

Six Tests You Need Now for Hyperscale Networking

ENSURING HIGH-QUALITY INNOVATIONS THAT MAKE THE NETWORK

Introduction

Distributed, disaggregated digital transformation leaves no network element untouched. Cloud migration, software-defined wide area network (SD-WAN), data center upgrades, advanced cybersecurity capabilities, the Internet of Things, and application proliferation are examples of significant technology shifts. Organizations are embracing these shifts through digital transformation, which itself brings significant technical challenges.

The converged data center, along with the increasing importance of on-demand scale with virtualization in hyperscale data center networks, is shifting fundamental approaches to building these networks. New applications such as machine learning and artificial intelligence are changing how workloads use data center resources. Technologies such as Remote Direct Memory Access over Converged Ethernet version 2 (RoCEv2) and Media Access Control Security (MACsec) are being recast to deal with new problems like increasing storage workload transfer and the inability of IP-based encryption to keep up with modern data center traffic demands.

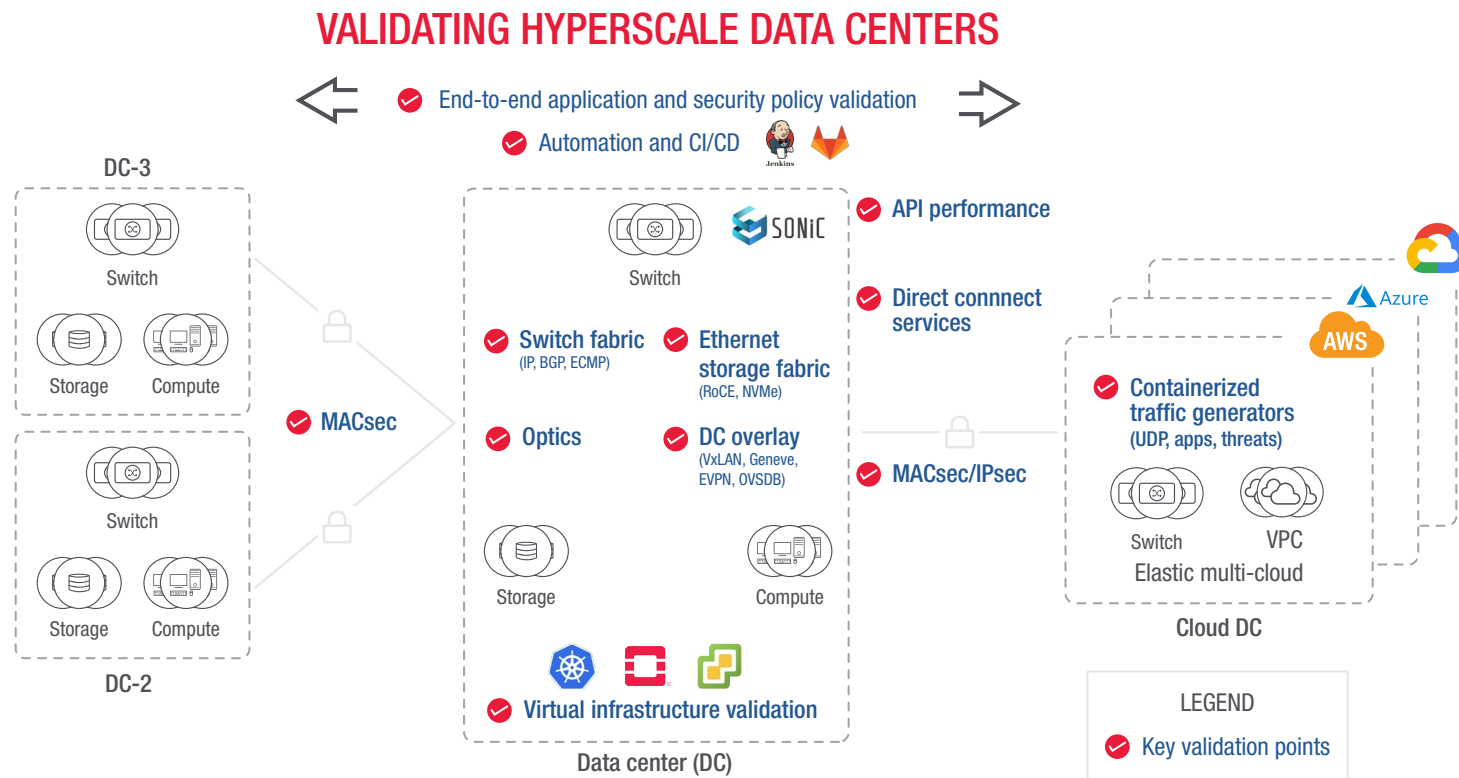


Figure 1. Key validation points for hyperscale data center technologies

Network equipment manufacturers (NEMs) are innovating faster than ever before to deliver the solutions required to build these hyperscale data center 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 data center 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.

Contents



CHAPTER 1

Converged Data Center Storage

Introduction

The convergence of compute, networking, and storage brings significant savings in equipment costs, energy consumption, and hardware footprints. It also provides the needed infrastructure to enable machine learning, artificial intelligence, and storage network scale-out. RoCEv2 and Non-Volatile Memory Express over Fabrics (NVMe-oF) are two technologies set to address modern storage performance requirements over converged Ethernet fabrics.

RoCEv2 promises high throughput and low latency for the massive data volume transfers many modern data center applications need. However, it requires a lossless Ethernet foundation, which is achievable by combining RoCEv2 with data center bridging standards. Incorrectly configured or non-optimized buffering and other transient misbehaviors in a data center Ethernet switching fabric will result in poor application performance, especially under high load.

CHAPTER 1

Converged Data Center Storage

NVMe-oF enables the transfer of storage workloads between a host and a storage system. It has emerged as another higher-performance and lower-latency solution to transfer storage workloads in a data center. With NVMe solid-state drives getting faster, the transport network is becoming the bottleneck for hyperscale data centers, especially during network congestion.

In today's high-performance application scenarios, dynamic delay caused by congestion and packet loss will have a much greater impact on the overall performance.

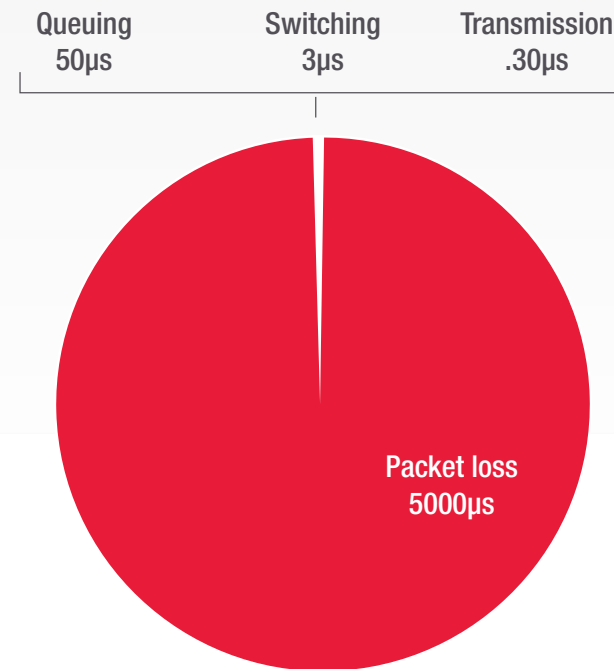


Figure 2. Delay distribution per various events / operations
(diagram source: China Mobile)

Key Test Requirements

Lack of commercial test tools to emulate storage network workloads has led to a compromise in testing cycles and the use of homegrown, server-based testbeds. Such testbeds are hard to scale and manage and do not deliver consistent, repeatable workload patterns. Your validation solution for RoCE application workload performance in switches and switch fabrics will need to measure the effect of various flow control methods (PFC, ECN, DCQCN). It must also assess the impact on end-to-end application performance and latencies, especially in congestion scenarios. You'll also need detailed statistics on each queue pair (QP), useful to troubleshoot issues in the system under test (SUT). In a converged network, there is a significant volume of TCP traffic besides RoCE, so you will need to assess the SUT's ability to handle both traffic types simultaneously and prioritize for maximum efficiency.

Similarly, for NVMe-oF, it is prohibitive and inefficient to scale to realistic testing scenarios without a test solution that can simulate NVMe host systems and massive-scale users. Pushing the network under test and its components to the congestion point and providing relevant metrics is paramount in understanding behavior. Failover scenarios are also key aspects for validation.

Keysight Solutions

Keysight's [Ixia Data Center Storage 100GE Test Load Module](#) generates realistic RoCEv2 traffic at line rate to characterize the performance and latency impacts of various storage workloads and tune switching fabric parameters.

FURTHER READING



[Blog: RoCEv2 and Testing Disaggregated Storage Ethernet](#)





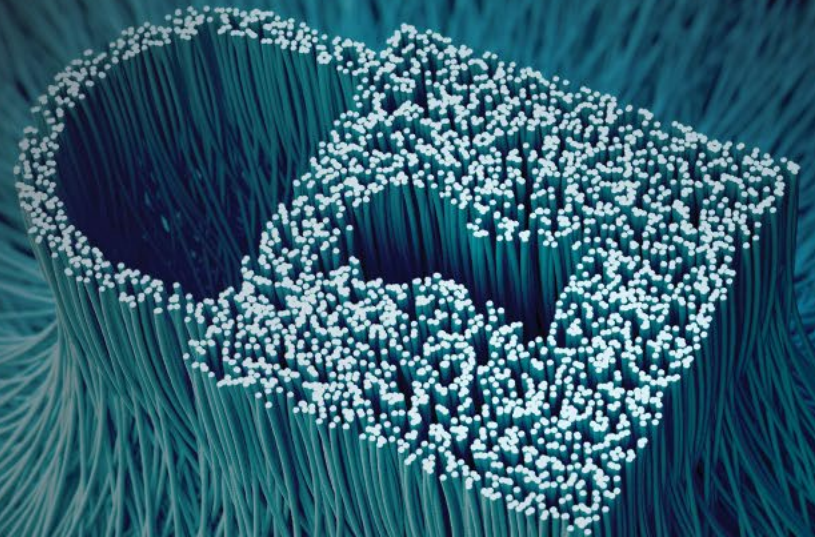
CHAPTER 2

MACsec Encryption

Introduction

While there are different ways to implement encryption for data in motion, MACsec makes line-rate encryption possible for high-speed Ethernet — critical for cloud and data center interconnect operation.

MACsec encrypts traffic between two or more nodes on an Ethernet network. It operates at OSI Layer 2, providing some advantages over other higher-layer and more common encryption approaches, including IPsec and Transport Layer Security (TLS) and Secure Sockets Layer. While the standard has been active for many years, MACsec is undergoing something of a renaissance. An increased focus on regulatory compliance, data privacy, and security has led to greater interest in protecting data in motion, even within data centers. Additionally, as demand for bandwidth on Ethernet WAN and SD-WAN increases, encryption has trouble keeping pace with the raw speed of encrypted links.



CHAPTER 2

MACsec Encryption

MACsec is a proven way to protect all the traffic on a particular network link and get around IPsec or TLS performance limitations. Hardware-driven MACsec works at line rate, ensuring that security does not create a performance bottleneck. Other approaches can max out before full line rate on the faster connections required today.

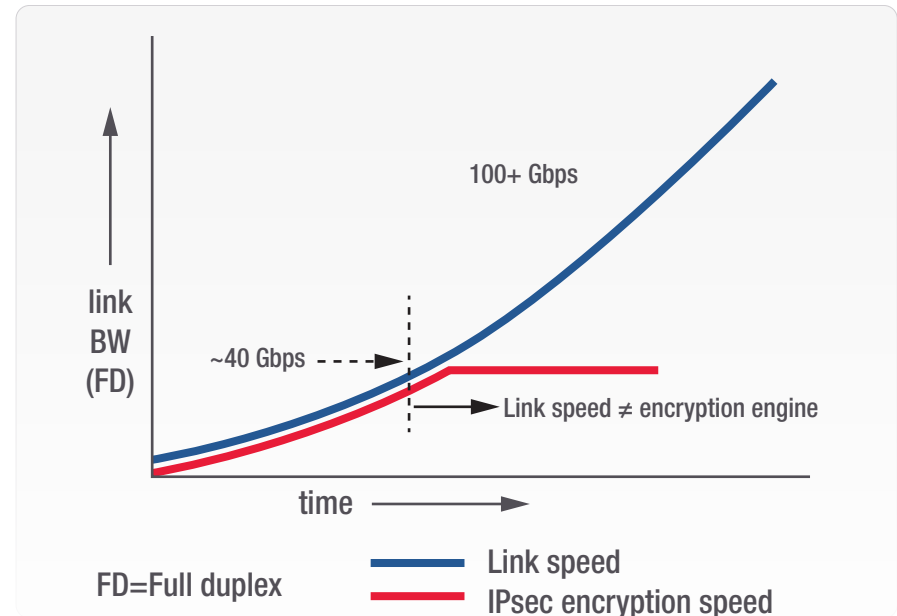


Figure 3. Layer 1 MACsec fills the gap caused by link speed outpacing Layer 3 to 7 encryption speed (source: Cisco, [Innovations in Ethernet Encryption \(802.1AE-MACsec\) for Securing High Speed \(1-100GE\) WAN Deployments](#), updated June 19, 2019)

Key Test Requirements

Because of a lack of effective tools on the market, one approach to MACsec validation has been back-to-back testing. The network vendor connects two devices capable of MACsec encryption and verifies that traffic flows as expected. But that approach has severe limitations. Like other black-box testing approaches, back-to-back testing fails to provide broad enough test coverage of realistic network conditions, nor does it provide visibility into the encryption / decryption state of the device under test (DUT). This lack of coverage and visibility can lead to false passes, interoperability, and other problems in the field.

Another area of interest is performance with diverse types of traffic. How well does your encryption engine handle line-rate traffic? What about smaller packet sizes or IMIX? How do QoS (Quality of Service), queues, and buffers interact? What about bursty traffic?

Other tests should include the implementation of various cipher suites (GCM-AES-128, GCM-AES-256); confidentiality offset; the impact of encryption on throughput, latency, and delay; the impact of rekeying; and mixed MACsec and non-MACsec traffic scenarios.

Keysight Solutions

Keysight's **IxNetwork MACsec Test Solution** is the industry's first for high-speed Ethernet, providing line-rate 100GE validation under a realistic traffic mix.

FURTHER READING



[Blog: MACsec Hardware Validation – Why Back-to-Back Validation Falls Short](#)

[Blog: MACsec MKA Validation – Why Back-to-Back Validation Falls Short](#)



CHAPTER 3

400GE and Beyond

Introduction

Technological evolution breeds complexity. The proliferation of 400GE has started and will grow over the next few years. The coming 800GE, based on the new 112 Gb/s electrical lane technology, demands that overall performance, scalability, and interoperability testing keep up. Partnering with your test vendor to ensure that you get the test tools you need when you need them is critical to being first to market with your innovations.



CHAPTER 3

400GE and Beyond

Key Test Requirements

Test platform port density is a boundary continually pressed to match the increasing port count of switches, routers, and other devices. To get the density you need to validate 25.6 Tbps and beyond switching platforms, look for high-port-count test solutions that can generate multiple terabytes of data and analyze up to 4 million traffic flows simultaneously. For high-performance testing, ensure that your test solution does not lose transmit stream capability and receive-side measurement tracking and measurement capability because of fan-out to 200GE, 100GE, and 50GE.

Flexibility to Validate Both PAM4- and NRZ-Encoded Technologies

Adoption of 400GE requires an 8 x 56 Gb/s electrical interface, PAM4-encoded technology. Most switch application-specific integrated circuits (ASICs) now support PAM4 modulation along with the legacy NRZ encoding used for lower-speed technologies, easing the transition from 100GE to 400GE. Testing all seven speeds from 10GE to 400GE on these platforms is a challenge. Bandwidth requirements for internet applications are driving the need for testing line-rate traffic of 3.2, 6.4, 12.8, and 25.6 Tbps ASICs.

Layer 1 BER and FEC Performance Testing

Reliable network performance rests on the ability to qualify optical transceivers, copper cables, and link partner performance. Test the functional interoperability of your devices and their long-term bit error rate (BER) and forward error correction (FEC) symbol performance. Knowing whether the device produces bursty errors over time and temperature ranges — and how to find these elusive bursty errors — is critical. Many vendors will also need

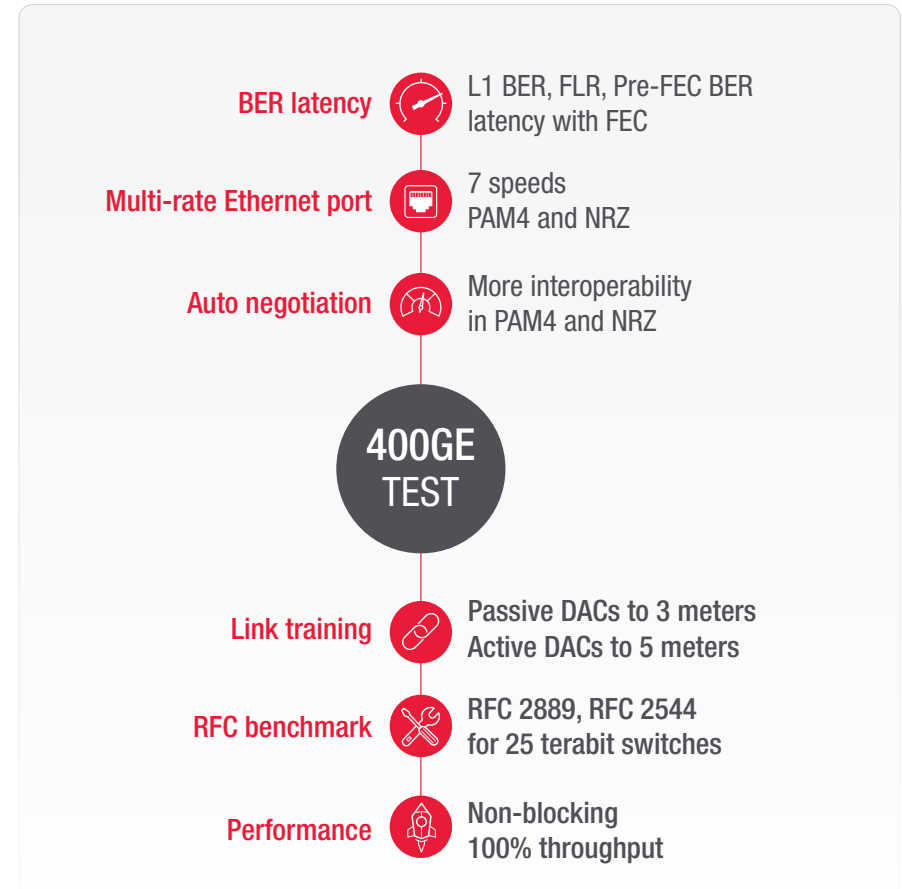



Figure 4. Critical test capabilities for 400GE systems



a test solution to characterize and quantify the actual BER and FEC performance of silicon devices, ASICs, fiber and copper interconnects, optical transceivers, and port electronics.

Field Upgrades to Grow with Test Needs

Many test solutions have features, capacity, or speeds you may need as you build out your product line. The most flexible test solutions are designed for field upgrades to increase your test capabilities. You'll get more cost-effective testing for current needs but have a fast and easy way to provide your development teams with the speeds and test options they need to create the networking technologies of the future.

Keysight Solutions

Keysight's Ixia **AresONE-S**, **AresONE High Performance**, and **AresONE** provide the world's highest-scale 400GE test traffic generation and network protocol emulation.

Keysight's Ixia **A400GE-QDD** is a dedicated BERT and FEC test system that makes the challenge of qualifying BER on 400GE electronics easier and affordable.

Keysight's **IxNetwork** is a comprehensive network infrastructure performance testing solution, capable of generating multiple terabytes of data and analyzing up to 4 million traffic flows simultaneously.

Keysight's **IxVerify** is the industry's only test solution purpose-built for pre-silicon verification and first-to-market with 800GE support.

FURTHER READING



White Paper: Validating the New World of 400 Gigabit Ethernet

Poster: 400GE Forward Error Correction (FEC)

Webinar: Eliminate FEC Frame Loss in 400GE Optical Links and Components



CHAPTER 4

SONiC Open Source Network Operating System

Introduction

Open source and disaggregation have had a significant impact on the world of IT. Just as Linux and the Open Compute Project (OCP) forever changed data center operating systems and server hardware, similar trends are gaining momentum in data center and hyperscale networking. One of these trends is the increasing use of the open source network operating system SONiC (Software for Open Networking in the Cloud). With origins at Microsoft, SONiC is now an OCP project with growing ecosystem support from ASIC vendors, NEMs, and extended ecosystem players providing management and application tools. With support from many of the industry's biggest players and well over 4 million ports in production, SONiC is a real and maturing option.

Key performance indicators (KPIs) around functionality, scale, performance, and resilience are the driving forces for success in data centers. With community-driven development, all these KPIs must be validated during each phase of integration, including reference boxes during ASIC development, original design manufacturing / original equipment manufacturing, and deployment by network operators.

CHAPTER 4

SONiC Open Source Network Operating System

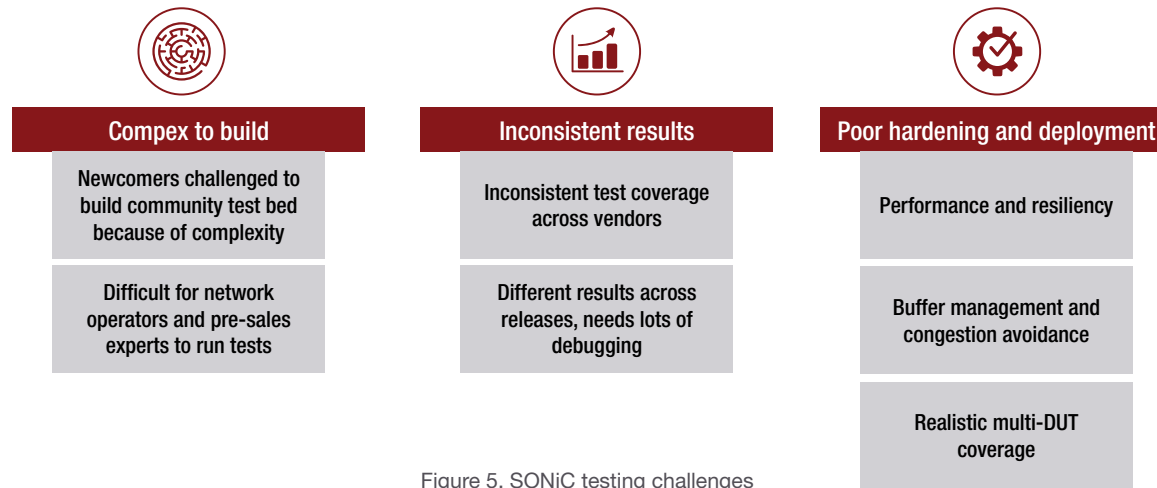


Figure 5. SONiC testing challenges

Key Test Requirements

Testing such a complex ecosystem is a challenge the community is working on as well. However, SONiC community test tools are not always intuitive or easy to use. They may require a fair amount of customization before they work for any particular use case. In addition, community members most involved in creating tests tend to have broad influence, so some testing ends up being vendor-specific.

To get above the noise and complexity, NEMs creating SONiC-ready switching equipment need turnkey test solutions that provide comprehensive, simplified testing. Such solutions will help them speed time to market by focusing on creating products, not piecemeal test solutions. Turnkey test solutions will also provide a vendor-neutral approach that ensures industry-standard test methodologies that offer cross-platform validation.

Look for holistic system integration testing for entire switching fabrics rather than individual device testing products. That way, you'll understand your networking solutions' true readiness to operate within the SONiC ecosystem.

Keysight Solutions

Keysight's **Ixia Open NOS Validation Suite for SONiC** is a simplified, plug-and-play test solution developed with Aviz Networks to fill gaps in today's community tests.

FURTHER READING



White Paper: Overcoming Go-to-Market Challenges of SONiC Solutions

Blog: Testing SONiC, the Linux of Networking

Solution Brief: Ixia Open NOS Validation suite for SONiC



CHAPTER 5

Hyperconverged, Hybrid Cloud Data Centers

Introduction

Applications are quickly transitioning to collections of microservices — often in containers — that can run in any environment and any location (core, cloud, or edge). SDN controls and hyperconverged infrastructure (HCI) solutions are key pillars of hyperscale data centers. These data center solutions need to orchestrate and optimize on-premises infrastructure, multiple clouds, and containerized applications. Virtualization's flexibility creates significant test challenges for NEMs that build both compute infrastructures and virtual network functions (VNFs) that need to support a diverse set of deployment environments, such as virtual machines on-premises and containers in a public cloud.

CHAPTER 5

Hyperconverged, Hybrid Cloud Data Centers

Key Test Requirements

Hyperconverged compute infrastructure runs diverse simultaneous workloads that interact on a massive scale. Testing needs to include the ability to verify proper infrastructure dimensioning and configuration. This process helps with performance and the user experience as you scale your infrastructure. It can also help your enterprise or service provider customers optimize their investments and troubleshoot performance issues on the underlying compute infrastructures that run their workloads.

As applications and data become distributed across multi-cloud, on-premises, and branch edges, networking solutions need to provide seamless end-to-end connectivity and consistent application and security policy management. These changes also bring major unknowns to the performance, scalability, and threat protection of network and security architectures. For a vendor creating networking and HCI solutions for use in such complex topologies, testing is critical to get the right balance of performance, user experience, and security.

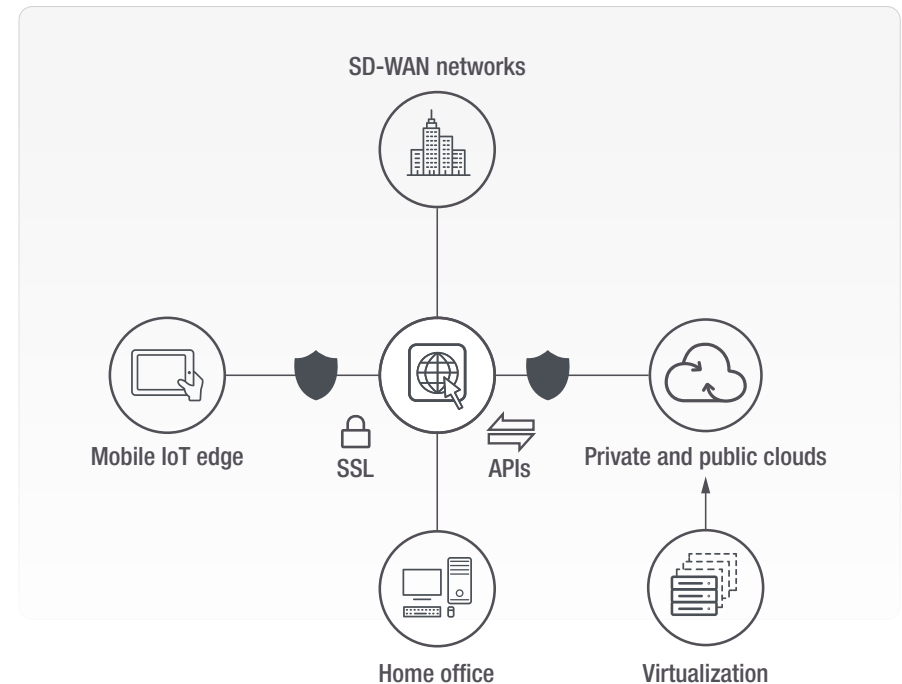


Figure 6. Test topology for distributed networks

Keysight Solutions

Keysight's Ixia **Cloud Peak** benchmarks the performance of virtualized network infrastructures by deploying real virtual machine or container workloads on top of hyperconverged infrastructure.

Keysight's **CyPerf** is the industry's first cloud-native software test solution that re-creates every aspect of a realistic workload across physical and cloud environments to tune the balance between user experience and security.

FURTHER READING



White Paper: Chaos to Control: Validating Distributed, Disaggregated Digital Transformation

Video: Introduction to CyPerf



Introduction

Over time, the security front has not gotten any simpler. Your products have to identify traditional hackers and individual or poorly organized criminal threat actors. They also must find increasingly sophisticated advanced persistent threats (APTs) that can laterally move within the data center and distributed denial-of-service (DDoS) and ransomware attacks. The nation-state APTs are particularly worrying because of their ability to come in low and slow and be persistent over time.

```

        elif operation == "MIRROR Y":
            mirror_mod.use_x = False
            mirror_mod.use_y = True
            mirror_mod.use_z = False
        elif operation == "MIRROR Z":
            mirror_mod.use_x = False
            mirror_mod.use_y = False
            mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror m
        mirror_ob.select= 1
        modifier_ob.select=1
        bpy.context.scene.objects.active = modifier_ob
        print("Selected" + str(modifier_ob)) #1 modifier ob is the a
        #mirror_ob.select = 0
        time = bpy.context.selected_objects[0]
        #bpy.data.objects[mirror_ob.name].select = 1

        #bpy.data.objects[mirror_ob.name].select = 1

        b1_idname =
        b1_label =

        @classmethod
        def poll(cls,
            context: bpy.types.Context):

```

CHAPTER 6

Hyperscale Network Security

Key Test Requirements

NEMs that create network security solutions need test tools that can validate performance, functionality, and security efficacy against real-world application and security traffic that scales to the largest DDoS attacks. They also need to perform proof of concepts for prospective customers with the most relevant traffic profiles. In all of these use cases, realism is the key to effective testing.

Application Traffic Realism

The workloads and traffic mixes you choose to simulate as you validate security appliances need to represent production networks. Getting this mix right is critical to know how security solutions will perform for specific customer types.

Content Realism

Ensure that the payloads in your workload simulation contain realistic, dynamic content, as this will exercise the deep packet inspection, content rules, and data leakage prevention capabilities of your security solutions. Also, the realism of simulated traffic profoundly impacts the observed CPU and memory performance of security devices. Unrealistic simulated traffic can also unfairly show a device in a poor light. A string of zeros in a payload might cause an intrusion prevention system engine to think there is something suspicious, increasing application latency and decreasing overall performance.

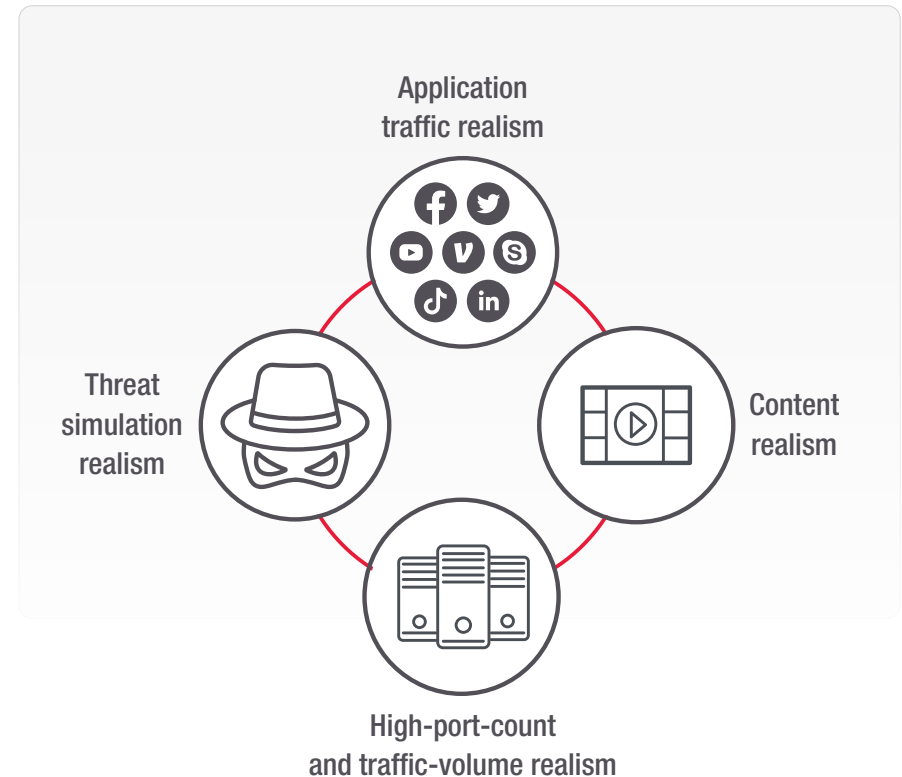


Figure 7. Security test requirements

Threat Realism

It is difficult to correctly measure your security solution's effectiveness as threats arrive with unprecedented diversity, volume, and velocity. Therefore, to truly validate security efficacy, you need threat simulation to emulate a diversified and realistic library of techniques, threats vectors, and kill chain modeling combined with legitimate user and application behavior. Daily malware updates will also keep your testing on the cutting edge.

Keysight Solutions

Keysight's **BreakingPoint** application and security test solution is the leader in simulating legitimate real-world traffic, DDoS, exploits, malware, and fuzzing to enable security infrastructure validation.

Keysight's **CyPerf** is the industry's first cloud-native software test solution that re-creates every aspect of a realistic workload across physical and cloud environments to tune the balance between user experience and security.

Keysight's **Threat Simulator** endpoint security validation capabilities challenge your security controls and validate the security efficacy against signature, behavior-based attacks.

Keysight's **Application and Threat Intelligence Research Center** ensures access to the latest applications, traffic profiles, threat vectors, and breach simulations across our portfolio of security solutions.

FURTHER READING



Blog: [Hyperscale data center environments challenging the status quo of traditional network security testing](#)

Case study: [Optimizing Massive Network Security Infrastructure Upgrade](#)

Case study: [SANS Product Review](#)



CONCLUSION

Testing That Enables High-quality Innovations

In the world of hyperscale data centers, the only constant is indeed change. The sheer volume and speed of data constantly increase. With this, we also see changes in technologies, architectures, compute, and storage, as well as changes in how workloads interact with the network. With all the changes in the data center, it is only reasonable to expect change in how you test and troubleshoot these new technologies and approaches. Getting all these components right is a real balancing act that you can master only through a systematic and robust test strategy and with a trusted partner.

While there are considerable differences in the details of the test areas covered in this eBook, there are also some powerful commonalities. One of the most significant is the importance of realism. The more realistic your test traffic and techniques, the more accurate and meaningful your results and the higher-quality products you produce.

Another factor to consider is that regardless of what you are testing, you are likely facing some sort of commercial time-to-market pressure. While some solutions, such as SONiC, have various free open source test solutions available, they often end up being very expensive in terms of time to test, usability, functionality, breadth, performance, density, and the availability of on-demand support.

Integration with your existing test automation framework is a further area of consideration. Will whatever test solution you are looking at support the APIs you need to play nicely in your continuous integration / continuous delivery workflow?

Another aspect to consider is your own API performance validation. Data center automation and analytics are vital components of an IT strategy. As such, vendors need to ensure that the APIs that manage and orchestrate a hybrid data center are robust, scalable, and high-performing.

When success or failure hinges on your ability to test quickly and effectively, other factors start to matter as well. In addition to the Keysight products highlighted in this document, we've simplified the way we do business with our customers by offering the following:

- **Attractive financing** – Do the testing you need with the budget you have with flexible, attractive finance offerings from [KeysightAccess](#). It can maximize the use of OPEX budget even in situations where you would typically use CAPEX budget.
- **Professional Services** – Keysight has an experienced team ready to help you reduce risk, supplement your staff, and accelerate your projects with [training](#), [consultation](#), [resident expert](#), and other offerings, including [network test-as-a-service](#).
- **Trade up** – Don't worry if some of your gear is old and no longer supported. You can trade in old gear for credit against the purchase of new gear. Keysight / Ixia gear eligible for this offer includes XM, XG, and XGS-HS chassis with Acceleron; NGY; XMV; and other load modules. Ask your Keysight representative for details.

