WatchGuard T115-W

WatchGuard Firebox T115-W User Manual

Model: T115-W (WGT116031)

1. INTRODUCTION

This manual provides essential information for the installation, configuration, and operation of your WatchGuard Firebox T115-W tabletop firewall. The Firebox T115-W is designed to deliver robust security and performance for solo professionals and micro-offices, featuring Wi-Fi 7 connectivity and a silent, fanless design.
It includes a 1-Year Basic Security Suite license, offering foundational protections such as intrusion prevention, gateway antivirus, URL filtering, and spam blocking.

2. PRODUCT OVERVIEW

The WatchGuard Firebox T115-W is a compact, high-performance security appliance engineered for small environments. Its fanless operation ensures silent deployment, making it suitable for noise-sensitive areas. The device integrates Wi-Fi 7 for wireless connectivity and features multiple Gigabit Ethernet ports for wired connections.

Figure 2.1: Front view of the WatchGuard Firebox T115-W. This image shows the compact red chassis with indicator lights and ports.

WatchGuard Security Services

WatchGuard offers the most comprehensive portfolio of network security services, from traditional IPS, GAV, application control, spam blocking, and web filtering to more advanced services for protecting against advanced malware, ransomware, and the loss of sensitive data. WatchGuard also offers a full suite of network visibility and management services.

FUNDAMENTAL SECURITY SERVICES

INTRUSION PREVENTION SERVICE (IPS)
IPS uses continually updated signatures to scan traffic on all major protocols to provide real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.

REPUTATION ENABLED DEFENSE SERVICE (RED)
A powerful, cloud-based reputation lookup service that protects web users from malicious sites and botnets, while dramatically improving web processing overhead.

NETWORK DISCOVERY
A subscription-based service for Firebox appliances that generates a visual map of all nodes on your network so you can easily see where you may be at risk.

WEBBLOCKER URL FILTERING
In addition to automatically blocking known malicious sites, WebBlocker's granular content and URL filtering tools enable you to block inappropriate content, conserve network bandwidth, and increase employee productivity.

APPLICATION CONTROL
Selectively allow, block, or restrict access to applications based on a user's department, job function, and time of day and to then see, in real-time, what's being accessed on your network and by whom.

GATEWAY ANTIVIRUS (GAV)
Leverage our continuously updated signatures to identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses. At the same time, heuristic analysis tracks down suspicious data constructions and actions to make sure unknown viruses don't slip by.

SPAMBLOCKER
Real-time spam detection for protection from outbreaks. Our spamBlocker is so fast and effective, it can review up to 4 billion messages per day.

ADVANCED SECURITY SERVICES

APT BLOCKER – ADVANCED MALWARE PROTECTION
APT Blocker uses an award-winning next-gen sandbox to detect and stop the most sophisticated attacks including ransomware, zero day threats and other advanced malware.

DATA LOSS PREVENTION (DLP)
This service prevents accidental or malicious data loss by scanning text and common file types to detect sensitive information attempting to leave the network.

DIMENSION COMMAND
Dimension translates data collected from all appliances across your network into actionable network and threat intelligence. Dimension Command gives you the power to take action to mitigate those threats instantly, from one central console.

THREAT DETECTION AND RESPONSE
Correlate network and endpoint security events with enterprise-grade threat intelligence to detect, prioritize and enable immediate action to stop malware attacks. Improve visibility by evolving your existing security model to extend past prevention, to now include correlation, detection and response.

WATCHGUARD TOTAL SECURITY

Figure 2.2: Rear view of the WatchGuard Firebox T115-W, highlighting the 3x 1Gb Ethernet ports and other connectivity options.

Figure 2.3: WatchGuard's commitment to real-world security solutions.

3. KEY FEATURES

- **Wi-Fi 7 Connectivity:** Integrated Wi-Fi 7 with external antennas for high-speed wireless access.

- **3x 1Gb Ethernet Ports:** Provides flexible wired connectivity for clean uplinks and VLAN segmentation.

- **Silent Fanless Design:** Ideal for quiet environments, ensuring unobtrusive operation.

- **Basic Security Suite:** Includes intrusion prevention, gateway antivirus, URL filtering, and spam blocking.

- **UTM Throughput:** Up to 280 Mbps with inspection on, suitable for small offices and remote work sites.

- **VPN Support:** Enables secure site-to-site VPN expansion for distributed networks.

- **WatchGuard Cloud Management:** Centralized management for security services and device configuration.

4. PACKAGE CONTENTS

Verify that your package contains the following items:

- WatchGuard Firebox T115-W Appliance
- Power Adapter
- Ethernet Cable
- External Wi-Fi Antennas (if applicable)
- Quick Start Guide
- Safety and Regulatory Information

5. HARDWARE DESCRIPTION

5.1 Front Panel

The front panel typically includes status indicator LEDs for power, system status, and network activity. Refer to the Quick Start Guide for specific LED behavior.

5.2 Rear Panel

The rear panel houses the primary connectivity ports:

- **Power Input:** Connects to the included power adapter.
- **Ethernet Ports (3x 1Gb):** Labeled for WAN (external network) and LAN (internal network) connections.
- **USB Ports:** For future expansion or specific configurations.
- **Antenna Connectors:** For attaching the external Wi-Fi antennas.

6. SETUP

6.1 Physical Installation

1. **Choose a Location:** Place the Firebox T115-W on a flat, stable surface in a well-ventilated area. Ensure it is away from direct sunlight and heat sources.
2. **Attach Antennas:** Screw the external Wi-Fi antennas onto their respective connectors on the rear panel.
3. **Connect Network Cables:**
   - Connect your internet modem/router to the designated WAN port (e.g., Eth0).
   - Connect your internal network devices (e.g., switch, computer) to the LAN ports (e.g., Eth1, Eth2).
4. **Connect Power:** Plug the power adapter into the Firebox T115-W and then into a power outlet. The device will power on automatically.

6.2 Initial Configuration

For initial configuration, refer to the WatchGuard Quick Start Guide included with your product or visit the official WatchGuard documentation website. Typically, this involves connecting a computer directly to a LAN port and accessing the device's web interface via a default IP address.
You will need to register your device with WatchGuard Cloud to activate your Basic Security Suite license and manage your security services.

7. OPERATING INSTRUCTIONS

7.1 Basic Security Suite

The Basic Security Suite provides essential protections:

- **Intrusion Prevention Service (IPS):** Detects and blocks network-based attacks.
- **Gateway Antivirus:** Scans incoming and outgoing traffic for malware.
- **URL Filtering:** Controls access to websites based on categories and policies.
- **Spam Blocking:** Filters unwanted email traffic.

These services are managed and configured through WatchGuard Cloud. Log in to your WatchGuard Cloud account to customize policies, view reports, and monitor security events.

7.2 Wi-Fi Configuration

The integrated Wi-Fi 7 can be configured via the WatchGuard Cloud interface. You can set up SSIDs, security protocols (WPA3 recommended), and guest networks. Ensure your Wi-Fi settings comply with local regulations.

8. MAINTENANCE

- **Firmware Updates:** Regularly check for and apply firmware updates through WatchGuard Cloud to ensure optimal performance and the latest security patches.

- **Configuration Backups:** Periodically back up your device configuration to prevent data loss.

- **Physical Cleaning:** Keep the device free from dust. Use a soft, dry cloth for cleaning. Do not use liquid cleaners.

- **Monitoring:** Regularly review logs and reports in WatchGuard Cloud for any unusual activity or performance issues.

9. TROUBLESHOOTING

9.1 No Power

- Ensure the power adapter is securely connected to both the device and a working power outlet.
- Verify the power outlet is functional by plugging in another device.

9.2 No Internet Access

- Check the physical connection of the WAN cable to your modem/router.
- Verify that your modem/router is working correctly and has an active internet connection.
- Review your network configuration in WatchGuard Cloud to ensure WAN settings are correct.

9.3 Wi-Fi Connectivity Issues

- Ensure external Wi-Fi antennas are properly attached.
- Check Wi-Fi settings (SSID, password, security type) in WatchGuard Cloud.
- Verify that the Wi-Fi radio is enabled.

For more advanced troubleshooting, consult the WatchGuard knowledge base or contact WatchGuard support.

10. SPECIFICATIONS

Feature	Detail
Model Number	T115-W (WGT116031)
Connectivity	Wi-Fi 7, 3x 1Gb Ethernet Ports
UTM Throughput	Up to 280 Mbps (with inspection on)
Security Features	Intrusion Prevention, Gateway Antivirus, URL Filtering, Spam Blocking
Form Factor	Tabletop, Fanless
Dimensions	*(Not provided in source data)*
Weight	*(Not provided in source data)*
Power Input	External Power Adapter

11. WARRANTY AND SUPPORT

Your WatchGuard Firebox T115-W comes with a standard manufacturer's warranty. The product includes a 1-Year Basic Security Suite license, which also typically covers basic support during its active period.

For detailed warranty information, technical support, or to renew your security suite license, please visit the official WatchGuard website or contact your authorized WatchGuard reseller.

WatchGuard Support Website: https://www.watchguard.com/support