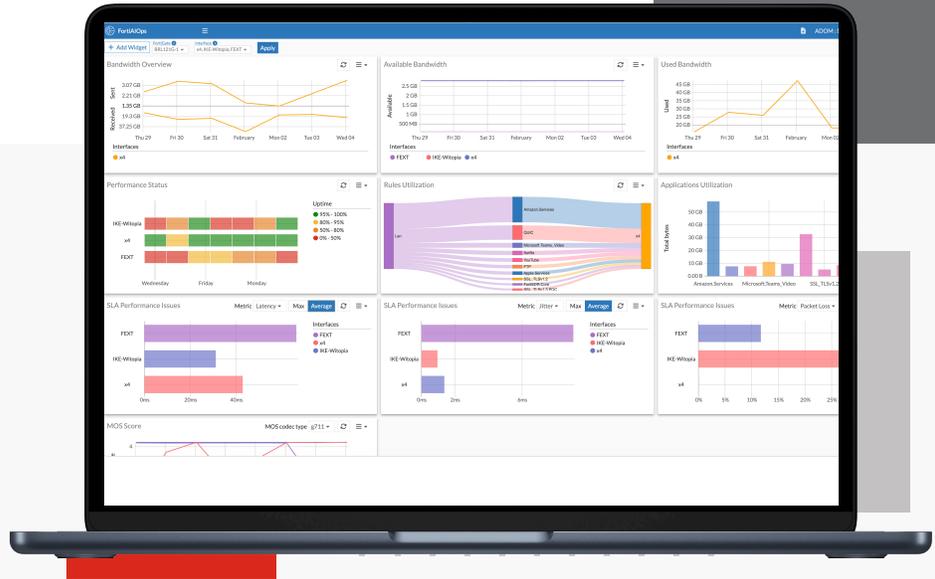


FortiAI Ops



Highlights

- **Extensive Visibility:** Monitoring and reporting of WLAN, LAN, SD-WAN, and 5G/LTE Gateway
- **AI-Powered Insights:** Correlate events and data from across the deployment to quickly identify issues
- **Data Sovereignty:** Sensitive data and AI processing stays within your private data center
- **Robust Troubleshooting Tools:** Built-in tools to validate your deployment at any network level
- **Reduced Trouble Tickets:** Identify and correct issues before they start impacting users
- **Lower TCO:** Reduce the Mean Time to Resolution

FortiAI-powered and automation-driven Network Operations

FortiAI Ops simplifies LAN and WAN network management and leverages artificial intelligence with machine learning for enhanced network operations.

FortiAI Ops delivers a simple and easy means to manage a Fortinet networking stack (FortiAP, FortiSwitch, FortiGate, and FortiExtender). Network monitoring functionality gives visibility and in-depth understanding at your fingertips. From Layer 1 diagnostic information to Layer 7 application visibility, FortiAI Ops covers Wi-Fi, Ethernet, SD-WAN, and 5G/LTE Gateway. Built-in troubleshooting tools enable active testing of network components to find faults and verify functionality.

The built-in Artificial Intelligence engine uses machine learning to catch issues, solve problems, and prevent network degradation. Artificial Intelligence can systematically consume the extensive amount of data being produced throughout the Security Fabric, correlate it, and analyze the results with Machine Learning so that you don't have to.

FortiAI Ops is available as a virtual machine. In all deployment scenarios it works natively with Fortinet NOC and SOC tools to unify and simplify the way you manage the Fortinet Security Fabric.

Available in



Appliance



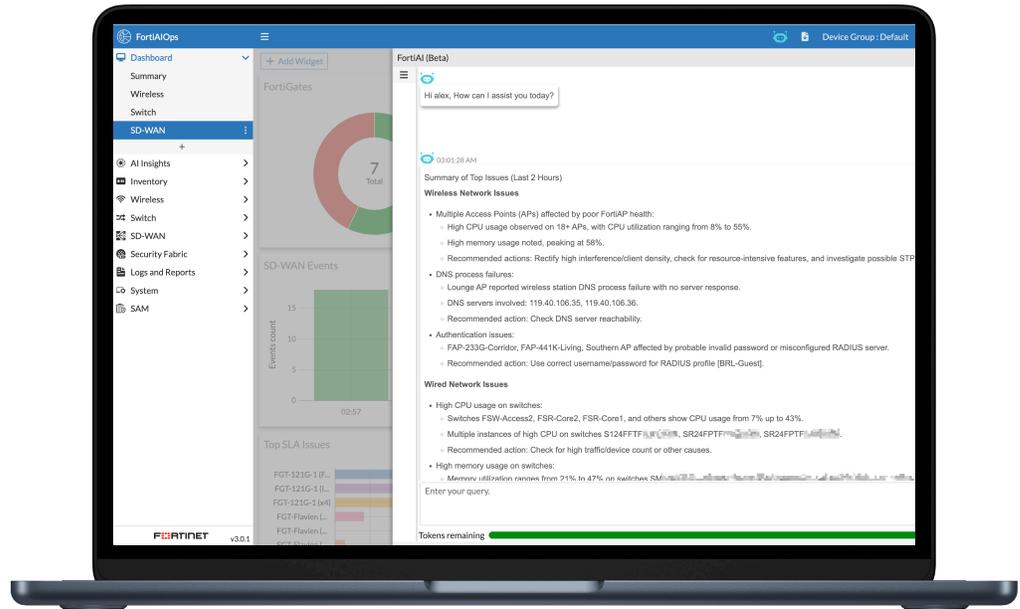
Virtual



BYOL using public cloud providers

AI Insights with Machine Learning

The AI Engine combs through all your data and pulls out key items that need attention, giving you drill down focus on problems and easy solutions to complex issues. Machine Learning can determine what's normal for your network and your traffic, then keep that performance across time.



FortiAI

FortiAI is Fortinet’s embedded artificial intelligence framework, integrated across the Security Fabric to defend against emerging threats, automate operations, and secure AI adoption. It spans three categories—FortiAI-Protect, FortiAI-Assist, and FortiAI-SecureAI.

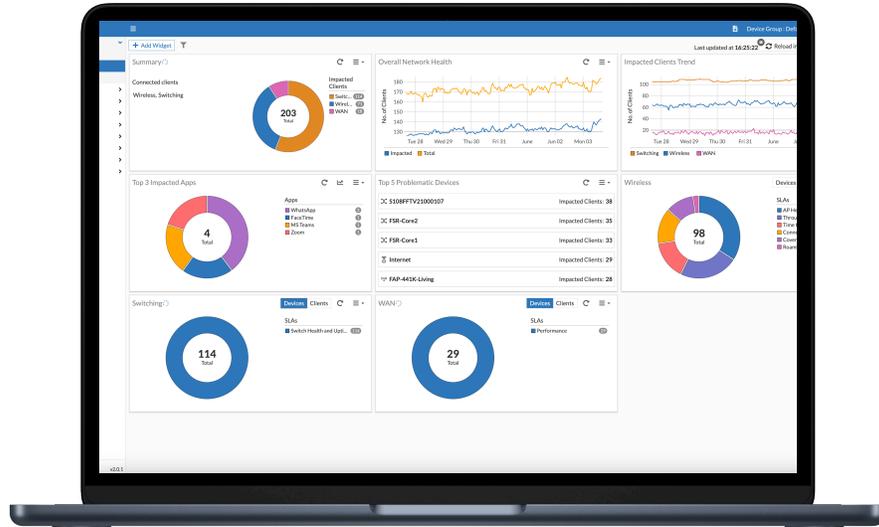
Within this framework, FortiAI-Assist brings generative AI and advanced reasoning to simplify network operations. FortiAIops leverages these Assist capabilities through a conversational, GenAI-powered interface for troubleshooting. Admins can ask natural-language questions—such as identifying roaming issues, diagnosing throughput problems, or checking SSID and network health—and instantly receive context-rich answers with likely causes and recommended remedies. By embedding FortiAI-Assist, FortiAIops accelerates troubleshooting, reduces noise, and improves overall operational efficiency.

FortiAIops leverages the same logs that FortiAnalyzer is already collecting, meaning there is no additional overhead on your network to add Artificial Intelligence to the Security Fabric. This activity is another benefit of a combined platform approach to Security-Driven Networking.



Monitor Desired Service Levels

Use trending information and configured SLAs determine the good or bad health of your network.



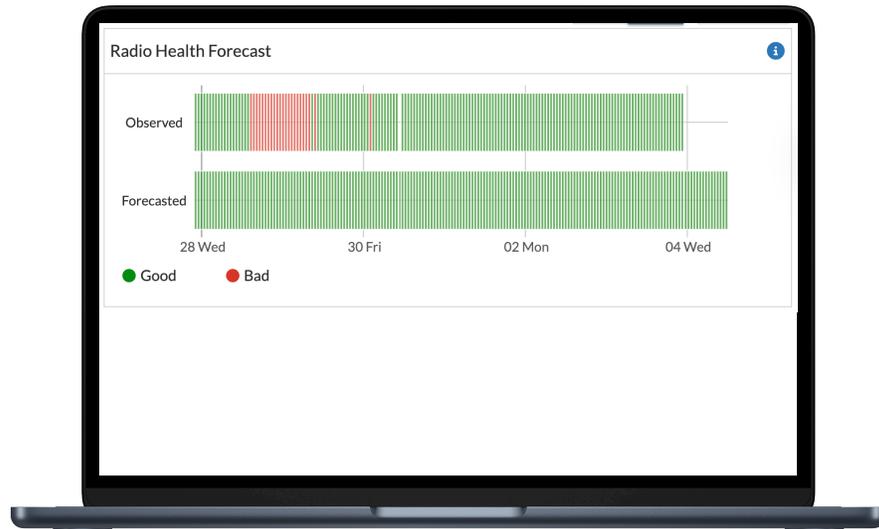
AI-Driven ARRP

AI-Driven ARRP automates and optimizes the management and distribution of wireless channels across all Access Points (APs) monitored by FortiAIops. The AI engine makes precise channel decisions by leveraging historical telemetry and deep insights gathered by FortiAIops.



Forecasting

AI/ML driven forecasting predicts SD WAN performance—latency, jitter, and packet loss—based on learned baselines, identifying deviations before users are impacted. Built in insights highlight trending issues and upcoming performance risks. For WLAN, RF level forecasting anticipates radio issues and optimizes channels through AI ARRP, enabling proactive and seamless network optimization.



Dynamic Baselineing

FortiAIOps analyzes recent telemetry to establish adaptive SLA thresholds for SD WAN and LAN metrics, dynamically updating baselines for latency, jitter, packet loss, and wired and wireless performance to identify meaningful deviations from normal behavior.

Health Score

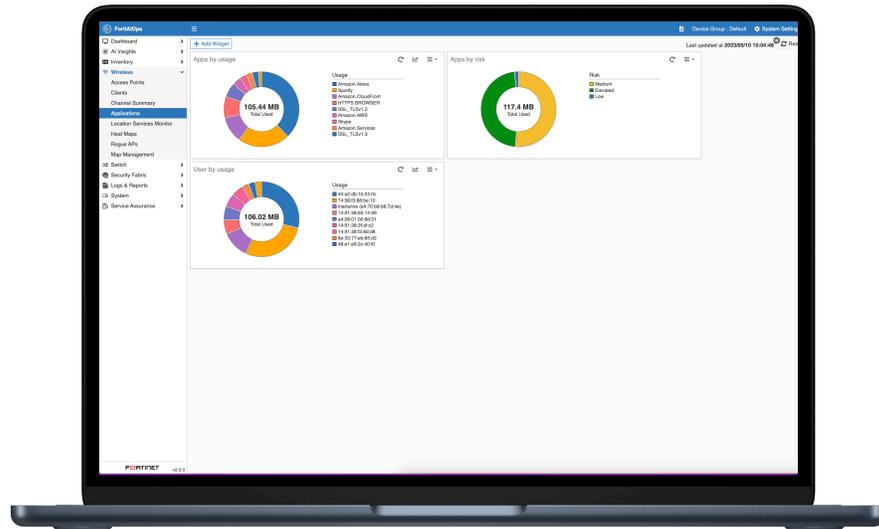
A Health Score is derived for each individual device based on all SLAs that have been triggered to ensure an accurate representation of overall system health. The Health Score is then classified as Good, Fair, or Bad to allow for an instant visual representation of the state of a particular device.

AI Insights	Performance
Good i SLA Health Score	
<input checked="" type="checkbox"/> Select All	Apply
<input checked="" type="checkbox"/> AP Health	100%
<input checked="" type="checkbox"/> Throughput	99.93%
<input checked="" type="checkbox"/> Coverage	99.7%
<input checked="" type="checkbox"/> Roaming	88.75%
<input checked="" type="checkbox"/> Time To Connect	63.64%
<input checked="" type="checkbox"/> Connection Failure	50.85%



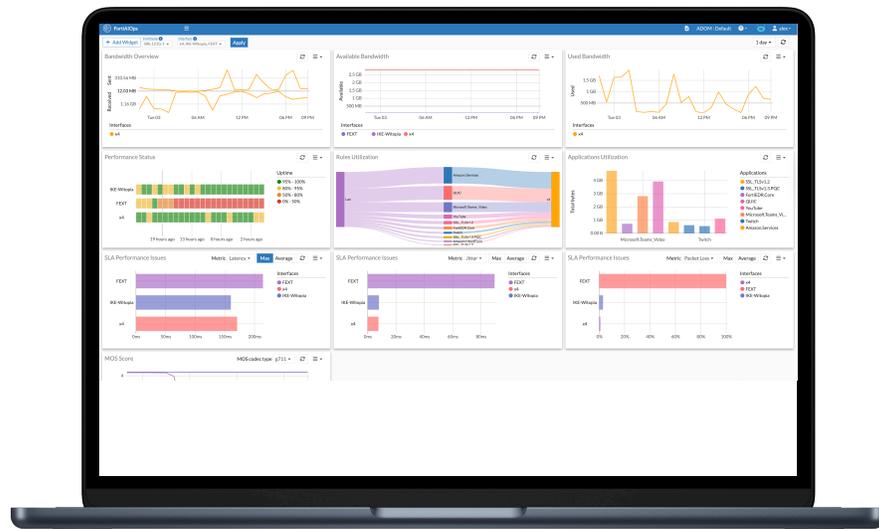
Application Monitoring

Get insights into what people are doing on your network with the FortiAI Ops DPI Application Monitoring feature. All detected or blocked applications will be listed with trend views available.



SD-WAN

Key functions include AI driven predictive modeling and deviation analysis to model and baseline normal network behavior across defined SLAs. Through dynamic baseline modeling, FortiAI Ops enables accurate performance forecasting and proactive anomaly detection, helping identify meaningful deviations early and maintain consistent, high quality network performance.



Automated Packet Capture Analysis

FortiAI Ops can obtain packet capture data from remote devices and perform AI assisted analysis, providing insight into the health of the network and aiding in network optimization.

FortiAI

Hi alex, How can I assist you today?

Jan 30 11:00 AM

Analyze the uploaded packet capture file: wifi7-connectivity-1.pcapng

Jan 30 11:00 AM

Key Observations

- **Majority of traffic is management frames (364 out of 641 WLAN frames).**
-> Indicates the capture primarily contains Wi-Fi management activity, such as beacons, probes, or authentication/association, rather than user data.
- **Very limited data traffic observed (only 19 data frames, 3271 bytes).**
-> Suggests minimal actual client data exchange; the capture likely covers a period of network setup or idle connectivity.
- **Presence of EAPOL frames (4 frames, 1222 bytes) within LLC layer.**
-> Points to WPA/WPA2 authentication or key exchange activity, possibly capturing a client joining or re-authenticating to the network.
- **Multiple Fortinet MAC addresses are top talkers, all targeting a masked destination (ff:ff:ff:ff:ff:ff).**
-> Implies the capture is from a Fortinet-managed environment, with anonymized or broadcast/multicast destinations, possibly for management or control traffic.

📄 If you'd like deeper analysis, try asking questions specific to this Wi-Fi capture (for example: "Can you identify if a client successfully authenticated?", "Are there signs of connectivity issues?", or "What SSIDs are visible in the management frames?").

Jan 30 11:01 AM

Any roaming issue?

Jan 30 11:01 AM

The packets show a successful Wi-Fi association sequence between a client and an access point, with no evidence of roaming issues. Based on the summaries, there is one Association Request from client 38:c0:ea:a9:de:b5 to AP a6:7b:46:cf:b0:2e for SSID "!!!kvasudevanwifi7", immediately followed by an Association Response with a status code of 0x0000 (success), indicating the association was accepted without error.

Would you like me to check for deauthentication or disassociation frames, or analyze for authentication failures to further confirm roaming stability?

Enter your query.

Tokens remaining

⚠ Responses are AI-generated and may be inaccurate.

Spectrum Analyzer

Detect, classify, and manage wireless interference. Spectrum Manager gathers interference data from a network of dedicated sensors. It can also gather data from the APs which can dedicate one of its radios to act as a sensor.



Specifications

FORTIAIOPS APPLIANCES**	FAO-100G	FAO-500G
Performance* in Combined mode (shipped/maximum)		
FortiGates	0 / 30	0 / 1000
FortiSwitch	0 / 90	0 / 3000
FortiExtender	0 / 30	0 / 1000
FortiAP	0 / 180	0 / 6000
Stations	0 / 3 000	0 / 25 000
Options		
FortiAI Ops Monitoring Subscription	FCX-10-AOIHR-673-01-DD	FCX-10-AOIHR-673-01-DD
FortiAI Ops Monitoring and AI Insights Subscription Bundle	FCX-10-AOIHR-1087-01-DD	FCX-10-AOIHR-1087-01-DD
FortiAI Ops SD-WAN Subscription	FCX-10-AOIHR-675-01-DD	FCX-10-AOIHR-675-01-DD
Hardware Specifications		
Form Factor (supports EIA/non- EIA standards)	1 RU Rackmount	2 RU Rackmount
Total Interfaces	4× 2.5GE RJ45	4× 1GE RJ45 + 2× 10GE SFP+
Console	RJ45 console	DB9 serial console
USB Ports	2x USB 3.0 ports	2x USB 3.0 ports
Storage Capacity (Max)	1× 3.84TB M.2 SDD	4× 2.5 in. hot-swappable 2TB SDD 8× 3.5 in. hot-swappable 4TB SAS HDD
Storage Capacity (shipped)	1× 3.84TB M.2 SDD	2× 2.5 in. hot-swappable 2TB SDD 4× 3.5 in. hot-swappable 4TB SAS HDD
Usable Storage	3.84TB	Hot/SSD = ~3.84 / 7.68 TB Warm/HDD = ~16 / 32 TB
Before RAID (Shipped / Max)		
Removable Hard Drives	—	⊙
RAID Levels Supported	—	RAID 0/1/5/10
RAID Type	—	Hardware / Hot Swappable
Default RAID Level	—	Hot/SSD : RAID 1 Warm/HDD : RAID 5
Redundant Hot Swap Power Supplies	—	⊙
Trusted Platform Module (TPM)	⊙	⊙
Dimensions		
Height x Width x Length (inches)	1.73 × 17.24 × 16.54	3.46 × 17.32 × 29.33
Height x Width x Length (mm)	44 × 438 × 420	88 × 440 × 745
Weight	12.1 lbs (5.47 kg)	50.2 lbs (22.8 kg)
Environment		
AC Power Supply	100-240Vac, 50~60Hz, 6A max	100-240Vac, 50~60Hz, 7A max
Power Consumption (Average/ Max)	98.5 W / 123 W	580 W / 705 W
Heat Dissipation	419.8 BTU/h (Max.)	2404 BTU/h (Max.)
Operating Temperature	32°F to 104° F (0°C to 40° C)	32°F to 104° F (0°C to 40° C)
Storage Temperature	-40°F to 158° F (-40°C to 70° C)	-4°F to 167° F (-20°C to 75° C)
Humidity	5% to 95% relative humidity, non-operating, non-condensing	5% to 95% relative humidity, non-operating, non-condensing
Forced Airflow	Front to Back	Front to Back
Operating Altitude	Up to 10 000 ft (3048 m)	Up to 10 000 ft (3048 m)
Compliance		
	FCC, ICES, CE, UKCA, RCM, VCCI, BSMI, UL, C-mark, CB	FCC, ISED, CE, RCM, VCCI, BSMI, UL/cUL, CB

*Please refer to Ordering Guide for full details on performance

** FortiAI Ops appliances do not have any license included. FortiAI Ops subscriptions need to be purchased separately.



Ordering Information

FortiAIOps offers subscriptions for Monitoring, AI Insights, or SD-WAN. For Monitoring or AI Insights, licensing is by number of extension devices (FortiSwitch or FortiAP), for SD-WAN licensing is by FortiGate devices. A bundle of both Monitoring and AI Insights is available as well.

VM Service Categories	SKU	Description
FortiAIOps Monitoring	FC1-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 25 extension device. Includes FortiCare Premium.
	FC2-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 500 extension device. Includes FortiCare Premium.
	FC3-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 2000 extension device. Includes FortiCare Premium.
	FC4-10-AOVMS-668-01-DD	FortiAIOps Monitoring subscription for 10000 extension device. Includes FortiCare Premium.
FortiAIOps Monitoring and AI Insights Bundle	FC1-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 25 extension device. Includes FortiCare Premium.
	FC2-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 500 extension device. Includes FortiCare Premium.
	FC3-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 2000 extension device. Includes FortiCare Premium.
	FC4-10-AOVMS-670-01-DD	FortiAIOps Monitoring and AI Insights subscription BUNDLE for 10000 extension device. Includes FortiCare Premium.
FortiAIOps SD-WAN	FC1-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 25 FortiGate device. Includes FortiCare Premium.
	FC2-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 500 FortiGate device. Includes FortiCare Premium.
	FC3-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 2000 FortiGate device. Includes FortiCare Premium.
	FC4-10-AOVMS-671-01-DD	FortiAIOps SD-WAN subscription for 10000 FortiGate device. Includes FortiCare Premium.
Appliance and Service Categories	SKU	Description
FortiAIOps-100G	FAO-100G	FortiAIOps-100G appliance, 4x 2.5 GE RJ45 ports, 1x RJ45 Serial Console port, 1x 3.84 TB SSD Storage.
	FC-10-AO1HG-247-02-DD	FortiCare Premium Support.
FortiAIOps-500G	FAO-500G	4x GE RJ45 ports, 2x 10 GE SFP+ ports, 1x RJ45 Serial Console port, 2x 1.92 TB SSD, 4x 3.5 in. 4 TB Storage.
	FC-10-A500G-247-02-DD	FortiCare Premium Support.
FortiAIOps Monitoring	FC1-10-AIOHR-673-01-DD	FortiAIOps Appliance Monitoring subscription for 25 extension device.
	FC2-10-AIOHR-673-01-DD	FortiAIOps Appliance Monitoring subscription for 500 extension device.
	FC3-10-AIOHR-673-01-DD	FortiAIOps Appliance Monitoring subscription for 2000 extension device.
	FC4-10-AIOHR-673-01-DD	FortiAIOps Appliance Monitoring subscription for 10000 extension device.
FortiAIOps Monitoring and AI Insights Bundle	FC1-10-AIOHR-1087-01-DD	FortiAIOps Appliance Monitoring and AI Insights subscription BUNDLE for 25 extension device.
	FC2-10-AIOHR-1087-01-DD	FortiAIOps Appliance Monitoring and AI Insights subscription BUNDLE for 500 extension device.
	FC3-10-AIOHR-1087-01-DD	FortiAIOps Appliance Monitoring and AI Insights subscription BUNDLE for 2000 extension device.
	FC4-10-AIOHR-1087-01-DD	FortiAIOps Appliance Monitoring and AI Insights subscription BUNDLE for 10000 extension device.
FortiAIOps SD-WAN	FC1-10-AIOHR-675-01-DD	FortiAIOps Appliance SD-WAN subscription for 25 FortiGate device.
	FC2-10-AIOHR-675-01-DD	FortiAIOps Appliance SD-WAN subscription for 500 FortiGate device.
	FC3-10-AIOHR-675-01-DD	FortiAIOps Appliance SD-WAN subscription for 2000 FortiGate device.
	FC4-10-AIOHR-675-01-DD	FortiAIOps Appliance SD-WAN subscription for 10000 FortiGate device.

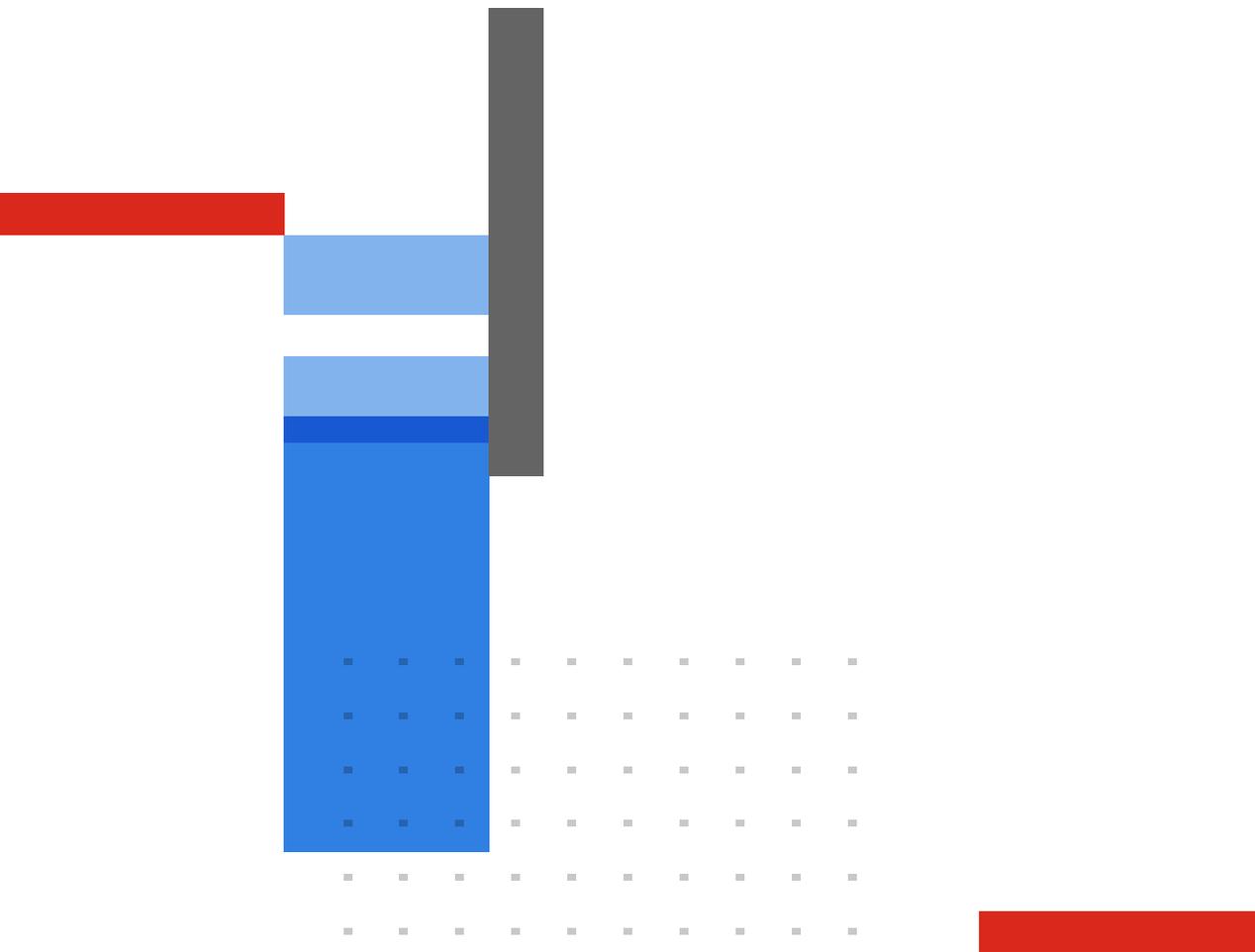
* FortiAIOps appliances do not have any license included. FortiAIOps subscriptions need to be purchased separately.

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



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](#).



www.fortinet.com

Copyright © 2026 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.