DEEP PACKET INSPECTION

Solution Guide

R&S®PACE 2

OEM DEEP PACKET INSPECTION SOFTWARE

ROHDE&SCHWARZ

Make ideas real

CONTENT

1. INTRODUCTION

Over the past years, the volume of internet traffic, the number of endpoints and the complexity of protocols have been increasing exponentially. Big data requirements are emerging with bandwidth-demanding applications and activities. Expanding technologies such as cloud computing, 5G, the internet of Things (IoT), the industrial internet of Things (IIoT) and widespread encryption are introducing new risks and opportunities that significantly challenge IT professionals. This applies especially to manufacturers of network products and solutions working in the areas of cybersecurity and telecommunications. To secure, maintain and shape future networks, they need to find ways to make network traffic visible and provide insights into application and protocol usage. The challenges they face in achieving traffic visibility include:

- High development costs in an increasingly competitive market
- High performance requirements due to data and application growth
- High efficiency requirements due to cost-sensitive environments and virtualization
- The need for accurate traffic visibility in real time due to more and more dynamic and individual services
- The need for deeper insights into network traffic in order to trace and identify sophisticated attacks
- Thorough coverage of applications and protocols despite their frequent changes
- Widespread encryption and obfuscation

To face these challenges, solutions that provide visibility of IP-based networks must meet the following criteria:

- Be accurate and reliable while classifying a very high percentage of network traffic at any time
- Cover a broad portfolio of network protocols and applications to classify any kind of traffic reliably
- Be up-to-date and frequently align with changes in applications and protocols
- Be easy to use and maintain with low maintenance costs

By embedding R&S®PACE 2, the deep packet inspection (DPI) engine by Rohde&Schwarz, in their solutions, vendors of network equipment and software get the real-time traffic visibility they need and can enhance their products with state-of-the-art protocol and application awareness capabilities. The software library uses advanced DPI techniques, including behavioral and statistical analysis, to classify network protocols and applications reliably, even in case of encrypted traffic. With weekly signature updates, the signature portfolio is always up-to-date. By licensing the market-leading DPI engine R&S®PACE 2, vendors can concentrate on their core competencies and significantly save on development and maintenance costs.

R&S®PACE 2 FAST FACTS	
CPU architectures	Any hardware with a C compiler: 32-bit and 64-bit x86, MIPS, ARM v7 and v8, Power PC, Cavium, etc.
Operating systems	Unix-based operating systems (Support for kernel and user space)
Performance	14 Gbps throughput per core, on average
Metadata extraction	Yes
Service and support	Individual SLAs Dedicated consulting engineers
Memory footprint	Library: No memory for initialization, 446 bytes per flow 649 bytes per endpoint
Written in	C
APIs	C public headers (events) Supports JSON serialization

2. LICENSING R&S®PACE 2 AS OEM

2.1 DPI as a service

Developing a DPI solution in-house takes a lot of time. R&S®PACE 2 instantaneously provides classification of a market-leading classification portfolio covering different regions, areas and verticals. Additionally, the costs of developing and maintaining solutions in-house are hard to estimate in advance while the licensing costs for R&S®PACE 2 are predictable and fixed.

Open source software, on the other hand, is free at first glance, but in-house developers still need to learn about the software and how to customize it. Oftentimes, this requires collaboration with third-party vendors to manage and add new features. Licensing DPI software with dedicated experts that add new signatures every week to a library that can be updated during runtime ensures that the DPI solution works reliably at any time. This is vital for vendors who make informed decisions based on reliable traffic classification. R&S®PACE 2, customized and deployed on-site by leading experts, reduces the costs and risks associated with internally developing and maintaining a highly complex technology.

2.2 Integration

With open APIs, integration examples and superior service and support, R&S®PACE 2 can be easily embedded in any solution – developed in-house or by third parties – and enhance it with real-time traffic visibility. R&S®PACE 2 is platform-agnostic (supporting x86, ARM, Cavium Octeon, Power PC, etc.) and runs on Unix operating systems, such as Linux, Mac, FreeBSD, etc., using a C interface.

Designed by developers with many years of experience in layer-7 awareness and continuously refined by feedback from customers around the globe, R&S®PACE 2 boosts an array of solutions in the areas of:

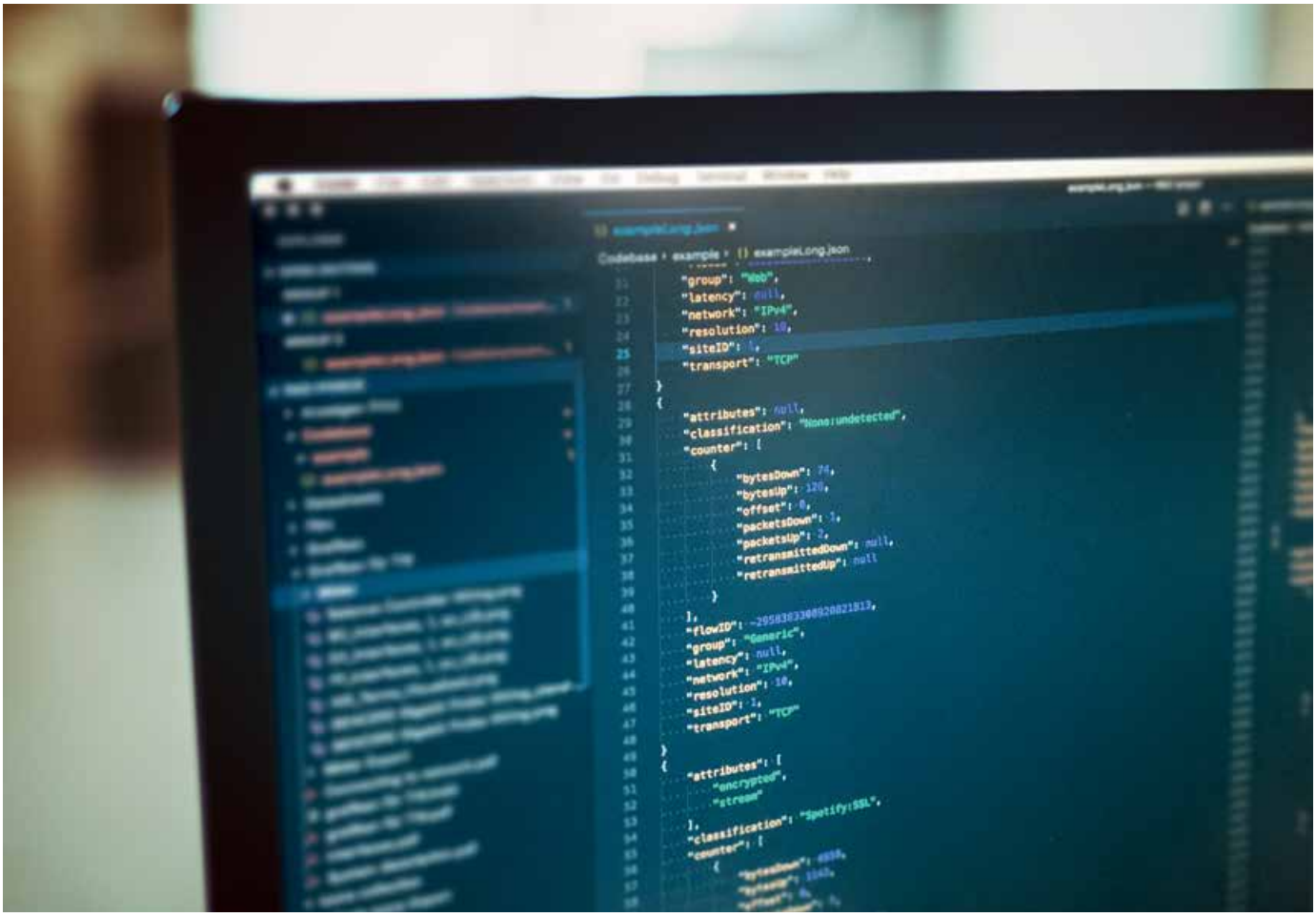
- Cybersecurity (IDS/IPS, next-generation firewalls, SIEM, etc.)
- Enterprise networks (SD-WAN, WAP, etc.)
- Telecommunications (vEPC, service assurance, etc.)

2.3 Key benefits of licensing R&S®PACE 2

- Time-to-market and cost savings – reduce development time and capex/opex by licensing R&S®PACE 2 software including updates and maintenance
- Easy and fast integration – highly flexible API for integration, platform-agnostic software, no external dependencies
- Superior service and support – adaptable to individual needs with designated support engineers
- Fast performance and linear scalability – throughput of 14 Gbps per core, on average
- High efficiency – most efficient memory usage and easiest CPU integration on the market
- Accuracy and reliability – classifies over 95 % of network traffic (no false positives) with a time resolution down to nanoseconds
- Coverage – real-time classification of protocols and applications for all verticals and regions across diverse operating systems, application versions and service types
- Metadata extraction – detailed insights into application-centric statistics for QoS/QoE, for example KPIs on network performance for applications such as VoIP and video streaming
- Always up-to-date – weekly signature updates, including additions to the classification library
- Encrypted traffic intelligence – reliable application classification despite encryption and obfuscation
- NAT transparency – detection of devices behind routers using network address translation (NAT), including smartphones using mobile tethering
- No downtimes thanks to dynamic upgrades
- Future-proof – prepared for network automation and optimized to run in virtual environments (supports KVM, VMware, Hyper-V and Xen)

Licensing R&S®PACE 2, customized and deployed on-site by leading experts, reduces the costs and risks associated with internally developing and maintaining a highly complex technology.

3. ARCHITECTURE



R&S®PACE 2 combines classification and metadata extraction of IP traffic and the related packet processing components in a unified library. A single, C-based API and a command-line interface facilitate integration, in a basic version using 400 lines of code, requiring only a couple of hours.

Flexibility

R&S®PACE 2 has no external dependencies, no memory allocation and is hardware-agnostic. Any hardware acceleration and packet processing framework such as DPDK, VPP, Napatech, etc. can easily be integrated. Thanks to dynamic upgrade techniques, weekly signature updates are installed smoothly during runtime. Market-leading performance values and the many ways to optimize performance make R&S®PACE 2 compatible with setups that require ambitious traffic throughput. Through its configurable event system, R&S®PACE 2 outputs information such as classification and metadata extraction results, processing states and errors. For example, reducing the number of thrown events or defining groups of events helps to optimize the performance and to adapt results to specific use cases. External applications can process the event lists output by R&S®PACE 2 without other dependencies, allowing for high flexibility.

Scalability

R&S®PACE 2 uses a shared-state system that allows to distribute all packets belonging to the same flow to the same worker. Distinct components, such as inter-process correlation (for setups with multiflow decoders) and an inherent symmetric multiprocessing capability, empower leading-edge classification and decoding results and almost linear scalability in multithreading setups.

3.1 Stages

The pipeline architecture of R&S®PACE 2 divides processing of a single frame into subsequent stages. Each stage can be configured to adapt easily to different setups and requirements. Depending on the setup, the activation of a stage can increase the classification results. Our support team gladly helps to find the best, individual solution for each given setup. Throwing events in an early stage, packets can be dropped to enhance performance. Some stage components, such as packet reordering or defragmentation, can be enabled or disabled without code changes to optimize performance and classification results.

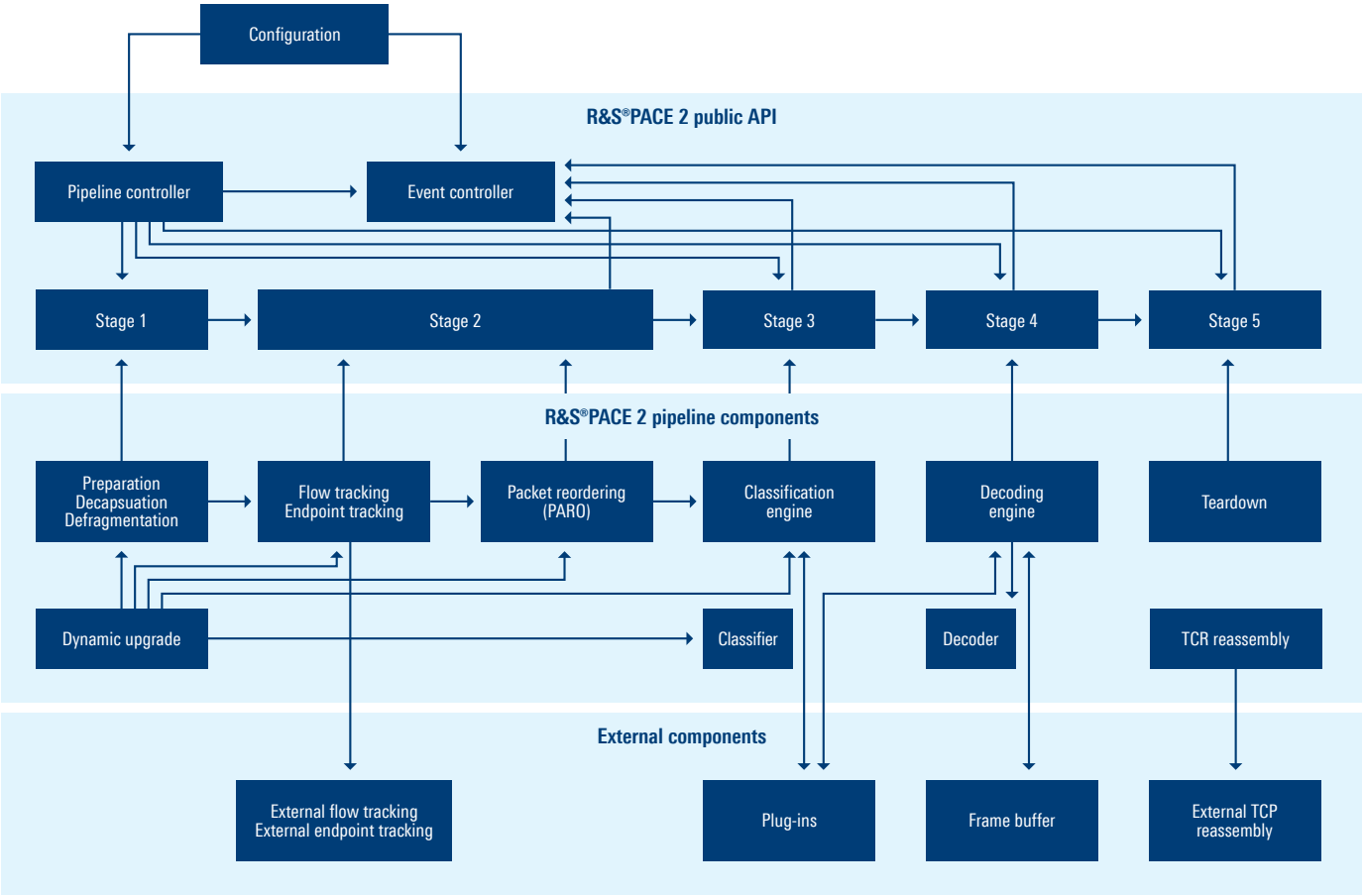
Stage 1: Decapsulation and defragmentation (optional)
Stage 1 is the packet preparation stage. This stage includes decapsulation and defragmentation functionalities. R&S®PACE 2 supports all commonly used tunnel protocol formats and all their possible combinations. Decapsulation covers all GTP versions as well as scenarios with multiple tunnels, such as IP in IP. IP defragmentation reassembles IP packets from layer 3 to layer 7. Transforming the IP flow is key for better classification results.

Stage 2: Packet reordering (optional)
The optional packet reordering stage buffers out-of-order packets until the missing packets arrive or up to a specific timeout. Packet reordering eliminates out-of-order sequences in a flow and can improve classification results.

Stage 3: Classification and basic metadata extraction
In stage 3, R&S®PACE 2 classifies protocols and applications, and extracts basic metadata for certain protocols using dissectors (for example HTTP, IP, TCP, H.264, SIP). Additionally, statistical metadata allow to determine key performance indicators (KPI) for network traffic. KPIs include jitter, packet loss, round-trip time, server response time, etc. For RTP traffic, statistical metadata help to measure performance to determine quality of service (QoS) and quality of experience (QoE) metrics in multiple use cases.

With subsequent processing stages, R&S®PACE 2 can be configured to adapt easily to different setups and requirements.

ARCHITECTURE OVERVIEW



Stage 4: Advanced metadata extraction (optional)
In stage 4, R&S®PACE 2 decodes network traffic to provide advanced metadata in real time. This intelligence empowers a wide array of use cases, such as application performance management (APM), network performance management (NPM), policy enforcement, network security and many others. Advanced metadata from IP traffic extraction includes but is not limited to:

- Identifiers: email sender/receiver addresses or any other ID that can be used to implement strong security rules
- Usage: HTTP, URL or client software information for intelligent traffic decisions and customer experience management
- DNS: detecting tunneling and identifying anomalies in DNS transactions for security and policy enforcement use cases

Advanced decoding options suit the requirements of different use cases and help to optimize the performance with regard to the decoding results. Decoding options include:

- Decoding interrupted flows in lower-quality networks
- A frame buffer interface for subsequent UDP decoding of complete flows if the required classification and correlation results are delayed
- Reassembling missing TCP payload segments of not yet processed packets with configurable timeouts

In addition, the configurable level of detail for the event output allows to adapt to individual requirements: For example, this can help to restrict decoding to HTTP payload and reconstruct all images or videos from internet sites.

Class decoders and context-based decoders
Internal aggregators gather decoding information from multiple decoders and bundle their information into contexts. For example, even if an email connection takes a long time, the full session information still provides all of the data in one place. Class decoders aggregate low-level protocol decoding results, for example POP, SMTP and IMAP, to create an abstract representation, for example "email". Context-based decoders (see section 3.2.2) process raw traffic data or the output of other decoders to provide a sequence of events arranged according to a hierarchical data model.

Decoding is especially useful in network security, for example for reconstructing PDF files in a sandbox environment or gathering upload and download statistics to detect data breaches. This way, next-generation firewalls can prevent data leakage, run deep security scans and control network access.

Stage 5: Timeout handling
The timeout handling stage creates timeout events from decoders and frees unused resources, thereby helping to optimize memory usage. This stage can also support buffered packets from stage 2.

3.2 Plug-ins

In addition to the core functionality, optional plug-ins adapt R&S®PACE 2 to a given use case. Plug-ins reflect changing demands and new technologies in the industry and allow customers to adjust to new challenges. The plug-in portfolio is extended regularly.

3.2.1 NAT/mobile tethering transparency

With network address translation (NAT), multiple network devices with distinct private IP addresses masquerade as a single public IP address. This can lead to misusing network resources. By combining multiple heuristic methods, for example leveraging the Google QUIC user agent, TTL and TCP timestamp, the NAT/mobile tethering transparency plug-in reliably detects devices behind NAT. The plug-in presents gathered data with a well-defined data structure, including a NAT detection state, information on main devices, the number of detected devices and device groups. With this data, enterprise IT departments can prevent cyberattacks and operators can uncover tethering fraud or charge optional tethering plans.

> By combining multiple heuristic methods, the NAT/mobile tethering transparency plug-in reliably detects devices behind NAT.

3.2.2 Context-based decoders

Context-based decoders are an optional complement to stage 4. Their hierarchical data model presents results in a standardized form in context. This way, relations between different parts of the output become visible. Context-based decoders require data aggregation at the customers' end. Presenting the decoding results in context reveals a coherent picture of the IP communication in focus. Thanks to a straightforward architecture, context-based decoders are easy to integrate and maintain.

3.2.3 Custom decoders

On demand, custom decoders extend the library by leveraging the plug-in architecture. For example, a botnet detection decoder can facilitate IIoT cybersecurity use cases.

4. FEATURES AND CAPABILITIES

4.1 Protocol and application classification

R&S®PACE 2 inspects and analyzes network traffic in real time. DPI-based packet classification is the core of the library and is based on a multitude of signatures that are updated on a weekly basis (see section 4.2). DPI provides granular IP traffic classification including protocols, applications and their service types, such as video, audio, file transfer, etc.

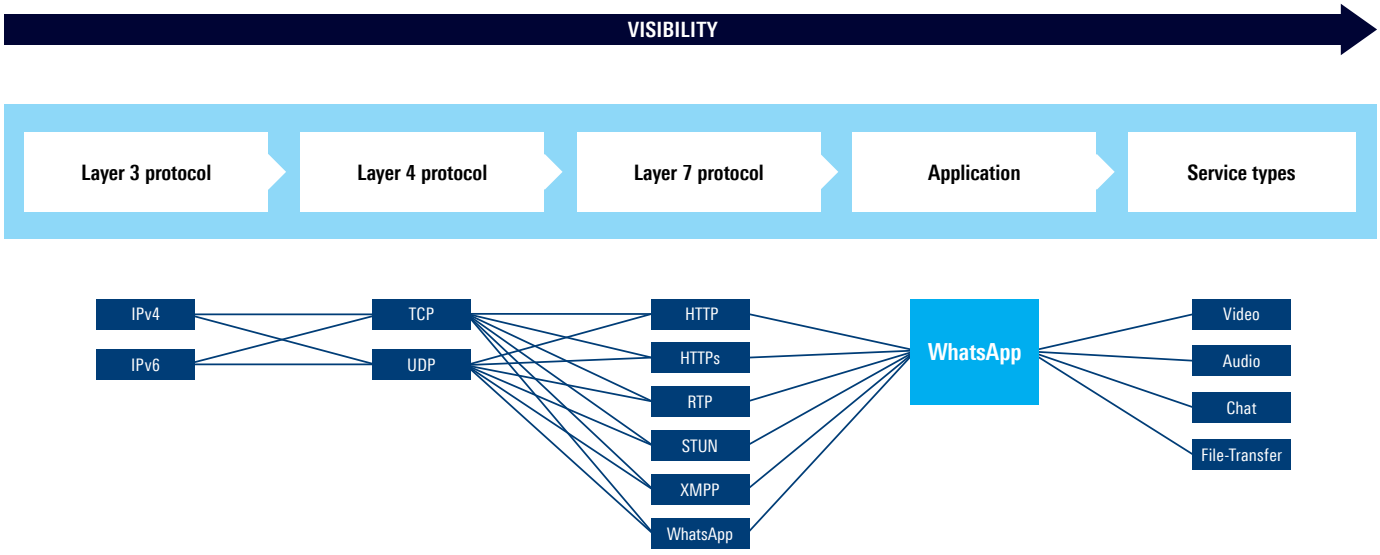
Granular classification results in real time are a prerequisite for a multitude of use cases in the telco and cybersecurity domains. Additional options, features and plug-ins extend the capabilities of R&S®PACE 2 to make it adaptable to any individual solution. For example, in analytics use cases, R&S®PACE 2 can use optional output buffers to serialize events to JSON for visualization. Options to group results, for example “video”, “audio”, “chat”, etc., facilitate data flow analysis and intelligent decisions for traffic management and policy enforcement solutions. To enhance the classification accuracy in case of interrupted sessions in lower-quality networks, R&S®PACE 2 can store SSL sessions with a session ID tracker to correlate flows.

R&S®PACE 2 delivers classification results in a customizable way, adaptable for different use cases.

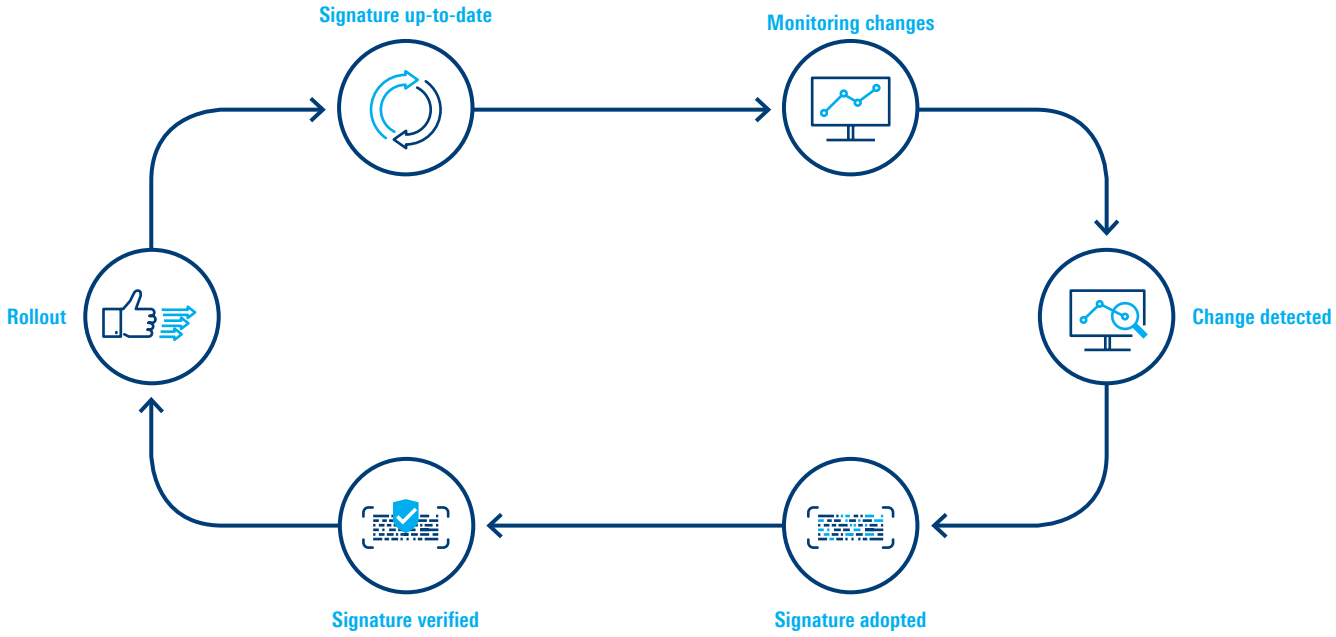
4.2 Classification accuracy

R&S®PACE 2 uses a wide variety of leading-edge techniques to classify network traffic. Thanks to this approach, R&S®PACE 2 can reliably detect network protocols and applications, even if they use advanced obfuscation and encryption techniques (see section 4.3). In many use cases, false positives in the classification results are not acceptable. For example, operators have to rule out false positives in the area of billing as this can have a negative revenue impact and potentially damage the brand image. In cybersecurity use cases, false positives can make a huge difference and enable attacks and data breaches. With sophisticated classification algorithms ruling out false positives, the R&S®PACE 2 signature library proves its worth.

CLASSIFICATION UP TO LAYER 7 AND BEYOND



UP-TO-DATE SIGNATURE UPDATES ON A WEEKLY BASIS



Thanks to the feedback and requirements from customers from different areas and verticals worldwide, R&S®PACE 2 has a very low rate of undetected applications (false negative rate). The application portfolio covers the IT, OT and IoT range and includes numerous business and mobile applications.

New releases of an application, such as new clients or new features, can change its behavior and cause classification problems. This requires constant attention since details for most application changes are not announced publicly. In addition, applications behave differently on different devices, on different operating systems and in different networks. As a result, reliable and accurate application classification does not only require a signature library, but ongoing maintenance and testing, particularly for frequently changing mobile applications. R&S®PACE 2 provides weekly signature updates to maintain a high level of classification accuracy at any time. Automated traffic monitoring and testing and our dedicated team of experts that continuously tests traffic captures for each new version of an application, ensure that the classification library is always up-to-date. With our expertise in network testing at Rohde&Schwarz, we even emulate radio cells to reveal patterns in application behavior, as applications may cause distinct patterns depending on the network characteristics. Consequently, when licensing R&S®PACE 2, our customers adopt a traffic classification solution that is always reliable.

Using leading-edge classification techniques, R&S®PACE 2 can accurately classify around 95 % of network traffic with no false positives.

Growing protocol complexity is mastered with weekly signature updates that lay the foundation for the unrivalled reliability of R&S®PACE 2.

4.3 Encrypted traffic intelligence

An increasing number of protocols and applications are encrypted, for example Skype, WhatsApp, BitTorrent, Facebook, Twitter, Dropbox, Gmail, Office 365 or Instagram. To classify these applications and their service types, R&S®PACE 2 uses a variety of advanced techniques. Checking packet sizes, packet timing, latency, throughput, entropy and jitter provides a lot of information on applications and protocols, even for encrypted flows. Video streams, for example, show a characteristic buffering behavior that is reflected in a sawtooth-like throughput pattern as opposed to the stable throughput pattern of file downloads. These techniques provide the basis for metrics and heuristics, even in case of encrypted traffic.

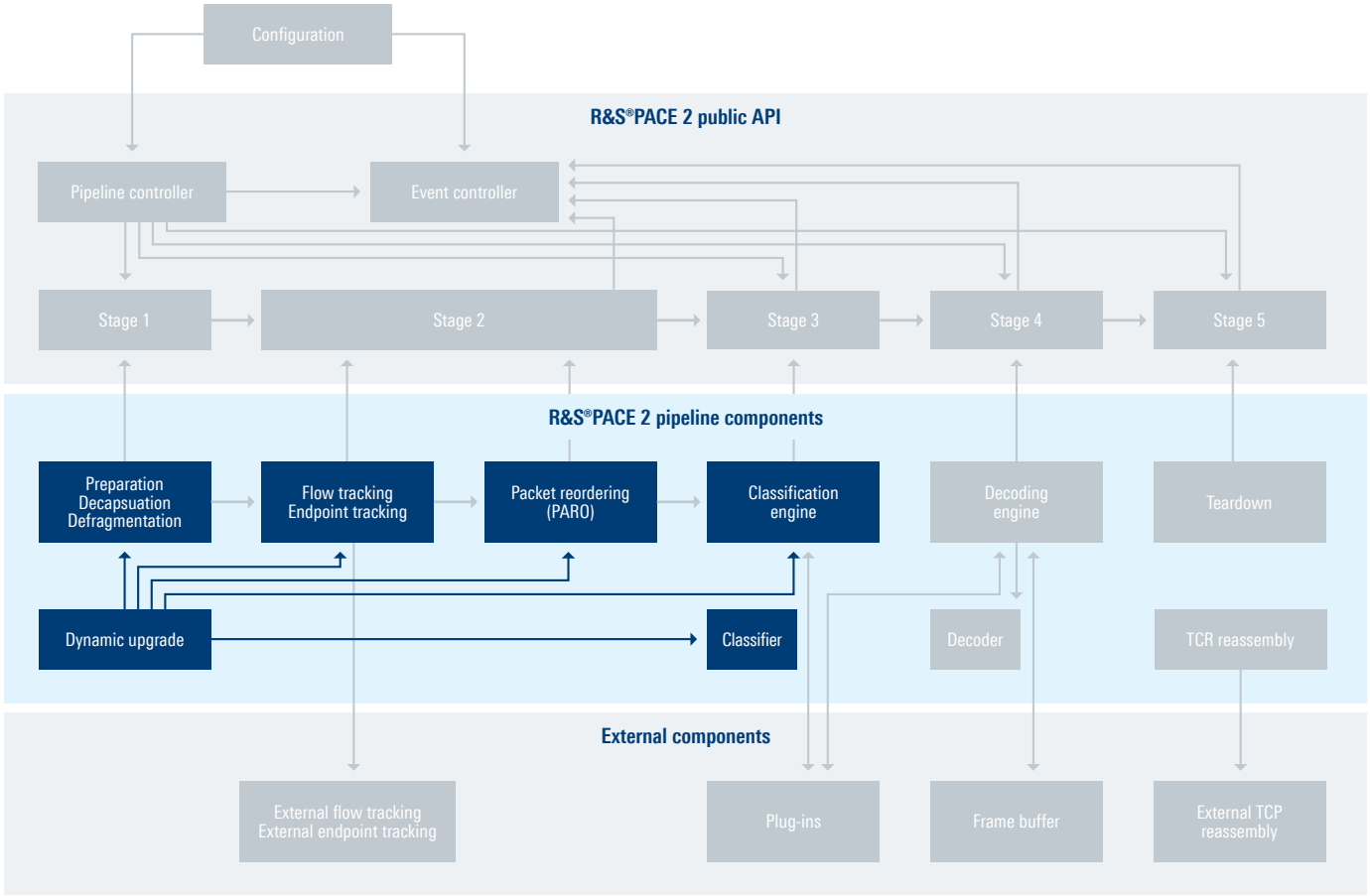
- Behavioral analysis: Scanning for patterns in the communication behavior of an application, including absolute and relative packet sizes, per-flow data and packet rates, number of flows and new flow rate per application.
- Statistical analysis: Calculating statistical indicators, including mean, median and variation of values collected as part of the behavioral analysis, and the entropy of a flow.

By combining behavioral and statistical analysis, R&S®PACE 2 can classify applications and protocols despite encryption and obfuscation. In addition, the metrics and heuristics provided by R&S®PACE 2 are not limited to connections based on SSL or TLS. They also apply to the classification of applications that are obfuscating or actively hiding, such as anonymizers or VPNs.

Encryption with TLS 1.3, ESNI, DNS over HTTPS/DNS over TLS and TLS 1.3 0-RTT and obfuscation techniques, such as randomization, tunneling and mimicry, pose a major challenge to conventional DPI. With a team of in-house data scientists in close collaboration with several universities, we research new classification techniques. By combining advanced statistical and classical machine learning, high-dimensional data analysis and deep learning approaches, we keep up with the technological development to ensure that even in fully TLS-1.3-encrypted scenarios, R&S®PACE 2 can reliably classify applications and protocols.

By combining various advanced techniques focusing on specific session behavior, R&S®PACE 2 can classify applications and protocols despite encryption and obfuscation.

DYNAMIC UPGRADE FEATURE



4.4 Additional features

Dynamic Upgrade
R&S®PACE 2 offers live updates without interruptions. The dynamic upgrading techniques smoothly integrate weekly software releases during runtime. The update releases include protocol and application signature updates, decoders and dissectors, improvements, bug fixes, documentation changes and new features. Occasionally, we include updates of the detection logic to improve the performance and detection results.

With live updates, weekly software releases can be integrated smoothly during runtime.

Extension Interface
With the Extension Interface, R&S®PACE 2 customers can implement their own code, such as traffic identifiers, at various stages during the packet processing and produce customized events. Different customer plug-ins can be chained together, combine multiple functionalities or work in parallel. A message-based controlling instance serves as a mediator between R&S®PACE 2 and the Extension Interface.

Multiprocessing
R&S®PACE 2 is designed for symmetric multiprocessing systems and supports uniform (UMA) and non-uniform memory access (NUMA). Implementing processing units as threads or single processes with individual flow and endpoint tracking allows for almost linear scalability with the number of used CPUs. This approach scales even better with NUMA architectures like AMD Opteron, because all flow and endpoint tracking tables can be stored in the local memory node.

Fastpath
The Fastpath feature speeds up the handling of common applications and uncritical traffic. If no additional processing is necessary, the Fastpath feature drops all upcoming packets of a flow after the flow has been classified. In addition, dedicated API functions can force upcoming packets of a current flow into Fastpath to improve performance — for example UDP flows after no layer 7 protocol is set after a certain number of packets.

Client-Server Indication
The Client-Server Indication feature (CSI) can identify if a host is mainly used as a client or as a server. The feature can distinguish client-to-server flows from server-to-client flows or server-to-server flows or even client-to-client flows in P2P networks. By revealing the internal side of networks, CSI enables targeted tracking of internal network users to significantly reduce memory requirements. In addition, CSI detects subscribers that host servers for policy enforcement use cases in enterprise networks.

Memory Management
The Memory Management feature provides particular ways to access memory blocks and manage their lifetimes. It is built on top of user-provided allocation hooks. This way, memory usage can be optimized in an individual way.

Configuration Dictionary
As an ABI-independent and API-stable configuration facility, the Configuration Dictionary provides a string-based and binary-compatible way to configure R&S®PACE 2 to handle options unknown to a specific software version.

Processing States
The Processing State feature (PS) provides performance values from R&S®PACE 2 during runtime. PS reveals the relative amount of time spent for processing particular components of the engine to save time when setting up complex performance tests or to generate statistics for a general performance overview.

R&S®PACE 2 is designed for symmetric multiprocessing systems and scales almost linearly with the number of used CPUs.

5. PERFORMANCE

R&S®PACE 2 is developed entirely in C to deliver high performance. This includes optimized code for high-end multicore technologies. Multiprocessing support enables almost linear scalability on multicore systems. With an average throughput of 14 Gbps per core, the performance of R&S®PACE 2 is market leading. By regularly conducting manual and automated tests, Rohde&Schwarz assesses the performance of R&S®PACE 2. Many factors have an impact on performance values, including:

- Hardware
- Optional features and stages of R&S®PACE 2 (see chapters 3–4)
- CPU and tracking technology
- Input (traffic mix, packet size, live traffic or offline traffic)
- Output options

To measure valid performance values, we use different traffic profiles that represent probable use cases. All listed profiles are based on different IP capture files corresponding to business areas where R&S®PACE 2 was successfully deployed. Each profile represents a specialized use case and covers a selection from a range of application scenarios, giving performance indications for individual use cases. All measurements are performed on a commercially available system in a single-thread setup. In multithreading scenarios, performance values scale almost linearly thanks to symmetric multiprocessing.

5.1 Profiles for live and offline traffic testing

Offline traffic tests with traffic data stored on a RAM disk use customer-centric traffic profiles selected and assembled from a range of application captures. Live traffic tests apply profile 4 in a TRex live traffic generator embedding R&S ®PACE 2 in the official DPDK L2 Forwarding (l2fwd) example. DPDK features such as prefetch data in cache, use of NIC head/tail registers and branch prediction bring significant performance gains compared to offline traffic processing.

5.2 Test environment

INTEL SELECT COMPLIANT/CASCADE LAKE NODE WITH QAT	
Chassis	Wolf Pass 2U Intel R2208WFQZS with QAT
CPU	2 × Xeon Cascade Lake Gold 6230N 2.3 GHz 27.5 MB cache, 20 cores, 135 W
Memory	24 × 16 GB 2666 Reg ECC 1.2V DDR4 = 384 GB
ATA hard drives	2 × 512 GB SSD M.2 SATA 3.0, 6 Gb/s
Network adapters	4 × XXV710-DA2 Dual Port 25 GbE Fortville
Chassis component	RMM – Remote Management Module 4 Lite 2 KVM Upgrade Intel AXXRMM4LITE2
PCIE hard drives	4 × 1.0 TB SSD 2.5 in PCIe NVMe 3.0 x4 Intel Cliffdale RE SE SSDPE2KX010T801 DC P4510 Series
Operating system	Ubuntu Server 18.04
Software version	R&S®PACE 2, version 20.01.24 (64-bit x86)

5.3 Test results measured single-threaded on one CPU core

OFFLINE

PROFILE 1: ENTERPRISE TRAFFIC

Applications: Akamai Cloud, Amazon Cloud, Amazon services, Apple Push Notification service (APNS), Apple services, Crashlytics, Facebook, Facebook Cloud, Google Ads, Google Analytics, Google APIs, Google Cloud, Google Drive, Google Maps, Google shared services, iCloud, iDrive, iOS AppStore, iTunes, Microsoft services, MoPub, Psiphon, QVOD, Thunder, VyprVPN, Yandex, Youtube

Protocols: DHCP, DNS, FTP, HTTP, ICMP, ICMPv6, IGMP, IPsec, ISAKMP, L2TP, Multicast DNS, NetBIOS, NTP, OCSP, OpenVPN, Psiphon, QUIC, QVOD, SMB/CIFS, SSDP, SSH, SSL, STUN, TCP, UDP

Average throughput:	10.73 GBit/s
Average pps:	1.86 Mpps
Total packet count:	28 M
Average packet size:	721.12 bytes

OFFLINE

PROFILE 2: STREAMING/MEDIA ON DEMAND TRAFFIC

Applications: Adform, Adjust, Adobe Creative Cloud, Adobe services, AdSafeProtected, Akamai Cloud, Amazon Cloud, Amazon Prime Video, Amazon services, Apple GeoLocation, Apple services, appsflyer, apptentive, apteligent, att-services, branch, Cloudflare, CNN, Conviva, Crashlytics, Criteo, directv, espn, Facebook, Fastly, Fox services, Fox Sports, FreeWheel, Google Ads, Google Allo, Google Analytics, Google APIs, Google App Engine, Google Cloud, Google FCM, Google Mail, Google Play, Google shared services, Hulu, iCloud, Instagram, iTunes, LinkedIn, Microsoft services, Moat, mParticle, Netflix, New Relic, Nintendo Network, Office 365, OpenX, Optimizely, Parsely, Pinterest, PlayStation Network, Rubicon Project, Salesforce, ScorecardResearch, Segment, SmartAdServer, Spotify, SpotX, StackPath Cloud, Taboola, Tealium, TUNE, Turner Broadcasting System, Twitter, Vimeo, WordPress, Xbox, Yahoo, YouTube, YouTube Music

Protocols: DHCPv6, DNS, Flash, HTTP, ICMP, ICMPv6, IGMP, IMAP, ISAKMP, MPEG, Multicast DNS, NetBIOS, NTP, OCSP, OGG, QUIC, QuickTime, RTMP, Spotify, SSDP, SSL, TCP, UDP, WindowsMedia, Zero

Average throughput:	13.52 Gbit/s
Average pps:	1.46 Mpps
Total packet count:	16 M
Average packet size:	1153.15 bytes

OFFLINE

PROFILE 3: MOBILE OPERATOR/PGW/EPC TRAFFIC

Applications: Adform, Adobe Creative Cloud, AdSafeProtected, Akamai Cloud, AliExpress, Amazon Cloud, Amazon services, Apple GeoLocation, Apple services, Brightcove, Cloudflare, CNN, Conviva, Crashlytics, Criteo, Facebook, Facebook Cloud, Fastly, FreeWheel, fyber, Google Ads, Google Analytics, google-apis, Google FCM, Google Maps, Google Play, Google shared services, iCloud, Instagram, iOS App Store, iTunes, Microsoft services, Moat, New Relic, OpenX, Optimizely, Rubicon Project, Salesforce, ScorecardResearch, Segment, Signal, Skype, Snapchat, Speedtest, SpotX, Twitter, WhatsApp, WordPress, Yahoo, Youku Tudou, YouTube

Protocols: DHCPv6, DNS, HTTP, ICMP, ICMPv6, IGMP, MPEG, Multicast DNS, NetBIOS, NTP, OCSP, QUIC, Speedtest, SSDP, SSL, STUN, TCP, UDP, WhatsApp, Zero

Average throughput:	11.03 Gbit/s
Average pps:	1.58 Mpps
Total packet count:	21 M
Average packet size:	872.80 bytes

OFFLINE VS. ONLINE

PROFILE 4: MIXED DPI/EPC LONGFLOW

This profile is used as a baseline for live traffic testing.

Applications: Facebook Cloud, Instagram, Skype, Spotify, YouTube

Protocols: SSL, TCP, QUIC

	Offline traffic	Live traffic
Average throughput:	14.28 Gbit/s	22.14 Gbit/s
Average pps:	1.94 Mpps	3.01 Mpps
Total packet count:	16 M	16 M
Average packet size:	920.60 bytes	920.60 bytes

6. USE CASES

R&S®PACE 2 can be deployed in a variety of network analytics solutions. The multitude of use cases and deployments reflects the adaptability, flexibility and scalability of R&S®PACE 2 and the benefits of licensing DPI software. The following sections list some reference use cases in the telco and cybersecurity domains and highlight the benefits R&S®PACE 2 has to offer in the respective use cases.

6.1 Digitial experience monitoring (DEM)/Application performance monitoring (APM)/SD-WAN

As the new digital habits require enterprise networks to connect any user seamlessly to any application, enterprises are seeing an increasingly critical need to develop real-time application monitoring and network management capabilities. Without packet-level analytics, there will be delays in diagnosing application performance issues and bottlenecks in the network. To offer high-quality services, enterprises must rely on a comprehensive library of business applications and network protocols to identify and analyze the traffic running in their networks. R&S®PACE 2 enables application-specific performance metrics such as bandwidth consumption, TCP round-trip time (RTT), out-of-order and retransmission counters, etc. Its vast signature portfolio contains business applications (such as Microsoft 365) and even differentiates between application service types (such as Microsoft Teams). Additionally, R&S®PACE 2 can classify encrypted protocols and applications that are used increasingly on enterprise networks. This way, DPI advances application performance management (APM), network performance management (NPM) and digital experience management (DEM) solutions with deep traffic visibility.

> R&S®PACE 2 enables application-specific performance metrics, such as bandwidth consumption, TCP round-trip time (RTT), out-of-order and retransmission counters, etc.

6.2 Service assurance and analytics

Gaining business intelligence from network and subscriber data is a fast-growing area as operators recognize they can unlock value by better understanding application usage and subscriber behavior. Marketing departments can use this information for targeted advertising and context marketing. Furthermore, with granular information about network bottlenecks and bandwidth demands, network planning and optimization departments can plan investments better and improve QoE per application. R&S®PACE 2 offers analytics vendors high performance and scalability for real-time analytics. Accurate identification of the applications subscribers are using, combined with a rich set of data such as mobile cell identification, traffic patterns or service types of OTT applications (chat vs audio vs video) reveals, for example, who the power users are and what the top applications are per subscriber segment or geographic location. In a typical integration, this application usage data is linked directly to third-party analytics or big data systems with the R&S®PACE 2 data serialization option. Additionally, with weekly signature updates and a broad signature portfolio covering different regions, verticals and metrics, R&S®PACE 2 supports analytics vendors with enhanced reporting features and fast time to market.

> With weekly signature updates and a broad signature portfolio covering different regions, verticals and metrics, R&S®PACE 2 supports analytics vendors with enhanced reporting features and fast time to market.

6.3 Wireless access points (WAP)

With significant growth expected in both data rates and bandwidth demands, particularly with bandwidth-consuming video traffic, WAP vendors are unable to meet the requirements of QoS, QoE and performance without proper IP traffic analytics capabilities. When embedded into new and existing wireless access point systems, DPI can help network professionals to dive deeper into the user activity data with intelligence about user-generated traffic, application usage, content communicated and anomalous patterns. With its broad application portfolio, R&S®PACE 2 enables WAP vendors to distinguish between specific applications (for example Hulu versus Salesforce) and then apply policies based on business rules. This strengthens network security and efficiency by limiting potential threats and prioritizing key business traffic.

By classifying traffic down to application attributes (for example voice versus chat), R&S®PACE 2 can separate traffic into classes such as low-latency (voice), guaranteed-latency (web traffic), guaranteed-delivery (application traffic) and best-effort delivery applications (file sharing). Using these classifications, internet access providers can better optimize resources for mission-critical traffic and police the use of noncritical traffic. The low memory footprint and the platform-agnostic design of R&S®PACE 2 allow integrations into legacy products and saving costs on hardware.

6.4 Virtualized evolved packet core (vEPC)

In 5G, the vEPC in mobile networks is a major breakthrough in network function virtualization (NFV). The development of multi-access edge computing (MEC) creates a powerful new network edge with user plane functions (UPF) involving packet routing and forwarding. UPF and MEC will essentially require real-time traffic visibility for the network as well as user analytics and application-specific information (for example, latency and type of content delivered), including packet inspection and QoS handling.

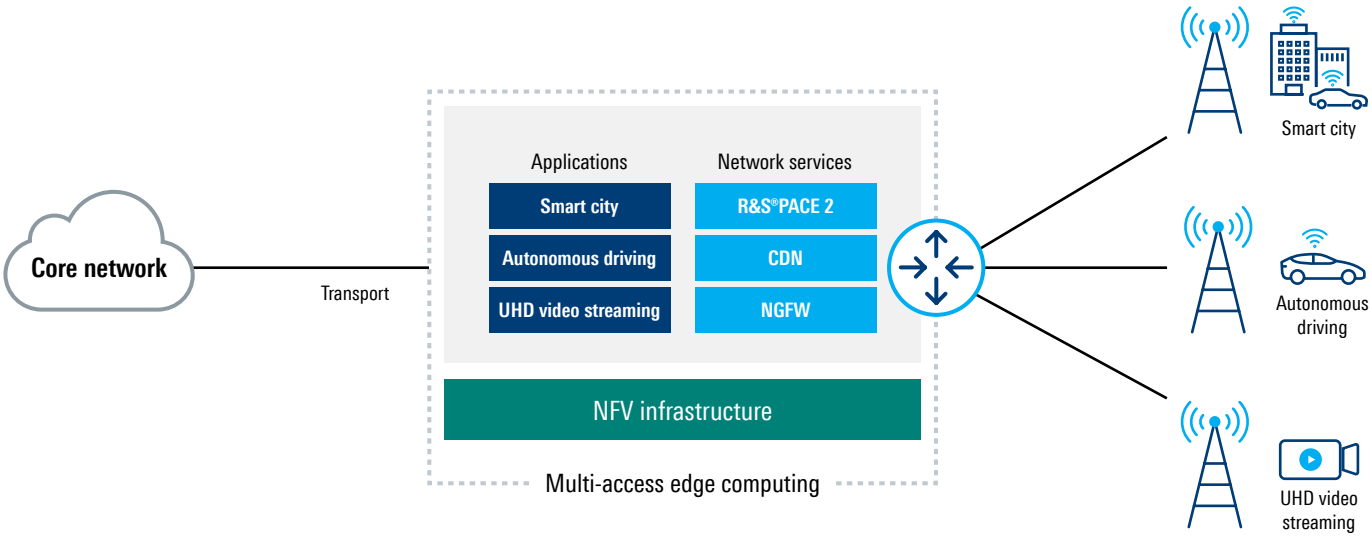
By embedding R&S®PACE 2 in their solutions, vEPC vendors can empower their customers with traffic visibility in real time, even in cases of encryption, obfuscation or tethering. For the vendors, this can unlock special benefits in countless business cases. Extensive coverage of VPNs and anonymizer signatures and detection of DNS tunneling allows vEPC vendors to prevent policy bypassing and zero-rating fraud. The broad signature portfolio, including machine-to-machine (M2M) and IoT protocols, allows fine-grained traffic management rules for each service class. Most importantly, despite ever-growing IP traffic rates, R&S®PACE 2 offers future-proof analytics capabilities in 5G architectures with high performance, linear scalability, and optimized support for DPDK and VPP.

Despite ever-growing IP traffic rates, R&S®PACE 2 offers future-proof analytics capabilities in 5G architectures with high performance, linear scalability and optimized support for DPDK and VPP.

6.5 Web application firewalls (WAF)

Protecting their customers' web servers against application-level attacks is an ever-growing challenge for web application firewall (WAF) vendors. With growing web protocol complexity, deeper insights into network traffic are a prerequisite to efficiently trace and identify malicious activities. These insights are required in real time to ensure that attacks are stopped before they reach web servers. R&S®PACE 2 empowers WAF vendors to reach beyond network addresses and ports. With fast and reliable detection of application vulnerabilities, WAFs can accept or deny specific application requests or commands by analyzing data formats such as HTML and JavaScript in real time. This uncovers malicious activity and helps to block threats. In addition to increased network security, this approach improves the performance and manageability of the network traffic.

This more refined visibility of network traffic covers not only highly reliable detection and classification of thousands of applications and protocols. With advanced DPI



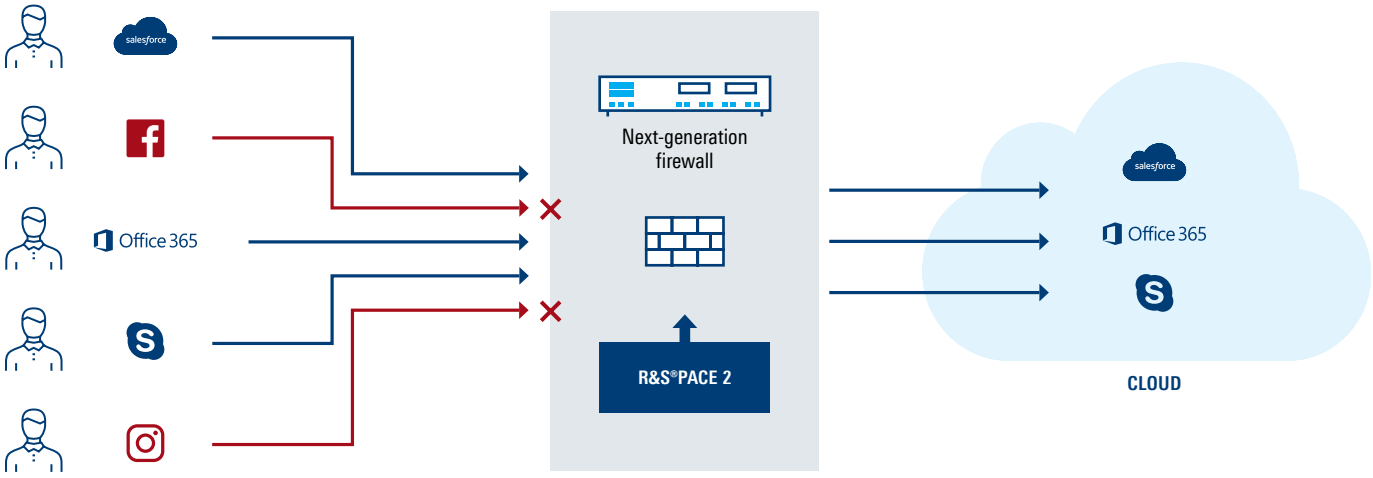
including behavioral and statistical traffic analysis, WAF vendors can examine the entire communication between clients and web applications even in cases of encryption, obfuscation and port hopping. Weekly signature updates and a vast application portfolio, maintained for our broad, worldwide customer base, provide WAF vendors with leading-edge application visibility.

6.6 Next-generation firewalls (NGFW)

The cloud era has done away with the perimeter that used to set a clear boundary between a network and the outside world. Cloud deployment, encryption and obfuscation in addition to the increasing mobile workforce that remotely accesses corporate software are just some of the challenges that firewall vendors are facing. The 'bring your own device' (BYOD) trend represents an attack surface with countless new attack vectors that cybercriminals can exploit to gain access to corporate networks. The IoT brings large numbers of unsecure devices that constitute an easy target for DDoS attacks. In order to protect their customers from rapidly evolving new cyberthreats, enterprise firewall vendors need granular insights into IP traffic to identify threats. With R&S®PACE 2, firewall vendors can easily differentiate between safe and malicious traffic, leveraging the highest protocol and application classification accuracy on the market — including business, messaging and IoT applications. Additionally, R&S®PACE 2 draws from an unrivalled portfolio of VPN, anonymizer and tunneling protocols. Thanks to weekly signature updates, firewall vendors can rely on a classification library that is always up-to-date by sourcing leading-edge technology.

With R&S®PACE 2, firewall vendors can easily differentiate between safe and malicious traffic, leveraging the highest protocol and application classification accuracy on the market — including business, messaging and IoT applications.

DPI-ENABLED APPLICATION CONTROL IN NEXT-GENERATION FIREWALLS



"I would absolutely recommend the DPI engine from Rohde & Schwarz. We have a very strong partnership and they always provide quick service and excellent support. Rohde & Schwarz has the capacity and the infrastructure to build their deep packet inspection technology and maintain it on a daily basis. It is very important for us that they respond to our ideas and new protocols swiftly, and that we get regular and frequent updates."

Bernhard Patsch, Director next-generation firewall engineering, Barracuda

7. INTEGRATION

7.1 Requirements

With its flexible and platform-agnostic design, R&S®PACE 2 can be integrated in solutions from small routers (ARM CPU) up to large carrier networks (multicore x86). Classification works in a source-agnostic way, requiring nothing but a data area in the memory with a valid IP packet (valid layer 2 header). This allows for any format (PCAP, text, network interface card memory, etc.) from any source (IP, Ethernet, etc.).

7.2 Integration process

The elaborated integration process includes a proof-of-concept (PoC) phase that enables customers to test R&S®PACE 2 and validate its benefits for a given solution, even remotely. To facilitate PoCs, we offer a framework (PACE 2 packet toolkit, PTK) for demo tools apt for analyzing (PACE 2 analyzing tool, PAT) or health monitoring and logging (PACE 2 information framework, PIF). Integration examples and an internal tracking component allow testing the integration of R&S®PACE 2 without much effort. Later on, integration examples can be used as a basis for customized solutions.

Qualification
In a first call, optionally with technical consultants on the line, we figure out whether R&S®PACE 2 can be installed on the customer's equipment and whether it can fulfill the expectations for the given business case.

Proof of Concept
After qualification, an individual account is created to download the demo version of R&S®PACE 2. Demo software packages include a variety of integration examples that help to quickly test a selection of features and options on PCAP files. At this stage, customers can create help tickets and ask questions in a dedicated PoC portal. These will be taken care of by highly specialized support engineers. Help options include on-site support, remote help and phone consulting. Optionally, we support customers with integrating a demo version of R&S®PACE 2 in their solution or a comparable system. With a single, C-based API and a command-line interface, all stages can be configured. In simple setups, R&S®PACE 2 can be integrated remotely in a couple of hours, with only a few hundred lines of code.

After signing a licensing contract, the full version of R&S®PACE 2 can be downloaded swiftly from the customer portal. From this moment on, weekly signature releases keep the licensed software up to date.

Custom implementations
In case of special setups or requirements, our support engineers can help customize R&S®PACE 2 with custom implementations. For example, we designed an early packet detection functionality for a customer to classify certain over-the-top (OTT) applications with the first incoming packet by leveraging IP ranges.

8. SERVICE AND SUPPORT

Sustainable technical support and service go far beyond basic troubleshooting. With continuous optimization and maintenance, R&S®PACE 2 ensures a smooth operation with calculable operating costs through the entire product lifecycle. Adaptable service level agreements (SLAs) with adjustable response times provide technical expertise tailored to customer's requirements.

Online ticket tracking
Customers receive dedicated access credentials to an online ticket tracking service to:
- Open and manage an unlimited number of troubleshooting requests
- Handle priority levels
- Keep up to date with the status of tickets
- Share documents and attachments

Monthly support performance report
With an overview of all pending requests, this report helps customers identify bottlenecks and understand the fulfillment rate of the agreed service level.

Customer portal: Releases and maintenance
Maintenance engineers work continuously on the weekly updates that include classification algorithms for new protocols and applications and updates for existing signatures. We roll out software updates with new features several times a year. In addition, we distribute maintenance releases that solve reported issues whenever necessary. Customers can download the weekly releases swiftly from the customer portal.

Support channels
Depending on the SLA, we provide different support channels:
- Web: Customer Portal and ticket tracking system
- Email: Customer Support email address
- Phone: Customer Support hotline

Remote consulting and assistance
Consulting engineers can coordinate and support integration into customer solutions remotely. Remote assistance sessions are an option to solve reported problems. Remote technical consulting can support product planning and evaluation.

Proactive communication and alerts
As soon as we become aware of issues that affect customers' solutions, our customer support team gets in touch right away before things get critical.

Dedicated support account manager
Customers are assigned a dedicated support account manager who is responsible for their service requests and is the central point of contact for any request.

On-site support
Support engineers visit customers for
- System performance optimization
- Hands-on trainings to test the functionality of R&S®PACE 2 under supervision, for example with new features
- Integration support

Individual consulting and feature request
Our consulting engineers offer additional R&S®PACE 2 know-how for our customers to meet technology challenges. Customers can influence the product roadmap of R&S®PACE 2, for example by requesting new application and protocol classifications for the library. In regular meetings, the account managers present product roadmap updates, assess further requirements for customers' solutions and keep up with their business strategy.

> We are extremely satisfied with the support and responses we have received from the Rohde&Schwarz team. Their strong understanding of our needs and prompt, expert service delivery exceeded our expectations.
> **Dr. Evgeny Fedchenko, CTO of Infotecs GmbH**

ipoque

ipoque, a Rohde & Schwarz company, is a global leader in the world of network analytics software. We leverage our deep domain expertise to create customized software solutions that empower our customers to transform data into intelligence. As a subsidiary of Rohde & Schwarz, we take advantage of potential synergies.

Rohde & Schwarz

The Rohde & Schwarz technology group develops, produces and markets innovative information and communications technology products for professional users. Rohde & Schwarz focuses on test and measurement, broadcast and media, cybersecurity, secure communications and monitoring and network testing, areas that address many different industry and government-sector market segments. Founded more than 80 years ago, the independent company has an extensive sales and service network in more than 70 countries.

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

ipoque GmbH
Augustusplatz 9 | 04109 Leipzig, Germany
Info: + 49 (0)341 59403 0
Email: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 3608.7309.62 | Version 01.02 | October 2020
Solution Guide | R&S®PACE 2

3608730962
3608.7309.62 01.02 PDP 1 en