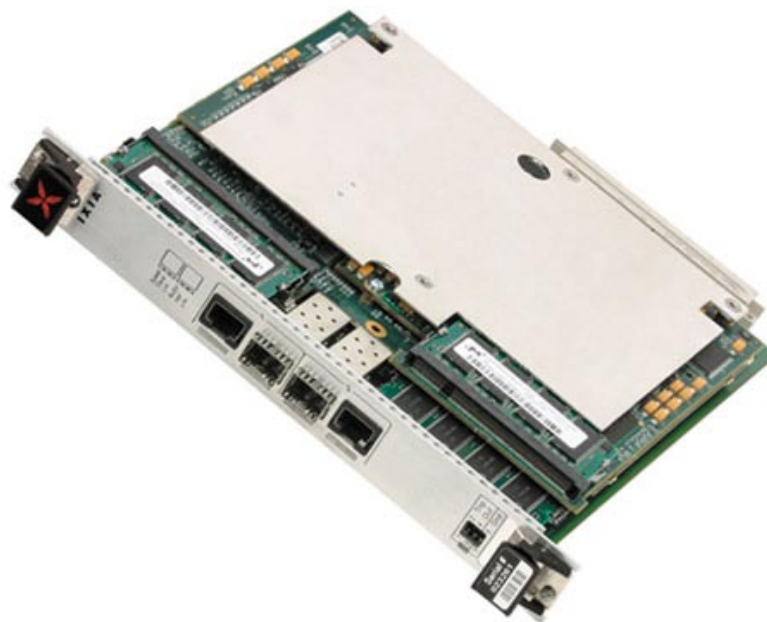


# Encryption Load Module



**Ixia's Encryption Load Module (ELM) enables high performance testing of IPSec VPN devices and networks.** With its custom hardware-based security processor operating in conjunction with Ixia's IxVPN test application, the ELM offers an extremely scalable solution for validating the performance of IPSec VPN gateways. The ELM emulates the functional requirements of today's VPN network with its extensive IPSec security features such as data encryption, device authentication and credential verification, data integrity, address hiding, and security-association (SA) key aging. The ELM offers two DualPHY (copper and fiber) 10/100/1000 Mbps Ethernet ports. With a RISC CPU per port running the Linux operating system plus a security co-processor per port for high performance encryption and decryption, the ELM delivers an unparalleled level of IPSec performance.

The ELM, in conjunction with IxVPN, implements a full IPSec and IKE protocol stack. It can emulate thousands of secure gateways and clients per test port, creating thousands of IPSec tunnels. Using multiple ports, a single Ixia test system can scale to test the largest IPSec VPN gateways and networks. Once the tunnels are set up, IxVPN measures the encryption and decryption performance of the IPSec gateway using standard RFC 2544 test methodology. This solution can also be combined with Ixia's IxChariot®, enabling application emulation using real-world Layer 4-7 traffic over secured networks.



## Specifications

<b>Number of ports, processors and security co-processors</b>	2 per Load Module
<b>Network Interfaces</b>	10/100/1000 Mbps Ethernet over copper or 1000Mbps Ethernet over fiber
<b>Network Connector Type</b>	RJ-45 or SFP
<b>Application Support</b>	IxVPN: VPN scalability and performance IxChariot®: Enterprise application emulation IxNetwork: IP control plane emulation IxLOAD: SSL performance and scalability testing
<b>IPSec Features</b>	AH, ESP or a combination Encryption algorithm: DES, 3DES, AES 128, AES 192, AES 256 Encapsulation mode: Tunnel mode and transport mode Hash/Authentication algorithm: MD5, SHA-1 DH group: Group 1, Group 2, Group 5, Group 14, Group 15, Group 16 Phase I authentication method: Certificates, Pre-shared keys Tunnel lifetime Perfect Forward Secrecy
<b>Statistics via IxVPN</b>	Tunnel capacity, tunnel setup latency, tunnel setup rate, tunnel attempts and failures Latency statistics per phase (IKE phase and IPSec phase) Re-key attempts, failures, and re-key rate Encryption and decryption latency, encryption and decryption throughput, packets/bytes encrypted and decrypted Real-time statistics, CSV, and HTML test logs Aggregate and per-tunnel statistics
<b>Addressing</b>	Each emulated gateway has a unique IP and a unique MAC address Multiple hosts behind each emulated gateway Multiple Phase 2 SAs per Phase 1 SA
<b>Diagnostics</b>	Diagnostic messages per-tunnel and per-phase
<b>Automation</b>	Tcl API for automation and custom test case development

## IxVPN Test Suites

### Tunnel Capacity

- Measures the rate at which tunnels are set up by the DUT
- Reports setup rate as a function of the number of tunnels established on the DUT

### Tunnel Setup Rate

- Measures re-key rate and failures
- Reports setup rate as a function of the number of tunnels established on the DUT

### Re-keying

- Measures re-key rate and failures
- Designed to test long-term stability of IPSec VPNs
- IxChariot® traffic over VPN tunnels
- Send a variety of application traffic over the IPSec tunnels to assess the impact on application performance
- Real-time graphs showing end-to-end throughput and latency IxChariot® traffic over VPN tunnels
- Measures encryption and decryption throughput, latency per RFC 2544
- Varying packet sizes
- Per-tunnel performance

### IxLOAD SSL Support

#### Features

- Supports SSLv2.0, SSLv3.0 and TLSv1.0
- SSL Session reuse
- Selectable ciphers for SSL handshake
- Configurable client and server side certificates for HTTPS connections
- Support for DH ephemeral key exchange

### Product Ordering Information

#### **ELM1000ST2**

Part Number: 944-0021

2-Port Dual-PHY (RJ-45 and SFP) 10/100/1000 Mbps Ethernet Encryption Load Module (does not include SFP transceivers); Requires OPTIPSEC configuration option

**IxVPN**

Application for testing IPSec devices

**IxLOAD**

Application for SSL performance and scalability testing

*This material is for informational purposes only and subject to change without notice. It describes Ixia's present plans to develop and make available to its customers certain products, features and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer.*