Barracuda Web Application Firewall

Powerful application-layer security for Web sites and Web servers

The Barracuda Web Application Firewall protects Web sites and Web applications from attackers leveraging protocol or application vulnerabilities to instigate data theft, denial of service, or defacement of an organization's Web site. Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP, HTTPS, or FTP traffic for Web applications, the Barracuda Web Application Firewall proxies this traffic and inspects it for attacks to insulate Web servers from direct access by hackers.
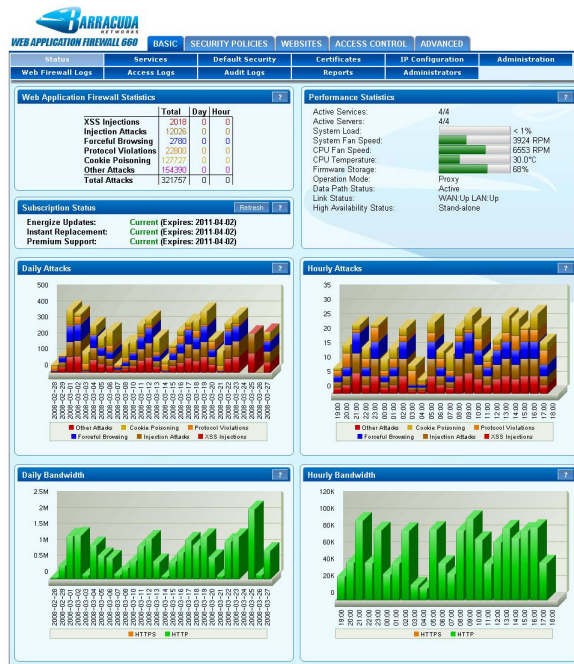
Comprehensive Web Site Protection

The Barracuda Web Application Firewall provides award-winning protection from all common attacks on Web applications, including SQL injections, cross-site scripting attacks, session tampering, and buffer overflows. As a full proxy, the Barracuda Web Application Firewall blocks or cloaks attacks, while preventing sensitive outbound data leakage such as credit card or Social Security numbers.
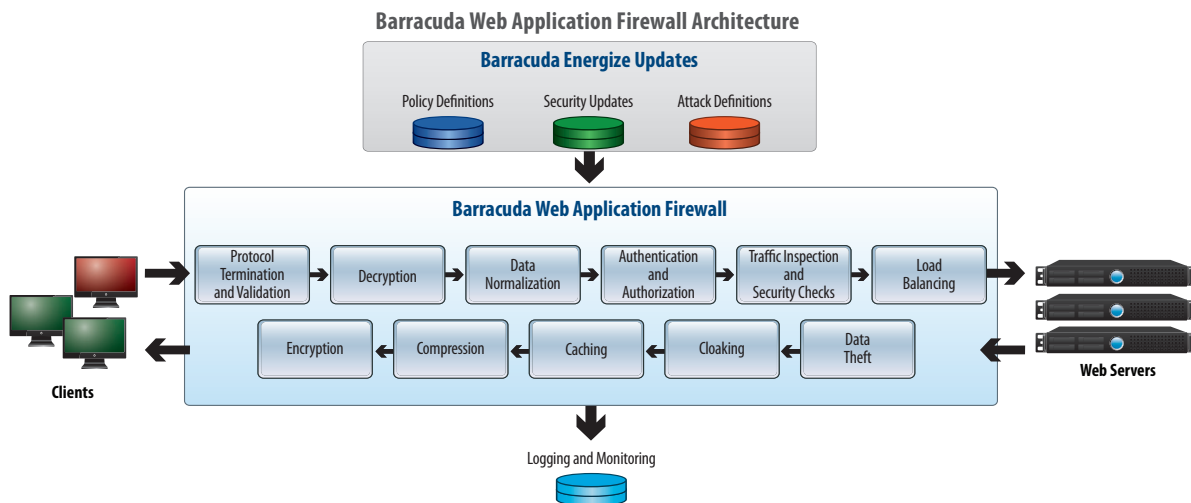
In addition, the Barracuda Web Application Firewall mitigates broken access control to applications by preventing cookie tampering and corruption of an application's access control system. Unlike intrusion detection systems that only analyze byte patterns, the Barracuda Web Application Firewall terminates HTTP traffic on behalf of the Web server to decode character sets, remove padded spacing, and normalize against common obfuscation techniques. For added security, the Barracuda Web Application Firewall provides full PKI integration for use with client certificates to verify identities of clients accessing the Web applications.

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

Advanced Traffic Management and Acceleration

To minimize ongoing administration associated with protecting Web sites against application vulnerabilities, the Barracuda Web Application Firewall automatically receives Energize Updates with the latest policy, security, and attack definitions. In addition to the comprehensive security benefits, there are also application delivery capabilities such as SSL offloading, SSL acceleration, and load balancing. These capabilities are designed to improve the performance, scalability, and manageability of today's most demanding data center infrastructures.

Barracuda Web Application Firewall Architecture

MODEL
360
460
660
860
960

Typical Deployment

Internet ↔ Network Firewall ↔ **Barracuda Web Application Firewall** ↔ Web Server

BARRACUDA WEB APPLICATION FIREWALL

MODEL
360
460
660
860
960

TECHNICAL SPECIFICATIONS

Key Features

WEB APPLICATION SECURITY
- HTTP/HTTPS/FTP protocol validation
- 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

WEB APPLICATION SECURITY (cont.)
- AV for file uploads
- Protocol limit checks
- File upload control
- Brute force protection
- Session tracking
- Rate control

AUTHENTICATION AND AUTHORIZATION
- LDAP/RADIUS/local user database
- Client certificates
- Single Sign-On
- RSA SecurID
- CA SiteMinder

LOGGING, MONITORING AND REPORTING
- System log
- Web Firewall log
- Access log
- Audit log
- PCI reports
- Syslog/FTP support

APPLICATION DELIVERY AND ACCELERATION
- High availability
- SSL offloading
- Load balancing
- Hardware SSL acceleration
- Caching
- Compression
- Content routing

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

System Features
- Graphical user interface
- Role-based administration
- Secure remote administration
- Ethernet bypass ("fail open")
- Shared policies
- Trusted host exemption

Hardware Features

CONNECTORS
- Ethernet
  - LAN port
  - WAN port
  - Management port
- Serial port (DB-9) for console

POWER REQUIREMENTS
- AC Input Voltage - 110-240 V AC
- Frequency - 50 / 60 Hz

Support Options

ENERGIZE UPDATES SUBSCRIPTION
- Standard technical support
- Policy definitions
- Security updates
- Attack definitions

INSTANT REPLACEMENT SERVICE
- Replacement unit shipped next business day
- 24x7 Technical Support

MODEL COMPARISON	MODEL 360	MODEL 460	MODEL 660	MODEL 860	MODEL 960
CAPACITY*					
Backend Servers Supported	1-5	5-10	10-25	25-150	150-300
Inbound Web Traffic	25 Mbps	50 Mbps	100 Mbps	600 Mbps	1 Gbps
HARDWARE					
Rackmount Chassis	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Dimensions (in.)	16.8 x 1.7 x 14	16.8 x 1.7 x 14	16.8 x 1.7 x 22.6	17.4 x 3.5 x 25.5	17.4 x 3.5 x 25.5
Dimensions (cm.)	42.7 x 4.3 x 35.6	42.7 x 4.3 x 35.6	42.7 x 4.3 x 57.4	44.2 x 8.9 x 64.8	44.2 x 8.9 x 64.8
Weight (lbs. / kg.)	12 / 5.4	12 / 5.4	26 / 11.8	46 / 20.9	52 / 23.6
Front Ethernet Ports	2 x 10/100	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
Back Ethernet Ports	1 x 10/100	1 x 10/100	1 x Gigabit	1 x Gigabit	1 x Gigabit
AC Input Current (Amps)	1.2	1.4	1.8	4.1	5.4
ECC Memory			✓	✓	✓
FEATURES					
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	✓	✓	✓	✓	✓
Protocol Limit Checks	✓	✓	✓	✓	✓
File Upload Control	✓	✓	✓	✓	✓
Logging, Monitoring and Reporting	✓	✓	✓	✓	✓
High Availability	✓	✓	✓	✓	✓
SSL Offloading	✓	✓	✓	✓	✓
Authentication and Authorization	✓	✓	✓	✓	✓
LDAP/RADIUS Integration		✓	✓	✓	✓
Load Balancing		✓	✓	✓	✓
Content Routing		✓	✓	✓	✓
XML Firewall			✓	✓	✓

US 13.0   Specifications subject to change without notice.   *Capacity depends on environment and selected options.