Saved from manuals.plus.
Open the live page for links to other documents and user manuals.

FORTINET FortiGate-VM04

Fortinet FortiGate-VM Virtual Appliance User Manual

Model: FortiGate-VM04

Brand: FORTINET

The Fortinet Virtual Appliance logo, featuring the brand name 'FORTINET' in bold black letters with a red square grid icon, and 'VIRTUAL APPLIANCE' below it, signifying the product type.

1. Product Overview

The Fortinet FortiGate-VM is a virtual appliance designed to provide comprehensive network security functions across various supported virtualized platforms. It offers the same robust security features as physical FortiGate appliances, including firewall, VPN, intrusion prevention, and more, but in a flexible, software-defined form factor.
This virtual appliance is configured with 4 vCPU cores and supports up to 6 GB of RAM, making it suitable for a wide range of deployment scenarios from small businesses to enterprise environments requiring scalable security solutions.

2. Setup and Installation

Setting up the FortiGate-VM involves deploying the virtual appliance image onto a compatible hypervisor environment. This process typically includes downloading the appropriate virtual machine image (e.g., OVF, VHD, QCOW2) from the Fortinet support portal and importing it into your virtualization platform.

2.1 Prerequisites

- Compatible hypervisor (e.g., VMware ESXi, Microsoft Hyper-V, KVM, Citrix XenServer).
- Sufficient hardware resources on the host server (CPU, RAM, storage, network interfaces).
- Network configuration details (IP addresses, subnet masks, gateway, DNS).
- Fortinet support account for image download and license activation.

2.2 Initial Deployment Steps

1. **Download VM Image:** Obtain the FortiGate-VM image file specific to your hypervisor from the Fortinet support website.
2. **Import/Deploy:** Use your hypervisor's management interface to import or deploy the downloaded VM image.
3. **Allocate Resources:** Configure the virtual machine's resources, ensuring 4 vCPU cores and at least 6 GB of

RAM are allocated.

4. **Network Configuration:** Map virtual network adapters to physical or virtual networks as required for your deployment.
5. **Power On:** Start the FortiGate-VM.
6. **Initial Configuration:** Access the FortiGate-VM console (via hypervisor console or SSH) to perform initial network configuration and set up administrative access.
7. **License Activation:** Apply the FortiGate-VM license key. This is crucial for full functionality and updates.



An image depicting a black box with 'FORTINET Activation Key' printed on it, alongside the Fortinet red square grid logo, symbolizing the software license required for the virtual appliance.

3. Operating the FortiGate-VM

Once deployed and licensed, the FortiGate-VM operates similarly to a physical FortiGate appliance. Management is primarily performed through its web-based graphical user interface (GUI) or command-line interface (CLI).

3.1 Key Operational Areas

- **Network Configuration:** Configure interfaces, routing, and VLANs to integrate the FortiGate-VM into your network infrastructure.
- **Firewall Policies:** Define security policies to control traffic flow between different network segments and the internet.
- **VPN:** Set up IPsec or SSL VPNs for secure remote access or site-to-site connectivity.
- **Security Profiles:** Enable and configure features like Antivirus, Intrusion Prevention System (IPS), Web Filtering, Application Control, and Data Loss Prevention (DLP).
- **User Authentication:** Integrate with directory services (e.g., LDAP, RADIUS) for user authentication.
- **Logging and Monitoring:** Utilize the extensive logging and reporting capabilities to monitor network activity and security events.

For detailed configuration and advanced features, refer to the official FortiGate documentation available on the Fortinet support website.

4. Maintenance

Regular maintenance is essential to ensure the optimal performance and security of your FortiGate-VM.

4.1 Recommended Maintenance Tasks

- **Firmware Updates:** Regularly check for and apply the latest FortiGate-VM firmware updates to benefit from new features, bug fixes, and security enhancements.
- **Security Definition Updates:** Ensure FortiGuard services (Antivirus, IPS, Web Filtering, etc.) are up-to-date to protect against the latest threats.
- **Configuration Backups:** Periodically back up your FortiGate-VM configuration to a secure location. This allows for quick recovery in case of data loss or misconfiguration.
- **Resource Monitoring:** Monitor the virtual machine's CPU, memory, and disk usage within your hypervisor to

ensure adequate resources are available.

- **Log Review:** Regularly review system logs and security logs for unusual activity or potential issues.

5. Troubleshooting

This section provides basic troubleshooting steps for common issues encountered with the FortiGate-VM.

5.1 Common Issues and Solutions

- **No Network Connectivity:**
  - Verify virtual network adapter mappings in the hypervisor.
  - Check FortiGate-VM interface IP configuration (IP address, subnet mask, gateway).
  - Ensure firewall policies allow the necessary traffic.
- **Slow Performance:**
  - Check CPU and memory utilization on the FortiGate-VM and the host hypervisor.
  - Ensure sufficient resources are allocated to the VM.
  - Review FortiGate-VM session table and resource usage from the CLI (`diagnose sys top`).
- **Cannot Access Web GUI:**
  - Confirm the FortiGate-VM is powered on and has an IP address.
  - Ensure HTTP/HTTPS access is enabled on the management interface.
  - Check for any local firewall rules on the client preventing access.
- **FortiGuard Updates Failing:**
  - Verify DNS resolution and internet connectivity from the FortiGate-VM.
  - Ensure the FortiGate-VM license is valid and active.
  - Check FortiGuard server reachability.

For more complex issues, consult the Fortinet troubleshooting guides or contact Fortinet support.

6. Specifications

Attribute	Value
Model Number	FortiGate-VM04
Manufacturer	FORTINET
vCPU Cores	4
RAM (Maximum)	Unlimited (up to 6 GB recommended for typical deployments)
Computer Memory Size	6 GB
RAM Memory Technology	DDR (Virtual)

Compatible Devices	Desktop, Server, Laptop (referring to host systems for virtualization)
Item Weight	1 pounds (virtual appliance, refers to conceptual weight)
Special Feature	Lightweight (virtual footprint)
ASIN	B07G8R43DK
Date First Available	August 7, 2018

7. Warranty and Support

Fortinet provides comprehensive support services and security subscriptions to ensure the continuous operation and protection of your FortiGate-VM.

7.1 FortiCare Support Services

FortiCare services offer technical support, hardware replacement (where applicable for physical devices, or software support for VMs), and access to Fortinet's knowledge base.

FortiCare 8x5 Service

Get access to technical support via the web portal, online chat system, and telephone during business hours (8 hours a day, 5 days a week). Includes fast and easy written access to technical support requests.

FortiCare 24x7 Service

Provides round-the-clock access to mission-critical support services (24 hours a day, 7 days a week, 365 days a year). This service is designed for environments requiring continuous technical assistance.

FortiCare 360 Service

FortiCare 360 Advanced Services Technical Support combines Fortinet's cloud-based analytics with premium support to enable organizations to proactively detect and remediate potential security and performance issues.



An image illustrating the three tiers of FortiCare Support Services: 8x5, 24x7, and 360, each represented by a laptop icon with a clock or circular arrow symbol, and accompanied by a brief description of the service level.

7.2 Security Subscriptions (FortiGuard Services)

FortiGuard services provide real-time threat intelligence and security updates to protect against evolving cyber threats. These subscriptions are critical for maintaining a strong security posture.



An image titled 'Security Subscriptions' with a background of network diagrams, describing how new cyber threats emerge and how FortiGuard Labs provides up-to-the-minute threat intelligence and countermeasures. It lists key benefits like up-to-the-minute threat intelligence, insight into threats, fast and comprehensive intelligence, high fidelity processes, prevention of new avenues of attack, and top-rated effectiveness.

Key FortiGuard Subscription Options:

- **Next Generation Application Control and IPS:** Provides application identification and control, along with intrusion prevention against known exploits.
- **Antivirus:** Detects and blocks malware, including viruses, spyware, and ransomware.
- **Antispam:** Filters unwanted email (spam) and phishing attempts.
- **Botnet IP and Reputation:** Blocks communication with known malicious IP addresses and botnet command-and-control servers.
- **Mobile Security Service:** Protects mobile devices from threats.
- **Web Filtering:** Controls access to websites based on categories and reputation.
- **Web Application Security Service:** Protects web applications from various attacks.
- **Vulnerability Scan:** Helps identify vulnerabilities on endpoints and in applications.
- **Database Security Control:** Provides security for databases.
- **Advanced Threat Protection (FortiSandbox Cloud):** Offers advanced threat detection and analysis using sandboxing technology.



An image detailing various FortiGuard subscription options, each with an icon and a brief description, including Next Generation Application Control and IPS, Antivirus, Antispam, Botnet IP and Reputation, Mobile Security Service, Web Filtering, Web Application Security Service, Vulnerability Scan, Database Security Control, and Advanced Threat Protection.

© 2023 FORTINET. All rights reserved. This manual is for informational purposes only.

Ask a question about this manual

Ask about setup, troubleshooting, compatibility, parts, safety, or missing instructions. Manuals+ will review the question and use this page's manual context to help answer it.

Name

Anonymous

Email

you@example.com

After a successful submission, we securely hash the supplied account or form email before sending it to Microsoft Advertising for conversion attribution. Privacy details.

Question

Example: How do I reset this device or fix this error?

Details

Model number, symptoms, what you tried, or the section of the manual you are using.

Submit question

Open the live page

https://manuals.plus/asin/B07G8R43DK

More documents and user manuals: **https://manuals.plus/**