National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

TechGuard Security PoliWall-CCF v. 2.01.01

Report Number: CCEVS-VR-VID10346-2011
Version 2.0
March 23, 2011

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6740

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is TechGuard Security PoliWall-CCF v. 2.01.01. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in February 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 4 (EAL4) augmented with ALC_FLR.1 (Flaw reporting procedures) and ASE_TSS.2 (TOE summary specification with architectural design summary). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (http://www.niap-ccevs.org/).

The Security Target (ST) defines the Information Technology (IT) security requirements for the TechGuard Security PoliWall. TechGuard Security PoliWall is a network boundary device that rapidly determines the country of origin (category) for all incoming packets using HIPPIE™ (High-speed Internet Protocol Packet Inspection Engine) technology. Packets are filtered according to customer-defined policies, PCELs, and exception lists that are bound to rule groups for specific network addresses and protocols. PoliWall also provides Administrators with the ability to create maps by specifying one or more countries that should be allowed and customize their workspace via a graphical user interface.

PoliWall performs the following:

- Protects networks by utilizing HIPPIE country/IP address maps and applying filters to the network's traffic
- Is an administrative-based appliance that allows for four distinct roles: Security Administrator, Audit Administrator, Cryptographic Administrator and Read-Only.
- Provides administrators the ability to create filtering policies by specifying one or more countries that should be allowed
- Allows Administrators to specify additional allow/deny rules for IP networks or addresses with as much granularity as desired across the entire IP address space
- Allows Administrators to specify large allow/deny lists (PCELs) that can contain up to 20 million unique IP addresses. These PCELs are created outside of the TOE and then manually updated onto the TOE. The TOE can then receive updates to these PCELs from the Auto-Update Server.

2 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product	TechGuard Security PoliWall-CCF v. 2.01.01
Sponsor & Developer	TechGuard Security, Chesterfield, MO
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	February 2011

CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL4 Augmented ALC_FLR.2 and ASE_TSS.2
Description	The TOE is the PoliWall appliance, which is a security hardware product developed by TechGuard Security as a Network Boundary Device.
Disclaimer	The information contained in this Validation Report is not an endorsement of the PoliWall product by any agency of the U.S. Government, and no warranty of the product is either expressed or implied.
PP	None.
Evaluation Personnel	Emmanuel Apau Christopher Gugel Arthur Leung John Schroeder Jeremy Sestok Amit Sharma
Validation Body	NIAP CCEVS

3 Identification

The product was evaluated is TechGuard Security PoliWall-CCF v. 2.01.01 on the 10 Gigabit, 1 Gigabit, 50 Megabit, and 10 Megabit hardware models.

4 Security Policy

4.1 Security Audit

4.1.1 Audit Logs

Included in the TOE is a Comprehensive Logging Utility that maintains large rotating log histories indexed for quick access and handles large sets of information that are available for analysis. The TOE provides the following logs that are indexed for quick access and searching:

- **Command Logs** - System commands executed by PoliWall administrators.
- **IPv4 Packet Logs** - Data for all dropped IPv4 packets by source IP, destination IP, protocol, cause and country.

- **IPv6 Packet Logs** - Data for all dropped IPv6 packets by source IP, destination IP, protocol, cause and country.
- **Message Logs** - Shows system information, warning and error messages.

These logs are maintained on the TOE as the following: Command Log Database, IPv4 Packet Log Database, IPv6 Packet Log Database, and Message Log Database.

The TOE records the (1) date and time of the event, (2) type of event, (3) subject identity (if applicable), and the outcome of the event (success or failure) within each audit record.

All log configurations and modifications take effect immediately and will persist when the box is rebooted if the running configuration is saved. However, the System Log Server is not included in the evaluated configuration. The TOE has the ability to associate the logs/audit data with the Administrator who initiated the audit event(s).

The following rules apply to data pertaining to or extracted from the audit trail:

- All Administrators have the ability to read data from the audit trail, with the exception of those prohibited from reading such data. That data must be presented in an interpretable fashion for the Administrator(s) viewing it.
- Searching and sorting of the audit data is permitted based on user identity and a range of one or more or both of dates and times.
- Audit log data should be protected against unauthorized deletion (the Audit Administrator is the only Administrator allowed to delete records) and/or modifications to the records contained in the audit trail (no Administrator is authorized to make modifications to audit records).
- If the audit trail has exceeded its threshold, an alert will be sent to the Security Administrator.
- If the audit trail's threshold has been reached and is full, the oldest stored audit records will be overwritten. Once this occurs a message will be sent to the remote management console notifying of such an occurrence.

4.1.2 Security Alarms

The TOE is able to generate security alarms when a potential security violation occurs, thus notifying the Security Administrator of such an event. The Security Administrator will be immediately notified of this alarm during their remote session. Some of these alarms occur when there are severe events that will affect the TOE and require it to enter Maintenance Mode. These specific alarms are failure of a self-test and a log filling up. The Security Administrator may configure the PoliWall to not enter maintenance mode when logs are full and instead automatically overwrite the oldest log records. Rules will be applied by the Security Administrator on how these audited events will be monitored, which will include:

- Excessive number of authentication failures by an Administrator has resulted in an account being locked out. This alarm will never cause the PoliWall to enter Maintenance Mode.

- An audit log (IPv4 Packet Log, IPv6 Packet Log, or Message Log) has reached the warning level threshold. This will never cause the PoliWall to enter Maintenance Mode.
- An audit log (IPv4 Packet Log, IPv6 Packet Log, or Command Log) has become full. This will cause the PoliWall to enter Maintenance Mode if configured to do so by the Security Administrator.
- A Self-Test has failed. This will always cause the PoliWall to enter Maintenance Mode.
- An Automatic Update failed. This will never cause the PoliWall to enter Maintenance Mode.

4.2 Cryptographic Support

The TOE utilizes cryptography across several different areas:

- Between the TOE and web interfaces
- Auto Updating (Country Database)
- IPsec
- NTP
- SNMP
- Communications with the Remote Management Console (RMC) Server
- Communications with the REACT Servers

It is essential that the TOE compensate for the generation, destruction, and encryption of keys that are produced. The following chart illustrates how each entity handles those keys:

Purpose	Usage	Algorithm	Size	Standard
Key Generation	[redacted]	RSA	2048	RFC 2313
Key Destruction	[redacted]	Key Zeroization	[redacted]	No Standard.
Crypto Operation (1)	Encryption/decryption	AES	256	RFC 3268
Crypto Operation (2)	Cryptographic Hashing	SHA-1	160	RFC 3174
Crypto Operation (3)	Cryptographic Hashing	SHA-256	256	FIPS 180-2

SHA-256 is the preferred hashing mechanism and is used whenever possible for the TOE. However some protocols supported by the TOE (SNMP and IPSEC) require SHA-1 for hashing instead of SHA-256.

OpenSSL-FIPS version 1.2 is used by the TOE. The FIPS compliance is currently vendor asserted, rather than FIPS asserted.

4.3 Identification & Authentication

In order to authenticate to the TOE and perform TOE processes, Administrators must either enter (1) their username and password or (2) their username, password, and client certificate which will be defined by the Security Administrator. Upon attempting to authenticate the TOE, Administrators will have anywhere between 2 and 25 attempts at successfully logging in. The amount of attempts is configuration by the Security Administrator, and when that limit is reached, the Administrator will be locked out from logging in and subsequently performing TOE operations. There are two ways that an account can be unlocked – either manually by the Security Administrator or automatically when the specified time from the account locking has elapsed. If authentication and identification has been successfully completed, the Administrator's attributes associated with the role will be displayed/granted.

4.3.1 Password Policy

The TOE comes preconfigured with mechanisms for creating a password and strictly enforces them. The mechanisms put in place for password creation are:

- must be an 8 character minimum
- must be at least 3 of the following 4 metrics: uppercase characters, lowercase characters, numbers, symbol
- is not one of the previous # used passwords, where # is definable by the Security Administrator
- has a maximum life of # days, where # is definable by the Security Administrator
- has a minimum life of # days, where # is definable by the Security Administrator
- has a maximum authentication attempts of # before a Administrator is locked out, where # is definable by the Security Administrator
- has a lockout duration of # minutes, where # is definable by the Security Administrator
- has a maximum inactive session of # minutes before re-authentication is required, where # is definable by the Security Administrator
- has a minimum session of # minutes before re-authentication is required, where # is definable by the Security Administrator

The only action this is permitted to be performed without authenticating to the TOE is ICMP (ping). This is wholly up to the discretion of the Security Administrator whether or not they will allow this action to be enabled or disabled without authenticating to the TOE; all other TOE actions require Administrators to properly authenticate to the TOE.

The TOE allows for the association of a Administrator's security attributes to be attributed to the Administrator acting on their behalf; the rules governing this association of attributes and the changing of those attributes will be strictly enforced by the Security Administrator.

4.4 Security Management

4.4.1 User/Role Association

The User/Role association information, i.e. the functions that system administrators are allowed to perform, is stored in an Object that is created for each authenticated session. The TOE tracks these sessions internally in the PoliWall process and they are associated with cookies that are set on the client.

The TOE has several roles and has the following rules associated with them:

1. Security Administrator – has the ability to perform all functions except the ability to manage cryptography and delete audit logs
2. Audit Administrator – has the ability to delete audit records
3. Cryptographic Administrator – Manages all cryptographic functionality
4. Read-Only - has the ability to read configuration information but may not make any changes to the TOE

It is the TOE's responsibility to ensure that the following conditions are satisfied:

- All roles shall be able to access the TOE remotely; Security Administrator, Audit Administrator, and Cryptographic Administrator will be able to administer the TOE, while Read-Only will only be able to view the configuration of the TOE.
- All three Administrator roles are distinct; that is, there shall be no overlap of operations performed by each default role, with the following exceptions:
    - All roles, including Read-Only, can review the audit trail;
    - The three administrator roles can invoke the self-tests and
    - The three administrator roles can accept alarms/acknowledgements

Additionally, all administrators can disable/enable security alarms, perform self-tests, have the ability to read audit records, and can accept notifications.

The TOE can revoke and enforce rules of the security attributes associated with an Administrator's information flow policy rule set and services available to unauthenticated Administrators.

4.4.2 Flow Control

The TOE enforces the Unauthenticated Information Flow Control SFP to restrict the ability to change, default, and query or modify the security attributes to the Security Administrator. The Unauthenticated Information Flow Control SFP must also provide restrictive values for security attributes to be used to enforce the SFP (i.e. deny all network traffic). The Security Administrator is the only Administrator with the ability to specify alternative initial values to override the aforementioned default values when an object/information is being created.

4.4.3 Quotas

Quotas for TOE data on transport-layer connections can only be determined by the Security Administrator. If the quota has been reached, all packets above and beyond the quota will be dropped. Quotas can also be placed on controlled connection-oriented resources by the Security Administrator. If the quota has been reached for these resources, the packets will be dropped.

4.5 User Data Protection

The TOE provides for enforcement of the Unauthenticated Information Flow SFP based on:

- Source Subject
- Destination Subject
- Information
- Operations

Stateful packet inspection should occur when it is received unless associated with an established session.

The information flow will be authorized when a flow has already been established and no changes to any policies have been made. The information flow will be rejected if the request for access or services where the presumed source ID of the information received by the TOE is not included in the set of source identifiers for the source subject. Any previous information content of a resource should be made unavailable upon the allocation or reallocation of the resource from the list of objects.

4.6 Trusted Path

The TOE comes pre-installed with a self-signed SSL certificate that is used to establish a secure encrypted session to the PoliWall configuration application. The appliance includes a generic server certificate. The pre-installed certificate will be overwritten after successfully configuring and installing a new server certificate. An assurance is made that a communication channel between the TOE and another IT product that provides assured identification and protection will be established. This communication will be for the purpose of updating the system time, category code database, PCELs, connection to Remote Management Console (RMC) Server, and establishment of connections from REACT Servers.

The TOE's client CA certificate specifies the certificate authority required to issue client certificates which identify Administrators connecting to the TOE. A Certificate Revocation List may be uploaded to the TOE to prevent revoked certificates issued by the client CA certificate from establishing connections to the TOE.

The TOE will provide a trusted communications path for remote Administrators to authenticate to.

4.7 Resource Utilization

A secure, stable state must be maintained when failures to the following resources occur:

- Auto Update Daemon
- PoliWall Process
- Auditing Modules
    - Msglogd, syslogd, pktlogd, pktlog6d

In the event of the failures of the Auto Update module, PoliWall process module (remote administration functions and access control), and auditing modules (msglogd, syslogd, pktlogd, pktlog6d), the TOE will maintain and operate in a secure state until these failed subsystem have come back online. Information flow control will remain in operation during this time.

Unauthenticated data to be processed by the TOE is subjected to prioritization based on QoS and quotas. Once the data has priority, an operation is made on it based on the unauthenticated information flow control.

When the total amount of traffic reaches the configured bandwidth limit, traffic from the high QoS countries will be allowed through the PoliWall before traffic from other countries.

4.8 TOE Access

Access to the TOE is controlled by the Administrator's IP address. The TOE can terminate sessions after a given amount of time of inactivity has occurred (which is predetermined by the Security Administrator). Before a session begins, a warning will be displayed alerting the Administrator that unauthorized access to the TOE is prohibited. Denials of access to the TOE can be made according to IP address, time, and day.

4.9 Protection of the TSF

The TOE will maintain a secure state even when failures to the Auto Update, PoliWall process, msglogd, syslogd, pktlogd, and pktlog6d occur. The TOE will also maintain and provide reliable timestamps to Administrators. In order to maintain the integrity of the TOE, the TSF will run a suite of self-tests during initial start-up, periodically during normal operation, and at the request of the authorized Administrator in order to demonstrate the correct operation of the TOE. All authorized Administrators will be able to verify the integrity of TOE data and stored TOE executable code. All authorized Administrators will be able to verify the integrity of TOE data and stored TOE executable code.

5 Assumptions

5.1 Threats to Security

Table 3 summarizes the threats that the evaluated product addresses.

Table 3 – Threats

A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
An administrator user may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.

An administrator's intentions may become malicious resulting in user of TSF data being compromised.
A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a User's action.
A malicious user or process may cause key, data, or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanism and the data protected by those mechanisms.
Unintentional or intentional errors in requirements speciation or design of the TOE may occur leading to flaws that may be exploited by a malicious user or program.
Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.
A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
An unauthenticated user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.
Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered.
A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).
A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.
An entity may misrepresent itself as the TOE to obtain authentication data.
A user may gain unauthorized access to an unattended session.
A user may gain access to services (by sending data through or to the TOE) for which they are not authorized according to the TOE security policy.
The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.
When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

5.2 Physical Assumptions

Table 4 – Physical Assumptions

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

5.3 Logical Assumptions

Table 5 – Logical Assumptions

Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

5.4 Organizational Security Policies

Table 6 – Organizational Security Policies

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
The authorized users of the TOE shall be held accountable for their actions within the TOE.
Administrators shall be able to administer the TOE remotely through protected communications channels.
The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signature operations.
The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the TechGuard Security PoliWall-CCF v. 2.01.01 product that is a hardware network boundary device installed in-line within a network.

6.1 Physical Boundary

The following are the specifications for the TechGuard PoliWall-CCF 10 Gigabit hardware:

- Processor: 2x Intel Xeon E5620 @ 2.4 GHz
- Memory: 48 GB standard
- Storage: 8x Internal 2.5” HDD 300 GB
- Cryptographic Protocols: Supports, AES 256, RSA 2048, SHA1, SHA256
- System Control and Indicator Power: LED x1, HDD LED x2 on each HDD, Power on/off switch x1, LED x2 on each RJ-45 receptacle
- Number of device interfaces: 2 CX4 ports, 4 Ethernet ports (1 used, 3 unused)
- Ethernet 1, 2: 10GbE with CX4 connector or Short-Range Fiber connector
- Ethernet 3, 4, 5, 6: 10/100/1000 (GbE) with RJ-45 connector
- System Console Port: COM port x 2 (1 x Rear), RS-232 & DB-9 receptacles, USB 2.0 x 4 (2 x Rear)
- Power Supply: 2x 870 W hot swap power supply

The following are the specifications for the TechGuard PoliWall-CCF 1 Gigabit hardware:

- Processor: Intel Xeon X3430 @ 2.4 GHz
- Memory: 16 GB standard
- Storage: Internal 3.5” HDD 160 GB
- Cryptographic Protocols: Supports, AES 256, RSA 2048, SHA1, SHA256
- System Control and Indicator Power: LED x1, HDD LED, Power on/off switch x1, LED x2 on each RJ-45 receptacle
- Number of device interfaces: 4 Ethernet ports (3 used, 1 unused)
- Ethernet 1, 2: 10/100/1000 (GbE) with RJ-45 connector or Short-Range Fiber connector
- Ethernet 3, 4: 10/100/1000 (GbE) with RJ-45 connector

- System Console Port: COM port x 2 (1 x Rear), RS-232 & DB-9 receptacles, USB 2.0 x 4 (2 x Rear)
- Power Supply: 250 W power supply

The following are the specifications for the TechGuard PoliWall-CCF 10 Megabit and 50 Megabit hardware:

- Processor: Intel Atom D510 @ 1.66 GHz
- Memory: 4 GB standard
- Storage: Internal 2.5" HDD 160 GB
- Cryptographic Protocols: Supports, AES 256, RSA 2048, SHA1, SHA256
- System Control and Indicator Power: LED x1, HDD LED x2, Power on/off switch x1, LED x2 on each RJ-45 receptacle
- Number of device interfaces: 4 Ethernet ports (3 used, 1 unused)
- Ethernet 1, 2, 3, 4: 10/100/1000 (GbE) with RJ-45 connector
- System Console Port: COM port (1 x Rear), RS-232 & DB-9 receptacles, USB 2.0 x 2 (2 x Rear), PS/2 Ports (2 x Rear)
- Power Supply: 200 W power supply

6.2 Operational Environment Components

6.2.1 NTP Server

The Network Time Protocol Server is used to assure accurate synchronization of computer clock times in a network of computers. It also synchronizes the PoliWall's clock with the other TOE-associated servers. The TOE's connection to this Operational Environment component can be optionally configured.

6.2.2 Auto Update Module

The Auto Update Module downloads the latest IP/Country Allocation information and Category Codes daily to the TOE for filtering of network traffic. This will also be used to download updates to the PCELs daily to the TOE for updates.

6.2.3 SNMP Server

A client may poll the TOE via the Simple Network Management Protocol (SNMP) Server to gather statistics for the traffic flowing through the TOE. Also, the TOE may be configured to send SNMP traps out to a specified external server when certain events occur, such as raising an alert to the Remote Management Console. The TOE's connection to this Operational Environment component can be optionally configured.

6.2.4 Remote Management Console (RMC) Server

The TOE may connect up to the Remote Management Console (RMC) Server to get configuration updates, such as new policies, resource group definitions, or exceptions. A user may log into the RMC Server and schedule changes to occur on many PoliWalls from one centralized server instead of having to log on to each PoliWall. Note that the RMC Server is excluded from the evaluation, but the trusted channel to the RMC is included. The TOE's connection to this Operational Environment component can be optionally configured.

6.2.5 REACT Server

A REACT Server may connect up to the PoliWall, authenticate, and then instruct the PoliWall to automatically block traffic from specific IP addresses for a period of time. These REACT Servers may be integrated into IDS units and provide fully automated blocking capabilities. An Administrator must configure the REACT Servers before the PoliWall will respond to them. The TOE's connection to this Operational Environment component can be optionally configured.

6.3 Excluded from the TOE

6.3.1 External System Log Server

The TOE performs all auditing functions as they are described in the ST. Additionally, the storage provided by the TOE is robust and has several features to allow the Audit Administrator to manage the TOE's auditing capabilities. The evaluated TOE does not include the ability to send audit data to external system log server.

6.3.2 Updating the firmware of the TOE

The TOE is the TechGuard Security PoliWall-CCF ® 2.01.01. Any updates to this firmware may introduce a new attack vector and would no longer be the evaluated TOE. Updates to the firmware were not permitted in the evaluation of the TOE.

6.3.3 Remote Management Console Server

This is a separately purchased product used for management of multiple PoliWalls concurrently. This product was excluded from evaluation, but the interface between itself and the PoliWall was included. This product allows for administrators to identify configuration changes, and then select which PoliWalls should perform those changes.

7 Architectural Information

The TOE's boundary has been defined in Figure 1.

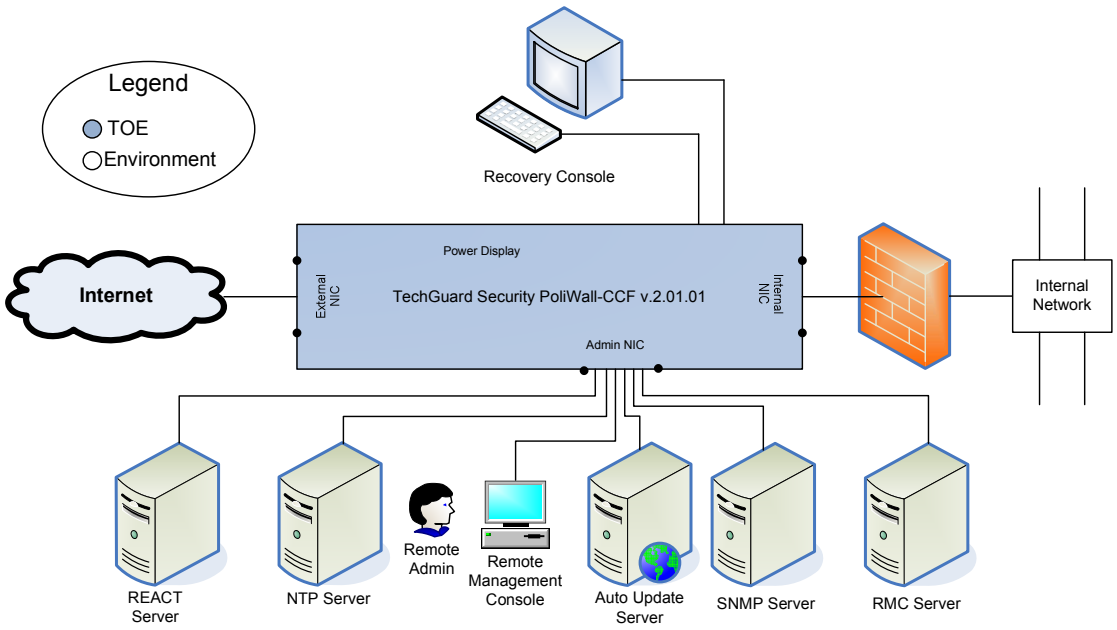

Figure 1 – TOE Boundary for TechGuard Security PoliWall-CCF v. 2.01.01

7.1 TOE Components

7.1.1 PoliWall

PoliWall is a network boundary device that can be rapidly deployed in-line with the network it protects, requiring no changes to an existing network. It uses HIPPIE country maps to filter packets by continent, registry, country, IP range or specific IP addresses. Unlike a traditional firewall, PoliWall is not configured in a NAT or Route mode. Instead, PoliWall is a Layer 2 bridge that filters traffic in-line. Since the device operates at Layer 2 of the OSI model, network IP addresses are not visible or searchable by anyone outside of the network, putting it out of reach of attackers. A transparent bridge reduces the configuration complexity and saves time. In addition to its use in large corporate and government networks, it is ideal for branch offices and smaller networks which may consist of a single WAN connection and a router. The bridge can be configured by an in-house IT team, and shipped to a branch location.

8 TOE Acquisition

The NIAP-certified PoliWall product is acquired via normal sales channels, and physical delivery of the TOE is coordinated with the end customer by TechGuard Security.

The documents provided with the TOE were evaluated to satisfy the customer facing assurance requirements:

- PoliWall-CCF User's Manual Version 2.01.01, January 2011
- PoliWall-CCF Quick Start Guide Version 2.01.01, January 2011

No other documents were provided within the TOE delivery and the evaluation team was able to complete the evaluation using the documents listed above.

9 IT Product Testing

9.1 Functional Testing

9.1.1 Functional Test Methodology

The evaluation team's test approach was to test the security mechanisms of the TechGuard Security PoliWall-CCF v. 2.01.01 by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in the relevant design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Security Architecture (ARC) and the vendor's test plans were used to demonstrate test coverage of all EAL4 augmented with ALC_FLR.2 and ASE_TSS.2requirements for all security relevant TOE external interfaces. TOE external interfaces that will be determined to be security relevant are interfaces that perform any of the following:

The test team's test approach was to test the security mechanisms of PoliWall by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), Low Level Design documents (LLDs), and the vendor's test plans were used to demonstrate test coverage of all *appropriate* EAL4 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that:

- Change the security state of the product,
- Permit an object access or information flow that is regulated by the security policy,
- Are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- Invoke or configure a security mechanism.

EAL4 requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

9.1.2 Functional Results

During the course of the evaluation, the Booz Allen evaluation team reviewed the vendor’s functional testing and determined that all *security relevant* TOE external interfaces were tested and all of the claimed functionality was tested by the vendor. The evaluation team then created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing developed by the evaluators. The

evaluators test suite emphasized on the product's primary functionality, and additional regression testing. Based upon the results of the vendor and evaluator testing; it has been determined that the product functionally operates as described.

9.2 Vulnerability Testing

9.2.1 Vulnerability Test Methodology

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, cve.mitre.org, and nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications

  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. This test was specialized for the following interfaces:

  - Admin Web GUI
  - PoliWall to Third-Party Sources
  - PoliWall to TechGuard Update Server

- Port Scanning

  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Vulnerability Scanner (Nessus)

  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probed a wide range of vulnerabilities that includes but are not limited to the following:

Backdoors	Gain root remotely	RPC
CGI abuses	General	Settings
Denial of Service	Miscellaneous	SMTP Problems
Finger abuses	Netware	SNMP

Firewalls	NIS	Untested
FTP	Port scanners	Useless services
Gain a shell remotely	Remote file access	

- Unauthenticated Access / Directory Traversal Attack

  This test used "URL hacking" to attempt to access protected TOE resources by injecting unexpected input into requests that are sent to the server. This is done using two different approaches to URL exploitation.

  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).
- SQL Injection / Cross Site Scripting Attack / Cross Site Request Forgery

  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were inputted into the various fields and variables and the output was analyzed for inconsistencies.
- Web Server Vulnerability Scanner

  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

File Upload. Interesting File / Seen in logs. Misconfiguration / Default File. Information Disclosure. Injection (XSS/Script/HTML). Remote File Retrieval	Denial of Service. Command Execution / Remote Shell. SQL Injection. Authentication Bypass. Software Identification Remote source inclusion.

- Vulnerability Scanner (Retina)

  This test used the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
  The scanner probed a wide range of vulnerabilities that includes but is not limited to the following:

Accounts Anti-Virus Backdoors CGI Scripts Database Issues	DoS IP Services Registry Remote Access RPC Services	Service Control Spyware Web Services CVE Issues SecurityFocus BID Issues

- Denial of Service – TCP Malformed Packet Flooding

This attack attempted to exercise the stability of the IP stack and its components by sending a large amount of TCP packets and malformed TCP packets in an attempt to overload the application. If successful, the TOE would have crash and not allowed any connections until the TOE was rebooted.

9.2.2 Vulnerability Results

During the vulnerability testing, the evaluation team determined that there were no issues discovered that could affect the security posture of a deployed system.

10 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the TechGuard Security PoliWall-CCF v. 2.01.01 TOE meets the security requirements contained in the Security Target.

The criteria against which the PoliWall TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the TechGuard Security PoliWall-CCF v2.01.01 TOE is EAL4 augmented with ALC_FLR.2 and ASE_TSS.2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in February 2011. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

11 Validator Comments/Recommendations

11.1 Secure Installation and Configuration Documentation

The “PoliWall-CCF User’s Manual Version 2.01.01” defines the recommendations and secure usage directions for the TOE as derived from the evaluation. This guidance can be found within Section 4.7 of that document.

11.2 FIPS 140-2 Validation

The TOE is also going through FIPS 140-2 validation which was not completed before the completion of this Common Criteria evaluation. Therefore, it must be assumed that all cryptography within this Common Criteria evaluation is vendor-asserted.

11.3 Flaw Remediation

TechGuard’s flaw remediation process allows customers to contact TechGuard’s support team via phone (1-877-POLIWALL) or email (support@techguardsecurity.com) regarding suspected security flaws. Once TechGuard has determined that a flaw has been discovered and created a solution to fix the flaw, they will directly contact all customers that reported that flaw. The remainder of the customer base can receive information about

fixed security flaws by registering to TechGuard's support web site (https://support.poliwall.com/) utilizing their registration code that is provided with the purchased product. On the support site, TechGuard posts updates regarding discovered flaws and fixes. The support site also provides a mechanism to allow customers to sign up for notifications when a new flaw and fix is posted to the web site.

12 Security Target

The security target for this product's evaluation is TechGuard Security PoliWall-CCF v. 2.01.01 Security Target, Version 0.6, January 26, 2011.

13 List of Acronyms

Acronym	Definition
ARP	Address Resolution Protocol
CC	Common Criteria
DB	Database
HIPPIE	High-Speed Internet Protocol Packet Inspection Engine
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IPSec	Internet Protocol Security
IT	Information Technology
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
OS	Operating System
PCEL	Pre-Compiled Exception List
PEM	Privacy Enhanced Mail
PSK	Pre-shared Key
RMC	Remote Management Console
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VLAN	Virtual Local Area Network
XML	Extensible Markup Language

14 Terminology

Terminology	Definition
Alarm	A message that is provided to all PoliWall administrators when a condition such as log filling up or excessive invalid logins is reached.
Alert	A SNMP Trap that is sent out when a Country or group of Countries has exceeded the trigger threshold for a Rule Group.
Command Log	System commands executed by PoliWall administrators.
Country Statistics	Tracks the number of allowed and denied packets that are processed by the PoliWall
Default Rule Groups	Serve as generic filtering targets for all ingress or egress network traffic.
Exception Lists	A list of IPv4 or IPv6 addresses or networks that the Administrator will prepare on the PoliWall. An Exception List may be used to allow or deny traffic.
Interfaces	Serve as generic filtering targets for all network traffic either without a VLAN tag or matching a specific 802.1q VLAN tag.
IPv4 Packet Log	Data for all dropped IPv4 packets by source IP, destination IP, protocol, cause and country

IPv6 Packet Log	Data for all dropped IPv6 packets by source IP, destination IP, protocol, cause and country
Overrides	Additional country-blocking restrictions applied to a specific rule group. These countries will continue to e blocked on the resource group/interface even if the Policy for that rule group is changed to allow traffic for that country.
Policy	A grouping of a Category (Country) Map, PCELs, and Exception Lists that identify which external IP addresses are to be allowed and which are to be denied. When a Policy is bound to a Rule Group, the it is applied to all rules for the Rule Group.
PreCompiled Exception List (PCEL)	A list of IPv4 and/or IPv6 addresses that is prepared off of the TOE and then uploaded to the TOE. A PCEL may be used to allow (whitelist) or deny (blacklist) traffic. PCELs may contain up to 20 million unique IP addresses.
Pre-Shared Key	An agreed upon that secret that is used to authenticate both ends of a connection.
Remote Management Console	The user GUI that is accessed to manage the PoliWall. This is a web site that runs on the PoliWall which the administrators access via an HTTPS connection.
Remote Management Console Server	A separately purchased product used for management of multiple PoliWalls. This product is excluded from evaluation, but the interface between itself and the PoliWall is included. This product allows for administrators to identify configuration changes, and then select which PoliWalls should perform those changes.
Rule Groups	Identify collections of internal network resources that are to be protected. For ingress rule groups, these network resources will be services that are being offered to the outside world. For egress rule groups, these network resources will be computers that are connecting out to the outside world.
System Log	System information, warning and error messages
VPN Destination Network	The IP address (or range) of the actual network to which a VPN connection is made through the Peer Address.
VPN Peer Address	IP address of the VPN endpoint

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. TechGuard Security PoliWall-CCF v. 2.01.01 Security Target, Version 0.6, January 26, 2011
6. Evaluation Technical Report for a Target of Evaluation "TechGuard Security PoliWall v. 2.01.01," Version 3.0, February 7, 2011.