SD-WAN and DPI A powerful combination for application-driven networking

White Paper | Version 01.01

ROHDE&SCHWARZ

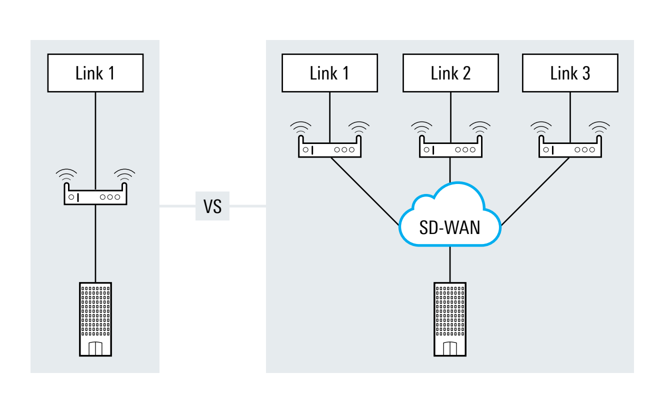
Table of contents

1. Defining SD-WAN

The software-defined wide-area network (SD-WAN) is a specific application of software-defined networking (SDN) technology applied to WAN connections, which are used to connect enterprise networks – including branch offices and data centers – over large geographic distances.[1]

SD-WANs are gaining traction with enterprises looking for more flexible and cost-effective WANs that support multiple transport modes suitable for every site: Internet, DSL, Ethernet or MPLS. A separate control and data plane offers companies a programmable network with more flexible traffic management, independent of the chosen transport mode. Network and IT departments have long wanted direct control over policy and routing of applications to assure apt performance. This becomes even more critical in times when companies increasingly rely on cloud applications hosted by private data centers as well as public cloud providers such as Amazon Web Services.

Traditional WAN versus SD-WAN



For managed services providers such as AT&T, Orange, Deutsche Telekom, etc., SD-WAN presents an opportunity to add Network as a Service to their portfolio, but also to attract commercial customers with valuable network management, application analytics and security tools.

Up-and-coming SD-WAN vendors such as Versa Networks, VeloCloud (now owned by VMWare), and Nuage Networks are introducing new solutions to the market while vendors from related business fields such as Riverbed, Infovista, or Citrix are also entering the SD-WAN field. Even established routing vendors the likes of Cisco are redefining their portfolio to react to market demands by acquiring startup SD-WAN vendors such as Viptela.

As with any new market, there are multiple facets to SD-WAN. SD-WAN is a single virtual network function (VNF) and can be delivered as part of virtual customer premises equipment (vCPE) or universal CPE (uCPE). It can also be delivered on its own on a lightweight appliance and may or may not replace legacy CPEs.

In combination with vCPE, SD-WAN is already one of the leading use cases of network functions virtualization (NFV). NFV is an architecture where VNFs are run on standard equipment (x86 servers). uCPE is a platform on which multiple VNFs can be delivered. This architecture allows companies to rapidly deploy functionalities to branch offices. uCPE supports VNFs such as SD-WAN, WAN optimization, firewalls, SIP trunking or routing. This is where being able to provision multi-vendor VNFs comes in handy for managed service providers. For example, SD-WAN could be combined with next generation firewalls, intrusion detection/prevention, unified communications etc. and delivered to a branch office in a single grey box.

SD-WAN as a strategic NFV application can be a massive opportunity for service providers, but only if they are able to add value beyond what they already offer as managed service providers. For SD-WAN vendors, the market is heating up. This is why it is of critical importance to be able to offer advanced features such as application analytics for policy and security so that service providers can build features to match them.

This paper explores the market trends, challenges and opportunities for vendors in the SD-WAN field. It then goes on to highlight the key value of deep packet inspection (DPI), which is in providing application visibility as the driving factor for dynamic path selection, application performance management and advanced security, all of which constitute crucial elements with which SD-WAN vendors can stand out as competition increases.

What is SD-WAN?

Gartner says SD-WAN has four characteristics

Must support multiple connection types
MPLS, internet, LTE, etc.

Can do dynamic path selection
Allows for load sharing across WAN connections

Provide a simple interface for managing WAN
Must support zero-touch provisioning at a branch, should be as easy to setup as a home Wi-Fi

Must support VPNs
As well as other third-party services, such as WAN optimization controllers, firewalls, webgateways, etc.

[1] https://www.sdxcentral.com/sd-wan/definitions/software-defined-sdn-wan

2. SD-WAN market trends and opportunities

The SD-WAN market is growing fast with increasing commercial interest and adoption plans. Growing competition among SD-WAN vendors means SD-WAN solutions need features and capabilities that differentiate them from competitors. With startup vendors competing against traditional CPE and networking vendors as well as other vendors that are moving into the SD-WAN field from related fields, being able to offer more than path selection and improved WAN management will prove to be of paramount importance.

Companies now provision Network on Demand solutions that have to support dynamic application service level agreements (SLAs). This poses new challenges to service providers and SD-WAN vendors as they will have to supply tools such as customer management portals that offer full visibility into network and application performance on a real-time basis. These can be a key point of difference. For example, companies may want to take advantage of video conferencing without over-provisioning bandwidth. With SD-WAN, they can increase their bandwidth temporarily and then turn it down again.

Another trend is universal CPE (uCPE), which accelerates branch office deployment by bringing offices online quickly. uCPE also simplifies the IT infrastructure without requiring different CPE and equipment for SD-WAN, firewall, intrusion detection/prevention, WAN optimization etc. Instead, these can be provisioned as software-based virtual network functions. SD-WAN, next generation firewalls and WAN optimization may still be required in the branch, but companies want more flexibility in deploying and consuming network functions as needed rather than having them all on a single platform.

Market opportunities

The opportunity to provide enterprises with additional services such as security, application monitoring and application optimization beyond basic connectivity is a compelling value proposition of SD-WAN. We expect to see more service providers offering SD-WAN as a managed service as well as resellers, systems integrators and IT services companies that are looking to expand their service range by giving companies more choices.

The digital transformation will require network infrastructures to seamlessly connect any user to any application. This will require SD-WAN to work across the branch, campus, data center and cloud with open and programmable architectures for vendor interoperability. Unified application delivery across the company will require centralized management, application visibility and monitoring to ensure greater agility as well as uniform security and an improved overall quality of experience for all users.

We also expect to see managed services providers increasing the value of SD-WAN services through real-time application visibility, advanced performance analytics and reporting. This could happen in form of reports to companies' IT departments on the performance of applications on the wide area network, suggestions etc.

For example, U.S. provider Windstream's SD-WAN service Concierge intends to „flip the service provider model on its head" by proactively offering IT departments an assessment of application performance over the network and, in many cases, helping identify unknown or rogue applications in the process. How networks consume bandwidth and how users perceive the applications' QoE will have greater significance. Another SD-WAN service provider is offering a dedicated Technical Service Manager which helps monitor, analyze and prioritize companies' real-time business communication services and optimize application performance.

SD-WAN also represents the first major software-defined networking (SDN)-based product offered by cable providers. It is poised to become a leading-edge product in cable providers' portfolios tailored for attract large companies and multi-site enterprises, helping them to increase their market share. SD-WAN provides a platform to layer virtual network functions (VNFs) that cable providers are exploring.

Besides cost and performance benefits, advanced SD-WAN security and analytics are important USPs helping providers to differentiate themselves from competitors. Most SD-WAN vendors offer encryption for branch-to-branch corporate traffic using IP Sec, which protects data in transit. However, in order to ensure holistic security, securing the edge is critical. Providers are increasingly offering firewall VNFs at branch sites, intrusion detection and prevention (IDS/IPS), quarantining or otherwise deflecting detected malware as well as web filtering to protect against break-ins, man-in-the-middle attacks, and malware that can cause denial of service or data theft.

> „Besides cost and performance benefits, offering advanced SD-WAN security and analytics is an important area where providers can differentiate themselves from competitors."

3. How DPI enables application-driven SD-WAN features

SD-WAN vendor solutions rely on an integrated deep packet inspection (DPI) library of applications and protocols to identify and analyze, in real time, the traffic running on their networks.

DPI enables SD-WAN to identify the application and application family types. The number of bytes of incoming and outgoing traffic is recorded for every application. This data can be viewed on a centralized management portal or customer dashboard at the defined polling interval. It can also be displayed as reports.

Application statistics enable companies to view detailed information on incoming traffic, outgoing traffic as well as the top applications, sites, and application families as reports. This provides a holistic view of network bandwidth usage, a feature for which IT departments have strong demand. Besides the real-time discovery and classification of applications, SD-WAN solution vendors and service providers can opt to enable DPI at particular sites or across all sites.

This application visibility and control can be useful to secure and segment traffic. For example, regional Internet exit points can break out specific applications rather than backhauling all traffic to a data center. This can be particularly useful in case of security breaches. In addition, once a packet is classified, the application identifier can be used in a firewall filter as a match criterion to identify this type of traffic.

3.1. Application-driven policy

A further selling point of SD-WAN is intelligent path control, which means that even if a network link is down, mission-critical enterprise applications can be re-routed without loss of performance. This is increasingly attractive to enterprises that are using third-party cloud application providers, e.g. Microsoft, Salesforce, Amazon Web Services etc., as well as companies with a high number of mobile workers and distributed companies such as banks or retailers with many small sites and branch offices.

DPI-enabled SD-WAN with application visibility and real-time data is required to support:

- Fine-grained policies on a per-application basis
- Dynamic, application-aware, performance-based routing
- Quality of experience and performance of applications, particularly cloud applications that businesses are increasingly dependent on (e.g. Office 365)
- Application SLA enforcement – SLA management based on application or service type based on latency, jitter, packet loss and voice MOS

3.2. Application visibility and performance control

Business customers want to be in control of their application and performance management (APM). DPI can help collect and closely monitor metrics, which are relevant to application performance monitoring:

The first set of performance metrics defines the performance experienced by end users of the application. One example metric of performance are the average response times under peak load. The components of the set include load and response times.

The second set of performance metrics measures the computational resources used by the application for the load. This metric set indicates whether enough resources are available to cope with the load, as well as if there are possible performance bottlenecks. Measuring these variables establishes an empirical performance baseline for the application.

A customized dashboard UI can provide easy access to these metrics as well as other application and traffic routing data (SLA-based, application policies, routes, sites).

Highly granular application identification allows for strong traffic engineering policies. For example, a specific website such as Facebook could automatically trigger the use of URL filtering policies and the assignment of broadband connectivity only.

> „SD-WAN vendor solutions rely on an integrated deep packet inspection (DPI) library of applications and protocols to identify and analyze, in real time, the traffic running on their networks."

3.3. Overview: DPI-enabled SD-WAN features

Feature	Benefit
Application visibility by site, app or app family	Identify over 3000 applications and be able to manage QoS and application security.
Application performance – per app, per session, per site	Gain insight into application delivery in order to proactively manage user experience, e.g. computed statistics in real time (e.g. Mean Opinion Score for VoIP).
Traffic management – inbound and outbound	Gain insight into application traffic and bandwidth usage and support secure cloud migration at branch offices.
Per-app policy control	Prioritize mission-critical apps – in case of bandwidth limitations, these apps can be dynamically routed with the fastest available transit time. Closed-loop automation – maintain high performance for mission-critical enterprise apps even if a link fails. High-bandwidth apps can be balanced across multiple links to provide steady performance for large file transfers.
Application-level security	Identify potentially malicious traffic and anomalies, prevent data-leakage and receive actionable security information in real time (e.g. forged or corrupted files are automatically identified). Enhance security and enable direct branch connection to cloud Internet and SaaS applications.Secure data with application-level visibility, security policies and data segmentation.
Application WAN optimization	A range of techniques such as TCP flow control, data compression, de-duplication and protocol optimization improve end-user experience and optimize bandwidth.
Management and Visibility	Report application delivery to users in the branch for monitoring and management portals. Export data to third-party applications that offer insight into networks and applications.
Hybrid WANs (MPLS and Internet)	Based on the underlying network infrastructure – MPLS or Internet site – map each application to the best path through the network and ensure high quality and a secure user experience.

4. How DPI enables advanced SD-WAN security

DPI adds an additional layer of protection to SD-WANs. This is required because many organizations are connecting their branch offices directly to the Internet, which risks exposing them to more security threats although SD-WAN features a secure overlay. DPI provides full application visibility and control to segment branch offices from the WAN to prevent attacks on any one branch from spreading across the entire company.

When paired with DPI, service chaining provides an effective way of securing SD-WAN networks. By means of DPI, traffic is collected from the edges of a network. Service chaining supports this by merging multiple security functions into a single, centralized hub that analyzes the traffic and identifies threats.

Deploying SD-WAN in combination with proprietary or third-party software-based security VNFs, additionally secures the WAN and Internet perimeters without the need for additional hardware. DPI grants application visibility, supporting software-based VNFs for unified threat management such as stateful and next-gen firewalls, malware protection, URL and content filtering, IPS, anti-virus or DDoS. DPI application visibility also prevents firewalls from accepting malicious traffic, as well as attempts to sneak malware through the gates unseen.

> "DPI provides application-level visibility for traffic leaving the branch perimeter, and this capability can accelerate the response to attacks by enabling the definition of dynamic policies for branch traffic based on L7 traffic analytics."

Overview: Enhanced SD-WAN security enabled by DPI

Feature	Benefit
Application visibility for next-generation firewalls	Policy rules based on application identity, IP blacklisting, whitelisting, geo-IP, customer app ID signatures, protection based on firewall SSL certificates, expired certificates, untrusted CAs, unsupported cyphers and key lengths.
Application visibility and control to segment traffic	Segment branch traffic and apply individual security policies to each segment. Create multiple virtual private networks (VPNs) on top of a single fabric to functionally segregate different types of traffic between private and public cloud environments. Steer traffic from a remote hub to a regional hub for inspection. Supports various treatments of client applications using encryption, e.g. surveillance, PCI, load balancing between circuits.
Multi-layer security at the application level	Supports predictive network analytics and unified threat management such as threat profile reports: URL filtering and captive portal actions, IDS/IPS, anti-virus, SSL certificate anomalies, packet capture for known/unknown applications and detected vulnerabilities etc.

5. Encrypted traffic analytics

An increasing number of protocols and applications such as Skype, WhatsApp, BitTorrent, Facebook, Twitter, Dropbox, Gmail, Office365, Instagram, are encrypted. Additionally, some protocols such as TOR, Freenet and other P2P apps such as Ultrasurf and YourFreedom can adapt to circumvent firewalls and DPI detection, for example when traffic generated by a specific protocol is limited or blocked.

Most encrypted connections on the internet are using transport layer security (TLS) or SSL for encryption. Both of these technologies are established with a handshake. All information that is necessary to classify a protocol application is transferred with this handshake.

While it is still possible to classify an encrypted application, end-to-end encryption entirely prevents metadata extraction. This means that there can be no insight into the content of a message.

The DPI engine R&S®PACE 2 delivers reliable classification results with a very low false negative rate and virtually no false positives, regardless of end-to-end encryption. This is achieved through a variety of detection techniques:

- **Pattern matching:** scanning for strings or generic bit and byte patterns anywhere in the packet, including the payload portion, usually at fixed locations.
- **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 that can be used to identify transmission types (e.g. real-time audio and video, chat, or file transfer), including mean, median and variation of values collected as part of the behavioral analysis, and the entropy of a flow.

Statistical and behavioral analytics provide the foundation for metrics and heuristics, such as packet sizes, packet timing, latency, throughput, entropy and jitter. Network performance metrics are especially important in security applications, as many sophisticated applications such as VPNs can only be detected by combining various metrics with specific session behavior. For example, packet sizes and packet timing are used to distinguish between messaging and file transfers in encrypted messaging apps such as Skype.

> “DPI can gather information about encrypted or obfuscated applications and protocols by using heuristic methods.”

DPI extracted metadata from encrypted and unencrypted traffic

Metadata category	Example metadata
Traffic volume	Per user, per protocol, per application, per flow, per direction
Service detection	Differentiation between e.g. Skype audio and video calls
Quality of Service	Jitter, throughput, latency, roundtrip time, ramp up time, packet loss, retransmissions
Security and data leakage	File up- and downloads, entropy-based DNS tunneling detection, prevention
Client information	HTTP / QUIC user agents, operating dystem

6. Build or buy DPI?

SD-WAN vendors rely on DPI application awareness as a key feature for policy control, critical traffic steering and application security. Consequently, they have to make a strategic choice between building in-house DPI libraries and licensing software from a DPI specialist.

A major challenge for SD-WAN vendors trying to build in-house DPI is the need to continually update their software with the latest applications and protocols so the SD-WAN can offer up-to-date network traffic visibility. A DPI engine is only as effective as its creators make it. The evolution of network traffic with new applications and protocols emerging non-stop means that DPI software is never complete.

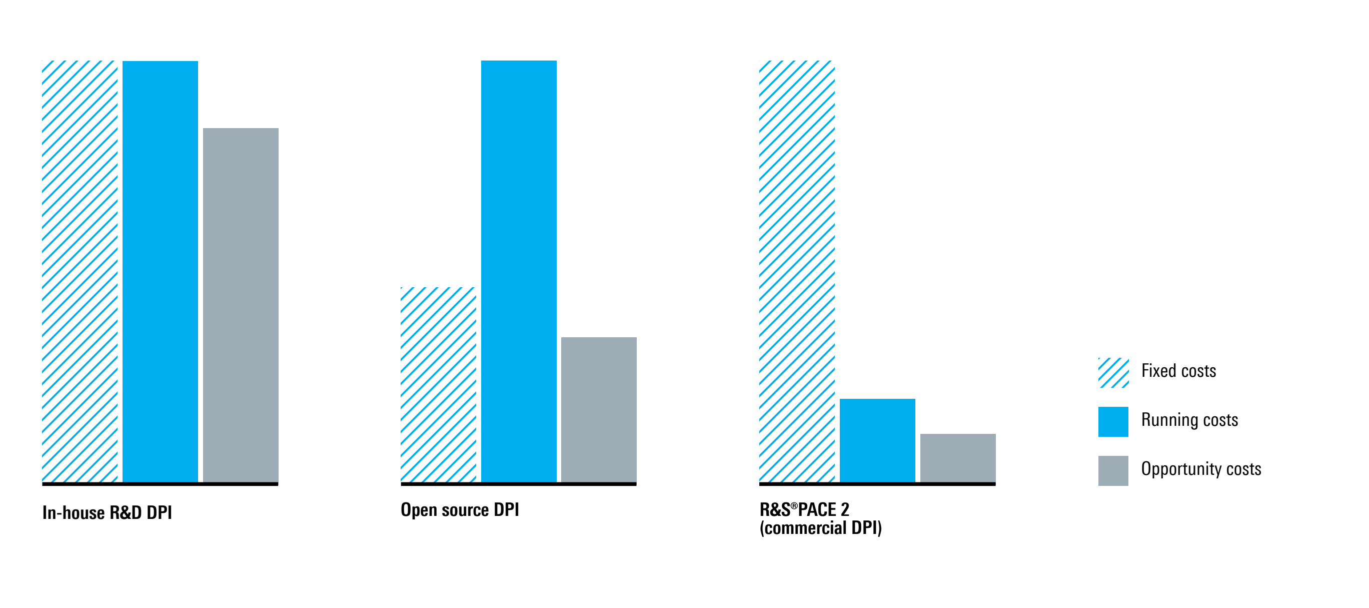
DPI software companies have dedicated DPI experts that add new application signatures on a weekly basis. This ensures that a high percentage of network traffic can be reliably classified, which is critical for SD-WAN solutions that need to make policy and routing decisions on the basis of reliably classified traffic. As a result of continuous performance and reliability testing, regular improvements can be made to the software to ensure all applications are detected.

Vendors may consider open-source DPI with the idea that it is free to use. However, there are both pros and cons to adopting an open-source DPI library. Open-source software often ends up not being free because it still requires in-house developers to learn how to use and, more importantly, how to customize the software. Frequently, this requires working with a third-party vendor to manage and add new features.

Most SD-WAN vendors simply do not have the in-house resources to track and classify the latest apps and protocols. Ready-to-use DPI software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally. Instead, SD-WAN vendors can spend their valuable time and resources on their core products in what is proving to be a highly competitive market.

> "Ready-to-use DPI software libraries reduce costs and risks associated with developing and maintaining a highly complex technology internally."

Commercial DPI reduces development costs



7. DPI engine by Rohde & Schwarz

SD-WAN vendors need to integrate behavioral, heuristic and statistical analytics to reliably detect network protocols and applications and extract metadata in real time. The DPI solution from Rohde & Schwarz for SD-WAN is the easiest to integrate, whether on an SD-WAN appliance or an SD-WAN vCPE platform. The R&S®PACE 2 protocol and application classification engine offers the industry's most efficient memory and CPU utilization, featuring the smallest processing footprint. R&S®PACE 2 only requires approx. 400 bytes per flow while using very little processing power (CPU-load) and no memory allocation during runtime.

The R&S®PACE 2 software can be implemented in the user space or the kernel space of the processor, reducing the impact on processing performance. The backwards-compatible R&S®PACE 2 software has an intuitive, highly flexible and platform-agnostic application programming interface (API) that speeds up integration and has no external dependencies. R&S®PACE 2 also simplifies upgrades by enabling automatic weekly signature updates without rebooting.

The R&S®PACE 2 software supports a wide range of operating systems and hardware architectures:

- Intel x86 (Linux, Solaris, FreeBSD, Windows)
- ARM (Linux, Android, BSD)
- Cavium Octeon (SE, BSD, Linux, HFA)
- PowerPC (Linux, BSD)
- MIPS (Linux, BSD)

R&S®PACE 2 accurately identifies applications up to Layer 7 of the OSI model and makes it possible to manage network and application performance in real time. By integrating R&S®PACE 2, SD-WAN vendors can keep up with dynamic changes in protocols and applications, ensuring a high detection rate in traffic management.

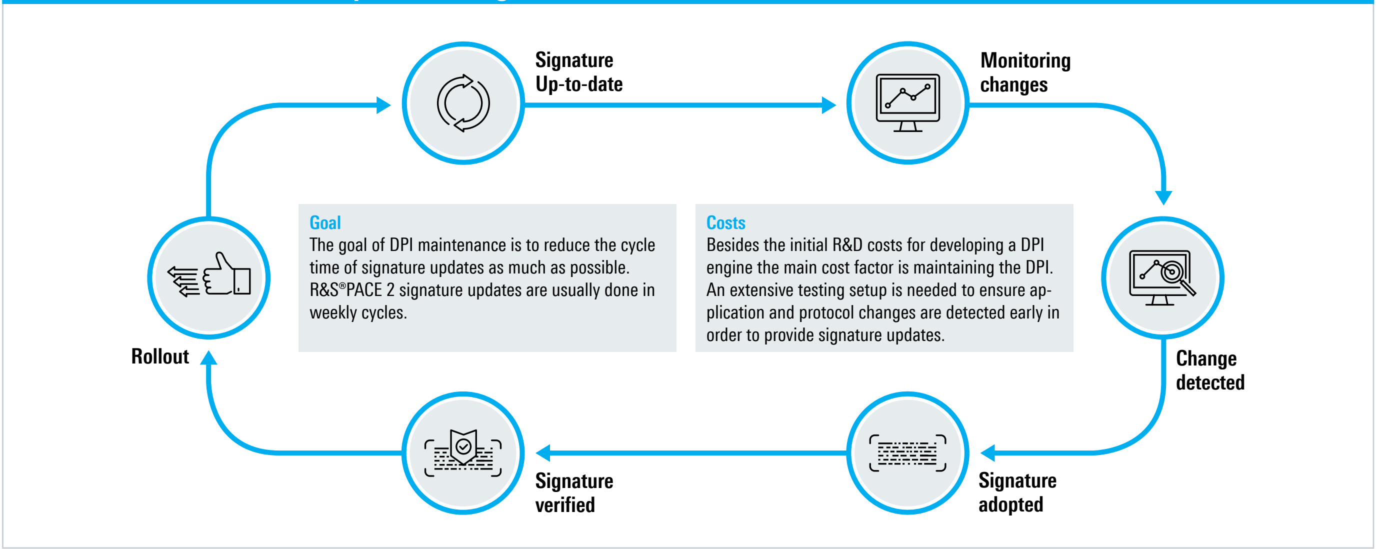
The R&S®PACE 2 software makes it easy to extract metadata and to report and handle information in real time. The modular DPI engine can be tailored to meet customer SD-WAN requirements including configurable event reporting to improve performance and customizable analysis that saves time and effort.

Customers also find many benefits from sourcing R&S®PACE 2:

- Weekly protocol and application signature updates
- Highest classification accuracy in the DPI market
- Focus on core competencies to become more efficient and profitable
- Speed up time-to-market by optimizing the development schedule
- Reduce and optimize development costs by outsourcing DPI
- Maximized return on investment (ROI)

Rohde & Schwarz is recognized globally as a leading developer of DPI software. It has more than 10 years of expertise in optimizing the performance of network equipment and IT security solutions with embedded DPI. With customers in over 60 countries worldwide in the areas of network analytics, traffic management and network security, its objective is customer satisfaction throughout the entire product lifecycle.

Rohde & Schwarz ensures up-to-date signatures



Goal
The goal of DPI maintenance is to reduce the cycle time of signature updates as much as possible. R&S®PACE 2 signature updates are usually done in weekly cycles.

Costs
Besides the initial R&D costs for developing a DPI engine the main cost factor is maintaining the DPI. An extensive testing setup is needed to ensure application and protocol changes are detected early in order to provide signature updates.

8. Summary

The SD-WAN market is growing fast, but so is competition. SD-WAN vendors need DPI to support critical features such as real-time application visibility and enhanced security features and analytics. This also caters to commercial customers' use cases. One example is the visualization of and reporting on application performance and security diagnostics at key customer sites and cloud data centers. With the help of DPI technology, SD-WAN vendors can now deliver intelligent routing, traffic steering and enterprise application performance with advanced reporting capability. However, cost and performance benefits are meaningless without strong end-to-end security. DPI offers an exponentially growing amount of information on the network and plays a key role in providing critical information on the health and performance of the network. The accuracy of the data and the frequency of data collection will also drive automation and efficiency in network management as well as enable more predictive application and security policies.

The SD-WAN market is highly competitive. Vendors cannot compete if they do not lower their development costs. Lowering costs is especially important when competing with service providers that want a piece of the fast-growing market and rapidly gain access to enterprise customers. Sourcing DPI can enable both: Reduction of development costs as well as market differentiation by partnering with a dedicated DPI expert with more than ten years of experience in the traffic analytics business.

The flexible and customizable R&S®PACE 2 software simplifies integration with on-premise and cloud-based SD-WAN products. The DPI software allows SD-WAN providers to further enhance real-time monitoring capabilities and intelligent routing based on dynamic network conditions and to strengthen application performance SLAs and security measures. The software is easy to implement and requires no in-house resources to track and classify the latest apps and protocols, simplifying the extraction of valuable metadata.

Service that adds value

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

ipoque

ipoque, a Rohde & Schwarz company, is a leading vendor of deep packet inspection software that adds protocol and application classification capabilities to network analytics, traffic management and cybersecurity solutions. Rohde & Schwarz also provides a holistic network traffic analytics system for communication service providers that allows deep insights into network behavior, network performance and trends to optimize both quality of experience and quality of service.

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
Info: + 49 (0)341 59403 0
E-Mail: info.ipoque@rohde-schwarz.com
www.ipoque.com

PD 5216.1170.52 | Version 01.01 | August 2018 (mh)
White paper | SD-WAN and DPI
Data without tolerance limits is not binding | Subject to change

5216117052