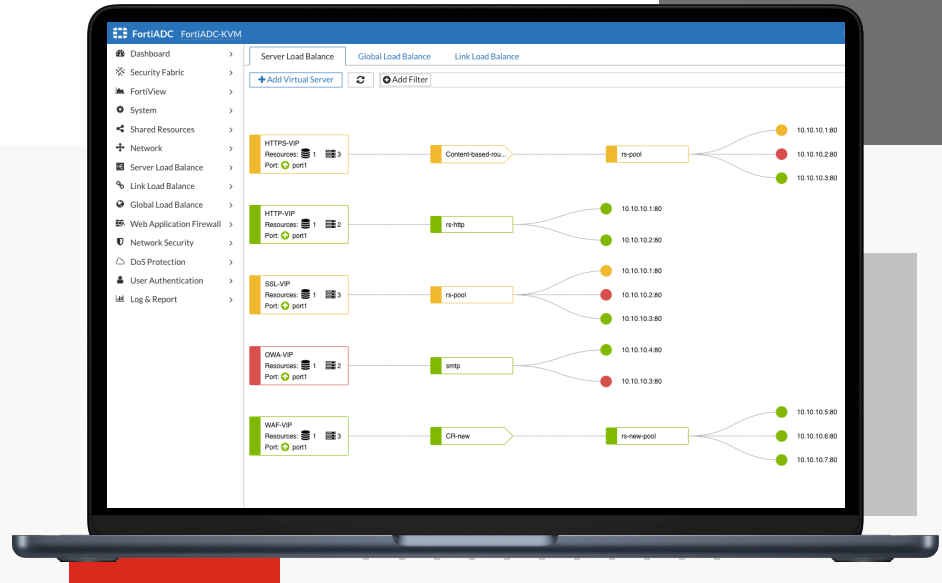


FortiADC™

Advanced Application Delivery Controller



Highlights

- Advanced Application Load Balancing
- Protection from the OWASP Top 10 - 2021 application attacks
- Multi-Deployment Mode with Hardware, VM, or Cloud Solution (PAYG/ BYOL)
- SSL Security and Visibility with Hardware-based Solution
- Automation and Fabric Connector to Third Party Solutions such as SAP, Cisco ACI, AWS, and K8s
- User Authentication and Authorization via MFA and SSO
- FortiGSLB Cloud Integration Maximizes Service Availability

Application Anywhere

FortiADC is an advanced Application Delivery Controller (ADC) that ensures application availability, application security, and application optimization. FortiADC offers advanced security features (WAF, DDoS, and AV) and application connectors for easy deployment and full visibility to your networks and applications. FortiADC can be deployed as a physical or virtual machine (VM), or as a Cloud solution.

Application Availability

24x7 application availability through automatic failover for business continuity with application automation, global server load balancing, and link load balancing to optimize WAN connectivity.

Application Optimization

Multi-core processor technology combined with hardware-based SSL offloading and server optimization to increase end-user QoE.

Application Protection

Advanced Web Application Firewall protection from the OWASP Top 10 - 2021 and threat detection with Fortinet FortiGuard Cloud Services.

Zero Trust Application Gateway

ZTNA (ZTAG) provides an automatic, encrypted tunnels for controlled validated per-session access to applications

Available in



Appliance



Virtual



Hosted



Cloud



FortiFlex

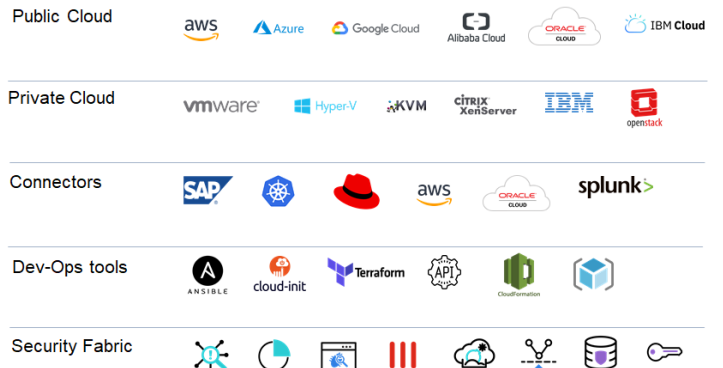
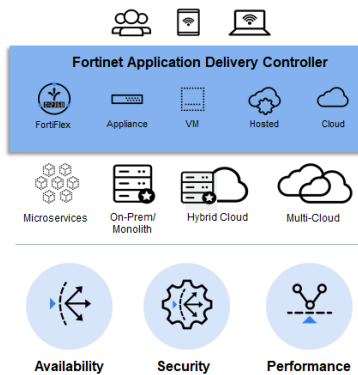


FortiCare Worldwide
24/7 Support
support.fortinet.com



FortiGuard Security Services
www.fortiguards.com

FortiADC Services



Highlights

Application Availability

Applications are the lifeblood of a company's online presence. Unresponsive applications can result in lost revenue and customers taking their future business elsewhere. Application performance, scalability, and resilience are key but none of this matters unless the end-user has a good experience and completes their transaction.

FortiADC is a dedicated Application Delivery Control solution that provides a multi-tenancy solution (VDOM), high availability, and scalability with hybrid solution deployment (on-premises and cloud offering) to your applications.

SSL Security

FortiADC delivers high capacity decryption and encryption with the latest cryptography standard using hardware-based SSL ASIC. FortiADC provides SSL offloading, SSL inspection and visibility to inspect traffic for threats, speeds up server response, and reduces the load on the backend server. FortiADC also integrates with Gemalto's SafeNet Enterprise Hardware Security Module (HSM).

Business Continuity

FortiADC's included Global Server Load Balancing (GSLB) module on-prem or in the cloud (FortiGSLB Cloud) makes your network reliable and available by scaling applications across multiple data centers for disaster recovery or to improve application response times. Customers can set up rules based on site availability, data center performance, and network latency.



Highlights

Application Protection

FortiADC offers multiple levels of protection to defend against attacks that target your web applications. FortiADC Web Application Firewall can detect a zero day attack and protect from **OWASP Top 10 - 2021** and many other threats with multi-vector protection. FortiADC also supports our FortiGuard Cloud which provides multi services such as IPS, Antivirus, and IP Reputation service (subscription required) that protects you from sources associated with DoS/DDoS attacks, phishing schemes, spammers, malicious software, and botnets.

Application Optimization

FortiADC provides multiple services that speed the delivery of applications to users. The PageSpeed suite of website performance enhancement tools can automatically optimize HTTP, CSS, Javascript, and image delivery to application users. FortiADC also provides Dynamic Caching and HTTP Compression and Decompression to improve end-user experience and server productivity.

FortiADC Security Fabric

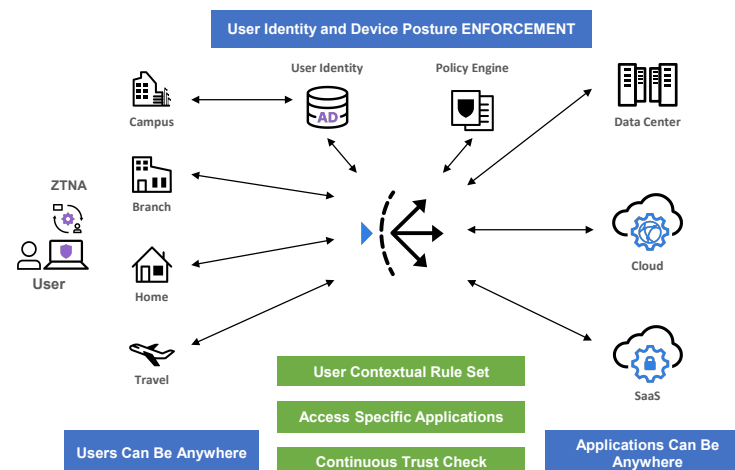
As the threat landscape evolves, many new risks require a multi-pronged approach for protecting applications. FortiADC's antivirus and integration with FortiSandbox extend basic security protections to scan file attachments for known and unknown threats.

Automation and Connectors

FortiADC Fabric Connectors provide open API-based integration and orchestration with multiple software-defined networks (SDN), cloud, management, and partner technology platforms. Fortinet Fabric Connectors deliver turnkey, open, and deep integration into third party services such as K8s, AWS, OCI, and SAP, in multi-vendor ecosystems, enabling scalability, security automation, and simplified management.

Zero Trust Application Gateway (ZTNA)

FortiClient ZTNA works with FortiADC to enable secure granular access to applications no matter if the user is local or remote. Each session is initiated with an automatic, encrypted tunnel from FortiClient to the FortiADC for user and device verification. If verified, access is granted for that session. You can also use multifactor authentication to provide an additional layer of security. With ZTNA, organizations benefit from both a better remote access solution and a consistent policy for controlled access to applications irrespective of endpoint location.



Highlights

Unleash the Power of Scripts

FortiADC Scripts provides the flexibility to create custom event-driven rules using predefined commands, variables, and operators. Using easy-to-create scripts, you get the flexibility you need to extend your FortiADC with specialized business rules that give you almost unlimited possibilities for server load balancing, health checks, application validation, content routing, and content rewriting to meet the needs of your organization.

Application Authentication

FortiADC provides centralized user authentication and authorization services to web applications. FortiADC acts as a gatekeeper to offload HTTP authentication and authorization to customer applications using single sign-on (SSO) services, SAML, LDAP, RADIUS, and MFA (using FortiToken Cloud and Google authenticator).

WAN Optimization

FortiADC provides a built-in link optimization with the Link Load Balancing module. Customers can create two or more WAN links (for inbound and outbound Link LB) to reduce the risk of outages or to add additional bandwidth to relieve traffic congestion.

Analytics and Visibility

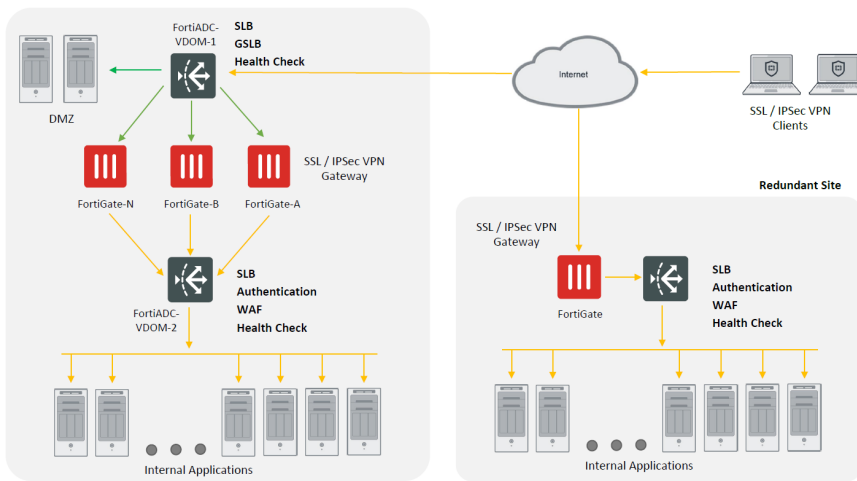
FortiADC offers a comprehensive monitoring system for your network and application. With FortiView, customers can get real-time and historical data into a single view on your FortiADC. We also provide a network logical topology of real-servers, user/application data-analytics, security threats, attack maps, and some other system events and alerts. FortiADC is integrated with third party solutions such as Splunk, FortiAnalyzer, and FortiSIEM for more visibility, correlation, automated response, and remediation.

FortiADC Centralized Management

FortiADC Manager is a web-based management tool that allows you to centrally manage multiple FortiADC devices remotely. Network administrators can better control their devices by logically grouping devices, efficiently managing jobs and licenses, quickly checking various logs, and monitoring threat statistics in real time.

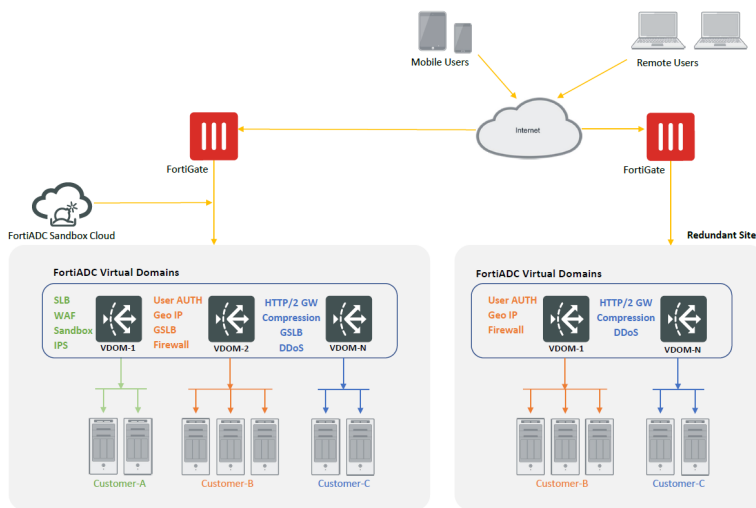


Use Cases



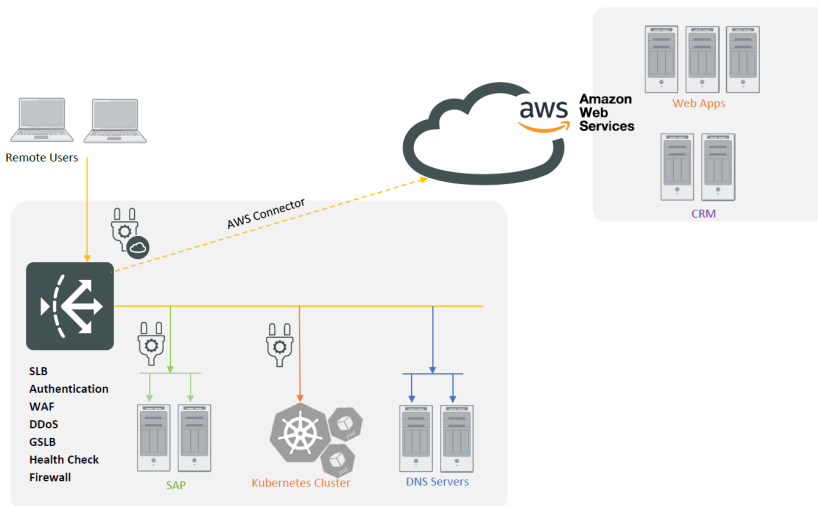
High Scale Performance with FortiADC and FortiGate (FWLB and SSL-VPN / IPSEC LB)

- Improved VPN performance and user QoE
- User redirection based on geolocation and round-trip time (RTT)
- Advanced health checks for applications and NGFW in improved site visibility and availability
- Application Load Balancing and WAF Protection



MSSP / SP Advanced Offering

- Fully virtualized environment
- Service tailored per customer (SLB, L7, GSLB, WAF, and Application Optimization)
- Can be managed via Single pane of glass (CM, API, and Cisco ACI)
- Fully managed services
- High redundancy



Hybrid Cloud Solution

- Cloud Connector for visibility and availability
- Fabric Connector to multiple applications for automation and service scaling
- Multi-Service solution (SLB, WAF, Authentication, and GSLB)



Features

Application Availability

- Virtual service definition with inherited persistence, load balancing method, and pool members
- Layer 4/7 application routing policy
- Layer 4/7 server persistence
- Custom scripting for SLB and content rewriting
- Scripting for event-driven rules using predefined commands, variables, and operators for SLB, content rewrite, persistence, and security
- Advanced L7 application health check with support script for a customized health check
- Clone Traffic Pools

Layer 4-7 Application Load Balancing

- TCP, UDP, IP, DNS, HTTP, HTTPS, HTTP3 (QUIC), HTTP 2.0 GW, FTP, SIP, RDP, RADIUS, MySQL, MSSQL, RTMP, RTSP, and more applications
- L7 Content Switching and Rewriting
 - HTTP Host, HTTP Request URL, and HTTP Referrer
 - Source IP Address
- Persistent IP, has IP/port, hash header, persistent cookie, hash cookie, destination IP hash, URI hash, full URI hash, host hash, and host domain hash
- URL Redirect, HTTP request/response rewrite (includes HTTP body)
- Layer 7 DNS load balancing, security, and caching

Link Load Balancing

- Inbound and outbound LLB
- Support for policy route and SNAT
- Multiple health check target support
- Configurable intervals, retries, and timeouts
- Tunnel Routing

Security Fabric Connector

- FortiGSLB Cloud (One-Click-GSLB)
- FortiAuthentication
- FortiSIEM
- FortiAnalyzer
- FortiADC-CM
- FortiSandbox
- FortiGate BanIP Integration

External Fabric Connectors

- Kubernetes Service
- SAP Application
- AWS / OCI Connector
- Splunk Integration

Global Server Load Balancing (GSLB)

- Global data center DNS-based failover of web applications
- Delivers local and global load balancing between multi-site SSL VPN deployments
- DNSSEC
- DNS Access Control Lists
- GSLB setup wizard

Deployment Modes

- One arm-mode (Proxy with X-forwarded for support)
- Router mode
- Transparent mode (switch)
- High Availability (AA/AP Failover)

Web Application Firewall

Application Protection

- OWASP Top-10 Wizard
- Web Attack Signature
- API Protection
- Sensitive Data Protection
- Bot Detection
- Web Vulnerability Scanner
- Third-party scanner integration (virtual patching)
- HTTP RFC compliance

Security Services

- SQLi/XSS Injection Detection
- OpenAPI Validation
- API Gateway
- API Discovery and Protection
- Web Scraping
- CSRF Protection
- Brute Force Protection
- Web Defacement Protection
- CAPTCHA Support
- Data Leak Prevention
- File Restriction
- Cookie Security
- XML/JSON/SOAP Validation
- HTTP Header Security

Bot Protection

- Threshold-based Protection
- Biometric Protection
- Crawler Detection
- Fingerprint Detection



Features

Application Acceleration

SSL Offloading and Acceleration

- Offloads HTTPS and TCPS processing while securing sensitive data
- Full certificate management features
- HTTP/S mirroring for traffic analyses and reporting
- Support TLS 1.3

HTTP and TCP Optimization

- 100x acceleration by off-loading TCP processing
- Connection pooling and multiplexing for HTTP and HTTPS
- HTTP Page Speed-UP for Web Server Optimization
- TCP buffering
- HTTP compression and decompression
- HTTP caching (static and dynamic objects)
- Bandwidth allocation with Quality of Service (QoS)

Authentication Offloading

- Local
- LDAP
- RADIUS
- Kerberos
- SAML 2.0 (SP and Idp)
- AUTH2.0
- NTLM
- Two-Factor Authentication — FortiToken/ FortiToken Cloud, and Google Authentication

Networking

- Static NAT, Hide NAT, and Dynamic NAT for flexibility and scalability)
- VLAN and port trunking support
- Support integration with Cisco ACI, Nutanix, OpenStack, and Ansible
- NVGRE and VXLAN Support
- BGP and OSPF with Route Health Inspection (RHI)
- IPv6 Support (SLB, interfaces, routing, and firewall)
- Support SR-IOV - VMware and KVM

Application Security

- FortiGuard Antivirus and FortiSandbox integration
- GEO IP security and logs (subscription required)
- Stateful Firewall
- Web Filtering (subscription required)
- IP Reputation (subscription required)
- IPv4 and six firewall rules
- Granular policy-based connection limiting
- Syn cookie protection
- Connection limits
- Intrusion Prevention System (subscription required)
- Application and Network DDoS Protection
- DNS Application Security
- ACME Support

Management

- Central management for multiple FortiADC devices
- SNMP with private MIBs with threshold-based traps
- Real-time Data Analytics
- Syslog support
- Role-based administration
- Real-time monitoring graphs
- Built-in reporting
- FortiView integration
- OWASP Top-10 Real-time monitoring
- Data analytics
- Virtual Domains (VDOMs)
- Support Inter-VDOM Connectivity

DevOps Tools

- RestFUL API
- Declarative and Imperative API
- Terraform
- Ansible
- Cloud.init



Specifications

	FortiADC 120F	FortiADC 220F
System Performance		
L4/L7 Throughput	3 Gbps / 2.2 Gbps	5 Gbps / 4 Gbps
L4 CPS	80 000	160 000
L4 HTTP RPS	230 000	500 000
Maximum L4 Concurrent Connection	4.5 M	6 M
L7 CPS (1:1) *	20 000	40 000
SSL CPS/TPS (1:1) 2K keys **	500	1200
SSL Bulk Encryption Throughput	500 Mbps	1.2 Gbps
Compression Throughput	1.3 Gbps	2 Gbps
SSL Acceleration Technology	Software	Software
Virtual Domains	10	10
Hardware Specifications		
Memory	8 GB	8 GB
Network Interfaces	6x GE RJ45	4x GE RJ45, 4x GE SFP
10/100/1000 Management Interface	—	—
Storage	64 GB SSD	120 GB SSD
Management	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP
Power Supply	Single	Single
Simultaneous Sources (M)	1U	1U
Trusted Platform Module	Yes	Yes
Dimensions		
Height x Width x Length (inches)	1.75 x 17.3 x 10.55	1.73 x 17.24 x 16.38
Height x Width x Length (mm)	44 x 440 x 268	44 x 438 x 416
Weight	9.9 lbs (4.5 kg)	22 lb (9.07 kg)
Environment		
Form Factor	1U Appliance	1U Appliance
Input Voltage	100–240V AC, 50–60 Hz	100–240V AC, 50–60Hz
Power Consumption (Average / Maximum)	40 W / 60 W	80W
Maximum Current	100V / 1.5A, 240V / 0.6A	100V/6A, 240V/3A
Heat Dissipation	132–163 BTU/h	273 BTU/h
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-4°–167°F (-20°–75°C)	-4°–167°F (-20°–75°C)
Humidity	10%–85% relative humidity, non-operating, non-condensing	5%–95% non-condensing
Forced Airflow	Front to Back	Front to Back
Compliance		
Regulatory Compliance	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/c	
Safety	CSA, C/US, CE, UL	



All performance values are “up to” and vary depending on the system configuration.

** Layer 7 CPS — measures number of new HTTP connections (1 HTTP request per TCP connection)

** Tested with 1 HTTP request per SSL connection; SSL Ciphers=AES256-SHA; 2K Keys



Specifications

	FortiADC 300F	FortiADC 400F	FortiADC 1200F/-DC
System Performance			
L4/L7 Throughput	8 Gbps	15 Gbps / 12 Gbps	40 Gbps / 30 Gbps
L4 CPS	300 000	400 000	1 000 000
L4 HTTP RPS	1M	1.5M	3 000 000
Maximum L4 Concurrent Connection	12M	12M	36 000 000
L7 CPS (1:1) *	100 000	120 000	220 000
SSL CPS/TPS (1:1) 2K keys **	4000	15 000	35 000
SSL Bulk Encryption Throughput	3 Gbps	6 Gbps	20 Gbps
Compression Throughput	6 Gbps	10 Gbps	20 Gbps
SSL Acceleration Technology	Software	ASIC	ASIC
Virtual Domains	10	20	45
Hardware Specifications			
Memory	16 GB	32 GB	32 GB
Network Interfaces	4x GE RJ45, 4x GE SFP	2x 10 GE SFP+, 4x GE SFP, 4x GE RJ45	8x RJ45 GE port, 8x SFP GE port, 8x SFP+ 10G Ports
10/100/1000 Management Interface	—	—	2
Storage	128 GB SSD	120 GB SSD	240 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
Power Supply	Single	Single (support hot-swap PSU)	Dual (support hot-swap PSU)
Trusted Platform Module (TPM)	No	No	Yes
Dimensions			
Height x Width x Length (inches)	1.73 × 17.24 × 16.38	1.73 × 17.24 × 16.38	1.73 × 21.5 × 17.3
Height x Width x Length (mm)	44 × 438 × 416	44 × 438 × 416	44 × 548 × 440
Weight	20 lbs (9.07 kg)	20 lbs (9.07 kg)	22.5 lbs (10.2 kg)
Environment			
Form Factor	1U Appliance	1U Appliance	1U Appliance
Input Voltage	100–240V AC, 50–60 Hz, 5-3A	100–240V AC, 50–60 Hz, 5-3A	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	90 W / 99 W	114 W / 137 W	251 W / 320 W
Maximum Current	100–240V AC / 6-3A, 50/60 Hz	100–240V AC, 50–60 Hz, 5-3A	120V / 7.1A, 240V / 3.5A
DC Power Supply	—	—	TBA
Heat Dissipation	337.8 BTU/h	467.4 BTU/h	856 BTU/h
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-13°–167°F (-25°–75°C)	-13°–167°F (-25°–75°C)	-4°–167°F (-20°–75°C)
Humidity	5%–95% non-condensing	5%–95% non-condensing	10%–85% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back
Compliance			
Regulatory Compliance	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/c		
Safety	CSA, C/US, CE, UL		



All performance values are “up to” and vary depending on the system configuration.

** Layer 7 CPS — measures number of new HTTP connections (1 HTTP request per TCP connection)

** Tested with 1 HTTP request per SSL connection; SSL Ciphers=AES256-SHA; 2K Keys

Specifications

	FortiADC 2200F/-DC	FortiADC 4200F/-DC	FortiADC 5000F
System Performance			
L4/L7 Throughput	60 Gbps / 35 Gbps	100 Gbps / 80 Gbps	250 Gbps / 220 Gbps
L4 CPS	1 200 000	1 800 000	4M
L4 HTTP RPS	4 000 000	5 000 000	18 000 000
Maximum L4 Concurrent Connection	72 000 000	144 000 000	160 000 000
L7 CPS (1:1) *	280 000	500 000	1 100 000
SSL CPS/TPS (1:1) 2K keys **	40 000	60 000	100 000
SSL Bulk Encryption Throughput	25 Gbps	50 Gbps	120 Gbps
Compression Throughput	22 Gbps	45 Gbps	150 Gbps
SSL Acceleration Technology	ASIC	ASIC	ASIC
Virtual Domains	60	90	90
Hardware Specifications			
Memory	64 GB	128 GB	384 GB
Network Interfaces	8x SFP ports, 12x 10GbE SFP+ ports	4x 40GbE QSFP, 8x 10G SFP+	4x 100 GE QSFP28, 8x 40 GE QSFP
10/100/1000 Management Interface	2	2	1
Storage	240 GB SSD	480 GB SSD	3.74 TB 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
Power Supply	Dual (support hot-swap PSU)	Dual (support hot-swap PSU)	Dual (support hot-swap PSU)
Trusted Platform Module (TPM)	Yes	Yes	No
Dimensions			
Height x Width x Length (inches)	1.73 x 21.5 x 17.3	3.46 x 21.5 x 17.3	3.4 x 17.2 x 30.2
Height x Width x Length (mm)	44 x 548 x 440	88 x 548 x 440	80.6 x 436.9 x 777.2
Weight	22.5 lbs (10.2 kg)	29.3 lbs (13.3 kg)	68.3 lbs (31 kg)
Environment			
Form Factor	1U Appliance	2U Appliance	2U Appliance
Input Voltage	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	220–240V AC
Power Consumption (Average / Maximum)	267 W / 340 W	269 W / 360 W	1120 W / 2200 W
Maximum Current	100V / 7A, 240V / 3.5A	100V / 7A, 240V / 3.5A	120V / 11.8A, 240V / 9.6A
DC Power Supply	TBA	TBA	—
Heat Dissipation	911 BTU/h	917 BTU/h	7506 BTU/hr
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	50°–95°F (10°–35°C)
Storage Temperature	-4°–167°F (-20°–75°C)	-4°–167°F (-20°–75°C)	-40°–140°F (-40°–60°C)
Humidity	10%–85% non-condensing	10%–85% non-condensing	8%–90% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back
Compliance			
Regulatory Compliance	FCC/ ICES, CE, RCM, VCCI, BSMI	FCC/ ICES, CE, RCM, VCCI, BSMI	CE, FCC, RCM, VCCI, BSMI
Safety	UL/ cUL, CB	UL/ cUL, CB	UL, CB, IEC



All performance values are “up to” and vary depending on the system configuration.

** Layer 7 CPS — measures number of new HTTP connections (1 HTTP request per TCP connection)

** Tested with 1 HTTP request per SSL connection; SSL Ciphers=AES256-SHA; 2K Keys



Specifications

	FORTIADC-VM01	FORTIADC-VM02	FORTIADC-VM04	FORTIADC-VM08	FORTIADC-VM16	FORTIADC-VM32
Hardware Specifications						
Hypervisor Support	VMware ESX/ESXi, Citrix XenServer, Open Source Xen, Microsoft Hyper-V, KVM, AWS, Azure, Google Cloud, Oracle Cloud. Please see the FortiADC-VM Install Guide for the latest hypervisor versions supported.					
L4 Throughput*	1 Gbps	2 Gbps	4 Gbps	10 Gbps	16 Gbps	24 Gbps
Virtual Domains	10	10	10	10	15	20
vCPU Support (Maximum)	1	2	4	8	16	32
Memory Support (Maximum)	Unlimited					
Network Interface Support (Maximum)	10	10	10	10	10	10
Storage Support (Minimum / Maximum)	Unlimited					
Throughput	Hardware Dependent					
Management	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP					

* Actual performance values may vary depending on the network traffic and system configuration. Performance results were observed using an appliance with an Intel CPU E5-1650 v2 @ 3.50 GHz running VMware ESXi 5.5.



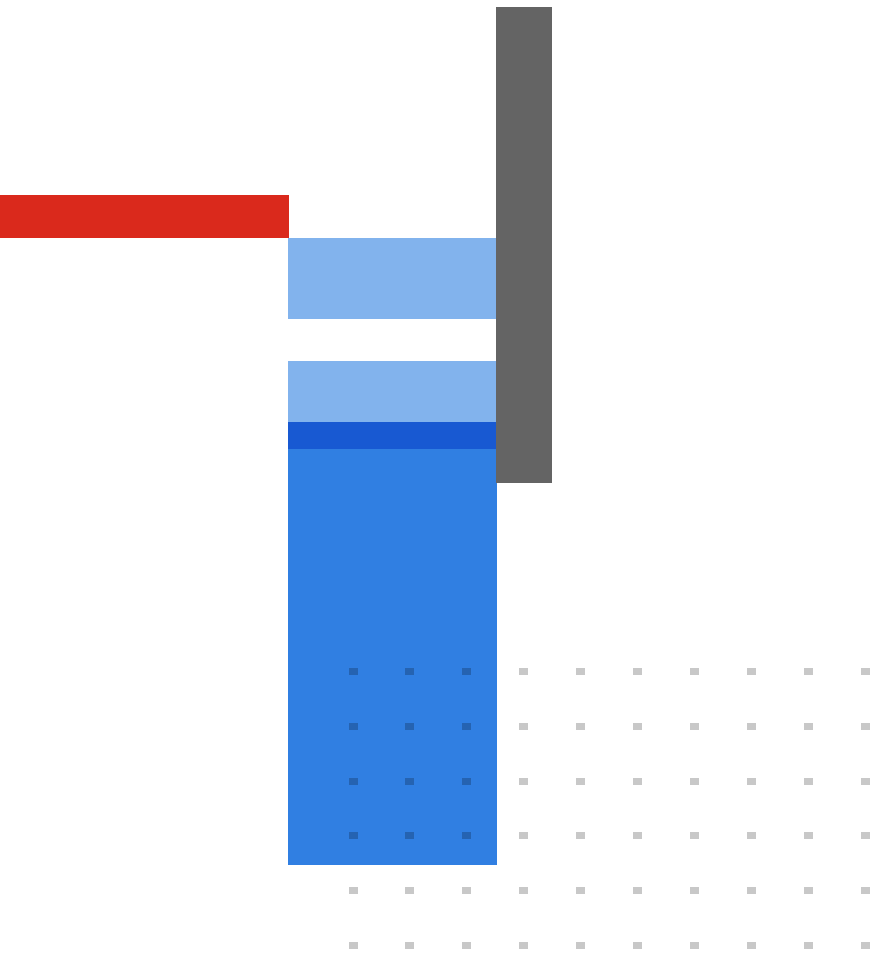
Ordering Information

Product	SKU	Description
FortiADC 120F	FAD-120F	FortiADC 120F, 6x GE ports, 1x64 SSD storage.
FortiADC 220F	FAD 220F	FortiADC 220F, 4x GE RJ45 ports, 4x GE SFP ports, 1x 120 GB SSD storage.
FortiADC 300F	FAD-300F	FortiADC 300F, 4x GE RJ45 ports, 4x GE SFP ports, 2x GE management ports, 1x 128 GB SSD storage.
FortiADC 400F	FAD-400F	FortiADC 400F, 4x GE RJ45 ports, 4x GE SFP ports, 2x 10 GE SFP+ ports, 2x management ports, 1x 120 GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU.
FortiADC 1200F	FAD-1200F	FortiADC 1200F, 8x 10 GE SFP+ ports, 8x GE SFP ports, 8x GE RJ45 ports, 2x GE RJ45 management port, 1x 240 GB SSD, dual AC power supplies.
FortiADC 1200F-DC	FAD-1200F-DC	FortiADC 1200F, 8x 10 GE SFP+ ports, 8x GE SFP ports, 8x GE RJ45 ports, 2x GE RJ45 management port, 1x 240 GB SSD, dual DC power supplies.
FortiADC 2200F	FAD-2200F	FortiADC 2200F, 12x 10 GE SFP+ ports, 8x GE SFP ports, 2x GE RJ45 management port, 1x 240 GB SSD, dual AC power supplies.
FortiADC 2200F-DC	FAD-2200F-DC	FortiADC 2200F, 12x 10 GE SFP+ ports, 8x GE SFP ports, 2x GE RJ45 management port, 1x 240 GB SSD, dual DC power supplies.
FortiADC 4200F	FAD-4200F	FortiADC 4200F, 4x 40 GbE QSFP+, 8x 10 GbE SFP+, 2x GbE RJ45 management port, 1x 480 GB SSD, dual AC power supplies.
FortiADC 4200F-DC	FAD-4200F-DC	FortiADC 4200F, 4x 40 GbE QSFP+, 8x 10 GbE SFP+, 2x GbE RJ45 management port, 1x 480 GB SSD, dual DC power supplies.
FortiADC 5000F	FAD-5000F	FortiADC 5000F, 4x 100 GE QSFP28, 8x 40 GE QSFP, 1x GE RJ45 management port, 1x 3.74 TB SSD, dual AC power supplies.
FortiADC-VM01	FAD-VM01	FortiADC-VM software virtual appliance. Supports up to 1x vCPU core.
FortiADC-VM02	FAD-VM02	FortiADC-VM software virtual appliance. Supports up to 2x vCPU cores.
FortiADC-VM04	FAD-VM04	FortiADC-VM software virtual appliance. Supports up to 4x vCPU cores.
FortiADC-VM08	FAD-VM08	FortiADC-VM software virtual appliance. Supports up to 8x vCPU cores.
FortiADC-VM16	FAD-VM16	FortiADC-VM software virtual appliance. Supports up to 16x vCPU cores.
FortiADC-VM32	FAD-VM32	FortiADC-VM software virtual appliance. Supports up to 32x vCPU cores.
Central Manager 10	FAD-CM-BASE	FortiADC Central Manager license key, manage up to 10 FortiADC devices, VMware vSphere.
Central Manager Unlimited	FAD-CM-UL	FortiADC Central Manager license key, manage unlimited number of FortiADC devices, VMware vSphere.
Optional Accessory	SKU	Description
FortiADC 400F Redundant Power Supply	SP-FAD400F-PS	AC power supply for FAD-400F.
VM Subscriptions	SKU	Description
FortiADC-VM01-S Standard	FC1-10-ADVMS-942-02-DD	Subscription license for FortiADC-VM (1 CPU) with Standard bundle. 24x7 FortiCare support included.
FortiADC-VM01-S Advanced	FC1-10-ADVMS-635-02-DD	Subscription license for FortiADC-VM (1 CPU) with Advanced bundle. 24x7 FortiCare support included.
FortiADC-VM02-S Standard	FC2-10-ADVMS-942-02-DD	Subscription license for FortiADC-VM (2 CPU) with Standard bundle. 24x7 FortiCare support included.
FortiADC-VM02-S Advanced	FC2-10-ADVMS-635-02-DD	Subscription license for FortiADC-VM (2 CPU) with Advanced bundle. 24x7 FortiCare support included.
FortiADC-VM04-S Standard	FC3-10-ADVMS-942-02-DD	Subscription license for FortiADC-VM (4 CPU) with Standard bundle. 24x7 FortiCare support included.
FortiADC-VM04-S Advanced	FC3-10-ADVMS-635-02-DD	Subscription license for FortiADC-VM (4 CPU) with Advanced bundle. 24x7 FortiCare support included.
FortiADC-VM08-S Standard	FC4-10-ADVMS-942-02-DD	Subscription license for FortiADC-VM (8 CPU) with Standard bundle. 24x7 FortiCare support included.
FortiADC-VM08-S Advanced	FC4-10-ADVMS-635-02-DD	Subscription license for FortiADC-VM (8 CPU) with Advanced bundle. 24x7 FortiCare support included.
FortiADC-VM16-S Standard	FC5-10-ADVMS-942-02-DD	Subscription license for FortiADC-VM (16 CPU) with Standard bundle. 24x7 FortiCare support included.
FortiADC-VM16-S Advanced	FC5-10-ADVMS-635-02-DD	Subscription license for FortiADC-VM (16 CPU) with Advanced bundle. 24x7 FortiCare support included.
FortiADC-VM32-S Standard	FC6-10-ADVMS-942-02-DD	Subscription license for FortiADC-VM (32 CPU) with Standard bundle. 24x7 FortiCare support included.
FortiADC-VM32-S Advanced	FC6-10-ADVMS-635-02-DD	Subscription license for FortiADC-VM (32 CPU) with Advanced bundle. 24x7 FortiCare support included.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).





FORTINET

www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

September 19, 2023

FAD-DAT-R52-20230919