WHITE PAPER

ixia

How to Maximize IT Investments with Data-Driven Proof of Concept (POC)

6-Step Guide to Ensure You are Making Defendable Decisions to Secure Your Network

915-4033-01 Rev A, April 2014

Table of Contents

Executive Summary

IT organizations are making major investments in consolidating and rebuilding data centers and enterprise-wide networks. Adopting new network technologies is unavoidable and even critical in the face of today's exploding bandwidth demands and shifting security landscape. In spite of the high costs, most organizations still feel at risk and uncertain of their investments. This is largely because most IT organizations make purchase decisions based on vendor marketing datasheets and anecdotal information from technology suppliers.

In spite of the high costs, most organizations still feel at risk and uncertain of their investments.

Much of today's important technologies are content-aware and respond differently to the kind of traffic that is presented. No generic datasheet or anecdotal reference can answer this question that is critical for IT decision makers, "How will this technology respond in my unique network?" To answer this question and instill confidence with all stakeholders, new technology must be tested against an enterprise's unique traffic that includes real-world user behavior and real-world security threats.

This is especially true when considering new innovative technologies that may perform better or are less expensive, but are offered by non-incumbent vendors. IT managers need a better way to conduct proof of concepts (POCs) in technology and vendor section to optimize investments and provide quantifiable data to validate decisions and instill confidence in their organization.

This paper presents a six-step methodology for conducting a competitive POC that provides advance insight into the performance, security, and stability of devices within production network and data center environments. By following the methodology presented in this paper, companies will:

- Select the firewall, intrusion prevention systems (IPS), unified threat management (UTM), load balancer, data loss prevention (DLP), storage solution, virtualized server, or other device that best meets business and IT objectives
- Save money on technology purchases by right-sizing your investment with definitive data
- Understand device capabilities to improve infrastructure planning and resiliency
- Save up to 50 percent on IT investments by showing your vendor what the actual performance of their gear is in real use, rather than the best-case numbers they hype
- Collect data to justify a decision to adopt innovative non-incumbent supplier technology or to stay with upgrades from established vendors
- Eliminate hundreds of man-hours in post-purchase configuration, troubleshooting, and tuning

Introduction

IT organizations embarking upon a network, security, or data center infrastructure upgrade need new methodologies and tools to test and validate the performance, security, and stability of today's content-aware devices. To make purchase decisions about firewalls, IPS, servers, load balancers, DLP, WAN optimization and so on, CIOs, CISOs, and other IT leaders need better information than traditional testing tools can provide.

Why? Because today's content-aware and application-aware devices employ deep packet inspection (DPI) capabilities to examine traffic in ways that legacy testing approaches were never designed to validate. Such devices—and the complex traffic they handle—

demand a new and deeper approach to comparative device testing that uses real application, attack, and malformed traffic at ever-increasing speeds. Without this improved approach, content-aware equipment cannot be stressed thoroughly enough to determine the true limits of its capabilities.

This paper explains the six steps that organizations must follow to validate content-aware devices and make fully-informed purchase decisions:

1. Create and prioritize specifications for products to be evaluated
2. Develop a POC testing plan around repeatable, quantitative principles
3. Use standardized scores to separate pretenders from contenders
4. Create individual test scenarios that mirror the production environment and are repeatable yet random
5. Execute a layered testing progression that includes load, application traffic, security attacks, and other stress vectors
6. Lay the groundwork for successful deployment and maintenance

Companies need an approach that allows them to impose their own conditions during pre-purchase evaluations—also known as proof of concept "bakeoffs"—so that they can rigorously validate device capabilities under real-world scenarios at line rate.

Why Marketing Claims Are Not Sufficient

Vendor performance claims are based on generic conditions within a vendor's lab, and will never be sufficient for making sound purchasing decisions. They can never accurately portray the resiliency—the performance, security, and stability—of devices as they handle the unique mix of traffic within a particular network. Test lab reports are equally inadequate. These labs follow a "vacuum" or "clean room" approach, in which device testing is done in isolation, without regard to the unique environments of companies. Also, test labs are often funded by device manufacturers, which invariably call into question the objectivity of test results.

Companies need an approach that allows them to impose their own conditions during pre-purchase evaluations—also known as proof-of-concept "bakeoffs"—so that they can rigorously validate device capabilities under real-world scenarios at line rate. Only by conducting this type of POC will IT buyers acquire the actionable answers needed to make informed purchase decisions and eliminate time-consuming post-deployment troubleshooting.

"... high-profile performance and security failures are bringing renewed focus to the importance of sufficient testing to ensure content-aware network devices can perform under real-world and peak conditions...Network equipment providers, service providers, and other organizations require testing solutions capable of rigorously testing, simulating, and emulating realistic application workloads and security attacks at line speed.

Equally important, these tools must be able to keep pace with emerging and more innovative products as well as thoroughly vet complex content-aware/DPI-capable functionality by emulating a myriad of application protocols and other types of content at ever-increasing speeds to ensure delivery of an outstanding quality of experience (QoE) for the customer and/or subscriber."

IDC Report: The Inevitable Failure of Content-Aware/DPI Network Devices — and How to Mitigate the Risk

Benefits of a Successful POC Validation

IT professionals responsible for choosing content- or application-aware network and security equipment should follow the steps outlined here to ensure that devices are fully evaluated before purchase and deployment. Using the findings of pre-purchase and pre-deployment testing, they can refine their understanding of the unique real-world conditions affecting their networks. By following the six steps for device POCs explained in this paper, IT organizations will ensure that they:

- **Select the right products to meet their business objectives.** Doing this requires a clear knowledge of device resiliency when handling a mix of real application traffic, security attacks, and malformed traffic under heavy load.
- **Understand device capabilities to improve infrastructure planning and resiliency.** The information gained during the POC process allows IT planners to right-size network and data center infrastructures to meet business needs for resiliency while controlling costs.
- **Save up to 50 percent on IT investments.** IT organizations that perform independent testing are able to right-size infrastructures and pay for only the performance they actually get from each device. As this paper will show, buyers negotiate better vendor discounts when armed with detailed information about the capabilities of devices under their own particular network conditions.
- **Justify leading-edge, but non-incumbent vendor technology.** Large enterprises are many times reluctant to adopt the startup mentality of investing in non-incumbent vendor gear, even when there is a better or less expensive technology. With technology advancing so quickly, this can put such enterprises at a disadvantage. Data from a POC provides IT managers with data-driven documentation to justify adopting new technologies or negotiating with incumbent vendors.
- **Eliminate hundreds of man-hours in post-purchase configuration and tuning.** Performing thorough pre-purchase validation gives IT organizations advance knowledge of device capabilities and prevents weeks of delays caused by post-deployment troubleshooting and vendor finger-pointing. This insight also helps IT organizations configure devices appropriately to avoid surprises and disruptions.

> "The providers of complex network security devices frequently make marketing claims that are unsupported by hard evidence and, in any case, do not reflect the real-world requirements of specific enterprises. The only solution for prospective buyers is to define their own enterprise-specific business, security, and operational requirements, and test devices rigorously against those requirements...
>
> Security professionals must be prepared to test in-line security products to confirm their security effectiveness and performance capabilities under real-world conditions."
>
> **Gartner Report: Guidelines for CISOs: A 10-Step Program for Selecting the Right Network Security Devices**

IT professionals responsible for choosing content- or application-aware network and security equipment should follow the steps outlined here to ensure that devices are fully evaluated before purchase and deployment.

Case Study: A Data-Driven POC

A financial institution made the decision to upgrade its existing stateful firewalls to next-generation firewalls and new 10Gbps networking. The bank wanted to adopt a single-vendor solution to ease integration and management. The company had four distinctive use cases across the enterprise network: office, public web, partner portal, and e-banking.

Using datasheets and anecdotal information, the IT department narrowed down the final section to three vendors, including the incumbent firewall vendor.

Using Ixia's BreakingPoint application and security test solution, traffic models were created for each of the enterprise use cases, as well as a synthetic TCP traffic flow to create a maximum throughput baseline.

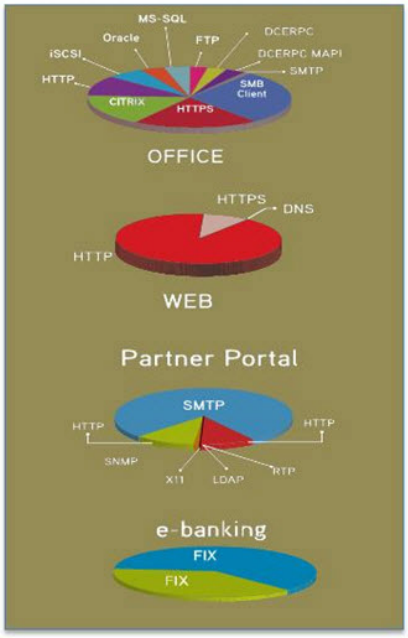

Figure 1: Test traffic needs to accurately model an individual company's actual traffic.

The TCP baseline indicated with simple synthetic traffic that all three vendors showed similar performance. However, it should be noted that each vendor advertised 10Gbps or greater performance and none reach 10Gbps with the baseline synthetic TCP traffic mix with target security modules enabled.

Subsequent performance tests were run with the defined four real-world traffic mixes that also had security attacks embedded into the traffic flow.

The time required to produce the charts and the data to back up the purchasing decision took three days to complete.

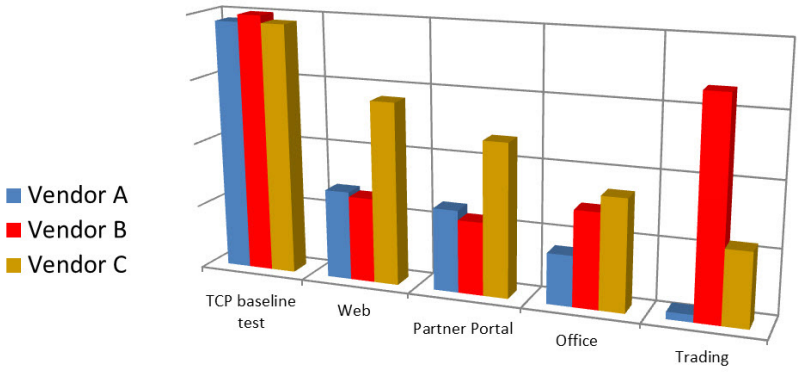

Figure 2: POC results show that with a baseline test, all three vendors are about equal, but in specific traffic tests, they varied greatly. Enterprises need this type of information to make the right decisions on new device purchases.

Which vendor do you think the bank chose? It wasn't the incumbent supplier, Vendor A.

Six Steps to the Perfect Competitive Device POC

Step 1: Create and Prioritize Specifications for the Product Being Evaluated

As with any project, it is wise to "begin with the end in mind" when planning a device POC bakeoff. Before considering any piece of equipment, IT decision makers should clearly define and prioritize the organization's needs for current and future infrastructure build-out. Otherwise, it is too easy to dive into questions of speeds and feeds without taking into account broader objectives. A good way to start is by asking fundamental questions such as:

- How should the infrastructure support key business objectives? For example, what are the transaction latency requirements?
- How important is the security of transactions in comparison to their speed?
- Which services are most sensitive, requiring the highest levels of security?
- Is application inspection necessary or not?

The answers to questions like these may not be as obvious as they initially appear. Obvious or not, they help establish the priorities for the infrastructure, which are then used to generate specific evaluation criteria for selecting the right product.

Making this selection is about more than finding the right make and model of device; it also means choosing the right amount of equipment to right-size the infrastructure while meeting business needs. To enable rightsizing, it is important to suspend assumptions about how many devices will be required, because the approach to POC described here often leads to surprising insights that overturn assumptions.

In one recent example, a large financial services organization had planned to purchase two sets of redundant firewalls for a particular installation. But the company was working from a false assumption about how many devices it would actually need. A scientific POC enabled the firewalls to be validated and properly tuned using the firm's actual network conditions instead of canned traffic or estimates. This process revealed that the firewalls performed better than expected. The company needed to buy only one set of redundant devices, not two, which cut its firewall bill in half.

To facilitate the capture and rigorous analysis of performance results, IT organizations may want to build out a Planning Matrix as shown in Figure 3. In a spreadsheet, each important feature of devices to be evaluated is given its own row, with the rows arranged in priority order. Weighted values are then assigned to each row. Each device being considered is given its own column, and the columns are filled in as results are gathered from the testing processes described below. When the matrix is fully populated with performance details, it should provide objective clarity about how well each device performed across all criteria.

"Testing is not necessarily about proving that the most-capable, most-expensive product is the best choice. A well-designed testing plan may actually show that a lower level of performance is acceptable at certain points on the network, and this can reduce purchase and deployment costs. IT organizations that do not perform relevant tests in-house may introduce serious security and performance issues to their networks by purchasing underspecified devices, or may overspend significantly on higher levels of performance and coverage that are not required."

Gartner Report: Protecting the Enterprise: Verifying the Performance of Complex Network Security Products

Metric	Weight	Device A	Device B	Device C
Security Coverage				
Attacks Blocked (%)	35%	65	72	73
Performance				
App Flows per Sec	35%	111,374	97,764	119,384
Max Concurrent Flow	20%	2,000,000	2,350,000	1,850,000
Throughput (Mbps)	15%	11,542	13,127	9,842

Figure 3: POC Planning Matrix

The entire plan must embrace a scientific methodology to accurately validate the capabilities of content aware devices, which means it must use repeatable experiments that yield clear, quantitative results.

Step 2: Rethink Testing around Repeatable, Quantitative Principles

IT organizations should use the specifications generated in Step 1 to create a plan for stressing each device under test (DUT) with real-world application, attack, and malformed traffic under load. Doing so is not as simple as taking older, ad hoc approaches to testing and injecting authentic traffic. The entire plan must embrace a scientific methodology to accurately validate the capabilities of content-aware devices, which means it must use repeatable experiments that yield clear, quantitative results. Only this approach ensures that the evaluation criteria established in Step 1 will translate into the specific parameters evaluated during the testing itself.

Elements to include in the plan:

- **Controlled Variables —** Throughout the planning and execution stages, the POC bakeoff must rigorously control variables. The goal should always be to isolate device capabilities and problem areas, which—as in any scientifisc investigation—requires repeating tests exactly and changing only one input at a time.
- **Accurate Baselines —** As a further control, each test process should include an initial run through a simple piece of cable to establish what the traffic looks like without intermediation by any device. Doing so creates a valid basis for comparison against the subsequent run of the same traffic through the DUT.
- **Uniform Configurations —** Consistent collection of data requires that devices be set up uniformly throughout the POC. This means that each vendor should configure its device to match standard settings established by the IT organization. It also means that settings for the testing equipment should be maintained across all DUTs.
- **Escalating Complexity —** To achieve a comprehensive understanding of device capabilities, POC testing should proceed by stages, evolving in complexity until it

fully reflects the IT organization's unique mix of traffic. The first of these stages, explained in Step 3 below, uses standards-based application, attack, and malformed traffic to evaluate a longer list of devices and quickly eliminate obviously unsuitable choices. The second stage, addressed in Steps 4 and 5, uses custom traffic mixes and progressive rounds of testing to precisely mirror the actual conditions that short-listed devices will face once they are deployed in the IT organization's infrastructure.

- **Precision Tools —** POCs must use testing tools that create precise real-world network conditions again and again and enable variables to be changed one at a time. These tools must also capture exact measurements of device behavior to enable accurate comparisons among devices.

In the past, network and security professionals have lacked the precision tools necessary to enforce truly-consistent, scientific standards across their testing processes. That has hampered their ability to make decisions based on hard quantitative data and forced them to make estimates about device resiliency based on whatever performance numbers they could gather. Today, however, superior tools create authentic application traffic and capture precise measurements of its effects, even for the complex interactions common in 10GE/40GE content-aware environments. Companies that lack such tools can employ them for the duration of a POC by contracting with a third party for on-demand device evaluation services.

Step 3: Use Standardized Scores to Separate Pretenders from Contenders

By using standardized scoring methods, IT organizations can turn a long list of candidate devices into a short list without performing comprehensive validation on each product. These scores can quickly eliminate from consideration equipment that clearly does not meet an organization's needs.

By using standardized scoring methods, IT organizations can turn a long list of candidate devices into a short list without performing comprehensive validation on each product.

For example, the Ixia BreakingPoint test solution features a Resiliency Score that is calculated using industry standards from organizations such as US–CERT, IEEE, and the IETF, as well as standard sets of security strikes and real-world traffic mixes from the world's largest service providers. This scientific, repeatable process is designed to enable meaningful comparisons without partiality to any particular vendor. It uses a battery of simulations to evaluate a DUT's capabilities in terms of throughput, sessions, and robustness in the face of corrupted traffic and security. The resulting score is presented as a numeric grade from 1 to 100. Devices may receive no score if they fail to pass traffic at any point or degrade to an unacceptable performance level. The Resiliency Score takes the guesswork and subjectivity out of validation and allows administrators to quickly understand the degree to which system security will be impacted under load, attack, and real-world application traffic.

The product certification firm Underwriters Laboratories (UL) has a similar standard, UL 2825, that uses a scientific evaluation system to validate network and security equipment. It serves as a vendor-neutral benchmark for the performance, security, and stability of devices. UL has published certifications for all equipment that meets the standards set forth in UL 2825.

IT organizations can use one of these standardized scores to evaluate a list of perhaps six to 10 candidate devices. Working from the scores, they can then choose the three or four most suitable devices for deep, customized testing. Using standardized scores at this stage saves time and money by quickly establishing which devices are the most likely to fulfill the business needs set out earlier in the process. Formulation of the custom tests for short-listed devices is covered in Step 4, while execution of them is addressed in Step 5.

Step 4: Create Individual Test Scenarios That Mirror the Production Environment and are Repeatable yet Random

Generating real stateful traffic, however, is not enough: validation processes must also be repeatable yet random.

With this step, the POC process moves into comprehensive testing to fully validate the capabilities of DPI-enabled devices. Authentic validation requires an accurate understanding of the application, network, and security landscape in which devices will be operating. Therefore, IT organizations should review their own traffic mix and the mixes of service providers before designing individual tests; this will ensure that their testing equipment reflects the latest versions and types of application traffic that traverse their network. They should also consult independent security research as well as the findings of their own in-house network or security operations centers for the latest information on security attacks, including malware and evasions. Companies that need help in collecting this information can turn to on-demand services that specialize in network security.

It is important to note that packet captures (PCAPs) of network traffic are inadequate for this survey of the landscape, since they attempt to substitute a tiny slice of real traffic for a steady flow of it. Modern application-aware devices typically come equipped with huge cache memory, allowing them to ignore repetitive traffic such as that found in PCAPs. Simplistic traffic such as plain UDP or HTTP packets, IMIX, or a blend of a few homogenous protocols is likewise inadequate, because it does not reflect the complexities under which DUTs will operate once they are put into production. For these reasons, real stateful application traffic, along with live attacks and malformed traffic, must be used to push devices to their limits.

Generating real stateful traffic, however, is not enough: validation processes must also be repeatable yet random. Repeatability demands that the testing equipment generate the same traffic in the same way for each DUT to ensure accurate “apples to apples” comparisons. Randomization makes test traffic behave like real-world traffic, creating unexpected patterns that force DUTs to work harder. Randomization prevents vendors from relying on self-published performance numbers achieved in sterile environments designed to show their wares in a favorable light. Creating repeatable yet random traffic requires the use of a pseudo-random number generator (PRNG). Using a PRNG, the IT organization sets a seed value, which the testing equipment uses to create standardized tests by generating all data variants in the same way for each test executed, whether for a single DUT or several.

> "Evaluate shortlisted network security devices against a realistic range of potential live attacks...
>
> Testing can expose performance-related problems caused by inappropriate security products, including high latency and frequent “fail closed events.” This, in turn, may result in active devices being deployed passively or blocking being disabled, making the devices significantly less effective."
>
> **Gartner Report: Guidelines for CISOs**

Creating test scenarios around these guidelines reinforces the quantitative, scientific principles laid down in Step 2 and prepares the way for the actual battery of customized tests to be performed in Step 5.

Step 5: Execute a Layered Testing Progression That Includes Load, Application Traffic, Security Attacks, and Other Stress Vectors

This stage is the "main event" of a competitive POC and, as such, deserves more detailed treatment here. During this stage, the wisdom of a progressive, scientific approach to testing will become clear. By changing only one variable at a time and testing the parameters set forth at earlier stages, this progression will reveal the specific strengths and weaknesses of each product, replacing guesswork or uncertainty with verifiable results.

Once deployed, a device will not be subjected to one type of stress at a time; instead, it must deal with application traffic, heavy user load, security attacks, and malformed traffic all at once. That is why the ultimate test in this progression will bring together all of those elements into a single battery of tests. But to develop a proper understanding of how a DUT handles specific types of stress, its ability to handle load and attacks will be tested separately first. Subsequent processes will combine validation of load, security, and stress vectors. During the POC, IT organizations should archive all of these tests so that they can be repeated exactly during the deployment phase explained in Step 6.

Load-Only Tests

A device's specialized capabilities—to block malicious traffic, detect trigger keywords, and so on—are not meaningful unless they perform adequately under heavy load. The processes described in this section ensure that the device being evaluated can easily handle the load it will face, in terms of both sessions and application throughput. If the device cannot pass these tests with traffic known to be free of attacks, there is no way it will process enough traffic once its security features are turned on or when it must also handle other stress vectors such as malformed traffic.

A device's specialized capabilities—to block malicious traffic, detect trigger keywords, and so on—are not meaningful unless they perform adequately under heavy load.

Sessions

This set of tests uses TCP traffic to validate the DUT's ability to (1) create and tear down TCP sessions at a prescribed rate and (2) handle a prescribed maximum number of concurrent sessions. Each of these tests can run in stair-step fashion, ramping up the degree of stress by steady increments until the device fails. This will determine whether the device achieves its advertised limits and how much headroom it has to handle peak traffic.

Application Traffic

These tests determine a device's ability to handle real stateful application traffic at high levels of load. Ixia BreakingPoint, for example, offers a standard enterprise application traffic mix that includes more than a dozen of the protocols most-commonly found traversing Global 2000 corporate networks. That mix can then be customized by changing the weighting of various protocols or by adding other protocols that better reflect the organization's unique network environment.

The session and application traffic processes should all be run three times. The first pass is a baseline run, using only a piece of cable and no DUT. The second pass is performed with the DUT in place but with no security or inspection policies turned on. This should result in the purest measure of the DUT's maximum ability to relay traffic. The third pass

is performed with the device's default security or inspection policies turned on. Since the device will be handling traffic that includes no attacks, evasions, or malformed packets, the policies should yield no positive results. But running this process will indicate the basic impact on performance that comes from having the target device's application-aware features engaged.

Having probed the DUT's ability to handle load without the complications of security attacks, it is time to try the opposite case: security without load.

Security-Only Tests

Having probed the DUT's ability to handle load without the complications of security attacks, it is time to try the opposite case: security without load. A firewall, IPS, or UTM device will never be better at blocking attacks than when it has no background traffic to contend with, so this portion of the testing will reveal how a DUT's security features perform under ideal conditions.

Keeping the device's default security policies in place, the IT organization runs a standard list of security attacks to see how well the DUT catches known malicious traffic. The IT organization then customizes the tests in two ways: (1) tailoring the strike list to exercise particular security policies within the device and then (2) tailoring the device's security policies to handle particular strikes relevant to the IT organization's network environment. As with all of the other processes in the POC, these variables should be changed one at a time so that each test-run can be used to isolate particular device capabilities and problem areas. Besides establishing the basic security capabilities of a firewall, IPS, or UTM, the customization in this portion of the POC will also give IT staff members an idea of what level of support they can expect from a manufacturer. Vendors will likely never be more responsive than when they are trying to close a sale, so the customer support during this phase should be excellent.

Load and Security Combined Tests

This phase of the POC combines the ultimate tests from the preceding Load and Security sections. While this does not complete the range of authentic conditions that will be included in the next testing phase, bringing these two validation processes together may be a watershed for some devices that simply cannot handle the combination of load and security attacks.

All Stress Vectors

The layering process concludes by adding other stress vectors that the DUT will encounter in a production environment.

Malformed Traffic

This traffic can appear maliciously, or simply from device malfunction. Either way, malformed traffic is a fact of life on every network and must be included in the POC plan. This portion of the POC progressively determines how a DUT responds to malformed traffic, including frame impairments at Layer 2, session fuzzing at Layers 3 and 4, and application fuzzing at Layer 7.

Evasions

At a minimum, this part of the POC should include TCP segmentation and IP fragmentation evasions. Depending on the IT organization's network conditions, custom lists of evasions

can be included as well. Adding these stress vectors to load and attacks completes the picture. Performing a POC in this way ensures that the device being considered can cope with the entire set of challenges it will face when deployed in the real world.

Step 6: Lay the Groundwork for Successful Negotiation, Deployment, and Maintenance

Deploying untested network and security devices creates serious problems for IT professionals, network and data center infrastructures, and organizations as a whole. Untested equipment requires weeks of post-deployment troubleshooting that is frustrating and time-consuming for staff members and that often leads to both finger-pointing and costly remediation steps. This is particularly true when device outages, security breaches, or unplanned bottlenecks impact the resiliency of entire infrastructures; such failures damage reputation and business value while leading to serious, even career-limiting, embarrassment for individuals. By contrast, conducting a rigorous POC minimizes the risk of all these problems and saves hundreds of hours of staff time by eliminating surprises and guesswork.

"Do not limit these testing procedures to the purchasing cycle alone; make them an integral part of the ongoing security maintenance regime by implementing a solid, continuous testing initiative."

Gartner Report: Guidelines for CISOs

POCs can also lower equipment prices. Before a purchase is completed, IT organizations should use the information generated during the POC to negotiate a discount with the chosen vendor. That information demonstrates the actual capabilities of the device under the company's own network conditions—not in the vendor's lab. The IT organization can use that data to argue for what the device should cost based on demonstrated performance rather than marketing claims. For example, a company might select a firewall that meets the specifications established in Step 1 of the POC process but that blocks attacks at only 70 percent of its advertised top speed. In that instance, it would be much easier for the IT organization to make the case that the vendor should offer a 30 percent discount on the price of the firewall.

Once a device is purchased, the tests archived during Step 5 should all be run again to enable proper configuration and ensure that the device is production-ready. The detailed information created by these tests gives IT organizations the advance insight needed to configure equipment to remediate weaknesses and achieve the optimal balance between performance and security.

Using real-world traffic to tune the device also promotes rightsizing, because it allows engineers to build in enough of a performance cushion to handle peak traffic, but without creating waste by overbuilding that cushion. The exact data collected from pre-deployment tests also makes it easier to work with vendors to remediate problems.

IT engineers can share definitive test results, forestalling arguments and allowing vendors to correct problems more quickly. All of these benefits enable staff members to deploy equipment smoothly, without wasting time and money on remediating problems after the fact.

The benefits of pre-deployment testing extend to entire infrastructures as well. Advance simulation with real-world conditions gives IT staff visibility into how device deployment will impact other infrastructure elements and how those elements will affect the device. These insights allow companies to install a new device with confidence that it will not disrupt the production environment, but without requiring the trouble and expense of deploying the device first in a test lab or disaster recovery backup environment. Beyond that, pre-deployment testing enables predictive modeling across a range of use-case scenarios, allowing the IT professional to understand how devices and infrastructures

Deploying untested network and security devices creates serious problems for IT professionals, network and data center infrastructures, and organizations as a whole.

will perform under different configurations and network conditions. It also enables IT organizations to hold vendors accountable for supporting and improving their products over time.

Ultimately, the benefits of pre-deployment testing extend to the entire company. POCs help IT organizations control costs and reduce risks while optimizing the performance, security, and stability of each device. Proper pre-deployment testing enables a company to meet the key objectives outlined in Step 1 to deliver higher value and meet business objectives. This approach mitigates the risks of outages and vulnerabilities, promotes rightsizing, and drastically reduces the time, money, and frustration required to deploy new devices.

Purchasers of network and security devices should follow the scientific, quantitative progression of testing described here to fulfill the unique needs of their network and data center infrastructures.

Summary

Purchasers of network and security devices should follow the scientific, quantitative progression of testing described here to fulfill the unique needs of their network and data center infrastructures. Without following this approach, they will be unable to accurately assess the DPI capabilities of today's content-aware devices operating in 10GE and beyond environments. It is particularly important that they clearly define necessary device specifications, use standard testing methodologies, and validate devices against network conditions that mirror reality. CISOs and other IT leaders can follow the technical recommendations laid out in this paper, or they can outsource the work to testing experts using on-demand professional services.

About Ixia PerfectStorm ONE POC-in-a-Box

PerfectStorm ONE network test and assessment solutions are developed specifically for enterprise IT managers, operations, and security personnel. Delivered in a compact form-factor, PerfectStorm ONE condenses Ixia's PerfectStorm massive-scale, stateful layer 4-7 testing platform to now support the enterprise.

PerfectStorm ONE 10GE 8-port SFP+ Options:

- 4-port 1GE SFP+ appliance
- 8-port 1GE SFP+ appliance
- 2-port 1GE/10GE SFP+ appliance
- 4-port 1GE/10GE SFP+ appliance
- 8-port 1GE/10GE SFP+ appliance

Software License Upgradable

PerfectStorm ONE 40GE 2-port QSFP+ Options:

- 2-port 40GE QSFP+ appliance with support for 8-port 10GE SFP+ via fan-out mode

The PerfectStorm ONE testing platform scales from 4Gbps to 80Gbps of application traffic in a small single, integrated system and supports a buy-only-what-you-need business model to align with enterprise budgets and future-proof your growing test needs.

It generates stateful application and malicious traffic that simulates thousands and even millions of real-world end-user environments to test and validate infrastructure, a single device, or an entire system. This includes complex data, video, voice, storage, and network application workloads.

It includes all the elements required to create real-world traffic and produce extensive reporting to conduct a thorough data-driven POC.

About Ixia Professional Services

Ixia provides the turnkey services that IT organizations need to gain advance insight into how devices, networks, and data centers will perform under their unique traffic mixes. Ixia professional services provide actionable results in only days by leveraging the company's patented products, dedicated security research team, and best practices from its Global 2000 customer-base. Unlike other offerings, these services enable IT professionals to create the real-world simulations required to quickly and cost-effectively harden IT resiliency, minimize IT risk, and even train their own cyber warriors.

Ixia Device Evaluation Service

The Ixia Device Evaluation Service provides a complete comparative evaluation or POC of content-aware network, security, and data center devices using a company's own network conditions. The service includes the setup and execution of high-performance stateful application and attack simulations that mirror real-world traffic for each device. In less than a week, the company will receive detailed analysis of the performance, stability, and security of devices such as application servers, load balancers, firewalls, IDS/IPS devices, virus and spam filters, and more. An Ixia Device Evaluation can be conducted as a one-time project, providing the advance insight needed to confidently benchmark, select, and negotiate the purchase of IT devices; or a yearly subscription service that includes ongoing device evaluations to ensure that equipment remains resilient over time.

www.ixiacom.com

The Ixia Device Evaluation Service provides a complete comparative evaluation or POC of content-aware network, security, and data center devices using a company's own network conditions.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
21 Serangoon North Avenue 5
#04-01
Singapore 554864

Sales +65.6332.0125
Fax +65.6332.0127