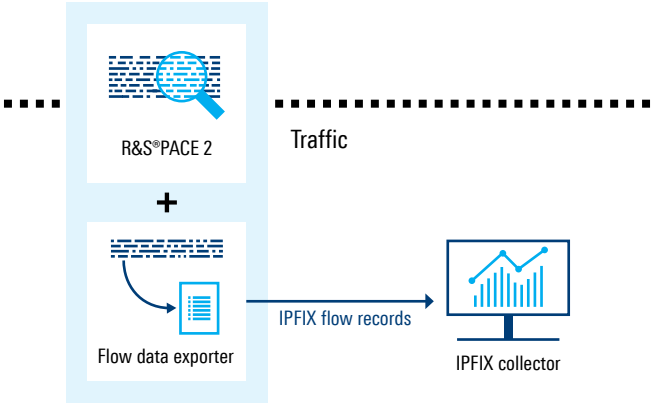
EXPORT IPFIX FLOW DATA RECORDS WITH THE DPI ENGINE R&S®PACE 2

R&S®PACE 2 flow data exporter plug-in

Deliver unparalleled insights into application traffic by augmenting IPFIX flow records with DPI-driven intelligence. Seamlessly bridge and integrate IPFIX and advanced deep packet inspection software analysis into your networking solution with granular insights into IP traffic up to layer 7 and beyond.

IP Flow Information Export (IPFIX) is an open IETF protocol that enables the transmission of IP flow records between network devices within an IP network. IPFIX-enabled devices log layer 3 and layer 4 telemetry information based on packet metadata such as IP addresses, port numbers, byte size, packet count, flow timing and type of service. The IPFIX protocol enables monitoring of traffic via a highly configurable, flexible and extensible mechanism for metering, formatting and exporting IP flow records in multi-vendor environments.



Challenges

A growing number of networks which deploy IPFIX-based monitoring also deploy packet payload filtering technologies such as deep packet inspection (DPI) for real-time, fine-grained traffic awareness. This leads to separate streams of traffic analyses within a single IP network, with a high degree of metering duplication and overlapping traffic records. As traffic volume rises, multiple logging and reporting mechanisms add to network latency and reduce network efficiencies. Network functionalities feeding on both streams experience analysis discrepancies due to different sampling and aggregation methodologies, while devices confined within an IPFIX reporting chain, for example network packet brokers and IP probes, forego access to DPI's advanced traffic insights altogether.

Flow data exporter

The flow data exporter plug-in by ipoque enhances IPFIX monitoring systems with DPI-driven advanced insights and capabilities, while addressing the challenges mentioned above. As an extension to ipoque's market leading DPI engine R&S®PACE 2, the plug-in acts as an intermediary between both systems. For any given IP flow, the flow data exporter plug-in logs all information elements (IE fields) using the internal flow-user-data structure and translates these into IPFIX flow records in the form of IPFIX-encoded messages via the configurable callbacks fn_init, fn_flow_dropped and fn_close. These callbacks can feed into TCP, UDP, SCTP and TLS-encrypted sockets and handle statistics as well as exporting to file handlers, enabling seamless delivery of DPI-based flow records to third-party IPFIX collectors and analyzers.

Plug-in key benefits

- Dedicated templates for IPv4 and IPv6 traffic
- Configurable IPFIX IE fields with various fields per template
- Real-time protocol and application awareness with support for DPI-related IE fields, such as application ID, name, category name, sub-category name, etc.
- Compatible with any IPFIX network
- API documentation and examples references
- Small memory footprint with only 104 bytes per flow
- Export to Netflow v10 (IPFIX)
- Supports input processing of sFlow samples

Enriching IPFIX-based monitoring with DPI capabilities

The flow data exporter plug-in boosts IPFIX-based monitoring with the following DPI capabilities:

- Library with over 6,000 classification signatures
- Encrypted traffic intelligence via machine learning and deep learning analysis
- Single-step plug-in integration using the configuration mechanism of R&S®PACE 2
- Symmetric (lock-free) multi-threading allows for linear scaling up to highest throughput requirements
- Dynamic upgrades during runtime for uninterrupted performance

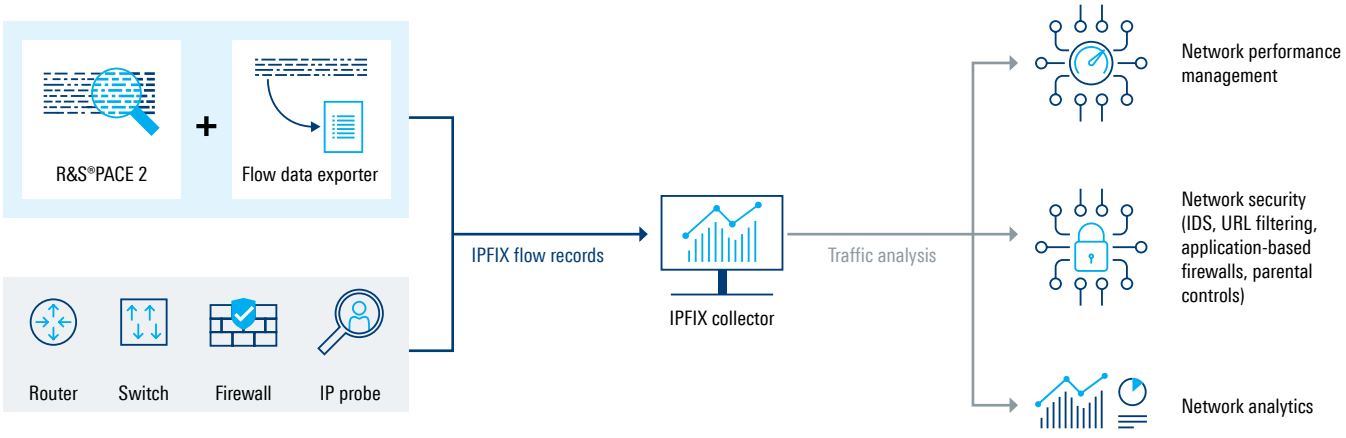
Use cases

The Flow data exporter plug-in removes metering redundancies and optimizes DPI and IPFIX reporting streams. It also enables IPFIX-based flow monitoring to take advantage of DPI's application awareness and higher processing throughput, to support the following use cases:

- **Network performance management (NPM):** NPM tools benefit from faster access to network performance data such as round trip time, speed, latency and jitter, enabling network events such as congestion and bottlenecks to be addressed in real time. Additionally, DPI's application awareness allows for application-aware policies such as compression, caching and premium routing to be executed seamlessly, especially in SDN environments.

- **Security:** DPI's ability to detect flows that are anomalous, malicious and suspicious equips security tools such as application-based firewalls, intrusion detection systems, URL filtering and parental controls with accurate and reliable insights. These insights, combined with IPFIX's flow records such as source/destination addresses and port numbers, allows real-time detection of attacks such as DDoS and malware, even for flows that are encrypted.

- **Analytics:** Granular insights from DPI enable network analytics tools to monitor application usage and user behavior in real time. This complements IPFIX traffic analysis, resulting in enhanced traffic intelligence for planning and policy purposes.



ipoque GmbH
A Rohde&Schwarz Company
Augustusplatz 9, 04109 Leipzig
Info: +49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3683.8296.32 | Version 01.00 | November 2022
Export IPFIX flow data records with the DPI engine R&S®PACE 2
Data without tolerance limits is not binding | Subject to change

3683829632

3683.8296.32 01.00 PDP 1 en