National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

CyberGuard Firewall/VPN Version 6.2.1

Report Number: **CCEVS-VR-05-0137**
Dated: **December 6, 2005**
Version: **1.04**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

CyberGuard Corporation
350 SW 12th Avenue
Deerfield Beach, Florida 33442
USA

Evaluation Personnel:
CygnaCom Solutions, McLean VA
Sai Pulugurtha (lead evaluator)
Swapna Katekaneni (evaluator)
Gary Grainger (evaluator)

Validation Personnel:
Scott Shorter, Orion Security Solutions
Olin Sibert, Orion Security Solutions

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the CyberGuard Firewall/VPN. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the CyberGuard Firewall/VPN was performed by the CygnaCom Solutions Common Criteria Testing Laboratory in the United States and was completed in September 2005. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by CyberGuard Corporation. The ETR and test report used in developing this validation report were written by CygnaCom Solutions. The evaluation team determined the product to be Part 2 and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4 (augmented with Systematic Flaw Remediation) have been met.

The CyberGuard Firewall/VPN is a network device that acts as a barrier between networks, typically between an organization's network and external networks. It provides controlled and audited access to services from the internal to the external network, by inspecting and performing access control and redirection on the data that it receives. As an application proxy, it enables controlled and authenticated FTP and telnet sessions from external to internal networks, and as a packet filter, it permits or denies the traversal of packets between external and internal networks based on the configured security policy. Figure 1 illustrates the physical configuration of the TOE.

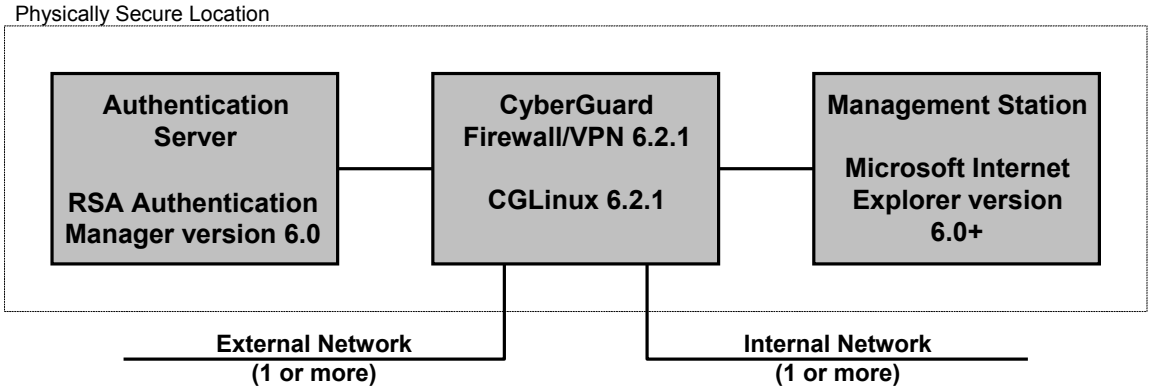

Figure 1 - TOE Hardware Components

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 4 evaluation. Therefore the validation team concludes that the CygnaCom CCTL findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called

Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL pay a fee for their product's NIAP Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	CyberGuard Firewall/VPN Version 6.2.1
Security Target	*CyberGuard Firewall/VPN Version 6.2.1,* ST revision 1.3, September 30, 2005
Protection Profiles	N/A
Evaluated Hardware	Models: *1150, 1250, 3100, 3400, 3600, 5100, 7100* Network Interface Cards: • Silicon 6-Port Copper Silicom • 4-Port Fiber Intel • PRO 1000MT Dual Copper • Intel PRO 1000MF Dual Fiber • Intel PRO100M Single 10/100 • Interphase 554
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation CyberGuard Firewall/VPN Version 6.2.1*; Version 1.0, September 30, 2005.
Conformance Result	CC Part 2 conformant, CC Part 3 conformant, EAL 4 augmented by ALC_FLR.3
Sponsor	CyberGuard 350 SW 12th Avenue Deerfield Beach, Florida 33442

Item	Identifier
Common Criteria Testing Lab (CCTL)	CygnaCom/Entrust 7925 Jones Branch Drive Suite 5200 McLean, VA 22102-3321
CCEVS Validator(s)	Scott Shorter, Orion Security Solutions Olin Sibert, Orion Security Solutions

3 Security Policy

The security policy enforced by the TOE consists of the *unauthenticated information flow policy* that controls the traffic filter functionality of the firewall, and the *authenticated information flow policy* that controls the application proxy functionality.

3.1 Unauthenticated information flow policy

The TOE shall permit or deny unauthenticated external IT entities to pass data traffic from internal to external networks (and vice versa) based on the following information security attributes:

- The presumed address of the source and destination, as specified by the source and destination IP addresses in each IP datagram ("packet");
- The transport layer protocol, as specified by the protocol ID field in each IP datagram; and
- The identity of the physical network interface on which the traffic arrives and departs the TOE, as specified by the hardware configuration of the TOE.

The flow shall be permitted under the following circumstances:

- All information security attribute values are unambiguously permitted by the security policy rules created by the authorized administrator, where such rules may be composed from all possible combinations of the values of the information security attributes;
- The presumed addresses of the source and destination translate to a network address on the appropriate network (i.e. packets received from an internal network interface must have source IP address corresponding to the internal network, etc);
- Only supported transport layer protocols are permitted (TCP and UDP);
- Received datagrams do not contain loopback or broadcast source addresses, nor do they specify the route (i.e., using IP options); and
- For application protocols supported by the TOE (Telnet, FTP, HTTP, SMTP), command requests conform to applicable published protocol specifications.[1]

For TCP datagrams, the unauthenticated information flow policy is enforced at the level of TCP sessions. When a datagram is received, the packet filter first determines if it belongs to an existing session, the datagram is handled normally, if no existing session is found then the datagram belongs to a new session and the packet filter rules are applied. The unauthenticated information flow policy is applied independently to each UDP datagram.

[1] Network protocol errors will be rejected before the information flow policies are applied.

3.2 Authenticated information flow policy

The TOE shall permit or deny human users or external IT entities the ability to send FTP, telnet, HTTP or SMTP traffic from internal to external networks (and vice versa) based on the following information security attributes:

- The presumed address of the source and destination, as specified by the source and destination IP addresses in each IP datagram ("packet");
- The transport layer protocol as specified by the protocol ID field in each IP datagram;
- The identity of the physical network interface on which the traffic arrives and departs the TOE, as specified by the hardware configuration of the TOE;
- The application service, as specified by the destination port number used in establishing the protocol session;
- The user identity, as specified by the identity and authentication information supplied to each protocol's authentication mechanism; and
- The security-relevant aspects of each protocol request.

The application level traffic shall be permitted under the following circumstances:

- All information security attribute values are unambiguously permitted by the security policy rules created by the authorized administrator, where such rules may be composed from all possible combinations of the values of the information security attributes;
- The presumed addresses of the source and destination translate to a network address on the appropriate network (i.e. packets received from an internal network interface must have source IP address corresponding to the internal network, etc);
- The appropriate protocol ID (TCP) and destination socket are present in the datagrams;
- Received datagrams do not contain loopback or broadcast source addresses, nor do they specify the route (i.e., using IP options);
- The human user initiating the FTP or telnet session authenticates either via password or single use authentication mechanism; and
- FTP and telnet command requests conform to applicable published protocol specifications.

4 Assumptions

4.1 Physical Security Assumptions

- All TOE components are protected from physical access.
- Information cannot flow between the internal and external networks without passing through the TOE.
- The TOE is administered locally.

The validators consider these assumptions to be reasonable for the operational environments to which this product is targeted. The very nature of a firewall product is consistent with physical protection.

4.2 Personnel Security Assumptions

- Authorized administrators are suitably qualified, non-hostile and follow all administrator guidance.

The validators consider this assumption to be reasonable for the operational environments to which this product is targeted. Administrative activities are required only to implement and maintain organizational policies, and are plausibly within the scope of security management personnel. The administrative interface is straightforward and does not require an unusual amount of knowledge or training to use effectively.

5 Architectural Information

The high level architecture of the TOE is shown in Figure 2. The CyberGuard Firewall/VPN Appliance, the central block of the figure, consists of compliance tested hardware, a specially developed Linux operating system with enhanced protections against bypassibility, and the application level firewall software.

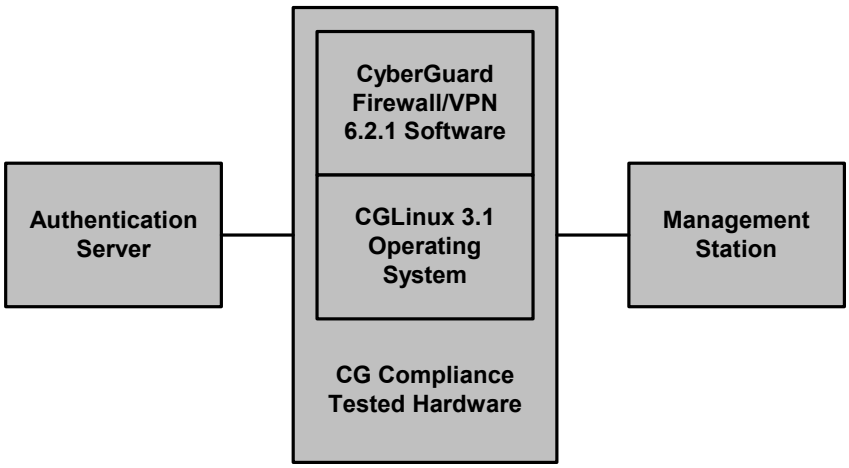

Figure 2 - TOE Architecture

5.1 Product Hardware

The hardware platform consists of processor, memory, disk, and network interface components that are assembled to CyberGuard's specifications and that provide the environment for running the CGLinux 3.1 operating system and the firewall software components. CyberGuard's specifications, analysis process, and compliance testing ensure that the hardware provides appropriate support for the software and does not expose extraneous security-relevant functions outside the TOE. The specific supported hardware components and configurations are described in the Security Target [10]. The Intel IA-32 processor architecture used by the hardware platform provides memory protection and user/supervisor mode protection to allow the CGLinux operating system to isolate and protect other firewall software components. Although the hardware includes these security-enforcing mechanisms, they are used solely as a structuring mechanism for the TOE software, and are not responsible for direct enforcement of any product security policies.

The hardware platform is delivered fully configured and operational by CyberGuard. The end user is not permitted to make changes to the hardware except for addition of network interfaces and memory (which must also satisfy the rules for valid evaluated configurations). The CGLinux operating system and firewall software are pre-installed on the hardware platform.

The Management Station is a workstation running a Microsoft Windows operating system and the Internet Explorer (version 6.0 or later) browser software. It interacts with the browser-based administration software that is part of the firewall product. The Management Station provides access to the administrative interfaces but performs no security functions of its own. It is connected to the main firewall hardware platform by a dedicated network link and interface, and may not be connected to any other networks or systems.

The Authentication Server is a dedicated computer system running the *RSA Authentication Manager Version 6.0* software supplied by RSA Security. The *RSA Authentication Manager Version 6.0* implements part of the firewall's single-use authentication mechanism and interacts with the firewall software through the RADIUS Authenticator plug-in component. It is connected to the main firewall hardware platform by a dedicated network link and interface, and may not be connected to any other networks or systems.

5.2 Product Software

The CGLinux 3.1 operating system provides the software environment in which all the firewall software components operate. It provides file system services (e.g., for storage of TOE software components, configuration data, and audit data), process management services (e.g., for establishing processes that implement firewall policies, such as proxy services), and network services (e.g., facilities to send and receive IP and UDP datagrams, and to communicate over TCP sessions).

The CGLinux 3.1 operating system includes security-relevant enhancements relative to the base capabilities of the standard Linux operating system:

- Kernel residual data protection (see kernel extensions subsystem below)
- Non-bypassibility (see kernel extensions subsystem below)
- Process Control (see kernel extensions subsystem below)
- Ruleset based access control
- Packet filter

In addition, the standard audit facilities of CGLinux 3.1 are used to implement audit data collection and storage mechanisms.

All software modules and processes running on the hardware platform are supplied as part of the CyberGuard Firewall/VPN 6.2.1 product. No software from other sources is ever permitted to run on the platform.

All administrative activities in normal operation are performed through the browser-based administrative interface. Certain aspects of system installation and failure recovery, however, rely on standard Linux commands to initialize the product into its evaluated configuration.

5.3 TSF Subsystems

The CyberGuard Firewall/VPN 6.2.1 is composed of distinct subsystems. Each provides functionality that is cleanly separated from the other subsystems as shown in Figure 3. The figure demonstrates the TSF enforcing components of the firewall software (implemented as independent processes running in user space) and the CGLinux operating system (running in kernel space). The separation of subsystems follows the natural separation based on the underlying functionality of each subsystem.

The following are the evaluated subsystems within the CyberGuard Firewall/VPN TOE:

- Administration subsystem
- CyberGuard Identification and authentication subsystem
- Audit subsystem
- Telnet proxy subsystem
- FTP proxy subsystem
- Ruleset based access control subsystem
- Packet filter subsystem
- Kernel extensions
- External network interfaces

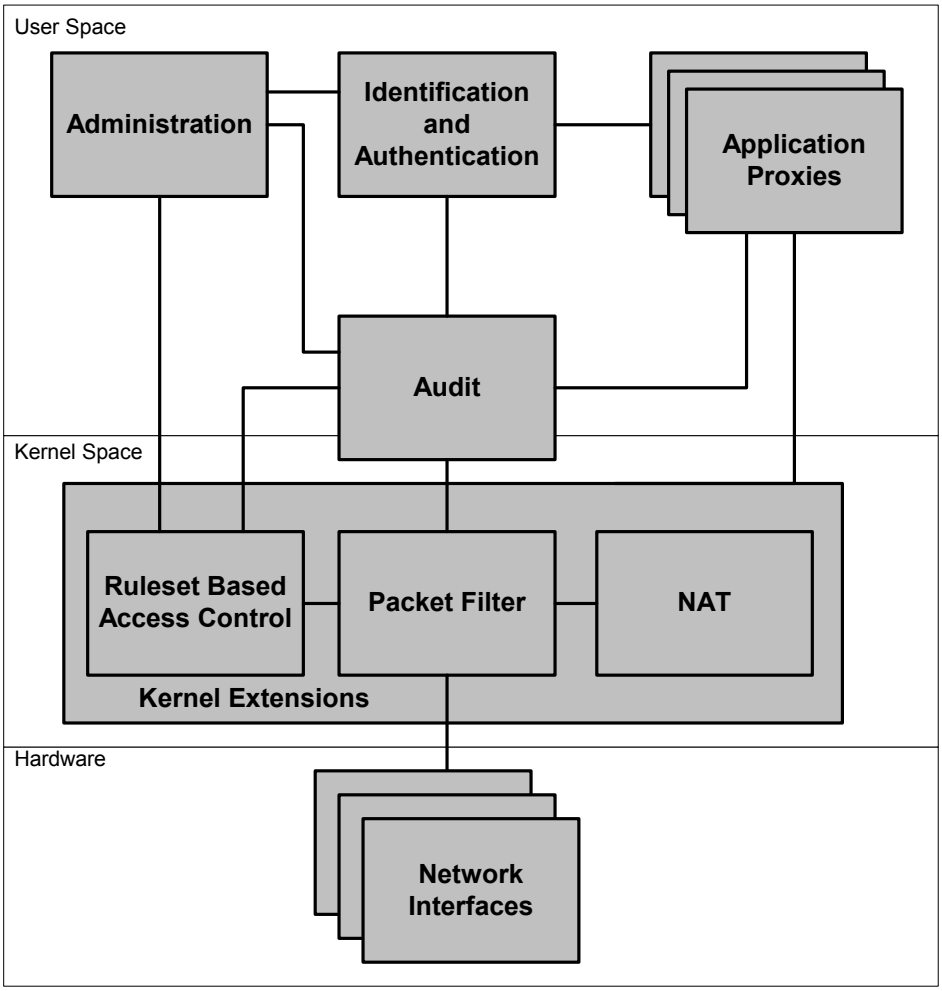

Figure 3 - CyberGuard Firewall/VPN Functional Architecture

5.3.1 Administration Subsystem

The administration subsystem provides the user interface that permits authorized administrators to modify the functionality and operations of the firewall, including modifying the rulesets that are used by the authenticated and unauthenticated information flow policies, managing the users for password based and single use authentication, and controlling audit settings and reviewing the audit logs.

5.3.2 CyberGuard Identification and Authentication Subsystem

The identification and authentication subsystem (called CGIA in the ST) controls both password based user authentication (with a database of users stored in the firewall) and single user authentication (via the RSA Authentication Manager and the RADIUS Authenticator plug-in components). It interoperates with both the telnet and FTP proxies since it performs authentication and identification services on their behalf, the audit subsystem by recording auditable events, and is configured by the administration subsystem.

5.3.3 Application Proxy Subsystems

The application proxy subsystems (Telnet, FTP, HTTM, and SMTP) implement the authenticated information flow policy for their respective services. They interface with the identification and authentication subsystem to manage user login to the service, utilize the audit subsystem to

record auditable events, and rely on the network services provided by the kernel portions of the TOE.

5.3.3.1 FTP Proxy Subsystem

The FTP proxy implements the authenticated information flow policy for the FTP service. It interfaces with the identification and authentication subsystem to manage user login to the service, and utilizes the audit subsystem to record auditable events.

5.3.4 Audit Subsystem

The audit subsystem records auditable events on behalf of the other subsystems of the TOE, storing the results in a protected audit file. All other subsystems use the audit subsystem to record events.

5.3.5 Kernel Extensions

The TOE includes enhancements for several kernel functions. Functions modified are the IP packet input and output handling functions to allow the packet filter to bind to network interfaces, and the memory release functions to guard against residual data in memory utilized for processing packets. These enhancements ensure that the Packet Filter engine processes all packets, that the TOE security mechanisms are not bypassable and that all memory is cleared upon release to the system.

5.3.6 Ruleset Based Access Control Subsystem

The ruleset based access control subsystem (RSBAC) operates in kernel space, and provides access control mechanisms for the TOE in terms of role enforcement and to create a separate domain of execution for the TOE and TOE security functions.

5.3.7 Packet Filter Subsystem

The packet filter subsystem operates in the kernel space, inspecting all packets entering the firewall system and enforcing the policy on them and enforcing the configured information flow policy. The packet filter subsystem interacts with the FTP and telnet proxies, providing the underlying information flow policy enforcement on their behalf, with the audit subsystem to record events.

5.3.8 Network Interfaces

The network interfaces provide the external interface from the TOE to external and internal networks. They interface only with the packet filter subsystem. The network interface hardware provides data validation at the lowest level of abstraction: they are responsible for ensuring that valid link-layer datagrams are presented to the packet filter subsystem.

5.4 TSF Interface

The TSF interface of the CyberGuard Firewall/VPN 6.2.1 product has two elements:

1. The network interface that connects other systems to the firewall and controls the traffic flows to and from those systems; and
2. The browser-based administrative interface that allows administrators to control, operate, and configure the product.

The network interface operates at several different levels of abstraction, following the ISO Reference Model:

- Physical: Network hardware electrical interface
- Link Layer: Ethernet datagram processing. ARP datagrams are processed.

- Network: IP datagram processing. Fragmentation, IP options, and ICMP datagrams are processed.

- Transport: TCP stream and UDP datagram processing. ICMP messages are processed with respect to established TCP connections.

- Session: Application proxy processing. Proxies are provided for the Telnet, FTP, HTTP, and SMTP protocols.

- Application: FTP and Telnet authentication processing and validation.

Security policies are applied, as appropriate, at each of these levels to ensure that protocol data is meaningful and that operational policies are enforced. The network interfaces are all potentially subject to external attack, and therefore are designed to be self-protecting at all levels of abstraction.

The administrative interface is physically restricted (by configuration rules) to access by an authorized administrator. Because of this configuration rule, the administrative interface is not subject to external attack.

6 Documentation

The following documentation is provided with the product:

- *CyberGuard Firewall Version 6.2.1 Reference Manual*

- *Read Me First Installation and Setup*, Document Number IN005-001, June 2005

- *Using RSA/ACE Server 6.0 with fortress 6.2.1*, Document No FCC023-002, May 2005

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

In particular, developer testing contained the following types of tests:

- Confirmation of proper behavior of each of the parameters of the unauthenticated information flow policies, e.g.:
    - Packet filter drops sessions arriving on an external interface where the IP source address is that of an internal network
    - Packet filter drops sessions arriving on an external interface where the source address is an external broadcast
    - Firewall drops IP packets using the Source Routing IP options feature
    - Ability of packet filter to enforce security policy – permit an information flow from internal network to external/other connected network based on presumed source IP address, presumed destination IP address, transport layer protocol, interface on which traffic arrives and departs and service
- Confirmation of proper behavior of each of the parameters of the authenticated information flow policies, e.g.:

    - Firewall enforces authentication and filters service commands for application traffic from internal sites to external sites
    - Ability to filter application commands (e.g. for FTP permit GET commands but not DELETE, or for HTTP permit GET but not TRACE commands, etc)
    - The firewall should allow the application sessions between the internal and external hosts to be established only after successful authentication
    - Firewall denies application command requests that do not conform to specification
- Testing the Network Address Translation functionality of the TOE
- Testing that user data is protected appropriately, e.g.:
    - Ensure that no information from previous packets is leaked out of the firewall
- Testing authentication capabilities, e.g.:
    - Confirming that user accounts are blacklisted after a number of failed authentication attempts
    - Testing that the internal authentication blacklist can override the authentication server
    - Confirmation that application level telnet and FTP proxies require authentication before access is granted to the server
- Testing management and audit functionality, e.g.:
    - Firewall allows only authorized administrator to delete and create packet filtering rules – Unauthenticated SFP
    - Firewall allows only authorized administrator to delete, modify, and add attributes to a packet-filtering rule – Authenticated SFP
    - Audit records are protected from unauthorized deletion

The above list is not intended to be comprehensive, but merely representative.

The validators considered the developer testing to be comprehensive and thorough. The developer's extensive test automation system provides immediate access to test procedures and results performed on different versions of the system through its development lifecycle through a convenient browser-based interface. The automation system ensures a close relationship among product components (i.e., source code) and associated test plans and designs.

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team also ensured that all subsystem interfaces were tested by the developer. The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. Although the evaluation team performed only a sample of the developer's test suite, the selected tests were representative of the TOE Security Functions.

The independent tests run by the evaluation team included the following types of tests:

- Test that the firewall distinguishes between information flows arriving on different interfaces
- Expanded testing of packet filter functionality, e.g.:
    - Exercising allow/deny rules based on source IP address
    - Exercising allow/deny rules based on destination IP address
    - Exercising allow/deny rules based on transport layer protocol
    - Exercising allow/deny rules based on physical interface on which traffic arrives and departs
- Further testing of audit functionality, e.g.:
    - Address spoofed packets being dropped are audited
    - IP datagrams with source routing options being dropped are audited

    - Confirming audit of application proxy authentication attempts
    - Confirming audit of application filtering actions
    - Tests that only an authorized administrator can store and restore audit archives.
- Testing of application validation functionality, e.g.:
    - The ability to filter HTTP requests that exceed certain number or length of headers
    - The ability to block Java content from HTTP
- Confirmation that the application proxies provide appropriate security behavior with and without Network Address Translation turned on at the firewall
- NIC capabilities
    - Confirm that the firewall drops IPv6 packets

The validators considered the evaluation team testing to be comprehensive and thorough, demonstrating a good understanding of the product's capabilities by the evaluators.

8 Evaluated Configuration

The evaluated configuration of the CyberGuard Firewall/VPN Version 6.2.1 software consists of the Intel platform (min speed 133 MHz) running CyberGuard CGLinux Version 3.1 and CyberGuard Firewall/VPN Version 6.2.1, equipped with both on-board[2] and PCI Network Interface Cards (NIC), a disk storage device, memory, and a CDRom device. The evaluated configuration also includes the Management Station containing the Microsoft Internet Explorer 6.0 or above and the 'RSA Authentication Manager 6.0' for single use authentication.

The evaluated configuration requires configuration of some specific values of features, as outlined below. More details on these security considerations can be found in the product's guidance documentation:

- The prospective customer must define, document, and follow a network security policy that is appropriate for their site. However, the following security considerations must also be implemented to be complaint with the evaluated configuration of TOE:
- The TOE must be secured so that only authorized personnel have physical access to the TOE.
- The minimum password length for users must be set at eight and the password must consist of a combination of alphanumeric and special characters. These combinations will place the password name space well beyond the range that might make the passwords guessable within a reasonable amount of time.
- It is recommended that configuration and management of the TOE be designated to one administrator who has all administrative roles assigned to them.
- The TOE must not be configured to allow remote administration, since remote administration is not included in the scope of this evaluation.
- Direct connections to the TOE from an unprotected network (example FTP connections) must not be allowed in the site security policy.
- The TOE's interfaces must be configured to protect against IP Spoofing attempts in which a packet arrives on an interface other than that identified by its source address.
- It is not recommended to change the default setting of the "audit full condition" for the TOE to any other settings, since the TOE by default is set to shut down the network traffic if the audit space becomes full in order not to allow any traffic to pass where the audit of such traffic is not taking place.

[2] In the evaluated configuration, the onboard NIC cards shall not be used for the means of providing external network interface(s).

- The TOE must be configured to proxy all Telnet network traffic.
- The TOE must be configured to proxy all FTP network traffic.
- Users of network services Telnet and FTP must be set up with a single-use token-based method of authentication, not reusable password mechanism.
- User blacklisting feature must be enabled (it is not enabled by default).
- The "Set Blacklist Duration (minutes)" checkbox must also be enabled (not enabled by default). This field, when checked specifies the duration of time a user remains blacklisted. It is recommended that a large value to be set for this field (maximum number 2,147,483,647), in order to keep a user blacklisted until the administrator reviews and releases such users.
- The "Number of Failed Logon Attempts" field for repeated unsuccessful login attempt is set to three by default. Although the site security policy may dictate a different value for this field, it is not recommended to set this allowable number of attempts to a very large value.
- A value of 60 seconds has been configured by default for "Time Duration (seconds)" field of the user-blacklisting page. This is the duration of time in which the users are allowed to attempt to authenticate. Although the site security policy may dictate a different value for this field, but it is not recommend setting this value to a very high values.
- Both the authentication server and the management station must be configured using either a direct connection to the TOE or from an internal protected network. They (authentication server and the management station) must also be afforded the same physical protection and access control as required for the TOE.
- Administrators should be aware that URL pattern matching for blocking traffic does not take into account the possibility of non-standard URL encoding schemes (%-escapes, Unicode, or UTF-8, for example). For this reason, administrators may wish to consider firewall rules that will match and block URL encoding schemes. The sponsor agreed to provide information about this in their online user guidance.

The validators consider the configuration rules and restrictions for the evaluated configuration to be reasonable and appropriate for the operational environments to which this product is targeted. Some of the product's capabilities are not included in the evaluated TOE, but the set of capabilities included in the TOE represents a product useful in real-world environments.

9 Flaw Remediation Procedures

CyberGuard's flaw remediation process provides for prompt distribution of software changes in response to discovered flaws in security and other critical product functionality. A security reporting contact e-mail address is provided to all CyberGuard customers, and guarantees a 10-day response time for analyzing the report and determining the severity of the flaw (if verified). For a verified flaw, a repair is guaranteed within 30 days. CyberGuard regularly reviews security-relevant mailing lists and the MITRE Common Vulnerabilities and Exposures (CVE) database for flaw reports that might be relevant to the CyberGuard product line. In the 7 years prior to evaluation completion, the flaw remediation process has been used 238 times to distribute patches to the predecessors of the evaluated product, none of which represented exploitable security flaws. Six (6) of those patches have been issued since the release of the evaluated product, As of October 20, 2005, there are no vulnerabilities in the CVE database that are applicable to the evaluated product or its direct predecessors[3], and no other reporting mechanisms have identified any critical security flaws.

[3] Notes that the URL pattern matching issue described above is in the CVE database as item CVE-2003-0106, but is currently in "candidate" status.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

CygnaCom Solutions has determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 augmented by ALC_FLR.3. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in September 2005.

11 Validator Comments

The validators were favorably impressed with the IT infrastructure the vendor had put in place to support the software development and flaw remediation process. Information about test results, defect tracking, software changes and configuration management were integrated in a way that lends confidence in the ability to detect, manage and eliminate bugs and security flaws. This product information database is readily accessible for querying and updates through a simple web-based interface that provides controlled access to development personnel in various roles. Product information is maintained through this database interface for the full CyberGuard product line, not just for the evaluated product.

As witnessed during testing, the management interface is straightforward and simple, permitting administrators to manage security rules pertaining to packet filtering, the internal authenticator database, and other management functionality easily.

The evaluated configuration is a useful product – a traffic filter firewall and an application proxy – and meets the requirements identified in the Security Target. The product contains very much more functionality than was covered by the evaluation, including network support services such as DHCP, DNS, and NTP, and significant security protocols such as IKE/IPSec VPN functionality. In addition, other types of application proxies are supported by the product beyond the evaluated configuration, including (but not limited to) NNTP, LDAP and a generalized TCP circuit proxy. The omission of remote administration does make for a product that is more challenging to administer (a dedicated administrative workstation, physically connected to the firewall system, is required for the evaluated TOE), but it does not impact the overall security.

Note that remote administration and other non-evaluated protocols were left out of the evaluated product to simplify the evaluation process. During the evaluation, no evidence was found that pointed to any specific security vulnerabilities associated with those features, but as they were not evaluated, and not covered by any claims in the Security Target, no further conclusions can be drawn.

12 Security Target

CyberGuard Firewall/VPN Version 6.2.1, ST revision 1.3, September 30, 2005

13 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated January 2004, Version 2.2.

[7] Final Evaluation Technical Report for a Target of Evaluation CyberGuard Firewall/VPN Version 6.2.1, Volume 1: Security Target Evaluation, Version 1.3, June 1, 2005

[8] Final Evaluation Technical Report for a Target of Evaluation CyberGuard Firewall/VPN Version 6.2.1, Volume 2: Evaluation of the TOE, Version 0.0.03, June 1, 2005

[9] Evaluation Team Plan for On-Site Audit and Testing of CyberGuard Firewall/VPN Version 6.2.1, Version 1.0, June 02, 2005

[10] CyberGuard Firewall/VPN Version 6.2.1, ST revision 1.3, September 30, 2005

[11] Common Criteria Evaluation and Validation Scheme for IT Security, *Guidance to Validators of IT Security Evaluations*. Scheme Publication # 3, Version 1.0, January 2002.