National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Xceedium GateKeeper Version 5.2.1

Report Number:	CCEVS-VR-VID10350-2010
Dated:	25 March 2011
Version:	1.0

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 20755-6940

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Xceedium Gatekeeper 5.2.1. The evaluation was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed in March 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria (CC), Version 3.1 Revision 2 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 2.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and Team Test Report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 and Part 3 conformant, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2. All security functional requirements are derived from the Part 2 of the Common Criteria.

The TOE is Xceedium Gatekeeper 5.2.1 provided by Xceedium, Inc. Xceedium Gatekeeper 5.2.1 provides FIPS-validated SSL -secured, in-band and out-of-band management and monitoring of networking equipment, UNIX, Linux, Macintosh and Windows servers, as well as remote power-management to either turn on, off, or reboot any attached device. Its purpose is to enable purchasers to remotely manage the activities of users from a central point to anywhere in the heterogeneous IT infrastructure, without modification of legacy systems.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org). The report presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

Identification

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

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 to which the product is conformant; and
- 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
TOE:	Xceedium GateKeeper Version 5.2.1
Protection Profile	None
ST:	Xceedium GateKeeper Version 5.2.1 Security Target, Version 2.9, 3 February 2011
Evaluation Technical Report	Evaluation Technical Report for Xceedium GateKeeper Version 5.2.1, Part 1 (Non-Proprietary), Version 2.0, 25 March 2011, Part 2 (Proprietary), Version 3.0, 25 February 2011.
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Conformance	CC Part 2 and Part 3 conformant, EAL 4 augmented with

Item	Identifier
Result	ALC_FLR.2
Sponsor	Xceedium, Inc.
Developer	Xceedium, Inc.
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation (SAIC), Columbia, MD

2 TOE Overview

The GateKeeper product provides FIPS-validated SSL -secured, in-band and out-of-band management and monitoring of networking equipment, UNIX, Linux, Macintosh and Windows servers, as well as remote power-management to either turn on, off, or reboot any attached device. Its purpose is to enable purchasers to remotely manage the activities of users from a central point to anywhere in the heterogeneous IT infrastructure, without modification of legacy systems.

The GateKeeper TOE consists of an appliance and zero or more backend agents running on Windows or UNIX servers. Management of the TOE is performed using a Java enable browser over an SSL connection. The following sections detail the TOE components and their capabilities.

3 Assumptions, Threats, and Organizational Security Policies

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be employed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and defines the threats that the product is designed to counter.

3.1 Assumptions

Following are the assumptions identified in the Security Target:

- It is assumed the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- It is assumed all network traffic will be configured to pass through the TOE.
- It is assumed there will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

- It is assumed the authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2 Threats

Following are the threats levied against the TOE and its environment as identified in the Security Target. The threats that are identified are mitigated by the TOE and its environment. All of the threats identified in the ST are addressed.

- A user may cause audit data to be inappropriately accessed (viewed, modified or deleted).
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- A malicious user may cause the TOE, configuration data, or sensitive user data to be inappropriately accessed (viewed, modified or deleted) allowing a breach in the TSF security policies.
- A user may gain unauthorized access to devices.

3.3 Organizational Security Policies

In addition to the threats, the following organizational security policies are identified in the Security Target.

- The TOE must provide authorized administrators with utilities to effectively manage the security functions of the TOE.
- The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
- Users of the system shall be accountable for their security relevant actions within the system.

4 Clarification of Scope

The TOE is an Information Technology (IT) management tool that provides the ability to remotely maintain multiple network devices (server, routers, and platforms). The TOE is accessed via any Java enabled browser. The communication between the TOE and the browser is protected by SSL. The TOE provides the administrators with the interfaces to manage users, devices, and access policies.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

The TOE is designed to reside between untrusted users on an unprotected network and a protected network. Its purpose is to limit access to the resources on the protected network and provide for management of those resources from a centralized location. The TOE is composed of the four main components described below:

- GateKeeper Appliance - The GateKeeper appliance is a rack mounted network device. It provides access control to the devices located on the protected network and provides management interfaces for its policies. The appliance contains an internal database to store its configuration information, access policies, and audit records. The appliance also contains a web server to communicate with administrators managing the appliance via browsers. Within the web server, the appliance implements SSLv3 to support its management connections.
- GateKeeper Agents (Socket Filter Agent) – The GateKeeper agents can run on Windows, UNIX or Linux servers located on the protected network. The purpose of the agents is to further limit access from servers on the protected network, to other devices within the protected network in order to enforce audit and access policies. Once users gain access via the policies supported on the appliance, the agents can further limit access by restricting which ports may be utilized to create outbound connections to other resources within the protected environment.
- Management Interface – Management of the TOE is performed by administrators using a Java enabled web browser. The TOE provides a set of graphical interfaces in which to perform the management functions for the appliance and agents. The TOE also provides an SNMP interface to allow Administrators to retrieve management configuration information.
- GateKeeper Client - A set of Java Applets used by end users to access the GateKeeper Appliance. The clients do not enforce any security policies.

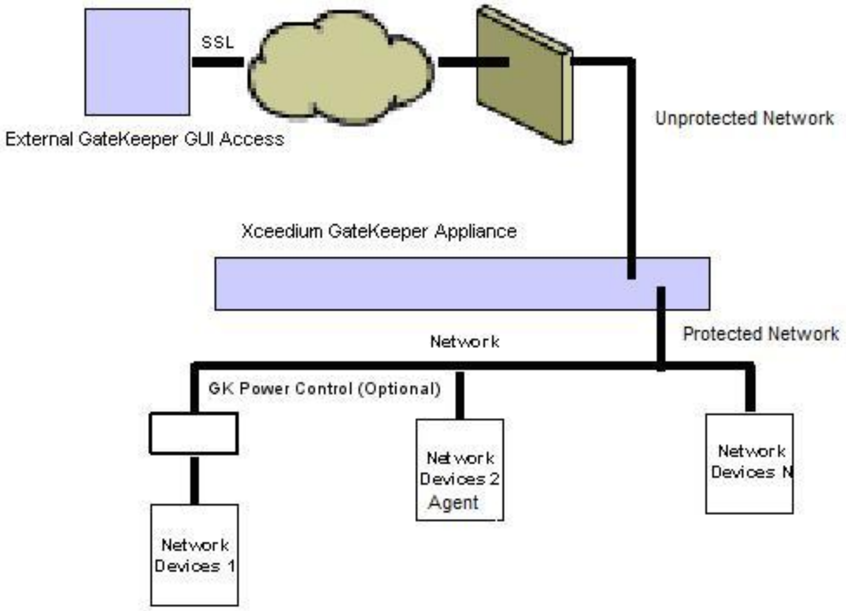


Figure 1: Xceedium GateKeeper TOE in its environment

The appliance requires all users to perform authentication to it using an identifier and a password. Once successful logon has occurred, administrators can perform management. When users log into the appliance they are doing so in order to access a device (e.g., service, network device) located on the protected network behind the appliance. Users are subject to an access control policy enforced by the appliance when they attempt to access a protected resource.

The access control policy enforced on users is based upon user identity and services provided by the backend device. Users are given access to particular services on specific devices. The set of services that are available for control are:

- ***VNC* (options: Standard, Linux, Web version)**– graphical access to a device (requires a VNC Server service to be installed and running on the device)
- ***Telnet*** – standard, unsecured Telnet access to a device
- ***SSH* –** secured, in-band console access to a device (requires a SSH v1 or v2 server (daemon) to be installed and running on the device)
- ***SSH2Telnet* –** allows secured access to a Telnet-enabled device by using the secure shell protocol for communications between the client and the GateKeeper appliance, All subsequent connections from the GateKeeper appliance to the target Telnet server (deamon) will be using the plain text Telnet protocol. This methodology allows for strict enforcement of only approved encrypted protocols outside of the protected network.
- ***R DP* –** Remote desktop connection (required the remote desktop connection enabled)
- ***Out-of-Band*** – serial (RS-232) console access of a device. (requires a network enabled serial concentrator supporting reverse telnet or reverse SSH)
- ***Power*** – remote boot (power on/off/reboot) of a device. (requires a network enabled “smart power” concentrator supporting reverse telnet or reverse ssh)
- ***Service*** – Other TCP/UDP services can also be defined by the authorized administrator for execution by end users. These services may include: fat client access such as SQL query frontends, mainframe clients, or any proprietary applications which use TCP or UDP connections. Note: As these services are defined and provided by the administrator, they are outside the scope of the TOE

Users are granted one or more services to a device. When a user attempts to access a device, the request is checked against the permitted services. With the support of the Socket Filter Agents, the appliance also supports a Socket Filter List in addition to the device access policy. This access policy permits an administrator to establish a set of sockets that are permitted for use on a backend device protected by the TOE by way of a proprietary agent installed on the target device.

6 Security Policy

The TOE logically supports the following security functions:

- Security Audit
- Identification and Authentication
- Security Management
- User Data Protection
- Protection of the TSF

- TOE Access

6.1 Security Audit

The TOE Web Server generates audit records related to the authentication and management of the TOE that are stored and protected in an internal database. The TOE records attempts to access itself, such as successful and failed authentication attempts, as well as the actions taken by users once authenticated. The appliance generates audit records for all access control decisions it makes. All auditable actions can be found in Active Logins, Sessions, Logs and Report interface. The Logs Report Parameters screen allows administrator selection of the specific report information to be generated.

6.2 Cryptographic Support

The TOE has been FIPS 140-2 evaluated and is configured to run in FIPS mode in the evaluated configuration. The TOE implements SSL to all user communication with the TOE. Users establish an SSL connection to the TOE before submitting a username/password to perform authentication. Users then use the SSL channel to transmit all information to the TOE. The TOE also supports x509v3 certificate generate and validation.

6.3 User Data Protection

The TOE enforces an access control policy that controls access between users and devices. Access to devices is limited based upon the user identifier associated with the requestor and device service access list. A user can access a given service on a given device if the device service access control list specifically allows access to the requested service for the device. The TOE also supports two additional policies that can be configured in addition to the basic device access policy. The first policy limits access to particular sockets on devices and the second perform keyword filtering on device commands.

6.4 Identification and Authentication

The TOE requires users to provide unique identification and authentication data before any access to the system is granted. The TOE supports password, client certificate, and external LDAP authentication. The TOE also maintains security privileges used for role assignments.

6.5 Security Management

An authorized administrator is any user that has an administrative privilege. Users with no administrative privileges are simply called users. The TOE is managed through the Administrative modules (Config, Services, Sessions, Users, Devices, Policy), accessed via a SSL web-based interface. Through this interface all TOE management can be performed, including user management and the configuration of IT devices access functions. This interface is restricted to authorized administrators, which provides the administrator the ability to set user attributes and privileges, as well as assign privileges for different levels of administrative access.

Administration functions are done using PERL scripts which are triggered by input via the GUI. A spadmin daemon accepts input from specific functions on the web server to control system configuration parameters. Scripts operate the features of the optional TOE power, console, and IP based KVM device components.

6.6 Protection of the TSF

The TOE is a hardware appliance that contains a custom operating system that runs in firmware, and supports only trusted processes. The GateKeeper appliance provides no file abstractions or permanent storage for user access for "executables" to remain for further execution. Furthermore, the TOE has been carefully designed to offer well-defined interfaces that ensure that access to protected resources is subject to the applicable GateKeeper security policies. The agents are service processes on Windows or daemon processes on UNIX. In either case, the operating system provides a separate address for the agent to run. Additionally, all communication between the appliance and agent is protected using SSL. If the TOE is configured in a cluster and one GateKeeper becomes unavailable, another GateKeeper will automatically start receiving all requests and will maintain a secure state. The TOE also generates timestamps for use within the audit trail or can optionally get time from an NTP server.

7 Documentation

Following is a list of the developer provided evaluation evidence that is available to end-users:

Document	**Version**	Date
Xceedium GateKeeper Administration Guide Release 5.2.1	Version 1	January 28, 2011
Xceedium GateKeeper 5.2.1 Security Target	Version 2.9	3 February 2011

8 IT Product Testing

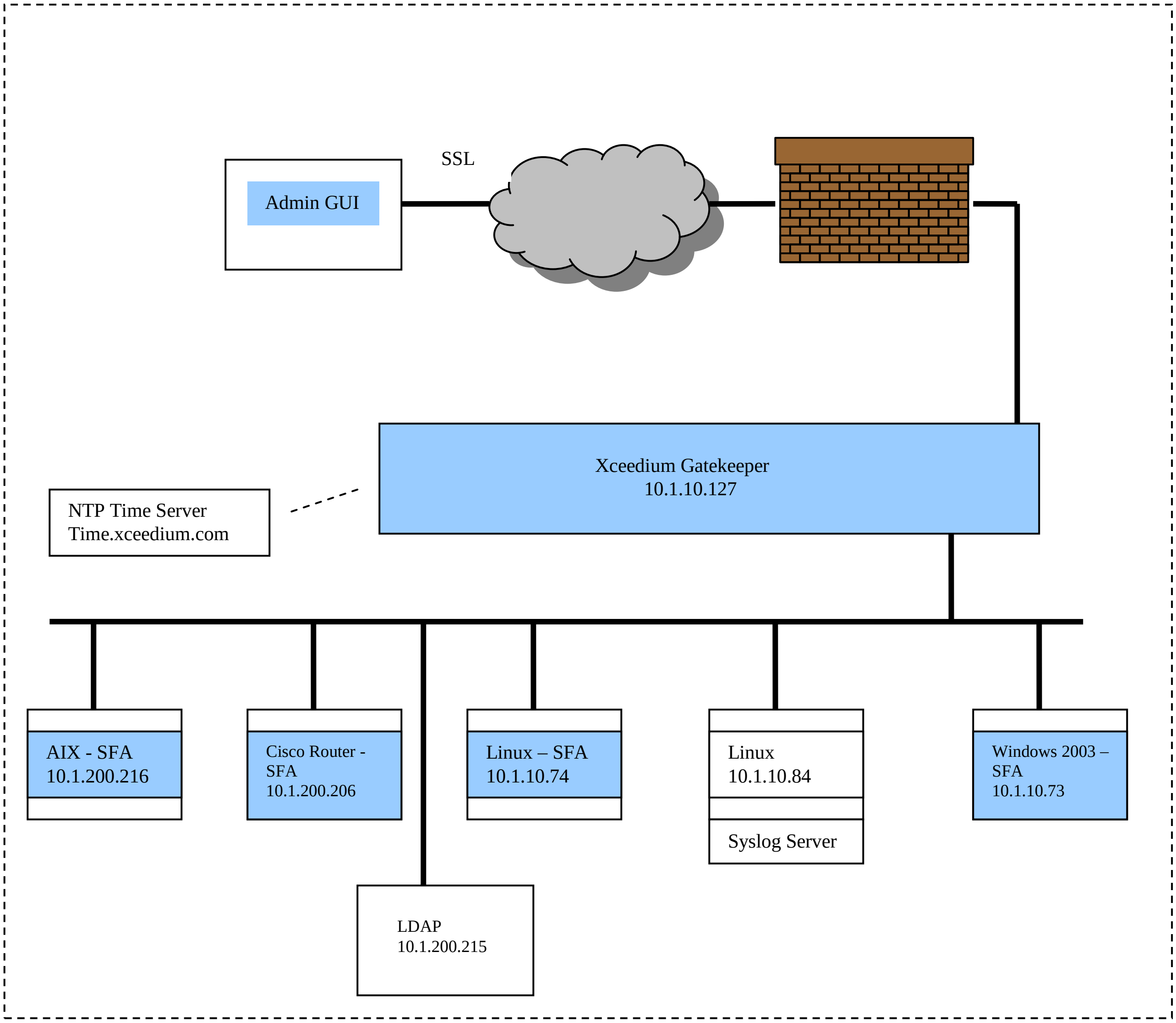
This section describes the testing efforts of the developer and the Evaluation Team.

8.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function, more specifically to the security functional requirements tested. The scope of the developer tests included all the TSFI. The testing covered the security functional requirements in the ST including: Security Audit, Cryptographic Support, Identification and Authentication, Security Management, User Data Protection, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

8.2 Evaluation Team Independent Testing

The evaluation team exercised the developer and independent team tests against the evaluated configuration of the TOE. The tests included a Windows 2003 Server, Linux (Red Hat) Server, and AIX as protected backend devices. Following is a diagram illustrating the test configuration.



In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

8.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

9 Evaluated Configuration

The TOE consists of the GateKeeper appliance, agents, and management interface. The appliance has three network interfaces – one to the unprotected network, an Agent interface and one to the protected network where it enforces a device access control policy. All users connect to the appliance using SSL via the unprotected network.

A third interface for the appliance is its LCD Panel and four configuration buttons on the front of the appliance. This external interface allows for basic network configuration of the device out of the box. Once the appliance basic network configuration has been completed via the LCD Panel and buttons that interface with the configuration firmware, the device is rebooted, and the web-based configuration of network parameters are completed via an Internet Browser (any Java-enabled web browser). Once in the evaluated configuration the appliance is assumed to be in a protected environment and the LCD Panel and buttons are not used and do not need any further description.

Agents reside on either Windows or UNIX servers on the protected network. The agents do not interface directly with users. The access control policy is pushed to the agent from the appliance where it is then applied.

The TOE web server provides an administrative interface for all TOE management functions called the Administrative Modules. From this GUI interface, the administrator manages user access. The actual browser and user workstation supporting the browser are not part of TOE.

All servers and devices on the protected network are in the IT Environment.

10 Results of the Evaluation

The evaluation was conducted in accordance with the CC and the CEM and the policies/procedures documented on the NIAP CCEVS web site (www.niap.ccevs.org). The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL4 assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. In the Final Evaluation Technical Report (ETR), all Fail or Inconclusive work unit verdicts have been resolved by the developer and the evaluation team. The details of the evaluation are recorded in the CCTL's ETR; Final Evaluation Technical Report for the Xceedium GateKeeper 5.2.1, Part 1 (Non-Proprietary) and Part 2 (Proprietary).

The evaluation confirmed that Xceedium gatekeeper 5.2.1 product is compliant with the CC functional requirements (Part 2 conformant) and assurance requirements (Part 3 conformant) for EAL4 augmented with ACL_FLR.2. The product was evaluated and tested against the claims presented in the Xceedium GateKeeper 5.2.1 Security Target, Version 2.9, 3 February 2011. The evaluation team performed independent functional and vulnerability tests as well as, a sample of the suite of the vendor tests. The evaluation team's assessment of the evaluation evidence demonstrated that the claims in the ST were met. The validation oversight reviews support the evaluation team's conclusion that Xceedium GateKeeper 5.2.1 meets the claims stated in the Security Target.

11 Validator Comments/Recommendations

All Validator concerns with respect to the evaluation have been addressed. No issues are outstanding.

12 Security Target

The Security Target is identified Xceedium GateKeeper 5.2.1 Security Target, Version 2.9, 3 February 2011. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.2.

13 List of Acronyms

The following definitions are used throughout this document:

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AGD	Administrator Guidance Document
ANSI	American National Standards Institute
CC	Common Criteria
CPU	Central Processing Unit
DDR	Double Data Rate
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication
GB	Gigabyte
GUI	Graphical User Interface
IP	Internet Protocol
IPC	Interprocess Communication
IT	Information Technology

KVM	Keyboard-Video-Mouse
LCD	Liquid Crystal Display
NTP	Network Time Protocol
PBX	Private Branch Exchange
PERL	Practical Extraction and Report Language
PP	Protection Profile
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
RSA	Rivest, Shamir, & Adleman (encryption algorithm)
SBC	Single Board Computer
SNMP	Simple Network Management Protocol
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control
TOE	Target of Evaluation
TSF	TOE Security Functions
VNC	Virtual Network Connection

14 Glossary of Terms

See the Glossary of definitions already defined by the ST, CC, or CEM

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007.

[3] Xceedium GateKeeper 5.2.1, Final Non-Proprietary ETR – Part 1, Version 2.0, 25 March 2011.

[4] Xceedium GateKeeper 5.2.1 Final Proprietary ETR – Part 2, Version 3.0 dated 25 March 2011 and Supplemental Team Test Report, Version 3.0, 25 March 2011.

[5] Xceedium GateKeeper 5.2.1 Security Target, Version 2.9, 3 February 2011.