FortiADC™ E-Series

Application Delivery Controllers

From simple server load balancing to enterprise-grade global traffic management, the FortiADC E-Series appliances can meet the needs of almost any web-based application. The FortiADC line-up of hardware-based solutions meets or outperforms competitive products costing up to 3 times as much. You pay for what you need and don't have to buy option after option to get a solution that fits your business requirements.

Reliable and Robust Load Balancing and Application Delivery

At its heart, the FortiADC is a tried-and-true load balancer. From simple L4 TCP and UDP to advanced L7 HTTP and HTTPS, FortiADC can provide basic load balancing to precise content switching with L7 Match Rules. FortiADC gathers real-time information about a server's status using ICMP Probes, TCP Probes, Active Content Verification (ACV) and Server Agents to route traffic based on easily configurable business rules. All FortiADCs support persistence using either cookies or IP addresses to reliably maintain server connections for your more advanced applications.

In the event that servers in a server pool are unable to satisfy a client's request, Responders can be assigned to L7 Match Rules to redirect users to another URL or display a custom message.

High Availability for 100% Application Uptime

Mission-critical applications need mission-ready solutions. FortiADC's 3-tier approach to application uptime means your applications are up and running with 5-nines reliability. The first tier is a server or application failure. If a server or application fails or becomes overloaded, FortiADC routes traffic automatically to healthy servers. For the second tier, FortiADC supports failover options to cover you should a FortiADC go down. Finally, the third level provides routing to an alternate data center(s) should your primary data center suffer a catastrophic or planned event.

FortiADC supports Active/Passive, Active/Active, N+1 or N+M failover configurations. FortiADC's Multi-Active N+M Failover allows a cluster of active FortiADCs to share the workload for a large application data center. Instead of requiring idle spares in standby mode as in other failover methods, Multi-Active N+M Failover puts all the FortiADCs to work load balancing and delivering applications. If a FortiADC in the N+M cluster should fail, the others seamlessly pick up the workload until you or your team can get the failed FortiADC back online.

Features and Benefits

- Intelligent traffic management for optimized application delivery and availability.
- Server offloading for improved application acceleration, scale and TCO.
- SSL offload for accelerating application performance.
- Comprehensive server load balancing for 99.999% application uptime.
- Global Server Load Balancing for geographic resilience.
- Smart Control Automation for virtual and physical resource control.
- Optimize WAN connectivity and ensure business continuity with Link Load Balancing.
- Accelerate content delivery with on the fly compression.
- Browser-based Web user interface for ease of management.

HIGHLIGHTS

Disaster Recovery with Global Server Load Balancing

FortiADC's included Global Server Load Balancing (GSLB) makes your network reliable and available by scaling applications across multiple data centers for disaster recovery or to improve application response times. Administrators can set up rules that direct traffic based on site availability, data center performance and network latency.

Advanced Networking Support

FortiADCs use Network Address Translation (NAT), Source NAT, Outbound NAT and spoofing to effectively and efficiently route traffic between clients and servers. With support for direct server return, Multi-Gateway and Multi-Netting, Link Aggregation (LACP), IPv6 routing, NTP and tagged VLAN support for up to 4094 802.1Q VLANs, you get the flexibility you need as your network topology evolves without having to buy new equipment.

Are you ready for the transition to IPv6? FortiADC can make it easier with 6in4 Tunneling supported on all FortiADCs. Through the use of a tunnel broker, you can assign IPv6 addresses to your server clusters making them available to any client on an IPv6 network.

FortiADC provides the ability to configure routing to match network topologies from the simplest to the very complex through Policy-based Routing. You can define routing behavior for each subnet, based on either destination IP address or source IP address of packets traversing FortiADC.

Link Load Balancing

Built-in Link Load Balancing gives you the option to connect your FortiADC to two or more WAN links to reduce the risk of outages or to add additional bandwidth to relieve traffic congestion. FortiADC supports inbound and outbound Link Load Balancing to manage traffic leaving or entering the device.

Blazing Fast SSL Offloading and Compression

All FortiADCs support SSL offloading to relieve your servers from the computational workload of SSL/TLS session negotiation, encryption and decryption, letting them instead focus on the applications they were meant to serve. Some models come equipped with hardware-based acceleration.

Not all applications were written with SSL in mind and many scale poorly when SSL is enabled. FortiADC's SSL offloading eliminates these problems with an easy to deploy acceleration solution. Processing is moved from your servers to FortiADC making applications significantly faster and secure without software or other intrusive changes.

FortiADC uses Gzip HTTP compression for content-rich applications. You can compress server generated data up to 5 times before it's delivered to a client using any modern web browser saving you bandwidth costs and improving response times to your users.

Automate Routine Tasks to Take Control of Your Applications

FortiADC's Smart Control framework with Smart Control Automation manages notifications, logging and corrections to your application environments. Intuitive construction of graphical or CLI-based rule sets let you configure responses to almost any condition including resource management to power up or power down IPMI-compliant servers in response to changes in demand.

Virtual Platform Support

If you're looking for a comprehensive set of tools to manage your VMware environment, FortiADC has you covered. Every FortiADC supports VMware load balancing using VMware's management API to retrieve real-time virtual server availability and resource utilization from a VMware vCenter console. With FortiADC's Smart Control Automation you get even deeper integration into VMware with the ability to load balance based on VM CPU and VM RAM and spin-up or spin-down VMs in response to demand.

Guaranteed Application Support

From basic static websites to enterprise Microsoft® Exchange installations, FortiADC can support virtually any internet-based application. Easy to follow deployment guides are available for the top Microsoft® applications including Exchange 2010 and 2013.

Enhanced Protection with IP Reputation Service

Attackers use many methods to infect and control devices to launch automated phishing, spamming, and DDoS attacks. The FortiGuard IP Reputation Service aggregates security data from around the world to provide up-to-date information about threatening sources. With feeds from distributed network gateways combined with world-class research done by FortiGuard Labs, organizations can stay up to date and proactively block attacks.

FortiGuard's IP Reputation Service categorizes and blocks threats from sources associated with:

- DoS and DDoS attacks
- Phishing attacks or hosted Phishing web sites
- Anonymous traffic arriving from paid or anonymous proxies used to disguise real client identity
- Malicious software
- Spammers
- Command and control communication

Flexible Management and Comprehensive Reporting

Do you prefer a command line or an intuitive graphical user interface? Either way FortiADC provides the tools you need to easily manage your device. The context-sensitive CLI provides complete control of every aspect of your FortiADC, not just

a subset of functions like some other manufacturers. Even if you're a CLI-jockey, you'll appreciate the thought-through layout and features of our graphical user interface for most tasks from setting up server pools to running sophisticated traffic reports. If you'd rather manage your FortiADC from another device or application, FortiADC's REST API gives you the flexibility you need.

FortiADC's Role-based Management lets you easily establish multiple users and groups allowing it to be managed by one or more data center personnel. As the administrator, you can assign read, write, create and delete permissions to individual users or groups to give as little or as much control over your FortiADC to fit the needs of your organization.

FEATURES

Application Availability

Intelligent and easy to configure Layer 4/7 policy and group management

- Virtual service definition with inherited persistence, load balancing method and pool members
- Static, default and backup policies and groups
- Layer 4/7 application routing policy
- Layer 4/7 server persistence
- Application load balancing based on round robin, weighted round robin, least connections, shortest response
- Granular real server control including warm up rate limiting and maintenance mode with session ramp down

Layer 4 Application Load Balancing

- TCP, UDP protocols supported
- Round robin, weighted round robin, least connections, shortest response
- Persistent IP, hash IP/port, hash header, persistent cookie, hash cookie
- RADIUS, DNS servers support

Layer 7 Application Load Balancing

- HTTP/HTTPS/FTP/RADIUS supported
- L7 content switching
  - HTTP Host, HTTP Request URL, HTTP Referrer
  - Source IP Address
- URL redirect, HTTP request/response rewrite
- 403 Forbidden Rewrite

Link Load Balancing

- Inbound and outbound LLB
- Multiple health check target support
- Configurable intervals, retries and timeouts

Global Server Load Balancing (GSLB)

- Global datacenter DNS based failover of web applications
- Delivers local and global load balancing between multi-site SSL VPN deployments

Deployment Modes

- Configurable proxy (NAT) or transparent (direct) mode per VIP
- X-Forwarded for configuration in proxy mode

High Availability

- Active/Passive Failover
- Active/Active Failover
- N+M Failover

Application Acceleration

SSL Offloading and Acceleration

- Offloads HTTPS processing while securing sensitive data

TCP Acceleration

- Connection pooling and multiplexing
- TCP buffering
- Client connection persistence
- HTTP Compression

Networking

- NAT for maximum flexibility and scalability
- VLAN and port trunking support
- IP Reputation (subscription required)

IPv6 Support

- IPv6 routing
- Full IPv6 Management
- IPv6 Layer 7 Services
- 6in4 Tunneling

Management

- Single point of cluster management
- CLI Interface for configuration and monitoring
- Secure SSH remote network management
- Secure Web UI access
- SNMP with private MIBs
- Syslog support
- Role-based administration
- In-build diagnostic utilities
- Real-time monitoring graphs
- Smart Control Automation
- REST API

FortiADC 300E

FortiADC 400E

FortiADC 600E

FortiADC 1000E

SPECIFICATIONS

	FORTIADC 300E	FORTIADC 400E	FORTIADC 600E	FORTIADC 1000E
Hardware Specifications				
L4 Throughput	4.8 Gbps	8.0 Gbps	13.0 Gbps	18.0 Gbps
L7 TPS	200,000	220,000	280,000	450,000
SSL TPS (2048 keys)	6,500	24,000	33,000	46,000
Compression Throughput	640 Mbps	1.8 Gbps	4.6 Gbps	5.8 Gbps
Memory	2 GB	2 GB	4 GB	4 GB
Network Interfaces	6x GE RJ45	8x GE RJ45	2x 10 GbE SFP+ slots, 8x GE ports	2x 10 GbE SFP+ slots, 8x GE ports
Storage	120 GB SSD	120 GB SSD	120 GB SSD	120 GB SSD
Management	HTTPS, SSH, CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH, CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH, CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH, CLI, Direct Console DB9 CLI, SNMP
10/100/1000 Management Interface	–	–	1	1
Power Supply	Single	Single	Single	Dual
Environment				
Form Factor	1RU	1RU	1RU	1RU
Input Voltage	90–264V AC, 47–63 Hz	100–240V AC, 50–60 Hz	110–240V AC, 50–60 Hz	111–240V AC, 50–60 Hz
Power Consumption (Average)	66 W	121.6 W	108 W	120 W
Maximum Current	100V/4A, 240V/2A	100V/4A, 240V/2A	110V/5A, 240V/2.5A	110V/10A, 240V/5A
Heat Dissipation	273 BTU/h	498 BTU/h	478 BTU/h	1,044 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)
Humidity	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing
Compliance				
Regulatory Compliance	FCC Part 15 Class A, C-tick, VCCI, CE, UL/c	FCC Part 15 Class A, C-tick, VCCI, CE, BSMI, UL/cUL, CB	FCC Part 15 Class A, C-tick, VCCI, CE, UL/c	FCC Part 15 Class A, C-tick, VCCI, CE, UL/c
Safety	CSA, C/US, CE, UL	CSA, C/US, CE, UL	CSA, C/US, CE, UL	CSA, C/US, CE, UL
Dimensions				
Height x Width x Length (inches)	1.75 x 17.05 x 13.86	1.73 x 17.32 x 16.22	1.75 x 17.25 x 18.25	1.75 x 17.25 x 21.00
Height x Width x Length (mm)	45 x 433 x 352	44 x 440 x 412	45 x 438 x 464	46 x 438 x 534
Weight	12.45 lbs (5.65 kg)	13.78 lbs (6.25 kg)	15.50 lbs. (7.0 kg)	18.0 lbs. (8.2 kg)

ORDER INFORMATION

Product	SKU	Description
FortiADC 300E	FAD-300E	FortiADC 300E, 6x GE ports, 1x 120 GB SSD storage.
FortiADC 400E	FAD-400E	FortiADC 400E, 8x GE ports, 1x 120 GB SSD onboard storage.
FortiADC 600E	FAD-600E	FortiADC 600E, 2x 10 GbE SFP+ slots, 8x GE ports, 1x 120 GB SSD onboard storage.
FortiADC 1000E	FAD-1000E	FortiADC 1000E, 2x 10 GbE SFP+ slots, 8x GE ports, 1x 120 GB SSD onboard storage.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480