DATA SHEET

IxLoad-IPsec Testing

IPsec Protocol Emulation

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 hundreds of thousands of secure gateways and/or IPsec clients.

Key Features

- Industry's highest performance and capacity with the PerfectStorm hardware family
- Supports all popular encryption, hash, and authentication algorithms
- Includes a complete set of IPsec benchmarking test methodologies (IPsec QuickTests)
- Measures control plane and data plane performance and capacity
- Generates real application traffic over encrypted tunnels
- Emulates IPsec scenarios over IPv4 and IPv6
- Dynamic tunnel setup and teardown options
- Supports IKEv1, IKEv2, and manual keying
- Integrated IPsec configuration wizards
- Site-to-site and remote access scenarios
- Comprehensive per-tunnel diagnostics and statistics

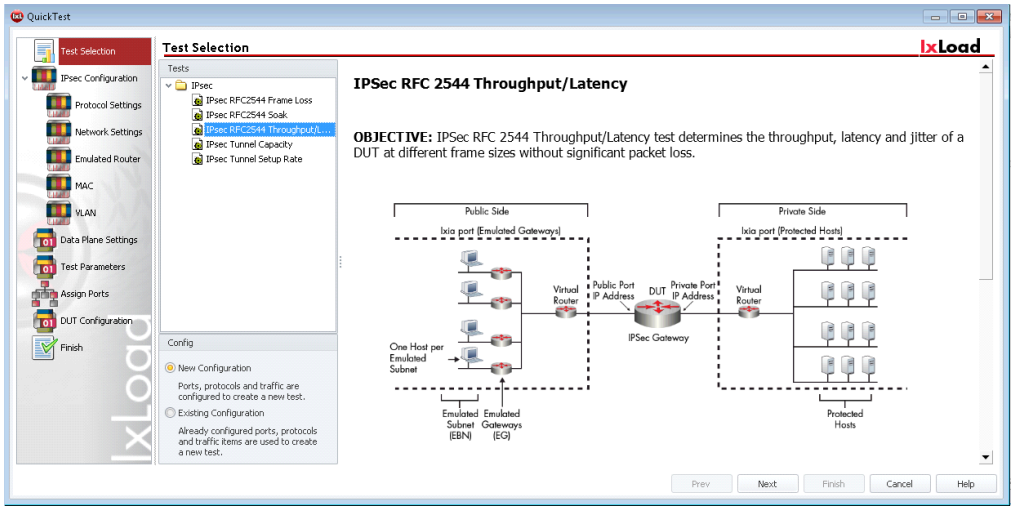
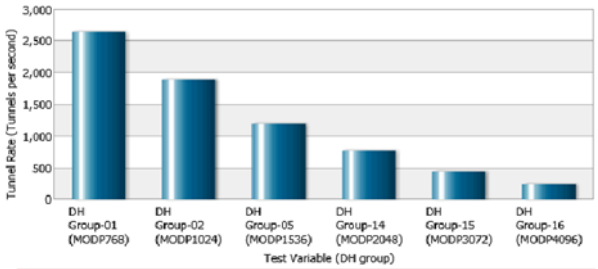


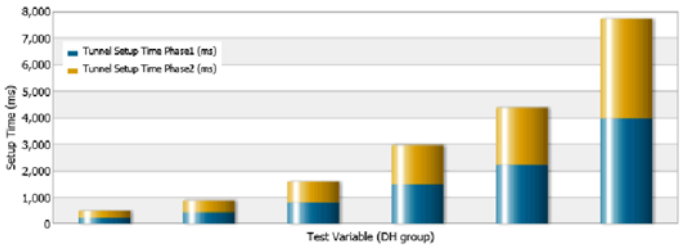
Figure 1: IPsec QuickTests

Key Features

- Industry's highest performance and capacity with the PerfectStorm hardware family
- Supports all popular encryption, hash, and authentication algorithms
- Includes a complete set of IPsec benchmarking test methodologies (IPsec QuickTests)

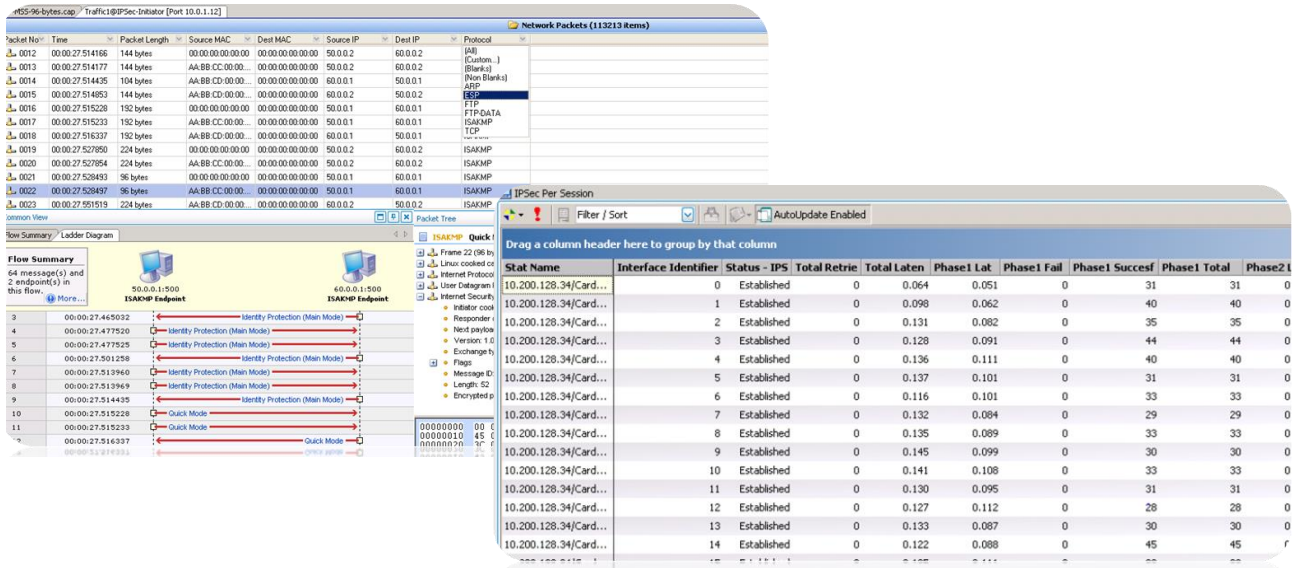


DH	Median Tunnel Rate
DH Group-01 (MODP768)	2,640
DH Group-02 (MODP1024)	1,889
DH Group-05 (MODP1536)	1,187
DH Group-14 (MODP2048)	768
DH Group-15 (MODP3072)	438
DH Group-16 (MODP4096)	243



DH	Phase1: Tunnel Setup Time (ms)	Phase2: Tunnel Setup Time (ms)
DH Group-01 (MODP768)	238	251
DH Group-02 (MODP1024)	433	441
DH Group-05 (MODP1536)	803	772
DH Group-14 (MODP2048)	1,486	1,470
DH Group-15 (MODP3072)	2,225	2,134
DH Group-16 (MODP4096)	3,975	3,743

- Measures control plane and data plane performance and capacity
- Generates real application traffic over encrypted tunnels
- Emulates IPsec scenarios over IPv4 and IPv6
- Dynamic tunnel setup and teardown options
- Supports IKEv1, IKEv2, and manual keying
- Integrated IPsec configuration wizards
- Site-to-site and remote access scenarios
- Comprehensive per-tunnel diagnostics and statistics



Specifications[i]

Keying methods	• IKEv1 • IKEv2 • Manual keying

IPsec parameters
IKE phase1/AUTH_SA
	• Main and aggressive mode
	• Hash algorithms:
	  ○ HMAC-MD5
	  ○ HMAC-SHA1
	  ○ AES-XCBC-MAC-96 (RFC3566)
	  ○ HMAC-SHA256
	  ○ HMAC-SHA384
	  ○ HMAC-SHA512
	• Encryption algorithms:
	  ○ DES
	  ○ 3DES
	  ○ AES-128-CBC
	  ○ AES-192-CBC
	  ○ AES-256-CBC
	  ○ AES-128-GCM ICV 8/12/16
	  ○ AES-192-GCM ICV 8/12/16
	  ○ AES-256-GCM ICV 8/12/16
	• Multiple Proposals
	• Xauth user authentication
	• ModeCFG address assignment
	• IKEv2 Suggested IP address
	• Pseudo-random functions
	  ○ HMAC-MD5
	  ○ HMAC-SHA1
	  ○ AES-XCBC
	  ○ HMAC-SHA256
	  ○ HMAC-SHA384
	  ○ HMAC-SHA512

IPsec parameters
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 and 3DES
	  ○ AES-128-CBC
	  ○ AES-192-CBC
	  ○ AES-256-CBC
	  ○ AES-128-GCM ICV 8/12/16
	  ○ AES-192-GCM ICV 8/12/16
	  ○ AES-256-GCM ICV 8/12/16
	  ○ AES-128-GMAC
	  ○ AES-192-GMAC
	  ○ AES-256-GMAC
	• Multiple Proposals
	• Perfect Forward Secrecy (PFS)
	• Lifetime negotiation and re-keying
	• IKEv1: Multiple Phase2 SAs over a single Phase1 SA
	• IKEv2: Multiple ChildSAs over a single IKE SA

Authentication
Method
	• Pre-shared key
	• RSA and ECDSA Certificates
	  ○ keys of 512, 1024, 2048, 4096, and 8192 bits for RSA
	  ○ prime256v1, secp384r1, secp521r1 for ECDSA
	• Chained Certificates
	• EAP (MD5, SIM, TLS, AKA)
	• EAP vs. PreSharedKeys
	• EAP vs. Certificates

Certificate Management	• SCEP (Simple Certificate Enrollment Protocol) • CMPv2 (Certificate Management Protocol) • CRL (Certificate Revocation List) • OSCP (Online Status Certificate Protocol)

DH Groups	• DH-01 (MODP-768) • DH-02 (MODP-1024) • DH-05 (MODP-1536) • DH-14 (MODP-2048) • DH-15 (MODP-3072) • DH-16 (MODP-4096) • DH-17 (MODP-6144) • DH-18 (MODP-8192) • DH-19 (ECP-256) • DH-20 (ECP-384) • DH-21 (ECP-512) • DH-22 (MODP-1024-S160) • DH-23 (MODP-2048-S224) • DH-24 (MODP-2048-S256) • DH-25 (ECP-192) • DH-26 (ECP-224)
IPsec features	• Site to Site and Remote Access test scenarios • IPsec initiator and responder modes • VLAN support • NAT-T • IPsec pre-fragmentation • IPsec post-fragmentation • Initial contact payload • IKEv2 redirect • Multiple Traffic Selectors (IKEv2)
Tunnel control	• Tunnel setup and tear down • Persistent and non-persistent tunnels • IPsec tunnel flapping (dynamic sessions) • Dead peer detection (DPD) • Rekeying support • IKE message retry timers • NAT Traversal (NAT-T) • Lifetime negotiation • Re-keying

Addressing	• IPv4/IPv4 • IPv6/IPv6 • IPv4/IPv6 • IPv6/IPv4 • Single or multiple hosts behind each emulated gateway • Unique MAC per emulated gateway • Unique VLAN per emulated gateway • Support for Virtual Router (Emulated Router)
IPsec Global Statistics (all ports and per test port)	• Sessions Initiated • Sessions Succeeded • Sessions Failed • Sessions Active • Initiated Tunnel Rate • Setup Tunnel Rate • Failed Tunnel Rate • Total Retries • Phase1 Failed Rekeys • Phase1 Successful Rekeys • Phase1 Total Rekeys • Phase1 Failed Rekeys Rate • Phase1 Successful Rekeys Rate • Phase1 Total Rekeys Rate • Phase2 Failed Rekeys • Phase2 Successful Rekeys • Phase2 Total Rekeys • Phase2 Failed Rekeys Rate • Phase2 Successful Rekeys Rate • Phase2 Total Rekeys Rate • Phase 1 Encryption Algorithms • Phase 2 Encryption Algorithms • Number of DPD Hellos sent • Number of DPD Hellos received • Number of DPD ACKs received • Number of ESP Replayed Packets • Tunnel Setup Time (Phase1) • Tunnel Setup Time (Phase2) • Tunnel Setup Time • Tunnel Teardown Time

	• Interfaces Up • Interfaces Down • Interfaces Failed • Interfaces Outstanding • Number of ESP Packets sent • Number of ESP Packets received • Number of ESP Bytes sent • Number of ESP Bytes received • ESP Decryption Errors • ESP Transmit Packet Rate • ESP Receive Packet Rate • ESP Transmit Bit Rate • EST Receive Bit Rate • Number of Redirect Notify Payload Packets sent • Number of Redirect Payload Packets received • Number of Redirect FROM Payload Packets sent • Number of Redirect Request Packets Rejected
IPsec per Tunnel Statistics	• Status • Total Retries • Total Latency • Phase 1 Latency • Phase 2 Latency • Phase 1 Failed Rekeys • Phase 1 Successful Rekeys • Phase 1 Total Rekeys • Phase 2 Failed Rekeys • Phase 2 Successful Rekeys • Phase 2 Total Rekeys • Number of DPD Hellos TX • Number of DPD Hellos RX • Number of DPD ACKs TX • Number of DPD ACKs RX • Number of ESP Replayed Packets • Encapsulation protocols • Encapsulation mode • Initiator IP Address • Responder IP Address • Initiator IP Subnet

	• Responder IP Subnet • IKE Mode Phase 1 • Encryption Algorithm Phase 1 • Encryption Algorithm Phase 2 • Hash Algorithm Phase 1 • Hash Algorithm Phase 2 • Number of ESP Packets sent • Number of ESP Packets received • Number of ESP Bytes sent • Number of ESP Bytes received • ESP Decryption Errors • ESP Transmit Packet Rate • ESP Receive Packet Rate • ESP Transmit Bit Rate • EST Receive Bit Rate • EAP Method • PFS Group Phase 2 • Phase 1 – Last Rekey Time (UTC) • Phase 2 – Last Rekey Time (UTC) • Number of Redirect Notify Payload Packets sent • Number of Redirect Payload Packets received • Number of Redirect FROM Payload Packets sent • Number of Redirect Request Packets Rejected
RFCs	• RFC 2394, 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

Recommended Hardware

Part Number	Description
PerfectStorm ONE Appliances Fusion*	
941-0028	PerfectStorm ONE 40GE Fusion 2-port APPLIANCE (PS40GE2NG), 40GE 2-port QSFP+. Requires BreakingPoint Application & Threat Intelligence (ATI) (909-0856), sold separately, at time of purchase.
941-0027	PerfectStorm ONE Fusion, 10 Gig 8-PORT SFP+ APPLIANCE (PS10GE8NG); Requires BreakingPoint Application & Threat Intelligence (ATI) (909-0856), sold separately, at time of purchase.
941-0031	PerfectStorm ONE Fusion, 10 Gig 4-PORT SFP+ APPLIANCE (PS10GE4NG); Requires BreakingPoint Application & Threat Intelligence (ATI) (909-0856), sold separately, at time of purchase.
941-0032	PerfectStorm ONE Fusion, 10 Gig 2-PORT SFP+ APPLIANCE (PS10GE2NG); Requires BreakingPoint Application & Threat Intelligence (ATI) (909-0856), sold separately, at time of purchase.
941-0033	PerfectStorm ONE Fusion, 1 Gig, 8-PORT SFP+ APPLIANCE (PS1GE8NG); Requires BreakingPoint Application & Threat Intelligence (ATI) (909-0856), sold separately, at time of purchase.
941-0034	PerfectStorm ONE Fusion, 1 Gig, 4-PORT SFP+ APPLIANCE (PS1GE4NG); Requires BreakingPoint Application & Threat Intelligence (ATI) (909-0856), sold separately, at time of purchase.
PerfectStorm ONE Appliances (Standard)*	
941-0036	PerfectStorm ONE 40GE 2-port standard APPLIANCE (PS40GE2), 40GE 2-port QSFP+.
941-0037	PerfectStorm ONE , 10 Gig 8-PORT SFP+ APPLIANCE (PS10GE8)
941-0038	PerfectStorm ONE , 10 Gig 4-PORT SFP+ APPLIANCE (PS10GE4)
941-0039	PerfectStorm ONE , 10 Gig 2-PORT SFP+ APPLIANCE (PS10GE2)
941-0044	PerfectStorm ONE , 1 Gig, 8-PORT SFP+ APPLIANCE (PS1GE8)
941-0045	PerfectStorm ONE , 1 Gig, 4-PORT SFP+ APPLIANCE (PS1GE4)

Part Number	Description
PerfectStorm Load Modules Chassis-Based Solution*	
940-0006	XGS12-HS 12-slot chassis bundle with High Performance Controller
940-0007	XGS12-HS 12-slot chassis bundle with Standard Performance Controller
944-1200	PerfectStorm 10GE Fusion 8-port (PS10GE8NG)
944-1201	PerfectStorm 40GE Fusion 2-port (PS40GE2NG)
941-1204	PerfectStorm 10GE 8-port (PS10GE8)
941-1205	PerfectStorm 40GE 2-port (PS40GE2)
Xcellon-Ultra XTS Appliances	
941-0019	Xcellon-Ultra XTS40-01, 2U Application Network Processor Server,4-10GE SFP+ test interfaces with IPsec hardware acceleration and 4-10GE SFP+ interfaces without IPsec hardware acceleration; REQUIRES 8 SFP+ transceivers 948-0013 10GBASE-SR, 948-0014 SFP+10GBASE-LR
941-0015	Xcellon-Ultra XTS08-01, 2U Application Network Processor Server, 8-1GE RJ45 test interfaces with IPsec hardware acceleration

* All PerfectStorm test interfaces provide IPsec hardware acceleration capabilities.

Hardware Performance

PerfectStorm ONE Performance

Metric	PerfectStorm ONE 40GE 2-port	PerfectStorm ONE 10/1GE 8-port	PerfectStorm ONE 1GE 8-port
IPsec Throughput	80 Gbps	80 Gbps	8 Gbps
IPsec Tunnel Rate	20,000	20,000	20,000
IPsec Tunnel Capacity	1 million	1 million	1 million
10/1 GE Test Ports	n/a	8 SFP+ 10/1GE	8 SFP+ 1GE
40 GE Test Ports	2 QSPF+	n/a	n/a

Performance measured using a **pair** of PerfectStorm ONE appliances (single appliance provides half of the performance). Same performance is valid for the corresponding PerfectStorm load modules

Xcellon-Ultra Performance

Metric	Xcellon-Ultra XTS40	Xcellon-Ultra XTS08	Xcellon-Ultra NP
IPsec Throughput	40 Gbps	8 Gbps	1 Gbps
IPsec Tunnel Rate	4,000	4,000	350
IPsec Tunnel Capacity	1 million	200,000	360,000
1 GE Test Ports	n/a	8	12
10 GE Test Ports	4 SFP+	n/a	XFP

Performance measured using a **pair** of XTS appliances or a pair of Xcellon-Ultra NP load modules.

Product Ordering Information

PerfectStorm ONE Appliances

Part Number	Description
925-6321	**IxLoad, PerfectStorm ONE Multiplay,** Software Bundle, Layer 4-7 Performance Test Application**; Data, Voice, Video, Access, VPN** and **Storage** bundle for PerfectStorm ONE appliances**;** includes: • 925-6111 IxLoad PerfectStorm ONE DATA • 925-6112 IxLoad PerfectStorm ONE VIDEO • 925-6113 IxLoad PerfectStorm ONE VOICE • 925-6114 IxLoad PerfectStorm ONE AUTH • 925-6115 IxLoad PerfectStorm ONE VPN/ACCESS • 925-6116 IxLoad PerfectStorm ONE STORAGE
925-6115	**IxLoad PerfectStorm ONE VPN/ACCESS,** Software Bundle, Layer 4-7 Performance Test Application Software bundle; includes: • 925-6101 IxLoad PerfectStorm ONE BASIC (HTTP, HTTPS, DNS, ADVNET-DHCP, Stateless Peer) • IPsec, IPsec SUITES B, IPsec Quick Tests, PPP, L2TP, L2TP/IPsec • IPv6 Transitioning: SLAAC, 6rd, DSLite • ADVNET: DHCP, DHCPv6 (client & server)

PerfectStorm Load Modules Chassis-Based Solution

Part Number	Description
925-3357	**IxLoad PerfectStorm TriplePlay-2012 Bundle**, Software Bundle, Layer 4-7 Performance Test Application; includes: Data • 925-3052 - HTTP (Basic, Advanced), SSL and FTP • 925-3656 - TCP • 925-3103 - MAIL • 925-3138 - TFTP • 925-3142 - App-Replay • 925-3153 - Stateless-Peer • 925-3056 - DNS Video • 925-3104 - STREAM • 925-3188 - IXLOAD-VIDEO-EMULATION • 925-3189 - IXLOAD-VIDEO-QOV • 925-3111 - Advanced Video Codec • 925-3156 - Flash Client • 925-3161 - Apple HLS Client • 925-3162 - MS Silverlight Client • 925-3179 - Adobe HDS Client • 925-3193 - TCP OTT QoVideo up to 10Gbps Voice • 925-3502 - Advanced SIP • 925-3510 - IXLOAD-VOICE-EMULATION • 925-3512 - IXLOAD-VOICE-QOV, QoVoice up to 10 Gbps • 925-3521 - Audio Codecs 925-3527 - IXLOAD-VOICE-VIDEO-EMULATION • 925-3528 - IXLOAD-VOICE-VIDEO-QOV Access Network • 925-3100 ADVNET (DHCP, IPsec, PPP and L2TP) • 925-3148 ADVNET-DHCPSERVER Analyzer • 932-0101 - Analyzer Server, Base Software, Chassis Component, Packet Capture, View and Analysis • 932-0102 - Analyzer, Client, Base Software, Media player tools, Node-Locked License • 932-0104 - Analyzer, Client, Advanced audio quality analysis tools, Node-Locked License

Part Number	Description
925-3345	**IxLoad-VPN-2012, Software Bundle**, Layer 4-7 Performance Test Application; it includes HTTP and FTP traffic, plus: • 925-3100 IXLOAD-ADVNET (DHCP, PPP, L2TP and IPsec) • 925-3410 IXLOAD, IPsec Quick Tests • 925-3153 IXLOAD, STATELESS PEER • 932-0101 Analyzer Server • 932-0102 Analyzer, Client, Base Software, Media player tools, Node-Locked License
925-3346	**IxLoad-ADVNET-ACCESS-2012, Software Bundle**, Layer 4-7 Performance Test Application; It includes: • 925-3100 IxLOAD-ADVNET, Advanced Networking Features (DHCP for IP address acquisition, PPP, L2TP and IPsec) • 925-3148 IXLOAD, ADVNET-DHCPSERVER • 925-3149 IXLOAD, ADVNET-8021X • 925-3150 IXLOAD, ADVNET-NAC • 925-3151 IXLOAD, ADVNET-WEBAUTH • 932-0101 Analyzer Server, Base Software, Chassis Component, Packet Capture, View and Analysis • 932-0102 Analyzer, Client, Base Software, Media player tools, Node-Locked License.

Xcellon-Ultra XTS Appliances

Part Number	Description
925-5355	**IxLoad CPD Multi Play-2012, Software Bundle**, Layer 4-7 Performance Test Application for the Appliance; Data-Video-Voice-Security package includes: Data: • 925-5003 IxLoad CPD HTTP-Basic, FTP • 925-5200 CPD U1, • 925-5201 CPD U1-Basic, • 925-5103 CPD MAIL, • 925-5138 CPD TFTP, • 925-5142 CPD Application-Replay, • 925-5165 CPD Database, Voice: • 925-5502 - CPD Advanced SIP, • 925-5504 - CPD H.323, • 925-5501 - CPD RTP Audio, • 925-5521 - CPD Audio Codecs, Video: • 925-5104 CPD STREAM, • 925-5192 CPD Video with video quality metrics for up to 10Gbps, • 925-5111 CPD Video-Advanced Video Codec, • 925-5156 CPD Flash Client, • 925-5161 CPD Apple HLS Client, • 925-5162 CPD Microsoft Silverlight Client, • 925-5179 CPD Adobe HDS Client, • 925-5193 CPD Video Quality Analysis for up to 10Gbps of TCP OTT Video, Security: • 925-5116 CPD ADVNET-IPsec, • 925-5148 CPD ADVNET-DHCPSERCER, Also includes support for ADVNET-DHCP, Impairment and Analyzer

Part Number	Description
925-5345	**IxLoad-CPD-VPN-2012, Software Bundle**, Layer 4-7 Performance Test Application for the Appliance; It includes: • 925-5115 IXLOAD-ADVNET-DHCP • 925-5116 IXLOAD-ADVNET-Ipsec, IPsec license • 925-5160 IXLOAD, CPD-IPSEC SUITE-B, Optional Software, Advanced IPsec Protocol Features • 925-5410 IXLOAD, CPD-IPSEC-QUICKTEST, Optional Software , Layer 4-7 Performance Test Application • 925-5153 IXLOAD, CPD Stateless-Peer, Opt. SW, Stateless UDP generation for the appliance • 925-5003 IXLOAD, CPD HTTP-Basic, FTP • 932-0101 Analyzer Server, Base Software, Chassis Component, Packet Capture, View and Analysis • 932-0102 Analyzer, Client, Base Software, Media player tools, Node-Locked License

Chassis-Based Solution (other than PerfectStorm cards)

Part Number	Description
925-3355	**IxLoad Multi Play-2012, Software Bundle**, Layer 4-7 Performance Test Application; Data-Video-Voice-Security package includes: Data: • 925-3052 HTTP, FTP • 925-3103 MAIL, • 925-3112 SSH, • 925-3113 RADIUS, • 925-3138 TFTP, • 925-3142 App-Replay, • 925-3153 Stateless-Peer, • 925-3053 DHCP, DNS, LDAP, Telnet, Video: • 925-3104 STREAM, • 925-3192 Video & QoVideo up to 10Gbps, • 925-3111 Advanced Video Codec, • 925-3156 Flash Client, • 925-3161 Apple HLS Client, • 925-3162 MS Silverlight Client, • 925-3179 Adobe HDS Client, • 925-3193 TCP OTT QoVideo up to 10Gbps, Voice: • 925-3106 - Bulk SIP & Mgcp, • 925-3502 - Advanced SIP, • 925-3504 - H.323, • 925-3511 - RTP Audio & QoVoice up to 10Gbps, • 925-3521 - Audio Codecs, • 925-3526 - Video Codec & QoVoice up to 10Gbps, • 925-3550 - VoLTE, Security: • 925-3100 ADVNET, • 925-3148 ADVNET-DHCPSERCER, • 925-3606 DDoSv2-Base, • 925-3601 SUBSCRIPTION-VULNERABILITIES, • 925-3603 VULNERABILITIES-MALWARE-T. Also includes support for ADVNET-DHCP, Impairment and Analyzer

Part Number	Description
925-3345	**IxLoad-VPN-2012, Software Bundle**, Layer 4-7 Performance Test Application; it includes HTTP and FTP traffic, plus: • 925-3100 IXLOAD-ADVNET (DHCP, PPP, L2TP and IPsec) • 925-3410 IXLOAD, IPsec Quick Tests • 925-3153 IXLOAD, STATELESS PEER • 932-0101 Analyzer Server • 932-0102 Analyzer, Client, Base Software, Media player tools, Node-Locked License
925-3346	**IxLoad-ADVNET-ACCESS-2012, Software Bundle**, Layer 4-7 Performance Test Application; It includes: • 925-3100 IxLOAD-ADVNET, Advanced Networking Features (DHCP for IP address acquisition, PPP, L2TP and IPsec) • 925-3148 IXLOAD, ADVNET-DHCPSERVER • 925-3149 IXLOAD, ADVNET-8021X • 925-3150 IXLOAD, ADVNET-NAC • 925-3151 IXLOAD, ADVNET-WEBAUTH • 932-0101 Analyzer Server, Base Software, Chassis Component, Packet Capture, View and Analysis • 932-0102 Analyzer, Client, Base Software, Media player tools, Node-Locked License.

[i] **AH and AH+ESP** is supported only on chassis-based load modules except PerfectStorm cards. Xcellon-Ultra XTS appliances and PerfectStorm hardware family supports only ESP.

IP Compression is not supported on the PerfectStorm hardware family.

Suite B cryptographic suite (e.g. ECDSA certificates; GCM and GMAC encryption algorithms; SHA256, SHA384 and SHA512 hashing functions; Elliptic Curve DH groups) is supported only on PerfectStorm hardware family and Xcellon-Ultra XTS appliances.