FIPS 140-2 Security Policy for WatchGuard XTM

XTM 515, XTM 525, XTM 535, XTM 545

Version: 2.2.7
August 28, 2013

WatchGuard XTM FIPS 140-2 Security Policy

Hardware:
XTM 515, XTM 525, XTM 535, XTM 545 (hardware model # NC2AE8)

Firmware Version:
Fireware XTM OS v11.5.5

Copyright Notice
This document may be copied without WatchGuard's explicit permission provided that it is copied in its entirety without any modification.

Trademarks
Fireware
WatchGuard

Regulatory compliance
FCC Class A Part 15

Contents

Introduction

This document is a FIPS 140-2 Security Policy for WatchGuard's XTM Extensible Threat Management Security System. This policy describes how the XTM 515, XTM 525, XTM 535, and XTM 545 models (hereafter referred to as the 'module' or the 'XTM module') meets the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner.

This policy was created as part of the Level 2 FIPS 140-2 validation of the XTM module.

The Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. 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.

XTM Module Overview

WatchGuard® XTM Extensible Threat Management appliances are built for enterprise-grade performance with blazing throughput and numerous connectivity options. Advanced networking features include clustering, high availability (active/active), VLAN support, multi-WAN load balancing and enhanced VoIP security, plus inbound and outbound HTTPS inspection, to give the strong security enterprises need. And the XTM appliances are completely configurable – turn on or off components and services to fit different network security deployment requirements.

WatchGuard's XTM product family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of application. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time — without degrading network performance. In addition to providing application level firewall protection, the XTM module delivers a full range of network-level services — VPN, intrusion prevention, web filtering, antivirus, antispam and traffic shaping — in dedicated, easily managed platforms.

The XTM Extensible Threat Management security system employs the powerful, secure, Fireware XTM OS to achieve breakthrough price/performance. This system provides a critical layer of real-time, network-based antivirus protection that complements host-based antivirus software and supports "defense-in-depth" strategies without compromising performance or cost. They can be easily configured to provide antivirus protection, antispam protection and content filtering in conjunction with existing firewall, VPN, and related devices, or as complete network protection systems.

The XTM module supports the IPSec industry standard for VPN, allowing VPNs to be configured between an XTM module and any client or gateway/firewall that supports IPSec VPN. The XTM module also provides SSLVPN services.

The XTM module is defined as a multi-chip standalone cryptographic module consisting of production grade components contained in a physically protected enclosure. The entire enclosure is defined as the

cryptographic boundary of the cryptographic module. The cryptographic boundary for FIPS 140-2 certification is equivalent to the TOE boundary for Common Criteria (CC) certification.

Security Level

The WatchGuard XTM appliances meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports Specification	2
Roles, Services, and Authentication	2
Finite State Machine	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	2

Roles, Services and Authentication

Module Access Methods

There are two convenient and secure ways to connect, configure and manage the module.

Web UI

The XTM module provides a web based GUI based access to the module, which is the convenient way to configure the module. The Web UI requires a web browser on the management computer and an Ethernet connection between the module and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.0 is required for remote access to the Web UI when the modules are operating in FIPS mode.

The web browser is not part of the validated module boundary.

Command Line Interface

The Command Line Interface (CLI) is a rich, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the modules. The CLI uses a console or a network (Ethernet) connection between the module and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required. SSH v1.0 is not supported in FIPS mode.

The Telnet or SSH client is not part of the validated module boundary.

Roles

The module provides two pre-defined roles for users: User (status) and Cryptographic Officer (admin) role. One of these roles can be assumed by an operator after authenticating to the module remotely or through a console connection using a username/password combination. The module does not allow the creation of additional operator accounts or roles.

An operator assuming the Cryptographic Officer role has full read/write access to all of the functions and services of the module, including configuration, resetting or shutting down the module. This also implies that the Cryptographic Officer role includes all the accesses and privileges the User has.

The User is not allowed to make any changes to the configuration of the module. The User role is only for viewing and reporting the configuration and status of the module and its functions.

Operator accounts are differentiated by the username during authentication. More than one operator with User role can be connected to the module at any given time. However, there can be only one Cryptographic Officer login at any given time. Concurrent login attempts by the Cryptographic Officer are refused by the module.

It is not possible to change roles without re-authentication.

Services

The following table details the FIPS approved services available for each role, the types of access for each role, and the Keys or CSPs they affect. The role names are abbreviated as follows:
Cryptographic Officer - CO
User - U

R=Read Access, W=Write/ Delete Access, X=Execute Access

The Key/CSP is documented in section "Cryptographic Key Management" on page 23.

Table 2: FIPS approved services in Command Line Interface and Web UI access mode

Service	U	CO	Key/ CSP
authenticate to module	X	X	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
show system status	R	R	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
show FIPS mode enabled/disabled	R	R	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
enable FIPS mode	N/A	WX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
disable FIPS mode	N/A	X	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
execute FIPS on-demand self-tests	N/A	X	4, 7, 8, 9, 10, 11, 12, 14, 15, 18, 19, 21
set/reset password	N/A	WX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
execute firmware download	N/A	X	4, 7, 8, 9, 10, 11, 12, 14, 15, 18, 19, 21
execute system reboot	N/A	X	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,12, 13, 14, 15, 18, 19, 20, 21
execute system shutdown	N/A	X	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,12, 13, 14, 18, 19, 20, 21
change system time	N/A	WX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
read/modify system/network configuration	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
read/modify firewall policies.	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
read/modify Gateway AV configuration	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
read/modify spamBlocker configuration	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
read/ modify WebBlocker configuration	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 21
read/ modify VPN configuration	R	RWX	1, 4, 7, 8, 9, 10, 11, 12, 14, 18, 19, 20, 21

read/modify IPS configuration	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 21
read/ modify logging configuration	R	RWX	4, 7, 8, 9, 10, 11, 12, 14, 18, 21
read log data	R	R	4, 7, 8, 9, 10, 11, 12, 14, 18, 21
manual Gateway AV/IPS signature update	N/A	RX	4, 7, 8, 9, 10, 11, 12, 14, 18, 21
backup image to USB	N/A	RWX	1, 4, 7, 8, 9, 10, 11, 12, 14, 17, 18, 20
restore image from USB	N/A	RWX	1, 4, 7, 8, 9, 10, 11, 12, 14, 17, 18, 20

Approved Algorithms

The cryptographic module implements the following FIPS approved algorithms:

- Hardware:
  - Triple-DES
  - AES
  - SHA-1
  - HMAC-SHA-1

Table 3: FIPS approved algorithms for hardware

Algorithm	FIPS Validation Certificate Number
Triple-DES (TCBC mode)	1079
AES (CBC mode)	1659
SHA-1	1453
HMAC-SHA-1	974

Please see NIST Special Publication SP 800-131A (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths), for caveats on use of the following algorithms and key lengths:

- Use of SHA-1 for digital signature generation
- Use of HMAC-SHA-1 for MAC generation with key length >= 80 bits and < 112 bits, and use of HMAC-SHA-1 for MAC verification with key length >= 80 bits and < 112 bits

- Firmware:
  - Triple-DES
  - AES
  - SHA-1
  - HMAC-SHA-1
  - RSA
  - ECDSA
  - RNG
  - DSA

Table 4: FIPS approved algorithms for firmware

Algorithm	FIPS Validation Certificate Number
Triple-DES (TCBC mode)	1380
AES (CBC mode)	2180
SHA-1	1890
HMAC-SHA-1	1334
RSA	1124
ECDSA	339
RNG (ANSI X9.31)	1103
DSA	684

Please see NIST Special Publication SP 800-131A (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths), for caveats on use of the following algorithms and key lengths:
- Use of SHA-1 for digital signature generation, and use of SHA-1 for digital signature verification
- Use of HMAC-SHA-1 for MAC generation with key length >= 80 bits and < 112, , and use of HMAC-SHA-1 for MAC verification with key length >= 80 bits and < 112 bits
- Use of ECDSA for digital signature verification with key length >= 160 bits and < 224 bits
- Use of ANSI X9.31 RNG
- Use of DSA with 1024 bit keys for digital signature generation, and use of DSA with 1024 bit keys for digital signature verification

Non-FIPS Approved Services

The cryptographic module provides the following non-FIPS approved services:

- Firecluster (high availability) in both Active/Active (A/A) and Active/Passive (A/P) configurations
- Mobile VPN with PPTP
- PPPoE

If any of these services are used, the cryptographic module is not operating in a FIPS approved mode of operation.

Non-FIPS Approved Algorithms

The cryptographic module implements the following non-FIPS approved algorithms:

- DES
- RC4
- MD5
- TKIP
- AES in CCM mode (counter with CBC-MAC)
- RSA key transport (with 2048 bit keys)
  - Key wrapping, key establishment methodology provides 112 bits of equivalent encryption strength

- Diffie Hellman
  - Key establishment, key agreement method provides between 80 and 112 bits of equivalent encryption strength
- Password Based Key Derivation Function (for 128 bit AES key)

Alternating Bypass

The primary cryptographic function of the module is to act as a firewall, and as a VPN device. Encrypt and decrypt operations are performed on traffic based on firewall policies. The cryptographic module implements an alternating bypass feature based on VPN tunnels and firewall policies. Traffic can be encrypted/decrypted or passed as plaintext, depending on the VPN tunnel and selected policy.

Two actions must be taken by the Cryptographic Officer to transition between VPN bypass states. The Cryptographic Officer must first create the VPN gateway. The Cryptographic Officer must then create the VPN tunnel and tunnel route, and associate the VPN tunnel with a VPN policy.

Whether VPN bypass is enabled or not can be determined by examining the list of VPN gateways and VPN tunnels.

Authentication

Cryptographic Officer or User (referred to as Operator) must authenticate with a username and password combination to access the modules remotely or locally via the console. Remote operator authentication is done over HTTPS (TLS 1.0) or SSH (v2.0). The access to the module is based on firewall policy and authentication by IP address.

For end users (including CO or U) using module functionality and invoking the SSLVPN or IPSec encrypt/decrypt services, the module supports authentication with a username/password combination. The authentication is done over HTTPS over a dedicated port and it does not allow access to the module for any of the administrative purposes whatsoever.

The minimum password length is 8 characters when in FIPS mode. Using a strong password policy, where operator and end user passwords are at least 8 characters in length and use a mix of alphanumeric (printable) characters from the ASCII character set, the odds of guessing a password are 1 in 94^8, which is far less than 1 in 1,000,000. The total password space is sufficiently large such that exceeding a 1 in 100,000 probability of correctly guessing the password in one minute would require approximately 6.1 x 10^{10} attempts per minute, which is beyond the operational capability of the module.

For end users invoking the IPSec encrypt/decrypt services, the module acts on behalf of the end user and negotiates a VPN connection with a remote module. The strength of authentication for IPSec services is based on the authentication method defined in the specific firewall policy: IKE pre-shared key or IKE RSA key (RSA certificate). The odds of guessing the authentication key for each IPSec method is:

- 1 in 94^8 for the IKE preshared key (based on an 8 character, ASCII printable key)
- 1 in 2^{112} for the IKE RSA key (based on a 2048 bit RSA key size, which is equivalent to 112 bits of security)

Therefore the minimum odds of guessing the authentication key for IPSec is 1 in 94^8 based on the IKE preshared key, or 1 in 2^{112} based on the IKE RSA key, which is far less than 1 in 1,000,000. The key size is

sufficiently large such that exceeding a 1 in 100,000 probability of correctly guessing the key in one minute would require approximately 6.1×10^{10} attempts per minute (for preshared key) or 5.2×10^{28} attempts per minute (for RSA key) , which is beyond the operational capability of the module.

Interfaces

Physical ports and interfaces on the XTM module can be categorized into the following logical interfaces:

- Data Input
- Data Output
- Control Input
- Status Output

All of the physical ports and interfaces are separated into the FIPS 140-2 logical interfaces, as described in the following tables. The logical interfaces may share a physical port. The firmware in the XTM module separates and routes data to the appropriate internal firmware task associated with a logical interface based on port number, session, and/or command context.

XTM 5 Series

Figure 1: XTM 5 Series Front View

Table 5: Front Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
RJ45 Ethernet Interfaces with link lights	7	Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
RJ45 Console Interface	1	Serial port for CLI access.	✓	✓	✓	✓
USB Interfaces	2	Used for backup and restore, or to store a support snapshot.	✓	✓		
LCD Screen	1	The LCD screen shows module status information and selected internal and network parameters.				✓

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
LCD MENU Buttons	4	Press the LCD buttons to see status information on the LCD.			✓	
Power Light	1	Lit green when the module is powered on.				✓
Arm/Disarm Light	1	This light is red after power-on or reboot. It turns green after successful module initialization.				✓
Storage Light	1	Lit yellow when there is activity on the compact flash.				✓

Figure 2: XTM 5 Series Rear View

Table 6: Rear Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Power Interface	1	Auto-sensing AC power supply.				
Power Switch	1	Controls power supplied to device.			✓	

FIPS 140-2 Compliant Operation

The XTM module meets FIPS 140-2 Level 2 requirements. This section describes how to place and keep the XTM module in a FIPS approved mode of operation.

Security Rules

The cryptographic module has the following security rules:

- The cryptographic module provides two distinct operator roles. These are the User role, and the Cryptographic Officer role.

- The cryptographic module provides role-based authentication relying upon usernames and passwords.

Self-Tests

- The cryptographic module performs the following self-tests at power-up:

  Hardware cryptographic algorithm tests:
  - Triple-DES encrypt/decrypt KAT
  - AES encrypt/decrypt KAT
  - SHA-1 KAT
  - HMAC-SHA-1 KAT

  Firmware cryptographic algorithm tests:
  - Triple-DES encrypt/decrypt KAT
  - AES encrypt/decrypt KAT
  - SHA-1 KAT
  - HMAC-SHA-1 KAT
  - RSA Sign/Verify KAT
  - ECDSA Sign/Verify KAT
  - ANSI X9.31 RNG KAT
  - DSA Sign/Verify KAT

  Firmware integrity test:
  - Firmware integrity test (using HMAC-SHA-1)

  The results of the power-up self-tests are displayed on the console during the power-up sequence. The self-tests are run automatically at power-up without any operator intervention. The power-up self-tests are run before any networking interfaces are started, so that data output is inhibited while self-tests are running.

The power-up self-tests can also be initiated on demand by issuing the CLI command **fips selftest**.
1. Sample output (FIPS mode currently enabled):

```
The box will reboot, Please wait for a moment…
```

If any of the power-up tests fail, the cryptographic module enters the error state. Errors are displayed on the console. No security services are provided in the error state and data output is inhibited (the XTM module is shutdown).

- The cryptographic module performs the following conditional tests:
  - RSA pairwise consistency test
  - DSA pairwise consistency test
  - PRNG continuous test
  - Bypass test
  - Firmware load test (using HMAC-SHA-1)

  If the RSA pairwise consistency test, DSA pairwise consistency test, PRNG continuous test, or bypass test fails, the cryptographic module enters the error state. Errors are displayed on the console or internal logs. No security services are provided in the error state and data output is inhibited (the XTM module is shutdown).

  If the firmware load test fails, the cryptographic module enters the firmware load test failure state. The new firmware image is not loaded. The XTM module resumes normal operation after the error is logged.

Cryptographic Officer Guidance

This section describes the responsibilities of the Cryptographic Officer for installing, configuring, and ensuring proper operation of the validated XTM module.

Secure Installation

The Cryptographic Officer must ensure that:
- The XTM module is installed in a secure physical location.
- Physical access to the XTM module is restricted to authorized personnel only.

Enabling FIPS Mode Operation

The cryptographic module is not configured to operate in FIPS mode by default. To operate in FIPS mode, do the following:

- Issue the CLI command **fips enable** to enable FIPS mode operation.
- Choose operator passwords (for Cryptographic Officer and User roles) with a minimum of 8 characters.
- Run **fips selftest** before making changes to the VPN configuration.

- SSLVPN tunnels use TLS 1.0. When configuring SSLVPN tunnels, only choose FIPS-approved authentication and encryption algorithms (SHA-1, SHA-256, SHA-512, Triple-DES, AES-128, AES-192, AES-256).
- When configuring IPSec VPN tunnels, only choose FIPS-approved authentication and encryption algorithms (SHA-1, SHA-256, SHA-512, Triple-DES, AES-128, AES-192, AES-256).
- When configuring VPN tunnels, choose Diffie-Hellman Group 2 (1024 bit) or Group 5 (1536 bit) for IKE Phase 1 negotiation.
- Only use RSA certificates for VPN and TLS.
- Use a minimum of 2048-bits for all RSA keys.
- Do not configure Firecluster high availability.
- Do not use Mobile VPN with PPTP.
- Do not use PPPoE.
- Do not use WatchGuard System Manager to manage the appliance.
- Web browsers must be configured to only use TLS 1.0 and FIPS approved cipher suites.
- Telnet and SSH clients must be configured to use the SSH V2.0 protocol and RSA or DSA authentication.
- When using backup and restore, the Cryptographic Officer must take possession of the USB device.
- Do not use the wireless interfaces.

Disabling FIPS Mode Operation

To disable FIPS mode, do the following:

- Issue the CLI command **restore factory-default all** (to disable FIPS mode and zeroize all keys and CSPs).

User Guidance

This section describes the responsibilities for Users of the validated XTM module.

The User can determine if the cryptographic module is operating in FIPS mode by issuing the CLI command **show FIPS**.

1. Sample output (FIPS mode currently not enabled):

```
--
-- Current FIPS status
--
FIPS status : disabled
```

2. Sample output (FIPS mode currently enabled):

```
--
-- Current FIPS status
--
FIPS status : enabled
```

Tamper Evidence

All Critical Security Parameters are stored and protected within each appliance's tamper evident enclosure. Tamper evident labels must be applied for the module to operate in a FIPS approved mode of operation. It is the responsibility of the Crytographic Office to properly place all tamper evident labels as described in this section. The security labels recommended for FIPS 140-2 compliance are separately ordered (SKU WG8566). 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.

The Cryptographic Officer must apply 3 tamper evident labels at the locations shown in the Figures. Before the labels are applied, the Cryptographic Officer should ensure that the surface is clean, and that the air temperature is at 10°C or above. After the labels are placed, the Cryptographic Officer should inspect the tamper evident labels periodically to verify they are intact.

If the tamper evident seals are found to be damaged or broken during inspection, the Cryptographic Officer can return the cryptographic module to a FIPS approved mode of operation by restoring the module to a factory default state, reinstalling, and applying new tamper evident labels.

Any attempt to open the device will damage the tamper evident seals or the material of the security appliance cover. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices.

The following is a photograph of the tamper evident labels that are used.

Figure 3: WatchGuard XTM Tamper Evident Label

XTM 5 Series

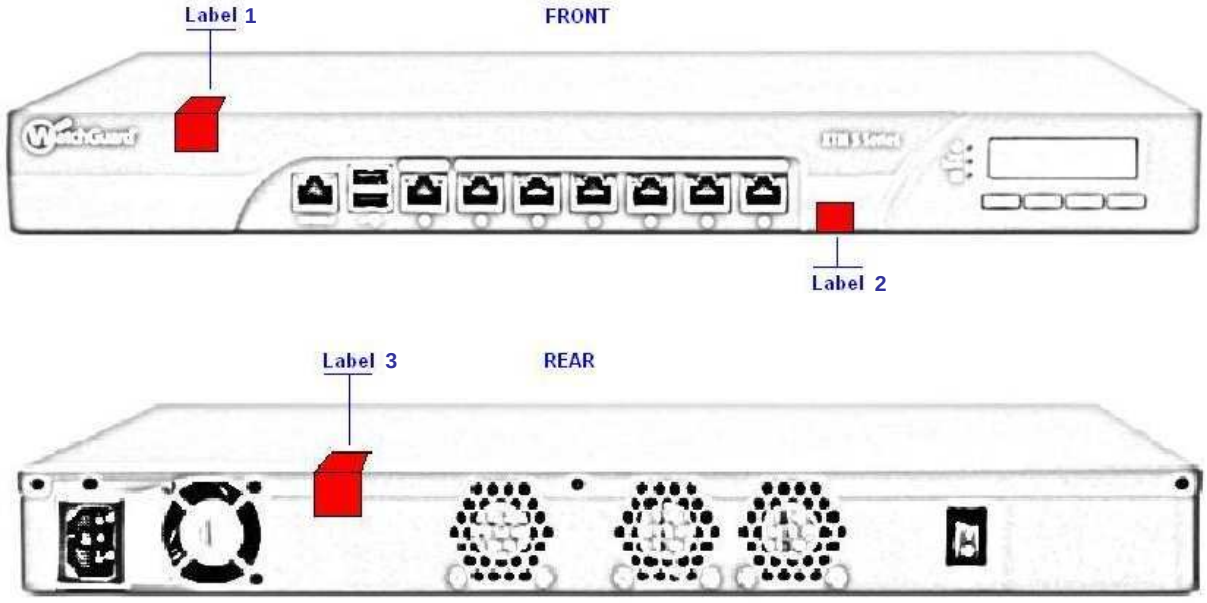

Figure 4: WatchGuard XTM 5 Series Tamper Evident Label Placement

Cryptographic Key Management

Cryptographic Keys and Critical Security Parameters

The following table lists the cryptographic keys and Critical Security Parameters (CSPs) used by the cryptographic module:

Table 7: Cryptographic Keys and Critical Security Parameters

#	Key/CSP	Usage	Storage	Input	Output	Generation	Zeroization
1	IKE pre-shared secret	Used by IKE during authentication.	CompactFlash and RAM (plain text)	✓	✓	Entered by Cryptographic Officer.[1]	Delete the IPSec VPN configuration. Power off the appliance.
2	IKE session authentication key	Used to authenticate IKE negotiations.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) during IKE phase-1 exchange.	Terminate the session, or power off the appliance.
3	IKE session encryption key	Used to encrypt IKE negotiations.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) during IKE phase-1 exchange.	Terminate the session, or power off the appliance.
4	RSA private key	The RSA private key in for IKE and TLS authentication.	CompactFlash and RAM (plain text)	✓	✓	Generated internally using ANSI X9.31 RNG or imported across an encrypted tunnel.	Restore the device to its factory default configuration.

#	Key/CSP	Usage	Storage	Input	Output	Generation	Zeroization
5	IPSec session authentication key	Exchanged using the IKE protocol. Used to authenticate IPSec traffic.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) during IKE phase-2 exchange.	Terminate the session, or power off the appliance.
6	IPSec session encryption key	Exchanged using the IKE protocol. Used to encrypt IPSec traffic.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) during IKE phase-2 exchange.	Terminate the session, or power off the appliance.
7	Diffie-Hellman private key	The private exponent used in Diffie-Hellman key exchange for IKE, TLS, and SSH sessions.	RAM (plain text)			Generated internally using ANSI X9.31 RNG.	Terminate the session, or power off the appliance.
8	Diffie-Hellman shared secret	Shared secret used in Diffie-Hellman key exchange for IKE, TLS, and SSH sessions.	RAM (plain text)			Generated internally using Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.
9	RNG seed value and RNG seed key	Seed value and seed key for RNG.	RAM (plain text)			Initial generation via entropy.	Power off the appliance.
10	HTTPS session key	Used for Web UI for session encryption and authentication.	RAM (plain text)			Generated internally using TLS protocol exchange.	Terminate the session, or power off the appliance.
11	SSH session key	Used by SSH for session encryption .	RAM (plain text)			Generated internally using Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.

#	Key/CSP	Usage	Storage	Input	Output	Generation	Zeroization
12	SSH HMAC-SHA-1 key	Used by SSH for data integrity.	RAM (plain text)			Generated internally using Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.
13	SSLVPN session key	Used for SSLVPN session encryption and authentication.	RAM (plain text)			Generated internally using TLS protocol exchange.	Terminate the session, or power off the appliance.
14	Passwords	Used to authenticate Crypto-Officer and User logins.	CompactFlash and RAM (plain text)	✓	✓	Entered by Cryptographic Officer or User.[1]	Overwrite with new password.
15	Firmware load HMAC-SHA-1 key	Used for firmware load test.	RAM (plain text)			Compiled into the firmware.	Install patch that deletes the firmware.
16	Firmware integrity HMAC-SHA-1 key	Used for firmware integrity test.	RAM (plain text)			Compiled into the firmware.	Install patch that deletes the firmware.
17	Log Server pre-shared secret	Used to authenticate connections to the log server.	CompactFlash and RAM (plain text)	✓	✓	Entered by Cryptographic Officer.[1]	Delete the log server configuration. Power off the appliance.
18	SSH DSA private key	Used by SSH for authentication.	CompactFlash and RAM (plain text)			Generated internally using ANSI X9.31 RNG.	Restore the device to its factory default configuration.
19	SSH RSA private key	Used by SSH for authentication.	CompactFlash and RAM (plain text)			Generated internally using ANSI X9.31 RNG.	Restore the device to its factory default configuration.

[1] Can be entered into the module in plain text over the serial console port from a non-networked computer.

Public Keys

The following table lists the public keys used by the cryptographic module:

Table 8: Public Keys

#	Key/CSP	Usage	Storage	Input	Output	Generation	Zeroization
20	RSA public key	Used by IKE peer to verify digital signatures.	RAM (plain text)	✓	✓	Generated using ANSI X9.31 RNG or imported across an encrypted tunnel.	Delete the IPSec VPN configuration. Power off the appliance.
21	Diffie-Hellman public key	The public key used in Diffie-Hellman key exchange for IKE, TLS, and SSH sessions.	RAM (plain text)		✓	Generated internally using Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.
22	ECDSA public key	The ECDSA public key used to verify the license signature.	RAM (plain text)			Compiled into the firmware.	Install patch that deletes the firmware.

Mitigation of Other Attacks

The XTM module includes optional capabilities of Intrusion Prevention System (IPS), Antivirus protection, Antispam and URL Filtering in addition to capabilities described earlier. These capabilities are backed up by the WatchGuard proprietary proxy technology.

The proprietary Proxy technology enables the blocking of oversized files, supports blocking by file extension and blocking of traffic based on any Protocol Anomaly Detection (PAD).

The module offers an inbuilt default threat protection that protects the internal networks by performing behavioral analysis of traffic passing through the module. This can protect the module from direct attacks, based on TCP, ICMP, UDP, and IP protocols, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), Synflood, and ping of death, etc. Access is denied or packets are dropped when an attack is detected. Attack parameters can be modified by the Cryptographic Officer to ensure that normal network traffic is not considered an attack.

Whenever a Gateway IPS, Gateway Antivirus, Antispam or WebBlocker event occurs, the module can record the event in the log and/or send an alarm to a Cryptographic Officer via a configured notification mechanism. The rest of this section provides additional information on different services of the XTM module.

Gateway IPS Service

The WatchGuard Gateway IPS is a signature based component for detecting attacks passing through the module. Signature based attack detection mechanism works by identifying transmission patterns and other codes that indicate that a system might be under attack. Each signature is designed to detect a particular type of attack. The signatures for real-time IPS service are updated through the WatchGuard Gateway Intrusion Prevention Service. The module can be configured to securely automatically check for and download updated IPS packages from the WatchGuard servers, or they can be downloaded manually by the Cryptographic Officer. The IPS package is signed with the WatchGuard server's private key and verified by the module using the WatchGuard server's public key.

Gateway Antivirus Service

The XTM Antivirus service scans web (HTTP), file transfer (FTP), Instant Messaging and email (POP3, IMAP, and SMTP) traffic passing through the module and removes and can optionally quarantine the infected content. The quarantined files and content are stored on the separate server outside the module. The Cryptographic Officer can review and delete quarantined files from the server. When any attachment is removed from the email, it is replaced with a replacement message that goes to the intended recipient of the email message.

The module can be configured to automatically check for and download updated AV signature and engine packages from the WatchGuard servers, or they can be downloaded manually by the Cryptographic Officer. The AV package is signed with the WatchGuard server's private key and verified

by the module using the WatchGuard server's public key. The module also is capable of updating the latest Antivirus engine securely through the Gateway Antivirus service.

Gateway Antivirus service also detects and removes malware such as adware, spyware, etc.

Quarantine Server which stores the emails and content is external to the module and not part of FIPS compliant module boundary.

spamBlocker Service

WatchGuard spamBlocker service can scan emails over SMTP, IMAP or POP3 protocols and can tag or discard email messages determined to be spam. Based on Recurrent Pattern Detection technology, optionally, this service can also quarantine the spam emails for review by the Cryptographic Officer. Spam detection methods also include black/white lists and return email DNS check. The spamBlocker Service also provides IP checking, URI address checking and email checksum analysis.

Quarantine Server which stores the emails and content is external to the module and is not part of the FIPS compliant module boundary.

WebBlocker Service

WatchGuard WebBlocker service offers URL filtering technology. WebBlocker service can be configured to scan HTTP and HTTPS protocol streams for banned URLs or web page content. The WebBlocker service uses a large database of URLs to block access to banned web sites and URLs based on content categories. The Cryptographic Officer can decide which categories of URLs are allowed by organization's security policy. The Cryptographic Officer can also configure URL filtering to block all or just some of the pages on a specific web site by using regular expressions. This feature can be used to deny access to parts of a web site without denying access to it completely. Also, the Cryptographic Officer can configure white and black lists to statically allow legitimate web pages or deny illegitimate web pages.

When a certain web page is blocked by the service, the end user is displayed a message that can be customized by the Cryptographic Officer using Web UI or Command Line Interface.

Definitions

AC – Alternating Current

AES – Advanced Encryption Standard

ANSI – American National Standards Institute

ASCII - American Standard Code for Information Interchange

AV – AntiVirus

CA – Certificate Authority

CBC – Cipher-Block Chaining

CC – Common Criteria

CLI – Command Line Interface

CO – Cryptographic Officer

CSP – Critical Security Parameter

DES – Data Encryption Standard

DH – Diffie-Hellman

DSA – Digital Signature Algorithm

ECDSA – Elliptic Curve Digital Signature Algorithm

FIPS – Federal Information Processing Standards

FTP – File Transfer Protocol

GUI – Graphical User Interface

HMAC – Hash Message Authentication Code

HTTPS – HyperText Transfer Protocol Secure

IMAP – Internet Message Access Protocol

IKE – Internet Key Exchange

IP – Internet Protocol

IPS – Intrusion Prevention System

IPSec – Internet Protocol Security

KAT – Known Answer Test

LAN – Local Area Network

LCD – Liquid Crystal Display

LED – Light-Emitting Diode

MAC – Message Authentication Code

MD5 – Message-Digest algorithm 5

NIST – National Institute of Standards and Technology

OS – Operating System

POP3 – Post Office Protocol 3

PPPoE – Point-to-Point Protocol over Ethernet

PPTP – Point-to-Point Tunneling Protocol

RADIUS – Remote Authentication Dial In User Service

RC4 – Rivest Cipher 4

RNG – Random Number Generator

RSA – Rivest, Shamir, & Adelman algorithm

SHA – Secure Hash Algorithm

SMTP – Simple Mail Transfer Protocol

SoHo – Small Office Home Office

SSH – Secure Shell protocol

SSLVPN – Secure Sockets Layer Virtual Private Network

TLS – Transport Layer Security

TOE – Target of Evaluation

Triple-DES – Triple Data Encryption Algorithm

UI – User Interface

USB – Universal Serial Bus

VLAN – Virtual Local Area Network

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network

WAN – Wide Area Network

WAP – Wireless Access Point

XTM – Extensible Threat Management