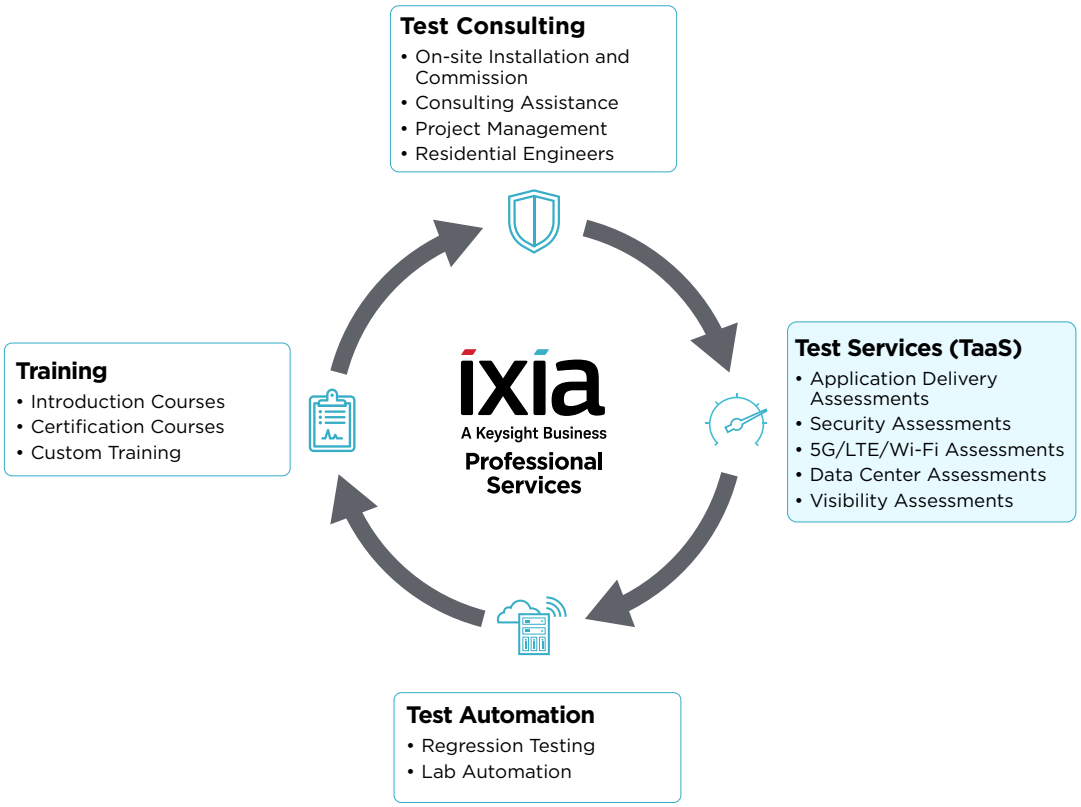
Professional Services
Test as a Service (TaaS)

ixia
A Keysight Business

TABLE OF CONTENTS

Ixia helps enterprises, service providers, and government agencies accelerate and secure application delivery



Just-in-Time Application Delivery and Security Validation

Optimize IT Investments While Minimizing Test Investments

When you need testing quickly—and completed right the first time—Ixia Test as a Service (TaaS) delivers a cost-effective, fast, and accurate approach. In addition to our highly experienced test experts, you'll get access to world-leading test equipment and proven, repeatable test plans and methodologies. Our deep expertise in testing network functions like firewalls, combined with state-of-the-art lab facilities and standardized test methodologies, enables us to deliver deep insights with a quick turn-around. Our professional assessments:

- Offer an easily expensed service that is categorized as an operational expenditure (OpEx)
- Create an easy, as-needed approach
- Deliver actionable analysis of your infrastructure
- Supplement your own technical staff with Ixia test experts
- Reduce project risk by performing timely, real-world testing

Test as a service has a strong return on investment (ROI) while reducing the strain on your internal resources. We help keep high-profile deployments on track, ensuring your end-users' ultimate quality of experience (QoE).

Professionals and Proven Test Plans to Fast-Track Your Test Needs

Our experienced test experts have developed proven plans and methodologies that reduce cost while fast-tracking actionable results. Testing includes:

- Functional, load, and performance validation
- Simulating unique network environments and peak traffic scenarios
- Benchmarking and optimizing device performance
- Assessing site readiness for strategic initiatives
- Validating upgrades and changes prior to deployment in live networks
- Along with standardized test plans that ensure efficiency and repeatability, TaaS assessments feature timely expert reporting and analysis that increases the reach and value of results.

Ixia's Professional Services Organization (PSO) works with leading equipment manufacturers, system integrators, and enterprises worldwide. Drawing on the world's largest, most trusted arsenal of test systems, methodologies, and expertise, Ixia TaaS assessments deliver data vital to making decisions, demonstrating value, and meeting customer expectations.

Ixia TaaS assessments help ensure the success of:

- Network infrastructure upgrades
- Unified communication (UC) rollouts
- Virtualization deployments
- Firewall and other device testing and evaluation

Leverage the World's Leading Test Products

To ensure complete application and security TaaS assessments, Ixia professional services experts leverage industry-leading test solutions that validate the security posture of devices and networks with real applications and a complete range of threat vectors:

- BreakingPoint for application and security testing
- IxLoad for multi-play application services and delivery platforms
- Virtual Edition (VE) for virtual network functions (VNF) testing
- CloudStorm and PerfectStorm for enterprise-scale traffic simulation

To ensure your devices are validated with the traffic profiles and maximum load expected on your unique network, the systems used in our TaaS offerings are the gold standard for application and security testing. These systems are part of our test experts' toolbox and are included as needed to best accomplish each test plan according to customer requirements.

Application and Security Testing

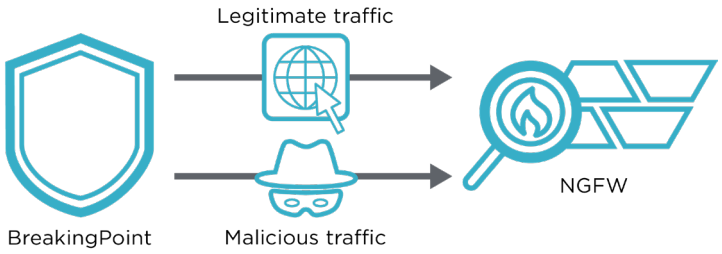
Firewall Efficacy and Performance Test Services

Every well-meaning organization strives to achieve higher security while having minimum impact to their regular business. Unfortunately, any device or function intending to provide added security will almost certainly add delays and impact device and overall network performance if not engineered properly.

By testing different operational modes of your next-generation firewall (NGFW), you can optimize configurations and maximize security effectiveness.

Delivers testing required for:

- Vendor bake-offs
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Network security audits



Firewall Test Topology

Firewall Test Package – Basic

This basic package is recommended for companies getting started with evaluating their NGFW device. As part of this program, the device under test (DUT) will be configured for different scenarios (firewall only, application ID, IPS/IDS) and comprehensively evaluated in the following areas:

- Layer 4 performance: TCP connection rate, TCP concurrent connections, UDP throughput
- Layer 7 performance: HTTP/HTTPS connection rate, HTTP/HTTPS concurrent connections, HTTP/HTTPS throughput, application mix performance
- Latency
- Application filtering

Firewall Test Package - Advanced

The advanced package includes the test cases from the basic package plus the following:

- Vulnerability protection: Security strikes/malware only, both security strikes/malware and legitimate traffic
- Stability: Fuzzing
- Forwarding Parsing

Ordering Information

972-6900 (3-day basic package); 972-6950 (5-day advanced package)

Delivery

Detailed test report with interpretation consultation

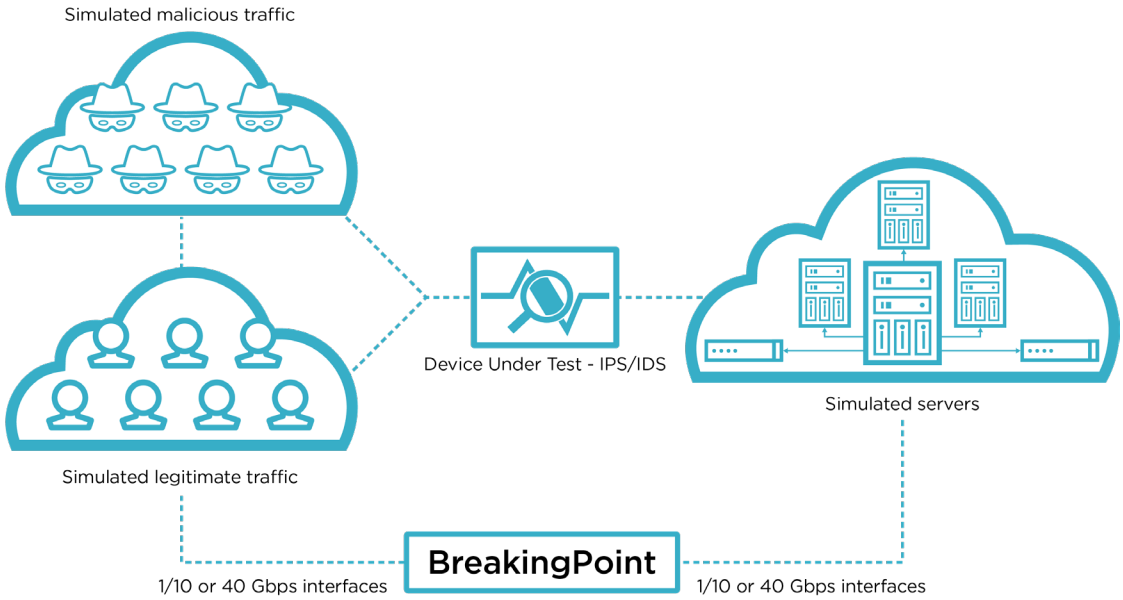
IPS/IDS/DLP Test Services

Intrusion prevention and detection systems (IPS/IDS) and data loss prevention (DLP) solutions promise advanced application visibility, controls, and threat protection to support each unique enterprise network. The policies set on these devices to adjust the level of security generally inversely impacts network performance.

By validating IPS/IDS/DLP under a real deployment scenario, you'll understand the trade-offs of functionality versus performance and the stability and efficacy of your solutions.

Delivers testing required for:

- Vendor bake-offs
- Installation of new security devices
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Network security audits



IPS/IDS/DLP Test Topology

IPS/IDS/DLP Test Package

This package is recommended for organizations purchasing or implementing new devices, setting policies for devices already in place, or undergoing network topology/upgrade changes. As part of this program, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- Layer 7 performance: HTTP/HTTPS transactions per second, HTTP/HTTPS concurrent connections, HTTP/HTTPS throughput, application mix performance, stability
- Markov text generation Security: TCP SYN flood, UDP flood, IP fragment attack, security strikes/malware
- Stability: IP fuzzing

Ordering Information

972-6901 (3-day basic package)

Delivery

Detailed test report with interpretation consultation

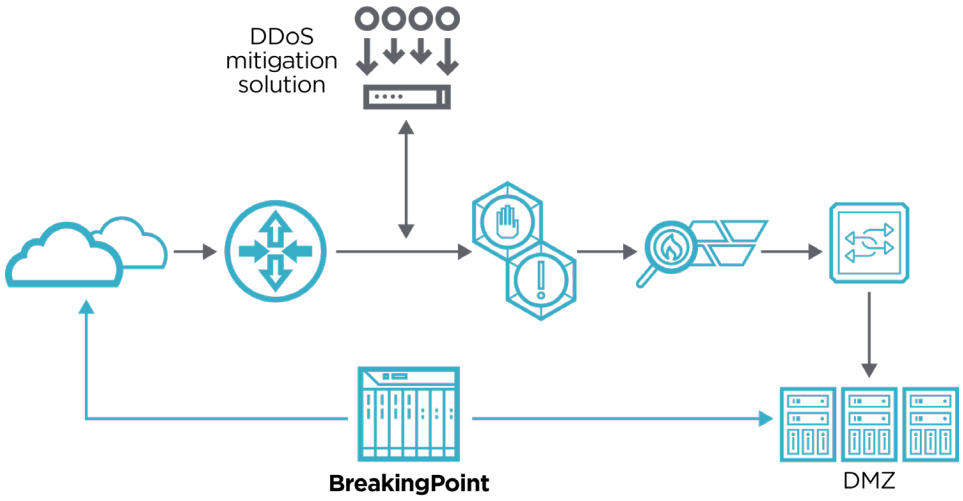
DDoS Test Services

One of the more mature forms of cyber threats, distributed denial of service (DDoS) attacks have evolved from focusing on the transport and network layers to the application layer where protection is more difficult. Today, the attacks are sophisticated, complex and well-orchestrated.

Enterprises are challenged to not only select the best security solution but optimize configuration to balance with network throughput and performance and validate ongoing security updates.

Delivers testing required for:

- Vendor bake-offs
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Network security audits



DDoS Test Topology

DDoS Test Package – Basic

The basic package is recommended for organizations purchasing or implementing new devices, setting policies for devices already in place, or undergoing network topology/upgrade changes. As part of this program, the DUT will be evaluated against the following test cases:

- Baseline Layer 4 performance:
  - TCP connection rate
  - TCP concurrent connections
  - UDP throughput
- Baseline Layer 7 performance:
  - HTTP/HTTPS connection rate
  - HTTP/HTTPS concurrent connections
  - HTTP/HTTPS throughput, application mix performance
- DDoS functional tests:
  - Pre-built DoS attacks

DDoS Test Package - Advanced

The advanced package includes the same types of attacks in the basic package plus the following:

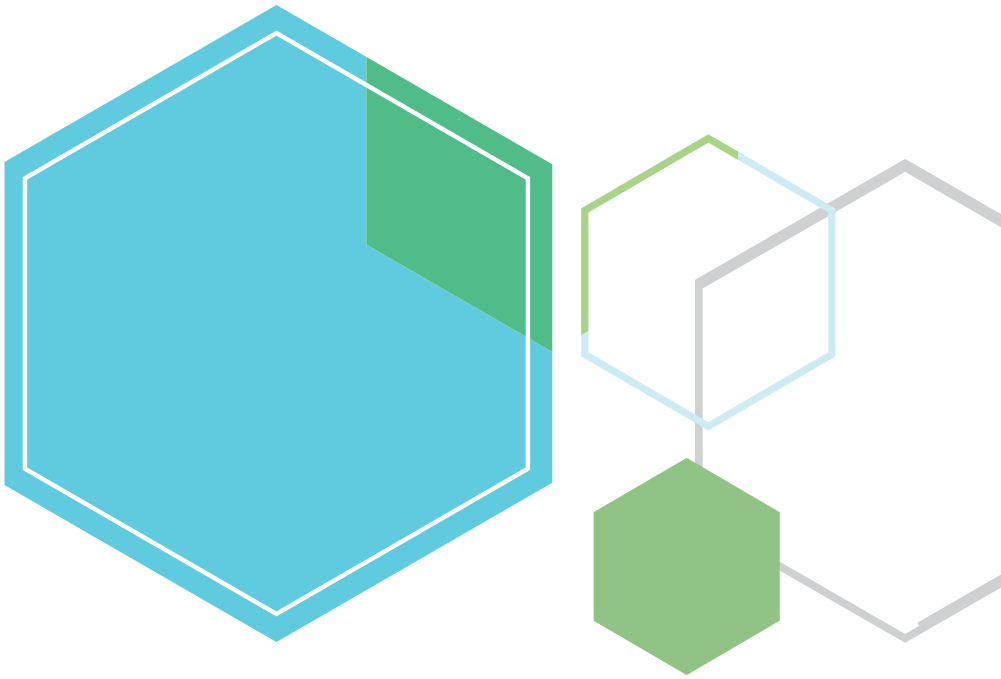
- DDoS functional tests:
  - Customized attack (e.g., UDP pause attack)
- Large Attacks:
  - 50/50 DDoS/legitimate traffic breakdown (certain attack types apply)
  - 80/20 DDoS/legitimate traffic breakdown (certain attack types apply)
- Single Target IP DDoS

Ordering Information

972-6902 (3-day basic package); 972-6952 (5-day advanced package)

Delivery

Detailed test report with interpretation consultation



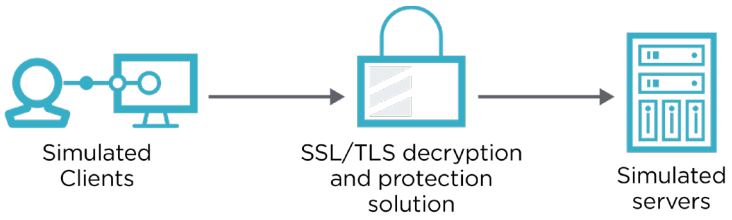
SSL/TLS Offload Test Services

Although secure sockets layer (SSL) and transport layer security (TLS) encryption ensures safe transmission of data across networks, malicious traffic is increasingly encrypted along with good traffic. To ensure all incoming and outgoing traffic is inspected for threats, SSL offloading takes the burden of CPU-intensive encryption and decryption tasks from dedicated security devices not designed for this purpose.

Validation is critical to ensure SSL/TLS offload solutions are high-performing and effective in encrypting/decrypting and load-balancing traffic.

Delivers testing required for:

- Vendor bake-offs
- Installation of new service
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Network security audits



SSL/TLS Offload Test Topology

SSL/TLS Offload Test Package

This package is recommended for companies doing evaluation, initial roll-out, or tuning of an SSL/TLS offload solution. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- SSL/TLS performance – connections per second, concurrent connections, throughput
- SSL/TLS inspection performance
- SSL/TLS decryption performance
- SSL/TLS negotiation on relevant ciphers and key sizes
- Security strikes/malware – ability to detect and block HTTP/HTTPS attacks
- Stability testing

Ordering Information

972-6903 (3-day basic package)

Delivery

Detailed test report with interpretation consultation

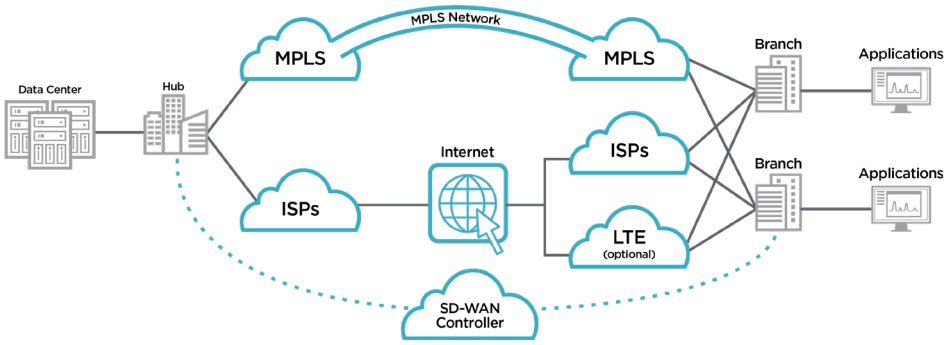
SD-WAN Test Services

Software defined wide area network (SD-WAN) solutions enable management from a central controller using global policies and hardware independence, while maximizing bandwidth efficiency, reducing cost, and simplifying IT management. But a major challenge is the fluid nature and dynamic environment that it introduces.

There is no "one-size-fits-all solution" for every network, so how do you know the best SD-WAN implementation for your particular network? Only by testing can you answer critical questions about how your SD-WAN will perform and how it will impact the rest of your network.

Delivers testing required for:

- Cut-over to SD-WAN network implementation
- Network topology changes/upgrades
- Configuration changes
- Network security audits



SD-WAN Test Topology

SD-WAN Test Package - Basic

The basic package is recommended for companies doing an initial roll-out of a SD-WAN implementation. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- VPN connectivity
- Hub and spoke VPN
- Hub default route
- Spoke default route
- TC005 QoS Application-aware routing

SD-WAN Test Package - Advanced

The advanced package includes the test cases from the basic package plus quality of experience (QoE) and performance analysis

Ordering Information

972-6904 (3-day basic package); 972-6954 (5-day advanced package)

Delivery

Detailed test report with interpretation consultation

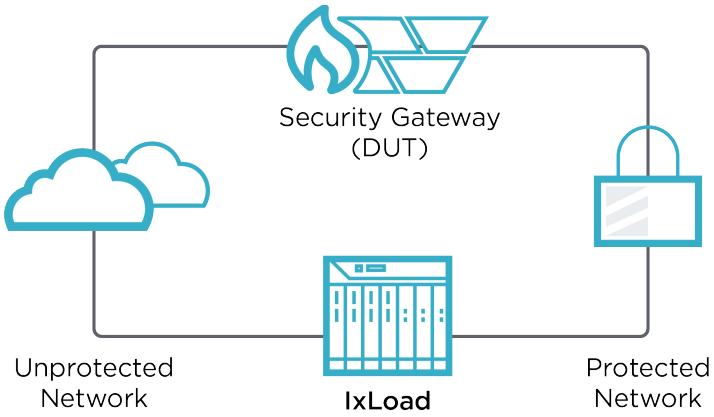
IPsec VPN Test Services

IPsec virtual private networks (VPNs) are part of everyday networks and their functionality and performance is critical for many businesses. The performance of these security gateways has a huge impact on the operation of multiplay networks, services, and applications, and subscriber QoE.

Service providers need pre-deployment validation that includes realistic simulation of dynamic interface setup and tear-down behavior linked with subscriber emulation and network 'blackouts' and 'brownouts'.

Delivers testing required for:

- Security gateway vendor bake-offs
- Subscriber VPN service QoE validation
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Network security audits



IPsec VPN Test Topology

IPsec VPN Test Package

This package is recommended for companies doing an evaluation, initial roll-out, or tuning of security gateways. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- VPN services for both site-to-site and remote access
- Maximum number of IPsec tunnels under various security settings
- Maximum tunnel setup rate
- IPsec throughput and latency measurements with stateless (UDP) and HTTP traffic
- IPsec soak test
- IPsec failover test

Ordering Information

972-6905 (3-day basic package)

Delivery

Detailed test report with interpretation consultation

SLB Test Services

Converged networks support a complex application delivery infrastructure that must recognize, prioritize, and manage multiplay traffic with differentiated classes of service. The emergence of integrated service routers (ISRs), application-aware firewalls, server load balancers (SLB), and deep packet inspection (DPI) devices is enabling businesses to deliver superior application performance and security while improving the quality of experience (QoE) for end users.

Delivers testing required for:

- Vendor bake-offs
- Introduction of new service
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Network security audits

Validating the capabilities, performance, and scalability of SLB begins with the ability to generate stateful application traffic such voice, video, peer-to-peer (P2P), and data services to measure the key performance indicators for each application.

SLB Test Topology

SLB Test Package - Basic

The basic package is recommended for companies getting started with evaluating their SLB solution. As part of this program, the DUT will be configured for different scenarios (basic load balancing, SSL offload, security, stability) and comprehensively evaluated in the following areas:

- Application performance (HTTP/HTTPS) – connections per second, concurrent connections, throughput
- Application forwarding performance under DoS/DDoS attacks
- Impact of filters and inspection rules on application forwarding performance
- Content inspection
- Web security filtering
- Stability testing

SLB Test Package - Advanced

The advanced package includes the test cases from the basic package plus the following:

- Equally distribute incoming traffic to up to 5 server endpoints
- Load balancing to an additional server based on a specific load (e.g. 50%) threshold
- Prioritize traffic to one or more of the server endpoints

Ordering Information

972-6906 (3-day basic package); 972-6956 (5-day advanced package)

Delivery

Detailed test report with interpretation consultation

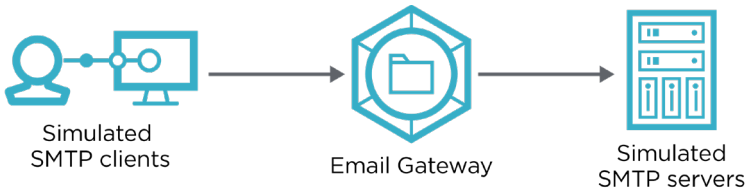
Email Gateway Test Services

The increasing number and complexity of phishing and ransomware attacks and SPAM many times circumvents traditional signature and reputation-based prevention solutions. T oday's networks require the advanced threat defense found in secure email gateways.

This test service employs a real-world legitimate and malicious traffic flows to validate email gateway performance in handling legitimate, malicious, and SPAM emails under high-stress conditions. Extended testing can include stress-testing email filtering engines, including content filtering and phishing attacks via email.

Delivers testing required for:

- Secure email gateway vendor bake-offs
- Network topology changes/upgrades
- Firmware updates
- Configuration changes
- Email gateway security audits



Email Gateway Test Topology

Email Gateway Test Package

This package is recommended for companies implementing advanced threat defense for email systems or making purchase decisions for secure email gateways or other email filtering engines. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- Email processing performance
- Mails per second
- Concurrent mails
- Content inspection – Malware detection
- Multi-languages
- Malicious URLs
- Keywords scanning
- Archive inspection
- Files with macros
- Files with Java scripts
- SPAM detection
- Phishing detection
- Email gateway stability

Ordering Information

972-6907 (3-day basic package)

Delivery

Detailed test report with interpretation consultation

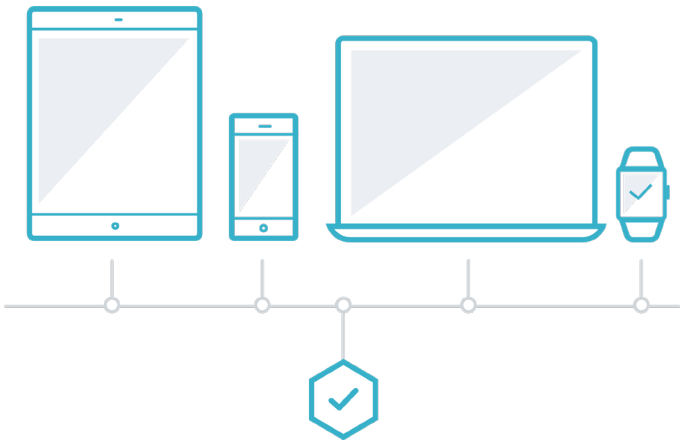
Application Delivery Test Services

In today's highly competitive landscape, organizations must meet stringent network quality requirements to deliver the best customer experience. However, a widening array of multimedia applications, and an increasing number of users, is making it harder—and more expensive—than ever to validate converged multiplay services and application delivery platforms.

Application testing ensures high end-user quality of experience (QoE) by validating with realistic scenario that include web, video, voice, storage, VPN, wireless, infrastructure, and encapsulation/security protocols.

Delivers testing required for:

- Subscriber QoE validation
- Right-sizing your investment
- SLA protection by analyzing the impact of new rollouts and subscriber growth on existing services



Application Delivery Test Topology

Application Delivery Test Package - Basic

The basic package is recommended for end-to-end testing of converged wireless and wired application delivery infrastructure and services. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- DNS testing against a DNS server in terms of number of queries and latency
- HTTP/HTTPS server testing (connections per second, concurrent connections, throughput, stability)
- SMTP server testing
- OTT Video server testing
- Voice over IP service testing

Application Delivery Test Package - Advanced

The advanced package includes the test cases from the basic package plus the following:

- Impact of transport to tailor TE policy to optimize the service
- ECN implementation in data center applications
- PFC implementation in data center applications

Ordering Information

972-6910 (3-day basic package); 972-6960 (5-day advanced package)

Delivery

Detailed test report with interpretation consultation

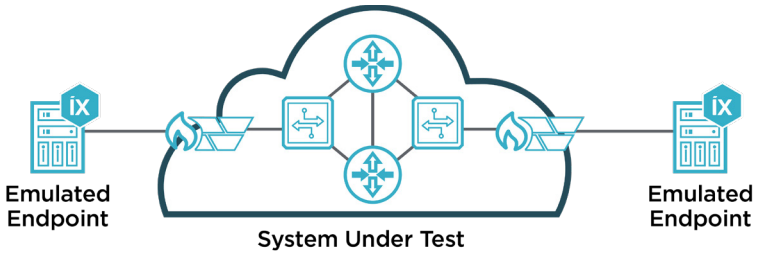
UC/SBC Testing Services

Providing users of mobile devices with rich unified communications (UC) functionality, enterprise-class security, and protected user privacy is no small task. Using a session border controller, IT departments can connect SIP-based UC clients without a VPN, while exposing only the resources needed for UC.

Because the SBC inspects sessions and data for unexpected SIP request behavior, IT groups must not just validate SBC performance and security efficacy but understand their impacts on end-user QoE.

Delivers testing required for:

- SBC QoE
- Capacity of the SBC in your network
- SBC configuration changes
- SBC security audits



UC/SBC Test Topology

UC/SBC Test Package - Basic

The basic package is recommended for companies doing an initial roll-out of a unified communication implementation. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- Determining the maximum call setup rate (CPS)
- VoIP quality of service in converged networks
- Subjective quality of voice
- Determining the maximum transaction rate for VoIP protocols

UC/SBC Test Package - Advanced

The advanced package includes the test cases from the basic package plus:

- Video
- Messaging

Ordering Information

972-6911 (3-day basic package); 972-6961 (5-day advanced package)

Delivery

Detailed test report with interpretation consultation

5G/LTE Testing

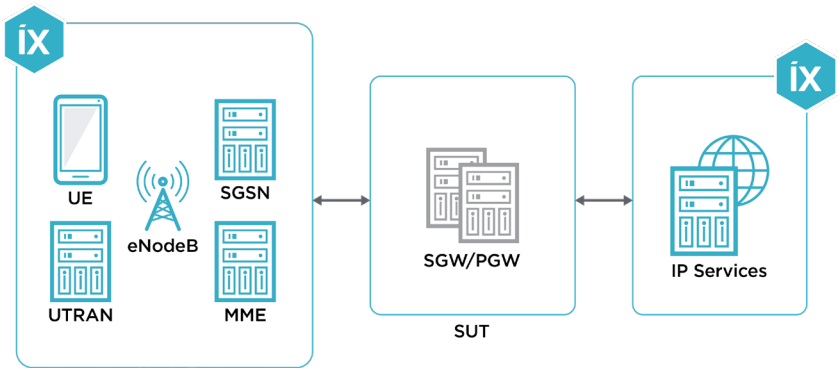
Virtual EPC SGW/PGW Testing Services

Service providers are under constant pressure to modernize networks and deliver an exceptional user experience. Virtualizing network functions, a necessary step in moving to 5G, brings new test challenges to ensure they are high-performing and cost-effective.

Delivers testing required for:

- SGW/PGW performance validation
- Vendor selection
- Software and hardware upgrade
- QoS validation

Scaling new services such as voice over LTE (VoLTE) requires validating at every level, including: scaling new services; optimizing equipment, systems, and applications from multiple vendors; withstanding spikes in already-hard-to-predict signaling traffic; handling simultaneous protocol requests for tunneling and session- or diameter-based signaling.



Virtual EPC SGW/PGW Test Topology

Virtual EPC SGW/PGW Test Package - Basic

The basic package presents a set of tests necessary for the validation of the performance, functionality, and stability of a vEPC device under a real deployment scenario. As part of this service, the DUT will be configured for different scenarios and comprehensively evaluated in the following areas:

- LTE attach/detach/Idle rates
- Handover downlink UDP streaming
- Downlink packet buffering
- UDP bidirectional streaming, HTTP, application throughput
- 5G CIoT throughput and downlink buffering

Virtual EPC SGW/PGW Test Package - Advanced

The advanced package includes the test cases from the basic package plus the following:

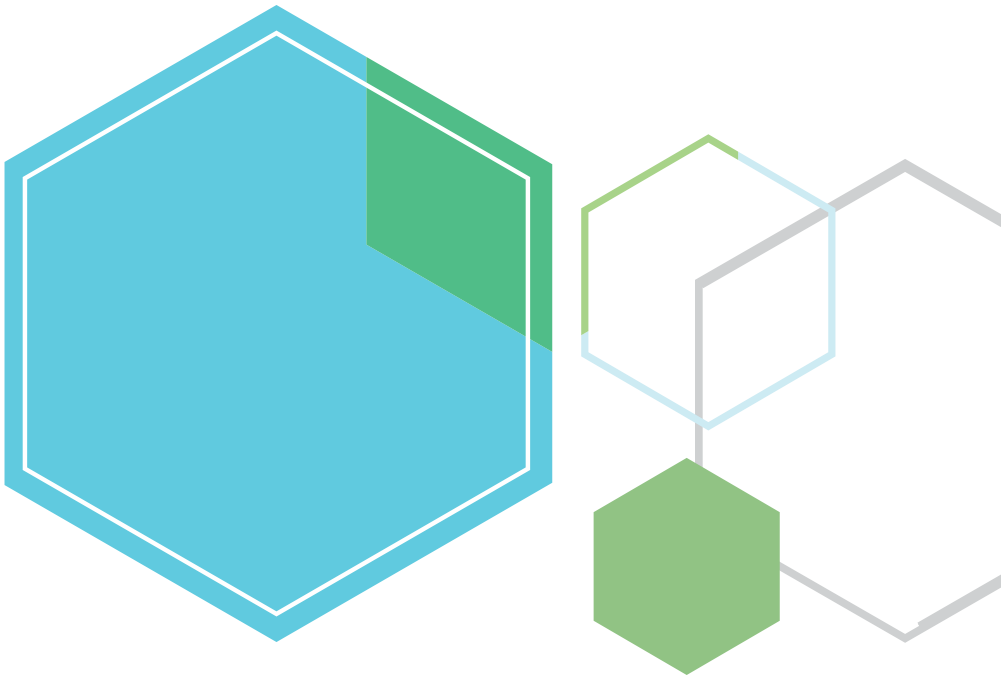
- Validate resource capacity planning for virtual deployments
- Ensure that virtual machines consume resources optimally, without overload or starvation
- Test resource load balancing in system
- Assure QoE is maintained per policy in challenging conditions

Ordering Information

972-3900 (5-day basic package); 972-3950 (10-day advanced package)

Delivery

Detailed test report with interpretation consultation



Schedule Professional Services Testing Today!

For more information about Ixia Test as a Service offerings, please visit www.ixiacom.com/products-services/testing-service-taas or e-mail us at professionalservices-sales.pdl-ix@keysight.com

Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info

915-866-01-2091 Rev A