



XTM FIPS Kit

This guide describes how to install and use your WatchGuard XTM device in compliance with the FIPS 140-2 standard.

Secure Installation

The Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules (FIPS 140-2), describes the United States Federal Government requirements for cryptographic modules. WatchGuard XTM devices meet the overall requirements for FIPS 140-2 Level 2 security when configured in a FIPS-compliant manner.

To use your XTM device in FIPS mode:

- Use the CLI command `fips enable` to enable FIPS mode operation.
- Configure the Admin and Status administrative accounts to use passwords with a minimum of 8 characters.
- When you configure VPN tunnels, you must choose only FIPS-approved authentication and encryption algorithms (SHA-1, SHA-256, SHA-512, 3DES, AES-128, AES-192, AES-256).
- When you configure VPN tunnels, you must choose Diffie-Hellman Group 2 or Group 5 for IKE Phase 1 negotiation.
- Use a minimum of 2048-bits for all RSA keys.
- Do not configure FireCluster for high availability.
- Do not use Mobile VPN with PPTP.
- Do not use PPPoE.
- Do not use WatchGuard System Manager to manage the appliance.
- Use RSA certificates for VPN and TLS connections.
- For access to the Fireware XTM Web UI, the web browser must be configured to use only TLS 1.0 and FIPS approved cipher suites.
- For network access to the CLI, telnet and SSH clients must use SSH V2.0 protocol.

Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at <http://csrc.nist.gov/groups/STM/cmvp/index.html>.

Tamper Evidence

To meet the requirements of the FIPS 140-2 standard, it is your responsibility to properly place tamper evident labels as described in this document. These security labels are designed to be very fragile and cannot be removed without visible signs of damage to the labels. Note that these labels are designed to be applied to a clean surface at 10 C or above.

After the labels are placed, you should inspect them on a regular basis to verify they are intact.

Any attempt to open the device will damage the security labels or the material of the security appliance cover. The labels can also be inspected for signs of tampering, which include curled corners, rips, and slices.

This is a photograph of the security labels provided in this kit.



Figure 1: WatchGuard XTM Tamper Evident Label

To make your XTM device FIPS-compliant, you must apply the tamper evident labels included in this kit to match the label placement diagram for your XTM device model.

XTM 21, 22, 23

These diagrams show where to apply the tamper evident labels for an XTM 21, 22, or 23 device.

UNDERSIDE / REAR VIEW



Figure 2: WatchGuard XTM 21/22/23 Tamper Evident Label Placement

UNDERSIDE / REAR VIEW



Figure 3: WatchGuard XTM 21/22/23 Wireless Tamper Evident Label Placement

XTM 25, 26, 33

These diagrams show where to apply the tamper evident labels for an XTM 25, 26, or 33 device.

UNDERSIDE / REAR VIEW

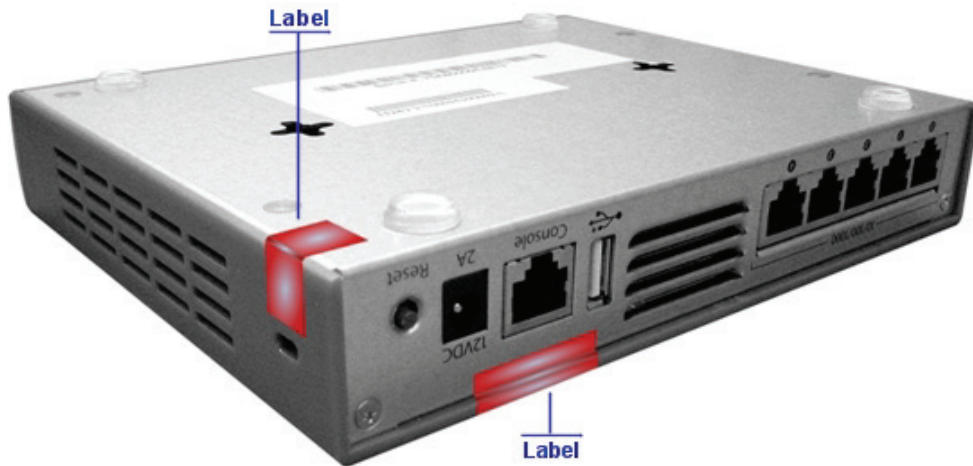


Figure 4: WatchGuard XTM 25/26/33 Tamper Evident Label Placement

UNDERSIDE / REAR VIEW

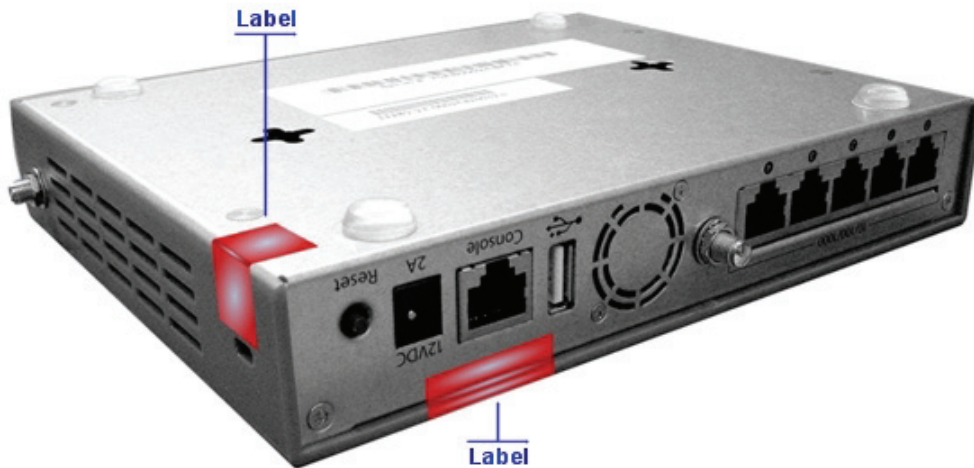


Figure 5: WatchGuard XTM 25/26/33 Wireless Tamper Evident Label Placement

XTM 330

These diagrams show where to apply the tamper evident labels for an XTM 330 device.

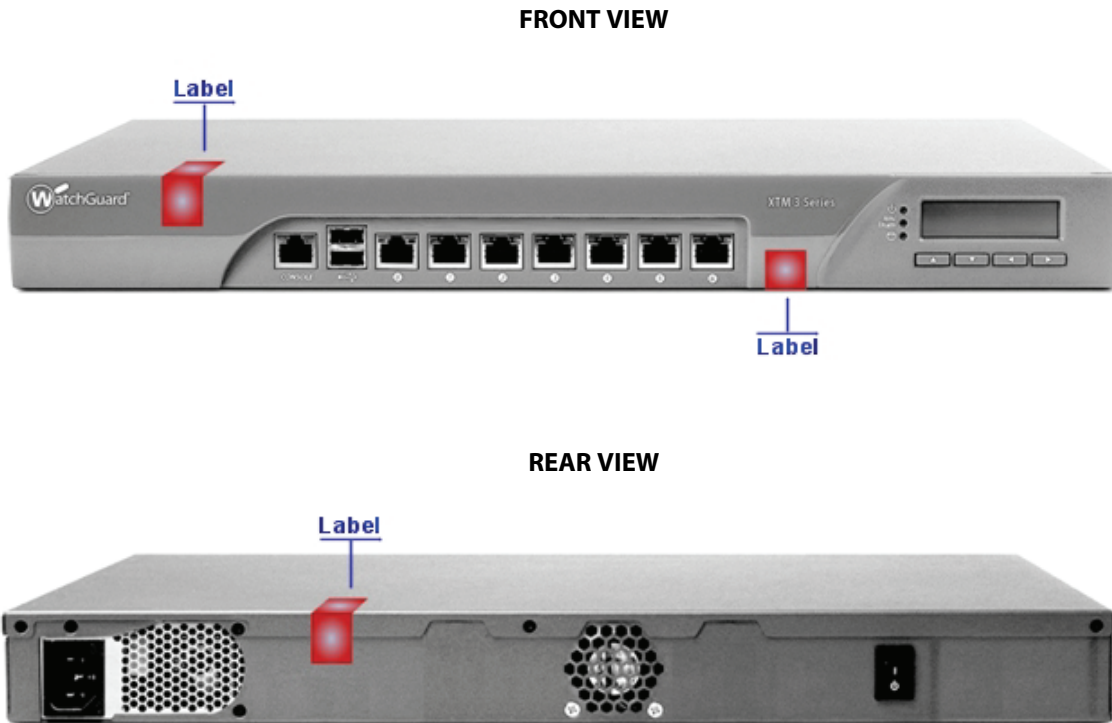


Figure 6: WatchGuard XTM 330 Tamper Evident Label Placement

XTM 5 Series

These diagrams show where to apply the tamper evident labels for an XTM 5 Series device.

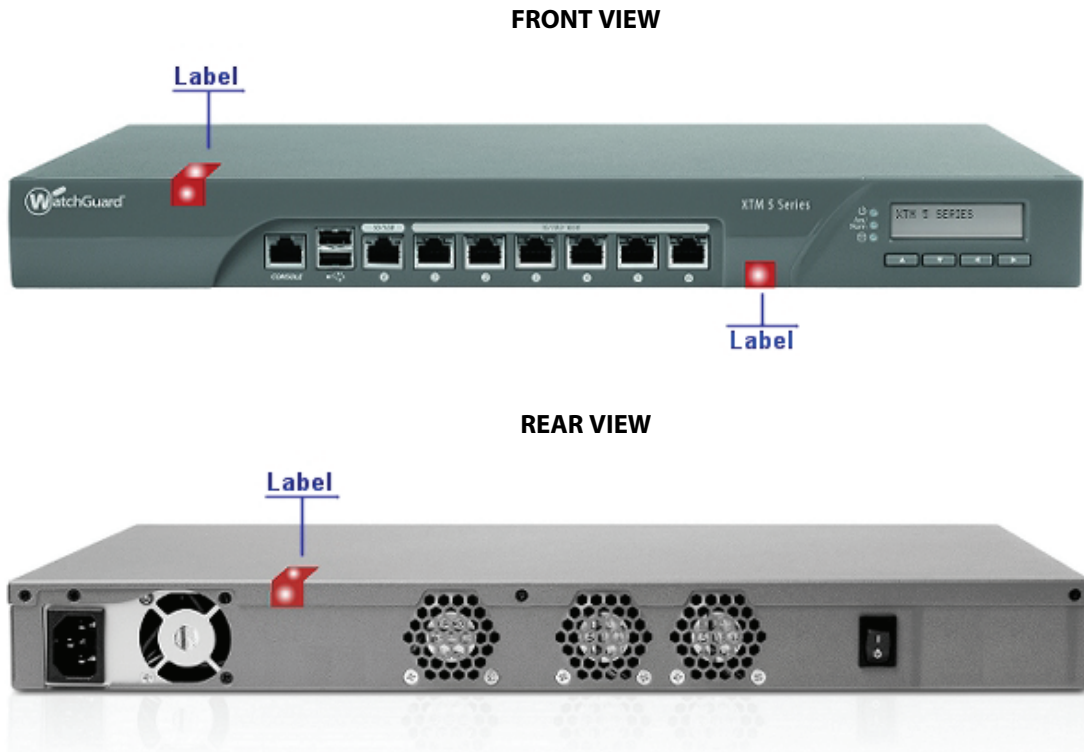


Figure 7: WatchGuard XTM 5 Series Tamper Evident Label Placement

XTM 8 Series

These diagrams show where to apply the tamper evident labels for an XTM 8 Series device.

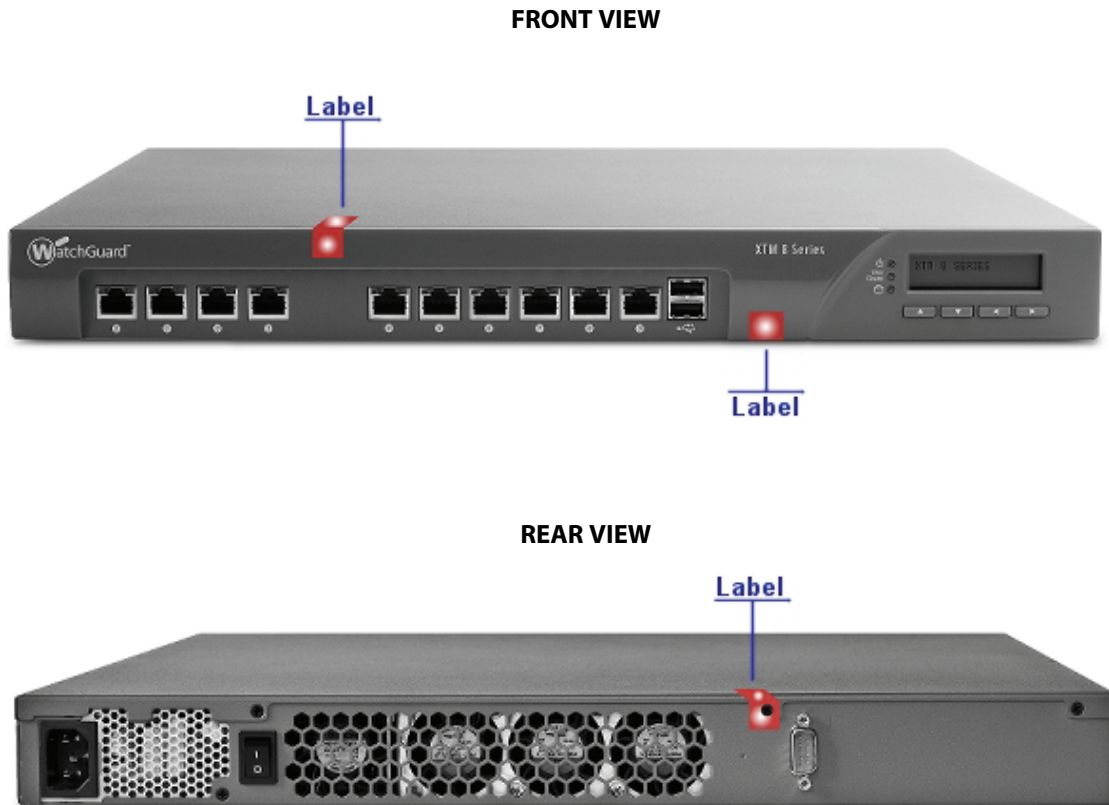


Figure 8: WatchGuard XTM 8 Series Tamper Evident Label Placement

XTM 1050

These diagrams show where to apply the tamper evident labels for an XTM 1050 device.

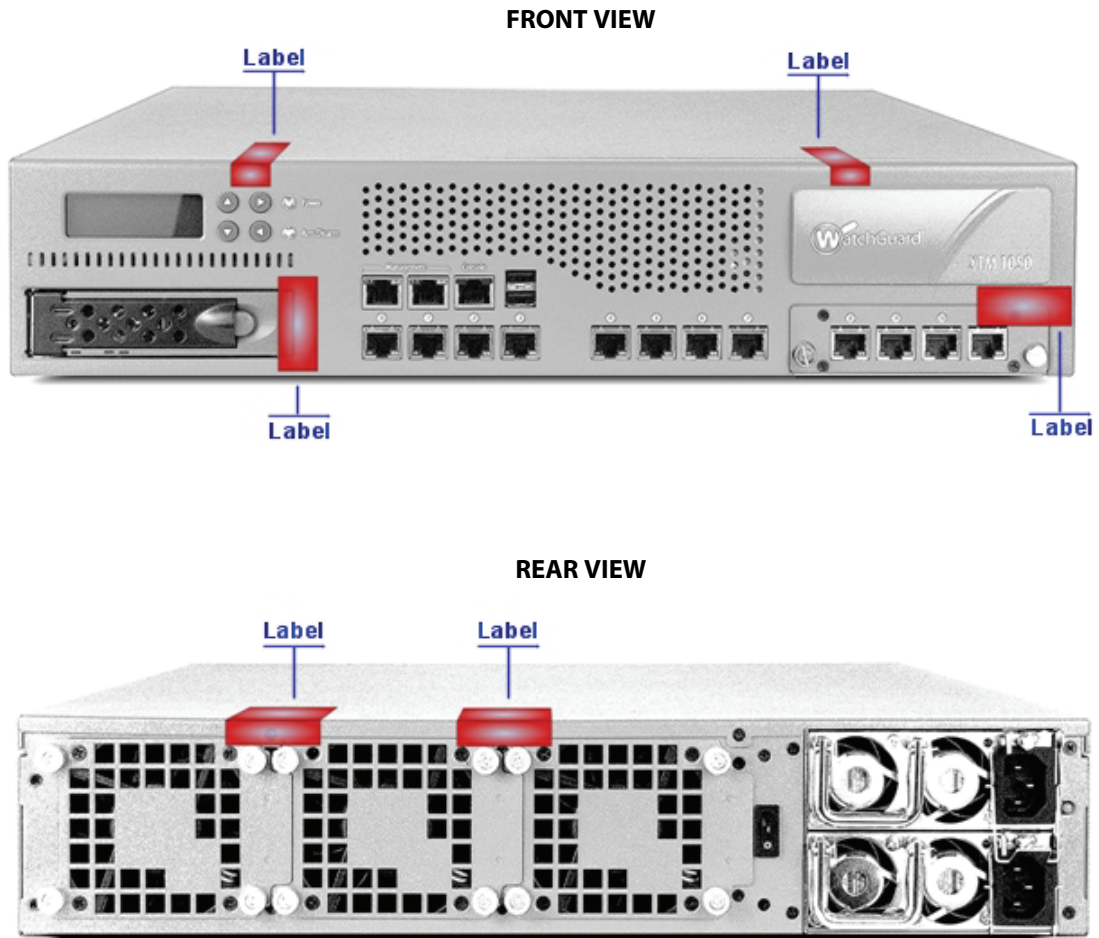


Figure 9: WatchGuard XTM 1050 Tamper Evident Label Placement

XTM 2050

These diagrams show where to apply the tamper evident labels for an XTM 2050 device.

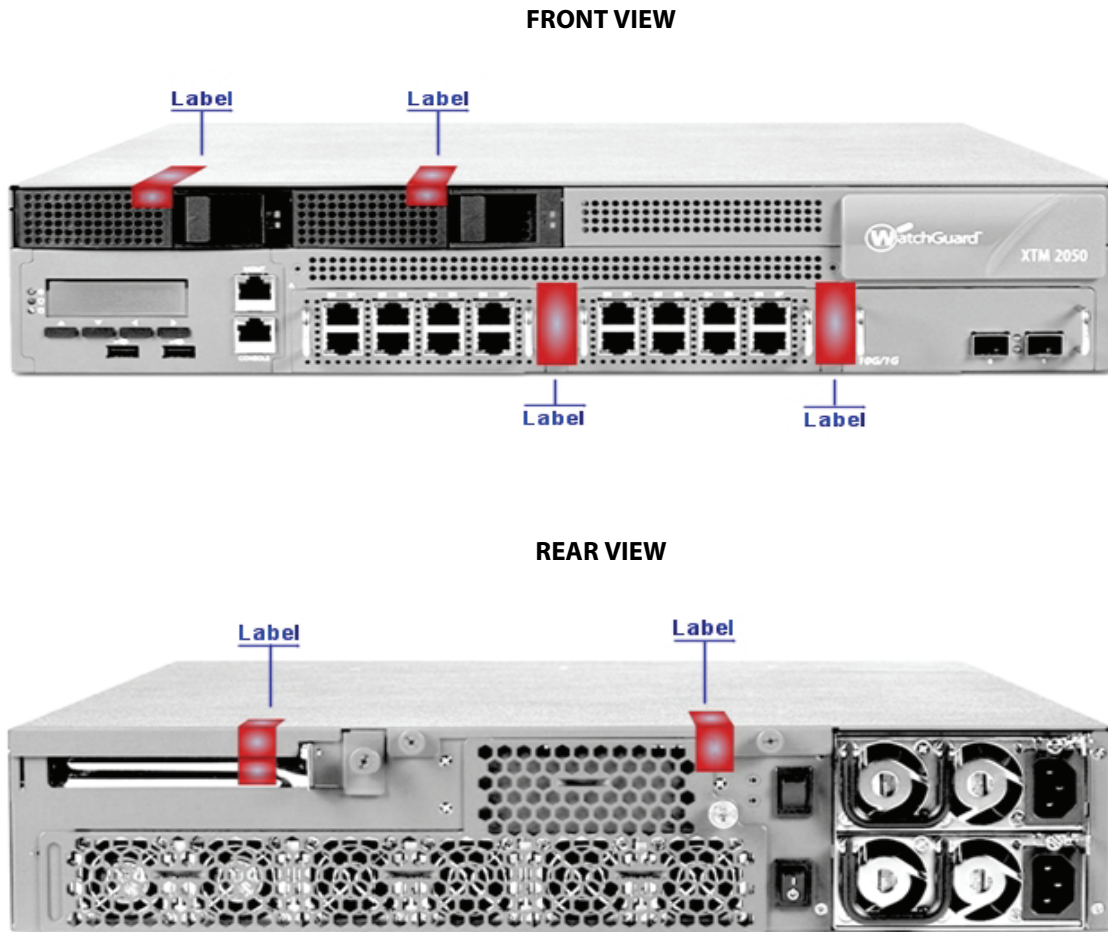


Figure 10: WatchGuard XTM 2050 Tamper Evident Label Placement

Copyright© 1998 - 2012 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, the WatchGuard logo, LiveSecurity, and any other mark listed as a trademark in the "Terms of Use" portion of the WatchGuard Web site that is used herein are either registered trademarks or trademarks of WatchGuard Technologies, Inc. and/or its subsidiaries in the United States and/or other countries. All other trademarks are the property of their respective owners.

Revision date: October 10, 2012

Part Number: 369-4115-001 Rev A