ENEA

Industry Guide

Traffic Visibility: The Fast Path to SASE Success

In the Secure Access Service Edge (SASE) framework, wide-area networking and cybersecurity are fully merged and delivered as a distributed cloud service. This simplifies network management and boosts performance by bringing users and resources closer together. SASE also enhances security by segmenting traffic and applying rules according to the unique profile and context of each traffic flow.

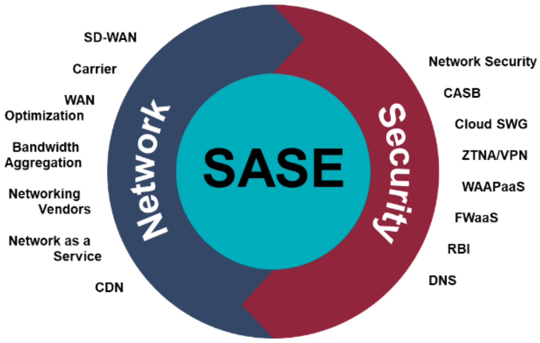
To successfully deliver on these SASE promises therefore requires comprehensive, real-time traffic visibility. It is this visibility that enables consistent, outstanding performance across today's continuously evolving, complex and distributed networks.

To achieve this visibility, SASE market leaders use a variety of inspection techniques that combine advanced traffic classification with new inspection methods to meet the very specific demands of the SASE framework. From accurately identifying applications from the first packet, even in encrypted traffic, to providing unique insights into users, devices, content and flows, this new approach provides the contextual foundation upon which superior SASE solutions are built. This guide outlines the technology and methods used by successful vendors whose offerings are already leading the way in SASE.

Helping Vendors Get on the Fast Path to SASE Success

Within the space of only a couple of years, SASE has evolved from a concept to market-ready products within a competitive field. Analyst firm Gartner sees SASE as “the fastest growth opportunity in the networking and network security market”, predicting that end-users will spend $6.8 billion on SASE in 2022 (a vertiginous rise of 42% from $4.8 billion in 2021)[1]. And they are not alone. Venture capitalists have invested 100s of millions of dollars in SASE providers, while software vendors are scrambling to acquire companies to round out their SASE offers.

$6.8B
2022 SASE Spending Forecast



As conceived by Gartner in 2019, SASE is a model in which WAN and cybersecurity are fully converged and delivered as a cloud service, with a distributed edge architecture that brings computing resources closer to the end users who need them.

The rapid adoption of SASE is not so surprising when you consider that shortly after the framework was introduced, there was an abrupt shift toward mobile work with the arrival of the covid pandemic, accompanied by an acceleration in the migration to the cloud. Within such a dynamic environment, SASE offers enterprises an appealingly simple solution to the challenge of delivering secure, anywhere/anytime access to applications and services.

The problem for vendors is that delivery of such a convenient solution is anything but simple. To ensure success in such a volatile market and reap the financial rewards, vendors need to understand the dynamics that are shaping SASE so that they can build a solid framework and a future-proof roadmap.

At Enea, through our Qosmos technologies, we’ve worked with start-ups and industry veterans to help them reap these rewards by addressing one of the most important challenges for SASE vendors: maintaining real-time, application-level traffic visibility across diverse, distributed networks. As a result, our technologies are used by four of the top five SASE solution providers.

This brief aims to guide vendors through the complex world of SASE, outlining at each stage the approaches, methodologies and traffic intelligence technologies used by successful solution providers for effective network control and security. Using this as a foundation, you can build solutions that deliver on the promises of SASE and join the market leaders on the fast path to success.

1. Gartner, Inc. 2022-2025 predictions: https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences

SASE Visibility Challenges & Solutions

Challenge 1: The Difference in Edge and PoP Visibility Requirements

In conventional network architectures, traffic visibility needs are often met by decrypting all traffic and running it through a deep packet inspection (DPI) engine. It is a familiar strategy, but one that is ill-suited to the scale and distributed nature of SASE solutions, especially as evolving encryption standards make decryption more complicated and expensive. In SASE, Edge and PoP visibility needs are very different, except in the case of hybrid SD-WAN/SASE deployments in which some Edges require advanced services normally performed at the PoP.

It is therefore necessary to have adaptive traffic intelligence that meets the diverse visibility needs of SASE Edges and PoPs, and delivers critical classification information without requiring decryption.

At the Edge

At the SASE Edge, rapid and reliable traffic identification is key. Applications and service categories, as well as important security indicators, need to be available from the very first packet. This enables safe, high-performance Internet breakout.

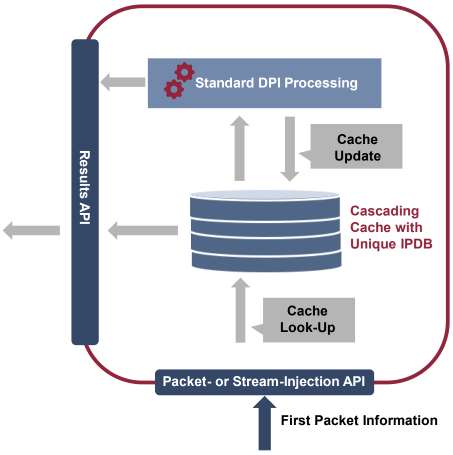
For locations that require on-premise security and more sophisticated application-based routing (hybrid SD-WAN/SASE deployments, for example), full DPI capabilities will be required at the edge.

At the PoP (or SD-WAN Edge in Hybrid SASE)

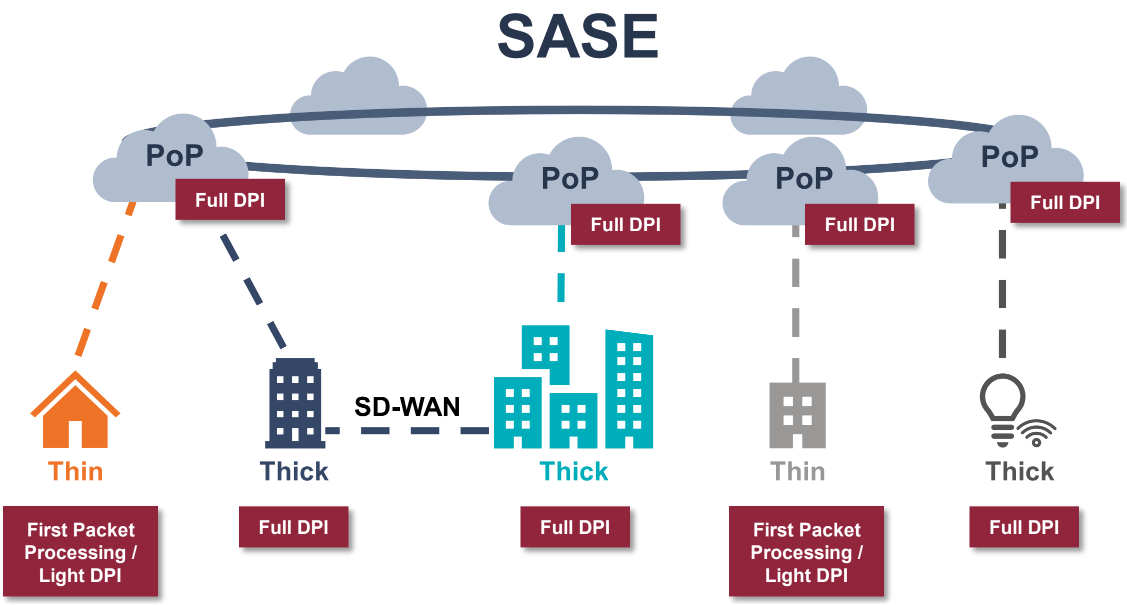
Within the PoP, highly scalable traffic classification, metadata generation, file extraction and deep packet inspection are necessary to support advanced traffic orchestration and cybersecurity services.

First Packet Processing

This example of first packet processing uses an innovative multi-tier cache system to boost application recognition and significantly improve accuracy.



Traffic Visibility Requirements in SASE Solutions



Examples of Edge and PoP Functions Requiring Traffic Visibility

Thin Devices

App/svc-based Routing to PoP
Optional NGFW Functions

Thick Devices

DLP
SWG
NGFW
Router

PoPs

Cloud Optimization
WAN Optimization
Global Route Optimization
Cloud Firewall with NGFW Capabilities
ZTNA segmentation
SWG
Advanced Threat Prevention

Dynamic traffic steering and the sharing of DPI results among multiple SASE functions are examples of additional capabilities that can be deployed to support diverse traffic intelligence needs and increase operational efficiency.

Raising SASE Performance: Traffic Steering

In a conventional service chain architecture, traffic is run through all networking and security functions in a serial fashion, with the same traffic decrypted, processed with DPI, and re-encrypted by each function. SASE demands a higher performance model.

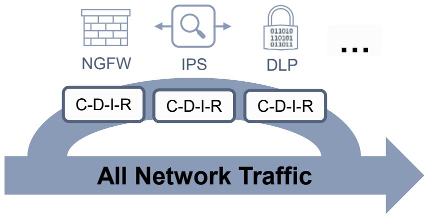
> **Selective decryption** minimizes the time and resources required to extract essential traffic intelligence.

One such model is the steering model, in which upstream encrypted traffic analytics are used to determine if a given flow should be decrypted for in-depth inspection or not, and if so, by which functions (IPS, NGFW, DLP, etc.).

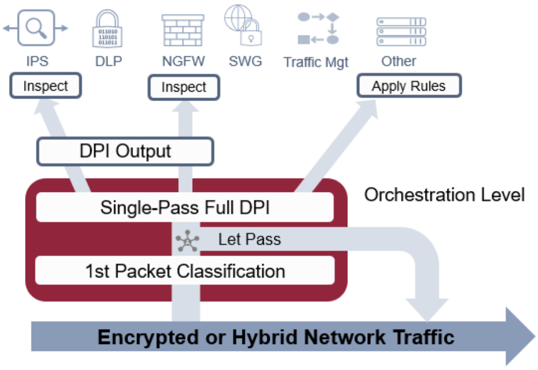
Using advanced DPI, it is possible, for example, to identify one encrypted flow as an MS Teams audio call, which does not require decryption, and another as a SharePoint file transfer, which does require decryption and content analysis.

Conventional Service Chaining

C-D-I-R: Classify-Decrypt-Inspect-Re-encrypt



Steering Model with Single-Pass DPI



Raising SASE Performance: Single-Pass DPI

When decryption and full DPI must be used, running DPI once and sharing the results (i.e., single-pass DPI) provides another way of maximizing SASE performance. Flexible form factor options enable further customization such as deployment as a standalone CNF for microservice environments.

Challenge 2: Maximizing Visibility Without Impacting Performance

DPI is the industry standard for meeting advanced traffic visibility needs. Given the critical role traffic intelligence plays in SASE, DPI is a must. But the performance demands on SASE are very high, and DPI can be a resource-intensive technology.

When seeking traffic visibility for SASE, it is therefore essential to deploy a DPI solution capable of minimizing resource requirements. One option is to maximize the use of first packet processing. However, not all first packet processing capabilities are the same, and whatever DPI solution is selected, it must support the strategic use of full DPI when required. For SASE, first packet processing needs to be fast, reliable and very accurate. In full DPI mode, the solution should include advanced features like extensive security metadata and full, multi-layer visibility into encapsulated protocols.

Other important performance capabilities include:

- Optimized multi-thread support for high scalability
- High performance under heavy metadata extraction loads
- Optimized code for the industry’s highest performance multicore processors
- Optimized integration with packet processing middleware (e.g., Intel DPDK)
- Support for VPP and hardware acceleration and offloading

Challenge 3: Preserving Visibility in Encrypted Environments

Universal, real-time application-awareness is a requirement for SASE. However, changes in encryption standards and the high-performance demands of SASE make it difficult for standard DPI to deliver adequate visibility in encrypted environments. Advanced DPI solutions use a variety of techniques to accurately classify encrypted flows. These include:

Handshake Analysis
Extraction of metadata in handshake messages that precede encrypted packets, and which remain clear

Binary Pattern Analysis
Detection & matching of binary patterns against known applications and services

Statistical Analysis
Analysis of packet and flow characteristics

Behavioral Analysis
Analysis of encrypted session behavior versus characteristic protocol behaviors

IP Address Analysis with IPDB
Analysis via a multi-tier cache that uses an Internet Protocol Database (IPDB) with 100s of millions of continuously updated, DPI-validated IP address/ application matches to accurately identify applications from the first packet

Advanced first packet processing can reliably identify:

- Applications
- Key Categories
- Security Indicators

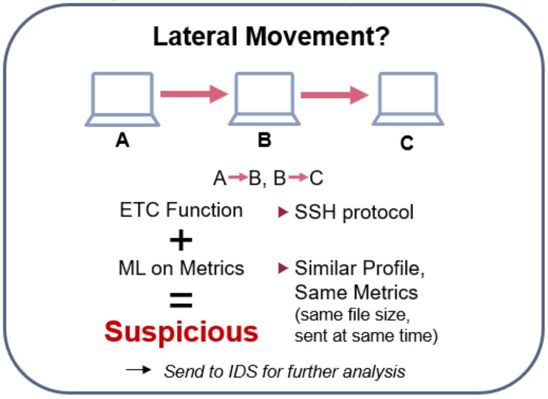
Full L2-L7 inspection of decrypted traffic extracts intelligence about:

- Applications
- Services
- Content (payload)
- Security Indicators
- Users
- Devices
- Flows, and more, with 1000s of types of metadata produced

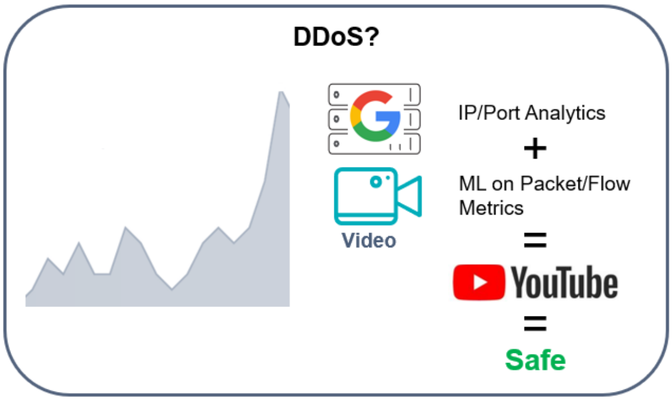
Machine Learning
The use of machine learning to boost the accuracy and service level granularity of first packet processing, to categorize applications and services, and to help identify potential security threats in fully encrypted traffic (i.e., traffic in which the handshake and other remaining clear data are obfuscated).

Machine learning can be combined with other techniques to support visibility, threat detection and analysis needs in fully encrypted streams.

Ex: Use existing ETA function & ML to detect possible lateral movement


Lateral Movement?
A
B
C
A→B, B→C
ETC Function
▸ SSH protocol
+
ML on Metrics
▸ Similar Profile, Same Metrics
(same file size, sent at same time)
=
Suspicious
→ Send to IDS for further analysis

Ex: Use IP/Port Analysis + ML to determine if a traffic spike is a possible DDoS



Challenge 4: Insight into Potential Threats

Whether a given flow is encrypted or not, advanced persistent threats continue to increase in frequency and sophistication and are inflicting higher levels of damage. So, a successful SASE solution needs to have a very robust, network-based threat detection and response capability. The performance of the NDR (Network Detection and Response) component is dependent on the quality and level of information it receives about the network traffic. Key factors are the range of protocol coverage and access to extracted and computed metadata, including, of course, security-related metadata. The more granular the traffic visibility, the more effective and accurate the NDR will be in the detection of evasive techniques.

This list gives examples of evasive techniques and the role played by traffic intelligence in detecting them:

- **Complex Tunneling**
  By identifying full protocol paths through multiple levels of encapsulation, advanced traffic intelligence will reveal traffic that is using complex tunneling.
- **Virtual Private Networks (VPNs)**
  The accurate identification of dozens of VPN applications, including those most commonly deployed for malicious activities, helps to detect malware.
- **Anonymizers**
  Anonymous proxy services can cloak harmful activities. Advanced traffic intelligence provides detailed information on these services, including those using multiple layers of encryption, to reveal any unusual or threatening activity.
- **Covert Communication Channels**
  DPI-based traffic identification can detect non-standard tunneling activities over legitimate protocols such as DNS or ICMP, which may indicate unauthorized or illegal activities.

> The more granular the traffic visibility, the more effective and accurate the NDR will be in the detection of evasive techniques.

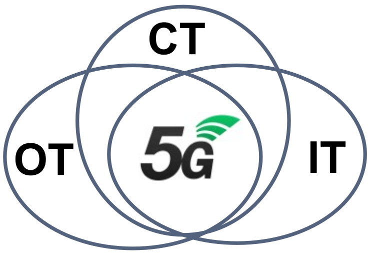
- **Domain Fronting**
  Routing schemes in Content Delivery Networks (CDNs) and other services can be used to mask the intended destination of HTTPS traffic (direct or tunneled). Traffic intelligence software will reveal the real use of these schemes.
- **Traffic Spoofing**
  Detailed traffic visibility will reveal applications (e.g., eProxy, HTTP Injector) that combine techniques such as protocol header customization, proxies, tunneling & domain fronting, to evade detection.
- **File Spoofing**
  Granular traffic intelligence will highlight inconsistencies such as a false MIME type or a mismatch between the original hash and computed hash.
- **P2P Misuse**
  The classification of P2P traffic supports forensics and behavioral modeling of network traffic to identify any misuse.

Challenge 5: Maintaining Complex Visibility Technology in a Fast-Moving Market

SASE, IT/OT/CT Convergence, and 5G

SASE not only represents the convergence of networking and security functions, it also brings together IT (information technology) and OT (operational technology) as enterprise networks expand and evolve to include new types of connected objects and edge cloud services.

Over the next decade, 5G will accelerate this IT/OT convergence, while adding communication technology (CT) to the mix. For 5G is not just the next in the series of 2G/3G/4G standards for wireless transport technologies. It is a complete architectural rewrite of the communications infrastructure. The 3GPP 5G specification is essentially a next-gen software-defined wide area network (SD-WAN) framework that reaches all the way back to the radio access network (RAN) and out to the clouds. It is, to put it simply, a blueprint for cloud-native, secure SD-WAN – just like SASE.



With 5G, a vendor can spin up an end-to-end virtual network that offers just the right connectivity and computing resources for a given use case, customer and/or application, and deploy this virtual private network across a shared, multi-tenant 5G infrastructure (i.e., advanced network slicing). This slicing capability plus 5G’s revolutionary latency, throughput and reliability capabilities will enable a wealth of new industrial, business and consumer services. And these use cases will blur the line between communication, information, and operational technologies to the point of vanishing.

What Does this Mean for SASE vendors?

First, this means current SASE vendors will face new competition from ‘5G SASE’ vendors entering from adjacent markets. Second, it means SASE vendors have to be prepared to meet the needs of the new generation of applications enabled by 5G (especially private 5G). This means SASE vendors should embrace a more holistic view of what constitutes a ‘network’. They should think of themselves as being in the IT, OT and CT business all at once as they develop their roadmaps and M&A strategies. They also need to pay special attention to the depth and breadth of traffic intelligence their DPI technology can provide. SASE vendors should ensure the DPI technology chosen provides deep support for consumer and industrial IoT, OT (SCADA/M2M) and CT protocols and applications, and integrates well into the cloud-native architectures common to both 5G and SASE. Finally, SASE vendors need to decide whether they should source or develop the traffic intelligence technology required to get the type of coverage and integration they seek.

Traffic Intelligence Technology – The Big Question: Build or Buy?

This is a question that many vendors ask. On paper, developing DPI-based traffic intelligence can look like an attractive and cost-effective solution to network visibility needs - especially if you use open source software. However, fully functional DPI is a very complex and constantly evolving technology. It requires a large, dedicated and highly specialized team to maintain. Given the competitive and fast-changing nature of the SASE market, trying to develop and maintain DPI in house can have a negative impact on time-to-market and competitiveness while open source DPI is insufficient in quality and performance to support SASE success.

The solution is to outsource DPI and traffic intelligence, embedding the technologies as a software component. There are commercial traffic intelligence products available that have been developed by dedicated experts over many years. The quality and level of detail is impossible to reach within project timelines by in-house developers. In addition to huge, ready-to-use protocol libraries, these products also use a variety of custom techniques to identify and classify encrypted traffic and provide full network traffic visibility. These ready-to-use components not only accelerate product development cycles, optimize costs and lower risks, but they also ensure that visibility levels are maintained over time through constant monitoring and updating of the protocol libraries.

Some commercial solutions propose integration accelerators to help speed and simplify deployment. They can include:

- **Optimized integration** with packet processing middleware (e.g., Intel DPDK).
- **Support for Vector Packet Processing (VPP) and Hardware Acceleration and Offloading**, with configuration options for optimal integration with custom flow managers.
- **Independent core-decoding framework** and protocol plugin library, which translates into fast flow signature updates while preserving engine stability. (Protocol plugins should always be hot-swappable.)
- **A highly configurable flow manager architecture** that can handle standard, tunneled and multiplexed flows while allowing different memory allocation modes with maximum flexibility.
- **Support for multiple instances of the DPI component** for maximum implementation flexibility.
- **Professional services** that can help with configuration and integration. They can speed deployment and ensure that product capabilities are fully leveraged within the SASE solution.

Conclusion

Every vendor has a unique approach to designing and implementing a SASE architecture, but all SASE solutions share a common need for universal, real-time application awareness.

This is a must-have for every networking and security function within SASE, such as SD-WAN, NGFW (Next Generation Firewall), CASB (Cloud Access Security Broker), SWG (Secure Web Gateway), DLP (Data Loss Prevention) and TDR (Threat Detection and Response).

To reap the full potential of SASE, it is essential to have full traffic visibility that adapts to the different needs of the network, providing rapid flow categorization and routing at the edge and granular details at the core, whether traffic is encrypted or not. This requires a high performance, commercial-grade traffic intelligence engine designed to meet the complex and very specific needs of the converged, cloud-based networking and security environment of SASE.

Qosmos ixEngine: Quick Overview

Enea's Qosmos ixEngine® is a good example of a commercial grade, advanced DPI-based traffic intelligence engine. It provides Layer 2 to Layer 7 traffic classification and metadata generation, plus additional capabilities essential for SASE success:

4 of the Top 5 SASE Vendors

Embed Qosmos ixEngine

Source: Reports by Gartner, Forrester, 650 Group & Dell'Oro

Maximum Visibility

- Broadest and most accurate protocol coverage
- 3600 protocols & 5400+ types of metadata
- Deepest coverage for Cloud/SaaS protocols & apps
- Deepest coverage for M2M (ICS/SCADA) & IoT protocols
- Custom signatures support
- Optional device classification for edge access networks
- First Packet Advantage for uniquely effective first-packet processing

Unique Insights

- Identification of anomalous and evasive traffic
- Complex tunneling visibility, with full protocol paths for up to 16 levels of encapsulation
- Extraction of files and embedded links
- ML-enhanced encrypted traffic classification

Fast Ramp Up

- Ready-to-deploy commercial-grade DPI
- Flexible form factor options (C library, VNF, CNF, SW Sensor)
- Optional built-in rules engine
- Granular, well-structured ready-to-use service and transaction metadata
- Global presence for professional services and support

Learn More

Would you like to know why 4 of the 5 top SASE vendors trust Enea Qosmos technology to fulfill their traffic intelligence needs?

→ Discover full details of the Qosmos ixEngine: www.qosmos.com/products/deep-packet-inspection-engine

→ Explore the list of protocols recognized by Qosmos technology: https://protobook.qosmos.com

→ Connect with our experts and see a product demo: www.qosmos.com/about-us/contact-us

→ Learn more about Enea Qosmos Traffic Intelligence and DPI technology: www.qosmos.com

ENEA

Enea is one of the world's leading specialists in software for telecommunications and cybersecurity. The company's cloud-native products are used to enable and protect services for mobile subscribers, enterprise customers, and connected devices. More than 4.5 billion people rely on Enea technologies in their daily lives.

www.enea.com