VIAVI Solutions

This Former Spirent Business is Now Part of VIAVI

Contact Us +1 844 GO VIAVI | (+1 844 468 4284)
To learn more about VIAVI, visit viavisolutions.com/en-us/spirent-acquisition

EXECUTIVE BRIEF

Security and Performance Testing for SASE & Zero Trust

Challenges, Recommendations, and Business Advantages

Introduction

SASE (Secure Access Service Edge) converges networking and security domains into a distributed cloud environment, where it secures applications and data using cloud-hosted security functions, independent of user location. Its dynamic, policy-based approach delivers benefits of the cloud that digital enterprises require, achieving significant advantages over VPNs deployed in a traditional centralized data center.

SASE is typically deployed in a Zero Trust (ZT) environment, which authenticates users based on real-time context and identity, and grants access to required business applications and data if authorized. By hosting security functions in the cloud, end users may securely access applications and data at any time, from anywhere, far more efficiently and securely than via a VPN.[1]

Three Guiding Principles for SASE Validation

To ensure security policies and functions behave as expected in the SASE environment:

1. **Test what will be deployed–** Realistic application and threat emulation is required to exercise real workloads in your networks, with test agents that can be deployed in hybrid, distributed environments. Security validation **reduces time-to-market** for new services by providing a smooth and transparent transition for security and application performance testing in the live environment.
2. **Characterize the new normal–** Start by baselining the KPIs — application transactions per second, concurrent users, per application latencies, quality of experience (QoE), etc. — and validate Zero Trust policies like microsegmentation and data loss prevention (DLP) to verify restricted access from certain regions and critical data and files are protected. In addition, perform cross-domain correlation to determine root cause and **business impact analysis** on all stages of the application lifecycle: design, pre-deployment, and production.
3. **Ensure scale and resiliency–** Validating cloud-native infrastructure robustness — as well as high-availability and auto-scale mechanisms — can be difficult. Realistic threat generation is needed to exercise application security inspection polices, and **QoE service recovery** times.

Challenges in SASE Testing

While SASE offers compelling advantages, it also increases testing complexity and introduces new risks:

- **Overcoming unknowns:** Validation of traffic shaping, data policies and performance targets as traffic traverses third-party networks
- **Validating edge cloud availability, security, and performance:** Enforcing SLAs, security controls and polices in hybrid clouds
- **Achieving optimum tradeoffs between performance, security, and QoE**

[1] SASE combines these capabilities with advanced techniques, applications, and devices such as Zero Trust Network Access (ZTNA), cloud access security brokers (CASB), data loss prevention (DLP), secure web gateways (SWG) and next-generation firewalls (NGFWs) to deliver a wide range of additional functionality.

Key Testing Considerations for SASE

The six recommendations below are critical in validating SASE security and performance.

1. **Take a vendor-neutral approach**
   When evaluating a new innovation or technology, consider the critical question: Who's setting the standards? Consider working with a neutral testing partner that has earned the trust of the community and participates and adopts relevant testing standards and specifications — including high-speed Ethernet, Wi-Fi 6, 5G, timing, network service assurance, and of course SD-WAN, SASE, and Zero Trust.

2. **Select the right traffic patterns and KPIs to exercise the network**
   Selecting the appropriate SASE traffic patterns and correct KPI measurements minimizes test durations and avoids faulty assessment of real-world behavior. QoE is the best unit of measure because it directly represents end-user satisfaction. It is based on performance, detection of errors, and variability for SSL/TLS based services and mean opinion score (MOS) for video and voice.

3. **Stress test prior to deployment**
   Rigorously test and validate the solution in pre-deployment by stressing software to the limit. Managed services offerings must operate in any network, on any cloud, whether in the 5G core or metro edge, quality assurance lab, or CI/CD/CT developer toolchains.

4. **Assess with real traffic**
   The ability to fully emulate application (L4-7) traffic, at scale, with real-world attack scenarios is essential. Simulated traffic simply is inadequate. Real-world traffic generation and test methodologies provide an accurate representation of all facets of the networking landscape — from discrete application behaviors to encrypted transmissions — and the ability to inject impairments (system errors or latencies) that reveal how the solution will perform under stress.

5. **Identify security and performance vulnerabilities**
   Simulated attacks with basic packet replay can lead to false results. Stateful emulation helps quantify and assess security countermeasures in real time against actual attack vectors to evaluate the impact security measures have on your business model and user experience.

6. **Provide intelligent reporting and data-driven predictions**
   Validating multiple levels of cloud and services infrastructure for complex use cases — such as 5G low-latency slicing or 360^0 security policy enablement for distributed environments — requires an additional level of intelligence. Business impact analysis exposes how new policies or service disturbances affect end customers and SLAs. Root cause analysis supplemented by anomaly detection predicts future issues and performance limitations.

Quantifiable Business Results

Spirent's SASE validation solutions deliver a range of business benefits based on your environment:

- **Lower costs** through reduced development time, pre-emption of failures in the field, visibility into whether investments are paying off as expected, lower procurement and training costs. Proactive visibility of the SASE security posture helps organizations prepare for and preempt catastrophic and costly security breaches.
- **Reduced risk** of security breaches, penalties and fines for compliance violations, and inability to respond quickly to new threats. While no product can guarantee security, Spirent rapidly reveals misconfigurations, human errors, avoidable bottlenecks, etc. by validating that security functions behave as expected.
- **Lower customer churn rates** through data-driven insights into how well new services are performing. Spirent provides measurable KPIs and reporting on user loads, latencies, QoS, and more, helping to improve QoE and reduce customer churn.
- **Faster innovation and time-to-market** because developers spend less time troubleshooting, testing and fewer refinement cycles.
- **Ability to scale new services** with confidence that performance and security will not be compromised.
- **Differentiated services** with tangible, reliable, sustainable advantages in security and performance.

About Spirent

Spirent is the leading global provider of automated test and assurance solutions for next-generation devices and networks. Our innovative portfolio of products and services addresses the test, assurance, and automation challenges of a new generation of technologies: SASE, 5G, SD-WAN, High-Speed Ethernet, Cloud, Autonomous Vehicles and beyond. Our network, cybersecurity, and positioning experts work closely with customers to understand their needs and deliver solutions that cover their entire technology lifecycle, from the lab to real-world deployment.

For more information visit:
www.spirent.com

Spirent solutions and advantages

Spirent offers a comprehensive portfolio of products and services for security and performance testing, including:

- CyberFlood delivers a comprehensive, easy-to-use test solutions to quickly assess and validate the performance, scalability, and security effectiveness of networks and security solutions. Lightweight software test agents are deployed at strategic measurement points (inside an on-premises network public cloud, private cloud, branch offices, etc.) to simulate distributed network topologies.

  CyberFlood then generates emulated traffic based on real application workloads and threat vectors and provides full visibility into whether security controls are effective, as well as the impact of these controls on network performance and QoE.

- Spirent Managed Solutions provides a variety of comprehensive managed testing services delivered by certified, seasoned professionals. Our security consultants act as an extension of your in-house security team, proactively identifying vulnerabilities and mitigating risks. Our testing professionals can assist you with:
  - Manual penetration testing
  - Automated scanning and reporting
  - Continuous compliance
  - Sector-specific vulnerability testing
  - Consulting

FOR MORE INFORMATION

Learn about the requirements for effective SASE and Zero Trust validation and related testing strategies in this companion white paper.

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com