National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

CloudShield
CS-2000 version 3.0.3

Report Number: CCEVS-VR-VID10321-2012

Dated: 2012-05-08

Version: 1.0

National Institute of Standards and Technology	**National Security Agency**
Information Technology Laboratory	**Information Assurance Directorate**
100 Bureau Drive	**9800 Savage Road STE 6940**
Gaithersburg, MD 20899	**Fort George G. Meade, MD 20755-6940**

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin, CISSP
The Aerospace Corporation
El Segundo, California

Michelle Brinkmeyer
National Security Agency/CCEVS
Fort Meade, Maryland

Evaluation Team

Trang Huynh and Jeremy Powell
atsec Information Security Corporation
Austin, Texas

Andreas Siegert and Rasma M. Araby
atsec Information Security GmbH
Munich, Germany

Table of Contents

1. EXECUTIVE SUMMARY

The Target of Evaluation (TOE) is the Cloudshield CS-2000 appliances with CPOS (CloudShield Packet Operating System) 3.0.3. The evaluation was performed by the atsec information security corporation, and was completed during April 2012. atsec information security corporation is an approved National Information Assurance Partnership (NIAP) Common Criteria Testing Laboratory (CCTL). 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 determined the product to be Common Criteria (CC) Version 3.1 Revision 3, Part 2 conformant, Part 3 conformant, and to meet the requirements of Evaluation Assurance Level 4 (EAL4) augmented by ALC_FLR.3. 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/).

This report documents the NIAP validators' assessment of the evaluation of the Cloudshield CS-2000 with CPOS (CloudShield Packet Operating System) 3.0.3. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the information technology (IT) product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The CS-2000 is a multi-function solution appliance without any pre-configured network capability set programmed into the system. CloudShield allows network operators (administrators) to define policies (in the form of rule sets) that instruct the TOE to analyze, make decisions, and take action on packet data received from the network. Possible actions that the TOE can be configured to execute include inspection of any packet data, capture of portions or all packet data, modification of packet data, insertion of new packets, drop or discard of packets, and algorithm processing. The heuristics of these actions are defined by applications (rule sets) written in a high-level data plane programming language, called RAVE, designed to make the development of packet processing policies and applications easier. The RAVE programming language is the interface for administrators to define the rules used to analyze and process packets; the RAVE language is translated to RAVE instructions by the Interactive Development Environment (part of the operating environment), and these programs are then loaded and executed on the CloudShield platform. The evaluation covers only programs written using the RAVE programming interface; the PacketC environment also supported within the development environment is outside of the scope of this evaluation.

The validation team agrees that the CCTL presented appropriate rationale to support the Results of Evaluation presented in Section 4, and the Conclusions presented in Section 5 of the Evaluation Technical Report (ETR). The validation team therefore concludes that the evaluation and the Pass result for the CloudShield CS-2000 version 3.0.3 is complete and correct.

The technical information included in this report was largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the evaluation team. The CloudShield CS-2000 with CPOS 3.0.3 Security Target version 1.0, dated 25 January 2012 identifies the specific version and builds of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the CloudShield appliance by any agency of the US Government and no warranty of the product is either expressed or implied.

2. IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a National Security Agency (NSA) 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 Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation granted by the National Institute of Standards and Technology (NIST).

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 and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's 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 Protection Profile (PP) to which the product is conformant;
- 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	CloudShield CS-2000 with CPOS 3.0.3 on the following hardware: • 1 CS-2000 Chassis Enclosure • 1 Application Server Module (either ASM or ASM2) • 1 Power Supply Modules • 1 Fan Tray Unit • and 1 or 2 of the following DPPM models: ◦ DPPM-500: Deep Packet Processing Module for GbE ◦ DPPM-510: Deep Packet Processing Module for GbE (includes high-speed interconnect support) ◦ DPPM-600: Deep Packet Processing Module for Packet over SONET and SDH (POS) ◦ DPPM-800: Deep Packet Processing Module for 10G Ethernet when configured in accordance with the CloudShield document "*CloudShield Secure Setup for Common Criteria Release 3.0.3*", version 2012_01_13_00.
Completion Date	March 2012
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009
CEM	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009
Protection Profile	None.
Security Target	*CloudShield CS-2000 with CPOS 3.0.3 Security Target Version 1.0, 2012-01-25*
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation* *Cloudshield CS-2000 with CPOS 3.0.3* *ETR Version 1.1 as of 2012-03-27*
Conformance Result	CC V3.1, Part 2 conformant, Part 3 conformant, EAL 4 augmented by ALC_FLR.3
Sponsor	CloudShield Technologies, Inc.
Developer	CloudShield Technologies, Inc.
Evaluators / CCTL	Trang Huynh, Jeremy Powell, Andreas Siegert, Rasma M. Araby **atsec information security corporation**
Validators	Common Criteria Evaluation and Validation Scheme Daniel Faigin, CISSP (Senior) **The Aerospace Corporation, El Segundo, California** Michelle Brinkmeyer (Lead) **NSA, Ft. Meade, Maryland** Mario Tinto, of The Aerospace Corporation, Columbia, Maryland assisted in the final review of the validation material.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Parity product by any agency of the U.S. Government, and no warranty of the system access control product is either expressed or implied.

3. SCOPE OF EVALUATION

This section details the scope of the evaluation and describes the logical and physical boundaries of the TOE. It also clarifies any exclusions from the evaluation scope.

3.1. Summary Product Description

Note: The following paragraphs are a summary of the more detailed material presented in Chapter 6, "ARCHITECTURAL INFORMATION". They are presented here to provide sufficient context for the policy discussion.

CloudShield is a multi-function solution appliance without any pre-configured network capability set programmed into the system. CloudShield allows network operators (administrators) to define policies (in the form of rule sets written in the RAVE programming language) that instruct the TOE to analyze, make decisions, and take action on packet data received from the network. Possible actions that the TOE can be configured to execute include inspection of any packet data, capture of portions or all packet data, modification of packet data, insertion of new packets, drop or discard of packets, and algorithm processing. These actions are defined by applications (rule sets) written in a high-level data plane programming language, called RAVE, designed to make the development of packet processing policies and applications easier. RAVE is the actual name of the programming language and is not an acronym. Administrators use the PacketWorks IDE (Integrated Development Environment) to develop RAVE applications (rule sets). The development of RAVE applications are performed on a separate personal computer executing the PacketWorks IDE and subsequently securely uploaded to the TOE through the management interfaces provided by the TOE. The PacketWorks IDE is not considered to be part of the TOE.[1] The flexibility of the RAVE programming language, including the ability to make decisions and actions on network traffic, permits the implementation of different capabilities to control or alter traffic flow, including the stateful filtering of packets.

The physical computer blade that carries out RAVE applications on packet data is called the **Deep Packet Processing Module** (DPPM). The DPPM is physically inserted into a CS-2000 chassis enclosure. It includes its own processors, memory, and physical interfaces and implements a RAVE execution engine to carry out the logic defined by a loaded RAVE application. There can be one or two instances of the DPPM blade in the evaluated CS-2000 configuration; each DPPM can be configured to independently execute a different RAVE application.

The physical computer blade that provides management access to the system is called the **Application Server Module** (ASM). The ASM is physically plugged into the same chassis enclosure as the DPPM blades. The ASM includes its own processor, memory, disk storage, and physical interfaces. There is a single instance of the ASM in the evaluated CS-2000 configuration used to manage DPPM blades within the same CS-2000 chassis. The ASM provides a serial port for

[1] This is similar to the approach taken in an operating system, where the compilers and development environment are not covered by the evaluation, but the programs are examined in their programming language, and the eventual executable images tested.

console access (used only during installation and setup) and its own network interfaces used to access the following CS-2000 management applications:

- **Web Management Interface (WMI)**. This is a graphical administrative interface used to manage TOE functions (for example, read audit trail data from the audit records, import rule sets that permit or deny information flows, and modify user attribute values). Administrators access the WMI over a TLS-protected HTTP channel using a web browser application in the operational environment.

- **Command Line Interface (CLI)**. This is a text-based administrative interface used to manage TOE functions (for example, read audit trail data from the audit records, import rule sets that permit or deny information flows, and modify user attribute values). Administrators access the CLI over an SSH interface using a terminal application in the operational environment. Telnet access, as well as the serial console access, to the CLI are disabled in the evaluated configuration.

- **Simple Network Management Protocol (SNMP) Interface**. This interface provides read-only access to appliance health, system statistics, and general state information. Users access the SNMP interface using an industry-standard server management application in the operational environment.

- **Dynamic Interfaces**. These interfaces provide two forms of dynamic data update mechanisms (specifically, modify attribute values of rule sets that permit or deny information flows and retrieve TOE statistics). One is called GODYN ("go dynamic"). This is a text-based interface, accessed through the CLI, with the application having to parse text commands. A newer interface is called Java-Script Object Notation (JSON, also known as GODYN2). The JSON interface is a programmatic interface with structured data. JSON can also be accessed directly (i.e. without using the CLI) via an SSL-protected network channel.

- **MySQL administrative interface**. This interface is not used in the evaluated configuration.

The CS-2000 2RU chassis supports dual, hot-swappable AC (Alternate Current) or DC (Direct Current) power supply modules and a redundant fan tray assembly accessible from the rear of the chassis. The ASM and one or two DPPM modules are physically inserted into the front of the chassis. All of these components are included in the evaluated CS-2000 configuration.

The TOE components and their relationships with each other are depicted in **Error! Reference source not found.**. Blades communicate with each other using an internal Gigabit Ethernet (GbE) network interface provided by the chassis that is not otherwise accessible.

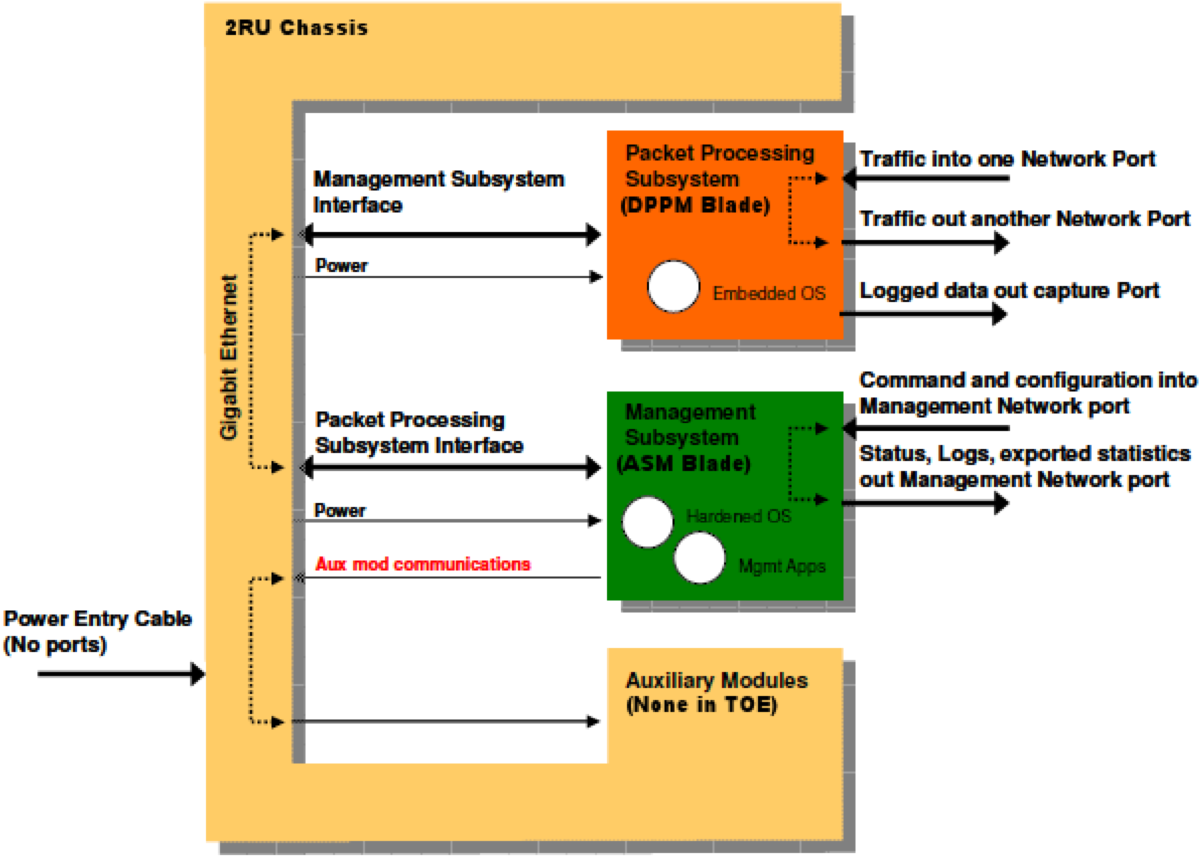
2RU Chassis
Gigabit Ethernet
Management Subsystem Interface
Power
Packet Processing Subsystem (DPPM Blade)
Embedded OS
Traffic into one Network Port
Traffic out another Network Port
Logged data out capture Port
Packet Processing Subsystem Interface
Power
Aux mod communications
Management Subsystem (ASM Blade)
Hardened OS
Mgmt Apps
Command and configuration into Management Network port
Status, Logs, exported statistics out Management Network port
Power Entry Cable (No ports)
Auxiliary Modules (None in TOE)

Figure 1. TOE Structure

3.2. Physical Scope

All CS-2000 installations include the following components:

- CS-2000 Chassis Enclosure.
- Application Server Module (ASM). The evaluation covered both the ASM and ASM2 modules. ASM2 provides a newer CPU and newer hardware components; the software executed by both is the same).
- Power Supply Modules.
- Fan Tray Unit.

All CS-2000 installations include at least one Deep Packet Processing Module (DPPM). The DPPMs supported by the TOE are:

- DPPM-500: Deep Packet Processing Module for Gigabit Ethernet (GbE).

- DPPM-510: Deep Packet Processing Module for GbE (includes high-speed interconnect support).
- DPPM-600: Deep Packet Processing Module for Packet over SONET and SDH (POS).
- DPPM-800: Deep Packet Processing Module for 10G Ethernet.

The TOE also includes the following user guidance documentation, which are provided with the TOE:

- *CloudShield CS-2000 Series Documentation Guide Release 3.0.3*, 2012-03-09
- *CloudShield Installation, and Hardware Reference, And Ordering Guide: CS2000 Series Release 3.0.3*, 2012-03-09
- *CloudShield CS-2000 Quick Start Guide Release 3.0.3*, 2012-03-09
- *CloudShield System Software Release Notes Release 3.0.3*, 2010-08-11
- *CloudShield CS-2000 Command Line Interface Reference Guide Release 3.0.3*, 2012-03-09
- *CloudShield CS-2000 Web management Interface User Guide Series Release 3.0.3*, 2012-03-09
- *CloudShield Application Integration User Guide 3.0.3*, 2012-03-09
- *Secure Setup For Common Criteria Guide Release 3.0.3*, 2012-01-13

With the exception of the *Secure Setup for Common Criteria Guide* and the *System Software Release Notes*, the user guidance is available on CD shipped along with the TOE system.

The Secure Setup For Common Criteria Guide is the authoritative documentation that must be used in order to place the TOE system and (and its operational environment) in the evaluated configuration. This document is available as an electronic download from the CloudShield Support Website (www.cloudshield.com/support).

The System Software Release Notes is available as a paper copy shipped with the TOE.

3.3. Logical Scope

The description of the security features of the product are described in further details in Section 4. In summary, these functions are:

- Auditing
- Cryptographic Support
- Information Flow Control
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access

3.4. Clarification of Scope

The following features are explicitly excluded from the evaluated configuration:

- User authentication using Remote Authentication Dial-In User Service (RADIUS)
- The PacketC interface
- The interface to the MySQL database
- Bypass Control Module (BCM)

RAVE applications are assumed to be protected by the environment during creation and prior to being uploaded to the TOE by an authorized administrator via TLS-protected HTTP giving access to the WMI or through the SSH channel allowing access to the CLI.

The Secure Setup document notes that Internet Explorer 8 and Firefox 3.6 are supported for access to the Web Management Interface. To be precise, later versions of these browsers are likely to work as well; however, the TOE has only been tested with Internet Explorer 8 and Firefox 3.6. As always, tools in the operational environment should always have security patches applied.

The Secure Setup document also notes that any application deployment package (ADP) developed by an administrator is outside the scope of the evaluation. To be precise, the evaluation does cover whether the instructions in that package work as advertised in the documentation—in other words, that the package does what it is programmed to do. What is *not* covered by the evaluation is that the package actually does what it claims to do—in other words, that the administrator programmed it correctly. Further, the evaluation does not cover any of the ADPs installed by default with the TOE, with the exception of the DROP ADP, which drops every package, and the FORWARD ADP, which forwards every packet.

4. SECURITY POLICY

The security functionality provided by the TOE is described in the next sections.

4.1. Auditing

The ASM part of the TOE collects audit data and generates system audit log records for all configuration and security-relevant user actions. This provides the ability to investigate unauthorized system security and configuration activities after they occur so that proper remedial action can be taken. Configuration changes and security-related events and failures are recorded in a security audit log. Operations invoked via the WMI, CLI, and GODYN / JSON type administrative interfaces provided by the ASM generate audit records[2]. All audit log records are maintained in the ASM system database.

The DPPM blades do not provide auditing, but do provide the ability for RAVE programs to log events. This is not considered "audit" in the Common Criteria sense for this TOE, but might be used by a RAVE application to implement audit to meet application needs.

The system restricts the ability to manage the security audit logs by a privilege assigned to an administrator role. Only authorized administrators who have been identified and authenticated have access to the audit functions. Using the WMI and CLI management interfaces, authorized security administrators have the ability to:

- View all information related to a security audit log. The system ensures that no user without the proper authorization is able to view the security audit logs. Any unauthorized attempt results in a security audit log. The logs may be sorted in ascending/descending order or by time, type, source IP address, or user name to facilitate searches.

- Generate a security audit log file to upload (to the ASM system database) for off-system archival and analysis

- Delete audit log entries and audit log files. The audit logs are protected from unauthorized deletion. Only authorized administrators who have been identified and authenticated have the ability to delete audit log records and files.

When the audit log fills up, the TOE allows the specification of one of the following behaviors:

- Stopping of traffic until a portion of the audit log is deleted

- Wrapping of the audit logs and overwriting the oldest entries

- Wrapping of the audit logs and overwriting the oldest entries and sending an alarm every five minutes.

Please note that the syslog functionality provided by the TOE (including the functionality to send syslog data to remote log hosts) is not considered to be the auditing functionality and therefore not covered by the security claim.

The DPPM inherently does not generate audit logs.

[2] With one exception. The DPPM blade supports a firmware database used to support application processing. This database contains a special type of storage called Content Addressable Memory (CAM). The JSON interface used to update CAM is designed to be a high-speed interface usable by another application only. These speed constraints prevent the TOE from being able to audit CAM updates, which can potentially modify RAVE application behavior. In order to implement full end-to-end auditing, the JSON client must be enabled to audit the modifications to its rule engine. Therefore, the administrator of the TOE must ensure that any user allowed access to the JSON interface (either via the CLI) or via JSONSSL complies with the organizational auditing requirements.

4.2. Cryptographic Support

The ASM blades include their own instance of a cryptographic library to support remote trusted IT products to initiate SSL connections with the TOE for the purposes of uploading rule sets and remote administration of the TOE implementing a trusted channel to a remote trusted entity. The WMI, CLI, and GODYN / JSON administrative interfaces provide secure system management through the use of SSH and TLS-protected HTTP for protection to access the ASM. Encryption is not utilized on the DPPM interfaces nor supported for encrypting or decrypting network content flowing through the DPPM, as the DPPM blade is the network analyzing portion of the TOE that is never the endpoint of a TLS communication.

The cryptography used in this product has not been FIPS 140-2 certified nor has it been analyzed for tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor. This Security Target claims compliance with the external standard for the cipher suites explained by the SFRs of FCS_COP.1 for the definition of the encryption algorithm. There are many ways of determining compliance with a standard. The vendor asserts the correctness of the cryptographic mechanisms.

4.3. Information Flow Control

The DPPM blades in the TOE enforce information flow control based on defined RAVE applications. The evaluation ensures that the RAVE language constructs behave as documented. The creation of the applications is outside the scope of the TOE. The applications are assumed to be protected by the environment during creation and prior to being uploaded to the TOE by an authorized administrator via TLS-protected HTTP giving access to the WMI or through the SSH channel allowing access to the CLI.

RAVE language constructs allow the specification of rules to identify Ethernet frames and subsequently act on identified frames. RAVE allows the specification of actions including forwarding the frame, altering the frame, generating a new frame or dropping the frame. The Security Target provides more details on the specific capabilities of the RAVE programming language.

The development environment distributes pre-defined RAVE subroutines that a developer can use to generate the intended RAVE application. The evaluation makes no claims to the correctness of these routines or their suitability for their claimed tasks with two exceptions: the predefined application that drops all packets, and the predefined application that forwards all packets.

The TOE also provides residual information protection, ensuring that data objects (i.e., packets) are cleared before they are reallocated for reuse.

4.4. Identification and Authentication (I&A)

The ASM part of the TOE maintains security attributes for each user account, and includes the ability to assign users to groups and to define access for users, providing administrative flexibility.

The TOE requires users to provide unique identification and authentication data before any administrative access to the system is granted. The TOE has the ability to lock a user's account if the authentication attempts threshold has been exceeded. Furthermore, it provides a password quality enforcement mechanism.

Specifically, the TOE provides an authentication mechanism that verifies that secrets meet the requirement: for each attempt to authenticate, the probability that a random attempt will succeed is less than one in 1,000,000. The mechanism provided accomplishes this by requiring that passwords contain at least eight characters but no more than 20 and the session is locked after three (three is the default – or administrator configurable integer between 1 and 8) unsuccessful authentication attempts or by using an SSL certificate.

The TOE supports the following password configuration values (defaults showing in parenthesis after the description):

- **Account Inactivity threshold**: Accounts not used for this duration are disabled and must be reenabled by an administrator. (Default: 45 days)

- **Password minimum length**: Minimum length for the password (must be at least 8 characters).

- **Minimum number of lowercase letters in password**: Minimum number of lowercase letters required in the password. (Default: 1)

- **Minimum number of uppercase letters in password**: Minimum number of uppercase letters required in the password. (Default: 1)

- **Minimum number of digits in password**: Minimum number of digits required in the password. (Default: 1)

- **Minimum number of non-alphanumeric character in password**: Minimum number of other characters (such as !, #, @) required in the password. (Default: 1)

- **Login delay**: Specifies the amount of time a user must wait before trying to log in again after each failed login attempt (where a CLI or Telnet attempt may include up to three efforts to enter the correct password). Any additional attempts during the delay period count as failures, even if the entered password is correct. For this reason, CloudShield recommends that this interval remain short (a few seconds at most). (Default: 4 seconds)

- **Password history**: Sets the number of old passwords (between 0 and 100) that cannot be repeated when changing passwords. Applied only when users are changing their own passwords. (Default: 5)

- **Password expiration**: Sets the number of days after which the password expires. This setting is ignored for the admin password, which never expires.

- **Password expiration warning**: Sets the number of days after which a warning is presented to the user upon login.

- **Minimum time between password changes**. Sets the minimum time (in hours, between 0 and 168) that must pass before a user can change a password. Applies only when users are changing their own passwords. (Default: 24)

User identification and authentication (I&A) is neither implemented nor required on the DPPM blade. This is because unauthenticated entities interact with the DPPM via the network interfaces through standard operation.

Also, it is noted that SNMP does not implement I&A as it does not access TSF data. JSON implements I&A through SSL certificates and certificate verification using a Pluggable Authentication Module (PAM) that audits user log on and log off.

4.5. Security Management

The supported ASM blades provide the authorized administrators the ability to define policies that define the access rules on the traffic received by the TOE. There are several functions available to the authorized administrator, such as manage user accounts and modify the behavior of the information flow policies. Modification of the rule sets can only be done using the RAVE programming language.

The TOE supports administrative roles that are defined by the groups assigned to human users by an authorized administrator at the time a user account is created.

Individual users are not assigned access rights directly. Access to the TOE is controlled by defined groups and their privileges and by assigning users to one or more of the groups. Once groups are defined, individual users are placed into the group or groups with the appropriate access levels.

User and Group definitions are stored in the MySQL database. Generally, the MySQL database is used to store configuration information as well as statistical data.

Each group is granted one of three privilege levels (Read/Write, Read-only, or None) to one or more of the five management areas on the TOE:

- Hardware
- Network
- Software
- Security
- Configuration

A sixth management area, the Database, defines access to the TOE system MySQL database, which is managed by the internal ASM software and can only be accessed remotely using SQL read-only queries through the administrative interfaces. However, the interface to the MySQL Database is disabled and disallowed in the evaluated configuration. The database is used to store the following configuration data:

- Administrative controls and safeguards enforced for access to the TOE
- Invalid login lockout thresholds and controls
- Password composition regulations
- Inactive session termination controls

4.6. Protection of the TSF

The architecture of the TOE provides protection mechanisms for its security functions as the TOE executes on stand-alone, protected hardware. The structure of the TOE ensures that non-administrative users on the managed networks do not have access to the TOE configuration mechanisms, and the operating system on the administrative blades ensure that only authorized users may configure the system—and, more important, the administrative blades do not provide the ability to execute code provided by untrusted users. Nonetheless, it is to be noted that the most important protection mechanism is the human user who is assumed to be competent to utilize the TOE securely, and trusted and abide by the instructions set forth in the TOE documentation.

Specifically, with respect to the FPT SFRs, the TOE provides appropriate time stamps used for the auditing system.

4.7. TOE Access

The TOE displays access banners before users perform identification and authentication. Interactive sessions of administrators can be configured to be locked when unattended.

5. ASSUMPTIONS

The evaluation makes the following assumptions on the TOE environment and personnel managing the TOE:

- The TOE is protected from unauthorized physical access. The application development environment is physically secured to a level of protection appropriate for the eventual deployment environment of the product.
- Administrative users are competent to manage the TOE securely. In addition, administrative users are competent to utilize the RAVE programming language.
- The operating system of the application development environment is patched regularly for known vulnerabilities. The RAVE compiler and equivalent tools are under the protection of

an integrity checking mechanism, and ensure the compilation tools used are the vendor-approved versions and in vendor-approved configurations. The mechanism used to transfer compiled and bundled application programs to the target product ensure the integrity of the files transferred.

- Users connecting to the ASM are competent to utilize the TOE securely, and trusted and abide by the instructions set forth in the TOE documentation.

- Users making use of the IDE must ensure this IDE and the associated RAVE code compiler to be securely protected and its integrity is ensured.

- Any other systems with which the ASM portion of the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

- In case of an in-line setup of the TOE, the information flow control functionality of the TOE establishes the only physical or logical network connection between the different networks that are to be protected by the information flow control rules enforced by the TOE.

6. ARCHITECTURAL INFORMATION

As noted in the introduction to Section 4, "SECURITY POLICY", on page 11, CloudShield is a multi-function solution appliance without any pre-configured network capability set programmed into the system. The CloudShield appliance contains two different types of processing blades: (a) the Deep Packet Processing Module (DPPM) blades, which execute programs written in the RAVE programming language) that instruct the TOE to analyze, make decisions, and take action on packet data received from the network; and (b) the Application Server Module (ASM) blade, which provides the management capabilities. Management of the DPPM blade is possible only from the ASM blade, which communicates with the DPPM over an internal gigabit Ethernet.

The TOE is deployable in various network topologies. When connected in-line, the DPPM executes a rule set that the TOE uses to actively mediate traffic between separate networks connected to different DPPM ports. The TOE receives packets on one port, processes them according to the RAVE application logic, and then if applicable, sends the same packets, modified packets or new packets out another port to return to the network. In an in-line configuration, the location of the TOE in the network ensures that network traffic cannot pass between networks without passing through the TOE processing logic.

When connected in a tap configuration, the TOE does not mediate traffic. Instead it receives a duplicate of the original network traffic (via a tap or span port) to perform passive analysis, statistics gathering, monitoring, and logging.

The TOE operates transparently to the IP infrastructure because the DPPM traffic forwarding interfaces do not own an IP address while providing a physically separate ASM implementing the functionality of system management, control, and monitoring applications. The ASM communicates with remote entities via network interfaces which are independent from the DPPM. This provides hardened protection since packet processing execution can only be controlled from the ASM, making it impossible to reach the network control logic, or assume control of the TOE, via the DPPM interfaces. Since a DPPM does not provide a MAC (Media Access Control) or IP address to the network, it is “invisible” to other network entities, regardless of whether it is deployed in an in-line or tap configuration.

The needs of the particular enterprise dictates how the TOE should be connected to the network. The use of the TOE for traffic management and control, network monitoring and reporting, network security, and/or security policy enforcement, will dictate whether the TOE should be located on the boundary between an organizations’ internal network and external networks or whether it should be placed within the enterprises’ networks. Guidance documents are provided to help users install the TOE in the correct location for its intended usage and CloudShield will assist customers if requested. For stateful filtering and traffic flow functions, the TOE should be placed within a topology so that it can see both sides of all network conversations of interest. A TOE enforcing active functions such as replication and filtering can be placed between routers, between a router and switch or between two switches. A TOE enforcing passive applications such as statistics gathering and logging can be placed between the network routers or simply attached (tapped) to a network segment. Placements can be made on the boundary between an organization’s internal network and external networks or between two networks both belonging to an organization. Graphical representations of these placements are depicted in the Technical Training documentation.

The following sections explore the architecture of the CloudShield appliance in greater detail.

6.1.1. Deep Packet Processing Module (DPPM)

Each DPPM consists of a network processing complex, a silicon database subsystem that provides a transient storage area to process streams of packets, a regular expression pattern matching sub-system, an ARM (Advanced RISC Machine) processor running an embedded Linux, three external physical connectivity options; Ethernet, OC-48 Packet over SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), or 10G Ethernet. In addition, each DPPM has a dedicated Gigabit Ethernet port for packet capture and logging.

The DPPM Control OS (Operating System) is an embedded Linux implementation that has been modified by CloudShield to support the DPPM blade hardware. The embedded version of Linux differs from non-embedded Linux in several major ways:

- It is intended to be used on dedicated devices (i.e., single-purpose product types) such as the DPPM blade.
- It is not intended for use as a multi-user operating system. For example it does not support memory protection (all processes can access the data of all other processes).
- It is built for speed (in a manner very similar to a Real-Time Operating System (RTOS)). For example, the Embedded Linux kernel is different than the standard versions in that it is pre-emptible (i.e., the kernel can be interrupted mid-task, so that other applications can continue to run when another application is working in the background).

Network data sent by unauthenticated external IT entities enters and exits the TOE through the physical DPPM network interfaces. Incoming traffic passes into a framer that recognizes and packages frames into packets – the logical unit of data in networks.

Each packet is forward to the Packet Switch Field-Programmable Gate Arrays (FPGA), abbreviated as PSW, for pre-processing and distribution. The PSW performs a checksum validation for ISO Level 3/Level 4 (L3/L4), a complete IP (Internet Protocol) header decode, and initializes a Packet Information Block (PIB) or metadata control structure, to accompany the incoming packet to the network processing complex where the RAVE rule set executes. In the DPPM-800, the PSW FPGA also incorporates a Traffic Control Subsystem (TCS) that provides adaptable selective traffic filtering and load-balancing to distribute high-speed 10G traffic streams over multiple DPPM-800 modules clustered together. The TCS analyzes traffic at layers 2-4 to direct packets to specific destinations based on the results of the analysis. Each destination is a port or DPPM network processing complex. Packets then pass from the PSW FPGA to the network processing complex (note: in the DPPM-800, the TCS may filter/drop packets before sending to the network processing complex).

The network processing complex receives and transmits packets to and from the PSW using board-level components called Packet Receivers and Packet Transmitters, respectively. Packets are placed into an input buffer and the network processing complex executes the rule set to examine or modify each packet and make logic decisions regarding the handling of each packet. Messages that span multiple packets are reassembled by the network processing complex.

A silicon database subsystem provides persistent storage for the network processing complex applications running on the DPPM. It is a firmware implementation of a relational database and supports the definition of database tables for state tracking and the storage of global data, arrays, and matrices.

A regular expression pattern matching subsystem performs unstructured packet processing of packets as requested from the network processing complex, the results of which are then returned to the network processing complex.

If the RAVE application logic transmits a packet back to the network, the packet is sent to the PSW for checksum re-calculation and then out the selected DPPM physical interface.

6.1.2. Application Server Module (ASM)

The ASM includes its own processor, memory, disk storage and system database, physical interfaces and executes a version of the Red-Hat Enterprise Linux (RHEL) operating system.

The TOE employs a multi-layered approach to security. A three-tiered architecture allows only the secure management plane to control packet processing through tightly controlled communications channels. Since packet processing execution can only be controlled from the ASM, it is not possible to assume control of, nor even compromise, the CS-2000 from the DPPM. The TOE enforces the following protection mechanisms: Identification and authentication mechanism is enforced whereby a user must enter a username and password to access the ASM. After a user successfully logs in, the CloudShield's Mandatory Access Control (MAC) System enforces roles which control further access to the TOE's management functions. In this sense, the term MAC does not refer to the traditional sense of controlling access to user data, but rather it restricts access to TSF data by the use of administrative roles.

The ASM used in this product is specific to Internet Protocol version 4 (IPv4) networks.

6.1.3. Network traffic rules – RAVE Applications

Network traffic processing rule sets are created using the CloudShield PacketWorks IDE application on a commodity PC in the operational environment. The rules are implemented using the RAVE programming language. The RAVE programming language is the interface for administrators to configure the TOE (the PacketC environment is outside of the scope of this evaluation).

Multiple rule sets may be combined together to form a single Application Deployment Package (ADP). An ADP incorporates a virtual patch panel concept to connect multiple rule sets through "virtual wires" that map between the start and stop nodes of each individual rule set. This allows programmers to combine the policy logic of different discrete network traffic features (e.g. Distributed Denial of Service (DDoS) protection, anti-virus, etc) effectively into one comprehensive rule set that can be deployed on a DPPM to support multi-mission policy enforcement.

The progression through an ADP represents the application of multiple discrete rule sets, or policies, according to the "virtual wire" connectivity. When one intermediate rule set completes execution, the "virtual wire" hands off processing to the next rule set. Processing terminates with the last rule set defined in the ADP.

From the IDE, an ADP is uploaded to the TOE using the Web Management Interface (WMI) or Command Line Interface (CLI) where it is saved into the ASM system database. Using the WMI or CLI, a user chooses an ADP from the selection stored in the database and commits (i.e. loads) it onto the ASM which in turn forwards it to the intended DPPM to configure the packet processing capabilities of the DPPM. If more than one DPPM is present in the TOE, each may receive an independent ADP rule set. Once loaded into the DPPM, all new incoming packets are subjected to the new rule set logic.

This evaluation confirms that the RAVE instruction set and patch panel work correctly, but does not and cannot confirm that any particular RAVE program is suitable for the tasked claimed by its author. This evaluation establishes confidence that the RAVE program will work as written.

The RAVE application can specify a particular rule that forwards the first 64 bytes of the processed IP packet to the syslog trail maintained by the ASM to support a logging of the ongoing communication. In addition, RAVE applications can specify a different rule which allow the IP packets to be stored in the MySQL database of the ASM. The MySQL database is a storage backend for statistical data and various configuration options.

7. PRODUCT TESTING

7.1. Sponsor Testing

The evaluator interviewed several CloudShield developers and observed the operation of several of their test cases. From this information, the following describes the overall test approach taken by the developer.

The developer has a test facility within the development site where development occurs. A team of several testers are assigned to specific modules of the product and are responsible for those modules. Each tester maintains spreadsheets for each of the test cases they are responsible for and uses them to report the test results to management.

The testing lab contains a large set of workstations that are networked together along with several TOE instances. These workstations control packet generator devices that can simulate real-world traffic patterns in order to fully test the TOE. Traffic patterns are sent to the DPPM side of the TOE and many different kinds of rule-sets are tested to fully test the RAVE opcodes. Also, automated test procedures and scripts are written to test all of the user interfaces on the ASM subsystem. These automated tests are easily reproducible.

When a test fails or a bug from a customer is received, the bug is tracked in their bug tracking system. Each bug is tagged with a severity, security related flag, and the responsible parties in charge of creating patches and accepting those patches. All test plans are kept within the CM system and final test results are also kept there. Intermediate test results are kept on a separate system in order to facilitate quick bug-fix turn rounds.

7.1.1. Testing results

The results were generated on the test configuration above and all test results were recorded as the tester observed. All test results provided are consistent with the expected results except a small percentage of test cases. These test cases were scrutinized by the evaluation team where they concluded that the failures did not indicate flaws in the TSF.

7.1.2. Test coverage

The functional specification identified the following TSF Interfaces:

- DPPM physical network interface
- ASM physical network interface
- Web Management Interfaces (through HTTP/HTTPS)

- Command Line Interfaces (through SSH)
- SNMP Interface
- GODYN/JSON Interface
- IP datagrams, which includes frame handling, TCS configuration file, Log accelerator configuration file/RAVE code, RAVE application
- SNMP protocol
- Physical console (KVM)
- NTP protocol

A mapping provided by the sponsor shows that the tests cover all individual TSFI identified for the TOE. An extension to this mapping developed by the evaluator as documented in the test case coverage analysis document shows that also significant details of the TSFI have been tested with the sponsor's test suite. This therefore satisfies the requirements for the evaluation.

7.1.3. Test depth

In addition to the mapping to the functional specification, the sponsor provided a mapping of test cases to subsystems of the high level design and the internal interfaces described in the high level design. This mapping shows that all subsystems the internal interfaces are covered by test cases.

The depth analysis between the components of the design and the available test cases is seen as sufficient by the evaluator, because each test case can be matched to a subsystem and vice versa, as shown in test coverage analysis mapping. All TSF covered by the subsystems of the high-level design are covered with test cases. The security-relevant internal interfaces can be linked to the test cases. The hardware subsystem is always implicitly tested by every software component that runs on it. Therefore, the hardware subsystem was not explicitly mentioned in test mapping.

Not all of the internal interfaces mentioned in the high-level design could be covered by direct test cases. Some internal interfaces were exercised indirectly by invoking the TSFI that use them.

7.2. Evaluator Testing

7.2.1. TOE test configuration

The evaluators independently installed the test systems according to the documentation in the Evaluated Configuration Guide and the test plan. This hardware was located at the evaluator facility in Austin, Texas. The hardware configuration was identical to the system used by the sponsor to perform testing, except that the developer has several automated tools to interact with the TOE that the lab did not have access to. Note that the evaluator testing did not cover all the DPPM models or all possible combinations of ASM models and DPPM models in a chassis that are supported by this evaluation; however, an equivalence argument was provided.

The independent testing effort performed testing on the ASM and the DPPM-510 inside the CS-2000 chassis enclosure. This is sufficient as the underlying hardware platform differences do not affect the SFRs that were sampled to be tested. The different DPPM blades only offer different physical layer network cards. The DPPM-800 does contain the Traffic Control Subsystem (TCS)[3], but this was not tested in independent testing, and its absence in the other platforms would not affect the results of the actual tests performed. The ASM and ASM2 only have faster hardware components (e.g., faster processors); therefore, the ASM is equivalent to ASM2 for the purposes of independent testing. There is only one chassis enclosure in the evaluated configuration.

7.2.2. Subset size chosen

The evaluator chose to reproduce two manual test plans of the sponsor test suite for auditing and identification and authentication TSFs for the TOE.

7.2.3. Evaluator tests performed

In addition to a subset of developer tests, the evaluator devised tests for a subset of the TOE. The tests are listed in the Evaluator Test Plan.

The evaluator chose these tests for the following reasons:

- The DPPM is the primary functionality of the TOE, and therefore should be tested carefully to ensure the TSF has no flaws.
- The DPPM contains the only attack surface[4] of the TOE, making it the critical subsystem in prevent attacks from compromising the TSF. The relevant tests performed by the evaluator include:
    - **Insecure initial state**. This test observes the initial state of the DPPM, and identifies any flaws in the TOE that could place the TOE in an insecure state.
    - **A.SEPERATION violation**. This test verifies whether the TOE can violate the ST assumption A.SEPERATION, which states that in case of an in-line setup of the TOE, the information flow control functionality of the TOE establishes the only physical or logical network connection between the different networks that are to be protected by the information flow control rules enforced by the TOE.

[3] The Traffic Control Subsystem provides adaptable selective traffic filtering and load-balancing to distribute high-speed 10G traffic streams over multiple DPPM-800 modules clustered together. This is not a security-relevant feature.

[4] That is, a surface accessable by untrusted users.

7.2.4. Summary of Evaluator Test Results

The evaluator testing effort consists of two parts. The first was the reproducing of the sponsor test execution, and the second was the execution of the tests created by the evaluator.

The tests were performed at the CCTL facility in Austin

In each case the system was accessible directly through its TSFI. The evaluator installed the TOE in the evaluated configuration according to the guidance. The test system was therefore configured according to the ST and the instructions in the Evaluated Configuration Guide. The evaluator reproduced the execution of the developer's test cases. The results were recorded directly in the Evaluator Test Plan.

All the test results conformed to the expected test results from the test plan.

In addition to running the tests that were provided by the sponsor according to the test plan from the sponsor, the evaluator decided to run some additional test cases on the provided test systems as defined in Evaluator Test Plan:

- Forward() opcode
- Terminate() opcode
- Drop() opcode
- Packet_Replicate() opcode
- Copy_Packet_Constant() opcode
- Search_Packet_Test() opcode
- Object Reuse in the DPPM
- Audit Record Test
- Auditing of the WMI

All tests passed successfully.

8. DOCUMENTATION

8.1. Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows (documents shown with * are not security relevant):

- *CloudShield CS-2000 Series Documentation Guide, Release 3.0.3,* 2012-03-09, Part No. 150-1126-00.*
- *CloudShield CS2000 Installation and Hardware Reference Guide, Release 3.0.3*, 2012-03-09, Part No. 150-1124-00.
- *CloudShield CS-2000 Quick Start Guide, Release 3.0.3*, 2012-03-09, Part No. 150-1125-00.
- *CloudShield System Software Release Notes, Release 3.0.3*, Build 2822, 2010-08-11, Part No. 150-1139-00.*
- *CloudShield CS-2000 Command Line Interface Reference Guide, Release 3.0.3*, 2012-03-09, Part No. 150-1122-00.
- *CloudShield CS-2000 Web management Interface User Guide Series Release 3.0.3*, 2012-03-09, Part No. 150-1123-00.
- *CloudShield Application Integration User Guide 3.0.3*, 2012-03-09, Part No. 150-1120-00.
- *CloudShield Secure Setup For Common Criteria Guide Release 3.0.3*, 2012-01-13. No Part Number.

The following documents are also user guidance in the sense that they deal with the RAVE programming interface:

- *CloudShield RAVE Language Users Guide, Release 3.1,* 2009_12_17_00, Part No. 160-1106-00.
- *CloudShield PacketWorks Regular Expressions User Guide, Release 3.1*, 2009_12_17_00. Part No. 150-1108-00.
- *Cloudshield PacketWorks Integrated Development Environment User Guide, Release 3.1.* 2010_10_23_00. Part No. 150-1107-00.

With the exception of the *Secure Setup For Common Criteria Guide* and *Software Release Notes*, the user guidance is available on CD shipped along with the TOE. Any other documentation delivered on the CD has not been examined as part of this evaluation and may not be applicable.

The *Secure Setup For Common Criteria Guide* can be obtained securely from the CloudShield CloudShield support website at https://www.cloudshield.com/support.

The *CloudShield System Software Release Notes* is available as paper copy shipped along with the TOE.

8.2. Evaluation Evidence

In addition to the guidance documentation listed above, the following documentation was submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents may be proprietary and not available to the general public. This list does not include small graphics files and email evidence.

Design Documentation	Version	Date
CloudShield Common Criteria Design Specifications, Generated by Doxygen 1.5.9	--	2009-11-23
CloudShield CS-2000 High-Level Design	1.6	2010-06-25
CloudShield Design	0.1	2009-03-03
Cloudshield MicroCode Specification, Version 1.0.4, 8/21/2002	1.0.4	2002-08-21
CloudShield RAVE Byte Codes Design Spec	0.33	2011-04-26
FSP Mapping: fsp_mapping.xls	--	2011-10-10
Opcodes: from generation to loading (IDE 3.0)	--	2011-02-07

Life Cycle Documentation	Version	Date
Agile CI Listing: `12-03-16 Agile CI Listing.xls`	--	2012-03-28
Bug List, Target Milestone 3.0.3	--	2012-02-14
Cloudshield CS-2000 with CPOS Configuration Management Plan, Document No. 150-410-00	5	2008-04-02
Cloudshield CS-2000 with CPOS Delivery Procedures, Document No. 151-003-00	4	2008-11-17
Cloudshield Processes and TOE Configuration	3	2010-06-25
Intel IXP2805 Network Processor Programmers Reference Manual, Order Number 310015	007	2006-04
The Bugzilla Guide - 3.0.5 Release	--	2008-08-12
Version Management with CVS for cvs 1.11.17	--	2004
Various Lifecycle, employee management, and configuration screenshots	--	--

Test Documentation	Version	Date
CloudShield CPOS 3.0.3 SNMP High Level Test Plan	2.3	2010-03-15
CloudShield Independent Test Plan, CloudShield CS-2000 with CPOS, v3.0.3 (atsec)	2	2011-04-14
CPOS 3.0.3 Security Test Plan	0.3	2012-02-14

CPOS 3.0.3 Top Level System Test Plan	1.1	2010-03-16
CPOS 3.0.3, Audit Log Test Procedures	0.4	2010-05-14
CPOS System Audit Log Test Plan	0.2	2010-03-03
Dynamic Update (DU-JSON) Test Plan	0.9	2009-06-12
Dynamic Update JSON API (DU-JSON) Test Procedures, CPOS 3.0.2	0.1	2009-06-09
Functional Test Specification for MicroCode – Release 3.0.3	0.2	2010-02-16
µCode Test Plan: `uCodeTestPlan.xls`	--	--
PSW Test Automation Functional Specification	1.0	2007-08-28
QA Test Specification for Multiple Applications	0.3	2010-05-14
QA Test Specification for Multiple Applications	0.2	2010-05-14
Simple Network Management Protocol (SNMP) Test Procedures, CPOS 3.0.3	0.9	2010-04-20
Test Failure Analysis Spreadsheet: `test-failure-analysis.xls`	--	2011-10-10
WMI/CLI/KVM Basic Password User Security Config. and Misc NTP Config. Test Cases	0.2	2010-06-17
Various test results, scripts, etc.	--	--

Security Target	**Version**	**Date**
CloudShield CS-2000 with CPOS 3.0.3 Security Target	1.0	2012-01-25

9. RESULTS OF THE EVALUATION[5]

The evaluation team determined the product to be CC Part 2 conformant, CC Part 3 conformant, and to meet the requirements of EAL 4 augmented by ALC_FLR.3. In short, the product satisfies the security technical requirements specified in CloudShield CS-2000 with CPOS 3.0.3 Security Target on platforms listed in Table 1: Evaluation Identifiers.

10. VALIDATOR COMMENTS

10.1. UNIX STIG Analysis

The CCTL used the UNIX STIG standard as input to the vulnerability analysis. However, since the interfaces to the TOE do not allow users access to the general purpose operating system features of the underlying operating system, the CCTL found no direct way of applying the UNIX STIG to vulnerability analysis.

[5] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

10.2. Integrity Checks on RAVE applications

There are no integrity checks performed on RAVE applications by the TOE. Therefore, it is important to note that the RAVE compiler and the RAVE language are extremely simplistic, and perform no boundary checking, type checking, overflow checking, or exception processing found in modern proactive systems and programming languages. As such, it is imperative that RAVE application developers adequately test and debug their applications for a wide variety of exceptional conditions.

It is noted for this evaluation, the RAVE language is considered one of the TOE interfaces, but the opcodes are what were tested. The translation from RAVE language to opcodes was implicitly tested but not formally analyzed. The PacketC interface translates from PacketC to RAVE language was neither tested nor analyzed as part of the evaluation.

10.3. Suitability to Task

As a reminder, the examination of the RAVE language only ensured that instructions in that language do what they claim to do. There was no evaluation that any supplied applications (other than the “drop all” and “pass all” applications) are suitable to do what they claim to do.

10.4. Vulnerabilities Not Part of the Attack Surface

The interfaces to the ASM are assumed to be only accessible by administrative users, and the administrators are assumed to be competent and trustworthy. These assumptions effectively remove the ASM interfaces from the attack surface of the TOE. Therefore, the evaluators did not test these interfaces for vulnerabilities that could be exploited by a malicious entity. However, the evaluators did include in their vulnerability analysis the possibility of implementation flaws that place the TOE in an insecure state. Implementation flaws may exist, for example, in the underlying operating system or in the web application server that provides the graphical interface. If those flaws cause normal usage by administrators to violate the security policy unwittingly, this would have been considered significant.

However, during testing efforts, the evaluators did not identify any flaws that would place the TOE in such a state. The evaluators did the following to provide assurance of this:

- Testing effort led the evaluators to install the TOE and operate the product using the user guidance, which would expose such flaws.

- Searching for vulnerabilities in public databases for vulnerabilities in the open source software running on the TOE.

- Building auto-run and bootable USB disks that administrators may be socially engineered to attach to the TOE and attempting to elicit insecure behavior from the TOE.

- Testing the reaction to malformed RAVE applications.

- Fuzz testing the web applications and the GODYN interfaces

As these penetration tests did not prove the evaluator’s flaw hypothesis concerning implementation bugs that put the TOE at risk of being configured insecurely, the evaluators concluded that there were no such flaws detectable at this assurance level.

10.5. Passwords Embedded in Example Scripts

The user guidance supplied by the vendor includes examples that demonstrate embedding plaintext passwords in administrative scripts. Note that the system does provide the ability to request user interaction to supply credentials for use in scripts. When administrative scripts are developed, user interaction is the best course to take. If passwords must be embedded, note that (a) such scripts must be protected using system access controls to the greatest extent possible, and (b) such embedded passwords may result in NIST SP 800-53 IA control compliance.

10.6. Administrative Audit

Note that the system does not audit all administrative actions: in particular, file management actions and updates to the CAM via JSON are not audited. Compensating mechanisms are required to account for such administrative actions if the system’s IA control set requires such auditing.

10.7. Field Diagnostics

The product supports the ability to do field diagnostics; use of this facility is not precluded in the evaluated configuration. However, the facility should be used with caution and in accordance with appropriate IA controls, such as those specified for non-local maintenance in the MA family in NIST SP 800-53.

10.8. Use of Cryptography

The cryptographic functions used by the TOE are not FIPS certified. Correctness of the encryption mechanisms used by the TOE is by Vendor Assertion.

11. SECURITY TARGET

The ST, *Cloudshield CS-2000 with CPOS 3.0.3 Security Target v1.0 is* included here by reference.

12. LIST OF ACRONYMS

AC	Alternate Current
ADP	Application Deployment Package

ARM	Advanced RISC Machine
ASM	Application Server Module
BCM	Bypass Control Module
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DC	Direct Current
DDoS	Distributed Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FPGA	Field-Programmable Gate Arrays
JSON	JavaScript Object Notation
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IDE	Integrated Development Environment
IP	Internet Protocol
IT	Information Technology
IPv4	Internet Protocol version 4
MAC	Mandatory Access Control
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency

NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PIB	Packet Information Block
POS	Packet over SONET and SDH
PP	Protection Profile
PSW	Packet Switch Field-Programmable Gate Arrays
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RTOS	Real-Time Operating System
SDH	Synchronous Digital Hierarchy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
STIG	Security Technical Implementation Guide
TCS	Traffic Control Subsystem
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
WMI	Web Management Interface

13. BIBLIOGRAPHY

[1] Atsec Evaluation Technical Report for a Target of Evaluation, ETR, v1.1, 2012-03-27

[2] Atsec Evaluation Technical Report, ADV, ADV_ARC.1, v2.0, 2012-03-13

[3] Atsec Evaluation Technical Report, ADV, ADV_FSP.4, v2.0, 2012-03-13

[4] Atsec Evaluation Technical Report, ADV, ADV_IMP.1.1, v2.0, 2012-03-13

[5] Atsec Evaluation Technical Report, ADV, ADV_TDS.3, v2.0, 2012-03-13

[6] Atsec Evaluation Technical Report, AGD, v2.0, 2012-03-21

[7] Atsec Evaluation Technical Report, ALC, v5.0, 2012-03-21

[8] Atsec Evaluation Technical Report, ASE, v3.0, 2012-03-13

[9] Atsec Evaluation Technical Report, ATE, v3.0, 2012-03-13

[10] Atsec Evaluation Technical Report, AVA, v3.0, 2012-03-13

[11] Atsec Evaluation Technical Report, IND, v2, 2012-03-13

[12] Atsec Independent Test Plan, CloudShield CS-2000 with CPOS v3.0.3, Version 0.1, 2011-04-14

[13] Atsec Site Visit Report, v1.2, 2012-03-21

[14] CloudShield Application Integration Guide, Release 3.0.3, 2012-03_09_00

[15] CloudShield Common Criteria Design Specifications, Generated by Doxygen 1.5.9,

[16] CloudShield CPOS 3.0.3 SNMP High Level Test Plan, v2.3, 3/15/2010

[17] CloudShield CS-2000 Command Line Interface Reference Guide, Release 3.0.3, 2012-03_09_00

[18] CloudShield CS-2000 High-Level Design, version 1.6, June 25, 2010

[19] CloudShield CS-2000 Quick Start Guide, Release 3.0.3, 2012-03_09_00

[20] CloudShield CS-2000 Web Management Interface User Guide, Release 3.0.3, 2012-03_09_00

[21] CloudShield CS-2000 with CPOS 3.0.3 Security Target, Version 0.10

[22] CloudShield Design, Version 0.1, 03.03.2009

[23] CloudShield Installation and Hardware Reference Guide, Release 3.0.3, 2012-03_09_00

[24] Cloudshield MicroCode Specification, Version 1.0.4, 8/21/02

[25] CloudShield PacketWorks Integrated Development Environment, User Guide Release 3.1, 2010_10_23_00

[26] CloudShield PacketWorks Regular Expressions User Guide Release 3.1, 2009_12_17_00

[27] Cloudshield Processes and TOE Configuration, Version 3, June 25, 2010

[28] CloudShield RAVE Byte Codes Design Spec, Revision 0.33, 04/26/11

[29] CloudShield RAVE Language Guide, User Guide, Release 3.1, 2009_12_17_00

[30] CloudShield Secure Setup for Common Criteria, Release 3.0.3, 2012_01_13_00

[31] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1.

[32] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1.

[33] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1.

[34] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, Version 3.1.

[35] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, Version 3.1.

[36] CPOS 3.0.3 Security Test Plan, v0.3, 2/14/12

[37] CPOS 3.0.3 Top Level System Test Plan, March 16, 2010

[38] CPOS 3.0.3, Audit Log Test Procedures, Rev 0.4, 5/14/2010

[39] CPOS System Audit Log Test Plan, Revision 0.2, 03/03/2010

[40] Dynamic Update (DU-JSON) Test Plan, Revision 0.9, 6/12/2009

[41] Dynamic Update JSON API (DU-JSON) Test Procedures, CPOS 3.0.2, June 9, 2009, Version 0.1.

[42] FSP Mapping: fsp_mapping.xls

[43] Functional Test Specification for MicroCode – Release 3.0.3. Revision 0.2, 02/16/2010

[44] Intel IXP2805 Network Processor Programmers Reference Manual, April 2006, Order Number 310015, Revision 007US

[45] µCode Test Plan: uCodeTestPlan.xls

[46] Opcodes: from generation to loading (IDE 3.0)

[47] PSW Test Automation Functional Specification, Revision 1.0, 8/28/2007

[48] QA Test Specification for Multiple Applications, v0.3, 5/14/2010

[49] Simple Network Management Protocol (SNMP) Test Procedures, CPOS 3.0.3, Version 0.9, 4/20/2010

[50] TestResults

[51] WMI/CLI/KVM Basic Password User Security Config. and Misc NTP Config. Test Cases, Rev 0.2, 06.17.2010