Blue Ridge Networks
BorderGuard 5000 and 6000 Series

FIPS 140-2
Security Policy

Version 5.1

1.0 Introduction

This document defines the security rules under which this product operates. The rules are enforced by the use of firmware modules. The use of the firmware is mandatory and is called automatically while exercising the module.

1.1 Identification

Hardware	BorderGuard 5100, 5200, 5400, 5500 and 5600 BorderGuard 6100, 6200, 6400, 6500 and 6600
Firmware	BG5000/6000 Firmware
Version	DPF1 V7.3
Vendor:	Blue Ridge Networks 14120 Parke Long Court, Suite 103 Chantilly, VA 20151

1.2 Description

The BorderGuard 5000 and 6000 series of devices are standalone Internet security appliances that take the form of an electronic hardware device containing a processor, memory, networking and crypto components, and firmware.

These devices are multi-function appliances that can perform many non-cryptographic network functions such as multi-protocol routing, bridging, and packet filtering. The cryptographic component and Cryptographic Module of the unit is often referred to in this document by its trade name, Data Privacy Facility (DPF.)

BorderGuard 5000 and 6000 devices are typically installed so that they forward network data packets entering and exiting a site or secure enclave. Using a Forwarding Policy specified by the Crypto-Officer, they selectively transform network packets inbound or outbound to a remote site/enclave or an individual user's host. These devices thus operates as a Virtual Private Network device capable of:

- Securing traffic between sites within an organization, or between two separate organizations.
- Securing access between a site and an individual remote user (remote access).

Externally, it interconnects two or three Ethernet Local Area Networks, and is able to exercise a Security Policy on Internet data packets (IP datagrams) that would normally flow between the connected networks. In addition to its network interfaces, it

FIGURE 1. BorderGuard 5000/6000 Chassis

provides a control and status interface through a serial console port that is, at the Crypto-officer’s discretion, accessible through Internet services such as Telnet.

There are ten different models in the BorderGuard 5000 and 6000 series. The intent in the model differentiation is to provide gradated capability and performance for potential users of the product. The essential differences between the models are summarized in Table 1. All BorderGuard 5000 and 6000 models run a completely identical load of firmware; the firmware activates model dependent features based on model designation switches located within the physical Cryptographic Boundary of the device.

Table 1: BorderGuard 5000 and 6000 Models and Features

Model	Nominal Advertised Speed	Hardware Crypto	Ethernet Ports	KeyGuard	4K RSA Authentication and Key Exchange	Max concurrent crypto sessions	X.509 Certificate Support
5100	20 Mbit/s	No	2 x 100Mbit	No	No	150	No
5200	45 Mbit/s	No	3 x 100Mbit	Optional	No	300	No
5400	100 Mbit/s	Yes	3 x 100Mbit	Optional	No	600	No
5500	200 Mbit/s	Yes	2 x 1Gbit 1 x 100Mbit	Optional	Yes	1000	No
5600	400 Mbit/s	Yes	2 x 1Gbit 1 x 100Mbit	Optional	Yes	1500	No
6100	20 Mbit/s	No	2 x 100Mbit	No	No	150	Yes
6200	45 Mbit/s	No	3 x 100Mbit	Optional	No	300	Yes
6400	100 Mbit/s	Yes	3 x 100Mbit	Optional	No	600	Yes
6500	200 Mbit/s	Yes	2 x 1Gbit 1 x 100Mbit	Optional	Yes	1000	Yes
6600	400 Mbit/s	Yes	2 x 1Gbit 1 x 100Mbit	Optional	Yes	1500	Yes

Model refers to the numeric designation of the BorderGuard device within the series. The model number is designated on both the front and back of the chassis.

Nominal Advertised Speed designates the maximum data throughput that is recommended for that model. Actual performance depends on many factors such as packet sizes and the cryptographic algorithms chosen.

Hardware Crypto indicates whether hardware assists are provided for the symmetric cryptographic algorithms and random number generation. These activities are performed in firmware on those models without the hardware capability.

Ethernet Ports refers to the complement of Ethernet connectors on the back of the chassis. Different models support both a different number of ports, and different maximum LAN speeds that the port is capable of negotiating.

KeyGuard refers to support for an optional token that must be inserted in the front of the chassis before the unit is activated.

4K RSA Authentication refers to the sizes of the keys used for RSA authentication and

Diffie-Hellman key exchange. All BorderGuard 5000/6000 models support 512, 1024, and 2048 bit keys for these algorithms; the two high end models also support 4096 bit RSA and Diffie-Hellman keys for session establishment.

Max Concurrent Crypto Sessions refers to the maximum number of VPN tunnels the model will establish at any one time.

Despite these differences, the various models have a great deal in common:

- All models of BG5000/6000 run an identical firmware image. The firmware determines the BorderGuard model in which it is running and activates the appropriate internal facilities. Thus all BG5000/6000's possess common Cryptographic Module firmware and an identical firmware Cryptographic Module boundary.
- All models have an identical chassis, and identical tamper resistant and tamper evident mechanisms.
- The board design and hardware logic is identical across all BorderGuard models. Depending on manufacturing costs and volumes, lower model BorderGuards may or may not have hardware crypto processors or Gigabit Ethernet PHYs populated on the logic board. Should such devices be present on a lower model BorderGuard, the firmware will ignore their presence and not initialize them for service.
- **X.509 Certificate Support** indicates that the firmware to send, receive, validate, and process X.509 public key certificates has been activated in the device.

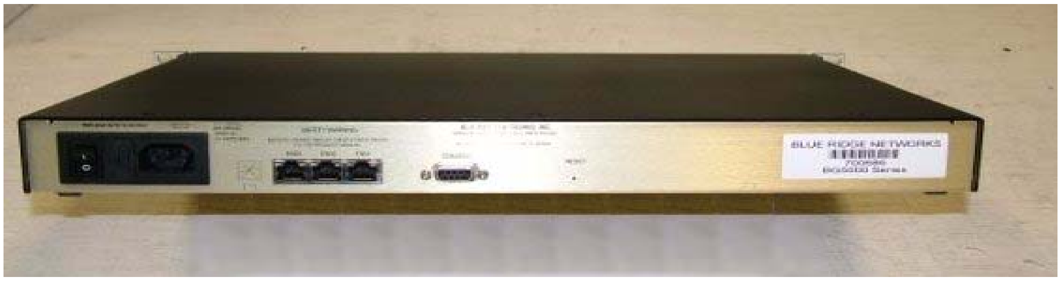
2.0 Device Description

The module is a multi-chip standalone embodiment, housed within a 1-unit high sheet metal chassis, protected by tamper evident seals and tamper proof screws. There are no user or administrator serviceable or configurable items inside the chassis. There is no reason for the customer to open the chassis, which must be returned to the factory should maintenance be required. The tamper evident seals must be inspected periodically to detect tampering.

The BG5000/6000 device and BG5000/6000 Cryptographic Module conform to FIPS 140-2 Level 2.

The module also conforms with the EMI/EMC requirements in FCC Part 15, Subpart J, Class A.

FIGURE 2. BorderGuard 5000/6000 Back Panel



2.1 Interfaces

- **Ethernets.** The BG5000/6000’s three Ethernet ports use an industry standard 100BaseT connector consisting of an RJ45 jack and four grounded signal lines. The BorderGuard 5100 model only activates two of the three Ethernet connectors (the ones designated EN01 and EN02), and the third (EN03) port is plugged with a plastic insert.
- **Serial Interface.** The serial interface may be used for console access by the Crypto-officer, and is a 9 pin RS-232C serial connector.
- **KeyGuard USB Port.** (optional) The USB port is used in applications where the entire unit is keyed to a USB token, and the BorderGuard will refuse to boot if the unique authentication token is not installed in the USB socket at boot time.
- **AC Power.** The unit has an industry standard power connector that can accept 50-60Hz, 110-230 VAC power.
- **LCD Display.** A 2x24 line alphanumeric LCD display gives unit status and statistics.

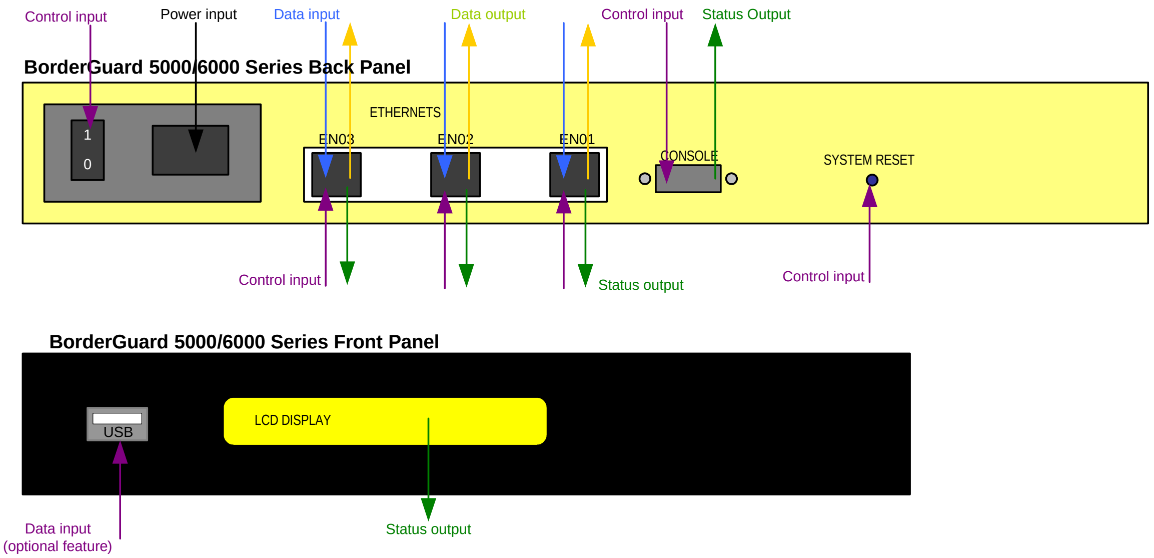
There are no accessible doors or openings. The chassis cover and access to a factory maintenance port are secured with tamper resistant screws and tamper evident tape.

2.2 Firmware

The firmware module common to all BorderGuard 5000 and BorderGuard 6000 models, and is designed to execute four major firmware components,:

- **Boot Code**, which is designed to Self Test the unit, and load Functional Firmware that performs the Operating System, Packet Forwarding, and Cryptographic Module functions.
- **Operating System Functional Firmware**, which provides the core services needed to manage memory, dispatch tasks, service interrupts, and provide file I/O and console access.

FIGURE 3. BorderGuard 5000 and 6000 Series Physical External Interfaces



- **Packet Forwarding Functional Firmware** (forwarding module), which controls the network media interfaces, performs a variety of Internet and LAN based packet forwarding procedures, and can selectively identify packets for implementation of a Security Policy through filtering and port selection mechanisms. The detailed operation of the packet forwarding firmware is not discussed in this document.
- **Cryptographic Functional Firmware**. This component executes the cryptographic functions.

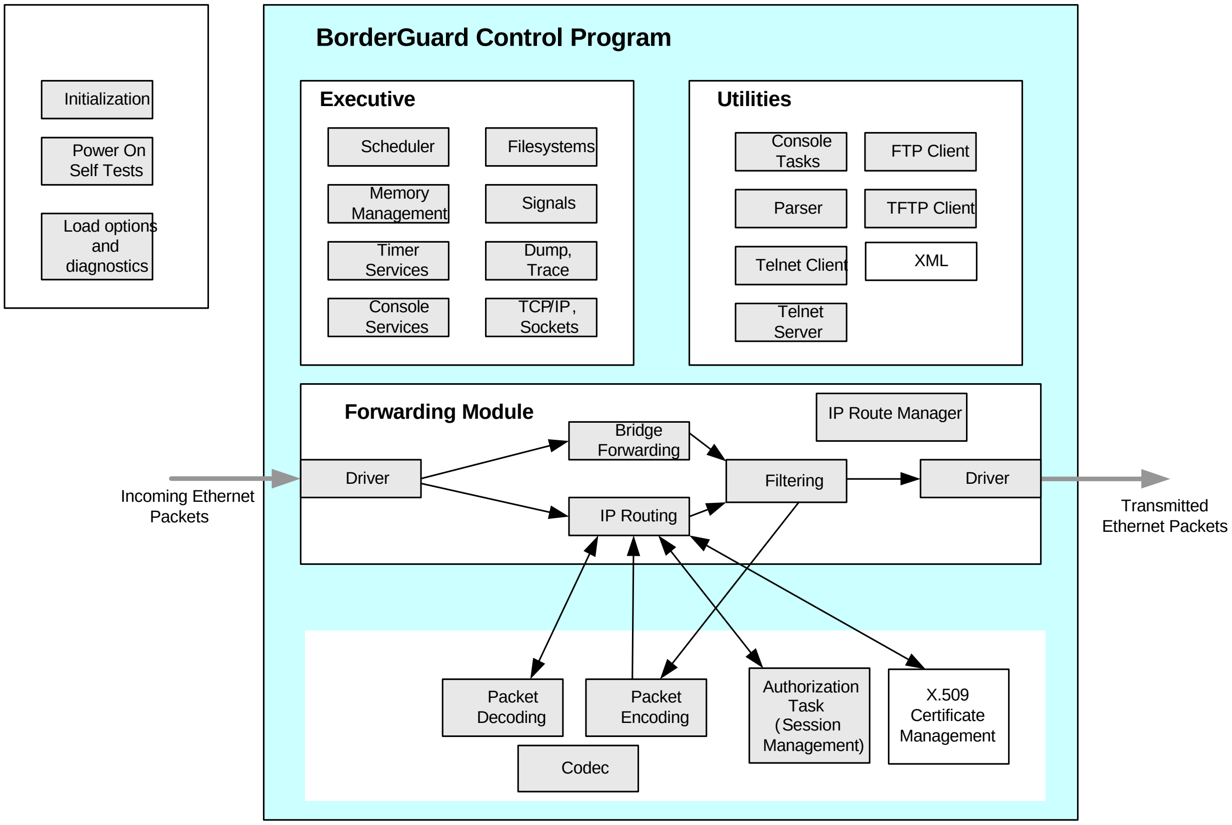
2.3 Cryptographic Boundary

The physical cryptographic boundary for the module consists of the entire BorderGuard chassis, including all circuit boards and components thereon, power supplies, interfaces, indicator lamps and chassis sheet metal. The unit is designed for rack mounting and is 18” x 12” x 1.75”.

2.4 States

The BG5000/6000 Cryptographic Module is designed as a finite state machine. The basic states are Power off, Boot, Initialization, Operating, and Error.

FIGURE 4. **BG5000/6000 Series Cryptographic Module**



2.5 Processors

The code is executed on an IBM (now AMCC) 440GX processor. When available on the proper models, hardware traffic encryption functions are performed with a HiFn 7855 encryption chip.

2.6 Firmware Security

The module is written in ANSI C. Some core cryptographic transforms are written in assembly code for better performance. The RSA Crypto-C static library is used for public key operations. None of the algorithms used in the Crypto-C library are FIPS Approved.

Integrity of the firmware is ensured through three independent mechanisms.

- A CRC32 checksum of both the firmware load and the independently loaded boot code check against hardware or operational errors in the handling of the firmware.
- A FIPS 113 compliant Data Authentication Code is associated with every load of FIPS compliant boot code and operating firmware. Firmware with an incorrect DAC cannot be loaded into the device.
- All released firmware versions have the SHA-1 residue of the firmware image published by Blue Ridge Networks. This residue can be calculated and checked both before the code is loaded on the device, and after it is loaded but before it is permitted to execute.

2.7 Embedded Control Program

The “operating system” for the BorderGuard is a proprietary embedded system control program written specifically for the BorderGuard product line. Blue Ridge does not consider this function to be an “operating system” as it provides no capability to execute code that is not integrated into the single firmware image. The control program is not accessible to the user nor is it shared with other applications. The control program does not permit the dynamic addition and execution of code from any source.

3.0 Identification and Authentication Policy

The module supports only two roles, that of crypto-officer and user. The crypto-officer has access to the console RS232 port and optionally via Telnet. The user has no access to the control inputs or status of the module.

The Cryptographic Module does not support a maintenance mode or a bypass mode.

3.1 Crypto-officer

The Crypto-officer is as an individual charged with installation and maintenance of the BG5000/6000, and the formulation and maintenance of a site Security Policy. The Crypto-officer role is the only one that can modify or inspect the state of the BG5000/6000.

Access to the device is restricted by an access password; it is typically further restricted by locating the device in a secured area.

Crypto-officer functions with the BG5000/6000 include:

- Installation of the unit, and monitoring of the unit's Self Test capabilities.
- Monitoring of the unit's operation.
- Definition of a Forwarding Policy and Security Policy, and maintaining those Policies in the face of ever-changing network requirements.

3.2 User

The Users of a BG5000/6000 are those host computers, their associated individuals, and other authenticated modules who generate network traffic to be processed by the BG5000/6000. Since these user data sources and destinations are networked devices, Users and their hosts do not have to be co-located with the BG5000/6000.

Operation of the BG5000/6000, and any decision as to whether the BG5000/6000's services will be performed for a User, are completely under the control of the Crypto-officer. Users may be completely unaware of the fact that the BG5000/6000 exists, or that it is securing data they are sending to remote locations.

User authentication consists of authenticating cryptographic sessions that will contain packets arriving from a remote site with other Users. This is performed with RSA public/private key pairs. A second, far weaker form of authentication consists of policies identifying Users in the interior site, and determining policy for one internal, local User versus another, based on originating IP address or other message contents.

RSA Public Key authentication takes place in both directions. The BG5000/6000 that initiates a session prepares a field consisting of a 32 bit nonce, a 128 bit MD5 message residue, and about 48 bytes of other session information. Before transmission, this field is encrypted with both its own private key *and* the public key of the remote BG5000 or BG6000. The remote unit returns the nonce and session information RSA encrypted with the public key of the originating BG5000/6000.

RSA keys of 512, 1024, 2048 or 4096 bits in length may be selected by the Crypto-officer.

Table 2: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	RSA 512 bit Public Keys	32 bit nonce + 48 bytes variable session data + MD5 hash.
User	RSA 1024 bit Public Keys	32 bit nonce + 48 bytes variable session data + MD5 hash.
User	RSA 2048 bit Public Keys	32 bit nonce + 48 bytes variable session data + MD5 hash.
User (5500, 5600. 6500, 6600 models only)	RSA 4096 bit Public Keys	32 bit nonce + 48 bytes variable session data + MD5 hash.
Crypto-Officer	Logon Password	Fixed password

3.3 Policy Definition

The function of defining a site security policy for the module is described in Blue Ridge customer documentation such the BorderGuard 5000 Getting Started Guide, and the DPF Administrator's Guide.

The construction of an access policy by the Crypto-officer/system administrator consists of two major steps: defining a Forwarding Policy that identifies sets of remote User site traffic and non-User traffic, then defining a cryptographic Security Policy to secure User traffic moving between sites.

Forwarding Policy consists of identifying traffic as intended for delivery to a specific remote site based on its source and destination IP address, and other internal packet characteristics. Forwarding Policy also controls the disposition of traffic coming to or from locations that are not identifiably a remote site, such as general Internet traffic. To implement a Forwarding Policy, the Crypto-officer will need to identify:

- the connection points at which a BorderGuard 5000/6000 should be placed
- the complement of trusted sites, and the method to identify traffic intended for each of them.
- the type(s) of traffic to allow in from untrusted sites
- the type(s) of traffic to block from untrusted sites
- the type(s) of traffic to allow out to trusted sites
- the type(s) of traffic to block to trusted sites

Cryptographic Policy. For traffic to each trusted remote site, the local and remote Crypto-officers must agree on a Security Policy that meets both their needs. Security services offered by the BG5000/6000 include:

- Encryption — prevents untrusted parties from examining the contents of traffic moving between sites. Five Approved encryption algorithms (DES, TDES, AES128, AES192, AES256) are available. The DES algorithms are included for compatibility purposes only.
- Integrity Checking — performs a HMAC of each data packet, so that an enroute packet may not be altered by third parties, nor may they successfully introduce a new packet into the secured data stream. The Approved HMAC SHA-1 is available.
- Replay Prevention — prevents attacks caused by re-introducing a previously sent legitimate data packet into a secured data stream.

The BG5000/6000 also offers data compression services for traffic moving between secured sites.

FIPS Mode. The BG5000/6000 Cryptographic Module offers both Approved and non-Approved cryptographic transforms. The Crypto-officer must ensure that only Approved transforms are in use by:

- Selecting one of the AES128, AES192, AES256, DES[1], or Triple-DES cryptographic transforms.
- If packet integrity checking is desired, selecting the HMAC SHA-1 algorithm.

Proper selection of Approved algorithms can be confirmed through a console command

[1] The use of DES in FIPS mode is only approved for use during the transitional phase, valid until May 19, 2007.

(“`dpf show status`”) which will report the number of active sessions that are using fully Approved transforms and those which are not.

4.0 Access Control Policy

Access to the internals of the module is restricted to the Crypto-officer. The User may only perform encryption or decryption services and has no access to the internals of the module. Crypto-officer access control is by a password.

The nature of the unit as a network appliance usually means that the device is not in a User accessible location. Under most circumstances, it can be locked in a communications area only accessible to the Crypto-officer.

4.1 Access to Critical Security parameters

Items the crypto-officer can control:

- Generation of an RSA public/private key pair for the BG5000/6000 device. A separate key pair may exist for each of the 512, 1024, 2048, or 4096 bit keys. Once the key pair is generated, the public key is available for export to other devices. The private keys cannot be inspected or exported in any form.
- Definition of cryptographic network tunnels (sleeves), and the cryptographic quality of service used within the tunnel. Note however that the Crypto-officer does not have unilateral control over these definitions unless they are also the Crypto-officer for the remote unit they wish to have share in the activity. A remote unit will fail to connect and pass traffic to the local unit if the local Crypto-officer proposes a cryptographic policy the remote Crypto-officer does not agree with. Both need to define complementary service definitions.
- Installation and exchange of RSA Public Keys for remote units. These public keys are used to authenticate the sleeve before any traffic will be sent over it. Again, installation of public keys in remote BG5000/6000’s requires the explicit cooperation of the remote unit’s Crypto-officers.
- Control of the Forwarding Policy within the BorderGuard, which decides what traffic is to be presented to the Cryptographic Module, and which virtual cryptographic connection will be used to transport a specific data item.

The Crypto-officer does not have any access to:

- Cryptographic traffic keys. They are automatically generated for each cryptographic session, and zeroized when the session is complete. They cannot be inspected while in use, nor are there any facilities to manually introduce such keys into the unit.
- RSA private keys. RSA private keys for the unit may be generated by the Crypto-officer, but they cannot be inspected during or after generation. Only the public key associated with the private key is available for export.

4.2 Key Management

Keys used by the BG5000/6000 Cryptographic Module include the following:

- An RSA public/private key pair associated with the individual unit. The private key is not available to the operator, the public key is available to the crypto-officer. Only public keys can be entered or output from the module. The public/private key pair can be zeroized in both volatile and nonvolatile storage when a new key pair is generated, or when the keys are cleared by a specific operator command.

- Encryption traffic keys which include DES, TDES, IDEA and AES. These keys are generated through the Diffie-Hellman key agreement algorithm during session establishment and are associated with the session. The keys are zeroized immediately upon session termination. These keys cannot be set manually, nor may they be inspected.
- Keyed data strings used for HMAC MD5 and HMAC SHA-1 keyed hashes. These are used where a shared secret key is exchanged between sender and receiver and guards against a man-in-the-middle attack.These keys are generated through the Diffie-Hellmann key agreement algorithm during session establishment and are associated with the session. These keys are zeroized upon termination of the session.

Other authentication data used by the unit consists of:

- a logon password for the Crypto-officer, which may be entered when connectivity has been achieved through access to the serial port, or through a Telnet connection. The password is stored in hashed form in a data file (`profile`) on the BG5000/6000’s filesystem. The hashing algorithm is not of cryptographic quality; however the entire filesystem is not accessible to anyone save authenticated Crypto-officers.
- an optional USB “smart card” token which must be inserted into a receptacle on the front of the BorderGuard 5000/6000 in order for the unit to successfully boot. Authentication takes place in boot code, and normal smart card techniques of having the token do an MD5 hash of a specified 64 byte random string catenated with a 20 byte shared secret stored both on the token and in nonvolatile memory. If the hash and comparison fails, the unit will not boot, and the cryptographic firmware will not even be loaded into the unit.

Table 3: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
User Session Authentication; establishment of a cryptographic association between two BG5000/6000's	512, 1024, and 2048 bit RSA public/private key pairs; both BG5000/6000's authenticate themselves to the other. 4096 bit RSA key pairs are available on the 5500 and 5600 models. The BorderGuard will accept approximately 5 connection authentication attempts every second; with a 512 bit RSA key, the probability of a successful random guess of the key in one minute's time is 2.23x10^{-152}.
Packet Integrity Checking	FIPS 198 keyed hash is appended to each data packet; secret key material is generated via Diffie-Hellmann mechanisms during session authentication. Key material is obtained through Diffie-Hellman key exchange. 96 bits of hash are appended to the packet, making the probability of forging a packet with a correct hash value 2^{-96} or 7.92x10^{-28}. Presuming that the BorderGuard processed 10,000 forged IP packets per second, the probability that one of those packets would be accepted over a one minute interval is 4.75x10^{-34}.
Console logon by Crypto-Officer	Physical access to the device, or Telnet, followed by a fixed password of at least 4 and less than 32 alphanumeric characters. The password is reduced to a 32 bit value using the CRC32 algorithm, giving a maximum probability of a successful random guess of 62^{-4} or 6.77x10^{-8}. Assuming optimistically that the BorderGuard will accept 100 logon attempts per second, the probability of successfully guessing a password in one minute is 1.39x10^{-6}.
BG5000/6000 Token (optional)	This optional feature consists of a USB "smart card" chassis activation key external to the Cryptographic Module. It uses an MD5 hash of a 64 byte challenge string catenated with a 20 byte shared secret. The probability of a successful random guess is 2^{-128} or 2.94x10^{-39} Verification of the USB key is done once after a 10 second boot and Self Test process, permitting 6 attempts per minute; the probability of accepting a random forged key in one minute is 1.76x10^{-38}.

Table 4: Services Authorized for Roles

Role	Authorized Services
User	Symmetric Encryption/Decryption Asymmetric Encryption/Decryption (session authentication) DES MAC HMAC SHA-1 (packet authentication) X.509 PKI certificate exchange.
Crypto-officer	Public/private key generation. Export and import of public keys Cryptographic TOS for tunnels Forwarding policy — Direction of IP packets through designated tunnels. Module Configuration. Key Management. Module Initialization. Discretionary Self Test. Set/Change Crypto-Officer password. Zeroize keys. Show Status. Firmware load.

Table 5: Access to Critical Security Parameters

CSP Type	User Access	Crypto-officer Access
RSA private key	none	replacement or zeroization
RSA public key	none	inspection, export, replacement, zeroization of internal public key; import, inspection, and modification of external public keys
Traffic Encryption (DES, Triple-DES, AES, IDEA) Keys	none	none
HMAC (SHA-1, MD5) Keys	none	none
Console password	none	modification
USB Token (outside Cryptographic Boundary)	none	Usage through key insertion; Contents could be destroyed with third party tools, but not inspected
USB Token Authentication Data	none	none
Fixed Encryption Key (Triple-DES)	none	none

4.3 Key Protection

Private and secret keys are protected inside the module. No command, public or hidden, permits the display or export of these keys. In addition, the private keys are stored in Triple-DES encrypted form, using a fixed Triple-DES 192 bit key generated by hashing the chassis serial number and various constants located throughout the firmware. Since this Triple-DES key is fixed for any given chassis, from the vantage of FIPS 140-2 it is logically equivalent to plaintext key storage.

Secret keys are never stored or archived. During the session, the secret key is located in SDRAM data structures that are not accessible to any user or crypto-officer. All secret keys and key schedules are zeroized as soon as their session is terminated.

Only the RSA public key is distributed. Public keys are stored in plaintext form.

4.4 Key Destruction

The RSA public/private key pairs in the BG5000/6000 Cryptographic Module are stored in non-volatile memory. They are zeroized either through an explicit console command, or when the Crypto-officer directs that a new key pair be generated to supplant the old one.

Session keys and key schedules are destroyed (zeroized) when the cryptographic session is terminated, or when the unit is powered off.

Powering off the unit will destroy all session keys. Session keys can also be destroyed by pressing system reset.

The BG5000/6000 supports a “Factory Reset” capability that is intended to revert the device to its unconfigured state as originally shipped. This process will erase the flash memory containing all public/private key pairs, remote public keys, and all site configuration parameters. Factory reset may be invoked either through a console command, or by continuously holding down the system reset button for 10 seconds while the unit is powered up. The unit is then rebooted which will cause any critical security parameters in memory to be zeroized.

The console password may be modified, but it cannot be removed except through a Factory Reset.

The USB token contents are generated at the factory and are never modified. There is no mechanism in the BG5000/6000 to destroy the token contents.

4.5 Random Number Generation

Random number generation takes a different form depending on the support or presence of the HiFn 7855 cryptographic hardware processor.

4.5.1 Random Number Generation with Hardware Support (Models 5400, 5500, 5600, 6400, 6500, 6600)

The BG5000/6000 Cryptographic Module uses both a non-deterministic and deterministic random bit generation scheme. The HiFn 7855 crypto processor is used to generate a hardware-based, nondeterministic random bit sequence.

The hardware nondeterministic random number generator is not an Approved RNG.

The hardware RNG and its supplied firmware driver is constantly conditionally tested for failure to a constant value.

If any failure is detected in the HiFn 7855 processor, during initialization, Self Test, or normal cryptographic operations, the crypto processor is disabled and random number generation reverts to the firmware version discussed in Section 4.5.2.

4.5.2 Firmware Random Number Generation (Models 5100, 5200, 6100, 6200)

The BG5000/6000 Cryptographic Module uses a deterministic random bit generation scheme, with constant nondeterministic reseeding. An initial seed is generated from a 256 byte random bit string, unique to that unit’s serial number, that is installed at time of manufacture. This random seed is continuously XOR-ed with random 1 microsecond resolution packet arrival times to produce a changing 20 byte seed value. This seed is then the basis of the deterministic RNG, an implementation of the RSA Crypto-C 6.1.1 library. The deterministic RNG uses a SHA-1 hash of the seed for input.

The Crypto-C deterministic random number generator is not an Approved RNG.

The RNG is seeded as follows:

- At each device initialization, the random number seed is primed with a 256 byte random string generated as part of that serial number’s personality information. This random quantity is treated like a Critical Security Parameter and is never available for inspection.
- Every time a cryptographic tunnel management packet arrives, either for tunnel establishment or periodic keepalive messages, the low order 32 bits of the packet arrival time since device initialization, measured to a resolution of 1 microsecond, is added to the random number seed.
- Every 5 minutes, the random number seed is merged with 16 bytes of random information stored in the Nonvolatile RAM, then the next 16 bytes of generated pseudo-random data from the RNG is written back into the same 16 bites of NVRAM. This

ensures that the unpredictability of the RNG seed increases with time, even across resets and power cycles of the BorderGuard.

This reseeding algorithm takes place even if the cryptographic hardware is present and functioning in the 5400, 5500, 5600, 6400, 6500, and 6600 models. Thus if the crypto processor were to fail, the firmware RNG can immediately take over with the minimally predictable seeding discussed above.

The firmware RNG is constantly conditionally tested for failure to a constant value.

4.6 Cryptographic Algorithms

Table 6: BG5000/6000 Cryptographic Module — Algorithms

Algorithm	Mode	FIPS 140-2 Approved Algorithm	NIST Certificate Number	Usage	Test
AES128	Firmware	Yes FIPS 197	116	Encrypt/decrypt traffic	KAT
AES192	Firmware	Yes FIPS 197	116	Encrypt/decrypt traffic	KAT
AES256	Firmware	Yes FIPS 197	116	Encrypt/decrypt traffic	KAT
AES128	Hardware (HiFn 7855)	Yes FIPS 197	173	Encrypt/decrypt traffic	KAT
AES192	Hardware (HiFn 7855)	Yes FIPS 197	173	Encrypt/decrypt traffic	KAT
AES256	Hardware (HiFn 7855)	Yes FIPS 197	173	Encrypt/decrypt traffic	KAT
DES	Hardware (HiFn 7855)	Yes FIPS 46-3	271	Encrypt/decrypt traffic. (Transitional phase only — valid until May 19, 2007)	KAT
DES	Firmware	Yes FIPS 46-3	119	Encrypt/decrypt traffic; backup for DES hardware encryption. (Transitional phase only — valid until May 19, 2007)	KAT
TDES	Hardware (HiFn 7855)	Yes FIPS 46-3	275	Encrypt/decrypt traffic	KAT
TDES	Firmware	Yes FIPS 46-3	228	Encrypt/decrypt traffic; backup for TDES hardware encryption	KAT
IDEA	Firmware	No	none	Encrypt/decrypt traffic	KAT

Algorithm	Mode	FIPS 140-2 Approved Algorithm	NIST Certificate Number	Usage	Test
HMAC SHA-1	Hardware (HiFn 7855)	Yes FIPS 198	22	Integrity check traffic	KAT
HMAC SHA-1	Firmware	Yes FIPS 198	21	Integrity check traffic	KAT
HMAC MD5	Hardware (HiFn 7855)	No	none	Integrity check traffic	KAT
HMAC MD5	Firmware	No	none	Integrity check traffic	KAT
MD5	Hardware (HiFn 7855)	No	none	Integrity check traffic	KAT
MD5	Firmware	No	none	Integrity check traffic; backup for MD5 hardware	KAT
SHA-1	Hardware (HiFn 7855)	Yes FIPS 180-1	258	Integrity check traffic	KAT
SHA-1	Firmware	Yes FIPS 180-1	49	Integrity check traffic; backup for SHA hardware	KAT
SHA-1	Firmware	no	none	PKCS #1 signatures of X.509 certificates on BG6000's only.	none; cert transfer fails if error
Diffie-Hellmann	Firmware (RSA Crypto-C 6.1.1)	no	none	Session key negotiation	Pairs test
RSA	Firmware (RSA Crypto-C 6.1.1)	no	none	DPF Session Authentication	Pairs test
RSA	Firmware (SSH IPSec Express)	no	none	X.509 certificate management on BG6000's only.	none
FIPS 113 DAC DES MAC	Firmware	yes	119 (vendor affirmed)	Validates authenticity of firmware image. Transitional Phase only — valid until May 19, 2007.	firmware load fails if error
USB Token Validation	Firmware + "smart card" logic on token	no	none	Optionally determine if a unique USB token is inserted in the unit	firmware load fails if error

The BorderGuard contains both Approved and non-Approved cryptographic algorithms. Crypto-Officers have two mechanisms to ensure whether Approved algorithms are being used:

- By examining the definitions of cryptographic tunnels, and ensuring that only Approved algorithms as specified in Table 6 are specified.
- By entering the `dpf show status` console command, which will print a summary of the number of cryptographic sessions operating in Approved mode, and the number which are in non-Approved mode.

5.0 Physical Security Policy

The module is a multi-chip standalone embodiment, housed within a 1-unit high sheet metal chassis, protected by tamper evident seals and four tamper proof screws. The placement of the screws and tape on the chassis is shown in Figure 5 on page 18. The tamper resistant screws consist of a five pointed star receptacle with a center pin, and require a special tool licensed by the manufacturer to remove. The tamper evident tape shatters as it is removed.

There are no user or administrator serviceable or configurable items inside the chassis. There is no reason for the customer to open the chassis, which must be returned to the factory should maintenance be required.

The tamper evident seal must be inspected periodically to detect tampering.

The module conforms with the EMI/EMC requirements in FCC Part 15, Subpart J, Class A.

Physical security may also be enhanced with the optional USB token that is keyed to a particular BG5000/6000. Whenever the unit is powered on, boot code will not proceed to initialize the unit unless a cryptographic challenge between the BG5000/6000 and USB token succeeds. Thus if the USB token key is removed and kept in a safe location, the BG5000/6000 may not be placed into any type of service.

FIGURE 5. Placement of Physical Security Safeguards

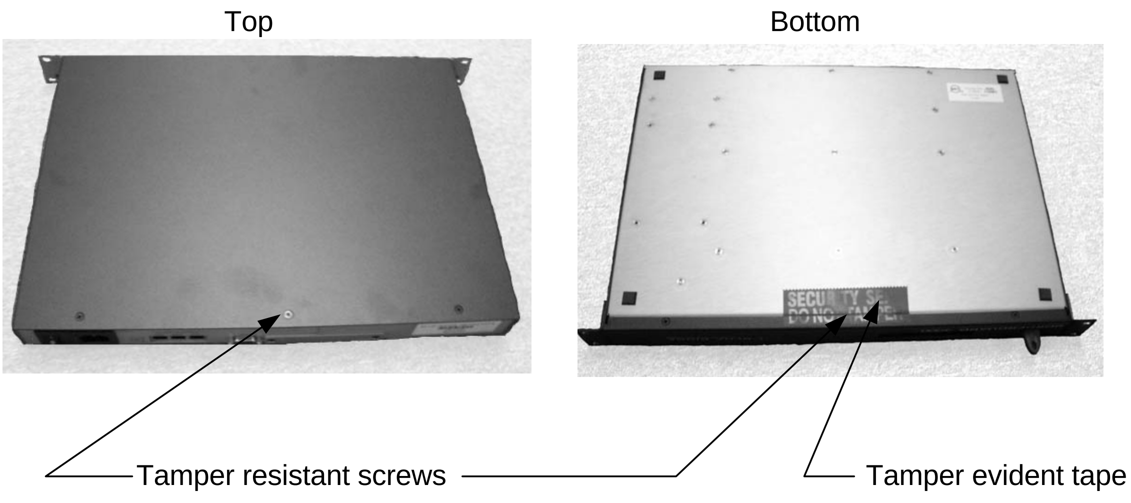


Table 7: Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Detail
Tamper evident tape	Variable; dependent of security of area in which the BG5000/6000 is located	Inspect tape for breaks; the tape cannot be removed without fragmenting into pieces

6.0 Mitigation of Other Attacks

6.1 Replay Prevention

The BG5000/6000 Cryptographic Module can also optionally institute replay protection by insuring that any packet is received only once. The module maintains a record of recently received sequence numbers. If the incoming packet has a sequence number that has already been recorded, the module will drop the packet and raise an alarm.

6.2 Denial of Service Attacks

The BG5000/6000 Cryptographic Module recognizes that service to legitimate users may be denied through illicit session establishment attempts that are recognized by the attacker to fail.

Should a session connect request be received that does not result in a successful connection, the IP address from which the request originated will be placed on an “unreachable” list for an exponentially increasing period of time, and further requests from that source will be ignored.

Similarly, if the BG5000/6000 originates a connection that fails for some reason (most likely because the partner BG5000/6000 is unreachable), it will defer connects to that device for an exponentially increasing period of time to avoid “thrashing” the authentication mechanism.

7.0 Self-Tests

7.1 Mandatory tests

Mandatory tests are performed at boot time, when the BG5000/6000 Cryptographic Module is in the initialization state. These include:

- On the BorderGuard 5400, 5500, 5600, 6400, 6500, and 6600 modules with hardware crypto support:
  - Testing the hardware cryptographic processor to check its register and data transfer operation.
  - Testing the Approved DES and TDES hardware based encryption and decryption algorithms with a known answer test.
  - Testing the Approved AES-128, AES-192, and AES-256 hardware based encryption and decryption algorithms with a known answer test.

  - Testing the Approved HMAC SHA-1 and un-approved HMAC MD5 hardware based hashes with a known answer test.
- Testing the firmware implemented AES-128, AES-192, AES-256, DES, and Triple-DES encryption algorithms with a Known Answer Test.
- Testing the Approved HMAC SHA-1 and non-Approved SHA-1 firmware based hashing algorithm with Known Answer Tests.
- Testing the random number generator using the Ones, Poker, Runs and Long Runs tests as previously specified in FIPS 140-2 section 4.9.1.
- Testing the non-Approved HMAC MD5 and MD5 firmware based hashes with a known answer test.

7.2 Conditional Tests

The BG5000/6000 Cryptographic Module performs several Conditional tests during operation

- The output of the Random Number Generator is continuously checked to ensure that it is not returning a constant value.
- RSA public/private key pairwise consistency test.
- Firmware load test.

7.3 Optional self-tests

Optional self tests are available to the crypto-officer for discretionary module testing and include all of the KATs above.

All Mandatory tests detailed above may be run at any time though console commands entered by the Crypto-officer.

Additional optional tests exist for:

- Pairwise consistency of Diffie-Hellman operation at all supported key lengths.
- KAT's for the non-Approved IDEA encryption algorithm.

7.4 Failure of self-test

In the event of a self test failure of the cryptographic hardware, or if an error is detected during continuing operation of the cryptographic hardware, the BG5000/6000 Cryptographic Module will disable the hardware processor and proceed to perform all cryptographic transforms using firmware. Errors encountered are shown on both the front panel LCD display and any attached serial console.

The BG5000/6000 has no specific provisions for failure of the firmware algorithms, as this indicates either an internal failure of the controlling 440GX processor, or run-time corruption of the code or SDRAM memory access. In these circumstances, the BG5000/6000 will cease useful program execution and pass no further data of any type.

Appendix A Glossary of Acronyms

AES Advanced Encryption Standard. An Approved algorithm defined in FIPS 198, supporting 128, 192 and 256 bit keys.

ANSI American National Standards Institute. In the context of this document, ANSI is responsible for the definition of the C programming language used for most of the BG5000 firmware.

CRC32 32 bit Cyclic Redundancy Check. A common mechanism to detect data corruption (but not cryptographic attack) in a stream of data.

CSP Critical Security Parameter. A value such as a cryptographic key, whose disclosure or modification might compromise the security of the system.

DES Data Encryption Standard. A once widely used encryption algorithm defined in FIPS 46-3.

DPF Data Privacy Facility. The Blue Ridge Networks trade name for its cryptographic function, and the designation for the Cryptographic Module.

EMC Electromagnetic Compatibility. The degree with which a device will tolerate EMI from nearby devices.

EMI Electromagnetic Interference. A measure of the degree to which radio frequencies emitted by a device might interfere with the operation of other nearby appliances.

HMAC A keyed message authentication algorithm, where the message contents and a secret key are cryptographically hashed so that an attacker cannot produce a message deemed genuine to the receiver without knowledge of the key.

IDEA International Data Encryption Algorithm. A non-Approved cryptographic algorithm in moderately wide use.

IP Internet Protocol, as defined in RFC 791.

KAT Known Answer Test. The process of presenting fixed inputs to a cryptographic algorithm, and comparing the compute result with a published, expected result.

MD5 Message Digest (version 5). A non-Approved cryptographic hashing algorithm.

PHY In the context of an Ethernet interface, the electronics that convert the transmit/receive bit stream to analog signals on the Ethernet medium and vice versa. Thus optical and twisted pair Ethernet interfaces would have different PHY’s.

RNG Random Number Generator.

RSA

1. RSA Data Security Inc., the supplier of the cryptographic library used for authentication, key exchange, and random number generation in the BG5000.

2. Rivest-Shamir-Adleman public/private key encryption algorithms. The basis of User authentication on the BG5000.

SDRAM Synchronous Dynamic Random Access Memory. A common electronic technology for high capacity, moderate speed random access memory.

SHA-1 Secure Hash Algorithm (version 1). An Approved cryptographic hashing algorithm.

Triple-DES A cryptographic block cipher using 112 or 168 bit keys. An Approved algorithm defined in FIPS 46-3.

TOS Type of Service. In the context of this document it specifically refers to the 4 bit Type of Service field in an Internet Protocol packet header that directs network equipment to optimize transmission for throughput, performance, etc.

USB Universal Serial Bus. A common standard for the connection of low and medium speed devices to personal computers. The BG5000 optionally takes advantage of USB based “smart card” tokens to unlock suitably configured BG5000 devices.

X.509 Refers to a large body of documents defining a Public Key Infrastructure, where Certificate Authority servers cryptographically sign public key “certificates” and distribute them to client hosts. Each host retains a private key matching the public key known to the Certificate Authority and properly designed messages from these hosts may be authenticated by other hosts with access to the Certificate Authority.