Inter Do

Version 3.0

Web Application Firewall

Are your assets and data wide-open to attacks?

Web Application Uncertainty

An unprecedented level of Web application attacks have dealt a significant blow to the business community in the last year and the situation continues to worsen. Hackers excel in technology innovation with amazing and dangerous scripts that are passed around like candy on the Web.

Security breaches can lead to loss of company assets, invasion of privacy, identity theft, costly mischief, or irreparable system damage. Unfortunately, traditional security measures remain unable to differentiate the threatening hacker activity from regular application activity.

The following is a highlighted list of vulnerabilities missed by traditional security measures:

WebServices Manipulation
Exploiting vulnerabilities inherent in WebServices formats, structure and operations

Manipulation of IT Infrastructure Vulnerabilities
Exploiting vulnerabilities in an integrated Internet environment, such as common files and folders

Parameters Tampering
Modifying parameters values and injecting additional parameters in the HTTP request submitted to the server

Cookie Poisoning
Changing or exploiting cookie content

Stealth Commanding
Planting hidden commands in text fields that cause the execution of malicious code

Backdoor and Debug Options
Exploiting vulnerabilities left open in the developed code

3rd Party Misconfiguration
Exploiting configuration errors in 3rd party components, such as Web and database servers

Database Sabotage
Linking various SQL commands to input fields or messages

Buffer Overflow Attacks
Sending large request messages to the application, attacking either 3rd party or internally developed code

Data Encoding
Sending requests using different data encoding standards such as Unicode, UTF-8, and UTF-16

Protocol Piggyback
Modifying the application protocol structure

Cross-Site Scripting
Attacks the end user’s browser revealing the end user’s session token, attack the local machine, or spoof content.

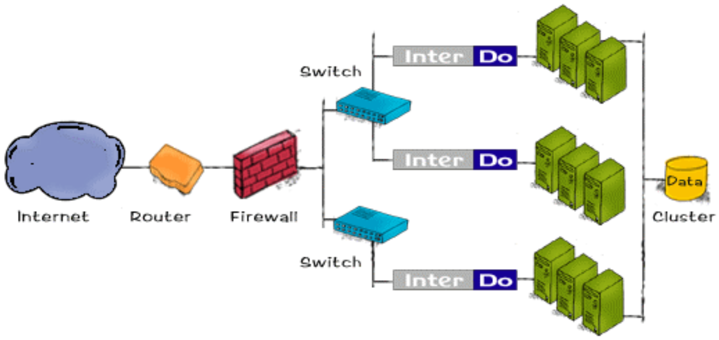
Why InterDo™ Is Essential to Security Arsenals

Traditional security measures do not address or prevent security breaches that exploit the unique logic, structure and technology of Web applications. Firewalls, Intrusion Detection Systems (IDS) and Public Key Infrastructures (PKI) are not designed to protect the application layer.

Web applications are given freedom to operate and interface with the back-end infrastructure where application activity is recognized as “trusted”.

A hacker can possess the application-privileges by exploiting application vulnerabilities, often gaining even greater privileges than the application has. Traditional security measures do not recognize the deviation and assume the hacker activity is that of the trusted Web application.

If an enterprise relies on traditional methods alone, there is a high likelihood that their applications can and will be penetrated.



How InterDo™ Works

Using a positive security model, *InterDo* monitors the data flowing into and out of the Web applications, validating and securing requests before they pass to the core of the business network, the back-end infrastructure.

By only allowing acceptable Web application use, *InterDo* helps prevent known and unknown forms of attacks that deviate from the implemented security policies.

Delivering comprehensive and adaptable application-layer security, *InterDo* complements other security components, extending protection beyond the IT infrastructure to protect applications and their business logic.

Inter Do

Version 3.0

Web Application Firewall

Web Application Protection without Compromise

Key Features:

Rigorous Security

- **Positive Security Model**
  Provides protection against known and unknown threats
- **Secures SOAP & WebServices**
  Allows implementation of security policies that recognize and secure these formats
- **Certificates Support**
  Supports both sever-side and client-side certificates, encrypts and securely stores private keys

Rapid Deployment

- **Multiple Configuration Methods**
  Features state-of-the-art learning engines, automatic policy generation with *KaVaDo's AutoPolicy*, Quick-Click policy refinement, and intuitive forms for data entry
- **Security Policy Template**
  Provides a security policy template that is automatically applied as a base configuration for each application policy

Maximum Flexibility

- **Multiple Platform Support**
  Offers compatibility with Solaris, Linux, and Windows platforms
- **Tailored Security Policy**
  Provides an independent and tailored security policy for each application
- **Virtual Hosting Support**
  Allows one or more security policy definitions for each virtual host (running on the same IP and port)

Simple Management

- **Security Dashboard**
  Provides a structural view and navigation of Web application security policies and their components
- **Centralized Alerts Publishing Server**
  Publishes and manages alerts for one or more *InterDo* servers from a centralized location
- **Enhanced Logging and Filtering Performance**
  Filters and controls the entries within log report

Scalability and Performance

- Support for thousands of concurrent connections
- Ability to handle millions of hits per day
- Protection for small, corporate-size or mega sites
- Unequalled performance of 900hps / 66mbps
- Ability to handle multiple network segments simultaneously

Technology & Standards

- Patent-pending AutoPolicy™
- Patent-pending Protected Path™
- SSL, Server & Client certificates
- FIPS-approved standard public-key encryption algorithms
- PKCS#12, PEM, ASN-1, DER certificate formats
- OPSEC certified

Log & Alerts

- Severity classification of alerts
- Centralized alert distribution service
- Multiple alert formats include: SNMP, SMTP, SysLog, Network message, and OPSEC ELA
- Compliance with major network management solutions (HP OpenView, IBM - Tivoli etc.)

Management Console

- Enterprise management console
- Remote management capabilities for multiple servers
- SSL encryption with authenticated communication to remote servers
- Logging of management activity allowing follow-up audits

Compatibility

- Solaris, Linux, and Windows
- HTTP and HTTPS – 1.0, 1.1
- SOAP 1.1 and WSDL 1.1
- ODBC, for storing logs in Oracle, MSSQL and MSAccess databases
- All major Web servers (Apache, IIS, etc.)
- All major application servers (BEA, WebSphere, etc.)
- All major Web browsers (IExplorer, Netscape, etc.)
- All major load balancers (F5, Radware etc.)
- All major application switches (F5, Radware etc.)
- All major Web statistics applications (WebTrends etc.)

System Requirements

Microsoft Windows

- OS: NT4, 2000
- CPU: P-III 800Mhz or greater
- Memory: 128MB or greater
- NIC: 10/100 Ethernet adapters
- 64MB of free disk space

Sun Solaris

- OS: 8, 9
- CPU: Sparc 400Mhz or greater
- Memory: 128MB or greater
- NIC: 10/100 Ethernet adapters
- 64MB of free disk space

RedHat Linux

- OS: 8
- CPU: P-III 800Mhz or greater
- Memory: 128MB or greater
- NIC: 10/100 Ethernet adapters
- 64MB of free disk space

KAVA DO

http://www.KaVaDo.com
sales@KaVaDo.com

KaVaDo Inc.
US Headquarters
130 West 42nd, Suite 850
New York, NY 10036
Tel: (US)
(800) 239-3203
Tel: (212) 302-2400

KaVaDo Europe Ltd.
European Headquarters
Gainsborough House 33 Throgmorton,
London EC2N 2BR England Tel: 44
(207) 397-3450