Security Policy

Blue Ridge Networks
BorderGuard 3000
Data Privacy Facility (DPF)
June 18, 2001

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

Name: BorderGuard 3000
Version: DPF1 V6.0
Vendor: Blue Ridge Networks, 14120 Parke Long Court, Suite 201, Chantilly, VA 20151

1.2 Description

The BorderGuard 3000 (henceforth abbreviated BG3000) is a standalone Internet security appliance that takes the form of an electronic chassis containing a processor, memory, networking and crypto components, and firmware.

The BG3000 is a multi-function appliance 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.)

The BG3000 is typically installed so that it forwards network data packets entering and exiting a site or secure enclave. Using a Forwarding Policy specified by the Crypto-Officer, it selectively transforms network packets inbound or outbound to a remote site/enclave or an individual user's host. It 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 Ethernet Local Area Networks or V.35 Wide Area Networks, and is able to exercise a Security Policy on Internet data packets (IP datagrams) that would normally flow between the two connected networks. In addition to its two network interfaces, it 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.

1.3 Basic Security Rules

1.3.1 Access to Critical Security Parameters (CSP)

Users: Users have no access to Critical Security Parameters, and never have access to the module's management capabilities. They have no option to enable or disable the cryptographic service, or any direct control over the Forwarding Policy selected for the unit.

Crypto-Officer: The crypto-officer has access to security relevant data. Items the crypto-officer can

control:

- 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 BG3000's requires the explicit cooperation of the remote unit's Crypto-officers.
- Control of the Forwarding Policy within the BG3000, 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 then 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. A single RSA private key for the unit may be generated by the Crypto-officer, but it cannot be inspected during or after generation. Only the public key associated with the private key is available for export.

1.4 Physical Security

The module is a multi-chip standalone embodiment, housed within a 1-unit (1 3/4") high sheet metal chassis, protected by tamper evident seals and tamper proof screws. There is no user serviceable or user 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 module conforms with the EMI/EMC requirements in FCC Part 15, Subpart J, Class A.

2.0 Design Concepts

The module 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.
- 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, which is the logical Cryptographic Module to which this Security Policy applies, executes the cryptographic functions.

2.1 Cryptographic Boundary

The physical cryptographic boundary for the module consists of the entire BG3000 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”.

The logical cryptographic boundary is the DPF cryptographic module. The DPF consists of a firmware module (cs31060.ffw) stored on FLASH memory. The DPF executes encryption, decryption and session management functions.

2.2 Interfaces

The physical interfaces are two 10BaseT/AUI Ethernet ports (via the forwarding module) and the console RS232 port. One of the Ethernet interfaces may optionally be factory replaced with a V.35 WAN interface. There is also a power interface for 120 VAC to a internal power supply, and eight status front panel LED’s.

The logical interfaces to the DPF Cryptographic Module are data input (plaintext and ciphertext), data output (plaintext and ciphertext), data output (discarded packets), control input, and status output to LED’s and the control terminal.

Accessible manual controls only consist of an AC power on/off switch.

No maintenance interface exists.

2.3 States

The module is designed as a finite state machine. The basic states are Power off, Boot, Initialization, Operating, and Error.

2.4 Processors

The code is executed on a Motorola 68EC060 processor; hardware logic for the Ethernet and V.35 WAN interfaces is supplied by a Motorola EC68360 processor. Hardware traffic encryption functions are performed with a HiFn 7711 encryption chip.

2.5 Firmware Security

The module is written in ANSI C. The software algorithms for DES, TDES, and IDEA algorithms are written in assembly language; however, reference C-code implementations of the algorithms are provided for these modules.The BSAFE static library and the NSC1 source code are proprietary and not available for inspection.

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 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.

2.6 Embedded Operating System

The operating system is a proprietary embedded system control program written specifically for the BorderGuard product line. The operating system is not accessible to the user nor is it shared with other applications. The operating system does not permit the dynamic addition and execution of code from any source.

3.0 Roles

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 internals of the module.

3.1 Crypto-officer

The Crypto-officer is as an individual charged with installation and maintenance of the BG3000, 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 BG3000.
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 BG3000 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 BG3000 are those host computers and their associated individuals who generate network traffic to be processed by the BG3000. Since these user data sources and destinations are networked devices, Users and their hosts do not have to be co-located with the BG3000.
Operation of the BG3000, and any decision as to whether the BG3000's services will be performed for a User, are completely under the control of the policies set by the Crypto-officer. Users may be completely unaware of the fact that the BG3000 exists, or that it is securing data they are sending to remote locations.

3.3 Policy Definition

The function of defining a site security policy for the module is described in the BorderGuard 3000 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 3000 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

Security 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 BG3000 include:

- Encryption — prevents untrusted parties from examining the contents of traffic moving between sites. Four encryption algorithms (DES, TDES, IDEA, NSC1) are available.
- Integrity Checking — digitally signs 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. SHA-1 and MD5 HMAC signatures are available.
- Replay Prevention — prevents attacks caused by re-introducing a previously sent legitimate data packet into a secured data stream.

The BG3000 also offers data compression services for traffic moving between secured sites.

4.0 Access Control

All access to module policy 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.

5.0 Key Management

Keys used by the module include the following:

- A 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.
- Encryption traffic keys which include DES, TDES, IDEA and NSC1. These keys are generated through the Diffie-Hellmann 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 MD5 and SHA-1 keyed hashes. These are used where a shared secret is exchanged between sender and receiver and guards against a man-in-the-middle attack. These keys are zeroized upon termination of the session.

5.1 Key Protection

Private and secret keys are protected inside the module. No command, public or hidden, permits the display or export of these keys. The memory dump command maintains a list of “forbidden” areas, and will display all zeros in lieu of private or secret keys. In addition, the private key is stored in encrypted form. Secret keys is are never stored or archived. During the session, the secret key is located in DRAM data structures that are not accessible to any user or crypto-officer.

Only the RSA public key is distributed; This distribution may be done in a secure way to prevent unauthorized alteration. Public keys are stored in plaintext form.

5.2 Random Number (Bit) Generation

The module uses both a non-deterministic and deterministic random bit generation scheme. A hardware chip, the Tundra RBG1210, is used to generate a random bit sequence. This random sequence is continuously XOR-ed with random 40 nanosecond resolution packet arrival times to produce a changing 16 byte seed value. This seed is then the basis of the deterministic RNG, an implementation of the BSAFE 3.0 library. The deterministic RNG uses a MD5 hash of the seed for input.

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

5.3 Cryptographic Algorithms

Algorithm	Mode	NIST Certificate Number	Usage	Test
DES	Hardware (HiFn 7711)	120	Encrypt/decrypt traffic	KAT
DES	Firmware	119	Encrypt/decrypt traffic; backup for DES hardware encryption	KAT
TDES	Hardware (HiFn 7711)	58	Encrypt/decrypt traffic	KAT
TDES	Firmware	57	Encrypt/decrypt traffic; backup for TDES hardware encryption	KAT
IDEA	Firmware	none	Encrypt/decrypt traffic	KAT
NSC1	Firmware	none	Encrypt/decrypt traffic	KAT
MD5	Hardware (HiFn 7711)	none	Integrity check traffic	KAT

Algorithm	Mode	NIST Certificate Number	Usage	Test
MD5	Firmware	none	Integrity check traffic; backup for MD5 hardware	KAT
SHA-1	Hardware (HiFn 7711)	50	Integrity check traffic	KAT
SHA-1	Firmware	49	Integrity check traffic; backup for SHA hardware	KAT
Diffie-Hellmann	Firmware (Bsafe 3.0)	none	Session key negotiation	Pairs test
RSA	Firmware (Bsafe 3.0)	none	Session Authentication	Pairs test

5.3.1 Replay Prevention

The Cryptographic Module can also optionally institute replay protection by insuring that any packet is received only once. The DPF 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.

6.0 Self-Test

6.1 Mandatory tests

Mandatory tests are performed at boot time, and when the DPF cryptographic module is in the initialization state. These include:

- Testing the cryptographic processor to check its register and data transfer operation.
- Testing the DES and TDES encryption and decryption with a known answer test. Both the cryptographic hardware algorithms and the firmware algorithms are tested.
- Testing the MD5 and SHA-1 hashes with a known answer test. Both the hardware and firmware algorithms are tested.
- Testing the random number generator for failure to a constant value. This test continues throughout the operation of the module.

6.2 Optional self-tests

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

Additional optional tests exist for:

- Pairwise consistency of RSA keys, both the native RSA keys of the device, and newly generated keys.
- Pairwise consistency of Diffie-Hellman operation.

- Statistical randomness of the random number generator.

6.3 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 DPF will disable the hardware processor and proceed to perform all cryptographic transforms using firmware.
A self test of the cryptographic algorithm firmware is also performed at initialization, whether or not the cryptographic hardware tests succeed. Should an error in the firmware self tests occur, the BG3000 fails and places itself in an inoperative state.