



# Barracuda Web Application Firewall Vx

Protects web applications and improves performance

The Barracuda Web Application Firewall Vx is a virtual appliance purpose-engineered to stop data theft through vulnerable web applications while optimizing web application performance. Using the same proven technology as the Barracuda Web Application Firewall hardware appliances, this virtual solution scans incoming application traffic to detect and block attacks and scans traffic outbound from the server to stop any transmission of sensitive data such as Social Security and credit card numbers. Simple to use and highly affordable, the Barracuda Web Application Firewall Vx is indispensable for secure, scalable application delivery for virtual environments.

## Leading Web Application Security

The Barracuda Web Application Firewall Vx intercepts SQL injection, cross scripting, OS command injection and other sophisticated attacks before being input to web applications. With security that cloaks error messages, cookies and other clues that facilitate attacks, this solution further hardens web application security. Data loss prevention technology actively scans for and blocks or cloaks outgoing Social Security Numbers, credit card numbers, directory data and other confidential information. Integrated with LDAP, RADIUS and other authentication protocols, the Barracuda Web Application Firewall Vx lets administrators customize user access policies for applications like SharePoint, OWA and others.

## Optimized Application Delivery

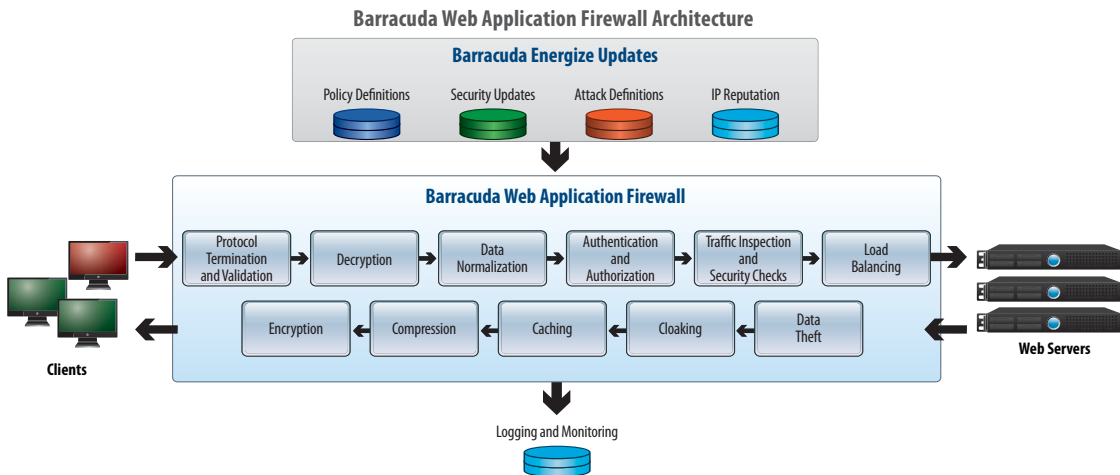
A built-in load balancer optimizes server utilization and maximizes performance. Using layer 7 content switching to route requests quickly to the right servers (content-based traffic forwarding) and with file compression, app acceleration, SSL acceleration, and caching to optimize traffic, application optimization is built in at no extra cost.

## Easy to use

It is simple to remotely download and install the Barracuda Web Application Firewall Vx in virtual environments. Default policies deliver instant web application security at deployment. A dashboard gives visibility into web app and threat activity. For further ease of use, security policy templates for Oracle, OWA, SharePoint and others simplify administration while Barracuda Energize Updates automatically update firmware and threat profiles. Reverse proxy security, a load balancer, caching, user authentication, data compression, SSL acceleration in one VM appliance simplifies DMZ architecture. Furthermore, the Barracuda Web Application Firewall Vx's intuitive GUI makes monitoring, management and reporting fast and easy.



The Barracuda Web Application Firewall Vx monitors and tracks common application attacks, performance statistics and bandwidth usage.



EDITION  
360 Vx  
460 Vx  
660 Vx



# BARRACUDA WEB APPLICATION FIREWALL Vx

EDITION  
360 Vx  
460 Vx  
660 Vx

## TECHNICAL SPECIFICATIONS

### Key Features

#### SUPPORTED WEB PROTOCOLS

- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML

#### IPV6 Ready

#### WEB APPLICATION SECURITY

- OWASP Top-Ten Protection
- Protection against common attacks
  - SQL Injection
  - OS command injection
  - Cross-site scripting
  - Cookie or forms tampering
- Form field meta data validation
- Adaptive security
- Web site cloaking
- Response control
  - Block client
  - Reset connection
  - Redirect
  - Custom response

- Outbound data theft protection
  - Credit card numbers
  - Social Security numbers
  - Custom pattern matching (regex)
- Granular policies to HTML elements
- Protocol limit checks
- File upload control
- Protection against Distributed Denial of Service
  - Brute force protection
  - Session Tracking
  - Slow client attack protection
  - Rate control
- Blocking based on Client IP Reputation
  - Geo IP location
  - Anonymous Proxy

#### AUTHENTICATION AND AUTHORIZATION

- LDAP/RADIUS/local user database
- Client certificates
- Single sign-on
- RSA SecurID<sup>2</sup>
- CA SiteMinder<sup>2</sup>

#### LOGGING, MONITORING AND REPORTING

- System log
- Web Firewall log
- Access log
- Audit log

#### SIEM Integrations

- RSA enVision
- Splunk
- ArcSight
- Symantec

#### APPLICATION DELIVERY AND ACCELERATION

- High availability
- SSL offloading
- Load balancing
- Content routing

#### XML FIREWALL

- XML DOS protection
- Schema / WSDL enforcement
- WS-I conformance checks

#### NETWORKING

- VLAN, NAT
- Network ACLs

#### System Features

- Graphical user interface
- Role-based administration
- Secure remote administration
- Optional ethernet bypass
- Trusted host exemption
- Vulnerability scanner integration

#### Virtualizer Support

- VMware ESX/ESXi
- VMware Server/Fusion/Workstation/Player
- Citrix XenServer
- Oracle VirtualBox

#### Support Options

- Energize Updates Subscription

EDITION COMPARISON	BWF 360 Vx	BWF 460 Vx	BWF 660 Vx
Back End Servers Supported	1- 5	5- 10	10-25
Inbound Web Traffic	25 Mbps	50 Mbps	100 Mbps
Number of CPU Cores Supported	2	3	4
HTTP/HTTPS/FTP Protocol Validation	✓	✓	✓
Protection Against Common Attacks	✓	✓	✓
Form Field Metadata Validation	✓	✓	✓
Web Site Cloaking	✓	✓	✓
Response Control	✓	✓	✓
Outbound Data Theft Protection	✓	✓	✓
Granular Policies to HTML Elements	✓	✓	✓
File Upload Control	✓	✓	✓
Logging, Monitoring and Reporting	✓	✓	✓
SSL Offloading	✓	✓	✓
Authentication and Authorization	✓	✓	✓
Vulnerability Scanner Integration	✓	✓	✓
Centralized Management	✓	✓	✓
Protection Against DDos Attacks	✓	✓	✓
Network Firewall	✓	✓	✓
High Availability: Active/Passive	✓	✓	✓
Caching and Compression		✓	✓
LDAP/RADIUS Integration		✓	✓
Load Balancing		✓	✓
Content Routing		✓	✓
High Availability: Active/Active			✓
Advanced Routing			✓
Adaptive Profiling			✓
AV for File Uploads			✓
XML Firewall			✓