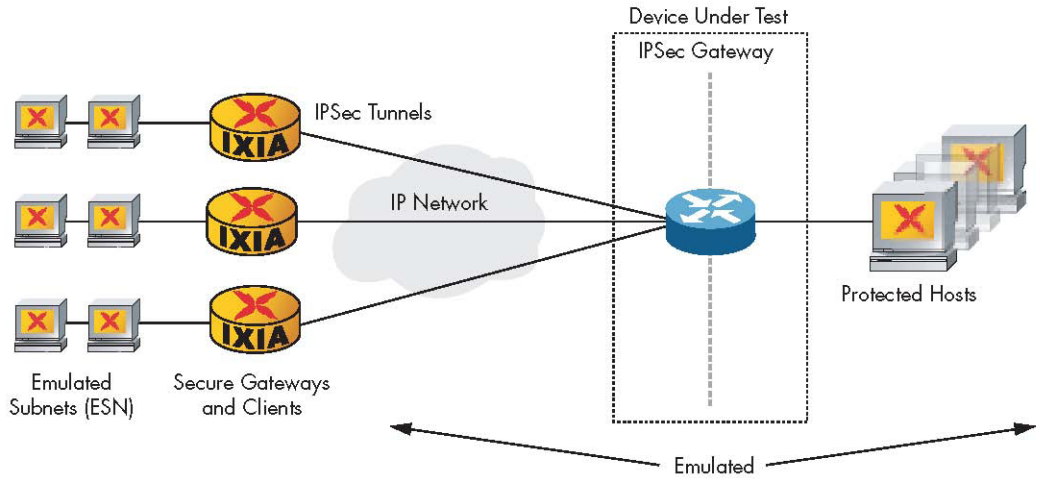
IxVPN

IxVPN provides Network Equipment Manufacturers, Service Providers, and organizations deploying IPSec VPNs an extremely scalable performance analysis solution for validating the performance of IPSec VPN gateways.

IxVPN utilizes Ixia's purpose-build Load Modules including the Encryption Load Module (ELM) with dedicated security processors. Each Load Module port implements a full IKE and IPSec protocol stack and can emulate thousands of Secure Gateways and clients, creating thousands of IPSec tunnels. Using multiple ports, a single Ixia test system can scale to test the largest IPSec VPN gateways and networks.

IxVPN measures the tunnel setup rate and capacity of IPSec gateways. After establishing tunnels, IxVPN measures the encryption and decryption performance of the IPSec gateway using the RFC 2544 methodology for benchmarking and soak tests for long term stability. IxChariot can be used to emulate a wide range of enterprise application traffic over IPSec tunnels.



Specifications

Load Modules Supported	• 10/100/1000 Encryption Load Module (ELM1000ST2) • 10/100/1000 Application Load Module (ALM1000T8) • 10/100/1000 Mbps Copper Ethernet (LM1000TXS4, LM1000TXS4-256) • 1000 Mbps Fiber Gigabit Ethernet (LM1000SFPS4, LM1000SFPS4-256) • 10/100/1000 Mbps Copper and Fiber Gigabit Ethernet (LM1000STSX4, LM1000STXS4-256, and LM1000STXS2)

IPSec Parameters	• IKE versions 1 and 2 • IPv4, IPv6, and combinations • Dynamic Multipoint VPNs (DMVPN) • GRE over IPSec • VLAN support • Phase 1 / AUTH_SA - Main and aggressive mode - Hash algorithms: HMAC-MD5, HMAC-SHA1 - Encryption algorithms: DES, 3DES, AES-128, AES-192, AES-256 - Xauth user authentication - Modecfg address assignment - Extended Authentication Protocol - User authentication - pre-shared keys and certificates - NAT Traversal (NAT-T) - Lifetime negotiation and re-keying - Manual keying • Phase 2 / CHILD_SA - AH, ESP, AH+ESP - Tunnel and transport mode - Hash algorithms: HMAC-MD5, HMAC-SHA1 - Encryption algorithms: NULL, DES, 3DES, AES-128, AES-192, AES-256 - Perfect Forward Secrecy (PFS) - IP Compression - Lifetime negotiation and re-keying - IPSec keep-alives and Dead Peer Detection (DPD)
Tests	Control Plane • Maximum number of tunnels • Tunnel setup rate • Long term stability Data Plane • RFC 2544 tests for benchmarking encryption and decryption • Soak test for long-term stability, with simultaneous bidirectional traffic • Multiple frame size and IMIX frame size combinations
Statistics	Control Plane • Tunnel capacity, tunnel setup latency, tunnel setup rate, tunnel attempts and failures • Setup time statistics per phase (IKE phase and IPSec phase) • Re-key attempts, failures, and re-key rat Data Plane • Encryption and decryption latency • Encryption and decryption throughput • Performance per frame size Real-time statistics, CSV, and html test logs • Aggregate and per-tunnel statistics
Addressing	• 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
Diagnostics	• Diagnostic messages per-tunnel and per-phase
	• Tcl API for automation and custom test case development • IXVPN will generate a Tcl program for the current GUI configuration

Ease-of-Use

IxVPN makes it very easy to configure a large number of tunnels with varying IPSec parameters. Users can assign a percentage distribution to each of the options, and the application will automatically create the mix of IPSec tunnels. Users can quickly create very complex test scenarios in a few simple steps using an intuitive GUI interface.

Test Suites

Tunnel Capacity

- Measures the maximum number of concurrent tunnels that can be sustained by the Device Under Test (DUT)

Tunnel Setup Rate

- 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

Re-keying

- Measures re-key rate and failures
- Designed to test long-term stability of IPSec VPNs

Soak Test

- Measures long term stability and performance
- Varying packet sizes and IMIX

RFC 2544 test over IPSec tunnels

- Measures encryption and decryption throughput, latency per RFC 2544
- Varying packet sizes and IMIX

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 per tunnel

Statistics and Diagnostics

IxVPN ports all the statistics in real time in a graphical format. Logs are also available. In addition to aggregate statistics across all the tunnels, per-tunnel statistics are available in real time. Statistics are provided on a per-phase basis helping to isolate performance problems.

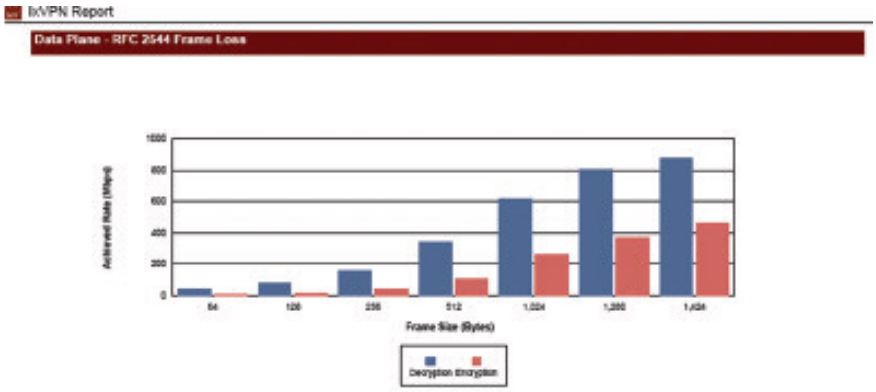
To assist in troubleshooting tunnel setup issues, extensive diagnostic information, on a per-tunnel basis, is provided.

Digital Certificates

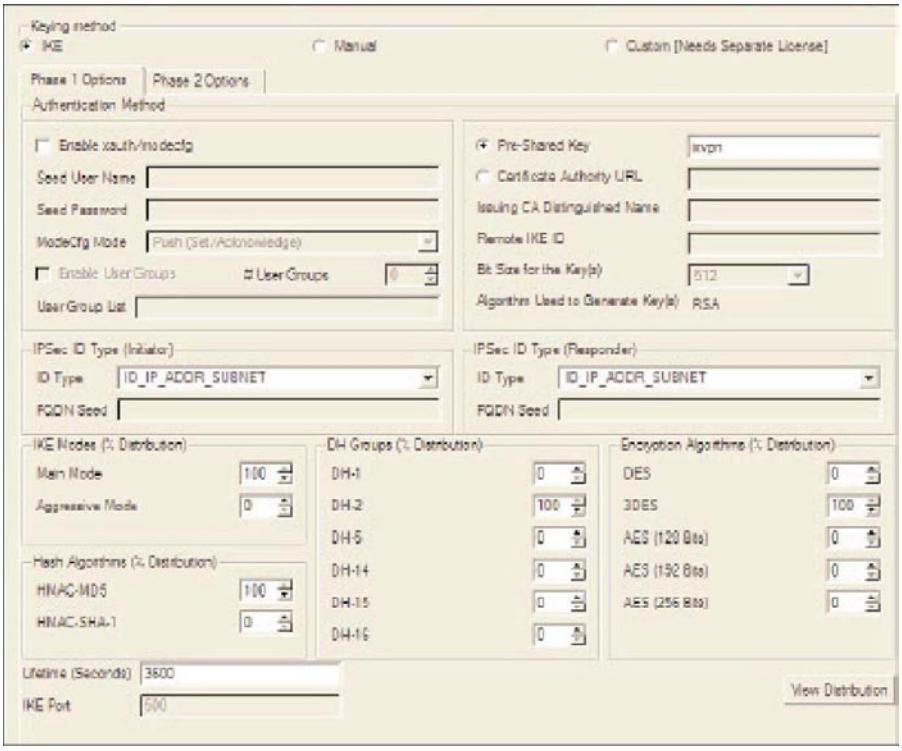
In addition to pre-shared keys, IxVPN also supports any standards compliant Certificate Authority (CA). IxVPN can be configured to get a certificate from a third party CA. This makes large-scale configurations much easier to set up and creates a real-world test scenario.

Automation

In addition to pre-shared keys, IxVPN also supports any standards compliant Certificate Authority (CA). IxVPN can be configured to get a certificate from a third party CA using SCEP. This makes large scale configurations much easier to set up and creates a real-world test scenario.



Direction	Requested Rate (Mbps)	Achieved Rate (Mbps)	Frame Size (Bytes)	# Frames Sent	# Frames Received	% Frame Loss
Encryption	1,000	4	64	76,169	76,169	0.0000
Decryption	1,000	45	64	874,903	211,684	75.8050
Encryption	1,000	16	128	143,578	126,301	12.0330
Decryption	1,000	83	128	809,910	187,682	76.2710



Product Ordering Information

IxVPN

IPSec Device Test Application