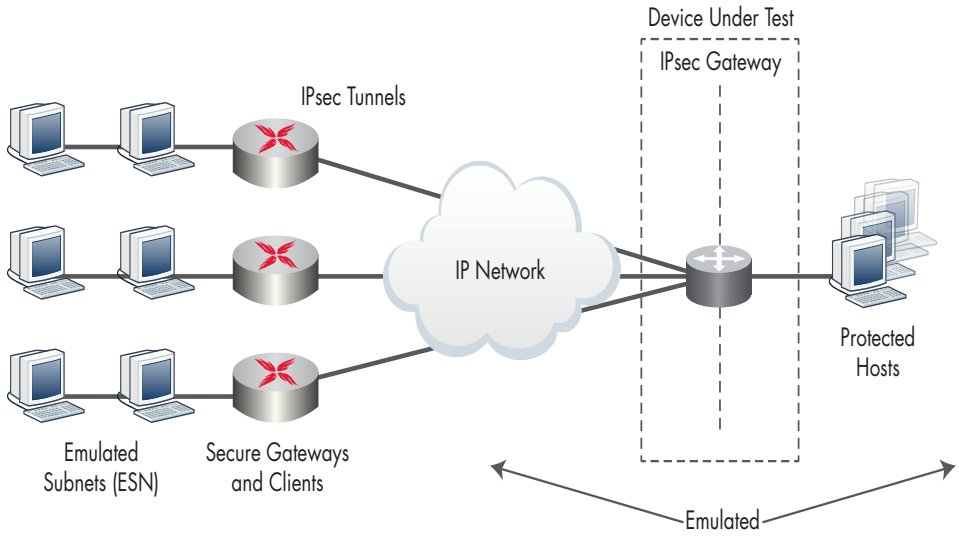
IxLoad-IPsec Enterprise Data Center / Cloud Assessment

IPsec (IP Security) is a framework of open standards for ensuring secure private communication over IP networks. IPsec virtual private networks (VPNs) use the services defined within IPsec to ensure confidentiality, integrity, and authenticity of data communications across networks such as the Internet.

IxLoad's IPsec plug-in provides network equipment manufacturers, service providers, and organizations deploying IPsec VPNs an extremely scalable solution for validating the performance and capacity of IPsec VPN gateways. IxLoad uses real application traffic over encrypted tunnels.



IxLoad operates in conjunction with Ixia's specialized load modules that implement a full IKE and IPsec protocol stack, emulating thousands of secure gateways and clients, and creating thousands of IPsec tunnels for testing.

Key Features

- An Xcellon-Ultra XTS40 appliance, with 4 x 10GE ports of IPsec hardware acceleration generates up to 40 Gbps of encrypted traffic*
- An Xcellon-Ultra XTS16 appliance, with 16 x 1GE ports of IPsec hardware acceleration generates up to 16 Gbps encrypted traffic*
- An Xcellon-Ultra XTS16 or XTS40 appliance creates up to 4,000 IKEv1/IKEv2 tunnels/sec*
- An Xcellon-Ultra XTS16 or XTS40 appliance creates up to 1,000,000 concurrent tunnels*
- Generates real application traffic (voice, data, and video) over encrypted tunnels
- Measures control and data plane capacity and performance
- Emulates IPsec scenarios over IPv4 and IPv6
- Dynamic tunnel setup and teardown options
- Supports both IKE versions 1 and 2 with pre-shared keys, EAP, RSA, and ECDSA certificates
- Site-to-site and remote access scenarios
- Includes all popular encryption, hash, and authentication algorithms
- Comprehensive per-tunnel diagnostics and statistics

Product	Xcellon-Ultra XTS16	Xcellon-Ultra XTS40
Port	16 x 1GE	4 x 10GE
Traffic Performance	16 Gbps of encrypted traffic*	40 Gbps of encrypted traffic*
ITunnel Setup Rate	Up to 4,000 IKEv2 tunnels/sec*	
Concurrent Tunnels	Up to 1 million tunnels*	

* Performance measured using a pair of Xcellon-Ultra XTS appliances

Feature	Options
Keying Methods	• IKE version 1 • IKE version 2 • Manual keying using IPv4 and IPv6
IPsec Features	• Initiator and responder modes • IPv4, IPv6, IPv4/IPv6, and IPv6/IPv4 • VLAN support • NAT-T • IPsec pre-fragmentation • Initial contact payload
Tunnel Control	• Tunnel setup and tear down • Persistent and non-persistent tunnels • Dynamic tunnel creation and tear down • Dead peer detection (DPD) • Rekeying support • IKE message retry timers
Authentication Methods	• Pre-shared key • RSA and ECDSA Certificates • EAP (MD5, SIM, TLS, AKA)
IPsec parameters IKE Phase 2/ CHILD_SA	• AH, ESP, AH+ESP • Tunnel mode • Transport mode • Hash algorithms: • HMAC-MD5-96 • HMAC-SHA1-96 • HMAC-SHA256-128 • HMAC-SHA384-192 • HMAC-SHA512-256 • Encryption algorithms: • NULL • DES, 3DES • AES-128-CBC, 192, 256 • Perfect Forward Secrecy (PFS) • Lifetime negotiation and re-keying • Multiple Phase2 SAs over a single Phase1 SA • Multiple ChildSAs over a single IKE SA

Feature	Options
Addressing	• Each emulated gateway may have a unique IP • Multiple hosts behind each emulated gateway • Unique MAC per emulated gateway • Unique VLAN per emulated gateway
RFCs	• RFC2394, IP Compression (DEFLATE algorithm) • RFC 2401, Security Architecture for the Internet Protocol • RFC 2402, IP Authentication Header • RFC 2406, IP Encapsulating Security Payload (ESP) • RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP • RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP) • RFC 2409, The Internet Key Exchange (IKE) • RFC3566, The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec • RFC 3715, IPsec-Network Address Translation (NAT) Compatibility Requirements • RFC 3748, Extensible Authentication Protocol (EAP) • RFC 3947, Negotiation of NAT-Traversal in the IKE • RFC 3948, UDP Encapsulation of IPsec ESP Packets • RFC 4306, Internet Key Exchange (IKEv2) Protocol • RFC 4718, IKEv2 Clarifications and Implementation Guidelines

For more information see http://www.ixiacom.com/solutions/testing_security/index.php

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