

Barracuda Load Balancer ADC

Secure Application Delivery Controller for Availability, Acceleration, and Control



Highly demanding enterprise networks require full-featured application delivery that **optimizes application load balancing and performance while providing protection from an ever-expanding list of intrusions and attacks.**

- Security
- Storage
- Application Delivery

The Barracuda Advantage

- Proven technology that has blocked more than 11 billion real-world attacks
- High-performance platform designed for data centers
- GeoIP-based application control
- Pre-built application templates for rapid deployment
- Available as a virtual appliance

Product Spotlight

- Multiprotocol platform with fiber and copper network interfaces
- Advanced Layer 4 & Layer 7 load balancing
- SSL offloading & application acceleration
- Global Server Load Balancing for application delivery across data centers
- Comprehensive attack protection and Data Loss Prevention



Acceleration

The Barracuda Load Balancer ADC is ideal for optimizing application performance. It offloads compute-intensive SSL transactions from the server, preserving resources for applications. In addition, optimization features such as caching, compression, and TCP pooling enable faster application delivery and ensure scalability.



Availability

Using health and performance checks, the Barracuda Load Balancer ADC distributes traffic for efficient use of server resources and employs server failover for high availability. Global Server Load Balancing allows redundancy across multiple sites enhancing availability and speeding disaster recovery.



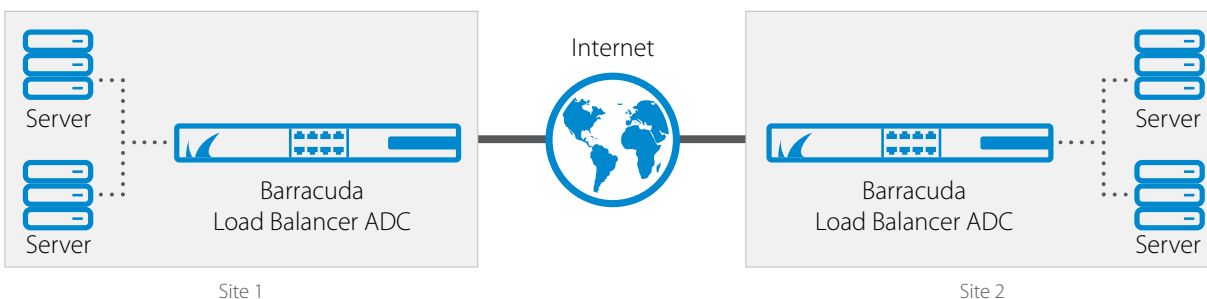
Control

Content routing and content rewrites enable full control of application traffic and customized application delivery based on users, regions, and/or devices. Client controls gives administrators the ability to throttle requests to ensure application availability even during periods of heavy traffic.



Security

Application Security provides superior protection against data loss, DDoS, and all known application-layer attack modalities. Automatic updates ensure comprehensive security for existing and emerging Layer 7 threats such as Cross-site Scripting (XSS), SQL injections (SQLi), and Cross-site Request Forgery (CSRF).



Barracuda has simplified everything. We set up two appliances within four hours, and the solution works great—for a fraction of what our previous solution cost.

Jeff Sharp
Network & Communications Director
Liberty Tax Service

Technical Specs

Availability

Load Balancing:

- Layer 4 & Layer 7 load balancing
- IPv6/IPv4 support
- Active/passive high availability
- Default load balancing
 - Round robin
 - Weighted round robin
 - Least connection
- Adaptive load balancing by CPU load, URL load, and terminal sessions
- Session and service group persistence
- Server health check and monitoring

Global Server Load Balancing:

- By priority, geographic IP, and region
- Health checks between multiple sites

Acceleration

- SSL offloading
- Caching & compression
- TCP connection pooling

Control

- Application traffic
 - Layer 7 content-based routing
 - Request/response rewrite
- Client & user limits
 - Brute-force
 - Rate control
 - GeolIP reputation

Network Security

- Layer 4 ACL
- VLAN, NAT

Application Security

- Security policies out of the box
- Website cloaking
- Form field metadata violation
- Protection against common attacks
 - OWASP Top 10
 - SQL injections
 - Cross-site Scripting
 - Cookie or form tampering
- Data Loss Prevention (DLP)
 - Credit card & SSN numbers
 - Custom patterns
- Granular policy management

Logging, Monitoring and Reporting

- Connection logs
- Audit logs
- Access logs
- Web Firewall logs
- Interactive and scheduled reports
- SNMP monitoring

Authentication/Authorization

- LDAP
- RADIUS
- Kerberos
- Two-factor authentication

Supported Protocols

- HTTP/S
- SSH
- SMTP
- IMAP
- POP3
- NNTP
- ASP
- DNS
- LDAP
- RADIUS
- TFTP
- RDP
- VDI
- WebSocket
- Windows Terminal Services
- Any TCP/UDP application

Support Options

Energyize Updates

- Firmware updates
- Application Security updates
- Standard technical support

Instant Replacement Service

- Unit replacement next business day
- 24x7 technical support
- Hardware refresh every four years

Management Features

- Customizable role-based administration
- Centralized management
- Real-time traffic statistics
- Web firewall, access, audit, and system logs
- Certified deployments with third-party applications

MODEL COMPARISON	240	340*	440*	540*	640*	641	642	840	841	842
CAPACITY										
Maximum Throughput	100M	1.2 Gbps	2 Gbps	5 Gbps	5 Gbps	10 Gbps	10 Gbps	5 Gbps	15 Gbps	15 Gbps
Real Servers Supported	10	35	50	100	250	250	250	500	500	500
HTTP Throughput		1 Gbps	2 Gbps	3.6 Gbps	3.6 Gbps	8.5 Gbps	8.5 Gbps	3.6 Gbps	13 Gbps	13 Gbps
HTTPS (SSL) Throughput		250 Mbps	400 Mbps	1 Gbps	1.3 Gbps	1.3 Gbps	1.3 Gbps	4.2 Gbps	4.2 Gbps	4.2 Gbps
Max. Compression Throughput				2 Gbps	2 Gbps	4 Gbps	4 Gbps	4 Gbps	7 Gbps	7 Gbps
Layer 4 Concurrent TCP Connections	500K	4M	10M	14M	16M	16M	16M	20M	20M	20M
Layer 4 TCP Connections per second	40K	40K	100K	120K	165K	165K	165K	360K	360K	360K
HTTP Connections per second		17K	22K	24K	60K	60K	60K	100K	100K	100K
HTTPS (SSL) Terminations per sec (2K Keys)		200	400	1400	8300	8300	8300	24000	24000	24000
HARDWARE										
Rackmount Chassis	1U	1U	1U	1U	1U	1U	1U	2U	2U	2U
Dimensions (in)	16.8x1.8x9	16.8x1.7x16	16.8x1.7x16	16.8x1.7x16	16.8x1.7x18	16.8x1.7x18	16.8x1.7x18	17.4x3.5x25.5	17.4x3.5x25.5	17.4x3.5x25.5
Weight (lb)	8	12	12	12	18	18	18	52	52	52
10/100 Copper Ethernet NICs	2									
1 Gb Copper		4	4	8	8	8	8	8	8	8
10 Gb Copper						2			4	
10 Gb Fiber NICs							2			4
AC Input Current (amps)	0.3	0.46	0.48	0.6	1	1	1	3.8	3.8	3.8
FEATURES										
Availability										
Layer 4 Load Balancing	•	•	•	•	•	•	•	•	•	•
Layer 7 Load Balancing		•	•	•	•	•	•	•	•	•
High Availability Cluster		•	•	•	•	•	•	•	•	•
Global Server Load Balancing			•	•	•	•	•	•	•	•
Link Bonding			•	•	•	•	•	•	•	•
Application Delivery										
SSL Offloading		•	•	•	•	•	•	•	•	•
Content Routing		•	•	•	•	•	•	•	•	•
AD and Kerberos Integration		•	•	•	•	•	•	•	•	•
HTTP Compression			•	•	•	•	•	•	•	•
Content Caching			•	•	•	•	•	•	•	•
Hardware Based SSL Offloading				•	•	•	•	•	•	•
SSL hardware acceleration				•	•	•	•	•	•	•
Application Security										
Inbound Attack Protection				•	•	•	•	•	•	•
Outbound Data Theft Protection				•	•	•	•	•	•	•
Protection Against DDoS Attacks				•	•	•	•	•	•	•

*Select Models Available as Virtualized Appliances †The SSL TPS numbers are based on a single handshake per transaction Specifications subject to change without notice.