National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

U.S. Government
Virtual Private Network (VPN) Boundary Gateway
Protection Profile for Medium Robustness Environments

Report Number: CCEVS-VR-06-0015

Dated: 21 April 2006

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Thomas Murphy

Mitretek Systems

Linthicum, Maryland

Dr. Jerome Myers

The Aerospace Corporation

Columbia, Maryland

Common Criteria Testing Laboratory

COACT, Incorporated

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validation team's assessment of the evaluation of the U.S. Government Virtual Private Network (VPN) Boundary Gateway Protection Profile for Medium Robustness Environments. It presents the evaluation results, their justifications, and the conformance results. It acknowledges that the requirements listed in the Protection Profile (PP) are comprehensive and consistent and may be used to develop products whose security targets, which conform to this profile, will satisfy the needs of the sponsoring Government Agency. This PP was generated under the Enclave Boundary Security Technologies and Solutions (EBST&S) Support Program, sponsored by the Security Agency (NSA).

The evaluation was performed by COACT Incorporated, an accredited Common Criteria Testing Laboratory (CCTL), and was completed during April 2006. The information in this report is largely derived from the PP, provided by the EBST&S Support Program of the NSA, and the Evaluation Technical Report (ETR) written by COACT. All security functional requirements are derived from Part 2 of the Common Criteria or special explicitly stated requirements using the format of the CC.

A VPN boundary gateway is a component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network. IP packets crossing from the private network to the public network will be encrypted if their destination is to another private network supporting the same VPN policy as the source network. Encryption of all packets between the two networks assures that the data communicated between the two networks is kept private, even though it traverses a public network.

Products, that is, Targets of Evaluation (TOE), that conform to this PP will provide the following security functions in its evaluated configuration:

- Identification and Authentication –The TOEs will exchange identities and will perform two types of authentication: device-level authentication of the remote device (peer TOEs, remote VPN gateways or VPN clients) and user authentication of the Authorized Administrator.

- Administrative roles - The TOE requires three separate administrative roles: Cryptographic Administrator, Audit Administrator and Security Administrator.

- Audit – The TOE provides for the detection of auditable events, the generation of audit records and alarms, and for audit management.

- Trusted Channel/Trusted Path - The TOE is required to provide two types of encrypted communications: trusted channel and trusted path. Trusted channel refers to the encrypted connection between the TOE and a non-human external source. Trusted path refers to the encrypted connection used to authenticate an external human user with the TOE.

- Encryption – the TOE must establish encrypted communications (acting as the initiator or responder) with authorized remote users and external IT entities. The PP defines the

minimum set of cryptographic attributes required by the TOE. The TOE's cryptographic module(s) must be FIPS PUB 140-2 validated and must meet, as a minimum, the security requirements of "Security Level 1". The ST author may implement the cryptographic module(s) in hardware, software, or a combination of both.

- The TOE shall implement VPN mechanisms using cryptography, key management, access control, authentication, and data integrity. There are several RFCs covering this area to which the TOE must conform. More notably, TOEs meeting this PP will implement and conform to the Internet Engineering Task Force (IETF) Internet Protocol Security (IPSEC) Encapsulating Security Payload (ESP) protocol as specified in RFC 2406.

- Information Flow Control – The TOE supports two information flow control policies: VPN and unauthenticated TOE services.

Further information about these security functions is provided in Section 3 on page 3 of this report.

The validation team monitored the activities of the COACT evaluation team, reviewed successive versions of the Protection Profile, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and customer responses. The validation team determined that the evaluation showed that the PP satisfies all of the APE security assurance requirements according to the Common Criteria for Information Technology Security Evaluation, Version 2.1 and Part 2 of the Common Methodology for Information Technology Security Evaluation, Version 2.1. Therefore, the validation team concludes that the COACT findings are accurate, the conclusions justified, and the conformance claims correct.

The information contained in this Validation Report is not an endorsement of the PP by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product and protection profile 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products or protection profiles 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 protection profile, including:

- The Protection Profile (PP): the fully qualified identifier of the PP as evaluated;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	Virtual Private Network(VPN) Boundary Gateway Protection Profile for Medium Robustness Environments, Version 1.0, February 23, 2006
Evaluation Technical Report	Evaluation Technical Report for the U.S. Government Virtual Private Network Boundary Gateway Protection Profile for Medium Robustness Environments, April 21, 2006
Version of CC	CC Version 2.1 [1], [2], [3], [4] and all applicable NIAP CCEVS and International Interpretations effective on July 10, 2002
Version of CEM	CEM Version 1.0 [5], and all applicable NIAP CCEVS and International Interpretations effective on July 10, 2002
Sponsor	National Security Agency (NSA) Enclave Boundary Security Technologies and Solutions Support Program
Developer	National Security Agency (NSA) Enclave Boundary Security Technologies and Solutions Support Program
Evaluators	COACT Incorporated
Validation Team	Tom Murphy: Mitretek Systems Dr. Jerome Myers: The Aerospace Corporation

2.1. Applicable Interpretations

The following NIAP CCEVS and International interpretations applied to this evaluation:

NIAP CCEVS Interpretations:

I-0405 – American English Is An Acceptable Refinement, 2000-12-20

I-0406 – Automated Or Manual Recovery Is Acceptable, 2003-07-17

I-0407 – Empty Selections Or Assignments, 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-0415 – User Attributes To Be Bound Should Be Specified, 2002-03-04

I-0421 – Application Notes in Protection Profiles Are Informative Only, 2001-06-22

I-0423 – Some Modifications To The Audit Trail Are Informative Only, 2001-06-22

i-0435 – Settable Failure Limits Are Permitted, 2000-12-05

I-0427 – Identification of Standards, 2001-06-22

I-0429 – Selecting One Or More, 2003-08-12

International Interpretations:

RI #3 – Unique identification of configuration items in the configuration list, 2002-02-11

RI #4 – ACM_SC..1C requirements unclear, 2001-11-12*

RI #19 – Assurance Iterations, 2002-02-11

RI #49 – Threats me by the Environment, 2001-02-16

RI #51 (Rev1) – Use of documentation without C & P elements, 2002-10-25

RI #64 – Apparent higher standard for explicitly stated requirements, 2001-02-16

RI #65 – No component to call out security function management, 2001-07-31

RI #84 – Aspects of objectives in TOE and environment, 2001-02-16

RI #85 – SOF Claims additional to the overall claim, 2002-02-11

RI #138 – Iteration and narrowing of scope, 2002-06-05

RI #137 – Rules governing binding should be specifiable, 2004-01-30

3. SECURITY POLICY

The PP requires that conformant TOEs satisfy security requirements that provide the following security policies: Identification and Authentication, Adminstrative Roles, Audit, Trusted Channel/Trusted Path, Encryption, and Information Flow. These policies are described in the following subsections.

3.1. Identification and Authentication Policy

The TOE will exchange identities and will perform two types of authentication: device-level authentication of the remote device (peer TOEs, remote VPN gateways or VPN clients) and user authentication of the Authorized Administrator. Device-level authentication enables a TOE to construct a secure channel with a trusted peer. The secure channel should be established only after each device authenticates itself. Device-level authentication is performed using authentication techniques specified in RFC 2409. The TOE will assure that the trust establishment is mutual. In other words, peers will mutually authenticate themselves to each other before establishing the secure channel.

3.2. Administrative Role Policy

"Administrators" refers to the roles assigned to the individuals responsible for the installation, configuration, and maintenance of the TOE. The TOE requires three separate administrative roles: Cryptographic Administrator, Audit Administrator and Security Administrator. The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE. The Audit Administrator is responsible for the regular review of the TOE's audit data. The Security Administrator is responsible for all other administrative tasks (e.g., creating the TOE security policy) not addressed by the other two administrative roles. It is important to note that while this PP requires the three administrative roles outlined above, it provides the ST author the option of including additional administrative roles as well.

3.3. Audit Policy

The PP requires that conformant TOEs provide generation of auditable events, audit records, alarms and audit management functionality. The PP lists the minimum set of auditable events that must be available to the Security Administrator for configuration on the TOE. Each auditable event must generate an audit record. The PP also provides a minimum list of attributes that must be included in

each audit record. The ST author may include additional auditable events and audit record attributes. If the ST author includes any additional functional requirements not specified by this PP, they must consider any security relevant events associated with those requirements and include them in the TOE's list of auditable events and records. In addition to generating auditable events, the TOE must monitor their occurrences and provide a Security Administrator configurable threshold for determining a potential security violation. Once the TOE has detected a potential security violation, an alarm is generated and a message is displayed at the TOE's local console as well as each active remote administrator console (all administrative roles included). Additionally, the Security Administrator can configure the TOE to generate an audible alarm to indicate a potential security violation. If an administrator console is not active, the TOE stores the message for display when the console becomes active (e.g. when the administrator establishes a remote session to the TOE). The message must contain the potential security violation and all audit records associated with the potential security violation. The message will be displayed at the various consoles until administrator acknowledgement of the message has occurred. As mentioned in the "Administrative" section above, the Audit Administrator's role is restricted to viewing the contents of the audit records and the deletion of the audit trail. The TOE does provide the Audit Administrator with a sorting and searching capability to improve audit analysis. The Security Administrator configures auditable events, backs-up and deletes audit data, and manages audit data storage. The TOE provides the Security Administrator with a configurable audit trail threshold to track the storage capacity of the audit trail. As soon as the threshold is met, the TOE generates an alarm and displays a message in the same fashion as described above, including the option of the audible alarm. In addition to displaying the message, the Security Administrator may configure the TOE to prevent all auditable events except for those performed by the Security and Audit Administrators or overwrite the oldest audit records in the audit trail.

Audit events include modifications to the group of individuals associated with the Authorized Administrator roles; use of the identification and authentication mechanisms (including any attempted reuse of authentication data); changes made to the TOE's security policy rules, mechanisms and data; actions taken due to imminent security violations; decisions made by the TOE to enforce security policy rules; changes to the TOE's date and time; and the use of other security functions. The decision to record auditable events will be made in accordance with organizational security policy and implemented by the Authorized Administrator. If the audit trail becomes full then the only auditable events that are recorded are those performed by the Authorized Administrator. Audit trail data is stamped with a dependable date and time when recorded.

3.4. Trusted Channel/ Trusted Path

The PP requires conformant TOEs to provide two types of encrypted communications: trusted channel and trusted path. Trusted channel refers to the encrypted connection between the TOE and a non-human external source. An encrypted connection between the TOE and authorized Information Technology (IT) entities (e.g., NTP server, certificate authority) is an example of trusted channel encryption. Trusted path refers to the encrypted connection used to authenticate an external human user with the TOE. Remote administrators establishing an encrypted link to authenticate to the TOE

are examples of trusted path encryption. The remote administrator's communication must remain encrypted throughout the remote session.

3.5. TOE Encryption Policy

The PP requires that conformant TOEs must establish encrypted communications (acting as the initiator or responder) with authorized remote users and external IT entities. The PP defines the minimum set of cryptographic attributes required by the TOE. The TOE's cryptographic module(s) must be FIPS PUB 140-2 validated and must meet, as a minimum, the security requirements of "Security Level 1". The ST author may implement the cryptographic module(s) in hardware, software, or a combination of both. The TOE must generate and distribute symmetric and asymmetric keys. The ST author is provided several implementation selections for key generation and may distribute keys manually, electronically, or both. The TOE must perform data encryption/decryption using the Advanced Encryption Standard (AES) algorithm with a minimum key size of 128 bits. Additional requirements for key destruction, digital signature generation/verification, random number generation and cryptographic hashing are provided in section 5.1.2.

The TOE shall implement VPN mechanisms using cryptography, key management, access control, authentication, and data integrity. TOEs meeting this PP will implement and conform to the Internet Engineering Task Force (IETF) Internet Protocol Security (IPSEC) Encapsulating Security Payload (ESP) protocol as specified in RFC 2406. All VPN traffic between peer TOEs shall use tunnel mode, support for transport mode is optional. TOE encryption mechanisms will conform to IETF *ESP CBC-Mode Cipher Algorithms* as specified in RFC 2451. The TOE shall, at a minimum, implement the Rijndael algorithm as specified in the Advanced Encryption Standard (AES), FIPS PUB 197. TOE data integrity mechanisms will conform to IETF *Use of HMAC-SHA-1-96 within ESP and AH* as specified in RFC 2404. The TOE shall utilize cryptographic modules that are conformant with FIPS PUB 140-2. The TOE shall perform key management and key exchange using the IETF specified Internet Key Exchange (IKE) (RFC 2409) which shall be FIPS PUB 140-2 compliant.

3.6. TOE Information Flow Policy

The PP requires a conformant TOE to support two information flow control policies: VPN and unauthenticated TOE services. The TOE's VPN SFP is instantiated by a device at each enclave boundary. The TOE is a VPN functional component that may either be hosted on a firewall or router, or may be a dedicated VPN gateway device. If the TOE is a firewall or router with VPN capability, the entire device, including all software and hardware that can affect the security functions and assurances of the VPN must meet the assurance requirements of this protection profile. Each TOE authenticates itself to the remote device (peer TOE, remote VPN gateway or VPN client), agrees upon cryptographic keys and algorithms, securely generates and distributes session keys as necessary, and encrypts network traffic in accordance with the TOE security policy. The TOE will enforce the same security policy between communicating peers.

The TOE will enforce a security policy as follows:

- for outbound traffic associated with a peer TOE, a remote VPN gateway or a VPN client, the local TOE will create or use an existing secure channel between the remote device if there exists an information flow control rule specifying that communication between the source and destination IP addresses must be encrypted;

- for outbound traffic not associated with a peer TOE, remote VPN gateway or VPN client, the local TOE will not invoke the security mechanisms and a secure channel will not be established;

- for inbound traffic associated with a peer TOE, remote VPN gateway or VPN client, the local TOE will create or use an existing secure channel between the devices if there exists an information flow control rule specifying that communication between the source and destination IP addresses must be encrypted; and

- for inbound network traffic not associated with a peer TOE, remote VPN gateway or VPN client, the local TOE will not invoke the security mechanisms and a secure channel will not be established.

The unauthenticated TOE services information flow control policy supported by the TOE provides the rules that apply to the unauthenticated use of any services provided by the TOE. ICMP is the only service that is required to be provided by the TOE, and the security attributes associated with this protocol allow the Security Administrator to specify what degree the ICMP traffic is mediated (i.e., the ICMP message type and code).

4. ASSUMPTIONS

This PP has only minor differences in its threats, policies, and assumptions from those recommended by the *Consistency Manual for the Development of U.S. Government Protection Profiles for use in Medium Robustness Environments, Version 3.0*. The target robustness level of "medium" is specified in the Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG). A medium robustness TOE is considered sufficient protection for environments where the likelihood of an attempted compromise is medium. This implies that the motivation of the threat agents will be average in environments that are suitable for TOEs of medium robustness. Note that while highly sophisticated threat agents will not be motivated to use great expertise or extensive resources in an environment where medium robustness is suitable, the wide spread availability of exploits and hacking tools available on the Internet provide less sophisticated threat agents with expertise (and indirectly resources) that they otherwise might not have access to. Medium Robustness Environments are also further discussed in section 3.0 of the subject PP and the above referenced consistency manual.

4.1. Environmental Assumptions

The following assumptions were made about the security environment and intended usage of the TOE:

- There are no general –purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.
- Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.

The first two assumptions are the standard recommendations for Medium Robustness environments. The third assumption is a common assumption for enclave boundary protection devices. Enclave boundary protection devices are only effective if the environment is configured so that all appropriate enclave traffic that crosses the enclave boundary is directed to pass through the boundary protection device.

4.2. Threats, Policies, and Clarification of Scope

Products that comply with this PP are considered to be suitable for use in Medium Robustness environments. There are twenty six stated Threats and Polices that are addressed by this PP. They are not stated here because they are almost precisely the same as the twenty three Threats and Policies that are recommended in the *Consistency Manual for the development of U.S. Government Protection Profiles for use in Medium Robustness Environments, Version 3.0*. The most noteworthy differences are the absence of the recommended threat, T.EAVESDROP, and the inclusion of a related additional policy, P.INTEGRITY,.

P.INTEGRITY states the following:

- The TOE shall support the IETF *Internet Protocol Security Encapsulating Security Payloa*d (IPSEC ESP) as specified in RFC 2406. Sensitive information transmitted to a peer TOE shall apply integrity mechanisms as specified in *Use of HMAC-SHA-1-96 within ESP and AH* (RFC 2404).

5. ARCHITECTURAL INFORMATION

TOEs claiming conformance to this PP are VPN boundary gateway devices used by the Department of Defense in Medium Robustness Environments. The operational environment for the TOE is at the boundary between a private network and a less-trusted network (e.g., the Internet). While the VPN gateway is a part of the private network, and its primary function is to protect data communication between private networks, it is exposed to threats from the less-trusted network.

A VPN boundary gateway is a component that performs encryption and decryption of IP packets as they cross the boundary between a private network and a public network. IP packets crossing from the private network to the public network will be encrypted if their destination is to another private network supporting the same VPN policy as the source network. Encryption of all packets between the two networks assures that the data communicated between the two networks is kept private, even though it traverses a public network. The TOE may be a dedicated device or an enhancement of some other network device, such as a firewall or router.

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.

6. RESULTS OF THE EVALUATION

The U.S. Government Virtual Private Network Boundary Gateway Protection Profile for Medium Robustness Environments has satisfied the evaluation requirements of the APE section of the CEM. The PP was assessed against the protection profile requirements as stated in the Common Criteria for Information Technology Security Evaluation Version 2.1 and all applicable CCEVS and International Interpretations in effect as of July 10, 2002.

7. VALIDATOR COMMENTS

The cryptography requirements section of this PP is quite extensive. The primary function of a VPN Boundary Gateway is the protected communication service that it provides to its environment. Many of the security requirements levied on the TOE are essential for the TOE to provide that communication service with meaningful assurance. However, the bulk of the protected communication service is provided to the environment through the correct implementation of a suite of encryption protocols and communication protocols that comply with published standards. Those standards include many detailed options; some of which are not suitable for Medium Robustness Environments. The extensive cryptography requirements section of this PP is needed to ensure the specification of the acceptable cryptographic options within the applicable standards.

8. LIST OF ACRONYMS

AES	Advanced Encryption Standard
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory

CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
EBST&S	Enclave Boundary Security Technologies and Solutions
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PP	Protection Profile
RFC	Request for Comments
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network

9. BIBLIOGRAPHY

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

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

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

[4] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[5] U.S. Government Virtual Private Network (VPM) Boundary Gateway Protection Profile (PP) for Medium Robustness Environments, Version 1.0, dated February 23, 2006.

[6] U.S. Government Virtual Private Network (VPM) Boundary Gateway Protection Profile (PP) for Medium Robustness Environments Evaluation Technical Report, dated April 21, 2006.