributions**

Open source and third-party licenses

Third-party atttributions **Plixer technical support**

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

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

4.4.1 FlowPro changelogs

Changelog entries are displayed in the format **DESCRIPTION (Ticket Number)**.

Note

- For more information on FlowPro, visit www.plixer.com or contact *Plixer Technical Support*.
- Please refer to our End of Life Policy for EOL schedule details.

4.4.1.1 Version 20.1.1 - (06/2025)

Changelog

New features

- Enable SMB Export for Analysis

Fixes

- Addressed various security issues
- Clarify AI engine setup verbiage (69)
- FlowPro Function Status UI (72)
- PCAP Event by Device/Rule (36)
- PCAP Time Consistency (68)
- Retained PCAPs Degraded or Not Present (69)
- Setup Order of Operations (70)
- Support certificate generation with flags (79)

4.4.1.2 Version 20.1.0 - (01/2025)

Changelog

New features

- Accept Token for ML Compat
- Application Performance Monitoring
- ERSPAN Version 2/Type III Support
- Include mon1 and mon2 by default
- Support KVM format

- Sync Capture Rules From UI

Enhancements

- Ask for NTP server during setup

Fixes

- Addressed various security issues
- APM Flow Export exclusively through mgmt interface (49)
- ERSPAN Interface Persistence (58)
- ERSPAN Network Routes when interfaces are on the same network (37)
- Issue with nested dot1q VLAN TAG (24)
- Same Subnet Multi-Interface Stability (57)
- Setup Script Help Descriptions (44)

4.4.1.3 Version 20.0.0 - (03/2024)

Changelog

New features

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

4.4.1.4 Version 19.1.2 - (10/2023)

Changelog

Fixes

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

4.4.1.5 Version 19.1.1 - (09/2023)

Changelog

Fixes

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

4.4.1.6 Version 19.1.0 - (10/2022)

Changelog

Fixes

- Hardware 10Gb FlowPro APM Understating (56)
- FlowPros Deploying with only 1 network (97)
- yum update breaks flowpro APM (114)

- Separate Observation domains per monitor interface by default to fix high MFSN's (117)

4.4.1.7 Version 19.0.0 - 10/2020

Changelog

New features

- Custom JA3 Blacklist Support (55)
- JA3 Fingerprinting Support (63)

Fixes

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

4.4.1.8 Version 18.12.14 - 1/21/2019

Changelog

New features

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

Fixes

- Defender no longer truncates logs on restart (377)

4.4.1.9 Version 18.5 - 5/22/2018

Changelog

Fixes

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

- APM won't start nProbe for more than one interface (25913)

4.4.1.10 Version 16.8 - 8/16/2016

Changelog

New features

- Defender now exports HTTP Header Fields (13509)

Fixes

- Domain Exclusion List – Now Applies to BotNet Detection (21010)

4.4.2 Glossary

This glossary is meant to serve as a reference for terms and concepts used in the FlowPro system software or this product manual.

4.4.2.1 FlowPro

View content

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

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

plixer.ini
FlowPro configuration file

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

4.4.2.2 General networking

View content

2LD (Second-level Domain)
Part of the naming convention for 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

ACK (Acknowledgment Code)
A unique signal sent by a computer to show that it has successfully transmitted data

ACL (Access Control List)
A set of rules governing access to a particular object or system resource

Active Directory / AD
Proprietary directory service offered by Microsoft, which allows for centralized management of users, devices, and other IT assets

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

ARP (Address Resolution Protocol)
Protocol that maps a dynamic IP address to a physical machine's permanent MAC address in a local area network (LAN)

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

CDP (Cisco Discovery Protocol)
Protocol used by Cisco devices to allow neighboring networking devices to learn about each other

CIDR (Classless Inter-Domain Routing)
An IP addressing method that improves the efficiency of allocating IP addresses

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

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

DHCP (Dynamic Host Configuration Protocol)
Network management protocol used to automatically assign IP addresses and other communication parameters to devices on an Internet protocol network

DNS (Domain Name System)
A 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

Endpoint
An entity (device, service, node, etc.) at the end of a network communication channel

Encapsulated Remote SPAN (ERSPAN)
Encapsulates mirrored traffic in GRE (Generic Routing Encapsulation) and sends it over Layer 3 networks

ESX (Elastic Sky X)
A pre-configured, ready-to-deploy virtual machine (VM) designed to run on VMware ESX or ESXi

Exporter
A networked device such as a router, switch, or server that generates data and sends it to the flow collector device

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

FQDN (Fully Qualified Domain Name)
The complete address of a computer, host, or any other entity on the Internet

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

Hyper-V
A pre-configured, ready-to-deploy virtual machine designed to run on Microsoft Hyper-V, typically packaged in VHD/VHDX format

ICMP (Internet Control Message Protocol)
A protocol used for devices within the network to determine possible network issues

Identity Provider (IdP)
A third-party entity and/or service that stores and manages identities and credentials for use by other websites, applications, or other digital resources

IP address
A unique numerical label assigned to a networked device

IPFIX (Internet Protocol Flow Information Export)
A protocol intended to collect and analyze the flow data from supported network devices

KVM (Kernel-based Virtual Machine)
A pre-configured virtual machine designed to run on KVM hypervisors, packaged in formats like QCOW2 or OVA for easy deployment in Linux-based virtualization environments

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 access and maintain directory services for assets in an Internet protocol network

LLDP (Link Layer Discovery Protocol)
A vendor-neutral protocol used by devices on IEEE 802 networks to advertise their identity, capabilities, and other information

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

MIB (Management Information Base)
A database that stores information used for managing a network

MTTR (Mean Time to Resolution)
The average amount of time between the detection and remediation of a security threat or incident

NDR (Network Detection and Response)
A cybersecurity solution that uses machine learning to detect cyber threats and aid remediation

Network interface
A (physical or software-based) point of connection between a network entity and the rest of the network

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

NID (Network Infrastructure Device)
Any device, such as an access point, router, or switch, that provides the means for entities to communicate with each other over a network

NTP (Network Time Protocol)
A networking protocol used to synchronize device clocks over the Internet

NXDOMAIN (No Existing Domain)
An error message that means that a domain mentioned in the Domain Name System (DNS) query does not exist

Open port
A TCP or UDP port that has been configured to accept packets

OUI (Organizationally Unique Identifier)
A unique 24-bit number in a MAC address that identifies the vendor or the manufacturer of the device

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

PDU (Protocol Data Unit)
An individual unit of information exchanged by entities on a network using the same protocol

PostgreSQL
An open-source relational database management system (RDBMS) that supports both SQL and JSON querying

PXE (Preboot Execution Environment)
A network booting protocol that allows computers to boot from a network rather than a local storage device like a hard drive or USB

RADIUS (Remote Authentication Dial-In User Service)
A client-server AAA (authentication, authorization, accounting) protocol used to manage remote user access to a network

Redundancy
The state of having duplicate or alternative services as backups to allow for continuous availability

REST API (Representational State Transfer Application Programming Interface)
A set of rules that allows systems to communicate over the web using standard HTTP methods

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

Single Sign-On (SSO)
A technology that enables users to access multiple applications with a single set of credentials through third-party authentication services

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)

SNMP (Simple Network Management Protocol)
An IP network protocol used to collect data related to state and/or behavior from devices on a network

SNMP trap
An alert message that is initiated by an SNMP-enabled device to notify the management system of significant events or changes in status

Software agent
A persistent piece of software that performs certain actions and/or interacts with its environment on behalf of a user or another program

SPAN (Switched Port Analyzer)
A dedicated port on a switch that takes a mirrored copy of network traffic from within the switch to be sent to a destination

SSDP (Simple Service Discovery Protocol)
A network protocol used for advertising and discovering network services

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

STIX (Structured Threat Information eXchange)
An industry-standard file format for the exchange of threat information between organizations and platforms

Suricata
A network threat detection engine used to analyze network traffic and identify potential security threats

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

SYN scan
A port scanning technique that allows for the discovery of the status of a communications port without establishing a full connection

Syslog
A cross-platform network logging protocol used to send and/or receive alerts between different devices on a network

TACACS+ (Terminal Access Controller Access-Control System)
A protocol where the remote access server and the authentication server provide validation for users attempting to access the network

TAXII (Trusted Automated eXchange of Indicator Information)
A protocol that allows the transmission of threat information, primarily in STIX format, between systems and organizations

TCP (Transmission Control Protocol)
A connection-oriented protocol that enables the bidirectional exchange of messages between devices on the same network

TLS handshake
The process that starts secure communication between a client and a server

TSIG (Transaction Signature)
A protocol that secures DNS packets and allows a Domain Name System to authenticate updates to the DNS database

TTL (Time To Live)
A field in the IP packet header that specifies the maximum number of hops (or router passes) a packet can take before being discarded

UDP (User Datagram Protocol)
A communication protocol for transmitting messages between applications and programs in a network

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

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

VPC (Virtual Private Cloud)
A secure and private cloud hosted in a public cloud

VRF (Virtual Routing and Forwarding)
A technology that separates routing tables to isolate management traffic to the management interface

Web server banner
A text-based greeting message, which includes information like open ports, services, and version numbers, returned by a web host

4.4.3 Third-party atttributions

Certain open source or other third-party software components are integrated and/or redistributed with FlowPro. The licenses are reproduced here in accordance with their licensing terms.

These terms only apply to the libraries themselves, not the FlowPro software.

4.4.3.1 Suricata

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

4.4.3.2 Golang

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

4.4.3.3 Badger

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

4.4.3.4 ET/Open Emerging Threats Open Ruleset

https://rules.emergingthreats.net/open/
Copyright (c) Proofpoint
Licensed under MIT License

4.4.3.5 Docker

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

4.4.3.6 Gorilla Mux

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