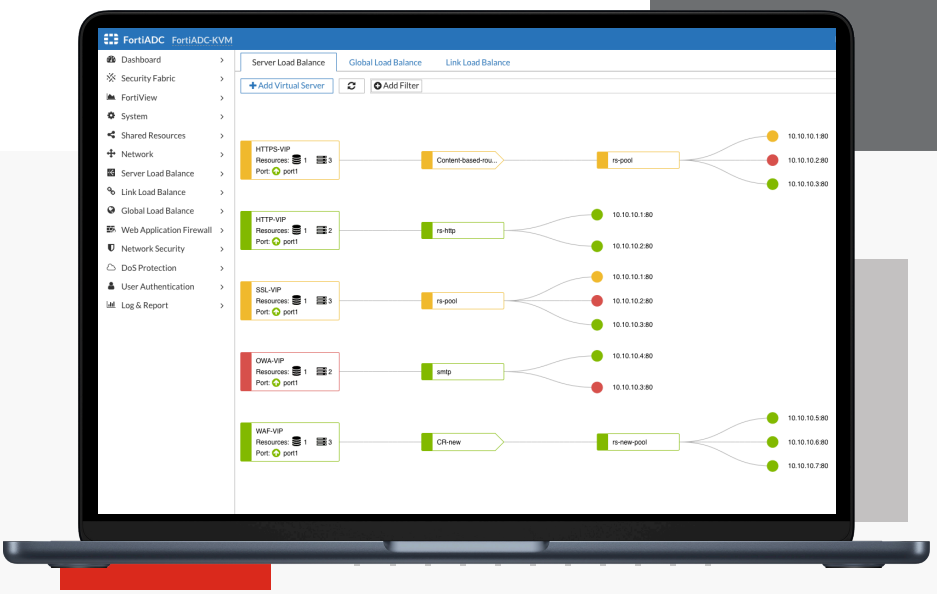
FortiADC™

Advanced Application Delivery Controller

Available in:

Appliance | Virtual Machine | Cloud | Hosted | FortiFlex



Highlights

- Advanced L4-L7 Application LB
- FortiGSLB cloud integration maximizes service availability
- AL (Adaptive Learning), and OWASP Top-10 protection and compliance with **web application firewall**
- Multi-deployment mode with hardware, VM, FortiFlex or Cloud providers (PAYG/BYOL)
- SSL security and visibility with hardware-based solution
- Automation and Fabric Connector to third party solutions such as K8s and OCP Ingress Controller, SAP, AWA and OCI
- User authentication and authorization via MFA and SSO
- Application anywhere with global server LB

Application Delivery with Security and Optimization

In recent years, the landscape of application delivery has undergone significant transformations influenced by evolving technology trends and the increasing adoption of cloud computing. Many organizations are integrating on-premises data centers with public cloud environments to optimize application performance, enhance scalability, and improve overall business agility.

Introduction

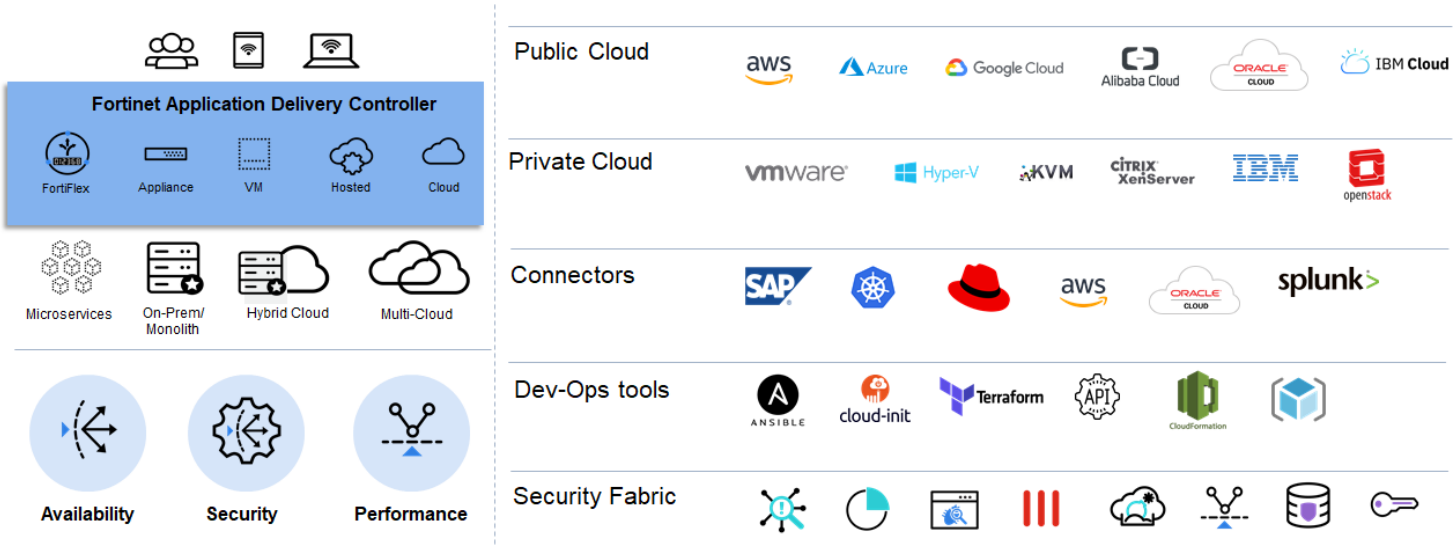
FortiADC, the advanced Application Delivery Controller (ADC), optimizes application delivery, enhances performance, and ensures application security whether hosted on-premises or in the cloud.

FortiADC offers robust L4-L7 load-balancing capabilities with Scripting support for content manipulation and Advanced SSL Services (Offloading and mirroring).

FortiADC also offers application acceleration, authentication, and built-in security features like Web Application Firewall protection for any application threats AL (Adaptive Learning), and OWASP Top10 Compliance Policy), DDoS Protection, ZTNA, and more.

With flexible deployment options (HW, VM, FortiFlex, and Cloud Providers) and integration into the Fortinet Security Fabric, FortiADC empowers businesses to deliver exceptional application experiences and security.

FortiADC Overview



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 and ADOM), high availability, and scalability with hybrid solution deployment (on-premises and cloud offering) to your applications.

Web Application Protection

FortiADC Web Application Firewall (WAF) provides a comprehensive security solution designed to protect web applications from a wide range of threats. Our WAF includes robust features such as AL (Adaptive Learning), which dynamically analyzes client and server traffic to build policies in real-time for blocking web attacks. In addition to adaptive learning, FortiADC WAF offers extensive WAF signatures, ensuring protection against the OWASP Top 10 vulnerabilities. It also includes advanced API security and safeguards against credential stuffing attacks, delivering a holistic and intelligent approach to application security.

Application Anywhere (GSLB)

The FortiADC 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 continued

Data 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.

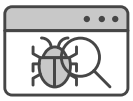
Application Access Management



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).

AI Security

FortiADC now supports AI security with Threat Analytics and FortiGuard Advanced Bot Protection.



- **Threat Analytics** continuously assesses your security posture by monitoring attacks on your web assets and evaluating your WAF and Security configuration and, based on the Insights, provides recommended actions that can enhance your WAF and Security configuration settings, block future attacks, and reduce false positives.



- **FortiGuard Advanced Bot Protection** is a comprehensive defense against the ever-present threat of bots. It provides a cutting-edge SaaS solution to safeguard your web applications and digital assets from the ever-evolving threat of bots using client and server telemetry and deep learning.

Key Features

Advanced Security Services



As the threat landscape evolves, many new risks require a multi-pronged approach for protecting applications. FortiADC provides multi-vector protections starting from the network—IPS, Antivirus, IP Reputation, and to the Applications—DLP, Sandbox, Credential Stuffing, and WAF Signatures, and up to AI Security with Threat Analytics and Advanced Bot Protection.

SSL Offloading and Visibility



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).

Scripts and DevOps Tools



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 an advanced content rewrite and application decisions. FortiADC also offers a range of DevOps tools, such as RestfulAPI, Declarative API, Terraform, cloud-init, and Ansible, enhancing the efficiency of application deployment, management, and automation.

Key Features continued

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.

Analytics and Visibility

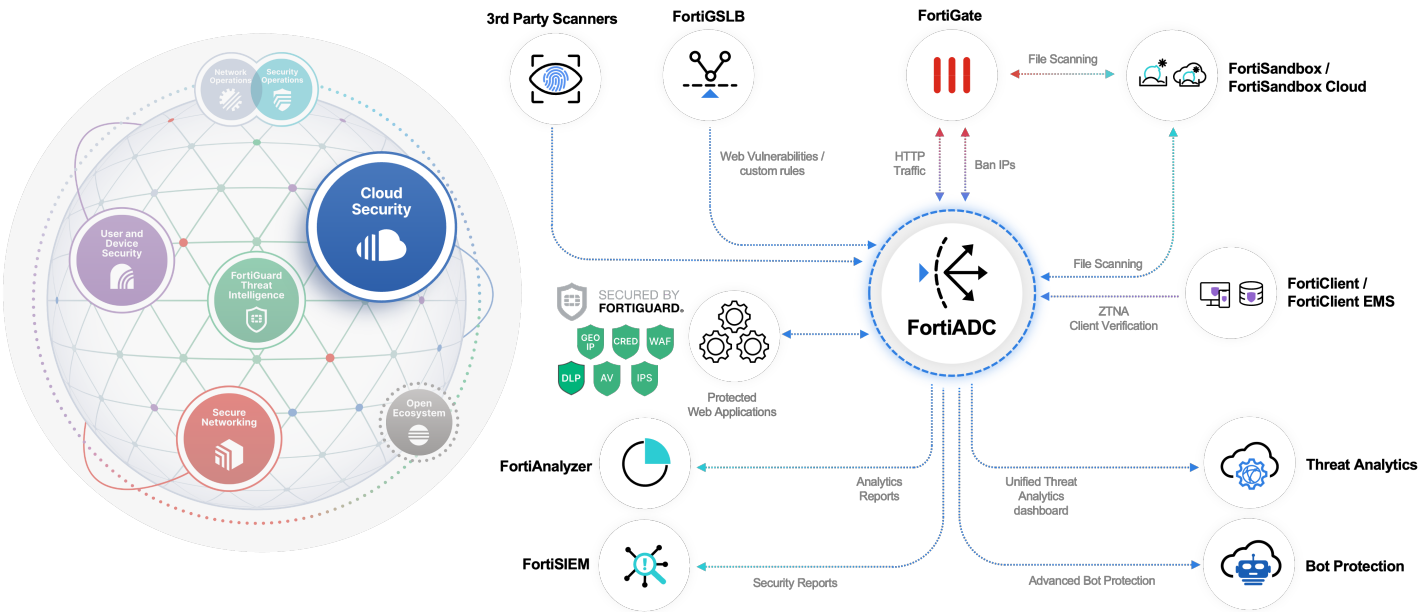
FortiADC offers a comprehensive monitoring system for your network and application. With FortiView, customers can get real-time and historical data into a single view on your FortiADC. We also provide a network logical topology of real-servers, user/application data-analytics, security threats, attack maps, and some other system events and alerts.

FortiADC supports ADC Manager to manage multiple FortiADC devices remotely, and integrates with third party solutions such as Splunk, FortiAnalyzer, and FortiSIEM for more visibility, correlation, automated response, and remediation.

Security Fabric Connectors

FortiADC fabric connectors seamlessly integrate FortiADC with various Fortinet Security Fabric solutions, enabling automated processes for managing dynamic security updates without manual intervention. These connectors define the type of integration and facilitate a cohesive ecosystem for Fortinet products to work together harmoniously.

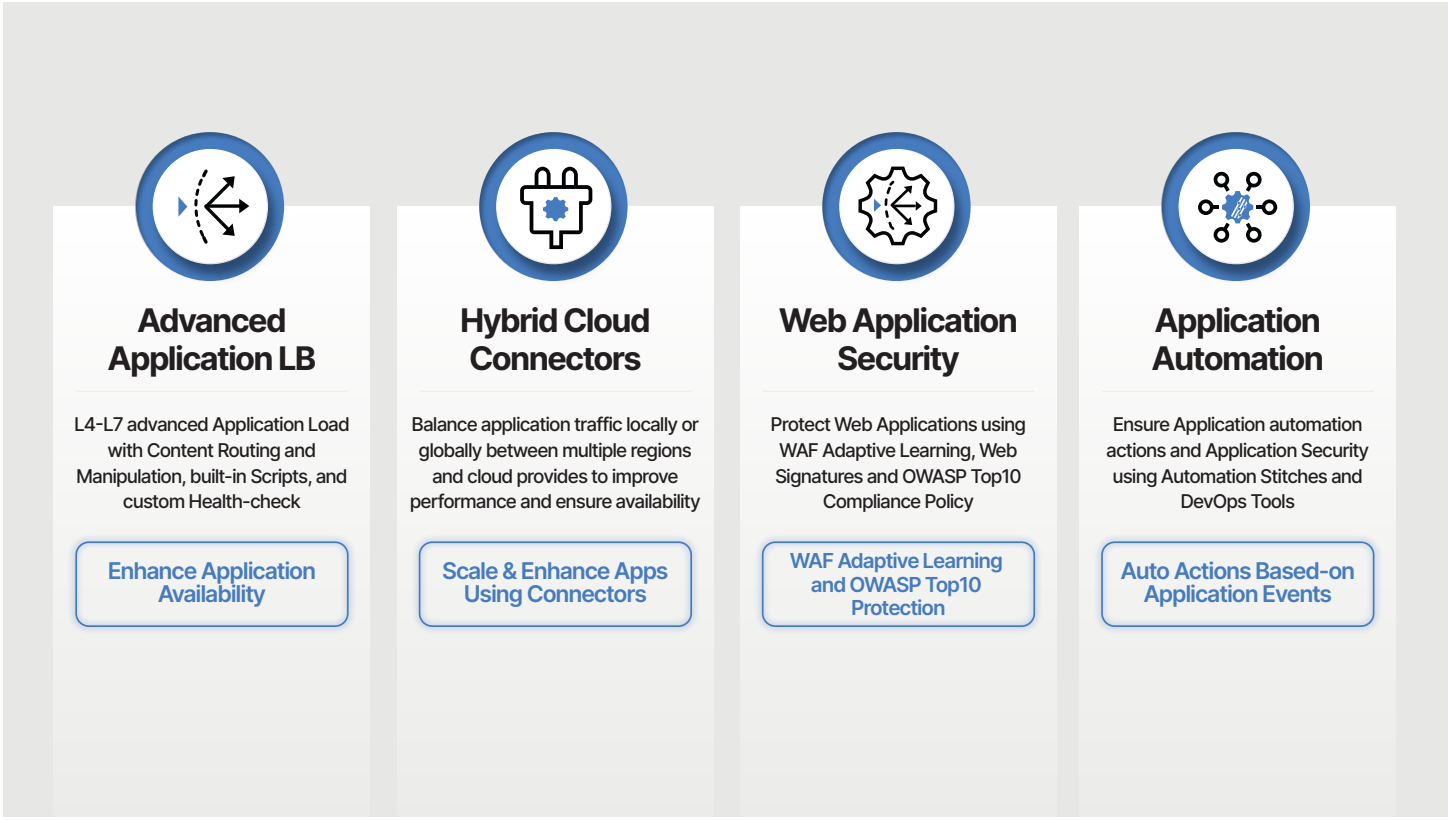
FortiADC supports a range of Security Fabric Integration with: FortiGate, FortiSIEM, FortiAnalyzer, FortiGSLB, Threat Analytics, and FortiGuard Advanced Bot Protection. The overarching goal is to enhance collaboration and automation across the Fortinet product suite through Fabric Connectors.



Use Cases

FortiADC supports multiple use cases for any organization (Telco, Education, Health-Care, Finance and more...).

Find out FortiADC key use-cases for your organization:



Experience with FortiADC Bundles

Elevating Security Across Networks, Applications, and Beyond

Networking Security



Fortify your infrastructure against any network threats with advanced networking security features. This bundle ensures robust protection, minimizes vulnerabilities, and safeguards your network integrity.

Application Security



Shield your applications from potential attacks with the comprehensive Application Security Bundle. Benefit from tailored defenses against application-specific threats, ensuring your critical applications' uninterrupted performance and reliability.

AI Security



Embrace the future of cybersecurity with the AI Security Bundle. Powered by cutting-edge AI/ML models, this bundle offers proactive defense against sophisticated attacks. Analyze threats in real-time, allowing you to stay ahead of cyber threats and respond effectively.

		Network Security	Application Security	AI Security
Network Security	IP Reputation and GeoIP	●	●	●
	Advanced Malware Protection	●	●	●
	Intrusion Prevention Service	●	●	●
Application Security	WAF Signatures and Adaptive Learning		●	●
	Credential Stuffing Defense		●	●
	Sandbox Cloud		●	●
	FortiGuard DLP		●	●
AI Security	Threat Analytics			●
	Advanced Bot Protection			●

FortiADC Features

USE CASES	SUPPORTED FEATURES
Application Availability	Advanced L4-L7 Load-balancing (Application and protocols)
	Presistency, Advanced Health-check, Content Routing, and Rewrite
	Scripting Support and L7 Content Routing and Manipulation
	SSL Advanced Services TLS1.3 (Offloading/Mirroring) and SSL Forward Proxy
	SSL Management (client/server side) + Let's Encrypt support
Application Anywhere	Global Server Load Balancing (Geo-location, RR, Weight, and more)
	Geo-IP Protection and IP Reputation
	DNS Security and DNSSEC
Application Optimization	Dynamic Caching and Compression
	HTTP Page Speed (Optimization and Multiplexing)
Application Protection	Web Application Firewall and Web Vulnerability Scanner
	API Security (OpenAPI, API-GW, API Discovery)
	WAF (AL) Adaptive Learning Support
	FortiGuard Web Application Security Signature
	Credential Stuffing Defense
	OWASP top-10 Compliance
	Advanced Bot Protection
Application Access Security	Application Authentication — Form, Basic, and SSO
	SAML, Kerberos, Auth2.0, LDAP, RADIUS, FortiToken, Google Auth
	FortiGuard Cloud Sandbox
	FortiGuard Data Loss Prevention
System and Networking	VDOM/ADOM Support
	Full NAT (1:1, Dynamic, Statis, and Hide-NAT)
	High Availability (VRRP A/A, A/P Failover)
	IPv4 and IPv6 Support
	Dyanmic Routing (BGP, OSPF) and NVGRE and VXLAN Support
Networking Security	DDoS Protection (Network and Application)
	Stateful Firewall
	Zero Trust Application Gateway
	FortiGuard Intrusion Prevention
	FortiGuard Malware (AV) Protection
Data Analytics and SecOps	FortiView — Data Analytics
	OWASP top-10 Real Time Monitoring
	Real Time Reporting, Monitoring, Logging, and SNMP
	Threat Analytics AI
Fabric Integration and DevOps Tools	Integration — SAP, K8s, OCP, AWS, MS (SharePoint, RDP, Exchange), Splunk, Cisco-ACI, and more
	Security Fabric — FortiGate, FortiSIEM, FortiAnalyzer, FortiClient, FortiAuthenticator, FortiGSLB
	Restful, and Declerative API, Ansible, Terraform, and Cloud-init
24×7 Premium Support	FortiCare Premium Support

* Feature availability is dependent on the subscription to specific license bundles.

Specifications

	FortiADC 220F	FortiADC 320F
System Performance		
L4/L7 Throughput	5 Gbps / 4 Gbps	10 Gbps
L4 CPS	160 000	350 000
L4 HTTP RPS	500 000	1.2M
Maximum L4 Concurrent Connection	6 M	12M
L7 CPS (1:1) *	40 000	120 000
SSL CPS/TPS (1:1) 2K keys **	1200	6000
SSL Bulk Encryption Throughput	1.2 Gbps	5 Gbps
Compression Throughput	2 Gbps	8 Gbps
SSL Acceleration Technology	Software	Software
Virtual Domains	10	25
Hardware Specifications		
Memory	8 GB	16 GB
Network Interfaces	4x GE RJ45, 4x GE SFP	2× 10 GE SFP+, 4x GE SFP, 4x GE RJ45
10/100/1000 Management Interface	—	2
Storage	120 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	No
Dimensions		
Height x Width x Length (inches)	1.73 × 17.24 × 16.38	1.75 × 17.0 × 15.0
Height x Width x Length (mm)	44 × 438 × 416	44.45 × 432 × 380
Weight	22 lb (9.07 kg)	11 lbs (5.5 kg)
Environment		
Form Factor	1U Appliance	1U Appliance
Input Voltage	100-240V AC, 50-60Hz	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	80W	40 W / 60 W
Maximum Current	100V/6A, 240V/3A	9A / 17A
DC Power Supply	—	—
Heat Dissipation	273 BTU/h	132–163 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4°F to 167°F (-20°C to 75°C)	-4°F to 167°F (-20°C to 75°C)
Humidity	5% to 95% non-condensing	10% to 85% relative humidity, non-operating, 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	FCC Part 15 Class A, RCM, VCCI Class A, CE, UL/c
Safety	CSA, C/US, CE, UL	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=RSA-AES256-SHA; 2K Keys.

Specifications

	FortiADC 420F	FortiADC 1200F/-DC
System Performance		
L4/L7 Throughput	20 Gbps	40 Gbps / 30 Gbps
L4 CPS	700 000	1 000 000
L4 HTTP RPS	2.1M	3 000 000
Maximum L4 Concurrent Connection	25M	36 000 000
L7 CPS (1:1) *	200 000	240 000
SSL CPS/TPS (1:1) 2K keys **	20 000	35 000
SSL Bulk Encryption Throughput	10 Gbps	19 Gbps
Compression Throughput	14 Gbps	20 Gbps
SSL Acceleration Technology	ASIC	ASIC
Virtual Domains	45	45
Hardware Specifications		
Memory	32 GB	32 GB
Network Interfaces	4× 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	2
Storage	120 GB SSD	240 GB SSD
Management	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP
Power Supply	Single (support Dual hot-swap PSU)	Dual (support hot-swap PSU)
Trusted Platform Module (TPM)	No	Yes
Dimensions		
Height x Width x Length (inches)	22.4 × 23.6 × 9	1.73 × 21.5 × 17.3
Height x Width x Length (mm)	44 × 438 × 420	44 × 548 × 440
Weight	14.11 lbs (6.4 kg)	22.5 lbs (10.2 kg)
Environment		
Form Factor	1U Appliance	1U Appliance
Input Voltage	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	68 W / 140 W	251 W / 320 W
Maximum Current	9A / 17A	100V / 7A, 240V / 3.5A
DC Power Supply	—	Supported
Heat Dissipation	232 BTU/h	856 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4°F to 167°F (-20°C to 75°C)	-4°F to 167°F (-20°C to 75°C)
Humidity	10% to 85% relative humidity, non-operating, non-condensing	10% to 85% 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	FCC/ ICES, CE, RCM, VCCI, BSMI
Safety	CSA, C/US, CE, UL	UL/ cUL, CB





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=RSA-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	5 000 000	5 000 000	18 000 000
Maximum L4 Concurrent Connection	72 000 000	144 000 000	216 000 000
L7 CPS (1:1) *	280 000	500 000	1 100 000
SSL CPS/TPS (1:1) 2K keys **	40 000	60 000	90 000
SSL Bulk Encryption Throughput	22 Gbps	37 Gbps	100 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, 12× 10GbE SFP+ ports	4× 40GbE QSFP, 8× 10G SFP+	4× 100 GE QSFP28, 8× 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 × 21.5 × 17.3	3.46 × 21.5 × 17.3	3.4 × 17.2 × 30.2
Height x Width x Length (mm)	44 × 548 × 440	88 × 548 × 440	80.6 × 436.9 × 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, 50–60 Hz
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 / 6A, 240V / 3A
DC Power Supply	Supported	Supported	—
Heat Dissipation	911 BTU/h	917 BTU/h	7506 BTU/hr
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	50°F to 95°F (10°C to 35°C)
Storage Temperature	-4°F to 167°F (-20°C to 75°C)	-4°F to 167°F (-20°C to 75°C)	-40°F to 140°F (-40°C to 60°C)
Humidity	10% to 85% non-condensing	10% to 85% non-condensing	8% to 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=RSA-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, IBM Cloud, Alibaba Cloud, Nutanix, and Proxmox. 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 8.0.

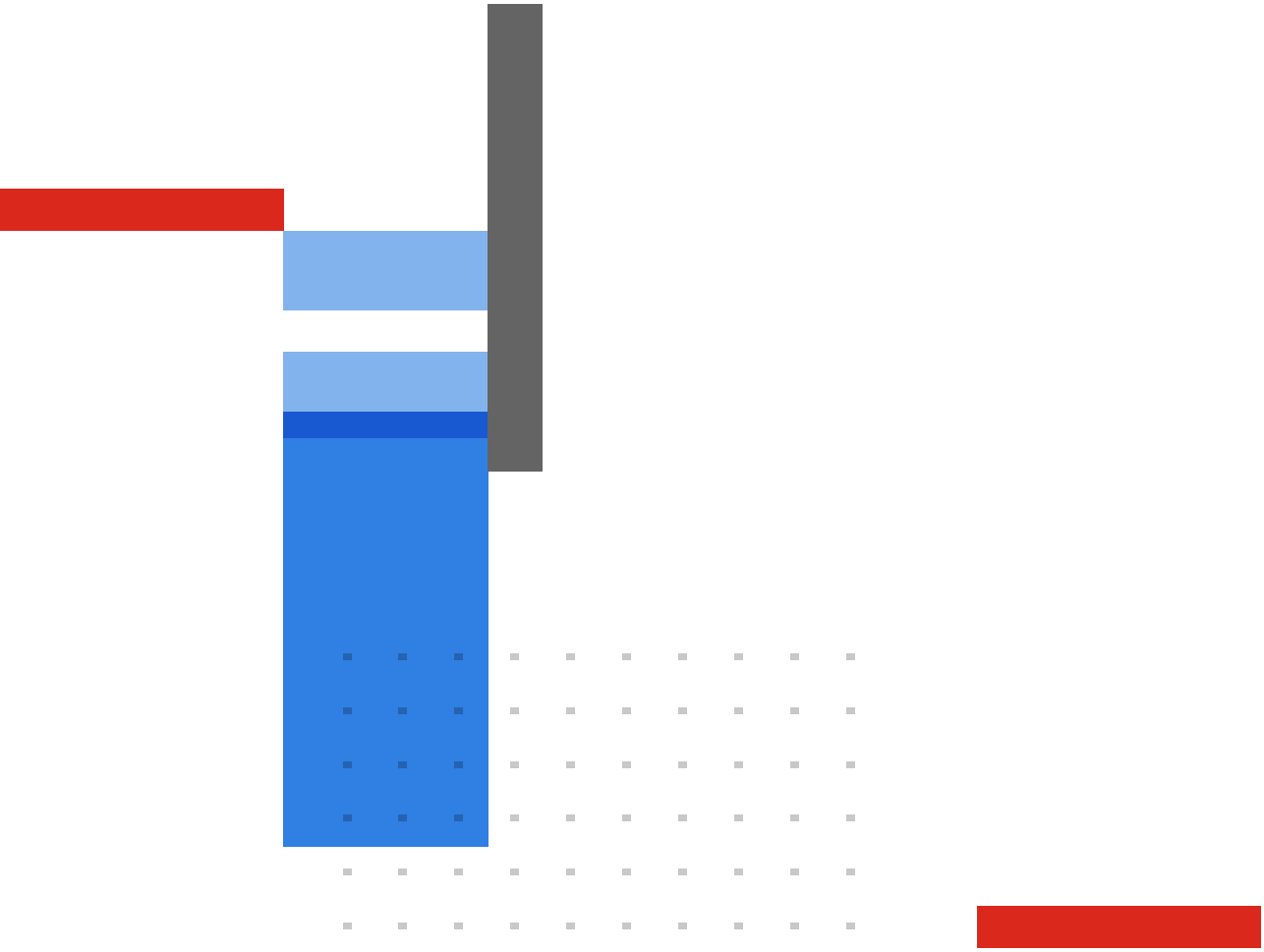
Ordering Information

Product	SKU	Description
FortiADC 220F	FAD 220F	FortiADC 220F, 4x GE RJ45 ports, 4x GE SFP ports, 1× 120 GB SSD storage.
FortiADC 320F	FAD-320F	FortiADC 320F, 4x GE RJ45 ports, 4x GE SFP ports, 2× 10 GE SFP+ ports, 2x GE management ports, 1× 120 GB SSD storage.
FortiADC 420F	FAD-420F	FortiADC 420F, 4x GE RJ45 ports, 4x GE SFP ports, 4× 10 GE SFP+ ports, 2x management ports, 1× 120 GB SSD storage, Hardware SSL Accelerator, Optional Redundant PSU.
FortiADC 1200F	FAD-1200F	FortiADC 1200F, 8× 10 GE SFP+ ports, 8x GE SFP ports, 8x GE RJ45 ports, 2x GE RJ45 management port, 1× 240 GB SSD, dual AC power supplies.
FortiADC 1200F-DC	FAD-1200F-DC	FortiADC 1200F, 8× 10 GE SFP+ ports, 8x GE SFP ports, 8x GE RJ45 ports, 2x GE RJ45 management port, 1× 240 GB SSD, dual DC power supplies.
FortiADC 2200F	FAD-2200F	FortiADC 2200F, 12× 10 GE SFP+ ports, 8x GE SFP ports, 2x GE RJ45 management port, 1× 240 GB SSD, dual AC power supplies.
FortiADC 2200F-DC	FAD-2200F-DC	FortiADC 2200F, 12× 10 GE SFP+ ports, 8x GE SFP ports, 2x GE RJ45 management port, 1× 240 GB SSD, dual DC power supplies.
FortiADC 4200F	FAD-4200F	FortiADC 4200F, 4× 40 GbE QSFP+, 8× 10 GbE SFP+, 2x GbE RJ45 management port, 1× 480 GB SSD, dual AC power supplies.
FortiADC 4200F-DC	FAD-4200F-DC	FortiADC 4200F, 4× 40 GbE QSFP+, 8× 10 GbE SFP+, 2x GbE RJ45 management port, 1× 480 GB SSD, dual DC power supplies.
FortiADC 5000F	FAD-5000F	FortiADC 5000F, 4× 100 GE QSFP28, 8× 40 GE QSFP, 1x GE RJ45 management port, 1× 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 Accessories	**SKU**	**Description**
FortiADC Redundant Power Supply	SP-FWB600F-PS	AC power supply for FWB-600F and FAD-420F; power cable SP-FGPCOR-XX sold separately.
	SP-FAD-1200F-PS	AC power supply for FAD-1200F, 2200F, and 4200F; power cable SP-FGPCOR-XX sold separately.
Fan Module 4200F	SP-FAD4200F-FAN	Fan module for FAD-4200F.
Fan Module 1200F/2200F	SP-FAD1200F-FAN	Fan module for FAD-1200F and 2200F.
5000F SSD	SP-FAD5000F-SSD	3.84 TB 2.5 inch SATA SSD with tray for FAD-5000F.
VM Subscriptions*	**SKU**	**Description**
VM Subscriptions are supported for all VMs from VM01 (1 CPU) and up to VM32 (32 CPU).		

* All Form Factors (HW/VM/VM subscription) are available with different bundle licenses such as Networks Security, Application Security, and AI Security.

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 © 2024 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 SVP Legal and above, 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.

July 29, 2024

FAD-DAT-R58-20240729