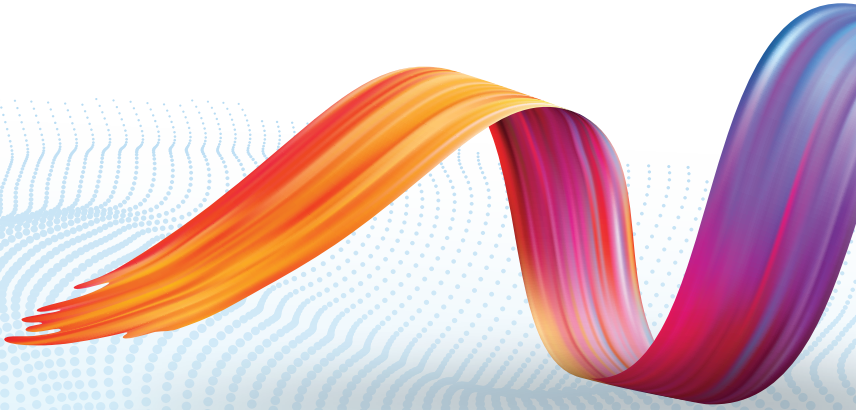
RADCOM

RADCOM Network Visibility



RADCOM Network Visibility is a dynamic, next-generation, network packet brokering solution for telecom operators to collect, process and distribute traffic across multiple domains (physical and virtual) for NFV and 5G networks.

Centrally managed via an easy to use, drag and drop web UI to manage all functionality across multiple clouds with a click of the mouse RADCOM Network Visibility is deployed as a Virtual Network Function (VNF) and orchestrated by NFV MANO platforms such as ONAP, OSM and more.

Each packet broker instance can be grouped and tagged so thousands of packet brokers can be easily managed at scale and reconfigured in minutes. Being cloud-native, RADCOM Network Visibility can be launched as well as scaled up and out on-demand to meet the challenges of collecting and distributing traffic in high capacity, virtual networks.

On-demand, next-generation, network visibility

Key Features:

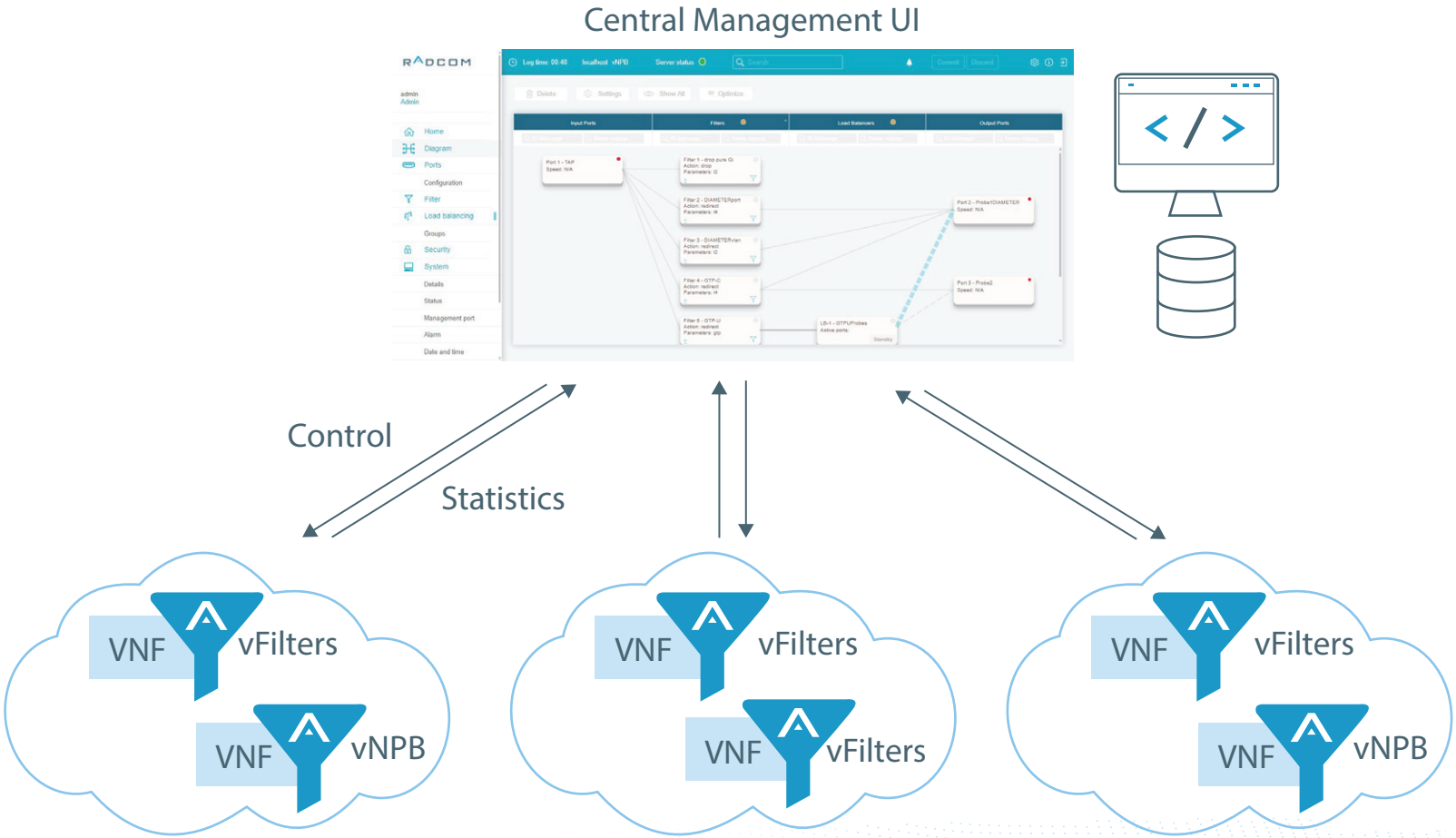
- Cloud-native offering deployed as a VNF that is spun up and down in minutes
- High performance using DPDK-based implementation and packet fetching from vNIC
- Highly scalable with up to 20k filters evaluated simultaneously
- Smart, session-aware load balancing and advanced filtering (by app/service, DPI-based)
- Centrally managed and configured using a friendly web UI for drag and drop control
- Flow analysis for network troubleshooting using IPFIX
- Compatible with NFVI/VIM platforms (such as OpenStack, VMware, and others)
- Orchestrated by NFV MANO platforms such as ONAP, OSM and more
- Advanced packet broker functionality such as; aggregation, header stripping, deduplication, data masking, packet slicing, time stamping, capture to disk, de-fragmentation
- Supports a 5G-ready cloud with integration into vMME, vGW, vDRA, and vIMS

RADCOM Network Visibility acquires network traffic using both legacy mirroring and tapping methods for hybrid networks (such as vSwitch port mirroring, and Top of Rack/End of Row tapping) as well as next-generation data acquisition methods (such as SR-IOV mirroring, and virtual tapping from within the virtual machine or container).
RADCOM Network Visibility provides comprehensive visibility across both environments and performs the same functionality on all traffic.

After receiving, filtering, sampling, capturing, aggregating, and manipulating network traffic from the switching layer (or close to the monitored VNF), RADCOM Network Visibility load balances and forwards traffic to analytics, monitoring, and security tools. RADCOM's visibility layer delivers full network visibility into east-west traffic, makes monitoring and security tools more effective, and ensures session-aware traffic is delivered to assurance probes for comprehensive customer experience insights. With the on-demand capabilities operators can smartly filter, sample, analyze and troubleshoot on the fly to dynamically optimize network performance and ensure service quality.

RADCOM's solution is fully integrated with NFVI/VIM platforms such as OpenStack and VMWare and orchestrated by NFV MANO platforms such as ONAP and OSM so operators can automatically deploy, manage and scale the visibility layer. With a distributed and highly scalable microservices architecture that meets cloud performance requirements and is highly efficient with limited cloud resources, RADCOM Network Visibility is built for tight integration into a 5G-ready cloud.

RADCOM Network Visibility is a stand-alone network packet broker solution for telecom operators looking for a cost-effective and cloud-native alternative to replace old, legacy packet brokering solutions that lack visibility into east-west traffic, are not cost-effective and lack on-demand capabilities and automation. RADCOM Network Visibility can also be deployed together with RADCOM Service Assurance and RADCOM Network Insights to provide telecom operators an automated, all in one solution for network tapping, assurance probing and customer/service experience management insights.



Dynamic, cloud-native components centrally managed across multiple clouds

vTap

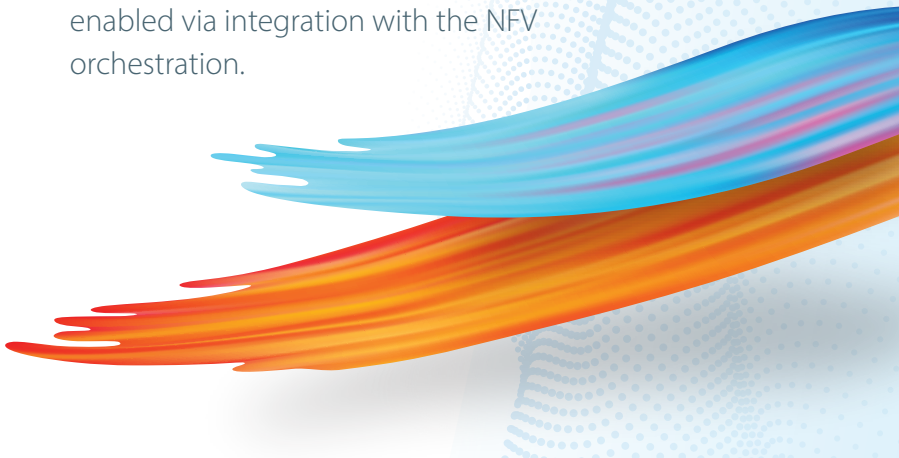
For efficient traffic acquisition in virtual networks, RADCOM deploys lightweight virtual Taps (vTaps) to acquire east-west VNF traffic from virtual machines and containers. vTaps are co-located with the monitored VNF to tap traffic while logically bypassing tapping on the vSwitch. As well as extracting traffic vTaps filter traffic before forwarding to the network packet broker layer which aggregates, samples, and load-balances the captured traffic and then sends to assurance probes or security tools. By filtering at the tapping point, vTaps save network resources. vTaps support both Linux kernel or DPDK based VNFs and can be deployed by injection during onboarding of the VNF or incorporated into the VNF's base-image as part of the standard monitoring tool package.

vFilter

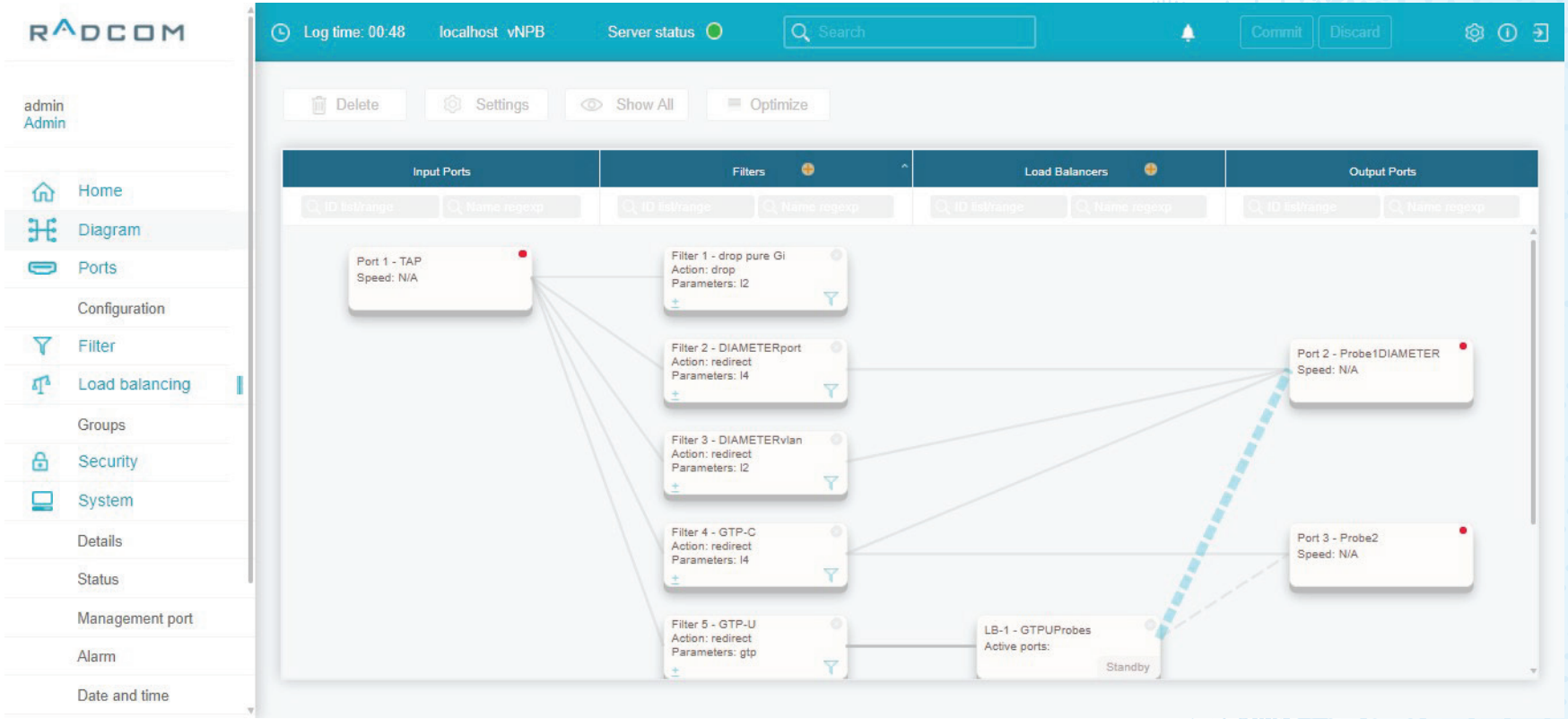
In single or multi-cloud environments traffic is distributed across many regions and multiple virtual machines or containers. RADCOM's vFilter provides operators with traffic aggregation, filtering and distribution capabilities across multiple networks. vFilter is a lightweight network packet broker with basic functionality for filtering and load balancing of traffic at scale. The vFilter can reside inside or outside the monitored VM environment/container to receive the replicated east-west traffic. vFilter then forwards the replicated traffic to the vNPBs, or directly to monitoring or security tools, through GRE or VXLAN tunnels. Central management of the distributed vFilters enables operators to dynamically deploy and configure an end-to-end network visibility layer across multiple clouds on-demand. Automation of the solution instantiation and scaling is enabled via integration with the NFV orchestration.

vNPB

vNPB (Virtual Network Packet Broker) is a fully-fledged network packet broker with advanced features like session-awareness, filters and actions (like smart load balancing, SSL decryption and capture to disk of certain IMSIs, packet duplication), as well as traffic sampling (like NetFlow, flow-based, subscriber-based sampling). The vNPB can reside inside or outside the monitored VM environment/container (depending on the resources) to receive the replicated east-west traffic. It then forwards the replicated traffic to monitoring or security tools, through GRE or VXLAN tunnels. Central management of the distributed vNPBs enables operators to dynamically deploy and configure an end-to-end network visibility layer across multiple clouds on-demand. Automation of the solution instantiation and scaling is enabled via integration with the NFV orchestration.



Central Management



Both the vFilters and vNPB are managed via a central management web UI in which operators can control thousands of vNPBs or vFilters instances across multiple clouds through a web UI. The management web UI allows users to dynamically modify flow definitions and traffic optimization functions via a simple drag and drop UI so that just by dragging a line between elements a user can configure filters and actions. With packet and flow-level access into all parts of the network and across multiple domains, operators can efficiently steer traffic to monitoring and security tools based on set rules and policies.

Management at scale

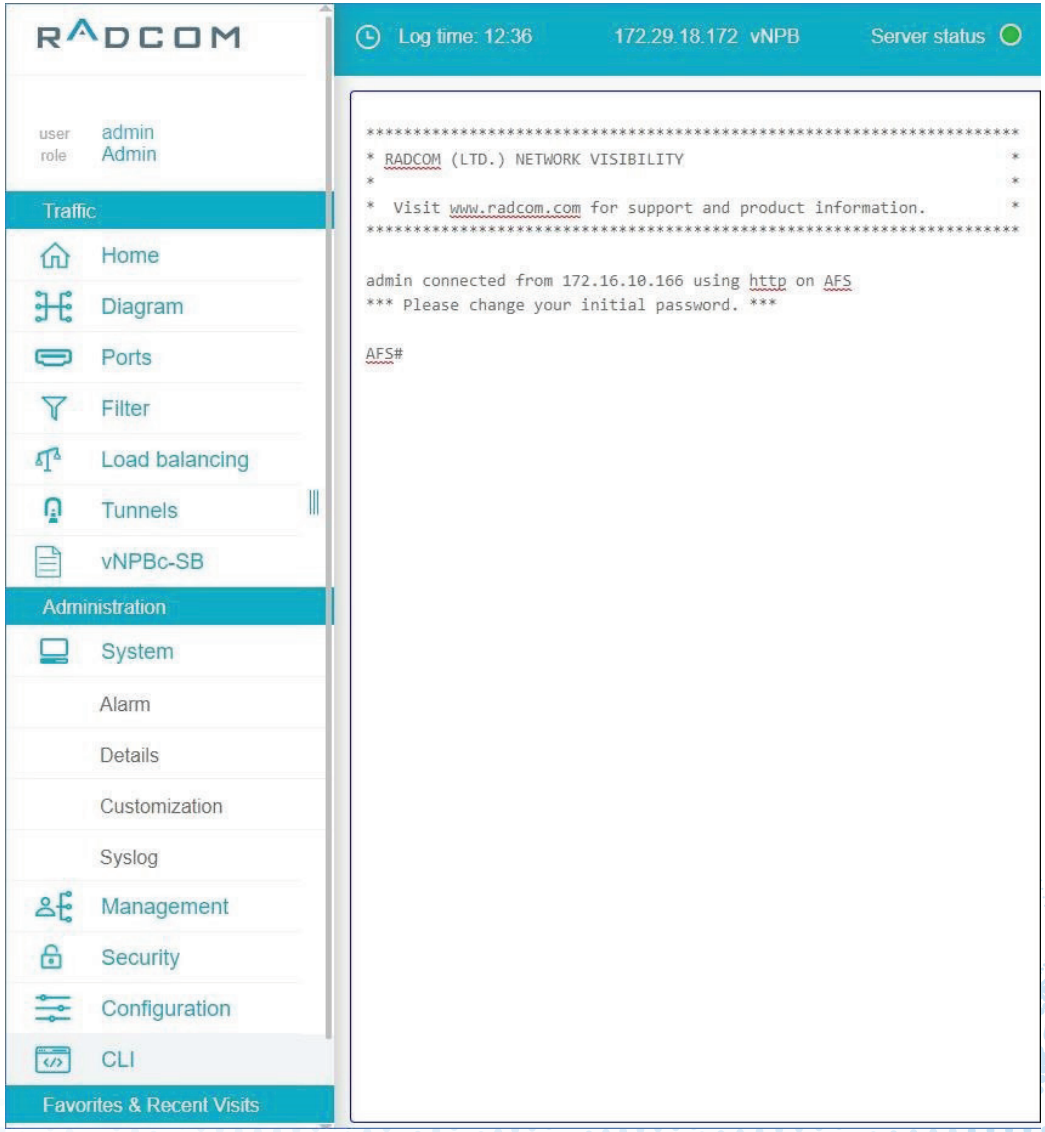


Figure 1 – RADCOM's Web UI contains an embedded CLI connection

Rules and configurations can be defined once and then automatically pushed to multiple vNPBs or vFilters in an instant. This is achieved by managing groups of vFilters and vNPBs based on logical grouping and labeling. The operator can then manage the entire RADCOM Network Visibility layer (incl. performance analytics and alarms) for large-scale network deployments and management. Management at scale lets operators define/edit user specific rules as well as a common set of rules for a vFilter and vNPB group, distribute the defined rule configuration and view reports showing the progress of the distribution and activation of these new rules.

In addition to the web UI, RADCOM Network Visibility can also be managed via a Command-line Interface (CLI), NETCONF/YANG, REST API, Simple Network Management Protocol (SNMP), Network Access Control List (ACL) and scripts. Having flexible, central management enables operators to gain end-to-end network visibility with unmatched simplicity, unrivaled cost-efficiency, and unlimited scalability.

RADCOM's Network Visibility solution offers operators advanced packet brokering functionality that can be installed on-demand allowing the operator to deploy the solution on-the-fly, filter traffic and troubleshoot efficiently.

Advanced filtering

Smart traffic filtering allows the operator to filter out or zoom in on specific traffic according to a wide set of criteria. Traffic matching the criteria can be either redirected or dropped. So, for example, if the operator wants to include or exclude traffic from specific applications, it's easy to set up via the web UI.

The operator can filter video streaming data from YouTube to a monitoring or analytics tool. This can be taken a step further by utilizing DPI-based filtering and filtering out different types of data types within an application. RADCOM Network Visibility provides the following smart filtering functionality;

- App-based filtering (Skype, YouTube, etc.)
- IMSI/MSISDN-based filtering
- DPI-based filtering (for example, forward encrypted video to target X and not target Y)
- Regular expressions with just a string (without a HEX offset)
- NOT functionality with all fields allowing data to be included or excluded
- Additional logical operations (e.g., and, etc.)
- Filtering by L2, L3 and L4 classifiers
- IP lists
- Provides statistics per filter
- Copy/forward packets for further processing

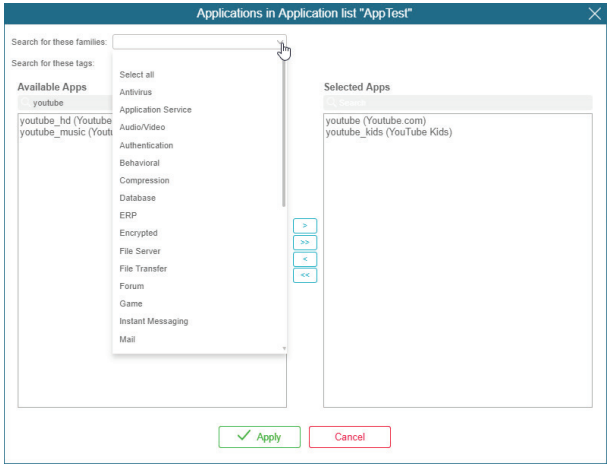
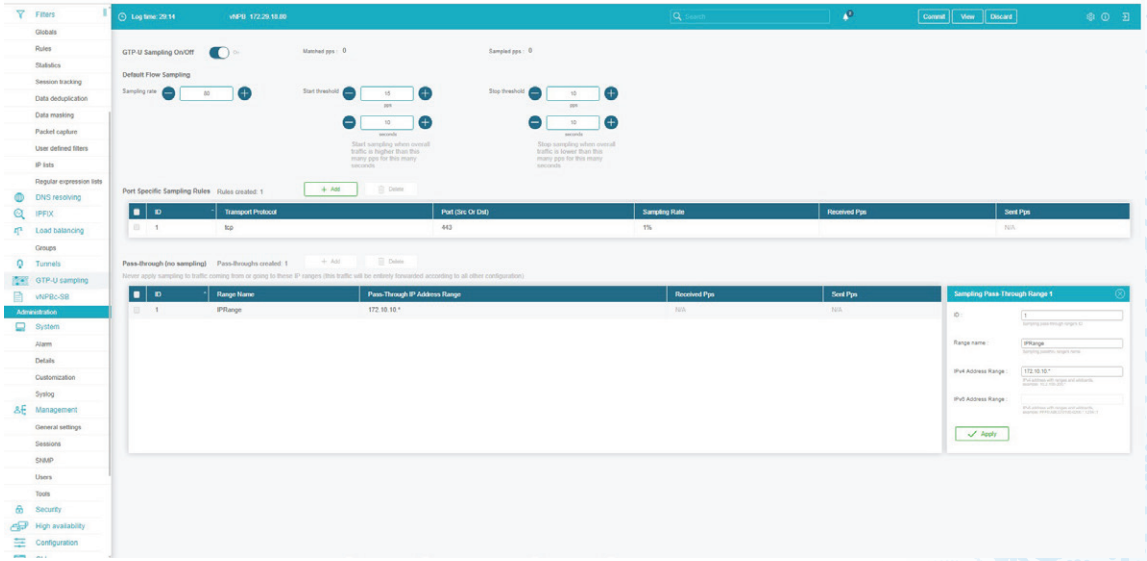


Figure 2 - DPI-based filtering options organized by categories (audio/video etc.)

Advanced functionality for smart filtering, intelligence traffic sampling, and session-aware load balancing

Intelligent traffic sampling

RADCOM Network Visibility enables traffic sampling in which only a specified amount of traffic (randomly sampled) is passed through the network packet broker to the monitoring and security tools. The rest of the traffic is dropped. Traffic sampling can be flow or subscriber based with sampling algorithms randomly selecting a group of sessions and forwarding only packets that belong to these sessions. Operators can configure the network packet brokers to preserve sessions of either 5-tuple flows or subscribers (MSIP/IMSI/MSISDN). If the overall traffic is higher/lower than expected, the algorithm will reduce/add sessions accordingly.



Session-aware load-balancing

In virtual networks, session-aware load balancing is an essential function for operators to assure the customer experience and troubleshoot network performance proficiently. In top-tier virtual networks, a single network element often needs to be covered by multiple probes to handle the traffic. Thus, to maintain subscriber session integrity operators, need session-aware load-balancing to evenly distribute traffic across multiple probes while delivering multiple protocols related to the same user/session to the same probe and enabling correlation of the whole session. Combined with smart filtering and traffic sampling, unwanted data can be dropped or routed to different tools allowing operators to focus on critical issues that affect the customer experience. Once defined, load balancing groups can act as filter outputs, causing matched traffic to be distributed between its members.

RADCOM Network Visibility supports load-balancing for GTP as well as vMME, vSGW, vDRA vIMS, and scales horizontally and vertically.

RADCOM Network Visibility enables operators to monitor and troubleshoot the network more efficiently by moving some of this functionality from the service assurance layer to the visibility layer, closer to the tapping point. Helping speed up network problem isolation, reduce resolution times and more effectively manage human and network resources.

An operator can decide on the fly what they want to analyze, filter the traffic, capture to disk and then perform on-demand troubleshooting — even streaming this data to RADCOM's packet-based, protocol analyzer - QAnalyzer - to view any packet flowing through the network for any selected subscriber or period. This data can also be exported as a full user-plane PCAP trace for even more in-depth troubleshooting.
Moving specific troubleshooting functions to the visibility layer and enabling on-demand troubleshooting means that operators can collect statistics from across the entire network and then when problems arise zoom in on selected subscribers, network elements or traffic sets based on app or service usage for further analysis.

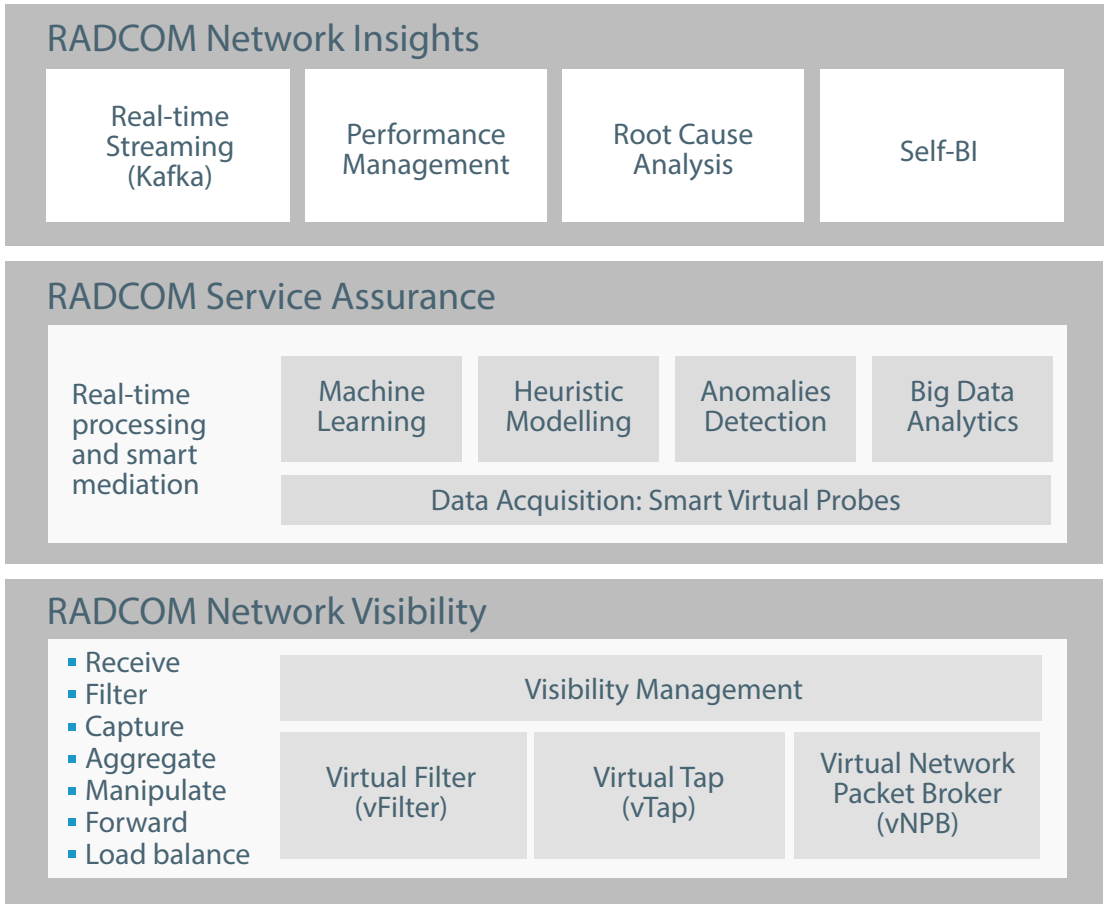
This approach enables a more rapid way to troubleshoot network issues and provides a disruptive, new method to network packet brokering that facilitates dynamic evaluation of network issues and provides the operator with actionable network insights more quickly and efficiently. RADCOM's intelligent virtual network packet brokers (vNPBs), come with enhanced user plane analysis letting operators apply application filtering and routing. For example, to identify SSL traffic and gain network insights without unnecessarily sending it to the service assurance solution. Or, by sending specific traffic types, like SIP to particular probes or by dropping entire sets of data to prevent unnecessary network utilization for unneeded traffic. RADCOM's vNPBs can provide operators the following data:

- NetFlow: Generate NetFlow records along with additional context-aware extensions like URLs from traffic fed to the visibility platform
- Stateless 'Netflow' counters
- Stateful correlated subscriber flow based CDRs

Efficient troubleshooting close to the tapping point

RADCOM Network Visibility can be deployed as a stand-alone network visibility solution. However, operators gain many benefits by deploying the entire RADCOM Network Intelligence solution that adds a cloud-native service assurance and network insights solution on top of the network visibility layer. With this end-to-end solution, operators can smartly aggregate and intelligently load balance network traffic while efficiently gaining real-time customer and service insights to assure the customer experience and optimize their end-to-end network services.

Designed from the ground up for automation, scalability, and integration into NFV orchestration as operators transition to a 5G-ready cloud RADCOM Network Intelligence provides an intelligent and cost-effective solution that scales for operators migrating to high-capacity networks such as NFV and 5G.



Fully Automated Network Visibility, Service Assurance, as well as Customer and Service Experience Insights

RADCOM's solution is built for operators transitioning to a 5G-ready cloud and delivers the following advanced network packet broker features and benefits:

	Feature	Benefit
Session Awareness TCP/UDP Flow Aware	**Session Aware (Mobile, Fixed and Voice)**	For example, when deployed on mobile networks operators can correlate between the Gi and Gn and thus report, filter and invoke actions based on the subscriber ID (IMSI, IEMI, etc.)
	Application Session Aware	▪ Classify the application per-flow using the built-in DPI engine ▪ Export application name + additional metadata per flow or aggregated ▪ Filter monitored traffic by application and invoke actions
Filters and Actions	**Smart Load Balancing**	Traffic can be distributed to a cluster of monitoring tools probes while ensuring all packets from a specific mobile subscriber, flow or IP address are forwarded to the same probe to provide correct customer experience analysis
	Intelligent Filtering	Filters out unwanted traffic from reaching the monitoring tools, so only traffic of interest is processed and analyzed
	Packet Manipulation	Advanced packet manipulation tools, such as packet deduplication, IP defragmentation, masking of sensitive data, slicing the packet payload, time-stamping, header-stripping, port-labeling
	Tunneling/IPSec	Receive traffic encapsulated in many types of tunnels and decapsulate/decrypt it before processing; Encapsulate/encrypt packets when forwarding packets to a monitoring tool over a tunnel
	SSL Decryption	Performs SSL decryption to gain more visibility into the network traffic
	Capture to Disk	Save packet headers and payload on disk for future analysis, and index that data for quick access and search

Features and Benefits

	Feature	Benefit
Traffic Sampling	Sampling (sFlow)	Send only a fraction of the overall packets to any monitoring tools that can work with statistical data
	NetFlow	Export flow information to any NetFlow (IPFix) collector
	Flow-based sampling	Reduce overall traffic forwarded to a bandwidth-limited monitoring tool, by automatically selecting a sub-group of flows and forwarding only traffic that belongs to this group
	Subscriber-based sampling	Reduce overall traffic forwarded to a bandwidth-limited monitoring probe, by automatically selecting a sub-group of subscribers and forwarding only traffic that belongs to this group
Management	Easy-to-use, drag, and drop web UI for control of all functionality across multiple clouds	Unified, central management for rapid deployment, configuration, control, and traffic flow optimization Additional management control; Command-line Interface (CLI), NETCONF/YANG, Simple Network Management Protocol (SNMP), Network Access Control List (ACL)
Central Management	Central Management Server	Configuration and health management (incl. performance analytics and alarms) of up to tens of thousands of vNPB instances
	Central Management web UI	Configure filter rules once and apply to a group of vNPB instances
NFV Integration	Compatible with NFVI/VIM platforms	Enables RADCOM Network Visibility to be deployed, configured and managed as a VNF on NFV platforms such as OpenStack, VMware, and others
	Compatible with NFV Orchestration	RADCOM Network Visibility is orchestrated by NFV MANO platforms such as ONAP, OSM and more

Use Cases

RADCOM Network Visibility empowers operators with the ability to capture, aggregate and manipulate network traffic from multiple clouds and enables more efficient usage of monitoring and network security tools for numerous use cases such as:

Use Case	Usage
Network Forensics and Analytics	▪ Direct traffic to the right tools (for example, video and VoLTE traffic to be analyzed in different tools) ▪ Leverage NetFlow and other flow standards (sFlow) for network behavior analysis to get a baseline reading on regular network traffic and detect anomalies such as malware propagation ▪ Monitor, record, and analyze network traffic for regulatory purposes or to collect legal evidence ▫ Deep packet inspection extracts network traffic about specific IP, MAC, and e-mail addresses; and more ▫ Data like credit card information must be protected and not exposed to unauthorized individuals. ▫ Data masking makes the data compliant and monitoring activities safe
Security	▪ Eliminate packet duplicates to keep security tools from wasting processing capacity handling redundant data ▪ Mask sensitive information such as credit card or Social Security numbers before passing it on to other monitoring tools and their administrators ▪ With Netflow data gain visibility into traffic types and usage patterns, to catch denial of service attacks, data extraction, and other events that represent security risks
Service Assurance	▪ Optimize network traffic flow to service assurance probes ▫ Filter unnecessary traffic to reduce overload ▫ Session-aware load-balancing to distribute traffic across multiple probes ▫ Traffic sampling of a specified amount of flows or subscriber data ▪ Facilitate on-demand troubleshooting ▫ Filter only relevant traffic to the issue being investigated ▫ Forward filtered data to a central checkpoint, or capture data close to the source for later inspection ▫ Detect root cause with advanced application intelligence ▫ Troubleshoot network outages and performance degradations ▫ Speed up network problem isolation with built-in protocol analysis

Summary

RADCOM Network Visibility is explicitly designed for telecom operators transitioning to a dynamic, next-generation 5G-ready cloud network. RADCOM offers operators an integrated cloud-native solution that ensures intelligent traffic distribution, smart, session-aware load balancing, and full end-to-end visibility across virtual networks and advanced packet brokering capabilities. RADCOM Network Visibility is cost-effective and deployed as a VNF, so dynamically deployed and scales efficiently with an NFV distributed approach to high scale packet brokering at scale.

For more information on virtual network visibility, visit **www.radcom.com**

Visit our website: **www.radcom.com**