

We secure the world's largest networks.

Safe, Simple, Scalable XML Firewall – XWall on X

Today more than ever large organizations are looking to systematically and consistently protect against XML (eXtensible Markup Language) intrusions, control Web service requests and responses, and apply transactional-specific SOA (Service-Oriented Architecture) security policies.

Crossbeam and Forum Systems have joined forces to offer the most scalable XML Web Services security offering for high performance and highly available business environments. Not only does the solution protect server-based resources, it also protects against tampering on outbound connections to hosted services and data repositories.

Forum XWall™, the industry's only embeddable Web Services Firewall, on the Crossbeam X-Series family, provides XML security with built-in load balancing, failover and dynamic provisioning. This highly integrated and scalable approach dramatically improves the economics of deploying XML security, an area becoming a major concern for IT Security administrators as XML traffic is the fastest growing area of network traffic. The solution is easily installed and lets security administrators fortify their Web Services deployments without having to involve the web services administrative team.

Forum XWall runs on one or multiple APMs in the X40, X45 and X80 chassis. Multiple Forum XWall APM groups can be created to design a complete defense-in-depth security model completely housed within a single X-Series security switch. Enterprises can consolidate multiple single application HW security appliances such as Firewall, Application FW, IDS, Content Filtering and XWall onto Crossbeam APMs, greatly simplifying network security deployments into a single chassis. This new architecture provides an immediate ROI on existing security deployments as well as providing a future-proof platform to protect against security threats of the future.

XML ATTACKS: HIGHLY SOPHISTICATED, MULTIPLYING RAPIDLY Forum XWall on Crossbeam X processes XML traffic flows to actively protect organizations against a growing XML-related threat profile that includes attacks such as:

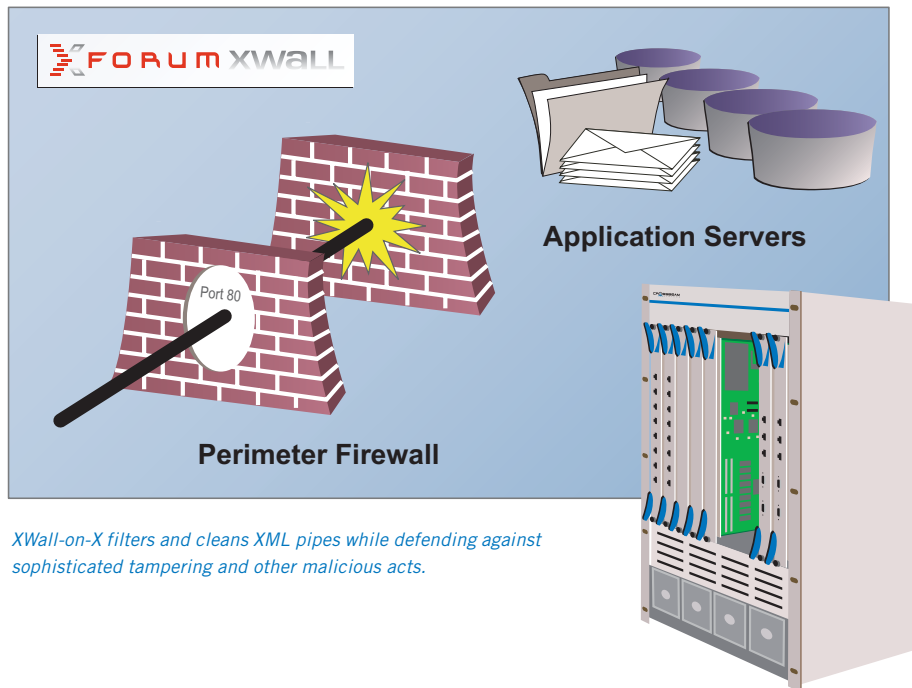
- Payload Parameter Tampering: Manipulated XML values are used to conduct fraudulent transactions
- XML Coercive Parsing: Corrupted XML/SOAP messages are used to disrupt and disable unprepared and vulnerable services
- XML Recursive Payload: Deeply nested XML documents are constructed to exhaust computing resources
- WSDL Scanning: Business API's are probed for sensitive data and vulnerabilities
- External Entity Attacks: External references can be made to import compromised data
- SOAP Routing Detours: Messages are re-directed to malevolent processing intermediaries
- SOAP with malicious software: SOAP hides and obscures viruses, spyware and other unwanted programs
- SQL Injections into SOAP: SQL code is modified and left undetected because it is embedded in XML
- WS-Security Spoofing: SOAP security contexts are overridden to gain unauthorized data access

Features

XWALL ON X: HIGHLY EFFECTIVE, HIGHLY SCALABLE XML PROTECTION Forum XWall is the perfect complement to a traditional perimeter firewall. Deployed on the X-Series platform, the application simply slides in as a blade and all XML traffic can be provisioned to flow through it either before or after perimeter firewall processing. In addition, the security administrator can deploy the solution without changes to the data center architecture and without having to involve the web services developers.

Once installed in the X-Series, the application immediately takes advantage of all the high performance, high availability and scaling features of Crossbeam security switches. For example, to increase capacity a second XWall blade is added, automatically provisioned and immediately available.

Forum on Crossbeam unleashes the full power of XML protections including parsing and inspection, schema conformance, tamper-proofing of parameters, WSDL operations and many more. The system can be used to protect against inbound attacks on application servers but also against attacks on outbound connections to hosted services. Thus, a sales administrator using a Salesforce.com™ service will have their transactions protected as well. This dual protection in one system is uniquely available as XWall on X. The end result is complete, easy-to-install XML protection at enterprise and carrier grade levels.

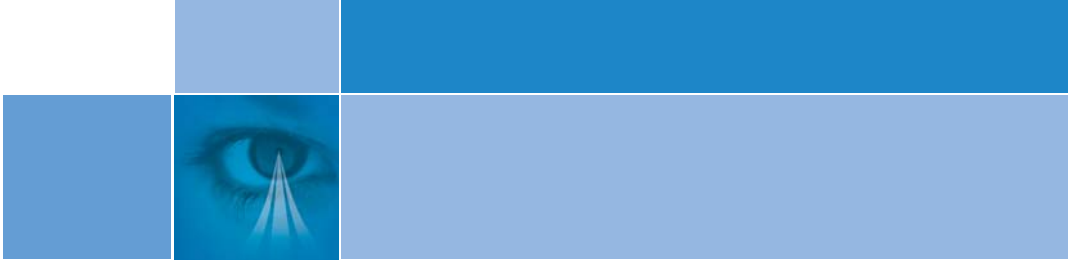


XML PROTECTION FEATURES

XML Intrusion Prevention	Anomaly and signature based detection of XML-vectored threats with pre-configured security profiles, attack signatures and response mechanisms
Web Services Standards	XML 1.0, XML Schema and DTD, SOAP 1.1/1.2, XPath, WSDL 1.1, WS-I Basic Profile 1.0, HTTP 1.1/1.0
XML Malware Scanning	Allows administrators to arrest the propagation of viruses, Trojans, worms, spyware and unwanted programs embedded in XML and SOAP
Vulnerability Containment Service	Threat discovery with Web services diagnostics for runtime and design time phases; XML-related vulnerability metabase and alert notification system
WS-Security 2004 1.1 Provider (Add-On)	WS-Security Headers, Username, X.509, SAML (1.0/1.1), Kerberos tokens, XML encryption, XML signature, SSL Mutual Authentication
WSDL Admission Control	Configure and consume policies to verify asserted identities and resolve access control decisions via a transport as well as message-based protocols Roles based access control, Granular (operation and message) policy administration, Wizard driven GUI
Web Services Identity Processing	Transform an identity that exists in one domain to an identity within another domain Credential conversion e.g. X.509 to Kerberos/WS-Security token Microsoft Active Directory, LDAP, Oracle COREid Access & Identity, IBM Tivoli Access Manager, CA SiteMinder, CA TransactionMinder Public Key Infrastructure Integration
Protocol Mediation (Add-On)	Broker policies, negotiate quality and translate application transport protocols IBM Websphere™ MQ, Tibco Rendezvous™, Tibco EMS™, SMTP, JMS, FTP , Mediate between messaging protocols , Propagate credential and authentication assertions across protocols

SCALABLE PLATFORM FEATURES

Management	Hot-swappable blades and easy software updating Separate, out-of-band management network to prevent hacker attacks Wizard-based installation System management functions such as fault, configuration, performance, and statistics SNMP support for secure retrieval of statistics and trap information Secure, standards-based management interfaces (SSH, HTTPS) to service management as well as operations and support management systems Full audit trail
Data Center – and Carrier-class Platform for Secure Application Delivery	High availability failover Full redundancy features built in at all layers of the system – no single point of failure Health monitoring agents assuring carrier-class 99.999% availability of security application services User traffic directed and processed by redundant application process during process recovery Standards-based port transfers from a failed link to another operational link Minimal power draw (1000W per complete 14-blade system)
Multiple Apps at Multi-Gigabit Speeds	Easy evolution of application functionality and scale enabled by in-service upgrades of system or application software In-line multiple security application throughput without performance degradation.



About Crossbeam Systems

Crossbeam Systems, Inc., is a leading global developer of total security solutions required for safer, simpler networks. Crossbeam enables companies to consolidate their security infrastructures while preserving their security policies, resulting in significant savings in capital and operational expenses. Crossbeam's patent-pending architecture integrates best-in-class security engines such as firewall, virtual private networks, intrusion detection and content security into high-performance, highly available, self-healing security services switches. The company has tailored solutions for global enterprises, carrier networks and medium-sized businesses. More information is available at www.crossbeamsystems.com.



www.crossbeamsystems.com

Corporate Headquarters
200 Baker Avenue
Concord, MA 01742 USA
p: [+1] 978-318-7500
f: [+1] 978-287-4210

European Headquarters
E. Space, Bat C.
45 allée des Ormes
06250 Mougins – France
p: [+33] (0)4 92 28 89 89
f: [+33] (0)4 92 28 72 60

Asia Pacific Headquarters
80 Raffles Place
Levels 36 UOB Plaza 1
Singapore 048624
p: [+65] 6248 4684
f: [+65] 6248 4988