

Vordel XML Firewall

Threat protection for XML applications

Vordel XML Firewall protects XML applications from malicious attack and unauthorized access. By blocking a wide range of attacks on XML applications, Vordel XML Firewall shields XML applications and allows them to be deployed in safety and confidence.

Vordel XML Firewall forms an integral component of any enterprise's SOA security infrastructure and can be deployed as part of a strategic architecture of XML firewalls, gateways and run time governance products. Vordel XML Firewall complements other application security and network security products by providing the XML data screening which other products do not provide.

Threat Awareness

Vordel XML Firewall provides full threat protection posture against XML attacks. Untrusted service invocations are denied by default.

Vordel XML Firewall filters applications which use SOAP, applications using "plain XML", and applications which are invoked using HTTP GET invocations (including AJAX and "Web 2.0" applications).

The firewall protects XML applications using a comprehensive set of pre-built content-filtering and traffic-analysis rules. It protects against XML Denial of Service, SOAP attachment viruses, buffer-overflow attempts, malformed or invalid XML, unexpected MIME-Types in SOAP attachments, application-level attacks including SQL Injection, service scanning, and brute-force 'flooding' denial-of-service attacks.

- Block "clogging" attacks**
 A clogging attack occurs when an attacker sends an extremely large XML file to a Web Service, in order to cause it to become overloaded as it processes the XML. Vordel blocks clogging attacks by allowing an administrator to configure the size bound for XML message sizes.
- Block Service Scanning**
 Service scanning involves an attacker probing for available services whose WSDL descriptors are available.
- Block covert channel attacks**
 XML messages can contain malicious content in parts which are intended to be ignored by screening applications. Vordel XML Firewall detects and blocks these attacks.
- Block XML Denial of Service**
 XML messages can be crafted to include deeply nested elements, false Schema invocations, attempts at recursion, and other techniques to cause denial-of-service at an application server. Vordel XML Firewall blocks these attacks.
- Block data-harvesting attacks**
 Data-harvesting attacks force applications to return back all data, rather than simply returning the prescribed data response. Blocking such attack involves enforcing size rules on response data. This is configurable on a per-operation basis, since operations will differ in the size of the XML content which they process.

- Block XML threats such as SQL Injection and XML Denial of Service**
 XML messages may harbour attacks such as SQL Injection and XPath Injection. Most XML Schemas do not discover these attacks, since they only check message structure, and not message content. Traditional Denial-of-Service attacks which use excessive traffic to overwhelm Web Service applications are also blocked.
- Protect against vulnerabilities associated with XML parsers, .Net and J2EE frameworks**
 Platform specific vulnerabilities exist for common platforms such as Apache Axis, Xerces, Microsoft .Net. Vordel's research team has been to the fore of identifying these weaknesses and ensures our products are designed to block these and enable our customers can use these platforms in confidence.

Client Authentication

Vordel XML Firewall performs authentication on clients using industry standard HTTP Authentication and X.509 Certificates with SSL. This is in compliance with the WS-I Basic Security Profile (2007).

Alerting on XML security events

Alert against attackers attempting to gain unauthorized access to an XML application, Email alerts are sent to security administrators notifying them of any attempted attacks.

Blacklisting with Network Firewalls

Blacklisting sources of malicious XML by alerting upstream network firewalls of the offending IP addresses. XML messages coming from an untrustworthy IP address will be detected, blocked, and may optionally also be logged.

Data Integrity control checks

Validate incoming XML and SOAP messages for conformance with XML Schemas, WS-I Basic Profile data integrity.

Rapid Deployment

Vordel provides pre-built policies which allow Vordel's customers to get up-and-running quickly with XML Firewalling.

Security for all flavors of XML applications

Vordel XML Firewall provides protection for all three classes of XML applications: SOAP-based Web Services, "plain XML" applications which do not use SOAP, and "REST style" applications which are invoked using HTTP GET. The device supports many XML dialects, including ACORD and FIXML.

Audit trail

Essential to any corporate governance framework is the ability to comply with industry regulations by maintaining an audit trail of external XML-based communications. Vordel XML Firewall can track usage, disruptions, and create an audit trail of all these activities. In conjunction with VordelReporter an interface to generate reports on all Web Services-based transaction archives is available.

Real Time Monitoring

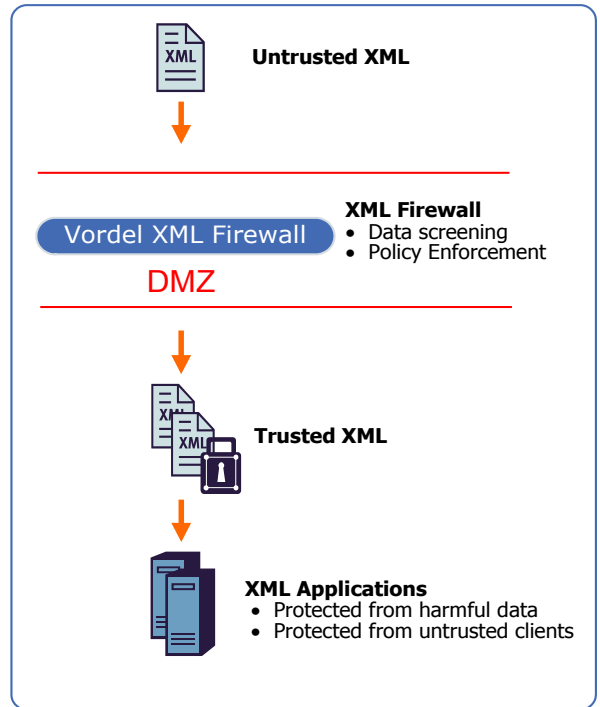
Vordel XML Firewall ships with a real-time Monitoring Console that provides color-coded message filtering status on message throughput. Administrators can search events on a per message or event type (e.g. Schema validation).

Performance Optimized VX Deployment Platform

Integrated into the firewall is Vordel's patented core VXA (XML security acceleration) engine. This processing engine accelerates the essential XML security primitives. The VX deployment platform includes cryptographic acceleration hardware embedded in the device and Gigabit Ethernet cards provide wire-speed network performance.

Deployment Options

Vordel XML Firewall	VX4000	VX8000	Windows	Linux	Solaris
	x	x	x	x	x



Deployment architecture showing in-line XML firewall in DMZ filtering incoming XML for malicious data and unauthorized access.

Vordel Offices

European HQ

Vordel
30 Pembroke street upper
Dublin 2, Ireland
Tel: +353 1 234 2500

US HQ

Washington DC Metro Headquarters
13800 Coppermine Rd. #306
Herndon, VA. 20171
Tel: 1-(866)-460-0987

Vordel Datasheet, Copyright © 2000 – 2009 Vordel Limited. All rights reserved. All content in this datasheet is for general information and promotional purposes only and neither constitutes a technical specification nor an offer to enter into contractual relations with Vordel or with any other party; and Vordel reserves the right to alter such content without notice at any time. The trademarks, logos and service marks displayed herein are registered and unregistered trademarks of Vordel and others.