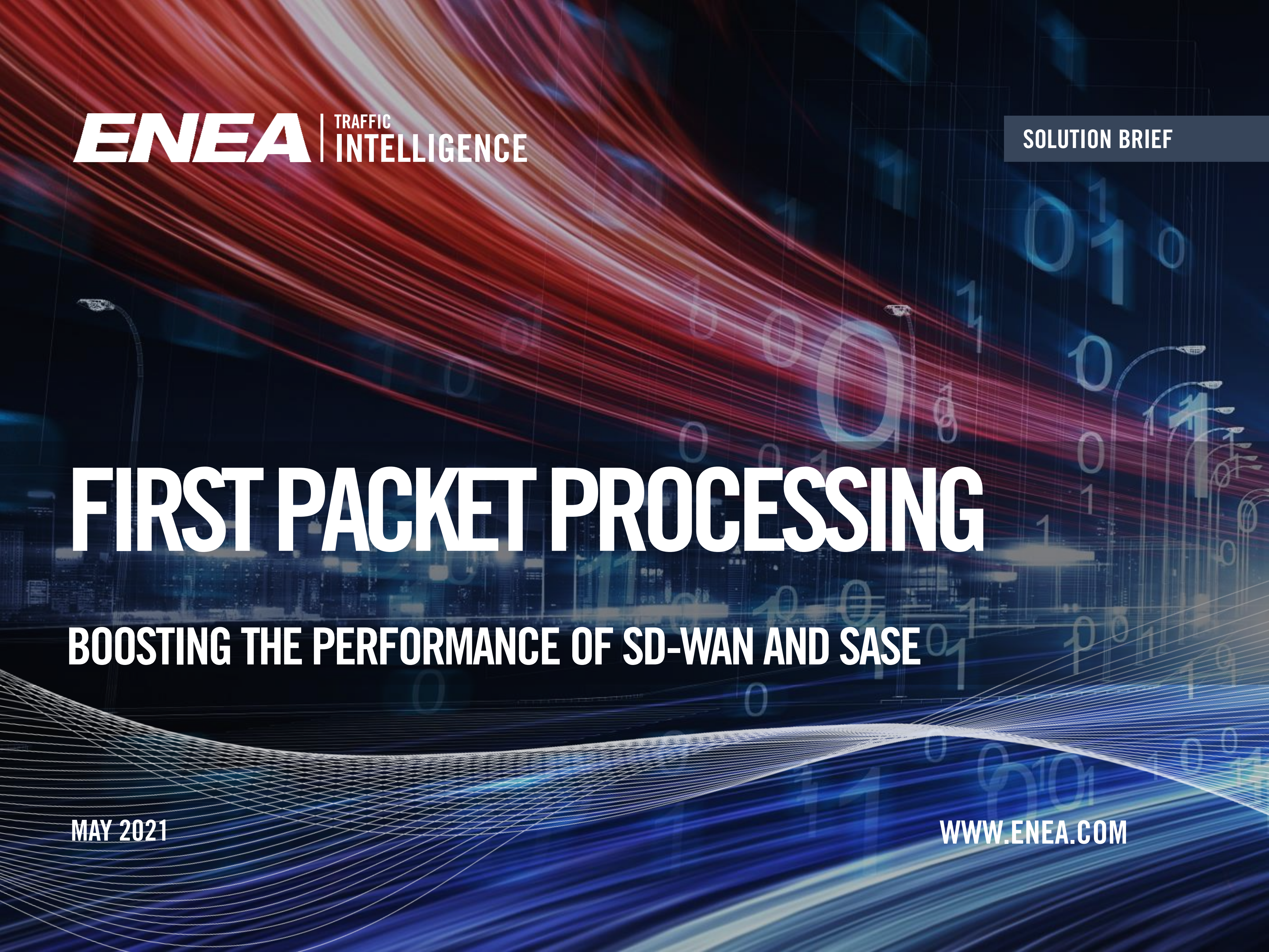


ENEA | TRAFFIC INTELLIGENCE

SOLUTION BRIEF

FIRST PACKET PROCESSING

BOOSTING THE PERFORMANCE OF SD-WAN AND SASE

MAY 2021

WWW.ENEA.COM

THE VISIBILITY CHALLENGE IN SD-WAN AND SASE

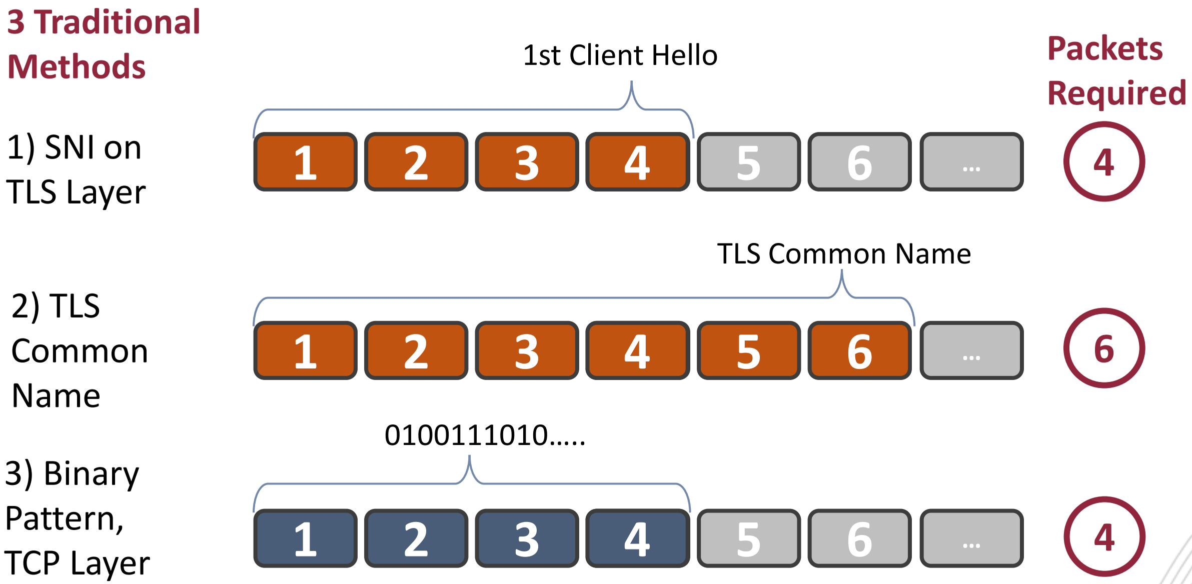
SD-WAN and SASE solutions are designed to bring agility, scalability and automation to the challenge of managing and securing distributed networks. This requires lightning-fast execution of complex, application-aware rules across high-volumes of traffic.

Deep packet inspection (DPI) has traditionally delivered this application-awareness in networking and security solutions. However, traditional DPI processing struggles to keep pace with the high-performance demands of SD-WAN and SASE.

This is because conventional DPI engines typically need to process multiple packets in a flow for accurate application identification. And many advanced SD-WAN and SASE steering and security functions simply cannot wait that long.

TRADITIONAL CLASSIFICATION REQUIRES PROCESSING OF MULTIPLE PACKETS

Example: 4-6 packets needed to identify WhatsApp



3 Traditional Methods

Packets Required

1) SNI on TLS Layer

2) TLS Common Name

3) Binary Pattern, TCP Layer

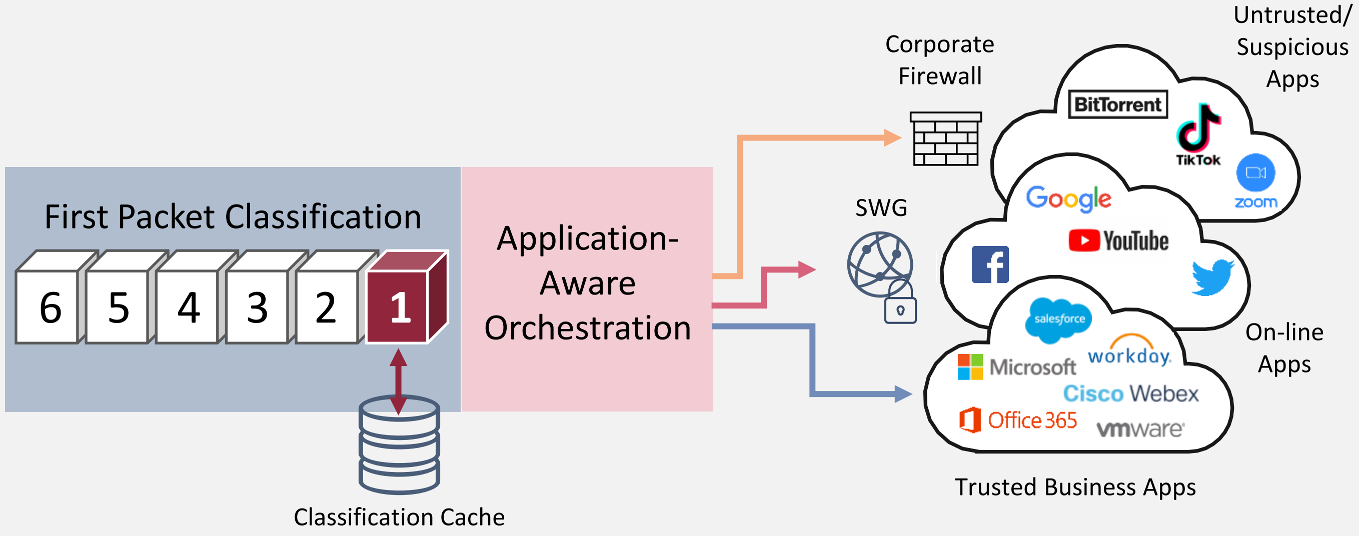
A BETTER WAY: FIRST PACKET PROCESSING

By adding a cache of classified traffic vendors of SD-WAN and SASE solutions can identify traffic from the very first packet. With a cache in place, trusted data available in the first packet (e.g., server IP addresses and port information) is sufficient to match a flow against previously classified traffic.

To initially deploy such a solution, a default route is established for all initial unclassified flows. Once these flows are classified, routes defined by the solution's orchestration component are tied to this classification cache, so that subsequent packets are steered from the very first packet.

This enables significant performance gains as flows matching the classification cache can be steered immediately - without having to go through multi-packet DPI processing.

However, not all first packet processing technologies are equal…



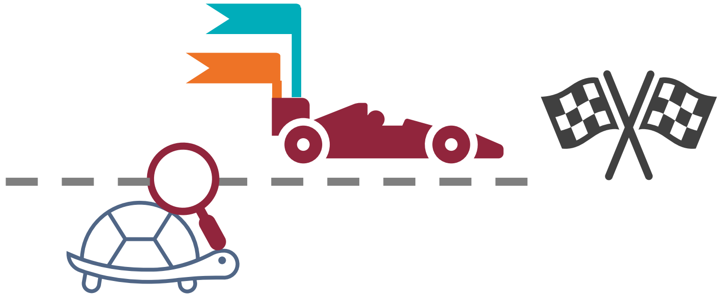
Most of today's traffic classification software leaves vendors with an unfortunate choice: speed OR accuracy

THE VALUE – AND HIDDEN CHALLENGE – OF TRADITIONAL FIRST PACKET PROCESSING

First packet processing is a key function for high-speed, application-aware traffic steering for SD-WAN and SASE, where dynamic selection of the optimal paths is determined by unique application requirements such as bandwidth, latency, QoS, security, etc. First packet processing brings a significant performance advantage to this process.

However, there is a serious challenge with most first packet processing technology: it can only accurately identify a very limited proportion of traffic, and generates a high volume of false-positive classifications.

This leaves vendors with an unfortunate choice between passing more traffic through DPI and reducing speed, or applying traffic steering and security policies based on limited information, thereby introducing potential security risks.

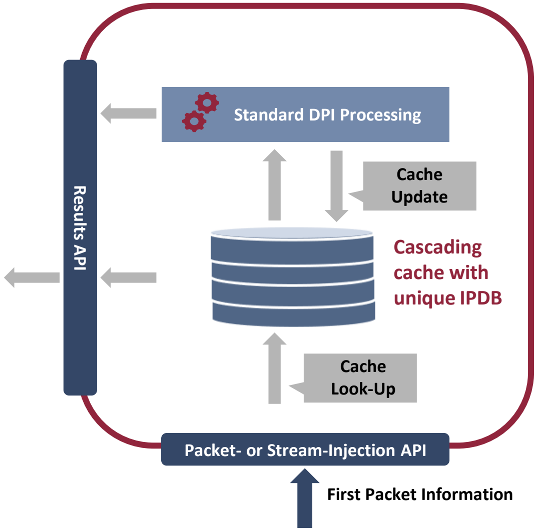


> Application awareness is essential for SD-WAN and SASE solutions, but many conventional traffic classification engines score poorly in accuracy, granularity and performance.
>
> A solution like Enea's First Packet Advantage, that operates with high accuracy in first packet mode, brings improved protection and performance to vendors and end-customers.
>
> - Roy Chua, Founder and Principal, AvidThink

ENEA FIRST PACKET ADVANTAGE

To solve this challenge, Enea developed First Packet Advantage.

Available as a standard feature in Qosmos ixEngine® and Qosmos ® Probe, First Packet Advantage (FPA) uses an innovative multi-tier cache system to boost application recognition and significantly improve accuracy.



FPA FIRST PACKET ADVANTAGE

GREATER ACCURACY & HIGHER PERFORMANCE

Enea Qosmos ixEngine®'s standard First Packet Advantage (FPA) feature improves on conventional cache-based first packet processing in four important ways.

1. It uses a multi-tiered, cascading cache structure that greatly expands the volume of traffic that can be accurately identified using first packet processing.
2. The cache leverages a unique Internet Protocol Database (IPDB) of hundreds of millions of rigorously and continuously-verified IP address and application matches for maximum accuracy and granularity across the broadest spectrum of traffic.
3. First Packet Advantage classifies Office 365 traffic based on first packet data alone, enabling ultra-efficient, category-based management of this widely used software suite.
4. FPA delivers valuable security information as a complement to application and service identification, providing additional contextual data to support security orchestration.

FPA takes first packet processing to a new level of visibility and accuracy

FPA
FIRST PACKET ADVANTAGE

SD-WAN & SASE vendors can use First Packet Advantage to improve security-aware traffic steering

ROBUST, SECURITY-RELATED INFORMATION

First Packet Advantage is unique in its ability to deliver robust, security-related information in addition to application and service classification.

This includes, for example, the identification of VPNs and anonymizers typically associated with malicious activities, the detection of complex tunneling protocols, and indicators of domain fronting.

This intelligence enhances existing security capabilities for SASE vendors and supports product evolution for SD-WAN vendors.

Spotting the threats

- VPNs
- Anonymizers
- Tunneling

CLASSIFICATION OF ENCRYPTED TRAFFIC

Though the primary benefit of First Packet Advantage today is performance, its ability to accurately identify protocols and applications in encrypted flows will grow in importance over the next several years as encryption standards evolve and harden.

For example, under the TLS 1.3 encryption standard and new versions of the QUIC protocol, some data that previously remained clear is now encrypted, and DNS exchanges will soon be encrypted as well.

This means there will be very limited data left for analytics without decryption: a few metadata from protocol layers and basic flow information such as IP address and port. This is the kind of lean data FPA can transform into accurate application identification.

In addition, SSL pinning will make it impossible in some circumstances to deploy a proxy server to perform decryption. And, when decryption can be used, the hardened standards will make the process more resource-intensive.

This means the situations in which proxies cannot be deployed to decrypt and inspect traffic, or in which doing so will become undesirable for performance reasons, are going to increase.

In these situations, First Packet Advantage will provide an important safeguard to help vendors maintain critical visibility for a broad range of needs, from traffic steering to performance monitoring to threat detection.

First Packet Advantage identifies and classifies encrypted traffic flows (without decryption)

CONCLUSION

First packet classification can significantly accelerate and optimize traffic management by enabling solutions to apply pre-programmed criteria for traffic steering as data flows arrive.

For non-traffic steering appliances, performance can also be boosted by choosing to omit the DPI software validation phase for flows that match the classification cache.

First packet Advantage provides a level of accuracy unavailable with other first packet processing technologies, and it delivers important security intelligence along with application identification.

It also helps vendors better position themselves for major industry changes, including fully encrypted environments and Artificial Intelligence (AI)-driven operations and analytics.

ACQUIRING FIRST PACKET ADVANTAGE

I'm already an Enea Qosmos customer:

If you already embed the Qosmos ixEngine or Qosmos Probe in your solution, First Packet Advantage is available as a standard feature. Simply activate it to enhance the performance of your existing solution.

I am not yet an Enea Qosmos customer:

Integrating the Qosmos ixEngine or Qosmos Probe with First Packet Advantage into your solution will enrich and extend your portfolio with high-value, high-speed traffic classification from the very first packet.

BENEFITS

- High speed traffic identification
- Accurate results
- Security intelligence
- Classification of encrypted traffic
- Easy installation and maintenance

Click here to request a product demo!

ENEA | TRAFFIC INTELLIGENCE

Enea is the world-leading supplier of innovative software components for telecommunications, networking and cybersecurity. Focus areas are cloud-native, 5G-ready products for mobile core, network virtualization, and traffic intelligence. More than 3 billion people rely on Enea technologies in their daily lives. Enea is listed on Nasdaq Stockholm.
For more information: www.enea.com

Enea's embedded traffic intelligence products classify traffic in real-time and provide granular information about network activities. The portfolio includes the Enea Qosmos ixEngine and the Enea Qosmos Probe. The products support a wide range of protocols and are delivered as software development kits or standalone network sensors to network equipment manufacturers, telecom suppliers, and vendors of cybersecurity software. For more information: www.qosmos.com

WWW.ENEA.COM