POLIWALL-CCF M10 [1], M50 [2], G01 [3] AND G10 [4] SERIES SECURITY APPLIANCE

WITH HIPPIE TECHNOLOGY

FIPS 140-2 Security Policy v1.7

Overall Security Level: 2

Prepared by

Booz | Allen | Hamilton

for

TECHGUARD SECURITY
...great walls of fire

Software Version: 2.02.3101

Hardware Models: PW-CCF-M10-01C [1], PW-CCF-M50-01C [2], PW-CCF-G01-01C [3], PW-CCF-G01-01F [3], PW-CCF-G10-01X [4], and PW-CCF-G10-01F [4]

Date	Version	Description	Author
07/21/2011	1.0	Initial Draft	S. Ayhan
10/05/2011	1.1	Added FIPS Error Mode description and update FSM	Derrick Oetting
10/10/2011	1.2	Corrected the FIPS certificate number for the OpenSSL FIPS certification; Added M10/M50 section to the Physical Security section	Derrick Oetting
10/26/2011	1.3	Updates algorithm certificate numbers	Derrick Oetting
11/16/2011	1.4	Added G01 and G10 Physical Security sections	Derrick Oetting
12/15/2011	1.5	Updated information regarding OpenSSL-FIPS	S. Ayhan
01/10/2012	1.6	Update M10/M50 and G10 Physical Security sections. Removed sections excluding the G10's HDs from the cryptographic boundary.	Derrick Oetting
2/8/2012	1.7	Several updates based on comments by reviewers	Derrick Oetting

Contents

1 Introduction 4
2 Product Overview 5
3 Cryptographic Module Specification 6
3.1 FIPS 140-2 Exclusions 6
4 Ports and Interfaces 8
4.1 10 Gigabit Model Ports and Interfaces 8
4.2 1 Gigabit Model Ports and Interfaces 11
4.3 50 Megabit and 10 Megabit Models 13
5 Authentication, Roles, and Services 16
6 Physical Security 24
6.1 M10/M50 24
6.2 G01 27
6.3 G10 30
6.4 Physical Security Inspection 35
7 Operational Environment 36
8 Key Management and Cryptographic Algorithms 37
8.1 Random Number Generators 40
8.2 Key Generation 40
8.3 Key Establishment 41
8.4 Key Entry and Output 41
8.5 Key Storage 42
8.6 Key Zeroization 42
9 EMI/EMC 43
10 Self-Tests 44
11 Mitigation of Other Attacks 47
Appendix A – Acronyms 48
Appendix B – Instructions to put module in FIPS approved mode 49

Figures

Figure 1: 10 Gigabit Model: Front View **8**
Figure 2: 10 Gigabit Model: Back Panel View **9**
Figure 3: 1 Gigabit Model: Front Panel View **11**
Figure 4: 1 Gigabit Model: Back Panel View **12**
Figure 5: 50 Megabit and 10 Megabit Models: Front View **14**
Figure 6: 50 Megabit and 10 Megabit Models: Back Panel View **14**
Figure 7: M10/M50 Rear Opacity Shield **25**
Figure 8: M10/M50 Front Opacity Shield **25**
Figure 9: M10/M50 Tamper Evident Label **26**
Figure 10: M10/M50 Tamper Evident Label **26**
Figure 11: M10/M50 Labeled Diagram (see Table 11) **26**
Figure 12: G01 Front and Lock Tamper Evident Labels **28**
Figure 13: G01 Rear Opacity Shield and Labels for RJ45 Model **28**
Figure 14: G01 Rear Opacity Shield and Labels for Fiber Model **28**
Figure 15: G01 Rear Labeled Diagram (see Table 12) **29**
Figure 16: G01 Front Labeled Diagram (see Table 12) **29**
Figure 17: G10 Labels on Front Bezel **31**
Figure 18: G10 Labels on Hard Drive Bays **31**
Figure 19: G10 Label on Top Cover **32**
Figure 20: G10 Rear Opacity Shield for CX4 Model **32**
Figure 21: G10 Rear Opacity Shield for Fiber Model **32**
Figure 22: G10 Front Labeled Diagram (see Table 13) **33**
Figure 23: G10 Rear Labeled Diagram (see Table 13) **34**
Figure 24: FIPS Mode Indicator **37**

Tables

Table 1: FIPS 104-2 Section Validation Levels **4**
Table 2: 10 Gigabit Model: Front View Ports and Interfaces **9**
Table 3: 10 Gigabit Model: Back Panel View Ports and Interfaces **10**
Table 4: 1 Gigabit Model: Front Panel View Ports and Interfaces **11**
Table 5: 1 Gigabit Model: Back Panel View Ports and Interfaces **12**
Table 6: 50 Megabit and 10 Megabit Models: Front Panel View Ports and Interfaces **14**
Table 7: 50 Megabit and 10 Megabit Models: Back Panel View Ports and Interfaces **14**
Table 8: Roles and Required Identification and Authentication **17**
Table 9: Strengths of Authentication Mechanisms **17**
Table 10: Authorized Services **19**
Table 11: M10/M50 Label Placement and Descriptions **27**
Table 12: G01 Label Placement and Descriptions **30**
Table 13: Inspection of Physical Security **35**
Table 14: PoliWall Processors **36**
Table 15: Validated Algorithms and Key Sizes **38**
Table 16: PoliWall Non Approved Algorithms **38**
Table 17: Cryptographic Keys, CSPs, and Other Security-Relevant Information **38**
Table 18: Key Management **39**
Table 19: PoliWall Self-Tests **44**
Table 20: Acronyms **48**

1 Introduction

This document is the non-proprietary Federal Information Processing Standard (FIPS) 140-2 Security Policy for TechGuard's PoliWall-CCF M10, M50, G01, and G10 Series Security Appliance. This security policy demonstrates how the PoliWall appliance meets validation requirements for an overall Level 2 FIPS 140-2 Validation with Level 3 Design Assurance.

The following table outlines the validation level for the requirements of each FIPS PUB 140-2 section.

Table 1: FIPS 104-2 Section Validation Levels

Section Number	FIPS 140-2 Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference/Electromagnetic Compatibility	2
9	Self-Test	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2 Product Overview

The TechGuard Security PoliWall is a network boundary device that rapidly determines the country of origin for all incoming packets using HIPPIE™ (High-speed Internet Protocol Packet Inspection Engine) technology. Packets are filtered according to defined policies, exception lists, and Pre-Compiled Exception Lists (PCEL) that are bound to rule groups for specific network addresses and protocols. PoliWall also provides administrators with the ability to create "maps" which exclude traffic from selected countries. PoliWall allows administrators to customize their workspace via a Graphical User Interface (GUI). PoliWall leverages some of the approved security functions defined in FIPS 140-2 Annex A and C from the OpenSSL-FIPS software module. OpenSSL-FIPS is a FIPS 140-2 Level 1 validated cryptographic module with certificate #1051, and is delivered in source code form. All required self-tests for these security functions are also implemented within OpenSSL-FIPS. The PoliWall module provides additional approved security functions, including key establishment techniques defined in FIPS 140-2 Annex D.

3 Cryptographic Module Specification

The cryptographic module is the PoliWall appliance. It is a multi-chip standalone device with its cryptographic boundary drawn around its entire platform enclosure, or in other words, around the PoliWall's chassis, including its standard hardware ports. All hardware components contained within the chassis are included in the cryptographic boundary. Moreover, all software running on the hardware components within the chassis are also included within the cryptographic boundary.

The PoliWall appliance comes in six different hardware models. These models are:

- 10 Gigabit CX4 (PW-CCF-G10-01X)
- 10 Gigabit Fiber (PW-CCF-G10-01F)
- 1 Gigabit RJ45 (PW-CCF-G01-01C)
- 1 Gigabit Fiber (PW-CCF-G01-01F)
- 50 Megabit RJ45 (PW-CCF-M50-01C)
- 10 Megabit RJ45 (PW-CCF-M10-01C)

The difference between these models' functionality is strictly performance based. There is no difference in core functionality or cryptographic services between the models. The 10 Gigabit, 1 Gigabit, and 50 Megabit models all have different hardware platforms; however, the 50 Megabit and 10 Megabit models operate on identical hardware platforms with the only difference between them being the amount of throughput they are licensed to handle. Diagrams of each model, including its physical ports, are included in the next section.

TechGuard product documentation refers to the Console CO mode as Maintenance Mode, however for the purposes of the FIPS 140-2 validation it shall be known as Console CO mode. This statement is made to avoid confusion with defined FIPS 140-2 terminology.

3.1 FIPS 140-2 Exclusions

All internal power supply components on all hardware models are excluded from the FIPS 140-2 requirements. The power supplies on the PoliWall devices have their own internal enclosure completely contained within the PoliWall chassis. The excluded components can be defined as any components within the internal enclosure of the power supply. The power supply components are excluded as they are not cryptography or security relevant. The components of the power supply solely perform Alternating Current (AC) to Direct Current (DC) conversion. If these power supply components malfunction, the PoliWall will not be able to receive power, making it impossible to compromise it or any of the data it handles in this malfunctioned state.

The Recovery Console is also excluded from the FIPS 140-2 requirements. It is used to initially configure the PoliWall's network interface, install licenses issued from TechGuard Security, or restore the PoliWall to its factory defaults. The Recovery Console does require physical access to the device itself, so it is advised to keep the PoliWall in a secure location at all times. The Recovery Console is excluded because it is only used to initially configure the PoliWall when

received directly from TechGuard Security, or to reset the PoliWall. It is not used during normal operation of the PoliWall and puts the device into "Bypass mode," meaning no traffic going through the device is filtered.

4 Ports and Interfaces

The PoliWall has several physical ports. These physical ports are logically categorized into one of the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The tables and figures in this section show all physical ports on the PoliWall models. Some physical ports may be mapped to more than one logical interface. Tables are provided that include a mapping of physical ports to FIPS 140-2 defined logical interfaces.

Note that the PoliWall appliances have unused physical ports. These are not configurable and serve no functional purpose. The unused ports do not allow for any sort of input or output and will therefore not be categorized into logical interfaces. All unused ports are listed in the tables found in this section.

4.1 10 Gigabit Model Ports and Interfaces

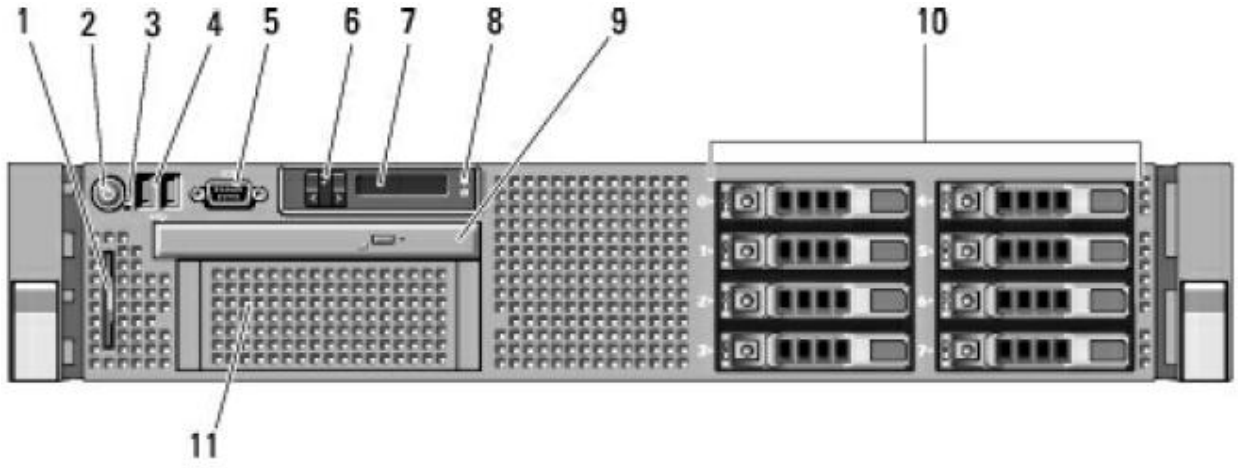

Figure 1: 10 Gigabit Model: Front View

The locations in the table below directly correspond to the numbers in the diagram directly above.

Table 2: 10 Gigabit Model: Front View Ports and Interfaces

Location	Physical Component	Description	Logical Interface
1	Information tag	Contains information on the appliance. This is not a port.	N/A
2	Power button	The button used to power on and off the appliance.	Control Input
2	Power indicator	Glows green when the appliance is powered on. It is off otherwise.	Status Output
3	Non-Maskable Interrupt button	Used by authorized technicians for troubleshooting the unit. Not used in normal operation of the PoliWall.	Control Input
4	2 USB 2.0 ports	Used to connect a keyboard in Console Mode. Menu item selections are sent over the Control Input interface. Authentication data are sent over the Data Input interface.	Control Input, Data Input
5	VGA port	Used to connect a monitor in Console Mode. Status messages go over the Status Output interface. Data messages (e.g. audit logs) go over the Data Output interface.	Status Output, Data Output
6	2 LCD menu buttons	Used to select diagnostic messages to display on the Liquid Crystal Display (LCD) panel.	Control Input
7	LCD panel	Backlit solid blue during normal operation, flashes blue if System identification button is pressed, backlit amber during error states. Will also display error messages.	Status Output
8	System identification button	Will cause LCD and System status indicator on back panel to flash. This helps to more easily identify the PoliWall on a rack with many machines.	Control Input
9	Optical drive	Used by manufacturer to initially install software and firmware. Not used during normal operation.	Control Input
10	Hard drive bays	Used to connect hard drives. Data written to the hard drive goes over the Data Input interface. Data read from the hard drive go over the Data Output interface.	Data Input, Data Output
11	Flex Bay	Not used.	N/A

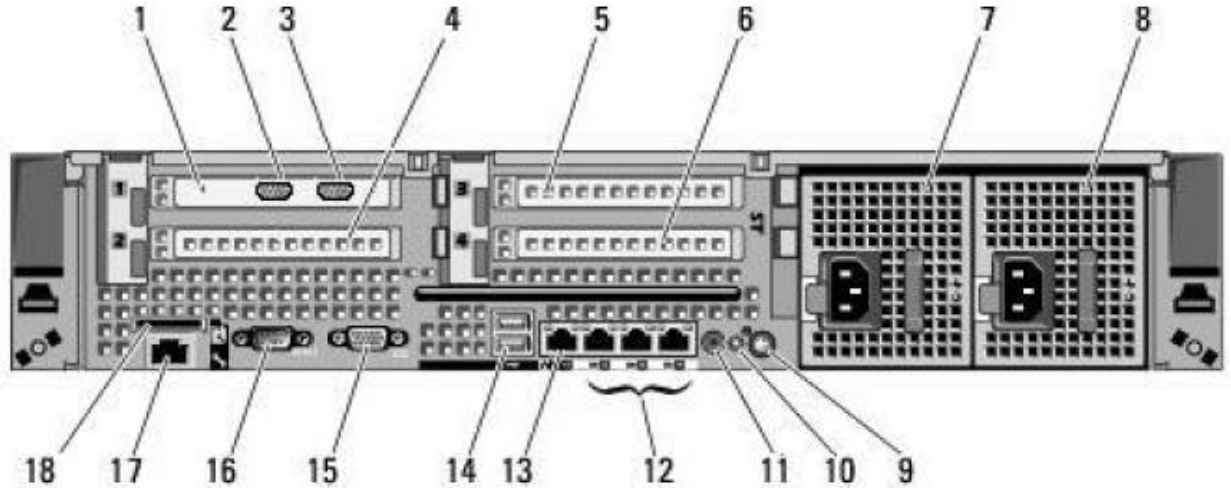

Figure 2: 10 Gigabit Model: Back Panel View

The locations in the table below directly correspond to the numbers in the diagram directly above.

Table 3: 10 Gigabit Model: Back Panel View Ports and Interfaces

Location	Physical Component	Description	Logical Interface
1	PCIe Slot 1	PCIe card slot containing a PCIe card. The card containing the Local Network Bridging Port and Internet Bridging Port is inserted here.	Data Input, Data Output
2	Local Network Bridging Port	Ethernet bridging port to local or internal network. Packets originating from inside the local network travel over the Data Input interface. Packets originating from outside the local network travel over the Data Output interface. This interface is either CX4 or Fiber depending on the model.	Data Input, Data Output
3	Internet Bridging Port	Ethernet bridging port to internet. Packets originating from outside the local network travel over the Data Input interface. Packets originating from inside the local network travel over the Data Output interface. This interface is either CX4 or Fiber depending on the model.	Data Input, Data Output
4	PCIe slot 2	Not used.	N/A
5	PCIe slot 3	Not used.	N/A
6	PCIe slot 4	Not used.	N/A
7, 8	Power ports	Ports to the appliance's power supplies	Power
7, 8	Power supply status lights	Light off: no power connected. Solid green: operating normally. Amber, or flashing green and amber: problem with power supply.	Status Output
9	System Identification button	Will cause LCD and System status indicator on back panel to flash. This helps to more easily identify the PoliWall on a rack with many machines.	Control Input
10	System Status Indicator	Blue when system is operating normally, yellow when there is a problem, flashing blue when System identification button is pressed.	Status Output
11	System identification connector	Not used.	N/A
12	3 Ethernet connectors	These three connectors are unused.	N/A
13	Administration Port	Ethernet port used by operators of the web interface. Data output from this interface (e.g. audit data) goes over the Data Output interface. Any actions taken on the web GUI with a mouse or keyboard are input via the Control Input interface. Status messages sent to the administrator are sent over the Status Output interface. Any non-control input data, including usernames or passwords, are sent over the Data Input interface.	Data Output, Data Input, Control Input, Status Output
13	Left Ethernet Status Light	Light off: not connected to a network. Green: connected to a 1 Gigabit network. Amber: connected to a 10 or 100 Megabit network.	Status Output
13	Right Ethernet Status Light	When there is network activity, this light flashes.	Status Output
14	2 USB 2.0 ports	Used to connect a keyboard in Console Mode. Menu item selections are sent over the Control Input interface. Authentication data are sent over the Data Input interface.	Control Input, Data Input

Location	Physical Component	Description	Logical Interface
15	VGA port	Used to connect to a monitor in Console mode. Status messages are sent over the status output interface. Data messages (e.g. audit data) are sent over the data output interface.	Status Output, Data Output
16	Serial Port	Used for terminal access in Console mode as an alternative to using the Universal Serial Bus (USB) and Video Graphics Array (VGA) ports. Any instructions sent via the serial port go over the Control Input interface and are input via a keyboard. Any data messages sent to the operator (e.g. audit data) are sent over the Data Output interface and may be displayed on a monitor. Any status messages sent to the operator are done over the Status Output interface and may be displayed on a monitor. Any non-control input data, including usernames or passwords, are sent over the Data Input interface.	Control Input, Data Input, Data Output, Status Output
17	Enterprise Port	Not used.	N/A
18	VFlash media slot	Not used.	N/A

4.2 1 Gigabit Model Ports and Interfaces

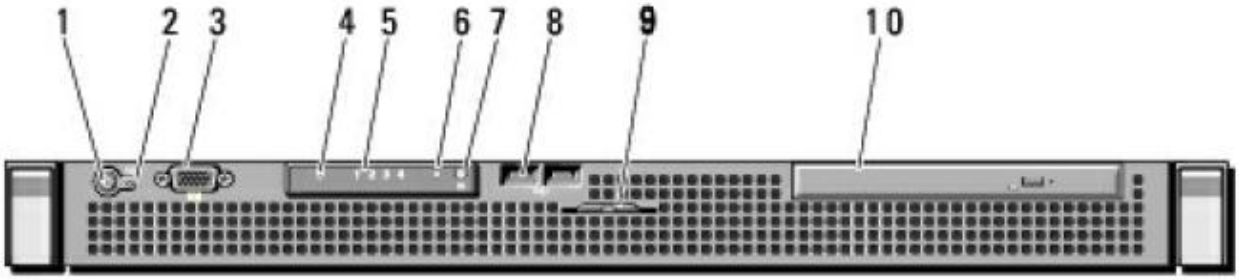

Figure 3: 1 Gigabit Model: Front Panel View

The locations in the table below directly correspond to the numbers in the diagram directly above.

Table 4: 1 Gigabit Model: Front Panel View Ports and Interfaces

Location	Physical Component	Description	Logical Interface
1	Power button	The button used to power on and off the appliance.	Control Input
1	Power indicator	Glows green when the appliance is powered on. It is off otherwise.	Status Output
2	Non-Maskable Interrupt button	Used for troubleshooting the unit.	Control Input
3	VGA port	Used to connect a monitor in Console Mode. Status messages go over the status output interface. Data messages (e.g. audit logs) go over the data output interface.	Status Output, Data Output
4	Hard drive activity light	Flashes when hard drive is in use.	Status Output
5	Diagnostic Indicator Lights	When there is a hardware failure, at least one of these lights is lit after the appliance boots up.	Status Output
6	System Status Indicator	Blue when system is operating normally, yellow	Status Output

Location	Physical Component	Description	Logical Interface
		when there is a problem, flashing blue when System identification button is pressed.	
7	System identification button	Will cause LCD and System status indicator on back panel to flash. This helps to more easily identify the PoliWall on a rack with many machines.	Control Input
8	2 USB 2.0 ports	Used to connect a keyboard in Console Mode. Menu item selections are sent over the Control Input interface. Authentication data are sent over the Data Input interface.	Control Input, Data Input
9	Information tag	Contains information on the appliance. This is not a port.	N/A
10	Optical drive	Used by manufacturer to initially install software and firmware. Not used during normal operation.	Control Input

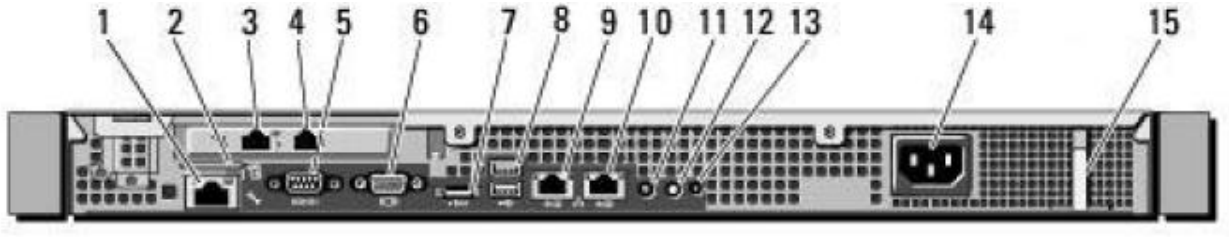

Figure 4: 1 Gigabit Model: Back Panel View

The locations in the table below directly correspond to the numbers in the diagram directly above.

Table 5: 1 Gigabit Model: Back Panel View Ports and Interfaces

Location	Physical Component	Description	Logical Interface
1	Enterprise Port	Not used.	N/A
2	VFlash media slot	Not used.	N/A
3	Local Network Bridging Port	Ethernet bridging port to local or internal network. Packets originating from inside the local network travel over the Data Input interface. Packets originating from outside the local network go over the Data Output interface. This interface is either RJ45 or Fiber depending on the model.	Data Input, Data Output
4	Internet Bridging Port	Ethernet bridging port to internet. Packets originating from outside the local network travel over the Data Input interface. Packets originating from inside the local network go over the Data Output interface. This interface is either RJ45 or Fiber depending on the model.	Data Input, Data Output
5	Serial Port	Used for terminal access in Console mode as an alternative to using the USB and VGA ports. Any instructions sent via the serial port go over the Control Input interface and are input via a keyboard. Any data messages sent to the operator (e.g. audit data) are sent over the Data Output interface and	Control Input, Data Input, Data Output, Status Output

Location	Physical Component	Description	Logical Interface
		may be displayed on a monitor. Any status messages sent to the operator are done over the Status Output interface and may be displayed on a monitor. Any non-control input data, including usernames or passwords, are sent over the Data Input interface.	
6	VGA port	Used to connect a monitor in Console Mode. Status messages go over the Status Output interface. Data messages (e.g. audit logs) go over the Data Output interface.	Status Output, Data Output
7	eSATA port	Not used.	N/A
8	2 USB 2.0 ports	Used to connect a keyboard in Console Mode. Menu item selections are sent over the Control Input interface. Authentication data is sent over the Data Input interface.	Control Input, Data Input
9	Administration Port	Ethernet port used by operators of the web interface. Data output from this interface (e.g. audit data) goes over the Data Output interface. Any actions taken on the web GUI with a mouse or keyboard are input via the Control Input interface. Status messages sent to the administrator are sent over the Status Output interface. Any non-control input data, including usernames or passwords, are sent over the Data Input interface.	Data Output, Data Input, Control Input, Status Output
9	Left Ethernet Status Light	Light off: not connected to a network. Green: connected to a 1 Gigabit network. Amber: connected to a 10 or 100 Megabit network.	Status Output
9	Right Ethernet Status Light	When there is network activity, this light flashes.	Status Output
10	Unused Ethernet connector	Not used.	N/A
11	System Status Indicator	Blue when system is operating normally, yellow when there is a problem, flashing blue when System identification button is pressed.	Status Output
12	System Identification button	Will cause LCD and System status indicator on back panel to flash.	Control Input
13	System identification connector	Not used.	N/A
14	Power supply status lights	Light off: no power connected. Solid green: operating normally. Amber, or flashing green and amber: problem with power supply.	Status Output
15	Retention Clip	Secures the power cord. This is not a port.	N/A

4.3 50 Megabit and 10 Megabit Models

The 50 Megabit and 10 Megabit PoliWall models operate on identical hardware platforms. Similarly, the ports and interfaces of the 50 Megabit and 10 Megabit models are identical.

Figure 5: 50 Megabit and 10 Megabit Models: Front View

The locations in the table below directly correspond to the numbers in the diagram directly above.

Table 6: 50 Megabit and 10 Megabit Models: Front Panel View Ports and Interfaces

Location	Physical Component	Description	Logical Interface
1	Indicator Light Panel	Contains five status lights. From left to right they are: overheat/fan failure light, NIC2 activity light (not used), NIC1 activity light indicating activity on the administration interface, Hard Disk Drive (HDD) access light, power light.	Status Output
2	Reset Button	Manually reboots the PoliWall when pressed.	Control Input
3	Power Button	Powers up/down the PoliWall	Control Input

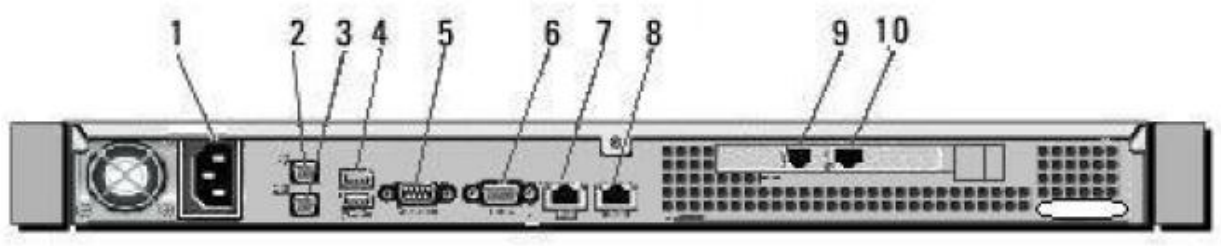

Figure 6: 50 Megabit and 10 Megabit Models: Back Panel View

The locations in the table below directly correspond to the numbers in the diagram directly above.

Table 7: 50 Megabit and 10 Megabit Models: Back Panel View Ports and Interfaces

Location	Physical Component	Description	Logical Interface
1	Power Port	Power port that allows external power to be input to the PoliWall.	Power
2	PS/2 Mouse port	Not used.	N/A
3	PS/2 Keyboard Port	Used to connect a keyboard to the PoliWall in place of a keyboard that is connected via USB. Used in Console CO Mode and in FIPS Error Mode.	Control Input, Data Input
4	2 USB 2.0 ports	Used to connect a keyboard to the PoliWall in place of a keyboard that is connected via PS/2. Used in	Control Input, Data Input

Location	Physical Component	Description	Logical Interface
		Console CO Mode and FIPS Error Mode. Menu item selections are sent over the Control Input interface. Authentication data are sent over the Data Input interface.	
5	VGA port	Used to connect a monitor during Console CO Mode and FIPS Error Mode. Status messages are sent over the Status Output interface. Audit logs and other non-status data are sent over the Data Output interface.	Status Output, Data Output
6	Serial Port: RS232-C connector	Can be used to display data and enter input in Console CO Mode and FIPS Error Mode, in place of a VGA port and USB or PS/2 port. Any menu selections are sent via the Control Input interface. Any status messages are sent over the Status Output interface. Any non-status output, such as output data, is sent over the Data Output interface. Any non-control input data, including usernames or passwords, are sent over the Data Input interface.	Control Input, Data Input, Status Output, Data Output
7	Administration Port	Ethernet port used for administering the PoliWall remotely via the web GUI. Any actions taken on the web GUI are sent over the Control Input interface. Any non-control input data, including usernames or passwords, are sent over the Data Input interface. Any status messages are sent out over the Status Output interface. Any non-status output data, including Public-Key Cryptography Standards #12 (PKCS12) files or audit messages, are sent over the Data Output interface.	Control Input, Data Input, Status Output, Data Output
8	Ethernet Connector	This port is unused.	N/A
9	Internet Bridging Port	Ethernet bridging port to internet. Packets originating from outside the local network travel over the Data Input interface. Packets originating from inside the local network go over the Data Output interface.	Data Input, Data Output
10	Local Network Bridging Port	Ethernet bridging port to local or internal network. Packets originating from inside the local network travel over the Data Input interface. Packets originating from outside the local network go over the Data Output interface.	Data Input, Data Output

5 Authentication, Roles, and Services

The PoliWall can be accessed by any of the following methods:

- Console port
- HTTPS/TLS

The appliance has seven default roles that operators can assume: six Cryptographic Officer (CO) roles and one User role per FIPS 140-2 definitions. The web interface allows multiple operators to be logged in concurrently, but the console only allows one operator to be logged in at a time. Logging in establishes a unique user session for the operator. Sessions are maintained until the operator logs out, the operator is inactive for a configurable amount of time, or there is an interruption in communication to the appliance (e.g. rebooting the PoliWall will terminate all active sessions). Operators of the web interface may hold more than one role. Operators with multiple roles may actively switch the role that they are currently in, but doing so requires re-authentication. The roles supported by the module and a full list of services available to each role are outlined in the tables of this section.

The PoliWall may be accessed in two different ways. The first is through the web GUI. Operators of the web GUI access the device by establishing a trusted channel to the PoliWall's web server. The trusted channel is encrypted using IPsec and/or Transport Layer Security (TLS) 1.0. Local administrators access the device by connecting a serial cable to the PoliWall's console port or by connecting a USB and VGA cable to their respective ports on the device. The purpose and location of each physical port is outlined in the "Ports and Interfaces" section of this Security Policy. Local operators only have access to Console CO Mode, which contains a separate set of services from the web operator roles.

Table 8: Roles and Required Identification and Authentication

FIPS 140-2 Role	Role	Description	Type of Access	Type of Authentication
Cryptographic Officer	Cryptographic Administrator	Manages all cryptographic functionality, including uploading certificates and keys.	Web	Role-based
	Security Administrator	Has access to non-cryptography related security services, including configuration of the automatic self-test interval and creation of new web interface operators.	Web	Role-based
	Audit Administrator	Has the ability to delete audit records.	Web	Role-based
	security_admin	Has the ability to reset accounts and configuration in Console CO Mode.*	Local	Role-based
	crypto_admin	Has the ability to zeroize keys in Console CO Mode.*	Local	Role-based
	audit_admin	Has the ability to view and delete audit records in Console CO Mode.*	Local	Role-based
User	Read-Only	Has the ability to read configuration items without the ability to change them.	Web	Role-based
*The term "Console CO Mode" used throughout the Security Policy is a PoliWall defined mode and is refered to as "Maintenance Mode" in the product documentation. The roles which have access to "Maintenance Mode" are not to be confused with a maintenance role defined by the FIPS 140-2. The PoliWall has no FIPS 140-2 defined maintenance role.				

All of the roles defined in the above table have access to all physical ports and their corresponding logical interfaces defined in the tables of the "Ports and Interfaces" section, with a few exceptions. Only operators of the security_admin, audit_admin, and crypto_admin roles have access to console ports, VGA ports, and USB ports on the device. Only operators of the Cryptographic Administrator, Security Administrator, Audit Administrator, and Read-Only roles have access to Administration Port on the device.

The two authentication methods employed by the PoliWall are X.509 certificates and username/passwords. All operators of the web interface must authenticate using their configured username and password. As an added security measure, Security Administrators may also configure the PoliWall to require client certificates as part of the authentication process. This also requires that a CA certificate be installed on the PoliWall. The client certificates installed in the web operator's browser must be allowed by the installed CA certificate. Note that client certificates are not unique per operator. The strength of the authentication mechanisms is provided below in the table entitled "Strength of Authentication Mechanisms".

Table 9: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
X.509 certificate	The X.509 certificates utilize RSA 2048 public keys which provide a false authentication probability that is far less than 1/1,000,000. The certificates are secure enough so that continuous authentication attempts in a one-minute interval will have a false acceptance probability far less than 1/100,000. Note that X.509certificates can be implemented in addition to username and password, but cannot be the only form of operator authentication.
Password	The password must contain at least 5 alphanumeric or special characters, so the

	password space is 94 ^ 5 = 7,339,040,224. This has a false authentication probability of less than 1/1,000,000. After a maximum of 12 failed login attempts, the account will be locked for at least 1 minute. Within 1 minute a user can attempt at most 12 logins. Therefore, the probability of a false authentication occurring in a one minute interval is 12 * (1/7,339,040,224) which is less than 1/100,000.

Each of the roles above share no overlap of service privileges with the following exceptions:

- Operators of all roles are permitted to view the audit trail and public key certificates.
- All web interface operators, except those with the Read-Only role, are permitted to activate self-tests.
- All web interface operators are able to view and acknowledge security alarms*, except operators of the Read-Only role. Read-Only users are only able to view security alarms.

*Security alarms are raised when certain events occur - e.g. an operator enters an incorrect password - and appear in the top right corner of the web GUI. The set of events that cause security alarms to be raised is configurable by operators of the Security Administrator role.

The cryptographic services available to each role are delineated in the following table (note: "PoliWall Configuration" and "Audit Data" are not Keys/CSPs, but are included to provide information on the type of data the service affects):

Table 10: Authorized Services

Role(s)	Authorized Service	Description	Keys/CSPs	Type of Access
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only, security_admin, crypto_admin, audit_admin	Show Status	Displays the status of the PoliWall. This service is continuously performed by the status indicators on the appliance.	N/A	N/A
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only	Log in to PoliWall web interface	Establishes a session with the PoliWall web server. Proper authentication is required.	X509 certificate, username/password	N/A
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only	Log out of the PoliWall web interface	Terminates an active operator session with the PoliWall web server.	N/A	N/A
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only	Change Role	Changes from one web interface role to another. Re-authentication is required.	N/A	N/A
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only	View security alarms	Displays security alarm text.	N/A	R
Cryptographic Administrator, Audit Administrator, Security Administrator	Acknowledge security alarms	Acknowledges and clears a security alarm.	N/A	R,W
Cryptographic Administrator, Audit Administrator, Security	View Alarm Settings	View settings for various alarms (raised, audible, etc.)	N/A	R

Role(s)	Authorized Service	Description	Keys/CSPs	Type of Access
Administrator, Read-Only				
Security Administrator	Modify Alarm Settings	Change settings for various alarms (raised, audible, etc.)	N/A	R,W
Cryptographic Administrator, Audit Administrator, Security Administrator	Perform self-tests	Performs all self-tests on demand. Note: these are not the full FIPS self-tests. To run the full FIPS self-tests, you must reboot the PoliWall.	N/A	N/A
Security Administrator	Reboot	Reboot the PoliWall	N/A	N/A
Security Administrator	Shutdown	Shutdown the PoliWall	N/A	N/A
Security Administrator	Firmware load test	A firmware load test is performed when attempting to update the firmware.	Firmware Public Key	R
Security Administrator	Create and manage operators	Manages web interface operator privileges. This includes assigning roles.	PoliWall Configuration	R,W
Security Administrator	Define policies for remote access to the PoliWall	Defines policies including restriction by IP and date/time (in User Accounts -> edit an account -> Edit Access Restrictions).	PoliWall Configuration	R,W
Security Administrator	Modify Password Policy	Changes character requirements for passwords.	PoliWall Configuration	R,W
Security Administrator	Configure self-test periodic interval	Configures the time between each automatic self-test. Note: these are not the full FIPS self-tests. To run the full FIPS self-tests, you must reboot the PoliWall.	PoliWall Configuration	R,W
Security Administrator	Modify Admin Session Policy	Configures settings to specify maximum session duration and inactivity timeout.	PoliWall Configuration	R,W
Security Administrator	Configure maximum failed authentication attempts	Configures the maximum number of times a web interface operator may incorrectly authenticate before being locked out.	PoliWall Configuration	R,W
Security Administrator	Configure lockout timer	Configures the length of time a web interface operator is prevented from authenticating when locked out. The default length is 30	PoliWall Configuration	R,W

Role(s)	Authorized Service	Description	Keys/CSPs	Type of Access
		minutes.		
Security Administrator	Unlocked locked user	Instantly unlocks a web interface operator in place of waiting for the lockout timer to expire.	N/A	N/A
Cryptographic Administrator	Generate public key certificate	Generates a public key certificate for the PoliWall.	X.509 public key certificate	R,W
Cryptographic Administrator	Generate private key for server	Generates a private key for the PoliWall.	X.509 private key	W
Cryptographic Administrator	Upload PKCS12 file	Uploads a PKCS12 file containing a public key certificate and private key.	X5.09 public key certificate, X.509 private key	W
Cryptographic Administrator	Install X.509 certificate used for client certificate authentication (CA Cert)	Installs X.509 certificate used for client certificate authentication.	X5.09 public key certificate	R,W
Cryptographic Administrator	Install CRL for client certificates	Install a certificate revocation list for client certificates.	PoliWall Configuration	R,W
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only	View server certificate	Displays a public key certificate.	X5.09 public key certificate	R
Cryptographic Administrator	Enable or disable client certificate requirement	Mandates whether or not a client certificate is required for authentication.	PoliWall Configuration	R,W
Cryptographic Administrator	Configure IPsec tunnel settings	Configures various settings for IPsec tunnels. These settings include encryption algorithm, authentication algorithm, DH group, and destination network.	PoliWall Configuration	R,W
Cryptographic Administrator	Activate FIPS mode	Turns on FIPS mode. This limits the algorithms and modes of operation to only those approved or allowed by FIPS 140-2.	PoliWall Configuration	R,W
Audit Administrator	Delete audit logs through web interface	Deletes audit messages from the selected audit log.	Audit Data	W
Cryptographic Administrator, Audit Administrator, Security Administrator, Read-Only	View all other configuration items provided by the PoliWall	The ability to view all other configuration items provided by the PoliWall, including Resources, Policies, etc.	PoliWall Configuration	R

Role(s)	Authorized Service	Description	Keys/CSPs	Type of Access
		through the web interface.		
Security Administrator	Modify all other configuration items provided by the PoliWall	The ability to modify all other configuration items provided by the PoliWall, including Resources, Policies, etc. through the web interface.	PoliWall Configuration	R,W
security_admin, crypto_admin, audit_admin	Log into the Console CO Mode interface.	Brings up a prompt to enter Console CO Mode if not already in Console CO Mode. If already in Console CO Mode, brings up menu choices for Console CO Mode services.	N/A	N/A
security_admin, crypto_admin, audit_admin	Log out of Console CO Mode.	Logs out of the Console CO Mode interface.	N/A	N/A
security_admin, crypto_admin, audit_admin	Enter Console CO Mode	Manually enters Console CO Mode after logging into the Console CO Mode interface. This can only be done if not already in Console CO Mode.	N/A	N/A
security_admin, crypto_admin, audit_admin	Reboot the PoliWall	Restarts the PoliWall appliance through Console CO Mode.	N/A	N/A
security_admin	Reset admin accounts	Restores default settings to all admin accounts. This is done through Console CO Mode.	PoliWall Configuration	W
security_admin	Reset administration interface	Restores default settings to the administration interface. This is done through Console CO Mode.	PoliWall Configuration	W
security_admin	Reset configuration	Resets all settings on the PoliWall to their factory defaults. This is done through Console CO Mode.	PoliWall Configuration	W
crypto_admin	Zeroize all cryptographic keys	Destroys all cryptographic keys on the appliance.	X509 certificate, X509 private key, passwords, IPsec parameters	W
audit_admin	View message logs	Displays messages from the message log file.	Audit Data	W
audit_admin	Delete IPv4 packet log messages	Specifies a percentage of audit records to delete from the IPv4 packet log.	Audit Data	W
audit_admin	Delete IPv6	Specifies a percentage	Audit Data	W

Role(s)	Authorized Service	Description	Keys/CSPs	Type of Access
	packet log messages	of audit records to delete from the IPv6 packet log.		
audit_admin	Delete message log messages	Specifies a percentage of audit records to delete from the message log.	Audit Data	W

When the module is operating in a non-FIPS approved mode, the following services may use non-FIPS approved algorithms:

- IPsec - DH groups 16, 17, and 18, MD5, DES, RSA with keys sizes under 1024 bits
- Web Server (SSL and Certificates) - MD5, DES, RSA with keys sizes under 1024 bits

6 Physical Security

The PoliWall must have opacity shields and serialized tamper evident stickers installed to ensure the device meets the opacity and tamper evident requirements. The required locations of the shields and stickers for each model are detailed below. The Cryptographic Officer must record the serial numbers of all stickers and must periodically inspect the device for signs of tampering and changed serial numbers. The tamper evident stickers and opacity shields shall be installed for the module to operate in a FIPS approved mode of operation.

6.1 M10/M50

The M10 and M50 PoliWall appliances run on the same hardware, therefore their physical security is identical. The appliances are built from production grade components and purchased from a commercial reseller (MBX). The manufacturers built the components using industry standard passivation techniques to meet commercial grade specifications for power, temperature, reliability, shock and vibration. The entire module is enclosed in a commercial grade hard sheet metal case. The part number of the M10/M50 FIPS Kit is PW-CCF-M10-FK1, which contains the following parts:

- Item 137821 – Blanking Plate Assembly
- Item 137823 – Fan Shield Assembly
- Item 137826 – One Rear IOS Cover Assembly
- Item 137076 – One Hardware Kit
- Item 138759 – Two 1 x 4 inch labels

Module Opacity

The M10/M50 PoliWalls have two opacity shields which are installed, one in the front and one in the rear, that prevent the viewing of the internal components but still allow air flow through the chassis. The opacity shield in the front is placed inside the chassis and prevents viewing components through the front louvers. It also contains a fan to increase airflow. The opacity shield in the rear is attached on the outside of the chassis with nuts on the inside and prevents viewing components through the rear air vents. It has louvered slots on one side to allow air flow and still prevent the viewing of components.

Tamper Evidence

Two (2) pieces of serialized, tamper evident tape are placed across the lid to ensure the lid cannot be removed without evidence of tempering. All of the shields are attached from the inside and cannot be removed without first removing the lid or destroying the shield and therefore showing evidence of tampering.

Figure 7: M10/M50 Rear Opacity Shield

Figure 8: M10/M50 Front Opacity Shield

Figure 9: M10/M50 Tamper Evident Label

Figure 10: M10/M50 Tamper Evident Label

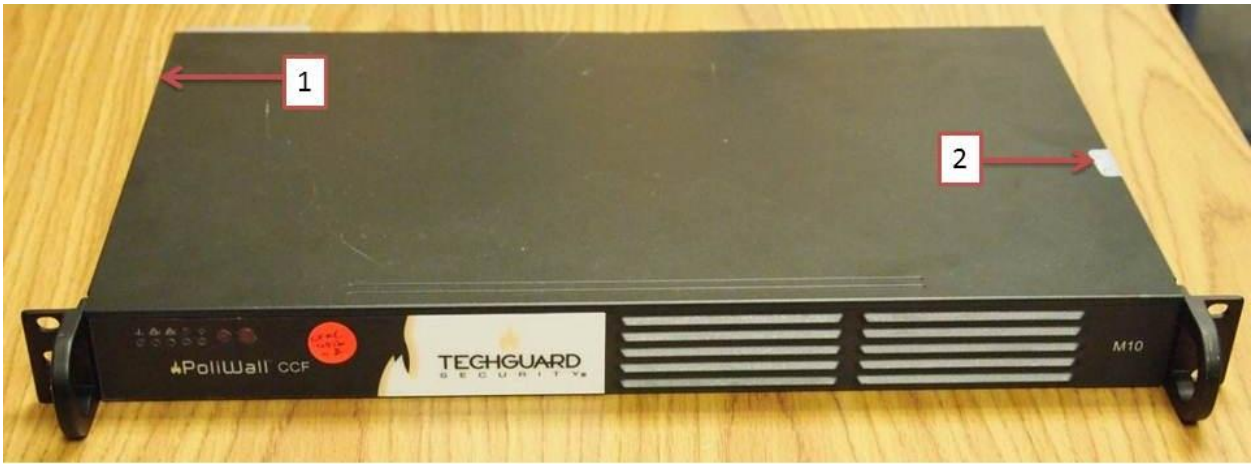

Figure 11: M10/M50 Labeled Diagram (see Table 11)

Location	Description
1	Tamper Evident Label
2	Tamper Evident Label

Table 11: M10/M50 Label Placement and Descriptions

6.2 G01

The G01 appliances are built from production grade components and purchased from a commercial reseller (Dell). The manufacturers built the components using industry standard passivation techniques to meet commercial grade specifications for power, temperature, reliability, shock and vibration. The entire module is enclosed in a commercial grade hard sheet metal case. The part number of the G01 FIPS Kit is PW-CCF-G01-FK1, which contains the following parts:

- TEC-210-F01 – One Opacity Shield
- TEC-210-F02 – One 5.5 x 1.75 inch label for the top cover
- TEC-210-F03 – One 3.25 x 0.5 inch label for the front
- TEC-710-F05 – Five 0.5 x 1 inch labels for various places

Module Opacity

The G01 PoliWalls have one (1) opacity shield with seven (7) tamper evident labels. The opacity shield covers ventilation holes in the rear. It has holes that allow sufficient airflow through the device but prevent the viewing of components inside the chassis. It is attached with two plastic fasteners and two tamper evident labels. Four (4) tamper evident labels are placed on the chassis to prevent the viewing of components through ventilation holes – one on the front bezel, one on the top cover and 2 on the rear. With these ventilation holes covered, there is still enough airflow through the system to keep it cool.

Tamper Evidence

Three (3) tamper evident labels are used to make the device tamper evident. One is placed on the top cover so the top cover cannot be removed without destroying the label. Two (2) labels are used on the edges of the opacity shield to show evidence of the shield being bent or moved. All of the labels are serialized so the Cryptographic Officer can verify that no labels have been replaced.

Figure 12: G01 Front and Lock Tamper Evident Labels

Figure 13: G01 Rear Opacity Shield and Labels for RJ45 Model

Figure 14: G01 Rear Opacity Shield and Labels for Fiber Model

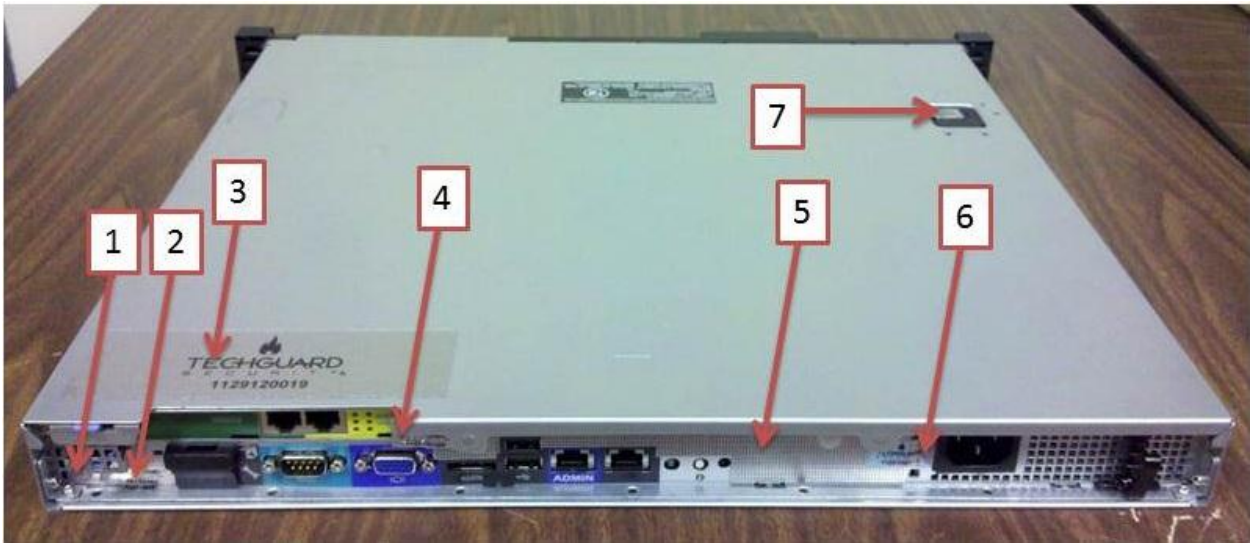

Figure 15: G01 Rear Labeled Diagram (see Table 12)

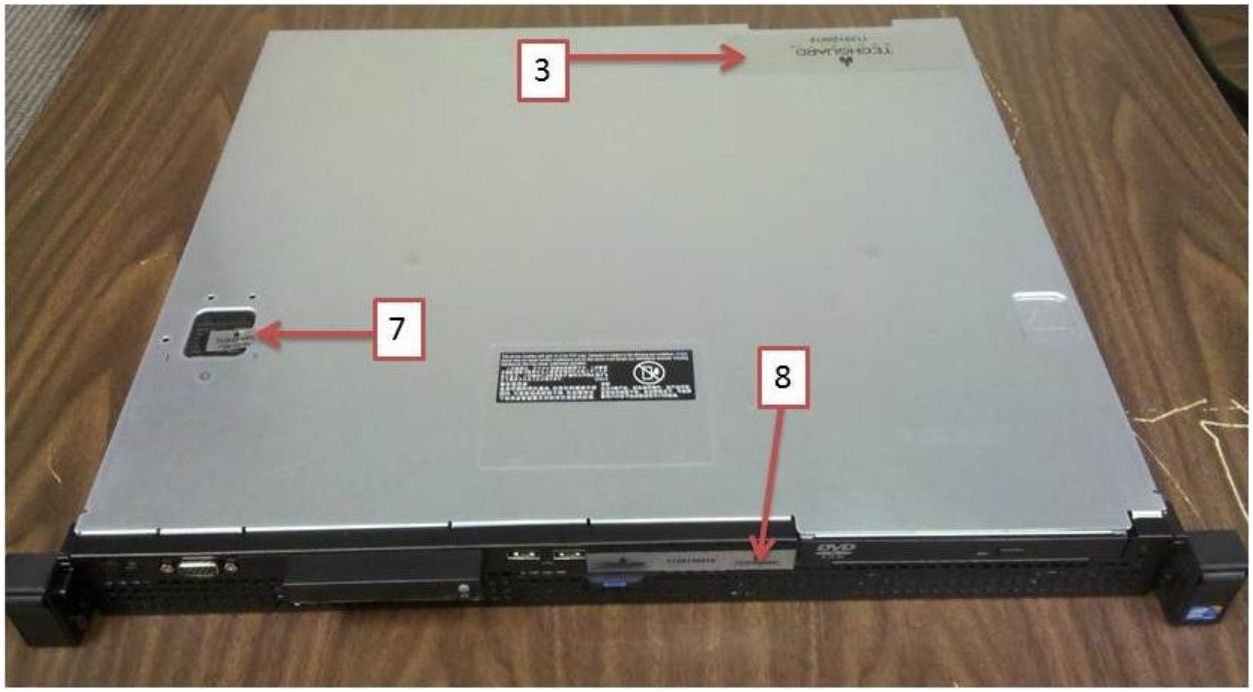

Figure 16: G01 Front Labeled Diagram (see Table 12)

Location	Description
1	0.5 x 1 inch tamper evident label
2	0.5 x 1 inch tamper evident label
3	5.5 x 1.75 inch tamper evident label

4	0.5 x 1 inch tamper evident label
5	Opacity Shield
6	0.5 x 1 inch tamper evident label
7	0.5 x 1 inch tamper evident label
8	0.5 x 3.25 inch tamber evident label

Table 12: G01 Label Placement and Descriptions

6.3 G10

The G10 appliances are built from production grade components and purchased from a commercial reseller (Dell). The manufacturers built the components using industry standard passivation techniques to meet commercial grade specifications for power, temperature, reliability, shock and vibration. The entire module is enclosed in a commercial grade hard sheet metal case. The part number of the G10 FIPS Kit is PW-CCF-G10-FK1, which contains the following parts:

- TEC-710-F01 – One Opacity Shield
- TEC-710-F02 – One 0.5 x 16.5 inch label for the cover
- TEC-710-F03 – One 2.5 x 11.5 inch label for the cover
- TEC-710-F04 – One 3.25 x 2 inch label for the front
- TEC-710-F05 – Five 0.5 x 1 inch labels for various places
- TEC-710-F06 – Two 0.5 x 6.5 inch labels for the hard drives

Module Opacity

The G10 PoliWalls have one (1) opacity shield with ten (10) tamper evident labels. The opacity shield covers ventilation hole in the rear. It has holes that allow sufficient airflow through the device but prevent the viewing of components inside the chassis. It is attached via the rear handle of the device. Three (3) tamper evident labels are placed on the chassis to prevent the viewing of components through ventilation holes – one on the front of the front bezel, one on the top of the front bezel and one on the top cover. With these ventilation holes covered, there is still enough airflow through the system to keep it cool.

Tamper Evidence

Seven (7) tamper evident labels are used to make the device tamper evident. One is placed on the top cover lock so the top cover cannot be removed without destroying the label. Four (4) of the labels are used on the corners of the opacity shield to show evidence of the shield being bent or moved. Two (2) labels are placed across the hard drive bays to show evidence of the hard

drives being tampered with. All of the labels are serialized so the Cryptographic Officer can verify that no labels have been replaced.

Figure 17: G10 Labels on Front Bezel

Figure 18: G10 Labels on Hard Drive Bays

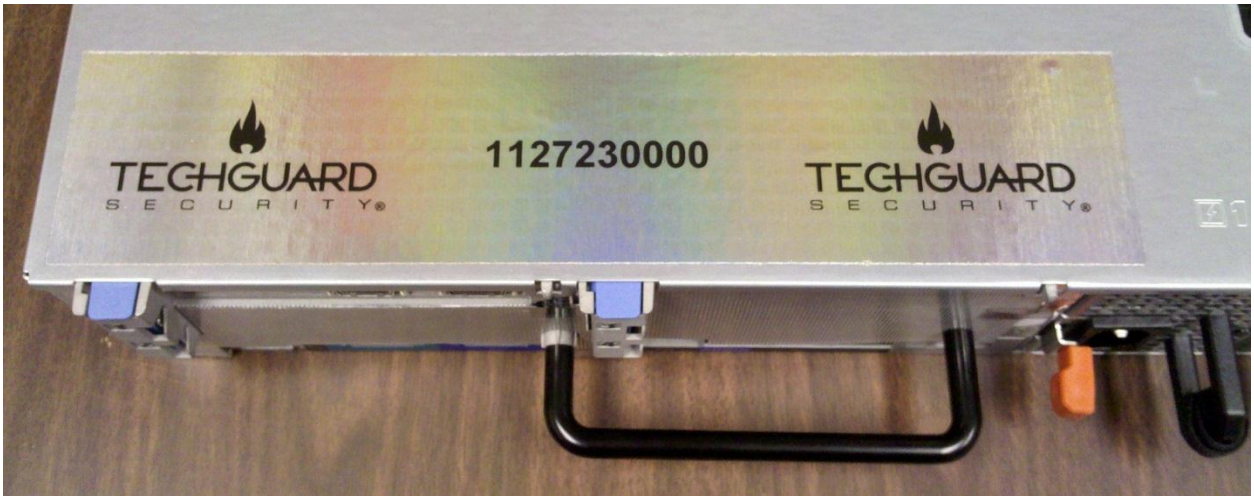

Figure 19: G10 Label on Top Cover

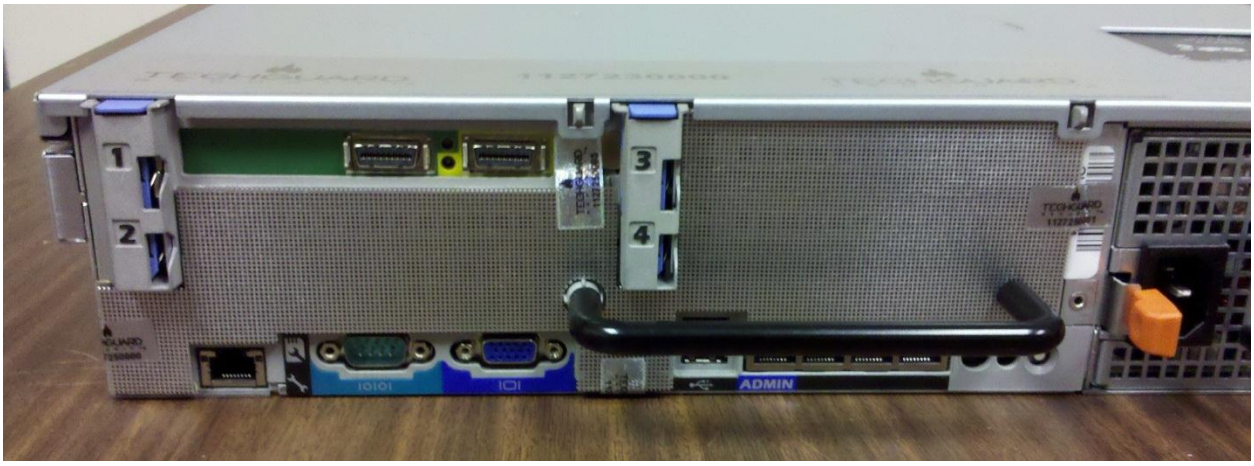

Figure 20: G10 Rear Opacity Shield for CX4 Model

Figure 21: G10 Rear Opacity Shield for Fiber Model

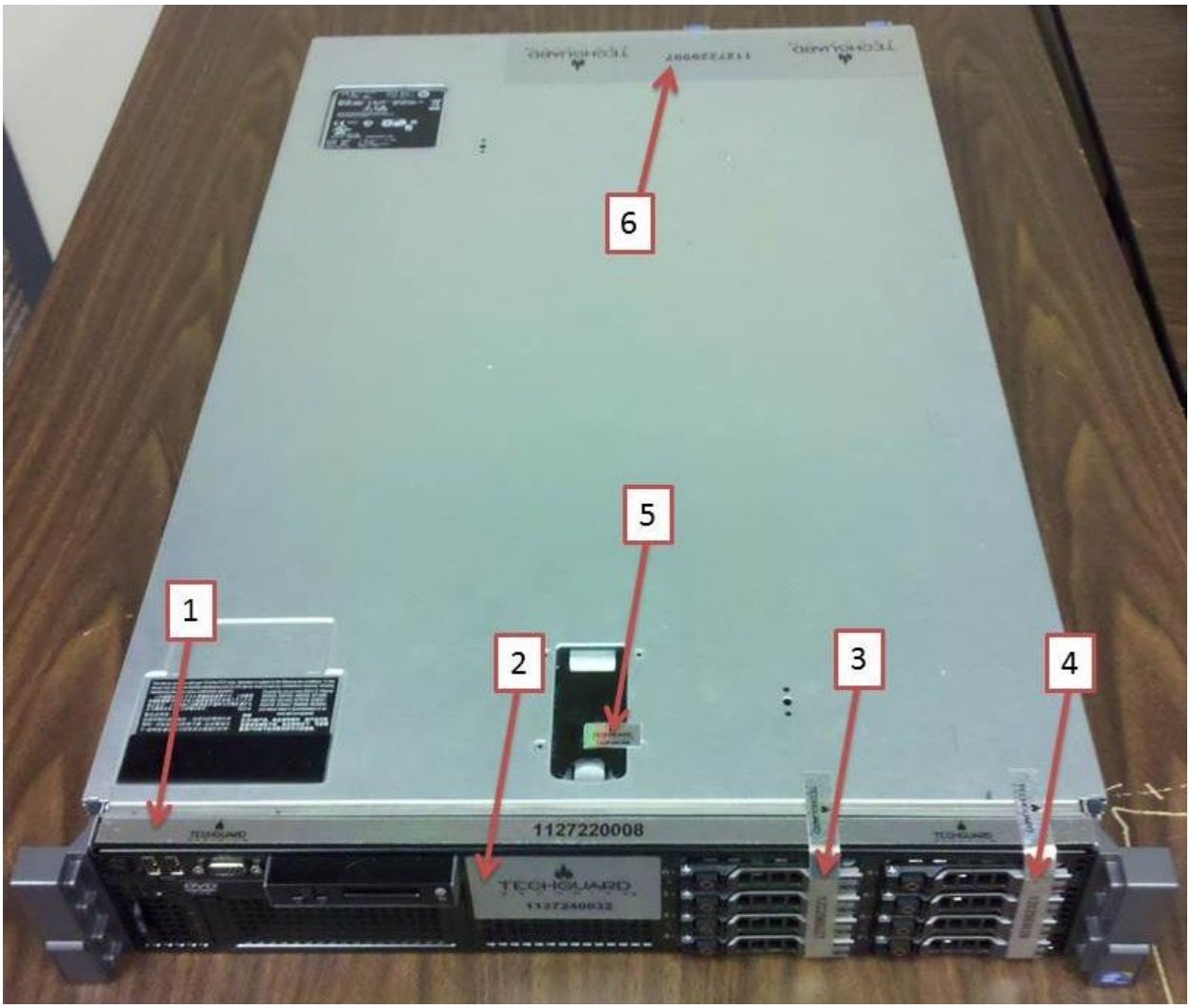

Figure 22: G10 Front Labeled Diagram (see Table 13)

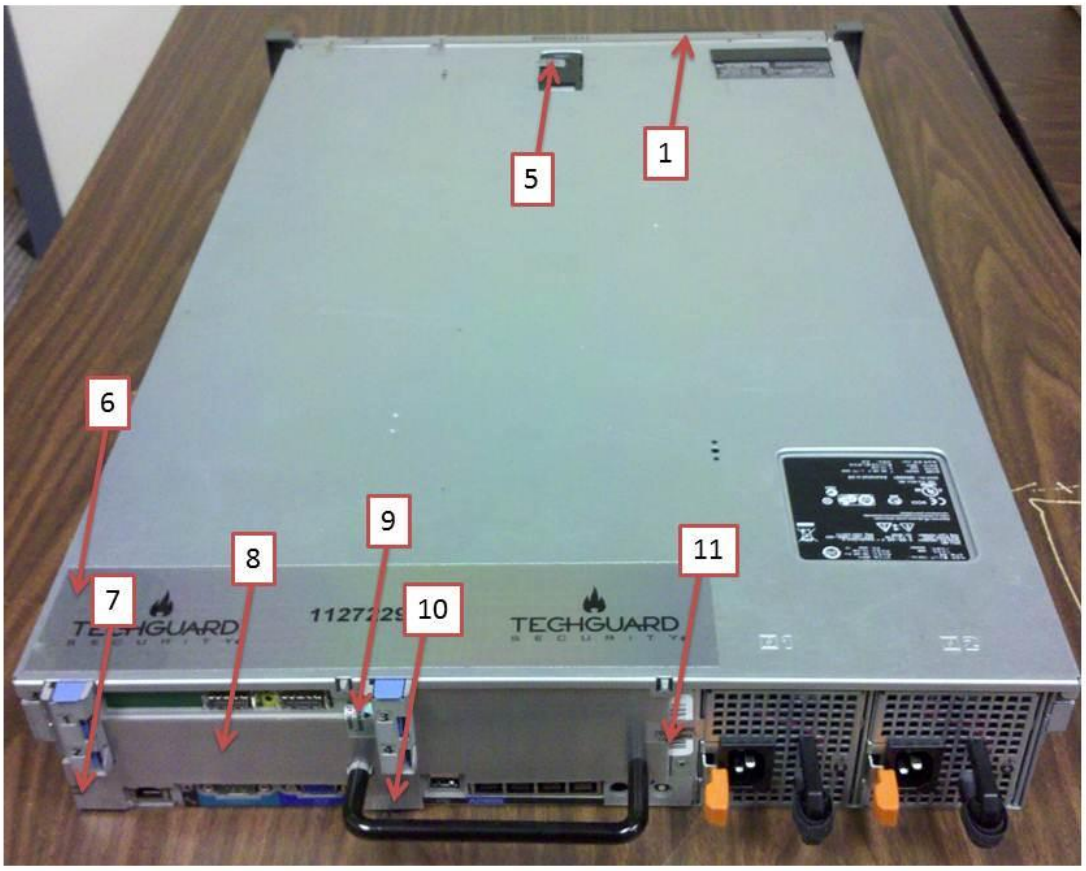

Figure 23: G10 Rear Labeled Diagram (see Table 13)

Location	Description
1	16.5 x 0.5 inch tamper evident label
2	3.25 x 2 inch tamper evident label
3	6.5 x 0.5 inch tamper evident label
4	6.5 x 0.5 inch tamper evident label
5	0.5 x 1 inch tamper evident label
6	11.5 x 2.5 inch tamper evident label
7	0.5 x 1 inch tamper evident label
8	Opacity Shield
9	0.5 x 1 inch tamper evident label

10	0.5 x 1 inch tamper evident label
11	0.5 x 1 inch tamper evident label

6.4 Physical Security Inspection

The Cryptographic Officer may be required to perform periodic inspections of the physical module to ensure the module has not been tampered with. Use the following table as a guideline.

Table 13: Inspection of Physical Security

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Labels	Monthly	Examine labels for any sign of tampering, removal, tearing, etc. Verify no serial numbers are different.
Module Enclosure	Monthly	Examine the module enclosure for any new openings, damage or other access to the internal module.

7 Operational Environment

The PoliWall appliances all run Linux as their Operating System (OS). The processors, however, differ by model and are shown in the following table.

Table 14: PoliWall Processors

PoliWall Model	Processor
10 Gigabit	2X Intel Xeon E5620 2.4 Ghz, 12M Cache, Turbo, HT
1 Gigabit	Intel Xeon X3430 2.4 Ghz, 8M Cache, Turbo
50 Megabit	Intel Atom D510 1.66 Ghz, 1M Cache
10 Megabit	Intel Atom D510 1.66 Ghz, 1M Cache

The PoliWall's Operational Environment (OE) is non-modifiable. There are no services available that allow modification of the OE, nor would a malicious attacker have any method of modifying the operational environment, even though illegitimate means.

8 Key Management and Cryptographic Algorithms

The PoliWall module can be configured in one of two modes of operation: an Approved mode and a non-Approved mode. To operate the module in a FIPS 140-2 compliant manner, only the Approved mode of operation shall be configured. Any security function provided by PoliWall in the non-Approved mode may not have been tested to the FIPS 140-2 standard and therefore may not be in compliance.

The Approved mode can only be accessed through the web Interface. A "FIPS mode" indicator, shown in the following figure, is visible whenever the module is operated in the Approved mode.

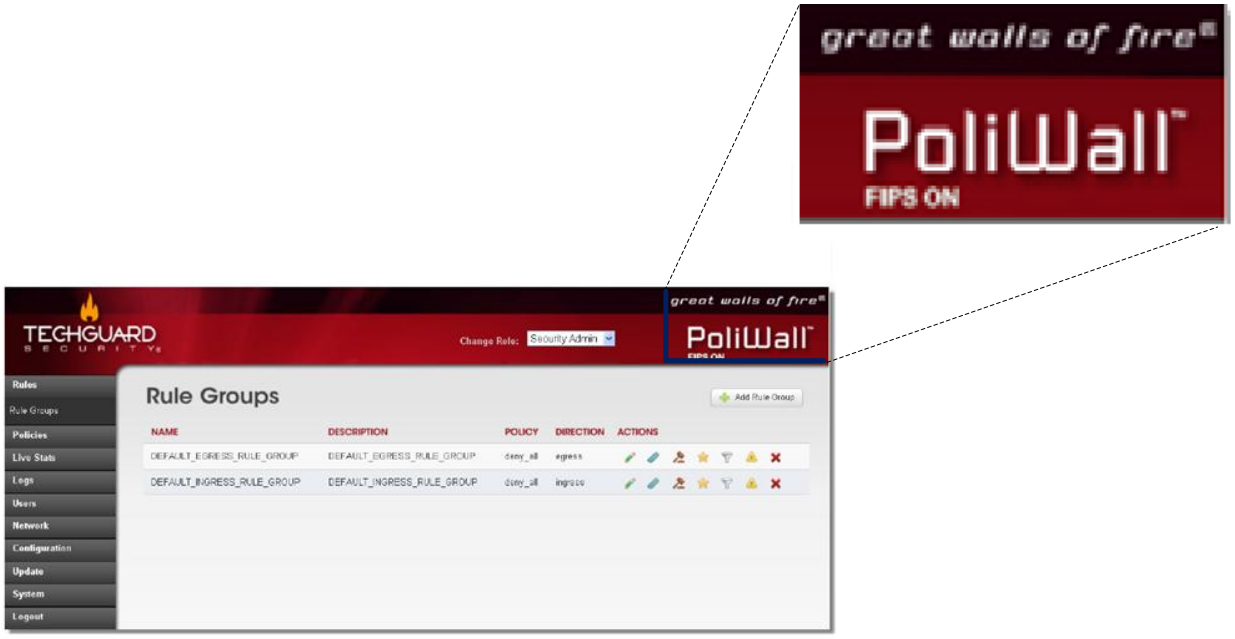

Figure 24: FIPS Mode Indicator

Operating the PoliWall in the Approved mode ensures that only FIPS 140-2 Approved and Allowed algorithms are used to handle cryptographic functionality. Only operators of the Cryptographic Administrator role have the ability to switch between the Approved mode and non-Approved mode.

For the PoliWall to operate in an approved mode, all the specifications in the Physical Security section above must be met for the particular hardware model. The Cryptographic Officer may then place the device in Approved mode. For information on putting the PoliWall in Approved mode, see the Cryptographic Settings section of the User's Manual.

A list of the Approved algorithms utilized in the Approved mode of operation, their key sizes, and their associated validation certificates issued by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP) are provided below.

The PoliWall does not implement any vendor affirmed security methods in the Approved Mode of Operation. MD5 is used within TLS for protocol compatibility only.

Table 15: Validated Algorithms and Key Sizes

Approved Algorithms	Certificate Number
Secure Hash Algorithm (SHA)-1	1412, 1413
SHA-256	1413
Advanced Encryption Standard (AES)-128	1600, 1601
AES-192	1600, 1601
AES-256	1600, 1601
RSA-1024	782
RSA-2048	782
RSA-3072	782
ANSI X9.31 using AES-256	857

When configured in the non-Approved mode of operation, the PoliWall can be configured to utilize the non-Approved algorithms listed in the following table, in addition to the algorithms listed above.

Table 16: PoliWall Non Approved Algorithms

Non-Approved Algorithms
Message Digest Algorithm 5 (MD5)
Data Encryption Standard (DES)
RSA (All key sizes under 1024 bits)
DH groups 16, 17, and 18

While the PoliWall is configured in the non-approved mode of operation, IPsec may be configured to use non-approved algorithms and the Web Server certificates and private keys may use non-approved algorithms.

The following table outlines the cryptographic keys, Critical Security Parameters (CSP), and other security relevant data that the PoliWall may use. The PoliWall protects these keys, CSPs, and security relevant data from unauthorized disclosure, modification, and disclosure through both the physical security it provides (See Section 6) and all aspects of key management covered in this section. Note that audit data is not included in this table because the captured audit data does not include any security or cryptographic information.

Table 17: Cryptographic Keys, CSPs, and Other Security-Relevant Information

Security Information	Description
X.509 certificates	Used for authentication to the web server.
X.509 private keys	Used for authentication to the web server.
PKCS12 files	Used to upload and export X.509 private keys and certificates from the PoliWall.
Passwords	Used to authenticate to the PoliWall through the web interface or to Console CO Mode.
IPsec keys	Keys used for IPsec encryption.

The table below outlines the key generation, storage, and zeroization methods of all keys, Critical Security Parameters (CSP), and security-relevant items.

Table 18: Key Management

Key Management					
Security Information	**Description**	**Generation Method**	**Storage**	**Zeroization[1]**	**Modification**
X.509 certificates	Used for authentication to the web server	X9.31 RSA Key Generation	Plaintext in RAM and encrypted with AES-256 on the hard drive	crypto_admin calls "Key Zeroization" function	This can only be modified by the Cryptographic Administrators. See section 3.8.7.2 Certificates (p. 140) in the user's manual.
X.509 private keys	Used for authentication to the web server	X9.31 RSA Key Generation	Plaintext in RAM and encrypted with AES-256 on the hard drive	crypto_admin calls "Key Zeroization" function	This can only be modified by the Cryptographic Administrators. See section 3.8.7.2 Certificates (p. 140) in the user's manual.
PKCS12 files	Used to upload and export X.509 private keys and certificates	X9.31 RSA Key Generation	Plaintext in RAM	N/A: Not persistent. These files are zeroized as soon as they are exported.	This can only be modified by the Cryptographic Administrators. See section 3.8.7.2 Certificates (p. 140) in the user's manual.
Passwords	Used to authenticate to the PoliWall through the web interface or to Console CO Mode	N/A: These are secret values that must adhere to the Password Policy. Each operator may change their own password. Security Administrators may reset other operators' passwords.	A salted[2] SHA-256 hash of the password is stored on the hard drive.	crypto_admin calls "Key Zeroization" function	Each operator can change their own. Security Administrators man reset other operators' passwords. See section 3.6.1.3.3 (p. 111) and section 3.6.1.5 (p. 115) in the user's manual.
IPsec keys	Keys used for IPsec encryption	X9.31 RNG using AES	Plaintext in RAM	N/A: Not persistent. These files are zeroized as soon as the IPsec session ends.	NA

Firmware Public Key	Public key used to sign firmware updates.	Compiled into the firmware.	Compiled into the binary firmware image.	This is part of the firmware and cannot be zeroized.	This cannot be modified.
IPsec parameters	IPsec parameters including DH group, encryption algorithm, hashing algorithm, etc.	Specified by the operator.	Plain text in the configuration database.	crypto_admin calls "Key Zeroization" function	This can only be modified by the Cryptographic Administrators. See section 3.7.3 IPSec Settings (p. 120) in the user's manual.
TLS X.509 certificates	X.509 certificates used in TLS certificate message	ANSI X9.31 using AES 256	Plaintext in RAM	Zeroized when TLS connection is closed	N/A
TLS Pre-Master secret	Public value transferred during TLS negotiation	ANSI X9.31 using AES 256	Plaintext in RAM	Zeroized when TLS connection is closed	N/A
TLS Master Secret	Secret value generated from pre-master secret and RNG. Used for encryption and decryption on established TLS session	ANSI X9.31 using AES 256, pre-master secret	Plaintext in RAM	Zeroized when TLS connection is closed	N/A
X9.31 Seed	128 bits seed implemented in the ANSI X9.31 using AES-256 RNG function	Continuously updated with the date/time vector	Plaintext in RAM	Replaced on each iteration of the RNG call	N/A: It cannot be modified. It is replaced upon each iteration of the RNG call
X9.31 Seed key	256 bits seed key implemented in the ANSI X9.31 using AES-256 RNG function	ANSI X9.31 using AES-256	Plaintext in RAM	N/A, Static	N/A

[1]All zeroization is performed by writing the hard drive with random data seven times.
[2]A salted hash is the output of a hash algorithm whose input is a string (in this case a username or password) appended with random bits.

8.1 Random Number Generators

The PoliWall utilizes ANSI X9.31 with AES-256 as its Approved Random Number Generator (RNG). The random numbers generated by this algorithm are used as input for all cryptographic algorithms within the module that require random number input. The ANSI X9.31 algorithm is provided entropy from two sources. First, the seed key for the RNG is generated upon initialization of the module. This seed key is created from bits gathered from /dev/urandom which is provided by the Linux kernel. The other source is a date/time vector that updates on every call to the RNG. Continuous RNG tests are provided for each source of entropy in addition to the output of the RNG itself. No other RNGs, Approved or non-Approved, are used by the PoliWall. The RNG algorithm is implemented in OpenSSL-FIPS version 1.2, which is in included in the PoliWall.

8.2 Key Generation

All keys created by the module are generated within the OpenSSL-FIPS version 1.2 component. The PoliWall supports only the approved key generation methods validated in the OpenSSL-FIPS component. These key generation methods make use of only Approved algorithms such as

X9.31 RNG using AES, and X9.31 RSA Key Generation. For symmetric keys the output of the X9.31 RNG is used directly, without modification.

8.3 Key Establishment

The PoliWall can be configured to utilize both key transport and key agreement for its method of key establishment. The PoliWall only uses allowed methods of key establishment. It performs key agreement with Internet Key Exchange version 2 (IKEv2) in its implementation of IPsec. The PoliWall's implementation of IKEv2 uses the following DH groups (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength):

- DH-14, which uses modp-2048 (2048 public/224 bit private)
- DH-15, which uses modp-3072 (3072 public/256 bit private)

Key transport is accomplished by wrapping the key using RSA-1024, RSA-2048, or RSA-3072. The RSA-1024, RSA-2048, and RSA-3072 algorithms are implemented within the OpenSSL-FIPS component.

8.4 Key Entry and Output

The web server key is the only cryptographic key that can be entered into the PoliWall appliances. Cryptographic Administrators may upload private keys through the use of PKCS12 files. These files contain both the web server's public key certificate and private key. The PoliWall is able to verify the RSA digital signature of client certificates to ensure that they originate from the correct Certificate Authority. The PoliWall supports RSA signatures of the following key sizes: 1024, 2048, and 3072. Any uploading of web server keys is done over an encrypted TLS 1.0 (SSL 3.1) session or IPsec session restricted to using only Approved or FIPS 140-2 Allowed algorithms, when the module is configured in the Approved mode of operation. These Approved and Allowed algorithms are:

- TLS 1.0 Approved and Allowed algorithms
    - SHA-1, SHA-256
    - AES-128, AES-192, AES-256
    - RSA-1024, RSA-2048, RSA-3072 (key wrapping; key establishment methodology provides between 80 and 128 bits of encryption strength)
    - MD5 (for TLS protocol compatibility only)
- IPSec Approved and Allowed algorithms
    - SHA-1
    - AES-128, AES-256, AES-192
    - DH groups 14 and 15 (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength)

Attempting to configure IPsec connection settings to use any non-Approved or non-Allowed algorithms is not supported in the Approved mode of operation.

The only CSPs that can be entered into the PoliWall appliances are passwords. Any operator performing remote administration through the web interface must do so over a trusted channel encrypted with TLS or IPsec. No other cryptographic keys or CSPs may be entered into the PoliWall.

The only keys that may be output from the appliances are web server keys, which are transmitted over an encrypted TLS 1.0 or IPsec channel. Cryptographic Administrators may export private keys and public key certificates for the web server in the form of PKCS12 files, which are transmitted over an encrypted TLS 1.0 or IPsec channel. No other keys or CSPs may be output from the PoliWall nor are any private keys displayed at any time. Additionally, no intermediate values generated during the key generation process are output from the module.

8.5 Key Storage

All cryptographic keys and security relevant data are stored on the device in Random Access Memory (RAM) when in use and in the hard drive when not in use. When stored on the hard drive, all keys and security-relevant data are in encrypted form, except for passwords which are stored as salted hashes. A salted hash is defined as the output of a string of bits appended with a random string of bits input into a hash function.

8.6 Key Zeroization

Keys in RAM may be zeroized by resetting the module. Since RAM is non-persistent memory, any key information will be lost as soon as the module is powered down. Additionally, an operator with the crypto_admin role is able to zeroize all the keys on the appliance in Console CO Mode.

9 EMI/EMC

All PoliWall hardware models have been tested for Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) and meet the corresponding FCC requirements. All testing was performed by an accredited test lab under specified and documented conditions. The PoliWall conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

10 Self-Tests

The PoliWall employs a number of self-tests. Power-up self-tests are executed on start, but a self-test can also be performed on demand by any web interface operator, except those of the Read-Only role. Self-tests are performed on demand by rebooting the poliWall. Self-tests performed by the PoliWall are outlined below.

Table 19: PoliWall Self-Tests

Self-Test	Description	Test Type
SHA-1 KAT (kernel space)	Known Answer Test for SHA-1 algorithm implemented in kernel space.	Power-on
SHA-1 KAT (user space)	Known Answer Test for SHA-1 algorithm implemented in user space.	Power-on
SHA-256 KAT (user space)	Known Answer Test for SHA-256 algorithm implemented in user space.	Power-on
AES-128 KAT encryption (kernel space)	Encryption Known Answer Test for AES-128 algorithm implemented in kernel space.	Power-on
AES-128 KAT decryption (kernel space)	Decryption Known Answer Test for AES-128 algorithm implemented in kernel space.	Power-on
AES-128 KAT encryption (user space)	Encryption Known Answer Test for AES-128 algorithm implemented in user space.	Power-on
AES-128 KAT decryption (user space)	Decryption Known Answer Test for AES-128 algorithm implemented in user space.	Power-on
AES-192 KAT encryption (kernel space)	Encryption Known Answer Test for AES-192 algorithm implemented in kernel space.	Power-on
AES-192 KAT decryption (kernel space)	Decryption Known Answer Test for AES-192 algorithm implemented in kernel space.	Power-on
AES-192 KAT encryption (user space)	Encryption Known Answer Test for AES-192 algorithm implemented in user space.	Power-on
AES-192 KAT decryption (user space)	Decryption Known Answer Test for AES-192 algorithm implemented in user space.	Power-on
AES-256 KAT encryption (kernel space)	Encryption Known Answer Test for AES-256 algorithm implemented in kernel space.	Power-on
AES-256 KAT decryption (kernel space)	Decryption Known Answer Test for AES-256 algorithm implemented in kernel space.	Power-on
AES-256 KAT encryption (user space)	Encryption Known Answer Test for AES-256 algorithm implemented in user space.	Power-on
AES-256 KAT decryption (user space)	Decryption Known Answer Test for AES-256 algorithm implemented in user space.	Power-on
RSA-1024 KAT signature (user space)	Signature creation Known Answer Test for RSA-1024 algorithm implemented in user space.	Power-on
RSA-1024 KAT verification (user space)	Signature verification Known Answer Test for RSA-1024 algorithm implemented in user space.	Power-on
RSA-2048 KAT signature (user space)	Signature creation Known Answer Test for RSA-2048 algorithm implemented in user space.	Power-on
RSA-2048 KAT verification (user space)	Signature verification Known Answer Test for RSA-2048 algorithm implemented in user space.	Power-on
RSA-3072 KAT signature (user space)	Signature creation Known Answer Test for RSA-3072 algorithm implemented in user space.	Power-on
RSA-3072 KAT verification (user space)	Signature verification Known Answer Test for RSA-3072 algorithm implemented in user space.	Power-on
ANSI X9.31 using AES-256 KAT (user space)	Known Answer Test for ANSI X9.31 using AES-256 PRNG implemented in user space.	Power-on

Self-Test	Description	Test Type
Software/Firmware integrity test	This test is performed by comparing the software's hash value to a known value when the module is powered on to ensure that the loaded software has not been modified.	Power-on
RSA-1024 pair-wise consistency test	This is a conditional test used to test the validity of RSA public/private key pairs.	Conditional
RSA-2048 pair-wise consistency test	This is a conditional test used to test the validity of RSA public/private key pairs.	Conditional
RSA-3072 pair-wise consistency test	This is a conditional test used to test the validity of RSA public/private key pairs.	Conditional
Continuous RNG test for X9.31 PRNG	This test ensures that consecutive sets of bits generated using the X9.31 algorithm are not equal.	Conditional
Firmware Load Test	This test verifies a firmware package is signed with the correct RSA key before the firmware package is installed.	Firmware Load

All cryptographic algorithms are tested against known values on start-up. All Approved algorithms listed have corresponding self-tests. These self-tests are all implemented within OpenSSL-FIPS v1.2 object module. The self-tests for algorithms implemented in the OpenSSL-FIPS component are also contained in the OpenSSL-FIPS component. After the user space OpenSSL-FIPS tests pass, the kernel space cryptographic algorithms are tested. These tests also compare the algorithm output to hard-coded known values. The userspace algorithm tests include AES KAT, SHA KAT, PRNG KAT, and RSA KAT. The kernel space algorithm tests include AES KAT and SHA KAT.

The PoliWall does not support critical functions tests, manual key entry tests, or Bypass tests, as none of these are applicable to the PoliWall. Note that the PoliWall does have a defined "Bypass Mode", but this is not a FIPS 140-2 defined bypass state. The PoliWall Bypass Mode deactivates any sort of traffic filtering that it is designed to do, so no inherent disabling of cryptography occurs.

The PoliWall performs a software/firmware load test when a new version of the firmware is uploaded to the module. The module uses an RSA signature to verify the new firmware. The only thing that can be loaded is an entire new firmware version of the module, and the RSA signature protects the entire firmware package. The RSA signature must verify before the new firmware is installed. Once the signature is verified and the new firmware installs the module reboots. If the RSA signature cannot be verified the module displays an invalid firmware error message to the operator and module continues running the original firmware version.

The PoliWall has two error states, Audit Full error state and FIPS Error Mode. The device will automatically enter Audit Full error state if the audit log storage fills to capacity without having audit overwrite configured. Entering the Audit Full error state requires a Crypto-Officer to enter the Console CO Mode to clear the error. Console CO Mode operators may also intentionally place the device in Console CO Mode in order to gain access to services only available in this mode. When in Console CO Mode, status messages may be displayed to the Console CO Mode

operator through the ports designated for use in this mode. Note that audit data may be output from the PoliWall while in Console CO Mode. However, audit data are not security relevant because they do not contain any cryptographic key, CSP, or security-relevant data. No other data can be output from the Data Output interfaces while in Console CO Mode. Anytime the device enters Console CO Mode, the mode that is entered is displayed on the console. In Console CO Mode, all network interfaces are shut down. The only way to exit Console CO Mode is to reboot the PoliWall. In Console CO Mode, the following operations can be performed by the specified role:

- Operations available to "security_admin"
  - Reset admin account
  - Reset admin interface
  - Reset configuration back to default
  - View alarms
  - Reboot
- Operations available to "crypto_admin"
  - Zeroize cryptographic keys.
  - View alarms
  - Reboot
- Operations available to "audit_admin"
  - Delete packet log messages
  - Delete system log message
  - View system logs
  - View alarms
  - Reboot

If the self-test fails because of a FIPS error or a firmware checksum error, the device will enter FIPS Error Mode. The device will also enter FIPS Error Mode if a conditional self-test fails. When the device enters FIPS Error mode, the only option is to reboot the PoliWall. Anytime the device enters FIPS Error Mode, the mode that is entered is displayed on the console. In FIPS Error mode all network interfaces are shut down and all processes that can perform cryptographic functions are terminated, therefore no cryptographic functions can be performed. In FIPS Error Mode, the only operation that can be performed is to reboot the PoliWall.

11 Mitigation of Other Attacks

The PoliWall claims no mitigation of other attacks.

Appendix A – Acronyms

The following acronyms are used throughout this document.

Table 20: Acronyms

Acronym	Expansion
AC	Alternating Current
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter
DC	Direct Current
DES	Data Encryption Standard
DH	Diffie-Hellman
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
eSATA	External Serial Advanced Technology Attachment
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HDD	Hard Disk Drive
HIPPIE	High-speed Internet Protocol Packet Inspection Engine
HTTPS	Hypertext Transfer Protocol Secure
IKEv2	Internet Key Exchange version 2
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LCD	Liquid Crystal Display
MD5	Message Digest Algorithm 5
NIST	National Institute of Standards and Technology
NVRAM	Non-volatile Random Access Memory
OE	Operational Environment
OS	Operating System
PCEL	Pre-compiled Exception List
PKCS12	Public-Key Cryptography Standards #12
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USB	Universal Serial Bus
VGA	Video Graphics Array

Appendix B – Instructions to put module in FIPS approved mode

All PoliWall CCF models are shipped with the physical security mechanisms (tamper evident labels and opacity shields) installed at factory and FIPS approved mode enabled. If the device was taken out of FIPS approved mode for any reason, follow the instructions below to place it back in FIPS approved mode.

1. Use the Physical Security section in the Security Policy and verify all requirements listed have been met for the model being checked.
2. If any of the requirements are not met, a new FIPS Kit must be ordered for your model and installed with the instructions included in the kit. The Physical Security section includes the model number of the FIPS kit that must be ordered for each PoliWall model.
3. Log into the PoliWall web interface and switch to the Crypto Admin role.
4. Go to Configuration -> Cryptographic Settings in the menu.
5. Verify that the Cryptographic Mode is set to FIPS Mode.
6. If it is not set to FIPS Mode, change it to FIPS Mode and click Submit. If there are any algorithms currently in use that are not allowed in FIPS Mode, the PoliWall will not enter FIPS Mode until those are changed.
7. If the Cryptographic Mode needed to be changed to FIPS Mode, the PoliWall will reboot and will then be in a FIPS approved mode. For more information on changing the Cryptographic Settings, see the Cryptographic Settings section in the PoliWall User's Manual.