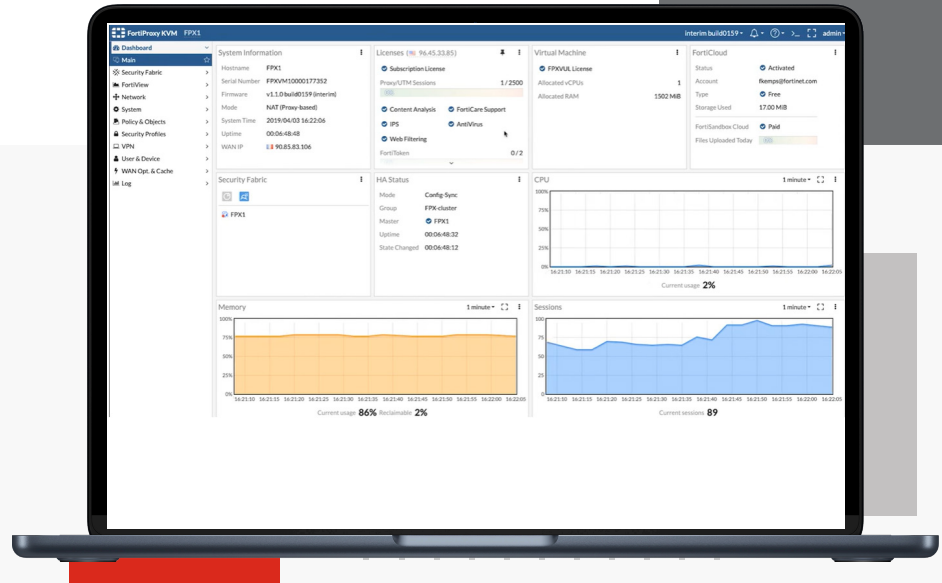


FortiProxy™



Highlights

- Advanced protection against threats
- Virtual domains high performance and scalability
- Content caching and WAN optimization

Fast, Secure, and Scalable Security for any Organization

FortiProxy is a secure web gateway that protects employees against internet-borne attacks by incorporating multiple detection techniques such as web, video, and DNS filtering, data loss prevention, antivirus, intrusion prevention, and Client Browser Isolation.

Available in



Appliance



Virtual



Cloud

Features

Advanced SSL Inspection

Powerful hardware that can perform SSL inspection to effectively remove blind spots in encrypted traffic, without compromising on performance.

Security Fabric

The Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises. FortiProxy integrates with key security fabric components such as FortiSandbox and FortiAnalyzer. It can also integrate with third-party security devices using ICAP and WCCP protocols.

High Performance, Scalability, and Low TCO

FortiProxy uses specialized ASICs in order to accelerate performance of the network and security modules. FortiProxy supports proxy speeds up to 15 Gbps, and can scale from small enterprises with 500 users all the way to larger enterprises of 50,000 users. FortiProxy provides great value to customers while maintaining a low total cost of ownership.

Advanced Protection Against Threats

- Integration with FortiGuard Threat Intelligence Service
- Web, Video, DNS filtering, and application control
- Client Browser Isolation for decreasing the attack surface
- Integration with FortiSandbox and FortiNDR cloud and on-premise appliance
- AV, IPS, DLP, and Content Analysis

High Performance and Scalability

- Custom-built security processing units for high performance
- License sharing across multiple devices (VM and HW)
- HA availability for redundancy
- Logical separation between virtual security domains

Content Caching and WAN Optimization

- Static and dynamic content caching
- Multiple Content Delivery Network
- Decrease Network Latency
- Lower bandwidth overhead



Secure Web Gateway Services

Web and Video Filtering

FortiGuard's cloud-delivered AI-driven web filtering service provides comprehensive threat protection to address threats including ransomware, credential-theft, phishing, and other web-borne attacks. It uses AI-driven behavior analysis and correlation to block unknown malicious URL's almost immediately, with near-zero false-negatives.

The Web Filtering service leverages industry-leading threat intelligence from FortiGuard labs. This is based on telemetry gathered from over 10 billion real-world events per day. FortiGuard Web Filtering has a database of hundreds of millions of URLs classified into 90+ categories to meet granular web controls and reporting. Help achieve regulatory compliance and granular video control with industry-first advanced video filtering.

DNS Filtering

Protect against sophisticated DNS-based threats including DNS tunneling, C2 server identification, and domain generation algorithms (DGAs). DNS filtering provides full visibility into DNS traffic while blocking high-risk domains including malicious newly registered domains (NRDs), parked domains, and more.

Granular and ZTNA Level Application Control

With the constant increase in the usage of social apps, it's vital for organizations to provide very granular controls. For instance, they may want to allow access but prevent specific actions like posts. FortiProxy supports all major SaaS and social websites and supports more than 3000 apps. Access can be granted or denied based on the user's group, client security posture or a combination of both. In addition, SaaS Apps can be classified using the cloud database that's maintained by FortiGuard.

Zero-Trust Browsing

Without Third party code running locally

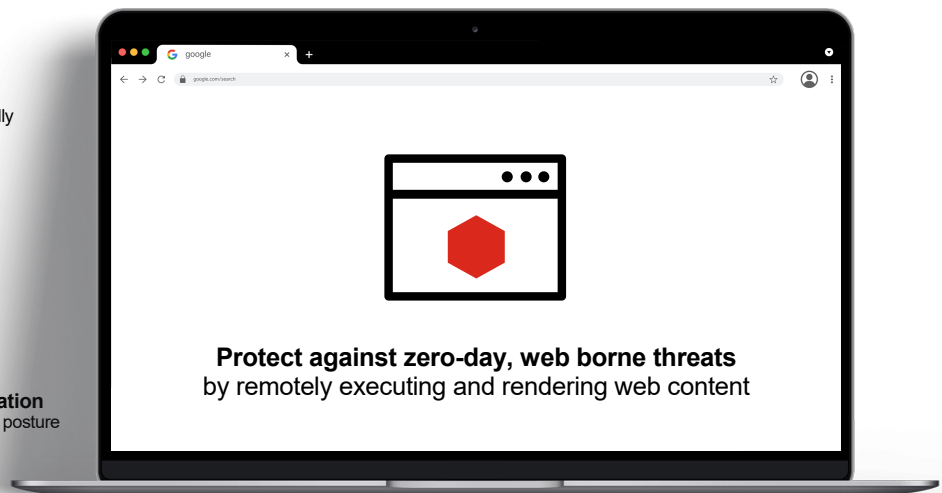
Selective Usage

for High-Risk Websites

Ability to Isolate and Freeze

Fortinet Security Fabric Integration

Seamless integration for broader web posture



Secure Web Gateway Services (continued)

Data Loss Prevention

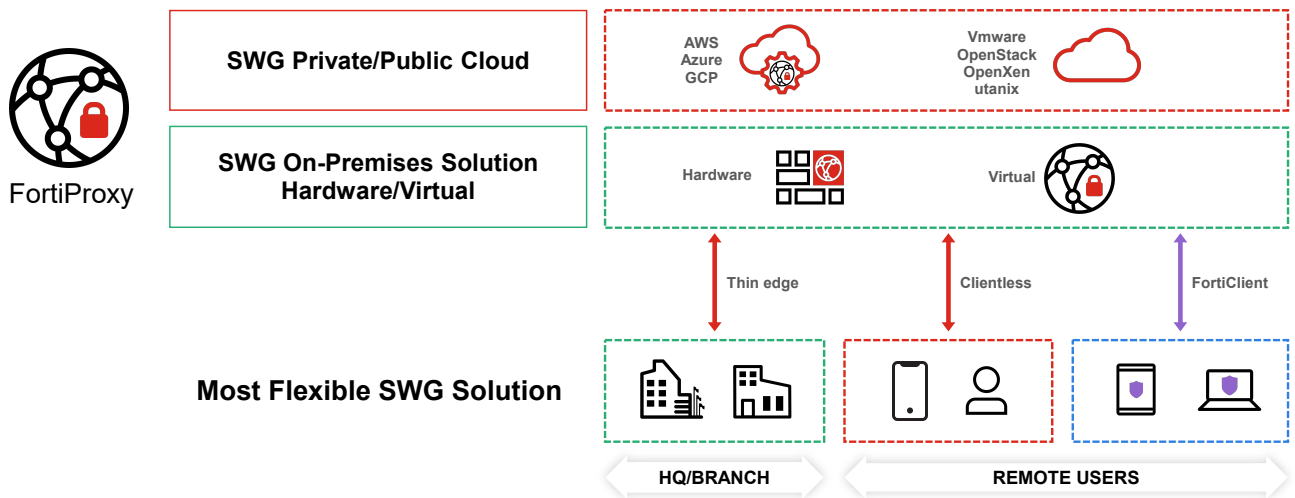
Protect sensitive data from leaving your network, ensure data privacy and regulatory compliance requirements. Sensitive files can be fingerprinted or watermarked and the outgoing traffic is examined to identify any data leakage. FortiProxy implements Optical Character Recognition to extract text from images and integrations with the FortiGuard DLP service to enhance its DLP capabilities by continuously scanning for more sensitive information patterns

Intrusion Prevention

FortiProxy uses a combination of signature as well as signature-less engines to prevent intrusions. IPS signatures can be based on exploits, known vulnerabilities or anomaly patterns. Signature-less techniques are used to detect SQL injection, domain generation algorithm attacks, java and flash exploits. FortiGuard Labs generates more than 100 IPS rules every week, blocking more than four million network intrusion attempts.

Client Browser Isolation

Client-based native browser isolation (NBI) uses a Docker container to isolate the browser from the external networks. Client browser isolation provides a full browser isolation to stop phishing, account takeover, and malware without performance overhead and without the need for SSL inspection. Windows machines with Chrome, Edge and Firefox browsers are supported.



Secure Web Gateway Services (continued)

Sandboxing

Complement with a two-step AI based sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis that quickly identifies known and emerging malware through FortiSandbox's ML powered static analysis. Second stage analysis is done in a contained environment to uncover the full attack lifecycle leveraging behavior-based ML with dynamic analysis detection engine more efficient and effective against new zero-day threats.

Content Analysis

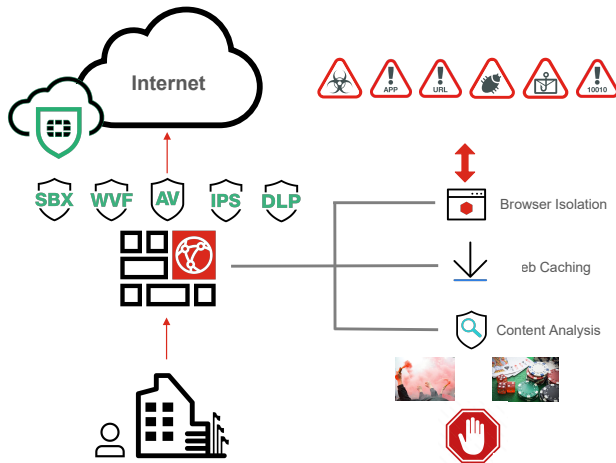
Enforce acceptable usage by detecting and preventing illicit images and videos with AI-driven content analysis. With the addition of the Content Disarm and Reconstruction service, you can reduce mean time to detection (MTTD) with low latency content sanitization. A broad range of file types are supported beyond traditional signature-based and reputation-based measures.

WAN Optimization and Advanced Caching

Today at many locations, bandwidth is a bottleneck, and to keep operation costs low, it may be prohibitive to provide additional bandwidth. In these environments, FortiProxy is also able to greatly optimize and accelerate the network by enabling caching of content and by enabling WAN Optimization features.



Use Cases



SWG Services

Methods Supported

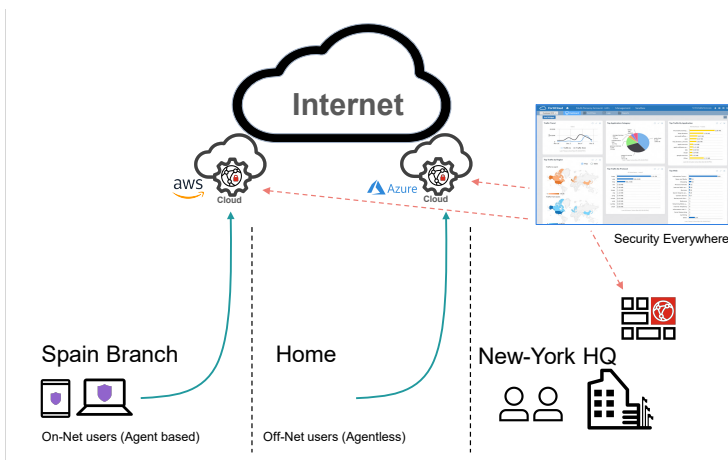
- Explicit Proxy, Transparent, PBR, and WCCP

Advanced Offering

- FortiProxy employs multiple FortiGuard services to protect users against the latest web threats and to enforce compliance
- Integration with FortiGuard Threat Intelligence Service

Benefits

- Advanced SWG Services
- Full Visibility
- All-Inclusive License
- Stackable License from 500 to 60K Users



Hybrid Cloud Solution

Methods Supported

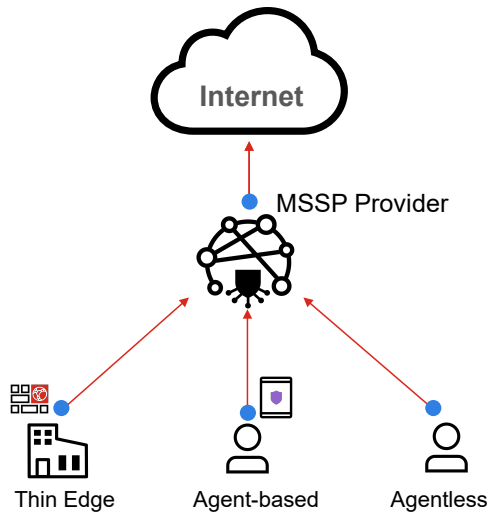
- On-prem HW/VM, Agent-based, Agentless

Advanced Offering

- Share license according to load/ time/ user
- Explicit Proxy with PAC File hosting support
- Centralized management of your FortiProxy devices from a single console

Benefits

- Auto Scaling
- Full Visibility
- Consistent Security Across all Users



Managed Security Service Providers

Methods Supported

- Thin Edge, Agent-based, Agentless

Advanced Offering

- Explicit Proxy with PAC File hosting support or VPN
- VDOM per customer - full integration and visibility

Benefits

- Easy Onboarding
- Full Visibility



Features Summary

System

- Wide range of deployment options:
 - Inline, Forward Proxy, Explicit proxy, WCCP/PBR
 - Hardware or virtual appliance
- IPv4 and IPv6 address support
- Application Support including HTTP/S
- HA available as active-active and active-backup with session synchronization
- Automation Stitches
- Virtual Domains

Threat Protection

- Integration with FortiGuard threat intelligence services for real-time threat updates
- Integration with cloud sandbox to detect advanced threats
- In-built security services requiring no additional appliance
- Web, Video, and DNS Filtering
 - Dynamic categorization of websites
 - Blocking of malicious and suspicious domains and URLs
 - Static blacklists and whitelists
- Application Control
 - Granular web application control for social websites
 - Support for 3000+ applications
- FortiGuard powered antivirus, botnet and DLP services
- Client Browser Isolation
- Virtual Domains
- Content Analysis
- Multiple ICAP servers support
- IPS signature and filters
- Web Rating Override
- SSL/SSH Inspection
- Custom Application Signature

Authentication

- Support for various authentication modes including Radius, SAML, LDAP, NTLM, Kerberos, FortiToken One-Time Password
- In-built authentication requiring no additional device

Advanced Caching

- Web and video caching
- Reverse web cache
- Traffic Shaping and QoS policies to prioritize Apps
- Dynamic adaptive streaming over HTTP
- Dynamic adaptive streaming over RTP and RTMPT

WAN Optimization

- Protocol Optimization – support HTTP, MAPI, CIFS, FTP, and TCP
- Secure tunneling over across WAN
- Wan Optimization Peers

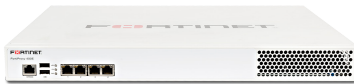
Management and Reporting

- FortiView Integration
- FortiAnalyzer Integration
- Support Syslog Server
- Granular Role-based Access
- Reporting and Logging
- Policy tests for ease of deployment



Specifications

	FORTIPROXY 400G	FORTIPROXY 2000G	FORTIPROXY 4000G
System Information			
License Capacity	500–6,000 users	500–20,000 users	500–60,000 users
Deployment Modes	Inline Proxy, Transparent/WCCP Proxy, Explicit Proxy, Routed Proxy		
Virtual Domain	up to 10 VDOM	up to 100 VDOM	up to 250 VDOM
Hardware Specifications			
Memory	16 GB	128 GB	256 GB
Management	HTTP/S, SSH, CLI, SNMP, Console RJ45	HTTP/S, SSH, CLI, SNMP, Console RJ45	HTTP/S, SSH, CLI, SNMP, Console RJ45
Network Interfaces	4x GE RJ45	2x 10 GE SFP+, 2x GE SFP ports, 4x GE RJ45 ports	4x 10 GE SFP+, 2x GE SFP ports, 4x GE RJ45 ports
Bypass Interfaces	-	2x GE RJ45 ports	2x GE RJ45 ports
Storage	4 TB (2 TB x2) Hard Disk	8 TB (2 TB x4) Hard Disk	8 TB (2 TB x4) Hard Disk
Power Supply	Single (Optional Dual)	Dual	Dual
Environment			
Form Factor	1U Appliance	2U Appliance	2U Appliance
Input Voltage	100–240V, AC 60–50 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	120 W / 151 W	289 W / 353 W	549 W / 670 W
Maximum Current	100V/5A, 240V/3A	100V/7.5A, 240V/3.9A	100V/10A, 240V/5A
Heat Dissipation	550 BTU/h	1,238 BTU/h	2,321 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°–158°F (-25°–70°C)	-13° to 158°F (-25° to 70°C)	-13° to 158°F (-25° to 70°C)
Humidity	5%–95% non-condensing	8%–90% non-condensing	10%–90% non-condensing
Dimensions			
Height x Width x Length (inches)	1.73 × 17.24 × 16.38	3.5 × 17.2 × 31.9	3.5 × 17.2 × 31.9
Height x Width x Length (mm)	44 × 438 × 416	88 × 445 × 810	88 × 445 × 810
Weight	25 lbs (11 kg)	43 lbs (19.4kg)	46 lbs (21kg)
Compliance			
Safety	FCC, ICES, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB		



FortiProxy 400G



FortiProxy 2000G



FortiProxy 4000G

VIRTUAL APPLIANCE	FORTIPROXY VM02	FORTIPROXY VM04	FORTIPROXY VM08	FORTIPROXY VM16	FORTIPROXY VMUL
System Information					
Hypervisor Support	VMware ESX/ESXi, KVM Platform, Microsoft HyperV	VMware ESX/ESXi, KVM Platform, Microsoft HyperV	VMware ESX/ESXi, KVM Platform, Microsoft HyperV	VMware ESX/ESXi, KVM Platform, Microsoft HyperV	VMware ESX/ESXi, KVM Platform, Microsoft HyperV
License Capacity	100–500 users	100–2,500 users	100–10,000 users	100–25,000 users	100–50,000 users
Virtual Domain	up to 10 VDOM	up to 25 VDOM	up to 50 VDOM	up to 100 VDOM	up to 500 VDOM
Hardware Specifications					
Storage	4 CPU, Unlimited GB RAM, 2 Disk	8 CPU, Unlimited GB RAM, 2 Disk	16 CPU, Unlimited GB RAM, 4 Disk	32 CPU, Unlimited GB RAM, 8 Disk	Unlimited CPU, Unlimited GB RAM, 16 Disk
Network Interface Support (Maximum)	10	10	10	10	10
Management	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP	HTTP/S, SSH, CLI, SNMP



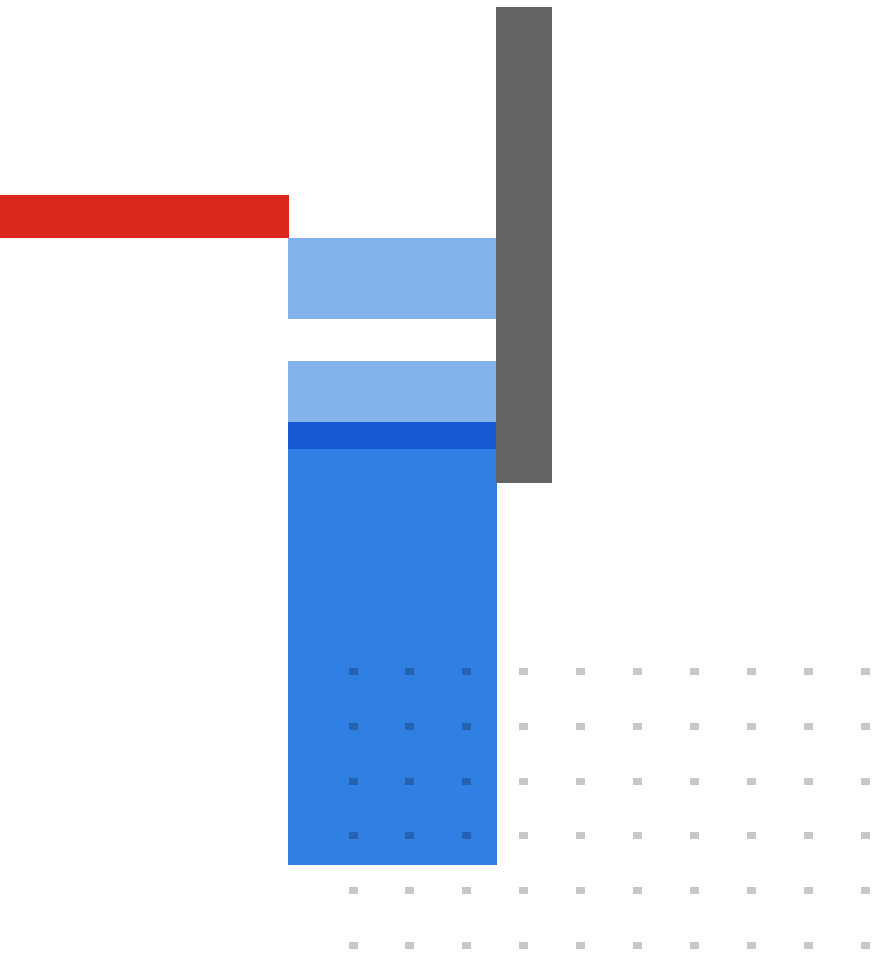
Ordering Information

Product	SKU	Description
FortiProxy 400G	FPX-400G	FortiProxy 400G, 4x GE RJ45 (up to 6,000 users).
FortiProxy 2000G	FPX-2000G	FortiProxy 2000G, 2x RJ45 GE, 2x RJ45 GE Bypass, 2x SFP GE, 2x SFP+ 10 GE (up to 20 000 users).
FortiProxy 4000G	FPX-4000G	FortiProxy 4000G, 4x 10/100/1000 RJ45 Ports, 2x 10/100/1000 RJ45 Bypass Ports, 2x GE SFP Ports, 4x 10 GE SFP+ Ports (up to 60 000 users).
SWG Protection Bundle	FC-10-XY400-514-02-DD FC-10-XY2KE-514-02-DD FC-10-XY4KE-514-02-DD	SWG Protection Bundle [Web Filtering, DNS Filtering, Application Control, DLP, AV, Botnet (IP/Domain), Sandbox Cloud] 500 User license with SWG Protection.
Content Analysis	FC-10-XY400-160-02-DD FC-10-XY2KE-160-02-DD FC-10-XY4KE-160-02-DD	500 User license with Content Analysis Service.
Client Browser Isolation	FC1-10-XY400-587-02-DD FC1-10-XY2KE-587-02-DD FC1-10-XY4KE-587-02-DD	Client Browser Isolation. 500 user license - Support Windows10 and Chrome.
FortiProxy-VM02	LIC-FPRXY-VM02	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 4x vCPU core, unlimited GB RAM, and 2 TB Disk.
FortiProxy-VM04	LIC-FPRXY-VM04	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 8x vCPU core, unlimited GB RAM, and 4 TB Disk.
FortiProxy-VM08	LIC-FPRXY-VM08	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 16x vCPU core, unlimited GB RAM, and 8 TB Disk.
FortiProxy-VM16	LIC-FPRXY-VM16	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. 32x vCPU core, unlimited GB RAM, and 8 TB Disk.
FortiProxy-VMUL	LIC-FPRXY-VMUL	FortiProxy-VM software virtual appliance designed for VMware ESX/ESXi platforms and KVM platform. Unlimited vCPU and RAM support.
Virtual Domain License Add 5	FPX-VDOM-5-UG	Upgrade license for adding 5 VDOMs to FortiProxy 7.2 and later, limited by VM maximum VDOM capacity.
FortiProxy 400G PSU	SP-FAD400F-PS	Optional Redundant Power Supply Unit for FortiProxy 400G.

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.