



ORDERING GUIDE

FortiProxy

Available in



Appliance



Virtual

NEXT GENERATION SECURE WEB GATEWAY

FortiProxy is a secure web gateway product that protects employees against Internet-borne attacks by incorporating multiple detection techniques such as Web & Video Filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention, Browser Isolation and advanced threat protection. It helps enterprises enforce Internet compliance using granular application control.

FortiProxy provides multiple detection methods, such as reputation lookup, signature-based detection, and sandboxing, to protect against known malware, emerging threats, and zero day malware.

FortiProxy is offered as a high performance physical appliance to support locations with large user populations, as well as various size virtual appliances to suit any size and deployment model that best suits the business. Virtual machines can be deployed on premise or in the public cloud.

PRODUCT OFFERINGS

FortiProxy is offered through a variety of product models and service add-ons as follows:

- **FortiProxy-HW:** three different hardware models that provide multicore processing combined with hardware-based SSL inspection.
- **FortiProxy-VM:** yearly subscription of our virtual FortiProxy supported on all common hypervisors and public cloud providers.
- **VDOM (optional license):** Virtual Domains (VDOMs) are used to divide a FortiProxy into virtual units that are managed and function independently.
- **SWG Protection Bundle:** when choosing a virtual or hardware FortiProxy, remember to add SWG Protection Bundle for advanced security services. SWG Protection Bundle is a yearly subscription. Otherwise, FortiProxy only performs caching and WAN optimization without any security services.
- **Data Protection Service (Optional license):** an image and content analysis service that enables the detection of visual threats and forbidden content types, as well as the analysis of written or visual text for known patterns. The service leverages AI for image analysis, FortiProxy OS features such as EDM and OCR, and FortiGuard DLP service. This service includes both former services known as content analysis and FortiGuard DLP.
- **Client Browser Isolation (optional license):** client-based native browser isolation (NBI) uses an isolated environment and memory space to contain potential malware, ransomware, and other zero-day threats.

Note that while SSL inspection is not listed as a service in the following tables, it is a horizontal needed for all services and is critical for the SWG market.

	HARDWARE ACCELERATED SUBSCRIPTIONS		
	400G	2000G	4000G
Licenses Offering			
Users License	500-6,000 users	500-20,000 users	500-60,000 users
SWG Protection Bundle	Add-on license	Add-on license	Add-on license
Advanced Caching	Included	Included	Included
WAN Optimization	Included	Included	Included
Data Protection Service	Add-on license	Add-on license	Add-on license
VDOM (5 VDOMs are included)	Add-on license (up to 10 VDOM)	Add-on license (up to 100 VDOM)	Add-on license (up to 250 VDOM)
Client Browser Isolation	Add-on license	Add-on license	Add-on license
Hardware			
10/100/1000	4GE	4 GE, 2 SPF	4 GE, 2 SPF
10G SPF+		2 SPF+	4 SPF+
Bypass Interfaces		2 GE	2 GE
Dual PS	Single (Optional Dual)	Dual	Dual
Form Factor	1U	2U	2U
SWG Protection Bundle			
Web & Video Filtering	☑	☑	☑
DNS Filtering	☑	☑	☑
Video Filtering	☑	☑	☑
Application Control	☑	☑	☑
IPS	☑	☑	☑
AntiVirus	☑	☑	☑
Virus Outbreak and Content Disarm & Reconstruct	☑	☑	☑
Botnet (IP/Domain)	☑	☑	☑
Sandbox Cloud	☑	☑	☑
Content Analysis	Add-on license	Add-on license	Add-on license
Client Browser Isolation	Add-on license	Add-on license	Add-on license
DLP	Add-on license	Add-on license	Add-on license

ORDER INFORMATION

HARDWARE ACCELERATED SUBSCRIPTIONS			
	400G	2000G	4000G
SWG Protection Bundle	FC1-10-XY40G-514-02-DD	FC1-10-XY2KG-514-02-DD	FC1-10-XY4KG-514-02-DD
Data Protection	FC1-10-XY40G-1005-02-DD	FC1-10-XY2KG-1005-02-DD	FC1-10-XY4KG-1005-02-DD
24x7 Support	FC-10-XY40G-247-02-DD	FC-10-XY2KG-247-02-DD	FC-10-XY4KG-247-02-DD
Client Browser Isolation	FC1-10-XY40G-587-02-DD	FC1-10-XY2KG-587-02-DD	FC1-10-XY4KG-587-02-DD
FortiGuard DLP Service	FC1-10-XY40G-589-02-DD	FC1-10-XY2KG-589-02-DD	FC1-10-XY4KG-589-02-DD
VDOM	FPX-VDOM-5-UG	FPX-VDOM-5-UG	FPX-VDOM-5-UG
Redundant Power Supply Unit	SP-FAD400F-PS	Included	Included

PRODUCT OFFERINGS

VIRTUAL MACHINE SUBSCRIPTIONS					
	VM02	VM04	VM08	VM16	VMUL
Licenses Offering					
Users License	100-75,000* users	100-2,500 users	100-10,000 users	100-25,000 users	100-50,000 users
SWG Protection Bundle	Add-on license	Add-on license	Add-on license	Add-on license	Add-on license
Advanced Caching	Included	Included	Included	Included	Included
WAN Optimization	Included	Included	Included	Included	Included
Data Protection Service	Add-on license	Add-on license	Add-on license	Add-on license	Add-on license
VDOM (5 VDOMs are included)	Add-on license (up to 10 VDOM)	Add-on license (up to 25 VDOM)	Add-on license (up to 50 VDOM)	Add-on license (up to 100 VDOM)	Add-on license (up to 500 VDOM)
Client Browser Isolation	Add-on license	Add-on license	Add-on license	Add-on license	Add-on license
SWG Protection Bundle					
Web & Video Filtering	☑	☑	☑	☑	☑
DNS Filtering	☑	☑	☑	☑	☑
Video Filtering	☑	☑	☑	☑	☑
Application Control	☑	☑	☑	☑	☑
IPS	☑	☑	☑	☑	☑
AntiVirus	☑	☑	☑	☑	☑
Virus Outbreak and Content Disarm & Reconstruct	☑	☑	☑	☑	☑
Botnet (IP/Domain)	☑	☑	☑	☑	☑
Sandbox Cloud	☑	☑	☑	☑	☑
Content Analysis	Add-on license	Add-on license	Add-on license	Add-on license	Add-on license
Client Browser Isolation	Add-on license	Add-on license	Add-on license	Add-on license	Add-on license
DLP	Add-on license	Add-on license	Add-on license	Add-on license	Add-on license

* VM02 is intended primarily for testing purposes and to act as Security Fabric Root (SFR) in large deployments where user licenses are attached to the VM02 and shared across the fabric. Hence the large user count, as licenses are expected to be shared across multiple devices.

ORDER INFORMATION

VIRTUAL MACHINE SUBSCRIPTIONS					
	VM02	VM04	VM08	VM16	VMUL
SWG Protection Bundle					
SWG Protection Bundle	FC1-10-XYVM2-514-02-DD	FC1-10-XYVM4-514-02-DD	FC1-10-XYVM8-514-02-DD	FC1-10-XYV16-514-02-DD	FC1-10-XYVUL-514-02-DD
Data Protection	FC1-10-XYVM2-1005-02-DD	FC1-10-XYVM4-1005-02-DD	FC1-10-XYVM8-1005-02-DD	FC1-10-XYV16-1005-02-DD	FC1-10-XYVUL-1005-02-DD
VDOM	FPX-VDOM-5-UG	FPX-VDOM-5-UG	FPX-VDOM-5-UG	FPX-VDOM-5-UG	FPX-VDOM-5-UG
Client Browser Isolation	FC1-10-XYVM2-587-02-DD	FC1-10-XYVM4-587-02-DD	FC1-10-XYVM8-587-02-DD	FC1-10-XYV16-587-02-DD	FC1-10-XYVUL-587-02-DD
FortiGuard DLP Service	FC1-10-XYVM2-589-02-DD	FC1-10-XYVM4-589-02-DD	FC1-10-XYVM8-589-02-DD	FC1-10-XYV16-589-02-DD	FC1-10-XYVUL-589-02-DD
24x7 Support	FC-10-XYVM2-248-02-DD	FC-10-XYVM4-248-02-DD	FC-10-XYVM8-248-02-DD	FC-10-XYV16-248-02-DD	FC-10-XYVUL-248-02-DD

The Space

Today, as attacks become more versatile, organizations need to protect their employees from infection by malicious web traffic, websites, and viruses.

Secure web gateway (SWG) addresses a set of security problems within one product. The greatest benefits of an SWG is to utilize URL filtering, advanced threat defense, and legacy malware protection to defend users from Internet-borne threats, and to help enterprises enforce Internet policy compliance.

Product Lineup

- **On-premise:** Any FortiProxy can be purchased as HW or VM. Models support 100 to 60K users. An additional license is not needed for advanced caching and WAN optimization features.
- **Cloud VM:** FortiProxy VM also runs on public cloud (AWS, Azure, and GCP). BYOL is supported.

Ordering Guide

Product Offerings:

- **FortiProxy-HW:** Hardware models should be selected by the model specific capacity to process user web browsing sessions (from 500 and up to 60,000 users). Without the SWG license, FortiProxy only performs caching and WAN optimization.
- **FortiProxy-VM:** provides yearly software subscription to run FortiProxy software as a virtual machine (VM) over a public or private cloud infrastructure. Without the SWG license, FortiProxy only performs caching and WAN optimization.
- **VDOM (HW/SW attached optional license):** VDOMs are used to divide a FortiProxy into virtual units that function independently and are assigned to a specific FortiProxy device or VM.

Seat/User software license add-ons

Seat-based licenses require a specific quote configuration based on the protected user count and number of devices. One seat based license line on a quote will only apply to 1 Serial Number (FortiProxy HW or VM device SN). If you are quoting for an order of more than 1 Device, you'll need to add as many seat based license lines on the quote as the number of devices the customer is purchasing. Multiple quantities on a quote line will multiply the number of seats on the SKU Unit Of Measure (UOM), so if you reflect quantity 2 for a SKU that has 500 seats as the UOM, you'll be receiving 1 license with 1000 seats that can only be applied to 1 device SN. The total seat UOMs, after allocated to the respective SNs, can then be shared across all the entitled devices using the FPX license sharing mechanism. If you intend to use a dedicated FortiProxy VM02 or HA Pair, you can purchase seat licenses and attach them to the VM02 and have them automatically propagate across the security fabric FortiProxy devices.

- **SWG Protection Bundle (Required license):** After choosing a hardware or virtual FortiProxy device type, add SWG Protection Bundle based on the number of users to protect spread across all the purchased devices. SWG Protection Bundle is a yearly subscription.
- **Content Analysis Service (Optional license):** an AI powered computer vision service that detects visual threats including pornography, extremism, and graphic violence. By leveraging advanced AI capabilities, the FortiProxy Content Analysis service enables security teams to restrict access to visual content not previously categorized. The Content Analysis service powers FortiProxy with OCR capabilities to be used by the DLP service.
- **Data Loss Prevention (optional license):** enables the identification, monitoring, and protection of an organization's data from data breaches and data exfiltration. FortiProxy DLP is powered by FortiGuard DLP rich library of content types and identifiable information.
- **Client Browser Isolation (optional license):** Client-based native browser isolation (NBI) uses a Docker container to isolate known and unknown malware, ransomware, and other zero-day threats within the browser.

Major Highlights

- **On-box AI engine:** helps intelligently rate on the fly and on-box images to reduce weapons, alcohol, gore, porn, extremism, and swim/underwear. This AI looks at the actual content itself on a per-image level.
- **Flexibility:** Flexible Transparent and Explicit mode deployment options are available via L2, L3, inline, and out-of-path topologies. Even more flexible than Symantec Proxy deployment mode.
- **Visibility:** with FortiView, clients can see what is happening on their networks in order to further refine policies.
- **Isolator Integration:** with Air Gap isolation solution (Fortisolator) to provide content to users in the securest manner.

Where to Find More Info

- [Demo:](#) Security Web Gateway, integration with isolation solution
- [What's New:](#) FortiProxy new features
- [Live Demo:](#) learn about FortiProxy features

NSE TRAINING AND CERTIFICATION

FortiProxy Training

Learn how to use FortiProxy features, including policy types, content analysis, and security profiles. You will also explore FortiProxy policies, deployment, user authentication, high availability, monitoring, and how to protect your web traffic using content inspection, such as IPS, antivirus, web filtering, application control, and logging. This course does not have a certification exam.

Course Description

For more information about prerequisites, agenda topics and learning objectives, please refer to the course description at https://training.fortinet.com/local/staticpage/view.php?page=library_fortiproxy.

Ordering Information

SKU	DESCRIPTION
FT-FPX	Instructor-led Training - 2 days
FT-FPX-LAB	On-demand Labs (self-paced)

Visit www.fortinet.com for more details



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 Chief Legal Officer, 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.