DATA SHEET

FireStorm 20: High Port Density Load Module for BreakingPoint Application and Security Testing

Ixia's FireStorm 20 sets the standard for price/performance as the only solution for real-world testing that supports numerous concurrent users in any large-scale development facility

Deep packet inspection (DPI) technology is not simply a feature of network security devices. Today's routers and switches, the foundation of our critical IT infrastructure are also becoming application-aware in order to provide even greater performance and functionality. Understanding how these devices recognize and handle blended application traffic is critical during development, and traditional bit-blasting test tools create a false sense of security and performance. The FireStorm 20 load module powers Ixia's BreakingPoint, providing a cost-effective solution for battle-testing these high-density products using the actual network traffic and user behavior seen in deployment.

FireStorm 20: Battle-test high-density network equipment

Exclusive Ixia Security Test Capabilities

- Enterprises, government agencies and contractors, service providers, and network equipment manufacturers rely on Ixia security test products to:
- Harden network infrastructures by assaulting them with a custom, global, and current blend of stateful applications, live security attacks, and high-stress load to probe every weakness and vulnerability
- Optimize data center resiliency by simulating the behavior of millions of users, a crush of real-world applications, and security attacks — all without deploying racks of high-speed servers and costly software
- Evaluate and select the most appropriate network equipment for critical infrastructure with standardized, repeatable, and deterministic product assessments
- Measure and harden the resiliency of routers, switches, firewalls, IPS, UTM, and other devices by subjecting them to real-world conditions prior to deployment and after patches or configuration changes

Providing twenty 10GE ports and 60 ports per 4U chassis, the Ixia's FireStorm 20 combines the high performance, realism and large port densities needed by the large-scale development and testing labs of equipment manufacturers and carriers. The FireStorm 20 is the perfect solution for any organization challenged by introducing sophisticated, real-world application and security testing to support numerous concurrent users, tests or port pairs.

The FireStorm 20 from is capable of creating massive-scale online behavior from more than 200 applications and 35K+ live security attacks — including malware, mobile malware and DDoS. Providing twenty 10GE ports and up to 60 ports per 4U chassis, the FireStorm 20 combines the high performance, realism and large port densities needed by the large-scale development and testing labs of equipment manufacturers and carriers. The FireStorm 20 is the perfect solution for any organization challenged by introducing sophisticated, real-world application and security testing to support numerous concurrent users, automated tests or network simulations.

The new FireStorm 20 allows organizations to:

- Reduce time-to-test to minimize costs and accelerate development of next-generation network, security and data center devices.
- Cost-effectively perform concurrent complex, real-world simulations in order to evaluate, test and optimize application-aware devices.
- Train and certify IT personnel to predict and prevent cyber attacks in larger environments than previously possible.

Stay Current with Comprehensive Applications, Attacks, Service, and Support

Ixia also provides the BreakingPoint Application and Threat Intelligence (ATI)™ Program, an all-in-one update service backed by a team of security experts, to complement the FireStorm. The most popular and dynamic Web and network application protocols are maintained even more frequently through the Ixia's BreakingPoint Evergreen Applications program. Together, these bi-weekly programs keep Ixia products updated with the latest security attacks and applications, as well as new features and performance upgrades.

Exclusive BreakingPoint Capabilities

Enterprises, government agencies and contractors, service providers, and network equipment manufacturers rely on Ixia products to:

- Harden network infrastructures by assaulting them with a custom, global, and current blend of stateful applications, live security attacks, and high-stress load to probe every weakness and vulnerability
- Optimize data center resiliency by simulating the behavior of millions of users, a crush of real-world applications, and security attacks — all without deploying racks of high-speed servers and costly software
- Evaluate and select the most appropriate network equipment for critical infrastructure with standardized, repeatable, and deterministic product assessments
- Measure and harden the resiliency of routers, switches, firewalls, IPS, UTM, and other devices by subjecting them to real-world conditions prior to deployment and after patches or configuration changes
- Validate lawful intercept and data loss prevention systems with multilingual "needle-in-a-haystack" simulation
- Identify and remediate problem areas that require tuning and configuration changes
- Audit and maintain standards compliance throughout the life cycle of network devices
- Conduct research and train security experts with Ixia's advanced cyber range technology
- Analyze the impact of complex application traffic on network devices and systems to conduct research and train security experts

FireStorm 20 Features

- Assault networks, data centers, and devices with exact Internet conditions to harden and optimize resiliency
- The FireStorm 20 produces blended applications and the most current security attacks at global-scale performance levels while emulating many millions of users.
- Simulates 90 million simultaneous users and blended application traffic at live network speeds of up to 120 Gigabits per second from a single three-slot chassis
- Performs SSL bulk encryption at 25 Gbps with any cipher
- Ships with more than 250+ application protocols out of the box, including popular applications such as AOL® IM, BlackBerry® Services, eDonkey, Encrypted BitTorrent™, FIX, Google® Gmail, Gnutella, HTTP, IBM® DB2, MAPI, Microsoft® CIFS/SMB, MSN® Nexus, Oracle®, RADIUS, SIP, Skype™, VMware® VMotion™, Windows Live Messenger, World of Warcraft®, Yahoo!® Mail, Yahoo! Messenger, and many others
- Uses BreakingPoint's intuitive Web UI or extensive automation capabilities, with up to 10 users or concurrent tests per blade
- Will support industry testing standards such as Resiliency and RFC2544
- Provides 35K+ live security attacks out of the box, including malware, with new attacks made available bi-weekly
- Enables sophisticated attack simulation with more than 100 evasions, live malware, botnets, distributed denial of service (DDoS) attacks, and more
- Provides an optional Custom Application Toolkit and Custom Strike Toolkit to create and accelerate custom applications and security attacks
- Universal 10GigE / 1GigE SPF+ ports
- Interchangeable with existing Ixia Storm and FireStorm blades and usable in all BreakingPoint chassis
- Support up to 10 concurrent tests/users per blade (and up to 30 per chassis)
- Support multiple complex lab scenarios without re-wiring
- Incredibly high port density – up to 60 10Gb SFP+ ports in a 4U chassis
- Low power requirements – 120Gb traffic and 60 ports on 110v operation
- Integrated system controller

Reduce Total Cost of Ownership

- The FireStorm 20 is designed to adapt rapidly to change and ensure ongoing resiliency with the latest applications, security attacks, product features, and performance upgrades.
- All-inclusive pricing includes access to all applications and security attacks required for real-world simulations
- Backed by a dedicated group of security researchers and application protocol engineers committed to keeping the product completely current with frequent strike and protocol updates
- Easy to use by staff at all skill levels
- Automated point-and-click capabilities and a library of prebuilt profiles reduce configuration time
- Complete TCL test automation interface supports efficient, scalable lab automation
- Reduces the cost of LTE user simulation by more than 99% when compared to existing solutions
- Scales easily to replace costly server farms or cyber range operations with a small, easy-to-maintain product

Ixia FireStorm 20 Blade Specifications	
Selected Performance Information	• 40Gbps stateful application traffic • 30 million concurrent flows • 85,000 SSL transactions per second
FireStorm 20 Physical Specifications	• Rack Units: 4 • Installed: 17.4 in W x 7 in H x 19.5 in D (44.2 cm W x 17.8 cm H x 49.8 cm D) • Shipping Weight: 45 lb (20.4 kg) • Operating Environment: 15° C to 40° C • Nonoperating Environment: -20° C to 70° C • Power Requirements: 100 – 240V, 50/60 Hz • Maximum Power Consumption: 1200W • Regulatory Approvals: FCC Class A, CE, EN60950

System Configuration and Expansion Options	• 4U chassis
	• Up to 3 interface blades per chassis:
	  ○ 1GE Interface blade
	  ○ 4 ports
	  ○ SFP interfaces
	  ○ 1GB of capture buffer per port
	• Expansion options:
	  ○ 1GE Interface blade (as above)
	  ▪ 4-port add-on kit to expand to 8 ports
	  ○ 1GE Interface blade
	  ▪ 8 ports
	  ▪ SFP interfaces
	  ▪ 1GB of capture buffer per port
	  ○ 10GE Interface blade
	  ▪ 4 ports
	  ▪ XFP interfaces
	  ▪ 2GB of capture buffer per port
	  ○ FireStorm blade
	  ▪ 4 ports
	  ▪ SFP+ interfaces
	  ▪ 4GB of capture buffer per port
	  ○ FireStorm 20 blade
	  ▪ 20 ports
	  ▪ SFP+ interfaces
	  ▪ 200MB of capture buffer per port