FORTINET FC-10-FVM02-929-02-12

Fortinet FortiGate-VM02 Advanced Threat Protection User Manual

Brand: FORTINET | **Model:** FC-10-FVM02-929-02-12

Comprehensive guide for your FortiGate-VM02 Advanced Threat Protection service bundle.

1. Product Overview

The Fortinet FortiGate-VM02 Advanced Threat Protection (ATP) bundle is a comprehensive security solution designed to protect virtualized environments. This specific bundle includes a 1-year subscription to 24x7 FortiCare Plus services, along with Application Control, Intrusion Prevention System (IPS), Antivirus (AV), and FortiSandbox Cloud capabilities. It provides robust, multi-layered security against a wide range of cyber threats, ensuring the integrity and availability of your virtual infrastructure.

This service bundle is delivered as a virtual appliance license and associated security services, offering flexibility and scalability for your network security needs.

Image 1.1: Fortinet Virtual Appliance Logo. This image displays the Fortinet logo with "VIRTUAL APPLIANCE" text below it, indicating the nature of the product.

Image 1.2: Fortinet Activation Key Box. This image shows a black box with the Fortinet logo and "Activation Key" text, representing the physical or digital delivery of the product license.

2. Key Features and Services

The FortiGate-VM02 ATP bundle provides a robust suite of security features and support services:

- **24x7 FortiCare Plus:** Provides round-the-clock technical support, including web portal, online chat, and telephone assistance. It also includes advanced replacement service for hardware failures, ensuring minimal downtime.
- **Application Control:** Enables granular control over network applications, allowing administrators to identify, monitor, and block unwanted or malicious applications.
- **Intrusion Prevention System (IPS):** Protects against known and unknown threats by detecting and preventing malicious network activity, exploits, and vulnerabilities.
- **Antivirus (AV):** Offers real-time protection against viruses, malware, spyware, and other malicious content by scanning files and traffic.
- **FortiSandbox Cloud:** Provides advanced threat detection by executing suspicious files in a secure, isolated environment to identify zero-day threats and advanced persistent threats (APTs) before they can impact your

network.

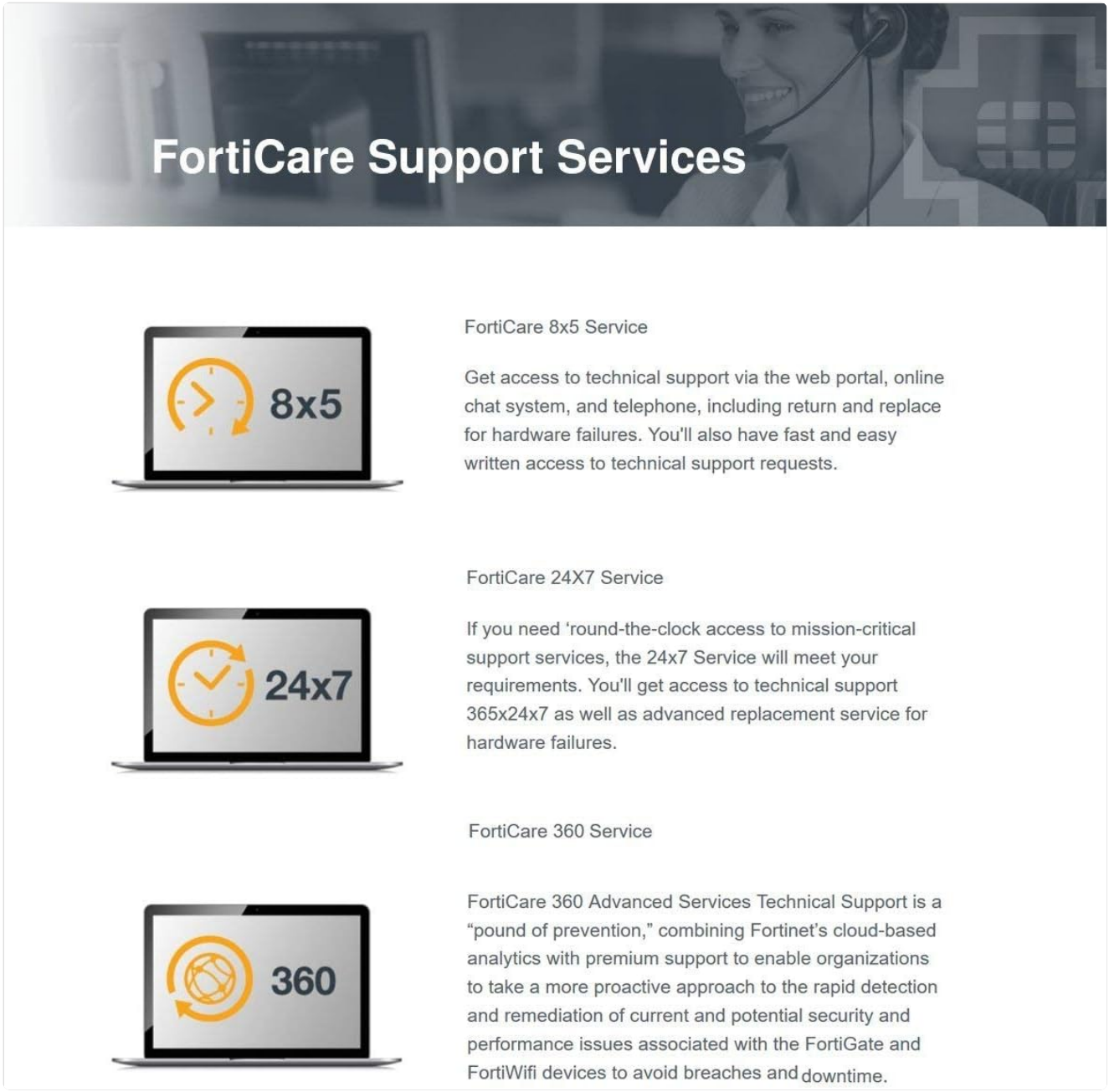

Image 2.1: FortiCare Support Services Overview. This image illustrates the different tiers of FortiCare support: 8x5, 24x7, and 360, detailing their respective service levels.

Image 2.2: Security Subscriptions Overview. This image provides a general description of FortiGuard security subscriptions, emphasizing their role in providing up-to-the-minute threat intelligence and comprehensive protection.

Image 2.3: FortiGuard Subscription Options. This image details various FortiGuard subscription services, including Next Generation Application Control, Web Filtering, Antivirus, Web Application Security, Antispam, Vulnerability Scan, Botnet IP, Database Security, Mobile Security, and Advanced Threat Protection (FortiSandbox Cloud).

3. Setup and Activation

Setting up your FortiGate-VM02 Advanced Threat Protection bundle involves several key steps, primarily focusing on the virtual appliance deployment and service activation.

1. **Virtual Appliance Deployment:**
    - Download the appropriate FortiGate-VM image for your virtualization platform (e.g., VMware ESXi, Microsoft Hyper-V, KVM, Xen).

- Deploy the virtual appliance according to the specific instructions for your chosen hypervisor. This typically involves importing the OVF/OVA file or creating a new virtual machine and attaching the virtual disk.
- Configure the virtual machine's network interfaces to connect to your network segments.

2. **Initial Configuration:**
   - Access the FortiGate-VM console via your hypervisor or SSH.
   - Configure basic network settings, including IP address, subnet mask, default gateway, and DNS servers.
   - Set up administrative access (username and password).
3. **License Activation:**
   - Register your FortiGate-VM02 serial number on the Fortinet Support Portal (support.fortinet.com).
   - Upload the license file to your FortiGate-VM through the web-based manager or CLI. This will activate your FortiCare Plus and ATP services.
   - Ensure the FortiGate-VM has internet connectivity to validate the license and receive FortiGuard updates.
4. **Service Configuration:**
   - Once licensed, configure security policies, firewall rules, VPNs, and other network settings as required for your environment.
   - Enable and configure Application Control, IPS, Antivirus, and FortiSandbox Cloud features through the FortiGate web-based manager.

For detailed, step-by-step instructions specific to your virtualization platform, please refer to the official Fortinet documentation available on their support website.

4. Operating the FortiGate-VM02 ATP

Operating your FortiGate-VM02 ATP involves continuous monitoring, policy management, and threat response.

- **Web-based Manager (GUI):** Access the FortiGate-VM through its web interface for intuitive configuration, monitoring, and reporting. This is the primary interface for most administrative tasks.
- **Command Line Interface (CLI):** For advanced configurations, scripting, and troubleshooting, the CLI provides direct access to the FortiGate's underlying system.
- **Security Policies:** Define and manage firewall policies to control traffic flow, apply security profiles (Application Control, IPS, AV), and enable FortiSandbox inspection.
- **Monitoring and Logging:** Regularly review logs, alerts, and reports to identify security incidents, monitor network activity, and assess the effectiveness of your security policies. FortiView provides real-time visibility into network and security events.
- **FortiGuard Updates:** Ensure your FortiGate-VM is configured to receive automatic FortiGuard updates for IPS signatures, antivirus definitions, web filtering categories, and application control databases. These updates are crucial for protection against the latest threats.

5. Maintenance and Best Practices

Regular maintenance is essential to ensure the optimal performance and security of your FortiGate-VM02 ATP.

- **Firmware Updates:** Periodically check for and apply the latest FortiGate firmware updates. Firmware updates often include new features, performance improvements, and critical security patches. Always review release

notes before upgrading.

- **Configuration Backups:** Regularly back up your FortiGate-VM configuration. This allows for quick recovery in case of misconfiguration or system failure.
- **Policy Review:** Periodically review your security policies to ensure they align with your current network requirements and security posture. Remove any unnecessary or redundant policies.
- **Resource Monitoring:** Monitor the virtual machine's resource utilization (CPU, memory, disk I/O) to ensure it has sufficient resources to handle network traffic and security processing.
- **Security Audits:** Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in your configuration.
- **User Management:** Implement strong password policies and use role-based access control (RBAC) for administrative accounts. Regularly review and revoke access for inactive users.

6. Troubleshooting Common Issues

This section provides general guidance for troubleshooting common issues with your FortiGate-VM02 ATP.

- **Connectivity Issues:**
  - Verify network cable connections (virtual NICs).
  - Check IP address, subnet mask, and default gateway settings.
  - Ensure firewall policies allow the necessary traffic.
  - Check ARP tables and routing tables.
- **License Not Active:**
  - Ensure the FortiGate-VM has internet access to reach FortiGuard servers.
  - Verify the license file was correctly uploaded and applied.
  - Check the serial number registration on the Fortinet Support Portal.
- **Slow Performance:**
  - Monitor CPU and memory utilization on the FortiGate-VM and the host hypervisor.
  - Ensure sufficient virtual machine resources are allocated.
  - Review security policies for overly complex rules or excessive logging.
- **FortiGuard Updates Failing:**
  - Verify DNS resolution and internet connectivity from the FortiGate-VM.
  - Check firewall policies to ensure FortiGuard traffic is allowed (ports 53, 80, 443).
  - Confirm license is active and valid.

For more in-depth troubleshooting, consult the Fortinet documentation, knowledge base, or contact FortiCare support.

7. Specifications

Attribute	Value
Model Number	FC-10-FVM02-929-02-12

Attribute	Value
Manufacturer	Fortinet
ASIN	B07BSRLNS2
Item Weight	1 pounds (*Note: This refers to the packaging/documentation, as the product is virtual*)
Date First Available	June 3, 2018
Product Type	Virtual Appliance License with Service Bundle
Included Services	1 Year 24x7 FortiCare Plus, Application Control, IPS, AV, FortiSandbox Cloud

8. Support and Warranty Information

Your Fortinet FortiGate-VM02 Advanced Threat Protection bundle includes comprehensive support and options for extended coverage.

8.1. FortiCare Support

This bundle includes **1 Year of 24x7 FortiCare Plus**. This service provides:

- **Technical Support:** Access to Fortinet's technical support team via web portal, online chat, and telephone, 24 hours a day, 7 days a week.
- **Firmware Upgrades:** Access to all major and minor firmware upgrades.
- **Advanced Replacement:** Expedited replacement of eligible hardware in case of failure (though less relevant for a virtual appliance, it applies to underlying physical FortiGate units if this were a hardware bundle).
- **FortiGuard Updates:** Continuous updates for threat intelligence, including antivirus definitions, IPS signatures, web filtering, and application control databases.

For support, visit the official Fortinet Support Portal:https://support.fortinet.com

8.2. Protection Plans

Additional protection plans may be available to extend or enhance your coverage:

- **4-Year Protection Plan:** An extended warranty or service plan for 48 months. This typically covers product defects or service continuity beyond the initial included period.
- **Complete Protect:** A comprehensive plan that may cover multiple eligible purchases, often offered on a monthly subscription basis.

Please refer to the specific terms and conditions of any additional protection plans purchased, as they are separate from the included FortiCare service.