

# VORDEL APPLICATION FIREWALL

Many business functions today are powered by web applications and web services, ranging from ordering, fulfillment, to payment. Attacks on these critical applications can result in loss of revenue and sensitive data. With the proliferation of client types ranging from mobile devices to Cloud based services, the chances of a service being brought down by poorly designed partner applications, is as likely as by malicious attacks against the web interface. Vordel protects your application across all its interfaces, including simple HTML and Web 2.0 AJAX user interfaces, SOAP and REST web services, and secure file transfer (SFTP and FTPS).

## Protection Across All Application Interfaces

Network firewalls do not block message level threats. Web application firewalls only protect web applications. Vordel Application Firewall detects and prevents threats across SOA, Cloud, Web, B2B, and mobile interfaces. Messages are scanned at the protocol header level (e.g. HTTP headers), SOAP header level (for security tokens and timestamps), XML level and at the attachment level.

## Protection In Breadth and In Depth

Vordel Application Firewall detects and prevents all common attacks against web applications and services, including those listed in the NIST SP800-95 and OWASP Top 10 guidelines. Vordel Application Firewall has integrated virus scanning of message content and attachments. Vordel offers out-of-the-box integration with leading anti-virus services, including CLAM AV, McAfee and Sophos.

## Turnkey Security Service

Vordel makes application security simple. Detection and prevention filters are prebuilt. Attack signatures are updated automatically. Vordel also has integrated authentication, authorization, and audit capabilities, along with out-of-the-box integration with all the leading identity management platforms such as CA, Entrust, IBM, Microsoft, Novell, Oracle, and RSA. With Vordel Application Firewall, application developers and administrators do not have to be security experts.

## Vordel Application Firewall Solution



## Feature Highlights

Vordel Application Firewall provides real-time protection for enterprise applications and SOA infrastructure.

### Prevent Threats

- Detect and prevent attacks on-the-wire
- Denial of service attacks
  - Command injection attacks
  - Malicious code, virus
  - Sniffing
  - Spoofing, tampering, and impersonation
  - Data harvesting
  - Privilege escalation
  - Reconnaissance

### Traffic Control

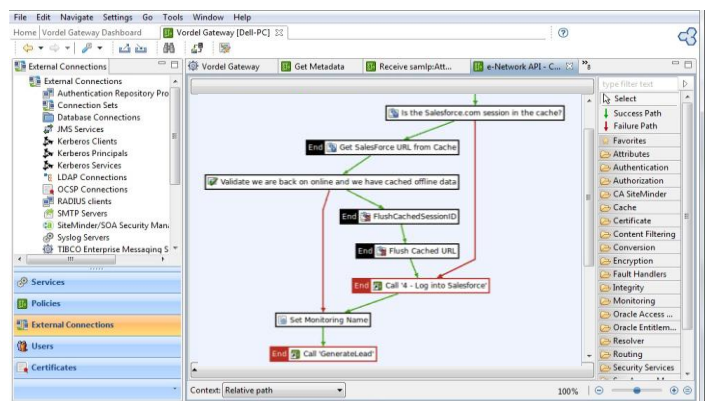
- Route, divert, throttle, and block traffic
- Route messages base on message type and size
  - Divert and quarantine suspect messages
  - Throttle suspicious and abnormal traffic

### Logging and Monitoring

- Log, trace, diagnose attacks and suspicious activity
- Configurable logging of transactions and events
  - Trace and debugging tools
  - Automated alerts
  - Real-time monitoring
  - Service level analytics
  - Automated report delivery
  - Integration with network management platforms

### Access Control

- Authenticate, authorize, and audit access
- Control access to web services, registry, and administration functions
  - Integrate with identity management platforms
  - Validate security tokens



Drag-and-Drop Policy Development

### Prevent Denial of Service Attacks

**Flooding** – The Firewall enforces maximum messages policy to divert or block message flooding.

**Recursive Payloads** – The Firewall disallows DTD and controls the maximum allowable number of nested elements and attributes per element.

**Oversized Payloads** – The Firewall controls the size of XML messages, both the XML body and any attachments.

**Memory Leak** – The Firewall controls allowable message size, maximum element count and maximum attribute count.

### Prevent Command Injection & Malicious Code

**Injections** – The Firewall uses attack signatures to detect and block SQL and XML injections, such as XPath injection).

**Cross-Site Scripting** – The Firewall uses attack signatures to detect and block cross-site scripting.

**Form Validation** – The Firewall validates variables for both GET and POST HTML forms against syntax and other requirements

**Malformed Content** – The Firewall blocks invalid XML or non well-formed XML by default.

**Logic Bombs, Trapdoors, and Backdoors** – Rogue services that may contain malicious content are blocked by default.

### Protect Confidentiality and Integrity

**Sniffing** – Firewall traffic is encrypted at both the transport level (SSL) and the message level (XML encryption).

**Parameter Tampering** – The Firewall applies XML Signature or HMAC Signature to parameters to prevent tampering.

**Schema Poisoning** – Vordel stores schemas in a protected cache and does not trust schemas within incoming messages.

**Spoofing of UDDI/ebXML messages** – Untrusted messages are blocked by default and the Firewall employs countermeasures such as replay attack blocking.

**Cookie Poisoning & Hijacking** – The Firewall detects the poisoning and unapproved use of another user's cookie.

**Checksum Spoofing** – The Firewall calculates checksums and compares the tally with the checksum in the message.

**Principal Spoofing** – The Firewall checks principle names contained in security tokens such as WS-Username and SAML.

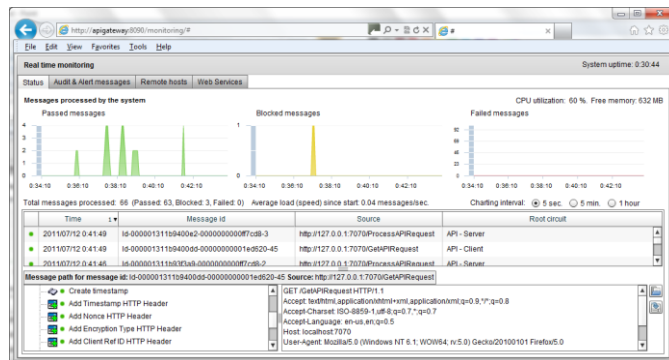
**Routing Detours** – Attempts to route messages to destinations beyond what is signed and validated within WS-Addressing "to" and "via" attributes are blocked by default.

**External Entity** – The Firewall disallows Document Type Definition (DTD) and the loading of local files by default.

**Canonicalization** - Canonicalization is part of Vordel's standard implementation of the XML Signature specification.

### Logging, Tracing, Monitoring, and Reporting

Vordel Application Firewall comes with fully configurable logging and easy-to-use tracing tools to help diagnose attacks and malfunctioning integrations. Real-time monitoring lets administrators monitor transactions in flight and reports can be automatically generated and delivered.



Advanced Reporting and Real-Time Monitoring

### Prevent Reconnaissance Attacks

**Code Templates** – Any request that searches for code templates is blocked by default unless allowed by policy.

**Forceful Browsing** – JavaScript code that redirects a browser is blocked using attack signatures.

**Directory Reversal/Traversal** – Firewall policies apply to relative paths (e.g. "/myservices/Service1"), so attempts to traverse the directory with URL such as "/myservices" is blocked by default.

**WSDL Scanning** – Access to the WSDL of a service is protected by Firewall policies.

**Registry Disclosure** – Access to registry content via SOAP and REST is protected by the Firewall. The Firewall can add encryption to protect registry content in transit.

### Prevent Privilege Escalation Attacks

**Dictionary** – Dictionary attacks are detected via repeated authentication failures. The Firewall enforces policies such as maximum allowable number of failed authentications per minute.

**Format String** – The Firewall uses attack signatures to detect non-ASCII characters and the presence of JavaScript.

**Buffer Overflow** – The Firewall imposes size limits on XML elements and attributes. Additional protection can be achieved by limiting memory use per thread.

**Race Conditions** – The Firewall assigns each request a unique ID number which eliminates race conditions.

**Symlink** – Traffic to symlinked services with no explicit policy applied are blocked by default.

**Unprotected Admin Interfaces** – Access to ports and services are blocked by default, including administrator interfaces.