Six Tests You Need Now for Distributed, Elastic Cloud Networking

ACCELERATING HIGH-QUALITY APPLICATION AND SECURITY INNOVATIONS THAT MAKE THE NETWORK

KEYSIGHT TECHNOLOGIES

Introduction

Geographically distributed, multi-cloud architectures are rapidly replacing on-premises infrastructures. While this new approach brings considerable agility and the ability to scale rapidly, it also introduces complexity. Multiple third-party cloud providers, best-effort interconnects, and other factors make the cloud far less deterministic than the traditional hardware and software approach.

The unknowns of this new dynamic, distributed, hybrid environment create considerable challenges for network equipment manufacturers (NEMs) developing products to deploy into these environments. Anyone who has experienced a dropped call, a frozen screen during a video or audio conference call, or a failed-to-load web page can attest to the challenges and potential impact of delivering business-class reliability and a positive user experience over best-effort networks.

Distributed, elastic cloud networking raises many questions and concerns for NEMS that standard Ethernet testing approaches are not able to validate or answer, including:

- Will my customer's mass migration to the hybrid cloud negatively impact how my solution effects user experience?
- How will my solutions for software-defined wide area network (SD-WAN), secure access service edge (SASE), content delivery network (CDN), or web application firewall (WAF) perform in a real-world hybrid customer environment?
- Will a disrupting event occur uniformly across my customer's entire distributed, disaggregated footprint, or will some locations be more affected than others?
- Are security policies dynamically adjusting to auto-scale events? Will the implementation of my solution introduce any new security gaps?

Network equipment manufacturers (NEMs) are innovating faster than ever before to deliver the solutions required to build these multi-cloud networks. That innovation includes what you test and how you test to get high-quality solutions to market ahead of the competition. Figure 1 shows key validation points for multi-cloud, distributed networks that organizations are building out today. To succeed, you need to be sure that your networking solutions interoperate and perform well not just in the data sheet benchmarks but in the complex, multivendor, open, distributed networks seen in your customer deployments. Effective testing is the only way to ensure customer success.

This eBook highlights key network test areas important to hyperscale and other data center NEMs. For each area, we provide a brief introduction, key test requirements, test solutions, and links to additional resources.

Validating Distributed, Elastic Cloud Networking

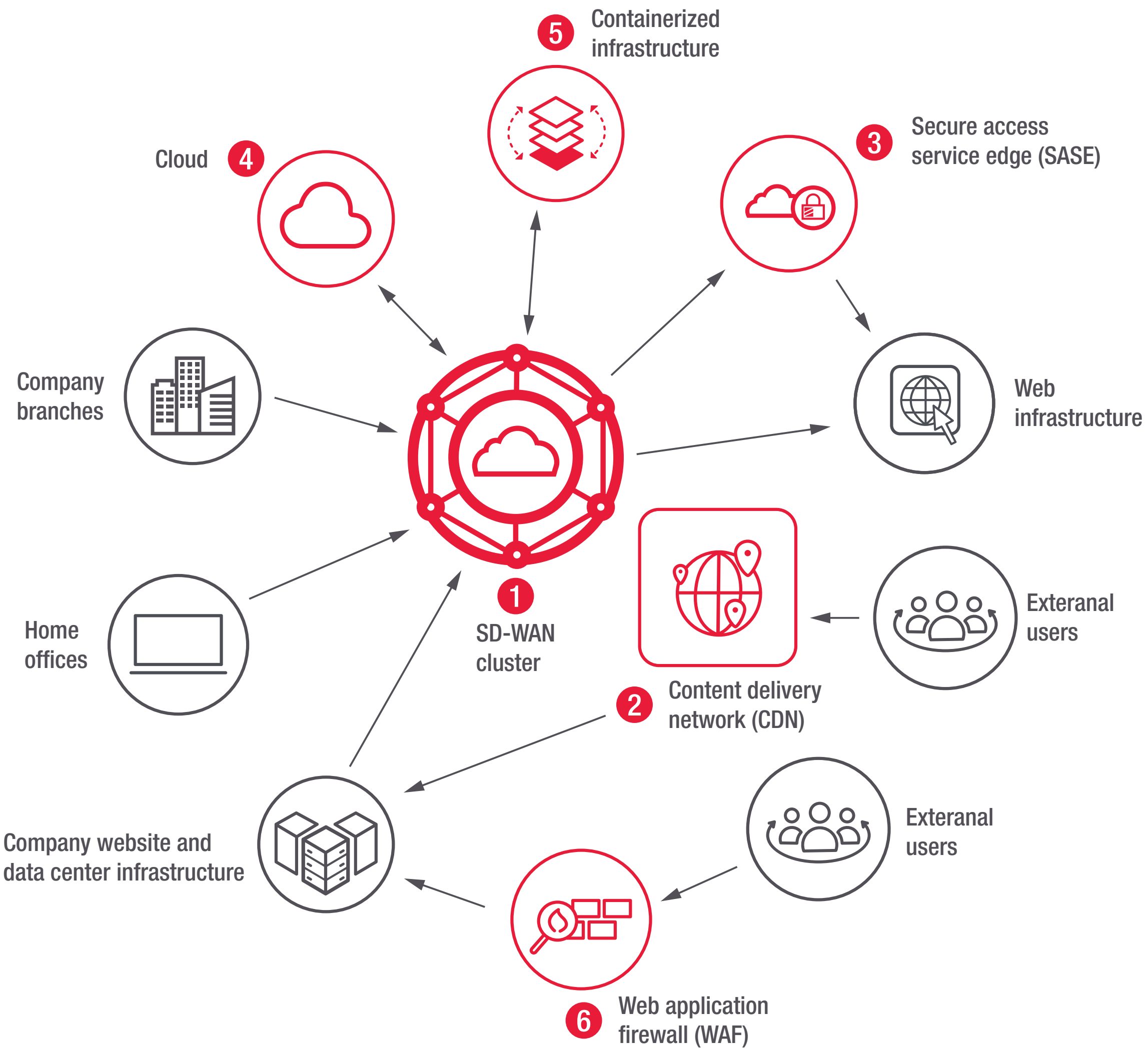
5
Containerized infrastructure
Cloud
4
3
Secure access service edge (SASE)
Company branches
Web infrastructure
1
SD-WAN cluster
Home offices
Exteranal users
2
Content delivery network (CDN)
Company website and data center infrastructure
Exteranal users
6
Web application firewall (WAF)

Figure 1. Key validation points for distributed, multi-cloud data center technologies (shown in red).

Contents

CHAPTER 1

Software-Defined Wide Area Network

CHAPTER 1

Software-Defined Wide Area Network

Organizations are adopting software-defined wide area network (SD-WAN) technologies at an accelerating pace regardless of whether they are replacing or enhancing multiprotocol label switching (MPLS). NEMs must ensure their SD-WAN solutions perform well not just in the lab, but in the complex geographically distributed sites and users over complex topologies with hybrid and multi-cloud environments.

Testing is critical to get it right. But validating SD-WAN performance and security efficacy is challenging in today's highly dynamic conditions that include a staggering number of cloud and hardware variables.

The smooth deployment of SD-WAN infrastructure over complex topologies like physically distributed branches, clouds, and data centers requires a test tool that enables you to:

- Test rigorously in a realistic simulation of the deployment environment. Picture the difference between testing a car in the real world with uneven road surfaces, stoplights, and congested traffic versus a clean, smooth test track.
- Measure key performance indicators, latencies, and quality of experience of the SD-WAN tunnels as they spread across wide area networks.
- Analyze the SD-WAN's ability to debug and remediate routes dropping, flapping, and other inconsistencies rampant in this environment.
- Understand the SD-WAN's security offerings – both efficacy and the potential impact on system performance and user experience.

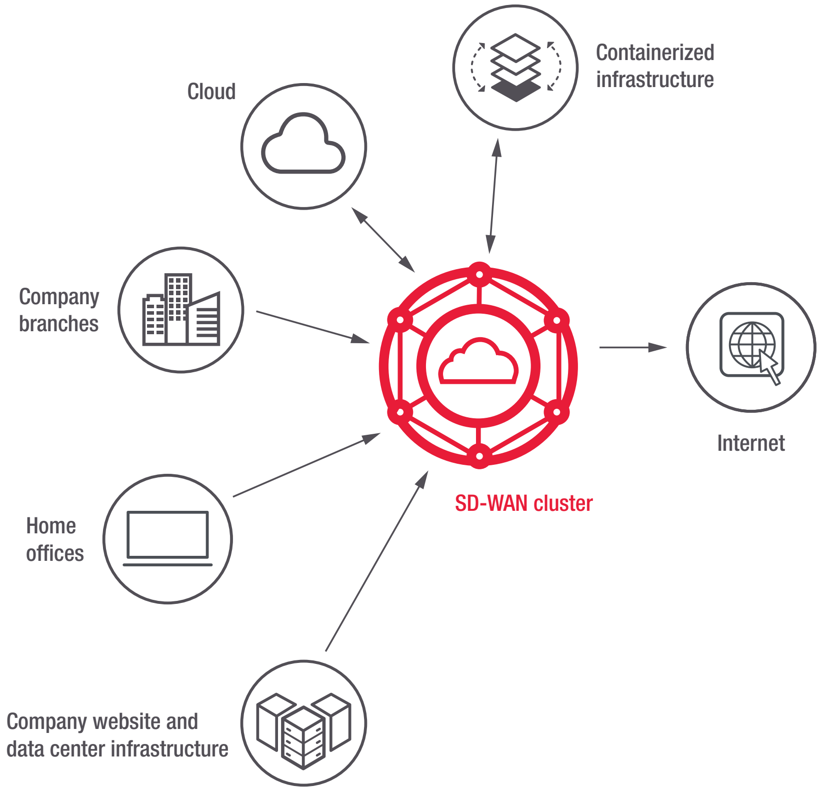
Cloud
Containerized infrastructure
Company branches
Internet
SD-WAN cluster
Home offices
Company website and data center infrastructure

Figure 2. The test tool should simulate clients and web servers (shown in grey) to validate the performance and security efficacy of SD-WAN devices and infrastructures.

Key Test Requirements

- Evaluate SD-WAN tunnels to understand maximum and average latencies, concurrency, throughput, and other key performance indicators.
- Generate both application and attack traffic to accurately evaluate the performance cost of security features to strike the right balance between security and quality of experience (QoE).
- Optimize SD-WAN deployments using geographically distributed test agents generating application traffic.
- Validate security features like application profiling and blocking, malware mitigation, exploit detection and blocking, URL filtering, and file inspection.
- Conduct relevant bake-offs, demos, and proof of concepts, and verify service-level agreements (SLAs).

With agents running in the cloud, CyPerf can replicate heavy traffic and volumetric attacks in an environment that closely mirrors the actual cloud environment so you can test your products the way your customers deploy them.

FURTHER READING

Flyer: SD-WAN Optimization – Application Performance and Security Validation

Webinar: Realize the Promise of Next-Generation SD-WAN with Edgeless Testing

CHAPTER 2

Content Delivery Networks

CHAPTER 2
Content Delivery Networks

Modern websites often rely on third-party content delivery networks (CDNs) to ensure reliable performance and quality of experience (QoE) for the end-user. Because of this, maintaining security and consistent QoE across geographically distributed points of presence (PoP) is critical for content delivery network (CDN) vendors. They need to:

- Maintain consistent QoE across distributed PoPs, including validation of new PoPs before deployment.
- Differentiate security offerings from other CDNs – web application firewall (WAF) and distributed denial of service (DDoS) mitigation and inspection.
- Detect issues and validate the fixes before deployment.
- Confirm updated security policies are working throughout the rollout process.
- Demonstrate to customers the immediate value of a CDN through live-traffic proof-of-concept demonstrations.

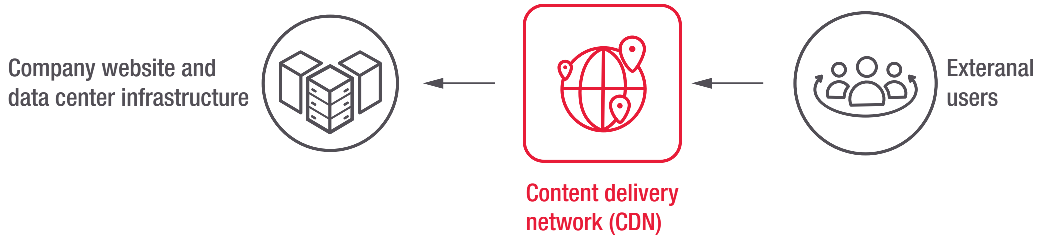
Company website and data center infrastructure
Content delivery network (CDN)
Exteranal users

Figure 3. To test the efficacy and performance of CDNs, your test tool should emulate external users and the company's distributed web infrastructure.

Key Test Requirements

- Evaluate CDN as accessed from various geographical locations to understand key performance indicators, including maximum and average latencies, caching efficiency, and load handling capacities like CPS, concurrency, and throughput.
- Verify service-level agreements for rate limiting, policing, and shaping.
- Perform customer proof-of-concepts with realistic traffic and reduce change management risk by validating changes before pushing to production.
- Check QoE metrics and compare performance across the network.
- Detect CDN security gaps with safe, closed-loop testing issues before they are reported by the customer and validate resolution.

FURTHER READING

Flyer: Content Delivery Network – Elastic Applications and Security Services Validation

CHAPTER 3

Secure Access Service Edge

CHAPTER 3

Secure Access Service Edge

The future of next-generation firewall technologies is in the cloud using secure access service edge (SASE) technology. A tectonic shift in how companies protect their data, intellectual property, and employees comes with new security challenges. For NEMs to ensure their technologies deliver the promised performance and protection, not to mention flexibility, cost savings, and simplification, you will need a new type of test tool, one that can help you:

- Maintain resiliency of SASE SD-WAN tunnels, debug and remediate tunnel disappearance and flapping, and locate other inconsistencies.
- Measure key performance indicators like latency and quality of experience and pinpoint the cause of network issues.
- Balance network performance and protection to ensure an appropriate mix of cost and QoE without compromised security.
- Validate the security efficacy of SASE offerings like URL filters, application controls, intrusion prevention systems (IPS), TLS inspection, and sandboxing.

Key Test Requirements

- Measure SASE security efficacy across a diverse geographic network, preferably with distributed agents.
- Test security features like exploit detection / blocking, application profiling / blocking, malware mitigation, URL filtering, and transport layer security (TLS) inspection using simulated attacks.
- Evaluate the performance / latency costs of security features, enable demos and proof of concepts, and verify service-level agreements and change management with a combination of application and attack traffic.
- Use realistic application simulation to validate unique SASE offerings like application shaping, policing, and control.

FURTHER READING

Flyer: Secure Access Service Edge – Elastic Applications and Security Services Validation

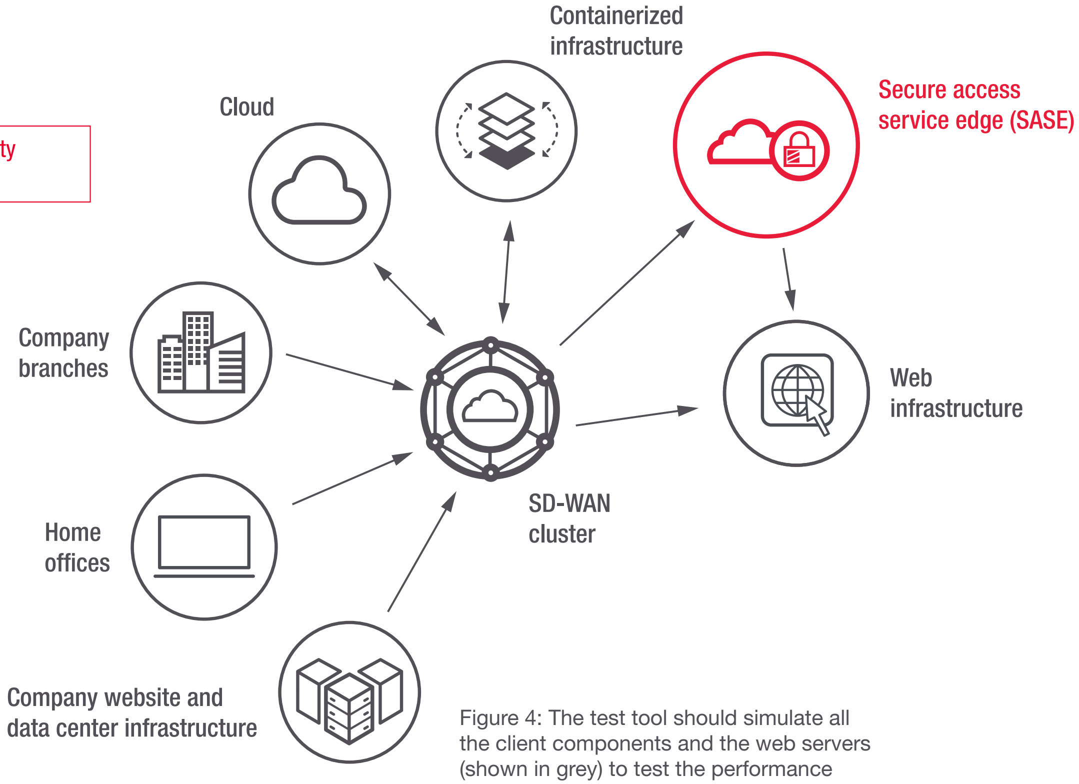
Containerized infrastructure
Cloud
Secure access service edge (SASE)
Company branches
Web infrastructure
Home offices
SD-WAN cluster
Company website and data center infrastructure

Figure 4: The test tool should simulate all the client components and the web servers (shown in grey) to test the performance and security efficacy of SASE device and infrastructures.

CHAPTER 4

Cloud

CHAPTER 4
Cloud

In a rush to move to the cloud, many organizations find it challenging to right-size deployments, optimize costs, and minimize user disruptions. To succeed with their data center customers, equipment and solution vendors must ensure high-performing products that operate well in a multi-vendor ecosystem. They need to:

- Test the efficacy of their solutions in dynamic, elastic environments.
- Isolate bottlenecks across instance types across different network infrastructures, third-party devices, and various implemented rules.
- Ensure that on-premises devices and technologies operate seamlessly and as expected in the cloud.

Key Test Requirements

- Cloud-native testing to help you benchmark true application performance of cloud instances and topologies that may involve switching, network address translating, or going through internet gateways to another cloud location using on-premises software.
- Realistic attack simulation to validate security features in web application firewalls (WAF) or next-generation firewalls (NGFW) to ensure they work like their on-premises counterparts.
- Elastic scalability to accurately measure the performance and security impact of elastic scale up or down per the policies of the auto-scale group.
- Validates individual security controls and cloud services like NGFW, IDS, WAF, and ELB for performance, scale, and security effectiveness.

FURTHER READING

Flyer: Cloud Migration – Elastic Applications and Security Services Validation

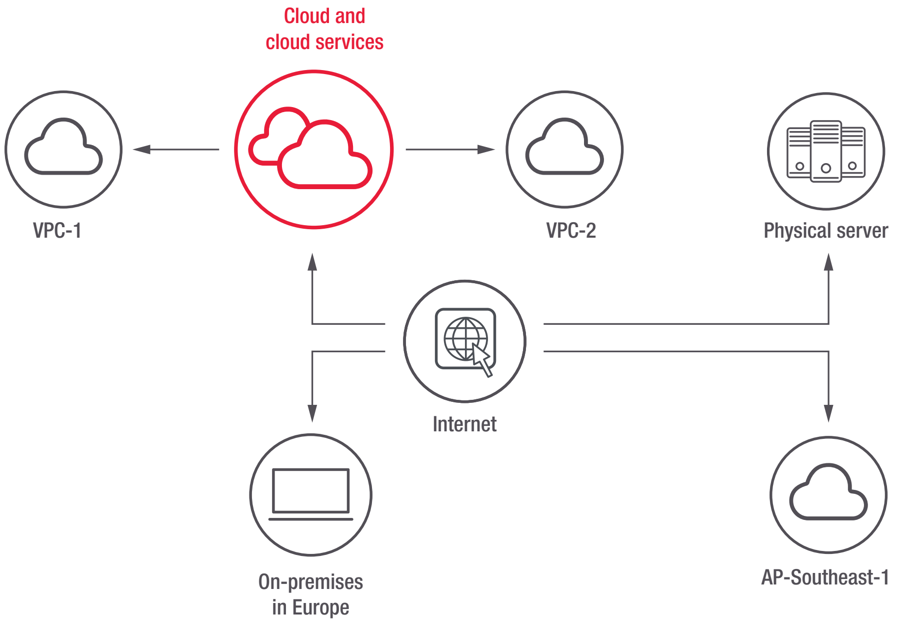

Figure 5. Test tool should seamlessly deploy in various cloud instances (shown in grey) to generate performance and security traffic through cloud and hybrid infrastructures.

CHAPTER 5

Containerized Infrastructure

CHAPTER 5
Containerized Infrastructure

Containerized infrastructure provides more flexibility than traditional resources. Applications running in containers are easily deployable to multiple isolated environments and operating systems using a standardized process. The ability to create hundreds of deployed containers or eliminate them in seconds based on demands are some of the reasons for the rising popularity. NEMs need to:

- Ensure the basics work by testing and resolving any issues before deployment.
- Test container security because the infrastructure needs to dynamically track and secure ephemeral systems as they are spinning up and shutting down.
- Validate products against various technologies like different container network interfaces (CNIs), Kubernetes, and more since each technology has its unique performance metrics and challenges.
- Check elasticity and resiliency to ensure the containers can expand, contract, and turn off while in operation without disruption to the user.

Key Test Requirements

- Measure the application performance and security efficacy of containerized next-generation firewalls.
- Ensure web application firewall and application load balancers that service containerized applications and databases are working correctly.
- Analyze performance comparisons using a container network interface like Calico or Flannel to determine the advantages or disadvantages of using one or the other.
- Evaluate Kubernetes implementations like Amazon Elastic Container Service, Amazon Web Services, or Google Kubernetes engine to determine which service best fits your requirements.
- Check deployment of application and security tools in various container network interface (CNI) and Kubernetes environments to gauge performance drops, latencies, and security issues.

FURTHER READING

Blog: Validating Containerization – What was small has become smaller, yet larger

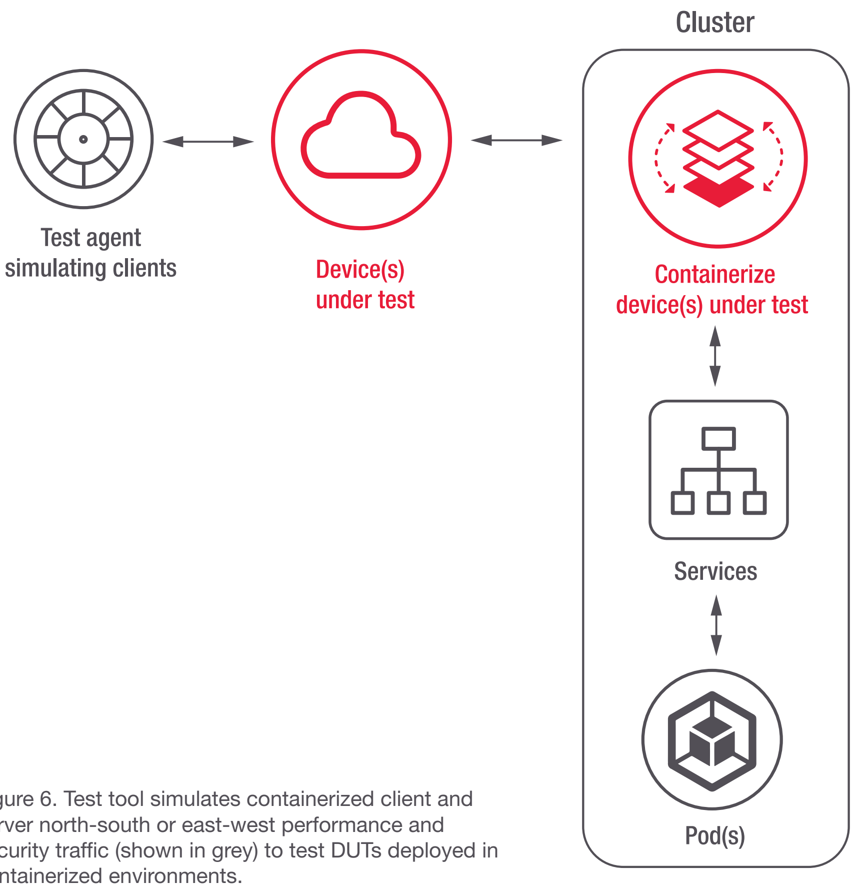
Cluster
Test agent simulating clients
Device(s) under test
Containerize device(s) under test
Services
Pod(s)

Figure 6. Test tool simulates containerized client and server north-south or east-west performance and security traffic (shown in grey) to test DUTs deployed in containerized environments.

CHAPTER 6

Web Application Firewall

CHAPTER 6

Web Application Firewall

A web application firewall (WAF) is critical for any website, providing key protection by inspecting inbound HTTP traffic and blocking attacks such as structured query language (SQL) injection and other types of cyberattacks against web services. Organizations that operate websites and the customers they serve expect nothing but the best from their WAFs. Vendors need to ensure consistent performance and security from a WAF regardless of its deployment (reverse / transparent proxy) and where it is deployed (cloud, on-premises, hybrid). As always, the right balance of security and quality of experience (QoE) is critical. To ensure high-performing devices and solutions, vendors must:

- Obtain consistent performance and security from your WAF regardless of the system's location and deployment.
- Understand the variation in performance benchmarks in different modes like transparent or reverse proxy.
- Secure complex websites and client browser technologies against a wide variety of threats.
- Tune the balance between QoE and security because enabling numerous features impacts network performance.
- Ensure system scalability to avoid performance bottlenecks or crashes when stressed by traffic at scale.

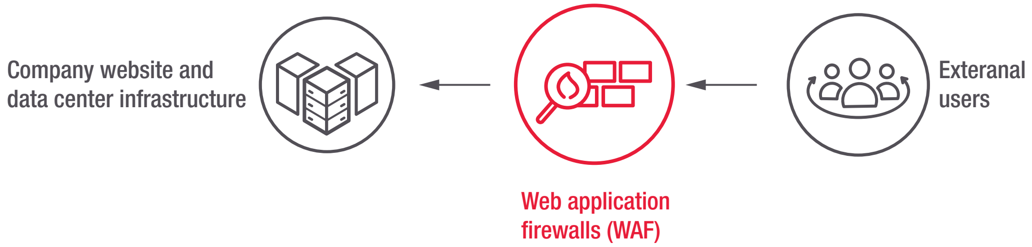
Company website and data center infrastructure
Web application firewalls (WAF)
Exteranal users

Figure 7. Test tool should simulate the client and server infrastructure as well as the user traffic (shown in grey) to test WAFs deployed in transparent or reverse proxy mode.

Key Test Requirements

- Check WAF performance using both HTTP and transport layer security (TLS) traffic, including popular websites like social media, e-commerce, banking, and video streaming.
- Perform Open Web Application Security Project (OWASP) top-10 attacks like injections and cross-site scripting and non-OWASP attacks like file inclusion and authentication bypass.
- Launch hybrid and proxied WAF deployments using a realistic mix of application and attack traffic.
- Simulate clients including Firefox, Safari, Chrome, iOS, and Android to check system performance.
- Simulate server technologies including JavaScript, CSS3, HTML5, and hypertext preprocessor (PHP) scripting.

FURTHER READING

Flyer: Web Application Firewall – Application Performance and Security Validation

Summary

With the promises of cost savings, better security and accessibility, and faster deployment, networks are increasingly multi-cloud, geographically diverse, and containerized. Vendors are rapidly evolving solutions to move networking along this trajectory to support new use cases. To capture your share of this burgeoning market with high-performing and secure solutions, you need flexible and rapidly advancing test tools that are purpose-made for this new environment.

Keysight's expertise and test solutions have a long history of helping equipment manufacturers validate their network gear and services. We understand that with a dramatic shift in how networks are built and operate, you need a new type of test solution that recreates realistic application and threat traffic across a variety of physical and cloud environments.

Keysight CyPerf employs lightweight agents deployed across a variety of heterogeneous environments to model a realistic mix of dynamic application traffic, user behavior, and threat vectors at scale. Validating pre-deployment and production devices and solutions, it delivers unprecedented insights into end-user experience, security posture, and performance bottlenecks for containerized, distributed and hybrid networks.

With CyPerf, you can now proactively and accurately measure performance and security efficacy in realistic multi-cloud distributed test topologies that closely resemble the production environment — testing that replicates the network in action.

FURTHER READING

Data sheet: Keysight CyPerf
Tutorials: CyPerf Intro and Tutorial Videos
Trial: CyPerf Free Trial

KEYSIGHT
TECHNOLOGIES

7121-1116.EN

Published in USA, August 5, 2021 | keysight.com