ixia

QUICK GUIDE

MITIGATING RISK IN NFV

WITH CONTINUOUS SIMULATION AND TESTING

The key to mitigating risk in NFV implementations is a continuous testing and remediation process, which includes the following steps:

First Step, **Develop** the next iteration of your NFV infrastructure and identify how it will operate in the real world:

- On the infrastructure side, which types of VNFs will be deployed and how many, what features they will have, service chaining for common network conditions, resilience characteristics, etc.
- On the end-user side, how many users, throughputs and loads, types of applications, services that are used consistently vs. on demand, etc.

Second Step, **Simulate** traffic and network conditions:

- Set up a staging environment with a realistic configuration of physical hosts, VMs and VNFs.
- Prepare a "test harness" that will allow you to automatically simulate real-life scenarios like failure of a VM, provisioning of new VNFs, etc.
- Artificially generate traffic—both "good" user traffic and "bad" traffic from security attacks or network malfunctions.
- Monitor how your infrastructure and applications respond to a realistic scale of simulated network requests.

To implement a process like this, you must be able to test and validate on demand.

Third Step, **Remediate**—identify problems such as performance issues, security vulnerabilities, and resilience issues and make the necessary changes on your staging environment. Run the tests again to make sure all is okay.

Fourth Step, **Deploy**—push your latest version to production and re-run the tests to make sure you have a solid baseline with none of the previously discovered issues.

Fifth Step, **Shakeup**—periodically re-run the same tests and see if everything still holds up. If problems are discovered, have development resources in place to prepare a quick patch, so you don't have to wait for the next release.

To implement a process like this, you **must be able to test and validate on demand**. It must be possible to comprehensively test your NFV infrastructure even on a staging environment that has no production traffic. You must be able to test anomalous types of traffic, such as security attacks, and simulate realistic loads, which for service providers can mean millions of requests.

The key to testing on demand is the second step—simulation. If you can realistically simulate traffic on the cloud, you can perform accurate tests at any stage of your development process.

MITIGATING NFV RISKS WITH TRAFFIC SIMULATION AND ACTIVE MONITORING

Risk	Ixia Solution
80% of traffic is hidden "East–west traffic" inside and between VMs, is essentially invisible to traditional monitoring architectures and creates a big blind spot for network operations. This could lead to difficulty in diagnosing network performance issues or failure to spot malicious agents within a virtualized data center.	**Phantom vTap**™ provides complete visibility into east–west traffic, which is invisible to traditional monitoring tools. Unlike other virtual tap solutions, which are limited to accessing the internal virtual switch layer, Ixia Phantom vTap monitors all inter-VM traffic, and is able to forward packets to any end-point tool, whether physical or virtual; local or remote. When it comes to mixed virtual/physical monitoring environments, vTap and Vision ONE™ network packet broker provide complete visibility of traffic passing between virtual machines, while delivering zero-loss advanced packet processing with deduplication and packet trimming.
New security risks and a security information explosion NFV introduces new security risks due to new software components introduced into the network, reduced isolation between network segments, sharing of risk between unrelated components, and "key escrow." This is in addition to the complexity of managing security across the physical, virtualized network zone and the application layers.	**BreakingPoint Virtual Edition (VE)** provides simulation of real-world applications and security threats, for the purpose of performance and security testing. Its elastic deployment model allows you to simulate enterprise-scale traffic and realistic threats, to verify the resilience of your security setup.

Risk	Ixia Solution
Continued	**BreakingPoint VE can also facilitate training.** When introducing disruptive technologies like NFV and SDN to your network, your organization will likely hire new talent with relevant skills and train existing employees on the new network environment. BreakingPoint VE can create a closed environment in which new and existing staff can train on operating the network in different security conditions, reacting to attacks and solve problems. With the help of BreakingPoint simulations, they can learn and validate security policies, and understand the performance/security impacts of network changes.
Performance bottlenecks: vSwitch and hardware acceleration To truly understand performance, you must simulate growth in network usage. If overall loads grow by 50%, how will VNF performance be impacted? And if all the load is centered on one type or pattern of traffic/usage vs. multiple? What is the expected performance degradation when using resource oversubscription? Different types of usage may require different service chains, impacting resources in a completely different way.	**IxNetwork® Virtual Edition (VE)** tests functional and performance aspects of physical and virtual network infrastructure. It can help you test capacity, scalability, and convergence, using scaled protocol emulation and simulated traffic. In virtualized data centers and cloud computing environments, IxNetwork VE benchmarks performance of virtualized servers by simulating data center traffic between virtual machines (VMs). It enables the ability to deploy virtual test ports inside virtualized network devices for end-to-end testing of NFV implementations. **IxLoad® Virtual Edition (VE)** provides functional and performance testing to validate Quality of Experience (QoE) in physical and virtual networks. IxLoad VE emulates web, video, voice, storage, VPN, wireless, and encapsulation or security protocols to create realistic scenarios. Real-time, detailed QoE metrics allow you to quickly identify degradation in network performance of functionality and isolate points of failure. The solution can scale elastically as your infrastructure grows. **BreakingPoint VE** helps you see how systems perform under a realistic mix of user traffic, attack traffic, and unwanted traffic. **Virtual taps** can help you access virtual east–west network traffic of interest and hand it off to benchmarking analytics tools to help you identify optimal strategies for hardware acceleration. **IxChariot®** lets you setup a testing “endpoint” within any part of your private cloud infrastructure—hypervisor, machine instances, user devices including mobile phones and tablets, and even servers in different data centers. You can then actively simulate traffic and get an on-demand network performance assessment between any or all of the endpoints.

Risk	Ixia Solution
What to do when something breaks When a host fails, are the VNFs running transitioned appropriately to other hosts? Are the correct rules set up to govern that transition? How long does it take for the VNFs to resume service, and is there an interruption of service? It is crucial to validate the answers to these questions in system testing and in production to prevent critical issues.	**IxNetwork VE** can emulate a router in the NFV infrastructure, or any other part of the NFV infrastructure, to allow you to test behaviors like failover, replication, and scaling up and down. **IxLoad VE** can be used to simulate user and application traffic, such as run different types of real traffic and see what happens when things break. If there are 50,000 users served by a VNF, one of its VMs drop, the failure is detected by the MANO layer and the VM is restored—do users experience interruption in service? How is their performance and functionality affected? **BreakingPoint VE** can be used to simulate a mix of "good" and "bad" traffic. For example, what happens when there is a distributed denial of service (DDoS) attack against a component of the NFV system? Does that component drop completely, or are users able to continue working? What is the performance degradation to expect, and which services will need to be turned off? **IxChariot** performs end-to-end performance testing of VMs, from the VM through to the external network, allowing you to assess your network before going live with NFV systems **Ixia's Hawkeye™** enables proactive monitoring of your virtualized network infrastructure by validating network performance, isolating problems, and proactively detecting issues with scheduled verification tests.

The above solutions can be used both to **test your automated systems** and to **test your IT team's ability to respond** to a more complex problem. If something breaks and the system is not able to recover the malfunctioning component, are IT teams alerted on time and do they have an action plan to resolve the problem?

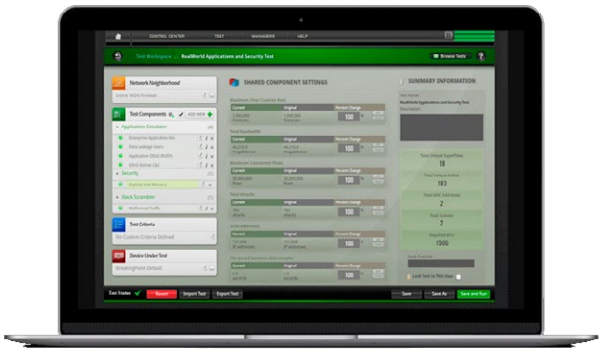
The main point: **Test until it becomes predictable**. Ixia solutions make testing easy, automated, and readily accessible, allowing you to quickly understand the impact of any change to NFV infrastructure.

The main point: Test until it becomes predictable.

BUILDING BLOCKS OF IXIA'S NFV TESTING AND MONITORING SOLUTION

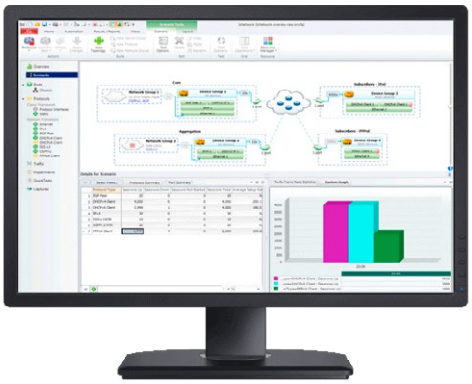
IXIA BREAKINGPOINT VE

End-to-end testing of NFV infrastructure and VNFs.



- Simulates more than 300 real-world application protocols
- Allows for customization and manipulation of any protocol, including raw data
- Generates a mix of protocols at high speed with realistic protocol weight
- Supports more than 36,000 attacks and malwares
- Delivers all types of traffic simultaneously from a single port—either physical NIC or virtual—including legitimate traffic, DDoS, and malware
- Bi-monthly updates ensure you're up-to-date on the latest applications and threats
- Able to run seamlessly as part of your deployed NFV architecture
- Rich API access enabling automated testing in the CI/CD pipeline
- Run realistic user testing with every deployment to a testing or production environment

IXNETWORK VE AND IXLOAD VE

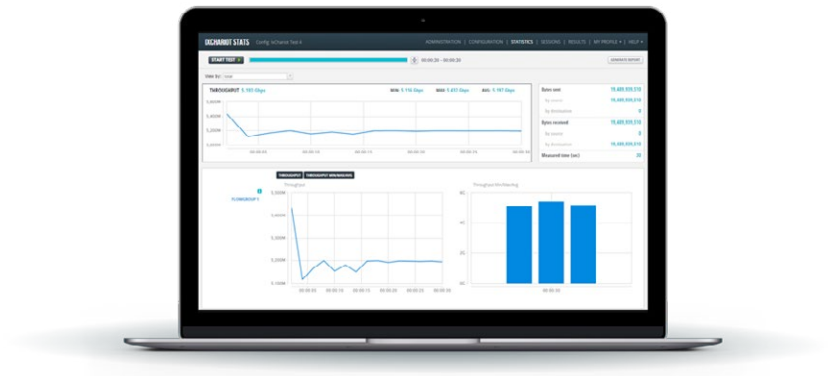


IxNetwork performs realistic performance testing by generating terabytes of data and analyzing up to 4 million traffic flows simultaneously. **IxLoad** can emulate web, video, voice, storage, virtual private network (VPN), and wireless traffic.

Together, the two products provide:

- End-to-end testing of NFV infrastructure and VNFs.
- Real-time insights into quality of experience—the only solution on the market that can model dynamic user behavior.
- A virtual software-based unit that can be deployed together with NFV infrastructure as part of the CI/CD pipeline or hardware-based to enable testing physical network ports and larger traffic scale.
- Comprehensive protocol coverage for routing/switching, multiprotocol label switching (MPLS), broadband, industrial Ethernet (IE), data center networking, OpenFlow, and software-defined networking (SDN).
- End-to-end test system automation, to enable effortless continuous testing.

IXCHARIOT

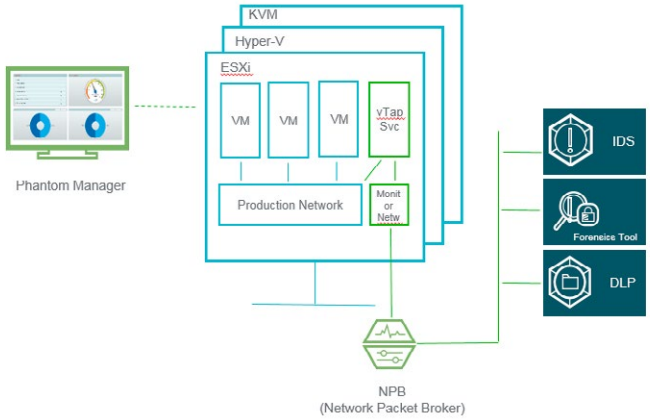


IxChariot performs end-to-end performance testing of VMs, from the VM through to the external network, allowing you to assess your network before going live with NFV systems. IxChariot enables:

- **Deploying software endpoints** to simulate application traffic between any two points in your cloud, or between the cloud and other integrated systems. Software endpoints can be easily deployed within any virtual machine and in any network location.
- **Emulating application traffic** and recording key performance metrics, including throughput, packet loss, jitter, delay, mean opinion score (MOS), application latency, video streaming, over-the-top (OTT) video, such as YouTube and Netflix, and more.
- **Testing VM-hypervisor integration performance:** Install software endpoints in any virtualized network component and measure full end-to-end performance, including the TCP/UDP stack, over the hypervisor.
- **Testing hypervisor performance:** Deploy 100s of VMs with software endpoints and perform mesh tests for hardware/software performance characterization.
- **Testing software-defined wide area network (SD-WAN) deployments:** Place software endpoints in virtual customer premise equipment (vCPEs) for service turn-up verification, including bandwidth and IP performance validation.

- **Assessing NFV migration:** Software endpoints can be deployed easily in your live network and used to validate end-to-end network architecture performance before going live with an NFV migration.

VIRTUAL TAPS AND PACKET BROKERS



- Bridges the physical and virtual, so that you can monitor the virtualized network with your existing set of tools
- Capable of capturing and then sending and inter-VM traffic (east–west Traffic) of interest to the tools that are already monitoring your physical network
- Enables monitoring for security and compliance in virtualized environments
- Applies existing physical monitoring tools, processes, and procedures to the virtual network
- Aggregates virtualized traffic, filters, and grooms to remove redundant information, load-balances, and passes traffic on to external tools for closer inspection

SEE FOR YOURSELF HOW IXIA HELPS MITIGATE NFV DEPLOYMENT RISK. SCHEDULE A DEMO.

WORLDWIDE HEADQUARTERS

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(FAX) 1.818.871.1805

www.ixiacom.com

EUROPEAN HEADQUARTERS

Ixia Technologies Europe LTD
Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

ASIA PACIFIC HEADQUARTERS

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127