

Fortinet Virtual FortiGate Security Appliance on IBM Cloud

Best-of-breed security for cloud workloads with comprehensive NGFW (next generation firewall) capabilities



Highlights

Comprehensive security for network, application and web traffic

Secure hybrid, multifeatured cloud firewall

Cloud infrastructure visibility and control

Secure access VPN (Virtual Private Networking)

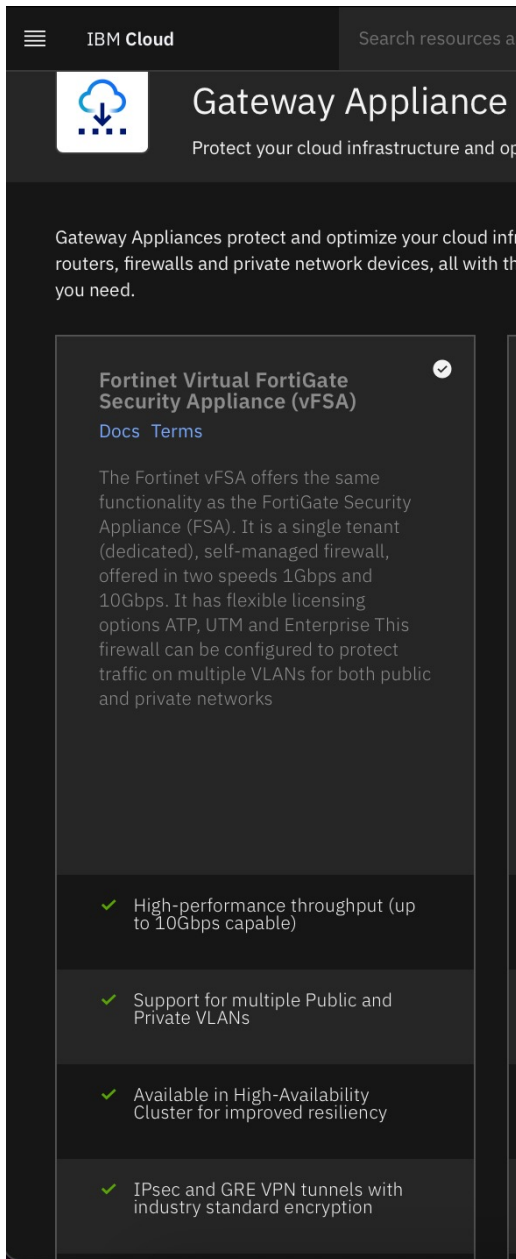
Intent-based segmentation

Ready for production workloads with managed licensing and complete administrative access

The vFSA (Virtual FortiGate Security Appliance) provides a scalable, portable version of the industry-leading Fortinet FortiGate next generation firewall appliance, allowing enterprises to implement the same comprehensive protection capabilities provided by Fortinet's hardware firewalls. This allows enterprises to avoid architectures with point solutions and network tromboning, making it possible to put firewall capabilities where they are needed for a truly distributed and secure network architecture. Fortinet's solutions encompass multiple workloads and use cases – Application Delivery, Email Security, SIEM (Security Information and Event Management), WAF (Web Application Firewall) – all of which are accessible through the FortiFlex licensing system.

Coupled with IBM Cloud's industry-standard, compliant and highly available public and hybrid cloud offerings, the vFSA offers financial institutions, enterprises and security-conscious cloud consumers with an immediate, comprehensive answer to security concerns with broad-spectrum protection.

Adding market leading managed next-generation firewall capabilities to the most secure financial services cloud in the industry.



Key Features

Secure hybrid cloud

FortiGate Next-Generation Firewalls (NGFWs) and cloud security solutions offer best-of-breed secure connectivity, network segmentation, and application security for hybrid cloud-based deployments. FortiGate NGFWs provide centralized, consistent security policy enforcement using high-speed VPN tunnel connections. FortiGate VMs deployed in the public cloud can securely communicate and share consistent policies with FortiGate NGFWs of any form factor provisioned in a private data center.

Cloud infrastructure visibility and control

The vFSA can protect all cloud components—such as configurations, user activity, and traffic flow logs. They also support compliance reporting requirements.

Secure access VPN

Remote access virtual private networks (VPNs) enable the use of cloud-based applications. The Fortinet Security Fabric delivers best-in-class performance for securing VPN traffic when remotely accessing IBM Cloud. By leveraging IBM's multiregional global infrastructure, organizations can instantaneously scale their services and offer remote access VPN termination close to the end-user.

Intent-based segmentation

Segmenting cloud environments presents challenges because dynamic provisioning results in constantly changing IP addresses. FortiGate VMs provide intent-based segmentation, which builds rules and segments based on user identity and business logic. Rules are adjusted dynamically in response to a continuous trust assessment. As a result, FortiGates can intuitively define which workloads and elements in the cloud are allowed to communicate with other workloads and elements, whether they are inside or outside the cloud.

Comprehensive Security for Network, Application and Web

The FortiGate virtual appliance brings many of the key benefits of hardware firewalls in a virtual form factor, providing a host of security capabilities beyond network firewalling. These capabilities include comprehensive web application security, Layer-7 firewalling and access control capabilities, intelligent/behavioral security, zero-day protections, threat intelligence feeds and URL and IP whitelisting/blacklisting.

A leader on the Gartner Firewall MQ, the FortiGate NGFW from Fortinet offers the highest level of protection against sophisticated cyber threats on the market today. It identifies, controls, and safely enables hybrid cloud workloads while simultaneously inspecting content for all threats and leverages dynamic and reactive adaptability to deliver exceptional service velocity.

Tested, standardized and dedicated VSI (Virtual Server Instance) profiles on IBM Cloud enable predictable, stable operations with a clear understanding of performance capabilities for scale planning. Dedicated infrastructure and IP addressing removes the security risk with resource sharing inherent in the shared infrastructure often used for virtual appliances.

Licensing Options

Three licensing options for different enterprise use cases

The vFSA is offered with three licensing options – Advanced Threat Protection (ATP), Unified Threat Management (UTM) and Enterprise. The features supported with each option are described below -

License Name	Features/Security Services
Advanced Threat Protection (ATP)	Application control Geo IP Updates Device/OS Detection IoT Mac Database Trusted Certificate Database Internet Service (SaaS) Database DDNS (v4/v6) Advanced Malware Protection (AMP) Antivirus Botnet Mobile Malware FortiGate Cloud Sandbox
Unified Threat Management (UTM)	All ATP Features/Security Services Web Security Web and Content Filtering Secure DNS Filtering Video Filtering AntiSpam
Enterprise	All UTM Features/Security Services IOT Query Service OT Protocol Service Security Fabric Rating and Compliance Monitoring FortiConverter Service

Adding market leading managed next-generation firewall capabilities to the most secure financial services cloud in the industry.

Conclusion

The IBM Cloud Virtual FortiGate Appliance delivers a scalable, secure and highly available firewalling solution that gives performance comparable to hardware form-factor appliances, while delivering flexibility through the ability to provision across all locations on IBM Cloud. With no risk of hardware turnover, the IBM Cloud vFSA offers unlimited upgradeability and continued availability for customers.

Why IBM?

- **Dedicated by Design:** the vFSA on IBM Cloud is Dedicated by Design; resources allocated to the vFSA are not shared, ensuring backend security and stability.
- **Strong IBM-Fortinet partnership:** IBM is an Expert tier FortiPartner, with deep expertise with Fortinet technologies. IBM and Fortinet share a lengthy partnership with many successful co-innovations and mutual partnership program involvements.
- **Cost-effective, global availability:** the vFSA offers a value-driven virtual firewall option for current Fortinet customers and new users looking for a globally available, feature-rich and cost-effective firewalling solution.
- **Provision-and-Run firewalls with no license management challenges:** the IBM Cloud vFSA allows customers to provision fully licensed firewalls that are ready to protect their critical infrastructure from Minute Zero.

For more information

To learn more about the Fortinet Virtual FortiGate Security Appliance on IBM Cloud, contact your IBM representative or IBM Business Partner, or visit cloud.ibm.com

© Copyright IBM Corporation 2024
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
April 2024

IBM, the IBM logo, and IBM Cloud are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

