APPLICATION AWARENESS

ENCRYPTED TRAFFIC VISIBILITY

Next-gen deep packet inspection, machine learning, deep learning and other methods to detect encrypted traffic

ROHDE&SCHWARZ
Make ideas real

CONTENT

1. INTRODUCTION

Encryption is rapidly becoming synonymous with network security and privacy. Organizations are leveraging the potential of encryption to encode and conceal data over both public and private networks ensuring data privacy, confidentiality and security. Google revealed in its Transparency Report[1] that as of January 2023, 92.0 % of all traffic on its Chrome browser on Windows operating systems was encrypted, compared to 57 % in January 2016. The corresponding figure for its own Chrome operating system was 99 %, having more than doubled during the same tenure from just 44 %. According to Fortinet[2], 85 % of all web traffic in 2020 was encrypted.

Encryption, however, presents challenges in the form of diminished visibility and control which can be disruptive to networks that are highly reliant on deep network insights into managing and securing their data and assets. In its '2021 State of Encrypted Attacks' report[3], Zscaler saw a 314 % rise in encrypted attacks. The cloud security vendor reported that 80 % of all cyber-attacks had used encrypted channels. Encryption, ironically, has rendered existing artillery ineffective against cyber-threats. It has similarly resulted in the impairment of various other network functionalities, including network performance management, analytics, traffic management and policy control.

This whitepaper reviews encryption protocols, loss of traffic visibility and the associated adverse impact on network functionalities. It is aimed primarily at assessing technologies that can deliver encrypted traffic intelligence.

A key technology, in regard to this aspect, is deep packet inspection (DPI). Encrypted traffic has always been a challenge for DPI, especially when it comes to classifying traffic flows. This has been aggravated in recent years with the rise of the latest, more stringent encryption protocols such as TLS 1.3, QUIC and ECH.

Despite continuous advancements in DPI techniques, new encryption protocols have progressively obscured critical traffic information from DPI, rendering its normal product evolution inadequate to addressing the traffic visibility needs of today's networks. Hence, in order to continue supporting network functionalities that rely on real-time detection of applications and services, DPI must be complemented with cutting-edge methodologies, including machine learning (ML) and deep learning (DL).

This publication illustrates how the combination of advanced technologies including ML and DL have given rise to next-generation DPI technologies. These advancements are able to deliver in-depth visibility for traffic, not only for encrypted flows, but also for traffic that is obfuscated and anonymized.

This whitepaper shares findings from the research report "Deep packet inspection and encrypted traffic visibility for IP networks" published by ipoque, a Rohde&Schwarz company[4].

1) "Google Transparency Report." Google, Jan. 2023, transparencyreport.google.com/https/overview
2) "The Challenges of Inspecting Encrypted Network Traffic." Fortinet, Aug. 2020, www.fortinet.com/blog/industry-trends/keeping-up-with-performance-demands-of-encrypted-web-traffic
3) "2021 State of Encrypted Attacks." Zscaler, Oct. 2021, www.zscaler.com/press/zscalers-2021-encrypted-attacks-report-reveals-314-percent-spike-https-threats
4) "Deep Packet Inspection and Encrypted Traffic Visibility for IP Networks." ipoque, March 2023, www.ipoque.com/report-DPI-encrypted-traffic-visibility

2. TRENDS IN ENCRYPTION

As network threats evolve, so do the protocols for encryption, delivering a double-edged sword of enhanced data protection against an increasing lack of visibility.

Encryption protocols typically used for enterprise networks include:

- **Transport layer security (TLS)**, one of the most common encryption methods used for securing HTTP and other internet protocols. The latest version, TLS 1.3, addresses security and speed issues with features such as encrypted server name indication (ESNI) and forward secrecy at the cost of decreasing visibility by encrypting site names and preventing packet analysis.
- **Internet protocol security (IPSec)** is most commonly used for virtual private networks (VPNs) and secure tunnels, which conceal site-to-site traffic from third parties on public networks. While popular with enterprises relying on remote network access, VPN traffic can be difficult to monitor due to protocols like encapsulating security payload (ESP) that conceal packet payloads and headers.

While both encryption protocols offer robust security by concealing data and destination information from third parties, network administrators as well as malicious parties are left in the dark when it comes to identifying and analyzing traffic flows.

Encryption, however, is here to stay. With the proliferation of internet-supported applications and services, concealing user data is critical in protecting sensitive information sent over public networks.

On the user and application level, enterprises are leveraging encryption to provide secure messaging services. They also use it to protect card / bank transactions and personally identifiable information (PII) from being visible to third parties.

Encryption on the enterprise level protects confidential business transactions, client data and information flows between different network domains. With a growing number of employees accessing enterprise networks remotely, it is essential that traffic flows moving in and out of the enterprise network perimeter are secured end-to-end, regardless of how far and dispersed users are.

Modern network frameworks, such as secure access service edge (SASE), require network and application-layer encryption to support the delivery of cloud-based security and WAN services. Also, these technologies ensure compliance with industry standards and best practices.

As more critical data migrates to the cloud and exceeds traditional network borders, encryption will likewise evolve towards a higher degree of data anonymity, leaving networks with little clue of the traffic they handle.

Encryption, however, is here to stay. With the proliferation of internet-supported applications and services, concealing user data is critical to protecting sensitive information sent over public networks.

3. ENCRYPTION CHALLENGES AND IMPACTS

Encryption protocols and methodologies, as they stand, cannot sustainably provide holistic security which modern enterprises require. Despite the sense of security it may provide, gaps in the very implementation of encription and execution lead to significant opaqueness in the network. This can in turn lead to massive security risks, network performance issues and lost revenue.

3.1. Loss of visibility

The core issue with encryption is how it conceals critical application, packet and network data from network administrators and monitoring services. Managers are limited in their ability to identify which data is entering and leaving the network or where it is going. Applications become opaque. It becomes difficult to determine which and when applications are being accessed. Traffic and destination information is increasingly harder to monitor.

Similarly, malware and data breaches become harder to track. An administrator does not know if a packet is a normal service request, a Trojan horse or has a payload of sensitive information that should not leave the network. This, in turn, leads to compliance issues, as administrators are not able to determine if network data is staying within regulatory parameters or where security vulnerabilities are within the network.

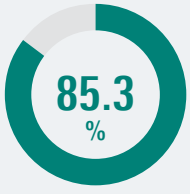
This results in a grievous impact on the network and the enterprise in terms of traffic management, analytics, policy control, performance management and security.

Especially for network environments comprising multiple clouds, servers, applications and variable access points, traffic management is essential. It ensures seamless delivery of packets throughout the network. Standard encryption practices prevent network managers from optimizing existing traffic routes or prioritizing traffic based on application requirements and traffic conditions, leading to slowdowns and resource inefficiencies.

Network analytics is also impacted by the abstraction level of encryption. It becomes difficult or impossible for tools such as network probes to gather granular traffic information that is needed to understand network behaviour across different types of protocols and applications. This impairs both short-term and long-term insights on the network, severely limiting an administrator ability to adjust network capacity and policies according to evolving traffic needs.

Policy management becomes a challenge since administrators are not able to execute application-based policy rules for different users and plan types. It also becomes impossible to determine unauthorized accesses to restricted applications and services. Likewise, it is extremely difficult to detect if legitimate users exceed application usage limits, require prioritization in terms of bandwidth allocation or need to be assigned different charging and pricing rules.

The impact on network performance monitoring is especially grave, possibly inducing extreme ramifications. Operations support systems become unable to respond to capacity and resource requests in a timely matter. It is impossible to diagnose impairments in QoS and attribute them to specific underlying applications that might be compromised or broken. The consequence is continuous poor performance across crucial services. The real-time analysis of user behaviour and network usage patterns lacks sufficient depth and granularity, leading to a slow response to complaints from users.



of networking vendors agree that the loss of traffic visibility, as a result of new encryption protocols, is a major concern for today's networks[5]

5) "Deep Packet Inspection and Encrypted Traffic Visibility for IP Networks." ipoque, March 2023, www.ipoque.com/report-DPI-encrypted-traffic-visibility

Ironically, encryption also has a negative impact on network security. While data navigating trough the network may be safer, intruders can still slip through the cracks of intrusion prevention systems by hiding malware among encrypted traffic. Encrypting and decrypting traffic reduces the performance of firewalls. Thus, administrators are not able to determine if an increase in traffic is due to a surge in site visitors or a distributed denial of service (DDoS) attack.

Encryption can also be used to hide malicious activity on the network. This includes data breaches and exfiltration when valuable data is intentionally tampered or copied out to unauthorized third parties. By mimicking the routine of authorized transactions, internal threat actors can camouflage their behaviour and keep their encrypted transactions undetected by data loss prevention tools.

Traffic management	Performance monitoring and management	Analytics	Policy control	Security
Routing	Service assurance	IP probes	Access and usage control	SIEM
Load balancer	OSS	DEM	User verification	ATP
Caching	QoS management	APM	Rating	NGFW
Compression	NPM	NPM	Charging	SD-WAN
Switching	SD-WAN	SD-WAN	SD-WAN	SASE
SD-WAN	SASE	SASE	SASE	SSE
SASE				CASB, ZTNA, SWG, DLP, IDS/IPS, FWAAS

Figure 1: Examples of networking functions impacted by encrypted traffic

3.2. A false sense of security

Encryption, in itself, comes with some inherent limitations. Despite being encrypted, traffic flows are still susceptible to some forms of attack such as:

- Downgrade attacks that exploit backward compatibility features in TLS 1.3 and older versions to gain the network encryption key or decrypt data into cleartext.
- Replay attacks that leverage TLS 1.3's 0-RTT session resumption feature – meant to increase traffic speed with easily-resumed user sessions – to copy requests and gain access to data. Ironically, encryption prevents administrators from seeing if these attacks are malicious copies or regular session resumptions.
- Brute force attacks, as attacker key/algorithm guessing systems become more advanced. Once an attacker has the key, the gates are basically unlocked.
- DNS tunneling that infiltrates servers by exploiting network protocols with a Trojan horse payload in domain name system (DNS) requests.

Contributing to these vulnerabilities is poor configuration within the network due to a lack of holistic management. Lack of diligence and unified monitoring, especially for larger and hybrid networks, can result in expired website certificates that can be exploited as an entryway into the network. Similarly, weak or outdated algorithms and systems running on older protocols can be used for downgrade attacks.

3.3. Practical deployment issues

Encryption can result in general network management overheads. Implementing and upgrading new encryption protocols can result in network downtime due to changes in software and hardware. These changes can quickly become unsustainable when not executed systematically, especially in decentralized networks.

Application, operating system and browser incompatibility lead to another issue, as upgrades may be unevenly applied if legacy systems are inoperable with new protocols. This may provoke both traffic management and security challenges and result in exploitation opportunities across the network.

3.4. Regulatory non-compliance

Non-compliance with regulations around sensitive data is another roadblock for encryption. Legal regulations and best practices in data governance dictate that data under the purview of acts such as HIPAA, the FTA Safeguards Rule, GDPR and others be strictly guarded and only accessible to authorized users within the network.

While encryption can protect data stored within the network, it prevents administrators from verifying the encrypted server certificates without inspecting the data – which is strictly prohibited by sensitive data regulations. Administrators thus have no means of seeing where sensitive data is headed in the network, as, once encrypted, it does not differ from other encrypted traffic.

4. THE IMPACT ON NETWORK OUTCOMES

Visibility gaps, as a consequence of encription, impact key traffic management and security functions and thus significantly affect network outcomes.

4.1. Performance impairment

Lack of fine-tuning, based on application/protocol metrics and rules, leads to blanket treatment of all traffic types. Services depending on ultra-reliable low latencies will be heavily impacted as bandwidth allocation remains rigid despite continuous degradation in user experience. Cloud gaming applications, real-time web conferencing and applications such as VR/AR will be severely impacted, leading to a loss of confidence in service reliability.

4.2. Higher network costs

Network inefficiencies due to poor optimization of network capacity and lags in policy responses can lead to huge CAPEX and OPEX in the form of increased computing and networking resources. Security breaches result in the need for more robust security systems, such as additional firewalls or monitoring services. Personnel time spent on manual configuration also increases, resulting in increased spend on wages and overtime.

4.3. Poor network decisions and design

Lack of granular traffic insights affect network design and planning. Deployment of additional WAN services such as content filtering and the use of load balancers and caching engines rely on detailed information on application usage and performance. Identification of critical applications contributing to network bottlenecks enable automated provisioning of additional capacity on MPLS links. The implementation of cloud and virtualized network functions requires insights on application performance. Without sufficient visibility into application traffic flows, network architecture remains unaligned to the needs of an enterprise.

4.4. SLA execution issues

Decreased visibility as a result of encryption can put service level agreements (SLAs) in jeopardy. Administrators are not able to ascertain if their network policies are delivering the intended KPIs. Consequently, they lose the ability to control and effectively fine-tune network parameters before users experience negative effects.

4.5. Poor application support

Encryption can impede application support services due to a lack of performance data at the transaction, service and application level. Issues relating to specific APIs, servers, clouds, links and even codes remain hidden as monitoring is confined to aggregated traffic measures. User and device issues and application abuse for example, cannot be relayed in real time to application managers as it takes many hours of diagnosis to single out the affected instances.

4.6. Threat detection impediments

Encrypted traffic renders many security tools ineffective. Existing and emerging encrypted threats can freely traverse enterprise networks, resulting in a surge in the frequency and volume of attacks. It will be no longer possible to use security inspection based on application risk profiles, as administrators resort to applying the same rigor to all flows. This will lead to an over-consumption of network resources. Additionally, the lack of application-level insights on past security events hinders the automated learning of threat patterns, necessitating threat intelligence updates to be implemented manually across the network.

70,6 % of networking vendors agree that encryption leads to an inability to identify and curtail threats, abuse and fraud;

52,9 % agree that encryption results in higher network costs; and

50 % agree that it impacts the ability to execute SLA-based plans[6]

6) "Deep Packet Inspection and Encrypted Traffic Visibility for IP Networks." ipoque, March 2023, www.ipoque.com/report-DPI-encrypted-traffic-visibility

5. USE CASES

5.1. SD-WAN and SASE

Secure access service edge (SASE) combines automated, multi-cloud, software-defined wide area networking (SD-WAN) with secure service edge (SSE) – an architecture that delivers security services from the cloud. SASE is highly dependent on encryption for protecting traffic flows traversing its points of presence, as both internal and external users access enterprise applications and data.

Encryption, however, can also significantly impact SASE's performance and service delivery as it leads to a loss of traffic visibility. This impairs not only cloud-based security applications such as zero-trust network access (ZTNA) and next generation firewalls (NGFW), but also traffic management functionalities such as routing and optimization.

Intelligent traffic management deployed in SD-WAN, for example, requires real-time insights into the underlying traffic flows. Without such visibility, traffic that can be offloaded to the Internet may be suboptimally transported over expensive MPLS routes. Also, low-latency applications may be backhauled to the main data center instead of being processed at the edge, closer to the user. Application visibility is also a pre-requisite for SD-WAN's application-aware networking. Its network policies are based on the sensitivity of applications to network conditions and user requirements.

Unified performance management, central to streamlining traffic policies across multiple nodes within a SASE network, becomes impossible when administrators fail to identify the underlying applications. The consequences are stand-alone policy decisions and ad-hoc resolutions to issues.

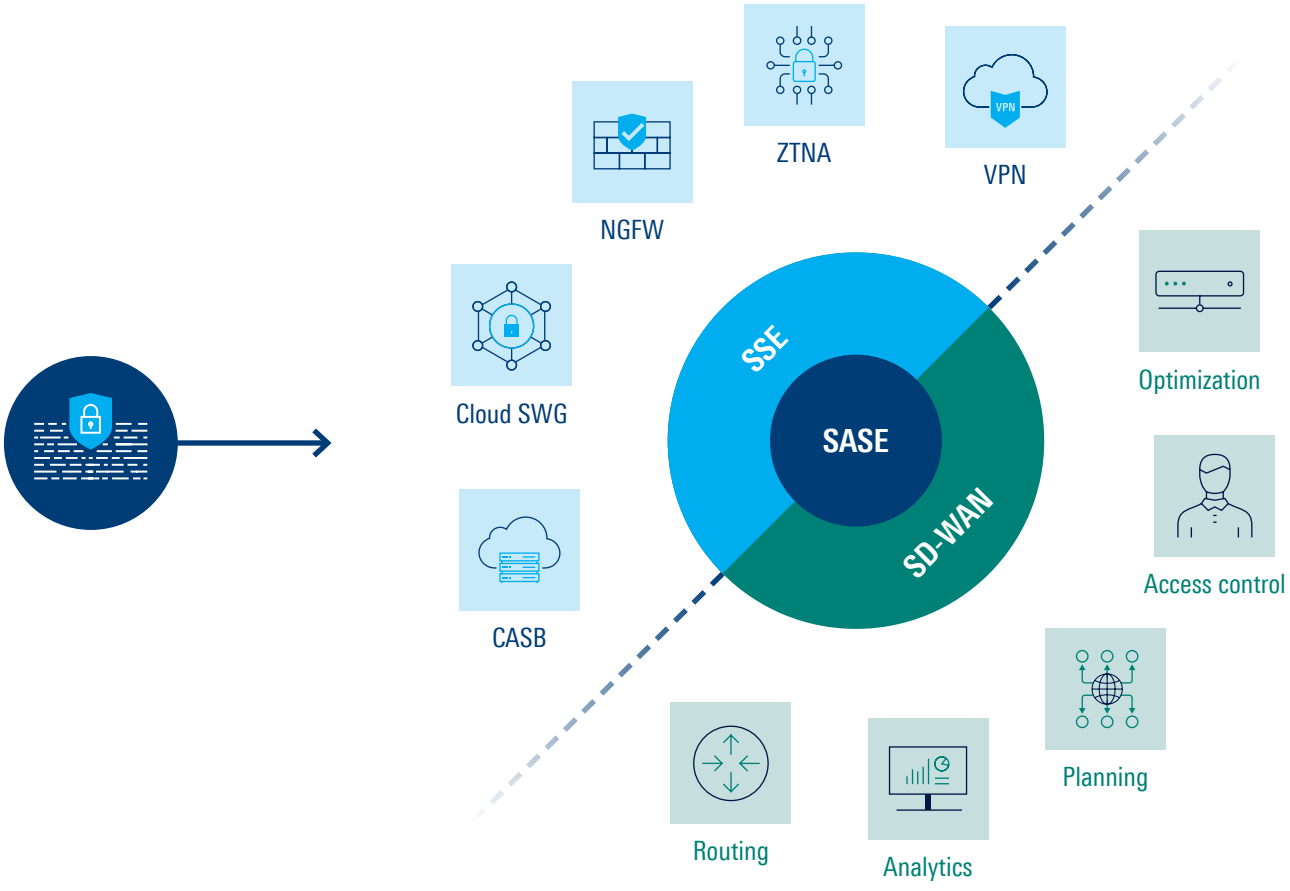


Figure 2: Networking functions within SD-WAN, SSE and SASE that are impacted by encryption

Without working knowledge of application usage patterns and user behavior, administrators are not able to automate network decisions. This leads to a high degree of manual configurations and human intervention, especially during times of volatility.

Additionally, SASE networks require the ability to inspect traffic at cloud scale. Additional rounds of traffic filtering to ascertain the nature of the underlying applications can easily introduce unwanted processing lags.

Threat management also becomes difficult. This is especially risky given that cloud-based architectures such as SSE often rely on digital identities and traffic intelligence derived at distributed PoPs to connect users to respective resources. With encryption, SSE services such as CASBs and NGFWs are no longer able to discern attack patterns or ascertain if sensitive data is leaving the network. Additionally, the process of decrypting and encrypting traffic can slow the network and hinder real-time responses to threats.

In the case of VPNs, once a session is established, administrators can no longer identify if the traffic is malicious. They also lose the ability to monitor user behavior, preventing the identification of threats or suspicious activities that can potentially jeopardize the network.

Overall, encryption, when implemented blanketly, can disrupt the balance of speed and security that SASE and cloud networks promise to deliver, resulting in lower performance, inefficiencies and poor user experience.

5.2. Telecom networks

Encryption protects voice, text and data communications on telecom networks. It safeguards traffic flows from being intercepted or tampered by third parties. Encryption however makes network monitoring, services assurance, policy control and security more difficult to manage.

5.2.1. Monitoring and analytics

To support millions of users and thousands of applications, operators require deep network analytics. Monitoring user requests, measuring network capacity from the RAN to the core, and identifying traffic load from different applications requires monitoring tools such as IP probes to record detailed information of the underlying applications and services. With more packets encrypted, such tools lose the ability to produce a complete view of the underlying flows. This lead to obvious gaps in traffic analyses, affecting analytics-dependent functions such as network optimization and service assurance.

5.2.2. Slicing, edge processing and automation

Network slicing, a critical part of managing traffic flows on 5G networks, becomes difficult with encryption. This includes the instantiation of network slices for different use cases such as eMBB, URLLC and mMTC and their continuous optimization.

Edge processing for low-latency and mission-critical applications such as autonomous driving, industry 4.0 and V2X communications rely entirely on traffic being identified in real-time and routed for processing at the edge.

AI and ML for autonomous networking are also affected, as both functions require granular traffic information. Without them, it becomes impossible to develop the algorithms needed to support the dynamic instantiation of virtualized instances and automated provisioning of capacity and network functions.

5.2.3. BSS and policy control

Encrypted traffic hinders policy engines from identifying the underlying applications and services. Zero-rating of selected applications becomes challenging. This can impact various user groups - from airplane passengers attempting to access tiered Internet services, to emergency services getting billed for using exclusive channels during times of crisis.

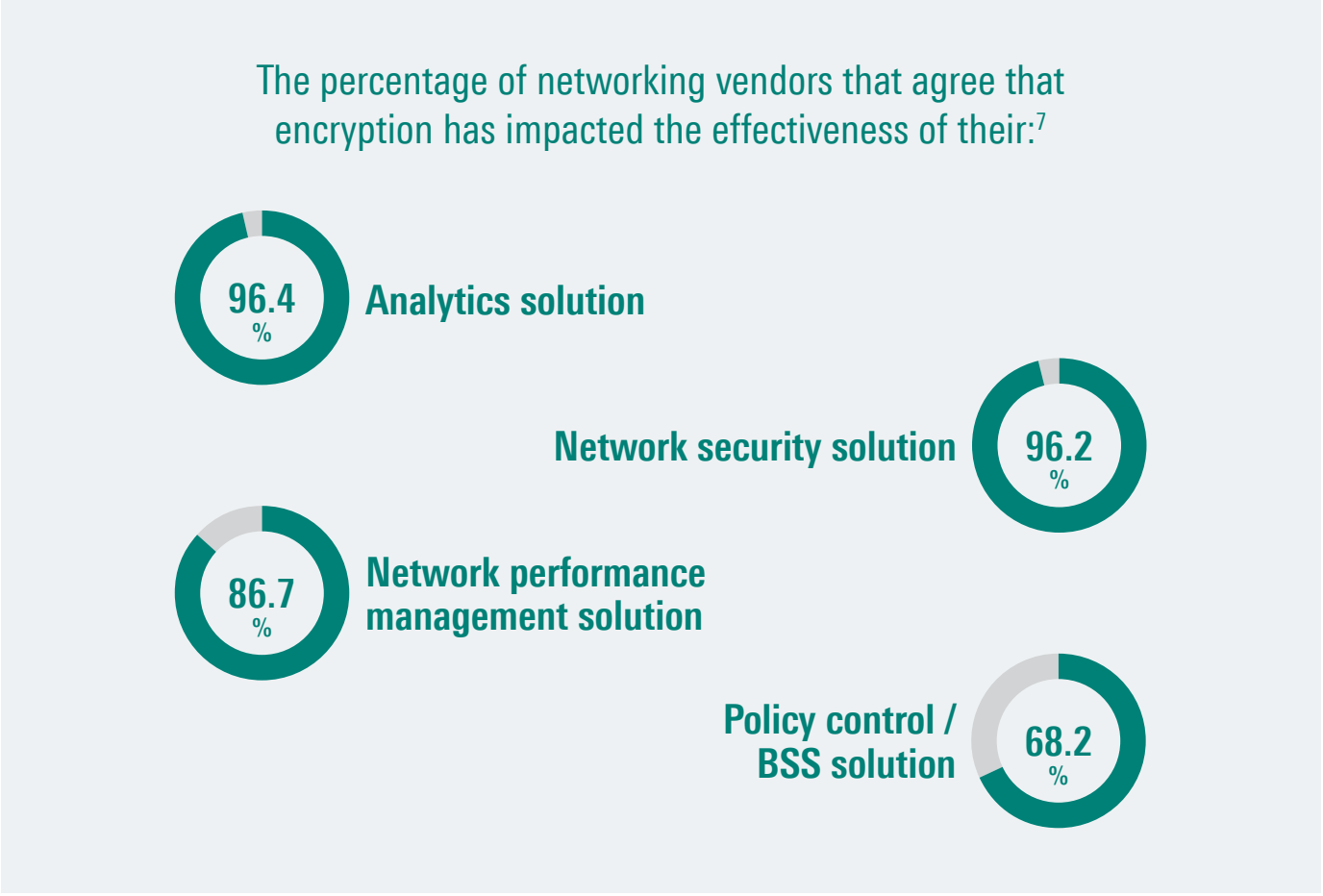
Implementing innovative service plans that drive operator monetization also requires real-time traffic intelligence. A video-streaming application that is charged at only a fraction of the usual rate, as part of a 5G mobile deal, must be differentiated from all other traffic originating from the same user. With encryption, such differentiation becomes impossible.

5.2.4. Security

There are many instances where encryption harms operator networks. Ransomware attacks that are encrypted are a good example. Targeting sensitive subscriber data, perpetrators often launch ransomware attacks on operator IT systems. This exposes subscriber credentials, resulting in both reputational and legal repercussions. It can also impact network operations if ransomware attacks escalate into data infiltration.

Malware attacks on IoT networks are another example, where encryption can be manipulated by threat actors, in this case infecting user and IoT devices. These devices are then programmed to mount DDoS attacks on neighbouring base stations as part of a jamming attack, impacting operator services.

Encryption can also be exploited to mask fraud and abuse on operator networks. The anonymity provided by encryption results in standard security tools not being able to detect illegal tethering, SIM cloning and rogue base stations as irregularities in the use of applications and protocols are not readily visible.



7) "Deep Packet Inspection and Encrypted Traffic Visibility for IP Networks." ipoque, March 2023, www.ipoque.com/report-DPI-encrypted-traffic-visibility

6. TOOLS FOR VISIBILITY INTO ENCRYPTED TRAFFIC

There are several tools and methodologies that reinstate a modicum of opacity and control into the network. These methodologies offer varying degrees of visibility into encrypted traffic and are based on different architectures and implementation systems.

6.1. SSL/TLS inspection

SSL/TLS inspection decrypts network traffic to achieve complete visibility into the payload of an encrypted packet.

SSL/TLS inspection is often deployed in a middlebox, such as a firewall or an intrusion detection system (IDS). This middlebox acts as a man-in-the-middle that intercepts network traffic, decrypts its SSL/TLS connection via a proxy server and a proxy certificate, analyzes the payload of the packet and then re-encrypts it.

When using this method, plaintext HTTP data is entirely exposed to networking functions and network administrators.

Limitations

SSL/TLS inspection has its own shortcomings as listed below:

Security
When decrypting data to be forwarded to inspection services, proxy servers transport and expose plaintext data within the network and create potential for breaches or interceptions. This allows attackers to not only access the data but also potentially access the network encryption key.

Regulatory
Healthcare, banking and other sensitive data sets are protected by law in many countries, preventing the decryption and inspection of the data that is attached to PII. This prevents or restricts entry-level inspection of data within the network and completely invalidates proxy server methods.

Resource utilization, high latency decryption, inspection and re-encryption consume both time and network resources. These procedures can quickly eat up processing power within a server, robbing it from critical functions and resulting in additional latencies.

Application blocking
Not all applications and clouds accept inspected traffic. Apple applications, for example, prevent packets that have undergone decryption due to internal security policies, requiring network owners to disable these features.

Lack of compatibility
TLS proxy servers, when configured to the latest standards, may prove incompatible with clients using older protocols or keys, such as RSA. While this can help prevent security issues from backward compatibility, many e-commerce and email suites still rely on RSA to encrypt messages and transactions.

Limited functionality
Certain middleboxes are able to inspect packets without decryption by inspecting the packet headers. This allows them to route the packet to its destination or filter packets from unauthorized sources. However, packet headers encrypted with SNI or full disk encryption are impossible for middleboxes to read, and thus cannot be processed without being decrypted.

Configuration issues
Server proxies require certificate authentication in order to authenticate host servers and establish trusted sessions before decrypting the data in question. However, depending on how the host server is configured and which browser the user is using, requesting the certificates and negotiating with the certificate authority can be time consuming and often has to be managed manually.

6.2. Behavioral / statistical analysis and heuristics

Behavioral / statistical analysis and heuristics rely on the physical attributes and movement patterns of packets to identify the underlying applications. These include static information such as the packet size and packets per flow, as well as dynamic data such as changing arrival times at every node.

Raw data captured in the system is processed to produce statistical outputs such as means, averages, variances and correlation coefficients for a wide range of measures such as throughput, speeds, latencies, inter-packet gaps/rates and packet loss.

This information, combined with packet metadata, allows classification of traffic into applications and services, without the need to decrypt and re-encrypt packets. Unique behaviour and statistical characteristics that correspond to known applications and threat patterns reveal the underlying applications and services to network administrators, enabling them to execute application-based policies.

Using behavioral / statistical and heuristic analyses for network decisions has its downsides. It may block legitimate users and traffic patterns, especially if the network is being accessed during unusual circumstances, for example a surge event. Additionally, collecting and inputting relevant behavioural data can be resource intensive, especially if the network requires continuous adaptation.

6.3. Machine learning and deep learning

Machine learning (ML) and deep learning (DL) take traffic analysis a step further by applying granular data patterns to adaptive algorithms. As a result, they allow for a more fine-tuned control of the network that adapts to new circumstances without the need for manual configuration.

These algorithms include the following assets. K-nearest neighbors (k-NN) enables filtering and data labeling in the network based on the range of data offered. Decision tree learning can apply policy based set parameters and adapt those parameters to new situations. Convolutional neural networks (CNN) can adaptively label and filter datasets. Recurrent neural networks (RNN) are used to recognize data patterns and respond according to the sequences presented. Long short-term memory (LSTM) is able to classify and process data sequences.

By their adaptive natures, ML and DL can respond more dynamically to network issues, enabling them to detect threats, identify bottlenecks and determine optimal network routes, even when faced with new datasets and circumstances.

Monitoring encrypted traffic:[8]

70,6 % of networking vendors use tools based on behavioural and statistical / heuristic analysis

55,9 % use tools based on machine learning and deep learning

52,9 % use tools that decrypt traffic for inspection

8) "Deep Packet Inspection and Encrypted Traffic Visibility for IP Networks." ipoque, March 2023, www.ipoque.com/report-DPI-encrypted-traffic-visibility

7. ML-POWERED DPI FOR ENCRYPTED TRAFFIC INTELLIGENCE

Using DPI to deliver real-time insights on IP traffic flows has been continuously challenged by encryption. In recent years, this limitation has been compounded by the introduction of newer, more complex encryption protocols, leading to a significant erosion in the ability of conventional DPI tools to classify encrypted applications and services.

ipoque, a Rohde&Schwarz company, addresses this limitation by enhancing its DPI solution with advanced ML and DL technologies, creating a future-proof solution that delivers granular, real-time insights and enhanced, end-to-end traffic intelligence for encrypted traffic flows.

The ipoque DPI engines, R&S®PACE 2 and R&S®vPACE, deliver these insights by combining original DPI technology rooted in signature-based pattern matching, statistical, heuristic and behavioral analysis, with encrypted traffic intelligence (ETI). ETI combines multiple highly-optimized ML and DL algorithms including decision tree learning, k-NN, CNN and RNN, along with high-dimensional data analysis. These algorithms boast over thousands of features, including statistical, time series and packet-level features. Enhancing encrypted traffic insights with DNS and service caching, R&S®PACE 2 and R&S®vPACE offer a holistic solution that circumvents the shortfalls of conventional DPI and middlebox solutions.

Visibility provided by R&S®PACE 2 and R&S®vPACE can be extended to obfuscated and anonymized traffic, enabling administrators to analyze traffic attempting to bypass network blocks, ISP throttling and IP bans.

Both engines can be embedded into hardware devices or integrated with cloud / virtualized functions in an abstracted architecture, allowing for simplified deployment in any part of a virtualized or hybrid network. Additionally, the engines can scale to environment-dependent packet processing, allowing networks to adjust their filtering capacity to traffic and application count. R&S®PACE 2, in particular, is configured to meet the needs of traditional architectures, while R&S®vPACE is a perfect fit for VPP-based cloud-native and heavy load computing environments. With built-in ETI capabilities, both engines boast zero performance and memory penalties.

DPI's capabilities

R&S®PACE 2 and R&S®vPACE's DPI capabilities for encrypted traffic extends to the following functions:

- **Protocol classification**
  Enabling network and flow level analytics, as well as detection of traffic irregularities and malicious activity
- **Application / service type classification**
  Allowing usage control and timely execution of network policies and security filtering based on different application risk tiers
- **Application classification**
  Enabling monitoring of application performance and security; and allowing granular policies for user access, traffic management and resource triage
- **Application usage classification**
  Delivering insights on application usage, impact, and resource utilization
- **Operating system and browser classification**
  Enabling monitoring of patterns in user behavior and devices while identifying relevant security vulnerabilities
- **Threat detection such as DNS tunnel detection**
  Enabling identification and blocking of external tunneling threats

Both R&S®PACE 2 and R&S®vPACE can be deployed on all ends of a network and remain updated with ipoque's library of traffic signatures, refreshed on a weekly basis. ipoque continually tests and improves its traffic detection technologies, addressing not only existing encryption protocols such as TLS 1.3, QUIC, ESNI and DoX, but also newer and more complex protocols that are yet to be released.

Leveraging the insights from R&S®PACE 2 and R&S®vPACE, network functions can be enhanced with added functionalities, while operators can deploy new services or plan types to improve monetization.

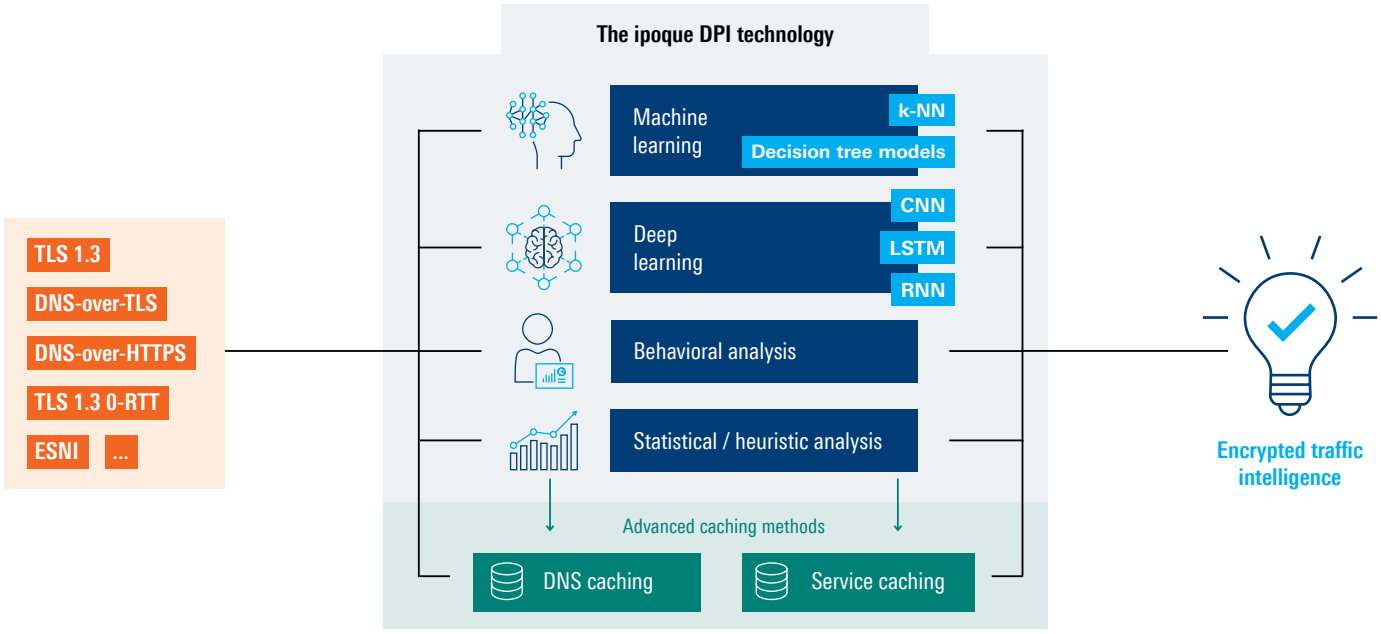


Figure 3: ipoque's encrypted traffic intelligence

8. CONCLUSION

Rapid digitalization and the growth of network complexities call for advanced means of securing and protecting traffic and network assets. This drives new advancements in encryption, obfuscation and anonymization techniques. These techniques inadvertently limit the visibility and control administrators have over their networks.

This whitepaper presents the findings of Rohde&Schwarz' research report 'Deep packet inspection and encrypted traffic visibility for IP networks'[9]. It is aimed at discussing the relationship between encrypted traffic and DPI, which is one of the key technologies used in identifying traffic flows in IP networks.

DPI faces numerous challenges as the share of encrypted traffic continues to rise. This document demonstrates how this is exacerbated by the introduction of newer and more sophisticated encryption protocols such as TLS 1.3. Additionally, tougher key exchanges and algorithms continue to restrict the traffic insights available to DPI tools. Another key point is how minimized visibility due to encryption impacts key network functionalities, such as security, analytics, network performance management, policy control and traffic management. This adversely impacts network performance, network costs, planning decisions, SLA fulfilment, application support and threat management.

The effectiveness of existing techniques for decrypting traffic, namely SSL/TLS inspection, is assessed. Concerns that limit the use of SSL/TLS inspection are also discussed. These include security, regulatory pressures, latency implications, compatibility issues and the need for extensive configurations.

The publication further highlights the importance of complementing existing DPI technologies with advanced methodologies, specifically ML and DL. Drawing examples from Rohde&Schwarz' suite of DPI solutions, this whitepaper illustrates how the incorporation of ETI, including cutting-edge ML / DL techniques, circumvents the limitations associated with conventional DPI. It demonstrates how ETI-powered DPI reinstates network visibility and delivers reliable and accurate, real-time classification of protocols, applications and services for encrypted traffic.

Ultimately, advanced DPI paves the way for granular performance and security analyses. Armed with such data, administrators are able to gain deep insights into the network and regain the control that encryption has wrested from them – allowing for a network that is safer, highly efficient and intelligent.

9) "Deep Packet Inspection and Encrypted Traffic Visibility for IP Networks." ipoque, March 2023, www.ipoque.com/report-DPI-encrypted-traffic-visibility

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 3683.9692.52 | Version 01.01 | March 2023
White paper | Session and subscriber awareness in mobile core networks

3683969252
3683.9692.52 01.01 PDP 1 en