National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

U. S. Government
Firewall Protection Profile
for Medium Robustness Environments,
Version 1.0,
Dated October 28, 2003

Report Number:	**CCEVS-VR-03-0049**
Dated:	**29 October 2003**
Version:	**1.1**

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Kathy Cunningham
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Evaluation Team
COACT, Inc., CAFÉ Lab
Rivers Ninety Five
9140 Guilford Road, Suite G
Columbia, MD 21046-2587

Table of Contents

1. Executive Summary

The evaluation of the U. S. Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0 was performed by COACT, Inc., CAFÉ Lab CCTL in the United States and was completed on 28 October 2003. The Protection Profile (PP) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the APE requirements of the Common Criteria for IT Security Evaluation (Version 2.1).

This Validation Report applies only to the specific version of the PP as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

The information contained in this Validation Report is not an endorsement of the U. S. Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0 by any agency of the US Government and no warranty of the PP is either expressed or implied.

The COACT, Inc., CAFÉ Lab evaluation team concluded that the Common Criteria requirements for a PP Evaluation have been met.

The technical information included in this report was obtained from the U. S. Government Firewall Protection Profile (PP) for Medium Robustness Environments, Version 1.0, produced by U.S Government and the U. S. Government Firewall Protection Profile for Medium Robustness Environments Evaluation Technical Report (ETR), Dated October 29, 2003, Document No. F4-1003-001(2), produced by COACT, Inc., CAFÉ Lab.

1.1 Evaluation Details

Dates of Evaluation: January 2003 through October 2003
Evaluated Protection Profile: U. S. Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0, Dated 0ctober 28, 2003
Developer: SPARTA, Aerospace, and National Security Agency (NSA), V33
CCTL: COACT, Inc., CAFÉ Lab, Columbia, MD
Validation Team: Kathy Cunningham, National Security Agency,
Ft. Meade, MD
Evaluation Class: EAL 4 augmented with ADV_IMP.2, ALC_FLR.2, ATE_DPT.2, and AVA_VLA.3
PP Conformance: N/A

1.2 Interpretations

National Interpretations

I-0405	American English Is An Acceptable Refinement, 2000-12-20
I-0407	Empty Selections Or Assignments, 2003-08-21
I-0409	Other Properties In FMT_MSA.3 Should Be Specified By Assignment, 2003-08-21
I-0410	Auditing of Subject Identity For Unsuccessful Logins, 2002-01-04
I-0414	Site Configurable Prevention of Audit Loss, 2003-07-17
I-0421	Application Notes In Protection Profiles Are Informative Only, 2001-06-22
I-0425	Settable Failure Limits Are Permitted, 2002-12-05
I-0427	Identification Of Standards, 2001-06-22
I-0429	Selecting One Or More, 2003-08-12

International Interpretations

003	Unique identification of configuration items in the configuration list, 2002-02-11
004	ACM_SCP.*.1C requirements unclear, 2001-11-12
019	Assurance Iterations, 2002-03-11
049	Threats met by environment, 2001-02-16
051	Use of ‘documentation’ without C&P elements, 2002-10-05
064	Apparent higher standard for explicitly stated requirements, 2001-02-16
065	No component to call out security function management, 2001-02-16
080	APE_REQ.1-12 does not use ‘shall examine .. to determine’, 2000-10-15
084	Separate objectives for TOE and environment, 2001-02-16
085	SOF Claims additional to the overall claim, 2002-02-11
138	Iteration and narrowing of scope, 2002-06-05

1.3 Threats to Security

The Protection Profile identified the following threats:

T.ADDRESS_MASQUERADE	A user on one interface may masquerade as a user on another interface to circumvent the TOE policy.
T.ADMIN_ERROR	An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
T.ADMIN_ROGUE	An administrator’s intentions may become malicious resulting in user or TSF data being compromised.
T.AUDIT_COMPROMISE	A malicious user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user’s action.

T.CRYPTO_COMPROMISE
A malicious user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromise the cryptographic mechanisms and the data protected by those mechanisms.

T.MASQUERADE
A user may masquerade as an authorized user or an authorized IT entity to gain access to data or TOE resources.

T.FLAWED_DESIGN
Unintentional or intentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a malicious user or program.

T.FLAWED_IMPLEMENTATION
Unintentional or intentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a malicious user or program.

T.POOR_TEST
Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered.

T.REPLAY
A user may gain inappropriate access to the TOE by replaying authentication information, or may cause the TOE to be inappropriately configured by replaying TSF data or security attributes (captured as it was transmitted during the course of legitimate use).

T.RESIDUAL_DATA
A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.

T.RESOURCE_EXHAUSTION
A malicious process or user may block others from TOE system resources (e.g., connection state tables) via a resource exhaustion denial of service attack.

T.SPOOFING
An entity may mis-represent itself as the TOE to obtain authentication data.

T.MALICIOUS_TSF_ COMPROMISE
A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.UNATTENDED_SESSION
A user may gain unauthorized access to an unattended session.

T.UNAUTHORIZED_ACCESS
A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.

T.UNIDENTIFIED_ACTIONS
The administrator may fail to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

T.UNKNOWN_STATE	When the TOE is initially started or restarted after a failure, design flaws, or improper configurations may cause the security state of the TOE to be unknown.

2. Identification

2.1 PP and TOE Identification

PP: U. S. Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0, Dated October 28, 2003.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 PP Overview

This PP specifies the minimum-security requirements for network boundary devices (hereafter referred to as the Target of Evaluation (TOE)) that provide controlled connectivity between two or more network environments used by the Department of Defense (DoD) in Medium Robustness Environments. The TOE may be a dedicated device such as a firewall, or an enhancement to some other network device such as a router. The target robustness level of "medium" is specified in the *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG)* and is further discussed in Section 3.0 of this PP.

The TOE supports user identification and authentication (I&A) where "user" is defined to be a human user acting in a role (i.e., Security Administrator, Cryptographic Administrator, and Audit Administrator) or an authorized IT entity. The TOE provides the capability to pass and block information flows based on a set of rules defined by the Security Administrator. Additionally, the TOE enforces security policies, which restrict host-to-host connections to common Internet services such as: Telnet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP). The TOE supports encryption for remote administration, remote users and authorized IT entities (e.g., certificate server, NTP server), and generates audit data of security relevant events.

This PP defines:

- assumptions about the security aspects of the environment in which the TOE will be used;
- security objectives of the TOE and its environment;
- functional and assurance requirements to meet those security objectives;
- rationale demonstrating how the requirements meet the security objectives, and how the security objectives address the threats.

The assurance requirements were originally based upon Evaluated Assurance Level (EAL) 4. In order to gain the necessary level of assurance for medium robustness environments explicit requirements have been created for some families in the ADV class both to remove ambiguity in the existing ADV requirements as well as to provide greater assurance than that associated with EAL4. The explicit assurance requirements are summarized in the Table below.

Assurance Class	Assurance Components	
Development	**ADV_ARC_EXP.1**	**Architectural Design**
	ADV_FSP_EXP.1	**Functional Specification with Complete Summary**
	ADV_HLD_EXP.1	**Security-Enforcing High-Level design**
	ADV_INT_EXP.1	**Modular Decomposition**
	ADV_LLD_EXP.1	**Security-Enforcing Low-Level design**
Vulnerability assessment	**AVA_CCA_EXP.2**	**Systematic cryptographic module covert channel analysis**

These explicit assurance requirements were deemed necessary by NSA to reduce the ambiguity in the associated CC assurance families and to provide the level of assurance appropriate for medium robustness environments. For more detail information on the assurance requirements, reference Section 5.3 of this PP.

2.3 IT Security Environment

This Protection Profile provides functional requirements for the IT Environment. The IT environment includes authorized IT entities (e.g., a certificate authority server, NTP server) and any IT entities that are used by administrators to remotely administer the TOE.

3. Security Policy

The Operational Security Policies defined for the TOE.

P.ACCESS_BANNER
The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

P.ACCOUNTABILITY
The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.ADMIN_ACCESS
Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.

P.CRYPTOGRAPHIC_FUNCTIONS
The TOE shall provide cryptographic functions for its own use, including encryption/decryption and digital signature operations.

P.CRYPTOGRAPHY_VALIDATED
Where the TOE requires FIPS-approved security functions, only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.;

generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key distribution, and random number generation services).

P.VULNERABILITY_ANALYSIS_TEST The TOE must undergo appropriate independent vulnerability analysis and penetration testing to demonstrate that the TOE is resistant to an attacker possessing a medium attack potential.

4. Assumptions

Personnel and Physical Assumptions

The specific conditions below are assumed to exist in a PP-compliant TOE environment.

A.NO_GENERAL_PURPOSE The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.

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

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

5. Architectural Information

TOEs claiming conformance to this Protection Profile (PP) are network boundary devices that provide controlled connectivity between two or more network environments used by the Department of Defense (DoD) in Medium Robustness Environments. The TOE may be a dedicated device such as a firewall, or an enhancement to some other network device such as a router. The target robustness level of "medium" is specified in the *Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG)* and is further discussed in Section 3.0 of the PP.

It is required that all hardware and software components necessary to construct a complete TOE are included in any Security Targets (ST) claiming conformance to this PP. The TOE functional requirements can be categorized as follows: Identification and Authentication, Administration, Information Flow Control, Trusted Channel/Path, Encryption, and Audit.

6. Documentation

U.S. Government, Firewall Protection Profile for Medium Robustness Environments, Version 1.0, Dated October 28, 2003.

7. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the APE section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the APE 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 PP.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., APE) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. No constraints or assumptions were identified in performing this evaluation.

Chapter 3, Evaluation Results, in the Evaluation Team's ETR, states:

"The *U.S. Government Firewall Protection Profile (PP) for Medium Robustness Environments* was successfully evaluated."

Chapter 4, Conclusions, in the Evaluation Team's ETR, states:

"The *U.S. Government Firewall Protection Profile for Medium Robustness Environments* has satisfied the requirements of the *APE Assurance Requirement*s. The PP was assessed against the requirements as stated in the *Common Methodology for Information Technology Security Evaluation Part 2, Version 1*.0."

8. Validation Comments/Recommendations

The validation team had no recommendations concerning the U. S. Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0.

Comments

The explicit cryptographic security functional requirements may seem long and complex as stated by the evaluators in the ETR. The purpose of these requirements is to guide the product developer in choices that are required for the FIPS 140-2 options. These requirements have specifics to tighten the cryptographic functions and bring the security level up to meet the medium robustness requirements.

The refinement for FPT_SEP.2-3 reflects the intent of the PP author, that the cryptographic portion of the TOE is maintained within its own address space.

Some of the Threats are not addressed by the TOE described herein: This arises from a misunderstanding of what threat statements are and has been propagated into this PP from other PPs.

This PP evaluation precedes the publication of the Consistency Manual for Medium Robustness Environment Profiles, which at the time of certification was under development.

9. Abbreviations

Abbreviations	Long Form
ASE	Advanced Encryption Standard
ATM	Asynchronous Transfer Method
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CM	Configuration Management
DES	Data Encryption Standard
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Patrol
ETR	Evaluation Technical Report
FIPS PUB	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
GIG	Global Information Grid
HTTP	Hypertext Transfer Protocol
IATF	Information Assurance Technical Framework
ICMP	Internet Control Message Protocol
ID	Identification
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSEC ESP	Internet Protocol Security Encapsulating Security Payload
IT	Information Technology
I&A	Identification and Authentication
MRE	Medium Robustness Environment
NBIAT&S	Network Boundary Information Assurance Technologies and Solutions Support
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OR	Observation Report
PC	Personal Computer
PKI	Public Key Infrastructure
PP	Protection Profile
QA	Quality Assurance
RNG	Random Number Generator
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function

Abbreviations	Long Form
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
UDP	User Datagram Protocol
URL	Uniform Research Locator
VPN	Virtual Private Network

10. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme

Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 1.0, August 2000.

[GIG] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG), June 2000.